上章回顾

- iptables规则表的匹配顺序是什么?
  - raw：用于标记、跟踪数据流
  - mangle：修改、设置数据包头，如TTL、协议等
  - nat：修改IP地址
  - filter：过滤数据包
- iptables链中规则的匹配顺序是什么?
  - 按顺序匹配从上到下
  - 匹配即停止，除log动作除外
- iptables中的动作
  - DROP：丢弃不提示
  - REJECT：拒绝
  - ACCEPT：允许
  - LOG：日志记录

本章内容

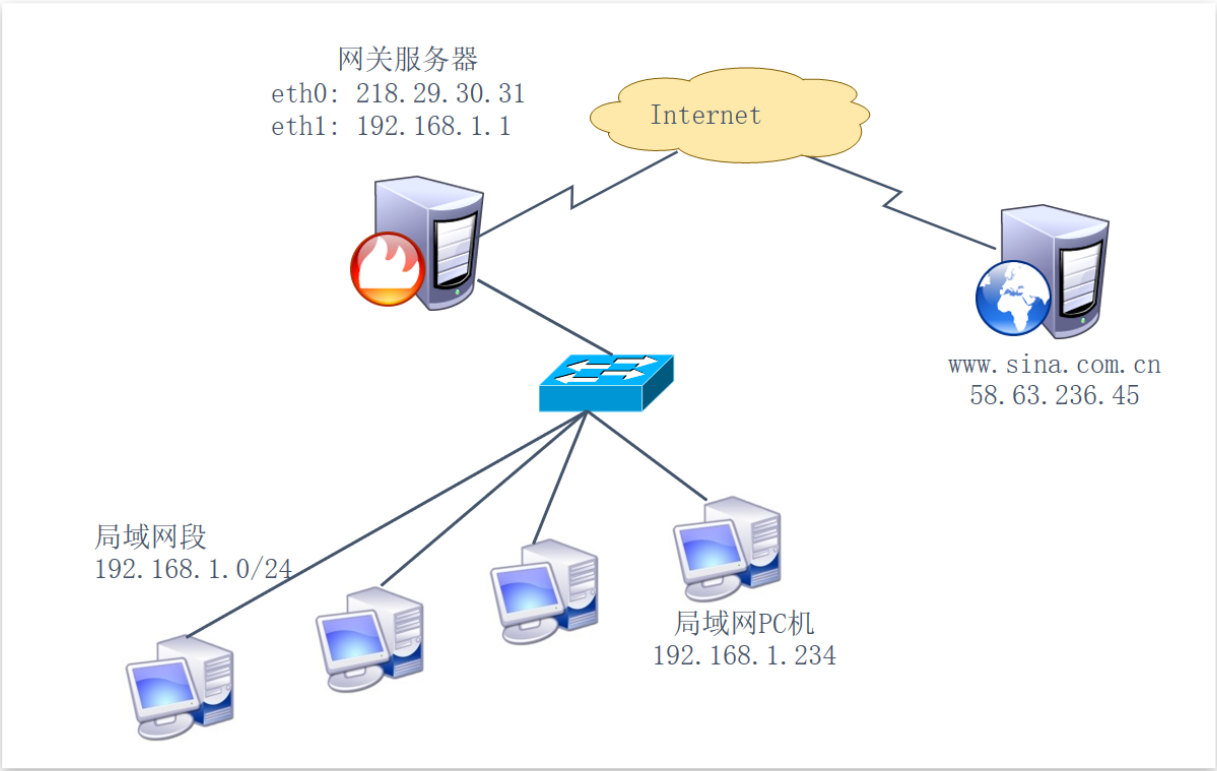
- 学会利用SNAT策略共享上网
- 学会利用DNAT策略发布内网服务器

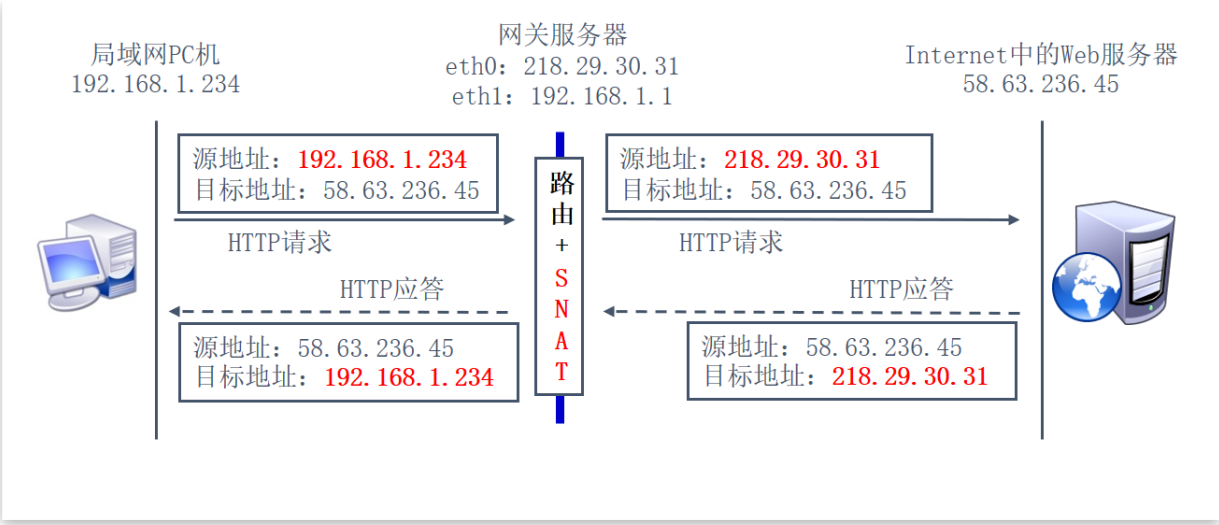
一、SNAT策略

1、源地址转换，Source Network Address Translation

2、数据包从网卡发送出去的时候，把数据包中的源IP地址（内网地址）部分替换为指定的IP（公网地址）

3、网络内部主机（私有网络）能够与外网（公有网络）通信





二、SNAT搭建实例

1、环境准备：

1）外网服务器：Linux - web

```
[root@webser ~]# ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 222.222.222.2  netmask 255.255.255.0  broadcast 222.222.222.255
        inet6 fe80::acb:669d:c75c:ea84  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:9b:40:d2  txqueuelen 1000  (Ethernet)
        RX packets 42144  bytes 2817443 (2.6 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 5888  bytes 1022175 (998.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

```

2）节点网关服务器：Linux - iptables

```
[root@localhost ~]# ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.1  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::df3c:ee2f:cd1d:295  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:38:57:c7  txqueuelen 1000  (Ethernet)
        RX packets 124  bytes 11859 (11.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 64  bytes 7909 (7.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

ens37: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
```

```
