Let's Encrypt wildcard certificate avec ACME

Lorsque vous hébergez un ou plusieurs site web sur votre réseau, il est possible de faire la gestion de certificat beaucoup plus facilement avec let's ecrypt grâce au paquet ACME de pfsense.

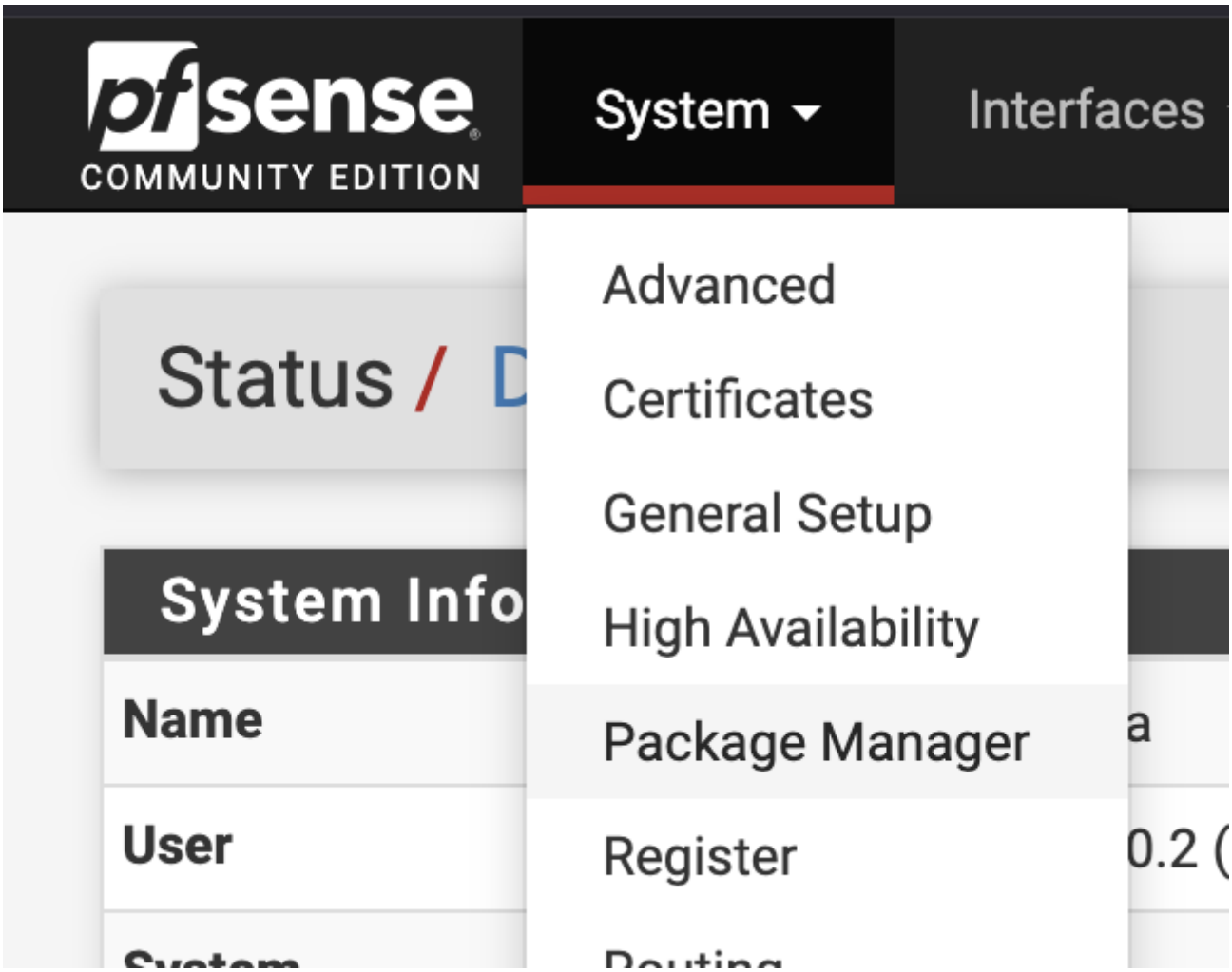
Vous n'aurez alors plus besoin de faire des demandes de certificat directement sur la machine.

