FirewallD Basic Commands

1. **How do you check the firewalld status?**
   systemctl status firewalld | grep active

```
[root@bharatitgyan ~]# systemctl status firewalld | grep active
   Active: active (running) since Sun 2024-02-18 16:59:32 IST; 2min 38s ago
[root@bharatitgyan ~]#
```

2. **To start the service and enable firewalld on boot:**
   systemctl start firewalld

```
[root@bharatitgyan ~]# systemctl start firewalld
[root@bharatitgyan ~]#
```

   systemctl enable firewalld

```
[root@bharatitgyan ~]# systemctl enable firewalld
[root@bharatitgyan ~]#
```

3. **To stop and disable it:**
   systemctl stop firewalld

```
[root@bharatitgyan ~]# systemctl stop firewalld
[root@bharatitgyan ~]#
```

   systemctl disable firewalld

```
[root@bharatitgyan ~]# systemctl disable firewalld
Removed symlink /etc/systemd/system/multi-user.target.wants/firewalld.s
ervice.
Removed symlink /etc/systemd/system/dbus-org.fedoraproject.FirewallD1.s
ervice.
[root@bharatitgyan ~]#
```

4. **How do you check the current configuration?**
   firewall-cmd --list-all --zone=[zone-name]

Firewall Basic commands

firewall-cmd --list-all --zone=public

```
root@bharatitgyan:~                                                    —  □  ×
[root@bharatitgyan ~]# firewall-cmd --list-all --zone=public
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: ens33
  sources:
  services: dhcpv6-client ssh
  ports:
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:

[root@bharatitgyan ~]#
```

5. How do you check the current services?
firewall-cmd --list-services

```
root@bharatitgyan:~                                                    —  □  ×
[root@bharatitgyan ~]# firewall-cmd --list-services
dhcpv6-client ssh
[root@bharatitgyan ~]#
```

6. How do you set a default zone in active?
firewall-cmd --set-default-zone [zone-name]
firewall-cmd --set-default-zone=home

```
root@bharatitgyan:~                                                    —  □  ×
[root@bharatitgyan ~]# firewall-cmd --set-default-zone=home
success
[root@bharatitgyan ~]#
```

7. How do you check default-zone?
firewall-cmd --get-default-zone [zone-name]
firewall-cmd --get-default-zone

```
root@bharatitgyan:~                                                    —  □  ×
[root@bharatitgyan ~]# firewall-cmd --get-default-zone
home
[root@bharatitgyan ~]#
```

Firewall Basic commands

8. How do you list all zones?

firewall-cmd --list-all-zones

```
root@bharatitgyan:~                                          —   □   ×
[root@bharatitgyan ~]#
[root@bharatitgyan ~]# firewall-cmd --list-all-zones
block
  target: %%REJECT%%
  icmp-block-inversion: no
  interfaces:
  sources:
  services:
  ports:
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:


dmz
  target: default
  icmp-block-inversion: no
  interfaces:
```

9. How do you check the ports open or not?

firewall-cmd --list-ports

```
root@bharatitgyan:~                                          —   □   ×
[root@bharatitgyan ~]# firewall-cmd --list-ports
80/tcp
[root@bharatitgyan ~]#
```

10. How do you open a port?

1) Open http port

firewall-cmd --zone=public --add-service=http

success

```
root@bharatitgyan:~                                          —   □   ×
[root@bharatitgyan ~]# firewall-cmd --zone=public --add-service=http
success
[root@bharatitgyan ~]#
```

firewall-cmd --zone=public --add-port=80/tcp

success

```
root@bharatitgyan:~                                          —   □   ×
[root@bharatitgyan ~]# firewall-cmd --zone=public --add-port=80/tcp
success
[root@bharatitgyan ~]#
```

Firewall Basic commands

2) Open https port
firewall-cmd --zone=public --add-service=https
success

```
root@bharatitgyan:~                                                    —  □  ×
[root@bharatitgyan ~]# firewall-cmd --zone=public --add-service=https
success
[root@bharatitgyan ~]#
```

firewall-cmd --zone=public --add-port=443/tcp
success

```
root@bharatitgyan:~                                                    —  □  ×
[root@bharatitgyan ~]# firewall-cmd --zone=public --add-port=443/tcp
success
[root@bharatitgyan ~]#
```

