

對Umbrella安全Web網關上的516個錯誤進行故障排除

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[概觀](#)

[516錯誤背景](#)

[Chrome行為更改](#)

[確定錯誤源](#)

[因應措施](#)

[516錯誤和電子郵件系統](#)

簡介

本文檔介紹如何對Umbrella安全Web網關上增加516個錯誤進行故障排除。

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Umbrella安全Web閘道(SWG)。

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

使用HTTPS檢查瀏覽Umbrella Secure Web Gateway(SWG)代理的使用者可以從2023年10月下半年開始更頻繁地接收516 Upstream Certificate CN Mismatch錯誤頁面。

當網站的證書與客戶端用於訪問網站的域名不匹配時，就會出現516錯誤頁面。

錯誤頁面增加是由於Chrome瀏覽器對使用HTTP (未加密) 方案的URL請求的處理發生變化。Chrome現在會嘗試先使用HTTPS (加密) 方案載入資源。當配置為[HTTPS檢查](#)時，SWG檢查網站的證書，如果證書不可接受，則返回顯示錯誤代碼 (例如516) 的網頁。

要解決此問題，客戶可以配置其Web策略以繞過HTTPS檢查請求，否則會導致516個錯誤。

516錯誤背景

簡而言之，當用於通過HTTPS訪問網站的域名沒有出現在伺服器的數位證書中時，Umbrella安全Web網關會返回516錯誤頁面。有關描述安全Web網關返回516錯誤頁原因的其他資訊，請參閱Umbrella知識庫文章「516 Upstream Certificate CN Mismatch」錯誤。

