

管理Umbrella漫遊客戶端和VPN相容性

目錄

[簡介](#)

[概觀](#)

[Umbrella漫遊客戶端如何與VPN客戶端一起運行](#)

[Umbrella漫遊客戶端不相容](#)

[VPN客戶端不相容的原因](#)

[虛擬裝置和受保護的網路](#)

[獨立式和思科安全客戶端+漫遊安全模組的特殊注意事項](#)

[適用於Windows 10和11的DNS繫結順序VPN相容模式](#)

[resolv.conf輸出示例](#)

[第三方VPN的特殊注意事項](#)

[永遠線上VPN](#)

[解決方案](#)

[粘度VPN](#)

[配置粘度](#)

[隧道布里克](#)

[Tunnelblick VPN斷開連線問題](#)

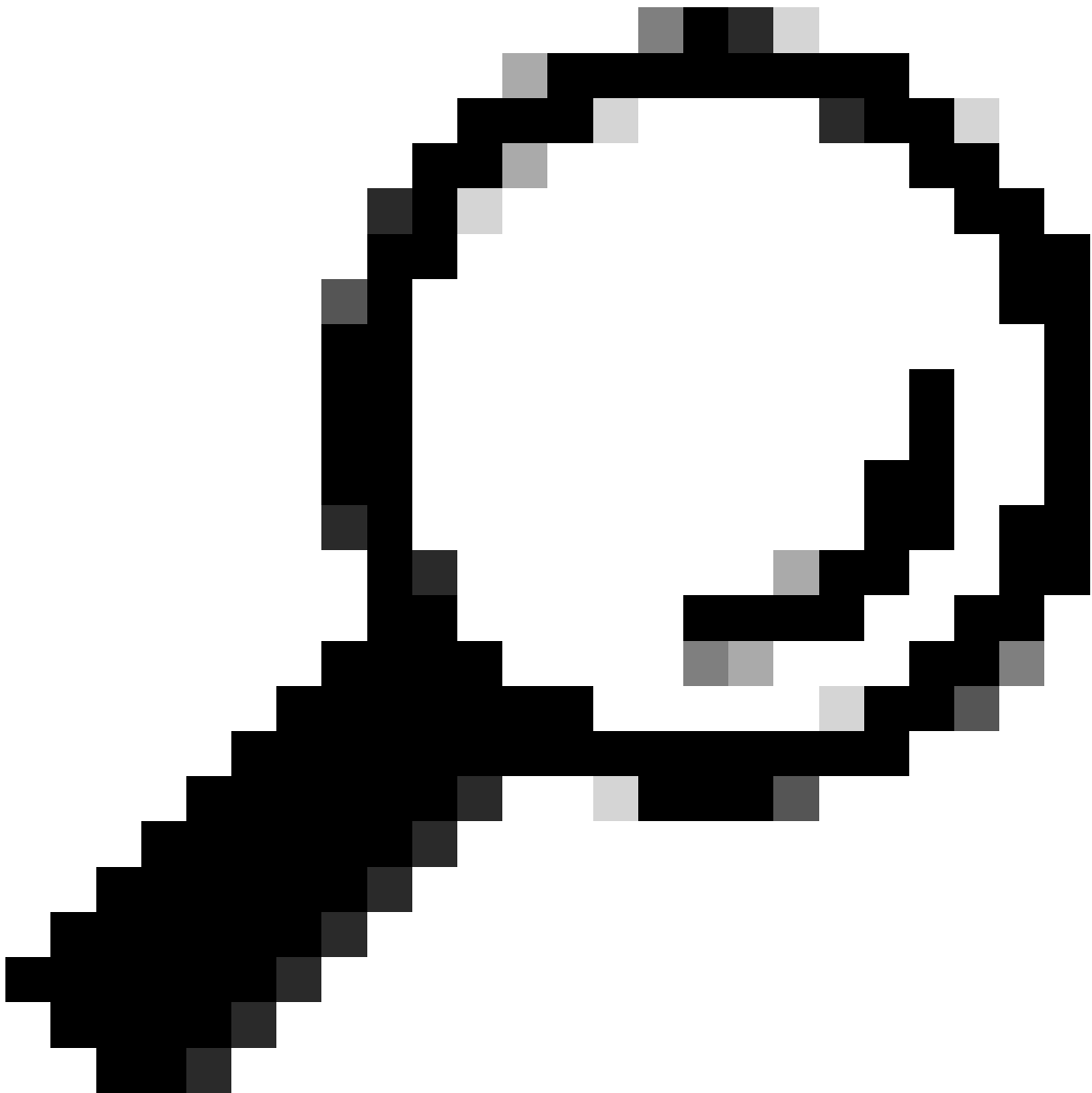
[光速火箭](#)

