對Umbrella中的非瀏覽器應用程式進行故障排除

目錄

簡介

本檔案介紹如何在Cisco Umbrella中對非瀏覽器應用進行疑難排解。

必要條件

需求

本文件沒有特定需求。

採用元件

本檔案中的資訊是根據Cisco Umbrella。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

概觀

本文說明配置非瀏覽器應用程式以與Umbrella安全Web網關一起運行的最佳實踐和故障排除步驟。在大多數情況下，不需要更改配置。但是，某些應用程式在安全/檢查功能（如SSL解密）上無法正常工作，必須新增例外才能使應用程式通過Web代理運行。這適用於Umbrella SWG及其他Web代理解決方案。

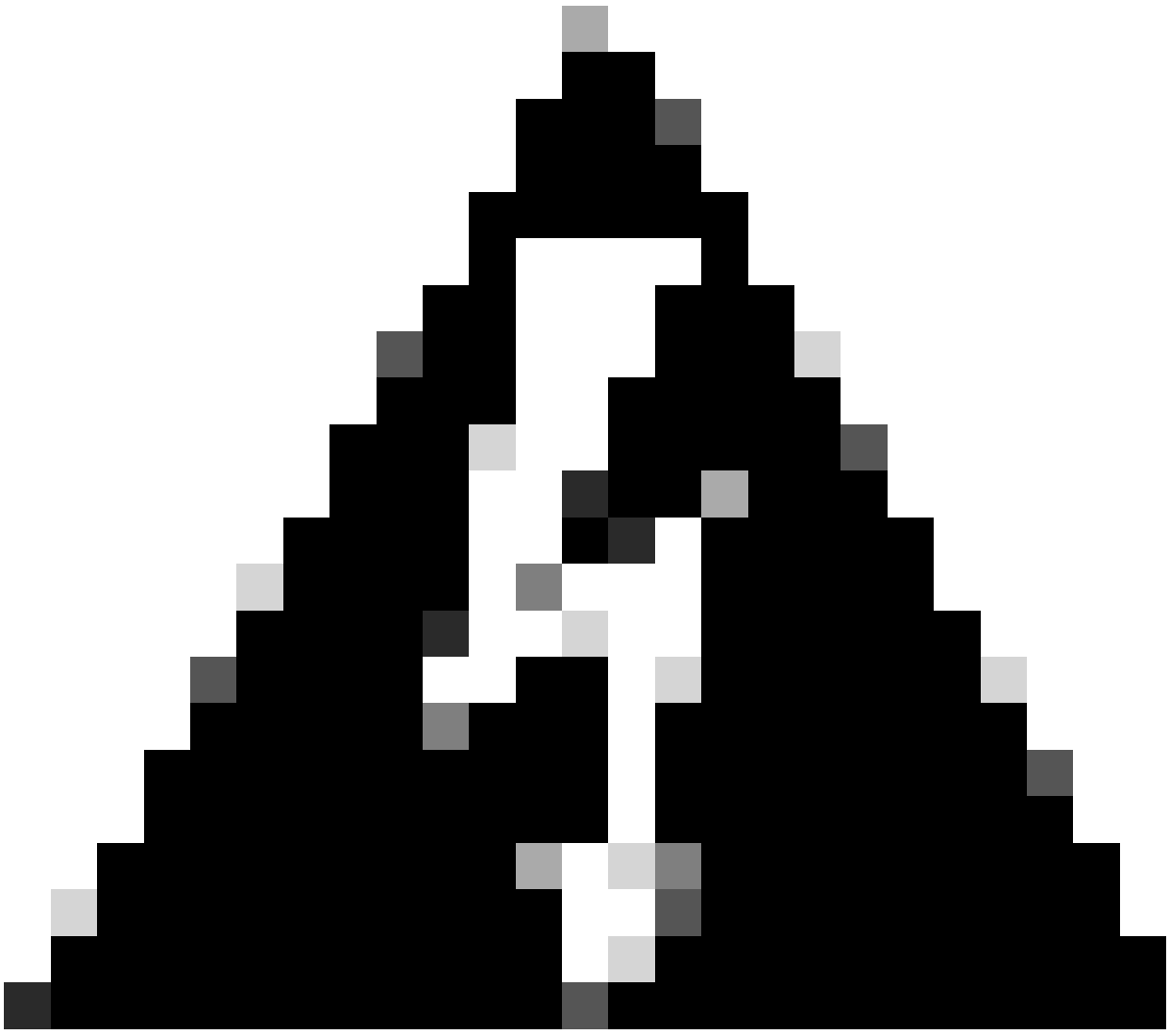
當應用程式的網站/瀏覽器版本工作正常，但應用程式的案頭/移動版本不工作時，該選項很有用。

