Firewalld

firewalld ist ein von Red Hat entwickelter Firewall-Daemon. Er verwendet standardmäßig nftables.

Firewalld bietet eine dynamisch verwaltete Firewall mit Unterstützung für Netzwerk-/Firewall-Zonen, die den Vertrauensgrad von Netzwerkverbindungen oder Schnittstellen definieren. Es bietet Unterstützung für IPv4- und IPv6-Firewall-Einstellungen, Ethernet-Brücken und IP-Sets. Es gibt eine Trennung von Laufzeit- und permanenten Konfigurationsoptionen. Es bietet auch eine Schnittstelle für Dienste oder Anwendungen, um Firewall-Regeln direkt hinzuzufügen.

Pakete

```
pacman -S firewalld ipset
```

Start

```
systemctl enable --now firewalld.service
```

Add & remove

Nach jeder Änderung sollte firewalld immer neu gestartet werden:

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

interface

```
firewall-cmd --change-interface=DEIN-INTERFACE --zone=home --permanent
```

or

```
firewall-cmd --add-interface=DEIN-INTERFACE --zone=home --permanent
firewall-cmd --remove-interface=DEIN-INTERFACE --zone=home --permanent
```

or

```
nmcli connection show
nmcli connection modify 'NAME' connection.zone home
```

Überprüfe die Namen deiner Schnittstelle/n mit `ip -o addr show scope global | awk '{print $2}'`.

service

Prüfe, ob der gewünschte Service bereits verfügbar ist `ls /usr/lib/firewalld/services/` oder `ls /usr/lib/firewalld/services/ | grep 'DEIN-SERVICE`. Andernfalls musst du deine eigenen erstellen.

```
firewall-cmd --add-service=kdeconnect --zone=home --permanent
firewall-cmd --remove-service=dhcpv6-client --zone=home --permanent
```

selbst erstellen

```
firewall-cmd --new-service=DEIN-NEUER-SERVICE --permanent
firewall-cmd --service=DEIN-NEUER-SERVICE --set-description=DEIN-NEUER-
SERVICE --permanent
firewall-cmd --service=DEIN-NEUER-SERVICE --set-short=DNS --permanent
firewall-cmd --service=DEIN-NEUER-SERVICE --add-port=1234/tcp --permanent
```

```
firewall-cmd --add-service=DEIN-NEUER-SERVICE --zone=home --permanent
```

port

```
firewall-cmd --add-port=80/tcp --zone=home --permanent
firewall-cmd --remove-port=80/tcp --zone=home --permanent
```

forwarding

```
firewall-cmd --add-forward-
port=port=12345:proto=tcp:toport=22:toaddr=192.168.1.50 --zone=home --
permanent
firewall-cmd --remove-forward-
port=port=12345:proto=tcp:toport=22:toaddr=192.168.1.50 --zone=home --
permanent
```

zone

```
firewall-cmd --new-zone=DEINE-ZONE --permanent
firewall-cmd --delete-zone=DEINE-ZONE --permanent
```

masquerade

```
firewall-cmd --add-masquerade --zone=home --permanent
firewall-cmd --remove-masquerade --zone=home --permanent
```

new policy

```
firewall-cmd --new-policy NAT_int_to_ext --permanent
firewall-cmd --policy NAT_int_to_ext --add-ingress-zone wireguard --
permanent
firewall-cmd --policy NAT_int_to_ext --add-egress-zone home --permanent
firewall-cmd --policy NAT_int_to_ext --set-target ACCEPT --permanent
```

Basierend auf wireguard.

List

active zones

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

zones

```
firewall-cmd --list-all-zones
firewall-cmd --info-zone=home
```

interface

```
firewall-cmd --get-zone-of-interface=DEIN-INTERFACE
```

Überprüfe die Namen deiner Schnittstelle/n mit `ip -o addr show scope global | awk '{print $2}'`.

services

```
firewall-cmd --get-services
firewall-cmd --list-services --zone=home
firewall-cmd --info-service DEIN-SERVICE
```

Selbst erstellt:

```
ls /etc/firewalld/services/
```

Vorgegebene:

```
ls /usr/lib/firewalld/services/
```

ports

```
firewall-cmd --list-ports --zone=home
```

rich rules

```
firewall-cmd --list-rich-rules --zone=home
```

policies

```
ls /usr/lib/firewalld/policies/
ls /etc/firewalld/policies/
```

Desktop tray

Nur wenn du eine Desktop-Umgebung auf deinem Server oder für deinen Desktop-Computer betreibst.

Die GUI kann auch hilfreich sein, wenn Sie Zonen an bestimmten Netzwerkstandorten schnell ändern müssen.

```
firewall-applet
```

```
nano ~/.config/firewall/applet.conf
```

```
[General]
notifications=true
show-inactive=true
```

Ändere runtime zu permanent

Die permanente Option `--permanent` kann verwendet werden, um Optionen dauerhaft zu setzen. Diese Änderungen werden nicht sofort wirksam, sondern erst nach einem Neustart/Neuladen des Dienstes oder einem Neustart des Systems. Ohne die Option `--permanent` wird eine Änderung nur Teil der Laufzeitkonfiguration (`--runtime`) sein.

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