PRINCE TOGBLE

REALISATION

SÉCURISATION DE L'ACCÈS À INTERNET ET MISE EN PLACE D'UNE DMZ

GUIDE COMPLET pFSENSE – STADIUMCOMPANY

1. Introduction

pfSense est le pare-feu principal de StadiumCompany.
Il assure :

- La segmentation réseau (VLAN 10/20/30/40)
- La DMZ (VLAN 40)
- Le routage inter-VLAN
- La sécurité (firewall, NAT, IDS/IPS, VPN)
- L'authentification LDAP/LDAPS
- Le portail captif pour le WiFi
- La gestion du trafic et des accès

Ce guide décrit **toutes les étapes**, de l'installation à la sécurité avancée, en utilisant **5 interfaces**.

2. Architecture réseau StadiumCompany

2.1 VLAN officiels

VLAN	Nom	Réseau	Rôle
10	Administration	172.20.1.0/24	AD, DNS, DHCP, GLPI, Nagios
20	Équipes	172.20.2.0/24	Postes utilisateurs
30	WiFi	172.20.3.0/24	WiFi employés
40	DMZ	172.20.4.0/24	Web, Zimbra, HAProxy

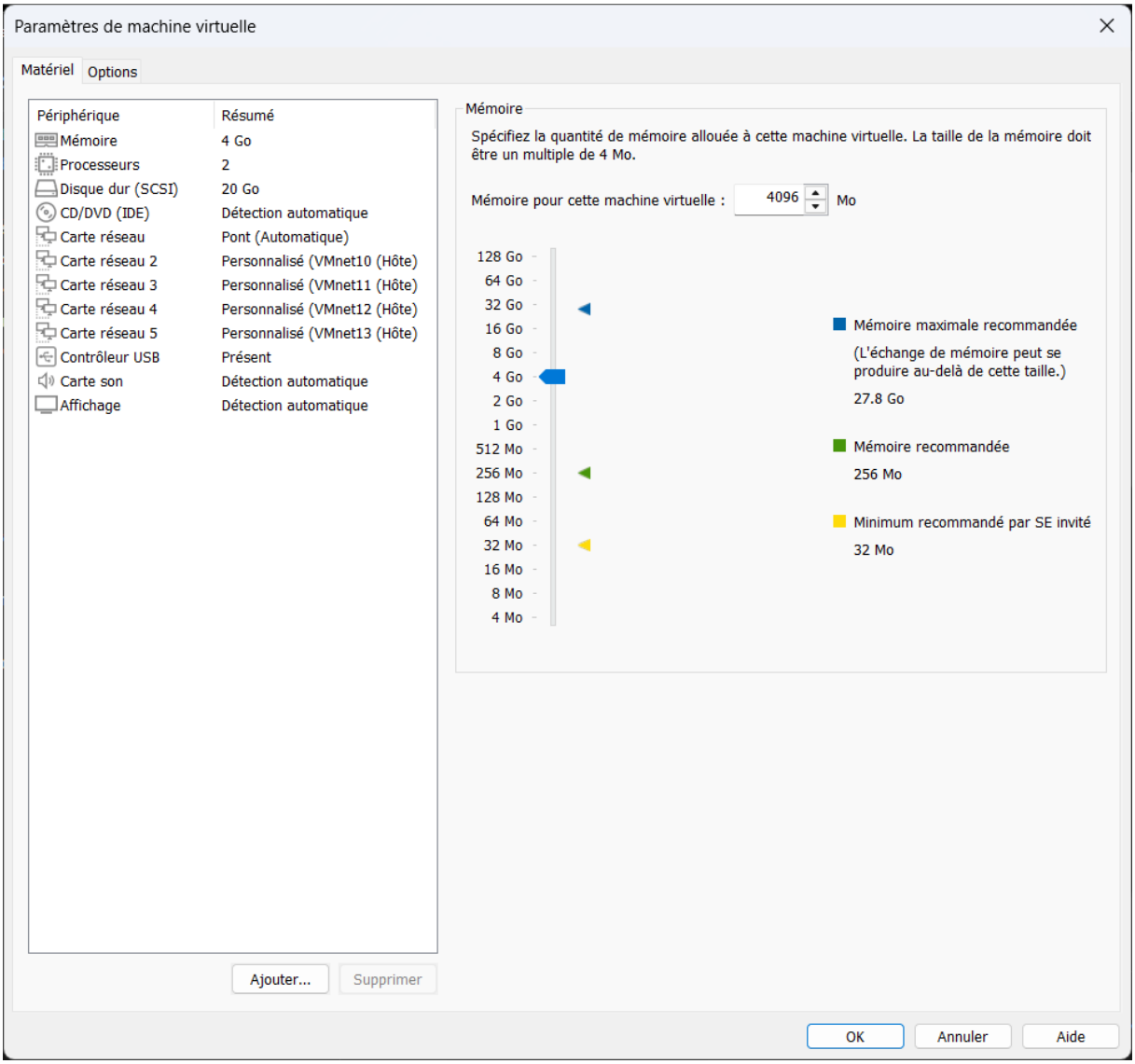
2.2 pfSense (Heimdall)

Interface	Rôle	IP pfSense
WAN	Accès Internet (bridge)	dépend de ta box
OPT1	VLAN 10 – Administration	**172.20.1.254**
OPT2	VLAN 20 – Équipes	**172.20.2.254**
OPT3	VLAN 30 – WiFi	**172.20.3.254**
OPT4	VLAN 40 – DMZ	**172.20.4.254**

3. Installation de pfSense

3.1 Création de la VM

- Type : **Personnalisée (avancée)**
- Compatibilité : **Workstation 16.x**
- OS : **FreeBSD 64 bits**
- Nom : **Heimdall-pfSense**
- Emplacement : `C:\VM\StadiumCompany\pfSense\`
- CPU : **2**
- RAM : **2 Go**
- Disque : **20 Go**, scindé
- Contrôleur : **LSI Logic**
- Type de disque : **SCSI**

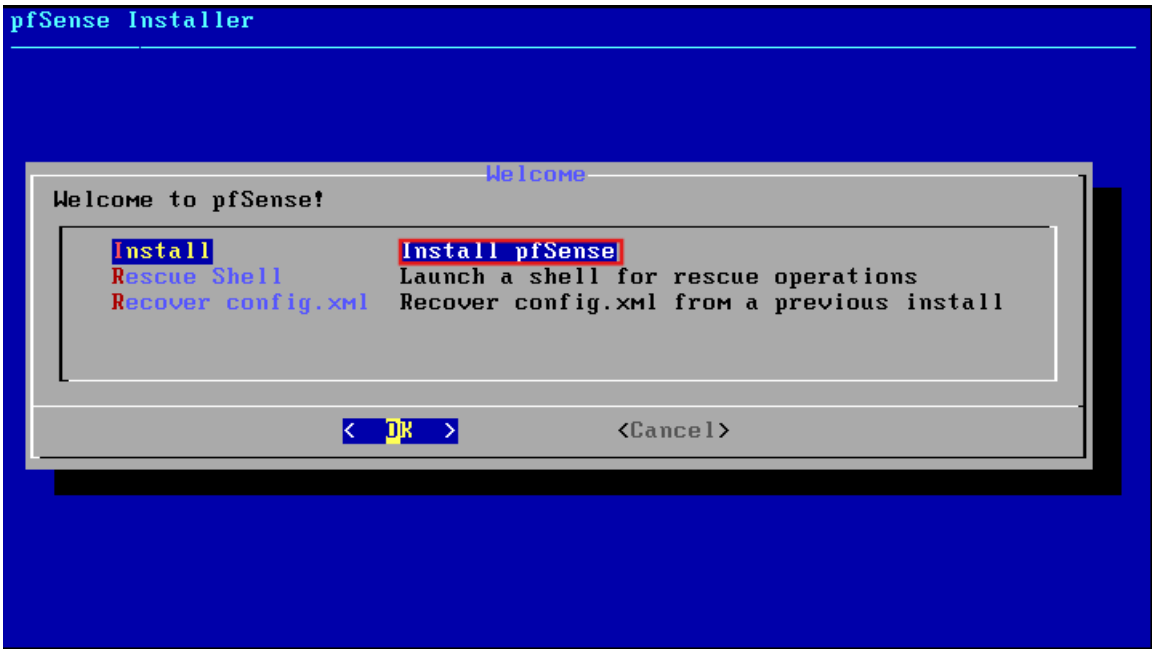


3.2 Configuration réseau (5 interfaces)

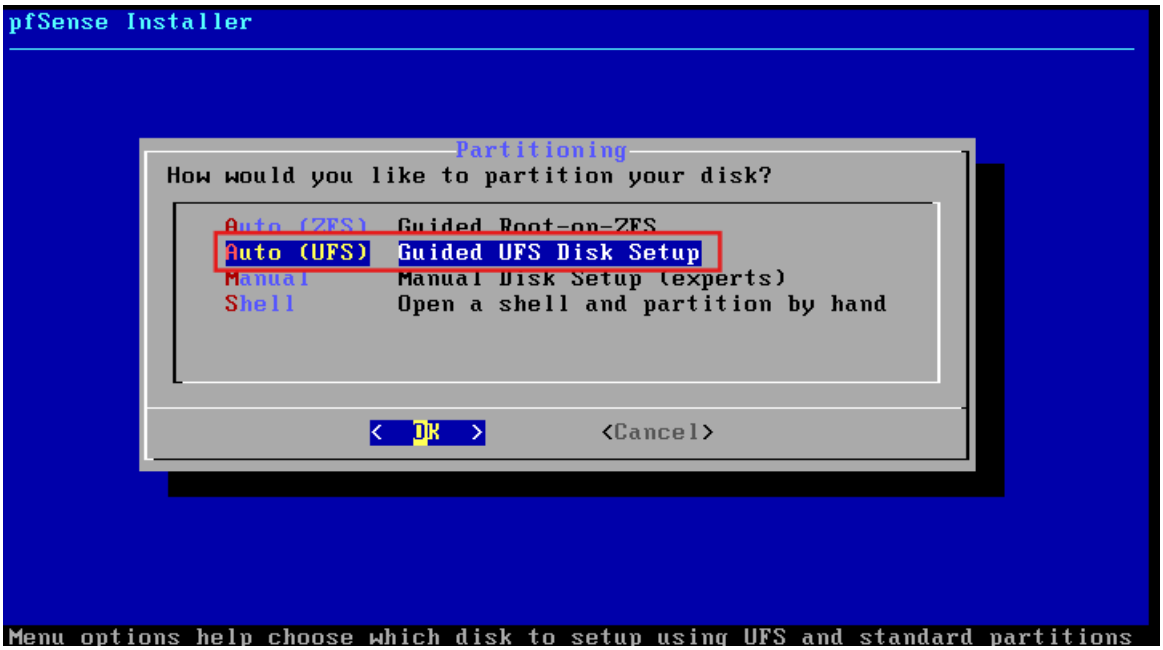
Interface VM	Rôle	VMware Network
NIC1	WAN	Bridge
NIC2	VLAN 10	VMnet10
NIC3	VLAN 20	VMnet11
NIC4	VLAN 30	VMnet12
NIC5	VLAN 40	VMnet13

4. Installation pfSense (ISO)

1. Monter l'ISO
2. Boot → Entrée
3. Install

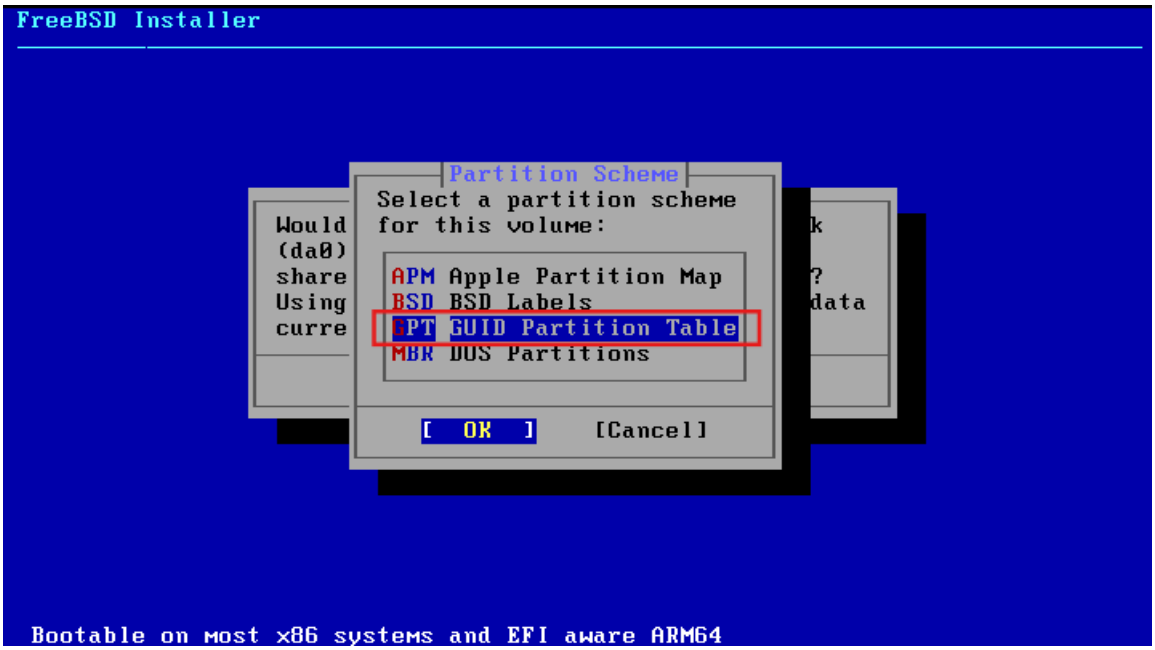


4. Clavier : **French**
5. Partitionnement : **Auto (UFS)**

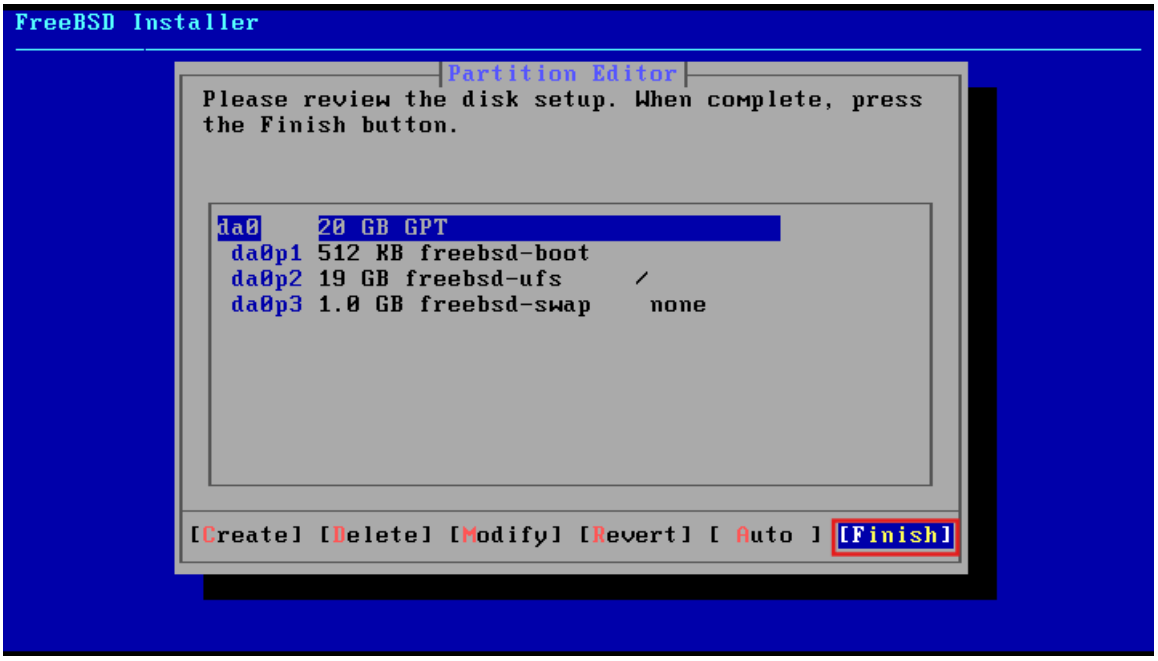


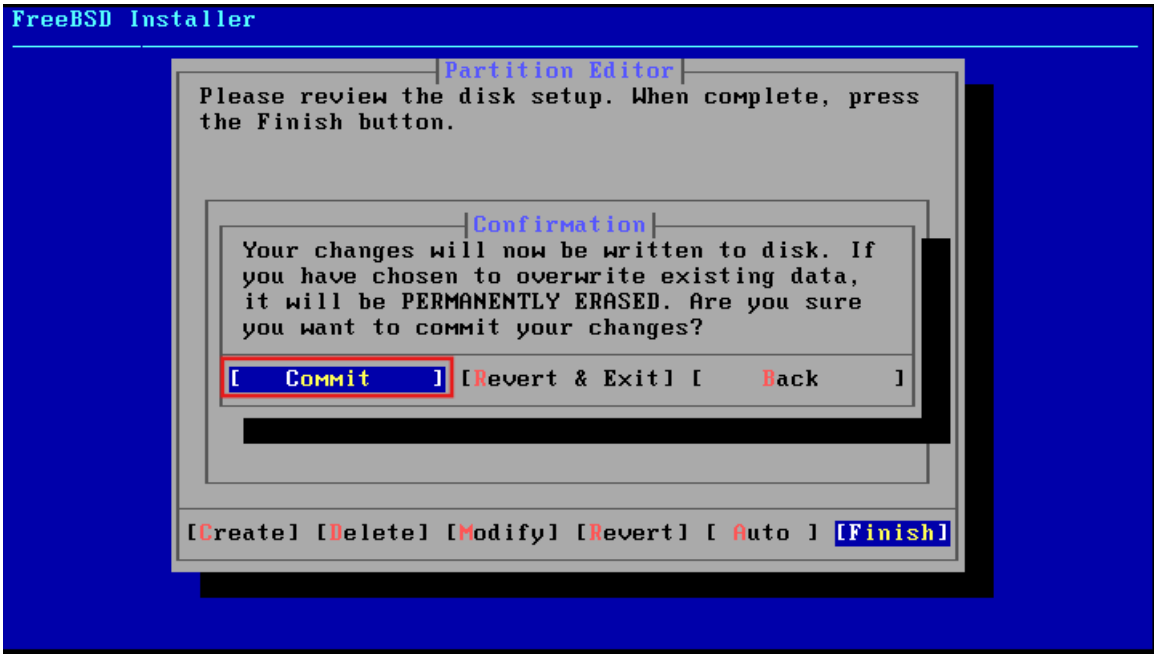
6. Disque entier

7. GPT



8. Finish -- Commit





9. Reboot
10. Retirer l'ISO

IMPORTANT : retirer l'ISO après reboot

Paramètres VM → CD/DVD (SATA)
→ **Utiliser le lecteur physique**

5. Configuration initiale des interfaces (5 interfaces)

5.1 Assignation des interfaces

Menu pfSense → Option **1**

```
Should VLANs be set up now? n

WAN  → em0
OPT1 → em1    (VLAN 10)
OPT2 → em2    (VLAN 20)
OPT3 → em3    (VLAN 30)
OPT4 → em4    (VLAN 40)
```

```
Enter the WAN interface name or 'a' for auto-detection
(em0 em1 em2 em3 em4 or a): em0

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(em1 em2 em3 em4 a or nothing if finished): em1

Enter the Optional 1 interface name or 'a' for auto-detection
(em2 em3 em4 a or nothing if finished): em2

Enter the Optional 2 interface name or 'a' for auto-detection
(em3 em4 a or nothing if finished): em3

Enter the Optional 3 interface name or 'a' for auto-detection
(em4 a or nothing if finished): em4

The interfaces will be assigned as follows:

WAN  -> em0
LAN  -> em1
OPT1 -> em2
OPT2 -> em3
OPT3 -> em4

Do you want to proceed [y|n]?
```

5.2 Configuration des IP

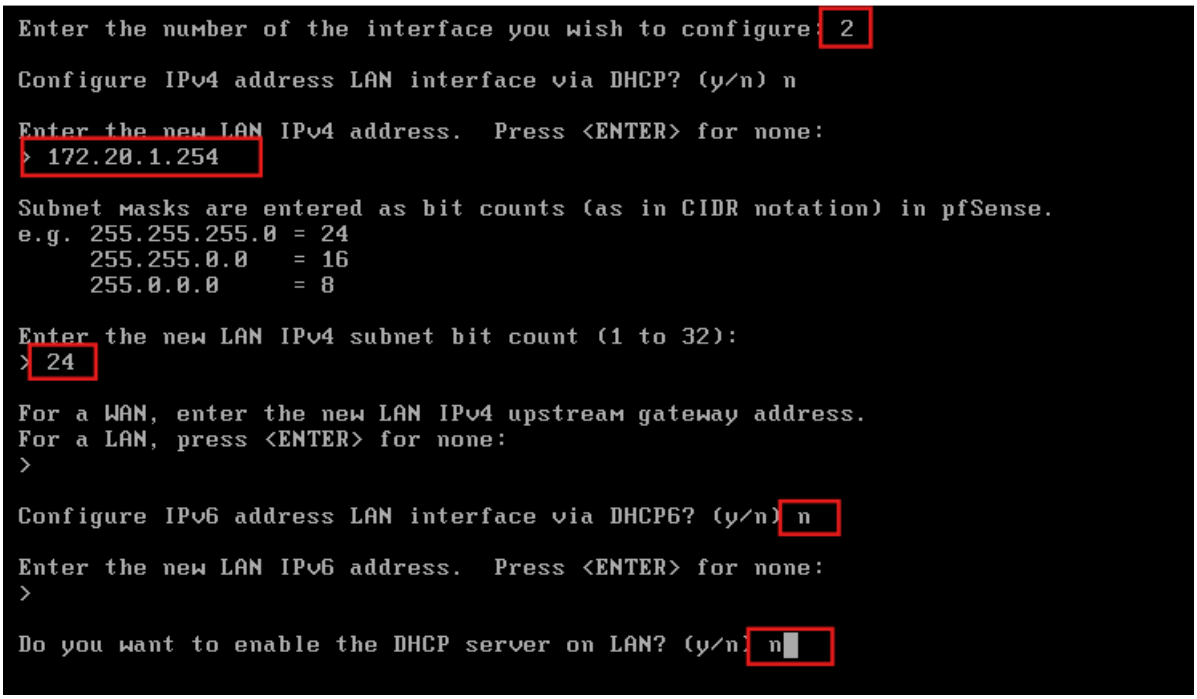
Menu → Option **2**

✓ WAN (bridge)

```
Enter the number of the interface you wish to configure: 1

Configure IPv4 address WAN interface via DHCP? (y/n) y

Configure IPv6 address WAN interface via DHCP6? (y/n) n

Enter the new WAN IPv6 address.  Press <ENTER> for none:
>
Disabling IPv4 DHCPD...
Disabling IPv6 DHCPD...

Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n

Please wait while the changes are saved to WAN...
 Reloading filter...
 Reloading routing configuration...
 DHCPD...

The IPv4 WAN address has been set to dhcp

Press <ENTER> to continue.
```

