某局点SecPath F5080-D(V7) 设备web页面无法登录故障排查经验案例

WEB管理 王周华 2022-02-26 发表

组网及说明

本次涉及设备的型号以及版本：SecPath F5080-D Version 7.1.064, Release 9620P2414

问题描述

现场两台F5080-D通过RBM的方式组网，保证设备的可靠性。反馈主设备的web页面出现无法登录现象，备设备web页面登录正常。telnet主设备地址的443端口可达，WEB页面登录报错截图如下。

过程分析

1、由于telnet设备的443端口可达，说明到设备的连通性没有问题，于是先检查设备管理口以及登录配置是否正确。

管理口配置：

```
interface GigabitEthernet1/2/4/0
port link-mode route
description management1
ip binding vpn-instance management1
ip address 10.167.193.98 255.255.255.0
```

使能HTTPS登录方式：

```
ip https enable
```

由于现场配置了HTTPS服务与SSL服务器端策略关联。那么需要检查SSL服务器端策略配置是否调用pki-domain,如果没有调用，会导致设备HTTPS登录异常。

```
ip https ssl-server-policy test
ssl server-policy test
 pki-domain test
pki domain test
 public-key rsa general name test
 undo crl check enable
```

以上管理口地址配置和HTTPS登录配置均未发现异常。

2、于是让现场收集HTTPS访问时的会话信息以及DEBUG信息分析，debug开关如下：

```
debugging ip packet
debugging ip info
debugging session session-table all
T    d
T     m
*Feb 16 14:35:43:162 2022 CAFD-DC-C2-18/19U-F5080D-DCFW-01 IPFW/7/IPFW_PACKET: -Chassis=1-Slot=2;
Receiving, interface = GigabitEthernet1/2/4/0
version = 4, headlen = 20, tos = 2
pktlen = 52, pktid = 55823, offset = 0, ttl = 125, protocol = 6
checksum = 21493, s = 10.167.249.12, d = 10.167.193.98
channelID = 0, vpn-InstanceIn = 2, vpn-InstanceOut = 2.
prompt: Receiving IP packet from interface GigabitEthernet1/2/4/0.
Payload: TCP
  source port = 65453, destination port = 443
  sequence num = 0xa4b54fb9, acknowledgement num = 0x00000000, flags = 0xc2
  window size = 64240, checksum = 0xadca, header length = 32.

*Feb 16 14:35:43:163 2022 CAFD-DC-C2-18/19U-F5080D-DCFW-01 SESSION/7/TABLE: -Chassis=1-Slot=2;
 Tuple5(EVENT): 10.167.249.12/65453-->10.167.193.98/443(TCP(6))
 Session entry was created.
*Feb 16 14:35:43:163 2022 CAFD-DC-C2-18/19U-F5080D-DCFW-01 IPFW/7/IPFW_PACKET: -Chassis=1-Slot=2;
Delivering, interface = GigabitEthernet1/2/4/0
version = 4, headlen = 20, tos = 2
pktlen = 52, pktid = 55823, offset = 0, ttl = 125, protocol = 6
checksum = 21493, s = 10.167.249.12, d = 10.167.193.98
channelID = 0, vpn-InstanceIn = 2, vpn-InstanceOut = 2.
prompt: Forwarding IP packet to upper layer.
Payload: TCP
  source port = 65453, destination port = 443
  sequence num = 0xa4b54fb9, acknowledgement num = 0x00000000, flags = 0xc2
  window size = 64240, checksum = 0xadca, header length = 32.
```

从DEBUG看设备已经收到了HTTPS的请求报文，并且建立了会话。

会话信息如下：

```
RBM_Pdis session table ipv4 source-ip 10.167.249.12 destination-ip 10.167.193.98 verbose
Slot 0 in chassis 1:
Total sessions found: 0
Slot 1 in chassis 1:
```

Total sessions found: 0

Slot 2 in chassis 1:

Initiator:

Source IP/port: 10.167.249.12/49459

Destination IP/port: 10.167.193.98/443

DS-Lite tunnel peer: -

VPN instance/VLAN ID/Inline ID: management1/-/-

Protocol: TCP(6)

Inbound interface: GigabitEthernet1/2/4/0

Source security zone: DC_Management

Responder:

Source IP/port: 10.167.193.98/443

Destination IP/port: 10.167.249.12/49459

DS-Lite tunnel peer: -

VPN instance/VLAN ID/Inline ID: management1/-/-

Protocol: TCP(6)

Inbound interface: InLoopBack0

Source security zone: Local

State: TCP_TIME_WAIT

Application: HTTPS

有对应流量的会话，但是TCP状态是TCP_TIME_WAIT，当TCP主动关闭方在发送四次挥手的最后一个ACK后会变为TIME_WAIT状态。那么可能是设备侧主动断开了TCP连接，现场将终端直接接入到管理口上依旧无法打开WEB页面，进一步排除了中间网络的问题。

3、经过确认，现场设备版本存在如下已知问题：

问题发生条件（步骤）：开启password-control功能之后，多用户登录

问题原因：版本R9620P2414，开启password-control功能之后，如果两个以上的用户同时登陆WEB界面，xmlcfg进程就会挂死，导致WEB界面无法登录。

解决方法

检查现场配置的确配置了password-control enable，该问题暂时恢复方案：重启设备。

解决方案：F5080-D设备升级至R9660P19版本解决。