解決516上游證書CN不匹配錯誤

目錄

簡介

本文說明如何解決516上游證書CN不匹配錯誤。

問題

當Umbrella安全Web閘道(SWG)代理設定為執行HTTPS檢查時，使用者在使用HTTPS URL瀏覽網站時可能會收到516 Upstream Certificate CN Mismatch錯誤頁面。

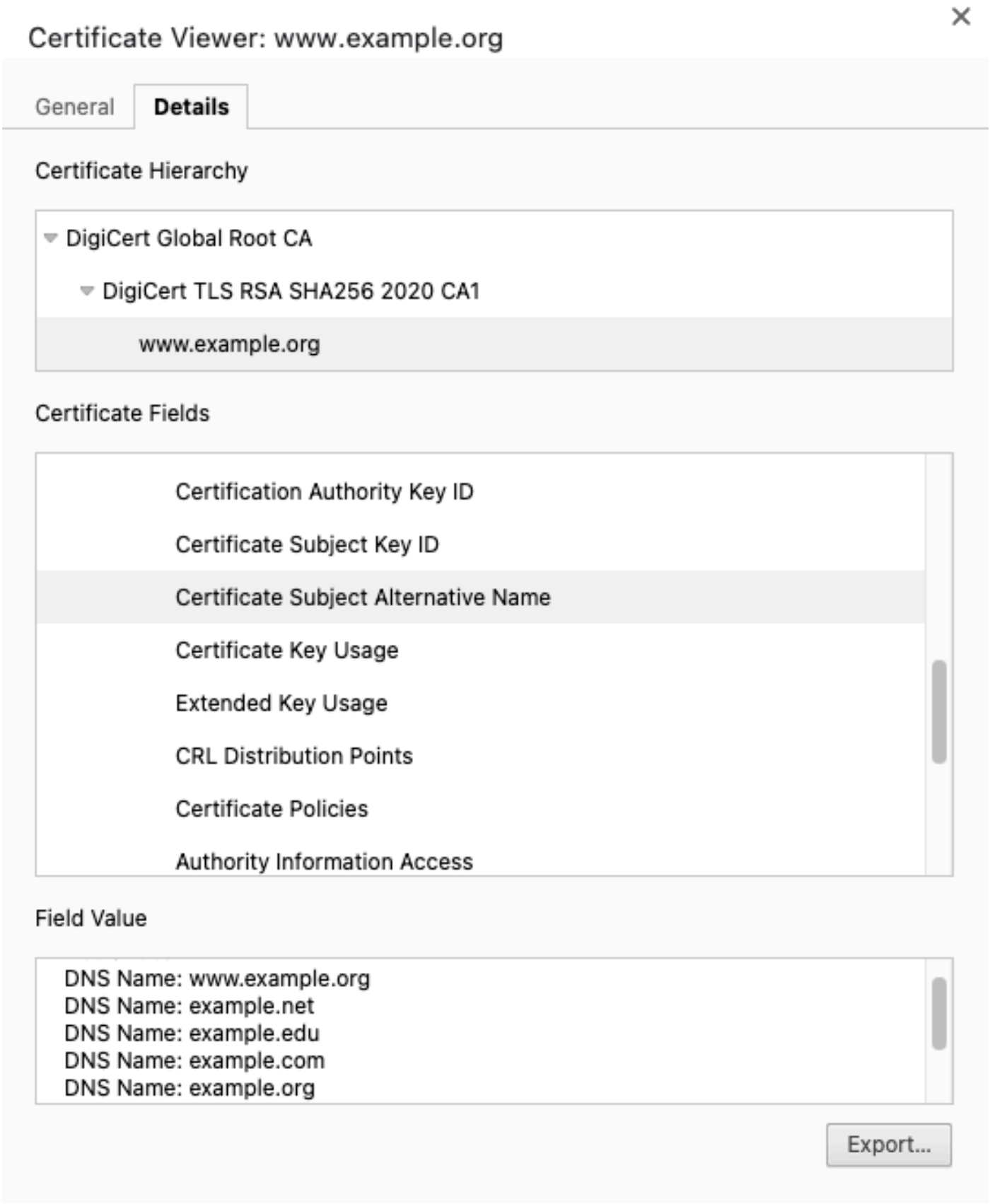
此錯誤並不表示網站憑證的「Subject」欄位中的一般名稱(CN)屬性存在問題。相反，此問題涉及證書的使用者替代名稱(SAN)擴展中的DNS名稱屬性。

