

MacOS休眠后安全客户端ZTNA DNS解析和连接丢失

目录

问题

在系统从睡眠或休眠模式恢复后，MacOS终端上的Cisco SecureClient ZTNA会遇到DNS解析故障和ZTA连接丢失。此问题会影响ZTNA IA（身份访问）和ZTNA PA（专用访问）功能。虽然基本IP连接仍可正常工作(对外部IP地址（如8.8.8.8和208.67.222.222）的ICMP ping操作成功运行），但DNS名称解析完全失败，阻止访问通过ZTNA配置的互联网资源和私有资源。

观察到的具体症状包括：

- 使用nslookup命令执行DNS查找失败（例如，通过8.8.8.8执行www.cisco.com的nslookup和208.67.222.222不起作用）。
- ZTNA IA和ZTNA PA连接变得不可用。
- 在终端休眠和唤醒周期后，问题始终发生。
- 当设备处于活动使用状态时，问题也可能随机发生。
- 终止ZTNA进程会导致立即重新启动，但连接问题通常仍然存在。
- 只有完整的系统重新启动才能恢复完整的DNS解析和ZTNA连接。

环境

- 操作系统：macOS（版本26.3已记录案例）
- Cisco SecureClient:5.1.14.x版（5.1.16之前的受影响版本）
- ZTNA模块：使用身份访问(IA)和专用访问(PA)配置进行活动
- 网络监控:可以包括Sentinel One等第三方安全解决方案

- 其他安全软件：可以包含思科安全终端
- DNS Servers :可通过ICMP访问外部DNS服务器(8.8.8.8、208.67.222.222)，但DNS解析失败
- UMB模块：未使用

分辨率

此问题已通过思科工程部门提供的软件修复解决。解决流程涉及以下各节中介绍的步骤。

步骤 1：问题识别和漏洞跟踪

Cisco Engineering将此确定为已知缺陷，并在Cisco Bug ID CSCwt24392（仅限注册用户）下记录该缺陷，其描述为“macOS:DNS停止使用ZTA SIA-all和NVM活动”。

步骤 2：诊断数据收集

收集此诊断信息以支持工程分析：

- 来自受影响终端的DART（诊断和报告工具）捆绑包。
- 数据包捕获文件(ZTNA Issue1.pcapng)。
- 显示连接故障的屏幕截图。
- 显示问题重现的屏幕录音。
- 显示com.cisco.secureclient.zta.app.service和系统扩展进程行为的进程交互日志。

步骤 3：工程修复程序开发

Cisco Engineering为CSCwt24392开发了一个针对性的修复程序，并将其包含在SecureClient版本5.1.16中。该修复程序专门解决在休眠/休眠周期后ZTA SIA-all和NVM在macOS系统上处于活动状态时发生的DNS解析故障。

步骤 4：软件更新安装

在受影响的macOS终端上安装Cisco SecureClient 5.1.16版或更高版本。此版本包含DNS解析和ZTA连接问题的修补程序。

步骤 5：验证测试

安装SecureClient 5.1.16后，执行以下验证步骤：

1. — 允许macOS终端进入睡眠或休眠模式。
2. — 将系统从睡眠或休眠状态唤醒。
3. — 使用nslookup命令测试DNS解析。
4. — 检验ZTNA IA和ZTNA PA与已配置资源的连接。
5. — 确认Internet访问和私有资源访问均正常工作，无需重新启动系统。

早期版本的解决方法

对于无法立即升级到SecureClient 5.1.16的环境，可以使用以下临时解决方法：

- 在每个休眠/休眠周期后执行完整的系统重新引导以恢复DNS解析和ZTNA连接。
- 如果睡眠/休眠问题显著影响工作效率，请考虑暂时从ZTNA注销（请注意，这样做会删除ZTNA保护）。

原因

此问题的根本原因在于5.1.16之前的Cisco SecureClient版本中存在软件缺陷，特别是被跟踪为

Cisco Bug ID CSCwt24392。当ZTA (零信任访问) SIA-all (安全互联网访问) 和NVM (网络可视性模块) 组件在macOS系统上处于活动状态时，会出现此缺陷。在睡眠或休眠和唤醒周期期间，这些组件无法正确恢复DNS解析功能，同时保持基本IP连接。这会导致ICMP流量(ping)正常运行，但DNS查询失败，从而有效地阻止对互联网资源和受ZTNA保护的私有资源的访问。在系统状态转换期间，问题涉及com.cisco.secureclient.zta.app.service进程与系统扩展进程之间的不当交互。

相关内容

- Cisco Bug ID CSCwt24392 - macOS:DNS停止使用ZTA SIA-all和NVM活动
- [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）。