Victor Jourdan SIO2

Année scolaire : 2025
Environnement : pfSense 2.7.2 – Proxmox VE – Réseau virtuel

Implémentation du protocole CARP et du service PFSYNC

Table des matières

1. Introduction

L'objectif de ce projet est de mettre en place un système de **haute disponibilité réseau** reposant sur deux pare-feux **pfSense** fonctionnant en **mode redondant** à l'aide des protocoles **CARP** (Common Address Redundancy Protocol) et **pfsync**.
L'ensemble est déployé dans un environnement de virtualisation **Proxmox VE**, afin de garantir la continuité du service réseau en cas de défaillance d'un des pare-feux.

Contexte

Dans une architecture réseau classique, un pare-feu unique constitue un point de défaillance critique.
Si celui-ci tombe, la connectivité Internet et l'accès aux services internes sont interrompus.
La mise en place d'un cluster pfSense redondant permet d'éviter cette situation : lorsqu'un des deux nœuds devient indisponible, le second prend automatiquement le relais sans coupure de service perceptible pour les utilisateurs.

Objectifs du projet

- Assurer la **redondance** des passerelles réseau internes et externes.
- Garantir la **continuité de service** pour les utilisateurs en cas de panne d'un pare-feu.
- Synchroniser les **états de connexion (pfsync)** et la **configuration complète (XMLRPC)** entre les deux machines.
- Tester et valider le **basculement automatique (failover)** sans perte de sessions actives.

Description de l'environnement

Le cluster pfSense est hébergé sur **Proxmox VE**, avec un réseau virtuel structuré en trois bridges :

Bridge Proxmox	Rôle	Réseau associé	Description
vmbr10	WAN	172.17.0.0/16	Sortie vers Internet
vmbr1140	LAN	192.168.1.0/24	Réseau interne des utilisateurs
vmbr1150	SYNC	10.0.0.0/30	Réseau dédié à la synchronisation pfsync/XMLRPC

Chaque pfSense dispose de trois interfaces réseau virtuelles connectées à ces bridges.

Pare-feu 1 (PF1 – Maître)

- **WAN (em0)** : 172.17.1.41/16
- **LAN (em1)** : 192.168.1.2/24
- **SYNC (vtnet0)** : 10.0.0.1/30
- **VIP CARP WAN** : 172.17.1.40/16
- **VIP CARP LAN** : 192.168.1.1/24

Pare-feu 2 (PF2 – Secondaire)

- **WAN (em0)** : 172.17.1.42/16
- **LAN (em1)** : 192.168.1.3/24
- **SYNC (vtnet0)** : 10.0.0.2/30
- **VIP CARP WAN** : 172.17.1.40/16
- **VIP CARP LAN** : 192.168.1.1/24

Fonctionnement attendu

- Le protocole **CARP** assure la gestion de l'adresse IP virtuelle (VIP).
  → Lorsque le nœud principal (PF1) est actif, il détient les adresses 172.17.1.40 et 192.168.1.1.

→ En cas de panne, PF2 reprend automatiquement ces adresses et devient la passerelle active.

- Le service **pfsync** synchronise les sessions TCP actives afin que les utilisateurs ne subissent aucune déconnexion lors du basculement.
- Le service **XMLRPC** assure la réplication automatique des règles, NAT, DHCP et autres paramètres entre les deux pfSense.

Cette architecture permet de démontrer la mise en œuvre d'un **système de tolérance aux pannes** complet, aligné avec les compétences SISR du BTS SIO :
administration de services réseaux, sécurisation d'infrastructures, et automatisation de déploiements.

2. Topologie réseau

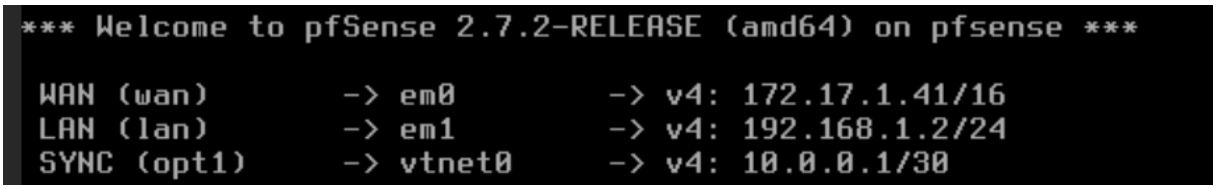
La topologie réseau mise en place vise à **assurer la haute disponibilité de la passerelle Internet** tout en isolant les différents flux (LAN, WAN, synchronisation).
L'architecture repose sur deux machines virtuelles **pfSense** hébergées sur **Proxmox VE**, configurées en **cluster CARP/pfsync**.
Cette structure permet :

- la **continuité de service** en cas de panne d'un nœud ;
- la **synchronisation automatique** des états et configurations ;
- un **environnement de test réaliste** pour démontrer la gestion d'une redondance réseau complète.