檢視本文後，如果您無法確定516錯誤頁的原因，請聯絡Umbrella技術支援，並向我們提供本文檔中證書身份錯誤部分中指定的資訊。

憑證身分識別機制

當請求HTTPS URL時，瀏覽器或其他Web客戶端通過TLS協商的Client Hello消息中的Server Name Indication(SNI)擴展將URL中的域名傳送到Web伺服器。伺服器使用此SNI值選擇返回客戶端的伺服器證書，因為伺服器通常託管多個網站，並且對於某些站點或所有站點可能具有不同的證書。

當Web客戶端接收到伺服器證書時，客戶端通過比較請求的域名與證書的Subject Alternative Names擴展的DNS Name屬性中的域名，來驗證證書是否是請求的正確證書。此圖顯示了伺服器證書中的這些SAN。



16796247745556

此Web伺服器返回此證書，以響應具有這些SNI值的請求以及欄位值面板中不可見的其他請求：

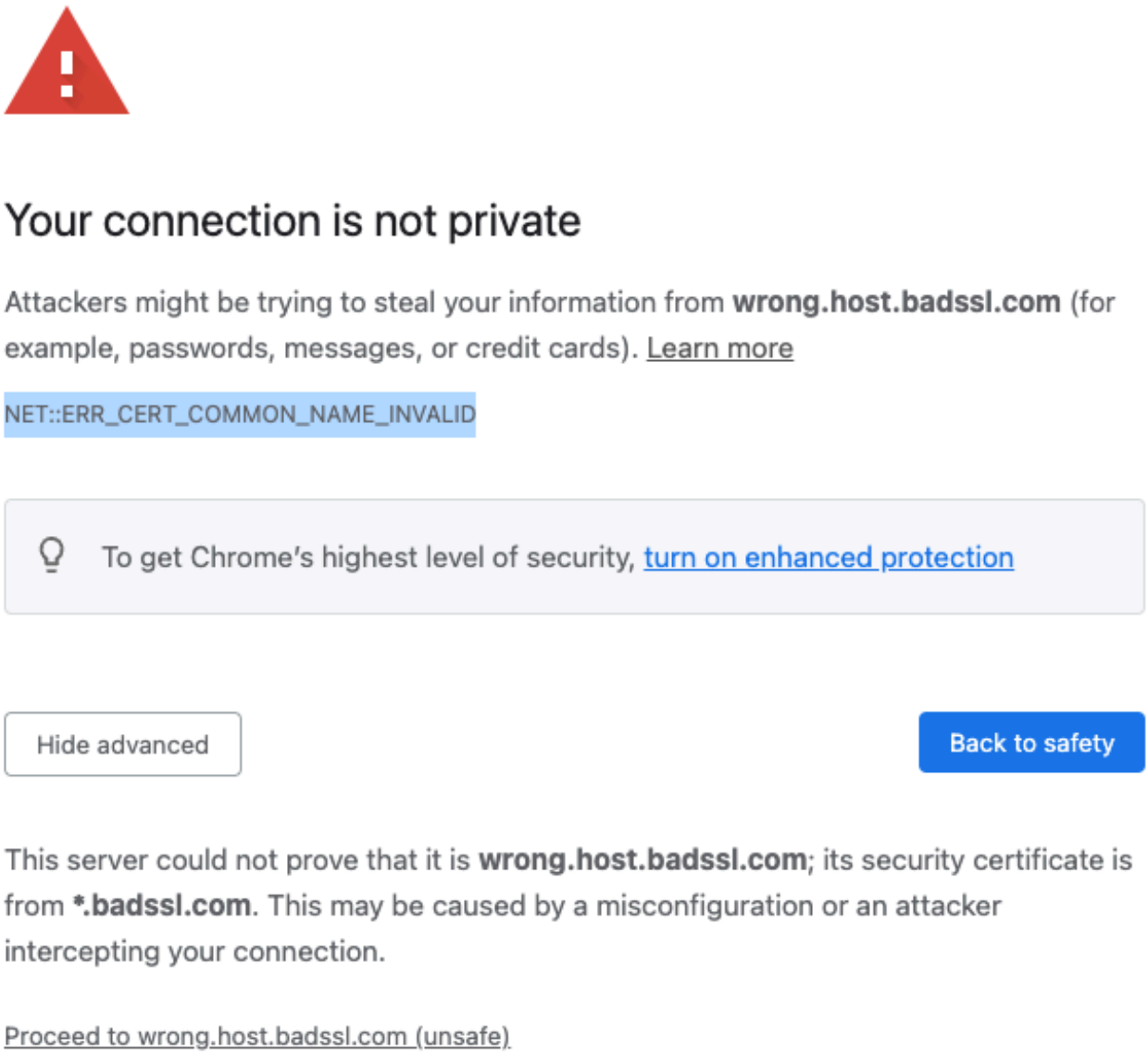
- www.example.org
- example.net

- example.edu
- example.com
- example.org