Prérequis

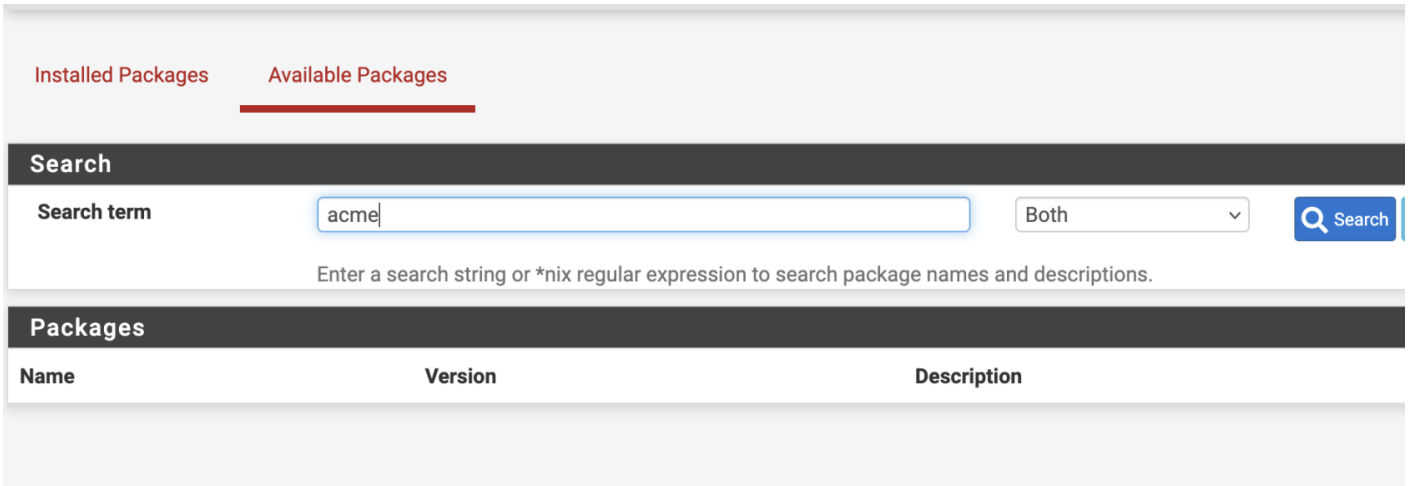
- Avoir un nom de domaine.
- Créer une clé api (Key / Secret) chez votre fournisseur de domaine.

Installation

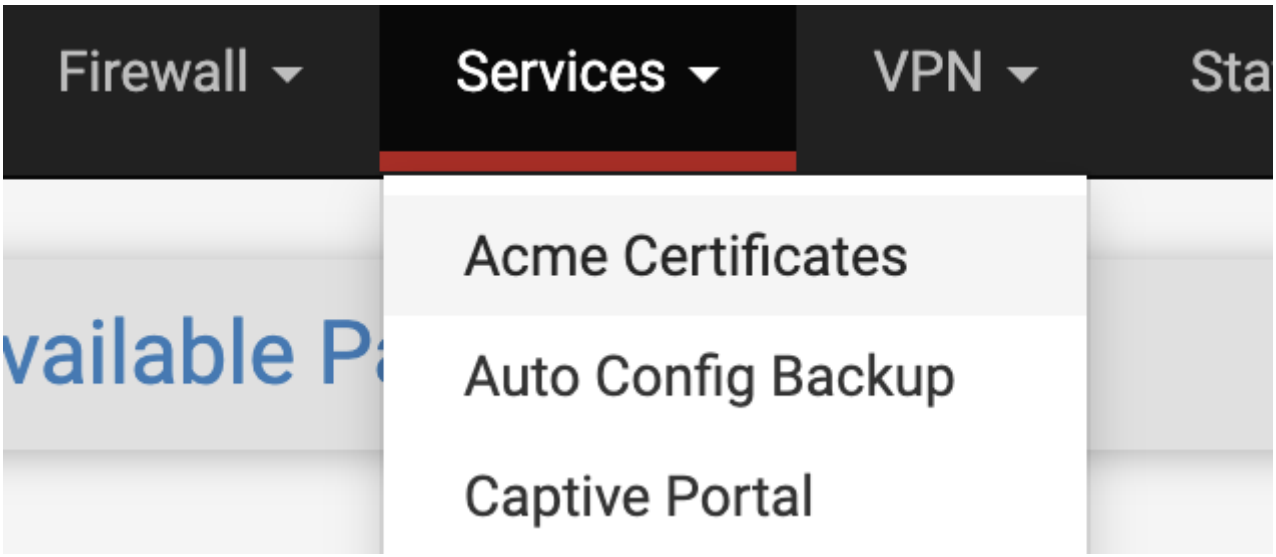
Rendez vous sur le Pacakage Manager de pfsense.



