PortailSIO

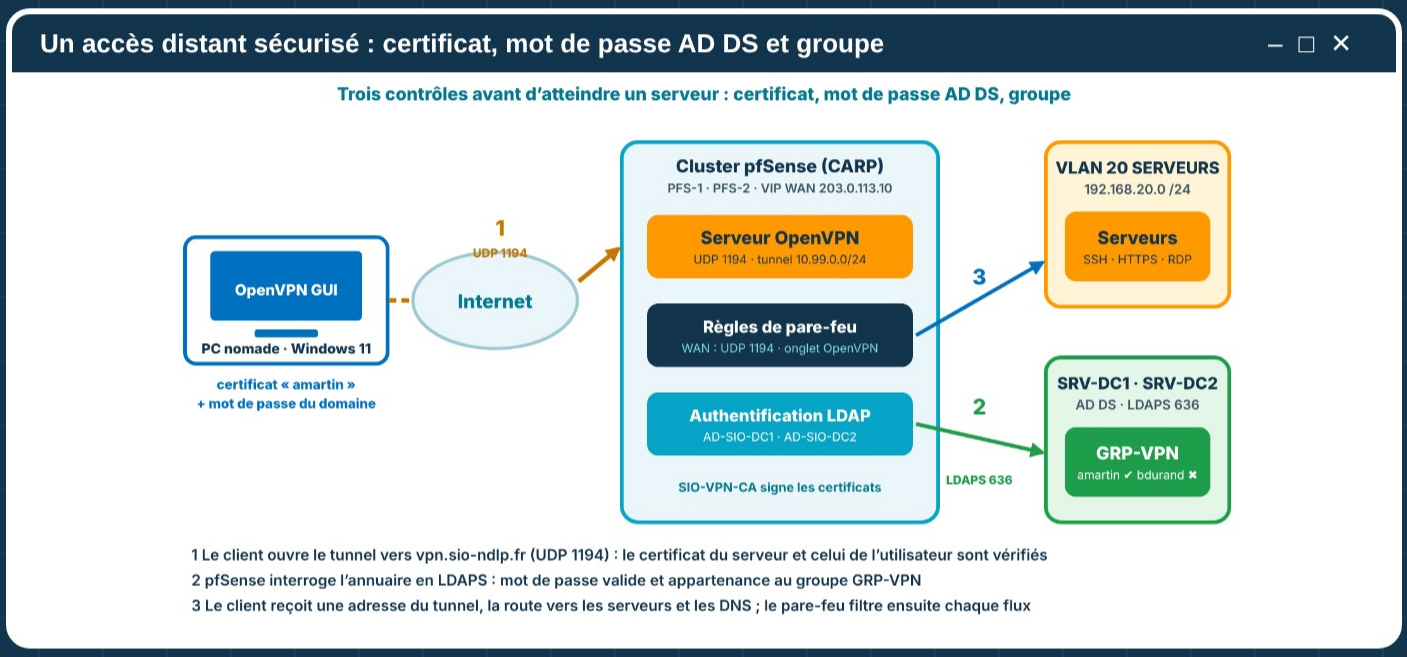
NOUVELLE FORMULE

TUTORIEL

PFSENSE · LDAPS · AD DS

Accès distant sécurisé avec OPENVPN

NIVEAU
Expert



1 Comprendre l'architecture et préparer AD DS	2 Importer SIO-CA et créer l'autorité de certification du VPN
3 Lier pfSense à l'annuaire en LDAPS et tester	4 Créer le serveur OpenVPN d'accès distant
5 Délivrer les certificats et ouvrir le pare-feu	6 Exporter, connecter un client et exploiter

CC BY-NC
Utilisation commerciale interdite
© PortailSIO – 11/2026

Ce tutoriel en ligne
Scannez le QR code. Tous les tutoriels :
portail.sio-ndlp.fr/tutoriels.php

Ce tutoriel a été réalisé avec l'hyperviseur © Proxmox VE. Il peut être réalisé dans un environnement de virtualisation personnel à l'aide des logiciels © VirtualBox ou © VMware Player. Il **suppose que vous avez réalisé les tutoriels précédents** : réplication AD DS (**SRV-DC1** et **SRV-DC2** sous Windows Server 2025), **activation de LDAPS** (autorité de certification **SIO-CA** et certificats des contrôleurs de domaine) et mise en place du **cluster pfSense en haute disponibilité** (nœuds **PFS-1** et **PFS-2**, adresses virtuelles CARP). Il faut aussi un **poste Windows 11 situé hors du réseau du lycée** (un partage de connexion de téléphone convient très bien) pour tester le VPN comme le ferait un utilisateur nomade.

Un **VPN d'accès distant** (*road warrior*) permet à un enseignant, un technicien ou un élève en stage de **rejoindre le réseau interne depuis Internet** : le poste nomade établit un tunnel chiffré avec le pare-feu, reçoit une adresse du réseau du VPN et peut alors joindre les serveurs autorisés comme s'il était sur place. Le point sensible, c'est la **gestion des comptes** : créer des utilisateurs à part dans le pare-feu, avec des mots de passe distincts de ceux du domaine, est une source d'oublis et de comptes qui survivent au départ de leur propriétaire. Nous allons donc **authentifier les utilisateurs auprès d'Active Directory**, avec **leur mot de passe habituel**, et limiter l'accès aux **membres d'un seul groupe**.

Les écrans de pfSense correspondent à la version **CE 2.9** ; ils sont très proches en 2.8 et sur pfSense Plus. L'interface est en anglais : les noms des menus et des champs sont donnés tels qu'ils s'affichent. Dans le cadre de ce tutoriel, nous utilisons les paramètres suivants (valeurs données à titre d'exemple : adaptez-les à votre réseau) :

Élément	Valeur	Remarque
Nom et adresse publics du VPN	vpn.sio-ndlp.fr → 203.0.113.10	Adresse virtuelle CARP du WAN (203.0.113.0 /24 est une plage réservée à la documentation : remplacez-la)
Port du serveur	UDP 1194	Le port par défaut d'OpenVPN
Réseau du tunnel	10.99.0.0 /24	Adresses attribuées aux clients ; ne doit chevaucher aucun réseau du lycée
Réseau accessible par le VPN	192.168.20.0 /24 (VLAN 20 SERVEURS)	Les autres VLAN restent inaccessibles
Serveurs DNS donnés aux clients	192.168.20.250 et 192.168.20.251	Les contrôleurs de domaine : les noms en sio.local fonctionnent à distance
Groupe AD autorisé	GRP-VPN	Seuls ses membres peuvent se connecter
Compte de lecture de l'annuaire	svc-pfsense	Compte ordinaire du domaine, sans aucun droit particulier
Autorité de certification du VPN	SIO-VPN-CA	Créée dans pfSense : elle signe le certificat du serveur et ceux des utilisateurs

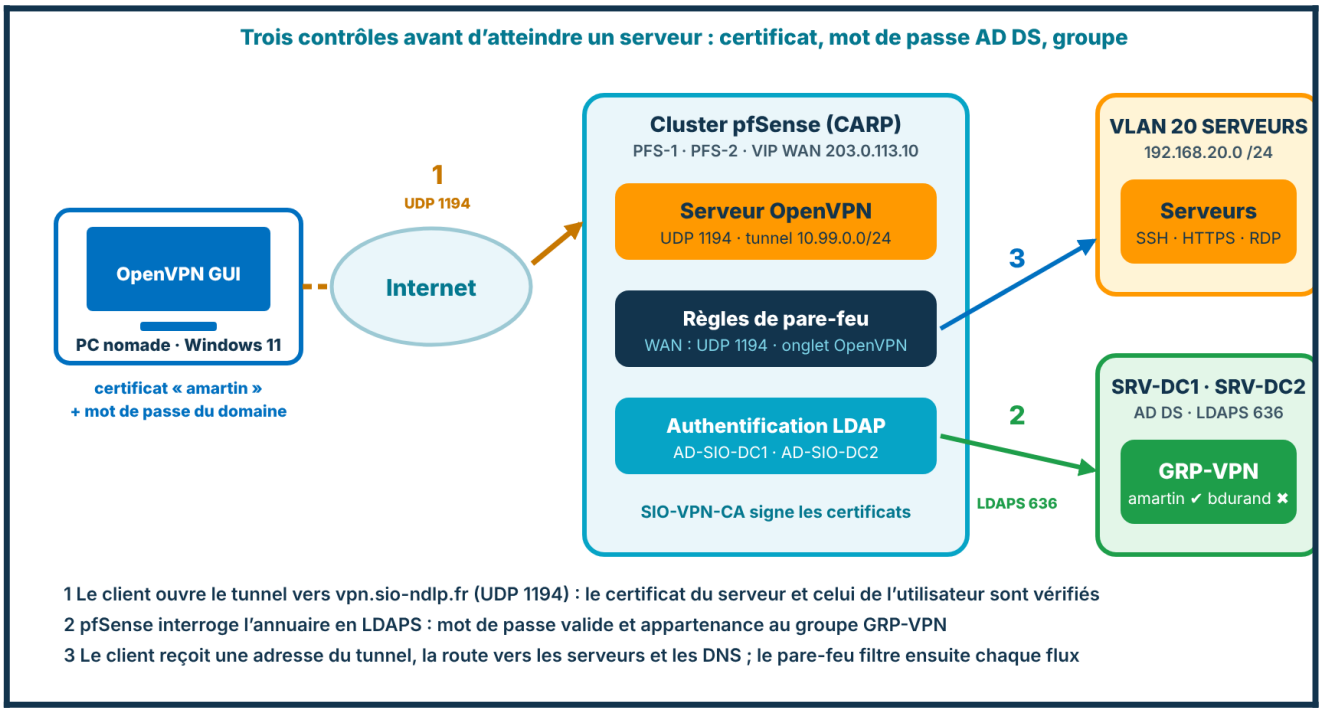
01 ÉTAPE 1 SUR 6 Comprendre l'architecture et préparer AD DS

A – Quel type d'authentification choisir ?

OpenVPN sait authentifier un utilisateur de trois façons. Le choix détermine ce que l'utilisateur doit **prouver** pour entrer :

Mode du serveur (pfSense)	Ce que le client présente	Verdict
Remote Access (SSL/TLS)	Un **certificat** par utilisateur, rien d'autre	Un ordinateur volé ou copié donne l'accès : pas de mot de passe à connaître
Remote Access (User Auth)	Un **mot de passe** du domaine, sans certificat personnel	Simple à déployer, mais un mot de passe volé ou deviné suffit
Remote Access (SSL/TLS + User Auth)	Un **certificat et** un **mot de passe** du domaine	Méthode retenue : deux éléments à réunir (ce que l'on possède et ce que l'on sait)

Notre VPN combine donc **trois contrôles**, que le schéma suivant résume. Le premier est cryptographique, les deux autres s'appuient sur l'annuaire : un client doit **présenter un certificat signé par SIO-VPN-CA**, **connaître le mot de passe** de son compte du domaine et **appartenir au groupe GRP-VPN**. Chaque contrôle écarte une catégorie d'intrus : le certificat arrête ceux qui ne possèdent pas le poste, le mot de passe arrête ceux qui ont trouvé le fichier, le groupe arrête les comptes valides qui n'ont aucune raison d'être là (un élève, un ancien collègue).



REMARQUE IMPORTANTE

L'authentification par **certificat seul** ou par **mot de passe seul** est une faiblesse connue des VPN d'accès distant. Le mot de passe est celui du **domaine** : il est donc **réutilisé** sur d'autres services et peut être exposé par une fuite ailleurs. Combiné à un certificat propre au VPN, il ne suffit plus. Pour aller plus loin, on ajoute un **second facteur** (code à usage unique) : cela demande un serveur RADIUS et sort du cadre de ce tutoriel.

