

Firewalld : un firewall simple à utiliser

Firewalld est un pare-feu que je trouve très agréable à utiliser, où on peut « cacher » la complexité de certains éléments de configuration derrière des noms simples à utiliser.

Par exemple, je peux avoir un service qui n'a pas spécialement de port dédié, donc qui n'est pas proposé par firewall. Mettons un **wireguard** qui écoute sur le port 9879. Plutôt que d'utiliser `9879/udp` dans ma configuration, je vais créer un service `wireguard`, et c'est ce service que j'autoriserai.

Ce sera bien plus parlant quand je relirai la configuration.

Liens :

- Documentation officielle : <https://firewalld.org/documentation/>
- <https://www.linuxtricks.fr/wiki/firewalld-le-pare-feu-facile-sous-linux>
- <https://www.rootusers.com/how-to-use-firewalld-rich-rules-and-zones-for-filtering-and-nat/>
- <https://kb.vander.host/security/firewalld-cheat-sheet/>

Principes

En très gros et en très résumé, on va avoir des zones, qui sont des ensembles d'adresses IP et la zone `public` qui concerne toutes les IPs, sauf celles qui sont dans d'autres zones.

On va aussi avoir des services, qui décrivent... des services : port et protocole (ex: `5666` et `tcp` pour nrpe).

On va aussi avoir des « rich rules » dans les zones, des exceptions aux règles appliquées dans la zone.

Toute la configuration est dans des fichiers XML très simples à lire, c'est très agréable. Tant qu'on ne surcharge pas la configuration par défaut, les fichiers sont dans `/usr/lib/firewalld/` mais dès qu'on modifie un élément de configuration, celui-ci se retrouvera copié dans `/etc/firewalld/` et modifié.

Test de configuration

Si on modifie de la configuration à la main (en écrivant dans `/etc/firewalld`, on prendra soin de tester la configuration avec les commandes suivantes :

Si `firewalld` est coupé :

```
firewall-offline-cmd --check-config
```

Si `firewalld` est lancé :

```
firewall-cmd --check-config
```

Attention

Quand on installe `firewalld`, le firewall démarre de suite en n'autorisant en public que `ssh` (et `dhcpv6-client`).

Il est donc préférable de l'installer et de le couper directement après :

```
apt install firewalld &&  
systemctl stop firewalld
```

On pourra créer la configuration tranquillement avec la commande `firewall-offline-cmd` et lancer le service une fois la configuration terminée.

Changements permanents

Si on veut rendre un changement permanent (c-à-d qu'il soit écrit dans la config au lieu d'être juste appliqué jusqu'au redémarrage), il faut ajouter ça aux commandes :

```
--permanent
```

Par contre, avec `--permanent`, il faut recharger la configuration pour appliquer les modifications (ou alors on applique une fois avec `--permanent` et une fois sans) :

```
firewall-cmd --reload
```

À l'inverse, on peut créer des règles sans le `--permanent` et ensuite écrire ces règles dans la configuration permanent avec la commande suivante :

```
firewall-cmd --runtime-to-permanent
```

NB : certaines commandes nécessitent forcément le `--permanent`.

Bloquer une adresse IP

On peut soit ajouter les adresses aux zones `drop` ou `block` :

```
firewall-cmd --zone=drop --add-source 192.0.2.0/24
firewall-cmd --zone=drop --add-source 192.0.2.0/24 --permanent
```

Soit ajouter une `rich-rule` (`man firewalld.richlanguage`) à la zone `public` :

```
firewall-cmd --zone public --add-rich-rule "rule family=ipv4 source address=192.0.2.0/24 reject"
firewall-cmd --zone public --add-rich-rule "rule family=ipv4 source address=192.0.2.0/24 reject" --permanent
```

Pour enlever un blocage :

```
firewall-cmd --zone drop --remove-source 51.159.0.0/16
firewall-cmd --zone drop --remove-source 51.159.0.0/16 --permanent
```

```
firewall-cmd --zone public --remove-rich-rule "rule family=ipv4 source address=51.159.0.0/16 reject"
firewall-cmd --zone public --remove-rich-rule "rule family=ipv4 source address=51.159.0.0/16 reject" --
permanent
```

Pour voir les blocages par `rich-rule` (la 1ère commande donne les blocages actuellement activés, l'autre ceux qui sont dans les fichiers de configuration. Il peut y avoir une différence... ou pas !) :

```
firewall-cmd --list-rich-rules
firewall-cmd --list-rich-rules --permanent
```

Pour bloquer un ipset (voir plus bas) :

```
firewall-cmd --zone=drop --add-source ipset:le_nom_de_l_ipset
firewall-cmd --zone=drop --add-source ipset:le_nom_de_l_ipset --permanent
```

Zones

Voir les zones disponibles :

```
firewall-cmd --get-zones
```

NB : la zone `public`, par défaut, n'autorise que le SSH et dhcpv6-client. L'installation de firewalld sur une machine va donc couper l'accès aux services. Il faut donc stopper firewalld juste après son installation, regarder les ports utilisés sur la machine et modifier la zone `public` soit en copiant `/usr/lib/firewalld/zones/public.xml` dans `/etc/firewalld/zones/`, soit en préparant une ligne de commande à lancer juste après le démarrage de firewalld.

