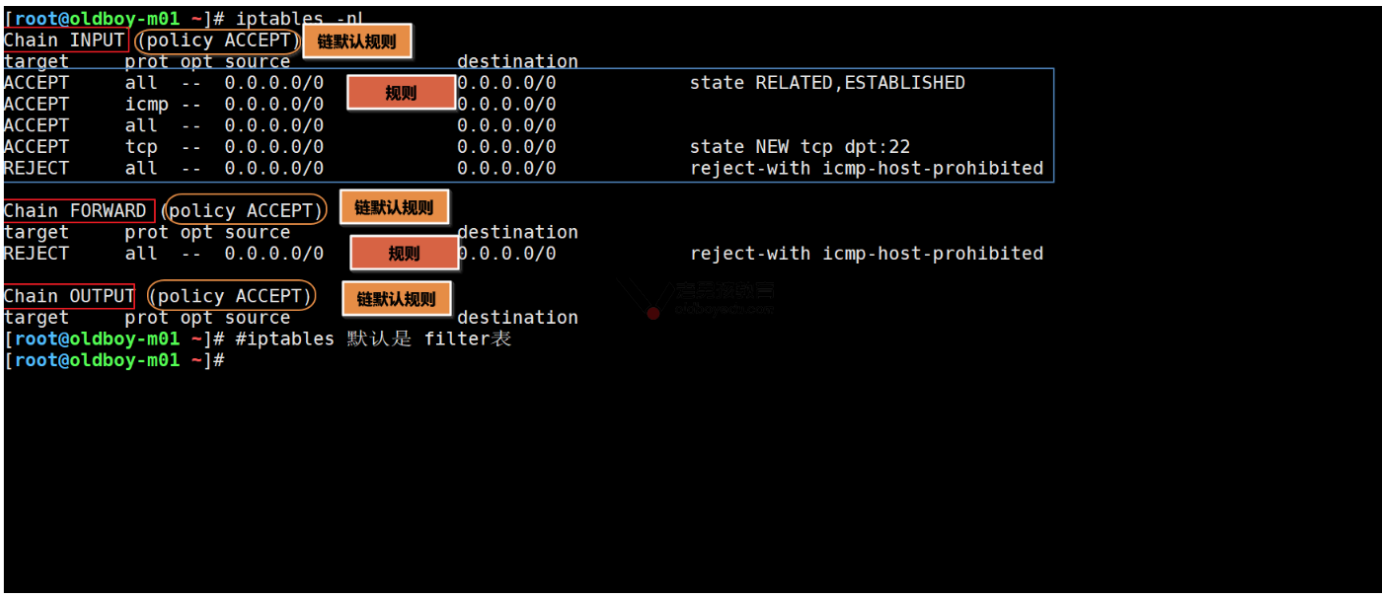
IPtables

1.软件部署

```
1.停止自带的firewalld，禁止开机启动
[root@m01 ~]# systemctl stop firewalld
[root@m01 ~]# systemctl disable   firewalld
2.安装iptables服务
[root@m01 ~]#yum install -y  iptables-services

3.加载对应的模块，临时
[root@m01 ~]#modprobe ip_tables
[root@m01 ~]#modprobe iptable_filter
[root@m01 ~]#modprobe iptable_nat
[root@m01 ~]#modprobe ip_conntrack
[root@m01 ~]#modprobe ip_conntrack_ftp
[root@m01 ~]#modprobe ip_nat_ftp
[root@m01 ~]#modprobe ipt_state

永久的写入/etc/profile /etc/rc.local
cat >>/etc/rc.local<<EOF
modprobe ip_tables
modprobe iptable_filter
modprobe iptable_nat
modprobe ip_conntrack
modprobe ip_conntrack_ftp
modprobe ip_nat_ftp
modprobe ipt_state
EOF


4.启动iptables并加入开机自启
[root@m01 ~]#systemctl start iptables
[root@m01 ~]#systemctl enable iptables

