新软周报
http://www.nusoft.com.tw
Internet Security Fighter
2008/12/8- 2008/12/21 第8期

邮件服务器 / ML 系列报导

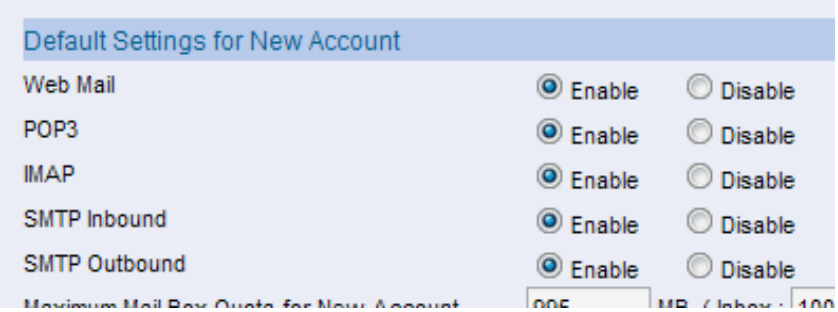
技術淺談與應用 - ML 也能做到進階的郵件管理功能

电子邮件早已成为各大企业联络通信最基本、最重要的通讯管道，顺利的为企业带来众多便利性，不但成功提升了整体工作效率，同时也为企业带来大量的商机，然而却也同时造成了网络信息安全的种种顾虑，相对的为企业带来不少信息安全上的风险。

根据统计有 65% 以上的人承认曾将企业的账号挪为私用，收送与公司内业务或公事上不相干的信件，甚至是利用 Web Mail 来收发私人信件、处理私人事情。此种情况下，公司内部重要文件也有可能轻而一举的就经由此管道而外泄，甚至是让病毒由此侵入。然而，企业所有员工真的都需要用到完整的电子邮件功能吗？对于像是生产、研发…部门，仅需要对内沟通；企业窗口、服务部门. . . 就必需随时要对外联络；在外奔波的业务人员则最需要 Web Mail 的平台好收发信件。诸如此类多样不同的电子邮件使用需求，管理人员又该如何去限制控管及规范呢？

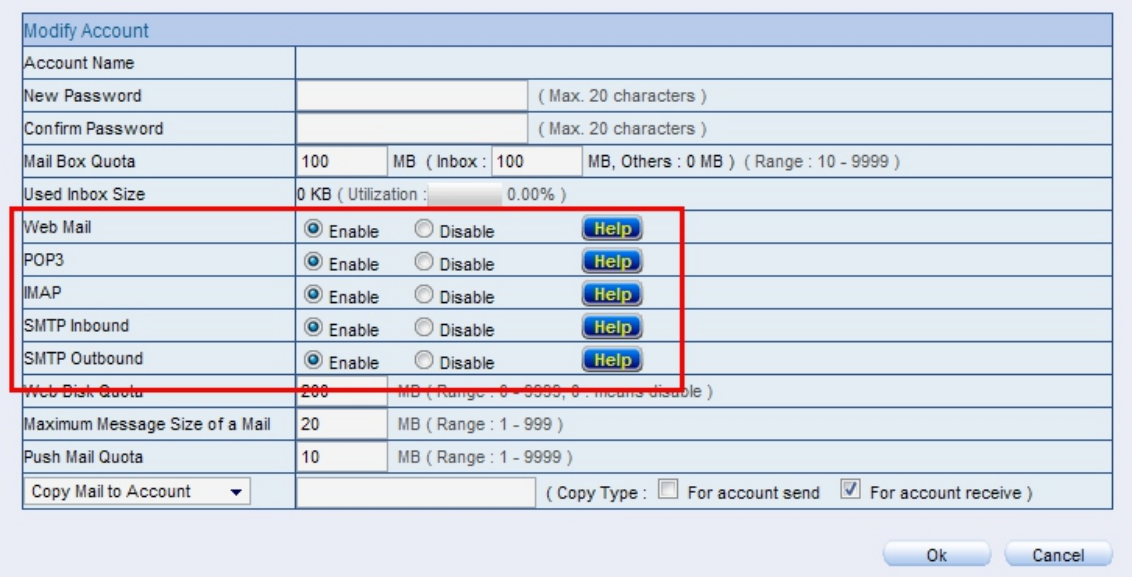
当公司内部管理人员面对邮件管理问题，不但要考虑其部门间的邮件需求方向为何，是否需要有对外的沟通，同时也要顾虑除此之外又有哪些特定之部门、人员电子邮件的往来是必需对内及对外都需求…等，种种不同的使用需求因素，多方面的顾虑下常常必须在安全与便利及重要性、需求性之间做到最适当的决定，经常因此而搞的手忙脚乱、一个头两个大。然而最常见的解决法式大多是利用公司所额外购入的邮件安全管理设备来做进一步的控管，但一般市售的邮件伺器虽然可达到针对底下员工的信件收发控管，但却无法再更进一步只针对特定群组及人员做细部的邮件设定管理。

