Haute disponibilité réseau avec pfSense : mise en œuvre du protocole CARP

- ▼ 🗒️ Sommaire
  - 🎯 Pourquoi avoir mis en place un pfSense en mode failover (CARP)
  - ⚠️ Prérequis avant la mise en place du failover avec pfSense
  - ▼ 🌐 Présentation de l’architecture pfSense (Failover)
    - 🔷 pfSense MASTER
    - 🔶 pfSense BACKUP
  - ▼ 🧱 Mise en place des IPs virtuelles CARP
    - 🎯 Objectif
    - 📩 Configuration à appliquer
    - 🖥️ Exemple de configuration
  - ▼ 🔁 Test du basculement CARP (failover)
    - 🧪 Scénario de test : simulation de panne du pfSense principal
  - ▼ 🔄 Mise en place de la synchronisation entre les deux pfSense
    - ⚙️ Synchronisation d’état (pfsync)
    - ⚙️ Synchronisation de configuration (XMLRPC Sync)
  - ▼ 🛡️ Mise en place des règles de pare-feu sur l’interface HA
    - ✅ Règles à mettre en place
    - 📌 Détails importants
  - ✅ Conclusion

🎯 Pourquoi avoir mis en place un pfSense en mode failover (CARP)

La mise en place d'un système pfSense en mode **failover** permet de **garantir la haute disponibilité du réseau** de l'entreprise Uranus.

En cas de panne du pare-feu principal, le **second pfSense prend automatiquement le relais**, assurant une **continuité de service** sans interruption pour les utilisateurs.

Cette solution professionnelle s'appuie sur le protocole **CARP**, simple à mettre en œuvre et efficace, permettant d'**éviter tout point de défaillance unique** dans l'infrastructure.

⚠️ Prérequis avant la mise en place du failover avec pfSense

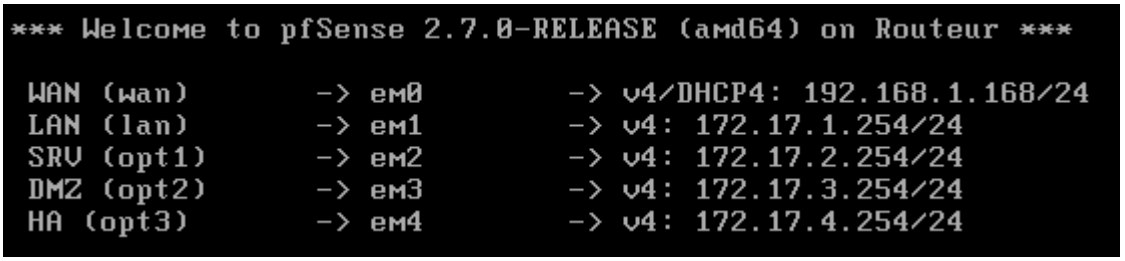
- Deux machines **pfSense identiques** (version et configuration)
- Interfaces réseau configurées de la **même manière** sur les deux pare-feux (LAN, DMZ, etc.)
- Une **IP propre** pour chaque pfSense + une **IP virtuelle (CARP)** par interface

🌐 Présentation de l'architecture pfSense (Failover)

Dans cette infrastructure, **deux pare-feux pfSense** ont été mis en place afin d'assurer une **haute disponibilité** (HA) via le protocole **CARP**. Cette configuration permet un **basculement automatique** du trafic réseau en cas de panne du pare-feu principal.

