

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

```

*** Welcome to pfSense 2.7.0-RELEASE (amd64) on Routeur ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.1.168/24
LAN (lan)      -> em1      -> v4: 172.17.1.254/24
SRV (opt1)     -> em2      -> v4: 172.17.2.254/24
DMZ (opt2)     -> em3      -> v4: 172.17.3.254/24
HA (opt3)      -> em4      -> v4: 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

```

*** Welcome to pfSense 2.7.0-RELEASE (amd64) on routeur2 ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.1.136/24
LAN (lan)      -> em1      -> v4: 172.17.1.253/24
SRV (opt1)     -> em2      -> v4: 172.17.2.253/24
DMZ (opt2)     -> em3      -> v4: 172.17.3.253/24
HA (opt3)      -> em4      -> v4: 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 : 172.171.252 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 :

Modifier l'IP virtuelle

Type ☐ Alias IP ☒ CARP ☐ Mandataire (proxy) ARP ☐ Autre

Interface LAN

Type d'adresse Adresse unitaire

Adresse(s) 172.17.1.252 / 24
Le masque doit être le masque de sous-réseau du réseau. Il ne spécifie pas une plage CIDR.

Mot de passe d'IP virtuelle *****
Entrez le mot de passe du groupe VHID. Confirmer

Groupe VHID 1
Entrez le nom du groupe VHID qui sera partagé.

Fréquence d'annonce 1 0
Base Biais
La fréquence à laquelle cette machine effectue ses annonces. Autrement, la plus petite combinaison des valeurs de la grappe déterminera le maître.

Description ip virtuelle CARP
Une description peut être saisie ici à des fins de référence administrative (non analysée).

Enregistrer

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

Modifier l'IP virtuelle

Type ☐ Alias IP ☒ CARP ☐ Mandataire (proxy) ARP ☐ Autre

Interface LAN

Type d'adresse Adresse unitaire

Adresse(s) 172.17.1.252 / 24
Le masque doit être le masque de sous-réseau du réseau. Il ne spécifie pas une plage CIDR.

Mot de passe d'IP virtuelle *****
Entrez le mot de passe du groupe VHID. Confirmer

Groupe VHID 1
Entrez le nom du groupe VHID qui sera partagé.

Fréquence d'annonce 1 100
Base Biais
La fréquence à laquelle cette machine effectue ses annonces. Autrement, la plus petite combinaison des valeurs de la grappe déterminera le maître.

Description ip virtuelle CARP
Une description peut être saisie ici à des fins de référence administrative (non analysée).

Enregistrer

⚠ 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.

Pare-feu / IPs virtuels				
Adresse IP virtuelle				
Adresse IP virtuelle	Interface	Type	Description	Actions
172.17.1.252/24 (vhid: 1)	LAN	CARP	ip virtuelle CARP	 
172.17.2.252/24 (vhid: 2)	SRV	CARP	ip virtuelle CARP	 
172.17.3.252/24 (vhid: 3)	DMZ	CARP	ip virtuelle CARP	 
172.17.4.252/24 (vhid: 4)	HA	CARP	ip virtuelle CARP	 
				 Ajouter

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** :

État / CARP

CARP Maintenance

Désactiver temporairement CARP

Entrer en mode de maintenance CARP persistant

Statut CARP

Interface and Vhid	Adresse IP virtuelle	État
LAN@1	172.17.1.252/24	MASTER
SRV@2	172.17.2.252/24	MASTER
DMZ@3	172.17.3.252/24	MASTER
HA@4	172.17.4.252/24	MASTER

PfSense **slave**:

État / CARP

CARP Maintenance

Statut CARP

Interface and VHID	Adresse IP virtuelle	État
LAN@1	172.17.1.252/24	BACKUP
SRV@2	172.17.2.252/24	BACKUP
DMZ@3	172.17.3.252/24	BACKUP
HA@4	172.17.4.252/24	BACKUP

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

Statut > CARP (failover)

Clique sur le bouton :

CARP Maintenance

Statut CARP

Interface and VHID	Adresse IP virtuelle	État
LAN@1	172.17.1.252/24	DISABLED
SRV@2	172.17.2.252/24	DISABLED
DMZ@3	172.17.3.252/24	DISABLED
HA@4	172.17.4.252/24	DISABLED

Le pfSense **slave** passe en **master**:

CARP Maintenance

Statut CARP

Interface and VHID	Adresse IP virtuelle	État
LAN@1	172.17.1.252/24	MASTER
SRV@2	172.17.2.252/24	MASTER
DMZ@3	172.17.3.252/24	MASTER
HA@4	172.17.4.252/24	MASTER

Lorsque le CARP est réactivé sur le pfSense principal :

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

CARP Maintenance		
🛑 Désactiver temporairement CARP 🔑 Entrer en mode de maintenance CARP persistant		
Statut CARP		
Interface and VHID	Adresse IP virtuelle	État
LAN@1	172.17.1.252/24	🟢 MASTER
SRV@2	172.17.2.252/24	🟢 MASTER
DMZ@3	172.17.3.252/24	🟢 MASTER
HA@4	172.17.4.252/24	🟢 MASTER

- Le pfSense secondaire repasse en **BACKUP**

CARP Maintenance		
🛑 Désactiver temporairement CARP 🔑 Entrer en mode de maintenance CARP persistant		
Statut CARP		
Interface and VHID	Adresse IP virtuelle	État
LAN@1	172.17.1.252/24	🟡 BACKUP
SRV@2	172.17.2.252/24	🟡 BACKUP
DMZ@3	172.17.3.252/24	🟡 BACKUP
HA@4	172.17.4.252/24	🟡 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)

Système / High Availability 🔍 ?

