

OpenVPN dans pfsense :

```
Starting syslog...done.
Starting CRON... done.
pfSense 2.6.0-RELEASE amd64 Mon Jan 31 19:57:53 UTC 2022
Bootup complete

FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)

VMware Virtual Machine - Netgate Device ID: 456d297e4f64e8a71d81

*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.18.135/24
LAN (lan)      -> em1      -> v4: 192.168.1.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option: █
```

pfSense - Login

Non sécurisé | <https://192.168.18.135>

Gmail YouTube Maps

pfSense

Login to pfSense

SIGN IN

admin

.....

SIGN IN

- Username : admin
- Password : pfsense

The screenshot shows the pfSense Status Dashboard. The left sidebar contains system information: FreeBSD 12.3-STABLE, CPU Type (Intel(R) Core(TM) i5-7300U), Hardware crypto, Kernel PTI (Enabled), MDS Mitigation (Inactive), Uptime (00 Hour 07 Minutes 13 Seconds), Current date/time (Sun Feb 12 19:36:43 UTC 2023), DNS server(s) (127.0.0.1, 192.168.18.2), Last config change (Sat Feb 11 21:37:18 UTC 2023), State table size (0% (83/19000)), MBUF Usage (0% (2376/1000000)), Load average (0.36, 0.70, 0.47), CPU usage (21%), Memory usage (68% of 190 MiB), and SWAP usage (4% of 1024 MiB). The right sidebar shows a message about upgrading to a Netgate Global Technical Assistance Center (TAC) Support subscription, followed by a table of network interfaces.

Interface	Speed	Duplex	IP Address
WAN	1000baseT	<full-duplex>	192.168.18.135
LAN	1000baseT	<full-duplex>	192.168.1.1

- ✓ Pfsense est configuré avec des interfaces WAN et LAN fonctionnelles on peut commencer la configuration du VPN.
- ✓ On va utiliser l'authentification par mot de passe et l'authentification par certificat.

Génération de l'autorité de certification (CA)

- Sélectionner Cert. Manager dans le menu de System.

The screenshot shows the pfSense System menu. The 'System' menu is open, and 'Cert. Manager' is highlighted. The menu options are: Advanced, Cert. Manager, General Setup, High Avail. Sync, Logout (admin), Package Manager, Register, Routing, Setup Wizard, Update, User Manager, and Release Date: Thu Nov 12 2020.

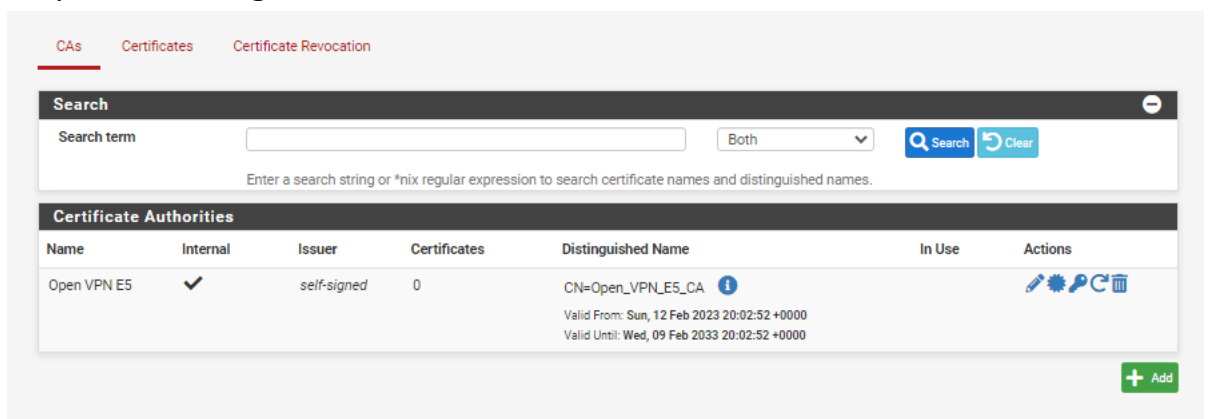
- Cliquez sur le bouton ajouter en bas à droite.

The screenshot shows the 'Certificate Authorities' section of a management interface. At the top is a search bar with the placeholder text 'Enter a search string or *nix regular expression to search certificate names and distinguished names.' Below the search bar is a table with the following columns: Name, Internal, Issuer, Certificates, Distinguished Name, In Use, and Actions. The table contains one entry for 'VPNE5-CA', which is marked as 'Internal' (checked), 'self-signed', and has 2 certificates. The distinguished name is 'O=CFA INSTA, L=PARIS, CN=VPNE5-CA, C=FR'. The 'In Use' column shows a green checkmark. The 'Actions' column contains icons for edit, refresh, and delete. At the bottom right of the table is a green '+ Add' button.

- Saisissez un nom pour votre autorité de certification. J'ai nommé Open VPN E5.
- Assurez-vous que Méthode est défini sur Créer une autorité de certification interne.
- Sélectionnez votre type de clé. J'ai gardé RSA.
- Définissez la longueur de votre clé. J'ai gardé 2048.
- Définissez votre algorithme Digest. J'ai gardé sha256.
- Temps de vie (lifetime days) j'ai gardé 3065.
- Choisissez un nom commun pour votre certificat ou laissez la valeur par défaut internal-ca. J'ai utilisé Open_VPN_E5_CA.

