

Thème 1 : Load Balancing et Fail-Over

Sommaire :

- 1) Pré-requis
- 2) Partie 1 : Load Balancing
 - Schéma de l'infrastructure réseau
 - Répartition des charges entre 2 serveurs web
 - Tests
- 3) Partie 2 : Mise en place du routeur de secours
 - Schéma de l'infrastructure réseau
 - Configuration de pfsync
 - Tests

Prérequis :

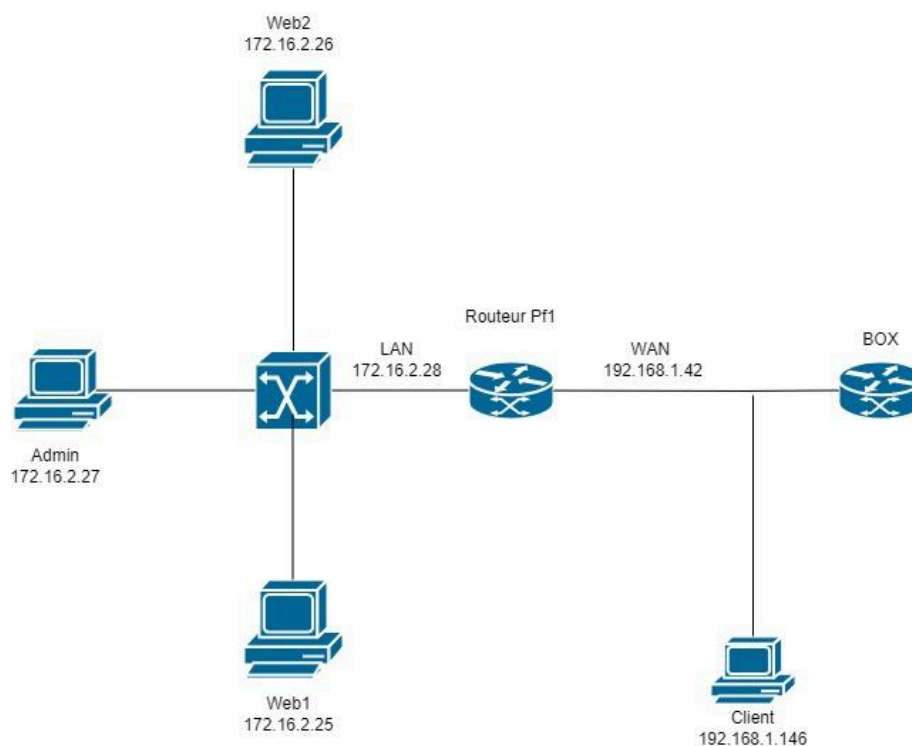
- 1 machine cliente
- 1 machine Admin Xubuntu 18.04
- 2 serveur Webs WordPress (Partie 1)
- 2 Routeurs PFSense

Partie 1 : Load Balancing

1) Schéma de l'infrastructure réseau

Réseau LAN : 172.16.0.0/16

Réseau WAN : 192.168.1.0/24



Nb : Afin de pouvoir continuer le TP en dehors du labo, j'ai dû me placer dans le même domaine de diffusion que ma box personnelle et donc être dans le réseau 1. Idem pour la partie 2

2) Répartition des charges entre 2 serveurs web

a) Ajout d'un Pool load-balancing

Services / Load Balancer / Pools

Refresh

Help

Stats

Menu

Help

Pools

Virtual Servers

Monitors

Settings

Pool

Name	Mode	Servers	Port	Monitor	Description	Actions
pool_serv_web	loadbalance	172.16.2.25 172.16.2.26	80	HTTP	pool_serveur_web	<div><div></div><div></div><div></div></div>

+

Add

On crée un pool d'adresse dans lequel sont regroupés les 2 serveurs web en port 80 HTTP afin que PFSense puisse gérer les requêtes et déterminer quel serveur répondra en premier

b) Création du Serveur Virtuelle

Services / Load Balancer / Virtual Servers




Pools

Virtual Servers

Monitors

Settings

Virtual Servers

Name	Protocol	IP Address	Port	Pool	Fallback pool	Description	Actions
Vserverweb	tcp	192.168.1.42	8084	pool_serv_web	none	serveur virtuelle	  

+

Add

Ensuite, on y ajoute un serveur virtuel. Ce serveur fonctionne comme une passerelle unique qui est liée au pool contenant les 2 serveurs web. Ils envoient leurs requêtes directement à l'adresse IP virtuelle (192.168.2.42) port 8084 publique

Règle de filtrage :




Floating


WAN


LAN


PFSYNC


Rules (Drag to Change Order)


<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓	1 / 476 KiB	IPv4 *	*	*	172.16.0.0/16	*	*	none		  

