消除SSL盲點的 6 大關鍵

SSL 檢 測 需 知

惡意流量可能正在存取您的系統

SSL的使用每年都一直在穩步增長，據估計到**2016**年時將有**67%**的網路流量為加密流量[1]。不幸的是，並非只有那些具安全意識的企業和用戶正開始轉向加密，駭客亦正在利用它來掩蓋其不當行為。雖然許多防火牆和威脅防護解決方案都能夠解密SSL流量，他們卻無法跟上不斷變化的解密需求。

如果駭客入侵企業網路，企業將面臨網路中斷、業務危機、客戶反彈，以及智慧財產權受損害。再加上高昂的成本損失，修復漏洞和修復企業聲譽造成的損害。

不爭的事實是：若沒有到位的**SSL**檢查，您的企業組織即是暴露在被攻擊的風險中。藏匿在加密流量中的駭客可以滲透到您的網路，安裝惡意軟體，並在多個端點竊取關鍵資料。

對付隱藏在SSL加密流量的惡意行為，最好的防禦便是能同時滿足以下6大關鍵需求的SSL檢測平台，

1. Sandvine Global Internet Phenomena Spotlight: Encrypted Internet Traffic report, May 2015.

防止駭客入侵的
6 大關鍵

評估潛在可合作的SSL檢查平台夥伴時，企業應謹記幾項要點 –
性能、**合規性**、**可用性**和**安全性**。
一個有效的SSL檢查平台應達到以下幾點：

01.

滿足SSL性能需求

在企業中任何新的解決方案，**性能均為一大關鍵**，尤其當該解決方案必須**不斷跟上持續增加的負載**時，性能就更為關鍵了。為確保SSL檢測平台的性能可以滿足當前和未來需求，企業必須:

- 測試SSL檢測功能於2048位元和4096位元SSL金鑰的速度
- 使用橢圓曲線加密演算法來評估
- 確認該平台可以處理的吞吐量可滿足需求，並可應付突發的流量高峰時的需求值

02.

滿足合規性任務

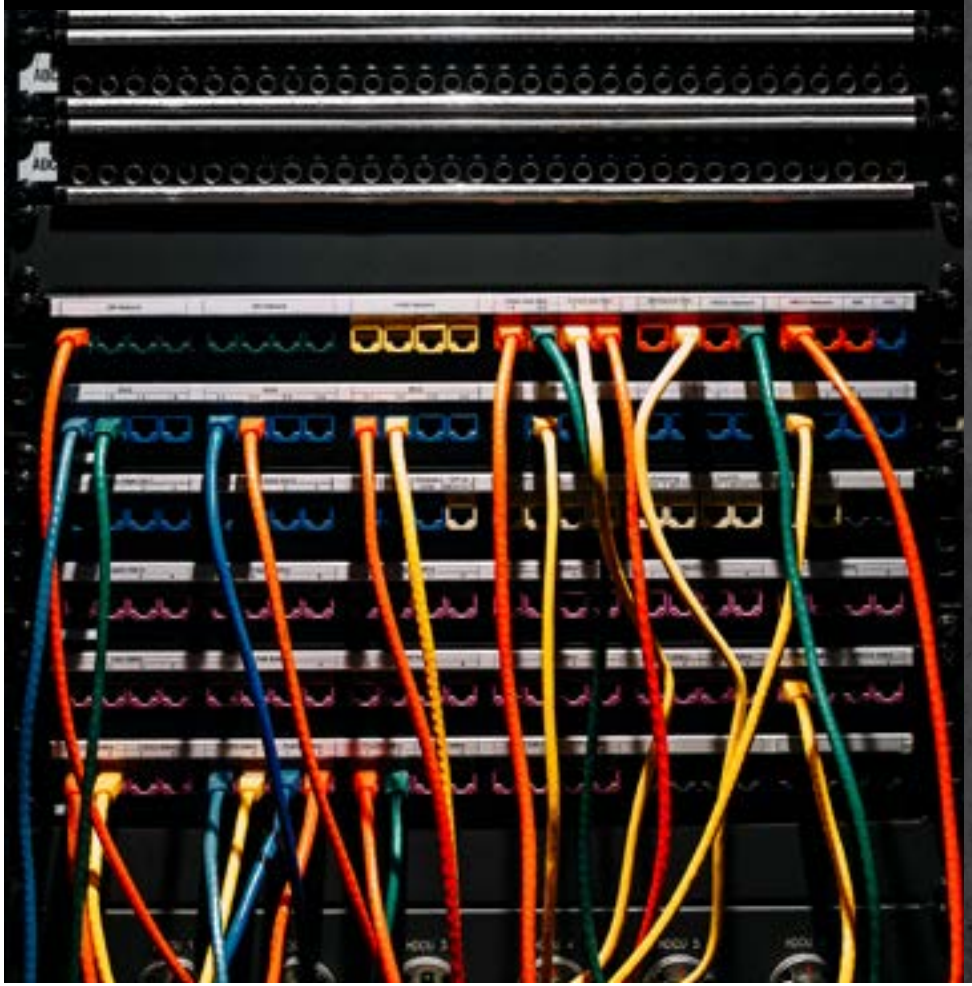
因為一些當地法律、法規如HIPAA和SOX，以及美國電子通訊隱私法 (ECPA) 等為了保護資料隱私的措施設立，**企業必須符合各種合規標準**。堅持這些法律也就意味著，許多企業 — 如金融和醫療保健相關產業，必須避開敏感的流量。

