【MVS】关于F5 Virtual-Server回应TCP RST ACK报文的问题分析

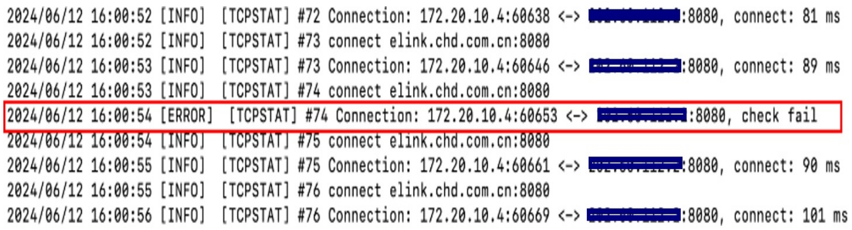
网络相关 胡伟 2024-06-13 发表

组网及说明

客户端（内网地址）————NAT设备（公网地址）———— （公网地址）F5负载均衡———— （内网地址）服务器

问题描述

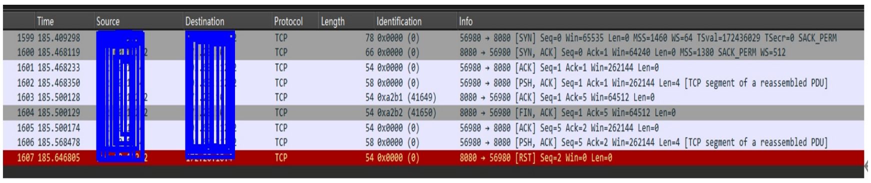
客户端通过针对F5设备对应业务虚服务的8080端口进行探测，发现概率性存在端口check fail故障现象存在。



```
2024/06/12 16:00:52 [INFO]  [TCPSTAT] #72 Connection: 172.20.10.4:60638 <-> [redacted]:8080, connect: 81 ms
2024/06/12 16:00:52 [INFO]  [TCPSTAT] #73 connect elink.chd.com.cn:8080
2024/06/12 16:00:53 [INFO]  [TCPSTAT] #73 Connection: 172.20.10.4:60646 <-> [redacted]:8080, connect: 89 ms
2024/06/12 16:00:53 [INFO]  [TCPSTAT] #74 connect elink.chd.com.cn:8080
2024/06/12 16:00:54 [ERROR]  [TCPSTAT] #74 Connection: 172.20.10.4:60653 <-> [redacted]:8080, check fail
2024/06/12 16:00:54 [INFO]  [TCPSTAT] #75 connect elink.chd.com.cn:8080
2024/06/12 16:00:55 [INFO]  [TCPSTAT] #75 Connection: 172.20.10.4:60661 <-> [redacted]:8080, connect: 90 ms
2024/06/12 16:00:55 [INFO]  [TCPSTAT] #76 connect elink.chd.com.cn:8080
2024/06/12 16:00:56 [INFO]  [TCPSTAT] #76 Connection: 172.20.10.4:60669 <-> [redacted]:8080, connect: 101 ms
```

