

# pfSense

---

Guide complet : Installation, Configuration, Sécurité, LDAP/LDAPS, Portail Captif et Snort IDS/IPS

01 Installation & Configuration

02 Sécurité & Certificats

03 LDAP / LDAPS

04 Portail Captif

05 Snort IDS/IPS

06 Tests d'intrusion



pfSense CE 2.5.x

# Sommaire

## **PARTIE 1 – INSTALLATION DE PFSense**

1. Introduction à PfSense
2. Prérequis matériels
3. Infrastructure du laboratoire
4. Téléchargement et vérification de l'intégrité
5. Lancement de l'installation
6. Configuration post-installation
  - 6.1 Configuration du clavier
  - 6.2 Déclaration des interfaces
  - 6.3 Assignation des adresses IP

## **PARTIE 2 – CONFIGURATION DE BASE**

7. Test de la connectivité
8. Assistant de configuration (Wizard)
9. Configuration permanente du clavier et des outils VMware

## **PARTIE 3 – SÉCURITÉ DE PFSense**

10. Sécurisation de la console par mot de passe
11. Sécurisation de l'accès SSH
12. Sécurisation de l'interface web par HTTPS
  - 12.1 Création d'une autorité de certification interne
  - 12.2 Génération du certificat web
  - 12.3 Injection du certificat dans PfSense

## **PARTIE 4 – AUTHENTIFICATION LDAP ET LDAPS**

13. Test de connectivité LDAP/LDAPS sur Active Directory
14. Création d'une autorité de certification sur hermes
15. Création des comptes utilisateurs AD
16. Configuration des authentifications LDAP/LDAPS sur PfSense
17. Analyse avec Wireshark et résolution du problème LDAPS
18. Test et utilisation des authentifications

## **PARTIE 5 – PORTAIL CAPTIF**

19. Introduction au portail captif
20. Activation et configuration du portail captif
21. Configuration du DHCP sur OPT1
22. Création des règles de pare-feu
23. Test du portail captif

## **PARTIE 6 – SNORT IDS/IPS**

24. Introduction à Snort et aux IDS/IPS
25. Création d'un compte Snort
26. Installation de Snort sur PfSense
27. Configuration de Snort
28. Test d'intrusion avec Nmap

# PARTIE 1 – INSTALLATION DE PFSENSE

## 1. Introduction à PfSense

PfSense est un pare-feu open source basé sur le système d'exploitation FreeBSD. Il utilise le pare-feu à états **Packet Filter**, des fonctions de routage et de NAT lui permettant de connecter plusieurs réseaux informatiques. Il comporte l'équivalent libre des outils et services utilisés habituellement sur des routeurs professionnels propriétaires. PfSense convient parfaitement pour la sécurisation d'un réseau d'entreprise.

## 2. Prérequis matériels

Voici les configurations minimale et recommandée pour un serveur PfSense :

- **Processeur** : 600 MHz minimum (recommandé : 1 GHz recommandé)
- **Mémoire vive** : 512 Mo minimum (recommandé : 1 Go recommandé)
- **Stockage** : > 6 Go (recommandé : > 6 Go)

## 3. Infrastructure du laboratoire

Pour ce laboratoire, trois machines sont nécessaires :

### Serveur PfSense (heimdall) – FreeBSD, réseau WAN

IP : 192.168.1.250 | Masque : 255.255.255.0 | Passerelle : 192.168.1.1

### Serveur Active Directory et DNS (hermes) – Réseau sitka\_lan

IP : 172.20.0.14 | Masque : 255.255.255.0 | Domaine : sitka.local

### Machine cliente (Debian/Ubuntu/Windows) – Réseau opt\_lan

Adresse IP : DHCP

Configuration des cartes réseau VMware :

```
• Network Adapter (Bridge) → 192.168.1.0/24 (WAN) • Network Adapter 2 (LAN_1) → 172.20.0.0/24 (sitka_lan) • Network Adapter 3 (LAN_2) → 192.168.2.0/24 (opt_lan)
```

## 4. Téléchargement et vérification de l'intégrité

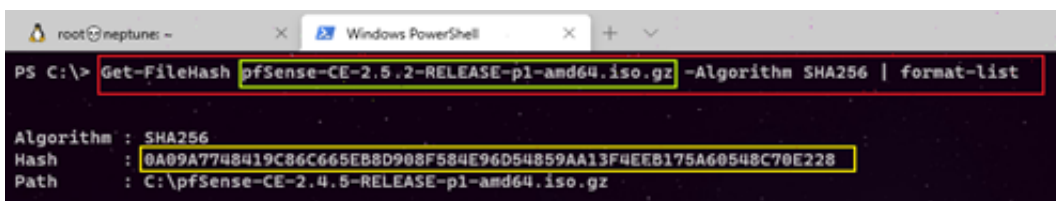
L'image ISO d'installation de PfSense est disponible sur le site officiel :

```
https://www.pfsense.org/download/
```

Après le téléchargement, il est impératif de vérifier l'intégrité du fichier en comparant son empreinte SHA256 avec celle fournie sur le site officiel :

```
Get-FileHash pfSense-CE-2.5.2-RELEASE-amd64.iso.gz -Algorithm SHA256 | Format-List
```

Si les deux empreintes sont identiques, le fichier est intègre et peut être utilisé.



```
PS C:\> Get-FileHash pfSense-CE-2.5.2-RELEASE-p1-amd64.iso.gz -Algorithm SHA256 | format-list

Algorithm : SHA256
Hash       : 0A09A7748419C86C665EB8D908F584E96D54859AA13F4EEB175A60548C70E228
Path       : C:\pfSense-CE-2.4.5-RELEASE-p1-amd64.iso.gz
```

Vérification de l'intégrité SHA256 du fichier ISO

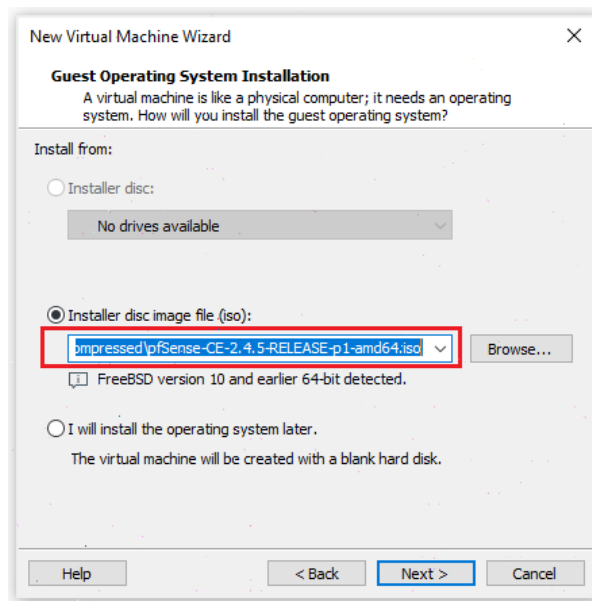
## 5. Lancement de l'installation

Après décompression de l'archive, on crée une nouvelle machine virtuelle VMware avec les paramètres suivants :

• Nom : pfsense • Stockage : 20 Go • RAM : 1 Go • 3 cartes réseau (Bridge + LAN\_1 + LAN\_2)

Les étapes d'installation sont les suivantes :

- Accepter le contrat de licence (Accept).
- Sélectionner **Install** puis valider avec OK.
- Choisir le clavier français (fr) et tester la configuration.
- Sélectionner le système de fichiers **UFS** pour la création des partitions.
- Choisir de ne pas ouvrir de shell supplémentaire et redémarrer.



Étape d'installation PfSense – écran 2



Étape d'installation PfSense – écran 3

New Virtual Machine Wizard

**Name the Virtual Machine**  
What name would you like to use for this virtual machine?

Virtual machine name:

Location:

The default location can be changed at Edit > Preferences.

< Back   Next >   Cancel

Étape d'installation PfSense – écran 4

New Virtual Machine Wizard

**Specify Disk Capacity**  
How large do you want this disk to be?

The virtual machine's hard disk is stored as one or more files on the host computer's physical disk. These file(s) start small and become larger as you add applications, files, and data to your virtual machine.

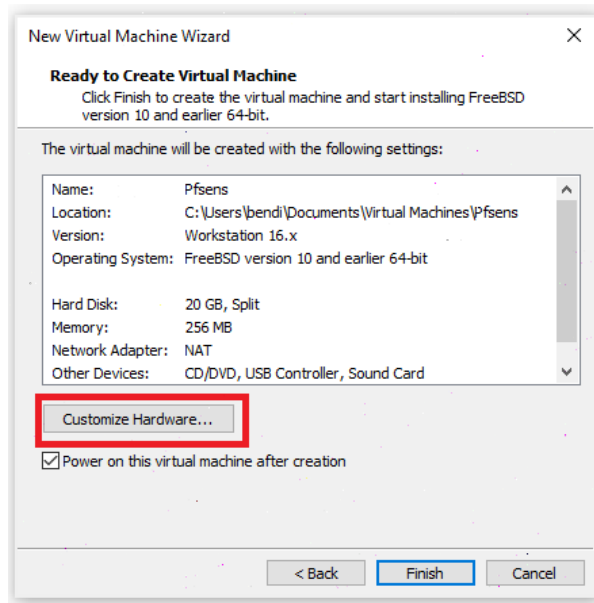
Maximum disk size (GB):

Recommended size for FreeBSD version 10 and earlier 64-bit: 20 GB

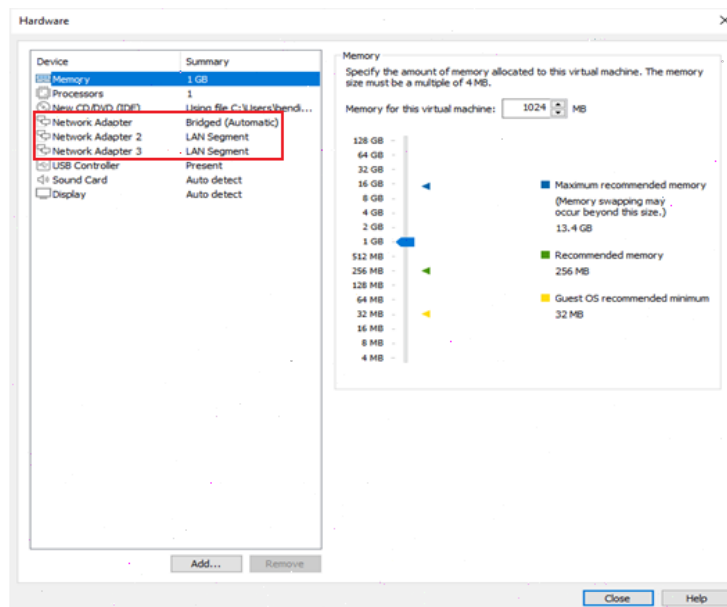
Store virtual disk as a single file  
 Split virtual disk into multiple files  
Splitting the disk makes it easier to move the virtual machine to another computer but may reduce performance with very large disks.

Help   < Back   Next >   Cancel

Étape d'installation PfSense – écran 5



Étape d'installation PfSense – écran 6



Étape d'installation PfSense – écran 7

## 6. Configuration post-installation

### 6.1 Configuration temporaire du clavier

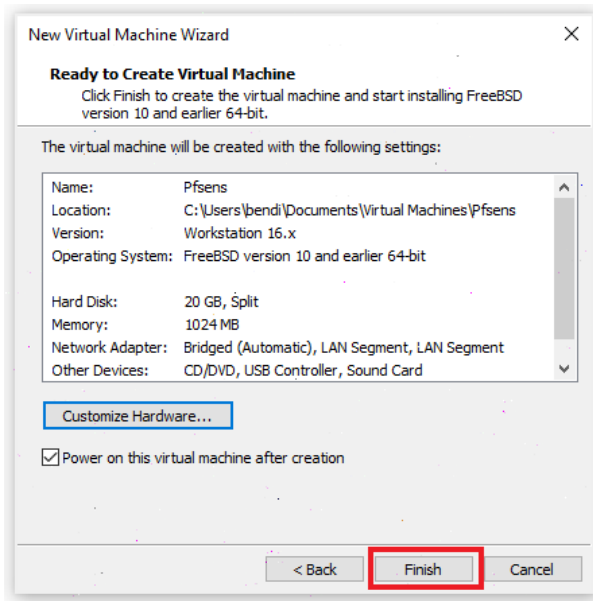
Après le redémarrage, le clavier est en QWERTY. Pour le passer temporairement en AZERTY (sera remis à zéro au prochain redémarrage), on utilise l'option 8 (shell) :

```
#kbdcontrol -l fr #_ou #kbdcontrol -l /usr/share/syscons/keymaps/fr.iso.kbd
```

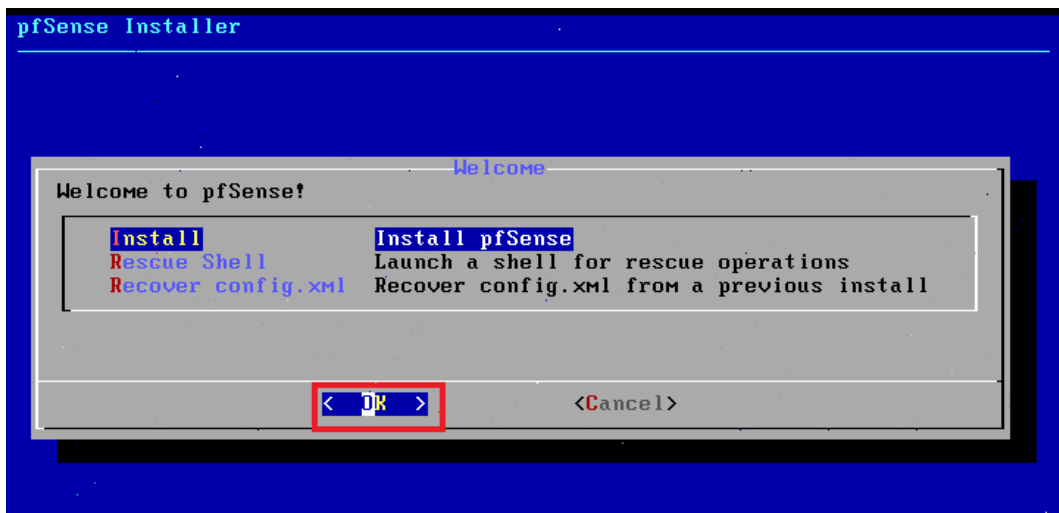
■■ Note : La configuration permanente du clavier sera effectuée via l'interface web dans la partie suivante.

### 6.2 Déclaration des interfaces

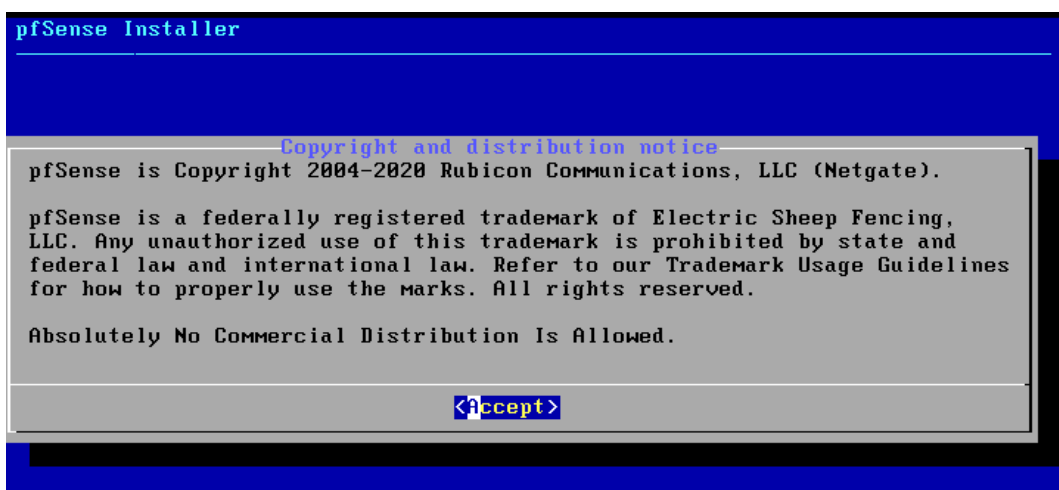
On choisit l'**option 1** dans le menu PfSense pour déclarer les trois interfaces (WAN, LAN et OPT1). À la fin de cette étape, les trois interfaces doivent être reconnues.



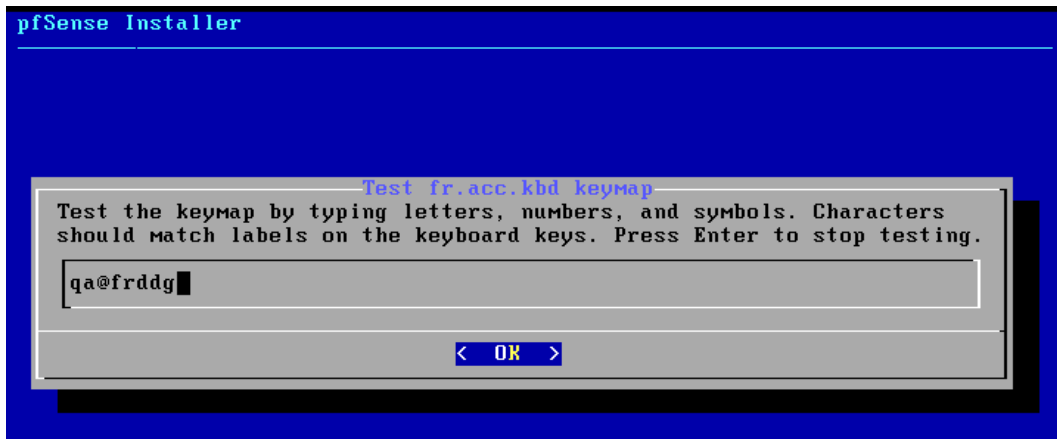
Configuration des interfaces réseau



Configuration des interfaces réseau



Configuration des interfaces réseau



Configuration des interfaces réseau

## 6.3 Assignation des adresses IP

### Interface WAN

L'adresse WAN dépend de la configuration de votre box internet. On effectue d'abord un **ipconfig /all** sur la machine physique pour identifier le réseau.

• Adresse IP : 192.168.1.250 • Masque : 255.255.255.0 • Passerelle : 192.168.1.1 • Pas de DHCP IPv6

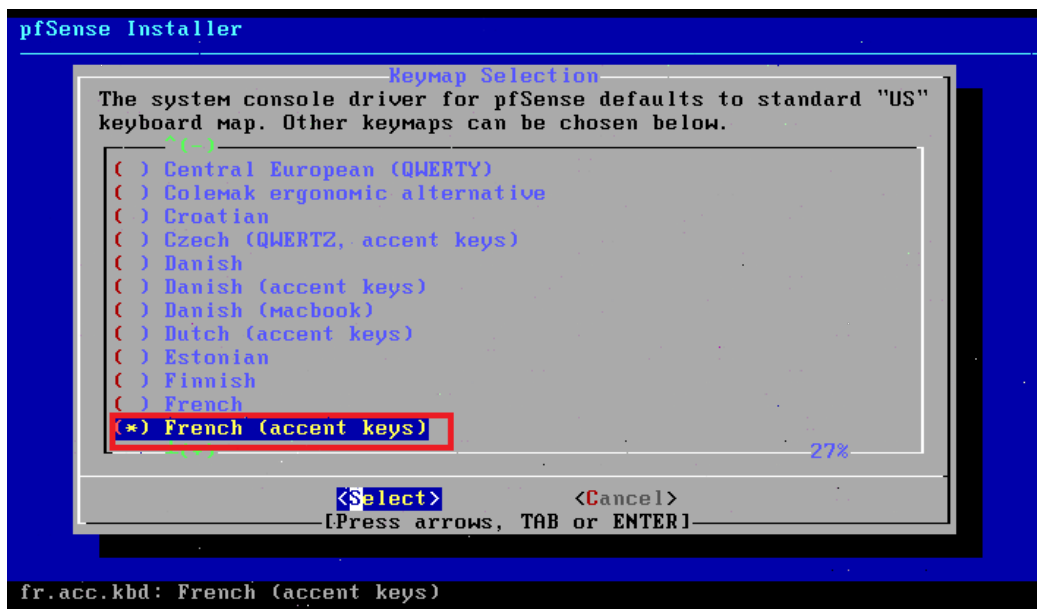
■ ■ Pour des raisons de sécurité, il est préférable de ne pas activer le configurateur web sur l'interface WAN.

