瞭解常見證書和TLS協定錯誤

目錄

簡介

本文檔介紹Umbrella Dashboard Activity Search中的常見證書和TLS協定錯誤。

概觀

由於證書和TLS錯誤而阻止的HTTP流量現在可在Umbrella Dashboard Activity Search中檢視。本文提供常見錯誤消息清單以及每個錯誤的簡要說明。

證書錯誤

上游證書已過期

網站提供的證書已過期。請聯絡網站管理員以報告此問題。

上游證書自簽名

網站提供的伺服器證書不是由證書頒發機構簽名的，因此Umbrella無法確定證書是否可信。

自簽名證書有時在伺服器託管用於受限受眾的資源時使用。例如，IT安全裝置的網路門戶通常預設使用自簽名證書。無法將Umbrella配置為信任自簽名證書。

缺少中間證書

Umbrella無法為所有中間機構獲取證書，因此無法驗證整個信任鏈。

Web伺服器證書通常由證書頒發機構的中間證書頒發/簽名。這些中間證書也可以由其他中間證書頒發。Web伺服器憑證（又稱「葉憑證」）與任何中間憑證形成回根憑證的鏈結。網站必須將中間證書與伺服器證書捆綁在一起，以便Umbrella驗證整個信任鏈。請聯絡網站管理員以報告此問題。

或者，如果證書包括「授權資訊訪問」擴展，Umbrella會嘗試自動獲取中間CA。請注意，啟用HTTPS解密和檔案檢查時，Umbrella僅支援AIA擴展。

上游證書缺少使用者名稱。

憑證的「Subject」欄位未包含識別名稱(DN)以識別此憑證。這是由憑證授權機構頒發的所有憑證的要求，因此也是Cisco Umbrella的要求。請聯絡網站管理員以報告此問題。

上游證書缺少公用名。

該網站提供的證書沒有公用名。Umbrella SWG需要Common Name(CN)欄位。其中包含證書主機名，驗證證書是否與使用者請求的資源匹配需要該主機名(例如，在瀏覽器中鍵入的地址)。 請聯絡網站管理員以報告此問題。

上游證書不受信任

Cisco Umbrella不信任該證書。此錯誤通常表示Cisco不信任頒發憑證的根CA。

Umbrella SWG具有內建的已知受信任的根證書頒發機構清單，可從信譽良好的源進行更新。如果網站的證書不是由此清單上的CA簽署，則證書驗證將失敗。如果您認為Umbrella缺少可信任的根CA，請與技術支援聯絡。

cert中的主機名與預期不同

使用者請求的資源(例如，在瀏覽器中鍵入的地址)與證書的公用名(CN)或使用者備用名(SAN)不匹配，因此Umbrella無法信任此請求的證書。請聯絡網站管理員以報告此問題。

已吊銷上游證書

網站提供的證書已被證書頒發機構吊銷。

Umbrella執行OCSP（線上證書狀態協定）檢查以確定證書是否被CA吊銷。請聯絡網站管理員以報告此問題。

TLS握手錯誤

不支援的上游密碼

無法完成TLS握手。這通常表示網站不支援Umbrella SWG使用的任何密碼套件清單。只支援較弱的

TLS密碼的較舊或過時的Web伺服器可能出現此錯誤。請聯絡網站管理員以報告此問題。

上游TLS版本不匹配

無法完成TLS握手，因為網站不支援與Umbrella SWG使用的TLS版本相同。目前，Umbrella SWG Proxy在與Umbrella SWG的客戶端連線以及從Umbrella SWG代理連線到目標Web伺服器的客戶端連線上均支援TLS 1.2和TLS 1.3。

小於1024位的上游DH金鑰

無法完成TLS握手，因為網站使用不受Umbrella支援的弱Diffie-Hellman金鑰。請聯絡網站管理員以報告此問題。

因應措施

可以通過在Cisco Umbrella中進行配置更改來解決這些問題。只有當您信任伺服器和證書的真實性時，才能執行此操作。

解決方法可以使用「選擇性解密清單」條目禁用解密，或使用「外部域」條目完全繞過Umbrella的流量。禁用解密時，Umbrella不執行證書驗證。請注意，在大多數情況下，當流量繞過Umbrella時，瀏覽器仍會顯示錯誤或警告 — Web瀏覽器會執行類似的證書驗證。

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）。