SSL 檢查終極指南

披露 SSL 流量中的威脅

白皮書

執行摘要

加密傳輸佔了所有網路傳輸活動的一大部分，而且比重不斷增加。採用 SSL 及其新版協定傳輸層安全協議 (TLS) 固然可喜可賀，然而加密在提高機密性與訊息完整性的同時，也為企業組織帶來了風險。如果安全裝置不檢查 SSL 流量，駭客就能利用加密來隱藏他們的惡意探索。

威脅有多嚴重？國際研究暨顧問機構 Gartner 最近一項調查指出：「僅有不到 20% 的企業組織，在採用防火牆、入侵防禦系統 (IPS)、整合式威脅管理平台 (UTM) 應用之餘，針對進出的 SSL 流量實施解密。」[1] 駭客只要透過加密流量的隧道攻擊，就能迴避 80% 以上的企業網路防禦系統。

若要阻止網路攻擊，企業組織必須對加密資料進行深入解析，因此需要專屬安全性平台來針對進出的 SSL 流量實施解密。

五大特色提供於選擇 SSL 檢查平台時應注意的事項

1	2	3	4	5
SSL 效能	合規性	異質網路整合	安全基礎架構	SSL 憑證與金鑰

本白皮書列述的五大特色，是企業組織評估 SSL 檢查平台時所應考量的重點，有助於 IT 安全團隊迅速界定評估標準，並避免常見的部署陷阱。

1 Gartner「資安領導者必須因應 SSL 流量遽增所帶來的威脅」，2013 年 12 月

目錄

當前的不安全狀態

隨著各個企業組織在其網路邊界建置防火牆，利用各式各樣安全產品檢查進出流量，在 2014[2] 年，全球在資安方面的挹注金額已達到驚人的 711 億美元。遺憾的是，隨著 SSL 流量的增加，這一份超過 700 億美元的安全投資，卻遠不足以保護數位資產。

攻擊者變得越來越聰明，並利用了企業防禦機制不足的漏洞。事實上，Gartner 的研究人員預測：「在 2017 年，針對企業的網路攻擊，將會有超過一半以上 (原本不到 5%)，利用加密的流量來迴避控管。」[3] 因此，未針對 SSL 通訊內容進行檢查的企業組織無異於門戶洞開，讓攻擊者得以侵入其防禦系統並竊取資料。為了阻止網路攻擊，企業必須檢查所有流量 (尤其是加密流量)，以防範進階威脅。

「在 2017 年，針對企業的**網路攻擊，將會有超過一半以上 (原本不到 5%)，利用加密的流量**來迴避控管。」[4]

現有的安全解決方案無法處理 SSL

雖然有一些安全解決方案能夠解密 SSL 流量，但是不斷增加的 SSL 頻寬需求和 SSL 金鑰長度，都可能讓許多安全解決方案失效。由美國國家標準技術研究所 (NIST) 所發布的 800-131A 標準，引發從 1024 到 2048 位元 SSL 金鑰長度的轉變，造成了重大的影響。NSS Labs 的分析顯示，對採用 2048 位元 SSL 加密法的流量進行解密，會讓七款頂尖的新一代防火牆，「產生平均 81% 的效能減損」[5]。如果企業組織想重新調整防火牆以進行 SSL 解密，將必須考慮其對於防火牆效能的影響。

審慎評估 SSL 檢查平台的重要性

「NSS Labs 發現，2048 位元的加密法，**會讓七款頂尖的新一代防火牆，產生平均 81% 的效能減損。**」[6]

為了消除企業防禦系統中的 SSL 盲點，企業組織應佈建解決方案，來解密 SSL 流量內容 (無論是進入企業伺服器的流量，或由內部使用者外傳至網際網路的流量)，以利所有分析網路流量的安全產品檢查加密的資料。

在選擇解決方案之前，企業組織必須仔細地評估 SSL 檢查平台的功能與效能。如果 IT 安全團隊倉促部署 SSL 檢查平台，日後可能會因為 SSL 頻寬需求不斷提高，或由於部署需求或法規的影響，而產生盲點。

隨著人們對於隱私權和政府窺探的擔憂日增，不斷成長的 SSL 流量，在可預見的未來也將持續增加。今日許多具有領導地位的網站，包括 Google、Facebook、Twitter 和 LinkedIn，都加密了其應用程式流量。不只是網路龍頭才會加密其通訊內容；2014 年，在百萬個最熱門的網站中，使用 SSL 網站的數目，比一年前增加了 48%。[7]

