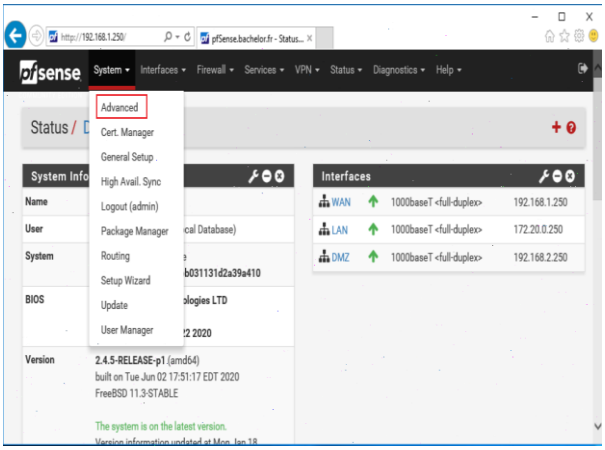
;

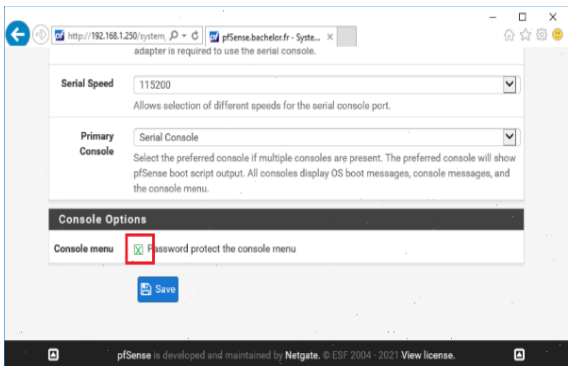
Sécurité

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

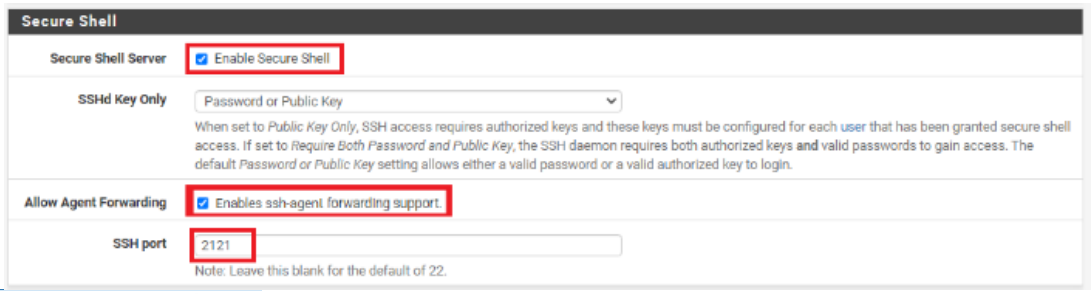


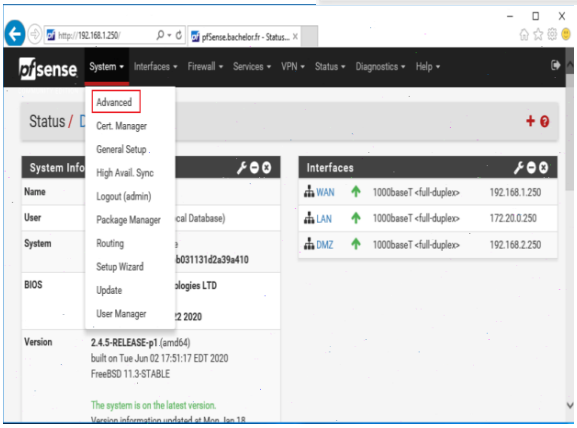


On constate que ma console à un login

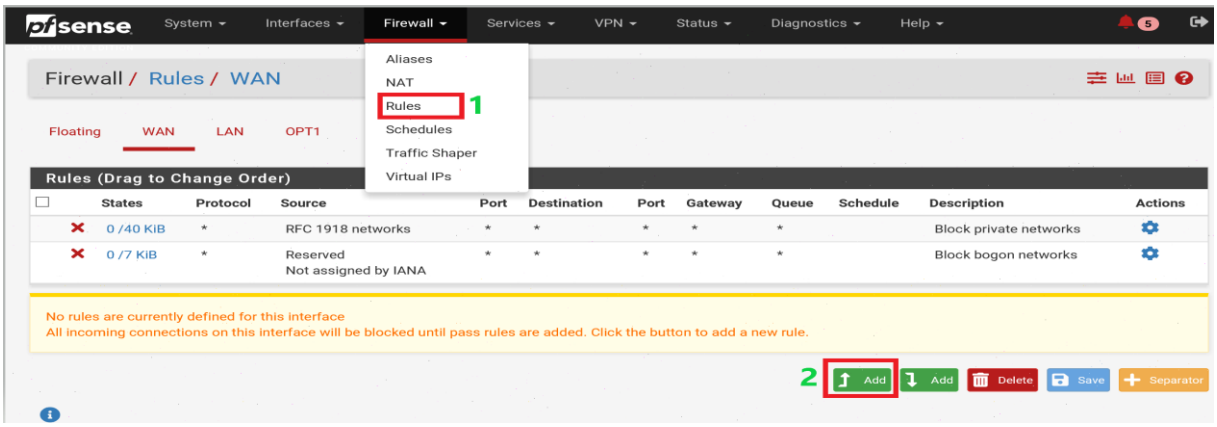
B- Sécurisez l'accès par ssh

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

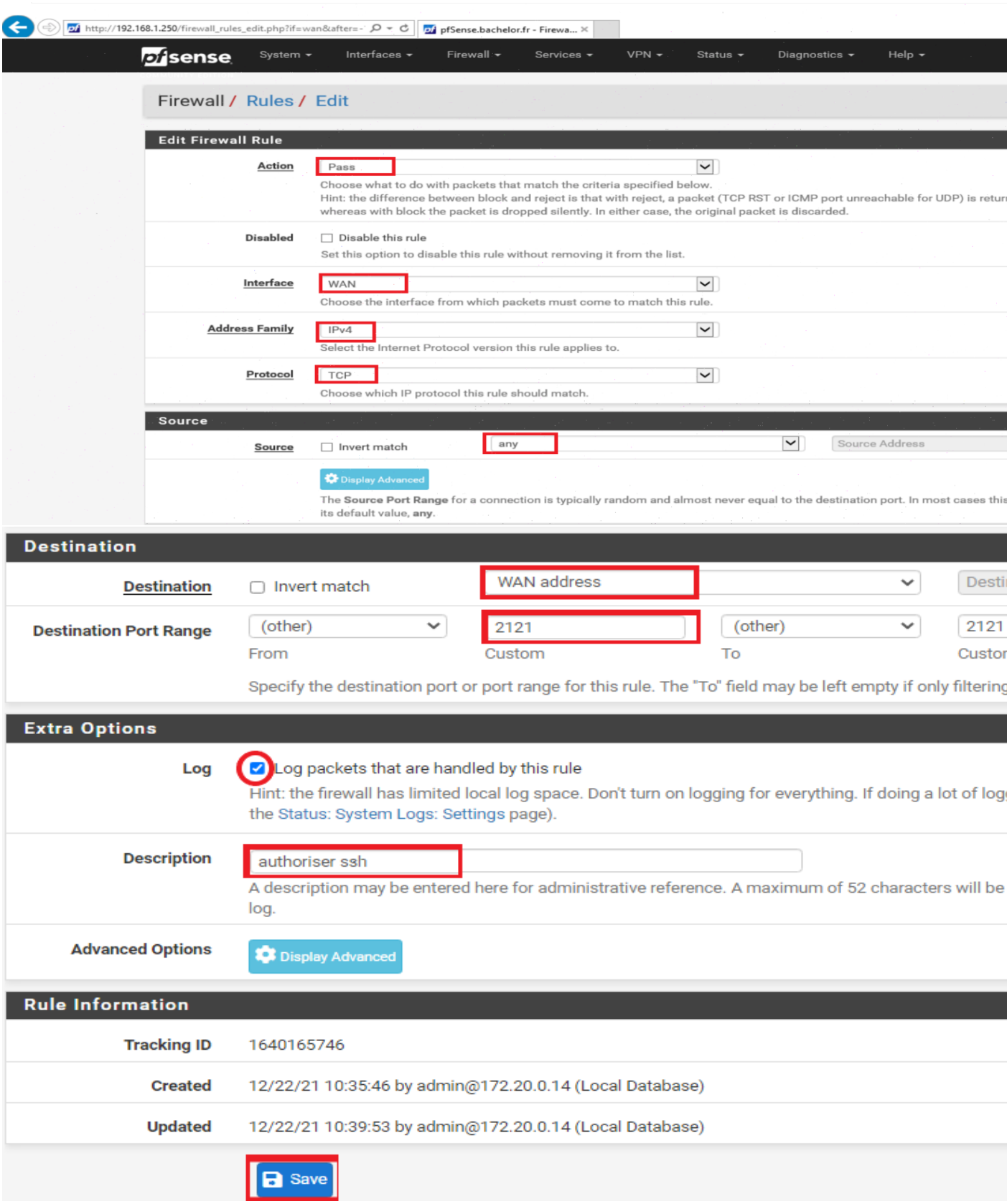




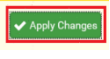
Maintenant il faut une **règle** autorisant **ssh** sur l'interface **Wan** on va dans le menu **interface +rule + ad**

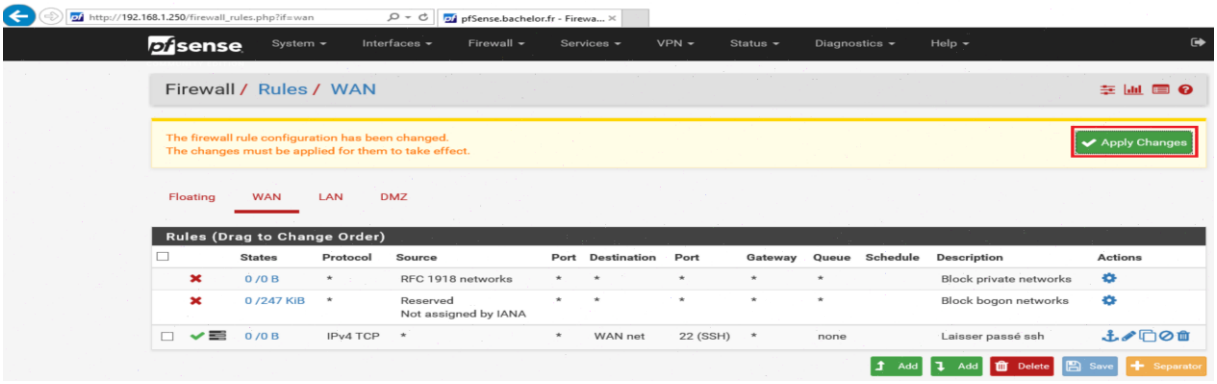


On rentre les choix ci-dessous après il ne faut pas oublier d'enregistrer et d'appliquer les changements comme indiqué dans ces captures d'écrans.