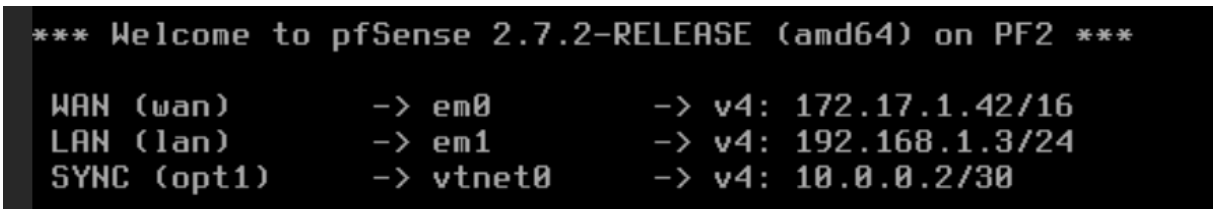
2.2 Description générale du schéma
Le réseau est segmenté en trois zones distinctes, chacune reliée à un bridge Proxmox :

Zone	Bridge Proxmox	Sous-réseau	Rôle principal
WAN	vmbr10	172.17.0.0/16	Connexion vers Internet / routeur amont
LAN	vmbr1140	192.168.1.0/24	Réseau interne des utilisateurs
SYNC	vmbr1141	10.0.0.0/30	Lien point-à-point entre les deux pfSense (pfsync & XMLRPC)

- **Communication SYNC (pfsync)** : assurée via le réseau 10.0.0.0/30 (trafic isolé).
- **Communication XMLRPC** : via HTTPS sur le même lien SYNC, IP cible https://10.0.0.2.
- **Routage et basculement** : CARP gère automatiquement la transition de la VIP entre les deux nœuds



Pf2



3. Mise en place du cluster pfSense

L'objectif de cette étape est de déployer deux pare-feux **pfSense** identiques, configurés pour fonctionner en **cluster redondant**.
Chaque pare-feu possède une configuration réseau cohérente (mêmes interfaces, mêmes noms, mêmes VLANs) afin de garantir la compatibilité du protocole **CARP** et du service **pfsync**.

Cette préparation constitue la base du mécanisme de **haute disponibilité** : les deux nœuds doivent être parfaitement synchrones sur le plan matériel et logique avant toute activation de redondance.

3.2 Préparation de l'environnement virtuel

Hyperviseur : Proxmox VE

- Les deux pare-feux sont virtualisés dans **Proxmox VE**, sur le même hôte physique.
- Chaque VM dispose de **3 interfaces réseau virtuelles** :
  - **vmbr10 (WAN)** : connectée au routeur ou à Internet, réseau 172.17.0.0/16.
  - **vmbr1140 (LAN)** : réseau interne 192.168.1.0/24.
  - **vmbr1150 (SYNC)** : réseau isolé 10.0.0.0/30 pour la synchronisation.

3.3 Installation et configuration initiale des pare-feux

Étape 1 – Installation de pfSense

- Installation classique à partir de l'image ISO officielle **pfSense 2.7.x**.
- Attribution d'un mot de passe administrateur commun aux deux pare-feux (admin / *****).
- Aucun paquet additionnel n'est nécessaire à ce stade.

Étape 2 – Assignation des interfaces

À la première ouverture de la console pfSense :

Interface	Nom pfSense	Bridge Proxmox	Rôle
em0	WAN	vmbr10	Vers Internet
em1	LAN	vmbr1140	Réseau interne
vtnet0	SYNC	vmbr1150	Lien de synchronisation

Pare-feu	Interface	IP / Masque	Rôle
PF1	WAN	172.17.1.41 / 16	Interface WAN maître
PF1	LAN	192.168.1.2 / 24	Interface LAN maître
PF1	SYNC	10.0.0.1 / 30	Lien de synchronisation
PF2	WAN	172.17.1.42 / 16	Interface WAN secondaire
PF2	LAN	192.168.1.3 / 24	Interface LAN secondaire
PF2	SYNC	10.0.0.2 / 30	Lien de synchronisation

3.5 Désactivation des filtrages WAN internes

Pour permettre la communication entre les deux pare-feux sur des plages privées, les options suivantes sont décochées sur les **deux** nœuds :

