pfSense

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

pfSense CE 2.5.x

Sommaire

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

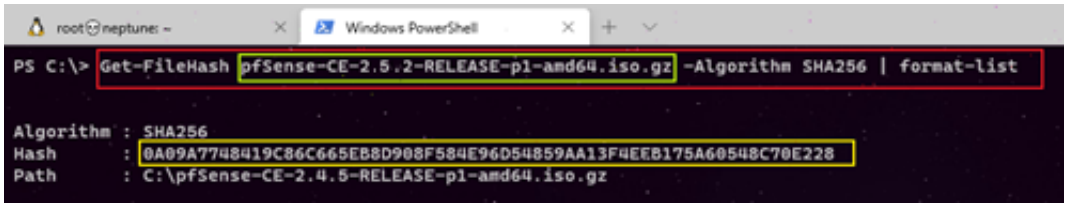
L'image ISO d'installation de PfSense est disponible sur le site officiel :

```
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.



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 :

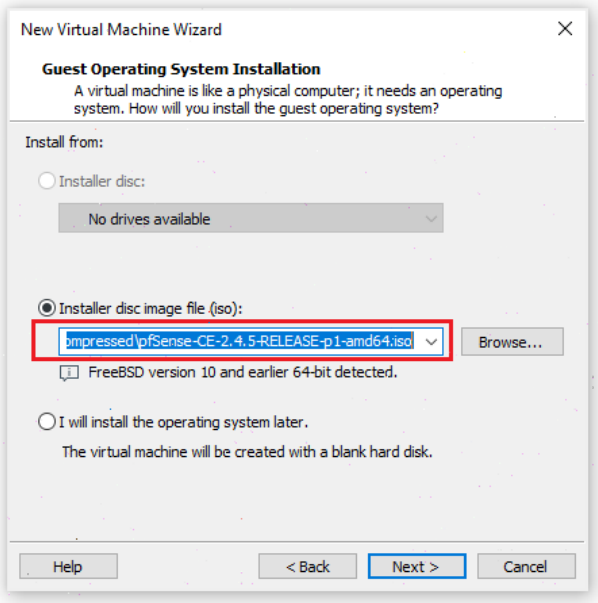
• Accepter le contrat de licence (Accept).

• Sélectionner **Install** puis valider avec OK.

• Choisir le clavier français (fr) et tester la configuration.

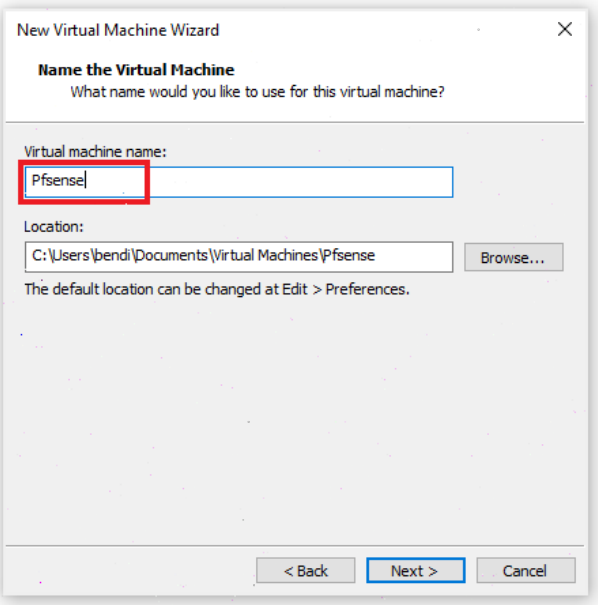
• Sélectionner le système de fichiers **UFS** pour la création des partitions.

• Choisir de ne pas ouvrir de shell supplémentaire et redémarrer.

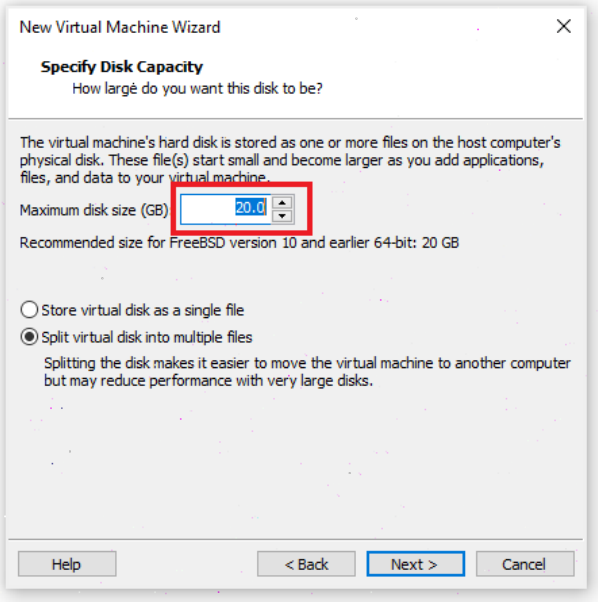


Étape d'installation PfSense – écran 2

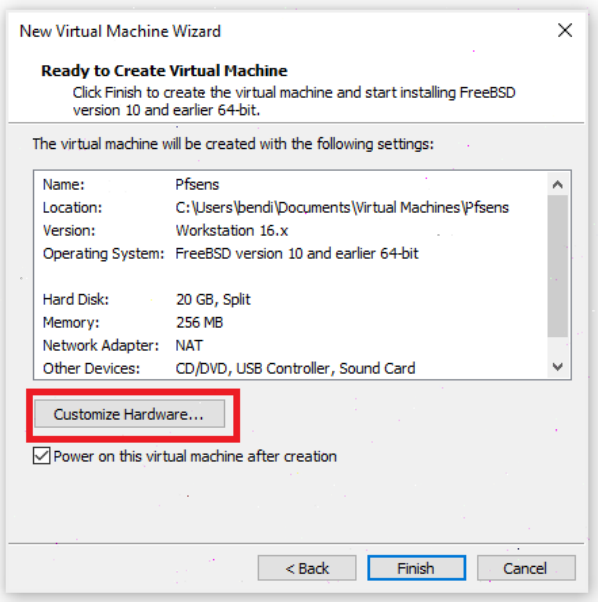
Étape d'installation PfSense – écran 3



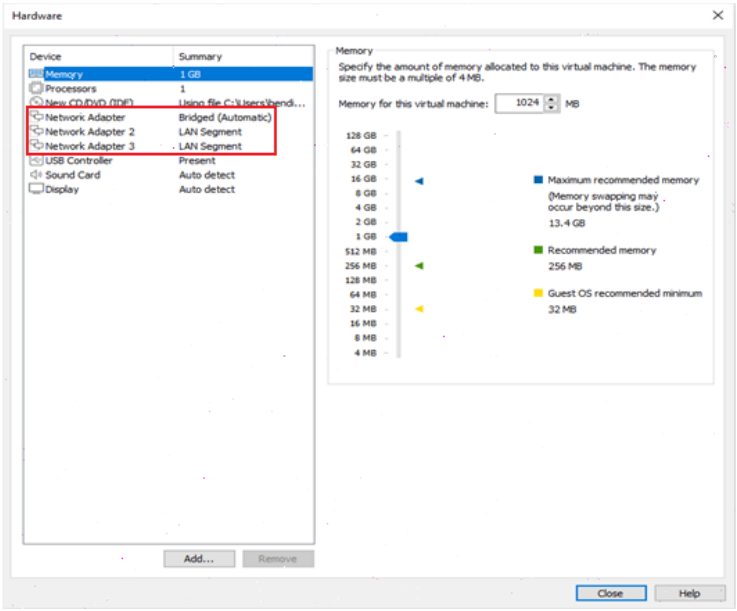
Étape d'installation PfSense – écran 4



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

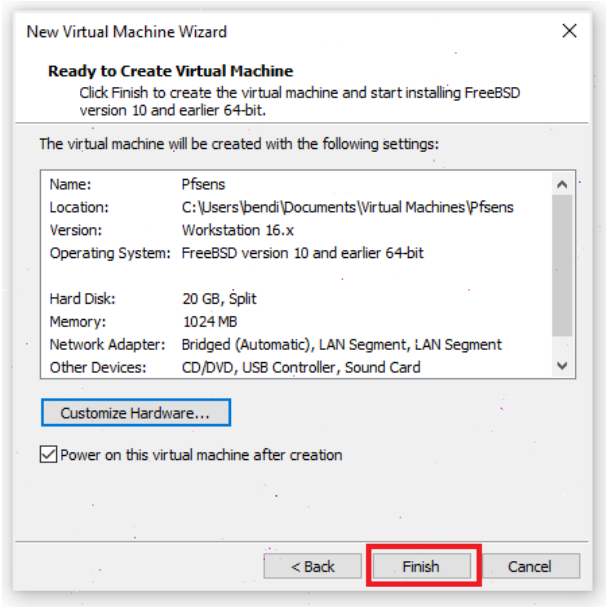
Après le redémarrage, le clavier est en QWERTY. Pour le passer temporairement en AZERTY (sera remis à zéro au prochain redémarrage), on utilise l'option 8 (shell) :

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

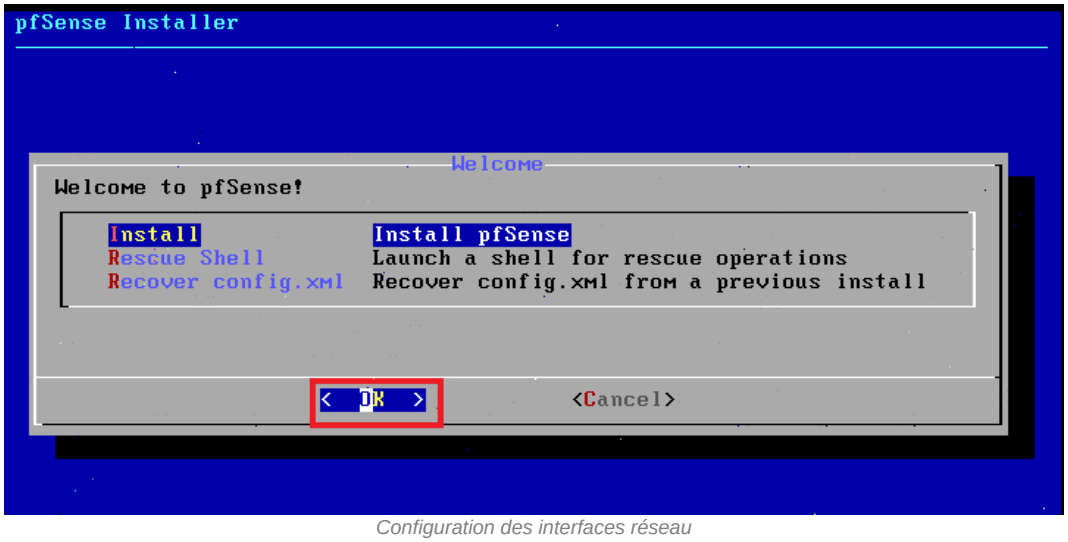
■■ Note : La configuration permanente du clavier sera effectuée via l'interface web dans la partie suivante.

6.2 Déclaration des interfaces

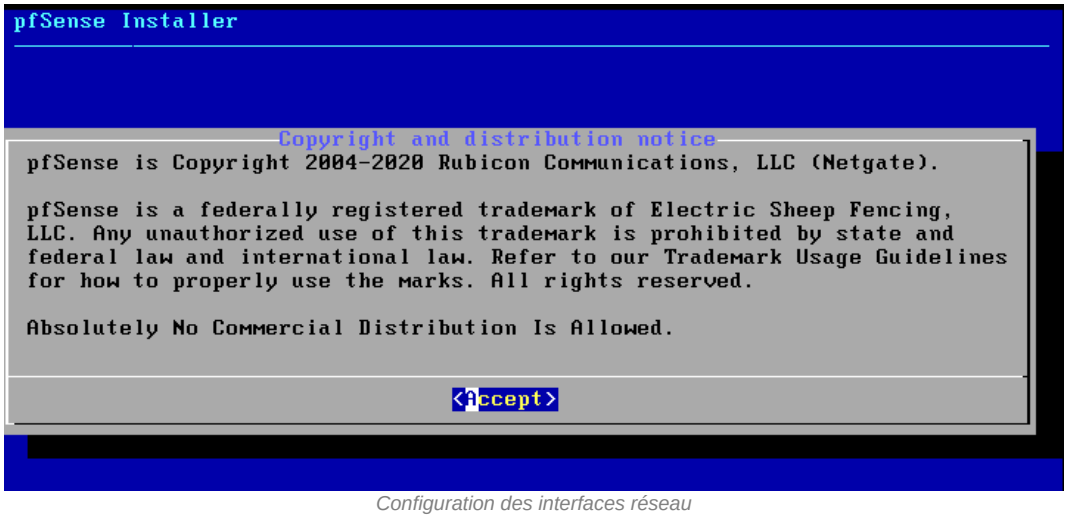
On choisit **l'option 1** dans le menu PfSense pour déclarer les trois interfaces (WAN, LAN et OPT1). À la fin de cette étape, les trois interfaces doivent être reconnues.



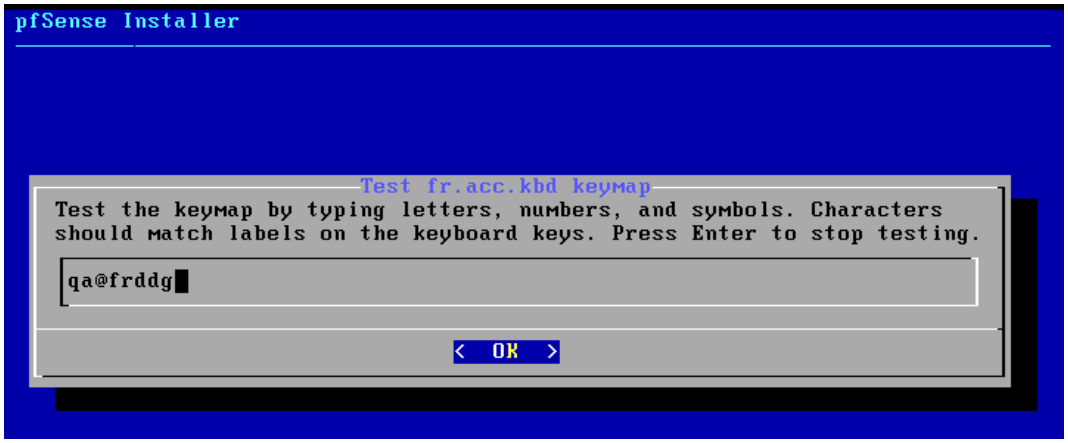
Configuration des interfaces réseau



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
```

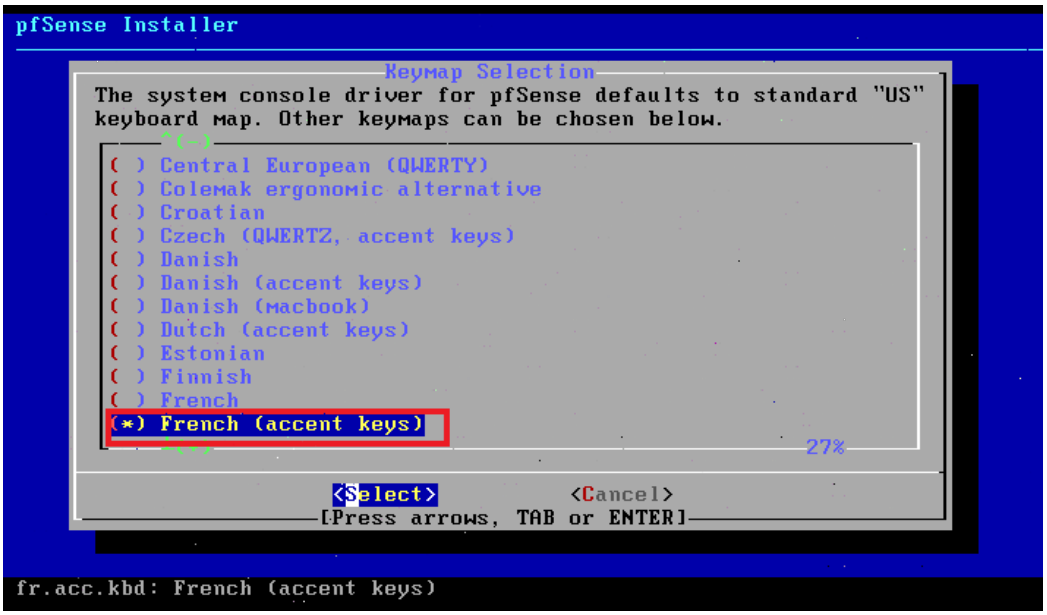
■■ Pour des raisons de sécurité, il est préférable de ne pas activer le configurateur web sur l'interface WAN.

Interface LAN (sitka_lan)

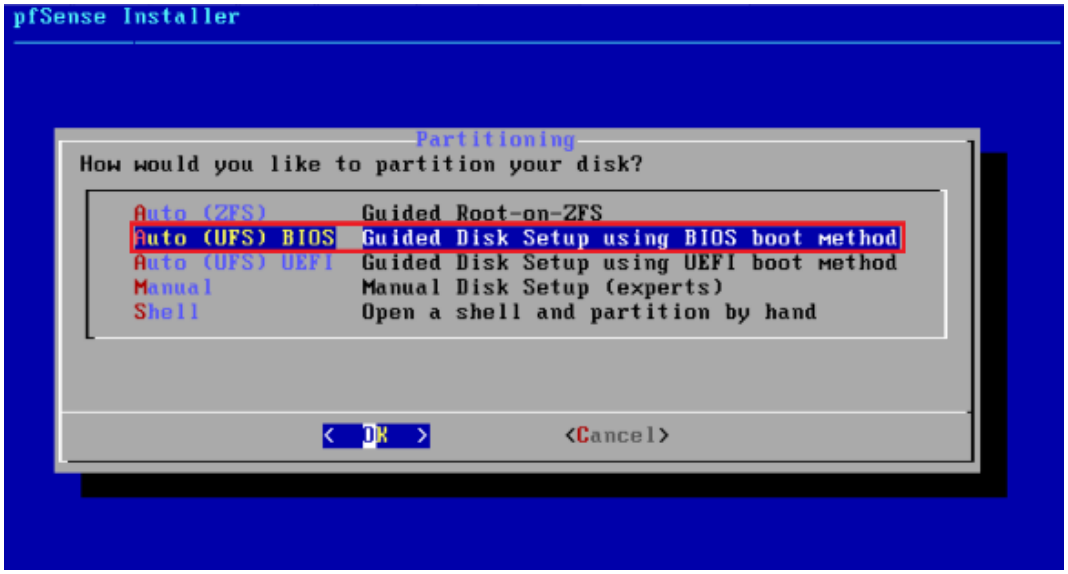
```
• Adresse IP : 172.20.0.250 • Masque : 255.255.255.0 • Pas de passerelle • DHCP activé : plage 172.20.0.20 → 172.20.0.30
```

Interface OPT1 (opt_lan)

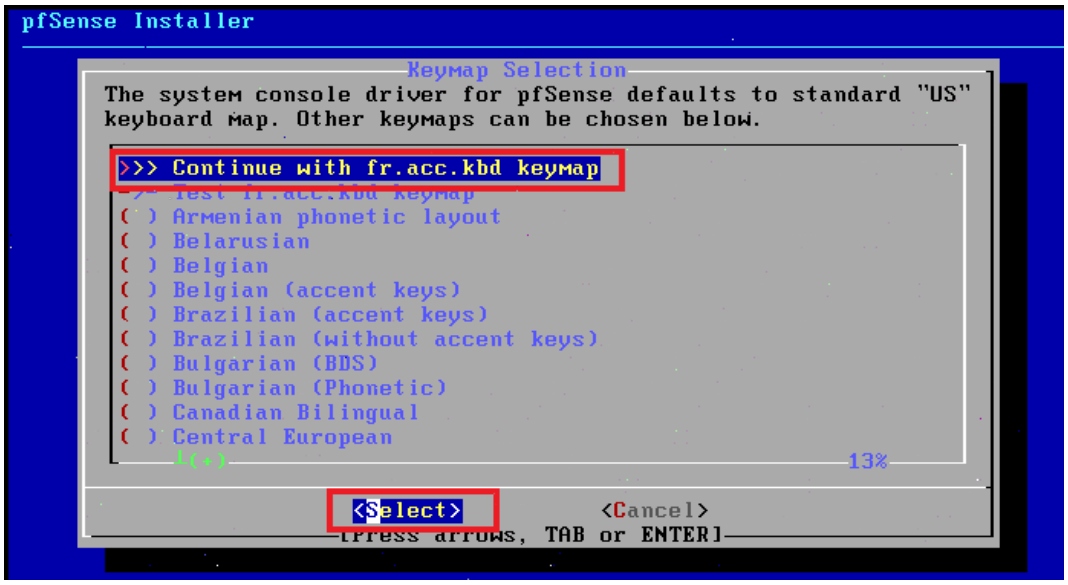
```
• Adresse IP : 192.168.2.250 • Masque : 255.255.255.0 • DHCP activé : plage à définir
```



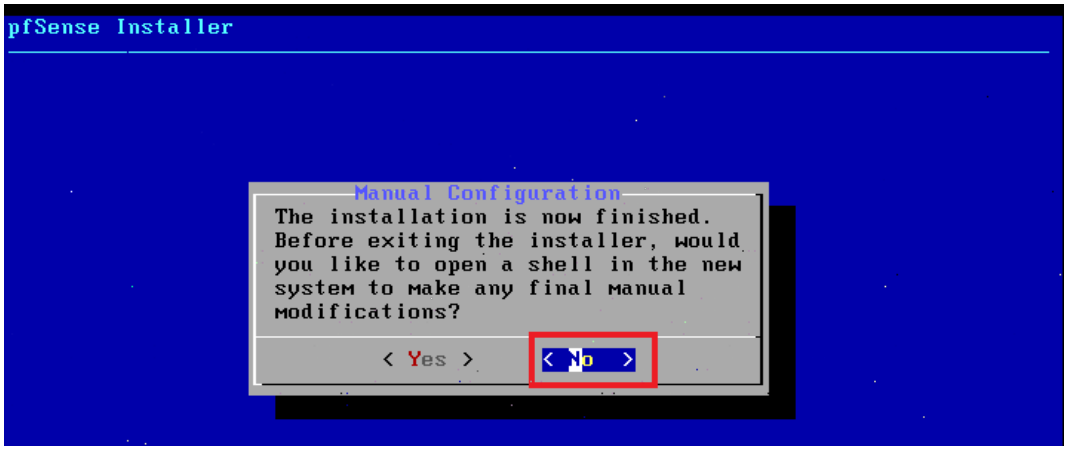
Configuration adresses IP – interface



Configuration adresses IP – interface



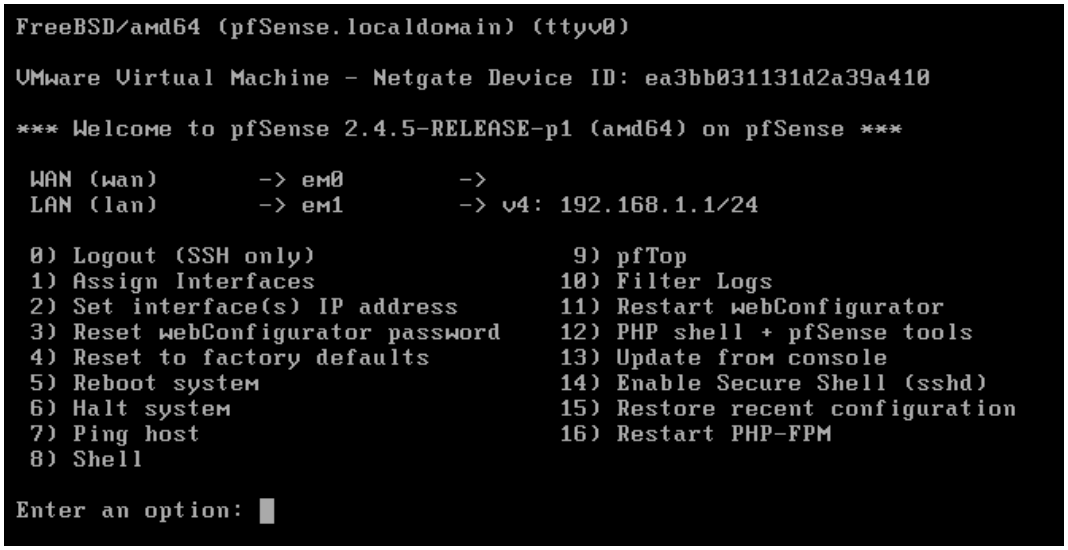
Configuration adresses IP – interface



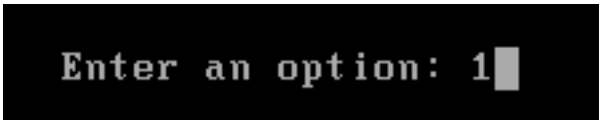
Configuration adresses IP – interface

Configuration adresses IP – interface

Configuration adresses IP – interface



Configuration adresses IP – interface



Configuration adresses 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 adresses IP – interface

