



# MISSION 1 - Mise en place CARP sur OPNsense

SIO2 - BLOC 2 SISR

**PETKOVIC Téo**
**SIO2**

# Compte rendu de mission — Mise en place de CARP sur OPNsense

## Sommaire



---

## 1. Contexte de la mission

La mission consiste à mettre en place la **haute disponibilité des passerelles réseau** sur l'infrastructure OPNsense GSB72 à l'aide de **CARP**.

L'infrastructure est composée de plusieurs firewalls OPNsense :

1. **PF-Externe** ;
2. **PF-Intermédiaire** ;
3. **PF-Interne** ;
4. **PF-Admin**.

Chaque firewall fonctionne en paire haute disponibilité avec un nœud **master** et un nœud **backup**. L'objectif est que les réseaux continuent de fonctionner même si le firewall master tombe.

---

## 2. Objectif de la mise en place CARP

L'objectif principal de CARP est de fournir une **adresse IP virtuelle stable** aux équipements des différents réseaux.

Sans CARP, les clients utilisent directement l'adresse IP physique d'un firewall comme passerelle. En cas de panne de ce firewall, la passerelle devient indisponible.

Avec CARP, les clients utilisent une **VIP CARP** comme passerelle. Cette VIP est portée par le master en fonctionnement normal. Si le master devient indisponible, le backup reprend automatiquement la VIP.

Exemple :

Client VLAN Service IT
Passerelle : 192.168.10.254

PF-Interne master : 192.168.10.252
VIP CARP : 192.168.10.254

Le client ne connaît que la VIP. Il n'a pas besoin de savoir quel firewall est master.

---

## 3. Principe de fonctionnement de CARP

CARP signifie **Common Address Redundancy Protocol**.

Son rôle est de permettre à plusieurs firewalls de partager une même adresse IP virtuelle.

Dans une paire HA :

Firewall master -> porte la VIP CARP
Firewall backup -> surveille le master

En fonctionnement normal :

VIP active sur le master

En cas de panne du master :

le backup devient master
le backup récupère la VIP
les clients gardent la même passerelle

CARP utilise le protocole IP 112 et communique vers l'adresse multicast :

224.0.0.18

Il est donc nécessaire d'autoriser le protocole CARP sur chaque interface qui possède une VIP CARP.

---

## 4. Pré-requis pour le cluster CARP

Pour que CARP fonctionne correctement, les conditions suivantes doivent être respectées :

1. les deux firewalls d'une même paire doivent avoir les mêmes interfaces ;
2. les interfaces correspondantes doivent être connectées au même réseau L2 ;
3. chaque interface physique doit avoir sa propre IP ;
4. la VIP CARP doit être dans le même sous-réseau que les IP physiques ;
5. les règles firewall doivent autoriser CARP ;
6. les clients doivent utiliser la VIP comme passerelle, pas l'IP physique du firewall.

Exemple :

Master : 172.19.4.253/24
Backup : 172.19.4.252/24
VIP : 172.19.4.254/24

La VIP .254 devient la passerelle du réseau.

---

## 5. Table d'adressage CARP par firewall

### 5.1 PF-Externe

| Interface | Réseau | IP master | VIP CARP | Rôle de la VIP |
|---|---|---|---|---|
| LAN | 172.19.4.0/24 | 172.19.4.253 | 172.19.4.254 | Passerelle DMZ reverse proxy / transit |
| OPT1 | 172.20.1.0/24 | 172.20.1.240 | 172.20.1.254 | Accès admin/transit vers PF-Externe |

Interfaces concernées par CARP sur PF-Externe :

LAN
OPT1

## 5.2 PF-Intermédiaire

| Interface | Réseau | IP master | VIP CARP | Rôle de la VIP |
|---|---|---|---|---|
| WAN | 172.19.4.0/24 | 172.19.4.2 | 172.19.4.1 | Passerelle amont côté DMZ transit |
| LAN | 172.19.2.0/24 | 172.19.2.253 | 172.19.2.254 | Passerelle vers PF-Interne |
| OPT1 | 172.19.3.0/24 | 172.19.3.250 | 172.19.3.254 | Passerelle DMZ services exposés |
| OPT2 | 172.20.1.0/24 | 172.20.1.242 | 172.20.1.253 | Accès admin/transit vers PF-Intermédiaire |

Interfaces concernées par CARP sur PF-Intermédiaire :

WAN
LAN
OPT1
OPT2

---

## 5.3 PF-Interne

| Interface | Réseau | IP master | VIP CARP | Rôle de la VIP |
|---|---|---|---|---|
| WAN | 172.19.2.0/24 | 172.19.2.2 | 172.19.2.1 | Passerelle côté transit interne |
| OPT1 | 172.19.1.0/24 | 172.19.1.249 | 172.19.1.254 | Passerelle services internes |
| OPT3 | 192.168.10.0/24 | 192.168.10.252 | 192.168.10.254 | Passerelle VLAN Service IT |

| Interface | Réseau | IP master | VIP CARP | Rôle de la VIP |
|---|---|---|---|---|
| OPT4 | 192.168.20.0/24 | 192.168.20.252 | 192.168.20.254 | Passerelle VLAN Direction |
| OPT5 | 192.168.30.0/24 | 192.168.30.252 | 192.168.30.254 | Passerelle VLAN Administratif |
| OPT6 | 172.17.127.0/17 | 172.17.127.249 | 172.17.127.254 | Passerelle zone serveurs |
| OPT7 | 192.168.40.0/24 | 192.168.40.252 | 192.168.40.254 | Passerelle VLAN Communications |

Interfaces concernées par CARP sur PF-Interne :

WAN
OPT1
OPT3
OPT4
OPT5
OPT6
OPT7

Le réseau 192.168.1.0/24 n'est pas utilisé pour CARP.

