

BTS SIO - E6

Situation professionnelle n°1

Déploiement d'un bastion de sécurité pfSense et configuration d'un service OpenVPN avec authentification par certificats

06/02/2026

Contexte et Problématique :

Une PME possède des données dispersées sur plusieurs postes de travail, sans sauvegarde centralisée ni gestion des droits. Cette situation pose des risques critiques : perte de données en cas de panne disque, accès non autorisés à des documents confidentiels (RH, Direction), et saturation de l'espace de stockage par des fichiers personnels (vidéos, musiques). La demande : Centraliser les données sur un serveur sécurisé, garantir la redondance des disques, cloisonner les accès par service et contrôler le type de fichiers stockés.

NOM	DATE	TAMPON
CHERIF SOULEYMANE	06/02/2026	

SOMMAIRE :

1. Cahier des charges	3 à 4
1.1. Objectif principal	3
1.2. Choix Techniques	3
1.3. Prérequis	3
1.4. Compétences	3
1.5. Déroulement	3-4
1.6. Contraintes	4
2. Mise en œuvre	5 à 21
2.1. Création de la PKI (Public Key Infrastructure)	5
2.1.1. Création de l'Autorité de Certification (CA) interne	5-7
2.1.2. Création du Certificat Serveur	7-8
2.1.3. Création de l'Utilisateur et de son Certificat Client	9-10
2.2. Configuration du Serveur OpenVPN	11-15
2.3. Gestion des accès utilisateurs	15 à
2.3.1. Installation de l'outil d'exportation.	15-16
2.3.2. Configuration de l'exportation	16-17
2.3.3. Téléchargement du fichier pour l'utilisateur	18
2.4. Règles de Pare-feu (Firewall Rules)	19 à 21
2.4.1. La règle sur l'interface WAN	19
2.4.2. La règle sur l'interface OpenVPN	19-21
3. Tests et Recettes	22 à ...
3.1. Tests et Vérifications	22-26
3.1.1. Vérification de l'établissement du tunnel	...
3.1.2. Test d'étanchéité et de rebond	...
4. Points futurs à pousser	...
5. Bilan	...

1. LE CAHIER DES CHARGES :

1. Objectif principal :

L'objectif est de déployer une solution de télétravail sécurisé pour la PME. Il s'agit de permettre aux employés (Compta, Direction) d'accéder aux ressources internes (le serveur de fichiers du projet E5) depuis l'extérieur, tout en garantissant que les données ne soient pas interceptées sur Internet.

1.2. Choix techniques :

Environnement technologique :

- Pare-feu/Routeur : pfSense (Bastion de sécurité).
- Protocole VPN : OpenVPN (choisi pour sa robustesse et sa facilité de passage à travers les box internet).
- Chiffrement : SSL/TLS avec algorithme AES-256-GCM.
- Authentification : Double facteur (Certificat numérique + Identifiant/Mot de passe).

1.3. Prérequis :

- Le pare-feu pfSense opérationnel avec une interface WAN (Internet) et une interface LAN.
- Une Autorité de Certification (CA) interne créée sur le pfSense.
- Le serveur Windows Server 2022 (E5) fonctionnel dans le LAN.

1.4. Compétences :

Compétences du référentiel mises en œuvre :

- Protéger les données à travers des flux chiffrés.
- Gérer l'identité par la gestion des certificats numériques (PKI).
- Sécuriser les accès distants des utilisateurs nomades.

1.5. Déroulement :

Phase 1 : Mise en place de l'Infrastructure à Clés Publiques (PKI)

- Création d'une Autorité de Certification (CA) interne sur le bastion pfSense.
- Génération d'un certificat serveur dédié au service OpenVPN pour garantir l'identité du point d'accès.

Phase 2 : Configuration du service d'accès distant (VPN)

- Paramétrage du serveur OpenVPN (chiffrement AES-256-GCM, port UDP 1194).
- Définition du réseau de tunnel (adressage virtuel) et routage vers le réseau local (LAN).

Phase 3 : Gestion des identités et des accès nomades

- Création des comptes utilisateurs et génération des certificats clients individuels.
- Configuration des règles de pare-feu (Firewall) pour autoriser le flux VPN et filtrer les accès vers le serveur de fichiers.

Phase 4 : Déploiement client et validation

- Installation du client OpenVPN sur les postes nomades.
- Tests de connectivité et vérification du chiffrement des flux pour valider la confidentialité.