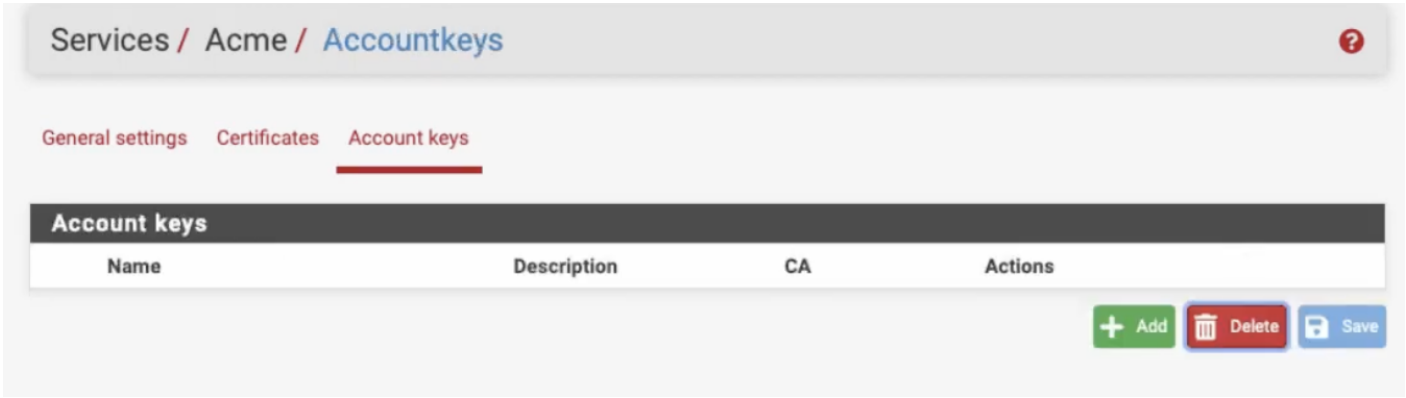
Sur les paquets disponibles, rechercher `acme` et installez le.



Une fois installé le paquet acme sera disponible sur `Services`



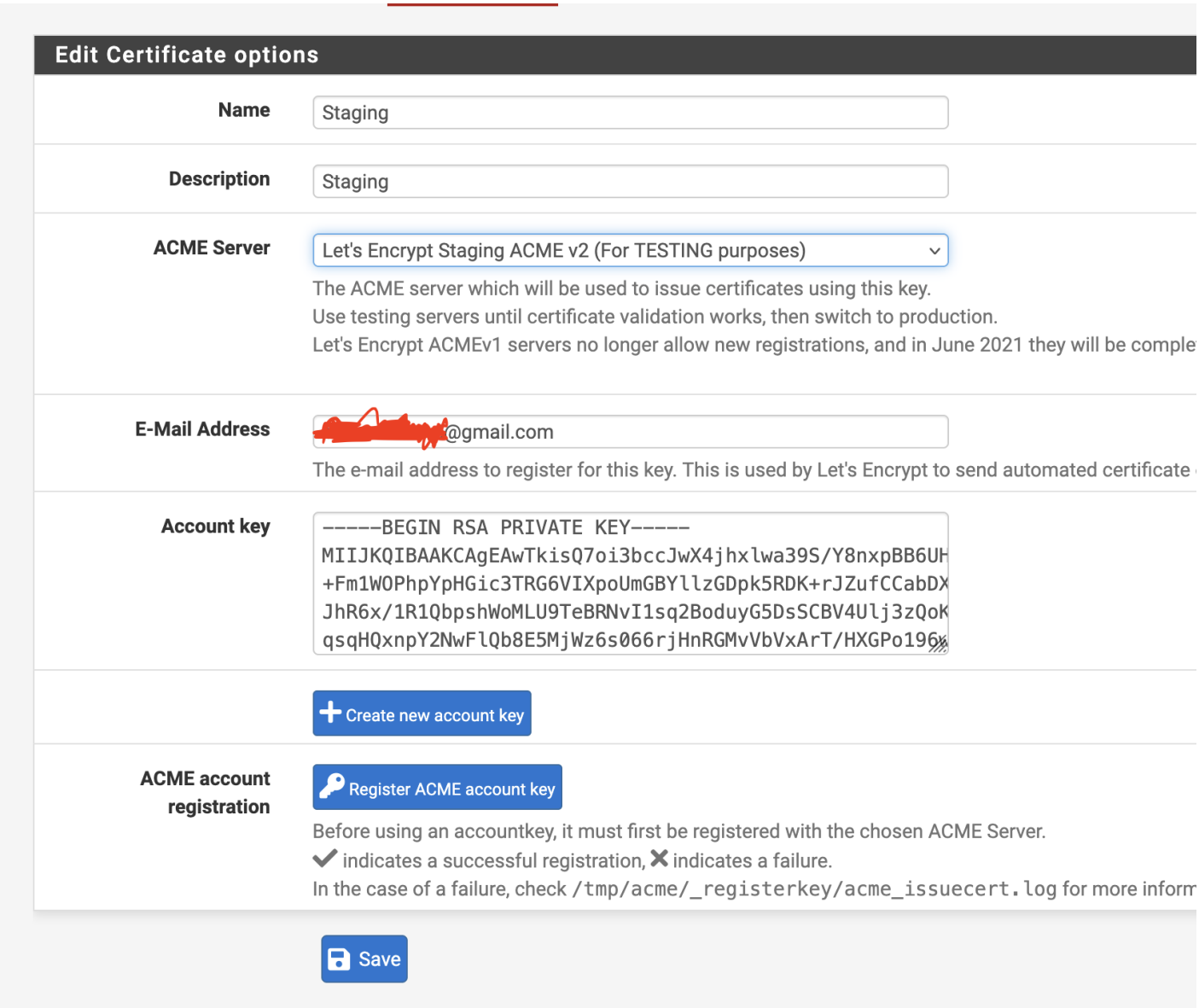
Une fois dessus, allez sur l'onglet `Accounts keys` et cliquez sur `Add` en bas à droite.