### Interface LAN (sitka\_lan)

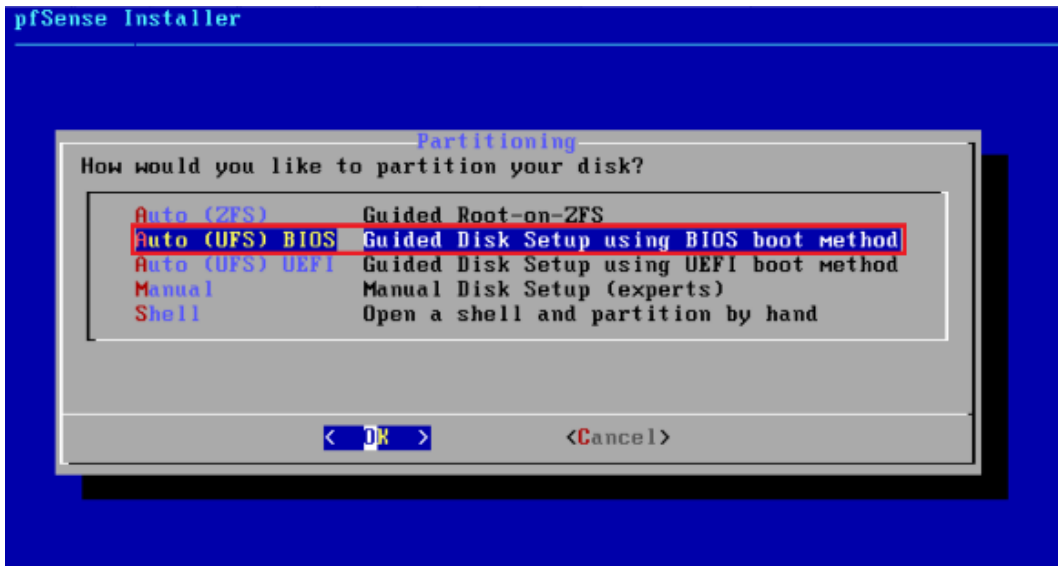
• Adresse IP : 172.20.0.250 • Masque : 255.255.255.0 • Pas de passerelle • DHCP activé : plage 172.20.0.20 → 172.20.0.30

### Interface OPT1 (opt\_lan)

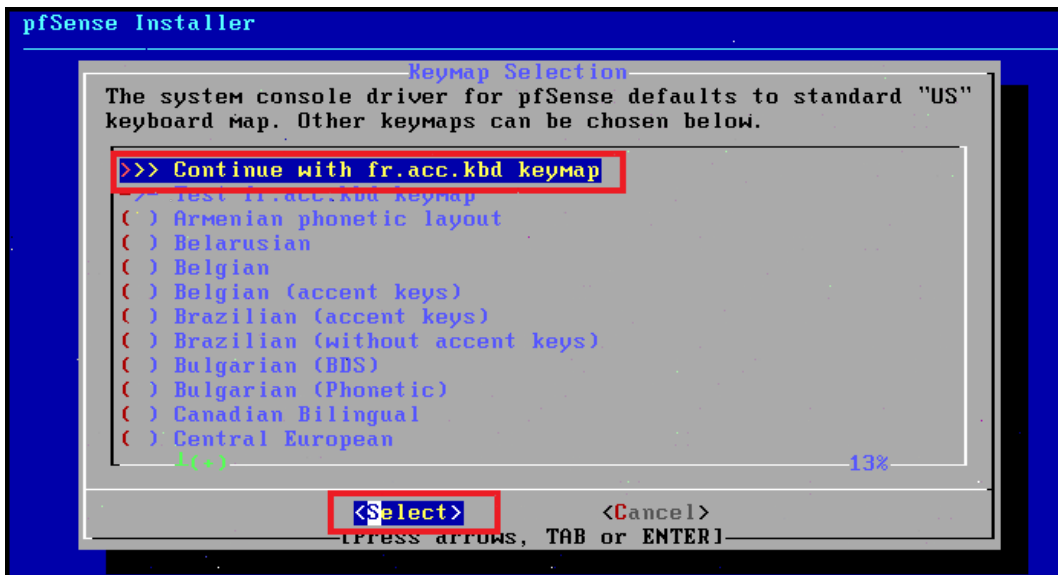
• Adresse IP : 192.168.2.250 • Masque : 255.255.255.0 • DHCP activé : plage à définir



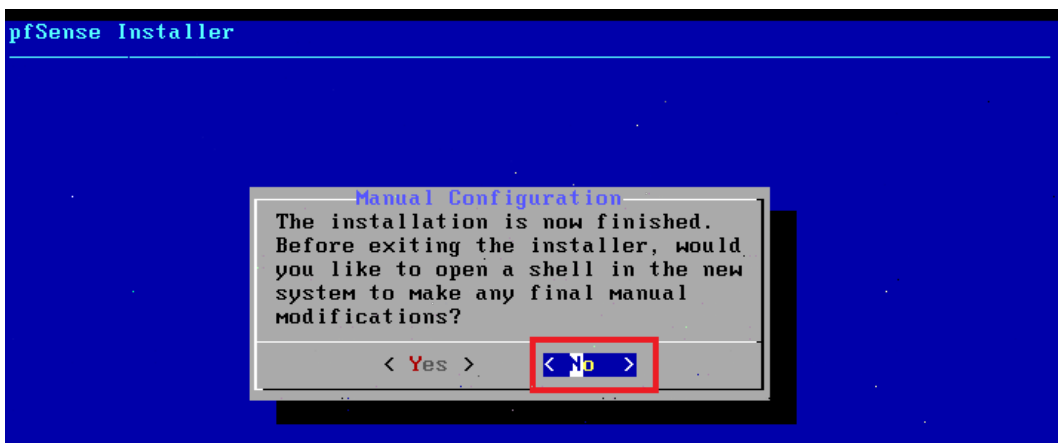
Configuration adresses IP – interface



Configuration addresses IP – interface



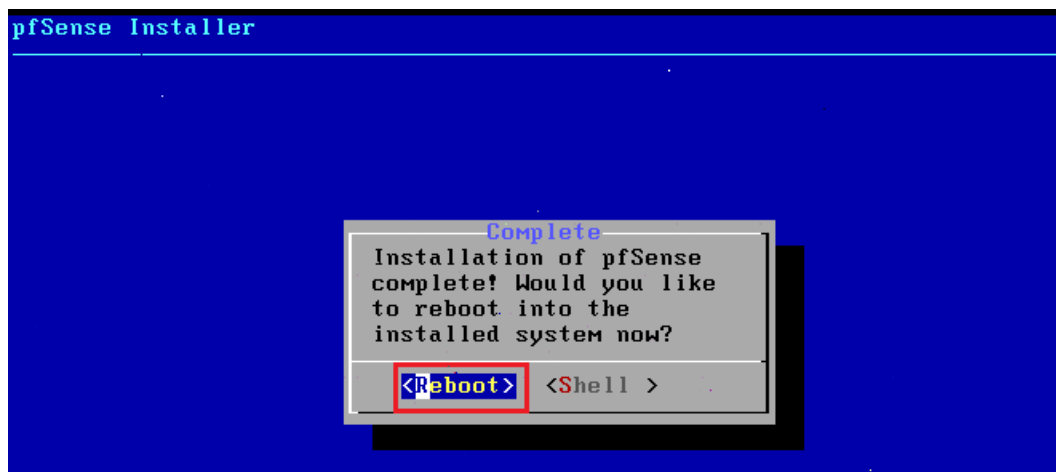
Configuration addresses IP – interface



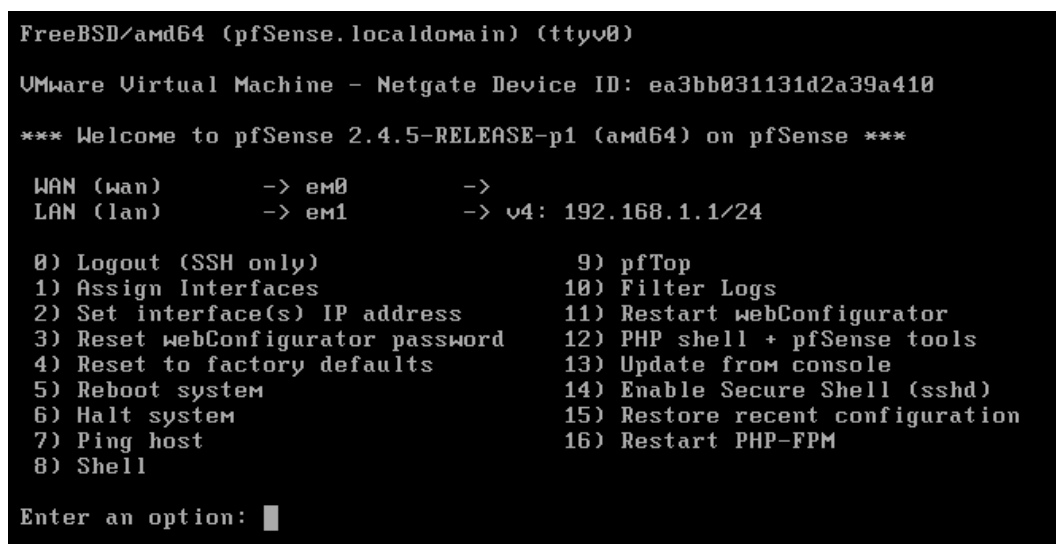
Configuration addresses IP – interface



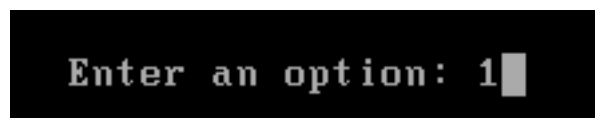
Configuration addresses IP – interface



Configuration addresses IP – interface



Configuration addresses IP – interface



Configuration addresses IP – interface

```

say no here and use the webConfigurator to configure VLANs later, if required.

Should VLANs be set up now [y!n]? n

If the names of the interfaces are not known, auto-detection can
be used instead. To use auto-detection, please disconnect all
interfaces before pressing 'a' to begin the process.

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

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

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

The interfaces will be assigned as follows:

WAN -> em0
LAN -> em1
OPT1 -> em2

Do you want to proceed [y!n]? y

```

Configuration addresses IP – interface

```

WAN (wan)      -> em0      ->
LAN (lan)     -> em1      -> v4: 192.168.1.1/24
OPT1 (opt1)   -> em2      ->

```

Configuration addresses IP – interface

```

Carte Ethernet Ethernet :

Suffixe DNS propre à la connexion. . . . :
Description. . . . . : Killer E2200 Gigabit Ethernet Controller
Adresse physique . . . . . : FC-AA-14-24-82-7B
DHCP activé. . . . . : Oui
Configuration automatique activée. . . : Oui
Adresse IPv6 de liaison locale. . . . . : fe80::b523:e2a4:2139:24c5%16(préfééré)
Adresse IPv4. . . . . : 192.168.1.142(préfééré)
Masque de sous-réseau. . . . . : 255.255.255.0
Passerelle par défaut. . . . . : 192.168.1.1
Serveur DHCP . . . . . : 192.168.1.1
IAID DHCPv6 . . . . . : 268216852
DUID de client DHCPv6. . . . . : 00-01-00-01-27-51-18-51-FC-AA-14-24-82-7B
Serveurs DNS. . . . . : 192.168.1.1
NetBIOS sur Tcpip. . . . . : Activé

```

Configuration addresses IP – interface

```

Enter an option: 2

```

Configuration addresses IP – interface

```
Configure IPv6 address WAN interface via DHCP6? (y/n) N
Enter the new WAN IPv6 address. Press <ENTER> for none:
>

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 192.168.1.250/24

Press <ENTER> to continue.
```

Configuration addresses IP – interface

```
Available interfaces:

1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - static)
3 - OPT1 (em2)

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

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

Enter the new WAN IPv4 address. Press <ENTER> for none:
> 192.168.1.250

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 WAN IPv4 subnet bit count (1 to 31):
> 24

For a WAN, enter the new WAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
> 192.168.1.1
```

Configuration addresses IP – interface

```
Do you want to enable the DHCP server on LAN? (y/n) y
Enter the start address of the IPv4 client address range: 172.20.0.20
Enter the end address of the IPv4 client address range: 172.20.0.40

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

The IPv4 LAN address has been set to 172.20.0.250/24
You can now access the webConfigurator by opening the following URL in your web
browser:
http://172.20.0.250/

Press <ENTER> to continue.
```

Configuration addresses IP – interface

```
Enter an option: 2
Available interfaces:
1 - WAN (em0 - static)
2 - LAN (em1 - static)
3 - OPT1 (em2)
Enter the number of the interface you wish to configure: 2
Enter the new LAN IPv4 address. Press <ENTER> for none:
> 172.20.0.250
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 31):
> 24
For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
> █
```

*Configuration addresses IP – interface*

```
Enter the new OPT1 IPv6 address. Press <ENTER> for none:
>
Do you want to enable the DHCP server on OPT1? (y/n) n
Please wait while the changes are saved to OPT1...
Reloading filter...
Reloading routing configuration...
DHCPD...
The IPv4 OPT1 address has been set to 192.168.2.250/24
Press <ENTER> to continue. █
```

*Configuration addresses IP – interface*

## PARTIE 2 – CONFIGURATION DE BASE

### 7. Test de la connectivité

Depuis la machine Active Directory, on vérifie la connectivité vers PfSense et vers Internet :

**PS C:\> ping 192.168.1.250** → Test vers l'interface WAN de PfSense

**PS C:\> ping 172.20.0.250** → Test vers l'interface LAN de PfSense

**PS C:\> ping 192.168.2.250** → Test vers l'interface OPT1 de PfSense

**PS C:\> ping 192.168.1.1** → Test vers la passerelle de la box internet

**PS C:\> ping 8.8.4.4** → Test de la connexion vers Internet

**PS C:\> ping www.google.fr** → Test de la résolution DNS

### 8. Assistant de configuration (Setup Wizard)

On accède à l'interface web de PfSense depuis la machine AD :

```
http://172.20.0.250 Login : admin | Mot de passe : pfsense
```

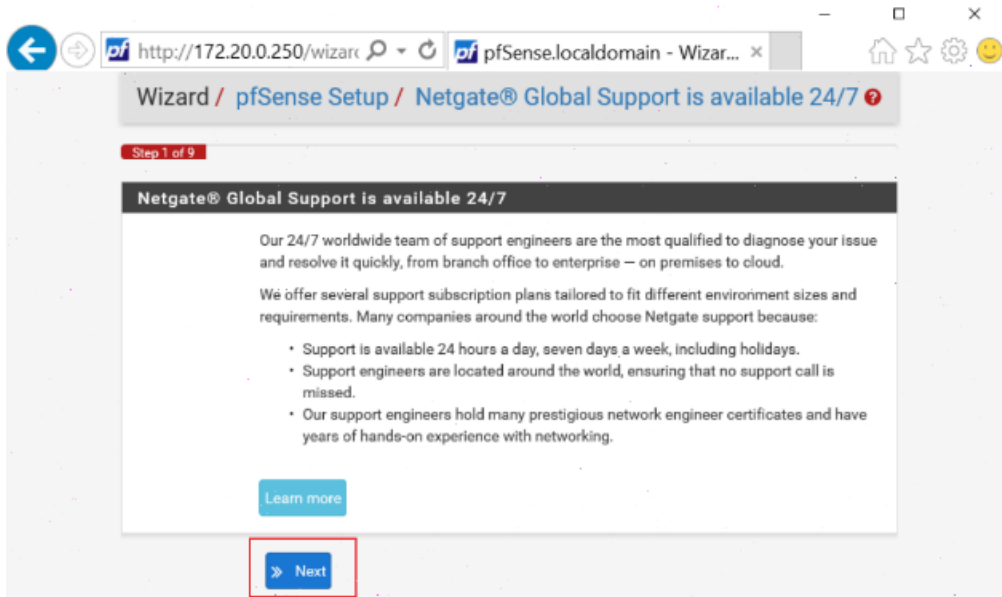
Un assistant en 9 étapes se lance automatiquement. Les éléments importants à configurer :

- Nom du serveur : **heimdall**
- Nom de domaine : **sitka.local**
- Serveur NTP : **fr.pool.ntp.org**
- Fuseau horaire : **Europe/Paris**
- Vérification des interfaces WAN et LAN (déjà configurées)
- Changement du mot de passe administrateur
- Cliquer sur **Reload** puis **Finish**

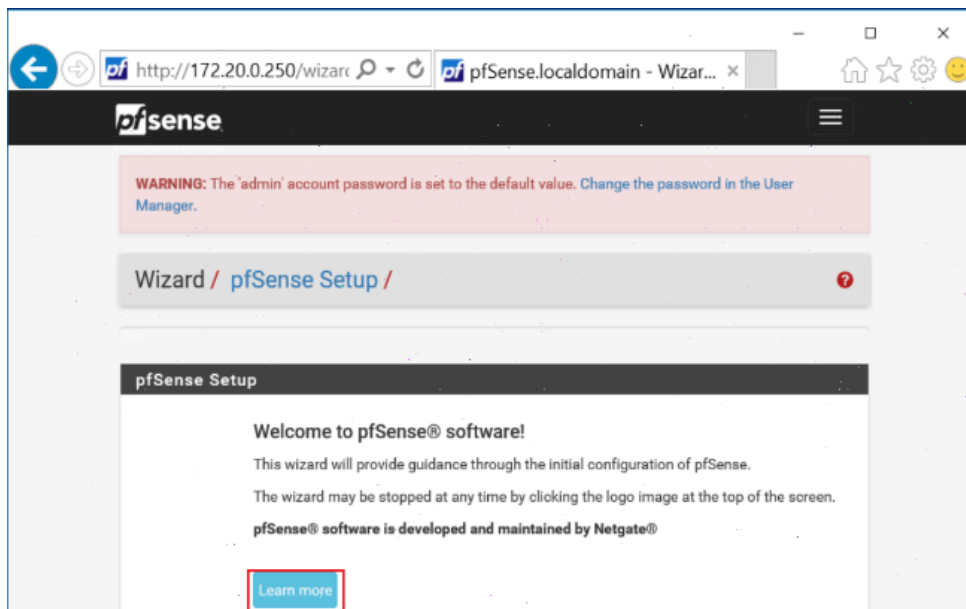
En cas d'erreur, le Wizard peut être relancé via : **Système** → **Setup Wizard**.



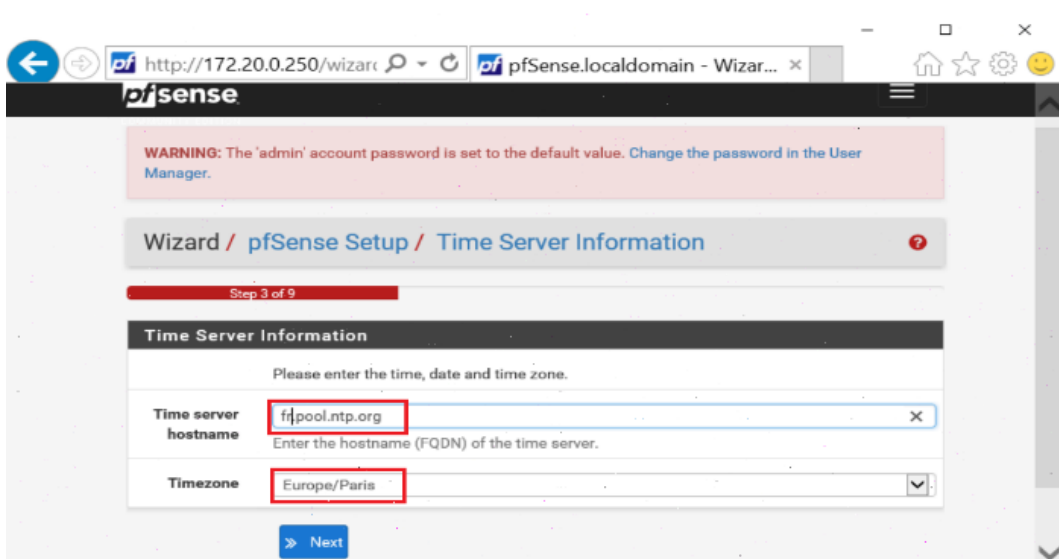
*Assistant de configuration PfSense – étape 1*



Assistant de configuration PfSense – étape 2



Assistant de configuration PfSense – étape 3



Assistant de configuration PfSense – étape 4

pfSense System Interfaces Firewall Services VPN Status Diagnostics Help

Wizard / pfSense Setup / General Information ?

Step 2 of 9

### General Information

On this screen the general pfSense parameters will be set.

**Hostname**  x  
EXAMPLE: myserver

**Domain**   
EXAMPLE: mydomain.com

The default behavior of the DNS Resolver will ignore manually configured DNS servers for client queries and query root DNS servers directly. To use the manually configured DNS servers below for client queries, visit Services > DNS Resolver and enable DNS Query Forwarding after completing the wizard.

**Primary DNS Server**

**Secondary DNS Server**

**Override DNS**   
Allow DNS servers to be overridden by DHCP/PPP on WAN

[» Next](#)

Assistant de configuration PfSense – étape 5

pfSense

WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Wizard / pfSense Setup / Configure LAN Interface ?

Step 5 of 9

### Configure LAN Interface

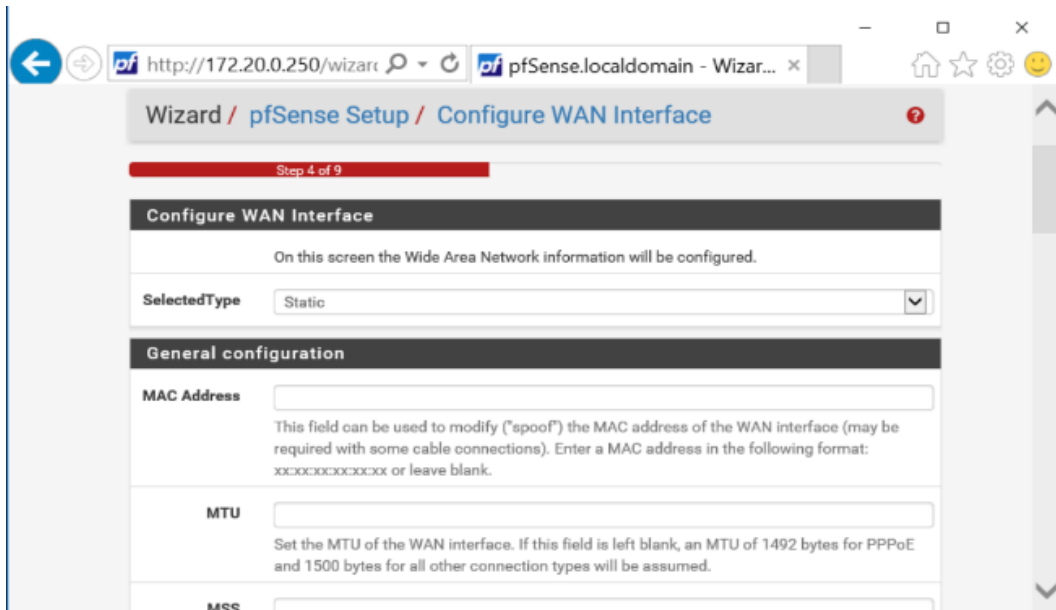
On this screen the Local Area Network information will be configured.

