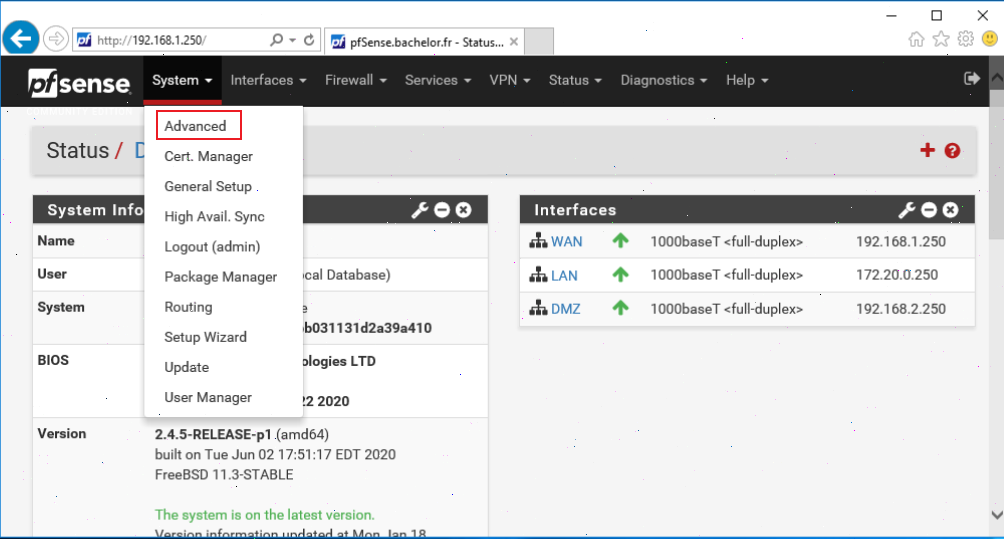
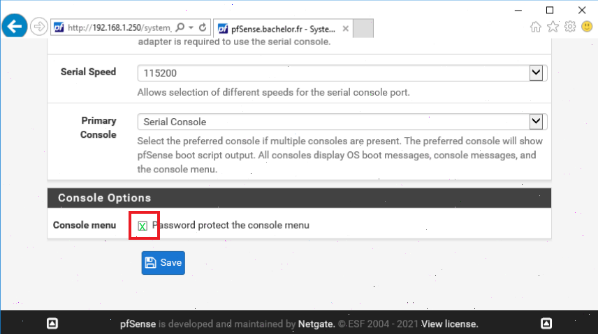
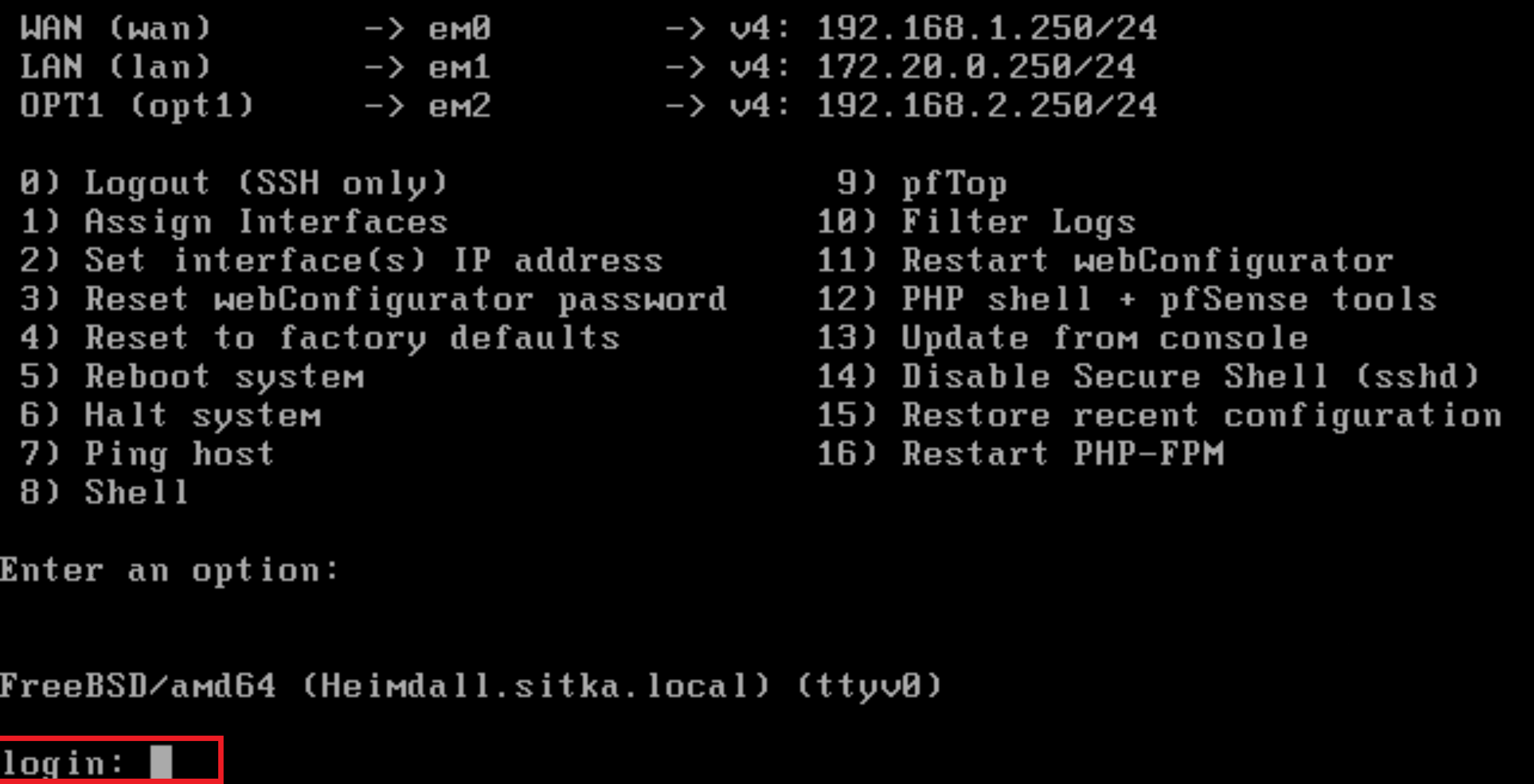
**Sécurité**

1. Sécurisez la console par mot de passe
2. Sécurisez l’accès par ssh
3. Sécurisez L’interface web par https
4. Créer une autorité de certification interne
5. Générer un certificat web
6. Injecter le certificat web dans mon serveur pfsense
7. Sécuriser la console Pfsense ss vous cochez la case console menu et vous

Sauvegardez

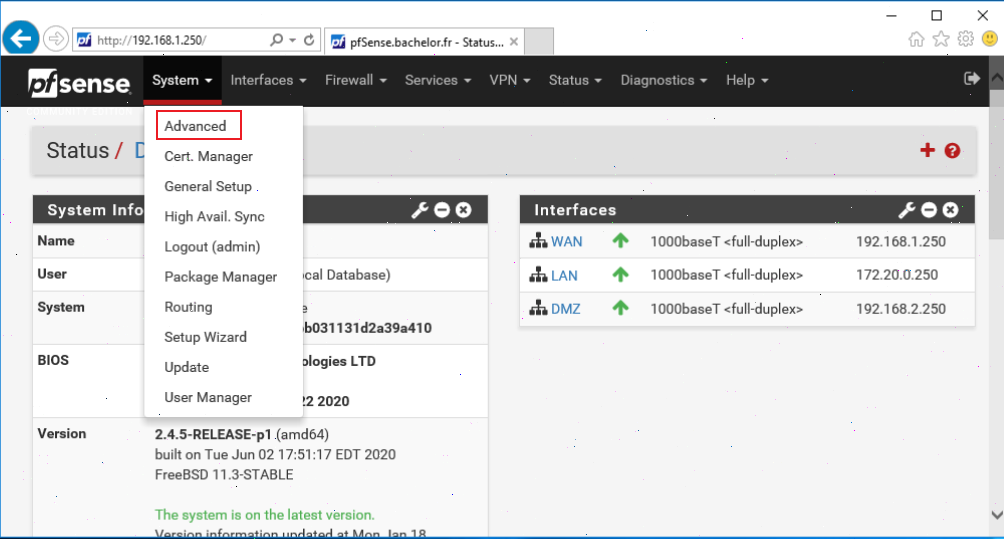
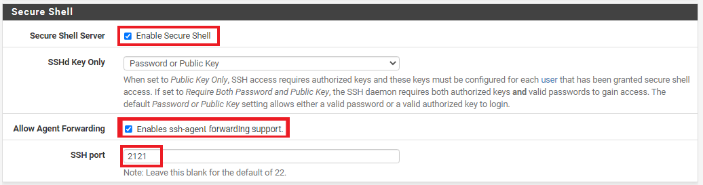