11. How do you close a port?
firewall-cmd --zone=public --remove-service=http
success

```
root@bharatitgyan:~                                                    —  □  ×
[root@bharatitgyan ~]# firewall-cmd --zone=public --remove-service=http
success
[root@bharatitgyan ~]#
```

firewall-cmd --zone=public --remove-port=80/tcp
success

```
root@bharatitgyan:~                                                    —  □  ×
[root@bharatitgyan ~]# firewall-cmd --zone=public --remove-port=80/tcp
success
[root@bharatitgyan ~]#
```

12. How do you make the firewall settings persistent?
firewall-cmd --permanent --zone=public --add-port=80/tcp

```
root@bharatitgyan:~                                                    —  □  ×
[root@bharatitgyan ~]# firewall-cmd --permanent --zone=public --add-port=80/tcp
success
[root@bharatitgyan ~]#
```

13. How do you reload the configuration?
firewall-cmd –reload

```
root@bharatitgyan:~                                                    —  □  ×
[root@bharatitgyan ~]# firewall-cmd --reload
success
[root@bharatitgyan ~]#
```

14. How do you change interfaces?
firewall-cmd --zone=public --change-interface=ens33

```
root@bharatitgyan:~                                          —   □   ×
[root@bharatitgyan ~]# firewall-cmd --zone=public --change-interface=ens33
success
[root@bharatitgyan ~]#
```

15. How do you add service in a specific zone?
firewall-cmd --add-service=ssh --zone=hpcsa

```
root@bharatitgyan:~                                          —   □   ×
[root@bharatitgyan ~]# firewall-cmd --add-service=ssh --zone=hpcsa
success
[root@bharatitgyan ~]#
```

16. How do you remove service in specific zones?
firewall-cmd --remove-service=http --zone=hpcsa

```
root@bharatitgyan:~                                          —   □   ×
[root@bharatitgyan ~]# firewall-cmd  --remove-service=http --zone=hpcsa
success
[root@bharatitgyan ~]#
```

17. How do you get running services in specific zones?
firewall-cmd --get-services | grep ssh

```
root@bharatitgyan:~                                          —   □   ×
[root@bharatitgyan ~]# firewall-cmd --get-services | grep ssh
RH-Satellite-6 RH-Satellite-6-capsule amanda-client amanda-k5-client amqp a
mqps apcupsd audit bacula bacula-client bgp bitcoin bitcoin-rpc bitcoin-tes
tnet bitcoin-testnet-rpc ceph ceph-mon cfengine condor-collector ctdb dhcp
dhcpv6 dhcpv6-client distcc dns docker-registry docker-swarm dropbox-lansyn
c elasticsearch etcd-client etcd-server finger freeipa-ldap freeipa-ldaps f
reeipa-replication freeipa-trust ftp ganglia-client ganglia-master git gre
high-availability http https imap imaps ipp ipp-client ipsec irc ircs iscsi
-target isns jenkins kadmin kerberos kibana klogin kpasswd kprop kshell lda
p ldaps libvirt libvirt-tls lightning-network llmnr managesieve matrix mdns
 minidlna mongodb mosh mountd mqtt mqtt-tls ms-wbt mssql murmur mysql nfs n
fs3 nmea-0183 nrpe ntp nut openvpn ovirt-imageio ovirt-storageconsole ovirt
-vmconsole plex pmcd pmproxy pmwebapi pmwebapis pop3 pop3s postgresql privo
xy proxy-dhcp ptp pulseaudio puppetmaster quassel radius redis rpc-bind rsh
 rsyncd rtsp salt-master samba samba-client samba-dc sane sip sips slp smtp
 smtp-submission smtps snmp snmptrap spideroak-lansync squid ssh steam-stre
aming svdrp svn syncthing syncthing-gui synergy syslog syslog-tls telnet tf
tp tftp-client tinc tor-socks transmission-client upnp-client vdsm vnc-serv
er wbem-http wbem-https wsman wsmans xdmcp xmpp-bosh xmpp-client xmpp-local
 xmpp-server zabbix-agent zabbix-server
[root@bharatitgyan ~]#
```

