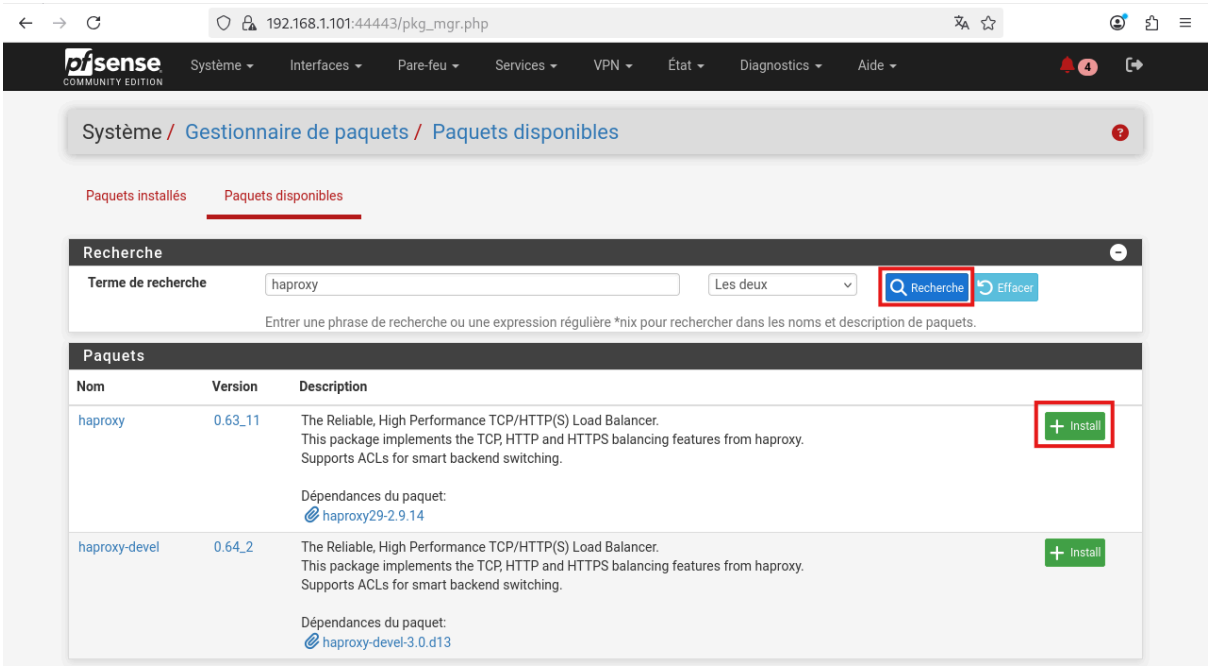
Chapitre 1 B2 Mission 2 Pfsense HAproxy

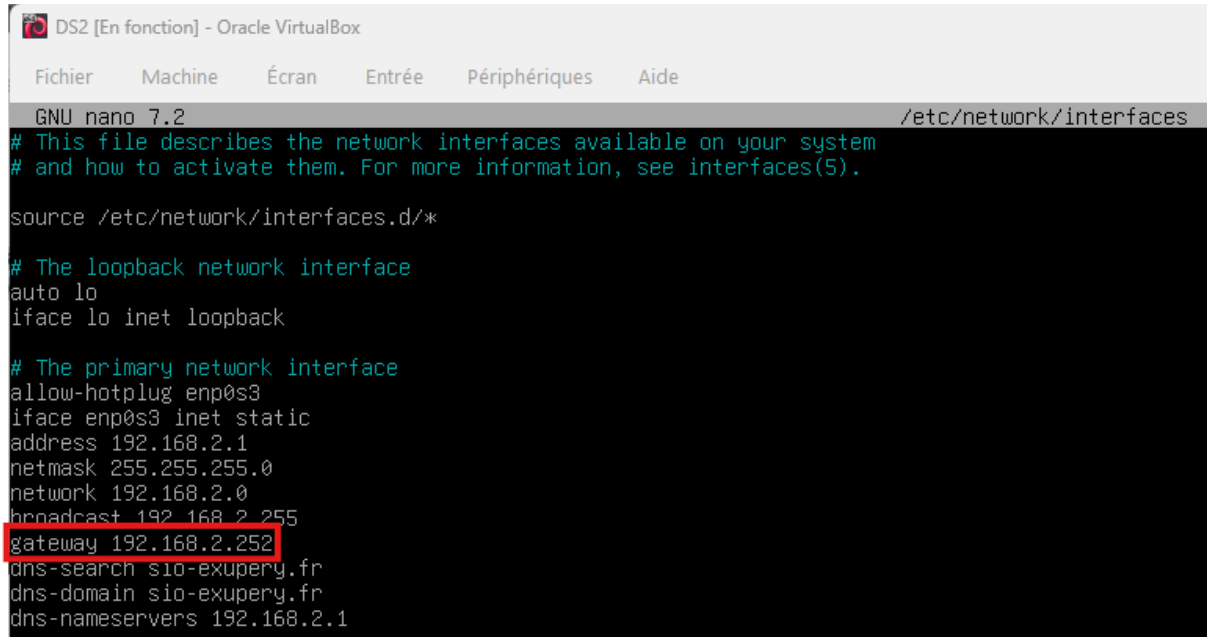