On constate que ma console à un login

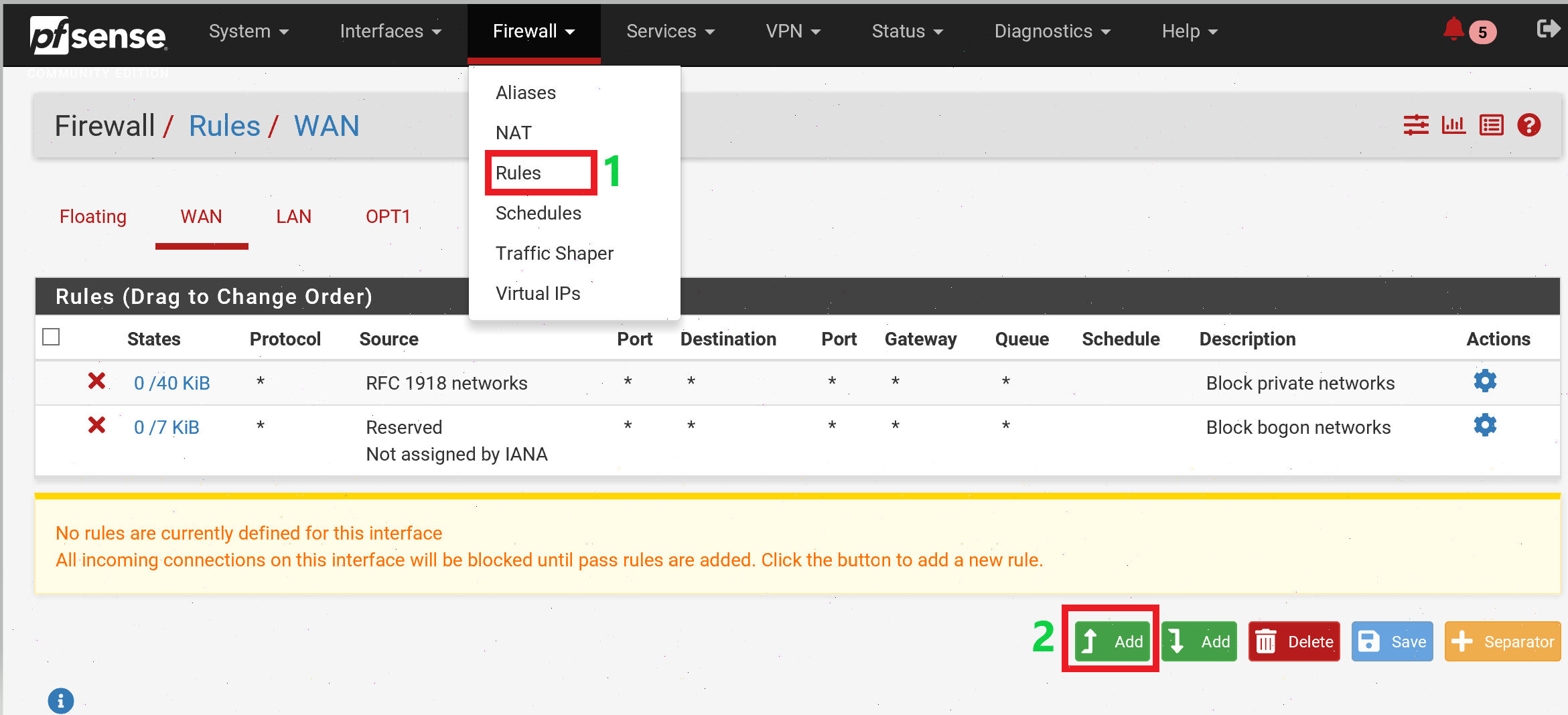


1. **Sécurisez l’accès par ssh**

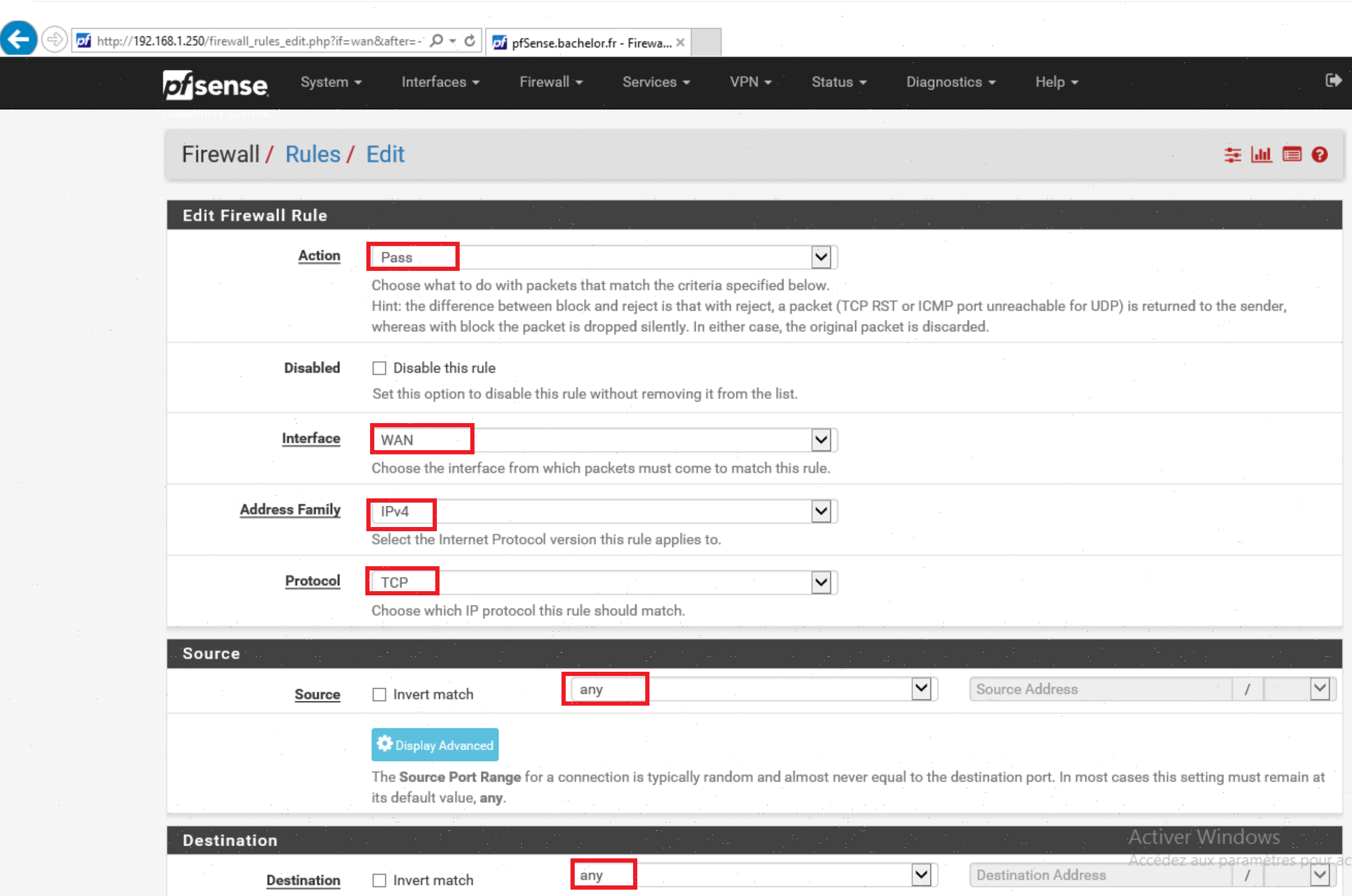
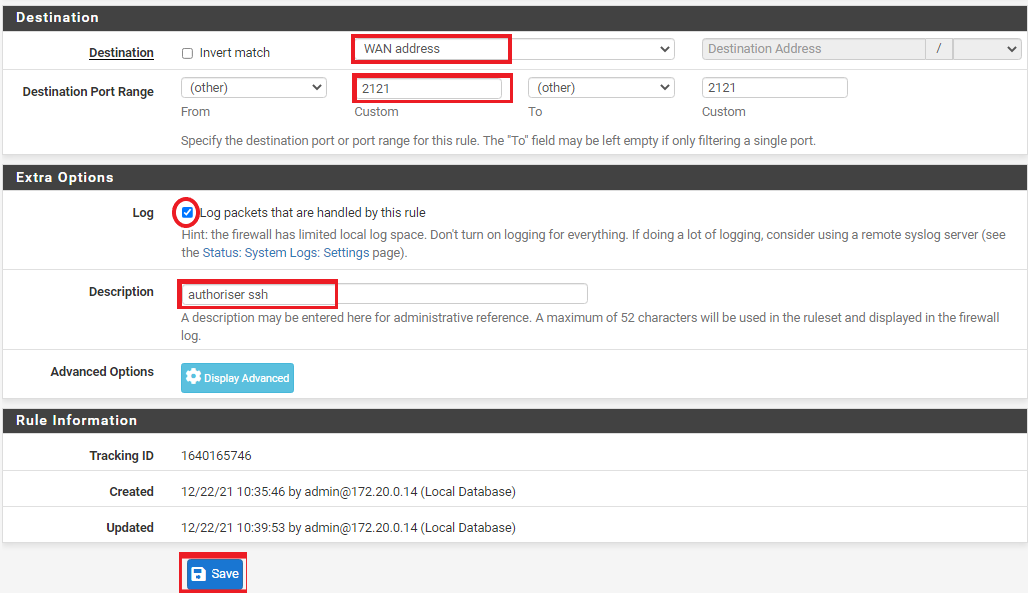
On active ssh pour accéder à la console de manière sécurisée on change le port par défaut en (2121) en terme de sécurité il est toujours conseillé de changer les port par défaut; on peut aussi faire une authentification avec clé **privé/publique** au lieu d’une authentification par mot de passe

