

**MODULE 6****METTRE EN PLACE LA
HAUTE DISPONIBILITE
SUR pfSENSE (redondance)**

SOMMAIRE

1. LA HAUTE DISPONIBILITE AVEC LE PROTOCOLE "CARP"
C'EST QUOI ?
2. PREPARATION DES ROUTEURS pfSENSE 2.7 SUR PROXMOX
3. MISE EN PLACE DE LA HAUTE DISPONIBILITE (HA)
4. TEST DE LA HAUTE DISPONIBILITE pfSENSE

© tutos-info.fr - 02/2024



DIFFICULTE



UTILISATION COMMERCIALE INTERDITE

1 – LA HAUTE DISPONIBILITE AVEC "CARP" C'EST QUOI ?

Les organisations, de nos jours, ont besoin d'une connexion Internet fiable et permanente pour assurer la disponibilité des services mis en place. La perte de connexion de quelques minutes peut engendrer des pertes financières considérables.

Afin d'assurer une "**haute disponibilité**", nous allons expliquer dans ce tutoriel comment mettre en place une **redondance de routeurs pfSENSE** à l'aide du protocole **CARP**.

Le protocole **CARP** pour "**C**ommon **A**ddress **R**edundancy **P**rotocol", est un protocole qui permet à plusieurs hôtes, sur le même réseau local, de **partager un ensemble d'adresses IP**. Ce **protocole est souvent utilisé** pour faire de la **répartition de charge** ou de la **tolérance de panne** sur des routeurs.

CARP est une alternative sécurisée et libre aux protocoles Virtual Router Redundancy Protocol (VRRP), Hot Standby Router Protocol (HSRP) et Foundry Standby Router Protocol (FSRP). CARP a été créé pour contourner des brevets.

Dans son fonctionnement, **on met dans un groupe plusieurs hôtes** (groupe de redondance) **qui partageront alors une même adresse IP dite "virtuelle"**. Derrière cette adresse IP virtuelle se "cacheront" plusieurs hôtes dont un maître qui prendra et traitera l'intégralité de requêtes en destination de l'IP virtuelle.

On appelle un groupe d'hôtes utilisant CARP un « groupe de redondance ». Le groupe de redondance se voit attribuer une adresse IP partagée entre les membres du groupe. **Au sein de ce groupe, un hôte est désigné comme « maître », les autres sont appelés « esclaves »**. **L'hôte maître** est celui qui « prend » **l'adresse IP partagée**. **Il répond à tout trafic** ou requête **ARP à destination de cette adresse**. Chaque hôte doit avoir une seconde adresse IP unique. Chaque hôte peut appartenir à plusieurs groupes de redondance.

Une **utilisation commune de CARP** est la création d'un **groupe de pare-feu redondants**. L'adresse IP virtuelle attribuée au groupe de redondance est désignée comme l'adresse du routeur par défaut sur les machines clientes. **Dans le cas où le pare-feu maître rencontre une panne** ou est déconnecté du réseau, **l'adresse IP virtuelle sera prise par un des pare-feu esclaves et le service continuera à être rendu sans interruption**.

CARP supporte IPv4 et IPv6 et a le numéro de **port TCP 112**.

2 – PREPARATION DES ROUTEURS pfSENSE SUR PROXMOX 8.1

Prérequis :

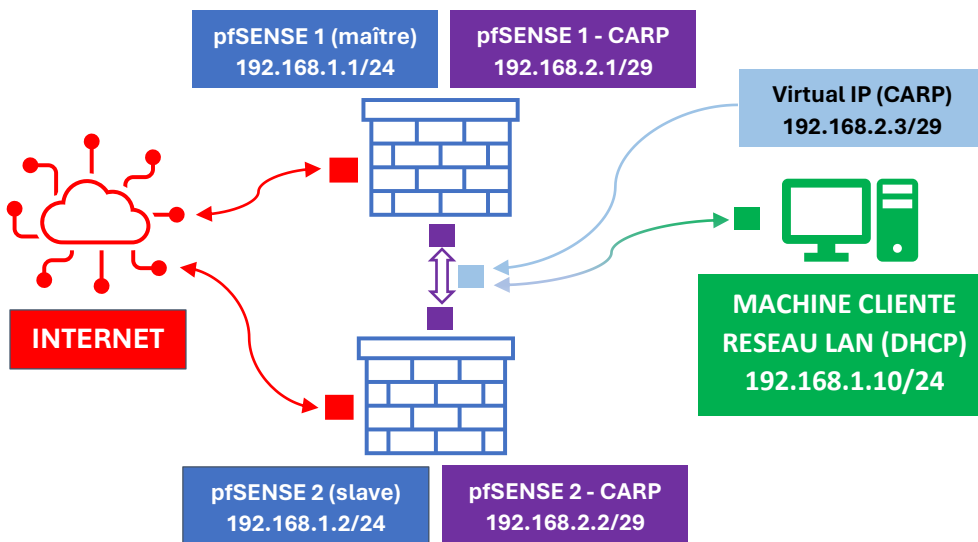
Pour réaliser ce tutoriel, vous devez avoir suivi les précédents modules (1 à 4) présentés sur ce site. Il vous faut également un environnement de virtualisation (Proxmox ou Virtualbox), plusieurs IP WAN (on peut également simuler ces adresses WAN au sein d'un home lab).

Dans ce tutoriel, nous allons mettre en place une haute disponibilité en créant **2 routeurs pfSENSE redondants**. Nous allons commencer par préparer les 2 routeurs pfSense. **Chaque routeur doit posséder 3 interfaces réseau :**

- une interface "**WAN**"
- une interface "**LAN**"
- une interface "**CARP**"

Nous aurons besoin, également, **d'une machine cliente connectée au réseau local** (Windows 10 pour ce tutoriel) afin de faire nos tests et vérifier que la tolérance de panne fonctionne bien.

