SSLVPN拨号登录提示“与VPN网关建立连接失败”问题处理过程

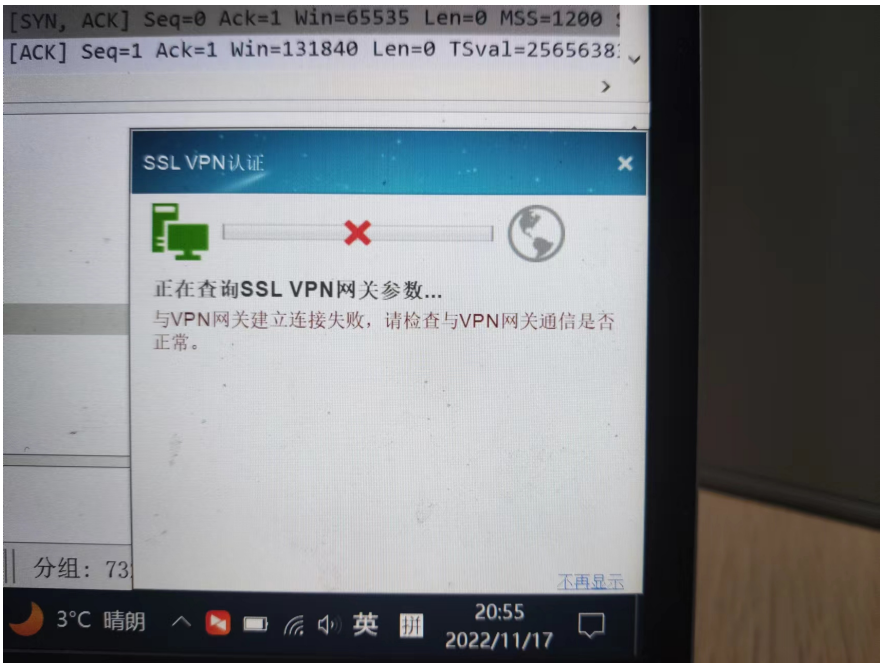
SSL VPN 孔凡安 2022-11-18 发表

组网及说明

不涉及

问题描述

sslvpn拨号失败提示“与VPN网关建立连接失败”



过程分析

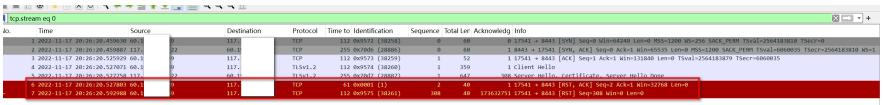
1. 检查设备配置无问题，网关处于UP状态。而且客户反馈是使用过程中出现问题的。所以配置存在问题的可能性不大

2. 检查网络层是否正常，客户端侧telnet或tcping网关+端口，发现可以正常建立连接，说明网络层通信无问题。

3. debug sslvpn aaa,event.error调试，发现无回显。猜测没有走到sslvpn的业务点。结合拨号的报错以及telnet能通这两点，怀疑三次握手后TLS交互存在问题。

4. 继续检查sslvpn的配置，查看设备是否自定义了证书，是否调用了SSL服务器端策略、证书是否正常等配置，发现没有问题。

5. 在防火墙上抓取拨号的报文，发现三次握手后，客户端回应了RST报文。注：60.X.X.X为客户端，117.X.X.X为SSLVPN网关地址。

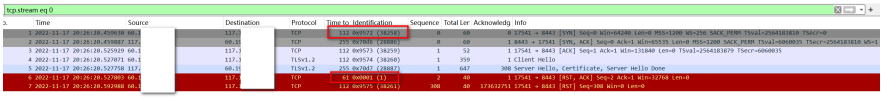


问题分析到这个地方，似乎已经“破案”了，客户的客户端异常，莫名其妙要中断连接，问题和防火墙无关。需要排查iNode或者PC的问题。

但是客户坚持说没做过变动，客户端不可能存在问题。

于是，我尝试用自己电脑拨号，同样也拨不上。抓包看报文和上图如出一辙，问题陷入了僵局。“终端为什么要发送RST报文呢？”

没办法，只能继续分析报文，我盯着No.6号报文看花了眼。此时，一个地方引起了我的注意，报文的TTL值以及报文的IP.ID值。



根据三次握手的SYN报文（No.1报文）来看，客户端发送到防火墙的TTL应该为112。但是观察No.6报文，TTL居然是61。第二个疑点就是报文的IP.ID数值，一般来说TCP交互过程中，报文的IP.ID值是逐一增大的，如图所示，38258---38259---38260，然后突然到1，这里面明显是存在问题的。

基于以上两点分析，怀疑是防火墙前端有网络安全设备伪装成客户端给防火墙发送RST报文，导致拨号异常。

解决方法

排查网络环境，找到代答设备。