Après avoire enregistrer 

on applique les changements 

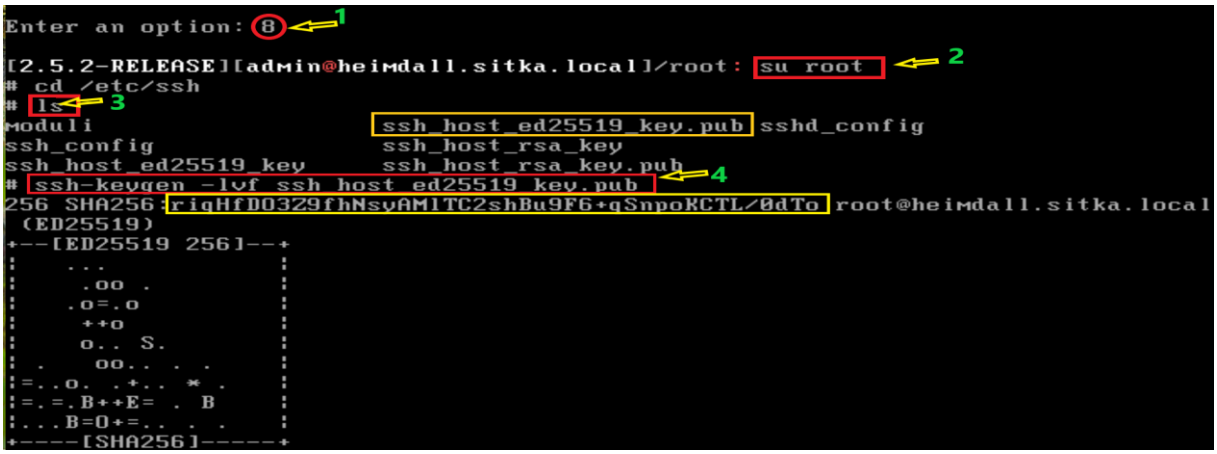


Attention sur Windows 2O16 ssh n'est pas installé nativement contrairement à Windows 2019 ou Windows 10 sur ces deux dernière version ssh est parmi les fonctionnalités qu'on peut installer. Donc pour Windows 2016 suivre la procédure du fichier ssh_2016.docs pour installer ssh

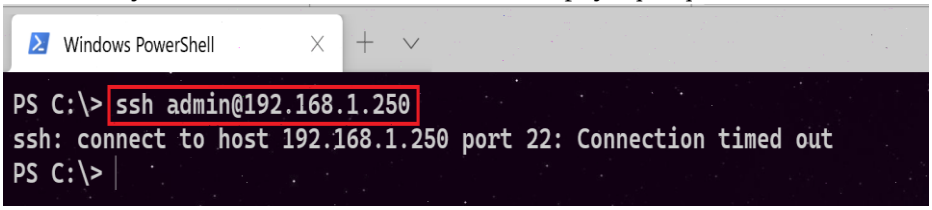
On teste la connexion à l'intérieure de notre périmètre j'utilise une des machines dans un Lan :
Je prends la machine AD je démarre le PowerShell et je me connecte sur une des interfaces de pfsense :
Le serveur pfsense m'envoie l'empreinte numérique de sa clé publique :

```
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:
```