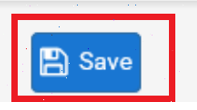


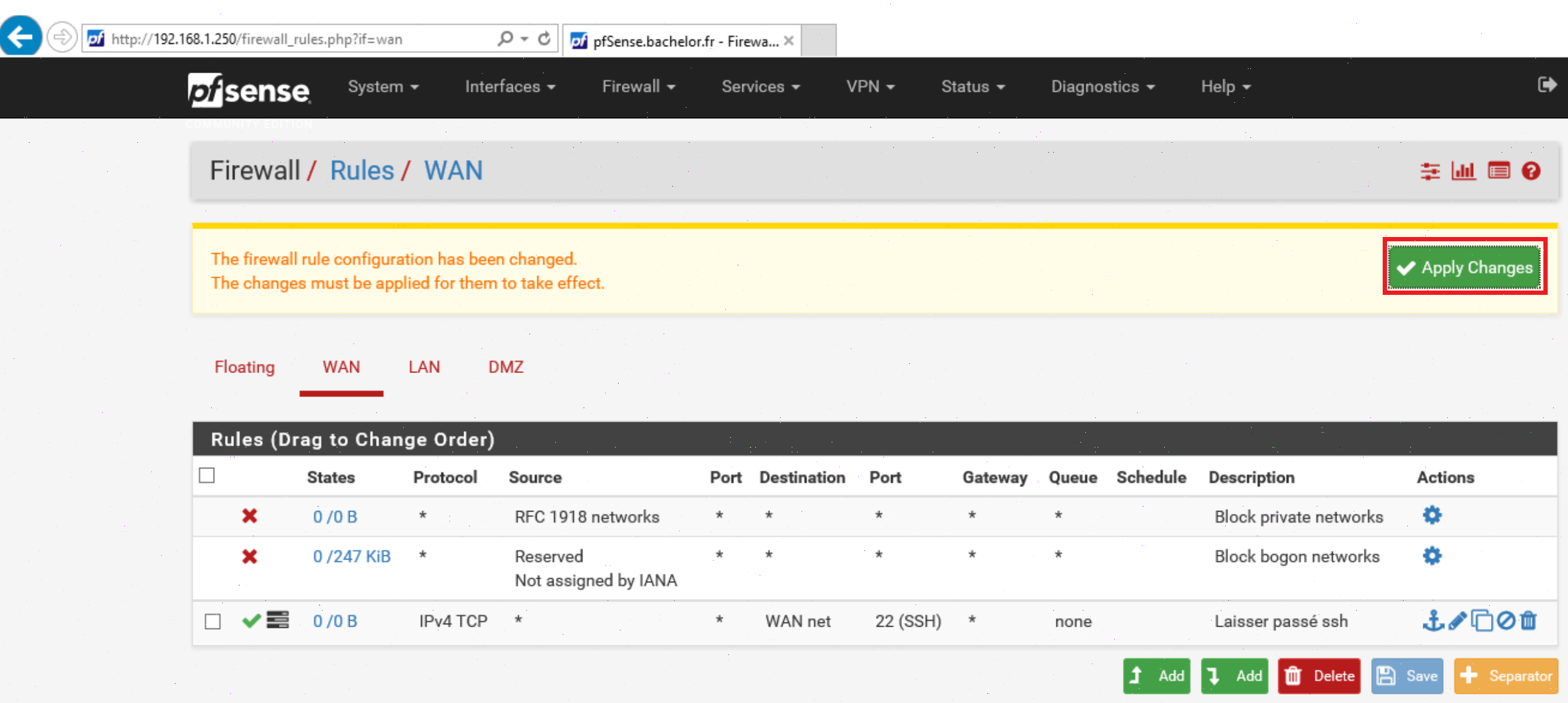
Maintenant il faut une **règle** autorisant **ssh** sur l’interface **Wan** on va dans le menu **interface +rule + ad**



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



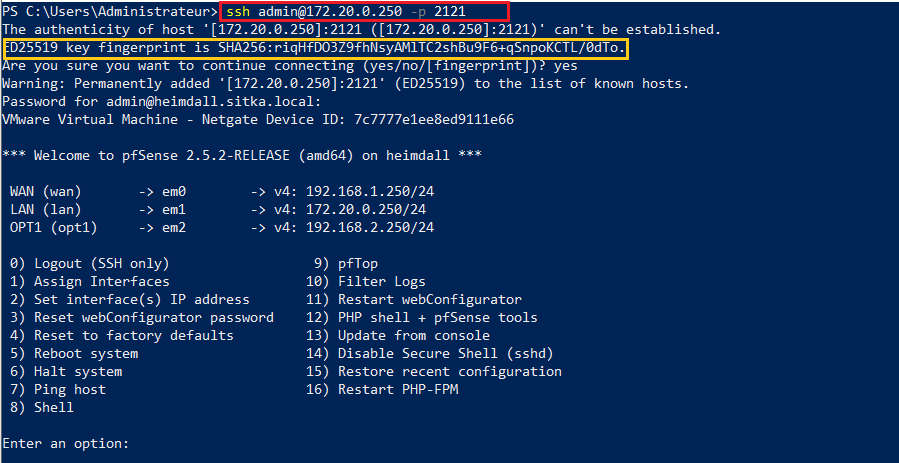
**Attention** sur Windows 2O16 ssh n’est pas installé nativement contrairement à Windows 2019 ou Windows 10 sur ces deux dernière version ssh est parmi les fonctionnalités qu’on peut installer.

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 :

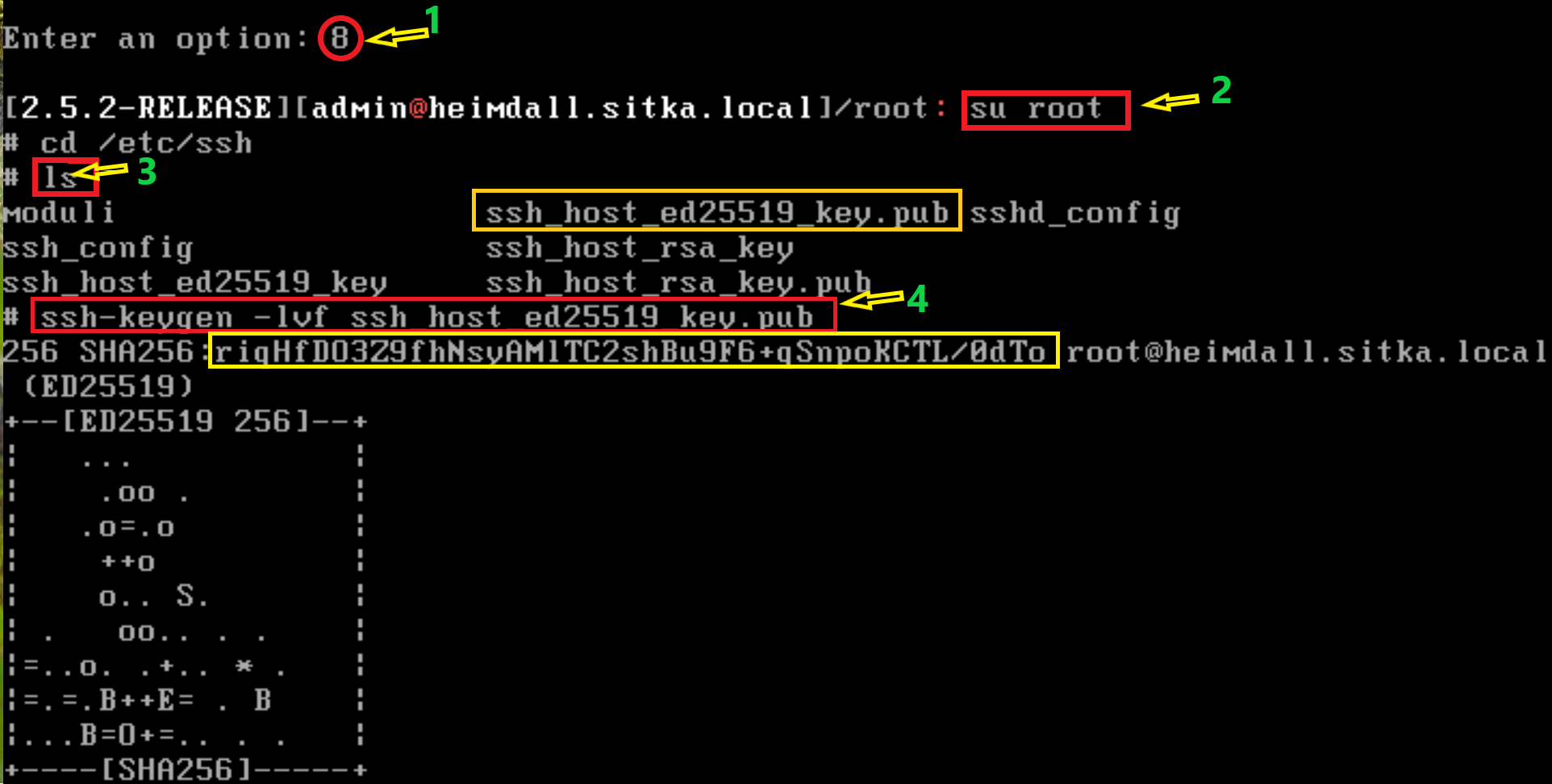
Le serveur pfsense m’envoie l’empreinte numérique de sa clé publique :