L'architecture réseau que l'on souhaite reproduire est la suivante :



Pour réaliser ce tutoriel, nous disposons d'une IP publique qui nous a été fournie par notre hébergeur (si vous 'en n'avez pas, simulez-là dans votre home lab). Notre IP WAN est sous la forme **212.83.147.xx1/32**

Chaque routeur pfSENSE est connecté à la même interface "**WAN**" qui est configurée ainsi :

Interface WAN (unique)	212.83.147.xx1/32
-------------------------------	--------------------------

Chaque routeur pfSENSE aura une interface "**LAN**" configurée ainsi (attention, **utilisez le même réseau**) :

Routeur pfSENSE 1 – Maître – LAN	192.168.1.1/24	Service DHCP ACTIF sur ce routeur
Routeur pfSENSE 2 – Esclave – LAN	192.168.1.2/24	Service DHCP NON ACTIF sur ce routeur
Virtual IP LAN (pour synchronisation)	192.168.1.3/24	Permettra la synchronisation du " LAN "

La "**virtual IP**" créée dans pfSENSE sur le réseau "**LAN**" permettra la synchronisation du "**LAN**". En cas de défaillance du routeur MAITRE, il faut que les machines du réseau "**LAN**" puissent continuer à accéder au web et utiliser les ressources locales (notion de haute disponibilité).

Chaque routeur pfSENSE aura une interface réseau nommée "**CARP**", **avec un adressage différent du LAN, en /29**. Comme expliqué en 1^{ère} partie de ce tutoriel, **l'interface CARP servira pour la synchronisation des 2 routeurs pfSENSE**. La mise en place de la haute disponibilité sera assurée via une "**virtual IP**" créée dans pfSENSE sur le réseau "**CARP**" :

Routeur pfSENSE 1 – Maître – CARP	192.168.2.1/29	IP statique (pas de service DHCP)
Routeur pfSENSE 2 – Esclave - CARP	192.168.2.2/29	IP statique (pas de service DHCP)
Virtual IP CARP (pour synchronisation)	192.168.2.3/29	Permettra la synchronisation des pfSENSE

1^{ère} étape : préparation des 2 routeurs pfSENSE

Cette étape a déjà été expliquée en détail dans les modules 1 à 4. Nous ne présentons pas cette étape dans le détail ici. Assurez-vous d'avoir un accès à chaque routeur soit depuis le LAN ou depuis l'extérieur (selon votre convenance et votre politique de sécurité).

Dans ce tutoriel, nous nous servons d'une machine virtuelle connectée au réseau "LAN" pour faire nos tests mais vous pouvez aussi configurer un accès distant si vous le souhaitez (voir module 2).

La configuration matérielle de chaque pfSENSE est la suivante (3 cartes réseau par routeur).

Les routeurs seront connectés au même "vmbr 0" qui correspond à l'IP Publique WAN unique fournie par notre hébergeur (adresse MAC identique ici) :

pfSENSE – MAITRE

⇄ Carte réseau (net0)	e1000=52:54:00:12:34:567:e0,bridge=vmbr0	← Interface WAN
⇄ Carte réseau (net1)	e1000=BC:24:11:16:09:C9,bridge=vmbr2	← Interface LAN
⇄ Carte réseau (net2)	e1000=BC:24:11:6F:1D:D1,bridge=vmbr9	← Interface CARP

pfSENSE - ESCLAVE

⇄ Carte réseau (net0)	e1000=52:54:00:12:34:567:e0,bridge=vmbr0	Sur le 2 ^{ème} routeur, utilisez les mêmes "vmbr" (les "vmbr" 2 et 9) peuvent changer en fonction de votre configuration.
⇄ Carte réseau (net1)	e1000=BC:24:11:E3:7B:DF,bridge=vmbr2	
⇄ Carte réseau (net2)	e1000=BC:24:11:DC:86:4F,bridge=vmbr9	

Lancez l'installation de vos routeurs (voir modules précédents n° 1 et 2).

Attention, **configurez un serveur DHCP sur l'interface "LAN" du pfSENSE MAITRE (exemple d'étendue : 192.168.1.10 → 192.168.1.20) mais ne configurez pas de DHCP sur le pfSENSE ESCLAVE.**

Une fois les 2 routeurs pfSENSE installés, vous devez avoir ce type de configuration réseau sur vos interfaces :

pfSENSE – MAITRE

```
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense-maitre ***
WAN (wan)      -> em0          -> v4: 2           0/32
LAN (lan)      -> em1          -> v4: 192.168.1.1/24
CARP (opt1)    -> em2          -> v4: 192.168.2.1/32
```

- L'interface "**WAN**" est configurée en statique (pas de DHCP)
- L'interface "**LAN**" est configurée en statique **avec le service DHCP activé** (étendue : 192.168.1.10 → 192.168.1.20)
- L'interface "**OPT1**" est configurée en statique et sera renommée en "**CARP**" dans la console (GUI) de pfSENSE (masque de sous-réseau en "/29" ; pas de DHCP)

```
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense-esclave ***  
  
WAN (wan)      -> em0      -> v4: 2      0/32  
LAN (lan)      -> em1      -> v4: 192.168.1.2/24  
CARP (opt1)    -> em2      -> v4: 192.168.2.2/32
```

- L'interface "**WAN**" est configurée en statique (pas de DHCP)
- L'interface "**LAN**" est configurée en statique et le service DHCP n'est pas activé
- L'interface "**OPT1**" est configurée en statique et sera renommée en "**CARP**" dans la console (GUI) de pfSENSE (masque de sous-réseau en "/29" ; pas de DHCP)

2^{ème} étape : préparation d'une machine de test connectée au réseau "LAN"

Nous avons également besoin d'une machine connectée au réseau local du pfSENSE MAITRE pour administrer nos pfSENSE. Dans notre hyperviseur, nous possédons une machine Windows 10 que nous avons connectée au "**vmbr2**", c'est-à-dire l'interface "**LAN**" de nos pfSENSE :



Une fois les 2 routeurs installés et préparés (voir précédents tutoriels pour les explications), nous nous connectons à l'interface de gestion du **pfSENSE MAITRE** avec notre machine locale Windows et en saisissant l'adresse <https://192.168.1.1> via un navigateur.