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

Configuration adresses IP – interface

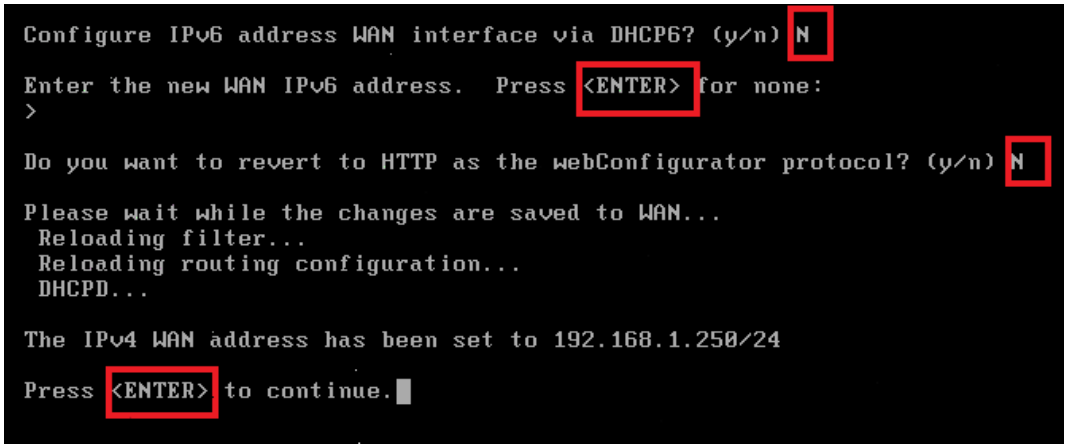
```
Carte Ethernet Ethernet :

   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(préféré)
   Adresse IPv4. . . . . . . . . . . . . . : 192.168.1.142(préféré)
   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
```

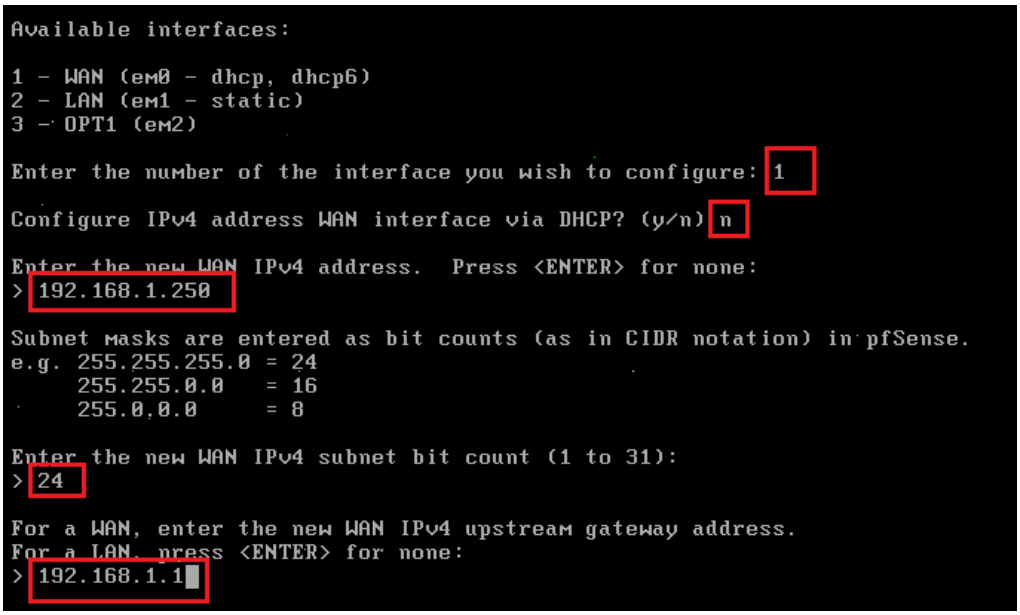
Configuration adresses IP – interface

```
Enter an option: 2
```

Configuration adresses IP – interface

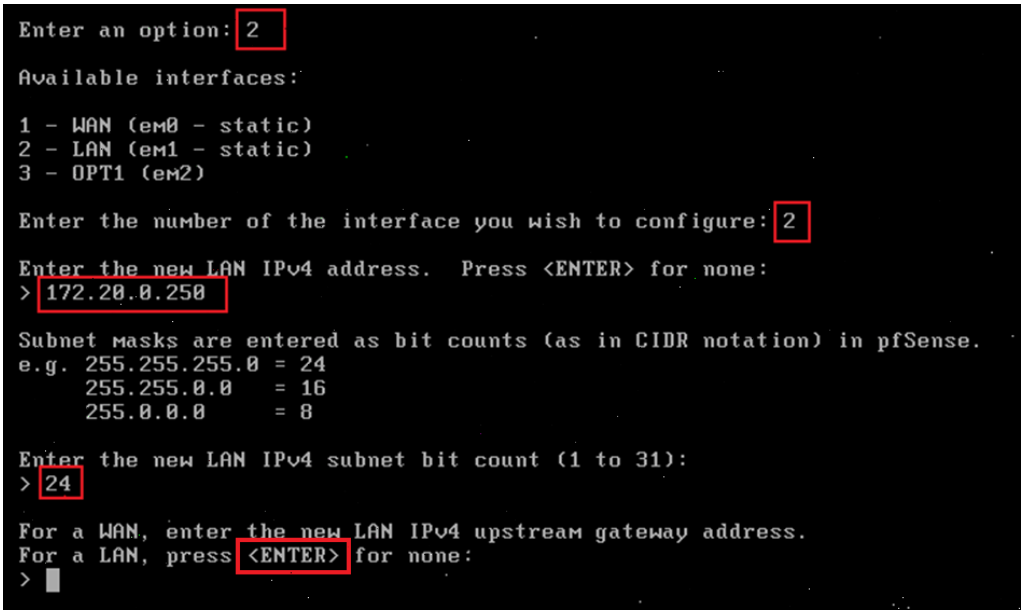


Configuration adresses IP – interface

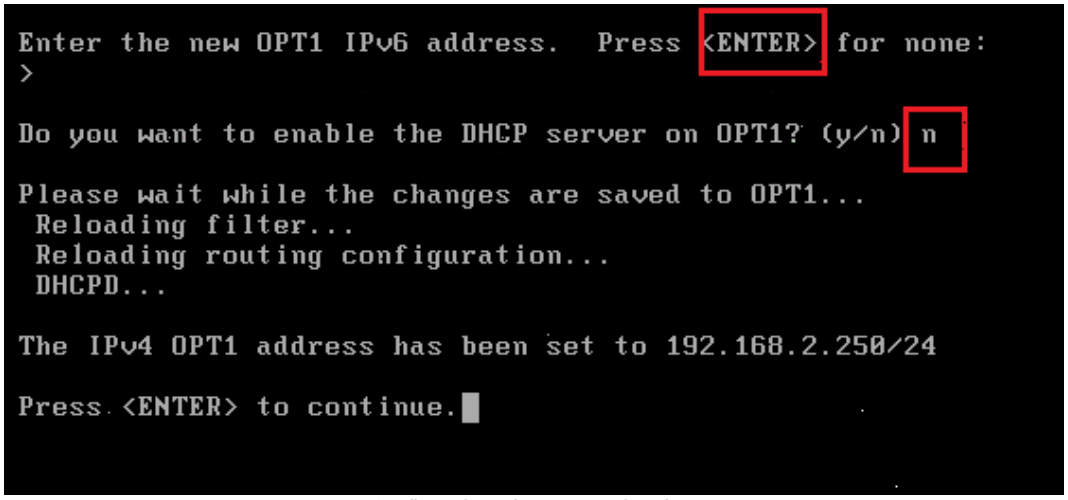


Configuration adresses IP – interface

Configuration adresses IP – interface



Configuration adresses IP – interface



Configuration adresses 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**

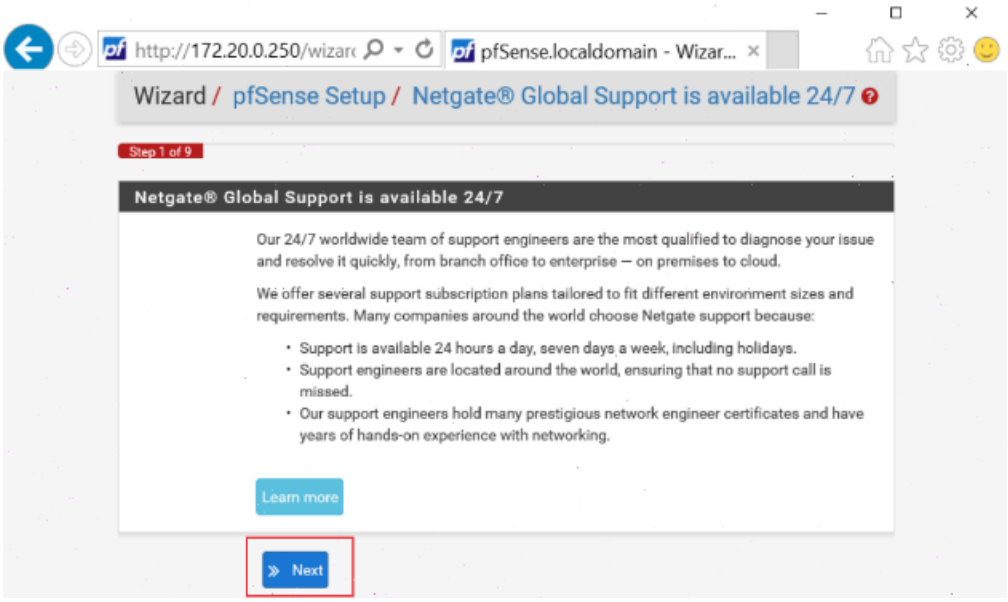
• Vérification des interfaces WAN et LAN (déjà configurées)

• Changement du mot de passe administrateur

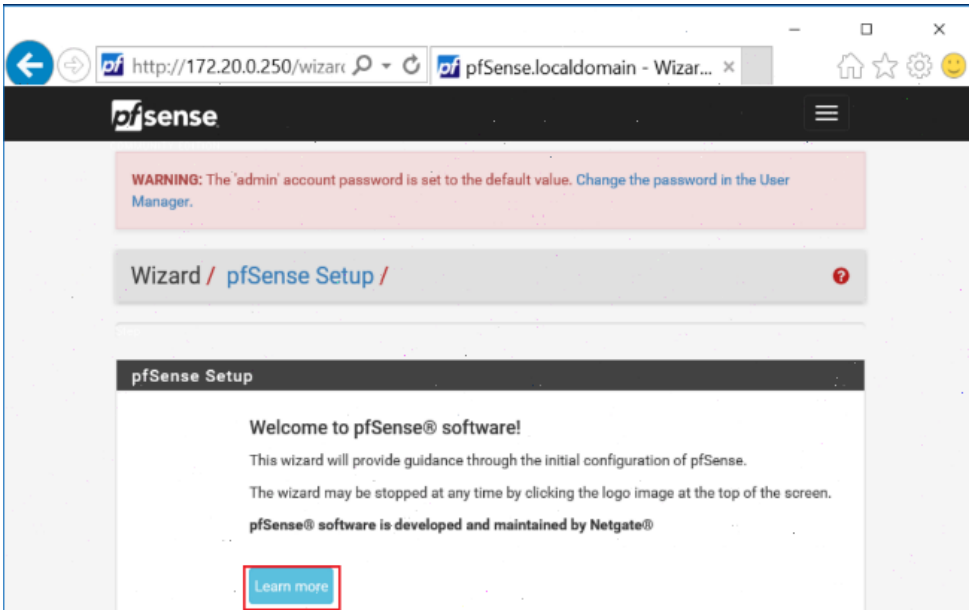
• Cliquer sur **Reload** puis **Finish**

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

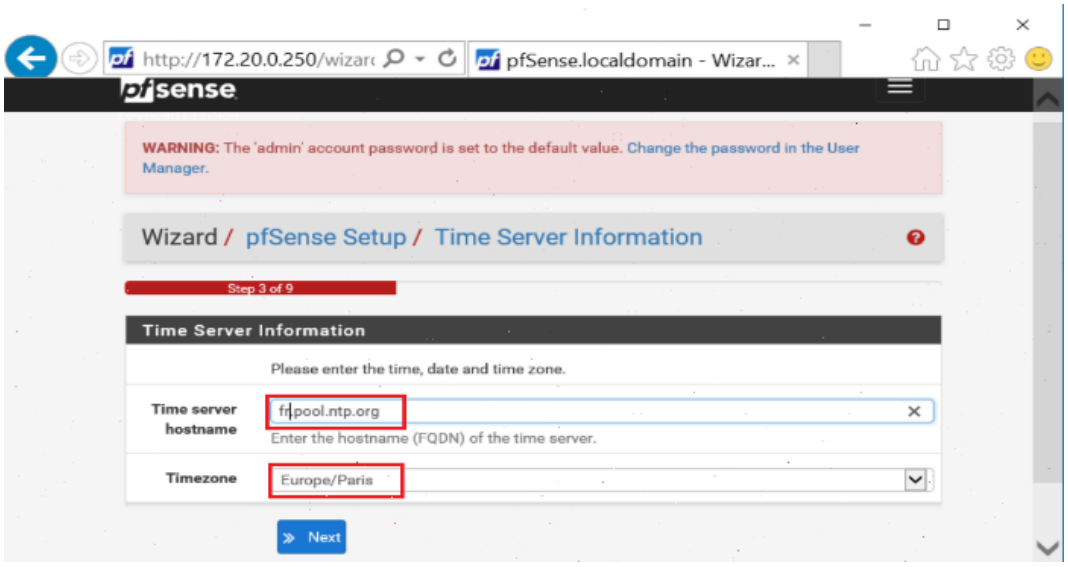
Assistant de configuration PfSense – étape 1



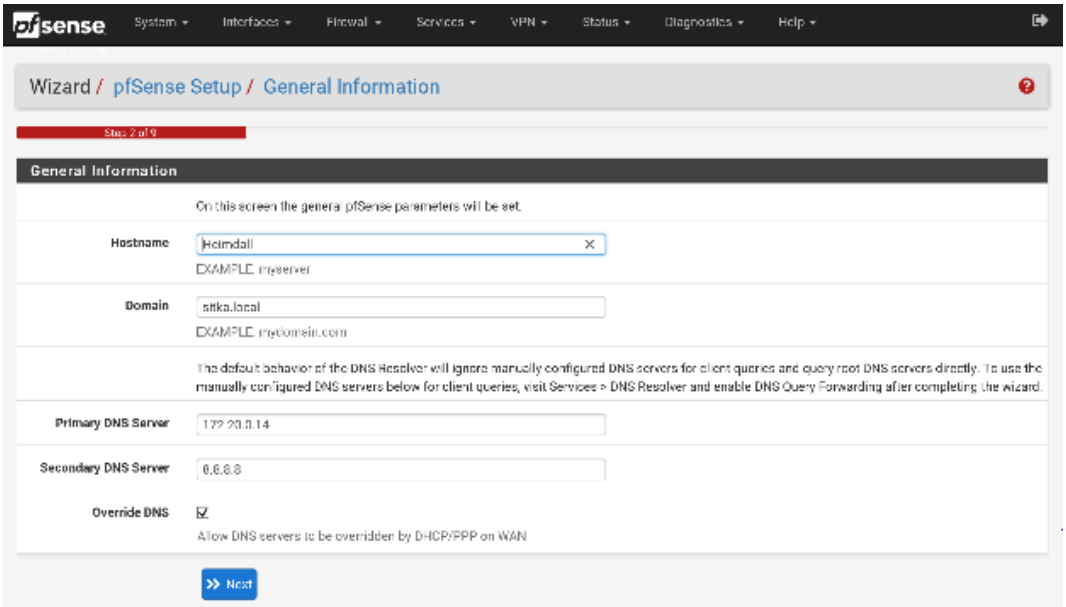
Assistant de configuration PfSense – étape 2



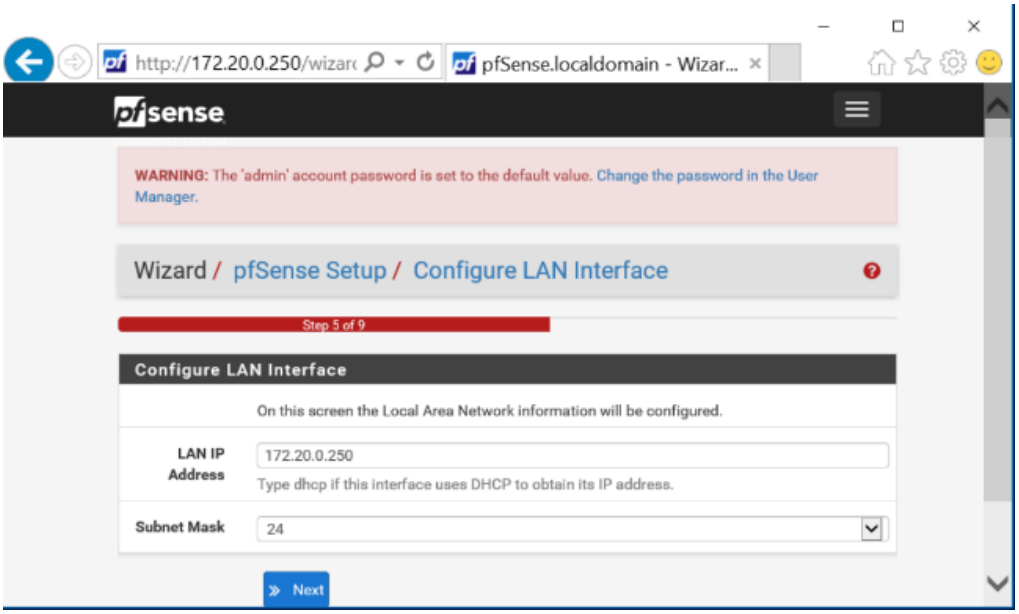
Assistant de configuration PfSense – étape 3



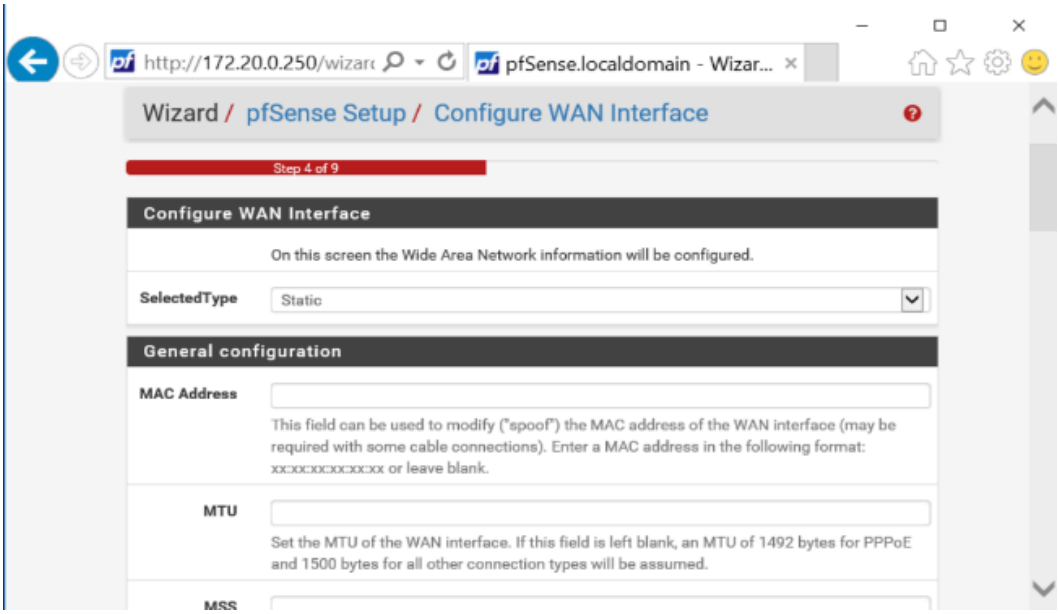
Assistant de configuration PfSense – étape 4



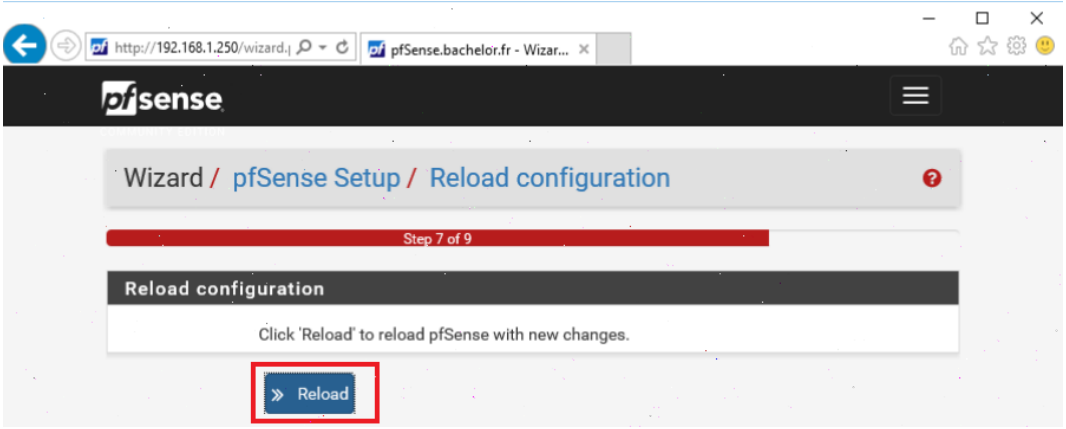
Assistant de configuration PfSense – étape 5



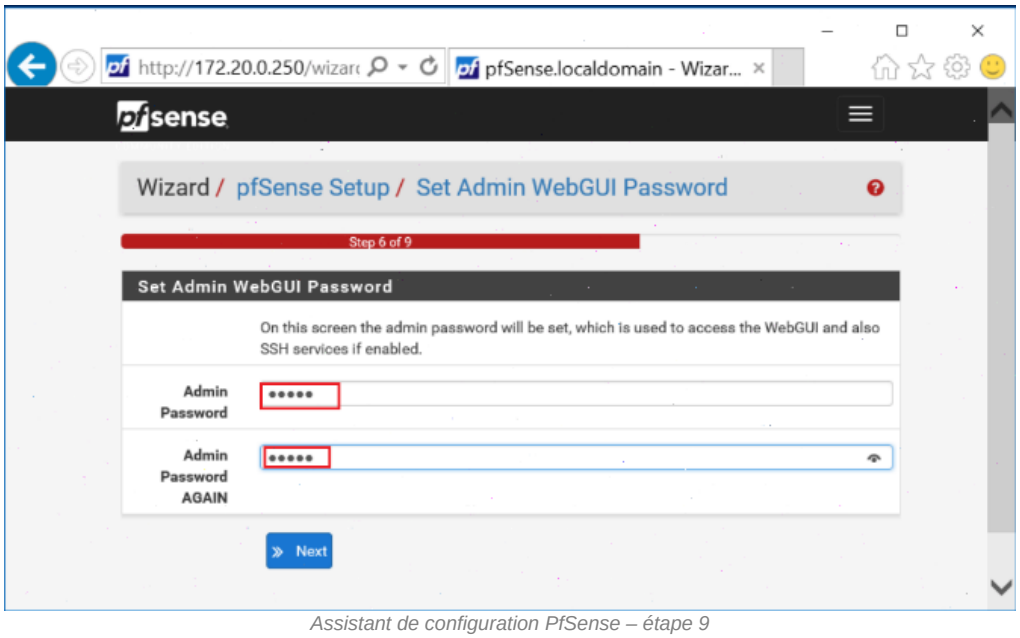
Assistant de configuration PfSense – étape 6



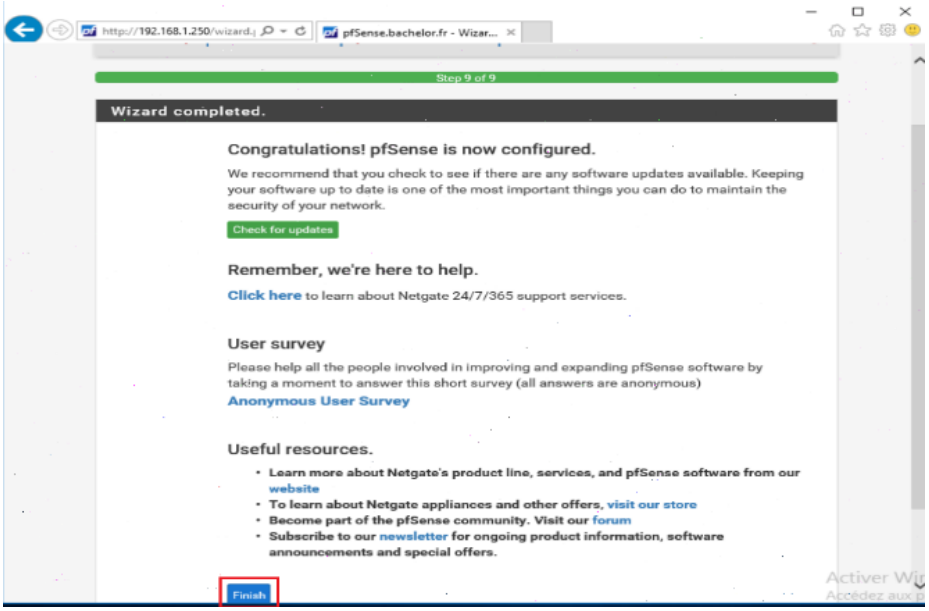
Assistant de configuration PfSense – étape 7



