

1) check firewall installed or not , if not then,

```
sudo apt install firewalld -y
```

2) check firewall is active or not

```
(kali㉿kali)-[~]
$ sudo systemctl status firewalld
o firewalld.service - firewalld - dynamic firewall daemon
  Loaded: loaded (/usr/lib/systemd/system/firewalld.service; disabled; preset: disabled)
  Active: inactive (dead)
  Docs: man:firewalld(1)

Aug 08 08:10:05 kali systemd[1]: Starting firewalld.service - firewalld - dynamic firewall daemon...
Aug 08 08:10:05 kali systemd[1]: Started firewalld.service - firewalld - dynamic firewall daemon.
Aug 08 08:18:25 kali systemd[1]: Stopping firewalld.service - firewalld - dynamic firewall daemon...
Aug 08 08:18:25 kali systemd[1]: firewalld.service: Deactivated successfully.
Aug 08 08:18:25 kali systemd[1]: Stopped firewalld.service - firewalld - dynamic firewall daemon.

(kali㉿kali)-[~]
$
```

3) active firewall first.

```
(kali㉿kali)-[~]
$ sudo systemctl start firewalld

(kali㉿kali)-[~]
$ sudo systemctl status firewalld
● firewalld.service - firewalld - dynamic firewall daemon
  Loaded: loaded (/usr/lib/systemd/system/firewalld.service; disabled; preset: disabled)
  Active: active (running) since Fri 2025-08-08 08:19:16 EDT; 1s ago
  Invocation: 5cf11a5b5760400a8808153c8fbd9338
  Docs: man:firewalld(1)
  Process: 11384 ExecStartPost=/usr/bin/firewall-cmd --state (code=exited, status=0/SUCCESS)
  Main PID: 11383 (firewalld)
  Tasks: 2 (limit: 4540)
  Memory: 28.5M (peak: 54.6M)
  CPU: 702ms
  CGroup: /system.slice/firewalld.service
          └─11383 /usr/bin/python3 /usr/sbin/firewalld --nofork --nopid

Aug 08 08:19:16 kali systemd[1]: Starting firewalld.service - firewalld - dynamic firewall daemon...
Aug 08 08:19:16 kali systemd[1]: Started firewalld.service - firewalld - dynamic firewall daemon.
```

4) list all firewall services

```
(kali㉿kali)-[~]  
$ firewall-cmd --list-all  
public (default, active)  
  target: default  
  ingress-priority: 0  
  egress-priority: 0  
  icmp-block-inversion: no  
  interfaces: eth0  
  sources:  
  services: dhcpv6-client ssh  
  ports:  
  protocols:  
  forward: yes  
  masquerade: no  
  forward-ports:  
  source-ports:  
  icmp-blocks:  
  rich rules:
```

