Installation et configuration OpenVPN sur pfSense avec LDAP/AD

IRATNI Hocine

Nom de l'enseignant :
Bernard FERNANDEZ

Date de soumission : 29 août 2025

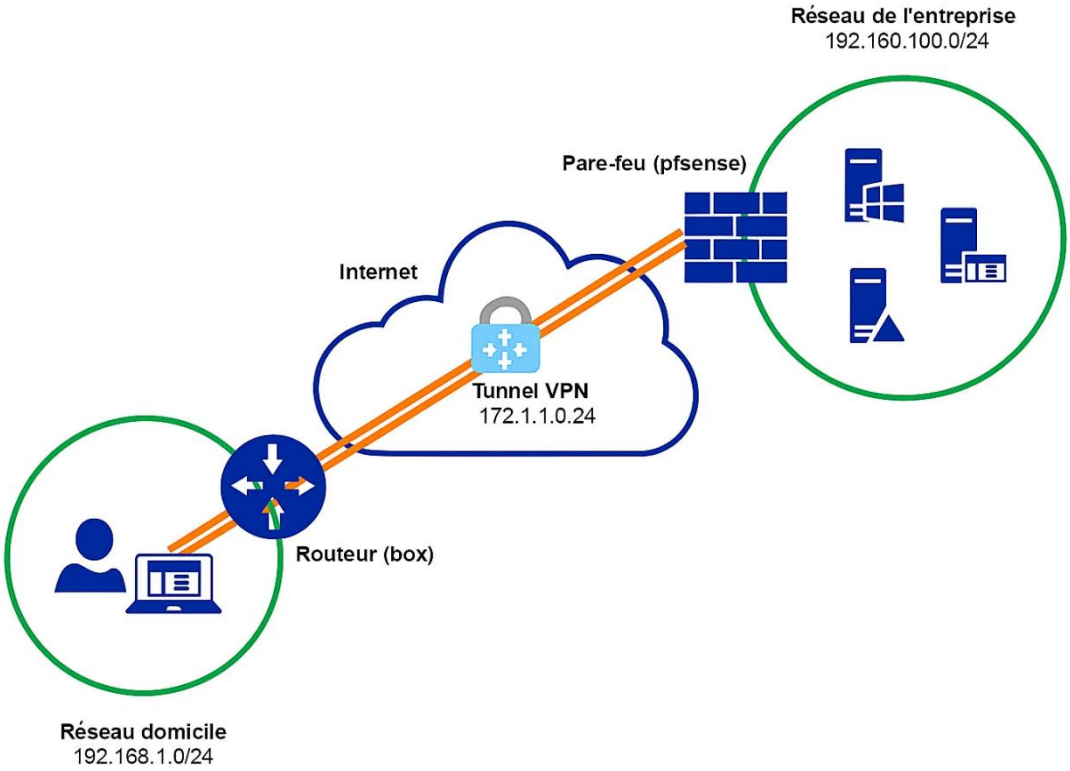
Table des matières

I. Introduction

Dans le cadre d'un projet de **BTS SIO SISR**, il est demandé de mettre en place une solution de **VPN sécurisé** permettant aux utilisateurs distants d'accéder aux ressources internes d'une entreprise. Pour cela, nous allons utiliser **OpenVPN** sur un pare-feu **pfSense**, en intégrant l'authentification des utilisateurs via un **Active Directory** (AD).

L'objectif est de permettre uniquement aux comptes contenus dans une **OU spécifique par exemple : « UtilisateurVPN »** de se connecter au VPN, garantissant ainsi un contrôle précis des accès.

Cette procédure détaillée couvre toutes les étapes nécessaires : préparation d'Active Directory, configuration de pfSense (certificats, LDAP, OpenVPN), export des profils clients et validation du fonctionne



