Firewalld

firewalld is a firewall daemon developed by Red Hat. It uses nftables by default.

Firewalld provides a dynamically managed firewall with support for network/firewall zones that define the trust level of network connections or interfaces. It has support for IPv4, IPv6 firewall settings, ethernet bridges and IP sets. There is a separation of runtime and permanent configuration options. It also provides an interface for services or applications to add firewall rules directly.

Packages

```
pacman -S firewalld ipset
```

Start

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

Add & remove

After every change firewalld should always be reloaded:

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

interface

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

or

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

or

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

Check your interface name/s with `ip -o addr show scope global | awk '{print $2}'`.

service

Check if the favoured service is available by default `ls /usr/lib/firewalld/services/` or `ls`

/usr/lib/firewalld/services/ | grep 'YOUR-SERVICE. Otherwise, you have to create your own.

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

custom made

```
firewall-cmd --new-service=YOUR-NEW-SERVICE --permanent
firewall-cmd --service=YOUR-NEW-SERVICE --set-description=YOUR-NEW-SERVICE --permanent
firewall-cmd --service=YOUR-NEW-SERVICE --set-short=YNS --permanent
firewall-cmd --service=YOUR-NEW-SERVICE --add-port=1234/tcp --permanent
```

```
firewall-cmd --add-service=YOUR-NEW-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=YOUR-ZONE --permanent
firewall-cmd --delete-zone=YOUR-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
```

Based on 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=YOUR-INTERFACE
```

Check your interface name/s with `ip -o addr show scope global | awk '{print $2}'`.

services

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

Self created:

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

Default:

```
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

Only if you are running a desktop environment on your server or for your desktop computer.

The GUI can also be useful if you need to quickly change zones at specific network locations.

```
python-pyqt6
```

```
firewall-applet
```

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

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

Change runtime to permanent

The permanent option `--permanent` can be used to set options permanently. These changes are not effective immediately, only after service restart/reload or system reboot. Without the `--permanent` option, a change will only be part of the `--runtime` configuration.

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