新軟週報
http://www.nusoft.com.tw
Internet Security Fighter
2007/4/30 - 2007/5/6 第24期

新軟系統 台中、高雄產品說明會報導

為了讓市場上的使用者對新軟系統有更深一步的認識，並使台灣中部與南部經銷商與一般用戶們能更加了解新軟系統各項資訊安全產品。特於四月下旬與台中 裕笠科技股份有限公司、高雄 禾翔資訊股份有限公司合作，舉辦了兩場產品說明會（台中、高雄）。參加這次產品說明會的主要人員來自 IT 產業的經銷商、業務工程師、業務人員、網管人員…等各界菁英。

產品說明會的內容以 多功能 UTM 、 網路記錄器 與 新軟郵件伺服器 這三款產品為主題：

1. 多功能 UTM：以網路安全機制、完整 VPN 架構、完善的管理機制為方向，針對企業普遍遇到的垃圾和病毒郵件困擾、異常流量影響整體網路運作、VPN 穩定性、外勤人員取回內部資料的安全疑慮、如何有效因應使用環境作最佳的頻寬規劃等議題，提供完美的解決方案，並加以解說和探討。（如下圖）

Nusoft Internet Security Fighter — UTM 超級比一比

	新軟系統 多功能 UTM	它牌 UTM
硬體規格	多 WAN 埠設計，擁有負載平衡、斷線備接功能。	僅單一 WAN 埠設計。
郵件通知機制	擁有郵件通知設計，使用者可自行取回被隔離信件。	需管理人員才能取回被隔離信件。
網路內部安全機制	異常流量偵測 聯合防禦機制	面對“異常流量”，往往無所適從。
完整VPN架構	1. PPTP / IPSec VPN 2. SSL VPN 3. VPN Trunk(備接)。	1. PPTP / IPSec VPN
完善的頻寬管理	1.最大 / 保證頻寬 2.個人化頻寬設計 可輕鬆管理企業頻寬。	僅有最大頻寬設計，無法完善管理企業頻寬。

2. 網路記錄器：以網路記錄分析、遠端資料備份、完善的管理機制為方向，針對企業在 e 化後，因網路濫用而衍生出的怠工、洩密、…侵蝕企業本身的頭痛問題，利用新軟系統獨步研發的封包辨識歸納、分流擷取技術，提供管理員流量監控、全方位記錄內容檢索…介面，以達到積極開放、分層和有效管理的雙贏目的。（如下圖）

Nusoft Internet Security Fighter 網路記錄器 超級比一比

	新軟系統 網路記錄器	它牌 網路記錄器
網路記錄分析	依使用者或種類記錄，並支援全方位搜尋記錄。	記錄不完整，但其搜尋功能不堪使用。
遠端資料備份	可自動備份至遠端 NAS，可輕鬆調閱記錄。	採用手動 CD 備份資料，資料調閱不易。
即時流量排行	幫助MIS管理員揪出佔用頻寬的摸魚員工。	不支援。
IM帳號認證管理	直接管理IM帳號。	不支援。
P2P使用管理	阻擋員工使用P2P佔用頻寬。	不支援。

3. 新軟郵件伺服器：以完善的郵件系統、快速方便的架設方式、信件大小不再受限為方向，深入剖析各企業在置換郵件伺服器時，所恐懼的停擺、帳號和信件遺失、…問題，並針對以往使用郵件服務所詬病的缺失，提出相映的解決方案。（如下圖）

Nusoft Internet Security Fighter 郵件伺服器 超級比一比

	新軟 郵件伺服器	它牌 軟體式 郵件伺服器	它牌 硬體式 郵件伺服器
完整的備份系統	雙主機備援（HA），搭配遠端NAS備份信件，郵件系統有保障。	不支援。	不支援。
垃圾、病毒郵件過濾系統	內建垃圾、病毒郵件過濾系統。	需額外安裝。	選購。
快速方便的架設方式	內建安裝精靈、帳號信件無痛移植。	安裝設定繁雜困難。	安裝設定繁雜困難。
信件大小不再受限	使用網路磁碟的超連結下載大檔案。	網路磁碟無法搭配電子郵件使用。	網路磁碟無法搭配電子郵件使用。
即時信件通知	支援 Push Mail 功能。（7月推出）	大部分不支援。	不支援。

會中最主要是一一將新軟各項產品的功能、特點、各項優勢與其適合環境…以深入淺出的方式介紹。並把新軟多年以來在網路資訊安全的相關經驗，分享給所有與會來賓。在會中，與會來賓與新軟工程師互動熱烈，不僅拉近彼此間的距離，更讓與會來賓獲得最新的產品資訊。本公司也從與會來賓的各項產品建言中獲益不少。而往後產品的發展方向，也將會尊重這些寶貴建議，讓新軟的產品能夠更加完善。