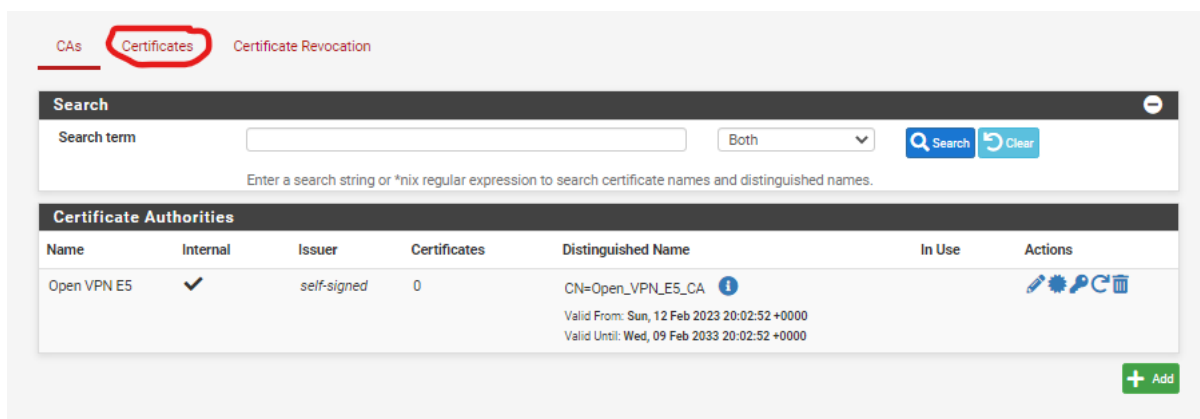
The screenshot shows the 'Create / Edit CA' form in the Certificate Manager. The form is divided into two main sections: 'Create / Edit CA' and 'Internal Certificate Authority'. The 'Create / Edit CA' section includes fields for 'Descriptive name' (Open VPN E5), 'Method' (Create an Internal Certificate Authority), 'Trust Store' (Add this Certificate Authority to the Operating System Trust Store), and 'Randomize Serial' (Use random serial numbers when signing certificates). The 'Internal Certificate Authority' section includes fields for 'Key type' (RSA), 'Key length' (2048), 'Digest Algorithm' (sha256), 'Lifetime (days)' (3065), 'Common Name' (Open_VPN_E5_CA), 'Country Code' (None), 'State or Province' (e.g. Texas), 'City' (e.g. Austin), 'Organization' (e.g. My Company Inc), and 'Organizational Unit' (e.g. My Department Name (optional)). A 'Save' button is located at the bottom of the form.

- Cliquez sur enregistrer en bas et votre autorité de certification sera créé.



Génération du certificat du serveur

- Sélectionner Certificat.



- Dans le sous-menu Certificats, cliquez sur le bouton Ajouter/Signer en bas à droite.
- Assurez-vous que Méthode est défini sur Créer un certificat interne.
- Entrez un nom descriptif pour votre certificat.
- Utilisez les mêmes valeurs que vous avez définies pour l'autorité de certification pour le type et la longueur de la clé, ainsi que pour l'algorithme Digest.
- Définissez la durée de vie sur 365 jours.
- Sélectionnez Certificat de serveur comme Type de certificat.

Add/Sign a New Certificate

Method

Create an internal Certificate

Descriptive name

Open VPN E5 Certificat

Internal Certificate

Certificate authority

Open VPN E5

Key type

RSA

2048

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

Digest Algorithm

sha256

The digest method used when the certificate is signed.
The best practice is to use an algorithm stronger than SHA1. Some platforms may consider weaker digest algorithms invalid

Lifetime (days)

365

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

Open_VPN_E5_CA

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

Country Code

None

State or Province

e.g. Texas

City

e.g. Austin

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

FQDN or Hostname

Type

Value

Enter additional identifiers for the certificate in this list. The Common Name field is automatically added to the certificate as an Alternative Name. The signing CA may ignore or change these values.

Add

+ Add

Save

➤ Cliquez sur enregistrer en bas et votre certificat sera créé.

CAs

Certificates

Certificate Revocation

Search

Search term









Both

Search

Clear

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

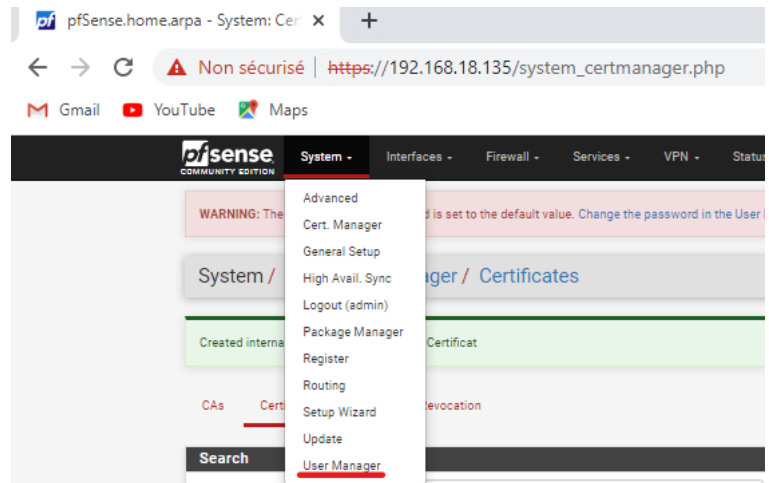
Certificates

Name	Issuer	Distinguished Name	In Use	Actions
webConfigurator default (63e7fae3d7e46) Server Certificate CA: No Server: Yes	self-signed	O=pfSense webConfigurator Self-Signed Certificate, CN=pfSense-63e7fae3d7e46 Valid From: Sat, 11 Feb 2023 20:30:27 +0000 Valid Until: Fri, 15 Mar 2024 20:30:27 +0000	webConfigurator	   
Open VPN E5 Certificat Server Certificate CA: No Server: Yes	Open VPN E5	CN=Open_VPN_E5_CA Valid From: Sun, 12 Feb 2023 20:21:17 +0000 Valid Until: Mon, 12 Feb 2024 20:21:17 +0000		   

+ Add/Sign

Création de notre utilisateur OpenVPN et notre certificat utilisateur

- Sélectionner gestionnaire d'utilisateurs dans le menu de System.



- Cliquez sur le bouton ajouter en bas à droite.
- Entrez un nom d'utilisateur et un mot de passe pour votre utilisateur. J'ai utilisé > Nom d'utilisateurs : **OpenVPNE5user** et Mdp : **pfsense**.

A screenshot of the 'System / User Manager / Users / Edit' page in pfSense. The page shows the 'User Properties' section with fields for Username (OpenVPNE5user), Password, Full name, Expiration date, and Custom Settings. The 'Group membership' section shows the user is a member of the 'admins' group. The 'Keys' section has fields for Authorized SSH Keys and IPsec Pre-Shared Key. A 'Save' button is at the bottom.