新软系统在『邮件服务器 - ML』中 Mail Management > Account Management 下加入了个人Web Mail、IMAP、POP3、SMTP Outbound、SMTP Inbound 开关，公司管理人员可轻松利用此功能来决定该使用者是否可使用上述之功能，以更进一步的邮件管理功能来达到分层管理及依重要性、必需性而决定开放的权限，如此一来不论是面对只需使用到内部信件收发的人员及部门、必需对外的业务及企业窗口、上层主管，对于种种不同电子邮件需求方向的人事与部门来说都可以个别去做各种最适合的搭配与设定，同时也可达到防止邮件资源遭滥用的情况，一举数得。并且此功能在系统中也可于一开始就设定好开放的设定值来当作预设的规则，方便日后于邮件的新增创建使用，管理人员则不必再另外一笔一笔的去做设定。



預設功能畫面截圖

倘若需要做个别的开放或阻挡也只需要在该账号上做点取，并且进入设定画面后就可以同样的做设定，如此一来管理人员也不用再烦脑一个规则就套用了所有的使用者，而无法因需要性而无法做个别的设定。



個別設定畫面截圖

功能選項	功能說明
Webmail	此將選項若設定設為『關閉(Disable)』時，則被設定之帳號無法登入 Web Mail。
POP3	此將選項若設定設為『關閉(Disable)』時，則被設定之帳號無法用 POP3 收信。
IMAP	此將選項若設定設為『關閉(Disable)』時，則被設定之帳號無法用 IMAP 收信。
SMTP Inbound	此將選項若設定設為『關閉(Disable)』時，只有本機內所擁有之帳號可寄信給此帳號，其他外部帳號寄給此新增帳號時，都將被拒絕。
SMTP Outbound	此將選項若設定設為『關閉(Disable)』時，此帳號只可寄信給本機內所擁有之帳號，寄給外部郵件帳號都將被拒絕。

功能說明比較表

文 陳殿鴻 kim@nusoft.com.tw

市場營銷報導 - 新軟郵件服務器能為企業帶來什麼樣的好處

电子邮件在目前的网络通讯中，对于公司、企业依然是占有相当重要的地位，然而要让电子邮件传输安全又稳定，自然涉及了邮件服务器系统本身的可靠度与整体架构的设计，若是单纯的只将各种不同性质的软件功能组合在邮件服务器中，所带来的风险就是在使用上效能可能不彰，若使电子邮件在传送中有导致漏信的状况发生，内容有可能是一封诉讼案件的关键，也可能是一笔报价单或一笔金额不小的订单，如此一来为公司所带来的则是一笔巨大的损失。

一个好的电子邮件系统就是需要面面俱到，不但要能够符合企业 IT 架构，还要达到稳定，并且同时也要兼具信息安全的议题。当然，还是要在实作上能做到确实的电子邮件控管，才是最为重要的。以上的问题新软系统『邮件服务器 - ML』都帮您考虑到了。