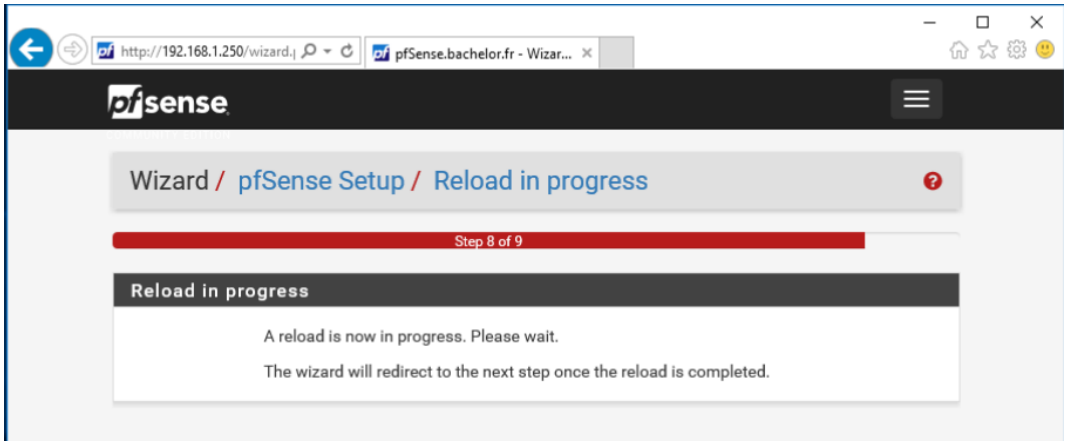
Assistant de configuration PfSense – étape 8



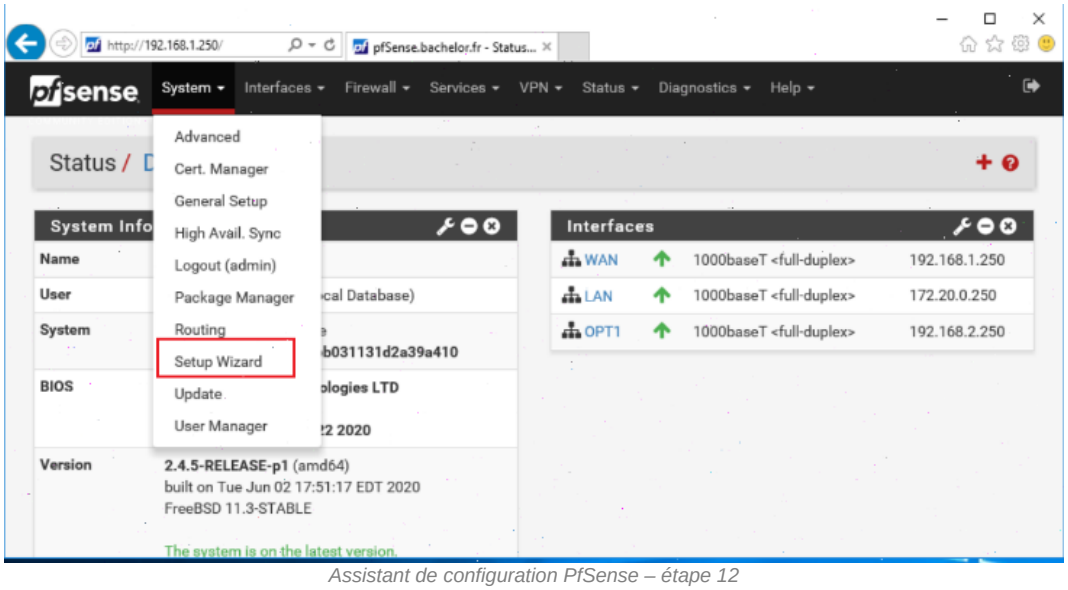
Assistant de configuration PfSense – étape 9



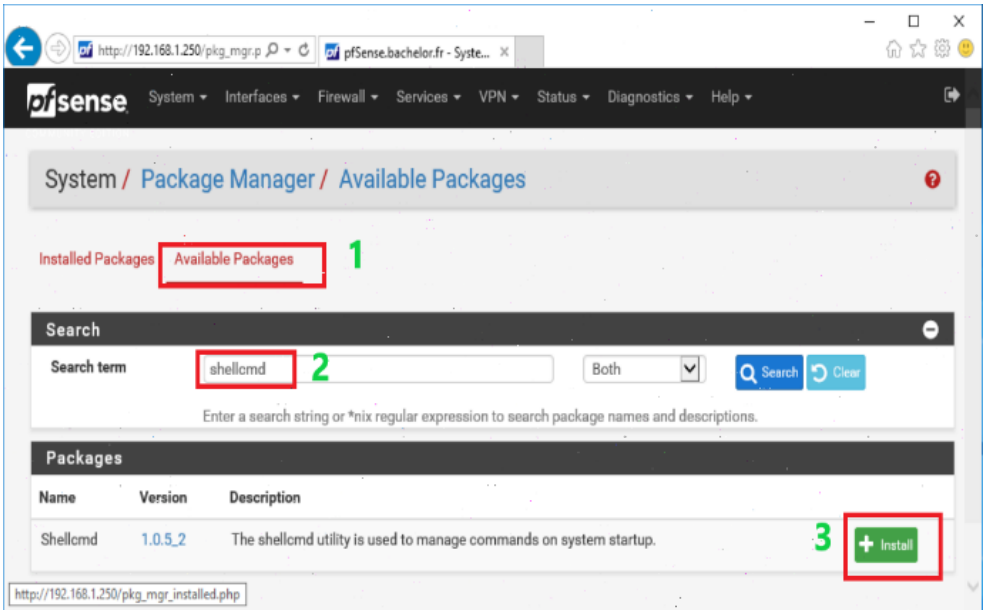
Assistant de configuration PfSense – étape 10



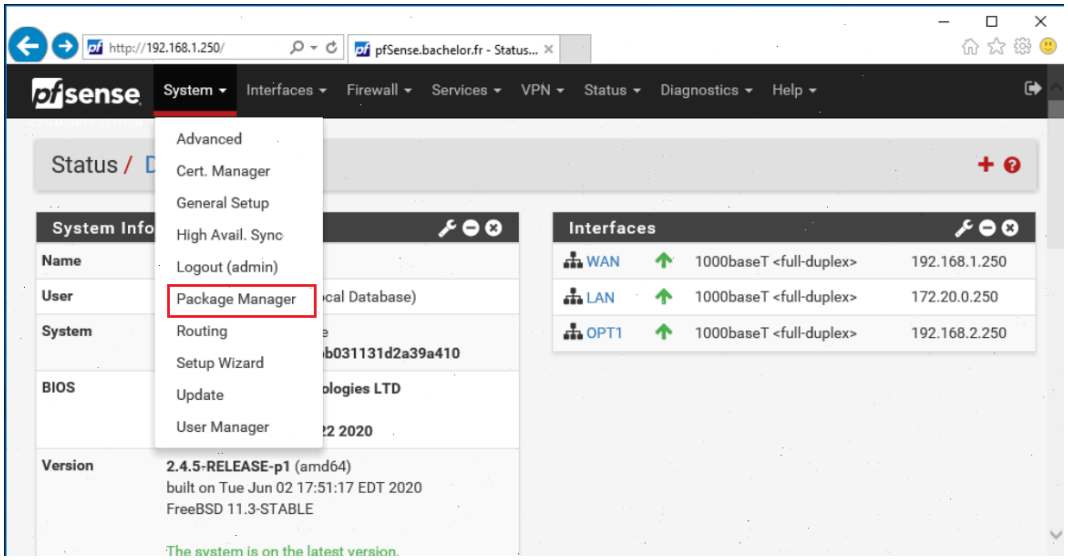
Assistant de configuration PfSense – étape 11



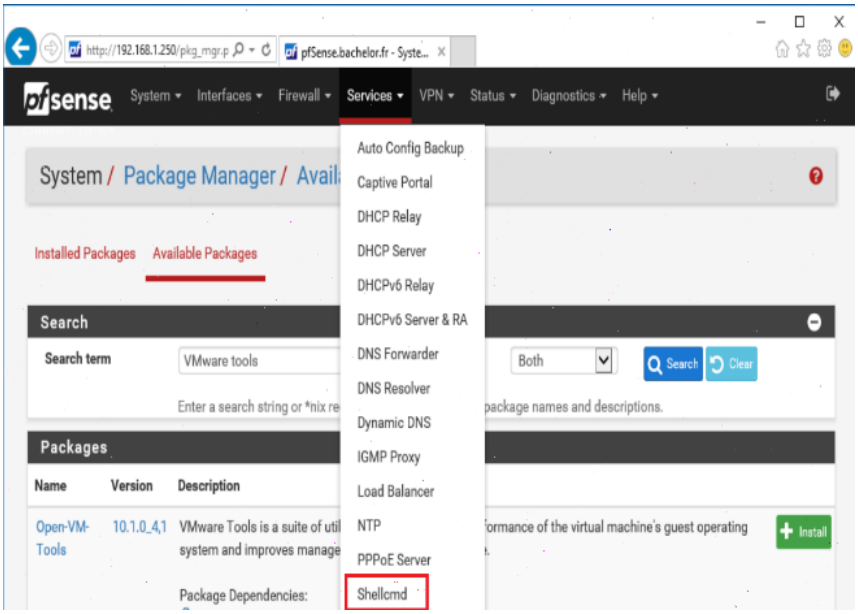
Assistant de configuration PfSense – étape 12



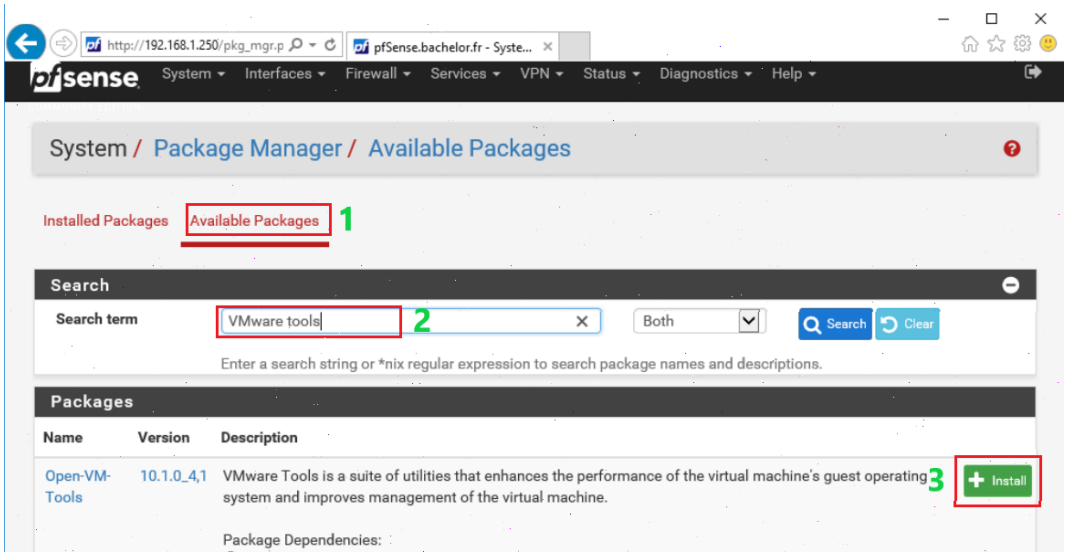
Assistant de configuration PfSense – étape 13



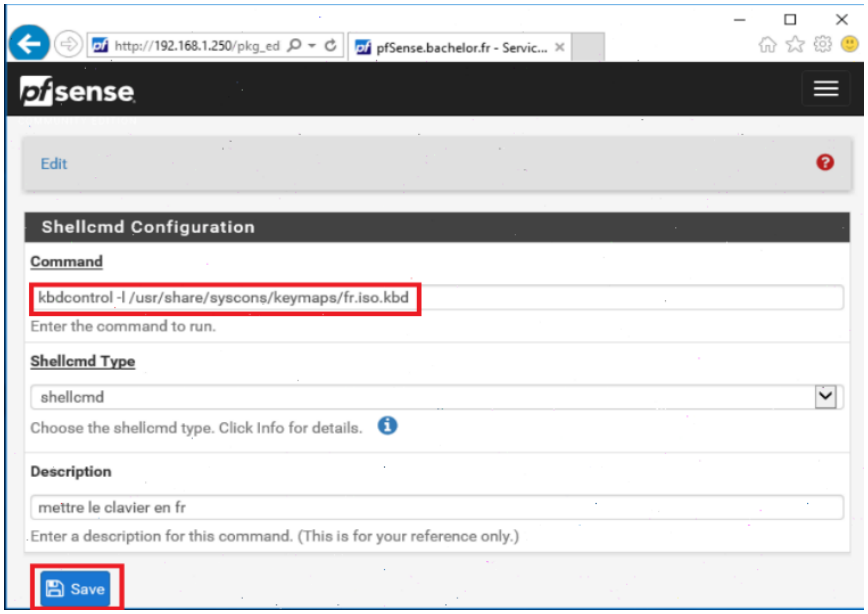
Assistant de configuration PfSense – étape 14



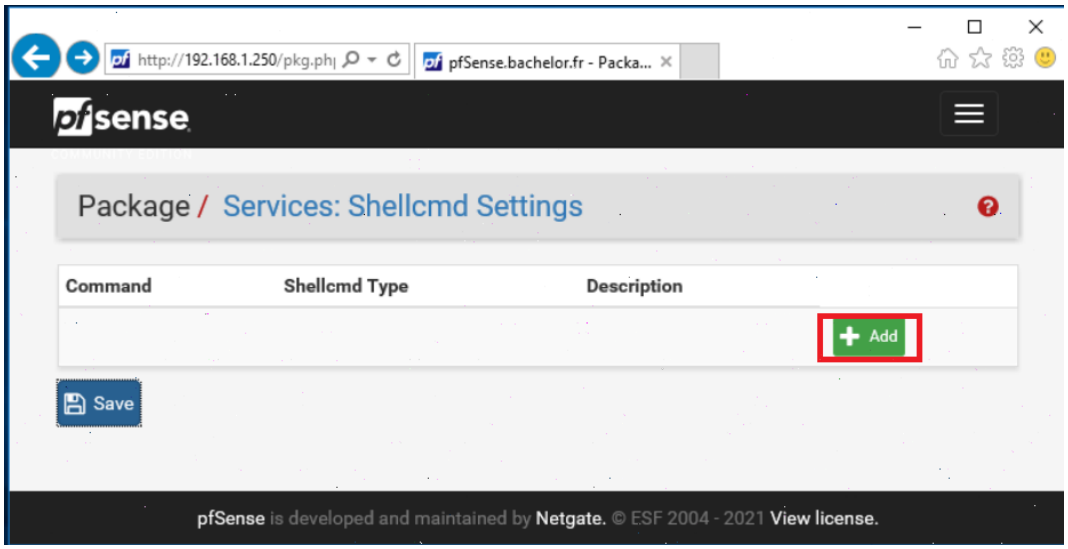
Assistant de configuration PfSense – étape 15



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

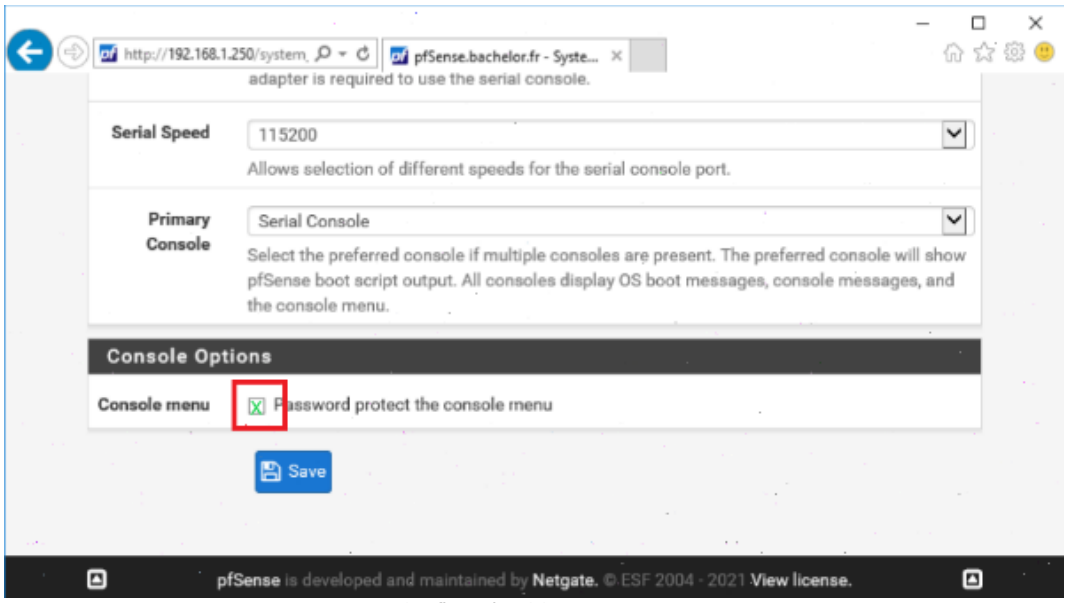
11. Sécurisation de l'accès SSH

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.

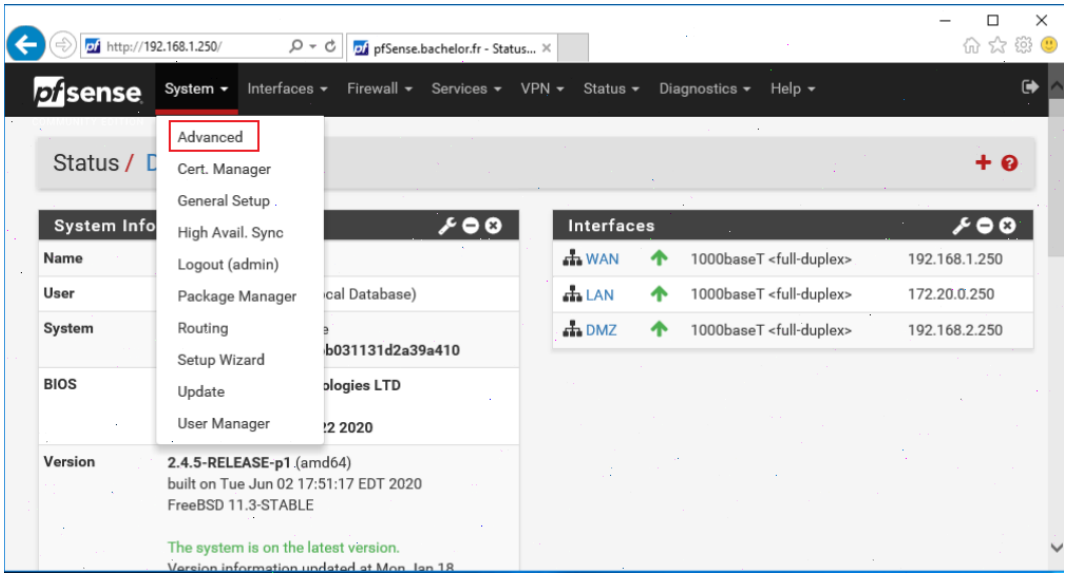
■■ Sur Windows Server 2016, SSH n'est pas installé nativement. Il est disponible nativement sur Windows 2019 et Windows 10.

Créer une règle autorisant SSH sur l'interface WAN :

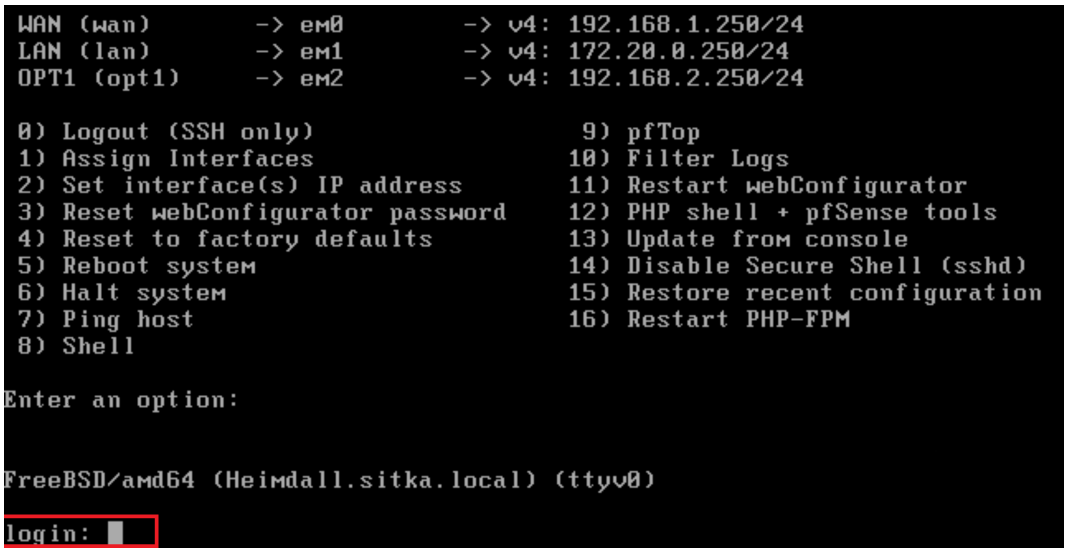
Aller dans **Firewall** → **Rules** → **WAN** → **Add** et renseigner les paramètres pour autoriser le port SSH configuré (2121). Enregistrer et appliquer les changements.