最後，在這邊要感謝台中 裕笠、高雄禾翔、還有各地的經銷商們。因為有他們的協助，此次產品說明會才能圓滿完成。

文 程智偉 rayearth@nusoft.com.tw

多功能 UTM / MS 系列報導

技術淺談與應用 - 交換器 MAC 表，聯合防禦的好幫手

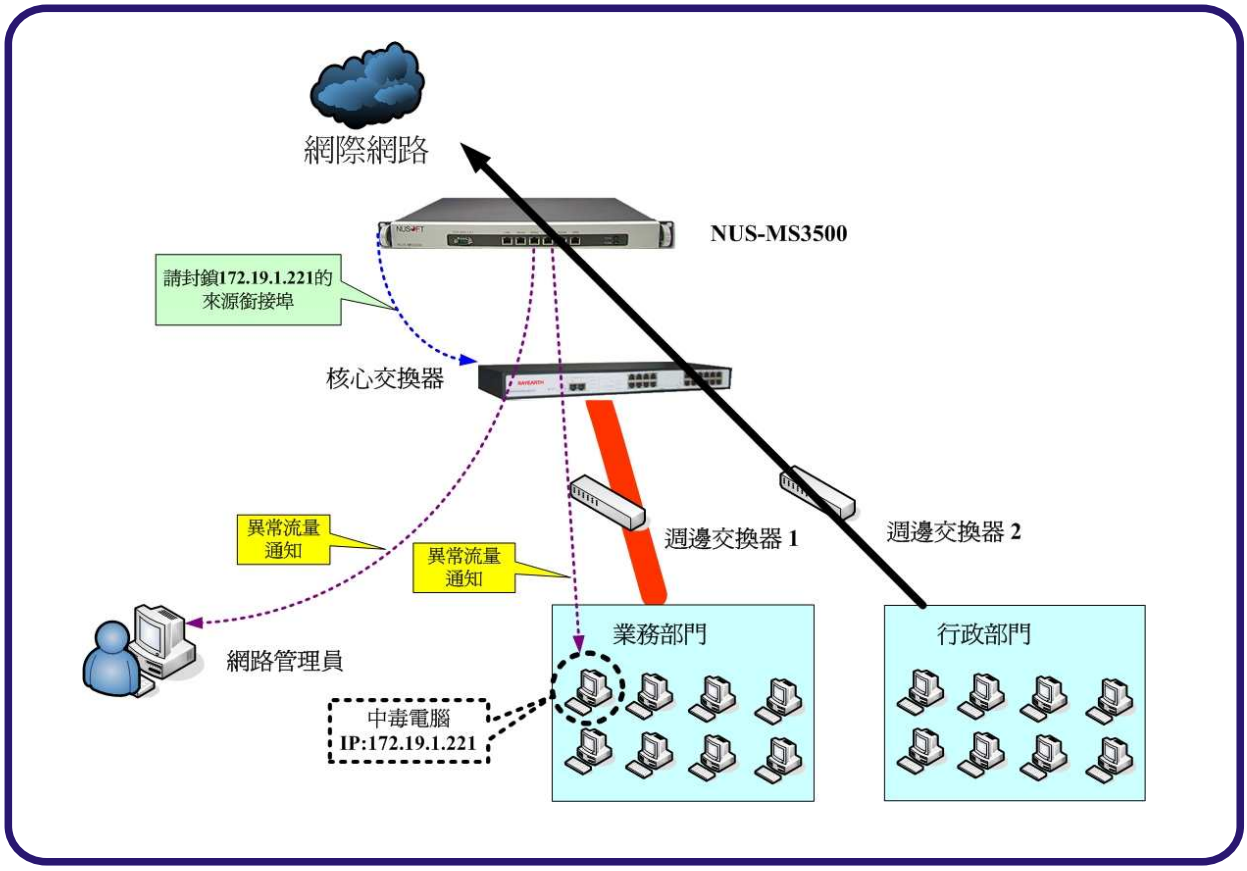
因為近年來企業作業流程大量 e 化與電子商務的興起，使得企業網路的安全性日益大增。為了保護企業網路的安全，絕大多數的企業都是採用架設防火牆的方式來確保整個企業網路的運作正常，保護企業網路抵禦來自 Internet 上的惡意攻擊行為。但是，倘若攻擊來自於內部網路企圖以阻斷式攻擊來癱瘓整個企業網路時，防火牆就無用武之地了。因此，新軟系統在多功能 UTM、多 WAN 路由分配器、網路記錄器這三款產品中，獨家推出聯合防禦機制來替企業完美解決這困擾問題。