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**

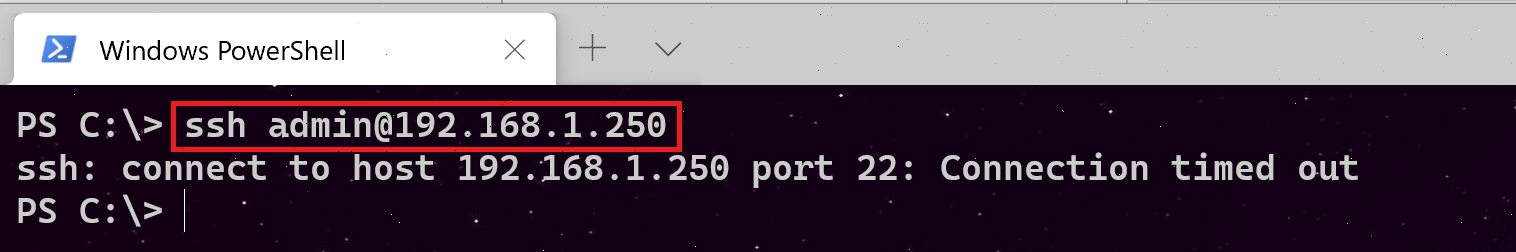
en suivant les étapes **1+2+3+4**

En fin je compare les deux empreintes on constate qu’elles sont identiques

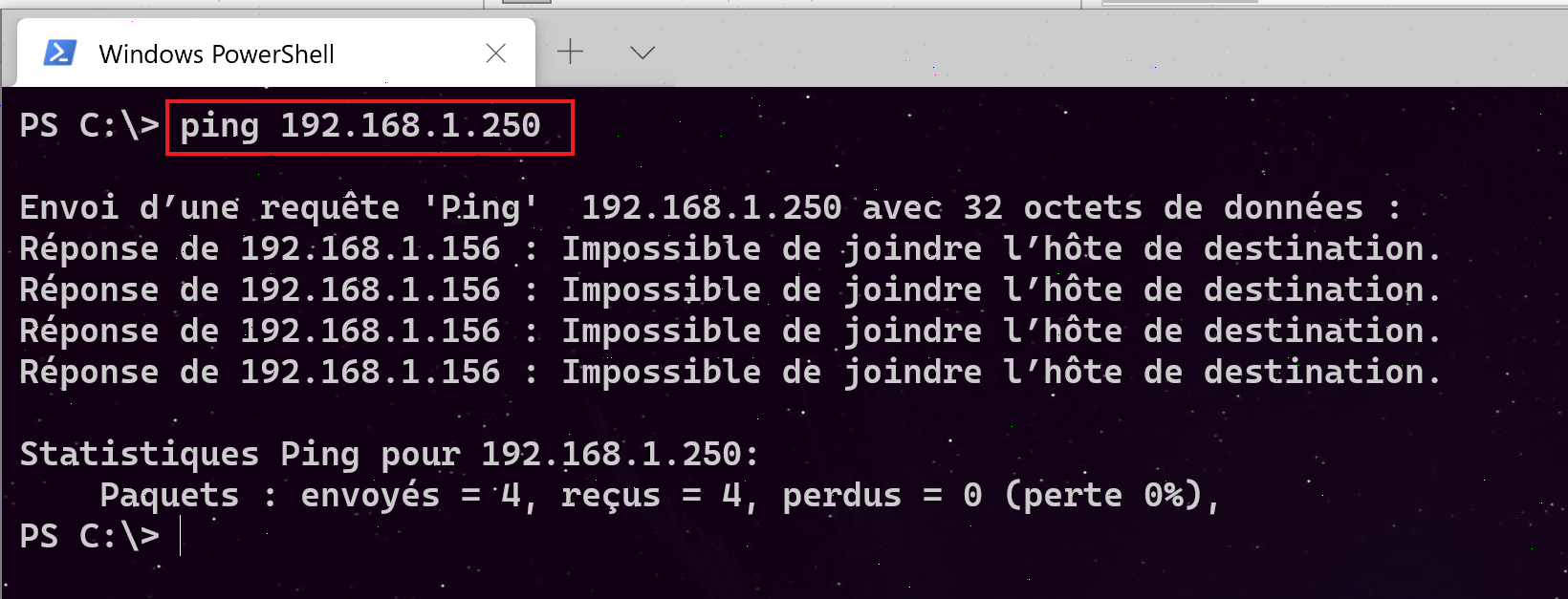


Maintenant on va tester la connexion en dehors de notre périmètre **Wan, sitka\_Lan et opt\_lan**

On va essayer une connexion de notre machine physique qui est en dehors de ce périmètre

