

IPtables

1.软件部署

```
1 1.停止自带的firewalld, 禁止开机启动
2 [root@m01 ~]# systemctl stop firewalld
3 [root@m01 ~]# systemctl disable firewalld
4 2.安装iptables服务
5 [root@m01 ~]#yum install -y iptables-services
6
7 3.加载对应的模块, 临时
8 [root@m01 ~]#modprobe ip_tables
9 [root@m01 ~]#modprobe iptable_filter
10 [root@m01 ~]#modprobe iptable_nat
11 [root@m01 ~]#modprobe ip_conntrack
12 [root@m01 ~]#modprobe ip_conntrack_ftp
13 [root@m01 ~]#modprobe ip_nat_ftp
14 [root@m01 ~]#modprobe ipt_state
15
16 永久的写入/etc/profile /etc/rc.local
17 cat >>/etc/rc.local<<EOF
18 modprobe ip_tables
19 modprobe iptable_filter
20 modprobe iptable_nat
21 modprobe ip_conntrack
22 modprobe ip_conntrack_ftp
23 modprobe ip_nat_ftp
24 modprobe ipt_state
25 EOF
26
27
28 4.启动iptables并加入开机自启
29 [root@m01 ~]#systemctl start iptables
30 [root@m01 ~]#systemctl enable iptables
31
```

2.iptables命令

```
[root@oldboy-m01 ~]# iptables -nl
Chain INPUT (policy ACCEPT) 链默认规则
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 规则 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) 链默认规则
target prot opt source destination
REJECT all -- 0.0.0.0/0 规则 0.0.0.0/0 reject-with icmp-host-prohibited

Chain OUTPUT (policy ACCEPT) 链默认规则
target prot opt source destination
[root@oldboy-m01 ~]# #iptables 默认是 filter表
[root@oldboy-m01 ~]#
```

```

1 查看默认的防火强规则:
2  [root@m01 ~]#iptables -nL
3  Chain INPUT (policy ACCEPT)
4  target     prot opt source                destination
5  ACCEPT     all  --  0.0.0.0/0             0.0.0.0/0           state RELATED,ESTABLISHED
6  ACCEPT     icmp --  0.0.0.0/0             0.0.0.0/0
7  ACCEPT     all  --  0.0.0.0/0             0.0.0.0/0
8  ACCEPT     tcp  --  0.0.0.0/0             0.0.0.0/0           state NEW tcp dpt:22
9  REJECT     all  --  0.0.0.0/0             0.0.0.0/0           reject-with icmp-host-prohibited
10
11 Chain FORWARD (policy ACCEPT)
12 target     prot opt source                destination
13 REJECT     all  --  0.0.0.0/0             0.0.0.0/0           reject-with icmp-host-prohibited
14
15 Chain OUTPUT (policy ACCEPT)
16 target     prot opt source                destination
17
18 2.清空默认的规则
19 [root@m01 ~]#iptables -F
20 [root@m01 ~]#iptables -X
21 [root@m01 ~]#iptables -Z
22 [root@m01 ~]#iptables -nL
23 Chain INPUT (policy ACCEPT)
24 target     prot opt source                destination
25
26 Chain FORWARD (policy ACCEPT)
27 target     prot opt source                destination
28
29 Chain OUTPUT (policy ACCEPT)
30 target     prot opt source                destination
31

```

3.iptables案例

案例1.禁止访问61的22端口

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

案例2.删除规则

```

1 进入到虚拟机中执行命令:
2  [root@m01 ~]# iptables -I INPUT -s 10.0.0.1 -j ACCEPT
3  [root@m01 ~]#iptables -nL
4  Chain INPUT (policy ACCEPT)
5  target     prot opt source                destination
6  ACCEPT     all  --  10.0.0.1              0.0.0.0/0
7  DROP       tcp  --  0.0.0.0/0             0.0.0.0/0           tcp dpt:22
8
9  Chain FORWARD (policy ACCEPT)
10 target     prot opt source                destination
11
12 Chain OUTPUT (policy ACCEPT)
13 target     prot opt source                destination
14
15 删除规则方式两种:
16 第一种序号删除
17 查看编号信息:
18 [root@m01 ~]#iptables -nL --line
19 Chain INPUT (policy ACCEPT)
20 num target     prot opt source                destination
21 1  ACCEPT     all  --  10.0.0.1              0.0.0.0/0
22 2  DROP       tcp  --  0.0.0.0/0             0.0.0.0/0           tcp dpt:22
23
24 删除INPUT链的第2条规则
25 [root@m01 ~]#iptables -D INPUT 2
26 [root@m01 ~]#iptables -nL
27 Chain INPUT (policy ACCEPT)

