解密最佳作法

Version 10.0 (EoL)

docs.paloaltonetworks.com

techDOCS paloalto NETWORKS

Contact Information

Corporate Headquarters:
Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054
www.paloaltonetworks.com/company/contact-support

About the Documentation

- To ensure you are viewing the most current version of this document, or to access related documentation, visit the Technical Documentation portal: docs.paloaltonetworks.com.
- To search for a specific topic, go to our search page: docs.paloaltonetworks.com/search.html.
- Have feedback or questions for us? Leave a comment on any page in the portal, or write to us at documentation@paloaltonetworks.com.

Copyright

Last Revised

October 28, 2020

Table of Contents

解密最佳作法

您無法保護您的網路遠離看不見的威脅，並進行檢查。Gartner 預測 2020 年超過 70% 的新惡意軟體活動將使用不同形式的加密。Google 的透明度報告顯示在大部分狀況下，不論您如何分析 Google 網頁流量，都會加密超過其 90%。解密 流量以保護您的網路遠離隱藏的威脅。

本文件為簡化的預部署、部署和後部署最佳作法核對清單，您可依照本清單來實施解密。每個章節皆包含《 PAN-OS 管理員指南》內詳細內容的連結，包含如何設定解密政策規定與設定檔。

- 規劃您的 SSL 解密最佳部署作法
- 使用最佳作法部署 SSL 解密
- 遵循後部署 SSL 解密最佳作法

規劃您的 SSL 解密最佳部署作法

透過發展解密戰略和推展計劃來預備部署解密。開啟解密可能會改變使用者與一些應用程式和網站間的互動，因此規劃、測試和教育使用者是成功部署的關鍵。

STEP 1 | 設定目標。

- ❑ 規劃解密沒有您防火牆資源那樣多的私人或敏感流量。這會透過暴露和避免加密威脅來減少攻擊面。了解您可以合法解密的流量相關法律與法規以及使用者通知要求。
- ❑ 在建立和部署解密原則規則之前，從以連接埠為基礎的安全性原則規則移轉至以應用程式為基礎的安全性原則規則。如果您根據基於連接埠的安全性政策建立解密規則，然後移轉至基於應用程式的安全性政策，則變更可能會導致解密規則封鎖您打算允許的流量，因為安全性政策規則可能使用應用程式預設連接埠來防止流量使用非標準連接埠。在部署解密前移轉基於 App-ID 的規則能確保當您進行解密部署測試時，將發現安全性政策設定錯誤並在將解密推展到一般使用者群眾前修復這些錯誤。

STEP 2 | 與利益相關方一同努力並教育他們，這些人包含如法律、財務、人資、主管、安全和 IT/支援方，以發展解密部署策略。

- ❑ 取得解密流量所需的核准來保護企業安全。
- ❑ 識別並排定要解密流量的優先次序：
  - 決定要解密的應用程式為何（認可、非認可）。不允許加密非認可的應用程式。
  - 決定要解密的設備為何（公司、自備工具、行動設備等）。

    企業不會控制 *BYOD* 裝置。如果您允許在你的網路上使用自備工具設備，則請加解密他們的流量，並使其遵守您應用在其他網路流量上相同的安全性政策。為此，請透過驗證入口網站重新導向 *BYOD* 使用者，指導他們如何下載和安裝 *CA* 憑證，並明確通知使用者將會對其流量進行解密。向 *BYOD* 使用者提供有關此過程的訓練，並將其納入貴公司的隱私權和電腦使用原則中。
  - 決定您是否想要對不同的群組使用相同的解密政策，如不同的員工、契約商、合作夥伴和訪客群組。
- ❑ 識別您無法解密的流量：
  - 基於技術原因（例如憑證釘選、不支援的密碼或相互驗證）而導致解密結束的流量。
  - 您選擇不解密的流量，如財務、健康、政府和其他敏感類別，包含如主管這類的使用者和群組。
  - 完全理解解密之外的流量。您無法看到加密的流量，且防火牆無法對加密的流量用防威脅設定檔。
- ❑ 備妥更新的法律和人力資源電腦使用原則，散佈給所有員工、承包商、合作夥伴、來賓和任何其他網路使用者，以便在部署解密時，使用者便已瞭解可以對其資料進行解密並掃描以發現威脅。
- ❑ 決定如何處理憑證認證。您的業務模式可能在安全性和使用者經驗間需要彼此妥協。了解您想要如何處理憑證認證有助於決定您要如何設定 SSL 正向代理程式解密設定檔。
- ❑ 識別要記錄的流量。了解當地法律和法規的不同，以及它們如何影響可記錄的流量以及可儲存流量的位置。