1.6. Contraintes :

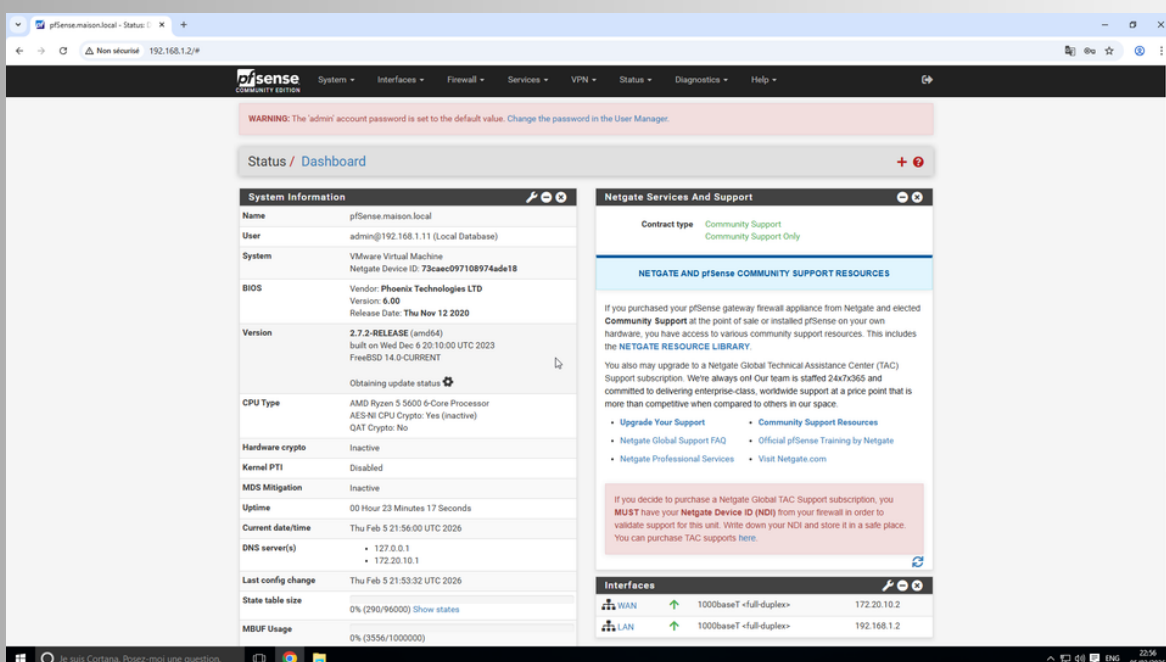
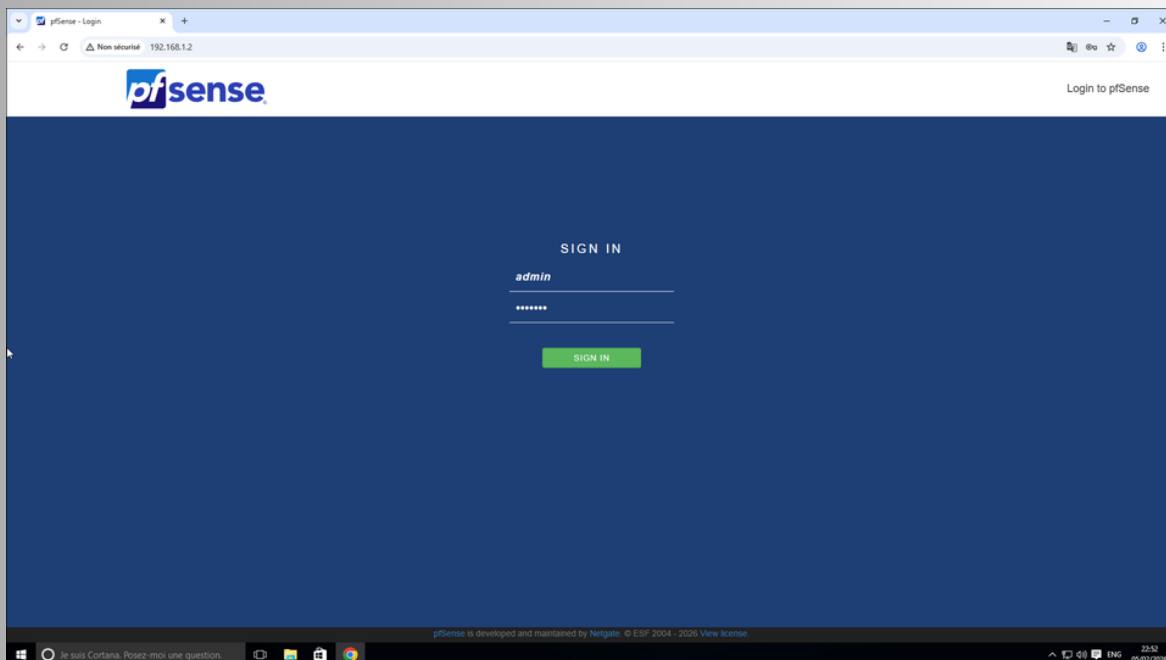
- **Contrainte de sécurité** : L'accès doit impérativement reposer sur une authentification forte (certificat + mot de passe) pour éviter toute usurpation d'identité en cas de vol de terminal.
- **Contrainte technique** : La solution VPN doit être capable de traverser les équipements réseaux domestiques (NAT des box internet) sans configuration complexe pour l'utilisateur final.
- **Contrainte de confidentialité** : Tous les flux transitant par Internet doivent être chiffrés avec un algorithme robuste pour empêcher l'interception de données sensibles de la PME.
- **Contrainte organisationnelle** : L'accès distant ne doit pas modifier les habitudes des utilisateurs ; les lecteurs réseau (Compta, Direction) configurés en E5 doivent être accessibles de la même manière via le tunnel.

2. MISE EN OEUVRE :

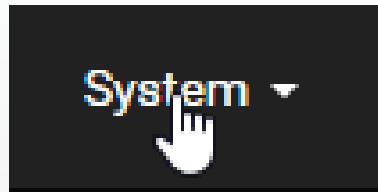
2.1. Création de la PKI (Public Key Infrastructure)

2.1.1. Création de l'Autorité de Certification (CA) interne

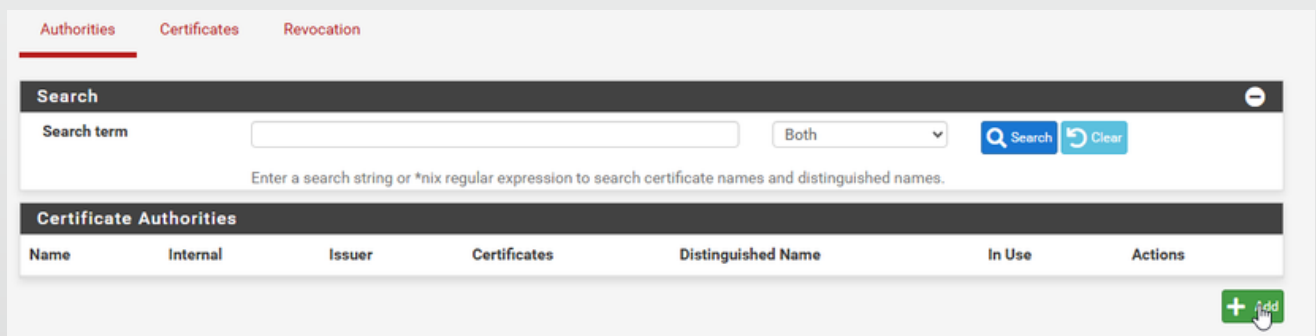
- Connexion au WebConfigurator de pfSense.



- Configuration de l'autorité de certificat interne.



- Cette autorité va signer tous les futurs certificats. Elle est la base de notre chaîne de confiance.



- Définition des paramètres nécessaires à l'autorité.

Create / Edit CA

Descriptive name

CA-VPN-GSB

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 ca-vpn.gsb.local

The following certificate authority 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)



Authorities **Certificates** **Revocation**

Search

Search term Both  

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
CA-VPN-GSB	✓	self-signed	0	CN=ca-vpn.gsb.local Valid From: Tue, 10 Feb 2026 11:20:33 +0000 Valid Until: Fri, 08 Feb 2036 11:20:33 +0000		   



- Autorité de certificat créée.

2.1.2. Création du Certificat Serveur

- Configuration du certificat serveur.

