

**MODULE 7****CONFIGURER LE
REVERSE-PROXY
HAPROXY AVEC ACME****SOMMAIRE**


1. Installation du package HAPROXY
2. Installation du packaCréatge ACME
3. Création du compte ACME
4. Configuration d'un enregistrement DNS « A » chez OVH
5. Génération d'un certificat Let's Encrypt avec ACME
6. Configuration du reverse-proxy avec HAPROXY
 - a. Configuration du Frontend
 - b. Configuration du Backend
7. TESTS

© tutos-info.fr - 01/2025

UTILISATION COMMERCIALE INTERDITE


Pour réaliser ce tutoriel, vous devez avoir suivi les modules précédents et avoir un pfSENSE fonctionnel. Dans ce guide, nous allons **mettre en place un reverse-proxy à l'aide du package HAPROXY** dans pfSENSE.

1 – INSTALLATION DU PACKAGE HAPROXY DANS pfSENSE

- Connectez-vous à l'interface web de gestion de votre routeur pfSENSE
- Cliquez le menu « **System** » et « **Package Manager** »
- Cliquez le lien « **Available packages** »
- Dans la liste, recherchez « **haproxy** » et cliquez le bouton vert « **+ Install** » 
- Patientez le temps de l'installation du package
- Vérifiez que le package est installé en cliquant « **Installed Packages** »

2 – INSTALLATION DU PACKAGE ACME DANS pfSENSE

L'Automated Certificate Management Environment (ACME) est un protocole standard pour **automatiser la validation de domaine, l'installation et la gestion des certificats X.509**. Le protocole ACME a été conçu par Internet Security Research Group et est décrit dans [IETF RFC8555](https://tools.ietf.org/html/rfc8555). ACME est largement adopté en tant que solution d'automatisation des certificats d'entreprise. En installant le package, nous pourrons ainsi gérer l'obtention et le renouvellement de certificats Let's Encrypt notamment (connexion sécurisée de type « https »).

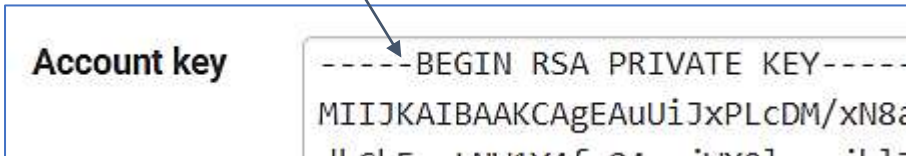
- Depuis l'interface de gestion de pfSENSE, cliquez le menu « **System** » et « **Package Manager** »
- Cliquez le lien « **Available packages** »
- Dans la liste, recherchez « **acme** » et cliquez le bouton vert « **+ Install** » 
- Patientez le temps de l'installation du package
- Vérifiez que le package est installé en cliquant « **Installed Packages** »

3 – CREATION DU COMPTE ACME

- Depuis l'interface de gestion de pfSENSE, cliquez le menu « **Services** » - « **ACME Certificates** »
- Cliquez le lien « **Account Keys** » et cliquez le bouton vert « **+ Add** »
- Complétez les 4 premiers champs :

Attention, le choix du serveur ACME « Production » vous limite dans vos tentatives de demandes de certificats ! Si vous souhaitez tester votre configuration dans un premier temps, optez plutôt pour le serveur ACME « Staging » !

- Cliquez sur « **Register ACME account key** » et patientez le temps que la clé privée soit générée ; elle apparaîtra sous cette forme :



- Cliquez le bouton « **Save** » ; votre compte ACME est prêt.

4 – CONFIGURATION D’UN ENREGISTREMENT DNS « A » CHEZ OVH

Dans le cadre de ce tutoriel, nous allons nous servir d’un nom de domaine hébergé chez OVH : **labo-sio.fr**. Si vous avez un autre hébergeur, il faudra adapter la procédure de création de l’enregistrement DNS-A.