B – Préparer l'annuaire : compte de service, groupe et membres

pfSense a besoin d'un compte pour **interroger l'annuaire** : il s'en sert pour retrouver l'utilisateur qui se connecte et vérifier son appartenance au groupe. Ce compte ne doit pas être un administrateur : il ne lit que ce que tout utilisateur du domaine peut lire. Sur **SRV-DC1**, ouvrez PowerShell en tant qu'administrateur, créez les unités d'organisation, le compte **svc-pfsense** et le groupe **GRP-VPN** (si ces objets existent déjà, ignorez les messages « existe déjà ») :

POWERSHELL

```
$base = "DC=sio,DC=local"
New-ADOrganizationalUnit -Name "Comptes de service" -Path $base
New-ADOrganizationalUnit -Name "Groupes" -Path $base
$mdp = Read-Host -AsSecureString "Mot de passe de svc-pfsense"
New-ADUser -Name "svc-pfsense" -SamAccountName "svc-pfsense" `
    -UserPrincipalName "svc-pfsense@sio.local" `
    -Path "OU=Comptes de service,$base" -AccountPassword $mdp `
    -Enabled $true -PasswordNeverExpires $true -CannotChangePassword $true
New-ADGroup -Name "GRP-VPN" -GroupScope Global -Path "OU=Groupes,$base"
```

Placez dans le groupe **uniquement les personnes autorisées**. Ici, **amartin** (créée dans les tutoriels précédents) peut se connecter ; **bdurand** a un compte valide mais n'est pas ajoutée : elle servira à vérifier que le refus fonctionne. Contrôlez ensuite le résultat :

POWERSHELL

```
Add-ADGroupMember -Identity "GRP-VPN" -Members amartin
Get-ADGroupMember "GRP-VPN" | Select Name, SamAccountName
Get-ADUser svc-pfsense | Select Name, Enabled, DistinguishedName
(Get-ADUser bdurand -Properties MemberOf).MemberOf
```

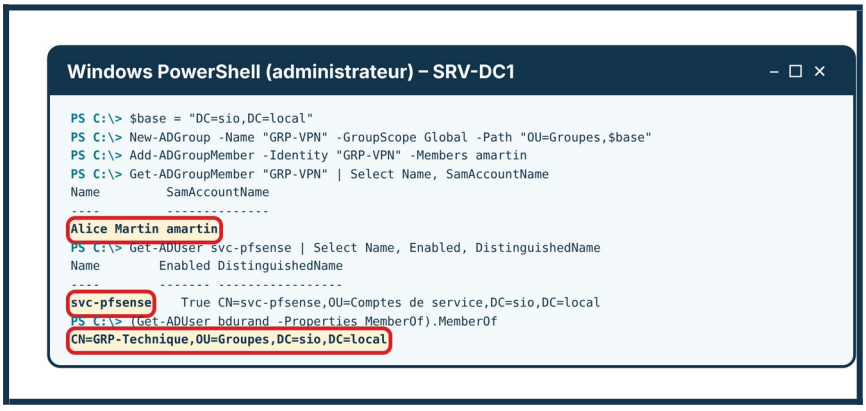


Figure 1 – PowerShell : groupe GRP-VPN, compte de service et membres

À SAVOIR

Retenez le chemin complet du groupe (**CN=GRP-VPN,OU=Groupes,DC=sio,DC=local**) : il sert à l'étape 3. Le mot de passe de **svc-pfsense** n'expire pas, sinon le VPN cesserait de fonctionner le jour de l'expiration.

À SAVOIR

Gérer l'accès au VPN revient désormais à **ajouter ou retirer une personne de GRP-VPN**, dans la console « Utilisateurs et ordinateurs Active Directory » : aucune modification dans pfSense. Quand un enseignant quitte l'établissement, la désactivation de son compte AD ferme aussi son accès VPN.

✔ POINT DE CONTRÔLE

- Le compte **svc-pfsense** existe, est activé et son mot de passe n'expire pas
- Le groupe **GRP-VPN** existe et contient **amartin** uniquement
- **bdurand** est un utilisateur valide qui **n'est pas** dans GRP-VPN

ÉTAPE 2 SUR 6

02 Importer SIO-CA et créer l'autorité de certification du VPN

Deux autorités de certification interviennent, pour **deux usages différents** qu'il ne faut pas confondre :

Autorité	Origine	Rôle dans ce tutoriel
SIO-CA	Existante (AD CS, sur SRV-DC1)	pfSense lui fait confiance pour **vérifier le certificat LDAPS** des contrôleurs de domaine (étape 3)
SIO-VPN-CA	Créée dans pfSense	Signe le **certificat du serveur VPN** et ceux des **utilisateurs** : seuls ces certificats sont acceptés par le VPN

On aurait pu réutiliser SIO-CA pour le VPN, mais tout certificat qu'elle a signé (un site web interne, un contrôleur de domaine…) serait alors **valable pour la première étape de la connexion**. Avec une autorité dédiée, **seuls les certificats délivrés pour le VPN** ouvrent la porte.

A – Exporter le certificat de SIO-CA (au format PEM)

pfSense attend le certificat de l'autorité au format **PEM** (du texte commençant par `-----BEGIN CERTIFICATE-----`). Sur **SRV-DC1**, exportez-le puis copiez son contenu dans le presse-papiers :

POWERSHELL

```
New-Item -ItemType Directory -Path C:\Temp -Force | Out-Null
certutil -ca.cert C:\Temp\SIO-CA.cer
certutil -encode C:\Temp\SIO-CA.cer C:\Temp\SIO-CA.pem
Get-Content C:\Temp\SIO-CA.pem -Raw | Set-Clipboard
```

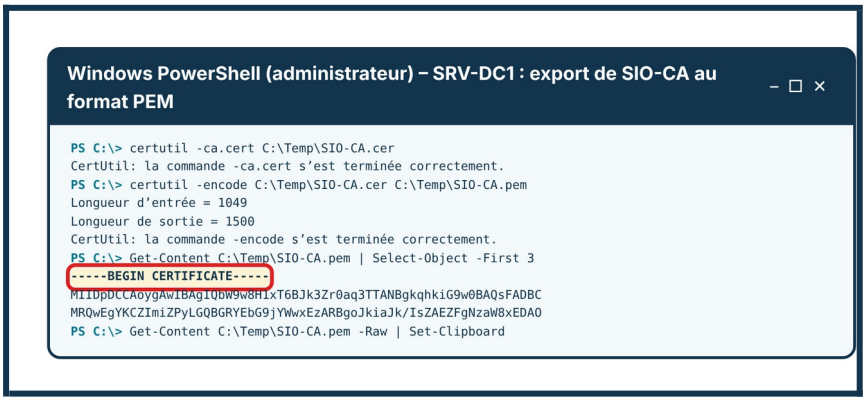


Figure 2 – Export de SIO-CA : conversion du fichier .cer en PEM

À SAVOIR

La commande « -ca.cert » produit un fichier binaire (DER) ; « -encode » le convertit en texte. Ce fichier ne contient que la partie **publique** de la CA : il peut circuler. N'exportez jamais sa clé privée.

B – Importer SIO-CA dans pfSense

Connectez-vous à l'interface web du nœud maître **PFS-1** (`https://pfs-1.sio.local`) puis effectuez les manipulations suivantes :

1. Cliquez le menu « **System** » puis « **Certificates** » (« **Cert. Manager** » dans les versions plus anciennes) et choisissez l'onglet « **Authorities** » ; cliquez « **+ Add** »
2. « **Descriptive name** » : `SIO-CA` ; « **Method** » : « **Import an existing Certificate Authority** »
3. « **Certificate data** » : collez le contenu du presse-papiers (Ctrl+V) ; laissez vide « **Certificate Private Key** » puis cliquez « **Save** » :

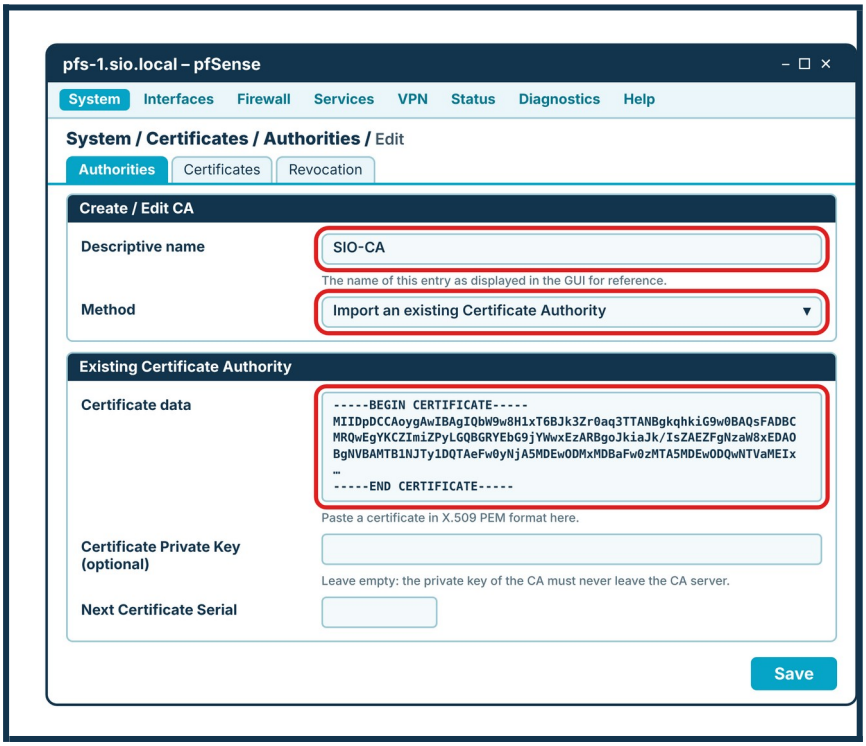


Figure 3 – System > Certificates > Authorities : importer SIO-CA

À SAVOIR

Le champ « Certificate Private Key » reste **vide** : pfSense n'a besoin que de la partie publique pour vérifier des certificats, pas pour en signer.

C – Créer l'autorité de certification du VPN

1. Dans l'onglet « **Authorities** », cliquez de nouveau « **+ Add** »
2. « **Descriptive name** » : `SIO-VPN-CA` ; « **Method** » : « **Create an internal Certificate Authority** »
3. « **Key type** » : « **RSA** » et « **4096** » ; « **Digest Algorithm** » : « **sha256** » ; « **Lifetime (days)** » : `3650` (dix ans : une autorité se renouvelle rarement, ses certificats bien plus souvent)

4 « **Common Name** » : `SIO-VPN-CA` ; renseignez le pays (`FR`), la région, la ville et l'organisation, puis cliquez « **Save** » :

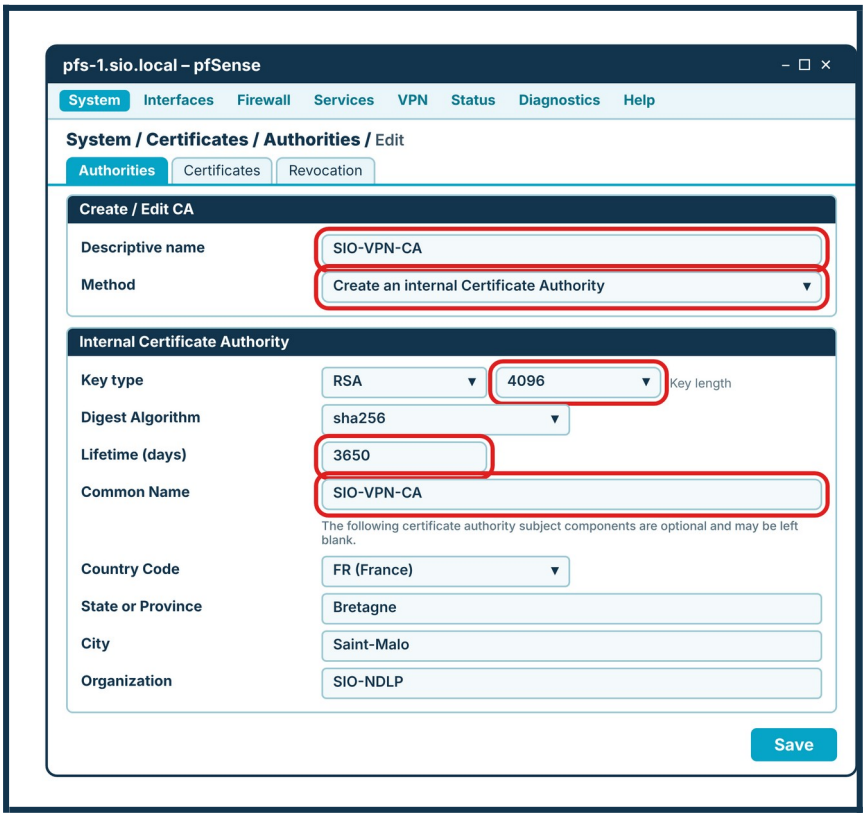


Figure 4 – System > Certificates > Authorities : créer SIO-VPN-CA

À SAVOIR

Les champs « State », « City » et « Organization » sont des informations d'exemple : renseignez celles de votre établissement. Ils apparaîtront dans tous les certificats que cette autorité signera.