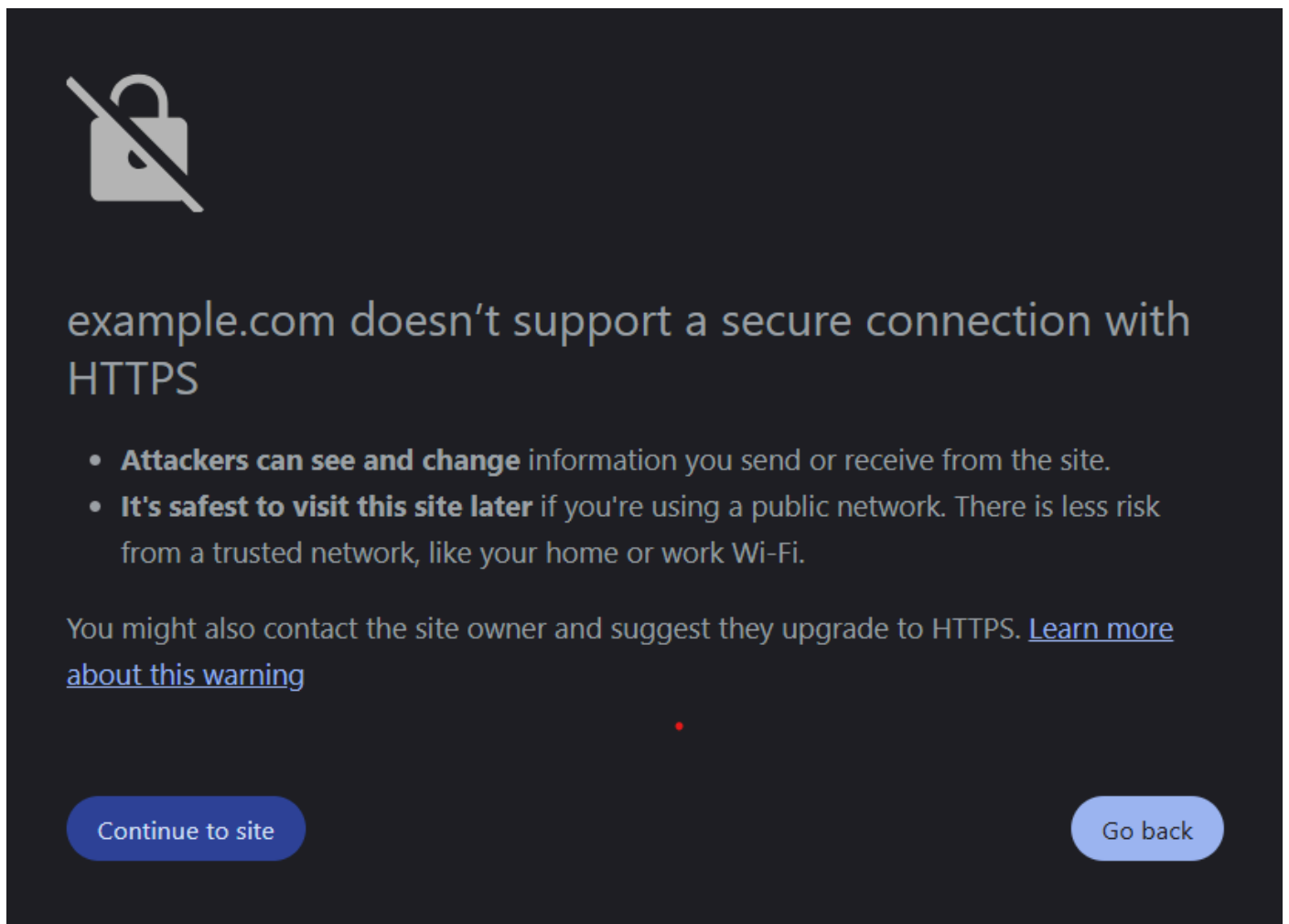
例如，假設一個網站以以下形式提供HTTP URL中的內容

：http://www.example.com/path_to_content。如果使用者要求等效HTTPS URL，但網站沒有其SAN與www.example.com相符的憑證(或許SAN僅與example.com相符合)，則如果要求由Umbrella的安全Web網關使用使用SWG的HTTPS檢查功能的Web原則處理，使用者會收到516錯誤。

Chrome行為更改

2023年10月下半月，Google完成了Chrome瀏覽器新功能的推出。在該日期之後，使用該URL的HTTPS版本自動請求該HTTP URL。例如，當使用者請求<http://www.example.com>時，Chrome會首先嘗試使用<https://www.example.com>完成請求。

如果Chrome在請求HTTPS URL時收到與HTTPS相關的錯誤，則Chrome會嘗試通過HTTP載入相同的內容。如果對HTTP URL的請求成功，Chrome會顯示一個包含文本指示站點不安全的註釋頁面和一個連結，使用者可以通過該連結繼續下面的影象。



這是Chrome新功能中的後備行為。

但是，當使用HTTPS檢查通過SWG瀏覽時，如果HTTPS請求從站點產生與HTTPS相關的錯誤（如「ERR_CERT_COMMON_NAME_INVALID」），SWG會攔截該錯誤，並將SWG錯誤頁面返回到Chrome（如516錯誤頁面）。Chrome不會將此SWG內容視為與HTTPS相關的錯誤，因此不會產生回退行為，並且會顯示SWG錯誤頁面，而不是前一影像中的頁面。