Contexte :

Nous possédons 4 serveurs Proxmox connectés à l’interface « **LAN** » de notre routeur pfSENSE. L’interface « **WAN** » du routeur pfSENSE est connectée à une ligne fibre optique possédant une adresse IP publique full-stack IPv4 (adresse fixe). Nous souhaitons accéder à chacun des serveurs depuis l’extérieur et avec une URL de type « proxmox1.labo-sio.fr », « proxmox2.labo-sio.fr », etc.

Bien entendu, nous souhaitons que la connexion à chaque serveur soit sécurisée avec HTTPS et l’obtention d’un certificat Let’s Encrypt via le protocole ACME.

On commence par la création de l’enregistrement DNS-A chez notre hébergeur (ici OVH) :

- Connectez-vous à l’interface de gestion de votre hébergeur
- Ajoutez, dans votre zone DNS, l’enregistrement « A » correspondant

La fenêtre s’apparente à ceci :

Ajouter une entrée à la zone DNS Étape 2 sur 3

* Les champs suivis d'un astérisque sont obligatoires.

1 **Sous-domaine** : proxmox1 .labo-sio.fr

TTL : Par défaut

2 **cible *** : 106

Le champ A actuellement généré est le suivant :

serveur1 IN A 106

3 **Suivant**

On indique ici le sous-domaine souhaité pour l'accès au 1^{er} serveur. Ici on a choisi « proxmox1 » afin d'avoir l'URL proxmox1.labo-sio.fr

On indique ici notre adresse IP publique qui pointe vers notre box.

On clique le bouton « Suivant » et on valide la création du sous-domaine.

5 – GENERATION D'UN CERTIFICAT LET'S ENCRYPT AVEC ACME

Le sous-domaine étant créé chez notre hébergeur, on va maintenant demander, depuis pfSENSE, la génération d'un certificat Let's Encrypt via le protocole ACME.

Dans ce tutoriel, nous allons générer les certificats selon la méthode du « **DNS-manual** » qui nécessite la création d'un enregistrement « **TXT** ». Nous verrons, dans un autre tutoriel, la génération de certificats « **wildcard** ».

- Connectez-vous à l'interface de gestion de pfSENSE
- Cliquez « **Services** » - « **ACME** » - « **Certificates** »
- Cliquez le bouton vert « **+ Add** » et complétez la fenêtre selon vos paramètres :

Edit Certificate options

1 Name proxmox1.labo-sio.fr On nomme ici le certificat (à votre convenance).
The name set here will also be used for the certificate.

2 Description CertificatLE_Proxmox On indique une brève description (à votre convenance).

Status Active

3 Acme Account certs.labo-sio.fr On vérifie que le compte ACME est bien sélectionné.

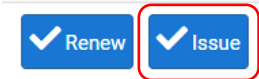
4 Private Key 2048-bit RSA On choisit le chiffrement de la clé, par exemple 2048-bit.

- Complétez le « **Domain SAN list** » en indiquant le sous-domaine enregistré précédemment chez notre hébergeur et sélectionnez « **DNS-Manual** » dans le champ « **Method** » :

Domain SAN list List all domain names that should be included in the certificate here, and how to validate ownership by using the following methods:
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/

Table		
Mode	Domainname	Method
<input type="checkbox"/>	proxmox1.labo-sio.fr	DNS-Manual

- Cliquez ensuite sur le bouton bleu « **Save** » en bas de l'écran
- Il faut maintenant demander le certificat en question, en cliquant le bouton bleu « **Issue** » :



Après avoir cliqué le bouton « Issue », on patiente quelques instants et, si vos paramètres sont corrects, une fenêtre s'affiche dans le haut de l'écran. Repérez, les 2 lignes nommées « **Add the following TXT record** » et « **TXT value** » (texte en vert) ; pour ce tutoriel, nous avons généré un certificat « proxmox5.labo-sio.fr » :

```
[Sat Jan 18 18:49:50 CET 2025] Single domain= proxmox5.labo-sio.fr
[Sat Jan 18 18:49:51 CET 2025] Getting webroot for domain='proxmox5.labo-sio.fr'
[Sat Jan 18 18:49:51 CET 2025] Add the following TXT record:
[Sat Jan 18 18:49:51 CET 2025] Domain: '_acme-challenge.proxmox5.labo-sio.fr'
[Sat Jan 18 18:49:51 CET 2025] TXT value: 'Vd460_50MAnzVOv9U18DCnM18vUbHJ a'
```

