CentOS7 防火墙详解

作者：pplsunny
原文链接：https://ld246.com/article/1540786075625
来源网站：链滴

CentOS7防火墙详解

centos 有两种防火墙 FirewallD和iptables防火墙。

centos7 使用的是FirewallD防火墙。

FirewallD 是 iptables 的前端控制器，用于实现持久的网络流量规则。它提供命令行和图形界面，在多数 Linux 发行版的仓库中都有。与直接控制 iptables 相比，使用 FirewallD 有两个主要区别：

FirewallD 使用区域和服务而不是链式规则。

它动态管理规则集，允许更新规则而不破坏现有会话和连接。

FirewallD 是 iptables 的一个封装，可以让你更容易地管理 iptables 规则 - 它并不是 iptables 的替品。虽然 iptables 命令仍可用于 FirewallD，但建议使用 FirewallD 时仅使用 FirewallD 命令。

1. firewalld的基本使用

- 启动： systemctl start firewalld

```
[root@ppl ~]# systemctl start firewalld
[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 Sun 2018-10-28 23:08:50 EDT; 2s ago
     Docs: man:firewalld(1)
 Main PID: 13750 (firewalld)
   CGroup: /system.slice/firewalld.service
           └─13750 /usr/bin/python -Es /usr/sbin/firewalld --nofork --nopid

Oct 28 23:08:49 ppl systemd[1]: Starting firewalld - dynamic firewall daemon...
```

```
Oct 28 23:08:50 ppl systemd[1]: Started firewalld - dynamic firewall daemon.
[root@ppl ~]#
```

- 关闭： systemctl stop firewalld

```
[root@ppl ~]# systemctl stop firewalld
[root@ppl ~]# systemctl status firewalld
● firewalld.service - firewalld - dynamic firewall daemon
   Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; vendor preset: enabled)
   Active: inactive (dead) since Sun 2018-10-28 23:07:40 EDT; 3s ago
     Docs: man:firewalld(1)
  Process: 673 ExecStart=/usr/sbin/firewalld --nofork --nopid $FIREWALLD_ARGS (code=exite
, status=0/SUCCESS)
 Main PID: 673 (code=exited, status=0/SUCCESS)

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.
Oct 28 23:07:39 ppl systemd[1]: Stopping firewalld - dynamic firewall daemon...
Oct 28 23:07:40 ppl systemd[1]: Stopped firewalld - dynamic firewall daemon.
[root@ppl ~]#
```

- 查看状态： systemctl status firewalld

```
[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 3 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 ~]#
```

- 开机禁用： systemctl disable firewalld
- 开机启用： systemctl enable firewalld

2. systemctl工具

systemctl是CentOS7的服务管理工具中主要的工具，它融合之前service和chkconfig的功能于一体。

启动一个服务：systemctl start firewalld.service

关闭一个服务：systemctl stop firewalld.service

重启一个服务：systemctl restart firewalld.service

显示一个服务的状态：systemctl status firewalld.service

在开机时启用一个服务：systemctl enable firewalld.service

在开机时禁用一个服务：systemctl disable firewalld.service

查看服务是否开机启动：systemctl is-enabled firewalld.service

```
[root@ppl ~]# systemctl is-enabled firewalld.service
enabled
[root@ppl ~]#
```

查看已启动的服务列表：systemctl list-unit-files|grep enabled

```
[root@ppl ~]# systemctl list-unit-files|grep enabled
auditd.service                              enabled
autovt@.service                             enabled
chronyd.service                             enabled
runlevel2.target                            enabled
runlevel3.target                            enabled
runlevel4.target                            enabled
[root@ppl ~]#
```

查看启动失败的服务列表：systemctl --failed

```
[root@ppl ~]# systemctl --failed
  UNIT           LOAD   ACTIVE SUB    DESCRIPTION
● postfix.service loaded failed failed Postfix Mail Transport Agent

LOAD   = Reflects whether the unit definition was properly loaded.
ACTIVE = The high-level unit activation state, i.e. generalization of SUB.
SUB    = The low-level unit activation state, values depend on unit type.

1 loaded units listed. Pass --all to see loaded but inactive units, too.
To show all installed unit files use 'systemctl list-unit-files'.
[root@ppl ~]#
```

3. 配置firewalld-cmd

查看版本： firewall-cmd --version

```
[root@ppl ~]# firewall-cmd --version
0.4.4.4
[root@ppl ~]#
```

查看帮助： firewall-cmd --help

显示状态： firewall-cmd --state

```
[root@ppl ~]# firewall-cmd --state
running
[root@ppl ~]#
```

查看所有打开的端口： firewall-cmd --zone=public --list-ports

```
[root@ppl ~]# firewall-cmd --zone=public --list-ports
80/tcp
[root@ppl ~]#
```

更新防火墙规则： firewall-cmd --reload

查看区域信息: firewall-cmd --get-active-zones

```
[root@ppl ~]#  firewall-cmd --get-active-zones
public
 interfaces: ens33
[root@ppl ~]#
```

查看指定接口所属区域： firewall-cmd --get-zone-of-interface=eth0

拒绝所有包：firewall-cmd --panic-on

取消拒绝状态： firewall-cmd --panic-off

查看是否拒绝： firewall-cmd --query-panic

4. 开启端口

- 添加

```
firewall-cmd --zone=public --add-port=80/tcp --permanent    （--permanent永久生效，没有参数重启后失效）
```

命令含义：

  - zone #作用域
  - add-port=80/tcp #添加端口，格式为：端口/通讯协议
  - permanent #永久生效，没有此参数重启后失效

- 重新载入

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

- 查看

```
[root@ppl ~]# firewall-cmd --zone=public --query-port=80/tcp
yes
[root@ppl ~]#
```

- 删除

```
[root@ppl ~]# firewall-cmd --zone=public --remove-port=80/tcp --permanent
success
```
