

firewall-cmd is a command to adjust the settings of firewalld.

## Start the firewall

<code>systemctl enable --now firewalld</code>	enable and start the firewall
---	-------------------------------

## Global options

<code>--permanent</code>	append to any command to make firewalld changes persistent
<code>--reload</code>	reload firewalld rules

## Firewall-cmd: managing zones

<code>--get-zones</code>	list all zones
<code>--get-active-zones</code>	list all active zones and all interfaces is each
<code>--zone=home --list-all</code>	list properties of zone <code>home</code>
<code>--change-interface=eth0 --zone=home</code>	add interface <code>eth0</code> to zone <code>home</code>
<code>--get-default</code>	get default zone
<code>--set-default-zone home</code>	set default zone to <code>home</code>
<code>--new-zone=work</code>	create new zone <code>work</code> (requires rule reload)

## Firewall-cmd: add ports and services

<code>--get-services</code>	list all defined services
<code>--add-service murmur --zone=home</code>	allow traffic on <code>murmur</code> ports in zone <code>home</code>
<code>--add-port=123/tcp --zone=home</code>	allow TCP traffic on port 123 in zone <code>home</code>

## Firewall-cmd: remove ports and services

<code>--remove-port 123/tcp --zone=home</code>	deny traffic on port 123 in zone <code>home</code>
<code>--remove-service murmur --zone=home</code>	deny traffic on <code>murmur</code> ports in zone <code>home</code>

## Direct rules

Direct rules can be passed through firewall-cmd. This allows complex configuration, for instance, when you want to allow traffic to and from a virtual machine through a network bridge.

<code>--direct --passthrough ipv6 -I FORWARD -o tap0 -j ACCEPT</code>	permit IPv6 traffic from tap0
<code>--direct --passthrough ipv6 -I FORWARD -i tap0 -j ACCEPT</code>	permit IPv6 traffic to tap0