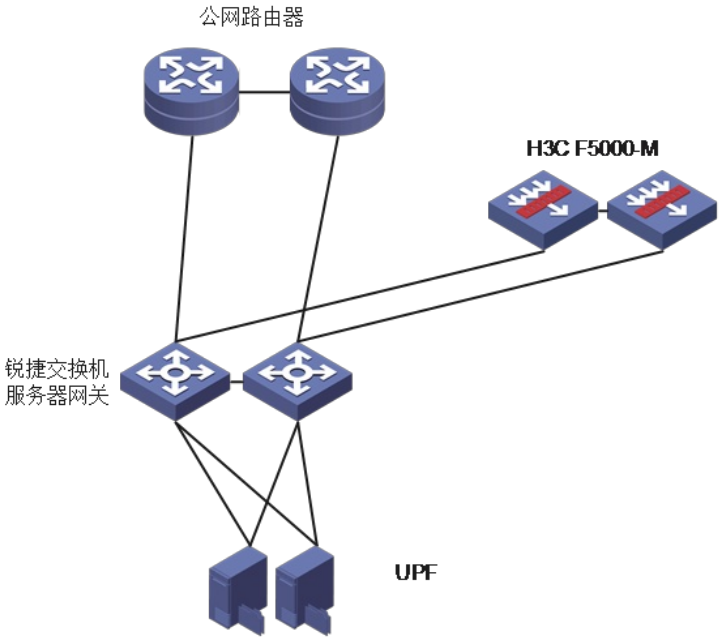
某局点F5000-M 防火墙转发丢包问题排查经验案例

会话同步 域间策略/安全域 ASPF 流量统计 **刘文峰** 2021-08-31 发表

组网及说明



问题描述

当前业务运行正常，UPF服务器往外ping 也是正常的，但是如果从锐捷交换机快ping 服务器会出现丢包问题，怀疑是锐捷交换机快ping机制问题导致，为了进一步定位，在防火墙上通过流量统计，看看是否丢在设备上。

过程分析

流统测试结果:

acl advanced 3990
 description liutong
 rule 0 permit icmp source x.x.x.2 0 destination x.x.x.40 0 counting
 rule 5 permit icmp source x.x.x.40 0 destination x.x.x.2 0 counting
#
traffic classifier liutong operator and
 if-match acl 3990
#
traffic behavior liutong
 filter permit
#
qos policy liutong
 classifier liutong behavior liutong
#
interface Route-Aggregation1.51
 description uT:Global:internet_untrust
 qos apply policy liutong inbound
 qos apply policy liutong outbound
 vlan-type dot1q vid 51
#
interface Route-Aggregation1.52
 description dT:Global:internet_trust
 qos apply policy liutong inbound
 qos apply policy liutong outbound
 vlan-type dot1q vid 52

```
SC-CD-4L&01-11A07&3U-HX-RGS6220-01#$rce[redacted].2 ntimes 500
Sending 500, 100-byte ICMP Echoes to [redacted].40, timeout is 2 seconds:
  < press Ctrl+C to break >
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!.!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 99 percent (498/500), round-trip min/avg/max = 1/2/4 ms.
SC-CD-4L&01-11A07&3U-HX-RGS6220-01#
SC-CD-4L&01-11A07&3U-HX-RGS6220-01#
```

```
<SC-CD-4L&01-11A07&16U-FW-F5000M-01>display qos policy interface Route-Aggregation 1.51 inbound
Interface: Route-Aggregation1.51
  Direction: Inbound
  Policy: liutong
   Classifier: liutong
     Matched : 500 (Packets) 73000 (Bytes)
     5-minute statistics:
      Forwarded: 0/0 (pps/bps)
      Dropped  : 0/0 (pps/bps)
     Operator: AND
     Rule(s) :
      If-match acl 3990
     Behavior: liutong
      Filter enable: Permit

<SC-CD-4L&01-11A07&16U-FW-F5000M-01>display qos policy interface Route-Aggregation 1.52 outbound
Interface: Route-Aggregation1.52
  Direction: Outbound
  Policy: liutong
   Classifier: liutong
     Matched : 500 (Packets) 73000 (Bytes)
     5-minute statistics:
      Forwarded: 0/0 (pps/bps)
      Dropped  : 0/0 (pps/bps)
     Operator: AND
     Rule(s) :
      If-match acl 3990
     Behavior: liutong
      Filter enable: Permit

<SC-CD-4L&01-11A07&16U-FW-F5000M-01>
```

```
<SC-CD-4L&01-11A07&16U-FW-F5000M-01>display qos policy interface Route-Aggregation 1.52 inbound
Interface: Route-Aggregation1.52
  Direction: Inbound
  Policy: liutong
    Classifier: liutong
      Matched : 500 (Packets) 73000 (Bytes)
      5-minute statistics:
      Forwarded: 0/0 (pps/bps)
      Dropped  : 0/0 (pps/bps)
      Operator: AND
      Rule(s) :
        If-match acl 3990
      Behavior: liutong
        Filter enable: Permit
<SC-CD-4L&01-11A07&16U-FW-F5000M-01>display qos policy interface Route-Aggregation 1.51 outbound
Interface: Route-Aggregation1.51
  Direction: Outbound
  Policy: liutong
    Classifier: liutong
      Matched : 498 (Packets) 72708 (Bytes)
      5-minute statistics:
      Forwarded: 0/0 (pps/bps)
      Dropped  : 0/0 (pps/bps)
      Operator: AND
      Rule(s) :
        If-match acl 3990
      Behavior: liutong
        Filter enable: Permit
<SC-CD-4L&01-11A07&16U-FW-F5000M-01>
```

