iptables语法  
iptables [-t 要操作的表] <操作命令> [要操作的链] [规则号码] [匹配条件] [-j 匹配后的动作]  
小写 大写 大写 小写 大写  
  
示例:  
iptables -L   
iptables -t filter -L   
iptables -t nat -L  
iptables -t raw -L  
iptables -t mangle -L  
========================================================  
  
常见的操作命令：  
-L 查看,v详细,n不反解 --line-number  
-A 追加，放置最后一条  
-I 插入，默认插入成第一条  
-D 删除  
-F 清空flush  
-P 设置默认策略policy  
-N 建立自定义链  
  
匹配的条件：  
-s 192.168.2.0/24 源地址  
-d 192.168.2.1 目标地址  
-p tcp|upd|icmp 协议  
-i lo input 从lo接口进入的数据包  
-o eth0 output 从eth0出去的数据包  
-p tcp --dport 80 目标端口是80,必须和-p tcp|udp 连用  
-p udp --dport 53 目标端口是53/udp  
匹配MAC地址  
匹配网卡  
处理方法：  
filter:  
-j ACCEPT 允许  
-j DROP 丢弃--------->不会给客户端返回任何消息  
-j REJECT 拒绝--------->会给客户端返回拒绝信息，尽量不要用drop，因为不容易拍错  
nat:  
-j SNAT 源地址转换  
-j DNAT 目标地址转换  
mangel:  
-j LOG 写日志  
-j MARK 打标记  
...  
========================================================  
  
七、Iptables匹配示例  
示例1：  
iptables -F  
iptables -A INPUT -j REJECT   
iptables -I INPUT -p tcp --dport 80 -j ACCEPT 插入一条规则在INPUT链，凡是tcp协议端口是80，都允许  
iptables -I INPUT -p tcp --dport 10:21 -j ACCEPT  
iptables -I INPUT -p tcp --dport 22 -j ACCEPT  
iptables -I INPUT -p icmp -j ACCEPT  
iptables -nL  
  
示例1存在的问题：  
1. 本机无法访问本机  
解决方案：iptables -I INPUT 2 -i lo -j ACCEPT  
  
2. 本机无法访问其它主机  
iptables -I INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT  
  
3. FTP无法访问  
方法一： 为vsftpd指定数据端口  
# iptables -I INPUT -p tcp --dport 21 -j ACCEPT  
# vim /etc/vsftpd/vsftpd.conf  
pasv\_min\_port=50000  
pasv\_max\_port=60000  
# iptables -I INPUT -p tcp --dport 50000:60000 -j ACCEPT  
方法二： 使用连接追踪模块  
[root@station230 ~]# iptables -I INPUT -m state --state ~~NEW,~~ESTABLISHED,RELATED -j ACCEPT  
[root@station230 ~]# iptables -I INPUT -p tcp --dport 21 -j ACCEPT   
[root@station230 ~]# modprobe nf\_conntrack\_ftp //加载连接追踪模块（临时）  
[root@station230 ~]# vim /etc/sysconfig/iptables-config //开机自动加载  
IPTABLES\_MODULES="nf\_conntrack\_ftp"  
ftp两种端口 ：控制端口（消息端口）和数据端口  
只要数据包是消息类型 走的都是控制端口   
只要是数据传输，走的都是数据端口，其中在数据端口中，主动模式下的数据端口是20，被动模式下的端口就不一定了  
所以如果配置了防火墙，ftp很可能不能访 问，因为无法确定数据端口的端口号，所以需要使用模块来将数据端口的链接  
从new识别为related，在防火墙配置中使用状态进行配置，将established和related都允许通过就OK了  
  
  
  
示例2： iptables标准流程  
========================================================  
[root@station230 ~]# iptables -F  
[root@station230 ~]# iptables -A INPUT -i lo -j ACCEPT  
[root@station230 ~]# iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT  
[root@station230 ~]# iptables -A INPUT -s 192.168.1.250 -j ACCEPT //允许公司内网任何访问  
[root@station230 ~]# iptables -A INPUT -s 192.168.3.0/24 -j ACCEPT //允许公司内网任何访问  
[root@station230 ~]# iptables -A INPUT -p tcp --dport 80 -j ACCEPT  
[root@station230 ~]# iptables -A INPUT -h 192.168.1.250 -p tcp --dport 22 -j ACCEPT  
[root@station230 ~]# iptables -A INPUT -p tcp --dport 21 -j ACCEPT  
[root@station230 ~]# iptables -A INPUT -j REJECT  
[root@station230 ~]# service iptables save  
[root@station230 ~]# chkconfig iptables on  
[root@station230 ~]# iptables -vnL INPUT  
[root@station230 ~]# vim /etc/sysconfig/iptables-config  
IPTABLES\_MODULES="nf\_conntrack\_ftp"  
[root@station230 ~]# service iptables restart  
  