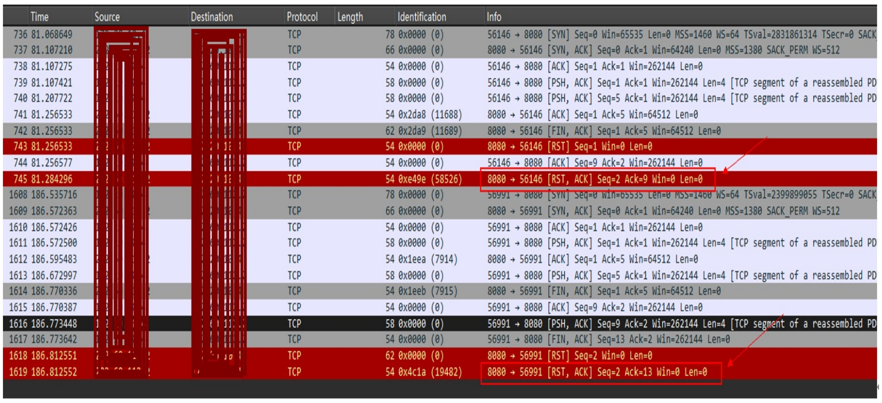
过程分析

经过抓包对比分析发现，正常业务探测的报文在收到TCP RST报文后是不会再收到TCP RST ACK报文。



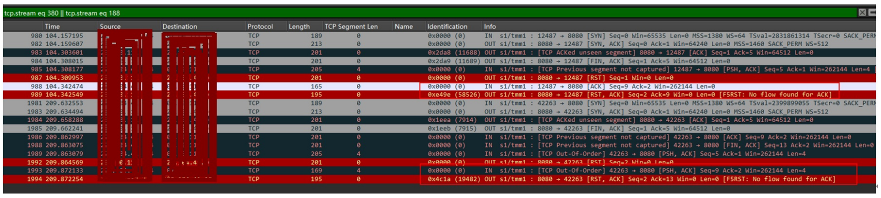
```
     Time        Source      Destination  Protocol  Length  Identification  Info
1599 185.409298  [redacted]  [redacted]   TCP              78 0x0000 (0)      56980 → 8080 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=172436029 TSecr=0 SACK_PERM
1600 185.468119  [redacted]  [redacted]   TCP              66 0x0000 (0)      8080 → 56980 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1380 SACK_PERM WS=512
1601 185.468233  [redacted]  [redacted]   TCP              54 0x0000 (0)      56980 → 8080 [ACK] Seq=1 Ack=1 Win=262144 Len=0
1602 185.468350  [redacted]  [redacted]   TCP              58 0x0000 (0)      56980 → 8080 [PSH, ACK] Seq=1 Ack=1 Win=262144 Len=4 [TCP segment of a reassembled PDU]
1603 185.500128  [redacted]  [redacted]   TCP              54 0xa2b1 (41649)  8080 → 56980 [ACK] Seq=1 Ack=5 Win=64512 Len=0
1604 185.500129  [redacted]  [redacted]   TCP              54 0xa2b2 (41650)  8080 → 56980 [FIN, ACK] Seq=1 Ack=5 Win=64512 Len=0
1605 185.500174  [redacted]  [redacted]   TCP              54 0x0000 (0)      56980 → 8080 [ACK] Seq=5 Ack=2 Win=262144 Len=0
1606 185.568478  [redacted]  [redacted]   TCP              58 0x0000 (0)      56980 → 8080 [PSH, ACK] Seq=5 Ack=2 Win=262144 Len=4 [TCP segment of a reassembled PDU]
1607 185.646805  [redacted]  [redacted]   TCP              54 0x0000 (0)      8080 → 56980 [RST] Seq=2 Win=0 Len=0
```