  將防火牆放置在可以看到所有網路流量的位置，以便沒有任何加密的流量因繞過防火牆而在無意間獲得網路的存取權。

STEP 3 | 發展推動您公開金鑰基礎結構 (PKI) 的計劃。

- ❑ 如果您已有 PKI，請從您的 Enterprise Root CA 產生 SSL Forward Trust CA 憑證作為次要憑證。這會讓部署更加輕鬆,因為網路裝置以信任此 Enterprise Root CA，讓您不會陷入憑證問題。若您沒有 Enterprise Root CA，請考慮取得一個。

  或者，可在防火牆上產生自簽 Root CA 憑證，並在該防火牆上建立從屬的 Forward Trust CA 憑證，以安裝在網路設備上。自簽憑證最適用於沒有 Enterprise Root CA 和概念驗證 (POC) 試驗的小型公司。

與自備工具裝置相似，企業不會控制訪客裝置。如果您允許在你的網路上使用訪客設備，則請加解密他們的流量，並使其遵守您應用在其他網路流量上相同的安全性政策。為此，請透過驗證入口網站重新導向訪客使用者，指導他們如何下載和安裝 *CA* 憑證，並明確通知使用者將會對其流量進行解密。包含您公司隱私和電腦使用原則的流程。

- 產生獨立的 Forward Trust 和 Forward Untrust CA 認證。不要對兩種憑證使用相同的 PKI 從屬 CA，不要用 Trusted Root CA 簽署 Forward Untrust 憑證！Forward Untrust 憑證會警告使用者，簽署伺服器的憑證不合法，且不應進入網站。如果 Trusted Root CA 簽署 Untrust 憑證，則用戶端會因用戶端信任此 Root CA，而信任本應不被信任的憑證。
- 為每個防火牆產生單獨的從屬 Forward Trust CA 憑證。使用單獨從屬 CA 可在不影響部署中其餘部分的情況下，讓您在停止使用裝置（或裝置配對）時撤銷憑證，並降低在需要撤銷憑證時的影響。單獨的 CA 憑證能協助技術支援人員處理使用者的問題，因為憑證錯誤訊息包含有關流量穿過的防火牆相關資料。雖然在所有防火牆上使用一個 Forward Trust 從屬 CA 部署較為容易，但在每一個防火牆使用單獨的憑證能提供最佳安全性。
- 如果您的私密金鑰需要額外的安全性，則請考慮將它們儲存至 HSM。

STEP 4 | 進行防火牆效能的基準線測量，了解資源使用和可用防火牆資源，讓您可以在部署解密後比較效能的基準線，以及預估需要支援您想要解密的流量數的防火牆部署規模。

- 與您的 Palo Alto Networks SE/CE 合作，確定防火牆部署的規模，避免出現錯誤調整。
- 請記下目前可用的防火牆資源。一般而言，安全性越高，解密所需資源就越多。影響您可以解密流量數的因素包含：
  - 要解密的 SSL 流量。
  - TLS 通訊協定版本。
  - 金鑰大小。
  - 金鑰交換演算法。完美轉送密碼 (PFS) 暫時演算法（如 DHE 和 ECDHE）比 RSA 消耗更多資源，但提供更高的安全性，因為防火牆會為每個工作階段產生新的密碼金鑰。如果攻擊者破壞工作階段金鑰，則 PFS 會阻止攻擊者使用它來解密相同用戶端與伺服器之間的其他工作階段，但 RSA 不會。
  - 憑證驗證。RSA 憑證驗證（這與 RSA 金鑰交換算法不同）會比 ECDSA 憑證認證耗費更少的 CPU 循環，但 ECDSA 提供更高等的安全性。
  - 加密演算法。金鑰交換演算法確定加密演算法是 PFS 還是 RSA。
  - 防火牆型號和資源。較新的防火牆型號比舊有型號擁有更多資源。
- 交易規模影響效能。測量所有流量的平均交易規模，然後測量 443 連接埠（HTTPS 加密流量預設連接埠）的流量平均交易規模，以了解防火牆上加密流量與整體流量的比率以及平均交易規模。

