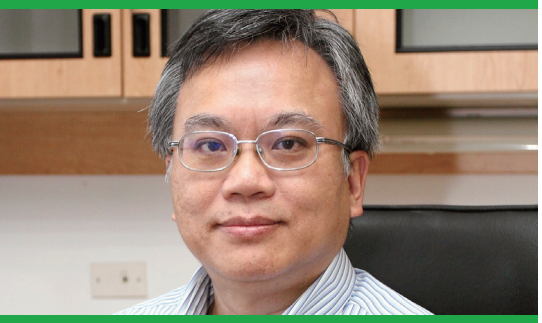
VMWARE 成功案例



長庚大學採用網路虛擬化平臺 VMware NSX 打造東西向安全防護機制

「長庚大學導入 VMware 網路虛擬化技術 NSX 來建立整體虛擬化環境的安全防護機制，並整合第三方資安管理工具，落實虛擬機安全管控政策，符合 ISO27001 資安規範要求。」

產業
教育業

位置
台灣 桃園市

主要成果

- 透過跨伺服器群組的邊界防火牆，以及在虛擬化環境中所建立的分散式防火牆，來對映兩者彼此的關係，並在分析網路流量的來源、目的地和通訊協定後，有效進行非法流量的阻絕防禦，提升虛擬環境的網路防護能力。
- VMware NSX 在分散式防火牆的管理可細微到虛擬伺服器內的網路卡。這樣的管控精細度對於全面虛擬化之後的網路管理完整性將有很大的助益。
- VMware NSX 平台功能運作的結果能提供即時的回饋資訊，作為修正相關設定的依據，主動改變相關的防禦措施等。

導入之 VMWARE 產品

- VMware NSX

單位介紹

位於桃園龜山的長庚大學，為台塑集團旗下的一員。校內共設有醫學院、工學院、管理學院、通識中心等超過 25 個獨立系所，以及 10 個以上的研究中心。全校學生人數約 7000 人 ,教職員則超過 1500 名。學校的資訊中心共有 11 位同仁，是國內積極推行雲端虛擬化工程的大學之一。

遭遇挑戰

長庚大學資訊中心主任張永華表示，長庚大學早在 2010 年就已經完成伺服器虛擬化環境的部署作業，而在 2014 年達成儲存虛擬化目標後，進一步投入軟體定義網路（SDN）規畫和建置。主要目的便是希望能讓 IT 資源的應用更有彈性，但也對導入 SDN 後如何與既有的實體網路架構互相搭配以達截長補短之效存有疑慮。因此，便聯繫 VMware 尋求專業團隊的協助，藉由進行概念性驗證（Proof of Concept，PoC）的機會尋求最合適的方案。

張永華強調，長庚大學導入網路虛擬化的目的，就在於其具有「彈性部署，有效運用」網路資源的特性；在整個網路環境中，虛擬機的數量越來越多，管理和環境的安全問題就會陸續產生，特別是虛擬機與虛擬機之間的資安防護，也是長庚大學針對 ISO 27001 資安管理策略需妥善因應的重點之一。因此，希望能透過導入網路虛擬化相關技術，將實體網路中的單一防火牆設備轉換為虛擬環境的分散式防火牆，建立更精細且可集中控管的網路安全管理架構。

VMware 解決方案

此外，張永華也強調，藉由網路虛擬化技術，防火牆也能夠在不同群組的虛擬環境下，達到資安隔離與管理，而且依據不同作業系統、不同地址、不同名稱等條件組合，能夠進一步定義出業務的相關性與排他性，建立一致的管控邏輯，大幅提升資安防護的精細度，和傳統實體資安設備比較起來，更具彈性和部署效率。

張永華指出，在釐清既有架構的不足之處與改善需求之後，長庚大學便和 VMware 團隊開始合作進行 PoC，過程中首先在實體網路 ESXi Server Pool 內建立了一個虛擬伺服器的封閉測試區。透過這樣的環境，不僅能測試跨伺服器群組的虛擬網路效能，也能驗證在虛擬環境內彈性部署與調整網路架構等關鍵項目。

張永華表示，PoC 有三項主要驗證內容。首先，執行面上，透過跨伺服器群組的邊界防火牆，以及在虛擬化環境中所建立的分散式防火牆，來對映兩者彼此的關係，並在分析網路流量的來源、目的地和通訊協定後，有效進行非法流量的阻絕防禦，提升虛擬環境的網路防護能力。而且在這樣的環境下，是否能有效支援各種通訊協定，具備支援動態與靜態路由的能力，符合長庚大學網路管理的要求。

其次，從效益面來看，VMware NSX 在提供網路虛擬化的功能中，分散式防火牆的管理可細微到虛擬伺服器內的網路卡。張永華指出，這樣的管控精細度對全面虛擬化之後的網路管理完整性將有很大的助益。

vmware®

麟瑞科技 RING LINE CORPORATION

「長庚大學導入 VMware 網路虛擬化技術 NSX 來建立整體虛擬化環境的安全防護機制，並整合第三方資安管理工具，落實虛擬機安全管控政策，符合 ISO27001 資安規範要求。」

長庚大學
資訊中心主任
張永華

第三，即便 VMware NSX 在資安管理上具備許多強大功能，而且這些功能是否方便使用與管理，以及這些功能運作的結果是否能提供即時的回饋資訊，作為修正相關設定的依據，主動改變相關的防禦措施等。這些都是期望藉由 PoC 獲得驗證的內容。

張永華指出，經過一系列包括防火牆驗證項目與情境、虛擬網路傳輸效能、部署與管理驗證等的測試後，結果都能符合長庚大學的需求。

事實上，在進行 PoC 之前，也有同仁提出質疑，在實體與虛擬網路並存的混合架構下，是否會造成互相衝突，甚至導致效能降低的狀況。對此，在完成了壓力與流量測試之後，結果顯示虛擬網路效能與實體網路差異並不大，而虛擬網路具備的高部署彈性與低維護成本則是實體網路架構難以企及之處。

對於 VMware NSX 所提供的網路虛擬化架構，經過測試之後，在整體效益上的表現，張永華的評價是，在虛擬機的零信任安全控管方面，透過微分段 (Micro-Segmentation) 安全架構，可以全面性的涵蓋虛擬環境的網路安全需求，大幅補強了虛擬環境的資安防護缺口。

而在自動化部署與管理方面，張永華則認為 NSX 兼具一致化的集中管理介面與簡單易用的追蹤除錯功能，讓不同專案承辦同仁皆能快速進行操作與維護，這些都是能有效降低維運與管理負擔之處。

未來展望與發展

在長庚大學藉 VMware NSX 建立網路虛擬化架構之後，張永華指出，資訊中心將朝虛擬化資安、服務自動化、以及軟體定義資料中心等方向發展。在虛擬化資安部分，以虛擬環境微切分來提升網路服務安全保護，提供現有虛擬環境零信任等級之安全防護；而自動化服務方面，則是建構服務自動化與邏輯網路接取混合雲或雙中心備援功能。最後在軟體定義資料中心方面，將業務服務系統完全虛擬化，並且建立應用服務感知管理流程。未來將持續推動校園資訊架構優化與採用合適的資訊技術，實現提供長庚大學師生優質資訊服務的目標。

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com
台北市 110 信義路五段七號台北 101 大樓 57 樓 C 室 電話 +886-2-8758-2804 傳真 +886-2-8758-2999 www.vmware.com/tw