REMARQUE IMPORTANTE

La **clé privée de SIO-VPN-CA** est stockée dans la configuration de pfSense : celui qui la détient peut fabriquer des certificats acceptés par le VPN. **Sauvegardez la configuration** (« **Diagnostics > Backup & Restore** ») après chaque création de certificat, conservez le fichier XML **hors du pare-feu** et protégez-le comme un secret. La synchronisation HA (étape 5) copie la clé sur PFS-2 : les deux nœuds sont donc à protéger.

D – Créer le certificat du serveur VPN

Ce certificat est celui que **présente le serveur** aux clients. Le client le vérifie : si son nom ne correspond pas à l'adresse qu'il contacte, ou s'il n'est pas signé par SIO-VPN-CA, la connexion est refusée. C'est ce qui empêche un faux serveur de se faire passer pour le vôtre.

1 Cliquez l'onglet « **Certificates** » puis « **+ Add/Sign** » ; « **Method** » : « **Create an internal Certificate** » ; « **Descriptive name** » : `vpn.sio-ndlp.fr`

2 « **Certificate authority** » : « **SIO-VPN-CA** » ; « **Key type** » : « **RSA** » et « **2048** » ; « **Lifetime (days)** » : `730`

3 « **Common Name** » : `vpn.sio-ndlp.fr` (le **nom que les clients utiliseront** pour se connecter)

4 Dans « **Certificate Attributes** » : « **Certificate Type** » : « **Server Certificate** » ; « **Alternative Names** » : ajoutez « **FQDN or Hostname** » = `vpn.sio-ndlp.fr` puis cliquez « **Save** » :

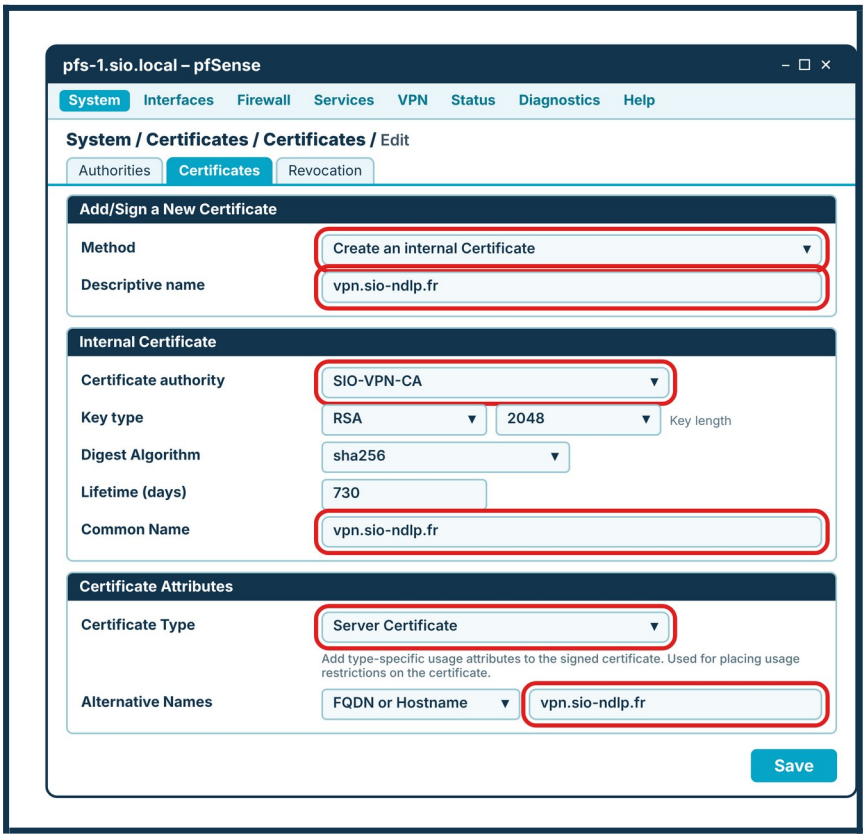


Figure 5 – System > Certificates > Certificates : certificat du serveur VPN

À SAVOIR

Le type « **Server Certificate** » ajoute l'usage « authentification de serveur » : le client OpenVPN refuse un certificat qui n'a pas cet usage, ce qui l'empêche d'accepter par erreur un certificat d'utilisateur comme serveur.

À SAVOIR

Le nom `vpn.sio-ndlp.fr` doit être **résolu par les clients** vers l'adresse virtuelle du WAN (203.0.113.10 dans l'exemple). Sur Internet, c'est un enregistrement DNS public ; en laboratoire, un fichier `hosts` du poste nomade ou l'adresse réelle de votre WAN suffit. Un certificat serveur se renouvelle avant son expiration (730 jours ici) : notez la date.

✔ **POINT DE CONTRÔLE**

- **SIO-CA** (importée) et **SIO-VPN-CA** (interne) figurent dans l'onglet « Authorities »
- Le certificat **vpn.sio-ndlp.fr** figure dans « Certificates » avec la mention « **Server Certificate** »
- La configuration de pfSense a été **sauvegardée** après la création de la CA

03 ÉTAPE 3 SUR 6 — Lier pfSense à l'annuaire en LDAPS et tester

pfSense interroge l'annuaire en **LDAPS** (LDAP chiffré par TLS, port **636**). Windows Server 2025 refuse en effet les mots de passe envoyés en LDAP clair : sans LDAPS, l'authentification échoue toujours, avec un message peu explicite. pfSense contrôle le certificat du contrôleur de domaine : il doit faire confiance à **SIO-CA** (étape 2) et contacter le contrôleur par son **nom complet** (`srv-dc1.sio.local`), celui du certificat, et non par son adresse IP.

A – Vérifier que pfSense joint le contrôleur de domaine

1. Cliquez « **System** » puis « **General Setup** » : les « **DNS Servers** » doivent être les contrôleurs de domaine (`192.168.20.250` et `192.168.20.251`) pour que pfSense résolve `srv-dc1.sio.local`
2. Cliquez « **Diagnostics** » puis « **Test Port** » : « **Hostname** » `srv-dc1.sio.local`, « **Port** » `636`, puis « **Test** » :

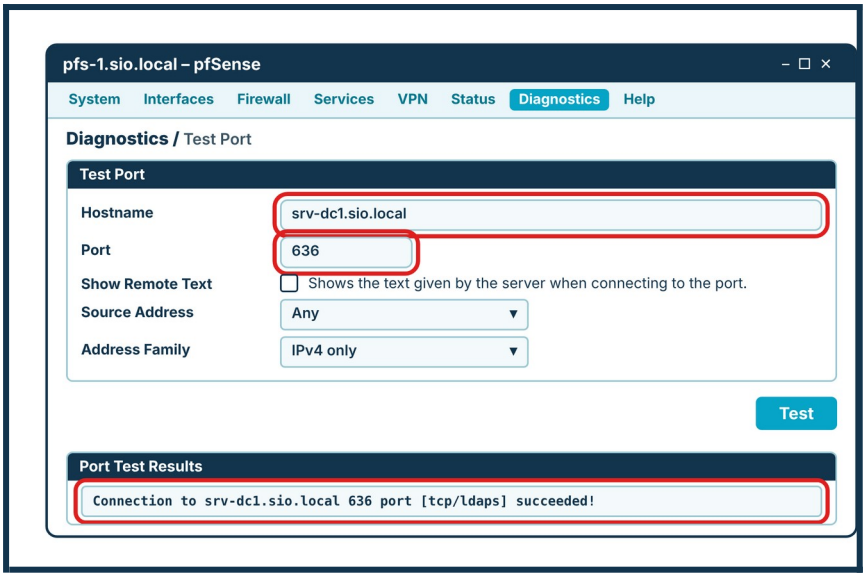


Figure 6 – Diagnostics > Test Port : le port LDAPS du contrôleur répond

À SAVOIR

Ce test prouve que le nom est résolu et que le port est joignable, pas que le certificat est valable : le certificat sera contrôlé par le test d'authentification (C).

B – Créer le serveur d'authentification

1. Cliquez « **System** » puis « **User Manager** », choisissez l'onglet « **Authentication Servers** » et cliquez « **+ Add** »
2. « **Descriptive name** » : `AD-SIO-DC1` ; « **Type** » : « **LDAP** » ; renseignez la partie « **LDAP Server Settings** » :

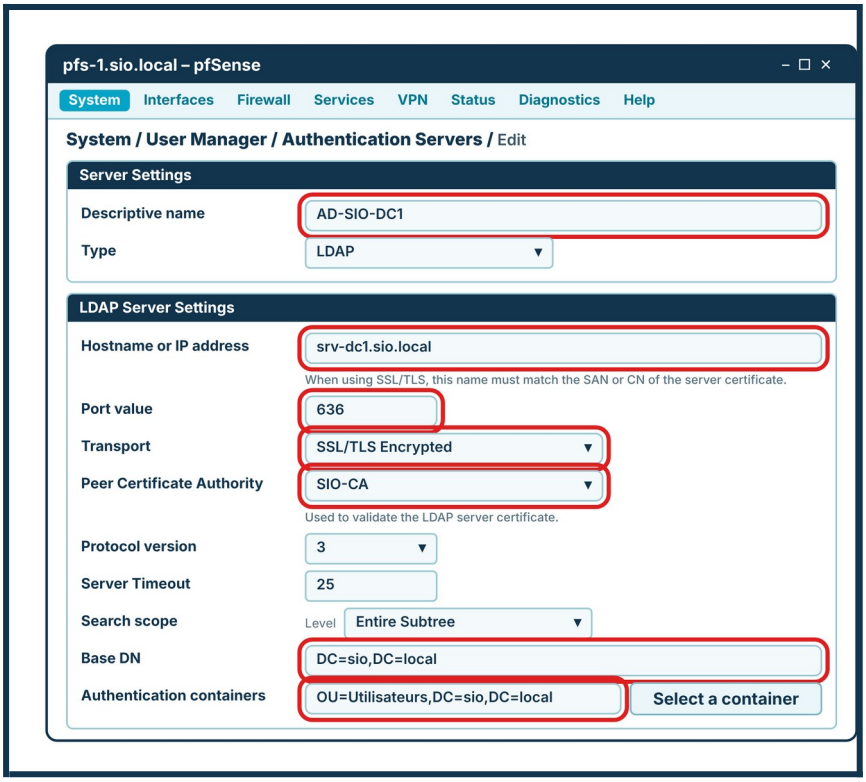


Figure 7 – Authentication Servers : connexion à SRV-DC1 en LDAPS

À SAVOIR

« Hostname » doit correspondre au nom du certificat du contrôleur. « Authentication containers » limite la recherche des utilisateurs à l'unité d'organisation **Utilisateurs** : un compte rangé ailleurs ne pourra pas se connecter.