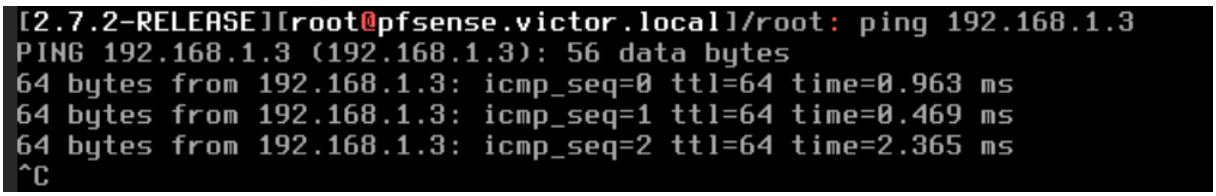
Menu : Interfaces → WAN

- *Block private networks and loopback addresses*
- *Block bogon networks*

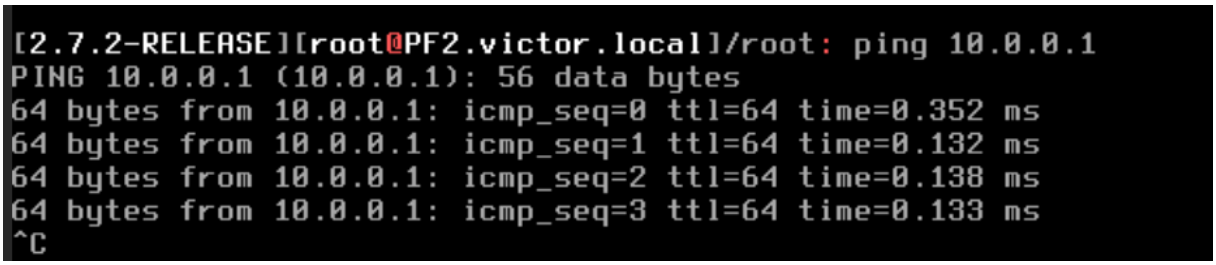
Cette étape est indispensable car le réseau WAN utilisé (172.17.0.0/16) appartient à une plage d'adressage privée (RFC1918) que pfSense bloque par défaut.

Test	Résultat attendu	
Ping PF1 ↔ PF2 sur LAN (192.168.1.x)	Communication bidirectionnelle	✅
Ping PF1 ↔ PF2 sur SYNC (10.0.0.x)	Communication bidirectionnelle	✅
Ping PF1 vers pf2 WAN 172.17.1.42	Réponse	✅
Ping PF2 vers pf1 WAN 172.17.1.41	Réponse	✅

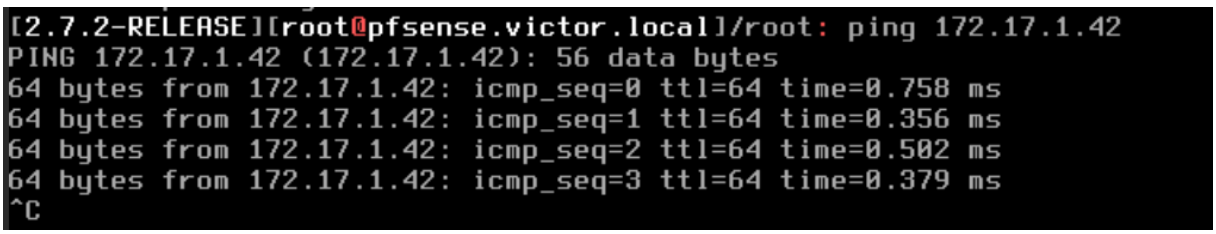
Test PF1 ➔ PF2



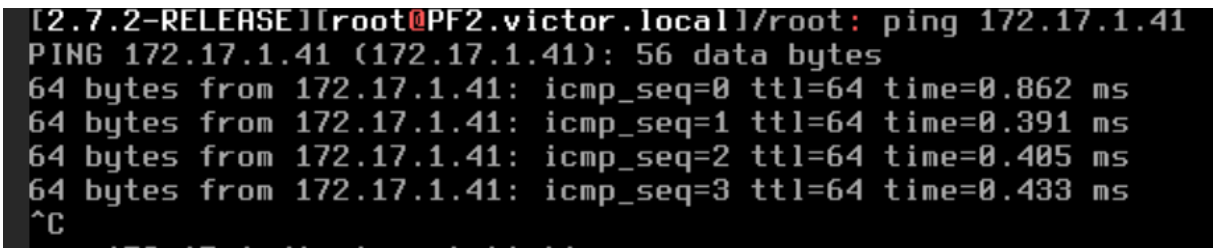
Test PF2 ➔ PF1 VIA SYNC



Test PF1 ➔ pf2 WAN



Test PF2 ➔ pf1 WAN



4. Configuration du protocole CARP

Le protocole **CARP (Common Address Redundancy Protocol)** permet de partager une **adresse IP virtuelle** entre plusieurs pare-feux.
Dans cette architecture, il assure que **l'un des deux pfSense** détient l'adresse utilisée comme **passerelle principale**, tandis que l'autre reste en veille prête à prendre le relais en cas de panne.
Le principe repose sur :

- une **adresse IP virtuelle (VIP)** partagée sur chaque réseau (WAN et LAN) ;
- un **identifiant unique (VHID)** par interface CARP ;
- un **mécanisme de priorité (advskew)** déterminant qui est le maître.

