

当安全客户端Umbrella SWG代理服务处于活动状态时，互联网访问失败

目录

问题

当Cisco Secure Client - Umbrella SWG Agent服务在Windows Dell笔记本电脑上运行时，用户无法访问任何网站。一旦Umbrella SWG代理服务停止，将恢复正常的Web访问。思科安全客户端5.1.14.145版出现问题，该版本包含AnyConnect VPN和Umbrella模块。OrgInfo.json文件存在于预期的目录中，并且思科安全访问根CA证书安装在受信任的根证书库中。

环境

- 产品:思科安全客户端 (AnyConnect VPN和Umbrella模块)
- 软件版本:5.1.14.145
- 操作系统 : Windows (戴尔笔记本电脑)
- Umbrella SWG代理服务已启用/已禁用
- %ProgramData%\Cisco\Cisco Secure Client\Umbrella\OrgInfo.json中存在OrgInfo.json
- 安装在受信任的根证书颁发机构库中的思科安全访问根CA
- 在安全访问控制面板中启用DNS/网络安全
- 已启用解密的已分配安全配置文件

分辨率

通过识别和更正客户端设备上的网络时间协议(NTP)同步失败解决了此问题。无法同步时间会阻止Umbrella SWG代理代理网络流量所需的安全通信，从而导致TCP重置(RST)数据包和Web访问丢失。一旦恢复NTP同步，Web访问将在SWG代理活动的情况下正常运行。

请遵循此全面的故障排除工作流程。

第1步：检验配置和必备条件

- 确保OrgInfo.json位于%ProgramData%\Cisco\Cisco Secure Client\Umbrella\OrgInfo.json。
- 确认Cisco Secure Access Root CA存在于受信任的根证书颁发机构库中。
- 检查安全访问控制面板中是否启用了DNS/Web安全。
- 验证分配的安全配置文件是否已启用解密。

第2步：捕获和分析网络流量

获取定向到SWG代理的客户端流量的数据包捕获，以识别异常行为，例如意外的TCP重置数据包。

显示问题的数据包捕获说明：

The packet capture revealed that TCP reset (RST) packets were being sent to the client, disrupting the

第4步：验证边界防火墙规则

- 检查边界防火墙规则，确保入口接口上允许进出交换机服务器的流量。

第5步：运行系统和协议诊断

在客户端上执行此命令以检查NTP同步错误：

```
curl ipinfo.io
```

诊断结果的说明：

The output indicated NTP timing was out of sync on the client device.

原因

根本原因是客户端设备上的NTP（网络时间协议）同步失败。此计时问题阻止了客户端和Umbrella SWG代理服务之间的安全通信，导致TCP重置数据包和在SWG代理服务处于活动状态时丢失Web访问。解决NTP同步问题恢复了Umbrella SWG代理的正常运行，允许安全地代理网络流量。

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）。