Projet 2 — Tolérance de panne avec Packet Filter

Administration Réseaux — Master 1 Computer Network Systems (CNS SR)
Université Paris-Saclay (Évry) | Encadrant : M. Petit | Étudiant : DIALLO Boubacar | N° 20244035

Introduction

Ce rapport présente la mise en place d'une architecture réseau redondante basée sur le pare-feu Packet Filter (PF) d'OpenBSD. L'objectif est de garantir la continuité de service en cas de défaillance d'un routeur, grâce aux mécanismes CARP (Common Address Redundancy Protocol) et pfsync.

L'architecture repose sur deux routeurs pare-feux (PF1 et PF2) configurés en mode maître/secours, et deux machines clientes (AT et BT) situées sur des réseaux distincts.

I. Mise en place du réseau — Description de la maquette

1.1 Plan d'adressage

Le réseau de test est organisé selon le schéma suivant :

- Machine AT — Réseau 192.168.10.0/24, adresse : 192.168.10.2, passerelle virtuelle CARP : 192.168.10.254
- Machine BT — Réseau 192.168.20.0/24, adresse : 192.168.20.2, passerelle virtuelle CARP : 192.168.20.254
- PF1 (maître) — em0 : 192.168.10.1 / em1 : 192.168.20.1 / em2 : 192.168.30.1 (synchronisation)
- PF2 (secours) — em0 : 192.168.10.3 / em1 : 192.168.20.3 / em2 : 192.168.30.3

> *Les passerelles par défaut des machines AT et BT correspondent aux adresses IP virtuelles CARP, ce qui leur permet de rester joignables quel que soit le routeur actif.*

1.2 Configuration des machines clientes

Machine AT

L'adaptateur réseau de la machine AT est configuré en mode « Host-only ». L'attribution d'adresse IP dynamique (DHCP) est désactivée au profit d'une configuration statique dans le fichier /etc/network/interfaces :

```
auto ens33
iface ens33 inet static
    address 192.168.10.2/24
    gateway 192.168.10.254
```

Machine BT

La procédure est identique pour la machine BT, avec une adresse IP différente adaptée à son réseau :

```
auto ens33
iface ens33 inet static
    address 192.168.20.2/24
    gateway 192.168.20.254
```

II. Configuration des routeurs en mode failover (tolérance de panne)

2.1 Configuration de PF1 — Routeur maître

Les interfaces réseau des routeurs PF1 et PF2 sont placées en mode « LAN Segment » afin d'isoler le réseau virtuel de test. PF1 est équipé de trois interfaces réseau physiques :

- em0 — connectée au réseau 192.168.10.0/24
- em1 — connectée au réseau 192.168.20.0/24
- em2 — dédiée à la synchronisation pfsync sur le réseau 192.168.30.0/24

Configuration des interfaces physiques

Chaque interface est configurée via son fichier de définition dans /etc/hostname.<interface> :

```
# /etc/hostname.em0
inet 192.168.10.1 255.255.255.0

# /etc/hostname.em1
inet 192.168.20.1 255.255.255.0

# /etc/hostname.em2
inet 192.168.30.1 255.255.255.0
```

Configuration des interfaces CARP

Le protocole CARP permet de partager une adresse IP virtuelle entre plusieurs hôtes. La machine qui détient cette adresse est dite « maître » ; les autres sont en mode « secours ». En cas de défaillance du maître, l'un des routeurs de secours prend automatiquement le relais.

PF1 est configuré comme maître grâce à une valeur advskew faible (100 < 200). Plus advskew est élevé, plus la priorité de l'interface est basse.

```
# /etc/hostname.carp1  (passerelle virtuelle réseau AT)
inet 192.168.10.254/24 NONE vhid 1 carpdev em0 pass 123 advskew 100

# /etc/hostname.carp2  (passerelle virtuelle réseau BT)
inet 192.168.20.254/24 NONE vhid 2 carpdev em1 pass 123 advskew 100
```

Détail des paramètres CARP :

- inet 192.168.x.254/24 — adresse IP virtuelle partagée et son masque de sous-réseau
- NONE — pas d'adresse de diffusion (broadcast) explicite
- vhid — identifiant unique du groupe CARP (doit être identique sur les deux routeurs)