請注意，SAN "example.com"與"www.example.com"的SNI不匹配。 但是，「*.example.com」的萬用字元SAN將匹配「www.example.com」的SNI，或包含單個標籤（不帶「。」的字串）的任何其他域名。 字元)字首example.com，但不包含多個標籤。例如，「www.hr.example.com」與「*.example.com」不匹配，因為「www.hr」由兩個標籤組成：「www」和「hr」。單個萬用字元只能匹配單個標籤。

證書標識錯誤

當Web客戶端收到伺服器證書時，如果SAN的DNS名稱與所請求的URL中的域名中的SNI不匹配，則Web客戶端通常會向使用者顯示錯誤。此圖顯示Chrome顯示「NET::ERR_CERT_COMMON_NAME_INVALID」間隙頁。



16794294817428

在映像中，請求的站點為「https://wrong.host.badssl.com」，該站點與任何SAN都不匹配。證書包含一個萬用字元SAN DNS名稱「*.badssl.com」，其萬用字元只能與單個標籤（如「host」）匹配。 此外，憑證沒有具有準確值「wrong.host.badssl.com」的SAN DNS名稱或萬用字元SAN*.host.badssl.com，因此使用者看到此錯誤。

要確定證書標識不匹配的原因，請使用瀏覽器的證書檢視功能檢查證書的SAN DNS名稱，並與所請求的URL中的域名進行比較。或者，也可以使用Qualys SSL Server Test等工具來診斷證書標識問題。