```

2.iptables命令




```

```

```
查看默认的防火强规则:
[root@m01 ~]#iptables -nL
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED
ACCEPT     icmp --  0.0.0.0/0            0.0.0.0/0
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           state NEW tcp dpt:22
REJECT     all  --  0.0.0.0/0            0.0.0.0/0           reject-with icmp-host-prohibited

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
REJECT     all  --  0.0.0.0/0            0.0.0.0/0           reject-with icmp-host-prohibited

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

2.清空默认的规则
[root@m01 ~]#iptables -F
[root@m01 ~]#iptables -X
[root@m01 ~]#iptables -Z
[root@m01 ~]#iptables -nL
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

```

3.iptables案例

案例1.禁止访问61的22端口

```
[root@m01 ~]#iptables -I INPUT -p tcp --dport 22 -j DROP
```

案例2.删除规则

```
进入到虚拟机中执行命令:
[root@m01 ~]# iptables -I INPUT -s 10.0.0.1 -j ACCEPT
[root@m01 ~]#iptables -nL
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  10.0.0.1             0.0.0.0/0
DROP       tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:22

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

删除规则方式两种:
第一种序号删除
查看编号信息:
[root@m01 ~]#iptables -nL --line
Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination
1    ACCEPT     all  --  10.0.0.1             0.0.0.0/0
2    DROP       tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:22

删除INPUT链的第2条规则
[root@m01 ~]#iptables -D INPUT 2
[root@m01 ~]#iptables -nL
Chain INPUT (policy ACCEPT)
```

```
target     prot opt source               destination
ACCEPT     all  --  10.0.0.1             0.0.0.0/0

第二种删除方法: 将I 或者A 修改为D
[root@m01 ~]#iptables -D INPUT -p tcp --dport 22 -j DROP
[root@m01 ~]#iptables -nL
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  10.0.0.1             0.0.0.0/0
```

案例3.限制来源IP地址

```
禁止10.0.0.7 访问10.0.0.61
[root@m01 ~]#iptables -I INPUT -s 10.0.0.7 -j DROP
```

案例5.限制网段

```
[root@m01 ~]#iptables -I INPUT -s 172.16.1.7/24 -j DROP
[root@m01 ~]#iptables -nL
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       all  --  172.16.1.0/24        0.0.0.0/0
```

面试题: 你用过iptables吗?

答: 用过

那你跟我说一下 如果禁止某个IP地址怎么写?

iptables -A INPUT -s ip地址 -j DROP

案例6.限制80端口

```
[root@m01 ~]#iptables -I INPUT -p tcp --dport 80 -j DROP
```

案例7.限制10.0.0.7不能访问61的80端口

```
[root@m01 ~]#iptables -I INPUT -s 10.0.0.7 -p tcp --dport 80 -j DROP
```

案例8.对源IP进行取反

```
除了10.0.0.1之前所有的IP地址都不能访问我的服务器(慎重使用)
[root@m01 ~]#iptables -I INPUT ! -s 10.0.0.1 -j DROP
```

案例9.修改默认的规则

```
1.配置先允许自己可以访问61
[root@m01 ~]#iptables -I INPUT  -s 10.0.0.1 -j ACCEPT
2.修改默认规则为DROP
[root@m01 ~]#iptables -P INPUT DROP
[root@m01 ~]#
[root@m01 ~]#iptables -nL
Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     all  --  10.0.0.1             0.0.0.0/0

```

案例10.多端口配置

```
允许80和443端口
[root@m01 ~]#iptables -I INPUT  -p tcp -m multiport --dport 80,443  -j ACCEPT

```

案例11.禁ping

```
禁ping 禁tracert
[root@m01 ~]#iptables -I INPUT  -p icmp --icmp-type 8  -j DROP
```

