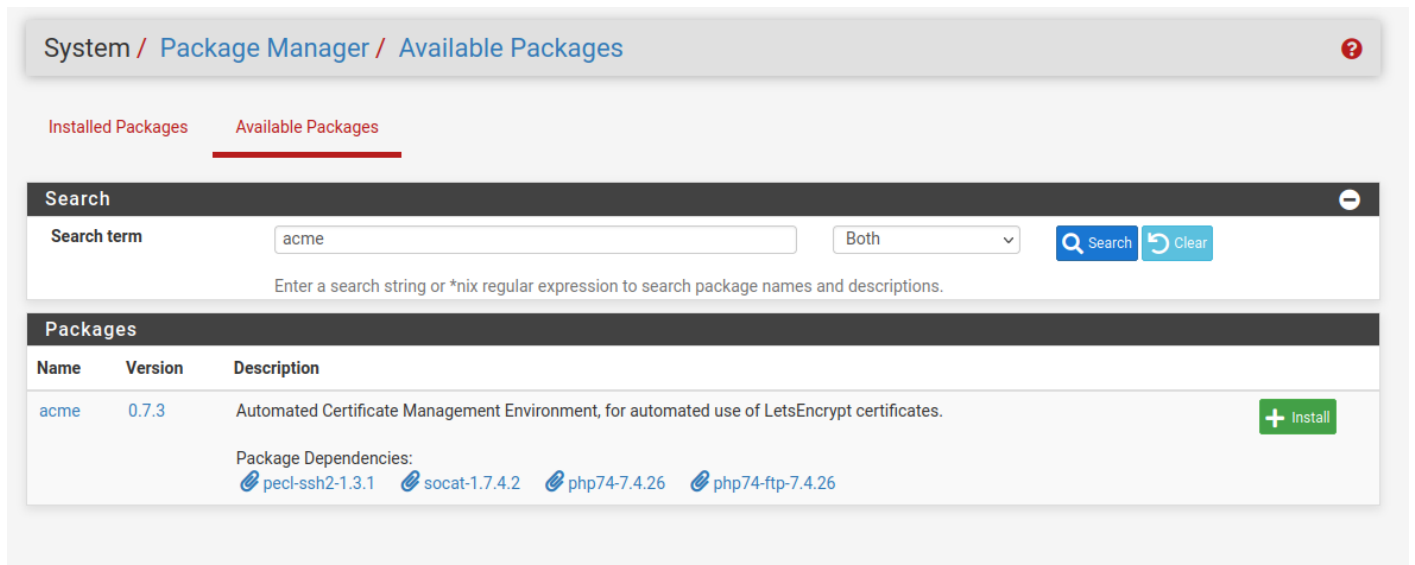


Acme Certificates with letsencrypt and cloudflare

This is to install and configure Acme certs with Letsencrypt as well as deploying HA Proxy for access to our internal services and add SSL services, we're using cloudflare for our cert verification.

On PfSense navigate to system/package manager/available packages

Search for acme and click install then on confirm



System / Package Manager / Available Packages

Installed Packages Available Packages

Search

Search term: Both

Enter a search string or *nix regular expression to search package names and descriptions.

Packages

Name	Version	Description
acme	0.7.3	Automated Certificate Management Environment, for automated use of LetsEncrypt certificates.

Package Dependencies: [pecl-ssh2-1.3.1](#) [socat-1.7.4.2](#) [php74-7.4.26](#) [php74-ftp-7.4.26](#)

[+ Install](#)

do the same for haproxy and install then click on confirm.

System / Package Manager / Available Packages

Installed Packages Available Packages

Search

Search term haproxy Both Search Clear

Enter a search string or *nix regular expression to search package names and descriptions.

Packages

Name	Version	Description	
haproxy	0.61_7	The Reliable, High Performance TCP/HTTP(S) Load Balancer. This package implements the TCP, HTTP and HTTPS balancing features from haproxy. Supports ACLs for smart backend switching. Package Dependencies:  haproxy18-1.8.30	+ Install

if you are installing this via the wan interface access, make sure you go back and disable packet filter as doing the installation will re enable, go to the shell and type `pfctl -d` to disable and gain access via WAN interface

Navigate to Services/Acme

go to Account keys and click add, fill out the information below, for ACME Server you can use production or test, its the same

click on create new account key then register acme account key, after you are done click save

Services / Acme / Certificate options: Edit ?

General settings Certificates Account keys

Edit Certificate options

Name

Description

ACME Server

Let's Encrypt Production ACME v2 (Applies rate limits to certificate r...

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-----
MIIJKAIBAAKCAgEAzfaaWYlmtw4A361bA/3WcodTgT6geufSp+ao,
oQm42DyEB3fuDCvesj24R0op4N5fyWUNYu0oZMgHBx16ykh9d3TQI
Uu5aR4pbANDBM+QmNi6oKpQ5LxE3NP/Sn10k14s5zffjWVBLkaDkl
cMYdcB/q/9cqZhJIkhICqWmos1ERN10qaAZDabfR88ysn1Y9DyJG...
```

☒ 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_issuercert.log for more information.

you have now your account key.

General settings Certificates Account keys

Account keys			
	Name	Description	CA
☐	tinodLAB	lab test	letsencrypt-production-2
<input checked="" type="button" value="Add"/> Delete Save			

Navigate to General Settings and select Enable Acme client renewal job to auto renew your certificates.

General settings Certificates Account keys

General settings

Cron Entry

☒ Enable Acme client renewal job. This will configure cron to renew certificates once a day at 3:16. Keeping track of the last successful renewal and the number of days set after to renew again. When renewal happens a service can be restarted or a shell script run to load the new certificate for services that need it, if needed this needs to be configured as an action under the certificate settings.

Write Certificates

☐ Write ACME certificates to /conf/acme/ in various formats for use by other scripts or daemons which do not integrate with the certificate manager.

now you can create your first certificate, navigate to certificates and click add, we're using cloudflare

General settings

Certificates

Account keys

Edit Certificate options

Name

pfsense

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

cert for pfsense

Status

Active

Acme Account

tinodLAB

Private Key

2048-bit RSA

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

Table

	Mode	Domainname	Method	Actions
☐	Enabled	*.tinod.c	DNS-Cloudflare	 
				 

For this lab we're using a wildcard certificate, for our domain we will do *.tinod.com

you need to get your key, token, account ID and Zone ID from cloudflare

Table			
Mode	Domainname	Method	Actions
☐ Enabled ▾	*.tinod.c	DNS-Cloudflare ▾	
Key: Cloudflare API Key			
Email: Cloudflare API Email Address			
Token: Cloudflare API Token			
Account ID: Cloudflare API Account ID			
Zone ID: Cloudflare API Zone ID			
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

click add and your cert will be ready and it will renew automatically

Revision #1
Created 31 March 2023 17:12:29 by Cesar Gzz
Updated 18 July 2023 01:43:01 by Cesar Gzz