iOS上用于远程访问VPN的Cisco安全客户端的DNS日志记录和设备注册行为

目录

问题

当使用iOS上的思科安全客户端(iPad)通过Microsoft Entra ID使用SAML身份验证与思科安全访问建立远程访问VPN时，DNS日志在VPN连接成功后不会显示在Secure Access中，即使正确生成了防火墙和Web日志。此外，建立VPN连接后，iPad不会显示在Secure Access控制面板中的Roaming Devices > Mobile Devices下。

观察到的具体症状包括：

- 远程访问日志在安全访问中显示成功的“连接”事件
- 生成防火墙和Web日志并显示经过SAML身份验证的用户身份
- 安全访问日志记录中完全没有DNS日志
- iPad设备信息未填充在安全访问漫游设备部分
- 所有流量流经VPN隧道（未配置分割隧道）

环境

- 运行iOS 26.2的iPad
- 思科安全客户端
- 身份提供程序：Microsoft Entra ID
- 安全连接器：未安装
- 配置了SSO身份验证的思科安全访问
- SAML身份验证实施

- 将DNS模式配置为默认模式的VPN配置文件
- 未配置分割隧道（所有流量通过VPN路由）
- 用于配置文件分发的移动设备管理(MDM)

分辨率

所观察到的行为适用于已记录的配置。iOS上的Cisco安全客户端充当VPN客户端（AnyConnect等效功能），默认情况下不包括RSM等效功能。安全连接器是iOS上与RSM等效的组件，是终端身份填充和Umbrella式DNS控制所必需的。

了解架构

缺少DNS日志和设备注册的原因是：

- Cisco安全客户端单独提供VPN连接，但缺少DNS可视性所需的终端代理功能
- 安全连接器（等同于Windows上的RSM）是安全访问中的DNS控制和设备注册所必需的
- 没有安全连接器，DNS查询由通过VPN获取的DNS服务器处理，无法查看Umbrella/Secure Access

通过流量导向的DNS日志记录解决方案

要启用DNS日志记录而不安装安全连接器，请配置流量引导以将DNS查询定向到Umbrella DNS服务器：

步骤 1：在安全访问中配置流量引导

导航到Traffic Steering > Add > Add a source，并将DNS服务器IP指定为源。

步骤 2：将DNS流量定向到Umbrella服务器

配置VPN配置文件以使用Umbrella DNS服务器（208.67.222.222和208.67.220.220）来确保DNS查询对安全访问可见。

步骤 3：验证DNS日志记录

实施流量引导配置后，DNS日志应显示在VPN会话的安全访问控制面板中。

VPN配置文件DNS模式设置

VPN配置文件中的“DNS模式”设置与此配置中没有DNS日志无关。无论此设置如何，RAVPN（远程访问VPN）会话都使用通过VPN获取的DNS服务器，日志记录可视性取决于DNS流量是否定向到受监控的DNS基础设施。

安全连接器安装选项

在iOS上安装安全连接器将启用：

- 安全访问中的DNS日志记录可视性
- 增强的终端身份和设备注册功能
- 伞式DNS控制和保护

安全连接器可以与安全客户端配合使用，但是需要适当的流量排除和设计注意事项来防止两个组件之间的冲突。

原因

根本原因是架构性：iOS上的Cisco Secure Client提供VPN连接，但不包括安全访问中的DNS可视性和设备注册所需的终端代理功能。此功能需要安全连接器安装或流量引导配置才能通过受监控的基础设施来引导DNS查询。如果没有这些组件，DNS查询会绕过安全访问监控，并且漫游设备部分不会填充设备身份信息。

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）。