簡介

本檔案介紹Cisco Umbrella漫遊客戶端與各種VPN軟體的互動和相容性。

概觀

Cisco Umbrella Roaming Client可與大多數VPN軟體配合使用，但可能需要執行其他步驟才能進行預期操作。Cisco Umbrella建議部署思科安全客戶端和漫遊安全模組以實現最大相容性。可以部署此模組而不使用VPN元件。



提示：本文檔可用作一般指導，並不作為受支援軟體的正式清單。Cisco Umbrella不測試、驗證或驗證任何第三方軟體或VPN客戶端的功能。

本文檔為可能需要進一步配置的特定VPN客戶端提供技術資訊和其它上下文。有關已知不相容的VPN軟體的清單，請參閱Umbrella漫遊客戶端不相容部分。DNS與漫遊客戶端的不相容性還可能導致帶SWG的Cisco安全客戶端+漫遊安全模組失敗，因為SWG客戶端還取決於能否成功建立DNS連線。

Umbrella漫遊客戶端如何與VPN客戶端一起運行

Umbrella漫遊客戶端繫結到所有網路介面卡，並將電腦上的DNS設定更改為127.0.0.1(localhost)。這允許Umbrella漫遊客戶端將所有DNS查詢直接轉發到Umbrella，同時允許通過內部域功能解析本地域。在建立與VPN伺服器的連線時，Umbrella漫遊客戶端在系統中檢測到新的網路連線，並更改

連線DNS設定以指向Umbrella漫遊客戶端。Umbrella漫遊客戶端依賴於對Umbrella AnyCast DNS IP地址(208.67.222.222/208.67.220.220)執行DNS查詢。

如果使用者連線到VPN，與VPN關聯的防火牆必須允許訪問Umbrella。

Umbrella漫遊客戶端不相容

Umbrella漫遊客戶端當前提供DNS層實施。DNS層是漫遊客戶端的主要功能，可在任何網路上應用基於DNS的安全策略。漫遊客戶端的此功能可能遇到已知的軟體不相容。根據支援團隊測試，Umbrella漫遊客戶端的DNS層與下面列出的客戶端不相容。Cisco Umbrella Engineering不驗證或測試這些客戶端，所有條目都要檢查。本文參考獨立式Umbrella漫遊客戶端。有關Umbrella Roaming Security Module for Cisco Secure Client (和舊版)的配套文章，請參閱相關文檔。

VPN使用者端	問題/不相容	解析
Pulse Secure	在斷開連線時，由於VPN連線期間的Pulse修改，儲存的本地DNS可以保留VPN值而不是WiFi/乙太網值。	已使用Umbrella模組解決 — 包含在大多數許可證中。
Avaya VPN	不相容。	已使用Umbrella模組解決 — 包含在大多數許可證中。
Windows VPN (尤其是始終在VPN上)	可能導致本地DNS無法解析為內部答案，儘管DNS主機名位於內部域清單中。	已使用Umbrella模組解決 — 包含在大多數許可證中。
在Windows通用平台上構建的VPN「應用」	這些應用必須使用要求將DNS傳送到本地NIC (而不是127.0.0.1) 的Microsoft連線API。因此，應用顯示一個錯誤，指示它無法連線。	已使用Umbrella模組解決 — 包含在大多數許可證中。
OpenVPN	不相容。	沒有可用的修補程式。
Palo Alto GlobalProtect VPN	3.0.110之後的任何獨立漫遊客戶端版本都無法使用。	已使用Umbrella模組修復 — 包含在大多數許可證中。
F5 VPN	不相容。	由Umbrella模組修復 — 包含在大多數許可證中。
檢查點VPN	僅限MacOS，僅限拆分隧道模式。	在macOS上禁用拆分隧道。