```

```
28 target    prot opt source          destination
29 ACCEPT    all  --  10.0.0.1        0.0.0.0/0
30
31 第二种删除方法：将I 或者A 修改为D
32 [root@m01 ~]#iptables -D INPUT -p tcp --dport 22 -j DROP
33 [root@m01 ~]#iptables -nL
34 Chain INPUT (policy ACCEPT)
35 target    prot opt source          destination
36 ACCEPT    all  --  10.0.0.1        0.0.0.0/0
37
38
39
```

案例3.限制来源IP地址

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

案例5.限制网段

```
1 [root@m01 ~]#iptables -I INPUT -s 172.16.1.7/24 -j DROP
2 [root@m01 ~]#iptables -nL
3 Chain INPUT (policy ACCEPT)
4 target    prot opt source          destination
5 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

```
1 [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

```
1 [root@m01 ~]#iptables -I INPUT -s 10.0.0.7 -p tcp --dport 80 -j DROP
2
```

案例8.对源IP进行取反

```
1 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)
2 [root@m01 ~]#iptables -I INPUT ! -s 10.0.0.1 -j DROP
3
```

案例9.修改默认的规则

```
1 1.配置先允许自己可以访问61
2 [root@m01 ~]#iptables -I INPUT -s 10.0.0.1 -j ACCEPT
3 2.修改默认规则为DROP
4 [root@m01 ~]#iptables -P INPUT DROP
5 [root@m01 ~]#
6 [root@m01 ~]#iptables -nL
7 Chain INPUT (policy DROP)
8 target     prot opt source                destination
9 ACCEPT     all  --  10.0.0.1                0.0.0.0/0
10
```

案例10.多端口配置

```
1 允许80和443端口
2 [root@m01 ~]#iptables -I INPUT -p tcp -m multiport --dport 80,443 -j ACCEPT
3
```

案例11.禁ping

```
1 禁ping 禁tracert
2 [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

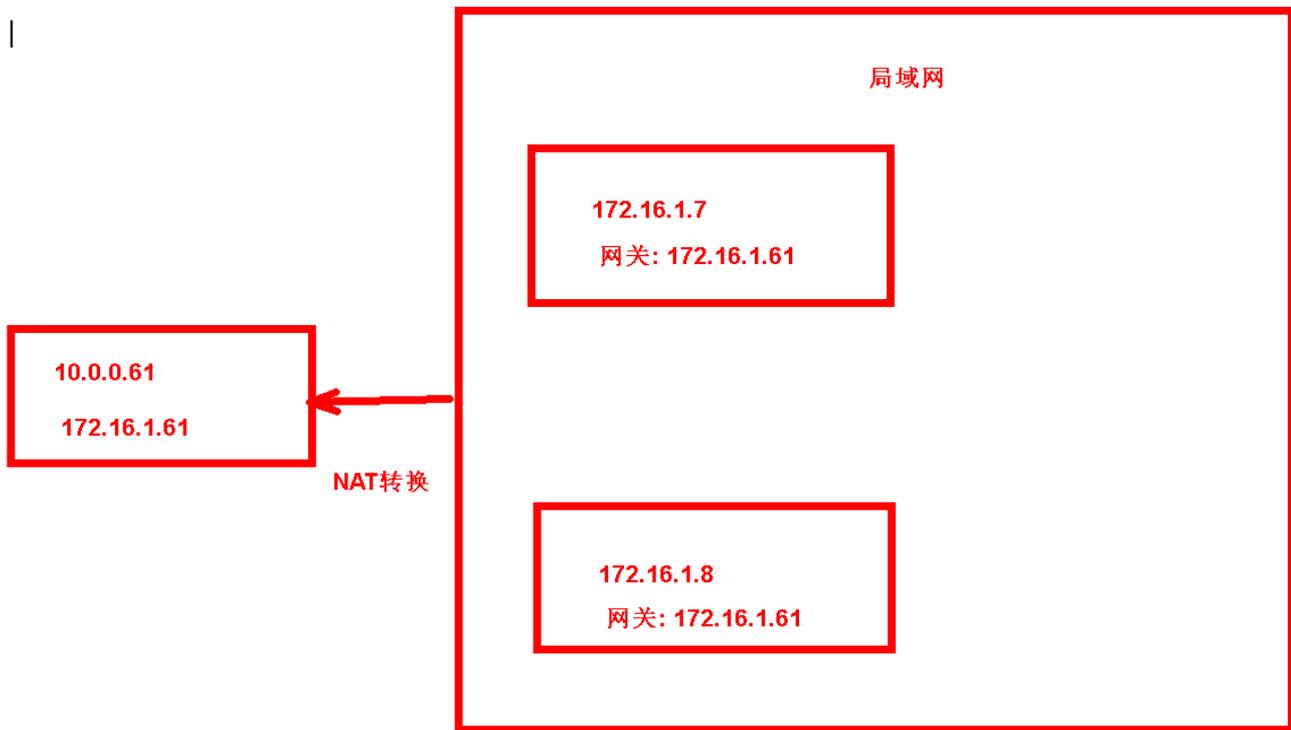
```
1 设置为1为禁ping
2 设置为0开启ping
3 [root@m01 ~]#echo 1 >/proc/sys/net/ipv4/icmp_echo_ignore_all
4 [root@m01 ~]#cat /proc/sys/net/ipv4/icmp_echo_ignore_all
5 1
6 [root@m01 ~]#echo 0 >/proc/sys/net/ipv4/icmp_echo_ignore_all
7 [root@m01 ~]#cat /proc/sys/net/ipv4/icmp_echo_ignore_all
8 0
9
```

案例11.iptables的保持与恢复

