

firewalld特性

在新版本的CentOS7上使用的防火墙管理工具firewalld，代替的以往的iptables。尽管这样，在CentOS7上依然可以使用iptables，只需要下载安装iptables-services包。iptables-services中包含的iptables、ip6tables服务。

1. 新一代的动态防火墙管理工具firewalld引入了zone的概念。
2. 相对以iptables规则管理工具，firewalld提供了直接通过服务或程序名称添加防火墙规则的接口。例如直接添加服务名称http到防火墙放行规则中，则防火墙会自动放行httpd服务所用到的80端口。
3. firewalld管理的防火墙规则，可以动态生效，即重载防火墙，当前的网络连接不受影响。旧版本的iptables，规则的更改，都需要重新读取加载/etc/sysconfig/iptables所有规则，而firewalld可以动态加载规则文件，仅仅加载改变了的规则。
4. iptables 服务在 /etc/sysconfig/iptables 中储存配置，而 firewalld 将配置储存 /usr/lib/firewalld/ 和 /etc/firewalld/ 中的XML文件里。

firewalld配置文件

```
1 |— firewalld.conf           #主配置文件
2 |— icmptypes
3 |— lockdown-whitelist.xml
4 |— services                 #服务配置文件，可以添加
   自定义服务到firewalld支持的服务列表中
5 |   └─ nginx.xml           #服务配置文件
6 └─ zones                    #区域配置文件目录
   └─ public.xml             #区域配置文件
```

zone的理解

每一个zone都是一套防火墙的规则集合，即每一个不同的zone，都对应一个防火墙规则方案。firewalld默认有9个不同zone。这9个zone分别是：drop、block、public、external、dmz、work、home、internal、trusted，这些区域根据不同的网络状况划分。

firewalld-cmd命令

全局命令

查看帮助信息

```
1 | firewall-cmd --help
```

查看firewalld服务当前状态

```
1 | firewall-cmd --state
```

重新加载防火墙规则，并不会中断当前连接

```
1 | firewall-cmd --reload
```

区域管理

显示当前区域支持的列表

```
1 | firewall-cmd --get-zones
```

显示当前处于活动的区域

```
1 | firewall-cmd --get-active-zone
```

设置默认区域

```
1 #命令设置
2 firewall-cmd --set-default-zone=ZONE_NAME
3 #配置文件设置
4 vim /etc/firewalld/firewalld.conf
5 Default=ZONE_NAME
```

查看指定区域对应的接口

```
1 firewall-cmd --get-zone-of-interface=INTERFACE_NAME
```

为某个区域增加一个接口

```
1 #命令增加
2 firewall-cmd --zone=ZONE_NAME --add-
  interface=INTERFACE_NAME
3 #通过编译接口配置文件为某区域增加接口
4 vim /etc/sysconfig/network-scripts/ifcfg-eth0
5 ZONE=ZONE_NAME
```

从区域移除一个接口

```
1 firewall-cmd --zone=ZONE_NAME --remove-
  interface=INTERFACE_NAME
```

查看指定区域对应的接口

```
1 firewall-cmd --zone=ZONE_NAME --list-interfaces
```

查看某个区域的所有配置

```
1 firewall-cmd --zone=ZONE_NAME --list-all
```

查看所有区域的所有配置

```
1 firewall-cmd --list-all-zones
```

服务管理

显示当前区域打开的服务

```
1 firewall-cmd --list-services
```

查看区域默认支持的服务

```
1 firewall-cmd --get-service
```

添加一个服务到防火墙规则，可设置超时时间即生效时间

```
1 firewall-cmd --zone=ZONE_NAME --add-  
  service=SERVICE_NAME [--timeout=<seconds>]
```

移除某服务

```
1 firewall-cmd --zone=ZONE_NAME --remove-  
  service=SERVICE_NAME
```

查看指定区域是否启用某服务

```
1 firewall-cmd --zone=ZONE_NAME --query-  
  service=SERVICE_NAME
```

查看firewalld下次加载后生效的服务

```
1 firewall-cmd --get-service --permanent
```

添加自定义服务

```
1 # 复制模板  
2 cp /usr/lib/firewalld/service/SERVICE_NAME.xml  
  /etc/firewalld/service/SERVICE_NAME.xml  
3 # 修改服务的端口号等配置项  
4 vim /etc/firewalld/service/SERVICE_NAME.xml  
5     <?xml version="1.0" encoding="utf-8"?>  
6     <service>  
7         <short>nginx services</short>
```

```
8         <description>HTTP</description>
9         <port protocol="tcp" port="80"/>
10    </service>
11    # 重载firewalld
12    firewall-cmd --reload
13    # 添加服务
14    firewall-cmd --add-service=nginx
15    firewall-cmd --add-service=nginx --permanent
16    firewall-cmd - reload
```

端口/协议管理

列出指定区域中打开的端口

```
1 firewall-cmd --zone=ZONE_NAME --list-ports
```

打开tcp协议的N端口通信，端口号可以是连续的例如11-22

```
1 firewall-cmd --zone=ZONE_NAME --add-port=PORT/tcp
```

禁用某端口和协议的组合

```
1 firewall-cmd --zone=ZONE_NAME --remove-port=PORT/tcp
```

查询某端口协议组合是否开启

```
1 firewall-cmd --zone=ZONE_NAME --query-port=PORT/tcp
```

启用某区域的IP伪装功能

```
1 firewall-cmd --zone=ZONE_NAME --add-masquerade
```

禁用某区域的IP伪装功能

```
1 firewall-cmd --zone=ZONE_NAME --remove-masquerade
```

端口转发

```
1 firewall-cmd --permanent --zone=ZONE_NAME --add-forward-  
port=port=SPORT:proto=PROTOCOL:toport=DPORT:toaddr=DIP  
2 #示例。将访问192.168.1.150，22端口的请求转发至254端口  
3 firewall-cmd --permanent --zone=public --add-forward-  
port=port=254:proto=tcp:toport=22:toaddr=192.168.1.150
```

恐慌模式

在紧急状况，例如遭受攻击时开启此模式，在开启恐慌模式后，正处于连接状态的通信不会断开。

```
1 firewall-cmd --panic-on      #开启恐慌模式  
2 firewall-cmd --panic-off    #关闭恐慌模式  
3 firewall-cmd --query-panic  #查询当前状态开启或关闭
```

注意

1. 缺少--permanent选项，可以立即生效，但是临时的；使用--permanent选项永久生效，但需要重新加载或系统重启方可生效。
2. 区域配置文件在/usr/lib/firewalld/zone/目录下，但不建议修改此目录下的文件，可以修改/etc/firewalld/zone/目录下的文件，如果/etc/firewalld/zone/下没有相关区域配置文件，则可以复制/usr/lib/firewalld/zone/目录下的文件，然后进行修改配置。默认优先使用/etc/firewalld/zone/目录下的文件，如果/etc/firewalld/zone/目录下没有与/usr/lib/firewalld/zone/目录下同名的文件，则使用/etc/lib/firewalld/zone/目录下的文件。
3. 区域中添加服务：