3. « **Hostname or IP address** » : `srv-dc1.sio.local` ; « **Port value** » : `636` ; « **Transport** » : « **SSL/TLS Encrypted** » ; « **Peer Certificate Authority** » : « **SIO-CA** »
4. « **Protocol version** » : `3` ; « **Search scope** » : « **Entire Subtree** » ; « **Base DN** » : `DC=sio,DC=local` ; « **Authentication containers** » : `OU=Utilisateurs,DC=sio,DC=local`
5. Descendez et renseignez la liaison, les attributs et **la restriction au groupe** :

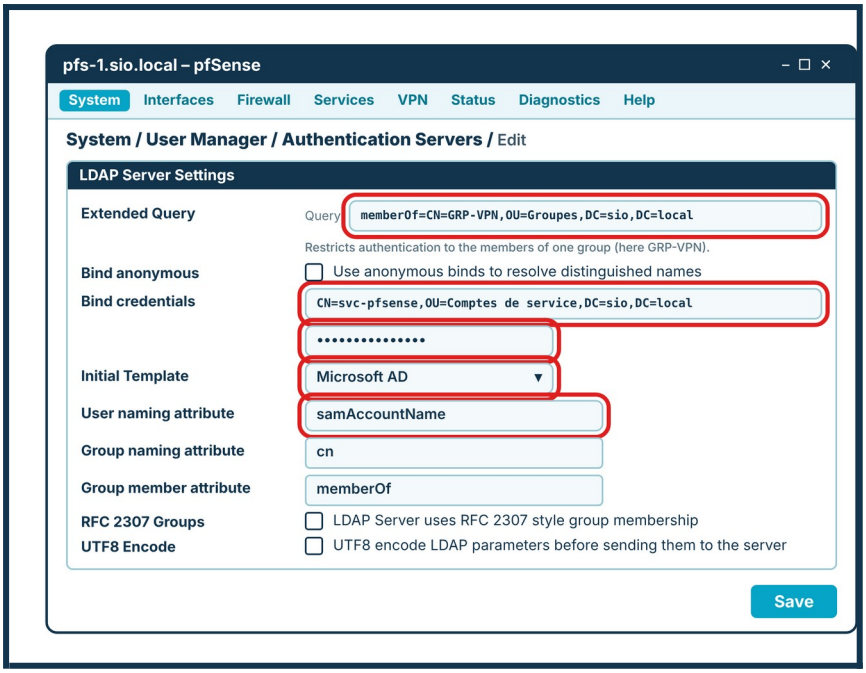


Figure 8 – Authentication Servers : compte de lecture, attributs et filtre de groupe

À SAVOIR

Le modèle « **Microsoft AD** » remplit les attributs : **samAccountName** (identifiant de connexion), **cn** et **memberOf**. Le filtre « Extended Query » est ajouté à chaque recherche : un utilisateur qui n'est pas dans GRP-VPN n'est tout simplement pas trouvé.

6. « **Extended Query** » : `memberOf=CN=GRP-VPN,OU=Groupes,DC=sio,DC=local`
7. Décochez « **Bind anonymous** » ; « **Bind credentials** » : `CN=svc-pfsense,OU=Comptes de service,DC=sio,DC=local` et le mot de passe du compte
8. « **Initial Template** » : « **Microsoft AD** » (cette liste ne sert qu'à pré-remplir les attributs) ; contrôlez « **User naming attribute** » = `samAccountName`, « **Group naming attribute** » = `cn`, « **Group member attribute** » = `memberOf`
9. Cliquez « **Save** » ; puis recréez le même serveur pour le second contrôleur : « **Descriptive name** » `AD-SIO-DC2` et « **Hostname** » `srv-dc2.sio.local`, tous les autres champs identiques

À SAVOIR

Les deux entrées permettent à OpenVPN d'**essayer le second contrôleur** si le premier ne répond pas (étape 4). Si les utilisateurs sont aussi membres de groupes **imbriqués**, remplacez le filtre par `memberOf:1.2.840.113556.1.4.1941:=CN=GRP-VPN,OU=Groupes,DC=sio,DC=local` : cette forme particulière demande à Active Directory de parcourir les groupes dans les groupes.

C – Tester l'authentification

Avant de toucher à OpenVPN, vérifiez que l'annuaire répond comme prévu. Cliquez « **Diagnostics** » puis « **Authentication** », choisissez « **AD-SIO-DC1** », saisissez l'identifiant `amartin` (**sans** `SIO\` ni `@sio.local`) et son mot de passe, puis cliquez « **Test** » :

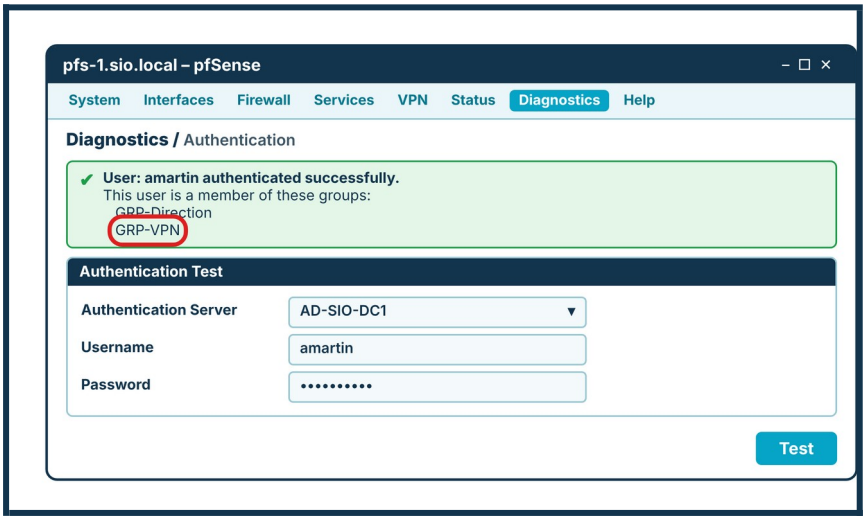


Figure 9 – Diagnostics > Authentication : amartin est authentifiée

À SAVOIR

pfSense affiche les groupes de l'utilisateur. Un succès prouve **trois choses à la fois** : le certificat LDAPS est accepté, le compte de liaison fonctionne et le mot de passe est correct.

Refaites le test avec `bdurand` et **son bon mot de passe** : elle existe dans l'annuaire mais n'appartient pas à GRP-VPN.

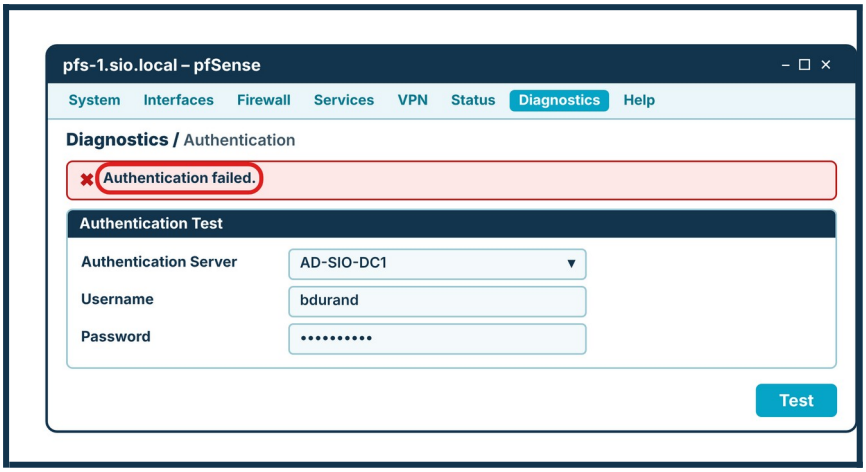


Figure 10 – Diagnostics > Authentication : bdurand est refusée

À SAVOIR

Le refus est **voulu** : le mot de passe est bon, mais le filtre de groupe écarte le compte. Si amartin est aussi refusée, voyez le dépannage en fin de tutoriel (certificat LDAPS, nom du contrôleur, compte de liaison).

✔ POINT DE CONTRÔLE

- Le test **Test Port 636** réussit vers SRV-DC1 et SRV-DC2
- **amartin** est authentifiée sur **AD-SIO-DC1** et sur **AD-SIO-DC2**
- **bdurand** (hors du groupe) obtient « **Authentication failed** » avec un mot de passe correct

04 ÉTAPE 4 SUR 6 Créer le serveur OpenVPN d'accès distant

Le menu « **VPN > OpenVPN > Wizards** » propose un assistant qui crée l'autorité, le certificat, le serveur et les règles en une suite d'écrans. Nous créons le serveur **à la main** : chaque paramètre est ainsi vu, expliqué et réutilisable. Cliquez « **VPN** » puis « **OpenVPN** », l'onglet « **Servers** » et « **+ Add** ». Le formulaire est long ; il se lit en trois parties.

A – Mode, authentification et point d'accès

1. « **Description** » : `VPN accès distant SIO` ; « **Server mode** » : « **Remote Access (SSL/TLS + User Auth)** »
2. « **Backend for authentication** » : sélectionnez **AD-SIO-DC1** puis, en maintenant Ctrl, **AD-SIO-DC2** (ne retenez pas « Local Database »)
3. « **Device mode** » : « **tun - Layer 3 Tunnel Mode** » ; « **Protocol** » : « **UDP on IPv4 only** » ; « **Local port** » : `1194`
4. « **Interface** » : l'**adresse virtuelle CARP du WAN** (`203.0.113.10`) et non « WAN » :