相容性問題

應用程式可能因以下原因不相容：

Umbrella根CA安裝	Cisco Umbrella根CA必須始終受信任才能進行無錯誤的TLS連線。 • 解決方案：對於非Web應用程式，請確保Cisco Umbrella Root CA在系統/本地電腦證書儲存中受信任。
證書固定	證書固定(PKP)是應用程式期望接收精確的枝葉（或CA證書）以驗證TLS握手時。 應用程式無法接受Web代理生成的證書，並且與SSL解密功能不相容。 • 解決方案：使用選擇性解密清單繞過來自SSL解密的應用程式或域(請參閱表後的警告) 有關已知受證書固定影響的應用程式的更多詳細資訊，請點選此處： 公鑰固定/證書固定
TLS版本支援	應用程式可以使用較舊的TLS版本/密碼，出於安全原因，SWG不支援該版本/密碼。 • 解決方案：使用外部域功能(PAC/AnyConnect)或VPN排除（隧道）繞過將流量傳送到Umbrella(請參閱表後的警告)。
非Web協定	某些應用程式使用非http(s)協定，但仍會通過SWG截獲的常見Web埠傳送此資料。SWG無法理解此流量。 • 解決方案：請諮詢應用程式供應商，以確定軟體使用的目標地址/IP範圍。 需要使用外部域(PAC/AnyConnect)或VPN排除（隧道）將此軟體從SWG中排除(請參閱表後的警告)。
SAML身份驗證	大多數非瀏覽器應用程式無法執行SAML身份驗證。 Umbrella不會對SAML的非瀏覽器應用程式發起質詢，因此基於使用者/組的過濾策略無法匹配。 • 解決方案： 啟用IP代理功能，以便可以快取使用者資訊以用於非瀏覽器應用程式。 • 備選: 允許基於網路或隧道身份(不是使用者/組)的Web規則中的應用程式/域。
HTTP範圍請求	有些應用程式在下載資料時使用HTTP「位元組範圍」請求；意味著一次只能下載一小部分檔案。由於安全原因，在SWG中禁用這些請求，因為也可以使用此技術繞過防病毒檢測。 • 解決方案(HTTPS):使用選擇性解密清單繞過Umbrella中的SSL Decryption*應用或域。

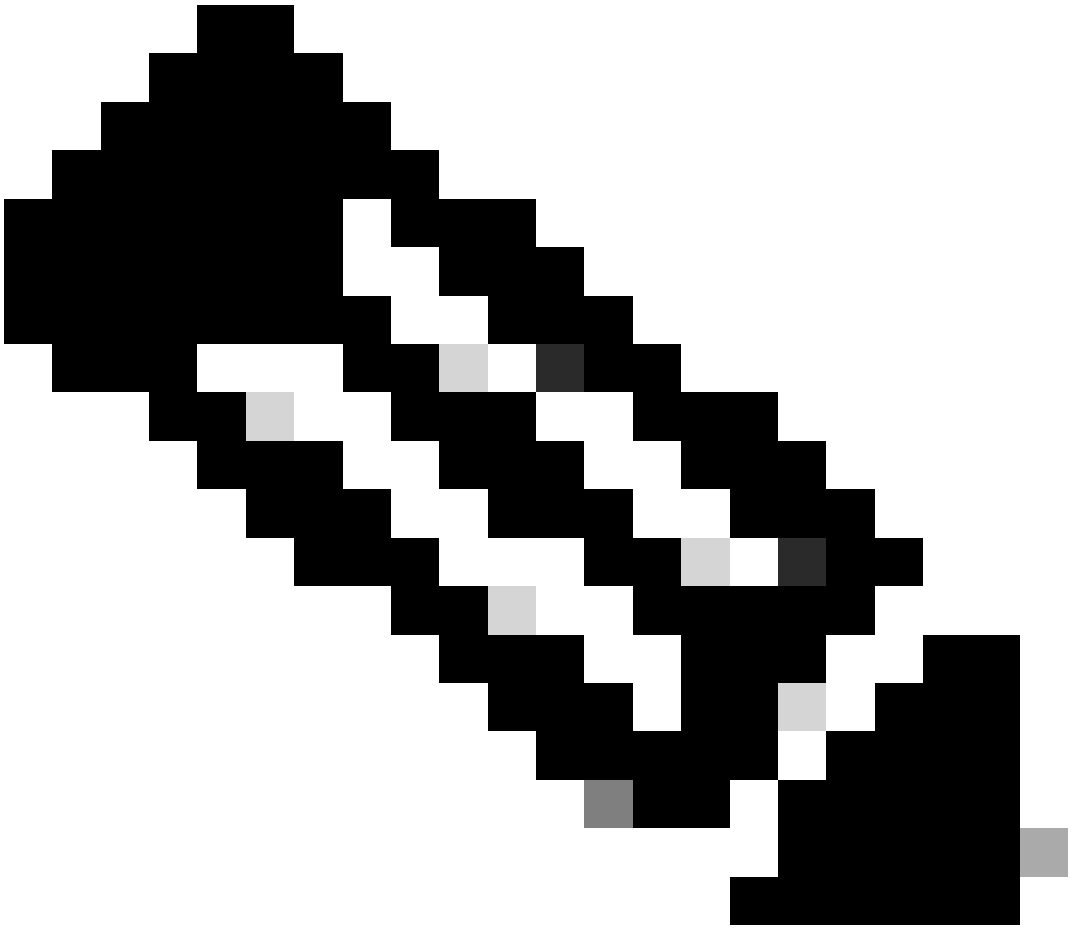
	• 解決方案(HTTP): 使用帶有Override Security選項的Web規則繞過防病毒掃描*中的應用程式或域。 • 備選: 如果您希望為您的組織預設啟用*範圍請求，請與Umbrella支援聯絡。
顯式代理相容性	某些應用程式不考慮系統代理設定(例如，PAC檔案)，並且通常與顯式Web代理不相容。在PAC檔案部署中，這些應用程式不通過Umbrella SWG路由。 • 解決方案：必須通過本地網路防火牆允許該應用。 有關允許的目標/埠的詳細資訊，請諮詢應用程式供應商。



