老男孩教育-day55-Iptables防火墙实战

1.课程内容

- [x] 常见防火墙选用
    - [x] 硬件
    - [x] 开源软件:iptables（默认规则改为 INPUT DROP）
    - [x] 云服务器:安全组（阿里云 白名单[默认是拒绝]）
- [x] Iptables使用 **执行过程**
- [x] Iptables **4表5链**

- [x] **filter nat** mangle raw
- [x] filter : INPUT
- [x] nat ： PREROUTING POSTROUTING

> pre prefix xxx之前
>
> routing route
>
> post xxx之后

- [x] 准备Iptables环境
- [x] Iptables功能之**防火墙**-filter
  - 封IP 封端口
  - 准许某个ip访问 网段访问
- [x] 实际生产iptables配置
- [x] Iptables功能之**内网服务器上外网（共享上网）**
- [x] Iptables功能之**端口转发**

2. 常见防火墙选用

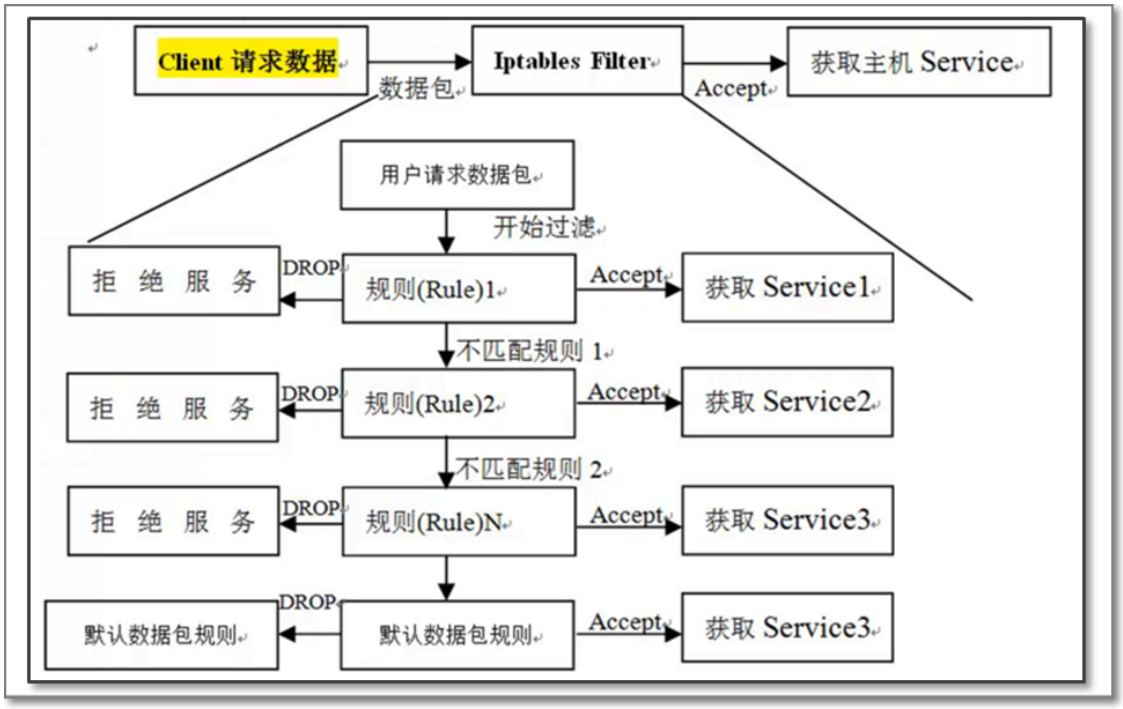
- 公司**网站入口**使用的**硬件防火墙**、**三层路**由带有防火墙功能
- Iptables访问量小 C5 C6 默认，CentOS 7 Firewalld（关闭 安装iptables）
- ~~SELinux~~

3. 名词（关系）与单词

名词	含义	对比
容器	存放内容/存放东西	
Netfilter/iptables	**Netfilter/iptables**是表的容器	国家
表（table)	**表**是用来存放链的容器	省
链 (chain)	链存放 规则容器	市
规则 (policy)	准许/拒绝访问	区县具体地点

