SecPath F100-C-G3(V7) 配置SSL VPN后 handshake_failure 导致无法正常拨入经验案例

SSL VPN 蒋笑添 2020-08-21 发表

组网及说明

null

问题描述

现场配置SSL VPN后，终端inode拨入时显示网络不可达，无法成功拨入VPN。debug sslvpn all 信息如下：

<F100-C-G3>*Aug 20 21:24:21:139 2020 F100-C-G3 SSLVPNK/7/SSLVPN_DEBUG_KSSL_INFO: SSL_accept: before SSL initialization.

*Aug 20 21:24:21:139 2020 F100-C-G3 SSLVPNK/7/SSLVPN_DEBUG_KSSL_HANDSHAKE: Receive: TLS 1.0Handshake [length 00c2].

*Aug 20 21:24:21:139 2020 F100-C-G3 SSLVPNK/7/SSLVPN_KSSL_PACKET:

16 03 01 00 c2

*Aug 20 21:24:21:139 2020 F100-C-G3 SSLVPNK/7/SSLVPN_DEBUG_KSSL_INFO: SSL_accept: before SSL initialization.

*Aug 20 21:24:21:139 2020 F100-C-G3 SSLVPNK/7/SSLVPN_DEBUG_KSSL_HANDSHAKE: Receive: TLS 1.0 [length 00c2], message type: ClientHello.

*Aug 20 21:24:21:139 2020 F100-C-G3 SSLVPNK/7/SSLVPN_KSSL_PACKET:

...

13 c0 09 00 33 00 32 00 31 00

30 00 9a 00 99 00 98 00 97 00

45 00 44 00 43 00 42 c0 0e c0

04 00 2f 00 96 00 41 00 07 c0

11 c0 07 c0 0c c0 02 00 05 00

...

*Aug 20 21:24:21:139 2020 F100-C-G3 SSLVPNK/7/SSLVPN_DEBUG_KSSL_HANDSHAKE: Send: TLS 1.0Alert [length 0002].

*Aug 20 21:24:21:139 2020 F100-C-G3 SSLVPNK/7/SSLVPN_KSSL_PACKET:

15 03 01 00 02

*Aug 20 21:24:21:140 2020 F100-C-G3 **SSLVPNK/7/SSLVPN_DEBUG_KSSL_HANDSHAKE: Send: TLS 1.0Alert [length 0002], level: fatal, reason: handshake_failure.**

*Aug 20 21:24:21:140 2020 F100-C-G3 SSLVPNK/7/SSLVPN_KSSL_PACKET:

02 28

*Aug 20 21:24:21:140 2020 F100-C-G3 SSLVPNK/7/SSLVPN_DEBUG_KSSL_INFO: SSL3 alert write, level: fatal, reason: handshake failure.

*Aug 20 21:24:21:140 2020 F100-C-G3 SSLVPNK/7/SSLVPN_DEBUG_KSSL_INFO: SSL_accept: error in error.

过程分析

从debug信息来看，初步判断为SSL协议版本不匹配导致握手失败。于是检测设备版本以及是否关闭部分SSL版本。

设备版本为 Release 9536P14，已支持所有SSL协议版本。且配置中没有关闭SSL版本。默认全部开启。

反馈开启 sslvpn gateway gw 与 sslvpn context 后又修改过相关配置。

解决方法

服务启动后修改过配置。可能会导致服务进程出错。重启服务就可以恢复正常。

把这两个服务undo service enable一下，再配置一下即可。