

Chapitre 1 B2 Mission 2 Pfsense HProxy

Table des Matières :

MISSION 2.....	2
----------------	---

MISSION 2

- Installation du paquet haproxy déjà faite (chapitre Bastion)

Système / Gestionnaire de paquets / Paquets disponibles

Paquets installés Paquets disponibles

Recherche

Terme de recherche haproxy Les deux Recherche Effacer

Entrer une phrase de recherche ou une expression régulière *nix pour rechercher dans les noms et description de paquets.

Nom	Version	Description	
haproxy	0.63_11	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. Dépendances du paquet: haproxy29-2.9.14	+ Install
haproxy-devel	0.64_2	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. Dépendances du paquet: haproxy-devel-3.0.d13	+ Install

- On réalise un clone de DS2, nous modifions le répertoire /etc/hostname, /etc/hosts ainsi que /etc/network/interfaces. La passerelle est la VIP DMZ.

```
DS2 [En fonction] - Oracle VirtualBox
Fichier  Machine  Écran  Entrée  Périphériques  Aide
GNU nano 7.2 /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug enp0s3
iface enp0s3 inet static
address 192.168.2.1
netmask 255.255.255.0
network 192.168.2.0
broadcast 192.168.2.255
gateway 192.168.2.252
dns-search sio-exupery.fr
dns-domain sio-exupery.fr
dns-nameservers 192.168.2.1
```

```

Clone de DS2.2 [En fonction] - Oracle VirtualBox
Fichier  Machine  Écran  Entrée  Périphériques  Aide
GNU nano 7.2 /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).
source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug enp0s3
iface enp0s3 inet static
address 192.168.2.2
netmask 255.255.255.0
network 192.168.2.0
broadcast 192.168.2.255
gateway 192.168.2.252
dns-search sio-exupery.fr
dns-domain sio-exupery.fr
dns-nameservers 192.168.2.2
    
```

- Nous ajoutons un Backend pour les deux serveurs web :

Services / HAProxy / Backend

Settings Frontend Backend Files Stats Stats FS Templates

Advanced	Name	Servers	Check	Frontend	Actions
	sio-exupery	2	HTTP	http_access_DS2	

Ajouter Supprimer Enregistrer

Services / HAProxy / Backend / Edit

Settings Frontend Backend Files Stats Stats FS Templates

Edit HAProxy Backend server pool

Nom: sio-exupery

Server list

Mode	Name	Forwardto	Address	Port	Encrypt(SSL)	SSL checks	Weight	Actions
<input type="checkbox"/>	active	DS2.1	Address+Port:	192.168.2.1	80	no	no	
<input type="checkbox"/>	active	DS2.2	Address+Port:	192.168.2.2	80	no	no	

Field explanations:

Loadbalancing options (when multiple servers are defined)

Balance

Aucun
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 checking	
Health check method	<input type="text" value="HTTP"/> <small>HTTP protocol to check on the servers health, can also be used for HTTPS servers (requires checking the SSL box for the</small>
Check frequency	<input type="text"/> milliseconds For HTTP/HTTPS defaults to 1000 if left blank. For TCP no check will be performed if left empty.
Log checks	<input checked="" type="checkbox"/> When this option is enabled, any change of the health check status or to the server's health will be logged. By default, failed health check are logged if server is UP and successful health checks are logged if server is DOWN, so the amount of additional information is limited.
Http check method	<input type="text" value="GET"/> 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 page then changing this to GET usually has the biggest chance of working, but might cause more processing overhead on the webserver and is less easy to filter out of its logs.
Url used by http check requests.	<input type="text"/> Defaults to / if left blank.
Http check version	<input type="text"/> Defaults to "HTTP/1.0" if left blank. Note that the Host field is mandatory in HTTP/1.1, and as a trick, it is possible to pass it after "\r\n" following the version string like this: <code>HTTP/1.1\r\nHost: www</code> Also some hosts might require an accept parameter like this: <code>HTTP/1.0\r\nHost: webservername:8080\r\nAccept: */*</code>

▪ Nous ajoutons un second Frontend (VIP WAN) :

The screenshot shows the pfSense HAProxy Frontend configuration page. A notification at the top states: "The haproxy configuration has been changed. You must apply the changes in order for them to take effect." Below this, there are tabs for Settings, Frontend, Backend, Files, Stats, Stats FS, and Templates. The "Frontends" section contains a table with the following data:

Primary	Shared	On	Advanced	Name	Description	Address	Type	Backend	Actions
<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	http_access_DS2	Cluster DS2.1 et DS2.2	192.168.1.103:80	http	sio-exupery (default)	Edit Delete Clone

Buttons at the bottom of the table include "Ajouter", "Supprimer", and "Enregistrer".

The screenshot shows the "Edit HAProxy Frontend" configuration page for the "http_access_DS2" frontend. The configuration fields are as follows:

- Nom:** http_access_DS2
- Description:** Cluster DS2.1 et DS2.2
- État:** Actif
- External address:** Define what ip:port combinations to listen on for incoming connections.

