Security-04

服务安全与监控

# iptables防火墙

## 什么是防火墙？

一道保护性的安全屏障,起到保护、隔离的作用

主机型防火墙：只在本机运行的防火请服务，只保护本机

网络型防火墙：单独一台机器运行防火墙服务，保护一片区域

## Linux包过滤防火墙

RHEL7默认使用firewall作为防火墙，但firewalld底层还是调用包过滤防火墙iptables

]# systemctl stop firewalld

]# systemctl disabled firewalld

]# yum -y install iptables-services //安装软件包

]# yum -y install iptables //机器默认安装的，但未启动服务

]# rpm -qa | grep iptables

]# service iptables status //查看服务状态

]# service iptables start //启动服务

]# chkconfig iptables on //设置服务开机自起

## iptables的表，链结构

### 4张表

raw表：状态跟踪表

mangle表：包标记表—给到达防火墙主机的ip包打标签

nat表：INPUT链等4条地址转换表(源地址转换、目标地址转换、端口转换)

filter表（默认表）：过滤表

### 5种链（ip包传输的方向）

INPUT链：匹配进入防火墙主机的ip包

OUTPUT链：匹配从防火墙出去的ip包

FORWARD链：处理经过防火墙主机的ip包

PREROUTING链：路由前

POSTROUTING链：路由后

### 包过滤匹配流程

规则（匹配到达防火墙主机的ip包 存放在链里）

规则链内的匹配顺序

顺序比对，匹配即停止（LOG除外）

若无任何挂匹配，则按该链的默认策略处理

## IPtables用法解析

## 主机型防火墙

### IPtables基本用法

管理程序位置：/sbin/iptables

指令组成：iptables [-t表名] 选项 [链名] [条件] [-j 目标操作]

### 注意事项/整体规律

可以不指定表，默认为filter表

可以不指定链，默认为对应表的所有链

如果没有匹配的规则，则使用防火墙默认规则

选项/链名/目标操作用大写字母，其余都小写

### 基本的目标操作（ip包到达防火墙服务后，与规则匹配之后的处理方式）

ACCEPT：允许通过/放行

DROP：直接丢弃，不给出任何回应

REJECT：拒绝通过，必要时会给出提示

LOG：记录日志，然后传给下一跳规则（匹配即停止，规则的唯一例外）

### 常用的管理选项

|  |  |  |
| --- | --- | --- |
| 类别 | 选项 | 用途 |
| 添加规则 | -A | 在链的末尾追加一条规则 |
| -I | 在链的开头（或指定序号）插入一条规则 |
| 查看规则 | -L | 列出所有的规则条目 |
| -n | 以数字形式显示地址、端口等信息 |
| --line-numbers | 查看规则时，显示规则的序号 |
| 删除规则 | -D | 删除链内的指定序号（或内容）的一条规则 |
| -F | 清空所有的规则 |
| 默认策略 | -P | 为指定的链设备默认规则 |
| **匹配规则** | | |
| 通用匹配 | 协议匹配 | -p 协议名 |
| 地址匹配 | -s 源地址 、-d 目标地址 |
| 接口匹配 | -i 源地址 、-o 发数据的网卡 |
| 隐含匹配 | 端口匹配 | --port 源端口、-dport 目标地址 |
| ICMP类型匹配 | --icmp-type ICMP类型 |

