Centos7系列（四）防火墙永久区域与富规则 推荐

原创 Mr大表哥 2017-05-17 07:59:25 评论(2) 976人阅读

博主QQ：819594300
博客地址：http://zpf666.blog.51cto.com/
有什么疑问的朋友可以联系博主，博主会帮你们解答，谢谢支持！

7）启用区域中的 IP 伪装功能（格式：firewall-cmd[--zone=区域] --add-masquerade）
说明：此操作启用区域的伪装功能。私有网络的地址将被隐藏并映射到一个公有IP。这是地址转换的一种形式，常用于路由。由于内核的限制，伪装功能仅可用于IPv4。
（外网卡的网卡接口在哪个区域，就在哪个区域启用IP地址伪装）
注意：启用伪装功能的主机同时也需要开启转发服务：
echo 1 > /proc/sys/net/ipv4/ip_forward
或
#vi /etc/sysctl.conf 添加如下内容
net.ipv4.ip_forward = 1
保存退出并执行#sysctl -p使修改生效

```
[root@localhost ~]# firewall-cmd --zone=external --add-masquerade
Warning: ALREADY_ENABLED
[root@localhost ~]#
```

警告：已启用

8）禁用区域中的 IP 伪装（格式：firewall-cmd[--zone=区域] --remove-masquerade）

```
[root@localhost ~]# firewall-cmd --zone=external --remove-masquerade
success
[root@localhost ~]#
```

9）查询区域的伪装状态（格式：firewall-cmd [--zone=区域] --query-masquerade）

```
[root@localhost ~]# firewall-cmd --zone=external --query-masquerade
no
[root@localhost ~]#
```

10）启用区域的 ICMP 阻塞功能（格式：firewall-cmd[--zone=区域] --add-icmp-block=icmp类型）

说明：此操作将启用选中的 Internet 控制报文协议（ICMP）报文进行阻塞。 ICMP 报文可以是请求信息或者创建的应答报文，以及错误应答。

```
[root@localhost ~]# firewall-cmd --zone=public --add-icmp-block=echo-request
success
[root@localhost ~]#
```

11）禁止区域的 ICMP 阻塞功能（格式：firewall-cmd[--zone=区域] --remove-icmp-block=icmp类型）

```
[root@localhost ~]# firewall-cmd --zone=public --remove-icmp-block=echo-request
success
[root@localhost ~]#
```

12）查询区域的 ICMP 阻塞功能（格式：firewall-cmd[--zone=区域] --query-icmp-block=icmp类型）

```
[root@localhost ~]# firewall-cmd --zone=public --query-icmp-block=echo-request
no
[root@localhost ~]#
```

13）在区域中启用端口转发或映射（格式：firewall-cmd [--zone=区域] --add-forward-port=port=portid[-portid]:proto=protocol[:toport=portid[-portid]][:toaddr=address[/mask]]）

说明：端口可以映射到另一台主机的同一端口，也可以是同一主机或另一主机的不同端口。端口号可以是一个单独的端口或者是端口范围 。协议可以为tcp或udp。目标端口可以是端口号或者是端口范围 。目标地址可以是 IPv4 地址。受内核限制，端口转发功能仅可用于IPv4。

例子：凡是来从external进来的22端口的数据包全部转发到另一台主机211.106.65.50。

```
[root@localhost ~]# firewall-cmd  --zone=external --add-forward-port=port=22:proto=tcp:toaddr=211.106.65.50
success
[root@localhost ~]#
```

14）禁止区域的端口转发或者端口映射（格式：firewall-cmd[--zone=] --remove-forward-port=port=portid[-portid]:proto=protocol[:toport=portid[-portid]][:toaddr=address[/mask]]）

```
[root@localhost ~]# firewall-cmd  --zone=external --remove-forward-port=port=22:proto=tcp:toaddr=211.106.65.5
0
success
[root@localhost ~]#
```

15）查询区域的端口转发或者端口映射（格式：firewall-cmd[--zone=]--query-forward-port=port=portid[-

portid]:proto=protocol[:toport=portid[-portid]][:toaddr=address[/mask]])

```
[root@localhost ~]# firewall-cmd  --zone=external --query-forward-port=port=22:proto=tcp:toaddr=211.106.65.50

no
[root@localhost ~]#
```

处理永久区域：

说明：永久选项不直接影响运行时的状态。这些选项仅在重载或者重启服务时可用。为了使用运行时和永久设置，需要分别设置两者。选项--permanent需要是永久设置的第一个参数。

1）获取永久选项所支持的服务

```
[root@localhost ~]# firewall-cmd --permanent --get-services
RH-Satellite-6 amanda-client bacula bacula-client dhcp dhcpv6 dhcpv6-client dns freeipa-ldap freeipa-ldaps fr
eeipa-replication ftp high-availability http https imaps ipp ipp-client ipsec iscsi-target kerberos kpasswd l
dap ldaps libvirt libvirt-tls mdns mountd ms-wbt mysql nfs ntp openvpn pmcd pmproxy pmwebapi pmwebapis pop3s
postgresql proxy-dhcp radius rpc-bind rsyncd samba samba-client smtp ssh telnet tftp tftp-client transmission
-client vdsm vnc-server wbem-https
[root@localhost ~]#
```

