

Problème de configuration de deux cartes réseau sur différents sous-réseaux

Table of Contents

[Problèmes](#)
[Résolution](#)
[Cause première](#)
[Options de rp_filter](#)
[Diagnostic](#)

Lorsque RHEL a plusieurs adresses IP configurées, une seule est accessible à partir d'un réseau distant

Problèmes

- RHEL ignore les paquets lorsque la route du trafic sortant diffère de la route du trafic entrant
- Red Hat Enterprise Linux 6 invalide/supprime les paquets lorsque la route du trafic sortant diffère de la route du trafic entrant
- Red Hat Enterprise Linux ne répond pas aux tentatives de connexion à une seconde carte réseau
- Un serveur ne peut pas recevoir de ping si `net.ipv4.conf.all.rp_filter` est défini sur le serveur
- On a un serveur avec 2 interfaces réseau et on a configuré les deux cartes réseau sur 2 sous-réseaux différents. Les postes de travail avec une seule carte réseau peuvent communiquer avec le serveur sur le réseau partagé, mais pas sur l'autre réseau.
- Lorsqu'on attribue une adresse IP à une nouvelle interface réseau, le système cesse de communiquer

Résolution

Définir la valeur du paramètre ajustable du noyau `net.ipv4.conf.all.rp_filter` sur 2 :

```
sysctl -w net.ipv4.conf.all.rp_filter=2
```

Pour rendre cette modification persistante lors des redémarrages, ajouter le paramètre réglable au fichier `/etc/sysctl.conf`.

Cause première

RHEL 6 et supérieur sont configurés par défaut pour appliquer le filtrage Strict Reverse Path Forwarding recommandé dans RFC 3704 - Ingress Filtering for Multihomed Networks.

Le filtrage strict signifie que lorsqu'un paquet arrive sur le système, le noyau prend l'adresse IP source du paquet et effectue une recherche dans sa table de routage pour voir si l'interface sur

laquelle le paquet est arrivé est la même interface que le noyau utiliserait pour envoyer un paquet. à cette IP. Si les interfaces sont identiques, le paquet a réussi le test de filtrage strict et il est traité normalement. Si les interfaces ne sont pas les mêmes, le paquet est rejeté sans autre traitement et dans RHEL 7+, le compteur IPReversePathFilter est incrémenté.

L'effet principal d'un filtrage strict est que pour une IP distante donnée, le système ne communiquera avec elle que via une interface spécifique. Configurez des routes statiques pour contrôler quelle interface répond à une adresse IP ou à un réseau distant donné.

La méthode de filtrage est contrôlée globalement par le `sysctl net.ipv4.conf.all.rp_filter` décrit dans la documentation du noyau : <https://www.kernel.org/doc/Documentation/networking/ip-sysctl.txt>. RHEL 6+ remplace la valeur par défaut du noyau de 0 (désactivé) pour ce paramètre et la définit sur 1 (strict).

Options de `rp_filter`

- **0** - Aucune validation de source.
- **1** - Mode strict tel que défini dans RFC3704 Strict: Reverse Path Chaque paquet entrant est testé par rapport au FIB et si l'interface n'est pas le meilleur chemin inverse, la vérification des paquets échouera. Par défaut, les paquets ayant échoué sont ignorés.
- **2** - Mode libre tel que défini dans RFC3704 Loose Reverse Path: L'adresse source de chaque paquet entrant est également testée par rapport au FIB et si l'adresse source n'est accessible via aucune interface la vérification des paquets échouera.

La pratique actuellement recommandée dans la RFC3704 consiste à activer le mode strict pour empêcher l'usurpation d'adresse IP par les attaques DDos. Si vous utilisez un routage asymétrique ou tout autre routage compliqué, le mode lâche est recommandé.

La valeur maximale de `conf/{all,interface}/rp_filter` est utilisée lors de la validation de la source sur l'`{interface}`.

La valeur par défaut est 0. Notez que certaines distributions l'activent dans les scripts de démarrage.

Le moyen le plus simple de désactiver la vérification stricte consiste à définir le `sysctl net.ipv4.conf.all.rp_filter` sur 2 (lâche) car cela remplacera les paramètres spécifiques à l'interface. Définir **`net.ipv4.conf.all.rp_filter`** sur 0 (désactivé) ne remplace pas les paramètres spécifiques à l'interface, il n'est donc pas recommandé.



Sans la vérification stricte, le système peut répondre à un paquet via une interface différente de celle sur laquelle il est arrivé. Que cela se traduise par la connectivité attendue dépend de nombreux facteurs externes au système, tels que la topologie du réseau physique et les politiques de pare-feu.

Une autre façon de configurer un système pour qu'il fonctionne avec **`rp_filter`** en mode strict consiste à configurer un routage basé sur une politique.





Dans RHEL 5 et versions antérieures, le noyau ne prenait pas en charge le filtrage strict. Ainsi, dans ces anciennes versions, le paramètre **net.ipv4.conf.all.rp_filter** n'a que deux valeurs possibles, 0 (désactivé) et 1 (libre). La valeur par défaut est 1 (libre).

Diagnostiques

Vérifier la valeur des **sysctls rp_filter**:

```
sysctl -a 2>/dev/null | grep "\.rp_filter"

net.ipv4.conf.all.rp_filter = 1
net.ipv4.conf.default.rp_filter = 0
net.ipv4.conf.enp0s31f6.rp_filter = 0
net.ipv4.conf.lo.rp_filter = 0
net.ipv4.conf.tun0.rp_filter = 0
net.ipv4.conf.virbr0.rp_filter = 0
net.ipv4.conf.virbr0-nic.rp_filter = 0
net.ipv4.conf.virbr1.rp_filter = 0
net.ipv4.conf.virbr1-nic.rp_filter = 0
net.ipv4.conf.wlp58s0.rp_filter = 0
```

Pour RHEL 7 et versions ultérieures, vérifier le compteur **SNMP IPReversePathFilter**. Si des paquets sont ignorés en raison d'un filtrage strict, ce compteur s'incrémentera à chaque fois que cela se produit :

```
nstat-rsz | grep IPReversePathFilter

TcpExtIPReversePathFilter 52537 0.0
```

```
netstat -s | grep IPReversePathFilter

IPReversePathFilter : 52537
```

Pour une adresse IP distante donnée dont les paquets semblent être ignorés par le système, effectuer une recherche de route pour voir quelle interface le système utilisera pour atteindre cette adresse IP distante. S'il ne s'agit pas de la même interface sur laquelle les paquets de l'IP distant arrivent, l'application stricte les rejettera :

```
ip route get <remote IP>
```

From:

<http://www.ouarte.garden/> - **dwndoc**

Permanent link:

<http://www.ouarte.garden/doku.php?id=issue:serveur-avec-deux-interfaces>

Last update: **2025/02/19 10:59**

