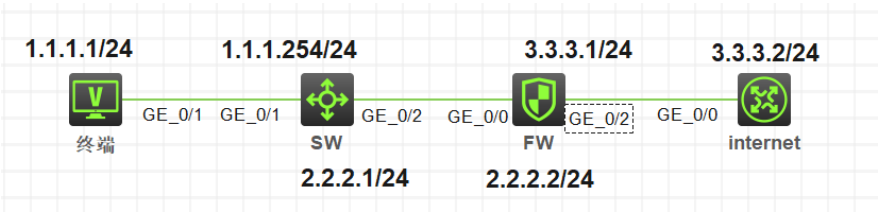
防火墙配置后无法ssh、telnet登录设备

NAT 杨玉琦 2022-03-28 发表

组网及说明



如上图组网，反馈远程登录设备配置后突然ssh中断，后无法远程登录设备，并且在SW上直连ping不通。

问题描述

远程登录设备配置后突然ssh中断，后无法远程登录设备，并且在SW上直连ping不通。

过程分析

1、排查路径上设备路由是否正常

通过dis ip routing-table x.x.x.x（目的地址）来排查路径上路由是否正常，排查后发现路由均存在

2、排查FW上安全策略以及安全域配置是否正常

通过dis security-zone查看接口是否有划入安全域，通过dis security-policy ip查看是否存在终端所在安全域到local的允许安全策略，排查后发现配置均正常

3、debug信息确认报文是否上到设备以及如何转发，查看会话看详细信息

debug ip packet acl xx（acl写ping测试的终端源地址与设备上的目的地址）
debug ip info acl xx
debug security-policy packet ip acl xx　//确认安全策略是否放行，避免其他未关注到策略导致报文被deny
debug aspf packet acl xx　　//确认是否为来回路径不一致导致丢包

排查后发现debug ip packet部分仅有入方向报文，此通过如下命令查看会话发现有回包的会话，但回包会话中的destination变成了其他的地址，而不是1.1.1.1。
dis session table ipv4 source-ip 1.1.1.1 destination-ip 2.2.2.2 verbose

后详细了解故障前客户配置了全局nat，检查后发现全局nat中存在策略的匹配条件为any，动作为dnat。因为匹配条件为any，因此终端ping防火墙的报文被转换目的地址，符合看会话中回包地址非1.1.1.1的情况。

解决方法

删除匹配条件为any的全局nat策略后正常。