防火墙

1 iptables

2 firewalld

3 服务的访问控制列表

iptables

策略与规则链

- 在进行路由选择前处理数据包（PREROUTING）；
- 处理流入的数据包（INPUT）；
- 处理流出的数据包（OUTPUT）；
- 处理转发的数据包（FORWARD）；
- 在进行路由选择后处理数据包（POSTROUTING）。

基本的命令参数

参数	作用
-P	设置默认策略
-F	清空规则链
-L	查看规则链
-A	在规则链的末尾加入新规则
-I num	在规则链的头部加入新规则
-D num	删除某一条规则
-s	匹配来源地址IP/MASK，加叹号“!”表示除这个IP外
-d	匹配目标地址
-i网卡名称	匹配从这块网卡流入的数据
-o网卡名称	匹配从这块网卡流出的数据
-p	匹配协议，如TCP、UDP、ICMP
--dport num	匹配目标端口号

命令实例

```
[root@localhost ~]# iptables -F
[root@localhost ~]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
#默认INPUT全部允许
```

禁止ping

```
[root@localhost ~]# iptables -I INPUT -p icmp -j DROP
[root@localhost ~]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       icmp --  anywhere             anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
[root@localhost ~]#
```

查看规则

```
[root@localhost ~]# iptables -L -n --line-numbers
Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination
1    DROP       icmp --  0.0.0.0/0            0.0.0.0/0

Chain FORWARD (policy ACCEPT)
num  target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
num  target     prot opt source               destination
```

删除规则

```
[root@localhost ~]# iptables -D INPUT 1
[root@localhost ~]# iptables -L -n --line-numbers
Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
num  target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
num  target     prot opt source               destination
```

只允许指定网段的主机访问本机的22端口

```
[root@localhost ~]# iptables -I INPUT -s 192.168.9.0/24 -p tcp --dport
22 -j ACCEPT
[root@localhost ~]# iptables -A INPUT -p tcp --dport 22 -j REJECT
[root@localhost ~]# iptables -L -n --line-numbers
Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination
1    ACCEPT     tcp  --  192.168.9.0/24       0.0.0.0/0            tcp
dpt:22
2    REJECT     tcp  --  0.0.0.0/0            0.0.0.0/0            tcp
dpt:22 reject-with icmp-port-unreachable

Chain FORWARD (policy ACCEPT)
num  target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
num  target     prot opt source               destination
```

保存规则

```
[root@localhost ~]# service iptables save
iptables: Saving firewall rules to
/etc/sysconfig/iptables:[  确定  ]
```

保存出错时的解决方案

如果保存命令执行失败报出：

```
The service command supports only basic LSB actions (start, stop,
restart, try-restart, reload, force-reload, status). For other actions,
please try to use systemctl.
```

解决方案：

```
systemctl stop firewalld 关闭防火墙
yum install iptables-services 安装或更新服务
再使用systemctl enable iptables 启动iptables
最后 systemctl start iptables 打开iptables
再执行service iptables save


重启iptables服务
service iptables restart

执行完毕之后/etc/syscofig/iptables文件就有规则了
```

firewalld

firewalld

区域	默认策略规则
trusted	允许所有的数据包
home	拒绝流入的流量，除非与流出的流量相关；而如果流量与ssh、mdns、ipp-client、amba-client与dhcpv6-client服务相关，则允许流量
internal	等同于home区域
work	拒绝流入的流量，除非与流出的流量数相关；而如果流量与ssh、ipp-client与dhcpv6-client服务相关，则允许流量
public	拒绝流入的流量，除非与流出的流量相关；而如果流量与ssh、dhcpv6-client服务相关，则允许流量
external	拒绝流入的流量，除非与流出的流量相关；而如果流量与ssh服务相关，则允许流量
dmz	拒绝流入的流量，除非与流出的流量相关；而如果流量与ssh服务相关，则允许流量
block	拒绝流入的流量，除非与流出的流量相关
drop	拒绝流入的流量，除非与流出的流量相关

终端管理工具

参数	作用
--get-default-zone	查询默认的区域名称
--set-default-zone=<区域名称>	设置默认的区域，使其永久生效
--get-zones	显示可用的区域
--get-services	显示预先定义的服务
--get-active-zones	显示当前正在使用的区域与网卡名称
--add-source=	将源自此IP或子网的流量导向指定的区域
--remove-source=	不再将源自此IP或子网的流量导向某个指定区域
--add-interface=<网卡名称>	将源自该网卡的所有流量都导向某个指定区域
--change-interface=<网卡名称>	将某个网卡与区域进行关联
--list-all	显示当前区域的网卡配置参数、资源、端口以及服务等信息
--list-all-zones	显示所有区域的网卡配置参数、资源、端口以及服务等信息
--add-service=<服务名>	设置默认区域允许该服务的流量
--add-port=<端口号/协议>	设置默认区域允许该端口的流量
--remove-service=<服务名>	设置默认区域不再允许该服务的流量
--remove-port=<端口号/协议>	设置默认区域不再允许该端口的流量
--reload	让“永久生效”的配置规则立即生效，并覆盖当前的配置规则
--panic-on	开启应急状况模式
--panic-off	关闭应急状况模式

