新软周报
http://www.nusoft.com.tw
Internet Security Fighter
2007/7/16- 2007/7/22 第34期

多功能 UTM / MS 系列报导

技术浅谈与应用 - MS、MH 系列与 ML 系列 HA 机制的差异性

由于 e 化可为企业带来丰厚的商机与方便性，所以绝大部分的企业或多或少将其各项业务搬上网络－网络已成为企业最为重要的营运工具。因此，维持网络设备正常运作对于企业来说极其重要。

想想看，若在业务最繁忙时，企业网络设备无法正常运作，这是一件多大的灾难啊！临时找到的替代机器又必须花上好一段时间重新做设定根本缓不济急。若企业在当初建构网络时有备援机制的设计，则能在设备无法运作时适时地替代运作，维持公司网络正常运行。

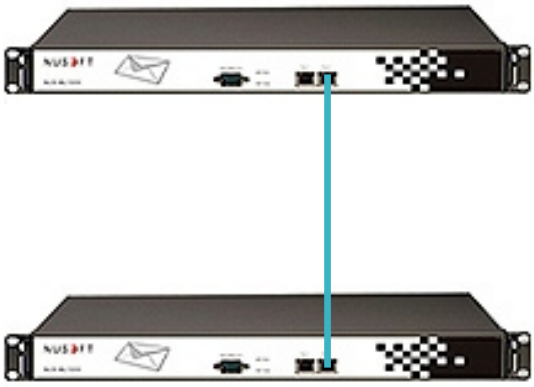
新软系统所推出的 MS、MH 系列产品（NUS-MS1500、NUS-MS2000A、NUS-MS3500，NUS-MH1500、NUS-MH2400），以及 ML 系列产品均有 HA 设计（High Availabilit，高可用性，双主机备援）机制，可有效防止因设备运行不正常导致网络服务中断的问题，以达到企业网络永续运作之目的。

MS、MH 系列与 ML 系列的 HA 机制，均必须使用在两台相同的型号机种。虽然这两种硬件备援的结果虽然一样，但在运作方式上却有极大差异。MS、MH 系列的 HA 机制不仅需要相同的设备并且其韧体版本需要一致。且在系统设定上必须将其中一台设定为 Master 另一台设定为 Backup，此后双方系统方可进行组态档同步化。MS、MH 的 HA 机制除了手动立即同步外，亦可排定行程在特定的时间进行同步化作业。

相较于 MS、MH 系列的 HA 机制，ML 系列的设定方法简单多了。管理人员只需将主要的 ML 的 HA 功能开启并设定好 HA 之管理 IP Address，再连接两台设备的 HA Port 即可立即自动进行同步化，不需太多步骤即可快速完成设定。此外，ML 系列与 MS、MH 系列的 HA 机制所同步的数据并不相同：MS、MH 系列仅限于组态文件同步，而 ML 系列则可以将硬盘数据、组态文件以及韧体版本同步化。

以上两种 HA 机制除了有上述差异之外，ML 系列的 HA 机制还有一项极大的特点－实时同步。Mail Server 最重要的使命就是不能遗漏任何一封信件，所以 ML 系列的 HA 机制需要强调同步的实时性。只要 Master ML 有收到任何的信件或是设定上的改变，将会自动立即的进行同步化作业以防止部分邮件未备份到 Backup ML 的情况发生。也因此，ML 系列产品在第一次 HA 同步时，需要花上大量的时间同步硬盘数据（约十小时，此时 ML 仍可正常收发信件）。

MS、MH
连接 LAN port 以做 HA



ML
连接 HA(port 2)port 以做 HA

	MS、MH	ML
设备	需相同的型号及韧体版本	只需相同的型号
连接 Port	LAN Port	HA Port
同步化设定	排程或手动立即同步	自动实时同步
韧体同步	×	○
组态档同步	○	○
硬盘内容同步	×	○
第一次同步所花时间	不需花费时间	10 小时左右

