

firewalld



context

dit document beschrijft de werking van firewalld, de firewall die op centos/redhat wordt gebruikt.

algemeen

- meest opmerkelijke is de ondersteuning voor **zones** waaraan je interfaces toevoegt en die de firewall config uit die zone overnemen.
Enkele voorbeelden: public, home, block, internal, ...
- toegangen worden gedefinieerd in **services** waarbij je protocol en poort tot een herbruikbaar geheel samenvoegt.
bv: ssh: tcp/22, dns: udp/53, ...
- zones, services, ports worden bewaard in xml-bestanden die bij starten van de firewall worden ingeladen.
Die kan je vinden onder /etc/firewalld/
- all beschikbare configuraties kan je vinden onder /usr/lib/firewalld
- beheer doe je in grote make ahv `firewall-cmd`

zones

- overzicht van alle (configureerbare) zones:

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

- overzicht van alle actieve zones.
Indien geen output (en de firewall is actief) is het de default zone

```
sudo firewall-cmd --get-active-zones
```

- default zone:

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

services

- actieve configuratie van een zone:

```
sudo firewall-cmd --zone=<zone>--list-services
```

- overzicht van alle beschikbare services (/usr/lib/firewalld/services):

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

- service toevoegen:

```
firewall-cmd --zone=<zone> --add-service=<naam service>
```

- service permanent toevoegen aan de firewall config:

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

poorten

- poort toevoegen:

```
firewall-cmd --zone=<zonenaam> --add-port=<poortnummer>/<protocol> --permanent
```

- voorbeeld:

```
firewall-cmd --zone=public --add-port=10000/tcp --permanent
```

beheer

start/stop

- starten, stoppen en reload config:

```
sudo systemctl start|stop|restart|status firewalld
```

eigen service toevoegen

- `firewall-cmd --permanent --new-service-from-file=<existingService>.xml --name=nieuweService`
- bewerk /etc/firewalld/services/<nieuweService>.xml
- reload de firewall: `systemctl reload firewalld`
- voeg de service toe aan de zone: `firewall-cmd --zone=public --add-service=<nieuweService>`

- voeg service aan permanente configuratie toe:

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

- herstart firewalld service: `systemctl restart firewalld`

eigen service verwijderen

- `firewall-cmd --permanent --delete-service=serviceNaam`

logging

Important: TODO

meer info

1. [firewalld: getting started](#)
2. [adding our own service](#)

[Linux](#), [firewalld](#)

From:

<https://louslab.be/> - Lou's lab

Permanent link:

<https://louslab.be/doku.php?id=linux:firewalld>

Last update: **2024/11/16 18:14**