NB : les zones peuvent avoir une `target`, l'action à appliquer aux connexions qui correspondent à la zone. Voir [la doc](#).

NB : Une adresse IP ne peut se trouver que dans une seule zone mais on peut ajouter dans une zone un réseau qui contient une adresse IP déjà présente dans une autre zone. Cependant, le comportement peut ne pas être celui attendu. Il vaut mieux ajouter une `rich-rule` à la zone pour faire une exception aux règles de la zone.

Voir la zone par défaut (celle sur laquelle s'appliqueront les modifications si on ne spécifie pas la zone) :

```
firewall-cmd --get-default-zone
```

Définir la zone par défaut :

```
firewall-cmd --set-default-zone work
```

Voir la configuration de la zone :

```
firewall-cmd --info-zone lazone
```

Voir la configuration de toutes les zones :

```
firewall-cmd --list-all-zones
```

Créer une zone :

```
firewall-cmd --permanent --new-zone mazonne  
firewall-cmd --reload
```

Supprimer une zone :

```
firewall-cmd --permanent --delete-zone mazonne  
firewall-cmd --reload
```

Chaque interface du système peut être attribuée à une zone. Pour ajouter l'interface ens192 à la zone work en l'enlevant de sa précédente zone :

```
firewall-cmd --change-interface ens192 --zone work [--permanent]
```

Pour retirer l'interface ens192 de la zone work :

```
firewall-cmd --remove-interface ens192 --zone work [--permanent]
```

Pour ajouter l'interface ens192 à la zone work (interface qui ne soit pas être affectée à une zone) :

```
firewall-cmd --add-interface ens192 --zone work [--permanent]
```

Ajouter des adresses IP ou un réseau à une zone :

```
firewall-cmd --zone work --add-source 192.0.2.0/24 [--permanent]  
firewall-cmd --zone work --add-source 192.0.2.200 [--permanent]
```

Retirer des adresses IP ou un réseau d'une zone :

```
firewall-cmd --zone work --remove-source 192.0.2.0/24 [--permanent]  
firewall-cmd --zone work --remove-source 192.0.2.200 [--permanent]
```

Pour basculer une adresse IP ou un réseau d'une zone à une autre :

```
firewall-cmd --zone l_autre_zone --change-source 192.0.2.0/24 [--permanent]  
firewall-cmd --zone l_autre_zone --change-source 192.0.2.200 [--permanent]
```

Si l'adresse IP / le réseau était dans une autre zone, ça équivaut à un `--remove-source` suivi d'un `--add-source`, si ce n'était pas le cas, ça fait juste comme un `--add-source`.

Voir la `target` d'une zone :

```
firewall-cmd --permanent --get-target --zone drop
```

Définir la `target` d'une zone :

```
firewall-cmd --permanent --set-target [default|ACCEPT|DROP|REJECT] --zone drop
```

Pour voir dans quelle zone est une adresse IP :

```
firewall-cmd --get-zone-of-source=<adresse IP ou réseau en notation CIDR ou adresse MAC ou ipset>
```

Si ça répond `no zone`, c'est que l'IP ou le réseau n'est pas explicitement associé à une zone.

Attention : si un réseau est enregistré dans une zone, lancer la commande sur une IP du réseau ne renverra pas la zone en question !

Services

Voir les services existants :

```
firewall-cmd --get-services
```

Voir le détail d'un service :

```
firewall-cmd --info-service ssh
```

Créer un nouveau service :

```
firewall-cmd --permanent --new-service influxdb  
firewall-cmd --permanent --service influxdb --set-description InfluxDB  
firewall-cmd --permanent --service influxdb --add-port 8086/tcp
```

Ajouter un service à une zone :

```
firewall-cmd --zone public --add-service nrpe [--permanent]
```

Retirer un service d'une zone :

```
firewall-cmd --zone public --remove-service nrpe [--permanent]
```

Voir les services d'une zone :

```
firewall-cmd --list-services --zone work
```

Si on ne souhaite pas créer de service mais autoriser un certain port et protocole, on peut les ajouter directement à la zone :

```
firewall-cmd --zone work --add-port 1234/udp [--permanent]
```

Et pour les supprimer :

```
firewall-cmd --zone work --remove-port 1234/udp [--permanent]
```

Pour voir les ports/protocoles d'une zone (ça ne listera pas les services !) :

```
firewall-cmd --list-ports --zone work
```

IPSet : groupes d'adresses

Doc : https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/security_guide/sec-setting_and_controlling_ip_sets_using_firewalld

Cas d'usage : on voit plein de spammeurs venant du VPN d'Avast. On fait un `whois`, on voit le numéro d'**AS** des serveurs d'Avast, on va sur <https://asnlookup.com/> pour choper leur liste d'adresses IP et on en fait un ipset pour les bloquer.