Certificates

Name	Issuer	Distinguished Name	In Use	Actions
GUI default (69811bf02b0e7) Server Certificate CA: No Server: Yes	self-signed	O=pfSense GUI default Self-Signed Certificate, CN=pfSense-69811bf02b0e7 Valid From: Mon, 02 Feb 2026 21:49:36 +0000 Valid Until: Sun, 07 Mar 2027 21:49:36 +0000		   



Add/Sign a New Certificate

Method Create an internal Certificate

Descriptive name CERT-SRV-VPN-GSB

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: ?, >, <, &, /, \, ", '.

Internal Certificate

Certificate authority CA-VPN-GSB

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 cert-srv-vpn.gsb.local

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)

- Définition du certificat en 'Server Certificate'

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
Server Certificate
User Certificate

Alternative Names
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 SAN Row + Add SAN Row

Save

- Certificat de serveur créé.

Authorities Certificates Certificate Revocation

Search

Search term Both Search Clear

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

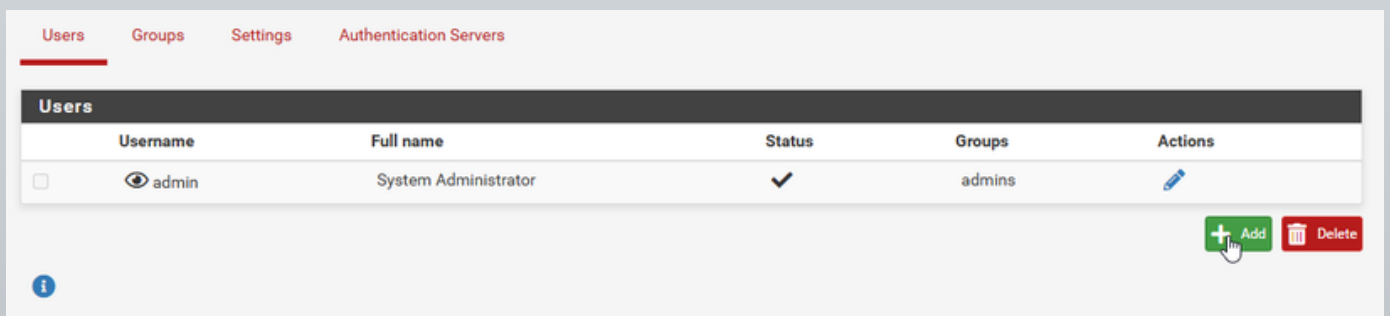
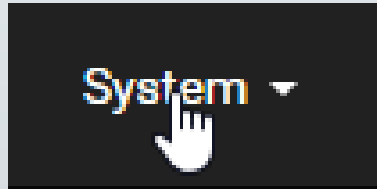
Name	Issuer	Distinguished Name	In Use	Actions
GUI default (69811bf02b0e7) Server Certificate CA: No Server: Yes	self-signed	O=pfSense GUI default Self-Signed Certificate, CN=pfSense-69811bf02b0e7 Valid From: Mon, 02 Feb 2026 21:49:36 +0000 Valid Until: Sun, 07 Mar 2027 21:49:36 +0000		
CERT-SRV-VPN-GSB Server Certificate CA: No Server: Yes	CA-VPN-GSB	CN=cert-srv-vpn.gsb.local Valid From: Tue, 10 Feb 2026 11:29:35 +0000 Valid Until: Fri, 08 Feb 2036 11:29:35 +0000		

+ Add/Sign

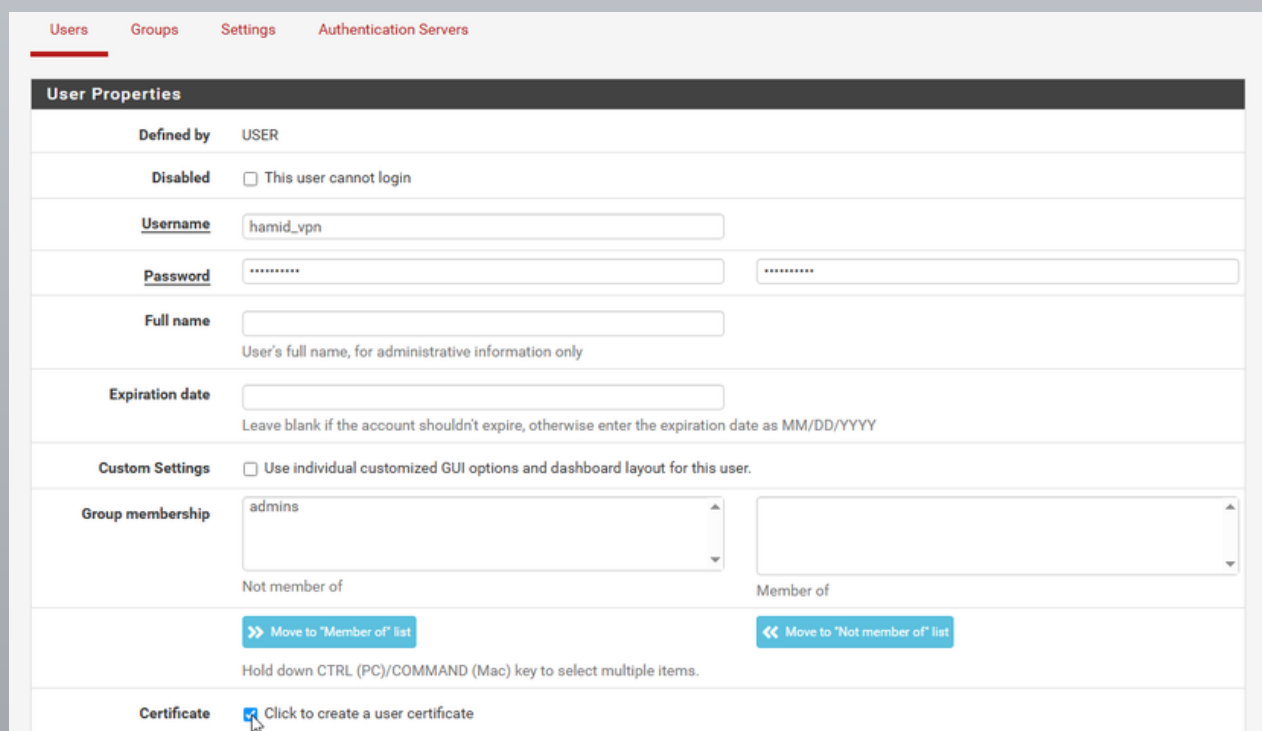
- Ce certificat permet au pfSense de prouver son identité aux clients qui tentent de se connecter

2.1.3. Création de l'Utilisateur et de son Certificat Client

- Configuration de l'utilisateur "hamid_vpn" ainsi que de la liaison avec l'autorité de certificat



- Bien cocher le case "Certificate" pour que la liaison utilisateur autorité soit faite.



