Nusoft 新软周报
http://www.nusoft.com.tw
Internet Security Fighter
2007/4/30 - 2007/5/6 第24期

新软系统 台中、高雄产品说明会报导

为了让市场上的使用者对新软系统有更深一步的认识，并使台湾中部与南部经销商与一般用户们能更加了解新软系统各项信息安全产品。特于四月下旬与台中 裕笠科技股份有限公司、高雄 禾翔信息股份有限公司合作，举办了两场产品说明会（台中、高雄）。参加这次产品说明会的主要人员来自 IT 产业的经销商、业务工程师、业务人员、网管人员…等各界菁英。

产品说明会的内容以 多功能 UTM 、 网络记录器 与 新软邮件服务器 这三款产品为主题：

1. 多功能 UTM：以网络安全机制、完整 VPN 架构、完善的管理机制为方向，针对企业普遍遇到的垃圾和病毒邮件困扰、异常流量影响整体网络运作、VPN 稳定性、外勤人员取回内部数据的安全疑虑、如何有效因应使用环境作最佳的带宽规划等议题，提供完美的解决方案，并加以解说和探讨。（如下图）

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. 网络记录器：以网络记录分析、远程数据备份、完善的管理机制为方向，针对企业在 e 化后，因网络滥用而衍生出的怠工、泄密、...侵蚀企业本身的头痛问题，利用新软系统独步研发的封包辨归、分流撷取技术，提供管理员流量监控、全方位记录内容检索…接口，以达到积极开放、分层和有效管理的双赢目的。（如下图）

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. 新软邮件服务器：以完善的邮件系统、快速方便的架设方式、信件大小不再受限为方向，深入剖析各企业在置换邮件服务器时，所恐惧的停摆、账号和信件遗失、...问题，并针对以往使用邮件服务所诟病的缺失，提出相映的解决方案。（如下图）

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	使用網路磁碟的超速結下載大檔案。	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。

会中最主要是一一将新软各项产品的功能、特点、各项优势与其适合环境…以深入浅出的方式介绍。并把新软多年以来在网络信息安全的相关经验，分享给所有给与会来宾。在会中，与会来宾与新软工程师互动热烈，不仅拉近彼此间的距离，更让与会来宾获得最新的产品信息。本公司也从与会来宾的各项产品建言中获益不少。而往后产品的发展方向，也将会尊重这些宝贵建议，让新软的产品能够更加完善。