Table des Matières :

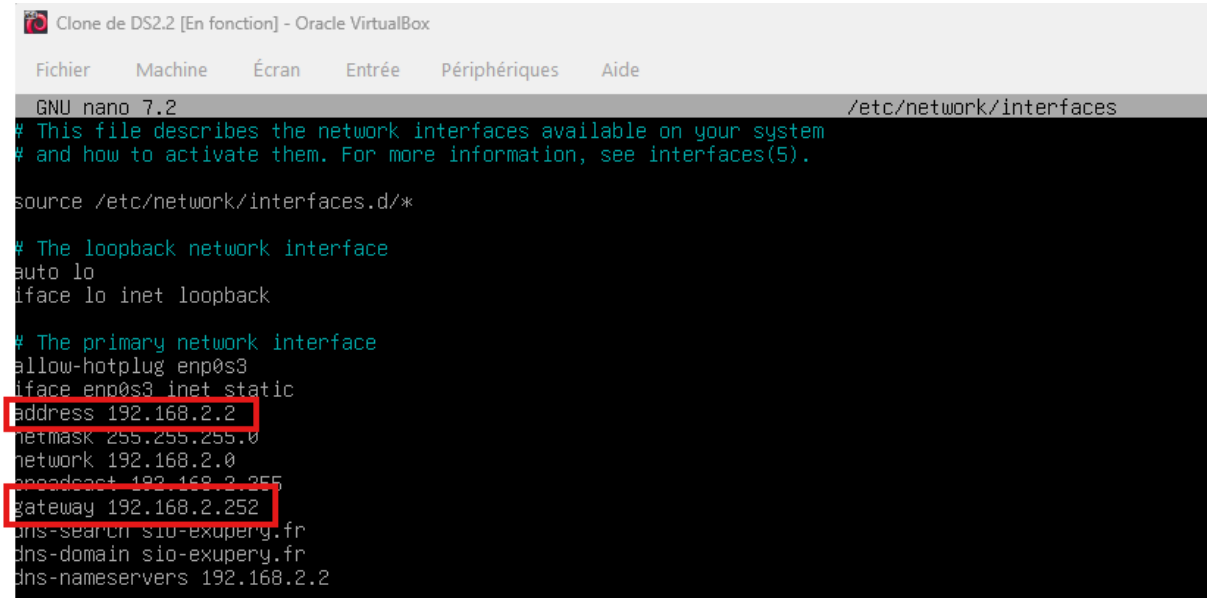
MISSION 2

▪ Installation du paquet haproxy déjà faite (chapitre Bastion)

