Firewalld

Table of Contents

firewalld est un pare-feu sous Linux qui est facile à mettre en oeuvre et paramétrer, par rapport à **iptables** ou son successeur **nftables**.

Il est livré par défaut sous **CentOS** et **Fedora**, mais il est possible de l'installer sur d'autres distributions Linux telles que **Gentoo** ou **Debian**.

firewalld est un outil de gestion de pare-feu pour les systèmes d'exploitation Linux. Il fournit des fonctionnalités de pare-feu en agissant comme un frontal pour le framework **netfilter** du noyau Linux. Le backend par défaut actuel de **firewalld** est **nftables**.

Installation

installation de firewalld

```
dnf install firewalld
```

Activation de firewalld

```
systemctl start firewalld.service
systemctl enable firewalld.service
```

Gestion des erreurs

Reload échoue

Firewalld utilise **iptables-restore** afin d'injecter les précédentes règles du pare-feu, si une règle est mal formulée, la commande `firewall-cmd -reload` peut échouer avec ce type de message:

```
Error: COMMAND_FAILED: Direct: '/usr/sbin/iptables-restore -w -n' failed:
```

```
iptables-restore v1.8.4 (nf_tables): unknown option "--to-destination"
Error occurred at line: 2
Try `iptables-restore -h' or 'iptables-restore --help' for more information.
```

La ligne 2 des règles de pare-feu contient une option non reconnue.

Habituellement, les fichiers qui contiennent ces règles se trouvent dans `/etc/firewalld/*/*.xml` (bien que l'on puisse modifier les fichiers fournis par le “système” pour un effet similaire).

Il faut donc retirer la règle incriminée afin de pouvoir recharger la configuration du pare feu.