User Properties

Defined by: USER

Disabled: ☐ This user cannot login

Username: hamid_vpn

Password: [masked]

Full name: [empty]

Expiration date: [empty]

Custom Settings: ☐ Use individual customized GUI options and dashboard layout for this user.

Group membership: admins

Not member of: [empty]

Member of: [empty]

Move to "Member of" list

Move to "Not member of" list

Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.

Certificate: ☒ Click to create a user certificate

Create Certificate for User

Descriptive name

CERT-HAMID-VPN

Certificate authority

CA-VPN-GSB

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

Keys

Authorized SSH Keys

Enter authorized SSH keys for this user

IPsec Pre-Shared Key

Shell Behavior

Keep Command History

☐ Keep shell command history between login sessions
 If this user has shell access, this option preserves the last 1000 unique commands entered at a shell prompt between login sessions. The user can access history using the up and down arrows at an SSH or console shell prompt and search the history by typing a partial command and then using the up or down arrows.

Save

- Utilisateur bien créé.

Users

Groups

Settings

Authentication Servers

Users

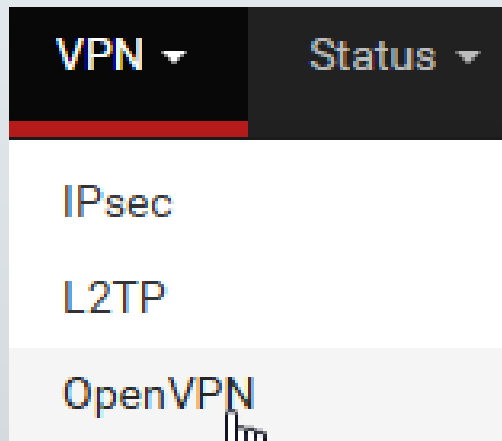
	Username	Full name	Status	Groups	Actions
☐	admin	System Administrator	✓	admins	
☐	hamid_vpn		✓		

+ Add

Delete

- Chaque utilisateur possède son propre certificat X.509. Si un employé quitte l'entreprise, on peut révoquer son certificat sans bloquer les autres.

2.2. Configuration du Serveur OpenVPN



- Accéder au menu “Wizard” dans OpenVPN et configurer l’accès à distance.
- Choisir “Local User Access”.

A screenshot of the 'OpenVPN Remote Access Server Setup Wizard' interface. The breadcrumb trail at the top reads 'Wizard / OpenVPN Remote Access Server Setup /'. The main heading is 'OpenVPN Remote Access Server Setup'. Below it, a message states: 'This wizard will provide guidance through an OpenVPN Remote Access Server Setup . The wizard may be stopped at any time by clicking the logo image at the top of the screen.' The section 'Select an Authentication Backend Type' contains a dropdown menu labeled 'Type of Server' with 'Local User Access' selected. A note below reads: 'NOTE: If unsure, leave this set to "Local User Access."' At the bottom, there is a blue button with a double arrow and the text 'Next', which a mouse cursor is clicking.

- Sélectionner l’autorité de certificat.

A screenshot of the 'OpenVPN Remote Access Server Setup Wizard' interface at Step 5 of 11. The breadcrumb trail at the top reads 'Wizard / OpenVPN Remote Access Server Setup / Certificate Authority Selection'. A red progress bar indicates the current step. The main heading is 'Certificate Authority Selection'. Below it, the text 'OpenVPN Remote Access Server Setup Wizard' is displayed. The section 'Choose a Certificate Authority (CA)' contains a dropdown menu labeled 'Certificate Authority' with 'CA-VPN-GSB' selected. At the bottom, there are two blue buttons: 'Add new CA' and 'Next'. A mouse cursor is clicking the 'Next' button.

- Ensuite sélectionner le certificat de serveur.

Wizard / OpenVPN Remote Access Server Setup / Server Certificate Selection ?

Step 7 of 11

Server Certificate Selection

OpenVPN Remote Access Server Setup Wizard

Choose a Server Certificate

Certificate: CERT-SRV-VPN-GSB

[Add new Certificate](#) [Next](#)

- Choix du Protocol “UDP” pour plus de performances.

Server Setup

OpenVPN Remote Access Server Setup Wizard

General OpenVPN Server Information

Description: SRV-R_ACC-OPNVPN-GSB

A name for this OpenVPN instance, for administrative reference. It can be set however desired, but is often used to distinguish the purpose of the service (e.g. "Remote Technical Staff"). It is also used by OpenVPN Client Export to identify this VPN on clients.

Endpoint Configuration

Protocol: UDP on IPv4 only

Protocol to use for OpenVPN connections. If unsure, leave this set to UDP.

Interface: WAN

The interface where OpenVPN will listen for incoming connections (typically WAN.)

Local Port: 1194

Local port upon which OpenVPN will listen for connections. The default port is 1194. This can be left at its default unless a different port needs to be used.

- Pour garantir la confidentialité des flux, j'ai implémenté l'algorithme de chiffrement AES-256-GCM. Ce choix permet d'allier une sécurité de niveau industriel à une haute performance de transfert, essentielle pour l'accès aux dossiers partagés du serveur GSB.

Cryptographic Settings	
TLS Authentication	☒ Enable authentication of TLS packets.
Generate TLS Key	☒ Automatically generate a shared TLS authentication key.
TLS Shared Key	Paste in a shared TLS key if one has already been generated.
DH Parameters Length	2048 bit Length of Diffie-Hellman (DH) key exchange parameters, used for establishing a secure communications channel. The DH parameters are different from key sizes, but as with other such settings, the larger the key, the more security it offers, but larger keys take considerably more time to generate. As of 2016, 2048 bit is a common and typical selection.
Data Encryption Algorithms	AES-256-GCM AES-128-GCM CHACHA20-POLY1305 List of algorithms clients can negotiate to encrypt traffic between endpoints. The best practice is to use the exact algorithms listed above, in that order. Certain algorithms will perform better on different hardware, depending on the availability of supported VPN accelerator chips. Edit the server after finishing the wizard for additional choices.
Fallback Data Encryption Algorithm	AES-256-CBC (256 bit key, 128 bit block) The algorithm used to encrypt traffic between endpoints when data encryption negotiation is disabled or fails.
Auth Digest Algorithm	SHA256 (256-bit) The method used to authenticate traffic between endpoints. This setting must match on the client and server side, but is otherwise set however desired.
Hardware Crypto	Intel RDRAND engine - RAND The hardware cryptographic accelerator to use for this VPN connection, if any.

