# Linux 防火墙设置

linux 防火墙的工具有iptables、firewalld等....

## 一，iptable 命令

传统的iptables规则表有：fileter表（过滤规则表）、nat表（地址转换规则表）、

mangle表（修改数据标志位规则表）、raw表（跟踪数据表规则）。

每个规则表中包含多个数据链：INPUT（入站数据过滤）、OUTPUT（出站数据过滤）、

FORWARD（转发数据过滤）、PREROUTING（路由前过滤）和POSTROUTING（路由后过滤），防火墙则需要写入到和谐具体的数据链中。

如果是外部主机发送数据包给防火墙本机，数据将会经过PREROUTING链与INPUT链；如果是防火墙本机发送数据包到外部主机，数据将会经OUTPUT链与POSTROUTING链；如果防火墙作为路由负责转发数据，则数据将经过PREROUTING链、FORWARD链以及POSTROUTING链。

### iptables防火墙语法格式

命令描述：netfilter防火墙规则管理工具

用法：iptables [-t 表名] {-A|-D|-I|-D|-F|-L|-Z|-P} 链名 rule-specification

选项：

-t 制定需要维护的防火墙规则表，不使用-t时，则默认操作对象为filter表

-A 追加防火墙规则

-D 删除防火墙规则

-I 插入防火墙规则

-F 清空防火墙规则

-L 列出防火墙规则

-R 替换防火墙规则

-Z 情况防火墙数据包统计信息

-P 设置链默认规则

匹配参数：

[!] -p 匹配协议，!代表取反

[!] -s 匹配源地址

[!] -d 匹配目标地址

[!] -i 匹配入站网口接卡

[!] -o 匹配出站网口接卡

[!] --sport 匹配源端口

[!] --dport 匹配目标端口

[!] --src-range 匹配源地址范围

[!] --dst-range 匹配目标地址范围

[!] --limit 匹配数据表速率

[!] --mac-source 匹配源MAC地址

[!] --sports 匹配源端口

[!] --dports 匹配目标端口

[!] --state 匹配状态（INVALID,ESTABLISHED,NEW,RELATED）

[!] --string 匹配应用层字串

触发动作：

ACCEPT 允许数据包通过

DROP 丢弃数据包

REJECT 拒接数据包通过

LOG 将数据信息记录syslog日志

DNAT 目标地址转换

SNAT 源地址转换

MASQUERADE 地址欺骗

REDIRECT 重定向

iptables防火墙规则的非常重要，内核按顺序检查这些规则，如果发现有匹配的规则条目，在立刻执行相关动作，停止继续向下查找规则条目，如果所有的防火墙规则都未能匹配成功，则按照默认策略进行处理。