 Add

 Add

 Delete

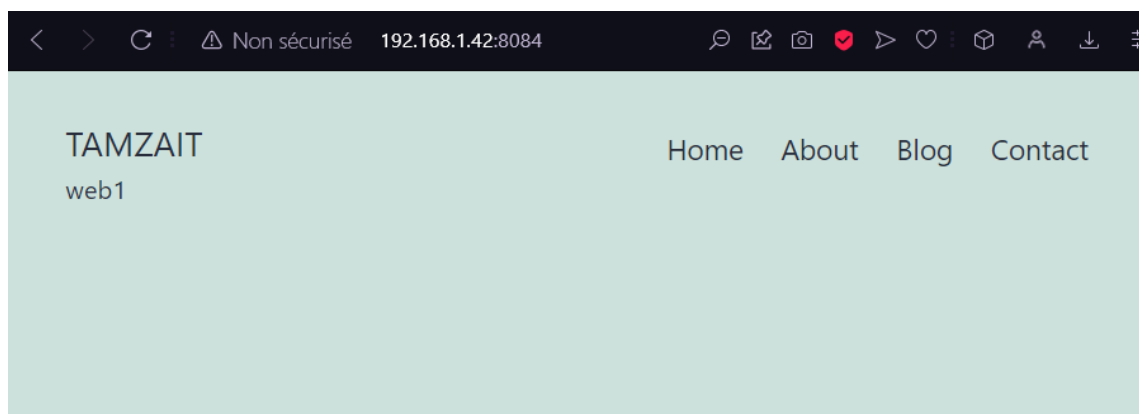
 Save

 Separate

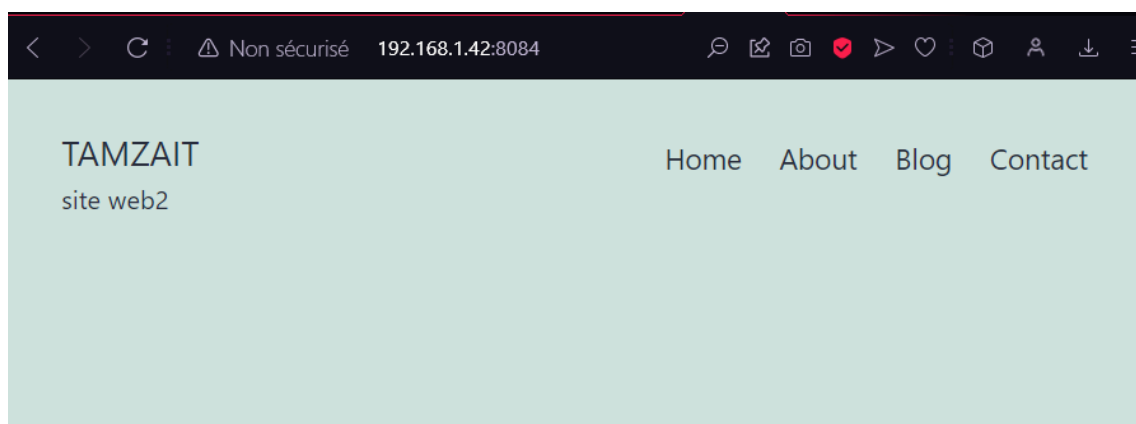
Afin d'ajouter une sécurité supplémentaire, on ajoute une règle ou on autorise toutes connexion entrante (depuis n'importe quelle IP et port source) a destination du réseau 172.16.0.0/16

3) Tests

Depuis une machine cliente hors réseau interne, on saisit depuis un navigateur, l'IP et le port du serveur virtuelle



En rafraichissant la page, pfsense effectue un basculement vers le deuxième site web et inversement

