

问题描述

现场使用V7平台防火墙插卡配置SSL VPN，使用INODE连接中出现无法访问SSL网关问题。

分析过程：

一般SSL VPN在资源未配置只导入证书情况下，使用浏览器打开公网地址:XXXX时WEB界面是可以打开的。但是现场通过60.X.49.194:2000打开WEB界面却提示：没有双方共用的加密算法，错误代码：SSL_ERROR_NO_CYPHER_OVERLAP。

建立安全连接失败

连接到 60.X.49.194:2000 时发生错误。无法安全地与对等端通信：没有双方共用的加密算法。错误代码：SSL_ERROR_NO_CYPHER_OVERLAP

- 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...

报告此类错误，帮助 Mozilla 识别与拦截恶意网站

重试

解决方法

已经判断为是证书部分问题，所以排查证书部分配置，但是排查中发现证书导入正常。排查配置发现在SSL策略中客户只调用了一种加密算法，导致客户端与设备的加密算法无法匹配。

#

pki domain sslvpn

public-key rsa general name sslvpn

undo crl check enable

#

ssl server-policy ssl

pki-domain sslvpn

ciphersuite dhc_rsa_aes_128_cbc_sha

解决方法：



在设备WEB界面中选择资源>SSL后将所有加密套件勾选后问题解决。