排除錯誤"517 Upstream Certificate Revoced"

目錄

簡介

本檔案介紹在瀏覽到HTTPS URL時，如何疑難排解錯誤「517 Upstream Certificate Revoced」。

問題

當Umbrella安全Web閘道(SWG)Web代理設定為執行HTTPS檢查時，使用者會收到517 Upstream Certificate Revoced錯誤頁面。此錯誤表示請求的網站在TLS協商中傳送了一個數位證書，根據該證書的頒發者或類似頒發機構的狀態，該數位證書的狀態為「已吊銷」。已吊銷的證書不再有效。

原因

當Umbrella客戶端通過Umbrella安全Web網關發出HTTPS請求時，SWG會使用線上證書狀態協定(Online Certificate Status Protocol，OCSP)執行證書撤銷檢查。OCSP提供證書的吊銷狀態。SWG代表Umbrella客戶端發出OCSP證書撤銷狀態請求。

SWG確定所請求Web伺服器的證書以及受信任的根證書路徑中所有頒發中間證書的證書吊銷狀態。這些檢查可確保有效的信任鏈自頒發後未變為無效。

在使用OCSP撤銷檢查的數位證書中，「授權資訊訪問」X.509擴展包含了一個或多個「OCSP」欄位。欄位包含可查詢證書撤銷狀態的OCSP「端點」（Web伺服器）的HTTP URL。SWG向證書中的每個OCSP URL發出請求，直到收到響應（表示以下其中之一）：

- 證書有效（未吊銷），此時SWG允許Web請求繼續，或者
- 除OCSP「證書有效」響應（例如，證書被吊銷、伺服器當前無法應答、HTTP錯誤狀態、網路/傳輸層超時等）之外的任何內容，此時SWG顯示相應的錯誤頁面/消息，並且Web請求失敗

請注意，OCSP響應通常快取並用於響應將來的檢查。快取時間由伺服器在OCSP響應中設定。

直接瀏覽時的不同行為

Web客戶端可以使用各種撤銷檢查機制，具體取決於客戶端。例如，預設情況下，Google的Chrome瀏覽器不使用OCSP或標準CRL方法。相反，Chrome使用名為CRLSet的CRL的專有版本，Secure Web Gateway不使用此版本。因此，Chrome在檢查憑證的撤銷狀態時可能不會產生與SWG相同的結果。

但請注意，如CRLSet文檔所述，「在某些情況下，無論Chromium執行什麼操作，底層系統證書庫始終會執行這些檢查。」 因此，根據您的本地環境，OCSP和/或CRL檢查可以由您的瀏覽器或作業系統的加密服務庫（如SChannel、Secure Transport或NSS）執行。

另請注意，OCSP和CRL檢查不能保證產生相同的結果。

請參閱您的瀏覽器或作業系統供應商的文檔，以確定您的客戶端在瀏覽時執行哪些證書撤銷檢查。

解析

使用有效證書是WebServer管理員的責任。必須由伺服器管理員在伺服器上執行已吊銷證書的補救。Cisco Umbrella無法在此過程中提供幫助。

Cisco Umbrella強烈建議不要訪問使用吊銷證書的網站。僅當使用者完全理解站點使用撤銷證書的原因並完全接受任何風險時，才能使用解決方法。

為了避免該錯誤，可通過建立包含站點域名的選擇性解密清單來免除站點的HTTPS檢查。選擇性解密清單將應用於允許訪問該網站的Web策略。或者，可以將站點新增到外部域清單，以繞過SWG直接將流量傳送到站點。

其他資訊

希望確認伺服器證書是否已撤銷的客戶可以使用旨在檢查撤銷狀態的第三方工具。最明顯的是，Qualys SSL Labs的SSL Server Test工具除了提供其他證書有效性資訊外，還執行OCSP和CRL檢查。該工具可從以下網址線上獲得：

- https://www.ssllabs.com/ssltest/analyze.html

建議在使用思科Umbrella開啟支援案例之前，使用此工具檢查產生517 Upstream Certificate Revoked錯誤的站點。

另請參閱：https://support.umbrella.com/hc/en-us/articles/4406133198100-Certificate-and-TLS-Protocol-Errors

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）。