Paramètres de synchronisation d'état (pfsync)

Etat de la synchronisation

☒ Messages de pfsync pour état d'insertion, transfert, et suppression entre firewalls.
 Chaque pare-feu envoie ces messages via multicast sur une interface spécifiée, en utilisant le protocole PFSYNC (protocole IP 240). Il écoute également cette interface pour des messages similaires provenant d'autres pare-feux et les importe dans la table d'état locale.
 Ce paramètre devrait être activé sur tous les membres d'un groupe de basculement.
 Cliquer sur "Enregistrer" forcera une synchronisation de configuration Si elle est activée! (Voir Paramètres de synchronisation de configuration ci-dessous)

Synchroniser l'interface

HA

▼

Si les états de synchronisation sont activés, cette interface sera utilisée pour la communication.
 Il est recommandé de configurer cette option sur une interface autre que LAN ! Une interface dédiée fonctionne le mieux.
 Une IP doit être définie sur chaque machine participant à ce groupe de basculement.
 Une IP doit être affecté à l'interface sur les nœuds de synchronisation participants.

Filter Host ID

8ef5b46b

Custom pf host identifier carried in state data to uniquely identify which host created a firewall state.
 Must be a non-zero hexadecimal string 8 characters or less (e.g. 1, 2, ff01, abcdef01).
 Each node participating in state synchronization must have a different ID.

IP de synchronisation pfsync du pair

172.17.4.253

Le réglage de cette option obligera Pfsync à synchroniser sa table d'état avec cette adresse IP. La sélection par défaut est multicast dirigé.

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

Paramètres de synchronisation de configuration (XMLRPC Sync)

Synchroniser la configuration avec IP

172.17.4.253

Entrez l'adresse IP du pare-feu à laquelle les sections de configuration sélectionnées doivent être synchronisées.

La synchronisation XMLRPC n'est actuellement prise en charge que sur les connexions utilisant le même protocole et le même port que ce système - assurez-vous que le port et le protocole du système distant sont définis en conséquence !
N'utilisez pas l'option Synchroniser la configuration sur IP et le mot de passe sur les membres du cluster de sauvegarde!

Nom d'utilisateur du système distant

admin

Entrez le nom d'utilisateur de WebConfigurator du système saisi ci-dessus pour la synchronisation de la configuration.

N'utilisez pas l'option Synchroniser la configuration sur IP et le nom d'utilisateur sur les membres du cluster de sauvegarde !

Mot de passe du système distant

Entrez le mot de passe du système de configuration Internet configuré ci-dessus pour la synchronisation de la configuration.

N'utilisez pas l'option Synchroniser la configuration sur IP et mot de passe sur les membres du cluster de sauvegarde !

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.

Sélectionnez les options à synchronizer

☒ Gestion d'utilisateurs: Utilisateurs et Groupes
☒ Serveurs d'authentification (e.g LDAP, RADIUS)
☒ Listes des Autorités de Certification, Certificats, et Certificats de Révocation
☒ Règles du Pare-feu
☒ Planifications du Pare-feu
☒ alias du Pare-feu
☒ Configuration NAT
☒ Configuration IPsec
☒ OpenVPN configuration (Implies CA/Cert/CRL Sync)
☒ Paramètres du serveur DHCP
☒ DHCP Relay settings
☒ DHCPv6 Relay settings
☒ Paramètres du serveur WoL
☒ Configuration des routes statiques
☒ Adresses IP virtuel
☒ Configuration du régulateur de flux
☒ Configuration des limitations du régulation du trafic
☒ Configurations du DNS Forwarder et du DNS Resolver
☒ Portail captif
☒ Toggle All

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)

Flottant(e)

WAN

LAN

SRV

DMZ

HA

Règles (Faire glisser pour changer l'ordre)

☐	États	Protocole	Source	Port	Destination	Port	Passerelle	File d'attente	Ordonnancement	Description	Actions
☐	✓	0/0 B	IPv4 PFSYNC	HA net	*	Ce pare-feu	*	*	aucun	Synchronisation des états (pfsync)	   
☐	✓	0/0 B	IPv4 TCP	HA net	*	Ce pare-feu	443 (HTTPS)	*	aucun	Autoriser XMLRPC	   

 Ajouter

 Ajouter

 Supprimer

 Toggle

 Copier

 Enregistrer

 Séparateur

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**.