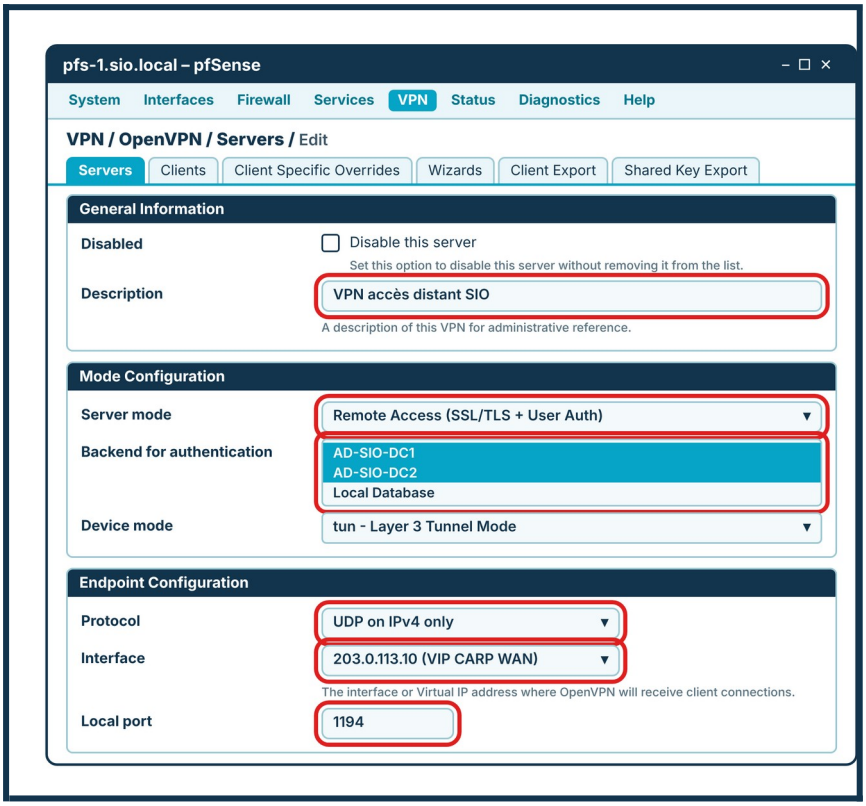


Figure 11 – VPN > OpenVPN > Servers : mode, authentification et interface

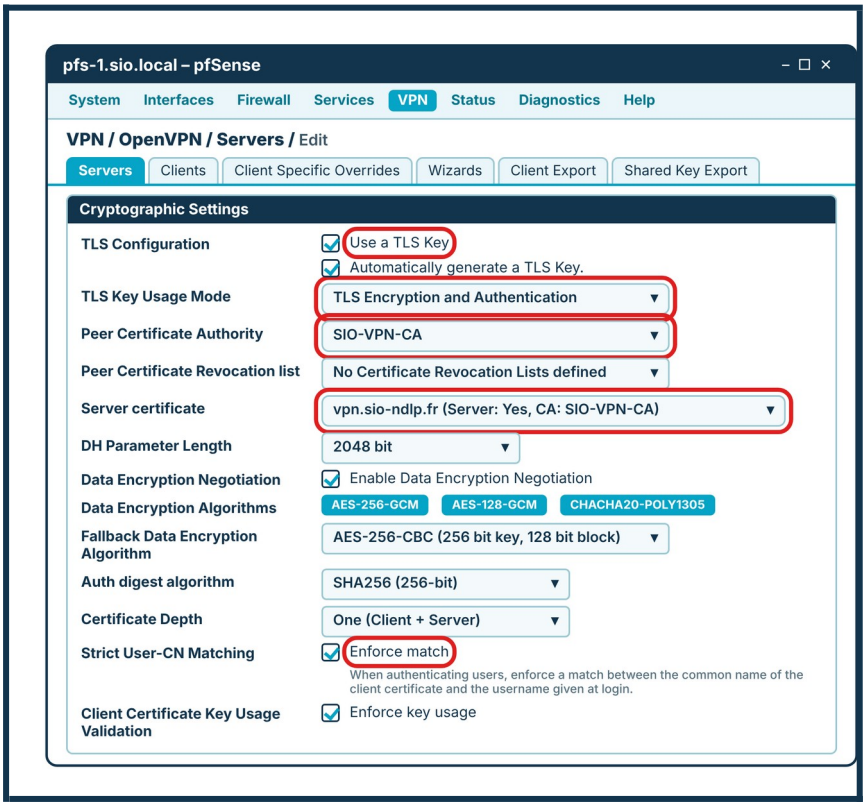
À SAVOIR

Lier le serveur à l'**adresse virtuelle CARP** garantit que le VPN répond à la même adresse, quel que soit le nœud maître. Choisir « WAN » le ferait écouter sur l'adresse propre du nœud, qui change à la bascule.

B – Paramètres cryptographiques

1. Cochez « **Use a TLS Key** » et « **Automatically generate a TLS Key** » ; « **TLS Key Usage Mode** » : « **TLS Encryption and Authentication** »
2. « **Peer Certificate Authority** » : « **SIO-VPN-CA** » ; « **Server certificate** » : « **vpn.sio-ndlp.fr** »
3. « **DH Parameter Length** » : `2048 bit` ; « **Data Encryption Algorithms** » : `AES-256-GCM`, `AES-128-GCM` et `CHACHA20-POLY1305` ; « **Auth digest algorithm** » : `SHA256`

4 Cochez « **Strict User-CN Matching** » (« **Enforce match** ») et « **Client Certificate Key Usage Validation** » :



À SAVOIR

La **clé TLS** cache le port aux scanners : un paquet sans la bonne clé est ignoré sans réponse. « **Strict User-CN Matching** » exige que le **nom du certificat soit identique à l'identifiant saisi** : amartin ne peut pas utiliser le certificat de bdurand.

Figure 12 – VPN > OpenVPN > Servers : paramètres cryptographiques

C – Réseau du tunnel et paramètres envoyés aux clients

1 « **IPv4 Tunnel Network** » : `10.99.0.0/24` ; **ne cochez pas** « **Redirect IPv4 Gateway** » (seul le trafic destiné au lycée entre dans le tunnel, le reste d'Internet sort directement)

2 « **IPv4 Local Network(s)** » : `192.168.20.0/24` (la route envoyée aux clients) ; « **Concurrent Connections** » : `10`

3 Laissez décochées « **Inter-client communication** » et « **Duplicate Connections** » : les clients ne se voient pas entre eux et un même compte ne peut pas se connecter deux fois

4 « **Topology** » : « **Subnet** » ; cochez « **DNS Default Domain** » (`sio.local`) et « **DNS Servers** » (`192.168.20.250` et `192.168.20.251`) ; cliquez « **Save** » :

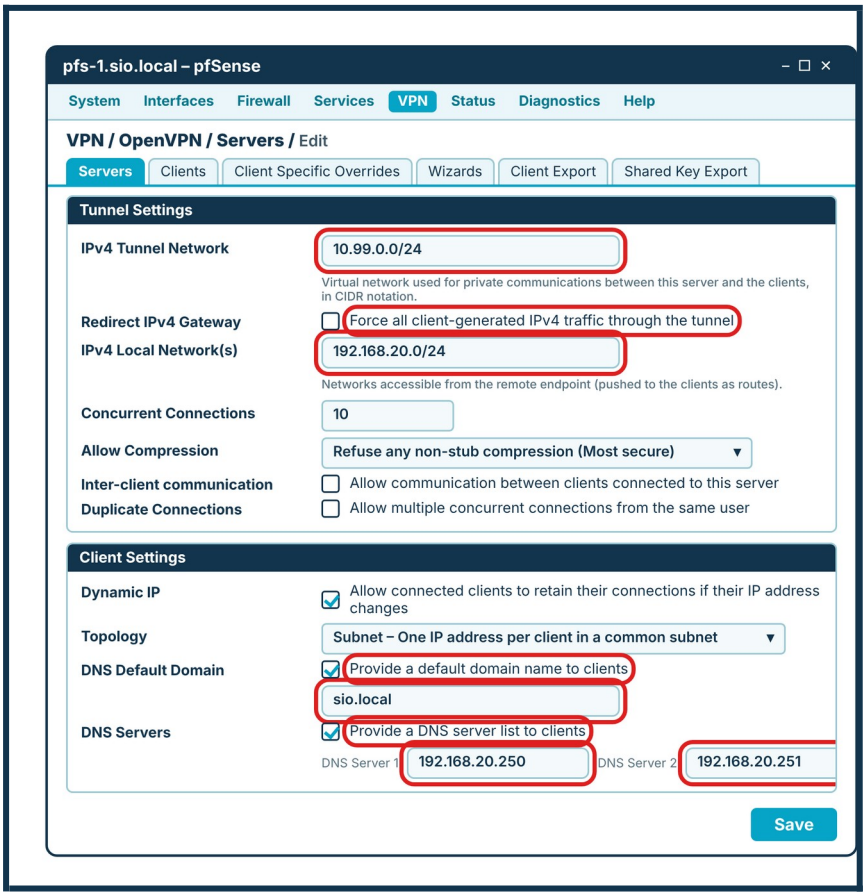


Figure 13 – VPN > OpenVPN > Servers : tunnel, routes et DNS

À SAVOIR

Seule la route **192.168.20.0/24** est envoyée : ce choix, appelé *split tunnel*, limite les flux du VPN. Le serveur DNS poussé permet d'utiliser les noms (`srv-dc1.sio.local`) plutôt que des adresses.

À SAVOIR

« **Redirect IPv4 Gateway** » envoie **tout** le trafic du poste nomade dans le tunnel, y compris la navigation web : le lycée filtre alors ce trafic, mais il doit aussi en supporter le débit. On l'active pour des postes gérés par l'établissement, rarement pour des personnels qui utilisent leur ordinateur personnel.

✔ **POINT DE CONTRÔLE**

- Le serveur « **VPN accès distant SIO** » apparaît dans l'onglet « **Servers** »
- Il écoute sur **UDP 1194**, adresse virtuelle **203.0.113.10**, réseau **10.99.0.0/24**
- Le **mode** est « SSL/TLS + User Auth » et les **deux** serveurs AD figurent comme « Backend »

05 ÉTAPE 5 SUR 6 — Délivrer les certificats et ouvrir le pare-feu

A – Créer un certificat par utilisateur

Chaque utilisateur reçoit un certificat dont le **nom est son identifiant du domaine** (« Strict User-CN Matching ») :

1 Cliquez « **System > Certificates** », l'onglet « **Certificates** » puis « **+ Add/Sign** »

2. « **Method** » : « **Create an internal Certificate** » ; « **Descriptive name** » : `amartin`
3. « **Certificate authority** » : « **SIO-VPN-CA** » ; « **Lifetime (days)** » : `365` ; « **Common Name** » : `amartin` (identique à l'identifiant AD, en minuscules)
4. « **Certificate Type** » : « **User Certificate** » puis cliquez « **Save** » :

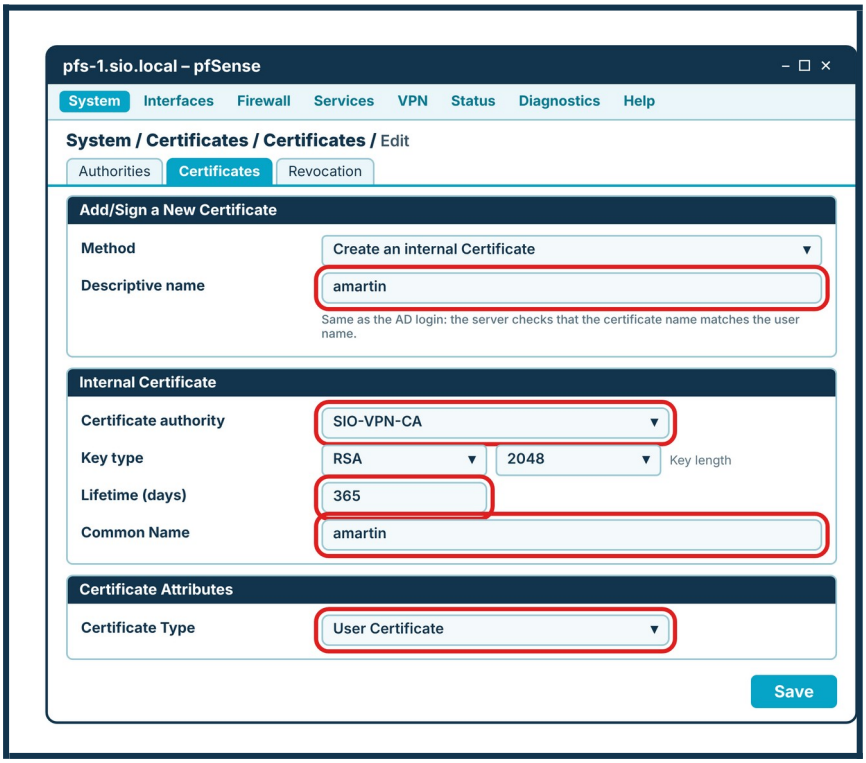


Figure 14 – System > Certificates > Certificates : certificat de l'utilisateur amartin

À SAVOIR

Un certificat d'utilisateur dure **un an** : une personne qui part n'emporte pas indéfiniment un accès, et le renouvellement annuel permet de faire le point sur les utilisateurs. Notez les dates d'expiration.

