Installation

1- Introduction
2- Infrastructure
3- Installation de pfsense
   a- Téléchargement de pfsense
   b- Vérification de l'intégrité du fichier téléchargé pfsense
   c- Lancement de l'installation
4- Configuration post instalation
   a- Déclaration des interfaces
   b- Assignement des adresses aux interfaces wan, lan et opt1
      - L'interface Wan
      - L'interface lan
      - L'interface opt

1- Introduction

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 pour la sécurisation d'un réseau d'entreprise.

Prérequis pour une machine PfSense

	Configuration minimale	Configuration recommandée
Processeur	600 MHz	1 GHz
Mémoire vive	512 Mo	1 Go
Stockage	> 6 Go	

2- Infrastructure

Pour notre Labo :il faut 3 machines

-Machine Pfsense FreeBSD dans le réseau Wan

Nom du serveur : heimdall
Adresse IP : 192.168.1.250
Net masque : 255.255.255.0
Passerelle : 192 .168.1.1
DNS : adresse de votre serveur DNS

-Une machine avec active directory et DNS (nom du domaine Dns et active directory est sitka.local) dans le réseau sitka_lan

-une machine Debian dans le réseau opt_lan

-Machine AD dans le réseau sitka_lan

Nom du serveur : hermes
Adresse IP : 172.20.0.14
Net masque : 255.255.255.0
Passerelle : 172.20.0.250
DNS : adresse de votre serveur DNS

-Une machine Debian ou Ubuntu et Windows dans le réseau opt_lan

Adresse IP : DHCP

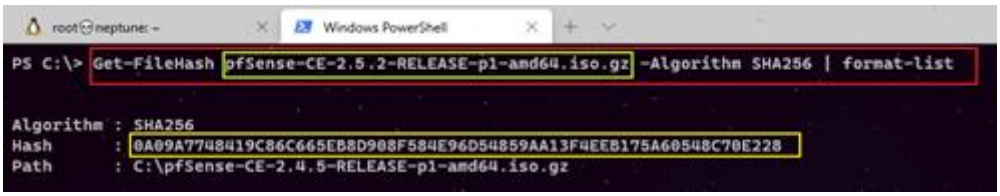
3- Installation de pfsense

a- Téléchargement de pfsense

Pour installer pfSense il faut télécharger l'iso d'installation sur le site officiel à l'adresse :
https://www.pfsense.org/download/
Le lien de téléchargements est ci-dessous
https://atxfiles.netgate.com/mirror/downloads/pfSense-CE-2.6.0-RELEASE-amd64.iso.gz

b- Vérification de l'intégrité du fichier téléchargé pfsense

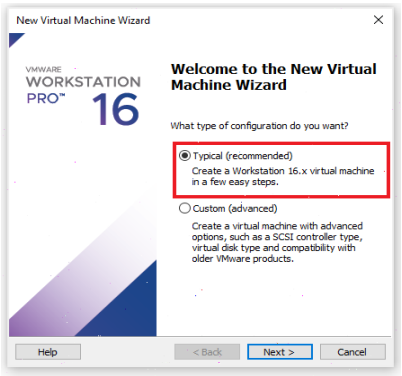
Une fois le fichier télécharger on va vérifier l'integrité du fichier telechargé avec la commande :
Get-FileHash pfSense-CE-2.6.0-RELEASE-p1-amd64.iso.gz -Algorithm SHA256 | format-list



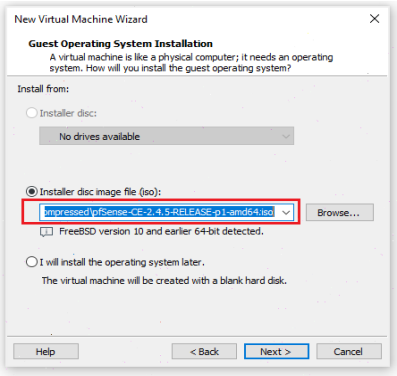
Comparer les deux empreintes **1** et **2** si les deux empreinte sont identique ceci implique que le fichier telechargé et intègre

c- Lancement de l'installation

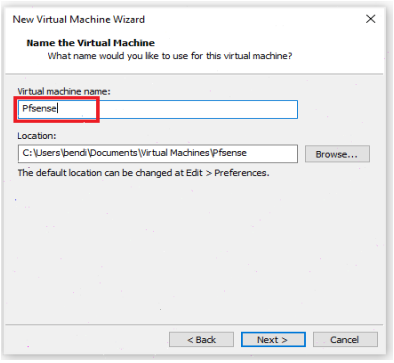
il faut maintenant dézziper notre fichier pour avoir l'iso et lancer l'installation sur vmware



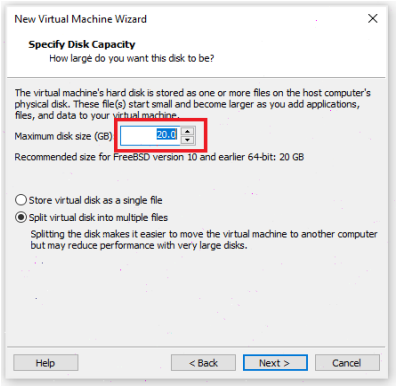
On pointe vers le fichier iso de pfsense



On choisit pfsense comme nom



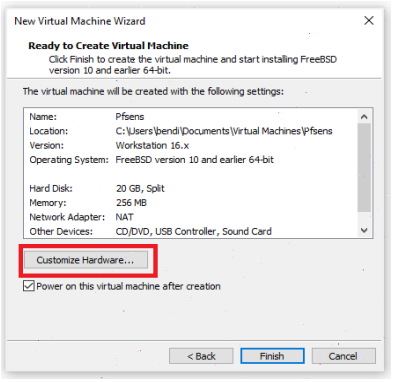
On laisse 20 gb par défaut

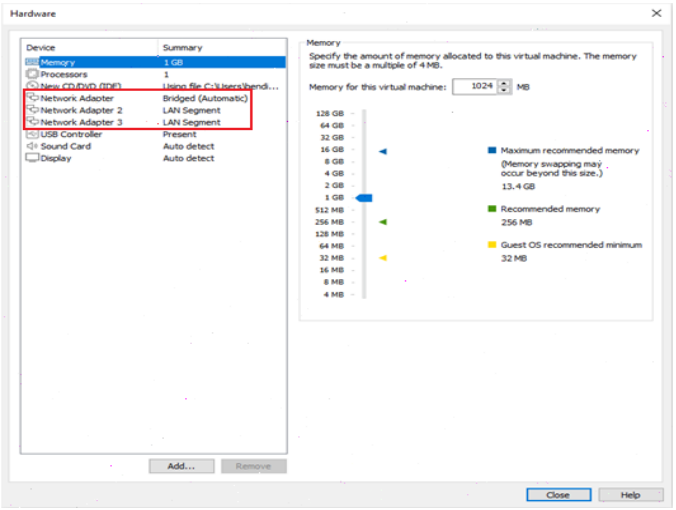


Pour cette étape On mettra en place 3 cartes

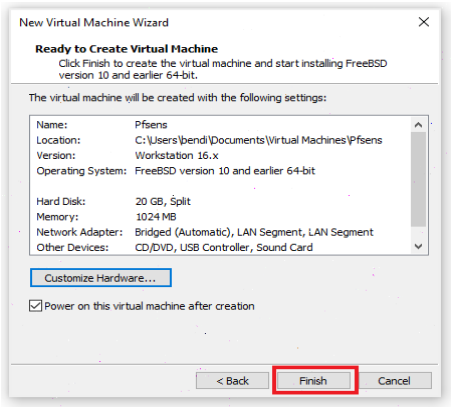
Network Adapter en bridge----------→192.168.1.0/24
Network Adapter2 en Lan_1----------→172.20.0.0/24
Network Adapter3 en Lan_2----------→192.168.2.0/24
On mettra 1GB de mémoire

```
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
```

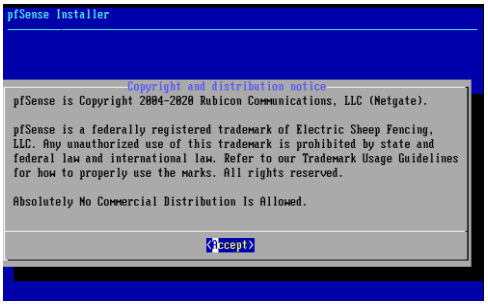




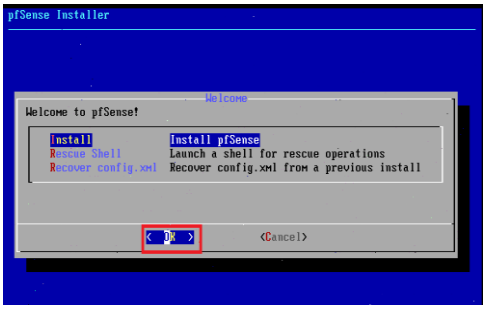
On clique sur finish et on commence l'installation



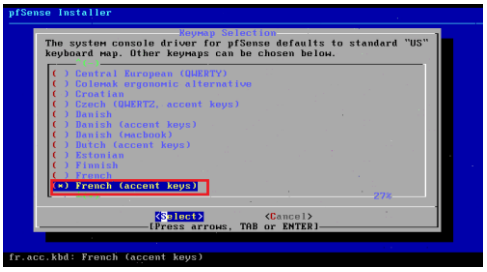
On accepte le contrat



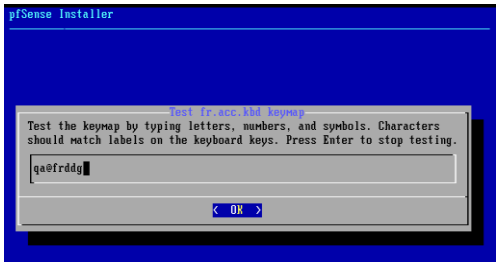
On sélectionne Install puis ok



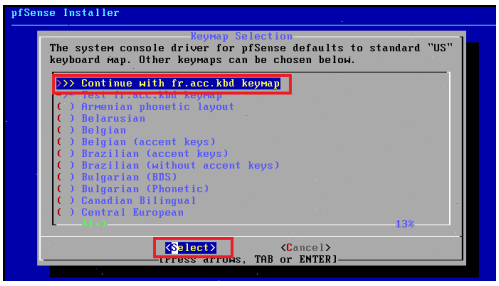
On choisit le clavier français



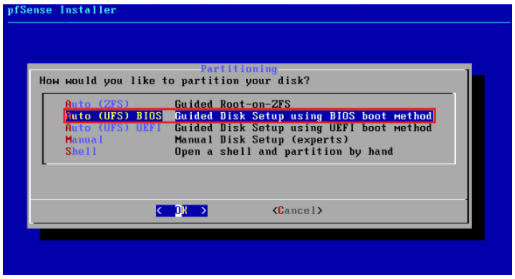
On test le clavier



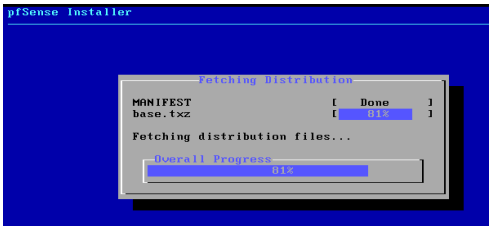
Puis on continue l'installation

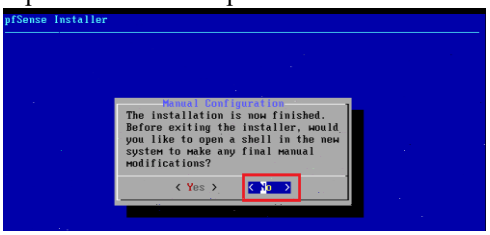


On choisit le système UFS pour créer nos partitions



On nous demande si on veut aller sur le Shell pour d'autres manipulations on dit non

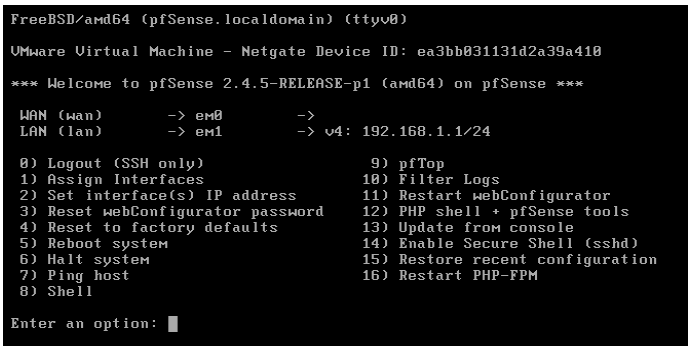




Puis on redémarre la machine

Une fois la machine a redemarrer on tombe sur l'interface menu

On remarque qu'il ya que deux interfaces qui sont reconnue **em0** et **em1** et que le clavier est en qwerty malgré notre choix pendant l'installation d'un clavier français

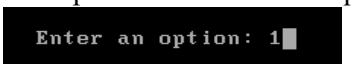


4- Configuration post instalation

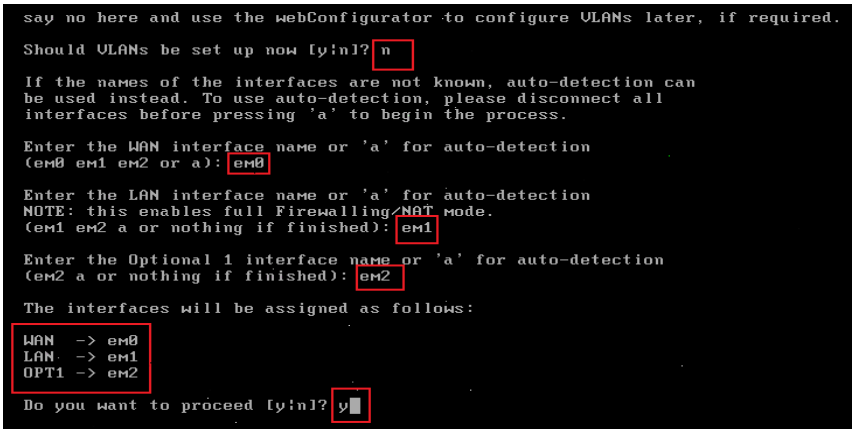
Mannuellement on va mettre notre clavier en français mais temporairement car en redemarrant notre serveur le clavier redevient en qwerty ; on le configurera d'une façon permanente avec l'interface web:
On choisit **l'option 8** pour demarrer le shell puis on tape la commande suivante
#kbdcontrol -l fr ou #kbdcontrol -l /usr/share/syscons/keymaps/fr.iso.kbd

a- Déclaration des interfaces

Maintenant on va déclarer nos trois interfaces : Wan, lan et opt1 :
C'est pour cela on choisit l'option 1



Après il faut prendre les choix encadrés en rouge



A la fin on doit avoir le résultat suivant

Maintenant on va affecter les adresses IP à nos trois interfaces,

b- Assignement des adresses aux interfaces wan, lan et opt1

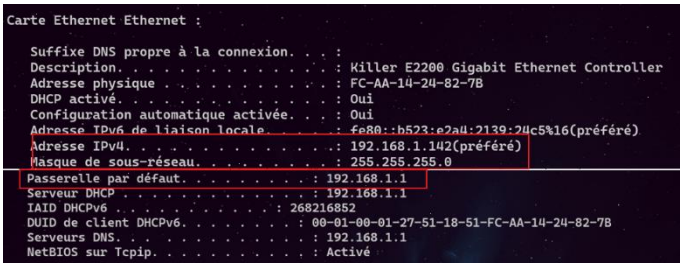
- L'interface Wan.

Le choix de des adresses qu'on va affecter à cette interface dépend de la configuration de notre box internet c'est pour cela il faut faire une **ipconfig /all** sur la machine physique pour déterminer la passerelle et l'ID réseau utilisé

Donc notre réseau est

Id réseau **192.168.1.0/24**

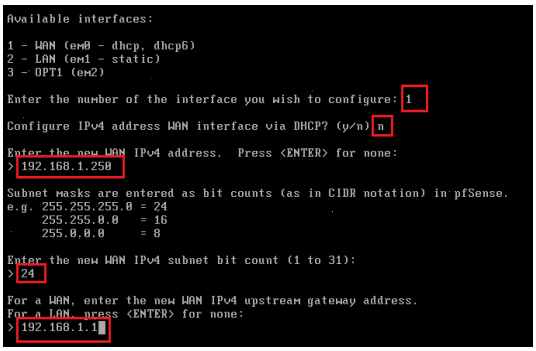
DNS/Passerelle **192.168.1.1**

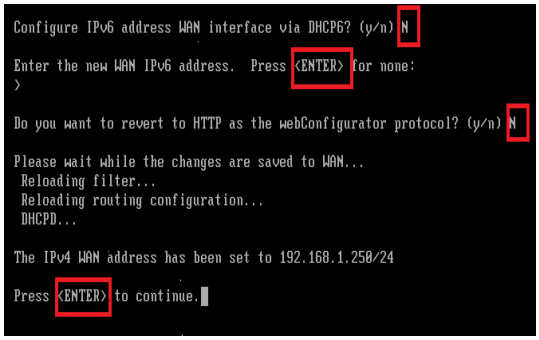


On choisit l'option 2

Et on fait les choix suivants

@ip :192.168.1.250
Masque de sous réseau 255.255.255.0
Passerelle 192.168.1.1
Pas de DHCP IPv5
Pas de IPv6
Pas de DHCP6
Le webconfigurateur pour des raisons de sécurité il est préférable de ne pas le mettre sur l'interface Wan

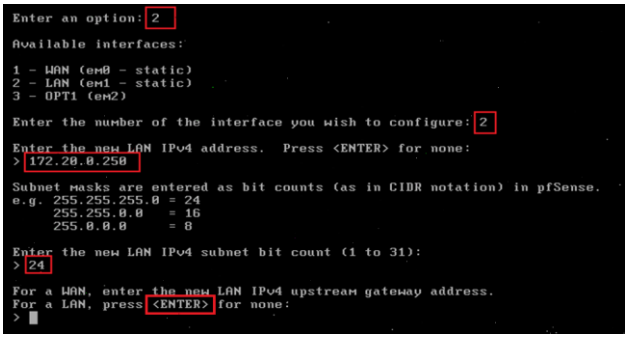


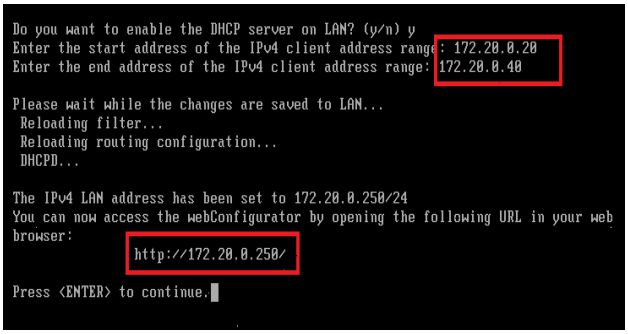


- L'interface lan

Et on fait les choix suivants

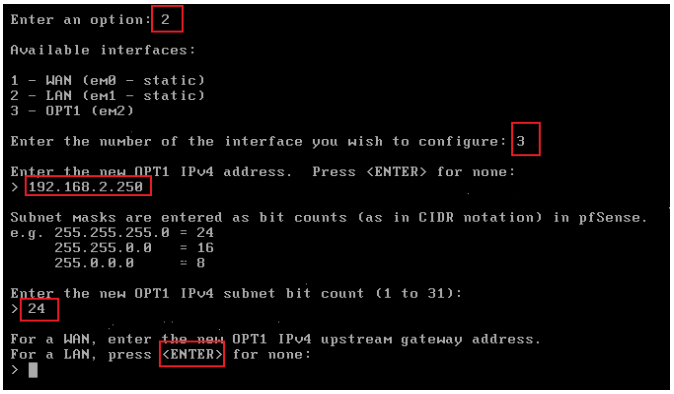
@ip :172.20.0.250
Masque de sous réseau 255.255.255.0
Passerelle : non
DHCP IPv5 oui on crée un étendu de : 172.20.0.20--→172.20.0.30
Pas de IPv6
Pas de DHCP IPV6
Le web configurateur **oui** on le met sur l'interface Lan

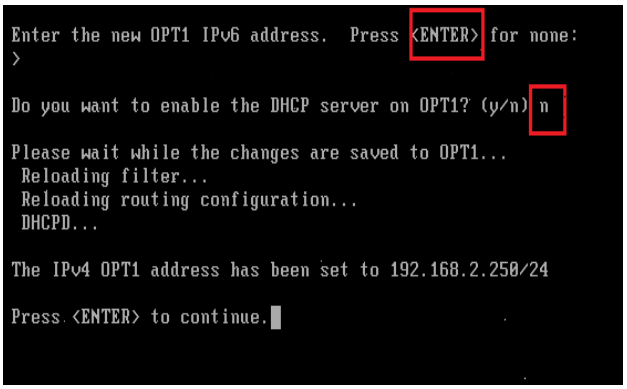




- L’interface opt

@ip :192.168.2.250
Masque de sous réseau 255.255.255.0
Passerelle : non
Pas de DHCP IPv5
Pas de IPv6
Pas de DHCP6





1- Teste de la connectivité
2- Exécution du Wizard de la configuration de base
3- La mise en place de la configuration du clavier en fr de façon permanente

1- Teste de la connectivité

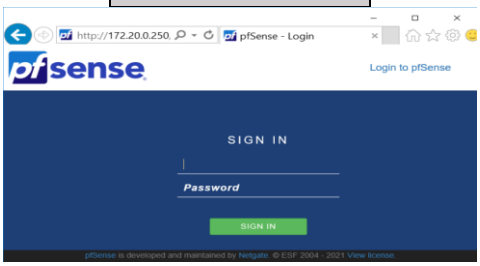
Sur la machine active directory on va tester la liaison avec pfsense et tester la table de routage en allant sur internet

```
PS C:\>ping 192.168.1.250
PS C:\>ping 172.20.0.250
PS C:\>ping 192.168.2.250
PS C:\>ping 192.168.1.1          (la passerelle de votre box)
PS C:\>ping 8.8.4.4              (teste de la connexion vers Inetrnet)
PS C:\>ping www.google.fr         (pour tester la résolution Dns)
```

Maintenant on va accéder à l'interface web de PfSense en tapant l'adresse :

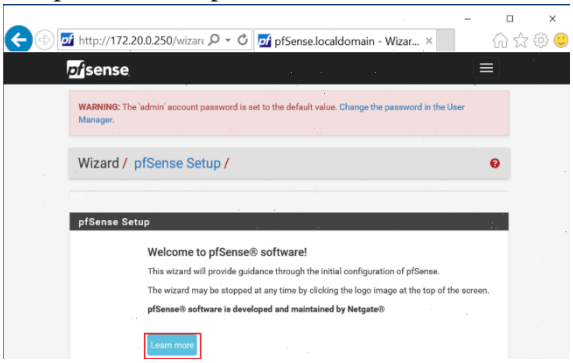
http://172.20.0.250

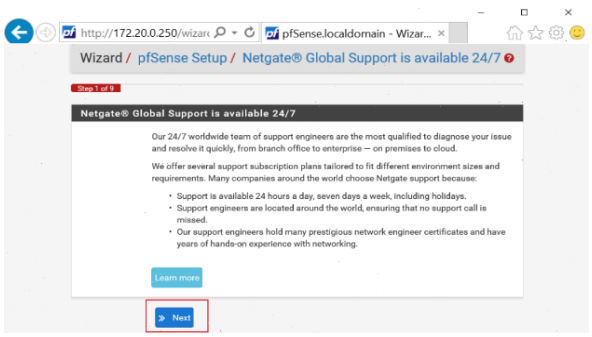
Login : **admin**
Password : **pfsense**



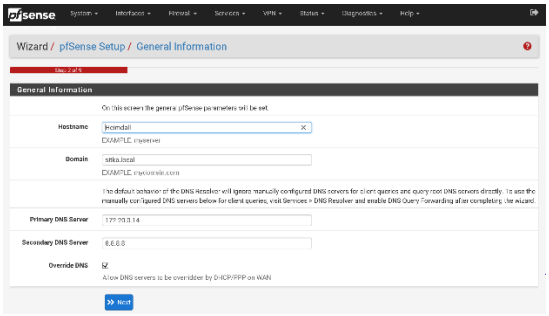
2- Exécution du Wizard de la configuration de base

Un Wizard à 9 étapes va s'exécuter par défaut
Les premières étapes sont des informations d'ordre générales traitant le SAV Netgate

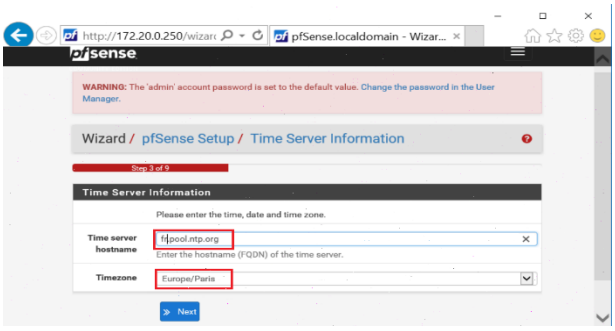




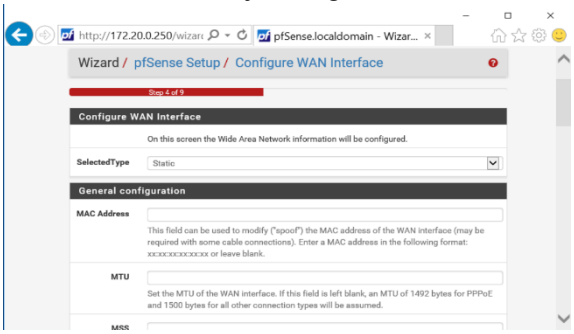
On rentre notre nom du serveur heimdall
le nom de domaine sitka.local



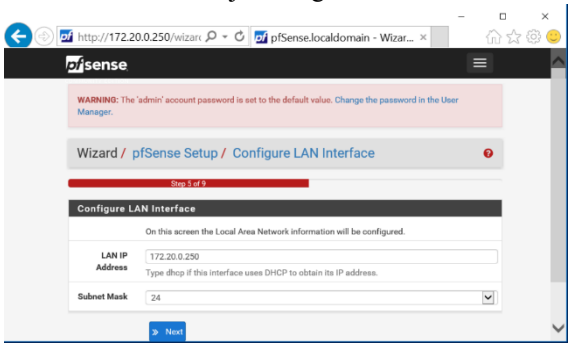
On configure le serveur NTP sur **fr.pool.org**
et le Timezone sur **Europe/Paris**



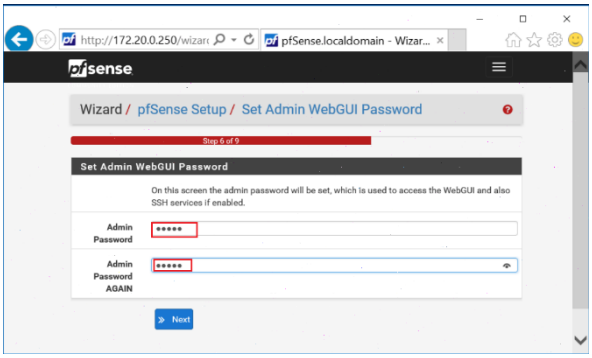
L’interface Wan est déjà configurée



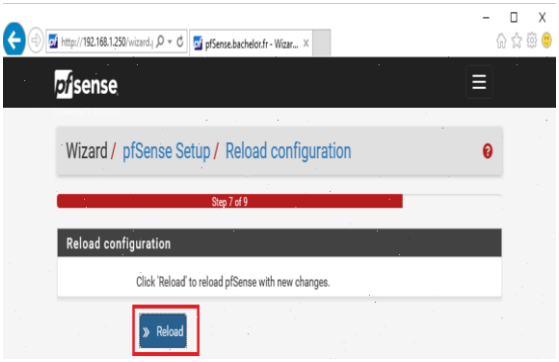
L’interface Lan est déjà configurée

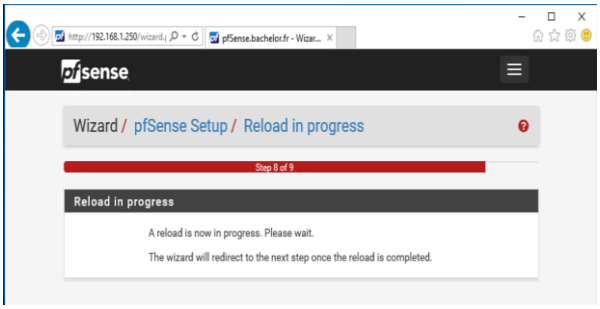


On change le mot de passe de l’admin Par défaut

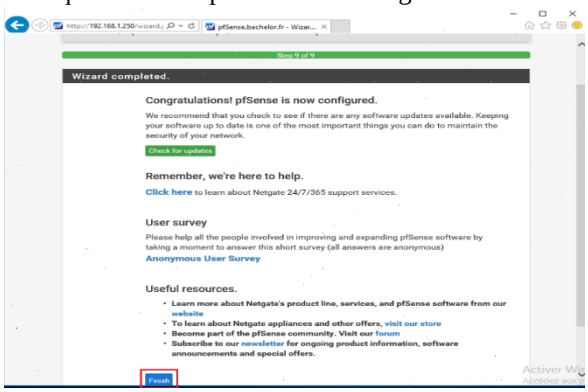


On clique sur reload pour appliquer la configuration

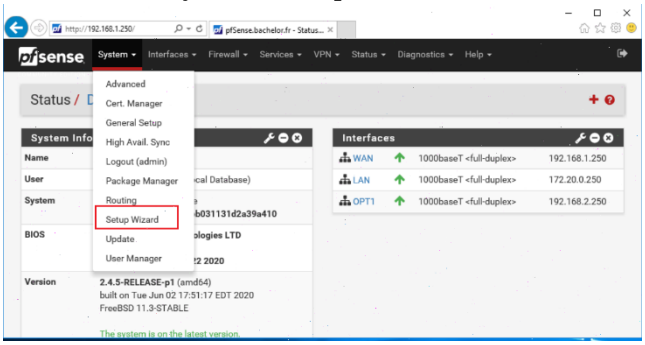




On clique sur finish pour finir la configuration

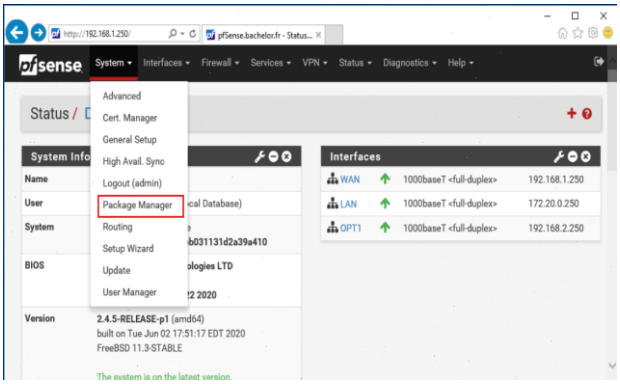


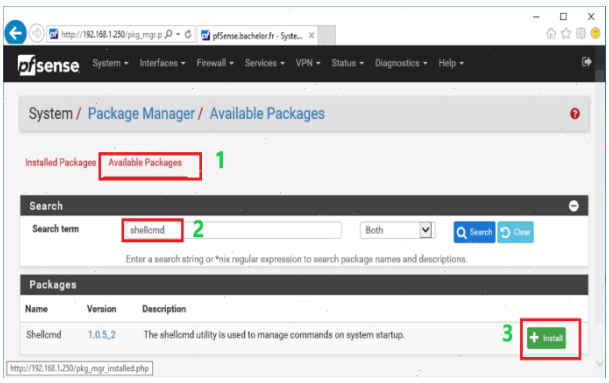
On peut relancer le Wizard en cas d’erreurs
En allant dans **Système +Setup Wizard**

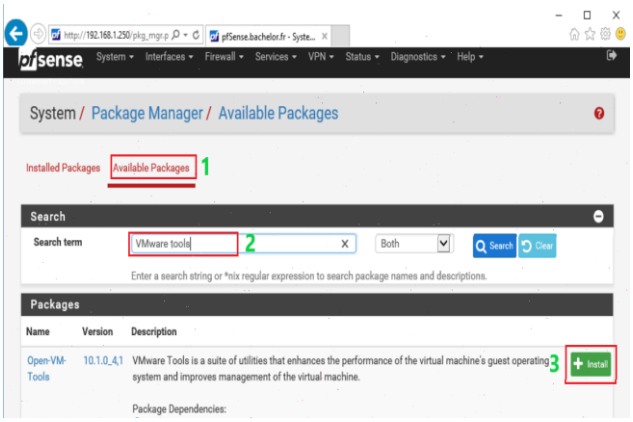


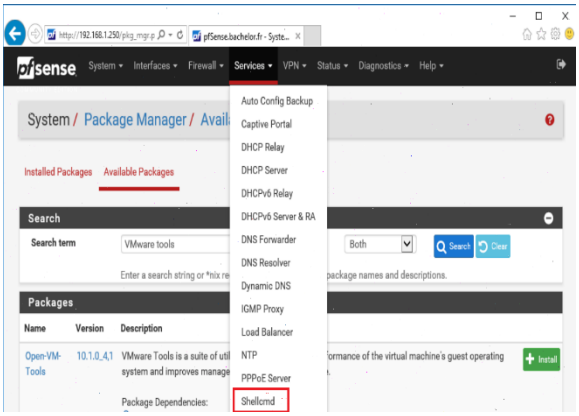
3- La mise en place de la configuration du clavier en fr de façon permanente En même temps on en profite pour installer VMware tools

Dans cette étape on installe les paquets **shellcmd** et **VMWare tools**

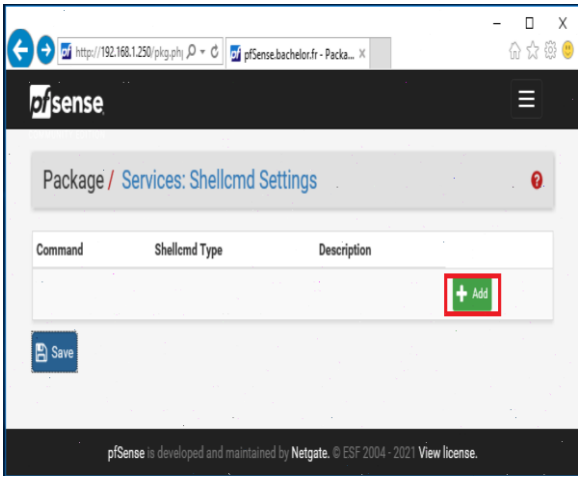


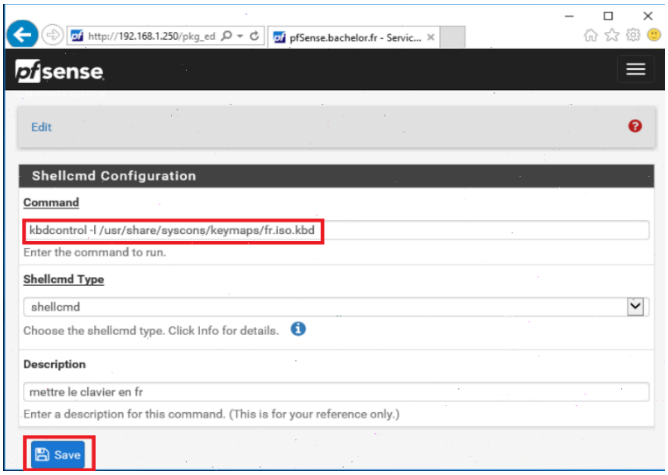






Tapez cette commande **kbdcontrol -l /usr/share/syscons/keymaps/fr.iso.kbd** dans le champ commande puis redémarrer votre machine pfsense et vérifiez que le clavier est en AZERTY



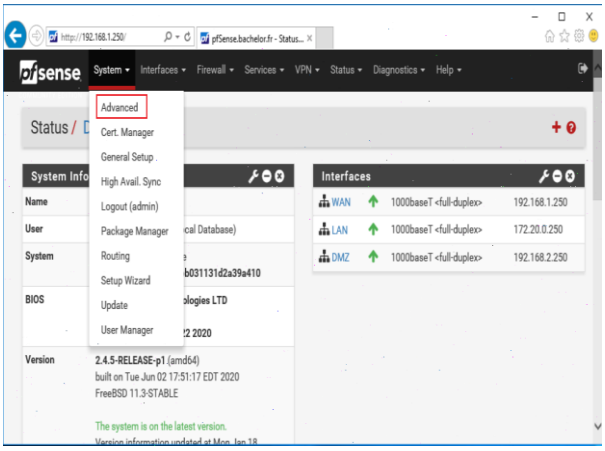


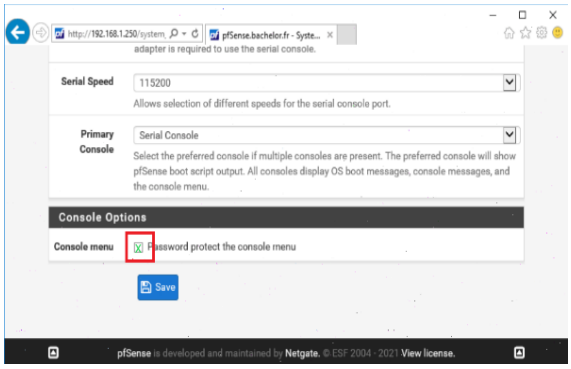
Sécurité

A- Sécurisez la console par mot de passe
B- Sécurisez l'accès par ssh
C- Sécurisez L'interface web par https
   a- Créer une autorité de certification interne
   b- Générer un certificat web
   c- Injecter le certificat web dans mon serveur pfsense

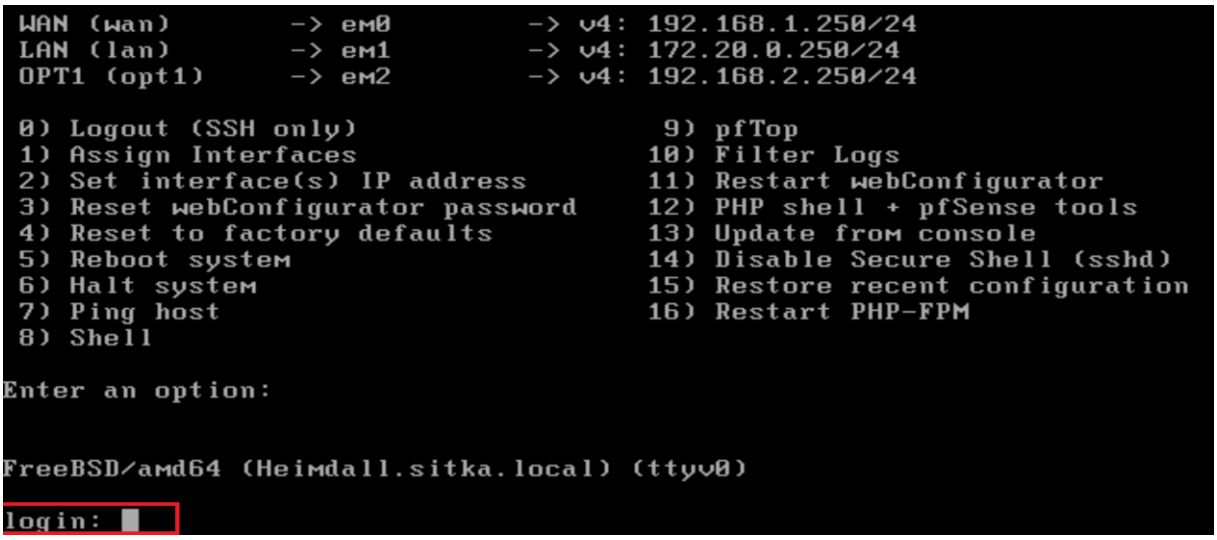
A- Sécuriser la console Pfsense

vous cochez la case console menu et vous Sauvegardez



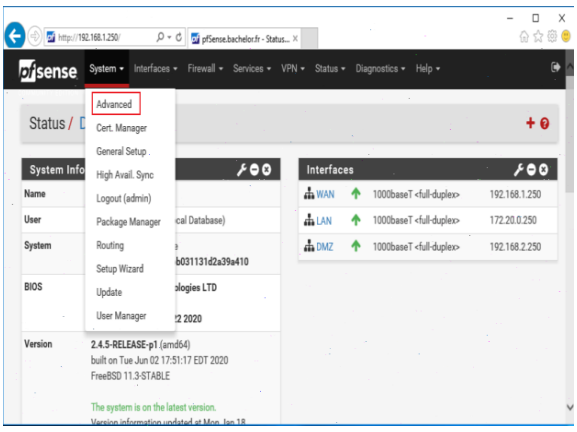


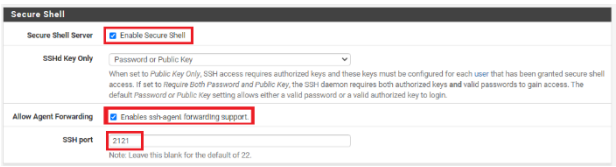
On constate que ma console à un login



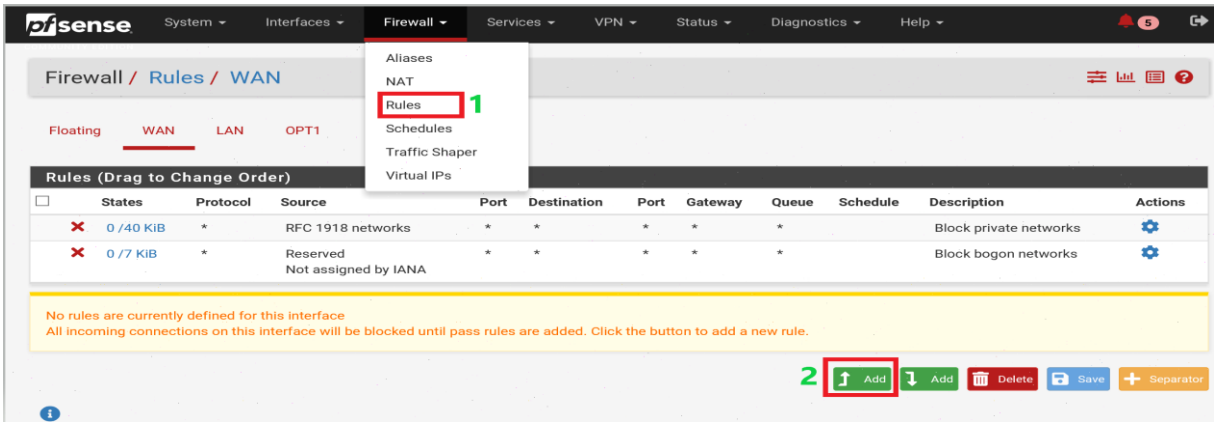
B- Sécurisez l'accès par ssh

On active ssh pour accéder à la console de manière sécurisée on change le port par défaut en (2121) en terme de sécurité il est toujours conseillé de changer les port par défaut; on peut aussi faire une authentification avec clé **privé/publique** au lieu d'une authentification par mot de passe