✓ OPT1 – VLAN 10 (Administration)

```
IP : 172.20.1.254
Mask : 24
Gateway : none
DHCP : non
```



→ **Même procédure pour les autres interfaces**

✓ OPT2 – VLAN 20 (Équipes)

```
IP : 172.20.2.254
Mask : 24
Gateway : none
DHCP : non
```

✓ OPT3 – VLAN 30 (WiFi)

```
IP : 172.20.3.254
Mask : 24
Gateway : none
DHCP : non
```

✓ OPT4 – VLAN 40 (DMZ)

```
IP : 172.20.4.254
Mask : 24
Gateway : none
DHCP : non
```

→ **Résultats Attendu**

```
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on heimdall ***

 WAN (wan)       -> em0        -> v4/DHCP4: 192.168.1.158/24
 LAN (lan)       -> em1        -> v4: 172.20.1.254/24
 OPT1 (opt1)     -> em2        -> v4: 172.20.2.254/24
 OPT2 (opt2)     -> em3        -> v4: 172.20.3.254/24
 OPT3 (opt3)     -> em4        -> v4: 172.20.4.254/24

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

6. Configuration de base (Wizard)

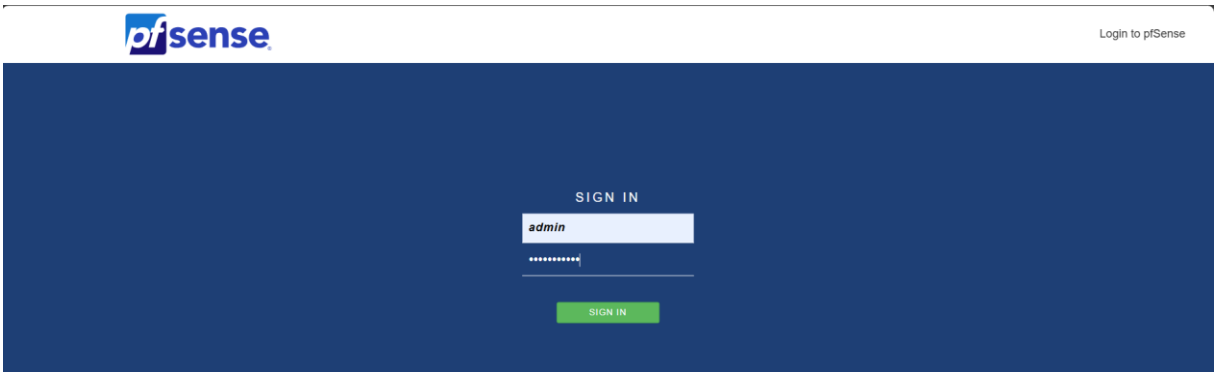
6.1 Accès Web

Depuis un poste du VLAN 10 :

https://172.20.1.254

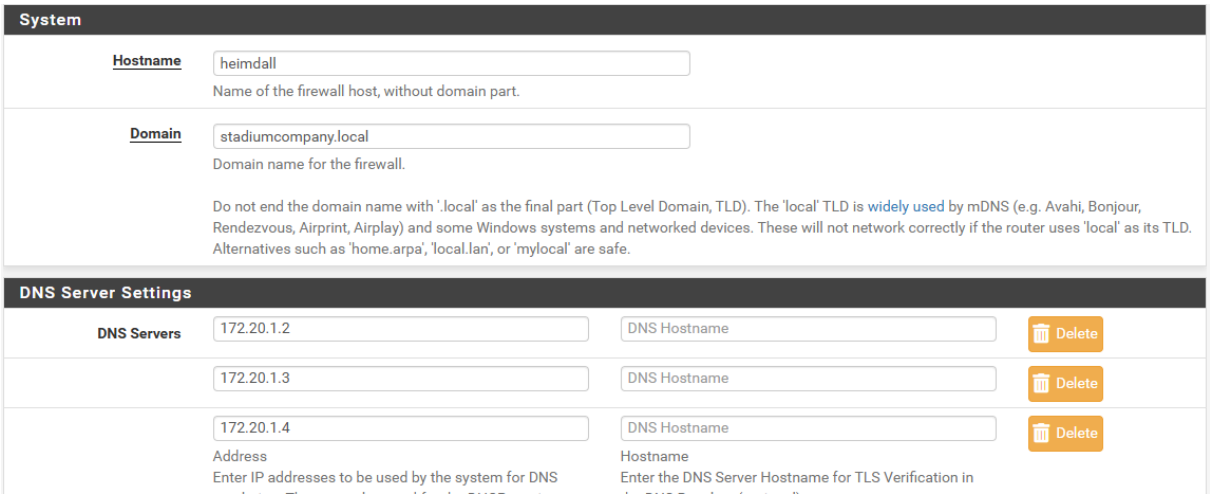
Identifiants :

- admin
- pfsense



6.2 Wizard (9 étapes)

- Hostname : **heimdall**
- Domaine : **stadiumcompany.local**
- DNS :
- `172.20.1.2`
- `172.20.1.3`
- `172.20.1.4`



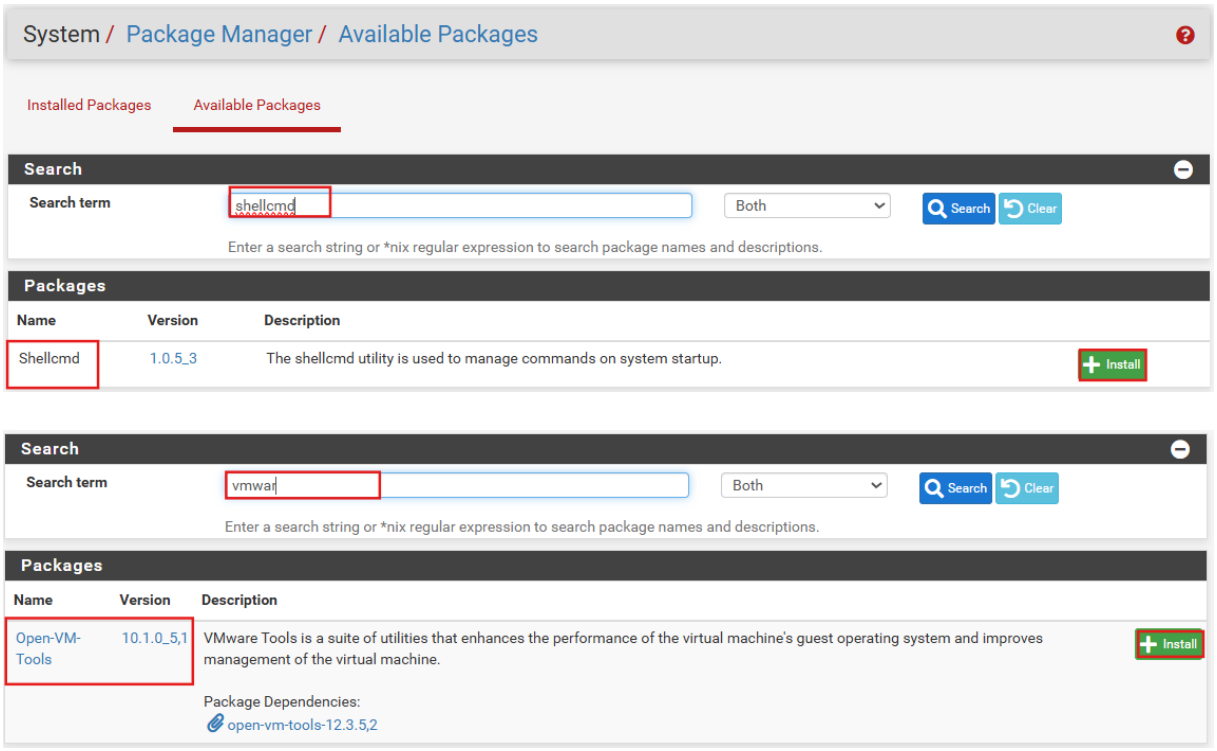
- NTP : fr.pool.ntp.org
- Timezone : Europe/Paris
- WAN : déjà configuré
- OPT1/2/3/4 : déjà configurés
- Changer mot de passe admin
- Reload → Finish

6.3 Clavier AZERTY permanent

Installer :

- **shellcmd**
- **VMware Tools**

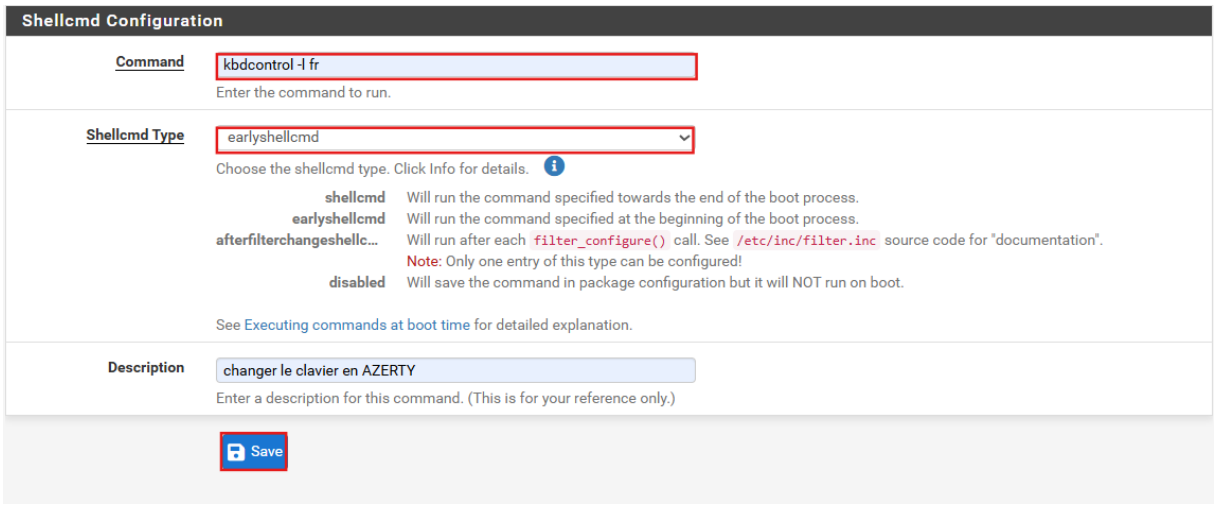
System → Package Manager → Available Packages



Puis :

Services → Shellcmd → Add

```
Command : kbdcontrol -l fr
Type : earlyshellcmd
```



Save.

7. Tests de connectivité

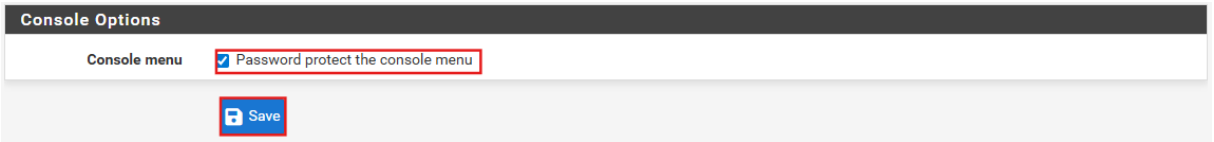
Depuis Hermes :

```
ping 172.20.1.254
ping 172.20.2.254
ping 172.20.3.254
ping 172.20.4.254
ping 192.168.1.1
ping 8.8.8.8
ping www.google.fr
```

8. Sécurisation pfSense

8.1 Sécuriser la console

System → Advanced → Admin Access
→ Activer **Console Password**



8.2 Sécuriser l'accès SSH sur pfSense (procédure détaillée)

L'objectif est de :

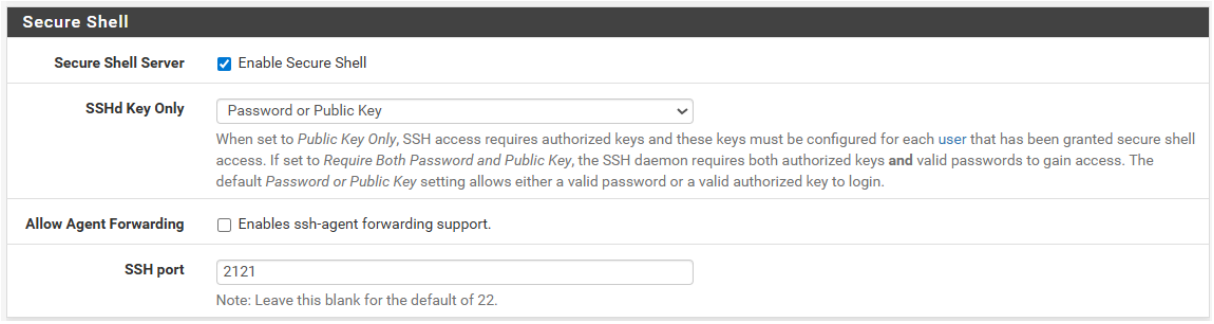
- **Activer SSH** pour administrer pfSense à distance
- **Changer le port par défaut** (22 → 2121) pour réduire les attaques automatisées
- **Créer une règle firewall WAN** pour autoriser ce port
- **Tester la connexion SSH** depuis un poste interne

Étape 1 — Activer SSH dans pfSense

1. Connecte-toi à l'interface Web pfSense
2. Va dans :
   System → Advanced → Admin Access
3. Descends jusqu'à la section **Secure Shell**
4. Coche :
   ✓ **Enable Secure Shell**

5. Dans **SSH Port**, remplace :
6. `22 → 2121`
7. Clique sur **Save**

☞ À ce stade, SSH est activé, mais **le firewall bloque encore le port 2121**.
Il faut donc créer une règle.

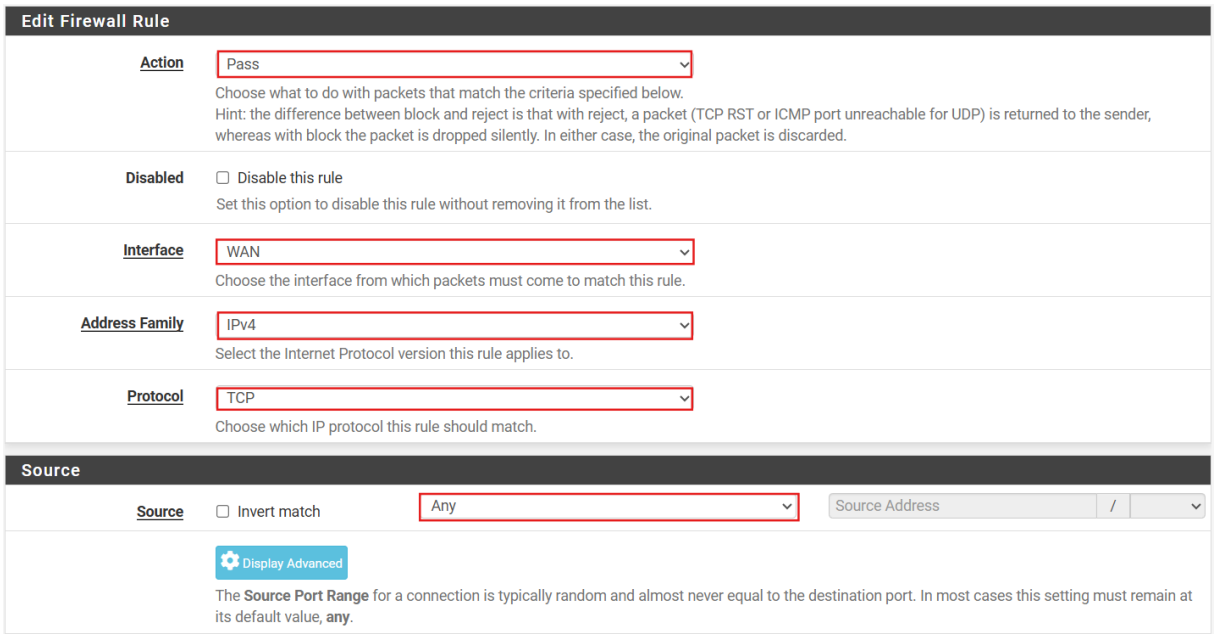


Étape 2 — Créer la règle firewall sur l'interface WAN

1. Va dans :
   Firewall → Rules → WAN
2. Clique sur **Add** (flèche vers le haut pour ajouter en haut)
3. Configure la règle :

✓ Paramètres de la règle

- **Action** : Pass
- **Interface** : WAN
- **Address Family** : IPv4
- **Protocol** : TCP
- **Source** : any

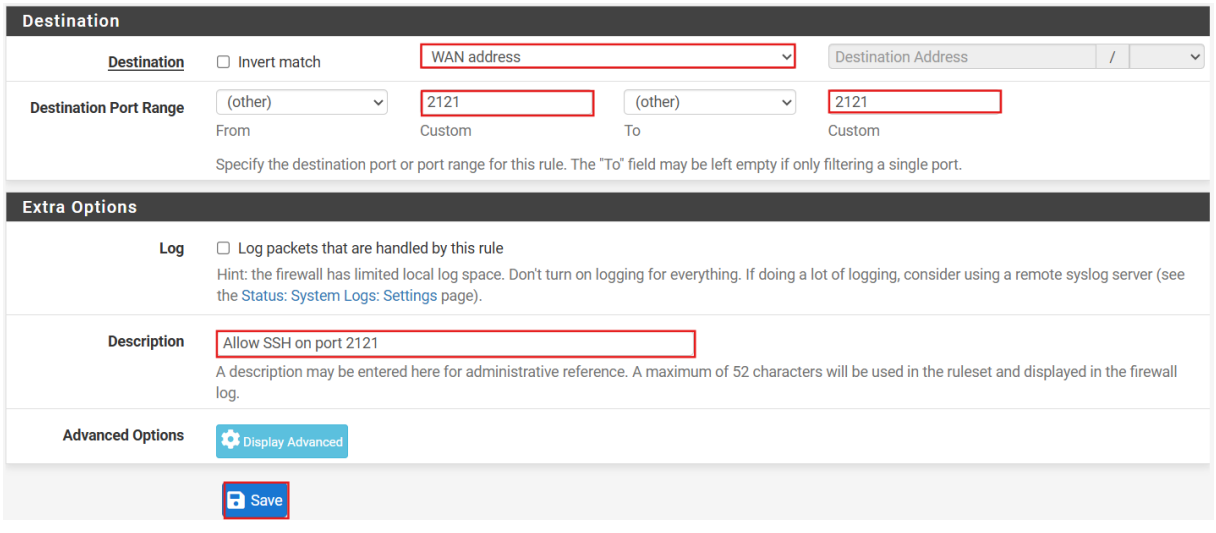


- **Destination** : WAN address
- **Destination port range** :
- `From : 2121`
- `To : 2121`

✓ Description

```
Allow SSH on port 2121
```

4. Clique sur **Save**
5. Clique sur **Apply Changes**

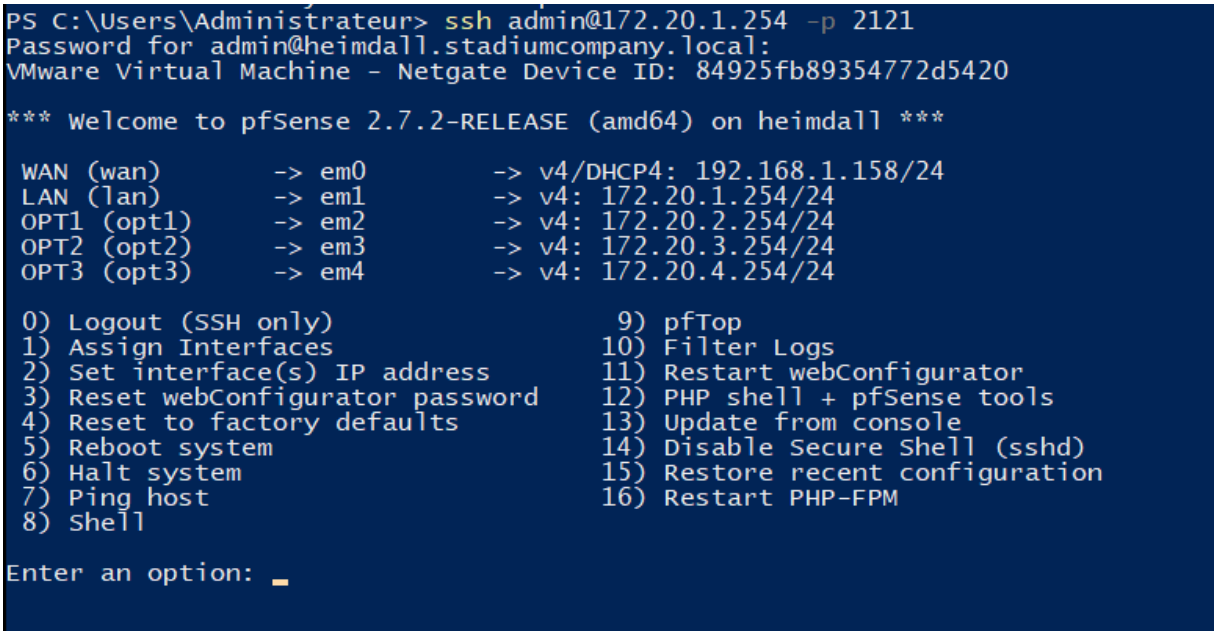


☞ Maintenant, pfSense accepte les connexions SSH sur le port 2121.

Étape 3 — Tester la connexion SSH

Depuis un poste du VLAN 10 (Administration), ouvre PowerShell :