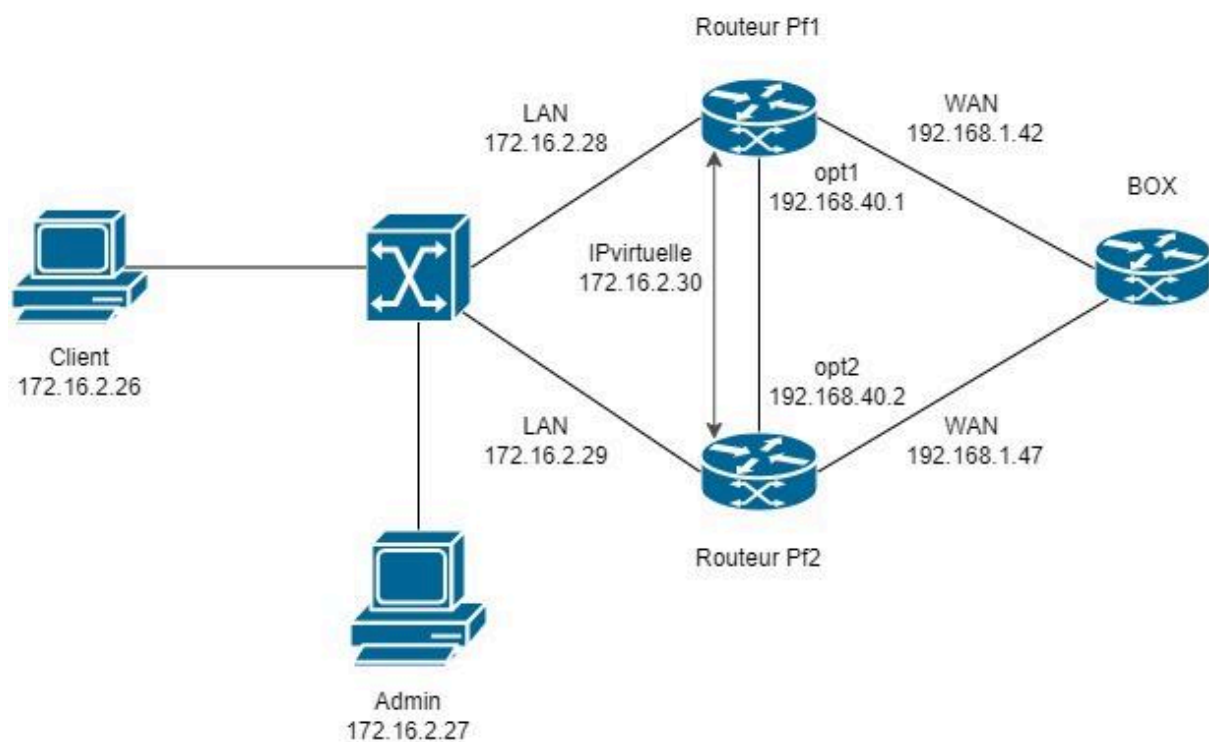


Partie 2 : Mise en place du routeur de secours

1) Schéma de l'infrastructure réseau

ajout d'un routeur esclave Pfense 2

ajout de l'interface pfsync sur les 2 routeurs + sur interface pfSense



Pf1 :

```
*** Welcome to pfSense 2.4.5-RELEASE-p1 (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4: 192.168.1.42/24
LAN (lan)      -> em1      -> v4: 172.16.2.28/16
PFSYNC (opt1)  -> em2      -> v4: 192.168.40.1/24
```

WARNING: The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

Status / CARP

[Temporarily Disable CARP](#) [Enter Persistent CARP Maintenance Mode](#)

CARP Interface	Virtual IP	Status
LAN@1	172.16.2.30/16	MASTER

pfSync Nodes

pfSync nodes:

- 59fda9de
- 9ac3f569

Pf2 :

```
*** Welcome to pfSense 2.4.5-RELEASE-p1 (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4: 192.168.2.47/24
LAN (lan)      -> em1      -> v4: 172.16.2.29/16
PFSYNC (opt1)  -> em2      -> v4: 192.168.40.2/24
```

WARNING: The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

Status / CARP

[Temporarily Disable CARP](#) [Enter Persistent CARP Maintenance Mode](#)

CARP Interface	Virtual IP	Status
LAN@1	172.16.2.30/16	BACKUP



pfSync Nodes

pfSync nodes:

