

為企業網路上的Umbrella漫遊客戶端禁用受保護的網路

目錄

[簡介](#)

[背景資訊](#)

[什麼是受信任網路域功能？](#)

[IPv6行為，Windows與MacOS](#)

[如何啟用此功能？](#)

[如何在一台電腦上測試該功能？](#)

簡介

本文描述如何在公司網路上禁用Umbrella漫遊客戶端（獨立客戶端和AnyConnect），並在公司網路上啟用該客戶端。

背景資訊

本文面向管理員。如果您不想在網路中退出漫遊客戶端，請在此處停止。

Umbrella protected networks功能專用於單個出口網路。對於有多個出口的任何網路，都需要備用功能。

如今，此功能作為可信網路域功能存在於生產中。請繼續閱讀，瞭解如何請求此功能以及您的網路需要什麼。

什麼是受信任網路域功能？

受信任網路逐域功能是禁用公司網路上的漫遊客戶端，但保持其啟用遠離網路的方法。啟用後，此功能：

- 禁用漫遊客戶端提供的DNS保護
 - 將策略推遲至網路策略
- 停止除受信任網路域檢查之外的所有網路探測
 - 非常適合繁忙的網路！
 - VA回退的絕佳替代方案
 - 與VA配合使用可減少網路通話

IPv6行為，Windows與MacOS

- 在Windows上，域在IPv4和IPv6上查詢。關閉行為在每個網路堆疊上單獨處理。例如，如果域

在IPv4上解析，而非IPv6上解析，則漫遊客戶端僅在IPv4上關閉，在IPv6上保持運行。如果您希望完全關閉客戶端，則必須解析IPv4 和IPv6查詢。

- 在MacOS上，域在IPv4和IPv6上查詢。與Windows不同，如果域在任一網路堆疊上解析，則漫遊客戶端將同時關閉IPv4和IPv6。

如何啟用此功能？

此功能現在在儀表板中控制。請參閱漫遊電腦設定。

- 所需的Umbrella禁用子域。此域必須：
 - 具有解析為RFC-1918內部IP地址（用於IPv4）的A記錄
 - 具有解析為RFC-4193 IPv6上的IP的AAAA記錄（如果使用IPv6）
 - RFC-1918 IP通常像10.x.x.x、172.x.x.x或192.168.x.x
 - RFC-4193 IPv6地址以「FD」開頭
 - IP地址不必可訪問
 - 必須是子域
 - sub.domain.com — 很好！
 - subdomain.com — 不好。
 - 將網路解析為NXDOMAIN、NODATA或公共IP地址（因此在此情況下客戶端保持啟用狀態）
 - 沒有SERVFAIL，請
 - 成為您控制的區域中的域，以確保您控制公共空間和本地空間
- 支援：
 - Umbrella漫遊客戶端
 - 僅AnyConnect Umbrella漫遊安全模組4.5 MR4+

如何在一台電腦上測試該功能？

要在Umbrella團隊全域性應用設定之前進行本地測試，請應用此覆蓋。

1. 建立檔案「customer_network_probe.flag」
 1. 確保檔案不是.flag.txt
2. 將所需的域放入檔案的內容中
3. 將檔案放入：
 1. 漫遊客戶端
 1. Windows:%ProgramData\OpenDNS\ERC\
 2. AnyConnect
 1. Windows:%ProgramData%\Cisco\Cisco AnyConnect Security Mobility Client\Umbrella\data\
 3. 思科安全使用者端
 1. Windows:C:\ProgramData\Cisco\Cisco安全Client\Umbrella\data\
 2. macOS:/opt/cisco/secureclient/umbrella/data/
4. 重新啟動漫遊客戶端
 1. 漫遊客戶端：Umbrella漫遊客戶端：手動禁用或重新啟動。
 2. AnyConnect:重新啟動父vpnagent AnyConnect服務



附註：MacOS漫遊客戶端，AnyConnect版本不支援此標誌。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。