3^{ème} étape : renommez les interfaces "OPT1" en "CARP" depuis l'interface GUI de pfSENSE

Cette étape n'est pas obligatoire mais permet de renommer l'interface "OPT1" en "CARP" pour faciliter la configuration et la compréhension de ce tutoriel :

- Cliquez le menu "**Interfaces**" – "**Assignments**"
- Cliquez sur l'interface "**OPT1**" et renommez-la en "**CARP**"
- Cliquez les boutons "**Save**" et "**Apply Changes**" pour valider vos nouveaux paramètres

Faites de même avec le routeur esclave (vous pouvez nommer l'interface "CARP" également).

Principe de fonctionnement de la réplication avec pfSENSE

pfSENSE communique sur les réseaux LAN et WAN avec des adresses IP virtuelles ; il n'utilise jamais l'adresse IP assignée à son interface.

En cas de défaillance du pfSENSE MAITRE, le pfSENSE ESCLAVE prend le relais sans aucune interruption de service. La bascule est totalement transparente.

Afin d'assurer la réplication, 3 éléments doivent être configurés :

- **CARP**
- **pfsync**
- **XML-RPC**

QU'EST-CE QUE "CARP" ?

CARP (*C*ommon *A*ddress *R*edundancy *P*rotocol) est un **protocole permettant à plusieurs hôtes présents sur un même réseau de partager une adresse IP**.

Ici, nous utiliserons CARP afin de partager une adresse virtuelle LAN et une adresse IP virtuelle CARP sur nos routeurs pfSENSE pour **communiquer sur le réseau**. Ainsi, en cas de défaillance du pfSENSE MAITRE, le pfSENSE ESCLAVE prendra le relais de manière transparente au niveau réseau (reprise de l'adresse IP virtuelle).

CARP est un protocole travaillant sur les couches 2 et 3 du modèle OSI. Dans son fonctionnement, on met dans un groupe plusieurs hôtes (groupe de redondance) qui partageront alors une même adresse IP et auront une adresse MAC dite « virtuelle ». Derrière cette adresse IP qui sera virtuelle se cacheront deux ou plusieurs hôtes dont un "maître" qui prendra et traitera l'intégralité des requêtes en destination de l'IP virtuelle. Les hôtes du réseau communiqueront entre eux afin de vérifier que le maître est toujours actif. S'il vient à tomber, l'hôte désigné comme esclave prendra le relais afin d'accueillir et de traiter le trafic en destination de l'adresse IP virtuelle.

Ce genre de fonctionnement permet, si une passerelle tombe par exemple, de garder la même configuration en utilisant une passerelle physiquement différente car les hôtes se « cachent » derrière une IP unique.

QU'EST-CE QUE "pfsync" ?

pfsync est un **protocole permettant de synchroniser entre deux routeurs pfSENSE l'état des connexions en cours** (et de manière plus large entre deux serveurs exécutant le firewall Packet Filter). Ainsi, **en cas de défaillance du routeur primaire, l'état des connexions en cours est maintenu sur le routeur secondaire**. Il n'y a donc pas de coupure liée à la bascule des services du pfSENSE MAITRE vers le pfSENSE ESCLAVE.

Il est recommandé d'effectuer cette synchronisation sur un lien dédié entre les deux serveurs pfSENSE. C'est pour cela que nous avons dédié une interface réseau à cet usage (l'interface "CARP"). À défaut, le lien LAN peut être utilisé.

Les messages pfsync sont envoyés en multicast, c'est pour cela qu'il est recommandé de mettre une interface dédiée au pfsync par souci de sécurité. En effet, en étant à l'écoute sur ce canal multicast, un pirate peut recevoir les messages de création, de mise à jour et de suppression des états de connexions et pourrait même se faire passer pour un routeur en envoyant des paquets pfsync afin de perturber le bon fonctionnement du Fail-Over.

C'EST QUOI "XML-RPC" ?

XML-RPC est un **protocole permettant la répliquon de données d'un routeur vers un autre**. Il est utilisé dans pfSENSE afin de **répliquer la configuration du routeur primaire vers le routeur secondaire**. Pour garantir son bon fonctionnement, **il est important qu'il utilise la même interface que celle utilisée par le protocole pfsync (c'est-à-dire notre interface "CARP" ici)**.

CARP

pfsync

XML-RPC

3 – MISE EN PLACE DE LA HAUTE DISPONIBILITE pfSENSE

1^{ère} étape : création des "Virtual IP" sur chaque routeur pfSENSE (pour la synchronisation)

Travail à réaliser sur le routeur MAITRE

- Sur le routeur MAITRE, cliquez le menu "Firewall" – "Virtual IPs" et cliquez le bouton vert "Add"
- Configurez votre adresse IP virtuelle pour le réseau "CARP" ainsi :

Firewall / Virtual IPs / Edit

Edit Virtual IP

Type IP Alias CARP Proxy ARP Other

Interface

Address type

Address(es) /

Virtual IP Password

VHID Group

Advertising frequency Base Skew

Description

Choisir le type "CARP"

Choisir l'interface "CARP"

Saisir l'IP virtuelle souhaitée et le masque

Saisir un mot de passe pour l'IP virtuelle

Base = délai 1 seconde avant bascule si défaillance. Skew = le "0" stipule que ce routeur est le MAITRE. Saisir une description pour cette IP virtuelle.

- Cliquez les boutons "Save" et "Apply Changes" pour valider vos paramètres
- Cliquez à nouveau sur le menu "Firewall" et "Virtual IPs" et cliquez le bouton vert "Add"
- Configurez votre adresse IP virtuelle pour le réseau "LAN" ainsi :

Firewall / Virtual IPs / Edit

Edit Virtual IP

Type IP Alias CARP Proxy ARP Other

Interface

Address type

Address(es) /

Virtual IP Password

VHID Group

Advertising frequency Base Skew

Description

Base = délai 1 seconde avant bascule si défaillance.

Étant donné que vous avons un serveur DHCP sur le routeur MAITRE, le "skew" doit obligatoirement être supérieur ou égal à "20".