```
ssh admin@172.20.1.254 -p 2121
```



8.3 Sécuriser l'accès HTTPS sur pfSense

L'objectif est de :

- remplacer le certificat auto-signé par défaut
- créer une **Autorité de Certification interne (CA)**
- créer un **certificat Web** signé par cette CA
- appliquer ce certificat à l'interface Web pfSense
- forcer l'accès en **HTTPS uniquement**
- désactiver totalement **HTTP**

Étape 1 — Créer une Autorité de Certification interne (CA)

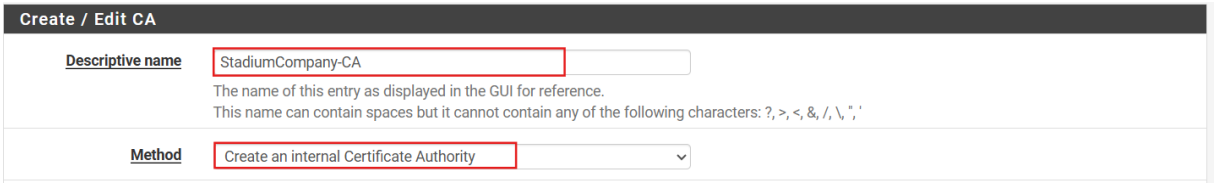
1. Connecte-toi à pfSense
2. Va dans :
   System → Certificates

3. Clique sur l'onglet **Authorities**
4. Clique sur **Add**

✓ Remplis les champs comme suit :

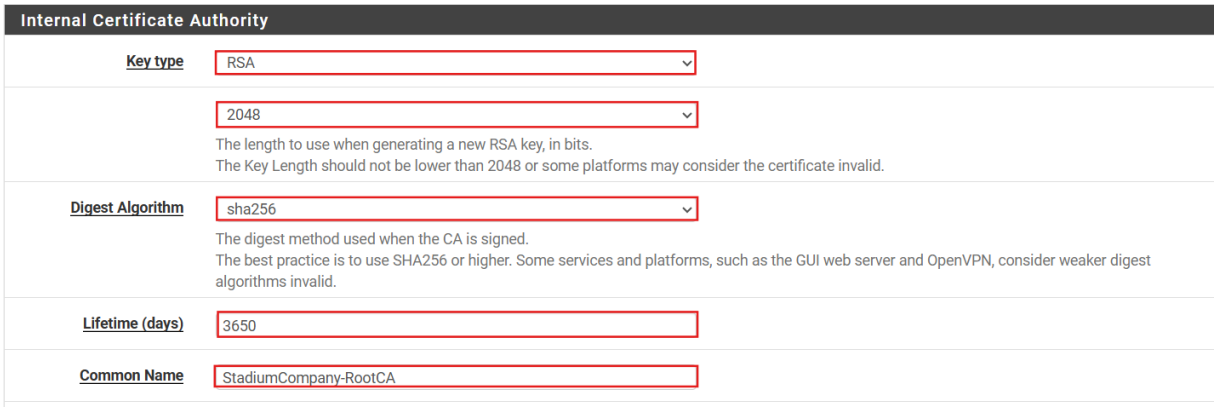
Informations générales

- **Descriptive Name :** `StadiumCompany-CA`
- **Method :** `Create an internal Certificate Authority`



Paramètres cryptographiques

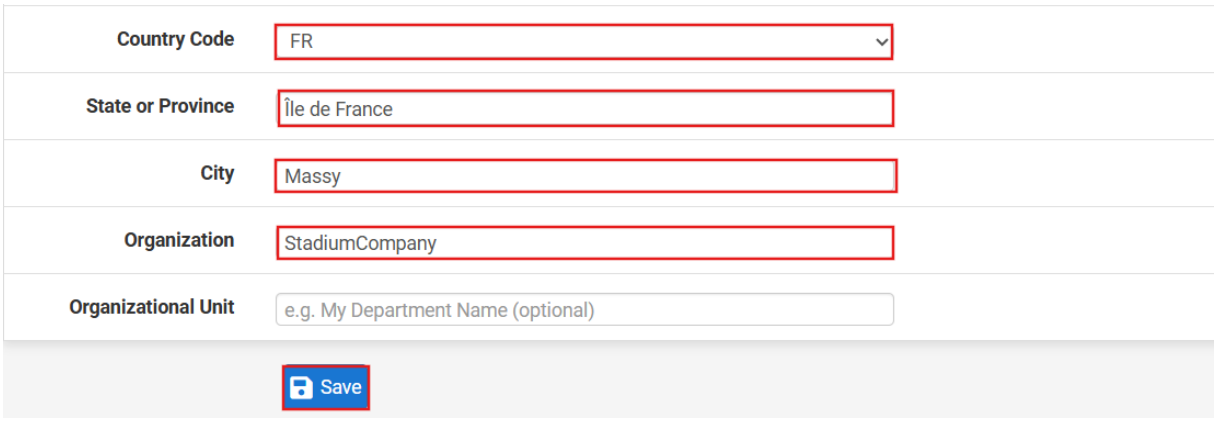
- **Key Type :** RSA
- **Key Length :** 2048 bits (ou 4096 si tu veux plus sécurisé)
- **Digest Algorithm :** SHA256
- **Lifetime (days) :** 3650 (10 ans)



Informations du certificat

- **Country Code :** FR
- **State :** Île de France
- **City :** Massy
- **Organization :** StadiumCompany
- **Common Name :** `StadiumCompany-RootCA`

5. Clique sur **Save**



☞ **Ta CA interne est maintenant créée.**

Elle servira à signer tous les certificats internes (dont celui du WebGUI).

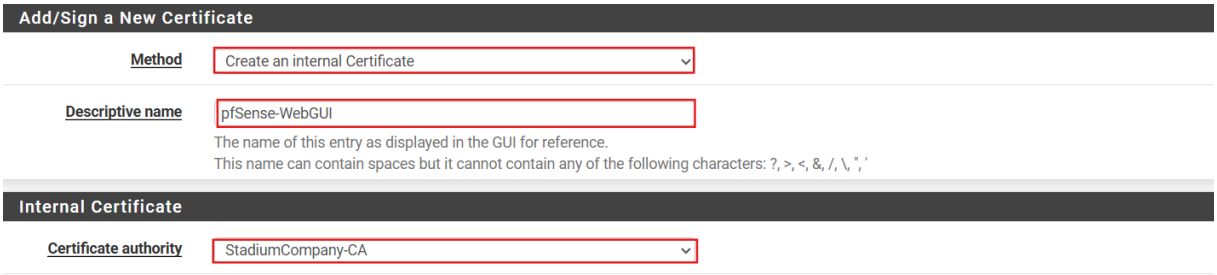
Étape 2 — Créer le certificat Web pour pfSense

1. Reste dans :
   System → Certificates
2. Clique sur l'onglet **Certificates**
3. Clique sur **Add/Sign**

✓ Remplis les champs :

Informations générales

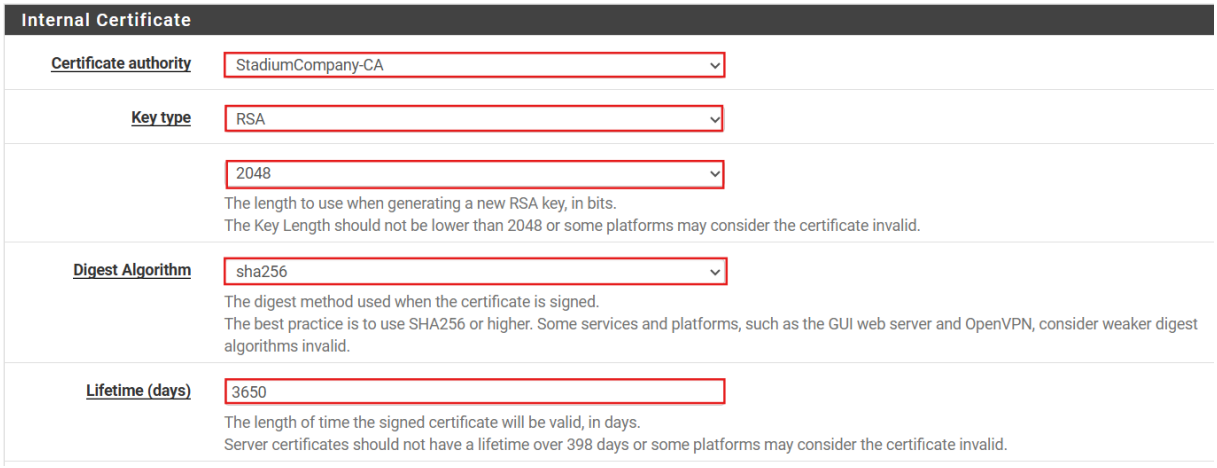
- **Method :**
- `Create an internal certificate`
- **Descriptive Name :** `pfSense-WebGUI`
- **Certificate Authority :** `StadiumCompany-CA`



Paramètres cryptographiques

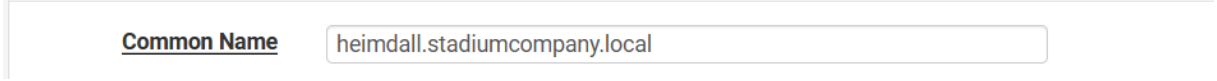
- **Key Type :** RSA

- **Key Length :** 2048 bits
- **Digest Algorithm :** SHA256
- **Lifetime :** 3650



Informations du certificat

- **Common Name :** `heimdall.stadiumcompany.local`



✓ Alternative Names (SAN)

Tu dois ajouter **3 lignes** :

◆ 1ère ligne SAN

- **Type :** FQDN or Hostname
- **Value :** `heimdall`

◆ 2ème ligne SAN

Clique sur **+ Add SAN Row**

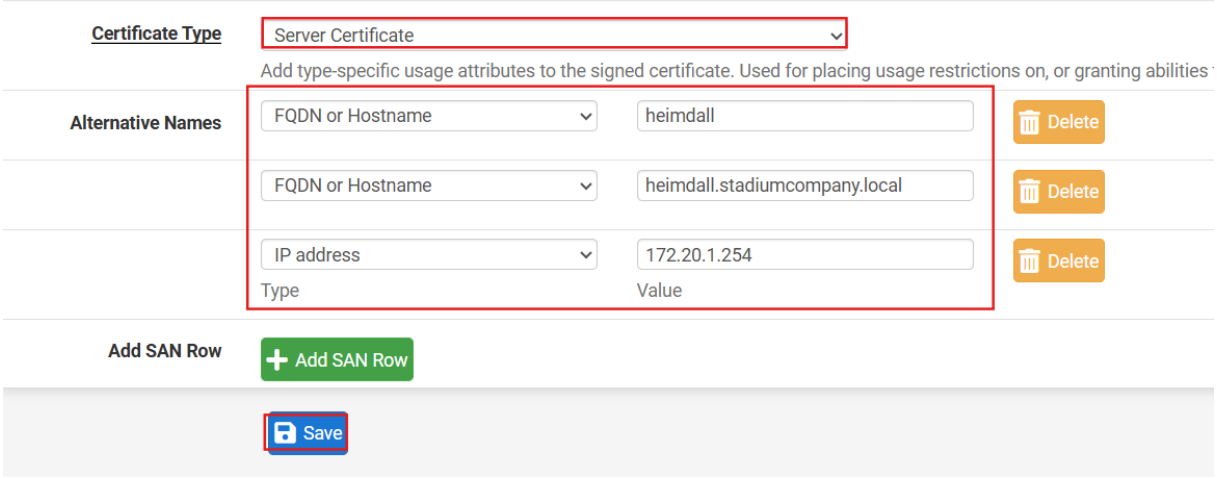
- **Type :** FQDN or Hostname
- **Value :** `heimdall.stadiumcompany.local`

◆ 3ème ligne SAN

Clique encore sur **+ Add SAN Row**

- **Type :** IP address
- **Value :** `172.20.1.254`

4. Clique sur **Save**



☞ Tu viens de créer un certificat Web parfaitement valide, signé par ta CA interne, compatible avec :

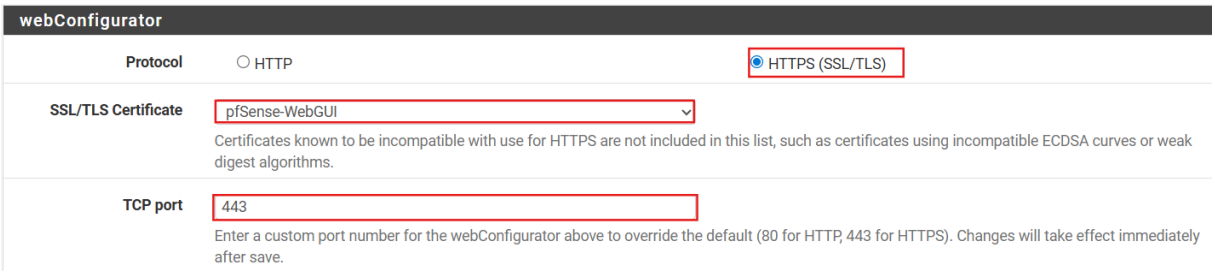
- le nom court : **heimdall**
- le FQDN : **heimdall.stadiumcompany.local**
- l'IP : **172.20.1.254**

Étape 3 — Appliquer le certificat à l'interface Web

1. Va dans :
   System → Advanced → Admin Access
2. Section **WebConfigurator**

✓ Paramètres à modifier :

- **Protocol :** HTTPS
- **SSL Certificate :** `pfSense-WebGUI`
- **TCP Port :** 443 (par défaut)



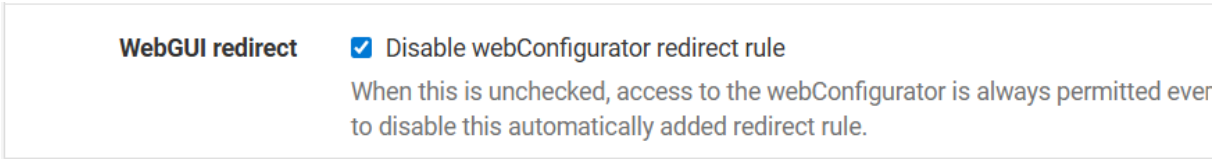
3. Clique sur **Save**

pfSense redémarre automatiquement le service Web.

Étape 4 — Forcer l'accès HTTPS

Toujours dans **System → Advanced → Admin Access** :

- Coche :
  ✓ Disable webConfigurator redirect rule



Cela empêche pfSense de rediriger automatiquement HTTP → HTTPS.

Étape 6 — Tester l'accès sécurisé

Dans ton navigateur :

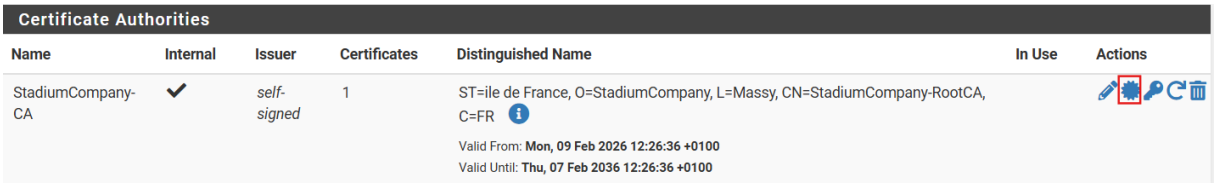
```
https://172.20.1.254
```

Tu dois voir :

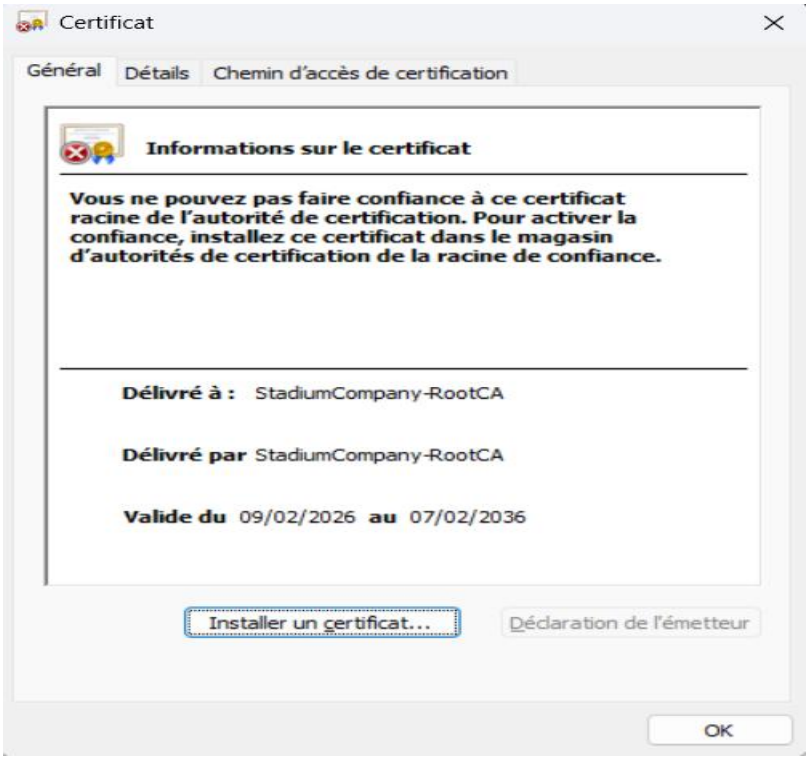
- un cadenas (si tu installes la CA sur ton PC)
- le certificat signé par **StadiumCompany-CA**
- plus aucun accès en HTTP

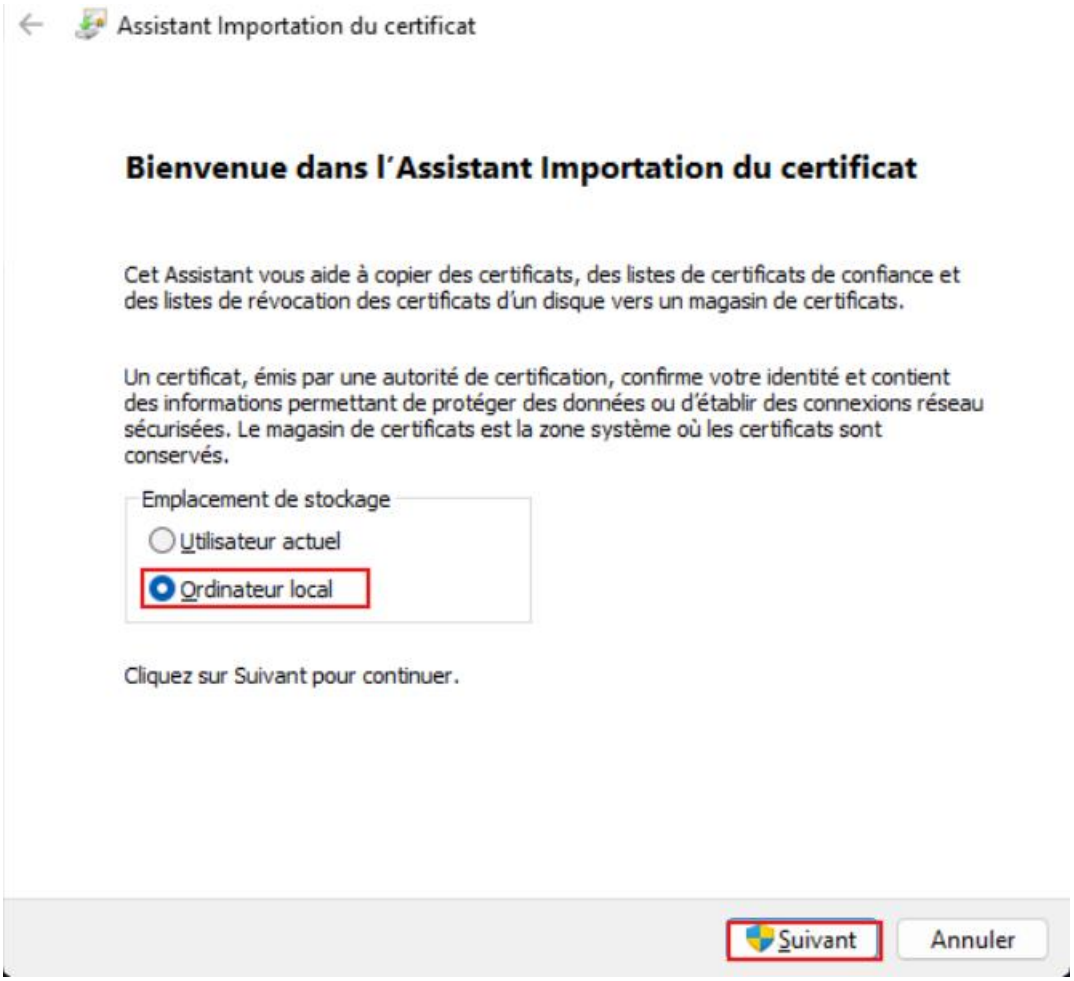
Pour éviter l'avertissement du navigateur :

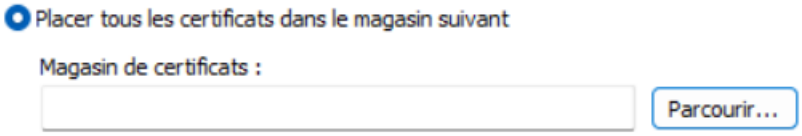
1. Va dans :
   System → Certificates → Authorities
2. Clique sur **Export** de ta CA

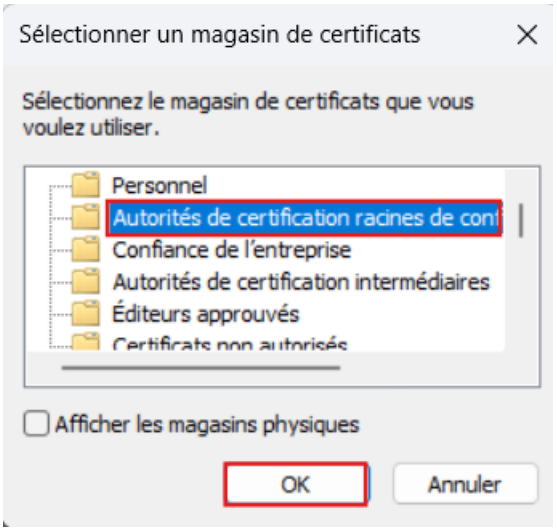


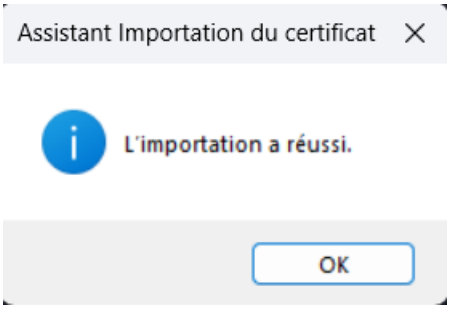
3. Ouvre le fichier `.crt`
4. Installe-le dans :
   Autorités de certification racines de confiance




Assistant Importation du certificat
Bienvenue dans l'Assistant Importation du certificat
Cet Assistant vous aide à copier des certificats, des listes de certificats de confiance et des listes de révocation des certificats d'un disque vers un magasin de certificats.