- 59fda9de
- 9ac3f569

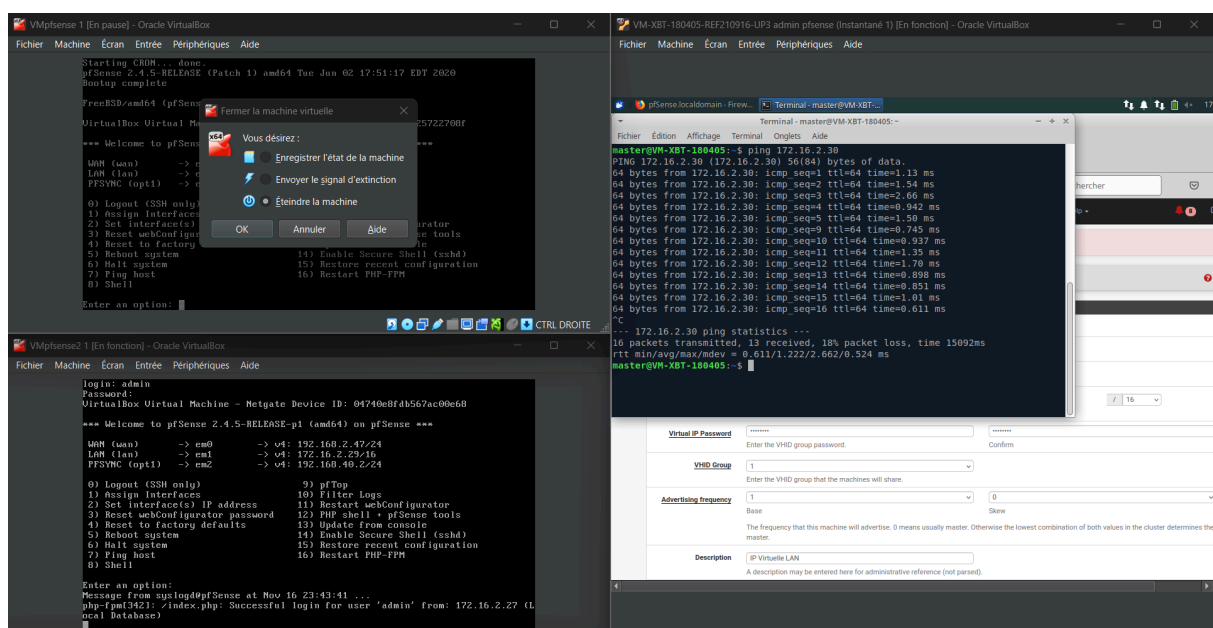
2) Configuration de pfsync

L'activation de la synchronisation s'effectue à l'aide du protocole CARP (protocole permettant à plusieurs machines de partager une même adresse IP) dans lequel on ajoute l'IP virtuel : 172.16.2.30 sur le routeur maître. Celui-ci traite tout le trafic et va transmettre ses informations (règles de filtrage, IP virtuelle etc...) vers l'esclave qui tourne en arrière-plan. Dans le cas où le maître tombe en panne, l'esclave prendra donc le rôle du routeur principal.

Firewall / Virtual IPs				
Virtual IP Address				
Virtual IP address	Interface	Type	Description	Actions
172.16.2.30/16 (vhid: 1)	LAN	CARP	IP Virtuelle LAN	 

3) Tests

Depuis la machine admin, on effectue un ping de l'IP virtuelle commun aux deux routeurs en arrêtant brusquement le routeur principal



The screenshot displays the pfSense configuration interface and terminal output. The top left window shows the 'Virtual IP Address' table with the entry 172.16.2.30/16 (vhid: 1) on the LAN interface. The top right window shows a terminal window running a ping command to 172.16.2.30, showing successful results. The bottom left window shows the pfSense command line interface with a list of configuration steps. The bottom right window shows the 'Virtual IP Password' dialog box.

Dans un premier temps, lorsque les 2 machines étaient en marche, étant donné que le routeur principal fonctionnait, tous les flux étaient redirigés à destination du maître.

Cependant, au moment où on a interrompu le routeur principal, le protocole CARP a détecté que le routeur principal ne parvenait plus à traiter les requêtes. Après un délai de quelques secondes (recensé dans le ping), l'esclave est passé en tant que maître.

https://172.16.2.29/status_carp.php80 %

Rechercher

pfSense

COMMUNITY EDITION

System

Interfaces

Firewall

Services

VPN

Status

Diagnostics

Help

WARNING: The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

Status / CARP

Temporarily Disable CARP

Enter Persistent CARP Maintenance Mode

CARP Interfaces

CARP Interface	Virtual IP	Status
LAN@1	172.16.2.30/16	MASTER

pfSync Nodes

pfSync nodes:

30f0da20

a8e9385f

b1023abf

Thème 2 : Mise en place d'un Failover accompagné d'un Portail Captif

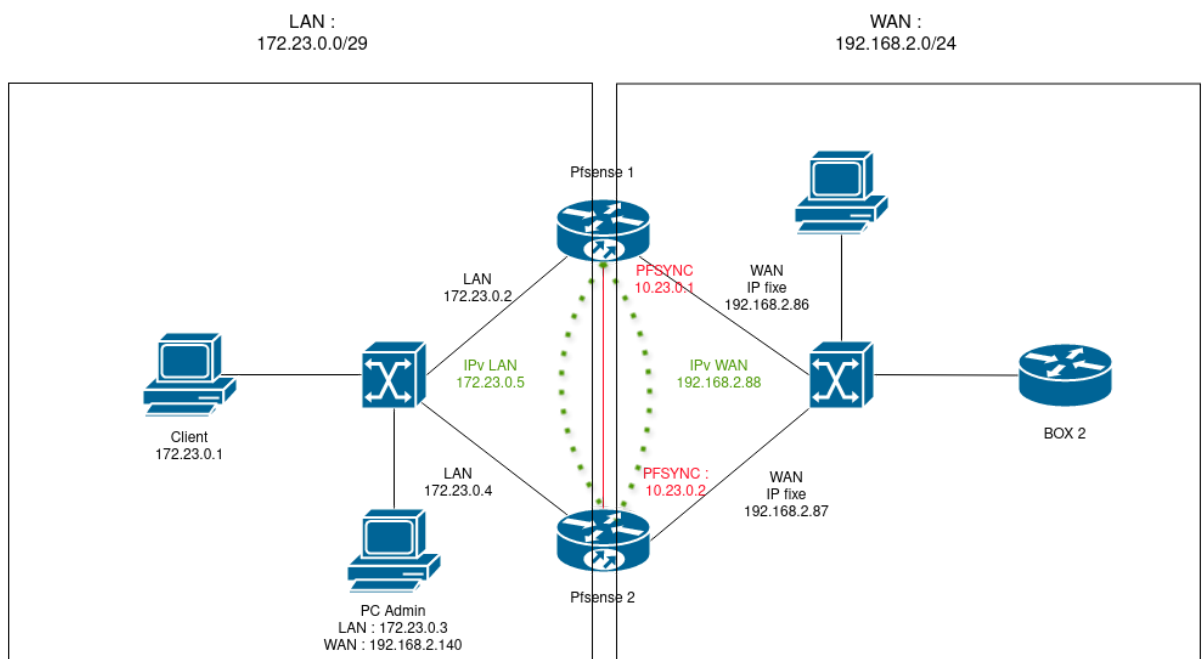
Sommaire :