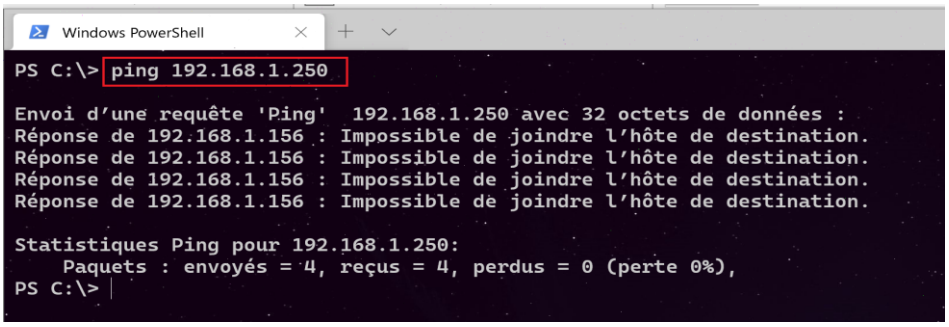
On peut vérifier si l'empreinte numérique sur le serveur ssh est la même que celle envoyée par le serveur j'affiche le contenu détaillé du répertoire /etc/ssh après je génère l'empreinte numérique de la clé publique **ssh_host_ed25519_key.pub**
en suivant les étapes **1+2+3+4**
En fin je compare les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



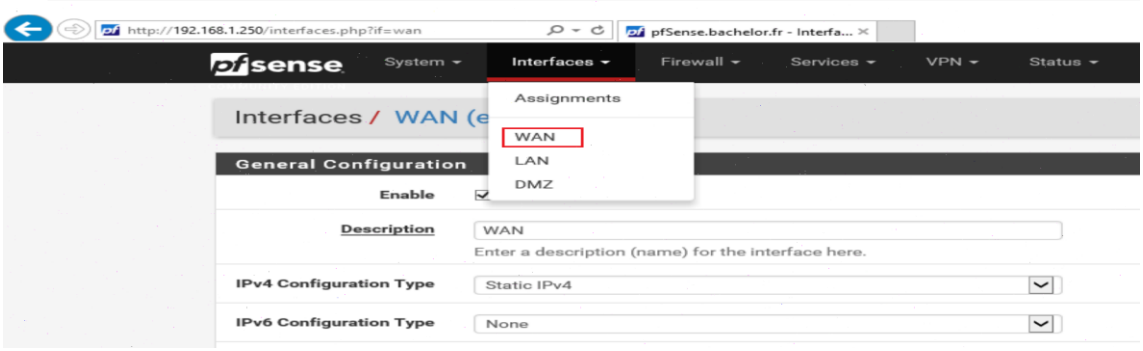
Maintenant on va tester la connexion en dehors de notre périmètre **Wan, sitka_Lan et opt_lan**
On va essayer une connexion de notre machine physique qui est en dehors de ce périmètre

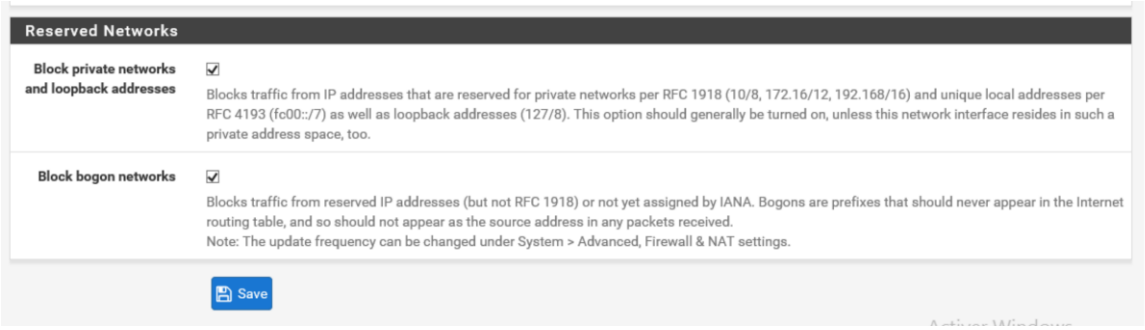


On remarque qu'il y'a **échec de connexion** ; on essaye de faire un **ping** sur cette interface, même constat

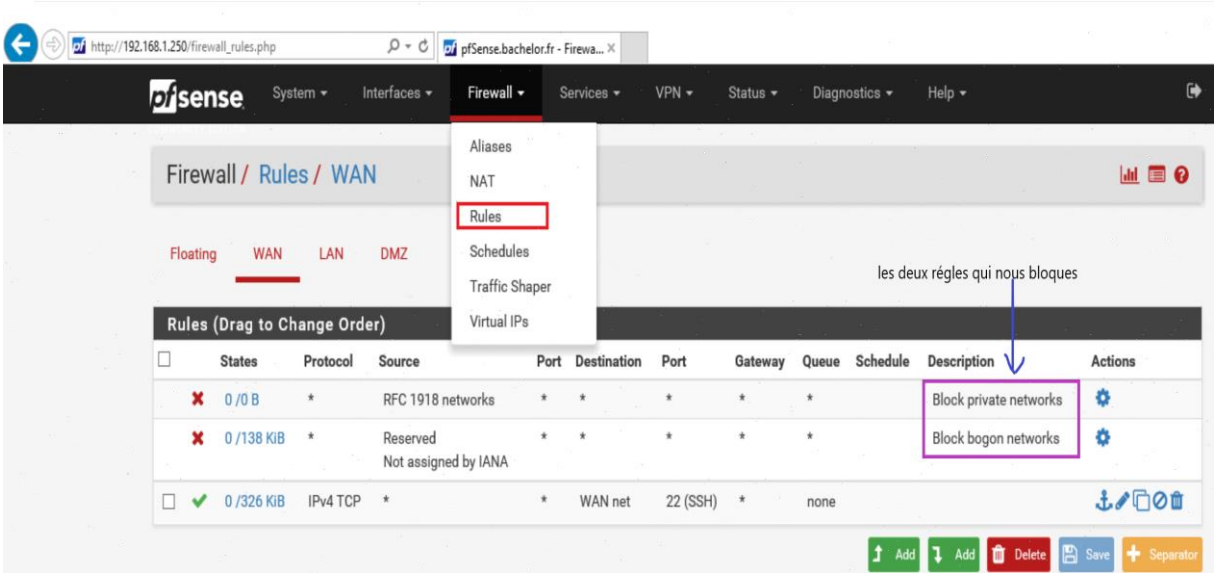


Cet échec est normal car PfSense bloque toutes requêtes venant d'une adresse privée en dehors de son périmètre **Wan, sitka_lan et opt_lan,** on peut vérifier ceci aisément en allant dans le menu **Interface + Wan** tout en bas de la page on trouve deux cases cochées ce qui explique ce blocage





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 :

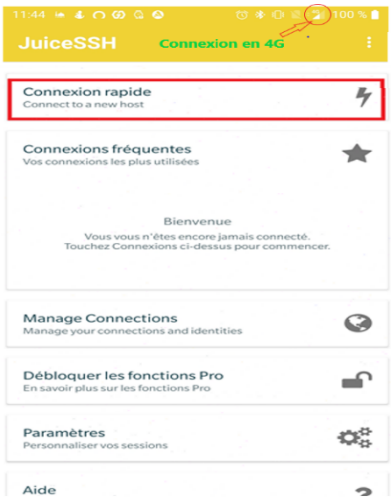
1- Il faut accéder à la boxe internet et ouvrir le port 22 en créant une redirection de port

