新軟週報
http://www.nusoft.com.tw
Internet Security Fighter
2007/7/16- 2007/7/22 第34期

多功能 UTM / MS 系列報導

技術淺談與應用 - MS、MH 系列與 ML 系列 HA 機制的差異性

由於 e 化可為企業帶來豐厚的商機與方便性，所以絕大部分的企業或多或少將其各項業務搬上網路－網路已成為企業最為重要的營運工具。因此，維持網路設備正常運作對於企業來說極其重要。

想想看，若在業務最繁忙時，企業網路設備無法正常運作，這是一件多大的災難啊！臨時找到的替代機器又必須花上好一段時間重新做設定根本緩不濟急。若企業在當初建構網路時有備援機制的設計，則能在設備無法運作時適時地替代運作，維持公司網路正常運行。

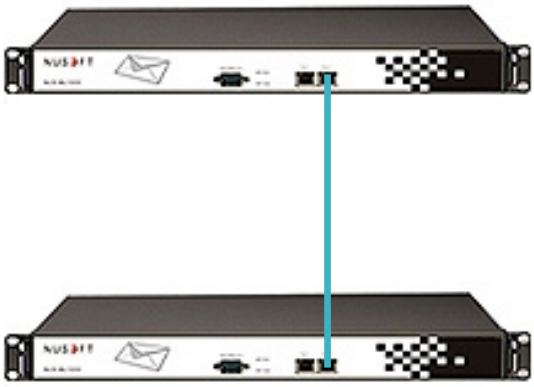
新軟系統所推出的 MS、MH 系列產品（NUS-MS1500、NUS-MS2000A、NUS-MS3500，NUS-MH1500、NUS-MH2400），以及 ML 系列產品均有 HA 設計（High Availabilit，高可用性，雙主機備援）機制，可有效防止因設備運行不正常導致網路服務中斷的問題，以達到企業網路永續運作之目的。

MS、MH 系列與 ML 系列的 HA 機制，均必須使用在兩台相同的型號機種。雖然這兩種硬體備援的結果雖然一樣，但在運作方式上卻有極大差異。MS、MH 系列的 HA 機制不僅需要相同的設備並且其韌體版本需要一致。且在系統設定上必須將其中一台設定為 Master 另一台設定為 Backup，此後雙方系統方可進行組態檔同步化。MS、MH 的 HA 機制除了手動立即同步外，亦可排定行程在特定的時間進行同步化作業。

相較於 MS、MH 系列的 HA 機制，ML 系列的設定方法簡單多了。管理人員只需將主要的 ML 的 HA 功能開啟並設定好 HA 之管理 IP Address，再連接兩台設備的 HA Port 即可立即自動進行同步化，不需太多步驟即可快速完成設定。此外，ML 系列與 MS、MH 系列的 HA 機制所同步的資料並不相同：MS、MH 系列僅限於**組態檔**同步，而 ML 系列則可以將**硬碟資料**、**組態檔**以及**韌體版本**同步化。

以上兩種 HA 機制除了有上述差異之外，ML 系列的 HA 機制還有一項極大的特點－即時同步。Mail Server 最重要的使命就是不能遺漏任何一封信件，所以 ML 系列的 HA 機制需要強調同步的即時性。只要 Master ML 有收到任何的信件或是設定上的改變，將會自動立即的進行同步化作業以防止部分郵件未備份到 Backup ML 的情況發生。也因此，ML 系列產品在第一次 HA 同步時，需要花上大量的時間同步硬碟資料（約十小時，此時 ML 仍可正常收發信件）。

MS、MH
連接 LAN port 以做 HA



ML
連接 HA(port 2)port 以做 HA

	MS、MH	ML
設備	需相同的型號及韌體版本	只需相同的型號
連接 Port	LAN Port	HA Port
同步化設定	排程或手動立即同步	自動即時同步
韌體同步	×	○
組態檔同步	○	○
硬碟內容同步	×	○
第一次同步所花時間	不需花費時間	10 小時左右