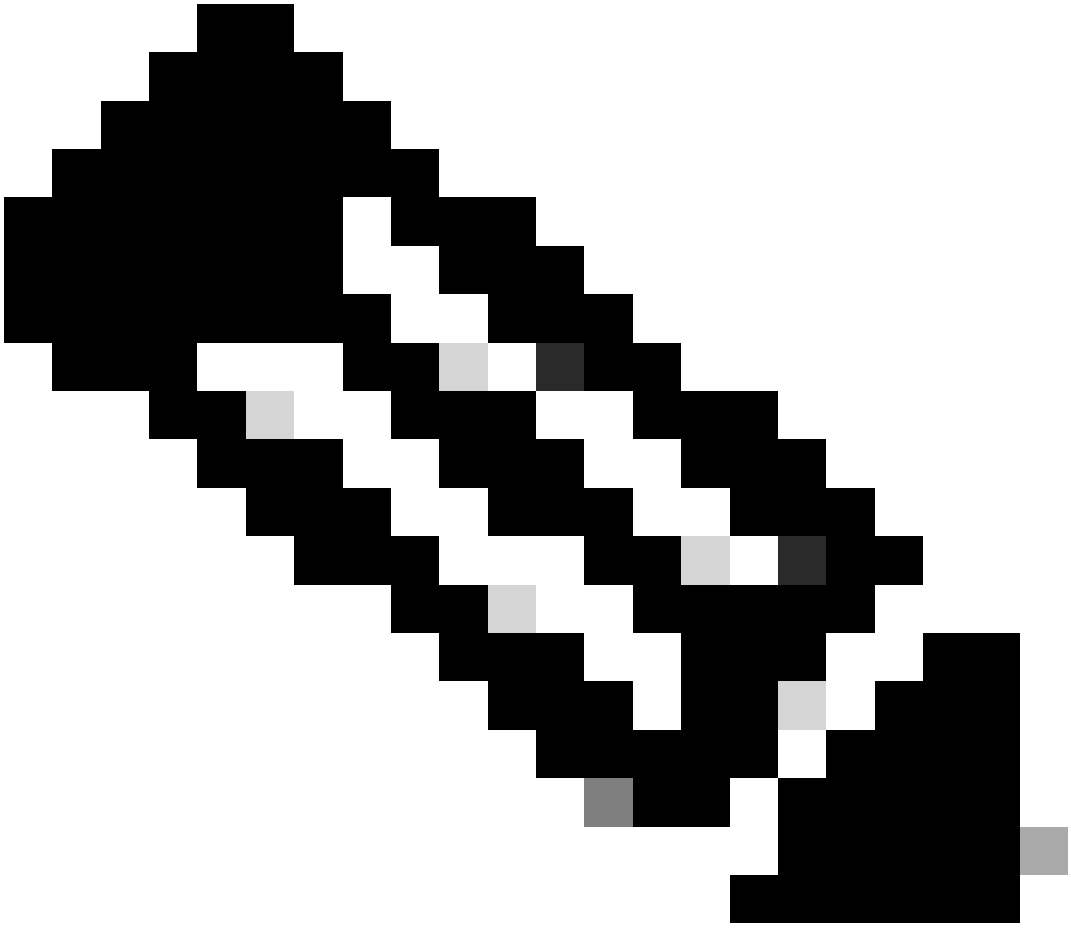
如果在使用本節中的資訊後無法確定516錯誤的原因，或者無法使用下一部分中的解決方案和解決方法，請用Umbrella技術支援開啟一個案例並提供：

1. 截圖
    - 顯示所請求的URL的瀏覽器位址列
    - 整個516錯誤頁面（請參見下一節中的影象）
2. 從位址列複製的URL文本

解析

要解決此問題，請使用與證書中的某個SAN DNS名稱匹配的域名訪問伺服器。這可能要求網站管理員將匹配的域名新增到區域的DNS中。或者，管理員可以重新頒發證書，以將URL的域名包含在一個SAN DNS名稱中。

作為解決方法，可以將URL的域名新增到安全Web網關代理的選擇性解密清單或智慧代理中的目標清單。將清單應用於適當的Web策略規則集設定（安全Web網關）或DNS策略允許清單（智慧代理）。 這阻止了對該網站的請求被代理解密，從而阻止代理顯示516錯誤頁面。



附註：不支援同時使用安全Web網關代理和智慧代理。每個組織只能採用一種代理技術。建議訂用安全Web網關的組織使用SWG，而不使用智慧代理。

公用名已棄用

Web使用者端最初將所請求URL中的網域名稱與憑證的「Subject」欄位中的「Common Name(CN)」屬性進行匹配。此機制在現代Web客戶端中已過時；現在，域將與主體替代名稱擴展的DNS名稱匹配。但是，錯誤消息文本通常繼續引用已棄用的機制，如Chrome中的「NET::ERR_CERT_COMMON_NAME_INVALID」。

同樣地，當SWG代理從Web伺服器請求URL時，Umbrella SWG會顯示包含此文本的516錯誤頁面，並且發生SAN DNS名稱不匹配的情況：

16794325789332

Cisco Umbrella計畫在未來更新此文本，以更好地反映當前行為。

其他資訊

請參閱RFC 5280:Internet X.509公鑰基礎設施證書和證書撤銷清單(CRL)配置檔案，有關證書主題的資訊的4.1.2.6部分，以及有關主題備用名稱的資訊的4.2.1.6部分。

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）。