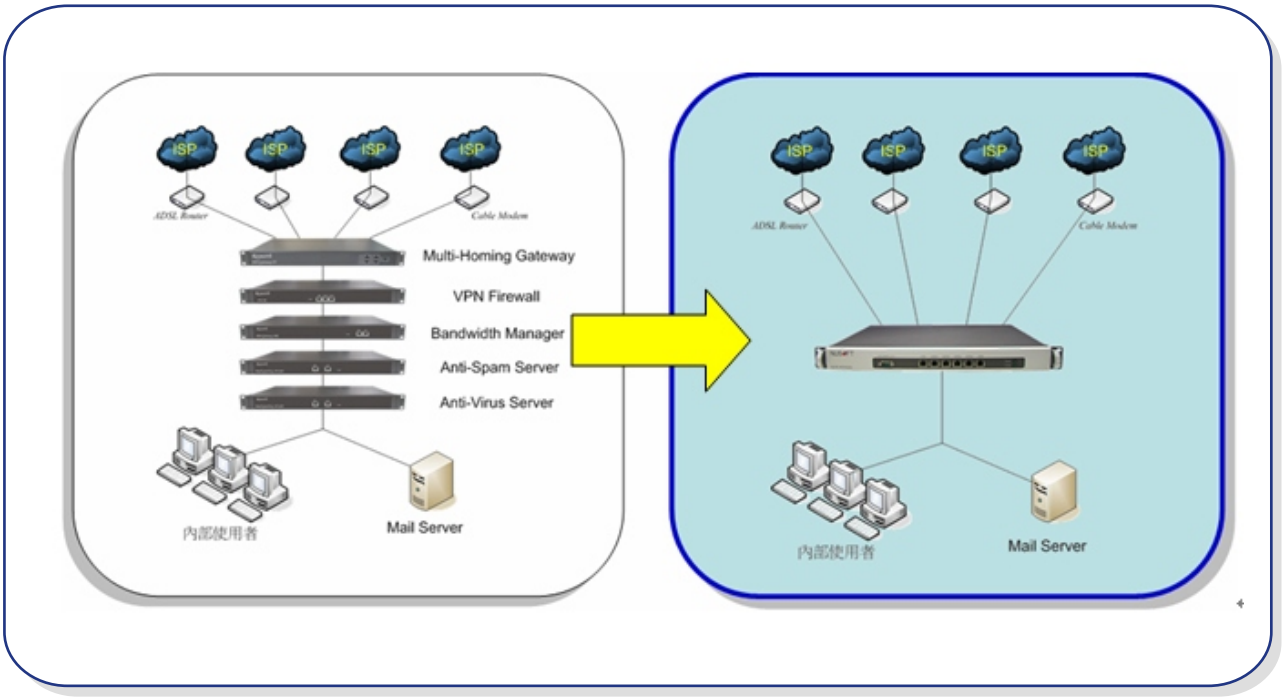
文 黄智杰 alex@nusoft.com.tw

市场营销报导 - 企业为何要采用UTM产品

因特网的蓬勃发展，提供了快速便利之沟通管道。绝大部分的企业都将其业务搬上网络，以便从中获取丰厚之商机。就是因为网络对于企业来说，已成为不可或缺之重要生财工具。为了保护其安全，企业以往都是采用防火墙来防护。但是现在，各种危害因特网安全的新式病毒、垃圾邮件、间谍软件、广告软件、网络钓鱼...有如雨后春笋的出现，一般所采用的传统防火墙再也不敷使用。为了应付这些网络威胁，企业只有不停的追加其信息安全成本，添购各种设备来因应。

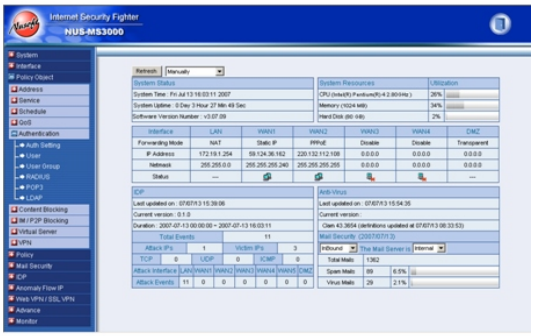
多台设备所建构之网络安全架构虽可解决目前各项网络威胁，但其成本却非一般企业可承受的（设备采购费用、电费、维护费用...）。况且，设备与设备间的整合、兼容性与管理上的方便性也是一大问题－越大越复杂的网络架构，越容易造成管理上的负担与网络安全之风险。为了协助企业防御种种来自于因特网的各项威胁，新软系统融合了多年之信息安全经验，推出了整合式信息安全产品－新软多功能UTM。

