某局点过M9K防火墙IPV6业务时通时不通问题处理过程分享

IRF 域间策略/安全域 孔凡安 2023-06-16 发表

组网及说明

不涉及

告警信息

不涉及

问题描述

某局点反馈过M9K防火墙IPV6的SSH访问出现时通时不通的情况，而且故障时候看主会话和备份会话匹配了不同的安全策略。如下：

```
CPU 1 on slot 4 in chassis 1:
Initiator:
  Source      IP/port: 2409:806A:5AF0:2000::AC8:7278/55686
  Destination IP/port: 2409:806A:5AF0:2000::C447/22
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: Route-Aggregation11.3000
  Source security zone: Untrust
Responder:
  Source      IP/port: 2409:806A:5AF0:2000::C447/22
  Destination IP/port: 2409:806A:5AF0:2000::AC8:7278/55686
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: Route-Aggregation1.1998
  Source security zone: Trust
State: TCP_ESTABLISHED
Application: SSH
Rule ID: 20000
Rule name:
Start time: 2023-06-16 16:03:59  TTL: 1199s
Initiator->Responder:           9 packets       856 bytes
Responder->Initiator:         256 packets     28880 bytes

Total sessions found: 1

Slot 0 in chassis 2:
Total sessions found: 0

Slot 1 in chassis 2:
Total sessions found: 0

CPU 1 on slot 3 in chassis 2:
Total sessions found: 0

CPU 1 on slot 4 in chassis 2:
Initiator:
  Source      IP/port: 2409:806A:5AF0:2000::AC8:7278/55686
  Destination IP/port: 2409:806A:5AF0:2000::C447/22
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: Route-Aggregation11.3000
  Source security zone: Untrust
Responder:
  Source      IP/port: 2409:806A:5AF0:2000::C447/22
  Destination IP/port: 2409:806A:5AF0:2000::AC8:7278/55686
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: Route-Aggregation1.1998
  Source security zone: Trust
State: INACTIVE
Application: SSH
Rule ID: 23
Rule name:
Start time: 2023-06-16 16:03:59  TTL: 282s
Initiator->Responder:           0 packets         0 bytes
```

```
Responder->Initiator:           0 packets         0 bytes
```

过程分析

首先根据会话字段State可知1框上的会话（TCP_ESTABLISHED）为主会话，2框上的会话为备份会话（INACTIVE）。

其次，查看主备会话发现两条会话匹配了不同的安全策略，Rule23和Rule2000区别不做过多赘述。区别在于Rule2000是一条全通的策略，Rule23为明细化的策略。

现场主会话和备份会话对应的安全策略不同，怀疑存在流量二次上墙的情况，导致主会话的安全策略被刷新。备份会话无变化，所呈现的还是一开始匹配的安全策略。整个过程为：会话在1框创建，并同步给2框。此后流量从不同的接口上来，源目安全域无法匹配原来的策略，设备存在全通的策略，因此安全策略被刷新。但是2框同步过去的会话不会改变，依然匹配原来的明细策略。

根据该思路，进行debug调试，打印如下：

```
*Jun 16 16:12:08:360 2023 GA-6-A-7-M9006-(CMNET)-01 IP6FW/7/IP6FW_PACKET: -Chassis=1-Slot=4.1;
Receiving, interface = Route-Aggregation11.3000, version = 6, traffic class = 0,
flow label = 647106, payload length = 40, protocol = 6, hop limit = 61,
Src = 2409:806a:5af0:2000::ac8:7278, Dst = 2409:806a:5af0:2000::c447,
prompt: Received an IPv6 packet.

*Jun 16 16:12:08:360 2023 GA-6-A-7-M9006-(CMNET)-01 SESSION/7/TABLE: -Chassis=1-Slot=4.1;
 Tuple5(EVENT): 2409:806a:5af0:2000::ac8:7278/55600-->
                2409:806a:5af0:2000::c447/22(TCP(6))
 Session entry was created.
*Jun 16 16:12:08:360 2023 GA-6-A-7-M9006-(CMNET)-01 FILTER/7/PACKET: -Chassis=1-Slot=4.1; The packet is permitted. Src-ZOne=Untrust, Dst-ZOne=Trust;If-In=Route-Aggregation11.3000(7005), If-Out=Route-Aggregation1.1998(7006); Packet Info:Src-IP=2409:806a:5af0:2000::ac8:7278, Dst-IP=2409:806a:5af0:2000::c447, VPN-Instance=,Src-Port=55600, Dst-Port=22, Protocol=TCP(6), Application=ssh(13), Url-category=invalid(65535), ACL=3007, Rule-ID=23.

*Jun 16 16:12:08:360 2023 GA-6-A-7-M9006-(CMNET)-01 IP6FW/7/IP6FW_PACKET: -Chassis=1-Slot=4.1;
Sending, interface = Route-Aggregation1.1998, version = 6, traffic class = 0,
flow label = 647106, payload length = 40, protocol = 6, hop limit = 60,
Src = 2409:806a:5af0:2000::ac8:7278, Dst = 2409:806a:5af0:2000::c447,
prompt: Sending the packet from Route-Aggregation11.3000 through Route-Aggregation1.1998.

*Jun 16 16:12:08:360 2023 GA-6-A-7-M9006-(CMNET)-01 SESSION/7/TABLE: -Chassis=1-Slot=4.1;
 Tuple5(EVENT): 2409:806a:5af0:2000::ac8:7278/55600-->
                2409:806a:5af0:2000::c447/22(TCP(6))
 Session entry was backuped.
*Jun 16 16:12:08:576 2023 GA-6-A-7-M9006-(CMNET)-01 SESSION/7/TABLE: -Chassis=2-Slot=4.1;
 Tuple5(EVENT): 2409:806a:5af0:2000::ac8:7278/55600-->
                2409:806a:5af0:2000::c447/22(TCP(6))
 Session entry was restored.
*Jun 16 16:12:08:362 2023 GA-6-A-7-M9006-(CMNET)-01 SESSION/7/TABLE: -Chassis=1-Slot=4.1;
 Tuple5(EVENT): 2409:806a:5af0:2000::ac8:7278/55600-->
                2409:806a:5af0:2000::c447/22(TCP(6)) ICMPv6_ERROR INTERNAL MATCHED
*Jun 16 16:12:09:380 2023 GA-6-A-7-M9006-(CMNET)-01 SESSION/7/TABLE: -Chassis=1-Slot=4.1;
 Tuple5(EVENT): 2409:806a:5af0:2000::ac8:7278/55600-->
                2409:806a:5af0:2000::c447/22(TCP(6)) ICMPv6_ERROR INTERNAL MATCHED
*Jun 16 16:12:09:425 2023 GA-6-A-7-M9006-(CMNET)-01 SESSION/7/TABLE: -Cha
```

