

# 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

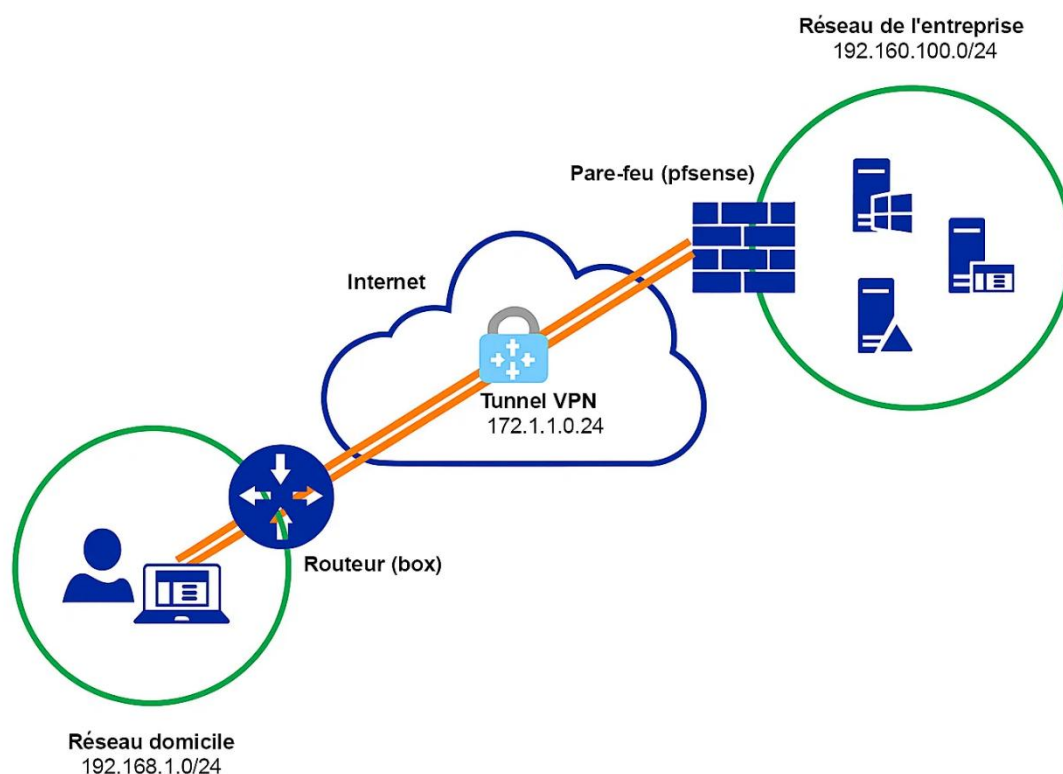
I.	Introduction .....	3
II.	Configuration d'Active Directory (Windows Server).....	4
III.	Certificats sur pfSense .....	6
IV.	Déclarer l'AD (LDAP) dans pfSense.....	8
V.	Configuration d'OpenVPN via l'assistant pfSense .....	9
VI.	Exportation et installation du client OpenVPN .....	12
VII.	Vérification depuis un mobile (OpenVPN Connect).....	13

# 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)**.

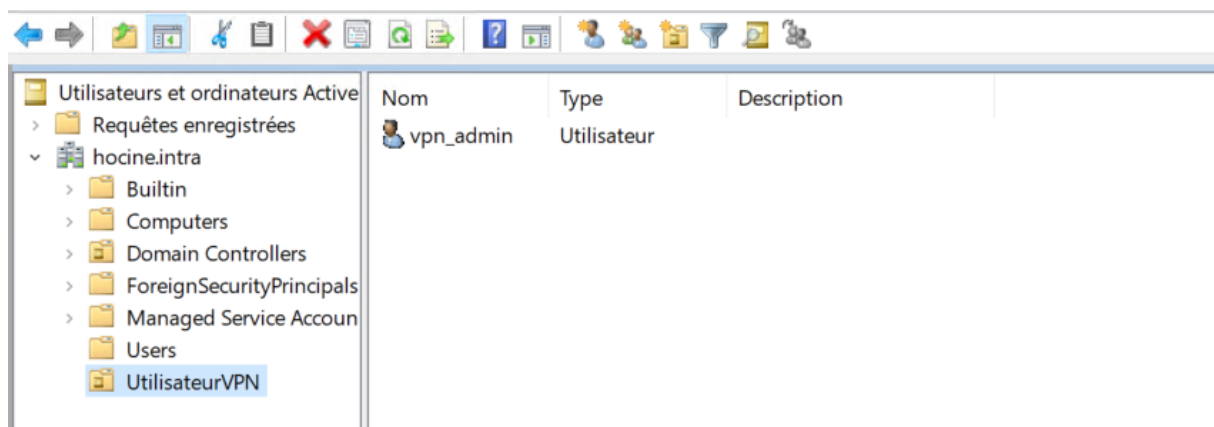
L'objectif est de permettre uniquement aux comptes contenus dans une **OU spécifique** par exemple : « **UtilisateurVPN** » de se connecter au VPN, garantissant ainsi un contrôle précis des accès.