        inet 222.222.222.1  netmask 255.255.255.0  broadcast 222.222.222.255
        inet6 fe80::c098:9afe:fb09:cf4b  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:38:57:d1  txqueuelen 1000  (Ethernet)
        RX packets 127  bytes 11344 (11.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 83  bytes 7334 (7.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

```

3）内部客户机：windows 7

```
C:\Users\Administrator>ipconfig


   IPv4 地址 . . . . . . . . . . . . : 192.168.1.100
   子网掩码  . . . . . . . . . . . . : 255.255.255.0
   默认网关. . . . . . . . . . . . . : 192.168.1.1
```

2、iptables-SNAT条目编写

1）清空原有filter、nat表中的条目

```
[root@localhost ~]# iptables -F
[root@localhost ~]# iptables -t nat -F
```

2）开启路由转发功能

```
#临时开启路由转发功能
[root@localhost ~]# echo 1 > /proc/sys/net/ipv4/ip_forward
[root@localhost ~]# cat /proc/sys/net/ipv4/ip_forward
1

#永久开启路由转发功能
[root@localhost ~]# vim /etc/sysctl.conf

net.ipv4.ip_forward = 1         #添加一下内容

[root@localhost ~]# sysctl -p    #刷新/etc/sysctl.conf系统配置文件，使修改生效
```

```
net.ipv4.ip_forward = 1

[root@localhost ~]# sysctl -a | grep ip_forward    #查看修改的内核参数配置
net.ipv4.ip_forward = 1
net.ipv4.ip_forward_use_pmtu = 0
```

3）实现全网 ping 正常

```
C:\Users

正在 Ping 222.222.222.2 具有 32 字节的数据:
来自 222.222.222.2 的回复: 字节=32 时间<1ms TTL=63
```

4）编写SNAT条目

```
[root@localhost ~] iptables -t nat -I POSTROUTING -s 192.168.1.0/24 -o ens37 -j SNAT --to-source 222.222.222.1
#或者
[root@localhost ~] iptables -t nat -I POSTROUTING -s 192.168.1.0/24 -o ens37 -j SNAT  MASQUERADE
```