下面简单演示iptable命令的使用方法：

1，查看filter表的所有规则：

**[root@centos7 ~]# iptables -nL**

2，查看nat表的所有规则：

**[root@centos7 ~]# iptables -t nat -nL**

3，清空filter表中的所有规则：

**[root@centos7 ~]# iptables -F**

4，往filter表中添加一条新的入站规则，丢弃192.168.0.1主机发送给防火墙本机的所有数据包

**[root@centos7 ~]# iptables -A INPUT -s 192.168.0.1 -j DROP**

5，往filter表中插入一条新的入站规则，拒绝192.168.0.22ping防火墙本机

**[root@centos7 ~]# iptables -I INPUT -s 192.168.0.22 -p icmp -j REJECT**

6，查看filter表中防火墙规则并显示编号规则：

**[root@centos7 ~]# iptables -nL --line-number**

7，删除filter表中INPUT链的第一条规则：

**[root@centos7 ~]# iptables -D INPUT 1**

8，替换filter表中INPUT链的第二条规则，拒绝192.168.0.254之外的任何主机链接防火墙本机：

**[root@centos7 ~]# iptables -R INPUT ! -s 192.168.0.254 -j REJECT**

9，修改filter表中INPUT链的默认规则为接收数据包：

**[root@centos7 ~]# iptables -t filter -P INPUT ACCEPT**

10，将192.168.0.10主机发送给防火墙本机22端口的所有数据包信息记录到message日志：

**[root@centos7 ~]# iptables -I INPUT -s 192.168.0.10 -p tcp --dport 22 -j LOG**

11，允许任何主机从eno16777736网络接口访问防火墙本机的80端口：

**[root@centos7 ~]# iptables -I INPUT -i eno16777736 -p tcp --dport 80 -j ACCEPT**

### 常见iptables案例

案例1：允许任意客户端访问服务器主机提供的日常服务（HTTP、HTTPS、DNS、NTP、SMTP、POP3、SSH），在Linux系统中，/etc/services文件可以帮助我们找到各种服务所对应的标准端口信息。

[root@centos7 ~]# iptables -A INPUT -p tcp --dport 22 -J ACCEPT

[root@centos7 ~]# iptables -A INPUT -p tcp --dport 25 -J ACCEPT

[root@centos7 ~]# iptables -A INPUT -p tcp --dport 53 -J ACCEPT

[root@centos7 ~]# iptables -A INPUT -p udp --dport 53 -J ACCEPT

[root@centos7 ~]# iptables -A INPUT -p tcp --dport 80 -J ACCEPT

[root@centos7 ~]# iptables -A INPUT -p tcp --dport 110 -J ACCEPT

[root@centos7 ~]# iptables -A INPUT -p tcp --dport 143 -J ACCEPT

[root@centos7 ~]# iptables -A INPUT -p tcp --dport 123 -J ACCEPT

[root@centos7 ~]# iptables -P INPUT DROP

[root@centos7 ~]# iptables -P OUTPUT ACCEPT

案例2：公司拥有一个共有IP，使用防火墙实现局域网中的所有主机通过SNAT共享上网。使用CentOS 7作为公司软路由，公司内部所有192.168.0.0/24网段内的主机连接外网时，防火墙自动将所有数据表的源地址修改为路由器上的公有IP，最后互联网将信息返回路由后，有路由再转交给真正的后端主机。防火墙源地址转换（SNAT）规则需要被写入到NAT表的POSTROUTING链。

[root@centos7 ~]# vim /etc/sysctl.conf

# System default settings live in /usr/lib/sysctl.d/00-system.conf.

# To override those settings, enter new settings here, or in an /etc/sysctl.d/<name>.conf file

#

# For more information, see sysctl.conf(5) and sysctl.d(5).

# 开启路由转发，实现基于Linux的软路由功能

net.ipv4.ip\_forward = 1

[root@centos7 ~]# sysctl -p # 重新加载内核参数配置文件/etc/sysctl.conf

[root@centos7 ~]# iptables -t nat -I POSTROUTING -s 192.168.0.0/24 \

> -j SNAT --to-source 124.126.199.84

案例3：公司对外有一个公有IP，内部有HTTP、MAIL两台核心服务器，通过防火墙实现客户可以从互联网的任意位置访问位于公司内部的两台服务器资源。

[root@centos7 ~]# vim /etc/sysctl.conf

# System default settings live in /usr/lib/sysctl.d/00-system.conf.

# To override those settings, enter new settings here, or in an /etc/sysctl.d/<name>.conf file

#

# For more information, see sysctl.conf(5) and sysctl.d(5).

# 开启路由转发，实现基于Linux的软路由功能

net.ipv4.ip\_forward = 1

[root@centos7 ~]# sysctl -p # 重新加载内核参数配置文件/etc/sysctl.conf

[root@centos7 ~]# iptables -t nat -I PREROUTING -d 124.126.199.84 -p tcp --dport 80 \

> -j DNAT --to-destination 192.168.0.100

[root@centos7 ~]# iptables -t nat -I PREROUTING -d 124.126.199.84 -p tcp --dport 25 \

> -j DNAT --to-destination 192.168.0.100

[root@centos7 ~]# iptables -t nat -I PREROUTING -d 124.126.199.84 -p tcp --dport 110 \