- 1) Pré-requis
- 2) Schéma de l'infrastructure réseau
- 3) Accès à Internet depuis le réseau local
- 4) Mise en place du failover entre routeurs
- 5) Création du portail captif

1) Pré-requis

- 1 Client Xubuntu 18.04
- 2 routeurs Pfsense
- 1 machine d'administration Xubuntu 18.04

2) Schéma de l'infrastructure réseau (solutions attendue)



3) Accès à Internet depuis le réseau local

Côté client, on le redirige vers la "PAT" du routeur 1 pfsense

Modification de Connexion filaire 2

Nom de la connexion : Connexion filaire 2

Général | Ethernet | Sécurité 802.1X | DCB | Proxy | Paramètres IPv4 | Paramètres IPv6

Méthode : Manuel

Adresses

Adresse	Masque de réseau	Passerelle
172.23.0.1	29	172.23.0.2

Ajouter
Supprimer

Serveurs DNS :
Domaines de recherche :
ID de client DHCP :

☒ Requiert un adressage IPv4 pour que cette connexion fonctionne

Routes...

Annuler Enregistrer

On permet ensuite la translation d'adresse côté LAN privé à accéder au réseau publique

https://192.168.2.86/firewall_nat_out.php

pfSense COMMUNITY EDITION

System - Interfaces - Firewall - Services - VPN - Status - Diagnostics - Help

WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Firewall / NAT / Outbound

Port Forward 1:1 Outbound NAT

Outbound NAT Mode

Mode

- Automatic outbound NAT rule generation (IPsec passthrough included)
- Hybrid Outbound NAT rule generation (Automatic Outbound NAT + rules below)
- Manual Outbound NAT rule generation (ACN - Advanced Outbound NAT)
- Disable Outbound NAT rule generation (No Outbound NAT rules)

Save

Mappings

Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description
WAN	127.0.0.0/8	1:1	172.23.0.0/29	10.23.0.0/16	*	*	500	WAN address

Automatic Rules

Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description
WAN	127.0.0.0/8	1:1	172.23.0.0/29	10.23.0.0/16	*	*	*	WAN address

pfSense is developed and maintained by Nergate. © 2014 - 2025 View license.

Le NAT permettra à la box du labo d'ajouter dans sa table de routage, le réseau 172.23.0.0/29

A l'aide d'un traceroute, nous pouvons voir par où les paquets sont acheminés. Cela passe bien à travers le réseau publique (quad9)

```
master@VM-XBT-180405:~$ sudo su
[sudo] Mot de passe de master :
root@VM-XBT-180405:/home/master# traceroute 9.9.9.9
traceroute to 9.9.9.9 (9.9.9.9), 30 hops max, 60 byte packets
 1 pfsense.home.arpa (172.23.0.2)  1.225 ms  1.148 ms  1.310 ms
 2 192.168.2.254 (192.168.2.254)  2.093 ms  2.875 ms  2.843 ms
 3 145.239.153.28 (145.239.153.28)  17.748 ms  17.709 ms  18.785 ms
 4 145.239.153.163 (145.239.153.163)  18.694 ms  20.686 ms  20.653 ms
 5 10.200.2.67 (10.200.2.67)  20.463 ms  20.835 ms  20.723 ms
 6 10.200.200.5 (10.200.200.5)  35.938 ms  38.881 ms  55.121 ms
 7 10.200.200.13 (10.200.200.13)  29.733 ms  10.200.200.7 (10.200.200.7)  27.163 ms  10.200.200.5 (10.200.200.5)  52.152 ms
 8 10.200.2.64 (10.200.2.64)  18.318 ms  10.200.2.0 (10.200.2.0)  16.927 ms  10.200.2.64 (10.200.2.64)  18.084 ms
 9 10.200.2.71 (10.200.2.71)  47.748 ms  47.715 ms  47.694 ms
10 pch1.par.franceix.net (37.49.236.92)  18.672 ms  18.649 ms  19.813 ms
11 dns9.quad9.net (9.9.9.9)  19.746 ms  19.722 ms  19.840 ms
root@VM-XBT-180405:/home/master#
```