Ces 2 lignes sont importantes car vous devez les configurer dans l'interface de gestion des zones DNS de votre hébergeur. Pour cela, effectuez les manipulations suivantes (à adapter en fonction de votre hébergeur) :

- Ajoutez une entrée DNS dans votre zone qui sera de type « **TXT** » et complétez la fenêtre ainsi :

Ajouter une entrée à la zone DNS Étape 2 sur 3

* Les champs suivis d'un astérisque sont obligatoires.

1 Sous-domaine

TTL

2 Valeur *

On colle, ici, le contenu de « Domain » obtenu précédemment (écran avec texte vert).

On colle, ici, la valeur de la clé fournie (texte vert) SANS les apostrophes « ' » !

Le champ TXT actuellement généré est le suivant :

```
_acme-challenge.proxmox5 IN TXT "Vd460_50MAnzVOv9U18DC"
```

- Validez cette nouvelle entrée DNS

- Revenez dans l'interface de gestion des certificats (sur pfSENSE) et cliquez le bouton « **Renew** » ; une petite roue crantée s'affiche pendant la validation de l'opération :



Si l'opération est réussie (les paramètres saisis ont été validés), la fenêtre affiche ceci :

```
[Sat Jan 18 19:01:23 CET 2025] Pending. The CA is processing your order, please wait. (1/30)
[Sat Jan 18 19:01:25 CET 2025] Success
[Sat Jan 18 19:01:25 CET 2025] Verification finished, beginning signing.
[Sat Jan 18 19:01:25 CET 2025] Let's finalize the order.
[Sat Jan 18 19:01:25 CET 2025] Le_OrderFinalize='https://acme-v02.api.letsencrypt.org/acme/finalize/215
[Sat Jan 18 19:01:26 CET 2025] Downloading cert.
[Sat Jan 18 19:01:26 CET 2025] Le_LinkCert='https://acme-v02.api.letsencrypt.org/acme/cert/03e9e8ce8a
[Sat Jan 18 19:01:27 CET 2025] Cert success.
—BEGIN CERTIFICATE—
MIIE+DCCA+CgAwIBAgISA+nozopOYLu5IFFbMHvTGkwM...
MDMxCzAJBgNVBAYTAIVTMRYwFAYDVQQKEw1MZXQnc...
EwNSMTAwHhcNMjUwMTE4MTcwMjU2WhcNMjUwND...
ExRwcm94bW94NS5sYWJvLXNpb25mciCCASlwDOYJKoZIhvcNAQEBB0ADAAEPADCC
```

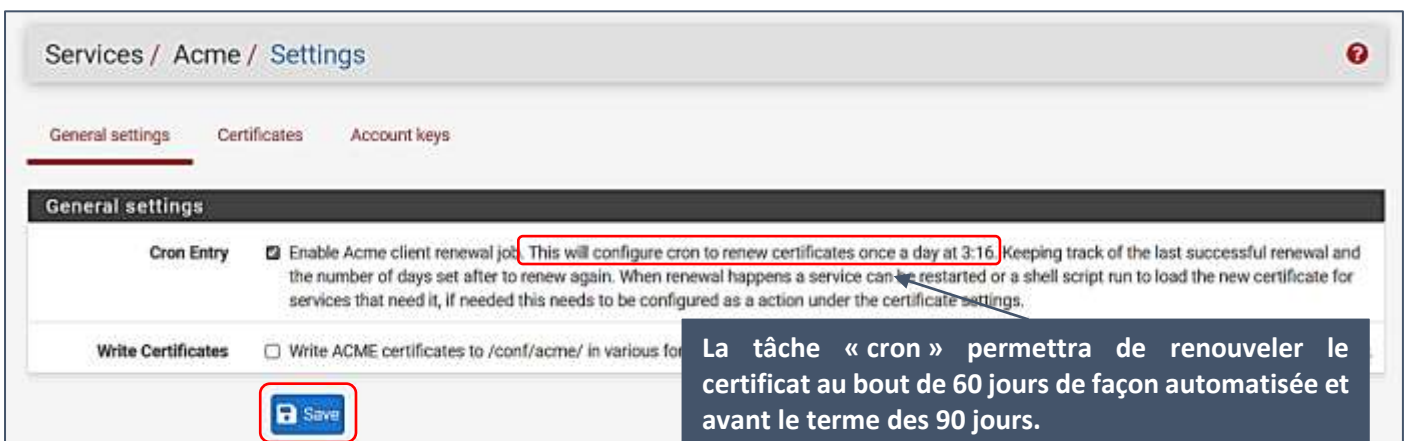
Le certificat a bien été généré avec succès auprès de Let's Encrypt.

