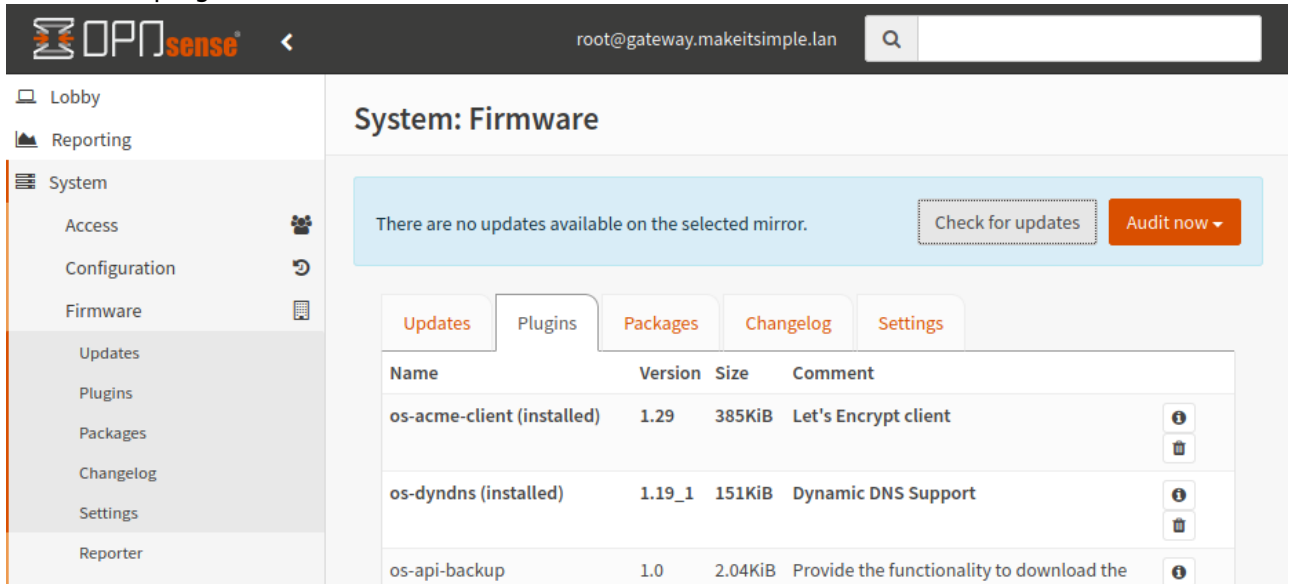


OPNSense & Let's Encrypt

Installer le package

1. Dans System → Firmware → Plugins, faire un Check for updates
2. Installer le plugin OS-ACME-CLIENT

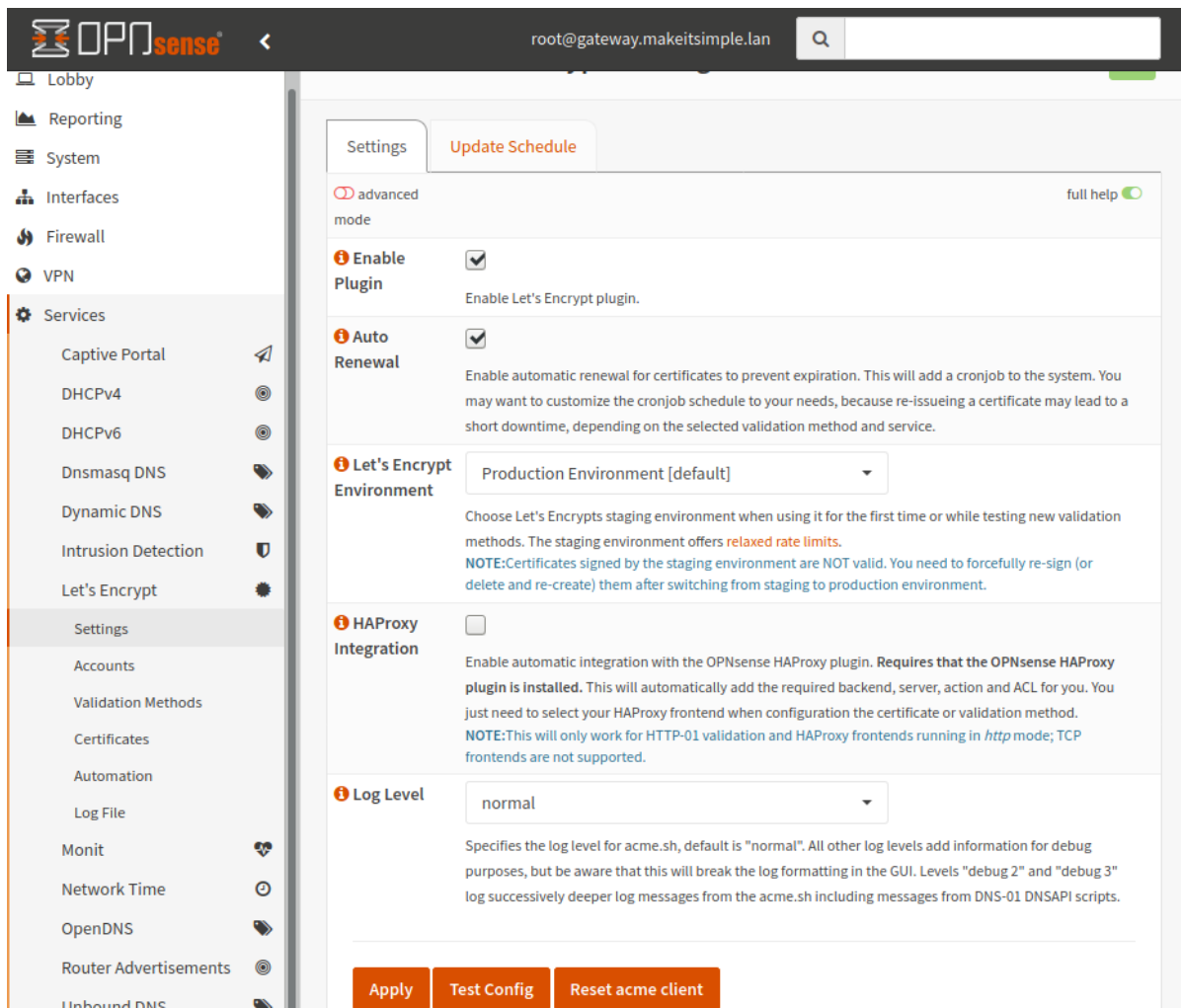


The screenshot shows the OPNSense web interface. The top navigation bar includes the OPNSense logo, a search bar, and the user 'root@gateway.makeitsimple.lan'. The left sidebar shows the 'System' menu with sub-items: Access, Configuration, Firmware, Updates, Plugins, Packages, Changelog, Settings, and Reporter. The main content area is titled 