

PRINCE TOGGLE

REALISATION

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

 **sense**®

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

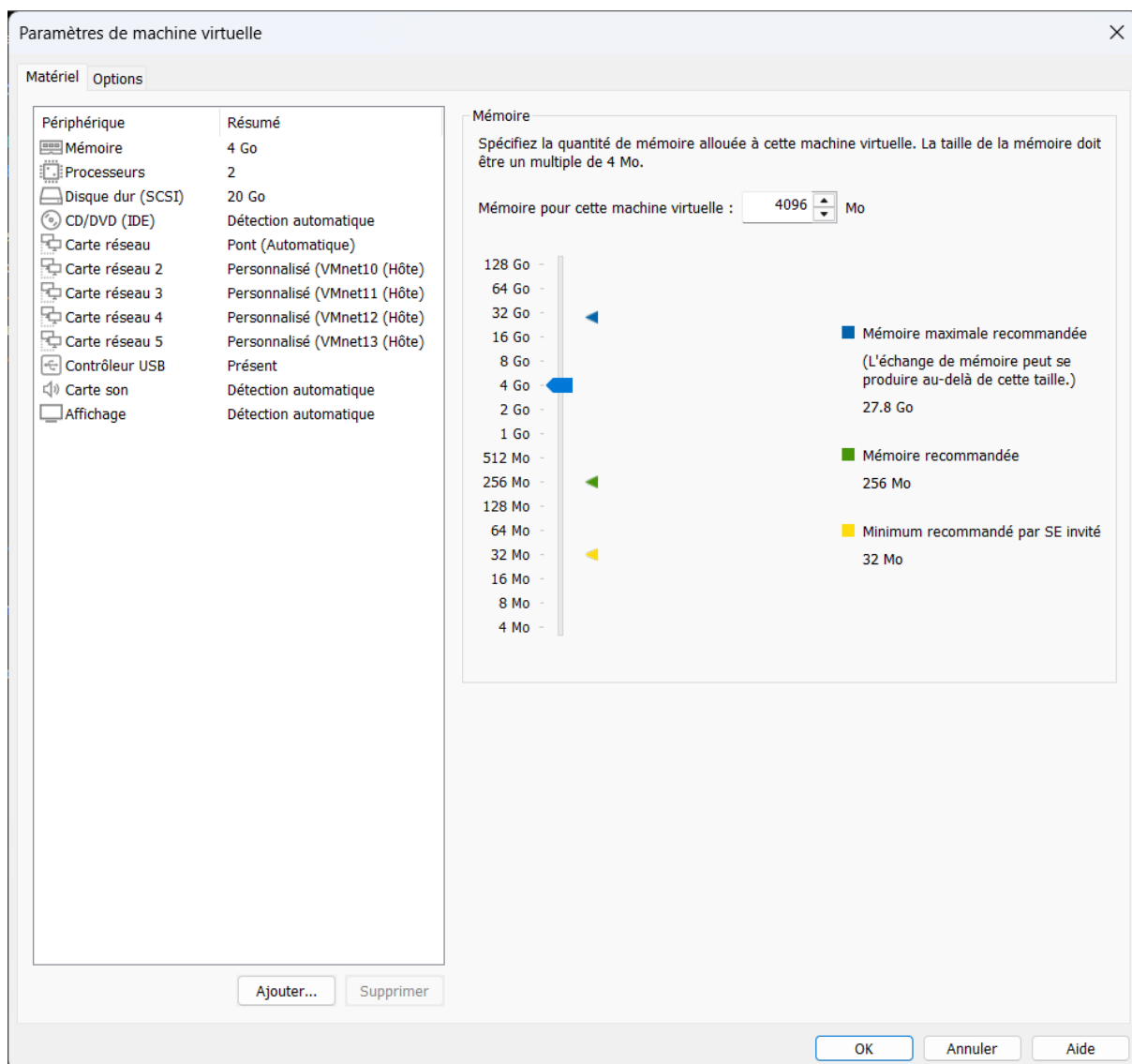
2.2 pfSense (Heimdall)

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**

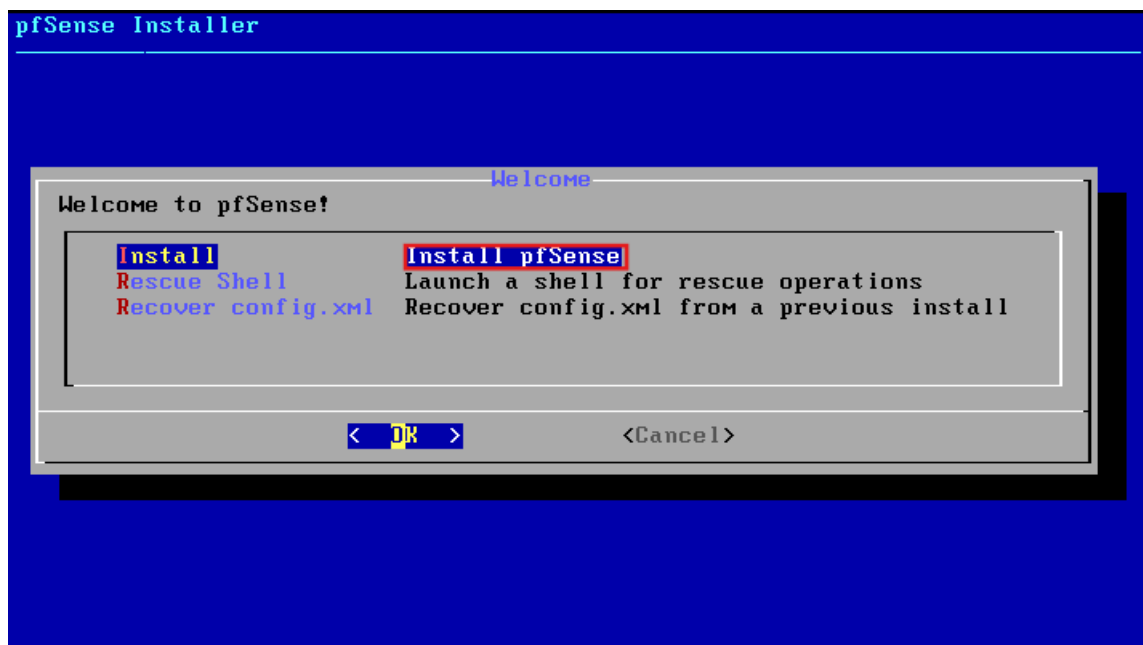


3.2 Configuration réseau (5 interfaces)

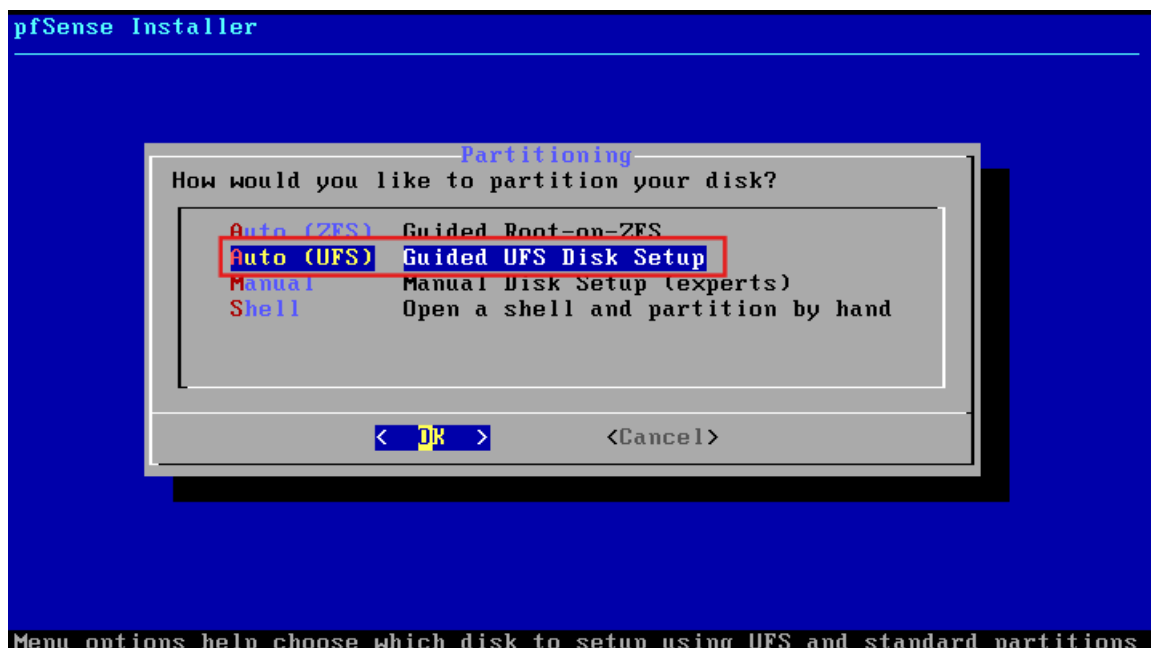
Interface VM	Rôle	VMware Network
NIC1	WAN	Bridge
NIC2	VLAN 10	VMnet10
NIC3	VLAN 20	VMnet11
NIC4	VLAN 30	VMnet12
NIC5	VLAN 40	VMnet13

4. Installation pfSense (ISO)

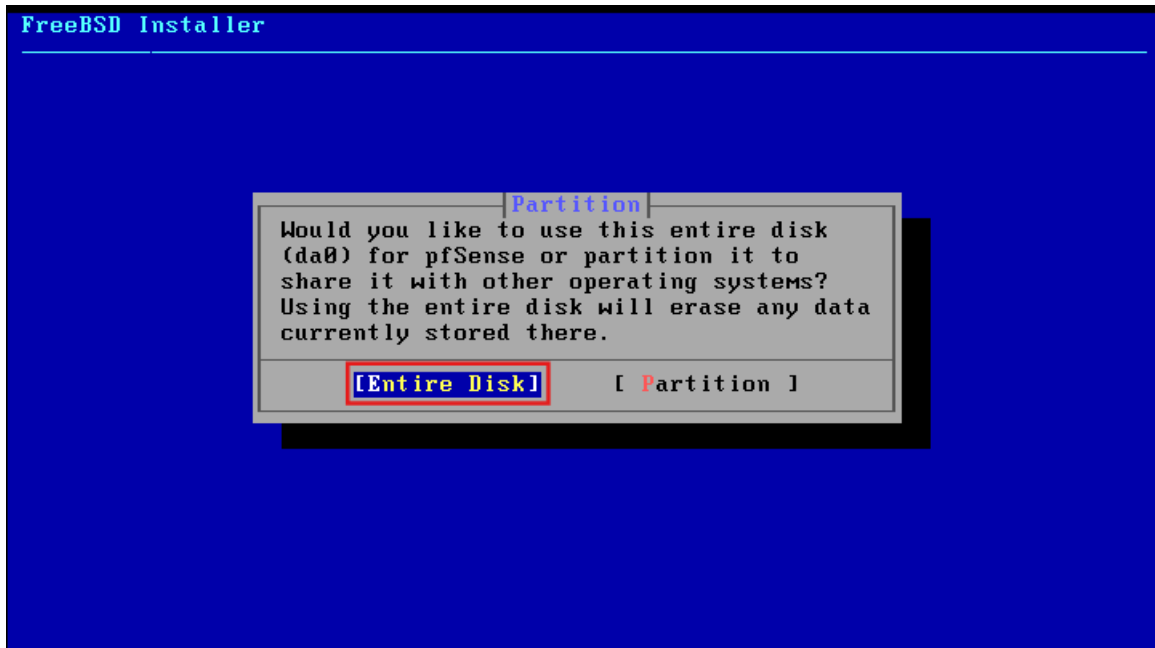
1. Monter l'ISO
2. Boot → Entrée
3. Install