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**

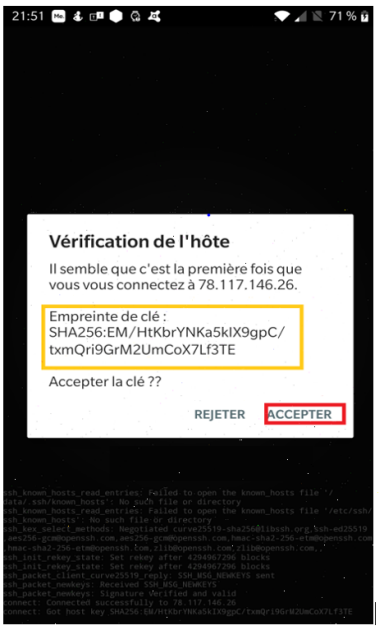
4- Sur notre smartphone il faut qu'on se mette en 4G et non en wifi car il na faut pas oublier que PfSense bloque les connexions provenant d'adresse IP en dehors de son périmètre.
5- On ouvre l'application et on commence à établir notre connexion ssh

On sélectionne connexion rapide

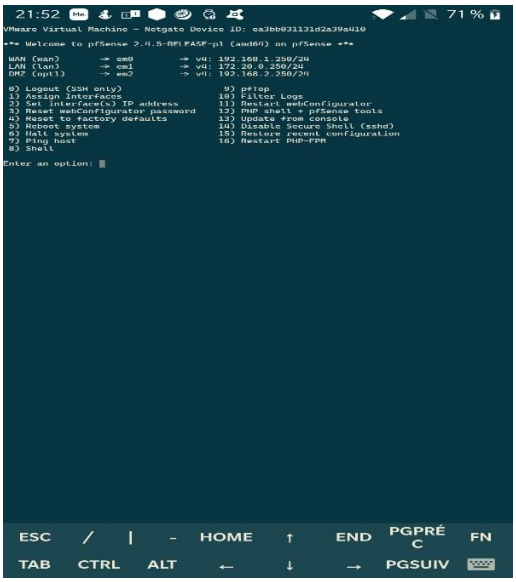


ssh admin@ adresse publique

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**



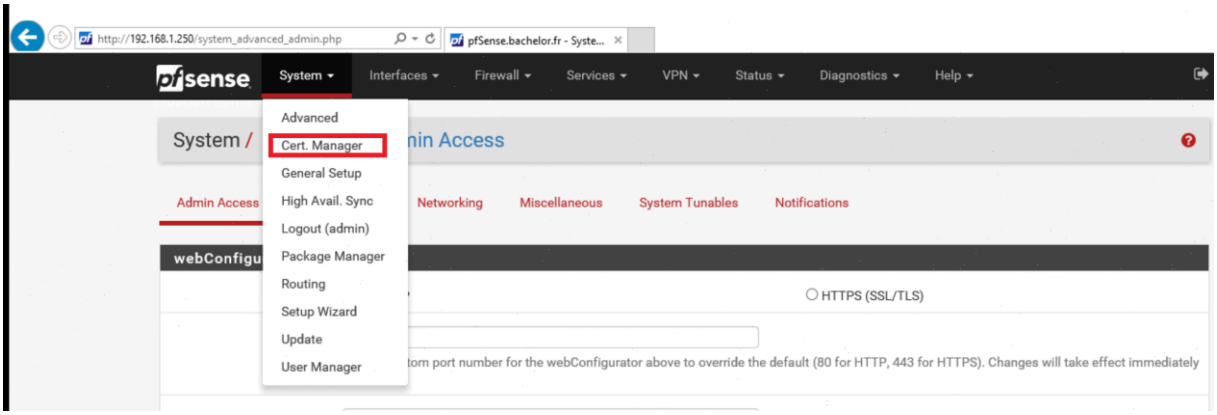
Après on tombe sur notre console PfSense



