

# **BASIC COMMANDS OF FIREWALLD ON RHEL 8.4 SERVER**

## **Firewalld**

firewalld is a firewall management tool for Linux operating systems. A firewall is a way to protect machines from any unwanted traffic from outside. It enables users to control incoming network traffic on host machines by defining a set of firewall rules.

## **Installation**

```
#sudo yum install firewalld
```

**To start firewalld service, run the following command:**

```
#sudo systemctl start firewalld
```

**To enable firewalld service, run the following command:**

```
#sudo systemctl enable firewalld
```

**To stop firewalld service, run the following command:**

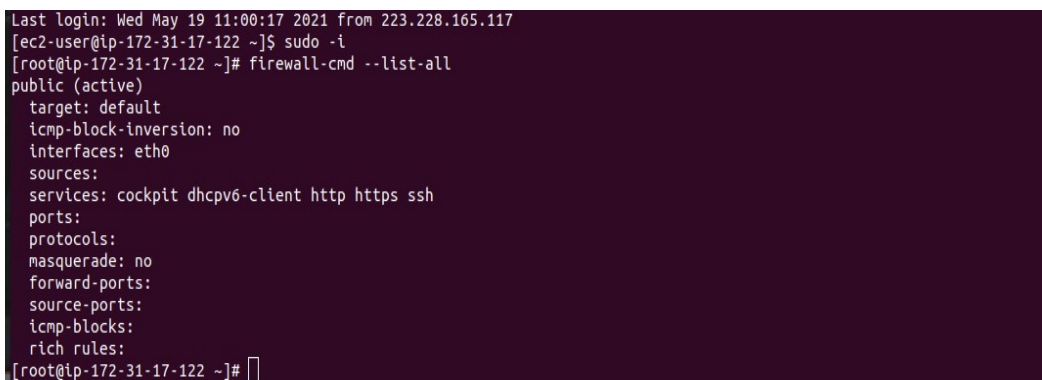
```
#sudo systemctl stop firewalld
```

**To get the status of the firewalld service**

```
#sudo systemctl status firewalld
```

## **To display the firewall settings**

```
#firewall-cmd --list-all (use this command as root user)
```



```
Last login: Wed May 19 11:00:17 2021 from 223.228.165.117
[ec2-user@ip-172-31-17-122 ~]$ sudo -i
[root@ip-172-31-17-122 ~]# firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: eth0
  sources:
  services: cockpit dhcpv6-client http https ssh
  ports:
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
[root@ip-172-31-17-122 ~]#
```

The --list-all option shows a complete overview of the firewalld settings

## Firewalld Zones

The firewalld daemon manages groups of rules using entities called “zones”. Firewalld can be used to separate networks into different zones according to the level of trust that the user has decided to place on the interfaces and traffic within that network

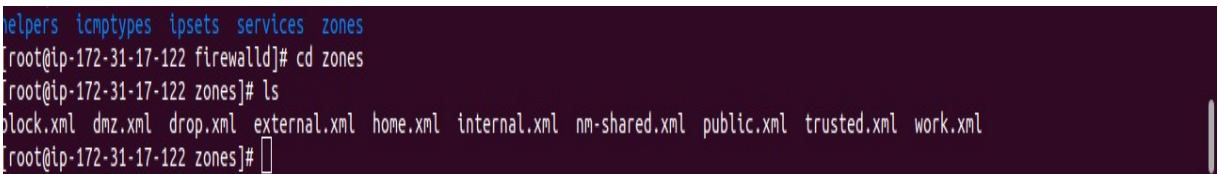
**You can list all available zones with the following command:**

```
#firewall-cmd --get-zones
```

**To list all the available zones:**

```
#cd /usr/lib/firewalld/zones  
#ls zones
```

You should see the following output:



```
helpers icmp types ipsets services zones  
[root@ip-172-31-17-122 firewalld]# cd zones  
[root@ip-172-31-17-122 zones]# ls  
block.xml dmz.xml drop.xml external.xml home.xml internal.xml nm-shared.xml public.xml trusted.xml work.xml  
[root@ip-172-31-17-122 zones]#
```

**Details of each zones given below:**

- **block** : This zone will reject all incoming network connections with an icmp-host-prohibited message.
- **Dmz** : This zone publicly-accessible with limited access to your internal network.
- **Drop** : This zone will drop all incoming network connections and only outgoing network connections allowed.
- **External** : This zone is used for the internal portion of a gateway especially for routers.
- **Home** : This zone is useful for home computers such as laptop and desktop.
- **Internal** : This zone is used for internal networks when other systems on this network are trusted.
- **Public** : This zone is used in untrusted public areas.
- **trusted** : This zone is used for dedicated servers connected to WAN.
- **work** : This zone is used for work machines where other systems on this network are trusted

**To see detailed information for all zones:**

```
# firewall-cmd --list-all-zones
```

For example:

```

ec2-user@ip-172-31-17-122 ~]$ sudo -i
root@ip-172-31-17-122 ~]# firewall-cmd --get-zones
lock dmz drop external home internal nm-shared public trusted work
root@ip-172-31-17-122 ~]# firewall-cmd --list-all-zones
lock
  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:
  sources:
  services: ssh
  ports:
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:

drop

```

To see the settings for particular information such as service or ports use a specific option. Get a list of option using the following command:

```
# firewall-cmd --help
```

### **ALLOW PORTS AND SERVICES IN FIREWALLD**

**You can allow ports and service in firewalld using the following commands:**

For example http service ;

```
#firewall-cmd --zone=public --add-service=http --permanent
```

```
#firewall-cmd --zone=public --add-service=https --permanent
```