On peut vérifier que le certificat a bien été généré en cliquant à nouveau sur « **Certificates** » :



Ici, le certificat Let's Encrypt est généré et est valide pour une période de 90 jours. Nous allons maintenant activer une tâche « **cron** » qui permettra un renouvellement automatique du certificat au bout de 60 jours par mesure de sécurité. Pour cela :

- Cliquez le lien « **General settings** »
- Cliquez la petite case « **Cron Entry** »
- Cliquez le bouton bleu « **Save** » :



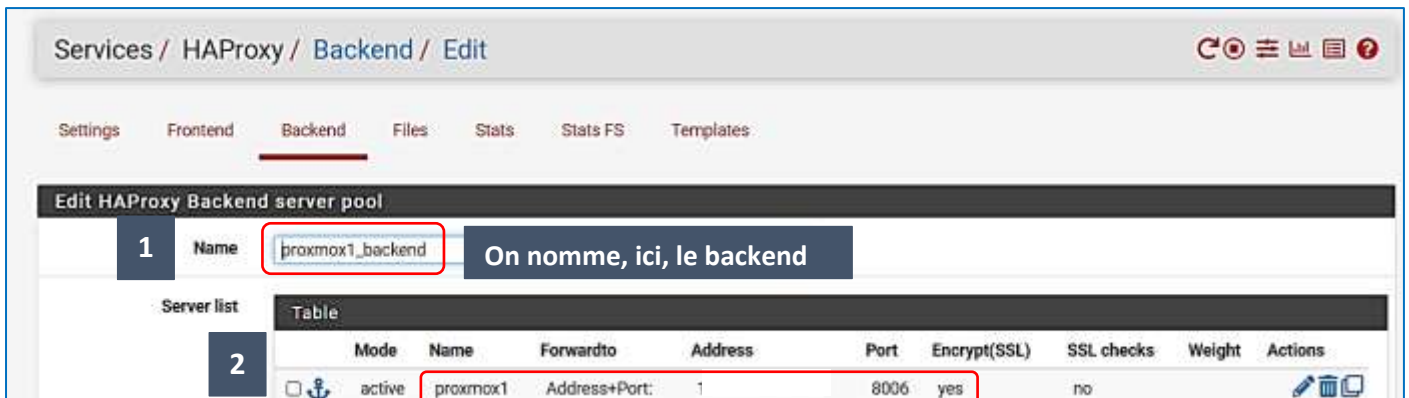
Notre certificat est prêt et fonctionnel. Il ne reste plus qu'à configurer le reverse-proxy.

6 – CONFIGURATION DU REVERSE-PROXY AVEC HAPROXY

Le reverse-proxy HAPROXY que nous avons installé au début de ce guide va permettre de rediriger les requêtes, arrivant sur l'interface WAN de notre routeur pfSENSE, vers le bon serveur. La mise en œuvre s'effectue en configurant le « frontend » (les requêtes entrantes) et le « backend » (la redirection des requêtes entrantes vers le bon serveur). **On commence par la configuration du backend** en suivant les étapes suivantes :