綜合這些因素可確定解密如何耗用防火牆處理資源。如果防火牆資源存在問題，請對較高優先順序和較高風險的流量使用較強解密，並使用需要較少處理器的解密來解密和檢查較低優先順序的流量，直到您可以增加可用資源為止。

調整防火牆大小，以包含解密流量數成長的空間，因為每天會加密更多流量。

STEP 5 | 規劃分階段和優先次序的部署。

- 確定早期採用者以支持解密並讓部門經理參與該計劃。
- 設定 POC 以在您將它推展的一般使用者大眾時，可以先測試部署策略。測量解密 POC 部署影響防火牆 CPU 和記憶體用量的方式，以協助了解防火牆調整是否正確。POC 也可以顯示在技術上破壞解密的應用程式。
  - 教育 POC 參與者相關變更以及如何聯絡技術支援。
  - 為解密 POC 設定技術支援 POC，以便支援人員有機會開發支援推展的最佳方法。
  - 解密階段。計劃先解密風險最高的流量（最有可能存在賭博或高風險這類惡意流量的 URL 類別），然後隨著經驗積累解密更多流量。或者，先解密不會影響業務的 URL 類別（因此，出現問題時，也不會發生影響業務的問題），例如新聞資訊來源。在這兩種狀況下，解密一些 URL

類別、聽取使用者回饋、執行報告以及檢查解密日誌，確保解密如預期運作，然後逐步解密更多 URL 類別等。如果您因技術原因無法解密或因您選擇不要解密那些網站，則計劃進行解密例外以免除網站的解密。

- 衡量 POC 的成功，並微調部署作法。

- ❑ 在開始推展前教育使用者大眾。POC 有助於識別通訊要點。
- ❑ 向所有員工、承包商、合作夥伴、訪客和任何其他網路使用者散發更新的法律和人資電腦使用政略。確保所有人都了解在向每個部門或群組推出解密時，可以解密和掃描其資料以找出威脅。
- ❑ 建立合理的時間表，留下評估推展每一階段的時間。

使用最佳作法部署 SSL 解密

STEP 1 | 產生並散布解密政策金鑰與憑證。

- 若您擁有 Enterprise PKI，為來自您 Enterprise Root CA 的轉發代理流量產生 Forward Trust CA 憑證。不然，可在防火牆上產生自簽 Root CA 憑證，在讓防火牆上建立從屬 CA，然後將自簽憑證散佈到所有用戶端系統中。自我簽署憑證適用於實驗室測試、小型部署和 POC。
- 為每個防火牆產生一個唯一從屬 Forward Trust CA（或為所有防火牆產生一個 Forward Trust CA，根據規劃—一個憑證較容易部署，但單獨的憑證提供最佳安全性和其他優點）。不同的 PKI 平台對調整憑證管理有不同的功能。
- 如果您未使用 Enterprise CA，則可以將 Forward Trust CA 憑證匯入用戶端系統的信任 CA 儲存空間中。
- 不要將 Forward *Untrust* CA 憑證匯入用戶端系統的 CA 信任儲存庫中，否則不信任的憑證不會作為不信任的網站的觸發器。（不過，如果防火牆自我簽署 Root CA 未在用戶端系統上安裝為受信任簽發者，則可以使用自我簽署 Forward Untrust 憑證）。
- 使用自動化方式散布 Forward Trust 憑證至連線的設備，如 Palo Alto Networks GlobalProtect Portal、Microsoft AD Certificate Services（使用 Group Policy Objects）、商業工具或開源工具。
- 如果您從 Enterprise Root CA 產生憑證的話，則在防火牆上匯入憑證。
- 在安全庫中為防火牆的 Forward Trust CA 憑證備分私密金鑰（非防火牆的主要金鑰），好在問題發生時，您仍然可以存取 Forward Trust CA 憑證。
- 如果您從 Enterprise Root CA 產生憑證和私密金鑰，則請封鎖匯出私密金鑰。（您可以將它們從 Enterprise CA 安裝在新的防火牆和 Panorama 上，因此您不需要從 PAN-OS 匯出它們）。
- 如果您計劃使用 HSM 呼叫，則請將私密金鑰存放至 HSM。

