強化校園網路防禦 阻絕安全威脅與攻擊

嘉南藥大以新世代防火牆控管校園網路安全

文◎沈欣蓓

有鑑於傳統防火牆與既有整合型UTM設備的效能不彰，位於台南的嘉南藥理科技大學在日前採用了Palo Alto的新世代防火牆（NGFW）作為校園網路的第一道把關，除了改善過去常遭受到的網路攻擊事件之外，在兼顧網路效能與安全性方面，該單位也從新世代防火牆中獲得了平衡與滿足。接下來讓我們看看，實際評估與採用的過程如何。

問題龐雜的校園網路

學校樹大招風的特性與學生使用網路的方式，讓校園網路向來問題繁雜難以管理，嘉南藥理科技大學也不例外，嘉南藥理科技大學圖書資訊館網路資訊組王調榮即表示：「過去我們曾遇過不少網路攻擊，像是只要遇到學校特殊日子就會發動的安全攻擊、使用者打開學校網站時出現即時通訊QQ的廣告視窗等等，所以當安全設備進入汰換期，我們便決定換掉既有的整合型UTM設備，並評估新的防火牆產品。」

王調榮說，早期嘉南藥大遇到的網路安全事件，一年至少20件，頻率之高讓網管人員頭痛不已，他舉例，有一次發現學生只要輸入學校網域名稱進入學校網站，就出現即時通訊QQ的廣告視窗，網管人員仔細檢查網站主機後，卻沒有發現網路安全問題，最後才知道原來問題是源自校園內部網路使用者的電腦，「這樣的情況發生後，我們一一比對log紀錄，並將異常使用行為以阻擋的方式防堵了這個問題，也就是阻斷使用者連線存取中國該網站。」

王調榮表示，既有UTM對於網路攻擊與安全威脅的過濾與控管能力不足以應付學校網路安全事件，雖然能夠消極被動地阻斷有問題的網路連線，卻因為無法偵測到諸如此類的攻擊行為，而只能達到事後解決，無法提供事前防範能力。

此外，為了符合智慧財產權的規範，嘉南也明定全面禁止P2P應用程式，「傳統防火牆與UTM設備可以阻擋主流P2P應用程式，但是越來越多元的P2P應用程式則防不勝防。」而這些都是嘉南藥理科技大學亟待解決的網路政策與安全問題。

測試與導入過程 即時解決問題的特性受肯定

在採用Palo Alto新世代防火牆之前，嘉南挑選了市場上主流的各家解決方案進行實際環境測試與評

▲（圖左至右）嘉南藥理科技大學圖書資訊館網路資訊組王調榮、陳政文、陳進祥。

估，王調榮說，學校和企業環境不同，會遇到的網路安全問題也不盡相同，因此還是實際測試學校的主機設備與網路環境所遇到的安全事件，結果較為精準，在經過半年左右的測試期之後，嘉南決定選擇效能與安全表現最為符合嘉南需求的Palo Alto PA-4020作為新的防火牆設備。

通過測試之後，王調榮表示，導入期花了約4個月左右的時間，當中其實曾遇過問題，「當時是學校的選課日，卻發生防火牆異常忙碌的情況，CPU使用率接近100%、連線數則飆高到60至100萬（平日正常數值為5萬以內）。仔細一查，竟然是遭受到來自世界各地的DDoS攻擊。合作廠商便協助我們將過載連線阻斷。」

王調榮接著表示，雖然當下發生狀況，但Palo Alto的研發人員馬上幫嘉南調整設備，再重新上線使用，「重新調整設定之後，阻斷功能即可正常開啟使用。」他認為，此次事件讓嘉南發現Palo Alto的兩項好處，一是快速反應與解決客戶問題的能力，另一則是其硬體設計區分為Data Panel與Control Panel，即使設備過度負載，仍能進行即時反應與控制，而不會像傳統設備毫無招架能力。

有效防範網頁攻擊與殭屍網路

從嘉南藥理科技大學較常遇到的網路安全攻擊行為來看，其大多偏向網頁式攻擊形態，如SQL Injection、Cross Site Scripting等，另外嘉南藥理科技大學圖書資訊管網路資訊組陳政文也表示，學校常常成為殭屍網路（BotNet）的攻擊目標，而遭受殭屍網路攻擊之後，平時不會發作，卻在特定情況下很容易讓學校網路成為網路攻擊的一員，尤其在人力較少的特殊日（如選課日或寒暑假），更容易遭受此類攻擊，而讓學校受到檢舉與網路管理的困難。

「我們發現Palo Alto在防範網頁式攻擊以及殭屍網路的表現，相較於其他競爭廠牌來得優異，這也是我們選擇Palo Alto的原因之一。」王調榮進一步解釋，透過Palo Alto的程式命令中心（Application Command Center，ACC），網管人員能夠觀察網路上的各種應用程式和URL連結，進而以行為角度分析使用者使用行為，可有效預防潛在威脅發生。

▲位於台南市仁德區的嘉南藥理科技大學，學校樹大招風的特性與學生使用網路的方式，讓校園網路向來問題繁雜多變而難以管理。

王調榮強調，Palo Alto新世代防火牆識別使用者、內容以及應用程式的能力，讓學校網管人員比過去能更容易控管並預防網路安全攻擊事件，再加上其所提供的報表分析功能，也使其有利於事後稽核與追蹤使用。

「自從去年（2010）8月將該設備上線使用至今，我們爆發的資安事件從過去一年約20件的頻率，降到了0件。也就是說，採用Palo Alto到目前為止，並未發生任何資安攻擊事件（此指的是受到主管機關通報的資安事件）。顯見該防火牆的能力十分符合我們的需求。」嘉南藥理科技大學網路資訊組陳進祥也說，雖然仍有部分零星的自行發現與解決的資安攻擊，不過與過去相比，發生頻率也大幅降低。

王調榮最後表示，唯一希望原廠能夠再精進的地方在於原廠提供人力支援的即時性，他解釋：「嘉南藥理科技大學位於台南，而Palo Alto原廠與代理商都以北部為主，其他當地經銷商的技術支援能力較有限，雖然原廠與代理商會在特殊日提前提供人力現場支援，然而當突發事件發生時，仍可能無法馬上因應。」不過他也同意，隨著原廠在台灣深耕時間，相信在經銷代理體系的人力培養與調度上，也能夠有所改善。網管人