安全訪問中的SSL解密證書錯誤處理

目錄

問題

在Cisco Secure Access中啟用SSL解密時，使用者遇到與證書相關的錯誤頁面。已收到有關三種特定憑證錯誤型別的多個查詢：

- 源伺服器證書過期錯誤
- 證書CN/SAN不匹配錯誤，其中證書上列出的公用名稱或使用者替代名稱與訪問的域不匹配
- 源伺服器證書中嵌入的證書吊銷清單(CRL)連結導致連線問題

這些證書錯誤類似於通常在Web瀏覽器中顯示的警告。問題是，Cisco Secure Access能否通過顯示警告頁面（類似於瀏覽器或內容過濾器），然後在顯示警告後允許訪問，或在所有情況下允許訪問來處理與證書相關的錯誤。此外，需要了解禁用SSL解密時的行為，以及流量是否經過而不管證書問題。

環境

- Cisco Secure Access - Internet Access（漫遊模組、VA、DNS、SWG、PAC、IPS、證書）
- 已啟用SSL解密功能
- 多個域遇到證書驗證問題
- 具有各種證書問題（包括到期和域不匹配）的源伺服器

解析

證書錯誤處理限制

與證書相關的錯誤處理在Cisco Secure Access中不可用。該產品不支援：

- 呈現類似於瀏覽器的證書問題警告頁面
- 處理配置時出現域特定證書錯誤
- 基於目標域的自定義錯誤處理
- 包含使用者覆蓋選項的內容過濾器樣式警告頁面

SSL解密排除解決方法

推薦的方法是使用安全配置檔案解密設定從SSL解密中排除有問題的域。可通過以下方式配置此項：

導航到Security Profile > Decryption Settings部分以從SSL檢查中排除特定域。

從SSL解密中排除域時，會發生以下行為：

- 排除的域的流量完全繞過SSL檢查
- 安全訪問未執行證書驗證
- 使用者不會遇到由Secure Access生成的證書錯誤頁面
- 如果憑證問題持續存在，則原始憑證錯誤可能仍會在使用者瀏覽器中看到

SSL解密已禁用行為

當域或全域性禁用SSL解密時，思科安全訪問將通過（轉發）流量，而不考慮任何證書問題。在未啟用解密時，產品不會檢查或驗證證書，從而有效地允許所有HTTPS流量透明通過。

原因

證書錯誤是由源伺服器上的合法證書驗證問題引起的，包括過期證書、CN/SAN不匹配和CRL連線問題。思科安全訪問在其SSL解密過程中執行證書驗證，當這些驗證失敗時，產品會生成錯誤頁以防止可能的不安全連線。這是SSL檢查功能的預期安全行為。

相關內容

- 思科安全訪問解密配置文檔
- 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）。