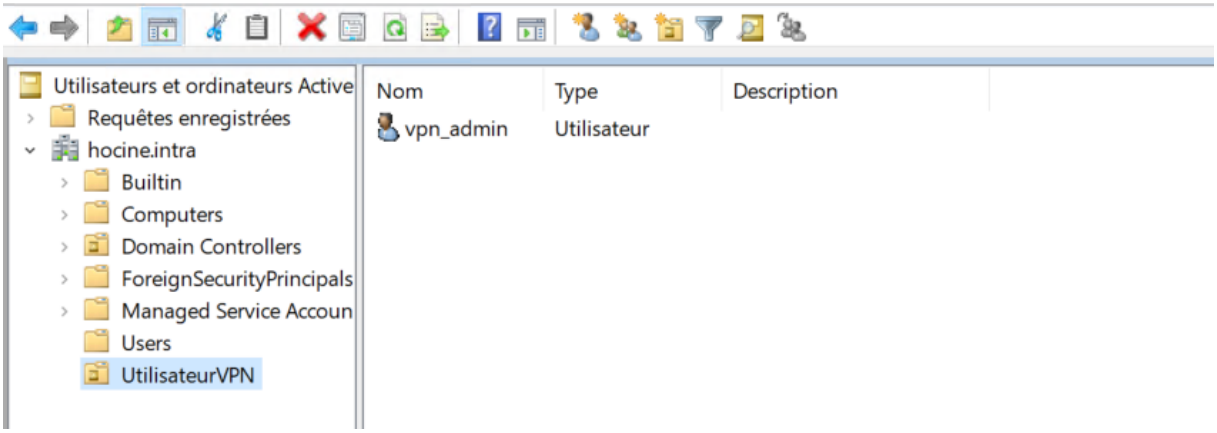
II. Configuration d'Active Directory (Windows Server)

- **Pour consulter la procédure d'installation et de configuration de l'Active Directory** cliquer ici

1. **Installer les rôles AD DS** via **Gestionnaire du Serveur → Ajouter des rôles et fonctionnalités.**

2. Promouvoir le serveur en **contrôleur de domaine** (créer une nouvelle forêt, etc.)

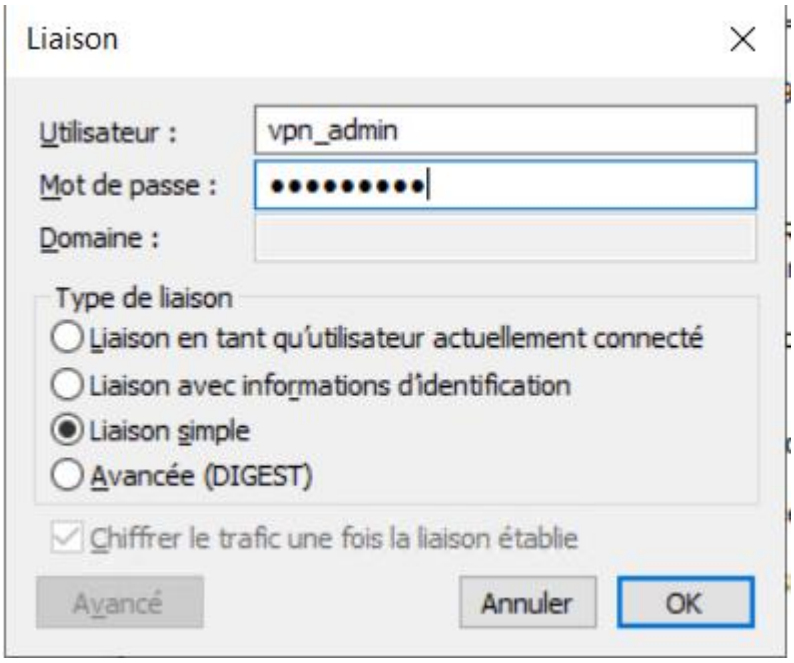
3. Toujours dans via **Gestionnaire du Serveur** allez dans **Utilisateurs et Ordinateurs Active Directory,** et créer une **OU** « UtilisateurVPN » et un utilisateur (ex. vpn_admin)