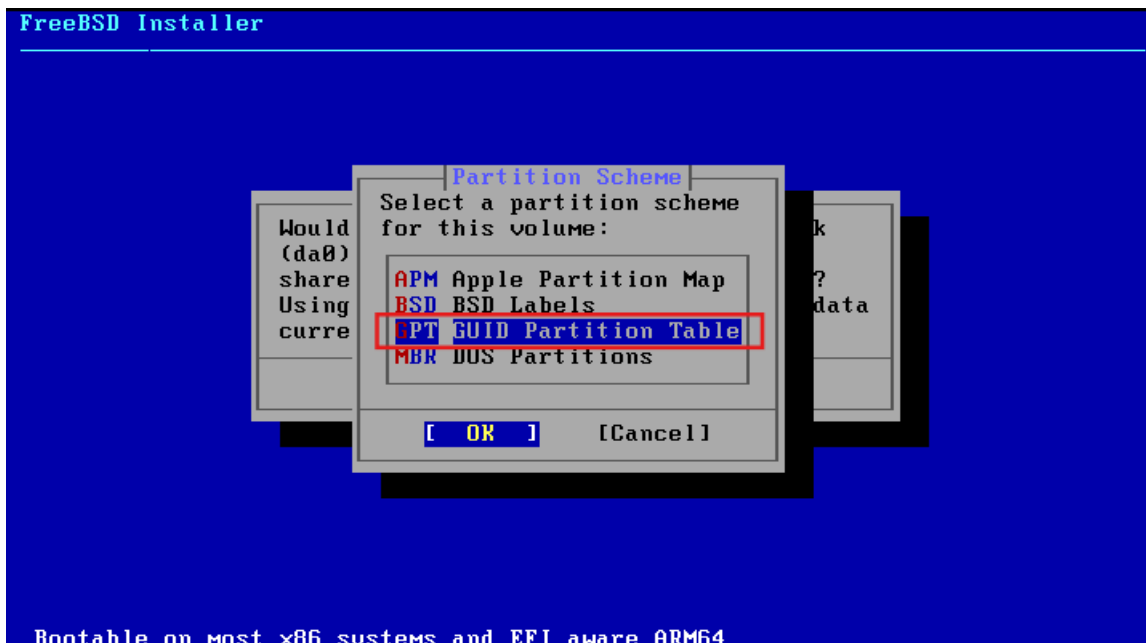
4. Clavier : **French**
5. Partitionnement : **Auto (UFS)**



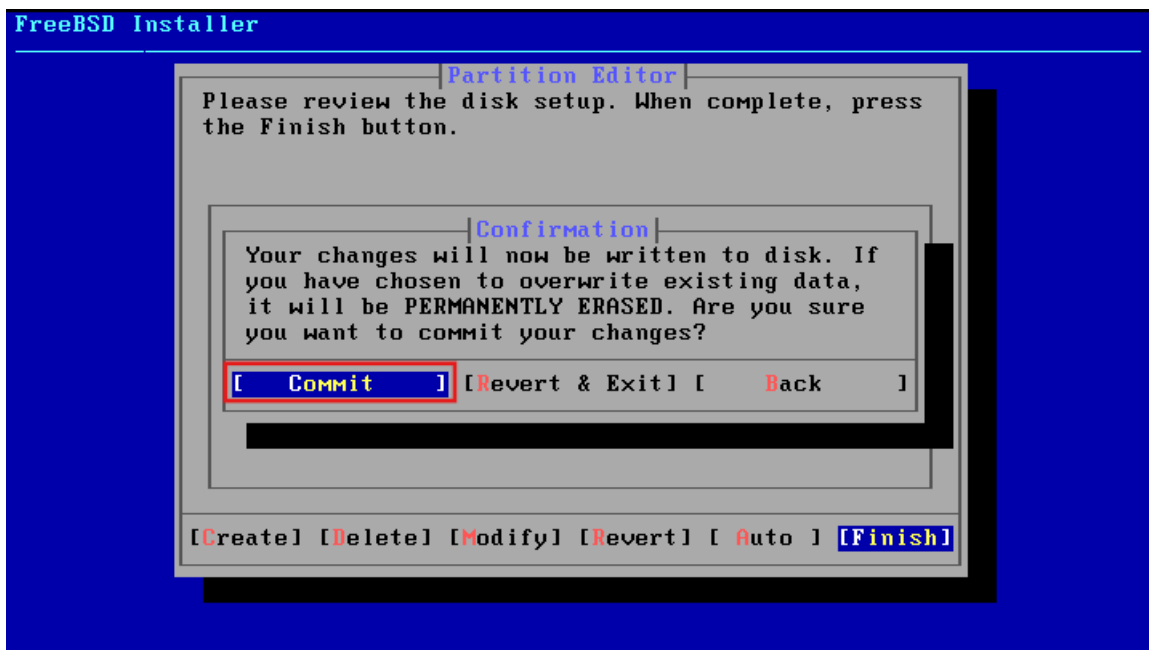
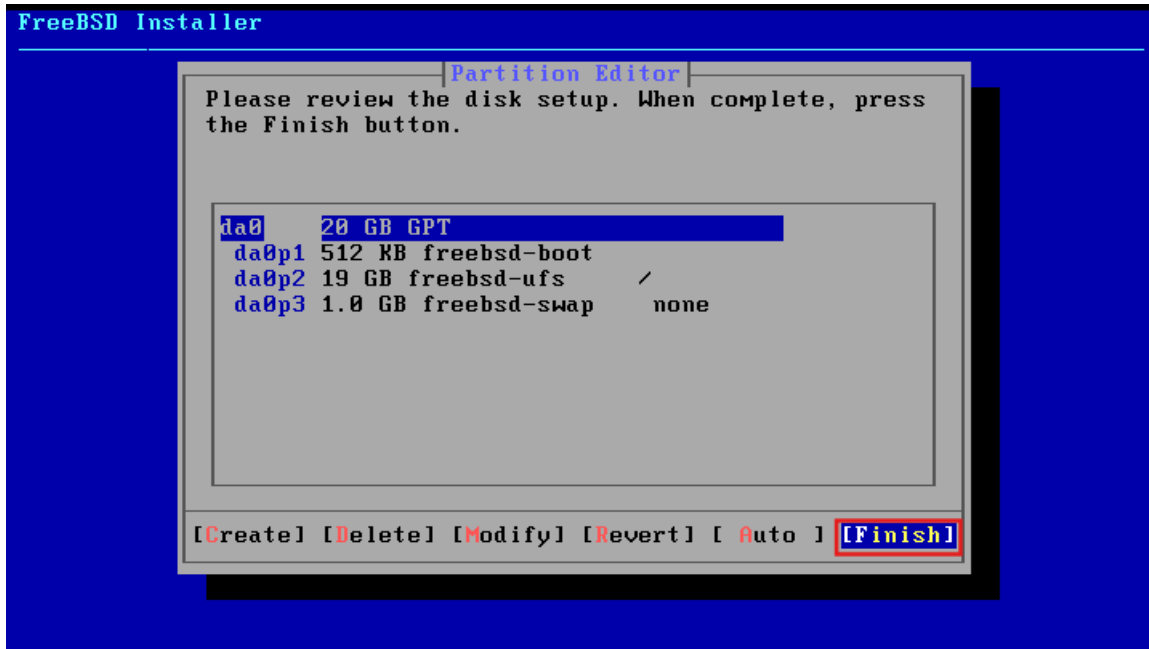
6. Disque entier



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 Assignment 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 DHCP? (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
```

```

Enter the number of the interface you wish to configure: 2
Configure IPv4 address LAN interface via DHCP? (y/n) n
Enter the new LAN IPv4 address. Press <ENTER> for none:
> 172.20.1.254
Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0    = 8
Enter the new LAN IPv4 subnet bit count (1 to 32):
> 24
For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>
Configure IPv6 address LAN interface via DHCP6? (y/n) n
Enter the new LAN IPv6 address. Press <ENTER> for none:
>
Do you want to enable the DHCP server on LAN? (y/n) n

```

→ 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)

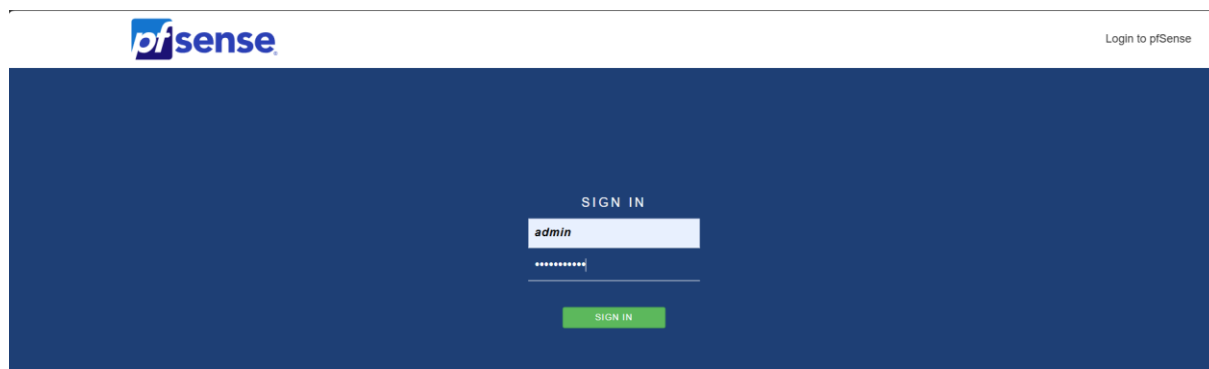
6.1 Accès Web

Depuis un poste du VLAN 10 :

<https://172.20.1.254>

Identifiants :

- admin
- pfsense



pfSense

Login to pfSense




SIGN IN

admin

SIGN IN

6.2 Wizard (9 étapes)

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

System			
Hostname	<input type="text" value="heimdall"/>	Name of the firewall host, without domain part.	
Domain	<input type="text" value="stadiumcompany.local"/>	Domain name for the firewall.	
Do not end the domain name with '.local' as the final part (Top Level Domain, TLD). The 'local' TLD is widely used by mDNS (e.g. Avahi, Bonjour, Rendezvous, Airprint, Airplay) and some Windows systems and networked devices. These will not network correctly if the router uses 'local' as its TLD. Alternatives such as 'home.arpa', 'local.lan', or 'mylocal' are safe.			
DNS Server Settings			
DNS Servers	<input type="text" value="172.20.1.2"/>	<input type="text" value="DNS Hostname"/>	 Delete
	<input type="text" value="172.20.1.3"/>	<input type="text" value="DNS Hostname"/>	 Delete
	<input type="text" value="172.20.1.4"/>	<input type="text" value="DNS Hostname"/>	 Delete
	Address Enter IP addresses to be used by the system for DNS	Hostname Enter the DNS Server Hostname for TLS Verification in	

- 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

System / Package Manager / Available Packages

Installed Packages Available Packages

Search

Search term: Both

Enter a search string or *nix regular expression to search package names and descriptions.

Packages

Name	Version	Description
Shellcmd	1.0.5.3	The shellcmd utility is used to manage commands on system startup.

Search

Search term: Both

Enter a search string or *nix regular expression to search package names and descriptions.

Packages

Name	Version	Description
Open-VM-Tools	10.1.0.5.1	VMware Tools is a suite of utilities that enhances the performance of the virtual machine's guest operating system and improves management of the virtual machine.

Package Dependencies:
[open-vm-tools-12.3.5.2](#)

Puis :

Services → Shellcmd → Add

Command : kbdcontrol -l fr
 Type : earlyshellcmd

Shellcmd Configuration

Command
 Enter the command to run.

Shellcmd Type
 Choose the shellcmd type. Click Info for details. ⓘ

- shellcmd** Will run the command specified towards the end of the boot process.
- earlyshellcmd** Will run the command specified at the beginning of the boot process.
- afterfilterchangeshellc...** Will run after each `filter_configure()` call. See `/etc/inc/filter.inc` source code for "documentation".
Note: Only one entry of this type can be configured!
- disabled** Will save the command in package configuration but it will NOT run on boot.

See Executing commands at boot time for detailed explanation.

Description
 Enter a description for this command. (This is for your reference only.)

Save.

7. Tests de connectivité

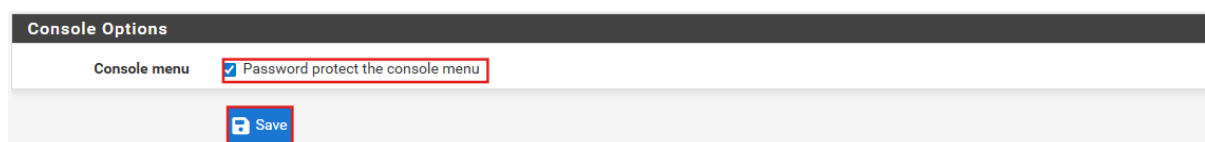
Depuis Hermes :

