使用 iptables 转发内网端口 | yyrcd

https://blog.yyrcd.com/posts/iptables/

None Tue May, 18 15:18

术语

LAN: Local Area Network WAN: Wide Area Network

NAT: Network Address Translation

SNAT: Source Network Address Translation 内网多台机器由路由器连起来，内网机器访问外网，路由器将数据包的报头中的源地址替换成路由器的ip。

DNAT: Destination Network Address Translation 外网通过防火墙访问处于内网的web服务，外网访问防火墙，防火墙将目标地址改写成web服务器的内网ip。

内网端口转发

例如：转发内网服务器中的 redis 端口 内网服务器 ip: 10.11.11.11 公网服务器 ip: 69.12.12.12 redis 在内网服务器 30000 端口

开启系统端口转发

```
sudo vim /etc/sysctl.conf
```

```
net.ipv4.ip_forward=1
```

设置 iptables

```
sudo iptables -t nat -A PREROUTING -p tcp -d 69.12.12.12 --dport 30000 -j DNAT --to-destination 10.11.11.11
sudo iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
```

确认结果

```
sudo iptables -t nat -L -vn
Chain PREROUTING (policy ACCEPT 4 packets, 208 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 DNAT       tcp  --  *      *       0.0.0.0/0            69.12.12.12       tcp dpt:30000 to:10.11.11.11

Chain POSTROUTING (policy ACCEPT 5 packets, 403 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 MASQUERADE  all  --  *      eth0     0.0.0.0/0            0.0.0.0/0
```

ufw 配置 forward policy

如果开启了ufw，forward 默认 policy 被更改为 drop 可以用以下命令来确认

```
sudo iptables -L FORWARD
```

output为

```
Chain FORWARD (policy DROP)
target     prot opt source               destination
```

解决办法为 ufw 可以配置转发规则，例如：开启经过 eth0 网卡，转发至 10.11.11.11:30000 端口的所有 tcp 数据包

```
sudo ufw route allow in on eth0 out on eth0 to 10.11.11.11 port 30000 proto tcp
```

Reference:

- iptables详解 | Bruce's Blog
- 通过iptables实现端口转发和内网共享上网
- 利用 iptables 实现中继(中转/端口转发)加速 | 轻时代
- iptables中DNAT、SNAT和MASQUERADE的理解-Linux运维日志
- tcpdump - Linux Wiki