在公司網路上配置Umbrella漫遊客戶端

目錄

簡介

本文檔介紹貴公司網路上的Umbrella漫遊客戶端的配置。

概觀

Umbrella漫遊客戶端是保護遠端使用者的絕佳工具，但它也可以保護企業網路上的使用者，從而增加一層安全保護。根據業務需要，有些管理員希望繼續保護企業網路上的Umbrella漫遊客戶端，而其他管理員則希望讓Umbrella漫遊客戶端「後退」以利於其他Umbrella策略。

Umbrella為Umbrella漫遊客戶端進入您的網路時的運行方式提供了靈活性。本文概述了這些不同的方法。

目標

Q)。 我為什麼要禁用公司網路上的Umbrella漫遊客戶端？

通常，不需要禁用Umbrella漫遊客戶端來使內部和外部DNS工作。Umbrella漫遊客戶端使用域管理功能將您的內部DNS流量定向到您的普通DNS伺服器。這樣，當Umbrella漫遊客戶端在網路中的終端上運行時，您可以同時保留保護和連線。

但是，有時會有理由考慮禁用漫遊客戶端保護……

- 為離開網路的漫游使用者提供不同的「網路內」和「網路外」策略。
- 在公司網路上使用內部DNS伺服器在快取和減少傳出DNS流量方面有一些優勢。
- Umbrella漫遊客戶端定期發送探測消息，以驗證與Umbrella的連線。當您擁有大量客戶端時，可能不需要這種額外的流量。

問：我為什麼希望在我的公司網路上繼續啟用Umbrella漫遊客戶端？

另一方面，保持漫遊客戶端始終處於啟用狀態有一些很好的理由：

- 確保Umbrella漫遊客戶端電腦始終使用相同的策略。
- 始終在報告中可識別Umbrella漫遊客戶端的主機名（而不是網路標識）— 用於精細報告。
- 漫遊客戶端使用「加密的DNS」流量增強隱私
- 對於Secure Web網關使用者（使用AnyConnect），客戶端必須保持啟用狀態以提供SWG網路過濾。

工作模式

始終開啟

即使在公司網路上使用時，Umbrella漫遊客戶端也可以保持開啟。在此模式下，使用Umbrella漫遊客戶端標識配置策略，並且此標識顯示在報告中。

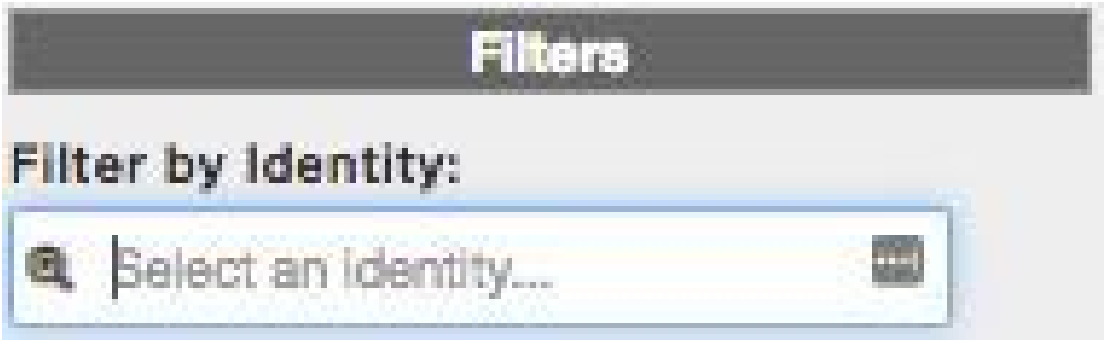
政策	始終使用Umbrella漫遊客戶端標識。
報告	Umbrella漫遊客戶端標識始終顯示在提供每電腦粒度的報告中
DNS流量	• Umbrella漫遊客戶端繼續將DNS查詢直接傳送到Umbrella，即使在公司網路上也是如此。 • 傳送到Umbrella的查詢已加密，從而提供額外的安全性。 • 對「內部域」的查詢將路由到您的普通DNS伺服器，而不是傳送到Umbrella。
探測消息	Umbrella漫遊客戶端繼續傳送探測消息以確定Umbrella的可用性。