4) Mise en place du failover entre routeurs

ajout et configuration de la synchronisation PFSYNC

pf1 :

```
VirtualBox Virtual Machine - Netgate Device ID: b54bcb56677e680bb91e
*** Welcome to pfSense 2.7.0-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4: 192.168.2.86/24
LAN (lan)      -> em1      -> v4: 172.23.0.2/29
PFSYNC (opt1)  -> em2      -> v4: 10.23.0.1/16
```

éléments qui seront synchronisés sur l'esclave

Configuration Synchronization Settings (XMLRPC Sync)

Synchronize Config to IP

10.23.0.2

Enter the IP address of the firewall to which the selected configuration sections should be synchronized.

XMLRPC sync is currently only supported over connections using the same protocol and port as this system - make sure the remote system's port and protocol are set accordingly!

Do not use the Synchronize Config to IP and password option on backup cluster members!

Remote System Username

admin

Enter the webConfigurator username of the system entered above for synchronizing the configuration.

Do not use the Synchronize Config to IP and username option on backup cluster members!

Remote System Password

Confirm

Enter the webConfigurator password of the system entered above for synchronizing the configuration.

Do not use the Synchronize Config to IP and password option on backup cluster members!

Synchronize admin

☐ synchronize admin accounts and autoupdate sync password.

By default, the admin account does not synchronize, and each node may have a different admin password.

This option automatically updates XMLRPC Remote System Password when the password is changed on the Remote System Username account.

Select options to sync

☒ User manager users and groups

☒ Authentication servers (e.g. LDAP, RADIUS)

☒ Certificate Authorities, Certificates, and Certificate Revocation Lists

☒ Firewall rules

☒ Firewall schedules

☒ Firewall aliases

☒ NAT configuration

☒ IPsec configuration

☒ OpenVPN configuration (Implies CA/Cert/CRL Sync)

☒ DHCP Server settings

☒ DHCP Relay settings

☒ DHCPv6 Relay settings

☒ WoL Server settings

☒ Static Route configuration

☒ Virtual IPs

☒ Traffic Shaper configuration

☒ Traffic Shaper Limiters configuration

☒ DNS Forwarder and DNS Resolver configurations

☒ Captive Portal

☒ Toggle All

Save

pfSense is developed and maintained by Netgate. © ESF 2004 - 2025 View license.

pf2 :

```
VirtualBox Virtual Machine - Netgate Device ID: 194b3372a152169460e7
*** Welcome to pfSense 2.7.0-RELEASE (amd64) on pfSense2 ***
WAN (wan)      -> em0      -> v4: 192.168.2.87/24
LAN (lan)      -> em1      -> v4: 172.23.0.4/29
PFSYNC (opt1)  -> em2      -> v4: 10.23.0.2/16
```

Etant donné que l'esclave est le receveur de configuration, il faut juste activer l'option de synchronisation

System / High Availability

State Synchronization Settings (pfsync)

Synchronize states ☒ pfsync transfers state insertion, update, and deletion messages between firewalls.
 Each firewall sends these messages out via multicast on a specified interface, using the PFSYNC protocol (IP Protocol 240). It also listens on that interface for similar messages from other firewalls, and imports them into the local state table.
 This setting should be enabled on all members of a failover group.
 Clicking "Save" will force a configuration sync if it is enabled! (see Configuration Synchronization Settings below)

Synchronize Interface PFSYNC
 If Synchronize States is enabled this interface will be used for communication.
 It is recommended to set this to an interface other than LAN! A dedicated interface works the best.
 An IP must be defined on each machine participating in this failover group.
 An IP must be assigned to the interface on any participating sync nodes.

Création de l'IP Virtuelle :

Côté LAN

Firewall / Virtual IPs / Edit

Edit Virtual IP

Type ☐ IP Alias ☒ CARP ☐ Proxy ARP ☐ Other

Interface LAN

Address type Single address

Address(es) 172.23.0.5 / 29
 The mask must be the network's subnet mask. It does not specify a CIDR range.

Virtual IP Password ***** *****
 Enter the VHID group password. Confirm

VHID Group 86
 Enter the VHID group that the machines will share.

Advertising frequency 1 0
 Base Skew
 The frequency that this machine will advertise. 0 means usually master. Otherwise the lowest combination of both values in the cluster determines the master.