Skew = le "22" stipule que ce routeur est le MAITRE.

Saisir une description pour cette IP virtuelle.

- Cliquez les boutons "Save" et "Apply Changes" pour valider vos paramètres

Travail à réaliser sur le routeur ESCLAVE

- Sur le routeur ESCLAVE, cliquez le menu "Firewall" – "Virtual IPs" et **faites exactement la même chose, à savoir la création des 2 IP virtuelles**. Attention, **pensez à bien saisir les mêmes paramètres**.

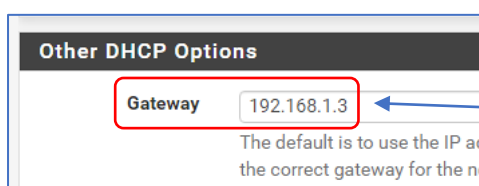
Une fois que les adresses IP virtuelles sont paramétrées **de manière identique sur les 2 routeurs** pfSENSE, **toutes les étapes qui suivent sont à réaliser SUR LE ROUTEUR MAITRE !**

2^{ème} étape : configuration de la passerelle sur le serveur DHCP actif sur le pfSENSE MAITRE

Attention, travail à réaliser sur le routeur pfSENSE MAITRE (pas de manipulation à faire sur l'esclave puisque la réplication effectuera le travail pour vous !).

Étant donné que nous avons un serveur DHCP actif sur le réseau "LAN" du routeur pfSENSE MAITRE, **il faut maintenant indiquer au service DHCP que la passerelle à utiliser, en cas de défaillance du MAITRE, sera l'IP virtuelle du réseau "LAN"** (soit 192.168.1.3 dans notre cas). Pour cela effectuez les manipulations suivantes :

- Cliquez le menu "**Services**" – "**DHCP Server**"
- Sélectionnez l'interface "**LAN**"
- Indiquez, au niveau de la rubrique "**Other DHCP Options**", l'adresse IP virtuelle du réseau "**LAN**" :



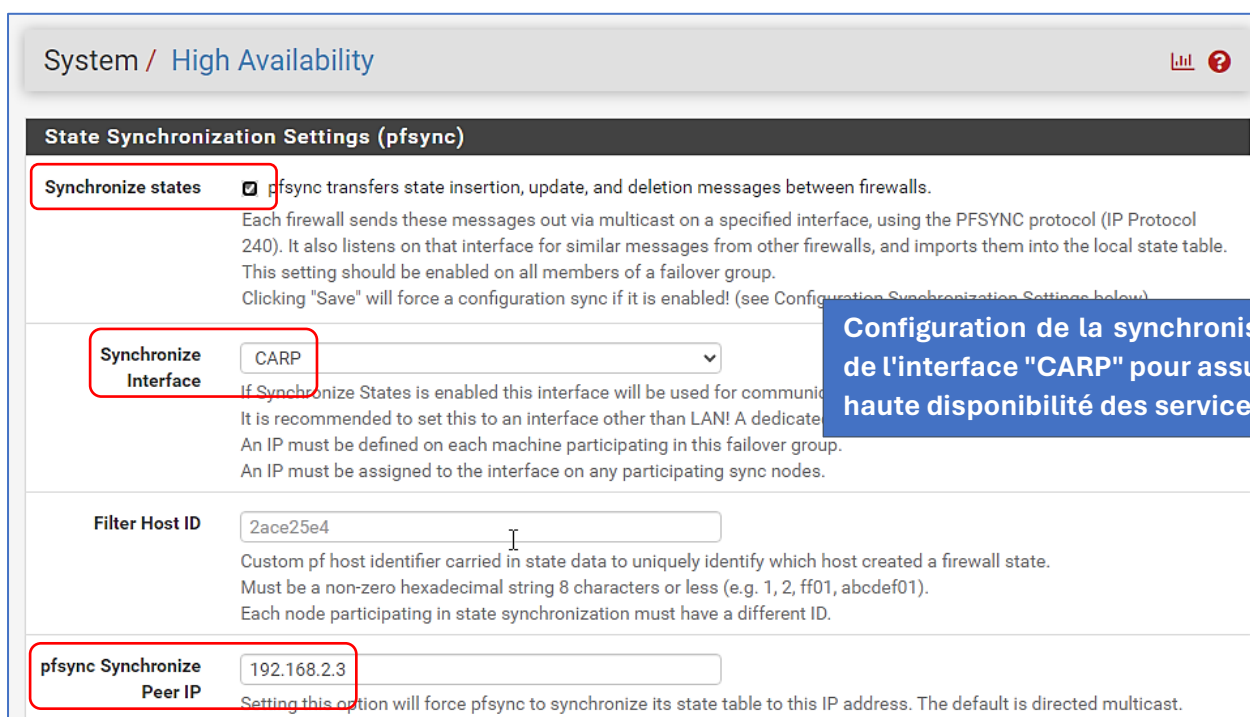
On indique ici l'IP virtuelle du réseau "LAN" précédemment définie dans les "Virtual IPs".

- Cliquez les boutons "**Save**" et "**Apply Changes**" pour valider vos paramètres

3^{ème} étape : mise en place de la haute disponibilité (depuis le routeur pfSENSE MAITRE) :

Attention, travail à réaliser sur le routeur pfSENSE MAITRE (pas de manipulation à faire sur l'esclave puisque la réplication effectuera le travail pour vous !).

- Cliquez le menu "**System**" – "**High availability**"
- Configurez la haute disponibilité ainsi :



Configuration de la synchronisation de l'interface "CARP" pour assurer la haute disponibilité des services.

Configuration Synchronization Settings (XMLRPC Sync)

Synchronize Config to IP **Saisir l'adresse IP du routeur pfSENSE ESCLAVE**
 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
 Enter the webConfigurator username of the system entered above for synchronization.
 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

Si vous souhaitez une synchronisation complète, cochez l'ensemble des cases (à adapter à votre stratégie).

- Cliquez le bouton "Save" pour valider vos paramètres

4^{ème} étape : paramétrage des règles de pare-feu

Il faut maintenant paramétrer les règles de trafic pour autoriser les flux sur les interfaces.

