SecPath F1000-AI-65(V7) 基于应用的出链路负载均衡针对抖音短视频无效

outbound链路负载均衡 应用审计 特征库 孔凡安 2021-12-06 发表

组网及说明

不涉及

问题描述

现场配置了基于应用的出链路负载均衡，对于某些应用（抖音短视频）不生效。
出链路有三条：

link 1-interface vlan200（移动500M） 专门用来跑视频，下载等业务类似抖音浏览绑定应用组app-group_video；
link 2-G1/0/3（移动500M）专门用来跑非关键业务，绑定应用组app-group_office；
link 3-dialer 0（电信adsl跑默认的，link 1 2不生效时，默认走这条）。
手机连上wifi刷抖音时，link3的数据一直在增加，link1变化不大。

过程分析

查看会话有些应用可以正确识别，走link1出去，但是抖音短视频并没有。

```
[QHWXC-B01_INT_WLAN_FW-F65]dis session ta ipv4 source-ip 172.17.64.30 destination-ip
59.39.0.152 v
Slot 1:
Initiator:
  Source      IP/port: 172.17.64.30/37446
  Destination IP/port: 59.39.0.152/443
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: Route-Aggregation1
  Source security zone: Trust
Responder:
  Source      IP/port: 59.39.0.152/443
  Destination IP/port: 116.25.47.2/5014
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: Dialer0
  Source security zone: Untrust
State: TCP_ESTABLISHED
Application: DOUYINDUANSHIPIN
Rule ID: 1
Rule name: test
Start time: 2021-12-01 14:27:10  TTL: 1183s
Initiator->Responder:          24 packets      2824 bytes
Responder->Initiator:          17 packets      6789 bytes
```

查看调度选的默认的链路3（Dialer口出去）

```
[QHWXC-B01_INT_WLAN_FW-F65]loadbalance schedule-test ip protocol tcp destination
59.39.0.152 destination-port 443 source 172.
17.64.30 source-port 37446
Slot 1:
    Matched virtual server: ##defaultvsforllbipv4##%%autocreatedbyweb%%
    Matched the default class.
    Forward type: Forwarding to link
    Selected link: link3
        Scheduling algorithm: Predictor

Slot 2:
    Matched virtual server: ##defaultvsforllbipv4##%%autocreatedbyweb%%
    Matched the default class.
    Forward type: Forwarding to link
    Selected link: link3
        Scheduling algorithm: Predictor
```

对比选对出接口的应用，如下：

```
Initiator:
  Source      IP/port: 172.17.64.47/40404
  Destination IP/port: 123.129.240.19/17788
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: UDP(17)
  Inbound interface: Route-Aggregation1
  Source security zone: Trust
Responder:
  Source      IP/port: 123.129.240.19/17788
  Destination IP/port: 183.239.166.10/30686
```

DS-Lite tunnel peer: -
VPN instance/VLAN ID/Inline ID: -/-/-
Protocol: UDP(17)
Inbound interface: Vlan-interface200
Source security zone: Untrust
State: UDP_READY
Application: IQIYIPPS
Rule ID: 1
Rule name:

Start time: 2021-12-01 14:18:33 TTL: 1190s
Initiator->Responder: 110 packets 8983 bytes
Responder->Initiator: 1 packets 149 bytes

解决方法
无
属于理解问题

收集设备的NBAR表项，没有地址和端口59.39.0.152/443。
所以一开始访问抖音，三次握手的时候无法识别成抖音，只能走默认出口。
看会话信息显示抖音是因为后续根据交互数据通过dpi识别出来了，这条流也不会更改出口，否则业务就断了。
后续会把目的ip和端口加入nbar表里，下次再访问抖音的时候，第一个包就识别出来了，链路负载生效。