4. 防火墙执行过程

1. 防火墙是层层过滤的，实际是按照配置**规则**的顺序**从上到下**，**从前到后**进行过滤的。
2. 如果**匹配**上规则，即明确表示是阻止(DROP)还是通过(ACCEPT)数据包就**不再向下匹配新的规则。**
3. 如果规则中没有明确表明是阻止还是通过的，也就是没有匹配规则，向下进行匹配，直到匹配**默认规则**得到明确的阻止还是通过。
4. 防火墙的默认规则是所有规则执行完才执行的。



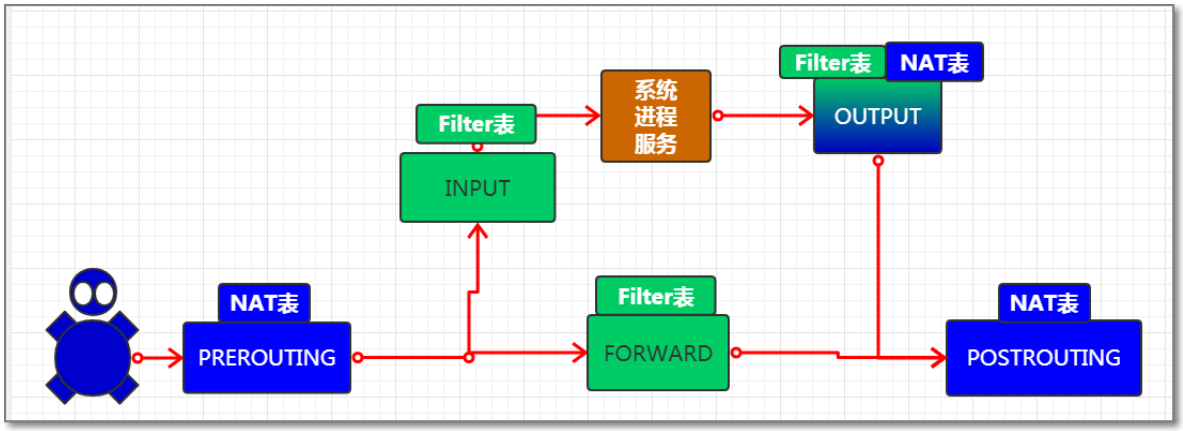
5. 四表五链

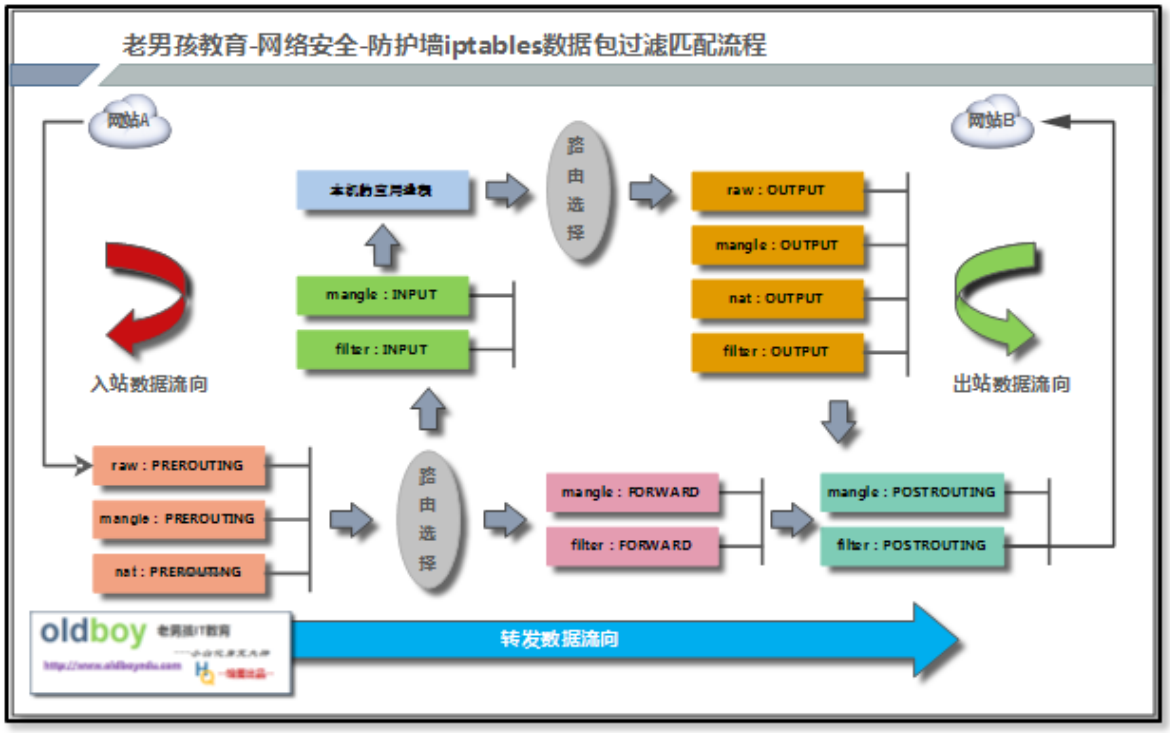
5.1 整体说明 4表及作用

表	功能
Filter	**过滤，默认的表，防火墙功能**
NAT	**实现NAT转化:1.共享上网 2.端口转发**
mangle	
raw	

> 参考查询帮助: man iptables

5.2 4表中的5链





5.2.1 filter表

filter表	企业工作场景：主机防火墙	
INPUT	**就是过滤进入主机的数据包**	
FORWARD	负责转发流经主机的数据包。	
OUTPUT	就是处理从主机发出去的数据包	

5.2.2 nat表

nat表		
PREROUTING	**处理用户请求中的目的地址 目的端口 端口转发 ip映射**	
POSTROUTING	处理离开服务器的请求 源端口 源ip ：**共享上网**	
OUTPUT	和主机放出去的数据包有关，改变主机发出数据包的目的地址。	

5.2.3 Mangle表

主要负责修改数据包中特殊的路由标记，如TTL，TOS，MARK等，这个表定义了5个链（chains）：

6. 防火墙之filter表

6.1 环境准备

> m01 iptables
>
> db01

```
yum install  iptables  iptables-services
```

```
[root@m01 ~]# rpm -qa  iptables-services
iptables-services-1.4.21-28.el7.x86_64
[root@m01 ~]# rpm -ql  iptables-services
/etc/sysconfig/ip6tables
/etc/sysconfig/iptables    #iptables 配置文件
/usr/lib/systemd/system/ip6tables.service
/usr/lib/systemd/system/iptables.service  #iptables服务管理配置

```

启动防火墙：

```
systemctl start iptables.service
systemctl enable iptables.service
```

检查防火墙内核模块是否加载成功:

```
[root@m01 ~]# lsmod |egrep 'nat|ipt|filter'
ipt_REJECT             12541  2