4.2 Préparation à la configuration CARP
Avant d'ajouter les VIP, chaque pare-feu dispose déjà de ses adresses réelles :

Pare-feu	Interface	IP réelle	Réseau	Description
PF1	WAN	172.17.1.41	172.17.0.0/16	Interface WAN principale
PF1	LAN	192.168.1.2	192.168.1.0/24	Interface LAN principale
PF2	WAN	172.17.1.42	172.17.0.0/16	Interface WAN secondaire
PF2	LAN	192.168.1.3	192.168.1.0/24	Interface LAN secondaire

Les adresses virtuelles (VIP) seront ensuite créées pour permettre le basculement automatique :

Interface	Adresse virtuelle (CARP)	VHID	Maître (advskew=0)	Secondaire (advskew=100)
WAN	172.17.1.40	10	PF1	PF2
LAN	192.168.1.1	20	PF1	PF2

4.3 Création des VIP sur PF1 (Maître)
Menu : Firewall → Virtual IPs → Add

- **Type :** CARP
- **Interface :** WAN
- **Address :** 172.17.1.40 / 16
- **VHID Group :** 10
- **Advbase :** 1
- **Advskew :** 0
- **Password :** (identique sur les deux nœuds)

Procède de la même manière pour le **LAN** :

- **Interface :** LAN
- **Address :** 192.168.1.1 / 24
- **VHID Group :** 20
- **Advskew :** 0

Pf1

Adresse IP virtuelle	Interface	Type	Description	Actions
172.17.1.40/16 (vhid: 10)	WAN	CARP	victor	
192.168.1.1/24 (vhid: 20)	LAN	CARP		

4.4 Création des VIP sur PF2 (Secondaire)
Répète la même configuration dans Firewall → Virtual IPs → Add, mais avec **Advskew = 100** pour indiquer que ce pare-feu est **en mode BACKUP**.
Le VHID et le mot de passe doivent être identiques à ceux de PF1 pour chaque réseau.

4.5 Vérification de l'état CARP
Sur chaque pare-feu :
Menu : Status → CARP (Failover)
Tu dois observer :

- PF1 : **MASTER** sur VHID 10 et 20
- PF2 : **BACKUP** sur VHID 10 et 20

Les deux VIP (172.17.1.40 et 192.168.1.1) doivent apparaître comme "Active".

Tests de fonctionnement
Test 1 — Vérification des VIP
Depuis un poste du LAN :

- Ping **192.168.1.1** → Réponse (VIP active sur PF1).
  Depuis le réseau amont :
- Ping **172.17.1.40** → Réponse (VIP WAN active sur PF1).

Test 2 — Simulation de panne

- Éteindre la VM **PF1** ou désactiver CARP depuis :
  Status → CARP → Disable CARP

- Observer sur PF2 :
  → Les deux interfaces passent automatiquement en **MASTER**.
- Le ping sur les deux VIP continue sans coupure perceptible.

Test 3 — Rétablissement

- Redémarrer PF1.
- Vérifier que PF1 reprend le rôle **MASTER**, PF2 repasse en **BACKUP**.

Analyse du fonctionnement CARP

- Le **champ VHID** permet de distinguer les interfaces synchronisées.
  Chaque VHID doit être **unique par sous-réseau** pour éviter les conflits.
- Le **champ Advskew** détermine la priorité :
  - Valeur basse → priorité élevée (MASTER).
  - Valeur haute → priorité faible (BACKUP).
- Le **protocole multicast 224.0.0.18** est utilisé pour échanger les annonces CARP entre les nœuds.
  Si ce trafic est bloqué (bridge ou firewall), la bascule échouera.

Résultats obtenus

Situation	Pare-feu actif	Rôle CARP	Connectivité LAN/WAN
PF1 en service	PF1	MASTER	✅
PF1 arrêté	PF2	MASTER	✅
PF1 redémarre	PF1	MASTER (retour automatique)	✅

Conclusion

Le protocole CARP est désormais pleinement fonctionnel :

- Les deux pare-feux partagent des adresses IP virtuelles communes.
- Le basculement est transparent pour les utilisateurs.
- Le cluster est prêt à recevoir la configuration **pfsync**, qui permettra la synchronisation des états de connexion en temps réel.

5. Configuration du service pfsync

Le service **pfsync** permet la **synchronisation en temps réel des états de connexion** entre les deux pare-feux du cluster.
Lorsqu'un utilisateur établit une connexion (HTTP, SSH, ICMP…), cette information est automatiquement répliquée sur le pare-feu secondaire.
Ainsi, en cas de basculement (failover), les sessions actives ne sont pas interrompues.
L'association de **pfsync** (synchronisation des états) et **CARP** (synchronisation des adresses virtuelles) garantit une **haute disponibilité totale**, sans perte de connectivité.

Préparation de l'interface SYNC

Le lien de synchronisation est établi via un réseau dédié, isolé du LAN et du WAN pour des raisons de sécurité et de performance.
Ce réseau passe par le bridge **vmbr1150** de Proxmox.

Pare-feu	Interface	Nom	Adresse IP	Rôle
PF1	vtnet0	SYNC	10.0.0.1 / 30	Maître
PF2	vtnet0	SYNC	10.0.0.2 / 30	Secondaire

Étapes de configuration :

1. Aller dans **Interfaces → Assignments**.
2. Ajouter la 3e carte réseau (vtnet0) et la nommer **SYNC**.
3. Activer l'interface, cocher *Enable Interface*.
4. Définir une **adresse statique IPv4** :
   - PF1 → 10.0.0.1 / 30
   - PF2 → 10.0.0.2 / 30
5. Aucun serveur DHCP ni passerelle ne doit être configuré sur cette interface.