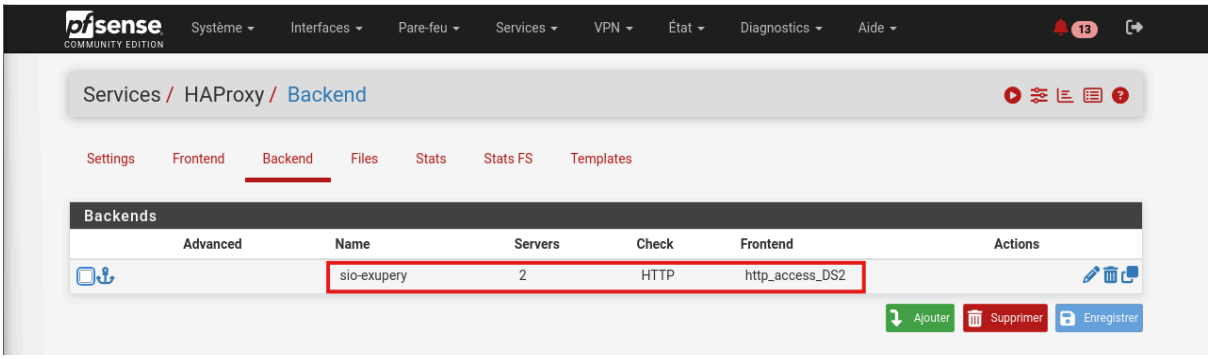


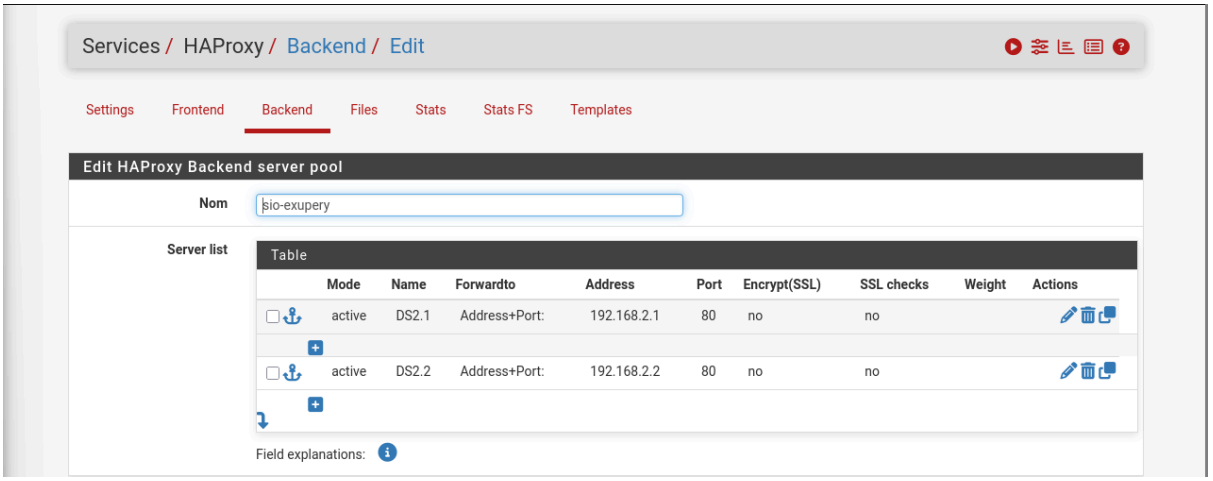
▪ On réalise un clone de DS2, nous modifions le répertoire /etc/hostname, /etc/hosts ainsi que /etc/network/interfaces. La passerelle est la VIP DMZ.

