目录

原理 1
配置 1
我们访问银行 1
阿里云上的配置 1
xx 中心防火墙上的配置 1
iptables 代理配置 1
银行访问我们 2
专线路由器配置 2
iptables 代理配置 2

原理

数据包流转

我们访问银行：
阿里云服务器--→xx 中心防火墙--->iptables 服务器--->专线路由器--->银行

银行访问我们：
银行--→专线路由器--→iptables 服务器--→市民中心防火墙--->阿里云服务器

配置

我们访问银行

阿里云上的配置

将发向 12.1.1.117 的数据包目的地址转发到市民中心防火墙
#-A OUTPUT -p tcp -d 12.1.1.x/32 -j DNAT --to-destination 122.224.66.xx
-A OUTPUT -p tcp -d 12.1.1.1x7/32 -j DNAT --to-destination 122.224.66.xx

市民中心防火墙上的配置

防火墙接受请求，配置 nat，转发到内网的 iptables 服务器上
interface GigabitEthernet0/2
nat server protocol tcp global 122.224.66.xx 12074 inside 192.168.1.15 12074

iptables 代理配置

将源地址为 120.26.122.xx 的数据包目的地址改为 12.1.1.xx，通过专线到银行
-A PREROUTING -s 120.26.122.xx/32 -i eth1 -p tcp -m tcp --dport 12074 -j DNAT --to-destination 12.1.1.117
-A POSTROUTING -s 120.26.122.xx/32 -p tcp -j SNAT --to-source 192.168.0.200

至此我们访问银行 ok！

银行访问我们

银行访问我们是直接访问专线地址，我们自己转发到我们的阿里云服务器上

专线路由器配置

将银行的请求转发到内网的 iptables 服务器上

iptables 代理配置

将目的端口为 9011 的数据包的目的地址改为 120.26.122.xx，转发到我们服务器上

-A PREROUTING -i eth0 -p tcp -m tcp --dport 9011 -j DNAT --to-destination 120.26.122.xx

-A POSTROUTING -p tcp -m tcp --dport 9011 -j SNAT --to-source 192.168.1.15

至此银行访问我们 ok！

重点

路由是重点，如果路由配置不对，也会导致不同，毕竟一台服务器连了两个网络

```
[root@route ~]# route  -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
112.124.49.247  192.168.1.1     255.255.255.255 UGH   0      0        0 eth1
120.26.122.216  192.168.1.1     255.255.255.255 UGH   0      0        0 eth1
12.1.1.117      192.168.0.1     255.255.255.255 UGH   0      0        0 eth0
12.1.1.0        192.168.0.1     255.255.255.0   UG    0      0        0 eth0
192.168.1.0     0.0.0.0         255.255.255.0   U     0      0        0 eth1
192.168.0.0     0.0.0.0         255.255.255.0   U     0      0        0 eth0
169.254.0.0     0.0.0.0         255.255.0.0     U     1002   0        0 eth0
0.0.0.0         192.168.0.1     0.0.0.0         UG    0      0        0 eth0
```

重要默认路由指向专线

route add default gw 192.168.0.1