5) list all service that firewall knew.

```
(kali㉿kali)-[~]  
$ firewall-cmd --get-services  
0-AD RH-Satellite-6 RH-Satellite-6-capsule afp alvr amanda-client amanda-k5-client amqp amqps anno-1602 anno-1800 apcupsd aseqnet audi  
ausweisapp2 bacula bacula-client bareos-director bareos-filedaemon bareos-storage bb bgp bitcoin bitcoin-rpc bitcoin-testnet bitcoin-  
estnet-rpc bittorrent-lsd ceph ceph-exporter ceph-mon cfengine checkmk-agent civilization-iv civilization-v cockpit collectd condor-co  
lector cratedb ctdb dds dds-multicast dds-unicast dhcp dhcpv6 dhcpv6-client distcc dns dns-over-quic dns-over-tls docker-registry dock  
r-swarm dropbox-lansync elasticsearch etcd-client etcd-server factorio finger foreman foreman-proxy freeipa-4 freeipa-ldap freeipa-lda  
s freeipa-replication freeipa-trust ftp galera ganglia-client ganglia-master git gpsd grafana gre high-availability http http3 https i  
ent imap imaps iperf2 iperf3 ipfs ipp ipp-client ipsec irc ircs iscsi-target isns jenkins kadmin kdeconnect kerberos kibana klogin kpa  
swd kprop kshell kube-api kube-apiserver kube-control-plane kube-control-plane-secure kube-controller-manager kube-controller-manager-  
ecure kube-nodeport-services kube-scheduler kube-scheduler-secure kube-worker kubelet kubelet-readonly kubelet-worker ldap ldaps libvi  
t libvirt-tls lightning-network llmnr llmnr-client llmnr-tcp llmnr-udp managesieve matrix mdns memcache minecraft minidlna mndp mongod  
mosh mountd mpd mqtt mqtt-tls ms-wbt mssql murmur mysql nbd nebula need-for-speed-most-wanted netbios-ns netdata-dashboard nfs nfs3 n  
ea-0183 nrpe ntp nut opentelemetry openvpn ovirt-imageio ovirt-storageconsole ovirt-vmconsole plex pmcd pmproxy pmwebapi pmwebapis pop  
pop3s postgresql privoxy prometheus prometheus-node-exporter proxy-dhcp ps2link ps3netsrv ptp pulseaudio puppetmaster quassel radius  
adsec rdp redis redis-sentinel rootd rpc-bind rquotad rsh rsyncd rtsp salt-master samba samba-client samba-dc sane settlers-history-co  
lection sip sips slimevr slp smtp smtp-submission smtps snmp snmptls snmptls-trap snmptrap spideroak-lansync spotify-sync squid ssdp s  
h statsrv steam-lan-transfer steam-streaming stellaris stronghold-crusader stun stuns submission supertuxkart svdrp svn syncthing sync  
hing-gui syncthing-relay synergy syscomlan syslog syslog-tls telnet tentacle terraria tftp tile38 tinc tor-socks transmission-client t  
rn turns upnp-client vdsms vnc-server vrrp warpinator wbem-http wbem-https wireguard ws-discovery ws-discovery-client ws-discovery-host  
ws-discovery-tcp ws-discovery-udp wsdd wsdd-http wsman wsmans xdmcp xmpp-bosh xmpp-client xmpp-local xmpp-server zabbix-agent zabbix-j  
va-gateway zabbix-server zabbix-trapper zabbix-web-service zero-k zerotier
```

6) see how many zones of firewall

```
File Actions Edit View Help
(kali㉿kali)-[~]
$ firewall-cmd --get-zones
block dmz drop external home internal nm-shared public trusted work

(kali㉿kali)-[~]
$
```

7) how many active zones ,check first.

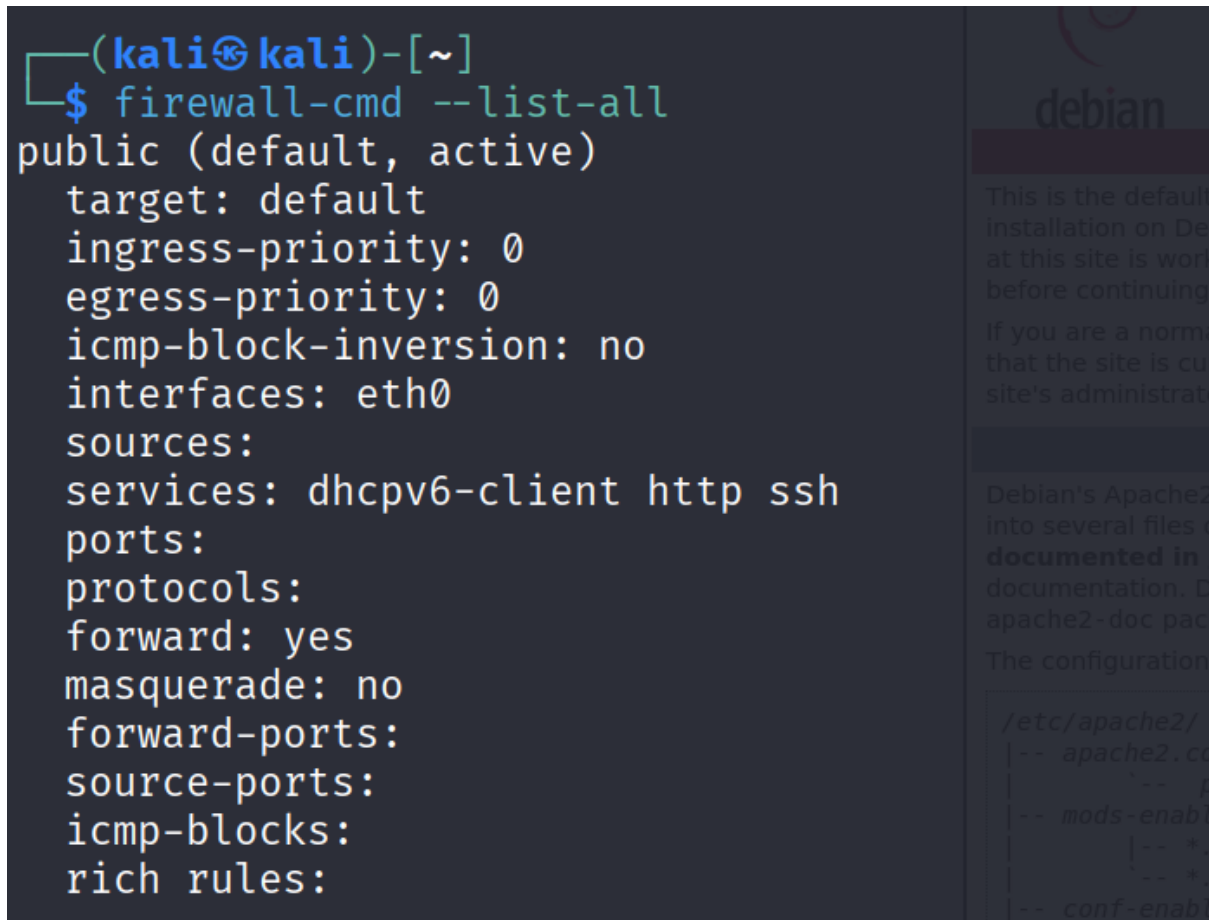
```
(kali㉿kali)-[~]
$ firewall-cmd --get-active-zones
public (default)
interfaces: eth0
```