隨著 SSL 流量內容佔所有網際網路傳輸量的比例不斷提高，IT 安全團隊在評估 SSL 檢查解決方案時，也必須考量到效能的需求和未來的頻寬使用量。安全團隊也應確定自己所提議的架構，符合健康保險可攜性及責任法案 (HIPAA) 等法規的要求。

2 Gartner「展望：全球資訊安全產業，2012-2018 年」，2014 年第 3 季更新
3 Gartner「資安領導者必須因應 SSL 流量遽增所帶來的威脅」，2013 年 12 月
4 Gartner「資安領導者必須因應 SSL 流量遽增所帶來的威脅」，2013 年 12 月
5 NSS Labs，「SSL 效能問題」，2013 年 6 月
6 NSS Labs，「SSL 效能問題」，2013 年 6 月
7 Netcraft，「2014 年 1 月 Web 伺服器調查」

選擇 SSL 檢查平台時應注意的五大特色

由於 SSL 檢查機制可能涵蓋了眾多不同的安全產品，包括從防火牆和入侵防禦系統 (IPS)，到資料外洩防護 (DLP) 和進階威脅預防系統等，因此企業組織必須制定一系列標準，並藉此評估 SSL 檢查平台後，再行選擇解決方案。本白皮書說明了所有 SSL 檢查平台都應該具備的五項功能，有助於 IT 安全團隊迅速界定評估標準，並避免常見的部署陷阱。

「若要阻止網路攻擊，企業組織必須對加密資料進行深入解析……因此需要**專屬安全性平台來針對進出的 SSL 流量實施解密。**」

SSL 檢查平台應該能夠：

1 滿足目前與未來的 SSL 效能需求

「效能」或許是評估 SSL 檢查平台的首要標準。企業組織必須評估自己目前的網際網路頻寬需求，並確定其 SSL 檢查平台能夠處理未來的 SSL 傳輸量需求。

從 2013 到 2018 年，IP 傳輸量預計每年增長 21%[8]，因此企業組織也必須考慮 SSL 流量的成長。SSL 流量目前佔所有網際網路流量的 25% 到 35%，在某些網路的比例則高達 70%。[9] 此外，加密流量增加的速度，比整體 IP 流量的成長還快，而且越來越多的網站採用需要大量運算的 4096 位元 SSL 金鑰和迪菲 - 赫爾曼 (Diffie-Hellman) 加密法。

在評估 SSL 檢查效能時，IT 安全團隊應該要：

使用 2048 和 4096 位元的 SSL 金鑰，**來測試 SSL 的檢查速度**。

使用 Diffie-Hellman 和橢圓曲線加密法，**來評估混合的流量**。

為尖峰時間的傳輸量保留額外的餘量，**以確保 SSL 檢查平台能夠處理傳輸量需求**。

啟用必要的安全與連網功能，**以分析設備效能**。在測試 SSL 解密速度時，如果未考慮到深度封包檢測 (DPI)、URL 分類或其他功能，將無法清楚瞭解實際效能。

充分評估效能基準的企業組織，在面對生產環境時將不至於有太大的落差。

8 Cisco，「Zettabyte 的年代：趨勢與分析」
9 NSS Labs，「SSL 效能問題」，2013 年 6 月

2 滿足合規性要求

隱私權和法規考量，已成為讓企業組織無法檢查 SSL 流量內容的頭號障礙之一。在 IT 安全團隊部署各種產品，以偵測攻擊、資料洩漏和惡意軟體活動的同時（理所當然應該這麼做），也必須在保護員工和智慧財產權之間拿捏分寸，避免侵犯員工的隱私權。

「為了滿足法規的要求……SSL 檢查平台應能避開內容敏感的流量……」

為了因應法規的要求，例如 HIPAA、聯邦資訊安全管理法 (FISMA)、支付卡產業資料安全標準 (PCI DSS) 和沙賓法案 (Sarbanes-Oxley, SOX) 等，SSL 檢查平台應能避開敏感的流量，例如傳輸至銀行和健康醫療照護網站的內容。略過內容敏感的流量，可讓 IT 安全團隊放心，因為機密的銀行或醫療記錄將不會傳送至安全裝置，或儲存於日誌管理系統。

IT 安全團隊應尋找具備下列功能的 SSL 檢查平台：

- 使用自動化的 URL 分類服務，來將網站流量分類。透過將網站內容分類，機構可略過與銀行和健康醫療照護網站的通訊，並確保機密資料維持加密狀態。
- 支援手動定義的 URL 避略清單，其中包含成千上萬筆的 URL 記錄。
- 在使用者首次上網時，顯示量身打造的訊息，告知其網頁傳輸和加密的流量可能會受到監控，以防止網路威脅和未經授權的活動。