STEP 2 | 配置解密設定檔以控制通訊協定、憑證認證以及故障處理。

- SSL 正向代理程式解密設定檔控制伺服器匯出流量的憑證認證、工作階段模式和故障檢視。以過期憑證、不信任的發行者、不支援的版本和不支援的密碼套裝軟體封鎖工作階段。除非有重要的應用程式需要工作階段，否則以用戶端授權封鎖工作階段，在這個狀況下您應建立允許用戶端授權的單獨解密設定檔，並僅應用於需要用戶端授權的流量上。
- SSL 輸入檢查解密設定檔 控制伺服器匯入流量的工作階段模式和故障檢視。以不支援的版本和不支援的密碼套裝軟體封鎖工作階段。
- SSL 通訊協定設定控制加密套件元素：用於 SSL 正向 Proxy 和 SSL 輸入檢查流量的通訊協定版本、金鑰交換演算法、加密演算法和驗證演算法。使用您可以使用的最強密碼。對於正向 Proxy，將通訊協定 **Min Version**（最低版本）設定為 **TLSv1.2**，並將 **Max Version**（最高版本）設定為 **Max**（最高），以封鎖弱通訊協定。對於 SSL 輸入檢查，以符合您正在檢測匯入流量的伺服器能力的通訊協議設定，來建立單獨的設定檔。

  使用您可以使用的最強加密套件。建立單獨解密政策和設定檔，以將安全性最大化。如果您因業務目的而需要的傳統網站僅支援較弱的密碼，則請建立單獨解密設定檔來允許該流量，並且只在解密政策中將它套用至必要的網站。使用相同的技術來微調不同 *URL* 類別的安全性與效能。

  許多行動應用程式都使用釘選的憑證。因為 *TLSv1.3* 會加密憑證資訊，所以防火牆無法將這些行動應用程式自動新增至 *SSL* 解密排除清單。對於這些應用程式，確定解密設定檔 *Max Version*（最高版本）設定為 *TLSv1.2*，或將不解密政策套用至流量。
- 無解密設定檔控制您選擇不解密的幾個憑證認證。以過期憑證封鎖工作階段與不信任的發布者。

  將不解密設定檔套用至 *TLSv1.3* 流量。加密憑證資訊，讓防火牆無法根據憑證資訊來封鎖工作階段。
- 對於 SSL 正向代理程式和非解密流量，配置 Cerrtificate Revocation List (CRL) 與 Online Certificate Status Revocation (OCSP) 憑證撤消檢查，以確認該站點憑證並未被撤消。

- SSH 代理程式設定檔控制工作階段模式與 SSH 通道流量錯誤檢查。以不支援的版本和不支援的演算法封鎖工作階段。

數據中心與週邊（網際網路通道）最佳作法解密設定檔使用的案例與一般最佳作法設定檔稍有不同。

STEP 3 | 配置解密政策規則以定義要解密的流量，並為您選擇不要解密的流量進行基於政策的例外。

- 建立政策規則以排除特定目的地 IP 位址（例如金融伺服器）、來源使用者和群組（例如主管或人資）、來源裝置以及您選擇不要解密的應用程式連接埠。將這些規定置頂於解密規則庫，解密流量規定前。針對 TLSv1.3 流量以外的所有流量，對它們附加不解密設定檔，以將 SSL 伺服器憑證驗證控制套用至加密流量。這可以防止無意中解密您不想解密的流量。
- 使用 URL 類別、自訂 URL 類別和外部動態清單 (EDL) 來指定不要解密的 URL，例如金融服務、健康與醫療、政府，以及基於業務、法律或法規原因而不想要解密的任何其他類別。在具有動態變更的 IP 位址（例如 Office 365）或頻繁變更成員的環境中使用 EDL 以進行更新，而不需要提交。