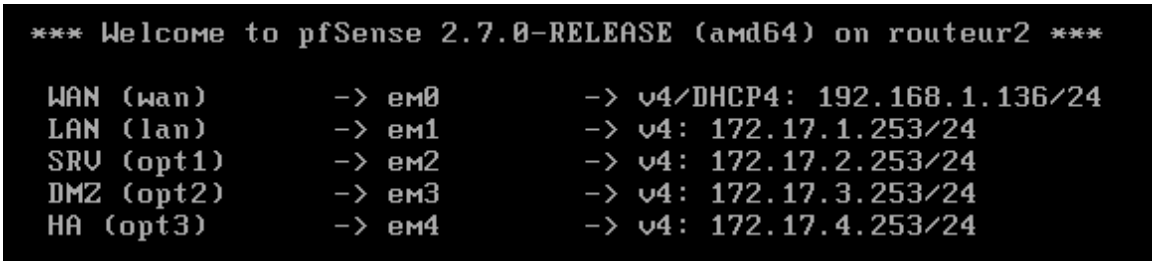
🔷 pfSense MASTER

- **Rôle** : Pare-feu principal (maître)
- **Nom** : `Routeur (MASTER)`
- **Version** : pfSense 2.7.0-RELEASE
- **Interfaces configurées** :
  - WAN → 192.168.1.168/24 *(DHCP)*
  - LAN → 172.17.1.254/24
  - SRV → 172.17.2.254/24
  - DMZ → 172.17.3.254/24
  - HA (interface dédiée HA Sync) → 172.17.4.254/24



🔶 pfSense BACKUP

- **Rôle** : Pare-feu secondaire (backup)
- **Nom** : `Routeur (BACKUP)`
- **Version** : pfSense 2.7.0-RELEASE
- **Interfaces configurées** :
  - WAN → 192.168.1.168/24 *(DHCP)*
  - LAN → 172.17.1.253/24
  - SRV → 172.17.2.253/24
  - DMZ → 172.17.3.253/24
  - HA (interface dédiée HA Sync) → 172.17.4.253/24



🧰 Mise en place des IPs virtuelles CARP

Afin d'assurer un **failover automatique** entre deux pare-feux pfSense, on utilise le protocole **CARP** (Common Address Redundancy Protocol), qui permet d'avoir des **IPs virtuelles partagées** entre le pare-feu principal (master) et le secondaire (backup).

🎯 Objectif

Créer une IP virtuelle CARP **par interface** (LAN, SRV, DMZ et HA) pour que tous les clients et serveurs utilisent **une seule passerelle**, automatiquement prise en charge par le pfSense actif.

📥 Configuration à appliquer

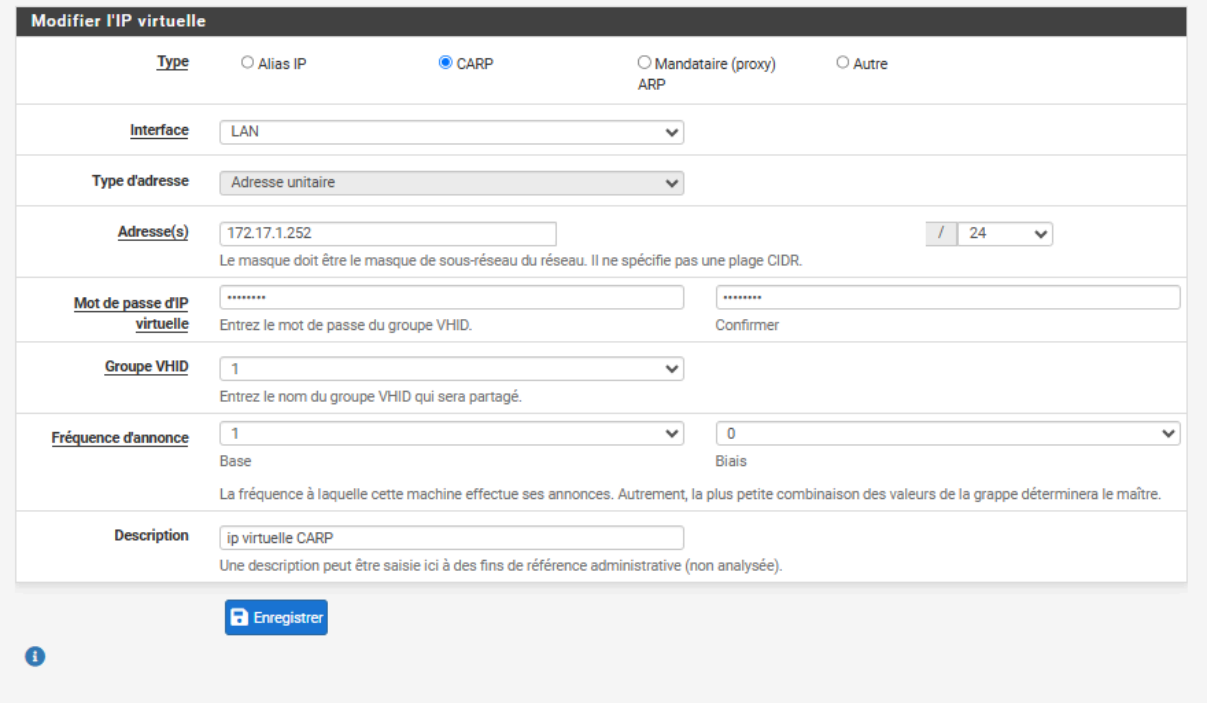
Sur les deux pfSense (master et backup), il faut :