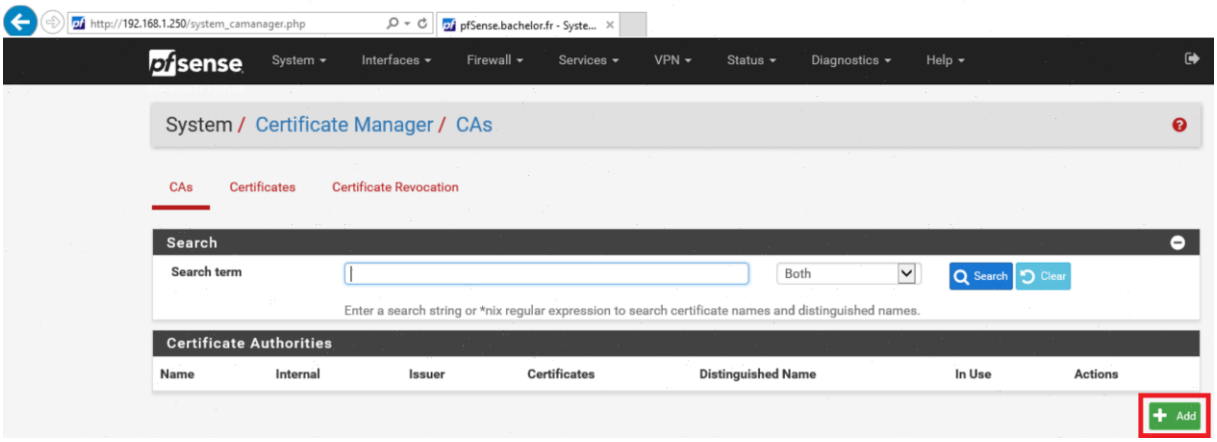
D- Sécurisez L'interface web par https

1- Créer une autorité de certification interne

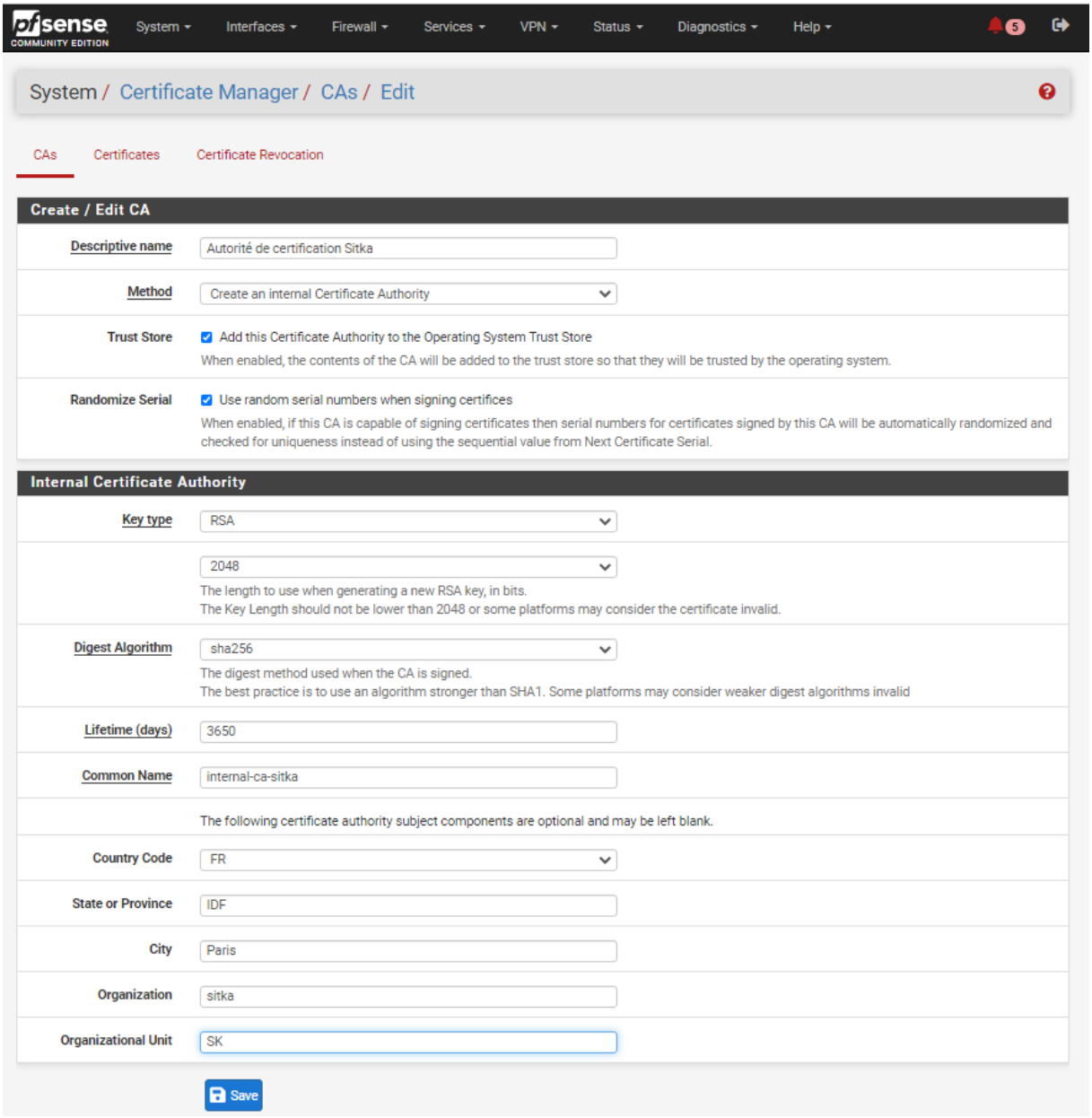
On va dans le menu **système + CertManager**



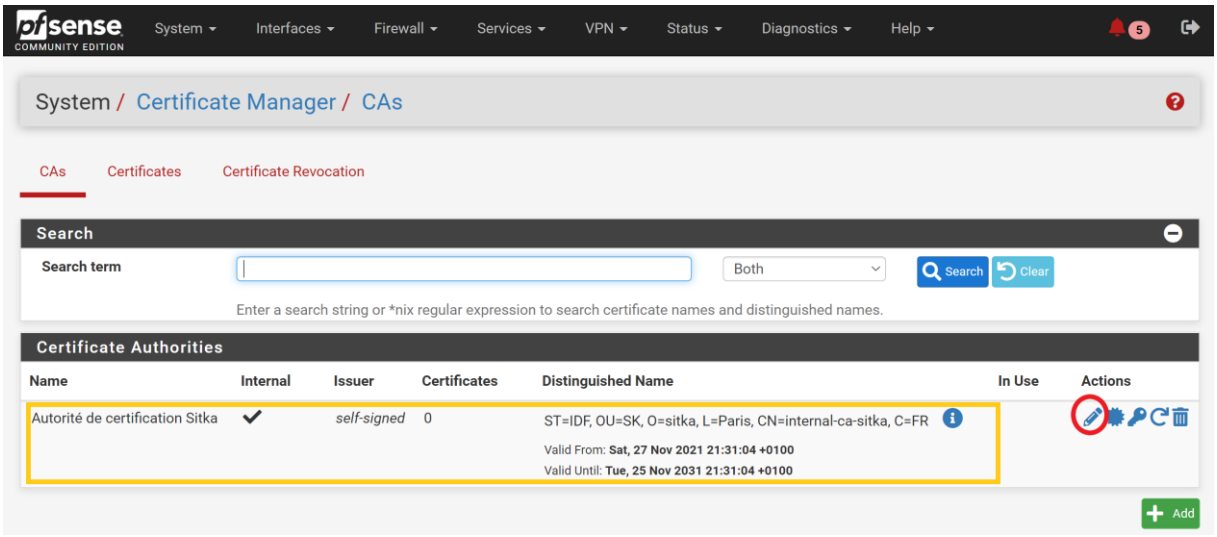
On commence à créer une autorité de certification interne