- Cliquez sur enregistrer et votre utilisateur sera créé.

System / User Manager / Users

Users

Groups

Settings

Authentication Servers

Users

	Username	Full name	Status	Groups	Actions
<input checked="" type="checkbox"/>	OpenVPNE5user		✓		
<input type="checkbox"/>	admin	System Administrator	✓	admins	

Add

Delete

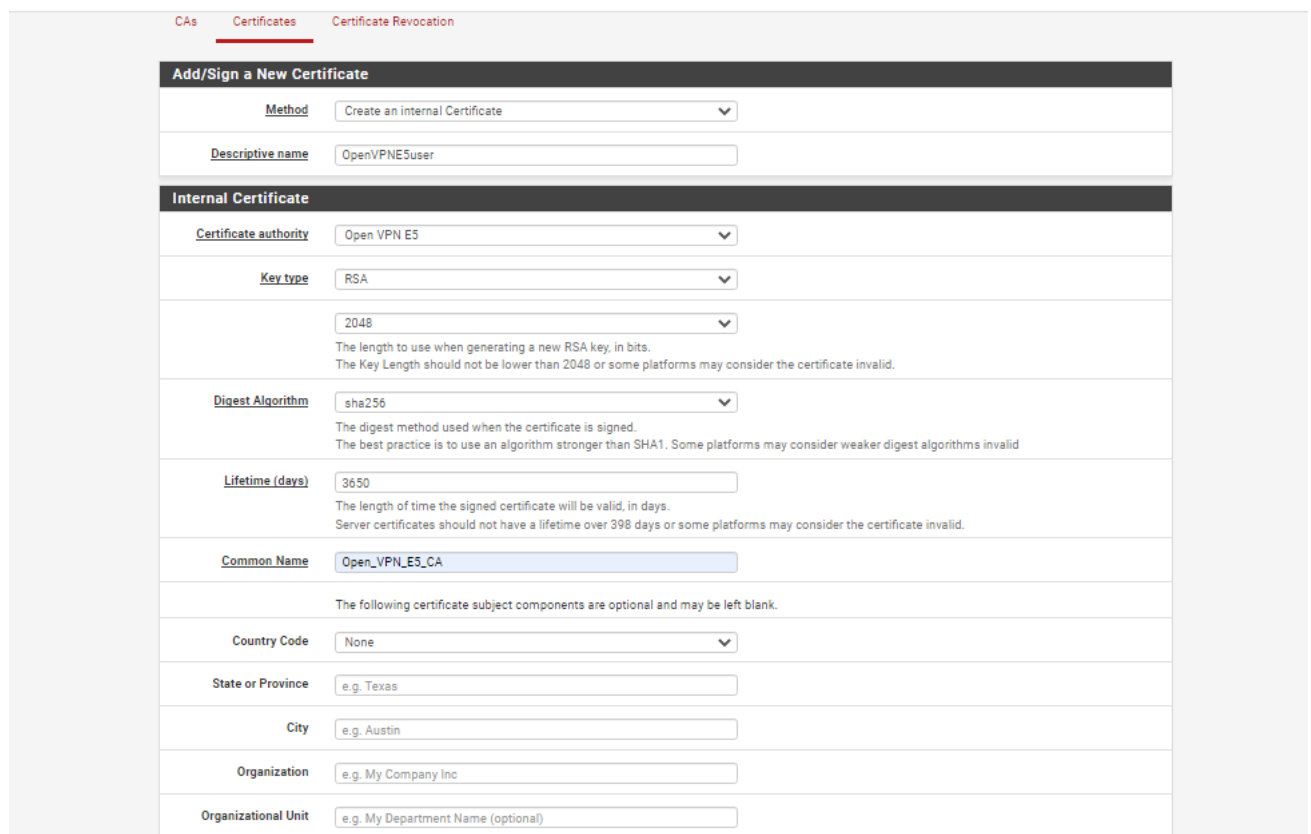
- Pour créer le certificat de l'utilisateur aller dans modifier l'utilisateur puis dans la partie user certificates cliquez sur ajouter.



Name	CA
------	----

+ Add

- On va mettre la même chose que pour le certificat du serveur puis cliquez sur ajouter.



CA's Certificates Certificate Revocation

Add/Sign a New Certificate

Method Create an internal Certificate

Descriptive name OpenVPNESuser

Internal Certificate

Certificate authority Open VPN E5

Key type RSA

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

Digest Algorithm sha256
The digest method used when the certificate is signed.
The best practice is to use an algorithm stronger than SHA1. Some platforms may consider weaker digest algorithms invalid

Lifetime (days) 3650
The length of time the signed certificate will be valid, in days.
Server certificates should not have a lifetime over 398 days or some platforms may consider the certificate invalid.

Common Name Open_VPN_E5_CA

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

Country Code None

State or Province e.g. Texas

City e.g. Austin

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 User 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 FQDN or Hostname
Type Value
Enter additional identifiers for the certificate in this list. The Common Name field is automatically added to the certificate as an Alternative Name. The signing CA may ignore or change these values.

Add + Add

Save

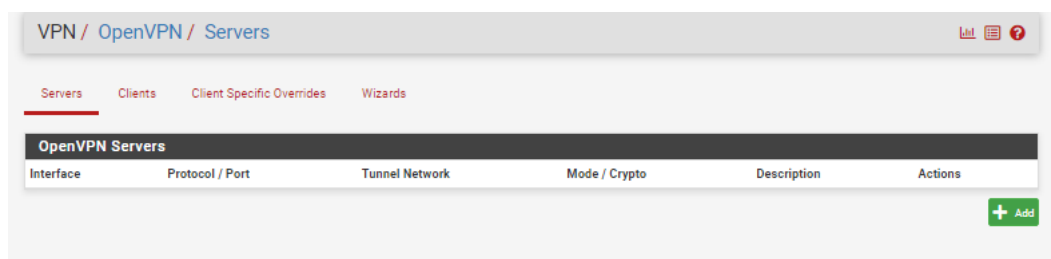
- Vous êtes redirigé automatiquement vers le gestionnaire d'utilisateur.