Firewall Basic commands

18. How do you check particular zone list all parameter?

firewall-cmd --zone=private --list-all

```
root@bharatitgyan:~                                                    —  □  ×
[root@bharatitgyan ~]# firewall-cmd --zone=private --list-all
private
  target: default
  icmp-block-inversion: no
  interfaces:
  sources:
  services:
  ports:
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:

[root@bharatitgyan ~]#
```

19. How do you check active zone?

firewall-cmd --get-active-zone

```
root@bharatitgyan:~                                                    —  □  ×
[root@bharatitgyan ~]# firewall-cmd --get-active-zone
public
  interfaces: ens33
[root@bharatitgyan ~]#
```

20. How do you add new zone?

firewall-cmd --permanent --new-zone=[zone-name]
e.g firewall-cmd --permanent --new-zone=BiG

```
root@bharatitgyan:~                                                    —  □  ×
[root@bharatitgyan ~]# firewall-cmd --permanent --new-zone=BiG
success
[root@bharatitgyan ~]#
```

21. How do you check interfaces in specific zone?

firewall-cmd --zone=public --list-interfaces

```
root@bharatitgyan:~                                                    —  □  ×
[root@bharatitgyan ~]# firewall-cmd --zone=public --list-interfaces
ens33
[root@bharatitgyan ~]#
```

22. How do you add multiple port in a specific zones?

firewall-cmd --add-port={443/tcp,53/udp,3336/tcp} --zone=hpcsa

```
root@bharatitgyan:~                                                    —  □  ×
[root@bharatitgyan ~]# firewall-cmd --add-port={443/tcp,53/udp,3336/tcp} --
zone=hpcsa
success
[root@bharatitgyan ~]#
```

BHARAT ITGYAN

Firewall Basic commands

23. **How do you add or remove range of port in specific zones?**
firewall-cmd --add-port=2500-3000/tcp --zone=hpcsa
firewall-cmd --remove-port=2500-3000/tcp --zone=hpcsa

```
[root@bharatitgyan ~]# firewall-cmd --add-port=2500-3000/tcp --zone=hpcsa
success
[root@bharatitgyan ~]# firewall-cmd --remove-port=2500-3000/tcp --zone=hpcsa
success
[root@bharatitgyan ~]#
```

24. **How do you add protocol?**
firewall-cmd --add-protocol=icmp --zone=hpcsa
firewall-cmd --remove-protocol=icmp --zone=hpcsa

```
[root@bharatitgyan ~]# firewall-cmd --add-protocol=icmp --zone=hpcsa
success
[root@bharatitgyan ~]# firewall-cmd --remove-protocol=icmp --zone=hpcsa
success
[root@bharatitgyan ~]#
```

25. **How do you add icmp block on that zone? (Go to this specific zone)**
firewall-cmd --add-icmp-block=echo-request --permanent;
firewall-cmd --reload

```
[root@bharatitgyan ~]# firewall-cmd --add-icmp-block=echo-request --permanent
success
[root@bharatitgyan ~]# firewall-cmd --reload
success
[root@bharatitgyan ~]#
```

26. **How do you remove icmp block from that zone?(Go to this specific zone)**
firewall-cmd --remove-icmp-block=echo-request --permanent;
firewall-cmd –reload

```
[root@bharatitgyan ~]# firewall-cmd --remove-icmp-block=echo-request --permanent;
success
[root@bharatitgyan ~]# firewall-cmd --reload;
success
[root@bharatitgyan ~]#
```

27. **How do you query icmp block from that zone?**
firewall-cmd --query-icmp-block=echo-request --permanent;
firewall-cmd --query-icmp-block=echo-reply --permanent;
firewall-cmd –reload

```
[root@bharatitgyan ~]# firewall-cmd --query-icmp-block=echo-request --permanent;
no
[root@bharatitgyan ~]# firewall-cmd --query-icmp-block=echo-reply --permanent;
no
[root@bharatitgyan ~]# firewall-cmd --reload
success
[root@bharatitgyan ~]#
```