```
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.

Secure Shell	
Secure Shell Server	<input checked="" type="checkbox"/> Enable Secure Shell
SSHD Key Only	Password or Public Key <input type="text"/> <small>When set to <i>Public Key Only</i>, SSH access requires authorized keys and these keys must be configured for each <i>user</i> that has been granted secure shell access. If set to <i>Require Both Password and Public Key</i>, the SSH daemon requires both authorized keys and valid passwords to gain access. The default <i>Password or Public Key</i> setting allows either a valid password or a valid authorized key to login.</small>
Allow Agent Forwarding	<input type="checkbox"/> Enables ssh-agent forwarding support.
SSH port	<input type="text" value="2121"/> <small>Note: Leave this blank for the default of 22.</small>

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

Edit Firewall Rule

Action	<input style="width: 90%;" type="text" value="Pass"/>	Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.
Disabled	<input type="checkbox"/> Disable this rule Set this option to disable this rule without removing it from the list.	
Interface	<input style="width: 90%;" type="text" value="WAN"/>	Choose the interface from which packets must come to match this rule.
Address Family	<input style="width: 90%;" type="text" value="IPv4"/>	Select the Internet Protocol version this rule applies to.
Protocol	<input style="width: 90%;" type="text" value="TCP"/>	Choose which IP protocol this rule should match.

Source

Source	<input type="checkbox"/> Invert match	<input style="width: 90%;" type="text" value="Any"/>	<input style="width: 90%;" type="text" value="Source Address"/> / <input style="width: 90%;" type="text"/>
<input type="button" value="Display Advanced"/>			
The Source Port Range for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any .			

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

✓ Description

Allow SSH on port 2121

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

Destination

Destination	<input type="checkbox"/> Invert match	<input style="width: 90%;" type="text" value="WAN address"/>	<input style="width: 90%;" type="text" value="Destination Address"/> / <input style="width: 90%;" type="text"/>
Destination Port Range	<input style="width: 90%;" type="text" value="(other)"/>	<input style="width: 90%;" type="text" value="2121"/>	<input style="width: 90%;" type="text" value="(other)"/>
	From	Custom	To
			Custom
Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.			

Extra Options

Log	<input type="checkbox"/> Log packets that are handled by this rule Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).	
Description	<input style="width: 90%;" type="text" value="Allow SSH on port 2121"/>	A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.
Advanced Options	<input type="button" value="Display Advanced"/>	
<input style="width: 50px; height: 20px;" type="button" value="Save"/>		

☞ 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
```

```
PS C:\Users\Administrateur> ssh admin@172.20.1.254 -p 2121
Password for admin@heimdall.stadiumcompany.local:
VMware Virtual Machine - Netgate Device ID: 84925fb89354772d5420
*** 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

