iptables NAT转发

ssooking
2020-03-24 00:00:00 攻防渗透 流量转发

NAT

一. 什么是 NAT

NAT（Network Address Translation）译为网络地址转换。通常路由器在转发我们的数据包时，仅仅会将源MAC地址换成自己的MAC地址，但是NAT技术可以修改数据包的源地址、目的地址以及源端口、目的端口等信息。

二. NAT的作用

NAT技术最常见的应用就是通过修改源IP地址实现内网多主机使用一个公网地址接入互联网。NAT技术通常用于端口和流量的转发、重定向，实现如端口映射、跨网络访问、流量代理等功能。

二. iptables实现NAT转发

1.语法及参数介绍

```
1  iptables [-t TABLE] COMMAND CHAIN [num] 匹配条件 -j 处理动作
```

要使用iptables的NAT功能，我们首先需要**启用网卡的IP转发功能**

```
1  echo 1 > /proc/sys/net/ipv4/ip_forward
```

如果想要永久生效，我们要编辑 `/etc/sysctl.conf` 文件，设置 `net.ipv4.ip_forward = 1` ，然后用 `sysctl -p` 命令使配置文件生效。

我们使用** `-t nat` **参数指明使用nat表，因为iptables默认使用filter表。
nat表同filter表一样有三条缺省的"链"(chains):

```
1  POSTROUTING:定义进行源地址转换规则，重写数据包的源IP地址
2  PREROUTING:定义进行目的地址转换的规则，可以把外部访问重定向到其他主机上
3  OUTPUT:定义对本地产生的数据包的目的转换规则。
```

我们要利用iptables进行NAT转换时，使用的动作主要为SNAT、DNAT和REDIRECT:

```
1  SNAT:源地址转换
2  DNAT:目的地址转换
3  REDIRECT:端口重定向
```

(1) 规则操作

```
1  -A:在链的尾部添加一条规则
2  -D CHAIN [num]: 删除指定链中的第num条规则
3  -I CHAIN [num]:在指定链内第num条位置插入一条规则
4  -R CHAIN [num]: 替换链内指定位置的一条规则
```

(2) 源/目的IP地址

```
1  -s:指定源地址
2  --dst:指定目的地址
```

(3) 网络接口

```
1  -i:入站接口。对于`PREROUTING`链，只能用-i指定进来的网络接口
2  -o:出站接口。对于POSTROUTING和OUTPUT，只能用-o指定出去的网络接口
```

(4) 动作

```
1  ACCEPT:放行
2  DROP:丢弃
3  REJECT:拒绝
4  MASQUERADE:地址伪装
5  LOG:日志
6  MARK:标记
```

三. 源/目的转发实例

1.源NAT（SNAT）
更改所有来自192.168.1.0/24的数据包的源IP地址为123.4.5.100

```
1  iptables -t nat -A POSTROUTING -s 192.168.1.0/24 -o eth0 -j SNAT --to 123.4.5.100
```

2.目的NAT（DNAT）
更改所有来自192.168.1.0/24的数据包的目的ip地址为123.4.5.100

```
1  iptables -t nat -A PREROUTING -s 192.168.1.0/24 -i eth1 -j DNAT --to 123.4.5.100
```

3.IP映射实例
假设有这样的情况：A、B单位给自内网中部分用户要求建立自己的Web服务器对外发布信息。我们可以在防火墙的外部网卡上绑定多个合法公网IP地址，然后通过ip映射使发给其中某一个IP地址的包转发至内部某一用户的Web服务器上，并将该内部Web服务器的响应包伪装成该公网IP发出的包。

节点	内网IP	公网IP
A单位Web服务器	192.168.1.100	123.4.5.100
B单位Web服务器	192.168.1.200	123.4.5.200
linux防火墙	192.168.1.1（eth1）	123.4.5.1（eth0）

在进行NAT之前，我们需要先将分配给A、B单位的公网ip绑定到防火墙的外网接口：

```
1  ifconfig eth0 add 123.4.5.100 netmask 255.255.255.0
2  ifconfig eth0 add 123.4.5.200 netmask 255.255.255.0
```

对防火墙接收到的目的ip为123.4.5.100和123.4.5.200的所有数据包进行目的NAT(DNAT):

```
1  iptables -A PREROUTING -i eth0 -d 123.4.5.100 -j DNAT --to 192.168.1.100
2  iptables -A PREROUTING -i eth0 -d 123.4.5.200 -j DNAT --to 192.168.1.200
```

其次，对防火墙接收到的源ip地址为192.168.1.100和192.168.1.200的数据包进行源NAT(SNAT):

```
1  iptables -A POSTROUTING -o eth0 -s 192.168.1.100 -j SNAT --to 123.4.5.100
2  iptables -A POSTROUTING -o eth0 -s 192.168.1.200 -j SNAT --to 123.4.5.200
```

这样，所有目的ip为123.4.5.100和123.4.5.200的数据包都将分别被转发给192.168.1.100和192.168.1.200;
而所有来自192.168.1.100和192.168.1.200的数据包都将分别被伪装成由123.4.5.100和123.4.5.200，从而也就实现了ip映射。

四.端口转发实例

1.本机端口转发

把发往本机80端口的数据重定向到8080端口

```
1  iptables -t nat -A PREROUTING -p tcp --dport 80 -j REDIRECT --to-ports 8080
```

2.远程端口转发

把访问123.4.5.100:8080的数据包转发到123.4.5.200:80

```
1  iptables -t nat -A PREROUTING -d 123.4.5.100 -p tcp --dport 8080 -j DNAT --to-destination 123.4.5.200:8
```

多网卡问题：iptables学习笔记：端口转发命令优化

❮ nc端口转发

cobaltstrike4.0 cracked ❯