Attention, travail à réaliser sur le routeur pfSENSE MAITRE (pas de manipulation à faire sur l'esclave puisque la répliquera effectuera le travail pour vous !).

REGLAGE DU NAT SORTANT SUR L'INTERFACE "WAN"

- Cliquez le menu "Firewall" - "NAT"
- Cliquez sur "Outbound" et activez le mode "Hybrid"
- Cliquez les boutons "Save" et "Apply Changes" pour valider le mode :

Firewall / NAT / Outbound

Port Forward 1:1 **Outbound** NPT

Outbound NAT Mode

Mode	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
	Automatic outbound NAT rule generation. (IPsec passthrough included)	Hybrid Outbound NAT rule generation. (Automatic Outbound NAT + rules below)	Manual Outbound NAT rule generation. (AON - Advanced Outbound NAT)	Disable Outbound NAT rule generation. (No Outbound NAT rules)

- Cliquez à nouveau sur le menu "Firewall" – "NAT"
- Sélectionnez "Outbound"
- Dans la rubrique "Mappings", cliquez le bouton vert "Add" pour configurer la règle comme indiqué ci-dessous :

Edit Advanced Outbound NAT Entry

Disabled Disable this rule

Do not NAT Enabling this option will disable NAT for traffic matching this rule and stop processing Outbound NAT rules. In most cases this option is not required.

Interface WAN

The interface on which traffic is matched as it exits the firewall. In most cases this is "WAN" or another externally-connected interface.

Address Family IPv4+IPv6

Select the internet Protocol version this rule applies to.

Protocol Any

Choose which protocol this rule should match. In most cases "any" is specified.

Source Any / 24

Type Source network for the outbound NAT mapping. Port or Range

Destination Any / 24

Type Destination network for the outbound NAT mapping. Port or Range

Not

Invert the sense of the destination match.

Translation

Address ▼

Type

Connections matching this rule will be mapped to the specified address. If specifying a custom network or alias, it must be routed to the firewall.

Port or Range Static Port

Enter the external source **Port or Range** used for remapping the original source port on connections matching the rule.

Port ranges are a low port and high port number separated by ":".
Leave blank when **Static Port** is checked.

Misc

No XMLRPC Sync Prevents the rule on Master from being overwritten on Slave. **Ne pas cocher cette case sinon la synchronisation ne pourra pas fonctionner !**

Description

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

- Cliquez les boutons **"Save"** et **"Apply Changes"**

Nous allons maintenant configurer les règles nécessaires au bon fonctionnement de la haute disponibilité en paramétrant les différents flux autorisés dans le pare-feu :

- Cliquez à nouveau sur le menu **"Firewall" – "Rules"**
- Sélectionnez l'interface **"CARP"** et cliquez le bouton vert **"Add"** pour configurer la règle comme indiqué ci-dessous (nous aurons 4 règles à créer) :

REGLE 1 – CONFIGURATION DU PROTOCOLE "pfsync"

Firewall / Rules / Edit

Edit Firewall Rule

Action ▼

Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled Disable this rule

Set this option to disable this rule without removing it from the list.

Interface ▼

Choose the interface from which packets must come to match this rule.

Address Family ▼

Select the Internet Protocol version this rule applies to.

Protocol ▼

Choose which IP protocol this rule should match.

Source

Source Invert match CARP subnets Source Address /

Destination

Destination Invert match This Firewall (self) Destination Address /

- Cliquez les boutons "Save" et "Apply Changes" pour valider la règle autorisant le protocole CARP.

REGLE 2 – CONFIGURATION DU PROTOCOLE "XML-RPC"

- Cliquez le bouton vert "Add" pour ajouter la 2^{ème} règle et configurez-la comme indiqué ci-dessous :

Edit Firewall Rule

Action Pass

Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled Disable this rule
Set this option to disable this rule without removing it from the list.

Interface CARP
Choose the interface from which packets must come to match this rule.

Address Family IPv4
Select the Internet Protocol version this rule applies to.

Protocol TCP
Choose which IP protocol this rule should match.

Source

Source Invert match CARP subnets Source Address /

Display Advanced

The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any.

Destination

Destination Invert match This Firewall (self) Destination Address /

Destination Port Range

From HTTPS (443) Custom To HTTPS (443) Custom

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Extra Options

Log Log packets that are handled by this rule
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).

Description Autoriser XML RPC

A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

- Cliquez les boutons "Save" et "Apply Changes" pour valider la règle autorisant le flux XML-RPC

REGLE 3 – CONFIGURATION DES FLUX AU SEIN DU RESEAU "CARP"

- Cliquez le bouton vert **"Add"** pour ajouter la 3^{ème} et dernière règle comme ci-dessous :

Edit Firewall Rule

Action Pass
Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled Disable this rule
Set this option to disable this rule without removing it from the list.

Interface CARP
Choose the interface from which packets must come to match this rule.

Address Family IPv4
Select the Internet Protocol version this rule applies to.

Protocol CARP
Choose which IP protocol this rule should match.

Source
 Invert match CARP subnets Source Address /

Destination
 Invert match Any Destination Address /

- Cliquez les boutons **"Save"** et **"Apply Changes"** pour valider la règle autorisant les flux sur l'interface CARP.

REGLE 4 – CONFIGURATION DE LA PASSERELLE UNIQUE SUR LE RESEAU "LAN"

Cette règle permet, à l'interface "LAN" de toujours utiliser la passerelle unique, fournie par notre hébergeur, pour naviguer sur Internet. En effet, ce dernier propose d'utiliser une passerelle unique sur tous ses serveurs hébergés afin de faciliter la gestion des passerelles.

Pour définir cette passerelle unique qui est à utiliser par défaut, suivez la manipulation suivante :

- Cliquez le menu **"System" – "Routing"**
- Sélectionnez **"Gateways"** et définissez votre passerelle unique par défaut en cliquant le bouton vert **"Add"** :

System / Routing / Gateways

Gateways Static Routes Gateway Groups

Name	Default	Interface	Gateway	Monitor IP	Description	Actions
WANGW	Default (IPv4)	WAN	62.210.0.1	62.210.0.1	Interface wan Gateway	

Save + Add

Default gateway

Default gateway IPv4 WANGW
Select a gateway or failover gateway group to use as the default gateway.