警告：建立這些例外可以禁用安全檢查功能，包括防病毒掃描、DLP掃描、租戶控制、檔案型別控制和URL檢查。 只有在您願意信任這些檔案的源時才能執行此操作。必須權衡應用程式的業務需求與禁用這些功能的安全影響。

Microsoft 365應用程式

Microsoft 365相容性功能自動將許多Microsoft域從SSL解密和策略實施功能中排除。可以啟用此功能以解決案頭版本的Microsoft應用的問題。 有關詳細資訊，請參閱管理全域性設定。

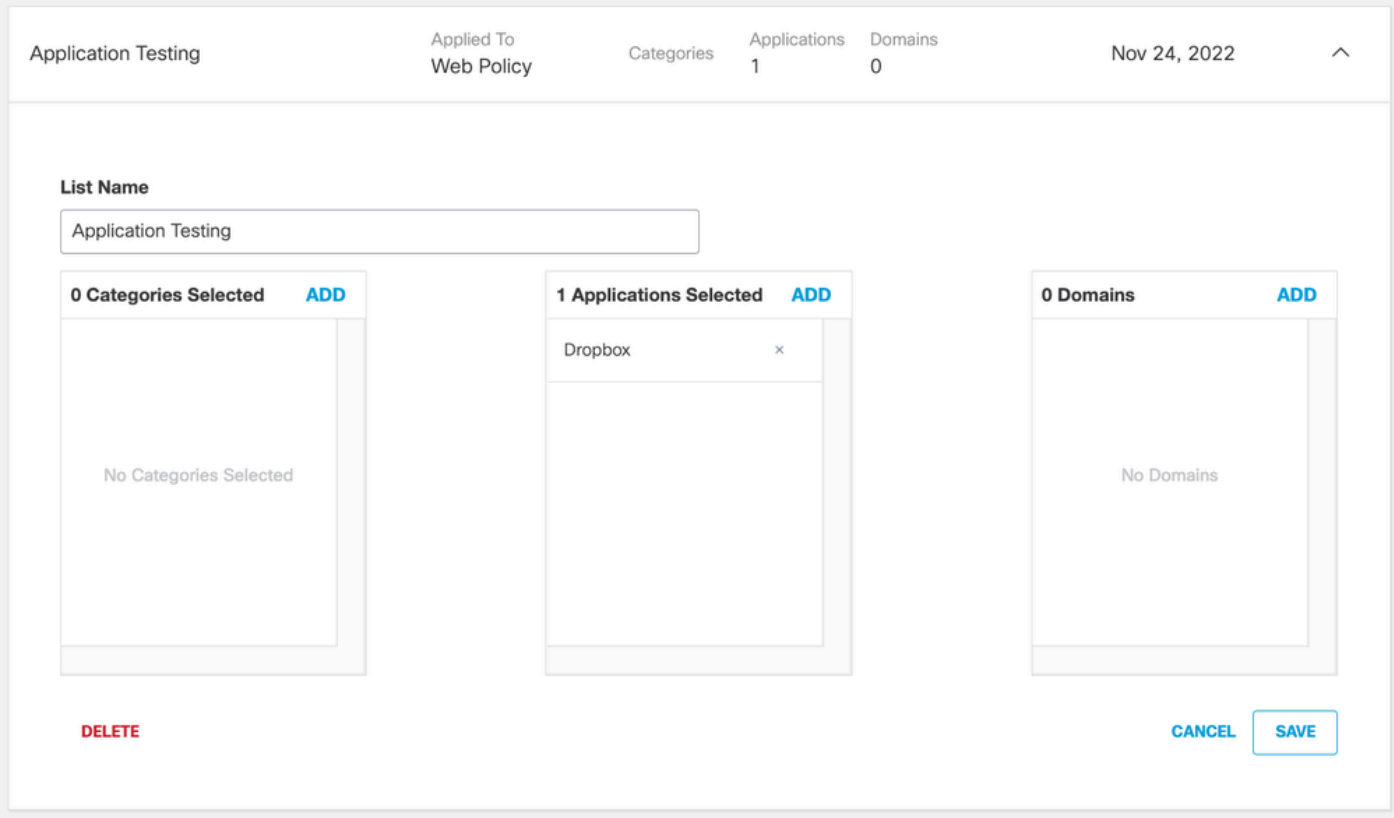


