

1. firewalld

- Linux 2.2 ipchains / 가 2.4
- iptables netfilter 가
- iptables iptables 가
- iptables RHEL/CentOS 7 iptables firewalld firewall-cmd , GUI 가 firewall-config
- firewall-cmd firewalld
-reload 가
firewall-cmd -permanent 가
firewall-cmd -reload
- firewalld 가

	firewall-cmd	firewall-cmd -permanent
(firewall-cmd -reload)		

- firewall-cmd 가
firewall-cmd -reload
- firewall-cmd -permanent 가
firewall-cmd -reload
가

2.

```
# ( running, not running )
[root@dns ~] firewall-cmd --state #

#not running
[root@dns ~] systemctl enable firewalld # 가

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

3.

```
[root@dns ~] yum install firewalld #
[root@dns ~] systemctl start firewalld #
[root@dns ~] systemctl enable firewalld #
```

4. IP

IP

```
#IP
[root@dns ~] firewall-cmd --permanent --add-source=10.10.10.10

#IP
[root@dns ~] firewall-cmd --permanent --remove-source=10.10.10.10
```

IP

```
#IP
[root@dns ~] firewall-cmd --permanent --add-source=10.10.10.0/24

#IP
[root@dns ~] firewall-cmd --permanent --remove-source=10.10.10.0/24
```

- /24 IP
10.10.10.0 10.10.10.255

```
# [root@dns ~] firewall-cmd --permanent --add-port=80/tcp  
# [root@dns ~] firewall-cmd --permanent --remove-port=80/tcp
```

```
# [root@dns ~] firewall-cmd --permanent --add-port=1000-2000/tcp  
# [root@dns ~] firewall-cmd --permanent --remove-port=1000-2000/tcp
```

IP

```
#IP
[root@dns ~] firewall-cmd --permanent --add-rich-rule='rule family="ipv4"
source address=10.10.10.10 port port="80" protocol="tcp" accept'

#IP
[root@dns ~] firewall-cmd --permanent --remove-rich-rule='rule family="ipv4"
source address=10.10.10.10 port port="80" protocol="tcp" accept'
```

IP

```
#IP
[root@dns ~] firewall-cmd --permanent --add-rich-rule='rule family="ipv4"
source address=10.10.10.10 drop'

#IP
[root@dns ~] firewall-cmd --permanent --remove-rich-rule='rule family="ipv4"
source address=10.10.10.10 drop'
```

Rule

```
#      Rule
[root@dns ~] firewall-cmd --reload

#      Rule
[root@dns ~] firewall-cmd --list-all
```

5. Network Zone

- firewalld
 - zone
 - zone
 - zone

```
[root@dns ~] sudo firewall-cmd --get-zones

work drop internal external trusted home dmz public block
```

- zone
 - zone
 - zone
 - zone

```
[root@dns ~] sudo firewall-cmd --list-all-zones
```

```
dmz
target: default
icmp-block-inversion: no
interfaces:
sources:
services: ssh
ports:
protocols:
masquerade: no
forward-ports:
sourceports:
icmp-blocks:
rich rules:
```

```
internal
target: default
icmp-block-inversion: no
interfaces:
sources:
services: dhcpcv6-client mdns samba-client ssh
ports:
protocols:
masquerade: no
forward-ports:
sourceports:
icmp-blocks:
rich rules:
```

- zone services zone
, dmz ssh , internal dhcpcv6-client, mdns
- zone --get-active-zone
zone public .(default)

```
[root@dns ~] firewall-cmd --get-active-zone
```

```
public
interfaces: eno0
```

(--list-all)

- --list-all

- dmz 10022 port가

```
[root@dns ~] sudo firewall-cmd --list-all

dmz (active)
target: default
icmp-block-inversion: no
interfaces: enp5s0f0 enp5s0f1
sources:
services: ssh http https
ports: 10022/tcp 2120-2121/tcp 20/tcp 2120-2142/tcp 10000/tcp
protocols:
masquerade: no
forward-ports:
source-ports:
icmp-blocks:
rich rules:
```

- `--set-default-zone={ZONE_NAME}`

dmz

```
[root@dns ~] firewall-cmd --set-default-zone=dmz
```

- firewalld zone `--new-zone`

zone webserver

```
[root@dns ~] firewall-cmd --permanent --new-zone=webserver
```

- firewalld `--reload`

firewalld

6.

- firewalld `-get-services`

```
[root@dns ~] firewall-cmd --get-services
RH-Satellite-6 RH-Satellite-6-capsule amanda-client amanda-k5-client amqp
```

amqps apcupsd audit bacula bacula-client bgp bitcoin bitcoin-rpc bitcoin-testnet bitcoin-testnet-rpc ceph ceph-mon cfengine condor-collector ctdb dhcp dhcpcv6 dhcpcv6-client distcc dns docker-registry docker-swarm dropbox-lansync elasticsearch etcd-client etcd-server finger freeipa-ldap freeipa-ldaps freeipa-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 ldap ldaps libvirt libvirt-tls lightning-network llmnr managesieve matrix mdns minidlna mongodb mosh mountd mqtt mqtt-tls ms-wbt mssql murmur mysql nfs nfs3 nmea-0183 nrpe ntp nut openvpn ovirt-imageio ovirt-storageconsole ovirt-vmconsole plex pmcd pmproxy pmwebapi pmwebapis pop3 pop3s postgresql privoxy 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-streaming svdrp **svn** syncthing syncthing-gui synergy syslog syslog-tls telnet tftp tftp-client tinc tor-socks transmission-client upnp-client vdsm vnc-server wbem-http wbem-https wsman wsmans xdmcp xmpp-bosh xmpp-client xmpp-local xmpp-server zabbix-agent zabbix-server

가


```
[root@dns ~] firewall-cmd --permanent --zone=webserver --add-service=http  
[root@dns ~] firewall-cmd --permanent --zone=webserver --add-service=http
```

- **`-remove-service=SERVICENAME`** [http/https://](http://https://)

```
[root@dns ~] firewall-cmd --permanent --zone=webserver --remove-service=http  
[root@dns ~] firewall-cmd --permanent --zone=webserver --remove-  
service=https
```

Tip

```
firewall-cmd --state #  
  
firewall-cmd --get-zones # Zone  
  
firewall-cmd --get-default-zone # Zone
```

```
firewall-cmd --list-all #      ↵      /  
firewall-cmd --reload #
```

Troubleshooting

Failed to restart firewalld.service: Unit is masked.

- mask 가 가 , , 가 firewalld 가 가 restart
· , unmask ·

```
[root@dns ~] systemctl unmask firewalld
```

- [firewall-cmd error on polkit](#)

Ref

- [firewalld](#)
 - [\[Linux\] firewalld](#)
 - [\[CentOS 7\] Firewalld](#)
 - [CentOS 7 \(Firewall\) IP](#)
 - [\[CentOS 7\] - firewall-cmd](#)
- , [linux](#), [centos](#), [firewall](#), [firewalld](#),

From:

<http://rwiki.repia.com/> -

. - 2023.12

Permanent link:

<http://rwiki.repia.com/doku.php?id=wiki:os:linux:firewall&rev=1647232038>



Last update: **2022/03/14 13:27**