- **Créer les mêmes IPs virtuelles**, avec les **mêmes paramètres**
- **Utiliser les mêmes VHID**
- **Renseigner le même mot de passe de synchronisation CARP**
- **Utiliser les mêmes interfaces**

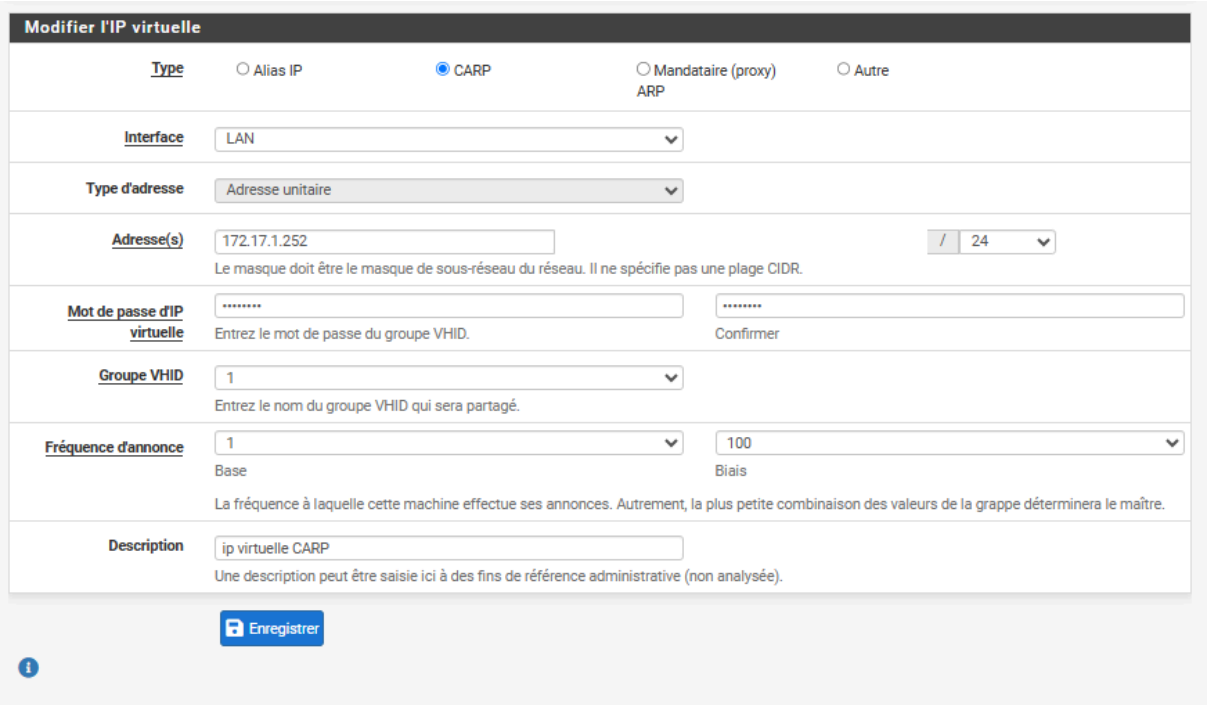
🖥️ Exemple de configuration (capture ci-dessous)