聯合防禦機制會主動檢查每位使用者的使用流量。當聯合防禦機制發現有電腦發出大量連線（中毒）企圖妨礙企業網路正常運作時，會在第一時間內主動發出警訊給該用戶及網管人員知曉，並立即要求核心交換器(Core Switch)封鎖中毒電腦所銜接的連接埠。讓中毒電腦無法再經由核心交換器來傳送任何封包，以防病毒利用企業內部網路擴散至其他的電腦，以最快速的時間確保網路安全，避免內部資安事件擴大。

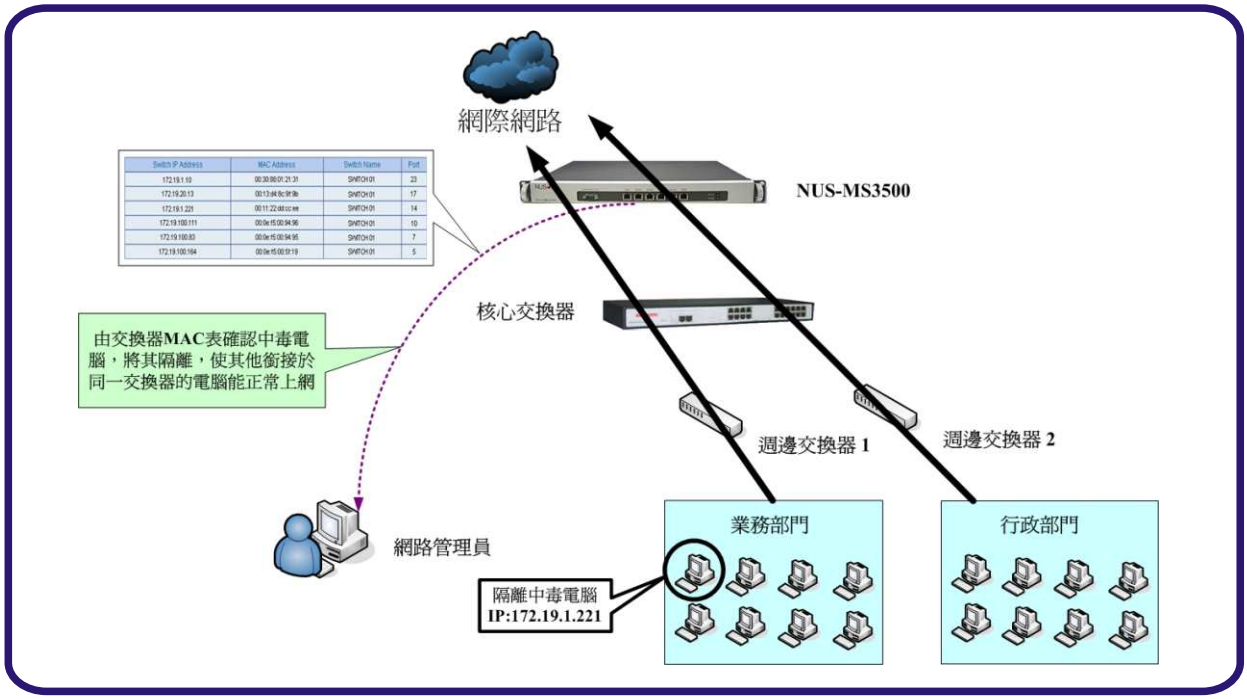
正因為聯合防禦機制是全面封鎖攻擊來源的核心交換器之連接埠。所以，當核心交換器的連接埠所銜接的非單一電腦，而是銜接另一個交換器時，會發生使用該交換器的所有使用者將無法正常上網之窘境。此時新軟系統在最近推出的“交換器 MAC 表”功能就立刻顯現出其重要性。

“交換器 MAC 表”可與企業所使用的“周邊交換器（Edge Switch）”連線，清楚表列所有企業“周邊交換器（Edge Switch）”每個連接埠所銜接設備的 MAC 與 IP。管理員可利用“交換器 MAC 表”清楚得知，中毒電腦是利用“周邊交換器”的哪一個連接埠來與企業網路銜接，先行將中毒電腦從企業網路中移開，中斷其攻擊行為。促使聯合防禦機制解除核心交換器的封鎖警報，好讓與中毒電腦使用相同周邊交換器的使用者能正常上網，再來處理中毒電腦。利用聯合防禦機制與交換器 MAC 表搭配之方式，輕鬆解決企業困擾已久的問題。