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 laissez le port en **389**
2. Maintenant toujours dans ldp.exe allez dans **Connexion** → **Lier**, sélectionner l'option « **Liaison Simple** » et saisissez les informations de l'utilisateur créé précédemment, dans notre exemple c'est avec le compte « vpn\_admin »

Liaison

Utilisateur : vpn\_admin

Mot de passe : ••••••••

Domaine :

Type de liaison

☐ Liaison en tant qu'utilisateur actuellement connecté

☐ Liaison avec informations d'identification

☒ Liaison simple

☐ Avancée (DIGEST)

☒ Chiffrer le trafic une fois la liaison établie

Avancé Annuler OK

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

Idap://AD-Hocine.hocine.intra/DC=hocine,DC=intra

Connexion Parcourir Affichage Options Outils ?

```

1.2.840.113556.1.4.2206 = ( SEARCH_HINTS ); 1.2.840.113556.1.4.2211 = (
EXPECTED_ENTRY_COUNT ); 1.2.840.113556.1.4.2239 = ( POLICY_HINTS );
1.2.840.113556.1.4.2255 = ( SET_OWNER ); 1.2.840.113556.1.4.2256 = (
BYPASS_QUOTA ); 1.2.840.113556.1.4.2309 = ( LINK_TTL );
1.2.840.113556.1.4.2330; 1.2.840.113556.1.4.2354;
supportedLDAPPolicies (21): MaxPoolThreads; MaxPercentDirSyncRequests;
MaxDatagramRecv; MaxReceiveBuffer; MaxPreAuthReceiveBuffer;
InitRecvTimeout; MaxConnections; MaxConnIdleTime; MaxPageSize;
MaxBatchReturnMessages; MaxQueryDuration; MaxDirSyncDuration;
MaxTempTableSize; MaxResultSetSize; MinResultSets; MaxResultSetsPerConn;
MaxNotificationPerConn; MaxValRange; MaxValRangeTransitive;
ThreadMemoryLimit; SystemMemoryLimitPercent;
supportedLDAPVersion (2): 3; 2;
supportedSASLMechanisms (4): GSSAPI; GSS-SPNEGO; EXTERNAL; DIGEST-MD5;

-----
res = ldap_simple_bind_s(ld, 'vpn_admin', <unavailable>); // v.3
Authenticated as: 'HOCINE\vpn_admin'.
-----

```

Prêt NUM

### 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 différentes informations demandées, comme montré sur l'image ci-dessous

Authorities	Certificates	Revocation
<b>Create / Edit CA</b>		
<b>Descriptive name</b>	<input type="text" value="CA-Hocine"/> <small>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: ?, &gt;, &lt;, &amp;, /, \, " , ' ,</small>	
<b>Method</b>	<input type="text" value="Create an internal Certificate Authority"/>	
<b>Trust Store</b>	<input type="checkbox"/> Add this Certificate Authority to the Operating System Trust Store <small>When enabled, the contents of the CA will be added to the trust store so that they will be trusted by the operating system.</small>	
<b>Randomize Serial</b>	<input type="checkbox"/> Use random serial numbers when signing certificates <small>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.</small>	
<b>Internal Certificate Authority</b>		
<b>Key type</b>	<input type="text" value="RSA"/>	
	<input type="text" value="2048"/> <small>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.</small>	
<b>Digest Algorithm</b>	<input type="text" value="sha256"/> <small>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.</small>	
<b>Lifetime (days)</b>	<input type="text" value="3650"/>	
<b>Common Name</b>	<input type="text" value="internal-ca"/>	
<small>The following certificate authority subject components are optional and may be left blank.</small>		
<b>Country Code</b>	<input type="text" value="FR"/>	
<b>State or Province</b>	<input type="text" value="PACA"/>	
<b>City</b>	<input type="text" value="Marseille"/>	
<b>Organization</b>	<input type="text" value="HocineOrganisation"/>	
<b>Organizational Unit</b>	<input type="text" value="e.g. My Department Name (optional)"/>	