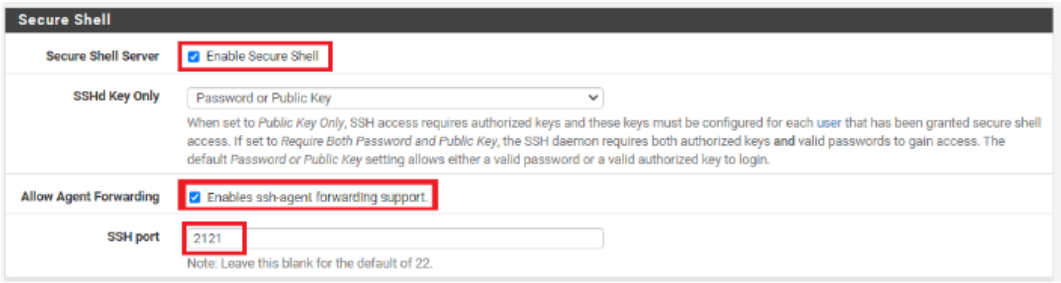
Configuration SSH – capture 1



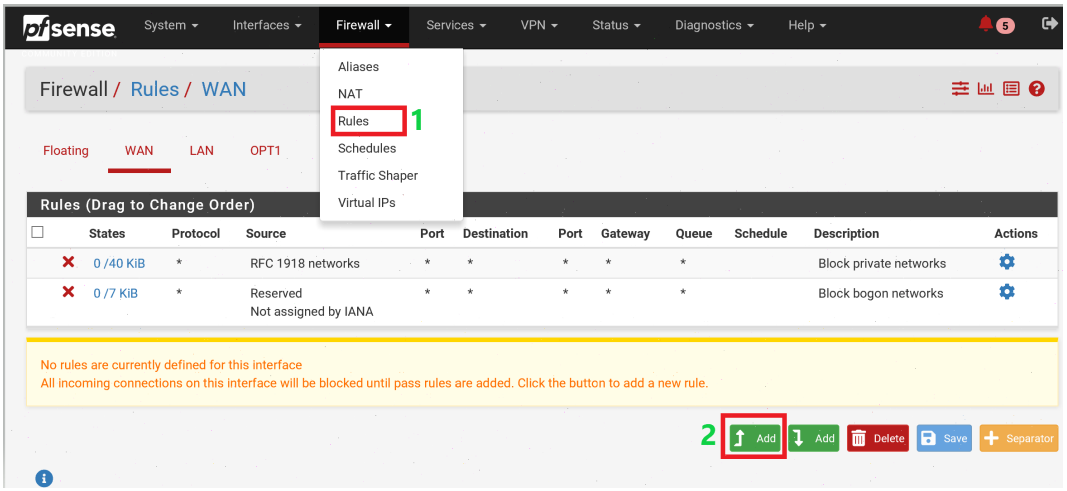
Configuration SSH – capture 2



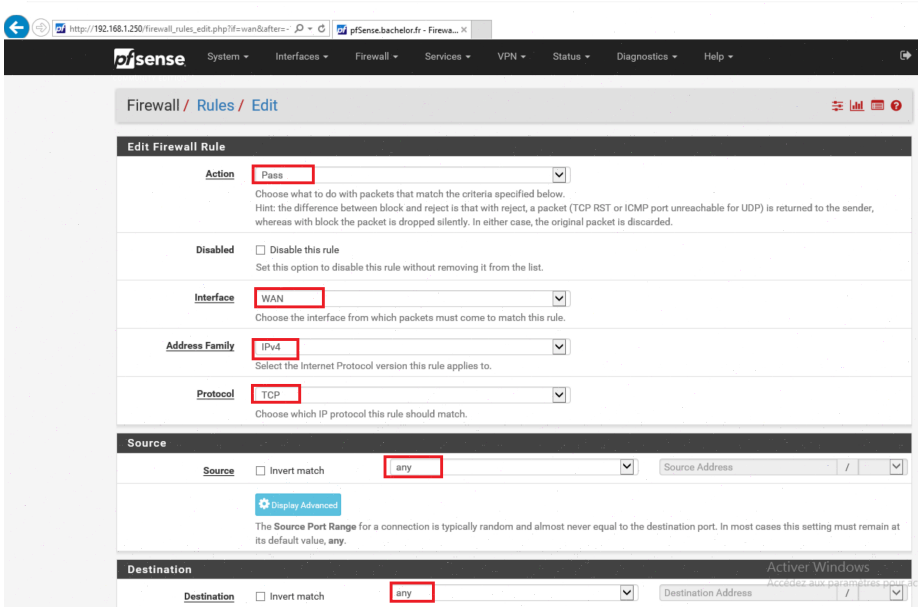
Configuration SSH – capture 3



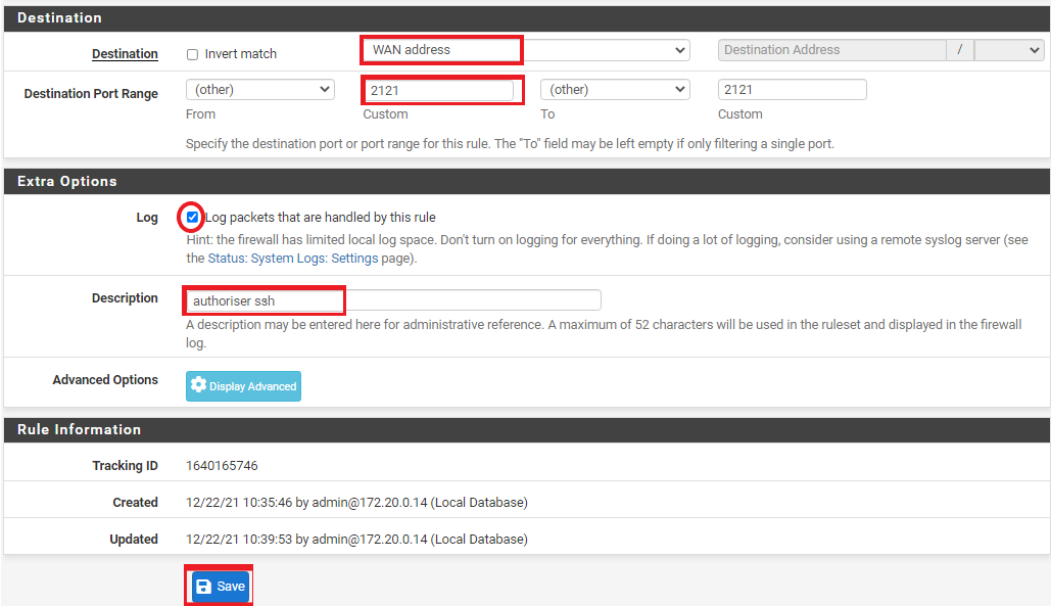
Configuration SSH – capture 4



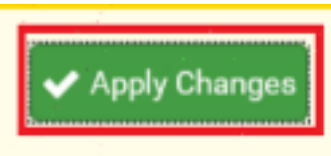
Configuration SSH – capture 5



Configuration SSH – capture 6



Configuration SSH – capture 7



Configuration SSH – capture 8

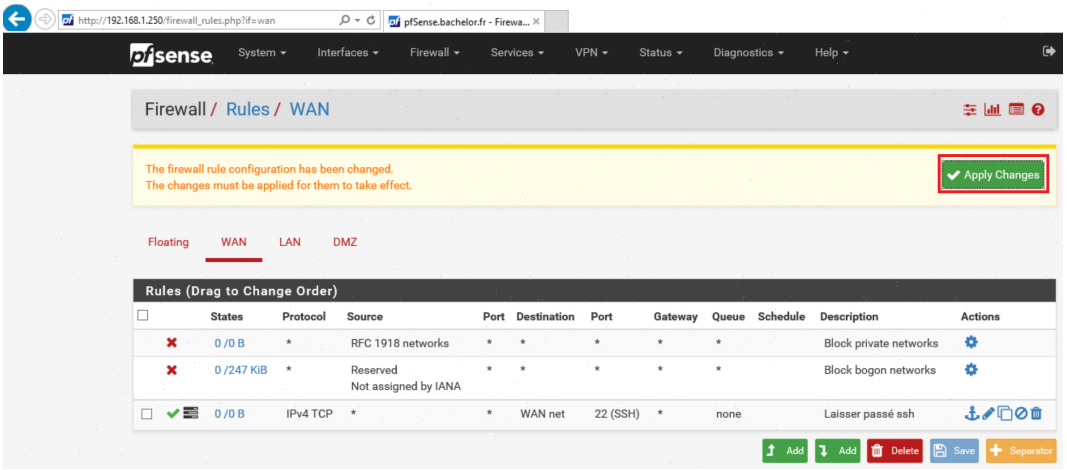
Configuration SSH – capture 9

Test de connexion SSH

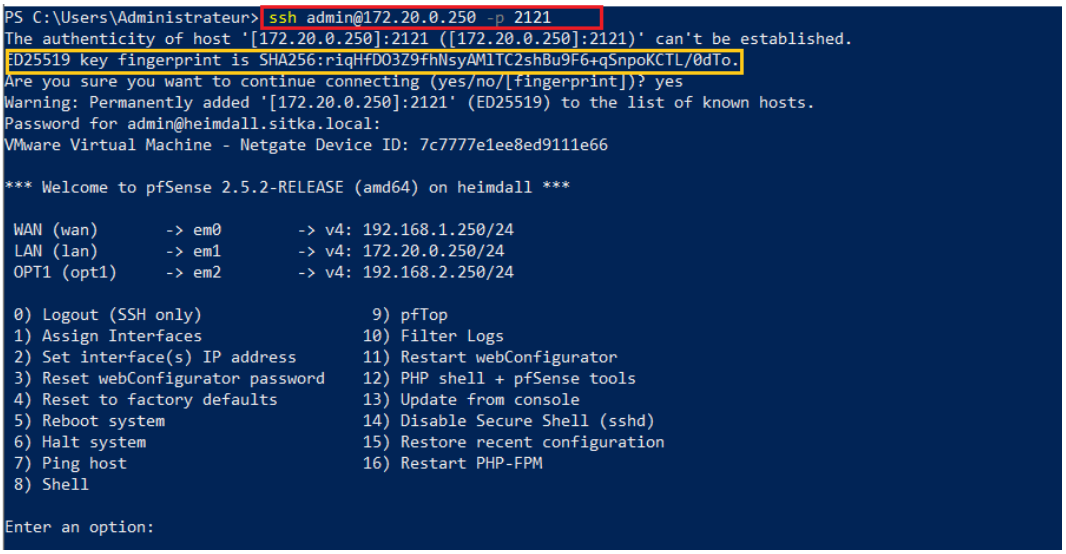
Pour tester la connexion depuis l'intérieur du réseau, depuis la machine AD :

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

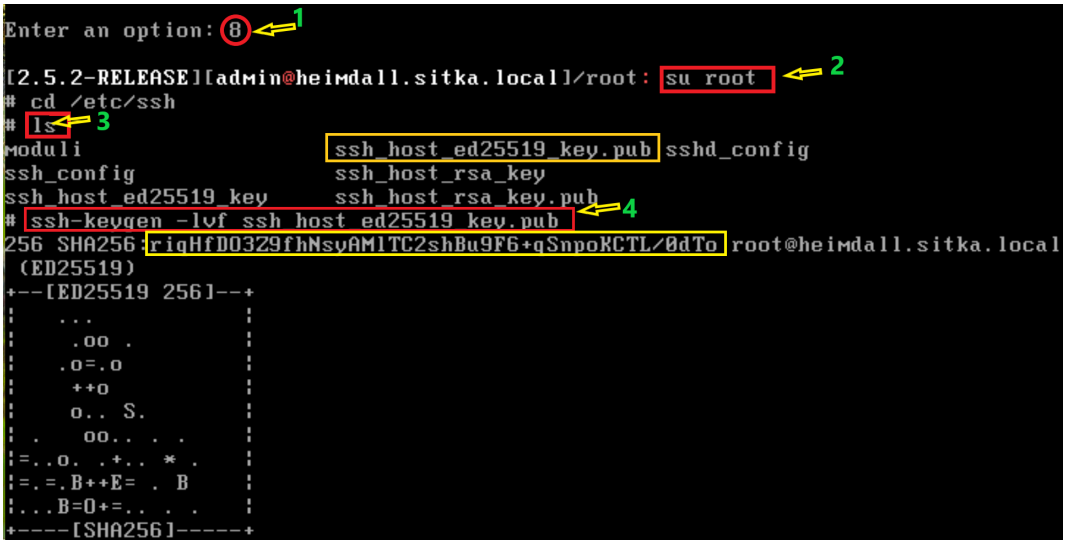
Pour une connexion depuis l'extérieur (via l'adresse publique), il faut : • Ouvrir le port sur la box internet (redirection de port) • Utiliser son adresse IP publique (vérifiable sur http://www.whatismyip.com) • Se mettre en 4G sur smartphone (pas en Wi-Fi du même réseau) • Utiliser un client SSH mobile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



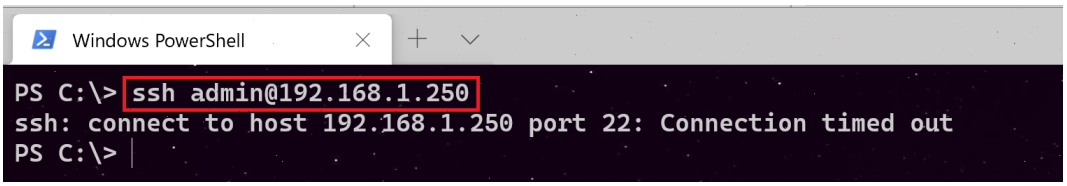
Test de connexion SSH



Test de connexion SSH



Test de connexion SSH

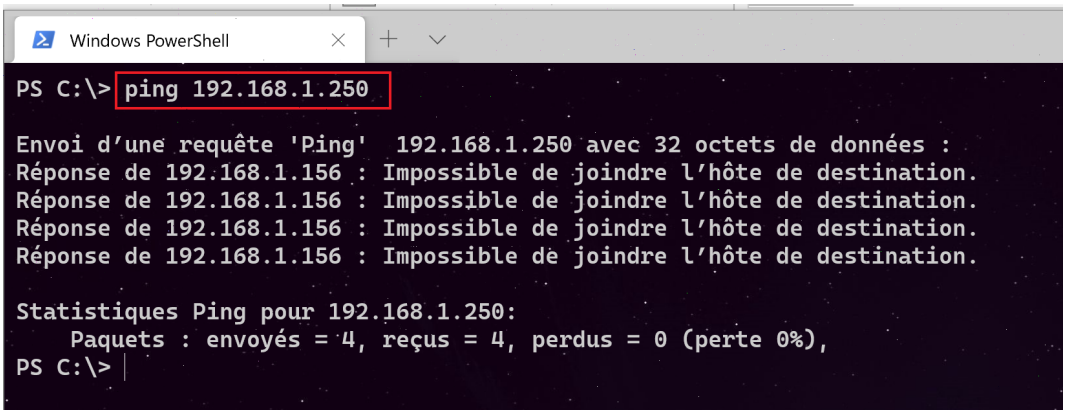


Test de connexion SSH

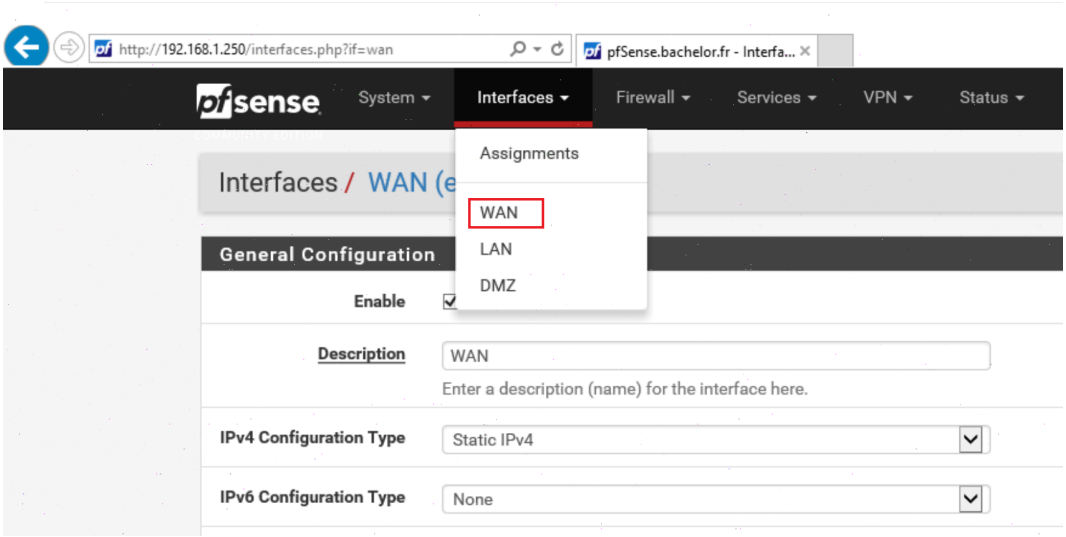
12. Sécurisation de l'interface web par HTTPS

12.1 Création d'une autorité de certification interne

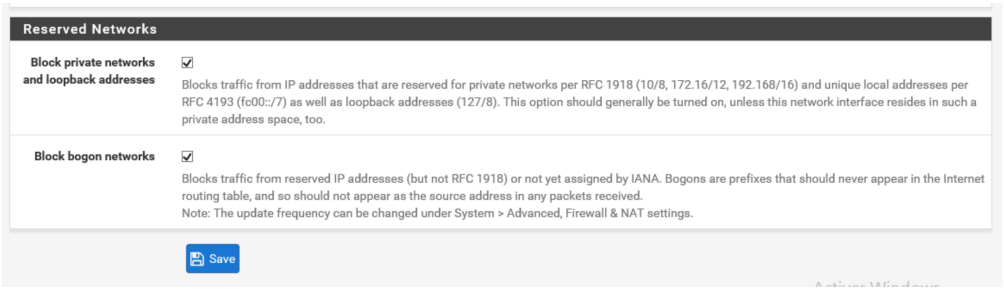
Aller dans **Système** → **Cert Manager** et créer une nouvelle autorité de certification interne en remplissant les champs requis (nom, pays, organisation, etc.).



Création de l'autorité de certification



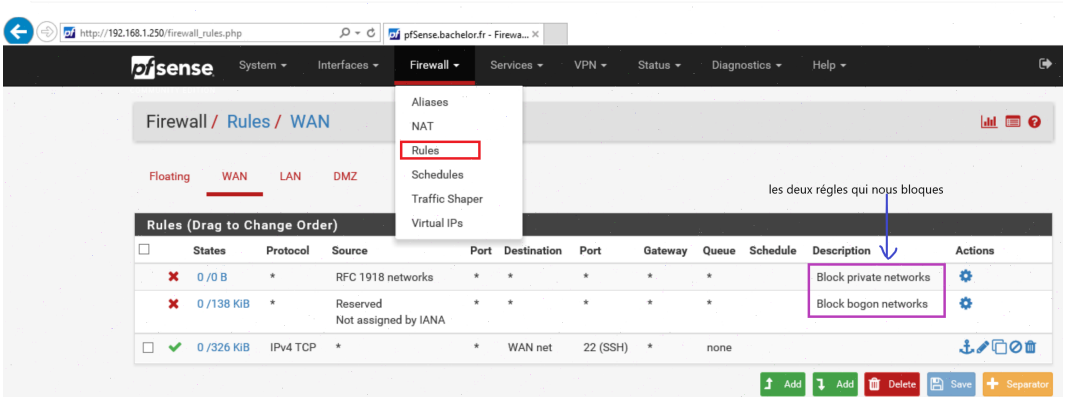
Création de l'autorité de certification



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.).