> -j DNAT --to-destination 192.168.0.100

案例4：数据包因为太大无法一次完成数据的传输，此时数据包将被分割为数据片段再发送出去。接收端接收玩数据后，将把这些数据片段重新组合成完整的数据包。但问题在于当数据被分割后，只有前面的出事数据片段包含全部的数据头部信息（IP、TCP、UDP、ICMP等），后续的数据片段仅包含数据包头部信息的一部分。这时再去检查后续数据片段的头部信息是不可能的。当然，如果你想匹配第二个及后面被分片的数据，可以使用“-f”选项。

丢弃发送至192.168.1.1的所有数据以及分片数据：

[root@centos7 ~]# iptables -A OUTPUT -f -d 192.168.1.1 -j DROP

案例5：目前网络上的攻击手法层出不穷，很多攻击会采用发送大量无效的数据包给服务器，造成服务器无法响应正常的请求包，iptables提供了一个limit扩展功能，可以显示单位时间内的数据包的个数。下面的规则是当每秒钟数据包个数为500时接受入站连接，否则拒绝连接。

[root@centos7 ~]# iptables -I INPUT -m limit -- limit 500/sec -j ACCEPT

[root@centos7 ~]# ipatbles -P INPUT DROP

案例6：企业环境中，服务器会面临各种各样的中级，iptables本身属于三层过滤防火墙，但也提供了string扩展功能，同过--string也可以根据关键字限制网络连接。将下面两条记录写入基于Linux的软路由服务器防火墙规则中，实现拒绝转发包含有关键词/etc/passwd以及qq的数据包，也就是防止将密码文件复制出局域网，并防止内部员工访问QQ网址。

[root@centos7 ~]# iptables -I FORWARD -m string --algo bm --string "/etc/passwd" -j REJECT

[root@centos7 ~]# iptables -I FORWARD -m string --algo bm --string "qq" -j REJECT

案例7：根据数据连接状态设置防火墙规则，放行所有的出战数据包。拒绝入站的新连接请求于无效连接，放行入站的回应请求。

[root@centos7 ~]# iptables -F

[root@centos7 ~]# iptables -A INPUT -m state --state NEW -j DROP

[root@centos7 ~]# iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

[root@centos7 ~]# iptables -P OUTPUT ACCEPT

案例8：公司采用基于Linux的软路由设备，要求再路由设备上设置防火墙规则，记录192.168.0.1至192.168.0.22地址段内所有的主机发送给路由要求转发的数据包，并允许转发这些数据包。

[root@centos7 ~]# iptables -A FORWARD -m iprange --src-range 192.168.0.1-192.168.0.10 \

> -p tcp --dport 80 -j LOG

[root@centos7 ~]# iptables -A FORWARD -m iprange --src-range 192.168.0.1-192.168.0.10 \

> -p tcp --dport 80 -j ACCEPT

### 防火墙备份与还原

默认的iptables防火墙规则会立刻生效，但如果不保存，当计算机重启后所有的规则都将丢失，所以对防火墙规则进行及时保存的操作时非常必要的。iptables软件包提供了两个非常有用的工具，可以使用工具处理大量的防火墙规则。这两个工具的最大又是时处理庞大的贵额集时熟读非常快。CentOS7系统中防火墙规则默认保存再/etc/sysconfig/iptables文件中，使用iptables-save将规则保存至该文件中可以实现保存防火墙规则的作用，计算机重启后会自动加载该文件中的规则。如果使用iptables-save将规则保存至其他位置，可以实现备份防火墙规则的作用。当防火墙规则需要做还原操作时，可以使用iptables-restore将备份文件直接导入当前的防火墙规则。

[root@centos7 ~]# iptables-save > /etc/sysconfig/iptables

[root@centos7 ~]# iptables-save > firewall.bak

[root@centos7 ~]# iptables-restore < firewall.bak

## 二，firewalld 命令

firewalld将所有的网络流量都分类灰机到zones中，firewalld通过zones管理防火墙规则。每一个进入系统的数据包，都会首先检查她的源IP地址和接口（进出的网卡接口），如果地址与某个zone匹配，则该zone中的规则将生效。而每个zone都会有开启或关闭的服务和端口的列表，以实现允许或拒绝连接服务和端口。如果数据包的源IP地址和网卡接口都不能和任何zone匹配，则该数据包将匹配默认zone,一般情况下时一个名称为public的默认zone。

firewalld会提供block、dmz、drop、external、home、internal、public、trusted、work这九个zone。

大部分zone都定义的有自己的允许规则，规则通过端口/协议（631/udp）或者预定义的服务（ssh）这是形式设置，如果数据包没有匹配这些允许的规则，则该数据包一般会被防火墙拒绝。但又一个名称trusted的zone，默认会运行所有的数据流量，如果有一个数据包进入该zone，则被允许访问所有的资源。

