firewalld Zone-based firewall

CONCEPTS

Without --zone, commands act on the default zone. Without --permanent, they change only the running firewall and are lost on reload or reboot.

Packet arrives on an interface or from a source
↓ matched to
Zone trust level
↓ checked against
Services, ports, rich rules allowed traffic
↓ otherwise
Zone target default: reject

Runtime and permanent are two separate configs. Test with a runtime change, then keep it with --runtime-to-permanent.

STATE AND RELOAD

firewall-cmd --state
Check the daemon is running

firewall-cmd --reload
Reload permanent config, drop runtime changes

firewall-cmd --runtime-to-permanent
Save runtime config as permanent

systemctl enable --now firewalld
Start the daemon now and at boot

ZONES

firewall-cmd --get-zones
List all zone names

firewall-cmd --get-active-zones
Zones with interfaces or sources

firewall-cmd --get-default-zone
Show the default zone

firewall-cmd --set-default-zone=*<zone>*
Change the default zone

firewall-cmd --list-all
Show a zone's full config

firewall-cmd --zone=*<zone>* **--list-all**
Inspect a specific zone

SERVICES AND PORTS

firewall-cmd --add-service=*<service>*
Allow a named service

firewall-cmd --remove-service=*<service>*
Stop allowing a service

firewall-cmd --list-services
Services allowed in a zone

firewall-cmd --add-port=*<port>***/tcp**
Open a TCP port

firewall-cmd --add-port=*<from>***-***<to>***/udp**
Open a UDP port range

firewall-cmd --remove-port=*<port>***/tcp**
Close a port

firewall-cmd --list-ports
Ports open in a zone

firewall-cmd --add-service=*<service>* **--timeout=10m**
Allow temporarily, auto-revert

RICH RULES

firewall-cmd --add-rich-rule='*<rule>***'**
Add a rule with conditions

firewall-cmd --list-rich-rules
Show rich rules in a zone

firewall-cmd --remove-rich-rule='*<rule>***'**
Remove a rule, exact text

Rich rule shapes

Goal	Rule
Block a host	`rule family="ipv4" source address="<ip>" reject`
Port from subnet	`rule family="ipv4" source address="<cidr>" port port="<port>" protocol="tcp" accept`
Service with rate	`rule service name="<service>" accept limit value="1/m"`
Log then drop	`rule family="ipv4" source address="<cidr>" log prefix="fw " level="warning" drop`