

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 encrypt grâce au paquet ACME de pfsense.

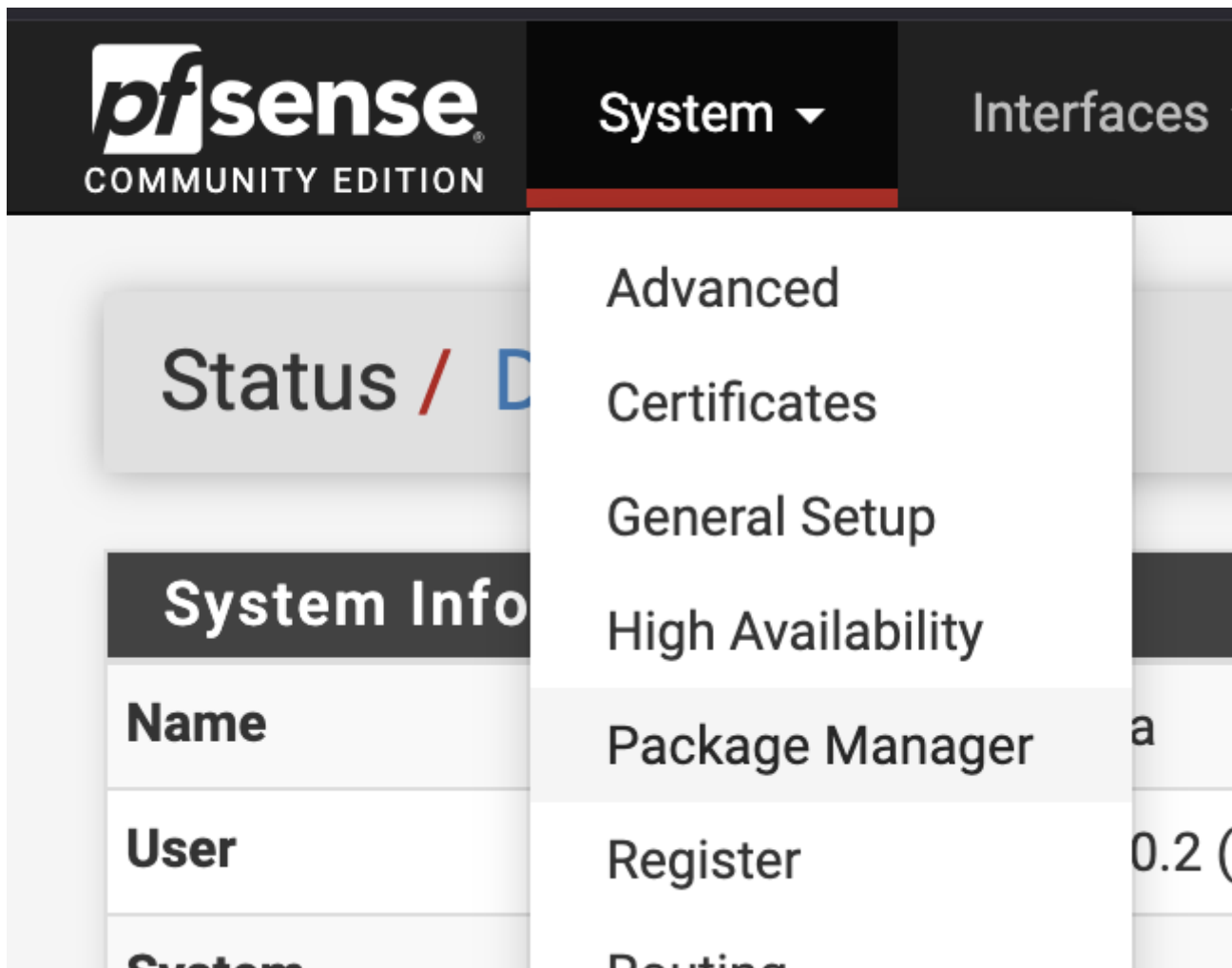
Vous n'aurez alors plus besoin de faire des demandes de certificat directement sur la machine.