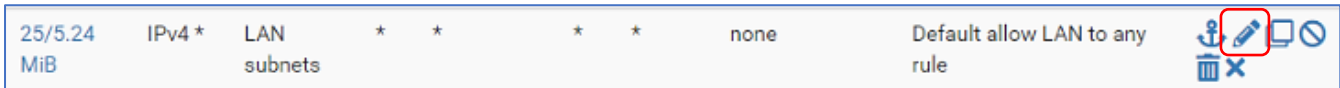
Default gateway IPv6 Automatic
Select a gateway or failover gateway group to use as the default gateway.

Save

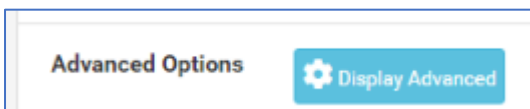
- Cliquez les boutons **"Save"** et **"Apply Changes"** pour valider cette passerelle unique.

Maintenant, nous allons modifier la règle de trafic sortant du "LAN" de manière à intégrer cette passerelle unique en suivant la procédure ci-dessous :

- Cliquez le menu **"Firewall" – "Rules"**
- Sélectionnez l'interface **"LAN"**
- Éditez la règle ci-dessous en cliquant sur le crayon à droite :



- Descendez au niveau de la rubrique **"Advanced Options"** et cliquez le bouton **"Display Advanced"** :



- Sélectionnez votre passerelle par défaut puis cliquez les boutons **"Save"** et **"Apply Changes"** :

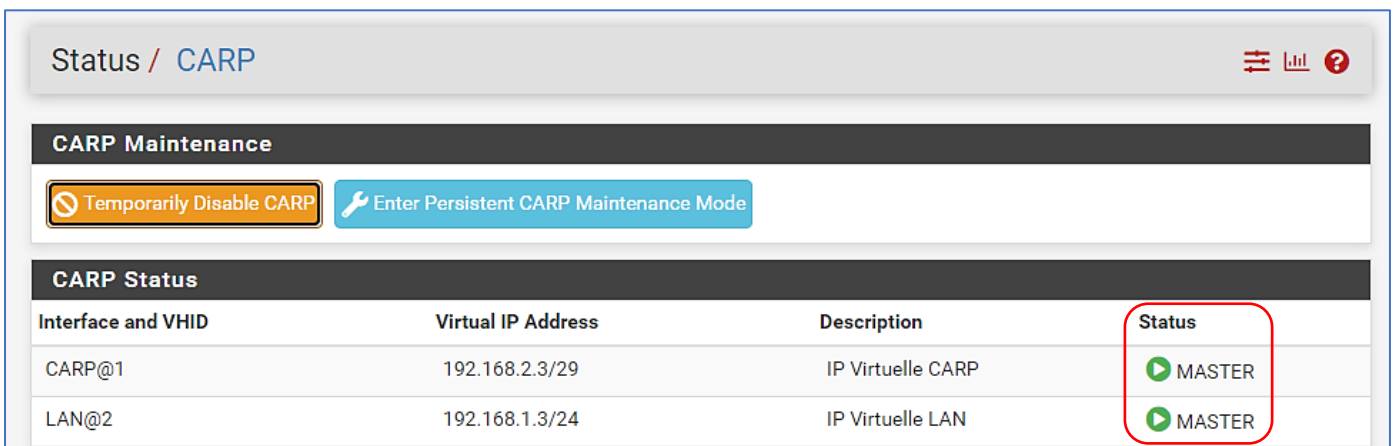


La configuration de la haute disponibilité est prête !

5^{ème} étape : vérification du bon fonctionnement de la réplication

Les IP virtuelles, la haute disponibilité et les règles de pare-feu étant configurées, nous pouvons déjà vérifier si le statut CARP de notre routeur pfSENSE MAITRE est fonctionnel. Pour cela :

- Cliquez le menu **"Status" – "CARP (failover)"** ; une fenêtre s'affiche :

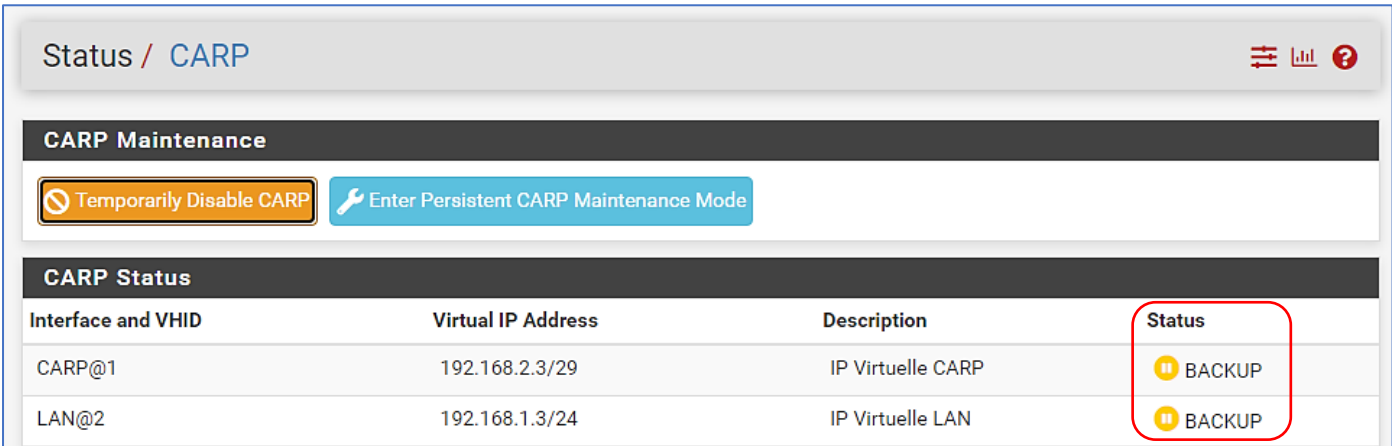


On peut constater, ici, que notre routeur pfSENSE MAITRE a bien le statut de **"MASTER"**. L'interface "CARP" et l'interface "LAN" sont bien répliquées sur l'autre routeur.