- Paramétrage des paramètres tunnel (liaison vers le pfSense).

Tunnel Settings	
IPv4 Tunnel Network	10.0.8.0/24 This is the virtual network used for private communications between this server and client hosts expressed using CIDR notation (eg. 10.0.8.0/24). The first network address will be assigned to the server virtual interface. The remaining network addresses will be assigned to connecting clients.
Redirect IPv4 Gateway	☐ Force all client generated traffic through the tunnel.
IPv4 Local Network	192.168.1.0/24 This is the network that will be accessible from the remote endpoint, expressed as a CIDR range. This may be left blank if not adding a route to the local network through this tunnel on the remote machine. This is generally set to the LAN network.
Concurrent Connections	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, which is potentially insecure.
Compression	Disable Compression [Omit Preference] Compress tunnel packets using the chosen option. Can save bandwidth, but is potentially insecure and may expose data. This setting has no effect if compression is not allowed. Adaptive compression will dynamically disable compression for a period of time if OpenVPN detects that the data in the packets is not being compressed efficiently.
Type-of-Service	☐ Set the TOS IP header value of tunnel packets to match the encapsulated packet's TOS value.
Inter-Client Communication	☐ Allow communication between clients connected to this server.
Duplicate Connections	☐ Allow multiple concurrent connections from clients using the same Common Name. NOTE: This is not generally recommended, but may be needed for some scenarios.
Duplicate Connection Limit	Limit the number of concurrent connections from the same user.

Client Settings

Dynamic IP

☒ Allow connected clients to retain their connections if their IP address changes.

Topology

Subnet -- One IP address per client in a common subnet

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".

- Paramétrage des paramètres clients avancés (liaison vers le serveur).
- En renseignant le suffixe DNS et l'adresse du contrôleur de domaine dans les paramètres du serveur VPN, je permets aux utilisateurs nomades de bénéficier de la résolution de noms interne, exactement comme s'ils étaient au bureau.

Advanced Client Settings

DNS Default Domain

maison.local

Provide a default domain name to clients.

DNS Server 1

192.168.1.10

DNS server IP to provide to connecting clients.

DNS Server 2

DNS server IP to provide to connecting clients.

DNS Server 3

DNS server IP to provide to connecting clients.

DNS Server 4

DNS server IP to provide to connecting clients.

NTP Server

Network Time Protocol server to provide to connecting clients.

NTP Server 2

Network Time Protocol server to provide to connecting clients.

NetBIOS Options

☐ Enable NetBIOS over TCP/IP.

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

NetBIOS Node Type

none

Possible options: b-node (broadcasts), p-node (point-to-point name queries to a WINS server), m-node (broadcast then query name server), and h-node (query name server, then broadcast).

NetBIOS Scope ID

A NetBIOS Scope ID provides an extended naming service for NetBIOS over TCP/IP. The NetBIOS scope ID isolates NetBIOS traffic on a single network to only those nodes with the same NetBIOS scope ID.

WINS Server 1

A Windows Internet Name Service (WINS) server IP to provide to connecting clients. Not desirable in most all modern networks.

WINS Server 2

A Windows Internet Name Service (WINS) server IP to provide to connecting clients. Not desirable in most all modern networks.

>> Next

Firewall Rule Configuration

OpenVPN Remote Access Server Firewall Rules

Rules control passing or blocking network traffic as it flows through the firewall.

Rules must be added which allow traffic to reach the OpenVPN server IP address and port, as well as to allow traffic from connected clients inside the OpenVPN tunnel.

The options on this step can add automatic rules to pass this traffic, or rules can be configured manually after completing the wizard.

Traffic from clients to server

Firewall Rule

☒ Add a rule to permit connections to this OpenVPN server instance from clients anywhere on the Internet.

Traffic from clients through VPN

OpenVPN rule

☒ Add a rule to allow all traffic from connected clients to pass inside the VPN tunnel.

>> Next

- Server OpenVPN créé.

Servers

Clients

Client Specific Overrides

Wizards

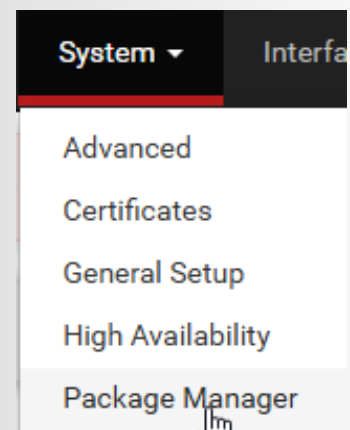
OpenVPN Servers

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-256-CBC Digest: SHA256 D-H Params: 2048 bits	SRV-R_ACC-OPNVPN-GSB	

+ Add

2.3. Gestion des accès utilisateurs

2.3.1. Installation de l'outil d'exportation.



Installed Packages	Available Packages
Installed Packages	
There are no packages currently installed.	

- Installation du packet “openvpn-client-export”

Installed Packages	Available Packages
Installed Packages	
There are no packages currently installed.	

Search			
Search term	openvpn-client	Both	Search Clear
Enter a search string or *nix regular expression to search package names and descriptions.			
Packages			
Name	Version	Description	
openvpn-client-export	1.9.2	Exports pre-configured OpenVPN Client configurations directly from pfSense software.	+ Install
Package Dependencies: openvpn-client-export-2.6.7 openvpn-2.6.8_1 zip-3.0_1 7-zip-23.01			

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

Installed Packages

Available Packages

Package Installer

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

Available Packages

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

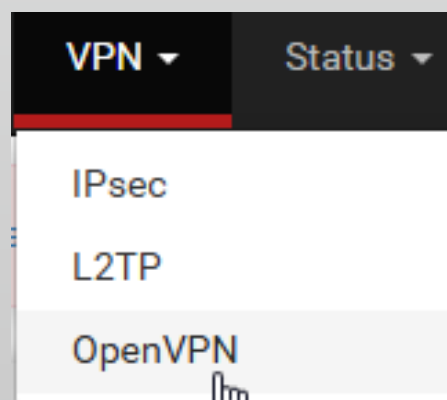
 = Remove  = Information  = Reinstall

Newer version available

Package is configured but not (fully) installed or deprecated

2.3.2. Configuration de l'exportation

- Configuration du Client Export



- Mise en relation avec l'interface WAN du pfSense (là où le VPN ira chercher l'internet)