VPN使用者端	問題/不相容	解析
SonicWall NetExtender	不相容。	由Umbrella模組修復 — 包含在大多數許可證中。
Zscaler VPN	不相容。	由Umbrella模組修復 — 包含在大多數許可證中。
Akamai端點保護 (ETPclient)	不相容。	由Umbrella模組修復 — 包含在大多數許可證中。
NordVPN	使用解決方法。	有兩個選項可用於新增相容性： 1. 使用How to set a manual connection on Windows using OpenVPN中介紹的OpenVPN連線方法 2. 在Advanced設定下允許自定義DNS。將DNS設定為208.67.220.220和208.67.222.222。
Azure VPN	不相容。	由Umbrella模組修復 — 包含在大多數許可證中。
AWS VPN	使用解決方法。	編輯配置檔案（手動從AWS下載），獲得第二行pull-filter ignore "block-outside-dns"。
普通VPN	不相容。	由Umbrella模組修復 — 包含在大多數許可證中。

VPN客戶端不相容的原因

某些VPN客戶端的DNS行為與Umbrella漫遊客戶端類似。如果VPN連線DNS伺服器更改為意外值，則VPN軟體會將系統DNS設定更改回最初連線時設定的VPN值。Umbrella漫遊客戶端也執行相同的操作，將任何DNS伺服器改回127.0.0.1。這種反複的行為在VPN和Umbrella漫遊客戶端之間造成衝突。此衝突會導致VPN連線重置的DNS伺服器無休止循環。漫遊客戶端檢測到此情況並禁用自身以維護VPN連線（如果可能）。