Prérequis

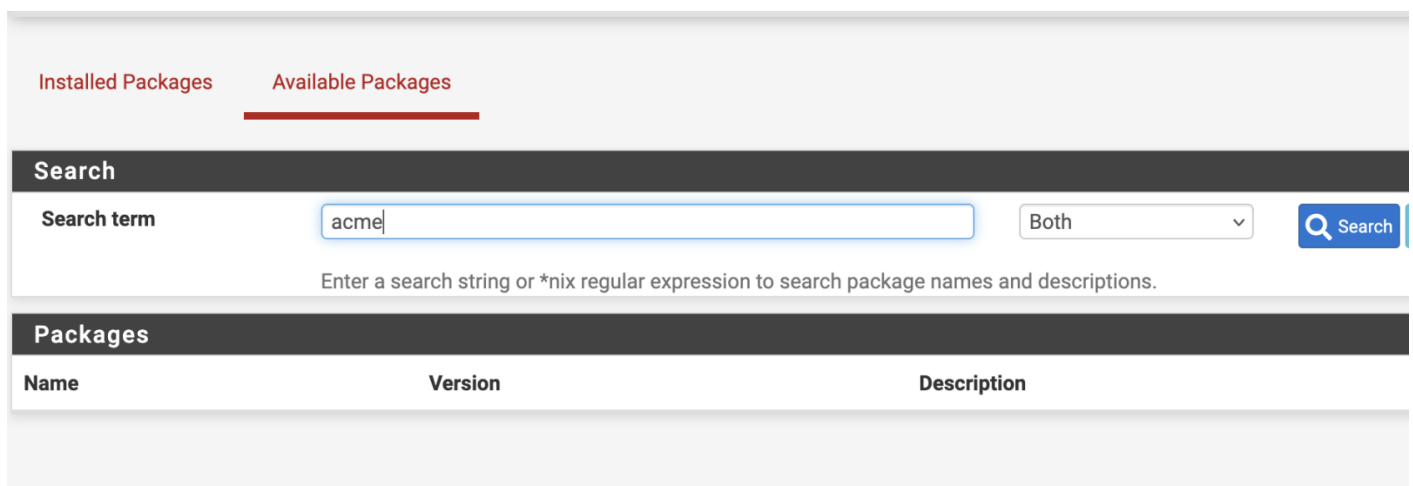
- Avoir un nom de domaine.
- Créer une clé api (Key / Secret) chez votre fournisseur de domaine.

Installation

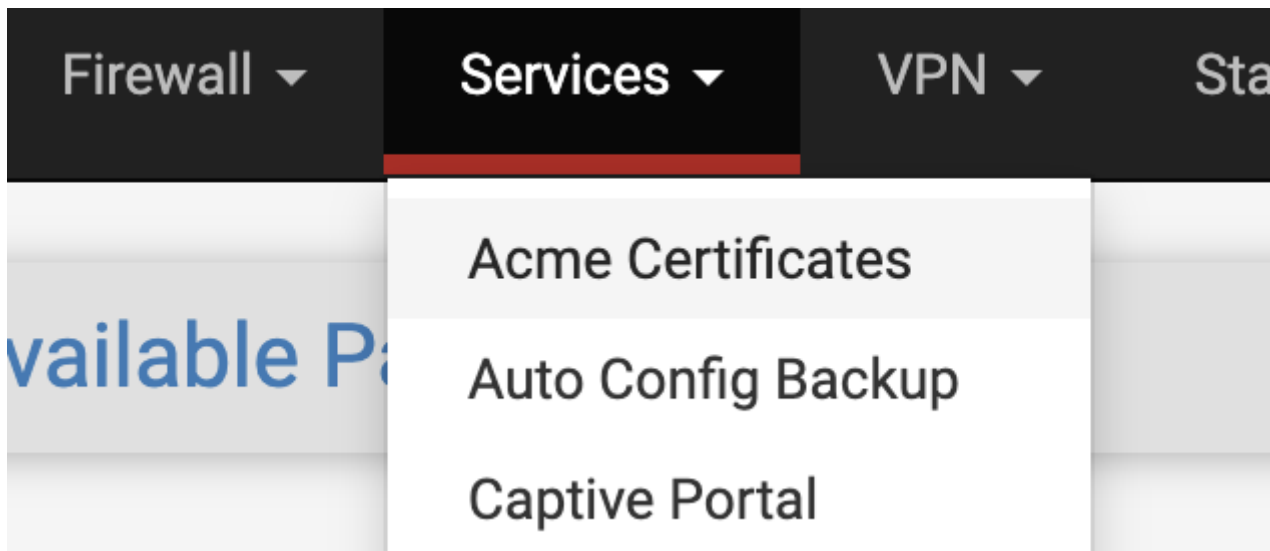
Rendez vous sur le Pacakage Manager de pfsense.



