# 揪出 HTTP/HTTPS 潛藏的危害

## 眾至新世代 UTM 針對 HTTPS 加密流量分析、過濾

近幾年來，各種 Web 2.0 運用與雲端服務，已逐漸取代傳統的應用程式，成為多數使用者習慣的網路操作工具。例如：Facebook、雲端免費儲存硬碟、Gmail、社群工具、搜尋引擎、即時訊息 APP，以及各類線上影音服務等，不僅讓使用者能便利入手，也能更快速分享資源。各種網路服務的興起，顛覆大家對網路操作習慣，而這些熱門的應用卻也成為惡意程式、病毒攻擊的最愛，透過這些服務模式，針對企業內部的主機、個人電腦植入木馬程式，進行竊取、攻擊行為。

## HTTP (80 埠) 與 HTTPS (443 埠) 是企業無法禁止的網路服務

同樣的情形也發生在 HTTP (80 埠) 與 HTTPS (443 埠) 的攻防戰上，因為使用者透過網路做存取動作是最方便的。對企業來說，再如何對網路做嚴密防範，在防火牆上還是必須打開 80 埠與 443 埠。然而一開放之後，對網路管理安全而言就等於開放了一個通道，讓蠕蟲、惡意程式、病毒、Botnet 攻擊有了滲透的管道。由於傳統 HTTP (80 埠) 連線，很容易遭到有心人士側錄、攔截或竄改用戶端端之間的傳輸內容，所以越來越多的網站服務採取 HTTPS，希望提升用戶端與網站之間的存取安全性，因為 HTTPS 是搭配安全加密技術的 HTTP 連線，可保護網站與用戶端之間的傳輸內容。然而，當這些網站全程都使用 SSL / TLS 加密服務時，很多資安管理的潛在危機就慢慢開始浮現了。

## HTTPS (443 埠) 潛在危機，危害企業網路安全

當採用加密連線服務時，企業 IT 網管人員可能只會知道，使用者有連到某一個 IP 位址，頂多可以再多了解其傳送的資料量、TCP 的連線數。但是裡面到底傳了哪些東西並不知道，這樣就很容易讓惡意攻擊伺機滲透到企業內部，或者管理者在渾然不覺的狀態下，讓公司機密的資料被傳送到外面去。當這些問題慢慢浮現時，也逼著管理者不得不去面對，如果企業內部的使用者存取網路的連線也是全程加密，但是本身的網路防護設備(例如：防火牆、入侵偵測設備、防毒牆)無法針對這些加密流量進行檢測，就會出現資安漏洞，因此企業強化本身的防護管制能力，已勢在必行。


台中總公司　04-2705-0888
台中市西屯區西屯路二段256巷6號3F-6

台北分公司　02-2501-1185
台北市中山區松江路129號6F-2

高雄分公司　07-229-8788
高雄市新興區民權一路251號8F-6

免付費專線　0800-666-188
官方網站 | www.sharetech.com.tw
銷售諮詢 | sales@sharetech.com.tw
技術支援 | help@sharetech.com.tw

## 眾至新世代 UTM 支援 HTTPS 加密流量偵測

以目前最好的解法就是在網路閘道端口，設法管控、偵測 HTTPS 流量與傳輸的內容，透過防火牆或 UTM 設備來處理，但是以目前能夠偵測、解析 SSL 加密連線流量這類型的資安設備，大多都是國外品牌的次世代防火牆。然而，眾至推出的新世代 UTM，同樣具有國際資安防護等級加密偵測、監控或控制阻擋功能。以臉書 (Facebook) 而言，它是一種應用程式，臉書交談 (Face Chat) 也是一種應用程式，對眾至新世代 UTM 而言，他們都可以個別獨立被偵測、監控與管制，可執行 SSL 流量的解密與重新加密，且 HTTPS 過濾，除了不僅掃描 SSL 流量中是否有包含病毒或惡意程式外，還可以針對使用者所開啟的 URL 網址進行過濾。