偵測加密的惡意軟體、避免內部人員的濫用，以及透過 SSL/TLS 傳輸的攻擊行動

3 滿足異質網路的各種部署與安全要求

企業組織必須對抗各式各樣的安全威脅，而這些威脅可能來自外部勢力或心懷不滿的員工。為了保護其數位資產，企業組織必須部署越來越多的安全產品，以阻止入侵、攻擊、資料外洩和惡意軟體等威脅。

這些安全產品有的是內嵌部署，有的則屬於非內嵌型態，只做為被動的網路監控器。有些產品分析所有網路流量，有些則只分析特定應用內容，例如 Web 或電子郵件通訊協定。不過，幾乎所有的安全產品，都必須以明文形式來檢查流量，以偵測不法活動。

因此，SSL 檢查平台應能與多家廠商所提供的各種安全產品互通。這些平台應可進行透明的部署，也能使用流量導向功能，將來自某個安全裝置的流量轉傳至另一個裝置。

「……SSL 檢查平台應能**與多家廠商所提供的各種安全產品互通。**」

企業組織應尋找具備下列功能的 SSL 檢查平台：

- **可針對外傳至網際網路和傳入企業伺服器的流量，進行解密的動作，並提供多種彈性的部署選項。**平台應支援通透式正向代理和外顯式代理配置，前者能夠以透明的方式截取流量，後者需要在瀏覽器中加以明確設定，使用代理程式。平台也應支援反向代理部署，將解密後傳送至企業伺服器的流量，並允許內嵌或非內嵌的安全裝置檢查流量。
- **利用流量導向功能，聰明轉傳流量。**SSL 檢查平台應可根據來源 IP 位址、通訊協定、檔案類型、URL 或其他參數，將流量轉傳至多個安全裝置。透過先進的流量導向功能，SSL 檢查平台可達成最佳化的網路安全裝置效能，並支援複雜的網路架構。
- **根據自訂的規則，以精細分級的方式來剖析和控管流量。**透過對第 7 層流量，進行可編程的程式化控管，管理員可檢查要求的標頭，並進行任意次數的動作，包括封鎖傳輸、將流量重新導向，或是修改內容。
- **與領導廠商所提供的各種安全解決方案整合。**透過驗證互通性，IT 安全團隊可確保其 SSL 檢查平台，將能與其他安全解決方案無縫地共同運作，並避免發生延遲部署工作的未預期問題。透過與各種安全解決方案的整合，企業組織也不需再部署多點解決方案，進而可降低成本。

企業組織希望部署由多家廠商提供的最佳安全產品，且不希望受限於使用單一廠商的解決方案。安全形勢不斷地演變，必須持續對抗新出現的威脅。在一、兩年內，企業組織可能想備置新的安全產品，並需要確定其 SSL 檢查平台可與這些產品互通。

如果所選擇的 SSL 檢查平台，能夠進行彈性的部署，並具備流量導向和精細分級的流量控管功能，企業組織就能在未來建置中避免受限於選擇 \ 安全解決方案。

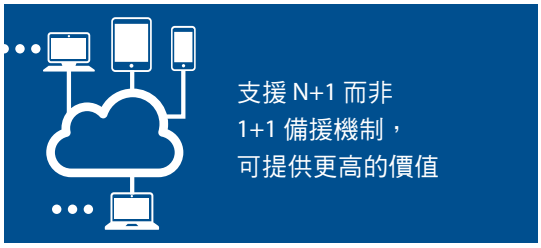
「……SSL 檢查平台不應只是分攤安全裝置的 SSL 處理工作，**也應協助達成這些裝置的最大正常運作時間和最高效能。**」

4 達成安全基礎架構的最大正常運作時間與最高整體能力

企業組織仰賴其安全基礎架構來阻斷網路攻擊，並防止資料外洩。如果其安全基礎架構失效，可能就會偵測不到威脅，使用者也無法執行業務關鍵的工作，而造成營收的損失和品牌形象的損害。

今日大多數的防火牆，都能以精細分級的方式，控制對應用程式的存取，並偵測入侵活動和惡意軟體。遺憾的是，分析網路流量以偵測網路傳播的威脅，這項工作將會耗用許多的資源。防火牆的功能雖然會與時俱進，但經常無法跟上網路的需求，尤其是當網路啟用了多項安全功能時（例如 IPS、URL 過濾和病毒偵測）。

因此，SSL 檢查平台不應只是分攤安全裝置的 SSL 處理工作，也應協助達成這些裝置的最大正常運作時間和最高效能。在評估 SSL 檢查平台時，機構應尋找具備下列功能的平台：