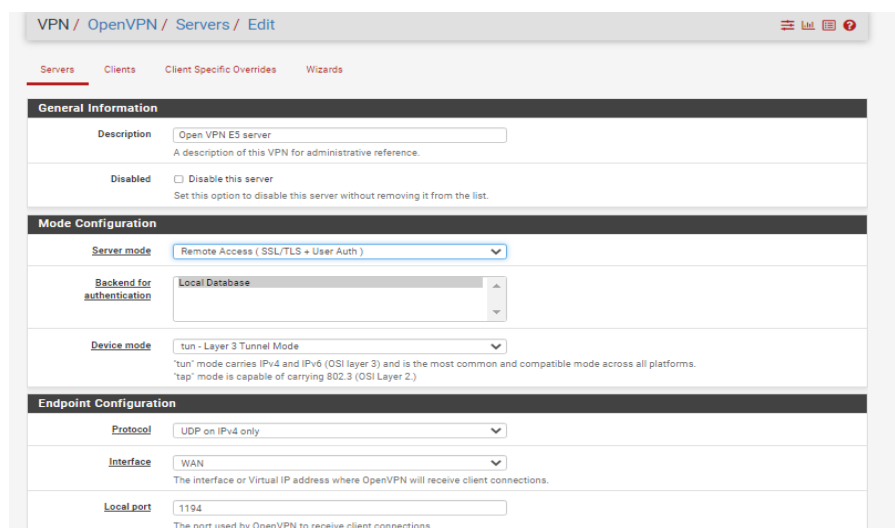
- Cliquez sur enregistrer en bas pour finir.

Création du serveur OpenVPN

- Sélectionner VPN dans le menu puis OpenVPN.



- Cliquez sur ajouter en bas à droite.
- Entrez un nom pour votre serveur dans le champ Description.
- Définissez le mode du serveur sur Accès à distance (SSL/TLS), Accès à distance (Authentification de l'utilisateur) ou Accès à distance (SSL/TLS + Authentification de l'utilisateur). Comme mentionné ci-dessus, j'utiliserai l'accès à distance (SSL/TLS + authentification utilisateur) pour cet exemple.
- Remplacez le port local par un port différent si la topologie de votre réseau l'exige ou laissez-le par défaut (1194).



- Assurez-vous d'utiliser une clé TLS et générer automatiquement une clé TLS.
- Assurez-vous que votre autorité de certification homologue est définie sur l'autorité de certification que nous avons créée précédemment.
- Définissez le champ Certificat de serveur sur le certificat de serveur que nous avons créé précédemment.
- Sélectionnez 4096 bits pour le réglage de la longueur du paramètre DH.
- Définissez l'algorithme Auth digest sur SHA3-512 (512 bits).

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 OpenVPN ES

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 OpenVPN ES Certificate (Server: Yes, CA: OpenVPN ES)

DH Parameter Length 4096 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 Negotiation ☒ Enable Data Encryption Negotiation
 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

Available Data Encryption Algorithms	Allowed 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-256-GCM AES-128-GCM CHACHA20-POLY1305

Click to add or remove an algorithm 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 SHA3-512 (512-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.

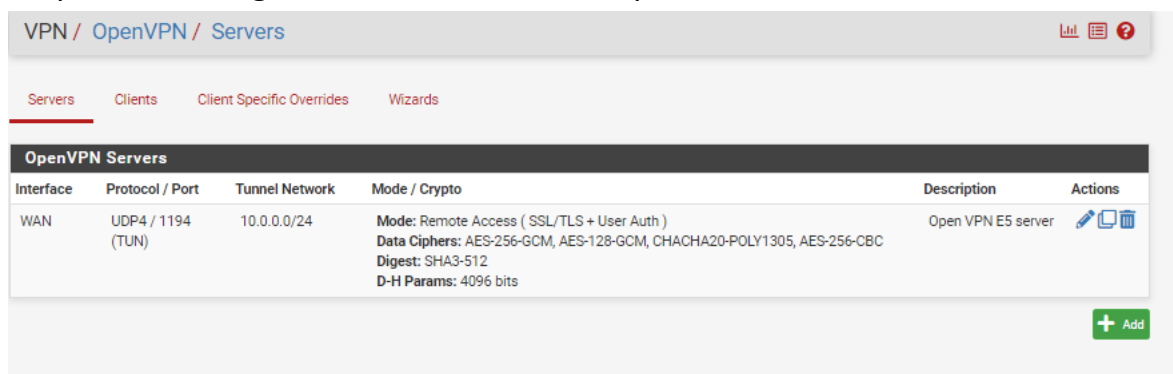
- Dans le champ IPv4 Tunnel Network, entrez un sous-réseau qui n'est pas présent sur votre réseau à utiliser comme sous-réseau interne du réseau OpenVPN. Dans mon cas, j'utilise 10.0.0.0/24.
- Activez Rediriger la passerelle IPv4 afin d'acheminer tout le trafic IPv4 via le tunnel VPN.

Tunnel Settings	
IPv4 Tunnel Network	<input type="text" value="10.0.0.0/24"/> <p>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. 10.0.0.0/24). 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.</p>
IPv6 Tunnel Network	<input type="text"/> <p>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.</p>
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"/> <p>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.</p>
Concurrent connections	<input type="text"/> <p>Specify the maximum number of clients allowed to concurrently connect to this server.</p>
Allow Compression	<input type="text" value="Refuse any non-stub compression (Most secure)"/> <p>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.</p> <p>Asymmetric compression allows an easier transition when connecting with older peers.</p>
Push Compression	<input type="checkbox"/> Push the selected Compression setting to connecting clients.
Type-of-Service	<input type="checkbox"/> Set the TOS IP header value of tunnel packets to match the encapsulated packet value.
Inter-client communication	<input type="checkbox"/> Allow communication between clients connected to this server
Duplicate Connection	<input type="checkbox"/> 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.
<p>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.</p>	

- Dans les configurations avancées activé les rapides UDP et cocher la case IPv4only.