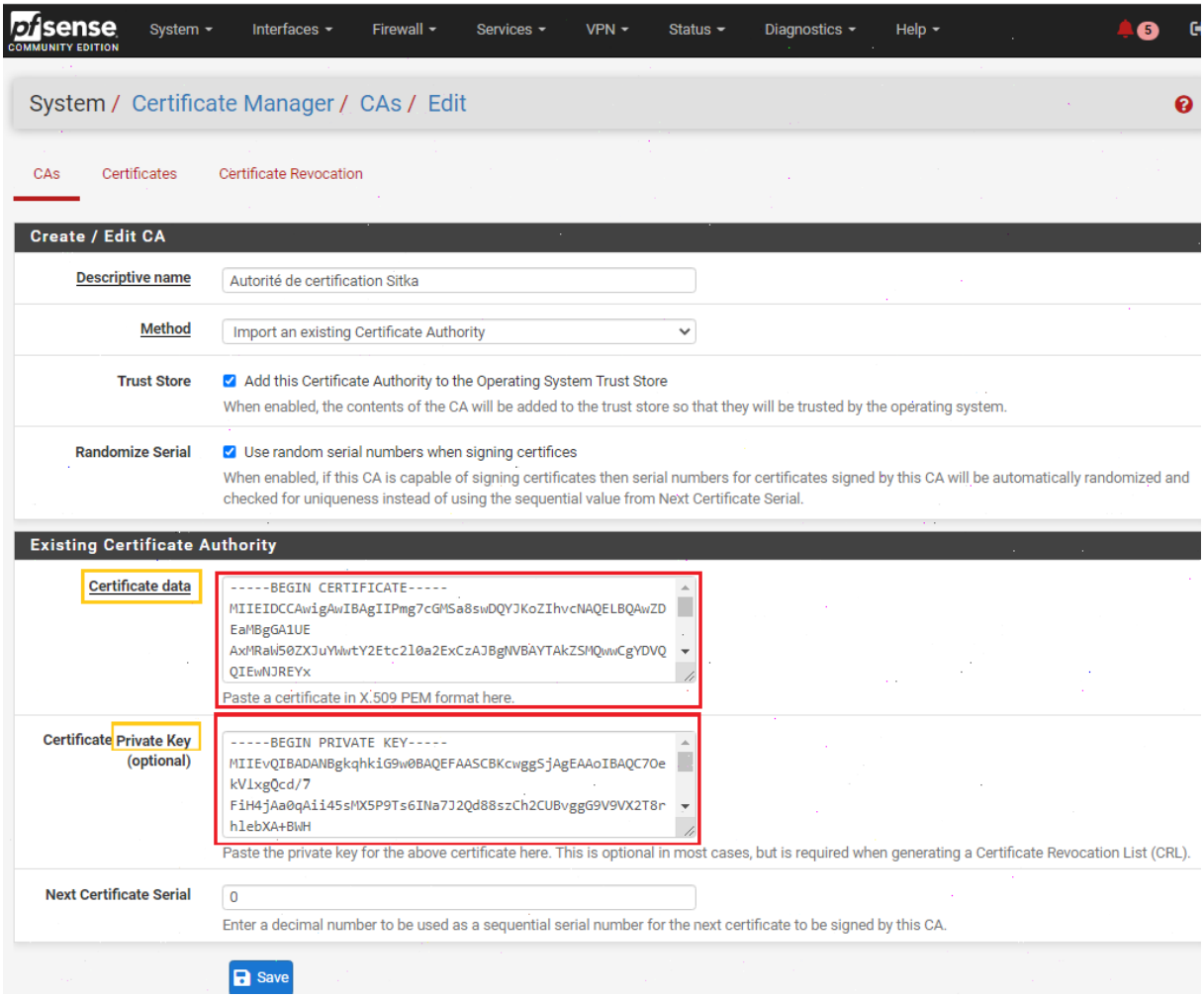
On remplit les champs suivants



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

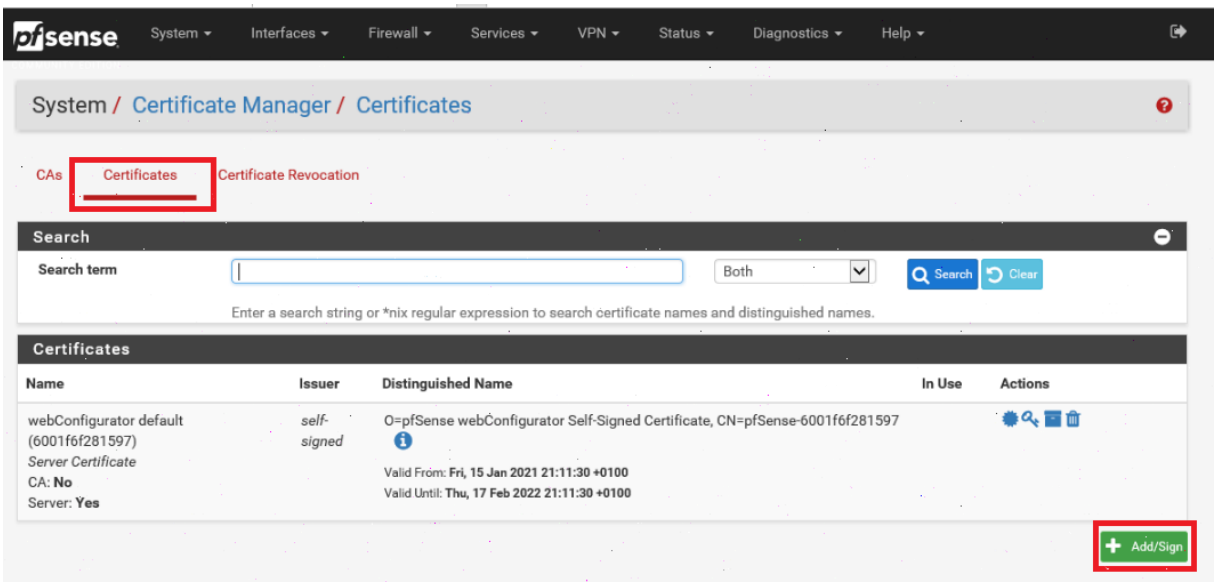


On affiche notre certificat et la clé publique qui lui est associé

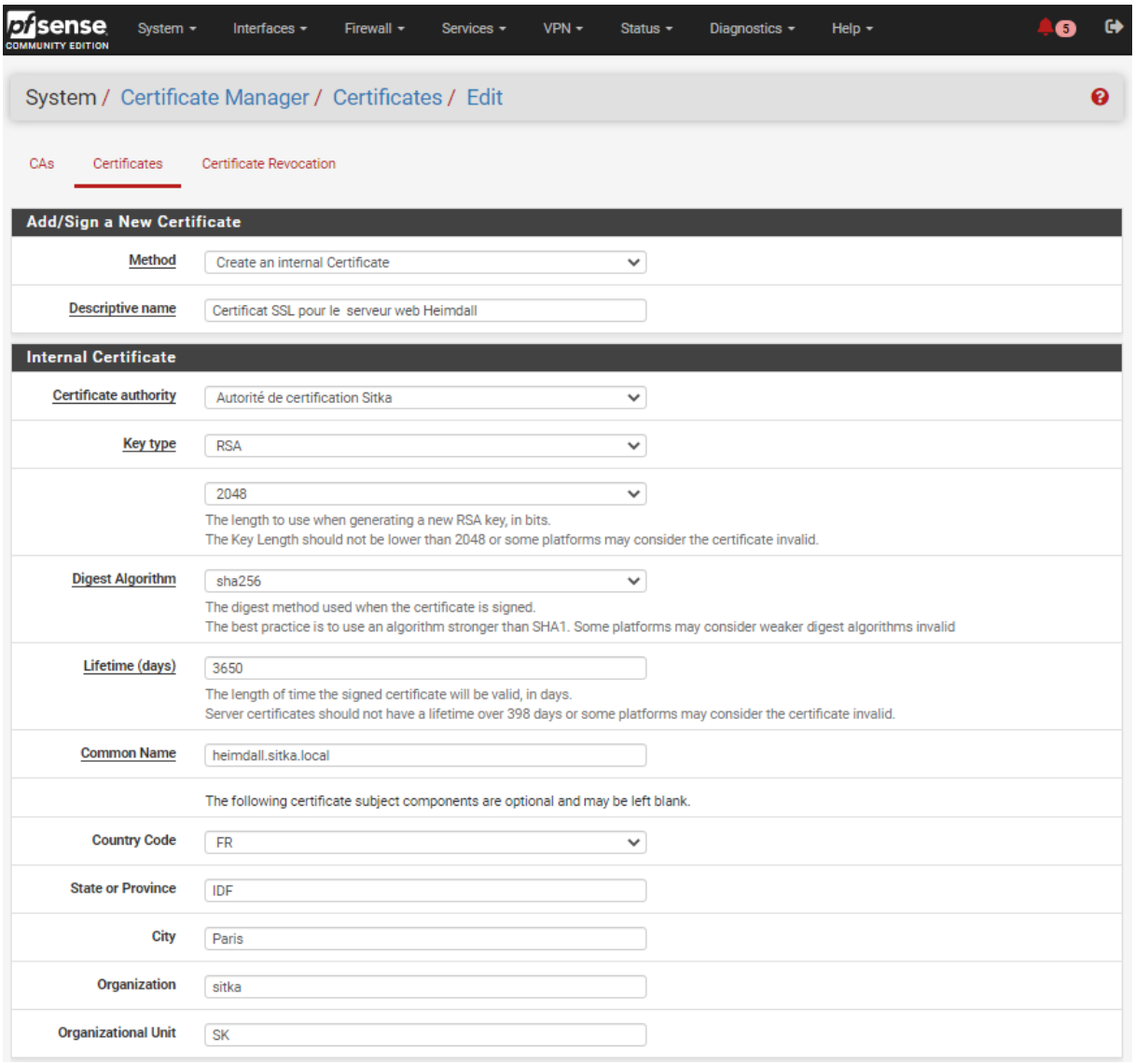


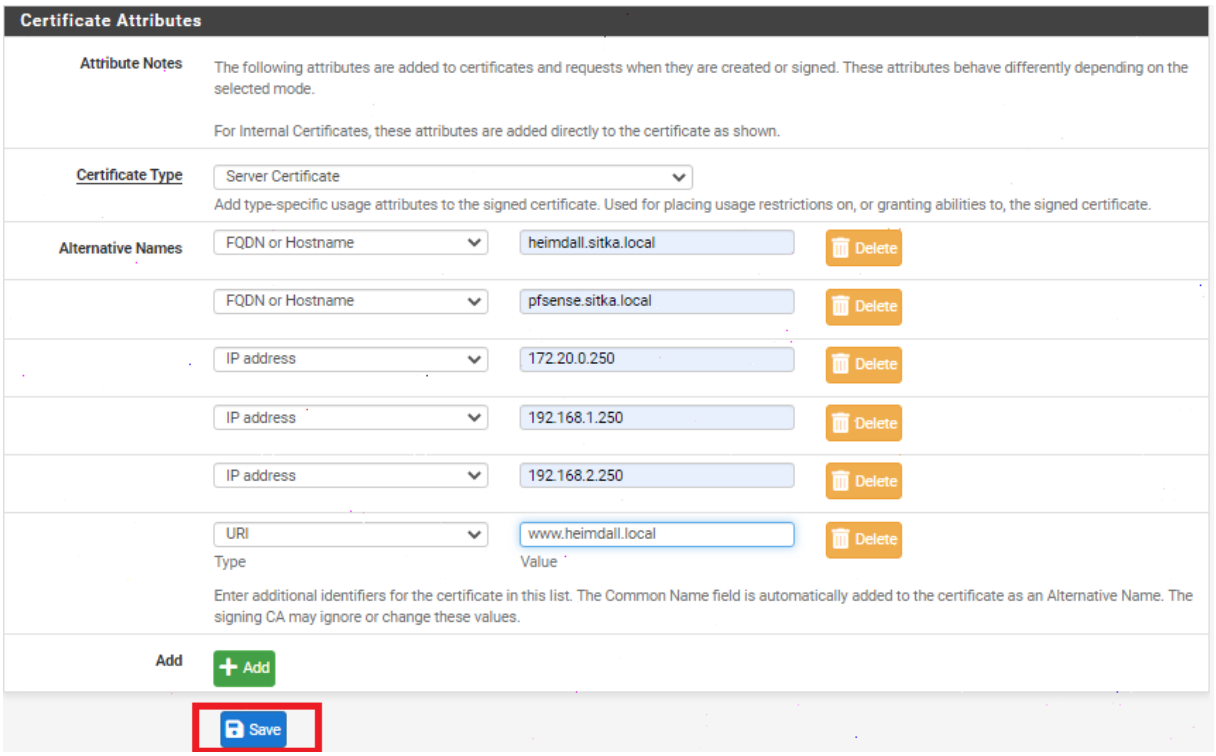
2- Générer un certificat web

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