- Nous allons créer deux account keys. Le premier s'appellera **Staging** il nous permettra de tester notre configuration et le second sera **Prod** qui sera le certificat de production.

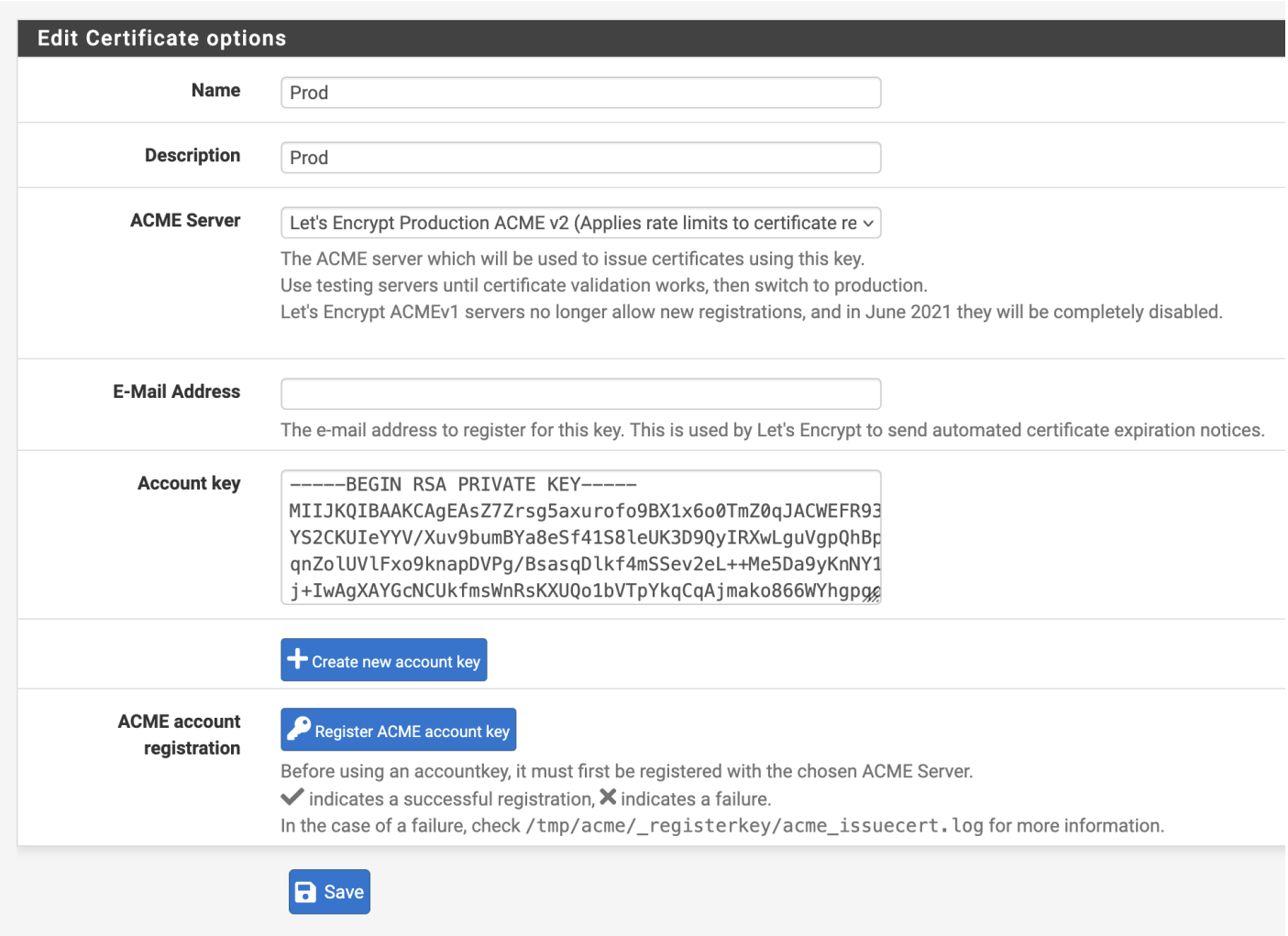
La différence c'est que Staging nous permettra de faire la demande de certificats plusieurs fois en cas d'erreur, alors que celui de production ne permet pas plusieurs demande, on basculera sur la Prod uniquement quand notre test sera ok.