Génération du certificat web

Génération du certificat web

Génération du certificat web

12.3 Injection du certificat dans PfSense

Aller dans **Système** → **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

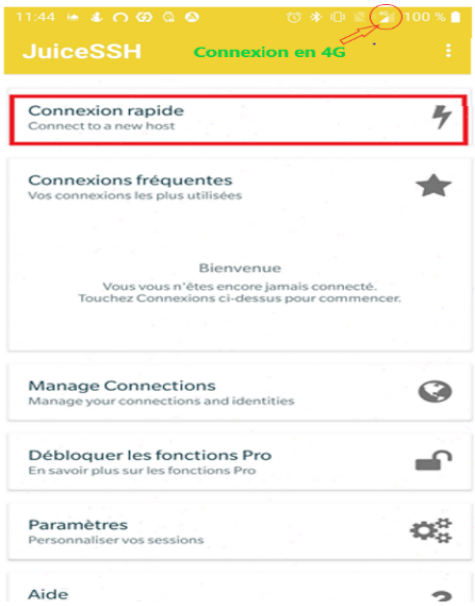
• Interdire au navigateur d'enregistrer les données de connexion

```
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.

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)

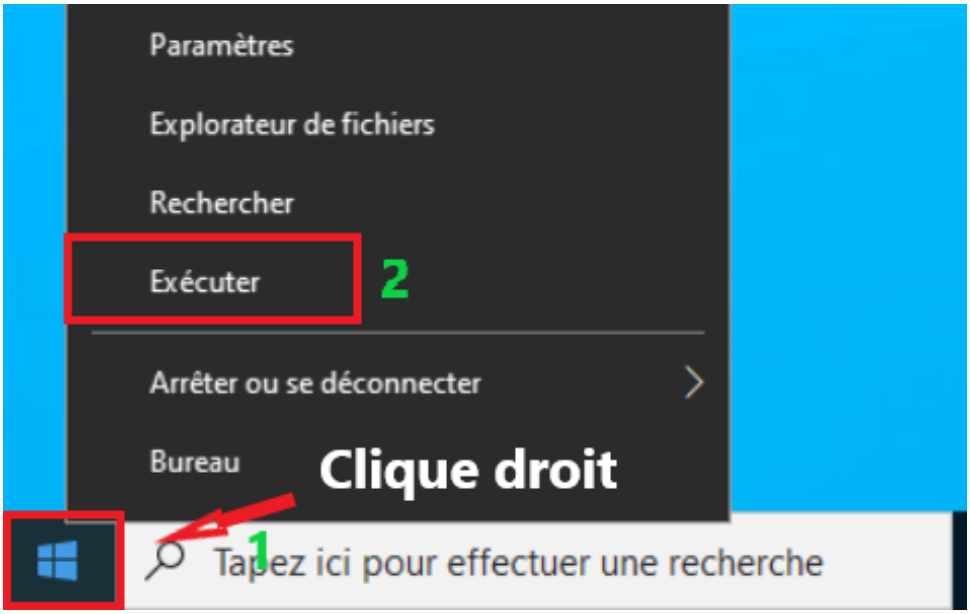
Sur le contrôleur de domaine hermes, tester la connectivité LDAP standard en ouvrant **ldp.exe** (clic droit sur Démarrer → Exécuter → ldp.exe). Se connecter avec le nom du serveur **hermes.sitka.local** et le port **389**.

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

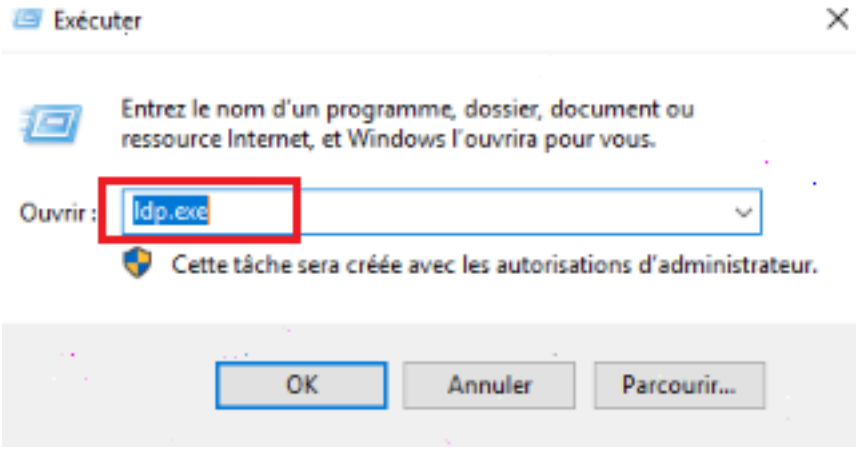


Erreur lors du test LDAPS (certificat manquant)

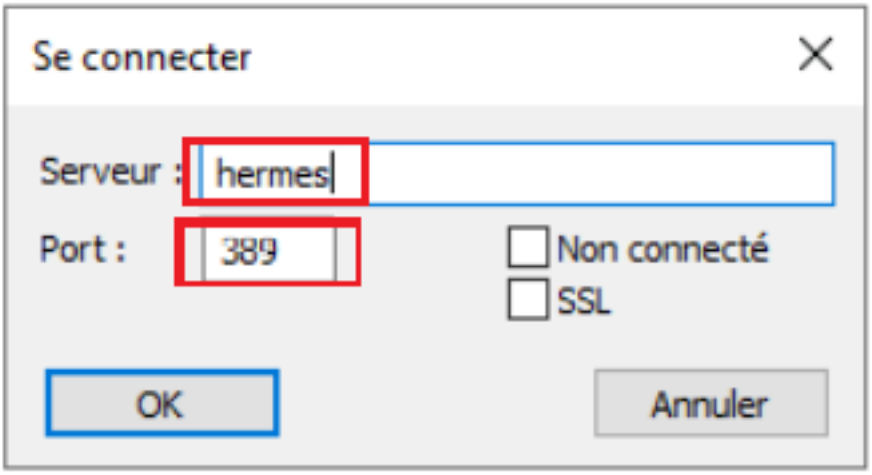
14. Création d'une autorité de certification sur hermes

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**.

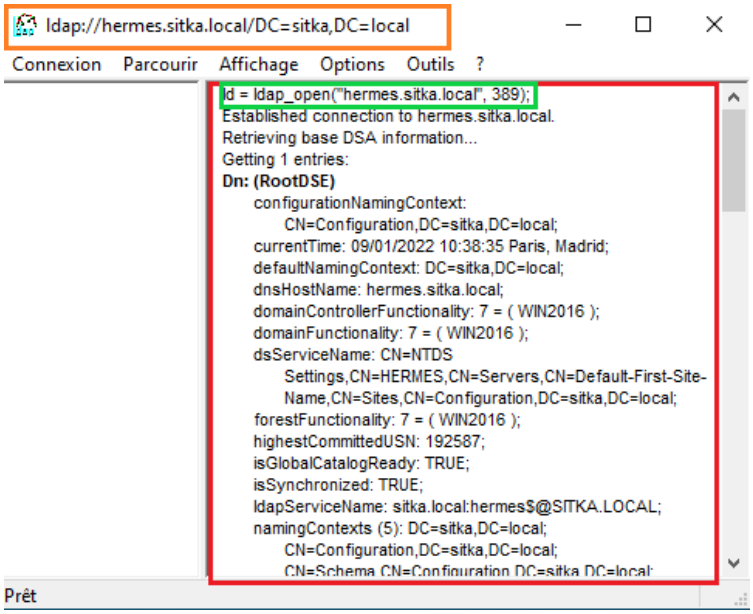


Installation du rôle Certificats Active Directory



Installation du rôle Certificats Active Directory

Installation du rôle Certificats Active Directory



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

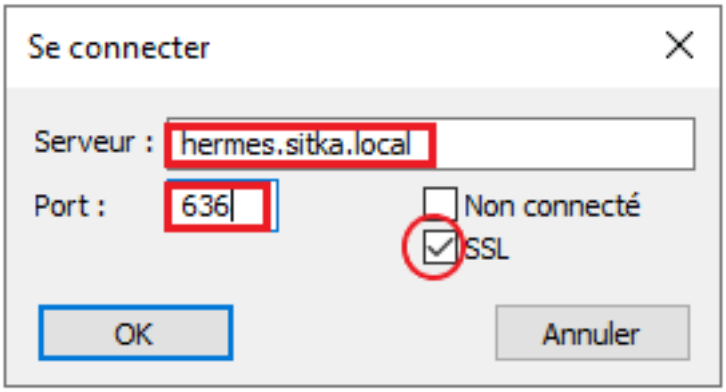
• Choisir les algorithmes de chiffrement (RSA 2048 bits recommandé)

• Définir le nom commun : **hermes-CA**

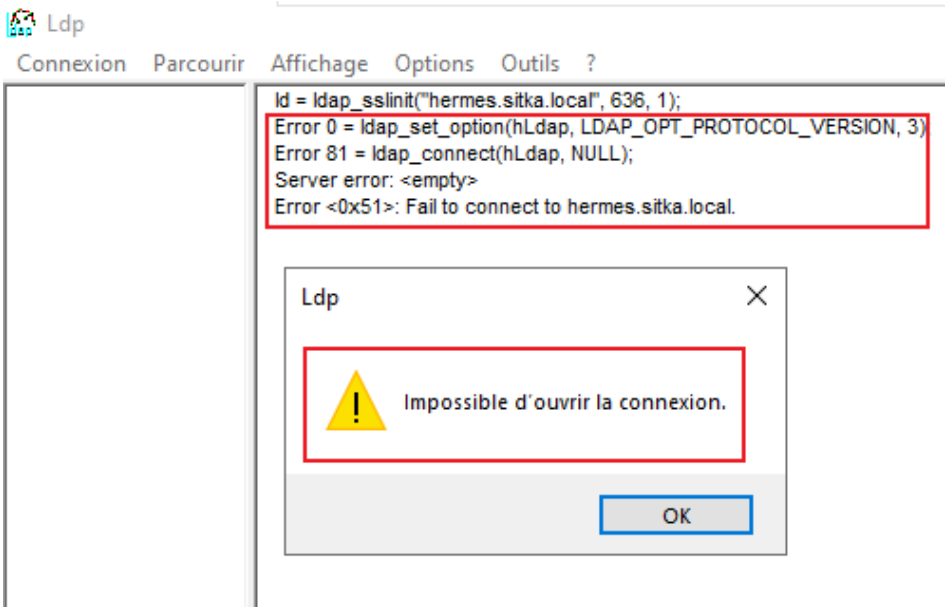
• Définir la période de validité (doit être supérieure aux certificats émis)

• Laisser les dossiers par défaut pour les bases de données

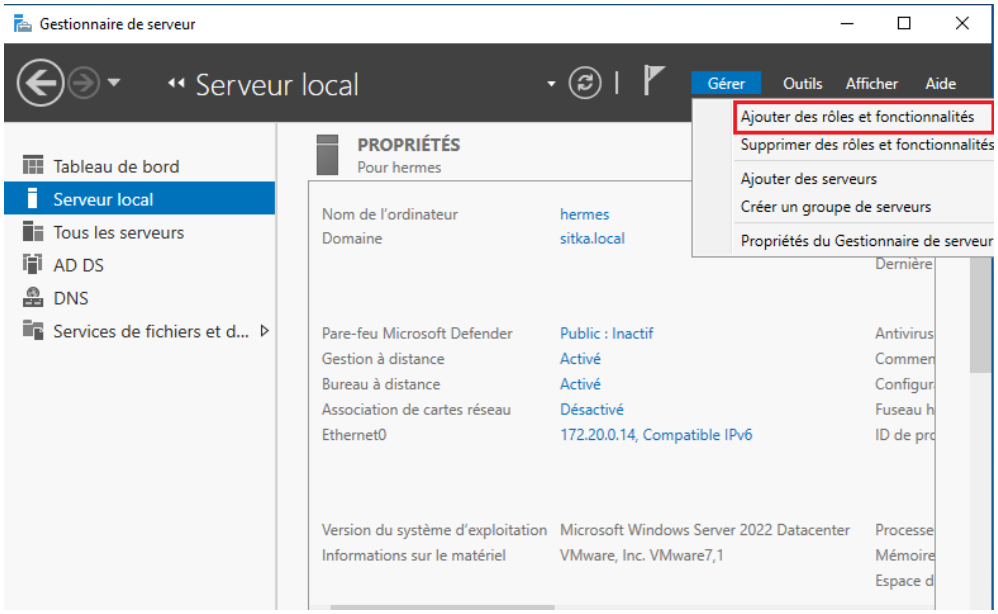
■■ Ce type d'autorité de certification couplé à Active Directory est adapté pour un intranet mais est déconseillé pour un accès public.



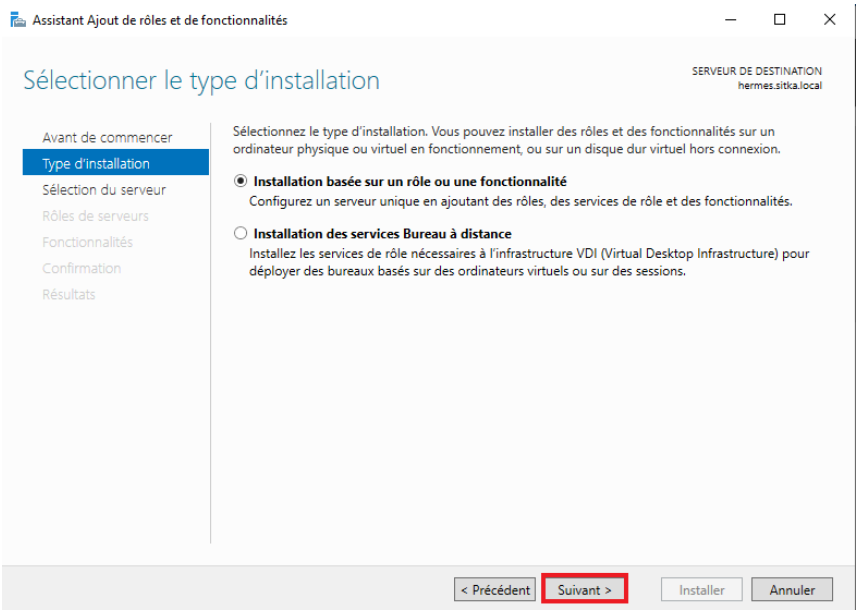
Configuration de l'autorité de certification hermes-CA



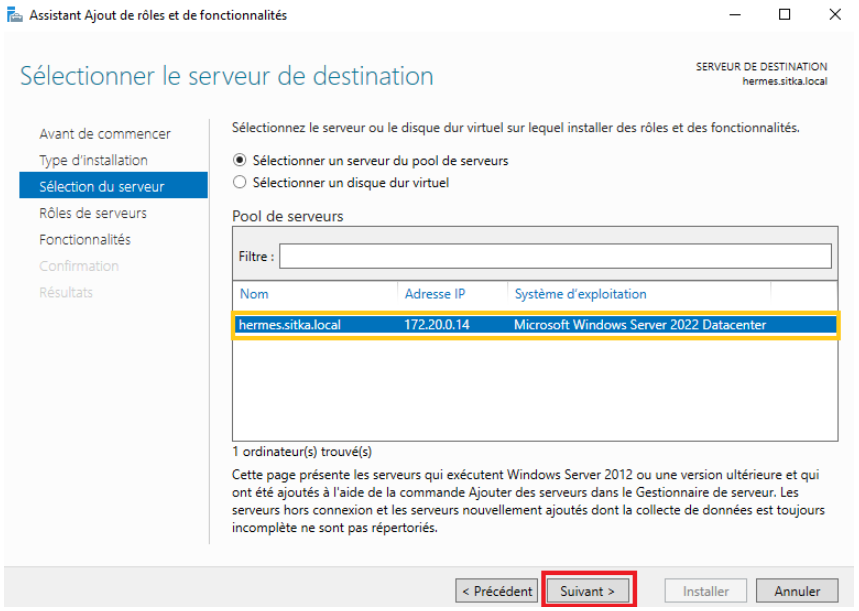
Configuration de l'autorité de certification hermes-CA



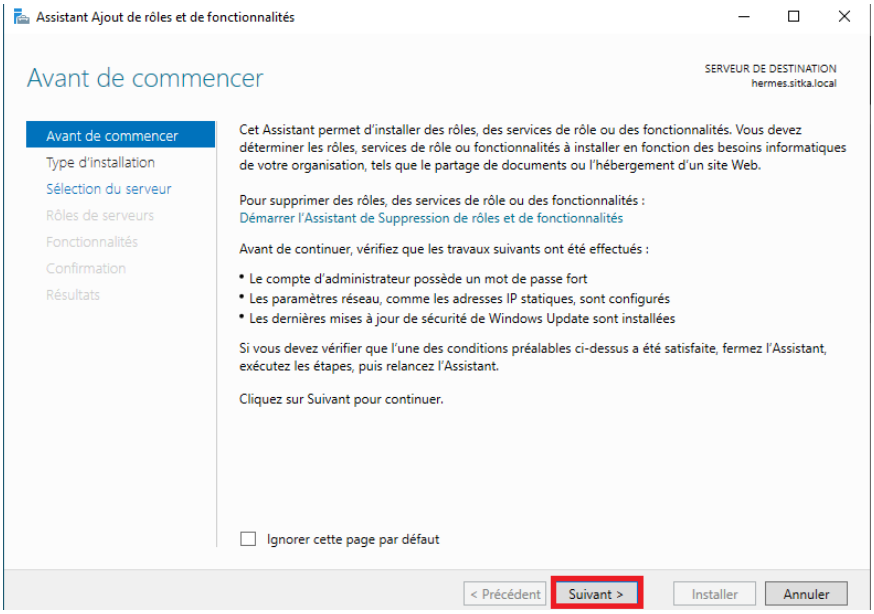
Configuration de l'autorité de certification hermes-CA



Configuration de l'autorité de certification hermes-CA

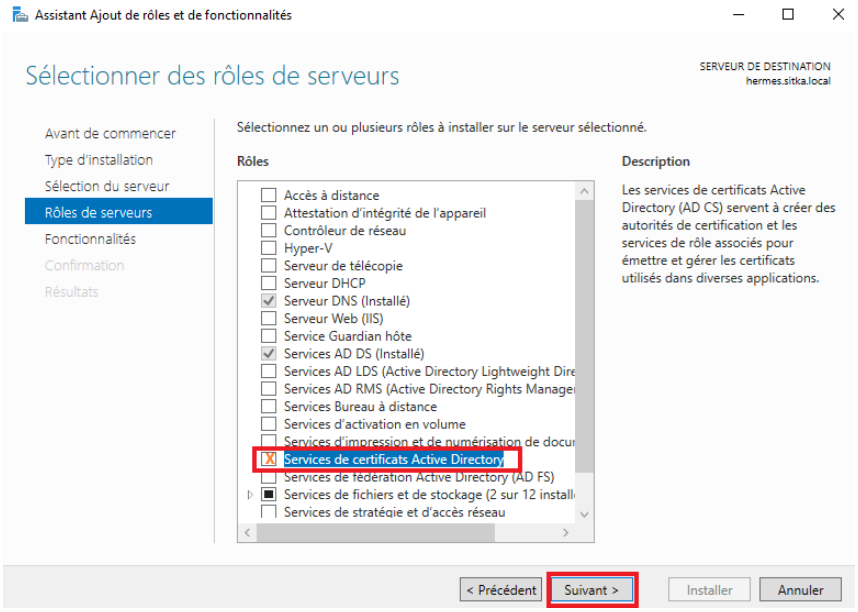


Configuration de l'autorité de certification hermes-CA



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

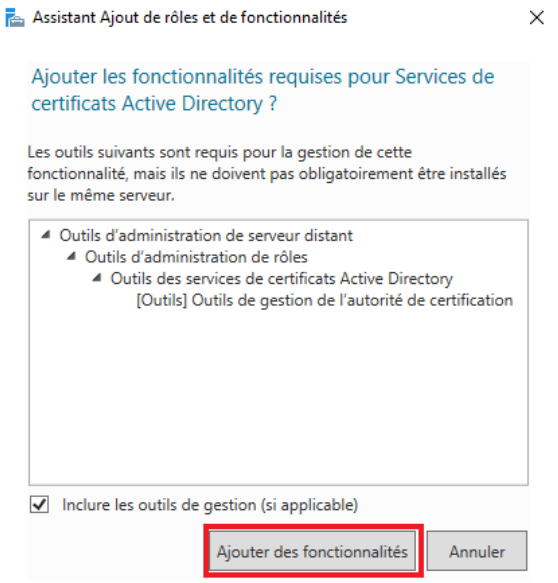
Sur le contrôleur de domaine hermes, créer les éléments suivants :

• **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



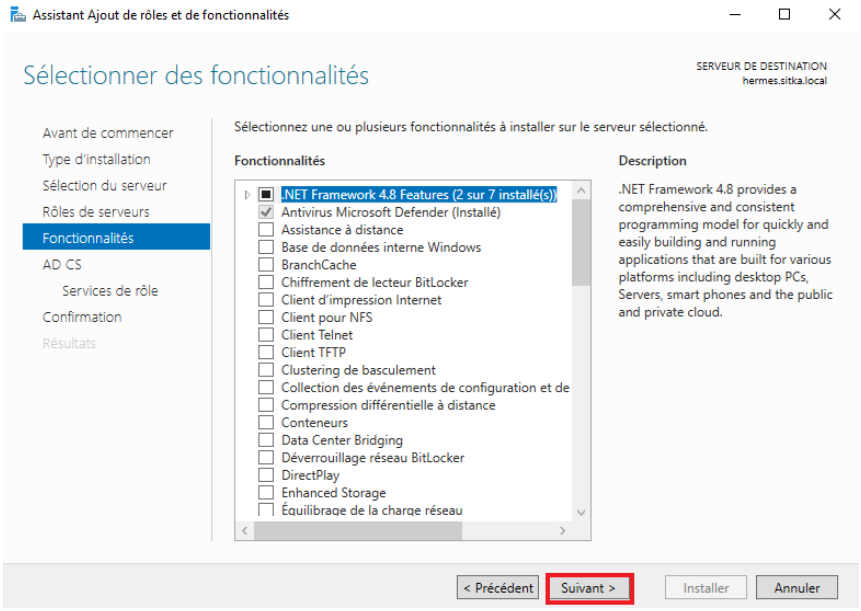
Création des utilisateurs et groupes Active Directory

16. Configuration des authentifications LDAP et LDAPS sur PfSense

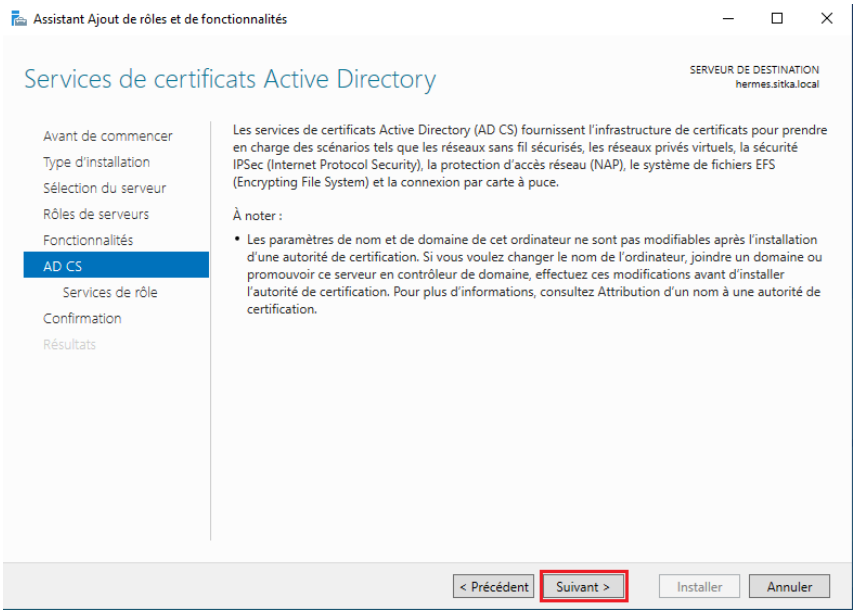
Sur PfSense, aller dans **Système** → **User Manager** → **Authentication Servers** et cliquer sur **Add** pour ajouter un serveur d'authentification.

16.1 Authentification LDAP (non chiffrée)

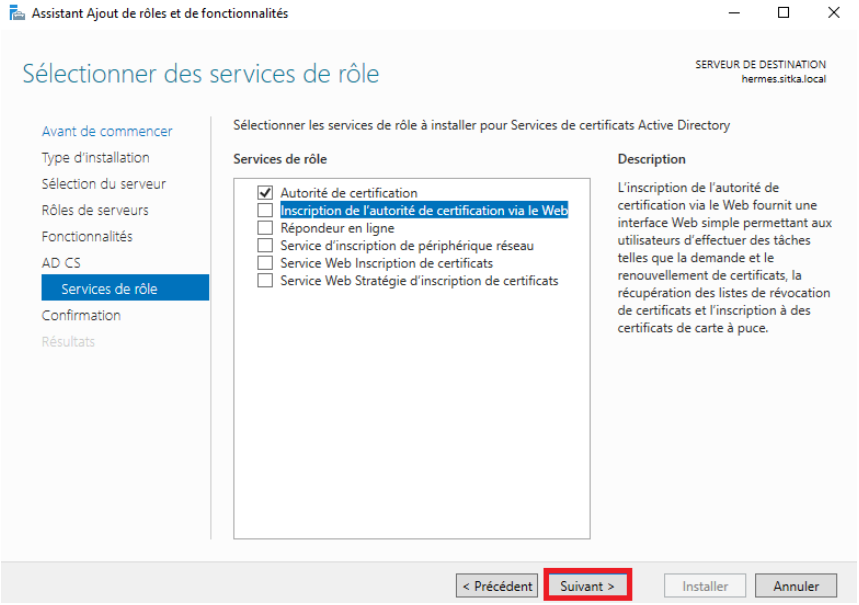
Remplir les champs en utilisant le port **389** pour LDAP standard. Dans le champ **Authentication containers**, taper **cn** puis cliquer sur **Select a container** pour sélectionner l'OU hébergeant les utilisateurs.



Configuration de l'authentification LDAP



Configuration de l'authentification LDAP

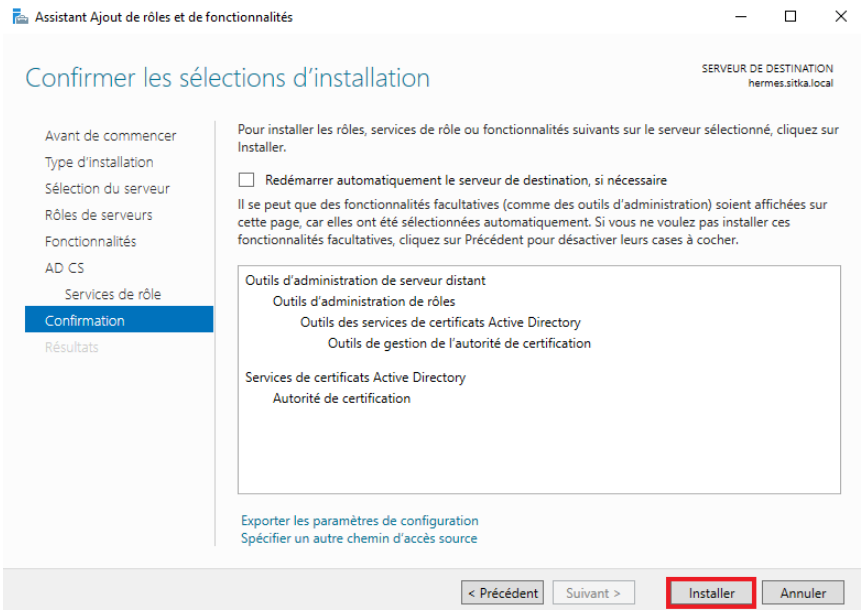


Configuration de l'authentification LDAP

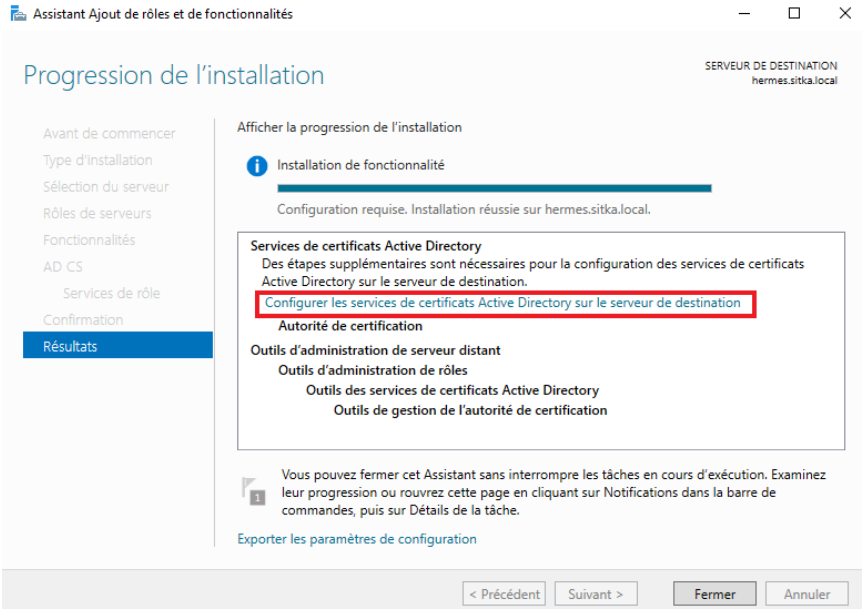
16.2 Authentification LDAPS (chiffrée SSL)

Même procédure que LDAP, mais avec les différences suivantes :

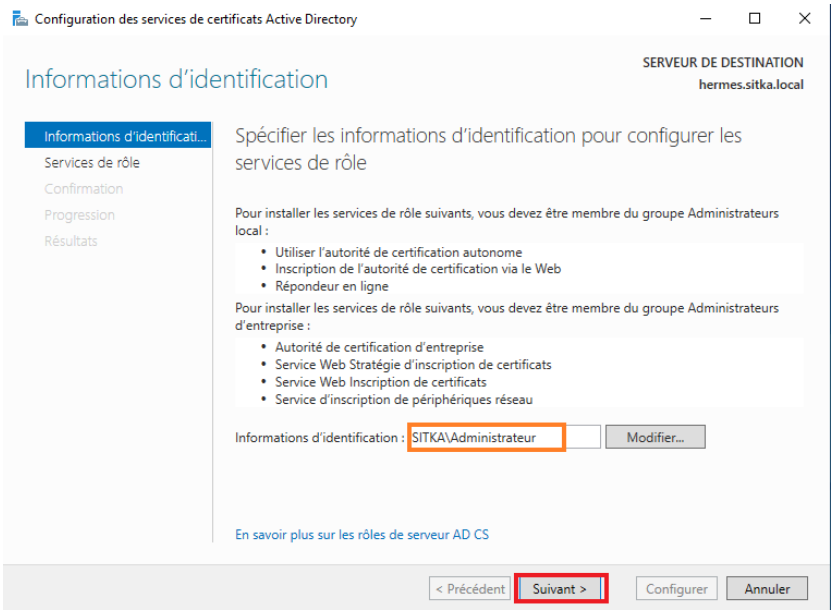
```
• Type de transport : SSL/TLS • Port : 636
```



Configuration de l'authentification LDAPS



Configuration de l'authentification LDAPS



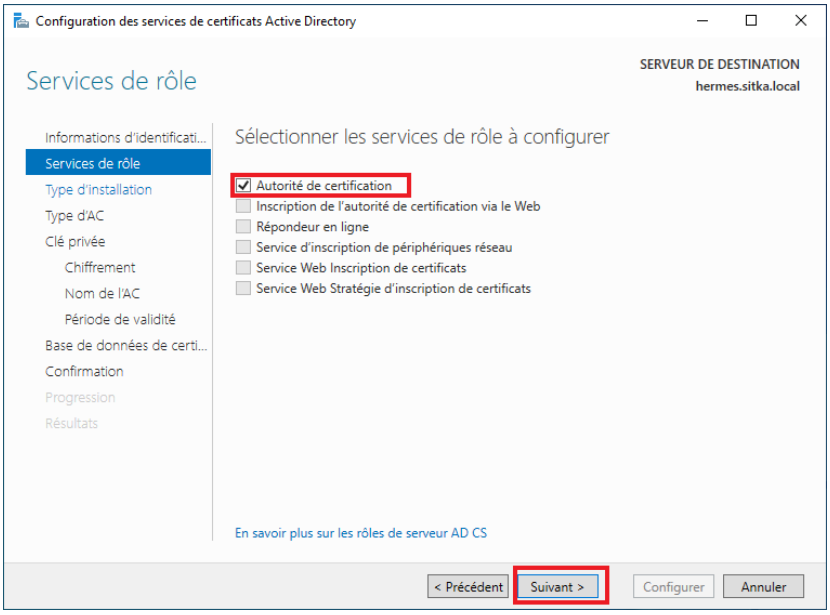
Configuration de l'authentification LDAPS

17. Diagnostic LDAPS avec Wireshark et résolution

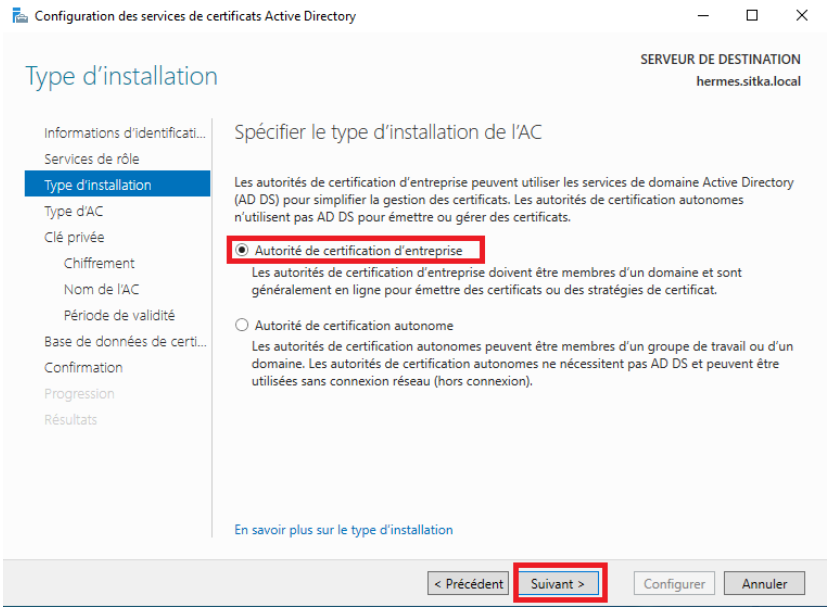
Si la boîte de dialogue de sélection de conteneur LDAPS ne s'ouvre pas, c'est que la connexion SSL échoue. On utilise Wireshark pour diagnostiquer le problème :