郵件過濾與安全防護

随着电子邮件日渐普及以来，电子邮件系统便经常容易遭受到多种攻击，到目前为止最常见也是最让人头痛不已的依然是属于垃圾邮件(SPAM)，这些无孔不入的垃圾邮件除了广告的性质外，常伴随着病毒(Virus)、间谍软件(Spyware)、钓鱼诈骗(Phishing)攻击等等，而且发送的手法不断更新，有可能您现在手中的计算机就已经被用来当作跳板，并且是帮忙发送垃圾邮件帮手之一的殭尸计算机，这样的情况进而可能对企业机密数据和业务管理造成相当的危害。因此，在公司内部部署一个邮件安全管理的网关，以保护所有进出的电子邮件，已经成为企业网络安全策略中不可或缺的环节。

新软系统『邮件服务器 - ML』，拥有准确的垃圾邮件辨识率及高效率的病毒侦测功能，保护邮件安全。系统中所内建垃圾邮件过滤功能（Anti-Spam），同时采用了指纹辨识数据库（Fingerprint）、贝氏规则过滤（Bayesian Filtering）、灰名单（Greylist Filtering）、垃圾邮件特征（spam signature）…多层扫描邮件，并能定时自动回馈学习贝式过滤数据库。再配合自订的邮件规则与黑白名单之使用，可达到 99% 的垃圾邮件判读。并拥有详细的邮件过滤报告，与多样化的处置方式，有效的帮公司彻底的除去恼人的垃圾邮件，还给公司内部一个干净的邮件环境。同时 ML 还拥有邮件通知功能，当信件被 ML 判定为垃圾邮件并隔离至隔离区时，ML 会定时以邮件通知的方式通知该收件者。让收件者自行审阅及决定是否将被隔离的邮件取回，完全不需再麻烦管理人员，如此一来让管理人员能有更多的时间安心去处理其它事务。

而对于邮件病毒侦测方面，ML 内建了 ClamAV、Sophos 两大扫毒引擎可供管理人员选用，有效过滤藏匿于电子邮件中的各种有害程序。各种病毒、蠕虫、木马程序以及钓鱼信件皆可有效的过滤出并加以阻挡，同时 ML 还可于 24 小时随时在线自动更新病毒码，让管理人员可以不必为了担心病毒的更新进度而必须额外的拨出时间去处理。其中 ClamAV 可永久免费更新病毒码，而且并无使用人数限制。这可让 ML 的病毒防护功能，以最少的成本将病毒码永远保持在最新的状态。大幅降低公司在电子邮件方面的时间、金钱、人力...之投资及日后维护的经费。

