

Umbrella漫遊客戶端的IP層實施功能生命週期結束

目錄

[簡介](#)

[概觀](#)

[補充資訊](#)

簡介

本文檔介紹Cisco Umbrella宣佈IP層實施已於2022年7月31日終止。

概觀

IP層強制是漫遊客戶端的一項可選功能，隨Umbrella智慧代理提供，適用於選定的Cisco Umbrella包。

2021年8月31日及之後客戶訂購的Cisco Umbrella軟體包中不再包含IP層實施。對於以前訂購包含IP層實施選項的軟體包的客戶，該功能將繼續工作到2022年7月31日。運行IP層實施所需的雲端服務已於2022年7月31日關閉。

Cisco Umbrella DNS Essentials和DNS Advantage軟體包提供易於部署、易於管理的強大DNS安全解決方案。這些DNS包繼續保護DNS訂戶，使其免受所有連線的惡意伺服器的侵害，甚至包括解析為惡意IP地址的未知未分類域，這些域以Umbrella DNS請求開頭（通過DNS層實施）。

Cisco Umbrella Secure Internet Gateway(SIG)資料包包括所有流量（DNS、IP、Web等）的更高級安全覆蓋。SIG包括一個用於分析Web埠（IP或域目標）上的所有流量的安全Web網關（「SWG」），以及一個除SWG外還層在基於雲的防火牆上的雲交付防火牆（「CDFW」）。這增強了思科雲安全效力產品組合，遠遠超出採用IP層實施的DNS的範疇，也超出了終端軟體提供多於DNS保護的需求。我們鼓勵需要超過DNS覆蓋的所有人考慮Umbrella SIG包。

使用Cisco Umbrella保護您的網路堆疊，立即與您的Cisco Umbrella客戶經理聯絡，瞭解有關Cisco Secure Internet Gateway解決方案的更多資訊。

補充資訊

AnyConnect版本支援

AnyConnect 4.x版通過IP層實施終止日期支援IP層實施。5.x版不支援IP層實施。思科安全客戶端品牌客戶端不包含IP層實施支援。現有的AnyConnect使用者必須繼續使用AnyConnect 4.x客戶端，以便通過IP層實施終止日期使用IP層實施功能。

思科替代方案

思科安全終端（前身為AMP）提供針對直接IP威脅的裝置內保護。其中包括稱為「DFC」的功能，用於評估新進程的新連線。此功能預計會增長以進一步取代Umbrella IPLE功能。請與您的客戶經理聯絡，討論將Cisco Secure Endpoint新增到ELA的問題。

SIG通過雲防火牆為SWG上的所有Web流量和所有公共Internet流量提供覆蓋。超過95%的IP地址塊是SWG覆蓋的網路流量！（通過TCP 443和80的網路流量）。此功能由SWG提供，不由IPLE供電。

檢視貴組織的IPLE附加值

要按百萬條日誌行計算組織的當前IP層實施塊，請執行以下步驟：

1. 登入到Umbrella Dashboard並開啟Activity Search報告。
2. 導航到「IP Layer Enforcement」日誌型別（從「All」更改）。
3. 匯出1,000,000行的CSV並下載匯出的報告。
4. 過濾掉不包含「Malware」或「Botnet」類別的所有行。
 - 排除「未授權的IP隧道流量」。此類別是指進入IPSec隧道的流量，該流量不是實施清單。它會自動從我們的服務中丟棄。
 - 注意流量埠。埠443和80將完全由我們的SIG Essentials軟體包覆蓋。
5. 塊總數是組織的塊計數。將此項與「總請求數」報告中的總DNS請求數進行比較，以計算有效性的百分比。

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）。