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

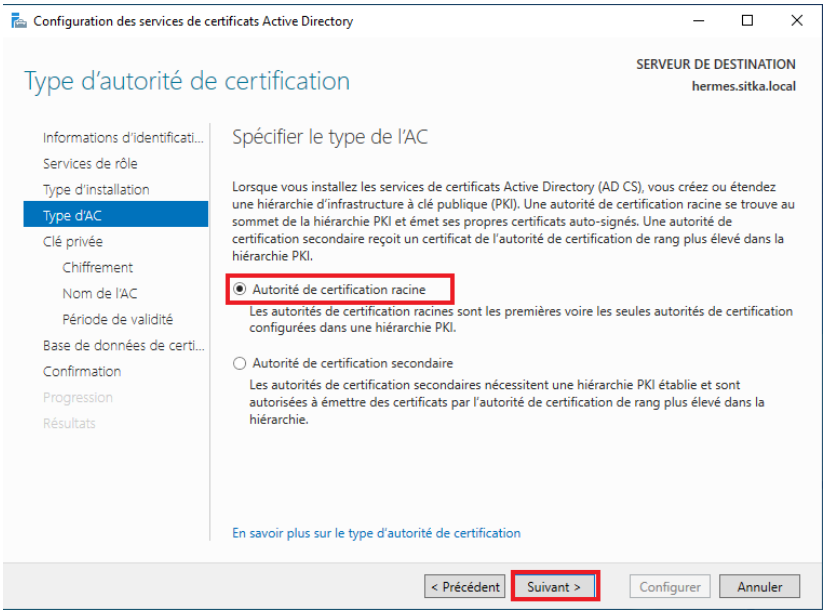
L'analyse des trames révèle que : • PfSense envoie un **Client Hello** • Hermes répond avec **Server Hello** et présente son certificat • PfSense envoie une alerte : il ne reconnaît pas le certificat



Capture Wireshark – échange LDAPS



Capture Wireshark – échange LDAPS



Capture Wireshark – échange LDAPS

Solution : Exporter et importer le certificat de l'AC

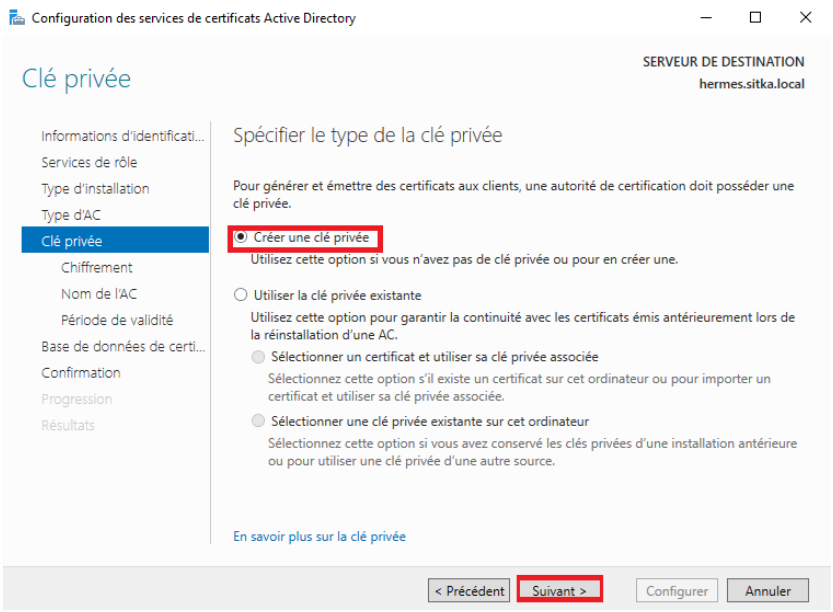
Sur hermes, ouvrir une console MMC, ajouter le composant Certificats pour ordinateur et exporter le certificat de l'autorité racine :

• Ne pas exporter la clé privée

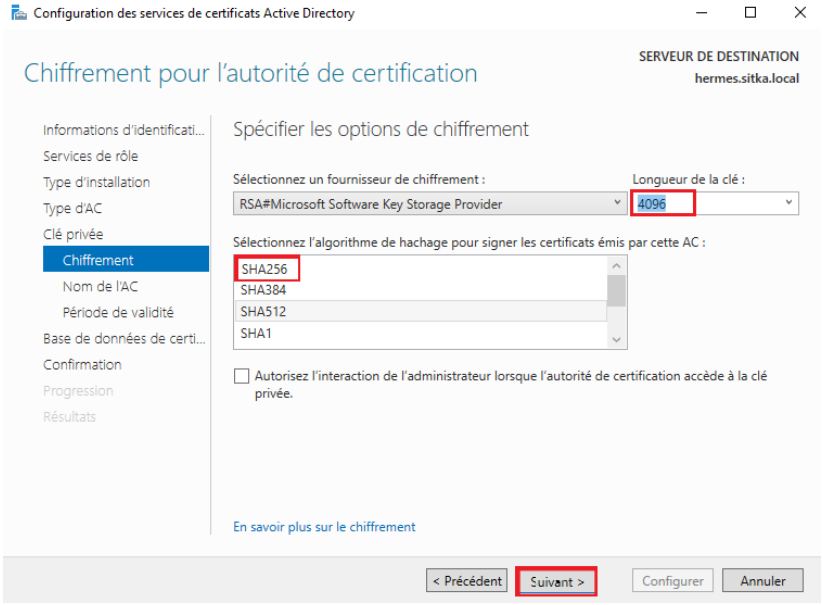
• Format : **X.509 encodé DER (*.cer)**

• Enregistrer sous le nom : **hermes-ca.cer**

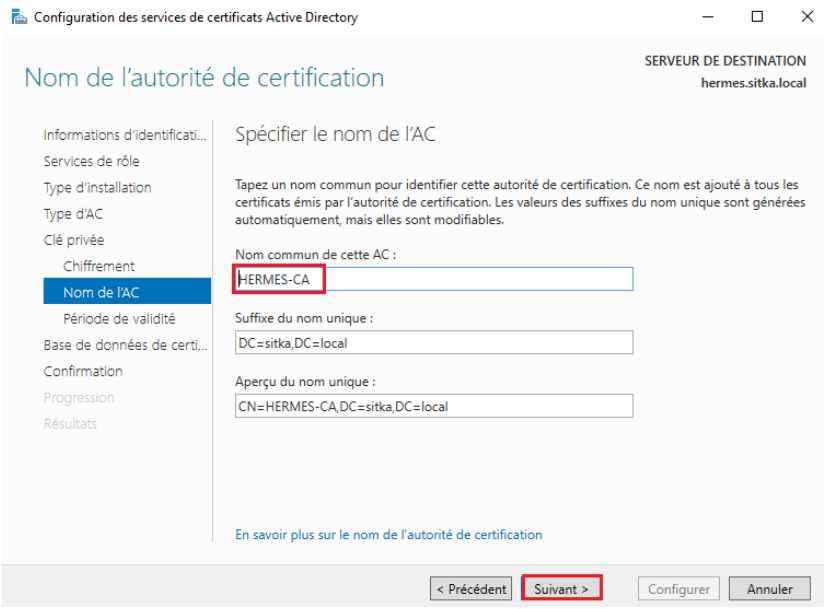
Ouvrir le fichier hermes-ca.cer avec le Bloc-notes pour afficher le certificat en base64 et le copier. Sur PfSense, aller dans **Système** → **Cert Manager** → **CAs** → **Add** et coller le certificat dans le champ prévu à cet effet.



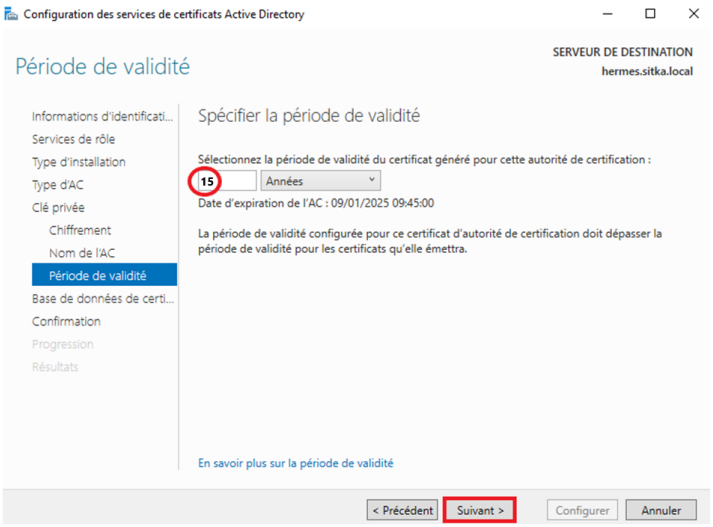
Export et import du certificat de l'AC



Export et import du certificat de l'AC



Export et import du certificat de l'AC



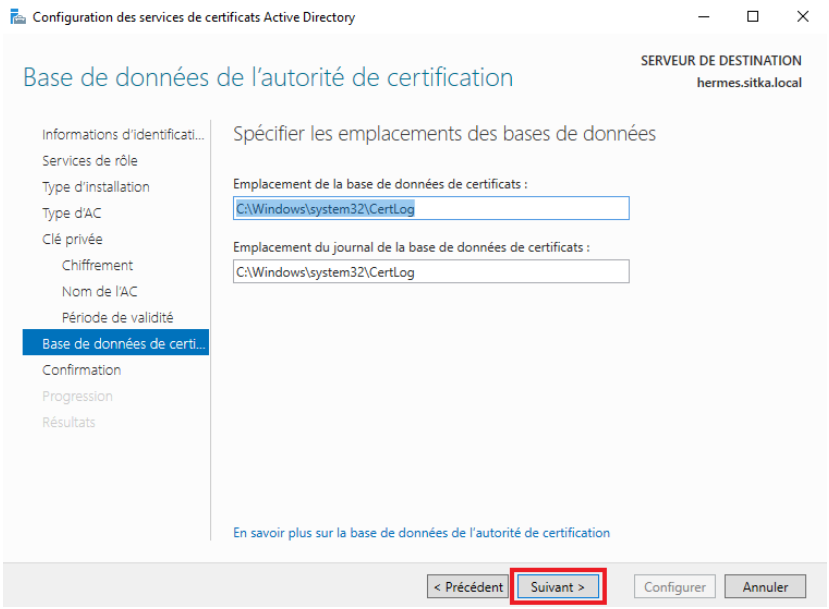
Export et import du certificat de l'AC

18. Test et utilisation des authentifications

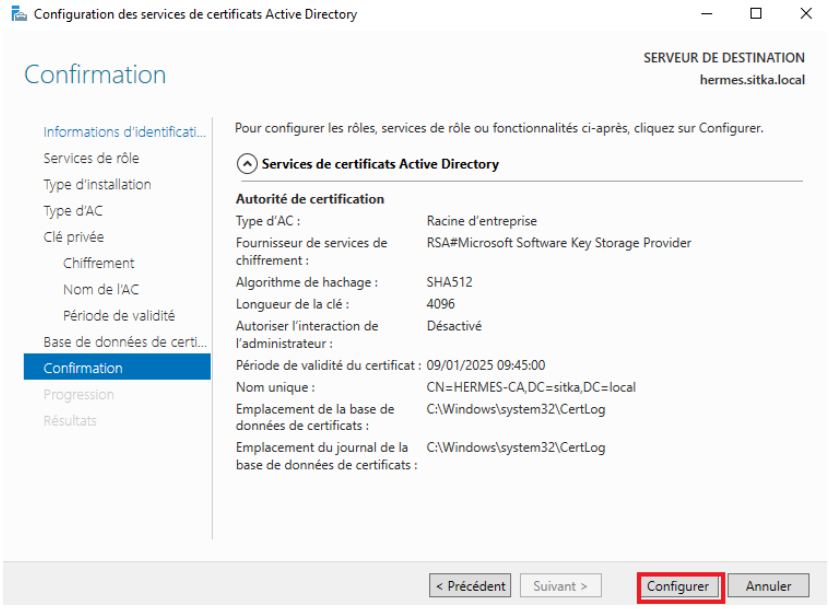
Une fois le certificat importé, tester la connexion SSL :

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

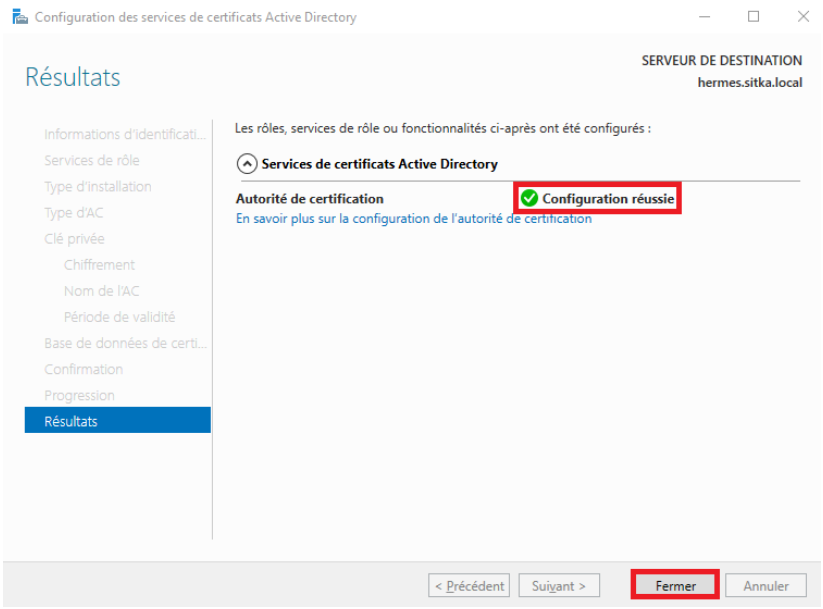
Puis tester les authentifications LDAP et LDAPS en utilisant les comptes créés (kaiser, cesar). Créer si nécessaire un groupe sur PfSense lié au groupe AD.



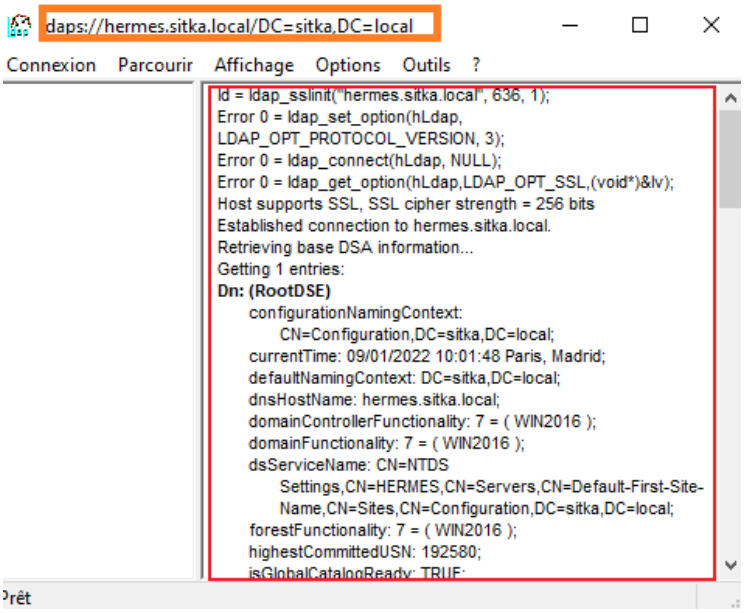
Test de connexion avec compte LDAP/LDAPS



Test de connexion avec compte LDAP/LDAPS



Test de connexion avec compte LDAP/LDAPS



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)

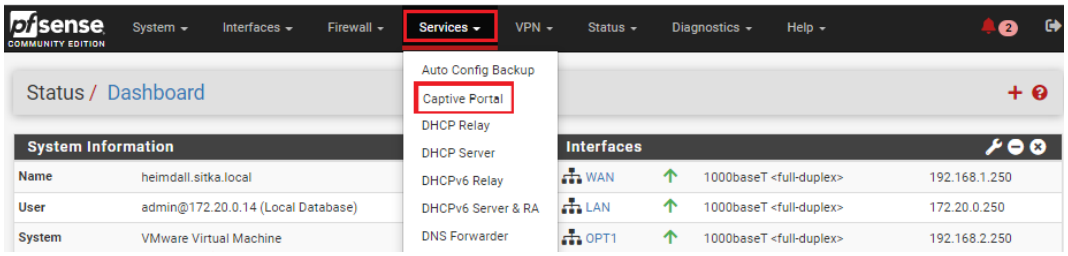
• **After authentication Redirection URL :** URL de redirection après authentification

• **Disable Concurrent user logins :** Activé (seule la connexion la plus récente est active)

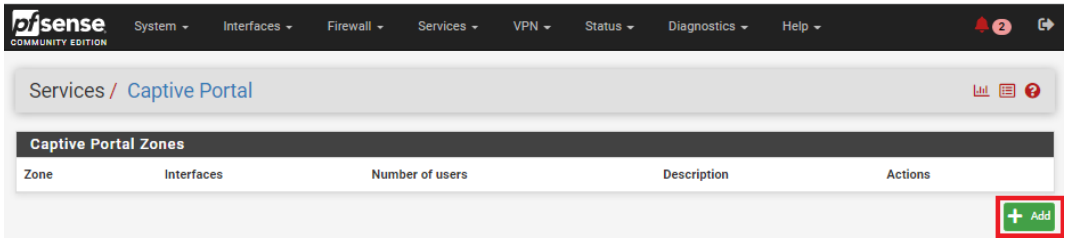
• **Disable MAC filtering :** Activé (si l'adresse MAC ne peut pas être déterminée)

• **Authentication backend :** LDAPS (méthode d'authentification)

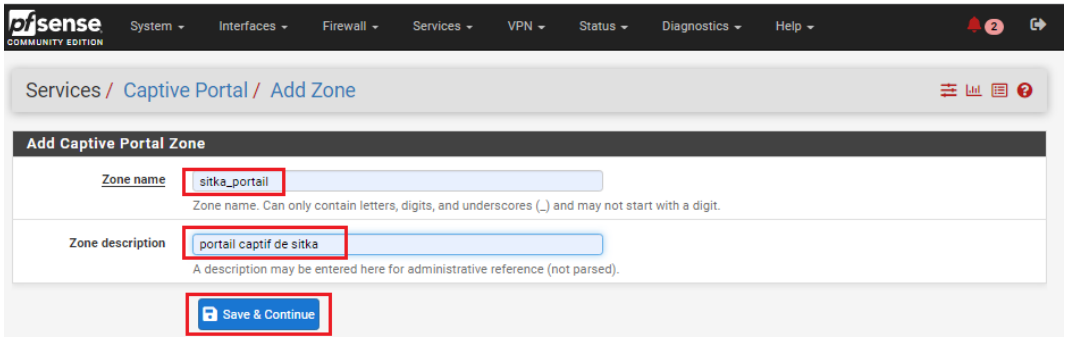
Configuration du portail captif



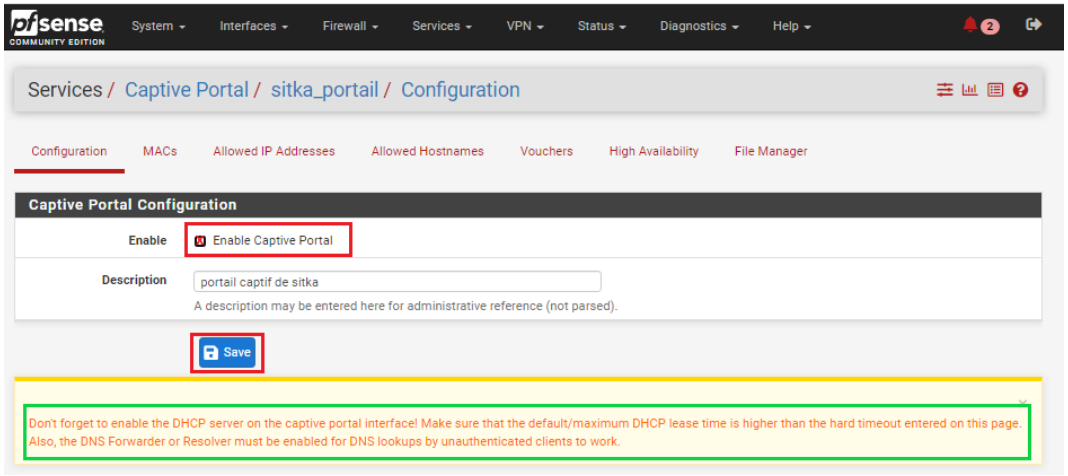
Configuration du portail captif



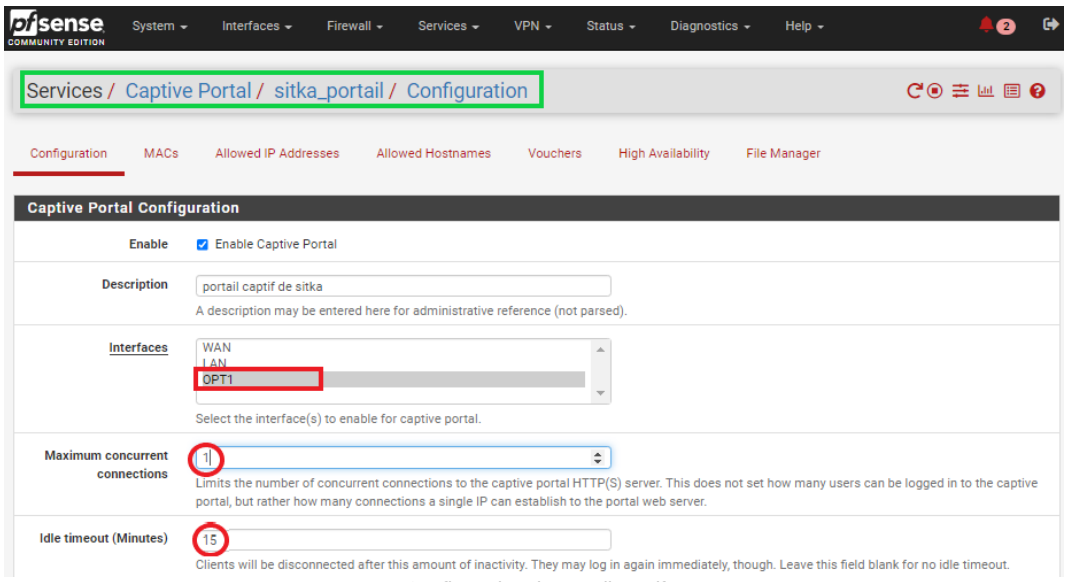
Configuration du portail captif



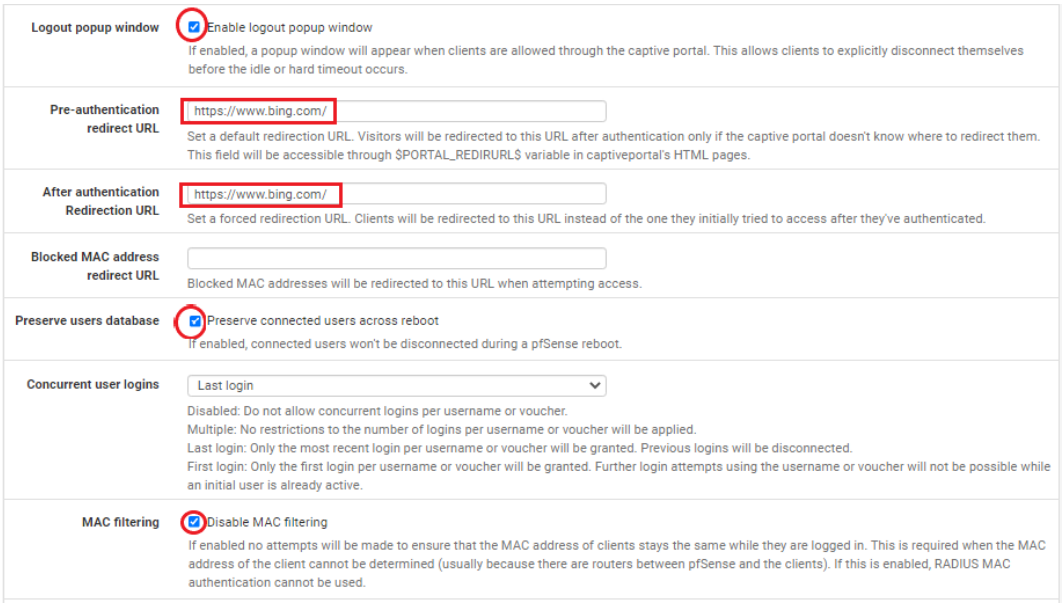
Configuration du portail captif



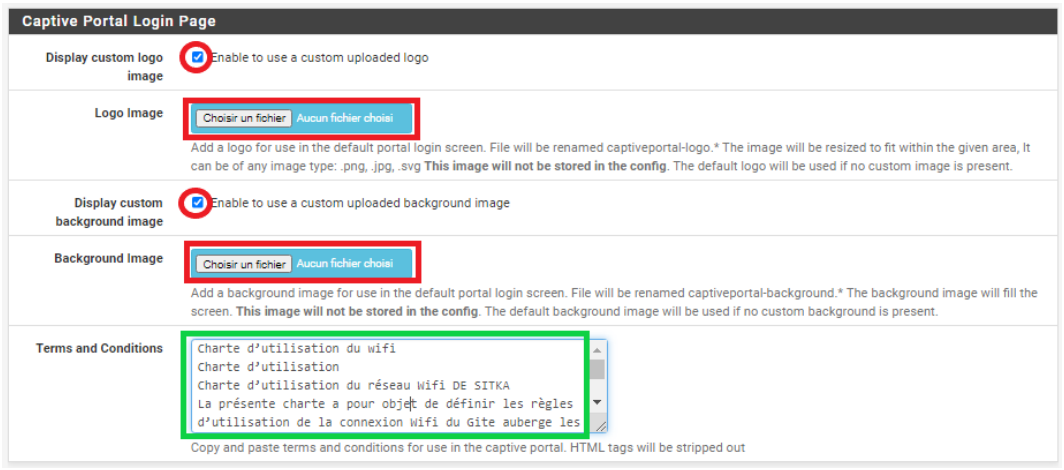
Configuration du portail captif



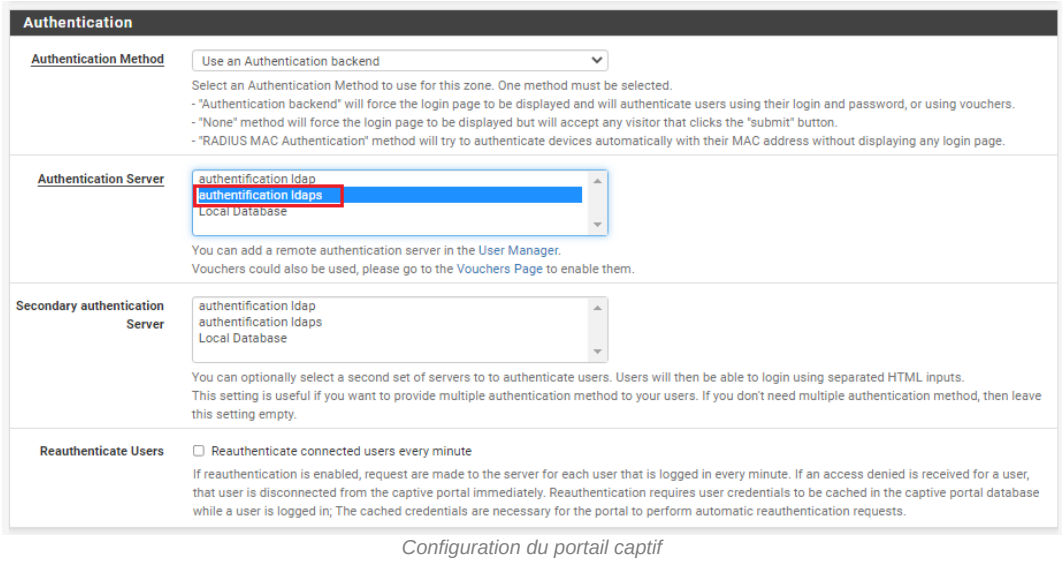
Configuration du portail captif



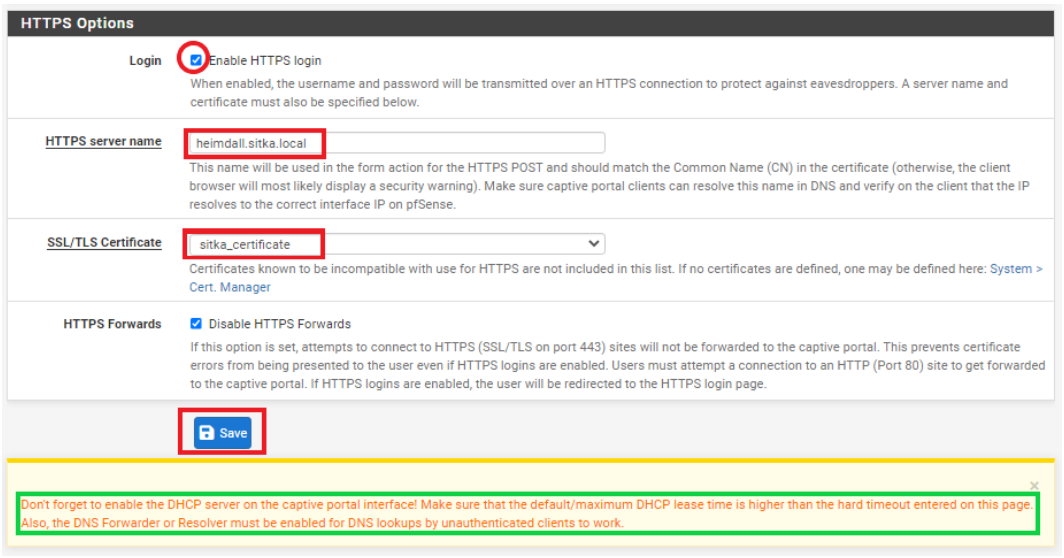
Configuration du portail captif



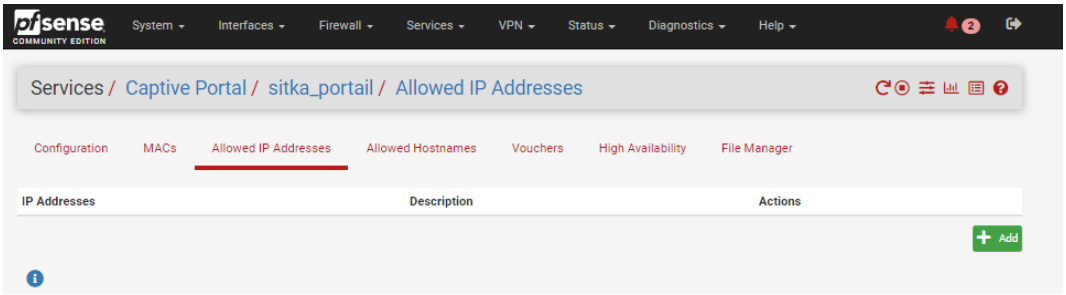
Configuration du portail captif



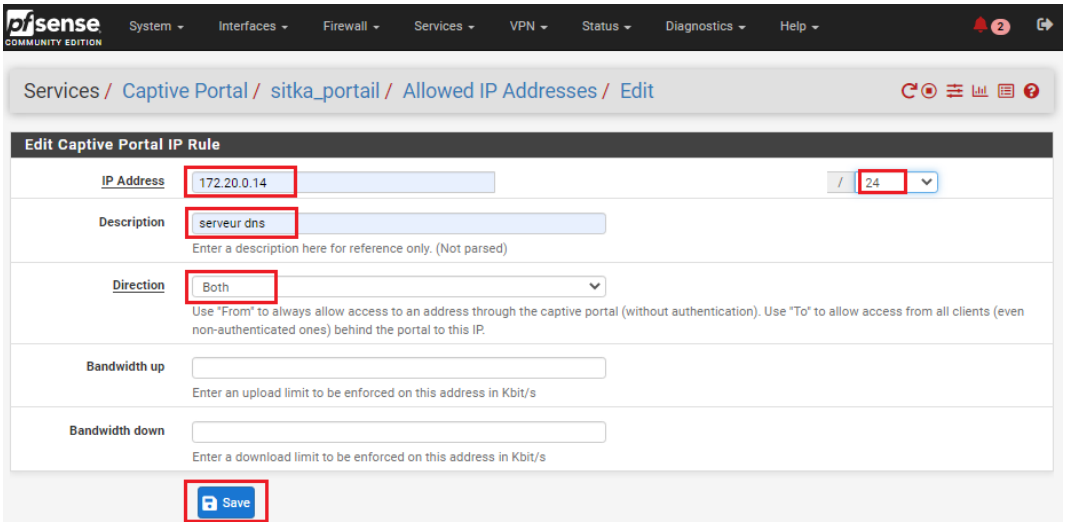
Configuration du portail captif



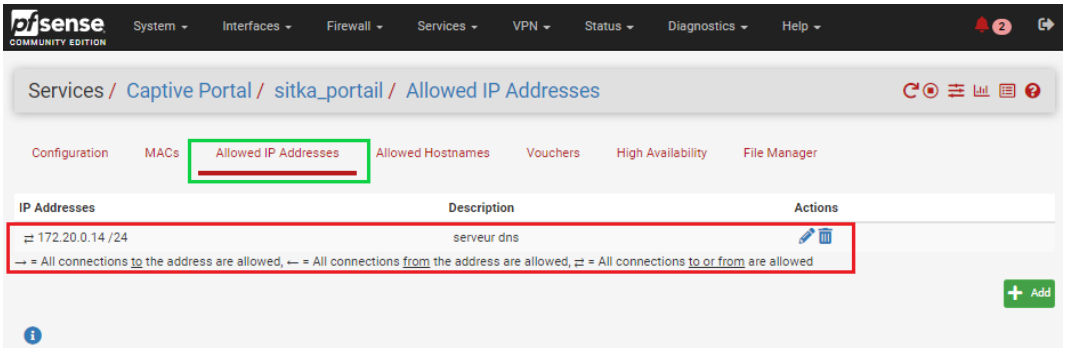
Configuration du portail captif



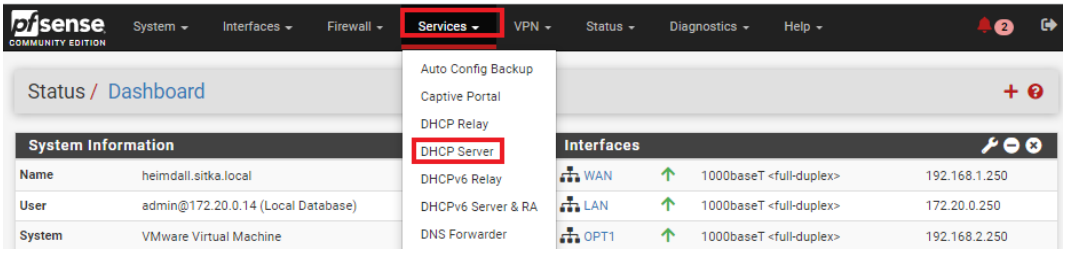
Configuration du portail captif



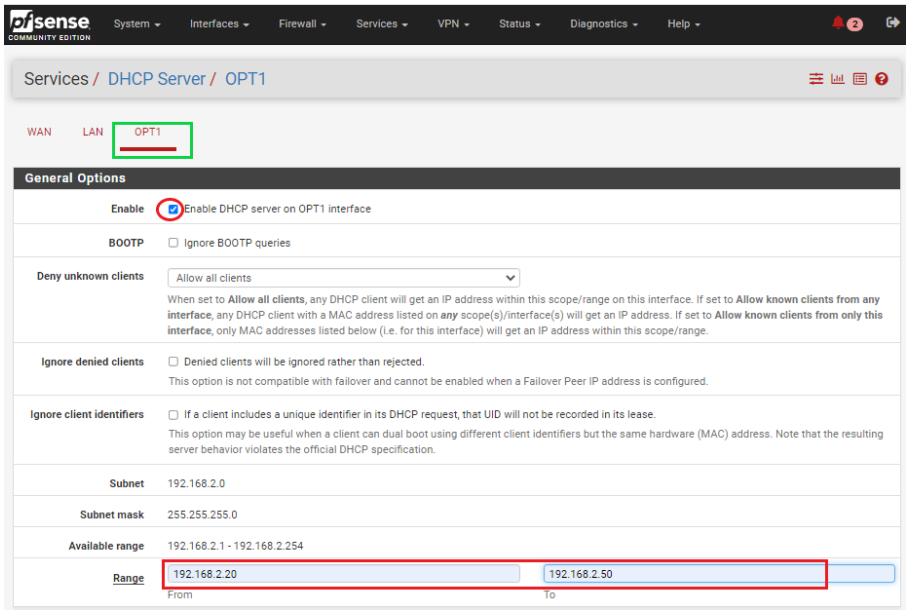
Configuration du portail captif



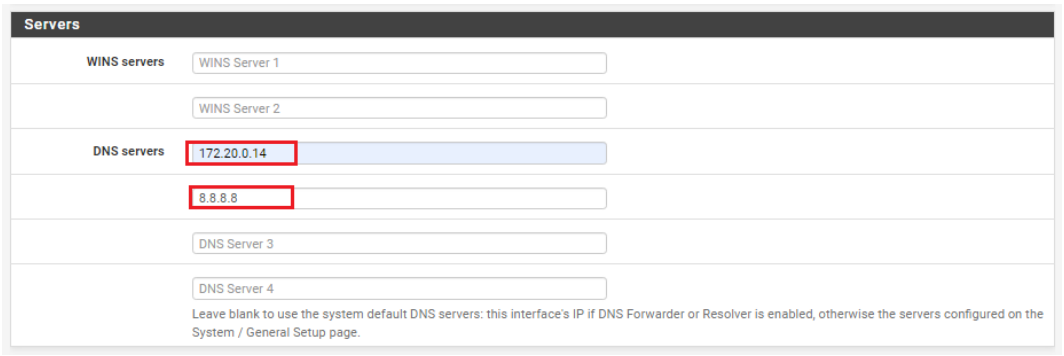
Configuration du portail captif



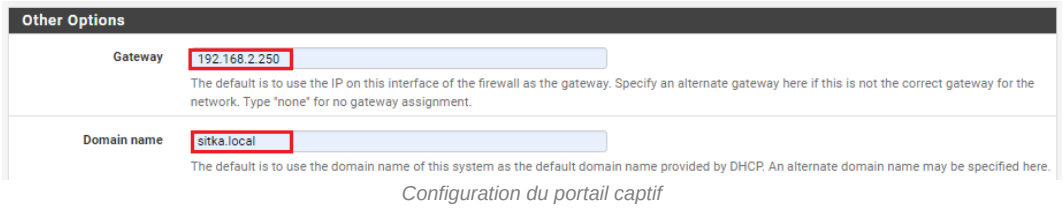
Configuration du portail captif



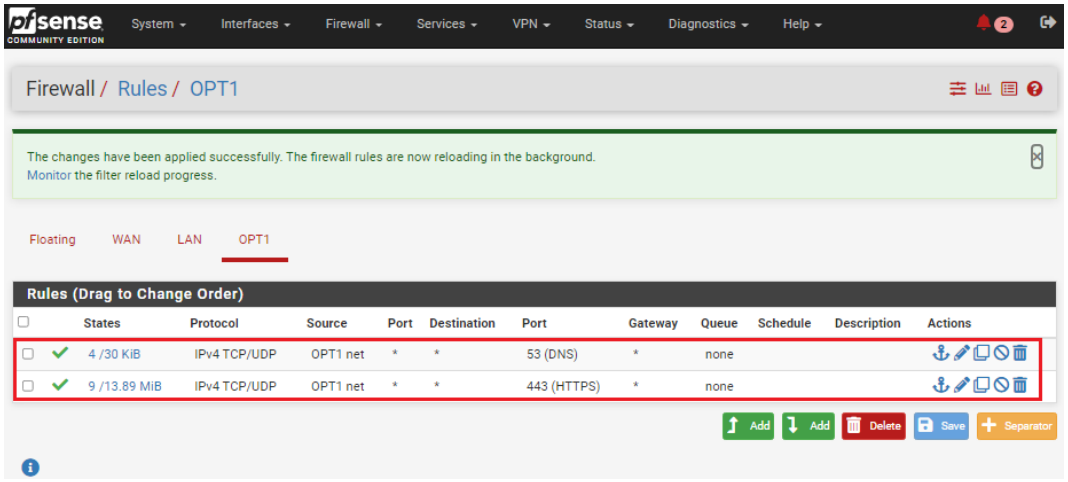
Configuration du portail captif



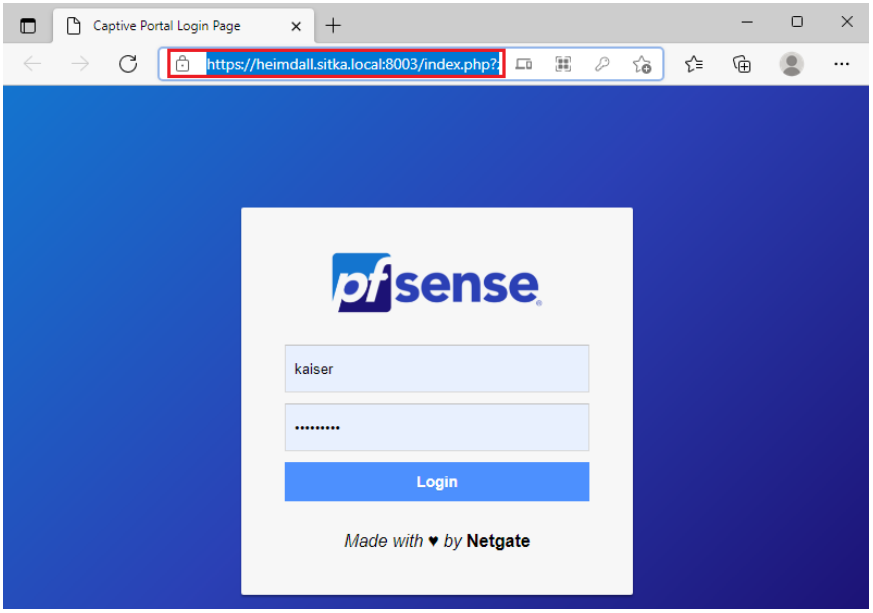
Configuration du portail captif



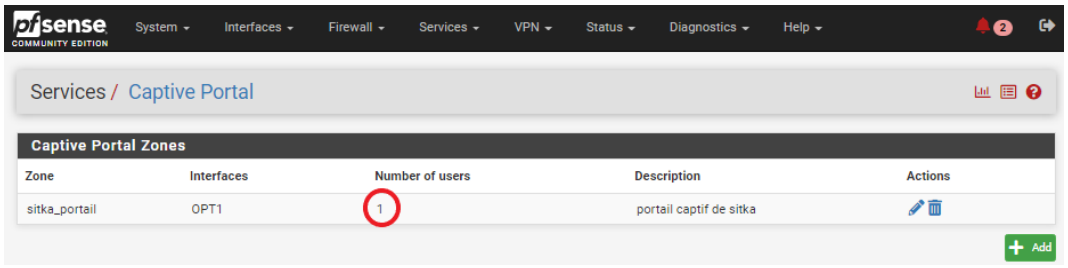
Configuration du portail captif



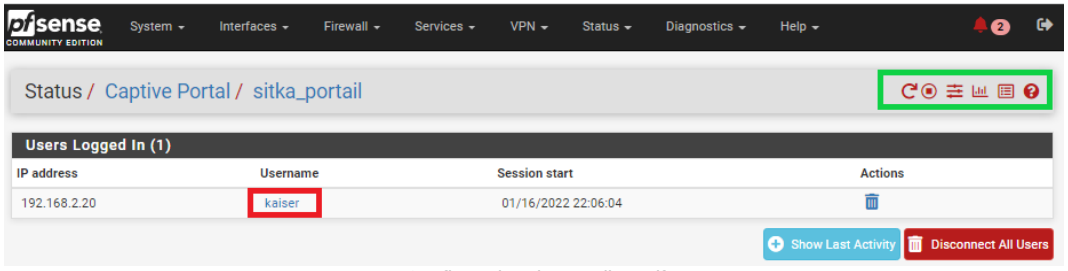
Configuration du portail captif



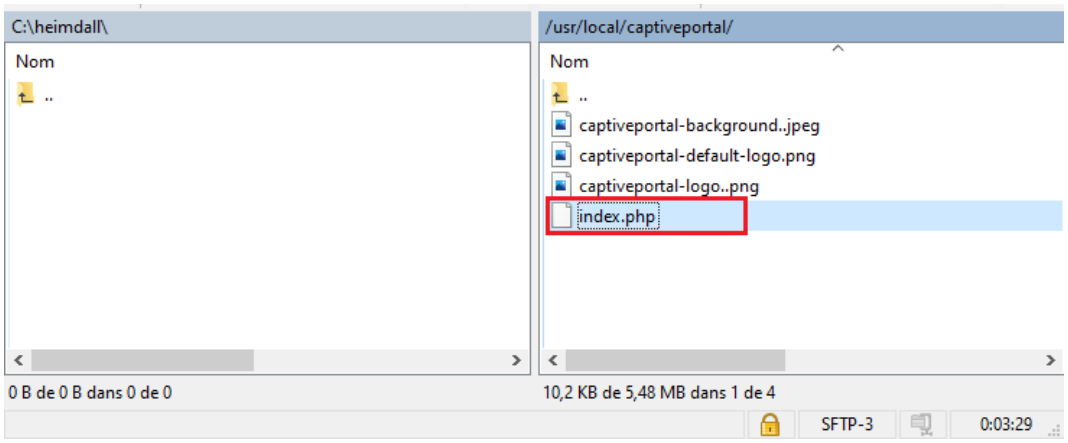
Configuration du portail captif



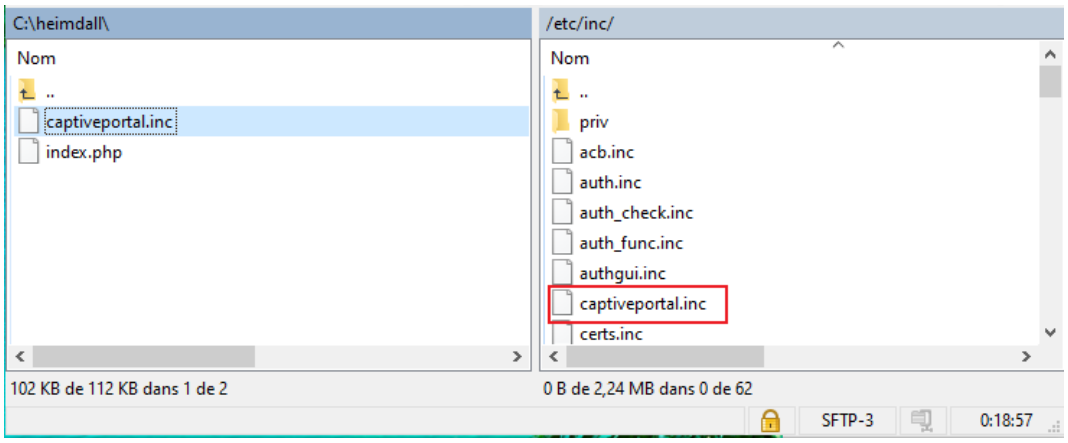
Configuration du portail captif



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
```