5. Répétez la création pour `bdurand` : son certificat est valable, mais elle sera refusée parce qu'elle n'appartient pas à GRP-VPN

La liste des certificats doit maintenant contenir celui du serveur et ceux des deux utilisateurs :

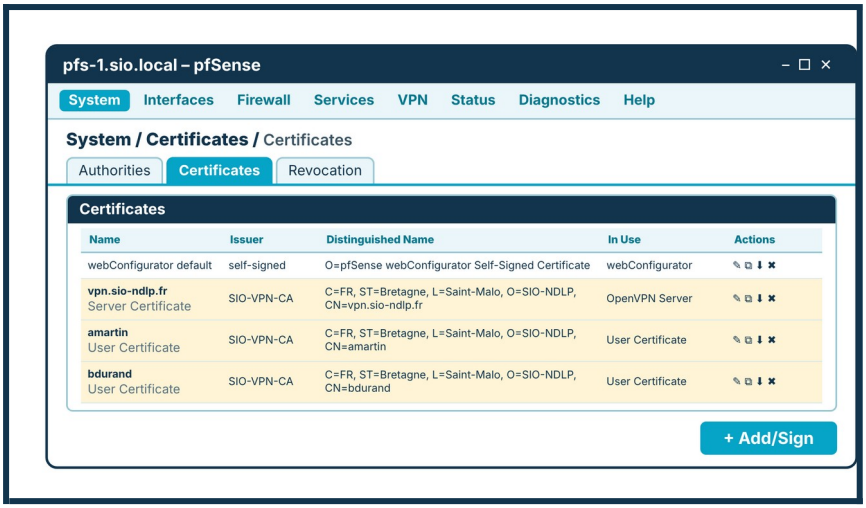


Figure 15 – System > Certificates > Certificates : serveur et utilisateurs

À SAVOIR

La colonne « In Use » indique que le certificat du serveur est utilisé par OpenVPN. Ne supprimez jamais un certificat **en cours d'utilisation** sans avoir d'abord modifié le service qui s'en sert.

B – Créer deux alias pour des règles lisibles

Les règles de pare-feu sont plus lisibles avec des **alias** (des noms pour des groupes d'adresses ou de ports). Cliquez « **Firewall > Aliases** » :

1. Onglet « **IP** » puis « **+ Add** » : « **Name** » `DC_SIO`, « **Type** » « **Host(s)** », deux entrées `192.168.20.250` et `192.168.20.251`, « **Description** » `Contrôleurs de domaine` ; cliquez « **Save** »
2. Onglet « **Ports** » puis « **+ Add** » : « **Name** » `PORTS_ADMIN`, « **Type** » « **Port(s)** », trois entrées `22`, `443` et `3389`, « **Description** » `SSH, HTTPS et RDP` ; cliquez « **Save** » puis « **Apply Changes** »

C – Autoriser le VPN sur le WAN, puis filtrer ce qui entre dans le tunnel

Il faut **deux séries de règles** : l'une laisse le client **atteindre** le serveur OpenVPN, l'autre décide de ce que le client **peut faire** une fois connecté. Commencez par le WAN : cliquez « **Firewall > Rules** », l'onglet « **WAN** » puis « **↑ Add** » :

1. « **Action** » : « **Pass** » ; « **Protocol** » : « **UDP** » ; « **Source** » : « **Any** »
2. « **Destination** » : « **Address or Alias** » et `203.0.113.10` ; « **Destination Port Range** » : « **OpenVPN (1194)** » (champs « From » et « To »)
3. « **Description** » : `OpenVPN : accès distant SIO` puis cliquez « **Save** » :

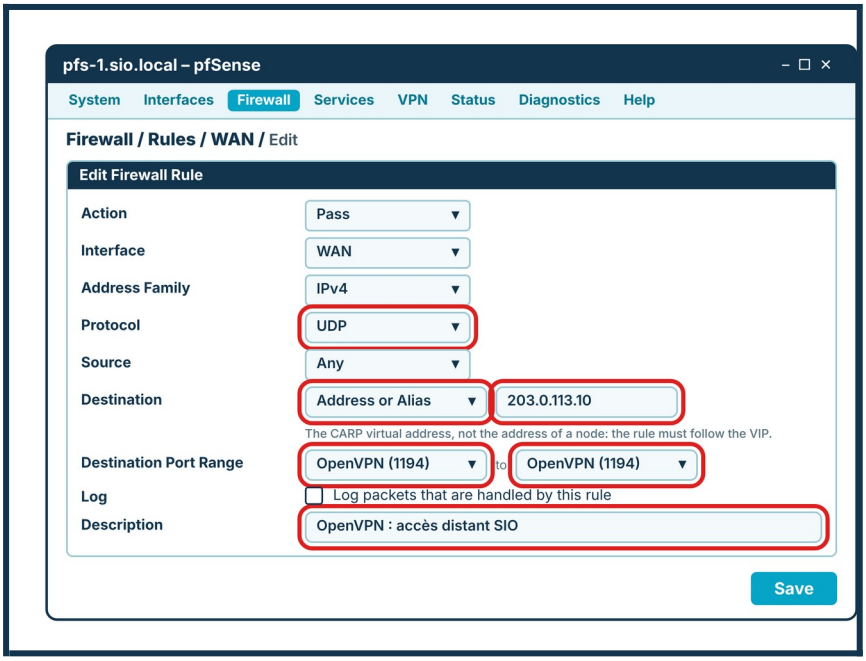


Figure 16 – Firewall > Rules > WAN : autoriser UDP 1194 vers le VPN

À SAVOIR

La destination est l'**adresse virtuelle CARP** et non « WAN address » : cette dernière désigne l'adresse propre du nœud, et la règle ne fonctionnerait plus après une bascule.

Passez ensuite à l'onglet « **OpenVPN** » (créé par pfSense dès qu'un serveur existe). Sans règle, **tout est refusé** dans le tunnel : créez les trois règles suivantes, de la plus précise à la plus large, avec « **Action** » « **Pass** » et « **Source** » « **Network** » `10.99.0.0/24` :

Protocole	Destination	Port	Description
ICMP (« any »)	Network 192.168.20.0/24	—	VPN : ping vers les serveurs
TCP/UDP	Address or Alias **DC_SIO**	DNS (53)	VPN : DNS vers les contrôleurs
TCP	Network 192.168.20.0/24	Alias **PORTS_ADMIN**	VPN : SSH, HTTPS, RDP vers les serveurs

Cliquez « **Save** » après chaque règle, puis « **Apply Changes** » :

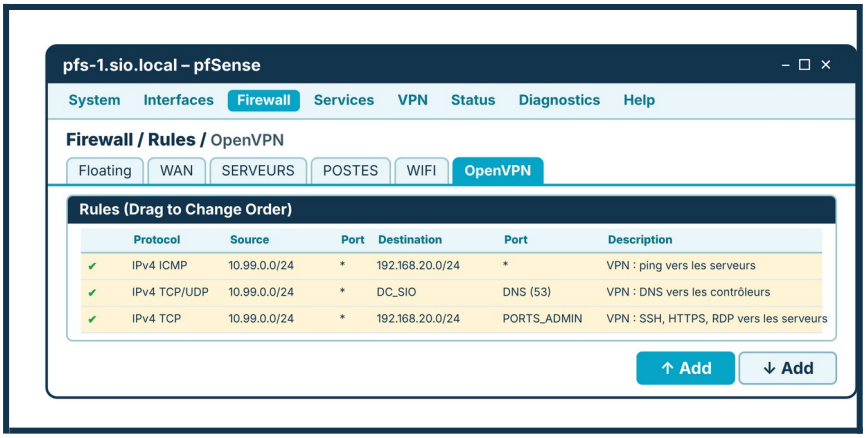


Figure 17 – Firewall > Rules > OpenVPN : ce que les clients VPN peuvent faire

À SAVOIR

Les règles suivent le **moindre privilège** : le client atteint les serveurs sur trois ports seulement, plus le DNS. Tout le reste, y compris le partage de fichiers (445), est refusé par la règle implicite de pfSense.

REMARQUE IMPORTANTE

Aucune règle de **NAT** n'est nécessaire ici : les serveurs du VLAN 20 ont pour passerelle l'adresse virtuelle de pfSense (192.168.20.254), donc leurs **réponses reviennent par le tunnel**. Si un serveur de ce VLAN utilise une autre passerelle, les réponses partent ailleurs et la connexion échoue : c'est la première chose à vérifier en cas de blocage.

D – Synchroniser la configuration sur le second nœud

Le cluster ne protège le VPN que si **PFS-2** possède la même configuration. Cliquez « **System** » puis « **High Availability Sync** » et vérifiez que les éléments suivants sont cochés (« **Select options to sync** ») avant de cliquer « **Save** » :

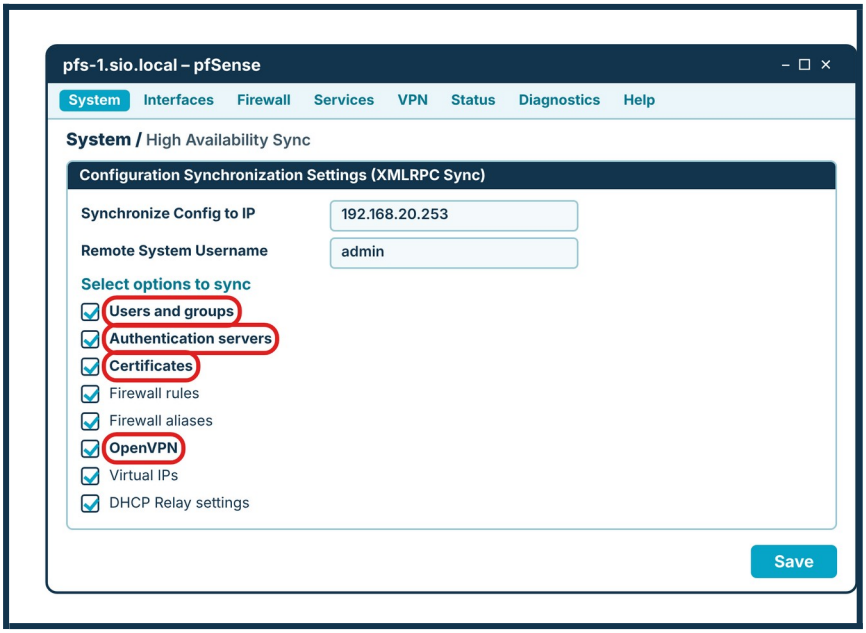


Figure 18 – System > High Availability Sync : éléments à synchroniser pour le VPN

À SAVOIR

Les **utilisateurs**, les **serveurs d'authentification**, les **certificats** (avec les clés privées) et **OpenVPN** doivent être copiés vers PFS-2. Les règles et les alias, déjà cochés pour le DHCP, couvrent le pare-feu.

Sur **PFS-2**, vérifiez que « **System > Certificates** » contient les certificats, que « **VPN > OpenVPN > Servers** » liste le serveur et que « **Firewall > Rules** » porte les mêmes règles : tout doit y apparaître sans intervention.

✔ POINT DE CONTRÔLE

- Les certificats de **amartin** et **bdurand** existent, signés par **SIO-VPN-CA**
- La règle **WAN UDP 1194** cible l'**adresse virtuelle** 203.0.113.10
- L'onglet **OpenVPN** contient les **trois règles** de filtrage
- **PFS-2** affiche les mêmes certificats, serveur et règles

06 ÉTAPE 6 SUR 6 Exporter, connecter un client et exploiter

A – Installer l'outil d'export des clients

Fabriquer à la main le fichier de configuration d'un client est long et source d'erreurs. Le paquet **openvpn-client-export** le génère : il assemble le certificat, la clé, l'autorité et les paramètres du serveur en un seul fichier `.ovpn`. Cliquez « **System > Package Manager** », l'onglet « **Available Packages** », saisissez `openvpn-client-export`, cliquez « **Search** » puis « **+ Install** » et « **Confirm** » :

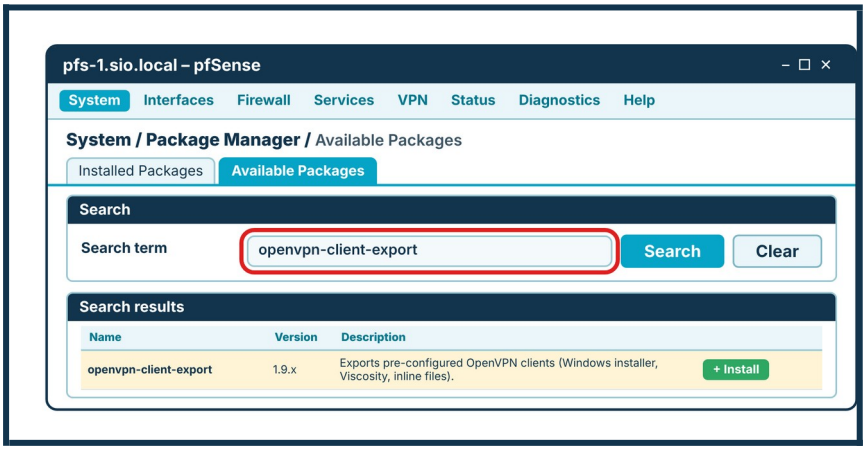


Figure 19 – System > Package Manager : installer openvpn-client-export

À SAVOIR

Installez le paquet **sur PFS-1 et sur PFS-2** si vous voulez pouvoir exporter les profils depuis l'un ou l'autre nœud : les profils obtenus sont identiques.