如何配置「Always ON」模式：

1. 導覽至Identities > Roaming Computers。
2. 按一下(漫遊客戶端設定)圖示。
3. 清除在Umbrella受保護網路上禁用DNS重定向，然後按一下Save。
4. 為Umbrella漫遊客戶端建立單獨的策略，並確保它是最高優先順序（位於清單的最頂部）。您的Umbrella漫遊客戶端策略的優先順序必須高於任何基於網路身份的策略。

使用常規網路策略

Umbrella漫遊客戶端已啟用，並且繼續直接與Umbrella對話，但是，網路身份用於策略和報告目的。只需將網路策略置於比Umbrella漫遊客戶端策略更高的優先順序即可啟用此模式。

政策	在受保護的網路上使用網路策略。這允許使用不同的開/關網路策略。
報告	• 報告與作為主要身份的網路身份相關聯。 • 報告仍允許您通過Umbrella漫遊客戶端主機名進行搜尋，以便僅過濾該客戶端的結果。 
DNS流量	• Umbrella漫遊客戶端繼續將DNS查詢直接傳送到Umbrella，即使在公司網路上也是如此。 • 傳送到Umbrella的查詢已加密，從而提供額外的安全性。 • 對「內部域」的查詢將路由到您的普通DNS伺服器，而不是傳送到Umbrella。
探測消息	Umbrella漫遊客戶端繼續傳送探測消息以確定Umbrella的可用性。

如何「使用常規網路策略」：

1. 導覽至Identities > Roaming Computers。
2. 按一下(漫遊客戶端設定)圖示。
3. 清除在Umbrella受保護網路上禁用DNS重定向，然後按一下Save。
4. 為您的網路建立單獨的策略。 確保您的網路策略的優先順序高於任何基於漫遊客戶端的策略。

在受保護網路後禁用（適用於小型網路）
Umbrella漫遊客戶端在檢測到它位於受保護的網路時可以「後退」。這意味著網路身份用於策略和

報告目的。

此模式在行為上與「使用常規網路策略」模式類似，不同之處在於Umbrella漫遊客戶端實際上會禁用自身，不會干擾DNS流量。

政策	在受保護的網路上使用網路策略。這允許使用不同的開/關網路策略。
報告	當在受保護網路上時，對於報告沒有每台電腦的粒度。報告僅與網路標識相關聯。
DNS流量	在受保護的網路上，Umbrella漫遊客戶端不會干擾DNS查詢，並且它們會轉到正常的內部DNS伺服器。
探測消息	Umbrella漫遊客戶端繼續傳送探測消息，以確定它是否位於受保護的網路上。

如何在受保護的網路後面配置Disable:

1. 導覽至Identities > Roaming Computers。
2. 按一下(漫遊客戶端設定)圖示。
3. 選擇Disable DNS redirection while on an Umbrella Protected Network，然後按一下Save。
4. 導航到Policies > Policies List。
5. 為您的網路建立單獨的策略。 確保您的網路策略的優先順序高於任何基於Umbrella漫遊客戶端的策略。
6. 您的本地DNS伺服器必須轉發到Umbrella解析程式，並且必須在Umbrella控制面板中正確註冊。
7. 要使用此功能，客戶端工作站使用的輸出IP必須註冊到與您的內部DNS伺服器使用的輸出IP相同的網路標識。有關全部詳細資訊，請參閱本文。

在受信任網路域之後禁用（適用於大型網路）

現在可以選擇客戶配置的「受信任網路域」。 客戶端嘗試解析此DNS域（A記錄），並在域成功解析時禁用保護。 這是僅用於內部的DNS記錄，僅當客戶端位於公司網路時才解析。

政策	只要檢測到受信任域，客戶端就會回退，並且不一定接收Umbrella策略或過濾。 我

	們建議新增其他Umbrella功能(例如網路保護)，確保策略仍應用於公司網路。
報告	只要檢測到受信任域，客戶端就會回退，並且不一定接收Umbrella策略或過濾。 如果網路受其他Umbrella功能(例如網路保護)，則流量出現在報告中的網路標識下。
DNS流量	在受信任的網路中，Umbrella漫遊客戶端不會干擾DNS查詢，並且它們會轉到正常的內部DNS伺服器。
探測消息	Umbrella漫遊客戶端在此狀態下禁用其大部分DNS「探測」測試，從而大大減少了漫遊客戶端生成的流量。