Paramètre	Valeur à configurer
Type	CARP
Interface	LAN, SRV, DMZ ou HA (à faire pour chaque interface)
Adresse	IP virtuelle ex : `172.17.1.252` pour le LAN
Masque CIDR	`/24`
Mot de passe d'IP virtuelle	Mot de passe identique sur les deux pare-feux
Groupe VHID	`1` (LAN), `2` (SRV), `3` (DMZ), `4` (HA)
Fréquence d'annonce	`1` Base (pfSense master), `100` Biais (pfSense backup)
Description	`ip virtuelle CARP`

📸 *Voici la capture correspondante à l'ajout de l'IP virtuelle sur l'interface LAN côté Master :*



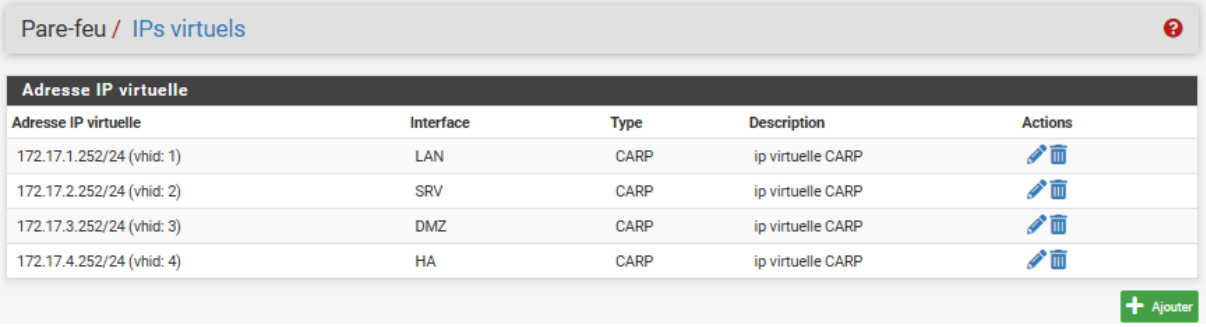
📸 *Voici la capture correspondante à l'ajout de l'IP virtuelle sur l'interface LAN côté Backup :*



⚠️ **Important** :

- Le **biais de 0** signifie que le pfSense est **prioritaire** (pare-feu principal)
- Le **biais de 100** est utilisé sur le **pfSense de secours**, pour éviter tout conflit

> Une fois configuré, vous verrez les IPs CARP apparaître dans Pare-feu > IPs virtuelles sur les deux pfSense.

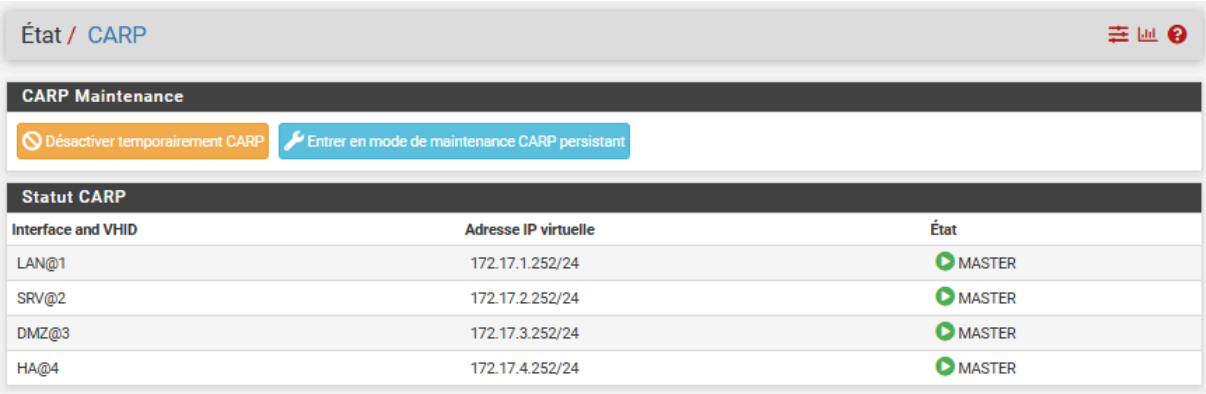


🔁 Test du basculement CARP (failover)

