firewalld Cheatsheet

By Dejan Panovski • Updated on Mar 25, 2026 • Download PDF

Quick reference for managing firewall rules with firewalld on Linux

firewalld is a dynamic firewall manager used on Fedora, RHEL, CentOS, and their derivatives. It organizes rules into zones and supports both runtime and permanent configuration. This cheatsheet covers service management, zones, ports, rich rules, and masquerading.

Basic Commands

Start, stop, and reload the firewalld service.

`firewall-cmd --state`	Check if firewalld is running
`sudo systemctl start firewalld`	Start the service
`sudo systemctl stop firewalld`	Stop the service
`sudo systemctl enable firewalld`	Enable at boot
`sudo systemctl disable firewalld`	Disable at boot
`sudo firewall-cmd --reload`	Reload rules without dropping connections
`sudo firewall-cmd --complete-reload`	Full reload, resets all connections

Runtime vs Permanent

By default, `firewall-cmd` changes apply at runtime only and are lost on reload. Add `--permanent` to persist a rule, then reload to activate it.

`sudo firewall-cmd --add-service=http`	Allow HTTP (runtime only)
`sudo firewall-cmd --add-service=http --permanent`	Allow HTTP (survives reload)
`sudo firewall-cmd --reload`	Activate permanent rules
`sudo firewall-cmd --runtime-to-permanent`	Save all runtime rules as permanent

Zones

Zones define trust levels for network connections. Each interface belongs to one zone.

`firewall-cmd --get-zones`	List all available zones
`firewall-cmd --get-default-zone`	Show the default zone
`sudo firewall-cmd --set-default-zone=public`	Set the default zone
`firewall-cmd --get-active-zones`	Show active zones and their interfaces
`firewall-cmd --zone=public --list-all`	List all settings for a zone
`sudo firewall-cmd --zone=public --change-interface=eth0`	Assign interface to zone (runtime)
`sudo firewall-cmd --zone=public --add-interface=eth0 --permanent`	Assign interface permanently
`sudo firewall-cmd --zone=public --remove-interface=eth0`	Remove interface from zone

Services

Allow or block named services defined in `/usr/lib/firewalld/services/`.

`firewall-cmd --get-services`	List all predefined services
`firewall-cmd --zone=public --list-services`	List services allowed in zone
`firewall-cmd --info-service=http`	Show ports and protocols for a service
`sudo firewall-cmd --zone=public --add-service=http --permanent`	Allow service permanently
`sudo firewall-cmd --zone=public --remove-service=http --permanent`	Remove service

Ports

Open or close individual ports when no predefined service exists.

`firewall-cmd --zone=public --list-ports`	List open ports in zone
`sudo firewall-cmd --zone=public --add-port=8080/tcp --permanent`	Open a TCP port
`sudo firewall-cmd --zone=public --add-port=4000-4500/tcp --permanent`	Open a port range
`sudo firewall-cmd --zone=public --remove-port=8080/tcp --permanent`	Close a port

Rich Rules

Rich rules allow fine-grained control over source, destination, port, and action.

`firewall-cmd --zone=public --list-rich-rules`	List rich rules in zone
`sudo firewall-cmd --zone=public --add-rich-rule='rule family="ipv4" source address="192.168.1.0/24" accept' --permanent`	Allow traffic from subnet
`sudo firewall-cmd --zone=public --add-rich-rule='rule family="ipv4" source address="203.0.113.10" reject' --permanent`	Reject traffic from IP
`sudo firewall-cmd --zone=public --add-rich-rule='rule family="ipv4" source address="192.168.1.0/24" port port="22" protocol="tcp" accept' --permanent`	Allow SSH from subnet
`sudo firewall-cmd --zone=public --remove-rich-rule='rule family="ipv4" source address="203.0.113.10" reject' --permanent`	Remove a rich rule

Masquerade (NAT)

Masquerading lets machines on a private network reach the internet through the firewall host.

`firewall-cmd --zone=public --query-masquerade`	Check if masquerading is enabled
`sudo firewall-cmd --zone=public --add-masquerade --permanent`	Enable masquerading
`sudo firewall-cmd --zone=public --remove-masquerade --permanent`	Disable masquerading

Logging

Control which denied packets are logged to help with debugging.

`firewall-cmd --get-log-denied`	Show current log-denied setting
`sudo firewall-cmd --set-log-denied=all`	Log all denied packets
`sudo firewall-cmd --set-log-denied=unicast`	Log denied unicast only
`sudo firewall-cmd --set-log-denied=off`	Disable denied-packet logging

Common Server Setup

Baseline rules for a web server using firewalld.

`sudo firewall-cmd --set-default-zone=public`	Set zone to public
`sudo firewall-cmd --zone=public --add-service=ssh --permanent`	Keep SSH access
`sudo firewall-cmd --zone=public --add-service=http --permanent`	Allow HTTP
`sudo firewall-cmd --zone=public --add-service=https --permanent`	Allow HTTPS
`sudo firewall-cmd --reload`	Activate all permanent rules
`firewall-cmd --zone=public --list-all`	Verify active rules