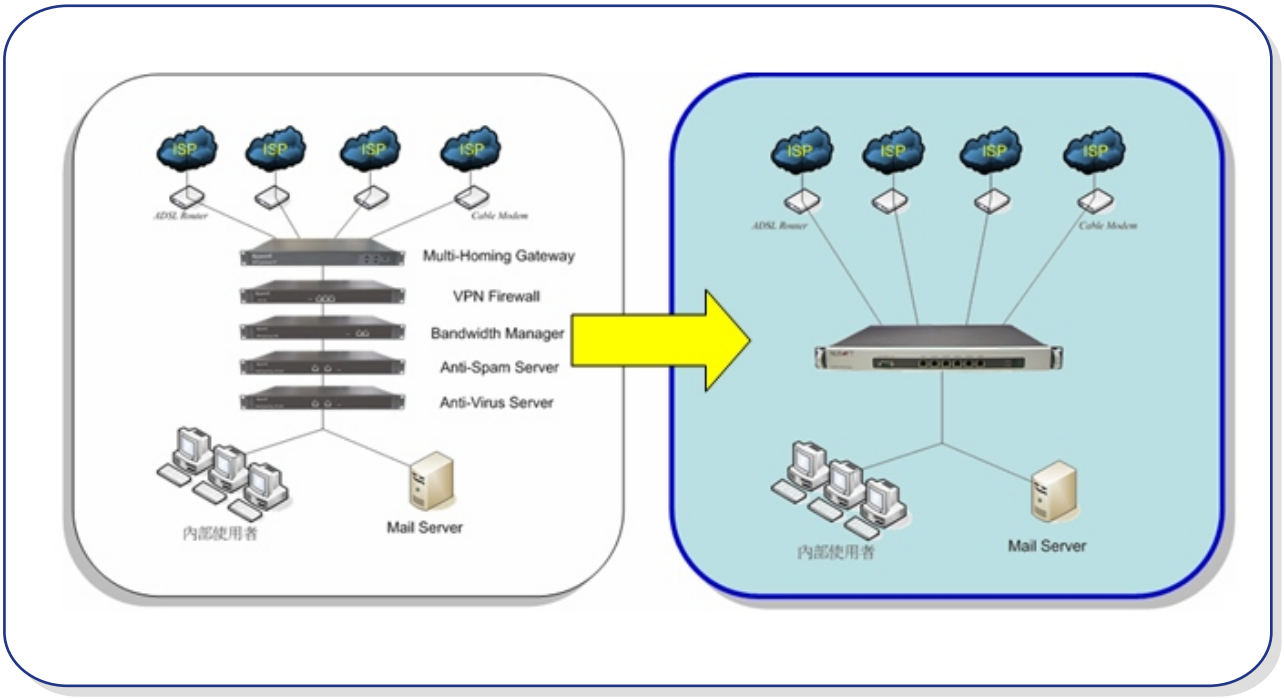
文 黃智傑 alex@nusoft.com.tw

市場行銷報導 - 企業為何要採用UTM產品

網際網路的蓬勃發展，提供了快速便利之溝通管道。絕大部分的企業都將其業務搬上網路，以便從中獲取豐厚之商機。就是因為網路對於企業來說，已成為不可或缺之重要生財工具。為了保護其安全，企業以往都是採用防火牆來防護。但是現在，各種危害網際網路安全的新式病毒、垃圾郵件、間諜軟體、廣告軟體、網路釣魚...有如雨後春筍的出現，一般所採用的傳統防火牆再也不敷使用。為了應付這些網路威脅，企業只有不停的追加其資訊安全成本，添購各種設備來因應。

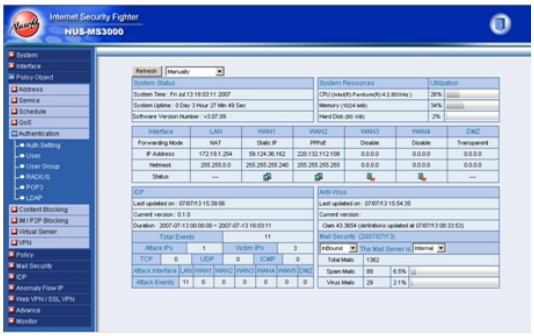
多台設備所建構之網路安全架構雖可解決目前各項網路威脅，但其成本卻非一般企業可承受的（設備採購費用、電費、維護費用...）。況且，設備與設備間的整合、相容性與管理上的方便性也是一大問題－越大越複雜的網路架構，越容易造成管理上的負擔與網路安全之風險。為了協助企業防禦種種來自於網際網路的各項威脅，新軟系統融合了多年之資訊安全經驗，推出了整合式資訊安全產品－新軟多功能 UTM。