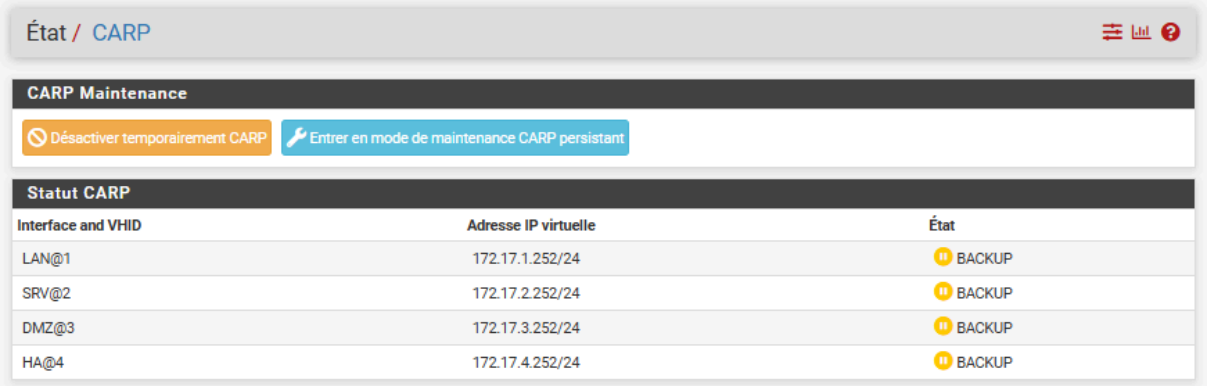
Une fois la **redondance CARP** configurée entre les deux pfSense (master et backup), il est essentiel de tester le bon fonctionnement du **basculement automatique**.

🧪 Scénario de test : simulation de panne du pfSense principal

PfSense **master** :



PfSense **slave**:

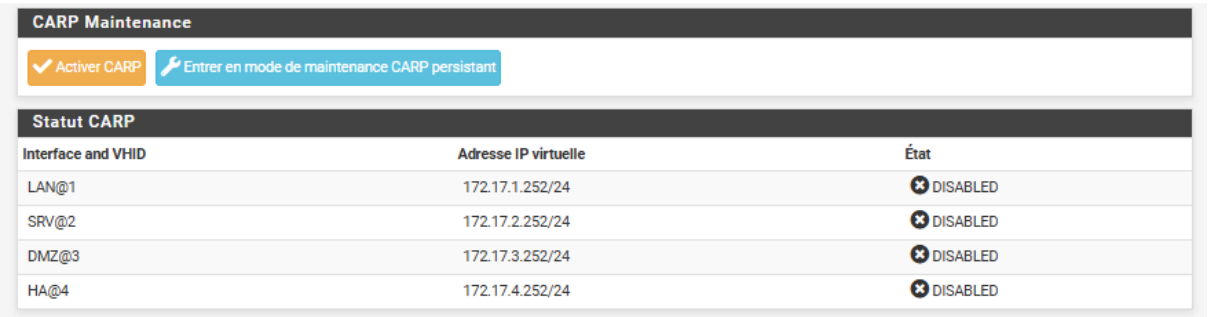


Sur le pfSense **master**, accède à la page :

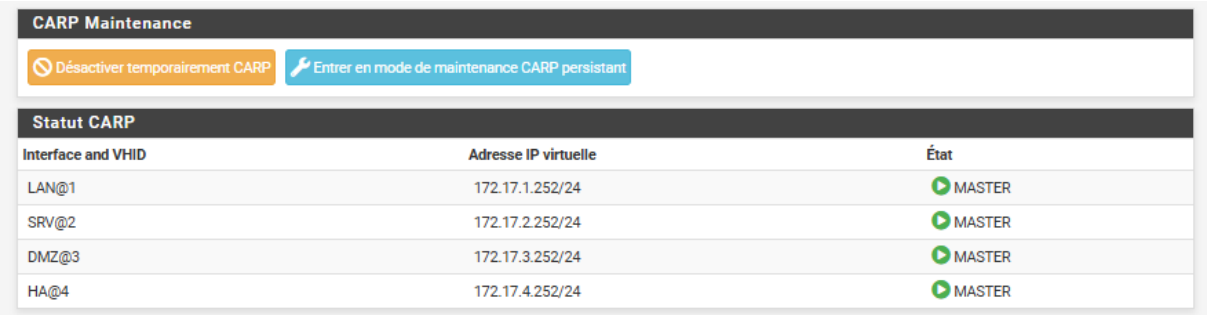
Statut > CARP (failover)

