新軟週報
http://www.nusoft.com.tw
Internet Security Fighter
2010/3/29- 2010/4/11 第114期

多功能 UTM / MS 系列報導

技術淺談與應用 - 管制條例的基礎概念

隨著時代的改變，資訊技術日異月新，過去公司內所架設安裝的資訊安全設備也從多台式的機架型設備轉變為單台整合式的設備，也就是多功能型的 UTM，並集其多項資訊安全功能於一身，如此一來則可有效的簡化公司內部安全部署以及人力資源的投資，讓公司可以以最少的成本來換取更大的回饋。

新軟系統多功能 UTM 使用單一操控畫面，集中控管所有功能，有效減輕管理人員負擔，而於多功能 UTM 系統中擔當集中控管的重要角色就是『管制條例』該項功能。管制條例中的參數包含有來源網路位址、目的網路位址、服務名稱、自動排程、認證名稱、VPN Trunk、管制動作，外部網路埠、流量監控、流量統計、IDP、內容管制、網站管制、應用程式管制、病毒偵測、頻寬管理、每個來源 IP 最大頻寬、每個來源 IP 最多連線數、最多連線數、Quota Per Session、Quota PerSource IP 及 Quota Per Day 等。系統管理員可以經由這些參數來管理、設定不同出入埠間的資料傳送以及服務項目，哪些網路物件、網路服務或應用程式的封包該予以攔截或放行。

新軟多功能 UTM 為了讓所有管理人員可更明白且輕鬆的為公司管理內部資源，依據不同來源位址的資料封包，管制條例設定功能詳細的區分為『內部至外部』、『外部至內部』、『外部至非軍事區』、『內部至非軍事區』、『非軍事區至內部』、『非軍事區至外部』六個方向，以便利系統管理員針對不同資料封包的來源 IP、來源埠、目的 IP、目的埠制訂管制規則，藉此達到更完善的多方面管理，讓公司能夠享有更安全、更有規劃的網路環境。

（一）【內部至外部】：來源網路位址是在內部網路區，目的網路位址是在外部網路區。
（二）【外部至內部】：來源網路位址是在外部網路區，目的網路位址是在內部網路區（如 IP 對映、虛擬伺服器）。
（三）【外部至非軍事區】：來源網路區是外部網路區，目的網路區是在非軍事區（如 IP 對映、虛擬伺服器）。
（四）【內部至非軍事區】：來源網路區是內部網路區，目的網路區是在非軍事區。
（五）【非軍事區至內部】：來源網路區是非軍事區，目的網路區是在內部網路區。
（六）【非軍事區至外部】：來源網路區是非軍事區，目的網路區是在外部網路區。

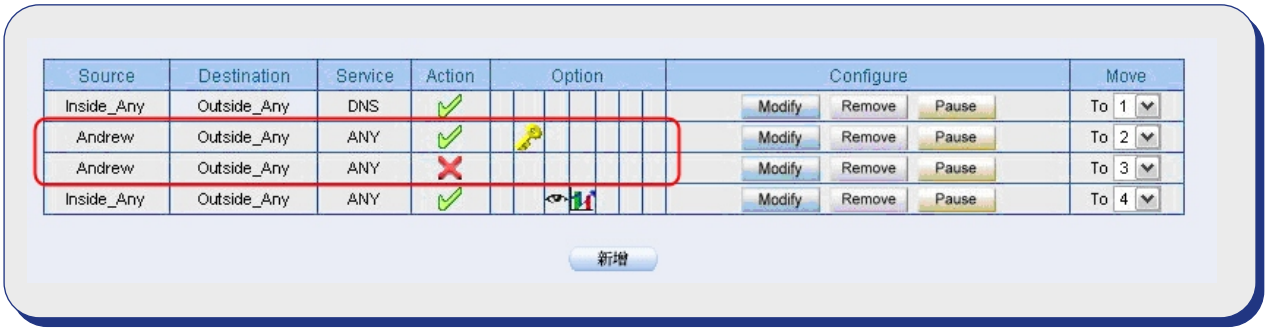
新軟『多功能 UTM-MS』所採用的是 SPI Firewall 架構，以『管制條列』為中心，將全部通路預設為阻擋，若無另行開放條例，封包便無法正常通過，有別於他其所採用 IP Sharing 先全部放行再自行設定阻擋的方式，SPI Firewall 的架構方式相對的讓公司安全更加有保障。也正因為所採用的是 SPI Firewall 架構，所以管理人員於一開始架設新軟多功能 UTM 時，最好暫時先於管理介面中“管制條例 > 內部至外部”下開放一條內部至外部為 Any 的條例，以供公司內部使用者能夠暫時正常使用網路資源，防止網路因一時無法使用而影響公司運作，當管理人員將系統設定完成後，建議最後要將 Any 的條例拿掉以防止部份使用者走該條例出去，而失去了其管制的意義。

暫時開放 Any 管制條例讓公司網路保持正常運作

此外，管理人員還要瞭解到 MS 中的管制條例運作的基本原理，於 MS 設備中管制條例是採用從上而下逐條比對的方式在運作(比對“來源位址”、“目的位址”、“服務”)，每一個封包在通過 MS 時，需要從上而下逐條檢查是否符合管制條例中所設定的條例內容。當封包的條件符合某條管制條例時，就會按該管制條例的設定來通過，而不會再向下檢查其他的管制條例，所以當管理人員在設定管制條例時一定要特別注意到條例排列順序，以免造成所設定的條例無實際作用。

封包通過管制條例，由上而下逐條比對，所以需注意排列順序

另外當 MS 比對到有需要認證的管制條例時，系統會先向下比對看是否有可以允許放行的條例，若有，則會走下方條例出去。因此，若系統管理人員欲設置使用認證功能時，在設定其認證的管制條例下方，需再另設定一條阻擋的條例，其用意是為了讓比對的動作到此為止，不再繼續向下做比對。