B – Exporter la configuration d'un utilisateur

1. Cliquez « **VPN > OpenVPN** » puis l'onglet « **Client Export** » ; « **Remote Access Server** » : « **VPN accès distant SIO UDP4:1194** »
2. « **Host Name Resolution** » : « **Other** » puis « **Host Name** » : `vpn.sio-ndlp.fr` (le nom du certificat, pas une adresse IP)
3. Laissez « **Verify Server CN** » sur « **Automatic** » et « **Use Random Local Port** » coché ; descendez sans autre changement

4 Dans la ligne de **amartin**, cliquez « **Inline Configurations** » > « **Most Clients** » : le fichier `.ovpn` se télécharge :

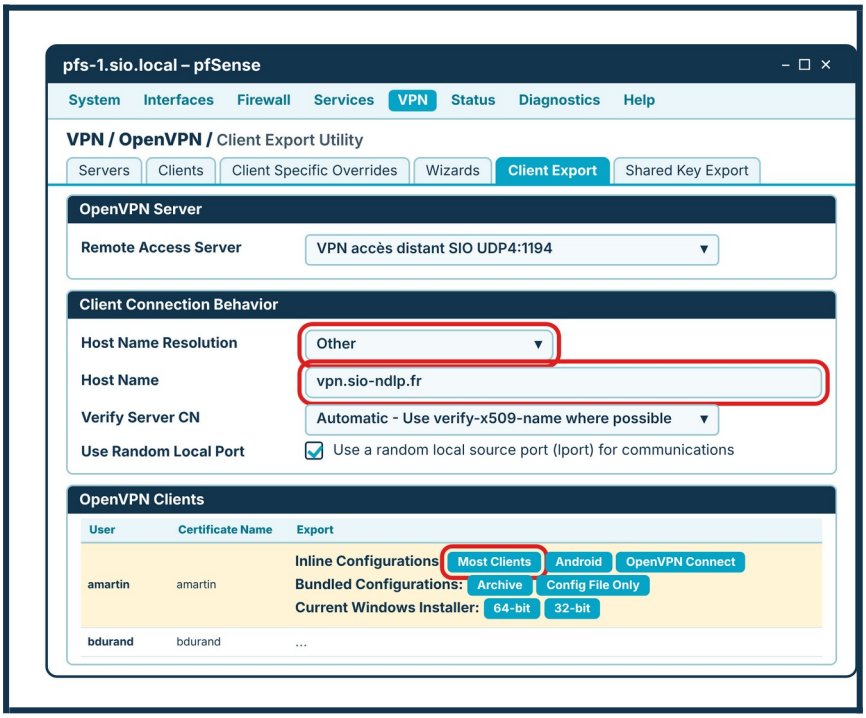


Figure 20 – VPN > OpenVPN > Client Export : exporter le profil d'amartin

À SAVOIR

Le fichier **contient le certificat et la clé privée** d'amartin : il se transmet de façon sûre (remise en main propre, coffre de mots de passe), jamais en pièce jointe d'un courriel ordinaire. Il ne contient pas son mot de passe : elle le saisit à chaque connexion.

À SAVOIR

Le **nom d'hôte** exporté dans le fichier est celui que le client contactera : si vous aviez laissé « Interface IP Address », il contiendrait l'adresse du nœud et non l'adresse virtuelle. C'est une cause fréquente de profils qui cessent de fonctionner après un changement d'adresse. Pour un poste sur lequel OpenVPN n'est pas installé, la ligne « **Current Windows Installer** » (**64-bit**) fournit un installeur déjà configuré avec le profil.

C – Installer le client sur le poste nomade et se connecter

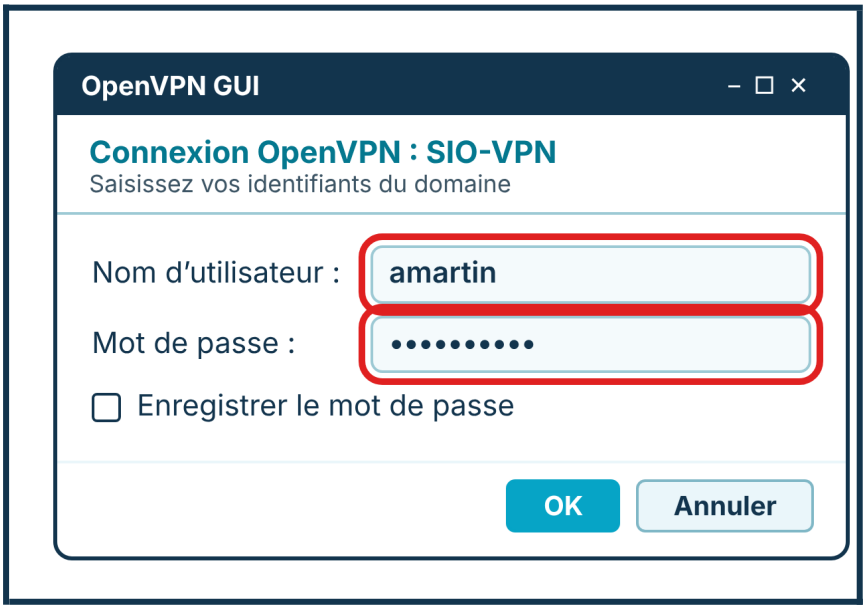
Sur le **poste Windows 11 situé hors du réseau du lycée**, installez **OpenVPN GUI**, le client libre pour Windows, téléchargé sur le site officiel d'OpenVPN (programme d'installation « Windows 64-bit MSI »). Copiez ensuite le fichier exporté dans le dossier des profils de l'utilisateur :

POWERSHELL (POSTE NOMADE)

```
Copy-Item "$env:USERPROFILE\Downloads\*.ovpn" `
    "$env:USERPROFILE\OpenVPN\config\"
```

1 Dans la zone de notification, faites un clic droit sur l'icône **OpenVPN GUI** puis cliquez « **Connecter** » (« **Connect** »)

2 Saisissez `amartin` et son mot de passe du domaine (**sans** `SIO\` ni `@sio.local`) puis cliquez « **OK** » :

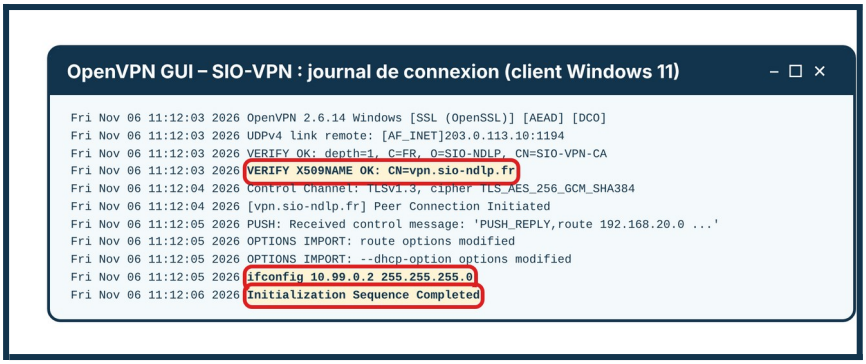


À SAVOIR

Les libellés de cette fenêtre suivent la langue de Windows. Ne cochez pas « Enregistrer le mot de passe » sur un poste partagé : le mot de passe resterait utilisable par quiconque ouvre la session.

Figure 21 – OpenVPN GUI : saisie de l'identifiant et du mot de passe du domaine

Une fenêtre de journal s'ouvre pendant la négociation, puis l'icône devient verte. Le journal doit se terminer par **Initialization Sequence Completed** :



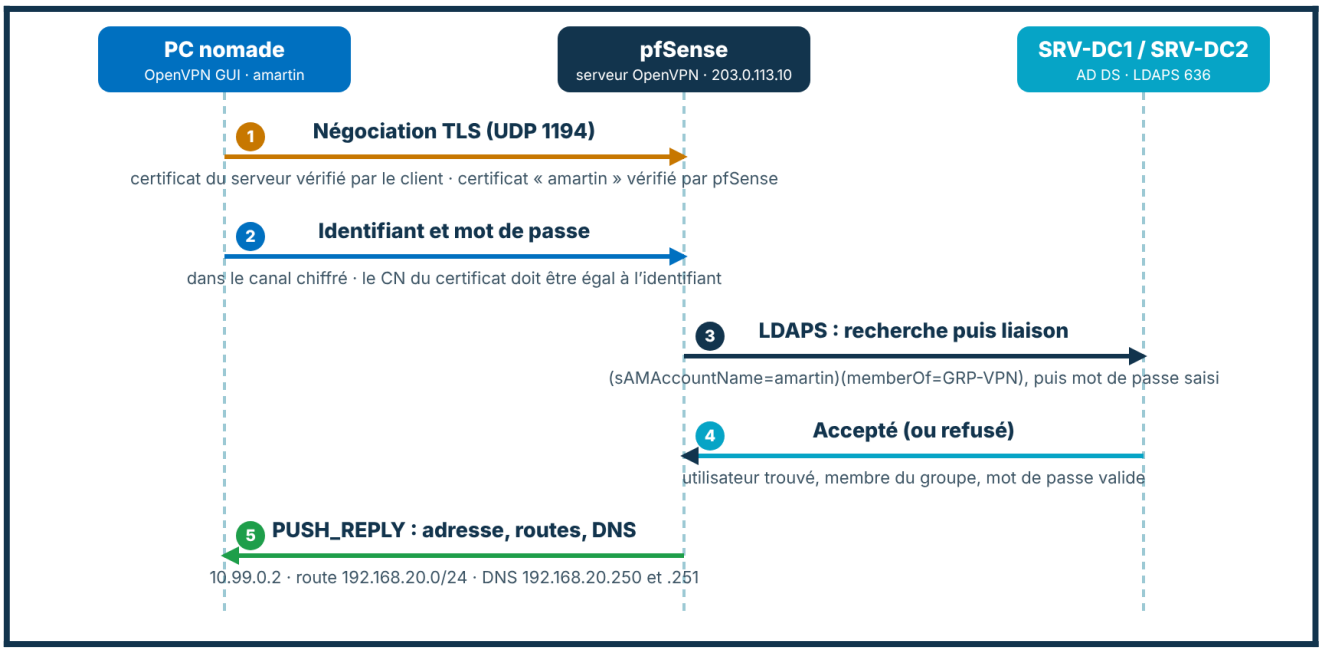
À SAVOIR

Les lignes « VERIFY » prouvent que le client a **vérifié le serveur** (autorité et nom). « ifconfig 10.99.0.2 » est l'adresse reçue dans le tunnel. « Initialization Sequence Completed » signale que le tunnel est monté.