Clique sur le bouton :

Désactiver temporairement CARP

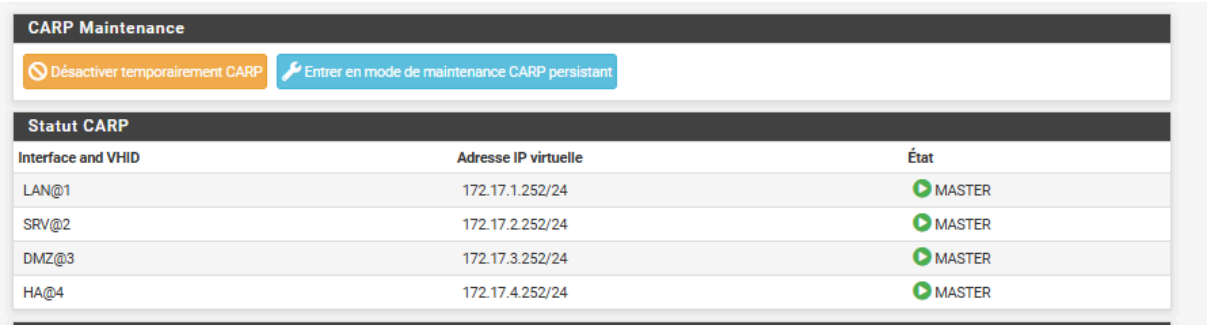


Le pfSense **slave passe en master:**

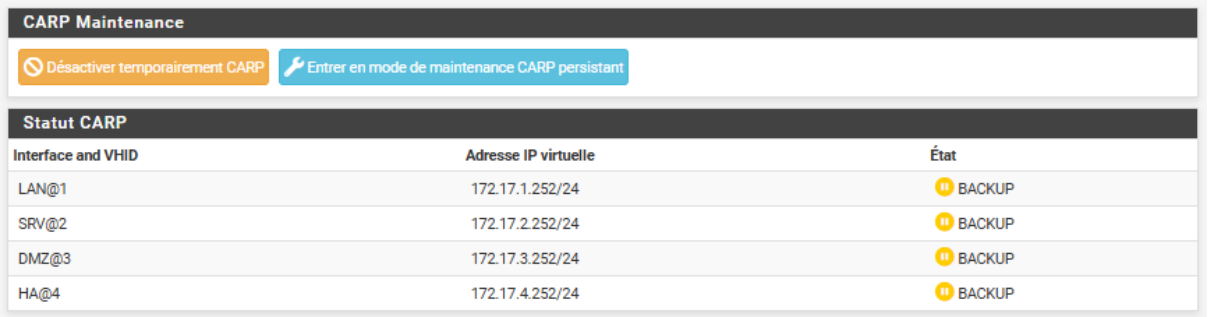


Lorsque le CARP est réactivé sur le pfSense principal :

