为使用Umbrella模块的安全客户端启用所有DNS隧道

目录

简介

背景信息

问题和影响

建议

简介

本文档介绍如何为带有Umbrella模块的思科安全客户端启用所有DNS隧道。

背景信息

思科于2023年宣布了Cisco AnyConnect的生命周期终止，并于2024年宣布了Umbrella漫游客户端。许多Cisco Umbrella客户已经从迁移到Cisco安全客户端中受益，我们鼓励您尽快开始迁移，以获得更好的漫游体验。阅读此知识库文章的更多信息：如何安装带有Umbrella模块的思科安全客户端？

带有Umbrella（以前称为AnyConnect漫游安全）模块的Cisco Secure Client(CSC)模块设计用于几乎所有CSC VPN模式，无需额外配置。

但是，当这些条件都成立时，还需要考虑以下因素：

- 已启用分割隧道
- “Tunnel All DNS”功能已启用

问题和影响

启用“Tunnel All DNS”后，DNS流量会在内核级别被拦截，如果流量未从正确的VPN接口流出，则会被拦截。如果Cisco Umbrella解析器不是分割隧道(Include)配置的一部分，这会为CSC模块带来问题。

此问题的影响最小，因为默认情况下，CSC模块使用加密DNS（UDP端口443），它不会被“Tunnel All DNS”阻止。 因此，问题只发生在DNS加密不可用的网络上。

场景如下：

- 漫游模块尝试通过普通局域网接口将流量路由到Cisco Umbrella。
- 本地网络不允许DNS加密，因此会发送标准的未加密DNS查询。
- 此流量被“Tunnel All DNS”功能阻止，该功能要求DNS进入VPN。

在这种情况下，DNS无法按预期运行。

建议

为确保此情况无法实现，Cisco Umbrella建议采取以下措施之一。

- 在VPN组策略中禁用“Tunnel All DNS”。CSC模块处理DNS路由。
  或者
- 将以下Cisco Umbrella DNS解析器添加到拆分隧道(Include)配置：
  - 208.67.222.222
  - 208.67.220.220
  - 208.67.222.220
  - 208.67.220.222

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）。