客户端连接显示check fail的主要原因是在收到TCP RST报文后又收到了相同端口的TCP RST ACK报文。



```
     Time        Source      Destination  Protocol  Length  Identification  Info
 736 81.068649   [redacted]  [redacted]   TCP              78 0x0000 (0)      56146 → 8080 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=2831861314 TSecr=0 SACK
 737 81.107210   [redacted]  [redacted]   TCP              66 0x0000 (0)      8080 → 56146 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1380 SACK_PERM WS=512
 738 81.107275   [redacted]  [redacted]   TCP              54 0x0000 (0)      56146 → 8080 [ACK] Seq=1 Ack=1 Win=262144 Len=0
 739 81.107421   [redacted]  [redacted]   TCP              58 0x0000 (0)      56146 → 8080 [PSH, ACK] Seq=1 Ack=1 Win=262144 Len=4 [TCP segment of a reassembled PD
 740 81.207722   [redacted]  [redacted]   TCP              58 0x0000 (0)      56146 → 8080 [PSH, ACK] Seq=5 Ack=1 Win=262144 Len=4 [TCP segment of a reassembled PD
 741 81.256533   [redacted]  [redacted]   TCP              54 0x2da8 (11688)  8080 → 56146 [ACK] Seq=1 Ack=5 Win=64512 Len=0
 742 81.256533   [redacted]  [redacted]   TCP              62 0x2da9 (11689)  8080 → 56146 [FIN, ACK] Seq=1 Ack=5 Win=64512 Len=0
 743 81.256533   [redacted]  [redacted]   TCP              54 0x0000 (0)      8080 → 56146 [RST] Seq=1 Win=0 Len=0
 744 81.256577   [redacted]  [redacted]   TCP              54 0x0000 (0)      56146 → 8080 [ACK] Seq=9 Ack=2 Win=262144 Len=0
 745 81.284296   [redacted]  [redacted]   TCP              54 0xe49e (58526)  8080 → 56146 [RST, ACK] Seq=2 Ack=9 Win=0 Len=0
1608 186.535716  [redacted]  [redacted]   TCP              78 0x0000 (0)      56991 → 8080 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=2399899055 TSecr=0 SACK
1609 186.572363  [redacted]  [redacted]   TCP              66 0x0000 (0)      8080 → 56991 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1380 SACK_PERM WS=512
1610 186.572426  [redacted]  [redacted]   TCP              54 0x0000 (0)      56991 → 8080 [ACK] Seq=1 Ack=1 Win=262144 Len=0
1611 186.572500  [redacted]  [redacted]   TCP              58 0x0000 (0)      56991 → 8080 [PSH, ACK] Seq=1 Ack=1 Win=262144 Len=4 [TCP segment of a reassembled PD
1612 186.595483  [redacted]  [redacted]   TCP              54 0x1eea (7914)   8080 → 56991 [ACK] Seq=1 Ack=5 Win=64512 Len=0
1613 186.672997  [redacted]  [redacted]   TCP              58 0x0000 (0)      56991 → 8080 [PSH, ACK] Seq=5 Ack=1 Win=262144 Len=4 [TCP segment of a reassembled PD
1614 186.770336  [redacted]  [redacted]   TCP              54 0x1eeb (7915)   8080 → 56991 [FIN, ACK] Seq=1 Ack=5 Win=64512 Len=0
1615 186.770387  [redacted]  [redacted]   TCP              54 0x0000 (0)      56991 → 8080 [ACK] Seq=9 Ack=2 Win=262144 Len=0
1616 186.773448  [redacted]  [redacted]   TCP              58 0x0000 (0)      56991 → 8080 [PSH, ACK] Seq=9 Ack=2 Win=262144 Len=4 [TCP segment of a reassembled PD
1617 186.773642  [redacted]  [redacted]   TCP              54 0x0000 (0)      56991 → 8080 [FIN, ACK] Seq=13 Ack=2 Win=262144 Len=0
1618 186.812551  [redacted]  [redacted]   TCP              62 0x0000 (0)      8080 → 56991 [RST] Seq=2 Win=0 Len=0
1619 186.812552  [redacted]  [redacted]   TCP              54 0x4c1a (19482)  8080 → 56991 [RST, ACK] Seq=2 Ack=13 Win=0 Len=0
```