28. How do you block ping?

firewall-cmd --add-icmp-block echo-request --zone=hpcsa

```
[root@bharatitgyan ~]# firewall-cmd --add-icmp-block echo-request --zone=hpcsa
success
[root@bharatitgyan ~]#
```

29. How do you unblock ping from all networks?

firewall-cmd --remove-icmp-block echo-request --zone=hpcsa

```
[root@bharatitgyan ~]# firewall-cmd --remove-icmp-block echo-request --zone=hpcsa
success
[root@bharatitgyan ~]#
```

30. How do you check if ping is blocked or note from all networks?

firewall-cmd --query-icmp-block echo-request --zone=hpcsa

```
[root@bharatitgyan ~]# firewall-cmd --query-icmp-block echo-request --zone=hpcsa
no
[root@bharatitgyan ~]#
```

31. How do you show all rich rules for specified zone?

firewall-cmd --permanent --zone=private --list-rich-rules

```
[root@bharatitgyan ~]# firewall-cmd --permanent --zone=private --list-rich-rules

[root@bharatitgyan ~]#
```

32. How do you write rich rule for ssh with log prefix and level?

firewall-cmd --add-rich-rule='rule family=ipv4 source
address=192.168.1.0/24 service name=ssh log prefix=" Allow SSH
Access" level="notice" accept'

```
[root@bharatitgyan ~]# firewall-cmd --add-rich-rule='rule family=ipv4 source addr
ess=192.168.1.0/24 service name=ssh log prefix="Allow SSH Access" level="notice"
accept'
success
[root@bharatitgyan ~]#
```

OR

33. How do you write rich rule for ssh without log prefix and level?

firewall-cmd --add-rich-rule='rule family=ipv4 source
address=192.168.1.0/24 service name=ssh accept'

```
[root@bharatitgyan ~]# firewall-cmd --add-rich-rule='rule family=ipv4 source addr
ess=192.168.1.0/24 service name=ssh accept'
success
[root@bharatitgyan ~]#
```

Firewall Basic commands

firewall-cmd --permanent --zone=testing --add-rich-rule='rule family=ipv4 source address=10.0.0.0/24 destination address=192.168.0.10/32 port port=8080-8090 protocol=tcp accept'

```
root@bharatitgyan:~                                              —    □    ×
[root@bharatitgyan ~]# firewall-cmd --permanent --zone=BiG --add-rich-rule='rule family=
ipv4 source address=10.0.0.0/24 destination address=192.168.0.10/32 port port=8080-8090
protocol=tcp accept'
success
[root@bharatitgyan ~]#
```

34. How do you Allow FTP connection only?

firewall-cmd --add-rich-rule='rule family=ipv4 source address=192.168.1.2/32 port port=21 protocol=tcp accept'

```
root@bharatitgyan:~                                              —    □    ×
[root@bharatitgyan ~]# firewall-cmd --add-rich-rule='rule family=ipv4 source address=
192.168.1.2/32 port port=21 protocol=tcp accept'
success
[root@bharatitgyan ~]#
```

35. How do you reject ping requests from all hosts with error message?

firewall-cmd --add-rich-rule='rule protocol value=icmp reject'

```
root@bharatitgyan:~                                              —    □    ×
[root@bharatitgyan ~]# firewall-cmd --add-rich-rule='rule protocol value=icmp reject'
success
[root@bharatitgyan ~]#
```

36. How do you open a port for web access?

firewall-cmd --zone=private --add-port=80/tcp --permanent
firewall-cmd --zone=private --add-port=443/tcp --permanent
firewall-cmd –reload

```
root@bharatitgyan:~                                              —    □    ×
[root@bharatitgyan ~]# firewall-cmd --zone=BiG --add-port=80/tcp --permanent
success
[root@bharatitgyan ~]# firewall-cmd --zone=BiG --add-port=443/tcp --permanent
success
[root@bharatitgyan ~]# firewall-cmd --reload
success
[root@bharatitgyan ~]#
```

BHARAT ITGYAN