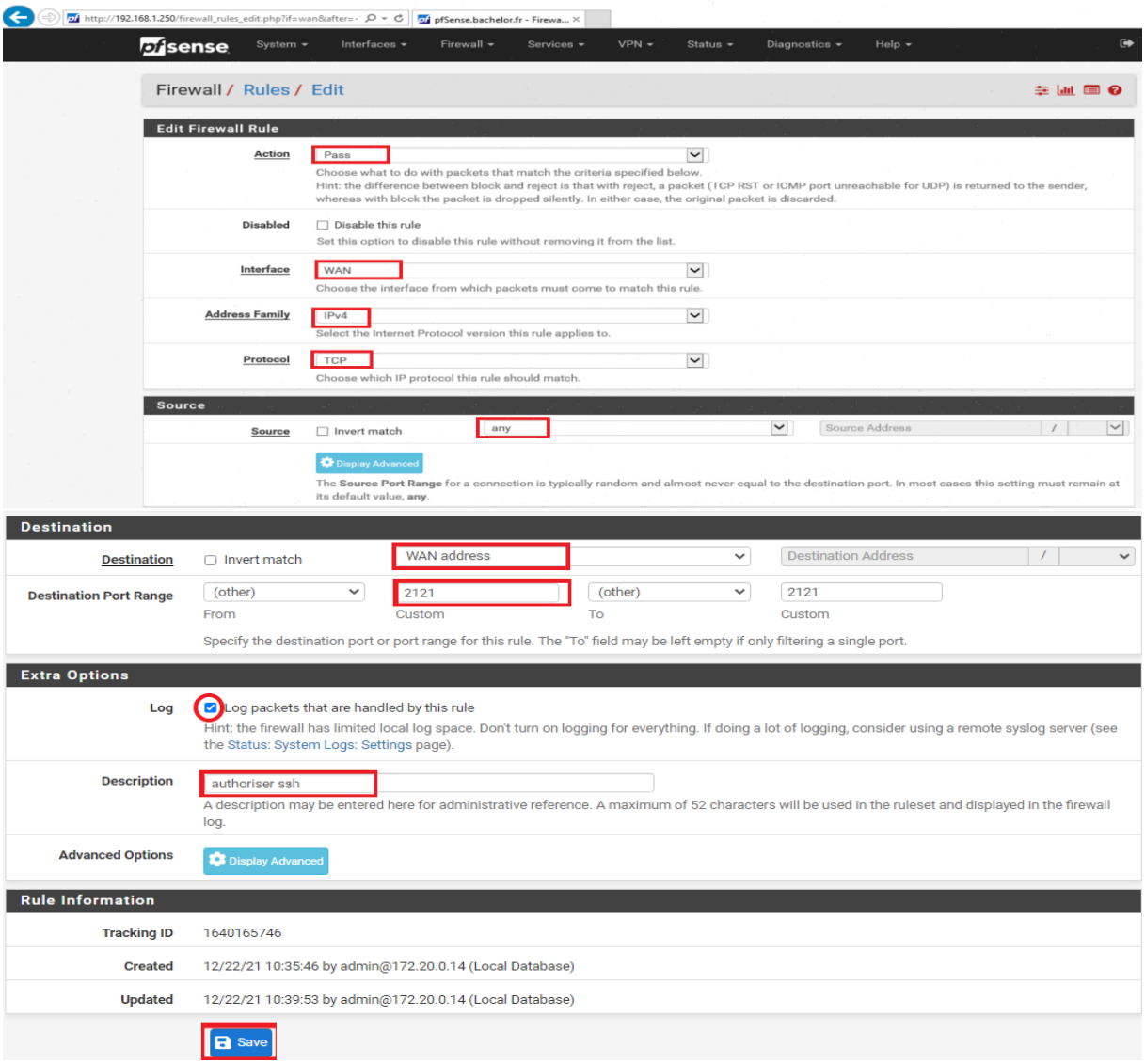




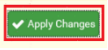
Maintenant il faut une **règle** autorisant **ssh** sur l'interface **Wan** on va dans le menu **interface +rule + ad**

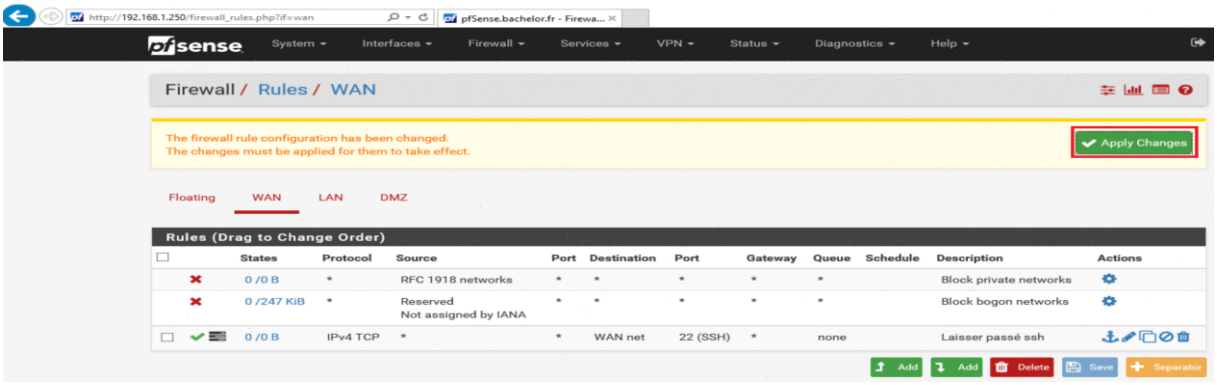


On rentre les choix ci-dessous après il ne faut pas oublier d'enregistrer et d'appliquer les changements comme indiqué dans ces captures d'écrans.



Après avoire enregistrer 

on applique les changements 



Attention sur Windows 2O16 ssh n'est pas installé nativement contrairement à Windows 2019 ou Windows 10 sur ces deux dernière version ssh est parmi les fonctionnalités qu'on peut installer.
Donc pour Windows 2016 suivre la procédure du fichier ssh_2016.docs pour installer ssh

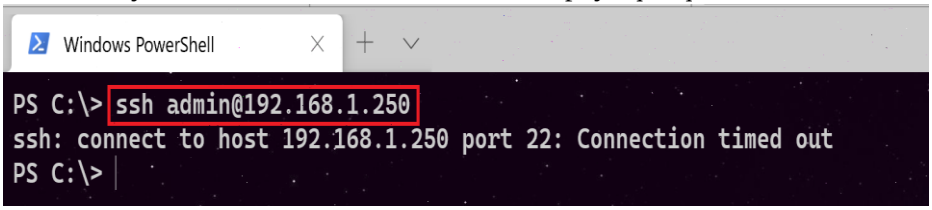
On teste la connexion à l'intérieure de notre périmètre j'utilise une des machines dans un Lan :
Je prends la machine AD je démarre le PowerShell et je me connecte sur une des interfaces de pfsense :
Le serveur pfsense m'envoie l'empreinte numérique de sa clé publique :

```
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:riqHfDO3Z9fhNsyAM1TC2shBu9F6+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:
```

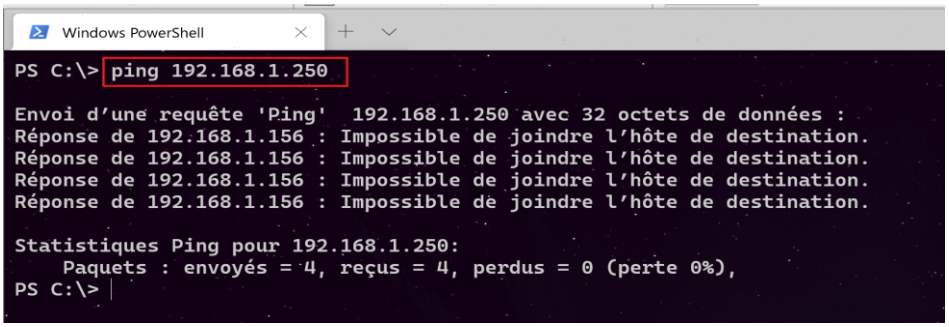
On peut vérifier si l'empreinte numérique sur le serveur ssh est la même que celle envoyée par le serveur j'affiche le contenu détaillé du répertoire /etc/ssh après je génère l'empreinte numérique de la clé publique **ssh_host_ed25519_key.pub**
en suivant les étapes **1+2+3+4**
En fin je compare les deux empreintes on constate qu'elles sont identiques

```
Enter an option: 8                                                    1
[2.5.2-RELEASE][admin@heimdall.sitka.local]/root: su root             2
# cd /etc/ssh
# ls                                                                  3
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                            4
256 SHA256:riqHfDO3Z9fhNsyAM1TC2shBu9F6+qSnpoKCTL/0dTo root@heimdall.sitka.local
 (ED25519)
+--[ED25519 256]--+
|     ...         |
|      .oo .      |
|    .o=.o        |
|     ++o         |
|     o.. S.      |
|  .   oo..  . .  |
| =..o.  .+..  * .|
|=.=.B++E=  .  B  |
|...B=O+=.  .  .  |
+----[SHA256]-----+
```

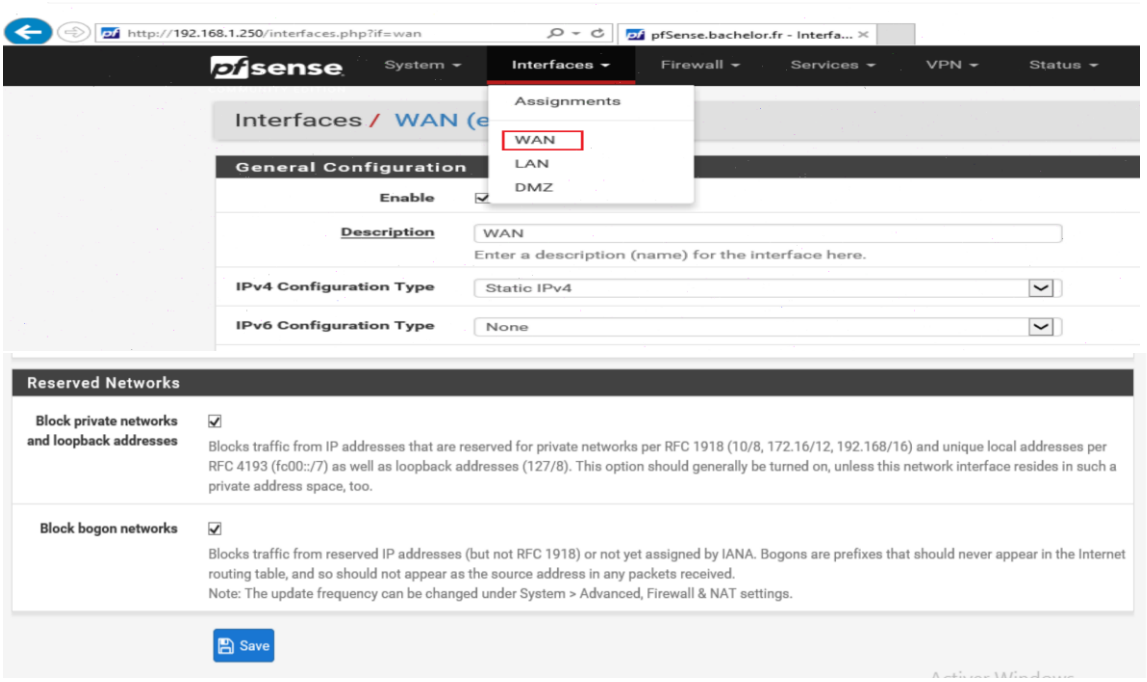
Maintenant on va tester la connexion en dehors de notre périmètre **Wan, sitka_Lan et opt_lan**
On va essayer une connexion de notre machine physique qui est en dehors de ce périmètre



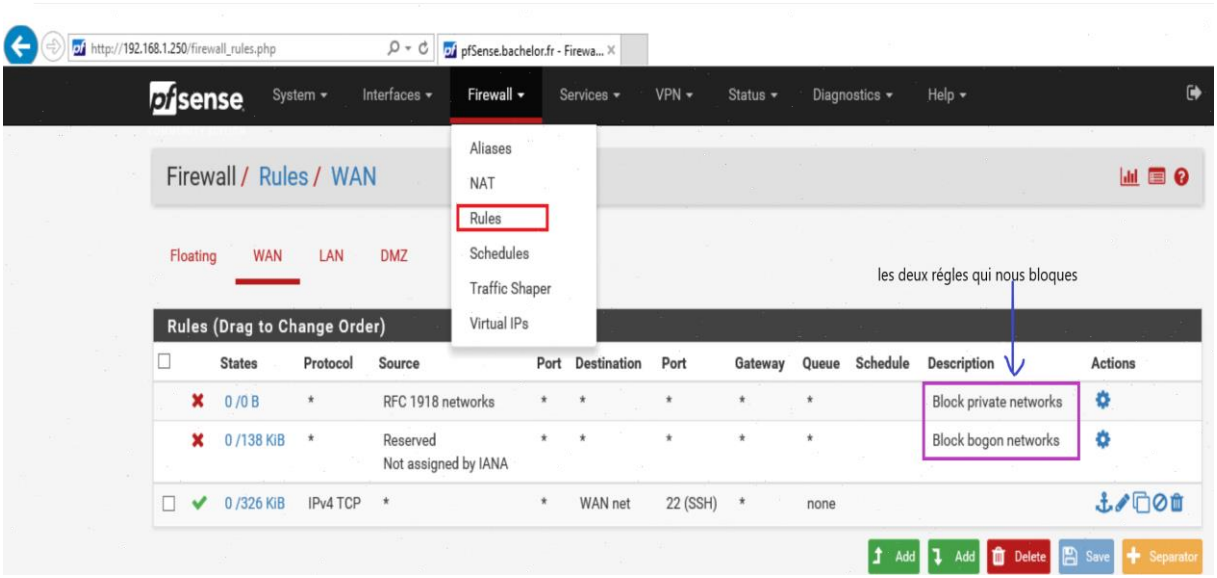
On remarque qu'il y'a **échec de connexion** ; on essaye de faire un **ping** sur cette interface, même constat



Cet échec est normal car PfSense bloque toutes requêtes venant d'une adresse privée en dehors de son périmètre **Wan, sitka_lan et opt_lan,** on peut vérifier ceci aisément en allant dans le menu **Interface + Wan** tout en bas de la page on trouve deux cases cochées ce qui explique ce blocage

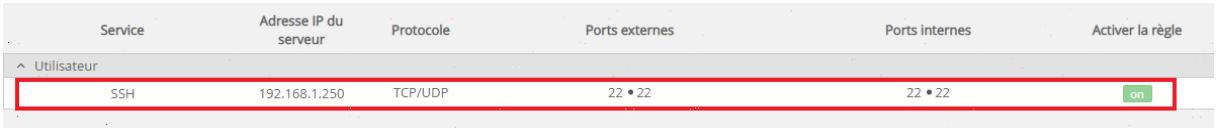


On trouve la même chose dans les règles par défaut de l'interface wan



Maintenant on va essayer d'accéder à notre serveur PfSense à partir de l'extérieur en utilisant notre adresse publique.
Tout d'abord :

1- Il faut accéder à la boxe internet et ouvrir le port 22 en créant une redirection de port



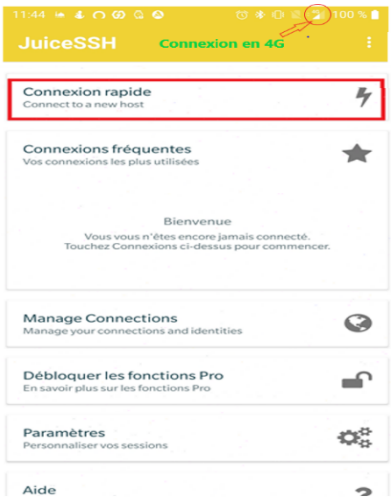
2- Ensuite il faut déterminer notre adresse publique soit à partir de la boxe ou un site internet http://www.whatismyip.com

3- Après sur notre smartphone on télécharge un client ssh sur Google Play google store **Juicessh**

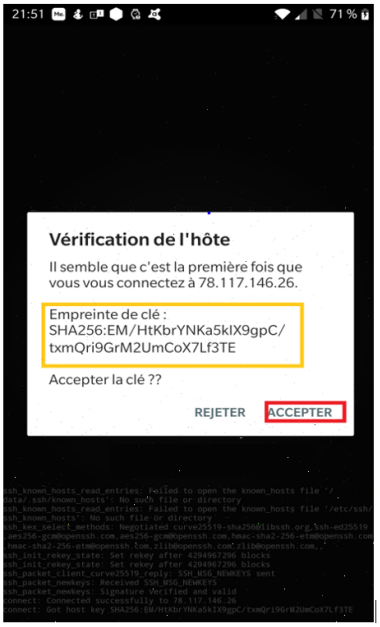
JuiceSSH - SSH Client

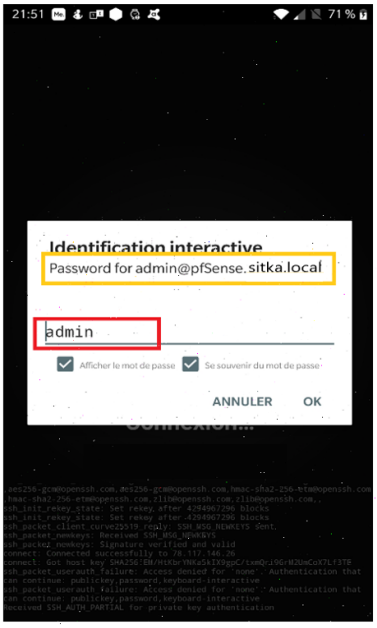
4- Sur notre smartphone il faut qu'on se mette en 4G et non en wifi car il na faut pas oublier que PfSense bloque les connexions provenant d'adresse IP en dehors de son périmètre.
5- On ouvre l'application et on commence à établir notre connexion ssh

On sélectionne connexion rapide ssh admin@ adresse publique

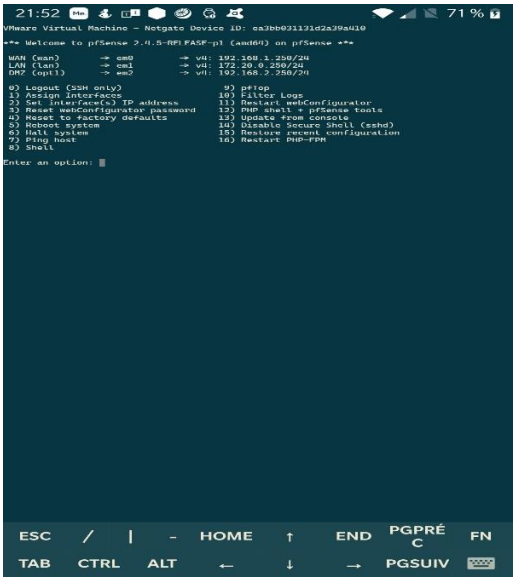


Le serveur nous envoie l'empreinte de sa clé publique
On constate que c'est la même que celle qu'on a calculé
Sur le serveur
EM/HtKbrYNKa5kIX9gpC/txmQri9GrM2UmCoX7Lf3TE rentre le mot de passe admin





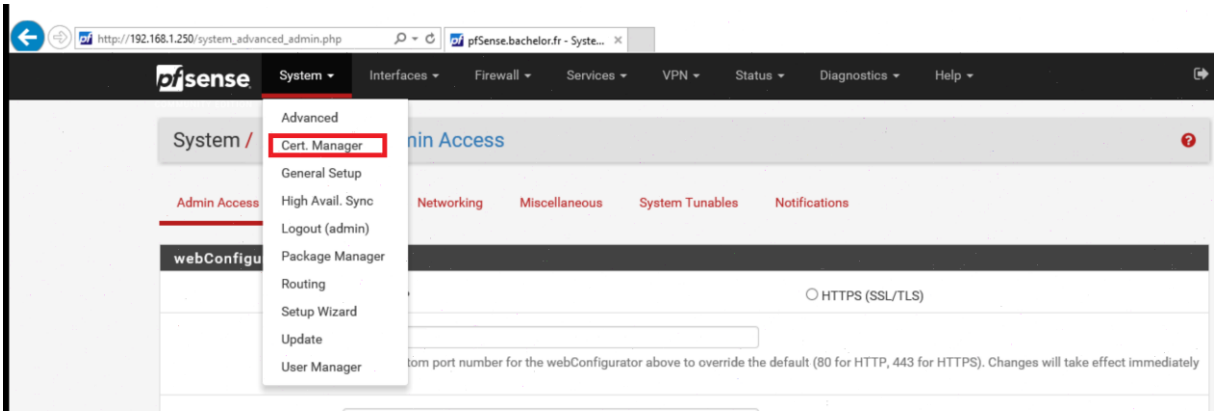
Après on tombe sur notre console PfSense



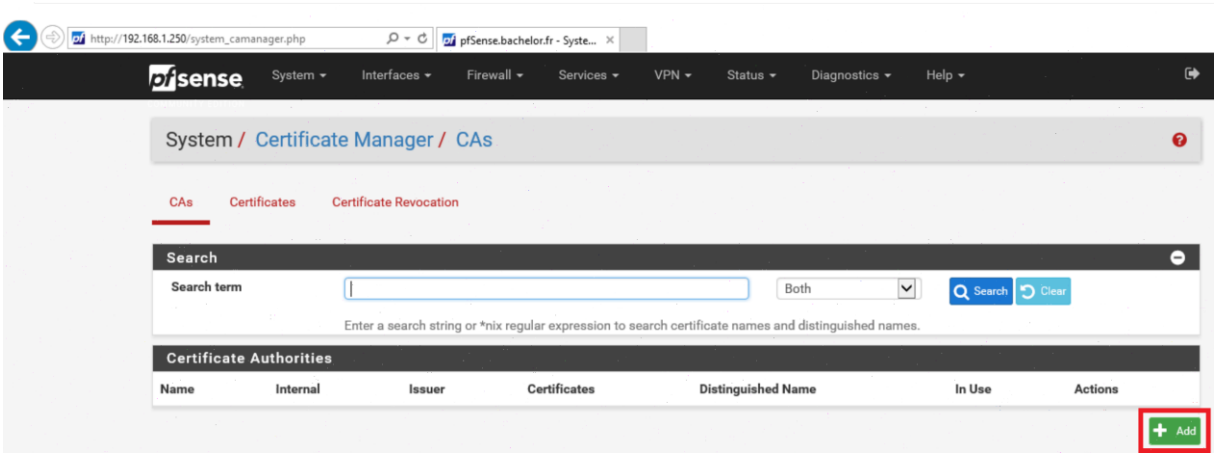
D- Sécurisez L'interface web par https

1- Créer une autorité de certification interne

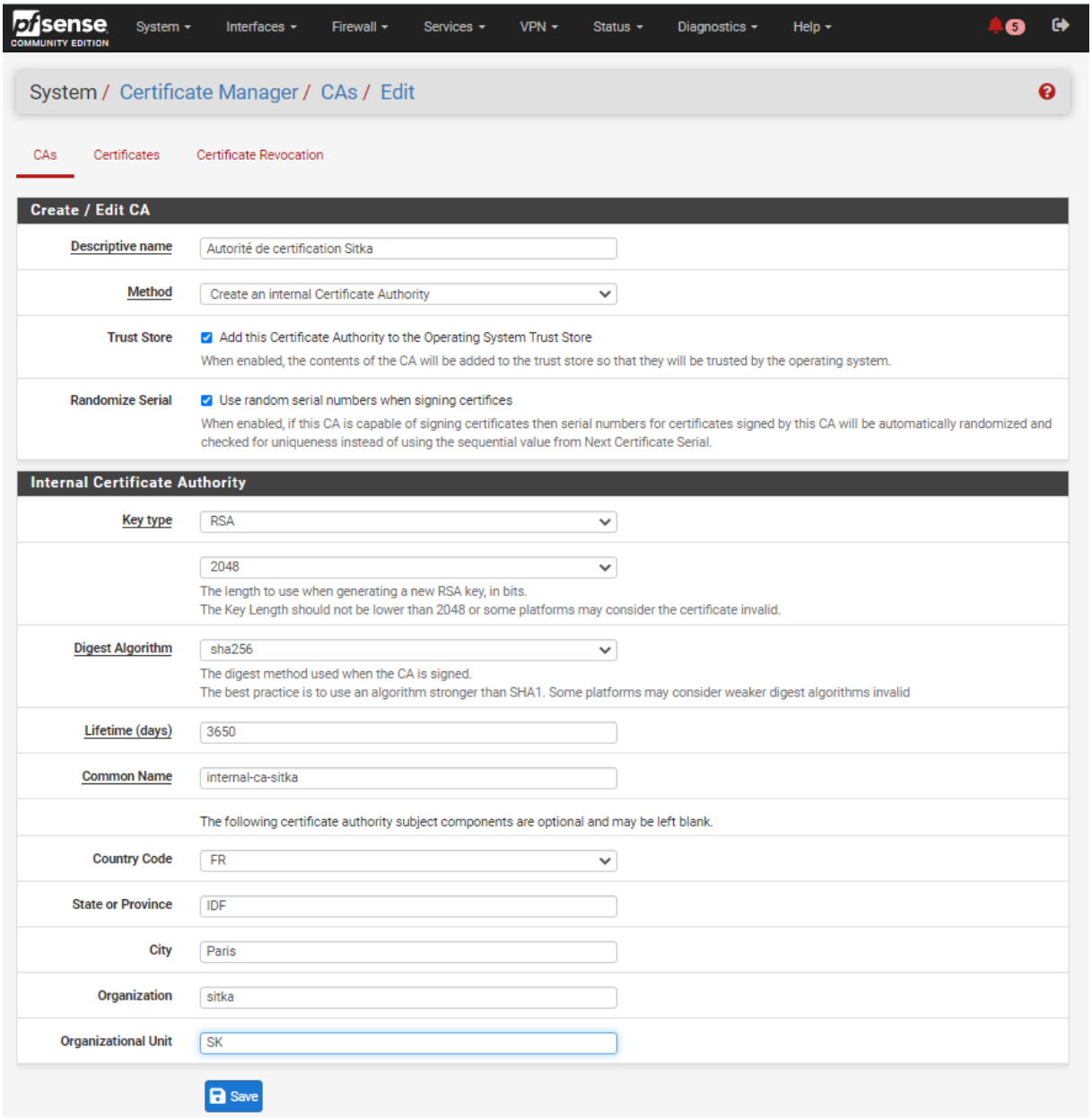
On va dans le menu **système + CertManager**



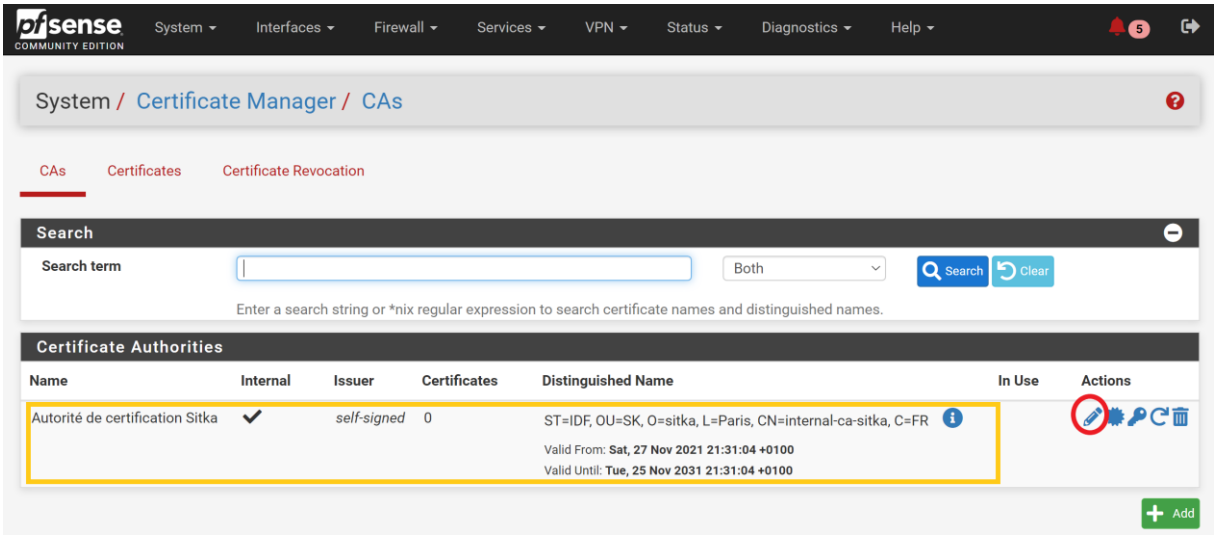
On commence à créer une autorité de certification interne



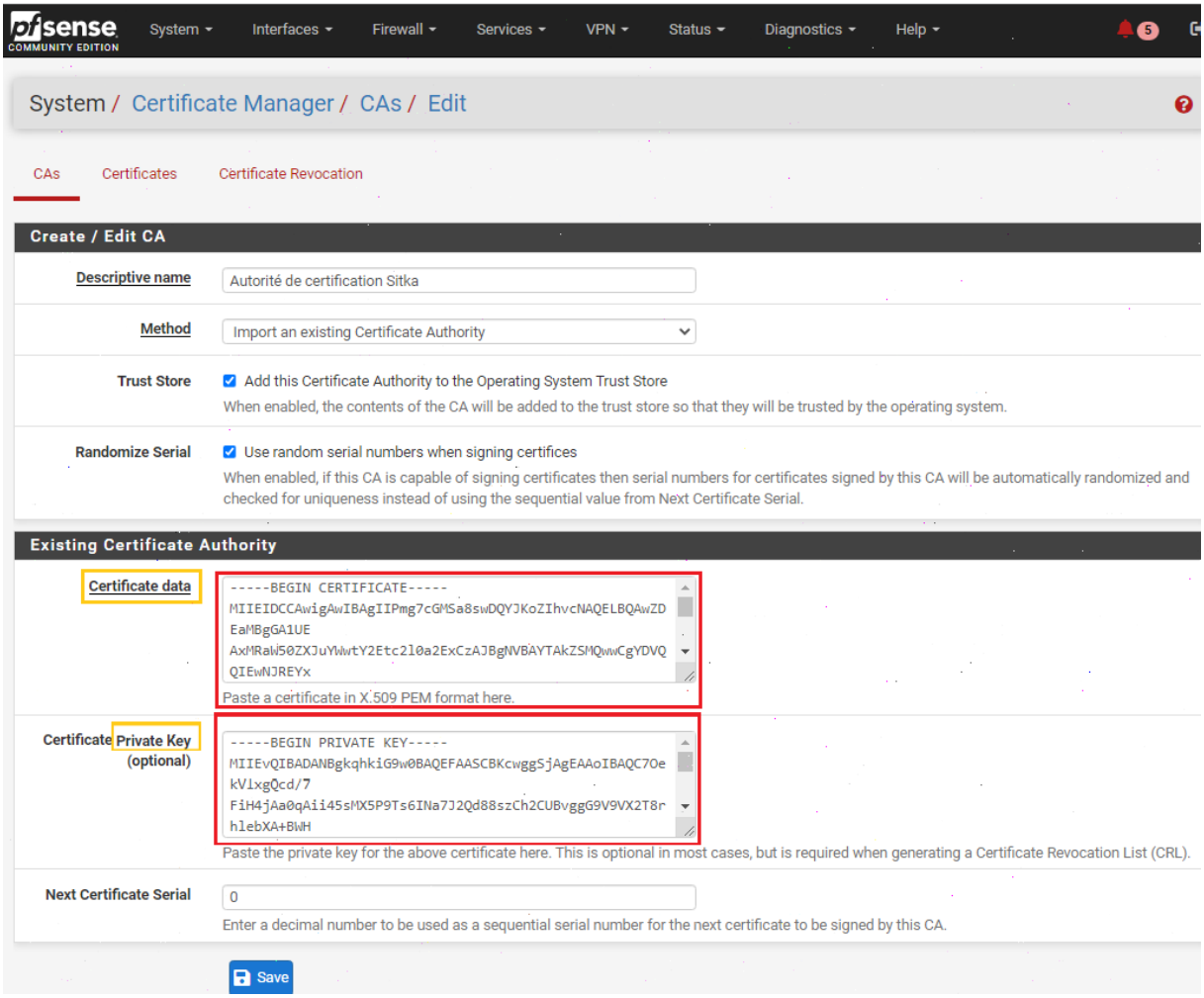
On remplit les champs suivants



Une fois qu'on enregistre nos paramètre notre autorité de certification apparait, on appuie sur le crayon pour éditer notre CA

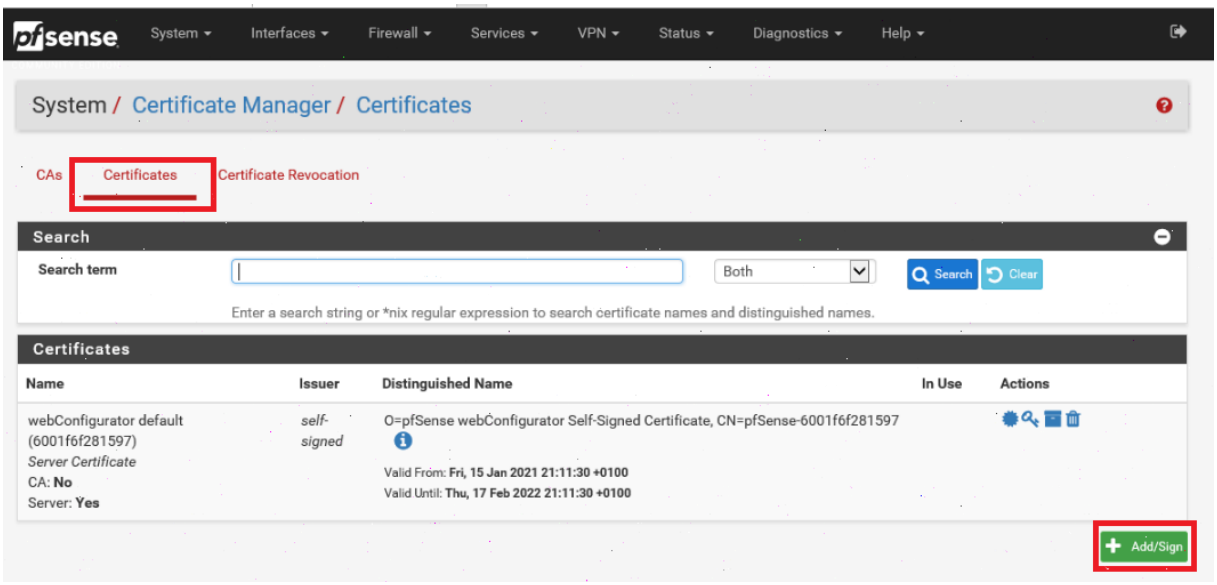


On affiche notre certificat et la clé publique qui lui est associé

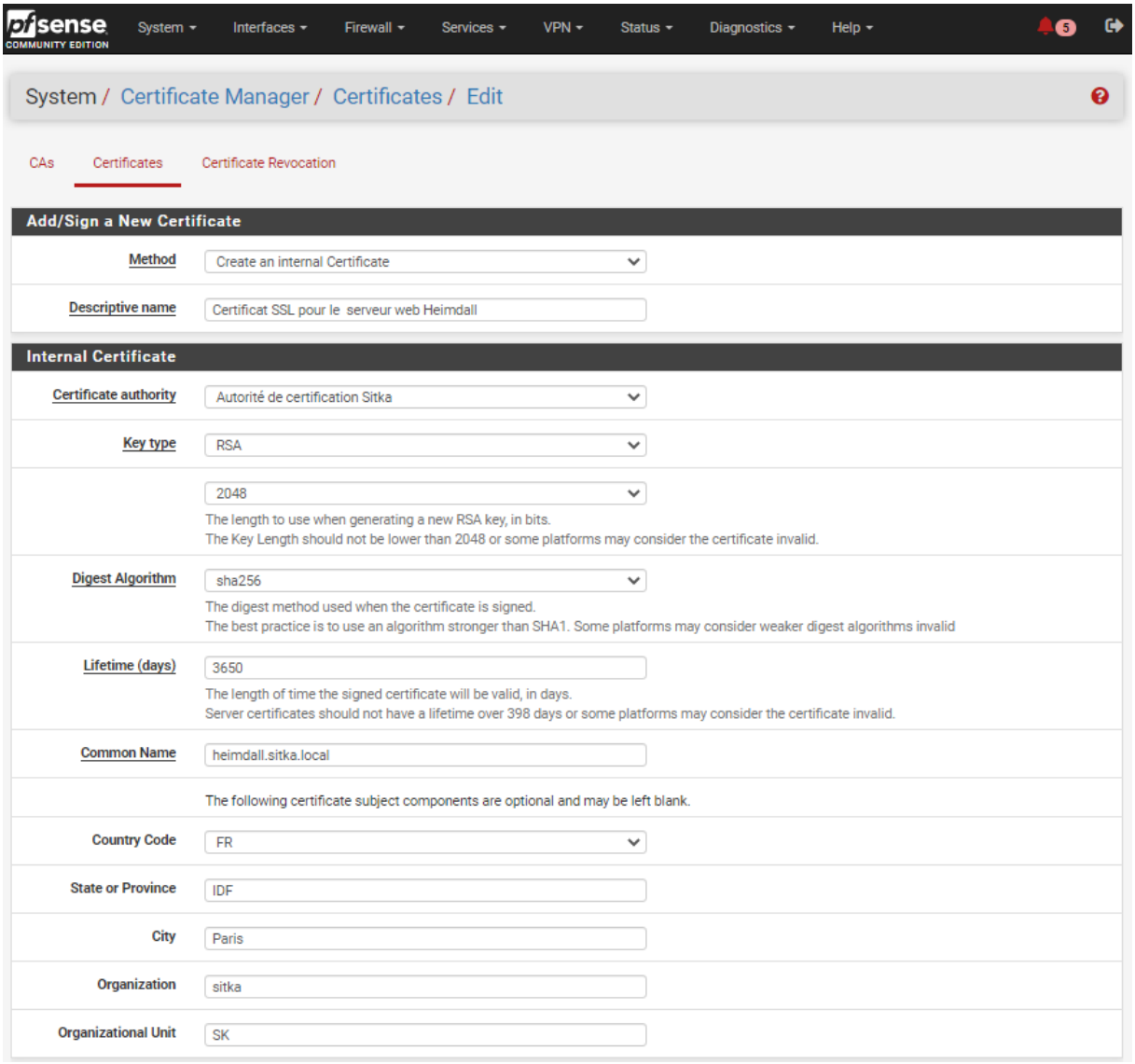


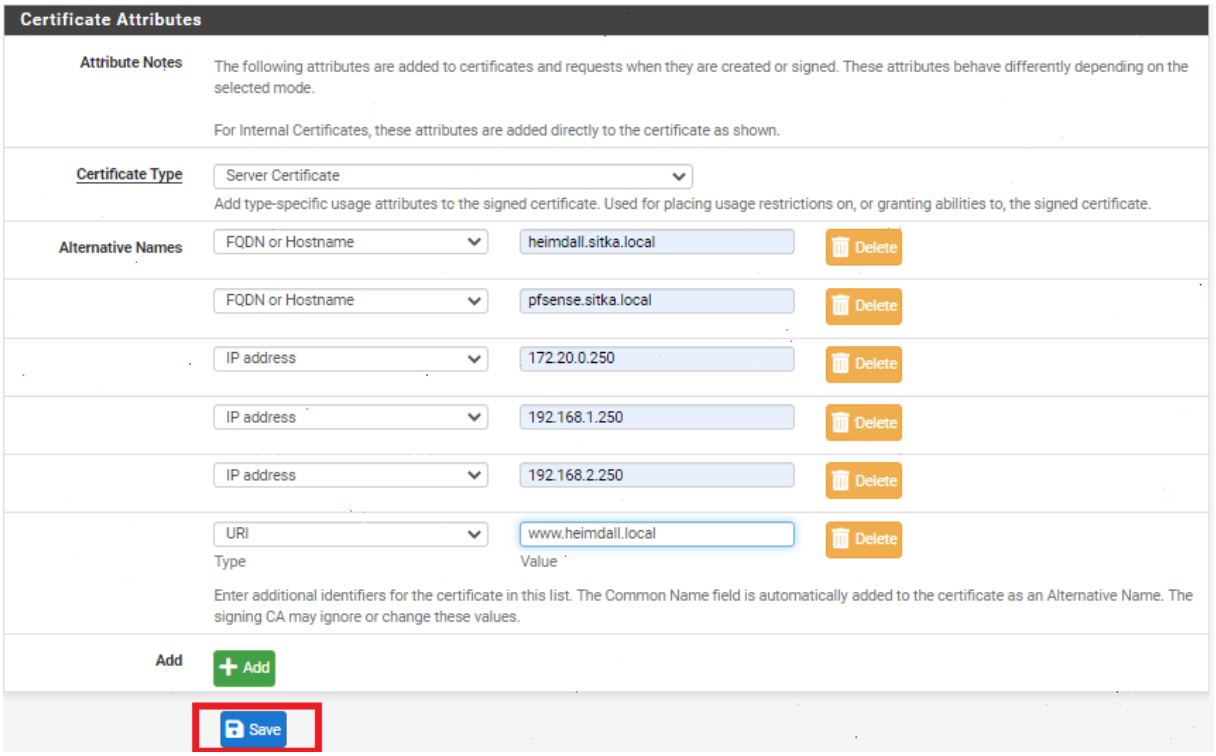
2- Générer un certificat web

Maintenant on va créer notre certificat web délivrer par la CA **autorité de certification sitka** qu'on a mis en place dans l'étape précédente il suffit de cliquer sur add et remplir les champs nécessaires