Remplissez les paramètres comme ceci :



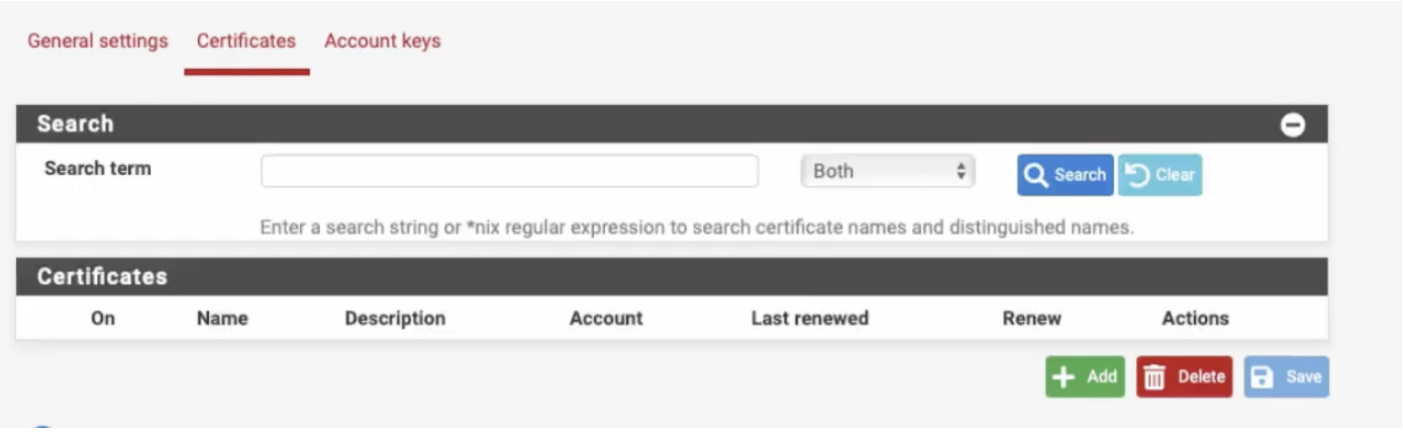
- Au niveau du `ACME Server` choisissez bien le premier avec (For TESTING purposes) à la fin.
- Remplissez une adresse email valide pour le champ mail
- Cliquez sur `Create new account key`
- Quelques secondes après l'affichage de la clé, cliquez sur `Register ACME account key`

Maintenant on va refaire exactement la même étape, mais cette fois pour le certificat de production, comme ci dessous.