Création des règles de pare-feu SYNC

Le protocole pfsync utilise un type de paquet spécifique (non TCP/UDP).
Pour autoriser le trafic de synchronisation, des règles dédiées sont nécessaires sur **chaque pare-feu** :
Menu : Firewall → Rules → SYNC

1. **Autoriser pfsync**
   - Action : *Pass*
   - Interface : SYNC
   - Protocol : *pfsync*
   - Source : any
   - Destination : any
   - Description : "Allow pfsync synchronization"
2. **Autoriser HTTPS (XMLRPC)**
   - Action : *Pass*
   - Interface : SYNC
   - Protocol : *TCP*
   - Destination port : *443*
   - Description : "Allow XMLRPC config sync"

Ces deux règles assurent la communication complète entre les pare-feux pour la synchronisation des états et des configurations.

Activation du service pfsync

Sur **les deux pare-feux** :
Menu : System → High Availability Sync

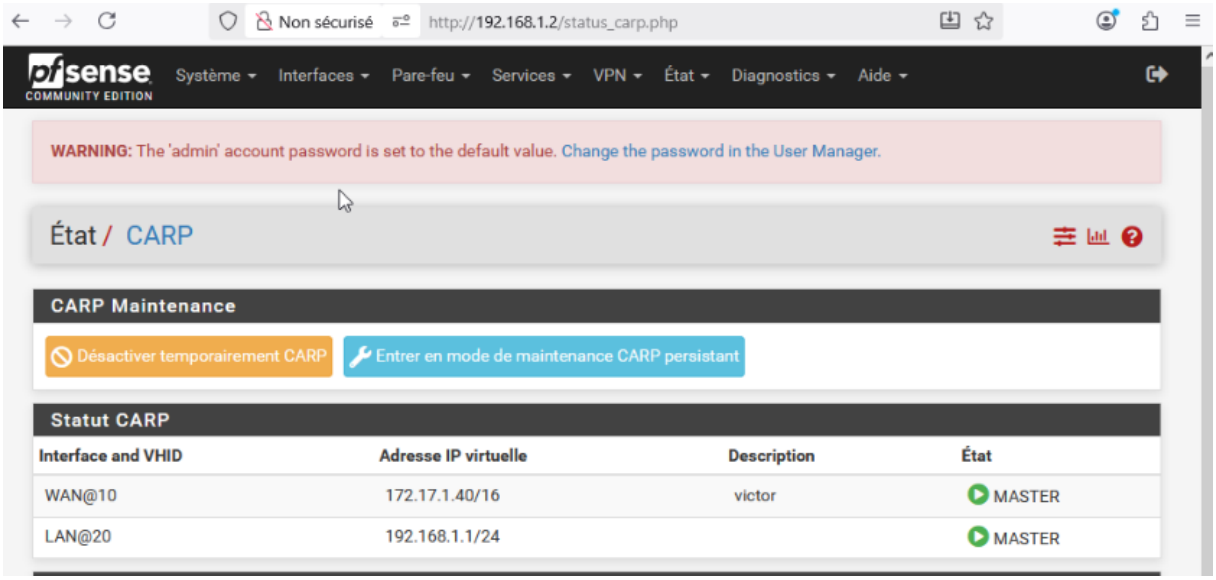
- ✅ *Synchronize States*
- *Synchronize Interface* : **SYNC**
- *pfsync Synchronize Peer IP* :
  - Sur PF1 → 10.0.0.2
  - Sur PF2 → 10.0.0.1

Aucune autre configuration n'est nécessaire à ce stade.