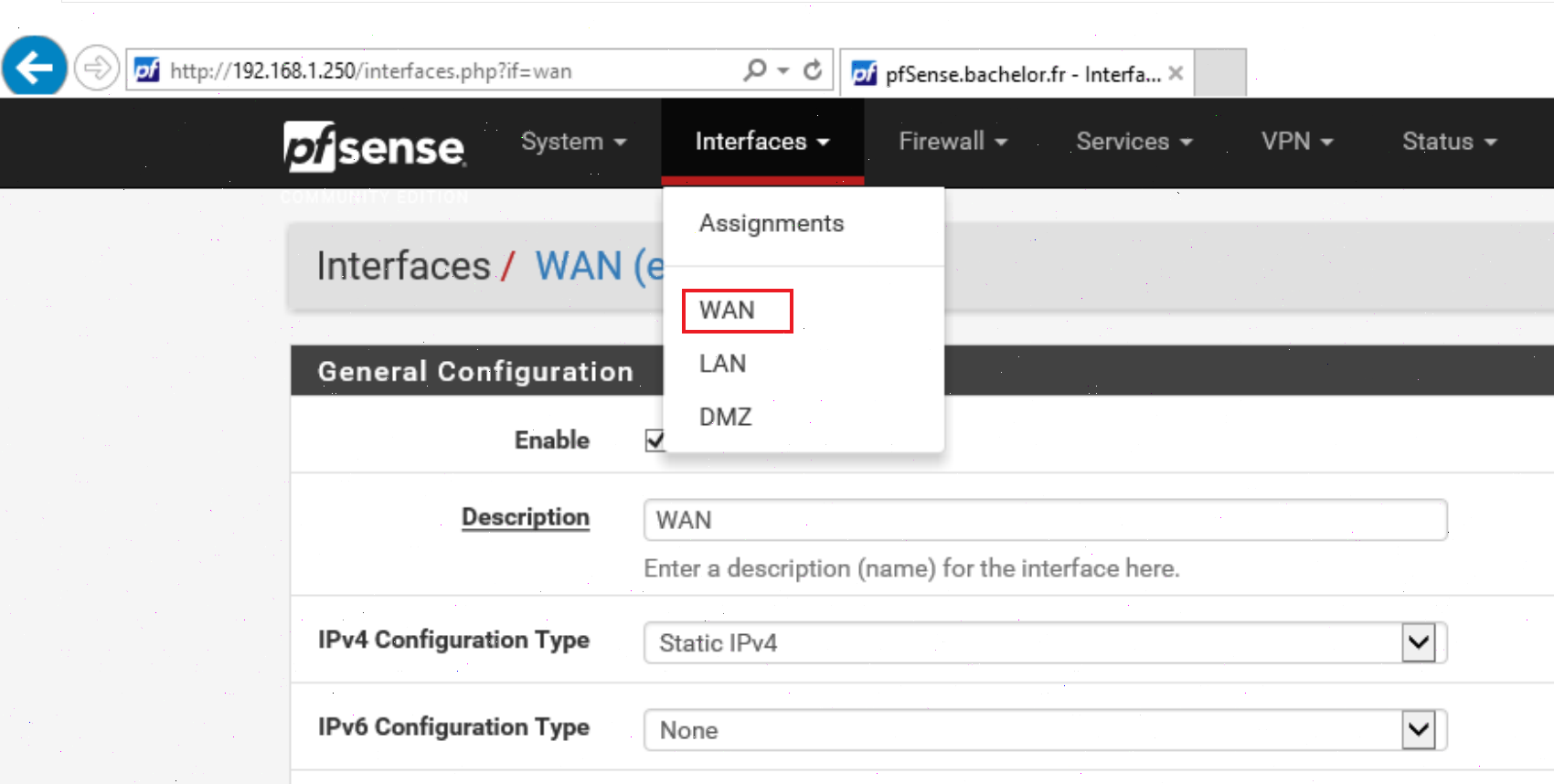


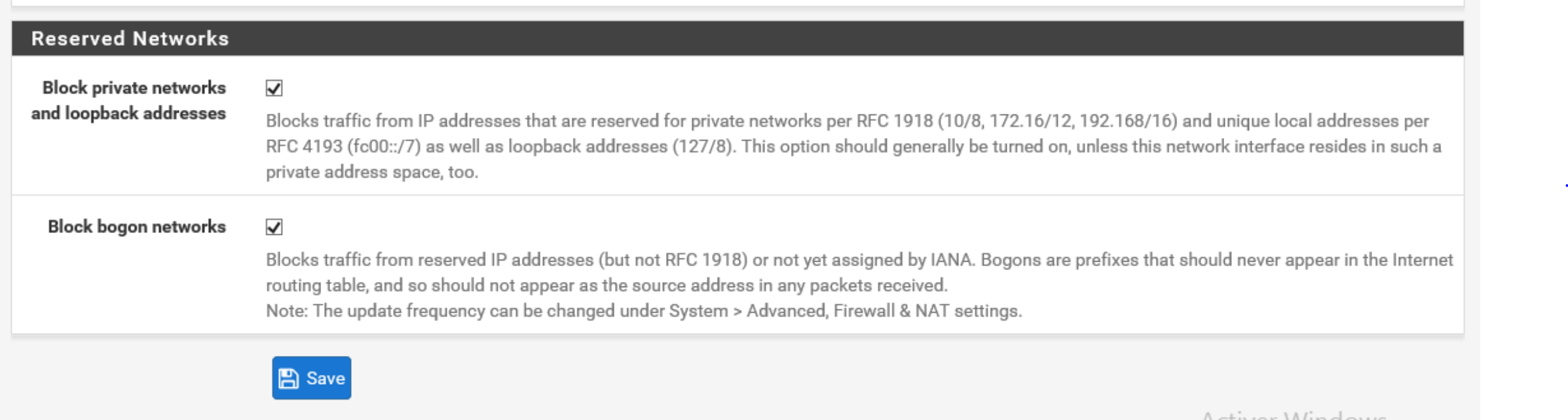
On remarque qu’il y’a **échec de connexion** ; on essaye de faire un **ping** sur cette interface, même constat



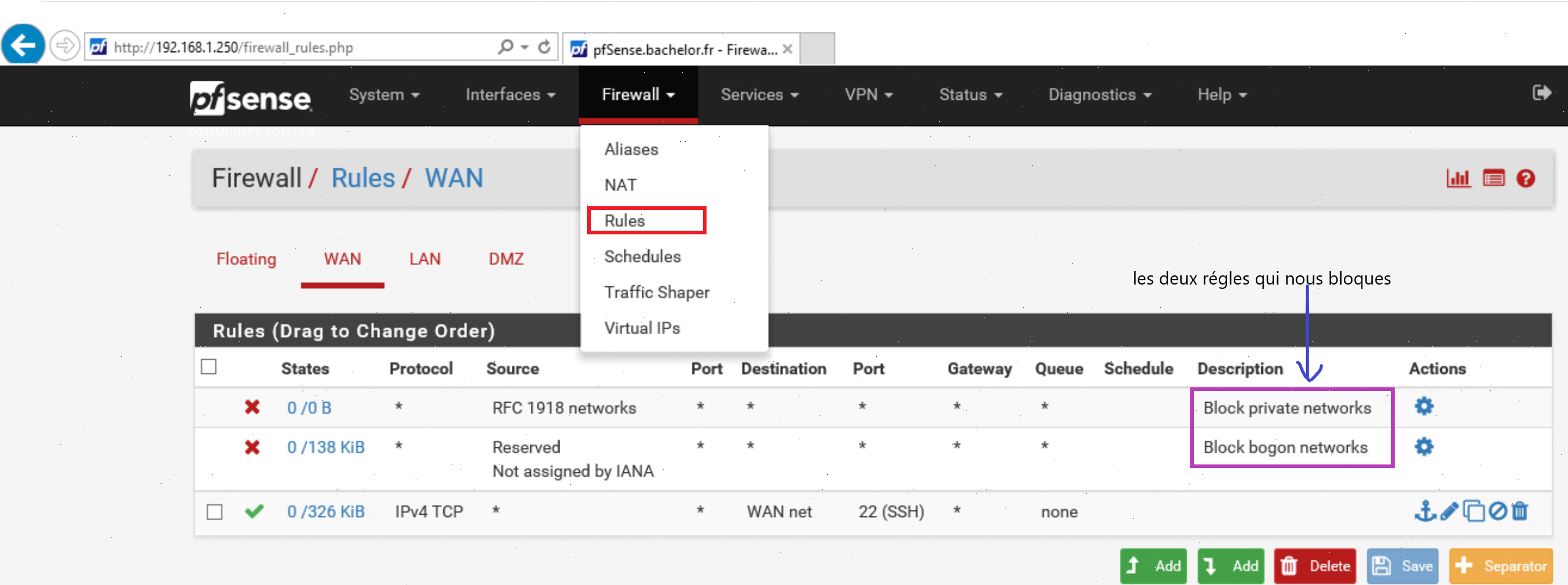
Cet échec est normal car PfSense bloque toutes requêtes venant d’une adresse privée en dehors de son périmètre **Wan, sitka\_lan et opt\_lan,** on peut vérifier ceci aisément en allant dans le menu

**Interface + Wan** tout en bas de la page on trouve deux cases cochées ce qui explique ce blocage





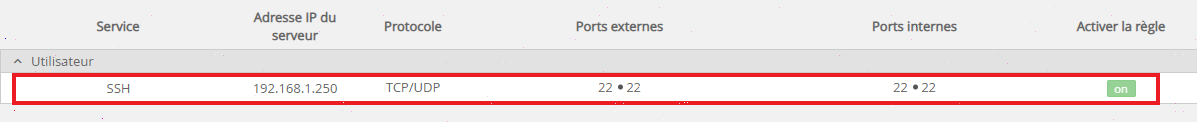
On trouve la même chose dans les règles par défaut de l’interface wan



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

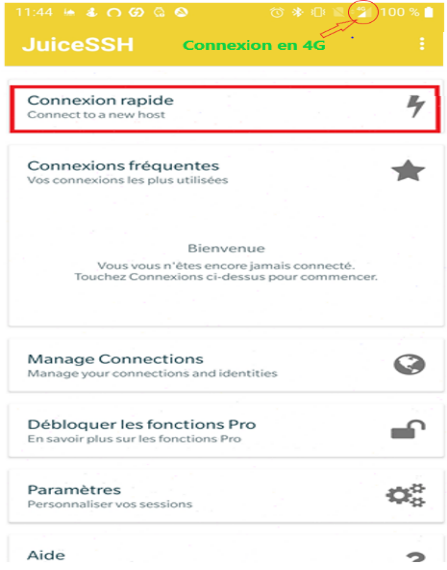


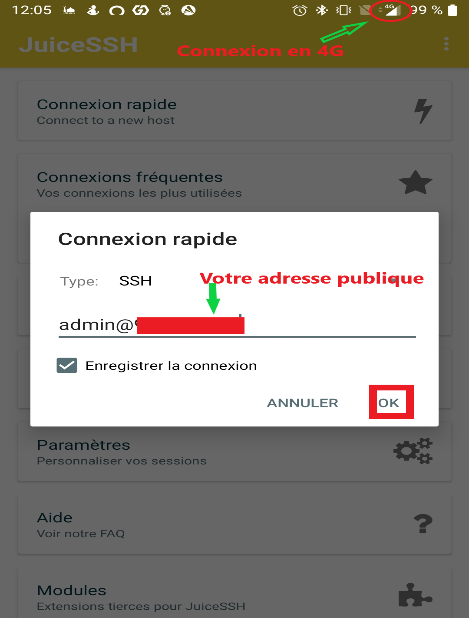
1. Ensuite il faut déterminer notre adresse publique soit à partir de la boxe ou un site internet [http://www.whatismyip.com](http://www.whatismyip.com/)
2. Après sur notre smartphone on télécharge un client ssh sur  google store **Juicessh**



1. 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.
2. On ouvre l’application et on commence à établir notre connexion ssh