nf_reject_ipv4         13373  1 ipt_REJECT
iptable_filter         12810  1
xt_nat                 12681  1
iptable_nat            12875  1
nf_nat_ipv4            14115  1 iptable_nat
nf_nat                 26787  2 nf_nat_ipv4,xt_nat
nf_conntrack          133095  4
nf_nat,nf_nat_ipv4,xt_conntrack,nf_conntrack_ipv4
ip_tables              27126  2 iptable_filter,iptable_nat
libcrc32c              12644  3 xfs,nf_nat,nf_conntrack
```

> 手动加载内核模块:
>
> ```
> modprobe ip_tables
> modprobe iptable_filter
> modprobe iptable_nat
> modprobe ip_conntrack
> modprobe ip_conntrack_ftp
> modprobe ip_nat_ftp
> modprobe ipt_state
> ```

6.2 配置规则-禁止访问22端口

```
[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

[root@m01 ~]# iptables  -t filter -A INPUT   -p tcp --dport 22  -j DROP

```

> 配置防火墙规则注意事项：
>
> 1. 去机房重启系统或者登陆服务器删除刚才的禁止规则。
> 2. 让机房人员重启服务器或者让机房人员拿用户密码登录进去
> 3. 通过服务器的**远程管理卡**管理（推荐）
> 4. **先写一个定时任务，每5分钟就停止防火墙**
> 5. 测试环境测试好，写成脚本，批量执行

6.3 iptables 命令及参数

iptables		
-t	指定表 filter(默认) nat	
-A	append 把规则追加到**末尾**	
-I (大写字母I)	insert 把规则插入到规则的**第1条**（**添加拒绝类规则的时候**）	
-p	protocal 指定协议:tcp /udp/icmp	
--dport	**dest**ination port 目标端口	
--sport	source port 源端口	
-d	dest ip address 目标ip地址	
-s	source ip address 源ip地址	
-i	input 数据**进来**的时候通过的网卡	
-o	output 数据**出去**的时候通过的网卡	
-j	jump 方法 **DROP（拒绝） ACCEPT(准许)** REJECT（拒绝）	