Server
Client
Client Specific Overrides
Wizards
Client Export

OpenVPN Server

Remote Access Server
SRV-R_ACC-OPNVPN-GSB 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, Windows)

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;

Save as default

2.3.3. Téléchargement du fichier pour l'utilisateur

User	Certificate Name	Export
hamid_vpn	CERT-HAMID-VPN	- Inline Configurations: Download Clients Android OpenVPN Connect (iOS/Android) - Bundled Configurations: Archive Config File Only - Current Windows Installers (2.6.7-lx001): 64-bit 32-bit - Previous Windows Installers (2.5.9-lx601): 64-bit 32-bit - Legacy Windows Installers (2.4.12-lx601): 10/2016/2019 7/8/8.1/2012r2 - Viscosity (Mac OS X and Windows): Viscosity Bundle Viscosity Inline Config

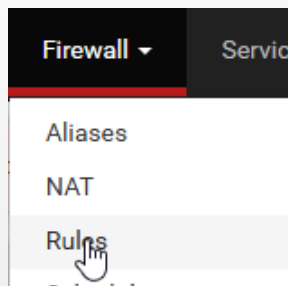
[pfSense-UDP4-1194-hamid_vpn-config.ovpn](#)

Source : <http://192.168.1.2>

- L'exportation du client permet de regrouper en un seul fichier sécurisé la configuration du tunnel, l'adresse de la passerelle et le certificat X.509 de l'utilisateur. Ce procédé simplifie le déploiement sur les postes nomades tout en garantissant que seul l'utilisateur possédant ce fichier et son mot de passe peut initier la connexion.

2.4. Règles de Pare-feu (Firewall Rules)

2.4.1. La règle sur l'interface WAN



Firewall / Rules / WAN

Floating **WAN** LAN OpenVPN

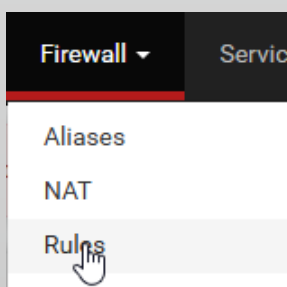
Rules (Drag to Change Order)

☐	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
☒	0/7 KIB	*	RFC 1918 networks	*	*	*	*	*	*	Block private networks	
☒	0/20 KIB	*	Reserved Not assigned by IANA	*	*	*	*	*	*	Block bogon networks	
☒	0/0 B	IPv4 UDP	*	*	WAN address	1194 (OpenVPN)	*	none		OpenVPN SRV-R_ACC-OPNVPN-GSB wizard	

Add Add Delete Toggle Copy Save Separator

- La règle a bien été créée.
- Cette règle est indispensable pour permettre aux paquets chiffrés venant d'Internet d'atteindre le service OpenVPN du bastion.

2.4.2. La règle sur l'interface OpenVPN (Le contrôle interne)



- Pour renforcer la sécurité, le filtrage sur l'interface OpenVPN restreint les flux des utilisateurs nomades vers les seules ressources nécessaires (serveur de fichiers), interdisant ainsi l'accès à l'administration du pare-feu ou aux autres équipements du LAN.

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 10.0.8.0 / 24

Destination

Destination ☐ Invert match Address or Alias 192.168.1.10 /

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 access restrictif au serveur GSB pour les nomades
 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	1770731800
Created	2/10/26 13:56:39 by OpenVPN Wizard
Updated	2/10/26 16:59:32 by admin@192.168.1.11 (Local Database)

Save

Firewall / Rules / OpenVPN

Floating WAN LAN OpenVPN

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
☐	✓	0/0 B	IPv4 *	10.0.8.0/24	*	192.168.1.10	*	*	none	access restrictif au serveur GSB pour les nomades	     

 Add  Add  Delete  Toggle  Copy  Save  Separator



- OpenVPN finaliser.

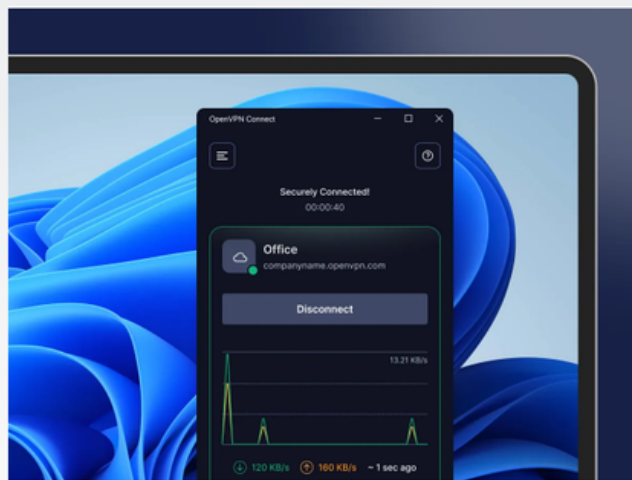
3. TESTS ET RECETTES :

3.1. TESTS ET VÉRIFICATIONS

3.1.1. Vérification de l'établissement du tunnel

- Côté client :

→ Installer OpenVPN Connect sur la machine Windows 10



Home > Downloads

OpenVPN Connect for Windows

Download official client application that enables you to securely access your organization's network resources.

