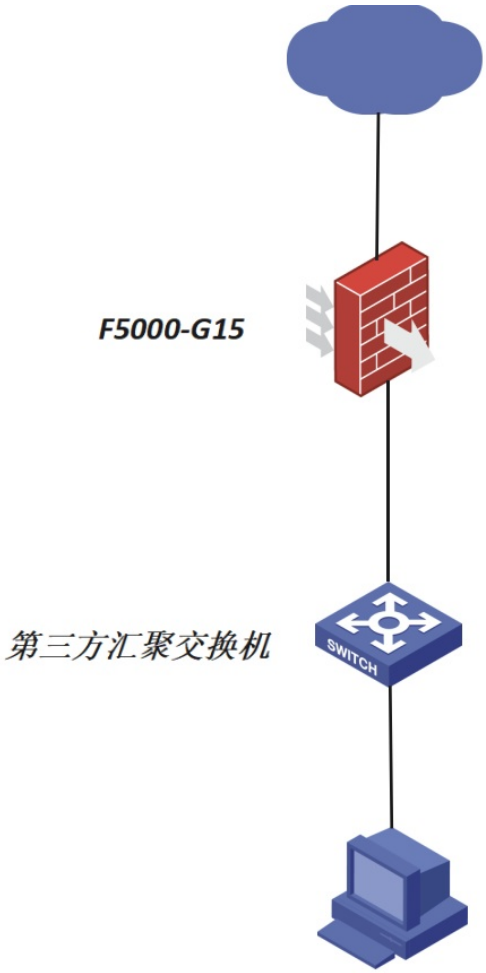
过防火墙tracert不通问题

攻击防范 ASPF 域间策略/安全域 zhiliao_HUFoOo 2022-10-28 发表

组网及说明



问题描述

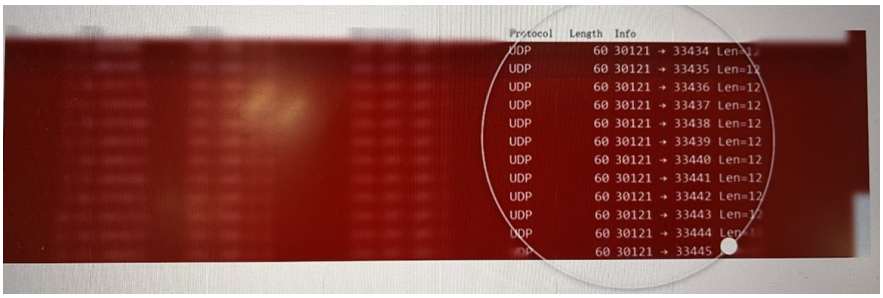
在汇聚第三方交换机上tracert互联网的某一个地址，不通，但是在我们的防火墙设备上tracert同一个互联网地址可以通，该交换机上有配置到华三防火墙的路由。因此怀疑问题是出在交换机到防火墙中间。

过程分析

1、首先开启命令dis session table ipv4 source-ip xxxx destination-i p xxxx verbose，发起测试，发现防火墙端生成了会话，接收到了报文，但是并没有发出去，但是之前在防火墙上tracert外网是可以通的所以不存在网络故障问题：

Initiator: Source IP/port: xxxx/30121 Destination IP/port: xxxx/33442 DS-Lite tunnel peer: - VPN instance/VLAN ID/Inline ID: -/-/- Protocol: UDP(17) Inbound interface: Vlan-interface100 Source security zone: Trust Responder: Source IP/port: xxxx/33442 Destination IP/port: xxxx/30121 DS-Lite tunnel peer: - VPN instance/VLAN ID/Inline ID: -/-/- Protocol: UDP(17) Inbound interface: Route-Aggregation1 Source security zone: Untrust State: UDP_OPEN Application: GENERAL_UDP Rule ID: 0 Rule name: T-U Start time: 2022-10-11 15:14:47 TTL: 21s Initiator->Responder: 1 packets 40 bytes Responder->Initiator: 0 packets 0 bytes

2、进一步tracert测试，在防火墙端开启全局抓包，发现我们确实收到了报文，但是没有继续往目的地址发包：



3、综上怀疑在防火墙上配置了一些操作导致数据包被丢弃，检查安全域的配置发现存在攻击防范，因此让渠道undo掉这个攻击防范，问题解决。

```
#
security-zone name Trust
 import interface GigabitEthernet1/0/1
 import interface Vlan-interface80
 import interface Vlan-interface100
 import interface Ten-GigabitEthernet1/1/0 vlan 1 to 4094
 import interface Ten-GigabitEthernet1/1/1 vlan 1 to 4094
 attack-defense apply policy 1
#
security-zone name DMZ
#
security-zone name Untrust
 import interface GigabitEthernet1/0/2
 import interface GigabitEthernet1/0/3
 import interface Route-Aggregation1
 attack-defense apply policy 1
#
```

解决方法

undo掉攻击防范策略问题解决