- carpdev — interface physique sous-jacente utilisée pour les annonces
- pass — mot de passe d'authentification (empêche l'usurpation de l'interface CARP)
- advskew — priorité relative : valeur plus faible = priorité plus haute = maître

Interface de synchronisation pfsync

L'interface pfsync permet de synchroniser les tables d'états du pare-feu entre PF1 et PF2. Ainsi, lors d'un basculement, PF2 dispose déjà des sessions actives et peut les maintenir sans interruption pour les utilisateurs.

```
# /etc/hostname.pfsync0
up syncdev em2
```

Activation du routage et de la préemption CARP

Le fichier /etc/sysctl.conf est modifié pour activer le transfert de paquets IP (routage) et permettre à PF1 de reprendre automatiquement son rôle de maître dès qu'il revient en ligne après une panne :

```
net.inet.ip.forwarding=1
net.inet.carp.preempt=1
```

Règles de filtrage — /etc/pf.conf

Le fichier de configuration de Packet Filter doit autoriser explicitement les protocoles CARP et pfsync, sans quoi les annonces de redondance et la synchronisation seraient bloquées :

```
lan = "em0"
wan = "em1"
carpwan = "carp1"

set skip on lo0
set block-policy drop

pass proto carp keep state
pass proto pfsync keep state

pass in on $lan from $lan:network to any keep state
pass out on $wan from $wan:network to any keep state
```

2.2 Configuration de PF2 — Routeur secours

La configuration de PF2 est identique à celle de PF1, à deux différences près :

- Les adresses IP physiques sont différentes : em0 → 192.168.10.3, em1 → 192.168.20.3, em2 → 192.168.30.3.
- La valeur advskew est fixée à 200 (supérieure à 100), ce qui place PF2 en position de secours.

> *Après démarrage, la commande ifconfig confirme que les interfaces CARP de PF1 ont le statut MASTER et celles de PF2 ont le statut BACKUP.*

III. Vérification de la connectivité réseau

3.1 Tests ICMP entre les machines

Des requêtes ping sont effectuées depuis AT vers toutes les interfaces de PF1, puis de PF2, afin de valider la configuration réseau et le routage.

Résultats observés :

- AT → PF1 (192.168.10.1, 192.168.20.1, 192.168.30.1) : 0 % de perte de paquets.
- AT → PF2 (192.168.10.3, 192.168.20.3, 192.168.30.3) : 0 % de perte de paquets.
- AT → BT (192.168.20.2) : communication inter-réseau fonctionnelle, le routage est opérationnel.
- BT → AT : la communication inverse fonctionne également, aucune règle de filtrage ne l'interdisant dans /etc/pf.conf.

IV. Test de la redondance et analyse des trames

4.1 Scénarios de basculement (failover)

Un ping continu est maintenu depuis AT vers BT. Un traceroute permet de vérifier par quel routeur transitent les paquets.

Scénario 1 — Fonctionnement normal

Le traceroute confirme que les paquets passent par PF1 (192.168.10.1), le routeur maître.

Scénario 2 — Panne simulée du maître

L'interface em0 de PF1 est désactivée manuellement :

```
bsd# ifconfig em0 down
```

PF2 prend automatiquement le relais (basculement). Le traceroute suivant montre que les paquets transitent désormais par PF2 (192.168.10.3). Le ping n'est pas interrompu.

Scénario 3 — Retour du maître

L'interface de PF1 est réactivée :

```
bsd# ifconfig em0 up
```

Grâce au paramètre net.inet.carp.preempt=1, PF1 reprend automatiquement son rôle de maître. Le traceroute confirme le retour du trafic via PF1 (192.168.10.1).