2）获取永久选项所支持的ICMP类型列表

```
[root@localhost ~]# firewall-cmd --permanent --get-icmptypes
destination-unreachable echo-reply echo-request parameter-problem redirect router-advertisement router-solici
tation source-quench time-exceeded
[root@localhost ~]#
```

3）获取支持的永久区域

```
[root@localhost ~]# firewall-cmd --permanent --get-zones
block dmz drop external home internal public trusted work
[root@localhost ~]#
```

4）配置防火墙在public区域打开http协议，并保存，以致重启有效

```
[root@localhost ~]# firewall-cmd --permanent --zone=public --add-service=http
success
[root@localhost ~]#
```

查看永久模式下public区域是否打开http服务。

```
[root@localhost ~]# firewall-cmd --permanent --zone=public --query-service=http
yes
[root@localhost ~]#
```

5）防火墙开放8080端口在public区域

```
[root@localhost ~]# firewall-cmd --permanent --zone=public --add-port=8080/tcp
success
[root@localhost ~]#
```

命令行配置富规则：

查看富规则（rule单词规则的意思）：

```
[root@localhost ~]# firewall-cmd --list-rich-rules
[root@localhost ~]#
```

没有结果显示，说明没建富策略

创建富规则：(以下是一些例子)

unrecognized arguments

无法识别的参数

全部释义和例句 试试人工翻译

```
[root@localhost ~]# firewall-cmd --add-rich-rule 'rule family=ipv4 source address=10.35.98.0/24 service name=
ftp log prefix=ftp level=info accept' --permanent
success
[root@localhost ~]#
[root@localhost ~]# firewall-cmd --add-rich-rule 'rule family=ipv4 source address=10.35.98.0/24 port port=80
protocol=tcp log prefix=80 level=info accept' --permanent
success
[root@localhost ~]#
[root@localhost ~]# firewall-cmd --add-rich-rule 'rule family=ipv4 source address=192.168.10.30 forward-port
port=808 protocol=tcp to-port=80 to-addr=10.10.10.2' --permanent
success
[root@localhost ~]#
```

富规则中使用伪装功能可以更精确详细的限制： （以下是例子）

```
[root@localhost ~]# firewall-cmd --add-rich-rule 'rule family=ipv4 source address=10.10.10.2/24 masquerade'
success
[root@localhost ~]# firewall-cmd --zone=public --list-all
public (default)
  interfaces:
  sources:
  services: dhcpv6-client ssh
  ports:
  masquerade: no
  forward-ports:
  icmp-blocks:
  rich rules:
        rule family="ipv4" source address="10.10.10.2/24" masquerade
```


仅允许部分IP访问本机服务配置： （以下是例子）

```
[root@localhost ~]# firewall-cmd --zone=public --add-rich-rule 'rule family=ipv4 source address=192.168.0.0/2
4 service name=http accept' --permanent
success
[root@localhost ~]#
```

禁止远程IP访问ssh： （以下是例子）

```
[root@localhost ~]# firewall-cmd --zone=public  --add-rich-rule 'rule family=ipv4 source address=192.168.0.0/
24 service name=ssh reject' --permanent
success
[root@localhost ~]#
```

reject:单词拒绝的意思

要想以上的永久富策略生效需要重载Firewalls防火墙。

删除上个例子rich规则：

```
[root@localhost ~]# firewall-cmd --zone=public --remove-rich-rule 'rule family=ipv4 source address=192.168.0.
0/24 service name=ssh reject' --permanent
success
[root@localhost ~]#
```

仅允许部分IP访问本机端口配置

```
[root@localhost ~]# firewall-cmd --zone=public --add-rich-rule 'rule family=ipv4 source address=192.168.0.0/2
4 port port=8080 protocol=tcp accept' --permanent
success
[root@localhost ~]#
```

创建rich规则，可以指定日志的前缀和输出级别：

```
[root@localhost ~]# firewall-cmd --zone=public --add-rich-rule 'rule family=ipv4 source address=192.168.0.4/2
4 port port=8080 protocol=tcp log prefix=proxy level=warning accept' --permanent
success
[root@localhost ~]#
```

指定了日志的日志可以在可以通过查看/var/log/messages日志文件。

端口转发。实验环境下，desktop访问server的5423端口，将访问server的80端口。

Server上的操作： （172.25.0.10是desktop的IP地址）

```
[root@localhost ~]# firewall-cmd --add-rich-rule 'rule family=ipv4 source address=172.25.0.10/32 forward-port
 port=5432 protocol=tcp to-port=80' --permanent
success
[root@localhost ~]#
```

192.168.10.0/24网段内的客户端不能访问主机的SSH

```
[root@localhost ~]# firewall-cmd --add-rich-rule 'rule family=ipv4 source address=192.168.10.0/24 service nam
e=ssh drop' --permanent
success
[root@localhost ~]#
```

