CentOS7+ 使用 Firewalld 防火墙

作者：alenx

原文链接：https://ld246.com/article/1531790565434

来源网站：链滴

介绍

FirewallD 提供了支持网络/防火墙区域(zone)定义网络链接以及接口安全等级的动态防火墙管理工具
它支持 IPv4, IPv6 防火墙设置以及以太网桥接，并且拥有运行时配置和永久配置选项。它也支持允许
务或者应用程序直接添加防火墙规则的接口。

安装

```
$ yum install firewalld
$ yum install firewall-config
```

zone

Firewall 能将不同的网络连接归类到不同的信任级别。

```
$ firewall-cmd --list-all-zones    #查看所有zone信息
```

Zone 提供了以下几个级别：

- drop: 丢弃所有进入的包，而不给出任何响应
- block: 拒绝所有外部发起的连接，允许内部发起的连接
- public: 允许指定的进入连接
- external: 同上，对伪装的进入连接，一般用于路由转发
- dmz: 允许受限制的进入连接
- work: 允许受信任的计算机被限制的进入连接，类似 workgroup
- home: 同上，类似 homegroup
- internal: 同上，范围针对所有互联网用户
- trusted: 信任所有连接

过滤规则

- source: 根据源地址过滤
- interface: 根据网卡过滤
- service: 根据服务名过滤
- port: 根据端口过滤
- icmp-block: icmp 报文过滤，按照 icmp 类型配置
- masquerade: ip 地址伪装
- forward-port: 端口转发
- rule: 自定义规则

过滤规则的优先级遵循如下顺序

1. source

2. interface

3. firewalld.conf

使用

```
$ systemctl start firewalld        # 启动
$ systemctl stop firewalld         # 关闭
$ systemctl enable firewalld       # 开机启动
$ systemctl disable firewalld      # 取消开机启动
```

具体的规则管理，可以使用 firewall-cmd,具体的使用方法

```
$ firewall-cmd --help

--zone=NAME                    # 指定 zone
--permanent                    # 永久修改，--reload 后生效
--timeout=seconds              # 持续效果，到期后自动移除，用于调试，不能与 --permanent
时使用
```

查看规则

查看运行状态

```
$ firewall-cmd --state
```

查看已被激活的 Zone 信息

```
$ firewall-cmd --get-active-zones
public
  interfaces: eth0 eth1
```

查看指定接口的 Zone 信息

```
$ firewall-cmd --get-zone-of-interface=eth0
public
```

查看指定级别的接口

```
$ firewall-cmd --zone=public --list-interfaces
eth0
```

查看指定级别的所有信息，譬如 public

```
$ firewall-cmd --zone=public --list-all
public (default, active)
  interfaces: eth0
  sources:
```

```
  services: dhcpv6-client http ssh
  ports:
  masquerade: no
  forward-ports:
  icmp-blocks:
  rich rules:
```

查看所有级别被允许的信息

```
$ firewall-cmd --get-service
```

查看重启后所有 Zones 级别中被允许的服务，即永久放行的服务

```
$ firewall-cmd --get-service --permanent
```

管理规则

```
$ firewall-cmd --panic-on          # 丢弃
$ firewall-cmd --panic-off         # 取消丢弃
$ firewall-cmd --query-panic       # 查看丢弃状态
$ firewall-cmd --reload            # 更新规则，不重启服务
$ firewall-cmd --complete-reload   # 更新规则，重启服务
```

添加某接口至某信任等级，譬如添加 eth0 至 public，永久修改

```
$ firewall-cmd --zone=public --add-interface=eth0 --permanent
```

设置 public 为默认的信任级别

```
$ firewall-cmd --set-default-zone=public
```

a. 管理端口

列出 dmz 级别的被允许的进入端口

```
$ firewall-cmd --zone=dmz --list-ports
```

允许 tcp 端口 8080 至 dmz 级别

```
$ firewall-cmd --zone=dmz --add-port=8080/tcp
```

允许某范围的 udp 端口至 public 级别，并永久生效

```
$ firewall-cmd --zone=public --add-port=5060-5059/udp --permanent
```

b. 网卡接口

列出 public zone 所有网卡

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

将 eth0 添加至 public zone，永久

```
$ firewall-cmd --zone=public --permanent --add-interface=eth0
```

eth0 存在与 public zone，将该网卡添加至 work zone，并将之从 public zone 中删除

```
$ firewall-cmd --zone=work --permanent --change-interface=eth0
```

删除 public zone 中的 eth0，永久

```
$ firewall-cmd --zone=public --permanent --remove-interface=eth0
```

c. 管理服务

添加 smtp 服务至 work zone

```
$ firewall-cmd --zone=work --add-service=smtp
```

移除 work zone 中的 smtp 服务

```
$ firewall-cmd --zone=work --remove-service=smtp
```

d. 配置 external zone 中的 ip 地址伪装

查看

```
$ firewall-cmd --zone=external --query-masquerade
```

打开伪装

```
$ firewall-cmd --zone=external --add-masquerade
```

关闭伪装

```
$ firewall-cmd --zone=external --remove-masquerade
```

e. 配置 public zone 的端口转发

要打开端口转发，则需要先

```
$ firewall-cmd --zone=public --add-masquerade
```

然后转发 tcp 22 端口至 3753

```
$ firewall-cmd --zone=public --add-forward-port=port=22:proto=tcp:toport=3753
```

转发 22 端口数据至另一个 ip 的相同端口上

```
$ firewall-cmd --zone=public --add-forward-port=port=22:proto=tcp:toaddr=192.168.1.100
```

转发 22 端口数据至另一 ip 的 2055 端口上

```
$ firewall-cmd --zone=public --add-forward-port=port=22:proto=tcp:toport=2055:toaddr=1
2.168.1.100
```

f. 配置 public zone 的 icmp

查看所有支持的 icmp 类型

```
$ firewall-cmd --get-icmptypes
destination-unreachable echo-reply echo-request parameter-problem redirect router-adverti
ement router-solicitation source-quench time-exceeded
```

列出

```
$ firewall-cmd --zone=public --list-icmp-blocks
```

添加 echo-request 屏蔽

```
$ firewall-cmd --zone=public --add-icmp-block=echo-request [--timeout=seconds]
```

移除 echo-reply 屏蔽

```
$ firewall-cmd --zone=public --remove-icmp-block=echo-reply
```

g. IP 封禁

```
$ firewall-cmd --permanent --add-rich-rule="rule family='ipv4' source address='222.222.222.
22' reject"
```

当然，我们仍然可以通过 ipset 来封禁 ip

封禁 ip

```
$ firewall-cmd --permanent --zone=public --new-ipset=blacklist --type=hash:ip
$ firewall-cmd --permanent --zone=public --ipset=blacklist --add-entry=222.222.222.222
```

封禁网段

```
$ firewall-cmd --permanent --zone=public --new-ipset=blacklist --type=hash:net
$ firewall-cmd --permanent --zone=public --ipset=blacklist --add-entry=222.222.222.0/24
```

倒入 ipset 规则

```
$ firewall-cmd --permanent --zone=public --new-ipset-from-file=/path/blacklist.xml
```

然后封禁 blacklist

```
$ firewall-cmd --permanent --zone=public --add-rich-rule='rule source ipset=blacklist drop'
```

重新载入以生效

```
$ firewall-cmd --reload
```