安全访问中MX75网络隧道的安全客户端身份可视性问题

目录

问题

当使用安全客户端的终端部署在连接到安全访问的MX75网络隧道之后时，漫游客户端和用户身份在系统中无法正确可见。观察到以下特定行为：

- 当终端位于MX75后面时，配置为优先于网络隧道连接的安全客户端的回退设置无法按预期运行
- 基于域的流量引导规则不适用，因为流量仅归属于网络隧道身份而不是漫游客户端
- 活动搜索显示不完整的源位置信息，仅显示网络隧道身份，同时忽略用户和漫游客户端身份
- 基于身份的流量引导规则（例如基于Active Directory用户或漫游客户端身份的规则）无法应用于通过MX75隧道的流量

此行为会阻止通过网络隧道基础设施连接的终端进行适当的身份分离和策略应用。

环境

- 思科安全访问部署
- MX75设备，通过网络隧道配置实现安全访问
- 在所有终端上安装的安全客户端代理
- 在漫游客户端上禁用回退设置，以优先于网络隧道连接的安全客户端
- 为基于域的路由配置的流量引导规则
- 为Active Directory用户和漫游客户端配置的基于身份的策略

分辨率

通过使用注册网络方法实施解决方法配置而不是依赖通过MX75网络隧道的漫游身份可视性来解决

问题。

解决方法实施

步骤 1：使用注册网络配置RSM（漫游安全模块）

将现有网络隧道配置替换为RSM部署与注册网络设置相结合。此配置允许正确的身份属性和策略应用。

步骤 2：验证身份可视性

实施注册网络配置后，请验证：

- 用户身份在“活动搜索”中正确显示
- 漫游客户端身份可见且属性正确
- 基于用户和客户端身份功能的流量引导规则（如预期）

步骤 3：测试流量控制功能

确认基于域的流量引导规则和基于身份的策略正确应用于新配置。

替代方法

对于不需要通过专用网络进行身份隔离的环境，请考虑实施RSM - Internet配置。此方法将RSM流量直接发送到互联网，而不是通过专用网络隧道，后者可以在保持安全控制的同时提供正确的身份可视性。

技术分析

在故障排除期间，使用policy.test.sse.cisco.com收集诊断输出，以演示终端在MX75隧道后面时的身份属性行为。分析确认，虽然通过网络隧道路由漫游身份在技术上可行，但是对于此特定部署方案，它不是推荐或支持的操作流程。

原因

根本原因与安全访问在流量通过网络隧道基础设施时如何处理身份属性有关。当终端通过MX75网络隧道连接时，系统会将所有流量归属于隧道身份，而不是保留各个漫游客户端和用户身份。此行为是为网络隧道连接而设计的，但会与个人身份可视性和策略应用的要求冲突。

虽然从技术上来说可以通过网络隧道路由漫游身份，但由于上述身份属性限制，不建议或不支持将此配置作为标准操作流程。

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）。