## 基本的匹配条件

### 通用匹配：

可直接使用，不依赖与其他条件或扩展

包括网络协议、IP地址、网络接口等条件

### 隐含匹配：

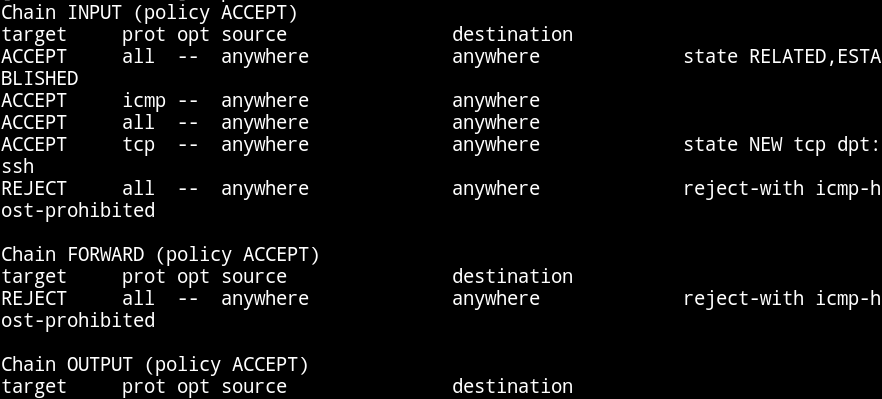
要求以特定的协议匹配作为前提

包括端口、TCP标记、ICMP类型等条件

需要取反条件时，用叹号！

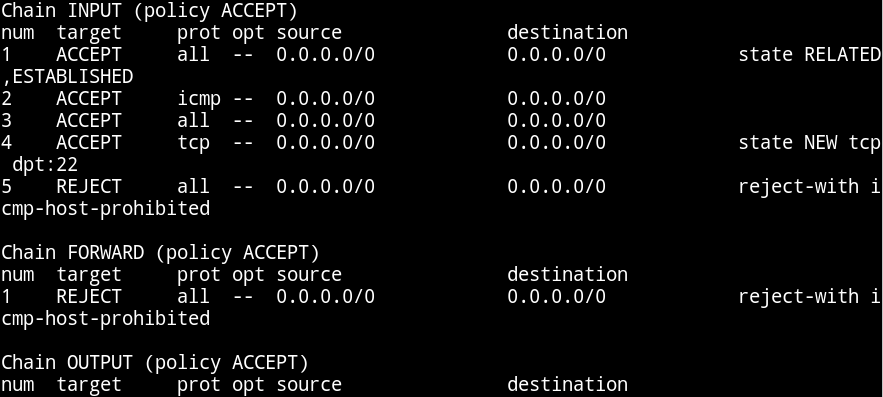
### 查看、删除表的默认规则

]# iptables -t filter -L 或 ]# iptables -L



]# iptables --line-numbers -L //显示规则的序号

]# iptables --line-numbers -L -n //规则中地址、端口以数字形式显示



]# iptables -L INPUT --line-numbers

]# iptables -t nat -L POSTROUTING --line-numbers

]# iptables -D INPUT 3 //删除默认表中的INPUT链的第3条记录

]# iptables -t nat -F //清空表内的所有规则

]# service iptables save //保存对于防火墙的操作

### 添加新的规则

只允许宿主机连机50主机的ssh服务，其他机器都不可以连接

]# iptables -t filter -A INPUT -p tcp -s 192.168.4.254 --dport 22 -j ACCEPT

]# iptables -t filter -P INPUT DROP

]# service iptables save

**放行网站访问**

]# iptables -t filter -A INPUT -p tcp --dport 80 -j ACCEPT

50主机可以ping其他主机

]# iptables -t filter -A INPUT -p icmp -j ACCEPT

其他主机ping不了50主机

]# iptables -t filter -A INPUT -s 192.168.4.51 -p icmp -j REJECT

//还是可以ping通，因为大范围被允许，匹配即停止

]# iptables -D INPUT 4

]# iptables -t filter -I INPUT 3 -p icmp -s 192.168.4.51 -j REJECT

//在大范围之前添加拒绝51主机ping的条目，给予回应

]# iptables -t filter -I INPUT 3 -p icmp -s 192.168.4.52 -j DROP

//拒绝52主机ping请求，不给回应

删除记录只留前两条

echo-request (ping) //发送的ping请求

echo-reply (pong) //应答包

**实验机可以ping通网段内的其他主机，但其他主机ping不通实验机(ping自己亦ping不通)**

]# iptables -t filter -A INPUT -p icmp --icmp-type echo-reply -j ACCEPT

**允许某一台主机可以ping通实验机**

]# iptables -t filter -I INPUT 3 -s 192.168.4.51 -p icmp -j ACCEPT

**结束时，先将默认的规则修改，在删除所有规则，不然当前宿主机所连接自己的终端会断开**

]# iptables -t filter -P INPUT ACCEPT

]# iptables -t filter -F

### 设置默认规则

所有链的初始默认规则均为ACCEPT

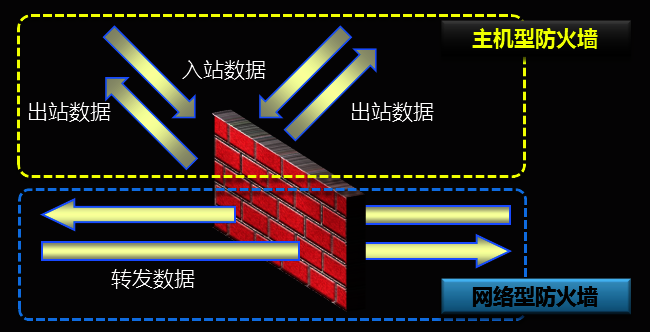
通过-P选项可重置默认规则

-ACCEPT或者DROP(INPUT的默认规则)

