

组网及说明

无

问题描述

某局点客户反馈经过设备L1000-M NAT之后内网用户登录不了https://email.163.com (解析地址是123.125.50.22) 但是http://email.163.com可以正常使用且其他所有网站访问都正常。

过程分析

第一步

同一个终端直接配置运营商公网地址访问测试是可以打开https 163邮箱的

第二步

查看LB会话信息 可以看到客户端192.1.59.252 和服务器三次握手是可以建立的

```

Source      IP/port: 123.125.50.22/443
Destination IP/port: 218.10.148.122/25900
DS-Lite tunnel peer: -
VPN instance/VLAN ID/Inline ID: -/-/-
Protocol: TCP(6)
Inbound interface: GigabitEthernet1/0/16
State: TCP_ESTABLISHED
Application: HTTPS
Start time: 2018-04-10 15:14:47  TTL: 596s
Initiator->Responder:          4 packets          793 bytes
Responder->Initiator:          4 packets          348 bytes

Initiator:
Source      IP/port: 192.1.59.252/65297
Destination IP/port: 123.125.50.22/443
DS-Lite tunnel peer: -
VPN instance/VLAN ID/Inline ID: -/-/-
Protocol: TCP(6)
Inbound interface: Route-Aggregation10
Responder:
Source      IP/port: 123.125.50.22/443
Destination IP/port: 218.10.148.122/25904
DS-Lite tunnel peer: -
VPN instance/VLAN ID/Inline ID: -/-/-
Protocol: TCP(6)
Inbound interface: GigabitEthernet1/0/16
State: TCP_ESTABLISHED
Application: HTTPS
Start time: 2018-04-10 15:14:47  TTL: 595s
Initiator->Responder:          4 packets          793 bytes
Responder->Initiator:          4 packets          348 bytes

Total sessions found: 2
<LB>
<LB>
<LB>
<LB>display session table ipv4 destination-ip 123.125.50.22 verbose
Slot 1:
Total sessions found: 0
<T.R>

```

第三步 终端抓包分析

Wireshark抓包只发现终端主动发送了断开三次握手报文，没有具体原因，考虑现场是访问https的，建议使用HttpWatch抓包。

Wireshark抓包

No.	Time	Source	Destination	Protocol	Length	Info
7	5.878934	192.1.59.252	123.125.50.22	TCP	66	65244 > https [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_P
37	5.907887	123.125.50.22	192.1.59.252	TCP	66	https > 65244 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1024 SACK_P
38	5.907959	192.1.59.252	123.125.50.22	TCP	54	65244 > https [ACK] Seq=1 Ack=1 Win=65536 Len=0
40	5.911652	192.1.59.252	123.125.50.22	TLSv1.2	571	Client Hello
97	5.939434	123.125.50.22	192.1.59.252	TCP	60	https > 65244 [ACK] Seq=1 Ack=518 Win=6912 Len=0
98	5.942598	123.125.50.22	192.1.59.252	TLSv1.2	1078	Server Hello
99	5.942600	123.125.50.22	192.1.59.252	TCP	1078	[TCP segment of a reassembled PDU]
101	5.942721	192.1.59.252	123.125.50.22	TCP	54	65244 > https [ACK] Seq=518 Ack=2049 Win=65536 Len=0
129	5.971301	123.125.50.22	192.1.59.252	TLSv1.2	1078	Certificate
130	5.971302	123.125.50.22	192.1.59.252	TLSv1.2	186	Server Key Exchange, Server Hello Done
131	5.971409	192.1.59.252	123.125.50.22	TCP	54	65244 > https [ACK] Seq=518 Ack=3205 Win=65536 Len=0
137	5.975474	192.1.59.252	123.125.50.22	TLSv1.2	204	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Mes
154	6.003922	123.125.50.22	192.1.59.252	TLSv1.2	336	Encrypted Handshake Message, Change Cipher Spec, Encrypted Hand
178	6.044475	192.1.59.252	123.125.50.22	TCP	54	65244 > https [ACK] Seq=668 Ack=3487 Win=65024 Len=0
213	10.921813	192.1.59.252	123.125.50.22	TLSv1.2	107	Encrypted Alert
214	10.921867	192.1.59.252	123.125.50.22	TCP	54	65244 > https [FIN, ACK] Seq=721 Ack=3487 Win=65024 Len=0
228	10.949561	123.125.50.22	192.1.59.252	TCP	60	https > 65244 [FIN, ACK] Seq=3487 Ack=722 Win=8064 Len=0
229	10.949626	192.1.59.252	123.125.50.22	TCP	54	65244 > https [ACK] Seq=722 Ack=3488 Win=65024 Len=0
326	20.591664	192.1.59.252	123.125.50.22	TCP	66	65259 > https [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_P
331	20.619784	192.1.59.252	123.125.50.22	TCP	66	65263 > https [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_P
332	20.624758	123.125.50.22	192.1.59.252	TCP	66	https > 65259 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1024 SACK_P