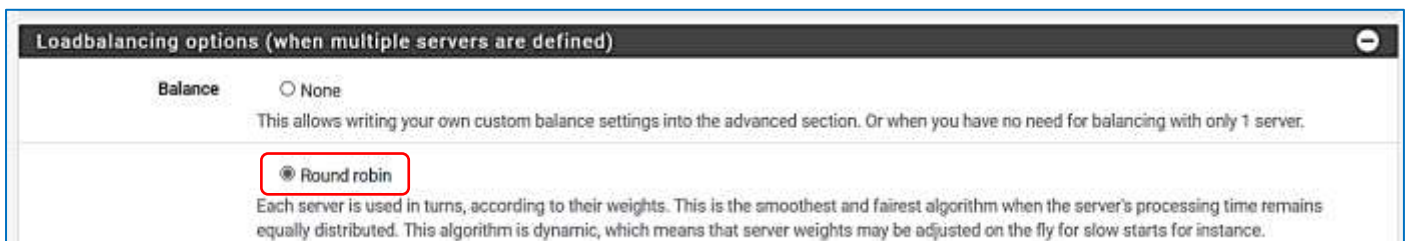
a) Configuration du Backend HAProxy

- Dans l'interface de gestion de pfSENSE, cliquez « **Services** » - « **HAProxy** »
- Cliquez sur « **Backend** » et sur le bouton vert « **Add** » ; on peut compléter la fenêtre suivante :

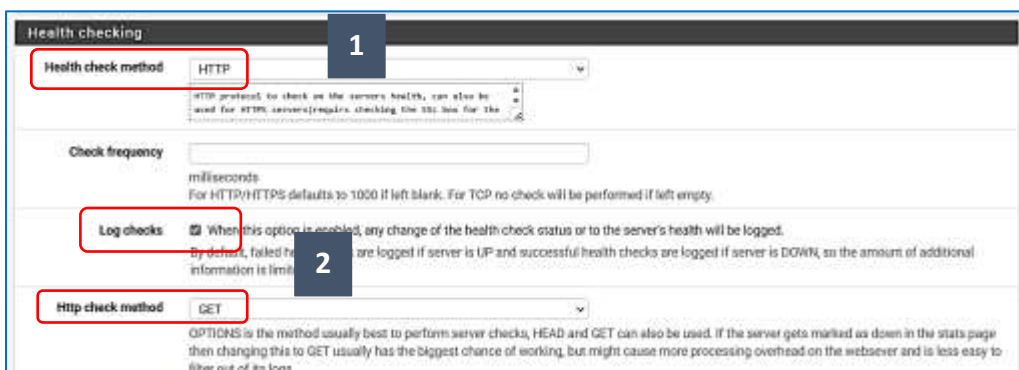


Dans la 2^{ème} étape, on indique le nom de notre serveur (ici « proxmox1 » avec son adresse IP locale, le port d'écoute du serveur (« 8006 » pour Proxmox) et on clique la petite case « **Encrypt SSL** » afin que l'indication « **yes** » soit affichée.

Dans la partie « **Loadbalancing options** », si plusieurs serveurs doivent être ajoutés au backend, on peut cliquer l'option « **Round robin** » :



Dans la partie « **Health checking** », on active diverses options (voir ci-dessous) :



On peut cliquer le bouton bleu « **Save** » une fois les paramètres saisis correctement.

b) Configuration du Frontend HAProxy

- Dans l'interface de gestion de pfSENSE, cliquez « **Services** » - « **HAProxy** »
- Cliquez sur « **Frontend** » et sur le bouton vert « **Add** » ; complétez la fenêtre suivante :

Services / HAProxy / Frontend / Edit

Settings Frontend Backend Files Stats Stats FS Templates

Edit HAProxy Frontend

1 Name proxmox_frontend On nomme, ici, le frontend

2 Description accès_srv_proxmox On indique une brève description du frontend

3 Status Active On sélectionne le statut « Active »

External address Define what ip:port combinations to listen on for incoming connections:

4

Listen address	Custom address	Port	SSL Offloading	Advanced	Actions
<input type="checkbox"/> WAN address (IPv4)		443	<input checked="" type="checkbox"/>		<input type="checkbox"/> <input type="checkbox"/>

- Sélectionnez « **http/https (offloading)** » dans la rubrique « **Type** » :

Type http / https(offloading)

This defines the processing type of HAProxy, and will determine the available options for acl checks and also several other options. Please note that for https encryption/decryption on HAProxy with a certificate the processing type needs to be set to "http".

