**Morning：**

1、iptables防火墙

firewalld底层还是调用iptables，生产环境一般直接用iptables。

**-安装iptables-service**

[root@proxy ~]# yum -y install iptables-service

[root@proxy ~]# systemctl start iptables.service

[root@proxy ~]# service iptables save

#防火墙规则永久生效

**-iptables框架**

1）iptables的4个表（区分大小写）：

-nat表（地址转换表）

-filter表（数据过滤表）

-raw表（状态跟踪表，占用cpu较少使用）

-mangle表（包标记表，如修改TTL标记位，较少使用）

2）iptables的5个链（区分大小写）：

-INPUT链（入站规则）

-OUTPUT链（出站规则）

-FORWARD链（转发规则，路由）

-PREROUTING链（路由前规则）

-POSTROUTING链（路由后规则）

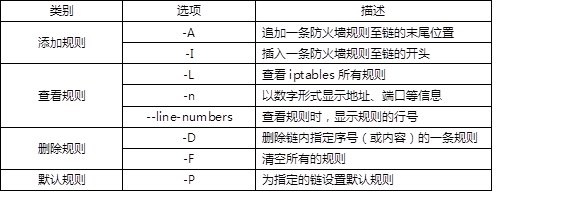
#每个表有5个链，在链里面添加规则

#从上往下读取规则，匹配即停止；如果没有匹配，则按默认规则(自定义)

**-iptables命令**

1）语法说明

**iptables** [-t 表名] **选项** [链名] [条件] [-j 处理方式]



#不写表名，默认为filter表

#不写链名，默认为对应表的所有链

#选项：增删查(如上表)

#条件：指定协议、IP、端口等

#处理方式：ACCEPT(允许通过)、REJECT(拒绝通过,给出提示)、

DROP(直接丢弃,不给回应)、LOG(记录日志,不允许也不拒绝)

SNAT(地址转换)

#默认规则：只能设置为ACCEPT或DROP

#选项/链名/处理方式用大写字母，其余都小写

2）使用案例

[root@proxy ~]# iptables -I INPUT 2 -p icmp -j REJECT

#filter.INPUT链第2行插入规则

[root@proxy ~]# iptables -D INPUT 2

#删除filter.INPUT链第2行规则

[root@proxy ~]# iptables -F

#清空filter表所有规则

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

#设置filter.INPUT链的默认规则

[root@proxy ~]# iptables -nL INPUT --line-number

#查看filter.INPUT链所有规则(显示行号)

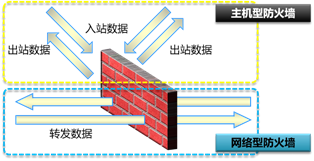
Chain INPUT (policy DROP)

num target prot opt source destination

1 ACCEPT tcp -- 0.0.0.0/0 0.0.0.0/0

2 REJECT icmp -- 0.0.0.0/0 0.0.0.0/0 reject-with icmp-port-unreachable

2、filter过滤与转发控制



**-iptables的条件**



Tips：一般不用--sport，因为每次访问的源端口为随机。

**-主机型防火墙案例**

~]# iptables -I INPUT -s 192.168.4.55 -p icmp -j REJECT

#拒绝接收4.55的icmp包

~]# iptables -I INPUT -i eth0 -p icmp -j REJECT

#拒绝接收从eth0进来的icmp包

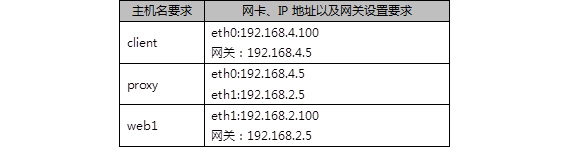
~]# iptables -A INPUT -s 192.168.4.0/24 -p tcp --dport 22 -j REJECT

#拒绝4.0/24网段使用tcp协议远程连接本机ssh(22端口)