On sélectionne connexion rapide ssh admin@ adresse publique



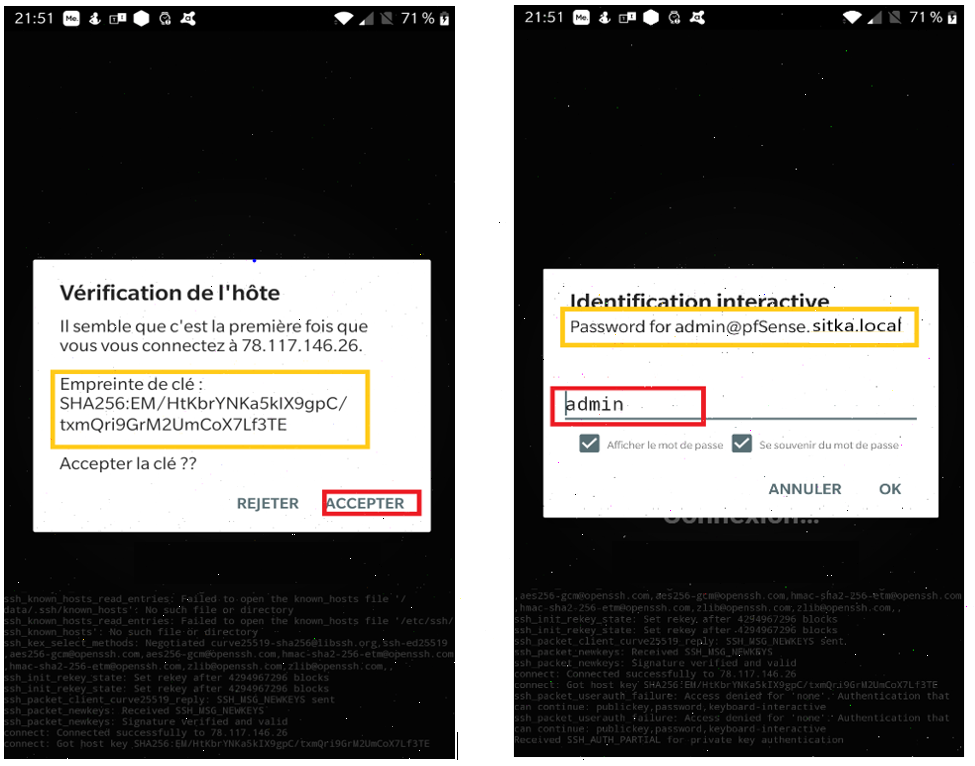


Le serveur nous envoie l’empreinte de sa clé publique

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**

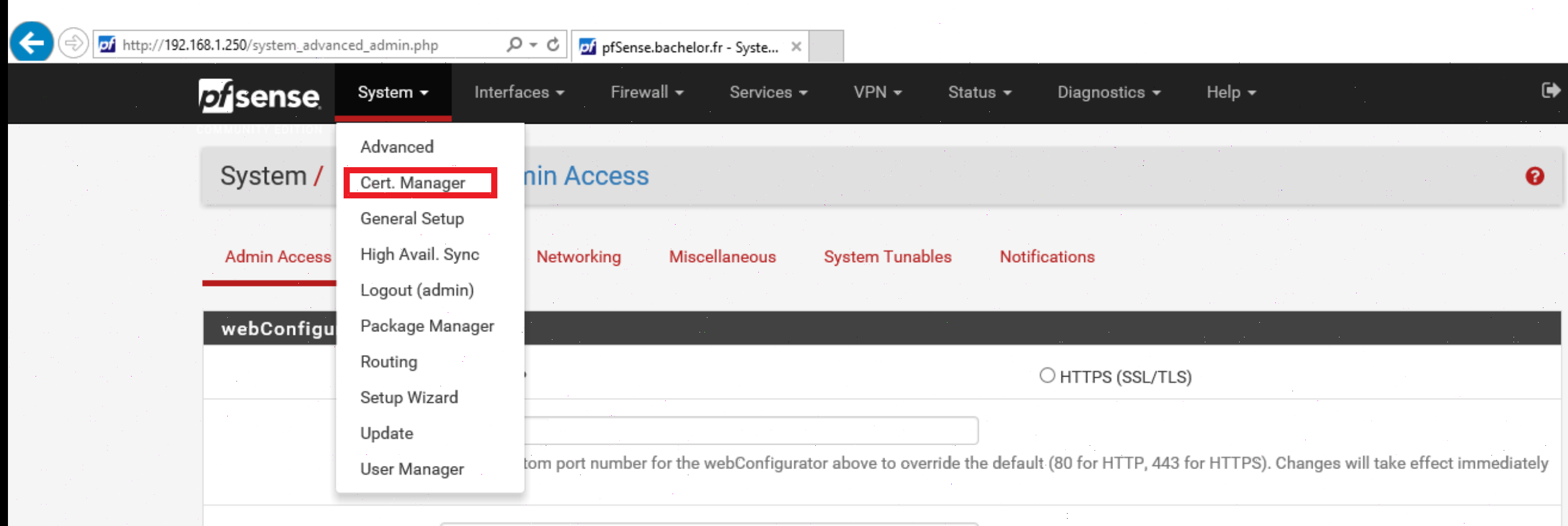


**Après on tombe sur notre console PfSense**

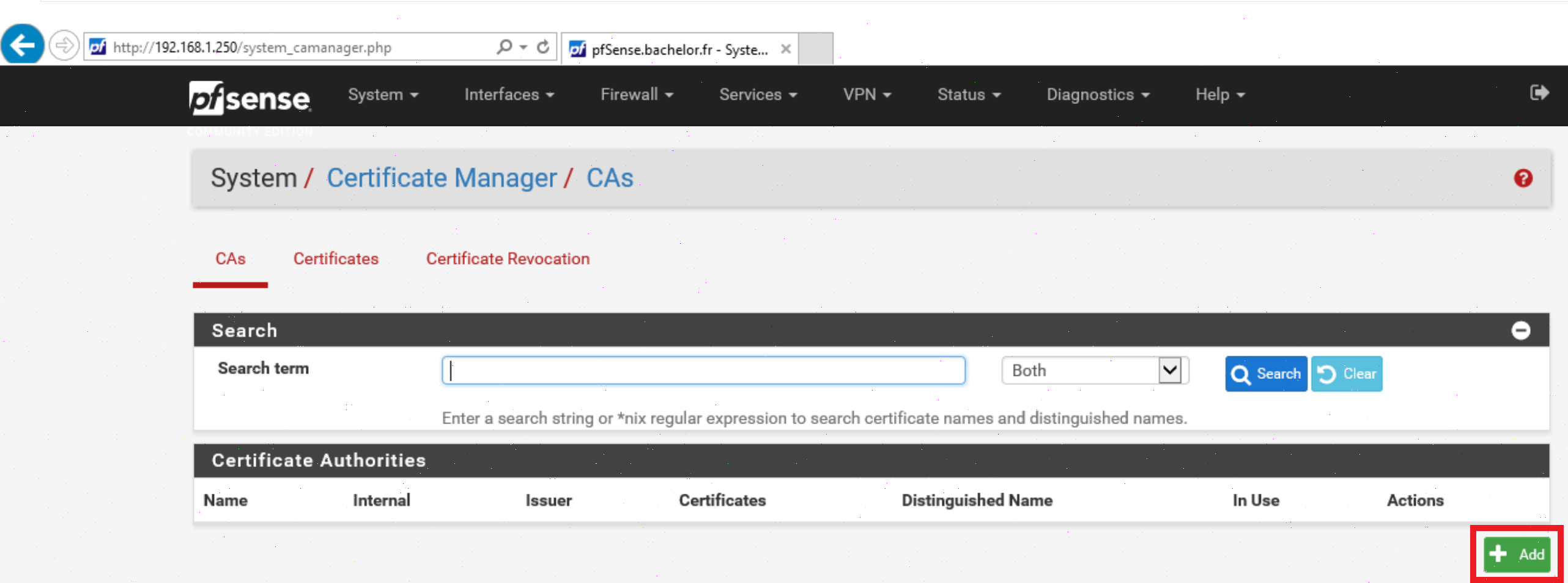


1. Sécurisez L’interface web par https
2. Créer une autorité de certification interne

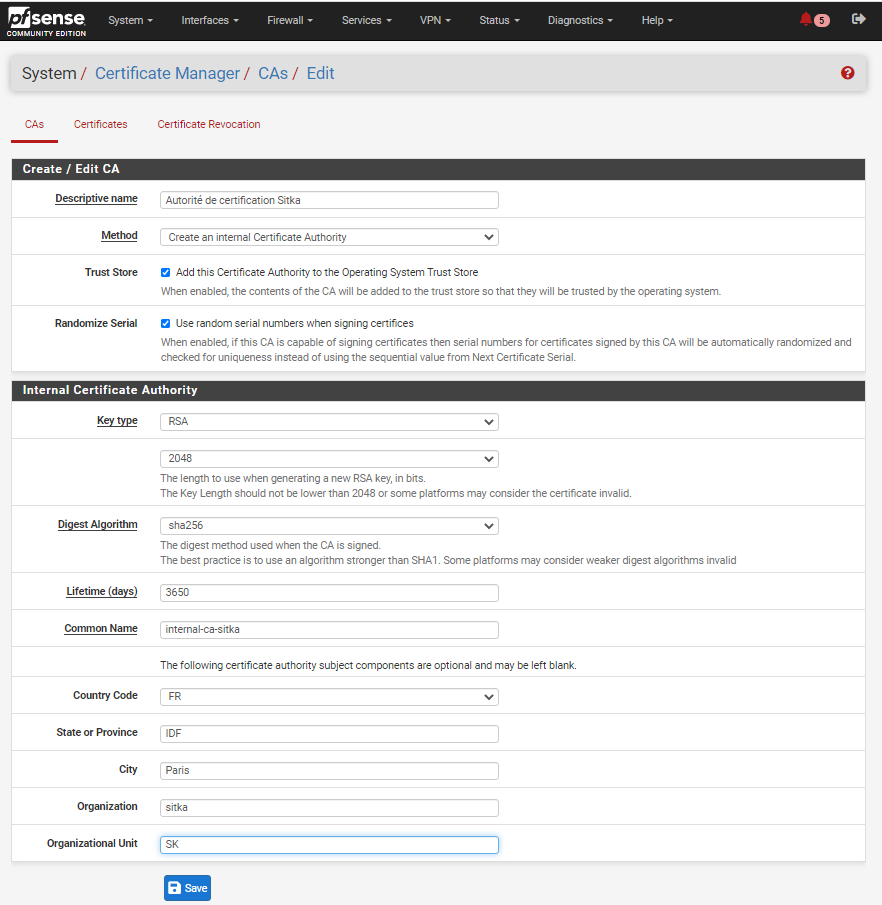
On va dans le menu **système + CertManager**