## HttpWatch抓包

Started	Time Chart	I/P	Time	Sent	Received	Method	Result	Type	URL
00:00:00.000									
+ 9.000			42.026	0	0	GET	ERROR: INTERNET_CANNOT_CONNECT		https://webzj2.reg.163.com/1.0.1/ubb/index_d.htm?MGID=52242479217_79823ad6d4-4p4d...
-42.026			42.026	0	0	request			
00:02:09.137			42.028	0	0	GET	ERROR: INTERNET_CANNOT_CONNECT		https://webzj2.reg.163.com/1.0.1/ubb/index_d.htm?MGID=52242479217_79823ad6d4-4p4d...
+ 9.915			50.334	0	0	GET	(Aborted)		https://id.reg.163.com/getCarPoolBack-n-RS-200P1533423610118q4d-9f9Gj05Spd-mal1658...
-1.770			50.164	0	0	POST	(Aborted)		https://auth.com/v3/register/1.1/ubb/index_d.htm?MGID=479167961637K_Net383aard16u4d6a...

通过上述抓包可以判断出业务异常是因为访问webzj2.reg.163.com时出现异常的，再次分析PC的抓包文件，这个域名解析出地址是59.111.160.204

Frame 298: 94 bytes on wire (752 bits), 94 bytes captured (752 bits)
Ethernet II, Src: 70:f9:6d:e9:e8:8e (70:f9:6d:e9:e8:8e), Dst: Flextron_5d:4b:64 (00:21:cc:5d:4b:64)
Internet Protocol Version 4, Src: 202.97.224.69 (202.97.224.69), Dst: 192.1.59.252 (192.1.59.252)
User Datagram Protocol, Src Port: domain (53), Dst Port: 61122 (61122)
Domain Name System (response)
[Request In: 294]
[Time: 0.263794000 seconds]
Transaction ID: 0xbb2e
Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 1
Authority RRs: 0
Additional RRs: 0
Queries
webzj2.reg.163.com: type A, class IN
Answers
webzj2.reg.163.com: type A, class IN, addr 59.111.160.204

继续查看PC抓包发现SYN报文直接被告知TTL超时了

150 5.986329 100.71.52.253 192.1.59.252 ICMP 94 Time-to-live exceeded (Time to live exceeded in transit)
Frame 150: 94 bytes on wire (752 bits), 94 bytes captured (752 bits)
Ethernet II, Src: 70:f9:6d:e9:e8:8e (70:f9:6d:e9:e8:8e), Dst: Flextron_5d:4b:64 (00:21:cc:5d:4b:64)
Internet Protocol Version 4, Src: 100.71.52.253 (100.71.52.253), Dst: 192.1.59.252 (192.1.59.252)
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
Total Length: 80
Identification: 0x05f4 (1524)
Flags: 0x00
Fragment offset: 0
Time to live: 254
Protocol: ICMP (1)
Header checksum: 0x2177 [correct]
Source: 100.71.52.253 (100.71.52.253)
Destination: 192.1.59.252 (192.1.59.252)
Internet Control Message Protocol
Type: 11 (Time-to-live exceeded)
Code: 0 (Time to live exceeded in transit)
Checksum: 0xcd5f [correct]
Internet Protocol Version 4, Src: 192.1.59.252 (192.1.59.252), Dst: 59.111.160.204 (59.111.160.204)
Transmission Control Protocol, Src Port: 65251 (65251), Dst Port: https (443), Seq: 2455750051

并且差错报文透露了以下信息:

150 5.986329 100.71.52.253 192.1.59.252 ICMP 94 Time-to-live exceeded (Time to live exceeded in transit)
Frame 150: 94 bytes on wire (752 bits), 94 bytes captured (752 bits)
Ethernet II, Src: 70:f9:6d:e9:e8:8e (70:f9:6d:e9:e8:8e), Dst: Flextron_5d:4b:64 (00:21:cc:5d:4b:64)
Internet Protocol Version 4, Src: 100.71.52.253 (100.71.52.253), Dst: 192.1.59.252 (192.1.59.252)
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
Total Length: 80
Identification: 0x05f4 (1524)
Flags: 0x00
Fragment offset: 0
Time to live: 254
Protocol: ICMP (1)
Header checksum: 0x2177 [correct]
Source: 100.71.52.253 (100.71.52.253)
Destination: 192.1.59.252 (192.1.59.252)
Internet Control Message Protocol
Type: 11 (Time-to-live exceeded)
Code: 0 (Time to live exceeded in transit)
Checksum: 0xcd5f [correct]
Internet Protocol Version 4, Src: 192.1.59.252 (192.1.59.252), Dst: 59.111.160.204 (59.111.160.204)
Transmission Control Protocol, Src Port: 65251 (65251), Dst Port: https (443), Seq: 2455750051

TTL为254，说明就相隔2跳，离PC很近，目前怀疑访问59.111.160.204的流量，产生了三层环路，建议现场利用tracert确认环路设备。

## 解决方法

最后客户排查路由，确实是核心设备到59.111.160.204地址有路由环路，修改路由之后163邮箱访问正常，非LB设备问题。