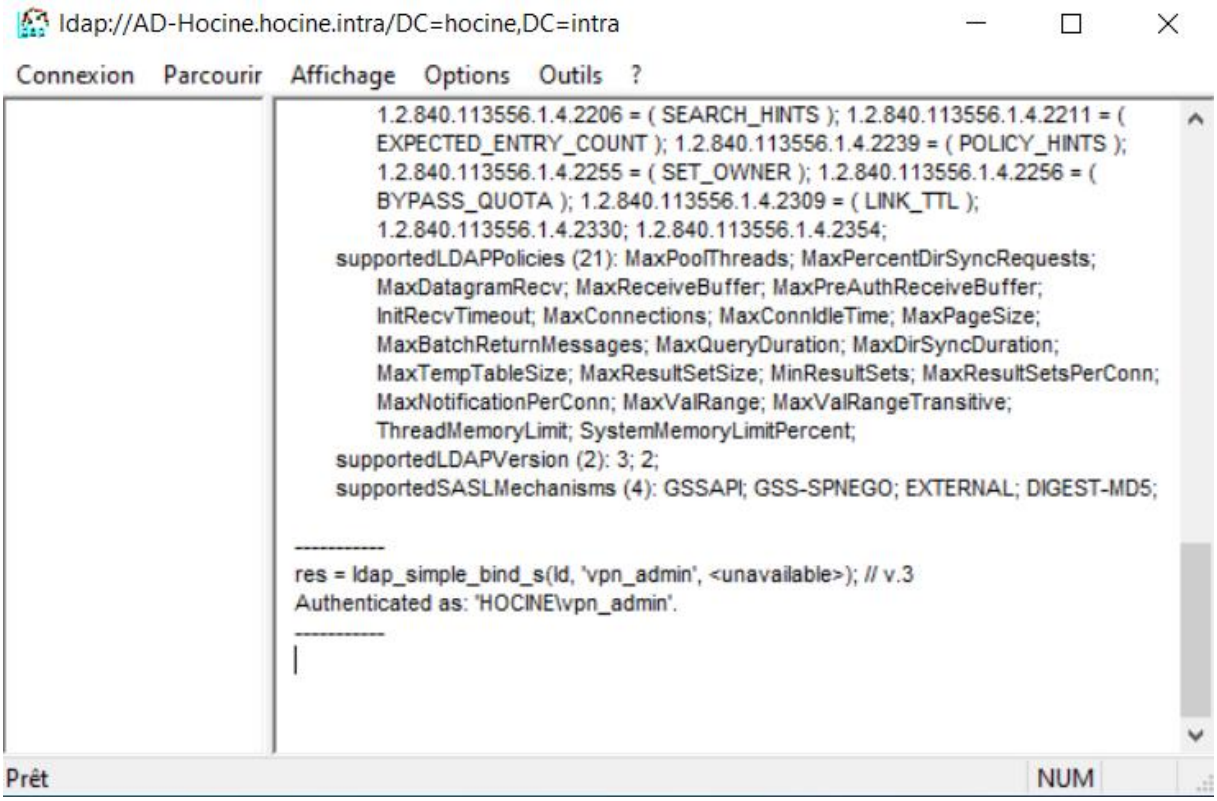
2) Test de la connectivité LDAP

1.Depuis le Server Windows, lancer **ldp.exe → Connexion → Se connecter,** saisissez l'adresse IP de votre Serveur AD dans « Serveur » et laisser le port en **389**

2. Maintenant toujours dans ldp.exe allez dans **Connexion → Lier**, sélectionner l'option « **Liaison Simple** » et saisirez les informations de l'utilisateur créer précédemment, dans notre exemple c'est avec le compte « vpn_admin »