由于客户端发出的报文在公网出口做了SNAT，源地址和源端口发生变化，但是IP报文的标识没有变化，根据两个TCP RST ACK报文的标识分别为ip.id == 58526和ip.id == 19482，在F5侧进行抓包可以此标识进行过滤和跟踪对应的异常流。



```
tcp.stream eq 380 || tcp.stream eq 188
     Time        Source      Destination  Protocol  Length  TCP Segment Len  Name  Identification  Info
 980 104.157195  [redacted]  [redacted]   TCP          189  0                      0x0000 (0)      IN  s1/tmm1 : 12487 → 8080 [SYN] Seq=0 Win=65535 Len=0 MSS=1380 WS=64 TSval=2831861314 TSecr=0 SACK_PERM
 982 104.159607  [redacted]  [redacted]   TCP          213  0                      0x0000 (0)      OUT s1/tmm1 : 8080 → 12487 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=512
 983 104.303601  [redacted]  [redacted]   TCP          201  0                      0x2da8 (11688)  OUT s1/tmm1 : [TCP ACKed unseen segment] 8080 → 12487 [ACK] Seq=1 Ack=5 Win=64512 Len=0
 984 104.308015  [redacted]  [redacted]   TCP          201  0                      0x2da9 (11689)  OUT s1/tmm1 : 8080 → 12487 [FIN, ACK] Seq=1 Ack=5 Win=64512 Len=0
 985 104.308177  [redacted]  [redacted]   TCP          205  4                      0x0000 (0)      IN  s1/tmm1 : [TCP Previous segment not captured] 12487 → 8080 [PSH, ACK] Seq=5 Ack=1 Win=262144 Len=4 [
 987 104.309953  [redacted]  [redacted]   TCP          201  0                      0x0000 (0)      OUT s1/tmm1 : 8080 → 12487 [RST] Seq=1 Win=0 Len=0
 988 104.342474  [redacted]  [redacted]   TCP          165  0                      0x0000 (0)      IN  s1/tmm1 : 12487 → 8080 [ACK] Seq=9 Ack=2 Win=262144 Len=0
 989 104.342549  [redacted]  [redacted]   TCP          195  0                      0xe49e (58526)  OUT s1/tmm1 : 8080 → 12487 [RST, ACK] Seq=2 Ack=9 Win=0 Len=0 [F5RST: No flow found for ACK]
1981 209.632553  [redacted]  [redacted]   TCP          189  0                      0x0000 (0)      IN  s1/tmm1 : 42263 → 8080 [SYN] Seq=0 Win=65535 Len=0 MSS=1380 WS=64 TSval=2399899055 TSecr=0 SACK_PERM
1983 209.634494  [redacted]  [redacted]   TCP          213  0                      0x0000 (0)      OUT s1/tmm1 : 8080 → 42263 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=512
1984 209.658288  [redacted]  [redacted]   TCP          201  0                      0x1eea (7914)   OUT s1/tmm1 : [TCP ACKed unseen segment] 8080 → 42263 [ACK] Seq=1 Ack=5 Win=64512 Len=0
1985 209.662241  [redacted]  [redacted]   TCP          201  0                      0x1eeb (7915)   OUT s1/tmm1 : 8080 → 42263 [FIN, ACK] Seq=1 Ack=5 Win=64512 Len=0
1986 209.862997  [redacted]  [redacted]   TCP          201  0                      0x0000 (0)      IN  s1/tmm1 : [TCP Previous segment not captured] 42263 → 8080 [ACK] Seq=9 Ack=2 Win=262144 Len=0
1988 209.863075  [redacted]  [redacted]   TCP          201  0                      0x0000 (0)      IN  s1/tmm1 : [TCP Previous segment not captured] 42263 → 8080 [FIN, ACK] Seq=13 Ack=2 Win=262144 Len=0
1989 209.863079  [redacted]  [redacted]   TCP          205  4                      0x0000 (0)      IN  s1/tmm1 : [TCP Out-Of-Order] 42263 → 8080 [PSH, ACK] Seq=5 Ack=1 Win=262144 Len=4
1992 209.864569  [redacted]  [redacted]   TCP          201  0                      0x0000 (0)      OUT s1/tmm1 : 8080 → 42263 [RST] Seq=2 Win=0 Len=0
1993 209.872133  [redacted]  [redacted]   TCP          169  4                      0x0000 (0)      IN  s1/tmm1 : [TCP Out-Of-Order] 42263 → 8080 [PSH, ACK] Seq=9 Ack=2 Win=262144 Len=4
1994 209.872254  [redacted]  [redacted]   TCP          195  0                      0x4c1a (19482)  OUT s1/tmm1 : 8080 → 42263 [RST, ACK] Seq=2 Ack=13 Win=0 Len=0 [F5RST: No flow found for ACK]
```

通过对F5侧抓包进行分析发现，F5侧收到的报文相对客户端发出的报文有存在缺失（Tcp Previous Segment Not captured）和乱序（Tcp Out-Of-Order）现象，说明中间通信链路不稳定。同时F5发出的TCP RST ACK报文提示为[f5rst: no flow found for ack],这是因为在先前的连接中业务侧已经发出RST报文重置连接，对应的F5设备上的connection表项已经释放，此时如果因为客户发包异常（第一条流客户收到TCP RST之后又发送TCP ACK报文）或者报文乱序导致F5侧再收到相同端口同时携带ACK标识的TCP报文，由于F5是全代理架构需要检查TCP连接状态，由于先前对应端口

的connection表项已释放，此次F5侧会直接回应报文TCP RST ACK给到客户端。

解决方法

从上面的分析可以知道，F5侧发送TCP RST ACK报文机制并无异常，主要原因是中间网络波动导致的报文丢失和乱序问题以及客户端发包机制异常问题。

由于这种异常情况主要发生在业务端口短连接测试的TCP连接断开场景中，在实际业务运行的长连接场景下故障现象可能不会有感知，建议现场进一步测试观察。