- Créez, ensuite, **une ACL** dans la partie « **Default backend, access control lists and actions** » :

Default backend, access control lists and actions

Access Control lists Use these to define criteria that will be used with actions defined below to perform them only when certain conditions are met.

Name	Expression	CS	Not	Value	Actions
<input type="checkbox"/> acl_proxmox1	Host matches:	<input type="checkbox"/>	<input type="checkbox"/>	proxmox1.labo-sio.fr	<input type="checkbox"/> <input type="checkbox"/>

Dans la partie « **Actions** », on effectue la configuration suivante :

Actions Use these to select the backend to use or perform other actions like calling a lua script, blocking certain requests or others available.

Action	Parameters	Condition acl names	Actions
<input type="checkbox"/> Use Backend	See below	acl_proxmox1	<input type="checkbox"/> <input type="checkbox"/>

backend: proxmox1_backend

Dans la partie « **Advanced settings** », activez les paramètres suivants :

Advanced settings

Client timeout

the time (in milliseconds) we accept to wait for data from the client, or for the client to accept data (default 30000).

Use "forwardfor" option Use "forwardfor" option.

the "forwardfor" option creates an HTTP "X-Forwarded-For" header which contains the client's IP address. This is useful to let the final web server know what the client address was. (eg for statistics on domains)

Use "httpclose" option

By default HAProxy operates in keep-alive mode with regards to persistent connections: for each connection it processes each request and response, and leaves the connection alive on both sides between the end of a response and the start of a new request.

Dans la partie « **SSL Offloading** », sélectionnez le certificat Let's Encrypt généré précédemment :

SSL Offloading

Note SSL Offloading will reduce web servers load by maintaining and encrypting connection with users on internet while sending and retrieving data without encryption to internal servers. Also more ACL rules and http logging may be configured when this option is used. Certificates can be imported into the pfSense "Certificate Authority Manager" Please be aware this possibly will not work with all web applications. Some applications will require setting the SSL checkbox on the backend server configurations so the connection to the webserver will also be a encrypted connection, in that case there will be a slight overall performance loss.*

SNI Filter

Specify a SNI filter to apply below SSL settings to specific domain(s), see the "crt-list" option from haproxy for details.
EXAMPLE: *.securedomain.tld !public.securedomain.tld

Certificate

Choose the cert to use on this frontend.

Add ACL for certificate CommonName. (host header matches the "CN" of the certificate)

Add ACL for certificate Subject Alternative Names.

Une fois les paramètres saisis, on peut cliquer le bouton bleu « **Save** » en bas de la fenêtre. Le reverse-proxy HAProxy est maintenant prêt. Il ne reste plus qu'à l'activer de la façon suivante :

- Cliquez « **Settings** » dans les services HAProxy de votre pfSENSE
- Cliquez la petite case « **Enable HAProxy** » :

Services / HAProxy / Settings

Settings Frontend Backend Files Stats Stats FS Templates

General settings

Enable HAProxy

Installed version 2.8.3-86e043a

Maximum connections per process.

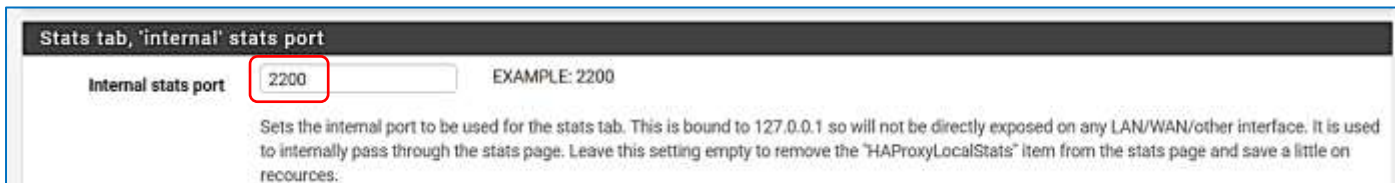
Sets the maximum per-process number of concurrent connections to X.
NOTE: setting this value too high will result in HAProxy not being able to allocate enough memory.
Current memory usage: 35928 kB.
Current 'System Tunables' settings:
%kern.maxfiles: 119382
%kern.maxfilesperproc: 107442
Full memory usage will only show after all connections have actually been used.