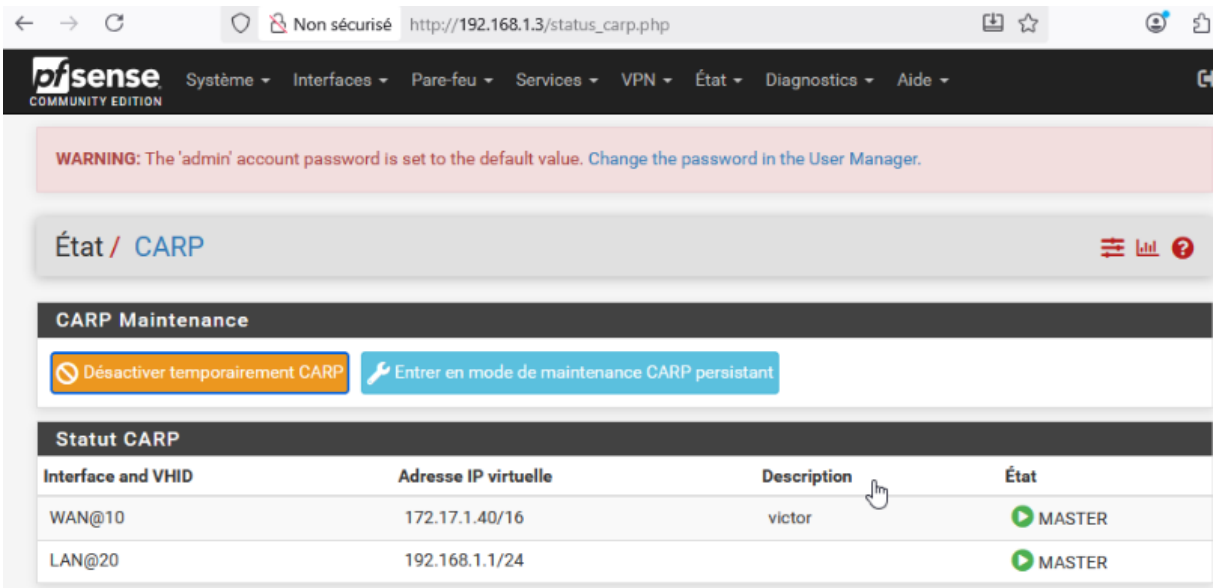
Test — Coupure du maître

- Éteindre ou désactiver CARP sur PF1.
- Observer PF2 : il devient automatiquement **MASTER**.
- Le ping du poste LAN vers Internet continue sans interruption : preuve que les états TCP/ICMP ont été répliqués via pfsync.

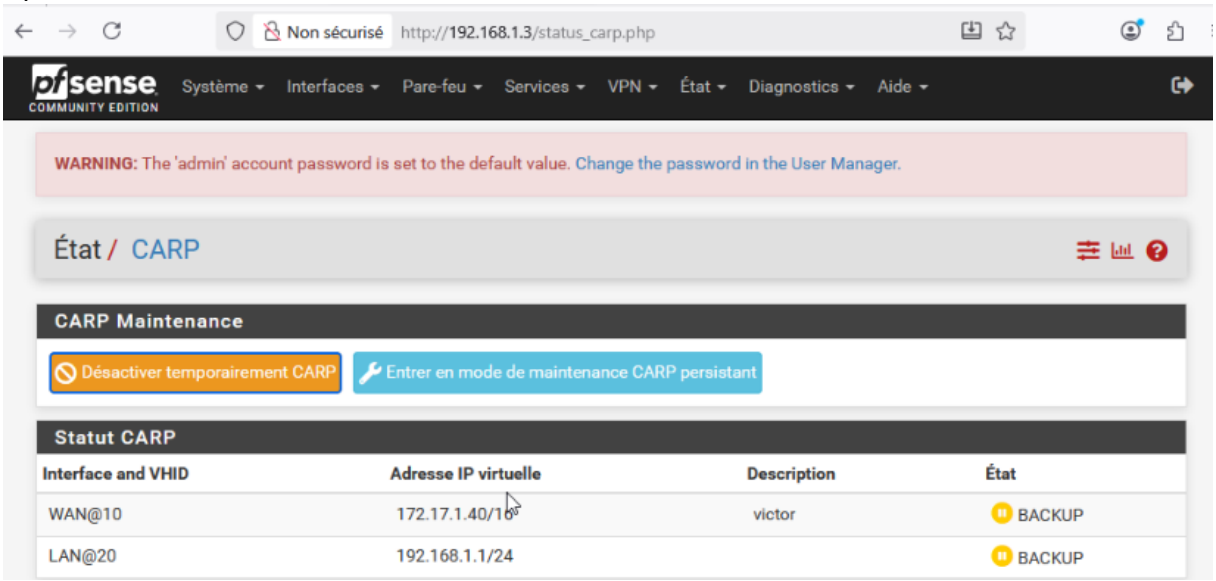
Avant reboot sur le PF1



En cours de reboot



Après reboot



Conclusion
Le service **pfsync** assure une continuité totale des connexions actives entre les deux pare-feux.
Combiné au protocole **CARP**, il permet de garantir une **tolérance de panne complète**, sans perte de session utilisateur.
Cette configuration est désormais prête pour l'étape suivante : la **synchronisation de la configuration via XMLRPC**, qui maintiendra les deux nœuds identiques sur le plan logiciel.

6. Configuration de la synchronisation XMLRPC

La synchronisation **XMLRPC** permet à un pare-feu pfSense (le maître) de **répliquer automatiquement sa configuration** vers le second pare-feu (le backup).
Contrairement au protocole **pfsync**, qui ne synchronise que les états des connexions, **XMLRPC** gère la réplication complète de la configuration :
règles de pare-feu, NAT, DHCP, IP virtuelles, VPN, etc.
Ainsi, toute modification réalisée sur le pfSense principal est automatiquement appliquée au second, assurant une **cohérence parfaite du cluster**.

Conditions préalables
Avant la mise en place de la synchronisation XMLRPC :

- La communication HTTPS entre les deux pare-feux doit être **fonctionnelle** via le lien SYNC (10.0.0.0/30).
- Le service pfsync doit être **actif et opérationnel**.
- Les interfaces et noms de réseaux doivent être **identiques** sur les deux pfSense (WAN, LAN, SYNC).
- Les pare-feux doivent posséder **la même version** de pfSense.