**LAN IP Address**   
Type dhcp if this interface uses DHCP to obtain its IP address.

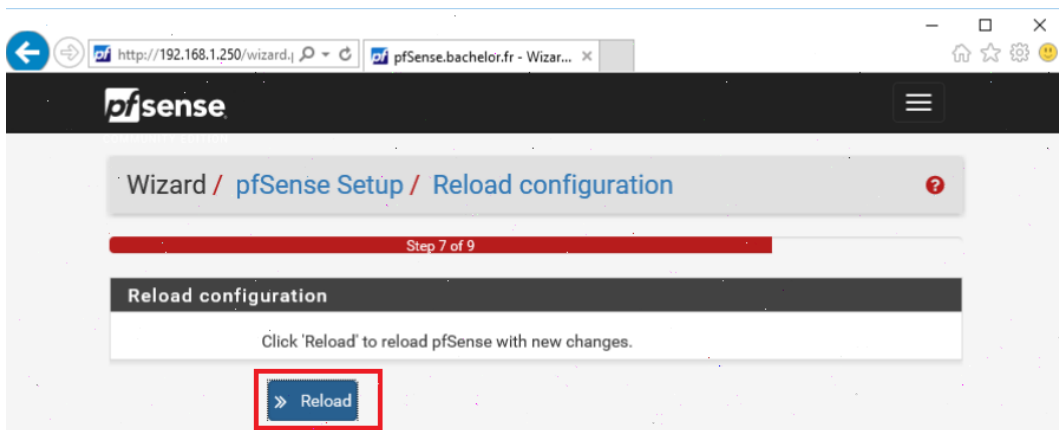
**Subnet Mask**

[» Next](#)

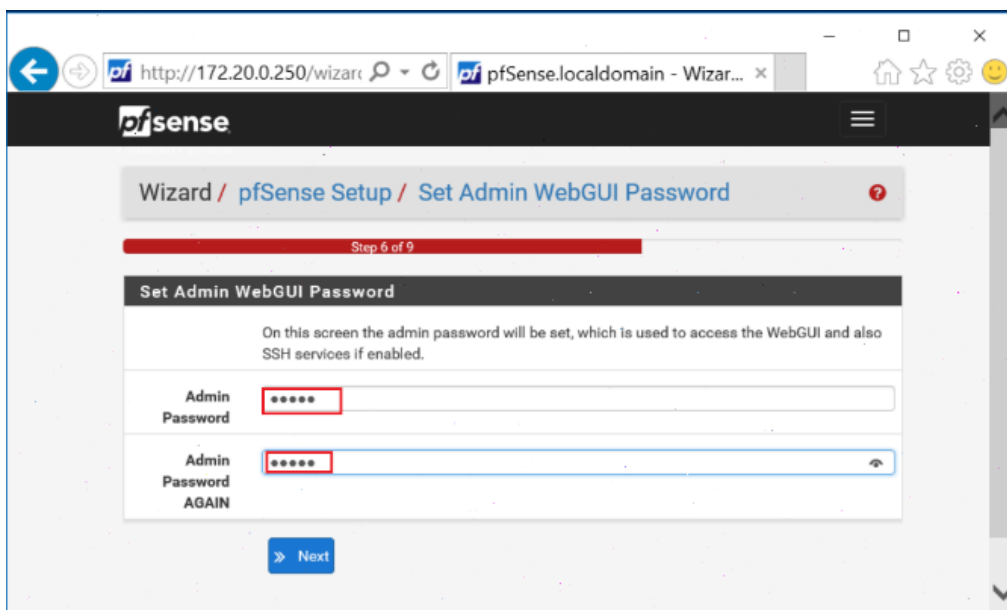
Assistant de configuration PfSense – étape 6



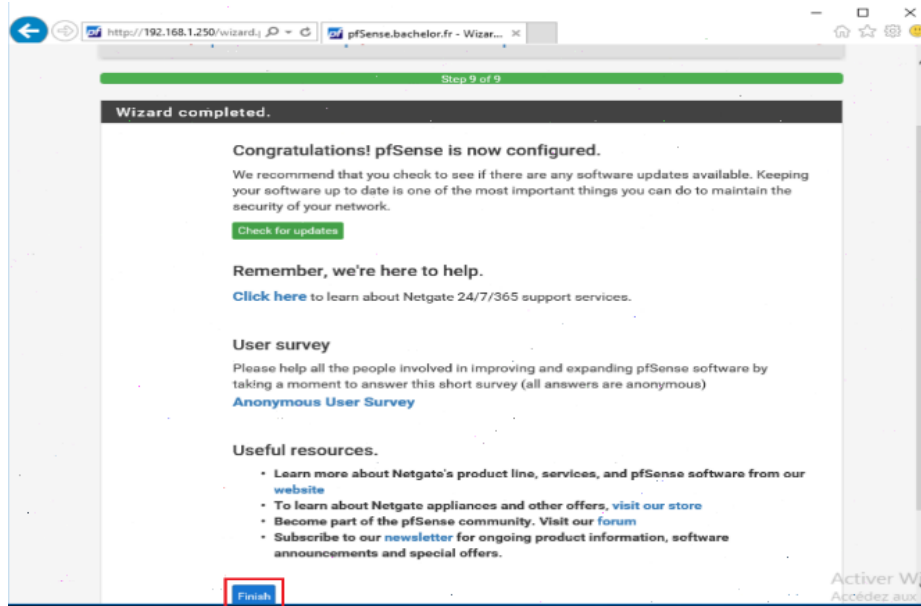
Assistant de configuration PfSense – étape 7



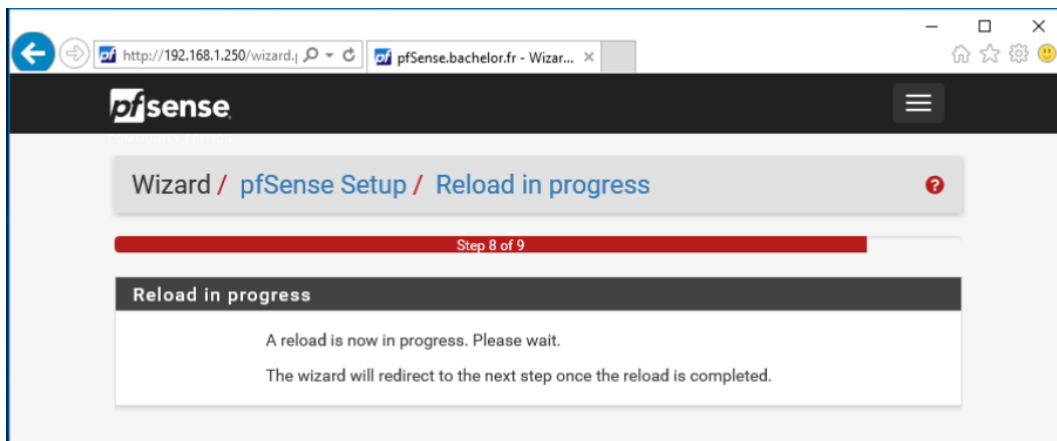
Assistant de configuration PfSense – étape 8



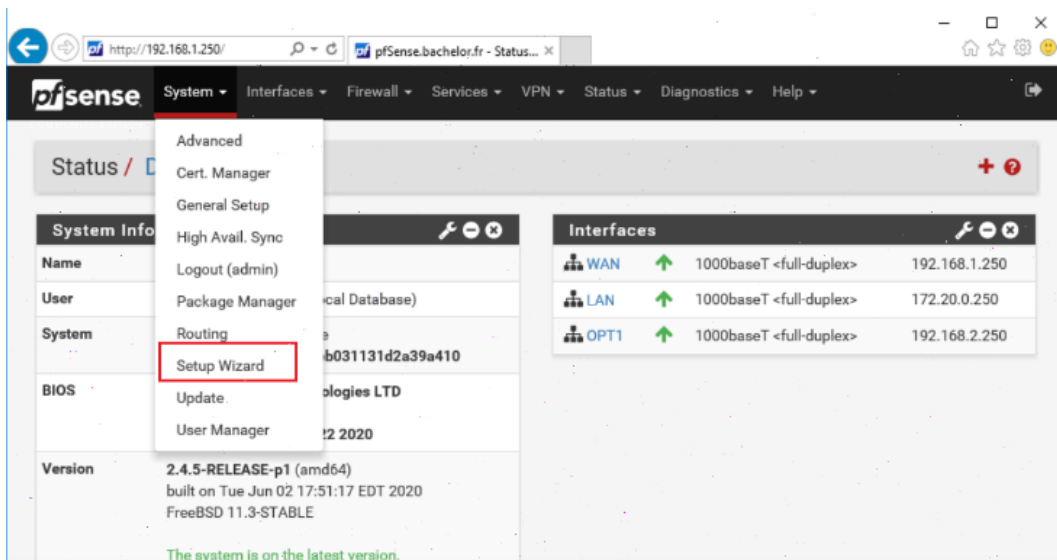
Assistant de configuration PfSense – étape 9



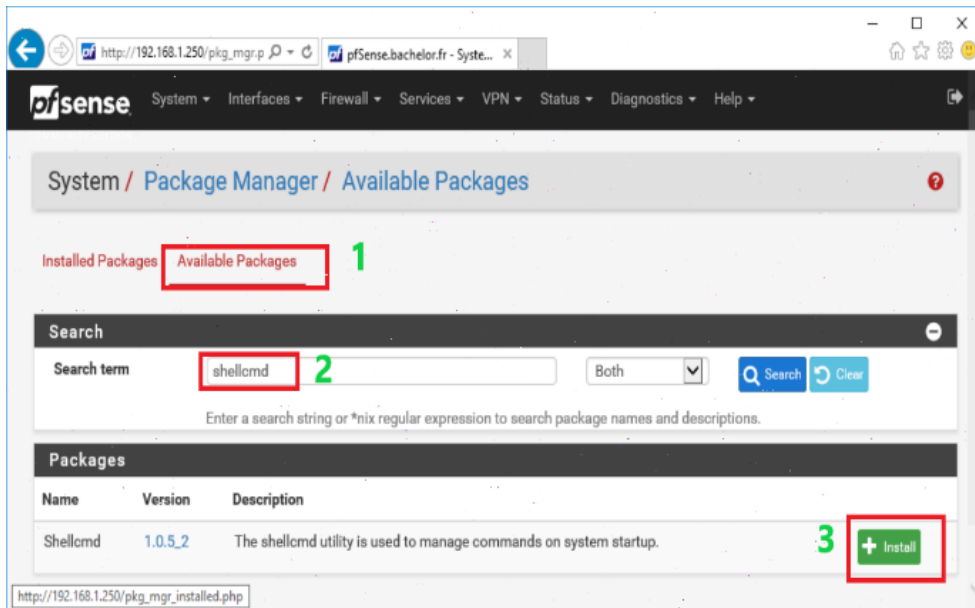
Assistant de configuration PfSense – étape 10



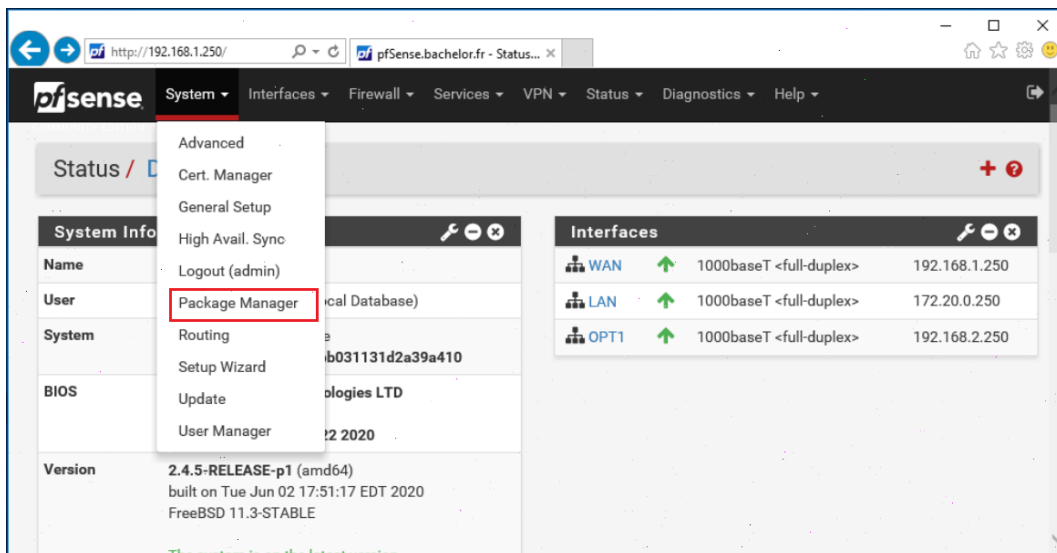
Assistant de configuration PfSense – étape 11



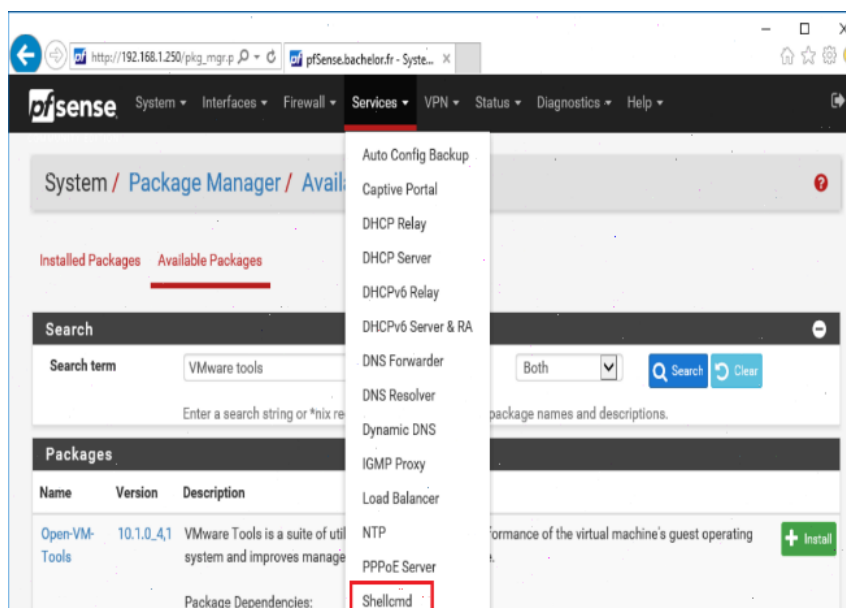
Assistant de configuration PfSense – étape 12



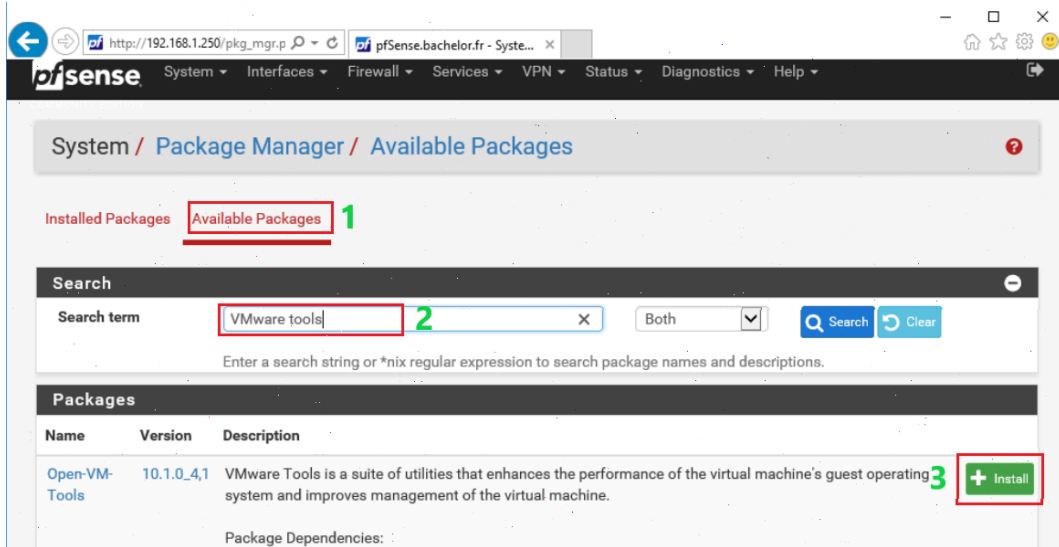
Assistant de configuration PfSense – étape 13



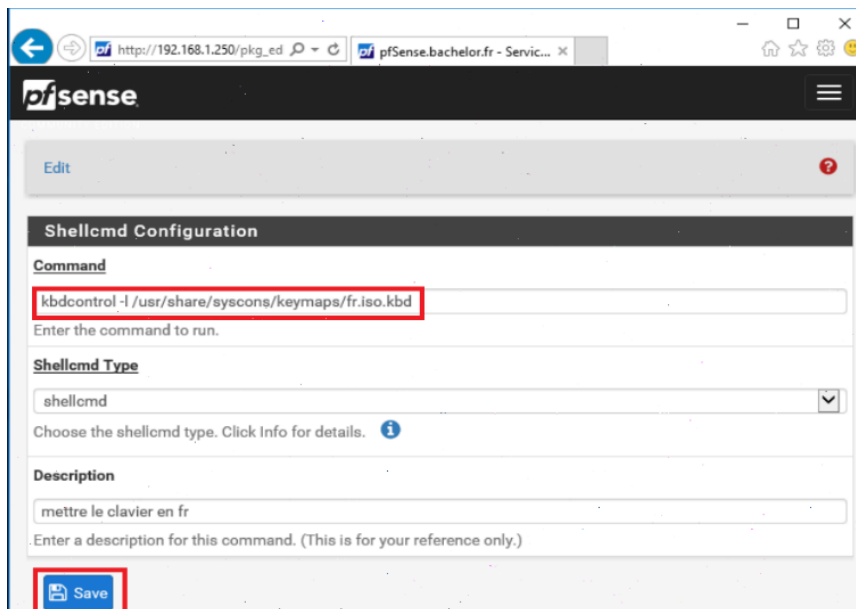
Assistant de configuration PfSense – étape 14



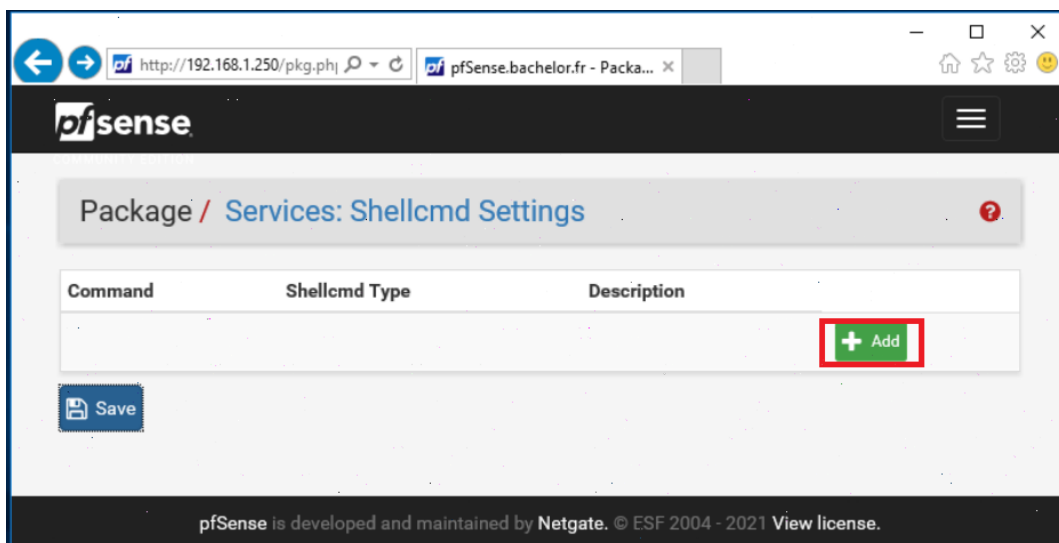
Assistant de configuration PfSense – étape 15



Assistant de configuration PfSense – étape 16



Assistant de configuration PfSense – étape 17



Assistant de configuration PfSense – étape 18

## 9. Configuration permanente du clavier et des outils VMware

Pour configurer le clavier en AZERTY de façon permanente, on installe les paquets **shellcmd** et **VMware Tools** via **Système** → **Package Manager**.

Dans le champ commande de shellcmd, on ajoute :

```
kbdcontrol -l /usr/share/syscons/keymaps/fr.iso.kbd
```

Après redémarrage, le clavier doit être en AZERTY.

## PARTIE 3 – SÉCURITÉ DE PFSENSE

### 10. Sécurisation de la console par mot de passe

Pour protéger la console physique de PfSense par un mot de passe, aller dans **Système** → **Avancé** → **Admin Access** et cocher la case **Console menu**. Sauvegarder les modifications. Désormais, un login sera requis pour accéder à la console.