新軟多功能 UTM（Unified Threat Management 整合式威脅控管系統）是新一代資訊安全防護設備。其中整合了多項安全功能，全面涵蓋了企業所需的各項網路安全防禦措施，能夠針對多種威脅進行防護，一機滿足企業對與網路安全的所有需求。同時其簡單明瞭管理介面，降低了設定的複雜性。企業網路安全政策的訂定只需在同一控制介面就可完成設定，減少了管理人員對於維護企業網路的工作量。



圖一 採用 UTM，可有效減少維護成本高、設備相容性差、佔用機架空間...問題

多台設備建構網路：
眾多的控制介面，讓人無所適從



新軟多功能 UTM：
單一控制介面，操控簡單明瞭

圖二 整合性控制介面，輕鬆控管企業網路

	多台設備所建構 之網路安全架構	新軟多功能 UTM
建構成本	高（需採購多台設備）	低
維護成本 （電費、維護費用...）	高	低
整合性 （設備間的相容性）	極差	完美整合各項功能
設定難易度	多操控介面，操控複雜	單一控制介面，操控簡單
網路安全風險	高	低

表一 多台設備建構網路安全架構 V. S. 新軟多功能 UTM

新軟多功能 UTM 重點介紹：

病毒防護－

一般企業添購病毒防禦設備最重要的原因有兩點：

一.管理人員無法確認企業內部所有電腦（員工與來賓的電腦）是否安裝防毒軟體或是已將病毒碼更新，造成病毒防護漏洞。

二.將企業所有的電腦安裝防毒軟體所費不貲，且須每年安排不少預算續約、升級防毒軟體。

而新軟多功能 UTM 的病毒防護措施可在網路流量上直接檢查所有傳遞之封包。輕易找出藏匿於電子郵件、網頁、FTP、IM 傳輸、P2P...的病毒、蠕蟲、間諜軟體、網路釣魚...各種有害程式與網站，進而阻擋、隔離。並可自動更新病毒碼、防毒引擎，完全不需管理人員花費心力管控。

更值得一提的是，新軟多功能 UTM 內建之 ClamAV 掃毒引擎可永久免費更新，且無使用人數上的限制。企業可以最少之成本讓其病毒防護維持在最新狀態。

垃圾郵件過濾－

垃圾郵件氾濫，大概是所有電腦使用者的痛。滿坑滿谷的垃圾信件掩蓋了重要的客戶來信、高額訂單...。況且，垃圾郵件是病毒、木馬、釣魚網站...最佳傳遞者。儘管政府單位、ISP 業者紛紛立法或設法阻擋，但還是無法有效阻擋垃圾郵件來襲。因此，企業會採購各式垃圾郵件過濾措施來防堵日益增多的垃圾郵件。

新軟多功能 UTM 的垃圾防禦功能採用多重過濾機制，並與病毒郵件防護功能完美結合，可直接將垃圾、病毒信件擋在企業網路之外。讓它無法進入企業網入內，還給使用者一個乾淨的電子郵件空間。

入侵偵測防禦－

保護企業伺服器除了採用防火牆、防毒機制之外，最有效的保護方式就是入侵偵測防禦系統（IDP）。要知道，有愈七成的網路攻擊主要是針對開放的伺服器，而這些網路攻擊一般防火牆根本無法有效防禦。

新軟多功能 UTM 內建的入侵偵測防禦系統可針對網際網路 OSI 4 到 7 層檢測；可找出隱藏在應用層的惡意攻擊程式與駭客攻擊，並與其防火牆機制結合，完全封鎖攻擊。在企業網路的最前端將攻擊或危險阻絕於外，保護企業伺服器的安全。

其他管理功能－

要良好管控一個龐大的企業網路，除了上述之安全防護機制外，亦需要許多管理機制（頻寬管理、VPN、線路備援、3A Server、認證系統、IM/P2P 管理...）方能運作正常。而新軟多功能 UTM 將這些管理機制全數整合於一身，並藉由完美的整合，管理人員可以輕鬆控管企業網路。

文 程智偉 rayearth@nusoft.com.tw