Configuration sur le pare-feu principal (PF1)
Menu : System → High Availability Sync

Section : *Configuration Synchronization Settings (XMLRPC Sync)*

Champ	Valeur à renseigner
Synchronize Config to IP	https://10.0.0.2
Remote System Username	admin
Remote System Password	mot de passe administrateur de PF2
Disable Certificate Verification	✅ coché

Synchronize the following sections coche les cases suivantes :

- Firewall Rules
- Firewall NAT
- Virtual IPs
- DHCP Server
- DNS Resolver / Forwarder
- IPsec / OpenVPN (si utilisé)
- System Tunables (facultatif) |

Une fois la configuration saisie, clique sur **Save**.

6.4 Vérification sur le pare-feu secondaire (PF2)

Sur PF2, **aucune configuration XMLRPC ne doit être activée**.
Ce nœud ne fait que recevoir la configuration envoyée par PF1.
Pour vérifier :

- Menu : System → High Availability Sync
- Toutes les cases de la section *XMLRPC Sync* doivent être **vides**.

6.5 Règles de pare-feu nécessaires sur l'interface SYNC

Sur **les deux pfSense** :

- Firewall → Rules → SYNC
- Ajoute ou vérifie la règle suivante :

Champ	Valeur
Action	Pass
Protocol	TCP
Destination port	443
Source	any
Destination	any
Description	"Allow HTTPS (XMLRPC)"

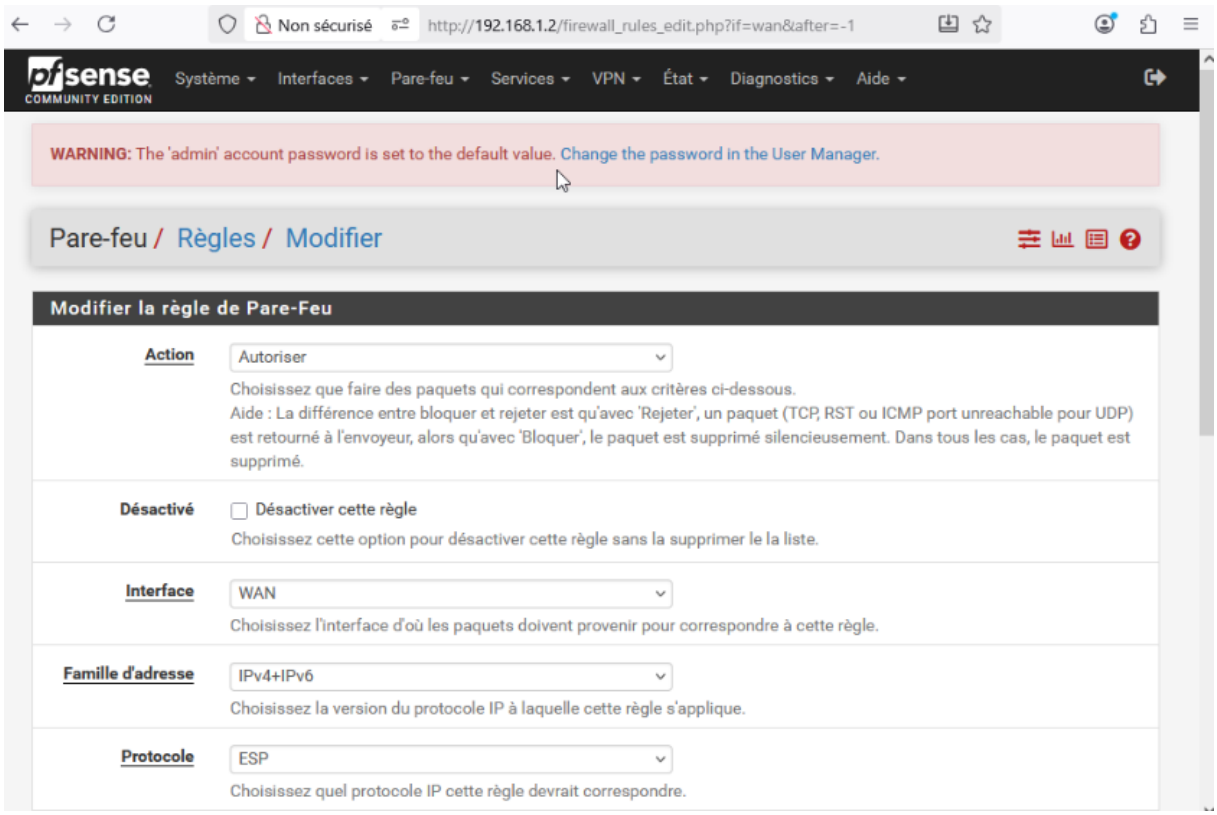
Cela permet à PF1 d'atteindre l'interface web sécurisée (port 443) de PF2 pour transmettre les configurations.