iptables查看 删除		
-F	清除链中所有的规则	
-X	清空自定义链的规则	
-Z	清空计数器	
-n	不要把端口解析服务名字	
-L	显示表中的规则	
--line-number	给每个链中的规则加上行号	
-D	删除规则 根据规则的号码进行删除	-D INPUT 2

```
[root@m01 ~]# iptables -nL  --line-number
Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination
1    DROP       tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:22
2    DROP       tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:23

Chain FORWARD (policy ACCEPT)
num  target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
num  target     prot opt source               destination
[root@m01 ~]# iptables -t filter -D INPUT 2
[root@m01 ~]# iptables -t filter -D INPUT 1
[root@m01 ~]# iptables -nL  --line-number
Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
num  target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
num  target     prot opt source               destination
```

6.4 filter表其他规则配置

6.4.1 只让10.0.0.0/24网段进行访问

> 只要是10.0.0.0/24 局域网的用户 访问m01 都ACCEPT
>
> 此例子主要限制：网段或ip地址

```
[root@m01 ~]# iptables -I INPUT  -p tcp  ! -s 10.0.0.0/24   -j DROP
[root@m01 ~]# iptables -nL
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       tcp  -- !10.0.0.0/24          0.0.0.0/0

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
[root@m01 ~]#
```

6.4.2 准许或禁止端口

> **多个端口：表示范围 1-1024范围**

```
[root@m01 ~]# iptables -I INPUT -p tcp ! --dport 1:1024  -j DROP
[root@m01 ~]# iptables -nL
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       tcp  --  0.0.0.0/0            0.0.0.0/0            tcp
dpts:!1:1024
DROP       tcp  -- !10.0.0.0/24          0.0.0.0/0

Chain FORWARD (policy ACCEPT)


```

> nc用法:

> nc -l 指定监听端口
>
> nc/telnet 连接

> > nc 服务端:

```
[root@m01 ~]# nc -l 99   >/tmp/new.txt
[root@m01 ~]# cat /tmp/new.txt
127.0.0.1   localhost localhost.localdomain localhost4
localhost4.localdomain4
::1         localhost localhost.localdomain localhost6
localhost6.localdomain6
172.16.1.5      lb01
172.16.1.6      lb02
172.16.1.7      web01
172.16.1.8      web02
172.16.1.31     nfs01
172.16.1.41     backup
172.16.1.51     db01 db01.etiantian.org
172.16.1.61     m01
```

> > nc客户端

```
[root@m01 ~]# cat  /etc/hostname    |nc   10.0.0.61 99
```

> 多个端口 不连续 80,433,52113,22

```
[root@m01 ~]# iptables -I INPUT -p tcp -m multiport ! --dport 80,443,22   -
j DROP
[root@m01 ~]# iptables -nL
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       tcp  --  0.0.0.0/0            0.0.0.0/0           multiport
dports  !80,443,22
DROP       tcp  -- !10.0.0.0/24          0.0.0.0/0

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

6.4.3 准许或禁止ping

```
[root@m01 ~]# ping 10.0.0.61
PING 10.0.0.61 (10.0.0.61) 56(84) bytes of data.
64 bytes from 10.0.0.61: icmp_seq=1 ttl=64 time=0.033 ms
64 bytes from 10.0.0.61: icmp_seq=2 ttl=64 time=0.062 ms
^C
--- 10.0.0.61 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 999ms
rtt min/avg/max/mdev = 0.033/0.047/0.062/0.016 ms
```

```
[root@m01 ~]# ping 172.16.1.61
PING 172.16.1.61 (172.16.1.61) 56(84) bytes of data.
64 bytes from 172.16.1.61: icmp_seq=1 ttl=64 time=0.037 ms
^C
--- 172.16.1.61 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.037/0.037/0.037/0.000 ms

[root@m01 ~]# iptables -I INPUT  -p icmp   --icmp-type any   -j   DROP

[root@m01 ~]# iptables -nL
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       icmp --  0.0.0.0/0            0.0.0.0/0            icmptype 255

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
[root@m01 ~]# ping 172.16.1.61
PING 172.16.1.61 (172.16.1.61) 56(84) bytes of data.
--- 172.16.1.61 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 1999ms

[root@m01 ~]# ping 10.0.0.61
PING 10.0.0.61 (10.0.0.61) 56(84) bytes of data.
--- 10.0.0.61 ping statistics ---
1 packets transmitted, 0 received, 100% packet loss, time 0ms