附註：Microsoft 365相容性功能並不排除所有Microsoft域。 Umbrella使用Microsoft對必須排除在過濾之外的域清單的建議。有關詳細資訊，請參閱新建Office365終結點類別。

證書固定繞過

證書固定(PKP)是應用相容性問題的常見原因。 思科提供可配置為繞過SSL解密來應對的命名應用的綜合清單。選擇性解密可在Policies > Selective Decryption Lists中設定。

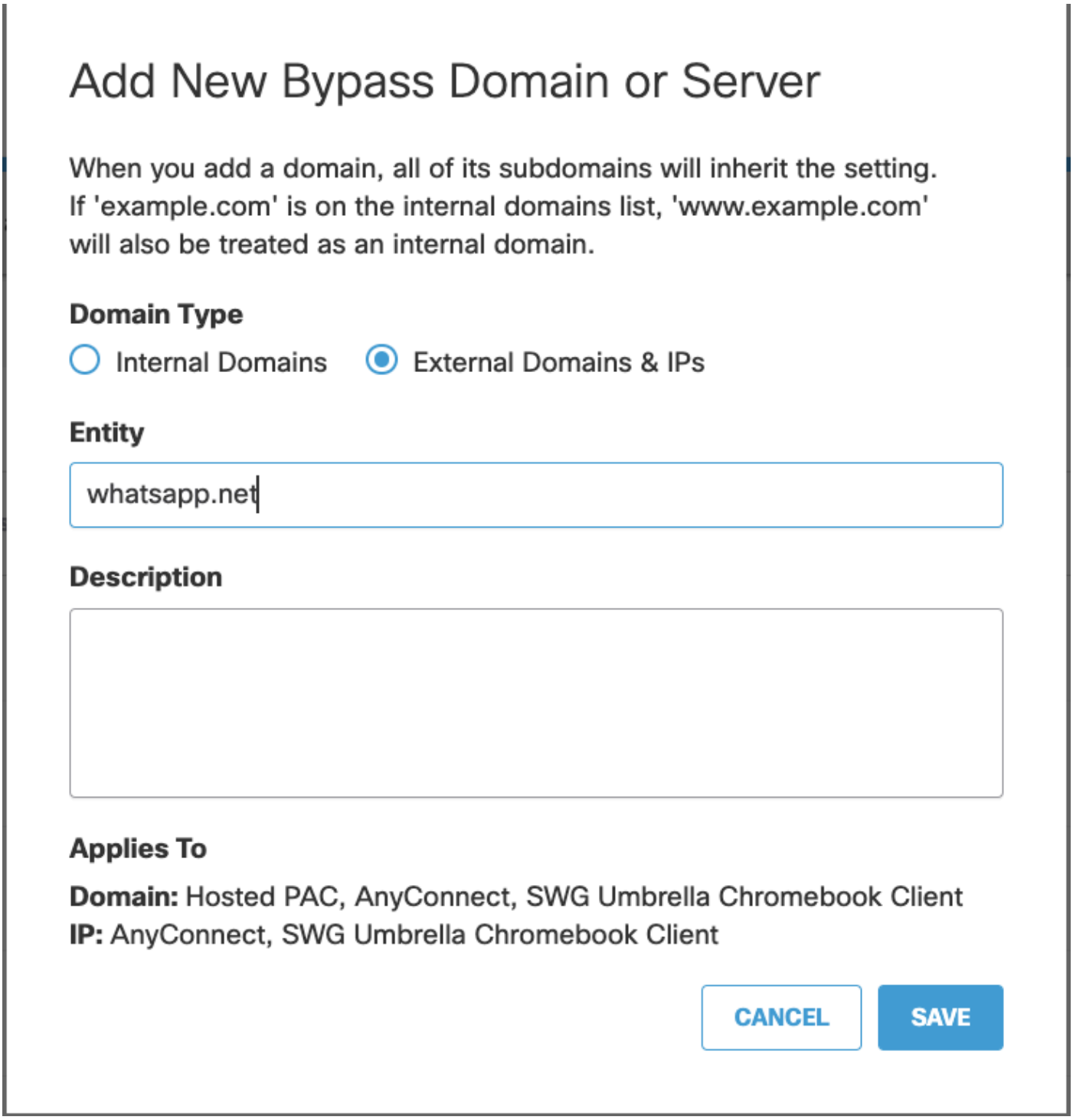
在大多數情況下，管理員只需通過按應用程式名稱排除該應用程式即可解決證書固定問題。這意味著，無需學習或維護域清單即可解決這些問題。