最后，在这边要感谢台中 裕笠、高雄禾翔、还有各地的经销商们。因为有他们的协助，此次产品说明会才能圆满完成。

文 程智伟 rayearth@nusoft.com.tw

多功能 UTM / MS 系列报导

技术浅谈与应用 – 交换器 MAC 表，联合防御的好帮手

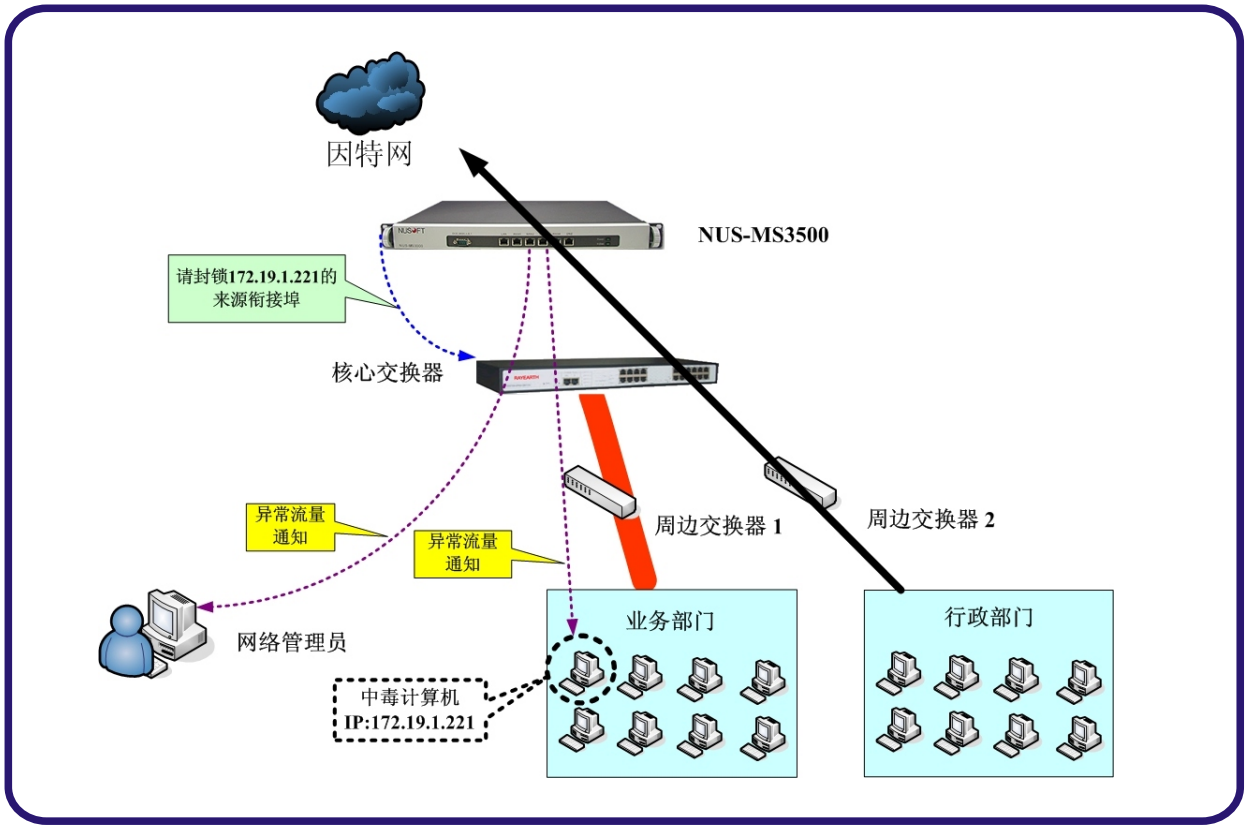
因为近年来企业作业流程大量 e 化与电子商务的兴起，使得企业网络的安全性日益大增。为了保护企业网络的安全，绝大多数的企业都是采用架设防火墙的方式来确保整个企业网络的运作正常，保护企业网络抵御来自 Internet 上的恶意攻击行为。但是，倘若攻击来自于内部网络企图以阻断式攻击来瘫痪整个企业网络时，防火墙就无用武之地了。因此，新软系统在多功能 UTM、多 WAN 路由分配器、网络记录器这三款产品中，独家推出联合防御机制来替企业完美解决这困扰问题。

联合防御机制会主动检查每位使用者的使用流量。当联合防御机制发现有计算机发出大量联机（中毒）企图妨碍企业网络正常运作时，会在第一时间内主动发出警讯给该用户及网管人员知晓，并立即要求核心交换器(Core Switch)封锁中毒计算机所衔接的连接端口。让中毒计算机无法再经由核心交换器来传送任何封包，以防病毒利用企业内部网络扩散至其它的计算机，以最快速的时间确保网络安全，避免内部资安事件扩大。