NB : un ipset ne peut contenir qu'un type d'adresses, IPv4 ou IPv6, pas les deux.

NB : **Fail2ban**, lorsqu'il utilise firewalld, utilise des ipset, mais à un niveau un peu plus bas (nftables). Ces ipset ne sont pas vus par firewalld. On peut voir tous les ipset, même bas niveau avec la commande `ipset list -name` (`ipset list le_nom_de_l_ipset` pour voir les adresses et le détail de l'ipset).

Un ipset sert à regrouper des adresses pour leur appliquer des règles facilement.

Voir les types d'ipset disponibles :

```
firewall-cmd --get-ipset-types
```

Voir les ipsets existants :

```
firewall-cmd --permanent --get-ipsets
```

Créer un ipset :

```
firewall-cmd --permanent --type hash:net --new-ipset test
```

Pour un ipset IPv6 :

```
firewall-cmd --permanent --type hash:net --option "family=inet6" --new-ipset test-v6
```

Supprimer un ipset :

```
firewall-cmd --permanent --delete-ipset test
```

Voir les infos d'un ipset :

```
firewall-cmd --info-ipset test [--permanent]
```

Ajouter une adresse IP à un ipset :

```
firewall-cmd --ipset test --add-entry 192.0.2.1 [--permanent]
```

Supprimer une adresse IP d'un ipset :

```
firewall-cmd --ipset test --remove-entry 192.0.2.1 [--permanent]
```

Voir les adresses IP d'un ipset :

```
firewall-cmd --ipset test --get-entries [--permanent]
```

Ajouter un paquet d'IP d'après un fichier :

```
cat > iplist.txt <<EOL
192.0.2.2
192.0.2.3
198.51.100.0/24
203.0.113.254
EOL
firewall-cmd --ipset test --add-entries-from-file iplist.txt [--permanent]
```

Supprimer un paquet d'IP d'après un fichier :

```
firewall-cmd --ipset test --remove-entries-from-file iplist.txt [--permanent]
```

Ajouter un ipset dans une zone :

```
firewall-cmd --zone drop --add-source ipset:test [--permanent]
```

Supprimer un ipset d'une zone :


```
firewall-cmd --zone drop --remove-source ipset:test [--permanent]
```

Créer des exceptions avec des règles riches

Cas classique : on bloque un pays avec des ipset et quelqu'un a besoin d'accéder à nos services depuis là-bas.

L'ipset est dans la zone `drop`. On va ajouter une `rich-rule` pour faire une exception :

```
firewall-cmd --zone drop --add-rich-rule='rule family="ipv4" source address="192.0.2.29" port
port="443" protocol="tcp" accept'
firewall-cmd --zone drop --add-rich-rule='rule family="ipv4" source address="192.0.2.29" port port="80"
protocol="tcp" accept'
firewall-cmd --zone drop --permanent --add-rich-rule='rule family="ipv4" source address="192.0.2.29" port
port="443" protocol="tcp" accept'
firewall-cmd --zone drop --permanent --add-rich-rule='rule family="ipv4" source address="192.0.2.29" port
port="80" protocol="tcp" accept'
```

Pour supprimer l'exception :

```
firewall-cmd --zone drop --remove-rich-rule 'rule family="ipv4" source address="192.0.2.29" port
port="80" protocol="tcp" accept'
firewall-cmd --zone drop --remove-rich-rule 'rule family="ipv4" source address="192.0.2.29" port
port="443" protocol="tcp" accept'
firewall-cmd --zone drop --permanent --remove-rich-rule 'rule family="ipv4" source address="192.0.2.29" port
port="80" protocol="tcp" accept'
firewall-cmd --zone drop --permanent --remove-rich-rule 'rule family="ipv4" source address="192.0.2.29" port
port="443" protocol="tcp" accept'
```

On peut utiliser des services dans les règles riches :

```
firewall-cmd --zone drop --add-rich-rule='rule family="ipv4" source address="192.0.2.29" service name=https
accept'
```

On peut utiliser des ipset dans les règles riches :

```
firewall-cmd --zone drop --add-rich-rule='rule family="ipv4" source ipset="test-v6" service name=https accept'
```

NB : ajouter l'adresse IP en source dans la zone `public` ne servirait strictement à rien.

Blocage geoIP

On peut se baser sur le script de <https://github.com/simonbouchard/geoip-blocking-w-firewalld> (le fork de Framasoft).

On modifie les pays à bloquer dans `/etc/default/firewalld-geoip` et on lance le script. À mettre dans un cron pour mettre à jour les adresses.

Faire du NAT

Voir la partie `Network Address Translation (NAT)` de <https://www.rootusers.com/how-to-use-firewalld-rich-rules-and-zones-for-filtering-and-nat/>.

Revision #1

Created 13 February 2025 21:11:48 by Nicolas

Updated 13 February 2025 21:16:34 by Nicolas