远程查看现场抓包发现ping的方式，发现是每个包都会更改参数，因此在防火墙上每个包都会建立一条会话，出口现象会遵循这个

<SC-CD-4L&01-11A07&16U-FW-F5000M-01>dis session table ipv4 destination-ip x.x.x.40 p i v

Slot 1

Initiator:

Source IP/port: x.x.x.2/36860

Destination IP/port: x.x.x.40/2048

DS-Lite tunnel peer: -

VPN instance/VLAN ID/Inline ID: -/-/-

Protocol: ICMP(1)

Inbound interface: Route-Aggregation1.51

Source security zone: internet_Untrust

Responder:

Source IP/port: x.x.x.40/36860

Destination IP/port: x.x.x.2/0

DS-Lite tunnel peer: -

VPN instance/VLAN ID/Inline ID: -/-/-

Protocol: ICMP(1)

Inbound interface: Route-Aggregation1.52

Source security zone: internet_trust

State: ICMP_REQUEST

Application: ICMP

Rule ID: 15

Rule name: icmp_any

Start time: 2021-08-30 12:51:53 TTL: 28s

Initiator->Responder: 1 packets 128 bytes

Responder->Initiator: 0 packets 0 bytes

Initiator:

Source IP/port: x.x.x.2/36710

Destination IP/port: x.x.x.40/2048

DS-Lite tunnel peer: -

VPN instance/VLAN ID/Inline ID: -/-/-

Protocol: ICMP(1)

Inbound interface: Route-Aggregation1.51

Source security zone: internet_Untrust

Responder:

Source IP/port: x.x.x.40/36710

Destination IP/port: x.x.x.2/0

DS-Lite tunnel peer: -

VPN instance/VLAN ID/Inline ID: -/-/-

Protocol: ICMP(1)

Inbound interface: Route-Aggregation1.52

Source security zone: internet_trust

State: ICMP_REQUEST

Application: ICMP

Rule ID: 15

Rule name: icmp_any

Start time: 2021-08-30 12:51:38 TTL: 12s

Initiator->Responder: 1 packets 128 bytes

Responder->Initiator: 0 packets 0 bytes

Initiator:

Source IP/port: x.x.x.2/36677

Destination IP/port: x.x.x.40/2048

DS-Lite tunnel peer: -

VPN instance/VLAN ID/Inline ID: -/-/-

Protocol: ICMP(1)

Inbound interface: Route-Aggregation1.51

Source security zone: internet_Untrust

Responder:

Source IP/port: x.x.x.40/36677

Destination IP/port: x.x.x.2/0

DS-Lite tunnel peer: -
VPN instance/VLAN ID/Inline ID: -/-/-