



链滴

# Centos7 防火墙设置续

作者: [pplsunny](#)

原文链接: <https://ld246.com/article/1540628893470>

来源网站: [链滴](#)

许可协议: [署名-相同方式共享 4.0 国际 \(CC BY-SA 4.0\)](#)



## Centos7防火墙设置续

在 Centos 7 或 RHEL 7 或 Fedora 中防火墙由 firewalld 来管理，而不是 iptables。

### 一、firewalld 防火墙

语法命令如下：启用区域端口和协议组合

```
firewall-cmd [--zone=<zone>] --add-port=<port>[-<port>]/<protocol> [--timeout=<seconds>]
```

此举将启用端口和协议的组合。

端口可以是一个单独的端口 `<port>` 或者是一个端口范围 `<port>-<port>`。

协议可以是 tcp 或 udp。

#### 查看 firewalld 状态

```
[root@ppl ~]# systemctl status firewalld
● firewalld.service - firewalld - dynamic firewall daemon
  Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; vendor preset: enabled)
  Active: active (running) since Thu 2018-10-18 23:06:22 EDT; 1 weeks 1 days ago
    Docs: man:firewalld(1)
  Main PID: 673 (firewalld)
  CGroup: /system.slice/firewalld.service
          └─673 /usr/bin/python -Es /usr/sbin/firewalld --nofork --nopid
```

```
Oct 18 23:06:19 ppl systemd[1]: Starting firewalld - dynamic firewall daemon...
```

```
Oct 18 23:06:22 ppl systemd[1]: Started firewalld - dynamic firewall daemon.
```

```
[root@ppl ~]#
```

## 开启 firewalld

```
systemctl start firewalld
```

## 开放端口

```
// --permanent 永久生效,没有此参数重启后失效  
firewall-cmd --zone=public --add-port=80/tcp --permanent  
firewall-cmd --zone=public --add-port=1000-2000/tcp --permanent
```

## 示例

```
[root@ppl ~]# firewall-cmd --zone=public --add-port=3306/tcp --permanent  
success  
[root@ppl ~]#
```

## 重新载入

```
[root@ppl ~]# firewall-cmd --reload  
success  
[root@ppl ~]#
```

## 查看

```
[root@ppl ~]# firewall-cmd --zone=public --query-port=3306/tcp  
yes  
[root@ppl ~]#
```

## 删除

```
[root@ppl ~]# firewall-cmd --zone=public --remove-port=3306/tcp --permanent  
success  
[root@ppl ~]# firewall-cmd --reload  
success  
[root@ppl ~]# firewall-cmd --zone=public --query-port=3306/tcp  
no  
[root@ppl ~]#
```

## 二、iptables 防火墙

也可以还原传统的管理方式使用 iptables

```
systemctl stop firewalld  
systemctl mask firewalld
```

## 安装 iptables-services

```
yum install iptables-services
```

## 设置开机启动

```
systemctl enable iptables
```

## 操作命令

```
systemctl stop iptables  
systemctl start iptables  
systemctl restart iptables  
systemctl reload iptables
```

### 保存设置

```
service iptables save
```

### 开放某个端口 在 /etc/sysconfig/iptables 里添加

```
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 8080 -j ACCEPT
```

---

技术改变人生 Q群: 702101215

爱学习: [www.aixx123.com](http://www.aixx123.com)

---