案例命令

```
[root@localhost ~]# firewall-cmd --get-default-zone \查询默认区域
[root@localhost ~]# firewall-cmd --get-zone-of-interface=eno16777736    \查询接口所属区域
[root@localhost ~]# firewall-cmd --permanent --zone=external --change-interface=eno16777736
\修改接口区域
[root@localhost ~]# firewall-cmd --get-zone-of-interface=eno16777736    \获取接口区域
[root@localhost ~]# firewall-cmd --permanent --get-zone-of-interface=eno16777736
external    \永久模式下查询
[root@localhost ~]# firewall-cmd --set-default-zone=public  \设置默认区域
[root@localhost ~]# firewall-cmd --get-default-zone     \查询默认区域
public
[root@localhost ~]# firewall-cmd --zone=public --query-service=ssh
[root@localhost ~]# firewall-cmd --zone=public --query-service=https
[root@localhost ~]# firewall-cmd --zone=public --query-service=ssh
[root@localhost ~]# firewall-cmd --zone=public --query-service=https
[root@localhost ~]# firewall-cmd --zone=public --add-service=https
[root@localhost ~]# firewall-cmd --zone=public --add-service=https --permanent
[root@localhost ~]# firewall-cmd --reload
```

案例命令

```
[root@localhost ~]# firewall-cmd --zone=public --add-port=8080-8081/tcp
--permanent
success
[root@localhost ~]# firewall-cmd --zone=public --list-ports --permanent
8080-8081/tcp
[root@localhost ~]# firewall-cmd --zone=public --add-forward-
port=port=888:proto=tcp:toport=22:toaddr=192.168.179.142
success
[root@localhost ~]# firewall-cmd --reload
success
[root@localhost ~]# firewall-cmd --permanent --zone=public --add-rich-
rule="
rule family="ipv4" source address="192.168.179.0/24" service name="ssh"
reject"
    \\拒绝192.168.179.0/24所有用户访问本机ssh
success
```

TCP Wrappers

TCP Wrappers

TCP Wrappers是RHEL 7系统中默认启用的一款流量控制程序，它能够根据来访主机的地址与本机的目标服务程序作出允许或拒绝的操作。

系统将会先检查允许控制列表文件（/etc/hosts.allow），如果匹配到相应的允许策略则放行流量；如果没有匹配，则去进一步匹配拒绝控制列表文件（/etc/hosts.deny），若找到匹配项则拒绝该流量。如果这两个文件全都没有匹配到，则默认放行流量。

在配置TCP Wrappers服务时需要遵循两个原则：

- 编写拒绝策略规则时，填写的是服务名称，而非协议名称；
- 建议先编写拒绝策略规则，再编写允许策略规则，以便直观地看到相应的效果。

规则

客户端类型	示例	满足示例的客户端列表
单一主机	192.168.10.10	IP地址为192.168.10.10的主机
指定网段	192.168.10.	IP段为192.168.10.0/24的主机
指定网段	192.168.10.0/255.255.255.0	IP段为192.168.10.0/24的主机
指定DNS后缀	.eagleslab.com	所有DNS后缀为.eagleslab.com的主机
指定主机名称	www.eagleslab.com	主机名称为www.eagleslab.com的主机
指定所有客户端	ALL	所有主机全部包括在内

```
[root@localhost ~]# vi /etc/hosts.deny
#
# hosts.deny          This file contains access rules which are used to
#                     deny connections to network services that either use
#                     the tcp_wrappers library or that have been
#                     started through a tcp_wrappers-enabled xinetd.
#
#                     The rules in this file can also be set up in
#                     /etc/hosts.allow with a 'deny' option instead.
#
#                     See 'man 5 hosts_options' and 'man 5 hosts_access'
#                     for information on rule syntax.
#                     See 'man tcpd' for information on tcp_wrappers
#
httpd:*
[root@localhost ~]# vi /etc/hosts.allow
#
# hosts.allow         This file contains access rules which are used to
#                     allow or deny connections to network services that
#                     either use the tcp_wrappers library or that have been
#                     started through a tcp_wrappers-enabled xinetd.
#
#                     See 'man 5 hosts_options' and 'man 5 hosts_access'
#                     for information on rule syntax.
#                     See 'man tcpd' for information on tcp_wrappers
#
httpd:192.168.179.
[root@localhost ~]#
```