8) add service in firewall rule.

```
File Actions Edit View Help
(kali㉿kali)-[~]
$ firewall-cmd --add-service=http
success
```

9) after adding a service, check again list of all services

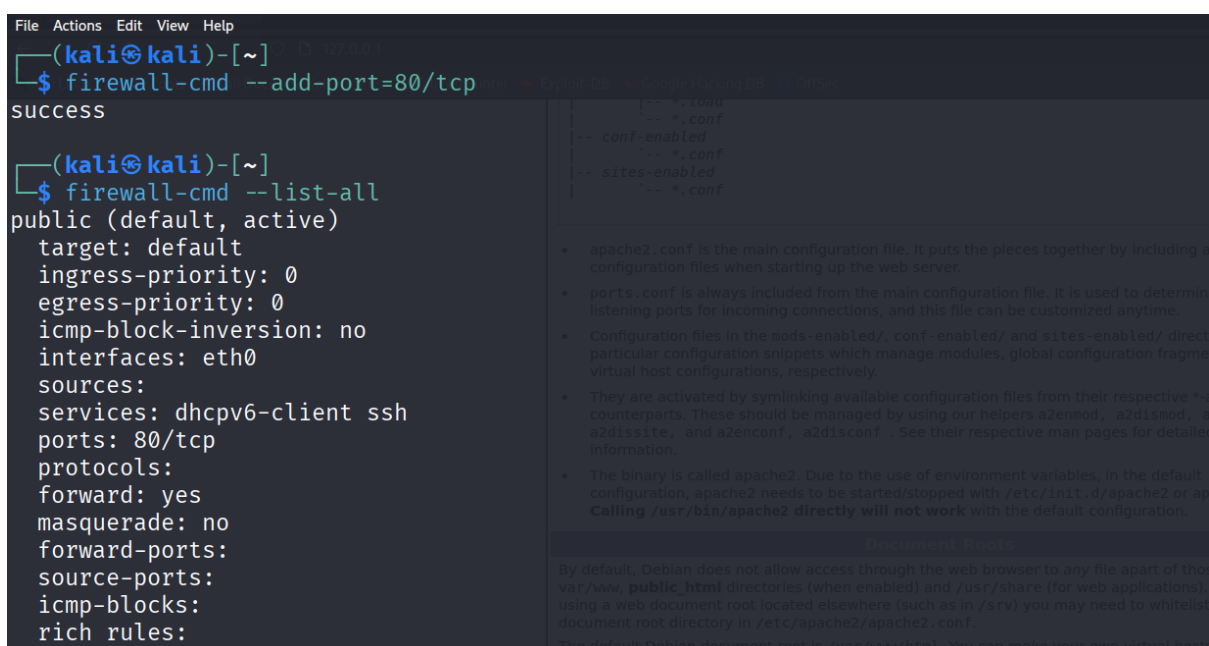
```
(kali㉿kali)-[~]
$ firewall-cmd --list-all
public (default, active)
  target: default
  ingress-priority: 0
  egress-priority: 0
  icmp-block-inversion: no
  interfaces: eth0
  sources:
  services: dhcpv6-client http ssh
  ports:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```



10) add a port instead of service

