

# firewalld

Trois outils disponibles

- iptables (deprecated)
- firewall-config (GUI)
- firewall-cmd (CLI)

Firewall statefull par défaut.

Le service iptables ne doit pas être lancé avec firewalld, ces outils sont exclusifs. `systemctl mask iptables` pour l'empêcher de se lancer si il est présent.

Une zone est une collection de rules qui sont appliquées aux paquets entrant correspondant à une sources spécifique ou une interface. Par défaut le filtrage ne s'applique qu'en entrée, pas en sortie.

Les multiples zones par défaut servent surtout aux serveurs à plusieurs interface. Sur un serveur avec une seule interface, utiliser la zone par défaut.

Zones par défaut

- block
- dmz
- drop
- external
- home
- internal
- public (zone par défaut)
- trusted
- work

Liste des services définis

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

Emplacement des services

```
/usr/lib/firewalld/services  
ou  
/etc/firewalld/services
```

```
firewall-cmd --get-default-zone  
firewall-cmd --get-zones  
Tout ce qu'on peut obtenir comme informations  
firewall-cmd --get  
firewall-cmd --list-all  
firewall-cmd --list-all --zone=public
```

Ajouter un service à la zone par défaut en mémoire (non persistant)

```
firewall-cmd --add-service=vnc-server
```

Vérifier qu'il est bien ajouté

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

```
firewall-cmd --permanent --add-service=vnc-server
```

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

Utiliser si possible en priorité les services déjà définis mais pour ouvrir un port spécifique

```
firewall-cmd --permanent --add-ports=2022/tcp
```

```
firewall-cmd --state
```

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

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

```
firewall-cmd --add-rich-rule
```

```
man firewalld.richlanguage
```

Redémarrer le service basé sur la configuration persistante

```
systemctl restart firewalld
```

ou

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

firewall-config (GUI)

services

port

rich rules

Port masquerading

NAT

From:

<https://wiki.ouieuhtoutca.eu/> - kilsufi de noter

Permanent link:

<https://wiki.ouieuhtoutca.eu/firewalld>

Last update: **2021/01/21 21:42**