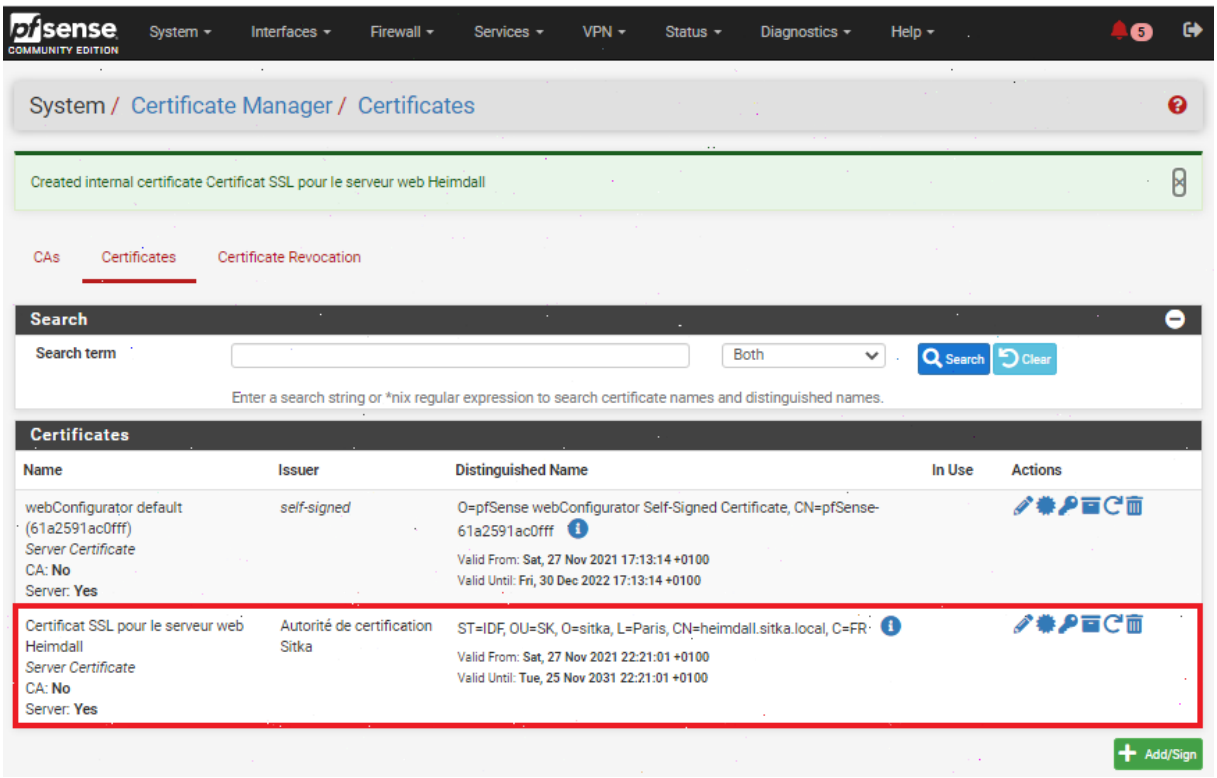


ci-dessous les champs remplie pour créer notre certificat


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



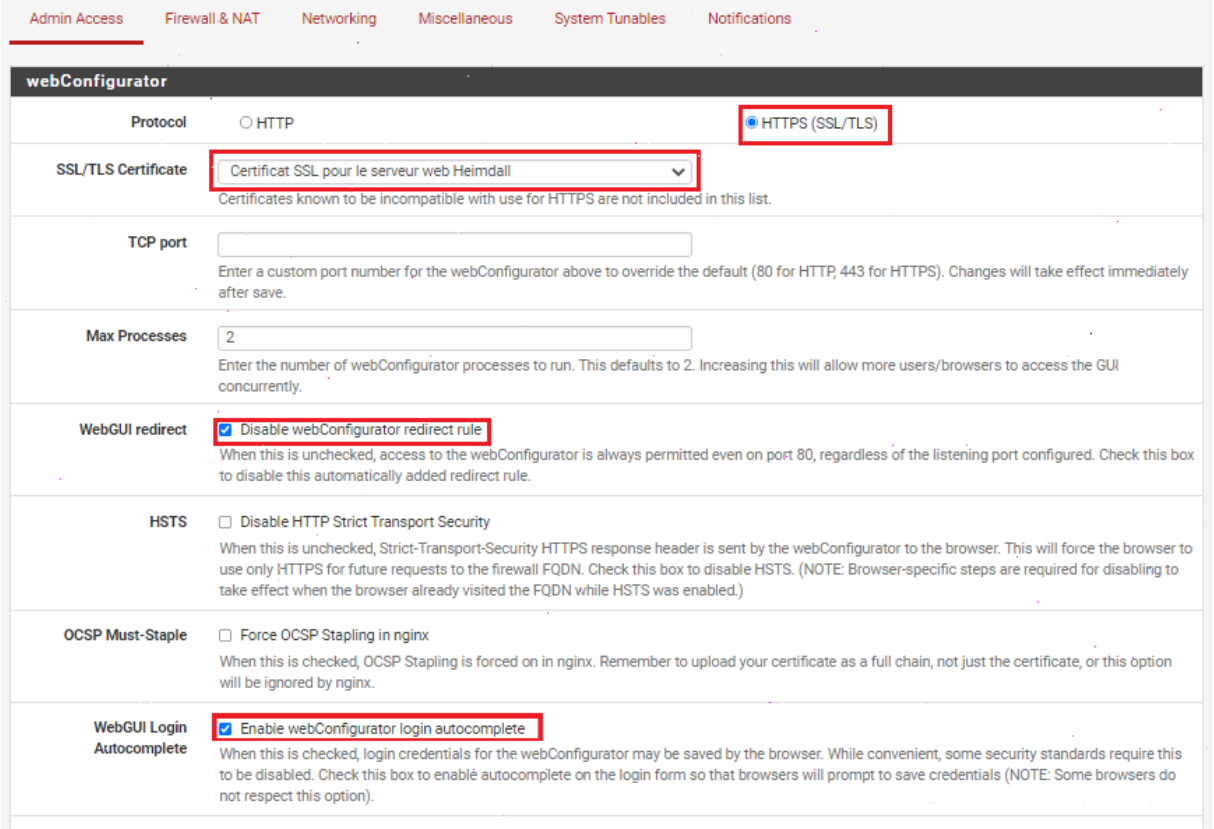
Une fois qu'on enregistre notre certificat apparait



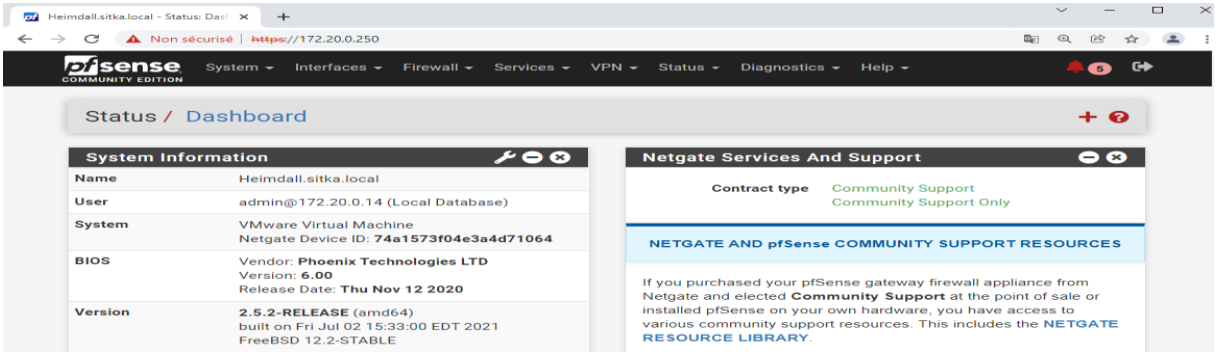
3- Injecter le certificat web dans mon serveur PfSense

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