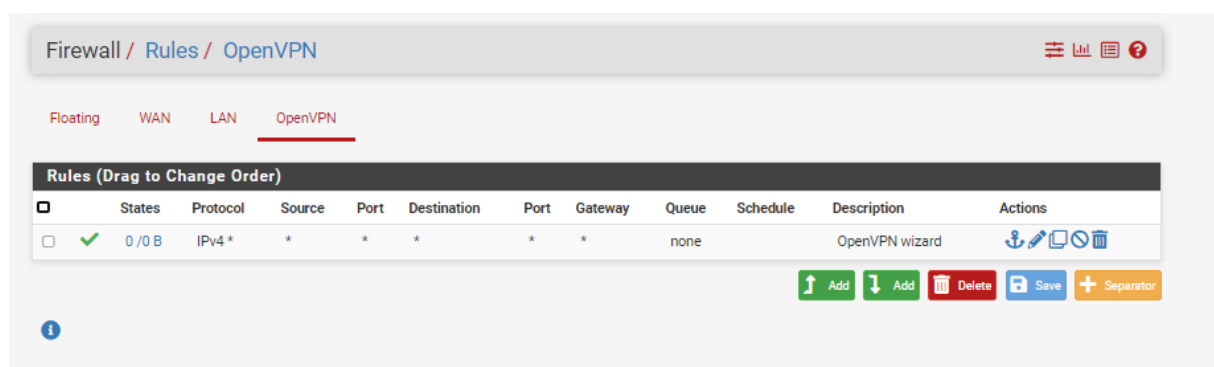
Advanced Configuration	
Custom options	<input type="text"/> <p>Enter any additional options to add to the OpenVPN server configuration here, separated by semicolon. EXAMPLE: push 'route 10.0.0.0 255.255.255.0'</p>
Username as Common Name	<input type="checkbox"/> Use the authenticated client username 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	<input checked="" type="checkbox"/> 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	<input type="text" value="Reconnect to this server / Retry once"/> <p>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.</p>
Send/Receive Buffer	<input type="text" value="Default"/> <p>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.</p>
Gateway creation	<input type="radio"/> Both <input checked="" type="radio"/> IPv4 only <input type="radio"/> 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	<input type="text" value="default"/> <p>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.</p> <p>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</p>
<input type="button" value="Save"/>	

- Cliquez sur enregistrer et votre serveur OpenVPN sera créé.



Créer des règles de pare-feu

- Sélectionner Firewall dans menu puis Rules puis le sous menu OpenVPN et cliquez sur le bouton ajouter.



- Définissez la famille d'adresses sur IPv4.
- Définissez le champ Protocole sur N'importe lequel.
- Définissez la Source sur Réseau.
- Entrez le sous-réseau OpenVPN que vous avez spécifié précédemment dans le champ Adresse source mais sans le /24.
- Sélectionnez 24 dans le menu déroulant à droite du champ Adresse source.
- Saisissez une description pour cette règle dans le champ description.

Firewall / Rules / Edit

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 Network 10.0.0.0 / 24

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

Advanced Options [Display Advanced](#)

Rule Information

Tracking ID	1676150149
Created	2/11/23 21:15:48 by OpenVPN Wizard
Updated	2/12/23 22:14:17 by admin@192.168.1.101 (Local Database)

[Save](#)

- Cliquez sur enregistrer et cliquez sur appliquer les modifications. Le trafic sera désormais autorisé à sortir du pare-feu à partir du sous-réseau OpenVPN.

Firewall / Rules / OpenVPN

The firewall rule configuration has been changed.
 The changes must be applied for them to take effect. [Apply Changes](#)

Floating WAN LAN OpenVPN

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓	0/0 B	IPv4 *	10.0.0.0/24	*	*	*	*	none	OpenVPN wizard	Anchor Edit Copy Delete

[Add](#) [Add](#) [Delete](#) [Save](#) [Separator](#)

[Info](#)

- Ensuite sélectionnez le sous-menu WAN.
- Cliquez sur le bouton Ajouter pour créer une nouvelle règle en haut de la liste.
- Définissez la famille d'adresses sur IPv4.
- Assurez-vous que Source est défini sur Any.
- Définissez le champ Protocole sur UDP.
- Définissez la plage de ports de destination sur 1194.

- Saisissez une description pour cette règle dans le champ Description.

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 / /

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

Destination

Destination ☐ **Invert match** WAN address Destination Address / /

Destination Port Range (other) 1194 (other) 1194
From Custom To Custom
Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Extra Options

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

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

Advanced Options [Display Advanced](#)

[Save](#)

- Cliquez sur enregistrer. Et cliquez sur appliquer les modifications. Le trafic sera désormais autorisé depuis Internet vers le serveur OpenVPN.

Firewall / Rules / WAN

The firewall rule configuration has been changed.
The changes must be applied for them to take effect. [Apply Changes](#)

Floating WAN LAN OpenVPN

Rules (Drag to Change Order)