```
File Actions Edit View Help
(kali㉿kali)-[~]
$ firewall-cmd --add-port=80/tcp
success

(kali㉿kali)-[~]
$ firewall-cmd --list-all
public (default, active)
  target: default
  ingress-priority: 0
  egress-priority: 0
  icmp-block-inversion: no
  interfaces: eth0
  sources:
  services: dhcpv6-client ssh
  ports: 80/tcp
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```



11) block ip address that cant reach us,(192.168.29.96 cant reach)

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ firewall-cmd --add-rich-rule='rule family="ipv4" source address="192.168.29.96" reject'  
success  
tags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
inet 192.168.29.36 netmask 255.255.255.0 broadcast 192.168.29.255  
(kali@kali)-[~]  
$
```

```
File Actions Edit View Help  
(kali@kali)-[~]  
$ firewall-cmd --list-all  
public (default, active)  
target: default  
ingress-priority: 0  
egress-priority: 0  
icmp-block-inversion: no  
interfaces: eth0  
sources:  
services: dhcpv6-client ssh  
ports: 80/tcp  
protocols:  
forward: yes  
masquerade: no  
forward-ports:  
source-ports:  
icmp-blocks:  
rich rules:  
rule family="ipv4" source address="192.168.29.96" reject
```

```
Command Prompt  
C:\Users\Hope>ping 192.168.29.36  
  
Pinging 192.168.29.36 with 32 bytes of data:  
Reply from 192.168.29.36: bytes=32 time<1ms TTL=64  
Reply from 192.168.29.36: bytes=32 time<1ms TTL=64  
Reply from 192.168.29.36: bytes=32 time<1ms TTL=64  
Reply from 192.168.29.36: bytes=32 time=2ms TTL=64  
  
Ping statistics for 192.168.29.36:  
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
Minimum = 0ms, Maximum = 2ms, Average = 0ms  
  
C:\Users\Hope>ping 192.168.29.36  
  
Pinging 192.168.29.36 with 32 bytes of data:  
Reply from 192.168.29.36: Destination port unreachable.  
Reply from 192.168.29.36: Destination port unreachable.  
Reply from 192.168.29.36: Destination port unreachable.  
Reply from 192.168.29.36: Destination port unreachable.  
  
Ping statistics for 192.168.29.36:  
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
  
C:\Users\Hope>
```

12) block outgoing rule for a url or ip address

```
(kali㉿kali)-[~]  
└─$ ping www.facebook.com  
PING www.facebook.com (2a03:2880:f16e:81:face:b00c:0:25de) 56 data bytes  
64 bytes from edge-star-mini6-shv-01-pnq1.facebook.com (2a03:2880:f16e:81:face:b00c:0:25de): icmp_seq=1 ttl=57 time=191 ms  
64 bytes from edge-star-mini6-shv-01-pnq1.facebook.com (2a03:2880:f16e:81:face:b00c:0:25de): icmp_seq=2 ttl=57 time=29.6 ms  
64 bytes from edge-star-mini6-shv-01-pnq1.facebook.com (2a03:2880:f16e:81:face:b00c:0:25de): icmp_seq=3 ttl=57 time=32.2 ms  
^Z  
zsh: suspended ping www.facebook.com  
  
(kali㉿kali)-[~]  
└─$ host -t a www.facebook.com  
www.facebook.com is an alias for star-mini.c10r.facebook.com.  
star-mini.c10r.facebook.com has address 157.240.16.35  
  
(kali㉿kali)-[~]  
└─$ firewall-cmd --direct --remove-rule ipv4 filter OUTPUT 0 -d 157.240.242.35 -j DROP
```

After that we cant ping facebook.com