Figure 22 – OpenVPN GUI : journal d'une connexion réussie

D – Comprendre ce qui vient de se passer

Un échange complet se déroule en quelques secondes. Le schéma suivant en donne l'ordre, utile pour interpréter les journaux en cas de panne :



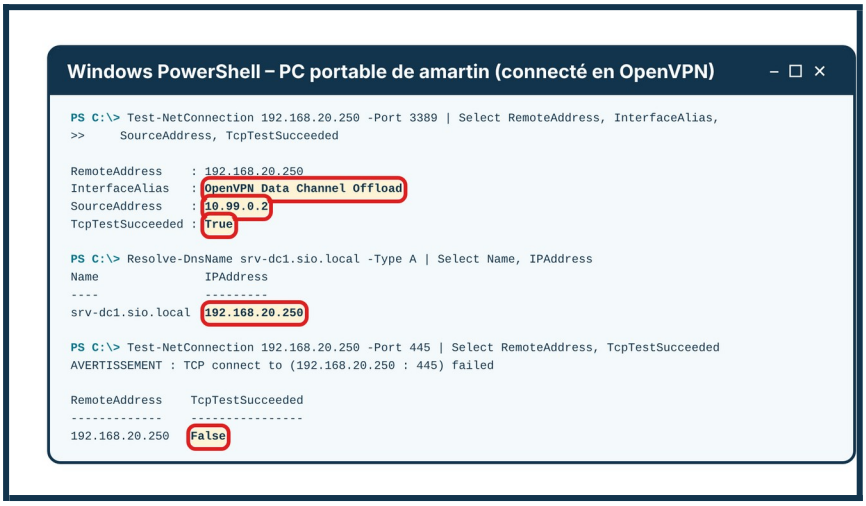
1. **1.** Négociation TLS : le client vérifie le certificat du serveur, pfSense vérifie celui d'amartin (signé par SIO-VPN-CA)
2. **2.** Le client envoie l'identifiant et le mot de passe dans le canal déjà chiffré ; « Strict User-CN Matching » compare l'identifiant au nom du certificat
3. **3 et 4.** pfSense interroge le contrôleur de domaine en LDAPS : recherche du compte **dans GRP-VPN**, puis contrôle du mot de passe ; la réponse est « accepté » ou « refusé »
4. **5.** En cas d'acceptation, pfSense envoie au client son adresse, la route vers 192.168.20.0/24 et les serveurs DNS ; le tunnel est monté

E – Vérifier l'accès aux serveurs

Depuis PowerShell, sur le poste nomade connecté, contrôlez que le trafic **passe par le tunnel** pour les ports autorisés et qu'il est **bloqué** pour les autres :

POWERSHELL (POSTE NOMADE)

```
Test-NetConnection 192.168.20.250 -Port 3389
Resolve-DnsName srv-dc1.sio.local -Type A
Test-NetConnection 192.168.20.250 -Port 445
```

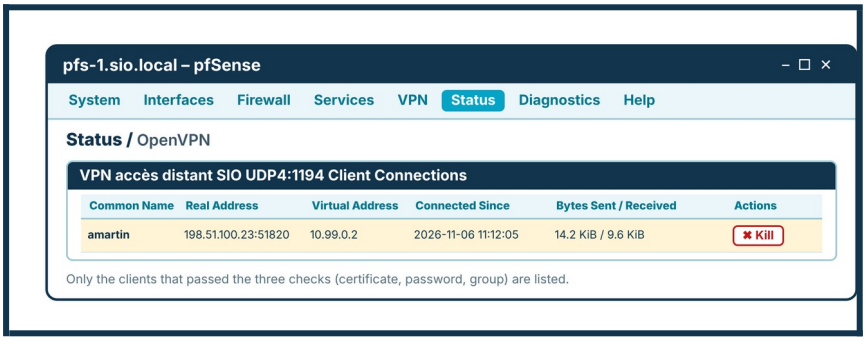


À SAVOIR

« SourceAddress » = 10.99.0.2 prouve que le trafic part du tunnel. Le port 3389 (RDP) passe, le port 445 (partage de fichiers) est refusé : les règles de l'onglet OpenVPN s'appliquent bien.

Figure 23 – PowerShell : accès autorisé (3389), nom résolu et accès refusé (445)

Côté pfSense, cliquez « **Status** » puis « **OpenVPN** » : le client connecté est listé avec son adresse réelle, son adresse dans le tunnel et le volume échangé :



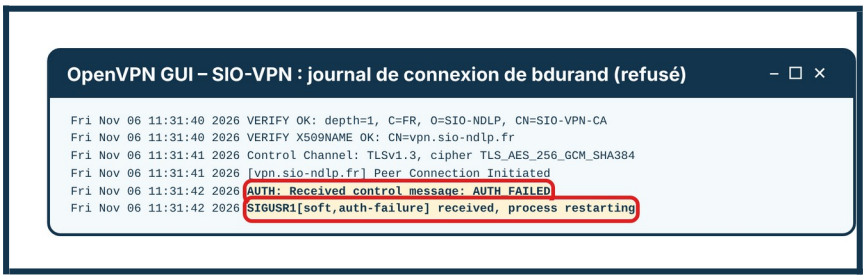
À SAVOIR

« Common Name » = amartin : c'est le nom du certificat. Le bouton « **Kill** » coupe la session sur-le-champ : utile si un poste est perdu ou si un compte est compromis.

Figure 24 – Status > OpenVPN : le client amartin est connecté

F – Vérifier le refus d'un utilisateur hors du groupe

Exportez le profil de **bdurand** (étape B) et tentez de vous connecter avec **son identifiant et son bon mot de passe**. Le certificat est valide et le mot de passe correct, mais bdurand n'est pas dans GRP-VPN :



À SAVOIR

Le client voit seulement « AUTH_FAILED » : il ne sait pas **quel** contrôle a échoué, ce qui est voulu. Pour le savoir, consultez le journal de pfSense (« Status > System Logs > OpenVPN »).

Figure 25 – OpenVPN GUI : la connexion de bdurand est refusée

Pour terminer, ajoutez `bdurand` à GRP-VPN (`Add-ADGroupMember "GRP-VPN" -Members bdurand`) : sa connexion fonctionne aussitôt, **sans rien modifier dans pfSense**. Retirez-la pour retrouver l'état précédent.

G – Exploiter : les opérations courantes

Je veux…	Je fais…
Autoriser un nouvel utilisateur	L'ajouter à **GRP-VPN** (AD) ; créer son certificat (**CN = identifiant**) dans pfSense ; exporter son profil et le lui remettre de façon sûre
Retirer l'accès d'un utilisateur	Le retirer de **GRP-VPN** : refusé à la prochaine connexion. Pour couper une session en cours : « **Status > OpenVPN** » puis « **Kill** »
Bloquer un poste perdu ou volé	Révoquer son certificat : « **System > Certificates > Revocation** », créer une liste de révocation pour SIO-VPN-CA et y ajouter le certificat, puis la choisir dans « **Peer Certificate Revocation list** » du serveur
Renouveler un certificat qui expire	Créer un nouveau certificat (même nom commun), exporter un nouveau profil, le remettre ; supprimer l'ancien après remplacement
Changer le mot de passe d'un utilisateur	Rien à faire dans pfSense : le mot de passe est celui du **domaine**
Surveiller les connexions	« **Status > OpenVPN** » pour les sessions actives, « **Status > System Logs > OpenVPN** » pour l'historique

À SAVOIR

Le VPN est **en haute disponibilité** : à la bascule de pfSense, les sessions en cours sont interrompues et les clients se **reconnectent automatiquement** en une minute environ. Vous pouvez le vérifier avec « **Status > CARP (failover)** » puis « **Enter Persistent CARP Maintenance Mode** » sur PFS-1 pendant qu'un client est connecté.

✔ **POINT DE CONTRÔLE**

- Le client **amartin** se connecte et reçoit l'adresse **10.99.0.2**
- Le **port 3389** de SRV-DC1 répond par le tunnel, le **port 445** est refusé
- **bdurand** est refusée tant qu'elle n'est pas dans **GRP-VPN**
- La session est visible dans **Status > OpenVPN**

Notre accès distant est maintenant **authentifié par l'annuaire** : un certificat propre au VPN, le mot de passe du domaine et l'appartenance à un groupe sont réunis pour entrer, les droits dans le tunnel sont réduits au strict nécessaire et la panne d'un pare-feu n'interrompt le service que quelques secondes.

Dépannage : les symptômes les plus fréquents

Symptôme	Cause probable	Solution
« Authentication failed » pour amartin dans Diagnostics > Authentication	Certificat LDAPS non reconnu, mauvais nom de contrôleur, compte de liaison ou filtre de groupe erroné	Vérifier « Peer Certificate Authority » (SIO-CA) et que « Hostname » est le nom du certificat ; contrôler le DN du compte et celui du groupe ; tester avec ldapsearch en ldaps depuis un serveur Linux
Le test d'authentification réussit mais pas la connexion VPN	Le serveur OpenVPN n'utilise pas les serveurs AD comme « Backend »	Serveur OpenVPN > « Backend for authentication » : sélectionner AD-SIO-DC1 et AD-SIO-DC2
Client : « TLS key negotiation failed to occur within 60 seconds »	Les paquets UDP 1194 n'atteignent pas le serveur	Vérifier la règle WAN (adresse virtuelle et port 1194), le DNS de vpn.sio-ndlp.fr et, derrière une box, la redirection du port ; Diagnostics > Packet Capture sur le WAN (port 1194)
Client : « certificate verify failed » ou nom du serveur refusé	Profil exporté avant un changement de certificat, ou nom d'hôte différent du nom du certificat	Réexporter le profil avec le bon « Host Name » (vpn.sio-ndlp.fr)
Client : AUTH_FAILED alors que le mot de passe est correct	Utilisateur hors de GRP-VPN, identifiant tapé avec le domaine, ou certificat d'un autre nom	Saisir l'identifiant seul (amartin) ; vérifier le groupe ; consulter Status > System Logs > OpenVPN : « Strict User-CN » signale une différence de nom, majuscules comprises
Connecté, mais aucun serveur ne répond	Règle OpenVPN manquante, route non poussée, ou passerelle du serveur différente de pfSense	Contrôler les règles de l'onglet OpenVPN ; « IPv4 Local Network(s) » ; `route print` sur le client ; la passerelle du serveur (192.168.20.254)
Les adresses IP répondent mais pas les noms	DNS non envoyés ou suffixe absent	Cocher « DNS Servers » dans le serveur ; sur le client, `ipconfig /all` doit montrer 192.168.20.250 ; utiliser le nom complet (srv-dc1.sio.local)
Le VPN ne répond plus après une bascule CARP	Serveur lié à l'adresse du nœud, ou configuration non synchronisée	Serveur > Interface = adresse virtuelle ; System > High Availability Sync : cocher OpenVPN et Certificates ; contrôler Status > OpenVPN sur le nouveau maître
« certificate has expired » sur le client	Certificat d'utilisateur (1 an) ou de serveur (2 ans) échu	Créer un nouveau certificat et réexporter le profil ; noter les échéances

Pense-bête : où regarder

Où / commande	Utilité
Diagnostics > Authentication (pfSense)	Teste un identifiant et un mot de passe avec un serveur d'authentification, sans passer par OpenVPN
Diagnostics > Test Port (pfSense)	Vérifie qu'un port TCP (ici 636) d'un serveur répond
Status > OpenVPN (pfSense)	Sessions actives : nom, adresses, volume, bouton « Kill »
Status > System Logs > OpenVPN (pfSense)	Journal du serveur : négociation TLS, refus de certificat, échec d'authentification
Firewall > Rules et Status > System Logs > Firewall	Règles WAN et OpenVPN ; paquets bloqués
Diagnostics > Packet Capture (pfSense)	Capture sur le WAN (UDP 1194) ou sur le VLAN SERVEURS
System > Certificates (pfSense)	Autorités, certificats, dates d'expiration, révocation
Get-ADGroupMember "GRP-VPN"	Liste les utilisateurs autorisés à utiliser le VPN
Journal d'OpenVPN GUI (client)	Détail de la connexion côté poste : lignes VERIFY, AUTH, PUSH_REPLY
Test-NetConnection <serveur> -Port <port>	Teste un flux à travers le tunnel (client)