---

### 5.4 PF-Admin

| Interface | Réseau | IP master | VIP CARP | Rôle de la VIP |
|---|---|---|---|---|
| WAN | 172.20.1.0/24 | 172.20.1.2 | 172.20.1.1 | VIP admin/transit |
| LAN | 172.20.2.0/24 | 172.20.2.253 | 172.20.2.254 | Passerelle réseau administration |
| OPT1 | 172.20.3.0/24 | 172.20.3.253 | 172.20.3.254 | Passerelle supervision |

| Interface | Réseau | IP master | VIP CARP | Rôle de la VIP |
|---|---|---|---|---|
| OPT2 | 172.17.127.0/17 | 172.17.127.252 | 172.17.127.253 | Administration zone serveurs |
| OPT3 | 172.19.3.0/24 | 172.19.3.252 | 172.19.3.253 | Administration DMZ services |
| OPT4 | 172.19.1.0/24 | 172.19.1.252 | 172.19.1.253 | Administration services internes |

Interfaces concernées par CARP sur PF-Admin :

WAN
LAN
OPT1
OPT2
OPT3
OPT4

---

## 6. Interfaces concernées par CARP

Récapitulatif des interfaces où une règle CARP doit être présente :

| Firewall | Interfaces avec VIP CARP |
|---|---|
| PF-Externe | LAN, OPT1 |
| PF-Intermédiaire | WAN, LAN, OPT1, OPT2 |
| PF-Interne | WAN, OPT1, OPT3, OPT4, OPT5, OPT6, OPT7 |
| PF-Admin | WAN, LAN, OPT1, OPT2, OPT3, OPT4 |

Les interfaces pfsync ne sont pas concernées par CARP.

---

## 7. Règles firewall nécessaires pour CARP

Sur chaque interface qui possède une VIP CARP, il faut autoriser le protocole CARP.

Règle type :

Action : Pass
Interface : interface concernée
Protocol : CARP

Source : any
Destination : 224.0.0.18
Description : Allow CARP

Cette règle doit être placée avant d'éventuelles règles de blocage générales.

Exemple pour PF-Intermédiaire :

WAN : PASS CARP -> 224.0.0.18
LAN : PASS CARP -> 224.0.0.18
OPT1 : PASS CARP -> 224.0.0.18
OPT2 : PASS CARP -> 224.0.0.18

Sans cette règle, les annonces CARP peuvent être bloquées et le basculement master/backup ne fonctionnera pas correctement.

---

## 8. Logique de bascule master/backup

Chaque paire de firewalls fonctionne selon le même principe :

Master actif : porte les VIP CARP
Backup passif : surveille les annonces CARP

En cas de panne du master :

1. Le backup ne reçoit plus les annonces CARP du master.
2. Le backup devient master.
3. Le backup récupère les VIP CARP.
4. Les clients continuent d'utiliser la même passerelle.

Exemple sur un VLAN interne :

Avant panne :
PF-Interne master porte 192.168.10.254

Après panne :
PF-Interne backup récupère 192.168.10.254

Côté client :
la passerelle reste 192.168.10.254

La bascule est donc transparente pour les équipements du réseau.

---

## 9. Vérifications à effectuer

Après la configuration CARP, plusieurs vérifications sont nécessaires.

### 9.1 Vérifier l'état des VIP

Dans OPNsense :

Interfaces > Virtual IPs > Status

Le master doit afficher les VIP en état actif.

Le backup doit afficher les VIP en état backup.

### 9.2 Vérifier les annonces CARP

Les règles firewall doivent autoriser le protocole CARP vers :

224.0.0.18

Sur chaque interface avec VIP, la règle CARP doit être présente.

### 9.3 Vérifier la passerelle des clients

Les clients ne doivent pas utiliser l'adresse physique d'un firewall.

Ils doivent utiliser la VIP CARP.

Exemples :

VLAN Service IT -> passerelle 192.168.10.254
VLAN Direction -> passerelle 192.168.20.254
DMZ services exposés -> passerelle 172.19.3.254
Services internes -> passerelle 172.19.1.254
Réseau admin -> passerelle 172.20.2.254

### 9.4 Tester une bascule

Pour tester le fonctionnement :

1. Vérifier que le master porte les VIP.
2. Désactiver temporairement l'interface CARP ou arrêter le master.
3. Vérifier que le backup devient master.
4. Vérifier que les VIP sont reprises.
5. Tester un ping vers les passerelles VIP.
6. Remettre le master en service.

---

## 10. Résultat attendu

Après mise en place de CARP, les réseaux doivent utiliser les VIP comme passerelles.

Le résultat attendu est le suivant :

1. les VIP CARP sont actives sur les firewalls master ;
2. les firewalls backup sont prêts à reprendre les VIP ;
3. les clients utilisent les VIP comme passerelles ;

4. une panne du master ne change pas l'adresse de passerelle des clients ;

5. la continuité de service est assurée au niveau des passerelles.

---

## 11. Conclusion

La mise en place de CARP permet d'apporter de la haute disponibilité aux firewalls OPNsense de l'infrastructure GSB72.

Les VIP CARP deviennent les adresses de référence pour les passerelles des différents réseaux. Les adresses physiques des firewalls servent uniquement aux équipements master et backup, tandis que les clients utilisent les VIP.

La configuration permet donc de garantir que, si un firewall master tombe, son backup peut reprendre automatiquement les VIP et maintenir la connectivité réseau.

La mission CARP est validée lorsque :

- toutes les VIP sont configurées ;
- les interfaces avec VIP autorisent le protocole CARP ;
- les clients utilisent les VIP comme passerelles ;
- le basculement master/backup fonctionne correctement.