VPN客户端无法成功验证IP转发表修改错误(&n)：安全客户端RAVPN拆分隧道/默认DNS

目录

问题

在连接到Cisco安全客户端VPN时，Mac用户在尝试对内部应用程序进行CLI身份验证时遇到间歇性故障。在CLI身份验证期间和使用curl等命令时，这些故障显示为“未发现主机”错误。但是，nslookup和dig等DNS解析命令会成功。此问题会随机发生，可以通过重新连接VPN来临时解决，连接将在问题再次出现之前短时间运行。正在使用拆分隧道VPN，并且Cisco Umbrella处于活动状态。使用Palo Alto GlobalProtect VPN时不会发生问题。

- 错误消息：“host not found”(找不到CLI身份验证和curl命令上的host not found)。
- 错误消息： VPN客户端无法成功验证IP转发表修改。连接私有资源时存在域名服务器(DNS)解析问题
- nslookup和dig命令成功
- 重新连接VPN后间断连接
- 已启用拆分隧道远程访问VPN和Umbrella模块
- 问题只能在MacOS设备上通过Cisco安全客户端VPN重现

环境

- 产品：带有多个模块的思科安全客户端(CSC)
- 平台：企业Mac设备
- VPN配置文件配置：远程访问VPN配置文件 — 绕过安全访问 — 拆分隧道模式和DNS模式选择为“默认DNS”
- DNS过滤：启用Cisco Umbrella
- 模块版本：
  - 云管理v1.0.0.23
  - AnyConnect VPN v5.1.13.177
  - Umbrella v5.1.13.177
  - DART v5.1.13.177
  - 安全防火墙安全评估v5.1.13.177
  - 网络可视性模块v5.1.13.177
- 诊断数据：收集用于分析的DART捆绑包
- 仅在思科安全客户端VPN上观察（不在Palo Alto GlobalProtect上）

分辨率

- 在调试客户端上的VPN配置文件(naic.org)拆分隧道配置和AnyConnect VPN路由表时，观察

到以下行为：
    - 工作方案 — 对Vault非生产性本地域执行`nslookup`时，VPN配置文件中配置的DNS服务器处理的DNS请求正确解析为10.x地址。相应地，路由表在非安全路由下使用解析的IP（例如，10.59.130.193）进行更新。
    - 非工作场景 — 但是，当在untun4和en0适配器上配置的macOS系统的本地DNS(192.168.x.x)而不是在VPN配置文件中定义的DNS服务器处理相同的DNS请求时，在发现问题时从数据包捕获中清楚地观察到此行为。
    - 私有域已解析为IP范围34.x.x.x ，这导致了连接问题。Wireshark捕获可帮助确定此问题的根本原因。
- 从设计和配置的角度来看，对于拆分隧道VPN配置文件设置，建议使用拆分DNS，而不是依赖本地系统DNS/默认DNS。
- 此外，还添加了`us-east-eks-amazonaws.com`条目，以确保此EKS集群的流量通过远程隧道接口正确引导。
- 还讨论了RAVPN接口必须优先于Umbrella模块，且不应与包含Umbrella组织ID的`OrgInfo.json`文件冲突。
- 在我们的故障排除过程中，我们完成了没有Umbrella模块的CSC客户端全新安装，在该场景中我们未能发现问题。我也可以从Umbrella的视角查看，在内部域列表中配置的根域naic.org绕过Umbrella，这意味着本地域解析被转发到macOS配置的系统DNS，该系统DNS未被内核级环回接口的Umbrella DNS模块截取。

这与没有Umbrella模块时的问题解决保持一致。通过适当的VPN配置文件配置（包括流量控制规则中的正确域和拆分DNS配置），即使在Umbrella型号为ON时，我们也不应该看到问题。

用户确认，在将DNS模式修改为拆分隧道并编辑VPN配置文件配置后，问题已得到解决。

原因

VPN配置文件 — 绕过安全访问 — DNS模式应设置为拆分隧道（使用案例场景中最常见的选项），并包含拆分DNS配置下的所有专用/内部应用域以解决问题。

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）。