3、客户机访问web服务器验证结果

1）安装httpd服务，tail -f 方式查看日志文件

2）客户机访问web页面查看结果

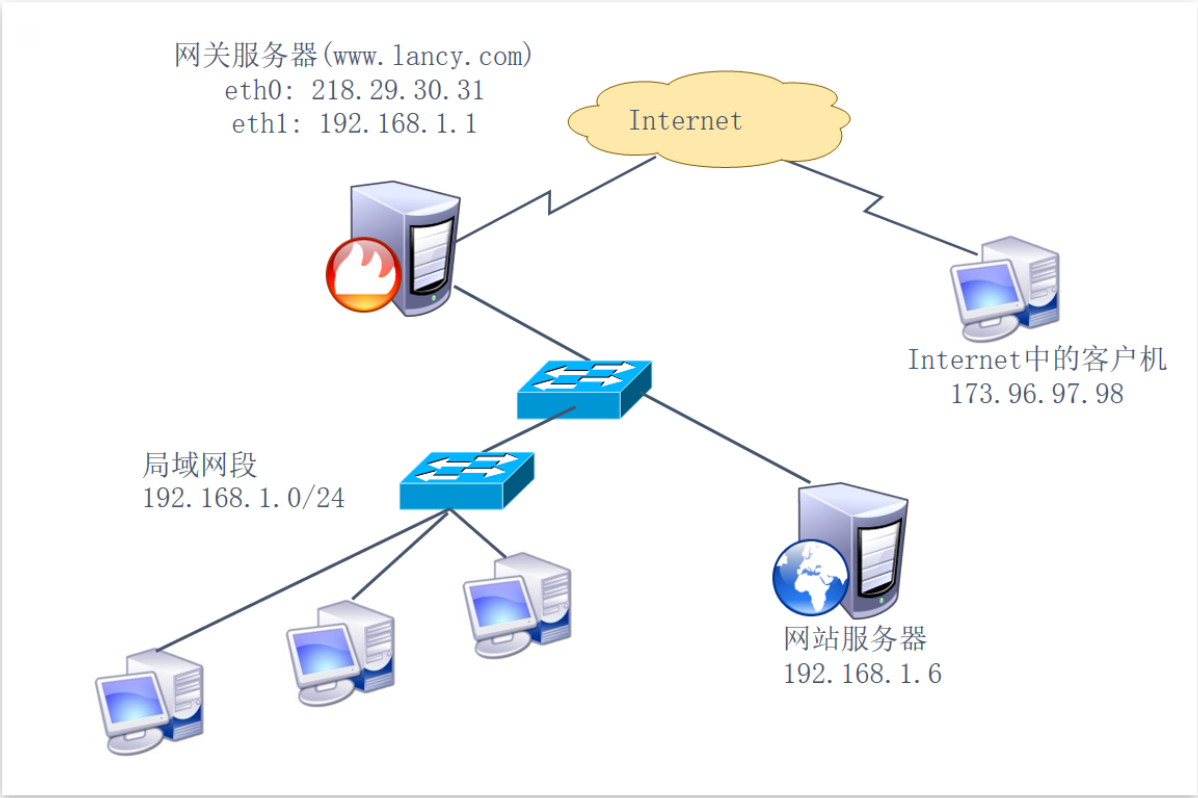
```
[root@webser ~]# echo "11111" > /var/www/html/index.html
[root@webser ~]# systemctl start httpd
[root@webser ~]# tail -f /var/log/httpd/access_log
222.222.222.1 - - [13/Jan/2024:16:43:54 +0800] "GET / HTTP/1.1" 200 6 "-" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729)"
222.222.222.1 - - [13/Jan/2024:16:43:54 +0800] "GET /favicon.ico HTTP/1.1" 404 209 "-" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729)"
```