*Activation de la protection de la console par mot de passe*

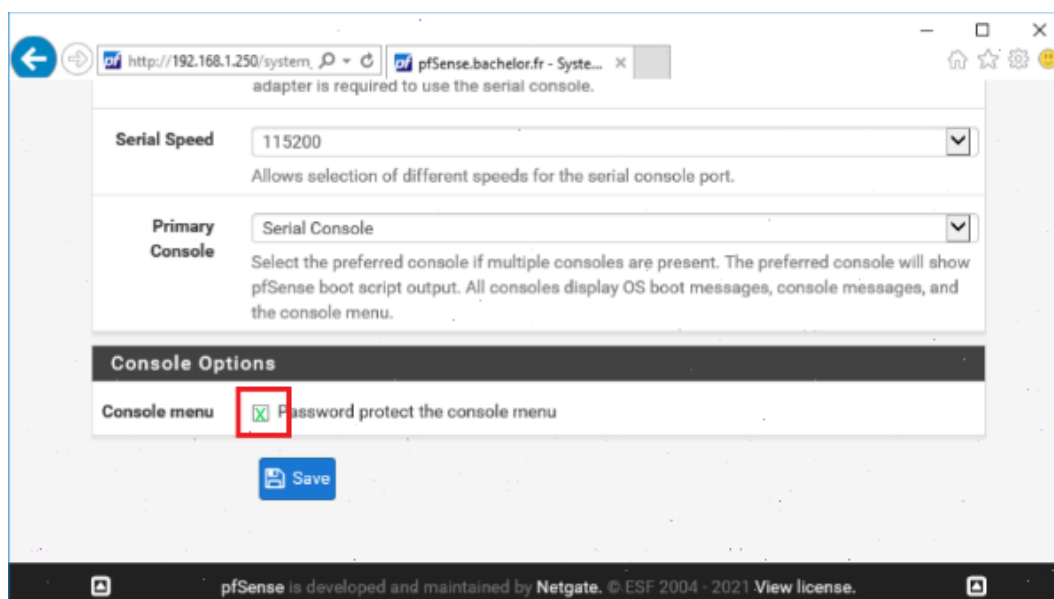
### 11. Sécurisation de l'accès SSH

On active SSH pour accéder à la console de manière sécurisée. Il est recommandé de changer le port par défaut (22) pour un port personnalisé, par exemple **2121**. On peut aussi opter pour une authentification par clé publique/privée.

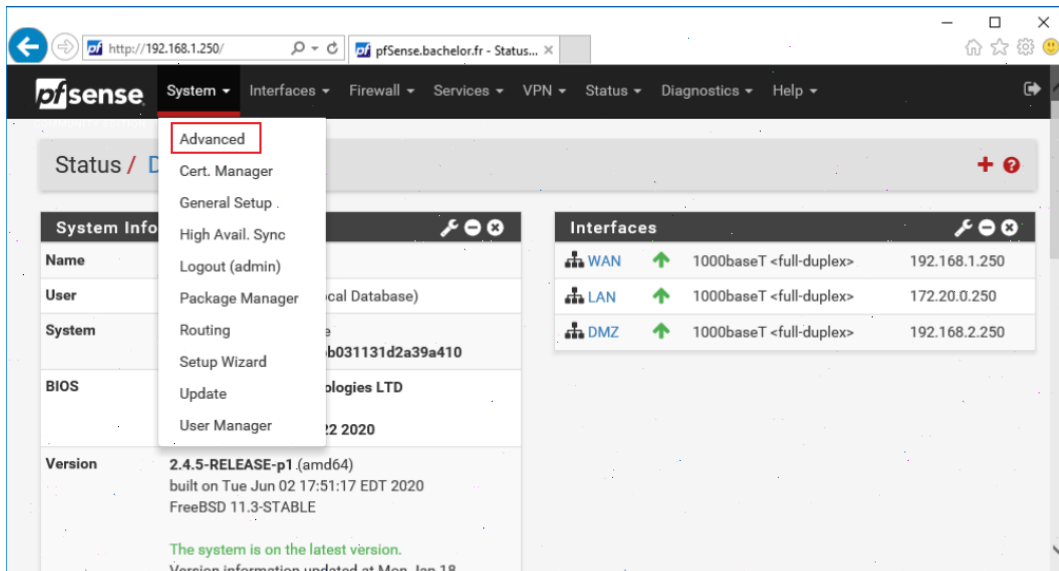
■ ■ Sur Windows Server 2016, SSH n'est pas installé nativement. Il est disponible nativement sur Windows 2019 et Windows 10.

**Créer une règle autorisant SSH sur l'interface WAN :**

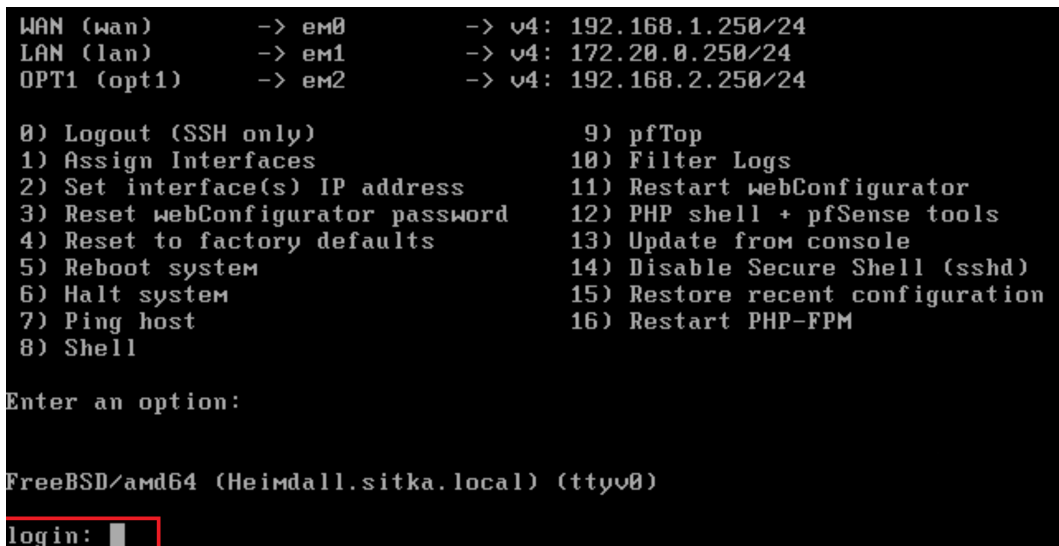
Aller dans **Firewall** → **Rules** → **WAN** → **Add** et renseigner les paramètres pour autoriser le port SSH configuré (2121). Enregistrer et appliquer les changements.



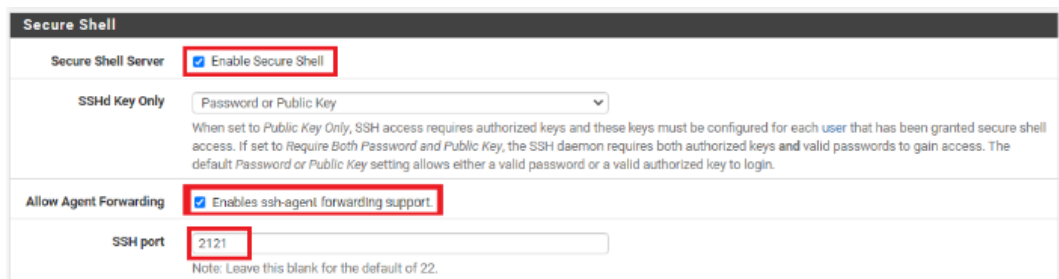
*Configuration SSH – capture 1*



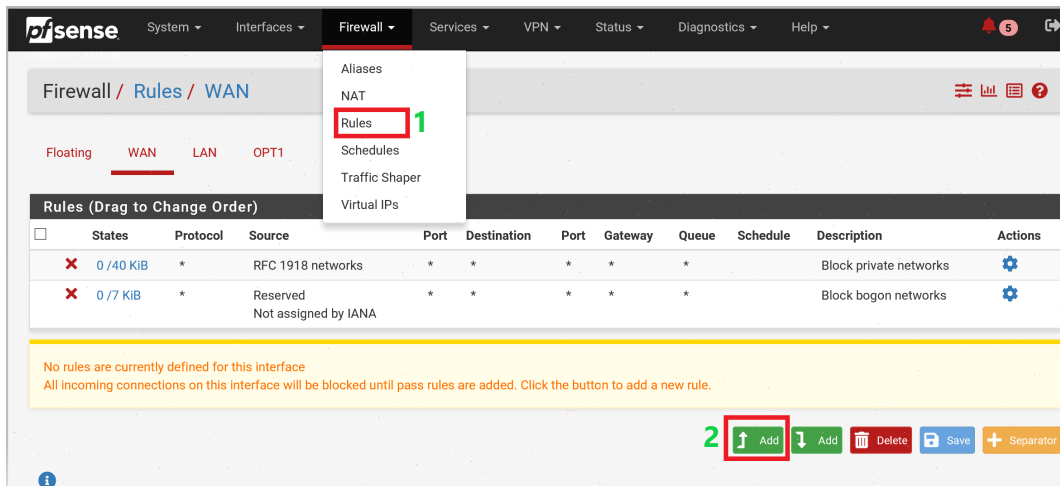
Configuration SSH – capture 2



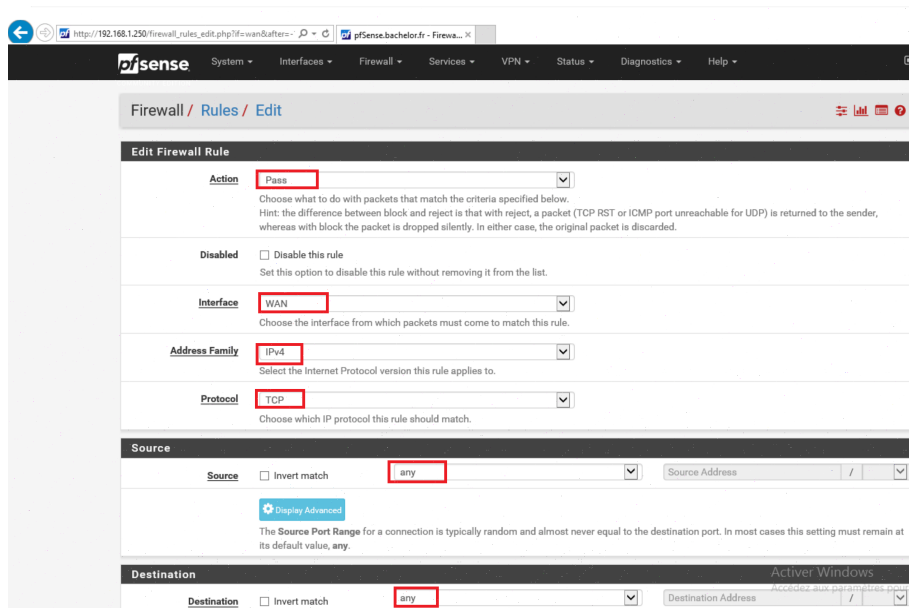
Configuration SSH – capture 3



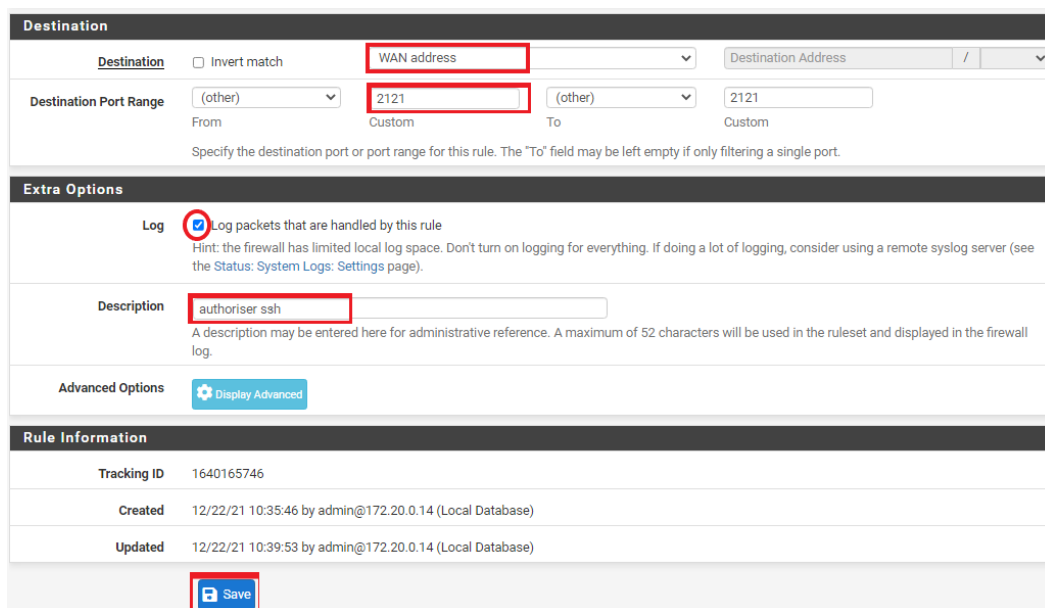
Configuration SSH – capture 4



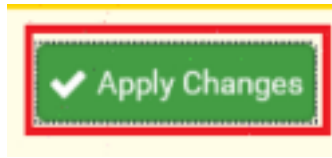
Configuration SSH – capture 5



Configuration SSH – capture 6



Configuration SSH – capture 7



Configuration SSH – capture 8



Configuration SSH – capture 9

## Test de connexion SSH

Pour tester la connexion depuis l'intérieur du réseau, depuis la machine AD :

```
ssh admin@172.20.0.250 -p 2121
```

Pour une connexion depuis l'extérieur (via l'adresse publique), il faut : • Ouvrir le port sur la box internet (redirection de port) • Utiliser son adresse IP publique (vérifiable sur <http://www.whatismyip.com>) • Se mettre en 4G sur smartphone (pas en Wi-Fi du même réseau) • Utiliser un client SSH mobile comme JuiceSSH

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
0/0 B	*	RFC 1918 networks	*	*	*	*	*	*	Block private networks	⚙️
0/247 KIB	*	Reserved Not assigned by IANA	*	*	*	*	*	*	Block bogon networks	⚙️
0/0 B	IPv4 TCP	*	*	WAN net	22 (SSH)	*	none		Laisser passé ssh	📌 🔄 🗑️

Test de connexion SSH

```

PS C:\Users\Administrateur> ssh admin@172.20.0.250 -p 2121
The authenticity of host '[172.20.0.250]:2121 ([172.20.0.250]:2121)' can't be established.
ED25519 key fingerprint is SHA256:riqHfD03Z9fhNsyAM1TC2shBu9F6+qSnpoKCTL/0dTo.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[172.20.0.250]:2121' (ED25519) to the list of known hosts.
Password for admin@heimdall.sitka.local:
VMware Virtual Machine - Netgate Device ID: 7c7777e1ee8ed9111e66

*** Welcome to pfSense 2.5.2-RELEASE (amd64) on heimdall ***

WAN (wan)      -> em0      -> v4: 192.168.1.250/24
LAN (lan)     -> em1      -> v4: 172.20.0.250/24
OPT1 (opt1)   -> em2      -> v4: 192.168.2.250/24

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:

```

Test de connexion SSH

```

Enter an option: 8
[2.5.2-RELEASE][admin@heimdall.sitka.local]/root: su root
# cd /etc/ssh
# ls
moduli          ssh_host_ed25519_key.pub  sshd_config
ssh_config      ssh_host_rsa_key
ssh_host_ed25519_key  ssh_host_rsa_key.pub
# ssh-keygen -lvf ssh_host_ed25519_key.pub
256 SHA256:riqHfD03Z9fhNsyAM1TC2shBu9F6+qSnpoKCTL/0dTo root@heimdall.sitka.local
(ED25519)
+---[ED25519 256]---+
|..                |
|..oo..            |
|..o=.o            |
|..++o             |
|..o..S..          |
|..oo..            |
|..=..o..+..*..    |
|..=.B++E=.B      |
|..B=O+=..        |
+---[SHA256]-----+

```

Test de connexion SSH

```

Windows PowerShell
PS C:\> ssh admin@192.168.1.250
ssh: connect to host 192.168.1.250 port 22: Connection timed out
PS C:\>

```

Test de connexion SSH

## 12. Sécurisation de l'interface web par HTTPS

### 12.1 Création d'une autorité de certification interne

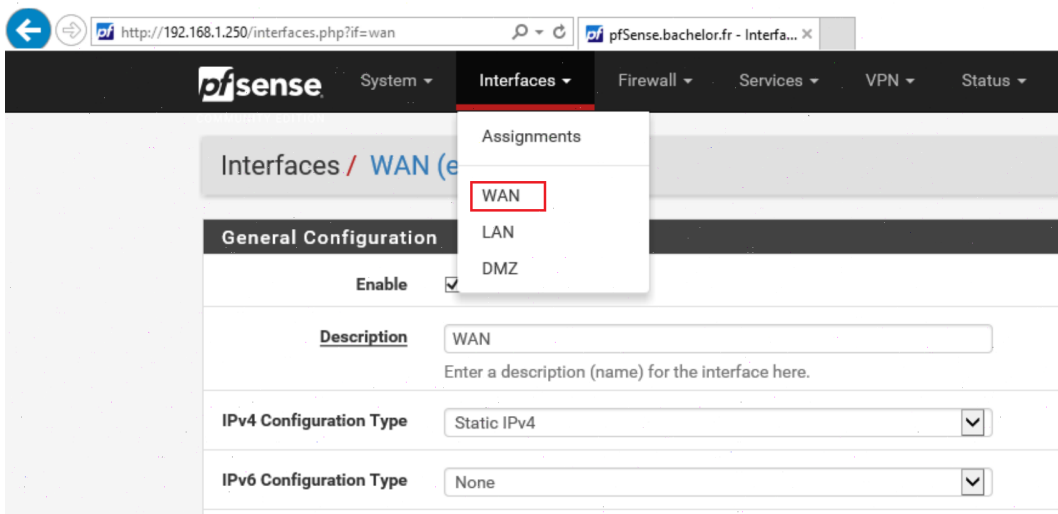
Aller dans **Système** → **Cert Manager** et créer une nouvelle autorité de certification interne en remplissant les champs requis (nom, pays, organisation, etc.).

```
Windows PowerShell
PS C:\> ping 192.168.1.250

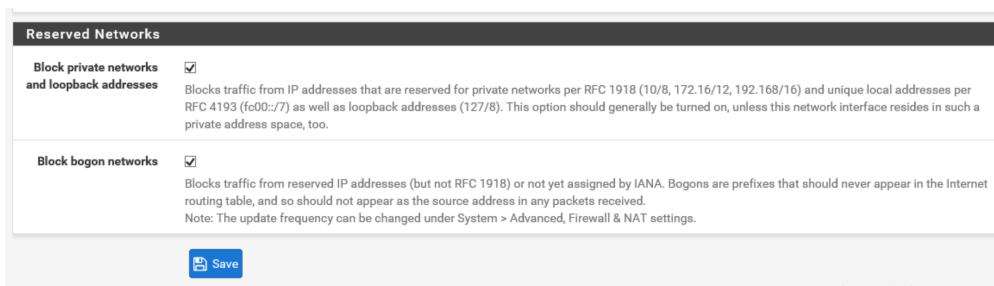
Envoi d'une requête 'Ping' 192.168.1.250 avec 32 octets de données :
Réponse de 192.168.1.156 : Impossible de joindre l'hôte de destination.
Réponse de 192.168.1.156 : Impossible de joindre l'hôte de destination.
Réponse de 192.168.1.156 : Impossible de joindre l'hôte de destination.
Réponse de 192.168.1.156 : Impossible de joindre l'hôte de destination.

Statistiques Ping pour 192.168.1.250:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
PS C:\>
```

Création de l'autorité de certification



Création de l'autorité de certification



Création de l'autorité de certification

## 12.2 Génération du certificat web

Créer un certificat web signé par l'autorité de certification interne créée à l'étape précédente. Cliquer sur **Add** et remplir les champs nécessaires (CN, SAN, durée de validité, etc.).

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✗ 0/0 B	*	RFC 1918 networks	*	*	*	*	*	*	Block private networks	⚙️
✗ 0/138 KiB	*	Reserved Not assigned by IANA	*	*	*	*	*	*	Block bogon networks	⚙️
☑ 0/326 KiB	IPv4 TCP	*	*	WAN net	22 (SSH)	*	none			🔗 📄 🗑️

Génération du certificat web

Service	Adresse IP du serveur	Protocole	Ports externes	Ports internes	Activer la règle
Utilisateur					
SSH	192.168.1.250	TCP/UDP	22 • 22	22 • 22	on

Génération du certificat web



Génération du certificat web

## 12.3 Injection du certificat dans PfSense

Aller dans **Systeme** → **Avancé** et configurer :

- Sélectionner le certificat créé
- Conserver le port HTTPS par défaut
- Limiter à 2 connexions simultanées maximum
- Refuser les connexions en HTTP non sécurisé
- Interdire au navigateur d'enregistrer les données de connexion

Après sauvegarde, se connecter via : **https://172.20.0.250**

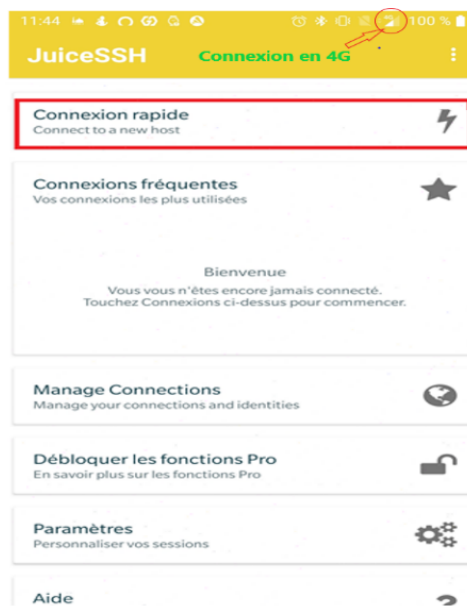
Le navigateur affichera un avertissement de certificat car l'autorité de certification interne n'est pas dans le magasin de confiance. Pour résoudre ce problème, il faut importer le certificat de l'autorité racine dans le système.