其他渠道更改：也可通过配置以下XML文件，进行对防火墙的配置修改

```
[root@localhost ~]# cd /etc/firewalld/zones/
[root@localhost zones]# ls
public.xml  public.xml.old
[root@localhost zones]# vim public.xml
```

```
1  <?xml version="1.0" encoding="utf-8"?>
2  <zone>
3    <short>Public</short>
4    <description>For use in public areas. You do not trust the other computers on networks to not harm your
   computer. Only selected incoming connections are accepted.</description>
5    <service name="dhcpv6-client"/>
6    <service name="http"/>
7    <service name="ssh"/>
8    <port protocol="tcp" port="8080"/>
9    <rule family="ipv4">
10     <source address="192.168.10.30"/>
11     <forward-port to-addr="10.10.10.2" to-port="80" protocol="tcp" port="808"/>
12   </rule>
13   <rule family="ipv4">
14     <source address="192.168.0.0/24"/>
15     <port protocol="tcp" port="8080"/>
16     <accept/>
17   </rule>
18   <rule family="ipv4">
19     <source address="10.35.98.0/24"/>
20     <port protocol="tcp" port="80"/>
21     <log prefix="80" level="info"/>
22     <accept/>
23   </rule>
24   <rule family="ipv4">
25     <source address="10.35.98.0/24"/>
26     <service name="ftp"/>
27     <log prefix="ftp" level="info"/>
28     <accept/>
29   </rule>
30   <rule family="ipv4">
31     <source address="172.25.0.10/32"/>
32     <forward-port to-port="80" protocol="tcp" port="5432"/>
```

总结：

netfilter 防火墙总是容易受到规则顺序的影响，因为一条规则在链中没有固定的位置。在一条规则之前添加或者删除规则都会改变此规则的位置。在静态防火墙模型中，改变防火墙就是重建一个干净和完善的防火墙设置，默认链通常也没有安全的方式添加或删除规则而不影响其他规则。

动态防火墙有附加的防火墙功能链。这些特殊的链按照已定义的顺序进行调用，因而向链中添加规则将不会干扰先前调用的拒绝和丢弃规则。从而利于创建更为合理完善的防火墙配置。

通过iptables -vnL命令可以查看Firewalls防火墙最底层的表链（跟iptables防火墙跟相似）。

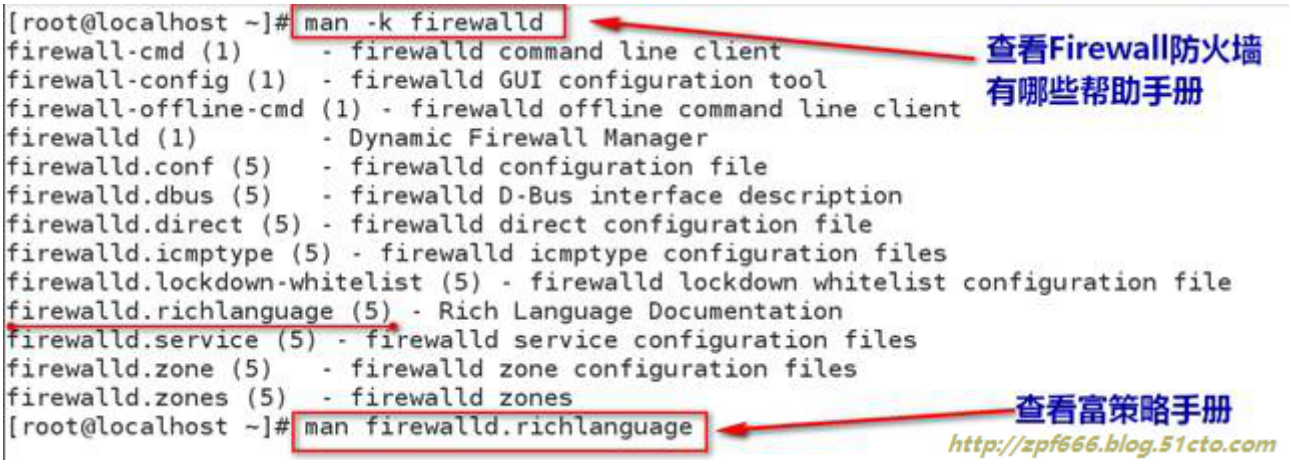
区域中表的链的匹配策略顺序是：

Log→deny→allow（说明：当有数据包通过时，log策略不对数据包做任何放行和阻止的操作，它只记录，不对数据包有任何影响。当deny和allow都没有的时候，默认当做deny对待）

firewall daemon 主要的配置工具是firewall-config。它支持防火墙的所有特性。管理员也可以用它来改变系统或用户策略。

命令行客户端firewall-cmd是命令行下提供大部分图形工具配置特性的工具。

附录：要想了解更多firewall防火墙更多知识可以查看firewall的相关手册页，：



例如：允许icmp协议的数据包通信