### **To allow ports 21 and 25 in firewalld**

Example for ports;

```
#firewall-cmd --zone=public --add-port=21/tcp --permanent
```

```
#firewall-cmd --zone=public --add-port=25/tcp --permanent
```

In an emergency situation like system attack, it is possible to disable all network traffic using this command:

```
# firewall-cmd --panic-on
```

### (IMPORTANT)

Enabling panic mode stops all networking traffic. For this reason, it should be used only when you have the physical access to the machine or if you are logged in using a serial console)

➤ **To switch-off the panic mode**

```
# firewall-cmd --panic-off
```

➤ **To show the status**

```
#firewall-cmd --query-panic
```

## Controlling traffic with predefined services

The most straight forward method to control traffic is to add a predefined service to firewalld. This opens all necessary ports and modifies other settings according to the service definition file.

➤ **To see which services are allowed in the current zone:**

```
#firewall-cmd --list-services
```

```
Make sure polkit agent is running or run the application as superuser.
[ec2-user@ip-172-31-17-122 ~]$ sudo -i
[root@ip-172-31-17-122 ~]# firewall-cmd --list-services
cockpit dhcpv6-client http https ssh
[root@ip-172-31-17-122 ~]#
```

➤ **List all predefined services:**

```
#firewall-cmd --get-services
```

```
[ec2-user@ip-172-31-17-122 ~]$ sudo -i
[root@ip-172-31-17-122 ~]# firewall-cmd --list-services
cockpit dhcpv6-client http https ssh
[root@ip-172-31-17-122 ~]# firewall-cmd --get-services
RH-Satellite-6 amanda-client amanda-k5-client amqp amqps apcupsd audit bacula bacula-client bb bgp bitcoin bitcoin-rpc bitcoin-testnet bitcoin
-testnet-rpc bittorrent-lsd ceph ceph-mon cfengine cockpit collectd condor-collector ctdb dhcp dhcpv6 dhcpv6-client distcc dns dns-over-tls do
cker-registry docker-swarm dropbox-lansync elasticsearch etcd-client etcd-server finger freeipa-4 freeipa-ldap freeipa-ldaps freeipa-replicati
on freeipa-trust ftp galera ganglia-client ganglia-master git grafana gre high-availability http https imap imaps ipp ipp-client ipsec irc irc
s iscsi-target isns jenkins kadmin kdeconnect kerberos kibana klogon kpasswd kprop kshell kube-apiserver ldap ldaps libvirt libvirt-tls lightn
ing-network llmnr managesieve matrix mdns memcache minidlna mongodb mosh mountd mqtt mqtt-tls ms-wbt mssql murmur mysql nfs nfs3 nmea-0183 nrp
e ntp nut openvpn ovirt-imageio ovirt-storageconsole ovirt-vmconsole plex pmcd pmpoxy pmwebapi pmwebapis pop3 pop3s postgresql privoxy promet
heus proxy-dhcp ptp pulseaudio puppetmaster quassel radius rdp redis redis-sentinel rpc-bind rquotad rsh rsyncd rtsp salt-master samba samba-c
lient samba-dc sane sip sips slp smtp smtp-submission smtps snmp snmptrap spideroak-lansync spotify-sync squid ssdp ssh steam-streaming svdrp
svn syncthing syncthing-gui synergy syslog syslog-tls telnet tentacle tftp tftp-client tile38 tinc tor-socks transmission-client upnp-client v
dsm vnc-server wbm-http wbm-https wsman wsmans xdmcp xmpp-bosh xmpp-client xmpp-local xmpp-server zabbix-agent zabbix-server
[root@ip-172-31-17-122 ~]#
```

➤ **Add a service to the allowed services:**

```
#firewall-cmd --add-service=<servicename>
```

➤ **To list all allowed port:**

```
#firewall-cmd --list-ports
```

➤ **To add a port:**

```
#firewall-cmd --add-port=(port-number)/(port-type)
```

### **Adding a port to redirect**

Using firewalld, you can set up ports redirection so that any incoming traffic that reaches a certain port on your system is delivered to another internal port of your choice or to an external port on another machine.

Before you redirect traffic from one port to another port, or another address, you have to know three things:

- which port the packets arrive at
- what protocol is used
- where you want to redirect them.

### **Why do we need port forwarding**

port forwarding is used to keep unwanted traffic off networks. Port forwarding allows remote computers (for example, computers on the Internet) to connect to a specific computer or service within a private local-area network (LAN).

### **To redirect a port to another port:**

```
#firewall-cmd --add-forward-port=port=(port-number):proto=tcp|udp|sctp|  
dccp:toport=(port-number)
```

### **Redirecting TCP port 80 to port 88 on the same machine**

#### **\_Redirect the port 80 to port 88 for TCP traffic:**

```
#firewall-cmd --add-forward-port=port=80:proto=tcp:toport=88
```

#### **Make the new settings persistent:**

```
#firewall-cmd --runtime-to-permanent
```

#### **Check that the port is redirected:**

```
#firewall-cmd --list-all
```

### **Removing TCP port 80 forwarded to port 88 on the same machine**

#### **List redirected ports:**

```
#firewall-cmd --list-forward-ports  
port=80:proto=tcp:toport=88:toaddr=
```

#### **Remove the redirected port from the firewall:**

```
#firewall-cmd --remove-forward-port=port=80:proto=tcp:toport=88:toaddr=
```

#### **Make the new settings persistent:**

```
#firewall-cmd --runtime-to-permanent
```