以 MS3500 為例，當其和核心交換器(Core Switch)建立起聯合防禦機制時，若內部網路以部門歸類為多個區塊，並分別接於專屬的周邊交換器（Edge Switch），某一部門的電腦因中毒發出大量連線企圖癱瘓網路，MS3500 即會告知核心交換器(Core Switch)阻斷來源埠的連線，避免影響整體網路，並通知使用者和管理員立即做後續處理。此時，和異常電腦銜接在同一交換器的其他電腦，也會被連同限制上網，為快速恢復其他使用者的運作，管理員可以交由換器 MAC 表中，參照異常通知的訊息找出相映電腦的銜接埠號，先行移除維護。（如圖一、圖二）



圖一 聯合防禦機制的通知和阻絕動作



圖二 利用交換器MAC表排除異常電腦，使網路恢復正常

文 程智偉 rayearth@nusoft.com.tw

市場行銷報導 - UTM 應支援的基本功能

企業運用網路傳輸資料的普及化，同時也衍生出許多相關的安全性、穩定性問題，為了因應此情形，網路設備廠商也伴隨著各時期的需求，推出各式的產品，例如：VPN 防火牆、頻寬管理器、入侵偵測防禦設備、防毒牆、郵件閘道器、…。

企業網路架構隨著置入設備的增多而日趨複雜，需要花費許多精神去維護各設備的正常運行，常常為了符合實際的網路應用策略，在多台設備的管理介面中徘迴設定，大量的時間和金錢支出，反應在逐漸下滑的使用效益上。

隨著時間的推移，企業逐漸意識到簡化整體網路架構的重要性，因此，市面上漸漸充斥著標榜網路瘦身的 UTM 產品，將以往分由許多設備處理的資訊安全機制整合，提供簡單、方便、多方位的解決方案。

在琳瑯滿目的商品中，所謂的UTM（United Threat Management）設備，依據國際數據資訊（IDC）定義，最基本要包含下列功能：（如下表）

UTM包含的基本項目	功能描述
防火牆	在外部網路和內部網路之間，構築一道屏障，僅允許指定的封包，通過安全性的檢查後，才能進出內部網路，避免網路遭受入侵。
VPN	提供遠端用戶以加密的方式連入內部網路，執行安全、保密的檔案存取、傳輸動作。
入侵偵測防禦（IDP）	對於漏洞的保護、間諜程式和駭客入侵的阻攔、網路釣魚的防堵、病毒攻擊的阻擋、…，提供即時主動的偵防機制，並可隨時自動更新參照的特徵碼，避免新型態威脅產生之初潛伏的危機。
閘道防毒	將所有通過各管道要處理的封包逐一檢查，彌補內部病毒防禦機制的死角。

隨著市場多樣的需求，UTM 設備的定義愈來愈模糊，各廠家盡可能將各式各樣其他的功能，加入原本的設備中。例如：垃圾郵件過濾、病毒郵件過濾、頻寬管理、應用程式管控、內容過濾、IM / P2P 管理…。於此同時也衍生了 UTM 產品的效能問題，許多廠家只是一味的增加軟體功能，從未考慮到其可行性、可用性…，結果只是換來客戶的怨聲載道。

有鑑於此，新軟在研發 UTM 產品時，就依照市場普遍會運用到的防護機制做審慎的評估，藉以規劃各採用硬體的資源，達到完美的保護，又不失傳輸時效的特性。依照硬體的處理能力，結合能力承載範圍內的常用功能，充分發揮軟體的運作表現。讓 UTM 機器不再是大企業獨享的設備，中小型企業也能獲得適合其防護需求的解決方案。

一般的 UTM 產品，普遍都只是在原有的單 WAN Port 防火牆設備上，整合許多功能。隨著網路頻寬的費用日漸降低，Multi-homing 的需求逐漸增加，這類的產品，面臨著淘汰的瓶頸。所以，新軟在規劃 UTM 產品時，即預見此趨勢，結合了原本在市場上，需要獨立設備運作的 Multi-homing 機制，在提供網路安全機制之餘，更考慮到企業對網路穩定和永不斷線的需求。（如下表）

產品 / 軟硬體設計差異	新軟多功能 UTM	一般市售 UTM 設備
硬體	一開始即預見安全和穩定對於企業網路來說，是不可偏廢的兩項要素。在採用硬體的選擇上，無不以高處理效能、多 WAN 埠負載平衡和斷線備援為標的。	僅用原有的防火牆架構，不斷的加入新穎的防護機制，漸漸無法負荷。 單一WAN 埠，也無法因應網路費用持續下降，對 Multi-homing 的強烈需求。
軟體	將市場最為需求的保護機制，依照耗費的硬體資源適當規劃，提供符合各層需求的解決方案。	

由此，現在多數困擾著資安設備採購人員的 UTM 產品，藉由新軟精闢的規劃，使得採購的目標非常明確，避免誤入誇大其辭的陷阱。

文 陳昱昇 josh@nusoft.com.tw