



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 <u>mettre en place un reverse-proxy à l'aide du package HAPROXY</u> 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 <u>IETF RFC8555</u>. 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 :

Name	Mes_Certificats_LE		
Description	Certificata Letis Encrypt	Attention, le	e choix du serveur ACMI
ACME Server	Let's Encrypt Production ACME v2 (Applies rate limits to certificate The ACME server which will be used to issue certificates using this 10) Use testing servers until certificate validation works, then ewitch to production. Let's Encrypt ACMEv1 servers no longer allow new registrations, and in June 2021 they be	« Production » demandes de c votre configur	vous limite dans vos tentatives de ertificats ! Si vous souhaitez teste ration dans un premier temps
E-Mail Addreas	tutos info@tutos info.fr	optez plutôt po	our le serveur ACME « Staging » !
Account key			
ACME account registration	Create new second lar Project ACME second for 1 Before using an accounties, it measures are registered with the chosen ACME Server. Indicates a successful registration, X indicates a failure. In the case of a failure, check / tap/acme/_registerkey/acme_issuecert.log for mo To some 2	re information.	

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

Account key	BEGIN RSA PRIVATE KEY
	MIIJKAIBAAKCAgEAuUiJxPLcDM/xN8a

• 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 fullstack 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, <u>nous souhaitons que la connexion à chaque serveur soit sécurisée avec HTTPS</u> 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 e	ntrée à la zone DNS	Étape 2 sur 3	
* Les champs suivis d'un 1 Sous-domaine	astérisque sont obligatoires. proxmox1	.labo-sio.fr.	On indique ici le sous-domaine souhaité pour l'accès au 1 ^{er} serveur. Ici on a choisi « proxmoxr1 » afin d'avoir l'URL proxmox1.labo-sio.fr
TTL	Par défaut	~	
2 Cible *	10€ ◀	On indique ici no publique qui pointe	otre adresse IP vers notre box.
serveur1 IN A	106		
	Annuler Pré	3 écédent Suivant	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 optio	ns
1 Name	proxmox1.labo- (à votre convenance).
	The name set here will also be use
² Description	On indique une brève description (à votre convenance).
Status	Active
³ Acme Account	Certs.labo-sio . 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	Est all doma Examples: Domainname Method: Web Method: Web	e: www.example.com proot, Rootfolder: /u proot, Rootfolder: /tr	m sr/local/www/.well-known/a mp/haproxy_chroot/haproxy	icme-challenge/ webroot/.well-kno	wn/acme-challenge/
	Table				
	Table	Mode	5 Domainname		6 Method

- 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 » :

[001 001 10 10.49.00 0L1 2020]	olingie domain- proximoxoliabo siolit
[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_50MAnzVOv9U18DCnM18vUbH_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 :



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+CgAwlBAgISA+nozopOYLu5IFFbMHvTGkvwM
MDMxCzAJBgNVBAYTAIVTMRYwFAYDVQQKEw1MZXQnc
EwNSMTAwHhcNMjUwMTE4MTcwMjU2WhcNMjUwNDE4
ExRwcm94bW94NS5sYWJvLXNpbv5mciCCASIwDOYJKoZIhvcNAQEBBQADaaEPADCC

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

۰\$ ۰	1	proxmox5.labo-sio.fr	CertificatLE_proxmox5	certs.labo-sio.fr	Sat, 18 Jan 2025 19:01:27 +0100 Issued Certificate Dates:	Renew Issue
					Valid From: Sat, 18 Jan 2025 18:02:56 +0100 Valid Until: Fri, 18 Apr 2025 19:02:55 +0200	
					*	

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 » :

Services / Acme	/ Settings	0
eneral settings Cert	ificates Account keys	
eneral settings		
Cron Entry	Enable Acme client renewal job This will configure cro the number of days set after to renew again. When ren services that need it, if needed this needs to be config	in to renew certificates once a day at 3:16. Keeping track of the last successful renewal and rewal happens a service can be restarted or a shell script run to load the new certificate for ured as a action under the certificate settings.
Write Certificates	Write ACME certificates to /conf/acme/ in various for	La tâche « cron » permettra de renouveler le
	E Save	certificat au bout de 60 jours de façon automatisée et

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 :

Services / HAProxy / Backend / Edit							± ₩ 🗐 (
Settings	Frontend	Backend	File	s Stats	Stats FS	Templates					
dit HAProxy Backend server pool 1 Name proxmox1_backend On nomme, ici, le backend											
	1 Name	proximox	1_backen	d On	nomme, ici	, le backend					
	1 Name Server list	þroxmox Table	1_becken	d On	nomme, ici	, le backend					
	1 Name Server list 2	þroxmox Table	1_backen Mode	d On Name	nomme, ici Forwardto	, le backend Address	Port	Encrypt(SSL)	SSL checks	Weight	Actions

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** », <u>si plusieurs serveurs doivent être ajoutés au backend</u>, on peut cliquer l'option « **Round robin** » :

Loadbalancing optio	ns (when multiple servers are defined)
Balance	O None This allows writing your own custom balance settings into the advanced section. Or when you have no need for balancing with only 1 server.
	Round robin Each server is used in turns, according to their weights. This is the smoothest and fairest algorithm when the server's processing time remains equally distributed. This algorithm is dynamic, which means that server weights may be adjusted on the fly for slow starts for instance.