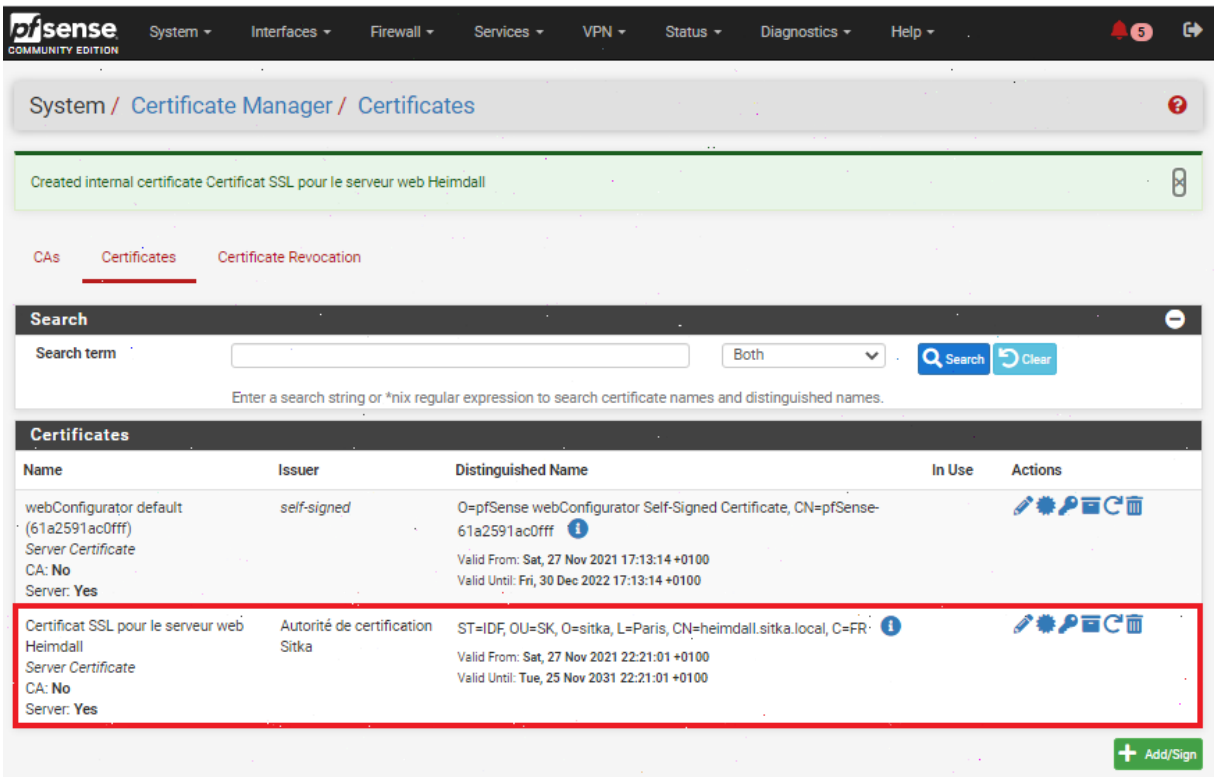


ci-dessous les champs remplie pour créer notre certificat


pfsense
COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
5
System / Certificate Manager / Certificates / Edit
CAs
Certificates
Certificate Revocation
Add/Sign a New Certificate
Method
Create an internal Certificate
Descriptive name
Certificat SSL pour le serveur web Heimdall
Internal Certificate
Certificate authority
Autorité de certification Sitka
Key type
RSA
2048
The length to use when generating a new RSA key, in bits.
The Key Length should not be lower than 2048 or some platforms may consider the certificate invalid.
Digest Algorithm
sha256
The digest method used when the certificate is signed.
The best practice is to use an algorithm stronger than SHA1. Some platforms may consider weaker digest algorithms invalid
Lifetime (days)
3650
The length of time the signed certificate will be valid, in days.
Server certificates should not have a lifetime over 398 days or some platforms may consider the certificate invalid.
Common Name
heimdall.sitka.local
The following certificate subject components are optional and may be left blank.
Country Code
FR
State or Province
IDF
City
Paris
Organization
sitka
Organizational Unit
SK



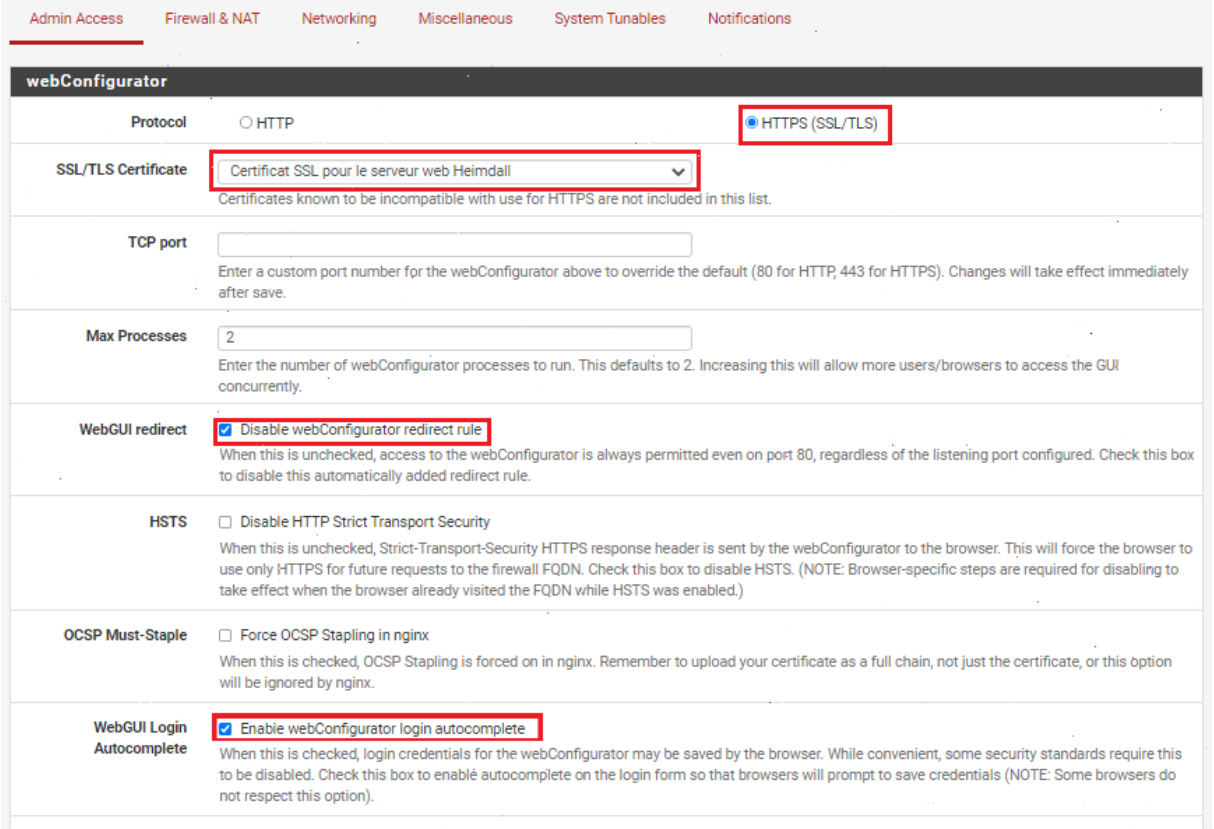
Une fois qu'on enregistre notre certificat apparait



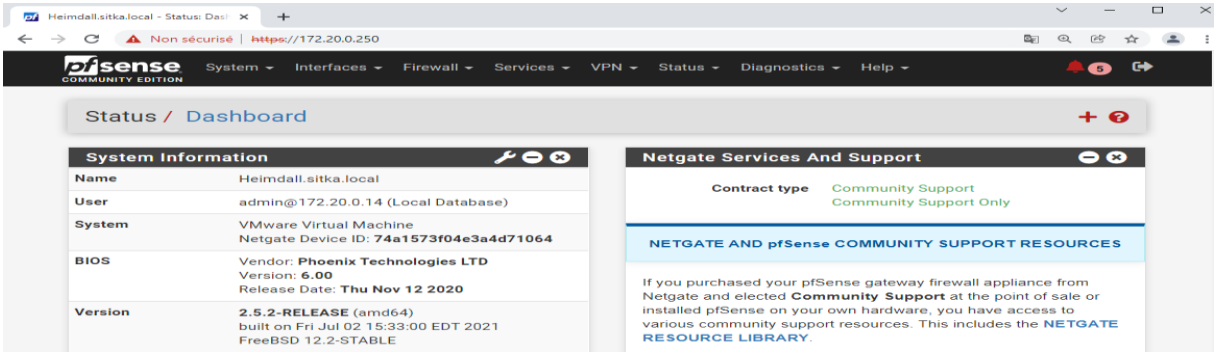
3- Injecter le certificat web dans mon serveur PfSense

Maintenant on va injecter notre certificat dans notre serveur web PfSense, donc on va dans **système + Avanced**

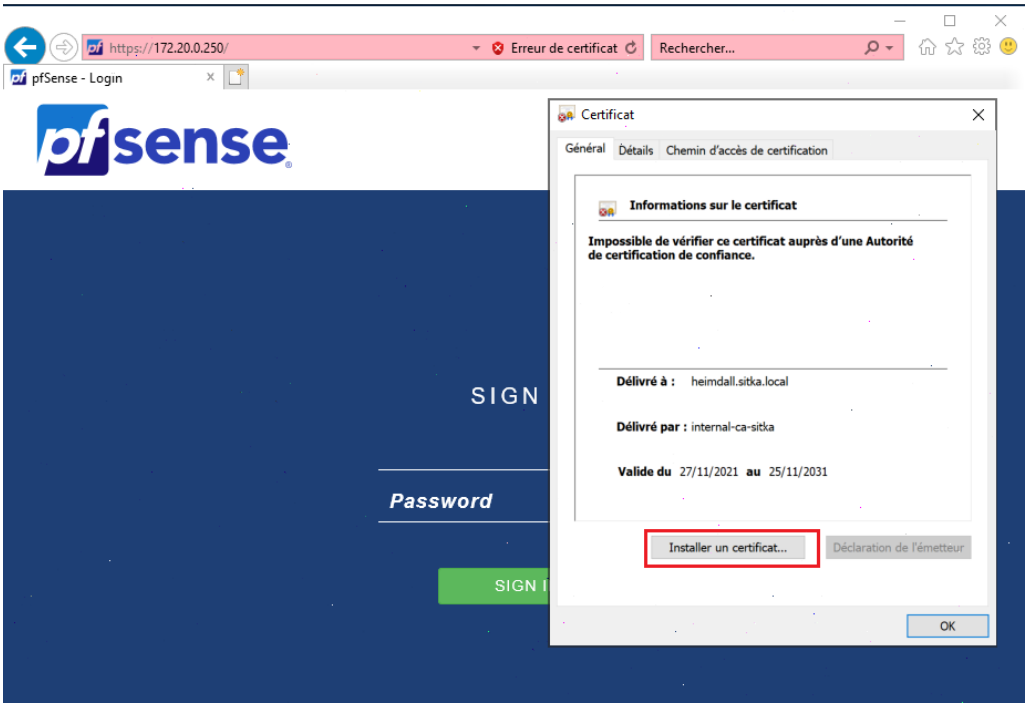
- On sélectionne notre certificat crée
- On laisse le port par défaut
- On laisse 2 en nombre de connexion simultané c'est-à-dire 2 personne max peuvent se connecter sur l'interface web PfSense
- On refuse la connexion en http
- On refuse que le navigateur enregistre les données de connexion



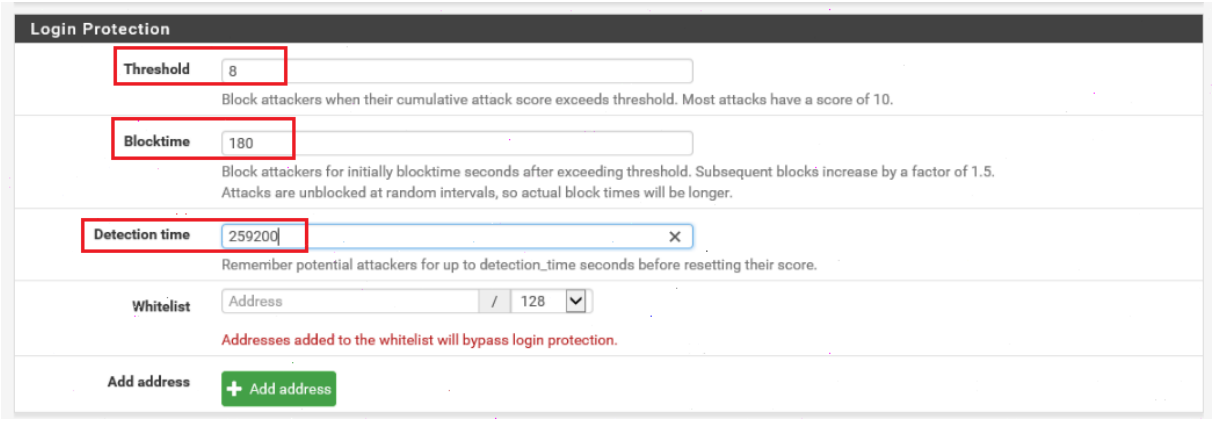
Après on sauvegarde notre navigateur va démarrer automatiquement
On se connecte sur l'interface https://172.20.0.250



Le certificat représente des erreurs car notre autorité de certification n'est pas de confiance donc il faut l'intégrer dans le magasin des autorités de certification de confiance en installant le certificat de l'autorité racine



Protection de la connexion



Authentification LDAP et LDAPS

A- Test de la connectivité LDAP et LDAP (LDAP sur SSL) sur le serveur active directory hermes

1- Connectivité LDAP
2- Connectivité LDAPS **(LDAP sur SSL)**

a- Création d'une autorité de certification sur le contrôleur de domaine hermes

i- Ajouter le rôle certificat sur hermes
ii- Configuration du rôle certificat sur hermes

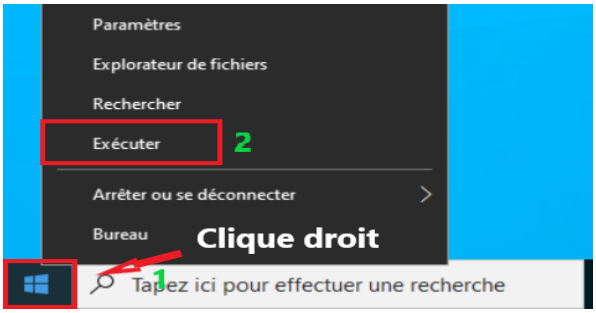
B- Test de la connectivité LDAP et LDAP (LDAP sur SSL) sur heimdall (pfsense)
C- Création des comptes utilisateurs sur le contrôleur de domaine
D- Création des authentifications LDAP et LDAPS sur le serveur pfsense
E- **Création de l'authentifications LDAP**
1- Création de l'authentifications LDAP
2- Création de l'authentifications LDAPS
a- Création du formulaire de l'authentification LDAPS
b- Analyse avec Wire Shark du trafic pfsense active directory
c- Exportation du certificat de l'autorité de certification hermes
d- Importation du certificat de l'autorité de certification racine
e- Test de la connexion ssl entre pfsense et le contrôleur de domaine

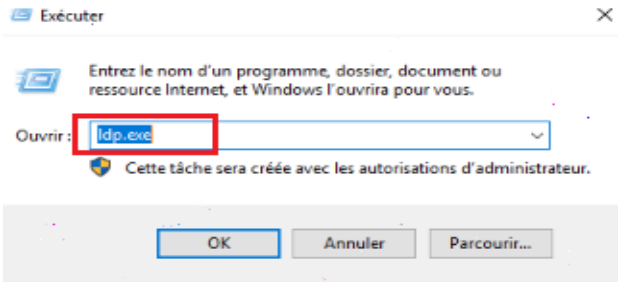
3- Utilisation des authentifications LDAP et LDAPS sur le serveur pfsense
a- Vérification de l'authentification LDAP et LDAPS
b- Création et configuration d'un groupes sur pfsense
c- Test de connexion sur l'interface web avec un compte ldap

A- Test de la connectivité LDAP et LDAPS sur le serveur active directory hermes

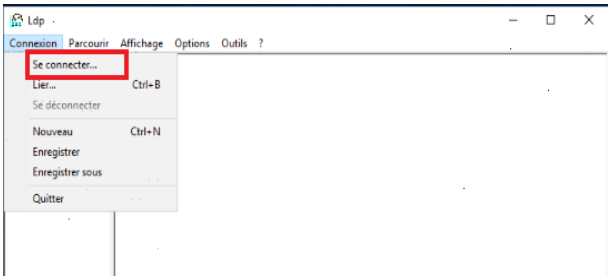
1- Connectivité LDAP

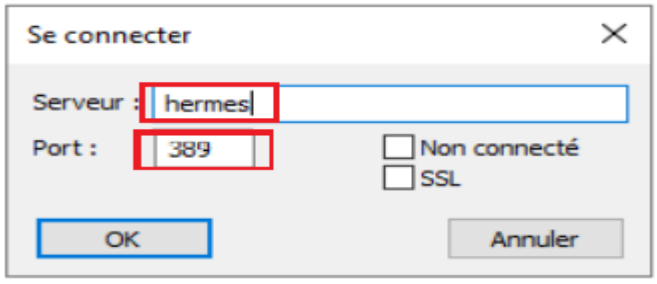
Sur le contrôleur de domaine on test la connectivité LDAP standard, donc clique droit sur le menu démarrer + exécuter puis on tape **ldp.exe** pour ouvrir l'explorateur LDAP



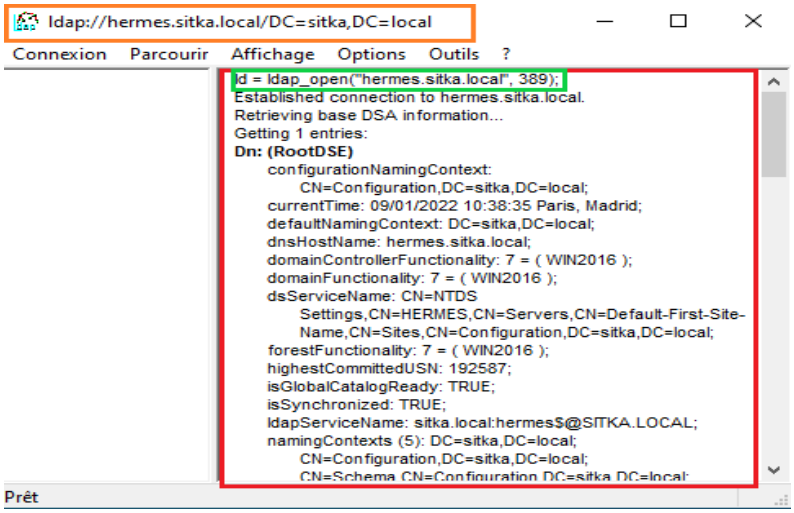


Un fois l'explorateur LDAP est ouvert l'explorateur on choisit le menu Se connecter et on rentre le nom du serveur **hermes.sitka.local** ainsi que le port de connexion **389**



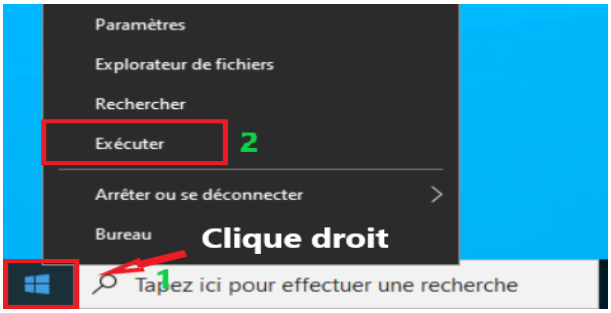


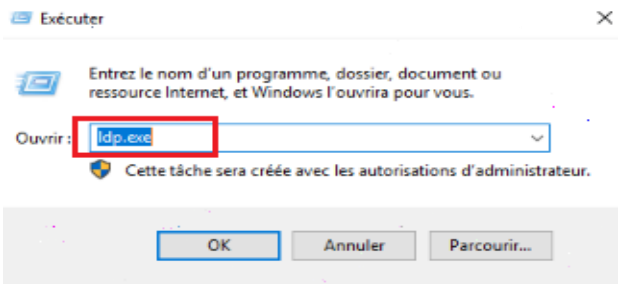
La connexion à la base d'annuaire fonctionne on peut identifier les partitions d'annuaire



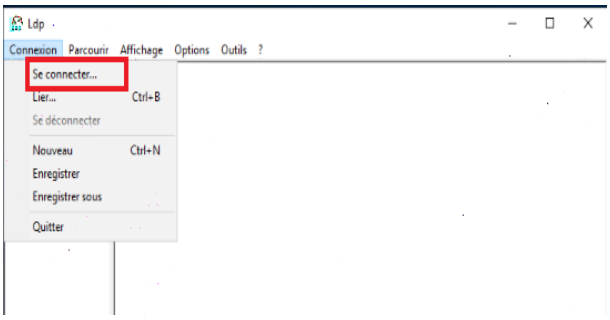
2- Connectivité LDAPS (LDAP sur SSL)

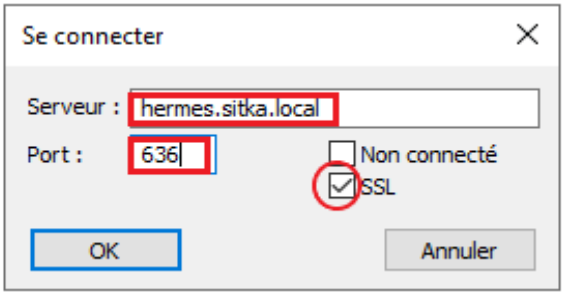
On fait la même chose que la procédure établissant une connexion standard on change juste le numéro de port et on coche ssl

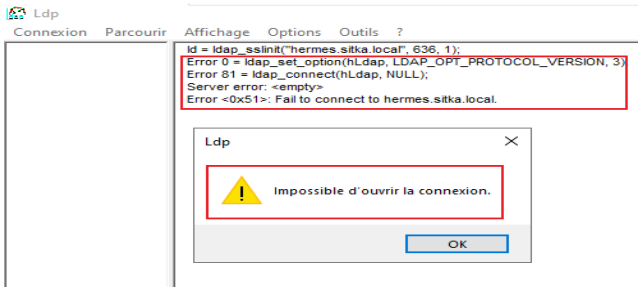




On tombe sur un message d'erreur, le contrôleur de domaine ne supporte pas LDAPS car il n'est pas associé à un certificat.







Il existe deux méthodes pour activer LDAPS (LDAP sur SSL) sur un contrôleur de domaine :

- Mettre un Certificat Racine sur le contrôleur de domaine en installant une autorité de certification racine sur hermes
- Utiliser un certificat tiers sur le contrôleur de domaine. (Hermes)

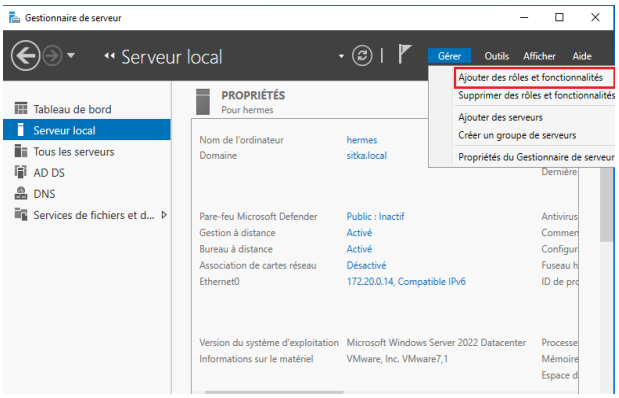
Pour notre procédure on choisira la première méthode, Donc il faut installer une autorité de certification afin de tirer parti de LDAPS

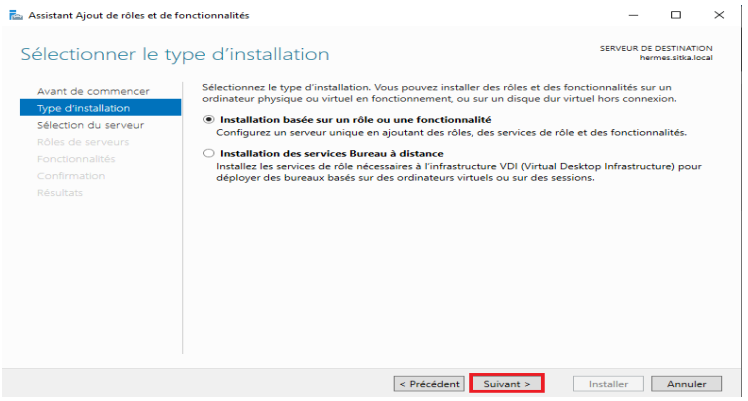
a- Création d'une autorité de certification sur le contrôleur de domaine hermes

Il est nécessaire d'installer le service autorité de certification. Pour fournir au contrôleur de domaine un certificat qui permettra au service LDAPS d'opérer sur le port 636.

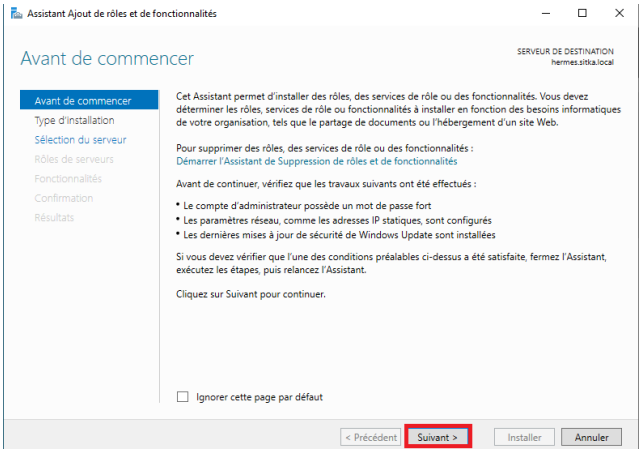
i- Ajouter le rôle certificat sur hermes

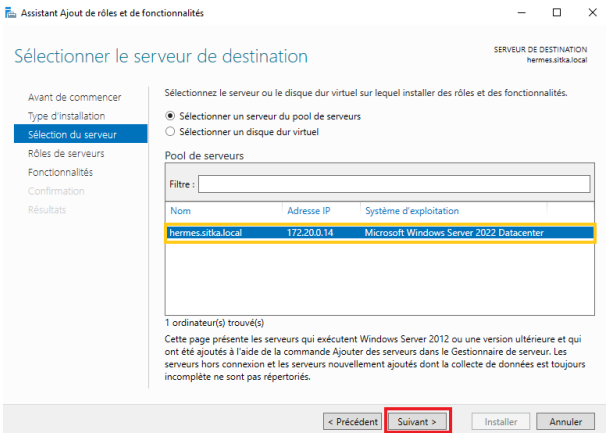
Accédez au menu Gérer et cliquez sur Ajouter des rôles et des fonctionnalités.



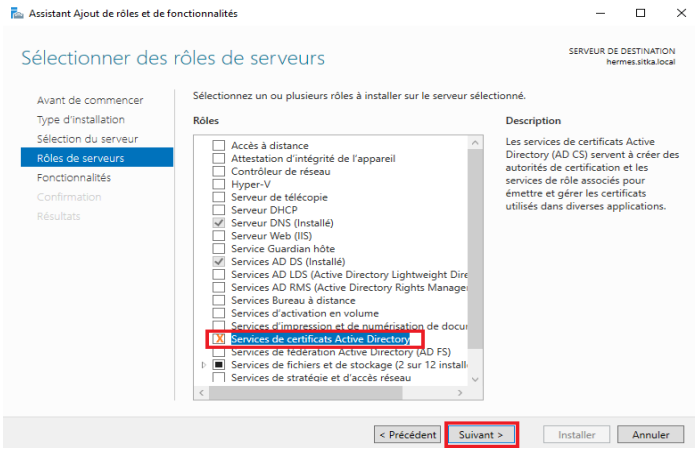


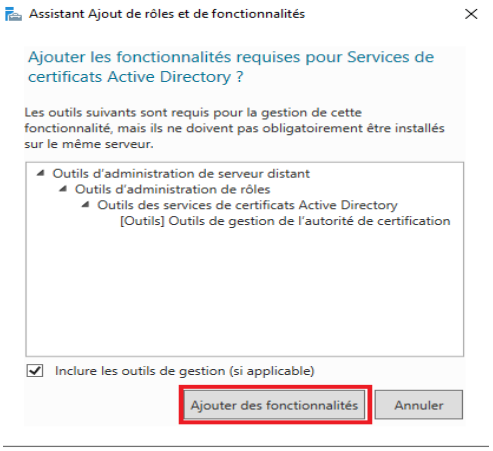
On vérifie le nom et l'adresse IP de notre serveur on clique après sur suivant



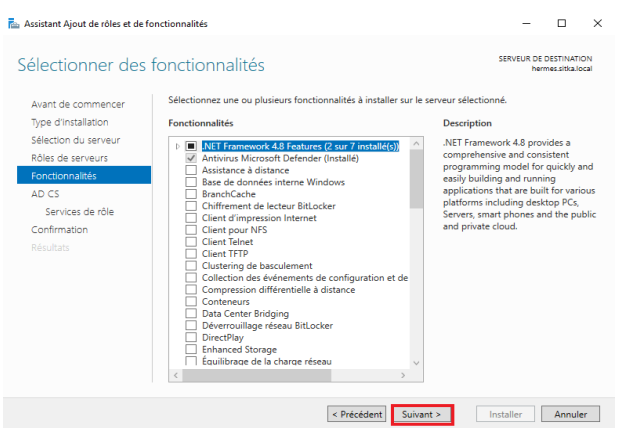


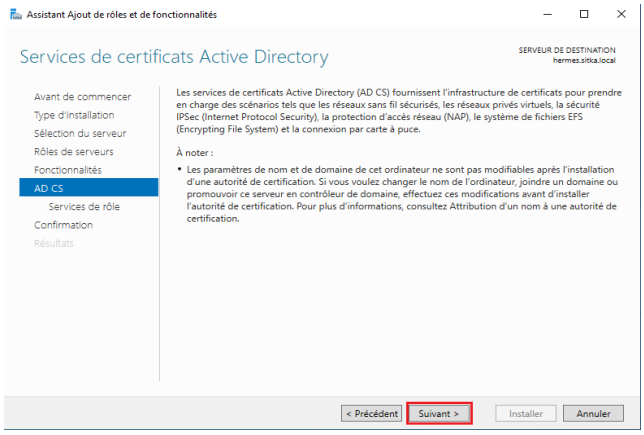
On coche Services de Certificats Active Directory et on rejoute les fonctionnalités



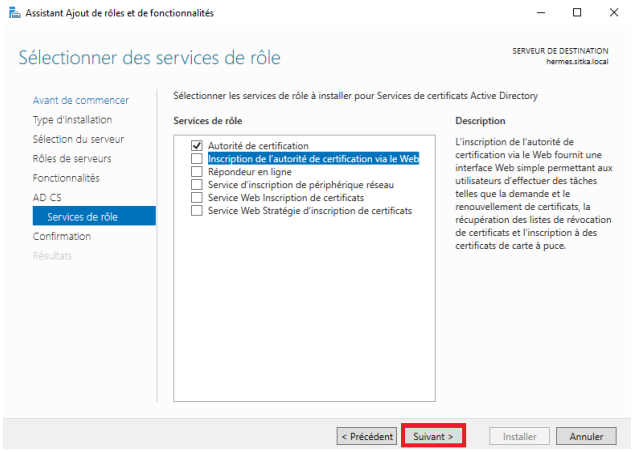


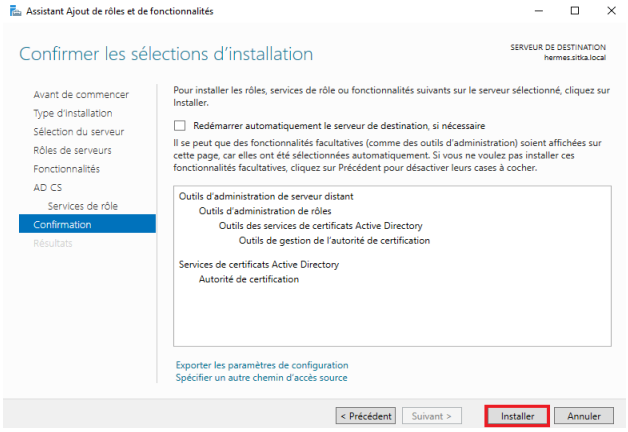
Sur les deux Boites de dialogues ci-dessous on laisse tout par défaut en faisant suivant.



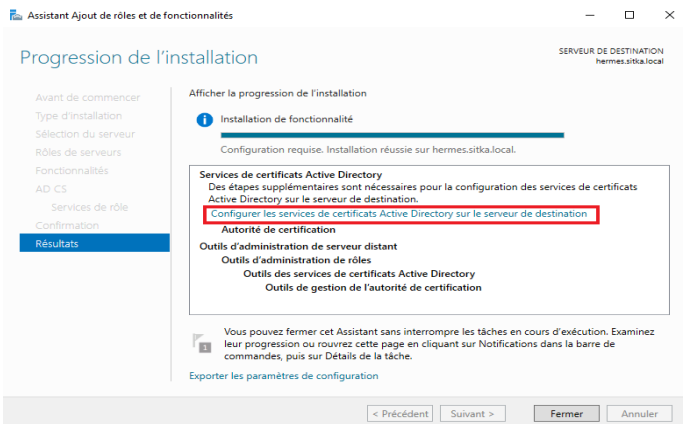


On sélectionne que l'option Autorité de certification





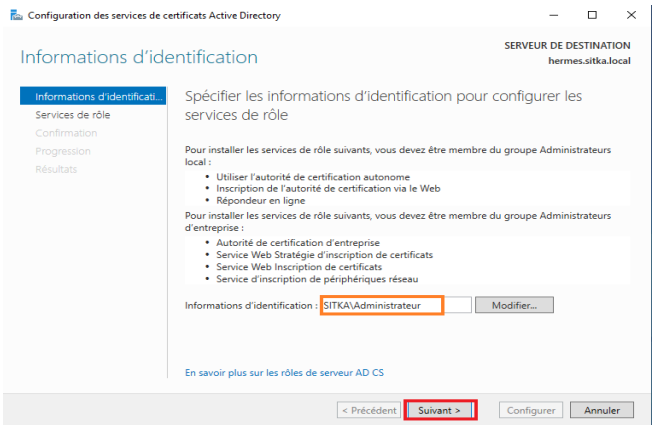
Dernière étape on clique sur le lien Configurer les services Active Directory sur le serveur de destination

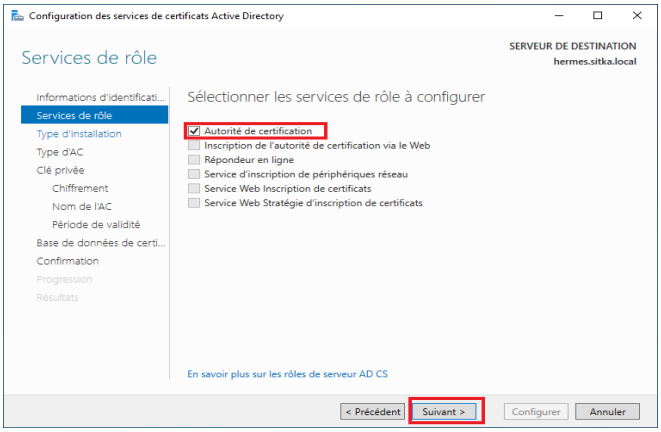


ii- Configuration du rôle certificat sur hermes

Une fois le rôle certificat est installé il faut maintenant le configurer, on vérifie les informations d'identification, il est obligatoire d'être connecté avec le compte de l'administrateur de l'entreprise (domaine\administrateur).