具体的firewalld预定义zone及其描述信息：

zone名称 描述

trusted 允许所有入站流量

home 许其他主机入展访问本机的ssh，mdns，ipp-client或者dhcpv6-client

这些预定义服务。

本机访问其他主机后，对方返回的入站数据，都将被允许。

拒绝其他所有入站数据包

internal 允许其他主机入展访问本机的ssh，mdns，ipp-client或者dhcpv6-client

这些预定义服务。

本机访问其他主机后，对方返回的入站数据，都将被允许。

拒绝其他所有入站数据包（与home相同）

work 允许其他主机入站访问本机的ssh或dhcpv6-client这些预定义服务

本机访问其他主机后，对方返回的入站数据，都将被允许。

拒绝其他所有入站的数据包

external 允许其他主机入站访问本机的ssh服务

本机访问其他主机后，对方返回的入站数据，都将被允许

拒绝其他所有入站数据包

通过本zone进行转发的IPv4数据包，都将会进行NAT后再转发出（不

管数据包的真实来源IP是多少，该数据包的源地址会被修改为防火

墙本机出站网卡的IP地址）

dmz 允许其他主机入站访问本机的ssh服务

本机访问其他主机后，对方返回的入站数据，都将被允许

拒绝其他所有入站数据包

block 本机拒绝访问其他主机后，对方返回的入站数据，都将被允许

拒绝所有其他入站数据包

drop 本机访问其他主机后，对方返回的入站数据，都将被允许

丢弃掉所有其他入站的数据包

public 允许其他主机访问本机的ssh或dhcpv6-client这些预定义的服务

本机访问其他主机后，对方返回的入站数据，都将被允许

拒绝其他所有入站的数据包

### firewalld-cmd 命令格式

命令描述：firewalld防火墙规则管理工具

用法：firewalld-cmd [选项...]