## 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

Add/Sign a New Certificate					
<b>Method</b>	Create an internal Certificate				
<b>Descriptive name</b>	OpenVPN-Server <small>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: ?, &gt;, &lt;, &amp;, /, \, ", '.</small>				
Internal Certificate					
<b>Certificate authority</b>	CA-Hocine				
<b>Key type</b>	RSA				
	2048 <small>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.</small>				
<b>Digest Algorithm</b>	sha256 <small>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.</small>				
<b>Lifetime (days)</b>	3650 <small>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.</small>				
<b>Common Name</b>	hocine.intra				
<small>The following certificate subject components are optional and may be left blank.</small>					
<b>Country Code</b>	FR				
<b>State or Province</b>	PACA				
<b>City</b>	Marseille				
<b>Organization</b>	HocineOrganisation				
<b>Organizational Unit</b>	e.g. My Department Name (optional)				
Certificate Attributes					
<b>Attribute Notes</b>	<p>The following attributes are added to certificates and requests when they are created or signed. These attributes behave differently depending on the selected mode.</p> <p>For Internal Certificates, these attributes are added directly to the certificate as shown.</p>				
<b>Certificate Type</b>	Server Certificate <small>Add type-specific usage attributes to the signed certificate. Used for placing usage restrictions on, or granting abilities to, the signed certificate.</small>				
<b>Alternative Names</b>	<table><tr><td>FQDN or Hostname</td><td>vpn.hocine.intra</td></tr><tr><td>Type</td><td>Value</td></tr></table> <p>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.</p>	FQDN or Hostname	vpn.hocine.intra	Type	Value
FQDN or Hostname	vpn.hocine.intra				
Type	Value				
<b>Add SAN Row</b>	<a href="#">+ Add SAN Row</a>				

## 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 »

The screenshot shows the 'Diagnostics / Authentication' page in pfSense. A green message box at the top states: 'User vpn\_admin authenticated successfully. This user is a member of groups:'. Below this is the 'Authentication Test' section, which includes a dropdown menu for 'Authentication Server' set to 'SRV', a text field for 'Username' containing 'vpn\_admin', and a password field. At the bottom, there is a 'Debug' checkbox labeled 'Set debug flag' with a description: 'Sets the debug flag when performing authentication, which may trigger additional diagnostic entries in the system log (e.g. for LDAP)'. A blue 'Test' button is located at the bottom of the form.



## 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

## 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 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 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.

<b>IPv4 Local Network</b>	<input type="text" value="192.168.100.0/24"/> <p>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.</p>
<b>Concurrent Connections</b>	<input type="text"/> <p>Specify the maximum number of clients allowed to concurrently connect to this server.</p>
<b>Allow Compression</b>	<input type="button" value="Refuse any non-stub compression (Most secure)"/> <p>Allow compression to be used with this VPN instance, which is potentially insecure.</p>
<b>Compression</b>	<input type="button" value="Disable Compression [Omit Preference]"/> <p>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.</p>
<b>Type-of-Service</b>	<input type="checkbox"/> Set the TOS IP header value of tunnel packets to match the encapsulated packet's TOS value.
<b>Inter-Client Communication</b>	<input type="checkbox"/> Allow communication between clients connected to this server.
<b>Duplicate Connections</b>	<input type="checkbox"/> Allow multiple concurrent connections from clients using the same Common Name. NOTE: This is not generally recommended, but may be needed for some scenarios.
<b>Duplicate Connection Limit</b>	<input type="text"/> <p>Limit the number of concurrent connections from the same user.</p>

**Client Settings**

<b>Dynamic IP</b>	<input checked="" type="checkbox"/> Allow connected clients to retain their connections if their IP address changes.
-------------------	--

<b>Topology</b>	<input type="button" value="Subnet – One IP address per client in a common subnet"/> <p>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".</p>
-----------------	---

**Advanced Client Settings**

<b>DNS Default Domain</b>	<input type="text"/> <p>Provide a default domain name to clients.</p>
<b>DNS Server 1</b>	<input type="text" value="8.8.8.8"/> <p>DNS server IP to provide to connecting clients.</p>
<b>DNS Server 2</b>	<input type="text" value="8.8.4.4"/> <p>DNS server IP to provide to connecting clients.</p>
<b>DNS Server 3</b>	<input type="text"/> <p>DNS server IP to provide to connecting clients.</p>
<b>DNS Server 4</b>	<input type="text"/> <p>DNS server IP to provide to connecting clients.</p>
<b>NTP Server</b>	<input type="text"/> <p>Network Time Protocol server to provide to connecting clients.</p>
<b>NTP Server 2</b>	<input type="text"/> <p>Network Time Protocol server to provide to connecting clients.</p>
<b>NetBIOS Options</b>	<input type="checkbox"/> Enable NetBIOS over TCP/IP. If this option is not set, all NetBIOS-over-TCP/IP options (including WINS) will be disabled.
<b>NetBIOS Node Type</b>	<input type="button" value="none"/>

- 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

5G

63

←

Imported Profile

Profile Name

pfSense-TP-TCP4-1194-config-1]

Server Hostname (locked)

5.51

Username

vpn\_admin

☒ Save password

Password

.....

PROFILES

CONNECT

1:07

5G

61

≡

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

SERVER PUBLIC IP

5.51

PORT

1194

VPN PROTOCOL

TCPv4

+