On coche après Autorité de certification, toutes les autres options on peut les installer après au besoin

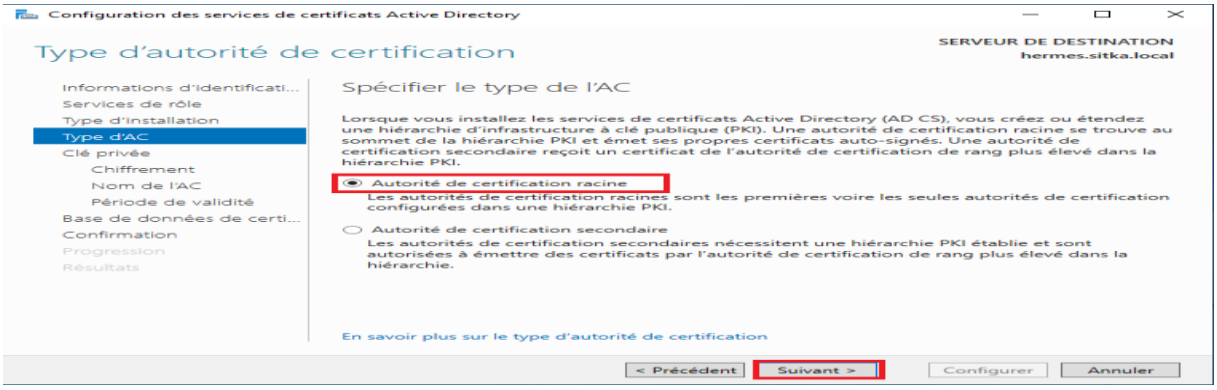




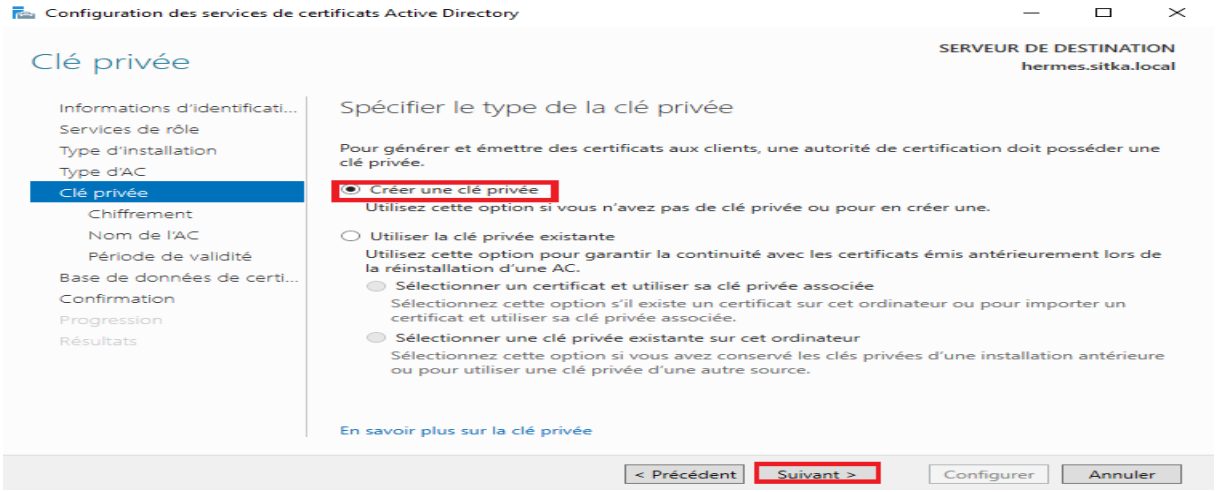
On sélectionne Autorité de certification d'entreprise afin que l'autorité de certification puisse utiliser l'annuaire LDAP

On sélectionne autorité de certification racine

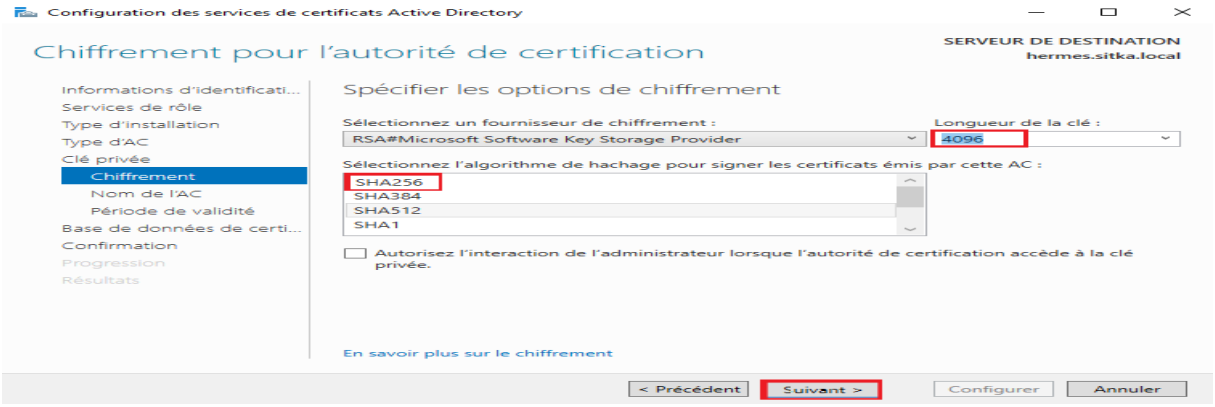
Ce type d'autorité de certification couplé avec un Active Directory est utile pour un intranet mais est déconseillée pour un accès public. Puisque notre autorité n'est pas listée parmi les autorités de certification de confiance, les personnes utilisant des certificats émis par notre autorité de certification auront un avertissement mentionnant que nos certificats ne sont pas de confiance.



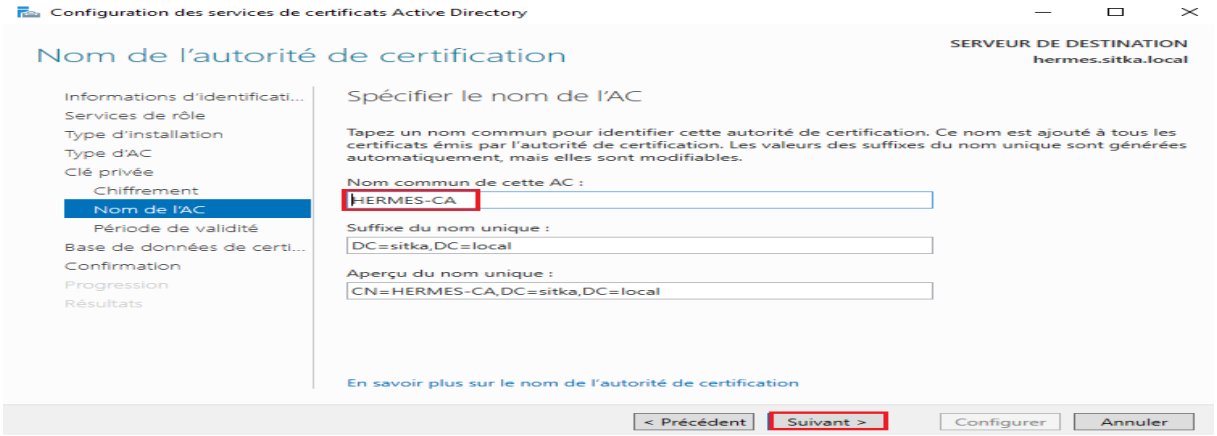
On choisit de créer une clé privée



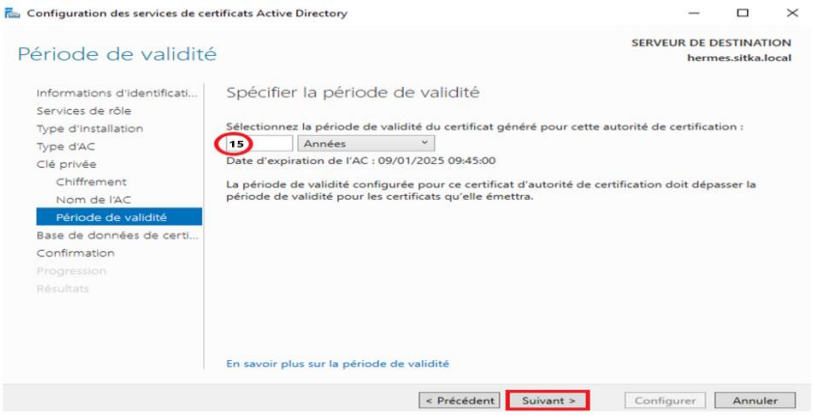
On choisit nos clés de chiffrage, plus les clés sont longues plus la sécurité est renforcée mais malheureusement les performances vont être impactées.



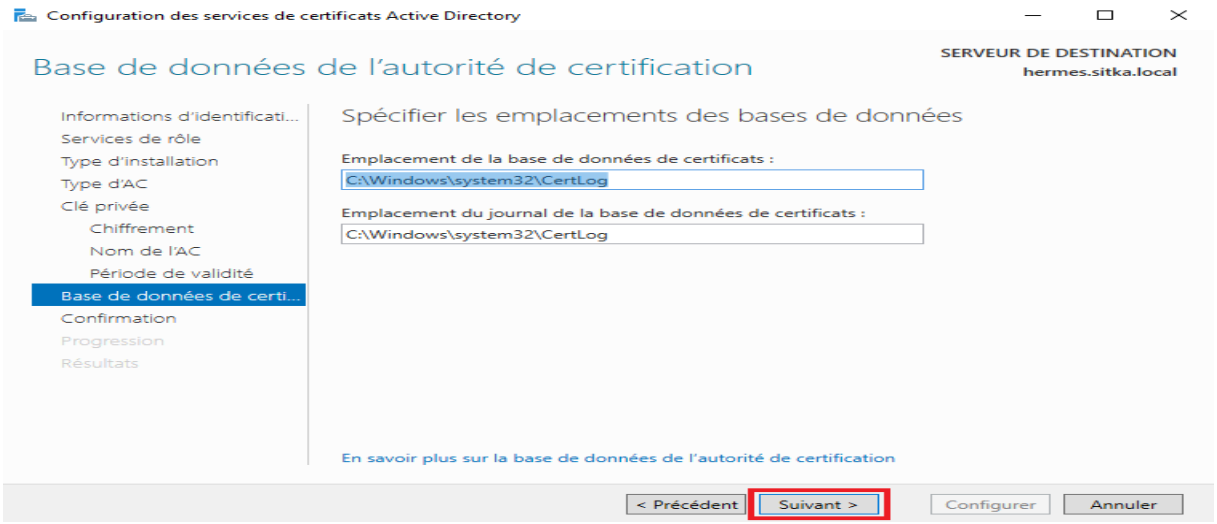
On peut modifier les valeurs par défaut ; je choisis hermes-CA comme nom commun de ACR



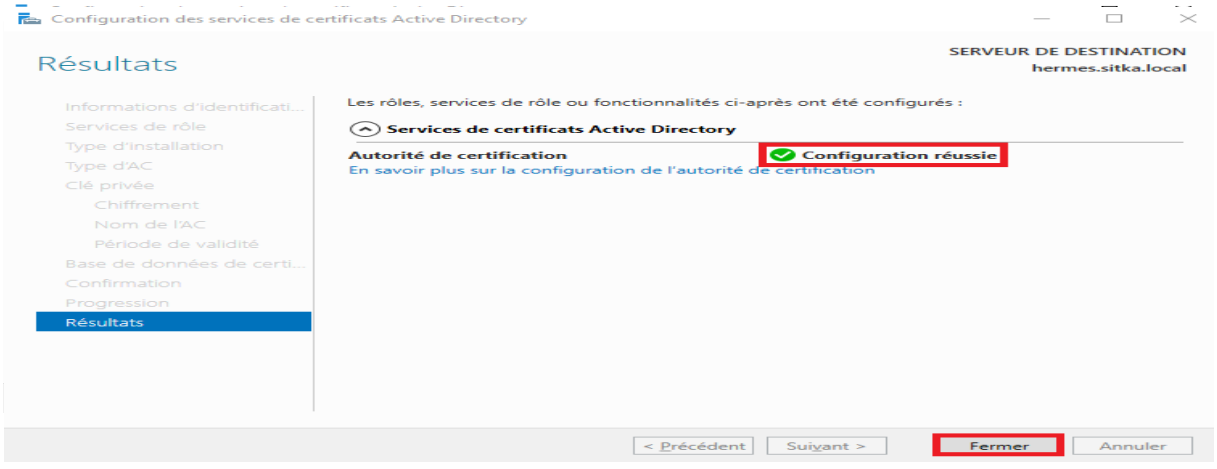
On rentre le période de validité pour le certificat de l'ACR., la période de validité du certificat de l'autorité de certification doit dépasser la période de validité des certificats émis.



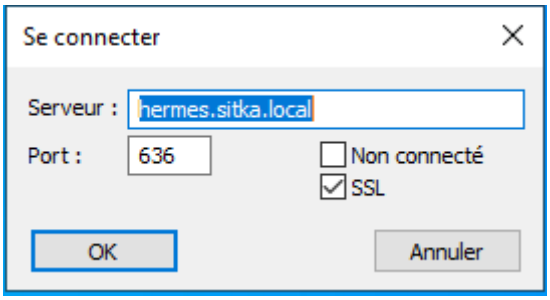
On laisse les dossiers des bases de données et des logs, par défaut.

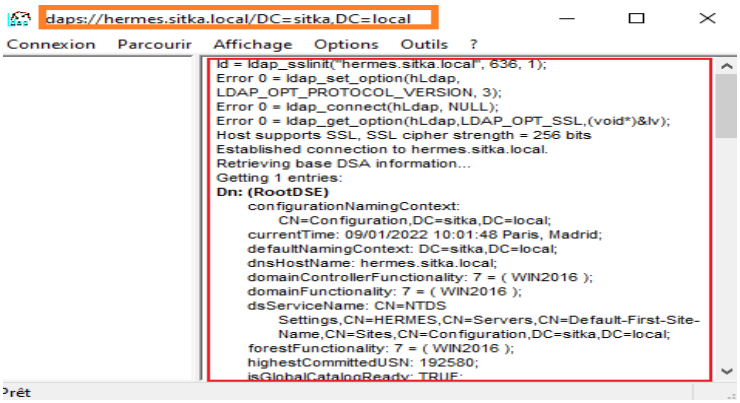


L'assistant nous affiche un résumé de la configuration choisit, on lance ensuite le processus de Configuration
On doit obtenir le message configuration réussie



On reteste maintenant notre connexion LDAPS à partir de l'explorateur LDAP
La connexion sécurisée utilisant le **ssl** sur le port **636** à la base d'annuaire fonctionne on peut identifier les partitions d'annuaire



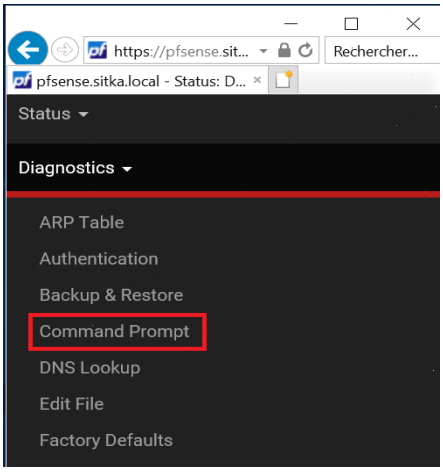


B- Test de la connectivité LDAP et LDAP (LDAP sur SSL) sur heimdall (pfsense)

Sur pfsense on test la connexion de pfsense à la base d'annuaire du controleur de domaine en tapant la commande suivante soit en ssh ou derectement sur pfsense:

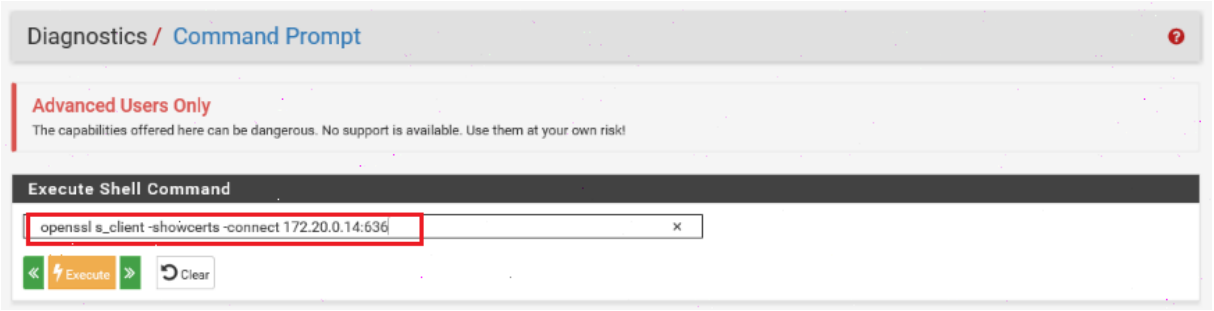
```
# openssl s_client -showcerts -connect 172.20.0.14:636 |less
```

On peut faire la meme chose sur l'interface web de pfsense pour tester la connexion de pfsense à la base d'annuaire du controleur de domaine, donc on va sur **Diagnostics** + **Command Prompt**

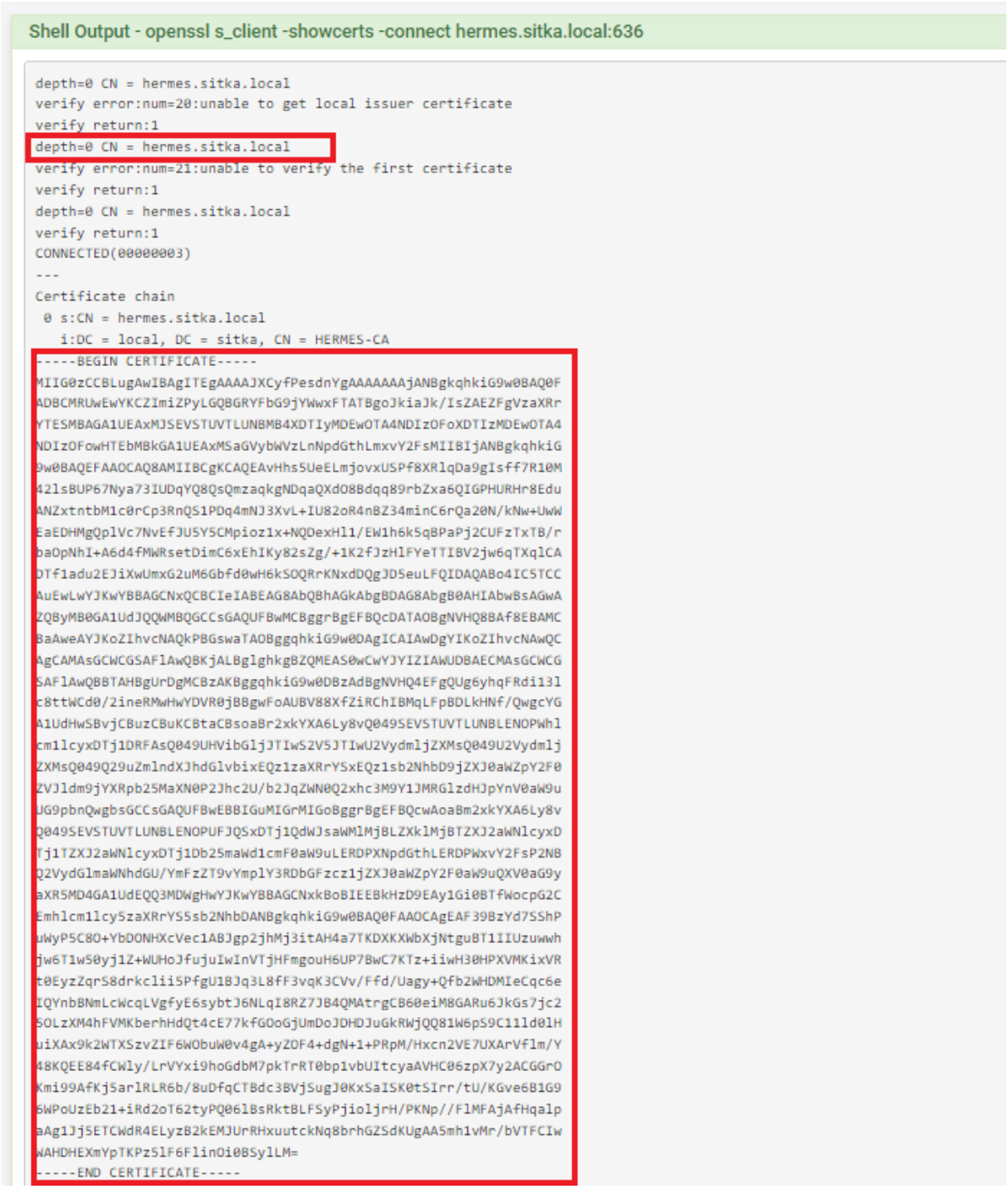


On tape la commande suivante :

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



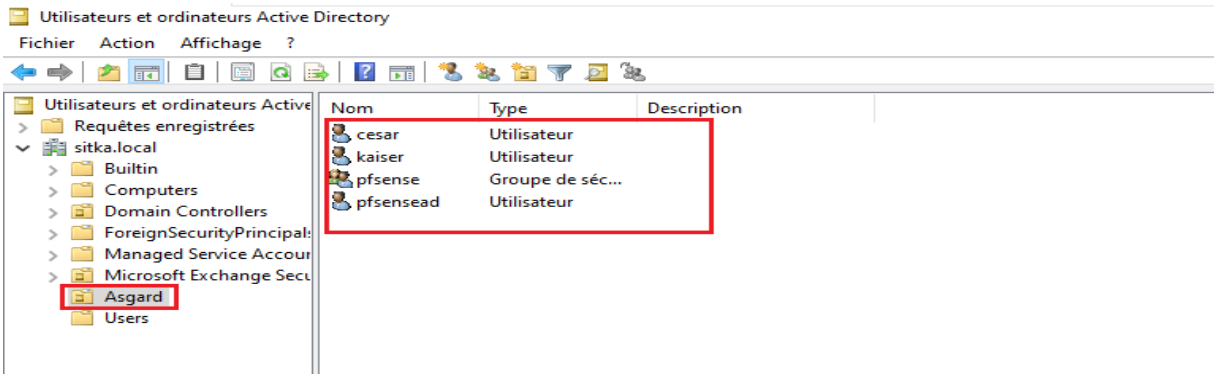
Le contrôleur de domaine nous envoie le certificat qu'il utilise pour appliquer le ssl



C- Création des comptes utilisateurs sur le contrôleur de domaine

Sur le contrôleur de domaine je crée :

- Un groupe **pfsense**
- Un utilisateur **kaiser** faisant partie du groupe **pfsense**
- Un utilisateur **cesar** faisant partie du groupe **pfsense**
- Un utilisateur **pfsensead** faisant partie du groupe **pfsense** et qui va servir de faire la liaison entre pfsense et le contrôleur de domaine



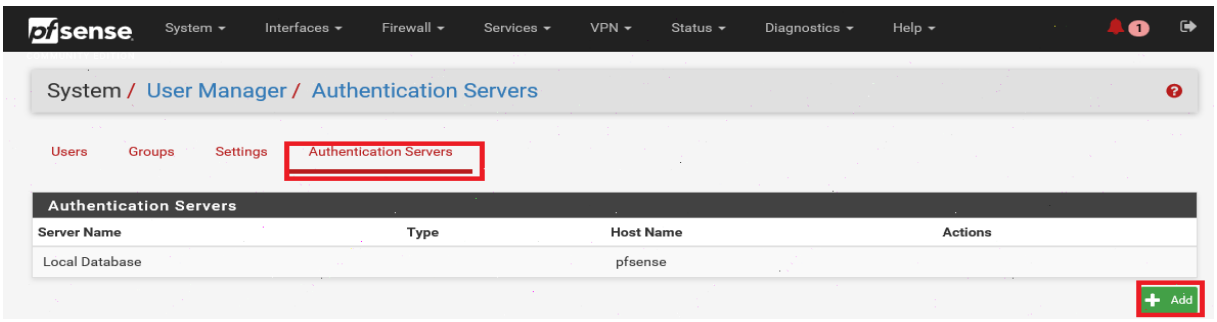
D- Création des authentifications LDAP et LDAPS sur le serveur pfsense

Sur pfsense il existe déjà une base locale permettant l'authentification des utilisateurs.
On va utiliser deux autres méthodes qui permettrons l'authentification en utilisant LDAP et LDAPS

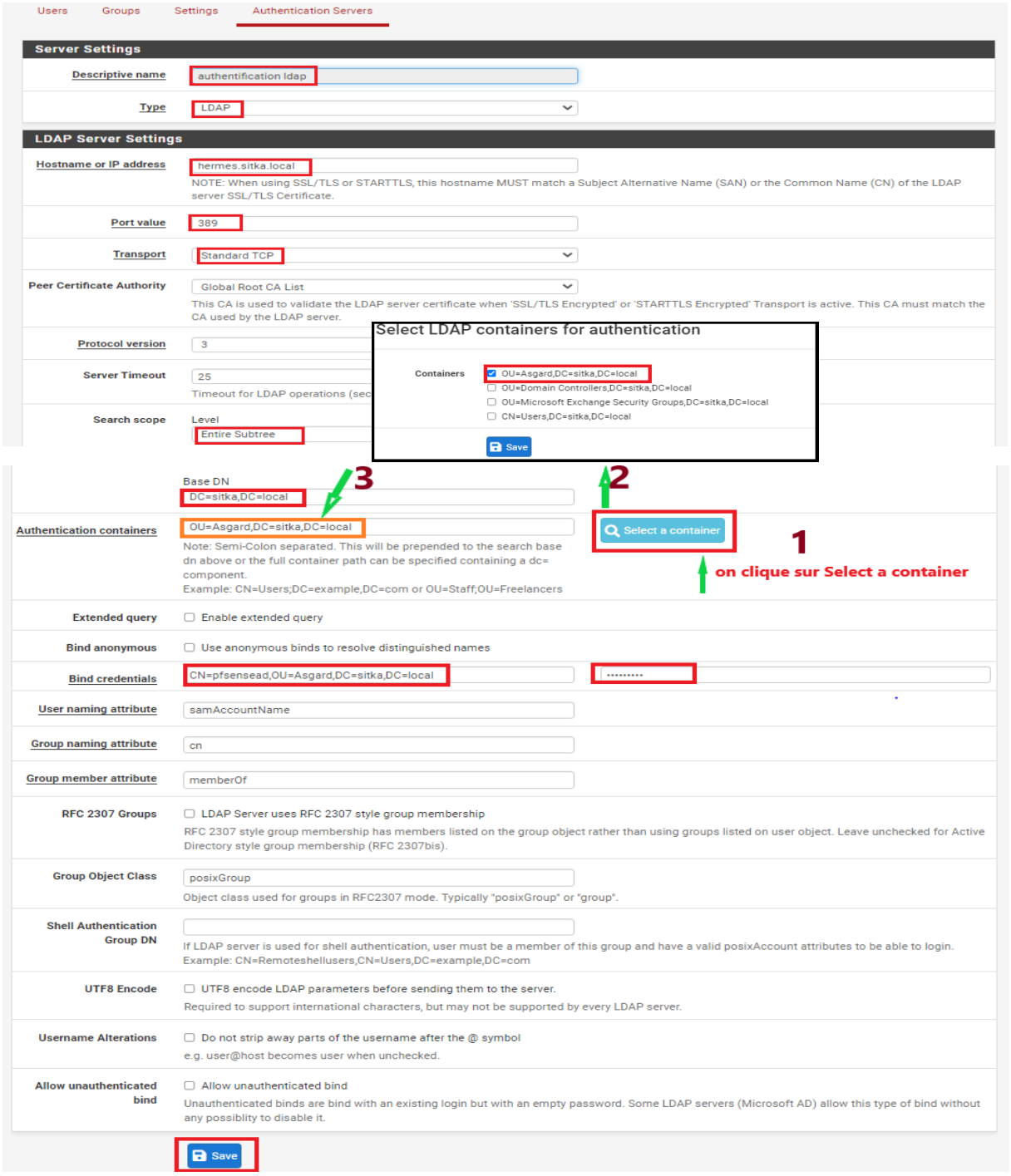
1- Création de l'authentifications LDAP

Maintenant on va créer une authentification LDAP sur pfsense à partir l'interface web on va sur System / User Manager / Authentication Servers

Et on clique sur + Add pour rajouter une authentification Servers

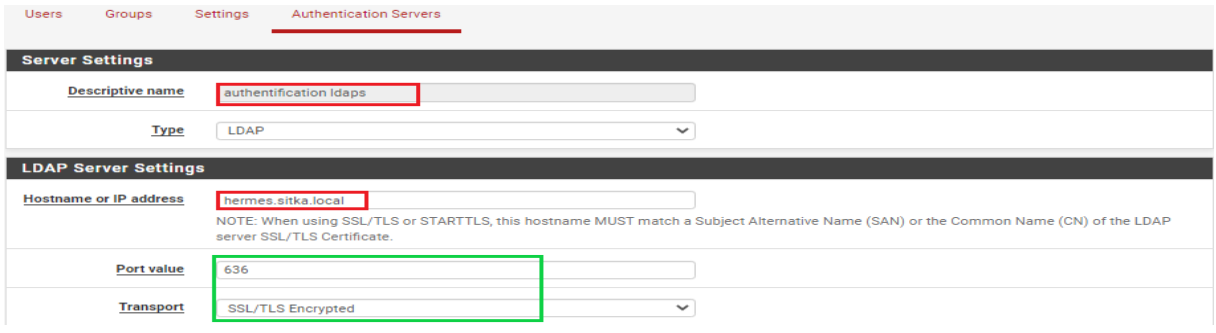


On remplit Les champs comme indiqué ci-dessous, les étapes 1,2 et 3 il faut les exécuter à la fin de notre procédure les faires : on tape cn dans le champ **Authentification containers** puis on clique sur **select a container**



2- **Création de l'authentifications LDAPS**

a- Création du formulaire de l'authentification LDAPS



Même procédure que l'authentification LDAP sauf pour les champs encadrés en **vert** on fait le choix de **SSL/TLS** et en utilise le port **636**

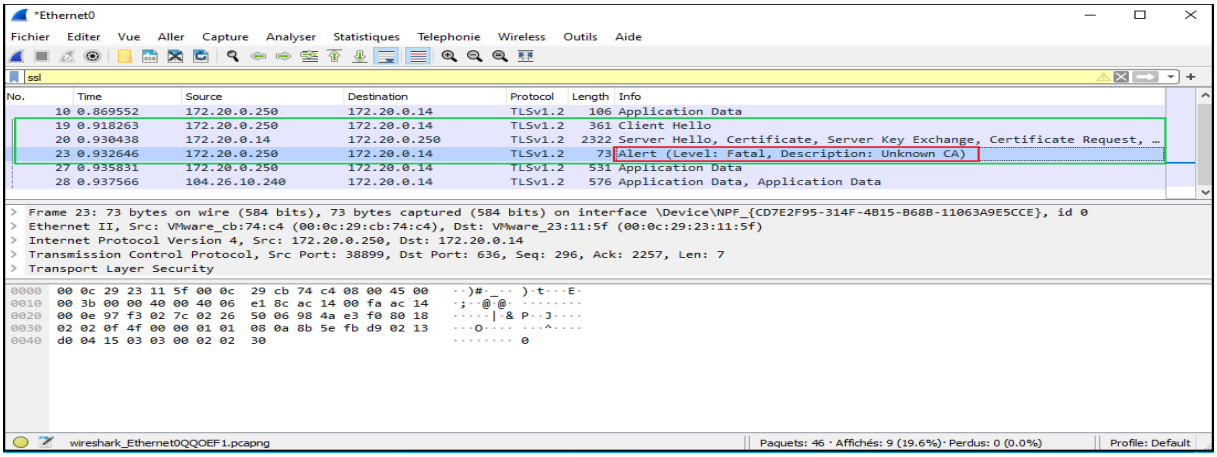
Dans **authentification containers** on tape cn puis on clique sur Select a container

La boite de dialogue qui nous permet de choisir l'OU qui héberge nos utilisateurs ne s'ouvre pas en plus on a un message d'erreur qui apparait en bas de la page

b- Analyse avec Wire Shark du trafic pfsense active directory

Donc l'authentification LDAPS ne fonctionne pas, on va essayer de faire un diagnostic en faisant une capture de trames avec Wire Shark pour identifier le problème.
On installe Wire Shark sur notre contrôleur de domaine, puis on déclenche une capture de trame en même temps on exécute la manipulation précédente
On fait un filtre ssl/tls dans notre capture de trame
Les trames qui représentent l'échange entre pfsense et le contrôleur de domaine sont encadrée en vert :

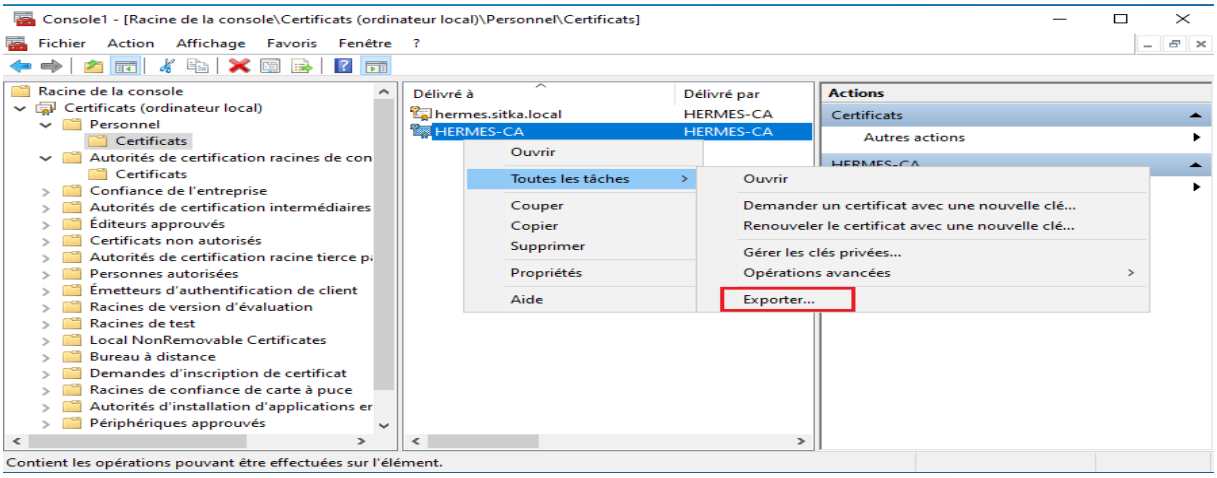
- Le dialogue commence par **client hello** la source est pfsense destination le hermes
- Hermes répond par **server hello** et présente son certificat à pfsense
- Pefsense répond par une alerte il ne reconnait pas le certificat



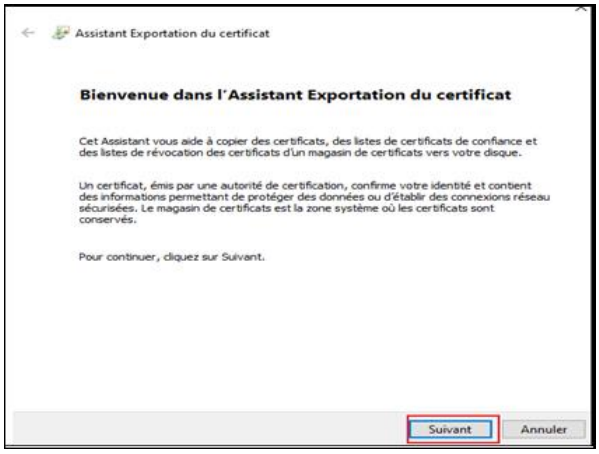
Donc le souci vient du fait que le certificat présenté par Hermes n'est pas reconnu par pfsense **pour contourner ce problème on va importer le certificat de l'autorité de certification racine installée sur hermes sur notre serveur pfsense.**

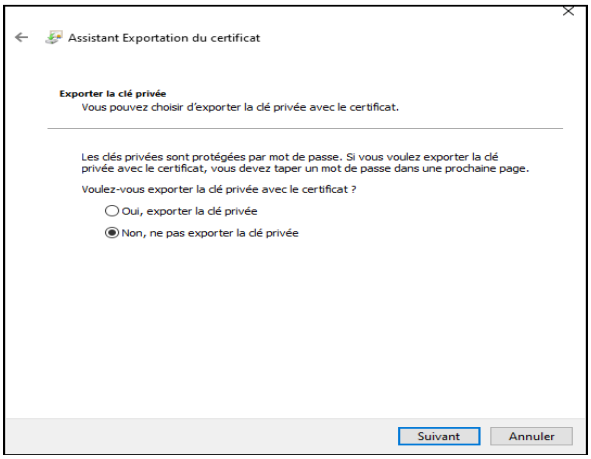
c- Exportation du certificat de l'autorité de certification hermes

- On ouvre une console mmc et on rajout Ajouter/Supprimer un composant logiciel enfichable... le composant certificat pour ordinateur
- On exporter le certificat de l'autorité de certification racine au format '.cer' on l'enregistre avec le nom qu'on choisit

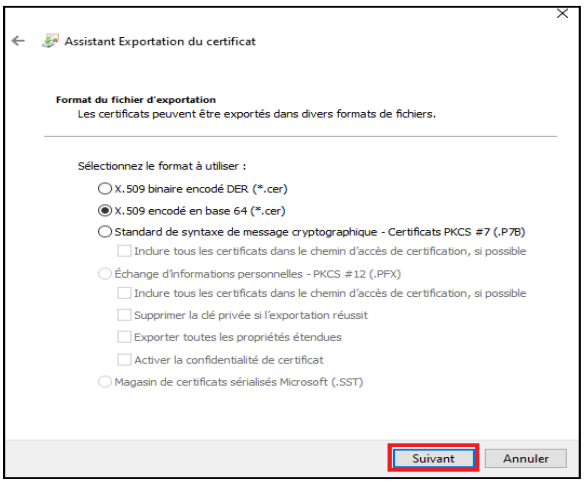


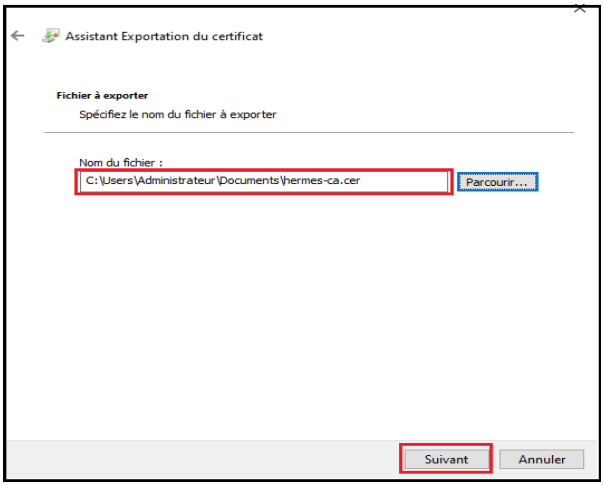
On choisit de ne pas exporter la clé privée



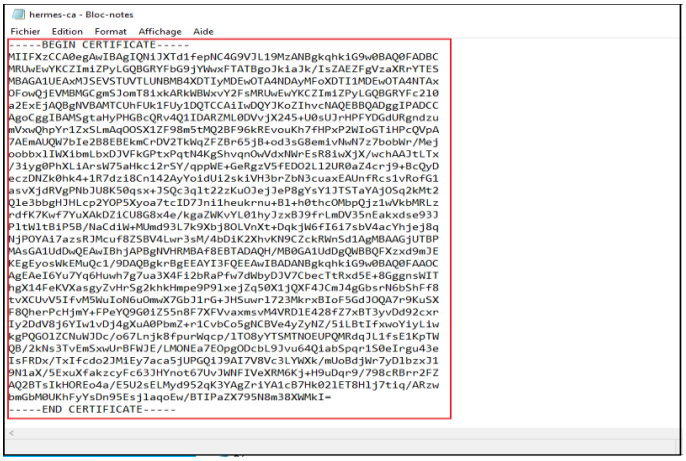


On choisit le format **X.509 encodé DER (*.cer)** et en l'enregistre avec le nom hermed-ca.cer



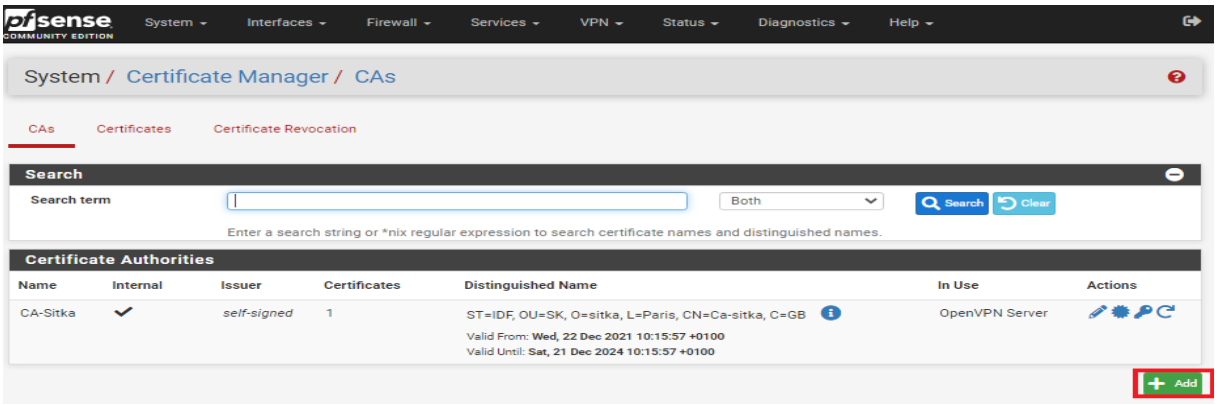


- J’ouvre mon fichier hermes-ca.cer avec le bloc note pour afficher le certificat de l’autorité de certification après on le copie pour l’insérer dans pfsense