- Il reprend automatiquement son rôle de **MASTER**



- Le pfSense secondaire repasse en **BACKUP**



🔄 Mise en place de la synchronisation entre les deux pfSense

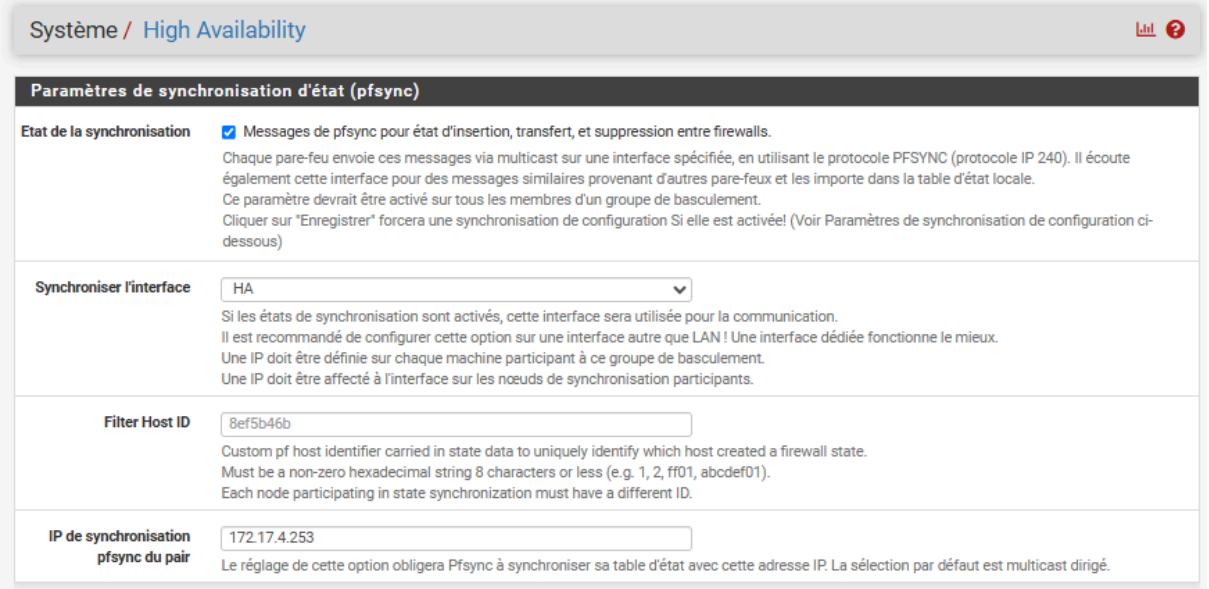
Une fois les IPs virtuelles configurées, il est essentiel d'assurer une **synchronisation entre le pare-feu principal (master)** et le **pare-feu secondaire (backup)**, afin de garantir un fonctionnement fluide en cas de basculement.

⚙️ Synchronisation d'état (pfsync)

La synchronisation d'état permet de partager les connexions actives (sessions) entre les deux pfSense. Ainsi, même en cas de basculement, les connexions établies ne sont pas interrompues.

📌 À configurer sur le pfSense **principal** :

- **Activer la synchronisation d'état**
- Choisir l'interface dédiée (dans notre cas : **HA**)
- Renseigner l'**IP du pare-feu secondaire** (172.17.4.253)

