台灣電腦網路危機處理暨協調中心
TAIWAN COMPUTER EMERGENCY RESPONSE TEAM / COORDINATION CENTER
TWCERT/CC 電子報

資訊安全新挑戰

第七期 電子報

淺談以「網路服務」替代「網路管理」概念之校園網路資訊安全規劃

亞洲大學資訊發展處 - 網路維運組 陳偉嵩組長、劉嘉政資訊長

前言

資訊安全相關議題於近年迅速成為業界討論的焦點，在各類資訊技術不斷提升的同時，大家開始意識到除了資訊技術的精進外，資訊安全的觀念也必須同步的提升。相關的議題包含層面既廣亦深，從早期的防毒觀念、存取保護、系統更新等，到近期的系統弱點掃描、社交工程手法到殭屍電腦控制，都是一連串資訊安全攻擊與防護的戰爭。不同的環境將面臨不同的資安威脅；而不同的資安威脅，應對的資安管理措施亦不相同。資訊安全的規劃必須符合管理者的期待，又應該符合使用者的需求，在各種不同產業中的使用者都有其獨特的資訊服務需求。「學校」是一個特別的環境，尤其是大專院校，本文中作者將分享亞洲大學內在網路使用上資訊安全的規劃與做法。

校園網路的環境特色

在一所大學的基本網路環境中，面臨了許多複雜的考驗，首當其衝就是有眾多的使用者，然而這些使用者多數是學生及老師、與其他網路環境不同的特色有兩個重點。首先、.這些多數的使用者不僅僅是使用網路，他們對於各類資訊網路的新技術更新速度更可能遠超過技術人員。其次、校園中的各項管理措施都必須基於「學術自由」的基礎下進行，當然網路管理亦不例外。分別看待以上兩點，實無特別之處，但若以上兩點同時存在於一個環境中，似乎能嗅出一些隱憂，管理人員如何在校園網路中進行有效的資安管理，又能盡可能的符合老師、學生對於網路使用的需求及達到學術研究要求，將會是一種挑戰。

從網路架構進行調整

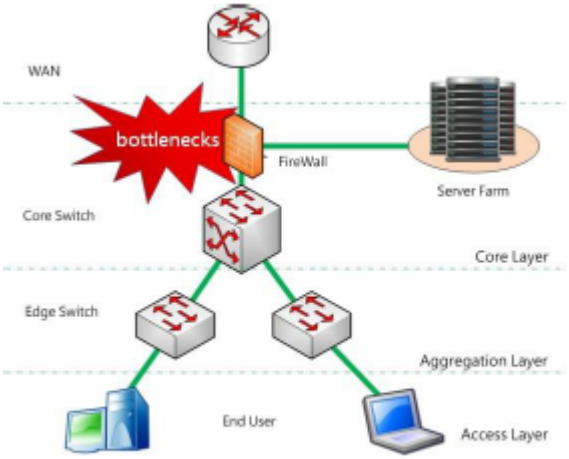
在校園網路的使用要求中，多數使用者的要求高速網路連線速度已經是一個基本要求，在此前提之下，必須將傳統的網路架構稍作修改，才能符合使用者對連線速度的期待，又同時能將資安的風險降到最低。

首先來了解一下原有架構中的設計概念。原有架構中所設置的防火牆，主要目的為管制由外對內的連線，對不受允許的連線服務給予管制，連線政策採用「原則管制，例外開放」的管理方式，將主機群服務置於 DMZ 區，由內部對 DMZ 區域的連線則以「原則開放，例外管制」的做法進行設定 (圖一)。如此的設計於一般大型企業內部網路並不會有太大的問題產生，不過當此網路架構位於一所大學內時，網路管理人員將面臨須多管理面的考驗。網路的啟用初期問題似乎不大，不過隨著使用者增加，及學術研究的種種應用需求產生，管理者在骨幹上的防火牆將不斷的增加管理政策來提供校內使用者對網路的使用需求，同時在內部使用者不斷的增加網路應用時，管理人員考量 DMZ 區的安全需求，亦將不斷增加 DMZ

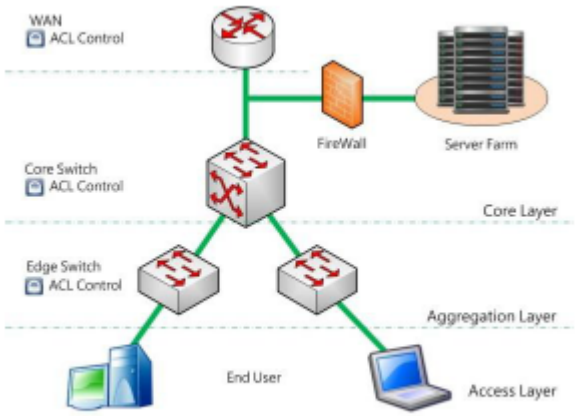
區的管制政策，時間長久累積，會造成的問題是校內使用者不斷抱怨校園網路管制過多，許多連線需求都必須提出申請才能使用，申請過程繁瑣，嚴重影響教學研究品質；管理人員面臨的狀況是連線管理政策完全與當初設計的觀念背道而馳，骨幹連線的政策已經由「原則管制，例外開放」轉變為「原則開放，例外管制」，在這樣的狀態下防火牆處理連線政策的負載明顯增加，最終將嚴重影響使用者對外的連線速度。