Un certificat, émis par une autorité de certification, confirme votre identité et contient des informations permettant de protéger des données ou d'établir des connexions réseau sécurisées. Le magasin de certificats est la zone système où les certificats sont conservés.
Emplacement de stockage
Utilisateur actuel
Ordinateur local
Cliquez sur Suivant pour continuer.
Suivant
Annuler


Placer tous les certificats dans le magasin suivant
Magasin de certificats :
Parcourir...


Sélectionner un magasin de certificats
Sélectionnez le magasin de certificats que vous voulez utiliser.
Personnel
Autorités de certification racines de conf
Confiance de l'entreprise
Autorités de certification intermédiaires
Éditeurs approuvés
Certificats non autorisés
Afficher les magasins physiques
OK
Annuler



🎯 Résultat final

Après cette procédure :

- pfSense n'accepte plus que **HTTPS**
- le certificat Web est **signé par ta CA interne**
- l'accès est **chiffré et authentifié**
- HTTP est totalement désactivé
- l'administration est **sécurisée**

9.0 Création des comptes AD nécessaires

Avant de configurer LDAP/LDAPS dans pfSense, il est essentiel de préparer correctement Active Directory.
Cette étape garantit que pfSense pourra :

- interroger l'annuaire AD
- authentifier les utilisateurs
- utiliser LDAPS pour le portail captif
- utiliser AD pour OpenVPN
- gérer les droits via un groupe dédié

Cette préparation comprend **3 éléments obligatoires** :

1. Un **compte de service** (Bind DN)
2. Un **groupe de sécurité**
3. Des **utilisateurs de test**

✓ 9.0.1 Créer le compte de service pfsensead

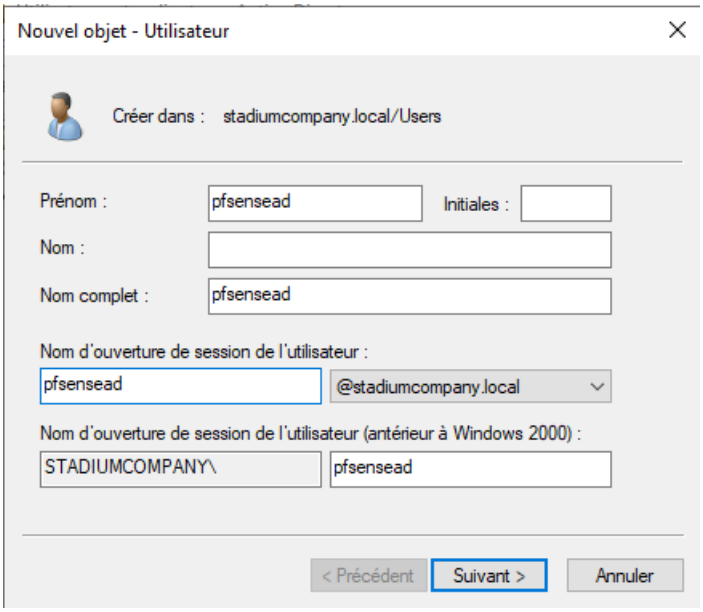
Ce compte permet à pfSense de :

- interroger Active Directory
- parcourir les OU
- vérifier les utilisateurs
- authentifier les connexions
- faire fonctionner LDAP, LDAPS, portail captif, VPN

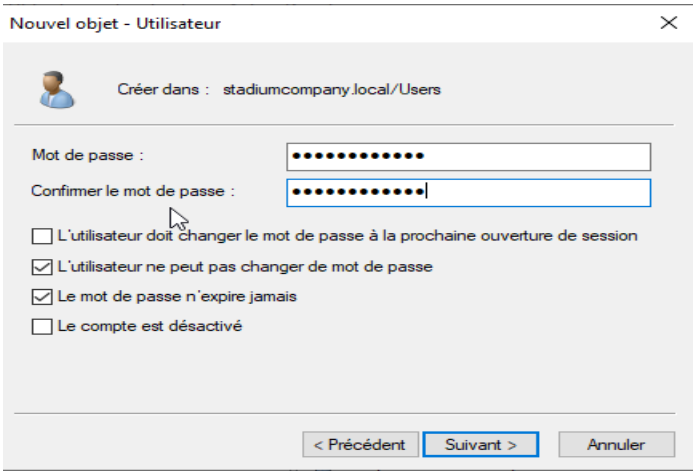
Procédure :

1. Ouvrir **dsa.msc**
2. Aller dans **Users**
3. Clic droit → **New → User**
4. Renseigner :

- First name : pfSense
- Last name : Service
- User logon name : **pfsensead**



5. Mot de passe :
   Exemple : `@azerty1234`
6. Décocher :
   ✓ User must change password at next logon
   ✓ Password never expires
7. Créer



☞ Ce compte sera utilisé comme **Bind DN** dans pfSense.

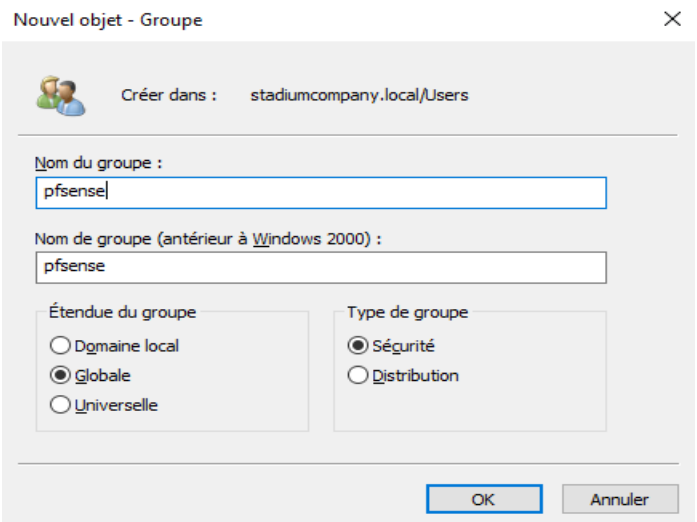
✓ 9.0.2 Créer le groupe pfsense

Ce groupe servira pour :

- accès WebGUI via AD
- VPN
- portail captif
- tests LDAP/LDAPS

Procédure :

1. dsa.msc → Users
2. New → Group
3. Nom : **pfsense**
4. Scope : Global
5. Type : Security
6. Créer



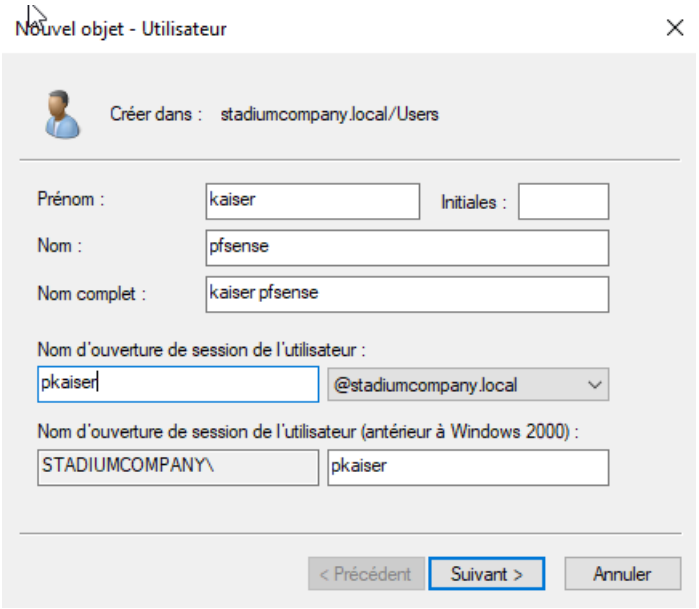
✓ 9.0.3 Créer les utilisateurs AD (ex : kaiser, cesar)

Ces comptes serviront pour les tests et les accès.

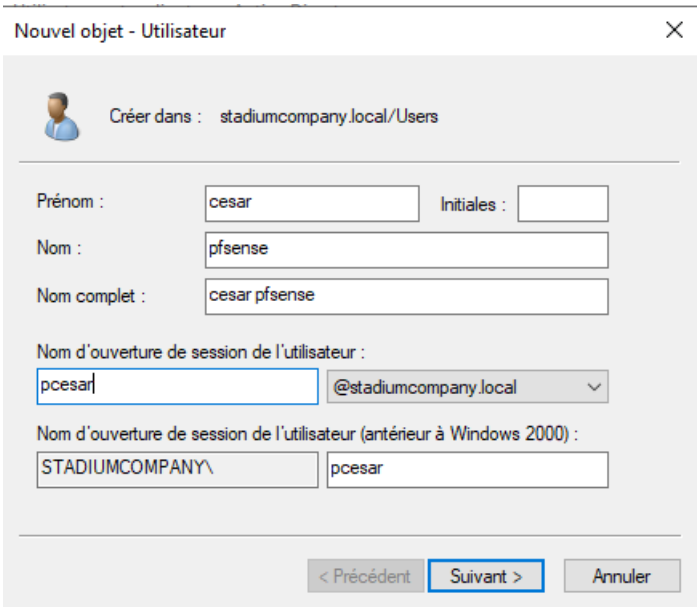
Procédure :

1. dsa.msc → Users
2. New → User
3. Exemple :

- User : **kaiser**



- User : **cesar**



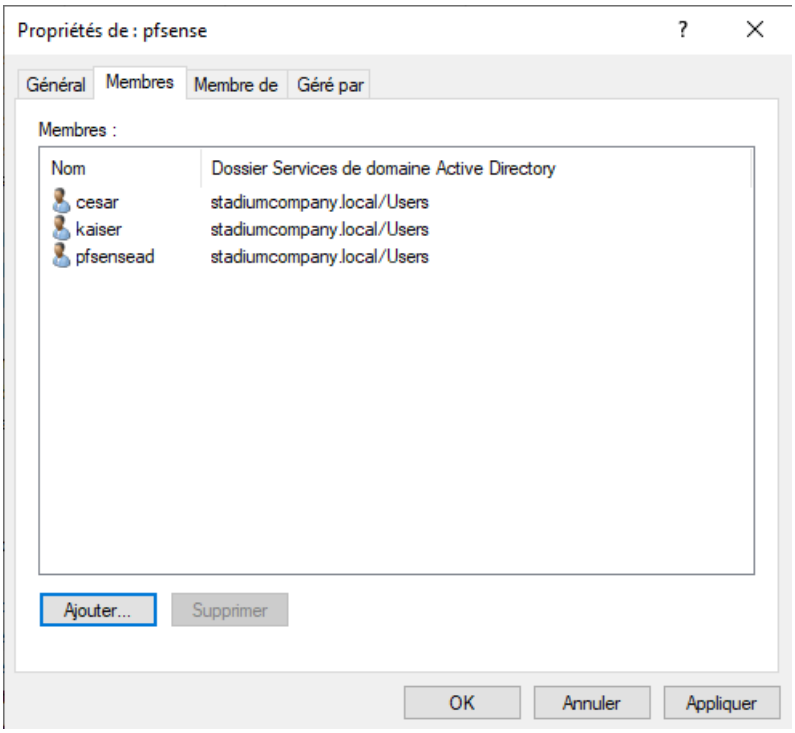
4. Mot de passe simple
5. Décocher "User must change password"
6. Ajouter ces utilisateurs au groupe **pfsense**

✓ 9.0.4 — Ajouter tous les comptes au groupe pfsense

Étape indispensable pour que pfSense reconnaisse les utilisateurs AD.

Procédure :

1. Dans **dsa.msc**, conteneur **Users**
2. Double-cliquer sur le groupe **pfsense**
3. Onglet **Members**
4. Cliquer sur **Add…**
5. Ajouter les comptes suivants : `pfsensead, kaiser, cesar`
6. Cliquer sur **Check Names**
7. Cliquer sur **OK**
8. Vérifier que les trois comptes apparaissent dans la liste
9. Valider avec **OK**



État final attendu

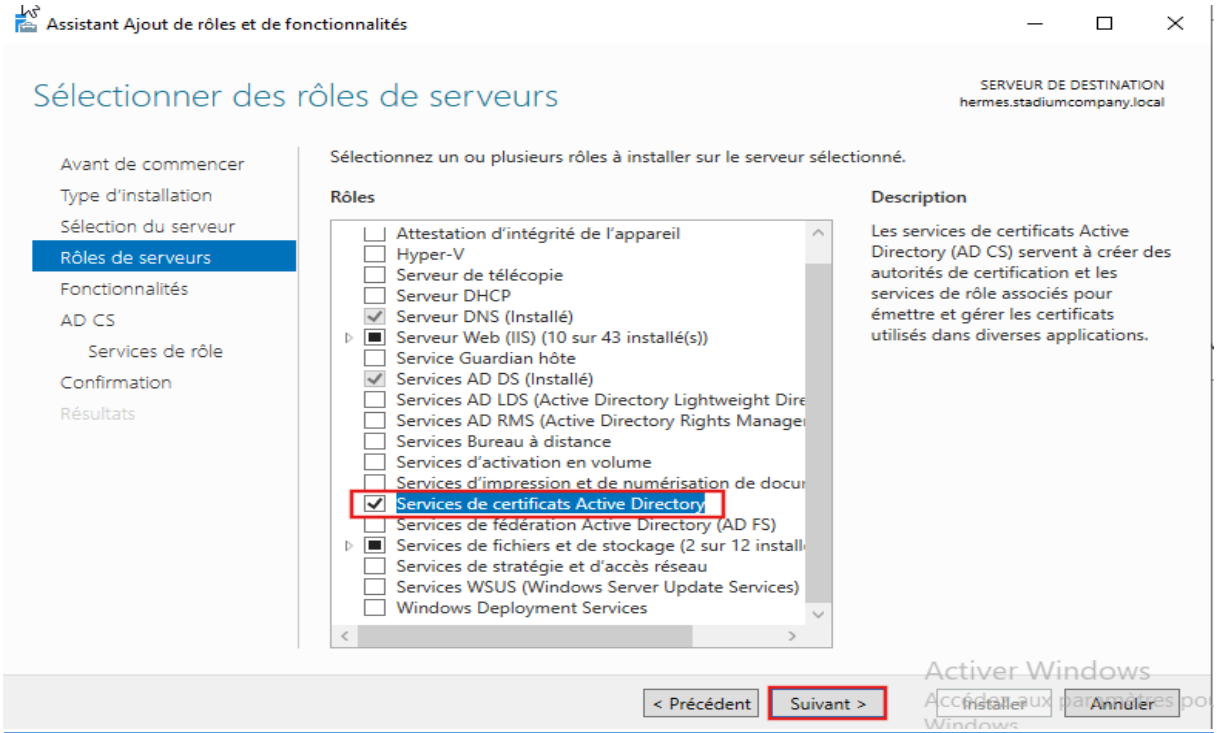
Élément	Statut	Commentaire
Groupe `pfsense`	✔ Créé	Groupe de sécurité global
Utilisateur `pfsensead`	✔ Créé	Compte de service (Bind DN)
Utilisateur `kaiser`	✔ Créé	Compte test
Utilisateur `cesar`	✔ Créé	Compte test
Tous membres du groupe `pfsense`	✔ OK	Prêt pour LDAP/LDAPS

9.1 Préparation côté Active Directory (Hermes)

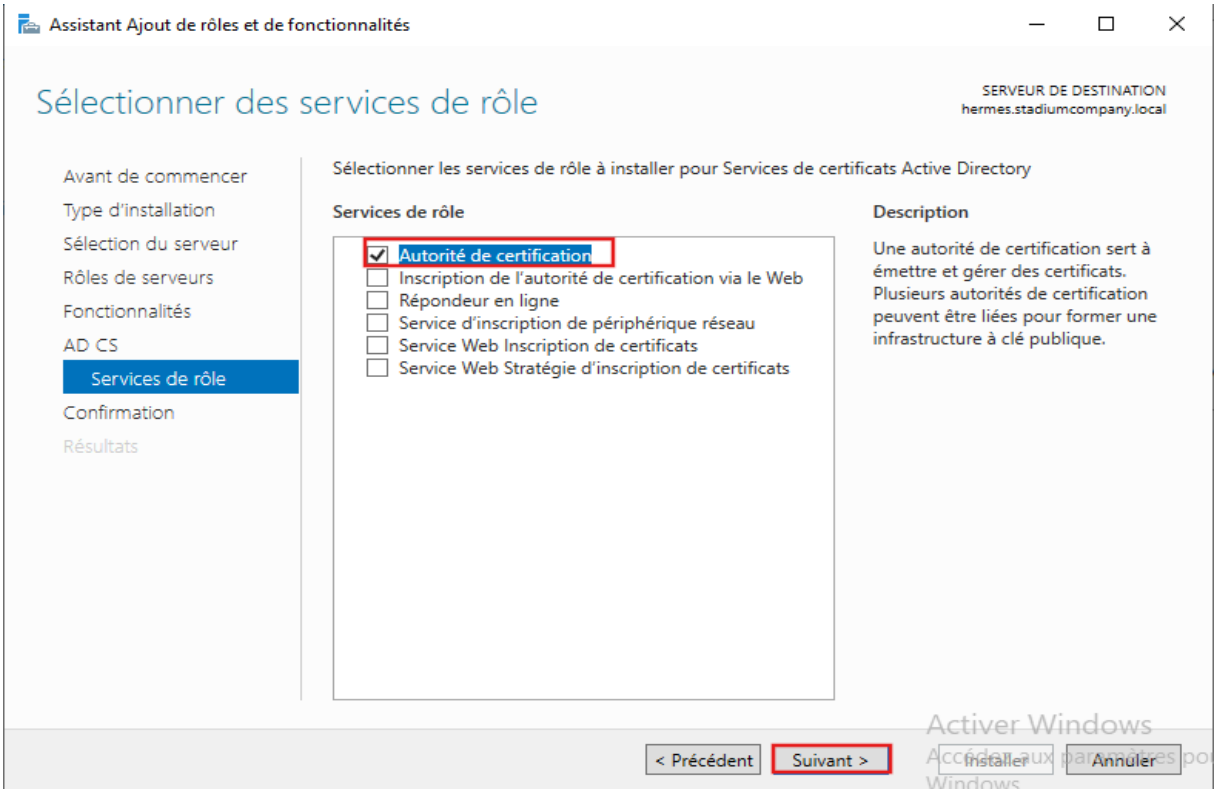
Sur ton serveur **Hermes (Windows Server)** :

✓ 1. Installer le rôle d'Autorité de Certification (CA)

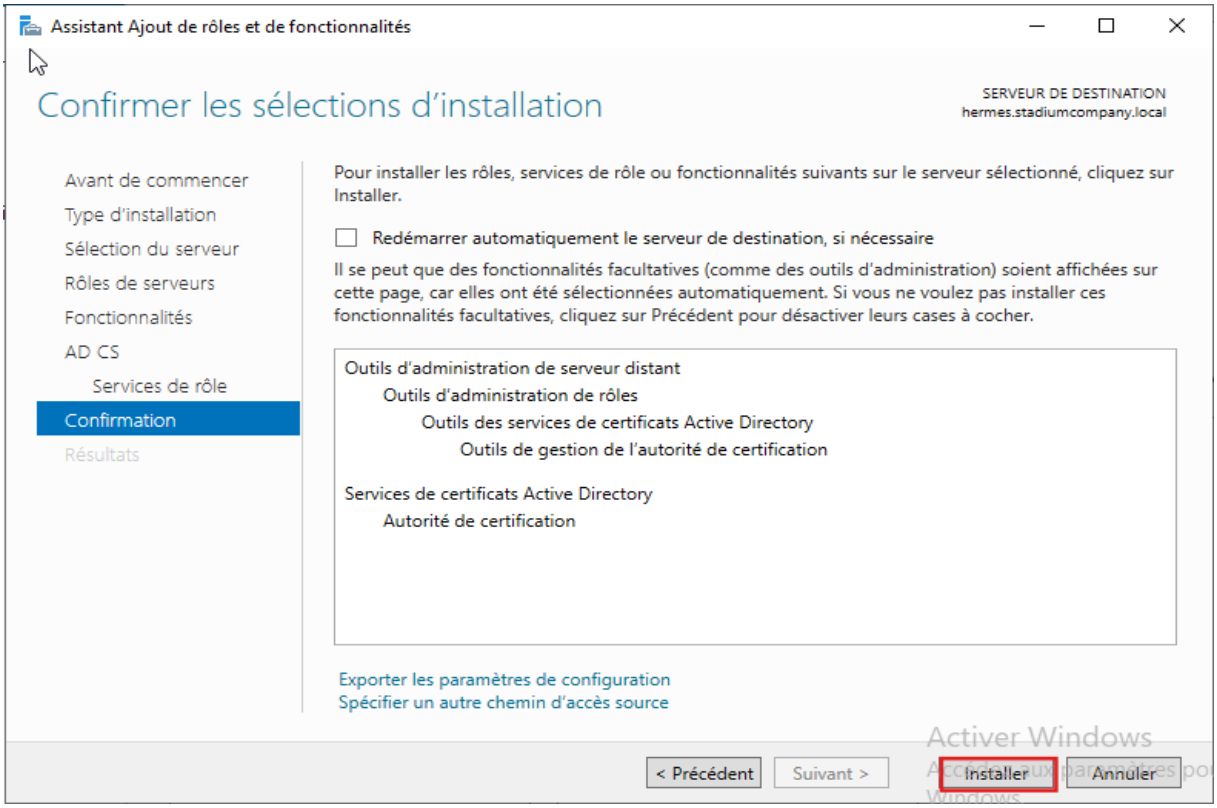
1. Ouvre **Server Manager**
2. Add Roles and Features
3. Active Directory Certificate Services



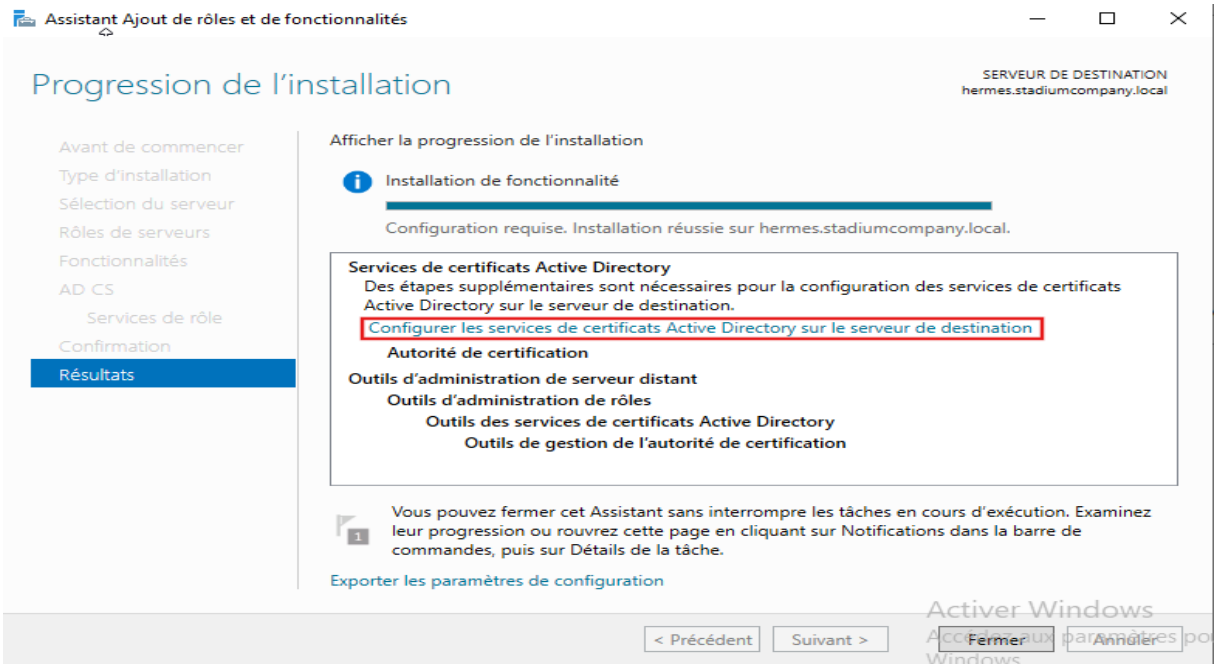
4. Sélectionne :
    - **Certification Authority**



5. Installe



6. Configure la CA en **Enterprise Root CA**



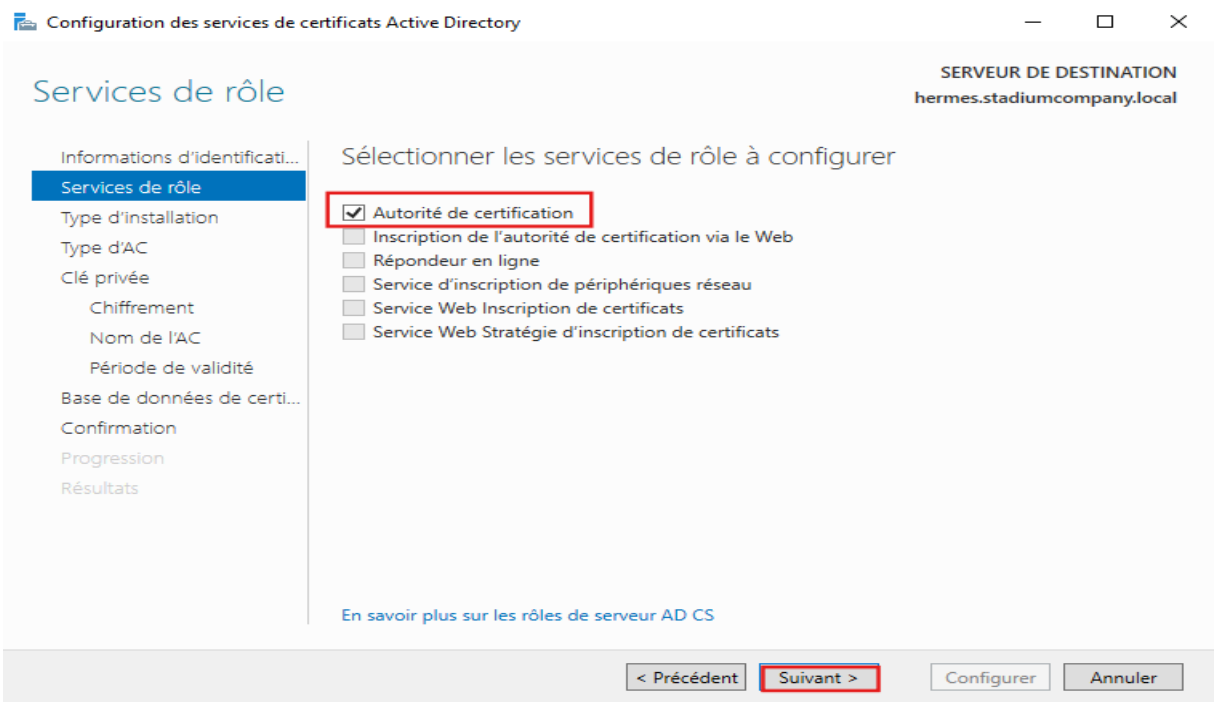
☞ Cela crée automatiquement une **racine de confiance** pour ton domaine.

✓ 1. Rôle à configurer

Coche uniquement :