~]# iptables -I OUTPUT -d 192.168.4.254 -p icmp -j REJECT

#禁止本机对4.254发送icmp包

**-网络型防火墙案例**



1）proxy开启路由转发功能

~]# echo 1 > /proc/sys/net/ipv4/ip\_forward #临时

~]# echo 'net.ipv4.ip\_forward=1' >> /etc/sysctl.conf #永久

2）proxy添加转发规则

~]# iptables -I FORWARD -s 192.168.4.100 -p tcp --dport 80 -j DROP

3）测试防火墙效果

[root@client ~]# curl 192.168.2.100 #无法访问

**-禁ping的相关策略**

~]# iptables -I INPUT -p icmp --help

~]# iptables -I INPUT -p icmp --icmp-type echo-request -j REJECT

#禁止其他主机ping本机、允许本机ping其他

**Afternoon：**

1、防火墙扩展规则

**iptables** [-t 表名] **选项** [链名] **-m 扩展模块 --具体扩展条件** -j 动作

**-MAC地址封锁规则**

[root@proxy ~]# nmap 192.168.4.100 #远程查看mac地址

[root@client ~]# ip link show eth0 #本机查看mac地址

[root@proxy ~]# iptables -I INPUT -p tcp --dport 22 \

> -m mac --mac-source 52:54:00:A7:12:1D -j REJECT

#--mac-source可以缩写为--mac

#client无法使用eth0网卡远程登陆proxy

**-开放多个tcp端口**

[root@proxy ~]# iptables -I INPUT -p tcp -m multiport --dports \

> 20:22,25,80,110,143,16501:16800 -j ACCEPT

**-IP范围封锁规则**

[root@proxy ~]# iptables -I INPUT -p tcp -dport 22 \

> -m iprange --src-range 192.168.4.10-192.168.4.20 -j ACCEPT

#允许10~20主机ssh登陆

#--src-range为范围内、--dst-range为范围外

[root@proxy ~]# iptables -A INPUT -p tcp --dport 22 \

> -s 192.168.4.0/24 -j DROP

#拒绝4.0/24网段其他主机ssh登陆

2、SNAT实现共享上网

**实验1：SNAT（源地址转换）**

1）开启路由转发功能

[root@proxy ~]# echo 1 > /proc/sys/net/ipv4/ip\_forward

1. 设置防火墙规则，实现SNAT地址转换

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

[root@proxy ~]# iptables -t nat -A POSTROUTING -s 192.168.4.0/24 \

> -p tcp --dport 80 -j SNAT --to-source 192.168.2.5

#POSTROUTING添加路由后规则(NAT转换都是在路由后执行)

3）查看web日志

[root@web1 ~]# tail /var/log/httpd/access\_log

192.168.4.100 - -... "GET / HTTP/1.1" 200 10 "-" "curl/7.29.0"

192.168.2.5 - -... "GET / HTTP/1.1" 200 10 "-" "curl/7.29.0"

4）[拓展]动态伪装IP

[root@proxy ~]# iptables -t nat -A POSTROUTING \

> -s 192.168.4.0/24 -p tcp --dport 80 -j MASQUERADE

#自动识别公网IP(用于公网地址不固定)

**实验2：实现虚拟机上网**

1. 虚拟机配置网关、DNS

[root@proxy ~]# nmcli connection modify eth0 -ipv4.method \

> manual ipv4.gateway 192.168.4.254 ipv4.dns 176.121.0.100

[root@proxy ~]# nmcli connection up eth0

2）真机配置SNAT

[root@room12pc2 ~]# echo 1 > /proc/sys/net/ipv4/ip\_forward

[root@room12pc2 ~]# iptables -t nat -A POSTROUTING \

> -s 192.168.4.0/24 -j SNAT --to-source 176.121.212.154

我的作业：

1. **iptables四表五链**

表：Filter（访问过滤）、nat（地址转换）、raw（状态跟踪）、mangle（包标记）

链：INPUT（入站）、OUTPUT（出站）、FORWARD（转发规则）、PREROUTING（路由前）、POSTROUTING（路由后）

1. **iptables命令语法（各项的可选值）**

**iptables -t 表名 选项 链名 条件 [ -m 拓展名 拓展条件 ] -j 执行动作**

选项：-A -I -L -nL --line-number -D -F -P

条件：-s -d -p --sport --dport -i -o --icmp-type echo-request

拓展名：mac iprange multiport

拓展条件： --mac-source --dports --src-range

执行动作： ACCEPT、REJECT、DROP、LOG、SNAT

1. **proxy拒绝client PING**

[root@proxy ~]# iptables -t filter -A INPUT -s 192.168.4.1 -p icmp -j REJECT

1. **proxy只允许真机访问22端口**

[root@proxy ~]# iptables -t filter -I INPUT -s 192.168.4.254 -p tcp --dport 22 -j ACCEPT

[root@proxy ~]# iptables -t filter -P INPUT DROP

1. **proxy可以Ping其他主机，其他主机不允许Ping proxy**

[root@proxy ~]# iptables -F

[root@proxy ~]# iptables -A INPUT -p icmp --icmp-type echo-request -j REJECT

1. **拒绝client通过proxy路由ping web1**

[root@proxy ~]# iptables -t filter -A FORWARD -s 192.168.4.1 -d 192.168.2.1 -p icmp -j REJECT

1. **proxy拒绝4.1～4.10的远程连接**

[root@proxy ~]# iptables -A INPUT -p tcp --dport 22 -m iprange --src-range 192.168.4.1-192.168.4.10 -j REJECT

1. **proxy拒绝client的eth0网卡发出的所有请求**

[root@proxy ~]# iptables -A INPUT -m mac --mac-source 52:54:00:8E:16:E7 -j REJECT

1. **web1只开放22，80端口**

[root@web1 ~]# iptables -P INPUT DROP

[root@web1 ~]# iptables -I INPUT -p tcp -m multiport --dports 22,80 -j ACCEPT

1. **web1可以联网**

[root@web1 ~]# nmcli connection modify eth1 ipv4.method manual ipv4.gateway 192.168.2.254 ipv4.dns 8.8.8.8 connection.autoconnect yes

[root@web1 ~]# nmcli connection up eth1

[root@room12pc2 ~]# echo 1 > /proc/sys/net/ipv4/ip\_forward

[root@room12pc2 ~]# iptables -t nat -I POSTROUTING -s 192.168.2.0/24 -j SNAT --to-source 176.121.212.154

[root@web1 ~]# firefox www.baidu.com