4. Vous devez avoir le message « Authenticated as "VOTRE-DOMAINE\vpn_admin" » tout en bas de la page.



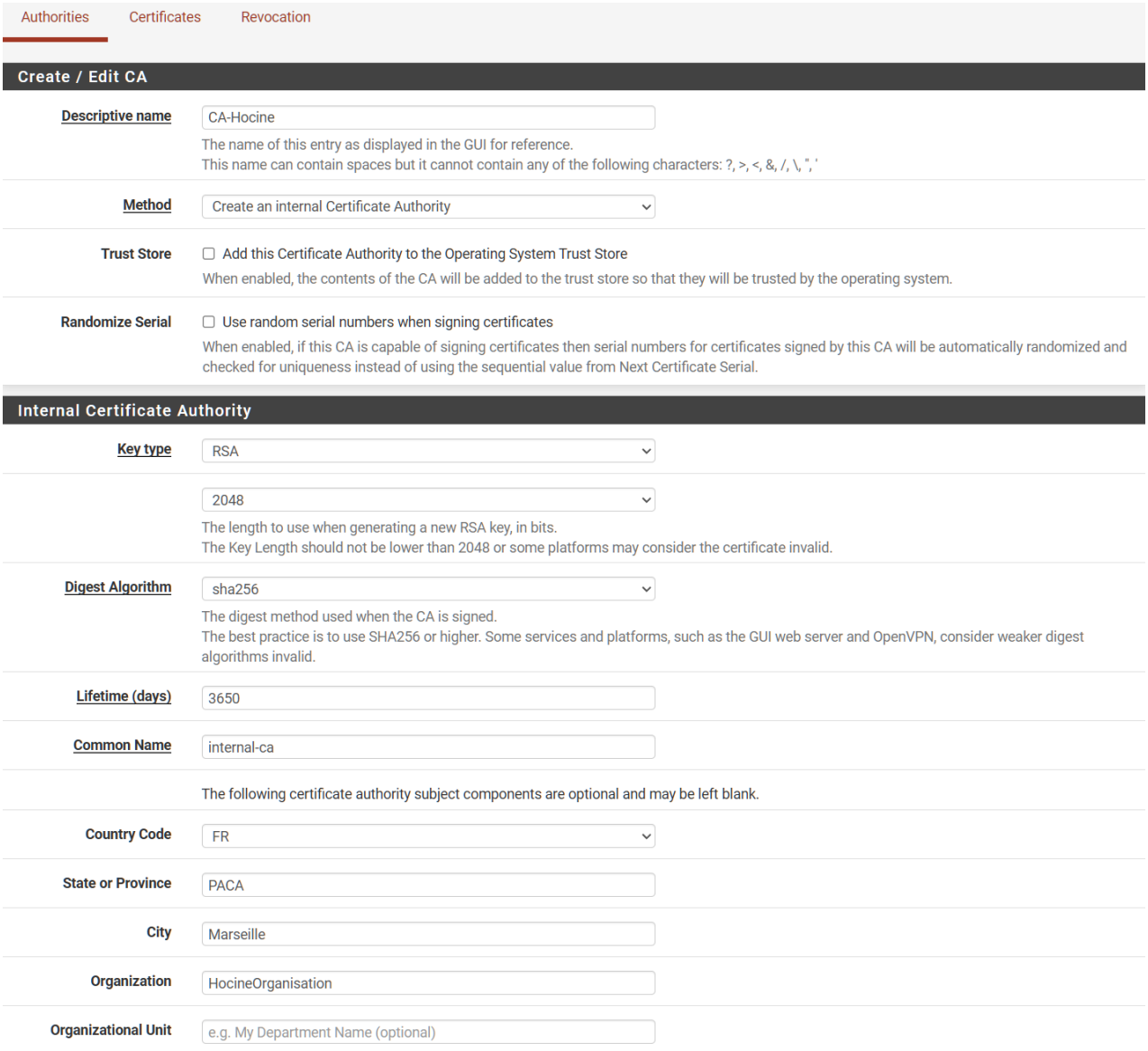
III. Certificats sur pfSense

- OpenVPN nécessite l'utilisation de certificats pour sécuriser la communication.

1. Créer une Autorité de Certification (CA)

1.1. Sur la page d'administration de Pfsense, accéder à **System** → Certificate → **Authorities → Add**

1.2. Sur cette page remplissez les differnet information demandé, comme montré sur l'image ci-dessous



2. Créer un certificat serveur OpenVPN

1.1 Naviguez dans **System > Cert. Manager > Certificates**.

1.2 Cliquer sur **Add/Sign**.

1.3 Renseigner un nom pour le certificat et veiller à choisir le type de certificat en « Server Certificate » ainsi qu'ajouter votre sous nom de domaine dans « Alternative Names » comme montré ci-dessous