[root@m01 ~]# ping 127.0.0.1
[root@m01 ~]# ping 127.0.0.1
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
--- 127.0.0.1 ping statistics ---
2 packets transmitted, 0 received, 100% packet loss, time 999ms
```

> 禁止后检测是否通畅：
>
> 可以使用
>
> - telnet
> - nc
> - nmap
> - **进行检查**

6.4.3 连接状态

NEW：已经或将启动新的连接

ESTABLISHED：已建立的连接

RELATED：正在启动的新连接

INVALID：非法或无法识别的

```
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A OUTPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
```

6.4.4 匹配网络限制策略(限制并发 访问的频率)

-m limit

-m limit --limit n/{**sec**ond/**min**ute/hour}:

解释：指定时间内的请求速率”n”为速率，后面为时间分别为：秒 分 时

--limit-burst [n]

解释：在同一时间内允许通过的请求”n”为数字，不指定默认为5

```
iptables -I INPUT -s 10.0.1.0/24 -p icmp --icmp-type 8 -m limit --limit 6/min
--limit-burst 5 -j ACCEPT
```

6.4.6 保存规则

```
[root@m01 ~]# iptables-save
# Generated by iptables-save v1.4.21 on Wed Jul  3 09:27:35 2019
*filter
:INPUT ACCEPT [276:20776]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [296:27334]
-A INPUT -p icmp -m icmp --icmp-type any -j DROP
COMMIT
# Completed on Wed Jul  3 09:27:35 2019
# Generated by iptables-save v1.4.21 on Wed Jul  3 09:27:35 2019
*nat
:PREROUTING ACCEPT [8:1767]
:INPUT ACCEPT [3:542]
:OUTPUT ACCEPT [63:3947]
:POSTROUTING ACCEPT [63:3947]

[root@m01 ~]# iptables-save   >/etc/sysconfig/iptables
[root@m01 ~]# iptables -nL
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       icmp --  0.0.0.0/0            0.0.0.0/0            icmptype 255

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
[root@m01 ~]# iptables -F
[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
[root@m01 ~]#
[root@m01 ~]# #iptables-save   >/etc/sysconfig/iptables
```

```
[root@m01 ~]# iptables-restore < /etc/sysconfig/iptables
[root@m01 ~]# iptables -nL
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       icmp --  0.0.0.0/0            0.0.0.0/0            icmptype 255

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
[root@m01 ~]# #systemctl restart  iptables.service
```

> 注意事项:
>
> - iptables-save >/etc/sysconfig/iptables
> - iptables 是关闭状态 stop/disable
> - 不要使用iptables -nL 查看状态,如果使用防火墙自动打开
> - 查看防火墙状态: `systemctl is-active  iptables`

7. 生产环境防火墙配置

> 1.逛公园: 防火墙默认的规则 默认规则都是准许 ACCEPT
>
> 2.电影院:默认规则是 拒绝DROP 凭票进入

7.1 配置允许SSH登陆端口进入

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

7.2 允许本机回环lo接口数据流量流出与流入

```
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT
```

> -i input 与 INPUT链一起使用
>
> -o output 与 OUTPUT 链一起使用

7.3 准许icmp协议通过

```
[root@m01 ~]# iptables -A INPUT  -p icmp --icmp-type 8  -j ACCEPT
```

7.4 准许用户使用的端口通过 80,443

```
iptables -A INPUT -p tcp --dport 80   -j ACCEPT
iptables -A INPUT -p tcp --dport 443   -j ACCEPT
```

7.5 允许用户与服务器建立连接

```
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A OUTPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
```

7.6 开启信任的IP网段**

```
iptables -A INPUT   -s 10.0.0.0/24 -p all   -j ACCEPT
iptables -A INPUT   -s 172.16.1.0/24 -p all -j ACCEPT
```

7.7 修改默认规则

```
iptables -P INPUT DROP
iptables -P FORWARD DROP
iptables -P OUTPUT ACCEPT
```

8. NAT表

PREROUTING	处理请求中的目标ip和端口 :: 端口转发（映射）	
POSTROUTING		
OUTPUT		

8.1 PREROUTING

```
[root@m01 ~]# #iptables-save  >/root/iptables.rule
[root@m01 ~]#
[root@m01 ~]# iptables -P INPUT ACCEPT
[root@m01 ~]# iptables -P FORWARD ACCEPT
[root@m01 ~]#
[root@m01 ~]# iptables -F
```

8.2 POSTROUTING

> 防火墙配置POSTROUTING规则
>
> 开启内核转发
>
> 检查iptable nat模块是否加载 lsmod

