



inode进行SSLVPN认证报网关错误

iNode

汤祺

2021-06-28 发表

组网及说明

inode联动防火墙设备进行SSLVPN认证。

问题描述

inode联动防火墙设备进行SSLVPN认证，认证时inode侧出现网管错误的报错。从终端测试防火墙网关及端口信息，网络皆正常，ip可ping通，端口也可正常通信，但认证时出现异常。

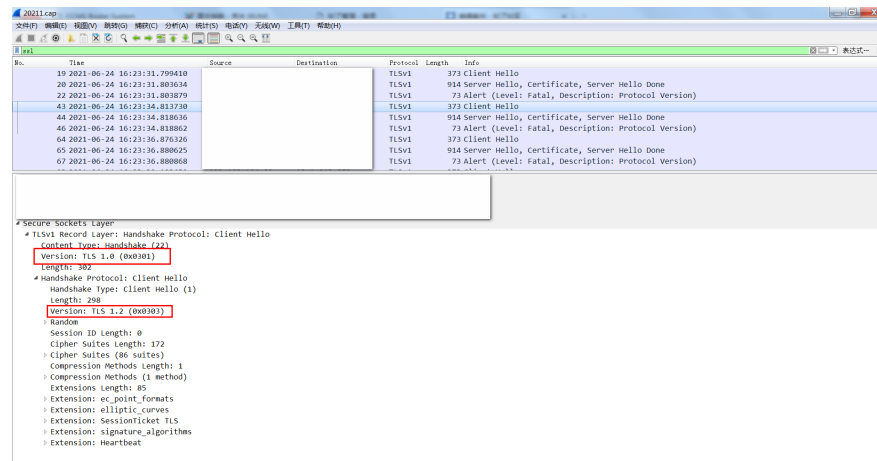
过程分析

查看inode详细级别日志，日志里报错，即认证过程中连接远程网关服务器失败：

```
[2021-06-25 10:44:52] [ERROR] [0x7fe8d37fe700] CHttpsAuth::sendAndRecvHttp failed to connect to the remote server, addr: xx.xx.xx.xx , errno: 336462231
```

```
[2021-06-25 10:44:52] [ERROR] [0x7fe8d37fe700] CHttpsAuth::getAuthParams failed to send data to remote, ip: xx.xx.xx.xx , port: 443, errno: 336462231
```

查看当时认证异常时，终端侧的抓包，发现tls连接有报错，提示协议版本。再查看握手报文，发现客户端要求使用tls1.2版本，而网关回应要求使用tls1.0，所以双方协商失败，报错返回，连接建立失败。



解决方法

综上，具体解决措施有两个：

1. 修改iNode版本，使用tls1.0的版本，在inode定制时，可选择inode使用的协议版本
2. 或者修改网关tls协议，使其支持tls1.2。

