為IPS和SWG解密旁路配置SSE不解密

目錄

問題

即使將財務類別或特定網域新增至不解密(DND)清單並應用相關存取規則，前往財務類別目的地的HTTPS流量仍會呈現Cisco SSE憑證，而不是原始網站憑證。通過零信任訪問客戶端(TIA)訪問站點時觀察到此行為，它特別影響對需要端到端證書可見性的金融相關網站(例如https://onlinesbi.sbi.bank.in/)的訪問。

預期行為是，當站點或內容類別新增到DND清單時，原始網站證書可以呈現給瀏覽器，而不是Cisco SSE證書。但是，Cisco SSE證書繼續顯示，表示儘管配置了DND，流量解密仍在進行。

環境

- 思科安全服務邊緣(SSE)
- 零信任訪問客戶端(TIA)連線
- 已啟用全域性IPS解密
- 訪問策略上活動的IPS
- 在安全配置檔案的「不解密」清單中配置的財務類別
- 應用了相應安全配置檔案的訪問規則

解析

解決方法包括瞭解Cisco SSE執行兩種不同的解密型別，並為這兩種解密型別配置適當的「不解密」設定。

瞭解SSE解密型別

Cisco SSE執行兩個獨立的解密過程：

- SWG（安全Web網關）解密- Web代理解密
- IPS解密 — 入侵防禦系統解密

在安全配置檔案中配置的「不解密」條目僅適用於SWG解密，並且不阻止IPS解密。如果啟用了全域性IPS解密，並且IPS在任何訪問策略中均處於活動狀態，IPS解密仍會發生，從而導致向瀏覽器顯示Cisco SSE證書。

設定步驟

步驟 1:將sites 或內容類別新增到系統提供的不解密清單。

系統提供的不解密清單應用於所有IPS配置檔案。向此系統提供的清單中新增站點或內容類別會導致顯示原始網站證書，從而有效地繞過IPS解密。

步驟 2:確認不需要進行其他策略更改。

無需在訪問策略內引用系統提供的不解密清單。該清單會自動應用於所有IPS配置檔案。

驗證測試

可以使用以下驗證方法來確認正確的配置：

方法1:將域新增到系統提供的「不解密」清單

將特定域新增到系統提供的不解密清單，可能會導致顯示原始網站證書，而不是思科SSE證書。

方法2:暫時禁用全域性IPS解密（僅用於測試）

暫時禁用全域性IPS解密還會導致檢測到測試站點的原始證書，從而確認IPS解密是思科SSE證書呈現的原因。

預期結果

正確設定後：

- 新增到系統提供的不解密清單的站點或內容類別提供其原始網站證書。
- 對於指定的站點或類別，SWG和IPS解密均被繞過。
- 瀏覽器顯示實際的網站證書而不是Cisco SSE證書。

原因

之所以會出現此問題，是因為Cisco SSE執行兩種不同的解密過程：SWG解密和IPS解密。在安全配置檔案中配置的「不解密」條目僅繞過SWG解密。當啟用全域性IPS解密且IPS在訪問策略上處於活動狀態時，IPS解密將繼續獨立進行，導致即使站點包含在安全配置檔案DND清單中，Cisco SSE證書也會呈現給瀏覽器。

要完全繞過兩種解密型別，必須將站點或內容類別新增到系統提供的不解密清單，該清單適用於所有IPS配置檔案，並防止SWG和IPS都進行解密。

相關內容

- 為安全訪問建立有效的「不解密」清單
- 排除故障並收集基本資訊以實現安全訪問
- 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）。