具有Zscaler SSL/TLS解密干扰的对等体重置思科安全客户端VPN连接

目录

问题

用户尝试使用Cisco安全客户端建立连接时遇到VPN连接故障。

环境

- 技术：思科安全访问 — 安全客户端远程访问（VPN、状态、专用资源）
- 产品系列：SECACCS
- 操作系统：macOS（基于显示/Users/admin/workspace/secure-client-macos_Raccoon_MR15/）的日志文件路径
- 第三方软件：客户端系统上安装的Zscaler
- VPN协议：CSTP（Cisco SSL隧道协议）
- TLS版本：TLS 1.3和密码TLS_AES_256_GCM_SHA384

分辨率

解决方案涉及识别和解决Cisco安全客户端与Zscaler的SSL/TLS解密功能之间的冲突。

步骤 1：日志分析和诊断

捕获和分析Cisco安全客户端DART日志以确定连接故障模式。日志将显示成功的TLS会话建立，然后立即重置连接。

日志中的主要诊断指标：

- 使用密码TLS_AES_256_GCM_SHA384建立TLS 1.3连接
- MTU计算和HTTP协商正常进行
- 对等体错误导致连接重置(返回代码：54)在套接字读取操作期间

TLS 1.3会话使用密码TLS_AES_256_GCM_SHA384成功建立，但会话建立后会立即发送重置数据包，该数据包将终止连接，导致VPN隧道断开。在日志中观察到的特定错误在套接字读取操作期间显示返回代码为54(0x00000036)的“对等体重置连接”。

在连接尝试期间出现以下错误序列：

```
2026-03-11 10 vpnagentd: (libvpncommon.dylib) [com.cisco.secureclient.vpn:csc_vpnagent] A TLS 1.3 conne
2026-03-11 vpnagentd: (libvpncommon.dylib) [com.cisco.secureclient.vpn:csc_vpnagent] Function: calculat
2026-03-11 17:01:48. vpnagentd: (libvpncommon.dylib) [com.cisco.secureclient.vpn:csc_vpnagent] Function
2026-03-11 17:01:48.356 vpnagentd: (libvpncommon.dylib) [com.cisco.secureclient.vpn:csc_vpnagent] Funct
```

步骤 2：第三方软件识别

检查是否存在可在客户端系统上执行SSL/TLS检测或解密的第三方安全软件。在这种情况下，Zscaler被确定为干扰应用。

步骤 3：SSL/TLS解密冲突解决方案

解决思科安全客户端VPN流量与Zscaler的SSL/TLS解密功能之间的冲突。VPN流量似乎正在由Zscaler进行SSL/TLS解密，这会干扰VPN隧道的建立并导致连接重置。

可能的解决方法包括：

- 将Zscaler配置为从SSL/TLS检查中排除Cisco安全客户端VPN流量
- 在Zscaler中为VPN服务器终端创建旁路规则
- 在VPN连接测试期间临时禁用Zscaler以确认冲突

- 与网络安全团队协调，确定适当的例外情况

原因

此问题的根本原因是思科安全客户端VPN流量与Zscaler的SSL/TLS解密功能之间的冲突。当Zscaler尝试解密或检查VPN的TLS流量时，它会干扰安全隧道建立过程。此干扰表现为在TLS会话建立后立即重置连接，阻止VPN隧道完成其协商阶段。重置数据包的定时（在成功建立TLS后但隧道完成前发生）是来自安全设备或软件的SSL/TLS检查干扰的特征。

相关内容

- 思科技术支持和下载

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。