When setting a high amount of allowed simultaneous connections you will need to add and/or increase the following two 'System Tunables' kern.maxfiles and kern.maxfilesperproc. For HAProxy alone set these to at least the number of allowed connections * 2 + 31. So for 100.000 connections these need to be 200.031 or more to avoid trouble, take into account that handles are also used by other processes when setting kern.maxfiles.

Connections	Memory usage
1	50 kB
1.000	48 MB
10.000	488 MB
100.000	4,8 GB

Calculated for plain HTTP connections, using ssl offloading will increase this.

On peut activer les statistiques du reverse-proxy en saisissant le port 2200 par exemple dans la rubrique « **Internal stats port** » :



On termine la configuration et l'activation du reverse-proxy en cliquant le bouton bleu « **Save** » dans le bas de la fenêtre.

7 – TESTS

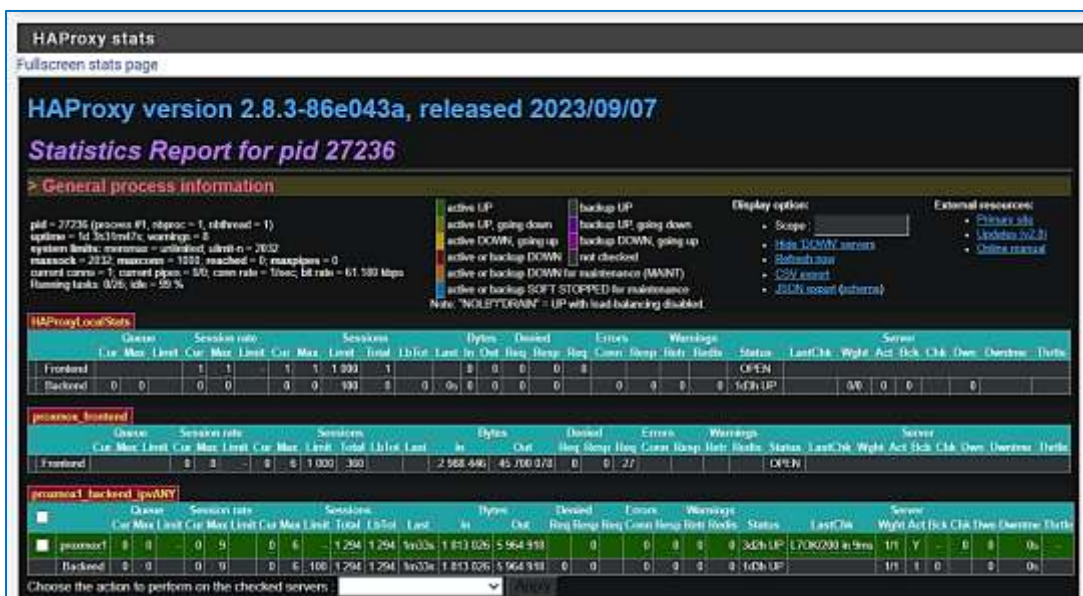
On peut tester la connexion à notre serveur « proxmox1 » depuis un navigateur et en saisissant l'URL paramétrée précédemment et vérifier que la connexion est bien sécurisée (HTTPS). **Il n'est plus utile d'indiquer le numéro de port « 8006 » de Proxmox**, la configuration est directement active depuis l'URL spécifiée :



Le certificat Let's Encrypt est bien valide :



Il est possible de consulter l'état du backend et des statistiques en cliquant « **Services** » - « **HAProxy** » - « **Stats** », on obtient ceci :



Dans un autre tutoriel, nous étudierons la génération des certificats Let's encrypt « wildcard ».