Si vous ne voyez pas le statut s'afficher, cela signifie que vous avez une incohérence dans les adresses IP virtuelles (erreur dans la saisie des adresses sur chaque routeur ou mot de passe de l'adresse virtuelle erroné).

Vérification de la réplication sur le routeur ESCLAVE :

- Connectons-nous au routeur pfSENSE ESCLAVE et vérifions son statut CARP :



Status / CARP

CARP Maintenance

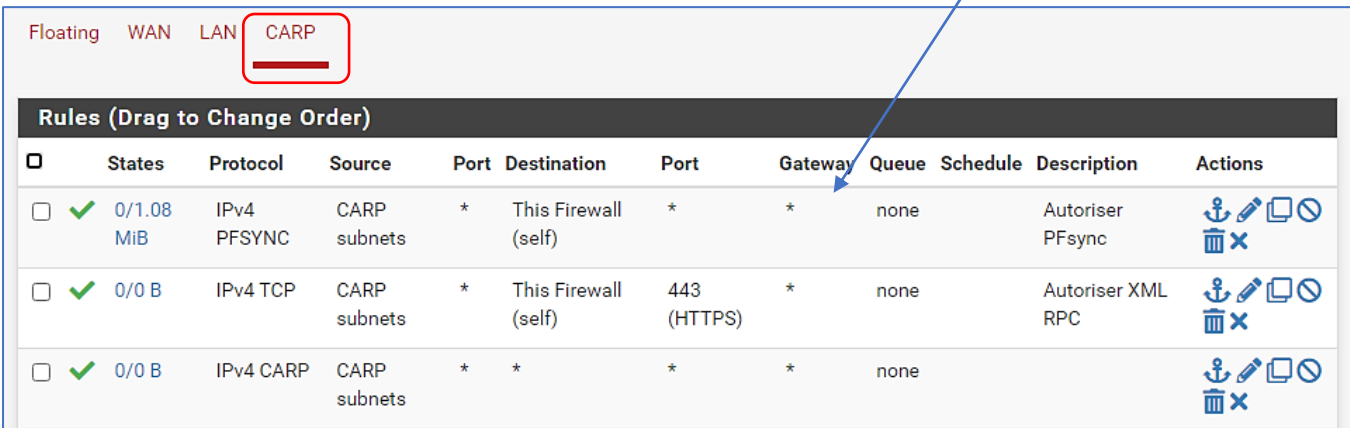
Temporarily Disable CARP Enter Persistent CARP Maintenance Mode

CARP Status

Interface and VHID	Virtual IP Address	Description	Status
CARP@1	192.168.2.3/29	IP Virtuelle CARP	BACKUP
LAN@2	192.168.1.3/24	IP Virtuelle LAN	BACKUP

On peut constater, ici, que notre routeur pfSENSE ESCLAVE a bien le statut de "**BACKUP**" qui signifie qu'il est "esclave" dans le cluster. La haute disponibilité est fonctionnelle puisque la communication est établie !

- Cliquez, sur le routeur pfSENSE ESCLAVE, le menu "**Firewall**" – "**Rules**" ; vous constaterez que les "**Règles**" saisies dans le routeur pfSENSE MAITRE ont été intégralement répliquées (!) :



Floating WAN LAN **CARP**

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 0/1.08 MiB	IPv4 PFSYNC	CARP subnets	*	This Firewall (self)	*	*	none		Autoriser PFSync	
<input type="checkbox"/>	✓ 0/0 B	IPv4 TCP	CARP subnets	*	This Firewall (self)	443 (HTTPS)	*	none		Autoriser XML RPC	
<input type="checkbox"/>	✓ 0/0 B	IPv4 CARP	CARP subnets	*	*	*	*	none			

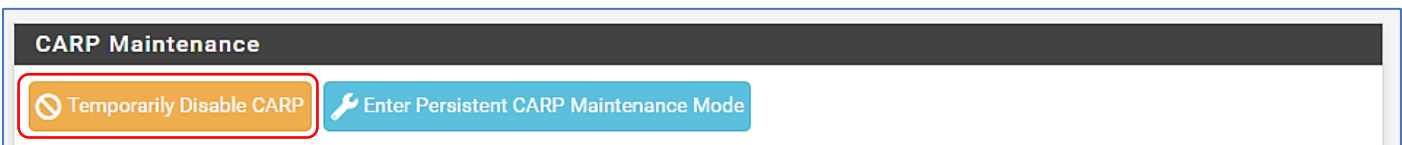
Votre cluster est prêt ! Bravo !

3 – TESTS DE LA HAUTE DISPONIBILITE DU CLUSTER pfSENSE

Nous allons, ici, simuler une "panne" du routeur pfSENSE MAITRE. Plutôt que de l'arrêter, on peut stopper le protocole CARP en cours sur celui-ci. Pour cela, effectuez les manipulations suivantes :

ARRET DU PROTOCOLE "CARP" SUR LE ROUTEUR MAITRE (simulation de panne)

- Cliquez le menu "**Status**" – "**CARP (failover)**"
- Cliquez le bouton orange "**TemporarilyDisable CARP**" :



CARP Maintenance

Temporarily Disable CARP Enter Persistent CARP Maintenance Mode

Instantanément, le statut du routeur MAITRE passe en mode **"DISABLED"** :

IPs have been disabled. Please note that disabling does not survive a reboot and some configuration changes will re-enable. ✕

CARP Maintenance

✓ Enable CARP 🔧 Enter Persistent CARP Maintenance Mode

CARP Status

Interface and VHID	Virtual IP Address	Description	Status
CARP@1	192.168.2.3/29	IP Virtuelle CARP	✕ DISABLED
LAN@2	192.168.1.3/24	IP Virtuelle LAN	✕ DISABLED

- Connectez-vous au routeur pfSENSE ESCLAVE et vérifiez son statut ; votre routeur pfSENSE ESCLAVE est maintenant passé au statut **"MASTER"**. La haute disponibilité est pleinement fonctionnelle :

CARP Status

Interface and VHID	Virtual IP Address	Description	Status
CARP@1	192.168.2.3/29	IP Virtuelle CARP	▶ MASTER
LAN@2	192.168.1.3/24	IP Virtuelle LAN	▶ MASTER

State Synchronization Status

Le routeur ESCLAVE devient maintenant le "maître" et assure la disponibilité des services de manière transparente.