Health check method	HITP
	WITE projects for these on the servers Soult's, can also be automatic server (require attacking the NDE has for the
Check frequency	
00 393	milliseconds For HTTP:HTTPS delautts to 1000 if left blank. For TCP no sheck will be performed if left empty.
Log checks	When this option is esobled, any change of the health check status or to the server's health will be logged.
	- by default, failed in 2 are logged if server is UP and successful health checks are logged if server is DOVIN, so the amount of additional information is limit.
Http check method	CET v
	OPTIONS is the method usually best to perform server checks, HEAD and GET can also be used. If the server gets marked as down in the stats part then changing this to GET usually has the biggest chance of working, but might cause more processing overhead on the websever and is less easy fiber out of this box.

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 :

Service	s / HAPro	xy / Front	end / E	dit					C) ≟ Ш 🗏 😯
Settings	Frontend	Backend	Files	Stats	Stats FS	Templates				
dit HAP	roxy Fronten	d					_			
	1 Name	proxmox_from	nteod	On no	omme, ici	, le frontend				
2 Description		accès_srv_proxmox		On indique une brève description du frontend						
	3 Status	Active		On sé	lectionne	le statut « Act	ive »			
Exte	ernal address	Define what ip	port comb	inations to	listen on for in	comming connections	Le front	end écoutera	le nort 443 d	sur la WAN
		Liste	n address	a 3	Custom addre	ss Port	Le mont	SSL Offloadin	g Advanced	Action
	4	O.P. WA	N address	(IPv4) v		443		8	-	a (

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

Туре	http / https(offloading)	~	
	This defines the processing Please note that for https e	pe of HAProxy, and will determine the availabe options for acl checks and also several other options ryption/decryption on HAProxy with a certificate the processing type needs to be set to "http".	4

• Créez, ensuite, une ACL dans la partie « 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.						
	Table						
	Name	Expression	CS Not Value Ac	tions			
	D.P. and provemoral	1 Host matches:	3	mc			

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

Table							
Action	Parameters	Parameters Condition acl names					
🗆 🔂 🛛 Use Backend	See below	acl_proxmox1 2	<u>ā</u> Q				

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

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 "forwardtor" option creates an HTTP "X-Forwarded-For" header which contains the client's IP address. This is useful to let the final web set know what the client address was. (eg for statistics on domains)					
the thread and and an	http://keep-alive.(default)					
use impose option						

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

Note	SSL Offloading will reduce web servers load by maintaining and encrypting connection with users on internet while sending and retrieving data without encrytion 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	proxmox1.labo-sio.fr (CA: Acmecert: O=Let's Encrypt, CN=R10, C=Ut Choose the cert to use on this frontend. Add ACL for certificate CommonName. (host header matches the "CN" of the certificate)				

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 » :

ervices / HAPro	C : ≠ !!!		
Frontend	Backend Files Stats Stats FS Templates		
neral settings	Enable HAProxy		
Installed version	2.8.3-86e043a		
laximum connections	1000 per process.		Connections Memory usage
	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.		1 50 kB 1.000 48 MB 10.000 488 MB 100.000 4,8 GB Calculated for plain HTTP connections, using sol offloading will increase that
	When setting a high amount of allowed simultaneous connections you v kem.maxfiles and kem.maxfilesperproc. For HAProxy alone set these to connections these need to be 200.031 or more to avoid trouble, take into kem.maxfiles.	vill need to add and or incre at least the number of allow account that handles are a	ase the following two 'System Tunables' wed connections * 2 + 31. So for 100.000 also used by other processes when setting

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). <u>Il n'est plus utile d'indiquer le numéro</u> <u>de port « 8006 » de Proxmox</u>, 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 :

HAProxy stats Iscreen slots page			
AProxy version 2.8.3-86e043a,	released 2023/09/0	07	
Statistics Report for pid 27236			
General process information	10	10.0012.0017	ACHERCICA ON AN
ald = 27/236 (pascess #1, stapsoc = 1, staffward = 1)) patiens = holts constraints = a fill staff (staff fill = 7032) samsock = 2012; macrosom = -1000; machael = 0; macpipes = 0 parter const = -7, content pipes = 100; machael = 10xxx; bit roke = 01, 500 kbps huming tasks = 0/26; olis = 50 %	active UP active UP, going down active DOWN, going go active DOWN, going go active or backap DOWN and clearbo active or backap DOWN and clearbo active or backap DOWN and clearbo active or backap SOWT STOPPED for m New "NOUTPERNM" - UP with head back	Chapley option: ping down - Scope - High DC/W annex - High DC/W ann	Extendi responset - Extendi Anternational - Unidea (02.2) - Unidea (02.2) - Unidea (02.2) - Unidea (02.2)
AProxyLocalStats Cause Season rate Season	Oytes Denied Enters	Wanibga	Server
For Max Limit Cur Max Limit Cor Max, Limit Total LDT	Lant In Out Reg Renar Reg Casen 10	enprilleter Harden Statum LantChik Wybe A	et Bok Dik Owe Ownine: Torte
Packend 0 0 0 0 0 0 100 1	1 9 6 0 0 0 0	0 0 0 1d0hUP 000	0 0 0
Rearry Bentend) Dense Sension ple Sension Car Mar Linet Car Mar Linet Car Mar Linet fold Liber La Franked 8 2 6 8 1000 300	Bytes Daniel in Chri Hog Reng Hog 23568.449 45.700.073 0 0 27	Errora Warninga Casar Kasap Hati Kada Status LantChir Web DPEN	Sarver 6 Act Dela Clak Own Owenene Herle
mannal backend ipv/U(Y Dase Sector talsSectors	Done Deped In	nn Wimins	Sever
Cer Mos Link Cor Mos Link Cur Mos Link Total 1556 La	z la Char Ring Hongs Ring Co	en liese kiel koolis Status LastCha A	Wynt Act ISck Chie The Overtities That
	ls 1 (1) 026 5 964 910 0	0 0 0 0 3dh LP L70K0200 in 9ms	111 Y = 0 0 06 -

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