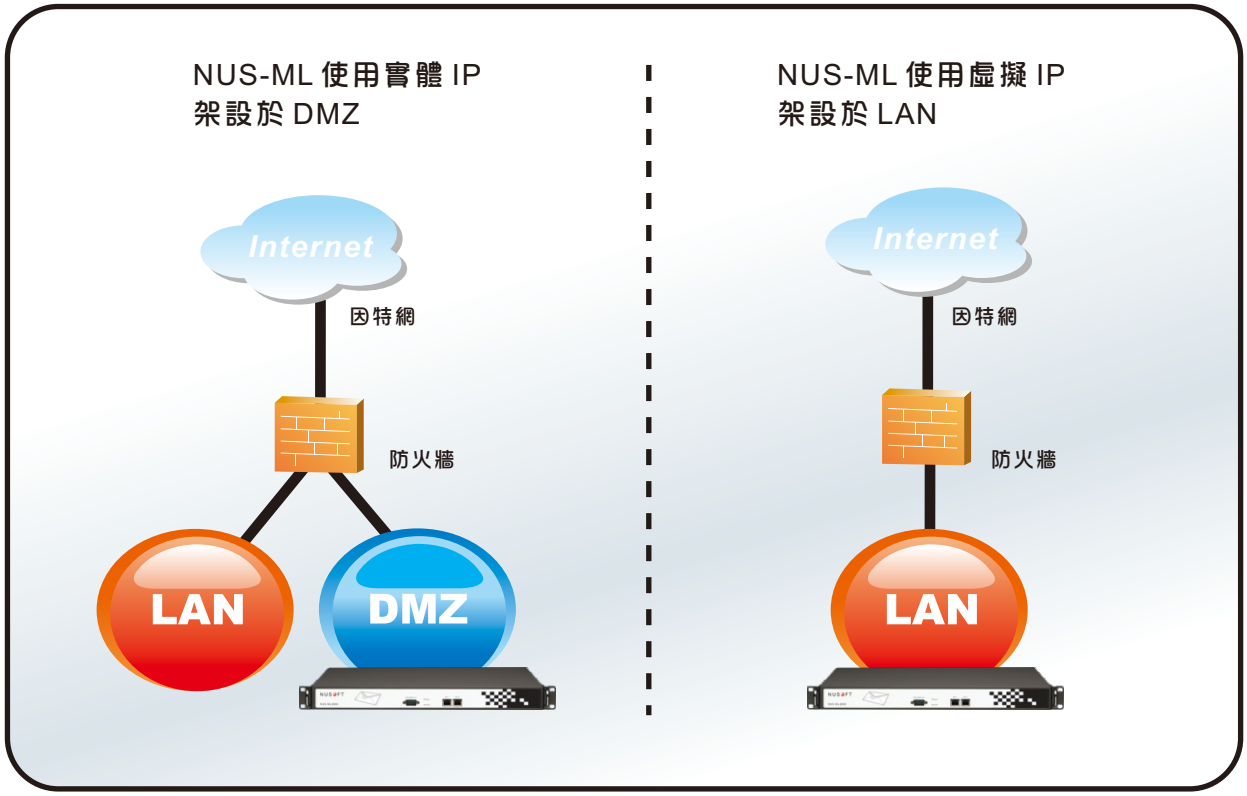
有效的提升工作效益

安装了新软系统『邮件服务器 - ML』后，所带来的效益，除了能够避免遭受攻击，造成电子邮件服务中断以及有效防范大量烦人的垃圾邮件、钓鱼信件与病毒邮件的攻击之外，另一项更大的附加价值则在于能够有效的提高员工的生产力，并且降低邮件系统管理的负担、节省邮件服务器之数量与储存空间以及减少带宽负担。系统中 Mail Notice 功能还可将判别为 Spam 之信件额外寄出通知信让收件者进行查阅，一但发现邮件中有需要收下之信件可实时点取下载取回，不必担心因系统误判而损失重要的信件，也不须再麻烦管理人员，同时 ML 并拥有多项安全设计（实时硬件备援、信箱灾难复原...），确保企业的电子邮件系统不会因突发状况而停摆，并且对于忙于在外奔波的业务人员，ML 还拥有 Push-Mail 功能，可将信件发送至业务手机中，让重要信件不会因为人不在计算机前而漏读，因此错失重要讯息，如此一来相对的就能更有效的提升工作效益为公司带来更多、更有利的商机。

符合企業之需求

任何一项设备、机制的导入当然都必须符合企业内部的需求，而 ML 的设计不但是有高捕获率、低误报率、能够轻易的让管理人员上手、并且还能够自动化的更新规则，同时还拥有安全实时硬件备援、信箱灾难复原，有效的确保企业的电子邮件系统不会因突发状况而停摆。ML 以满足不同规模企业为前提所设计，在使用上无使用人数限制。并且提供垃圾邮件特征码、ClamAV 病毒码...免费更新之服务。若是企业内部原本已有的邮件服务器而欲换上软系统『邮件服务器 - ML』时也不必担心账号移植麻烦的手序，ML 系统内设有新软独家研发的账号无痛移植机制；在 ML 取代原有邮件服务器时，可自动从企业原有之邮件服务器取得使用者的邮件账号、密码信息，完全不需管理人员手动键入。简单方便，不会有键入出错的问题发生，并且在进行自动账号移植的同时，倘若在原有邮件服务器中尚有未被下载之信件，ML 会自动移植这些信件，完全不需管理人员手动转移。人性化且高效能的设计绝对是企业的最佳选择。

新软系统『邮件服务器 - ML』架设方式简单易懂，让管理人员都能够轻易的上手。



ML 架設示意圖

文 陳殿鴻 kim@nusoft.com.tw