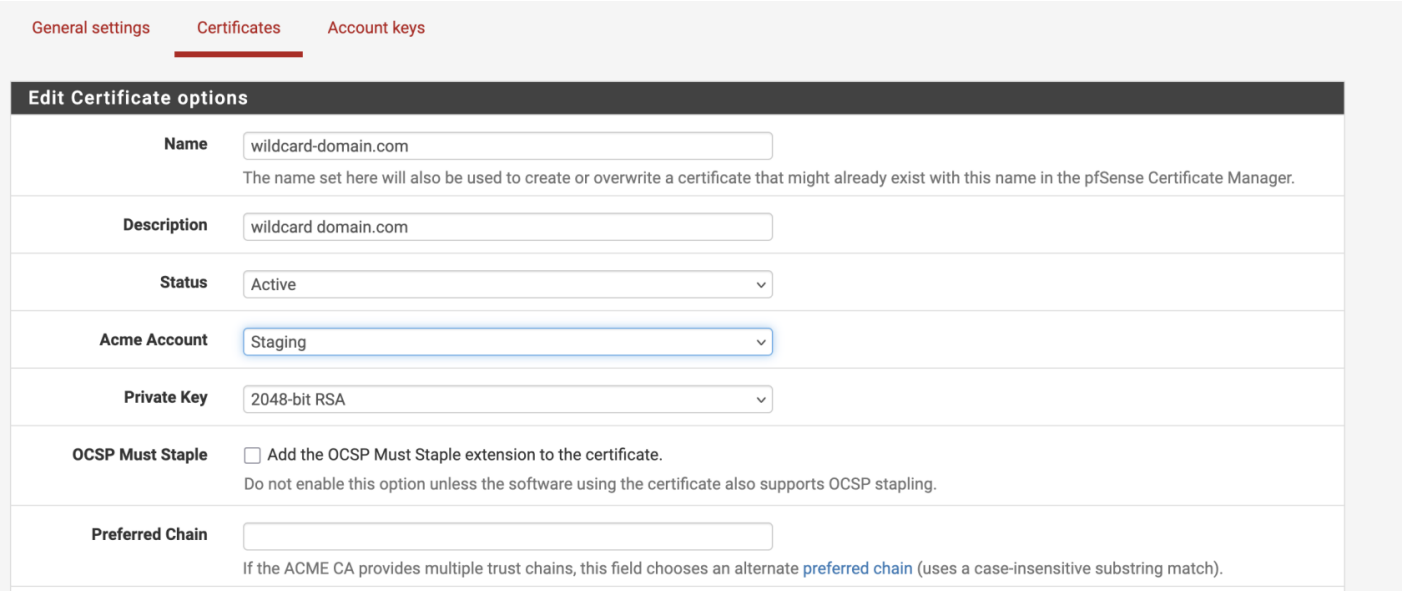


- Faudra changer le nom pour `Prod`
- Et aussi choisir comme ACME Server le deuxième choix, avec à la fin (Applies rate limits to certificate requests)

