

知 防火墙二层部署丢包典型案例分析

域间策略/安全域 孔凡安 2022-11-11 发表

组网及说明

不涉及

告警信息

不涉及

问题描述

防火墙二层部署，组网简化如下：

客户端----- (BAGG2) 防火墙 (BAGG1) -----服务器

现场过防火墙探测服务器的端口不通。

过程分析

首先查看防火墙会话信息如下：

```
Slot 2:
Total sessions found: 0
<B3F_wL_GF_Tencent_FW5030>disp se ta ipv4 sou 172.30.11.140 dest 172.30.146
Slot 1:
Initiator:
Source IP/port: 172.30.11.140/50029
Destination IP/port: 172.30.146.48/15139
DS-Lite tunnel peer: -
VPN instance/VLAN ID/Inline ID: -/713/-
Protocol: TCP(6)
Inbound interface: Bridge-Aggregation2
Source security zone: Trust
Responder:
Source IP/port: 172.30.146.48/15139
Destination IP/port: 172.30.11.140/50029
DS-Lite tunnel peer: -
VPN instance/VLAN ID/Inline ID: -/713/-
Protocol: TCP(6)
Inbound interface: Bridge-Aggregation1
Source security zone: Untrust
State: TCP_SYN_SENT
Application: GENERAL_TCP
Rule ID: 2
Rule name: 股份访问腾讯云
Start time: 2022-11-11 11:15:29 TTL: 29s
Initiator->Responder: 2 packets 140 bytes
Responder->Initiator: 0 packets 0 bytes

Total sessions found: 1
```

TCP连接状态为TCP_SYN_SENT,说明防火墙收到了第一个SYN报文。

由于防火墙二层部署,通过debug查看ip转发无回显,所以直接在防火墙上抓包,查看是否收到服务器端回应的syn/ack报文。

图示: 防火墙收到SYN报文,并转发。根据ip.id字段一致判断为同一个报文。

Time	Source	Destination	Protocol	Time to Identification	Total Len	Ac	Identify
1 2022-11-11 10:21:42.166667	172.30.11.140	172.30.146.48	TCP	127 86295 (12282)	52	0	0 [TCP Retransmission] [TCP Port numbers reused] 50240 + 15139 [SYN] Seq=0 Min=0 Len=0
2 2022-11-11 10:21:42.166667	172.30.11.140	172.30.146.48	TCP	127 86295 (12282)	52	0	0 [TCP Retransmission] [TCP Port numbers reused] 50240 + 15139 [SYN] Seq=0 Min=0 Len=0
3 2022-11-11 10:21:42.166667	172.30.146.48	172.30.11.140	TCP	63 86000 (0)	52	1	1 [TCP Retransmission] [TCP Port numbers reused] 50240 + 15139 [SYN] Seq=0 Min=0 Len=0
4 2022-11-11 10:21:43.205959	172.30.146.48	172.30.11.140	TCP	63 86000 (0)	52	1	1 [TCP Retransmission] [TCP Port numbers reused] 50240 + 15139 [SYN] Seq=0 Min=0 Len=0
5 2022-11-11 10:21:43.186656	172.30.146.48	172.30.11.140	TCP	127 86295 (12282)	52	0	0 [TCP Retransmission] [TCP Port numbers reused] 50240 + 15139 [SYN] Seq=0 Min=0 Len=0
6 2022-11-11 10:21:43.186657	172.30.11.140	172.30.146.48	TCP	127 86295 (12282)	52	0	0 [TCP Retransmission] [TCP Port numbers reused] 50240 + 15139 [SYN] Seq=0 Min=0 Len=0
7 2022-11-11 10:21:45.153379	172.30.146.48	172.30.11.140	TCP	63 86000 (0)	52	1	1 [TCP Retransmission] [TCP Port numbers reused] 50240 + 15139 [SYN] Seq=0 Min=0 Len=0
8 2022-11-11 10:21:47.207927	172.30.146.48	172.30.11.140	TCP	63 86000 (0)	52	1	1 [TCP Retransmission] [TCP Port numbers reused] 50240 + 15139 [SYN] Seq=0 Min=0 Len=0

通过抓包可以看出,防火墙收到了SYN/ACK报文,如果通过ip.id来看,似乎这是同一组报文,防火墙转发没有问题。

Time	Source	Destination	Protocol	Time to Identification	Total Len	Ac	Identify
1 2022-11-11 10:21:42.166667	172.30.11.140	172.30.146.48	TCP	127 86295 (12282)	52	0	0 [TCP Retransmission] [TCP Port numbers reused] 50240 + 15139 [SYN] Seq=0 Min=0 Len=0
2 2022-11-11 10:21:42.166667	172.30.11.140	172.30.146.48	TCP	127 86295 (12282)	52	0	0 [TCP Retransmission] [TCP Port numbers reused] 50240 + 15139 [SYN] Seq=0 Min=0 Len=0
3 2022-11-11 10:21:42.166667	172.30.146.48	172.30.11.140	TCP	63 86000 (0)	52	1	1 [TCP Retransmission] [TCP Port numbers reused] 50240 + 15139 [SYN] Seq=0 Min=0 Len=0
4 2022-11-11 10:21:43.205959	172.30.146.48	172.30.11.140	TCP	63 86000 (0)	52	1	1 [TCP Retransmission] [TCP Port numbers reused] 50240 + 15139 [SYN] Seq=0 Min=0 Len=0
5 2022-11-11 10:21:43.186656	172.30.146.48	172.30.11.140	TCP	127 86295 (12282)	52	0	0 [TCP Retransmission] [TCP Port numbers reused] 50240 + 15139 [SYN] Seq=0 Min=0 Len=0
6 2022-11-11 10:21:43.186657	172.30.11.140	172.30.146.48	TCP	127 86295 (12282)	52	0	0 [TCP Retransmission] [TCP Port numbers reused] 50240 + 15139 [SYN] Seq=0 Min=0 Len=0
7 2022-11-11 10:21:45.153379	172.30.146.48	172.30.11.140	TCP	63 86000 (0)	52	1	1 [TCP Retransmission] [TCP Port numbers reused] 50240 + 15139 [SYN] Seq=0 Min=0 Len=0
8 2022-11-11 10:21:47.207927	172.30.146.48	172.30.11.140	TCP	63 86000 (0)	52	1	1 [TCP Retransmission] [TCP Port numbers reused] 50240 + 15139 [SYN] Seq=0 Min=0 Len=0

但是结合会话状态来看,似乎无法对上。因为防火墙如果收到SYN/ACK报文并转发出去的话,状态机会变为TCP_SYN_RECV。

所以问题大概率可能出现在防火墙上。

继续查看报文,发现虽然No.3和No.4报文内容一样,但是时间确实相差1S多(上图绿色框),因此判断No.4报文为服务器侧重传的报文,而非防火墙转发的报文。

继续分析发现防火墙来回报文携带的vlan标签不一致,由于防火墙会话状态检测机制会检查报文携带的vlan标签,难道是安全策略阻断了?

但是现场反馈其他的IP是能通的,来回的vlan标签也不一致。

解决方法

基于以上分析判断现场应该开启了松散模式，但是没有放通反向的报文。

解决方案：松散模式下放通反向报文，使得反向报文能够建立会话。

