某局点 F1000-AI-55 安全策略匹配异常

域间策略/安全域 陈阳 2024-06-05 发表

组网及说明

不涉及

问题描述

某局点一台F1000-AI-55作为中间设备，二层透传，测试发现如果配置了any-any的全通策略，那么业务正常，但此时查看会话流量并未匹配全通策略，将全通策略禁用后，业务不通。

过程分析

从测试会话上分析，业务流量并未匹配全通策略，但全通策略禁用后，业务就不通了，为了进一步判断流量的匹配情况，先将全通策略禁用，在防火墙debugging security-policy，然后发起测试，此时命令行没有信息打印，所以怀疑报文没有到防火墙，往上行设备排查，查看路由情况，发现此设备没有对应路由。

进一步分析路由消失原因，发现配置的静态路由，并结合了track：

ip route-static 0.0.0.0 0 1.1.1.2 track 1

查看track 状态发现negative

```
[H3C]dis track all
Track ID: 1
  State: Negative
  Duration: 0 days 0 hours 0 minutes 2 seconds
  Tracked object type: BFD
  Notification delay: Positive 0, Negative 0 (in seconds)
  Tracked object:
    BFD session mode: Echo
    Outgoing interface: GigabitEthernet0/1
    VPN instance name: --
    Remote IP: 1.1.1.2
    Local IP: 1.1.1.1
```

BFD会话状态down：

```
[H3C]dis bfd session
 Total sessions: 1       Up sessions: 0       Init mode: Active
 IPv4 session working in echo mode:
 LD            SourceIP       DestinationIP   State   Holdtime    Interface
 33793          1.1.1.1        1.1.1.2         Down    0ms         GE0/1
```

测试将any-any全通策略启用后，BFD会话UP，track状态也正常，此时路由生效，报文转发正常。

解决方法

针对BFD的探测报文也进行放通即可。

业务流量过防火墙，特征并未匹配全通策略，但是却要启用全通规则才正常，一般有如下情况：

1、终端发起访问后，服务器会主动发起新的会话连接终端，这种情况就需要针对服务器的新会话进行放通；

2、安全策略影响了路由的学习或建立，一般出现在动态路由、结合NQA/Track探测的场景。

可以结合debug、抓包等手段辅助判断。