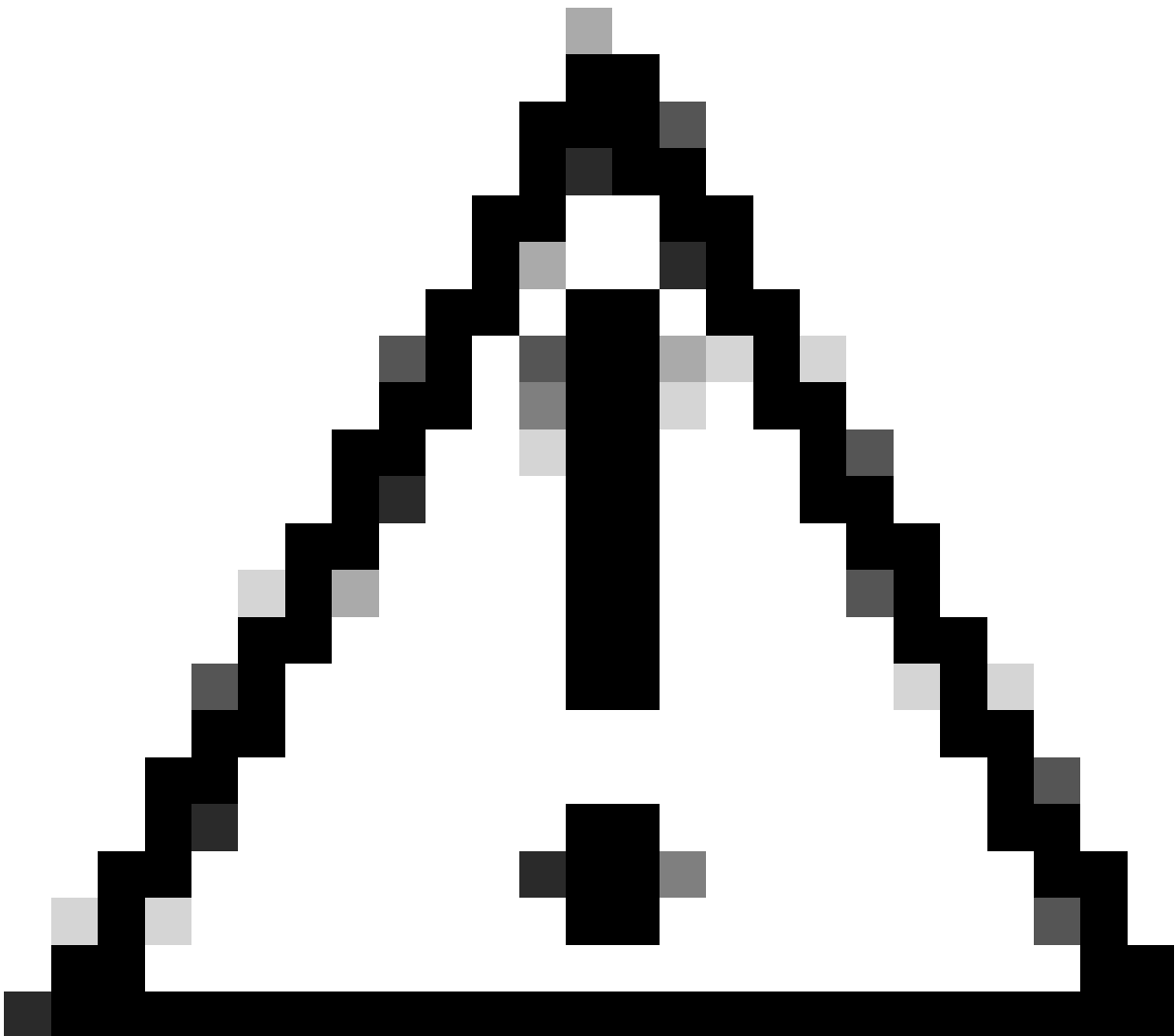
虛擬裝置和受保護的網路

當連線到使用Umbrella虛擬裝置(VA)或受保護網路功能的網路時，Umbrella漫遊客戶端的行為會有所不同。這適用於使用者是本地連線到網路還是通過VPN連線到網路。有關詳細資訊，請參閱漫遊客戶端和虛擬裝置或受保護網路文檔。

獨立式和思科安全客戶端+漫遊安全模組的特殊注意事項

此處提供的資訊是專用於獨立的Umbrella漫遊使用者端，不會延伸至思科安全使用者端(CSC)+漫遊安全模組。尋求簡單外掛安裝的使用者可以使用整合到CSC的Umbrella Roaming。如果VPN出現功能問題，Cisco安全客戶端VPN使用者必須遷移到CSC +漫遊安全模組。Cisco Umbrella需要在CSC +漫遊安全模組上進行驗證，並建議進行完全遷移。

Cisco安全客戶端VPN軟體提供了在VPN連線建立時系統如何處理DNS的選項。有關其他詳細資訊，請參閱[有關不同OS中的DNS查詢和域名解析的行為差異](#)一文。此資訊基於使用思科安全客戶端和Umbrella漫遊客戶端的經驗。建議在啟用思科安全客戶端VPN的情況下測試Umbrella漫遊客戶端，以確保內部和外部DNS解析功能如預期那樣運行。



注意：如果您還使用思科安全客戶端實現DNS服務相容性，思科要求使用CSC +漫遊安全模組。所提供的步驟僅適用於非整合漫遊客戶端（如果需要）。CSC +漫遊安全模組不需要執行這些步驟。

在全通道模式和分離通道模式下，需要特殊指令以允許漫遊客戶端在連線思科安全客戶端時工作。這是必需的，以便允許DNS流到漫遊客戶端，而不是被核心驅動程式覆蓋。對於全通道，症狀是客戶端被強制禁用。對於分割隧道，症狀是在連線到VPN時丟失內部DNS。

適用於Windows 10和11的DNS繫結順序VPN相容模式

有限的Windows 10使用者遇到一個特定問題，即本地LAN優先於用於DNS的VPN NIC。在這種情況下，當公共DNS正常運行時，漫遊客戶端的內部域清單上的本地DNS無法解析。這會影響版本2.0.338和2.0.341（預設）和所有較新版本。2.0.255版上未出現問題。

先前受影響的VPN客戶端包括：

- AnyConnect 3.x
- AnyConnect 4.x（AnyConnect Umbrella或CSC +漫遊模組不受影響）
- Sophos VPN
- 舊版本上的某些Palo Alto GlobalProtect配置
- WatchGuard行動VPN
- 精簡型軟VPN
- 梭魚VPN