On commence à créer une autorité de certification interne



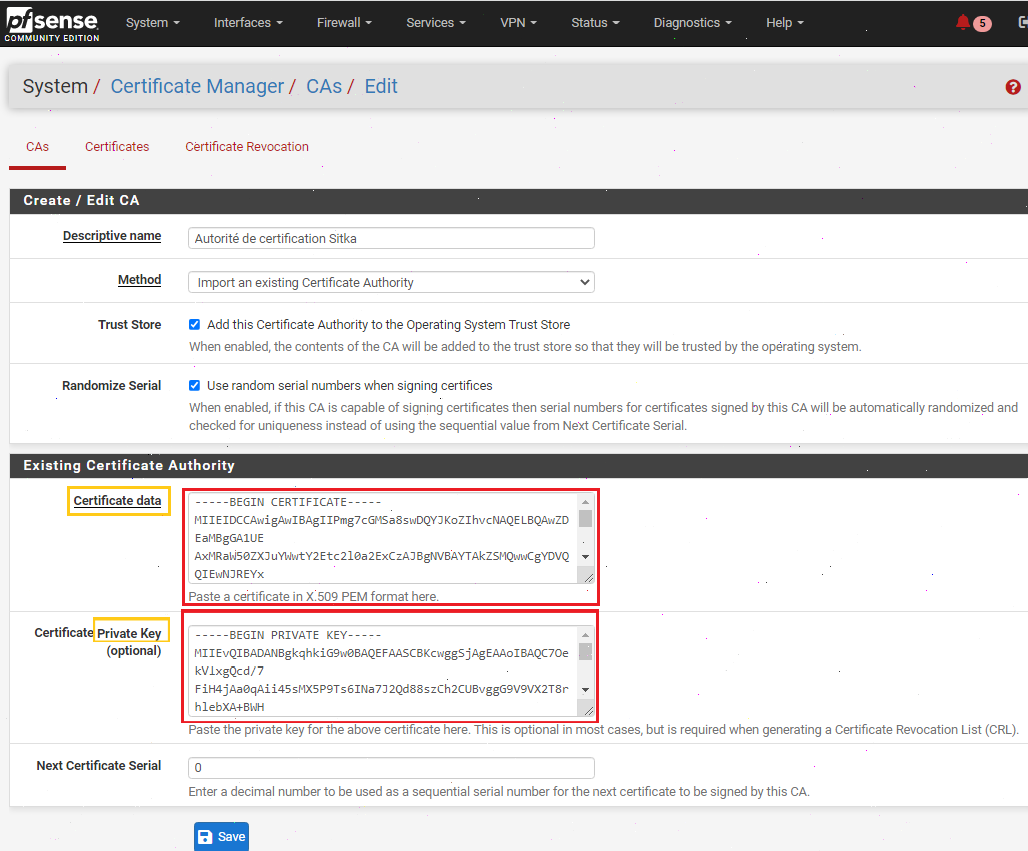
On remplit les champs suivants



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

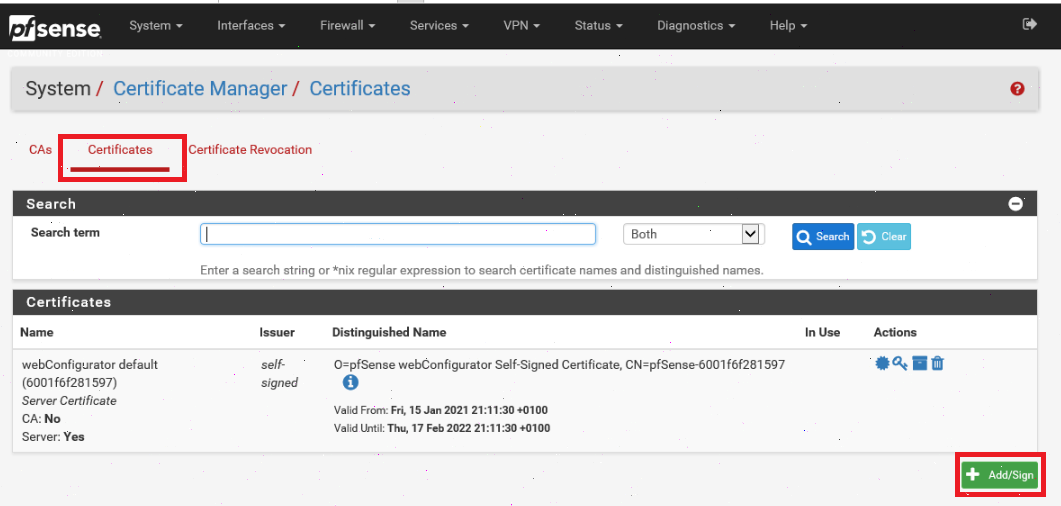


On affiche notre certificat et la clé publique qui lui est associé

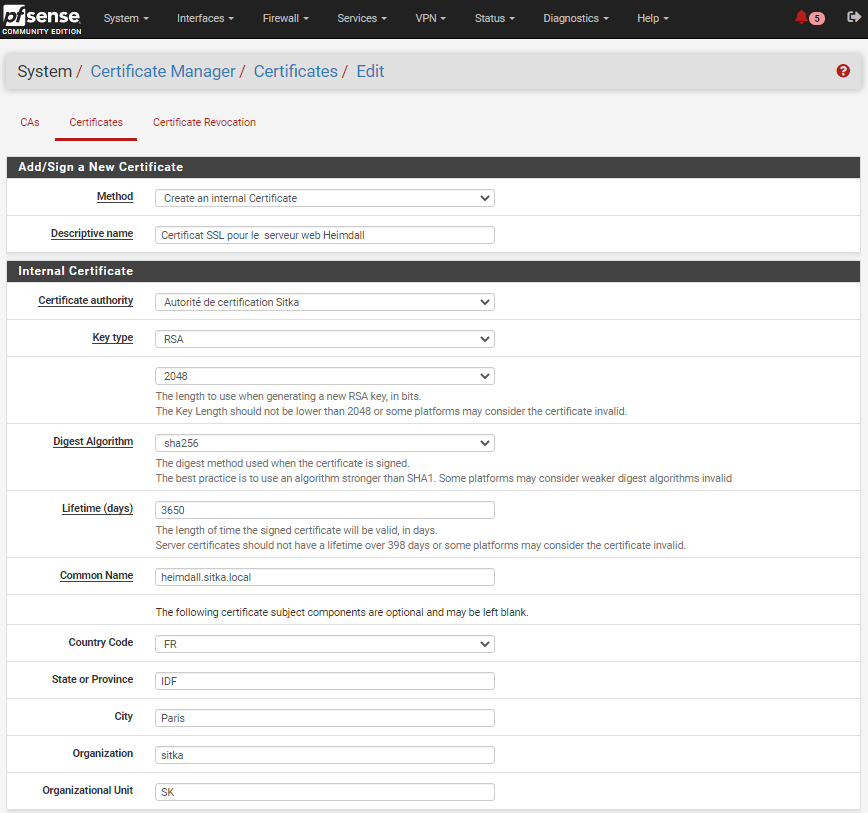
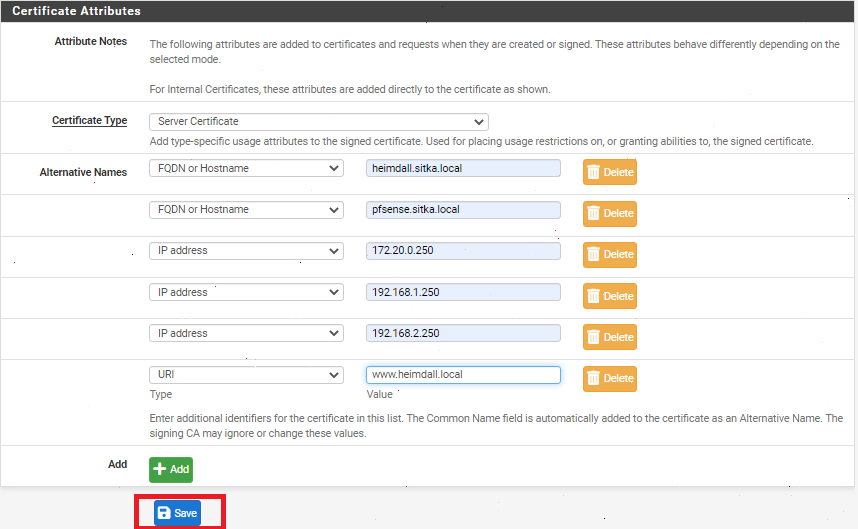