# JuiceSSH - SSH Client

Configuration HTTPS et injection du certificat



Configuration HTTPS et injection du certificat



Configuration HTTPS et injection du certificat

# PARTIE 4 – AUTHENTIFICATION LDAP ET LDAPS

## 13. Test de connectivité LDAP/LDAPS sur Active Directory

### 13.1 Connectivité LDAP (port 389)

Sur le contrôleur de domaine hermes, tester la connectivité LDAP standard en ouvrant **ldp.exe** (clic droit sur Démarrer → Exécuter → ldp.exe). Se connecter avec le nom du serveur **hermes.sitka.local** et le port **389**.

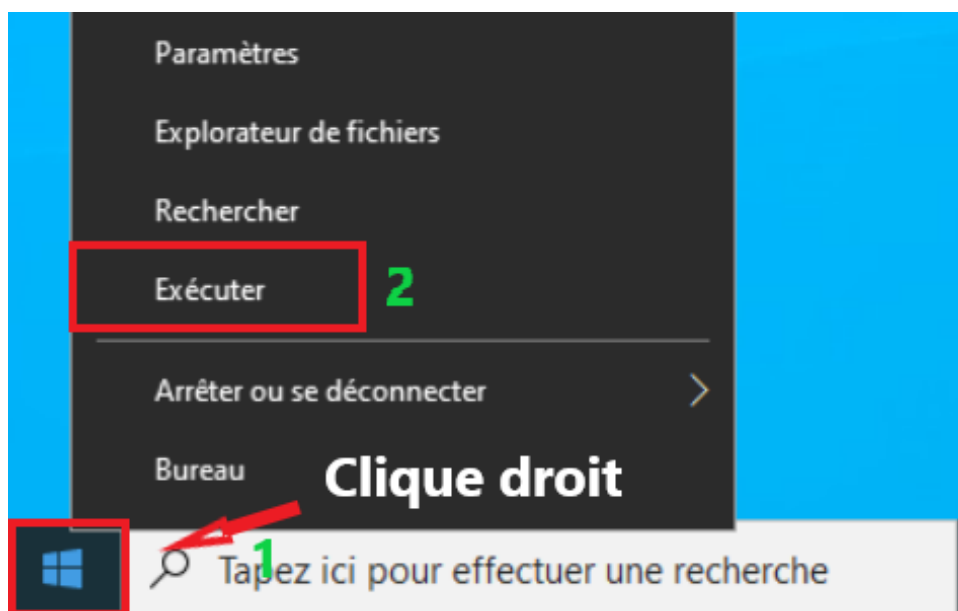


*Test de connectivité LDAP standard via ldp.exe*

### 13.2 Connectivité LDAPS (port 636, SSL)

Même procédure que LDAP mais avec le port **636** et la case **SSL** cochée. Un message d'erreur apparaîtra car le contrôleur de domaine ne possède pas encore de certificat pour LDAPS.

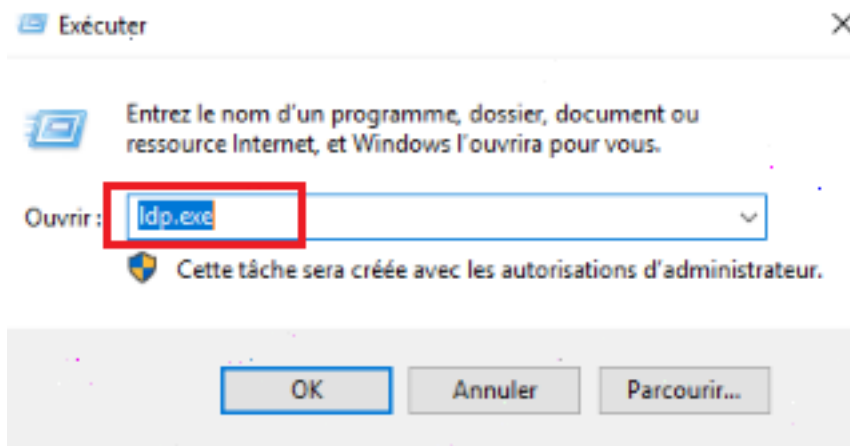
Il existe deux méthodes pour activer LDAPS sur un contrôleur de domaine : • Installer une autorité de certification racine sur hermes (méthode retenue ici) • Utiliser un certificat tiers



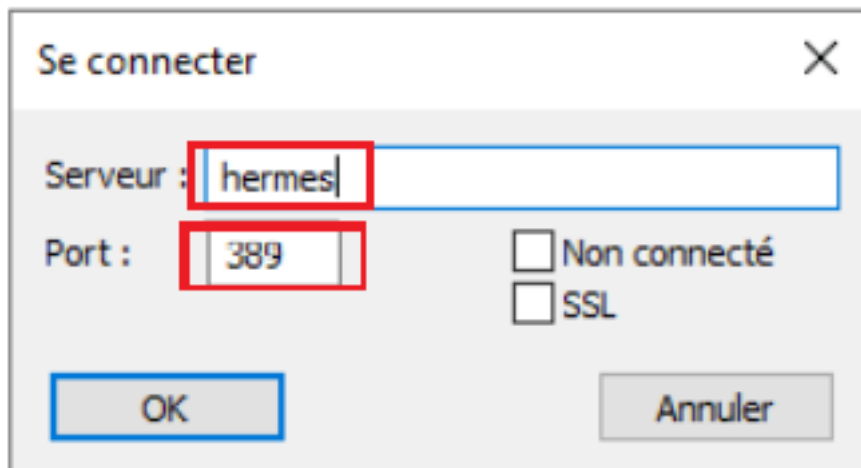
## 14. Création d'une autorité de certification sur hermes

### 14.1 Ajout du rôle Certificats Active Directory

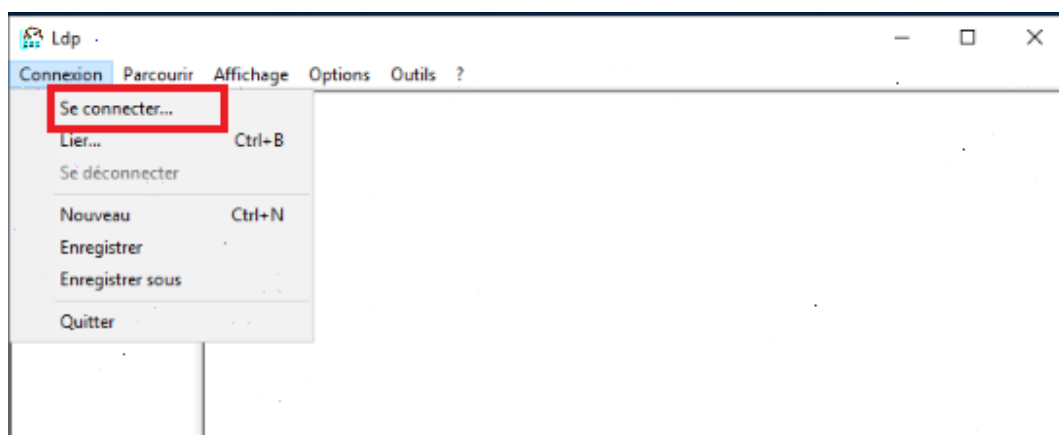
Accéder au **Gestionnaire de serveur** → **Gérer** → **Ajouter des rôles et fonctionnalités**. Cocher **Services de Certificats Active Directory**. Sélectionner uniquement **Autorité de certification**.



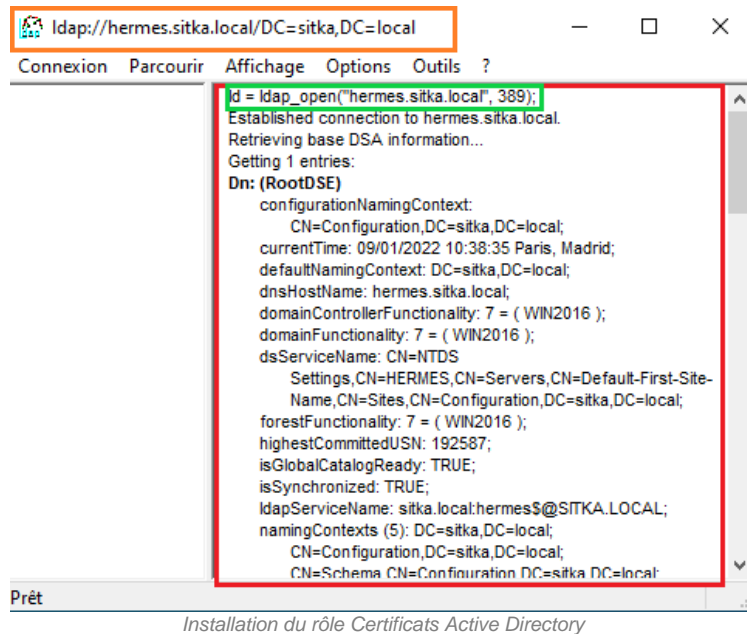
Installation du rôle Certificats Active Directory



Installation du rôle Certificats Active Directory



Installation du rôle Certificats Active Directory

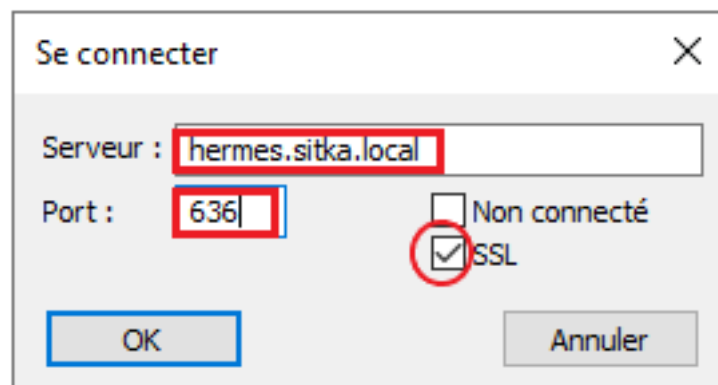


## 14.2 Configuration de l'autorité de certification

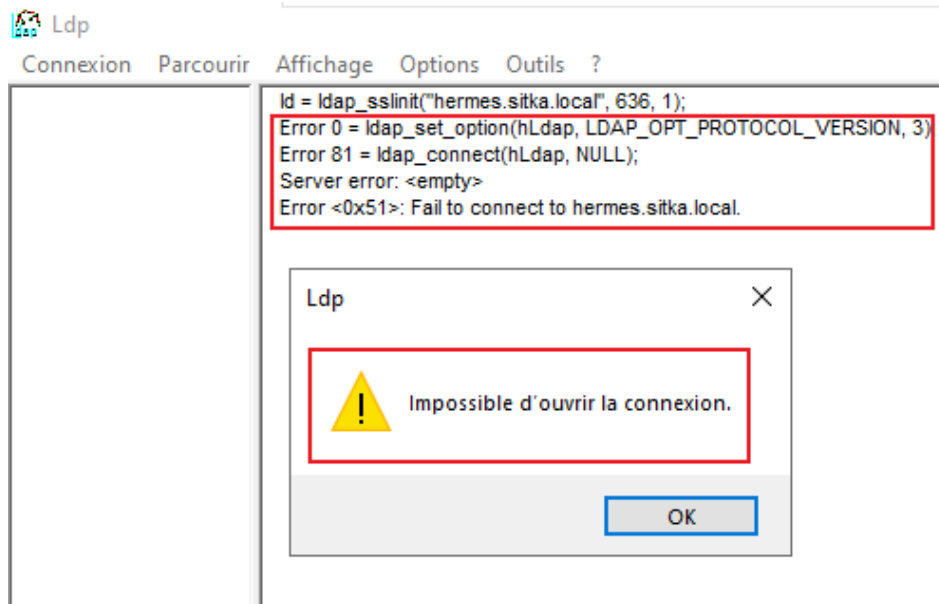
Une fois le rôle installé, le configurer avec les paramètres suivants :

- Vérifier les informations d'identification (compte Administrateur du domaine obligatoire)
- Cocher **Autorité de certification**
- Sélectionner **Autorité de certification d'entreprise**
- Sélectionner **Autorité de certification racine**
- Créer une nouvelle clé privée
- Choisir les algorithmes de chiffrement (RSA 2048 bits recommandé)
- Définir le nom commun : **hermes-CA**
- Définir la période de validité (doit être supérieure aux certificats émis)
- Laisser les dossiers par défaut pour les bases de données

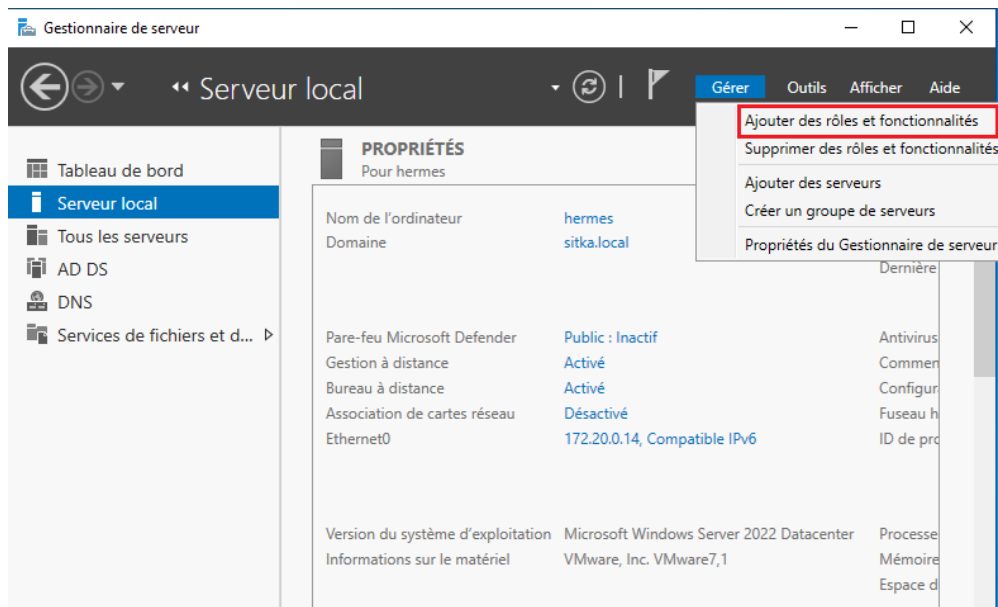
■■ Ce type d'autorité de certification couplé à Active Directory est adapté pour un intranet mais est déconseillé pour un accès public.



Configuration de l'autorité de certification hermes-CA



Configuration de l'autorité de certification hermes-CA



Configuration de l'autorité de certification hermes-CA

Assistant Ajout de rôles et de fonctionnalités

Sélectionner le type d'installation

SERVEUR DE DESTINATION  
hermes.sitka.local

Avant de commencer

Type d'installation

Sélection du serveur

Rôles de serveurs

Fonctionnalités

Confirmation

Résultats

Sélectionnez le type d'installation. Vous pouvez installer des rôles et des fonctionnalités sur un ordinateur physique ou virtuel en fonctionnement, ou sur un disque dur virtuel hors connexion.

**Installation basée sur un rôle ou une fonctionnalité**  
Configurez un serveur unique en ajoutant des rôles, des services de rôle et des fonctionnalités.

**Installation des services Bureau à distance**  
Installez les services de rôle nécessaires à l'infrastructure VDI (Virtual Desktop Infrastructure) pour déployer des bureaux basés sur des ordinateurs virtuels ou sur des sessions.

< Précédent Suivant > Installer Annuler

Configuration de l'autorité de certification hermes-CA

Assistant Ajout de rôles et de fonctionnalités

Sélectionner le serveur de destination

SERVEUR DE DESTINATION  
hermes.sitka.local

Avant de commencer

Type d'installation

Sélection du serveur

Rôles de serveurs

Fonctionnalités

Confirmation

Résultats

Sélectionnez le serveur ou le disque dur virtuel sur lequel installer des rôles et des fonctionnalités.

Sélectionner un serveur du pool de serveurs

Sélectionner un disque dur virtuel

Pool de serveurs

Filtre :

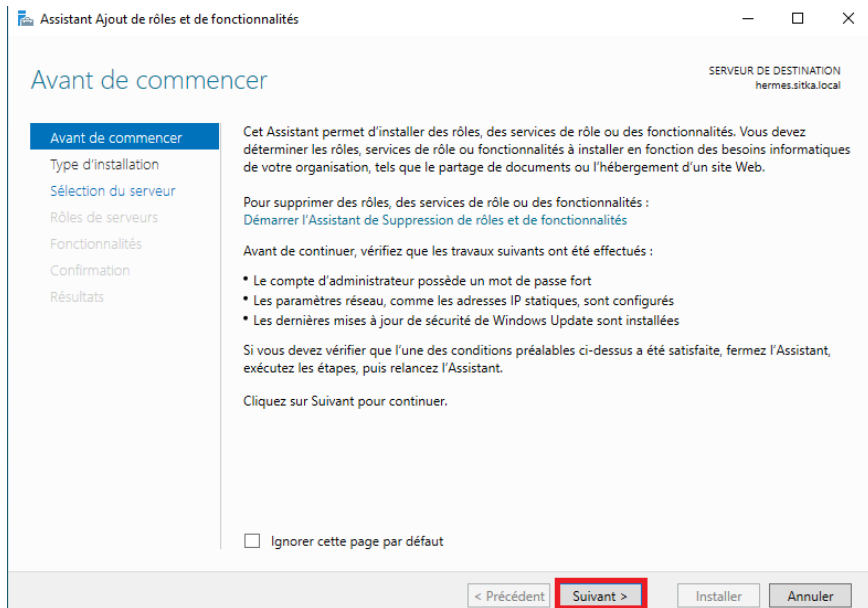
Nom	Adresse IP	Système d'exploitation
hermes.sitka.local	172.20.0.14	Microsoft Windows Server 2022 Datacenter

1 ordinateur(s) trouvé(s)

Cette page présente les serveurs qui exécutent Windows Server 2012 ou une version ultérieure et qui ont été ajoutés à l'aide de la commande Ajouter des serveurs dans le Gestionnaire de serveur. Les serveurs hors connexion et les serveurs nouvellement ajoutés dont la collecte de données est toujours incomplète ne sont pas répertoriés.

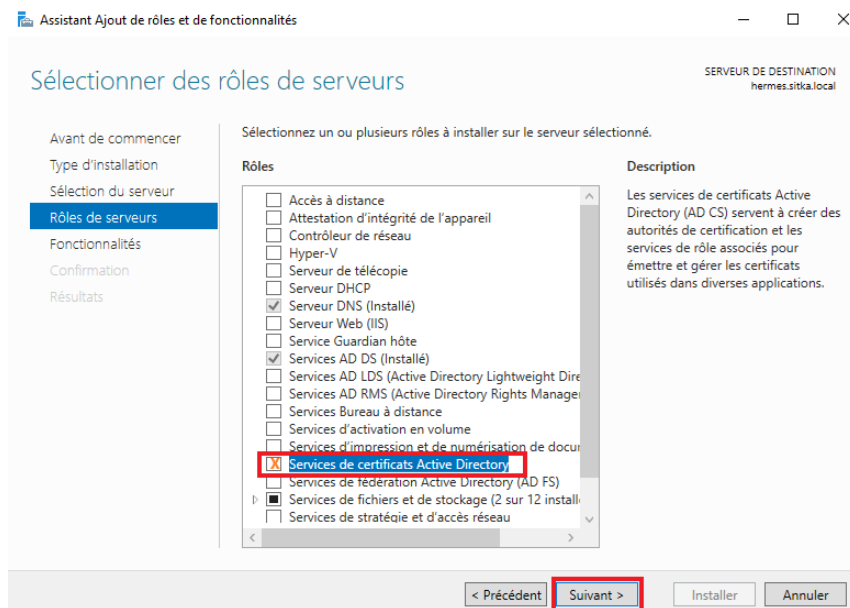
< Précédent Suivant > Installer Annuler

Configuration de l'autorité de certification hermes-CA



Configuration de l'autorité de certification hermes-CA

Retester LDAPS après l'installation de l'autorité de certification : la connexion sur le port 636 doit maintenant fonctionner.