Enter an option: _
```

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. Cliquez sur l'onglet **Authorities**
4. Cliquez sur **Add**

✓ Remplis les champs comme suit :

Informations générales

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

Create / Edit CA	
Descriptive name	<input type="text" value="StadiumCompany-CA"/>
	<small>The name of this entry as displayed in the GUI for reference. This name can contain spaces but it cannot contain any of the following characters: ?, >, <, &, /, \, " , ' ,</small>
Method	<input type="text" value="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)


Internal Certificate Authority	
Key type	<input type="text" value="RSA"/>
	<small>The length to use when generating a new RSA key, in bits. The Key Length should not be lower than 2048 or some platforms may consider the certificate invalid.</small>
Digest Algorithm	<input type="text" value="sha256"/>
	<small>The digest method used when the CA is signed. The best practice is to use SHA256 or higher. Some services and platforms, such as the GUI web server and OpenVPN, consider weaker digest algorithms invalid.</small>
Lifetime (days)	<input type="text" value="3650"/>
Common Name	<input type="text" value="StadiumCompany-RootCA"/>

Informations du certificat

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

5. Cliquez sur **Save**

Country Code	FR
State or Province	Île de France
City	Massy
Organization	StadiumCompany
Organizational Unit	e.g. My Department Name (optional)

 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

Add/Sign a New Certificate	
Method	Create an internal Certificate
Descriptive name	pfSense-WebGUI
	<small>The name of this entry as displayed in the GUI for reference. This name can contain spaces but it cannot contain any of the following characters: ?, >, <, &, /, \, ", '.</small>
Internal Certificate	
Certificate authority	StadiumCompany-CA

Paramètres cryptographiques

- **Key Type :** RSA

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

Internal Certificate	
Certificate authority	StadiumCompany-CA
Key type	RSA
	2048 The length to use when generating a new RSA key, in bits. The Key Length should not be lower than 2048 or some platforms may consider the certificate invalid.
Digest Algorithm	sha256 The digest method used when the certificate is signed. The best practice is to use SHA256 or higher. Some services and platforms, such as the GUI web server and OpenVPN, consider weaker digest algorithms invalid.
Lifetime (days)	3650 The length of time the signed certificate will be valid, in days. Server certificates should not have a lifetime over 398 days or some platforms may consider the certificate invalid.

Informations du certificat

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

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**

Certificate Type	Server Certificate		
	Add type-specific usage attributes to the signed certificate. Used for placing usage restrictions on, or granting abilities		
Alternative Names	FQDN or Hostname	heimdall	Delete
	FQDN or Hostname	heimdall.stadiumcompany.local	Delete
	IP address	172.20.1.254	Delete
	Type	Value	
Add SAN Row	+ Add SAN Row		
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)

webConfigurator	
Protocol	<input type="radio"/> HTTP <input checked="" type="radio"/> HTTPS (SSL/TLS)
SSL/TLS Certificate	<input type="text" value="pfSense-WebGUI"/> <small>Certificates known to be incompatible with use for HTTPS are not included in this list, such as certificates using incompatible ECDSA curves or weak digest algorithms.</small>
TCP port	<input type="text" value="443"/> <small>Enter a custom port number for the webConfigurator above to override the default (80 for HTTP, 443 for HTTPS). Changes will take effect immediately after save.</small>

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

WebGUI redirect	<input checked="" type="checkbox"/> Disable webConfigurator redirect rule <small>When this is unchecked, access to the webConfigurator is always permitted ever to disable this automatically added redirect rule.</small>
------------------------	--

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 :

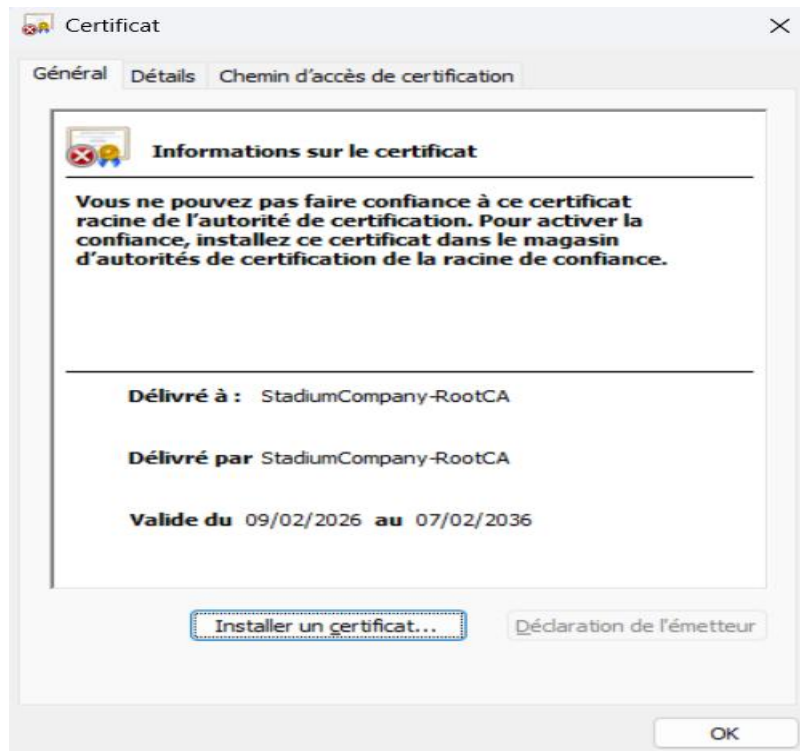
- un cadenas (si tu installes la CA sur ton PC)
- le certificat signé par **StadiumCompany-CA**
- plus aucun accès en HTTP

Pour éviter l'avertissement du navigateur :

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

Certificate Authorities						
Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
StadiumCompany-CA	✓	self-signed	1	ST=ile de France, O=StadiumCompany, L=Massy, CN=StadiumCompany-RootCA, C=FR ⓘ Valid From: Mon, 09 Feb 2026 12:26:36 +0100 Valid Until: Thu, 07 Feb 2036 12:26:36 +0100		   

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.

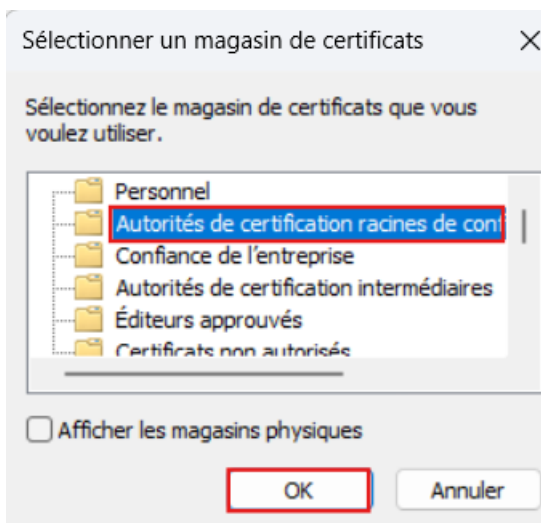
Suivant

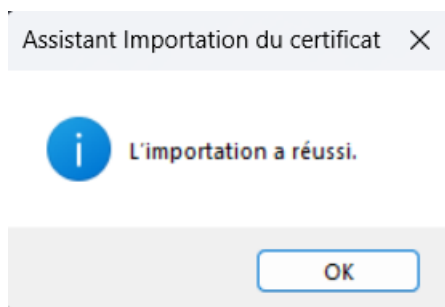
Annuler

Placer tous les certificats dans le magasin suivant

Magasin de certificats :

Parcourir...





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**

Nouvel objet - Utilisateur

Créer dans : stadiumcompany.local/Users

Prénom : pfsensead Initiales :

Nom :

Nom complet : pfsensead

Nom d'ouverture de session de l'utilisateur :
 @stadiumcompany.local

Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000) :

< Précédent **Suivant >** Annuler

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**

Nouvel objet - Utilisateur

Créer dans : stadiumcompany.local/Users

Prénom : Initiales :

Nom :

Nom complet :

Nom d'ouverture de session de l'utilisateur : @stadiumcompany.local

Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000) :

< Précédent **Suivant >** Annuler

- User : **cesar**

Nouvel objet - Utilisateur

Créer dans : stadiumcompany.local/Users

Prénom : Initiales :

Nom :

Nom complet :

Nom d'ouverture de session de l'utilisateur : @stadiumcompany.local

Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000) :

< Précédent **Suivant >** Annuler

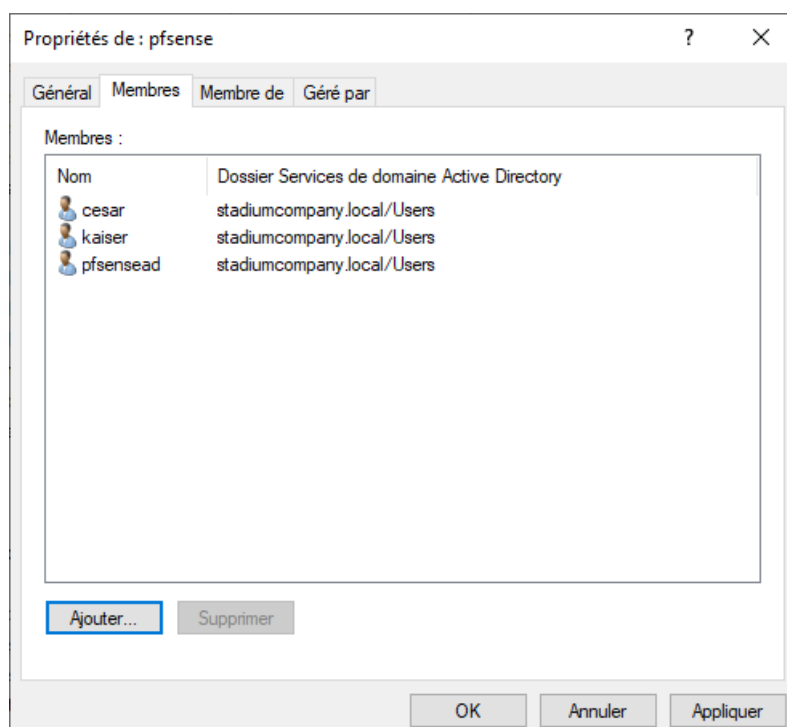
4. Mot de passe simple
5. Décocher "User must change password"
6. Ajouter ces utilisateurs au groupe **pfSense**

✓ 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

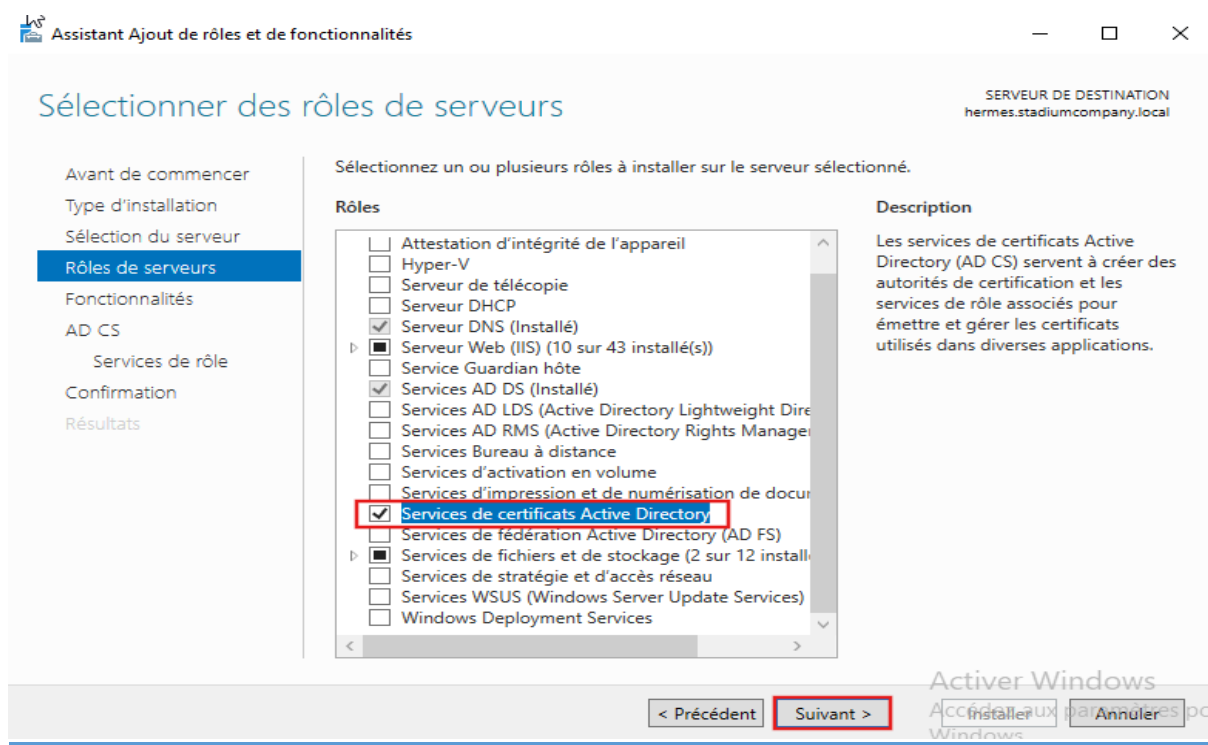
Élément	Statut	Commentaire
Groupe pfsense	✓ Créé	Groupe de sécurité global
Utilisateur pfsensead	✓ Créé	Compte de service (Bind DN)
Utilisateur kaiser	✓ Créé	Compte test
Utilisateur cesar	✓ Créé	Compte test
Tous membres du groupe pfsense	✓ OK	Prêt pour LDAP/LDAPS

9.1 Préparation côté Active Directory (Hermes)

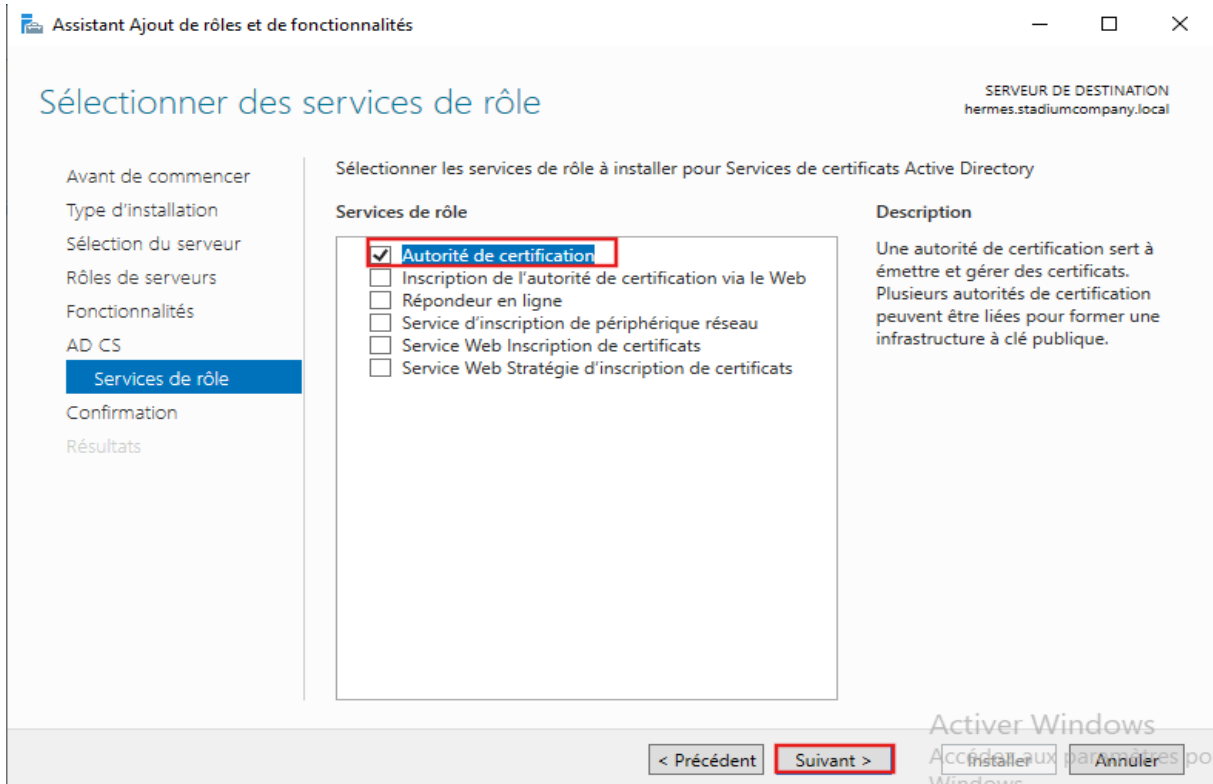
Sur ton serveur **Hermes** (Windows Server) :

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

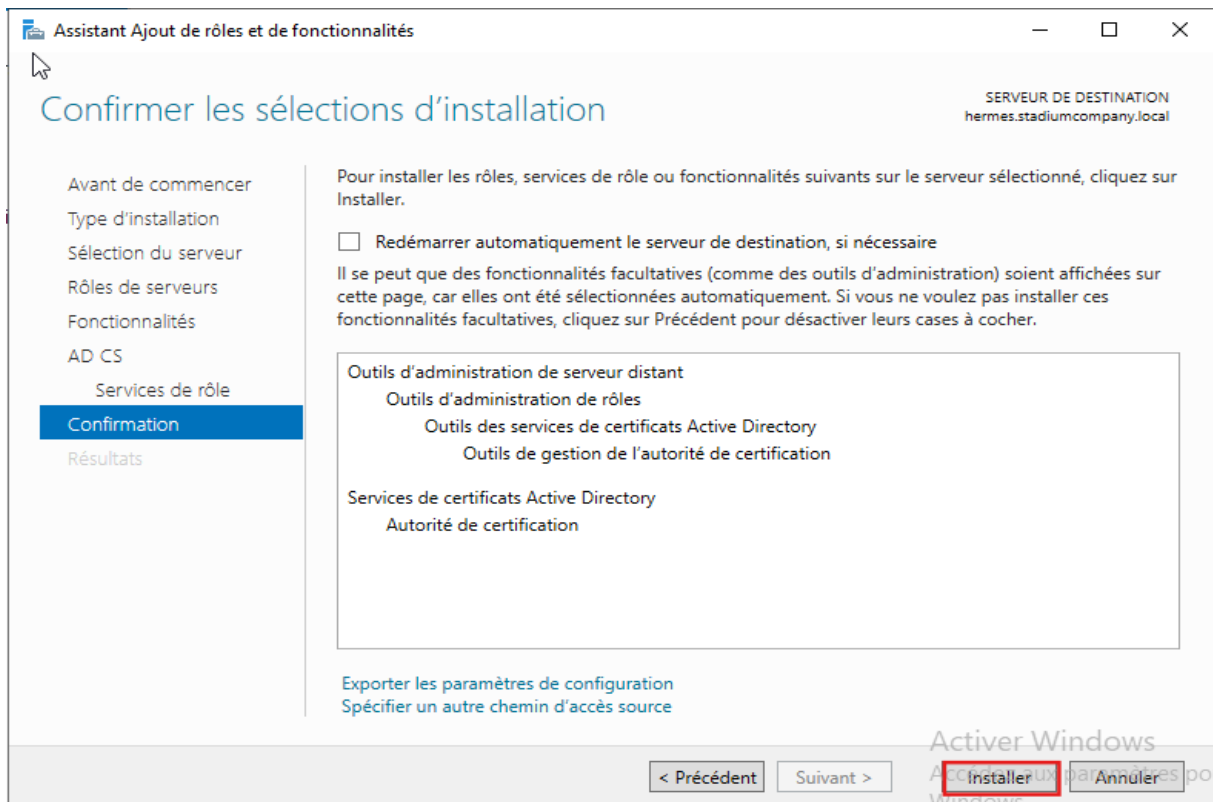
1. Ouvre **Server Manager**
2. Add Roles and Features
3. Active Directory Certificate Services



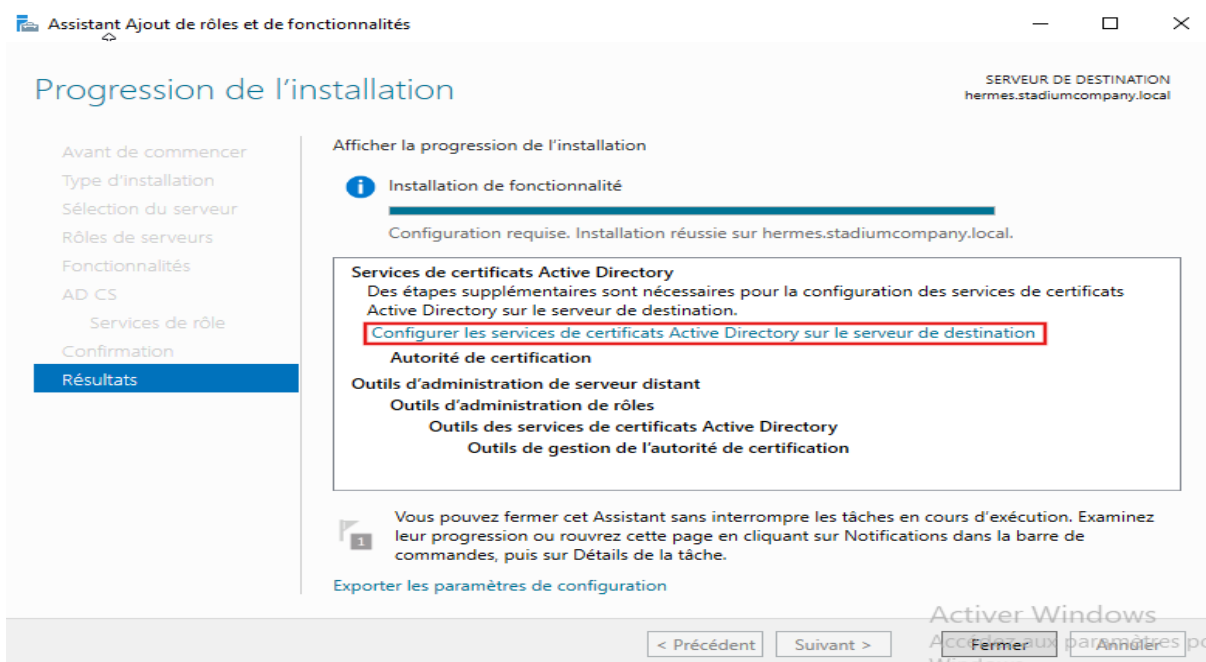
4. Sélectionne :
- Certification Authority



5. Installe



6. Configure la CA en Enterprise Root CA



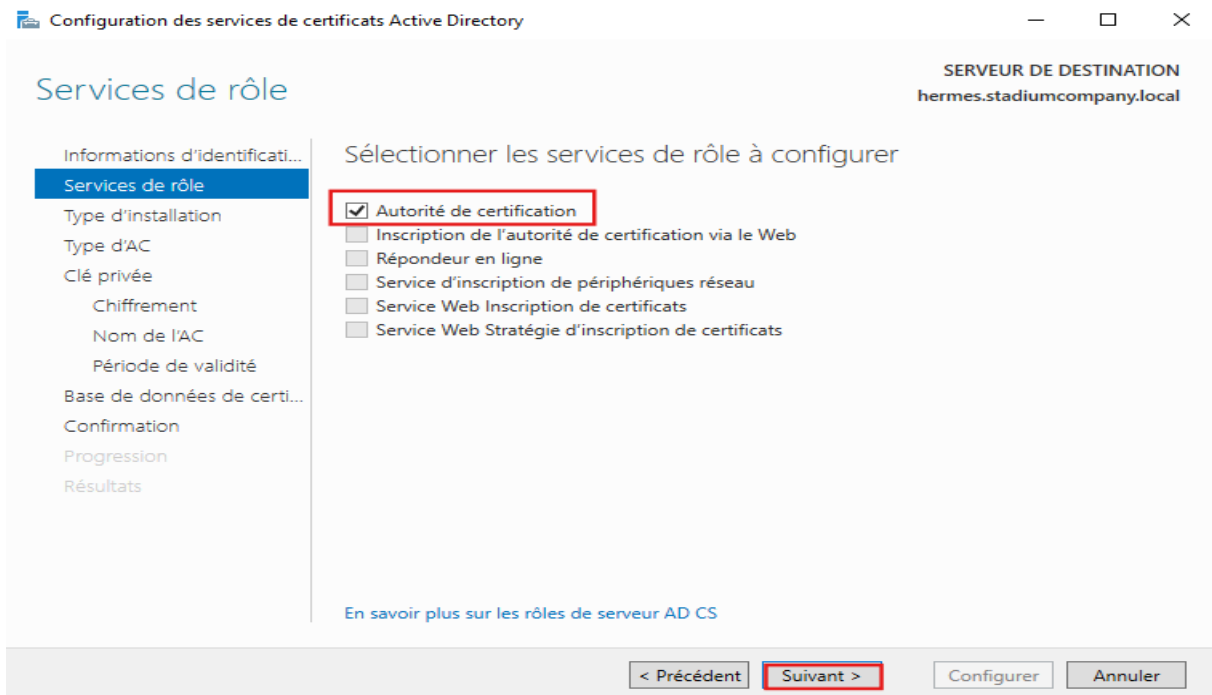
☞ Cela crée automatiquement une **racine de confiance** pour ton domaine.

✓ 1. Rôle à configurer

Coche uniquement :

Autorité de certification

Puis **Suivant**.



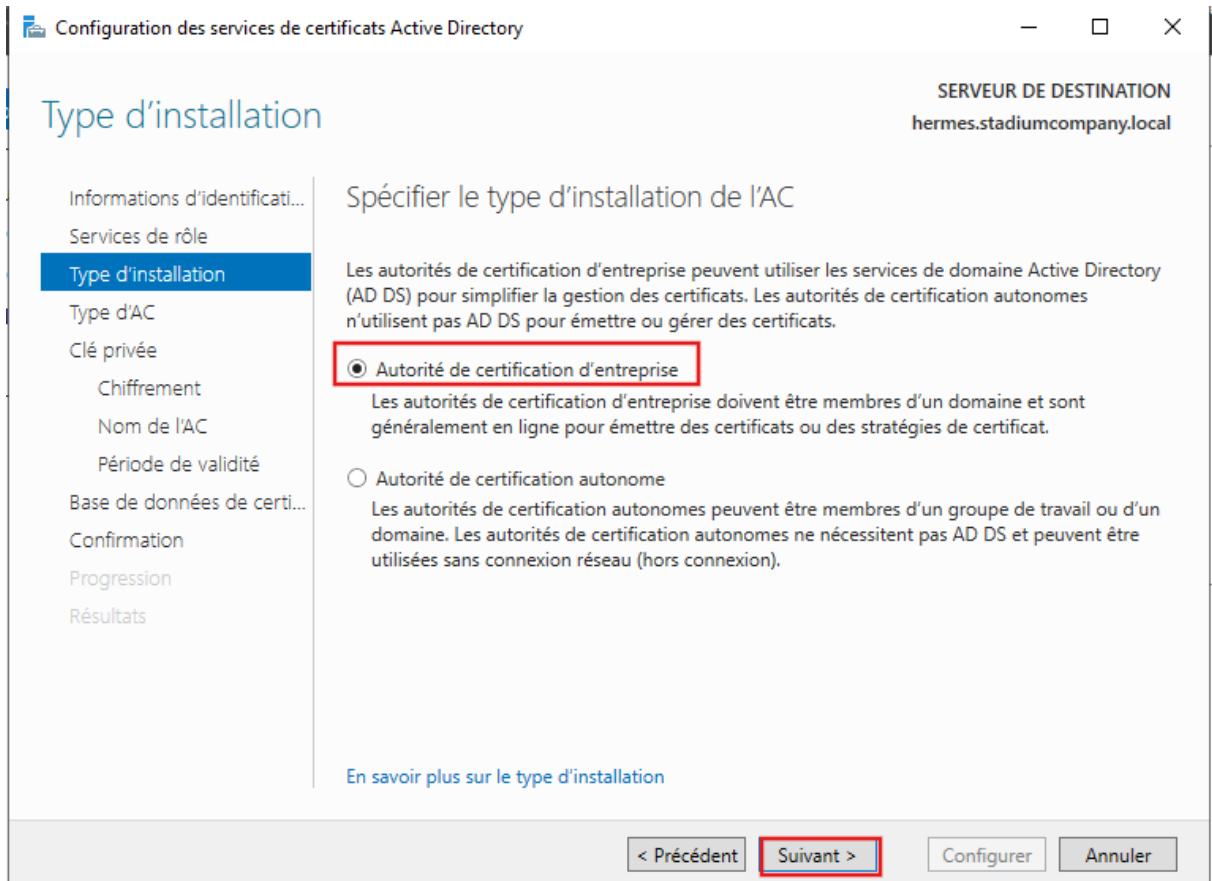
✓ 2. Type d'autorité

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.

Configuration des services de certificats Active Directory

SERVEUR DE DESTINATION
hermes.stadiumcompany.local

Type d'autorité de certification

Informations d'identificati...
Services de clé
Type d'installation
Type d'AC
Clé privée
Chiffrement
Nom de l'AC
Période de validité
Base de données de certi...
Confirmation
Progression
Résultats

Spécifier le type de l'AC

Lorsque vous installez les services de certificats Active Directory (AD CS), vous créez ou étendez une hiérarchie d'infrastructure à clé publique (PKI). Une autorité de certification racine se trouve au sommet de la hiérarchie PKI et émet ses propres certificats auto-signés. Une autorité de certification secondaire reçoit un certificat de l'autorité de certification de rang plus élevé dans la hiérarchie PKI.

Autorité de certification racine
Les autorités de certification racines sont les premières voire les seules autorités de certification configurées dans une hiérarchie PKI.

Autorité de certification secondaire
Les autorités de certification secondaires nécessitent une hiérarchie PKI établie et sont autorisées à émettre des certificats par l'autorité de certification de rang plus élevé dans la hiérarchie.

[En savoir plus sur le type d'autorité de certification](#)

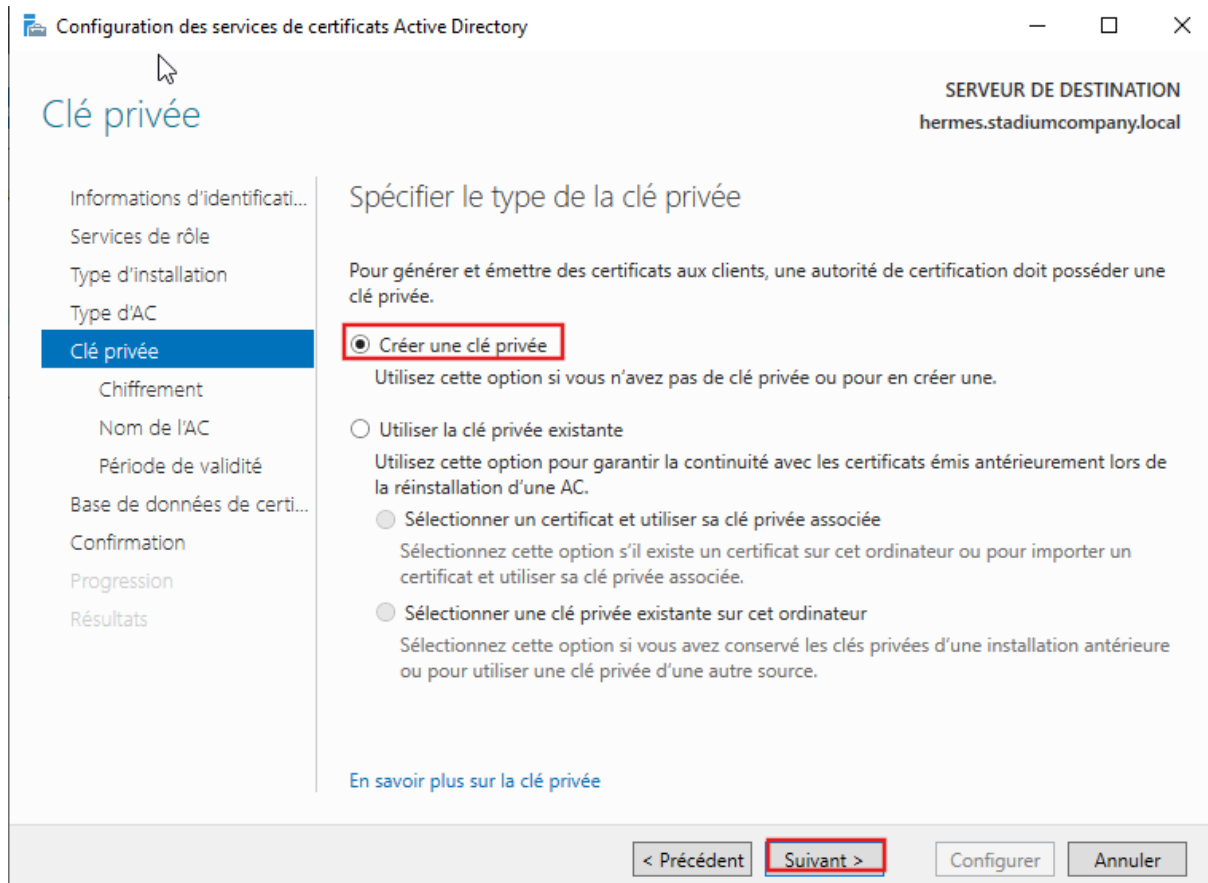
< Précédent **Suivant >** Configurer Annuler

✓ 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

Configuration des services de certificats Active Directory

Chiffrement pour l'autorité de certification

SERVEUR DE DESTINATION
hermes.stadiumcompany.local

Informations d'identificati...
Services de rôle
Type d'installation
Type d'AC
Clé privée
Chiffrement
Nom de l'AC
Période de validité
Base de données de certi...
Confirmation
Progression
Résultats

Spécifier les options de chiffrement

Sélectionnez un fournisseur de chiffrement :
RSA#Microsoft Software Key Storage Provider

Longueur de la clé :
2048

Sélectionnez l'algorithme de hachage pour signer les certificats émis par cette AC :
SHA256
SHA384
SHA512
SHA1

Autorisez l'interaction de l'administrateur lorsque l'autorité de certification accède à la clé privée.

[En savoir plus sur le chiffrement](#)

< Précédent **Suivant >** Configurer Annuler

✓ 6. Nom de l'autorité

Tu peux laisser tel quel. Suivant

✓ 7. Validité

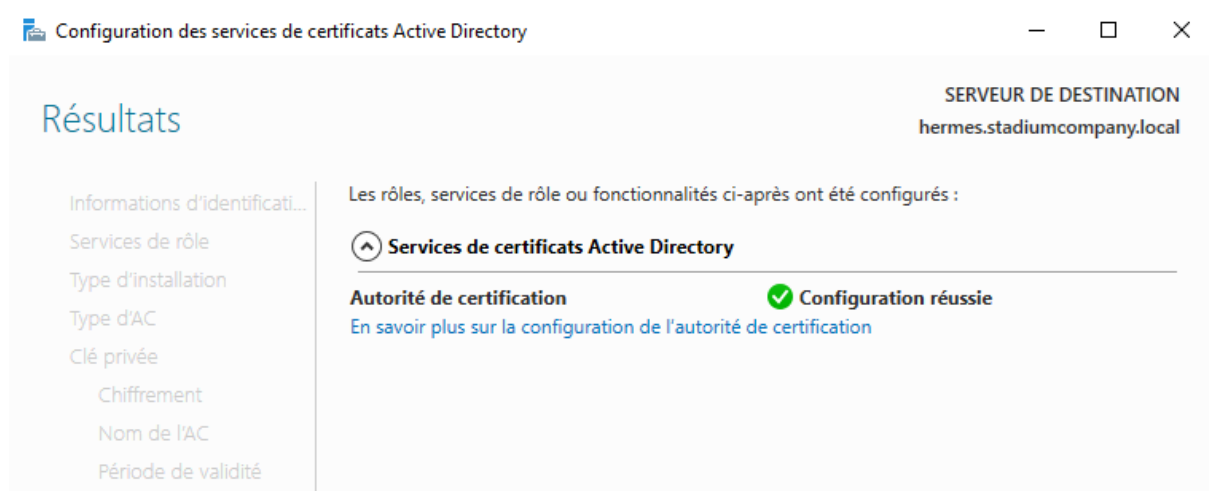
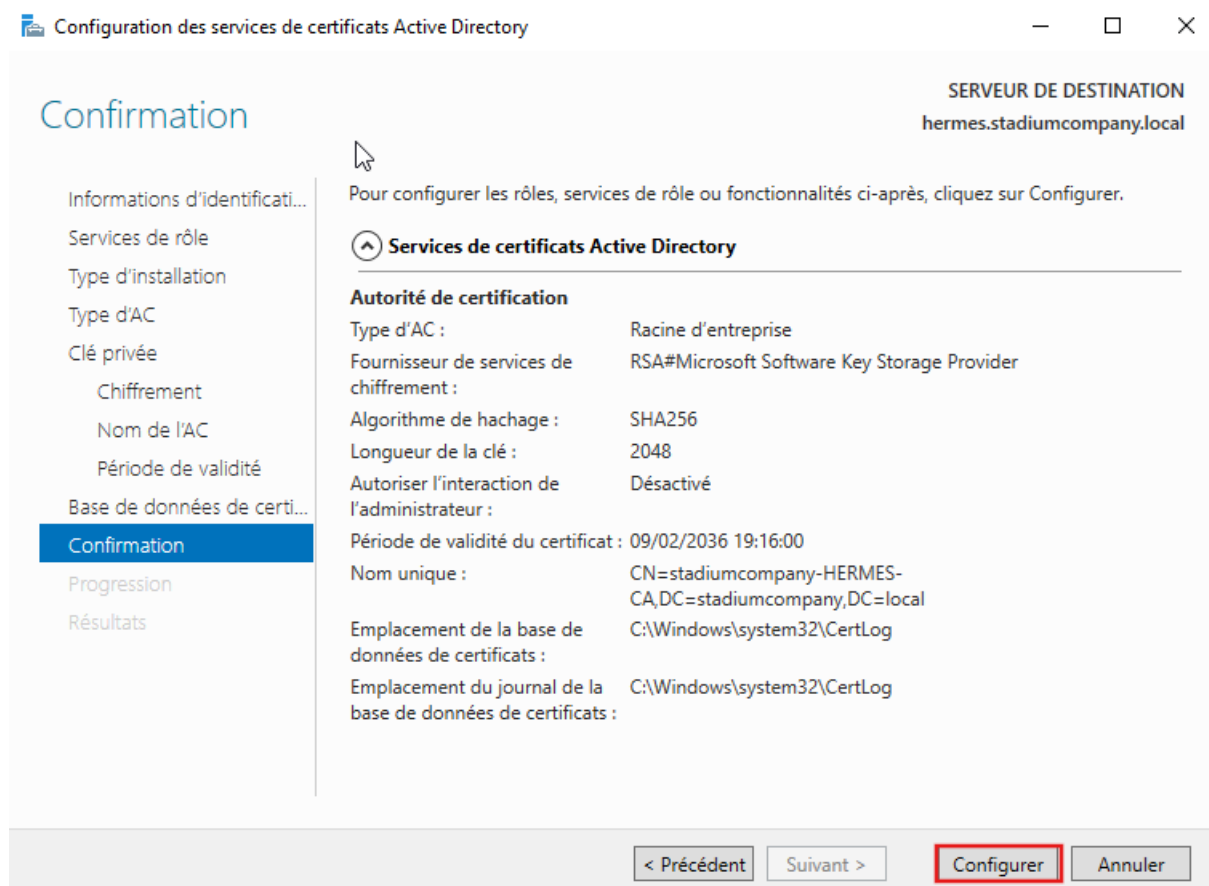
Choisis : 5 ans ou 10 ans puis suivant

✓ 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)

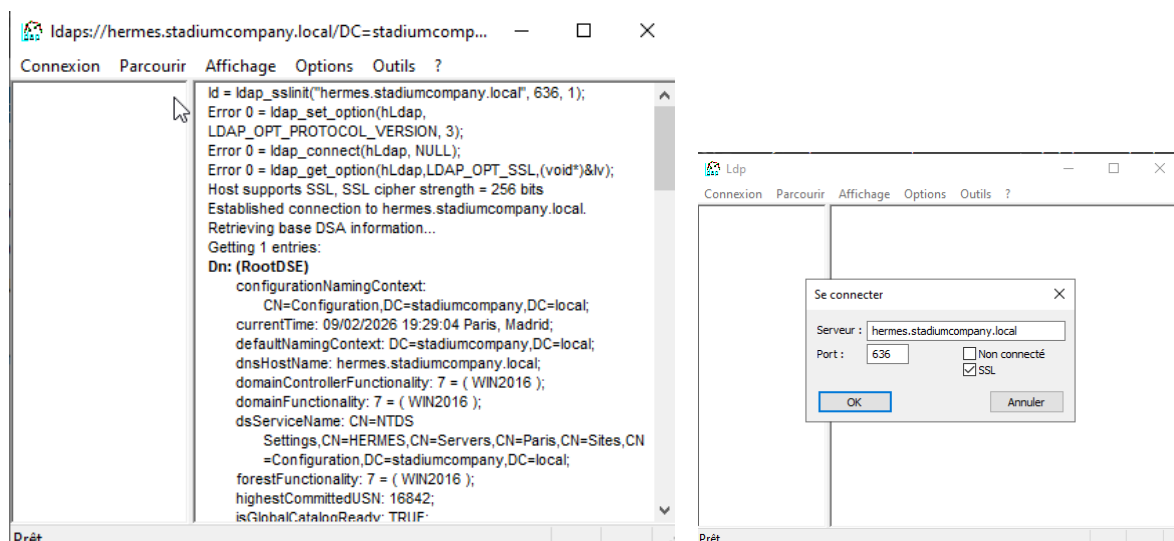
LDAPS est automatiquement activé dès que le serveur possède un certificat valide pour :

- FQDN du serveur
- Nom NetBIOS
- Nom complet AD

Pour vérifier :

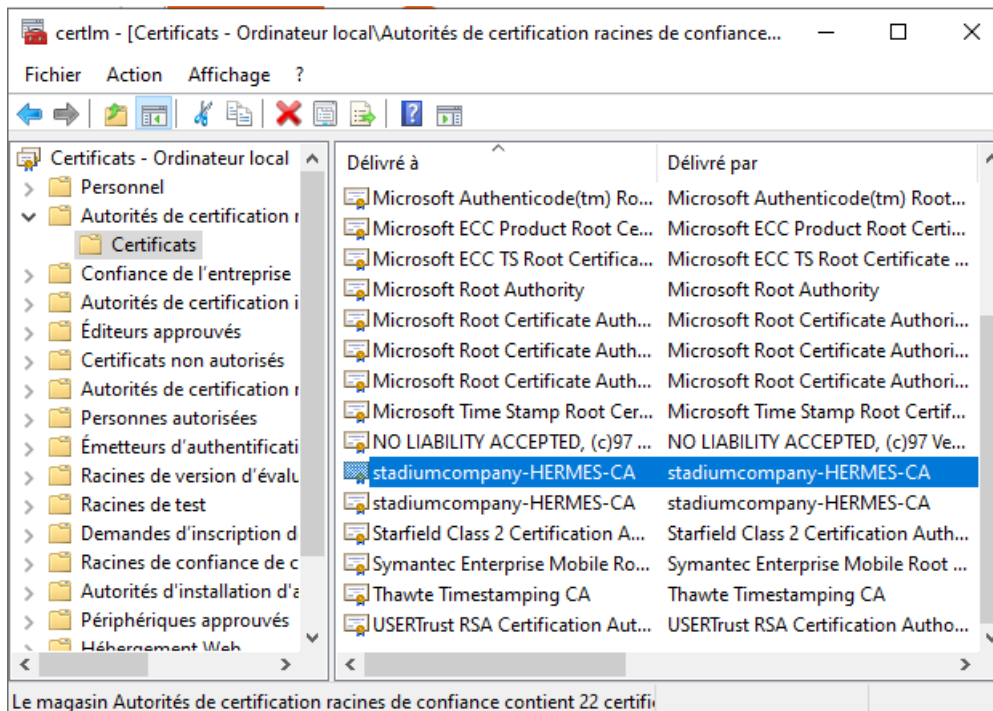
1. Ouvre **LDP.exe**
2. Connexion → Connect
3. Host : `hermes.stadiumcompany.local`
4. Port : **636**
5. Coche **SSL**

Si la connexion réussit → LDAPS est opérationnel.

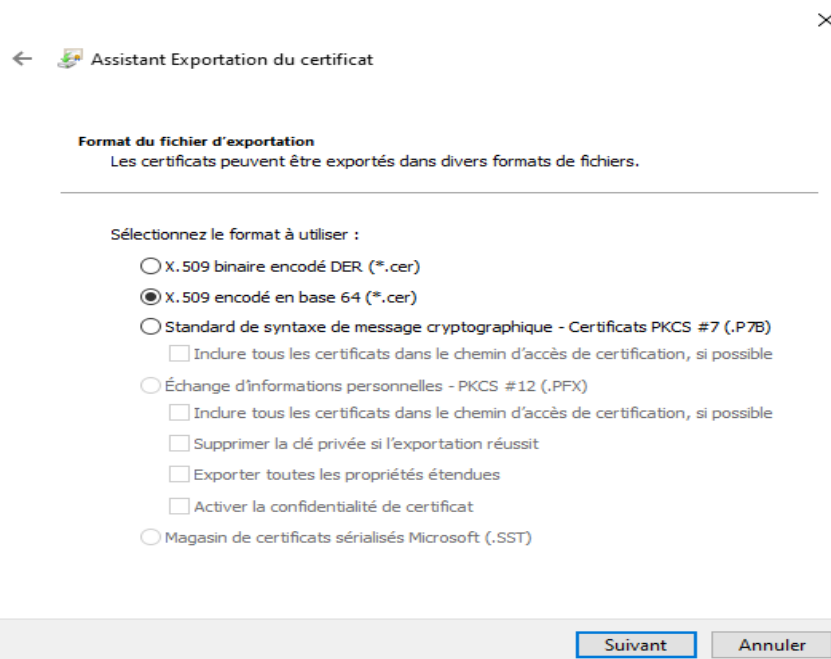


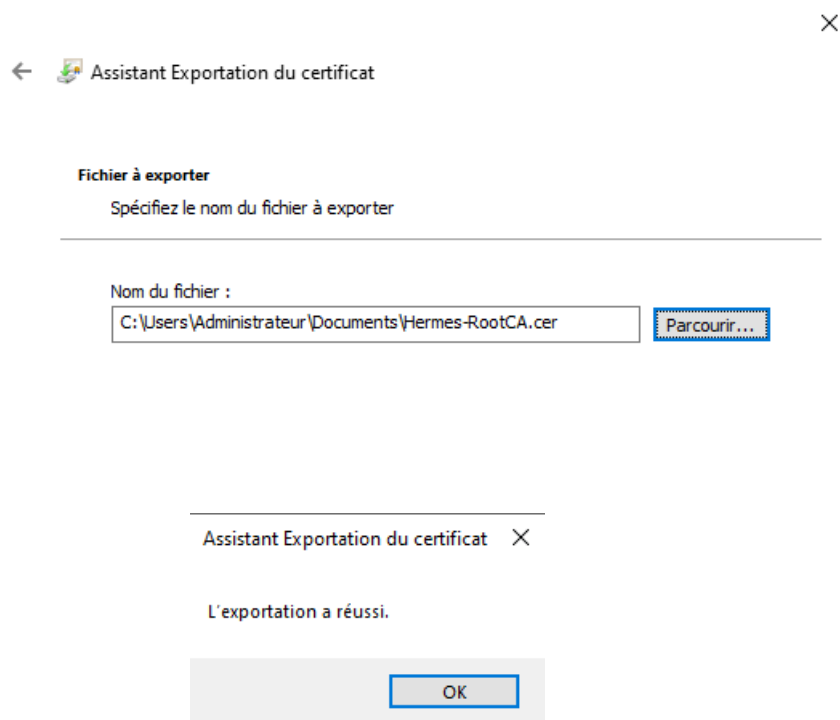
✓ 4. Exporter le certificat racine AD

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**

Create / Edit CA

Descriptive name
The name of this entry as displayed in the GUI for reference.
 This name can contain spaces but it cannot contain any of the following characters: ?, >, <, &, /, \, ' , "