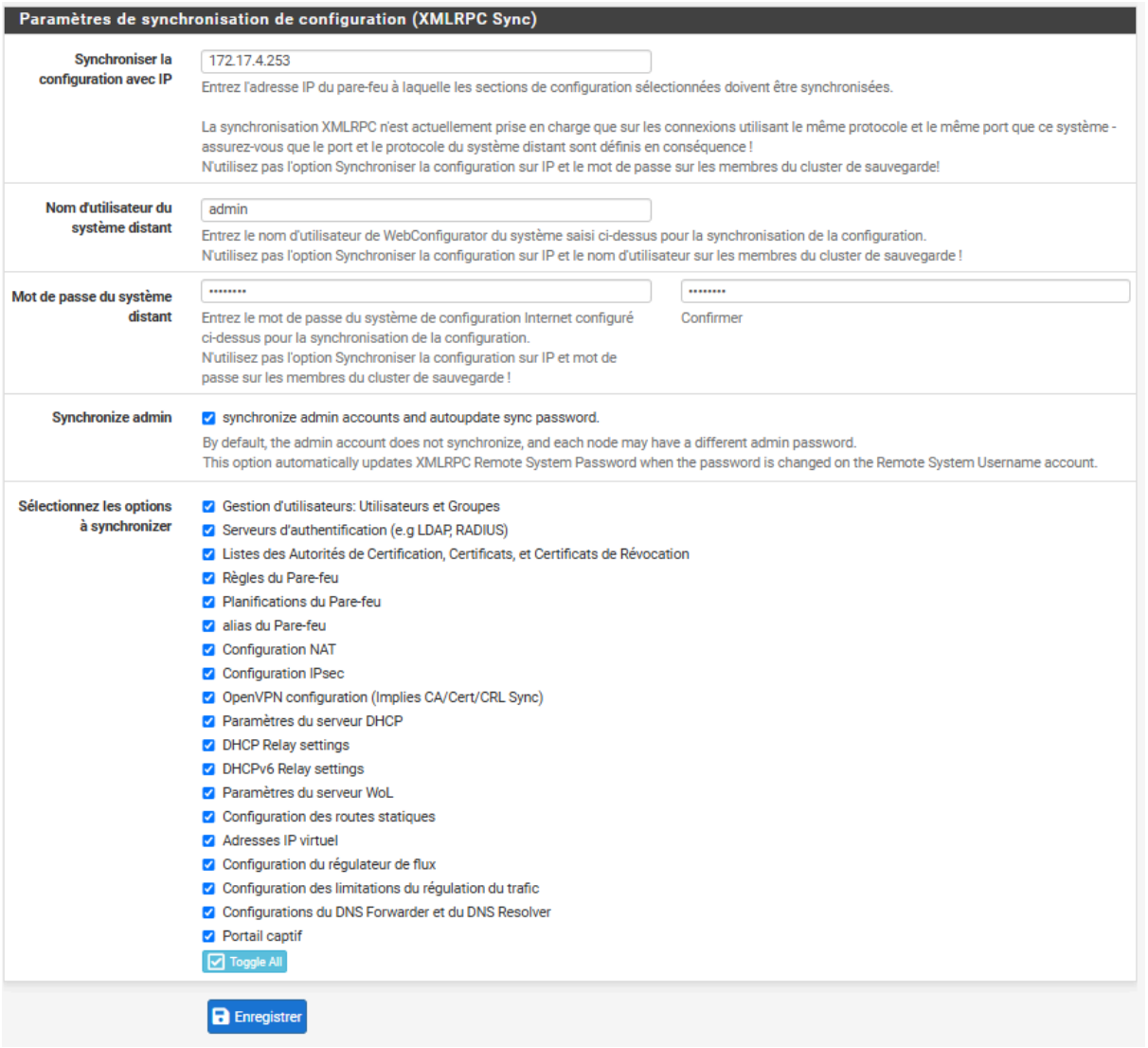


⚙️ Synchronisation de configuration (XMLRPC Sync)

La synchronisation de configuration permet de **répliquer automatiquement la configuration** du pfSense master vers le pfSense backup. C'est une étape clé pour garantir la cohérence des règles et services réseau.

📌 Toujours sur le pfSense **principal** :

- Renseigner l'IP de l'autre pare-feu (**172.17.4.253**)
- Rentrer les identifiants d'administration du système distant
- Cocher **Synchroniser admin**
- Sélectionner tous les éléments à synchroniser (✓ Toggle All)
- Puis enregistrer



🛡️ Mise en place des règles de pare-feu sur l'interface HA

Afin de permettre la **synchronisation complète entre les deux pare-feux pfSense**, deux règles doivent être configurées sur l'interface **HA** des **deux nœuds** (le pfSense principal et le pfSense de secours) :

✅ Règles à mettre en place

Protocole	Source	Destination	Port	Description

IPv4 TCP	HA net	Ce pare-feu	443 (HTTPS)	Autoriser XMLRPC
IPv4 PFSYNC	HA net	Ce pare-feu	* (tous ports)	Synchronisation des états (pfsync)

📌 Détails importants :

- La **règle XMLRPC** (port 443) permet la **synchronisation des configurations** depuis le pfSense principal vers le secondaire.
- La **règle PFSYNC** (protocole 240) permet la **synchronisation des connexions actives (états)** entre les deux pare-feux.
- Ces règles doivent être **appliquées sur les deux pfSense** pour assurer le bon fonctionnement du cluster en cas de basculement.
- Aucune autre règle ne doit bloquer ces flux sur l'interface HA.

✅ Conclusion

La mise en place d'un **cluster pfSense en mode failover (CARP)** assure une **tolérance aux pannes** au niveau du pare-feu, un composant critique de l'infrastructure réseau.

Grâce à cette configuration, l'entreprise **Uranus** bénéficie désormais d'une solution **fiable, sécurisée et hautement disponible**, garantissant la **continuité de service** même en cas de défaillance du pare-feu principal.

Cette démarche s'inscrit dans une logique de **professionnalisation de l'infrastructure**, en anticipant les incidents et en renforçant la **résilience globale du système d'information**.