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)

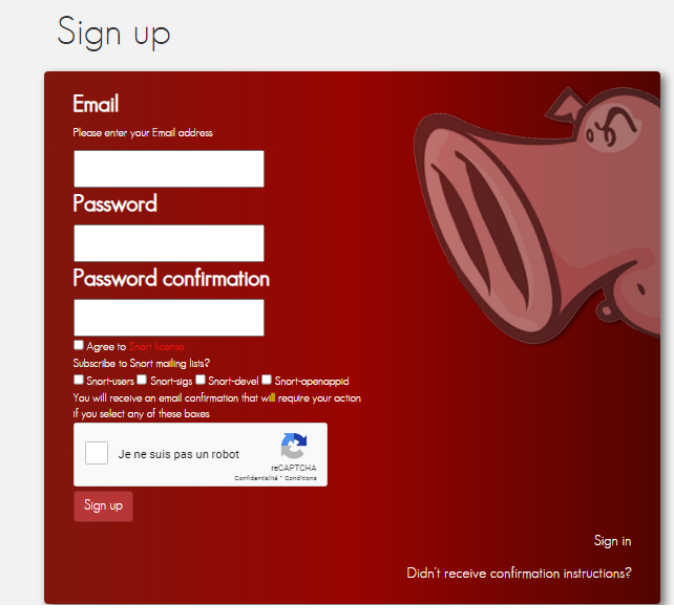
• **Update Interval** : 1 DAY

• **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 :

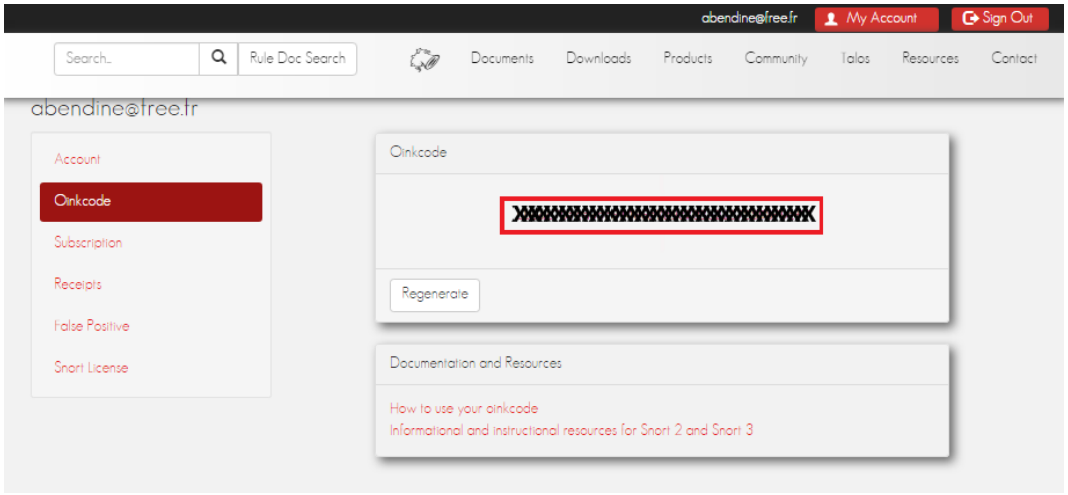
• **Connectivity :** Bloque les menaces majeures avec peu de faux positifs – idéal pour démarrer

• **Balanced :** Bon équilibre couverture/performance – recommandé pour une utilisation standard

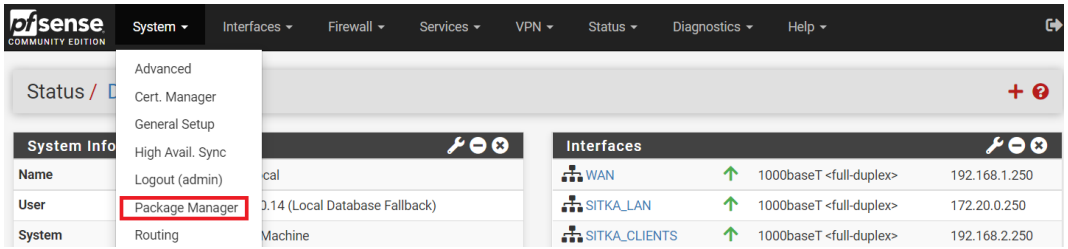
• **Security :** Politique stricte incluant des règles avancées (type Flash dans Excel)

• **Max-Detect :** Stratégie maximale pour les tests – à utiliser avec précaution en production

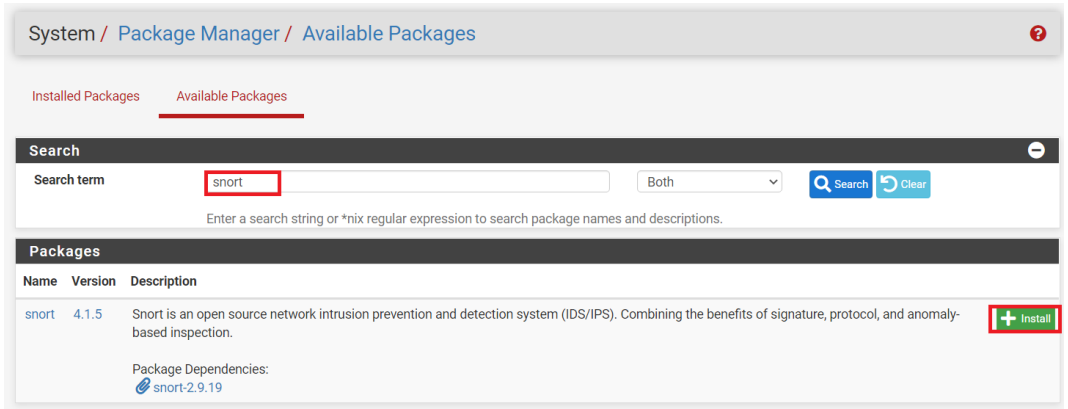
■■ L'activation de la politique IPS désactive la sélection manuelle des règles Snort Text Rules et Snort SO Rules. Les règles ET Open restent configurables manuellement.