  建立 EDL 或自訂 URL 類別，其中包含所有您選擇不解密的類別，因此它們只需要一個解密政策規則。

  將這些規則放在可解密解密規則庫中流量的規則上方。
- 設定解密記錄和日誌轉送。
- 若您使用解密鏡像複製並傳送解密的流量至流量收集工具，則小心本機隱私規定可能會禁止鏡像或控制您可鏡像的流量。
- 設定 SSL 正向 Proxy、SSL 輸入檢查和 SSH Proxy 規則來建立政策，以解密剩餘的流量。請務必解密線上儲存和備份、Web 式電子郵件、網頁託管、個人網站和部落格、內容傳送網路，以及高風險 URL 類別。限制只有管理員才能使用 SSH Proxy，而管理員可以管理網路裝置、記錄所有 SSH 流量並設定多因素驗證以防止未授權 SSH 的存取。

STEP 4 | 如果在 POC 測試期間技術性地破壞解密且並未列於排除清單，則將網站新增至SSL 解密排除清單（**Device**（裝置）> **Certificate Management**（憑證管理）> **SSL Decryption Exclusion**（**SSL** 解密排除））。（就技術而言，解密可封鎖解密的網站會導致封鎖該流量。）

STEP 5 | 在安全性政策中，封鎖快速 UDP 網際網路連線 (QUIC) 通訊協定。

Chrome 以及其他一些瀏覽器會使用 QUIC 而非 TLS 建立工作階段，但 QUIC 使用防火牆無法解密的專用加密手法，因此潛在危險的流量可能會如加密流量般進入網路。建立兩個規則，一個封鎖標準連接埠上的 QUIC 應用程式，一個則封鎖 UDP 連接埠 80 和 443。封鎖 QUIC 會強制讓瀏覽器使用 TLS。

STEP 6 | 將解密流量轉送至 WildFire以檢測惡意軟體。

STEP 7 | 慢慢推出解密。

解密一些 URL 類別、檢視使用者回饋並執行報告以確保解密如預期般運作。慢慢解密更多 URL 類別，直到您達成目標為止。從最優先的流量開始（URL 類別最有可能存在如遊戲這類惡意流量）並在經驗更豐富和細化流程後解密更多流量。另外一種更傳統的方法為先解密不影響您業務的 URL 類別，如：新聞饋送。

遵循後部署 SSL 解密最佳作法

在您部署解密後，確保每件事皆如預期般運作，並採取步驟以確保能如同預期般的運作。

STEP 1 | 證明解密如預期般運作。

STEP 2 | 測量防火牆性能以確保其在可接受的範圍內，因此可讓您了解解密對性能的影響。

如果您想要解密的流量超過防火牆資源可支援的流量，則請增加資源，讓您擁有足夠的資源可以解密所有要解密的流量並保護網路安全。

STEP 3 | 如果新進員工無法到達使用弱加密套件的特定網站，則在雇用他們時即教育他們，好讓他們了解您的解密政策，不致驚訝。

STEP 4 | 定期檢閱並更新解密政策和設定檔。

STEP 5 | 使用應用程式控管中心的 **SSL Activity**（**SSL** 活動）Widget 和解密日誌（**Monitor**（監控）> **Logs**（日誌）> **Decryption**（解密））這類解密疑難排解工具來監控解密流量以及解決解密問題。

解密疑難排解工作流程範例顯示如何使用這些工具來調查問題。

STEP 6 | 使用 Palo Alto Networks 文件與其他資源，好了解更多有關解密的事項，並查閱資料：

- PAN-OS 管理員指南提供 Palo Alto Networks 新世代防火牆的詳細資料。
- Palo Alto Networks Live 社群中大一張關於解密配置、設定和管理的 解密資源清單文章。
- 若要尋找遺失的中間憑證，請至SSL Labs (Qualys)。
- 若要尋找伺服器支援的密碼套裝軟體，請至 Qualys SSL Labs 的伺服器 SSL 測試頁面。
- 若要查看全球 15 萬個最熱門網站所使用的不同密碼和協議的百分比最新統計數字，以了解更多安全密碼和協議的現今趨勢以及其廣布全球的支援方式，請至 Qualys SSL Labs 的SSL Pulse 頁面。