> *Les trois scénarios sont validés par traceroute : maître → basculement sur PF2 → retour sur PF1.*

4.2 Analyse du protocole CARP avec tcpdump

La commande suivante capture les annonces CARP émises par PF1 sur l'interface em0 :

```
bsd# tcpdump -i em0 proto carp
```

Chaque ligne de capture correspond à une annonce CARP émise toutes les secondes (intervalle par défaut). Exemple d'entrée :

```
04:12:25.702599 CARPv2-advertise 36: vhid=1 advbase=1 advskew=100 demote=0
(DF) [tos 0x10]
```

Explication des champs :

- 04:12:25.702599 — horodatage précis de la capture. L'intervalle d'une seconde est bien observable.
- CARPv2-advertise — annonce CARP signalant que ce routeur est actif et disponible.
- vhid=1 — identifiant du groupe CARP concerné.
- advskew=100 — priorité de l'interface. La valeur 100 (inférieure à 200) confirme le statut de maître.
- demote=0 — l'interface n'est pas dégradée. Cette valeur augmente si des problèmes de performance sont détectés.
- tos 0x10 — drapeau indiquant que le paquet ne doit pas être fragmenté, ce qui est typique des annonces CARP devant être transmises de manière continue et immédiate.

Sur PF2, les mêmes annonces sont visibles, avec advskew=200, confirmant son rôle de secours.

Concernant les adresses IP : lorsque PF1 est maître, l'adresse source des annonces CARP est 192.168.10.1 (em0 de PF1). Après basculement, elle devient 192.168.10.3 (em0 de PF2). L'adresse de destination est toujours l'adresse multicast 224.0.0.18, utilisée par CARP pour annoncer l'état du maître à l'ensemble du segment réseau.

> *L'adresse MAC virtuelle associée à l'interface CARP ne change pas lors du basculement, ce qui garantit la transparence du mécanisme pour les machines clientes.*

> *CARP utilise un TTL de 255 pour s'assurer que les annonces ne traversent pas les routeurs et restent confinées au segment réseau local, limitant ainsi les risques de sécurité.*

4.3 Vérification de la synchronisation des états — pfsync

Le protocole pfsync synchronise en temps réel les tables d'états des connexions entre PF1 et PF2. Cela garantit qu'en cas de basculement, les sessions TCP et UDP actives sont maintenues sans interruption.

La commande pfctl -ss permet d'afficher les tables d'états. Avant le basculement, les tables de PF1 et PF2 contiennent les mêmes entrées, ce qui confirme la synchronisation. Après le basculement, PF2 reprend l'ensemble des états et le nombre d'entrées augmente, reflétant les nouvelles connexions prises en charge.

Un test pratique avec SSH illustre cette continuité : même en coupant PF1 pendant une session SSH active, la connexion n'est pas interrompue car PF2 dispose déjà de l'état de la session.

La commande systat pf permet également de visualiser le trafic en temps réel et de comparer le nombre d'états avant et après le basculement. Le nombre d'états est quasi identique sur les deux routeurs, ce qui confirme l'efficacité de la synchronisation pfsync.

4.4 Vérification dans les journaux système

La commande tail -f /var/log/messages permet d'observer en temps réel les transitions d'état CARP :

- Lors de la panne de PF1 : passage de MASTER → BACKUP sur PF1, et de BACKUP → MASTER sur PF2.
- Lors du retour de PF1 : passage de BACKUP → MASTER sur PF1, et de MASTER → BACKUP sur PF2.

> *Ces transitions confirment que la préemption est bien active et que PF1 reprend automatiquement son rôle de maître dès qu'il est à nouveau disponible.*

Conclusion

Ce projet a permis de mettre en œuvre une architecture réseau hautement disponible basée sur les technologies OpenBSD, CARP et pfsync. Les résultats démontrent que :

- Le mécanisme CARP assure la continuité de service en cas de panne d'un routeur grâce à la gestion automatique des rôles maître et secours.
- Le protocole pfsync garantit la synchronisation des tables d'états entre les deux pare-feux, permettant le maintien des sessions actives sans interruption perceptible pour les utilisateurs.
- La préemption (net.inet.carp.preempt=1) permet au routeur maître de reprendre automatiquement sa place dès son retour en ligne.
- L'ensemble du mécanisme est transparent pour les machines clientes, qui conservent la même passerelle virtuelle (adresse CARP) en permanence.

Cette infrastructure constitue une base solide pour des environnements de production exigeant une haute disponibilité, comme les datacenters ou les systèmes d'information critiques d'entreprise.