ssis=1-Slot=4.1;
Tuple5(EVENT): 2409:806a:5af0:2000::ac8:7278/55600-->
2409:806a:5af0:2000::c447/22(TCP(6)) ICMPv6_ERROR INTERNAL MAT
CHED
*Jun 16 16:12:11:428 2023 GA-6-A-7-M9006-(CMNET)-01 SESSION/7/TABLE: -Cha
ssis=1-Slot=4.1;
Tuple5(EVENT): 2409:806a:5af0:2000::ac8:7278/55600-->
2409:806a:5af0:2000::c447/22(TCP(6)) ICMPv6_ERROR INTERNAL MAT
CHED
*Jun 16 16:12:11:473 2023 GA-6-A-7-M9006-(CMNET)-01 SESSION/7/TABLE: -Cha
ssis=1-Slot=4.1;
Tuple5(EVENT): 2409:806a:5af0:2000::ac8:7278/55600-->
2409:806a:5af0:2000::c447/22(TCP(6)) ICMPv6_ERROR INTERNAL MAT
CHED
*Jun 16 16:12:15:505 2023 GA-6-A-7-M9006-(CMNET)-01 SESSION/7/TABLE: -Cha
ssis=1-Slot=4.1;
Tuple5(EVENT): 2409:806a:5af0:2000::ac8:7278/55600-->
2409:806a:5af0:2000::c447/22(TCP(6)) ICMPv6_ERROR INTERNAL MAT
CHED
*Jun 16 16:12:19:556 2023 GA-6-A-7-M9006-(CMNET)-01 SESSION/7/TABLE: -Cha
ssis=1-Slot=4.1;
Tuple5(EVENT): 2409:806a:5af0:2000::ac8:7278/55600-->
2409:806a:5af0:2000::c447/22(TCP(6)) ICMPv6_ERROR INTERNAL MAT
CHED
*Jun 16 16:12:23:826 2023 GA-6-A-7-M9006-(CMNET)-01 SESSION/7/TABLE: -Cha
ssis=1-Slot=4.1;
Tuple5(EVENT): 2409:806a:5af0:2000::ac8:7278/55600-->
2409:806a:5af0:2000::c447/22(TCP(6)) ICMPv6_ERROR INTERNAL MAT
CHED
*Jun 16 16:12:32:036 2023 GA-6-A-7-M9006-(CMNET)-01 SESSION/7/TABLE: -Cha
ssis=1-Slot=4.1;
Tuple5(EVENT): 2409:806a:5af0:2000::ac8:7278/55600-->
2409:806a:5af0:2000::c447/22(TCP(6)) ICMPv6_ERROR INTERNAL MAT
CHED
*Jun 16 16:12:40:210 2023 GA-6-A-7-M9006-(CMNET)-01 SESSION/7/TABLE: -Cha
ssis=1-Slot=4.1;
Tuple5(EVENT): 2409:806a:5af0:2000::ac8:7278/55600-->
2409:806a:5af0:2000::c447/22(TCP(6)) ICMPv6_ERROR INTERNAL MAT
CHED

解决方法

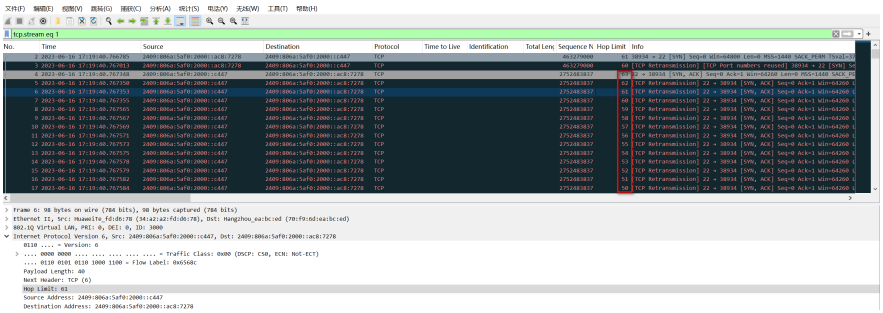
通过抓包判断，下行设备把报文又发到墙上导致环路，现场调整路由后正常。

debug以及抓包调试可以参考链接：

https://zhiliao.h3c.com/theme/details/215550

很遗憾，没有任何再次匹配安全策略的打印。怀疑是后续报文走了快转流程，debug打印不出来。

因此，建议现场抓取过防火墙的报文，查看是否存在流量二次上墙的情况。



通过抓包果然不负众望， syn/ack从RAGG11.3000发出去之后，又从RAGG11.3000收到了。然后再从RAGG11.3000发出去，如此循环往复，直到Hop Limit为零。