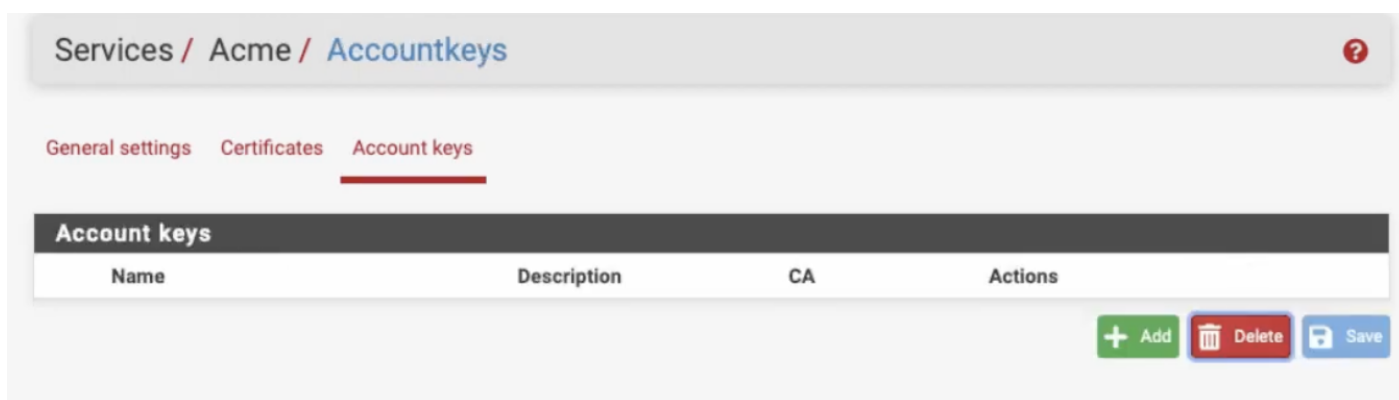
Sur les paquets disponibles, rechercher `acme` et installez le.



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 :

Edit Certificate options

Name Staging

Description Staging

ACME Server Let's Encrypt Staging ACME v2 (For TESTING purposes) ▾

The ACME server which will be used to issue certificates using this key.

Use testing servers until certificate validation works, then switch to production.

Let's Encrypt ACMEv1 servers no longer allow new registrations, and in June 2021 they will be complete

E-Mail Address [redacted]@gmail.com

The e-mail address to register for this key. This is used by Let's Encrypt to send automated certificate

Account key

-----BEGIN RSA PRIVATE KEY-----

```
MIIJKQIBAAKCAgEAWTkisQ7oi3bccJwX4jhxlwa39S/Y8nxB6UH  
+Fm1W0PhpYpHGic3TRG6VIXpoUmGBYllzGDpk5RDK+rJZufCCabDX  
JhR6x/1R1QbpshWoMLU9TeBRNvI1sq2BoduyG5DsSCBV4Ulj3zQoK  
qsqHqXnpY2NwFLQb8E5MjWz6s066rjHnRGMvVbVxArT/HXGPo196%
```

+ Create new account key

ACME account
registration

Register ACME account key

Before using an accountkey, it must first be registered with the chosen ACME Server.

✓ indicates a successful registration, ✗ indicates a failure.

In the case of a failure, check /tmp/acme/_registerkey/acme_issuecert.log for more inform

Save

- 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.

Edit Certificate options

Name

Prod

Description

Prod

ACME Server

Let's Encrypt Production ACME v2 (Applies rate limits to certificate re v

The ACME server which will be used to issue certificates using this key.
Use testing servers until certificate validation works, then switch to production.
Let's Encrypt ACMEv1 servers no longer allow new registrations, and in June 2021 they will be completely disabled.

E-Mail Address

The e-mail address to register for this key. This is used by Let's Encrypt to send automated certificate expiration notices.

Account key

```
-----BEGIN RSA PRIVATE KEY-----
MIIJKQIBAAKCAgEAsZ7Zrsg5axurofo9BX1x6o0TmZ0qJACWEFR93
YS2CKUIeYYV/Xuv9bumBYa8eSf41S8leUK3D9QyIRXwLguVgpQhBp
qnZo1UVlFxo9knapDVPg/BsasqDlkf4mSsev2eL++Me5Da9yKnNY1
j+IwAgXAYGcNCUKfmsWnRsKXUQo1bVTpYkqCqAjmako866WYhgpgg
```

+ Create new account key

ACME account registration

Register ACME account key

Before using an accountkey, it must first be registered with the chosen ACME Server.
✓ indicates a successful registration, ✗ indicates a failure.
In the case of a failure, check /tmp/acme/_registerkey/acme_issuecert.log for more information.

Save

- Faudra changer le nom pour
- 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

General settings

Certificates

Account keys

Search

Search term

Both

Search

Clear

Enter a search string or *nix regular expression to search certificate names and distinguished names.

Certificates

On	Name	Description	Account	Last renewed	Renew	Actions
						+ Add Delete Save

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

General settings **Certificates** Account keys

Edit Certificate options

Name
 The name set here will also be used to create or overwrite a certificate that might already exist with this name in the pfSense Certificate Manager.

Description

Status

Acme Account

Private Key

OCSP Must Staple ☐ Add the OCSP Must Staple extension to the certificate.
 Do not enable this option unless the software using the certificate also supports OCSP stapling.

Preferred Chain
 If the ACME CA provides multiple trust chains, this field chooses an alternate [preferred chain](#) (uses a case-insensitive substring match).