有關新Chrome行為的更多資訊，請參閱[Chromium](#) 部落格和該功能的[GitHub儲存庫](#)。

確定錯誤源

現在Chrome自動將HTTP URL提升為HTTPS URL，使用者會更頻繁地看到產生516個錯誤的網站。

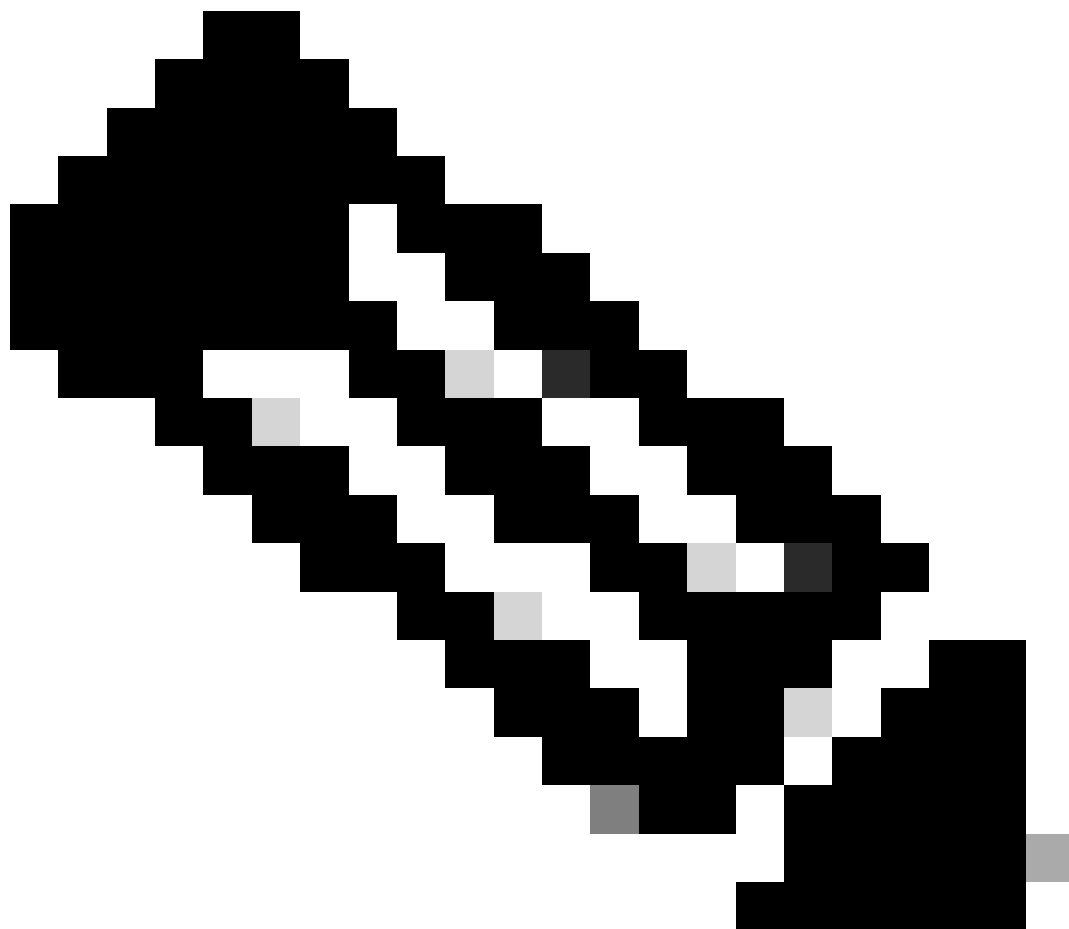
要確認網站是否導致HTTPS相關錯誤（如516響應），請從未使用Umbrella的案頭系統中使用Chrome瀏覽該網站。請務必在Chrome的Omnibox（類似位址列）中手動顯式輸入HTTPS版本的URL，而不是按一下HTTP超連結。如果超連結在SWG中生成516錯誤，則手動在Chrome中請求不帶SWG的HTTPS URL會生成錯誤消息「ERR_CERT_COMMON_NAME_INVALID」。此錯誤消息確認此問題是用於訪問網站的域名的錯誤證書。

或者，使用[Qualys SSL Server Test](#)站點等線上工具診斷網站問題。

因應措施

Umbrella管理員可以使用以下選項之一解決此問題：

1. 為這些站點[建立特定](#)的目標清單，並將該清單新增到無[HTTPS檢查](#)的[Web策略](#)。
2. 建立產生516個錯誤頁面的站點的選擇性解密清單，並將選擇性解密清單添加到所有相關的Web策略