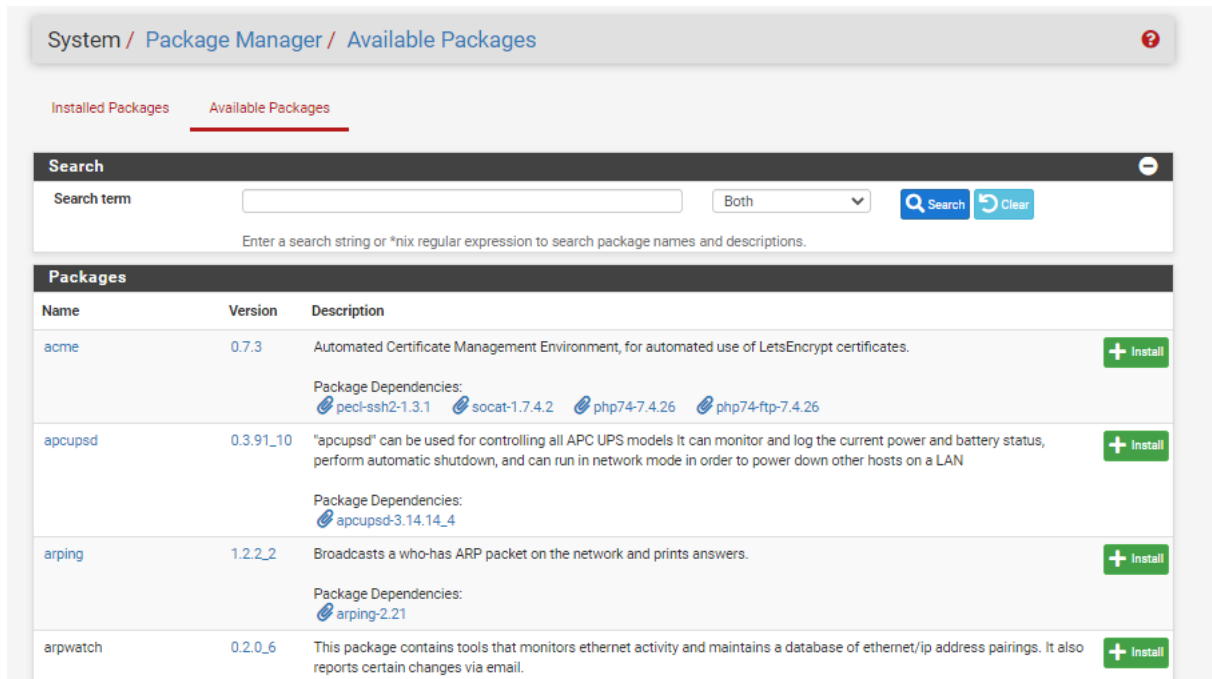
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✗ 0 /46 KiB	*	RFC 1918 networks	*	*	*	*	*		Block private networks	Settings
<input type="checkbox"/>	✗ 0 /0 B	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	Settings
<input type="checkbox"/>	✓ 0 /0 B	IPv4 UDP	*	*	WAN address	1194 (OpenVPN)	*	none		Open VPN ES	Anchor Edit Copy Paste Delete

[Add](#) [Add](#) [Delete](#) [Save](#) [Separator](#)

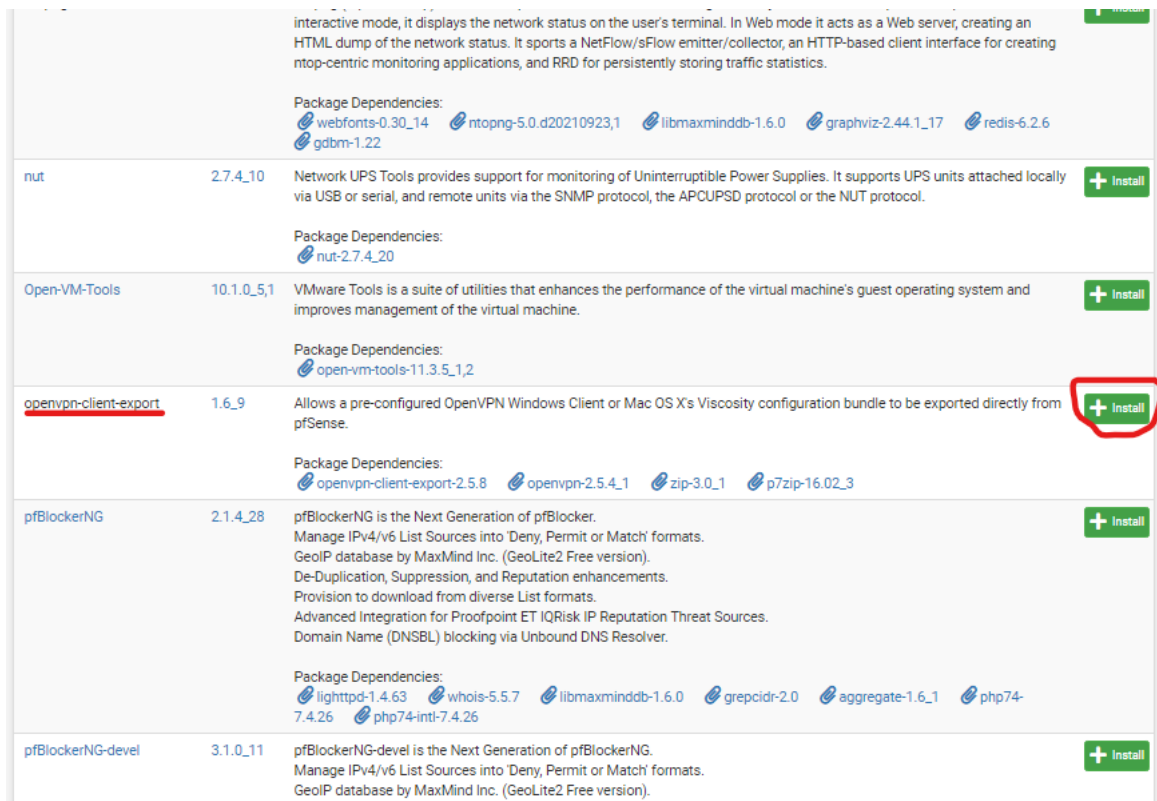
[Info](#)

Installez l'utilitaire d'exportation du client OpenVPN

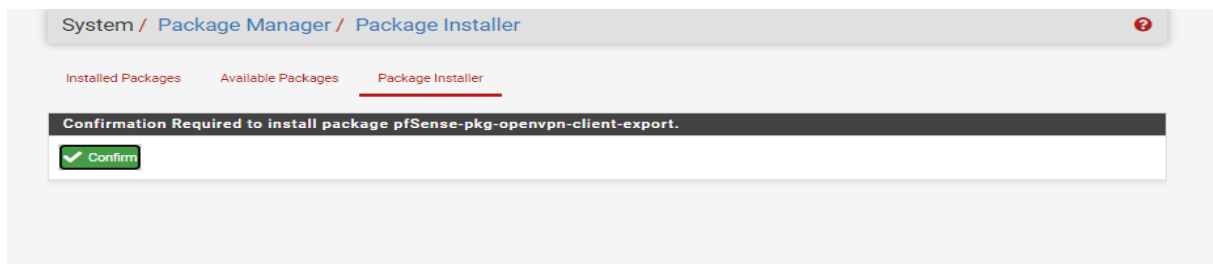
- Sélectionnez Système dans le menu puis Gestionnaire de packages puis le sous menu Available packages.



