取代Microsoft TMG的最佳方案

打造高安全的資安防護架構 Sophos UTM扮演核心角色

在市面上眾多資安產品之中，唯有Sophos UTM與Microsoft TMG的相容性接近100%，可以在不需要調整企業網路架構的前提下，協助企業無縫轉移，有效防堵駭客入侵事件發生

繼終止Windows XP技術支援之後，微軟又預計在2015年4月停止對Microsoft Threat Management Gateway（TMG） 的技術支援，也不再推出相同類型的後繼產品，此舉對已經採用該產品多年的企業用戶而言，唯一解決之道便是尋找其他資安廠商的替代方案，才能避免在微軟終止技術支援之際，遭到駭客趁隙而入。而在市面上眾多資安產品之中，唯有Sophos UTM與Microsoft TMG的相容性接近100%，可以在不需要調整企業網路架構的前提下，協助企業無縫轉移，有效防堵駭客入侵事件發生。

Sophos技術經理詹鴻基表示：「市面上有不少號稱可以取代Microsoft TMG的產品，但是仔細檢視功能之後，會發現其實都還需要外接其他設備。相較之下，Sophos UTM不僅功能相容性接近100%，而且防護功能更為強悍，加上我們的研究團隊會定時發佈最新威脅資訊，足以應付來自四面八方的資安威脅。」

Sophos UTM功能完整 備受Gartner研究報告肯定

從防毒軟體起家的Sophos，發現企業內部單點防護設備愈來愈多後，會造成資訊人員工作上的困擾，所以推出以一個模組化設備滿足全方位資安防護的Sophos UTM，功能涵蓋防火牆、VPN、IPS、電子郵件安全、網頁過濾和應用程式控制，是市面上少見功能完整、足以保護企業安全的資安產品。值得一提之處，在於操作介面採用直覺式的瀏覽器介面，完全沒有指令行介面、也不需要安裝用戶端軟體，即可快速完成參數的調整，而且各型號之間的功能都相同，因此即使是購買最基礎型號的小企業，亦可得到與大型企業相同的保護機制。

正因為如此，Sophos UTM在Gartner 2014 UTM魔術象限報告中，便被評為最簡單易用的設備，對缺乏專屬安全人員的中小企業，可以大幅降低設備設定上的難度，無須擔心參數調整的問題。其次，在不斷進步的硬體效能加持下，Sophos UTM也已經足以應付5,000人以上的大型企業使用；加上支援多國語言的操作介面，至今被廣泛安裝在60個國家中，保護超過100,000個網路環境以上。

Sophos技術經理 詹鴻基

詹鴻基解釋：「在新一代高效能硬體的加持下，Sophos UTM已經足以應付數千人以上的大型企業，能有效降低IT人員管理上的困擾。至於一般人誤以為UTM效能不彰的原因，通常來自於購買到不適宜的型號，以及沒有針對企業實際狀況來進行合適的評估(Sizing)。而Sophos與合作伙伴都會先深入瞭解企業需求之後，再推薦適合的機種，並且協助完成各項參數調整，確保Sophos UTM能夠發揮預期的防護措施。」

無縫取代Microsoft TMG 首選Sophos UTM

微軟自多年前跨足資安領域後，Microsoft Forefront TMG 2010便因為內建防火牆、網頁過濾、入侵偵測、VPN、Reverse Proxy等功能，加上價格非常經濟實惠，因此成為許多偏愛微軟產品、預算有限的企業用戶，建構資安防護往的選擇之一。尤其對公司內部已經有防火牆、入侵偵測等設備的企業，亦可只開啟Reverse Proxy的功能，透過黑名單過濾機制的方式，避免用戶端連上惡意或色情網站，除可降低駭客入侵的機率之外，亦可減少對其他資安設備的工作負擔。

在微軟宣布將在2015年4月停止對Microsoft TMG的技術支援之際，市面上有許多UTM品牌為搶食此換機潮，號稱可以協助企業做到無縫轉移；只是多數設備都缺乏Reverse Proxy的功能，即便有類似功能存在，也需要修改企業網路架構才能使用，要完全取代Microsoft TMG實有相當的困難，導致目前仍有許多客戶在轉換TMG到其他產品仍佇足不前。

「相較於其他品牌，Sophos UTM不僅內建Reverse Proxy的功能，而且其他功能也幾乎達到100%的相容性。」詹鴻基：「為降低企業轉移到Sophos UTM的難度，我們還在操作手冊中，詳細記載如何將在Sophos產品中啟動與Microsoft TMG相同的功能，甚至還包含參數的調整等等，資訊人員只需要按部就班設定，即可不需要更動企業網路架構。」

Sophos主動收集資安訊息 協助企業阻擋APT攻擊

Sophos UTM不僅僅是取代Microsoft TMG的最佳方案，還有許多先進的資安防護功能，如可集中管理所有端點上的防毒軟體和裝置，確保端點無論在何處都能保持最新防護狀態。此外，Sophos UTM也是第一款通過 VMware Ready 和 Citrix Ready 認證的UTM產品，因此可以在 Microsoft Hyper-V 和 KVM 虛擬環境中執行，可應付日益複雜的網路環境。

尤其在駭客慣用以APT手法攻擊企業的今日，Sophos UTM也因能夠即時更新最新威脅資訊，確保企業免於資安威脅之中。詹鴻基說：「我們擁有運作超過 25 年全球威脅情報分析實驗室的經驗，在全球有很多收集威脅事件的端點設備，不僅會透過雲端管理平台進行即時分析，還會立即將資料傳送給Sophos UTM等相關資安產品，因此可以有效阻擋APT攻擊或零時差攻擊等等，成為建置企業打造資安防護架構的最佳幫手」

隨著全球資安威脅日益嚴重，以及微軟終止Microsoft TMG的時間愈來愈近，企業不妨考慮以Sophos UTM作為企業資安防護架構核心，一來可降低資安設備管理的負擔之外，亦能在資安威脅頻傳的時代下，避免發生機密資料被竊取的狀況。