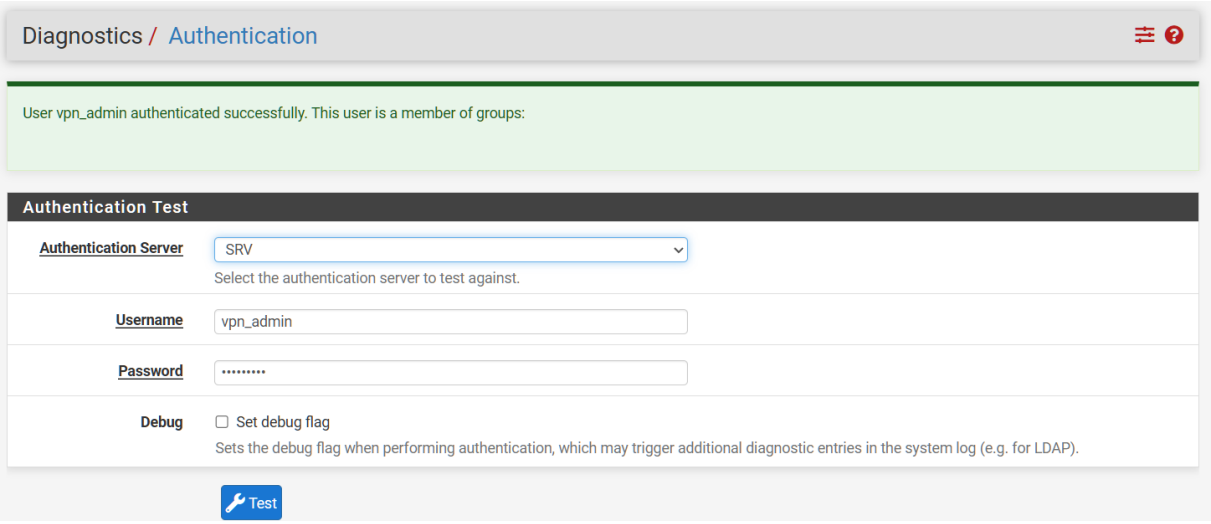
IV. Déclarer l'AD (LDAP) dans pfSense

Pour que pfSense puisse authentifier les utilisateurs VPN avec les comptes existants dans Active Directory, il est nécessaire de configurer un serveur LDAP dans pfSense. Cette étape permet de lier pfSense à l'AD et de restreindre l'accès uniquement aux utilisateurs autorisés.

1. pfSense → **System > User Manager > Authentication Servers** → **Add**.
2. Maintenant on doit saisir les informations suivantes :
    - **Descriptive name : Choisissez un nom de votre choix**
    - **Hostname/IP** : Adresse IP du Server AD
    - **Search scope :** Entire Subtree
    - **Base DN** : DC=domaine,DC=intra (dans notre exemple ça sera DC=hocine,DC=intra)
    - **Authentication containers :** OU=UtilisateurVPN,DC=hocine,DC=intra (N'oublier pas d'adapter selon votre infrastructure)
    - **Bind anonymous :** Décochez cette case
    - **Bind credentials** : DOMAINE\vpn_admin + Mot De Passe de l'utilisateur
    - **Initial Template : Microsoft AD**
    - **User naming attribute :** samAccountName

Test et validation :

- Allez dans Diagnostics → Authentication situé sur le menu supérieur de la page
- Tester avec un utilisateur de l'OU UtilisateurVPN
- Vous devrez avoir un message « Authentication successful »



V. Configuration d'OpenVPN via l'assistant pfSense

1. L'assistant va nous guider pour choisir l'authentification (ici, LDAP), la CA, le certificat serveur, et la configuration VPN.
    - Aller dans **VPN → OpenVPN → Wizards**. Et Sélectionner **LDAP**
    - **LDAP servers :** « Votre-Nom-Du-Server »
    - **Certificate Authority :** « CA Créer Précédemment »
    - **Certificate :** « Votre Certificat »

2. A l'étape 9 vous devez saisir ces informations ci-dessous :
    - Description : « Choisissez un nom de votre choix »
    - **Protocol :** Privilégier le TCP pour éviter la perte et la corruption de données et le UDP pour la vitesse de transfert, dans notre exemple nous allons choisir le protocole TCP IPv4
    - **Interface :** WAN
    - **IPv4 Tunnel Network :** ça sera l'IP de votre Tunnel VPN dans notre exemple nous allons choisir : 172.1.1.0/24
    - **Redirect IPv4 Gateway:** Cochez la case
    - **IPv4 Local Network :** vous pouvez définir un sou réseau local auquel les clients du VPN puissent accéder, dans notre exemple nous allons choisir : 192.168.100.0/24
    - **DNS Server 1 :** On choisit les DNS de google : 8.8.8.8
    - **DNS Server 2 :** 8.8.4.4

Step 9 of 11

Server Setup

OpenVPN Remote Access Server Setup Wizard

General OpenVPN Server Information

Description

VPN_Hocine

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

TCP 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.

Cryptographic Settings

TLS Authentication

☑ Enable authentication of TLS packets.

Generate TLS Key

☑ Automatically generate a shared TLS authentication key.

TLS Shared Key

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 diabled 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

No Hardware Crypto Acceleration

The hardware cryptographic accelerator to use for this VPN connection, if any.