# 防护类型及条件

### 主机/网络型防护

根据保护对象（本机、其他主机）区分



### 开启内核的IP转发

作为网关、路由的必要条件

echo ‘net.ipv4.ip\_forward=1’ >> /etc/sysctl.conf

或者

echo 1 > /proc/sys/net/ipv4/ip\_forward

## 扩展匹配

### 扩展条件的方法

前提条件：有对应的防火墙模块支持

基本用法：-m 扩展模块 --扩展条件 条件值

示例：-m mac --mac-source 52:54:00:29:b0:c9

### 常见的扩展条件类型

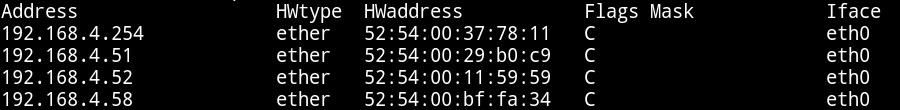
|  |  |  |
| --- | --- | --- |
| 类别 | 选项 | 用法 |
| 扩展匹配 | MAC地址匹配 | -m mac --mac-source MAC地址 |
| 多端口匹配 | -m multiport --sports 源端口列表  -m multiport --dports 目标端口列表 |
| IP范围匹配 | -m iprange --src-range IP1-IP2  -m iprange --dst-range IP1-IP2 |

### 根据MAC地址封锁主机

### ——适用于交换网络，针对源MAC地址

不管其IP地址如何变化，MAC地址是不会变化的

]# arp -n //获取ping过自己的所有主机的mac地址表



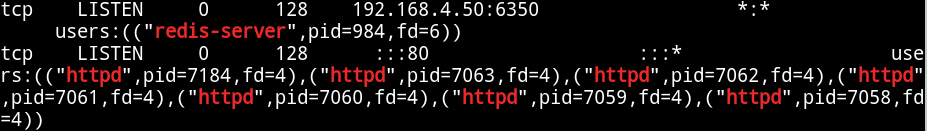
]# iptables -t filter -A INPUT -p icmp -m mac --mac-source 52:54:00:29:b0:c9 -j DROP

]# service iptables save

### 多端口案例

1. 规则开放多个端口（WEB、FTP、MAIL、SSH）

50 ~]# ss -natpul | grep redis-server && ss -natpul | grep httpd



]# iptables -t filter -A INPUT -p tcp -m multiport --dports 80,6350 -j DROP

//拒绝网络内的其他主机访问自己的网站服务和数据库服务

]# iptables -t filter -nL --line-numbers

**客户机51去访问主机50的网站服务和数据库服务**

[root@mysql51 ~]# curl 192.168.4.50/a.html

[root@mysql51 ~]# redis-cli -h 192.168.4.50 -p 6350

### 根据IP范围封锁主机

SSH登录的IP范围控制

拒绝网段内的所有主机的ping请求与ping回应

]# iptables -t filter -A INPUT -p icmp -m iprange --src-range 192.168.4.51-192.168.4.55 -j DROP

]# service iptables save

## NAT表应用——网络型防火墙

### 环境准备

|  |  |
| --- | --- |
| 主机 | IP |
| client50 | eth1:192.168.2.50 |
| mysql51 | eth0:192.168.4.51  eth1:192.168.2.51 |
| mysql52 | eth0:192.168.4.52 |