6.6 Tests de synchronisation

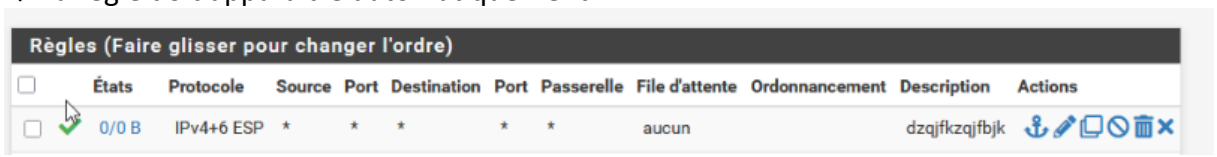
Test 1 – Règle de pare-feu

1. Sur **PF1**, crée une règle simple dans Firewall → Rules → LAN :
    - Action : Pass
    - Source/Destination : any
    - Clique **Save** puis **Apply Changes**.

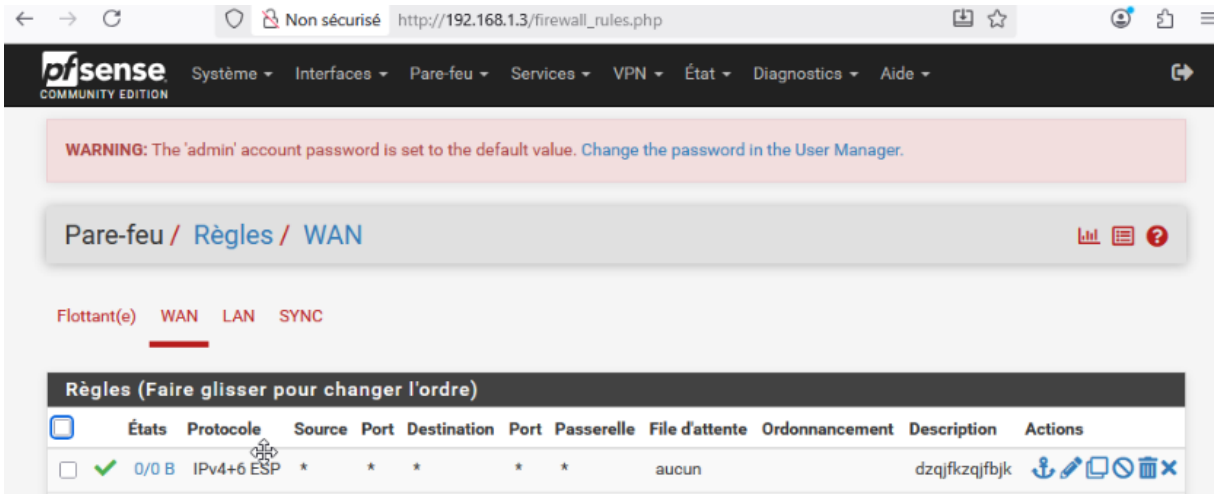
2. Sur **PF2**, vérifie dans le même menu :



→ La règle doit apparaître automatiquement.



Sur pf 2 ➔



La mise en place de la synchronisation XMLRPC assure une **cohérence totale de la configuration** entre les deux pare-feux. Associée à **CARP** et **pfsync**, elle complète la mise en œuvre d'une infrastructure de **haute disponibilité réseau** fiable et automatisée.
Toute modification effectuée sur PF1 est désormais répliquée sur PF2 sans intervention manuelle, garantissant un fonctionnement stable du cluster et un basculement transparent pour les utilisateurs.

9. Conclusion

La mise en place de la **haute disponibilité réseau** à l'aide de **pfSense**, du protocole **CARP** et du service **pfsync** a permis de démontrer une architecture robuste et résiliente, conforme aux exigences d'une infrastructure professionnelle.
Ce projet a abouti à la configuration complète d'un **cluster redondant** composé de deux pare-feux virtualisés sous **Proxmox VE**, capables d'assurer la continuité de service sans interruption perceptible pour les utilisateurs.
Grâce au protocole **CARP**, les deux pare-feux partagent des **adresses IP virtuelles** qui assurent un basculement automatique et transparent entre le nœud maître et le nœud secondaire. Le service **pfsync** garantit la **synchronisation instantanée des états de connexion**, permettant aux sessions en cours de survivre à une panne du maître.
Enfin, la synchronisation **XMLRPC** maintient l'uniformité des configurations entre les deux systèmes, renforçant la stabilité globale du cluster.
Sur le plan opérationnel, les différents tests effectués (ping, coupure volontaire de VM, désactivation CARP, vérification des logs et des états TCP) ont confirmé la **fiabilité du mécanisme de basculement**. Les connexions demeurent actives, les IP virtuelles basculent automatiquement, et le retour du maître se fait sans impact pour le réseau.
Cette infrastructure illustre concrètement plusieurs **compétences du référentiel BTS SIO option SISR**, notamment :

- *Gérer la disponibilité et la continuité des services informatiques* ;
- *Mettre en œuvre des solutions de virtualisation et de sécurité réseau* ;
- *Administrer des équipements réseaux et assurer la supervision des services.*

En conclusion, cette mise en œuvre d'un cluster pfSense haute disponibilité démontre la capacité à concevoir et administrer une architecture **fiable, sécurisée et tolérante aux pannes**, répondant aux standards professionnels actuels.
Elle constitue une base solide pour toute évolution future, notamment vers une réplication multi-site, une supervision centralisée ou une intégration avec des services cloud hybrides