Maintenant allez sur l'onglet Certificates et faites add

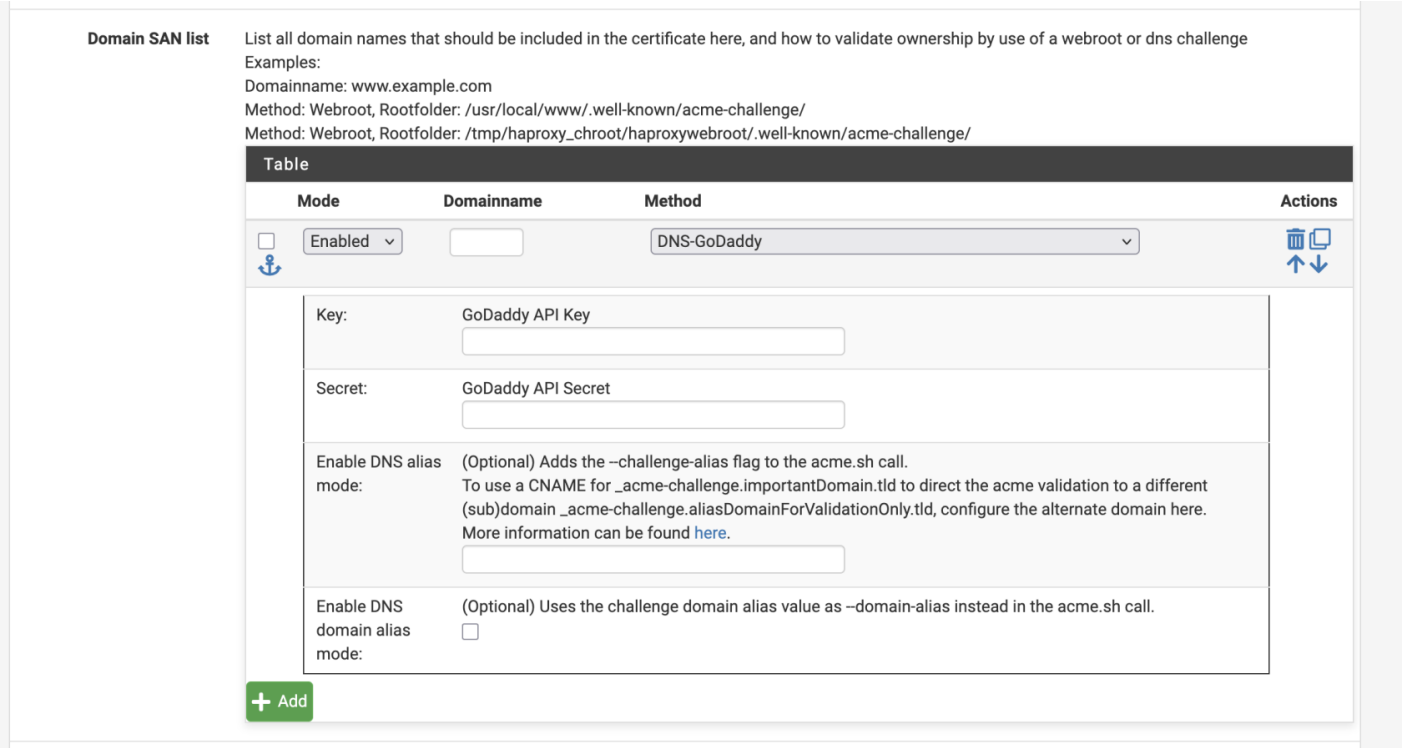


Nommez le wilcard-domain.com en remplaçant `domain` par votre nom de domaine.



Pour le acme account choisissez le staging. Laissez le reste par défaut à moins que vous souhaitez l'ajuster selon vos besoins.

Pour la partie Domain SAN list, nous allons utiliser une clé api

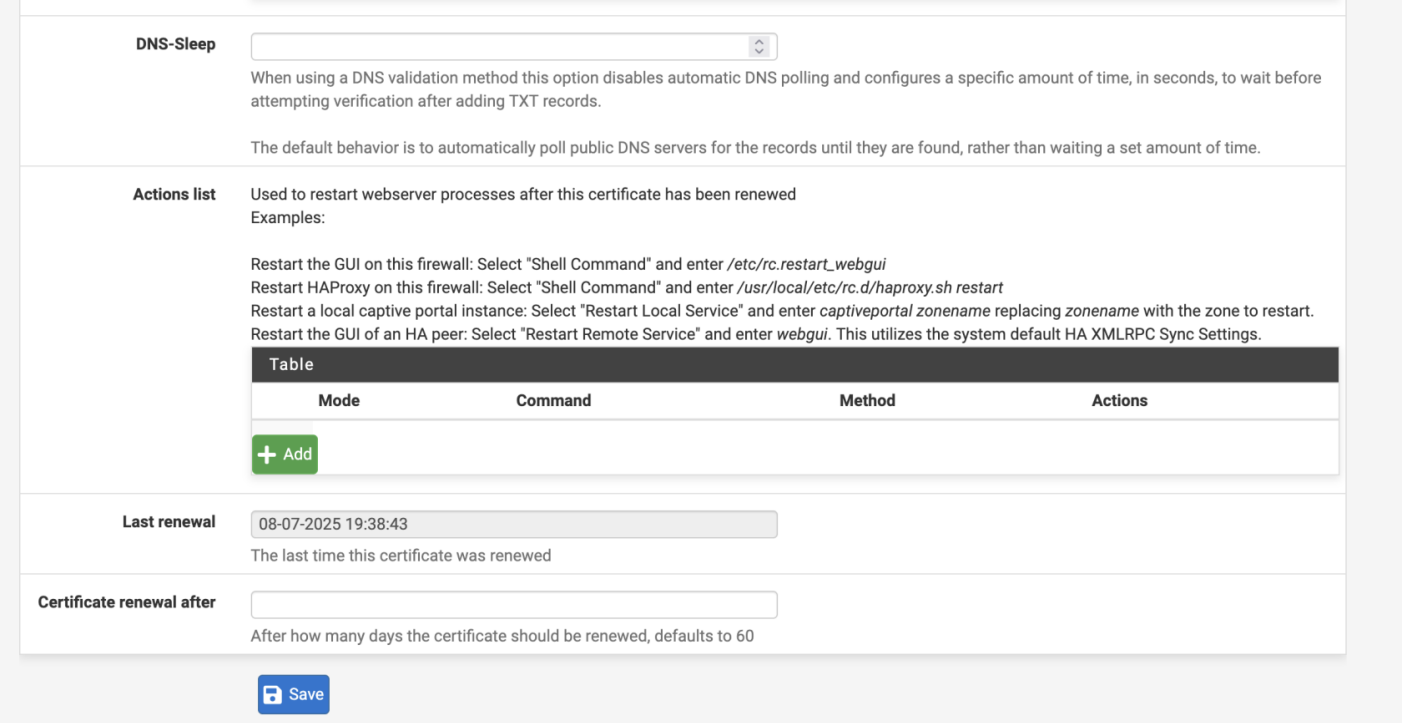


Il y'a énormement de choix au niveau de la partie `Method`, vous devez sélectionner celui de votre fournisseur de domaine et vous renseigner sur la création d'une clé api.