50主机：

[root@client50 ~]# systemctl stop NetworkManager

[root@client50 ~]# route add default gw 192.168.2.51

[root@client50 ~]# iptables -F

[root@client50 ~]# service iptables save

[root@client50 ~]# service iptables restart

51主机：

[root@mysql51 ~]# echo 'net.ipv4.ip\_forward = 1' >> /etc/sysctl.conf

[root@mysql51 ~]# sysctl -p

net.ipv4.ip\_forward = 1

[root@mysql51 ~]# service iptables restart

[root@mysql51 ~]# chkconfig iptables on

[root@mysql51 ~]# iptables -t filter -F

[root@mysql51 ~]# iptables -t nat -F

[root@mysql51 ~]# iptables -t raw -F

[root@mysql51 ~]# iptables -t mangle -F

[root@mysql51 ~]# service iptables save

52主机：

[root@mysql52 ~]# systemctl stop NetworkManager

[root@mysql52 ~]# route add default gw 192.168.4.51

在保证全网互通的情况下做以下实验

书写规则文件允许客户端50访问52的网站服务，拒绝数据库服务

**方式一：**

[root@mysql51 ~]# iptables -F

[root@mysql51 ~]# iptables -t filter -P FORWARD DROP

[root@mysql51 ~]# iptables -A FORWARD -p tcp --sport 80 -j ACCEPT

[root@mysql51 ~]# iptables -A FORWARD -p tcp --dport 80 -j ACCEPT

方式二：

[root@mysql51 ~]# iptables -F

[root@mysql51 ~]# iptables -t filter -P FORWARD DROP

[root@mysql51 ~]# iptables -A FORWARD -s 192.168.2.50 -p tcp --dport 80 -j ACCEPT

[root@mysql51 ~]# iptables -A FORWARD -d 192.168.2.50 -p tcp --sport 80 -j ACCEPT

测试：

[root@client50 ~]# curl <http://192.168.4.52/a.html> //成功

[root@client50 ~]# mysql -h 192.168.4.52 -p123asd...A //失败，被丢弃

[root@client50 ~]# ping -c 3 -W 1 192.168.4.52 //通信失败

**书写规则文件允许客户端访问52的数据库服务**

[root@mysql51 ~]# iptables -t filter -A FORWARD -p tcp --dport 3306 -j ACCEPT

[root@mysql51 ~]# iptables -t filter -A FORWARD -p tcp --sport 3306 -j ACCEPT

[root@client50 ~]# mysql -h 192.168.4.52 -p123asd...A //连接成功

**书写规则文件允许客户端的ping请求**

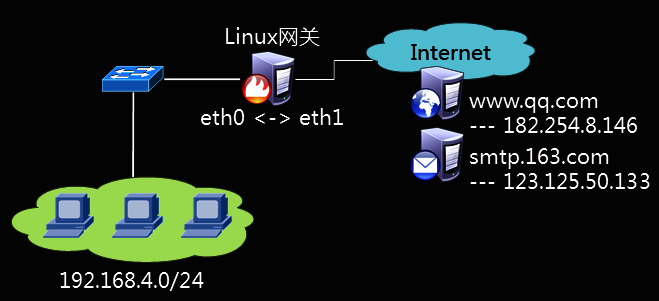
[root@mysql51 ~]# iptables -t filter -A FORWARD -p icmp -j ACCEPT