發生類似如此的問題時，多數的管理者會先想到的就是換一部更大的防火牆來解決效能的問題，不過可參考以下兩種方式重新思考防火牆應放置的位置，在搭配現有設備進行管理調整，似乎會比不斷的擴充防火牆設備來的有效且經濟。

1. 將防火牆設備移置主機群前，減少一般使用者對外連線時因防火牆影響速率，防火牆採用「原則管制，例外開放」管理政策，外部及內部一致的連線管制，可降低防火牆的負載，亦提升主機群之安全性 (圖二)。
2. 而使用者端的網路使用則變更為「原則開放，例外管制」，將必要的資安管理政策進行管理，管理政策即會簡化許多，並可將之移至核心層交換器或匯集層交換器以存取列表 (ACL) 進行管制，亦不需增加任何設備。



圖一 傳統網路架構



圖二 調整後之網路架構

便利使用者的管理政策

網路管理中的連線紀錄可協助管理者在發生網路問題甚至網路犯罪事件時，可透過連線紀錄進行追查，須確定使用者，並逕行管理及處理。在此前提下，必明確記載使用者的上網設備 IP，才能達成管理目標，建議透過以下的管理政策來達到便利使用與管理的目標。

非在線式的網路管理模式

校園網路不比其他商業或金融網路需要滴水不漏的安全措施，因為滴水不漏的管理措施帶來的就是層層的關卡所帶來的連線品質及服務問題。在校園的環境中，建議盡可能減少在線式的網路管理設備，避免在線式設備本身的效能問題反而增加網路瓶頸點的問題發生。一個可行的解決方式是透過非在線式的管理系統對校園的網路流量進行即時分析，比對出異常 IP 流量時以匯集層的第三層交換器透過存取列表方式 (ACL) 進行管制。雖然或許會有些許時間落差，依系統之分析能力速度，其應變時間可能延遲 5-20 分鐘不等，但評估其整體效益及其可能的資安風險，都是在可以接受的範圍。然非在線式的管理系統，完全不會因為本身

的系統異常直接對骨幹網路造成影響，在系統的安全度上是相對提升的。

1. 對使用者的電腦網路卡實體位址 (MAC) 進行驗證，以 DHCP 的模式自動派送專屬於使用者的 IP 位址，而使用者僅需於首次使用該設備時進行一次身分驗證後，即可完成個人身分 &IP&MAC 之資料註冊，使用者不需自行設定 IP 資料，減少相關設定步驟，大幅提升網路使用者的便利性。
2. 校園網路的使用者不僅僅是自家學校的老師及學生，研討會、學術活動、或學生之間的交流活動，都會有許多的校外師生、社會人士到校。這些校外人員到校後亦有網路的使用需求，規劃提供來賓的基本網路使用需求是必須的，但也必須同時考量安全的問題。此部分規劃使用者若透過 DHCP 的 IP 取得模式，該設備之 MAC 資料並不存在於資料庫中，可提供一獨立的 Vlan，並提供基本的網路服務 (如：web、msn)，對校內資訊系統則完全封鎖，每組 IP 流量限制超過 100MB 即給予停用，對於短期臨時使用之來賓可提供便利的網路服務。
3. 無線網路的使用量迅速成長，一般校園環境中均已建置無線網路環境，並提供使用者於每次連線使用時的認證機制，讓使用者透過瀏覽器進行認證使用無線網路。但目前大量手持裝置不斷透過學生、教師，進入校園網路中，這些手持裝置對於一般的認證畫面開啟似乎較為困難，然目前多數的無線網路設備供應商均能提供更佳的解決方案，但畢竟需要更多花費及改變使用習慣，簡易的做法可以提供使用者另一組免驗證的 SSID，而此組免驗證的 SSID 一樣僅提供基本網路，並嚴格限制此組 SSID 之使用者對校內資訊系統的存取，如此簡易的調整即可提供使用者更多便利的服務。

以上的管理做法，在安全性的考量上雖無法達到全面的作法，卻是在安全考量及使用著便利之間取的一個基本的平衡，亦是一項經濟的管理方式，無須動用大筆經費及耗時採購建置設備即可迅速的改變網路環境來提供兼具安全及便利的使用環境。

非在線式的網路管理模式

校園網路不比其他商業或金融網路需要滴水不漏的安全措施，因為滴水不漏的管理措施產生的就是層層的關卡所導致的連線品質及服務問題。在校園的環境中，建議盡可能減少在線式的網路管理設備，避免在線式設備本身的效能問題反而增加網路瓶頸點的問題發生。一個可行的解決方式是透過非在線式的管理系統對校園的網路流量進行即時分析，比對出異常 IP 流量時以匯集層的第三層交換器透過存取列表方式 (ACL) 進行管制。雖然或許會有些許時間落差，依系統的分析能力，其應變時間可能延遲 5-20 分鐘不等，但評估其整體效益及其可能的資安風險，都是在可以接受的範圍。然非在線式的管理系統，完全不會因為本身的系統異常直接對骨幹網路造成影響，在系統的安全度上是相對提升的。

結論

校園網路使用的 IP 數及連線數都相當大量，如何在資訊安全及使用者需求中取得平衡是一個不容易的課題，網路管理人員應如何改變傳統的管理觀念，是提供更優良的網路品質的基礎。對於大學內的網路使用，資訊單位所扮演的腳色已經不只是「網路管理」，而應提升為「網路服務」，以此為出發點才是改善網路品質最基本的觀念。