Method

Trust Store Add this Certificate Authority to the Operating System Trust Store
When enabled, the contents of the CA will be added to the trust store so that they will be trusted by the operating system.

Randomize Serial Use random serial numbers when signing certificates
When enabled, if this CA is capable of signing certificates then serial numbers for certificates signed by this CA will be automatically randomized and checked for uniqueness instead of using the sequential value from Next Certificate Serial.

Existing Certificate Authority








Certificate data
Paste a certificate in X.509 PEM format here.

Certificate Private Key (optional)
Paste the private key for the above certificate here. This is optional in most cases, but is required when generating a Certificate Revocation List (CRL).

Next Certificate Serial
Enter a decimal number to be used as a sequential serial number for the next certificate to be signed by this CA. This value is ignored when Randomize Serial is checked.

☞ pfSense fait maintenant confiance aux certificats émis par Hermes.

☞ LDAPS pourra fonctionner.

Certificate Authorities						
Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
StadiumCompany-CA	✓	self-signed	1	ST=ile de France, O=StadiumCompany, L=Massy, CN=StadiumCompany-RootCA, C=FR ⓘ		    
				Valid From: Mon, 09 Feb 2026 12:26:36 +0100 Valid Until: Thu, 07 Feb 2036 12:26:36 +0100		
Hermes-AD-CA	✗	self-signed	0	DC=stadiumcompany, DC=local, CN=stadiumcompany-HERMES-CA ⓘ		  
				Valid From: Mon, 09 Feb 2026 19:08:13 +0100 Valid Until: Sat, 09 Feb 2036 19:18:12 +0100		

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

Server Settings	
Descriptive name	LDAP-Hermes
Type	LDAP
LDAP Server Settings	
Hostname or IP address	hermes.stadiumcompany.local <small>NOTE: When using SSL/TLS or STARTTLS, this hostname MUST match a Subject Alternative Name (SAN) or the Common Name (CN) of the LDAP server SSL/TLS Certificate.</small>
Port value	389
Transport	Standard TCP
Peer Certificate Authority	Global Root CA List <small>This CA is used to validate the LDAP server certificate when 'SSL/TLS Encrypted' or 'STARTTLS Encrypted' Transport is active. This CA must match the CA used by the LDAP server.</small>
Protocol version	3
Server Timeout	25 <small>Timeout for LDAP operations (seconds)</small>

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

Search scope

 Base DN

Authentication containers [Select a container](#)
 Note: Semi-Colon separated. This will be prepended to the search base dn above or the full container path can be specified containing a dc= component.
 Example: CN=Users;DC=example,DC=com or OU=Staff;OU=Freelancers

Extended query Enable extended query

Bind anonymous Use anonymous binds to resolve distinguished names

Bind credentials

User naming attribute

Group naming attribute

Group member attribute

RFC 2307 Groups LDAP Server uses RFC 2307 style group membership
 RFC 2307 style group membership has members listed on the group object rather than using groups listed on user object. Leave unchecked for Active Directory style group membership (RFC 2307bis).

Group member attribute

RFC 2307 Groups LDAP Server uses RFC 2307 style group membership
 RFC 2307 style group membership has members listed on the group object rather than using groups listed on user object. Leave unchecked for Active Directory style group membership (RFC 2307bis).

Group Object Class
 Object class used for groups in RFC2307 mode. Typically "posixGroup" or "group".

Shell Authentication Group DN
 If LDAP server is used for shell authentication, user must be a member of this group and have a valid posixAccount attributes to be able to login.
 Example: CN=Remoteshellusers,CN=Users,DC=example,DC=com

UTF8 Encode UTF8 encode LDAP parameters before sending them to the server.
 Required to support international characters, but may not be supported by every LDAP server.

Username Alterations Do not strip away parts of the username after the @ symbol
 e.g. user@host becomes user when unchecked.

Allow unauthenticated bind Allow unauthenticated bind
 Unauthenticated binds are bind with an existing login but with an empty password. Some LDAP servers (Microsoft AD) allow this type of bind without any possibility to disable it.

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

Diagnostics / Authentication  

User cesar authenticated successfully. This user is a member of groups:

Authentication Test

Authentication Server	LDAP-Hermes 
	Select the authentication server to test against.
Username	cesar
Password
Debug	<input type="checkbox"/> Set debug flag Sets the debug flag when performing authentication, which may trigger additional diagnostic entries in the system log (e.g. for LDAP).

Test LDAPS (636)

Diagnostics → Authentication

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

Résultat attendu : Authentication successful

User cesar authenticated successfully. This user is a member of groups:

Authentication Test

Authentication Server ▼
Select the authentication server to test against.

Username

Password

Debug Set debug flag
Sets the debug flag when performing authentication, which may trigger additional diagnostic entries in the system log (e.g. for LDAP).