[root@client50 ~]# ping -c 3 -W 1 192.168.4.52 //可以通信

## NAT转换原理

### 私有地址的局限性

从局域网访问互联网的时候（看网页、收邮件......）,源地址为私有地址，服务器该如何给出回应



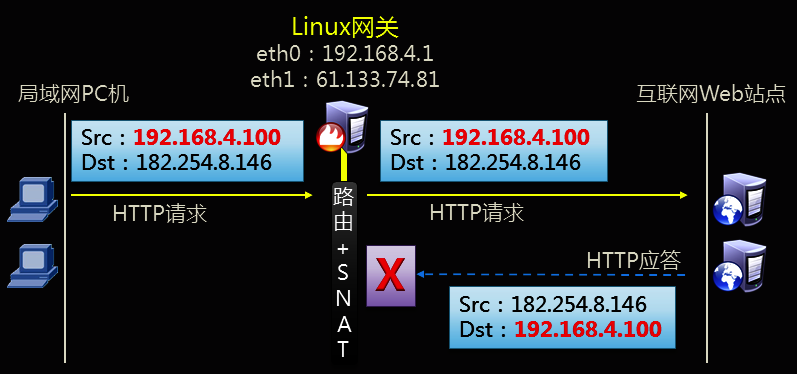
SANT源地址转换

Source Network Address Translation

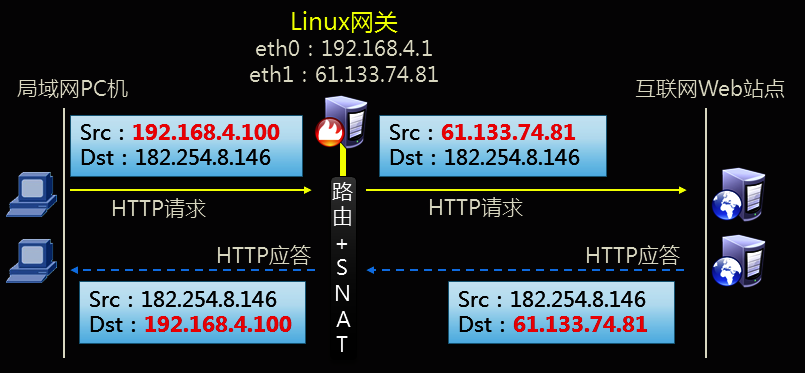
- 修改数据包的源地址

- 仅用于nat表的POSTROUTING

不修改源地址的情况：



修改源地址的情况：



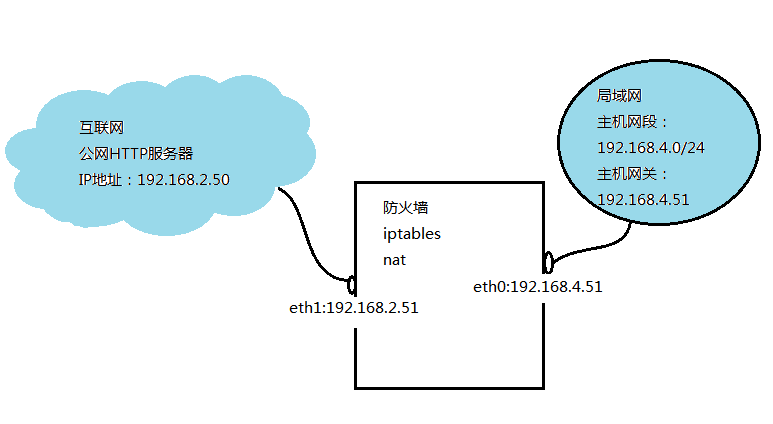
## 配置SNAT共享上网

### 配置的关键策略

选择路由之后，针对来自局域网、即将从外网接口发出去的包，将源IP地址修改为网关的公网IP地址

### 验证SNAT访问结果

拓扑结构：



还原环境：

让局域网的所有主机共享一个公网IP地址上网

50主机：做公网网站服务器

[root@client50 ~]# route del default gw 192.168.2.51

[root@client50 ~]# route -n

51主机：做防火墙主机

[root@mysql51 ~]# iptables -t filter -F

[root@mysql51 ~]# iptables -t filter -P FORWARD ACCEPT

[root@mysql51 ~]# service iptables save

[root@mysql51 ~]# ifconfig eth0 | head -2;ifconfig eth1 | head -2

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500

inet 192.168.4.51 netmask 255.255.255.0 broadcast 192.168.4.255

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500

inet 192.168.2.51 netmask 255.255.255.0 broadcast 192.168.2.255

53主机：做局域网内的主机

[root@mysql52 ~]# ifconfig eth0

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500

inet 192.168.4.52 netmask 255.255.255.0 broadcast 192.168.4.255

网络测试：ping自己的网关是可以通讯的

[root@client50 ~]# ping -c 2 192.168.2.51

[root@mysql52 ~]# ping 192.168.4.51

书写规则文件，使局域网主机可以访问互联网

[root@mysql51 ~]# iptables -t nat -nL

[root@mysql51 ~]# iptables -t nat -A POSTROUTING -s 192.168.4.0/24 -p tcp --dport 80 -j SNAT --to-source 192.168.2.51

192.168.4.0/24:源地址（局域网网段）

192.168.2.51：公网地址

进行测试：

[root@mysql52 ~]# curl <http://192.168.2.50/test.html> //可以访问

[root@mysql50 ~]# tail -f /etc/httpd/logs/access\_log

//动态查看日志看访问网站的主机IP

地址伪装策略

共享动态公网IP地址实现上网

主要针对外网接口的IP地址不固定的情况

将SNAT改为MASQUERADE即可

对于ADSL宽带拨号连接，网络接口可写为ppp+

只允许宿主机连机50主机的ssh服务，其他机器都不可以连接50主机可以ping其他主机，但其他主机ping不了50主机