```
Autorité de certification
```

Puis **Suivant**.

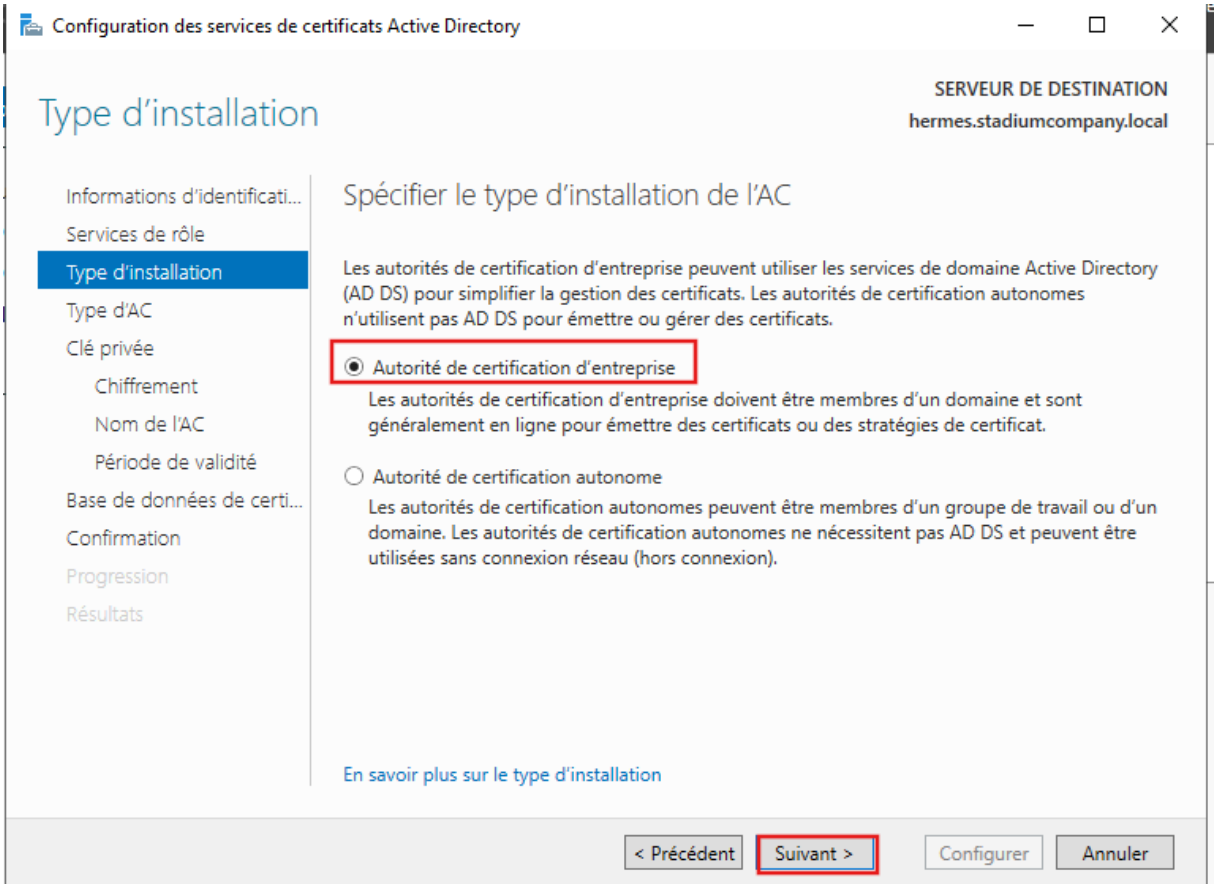


✓ 2. Type d'autorité

Choisis :

`Autorité de certification d'entreprise (Enterprise CA)`

Pourquoi ?
Parce que Hermes est un contrôleur de domaine et doit publier les certificats dans AD.

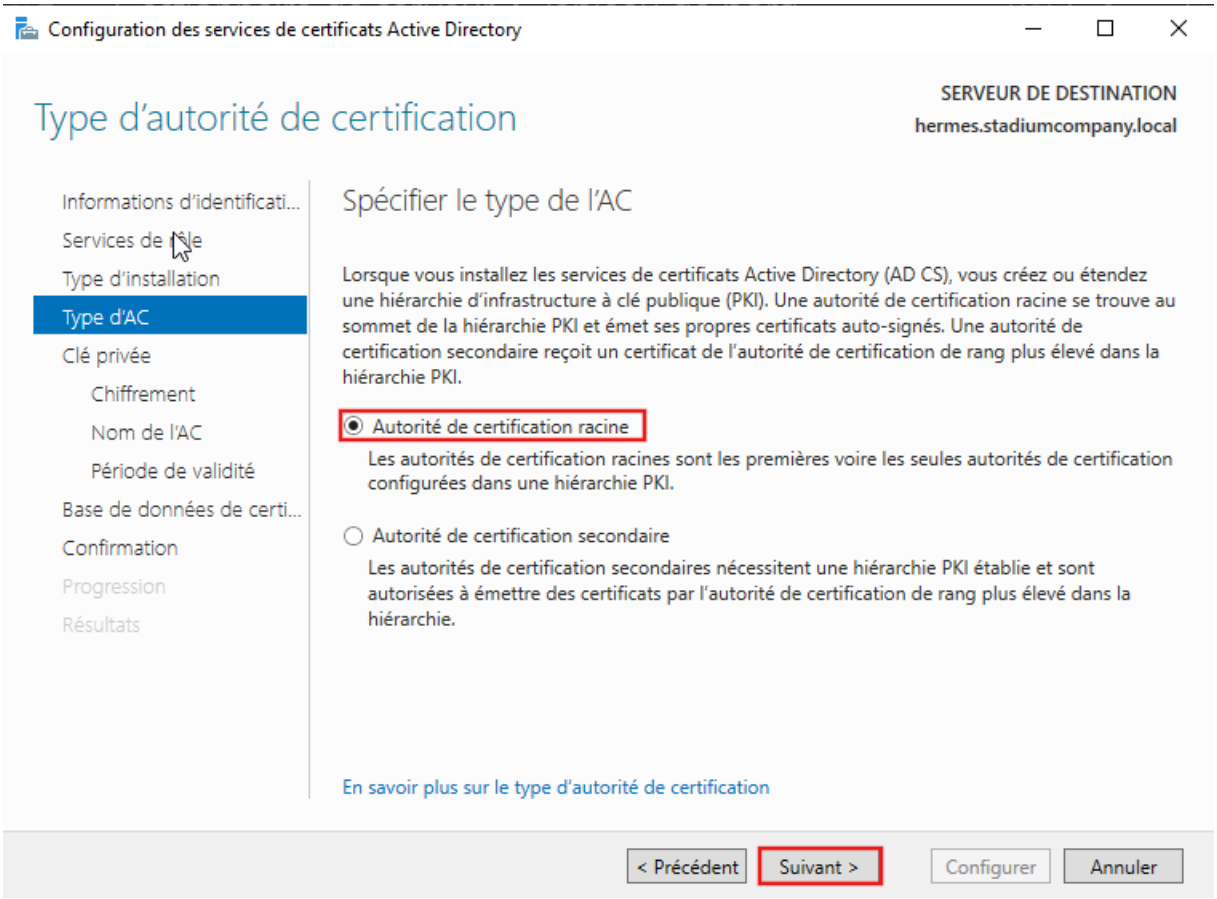


✓ 3. Type de CA

Choisis :