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

Group Properties

Group name

Scope ▼
Warning: Changing this setting may affect the local groups file, in which case a reboot may be required for the changes to take effect.

Description
Group description, for administrative information only

Group membership

Not members

Members

➤ Move to "Members"
⬅ Move to "Not members"

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

Save

SECURISATION DE L'ACCES A INTERNET ET MISE EN PLACE D'UNE DMZ

Name	Description	Action
------	-------------	--------

[+ Add](#)

[Save](#)

Group: pfsense

Assigned privileges

- System - HA node sync
- User - Config: Deny Config Write
- User - Notices: View
- User - Notices: View and Clear
- User - Services: Captive Portal login
- User - System: Copy files (scp)
- User - System: Copy files to home directory (chrooted scp)
- User - System: Shell account access
- User - System: SSH tunneling
- User - VPN: IPsec xauth Dialin
- User - VPN: L2TP Dialin
- User - VPN: PPPoE Dialin
- WebCfg - AJAX: Get Queue Stats
- WebCfg - AJAX: Get Service Providers
- WebCfg - AJAX: Get Stats
- WebCfg - All pages**
- WebCfg - Crash reporter
- WebCfg - Dashboard (all)
- WebCfg - Dashboard widgets (direct access)
- WebCfg - Diagnostics: ARP Table

[Save](#) [Filter](#) [Clear](#)

Allow access to all pages (This privilege effectively gives administrator-level access to users in the group)

Name	Description	Action
WebCfg - All pages	Allow access to all pages (admin privilege)	Delete

Security notice: Users in this group effectively have administrator-level access

[+ Add](#)

[Save](#)

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

On fait un test de connexion avec la base LDAP

Settings

Session timeout:
Time in minutes to expire idle management sessions. The default is 4 hours (240 minutes). Enter 0 to never expire sessions. NOTE: This is a security risk!

Authentication Server:

Password Hash Algorithm:
Selects which algorithm the firewall will use when creating hashes for local user passwords. The most secure option is currently bcrypt. Some users may prefer SHA-512-based crypt hashes for compatibility or compliance purposes.

Shell Authentication: Use Authentication Server for Shell Authentication
If RADIUS or LDAP server is selected it is used for console and SSH authentication. Otherwise, the Local Database is used. To allow logins with RADIUS credentials, equivalent local users with the expected privileges must be created first. To allow logins with LDAP credentials, Shell Authentication Group DN must be specified on the LDAP server configuration page.

Auth Refresh Time:
Time in seconds to cache authentication results. The default is 30 seconds, maximum 3600 (one hour). Shorter times result in more frequent queries to authentication servers.

[Save](#) [Save & Test](#)

LA connexion a reussi

LDAP settings ✕

Test results

Attempting connection to	hermes.stadiumcompany.local	OK
Attempting bind to	hermes.stadiumcompany.local	OK
Attempting to fetch Organizational Units from	hermes.stadiumcompany.local	OK

Organization units found

OU=Administration,DC=stadiumcompany,DC=local

OU=Camera-IP,DC=stadiumcompany,DC=local

OU=Domain Controllers,DC=stadiumcompany,DC=local

OU=Equipe,DC=stadiumcompany,DC=local

OU=Fournisseur,DC=stadiumcompany,DC=local

OU=Groupes,OU=Administration,DC=stadiumcompany,DC=local

OU=Groupes,OU=VIP-Presse,DC=stadiumcompany,DC=local

OU=Groupes,OU=Fournisseur,DC=stadiumcompany,DC=local

OU=Groupes,OU=Equipe,DC=stadiumcompany,DC=local

OU=Groupes,OU=Restaurant,DC=stadiumcompany,DC=local

OU=Ordinateurs,OU=Administration,DC=stadiumcompany,DC=local

OU=Ordinateurs,OU=VIP-Presse,DC=stadiumcompany,DC=local

OU=Ordinateurs,OU=Fournisseur,DC=stadiumcompany,DC=local

OU=Ordinateurs,OU=Equipe,DC=stadiumcompany,DC=local

OU=Ordinateurs,OU=Restaurant,DC=stadiumcompany,DC=local

OU=Restaurant,DC=stadiumcompany,DC=local

OU=Utilisateurs,OU=Administration,DC=stadiumcompany,DC=local

OU=Utilisateurs,OU=VIP-Presse,DC=stadiumcompany,DC=local

OU=Utilisateurs,OU=Fournisseur,DC=stadiumcompany,DC=local

OU=Utilisateurs,OU=Equipe,DC=stadiumcompany,DC=local


OU=Utilisateurs,OU=Restaurant,DC=stadiumcompany,DC=local

OU=VIP-Presse,DC=stadiumcompany,DC=local

OU=WIFI,DC=stadiumcompany,DC=local

CN=Users,DC=stadiumcompany,DC=local

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


Username or Password incorrect

SIGN IN

kaiser

.....

SIGN IN

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

The screenshot shows the pfSense dashboard. The 'System Information' panel displays the following details:

Name	heimdall.stadiumcompany.local
User	kaiser@172.20.1.1 (LDAP/LDAP-Hermes)
System	VMware Virtual Machine Netgate Device ID: 84925fb89354772d5420

The 'Netgate Services And Support' panel shows the contract type as 'Community Support' and 'Community Support Only'. A link for 'NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES' is also visible.

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

The screenshot shows the 'Services / Captive Portal' page. It features a table titled 'Captive Portal Zones' with the following columns: Zone, Interfaces, Number of users, Description, and Actions. A '+ Add' button is located at the bottom right of the table.