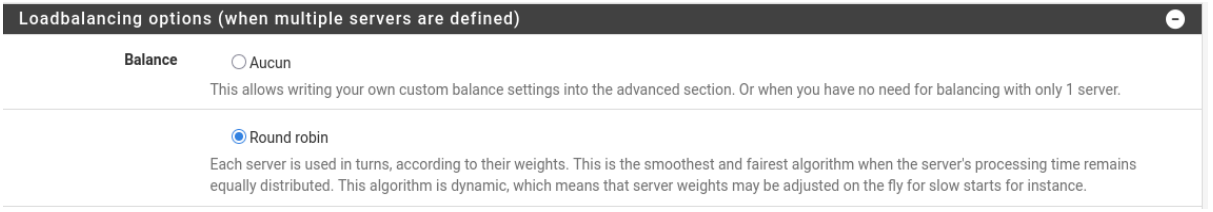




- Nous ajoutons un Backend pour les deux serveurs web :





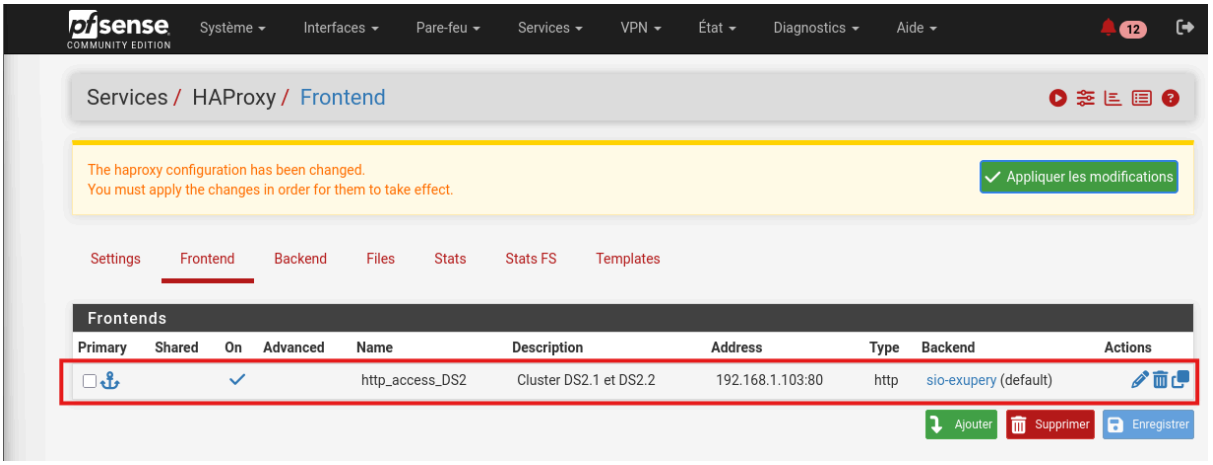


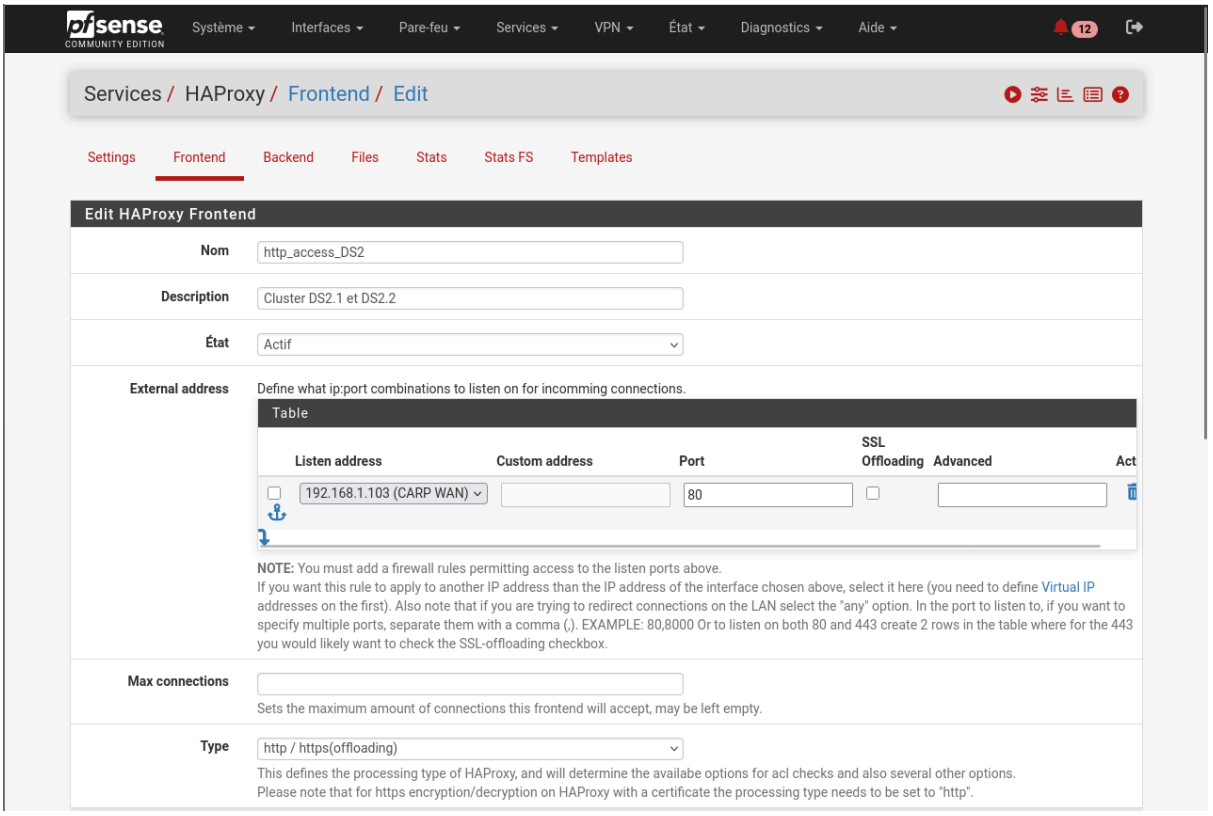
Health checking

Health check method	HTTP `HTTP protocol to check on the servers health, can also be used for HTTPS servers(requirs checking the SSL box for the`
Check frequency	milliseconds For HTTP/HTTPS defaults to 1000 if left blank. For TCP no check will be performed if left empty.
Log checks	☑ 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	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.	Defaults to / if left blank.

Http check version	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:
	`HTTP/1.1\r\nHost:\ www`
	Also some hosts might require an accept parameter like this:
	`HTTP/1.0\r\nHost:\ webservername:8080\r\nAccept:\ */*`

▪ Nous ajoutons un second Frontend (VIP WAN) :





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	Actions

- 'CS' makes the string matches 'Case Sensitive' so www.domain.tld wil 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
addHeaderAcl	SSL Client certificate valid			

acl's with the same name will be 'combined' using OR criteria.
For more information about ACL's please see HAProxy Documentation Section 7 - Using ACL's

