

Network Firewall

Software Firewall (Runs on operating system)

Hardware Firewall (Dedicated network appliance)

Modern Linux uses firewalld as front-end & nftables under the hood

- organises rules by "zones" (like public, home, work)
- exposes "services" (ssh, http, samba, nfs, etc.)
- temporary changes are active immediately but vanish on reload
- permanent changes are written to disk and take effect after reload
- unspecified zone will be applied to the default (public) zone
- services not on --list-all can be enabled by opening specific ports

Examples

- allow SSH from jump hosts
- open http/https on a web server
- open NFS only to specific subnets

Exam

- start/enable firewall, list zones, see active zone
- add/remove a service, open/close a port, make changes permanent
- reload, create, or use a custom XML service file
- basic rich rules for blocking a specific source IP
- temporary vs permanent

Basic Commands

dnf install firewalld	install firewalld
systemctl enable --now firewalld	enable now
systemctl status firewalld	details & uptime
firewall-cmd --state	status
firewall-cmd --get-active-zones	
firewall-cmd --get-zones	list predefined zone profiles <ul style="list-style-type: none">• public - locked down default• home/work - more relaxed• trusted - allow all• dmz/external - edge scenarios
firewall-cmd --list-all	shows all zones, rules, services (only a few enabled by default)

firewall-cmd --get-services	list of all services that can be a
firewall-cmd --reload	write permanent and custom r

Adding and Removing Temporary and Permanent Rules

firewall-cmd --add-service=http	add http (temporary)
firewall-cmd --permanent --add-service=http	add http (permanent)
firewall-cmd --remove-service=http	remove http (temporary)
firewall-cmd --permanent --remove-service=http	remove http (permanent)
firewall-cmd --add-port=1110/tcp	add TCP 1110 (temporary)
firewall-cmd --permanent --add-port=1110/tcp	add TCP 1110 (permanent)
firewall-cmd --remove-port=1110/tcp	remove TCP 1110 (temporary)
firewall-cmd --permanent --remove-port=1110/tcp	remove TCP 1110 (permanent)
firewall-cmd --add-rich-rule='rule family="ipv4" source address="192.168.0.25" reject'	block incoming packets from s
firewall-cmd --remove-rich-rule='rule family="ipv4" source address="192.168.0.25" reject'	remove
firewall-cmd --add-icmp-block=echo-request	block icmp (ping) requests
firewall-cmd --remove-icmp-block=echo-request	remove
firewall-cmd --direct --add-rule ipv4 filter OUTPUT 0 -d 203.0.113.10 -j DROP	block outgoing packets to IP (p
firewall-cmd --direct --remove-rule ipv4 filter OUTPUT 0 -d 203.0.113.10 -j DROP	remove
nano /etc/firewalld/services/sap.xml	add a custom service definition
xml version="1.0" encoding="utf-8" <service version=1.0> <short>SAP</short> <description>Third-party application service</description> <port protocol="tcp" port="3200"/> </service>	xml header for firewalld
firewall-cmd --get-services grep -i sap	verify
firewall-cmd --add-service=sap	add the custom rule (temporar
firewall-cmd --permanent --add-service=sap	add the custom rule (permane

dnf install -y httpd	install apache web service
systemctl enable --now httpd	
curl -I http://localhost	verify (403 Forbidden)

curl -I http://192.168.50.164/	verify (403 Forbidden)
---	------------------------

Revision #2

Created 2026-07-05 06:22:39 UTC by Admin

Updated 2026-07-05 06:23:16 UTC by Admin