✓ Paramètres essentiels

On va renseigner le Nom du Portail Captif et sa description :

Stadiumcompany_portal pour le nom de la zone

Portail captif Stadiumcompany pour la description de la zone

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

Add Captive Portal Zone

Zone name	<input style="width: 80%;" type="text" value="Stadiumcompany_portal"/>
	<small>Zone name. Can only contain letters, digits, and underscores (_) and may not start with a digit.</small>
Zone description	<input style="width: 80%;" type="text" value="Portail captif de Stadiumcompany"/>
	<small>A description may be entered here for administrative reference (not parsed).</small>

- 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)

Captive Portal Configuration

Enable	<input checked="" type="checkbox"/> Enable Captive Portal
Description	<input style="width: 80%;" type="text" value="Portail captif de Stadiumcompany"/>
	<small>A description may be entered here for administrative reference (not parsed).</small>
Interfaces	<div style="border: 1px solid #ccc; padding: 2px;"> WAN LAN OPT1 OPT2 </div> <small>Select the interface(s) to enable for captive portal.</small>
Maximum concurrent connections	<input style="width: 80%;" type="text" value="1"/>
	<small>Limits the number of concurrent connections to the captive portal HTTP(S) server. This does not set how many users can be logged in to the captive portal, but rather how many connections a single IP can establish to the portal web server.</small>
Idle timeout (Minutes)	<input style="width: 80%;" type="text" value="15"/>

- 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)

Logout popup window	<input checked="" type="checkbox"/> Enable logout popup window If enabled, a popup window will appear when clients are allowed through the captive portal. This allows clients to explicitly disconnect themselves before the idle or hard timeout occurs.
Pre-authentication redirect URL	<input type="text" value="https://www.bing.com/"/> Set a default redirection URL. Visitors will be redirected to this URL after authentication only if the captive portal doesn't know where to redirect them. This field will be accessible through \$PORTAL_REDIRECTURLS variable in captiveportal's HTML pages.
After authentication Redirection URL	<input type="text" value="https://www.bing.com/"/> Set a forced redirection URL. Clients will be redirected to this URL instead of the one they initially tried to access after they've authenticated.
Blocked MAC address redirect URL	<input type="text"/> Blocked MAC addresses will be redirected to this URL when attempting access.
Preserve users database	<input checked="" type="checkbox"/> Preserve connected users across reboot If enabled, connected users won't be disconnected during a pfSense reboot.
Concurrent user logins	<input type="text" value="Last login"/> Disabled: Do not allow concurrent logins per username or voucher. Multiple: No restrictions to the number of logins per username or voucher will be applied. Last login: Only the most recent login per username or voucher will be granted. Previous logins will be disconnected. First login: Only the first login per username or voucher will be granted. Further login attempts using the username or voucher will not be possible while an initial user is already active.
MAC filtering	<input checked="" type="checkbox"/> Disable MAC filtering If enabled no attempts will be made to ensure that the MAC address of clients stays the same while they are logged in. This is required when the MAC address of the client cannot be determined (usually because there are routers between pfSense and the clients). If this is enabled, RADIUS MAC authentication cannot be used.

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

Captive Portal Login Page	
Display custom logo image	<input checked="" type="checkbox"/> Enable to use a custom uploaded logo
Logo Image	<input type="button" value="Choisir un fichier"/> <input type="button" value="Aucun fichier choisi"/> Add a logo for use in the default portal login screen. File will be renamed captiveportal-logo.* The image will be resized to fit within the given area, it can be of any image type: .png, .jpg, .svg This image will not be stored in the config. The default logo will be used if no custom image is present.
Display custom background image	<input checked="" type="checkbox"/> Enable to use a custom uploaded background image
Background Image	<input type="button" value="Choisir un fichier"/> <input type="button" value="Aucun fichier choisi"/> Add a background image for use in the default portal login screen. File will be renamed captiveportal-background.* The background image will fill the screen. This image will not be stored in the config. The default background image will be used if no custom background is present.
Terms and Conditions	<div style="border: 1px solid green; padding: 5px;"> Charte d'utilisation du wifi Charte d'utilisation Charte d'utilisation du réseau Wifi DE SITKA La présente charte a pour objet de définir les règles d'utilisation de la connexion Wifi du Gite auberge les </div> Copy and paste terms and conditions for use in the captive portal. HTML tags will be stripped out

→ 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