选项：

--get-default-zone 获取默认zone信息

--set-default-zone=<zone> 设置默认zone

--get-active-zones 显示当前正在使用的zone信息

--get-zones 显示系统预定义的zone

--get-services 显示系统预定义的服务名称

--get-zone-of-interface=<interface> 查询某个接口与哪个zone匹配

--get-zone-of-source=<source>[/<mask>] 查询某个源地址与哪个zone匹配

--list-all-zones 显示所有的zone信息的所有规则

--add-service=<service> 向zone中添加允许访问的服务

--add-port=<portid>[-<portid>]/<protocol> 向zone中添加允许访问的端口

--add-interface=<interface> 将接口与zone绑定

--add-source=<source>[/<mask>] 将源地址与zone绑定

--list-all 列出某个zone的所有规则信息

--remove-service=<service> 从zone中移除允许某个服务的规则

--remove-port=<portid>[-<portid>]/<protocol>从zone中移除允许某个端口的规则

--remove-source=<source>[/<mask>] 将源地址与zone解除绑定

--remove-interface=<interface> 将网卡接口与zone解除绑定

--permanent 设置永久有效的规则，默认情况规则都是

临时的

--reload 重新加载防火墙规则

下面简单演示firewalld-cmd命令的使用方法：

1，查看默认zone，结果为trusted

[root@centos7 ~]# firewall-cmd --get-default-zone

2，设置默认的zone为trusted

[root@centos7 ~]# firewall-cmd --set-default-zone=trusted

3，显示当前正在使用的zone信息

[root@centos7 ~]# firewall-cmd --get-active-zones

4，显示系统预定义的zone，默认为九个zone

[root@centos7 ~]# firewall-cmd --get-zones

5，显示预定义的服务名称

[root@centos7 ~]# firewall-cmd --get-services

6，查询eno16777736接口与哪个zone匹配，网卡与trusted匹配，则该网卡的流量执行eno16777736中定义的规则，默认将允许访问所有服务

[root@centos7 ~]# firewall-cmd --get-zone-of-interface=eno16777763

7，显示所有zone及其对应的规则信息

[root@centos7 ~]# firewall-cmd --list-all-zones

8，在public这个zone中允许访问FTP服务规则

[root@centos7 ~]# firewall-cmd --add-service=ftp --zone=public

9，从public这个zone中删除允许访问FTP服务的规则

[root@centos7 ~]# firewall-cmd --remove-service=ftp --zone=public

10，在public这个zone中添加允许访问3306端口的规则

[root@centos7 ~]# firewall-cmd --add-port=3306/tcp --zone=public

11，从public这个zone中删除允许访问3306端口的规则

[root@centos7 ~]# firewall-cmd --remove-port=3306/tcp --zone=public

12，将eno16777736网卡与public绑定，以后从该接口进入的流量，匹配public中的规则

[root@centos7 ~]# firewall-cmd --add-interface=eno16777736 --zone=public

13，将eno16777736网卡接口与public解除绑定

[root@centos7 ~]# firewall-cmd --remove-interface=eno16777736 --zone=public

14，将源IP地址1.1.1.1与public绑定，以后该主机访问本机时匹配public的规则

[root@centos7 ~]# firewall-cmd --add-source=1.1.1.1 --zone=public

15，查看默认zone的规则列表

[root@centos7 ~]# firewall-cmd --list-all

16，查看public这个zone的规则列表

[root@centos7 ~]# firewall-cmd --list-all --zone=public

17，在public这个zone中添加一条永久规则（允许访问3306端口），该规则在重启防火墙后依然有效

[root@centos7 ~]# firewall-cmd --permanent --add-port=3306/tcp --zone=public

18，重新加载读取防火墙规则

[root@centos7 ~]# firewall-cmd --reload

注：在CentOS7 默认使用firewalld防火墙，若要使用iptables强的话，需要关闭firewalld防火墙，再配置iptables防火墙配置文件，在启动iptables服务。

[root@centos7 ~]# systemctl stop firewalld.service # 关闭firewalld防火墙

[root@centos7 ~]# systemctl disable firewalld.service # 禁止开机启动

[root@centos7 ~]# firewall-cmd --state # 查看firewalld防火墙状态

[root@centos7 ~]# yum -y install iptables-services # 安装iptables-service服务

[root@centos7 ~]# mv /etc/sysconfig/iptables.rpmnew /etc/sysconfig/iptables

[root@centos7 ~]# vim /etc/sysconfig/iptables # 编辑iptables配置文件

# sample configuration for iptables service

# you can edit this manually or use system-config-firewall

# please do not ask us to add additional ports/services to this default configuration

\*filter

:INPUT ACCEPT [0:0]

:FORWARD ACCEPT [0:0]

:OUTPUT ACCEPT [0:0]

-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT

-A INPUT -p icmp -j ACCEPT

-A INPUT -i lo -j ACCEPT

-A INPUT -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT

**-A INPUT -p tcp -m state --state NEW -m tcp --dport 80 -j ACCEPT**

**-A INPUT -p tcp -m state --state NEW -m tcp --dport 8080 -j ACCEPT**

-A INPUT -j REJECT --reject-with icmp-host-prohibited

-A FORWARD -j REJECT --reject-with icmp-host-prohibited

COMMIT

:wq! #保存退出

备注：这里使用80和8080端口为例。\*\*\*部分一般添加到“-A INPUT -p tcp -m state --state NEW -m tcp--dport 22 -j ACCEPT”行的上面或者下面，切记不要添加到最后一行，否则防火墙重启后不生效。

[root@centos7 ~]# systemctl restart iptables.service # 开启iptables防火墙服务

[root@centos7 ~]# systemctl enable iptables.service # 开机启动

如提示找不到iptables服务，则需要安装iptables-service软件包。

## 三，更多参考

<http://www.linuxso.com/linuxpeixun/10332.html>