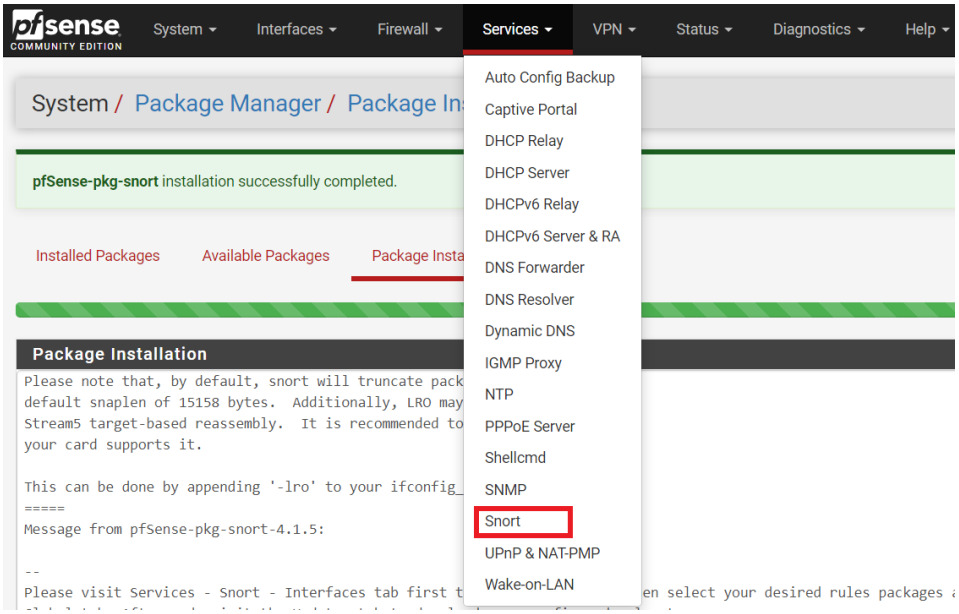
Configuration de Snort – interface et règles



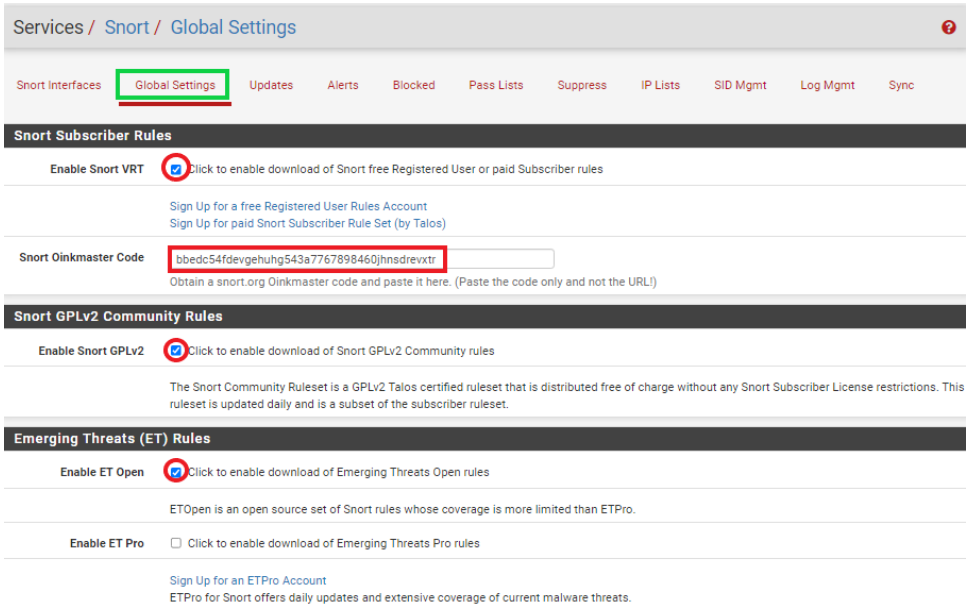
Configuration de Snort – interface et règles



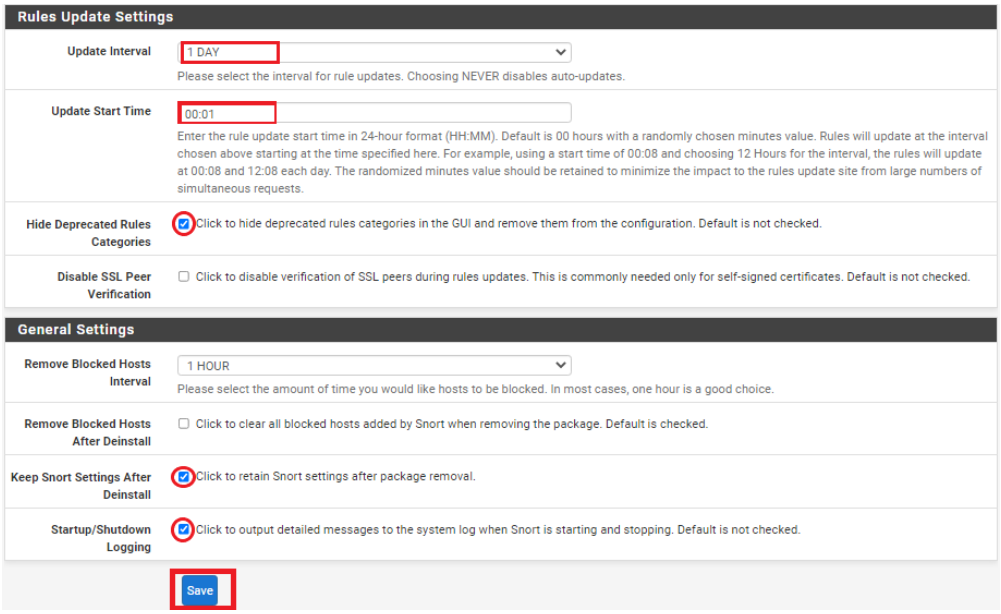
Configuration de Snort – interface et règles



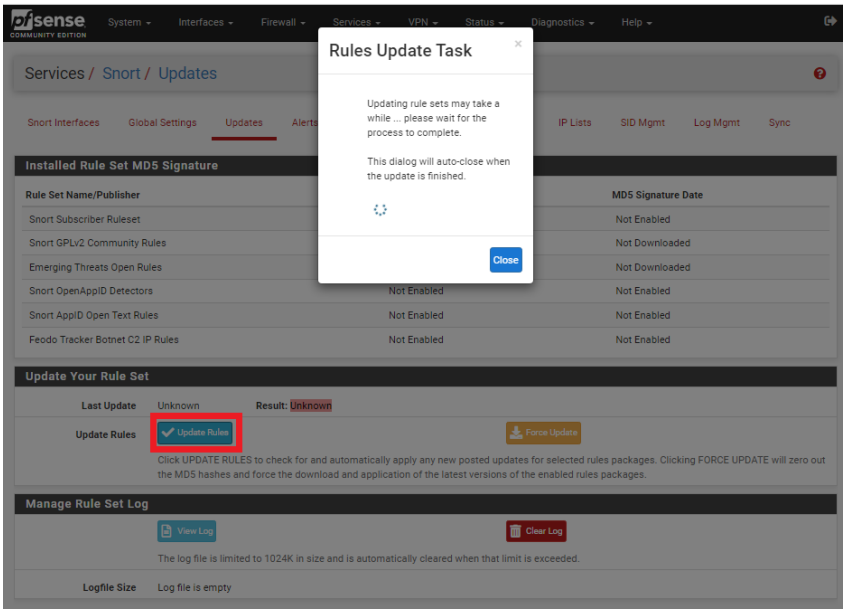
Configuration de Snort – interface et règles



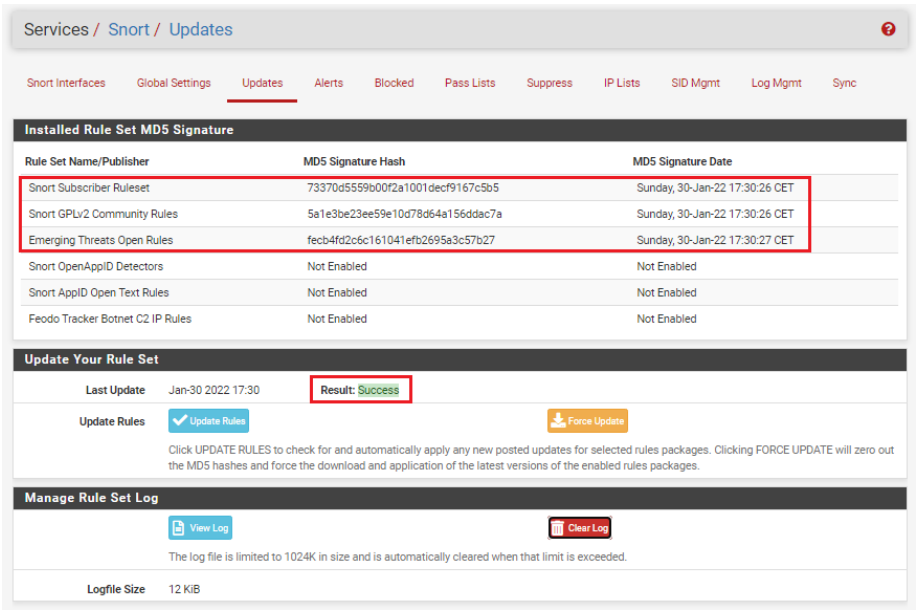
Configuration de Snort – interface et règles



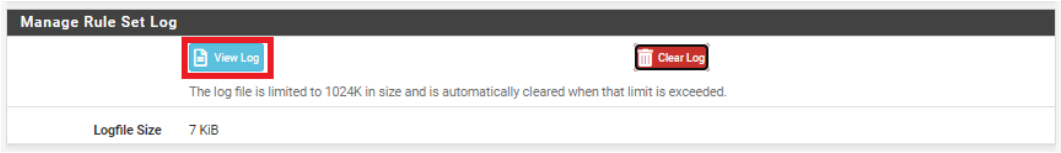
Configuration de Snort – interface et règles



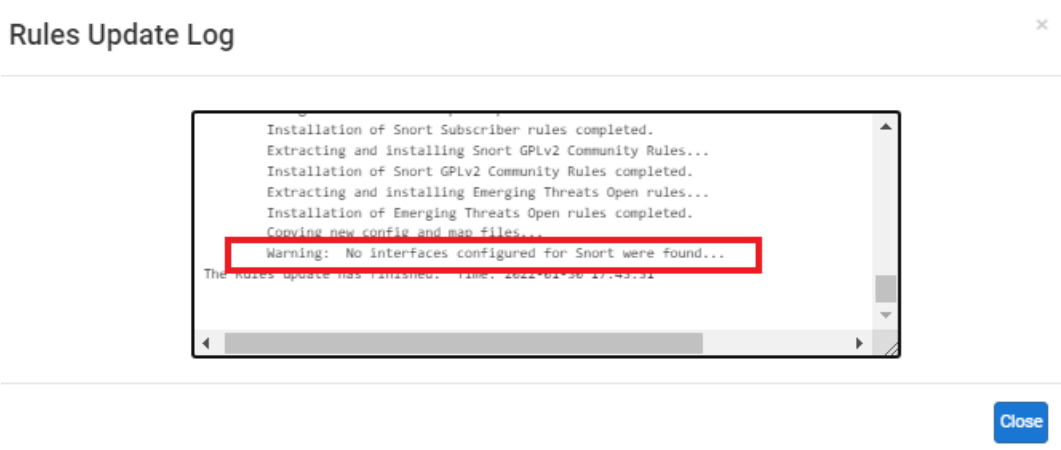
Configuration de Snort – interface et règles



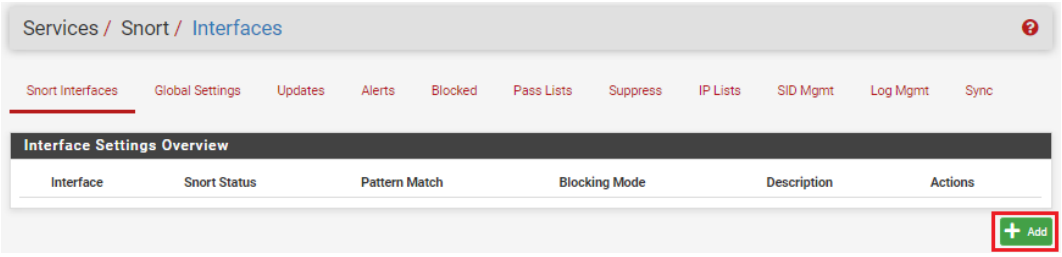
Configuration de Snort – interface et règles



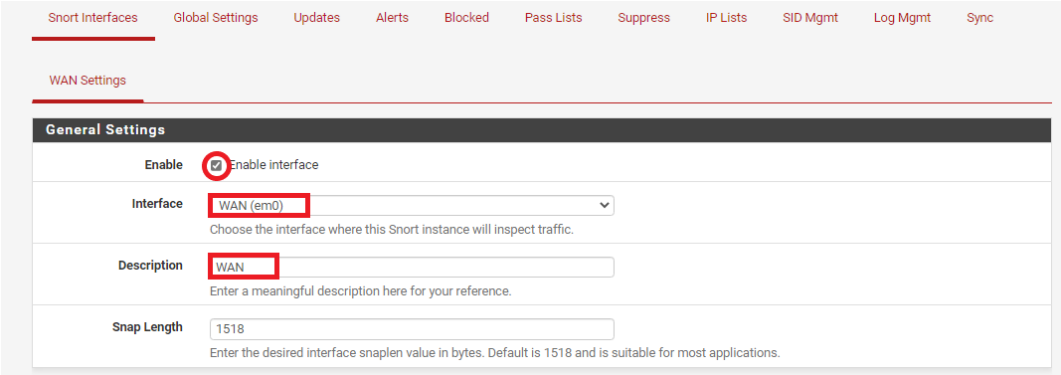
Configuration de Snort – interface et règles



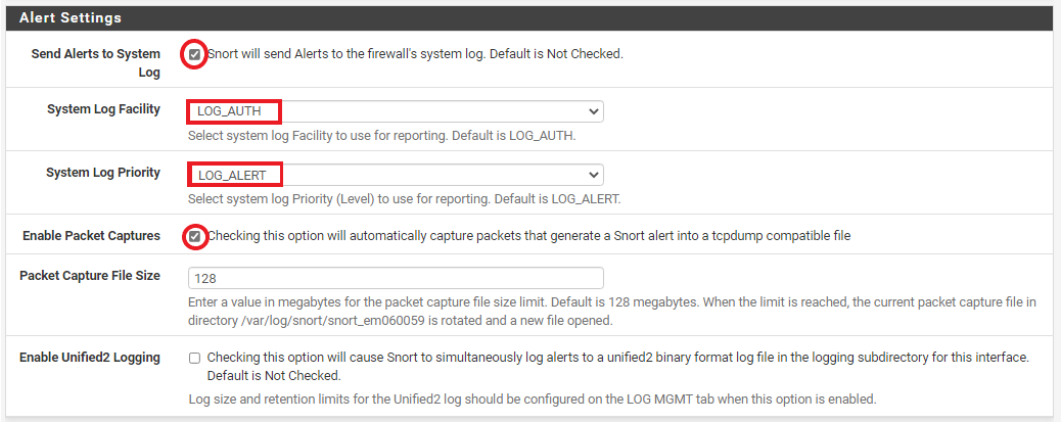
Configuration de Snort – interface et règles



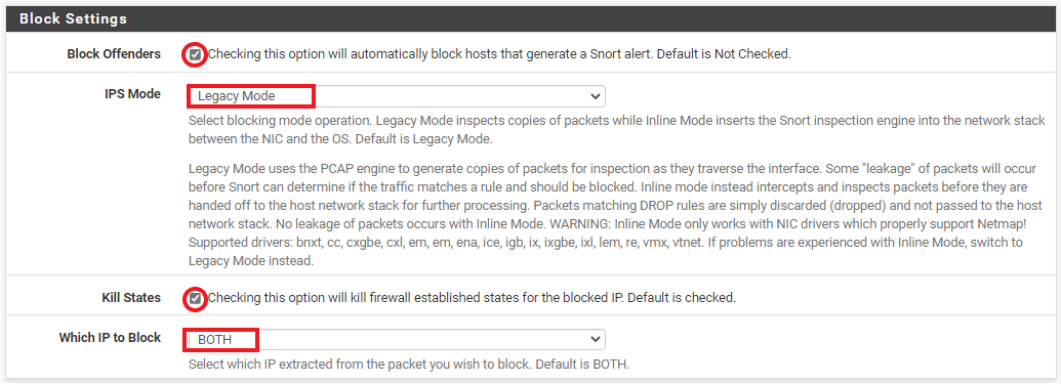
Configuration de Snort – interface et règles



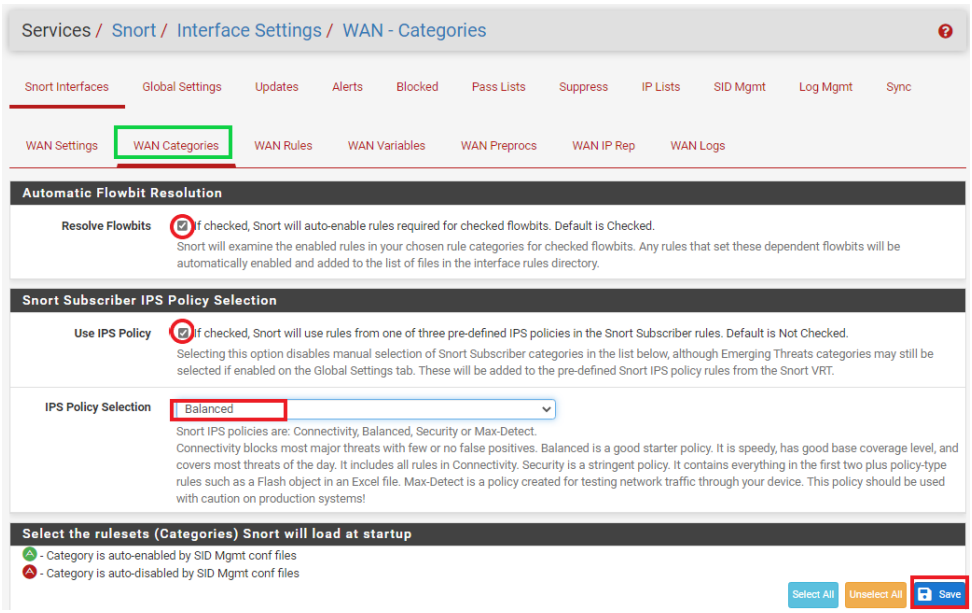
Configuration de Snort – interface et règles



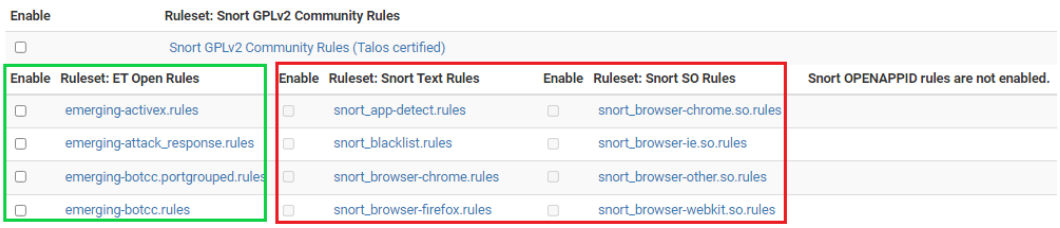
Configuration de Snort – interface et règles



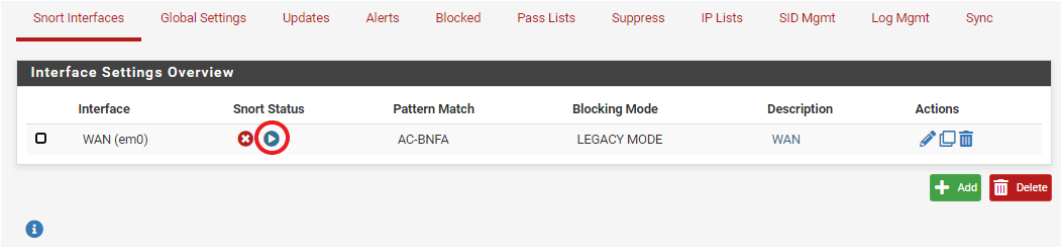
Configuration de Snort – interface et règles



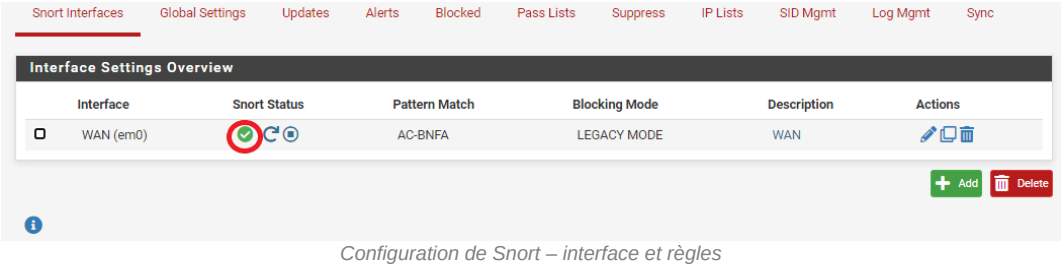
Configuration de Snort – interface et règles



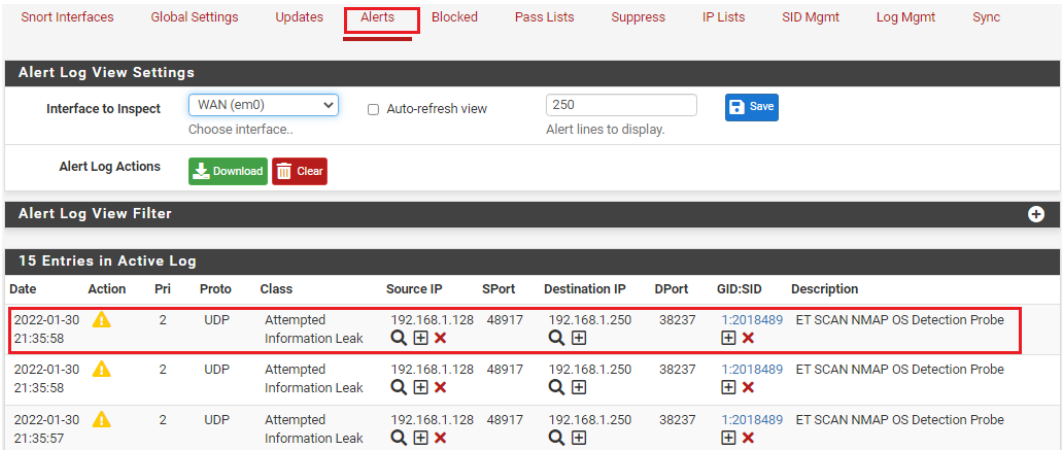
Configuration de Snort – interface et règles



Configuration de Snort – interface et règles



Configuration de Snort – interface et règles



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.