通过linux操作系统内核参数配置禁ping

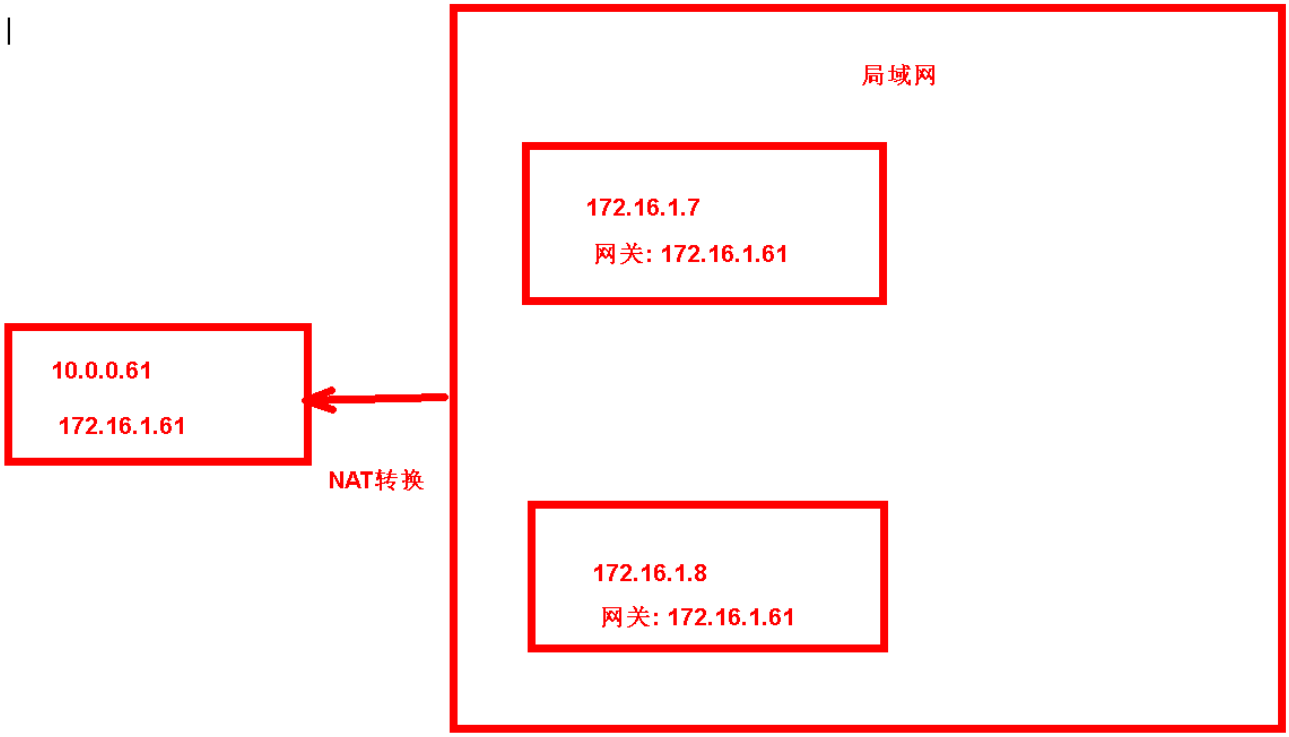
```
设置为1为禁ping
设置为0开启ping
[root@m01 ~]#echo  1  >/proc/sys/net/ipv4/icmp_echo_ignore_all
[root@m01 ~]#cat /proc/sys/net/ipv4/icmp_echo_ignore_all
1
[root@m01 ~]#echo  0  >/proc/sys/net/ipv4/icmp_echo_ignore_all
[root@m01 ~]#cat /proc/sys/net/ipv4/icmp_echo_ignore_all
0

```

案例11.iptables的保持与恢复

```
iptables-save将当前的配置保持到/etc/sysconfig/iptables
[root@m01 ~]#iptables-save
恢复iptabales
1.重启读取/etc/sysconfig/iptables 配置文件中的策略
systemctl restart iptables

2.使用命令恢复
iptables-restore  </etc/sysconfig/iptables
```