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

Domain SAN list List all domain names that should be included in the certificate here, and how to validate ownership by use of a webroot or dns challenge
 Examples:
 Domainname: www.example.com
 Method: Webroot, Rootfolder: /usr/local/www/.well-known/acme-challenge/
 Method: Webroot, Rootfolder: /tmp/haproxy_chroot/haproxywebroot/.well-known/acme-challenge/

Mode	Domainname	Method	Actions
☐ Enabled		DNS-GoDaddy	
Key: GoDaddy API Key Secret: GoDaddy API Secret Enable DNS alias mode: (Optional) Adds the --challenge-alias flag to the acme.sh call. To use a CNAME for _acme-challenge.importantDomain.tld to direct the acme validation to a different (sub)domain _acme-challenge.aliasDomainForValidationOnly.tld, configure the alternate domain here. More information can be found here. Enable DNS domain alias mode: (Optional) Uses the challenge domain alias value as --domain-alias instead in the acme.sh call. ☐			

[+ Add](#)

Il y'a énormément 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 **vosre_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 . 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.

DNS-Sleep

When using a DNS validation method this option disables automatic DNS polling and configures a specific amount of time, in seconds, to wait before attempting verification after adding TXT records.

The default behavior is to automatically poll public DNS servers for the records until they are found, rather than waiting a set amount of time.

Actions list

Used to restart webserver processes after this certificate has been renewed
Examples:

Restart the GUI on this firewall: Select "Shell Command" and enter `/etc/rc.restart_webgui`
Restart HAProxy on this firewall: Select "Shell Command" and enter `/usr/local/etc/rc.d/haproxy.sh restart`
Restart a local captive portal instance: Select "Restart Local Service" and enter `captiveportal zonename` replacing `zonename` with the zone to restart.
Restart the GUI of an HA peer: Select "Restart Remote Service" and enter `webgui`. This utilizes the system default HA XMLRPC Sync Settings.

Table

Mode	Command	Method	Actions
+ Add			

Last renewal

08-07-2025 19:38:43

The last time this certificate was renewed

Certificate renewal after

After how many days the certificate should be renewed, defaults to 60

Save

Voici un exemple de configuration à mettre

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

Ensuite cliquer sur le bouton

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

☐

☒

wilcard-domain.com

wilcard domain.com

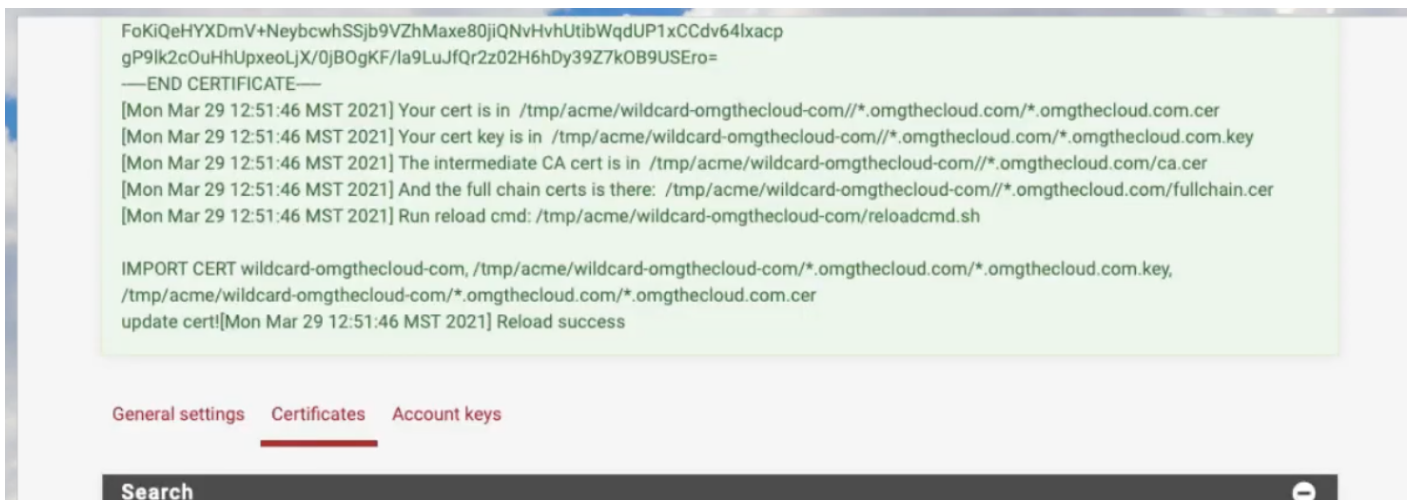
Staging

+ Add

Delete

Save

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 pour **Prod** au lieu de **Staging**.

Et cliquer sur 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