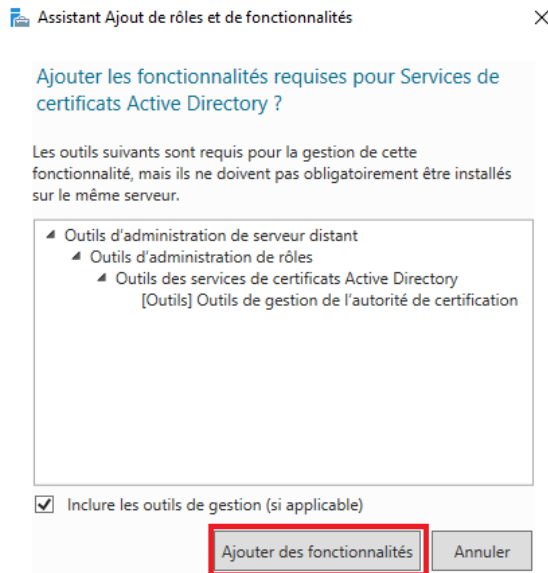


Test LDAPS réussi après installation de l'AC

## 15. Création des comptes utilisateurs Active Directory

Sur le contrôleur de domaine hermes, créer les éléments suivants :

- **Groupe : pfsense** – Groupe contenant les utilisateurs autorisés à se connecter à PfSense
- **Utilisateur : kaiser** – Membre du groupe pfsense
- **Utilisateur : cesar** – Membre du groupe pfsense
- **Utilisateur : pfsensead** – Compte de liaison entre PfSense et Active Directory



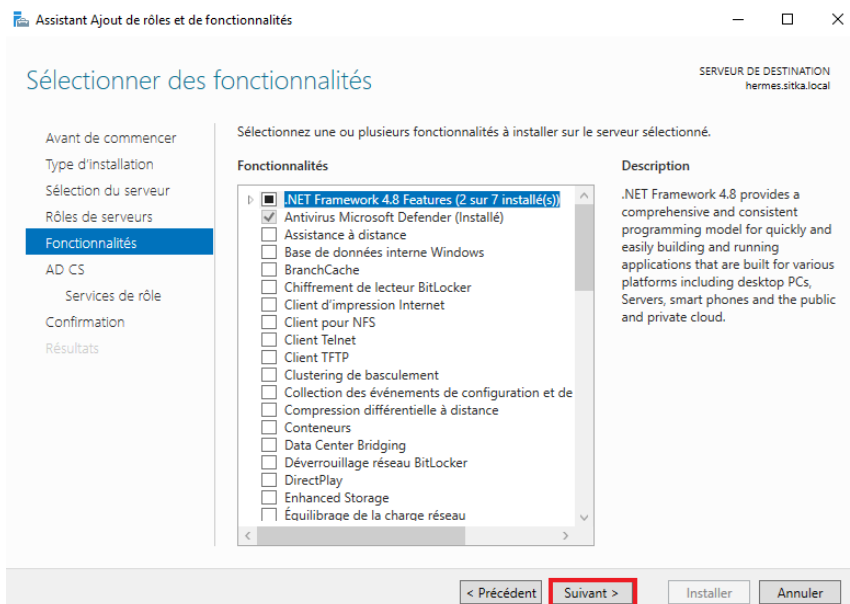
Création des utilisateurs et groupes Active Directory

## 16. Configuration des authentifications LDAP et LDAPS sur PfSense

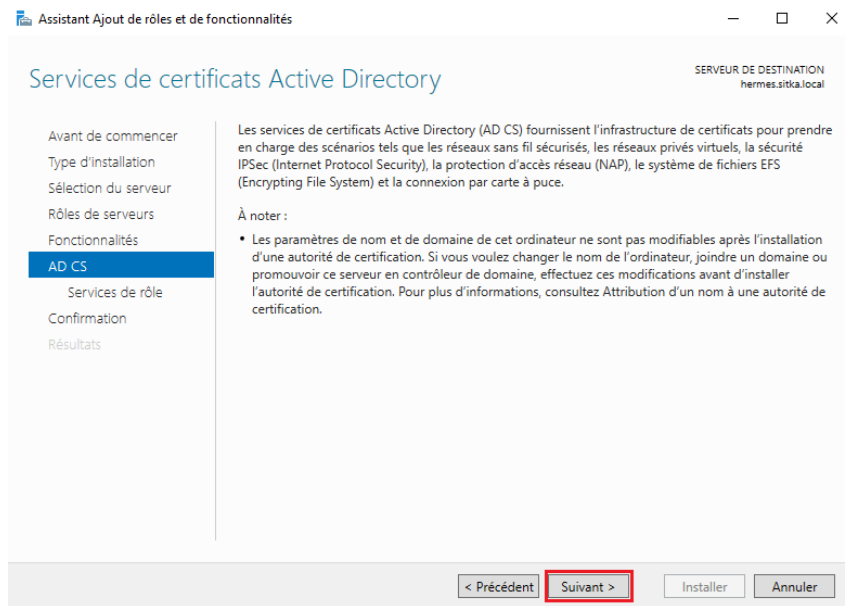
Sur PfSense, aller dans **Système** → **User Manager** → **Authentication Servers** et cliquer sur **Add** pour ajouter un serveur d'authentification.

### 16.1 Authentification LDAP (non chiffrée)

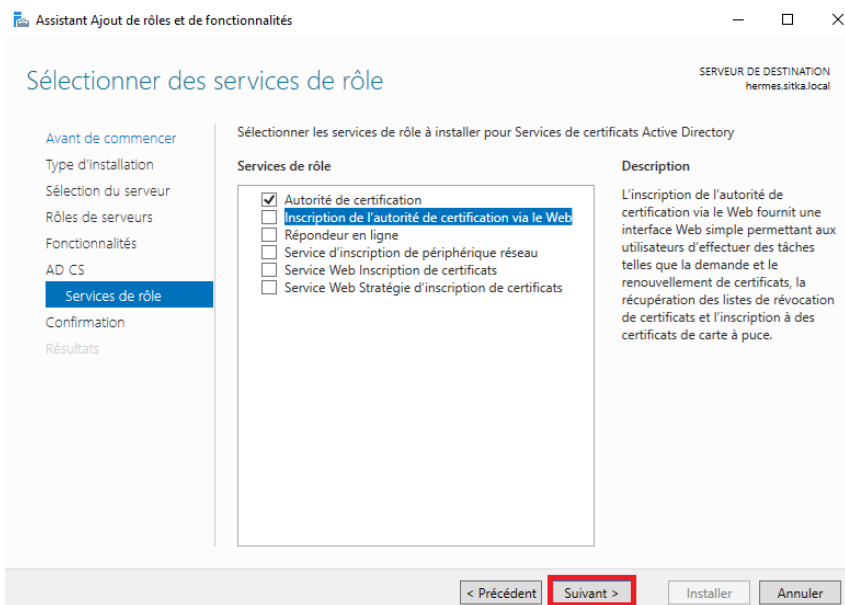
Remplir les champs en utilisant le port **389** pour LDAP standard. Dans le champ **Authentication containers**, taper **cn** puis cliquer sur **Select a container** pour sélectionner l'OU hébergeant les utilisateurs.



Configuration de l'authentification LDAP



Configuration de l'authentification LDAP



Configuration de l'authentification LDAP

## 16.2 Authentification LDAPS (chiffrée SSL)

Même procédure que LDAP, mais avec les différences suivantes :

- Type de transport : **SSL/TLS** • Port : **636**

## Confirmer les sélections d'installation

SERVEUR DE DESTINATION  
hermes.sitka.local

Avant de commencer

Type d'installation

Sélection du serveur

Rôles de serveurs

Fonctionnalités

AD CS

Services de rôle

Confirmation

Résultats

Pour installer les rôles, services de rôle ou fonctionnalités suivants sur le serveur sélectionné, cliquez sur Installer.

 Redémarrer automatiquement le serveur de destination, si nécessaire

Il se peut que des fonctionnalités facultatives (comme des outils d'administration) soient affichées sur cette page, car elles ont été sélectionnées automatiquement. Si vous ne voulez pas installer ces fonctionnalités facultatives, cliquez sur Précédent pour désactiver leurs cases à cocher.

Outils d'administration de serveur distant  
Outils d'administration de rôles  
Outils des services de certificats Active Directory  
Outils de gestion de l'autorité de certification

Services de certificats Active Directory  
Autorité de certification

[Exporter les paramètres de configuration](#)  
[Spécifier un autre chemin d'accès source](#)

&lt; Précédent

Suivant &gt;

Installer

Annuler

Configuration de l'authentification LDAPS

## Progression de l'installation

SERVEUR DE DESTINATION  
hermes.sitka.local

Avant de commencer

Type d'installation

Sélection du serveur

Rôles de serveurs

Fonctionnalités

AD CS

Services de rôle

Confirmation

Résultats

Afficher la progression de l'installation

**i** Installation de fonctionnalité

Configuration requise. Installation réussie sur hermes.sitka.local.

Services de certificats Active Directory  
Des étapes supplémentaires sont nécessaires pour la configuration des services de certificats Active Directory sur le serveur de destination.

**Configurer les services de certificats Active Directory sur le serveur de destination**

Autorité de certification

Outils d'administration de serveur distant  
Outils d'administration de rôles  
Outils des services de certificats Active Directory  
Outils de gestion de l'autorité de certification

**i** Vous pouvez fermer cet Assistant sans interrompre les tâches en cours d'exécution. Examinez leur progression ou rouvrez cette page en cliquant sur Notifications dans la barre de commandes, puis sur Détails de la tâche.

[Exporter les paramètres de configuration](#)

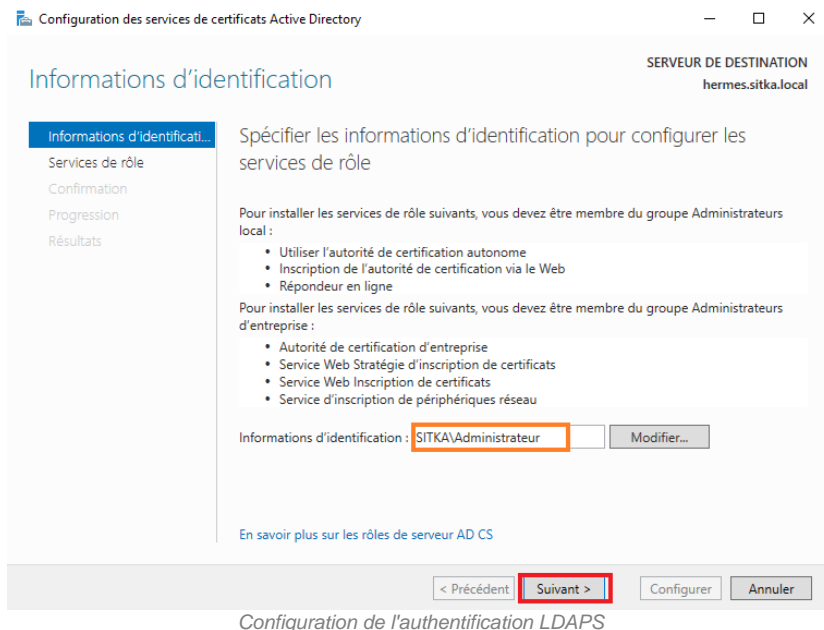
&lt; Précédent

Suivant &gt;

Fermer

Annuler

Configuration de l'authentification LDAPS

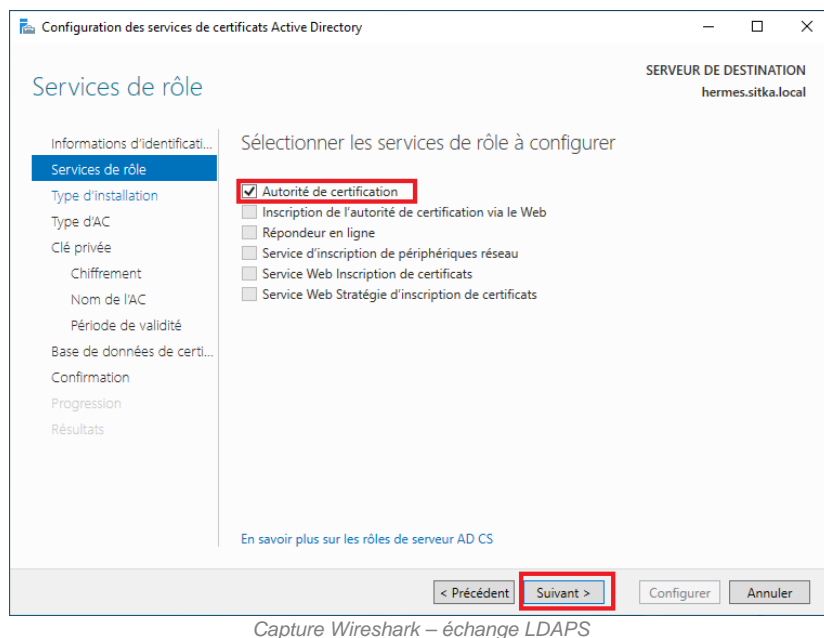


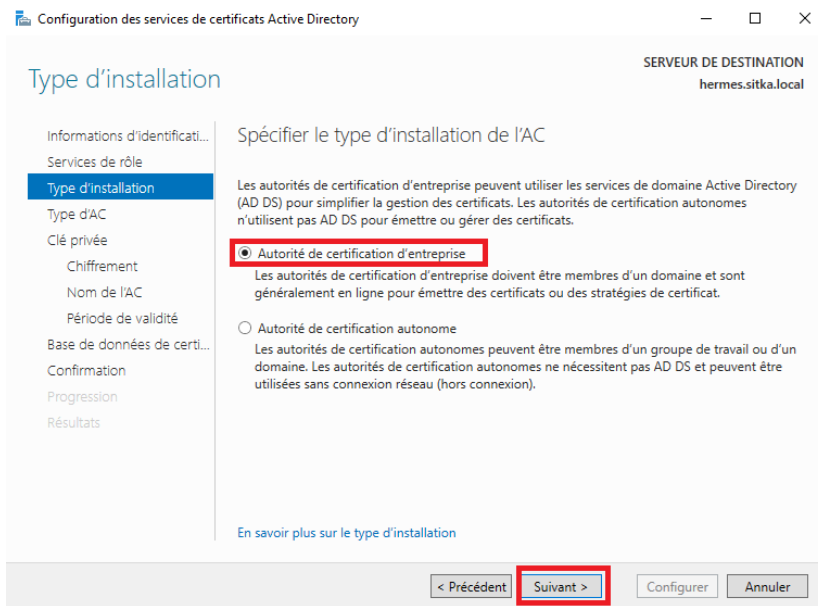
## 17. Diagnostic LDAPS avec Wireshark et résolution

Si la boîte de dialogue de sélection de contenu LDAPS ne s'ouvre pas, c'est que la connexion SSL échoue. On utilise Wireshark pour diagnostiquer le problème :

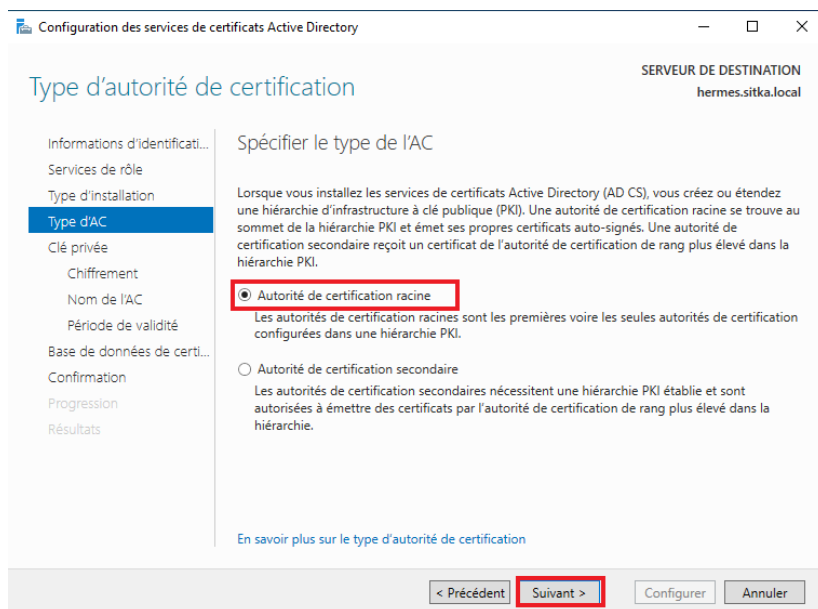
Installer Wireshark sur hermes et capturer le trafic réseau en déclenchant simultanément la connexion LDAPS depuis PfSense. Filtrer avec **ssl** ou **tls**.

L'analyse des trames révèle que : • PfSense envoie un **Client Hello** • Hermes répond avec **Server Hello** et présente son certificat • PfSense envoie une alerte : il ne reconnaît pas le certificat





Capture Wireshark – échange LDAPS



Capture Wireshark – échange LDAPS

## Solution : Exporter et importer le certificat de l'AC

Sur hermes, ouvrir une console MMC, ajouter le composant Certificats pour ordinateur et exporter le certificat de l'autorité racine :

- Ne pas exporter la clé privée
- Format : **X.509 encodé DER (\*.cer)**
- Enregistrer sous le nom : **hermes-ca.cer**

Ouvrir le fichier hermes-ca.cer avec le Bloc-notes pour afficher le certificat en base64 et le copier. Sur PfSense, aller dans **Système** → **Cert Manager** → **CAs** → **Add** et coller le certificat dans le champ prévu à cet effet.

Configuration des services de certificats Active Directory

Clé privée

SERVEUR DE DESTINATION  
hermes.sitka.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 le type de la clé privée

Pour générer et émettre des certificats aux clients, une autorité de certification doit posséder une clé privée.

**Créer une clé privée**  
Utilisez cette option si vous n'avez pas de clé privée ou pour en créer une.

Utiliser la clé privée existante  
Utilisez cette option pour garantir la continuité avec les certificats émis antérieurement lors de la réinstallation d'une AC.

Sélectionner un certificat et utiliser sa clé privée associée  
Sélectionnez cette option s'il existe un certificat sur cet ordinateur ou pour importer un certificat et utiliser sa clé privée associée.

Sélectionner une clé privée existante sur cet ordinateur  
Sélectionnez cette option si vous avez conservé les clés privées d'une installation antérieure ou pour utiliser une clé privée d'une autre source.

[En savoir plus sur la clé privée](#)

< Précédent **Suivant >** Configurer Annuler

Export et import du certificat de l'AC

Configuration des services de certificats Active Directory

Chiffrement pour l'autorité de certification

SERVEUR DE DESTINATION  
hermes.sitka.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 : Longueur de la clé :

RSA#Microsoft Software Key Storage Provider 4096

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

Export et import du certificat de l'AC

Configuration des services de certificats Active Directory

SERVEUR DE DESTINATION  
hermes.sitka.local

### Nom de l'autorité de certification

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 le nom de l'AC

Tapez un nom commun pour identifier cette autorité de certification. Ce nom est ajouté à tous les certificats émis par l'autorité de certification. Les valeurs des suffixes du nom unique sont générées automatiquement, mais elles sont modifiables.

Nom commun de cette AC :

Suffixe du nom unique :

Aperçu du nom unique :

[En savoir plus sur le nom de l'autorité de certification](#)

< Précédent **Suivant >** Configurer Annuler

Export et import du certificat de l'AC

Configuration des services de certificats Active Directory

SERVEUR DE DESTINATION  
hermes.sitka.local

### Période de validité

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 la période de validité

Sélectionnez la période de validité du certificat généré pour cette autorité de certification :

**15** | Années

Date d'expiration de l'AC : 09/01/2025 09:45:00

La période de validité configurée pour ce certificat d'autorité de certification doit dépasser la période de validité pour les certificats qu'elle émettra.

[En savoir plus sur la période de validité](#)

< Précédent **Suivant >** Configurer Annuler

Export et import du certificat de l'AC

## 18. Test et utilisation des authentifications

Une fois le certificat importé, tester la connexion SSL :

```
openssl s_client -showcerts -connect hermes.sitka.local:636
```

Puis tester les authentifications LDAP et LDAPS en utilisant les comptes créés (kaiser, cesar). Créer si nécessaire un groupe sur PfSense lié au groupe AD.

Configuration des services de certificats Active Directory

— □ ×

Base de données de l'autorité de certification

SERVEUR DE DESTINATION  
hermes.sitka.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 emplacements des bases de données

Emplacement de la base de données de certificats :  
C:\Windows\system32\CertLog

Emplacement du journal de la base de données de certificats :  
C:\Windows\system32\CertLog

En savoir plus sur la base de données de l'autorité de certification

< Précédent **Suivant >** Configurer Annuler

Test de connexion avec compte LDAP/LDAPS

Configuration des services de certificats Active Directory

— □ ×

Confirmation

SERVEUR DE DESTINATION  
hermes.sitka.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

Pour configurer les rôles, services de rôle ou fonctionnalités ci-après, cliquez sur Configurer.