解析

將Roaming Client設定Enable legacy VPN compatibility mode切換為enabled。

Roaming Computers Settings

Umbrella Roaming Client

- ☐ Disable DNS redirection while on an Umbrella Protected Network. 
- ☒ Enable Active Directory user and group policy enforcement and internal IP address visibility.
- ☒ Enable legacy VPN compatibility mode. [Learn More](#)

360027547111

要確認問題是否存在，請運行診斷測試並按一下的結果resolv.conf。如果首先列出VPN介面卡，則問

題不會影響使用者。如果VPN介面卡列在第二位，則問題可能影響使用者。

resolv.conf輸出示例

Results for: resolv.conf

C:\ProgramData\OpenDNS\ERC\Resolver1-76F52CE47B124D9FB05591D162777829-resolv.conf

resolvers for Local Area Connection

nameserver 192.168.2.1

C:\ProgramData\OpenDNS\ERC\Resolver1-76F52CE47B124D9FB05591D162777829-resolv.conf

resolvers for Cisco AnyConnect Secure Mobility

nameserver 10.1.1.27

nameserver 10.1.1.28

第三方VPN的特殊注意事項

永遠線上VPN

定義受信任的DNS伺服器時，獨立漫遊客戶端與Cisco Secure Client Always On VPN設定不相容。當處於活動狀態時，獨立漫遊客戶端始終將DNS設定為127.0.0.1，從而從NIC設定中刪除所有受信任的DNS伺服器。可以在網路上禁用漫遊客戶端以恢復DHCP設定；但是，配置後，所有與漫遊客戶端相關的保護都將停止。請與Umbrella支援部門聯絡，瞭解有關禁用受信任網路上的客戶端的詳細資訊。

解決方案

- CSC +漫遊安全模組 (Cisco Secure Client的漫遊客戶端) 不受影響，並可通過自動VPN策略有效運行。
- 將127.0.0.1新增到受信任DNS伺服器清單中。
- 確保定義了其他受信任檢測方法 (DNS名稱和伺服器)，以防止所有網路被宣告為受信任。

The screenshot shows the Cisco Secure Client configuration window. It has a light beige background. On the left, there are several settings with checkboxes and labels. On the right, there are input fields and buttons. The settings include:

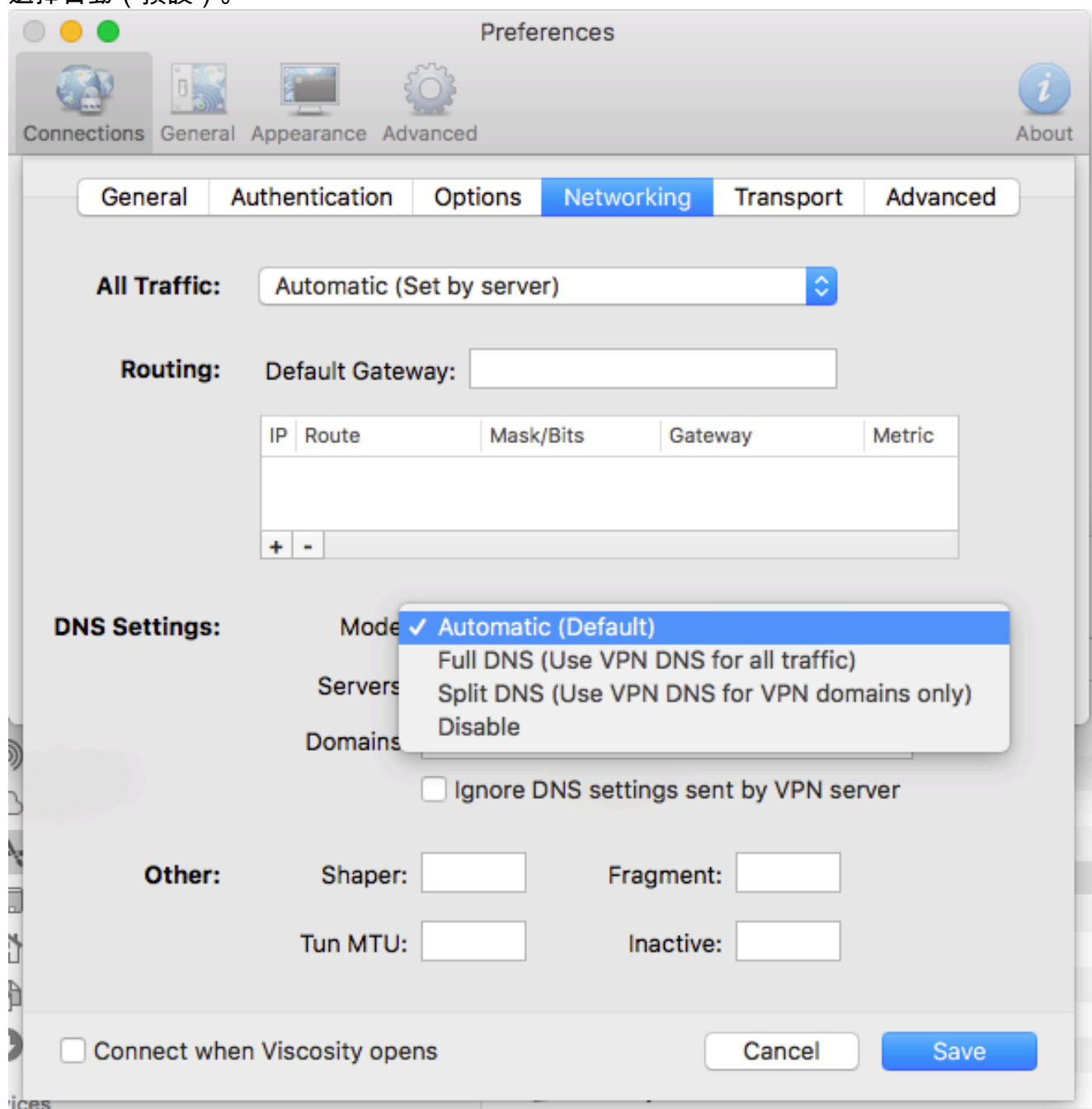
- ☒ Automatic VPN Policy
- Trusted Network Policy: Disconnect (dropdown menu)
- Untrusted Network Policy: Connect (dropdown menu)
- Trusted DNS Domains: mydomain.local (text field)
- Trusted DNS Servers: 172.16.191.1 (text field)
- Note: adding all DNS servers in use is recommended with Trusted Network Detection
- Trusted Servers @ https://<server>[:<port>]
- https:// (text field) with an Add button
- https://mysite.mydomain.local:443 (text field) with a Delete button

粘度VPN

粘性VPN需要更改設定才能使用Umbrella漫遊客戶端。如果未進行此更改，則Viscosity預設行為會模仿其他不相容的VPN的行為。此更改指示Viscosity對搜尋域中的所有域使用通過Umbrella伺服器推送的DNS設定，127.0.0.1繼續用於任何其他請求。

配置粘度

1. 在Viscosity中，導航到Preferences > Connections > <your connection>(site specific)> Networking > DNS Settings。
2. 選擇自動（預設）。