- Remplissez alors la `Key` et le `Secret`.
- Au niveau de `Domainname` mettez `votre_domaine.com`.
- Laissez le reste par défaut.

Ensuite faites add, et refaite exactement la même configuration, mais cette fois ci au niveau du Domainname mettez `*votre_domaine.com`. Par exemple si votre nom de domaine c'est otaku.com vous écrirez *otaku.com

Pour le reste vous pourrez le laissez par défaut et ajuster selon vos besoins.

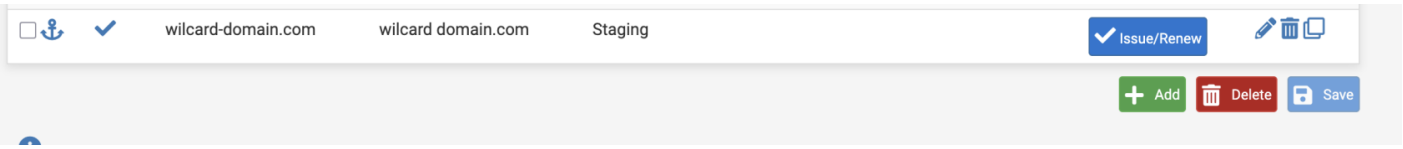


Voici un exemple de configuration à mettre

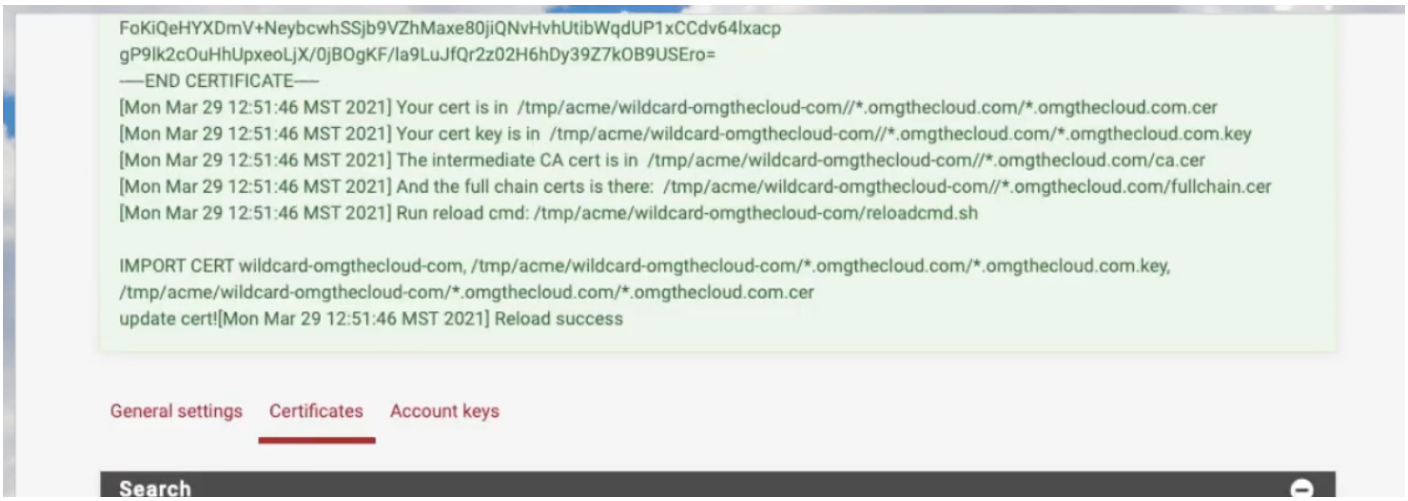
- DNS-Slepp : 120
- Certificate renewal after : 90

Ensuite cliquer sur le bouton `Issue/Renew`

L'opération peut prendre jusqu'à 2 minutes minimum, patientez.



S'il n'y a aucune erreur vous aurez un message de confirmation tout en vert comme ceci :



Après avoir eu la confirmation, modifié la configuration et changez le `Acme Account` pour **Prod** au lieu de **Staging**.

Et cliquer sur `Issue/Renew` encore une fois.

Après la validation, vous pourrez vous rendre sur System -> Certificate Manager -> Certificates et voir que le certificat à bien été configuré.

Revision #4
Created 8 July 2025 17:10:05 by Bibi
Updated 9 July 2025 06:16:23 by Bibi