
firewalld.direct

Fichier de configuration direct

Ce fichier de configuration donne un accès plus directe au firewall. Il nécessite de connaître les concepts ip(6)tables/ebtables. Un fichier de configuration direct contient des informations sur les chaînes directes permanentes

Exemple de structure de fichier de configuration directe :

```
<?xml version="1.0" encoding="utf-8"?>
<direct>
  [ <chain ipv="ipv4|ipv6|eb" table="table" chain="chain"/> ]
  [ <rule ipv="ipv4|ipv6|eb" table="table" chain="chain" priority="priority"> args </rule> ]
  [ <passthrough ipv="ipv4|ipv6|eb"> args </passthrough> ]
</direct>
```

direct Tag définissant la configuration directe

chain Définis les noms pour les chaînes additionnelles. Optionnel et peut être spécifié plusieurs fois. Une entrée chaîne a exactement 3 attributs :

ipv="ipv4|ipv6|eb" Famille d'IP où la chaîne doit être créée

table="table" Nom de la table où la chaîne doit être créée

chain="chain" Nom de la chaîne, qui sera créée

rule Permet d'ajouter des règles à une chaîne intégrée ou ajoutée. Optionnel et peut être utilisé plusieurs fois. Une règle a exactement 4 attributs :

ipv="ipv4|ipv6|eb" Famille d'IP où la règle doit être ajoutée

table="table" Nom de la table où la règle doit être ajoutée

chain="chain" Nom de la chaîne où la règle doit être ajoutée

priority="priority" Priorité utilisée pour ordonner les règles. 0 signifie d'ajouter la règle en haut de la chaîne

passthrough Permet d'ajouter des règles à une chaîne intégrée ou ajoutée. Optionnel et peut être utilisé plusieurs fois. Une règle a exactement un attribut :

ipv="ipv4|ipv6|eb" Famille d'IP où le passthrough doit être ajouté

Exemples

Blacklister les réseaux 192.168.1.0/24 et 192.168.5.0/24 en loggant et supprimant très tôt dans la table raw :

```
<chain ipv="ipv4" table="raw" chain="blacklist"/>
<rule ipv="ipv4" table="raw" chain="PREROUTING" priority="0">-s 192.168.1.0/24 -j blacklist</rule>
<rule ipv="ipv4" table="raw" chain="PREROUTING" priority="1">-s 192.168.5.0/24 -j blacklist</rule>
<rule ipv="ipv4" table="raw" chain="blacklist" priority="0">-m limit --limit 1/min -j LOG --log-prefix "blacklisted : "</rule>
<rule ipv="ipv4" table="raw" chain="blacklist" priority="1">-j DROP</rule>
```