Cheatsheet firewalld

Zone Concept
Any network packet entering in the network stack is associated with a zone • If the packet comes from a network address bound to a zone then it is associated with this zone • if the packet comes from a network interface bound to a zone then it is associated with this zone • otherwise the packet is associated with the default zone

Zone management	Command
Check status	systemctl status firewalld
Get default zone	firewall-cmd --get-default-zonefirewall-cmd --get-active-zones
List zones with interfaces	firewall-cmd --get-active-zones
List all zones	firewall-cmd --get-zones
Change default zone	firewall-cmd –set-default-zone=home
Add interface to zone	firewall-cmd --permanent --zone=internal –change-interface=eth0
Modify zone	nmcli con mod "System eth0" connection.zone internal
Bring up zone	nmcli con up "System eth0"
List zone associated with eth0	firewall-cmd –get-zone-of-interface=eth0
List permanent information	firewall-cmd --permanent --zone=public --list-all
Create new zone	Firewall-cmd --permanent --new-zone=test
Add source to zone	firewall-cmd --permanent --zone=trusted --add-source=192.168.2.0/24
Remove source from zone	firewall-cmd --permanent --zone=trusted --remove-source=192.168.2.0/24
	firewall-cmd --permanent --zone=internal --add-service=http
Add port 443 to zone	firewall-cmd --zone=internal --add-port=443/tcp
Add new service	firewall-cmd –permanent –new-service=haproxy
Create direct rule	firewall-cmd --direct --add-rule ipv4 filter INPUT 0 -p tcp --dport 9000 -j ACCEPT
Reload firewall	firewall-cmd --reload