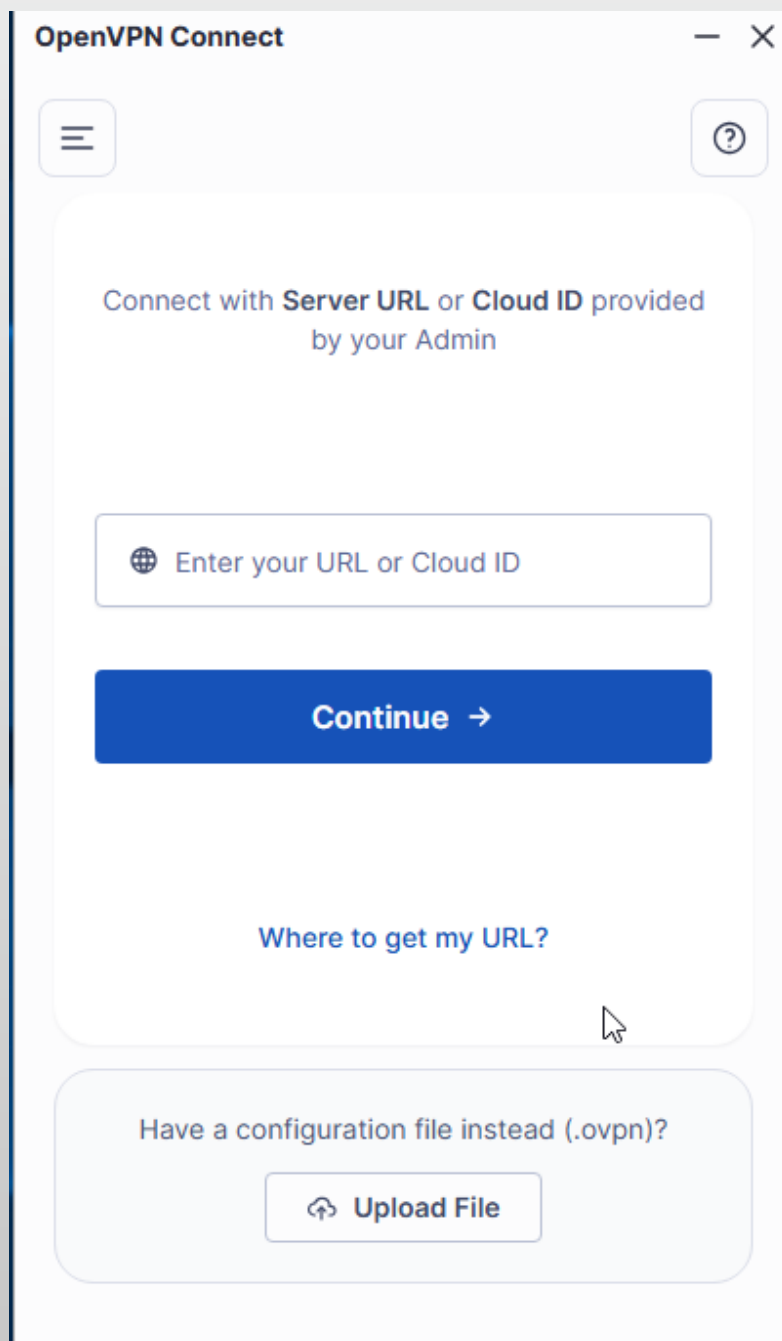
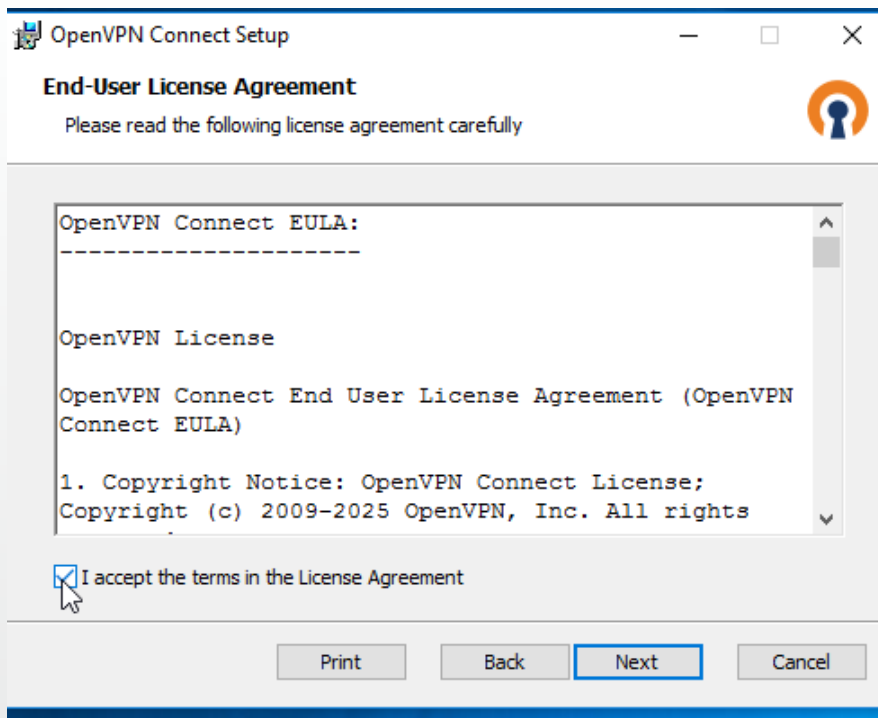
[Download .msi](#)

[View Installation Guide & Alternative Versions](#) →

Available for: Windows 10, and Windows 11
[Check what's new](#)

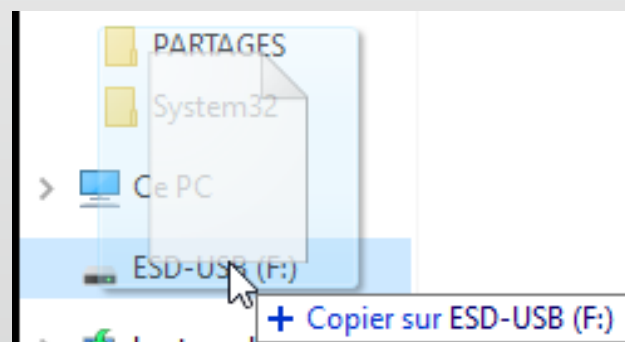
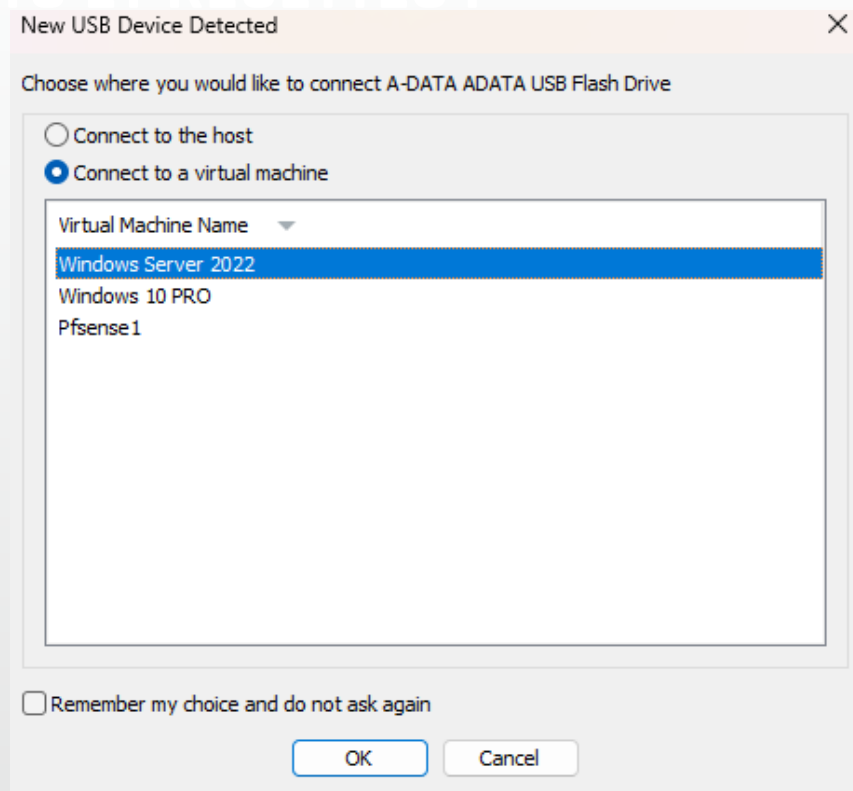
openvpn-connect-3.8.0.4528_signed	12/02/2026 16:55	Package Windows...	113 228 Ko
-----------------------------------	------------------	--------------------	------------



