为企业网络上的Umbrella漫游客户端禁用受保护的网络

目录

[简介](#)

[背景信息](#)

[什么是受信任网络域功能？](#)

[IPv6行为，Windows与MacOS](#)

[如何启用此功能？](#)

[如何测试一台计算机的功能？](#)

简介

本文档介绍如何在公司网络上禁用Umbrella漫游客户端（独立客户端和AnyConnect），并在公司网络上启用该客户端。

背景信息

本文面向管理员。如果您不想在网络中退出漫游客户端，请在此处停止。

Umbrella protected networks（Umbrella保护网络）功能适用于单个出口网络。对于有多个出口的任何网络，都需要备用功能。

如今，此功能作为受信任网络域功能存在于生产中。请继续阅读，了解如何申请该功能，以及您的网络需要什么。

什么是受信任网络域功能？

“按域划分受信任网络”功能是一种在公司网络上禁用漫游客户端，但将其从网络中保持启用状态的方法。激活后，该功能：

- 禁用漫游客户端提供的DNS保护
    - 将策略推迟至网络策略
- 停止除受信任网络域检查之外的所有网络探测
    - 非常适合繁忙的网络！
    - VA回退的绝佳替代方案
        - 与VA配合使用，减少网络通信

IPv6行为，Windows与MacOS

- 在Windows上，域在IPv4和IPv6上进行查询。关闭行为在每个网络堆栈上单独处理。例如，如

果域在IPv4上解析，而非IPv6上解析，则漫游客户端仅在IPv4上关闭，在IPv6上保持运行。如果您希望完全关闭客户端，则必须解决IPv4 和IPv6查询。
- 在MacOS上，在IPv4和IPv6上查询域。与Windows不同，如果域在任一网络堆栈上解析，则漫游客户端会同时关闭IPv4和IPv6。

如何启用此功能？

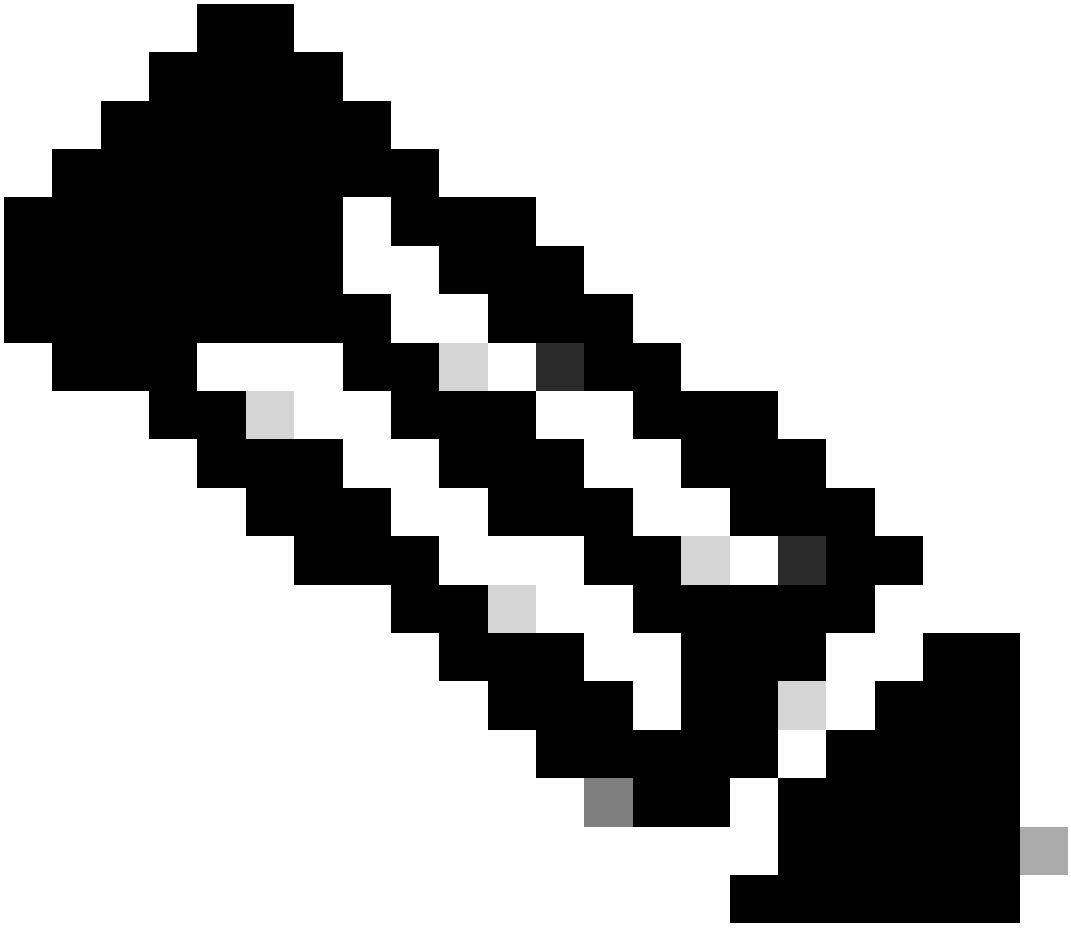
此功能现在在控制面板中控制。请参阅漫游计算机设置。

- 所需的Umbrella禁用子域。此域必须：
  - 拥有解析为RFC-1918内部IP地址（用于IPv4）的A记录
  - 拥有可解析为IPv6上的RFC-4193 IP的AAAA记录（如果使用IPv6）
    - RFC-1918 IP通常类似于10.x.x.x、172.x.x.x或192.168.x.x
    - RFC-4193 IPv6地址以“FD”开头
    - IP地址不必可访问
    - 必须是子域
      - sub.domain.com — 很好！
      - subdomain.com — 不好。
  - 将网络解析为NXDOMAIN、NODATA或公有IP地址（因此客户端在此情况下保持启用状态）
    - 请勿SERVFAIL
  - 成为您控制的区域中的域，以确保控制公共空间和本地空间
- 支持:
  - Umbrella漫游客户端
  - 仅AnyConnect Umbrella漫游安全模块4.5 MR4+

如何测试一台计算机的功能？

要在使Umbrella团队全局应用设置之前进行本地测试，请应用此覆盖。

1. 创建文件“customer_network_probe.flag”
    1. 确保文件不是.flag.txt
2. 将所需的域放入文件的内容中
3. 将文件放入：
    1. 漫游客户端
        1. Windows 窗口版本:%ProgramData\OpenDNS\ERC\
    2. AnyConnect
        1. Windows 窗口版本:%ProgramData%\Cisco\Cisco AnyConnect安全移动Client\Umbrella\data\
    3. 思科安全客户端
        1. Windows 窗口版本:C:\ProgramData\Cisco\Cisco安全Client\Umbrella\data\
        2. macOS:/opt/cisco/secureclient/umbrella/data/
4. 重新启动漫游客户端
    1. 漫游客户端：Umbrella漫游客户端：手动禁用或重新启动。
    2. AnyConnect：重新启动父vpnagent AnyConnect服务



注意：MacOS漫游客户端，AnyConnect版本不支持此标志。

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）。