或者，可以根據目標域/IP地址繞過應用程式。請與應用程式供應商聯絡以確定適用的域/IP清單，或參閱識別證書固定例外項。

TLS相容性繞過

傳統或自定義TLS版本是應用程式相容性問題的常見原因。這些問題可通過在部署>域管理>外部域和IP中排除來自Umbrella的流量來解決。在隧道部署中，只能通過在VPN配置中新增例外來排除流量。



與應用程式供應商聯絡以確定要排除的域/IP的適用清單，或檢視「識別不相容TLS版本的排除」（本文稍後部分）。

疑難排解（高級）

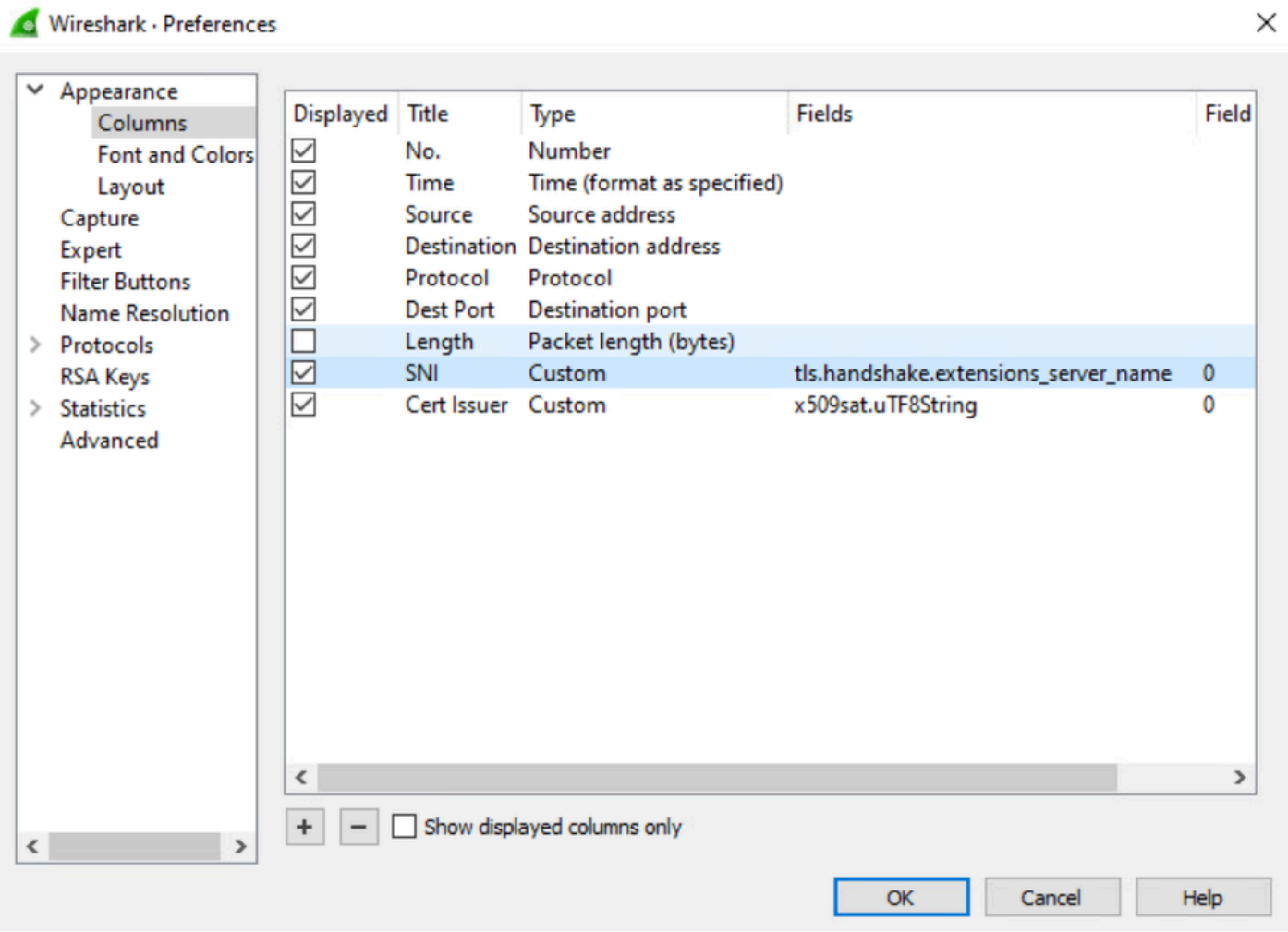
本文中的其餘說明使用Wireshark(www.wireshark.org)資料包捕獲進行故障排除。Wireshark可幫助確定應用程式使用哪些域來幫助實施自定義排除。開始之前，請在Wireshark中新增以下自定義列：