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.

Table

Action	Parameters	Condition acl names	Actions

Example:

Action	Parameters	Condition
Use Backend	Website1Backend	Backend1acl
http-request header set	Headername: X-HEADER-ClientCertValid New logformat value: YES	addHeaderAcl

Default Backend

sio-exupery

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

Enregistrer

pfSense COMMUNITY EDITION — Système — Interfaces — Pare-feu — Services — VPN — État — Diagnostics — Aide — 13

Services / HAProxy / Paramètres

Settings | Frontend | Backend | Files | Stats | Stats FS | Templates

General settings

Enable HAProxy

Installed version 2.9.14-7c591d5

Maximum connections 1000 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
1.000	48 MB
10.000	488 MB
100.000	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 1

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)

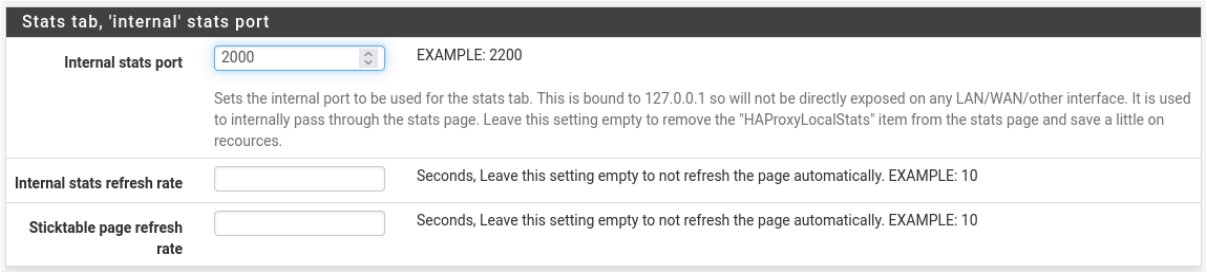
Note: when this option is selected, connections will be closed when haproxy is restarted. Otherwise the existing connections will be served by the old haproxy process until they are closed. Checking this option will interrupt existing connections on a restart (which happens when the configuration is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