Description IP Virtuelle
 A description may be entered here for administrative reference (not parsed).

Save

Côté WAN :

Firewall / Virtual IPs / Edit

Edit Virtual IP

Type ☒ IP Alias ☒ CARP ☐ Proxy ARP ☐ Other

Interface WAN

Address type Single address

Address(es) 192.168.2.88 / 24
The mask must be the network's subnet mask. It does not specify a CIDR range.

Virtual IP Password
Enter the VHID group password. Confirm

VHID Group 87
Enter the VHID group that the machines will share.

Advertising frequency 1 0
Base Skew
The frequency that this machine will advertise. 0 means usually master. Otherwise the lowest combination of both values in the cluster determines the master.

Description IP virtuelle WAN
A description may be entered here for administrative reference (not parsed).

[Save](#)

nb : Attribuer un VHID différent pour éviter "les conflits d'adresses MAC".

Vérification des rôles :

pfSense.home.arpa - Status: ...

pfSense.home.arpa - Status: CARP — Mozilla Firefox

https://192.168.2.86/status_carp.php

WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Status / CARP

CARP Maintenance

[Temporarily Disable CARP](#) [Enter Persistent CARP Maintenance Mode](#)

CARP Status

Interface and VHID	Virtual IP Address	Status
LAN@86	172.23.0.5/29	MASTER
WAN@87	192.168.2.88/24	MASTER

State Synchronization Status

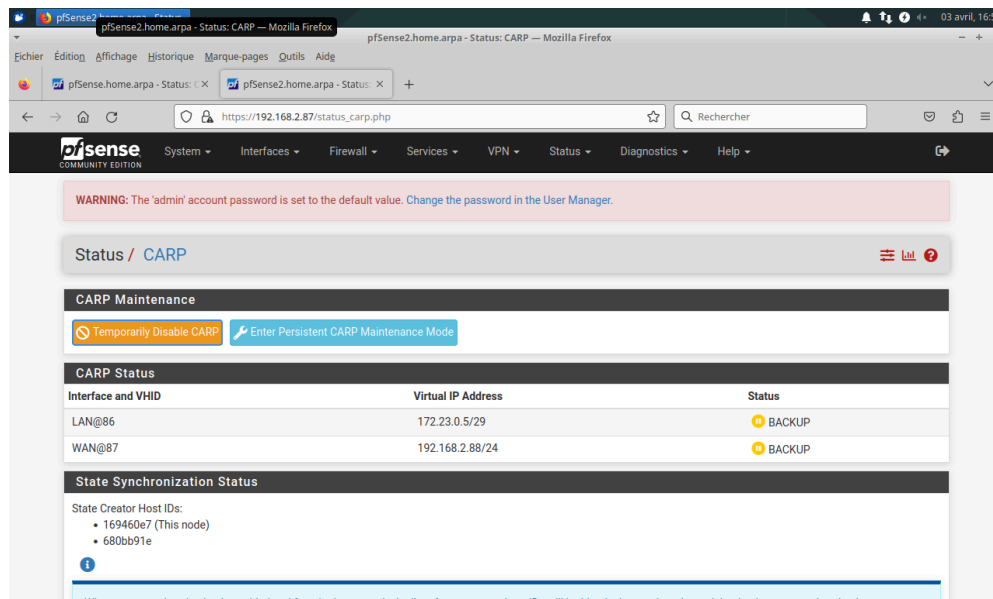
State Creator Host IDs:

- 16946027
- 680b891e (This node)

When state synchronization is enabled and functioning properly the list of state creator host IDs will be identical on each node participating in state synchronization.