新软多功能UTM（Unified Threat Management整合式威胁控管系统）是新一代信息安全防护设备。其中整合了多项安全功能，全面涵盖了企业所需的各项网络安全防御措施，能够针对多种威胁进行防护，一机满足企业对与网络安全的所有需求。同时其简单明了管理接口，降低了设定的复杂性。企业网络安全政策的订定只需在同一控制接口就可完成设定，减少了管理人员对于维护企业网络的工作量。



图一 采用UTM，可有效减少维护成本高、设备相容性差、占用机架空间...问题

多台设备建构网络：
众多的控制接口，让人无所适从



新软多功能 UTM：
单一控制接口，操控简单明了

图二 整合性控制接口，轻松控管企业网络

	多台设备所建构 之网络安全架构	新软多功能 UTM
建构成本	高（需采购多台设备）	低
维护成本 （电费、维护费用...）	高	低
整合性 （设备间的相容性）	极差	完美整合各项功能
设定难易度	多操控接口，操控复杂	单一控制接口，操控简单
网络安全风险	高	低

表一 多台设备建构网络安全架构 V.S. 新软多功能 UTM

新软多功能 UTM 重点介绍：

病毒防护－

一般企业添购病毒防御设备最重要的原因有两点：

一.管理人员无法确认企业内部所有计算机（员工与来宾的计算机）是否安装防毒软件或是已将病毒码更新，造成病毒防护漏洞。

二.将企业所有的计算机安装防毒软件所费不赀，且须每年安排不少预算续约、升级防毒软件。

而新软多功能 UTM 的病毒防护措施可在网络流量上直接检查所有传递之封包。轻易找出藏匿于电子邮件、网页、FTP、IM 传输、P2P...的病毒、蠕虫、间谍软件、网络钓鱼...各种有害程序与网站，进而阻挡、隔离。并可自动更新病毒码、防毒引擎，完全不需管理人员花费心力管控。

更值得一提的是，新软多功能 UTM 内建之 ClamAV 扫毒引擎可永久免费更新，且无使用人数上的限制。企业可以最少之成本让其病毒防护维持在最新状态。

垃圾邮件过滤－

垃圾邮件泛滥，大概是所有计算机使用者的痛。满坑满谷的垃圾信件掩盖了重要的客户来信、高额订单...。况且，垃圾邮件是病毒、木马、钓鱼网站...最佳传递者。尽管政府单位、ISP 业者纷纷立法或设法阻挡，但还是无法有效阻挡垃圾邮件来袭。因此，企业会采购各式垃圾邮件过滤措施来防堵日益增多的垃圾邮件。

新软多功能 UTM 的垃圾防御功能采用多重过滤机制，并与病毒邮件防护功能完美结合，可直接将垃圾、病毒信件挡在企业网络之外。让它无法进入企业网入内，还给使用者一个干净的电子邮件空间。

入侵侦测防御－

保护企业服务器除了采用防火墙、防毒机制之外，最有效的保护方式就是入侵侦测防御系统（IDP）。要知道，有愈七成的网络攻击主要是针对开放的服务器，而这些网络攻击一般防火墙根本无法有效防御。

新软多功能 UTM 内建的入侵侦测防御系统可针对因特网 OSI 4 到 7 层检测；可找出隐藏在应用层的恶意攻击程序与黑客攻击，并与其防火墙机制结合，完全封锁攻击。在企业网络的最前端将攻击或危险阻绝于外，保护企业服务器的安全。

其它管理功能－

要良好管控一个庞大的企业网络，除了上述之安全防护机制外，亦需要许多管理机制（带宽管理、VPN、线路备援、3A Server、认证系统、IM/P2P 管理...）方能运作正常。而新软多功能 UTM 将这些管理机制全数整合于一身，并藉由完美的整合，管理人员可以轻松控管企业网络。

文 程智伟 rayearth@nusoft.com.tw