為了保持合規性，同時能檢查SSL流量，IT安全團隊應該尋找的平台應該要能:

- 按網站流量類型分類，確保機密數據，如針對醫療保健和銀行網站間溝通的訊息，仍保持加密狀態
- 支援自動更新及手動定義的URL繞過清單

03.

支援複雜的部署需求



為了試圖保護所有的安全基礎，大多數企業已經部署了許多來自多個供應商的安全設備。**SSL檢測平台應該要能為這些設備解密流量**。要做到這一點，SSL檢測平台必須:

- 對出去到互聯網的流量與進到公司內部伺服器的流量進行解密
- 以進階的流量控制引導流量到多個安全設備
- 整合各個領導廠商的安全解決方案

04.

最大限度地提高安全基礎設施的正常運行時間和能力

安全基礎設施需保持啟動且完全可用狀態以阻擋網路攻擊，及防止資料外洩。如果安全基礎設施發生故障，威脅可能無法被發現而導致嚴重的攻擊，進而造成收入損失和品牌的損害。**一個有效的SSL檢查平台應能透過最大限度地提高現有安全基礎設施的正常運行時間，來降低風險**。此平台須能滿足以下幾點:

- 可以使用負載平衡來擴展安全設備的部署
- 透過偵測和繞過故障的安全設備周圍，避免網路運行中斷
- 支援進階監控，以迅速判定網路或應用程式錯誤

05.

安全地管理SSL憑證和金鑰

SSL 使用憑證和金鑰為加密通訊形成信任的基礎。如果受到威脅，攻擊者可以利用它們來竊取資料。作為提供進出互聯網的SSL流量可視性的一部分，**SSL檢測平台必須能夠安全地管理數百個至數千個SSL憑證和金鑰**。一個有效的SSL檢測平台應該能夠:

- 保護存儲在SSL檢測平台上的SSL金鑰
- 整合第三方SSL憑證管理解決方案，發現和控制憑證
- 支援FIPS 140-2 Level 2 和 Level 3 金鑰管理

06.

解密所有符合標準的加密流量

不單單是加密流量日益增加，企業組織和攻擊者使用的密碼複雜程度也逐漸升高。**如4096位元SSL金鑰，橢圓曲線密碼，完全順向機密(PFS)，以及其他技術均正在落實到位，以防止窺視**。要能符合這些需求，SSL 檢測平台應要能:

- 支援4096位元SSL金鑰長度和進階的SSL和TLS加密算法
- 解密所有資料，包括 SSL重複傳送(retransmissions)
- 當流量被無法解密進行告知

對於惡意加密流量，您的企業最好的防禦便是確保你有一個可以滿足這6大關鍵的SSL檢測平台。倘若您正依靠的平台尚不符合這些要求，您的企業將有可能面臨部署陷阱和外來威脅。

A10 Networks® Thunder® ADC 產品線中的 SSL Insight™ 功能可以透過分析所有網路資料(包括加密數據) 提供您的企業最完整全面的威脅防禦。

A10 SSL Insight 可讓您的企業:

- 透過高速解密SSL流量**消除企業防禦盲點**
- 透過負載平衡第三方安全設備使**正常運行時間最大化**
- **擴展性能和傳輸量**，從而成功地對付網路攻擊
- 透過快速檢測進階威脅，**防止成本高昂的資料外洩和知識產權的損失**

如果您的SSL檢測平台稍有不足，您的企業就可能會是下一個被攻擊的受害者

想了解更多關於A10 Thunder ADC如何幫助您的企業檢測加密流量的威脅，並保護關鍵數據和系統，請瀏覽 **www.a10networks.com/adc-security**或聯繫各地業務代表。

關於 A10 Networks

A10 Networks 睿科網路是全球應用網路技術領導廠商，提供一系列高性能應用網路解決方案，協助數以千計的大企業、服務供應商和超大型網路營運商確保其資料中心的應用程式與網路保持高可用性、加速性和安全性。A10成立於2004年，總部位於美國加州聖荷西市，並在世界各地設有辦事處為客戶提供服務。詳細資訊請瀏覽: **www.a10networks.com**

Part Number: A10-EB-14101-TW-01 OCT 2015