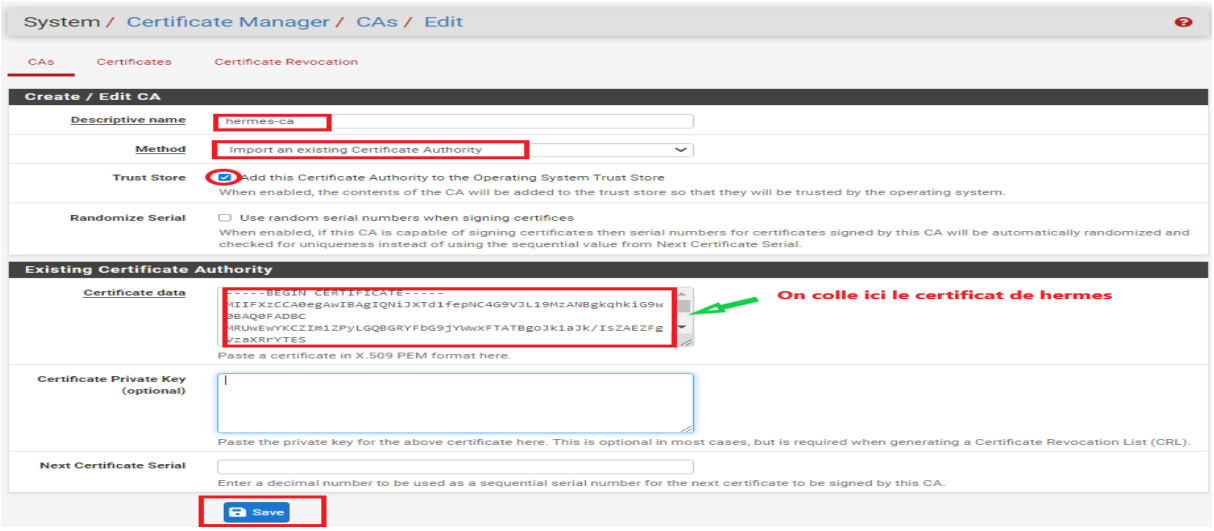
d- Importation du certificat de l’autorité de certification racine

On va sur **cerificate manager + Cas** on clique sur ad pour rajouter une autorité de certification



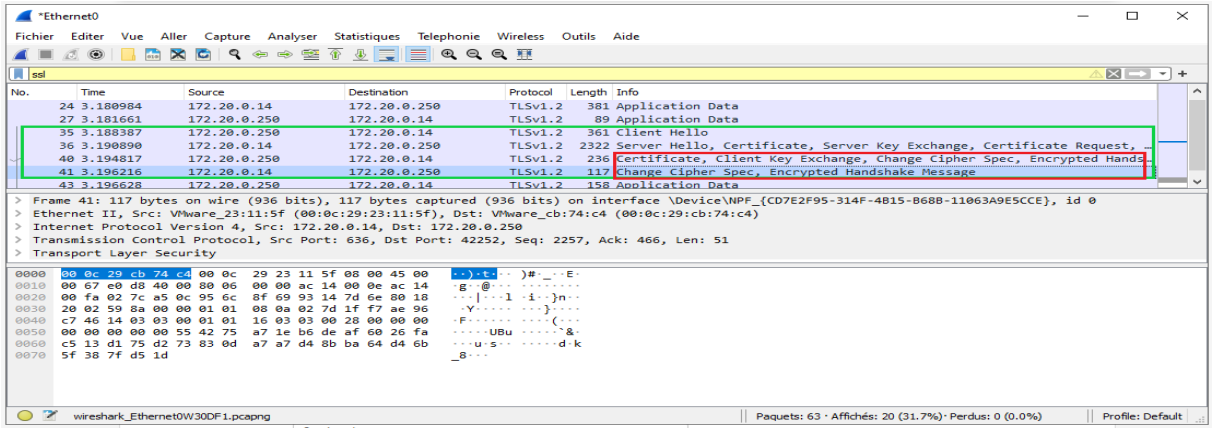
On donne un nom à notre autorité de certification et on choisit comme méthode **import an existing Certificate Autority**

Apres il suffit de coller le certificat de l’autorité de certification racine hermes dans le champ **certificate data**



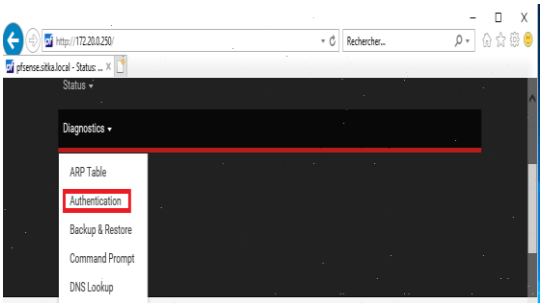
e- Test de la connexion ssl entre pfsense et le contrôleur de domaine

On constate qu'il n'y'a plus de messages d'erreurs que le message handshake (poignée de main) est établie et crypté on peut maintenant revenir pour terminer de remplir notre formulaire authentification LDAPS



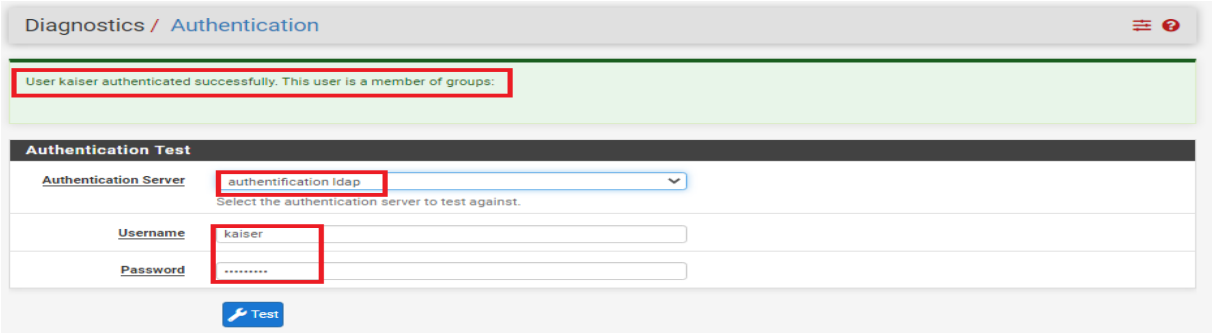
3- **Utilisation des authentifications LDAP et LDAPS sur le serveur pfsense**

Je vérifie l'authentification Active directory de mon compte **kaiser** à partir de l'interface web de pfsense, on va sur diagnostic + authentification

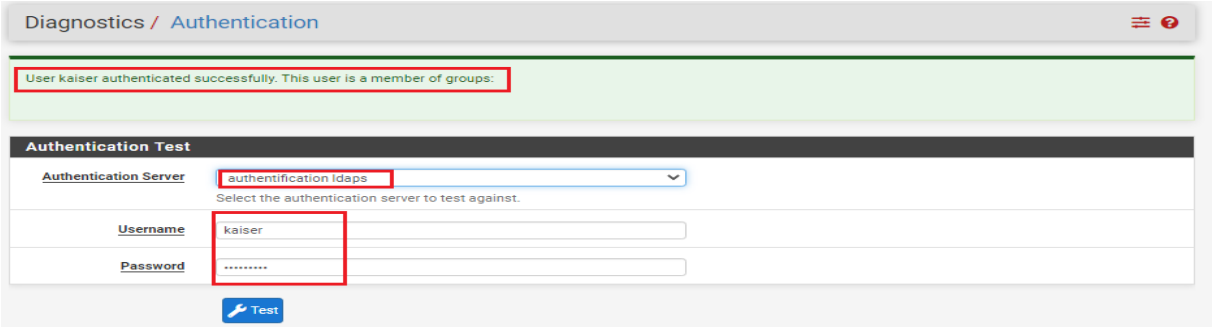


a- Vérification de l'authentification LDAP et LDAPS

- L'authentification Active directory en utilisant LDAP a réussit

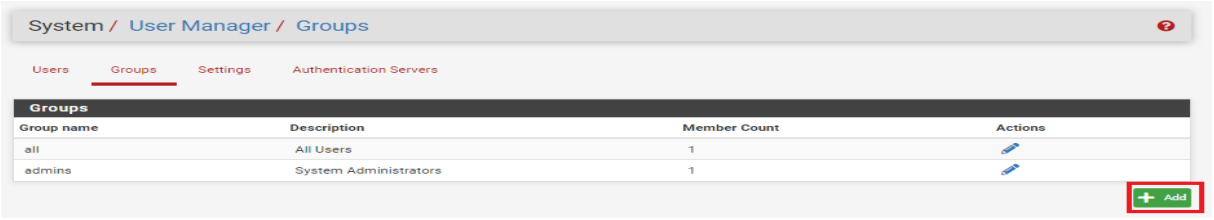


- L'authentification Active directory en utilisant LDAPS a réussit

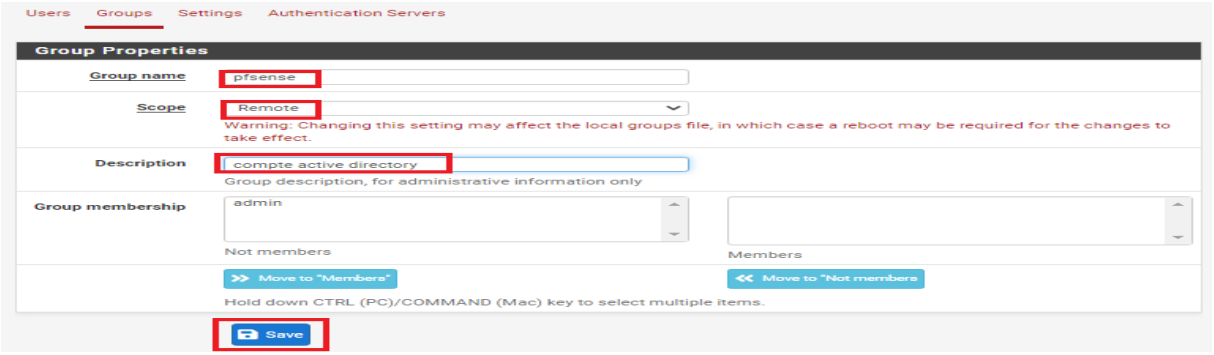


b- Configuration des groupes et des utilisateurs sur pfsense

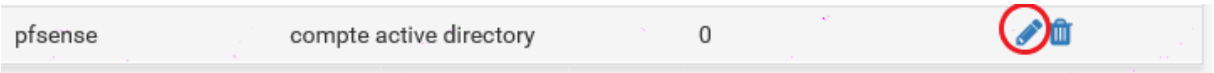
On crée un groupe de même nom que celui crée sur active directory le groupe **pfsense** on clique sur **add** pour rajouter un groupe



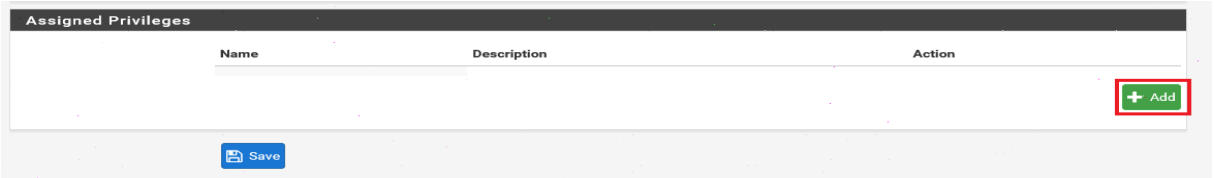
On remplit les champs comme indiqué ci-dessous puis on sauvegarde



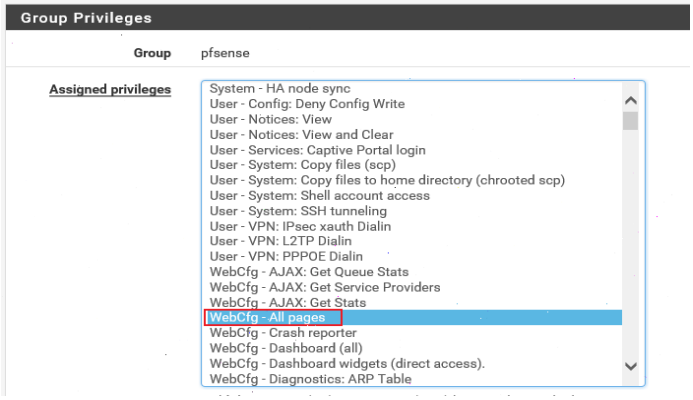
Dès que le groupe est créé je l'édite pour lui donner les droits admin



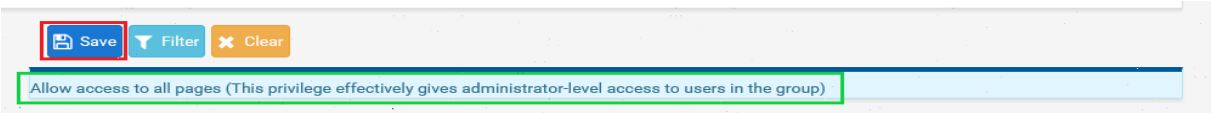
Dans assigned Privilèges je clique sur add



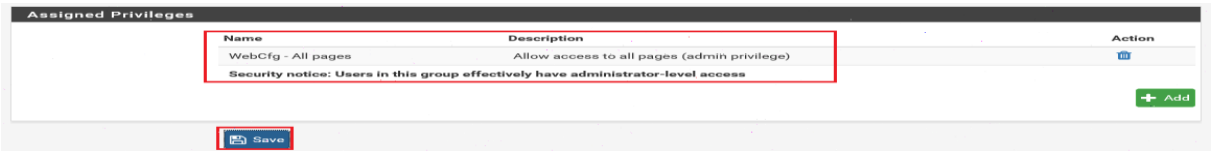
Je sélectionne **WebCfg – All pages** comme droit



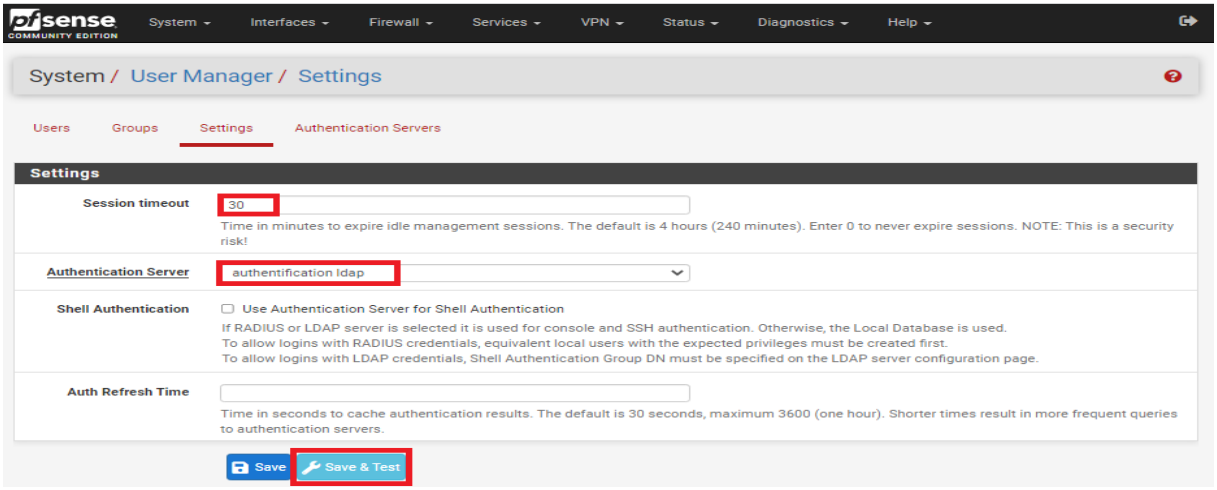
On remarque le groupe pfsense aura tous les droits



On enregistre notre configuration

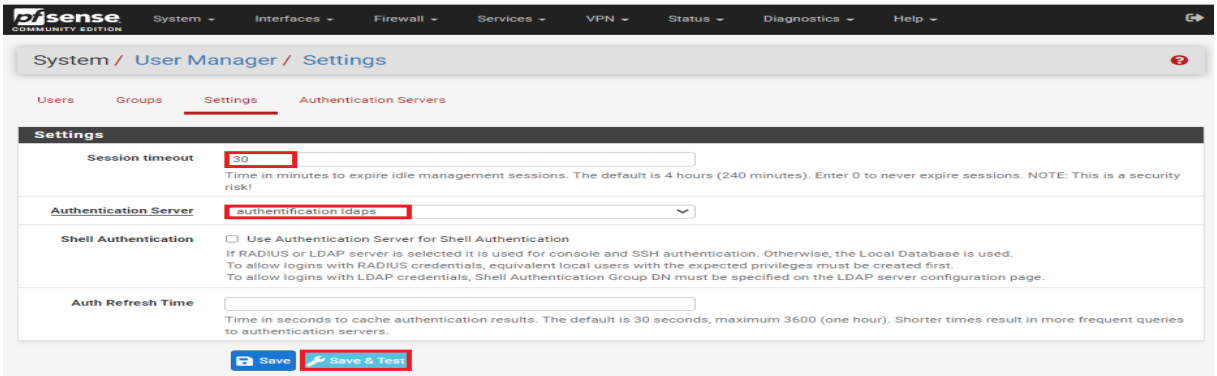


On fait un test de connexion avec la base LDAP



La connexion a réussi

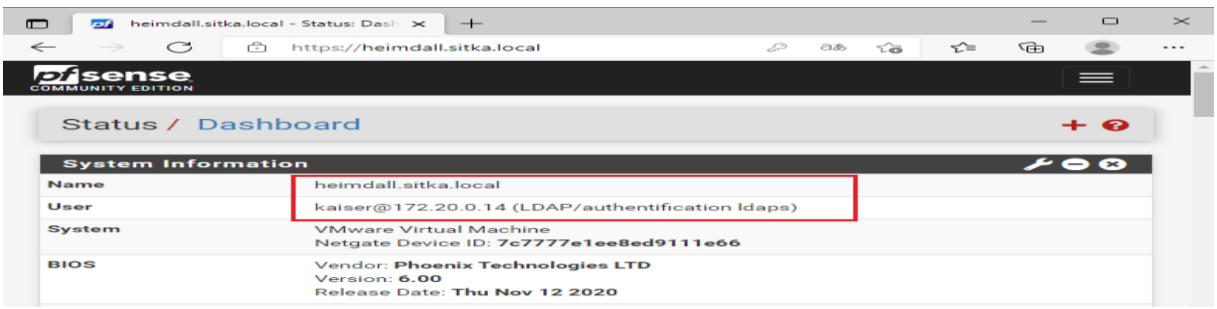
On fait un test de connexion avec la base LDAPS



La connexion a réussi

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

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



1- Introduction
2- Activation du portail captive
3- Configuration du DHCP
4- Création des règles sur le firewall
5- Test de notre portail captive

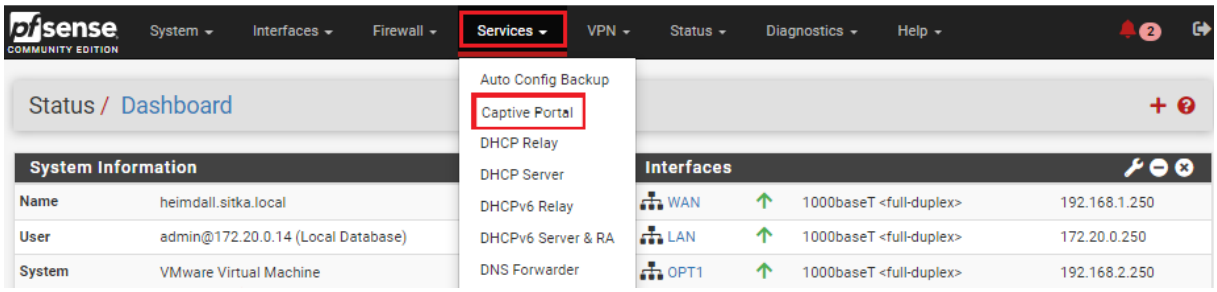
1- Introduction

Le portail captif est un moyen qui force les clients d'un réseau de passer par une page Web d'authentification pour pouvoir se connecter à Internet.

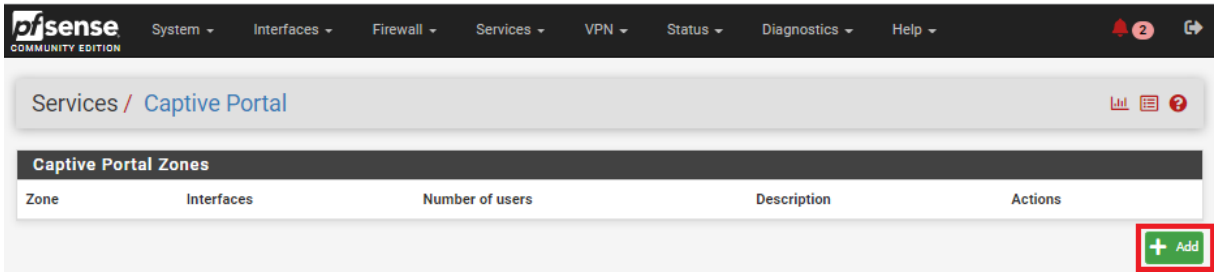
Il est utilisé dans des réseaux assurant un accès public comme certain espace de la SNCF, les hôtels, les établissement scolaires …

2- Activation du portail captive

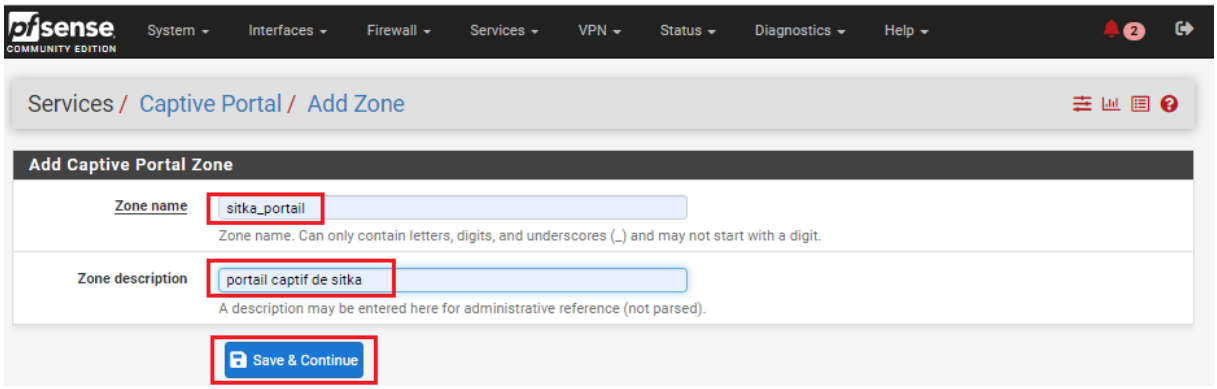
On se connecte sur l'interface de web de pfsense, après on va sur **Services + Captive Portal**



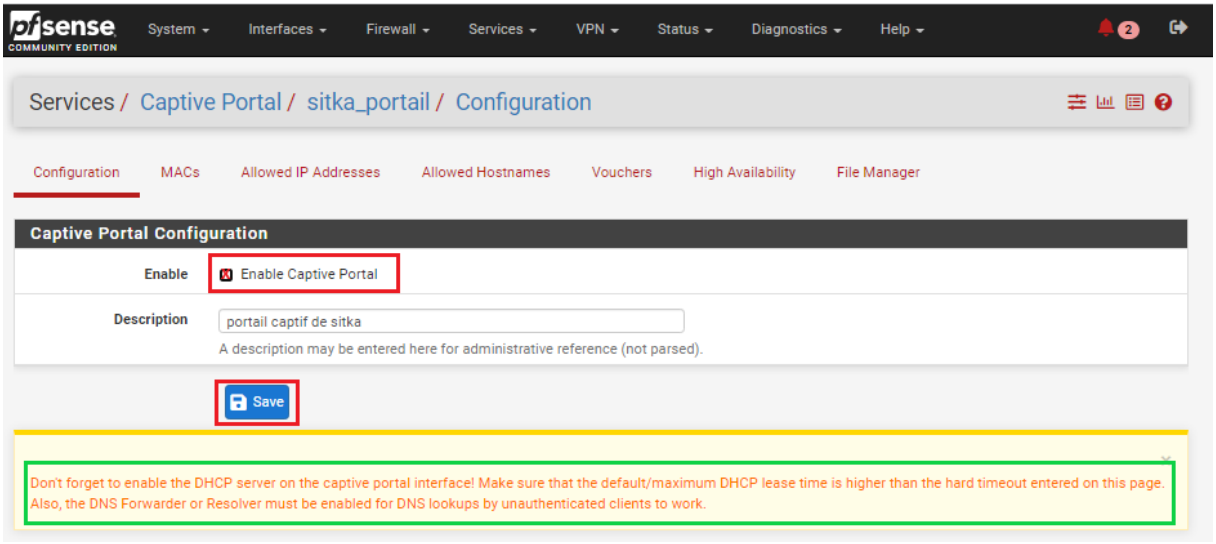
On clique sur **Add**



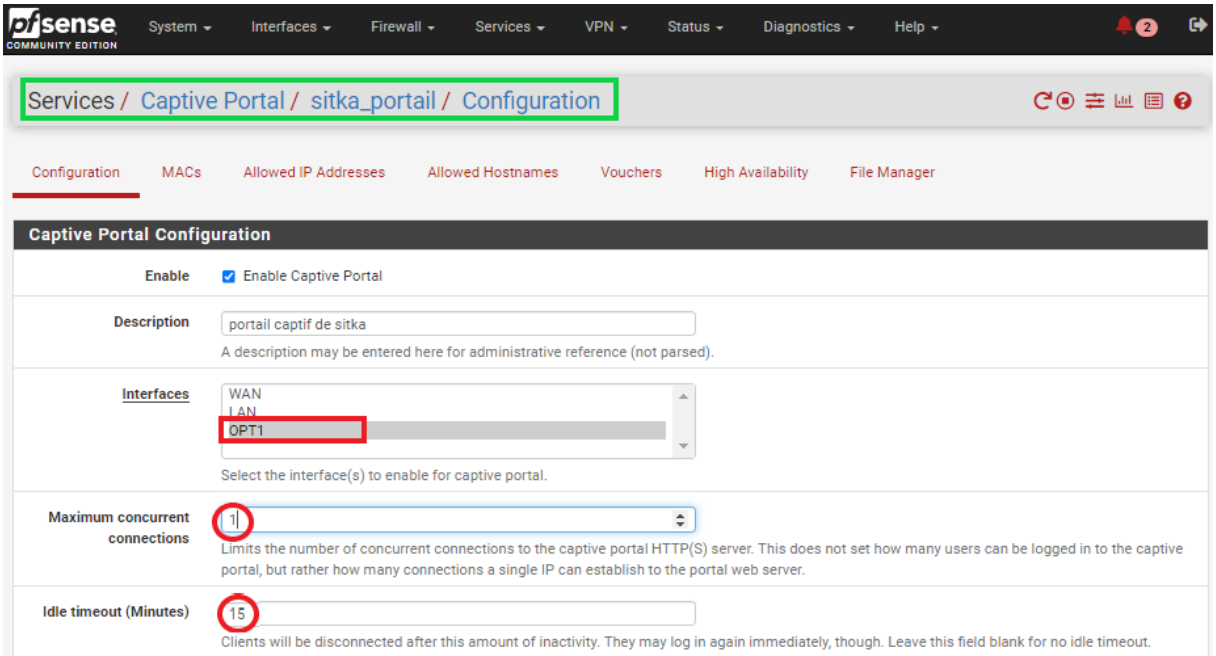
On renseigner le Nom du Portail Captif et sa description :
Sitka_portal pour le nom de la zone
Portail captive sitka pour la description de la zone



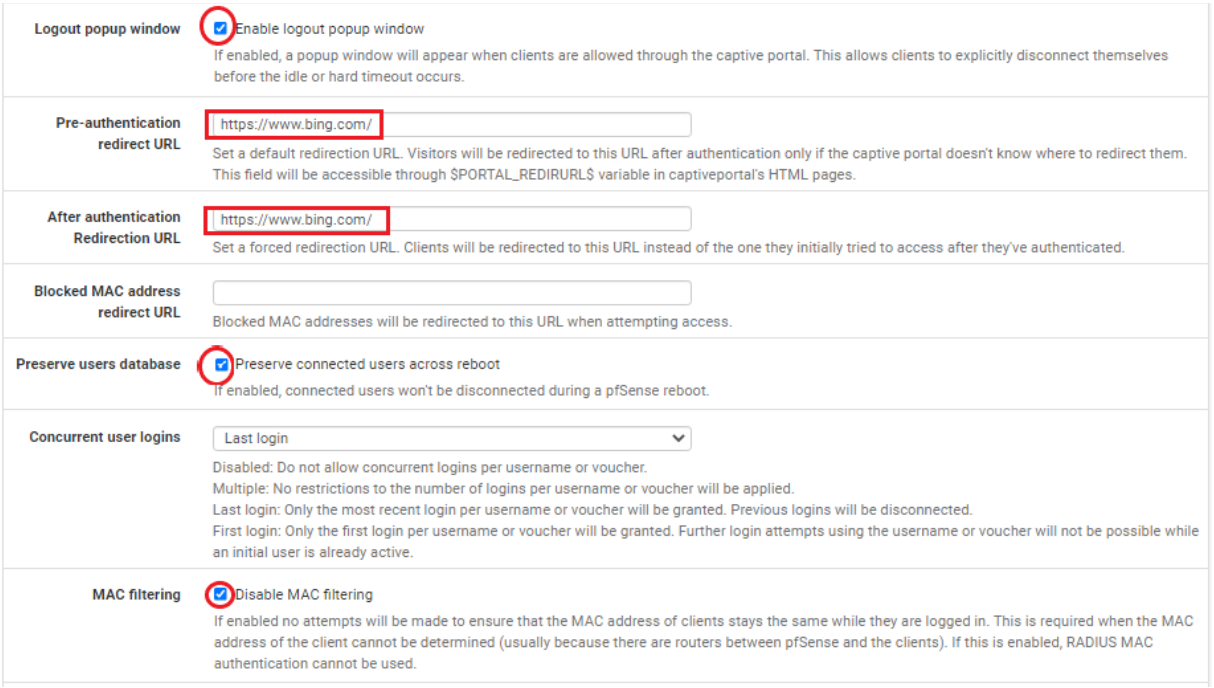
On active le portail et on enregistre



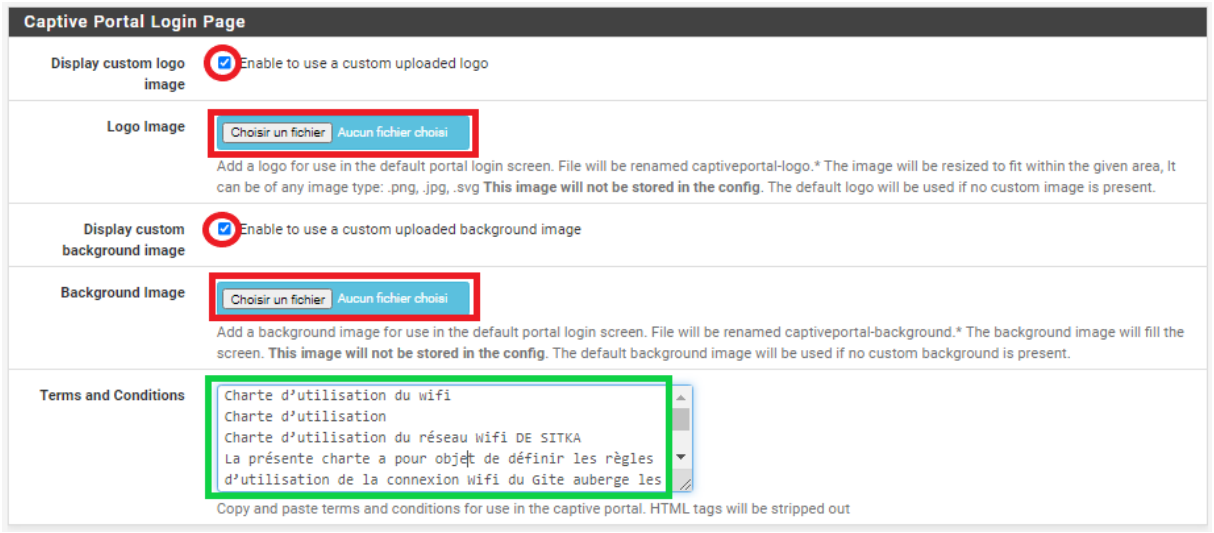
- On active **Enable Captive Portal**
- On sélectionne l'interface **Opt1**
- Maximum concurrent connections : **1** (Limite le nombre de connexions simultanées d'un même utilisateur)
- Idle timeout (Minutes) on choisit **15**:(Les clients seront déconnectés après cette période d'inactivité)



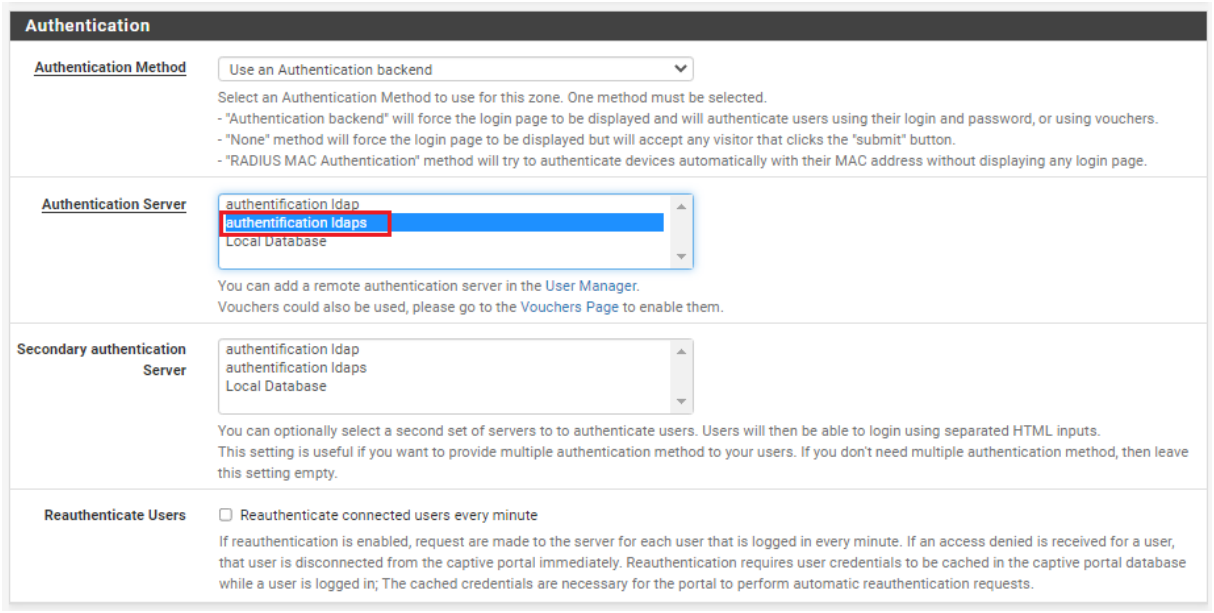
- Définir **After authentication Redirection URL** (**URL HTTP** de redirection Les clients seront redirigés vers cette URL au lieu de celle à laquelle ils ont tenté d'accéder après s'être authentifiés)
- Activer **Disable Concurrent user logins** (seule la connexion la plus récente par nom d'utilisateur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



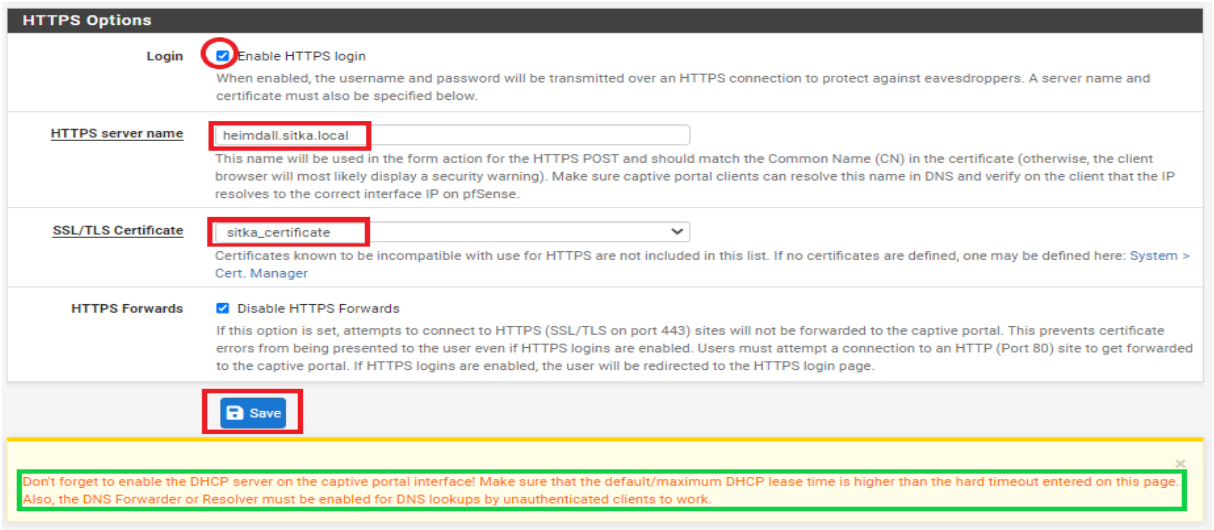
On peut choisir un logo et une image d'arrière-plan ainsi qu'un charte de connexion



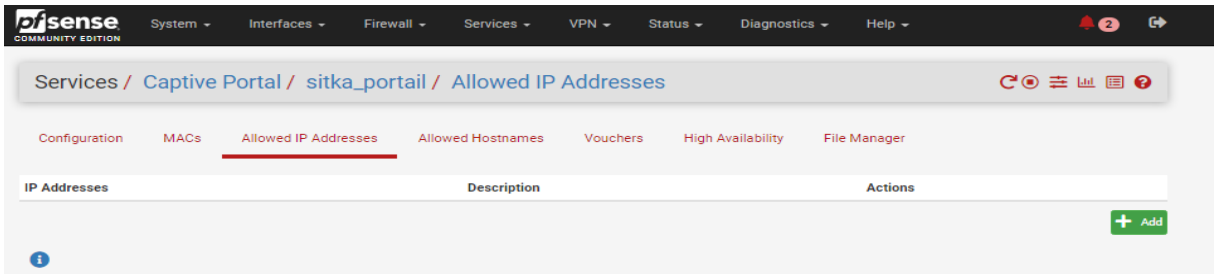
- On sélectionne **Use an Authentication backend**
- On sélectionne **Authentification LDAPS** comme méthode d'authentication