Tunnel Settings

IPv4 Tunnel Network

172.1.1.0/24

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.

- Enfin : **sélectionner les deux case « Firewall Rule » et « OpenVPN rule »**

VI. Exportation et installation du client OpenVPN

Cette étape permet de générer les profils utilisateurs VPN à partir de pfSense et de les déployer sur les postes clients.

1. **Installation du package OpenVPN Client Export :**
   - Aller dans **System → Package Manager → Available Packages**.
   - Rechercher **openvpn-client-export**.
   - Cliquer sur **Install** et attendre la confirmation.

2. **Exporter un profil utilisateur :**
   - Aller dans **VPN → OpenVPN → Client Export**.
   - Tout en bas de la page, on doit sélectionner l'option : **Inline Configurations « Most Clients »**

3. **Modification du fichier de configuration OpenVPN pour utiliser l'IP publique :**
   - Cette étape est utile si le serveur OpenVPN est derrière un NAT ou si le fichier. ovpn exporté contient l'IP privée du serveur. On remplace alors la destination par l'IP publique.
   - Télécharger le fichier. Ovpn et ouvrez le avec un éditeur de texte :
   - Chercher la ligne commençant par : **« remote 192.168.1.200 1194 »** (192.168.1.200 étant d'IP interne de pfSense qui se trouve derrière un Routeur).
   - Remplacer l'IP privée par l'**IP publique** ou le **FQDN public** de ton serveur pfSense **: « remote VOTRE-IP-PUBLIQUE 1194 »**

   Si le serveur pfSense se trouve derrière un **routeur NAT**, il faut **rediriger le port OpenVPN** (TCP 1194 par défaut) vers l'IP local du Pfsense.

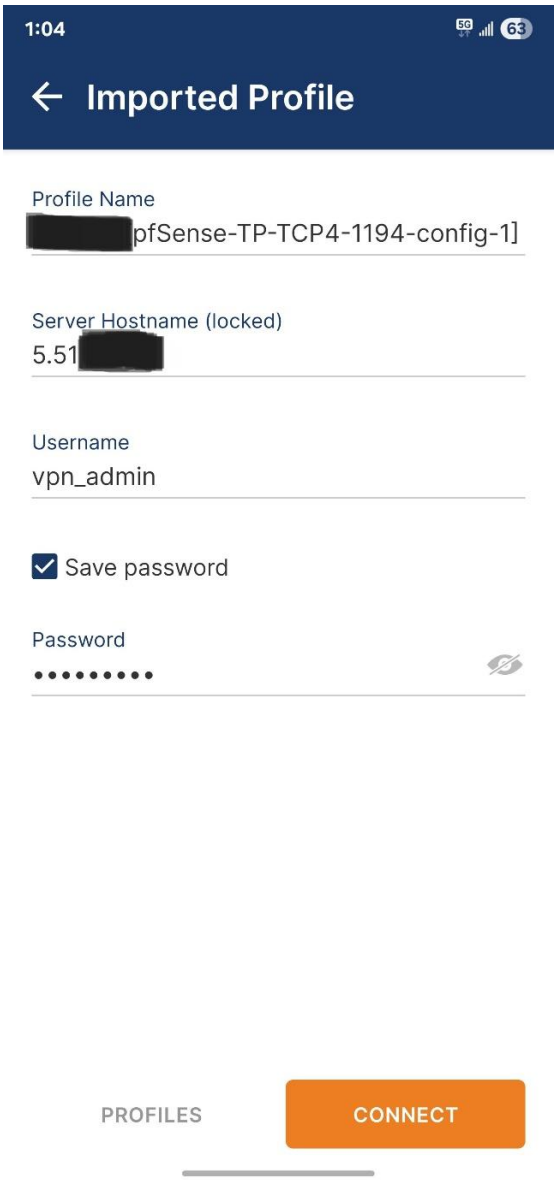
VII. Vérification depuis un mobile (OpenVPN Connect)