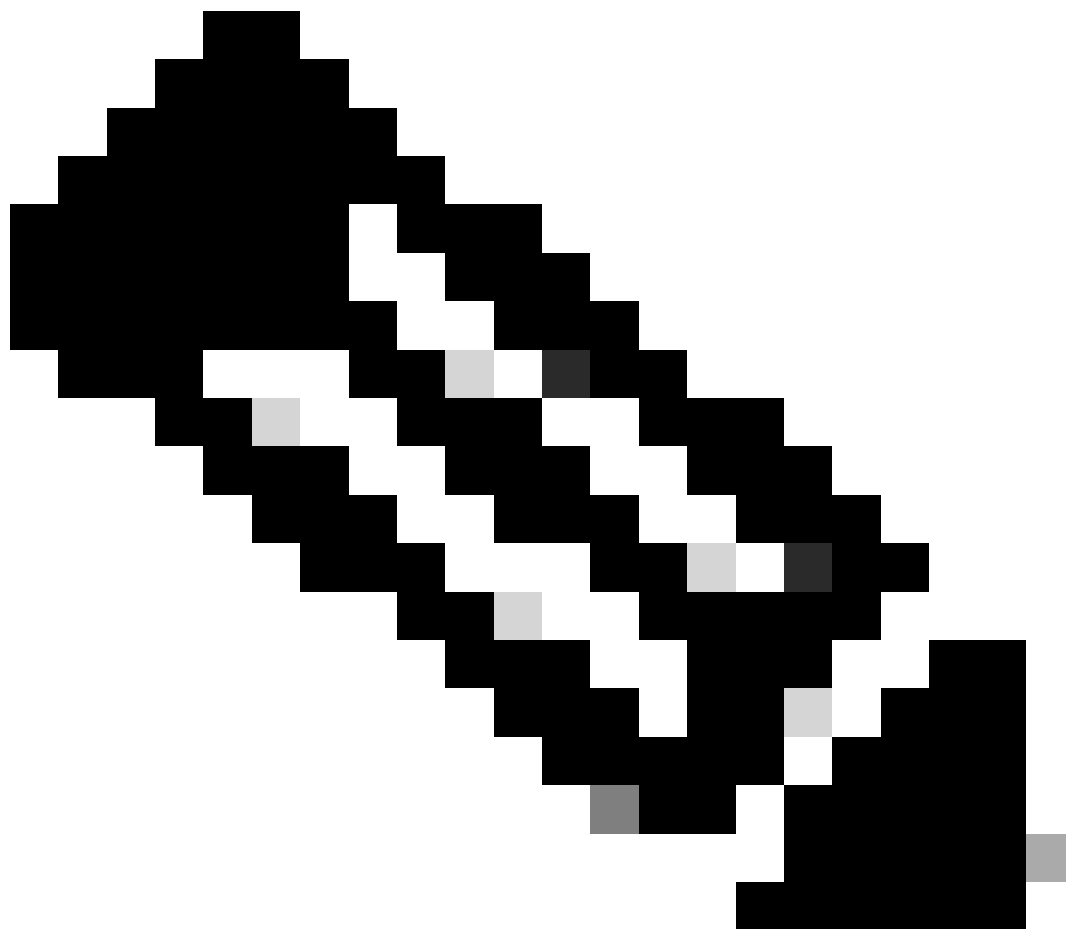
附註：HTTP重定向或郵件安全系統等用其服務的HTTPS URL代替原始HTTP URL的因素可能會掩蓋所需的域名。識別目標清單或選擇性解密清單的正確域名可能需要調查，包括使用特定工具（捲曲、Chrome開發人員工具、電子郵件安全供應商日誌等）。

516錯誤和電子郵件系統

如果電子郵件系統以HTML格式顯示電子郵件並允許電子郵件中的超連結，則會導致516錯誤頻率增加。撰寫電子郵件時，如果發件人鍵入域名或將域名貼上到電子郵件正文中，許多電子郵件系統會自動將純文字檔案域名提升為超連結。通常，建立連結時，方案是HTTP而不是HTTPS。

例如，在電子郵件中鍵入字串example.com可生成包含HTML代碼[\(顯示為超連結www.example.com\)](http://www.example.com)的電子郵件。

如果此類電子郵件的收件人按一下該HTTP超連結，則如果按一下開啟Chrome或者已經使用Chrome檢視電子郵件，則請求最初使用HTTPS。



附註：其他瀏覽器也可以將HTTP提升為HTTPS。

此外，故意使用HTTP方案的電子郵件中的超連結也會以類似方式處理。

一些常見的雲服務會通過HTTP超連結而不是HTTPS超連結傳送來自第三方事務性電子郵件服務提供商的電子郵件。Chrome自動嘗試載入的HTTPS站點可能會以證書錯誤響應電子郵件連結中的域名，如本例中[的Seegrid中的。](#)

當這些電子郵件具有大的收件人清單時，許多通過SWG傳送其點選（或請求）的使用者可能會報告錯誤，如516錯誤。請聯絡您的電子郵件服務提供商或傳送電子郵件的組織，以糾正證書錯誤。

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）。