小知识：  
常见协议的端口 /etc/services  
[root@station230 ~]# grep ^http /etc/services  
服务 协议 端口/传输协议  
ssh ssh 22/tcp  
http http 80/tcp  
https 443/tcp  
dns domain 53/udp,53/tcp  
mail smtp 25/tcp # 发信协议  
smtps 465/tcp # SMTP over SSL (TLS)  
pop3 110/tcp # 收信协议  
pop3s 995/tcp  
imap 143/tcp  
imaps 993/tcp  
dhcp bootps 67/udp # BOOTP server  
nfs nfs 2049/tcp  
samba 137,138,139/tcp  
445/tcp  
ftp ftp 21/tcp  
ftp-data 20/tcp  
ntp ntp 123/udp # Network Time Protocol  
syslog syslog 514/udp  
========================================================  
  
  
示例3： 真实环境配置实例  
一些常见允许外网访问的服务：   
网站 www http 80/tcp   
https 443/tcp   
邮件 mail smtp 25/tcp   
smtps 465/tcp   
pop3 110/tcp   
pop3s 995/tcp   
imap 143/tcp   
  
一些常见不允许外网访问的服务：   
文件服务器： NFS   
SAMBA   
FTP 20/tcp,21/tcp  
远程管理： ssh 22/tcp   
  
[root@station230 ~]# iptables -F  
[root@station230 ~]# iptables -A INPUT -i lo -j ACCEPT  
[root@station230 ~]# iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT  
[root@station230 ~]# iptables -A INPUT -s 192.168.2.0/24 -j ACCEPT  
[root@station230 ~]# iptables -A INPUT -s 192.168.3.0/24 -j ACCEPT  
[root@station230 ~]# iptables -A INPUT -p tcp --dport 80 -j ACCEPT  
[root@station230 ~]# iptables -A INPUT -p tcp --dport 22 -j ACCEPT  
[root@station230 ~]# iptables -A INPUT -p tcp --dport 25 -j ACCEPT  
[root@station230 ~]# iptables -A INPUT -p tcp --dport 110 -j ACCEPT  
[root@station230 ~]# iptables -A INPUT -j REJECT  
配置该策略后：  
1. 员工在公司内部（192.168.2.0/24,192.168.3.0/24）能访问服务器上的任何服务  
2. 当员工出差例如在上海，通过VPN连接到公司  
外网 （员工） ===拨号到==> VPN服务器 =====> 内网FTP，SAMBA，NFS，SSH  
========================================================  
防火墙开启路由转发：  
vim /etc/sysctl.conf  
  
  
八、防火墙NAT功能  
SNAT 源地址转换 出口POSTROUTING  
DNAT 目标地址转换 进口PREROUTING  
  
==SNAT,源地址转换  
作用：让内网用户可以通过NAT服务器访问外网  
  
内网 NAT服务器 外网  
client(192.168.5.80)--->eth0(192.168.5.240) NAT Server (1.1.1.254)eth1 ---> Web(1.1.1.1)   
  
1. iptables  
# iptables -t nat -A POSTROUTING -s 192.168.1.0/24 -j SNAT --to 1.1.1.254----->修改的地址必须是服务器已有的地址，否则回包回不来！  
# service iptables save  
当内网的数据包到达POSTROUTING链时，修改数据的源地址1.1.1.254  
  
2. 打开内核的路由转发机制----------->Linux默认不支持数据包的转发，需要手动开启  
# sysctl -a |grep ip\_forward  
net.ipv4.ip\_forward = 0  
# vim /etc/sysctl.conf  
net.ipv4.ip\_forward = 1------------->永久开启转发  
# sysctl -p 立即生效  
=========================================  
临时开启路由转发机制：  
echo 1 > /proc/sys/net/ipv4/ip\_forward  
=========================================  
客户端测试：所有内网将网关指定NAT服务器的内网地址：  
# links -dump 1.1.1.1  
welcome to china  
  
3. 限制上网  
# iptables -A FORWARD -s 192.168.2.168 -j REJECT //拒绝某个主机上网