```
Autorité de certification racine (Root CA)
```

C'est ta racine de confiance.

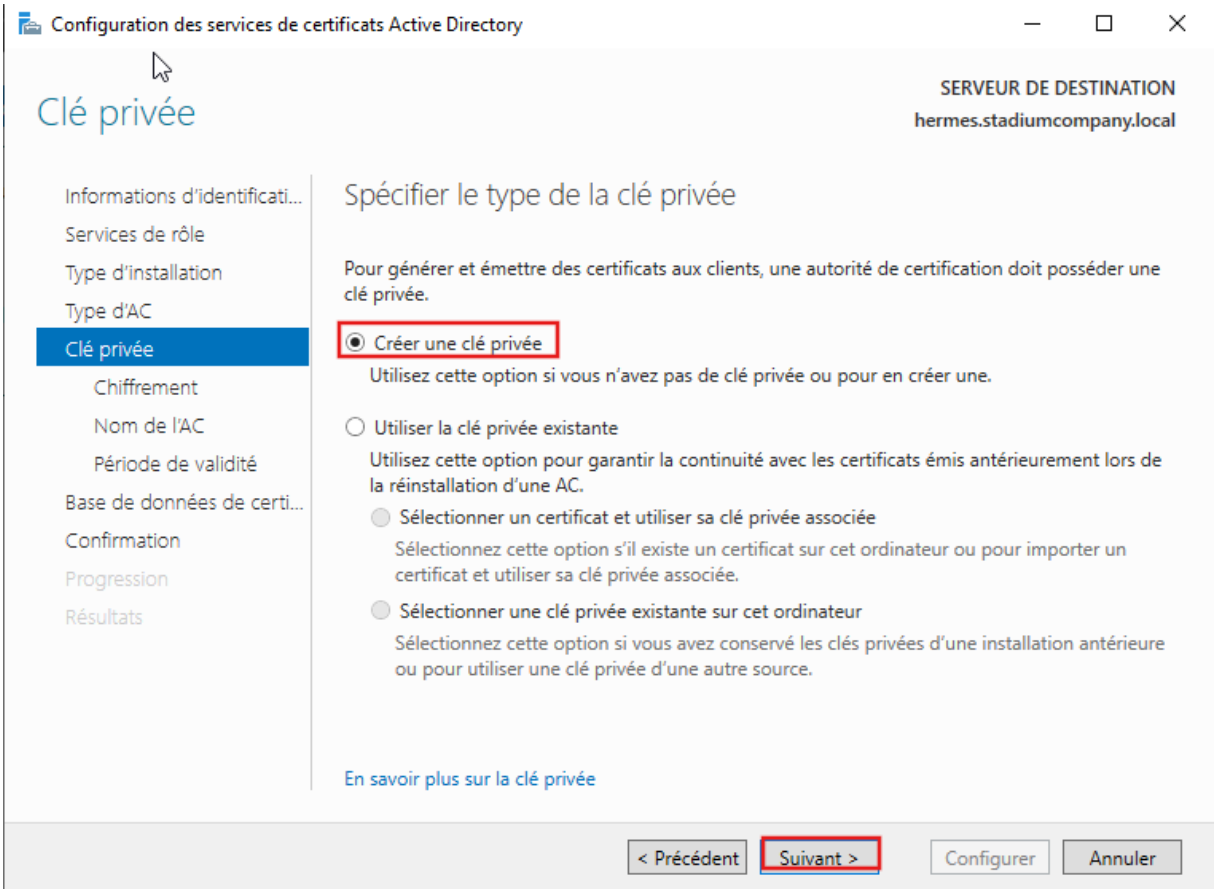


✓ 4. Clé privée

Choisis :

`Créer une nouvelle clé privée`

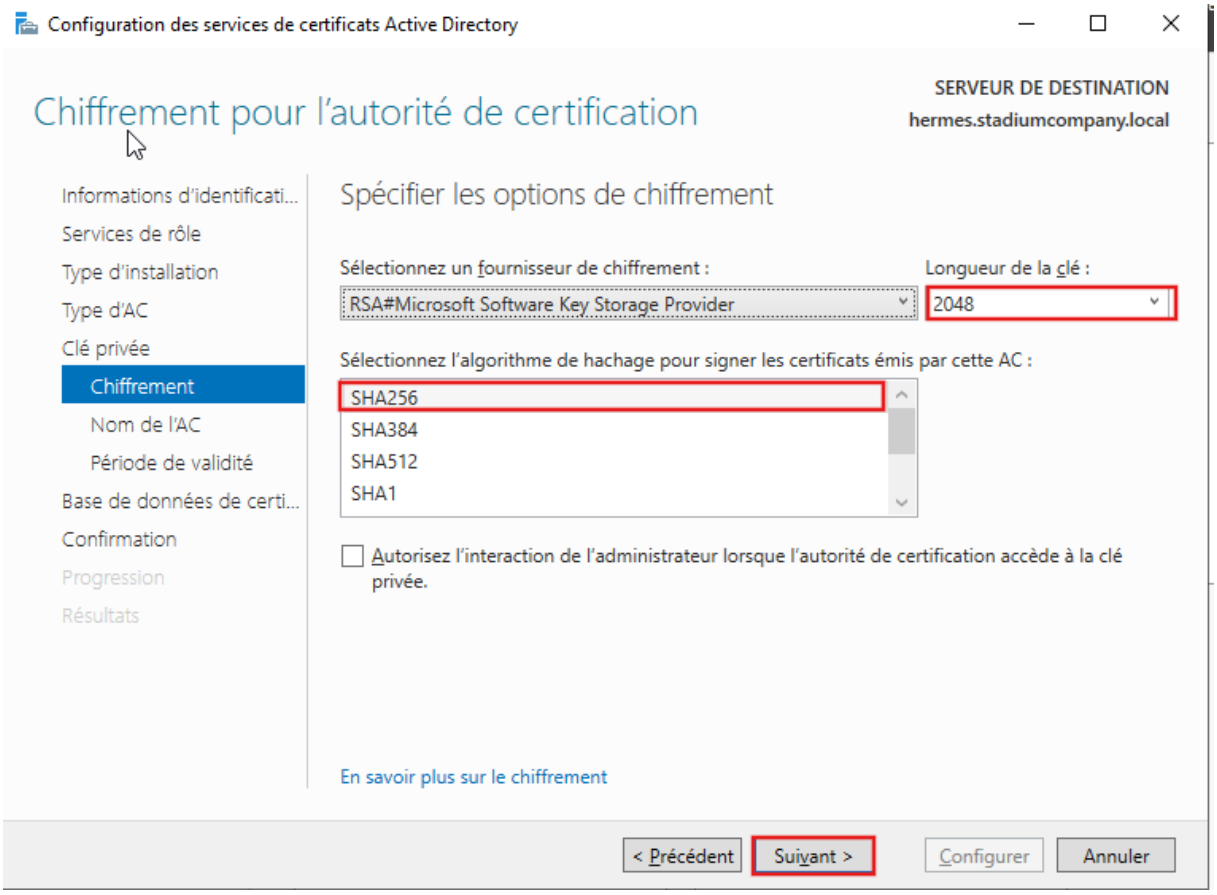
Toujours une clé neuve.



✓ 5. Paramètres cryptographiques

Choisis :

- **Longueur de clé :** 2048 ou 4096 bits
- **Algorithme de hachage :** SHA256



✓ 6. Nom de l'autorité

Tu peux laisser tel quel. Suivant

✓ 7. Validité

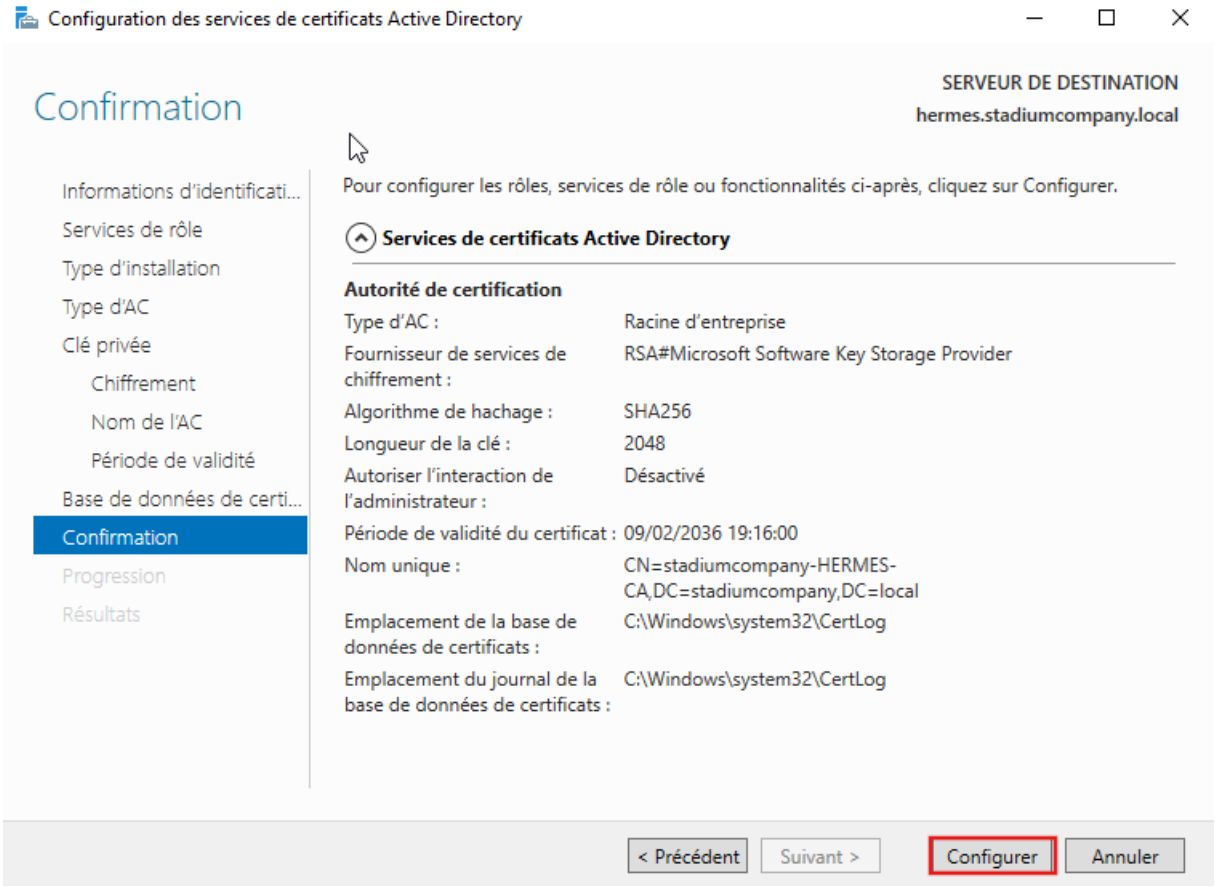
Choisis : `5 ans ou 10 ans puis suivant`

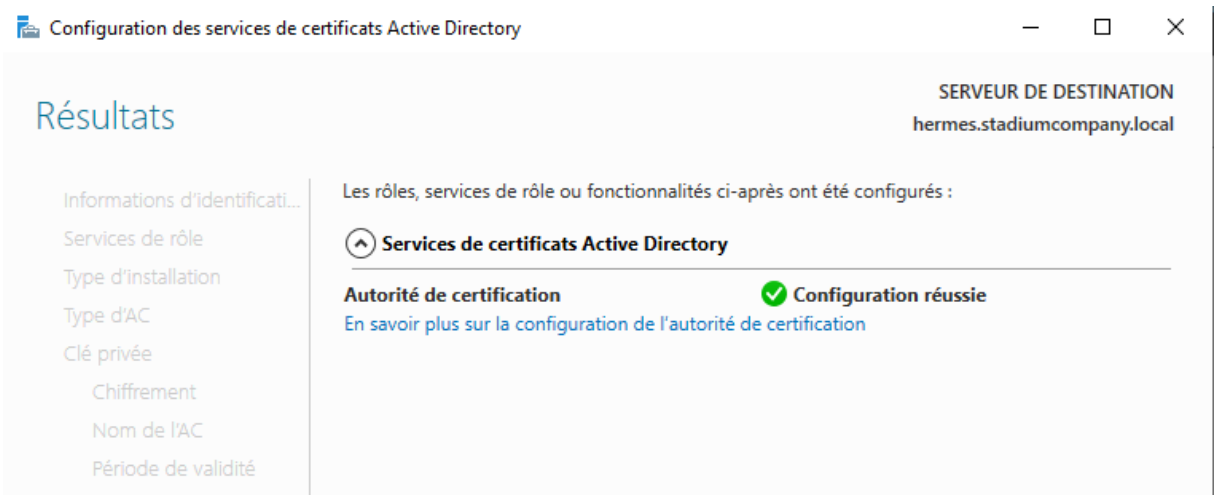
✓ 8. Emplacement de la base de données

Laisse les valeurs par défaut.

✓ 9. Confirmer et installer

Clique sur **Configurer**.





Une fois terminé :

- Hermes devient **CA racine** du domaine

- LDAPS (port 636) est automatiquement activé
- Tu pourras exporter le certificat racine pour pfSense
- Tu pourras configurer LDAP + LDAPS dans pfSense

✓ 3. Activer LDAPS (port 636)

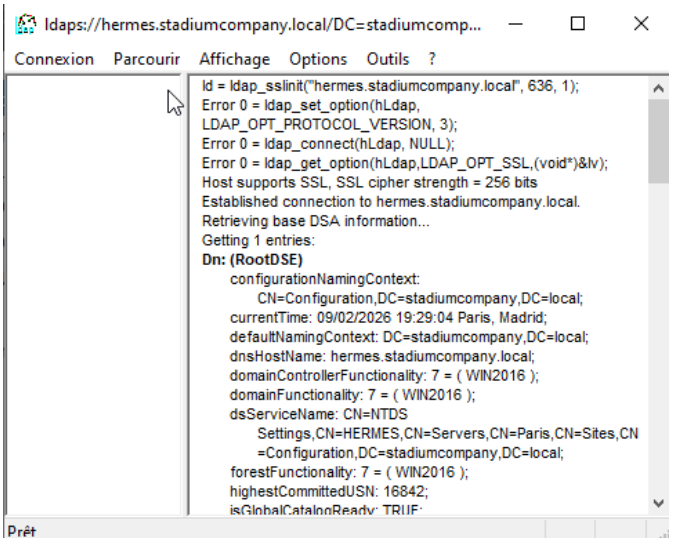
LDAPS est automatiquement activé **dès que le serveur possède un certificat valide** pour :

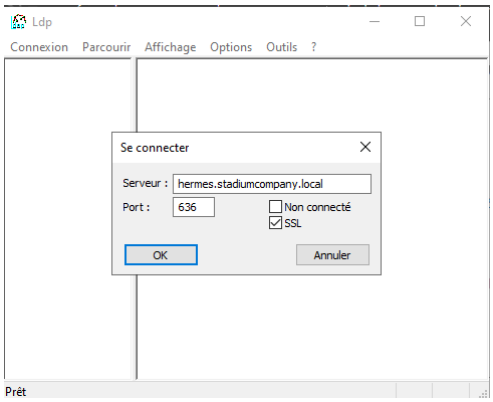
- **FQDN du serveur**
- **Nom NetBIOS**
- **Nom complet AD**

Pour vérifier :

1. Ouvre **LDP.exe**
2. Connexion → Connect
3. Host : `hermes.stadiumcompany.local`
4. Port : **636**
5. Coche **SSL**

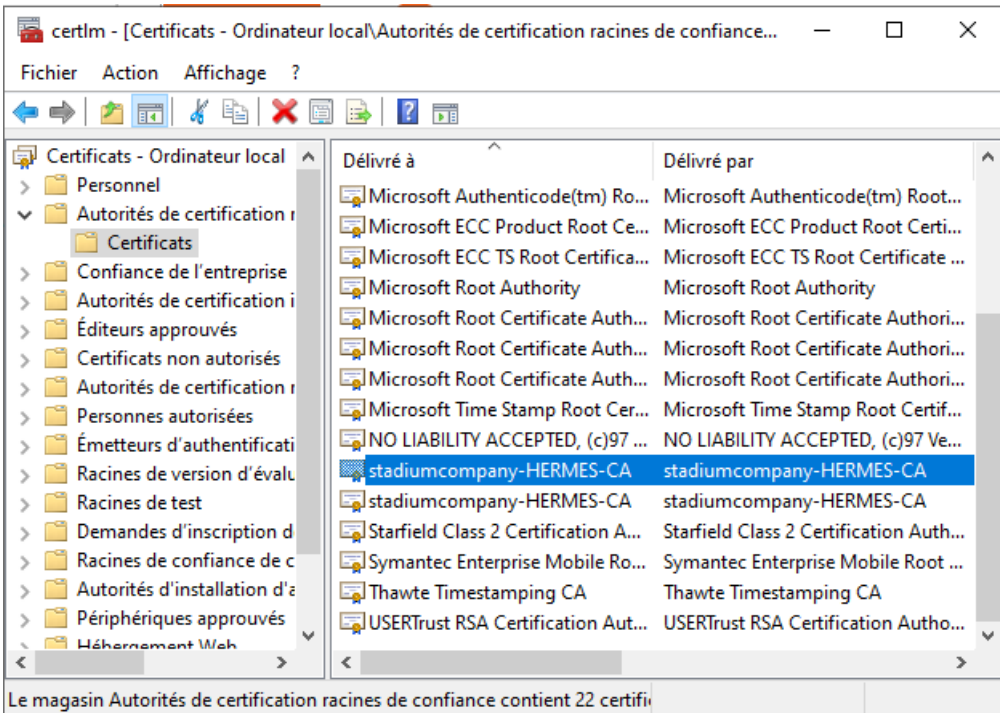
Si la connexion réussit → LDAPS est opérationnel.



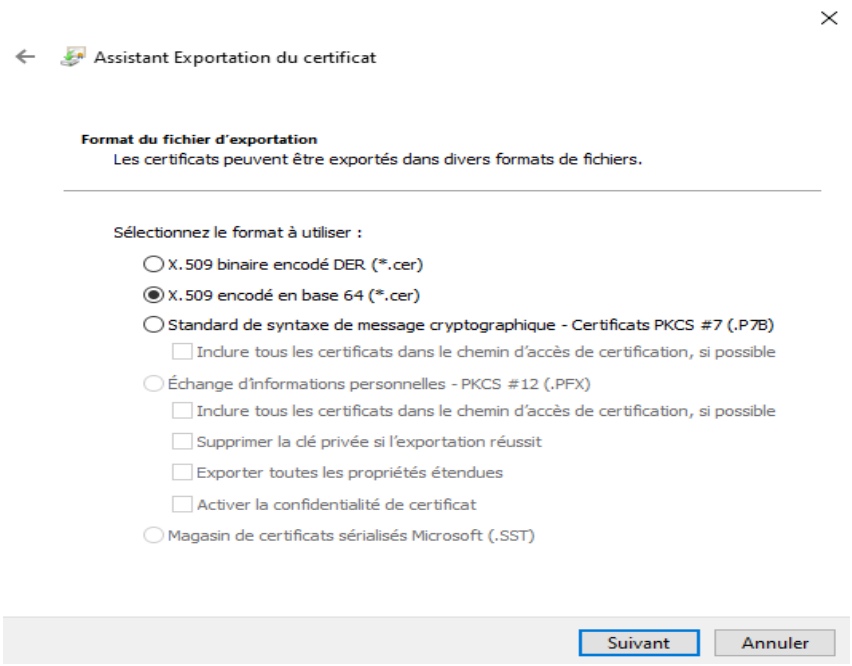


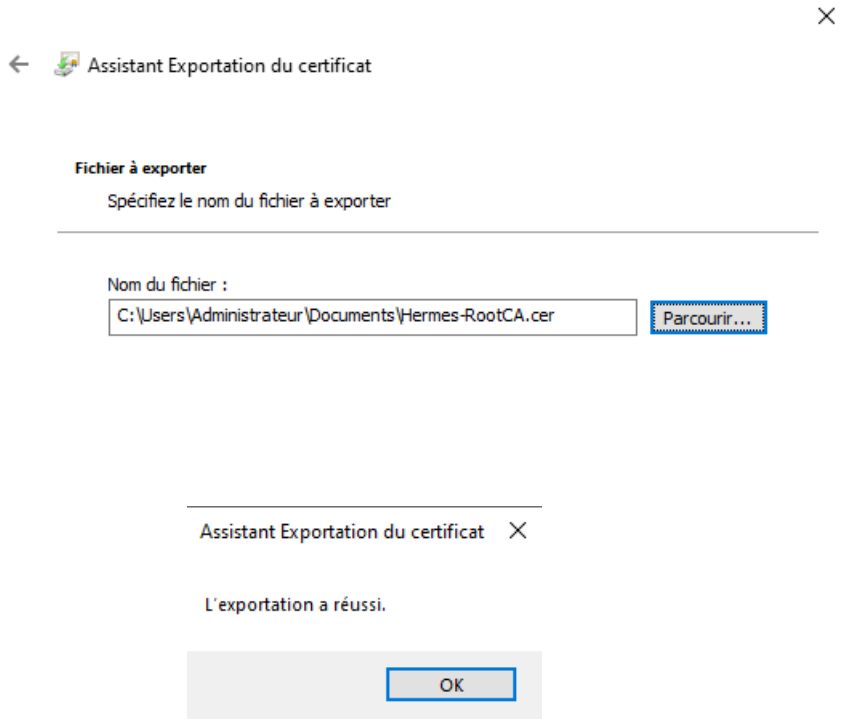
✓ 4. Exporter le certificat racine AD

1. Ouvre **certlm.msc**
2. Va dans :
   Autorités de certification racines de confiance → Certificats
3. Trouve ton certificat racine (ex : *Hermes-RootCA*)



4. Clic droit → **Exporter**
5. Format : **Base-64 (.cer)**



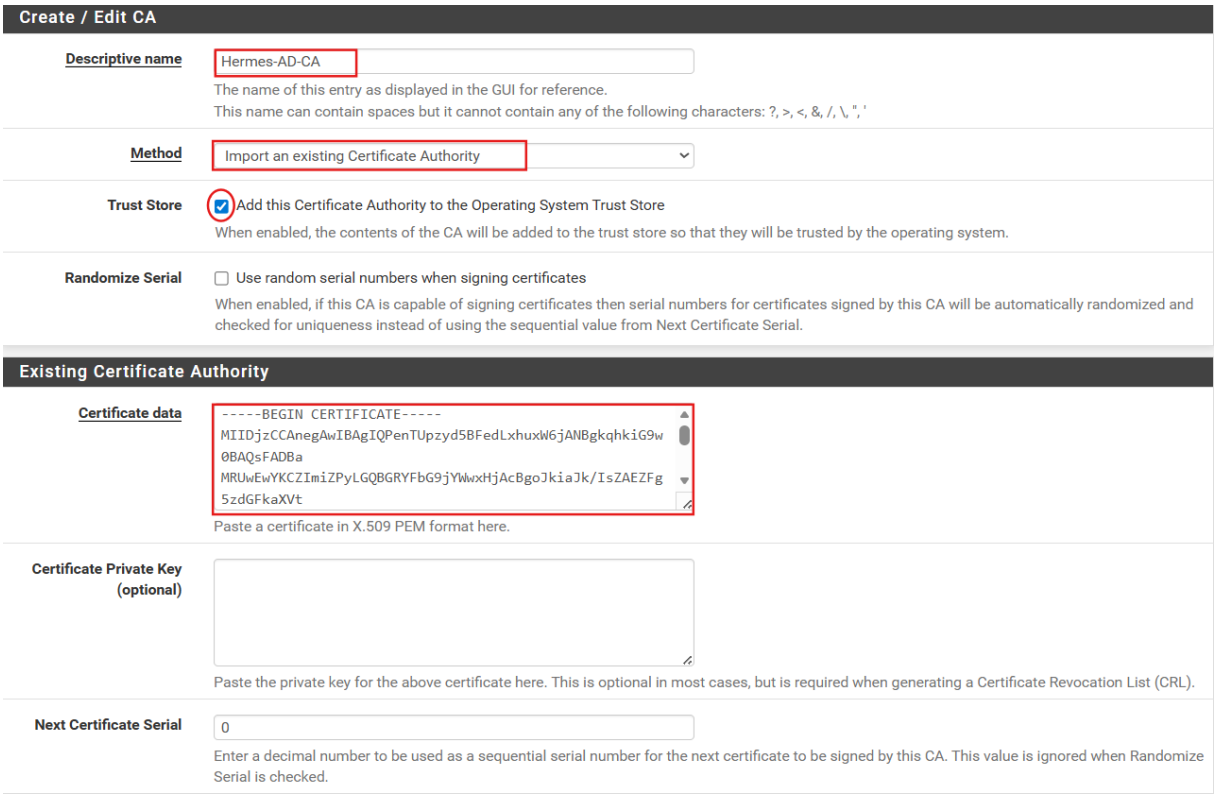


Ce fichier sera importé dans pfSense.

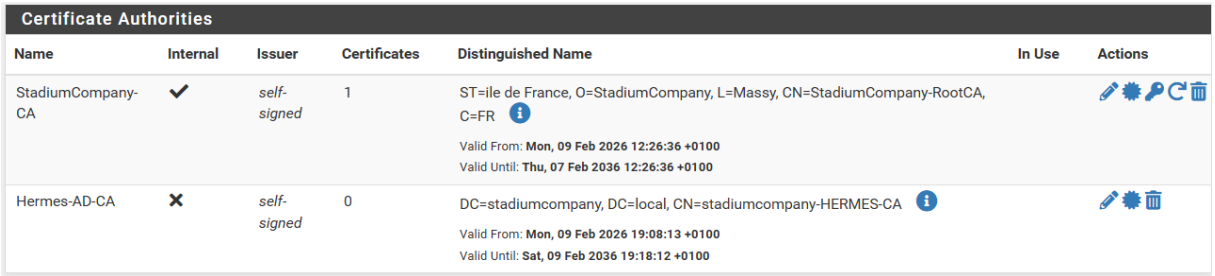
9.2 Importer la CA AD dans pfSense

Sur pfSense :

1. Aller dans :
   System → Certificates → Authorities
2. Cliquer sur **Add**
3. Méthode : `Import an existing Certificate Authority`
4. Coller le contenu du fichier **.cer** exporté depuis Hermes
5. Descriptive Name : `Hermes-AD-CA`
6. Cliquer sur **Save**



☞ pfSense fait maintenant confiance aux certificats émis par Hermes.
☞ LDAPS pourra fonctionner.



9.3 Configuration du backend LDAP (389)

Ce backend LDAP non chiffré sert uniquement pour les **tests initiaux**.
Il permet de valider que pfSense communique correctement avec Active Directory avant de passer au LDAPS sécurisé.

📌 Accès au menu

pfSense → **System → User Manager → Authentication Servers → Add**

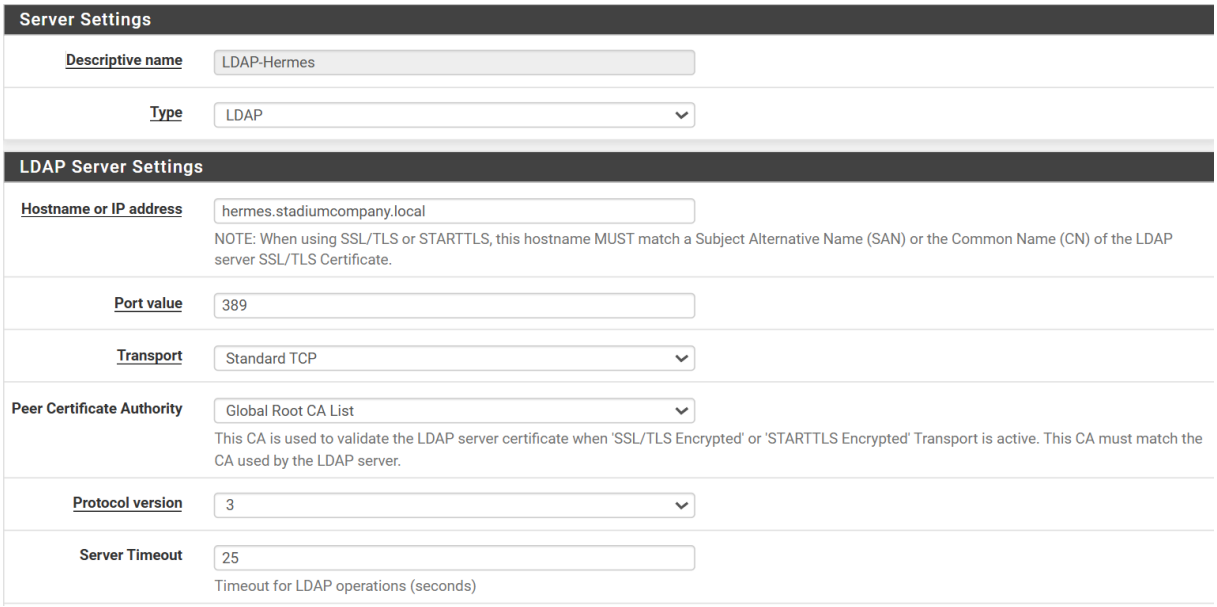
Paramètres LDAP (389) — Configuration correcte

Identification

- **Descriptive name** : `LDAP-389-Test / LDAP-Hermes`
- **Type** : `LDAP`

Connexion au serveur AD

Paramètre	Valeur
Hostname	`hermes.stadiumcompany.local`
Port	`389`
Transport	`TCP - Standard`
Protocol version	`3`
Server Timeout	`25`



Base de recherche

Paramètre	Valeur
Base DN	`DC=stadiumcompany,DC=local`
Authentication containers	`CN=Users,DC=stadiumcompany,DC=local`

Important :

- Toujours utiliser **CN=Users**, pas OU=Users
- Toujours séparer les DC par des virgules

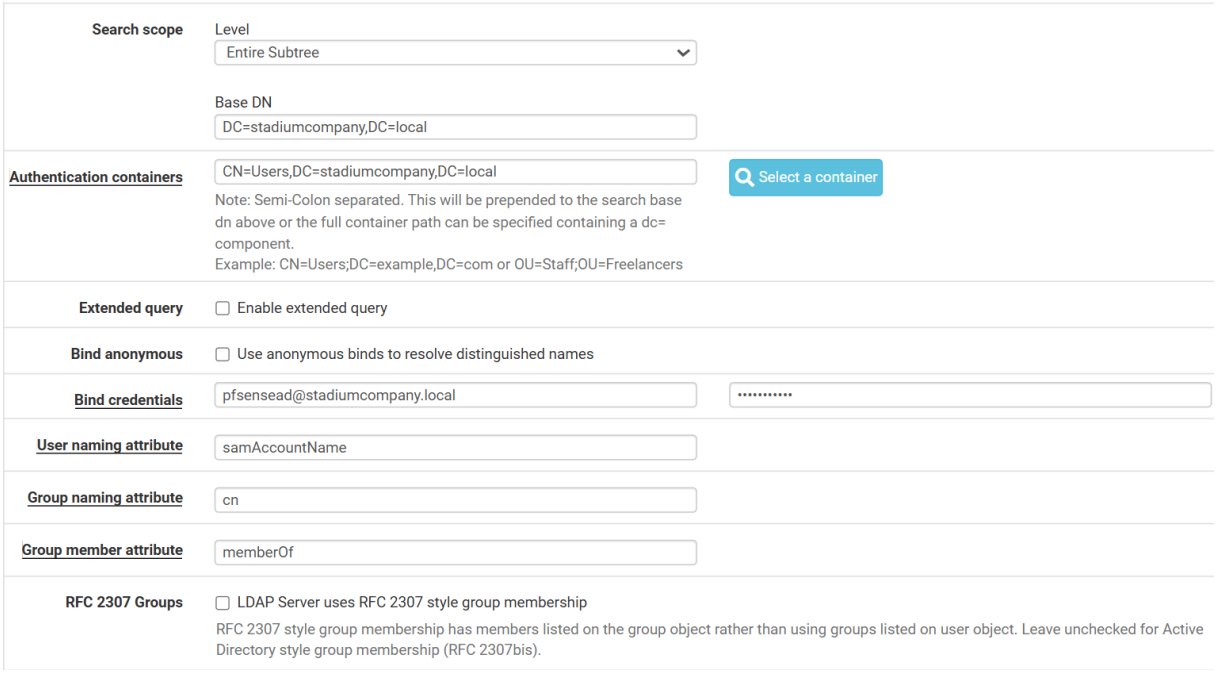
Bind DN (compte de service)

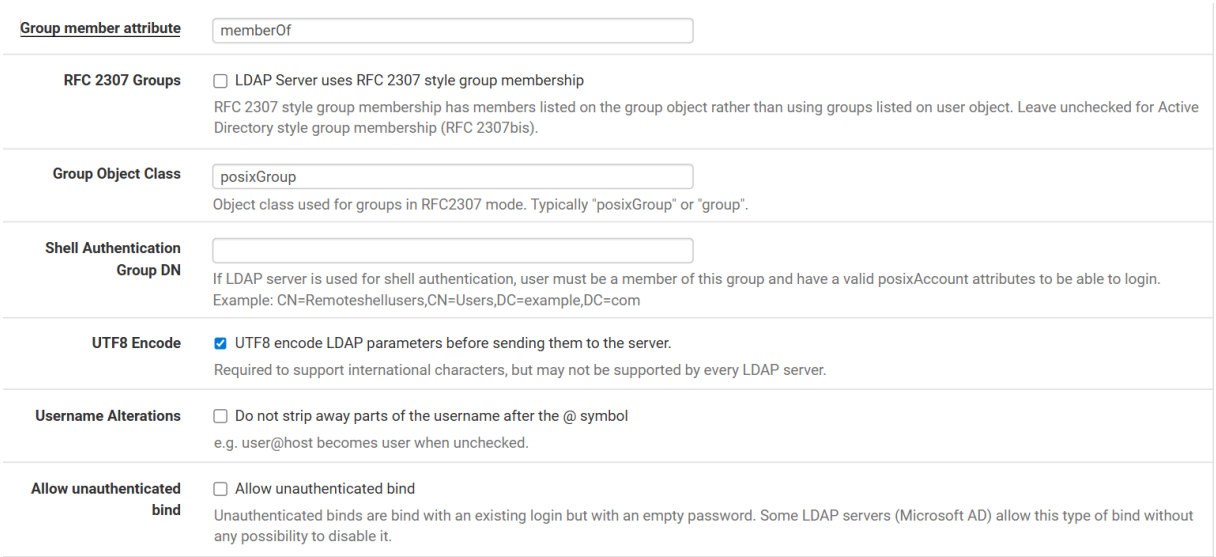
Paramètre	Valeur
Bind credentials	`pfsensead@stadiumcompany.local`
Password	Mot de passe du compte `pfsensead`

Le format **UPN** est recommandé pour Active Directory.

Attributs LDAP

Paramètre	Valeur	Explication
User naming attribute	`sAMAccountName`	Identifiant AD (ex : pcesar)
Group naming attribute	`cn`	Nom du groupe
Group member attribute	`memberOf`	AD utilise memberOf
RFC 2307 Groups	désactivé	AD n'utilise pas RFC2307
UTF8 Encode	activé	Support des accents





Options à désactiver absolument

- ❌ **Allow unauthenticated bind**
- ❌ **Bind anonymous**
- ❌ **Extended query**

🎯 Résultat attendu

Ce backend doit permettre de tester :

- `cesar`
- `kaiser`
- `pfsensead`

Dans **Diagnostics → Authentication**.

9.4 Configuration du backend LDAPS (636)

Ce backend LDAPS est **le backend principal**, utilisé pour :

- Portail captif
- OpenVPN
- Accès WebGUI via AD
- Authentification sécurisée

📌 Accès au menu

pfSense → **System → User Manager → Authentication Servers → Add**

Paramètres LDAPS (636) — Configuration correcte

Identification

- **Descriptive name** : `LDAPS-636-Prod`
- **Type** : `LDAP`

Connexion sécurisée au serveur AD

Paramètre	Valeur
Hostname	`hermes.stadiumcompany.local`
Port	`636`
Transport	`SSL/TLS Encrypted`
Peer Certificate Authority	`Hermes-AD-CA`

Le nom d'hôte doit correspondre au **CN ou SAN** du certificat AD.

Base de recherche

Paramètre	Valeur
Base DN	`DC=stadiumcompany,DC=local`
Authentication containers	`CN=Users,DC=stadiumcompany,DC=local`
Search scope	`Entire Subtree`

Bind DN (compte de service)

Paramètre	Valeur
Bind credentials	`pfsensead@stadiumcompany.local`
Password	Mot de passe du compte `pfsensead`

Attributs LDAP

Paramètre	Valeur
User naming attribute	`sAMAccountName`
Group naming attribute	`cn`
Group member attribute	`memberOf`
RFC 2307 Groups	désactivé
UTF8 Encode	activé

🎯 Résultat attendu

Ce backend LDAPS doit fonctionner pour :

- Portail captif
- OpenVPN
- Accès WebGUI
- Tests d'authentification sécurisés

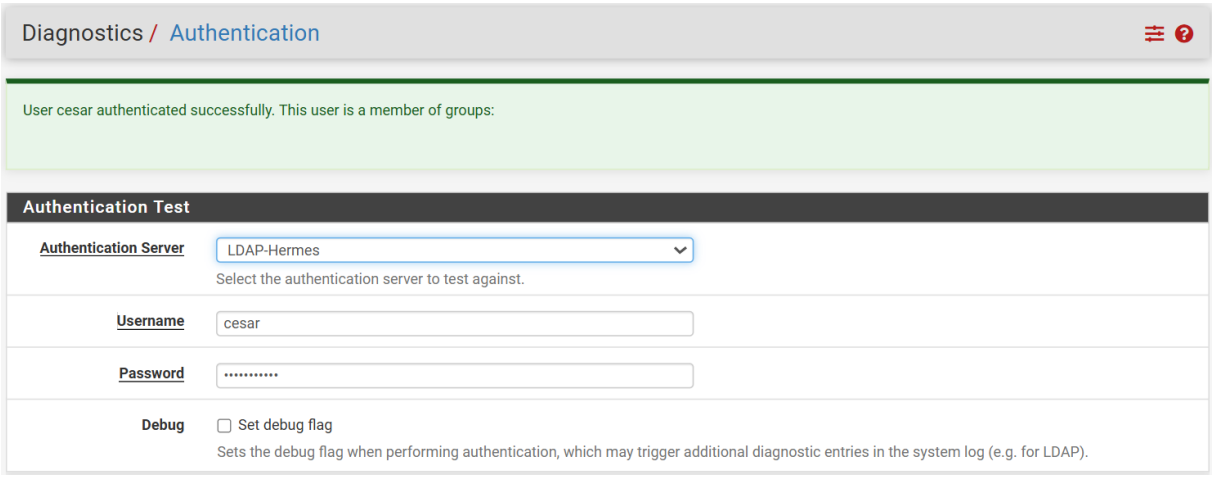
Tests après configuration

Test LDAP (389)

Diagnostics → Authentication

- Backend : `LDAP-389-Test`
- Username : `cesar`
- Password : mot de passe AD

Résultat attendu : `Authentication successful`

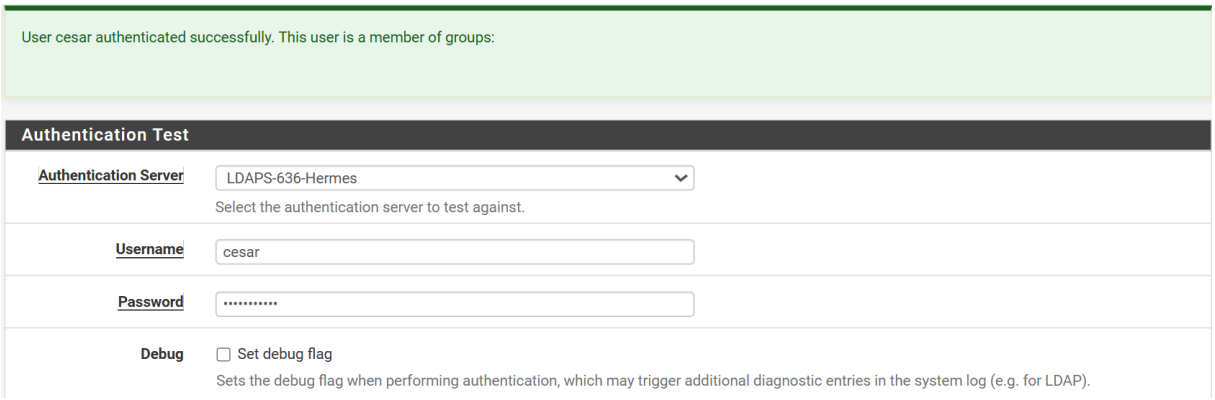


Test LDAPS (636)

Diagnostics → Authentication

- Backend : `LDAPS-636-Hermes`
- Username : `cesar`