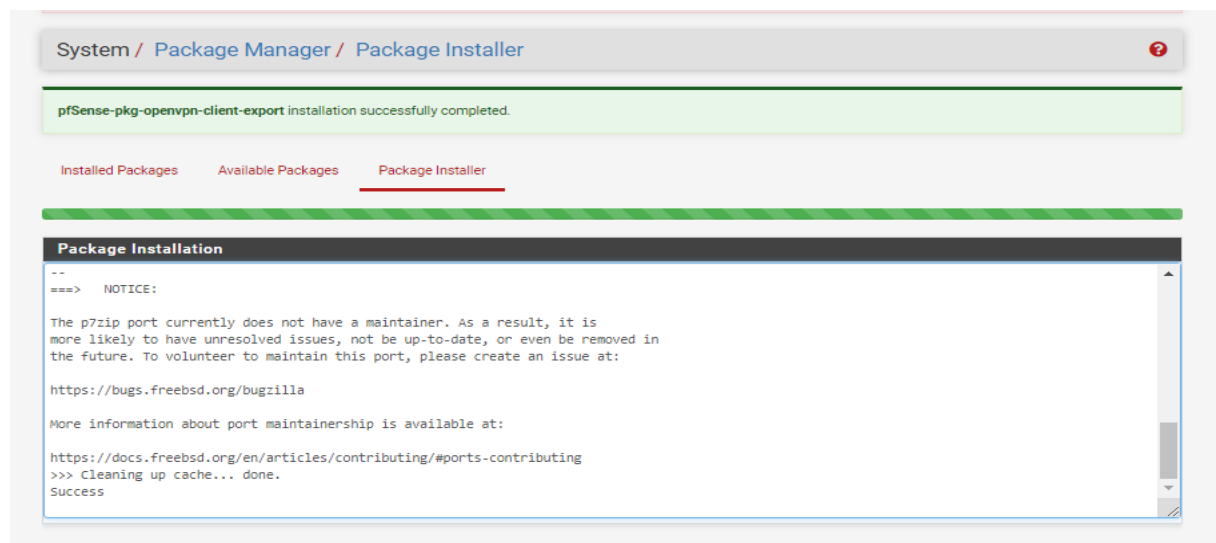
- Faites défiler vers le bas jusqu'à ce que vous trouviez openvpn-client-export puis cliquez sur installer.



➤ Confirmez l'installation.

