IT安全性不能以一種方案「一體適用」

Jezmynn Koh, 2015-04-08

This is adapated from the original post by Matt Miller.

今天的安全局勢具有高度複雜化的傾向，原因大致上可以歸咎於日益複雜化的網路攻擊本質，特別是從管理者的觀點來看。例如，分散式拒絕服務攻擊(DDoS)現在已達到400Gbps速度，目標包括網路和應用層。很顯然的，攻擊者持續進化，開發其他方法來繞過包括防火牆等傳統安全防護。

對於面對應用層DDoS攻擊威脅的企業而言，必須克服的挑戰在於如何區分人類流量與魁儡(bot)流量。

再者，攻擊背後的動機越來越複雜，特別是從政治與經濟觀點而言。例如，美國國家安全局(NSA)洩密案 - 前僱員Edward Snowden洩漏了包括美國、英國、澳洲、加拿大和紐西蘭等國政府的機密資訊 - 此一事件確實提醒了我們必須重視駭客活動。另外，現在IT安全的最大威脅之一就是組織化的網路竊盜與詐欺，因為那些聰明的犯罪者越來越了解可以藉由線上犯罪獲取可觀的財務利益。

因此，確保擁有適切的防護以杜絕網路攻擊，已成為企業的一項關鍵課題。一個有效的安全策略必須涵蓋員工存取的所有裝置、應用程式和網路，並且跨越企業本身的基礎設施。傳統安全方法例如新一代防火牆和被動回應的安全措施，已無法有效的對抗新類型的攻擊。現在的安全性非常重視對於應用程式的保護，以及使用者身分識別的加密和保護措施，而比較不偏重於基底的網路基礎設施。這是因為網路基礎設施已演變得比較沒那麼靜態，並且也已被證明它只是用來運行複雜應用程式的一個載具。

企業需要的是一個彈性且完整的安全策略，必須有能力將DNS安全性與DDoS保護、網路防火牆、存取管理、應用安全性等結合智慧型的流量管理。

Frost & Sullivan的一項報告(Frost Industry Quotient)指出，市場呈現了朝Web應用防火牆(Web Application Firewall; WAF)與應用交付控制器(Application Delivery Controller; ADC)平台整合的發展趨勢，而這促使F5針對應用交付市場開發了一個稱為F5新融合架構(F5 Synthesis)的新觀點。此一觀點提供了一個高效能分散網路架構(high performance network fabric)，為一個應用的基本單元(網路、DNS、SSL、HTTP)提供保護以防範複雜的DDoS攻擊威脅。

F5新融合架構透過業經測試的參考架構，在客戶朝軟體定義資料中心(software defined data centres; SDDS)轉移的過程中確保應用安全與可用性。再者，F5的DDoS防護方案提供目前市場上最完備的攻擊防護。DDoS攻擊的平均速度達到2.64 Gbps，而升級到F5的BIG-IP平台後，伺服器將能處理高達470 Gbps的攻擊威脅。這不僅提供了充裕的頻寬以舒緩DDoS攻擊，而且其額外的容量讓線上公司可以維護正常的商務營運 - 即使是在遭受攻擊的期間。

安全性不再是一種「一體適用」的方案。終端使用者期望擁有高效能服務，而企業必須確保他們所部署的安全方案不會變成一個瓶頸。我們可以預期見到多維(multi-dimension)或「雞尾酒」式的攻擊出現，亦即DDoS攻擊結合應用層攻擊與SQL安全弱點威脅。因此，傳統防火牆不再是一個有效的安全防衛，企業需要採行一種多堆疊的安全方法，並結合內部控管程序。面對來自不同裝置和多重面向的攻擊威脅，單一用途安全設備將被高功能的多用途設備取代。

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com