使用OpenVPN伺服器時，請確保伺服器端未啟用persist-tun，以確保斷開連線或重新連線時觸發網路更改。

隧道布里克

Tunnelblick要求進行兩項更改：

- 允許更改介面卡的DNS伺服器。
- 在隧道建立後應用DNS設定。

通過確保Advanced選單中提供的設定，Tunnelblick可以與Umbrella Roaming Client配合使用：

在「Connecting and Disconnecting(連線和斷開連線)」頁籤中，啟用以下兩種設定：

- 在連線或斷開連線後刷新DNS快取（預設）
- 在路由設定後而不是路由設定前設定DNS

在While Connected選項卡中，將此設定更改為Ignore：

- DNS:Servers > When更改到pre-VPN值，When更改到任何其他值。

使用OpenVPN伺服器時，請確保伺服器端未啟用persist-tun，以確保斷開連線或重新連線時觸發網路更改。

Tunnelblick VPN斷開連線問題

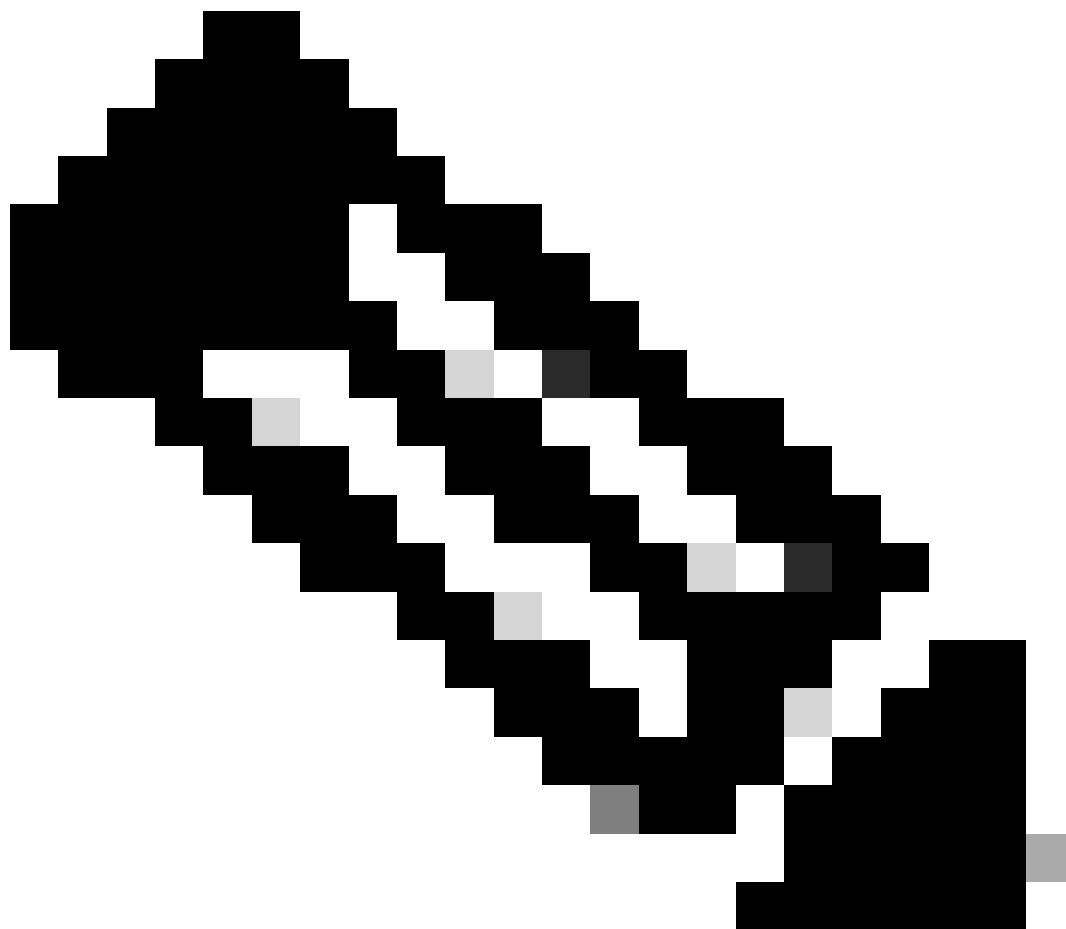
對於某些Tunnelblick版本，漫遊客戶端在VPN斷開連線後無法正確識別正確的內部DNS伺服器。如果VPN斷開連線後出現Internal Domains問題，Umbrella建議採取以下步驟：

此更改會導致Tunnelblick在VPN斷開連線後關閉和開啟主網路介面。在Tunnelblick配置面板的Settings頁籤上管理此項：

- 在舊版Tunnelblick（3.7.5beta03之前）中，使用斷開連線後重置主介面覈取方塊。
- 在新版Tunnelblick（3.7.5beta03及更高版本）上，將On expected disconnect和On expected disconnect設定都設定為Reset Primary Interface。

光速火箭

Lightspeed Rocket具有與Roaming Client不相容的某些功能。具體來說，對www.google.com的無SSL Search和SafeSearch CNAME重新導向的DNS修改nosssearch.google.com forcesafesearch.com，分別會導致所有www.google.com DNS解析失敗（只要啟用了Lightspeed Rocket DNS重新導向）。



附註：本文參考獨立式Umbrella漫遊客戶端。有關適用於Cisco安全客戶端和舊版軟體的Umbrella漫遊安全模組的隨附文章，請參閱相關文檔。

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）。