在認證的管制條例下方，再設定一條阻擋的條例，讓比對動作不再繼續向下

文 陳殿鴻 kim@nusoft.com.tw

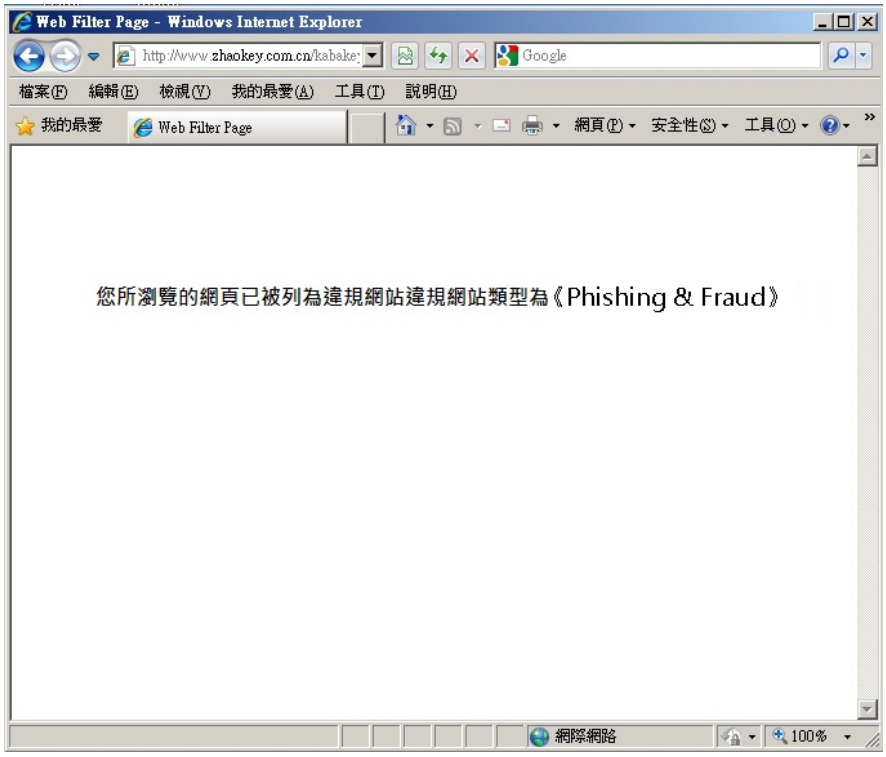
市場行銷報導 - 新軟多功能 UTM「網站管制」機制，讓你不用擔心再被“釣魚”！

近年來網路技術發展越來越迅速，使得網路科技逐漸融入人類生活中進而開始全面生活 e 化，這類趨勢使得許多人原本的生活模式漸漸開始「網路化」，最為顯著莫過於生活週遭中的食、衣、住、行、育、樂，例如：網路購物、交友網站、甚至是“網路銀行”等之類關於錢財方面的網路商業服務，這些網站都是駭客眼中非常適合“釣魚”的絕佳平台，因為駭客可以利用這些埋藏網路釣魚陷阱的網站，讓輕忽網路資安陷阱的一般使用者上鉤，藉此騙取使用者的帳號密碼來獲得他們所想要的利益。

網路上釣魚詐騙事件頻傳，一般企業防火牆、防毒牆亦無法提供完善保護

日前就傳出多起網路購物拍賣網站及網路銀行遭到駭客入侵並被植入釣魚網頁的案例；不肖人士企圖誘騙該網站會員在不自覺的情況下登入，進而騙取該網站會員的帳號密碼欲用來獲取不法利益。倘若發生此類問題將會帶來難以估計的嚴重後果，輕則人或企業的機密資料外洩、重則財產身家遭到歹徒洗劫一空，因此對於此類釣魚網站的防範將是時時刻刻不能掉以輕心的事，即便像是擁有防毒牆、防火牆的企業用戶來說，也是無法在第一時間上得到最完善保護的。

網路科技、一日千里，網路上的資安陷阱危機也是每天不斷地進化。而相同的，新軟系統產品設計也是一向隨著時代潮流趨勢而不斷研發、不斷進步；因此對於此類問題，有別於一般企業防毒牆、防火牆簡單的網路防禦機制，新軟多功能 UTM（MS1500G 以上機型）能提供使用者有效且完善的管制功能。為了能有效避免企業底下的使用者因為被釣魚網頁“釣魚”，所以提供給使用者有效的管制措施一「網站管制」機制；此機制能以新軟多功能 UTM 內強大的「網站類別資料庫」（內含 64 型網站分類包括：惡意網站、釣魚 & 詐騙網站、殭屍網站、垃圾郵件網站…等等）來判別目前使用者所欲瀏覽的網站是否為“釣魚網站”？若「是」，則會自動將使用者欲瀏覽連入的“釣魚網站”自動屏蔽掉而讓使用者無法順利連結，並且可在該屏蔽網頁上顯示予使用者知曉，藉此讓使用者知道“他被釣魚網站騙了！”；如此一來，便可以讓使用者免除於網路危機之外，也讓企業能夠妥善安穩的存在於安全保護之內。



新軟多功能 UTM 提供用戶有效的「防釣魚詐騙機制」，藉此獲得更完整的網路保護

新軟多功能 UTM 除了替企業達到最完善的防毒牆、防火牆保護之外，也為了網路上日趨強大的網路資安危害而不斷地研發更加完善的網路防護機制，最終的目標即是為了能輔助企業安全屹立於網路上，藉由網路的無限浩瀚，賺取更多的利益與商機，進而創造企業的營收高峰。

文 黃政銘 ming@nusoft.com.tw