Reload stop behaviour 15m

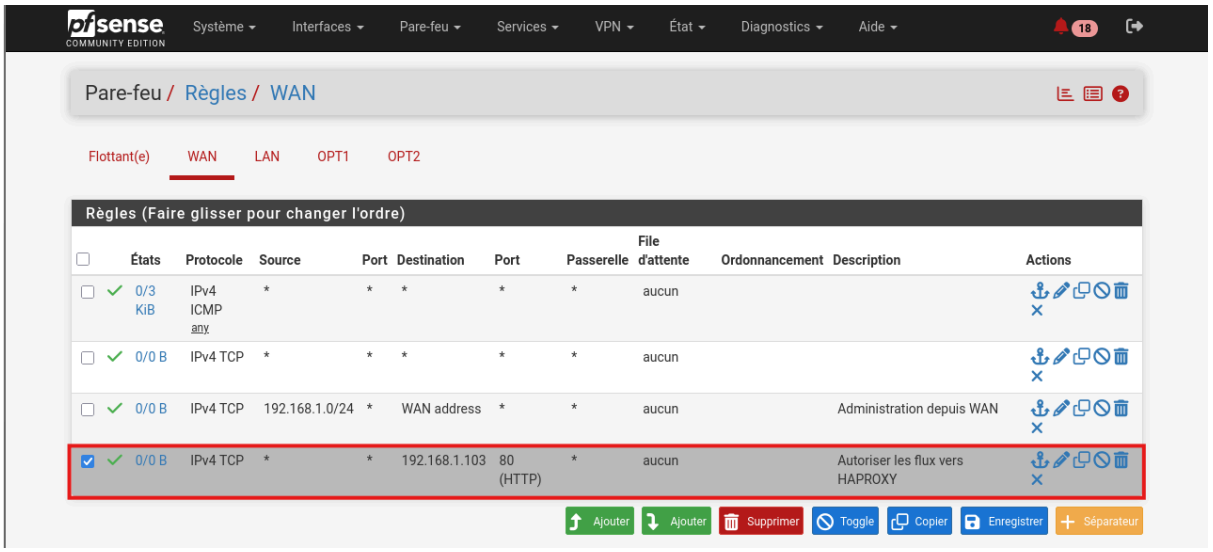
Defines the maximum time allowed to perform a clean soft-stop. Defaults to 15 minutes, but could also be defined in different units like 30s, 15m, 3h or 1d.