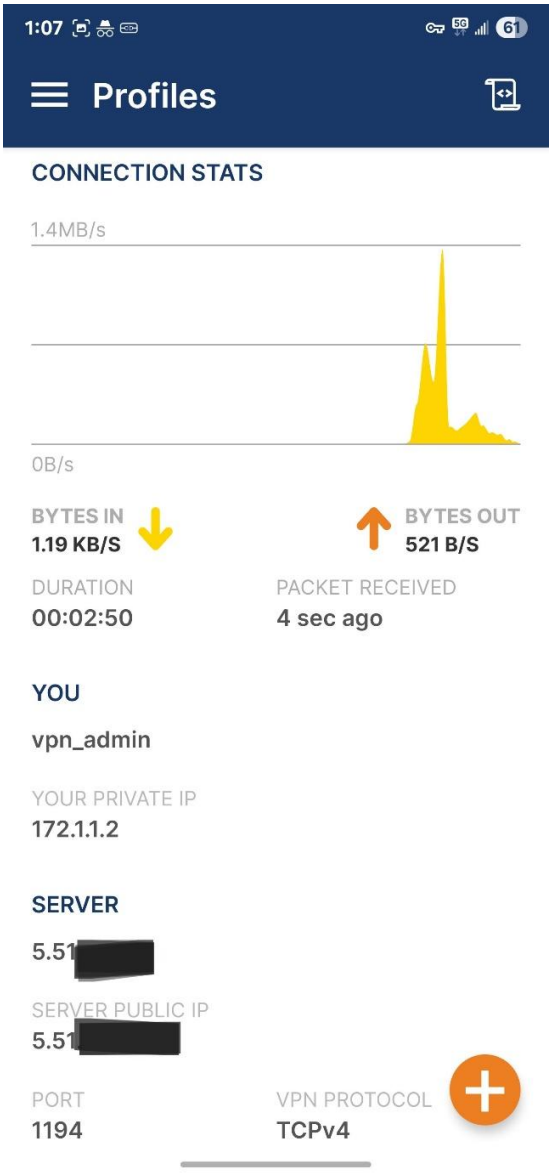
Cette étape permet de tester la connexion VPN depuis l'extérieur de ton réseau local (WAN), avec un appareil mobile utilisant une connexion 4G/5G.

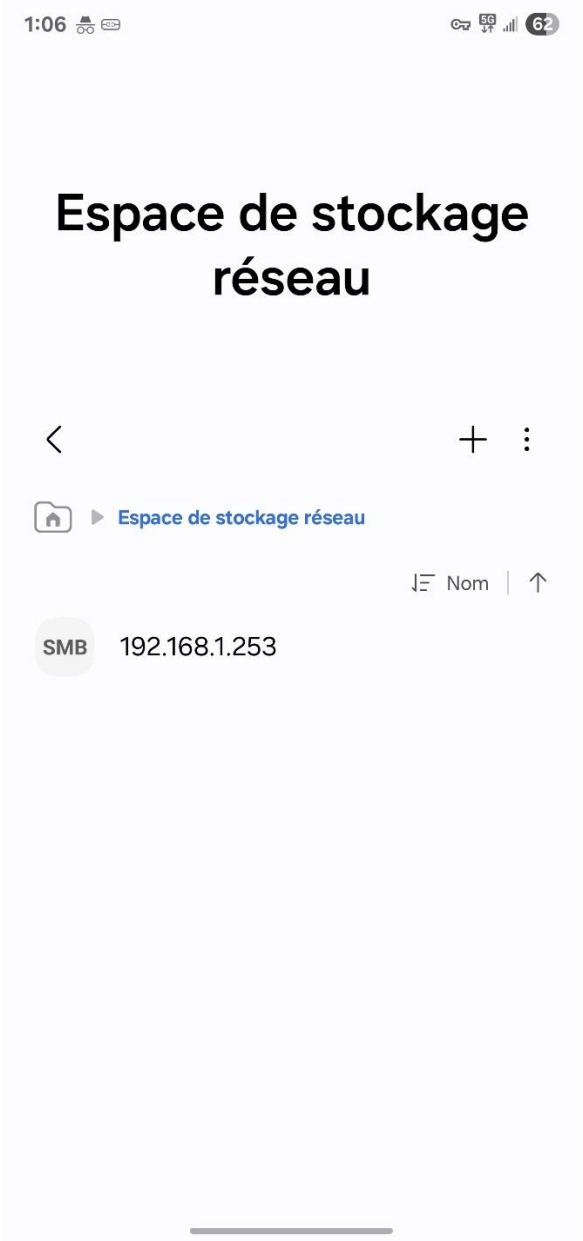
1. Installer l'application OpenVPN Connect
    - Télécharger **OpenVPN Connect** depuis l'App Store (iOS) ou Google Play (Android).