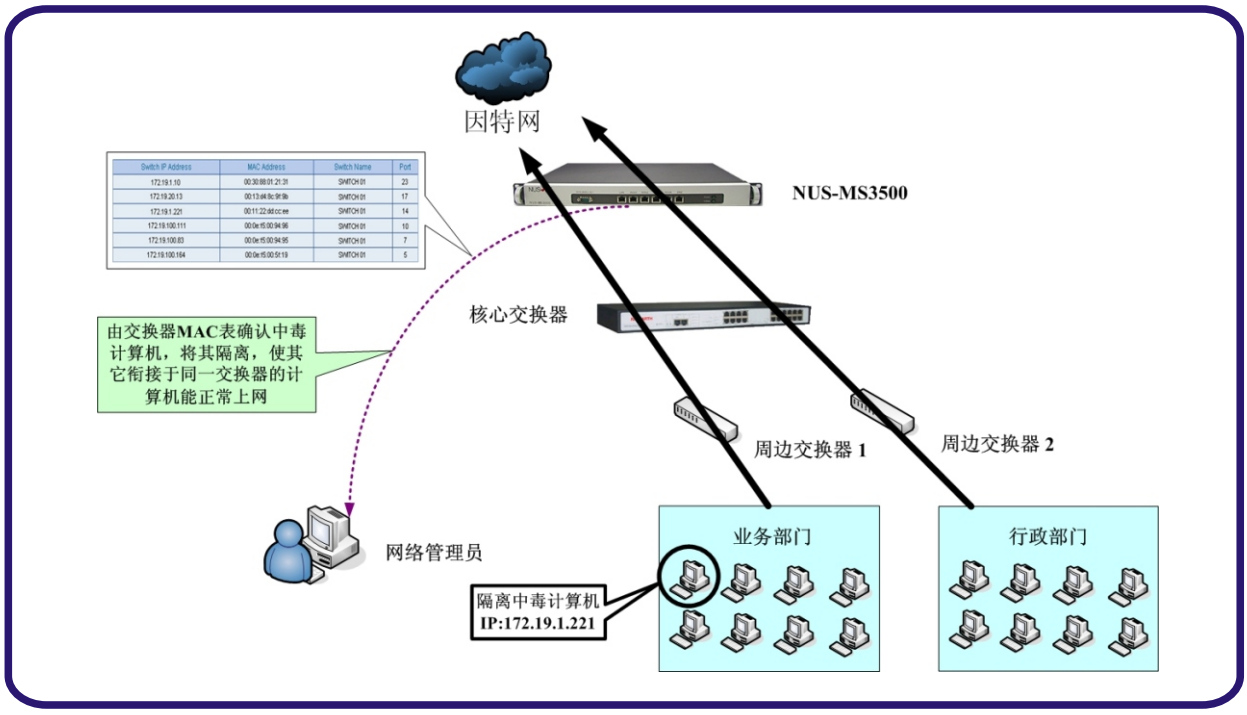
正因为联合防御机制是全面封锁攻击来源的核心交换器之连接埠。所以，当核心交换器的连接埠所衔接的非单一计算机，而是衔接另一个交换器时，会发生使用该交换器的所有使用者将无法正常上网之窘境。此时新软系统在最近推出的“交换器 MAC 表”功能就立刻显现出其重要性。

“交换器 MAC 表”可与企业所使用的“周边交换器（Edge Switch）”联机，清楚表列所有企业“周边交换器（Edge Switch）”每个连接埠所衔接设备的 MAC 与 IP。管理员可利用“交换器 MAC 表”清楚得知，中毒计算机是利用“周边交换器”的哪一个连接端口来与企业网络衔接，先行将中毒计算机从企业网络中移开，中断其攻击行为。促使联合防御机制解除核心交换器的封锁警报，好让与中毒计算机使用相同周边交换器的使用者能正常上网，再来处理中毒计算机。利用联合防御机制与交换器 MAC 表搭配之方式，轻松解决企业困扰已久的问题。

以 MS3500 为例，当其和核心交换器(Core Switch)建立起联合防御机制时，若内部网络以部门归类为多个区块，并分别接于专属的周边交换器（Edge Switch），某一部门的计算机因中毒发出大量联机企图瘫痪网络，MS3500 即会告知核心交换器(Core Switch)阻断来源埠的联机，避免影响整体网络，并通知使用者和管理员立即做后续处理。此时，和异常计算机衔接在同一交换器的其它计算机，也会被连同限制上网，为快速恢复其它使用者的运作，管理员可以交由换器 MAC 表中，参照异常通知的讯息找出相映计算机的衔接端口号，先行移除维护。（如图一、图二）