VERIFICATION DU BON FONCTIONNEMENT DE LA HAUTE DISPONIBILITE

Nous allons simuler une panne complète du routeur pfSENSE MAITRE en l'arrêtant complètement.

Dans la machine Windows connectée au réseau local, nous vérifions que la connectivité est toujours opérationnelle et qu'il est toujours possible de naviguer sur Internet. Le routeur ESCLAVE a bien pris le "relais" :

Non sécurisé | https://192.168.1.2/status_carp.php

pfSense MAITRE | pfSENSE - ESCLAVE

Status / CARP

CARP Maintenance

🛑 Temporarily Disable CARP 🔧 Enter Persistent CARP Maintenance Mode

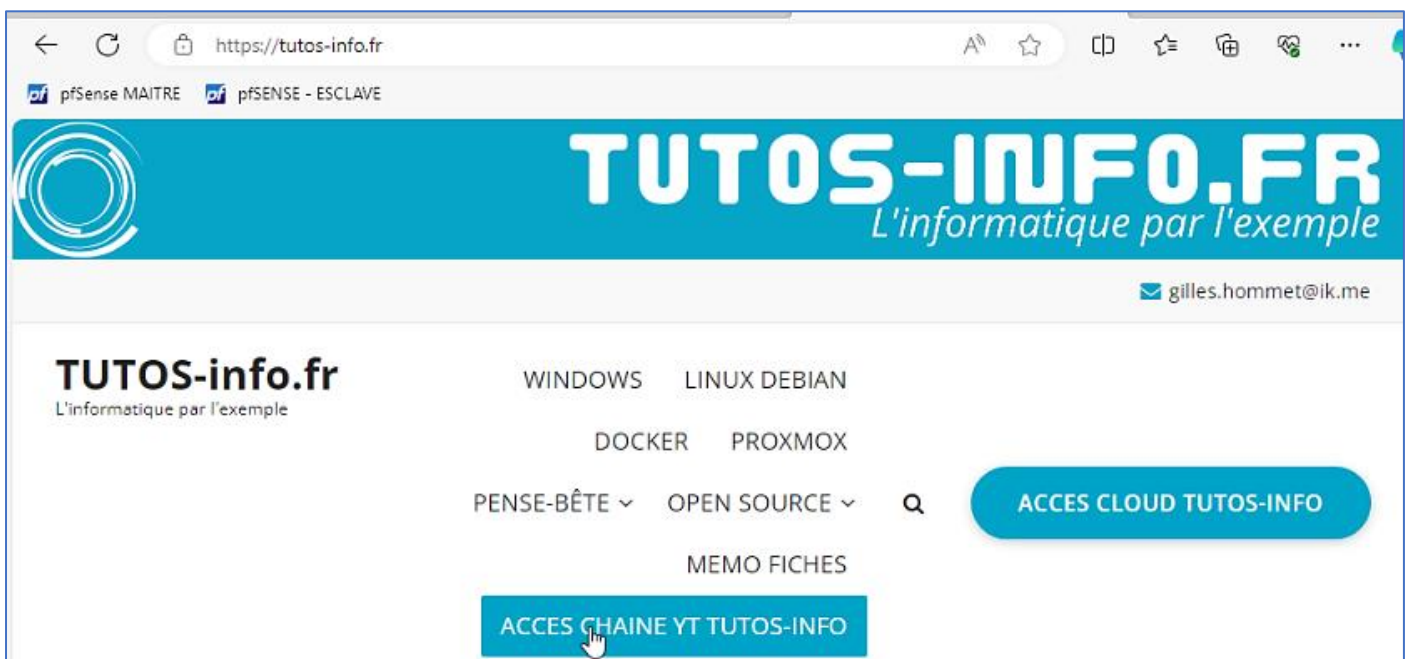
CARP Status

Interface and VHID	Virtual IP Address	Description	Status
CARP@1	192.168.2.3/29	IP Virtuelle CARP	▶ MASTER
LAN@2	192.168.1.3/24	IP Virtuelle LAN	▶ MASTER

Notre machine locale a bien un adressage IP en provenance du routeur pfSENSE ESCLAVE (le n° 2 ici) :

Propriété	Valeur
Suffixe DNS propre à la ...	pfsense2.lab
Description	Intel(R) PRO/1000 MT Network Connecti
Adresse physique	BC-24-11-71-9A-D0
DHCP activé	Oui
Adresse IPv4	192.168.1.10
Mask de sous-réseau ...	255.255.255.0
Bail obtenu	lundi 5 février 2024 08:30:20
Bail expirant	lundi 5 février 2024 10:30:19
Passerelle par défaut IPv4	192.168.1.3
Serveur DHCP IPv4	192.168.1.2
Serveur DNS IPv4	192.168.1.2

L'accès internet est bien opérationnel bien que le routeur MAITRE soit hors service :



Nous présenterons, dans d'autres modules pfSENSE, les multiples possibilités offertes par ce routeur Open Source, parmi lesquelles :

- le load-balancing
- l'utilisation de ACME, au sein de pfSENSE, pour générer des certificats Let's Encrypt
- l'utilisation de HA PROXY au sein de pfSENSE
- la mise en place d'un VPN, au sein de pfSENSE, avec le protocole Open VPN

Les possibilités sont variées et pfSENSE est une solution à envisager pour les entreprise ne disposant pas de budgets suffisamment importants pour investir dans des routeurs matériels onéreux.