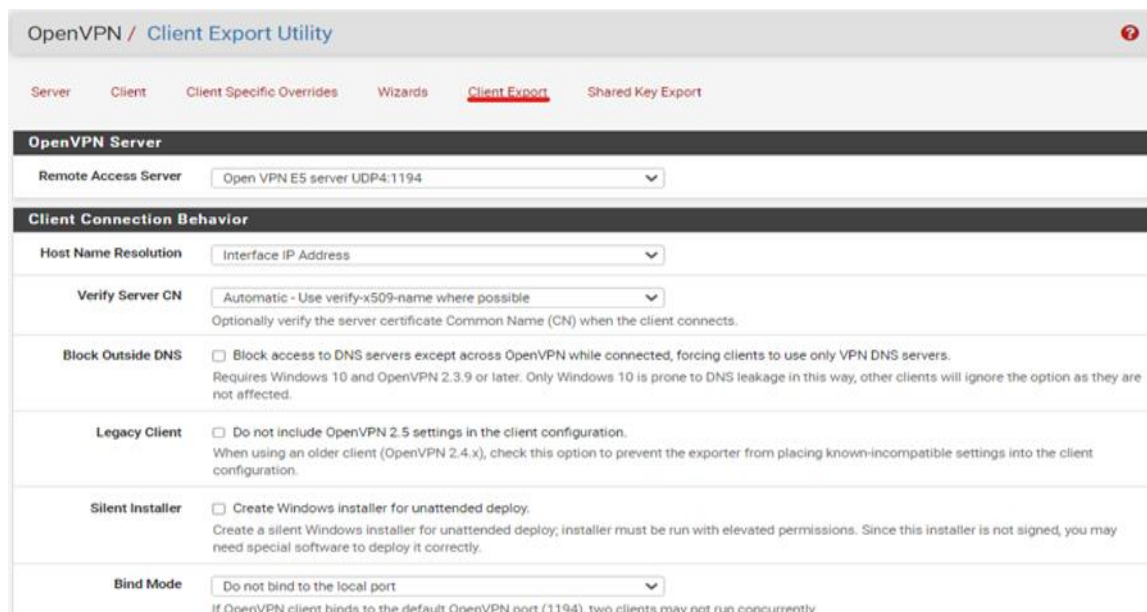


➤ L'installation a été un succès

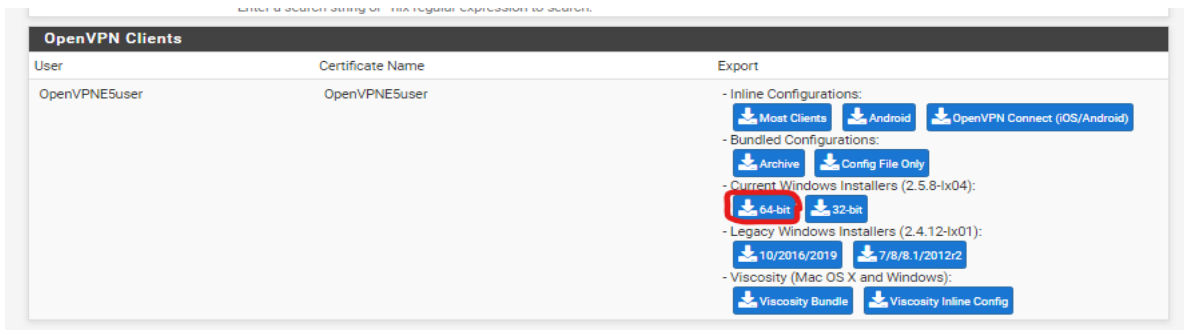


Exporter la configuration du client OpenVPN

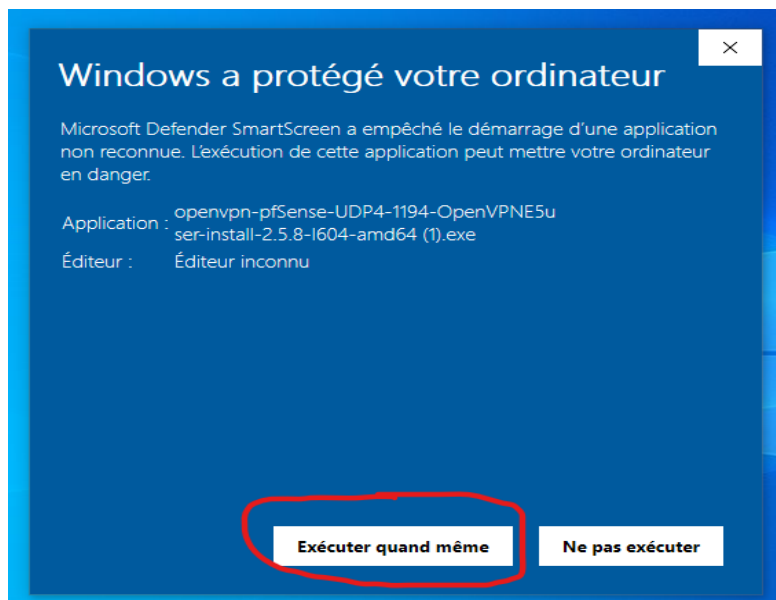
➤ Sélectionner VPN dans le menu puis OpenVPN puis sélectionner Client Export dans le sous menu.



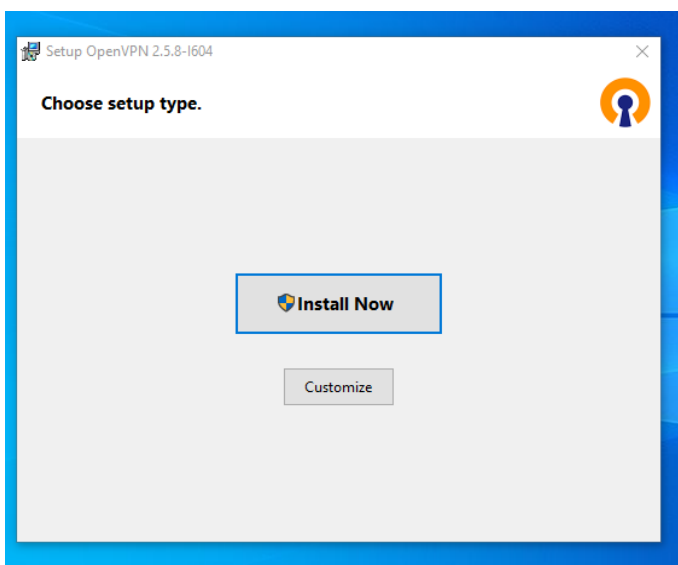
- Une fois dans le sous menus Client Export faite défiler la page vers le bas et vous trouverez des configurations générées pour divers systèmes et applications. Choisissez celle qui vous convient et téléchargez et installez-la. Pour ma part ce sera Windows 64bits.



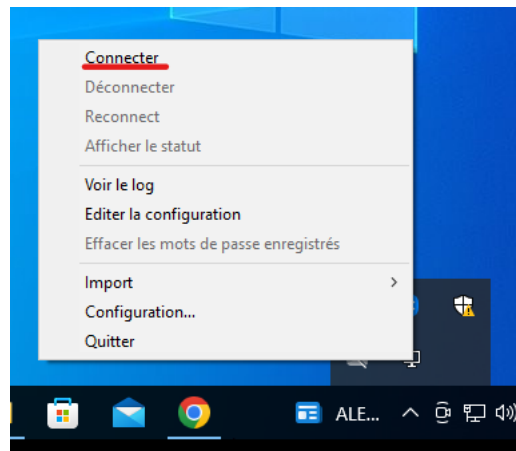
- Exécuter le fichier pour pouvoir le tester



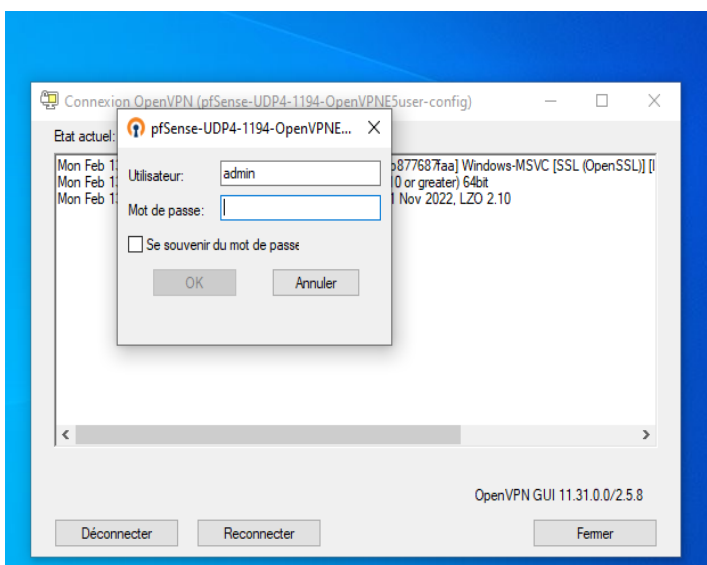
- Installer votre OpenVPN



- Choisissez l'écran avec un cadenas faite un clic droit et choisissez se connecter



- Entrez votre Nom d'utilisateur et votre mot de passe choisi au début de la configuration.



Dans mon cas :



- Username : admin
- Password : pfsense

- Votre VPN est désormais configuré et vous a assigné une adresse IP sur le réseau choisi lors de la configuration qui est 10.0.0.2.