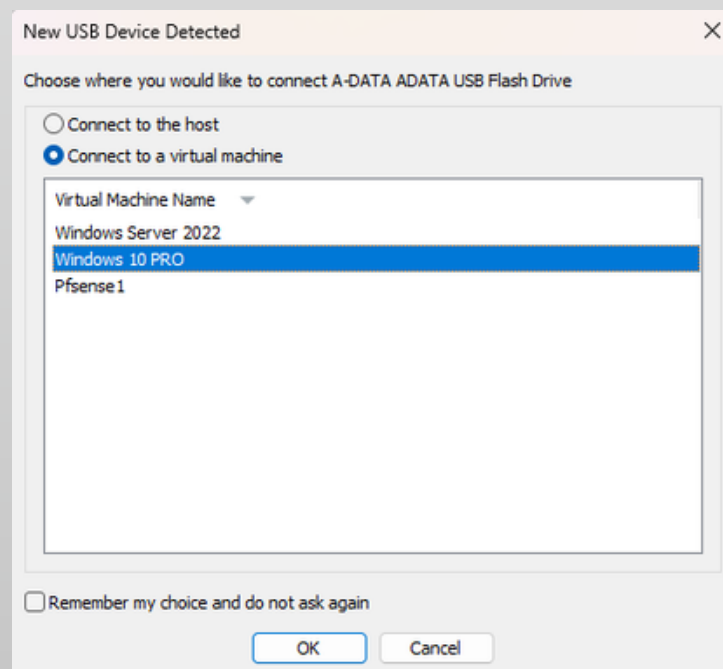


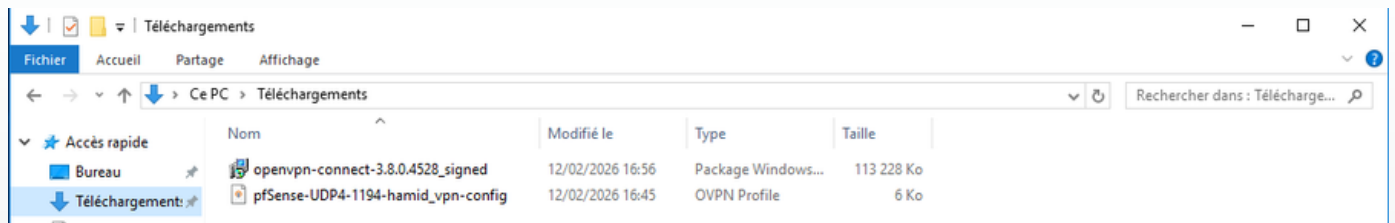
→ Importer le fichier .ovpn depuis le serveur

3. TESTS ET RECETTES :

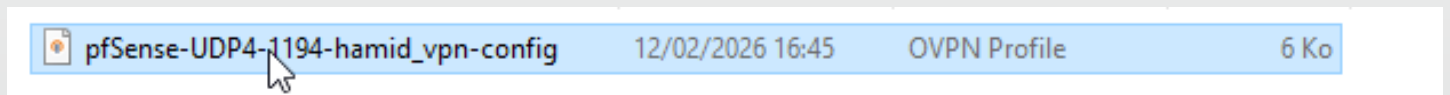
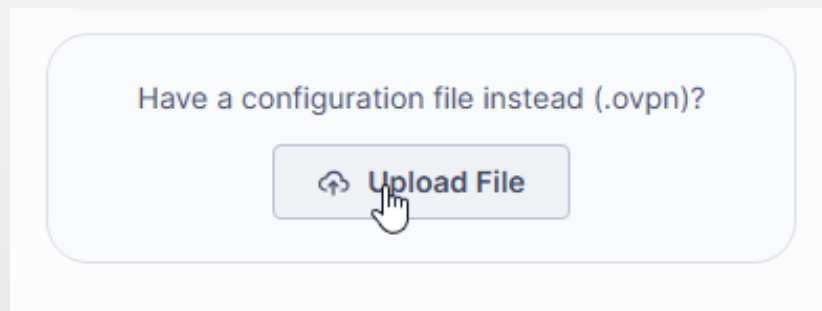


→ Importer le fichier .ovpn sur le windows

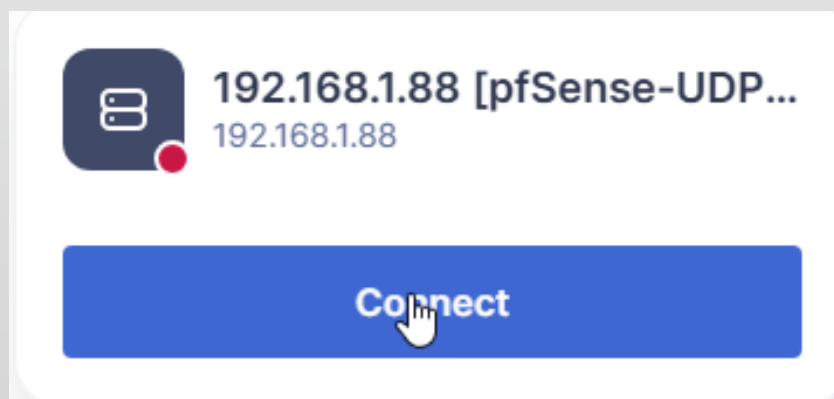




→ Importer le fichier .ovpn sur OpenVPN Connect



→ Connexion au VPN



Enter credentials



Profile:

192.168.1.88 [pfSense-UDP4-1194-hamid_vpn-config]

Username *

Password



Enter 

Cancel