ip-rule

Gestion de la base de stratégie de routage

ip rule manipule les règles de la base de stratégie de routage contrôlant l'algorithme de sélection de route. Les algorithmes classiques de routage utilisant dans l'Internet créent des décisions de routage basé seulement sur l'adresse de destination des paquets (et en théorie, mais pas en pratique, sur le champs TOS).

Dans certaines circonstances on veut router les paquets différemment en fonction d'autres champs du paquet : le protocole IP, ports du protocole de transport, etc. Cette tâche est appelée 'stratégie de routage'.

Pour résoudre cette tâche, la destination conventionnelle basée sur une table de routage, ordonnée en accord avec la règle de correspondance la plus longue, et remplacée avec une base de données de stratégie de routage (RPDB), qui sélectionne les routes en exécutant certains jeux de règles.

Chaque règle de stratégie de routage consiste d'un sélecteur et d'une action prédictive. Le RPDB est scanné dans l'ordre décroissant de priorité. Le sélecteur de chaque règle est appliqué à {source address, destination address, incoming interface, tos, fwmark} et, si le sélecteur matche le paquet, l'action est effectuée. La prédiction de l'action peut retourner un succès. Dans ce cas, il va soit donner une route ou une indication d'erreur et la recherche RPDB se termine. Sinon, le programme RPDB continue avec la règle suivante.

Sémantiquement, l'action naturelle est de sélectionner le prochain saut et le périphérique de sortie. Au démarrage le kernel configure le RPDB consistant des 3 règles :

1. Priorité : 0, Selecteur : match tout, Action : recherche dans la table de routage local (ID 255). La table local est une table de routage spéciale contenant des routes de contrôle hautement prioritaire pour les adresses locales et de broadcast. La règle 0 est spéciale, elle ne peut pas être supprimée ou écrasée.
2. Priorité : 32766, Sélecteur : match tout, Action : Recherche dans la table de routage main (ID 254). La table main est la table de routage normale contenant toutes les routes sans stratégie. Cette règle peut être supprimée et/ou écrasée.
3. Priorité : 32767, Sélecteur : match tout, Action : recherche dans la table de routage default (ID 253). La table default est vide. Elle est réservée pour certains pré-traitements si aucune règle par défaut précédente n'a séléctionné le paquet. Cette règle peut également être supprimée.

Chaque entrée RPDB a différents attributs additionnels. Par exemple, chaque règle a un pointer vers une table de routage. les règles NAT et masquerading ont un attribut pour sélectionner une nouvelle adresse IP à modifier. Derrière ça, les règles ont certains attributs optionnels, quelles routes ont, nommés realms. Ces valeurs n'écrasent pas celles contenue dans les tables de routage. Elles sont seulement utilisée si la route n'a sélectionné aucun attribut.

Le RPDB peut contenir des règles de types suivants :

unicast La règle stipule de retourner la route trouvée dans la table de routage référencée par la règle

blackhole La règle stipule de supprimer le paquet

unreachable La règle stipule de générer une erreur 'Network is unreachable'

prohibit La règle stipule de générer une erreur 'Communication is administratively prohibited'

nat La règle stipule de traduire l'adresse source du paquet IP en une autre valeur

add Insert une nouvelle règle

delete Supprime une règle

type TYPE le type de cette règle.

from PREFIX Sélectionne le préfixe source à matcher

to PREFIX Sélectionne le préfixe de destination à matcher

iif NAME Sélectionne le périphérique entrant à matcher. Si l'interface est la boucle locale, la règle matche seulement les paquets venant de cet hôte. Cela signifie que vous pouvez créer des tables de routage séparés pour les paquets venant des sockets locaux de ceux liés à un périphérique.

oif NAME Sélectionne le périphérique sortant à matcher. L'interface sortant est seulement disponible pour les paquets venant de sockets locaux qui sont liés à un périphérique.

tos TOS

dsfield TOS Sélectionne la valeur TOS à matcher

fwmark MARK Sélectionne la valeur fwmark à matcher

priority PREFERENCE La priorité de cette règle. Chaque règle devrait avoir un jeu explicite de valeur de priorité unique.

table TABLEID L'identifiant de table de routage à rechercher si la règle matche. Il est également possible d'utiliser une recherche au lieu d'une table

suppress_prefixlength NUMBER Rejète les décisions de routage qui on une longueur de préfix de NUMBER ou moins

suppress_ifgroup GROUP Rejète les décisions qui utilisent un périphérique appartenant au groupe d'interface spécifié.

realms FROM/TO domaine à sélectionner si la règle a matché et que la recherche dans la table de routage a réussie. realms TO est seulement utilisé si la route ne sélectionne aucun domaine.

nat ADDRESS La base du block d'adresse IP à traduire (pour les adresses source). ADDRESS peut être soit le début du block des adresses NAT (sélectionné par routes NAT) ou une adresse de l'hôte local (ou même 0). Dans le dernier cas le routeur ne traduit pas les paquets, mais les masquerade à cette adresse. Utiliser map-to au lieu de nat est la même chose.

flush dumps également toutes les tables supprimées

show Liste les règles