Carp monitor Désactivé

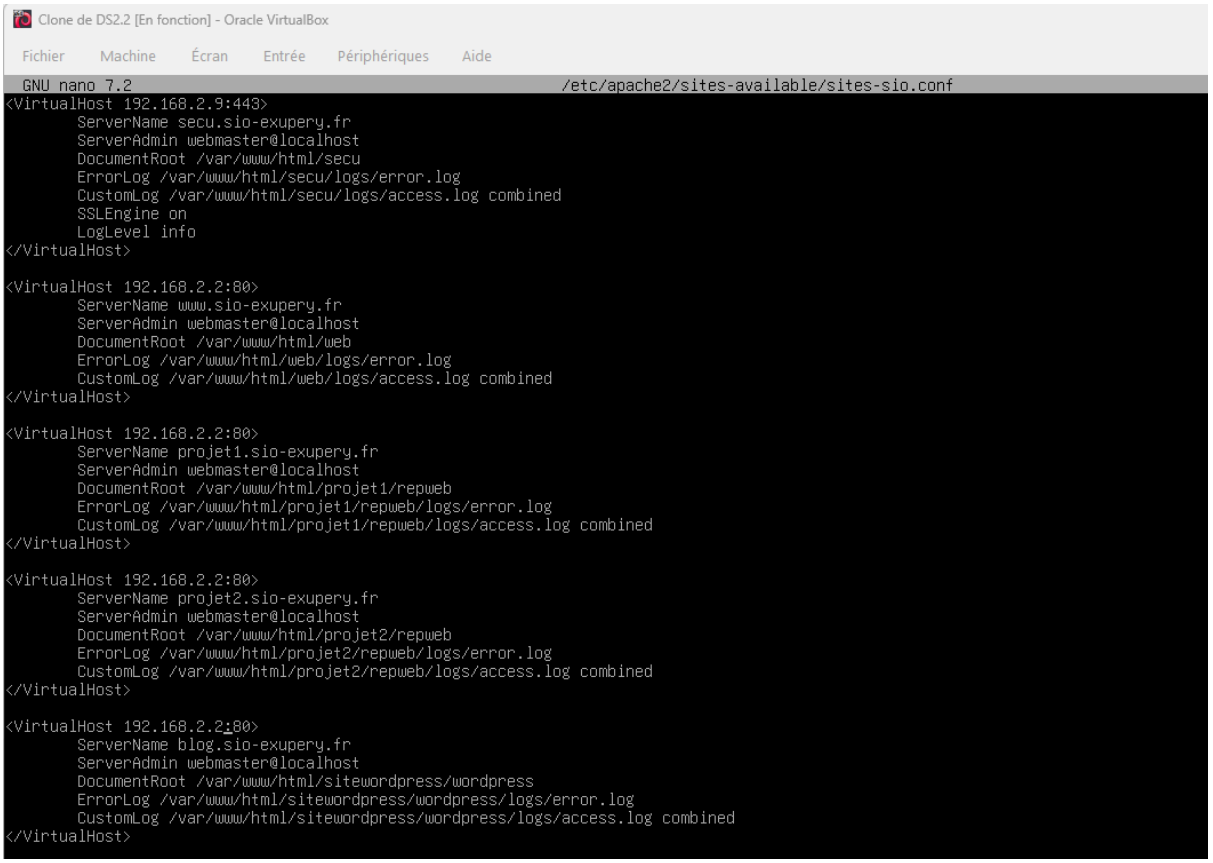
Monitor carp interface and only run haproxy on the firewall which is MASTER.



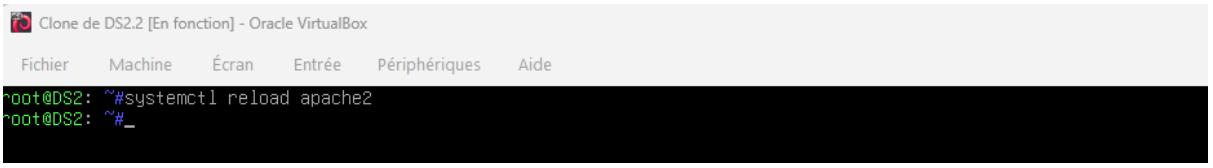
- Règle de pare feu pour autoriser les flux HAProxy sur la WAN :