'System: Firmware' and displays a message: 'There are no updates available on the selected mirror.' with buttons for 'Check for updates' and 'Audit now'. Below this, there are tabs for 'Updates', 'Plugins', 'Packages', 'Changelog', and 'Settings'. The 'Updates' tab is active, showing a table of installed packages:

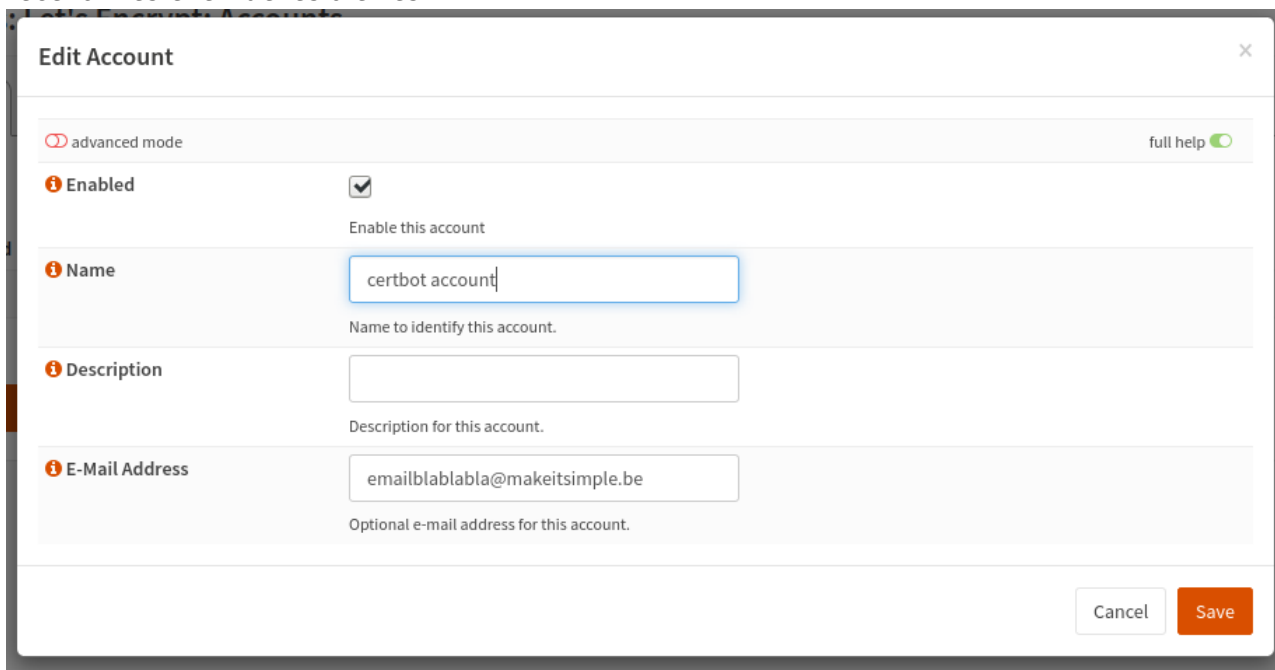
Name	Version	Size	Comment	
os-acme-client (installed)	1.29	385KiB	Let's Encrypt client	i x
os-dyndns (installed)	1.19_1	151KiB	Dynamic DNS Support	i x
os-api-backup	1.0	2.04KiB	Provide the functionality to download the	i