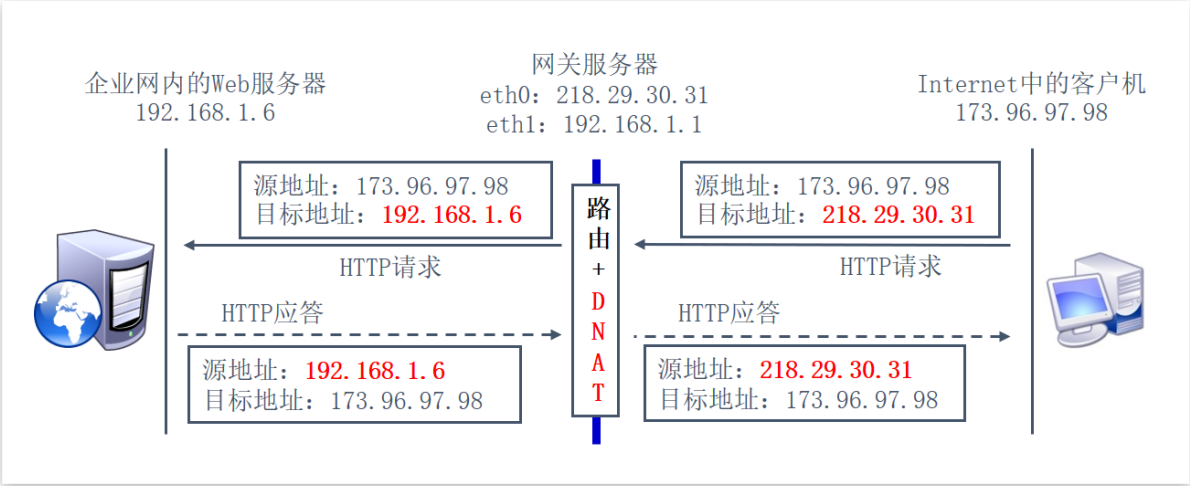
三、DNAT策略

1、目标地址转换，Destination Network Address Translation，在Internet中发布位于企业局域网内的服务器

2、改变数据包目的地址，当防火墙收到来自外网的数据包后，会将该数据包的目的IP地址进行替换

（源IP地址不变），重新转发到内网的主机





四、DNAT部署实例

1、准备环境

1）Linux - web：内部服务器

2）linux - iptables：节点服务器

3）windows 7：公网客户端

2、实现公网通过访问节点服务器的IP地址获取内部服务器的web页面

3、环境部署

1）IP 规划（内部服务器）

```
[root@webser ~]# ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.254  netmask 255.255.255.0  broadcast 192.168.1.255
```

```
        inet6 fe80::acb:669d:c75c:ea84  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:9b:40:d2  txqueuelen 1000  (Ethernet)
        RX packets 43111  bytes 2902680 (2.7 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 6444  bytes 1097601 (1.0 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

```

2）iptables 服务器

```
[root@localhost ~]# ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.1  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::df3c:ee2f:cd1d:295  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:38:57:c7  txqueuelen 1000  (Ethernet)
        RX packets 1198  bytes 105140 (102.6 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 536  bytes 64865 (63.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

ens37: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 222.222.222.1  netmask 255.255.255.0  broadcast 222.222.222.255
        inet6 fe80::c098:9afe:fb09:cf4b  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:38:57:d1  txqueuelen 1000  (Ethernet)
        RX packets 361  bytes 32197 (31.4 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 208  bytes 18046 (17.6 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

3）win 7 客户机

```
C:\Users\Administrator>ipconfig

以太网适配器 本地连接:
   连接特定的 DNS 后缀 . . . . . :
   本地链接 IPv6 地址. . . . . : fe80::8984:e309:d4ae:6774%11
   IPv4 地址 . . . . . : 222.222.222.222
   子网掩码  . . . . . : 255.255.255.0
```

```
   默认网关. . . . . . . . . . . . . : 222.222.222.1
```

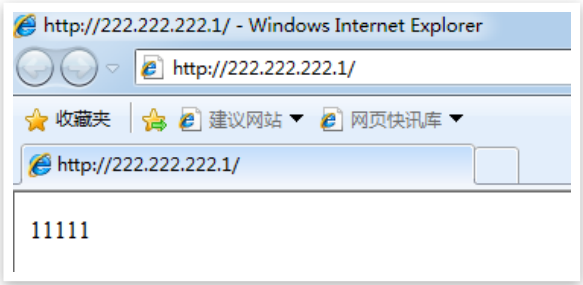
4、iptables 编写DNAT条目

```
[root@localhost ~] iptables -t nat -I PREROUTING -d 222.222.222.1 -p tcp --dport 80 -j DNAT --to-destination 192.168.1.254
```

5、验证结果

1）客户机通过访问iptables外网接口IP获得web资源

2）web服务器通过查看访问日志验证结果




```
[root@webser ~]# tail -2 /var/log/httpd/access_log
222.222.222.222 - - [13/Jan/2024:16:58:52 +0800] "GET / HTTP/1.1" 200 6 "-" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729)"
222.222.222.222 - - [13/Jan/2024:16:58:52 +0800] "GET /favicon.ico HTTP/1.1" 404 209 "-" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729)"
```

小结

1. SNAT策略的作用是什么，典型应用是什么?
2. 当外网接口使用动态IP地址时，如何使用SNAT策略?
3. DNAT策略的作用是什么，典型应用是什么?