- Password : mot de passe AD

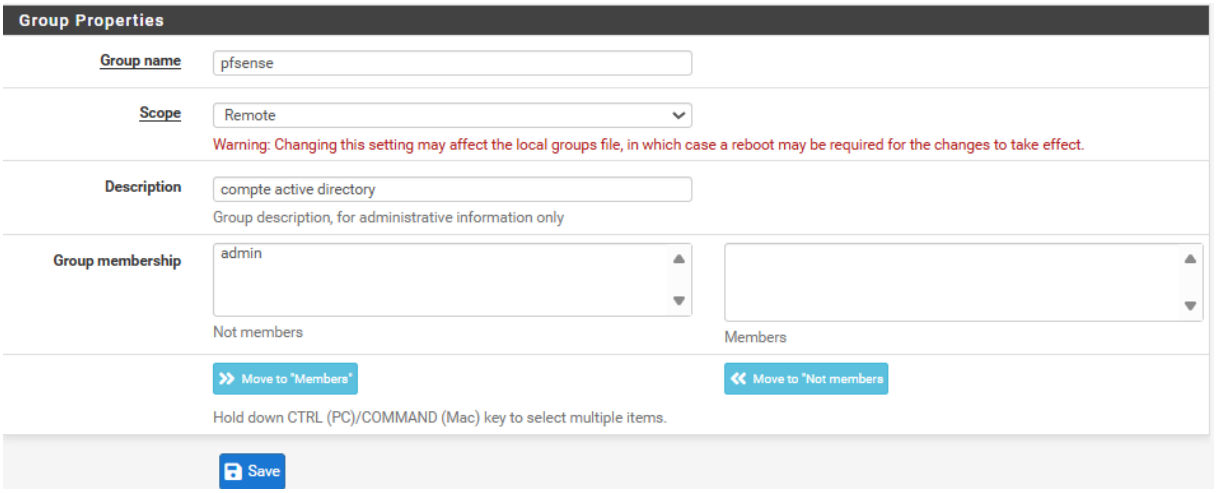
Résultat attendu : `Authentication successful`

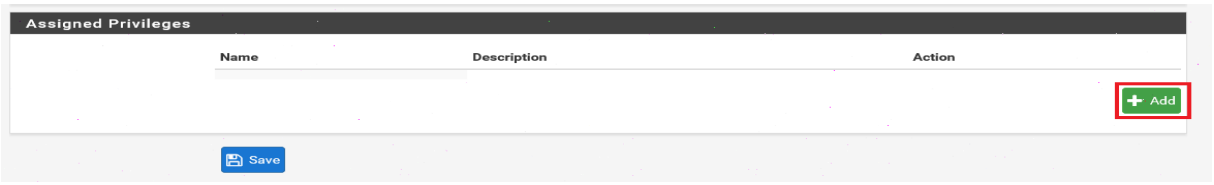


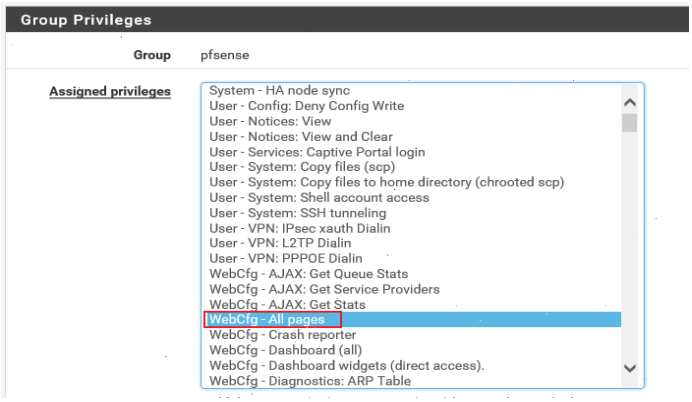
9.6 (Ajout) Donner les droits WebGUI au groupe pfsense

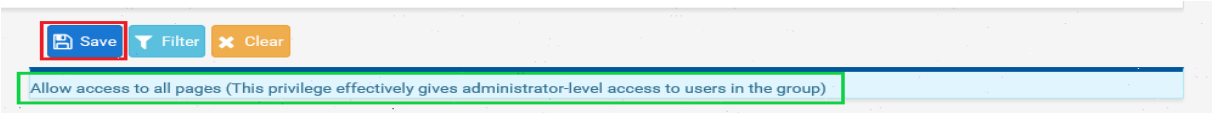
pfSense → System → User Manager → Groups → Add

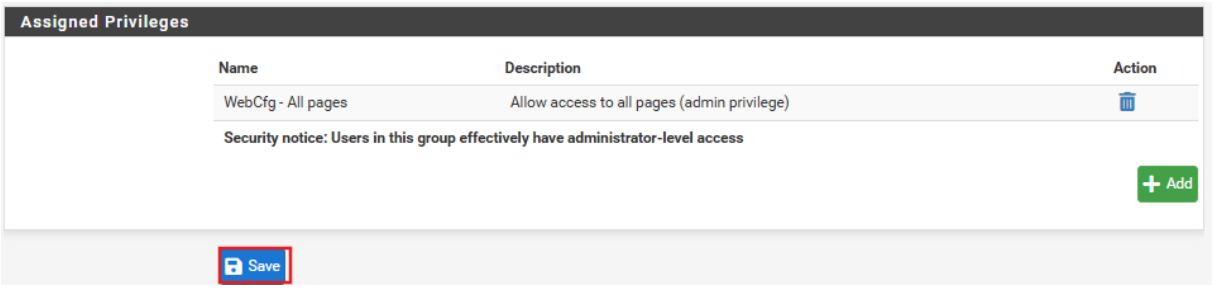
1. Nom : **pfsense**
2. Ajouter le privilège : **WebCfg – All pages**
3. Save





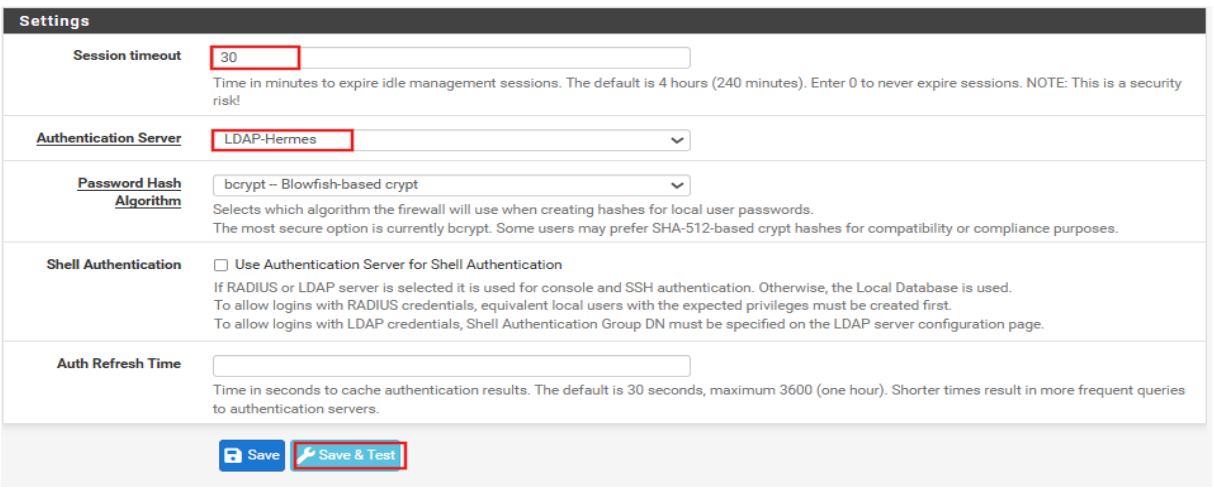




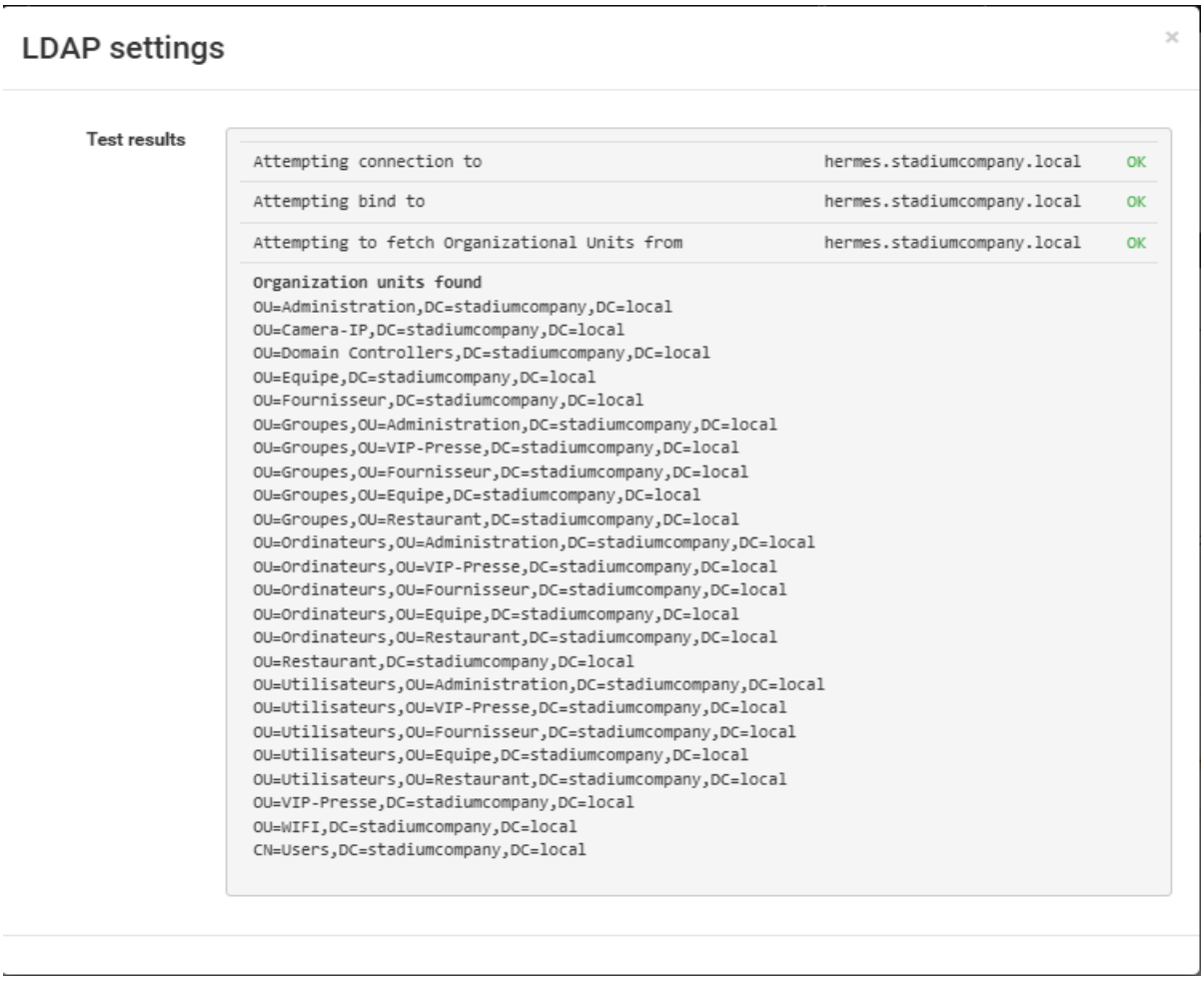


☞ Tous les utilisateurs AD du groupe pfsense pourront se connecter à pfSense.

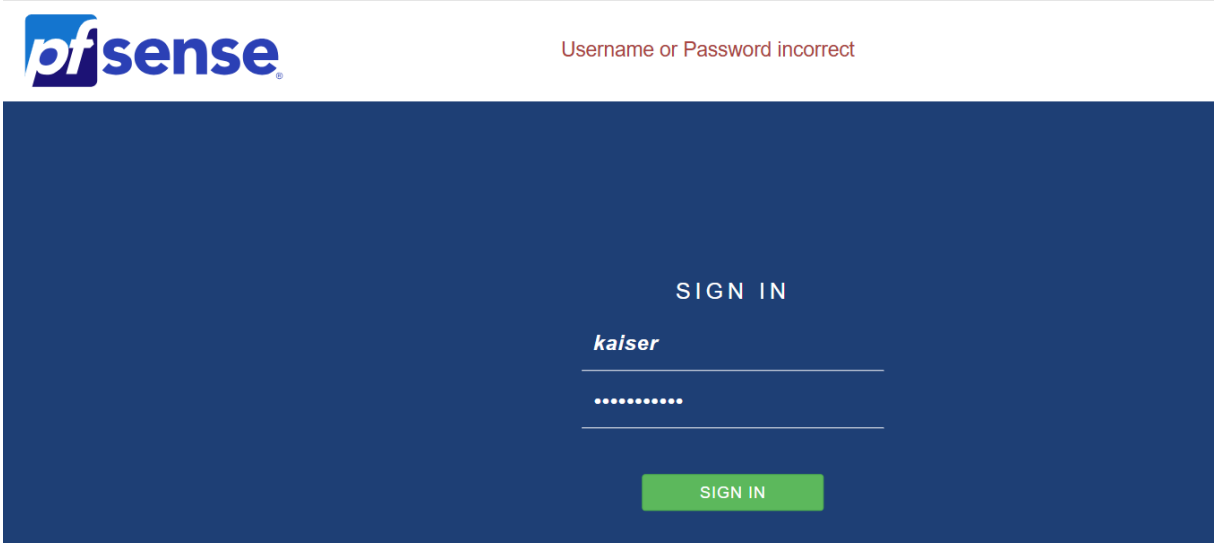
On fait un test de connexion avec la base LDAP



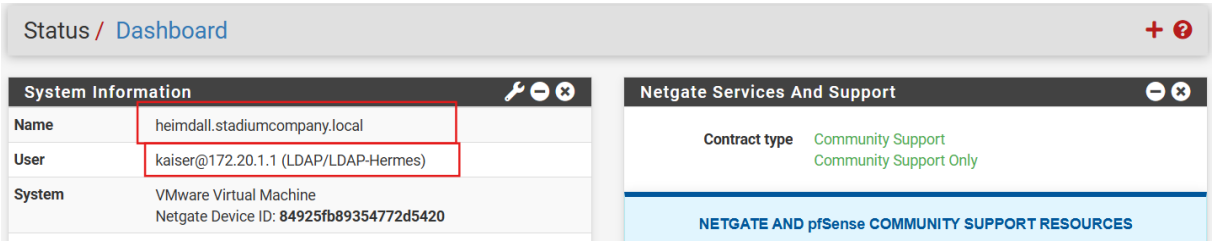
LA connexion a reussi



On teste notre configuration en se connectant avec notre compte **kaiser**



On verifie bien qu'on est connecter avec un compte issue de la base LDAP

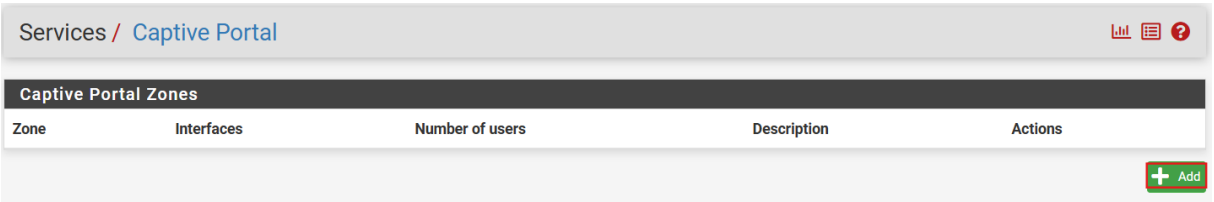


10. Portail Captif (VLAN 30 – WiFi)

Le portail captif permet de contrôler l'accès Internet des utilisateurs du VLAN 30 (WiFi).
Il intercepte les requêtes HTTP/HTTPS et redirige l'utilisateur vers une page d'authentification.
Dans StadiumCompany, l'authentification se fait via **LDAPS**, garantissant un accès sécurisé.

10.1 Activation du portail captif

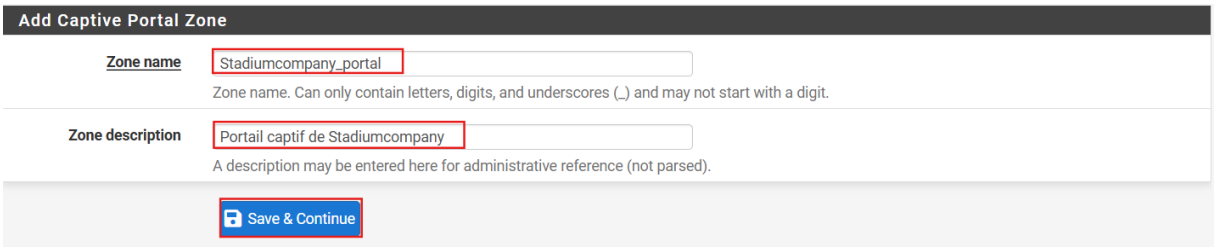
pfSense → **Services → Captive Portal → Add**



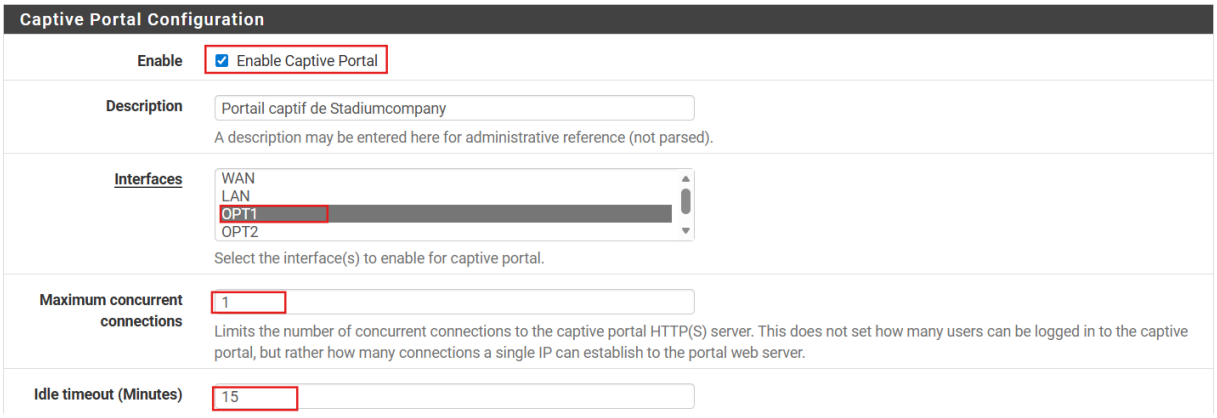
✓ Paramètres essentiels

On va renseigner le Nom du Portail Captif et sa description :
Stadiumcompany_portal pour le nom de la zone
Portail captive Stadiumcompany pour la description de la zone

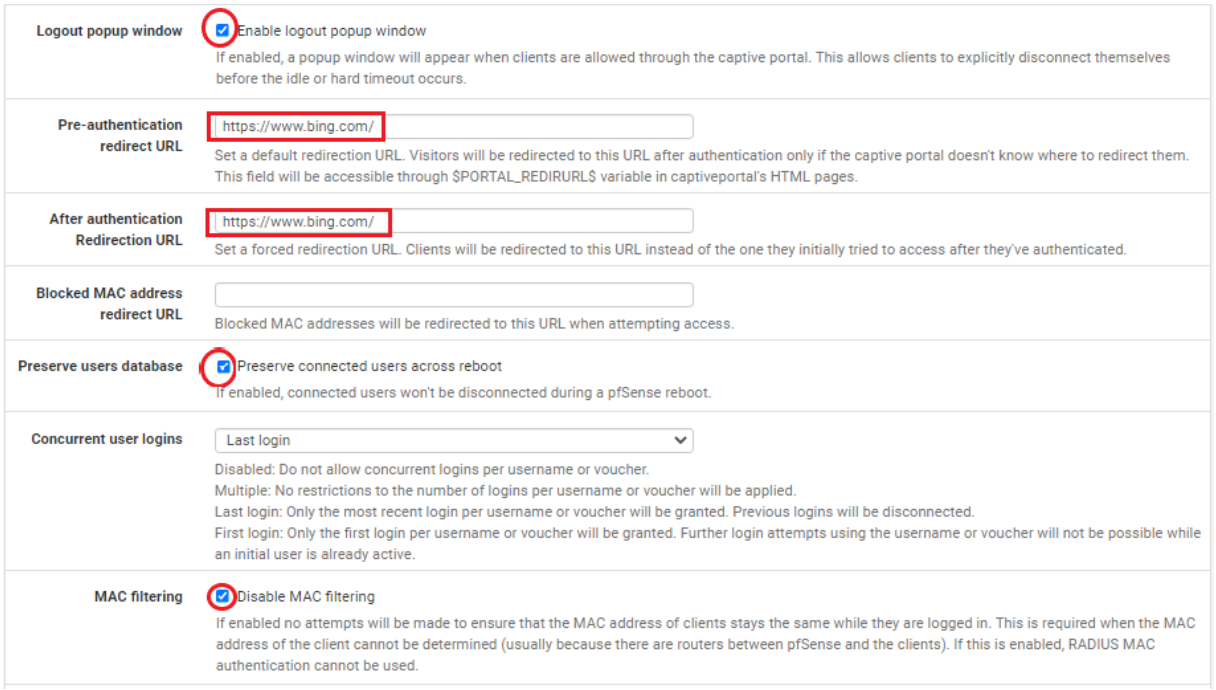
- **Zone name** : Stadiumcompany_portal
- **Zone description :** Portail captif de Stadiumcompany



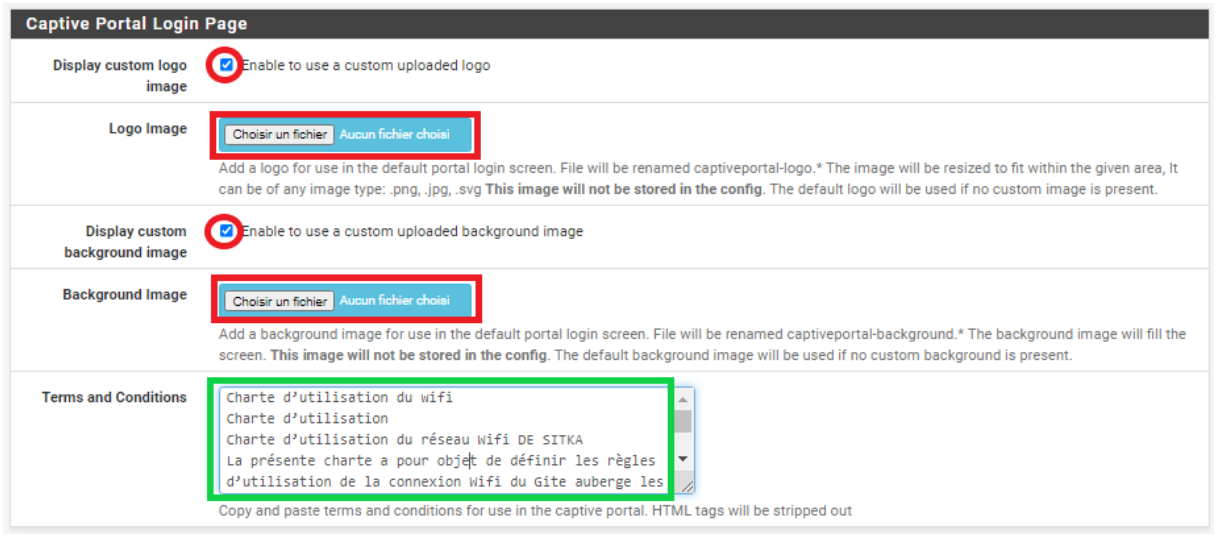
- On active **Enable Captive Portal**
- On sélectionne l'interface **Opt1**
- Maximum concurrent connections : **1** (Limite le nombre de connexions simultanées d'un même utilisateur)
- Idle timeout (Minutes) on choisit **15**:(Les clients seront déconnectés après cette période d'inactivité)



- Définir **After authentication** Redirection URL (URL HTTP de redirection Les clients seront redirigés vers cette URL au lieu de celle à laquelle ils ont tenté d'accéder après s'être authentifiés)
- **Disable concurrent user logins** : activé (seule la connexion la plus récente par nom d'utilisateur sera active)
- **Disable MAC filtering** : activé (lorsque l'adresse MAC du client ne peut pas être déterminée)



- On peut choisir un logo et une image d'arrière-plan ainsi qu'une charte de connexion



→ pfSense utilisera le certificat WebGUI configuré dans la section sécurité

✓ Fonctionnement

1. L'utilisateur se connecte au WiFi
2. Il reçoit une IP via DHCP

3. Toute tentative d'accès Internet est interceptée
4. pfSense affiche la page de login
5. L'utilisateur s'authentifie via LDAPS
6. pfSense ouvre l'accès Internet pour cet utilisateur

10.2 DHCP VLAN 30

pfSense → **Services → DHCP Server → OPT3**

✓ Paramètres DHCP

- **Plage d'adresses** : 172.20.3.10 → 172.20.3.200
- **DNS Server** : 172.20.1.2 (Hermes – DNS AD)
- **Gateway** : 172.20.3.254 (pfSense)
- **Domain name** : stadiumcompany.local

Pourquoi DNS = Hermes ?

→ Le portail captif utilise LDAPS → LDAPS nécessite une résolution DNS correcte → Hermes est le DNS du domaine.

10.3 Règles Firewall

pfSense → **Firewall → Rules → OPT3**

Créer **3 règles indispensables** :

1 Autoriser DNS

- Protocol : UDP/TCP
- Port : 53
- Destination : 172.20.1.2

2 Autoriser HTTPS (pour la page de login)

- Protocol : TCP
- Port : 443
- Destination : OPT3 address

3 Autoriser le portail captif

pfSense ajoute automatiquement une règle interne pour le portail captif.
Elle doit rester **au-dessus** des autres règles.

Après authentification

pfSense ajoute dynamiquement une règle permettant au client d'accéder à Internet.

10.4 Personnalisation de la page

Tu peux modifier les textes dans :

Services → Captive Portal → Edit → Portal Page

Modifier :

- "You are connected" → "Vous êtes connecté"
- "Invalid credentials" → "Informations invalides"
- "Logout" → "Déconnexion"

Personnalisation avancée

Fichier : `/etc/inc/captiveportal.inc`

Tu peux modifier :

- Titre
- Boutons
- Messages d'erreur
- Texte de déconnexion

10.5 Test complet du portail captif

1. Connecter un PC ou smartphone au WiFi VLAN 30
2. Vérifier l'IP : 172.20.3.x
3. Ouvrir un navigateur
4. Vérifier la redirection automatique vers la page de login
5. Se connecter avec un utilisateur AD (ex : kaiser)
6. Vérifier l'accès Internet
7. Vérifier dans pfSense → **Status → Captive Portal** que l'utilisateur apparaît

---

🛡 11. IDS/IPS Snort — Version Premium

Snort protège le réseau en détectant et bloquant les attaques.
Il fonctionne en mode IDS (détection) ou IPS (prévention).

11.1 Installation

pfSense → **System → Package Manager → Available Packages**

Installer : **Snort**

11.2 Configuration globale

Snort → **Global Settings**

Activer :

- **Enable Snort VRT** (règles Snort officielles)
- **Enable ET Open** (règles Emerging Threats)
- **Hide deprecated rules**
- **Keep Snort settings after uninstall**
- **Startup/Shutdown logging**

Update interval : **1 day**

11.3 Activation sur l'interface WAN

Snort → **Interfaces → Add → WAN**

✓ Paramètres essentiels

- **Enable** : activé
- **Block offenders** : activé
- **IPS Mode** : Enabled
- **Policy** : Balanced
- **Resolve Flowbits** : activé

Pourquoi Balanced ?

- Bon compromis entre sécurité et faux positifs
- Recommandé pour les environnements professionnels

11.4 Test d'intrusion

Depuis une machine externe :