SSL 檢查平台不應只是另一個單點產品，也不應帶來網路的風險，而是能夠達成最高可用性，及安全基礎架構的最大整體能力，進而降低風險。如此，企業組織才能完全發揮其 SSL 檢查平台的能力。

「……SSL 檢查裝置必須**能夠安全地管理 SSL 憑證和金鑰。**」

5 以安全的方式管理 SSL 憑證和金鑰

無論是提供外傳或傳入 SSL 流量資料的能見度，SSL 檢查裝置都必須安全地管理 SSL 憑證和金鑰。SSL 憑證和金鑰是加密通訊信任機制的基礎，如果遭到入侵，攻擊者將可利用這些資訊來冒充合法網站，並竊取資料。

在企業應用程式的前端部署 SSL 檢查裝置，以檢查傳入的資料時，這些裝置可能需要管理成千上百的憑證。隨著 SSL 金鑰與憑證組合的數量增加，憑證的管理也變得更具挑戰性。企業組織會持續不斷地新增、移除或重新安裝伺服器，以滿足業務的需求。這種多變而動態的環境，讓企業組織難以管理特定時點的所有 SSL 憑證，並確認憑證是否過期。

為了確保以安全的方式儲存和管理憑證，企業組織應尋找具備下列功能的 SSL 檢查平台：

可提供裝置層級的控管機制，**以保護 SSL 金鑰和憑證**

可與第三方的 SSL 憑證管理解決方案整合，進而**找出憑證，並加以分類、追蹤和統一管理**

支援 FIPS 140-2 第 2 級和第 3 級認證設備與硬體安全模組 (HSM)，這些設備能夠**偵測實體的篡改動作，並保護加密金鑰**

結論

人們對於隱私權的關切，推升了 SSL 的使用量；企業面臨日增的壓力，必須加密應用程式的流量，並保護資料的安全，使其免於遭到駭客和外國政府的竊取。此外，由於 Google 讓 HTTPS 網站的排行高於標準網站，因此應用服務的業主皆爭相加密其流量。但是在對抗網路攻擊和惡意軟體等威脅時，IT 安全團隊面臨了自己的一連串挑戰，因為這些威脅可以利用加密機制，來略過企業的防禦系統。

隨著 SSL 佔了企業傳輸量接近三分之一 10，以及越來越多的應用採用 2048 和 4096 位元 SSL 金鑰，企業組織無法再避免無法忽視的加密課題。如果企業組織想防止毀滅性的資料外洩事件，就必須深入解析 SSL 流量內容。為了達成這項目標，企業組織需要專屬的 SSL 檢查平台。

本指南說明了在佈建 SSL 檢查技術之前，企業組織所應考量的評估標準，像是效能、可用性和 SSL 金鑰管理等，將會是成功的關鍵。取得了這些資訊，企業組織就能進行掌握充分訊息的決策，避免落入 SSL 檢查可能會遭遇的部署陷阱。

瞭解更多資訊

若要瞭解關於 A10 Networks SSL 檢查解決方案的詳細資訊，請造訪
https://www.a10networks.com/products/ssl-decryption-encryption-and-inspection-ssl-insight

10 NSS Labs，「SSL 效能問題」，2013 年 6 月

關於 A10 Networks

A10 Networks 是應用網路的領導者，提供一系列的高效能應用網路解決方案，協助組織確保他們的資料中心應用和網路保持高度可用性、快速和安全。A10 Networks 於 2004 年成立，總部位於加州聖荷西 (San Jose)，在全球都有為客戶提供服務的辦事處。如需詳細資訊，請造訪：**www.a10networks.com**

企業總部

A10 Networks, Inc
3 West Plumeria Ave.
San Jose, CA 95134 USA
電話：+1 408 325-8668
傳真：+1 408 325-8666
www.a10networks.com

零件編號：A10-WP-21116-EN-02
2015 年 10 月

全球辦事處

北美
sales@a10networks.com

歐洲
emea_sales@a10networks.com

南美
latam_sales@a10networks.com

日本
jinfo@a10networks.com

中國
china_sales@a10networks.com

台灣
taiwan@a10networks.com

韓國
korea@a10networks.com

香港
HongKong@a10networks.com

南亞
SouthAsia@a10networks.com

澳洲 / 紐西蘭
anz_sales@a10networks.com

如需深入瞭解 A10 Thunder 應用程式服務閘道器及其改善業務的方式，請聯絡 A10 Networks：**www.a10networks.com/contact** 或來電諮詢 A10 業務代表。