

# 知 SecPath ACG1000 端口映射不成功案例

NAT 马雷勇 2019-08-16 发表

## 组网及说明

最简组网, ACG1000出口, ge11连外线, ge1连内线核心

## 问题描述

SecPath ACG1000 端口映射不成功, 将内部服务器http 8080端口映射到公网8080端口外网无法访问

## 过程分析

1、端口映射目的NAT配置查看,

### 目的NAT规则

源地址	any	+ 新建
目的地址	out_ip	+ 新建
服务	TCP8080	
接口	ge11	
转换类型	<input type="radio"/> 地址映射 <input checked="" type="radio"/> 端口映射 <input type="radio"/> 不转换	
转换后IP	10.20.50.3	
转换后端口	8080 (1-65535)	
日志	<input checked="" type="checkbox"/>	

out\_ip为公网ip,

2、测试外网端口连通性, 以及内网服务器连通性端口开放情况

- (1) 修改http服务端端口8080, 外网通可以登录设备
- (2) 设备上ping以及tcp syn测试内网服务器端口正常开放

目的地址	10.20.50.3 (4-253)
端口	8080 (1-65535)
探测包数目	3 (1-10)

TCP Syn包探测结果

```
tcpsyn to 10.20.50.3:8080
1 TCP ACK from 10.20.50.3:8080
2 TCP ACK from 10.20.50.3:8080
3 TCP ACK from 10.20.50.3:8080
```

3、外网口抓包如下, 但是内网口没有任何8080端口报文

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	128.143	32.234	TCP	74	55902 > http-alt [SYN] Seq=0 Win=5840 Len=0 MSS=1400 SACK_PERM=1 TSval=1559939684 TSecr=0
2	2.998418	128.143	32.234	TCP	74	55902 > http-alt [SYN] Seq=0 Win=5840 Len=0 MSS=1400 SACK_PERM=1 TSval=1559942684 TSecr=0
3	8.998337	128.143	32.234	TCP	74	55902 > http-alt [SYN] Seq=0 Win=5840 Len=0 MSS=1400 SACK_PERM=1 TSval=1559948684 TSecr=0

即外网口收到公网用户访问8080端口的请求, 但是没有从内网口发给内网服务器

4、telnet/ssh登录ACG1000查看有无nat转换

debug ip nat

访问后dis log debug x.x.128.143, 查看已匹配目的NAT进行转换

```
3C# dis log debug [redacted] 128.143
3C# dis log debug [redacted] 128.143
2019-08-15 18:26:55> NAT: srcIp=[redacted] 128.143, dstIp=[redacted] 32.234, inif=ge11, find dest nat rule:rule_id=1
2019-08-15 18:26:55> NAT: NAT*: [redacted] 128.143:1941 [redacted] 32.234:8080 >> [redacted] 128.143:19417 -> 10.20.50.3:8080
3C#
```

5、查看路由配置, 确认为何地址转换了但是没有从内网口发出

- (1) 路由表正常
- (2) 配置了策略路由

### 策略路由

新建 删除 优先级								
ID	入口	源地址	目的地址	用户	服务	应用	下一跳/出接口	操作
1	<input checked="" type="checkbox"/>	any	any	any	any	any	[redacted] 32.233	<input checked="" type="checkbox"/>

入口是any所有 (正常应该是内网接口、内网对应地址段), 所以外网发起的报文到了设备上查路由又匹配策略路由被强制扔到公网去了

## 解决方法

修改策略路由入接口为内网口或者删除策略路由