Configuration

1. Dans Services → Let's Encrypt → Settings
 1. Activer le service
 2. Choisir Auto Renewal
 3. Choisir Staging pour réaliser les essais (ou prendre Production si on est certain - attention le nombre de requêtes est limité)
 4. Faire Apply



2. Dans Services → Let's Encrypt → Account, créer un compte avec votre adresse email pour recevoir les éventuelles alertes





3. Dans Services → Let's Encrypt → Validation Method, créer une nouvelle méthode

1. L'activer
2. Choisir le challenge type DNS-01
3. Dans DNS-Service j'ai utilisé OVH, Kimsufi, soyoustart, à adapter selon vos besoins
4. Se rendre sur <https://api.ovh.com/createToken/> et

1. Choisir validity = **unlimited**
2. Rajouter des droits pour:
 1. GET : /domain
 2. POST : /domain
 3. PUT : /domain
 4. DELETE : /domain
 5. GET : /domain/*
 6. POST : /domain/*
 7. PUT : /domain/*
 8. DELETE : /domain/*
 9. Puis créer les clés
5. Encoder les clés créées sur OVH et les insérer dans le formulaire

Edit Validation Method
✕

 advanced mode
full help 

Enabled Enable this validation

Name Name to identify this validation.

Description Description for this validation.

Challenge Type DNS-01 Set the Let's Encrypt challenge type. You'll have to add configuration for the selected challenge type below.

DNS-01

DNS Service OVH, kimsufi, soyoustart and runabove API

Sleep Time The time in seconds to wait for all the TXT records to take effect after adding them to the DNS API. Defaults to 120 seconds.

OVH

Application Key

Application Secret

Consumer Key

Endpoint Specify the OVH endpoint, i.e. ovh-eu, ovh-ca, kimsufi-eu, etc. Please refer to the [acme.sh documentation](#) for further information.

Cancel Save

4. Dans Services → Let's Encrypt → Certificate, créer un nouveau certificat
 1. L'activer en cliquant sur Enabled
 2. Donner le nom du host dans CommonName
 3. Choisir le compte dans LE Account précédemment créé
 4. Choisir le Validation Method

Edit Certificate full help

Certificate Options

Enabled Enable this certificate

Common Name Common Name (CN) for this certificate.

Description Description for this certificate.

Alt Names Clear All
Configure additional names that should be part of the certificate, i.e. www.example.com or mail.example.com. Use TAB key to complete typing a FQDN.
NOTE:You need to forcefully re-issue the certificate if you change "Alt Names" after the certificate was signed by the Let's Encrypt Authority! Use the "issue" button in the Commands column in this case.

Let's Encrypt Settings

LE Account Set the Let's Encrypt account to use for this certificate.

Validation Method Set the Let's Encrypt validation method for this certificate.

Auto Renewal Enable automatic renewal for this certificate to prevent expiration.

Renewal Interval Specifies the days to renew the cert. The max value is 60 days.

5. Appuyer sur Save
6. Générer un nouveau certificat en cliquant sur ISSUE/RENEW

Services: Let's Encrypt: Certificates

Enabled	Common Name	Multi-Domain (SAN)	Description	Issue/Renewal Date	Last Acme Status
<input checked="" type="checkbox"/>	...	<input checked="" type="checkbox"/>	...	23/02/2020 à 08:37:45	OK

Issue/Renew Certificates Now

Use the Issue/Renew button to let the acme client automatically issue any new certificate and renew existing certificates (only if required). If you want to only issue/renew or revoke a single certificate, use the b certificate, even if it is not required. The process may take some time and thus will run in the background, you will not get any notification in the GUI. Use the log file to monitor the progress and to see erro

Une fois créé, on peut changer le certificat dans System → Trust → Certificates Il est possible d'aller plus loin en lançant via automation un restart

From:

<https://wiki.makeitsimple.be/> - **makeITsimple wiki**

Permanent link:

<https://wiki.makeitsimple.be/doku.php?id=reseau:opnsense:letsencrypt&rev=1582535229>

Last update: **2021/06/20 09:42**