案例12.使用iptables实现共享上网

SNAT: 源地址转换



服务端设置:

```
1.iptables设置SNAT
将来源IP是172.16.1.0网段的流量，全都转换成10.0.0.61去访问外网
[root@m01 ~]#iptables -t nat -A POSTROUTING  -s 172.16.1.0/24   -j SNAT  --to-source 10.0.0.61
2.配置内核转发(拥有路由器功能)
[root@m01 ~]#echo 'net.ipv4.ip_forward = 1'  >> /etc/sysctl.conf
3.刷新配置
[root@m01 ~]#sysctl -p
net.ipv4.ip_forward = 1
```

使用ADSL拨号的网络:

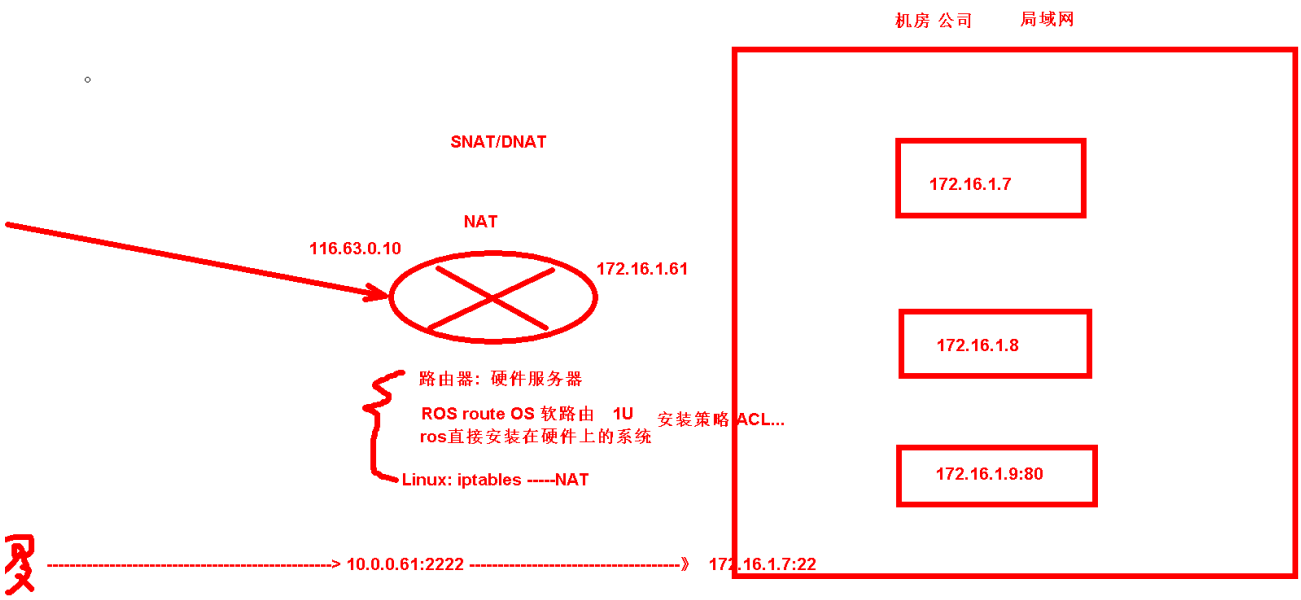
注意事项: 公网ip不固定: iptables -t nat -A POSTROUTING -s 172.16.1.0/24 -j MASQUERADE

客户端设置:

```
配置网关: 172.16.1.61 保证重启resolv.conf里DNS
[root@web01 ~]#cat /etc/sysconfig/network-scripts/ifcfg-eth1
TYPE=Ethernet
BOOTPROTO=none
NAME=eth1
DEVICE=eth1
ONBOOT=yes
IPADDR=172.16.1.7
PREFIX=24
GATEWAY=172.16.1.61
DNS1=223.5.5.5
重启生效:
[root@web01 ~]#systemctl restart network
```

案例13.IP地址映射

DNAT 目标地址转换




```
配置IP地址端口映射:
[root@m01 ~]#iptables -t nat -A PREROUTING    -d 10.0.0.61 -p tcp --dport 9000  -j DNAT --to-destination 172.16.1.7:22

```