```
1 iptables-save将当前的配置保持到/etc/sysconfig/iptables
2 [root@m01 ~]#iptables-save
3 恢复iptables
4 1.重启读取/etc/sysconfig/iptables 配置文件中的策略
5 systemctl restart iptables
6
7 2.使用命令恢复
8 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  1. iptables设置SNAT
2  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
3  [root@m01 ~]#iptables -t nat -A POSTROUTING -s 172.16.1.0/24 -j SNAT --to-source 10.0.0.61
4  2. 配置内核转发(拥有路由器功能)
5  [root@m01 ~]#echo 'net.ipv4.ip_forward = 1' >> /etc/sysctl.conf
6  3. 刷新配置
7  [root@m01 ~]#sysctl -p
8  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:

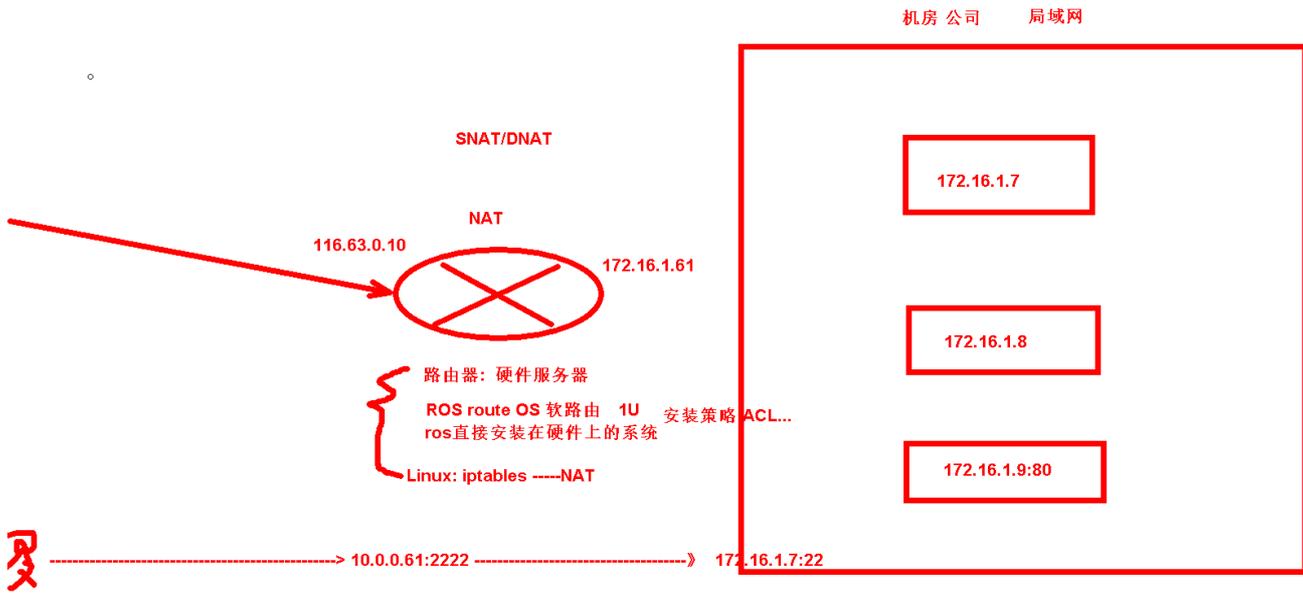
```

1  配置网关: 172.16.1.61 保证重启resolv.conf里DNS
2  [root@web01 ~]#cat /etc/sysconfig/network-scripts/ifcfg-eth1
3  TYPE=Ethernet
4  BOOTPROTO=none
5  NAME=eth1
6  DEVICE=eth1
7  ONBOOT=yes
8  IPADDR=172.16.1.7
9  PREFIX=24
10 GATEWAY=172.16.1.61
11 DNS1=223.5.5.5
12 重启生效:
13 [root@web01 ~]#systemctl restart network

```

案例13.IP地址映射

DNAT 目标地址转换



```
1 配置IP地址端口映射:
2 [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
3
```