SecPath ACG100 控制策略限制服务端口不生效

ACG1000 曾招维 2024-07-08 发表

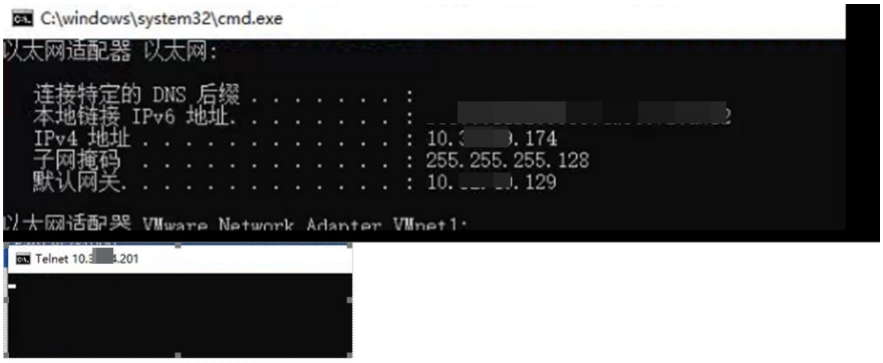
问题描述

设备新开局做了控制策略限制tcp 9000端口服务，发现不生效，但ICMP正常可控。控制策略有命中次数增加，ACG1000的web页面全局抓包看tcp三次握手成功，无全局白名单相关配置。

设备软件版本6616P02

现象：

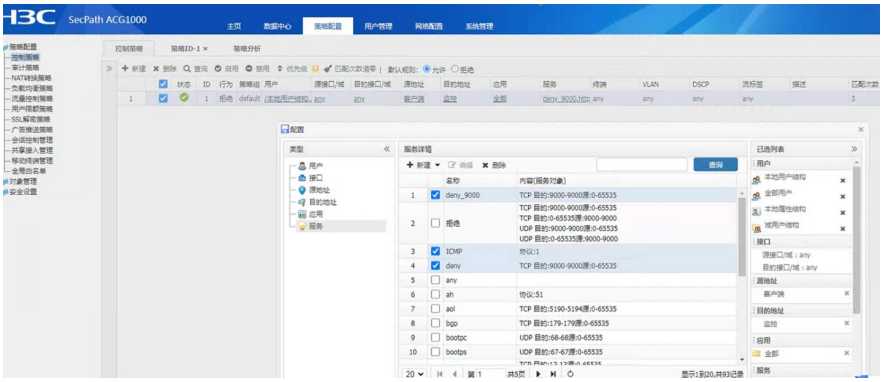
测试终端10.X.X.174 telnet 10.X.X.201 9000能通。

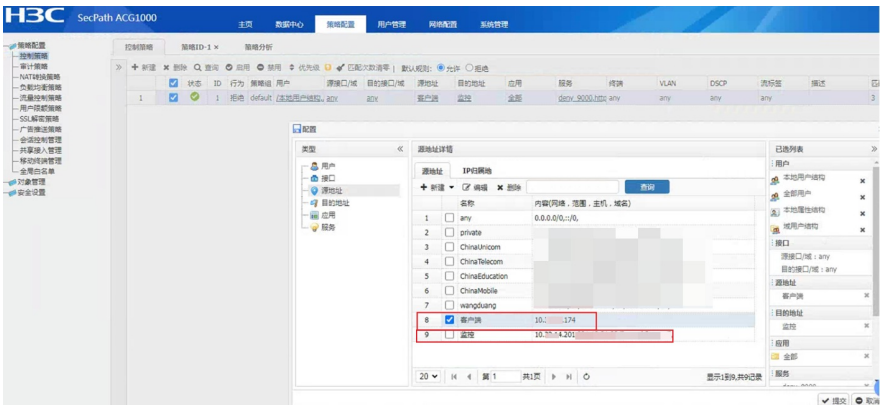


点击命中次数数值显示出测试流量

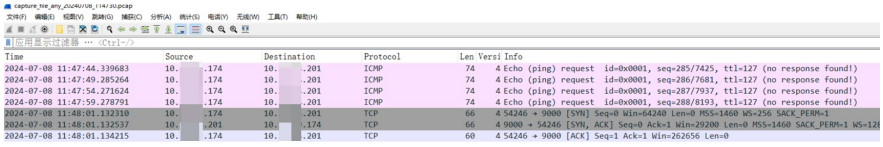
过程分析

1、基本配置确认：用户范围选择正确，源地址、目的地址、服务与真实流量特征相符。





2、ACG1000全局抓包，流量确实是上了ACG1000，ICMP正常拦截，9000端口流量未拦截。



3、检查命令行配置，无全局白名单配置，但控制策略白名单功能默认开启。

!policy-group
policy-group 缃戠笂浜ゆ槗
policy default-action permit
policy white-list enable
!

解决方法

进入命令行ACG1000-SE(config)# policy white-list disable 关闭控制策略白名单功能后，telnet测试发现已无法连接。

原因说明：

控制策略有一个报文放通识别应用的过程，即放通服务的tcp三次握手，识别出应用然后做控制动作，policy white-list enable 就是开启放通进行报文识别的过程。当前ACG1000只支持命令行关闭控制策略白名单功能，web界面无法单纯地限制tcp syn报文，后期建议通过应用层确认ACG1000的控制策略效果。