```
[root@m01 ~]# iptables -t nat -A POSTROUTING  -s 172.16.1.0/24 -o eth0   -j SNAT  --to-source 10.0.0.61
[root@m01 ~]# iptables -nL -t nat
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination

Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

```

```
Chain POSTROUTING (policy ACCEPT)
target     prot opt source               destination
SNAT       all  --  172.16.1.0/24        0.0.0.0/0            to:10.0.0.61
[root@m01 ~]# tail  /etc/sysctl.conf
[root@m01 ~]# tail  /etc/sysctl.conf
# /usr/lib/sysctl.d/, /run/sysctl.d/, and /etc/sysctl.d/.
#
# Vendors settings live in /usr/lib/sysctl.d/.
# To override a whole file, create a new file with the same in
# /etc/sysctl.d/ and put new settings there. To override
# only specific settings, add a file with a lexically later
# name in /etc/sysctl.d/ and put new settings there.
#
# For more information, see sysctl.conf(5) and sysctl.d(5).
net.ipv4.ip_forward = 1
[root@m01 ~]# sysctl -p
net.ipv4.ip_forward = 1
[root@m01 ~]# cat /proc/sys/net/ipv4/ip_forward
1
[root@m01 ~]# lsmod |egrep 'ipt|nat|filter'
ipt_REJECT             12541  0
nf_reject_ipv4         13373  1 ipt_REJECT
iptable_filter         12810  0
xt_nat                 12681  1
iptable_nat            12875  1
nf_nat_ipv4            14115  1 iptable_nat
nf_nat                 26787  2 nf_nat_ipv4,xt_nat
nf_conntrack          133095  4
nf_nat,nf_nat_ipv4,xt_conntrack,nf_conntrack_ipv4
ip_tables              27126  2 iptable_filter,iptable_nat
libcrc32c              12644  3 xfs,nf_nat,nf_conntrack
```

> 关闭eth0网卡
>
> 在eth1网卡中加入网关 指向 xxx.61

```
[root@db01 ~]# cat  /etc/sysconfig/network-scripts/ifcfg-eth0
TYPE=Ethernet
BOOTPROTO=none
NAME=eth0
DEVICE=eth0
ONBOOT=no
IPADDR=10.0.0.51
PREFIX=24
GATEWAY=10.0.0.254
DNS1=10.0.0.254
[root@db01 ~]# cat  /etc/sysconfig/network-scripts/ifcfg-eth1
TYPE=Ethernet
BOOTPROTO=static
IPADDR=172.16.1.51
PREFIX=24
NAME=eth1
DEVICE=eth1
ONBOOT=yes
GATEWAY=172.16.1.61
```

> 重启网卡 ，通过内网连接进来 并进行测试

```
[root@db01 ~]# ping baidu.com
PING baidu.com (123.125.114.144) 56(84) bytes of data.
64 bytes from 123.125.114.144 (123.125.114.144): icmp_seq=1 ttl=127 time=7.60 ms
64 bytes from 123.125.114.144 (123.125.114.144): icmp_seq=2 ttl=127 time=5.87 ms
64 bytes from 123.125.114.144 (123.125.114.144): icmp_seq=3 ttl=127 time=6.25 ms
64 bytes from 123.125.114.144 (123.125.114.144): icmp_seq=4 ttl=127 time=4.12 ms
64 bytes from 123.125.114.144 (123.125.114.144): icmp_seq=5 ttl=127 time=6.55 ms
64 bytes from 123.125.114.144 (123.125.114.144): icmp_seq=6 ttl=127 time=4.15 ms
^C
--- baidu.com ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5010ms
rtt min/avg/max/mdev = 4.123/5.760/7.601/1.263 ms
```

> iptables -t nat -A POSTROUTING -s 172.16.1.0/24 -o eth0 -j SNAT --to-source 10.0.0.61 #公网ip固定
>
> iptables -t nat -A POSTROUTING -s 172.16.1.0/24 -o eth0 -j SNAT --to-source MASQUERADE #伪装
>
> MAS QUE RADE 【mæskəˈreɪd】

9.防火墙小结

- [x] 防火墙4表5链
- [x] filter表 INPUT链 实现防火墙功能
- [x] nat 表 PREROUTING实现 端口转发
- [x] nat 表 POSTROUTING链实现 共享上网

10.练习题

https://www.jianshu.com/p/2180face8381