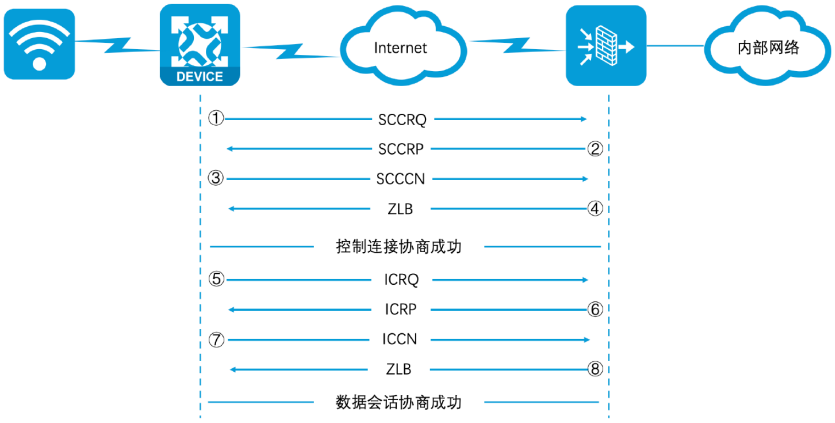
某局点防火墙接口震荡后L2TP业务终端用户无法正常上线问题处理

L2TP VPN 孔凡安 2024-05-17 发表

组网及说明

组网如下，防火墙作为LNS设备，与UPF（作为LAC）建立L2TP隧道。该隧道用来承载终端用户拨号之后建立对应的会话连接。



问题描述

故障现象：防火墙公网接口震荡之后，终端用户拨号失败，无法正常上线。查看防火墙上L2TP会话数量大约1000左右。

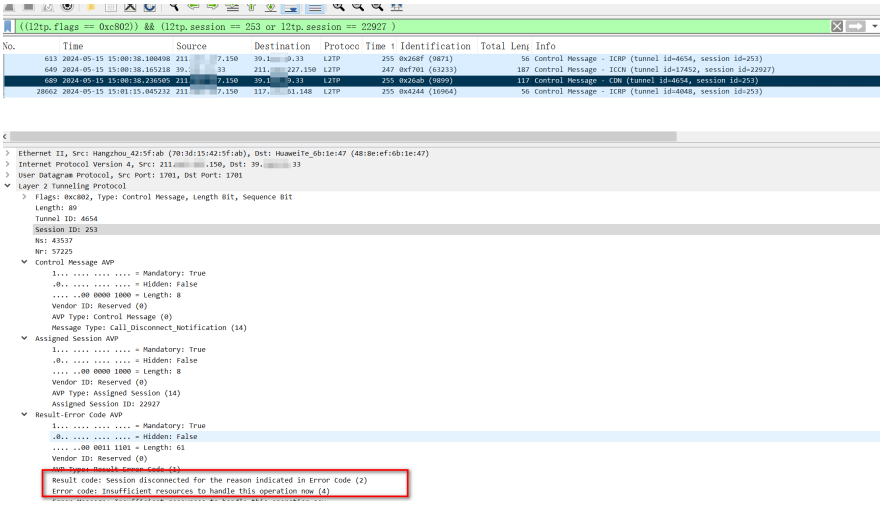
过程分析

分析防火墙CPU以及内存利用率均处于正常状态，初步判断问题与防火墙无关。对于L2TP的问题，最常见的排查方案就是抓取L2TP对应的报文。

对应的acl举例如下，1812和1813对应radius的认证和计费端口，如果涉及radius认证建议一并抓取。

```
#
acl advanced 3000
 rule 0 permit tcp destination-port eq 1812
 rule 5 permit tcp destination-port eq 1813
 rule 10 permit tcp destination-port eq 1701
 rule 15 permit udp destination-port eq 1812
 rule 20 permit udp destination-port eq 1813
 rule 25 permit udp destination-port eq 1701
 rule 30 permit udp source-port eq 1812
 rule 35 permit udp source-port eq 1813
 rule 40 permit udp source-port eq 1701
 rule 45 permit tcp source-port eq 1812
 rule 50 permit tcp source-port eq 1813
 rule 55 permit tcp source-port eq 1701
#
```

抓取报文后发现，设备（211.X.X.150）存在主动发送CDN拆线报文的的行为。如下图UPF发送ICCN报文建立会话连接之后，设备发送了CDN拆线报文结束了连接，报错原因显示为资源不足。



经过内部分析应该是L2TP高新建状态，LNS处理协议报文堵塞导致达到设备处理上限、客户端无法正常上线。

解决方法

对于存在批量用户上线的场景，应进行如下配置优化：

1.配置静态VA池，对应命令：

(1) 进入系统视图。

system-view

(2) 配置静态VA池。

l2tp virtual-template *template-number* **va-pool** *va-volume*

建议VA池大于最大用户上线数量，并关注内存占用。

2. 配置icrq报文限速，对应命令：**l2tp icrq-limit** 比如数值设置为50，让终端慢慢上线。

3. 关闭VA口反复updown的log信息：undo enable log updown （vt口下配置）