⤴ Services de certificats Active Directory

**Autorité de certification**

Type d'AC :	Racine d'entreprise
Fournisseur de services de chiffrement :	RSA#Microsoft Software Key Storage Provider
Algorithme de hachage :	SHA512
Longueur de la clé :	4096
Autoriser l'interaction de l'administrateur :	Désactivé
Période de validité du certificat :	09/01/2025 09:45:00
Nom unique :	CN=HERMES-CA,DC=sitka,DC=local
Emplacement de la base de données de certificats :	C:\Windows\system32\CertLog
Emplacement du journal de la base de données de certificats :	C:\Windows\system32\CertLog

< Précédent **Configurer** Suivant > Annuler

Test de connexion avec compte LDAP/LDAPS

Configuration des services de certificats Active Directory

RESEUR DE DESTINATION  
hermes.sitka.local

## Résultats

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**

Les rôles, services de rôle ou fonctionnalités ci-après ont été configurés :

Services de certificats Active Directory

**Autorité de certification** ✔ Configuration réussie  
En savoir plus sur la configuration de l'autorité de certification

< Précédent   Suivant >   **Fermer**   Annuler

Test de connexion avec compte LDAP/LDAPS

daps://hermes.sitka.local/DC=sitka,DC=local

Connexion   Parcourir   Affichage   Options   Outils   ?

```
ld = ldap_sslinit("hermes.sitka.local", 636, 1);
Error 0 = ldap_set_option(hLdap,
LDAP_OPT_PROTOCOL_VERSION, 3);
Error 0 = ldap_connect(hLdap, NULL);
Error 0 = ldap_get_option(hLdap,LDAP_OPT_SSL,(void*)&N);
Host supports SSL, SSL cipher strength = 256 bits
Established connection to hermes.sitka.local.
Retrieving base DSA information...
Getting 1 entries:
Dn: (RootDSE)
  configurationNamingContext:
    CN=Configuration,DC=sitka,DC=local;
  currentTime: 09/01/2022 10:01:48 Paris, Madrid;
  defaultNamingContext: DC=sitka,DC=local;
  dnsHostName: hermes.sitka.local;
  domainControllerFunctionality: 7 = ( WIN2016 );
  domainFunctionality: 7 = ( WIN2016 );
  dsServiceName: CN=NTDS
    Settings,CN=HERMES,CN=Servers,CN=Default-First-Site-
    Name,CN=Sites,CN=Configuration,DC=sitka,DC=local;
  forestFunctionality: 7 = ( WIN2016 );
  highestCommittedUSN: 192580;
  isGlobalCatalogReady: TRUE;
```

Prêt

Test de connexion avec compte LDAP/LDAPS

# PARTIE 5 – PORTAIL CAPTIF

## 19. Introduction au portail captif

Le portail captif est un mécanisme qui force les clients d'un réseau à passer par une page web d'authentification avant de pouvoir accéder à Internet. Il est couramment utilisé dans les espaces publics : hôtels, gares, établissements scolaires, etc.

## 20. Activation et configuration du portail captif

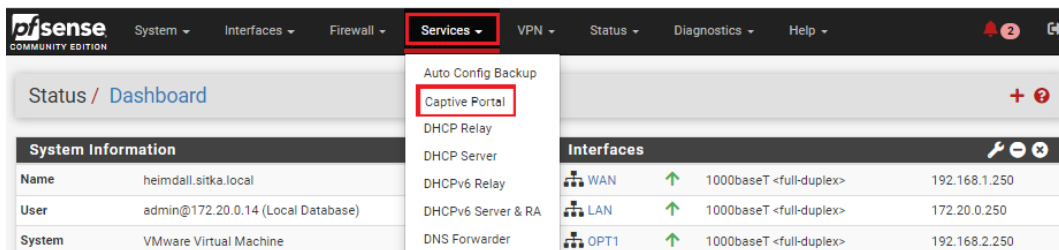
Sur l'interface web de PfSense, aller dans **Services** → **Captive Portal** et cliquer sur **Add**.

Configurer la zone avec les paramètres suivants :

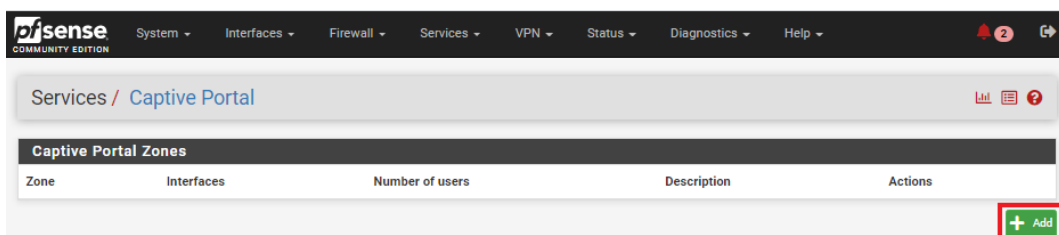
- **Nom de la zone** : Sitka\_portal
- **Description** : Portail captif sitka
- **Interface** : OPT1
- **Maximum concurrent connections** : 1 (une connexion simultanée par utilisateur)
- **Idle timeout** : 15 minutes (déconnexion après inactivité)
- **After authentication Redirection URL** : URL de redirection après authentification
- **Disable Concurrent user logins** : Activé (seule la connexion la plus récente est active)
- **Disable MAC filtering** : Activé (si l'adresse MAC ne peut pas être déterminée)
- **Authentication backend** : LDAPS (méthode d'authentification)



Configuration du portail captif



Configuration du portail captif



Configuration du portail captif

**pfSense** COMMUNITY EDITION System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

Services / Captive Portal / Add Zone

### Add Captive Portal Zone

**Zone name**   
Zone name. Can only contain letters, digits, and underscores (\_) and may not start with a digit.

**Zone description**   
A description may be entered here for administrative reference (not parsed).

Configuration du portail captif

**pfSense** COMMUNITY EDITION System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

Services / Captive Portal / sitka\_portail / Configuration

Configuration **MACs** Allowed IP Addresses Allowed Hostnames Vouchers High Availability File Manager

### Captive Portal Configuration

**Enable**  Enable Captive Portal

**Description**   
A description may be entered here for administrative reference (not parsed).

Don't forget to enable the DHCP server on the captive portal interface! Make sure that the default/maximum DHCP lease time is higher than the hard timeout entered on this page. Also, the DNS Forwarder or Resolver must be enabled for DNS lookups by unauthenticated clients to work.

Configuration du portail captif

**pfSense** COMMUNITY EDITION System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

Services / Captive Portal / sitka\_portail / Configuration

Configuration **MACs** Allowed IP Addresses Allowed Hostnames Vouchers High Availability File Manager

### Captive Portal Configuration

**Enable**  Enable Captive Portal

**Description**   
A description may be entered here for administrative reference (not parsed).

**Interfaces**   
  
  
Select the interface(s) to enable for captive portal.

**Maximum concurrent connections**   
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.

**Idle timeout (Minutes)**   
Clients will be disconnected after this amount of inactivity. They may log in again immediately, though. Leave this field blank for no idle timeout.

Configuration du portail captif

<b>Logout popup window</b>	<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.
<b>Pre-authentication redirect URL</b>	<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.
<b>After authentication Redirection URL</b>	<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.
<b>Blocked MAC address redirect URL</b>	<input type="text"/> Blocked MAC addresses will be redirected to this URL when attempting access.
<b>Preserve users database</b>	<input checked="" type="checkbox"/> Preserve connected users across reboot If enabled, connected users won't be disconnected during a pfSense reboot.
<b>Concurrent user logins</b>	<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.
<b>MAC filtering</b>	<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.

Configuration du portail captif

Captive Portal Login Page	
<b>Display custom logo image</b>	<input checked="" type="checkbox"/> Enable to use a custom uploaded logo
<b>Logo Image</b>	<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 <b>This image will not be stored in the config.</b> The default logo will be used if no custom image is present.
<b>Display custom background image</b>	<input checked="" type="checkbox"/> Enable to use a custom uploaded background image
<b>Background Image</b>	<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. <b>This image will not be stored in the config.</b> The default background image will be used if no custom background is present.
<b>Terms and Conditions</b>	<input type="text" value="Charte d'utilisation du wifi&lt;br/&gt;Charte d'utilisation&lt;br/&gt;Charte d'utilisation du réseau wifi DE SITKA&lt;br/&gt;La présente charte a pour objet de définir les règles d'utilisation de la connexion wifi du gîte auberge les"/> Copy and paste terms and conditions for use in the captive portal. HTML tags will be stripped out

Configuration du portail captif

Authentication	
<b>Authentication Method</b>	<input type="text" value="Use an Authentication backend"/> Select an Authentication Method to use for this zone. One method must be selected. - "Authentication backend" will force the login page to be displayed and will authenticate users using their login and password, or using vouchers. - "None" method will force the login page to be displayed but will accept any visitor that clicks the "submit" button. - "RADIUS MAC Authentication" method will try to authenticate devices automatically with their MAC address without displaying any login page.
<b>Authentication Server</b>	<input type="text" value="authentication ldap"/> <input type="text" value="authentication ldaps"/> <input type="text" value="Local Database"/> You can add a remote authentication server in the User Manager. Vouchers could also be used, please go to the Vouchers Page to enable them.
<b>Secondary authentication Server</b>	<input type="text" value="authentication ldap"/> <input type="text" value="authentication ldaps"/> <input type="text" value="Local Database"/> You can optionally select a second set of servers to to authenticate users. Users will then be able to login using separated HTML inputs. This setting is useful if you want to provide multiple authentication method to your users. If you don't need multiple authentication method, then leave this setting empty.
<b>Reauthenticate Users</b>	<input type="checkbox"/> Reauthenticate connected users every minute If reauthentication is enabled, request are made to the server for each user that is logged in every minute. If an access denied is received for a user, that user is disconnected from the captive portal immediately. Reauthentication requires user credentials to be cached in the captive portal database while a user is logged in, The cached credentials are necessary for the portal to perform automatic reauthentication requests.

Configuration du portail captif

### HTTPS Options

**Login**  Enable HTTPS login  
 When enabled, the username and password will be transmitted over an HTTPS connection to protect against eavesdroppers. A server name and certificate must also be specified below.

**HTTPS server name**   
 This name will be used in the form action for the HTTPS POST and should match the Common Name (CN) in the certificate (otherwise, the client browser will most likely display a security warning). Make sure captive portal clients can resolve this name in DNS and verify on the client that the IP resolves to the correct interface IP on pfSense.

**SSL/TLS Certificate**   
 Certificates known to be incompatible with use for HTTPS are not included in this list. If no certificates are defined, one may be defined here: [System > Cert. Manager](#)

**HTTPS Forwards**  Disable HTTPS Forwards  
 If this option is set, attempts to connect to HTTPS (SSL/TLS on port 443) sites will not be forwarded to the captive portal. This prevents certificate errors from being presented to the user even if HTTPS logins are enabled. Users must attempt a connection to an HTTP (Port 80) site to get forwarded to the captive portal. If HTTPS logins are enabled, the user will be redirected to the HTTPS login page.

Don't forget to enable the DHCP server on the captive portal interface! Make sure that the default/maximum DHCP lease time is higher than the hard timeout entered on this page. Also, the DNS Forwarder or Resolver must be enabled for DNS lookups by unauthenticated clients to work.

Configuration du portail captif

pfSense COMMUNITY EDITION

System - Interfaces - Firewall - Services - VPN - Status - Diagnostics - Help

Services / Captive Portal / sitka\_portal / Allowed IP Addresses

Configuration MACs **Allowed IP Addresses** Allowed Hostnames Vouchers High Availability File Manager

IP Addresses	Description	Actions
<input type="button" value="+ Add"/>		

Configuration du portail captif

pfSense COMMUNITY EDITION

System - Interfaces - Firewall - Services - VPN - Status - Diagnostics - Help

Services / Captive Portal / sitka\_portal / Allowed IP Addresses / Edit

#### Edit Captive Portal IP Rule

**IP Address**  /

**Description**   
 Enter a description here for reference only. (Not parsed)

**Direction**

**Bandwidth up**   
 Enter an upload limit to be enforced on this address in Kbit/s

**Bandwidth down**   
 Enter a download limit to be enforced on this address in Kbit/s

Configuration du portail captif

pfSense COMMUNITY EDITION

System - Interfaces - Firewall - Services - VPN - Status - Diagnostics - Help

Services / Captive Portal / sitka\_portal / Allowed IP Addresses

Configuration MACs **Allowed IP Addresses** Allowed Hostnames Vouchers High Availability File Manager

IP Addresses	Description	Actions
172.20.0.14 / 24	serveur dns	<input type="button" value="edit"/> <input type="button" value="delete"/>
→ = All connections to the address are allowed, ← = All connections from the address are allowed, ⇄ = All connections to or from are allowed		

Configuration du portail captif

The screenshot shows the pfSense Services menu. The 'Services' menu is open, and 'DHCP Server' is highlighted with a red box. The background shows the 'System Information' and 'Interfaces' sections.

System Information	
Name	heimdall.sitka.local
User	admin@172.20.0.14 (Local Database)
System	VMware Virtual Machine

Interfaces			
WAN	↑	1000baseT <full-duplex>	192.168.1.250
LAN	↑	1000baseT <full-duplex>	172.20.0.250
OPT1	↑	1000baseT <full-duplex>	192.168.2.250

Configuration du portail captif

The screenshot shows the 'DHCP Server' configuration page for the 'OPT1' interface. The 'Enable' checkbox is checked. The 'Available range' is set to '192.168.2.1 - 192.168.2.254'. The 'Range' is set to '192.168.2.20' to '192.168.2.50'.

**General Options**

- Enable  Enable DHCP server on OPT1 interface
- BOOTP  Ignore BOOTP queries
- Deny unknown clients: Allow all clients
- Ignore denied clients:  Denied clients will be ignored rather than rejected.
- Ignore client identifiers:  If a client includes a unique identifier in its DHCP request, that UID will not be recorded in its lease.
- Subnet: 192.168.2.0
- Subnet mask: 255.255.255.0
- Available range: 192.168.2.1 - 192.168.2.254
- Range: 192.168.2.20 (From) to 192.168.2.50 (To)

Configuration du portail captif

The screenshot shows the 'Servers' configuration page. The 'DNS servers' field is filled with '172.20.0.14' and '8.8.8.8'.

**Servers**

- WINS servers: WINS Server 1, WINS Server 2
- DNS servers: 172.20.0.14, 8.8.8.8, DNS Server 3, DNS Server 4

Leave blank to use the system default DNS servers: this interface's IP if DNS Forwarder or Resolver is enabled, otherwise the servers configured on the System / General Setup page.

Configuration du portail captif

The screenshot shows the 'Other Options' configuration page. The 'Gateway' is set to '192.168.2.250' and the 'Domain name' is set to 'sitka.local'.

**Other Options**

- Gateway: 192.168.2.250
- Domain name: sitka.local

The default is to use the IP on this interface of the firewall as the gateway. Specify an alternate gateway here if this is not the correct gateway for the network. Type "none" for no gateway assignment.

The default is to use the domain name of this system as the default domain name provided by DHCP. An alternate domain name may be specified here.

Configuration du portail captif

pfSense COMMUNITY EDITION

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

Firewall / Rules / OPT1

The changes have been applied successfully. The firewall rules are now reloading in the background. Monitor the filter reload progress.

Floating WAN LAN **OPT1**

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/> ✓ 4 /30 KiB	IPv4 TCP/UDP	OPT1 net	*	*	53 (DNS)	*	none			
<input type="checkbox"/> ✓ 9 /13.89 MiB	IPv4 TCP/UDP	OPT1 net	*	*	443 (HTTPS)	*	none			

Add Add Delete Save Separator

Configuration du portail captif

Captive Portal Login Page

https://heimdall.sitka.local:8003/index.php?

Made with ♥ by Netgate

Configuration du portail captif

pfSense COMMUNITY EDITION

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

Services / Captive Portal

Captive Portal Zones

Zone	Interfaces	Number of users	Description	Actions
sitka_portail	OPT1	1	portail captif de sitka	

Add

Configuration du portail captif

pfSense COMMUNITY EDITION

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

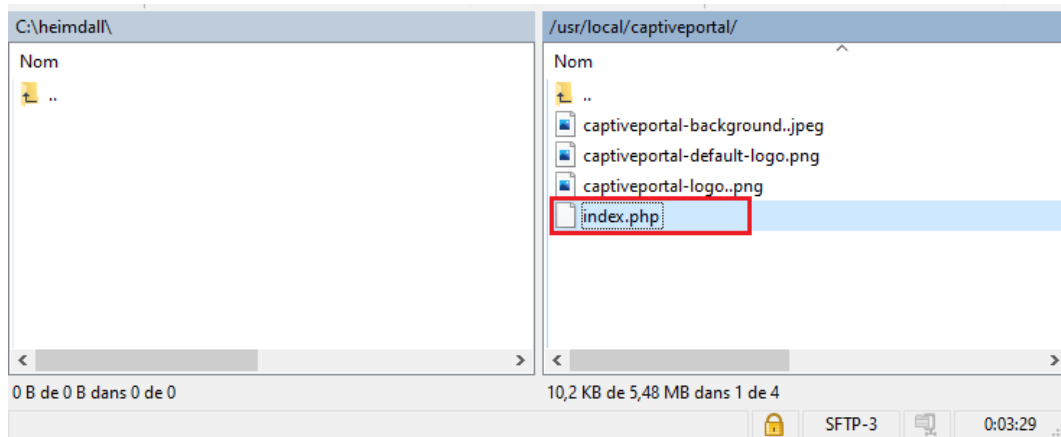
Status / Captive Portal / sitka\_portail

Users Logged In (1)

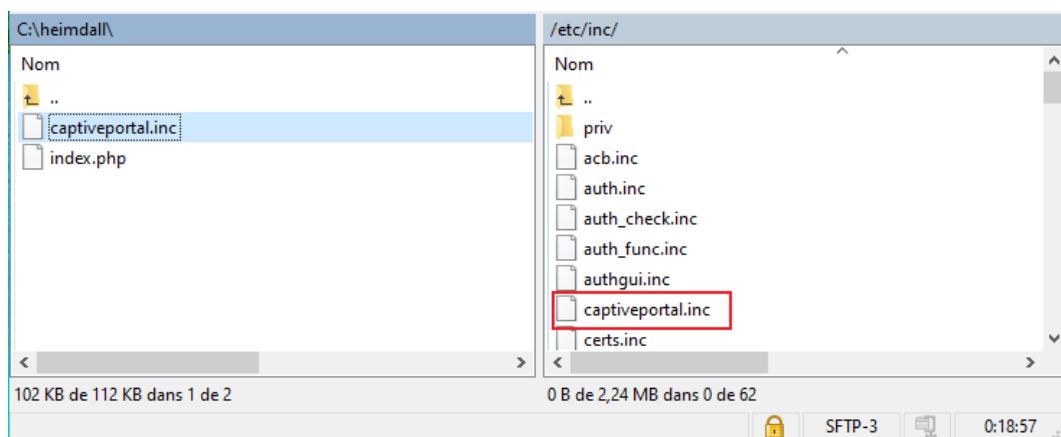
IP address	Username	Session start	Actions
192.168.2.20	kaiser	01/16/2022 22:06:04	

Show Last Activity Disconnect All Users

Configuration du portail captif



Configuration du portail captif



Configuration du portail captif

## 21. Configuration du DHCP sur OPT1

Activer et configurer le service DHCP sur l'interface OPT1 :

- Définir l'étendue DHCP • Renseigner l'adresse IP du serveur DNS (172.20.0.14) • Renseigner l'adresse de la passerelle et le nom de domaine

## 22. Création des règles de pare-feu

Créer deux règles sur l'interface OPT1 autorisant le trafic nécessaire au portail :

- Règle 1 : Autoriser le trafic DNS (port 53 UDP/TCP) vers 172.20.0.14 • Règle 2 : Autoriser le trafic HTTPS (port 443 TCP)

## 23. Test du portail captif

Se connecter avec une machine cliente sur l'interface OPT1. Le navigateur doit être redirigé automatiquement vers la page d'authentification du portail.

Pour franciser l'interface du portail, il est possible de modifier les fichiers de configuration :

- « You are connected » → « Vous êtes connecté »
- « Disconnecting... / You have been disconnected » → « Déconnexion... / Vous êtes déconnecté »
- « Invalid credentials specified » → « Les informations saisies sont invalides »
- « Captive Portal login Page » → « Portail Captif de sitka »

- « Login / Made with ... by ... Netgate » → « Connexion / Connectez-vous avec votre compte LDAPS »
- « User / Password » → « Utilisateur / Mot de passe »
- « Logout / Click the button below to disconnect » → « Déconnexion / Cliquez sur le bouton ci-dessous »

## PARTIE 6 – SNORT IDS/IPS

### 24. Introduction à Snort et aux IDS/IPS

Snort est un système de détection et de prévention d'intrusion open source qui s'intègre directement dans PfSense. Il analyse le trafic réseau en temps réel pour détecter et bloquer les menaces.

#### Différence entre IDS et IPS :

**IDS (Intrusion Detection System)** – Rôle passif : détecte et signale les intrusions sans les bloquer. Il utilise une base de données d'attaques pour :

- Analyser et surveiller le trafic réseau pour détecter une cyberattaque
- Détecter les violations de la politique de sécurité
- Détecter les logiciels malveillants et les scanners de ports

**IPS (Intrusion Prevention System)** – Rôle actif : bloque et rejette les paquets réseau identifiés comme menaçants en appliquant un profil de sécurité défini.

### 25. Création d'un compte Snort

Il est nécessaire de créer un compte sur le site officiel de Snort pour obtenir une clé Oinkmaster permettant le téléchargement et la mise à jour des règles :

[https://www.snort.org/users/sign\\_up](https://www.snort.org/users/sign_up)

Après confirmation de l'inscription par e-mail, se connecter sur le site Snort et récupérer le code **Oinkcode** dans le menu correspondant.



*Récupération du code Oinkmaster sur snort.org*

### 26. Installation de Snort sur PfSense

Sur PfSense, aller dans **Système** → **Package Manager** → **Available Packages**. Rechercher **Snort** et cliquer sur **Install**. Une fois installé, accéder à Snort via **Services** → **Snort**.