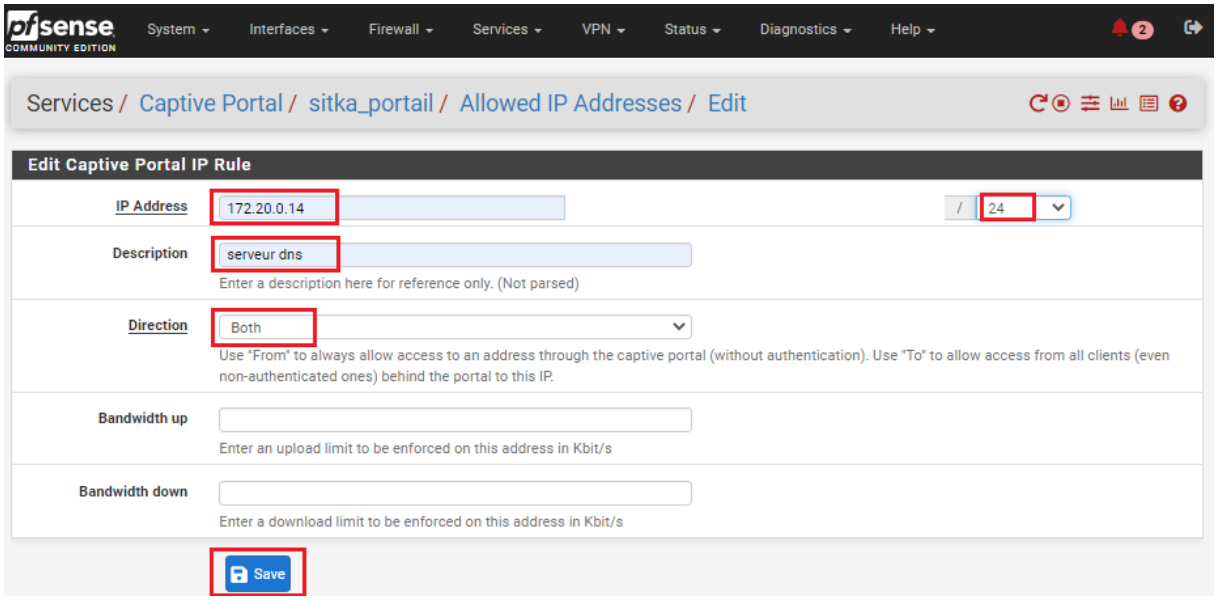


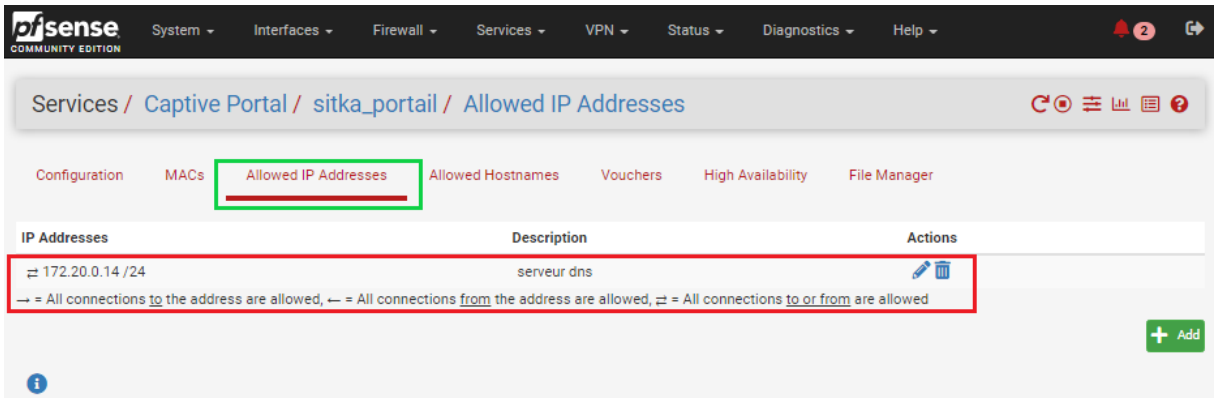
On active ssl pour notre portail active



Les clients ont besoin d'une résolution DNS donc on va autoriser cette résolution en autorisant l'adresse IP du DNS 172.20.0.14

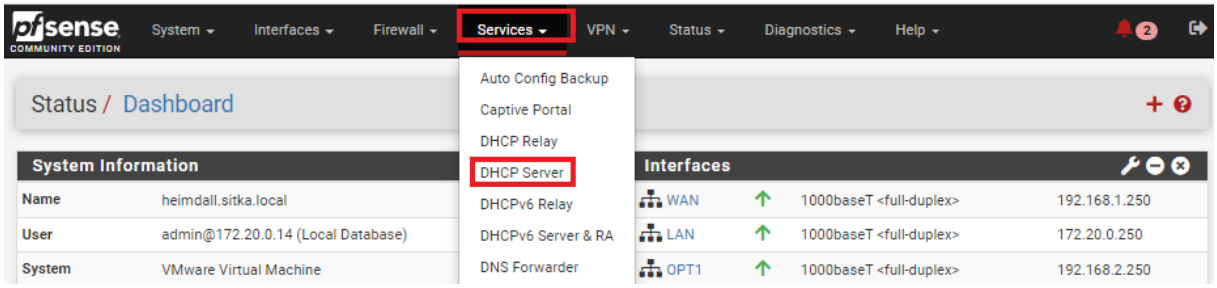




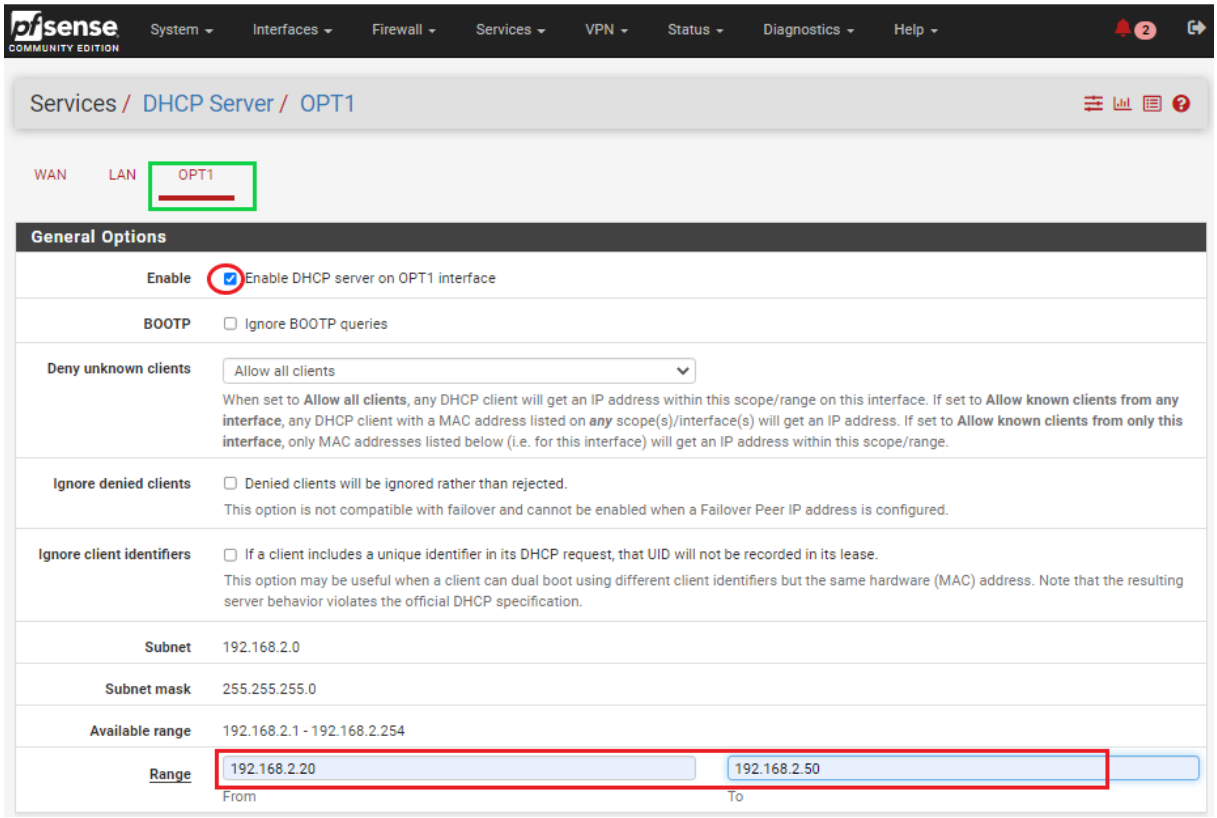


3- Configuration du DHCP

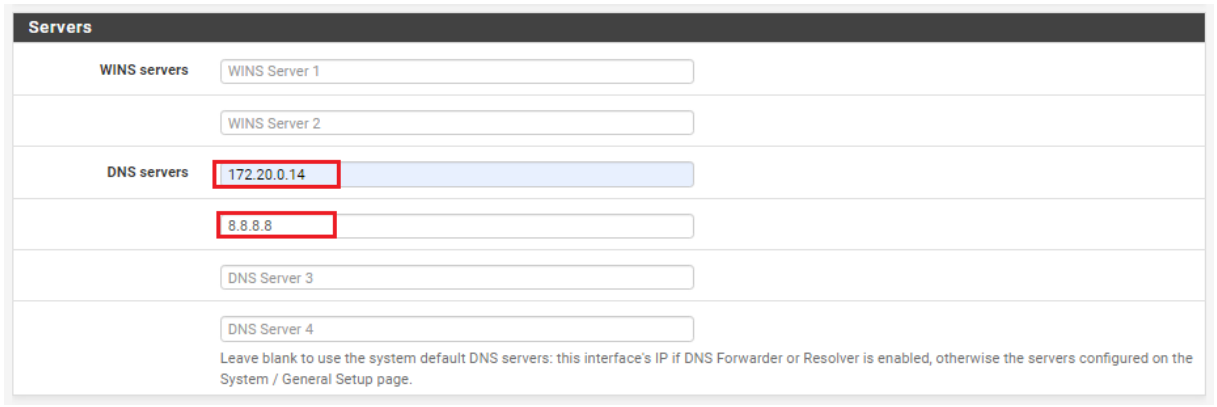
Maintenant On va activer le DHCP sur l'interface opt1



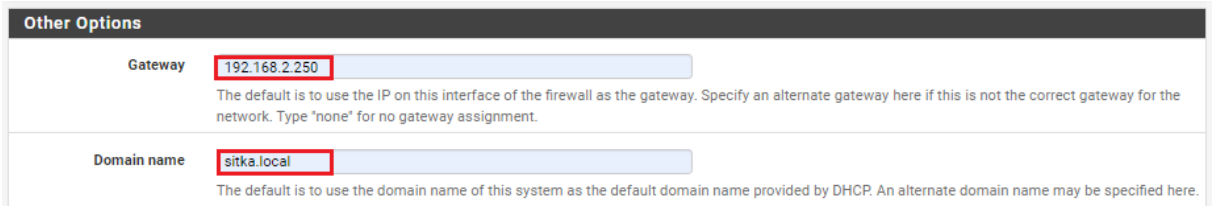
On déclare notre étendue



On rentre l'adresse de notre DNS

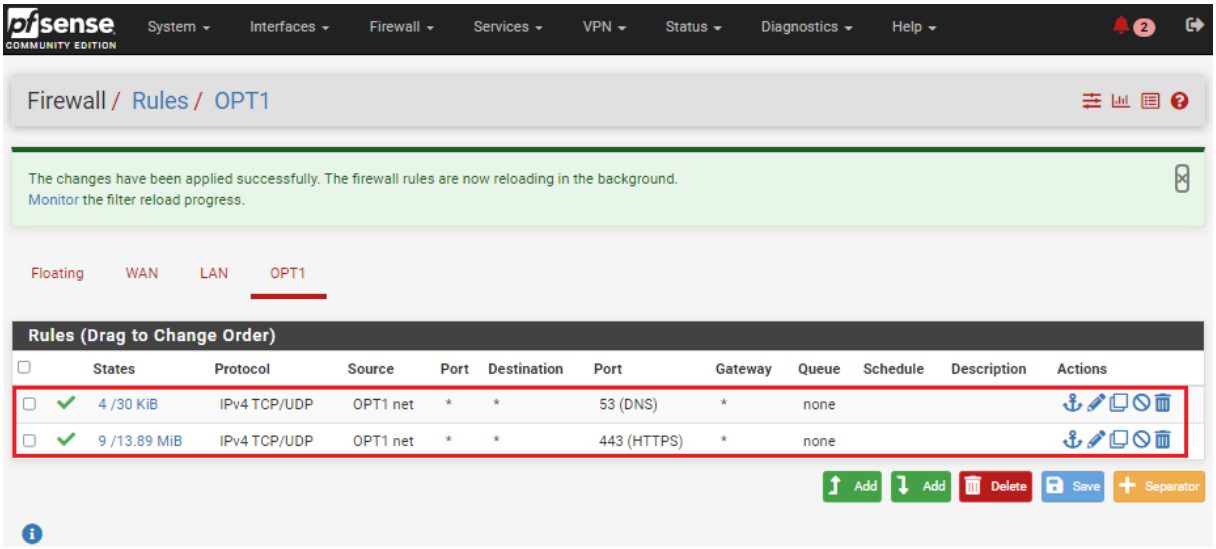


On rentre l’adresse de la passerelle et du nom de domaine



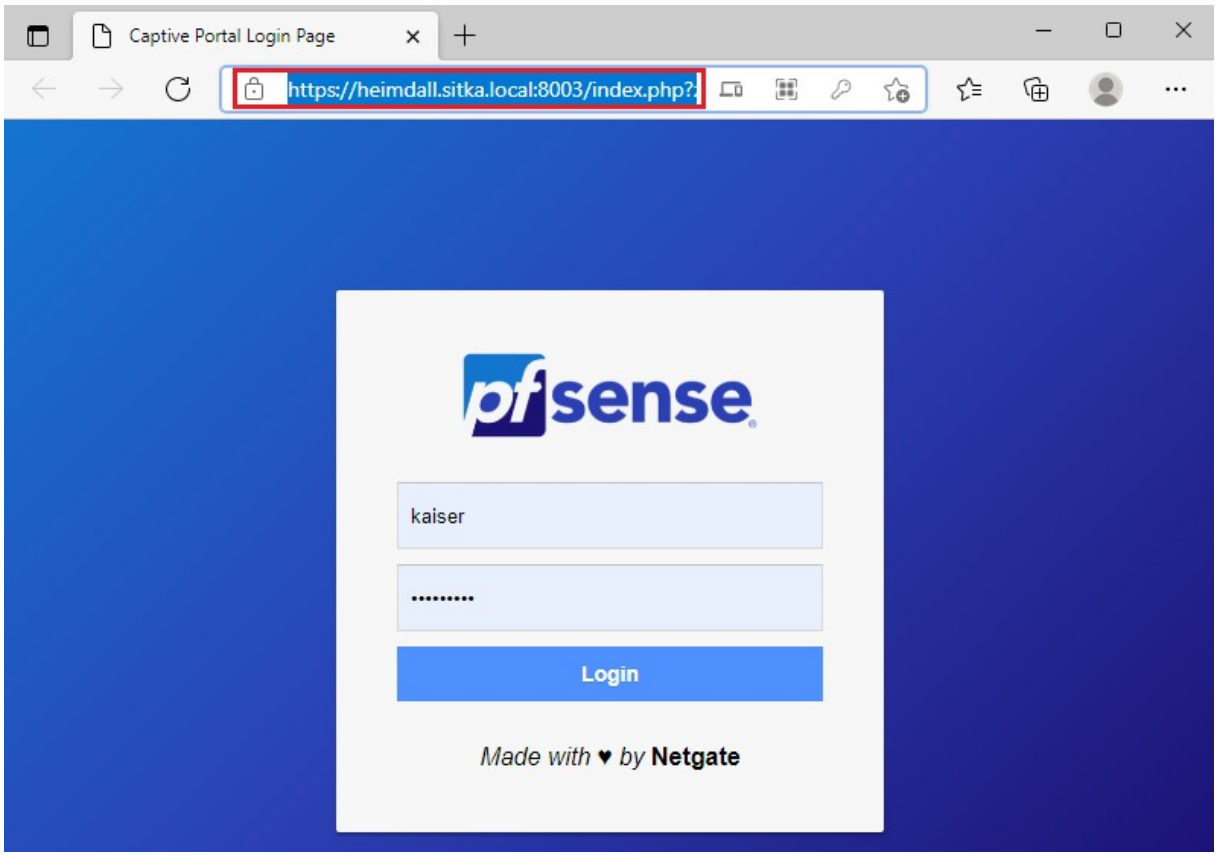
4- Création des règles sur le firewall

On Cree deux règles autorisant le DNS et le https

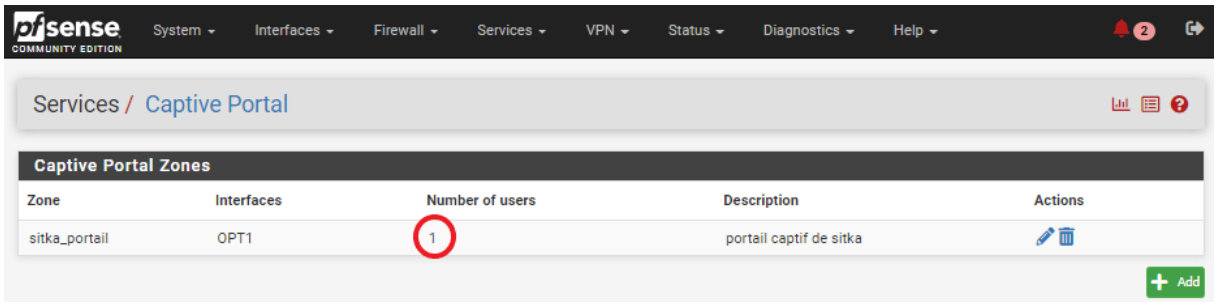


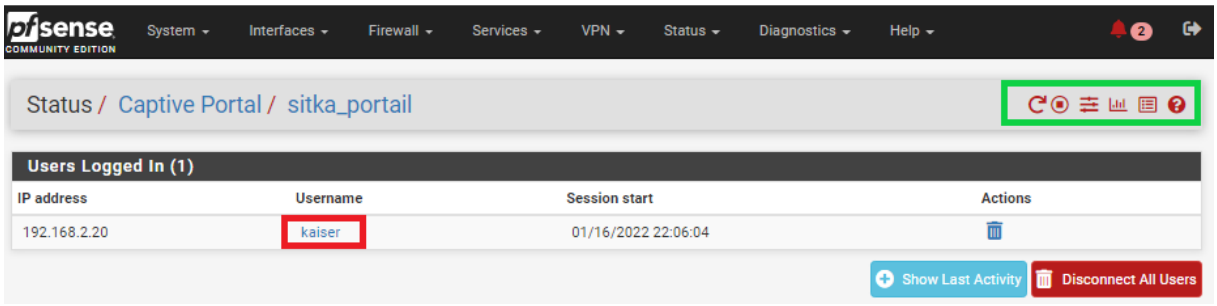
5- Test de notre portail captive

On fait notre test de connexion



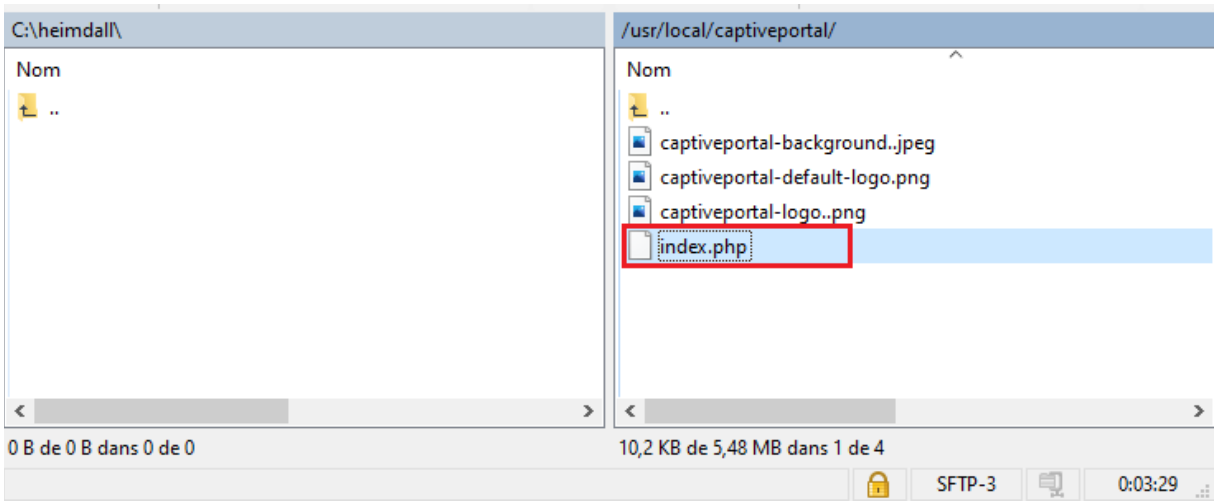
Sur pfsense on peut vérifier les connexions





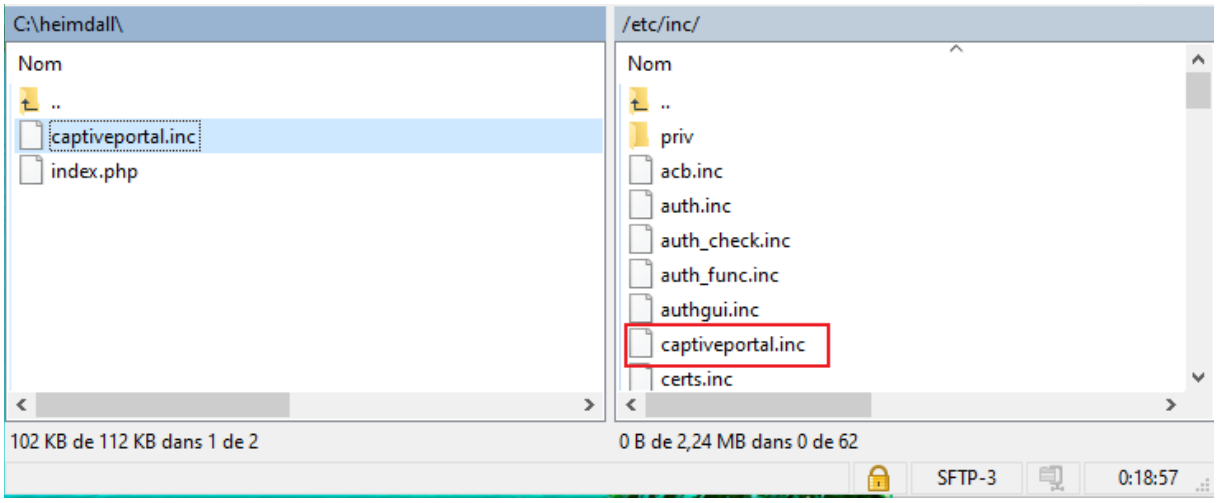
- On chercher **You are connected** et remplacer par **Vous êtes connecté**

- On chercher **Disconnecting...** et **You have been disconnected** et on remplacer par **Déconnexion...** et **Vous êtes déconnecté**
- On cherche **Invalid credentials specified** et on remplace **par Les informations saisies sont invalides,** il y a 2 lignes à modifier
- Après on enregistre les modifications



Maintenant on va sur /etc/inc puis et on ouvre captiveportal.inc

- On chercher Captive Portal login Page et on remplacer par : Portail Captif de sitka
- On chercher Login et Made with ... by ... Netgate et on remplacer par Connexion et Connectez-vous avec votre compte LDAPS
- On chercher User et Password et on Remplace par Utilisateur et Mot de Passe
- On rechercher Logout et Click the button below to disconnect on remplace par **Déconnexion et Cliquez sur le bouton ci-dessous pour vous déconnecter**
- On enregistre les modifications



1- Introduction
2- Création d'un compte dans Snort
3- Installation de Snort
4- Configuration de Snort
5- Test d'intrusion

1- Introduction

Dans cette partie consacrée à Pfsense on va voir comment installer le package Snort sur PfSense, et ainsi un IDS voir même un IPS !

On va d'abord voire un peu ce qu'est un IDS et un IPS et la différence entre eux.

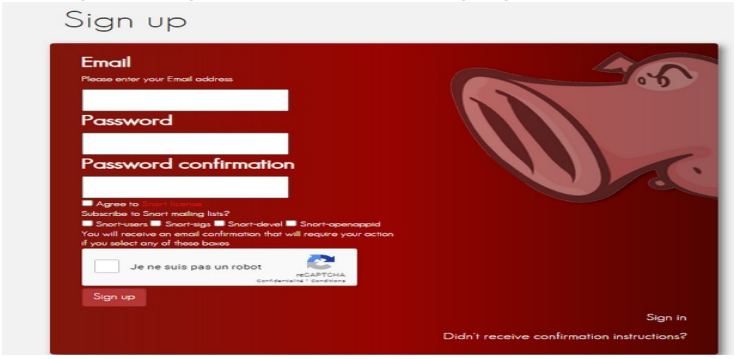
Les IDS (Intrusion Detection Systems) n'a pas comme rôle de bloquer les attaques, IDS utilisent une base de données d'attaques afin de :

- Analyser et surveiller le trafic réseau pour détecter une cyberattaque.
- Détecter les violations de la politique de sécurité,
- Détecter les malwares et les scanners de port.

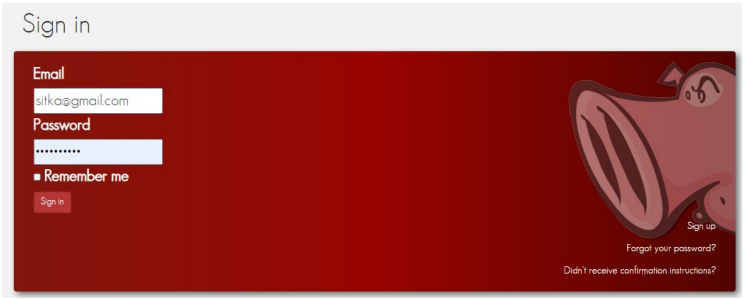
Les IPS (Intrusion Prevention Systems): Les IPS bloquent et rejettent les paquets réseau en utilisant un profil de sécurité en cas de menaces .

2- Création d'un compte dans Snort

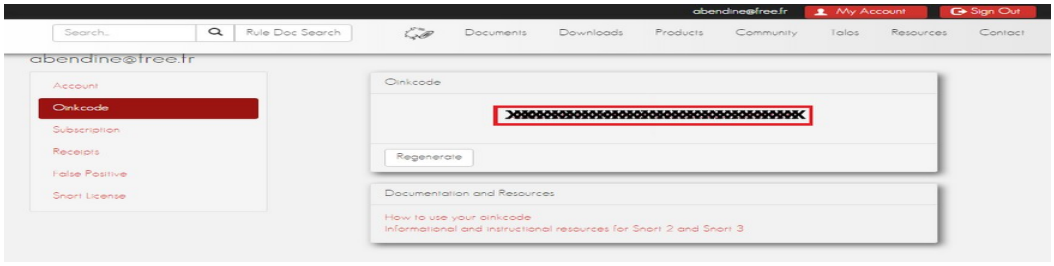
Il faut créer un compte sur le site officiel de Snort (https://www.snort.org/users/sign_up)
, car Snort va nous fournir une clé (**Snort Oinkmaster Code)** qui nous servira à la mise à jour des règle Snort.
Une fois le formulaire d'inscription est rempli il faut se rendre sur la messagerie qu'on a renseigné dans notre formulaire d'inscription pour confirmer notre inscription à partir du mail envoyé par Snort.



Une fois L'inscription confirmé on se rend sur le site de Snort https://www.snort.org/et on se connecte avec nos identifiants

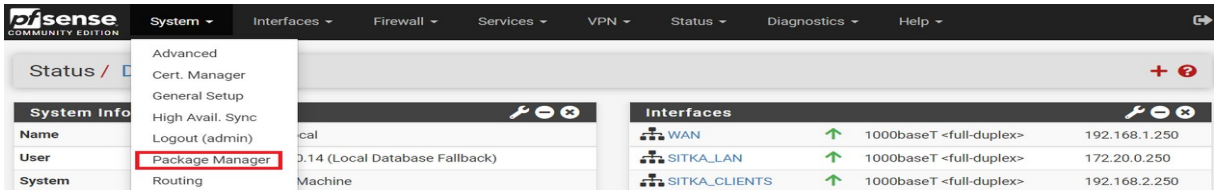


Une fois connecté on va dans le menu Oincode pour récupérer le code de téléchargement et de mise à jour des règles Snort

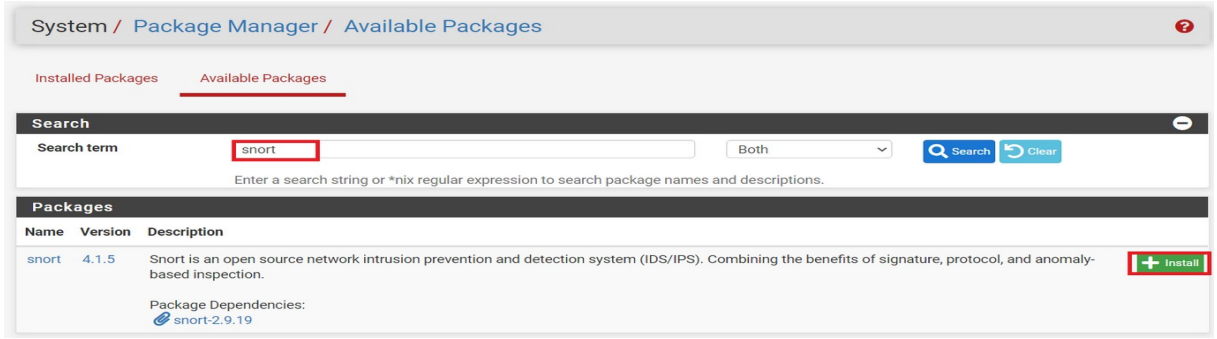


3- Installation de Snort

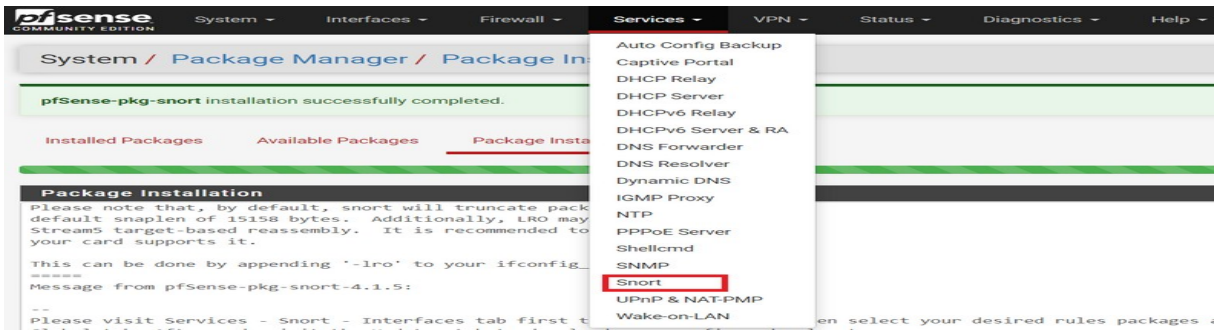
On accède au menu **System** et sélectionnez l'option de **Package Manager**.



Sur l'écran de **Package Manager**, accédez à l'onglet **Available Paquages**.
Sur le moteur de recherche, on cherche Snort et on installe le paquet Snort.



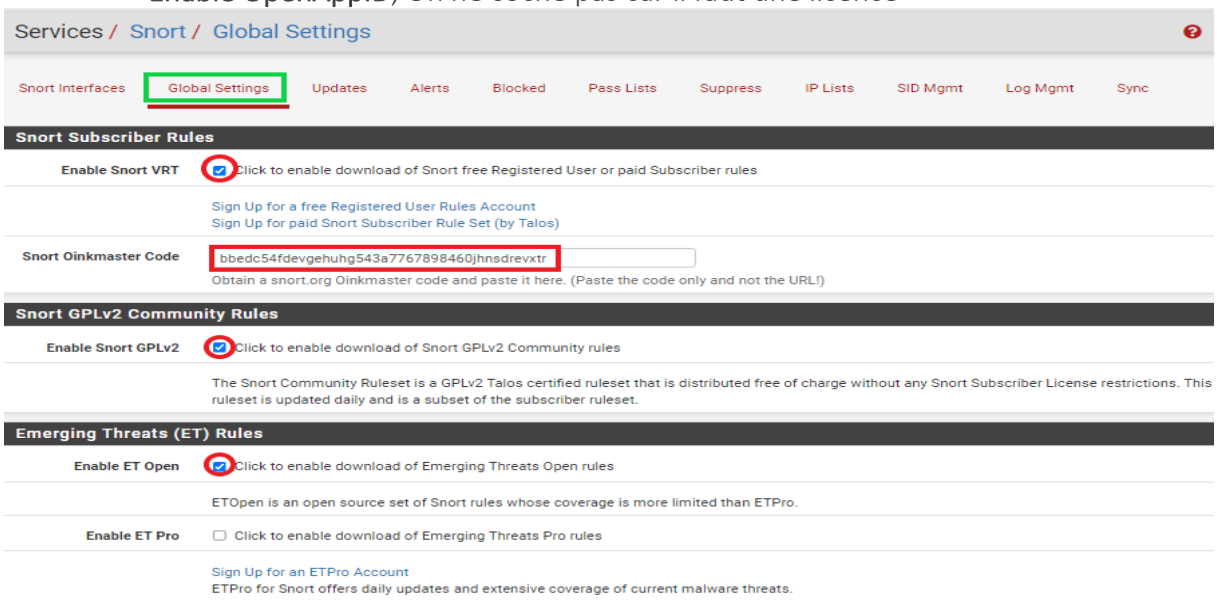
Accédez au menu Pfsense Services et sélectionnez l'option Snort.



4- Configuration de Snort

On va dans l'onglet **Global Settings**, dans cette étape on va activer le téléchargement de règles gratuites, en cochant la case **Enable Snort VRT**.
Et ensuite nous pouvons cocher les cases :

- **Enable Snort GPLv2**,
- **Enable ET Open**,
- **Enable OpenAppID**, On ne coche pas car il faut une licence



Dans la zone **Rules Update Settings** on effectue la configuration suivante :

Update Interval :1 DAY

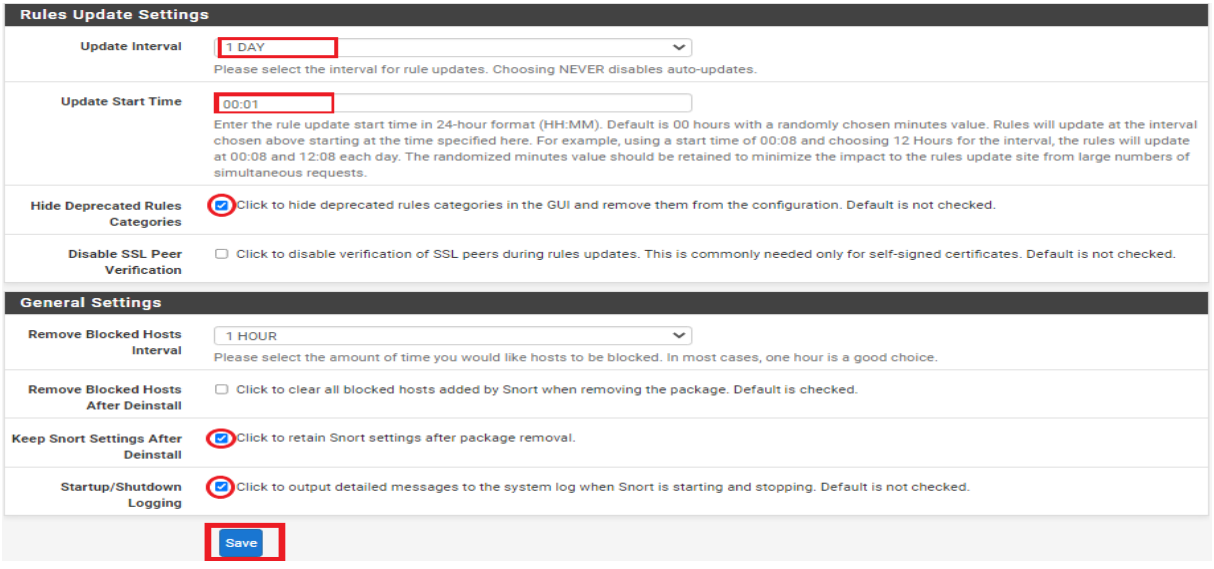
Update Start Time : 00 :01

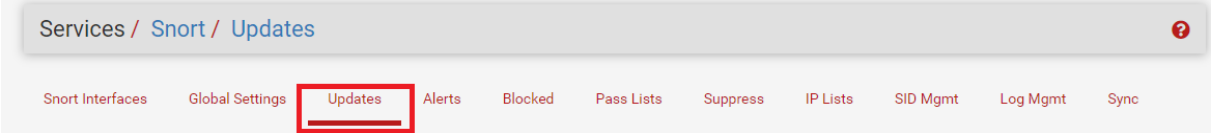
Hide Deprecated Rules Categories : On coche

Remove Blocked Hosts Interval : 1 HOUR

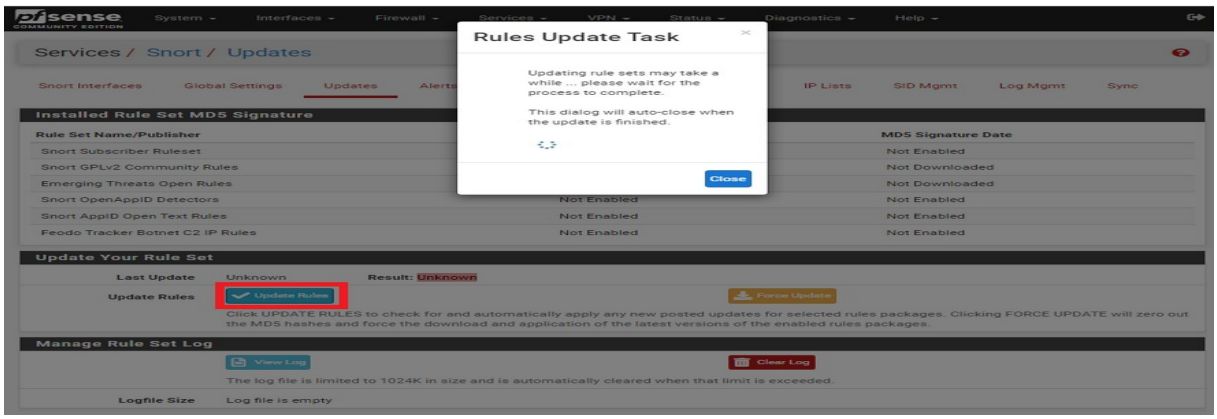
Keep Snort Settings After Deinstall : Si on désinstalle Snort on laisse les paramètres de configuration On coche

Startup/Shutdown Logging : pour avoir les log On coche

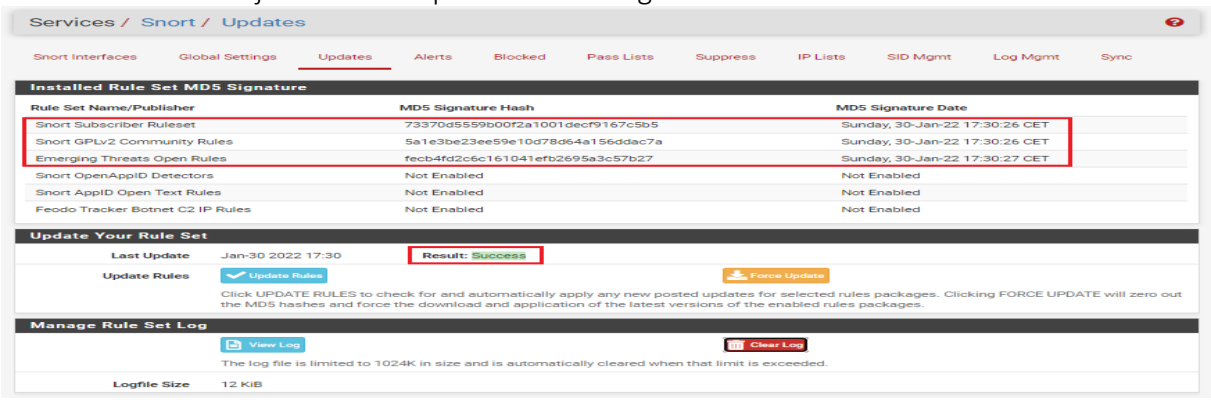




Sur l'onglet Mises à jour, cliquez sur le bouton Règles de mise à jour pour télécharger les règles Snort.



