

Umbrella和F5 BIG-IP边缘客户端VPN互操作性问题

目录

问题

同时启用Cisco Umbrella（安全客户端）和F5 BIG-IP边缘客户端VPN时，用户会遇到互联网访问完全丢失的情况。

问题表现如下：

- 当Cisco Umbrella处于活动状态时，连接到BIG-IP边缘客户端VPN后，互联网连接完全不可用。
- 该问题影响所有Internet资源和网站，而不仅仅是特定URL
- 与内部项目相关应用的VPN连接按预期工作
- 禁用Cisco Umbrella时，互联网访问功能正常
- 仅在两个服务同时运行时才会出现问题

环境

- 启用了Umbrella模块的思科安全客户端
- 为分割隧道配置的F5 BIG-IP边缘客户端VPN
- F5 DNS中继代理服务已启用
- Windows终端环境

分辨率

此互操作性问题需要实施两个受支持的解决方法之一，以解决Cisco Umbrella和F5 BIG-IP边缘客户端VPN之间的DNS流量冲突。

选项 1：禁用F5 DNS中继代理服务

第一种解析方法涉及在BIG-IP边缘客户端配置上禁用F5 DNS中继代理服务：

步骤 1：访问F5 BIG-IP边缘客户端配置接口

步骤 2：导航到DNS中继代理服务设置

步骤 3：禁用DNS中继代理服务



注意：此方法可恢复正常的Umbrella DNS功能，但可能会影响当前拆分隧道设计，具体取决于您的F5配置要求。

选项 2：配置F5 VPN拆分隧道排除

建议的解决方案涉及配置F5 BIG-IP边缘客户端以从VPN隧道中排除Umbrella流量：

步骤 1：请与F5管理员联系以修改BIG-IP边缘客户端配置

步骤 2：配置拆分隧道列表，以明确排除发往Umbrella DNS和代理IP范围的所有网络流量

步骤 3：应用配置更改以确保Umbrella安全流量与VPN连接一起运行



提示：此配置更改必须由F5管理员实施，并且需要特定的Umbrella DNS和代理IP范围知识，以确保从VPN隧道正确排除。

原因

此问题是由于Cisco安全客户端（Umbrella模块）和F5 BIG-IP边缘客户端VPN之间的已知互操作性限制，当VPN配置为使用启用F5 DNS中继代理服务的拆分隧道时。

根本原因是由于Umbrella客户端和F5 VPN客户端都尝试在终端级别拦截和代理DNS流量。当两个服务同时处于活动状态时，这会造成无法正确转发DNS请求的冲突，从而导致Internet连接完全中断。F5 DNS中继代理服务会干扰Umbrella DNS拦截机制，阻止对互联网资源进行适当的DNS解析。

此行为由思科和F5共同记录为已知限制，与任一产品中的特定软件缺陷无关。

相关内容

- [BIG-IP边缘客户端和Cisco Umbrella客户端的DNS问题](#)
- [了解Umbrella漫游客户端和F5 VPN兼容性](#)
- [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）。