



某局点MSR3610IEEAD ssl vpn拨入失败

SSL VPN

SSL

曾招维

2021-12-31 发表

组网及说明

MSR3610IEEAD当公网口设备，客户通过访问59.34.130.xxx:55555进行拨号。

问题描述

现场播入SSL VPN异常，检查配置无误，使用设备的缺省证书方式，安装多个软件版本后故障依旧，debug中报错bad record mac.，和使用web打开gateway的地址+端口报错内容相同。

inode客户端拨号报错与网关连接失败：



使用gateway的网关地址和端口访问web时有如下报错内容：

建立安全连接失败

连接到 59.34.130.222:55555 时发生错误。SSL 对等端报告了不正确的消息认证码。

错误代码：SSL_ERROR_BAD_MAC_ALERT

- 由于不能验证所收到的数据是否可信，无法显示您想要查看的页面。
- 建议向此网站的管理员反馈这个问题。

[详细了解...](#)

重试

公网访问SSL服务端可以建立TCP连接：

```
[C:\~]$  
[C:\~]$  
[C:\~]$ telnet 59.34.130.222 55555  
  
Connecting to 59.34.130.222:55555...  
Connection established.  
To escape to local shell, press 'Ctrl+Alt+J'.  
[C:\~]$
```

过程分析

- 1、配置未见异常（相同配置在其他设备上没有问题）；
- 2、公网口端口可达，尝试将0/3出口的tcp mss 修改为1200测试故障依旧。
- 3、网关使用缺省证书，但是浏览器打开https:// 59.34.130.222:55555无法正常打开web；

#

sslvpn gateway ga

ip address 59.34.130.xxx port 55555

service enable

#

- 4、debug ssl发现ssl过程有异常：

*Dec 28 20:45:24:884 2021 H3C SSLVPNK/7/SSLVPN_DEBUG_KSSL_HANDSHAKE: Send: TLS 1.0Alert [length 0002], level: fatal, **reason: bad_record_mac**.

*Dec 28 20:45:24:884 2021 H3C SSLVPNK/7/SSLVPN_KSSL_PACKET: 02 14

*Dec 28 20:45:24:884 2021 H3C SSLVPNK/7/SSLVPN_DEBUG_KSSL_INFO: SSL3 alert write, level : fatal, **reason: bad record mac**.

解决方法

这款型号设备硬件加密引擎不支持当前的算法，关闭硬件加密引擎，改为软件加密，就正常了。

probe视图下，关闭加密引擎crypto-engine accelerator disable

PS.

路由器有三种加密方式：加密卡加密、加密引擎加密、软件加密。其中加密卡是单独的加密板卡，如ANDE、SNDE、HNDE等；加密引擎是CPU自带的加密引擎，也是硬件加密的一种。如果有加密卡，且配置中使用了加密卡，则会使用加密卡进行加密；如果没有加密卡，且打开加密引擎（缺省即打开），则使用CPU自带的加密引擎进行加密；如果没有加密卡，且关闭加密引擎（配置undo cryptoengine enable 命令），则使用软件加密。

