Date de création	27 Avril 2026
Date de dernière mise à jour	27 Avril 2026
Auteur(s)	LALIGANT Pierre-Louis
Matière (E5-E6-E7-AP)	E6 - Solutions d'infrastructure, systèmes et réseaux
Compétence(s) validée(s)	Vérifier les conditions de la continuité d'un service informatique

REDONDANCE PARE-FEU

Dynfi

SOMMAIRE

1. Introduction

1.1 Contexte ou cahier des charges

Dans le cadre de la continuité de service de notre infrastructure, nous mettons en place une redondance de pare-feu via Dynfi afin qu'en cas de panne d'un firewall, le second prenne automatiquement le relais sans interruption de service

1.2 Ressources

- Deux machines (physiques ou virtuelles) avec Dynfi installé
- Un accès console/réseau aux deux machines
- Une IP virtuelle (VIP) partagée entre les deux firewalls
- Les deux interfaces WAN et LAN configurées

1.3 Définitions

Haute disponibilité (HA) : *Architecture réseau garantissant la continuité de service en cas de défaillance d'un équipement. Un second équipement identique prend automatiquement le relais sans interruption perceptible pour les utilisateurs.*

IP Virtuelle : *Adresse IP partagée entre les deux pare-feux. Elle est portée par le nœud actif (master) et bascule automatiquement vers le nœud secondaire (backup) en cas de panne. Les postes du réseau utilisent toujours cette même IP, quelle que soit la machine physiquement active.*

Failover : *Mécanisme automatique de basculement depuis un équipement défaillant vers un équipement de secours, afin de maintenir la continuité de service sans intervention humaine.*

Dynfi : *Solution open-source de gestion et supervision de pare-feux basée sur OPNsense/FreeBSD. Elle permet de gérer centralement plusieurs firewalls via une interface web unifiée, avec des fonctions de filtrage, NAT, VPN et haute disponibilité*

2. Installation

La redondance de pare-feu sur Dynfi repose sur le protocole CARP (Common Address Redundancy Protocol), qui permet de partager une IP virtuelle entre deux nœuds. Le nœud master (priorité 0) porte l'IP virtuelle ; si il tombe, le nœud backup (priorité 100) la prend automatiquement.

2.1 Prérequis

Les deux pare-feux Dynfi doivent être installés, accessibles et avoir la même configuration réseau de base (interfaces WAN/LAN identiques). Prévoir idéalement une interface réseau dédiée à la synchronisation d'état entre les deux nœuds (interface pfsync).

2.2 Créer l'IP Virtuelle CARP (sur le nœud principal)

Aller dans Interfaces > IP Virtuelles > Ajouter et renseigner :

- Type : CARP
- Interface : LAN (répéter ensuite pour WAN)
- Adresse IP : l'IP virtuelle choisie (ex : 192.168.1.254/24)
- Mot de passe CARP : un mot de passe (identique sur les deux nœuds)
- VHID : 1 (identifiant unique du groupe CARP)
- Fréquence : Base 1 — Skew 0 (= master)

Cliquer sur Sauvegarder puis Appliquer.
Sur le nœud secondaire, effectuer la même configuration avec uniquement le Skew à 100 (= backup).

2.3 Configurer la synchronisation d'état (pfsync)

Sur les deux nœuds, aller dans Système > Haute Disponibilité > Paramètres :

- Cocher Activer la synchronisation d'état
- Interface de synchronisation : sélectionner l'interface dédiée au lien entre les deux pare-feux
- IP du pair de synchronisation : saisir l'IP de l'autre nœud sur cette interface

Cliquer sur Sauvegarder.

2.4 Synchroniser la configuration

Toujours dans Système > Haute Disponibilité, aller dans l'onglet Synchronisation de la configuration :

- Renseigner l'IP du nœud secondaire ainsi que ses identifiants admin
- Cocher les éléments à synchroniser : Règles de filtrage, NAT, DHCP, Certificats, etc.

Cliquer sur Sauvegarder.

NOTE : Toutes les modifications de configuration doivent toujours être effectuées sur le nœud master. La synchronisation les pousse automatiquement vers le backup.

ATTENTION : Le mot de passe CARP doit être strictement identique sur les deux nœuds, sinon le basculement ne fonctionnera pas.

2.5 Vérifier l'état CARP

Sur le tableau de bord Dynfi du nœud master, l'IP virtuelle doit afficher l'état MASTER. Sur le nœud backup, elle doit afficher BACKUP. Pour tester, éteindre le nœud master : l'IP virtuelle doit basculer sur le backup en quelques secondes.

3. Utilisation

3.1 Administrateur

L'administrateur accède à l'interface web de chaque nœud Dynfi pour surveiller l'état de la haute disponibilité. Il peut consulter l'état CARP de chaque IP virtuelle (MASTER / BACKUP / INIT) depuis le tableau de bord. En cas de maintenance planifiée, il peut forcer manuellement le basculement en modifiant temporairement le Skew du nœud master à une valeur supérieure à 100. Il est également chargé de vérifier régulièrement que la synchronisation de configuration est bien active et que les deux nœuds ont bien les mêmes règles.

3.2 Utilisateur

L'utilisateur ne perçoit pas la redondance. En cas de panne du pare-feu principal, le basculement vers le nœud backup est automatique et transparent : la connexion réseau est maintenue sans action de sa part. Il continue d'utiliser les ressources réseau normalement.

4. Maintenance et dépannage

Si l'IP virtuelle ne bascule pas en cas de panne du master :

- Vérifier que le mot de passe CARP est identique sur les deux nœuds
- Vérifier que les deux nœuds sont bien sur le même réseau et que le trafic CARP (protocole IP 112) n'est pas bloqué

Si la synchronisation de configuration ne fonctionne pas :

- Vérifier que les identifiants admin du nœud secondaire sont corrects dans les paramètres de synchronisation
- Vérifier la connectivité réseau entre les deux nœuds sur l'interface de synchronisation

Si le nœud backup reste en état INIT et non BACKUP :

- Vérifier que le service CARP est bien activé sur les deux nœuds
- Relancer les interfaces concernées

Pour vérifier manuellement l'état CARP via la console :

```
ifconfig | grep carp
```

5. Sources utilisées

Documentation officielle Dynfi
Lien : https://dynfi.com/documentation/

Documentation OPNsense — Haute disponibilité / CARP
Lien : https://docs.opnsense.org/manual/hacarp.html

IT-Connect — Mettre en place la haute disponibilité sur OPNsense
Lien : https://www.it-connect.fr/