1. Générer un certificat web

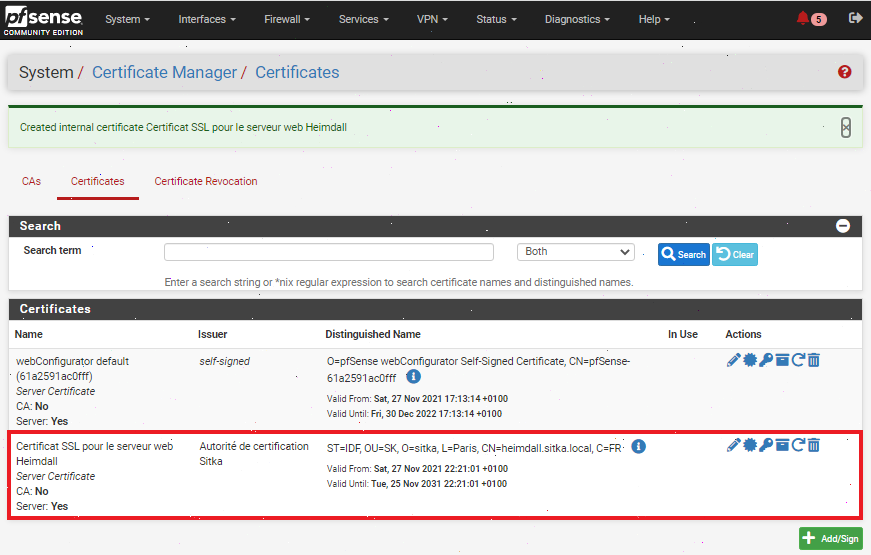
Maintenant on va créer notre certificat web délivrer par la CA **autorité de certification sitka** qu’on a mis en place dans l’étape précédente il suffit de cliquer sur add et remplir les champs nécessaires



ci-dessous les champs remplie pour créer notre certificat

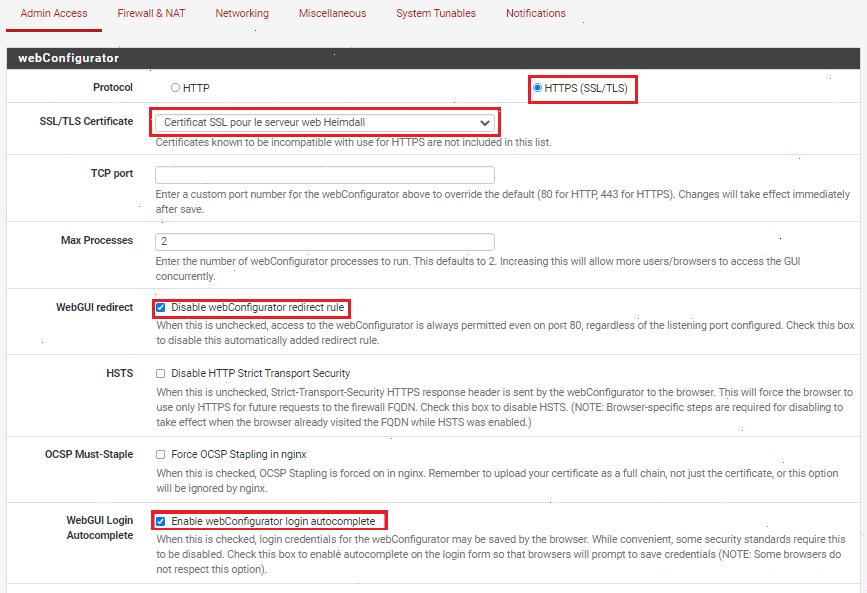
Une fois qu’on enregistre notre certificat apparait



1. Injecter le certificat web dans mon serveur PfSense

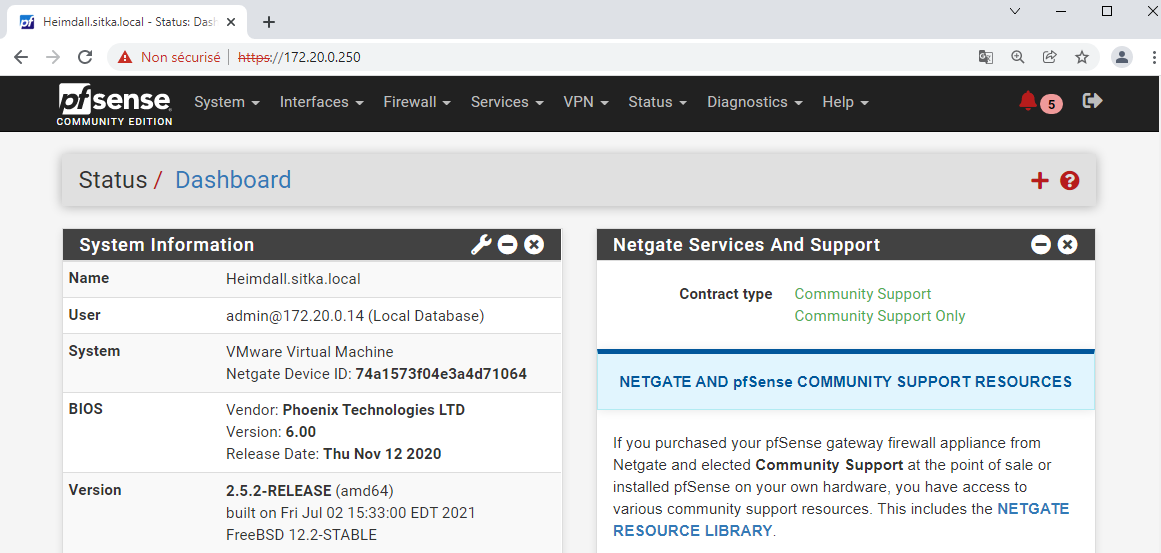
Maintenant on va injecter notre certificat dans notre serveur web PfSense, donc on va dans **système + Avanced**

* 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

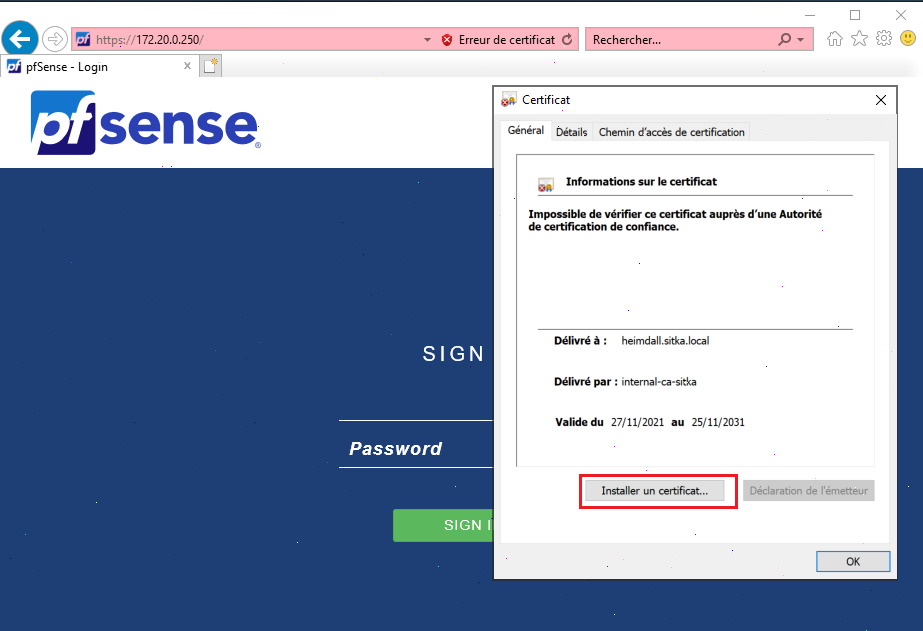
****

**Après on sauvegarde notre navigateur va démarrer automatiquement**

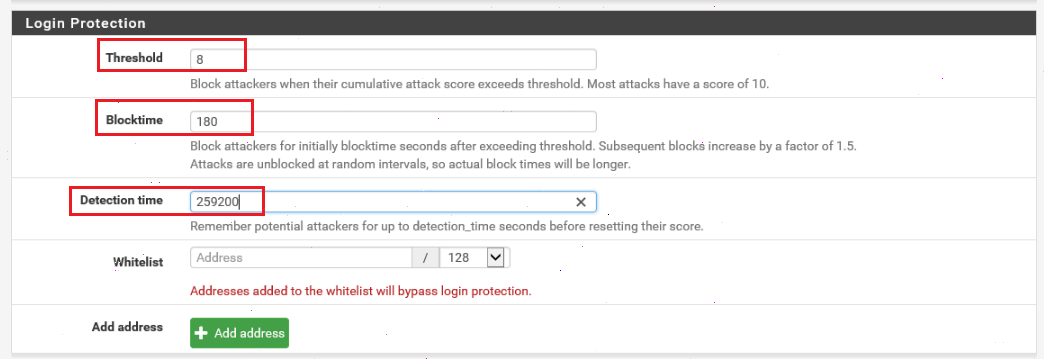
**On se connecte sur l’interface https://172.20.0.250**



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**

****