

澄清FTD上SSL/TLS解密的效能影響和最佳實踐

目錄

問題

使用者正計畫在防火牆威脅防禦(FTD)裝置上啟用SSL/TLS解密，並需要在實施前瞭解對裝置效能的潛在影響。主要關注事項包括：

- 影響防火牆吞吐量、延遲和整體流量處理效能。
- 啟用解密後，預期CPU和記憶體利用率會增加。
- 特定FTD模型的規模設定原則及效能基準。
- 對併發解密會話的建議限制。
- 生產部署的最佳做法和先決條件。

環境

- Firepower 4115。其他硬體平台也可能受到影響。
- FTD版本7.4.2 (內部版本172)。其他軟體版本也可能受到影響。
- 考慮SSL/TLS解密功能。
- 生產環境部署規劃。

解析

SSL/TLS解密確實增加了對Firepower 4115的處理開銷，但實際影響很大程度上取決於解密的流量以及解密後應用了何種檢查。

效能影響分析

SSL/TLS解密影響包括：

- 有效吞吐量更低。
- 延遲更高。
- Snort/檢查CPU使用率提高。
- CPU和記憶體增加，在沒有實際流量分佈分析的情況下，無法以固定百分比準確預測。

FPR 4115效能基準

思科發佈的Firepower 4115基準規格：

- TLS硬體解密吞吐量：6.5 Gbps。
- FW + AVC吞吐量：33 Gbps。
- 使用AVC的最大併發會話數：1500萬。
- 使用AVC時每秒的最大新連線數：21萬。

重要的規模調整註釋：6.5 Gbps TLS硬體解密基準基於特定測試條件。如果解密大量流量、使用入侵/檔案/惡意軟體策略檢查已解密的流量，或處理許多短期的TLS會話，則生產吞吐量可能會降低。

思科不會在FTD 7.4.2上為Firepower 4115發佈單獨的「最大併發解密會話數」數。實際上，容量是使用流量混合、併發會話、連線速率、密碼套件和檢查策略負載進行驗證的。

推薦的生產部署方法

步驟 1:先從有限的試點開始

- 最初不要啟用寬泛的「解密所有」規則。
- 從選定的使用者、子網或目標類別開始。
- 對於不需要檢查的流量，使用Do Not Decrypt保持預設處理保守性。

步驟 2:排除通常因解密而中斷的流量

- 銀行/金融網站。
- 保健門戶。
- 證書固定的應用程式。
- 一些軟體即服務(SaaS)和終端安全/雲應用。
- 敏感的業務關鍵型應用程式，除非經過明確測試。

步驟 3:保持SSL規則簡單且有序細緻

- 將特定的Do Not Decrypt排除置於更廣泛的解密規則之上。
- 儘可能避免過於寬泛或複雜的匹配。
- 請勿對Decrypt-Resign/Known-Key規則使用TLS版本或密碼套件條件，因為Cisco會記錄這會導致不可預測的行為。

步驟 4:驗證證書就緒性

- 對於出站Decrypt-Resign，簽名CA證書必須由客戶端端點信任。
- 對於入站已知金鑰解密，防火牆必須具有正確的伺服器證書/私鑰材料。

步驟 5:在推廣期間監控

- 跟蹤總體CPU，更重要的是跟蹤Snort/檢查CPU利用率。
- 每秒跟蹤併發連線和新連線。
- 檢視連線事件中的SSL流狀態/握手錯誤。
- 注意TLS超訂用指示符和特定於應用程式的故障。

有關如何監控CPU檢查的詳細資訊：

- <https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2026/pdf/BRKSEC-2362.pdf>
- [像TAC工程師一樣思考：思科安全防火牆最常見棘手問題指南](#)

要每秒跟蹤連線和新連線，請檢查：

- [日誌記錄最佳實踐](#)

要跟蹤連線事件檢查中的SSL流狀態/握手錯誤和TLS超訂用指示符檢查：

- [排除TLS/SSL超訂用故障](#)

步驟 6:回退或縮小範圍（如果您看到）：

- 持續檢測CPU飽和度。
- 使用者可見延遲增加。
- TLS握手失敗。
- 業務應用程式在解密後失敗。
- 超訂用或SSL錯誤過多。

步驟 7:考慮TLS 1.3影響

採用TLS 1.3會影響可視性和行為，因為某些握手和檢查特性與TLS 1.2不同。

原因

SSL/TLS解密需要額外的計算資源來解密、檢查和重新加密流量流。根據流量模式、應用於已解密流量的檢查策略以及特定部署配置，效能影響會顯著不同。如果沒有適當的規劃和逐步實施，組織可能會在生產環境中遇到意想不到的效能降級。

相關內容

- [思科安全防火牆管理中心裝置配置指南 — 解密規則](#)
- [思科安全防火牆解密策略指南](#)
- [解密策略規則順序的最佳實踐](#)
- [使用思科安全防火牆7.7簡化解密](#)
- [解密規則最佳實踐](#)
- [Cisco Firepower 4100系列產品手冊](#)
- [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）。