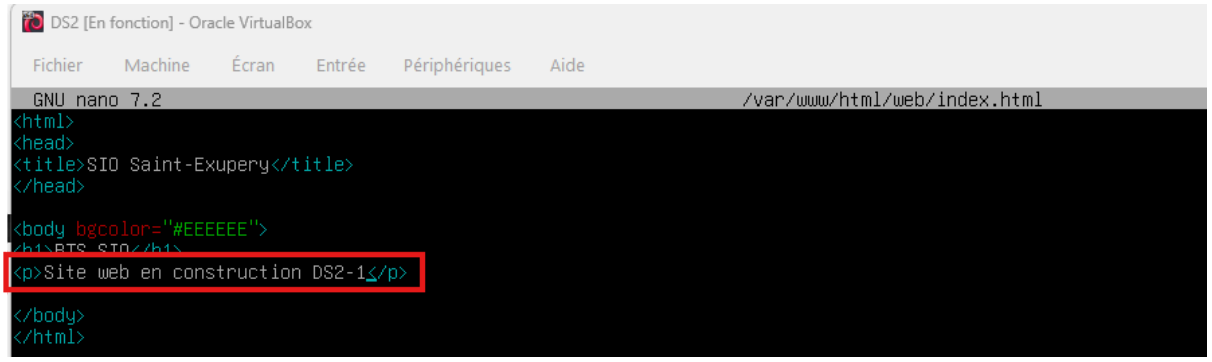
▪ On modifie le fichier des hôtes virtuels /etc/apache2/sites-available/sites-sio.conf de DS2-2 :

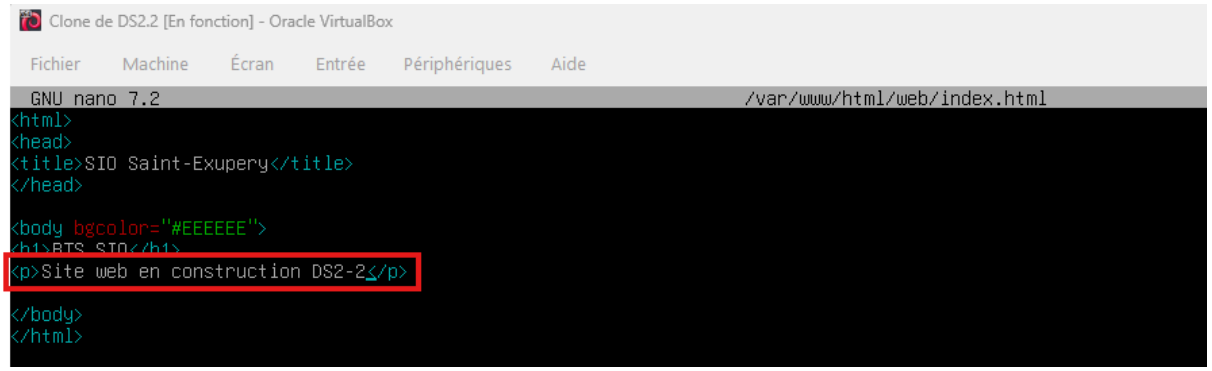


▪ Nous rechargeons Apache2 : systemctl reload apache2

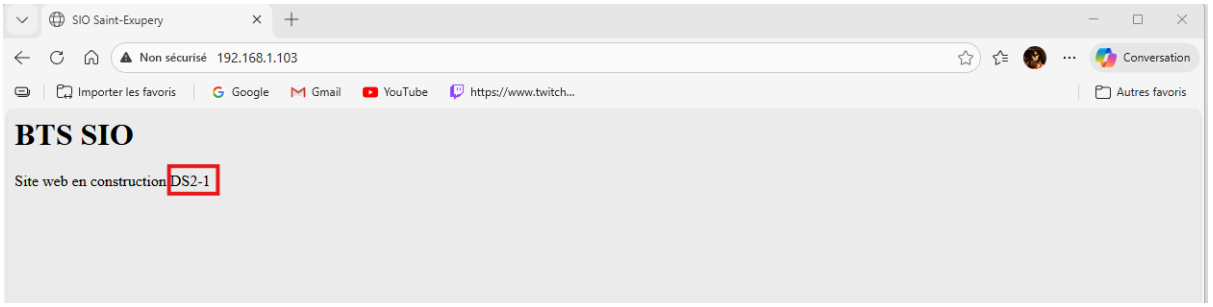


▪ Nous modifions la page index.html du répertoire /var/www/html/web pour les deux machines DS1-1 et DS2- 2 :





▪ Tests depuis la machine physique :



▪ Nous rafraîchissons la page