图一 联合防御机制的通知和阻绝动作



图二 利用交换器 MAC 表排除异常计算机，使网络恢复正常

文 程智伟 rayearth@nusoft.com.tw

市场营销报导 – UTM 应支持的基本功能

企业运用网络传输数据的普及化，同时也衍生出许多相关的安全性、稳定性问题，为了因应此情形，网络设备厂商也伴随着各时期的需求，推出各式的产品，例如：VPN 防火墙、带宽管理器、入侵侦测防御设备、防毒墙、邮件网关器、…。

企业网络架构随着置入设备的增多而日趋复杂，需要花费许多精神去维护各设备的正常运行，常常为了符合实际的网络应用策略，在多台设备的管理界面中徘回设定，大量的时间和金钱支出，反应在逐渐下滑的使用效益上。

随着时间的推移，企业逐渐意识到简化整体网络架构的重要性，因此，市面上渐渐充斥着标榜网络瘦身的 UTM 产品，将以往分由许多设备处理的信息安全机制整合，提供简单、方便、多方位的解决方案。

在琳琅满目的商品中，所谓的 UTM（United Threat Management）设备，依据国际数据信息（IDC）定义，最基本要包含下列功能：（如下表）

UTM包含的基本项目	功能描述
防火墙	在外部网络和内部网络之间，构筑一道屏障，仅允许指定的封包，通过安全性的检查后，才能进出内部网络，避免网络遭受入侵。
VPN	提供远程用户以加密的方式连入内部网络，执行安全、保密的档案存取、传输动作。
入侵侦测防御（IDP）	对于漏洞的保护、间谍程序和黑客入侵的阻拦、网络钓鱼的防堵、病毒攻击的阻挡、…，提供实时主动的侦防机制，并可随时自动更新参照的特征码，避免新型态威胁产生之初潜伏的危机。
网关防毒	将所有通过各管道要处理的封包逐一检查，弥补内部病毒防御机制的死角。

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，許多廠家只是一昧的增加軟體功能，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。

有鉴于此，新软在研发UTM产品时，就依照市场普遍会运用到的防护机制做审慎的评估，藉以规划各采用硬件的资源，达到完美的保护，又不失传输时效的特性。依照硬件的处理能力，结合能力承载范围内的常用功能，充分发挥软件的运作表现。让UTM机器不再是大企业独享的设备，中小型企业也能获得适合其防护需求的解决方案。

一般的UTM产品，普遍都只是在原有的单WAN Port防火墙设备上，整合许多功能。随着网络带宽的费用日渐降低，Multi-homing的需求逐渐增加，这类的产品，面临着淘汰的瓶颈。所以，新软在规划UTM产品时，即预见此趋势，结合了原本在市场上，需要独立设备运作的Multi-homing机制，在提供网络安全机制之余，更考虑到企业对网络稳定和永不断线的需求。（如下表）

产品 / 软硬件设计差异	新软多功能UTM	一般市售UTM设备
硬件	一开始即预见安全和稳定对于企业网络来说，是不可偏废的两项要素。在采用硬件的选择上，无不以高处理效能、多WAN端口负载平衡和断线备援为标的。	仅用原有的防火墙架构，不断的加入新颖的防护机制，渐渐无法负荷。 提供的单一WAN埠，也无法因应网络费用持续下降，对Multi-homing的强烈需求。
软件	将市场最为需求的保护机制，依照耗费的硬件资源适当规划，提供符合各层需求的解决方案。	

由此，现在多数困扰着资安设备采购人员的UTM产品，藉由新软精辟的规划，使得采购的目标非常明确，避免误入夸大其辞的陷阱。

文 陈昱升 josh@nusoft.com.tw