

瞭解安全訪問中的SSL證書和握手錯誤

目錄

問題

由於證書和TLS錯誤而阻止的HTTP流量現在可以在儀表板活動搜尋中檢視。本文提供常見錯誤消息清單以及每個錯誤的簡要說明。

環境

- Cisco安全訪問 — 安全Web網關SSL檢查

解析

上游證書已過期

網站的證書已超過其到期日期，因此Cisco Secure Access不信任該證書。此問題由網站所有者修復，因此請聯絡該網站的網站管理員並通知他們。

上游證書自簽名

網站提供其自己簽名的證書，而不是由受信任的證書頒發機構頒發的證書。由於沒有獨立機構擔保該證書，因此思科安全訪問無法確認該證書是真的。

您經常會看到資源上的自簽名證書，這些證書面向一小部分內部受眾 — IT安全裝置上的管理員門戶

就是一個典型示例。請注意，Cisco Secure Access無法設定為信任自簽名證書。

缺少中間證書

Cisco Secure Access無法收集它需要的所有中間證書，因此無法建立到根的完整信任鏈。

這一點之所以重要，原因如下：網站的證書（「枝葉」）由中間證書簽署，該證書又可由另一個中間證書簽署，以此類推，直至受信任的根目錄。要簽出此鏈，網站必須將其中間證書與其自己的證書一起傳送。如果缺少這些內容，驗證就會中斷，因此請讓網站的管理人員知道。

有一個例外：如果憑證包括「授權資訊存取」（AIA）擴充模組，思科安全存取可以嘗試自行取得遺失的中介軟體。請記住，僅當同時啟用HTTPS解密和檔案檢查時，此操作才有效。

上游證書缺少使用者名稱

該證書不包括使用者名稱（可分辨名稱）或使用者替代名稱，這意味著沒有明確標識證書所屬的內容。否則，思科安全訪問無法對其進行驗證。網站所有者需要更正此問題。

上游證書缺少公用名

證書沒有公用名(CN) — 該欄位通常保留站點的主機名，並幫助確認證書實際屬於您要訪問的站點。現在，該檢查確實取決於主體備用名(SAN),CN被視為舊欄位，但其缺失仍會觸發此錯誤。聯絡網路管理員進行定址。

不受信任的上游證書

Cisco Secure Access不信任此證書，通常是因為它無法識別頒發此證書的根CA。

Cisco Secure Access SWG保留受信任的根證書頒發機構的內建清單，該清單來自信譽良好的提供商，並且保持最新。如果站點的證書追溯到不在清單中的CA，驗證將失敗。如果您確信根CA是可以信任的，請與技術支援聯絡，我們就可以瞭解一下。

證書中的主機名與預期不同

您要求的地址與憑證上的名稱不相符，無論是其一般名稱(CN)還是其任何使用者替代名稱(SAN)。由於證書似乎不屬於您所訪問的站點，因此Cisco Secure Access對此請求不信任該證書。網站管理員需要解決這個問題。

已吊銷上游證書

頒發此證書的證書頒發機構已撤銷此證書，也就是說，它不再被視為有效。

思科安全存取使用線上憑證狀態通訊協定(OSCP)確認這點，該通訊協定會即時檢查憑證是否已被吊銷。讓網站管理員知道，以便他們更換網站。

TLS握手錯誤

不支援的上游密碼

無法完成TLS握手，因為網站不支援Cisco Secure Access SWG使用的任何密碼套件。這通常出現在只能提供較弱密碼的舊或過時伺服器上。修復程式位於伺服器端，因此請將其傳遞給網站管理員。

上游TLS版本不匹配

握手失敗，因為網站未使用Cisco Secure Access SWG支援的TLS版本。目前，Cisco安全訪問SWG代理與TLS 1.2和TLS 1.3配合使用 — 既適用於來自客戶端的連線，也適用於它通向目標伺服器的連線。

小於1024位的上游DH金鑰

握手無法完成，因為網站使用的Diffie-Hellman金鑰太弱（低於1024位），思科安全訪問無法接受。這是伺服器端限制，因此網站管理員需要對其進行強化。

因應措施

可以通過在Cisco Secure Access中更改配置來解決這些問題。

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」條目完全繞過來自Cisco Secure Access的流量。禁用解密時，思科安全訪問不執行證書驗證。

請注意，在大多數情況下，當流量從Cisco Secure Access - Web瀏覽器執行類似的證書驗證時，瀏覽器仍會顯示錯誤或警告。

原因

Cisco安全訪問SSL檢查代理無法完成TLS握手 — 最常見的原因是目標使用拒絕已重新簽名的CSA證書的證書固定。

- 證書固定：客戶端硬碼預期證書指紋
- 終端上不受信任的CSA CA:檢查CA證書未部署到受信任的根儲存

相關內容

- [思科技術支援與下載](#)

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）。