iptables防火墙

包过滤防火墙

RHEL7: firewall

RHEL6/5: iptables

Firewall底层也是调用iptables

表都是用小写,严格区分大小写

想实现什么功能就在命令行

结构:

表 . 链 . 规则

iptables默认有4个表:

nat表（地址转换表）、filter表（数据过滤表）、

raw表（状态跟踪表）、mangle表（包标记表）。

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）

PREROUTING链（路由前规则）

POSTROUTING链（路由后规则）

基本命令

iptables [-t 表名] 选项 [链名] [条件] [-j 目标操作]

不加表时,默认为filter表

匹配即停止(log除外)

// 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，然后传给下一条规则

]# iptables [-t 表名] -L

]# iptables -nL --line-numbers

Chain **INPUT** (policy **DROP**) <---默认规则

num target prot opt source destination

1 ACCEPT icmp -- 0.0.0.0/0 0.0.0.0/0 <-----规则

2 ACCEPT tcp -- 0.0.0.0/0 0.0.0.0/0 tcp dpt:80

链的默认配置

iptables -P INPUT DROP

添加规则

iptables -A INPUT -p tcp --dport 22 -j ACCEPT

删除规则

iptables -t nat -F

Iptables -t 表 -D 链 号

???????

保存配置

iptables-save > /etc/sysconfig/iptables

iptables -I INPUT -p tcp - -dport 80 -j ACCEPT

iptables -I INPUT -p icmp -j ACCEPT

能ping通别人,别人不能ping通自己

iptables -A INPUT -p icmp - -icmp-type echo-reply -j ACCEPT

icmp消息控制管理协议

网络防火墙

扩展匹配



Mac地址

Nat表

网关配置

route add default gw 网关

del //删除网关

私网转公网(伪装ip)

]# iptables -t nat -A POSTROUTING -s 192.168.2.0/24 -p tcp --dport 80 -j SNAT --to-source 192.168.4.92

外网IP不固定的情况可以执行下面的地址伪装，动态伪装IP

]# iptables -t nat -A POSTROUTING \

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

访问真机转发到虚拟机

Iptables -t nat -A PREROUTING -i br0 -d 真机ip -p tcp --dport 真机端口 -j DNAT --to 虚拟机ip:端口