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

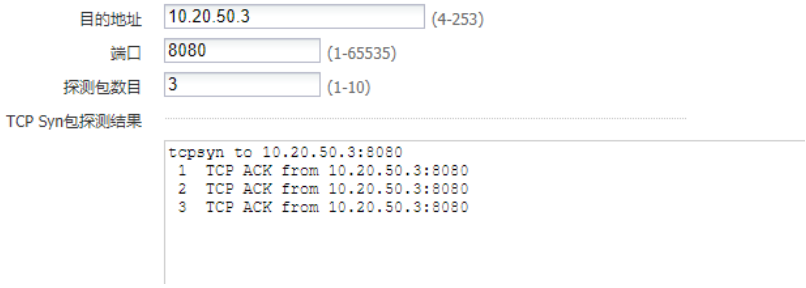
1、端口映射目的NAT配置查看，

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



3、外网口抓包如下，但是内网口没有任何8080端口报文

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

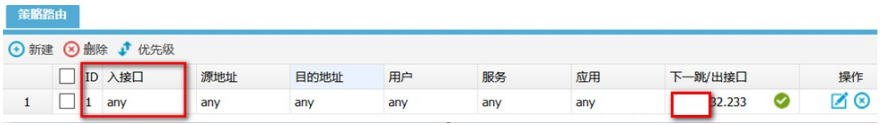
debug ip nat

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

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



入接口是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