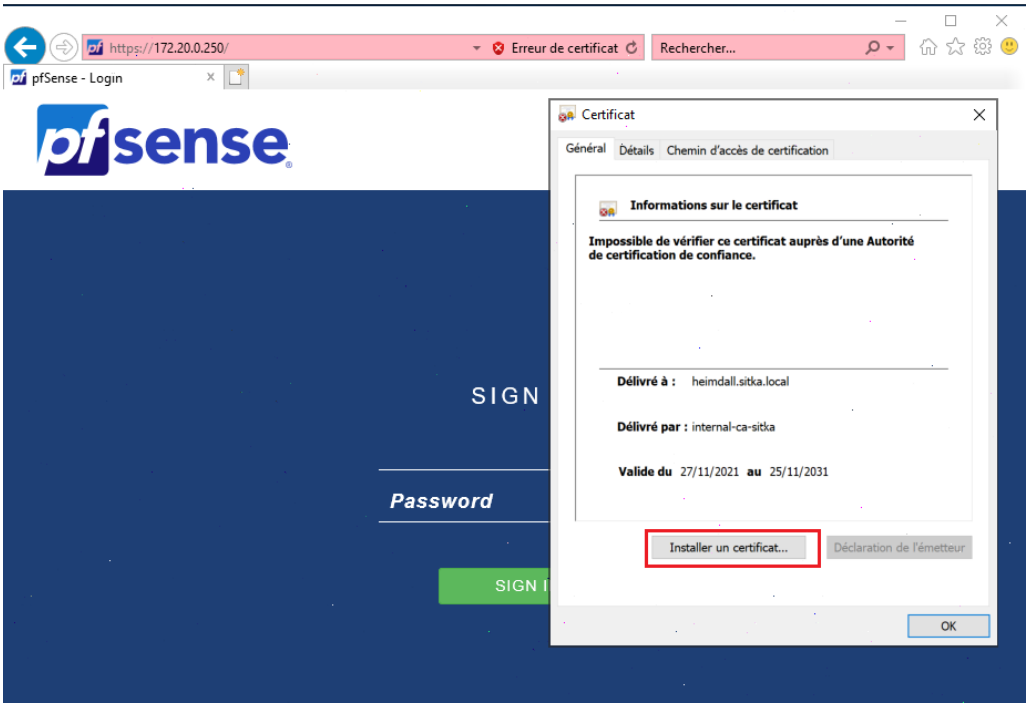
- On sélectionne notre certificat crée
- On laisse le port par défaut
- On laisse 2 en nombre de connexion simultané c'est-à-dire 2 personne max peuvent se connecter sur l'interface web PfSense
- On refuse la connexion en http
- On refuse que le navigateur enregistre les données de connexion



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