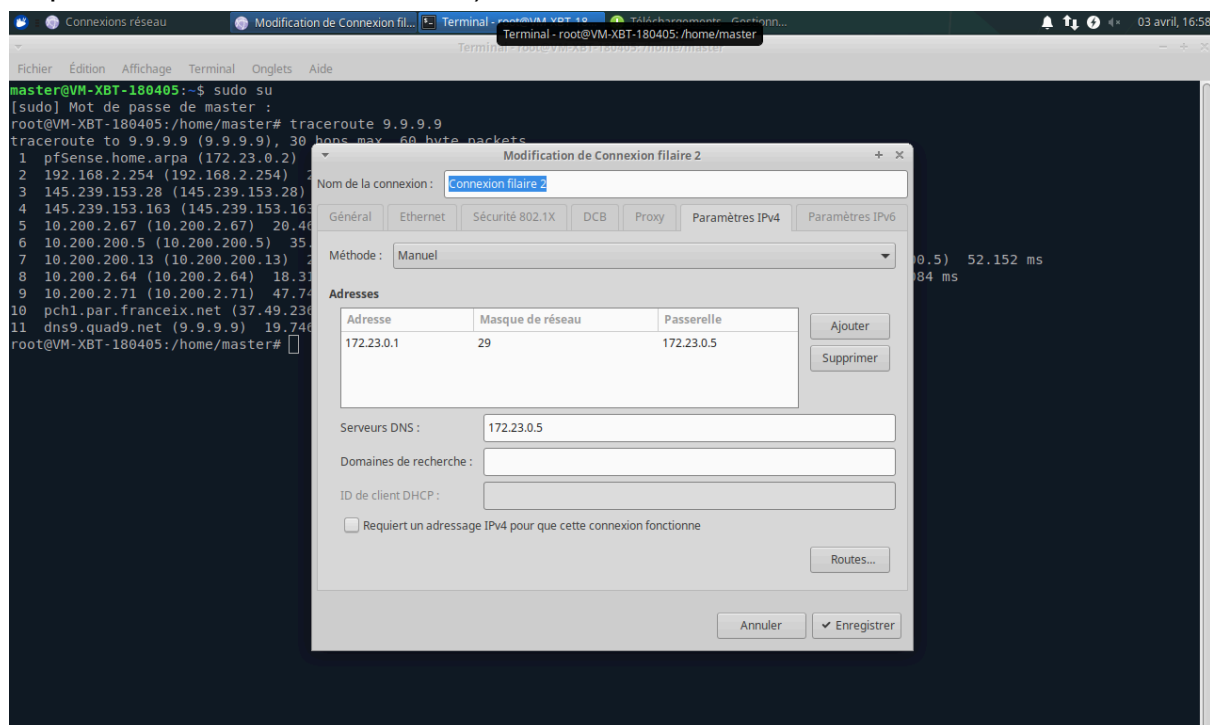
The state creator host ID for this node can be set to a custom value under System > High Avail Sync. If the state creator host ID has recently changed, the old ID will remain until all states using the old ID expire or are removed.

on peut donc voir que les 2 routeurs disposent bien d'un Fail-over



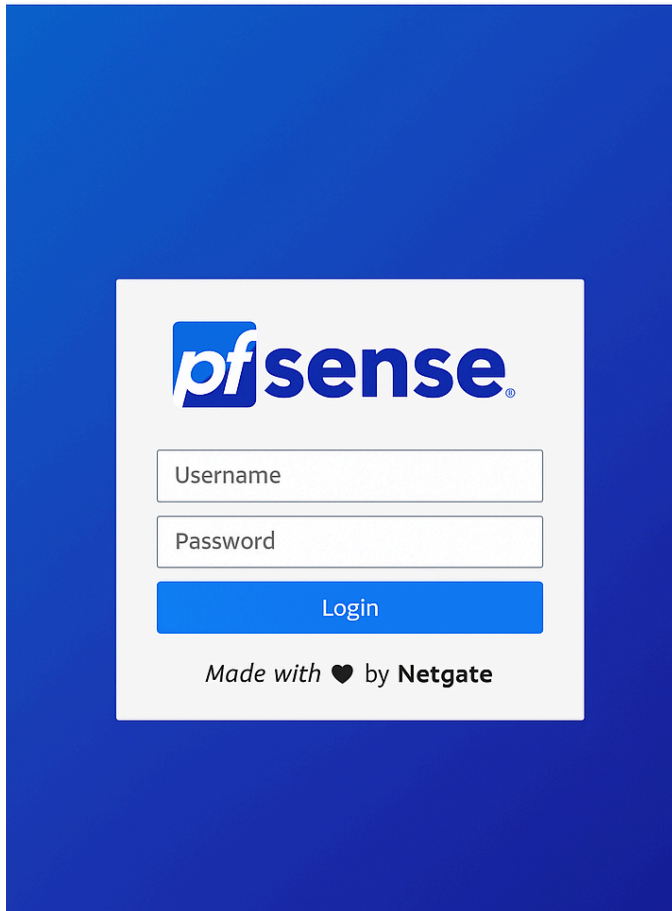
5) Création du Portail Captif

Ajout de l'IP virtuelle (pour conserver l'aspect haute disponibilité du service en cas de panne d'un des deux routeurs) côté LAN comme serveur DNS.



L'ajout de cette route va donc indiquer au client qu'il doit obligatoirement s'identifier s'il souhaite pouvoir consulter des sites. Celui-ci sera donc redirigé vers un portail captif.

que vous vous connectiez à un compte pour utiliser internet.

The image shows a captive portal login screen for pfSense. It features a blue background with a white rectangular box in the center. Inside the box, the pfSense logo is at the top. Below the logo are two input fields: 'Username' and 'Password'. Underneath these fields is a blue 'Login' button. At the bottom of the box, the text 'Made with ❤ by Netgate' is displayed.

Après s'être bien authentifié, l'utilisateur aura l'autorisation d'aller sur internet