```
nmap 172.20.1.254
```

Snort doit :

- détecter le scan
- générer une alerte
- bloquer l'IP source

Vérifier dans :

- Snort → Alerts
- Snort → Blocked

---

12. VPN OpenVPN

OpenVPN permet un accès distant sécurisé au réseau StadiumCompany.

12.1 CA & Certificat serveur

pfSense → **VPN → OpenVPN → Wizards**

1. Sélectionner la CA interne
2. Générer un certificat serveur OpenVPN

12.2 Configuration du serveur OpenVPN

✓ Paramètres essentiels

- **Mode** : Remote Access (User Auth)
- **Backend** : LDAPS
- **Port** : 1919/UDP
- **Tunnel Network** : 10.10.10.0/24
- **Local Networks** :
  - 172.20.1.0/24
  - 172.20.2.0/24
  - 172.20.3.0/24
  - 172.20.4.0/24
- **Topology** : net30
- **Dynamic IP** : activé

- **DNS Server** : 172.20.1.2
- **Domain** : stadiumcompany.local
- **Custom option** : `auth-nocache`

Pourquoi net30 ?

→ Chaque client reçoit un sous-réseau isolé → meilleure sécurité.

12.3 Règles Firewall

WAN

Autoriser :

- Protocol : UDP
- Port : 1919
- Destination : WAN address

OpenVPN

Autoriser :

- Tout trafic vers les VLAN internes
- Ou règles spécifiques selon les besoins

12.4 Export client

Installer : **openvpn-client-export**

pfSense → **VPN → OpenVPN → Client Export**

Télécharger :

- Installateur Windows
- Profil Android

12.5 Tests VPN

Windows

- Connexion

- Vérification IP : 10.10.10.x
- Ping Hermes
- Ping VLAN 1/2/3/4

Android

- Import du profil
- Connexion 4G
- Ping Hermes

---

13. Validation finale — Version Premium

13.1 Tests réseau

```
ping 172.20.1.254
ping 172.20.2.254
ping 172.20.3.254
ping 172.20.4.254
```

13.2 Tests Active Directory

- LDAP : OK
- LDAPS : OK
- Authentification AD dans pfSense : OK
- Portail captif avec utilisateur AD : OK

13.3 Tests sécurité

- SSH sur port 2121 : OK
- HTTPS avec certificat interne : OK
- Snort IPS : OK (détection + blocage)

13.4 Tests VPN

- Connexion Windows : OK
- Connexion Android : OK
- Accès aux VLAN : OK
- Ping Hermes : OK