1.從www.wireshark.org下載Wireshark。

2.轉至「編輯」>「首選項」>「列」。

3.使用以下欄位建立Custom型別的列：

```
http.host
tls.handshake.extensions_server_name
x509sat.uTF8String
```



要執行資料包捕獲，請完成以下說明或參閱Capture Network Traffic with Wireshark。

1.以管理員身份運行Wireshark。

2.在Capture > Options（捕獲>選項）中選擇相關的網路介面。

- 對於PAC/隧道部署，請在正常的LAN網路介面上捕獲。
- 對於AnyConnect部署，捕獲您的LAN網路介面和環回介面。

3.關閉除問題應用程式之外的所有其他應用程式。

4.刷新DNS快取：`ipconfig /flushdns`

5.啟動Wireshark捕獲。

6.快速複製問題並停止Wireshark捕獲。

識別證書固定例外項

在客戶端上強制實施證書固定，這意味著每個應用程式的準確行為和解決步驟不同。在capture輸出中，尋找TLS連線發生故障的跡象：

- TLS連線正在快速關閉或重置（RST或FIN）。
- 正在重複重試TLS連線。
- TLS連線的證書由Cisco Umbrella頒發，因此正在解密。

以下示例Wireshark過濾器可幫助檢視TLS連線的重要詳細資訊。

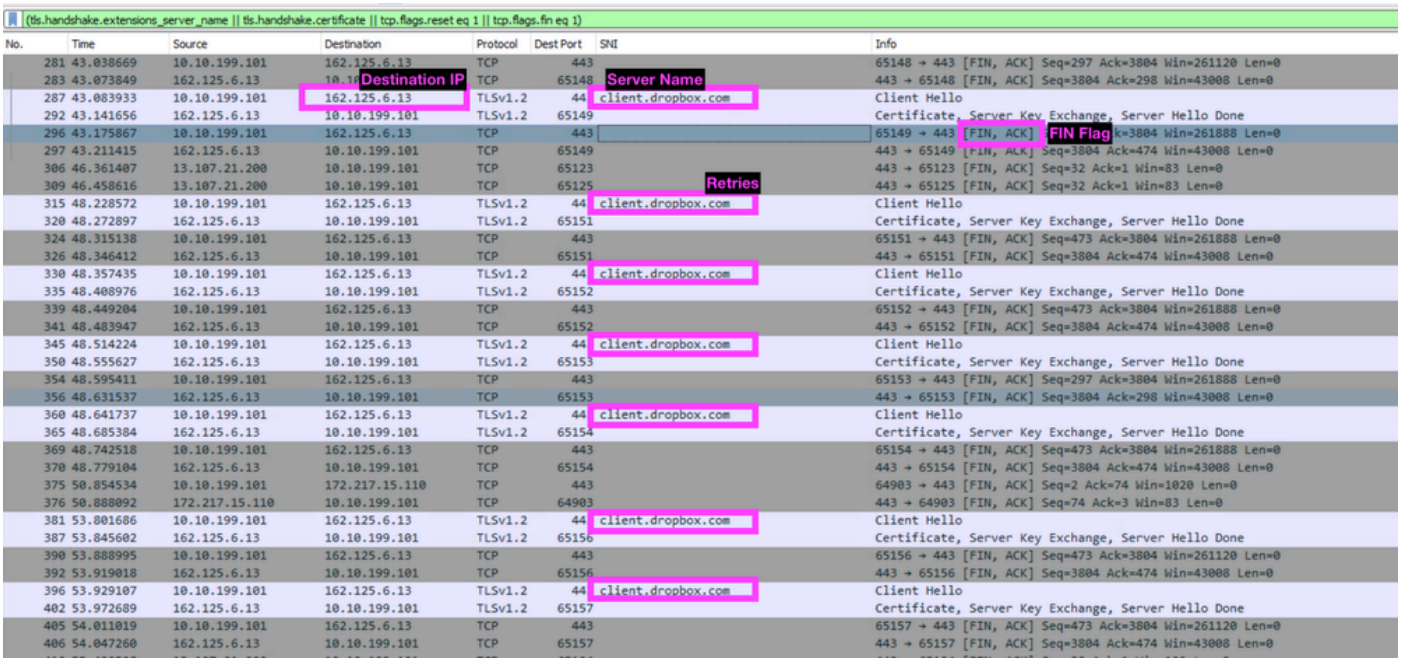
通道/AnyConnect

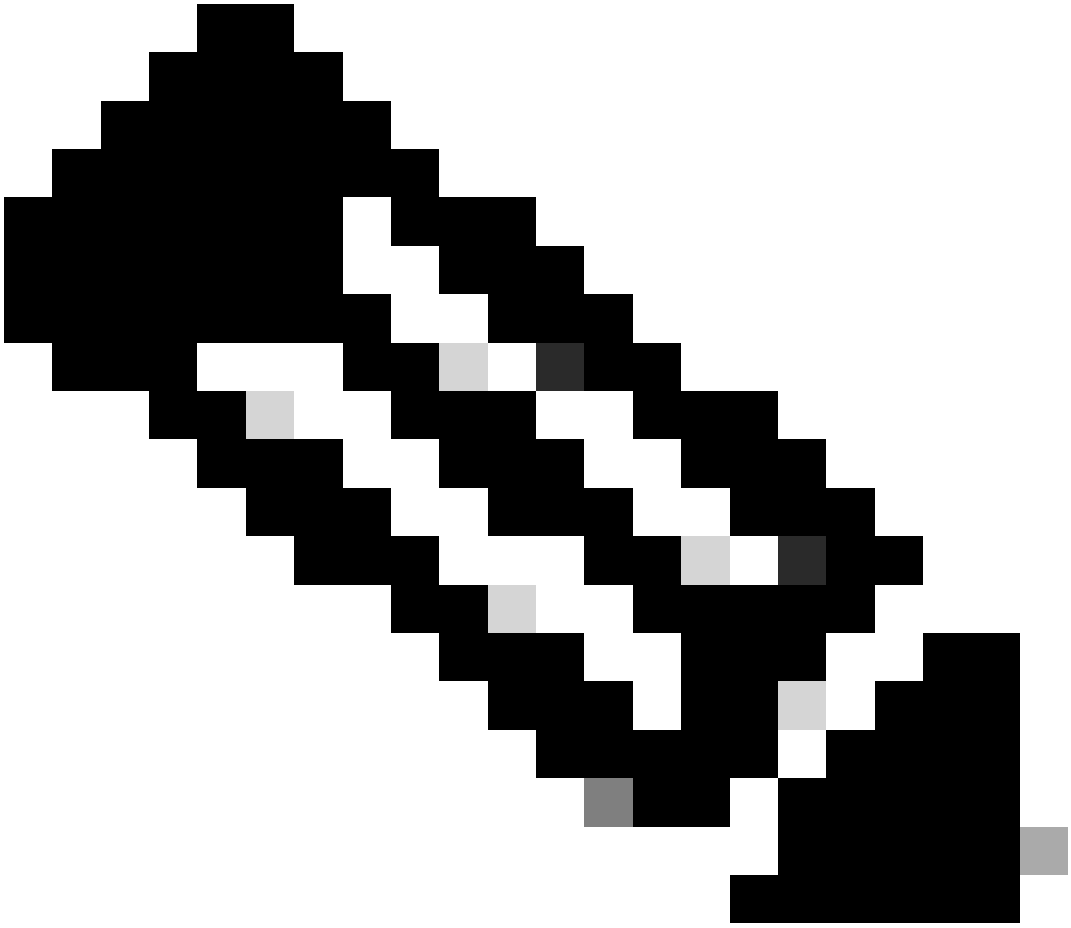
```
tcp.port eq 443 && (tls.handshake.extensions_server_name || tls.handshake.certificate || tcp.flags.rese
```

PAC/代理連結

```
tcp.port eq 443 && (http.request.method eq CONNECT || tcp.flags.reset eq 1)
```