Listen address	Custom address	Port	SSL Offloading	Advanced	Act
<input type="checkbox"/> 192.168.1.103 (CARP WAN)	<input type="text"/>	80	<input type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>

NOTE: You must add a firewall rules permitting access to the listen ports above.
If you want this rule to apply to another IP address than the IP address of the interface chosen above, select it here (you need to define Virtual IP addresses on the first). Also note that if you are trying to redirect connections on the LAN select the "any" option. In the port to listen to, if you want to specify multiple ports, separate them with a comma (,). EXAMPLE: 80,8000 Or to listen on both 80 and 443 create 2 rows in the table where for the 443 you would likely want to check the SSL-offloading checkbox.
- Max connections:** Sets the maximum amount of connections this frontend will accept, may be left empty.
- 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'.

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
Backend1acl	Host matches			www.yourdomain.tld	
addHeaderAc	SSL Client certificate valid				

- 'CS' makes the string matches 'Case Sensitive' so www.domain.tld will not be the same as WWW.domain.TLD
 - 'Not' makes the match if the value given is not matched
 Example:

Name	Expression	CS	Not	Value
Backend1acl	Host matches			www.yourdomain.tld
addHeaderAc	SSL Client certificate valid			

acl's with the same name will be 'combined' using OR criteria.
 For more information about ACLs please see [HAProxy Documentation](#) Section 7 - Using ACLs

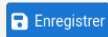
NOTE Important change in behaviour, since package version 0.32
 -acl's are no longer combined with logical AND operators, list multiple acl's below where needed.
 -acl's alone no longer implicitly generate use_backend configuration. Add 'actions' below to accomplish this behaviour.

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
Use Backend	Website1Backend	Backend1acl	
http-request header set	Headername: X-HEADER-ClientCertValid New logformat value: YES	addHeaderAc	

Default Backend

If a backend is selected with actions above or in other shared frontends, no default is needed and this can be left to "None".



pfSense COMMUNITY EDITION

Système Interfaces Pare-feu Services VPN État Diagnostics Aide

Services / HAProxy / Paramètres

Settings Frontend Backend Files Stats Stats FS Templates

General settings

Enable HAProxy

Installed version 2.9.14-7c591d5

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 'System Tunables' settings:
 'kern.maxfiles': 63729
 'kern.maxfilesperproc': 57348
 Full memory usage will only show after all connections have actually been used.

Connections	Memory usage
1	50 kB
1000	48 MB
10000	488 MB
100000	4.8 GB

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

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.

Number of threads to start per process
 Defaults to 1 if left blank (2 CPU core(s) detected).
 FOR NOW, THREADS SUPPORT IN HAPROXY 1.8 IS HIGHLY EXPERIMENTAL AND IT MUST BE ENABLED WITH CAUTION AND AT YOUR OWN RISK.

Reload behaviour Force immediate stop of old process on reload. (closes existing connections)
 Note: when this option is selected, connections will be closed when haproxy is restarted. Otherwise the existing connections will be served by the old haproxy process until they are closed. Checking this option will interrupt existing connections on a restart (which happens when the configuration is applied, but possibly also when pfSense detects an interface coming up or a change in its ip-address.)

Reload stop behaviour
 Defines the maximum time allowed to perform a clean soft-stop. Defaults to 15 minutes, but could also be defined in different units like 30s, 15m, 3h or 1d.

Carp monitor
 Monitor carp interface and only run haproxy on the firewall which is MASTER.

Stats tab, 'internal' stats port

Internal stats port EXAMPLE: 2200
 Sets the internal port to be used for the stats tab. This is bound to 127.0.0.1 so will not be directly exposed on any LAN/WAN/other interface. It is used to internally pass through the stats page. Leave this setting empty to remove the "HAProxyLocalStats" item from the stats page and save a little on resources.

Internal stats refresh rate Seconds, Leave this setting empty to not refresh the page automatically. EXAMPLE: 10

Sticktable page refresh rate Seconds, Leave this setting empty to not refresh the page automatically. EXAMPLE: 10

▪ Règle de pare feu pour autoriser les flux HAProxy sur la WAN :

pfSense SYSTEME | Interfaces | Pare-feu | Services | VPN | État | Diagnostics | Aide

Pare-feu / Règles / WAN

Flottant(e) | **WAN** | LAN | OPT1 | OPT2

Règles (Faire glisser pour changer l'ordre)

<input type="checkbox"/>	États	Protocole	Source	Port	Destination	Port	Passerelle	File d'attente	Ordonnement	Description	Actions
<input type="checkbox"/>	0/3 KiB	IPv4 ICMP any	*	*	*	*	*	aucun			
<input type="checkbox"/>	0/0 B	IPv4 TCP	*	*	*	*	*	aucun			
<input type="checkbox"/>	0/0 B	IPv4 TCP	192.168.1.0/24	*	WAN address	*	*	aucun		Administration depuis WAN	
<input checked="" type="checkbox"/>	0/0 B	IPv4 TCP	*	*	192.168.1.103	80 (HTTP)	*	aucun		Autoriser les flux vers HAPROXY	