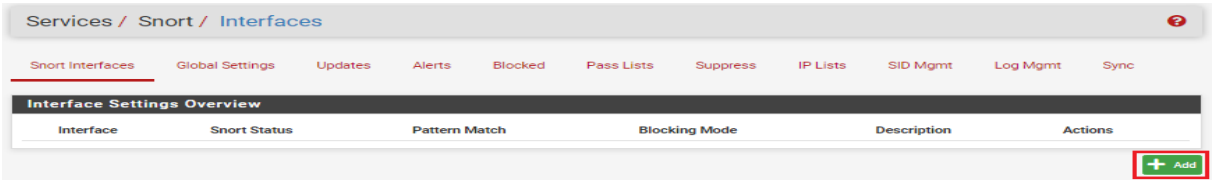
A la fin de la mise à jours on voit qu'on a le message **Result :Success**



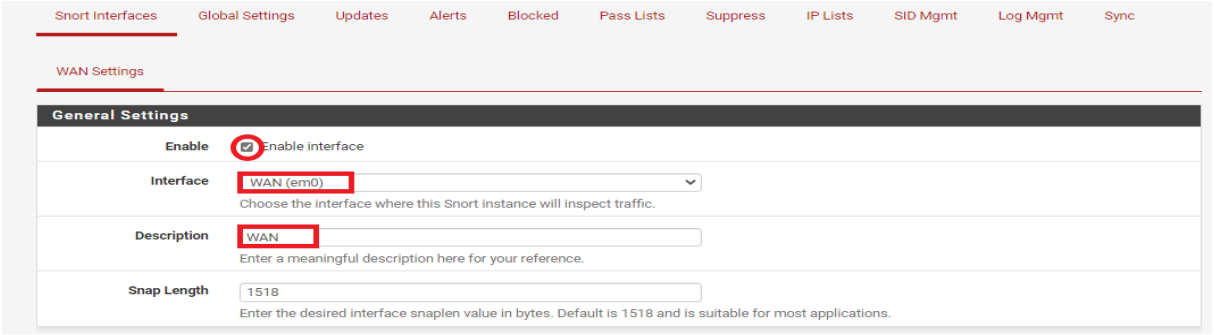
En affichant les logs on a un message qui précise que Snort n'est configuré sur aucune interface

Maintenant on va sur **Snort interfaces** pour choisir l'interface ou les interfaces sur laquelle Snort va analyser et écouter le trafic réseau **on clique sur add pour rajouter notre interface :**

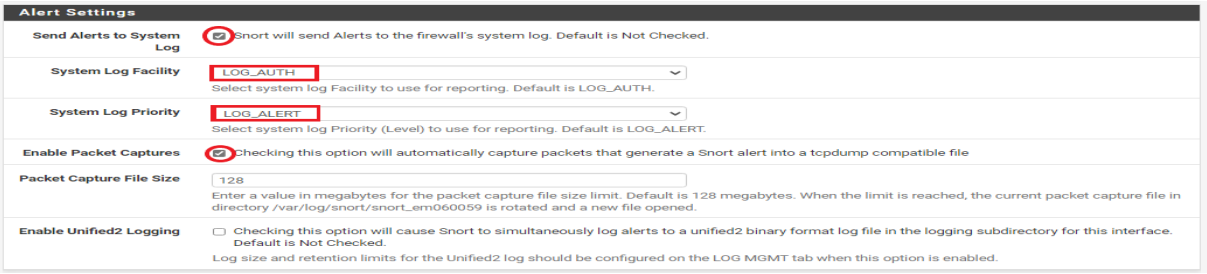
Snap Length est la longueur maximale des paquets capturés par Snort. Il permet de limiter la quantité de données qui sont stockées en mémoire pour chaque paquet, et donc de réduire la charge sur le système.



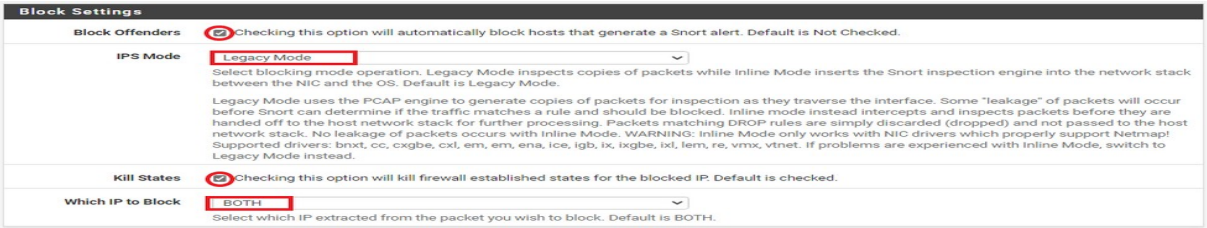
Dans la zone **General Setting** on activer l'interface wan qui est l'interface à surveiller



Localiser la zone **Alerts Settings** et effectuer la configuration suivante :
Send Alerts to System Log on active cette option pour avoir les alertes de snort



Dans la zone Block Settings on active le mode IPS en appliquant la configuration ci-dessous
Ceci permettra de bloquer les hôtes qui génère l'alerte



Après on laisse tout par défaut et clique sur le bouton **Save**.

Maintenant on accède à l'onglet **Wan Catégories** et on effectue la configuration suivante :

Resolve Flowbits (les "flowbits" sont une fonctionnalité de Snort qui permet de maintenir l'état de traitement des connexions réseau et d'ajouter des conditions supplémentaires à des règles en fonction de l'état de traitement de ces connexions) :

On active cette option Snort activera automatiquement les règles requises pour les flowbits et il examinera les règles activées dans les catégories de règles qu'on a choisies pour les **Resolve Flowbits**. Toutes les règles qui définissent ces flowbits dépendants seront automatiquement activées et ajoutées à la liste des fichiers dans le répertoire des règles de l'interface.

- **IPS Policy Selection** : On active cette option et on sélectionne comme politique IPS **Balanced.**

L'activation de cette option désactive le choix manuel des règles Snort **Snort Text Rules**, **Snort SO Rules** par-contre les règles **ET Open Rules reste manuelle**

Les politiques Snort IPS sont **Connectivity**, **Balanced**, **Sécurity** et **Max-Detect**:

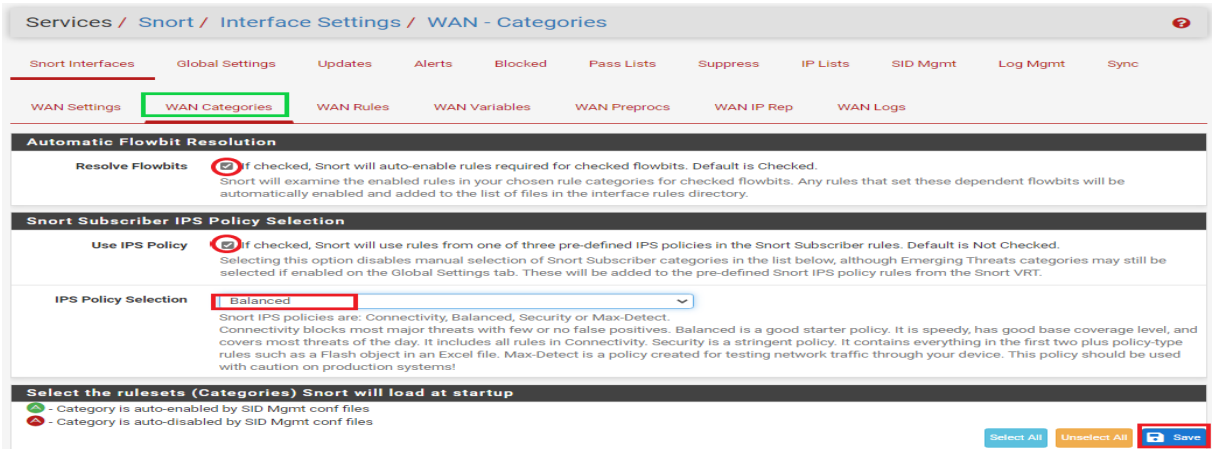
Connectivity bloque la plupart des menaces majeures avec peu ou pas de faux positifs.

Balanced est une bonne politique de départ. Il est rapide, a un bon niveau de couverture de base et couvre la plupart des menaces. Il inclut toutes les règles de Connectivité.

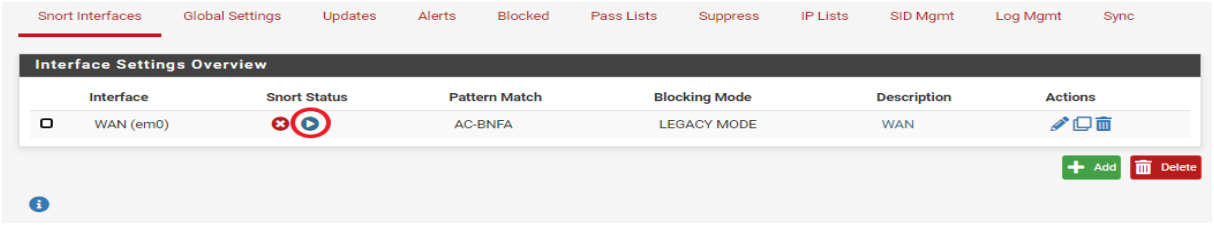
Sécurity est une politique stricte. Il contient tout ce qui se trouve dans les deux premiers plus les règles de type politique telles qu'un objet Flash dans un fichier Excel.

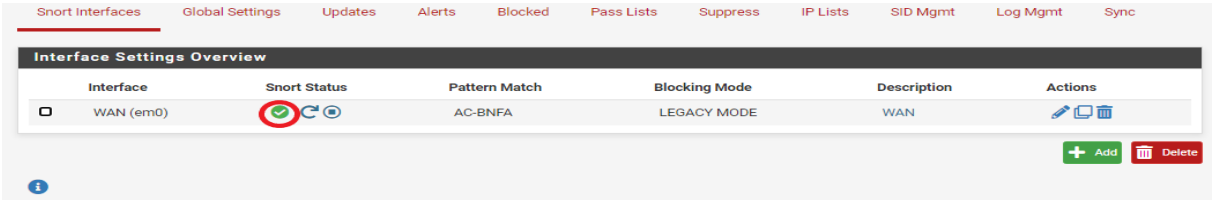
Max-Detect est une stratégie créée pour tester le trafic réseau via votre appareil. Cette politique doit être utilisée avec prudence sur les systèmes de production !

Après avoir terminé la configuration, cliquez sur le bouton Enregistrer (save)



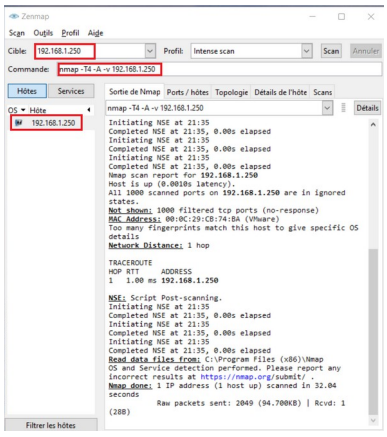
Maintenant on va démarrer notre Interface Snort



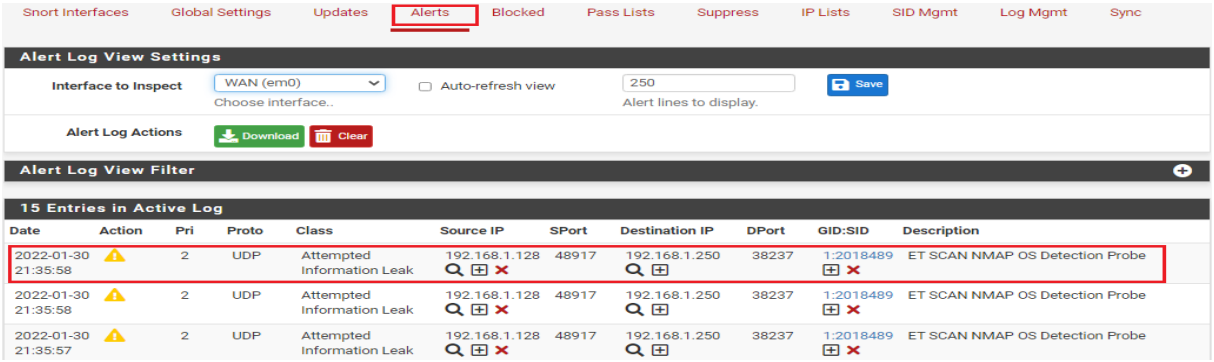


Test d'intrusion

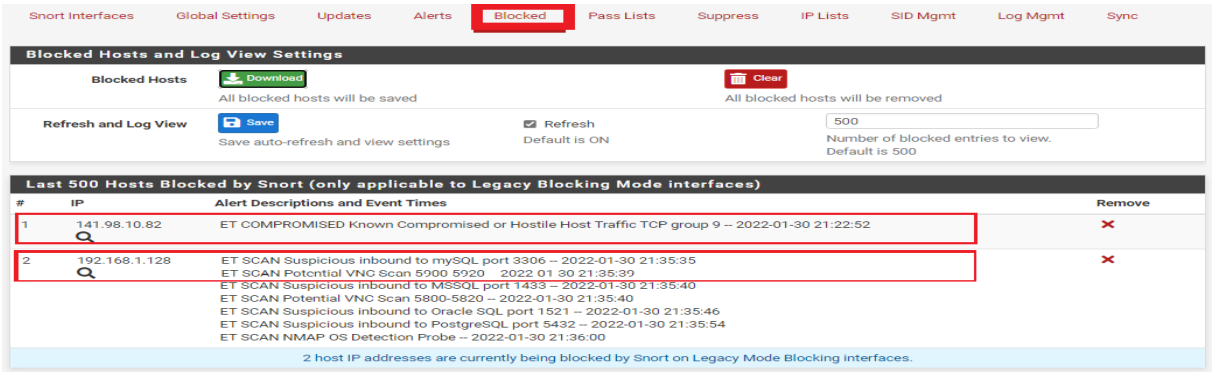
Sur Notre machine physique on installe un utilitaire nmap qui servira de scanner les ports de pfsense



Sur Pfsense dans l'onglet Alerte on relève des notifications d'attaques d'une machine dont l'adresse IP est 192.168.1.128 c'est l'adresse de notre machine physique, l'attaque détectée n'est que la requête nmap



Dans l'onglet Bloked on voit que la machine dont l'adresse IP est 192.168.1.128 est bloqué car elle est identifié comme hoste hostile



1- Introduction

Dans cette partie consacrée à Pfsense on va voir comment installer le package Snort sur PfSense, et ainsi un IDS voir même un IPS !

On va d'abord voire un peu ce qu'est un IDS et un IPS et la différence entre eux.

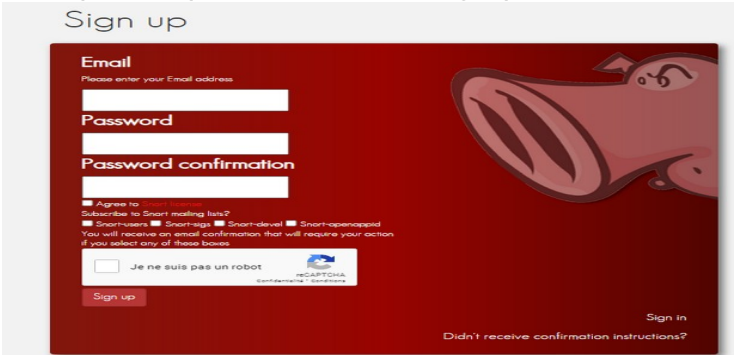
Les IDS (Intrusion Detection Systems) n'a pas comme rôle de bloquer les attaques, IDS utilisent une base de données d'attaques afin de :

- Analyser et surveiller le trafic réseau pour détecter une cyberattaque.
- Détecter les violations de la politique de sécurité,
- Détecter les malwares et les scanners de port.

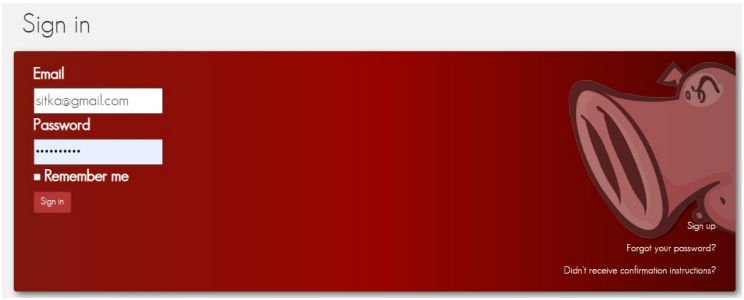
Les IPS (Intrusion Prevention Systems): Les IPS bloquent et rejettent les paquets réseau en utilisant un profil de sécurité en cas de menaces .

2- Création d'un compte dans Snort

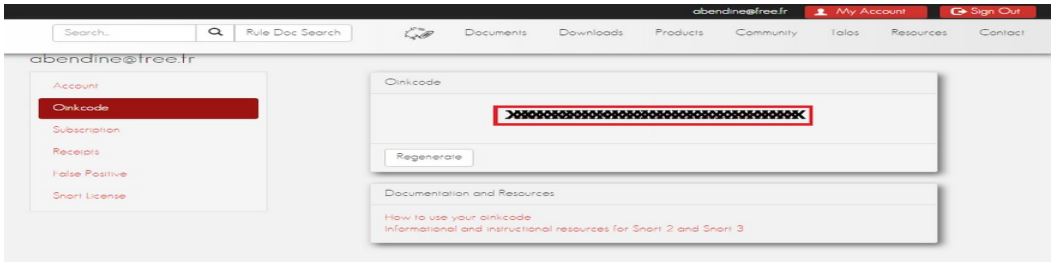
Il faut créer un compte sur le site officiel de Snort (https://www.snort.org/users/sign_up)
, car Snort va nous fournir une clé (**Snort Oinkmaster Code)** qui nous servira à la mise à jour des règle Snort.
Une fois le formulaire d'inscription est rempli il faut se rendre sur la messagerie qu'on a renseigné dans notre formulaire d'inscription pour confirmer notre inscription à partir du mail envoyé par Snort.



Une fois L'inscription confirmé on se rend sur le site de Snort https://www.snort.org/et on se connecte avec nos identifiants

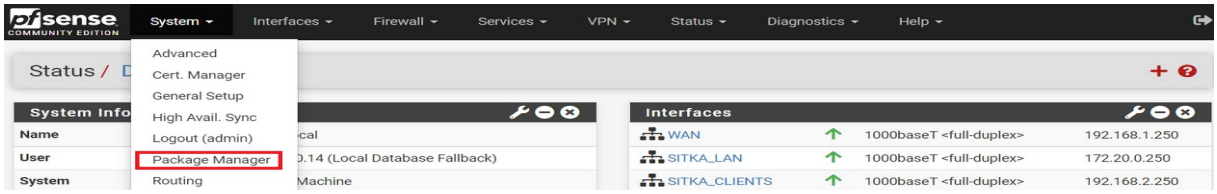


Une fois connecté on va dans le menu Oincode pour récupérer le code de téléchargement et de mise à jour des règles Snort

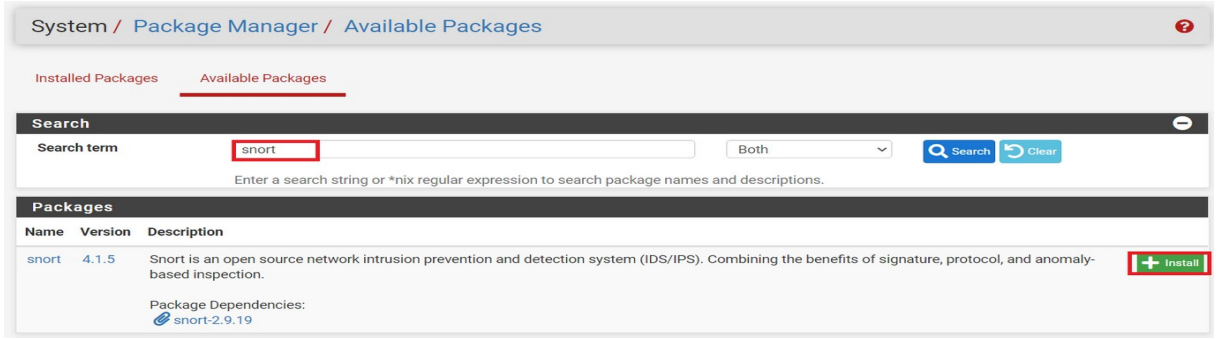


3- Installation de Snort

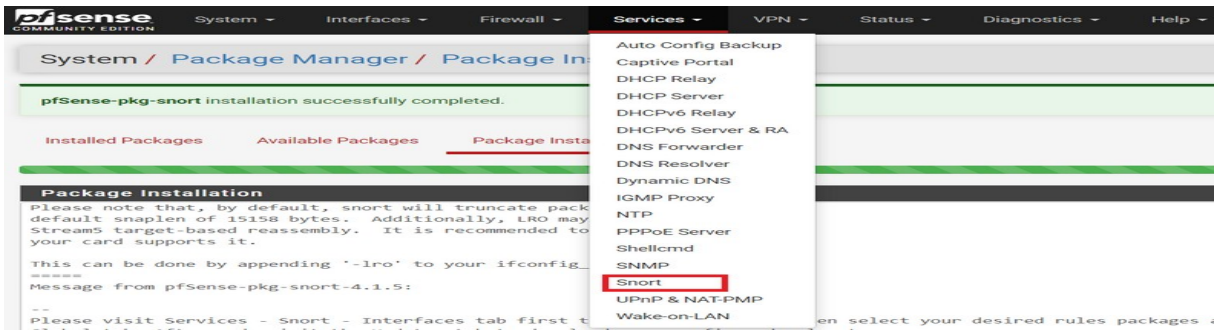
On accède au menu **System** et sélectionnez l'option de **Package Manager**.



Sur l'écran de **Package Manager**, accédez à l'onglet **Available Paquages**.
Sur le moteur de recherche, on cherche Snort et on installe le paquet Snort.



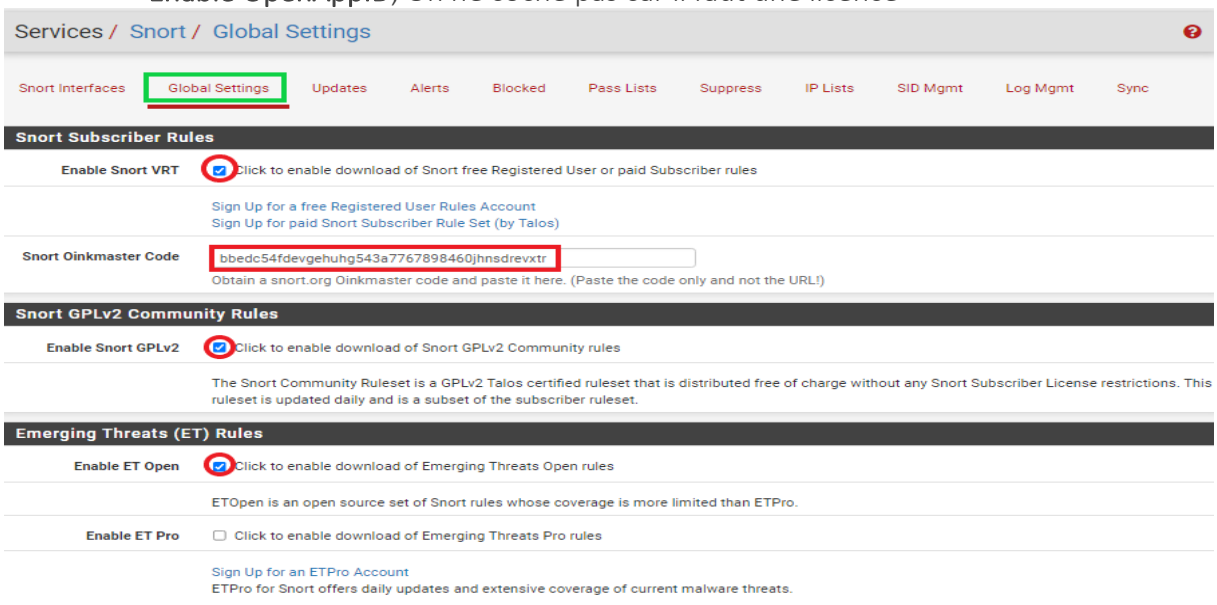
Accédez au menu Pfsense Services et sélectionnez l'option Snort.



4- Configuration de Snort

On va dans l'onglet **Global Settings**, dans cette étape on va activer le téléchargement de règles gratuites, en cochant la case **Enable Snort VRT**.
Et ensuite nous pouvons cocher les cases :

- **Enable Snort GPLv2**,
- **Enable ET Open**,
- **Enable OpenAppID**, On ne coche pas car il faut une licence



Dans la zone **Rules Update Settings** on effectue la configuration suivante :

Update Interval :1 DAY

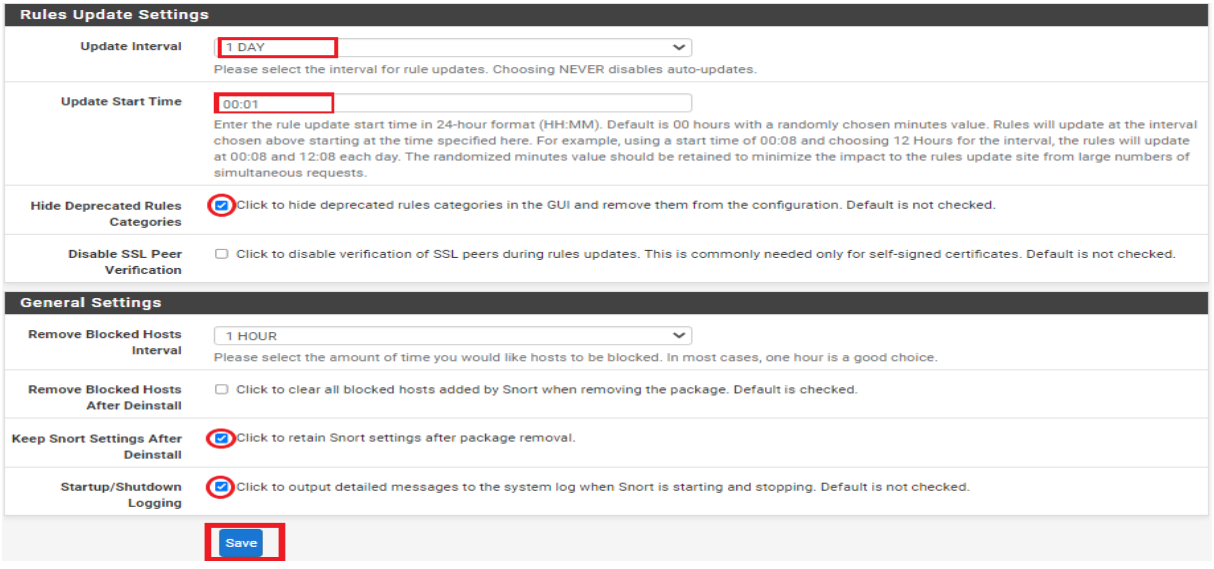
Update Start Time : 00 :01

Hide Deprecated Rules Categories : On coche

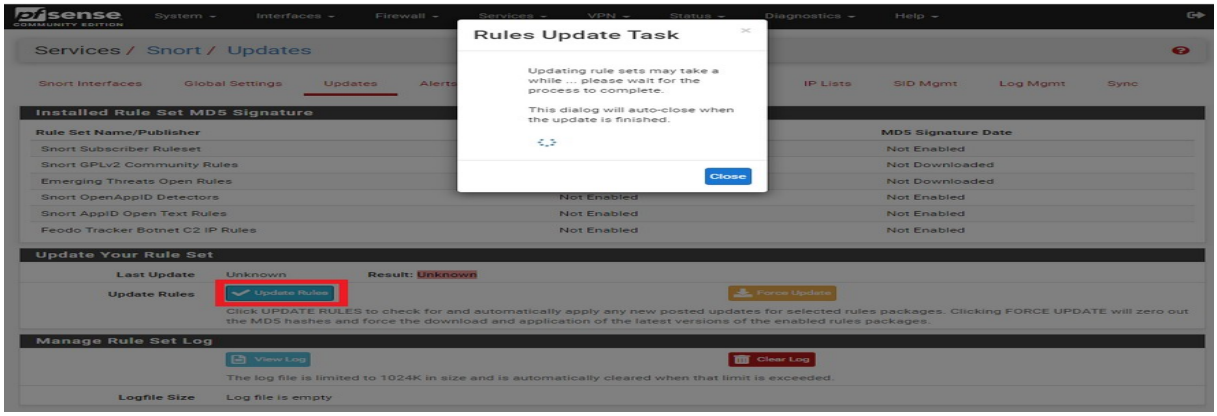
Remove Blocked Hosts Interval : 1 HOUR

Keep Snort Settings After Deinstall : Si on désinstalle Snort on laisse les paramètres de configuration On coche

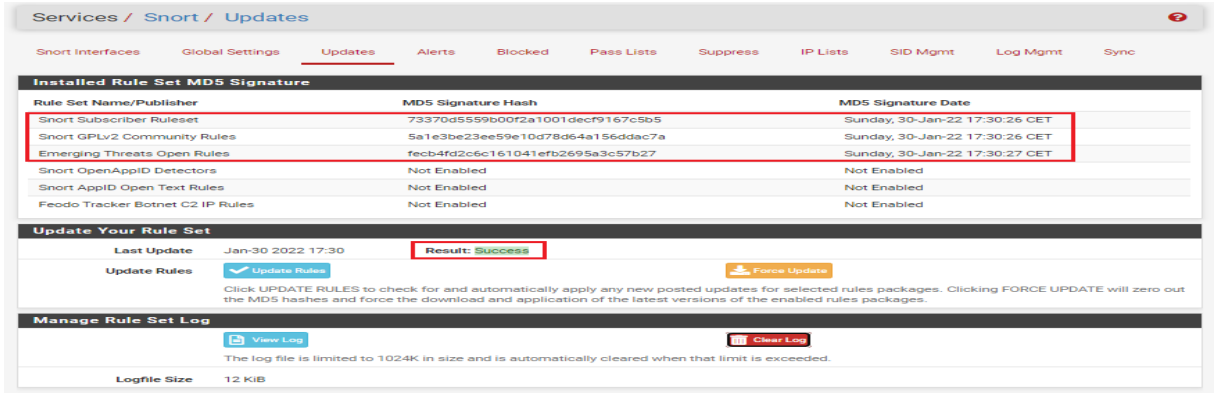
Startup/Shutdown Logging : pour avoir les log On coche



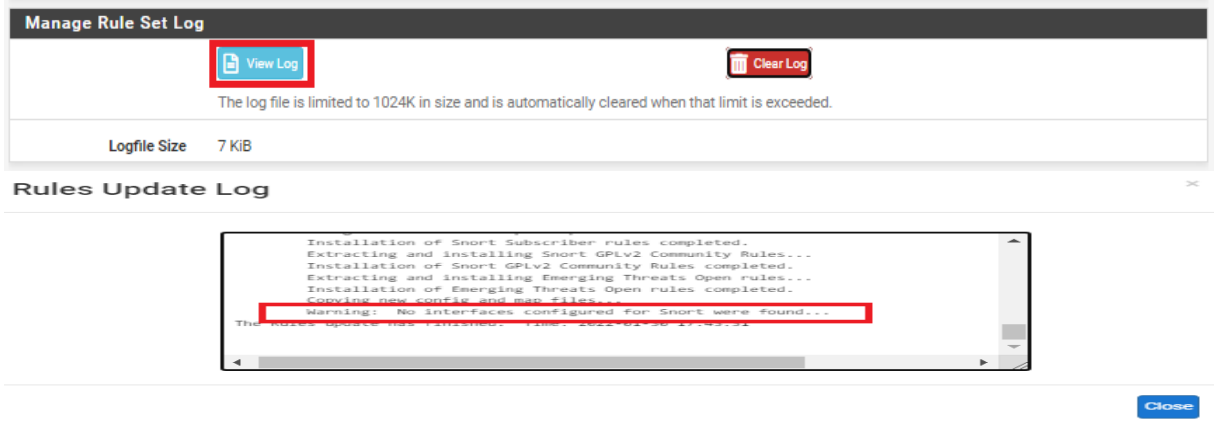
Sur l'onglet Mises à jour, cliquez sur le bouton Règles de mise à jour pour télécharger les règles Snort.



A la fin de la mise à jours on voit qu'on a le message **Result :Success**

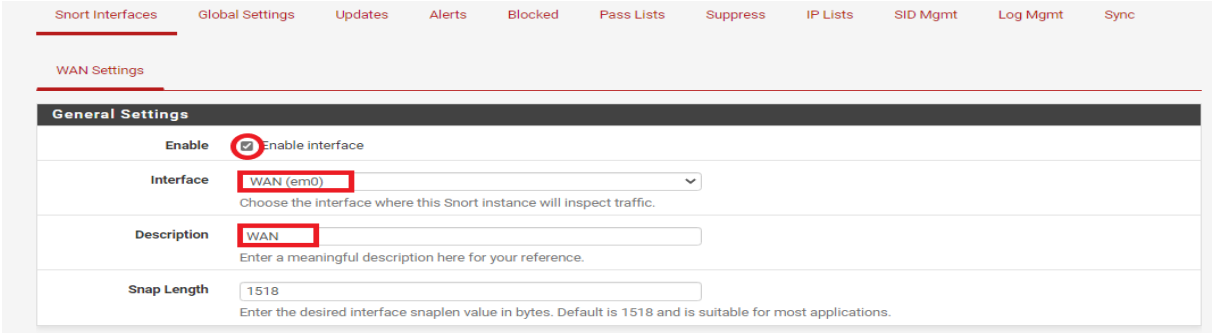


En affichant les log on un message qui précise que Snort n'est configuré sur aucune interface

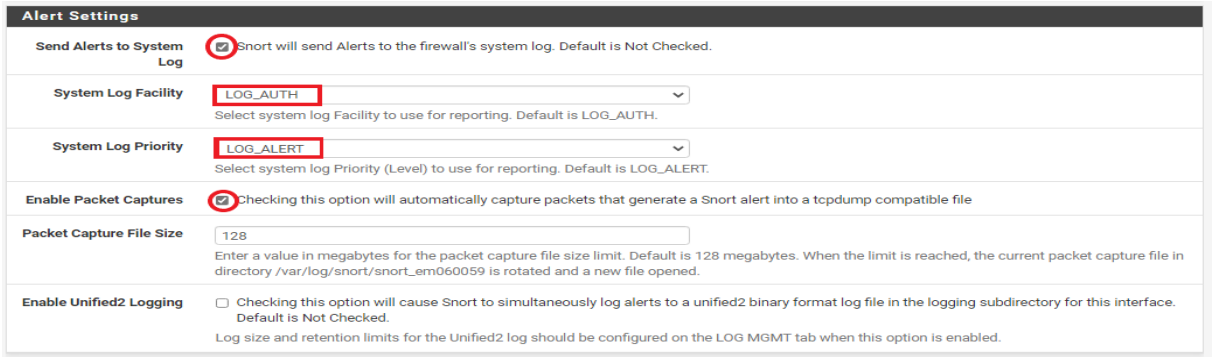


Maintenant on va sur **Snort interfaces** pour choisir l'interface ou les interfaces sur laquelle Snort va analyser et écouter le trafic réseau **on clique sur add pour rajouter notre interface :**

Dans la zone **General Setting** on activer l'interface wan qui est l'interface à surveiller

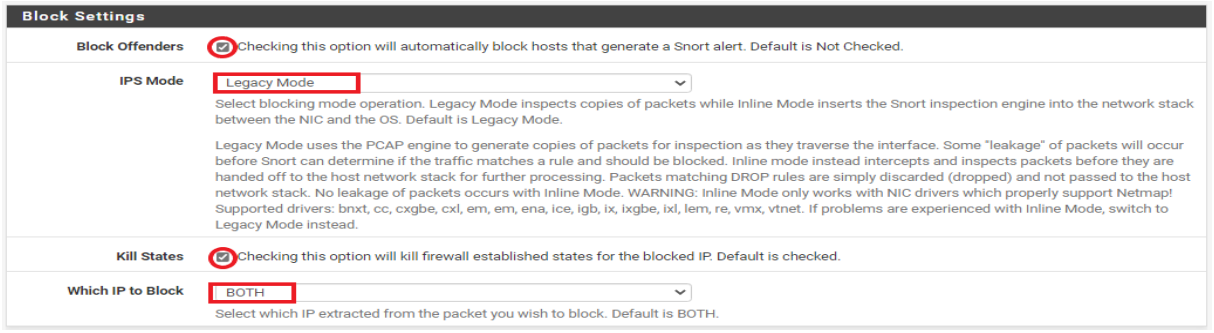


Localiser la zone **Alerts Settings** et effectuer la configuration suivante :
Send Alerts to System Log on active cette option pour avoir les alertes de snort



-

Dans la zone Block Settings on active le mode IPS en appliquant la configuration ci-dessous
Ceci permettra de bloquer les hôtes qui génère l'alerte



Après on laisse tout par défaut et clique sur le bouton Enregistrer.

Maintenant on accéde à l'onglet **Wan Catégories** et effectuez la configuration suivante :
Résoudre les débits - Oui
- Utiliser la politique IPS - Oui
Sélection des politiques IPS – Connectivité

Dans notre exemple, nous avons activé la fonctionnalité IPS et sélectionné la stratégie nommée **Connectivité**.

Après avoir terminé la configuration, cliquez sur le bouton Enregistrer et démarrez le service Snort sur

Introduction

1- Gestion des certificats
- Création de l'autorité de certification
- Création du certificat Server

2- Configurer le serveur OpenVPN

3- Créer les règles de firewall pour OpenVPN
a. A. Autoriser le flux OpenVPN
b. B. Autoriser les flux vers les ressources

4- Exportation de la configuration OpenVPN clientes

5- Test de la connexion VPN

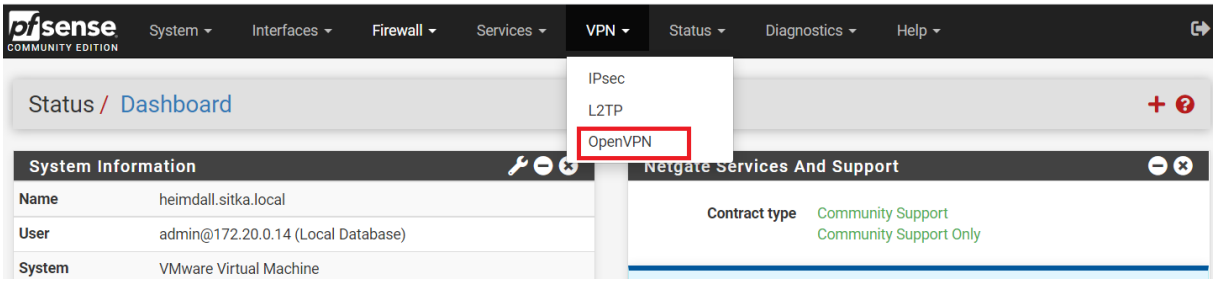
a. Test depuis un client Windows
b. Test depuis un client Android

Introduction

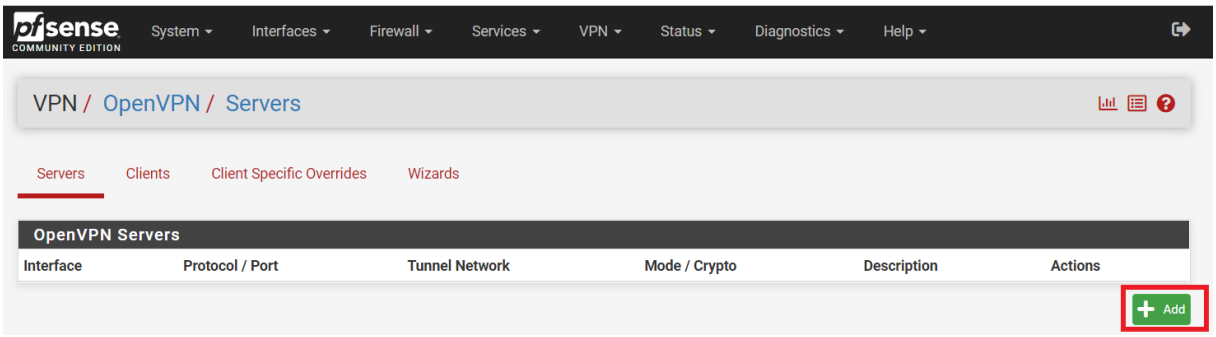
OpenVPN est un logiciel libre permettant de créer un réseau privé virtuel (VPN). Son développement a commencé le 13 mai 2001 grâce à James Yonan.
OpenVPN permet à des **pairs** de s'**authentifier** entre eux à l'aide d'une **clé privée** partagée à l'avance, de **certificats électroniques** ou de couples de noms d'utilisateur/**mot de passe**. Il utilise de manière intensive la **bibliothèque** d'authentification OpenSSL ainsi que le protocole **SSLv3/TLSv1**. Disponible avec une multitude d'environnements tel que **Solaris**, **OpenBSD**, **FreeBSD**, **NetBSD**, **Linux** (**Debian**, **Redhat**, **Ubuntu**, etc.), **Mac OS X**, **Windows 2000**, **XP**, **Vista**, **7**, **8** et **10**, il offre de nombreuses fonctions de sécurité et de contrôle.
OpenVPN n'est pas compatible avec IPsec ou d'autres logiciels VPN. Le logiciel contient un exécutable pour les connexions du client et du serveur, un fichier de configuration optionnel et une ou plusieurs clés suivant la méthode d'authentification choisie.