如何配置受信任網路域：

1. 在內部DNS伺服器上建立DNS A記錄(例如，magic.mydomain.tld)。
    1. 記錄必須是「子域」（最少3個DNS標籤）
    2. 記錄必須解析為內部RFC-1918地址
    3. 請注意確保該記錄不公開存在
2. 導覽至Identities > Roaming Computers。
3. 按一下(漫遊客戶端設定)圖示。
4. 選擇Trusted Network Domain選項並輸入域名(例如，magic.mydomain.tld)。 按一下「Save」。

將Umbrella漫遊客戶端與Umbrella虛擬裝置配合使用

作為Umbrella「Insights」產品的一部分(在Platform and Insights產品包中)，我們提供Virtual Appliance(VA)，它在您的網路中充當DNS轉發器。此VA是獲得有關您網路上DNS請求源的可視性的關鍵，也是我們的Active Directory整合所必需的。

預設情況下，如果Umbrella漫遊客戶端檢測到VA正用於DNS轉發，則它會禁用自身。如果已將VA分配為DNS伺服器（使用DHCP或靜態設定），則Umbrella漫遊客戶端會檢測到此情況並禁用自身。

VA回退

政策	啟用VA回退後，VA身份用於決定所選策略。可以基於以下身份建立策略： • AD使用者（僅當啟用AD整合時） • AD電腦（僅當啟用AD整合時） • 內部網路 • Umbrella站點名稱。 有關策略優先順序的詳細資訊，請按一下此處。
報告	啟用VA回退後，在VA後面時Umbrella漫遊客戶端被禁用，並且不會顯示在報告中。報告記錄為： • AD使用者（僅當啟用AD整合時） • AD電腦（僅當啟用AD整合時） • 內部網路 • Umbrella站點名稱。 此外，還會記錄每個請求的內部客戶端IP地址。 
DNS流量	• Umbrella漫遊客戶端不會干擾DNS查詢，它們會轉到虛擬裝置。 • VA將外部DNS查詢轉送到Umbrella（已加密）。 • VA會根據情況路由內部DNS查詢，並將其轉發到已配置的內部DNS伺服器。
探測消息	Umbrella漫遊客戶端仍然向Umbrella傳送探測消息，但以較低的速率傳送。

如何配置VA回退：

1. 此功能預設啟用，但您可以檢查其狀態（可以選擇將其禁用）
2. 導覽至Identities > Roaming Computers。
3. 按一下(漫遊客戶端設定)圖示。
4. 選擇VA回退選項

Cisco Umbrella AnyConnect漫遊安全模組

Cisco AnyConnect的Umbrella模組支援所有上述相同操作模式。 還提供另外兩種特定的AnyConnect模式。 這兩種模式都可在Identities > Roaming Computers頁面上的Umbrella Dashboard中啟用，但是AnyConnect VPN配置檔案中需要其他配置。

- 請遵守AnyConnect可信網路檢測。
  當Cisco AnyConnect確定Umbrella安全模組位於受信任網路時，此功能會將其禁用。 這依靠AnyConnect的受信任網絡檢測功能來識別網路。 受信任的域、DNS伺服器和URL可用於識別您的公司網路。 有關更多資訊，請參閱AnyConnect文檔。
- 當全通道VPN會話處於活動狀態時，禁用漫遊客戶端
  啟用此功能後，AnyConnect連線到全通道（或全通道DNS）VPN時，Umbrella模組被禁用。

禁用後，漫遊客戶端不會過濾DNS流量，因此確保您的網路受其他安全保護（如我們的網路保護功能）覆蓋非常重要。

更多資訊

如果您希望在公司網路上禁用漫遊客戶端，但需要更多控制，或者希望討論其他選項，請與Cisco Umbrella支援部門聯絡。

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）。