Ajouter | Ajouter | Supprimer | Toggle | Copier | Enregistrer | Séparateur

- On modifie le fichier des hôtes virtuels /etc/apache2/sites-available/sites-sio.conf de DS2-2 :

```
Clone de DS2.2 [En fonction] - Oracle VirtualBox
Fichier  Machine  Écran  Entrée  Périphériques  Aide
GNU nano 7.2 /etc/apache2/sites-available/sites-sio.conf
<VirtualHost 192.168.2.9:443>
  ServerName secu.sio-exupery.fr
  ServerAdmin webmaster@localhost
  DocumentRoot /var/www/html/secu
  ErrorLog /var/www/html/secu/logs/error.log
  CustomLog /var/www/html/secu/logs/access.log combined
  SSLEngine on
  LogLevel info
</VirtualHost>
<VirtualHost 192.168.2.2:80>
  ServerName www.sio-exupery.fr
  ServerAdmin webmaster@localhost
  DocumentRoot /var/www/html/web
  ErrorLog /var/www/html/web/logs/error.log
  CustomLog /var/www/html/web/logs/access.log combined
</VirtualHost>
<VirtualHost 192.168.2.2:80>
  ServerName projet1.sio-exupery.fr
  ServerAdmin webmaster@localhost
  DocumentRoot /var/www/html/projet1/repweb
  ErrorLog /var/www/html/projet1/repweb/logs/error.log
  CustomLog /var/www/html/projet1/repweb/logs/access.log combined
</VirtualHost>
<VirtualHost 192.168.2.2:80>
  ServerName projet2.sio-exupery.fr
  ServerAdmin webmaster@localhost
  DocumentRoot /var/www/html/projet2/repweb
  ErrorLog /var/www/html/projet2/repweb/logs/error.log
  CustomLog /var/www/html/projet2/repweb/logs/access.log combined
</VirtualHost>
<VirtualHost 192.168.2.2:80>
  ServerName blog.sio-exupery.fr
  ServerAdmin webmaster@localhost
  DocumentRoot /var/www/html/sitewordpress/wordpress
  ErrorLog /var/www/html/sitewordpress/wordpress/logs/error.log
  CustomLog /var/www/html/sitewordpress/wordpress/logs/access.log combined
</VirtualHost>
```

- Nous rechargeons Apache2 : systemctl reload apache2

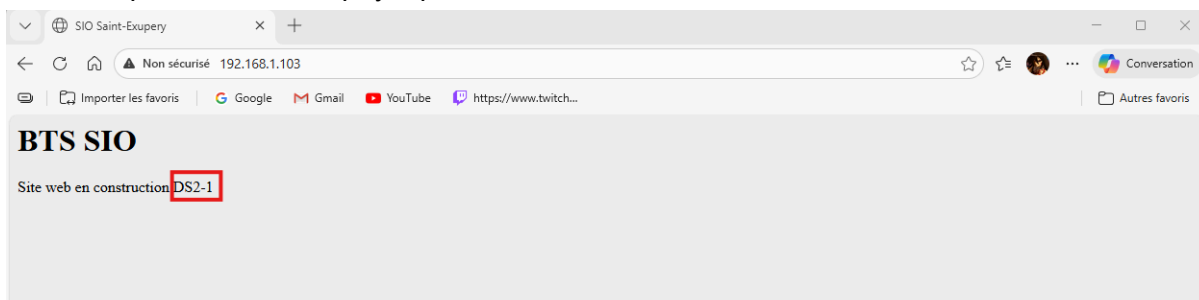
```
Clone de DS2.2 [En fonction] - Oracle VirtualBox
Fichier  Machine  Écran  Entrée  Périphériques  Aide
root@DS2: ~#systemctl reload apache2
root@DS2: ~#_
```

- Nous modifions la page index.html du répertoire /var/www/html/web pour les deux machines DS1-1 et DS2- 2 :

```
DS2 [En fonction] - Oracle VirtualBox
Fichier  Machine  Écran  Entrée  Périphériques  Aide
GNU nano 7.2 /var/www/html/web/index.html
<html>
<head>
<title>SIO Saint-Exupery</title>
</head>
<body bgcolor="#EEEEEE">
<h1>BTS SIO</h1>
<p>Site web en construction DS2-1</p>
</body>
</html>
```

```
Clone de DS2.2 [En fonction] - Oracle VirtualBox
Fichier  Machine  Écran  Entrée  Périphériques  Aide
GNU nano 7.2 /var/www/html/web/index.html
<html>
<head>
<title>SIO Saint-Exupery</title>
</head>
<body bgcolor="#EEEEEE">
<h1>BTS SIO</h1>
<p>Site web en construction DS2-2</p>
</body>
</html>
```

- Tests depuis la machine physique :



- Nous rafraîchissons la page