1- Gestion des certificats
   - Création de l'autorité de certification
   - Création du certificat Server
2- Configurer le serveur OpenVPN

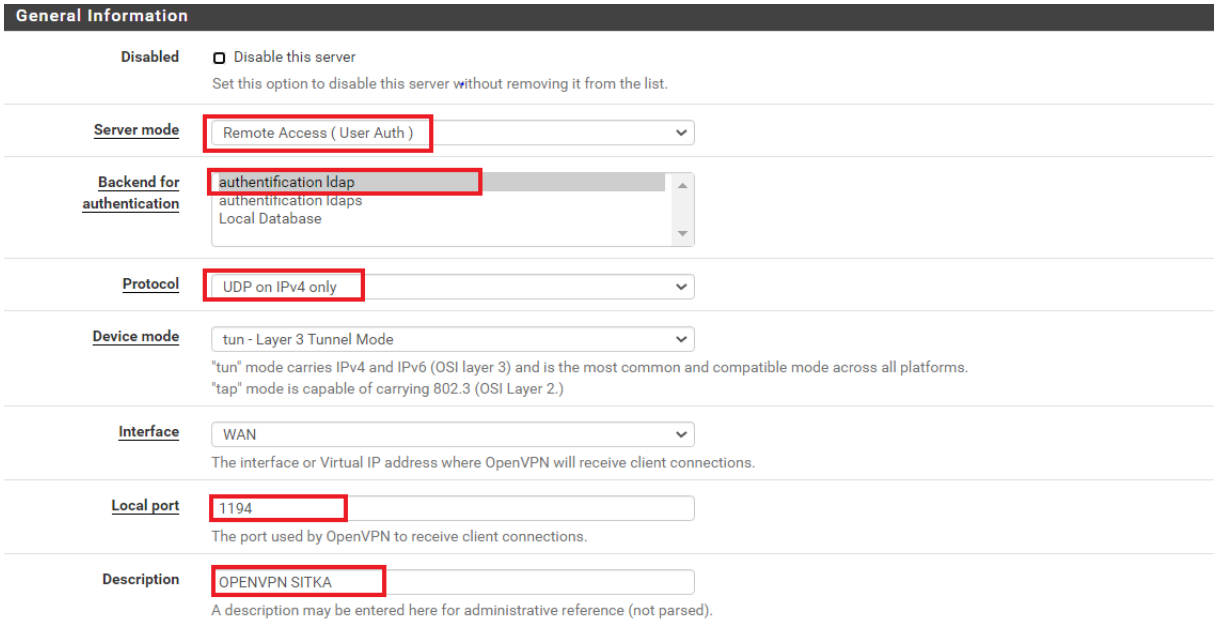
Pour configurer notre VPN on va cliquer sur le menu "**VPN**" puis "**OpenVPN**"



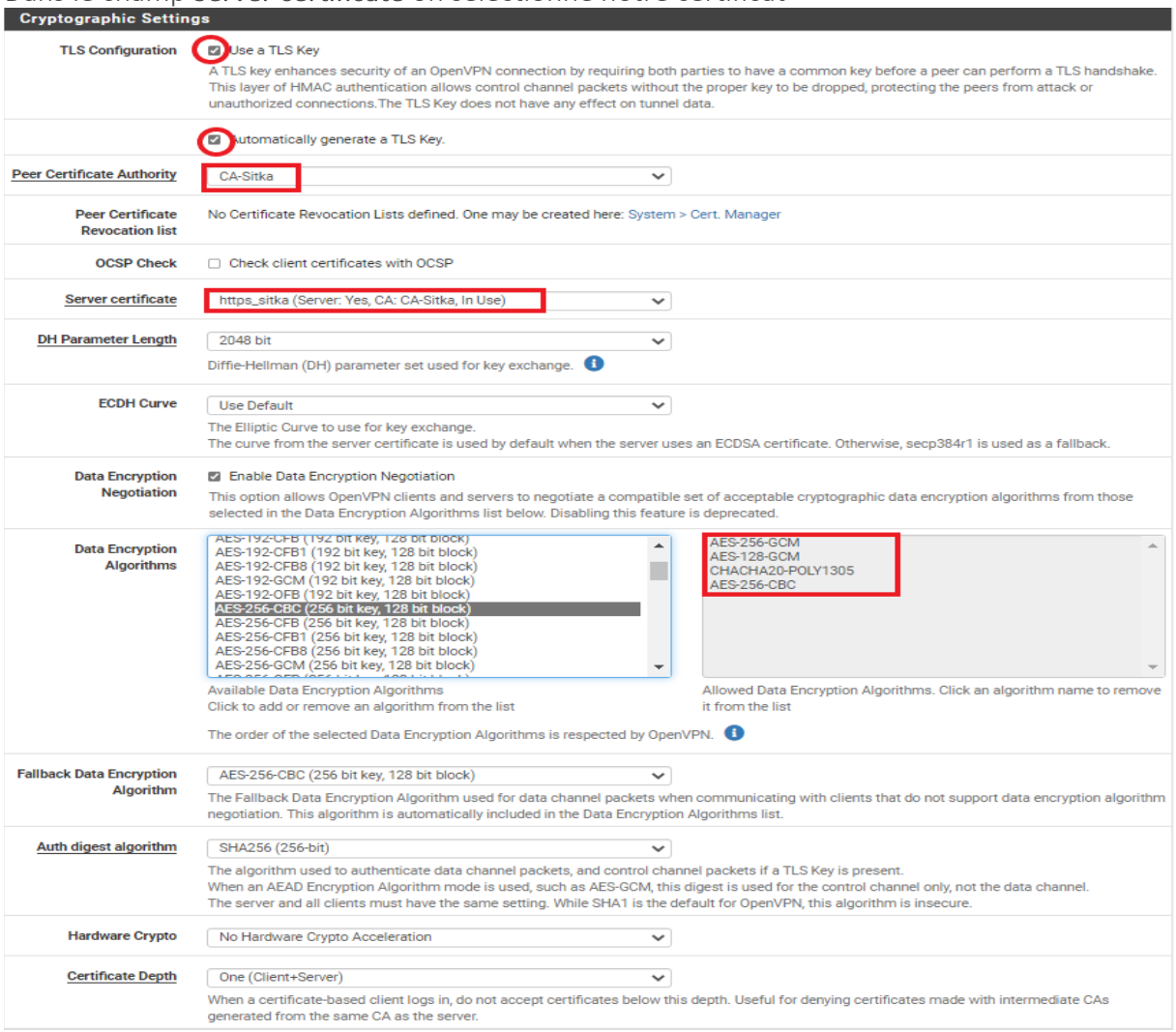
Dans l'onglet **Servers** on clique sur **Add afin de** créer une nouvelle configuration.



Dans "**Server Mode**" on choisit : **Remote Access (User Auth)**.
Le VPN utilise UDP, avec **le port 1194** par défaut on choisira **le port 1919 pour des raisons de securité.**
L'interface, utilisée est la WAN c'est l'interface qui sera utilisé pour notre connexion à distance.

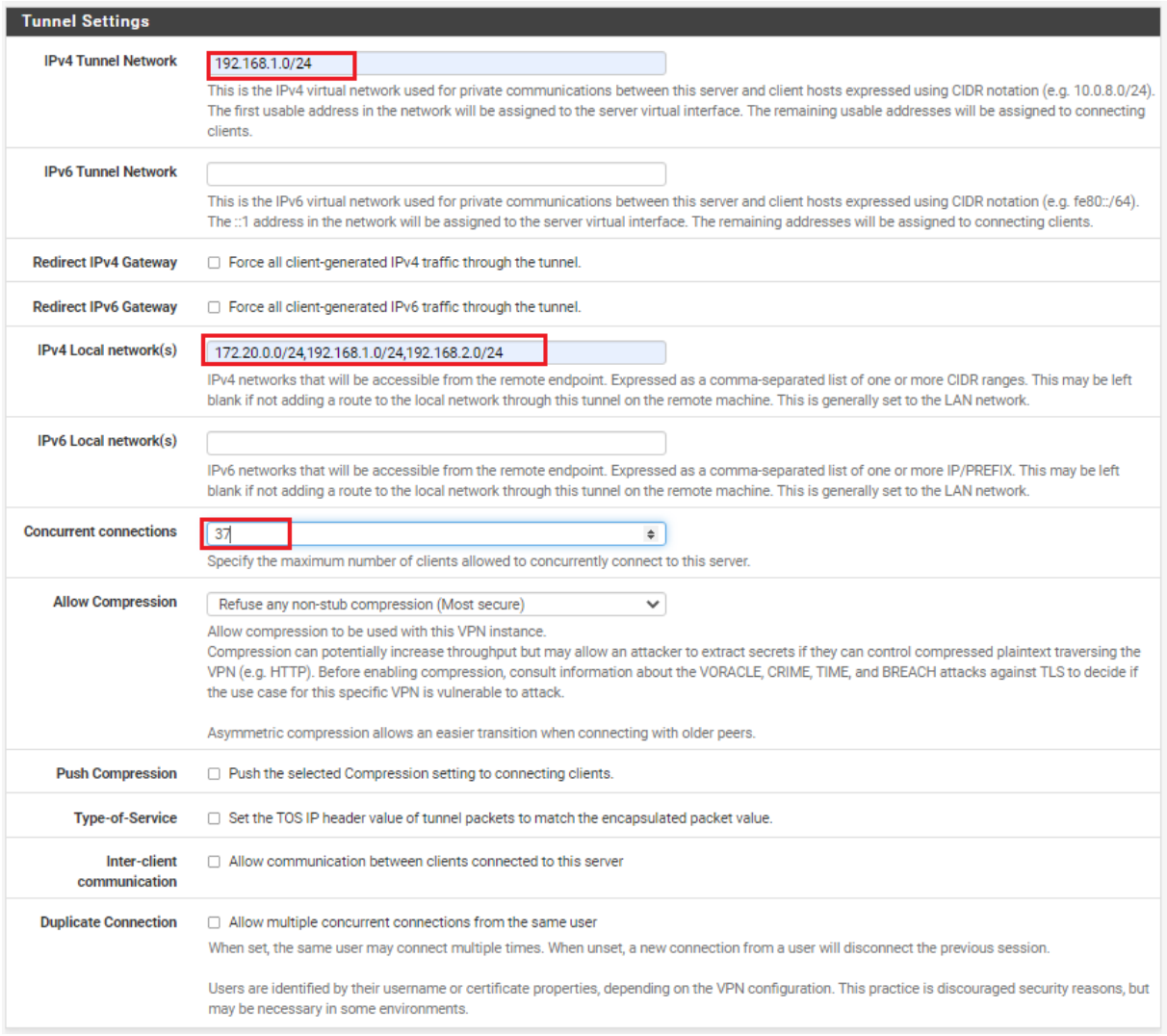


Dans le champ **Peer Certificate Authority** on sélectionne notre autorité de certification
Dans le champ **Server certificate** on sélectionne notre certificat

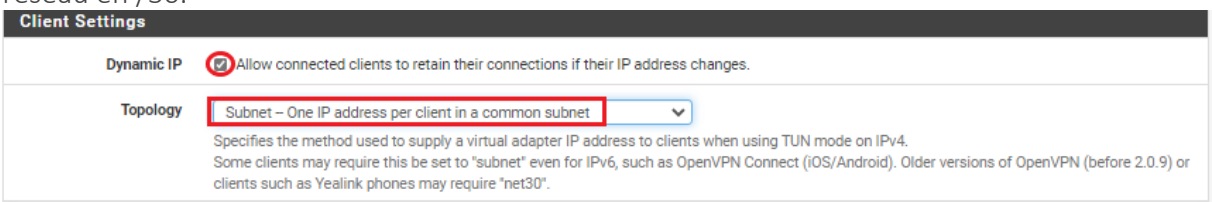


Maintenant on va configurer le tunnel VPN.

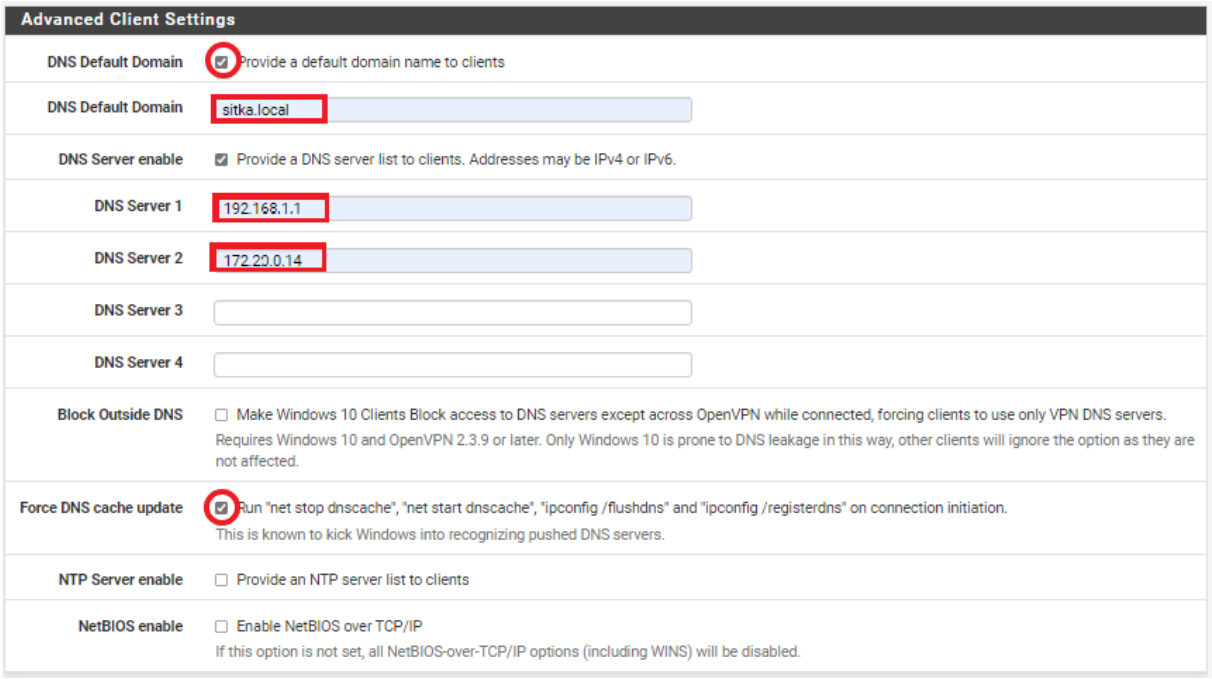
- IPv4 Tunnel Network : En se connectant en VPN le client obtiendra une adresse IP dans ce réseau
- IPv4 Local network : les LAN qu'on veut rendre accessibles via le tunnel VPN. Dans notre cas, on va rendre accessible les réseaux 192.168.1.0/24, 192.168.2.0/24, 172.20.0.0/24
- Concurrent connections : le nombre de connexions VPN simultanés autorisés.



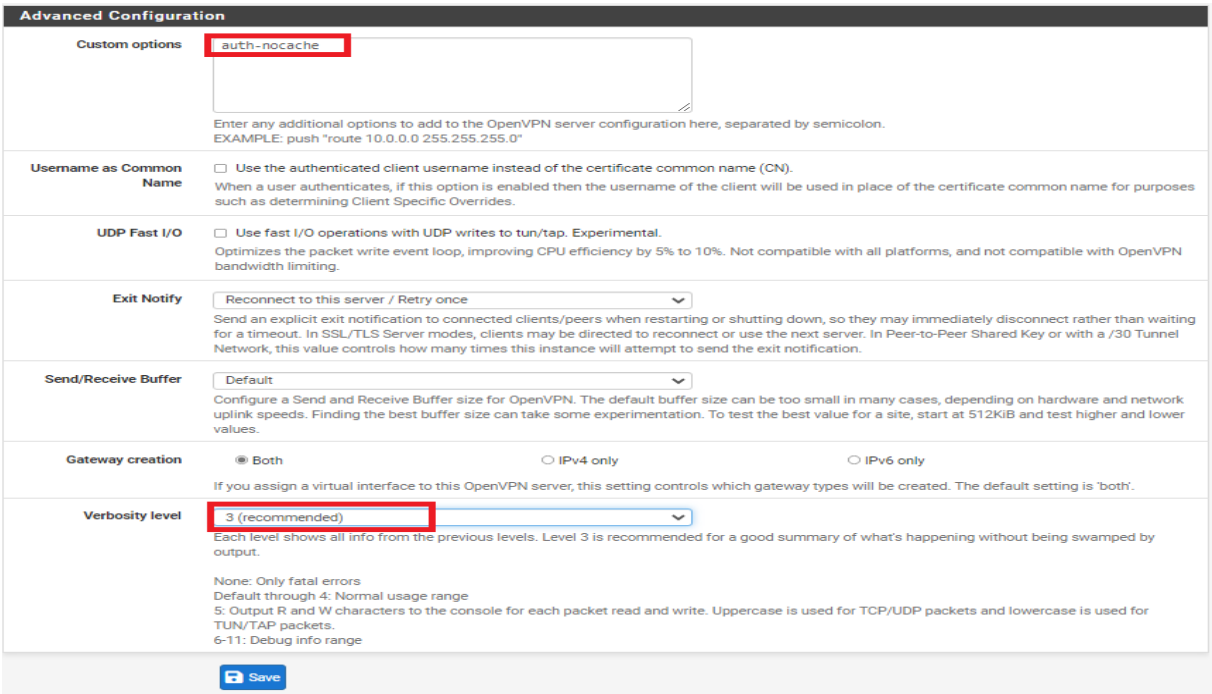
Pour les paramètres des clients, on coche Dynamic IP : Ceci aux client de garder leur connexion si l'adresse IP publique d'un client change, en se connectant via une connexion 4G . Au niveau de la Topology, : pour des raisons de sécurité, il vaut mieux utiliser la topologie net30 - isolated /30 network per client pour que chaque client soit isolé dans un sous-réseau de la plage réseau VPN afin que les clients ne puissent pas communiquer entre eux
Inconvénient de cette méthode la connexion VPN, va consommer 4 adresses IP : une adresse IP pour le PC, une adresse IP pour le pare-feu et les adresses de réseau et broadcast du sous-réseau en /30.



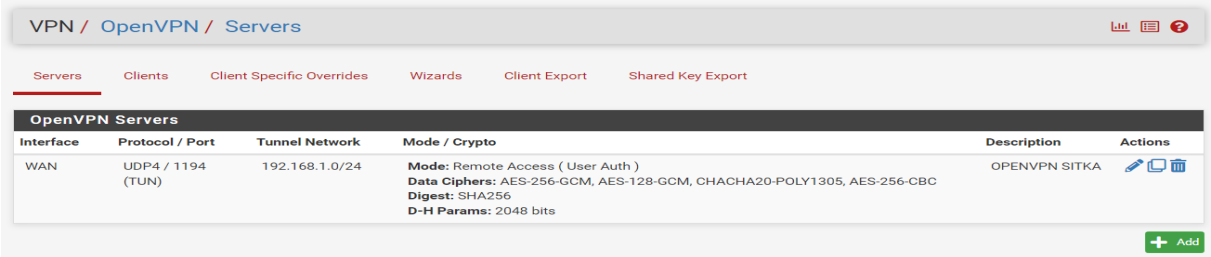
On coche l'option **Provide a DNS server list to clients.**
On indique le nom de domaine
On coche l'option "**Provive a default domain name to clients**" pour indiquer le nom de domaine local.
On indique les adresses IP de nos serveurs DNS
Aussi en force la mise à jour du cache dns



Dans la zone "**Custom options**", on tape : **auth-nocache**. Cette option refuse la mise en cache des identifiants



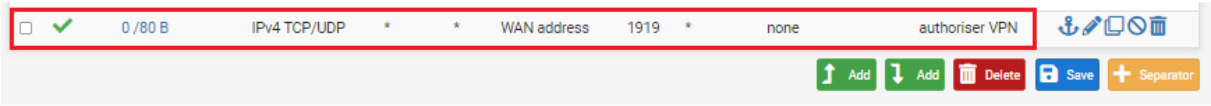
Maintenant on enregistre pour valider la configuration.de notre VPN



3- Création les règles de firewall pour OpenVPN

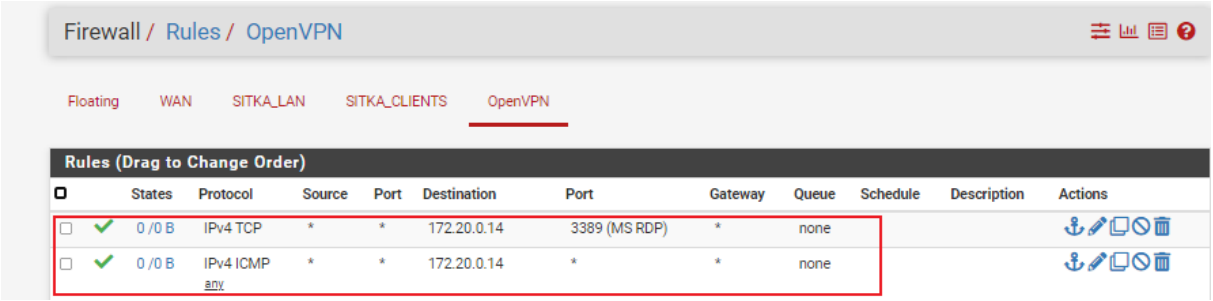
a. Autoriser OpenVPN sur l'interface Wan

Il ne faut pas oublier de créer une règle autorisant le VPN sur notre interface wan



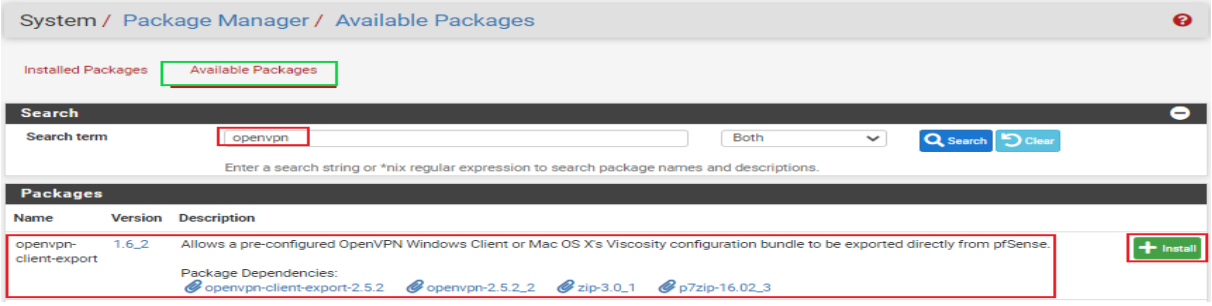
b. Autoriser l'accès aux ressources

Maintenant on va ajouter une règle, sur l'interface OpenVPN.
La règle va autoriser l'accès en RDP à l'hôte 172.20.0.14 au travers du tunnel VPN. On doit créer une ou plusieurs règles en fonction des ressources auxquelles nous voulons y accéder via le VPN.

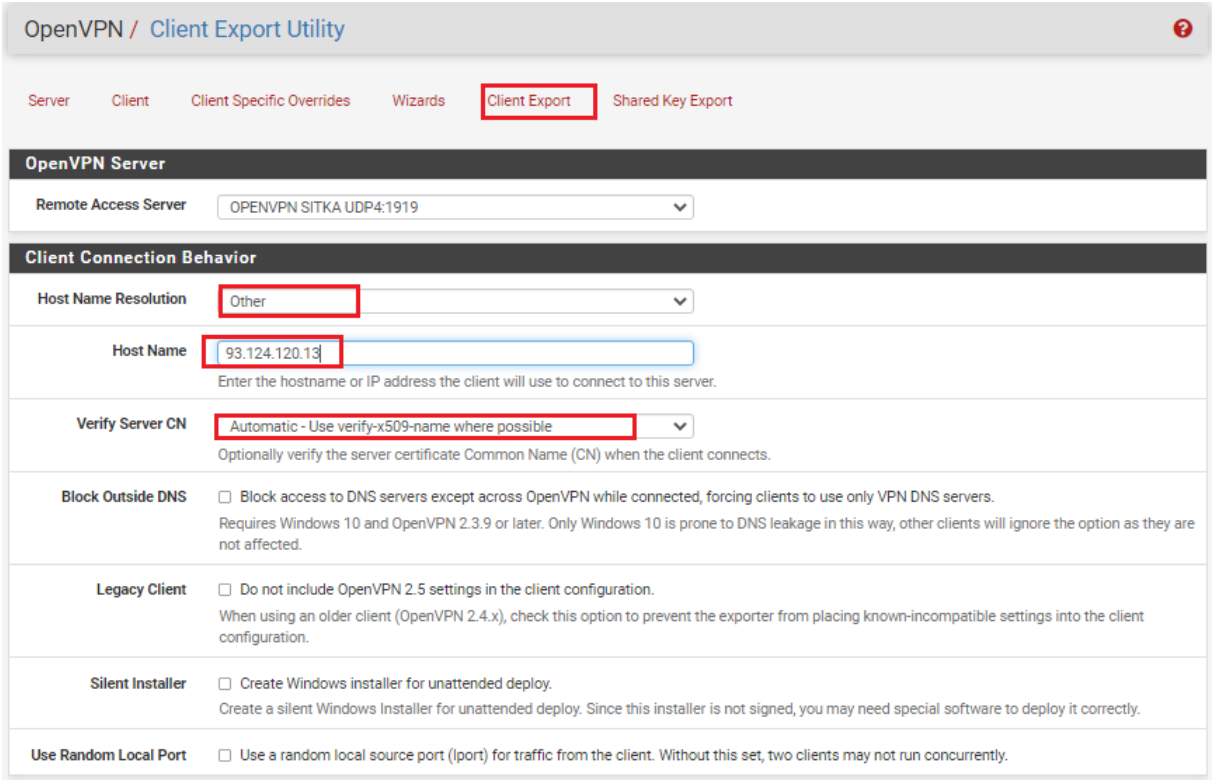


4- Exportation de la configuration OpenVPN

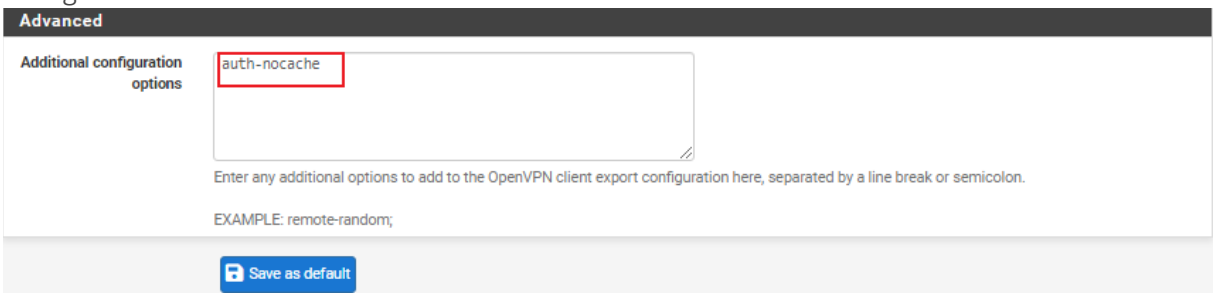
Pour exporter la configuration de notre openvpn pour les clients on va installer un paquet dont le nom est **openvpn-client-export** sur pfsense..
On va dans le menu suivant : **System > Package Manager > Available Packages**.
Recherchez "openvpn" et installez le paquet : **openvpn-client-export**.



Une fois l'installation est faite, on retourne dans le menu **OpenVPN** puis dans l'onglet **Client Export**.
Dans host name on rentre notre adresse IP publique pour nous connecter



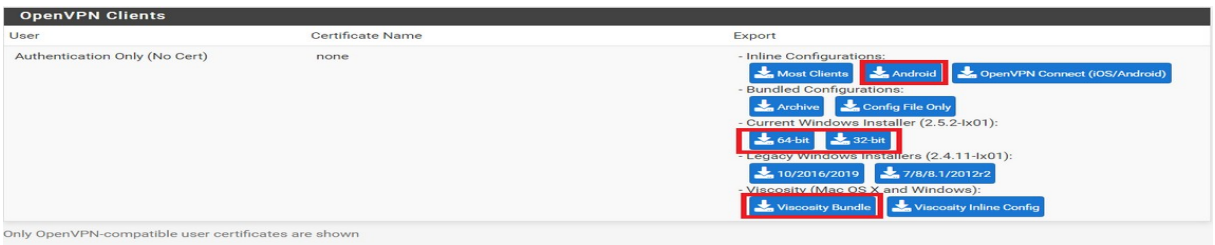
On tous les autres options par défaut, on rajoute seulement l'option **auth-nocache** ; après en enregistre



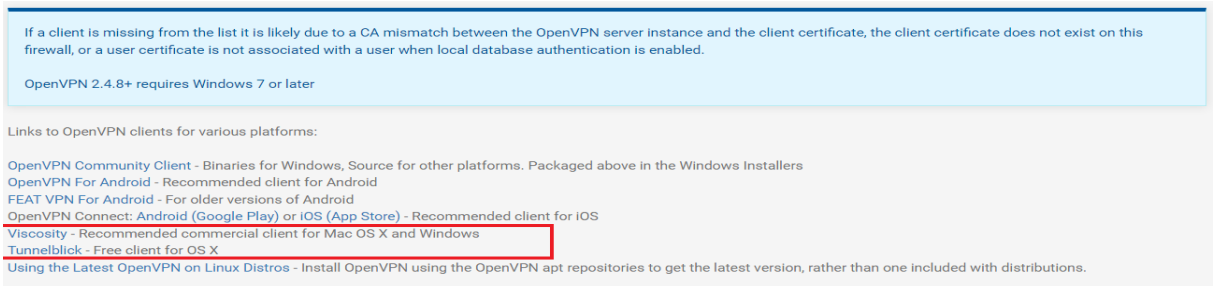
5- Test de la connexion VPN depuis un poste client

a- Téléchargement du client openvpn

Selon le client on télécharge le programme adéquate

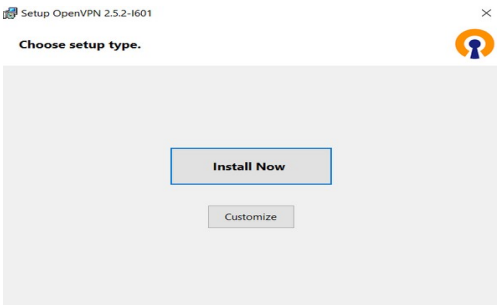


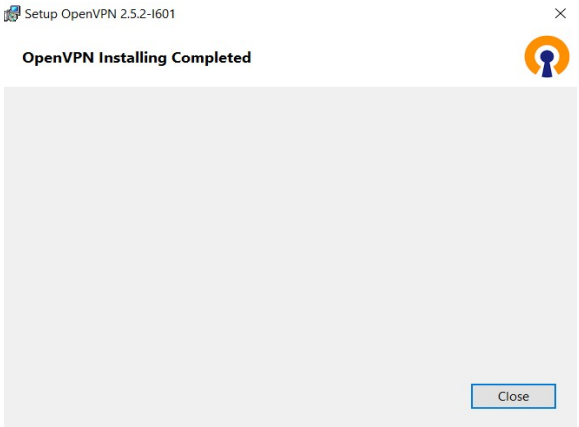
On teste l'accès distant depuis un poste client Windows, Android ou Apple . Pour apple on choisit Viscosity gratuit un mois après c'est payant ou Tunneblick qui est gratuit

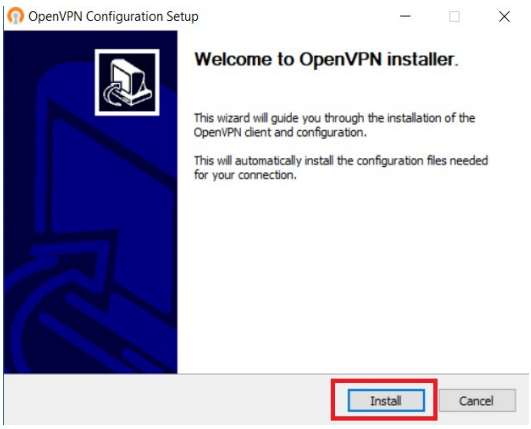


b- Test de connexion sur un client Windows

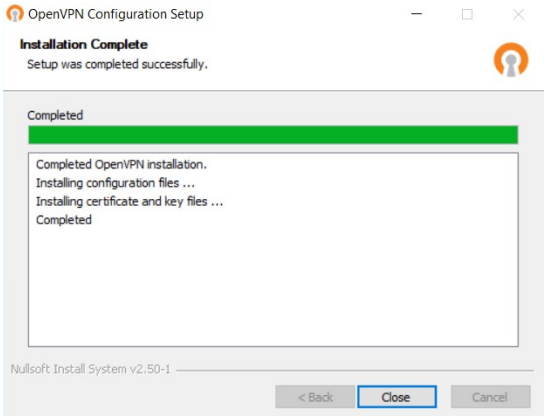
Sur un PC client, on installe le client **OpenVPN** openvpn-heimdall-UDP4-1919-install-2.5.2-I601-amd64

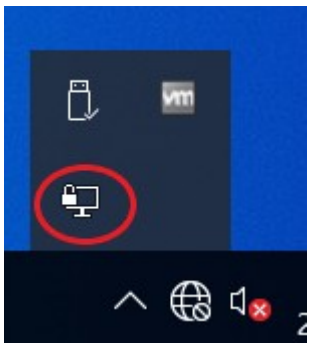


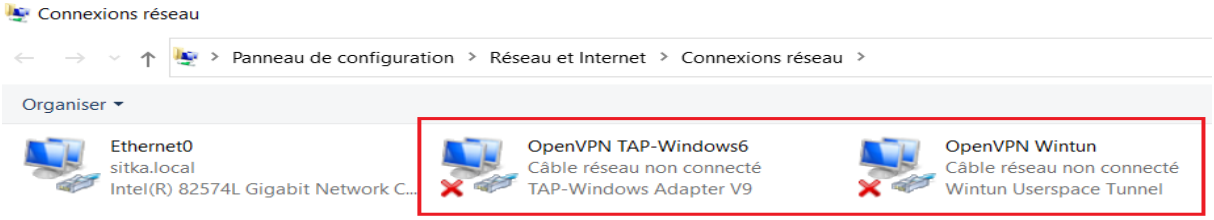




Une fois l'agent VPN est installé un icone dans la barre des taches apparait qui va ne permettre de se connecter à notre serveur VPN ainsi que les interfaces réseaux propre au VPN comme c'est illustré ci-dessous

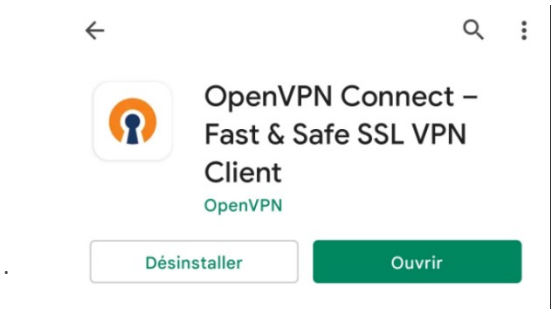




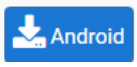


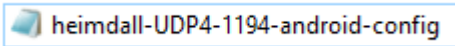
c- Test de connexion sur un client Android

Sur google store on télécharge l'application openvpn

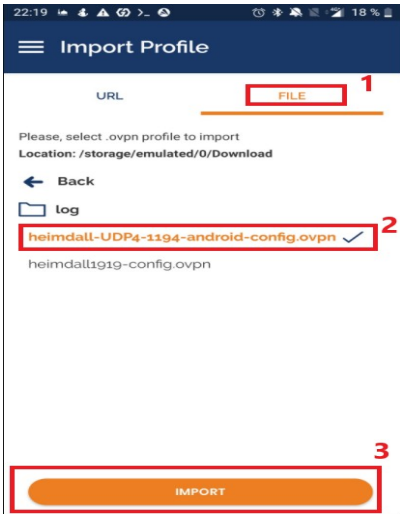


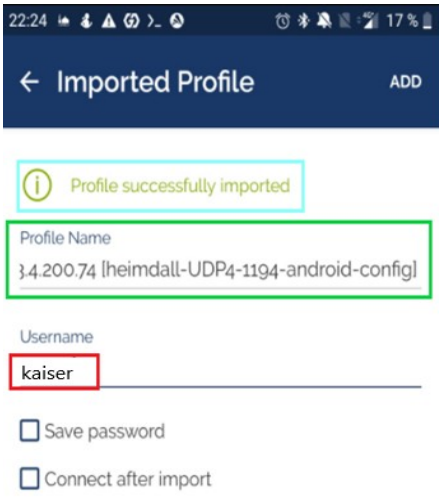
.

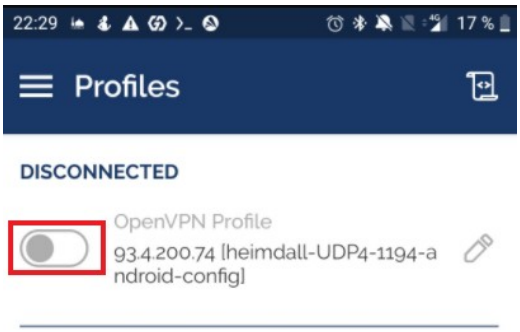
Sur l'interface web de pfsense on télécharge le client androïde pour smartphone en cliquant Sur 

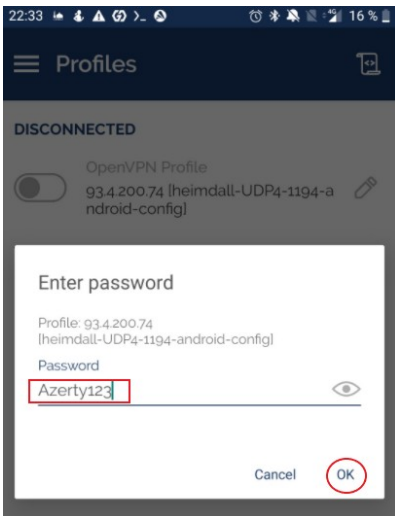
Une fois Le fichier que le fichier 

est téléchargé on l'envoi par mail et on le récupère sur notre messagerie sur le smartphone, Ce fichier on va l'enregistrer et on va l'injecter dans notre application openvpn Android, après on rentre notre identifiant utilisateur et notre mot de passe

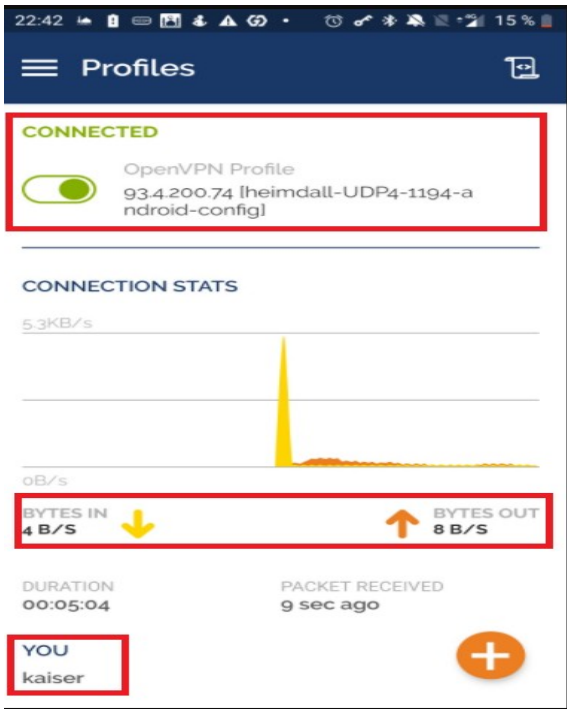








Voila la connexion est établie de mon smartphone connecté en 4G sur mon serveur Pfsense connecté sur la box Internet de mon fournisseur d'accès ; je peux vérifier mon accès à hermes avec un ping depuis mon smartphone



De même Sur l'interface web (Status+Openvpn] la connexion vpn du client Android est enregistré