在本示例中，嘗試連線到client.dropbox.com時，DropBox案頭應用程式受證書固定的影響。





附註：新增必要的排除項後，您可以多次重複這些步驟，以確定應用程式使用的所有目標。

識別不相容的TLS版本的排除

查詢不使用Umbrella SWG支援的強制TLS1.2+協定的SSL/TLS連線。這可以包括傳統協定（TLS1.0或更低版本）或由應用程式實施的定製協定。

此示例過濾器顯示初始TLS握手資料包以及DNS查詢。

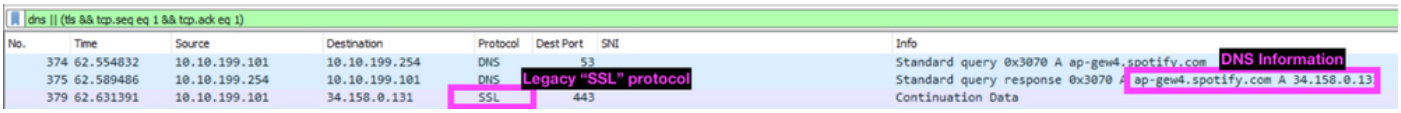
通道/AnyConnect

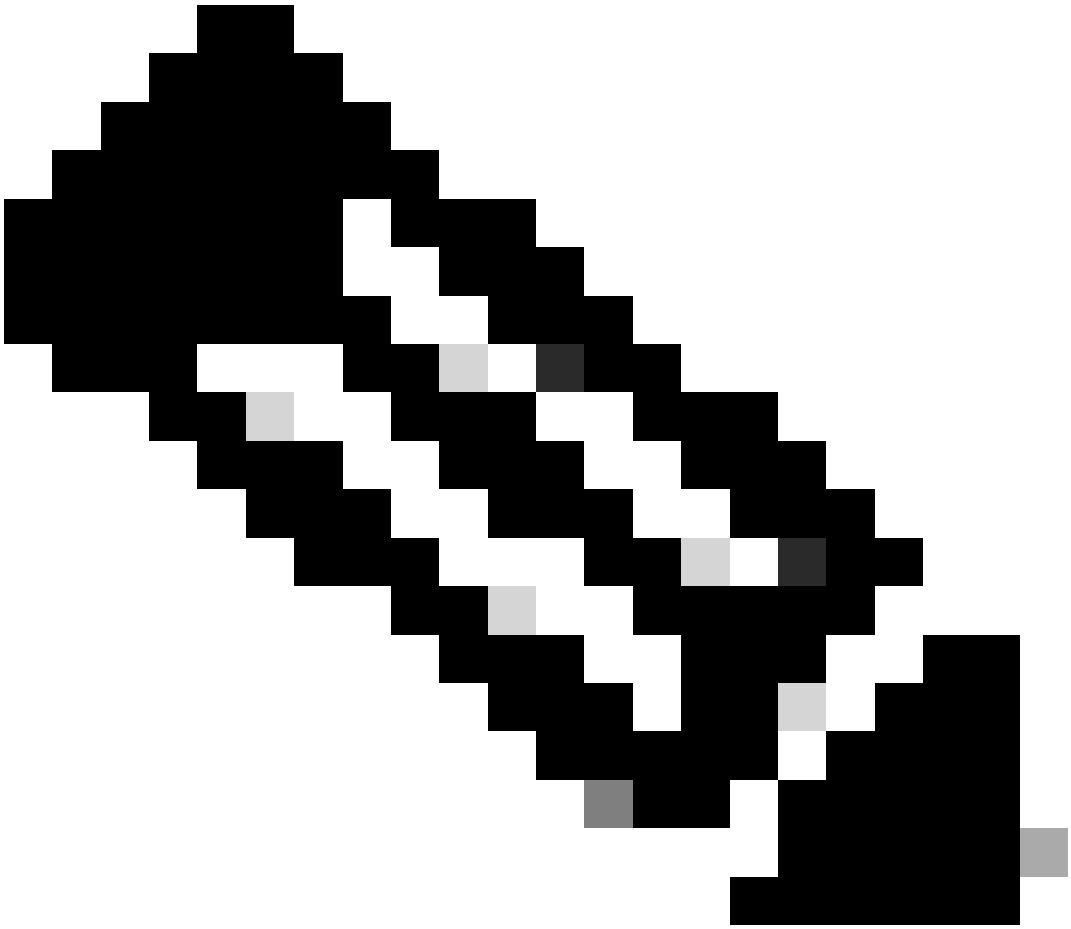
```
dns || (tls && tcp.seq eq 1 && tcp.ack eq 1)
```

PAC/代理連結

```
dns || http.request.method eq CONNECT
```

在本示例中，Spotify案頭應用程式正在嘗試使用無法通過SWG傳送的非標準或傳統「SSL」協定連線到ap-gew4.spotify.com。





附註：新增必要的排除項後，您可以多次重複這些步驟，以確定應用程式使用的所有目標。

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）。