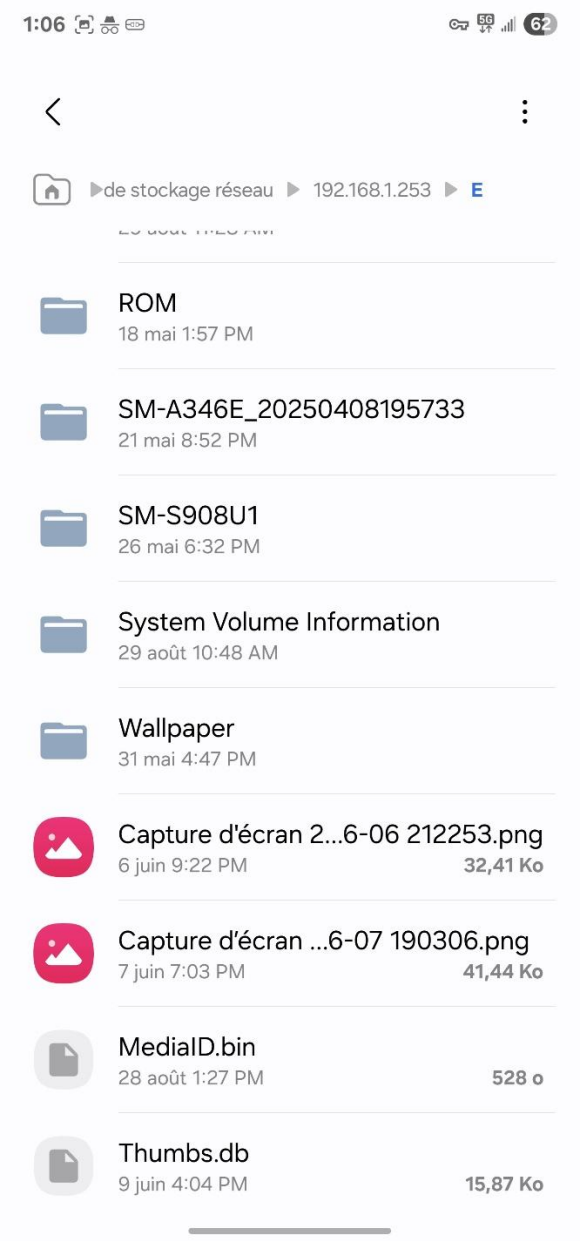
2. Importer le profil VPN :
    - Copier le fichier. ovpn sur le mobile
    - Dans OpenVPN Connect : **Importer le profil**.
    - Vérifier que le certificat et les informations d'authentification sont corrects.

3. Tests de connectivité :
    - Ping vers un serveur interne (ex. ping serveurAD.hocine.intra) si possible.
    - Vérifier l'accès à une ressource interne (partage réseau, application web interne).


1:04
Imported Profile
Profile Name
[redacted]pfSense-TP-TCP4-1194-config-1]
Server Hostname (locked)
5.51[redacted]
Username
vpn_admin
Save password
Password
••••••••••
PROFILES
CONNECT


1:07
Profiles
CONNECTION STATS
1.4MB/s
0B/s
BYTES IN
1.19 KB/S
BYTES OUT
521 B/S
DURATION
00:02:50
PACKET RECEIVED
4 sec ago
YOU
vpn_admin
YOUR PRIVATE IP
172.1.1.2
SERVER
5.51[redacted]
SERVER PUBLIC IP
5.51[redacted]
PORT
1194
VPN PROTOCOL
TCPv4


1:06
62
Espace de stockage réseau
Espace de stockage réseau
Nom
SMB
192.168.1.253


1:06
62
de stockage réseau
192.168.1.253
E
ROM
18 mai 1:57 PM
SM-A346E_20250408195733
21 mai 8:52 PM
SM-S908U1
26 mai 6:32 PM
System Volume Information
29 août 10:48 AM
Wallpaper
31 mai 4:47 PM
Capture d'écran 2...6-06 212253.png
6 juin 9:22 PM
32,41 Ko
Capture d'écran ...6-07 190306.png
7 juin 7:03 PM
41,44 Ko
MediaID.bin
28 août 1:27 PM
528 o
Thumbs.db
9 juin 4:04 PM
15,87 Ko