Installation du package Snort via le Package Manager



Menu Services → Snort

## 27. Configuration de Snort

### 27.1 Paramètres globaux (Global Settings)

Dans l'onglet **Global Settings**, activer et configurer les sources de règles :

- **Enable Snort VRT** : Activer les règles VRT (saisir la clé Oinkmaster)
- **Enable Snort GPLv2** : Activer les règles communautaires gratuites
- **Enable ET Open** : Activer les règles Emerging Threats
- **Enable OpenAppID** : Ne pas cocher (licence requise)
- **Update Interval** : 1 DAY
- **Update Start Time** : 00:01
- **Remove Blocked Hosts Interval** : 1 HOUR
- **Keep Snort Settings After Deinstall** : Cocher
- **Startup/Shutdown Logging** : Cocher

Configuration des paramètres globaux de Snort

## 27.2 Mise à jour des règles

Dans l'onglet **Updates**, cliquer sur **Update Rules** pour télécharger les règles Snort. À la fin de la mise à jour, le message **Result: Success** doit apparaître.

Mise à jour des règles Snort – Result: Success

## 27.3 Configuration de l'interface surveillée

Dans **Snort** → **Interfaces**, cliquer sur **Add** pour ajouter l'interface WAN à surveiller. Configurer les paramètres suivants :

- **General Settings** : Activer l'interface WAN
- **Alert Settings** → **Send Alerts to System Log** : Activer
- **Block Settings** : Activer le mode IPS

## 27.4 Catégories et politique IPS

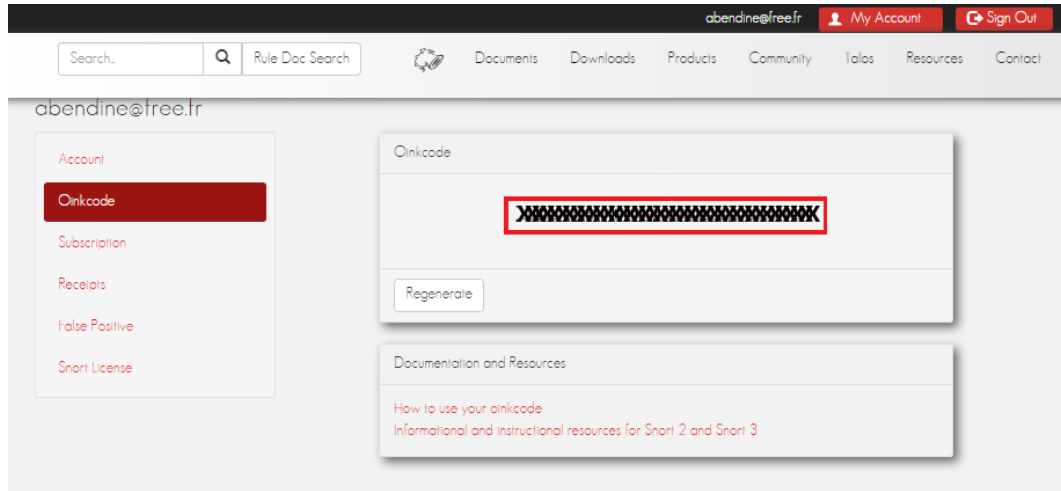
Dans l'onglet **WAN Categories**, activer l'option **Resolve Flowbits** et sélectionner la politique IPS **Balanced**.

Les politiques IPS disponibles sont :

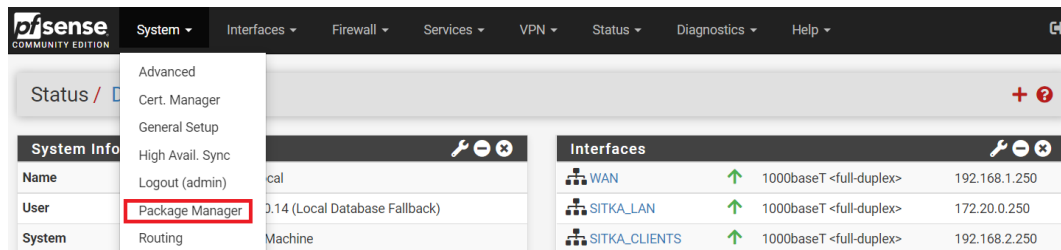
- **Connectivity** : Bloque les menaces majeures avec peu de faux positifs – idéal pour démarrer

- **Balanced** : Bon équilibre couverture/performance – recommandé pour une utilisation standard
- **Security** : Politique stricte incluant des règles avancées (type Flash dans Excel)
- **Max-Detect** : Stratégie maximale pour les tests – à utiliser avec précaution en production

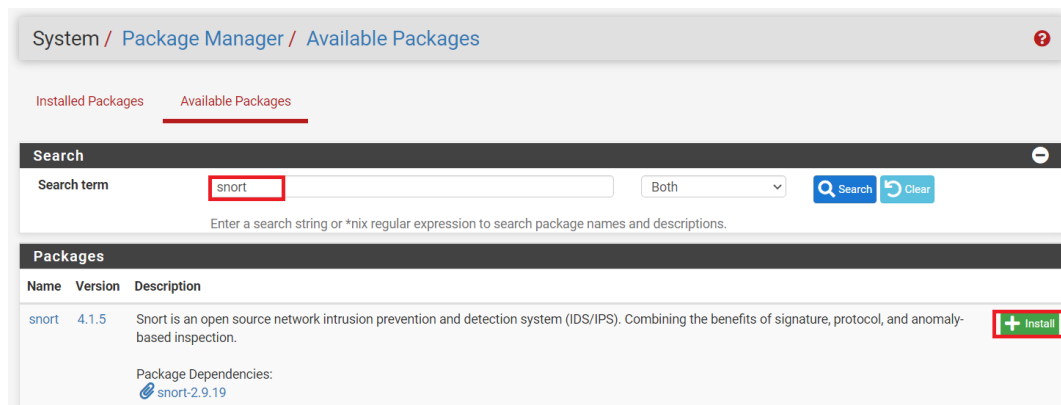
■ ■ ■ L'activation de la politique IPS désactive la sélection manuelle des règles Snort Text Rules et Snort SO Rules. Les règles ET Open restent configurables manuellement.



Configuration de Snort – interface et règles



Configuration de Snort – interface et règles



Configuration de Snort – interface et règles

pfSense  
COMMUNITY EDITION

System ▾ Interfaces ▾ Firewall ▾ **Services ▾** VPN ▾ Status ▾ Diagnostics ▾ Help ▾

System / Package Manager / Package Installation

pfSense-pkg-snort installation successfully completed.

Installed Packages Available Packages **Package Installation**

**Package Installation**

Please note that, by default, snort will truncate packets to a default snaplen of 15158 bytes. Additionally, LRO may be enabled on the Stream5 target-based reassembly. It is recommended to use a card that supports it.

This can be done by appending '-lro' to your ifconfig\_  
=====

Message from pfSense-pkg-snort-4.1.5:

--

Please visit Services - Snort - Interfaces tab first to configure the interface. Then select your desired rules packages :

- Auto Config Backup
- Captive Portal
- DHCP Relay
- DHCP Server
- DHCPv6 Relay
- DHCPv6 Server & RA
- DNS Forwarder
- DNS Resolver
- Dynamic DNS
- IGMP Proxy
- NTP
- PPPoE Server
- Shellcmd
- SNMP
- Snort**
- UPnP & NAT-PMP
- Wake-on-LAN

Configuration de Snort – interface et règles

Services / Snort / Global Settings

Snort Interfaces **Global Settings** Updates Alerts Blocked Pass Lists Suppress IP Lists SID Mgmt Log Mgmt Sync

**Snort Subscriber Rules**

**Enable Snort VRT**  Click to enable download of Snort free Registered User or paid Subscriber rules

[Sign Up for a free Registered User Rules Account](#)  
[Sign Up for paid Snort Subscriber Rule Set \(by Talos\)](#)

**Snort Oinkmaster Code**

Obtain a snort.org Oinkmaster code and paste it here. (Paste the code only and not the URL!)

**Snort GPLv2 Community Rules**

**Enable Snort GPLv2**  Click to enable download of Snort GPLv2 Community rules

The Snort Community Ruleset is a GPLv2 Talos certified ruleset that is distributed free of charge without any Snort Subscriber License restrictions. This ruleset is updated daily and is a subset of the subscriber ruleset.

**Emerging Threats (ET) Rules**

**Enable ET Open**  Click to enable download of Emerging Threats Open rules

ETOpen is an open source set of Snort rules whose coverage is more limited than ETPro.

**Enable ET Pro**  Click to enable download of Emerging Threats Pro rules

[Sign Up for an ETPro Account](#)  
ETPro for Snort offers daily updates and extensive coverage of current malware threats.

Configuration de Snort – interface et règles

### Rules Update Settings

**Update Interval**    
 Please select the interval for rule updates. Choosing NEVER disables auto-updates.

**Update Start Time**    
 Enter the rule update start time in 24-hour format (HH:MM). Default is 00 hours with a randomly chosen minutes value. Rules will update at the interval chosen above starting at the time specified here. For example, using a start time of 00:08 and choosing 12 Hours for the interval, the rules will update at 00:08 and 12:08 each day. The randomized minutes value should be retained to minimize the impact to the rules update site from large numbers of simultaneous requests.

**Hide Deprecated Rules Categories**  Click to hide deprecated rules categories in the GUI and remove them from the configuration. Default is not checked.

**Disable SSL Peer Verification**  Click to disable verification of SSL peers during rules updates. This is commonly needed only for self-signed certificates. Default is not checked.

---

### General Settings

**Remove Blocked Hosts Interval**    
 Please select the amount of time you would like hosts to be blocked. In most cases, one hour is a good choice.

**Remove Blocked Hosts After Deinstall**  Click to clear all blocked hosts added by Snort when removing the package. Default is checked.

**Keep Snort Settings After Deinstall**  Click to retain Snort settings after package removal.

**Startup/Shutdown Logging**  Click to output detailed messages to the system log when Snort is starting and stopping. Default is not checked.

Configuration de Snort – interface et règles

The screenshot shows the Snort web interface with a 'Rules Update Task' dialog box open. The dialog box contains the text: 'Updating rule sets may take a while ... please wait for the process to complete. This dialog will auto-close when the update is finished.' and a 'Close' button. In the background, the 'Update Rules' button is highlighted with a red box. The main interface shows a table of installed rule sets and their MDS signature dates, along with an 'Update Your Rule Set' section.

Rule Set Name/Publisher	MDS Signature Date
Snort Subscriber Ruleset	Not Enabled
Snort GPLv2 Community Rules	Not Downloaded
Emerging Threats Open Rules	Not Downloaded
Snort OpenAppID Detectors	Not Enabled
Snort AppID Open Text Rules	Not Enabled
Feodo Tracker Botnet C2 IP Rules	Not Enabled

**Update Your Rule Set**

Last Update: Unknown    Result: Unknown

Update Rules:    

Click UPDATE RULES to check for and automatically apply any new posted updates for selected rules packages. Clicking FORCE UPDATE will zero out the MDS hashes and force the download and application of the latest versions of the enabled rules packages.

**Manage Rule Set Log**

The log file is limited to 1024K in size and is automatically cleared when that limit is exceeded.

Logfile Size: Log file is empty

Configuration de Snort – interface et règles

Services / Snort / Updates

Snort Interfaces Global Settings Updates Alerts Blocked Pass Lists Suppress IP Lists SID Mgmt Log Mgmt Sync

**Installed Rule Set MD5 Signature**

Rule Set Name/Publisher	MD5 Signature Hash	MD5 Signature Date
Snort Subscriber Ruleset	73370d5559b00f2a1001decf9167c5b5	Sunday, 30-Jan-22 17:30:26 CET
Snort GPLv2 Community Rules	5a1e3be23ee59e10d78d64a156ddac7a	Sunday, 30-Jan-22 17:30:26 CET
Emerging Threats Open Rules	fecb4fd26c161041efb2695a3c57b27	Sunday, 30-Jan-22 17:30:27 CET
Snort OpenAppID Detectors	Not Enabled	Not Enabled
Snort AppID Open Text Rules	Not Enabled	Not Enabled
Feodo Tracker Botnet C2 IP Rules	Not Enabled	Not Enabled

**Update Your Rule Set**

Last Update Jan-30 2022 17:30 **Result: Success**

Update Rules

Click UPDATE RULES to check for and automatically apply any new posted updates for selected rules packages. Clicking FORCE UPDATE will zero out the MD5 hashes and force the download and application of the latest versions of the enabled rules packages.

**Manage Rule Set Log**

The log file is limited to 1024K in size and is automatically cleared when that limit is exceeded.

Logfile Size 12 KiB

Configuration de Snort – interface et règles

**Manage Rule Set Log**

The log file is limited to 1024K in size and is automatically cleared when that limit is exceeded.

Logfile Size 7 KiB

Configuration de Snort – interface et règles

## Rules Update Log

```

Installation of Snort Subscriber rules completed.
Extracting and installing Snort GPLv2 Community Rules...
Installation of Snort GPLv2 Community Rules completed.
Extracting and installing Emerging Threats Open rules...
Installation of Emerging Threats Open rules completed.
Copying new config and map files...
Warning: No interfaces configured for Snort were found...
The rules update has finished. Time: 2022-01-30 17:43:31
  
```

Close

Configuration de Snort – interface et règles

Services / Snort / Interfaces

Snort Interfaces Global Settings Updates Alerts Blocked Pass Lists Suppress IP Lists SID Mgmt Log Mgmt Sync

**Interface Settings Overview**

Interface	Snort Status	Pattern Match	Blocking Mode	Description	Actions
<input type="button" value="+ Add"/>					

Configuration de Snort – interface et règles

Snort Interfaces Global Settings Updates Alerts Blocked Pass Lists Suppress IP Lists SID Mgmt Log Mgmt Sync

WAN Settings

**General Settings**

Enable  Enable interface

Interface  Choose the interface where this Snort instance will inspect traffic.

Description  Enter a meaningful description here for your reference.

Snap Length  Enter the desired interface snaplen value in bytes. Default is 1518 and is suitable for most applications.

*Configuration de Snort – interface et règles*

**Alert Settings**

Send Alerts to System Log  Snort will send Alerts to the firewall's system log. Default is Not Checked.

System Log Facility  Select system log Facility to use for reporting. Default is LOG\_AUTH.

System Log Priority  Select system log Priority (Level) to use for reporting. Default is LOG\_ALERT.

Enable Packet Captures  checking this option will automatically capture packets that generate a Snort alert into a tcpdump compatible file

Packet Capture File Size  Enter a value in megabytes for the packet capture file size limit. Default is 128 megabytes. When the limit is reached, the current packet capture file in directory /var/log/snort/snort\_em060059 is rotated and a new file opened.

Enable Unified2 Logging  Checking this option will cause Snort to simultaneously log alerts to a unified2 binary format log file in the logging subdirectory for this interface. Default is Not Checked.  
Log size and retention limits for the Unified2 log should be configured on the LOG MGMT tab when this option is enabled.

*Configuration de Snort – interface et règles*

**Block Settings**

Block Offenders  Checking this option will automatically block hosts that generate a Snort alert. Default is Not Checked.

IPS Mode  Select blocking mode operation. Legacy Mode inspects copies of packets while Inline Mode inserts the Snort inspection engine into the network stack between the NIC and the OS. Default is Legacy Mode.  
  
Legacy Mode uses the PCAP engine to generate copies of packets for inspection as they traverse the interface. Some "leakage" of packets will occur before Snort can determine if the traffic matches a rule and should be blocked. Inline mode instead intercepts and inspects packets before they are handed off to the host network stack for further processing. Packets matching DROP rules are simply discarded (dropped) and not passed to the host network stack. No leakage of packets occurs with Inline Mode. WARNING: Inline Mode only works with NIC drivers which properly support Netmap! Supported drivers: bnxt, cc, cxgbe, cxl, em, em, ena, ice, igb, ix, ixgbe, ixl, lem, re, vmx, vtnet. If problems are experienced with Inline Mode, switch to Legacy Mode instead.

Kill States  checking this option will kill firewall established states for the blocked IP. Default is checked.

Which IP to Block  Select which IP extracted from the packet you wish to block. Default is BOTH.

*Configuration de Snort – interface et règles*

Services / Snort / Interface Settings / WAN - Categories

Snort Interfaces Global Settings Updates Alerts Blocked Pass Lists Suppress IP Lists SID Mgmt Log Mgmt Sync

WAN Settings **WAN Categories** WAN Rules WAN Variables WAN Preprocs WAN IP Rep WAN Logs

**Automatic Flowbit Resolution**

**Resolve Flowbits**  If checked, Snort will auto-enable rules required for checked flowbits. Default is Checked.  
 Snort will examine the enabled rules in your chosen rule categories for checked flowbits. Any rules that set these dependent flowbits will be automatically enabled and added to the list of files in the interface rules directory.

**Snort Subscriber IPS Policy Selection**

**Use IPS Policy**  If checked, Snort will use rules from one of three pre-defined IPS policies in the Snort Subscriber rules. Default is Not Checked.  
 Selecting this option disables manual selection of Snort Subscriber categories in the list below, although Emerging Threats categories may still be selected if enabled on the Global Settings tab. These will be added to the pre-defined Snort IPS policy rules from the Snort VRT.

**IPS Policy Selection** Balanced

Snort IPS policies are: Connectivity, Balanced, Security or Max-Detect.  
 Connectivity blocks most major threats with few or no false positives. Balanced is a good starter policy. It is speedy, has good base coverage level, and covers most threats of the day. It includes all rules in Connectivity. Security is a stringent policy. It contains everything in the first two plus policy-type rules such as a Flash object in an Excel file. Max-Detect is a policy created for testing network traffic through your device. This policy should be used with caution on production systems!

**Select the rulesets (Categories) Snort will load at startup**

▲ Category is auto-enabled by SID Mgmt conf files  
▲ Category is auto-disabled by SID Mgmt conf files

Configuration de Snort – interface et règles

Enable **Ruleset: Snort GPLv2 Community Rules**

Snort GPLv2 Community Rules (Talos certified)

Enable	Ruleset: ET Open Rules	Enable	Ruleset: Snort Text Rules	Enable	Ruleset: Snort SO Rules	Snort OPENAPPID rules are not enabled.
<input type="checkbox"/>	emerging-activex.rules	<input type="checkbox"/>	snort_app-detect.rules	<input type="checkbox"/>	snort_browser-chrome.so.rules	
<input type="checkbox"/>	emerging-attack_response.rules	<input type="checkbox"/>	snort_blacklist.rules	<input type="checkbox"/>	snort_browser-ie.so.rules	
<input type="checkbox"/>	emerging-botcc.portgrouped.rules	<input type="checkbox"/>	snort_browser-chrome.rules	<input type="checkbox"/>	snort_browser-other.so.rules	
<input type="checkbox"/>	emerging-botcc.rules	<input type="checkbox"/>	snort_browser-firefox.rules	<input type="checkbox"/>	snort_browser-webkit.so.rules	

Configuration de Snort – interface et règles

Snort Interfaces Global Settings Updates Alerts Blocked Pass Lists Suppress IP Lists SID Mgmt Log Mgmt Sync

**Interface Settings Overview**

Interface	Snort Status	Pattern Match	Blocking Mode	Description	Actions
<input type="checkbox"/> WAN (em0)	<span style="color: red;">⊗</span> <span style="color: blue;">▶</span>	AC-BNFA	LEGACY MODE	WAN	<input type="button" value="Edit"/> <input type="button" value="Refresh"/> <input type="button" value="Delete"/>

Configuration de Snort – interface et règles

Snort Interfaces Global Settings Updates Alerts Blocked Pass Lists Suppress IP Lists SID Mgmt Log Mgmt Sync

**Interface Settings Overview**

Interface	Snort Status	Pattern Match	Blocking Mode	Description	Actions
<input type="checkbox"/> WAN (em0)	<span style="color: green;">⊕</span> <span style="color: blue;">▶</span> <span style="color: blue;">⊕</span>	AC-BNFA	LEGACY MODE	WAN	<input type="button" value="Edit"/> <input type="button" value="Refresh"/> <input type="button" value="Delete"/>

Configuration de Snort – interface et règles

Snort Interfaces Global Settings Updates **Alerts** Blocked Pass Lists Suppress IP Lists SID Mgmt Log Mgmt Sync

**Alert Log View Settings**

Interface to Inspect: WAN (em0)  Auto-refresh view 250 **Save**  
 Choose interface.. Alert lines to display.

Alert Log Actions **Download** **Clear**

**Alert Log View Filter** +

**15 Entries in Active Log**

Date	Action	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	GID:SID	Description
2022-01-30 21:35:58	⚠	2	UDP	Attempted Information Leak	192.168.1.128	48917	192.168.1.250	38237	1:2018489	ET SCAN NMAP OS Detection Probe
2022-01-30 21:35:58	⚠	2	UDP	Attempted Information Leak	192.168.1.128	48917	192.168.1.250	38237	1:2018489	ET SCAN NMAP OS Detection Probe
2022-01-30 21:35:57	⚠	2	UDP	Attempted Information Leak	192.168.1.128	48917	192.168.1.250	38237	1:2018489	ET SCAN NMAP OS Detection Probe

Configuration de Snort – interface et règles

## 27.5 Démarrage du service Snort

Après avoir terminé la configuration, cliquer sur **Save** puis démarrer l'interface Snort en cliquant sur l'icône de démarrage correspondante.

## 28. Test d'intrusion avec Nmap

Pour tester le bon fonctionnement de Snort en mode IPS, on utilise l'outil **Nmap** installé sur la machine physique pour scanner les ports de PfSense.

```
nmap -sS 192.168.1.250
```

Dans l'onglet **Alerts** de Snort, des notifications d'attaques provenant de l'adresse IP de la machine physique (192.168.1.128) apparaissent : Snort a bien détecté le scan Nmap.

Dans l'onglet **Blocked**, la machine est automatiquement bloquée car elle a été identifiée comme un hôte hostile.