新软周报
http://www.nusoft.com.tw
Internet Security Fighter
2009/11/16- 2009/11/29 第105期

邮件服务器 / ML系列报导

技术浅谈与应用 - Mail Server 的两种 SMTP 认证机制不同之处与功能定位

垃圾邮件直到目前为止还依然持续影响着网络生态，不但是个人用户受到如此的困扰，各个大大小小公司也是同样不断在饱受垃圾邮件的扰人侵袭，为阻止及降低垃圾邮件所造成影响的种种问题，于公司内部导入相关防护设备也成为了所不可或缺的一项必备事情。也正因如此，为因应不同垃圾邮件之入侵方式，相对的防护机制也不断在更新，在众多之防护机制中，最为常见的一种则是利用 SMTP 之认证方式来做杜绝垃圾邮件的机制。

新软系统『邮件服务器 - ML』同样的也拥有 SMTP 认证的防护机制，但不同的地方则是，新软系统『邮件服务器 - ML』所提供之 SMTP 认证比一般外部防护设备所提供之认证方式还多了一种，分别为：『邮件服务器之 SMTP 认证』、『本机账号之 SMTP 认证』。这两种 SMTP 之认证方式有何不同呢？一般的 SMTP 认证或许还能够了解，但为何又需要多出『本机账号之 SMTP 认证』该项功能呢？到底两种认证之定位为何？为什么会需要分成两种认证方式？相信不少管理人也抱持着相同的疑问。

新软系统『邮件服务器 - ML』所提供的两种 SMTP 认证

『邮伺服务器之 SMTP 认证』

此种认证为一般最常见的 SMTP 认证，是利用寄件者于寄信时需提供邮件服务器正确的使用者名称与使用者密码，以通过 SMTP 之认证才能顺利的经由 ML 来寄信。利用如此的方式来达到防止外部有心人士利用 ML 当做垃圾邮件之跳板来进行垃圾邮件的传送。简单的来说，此认证之方式定位方向为对外做 SMTP 动作。

此外使用『邮件服务器之 SMTP 认证』该项功能时，还须特别注意到的重点则是：

一. ML 中的使用者账号及密码千万不可设定相同或是设定过于好猜测之密码。以免让有心人士利用此类型猜测方式来进行破解并加以利用，如此一来使用 SMTP 认证就完全失去其意义。

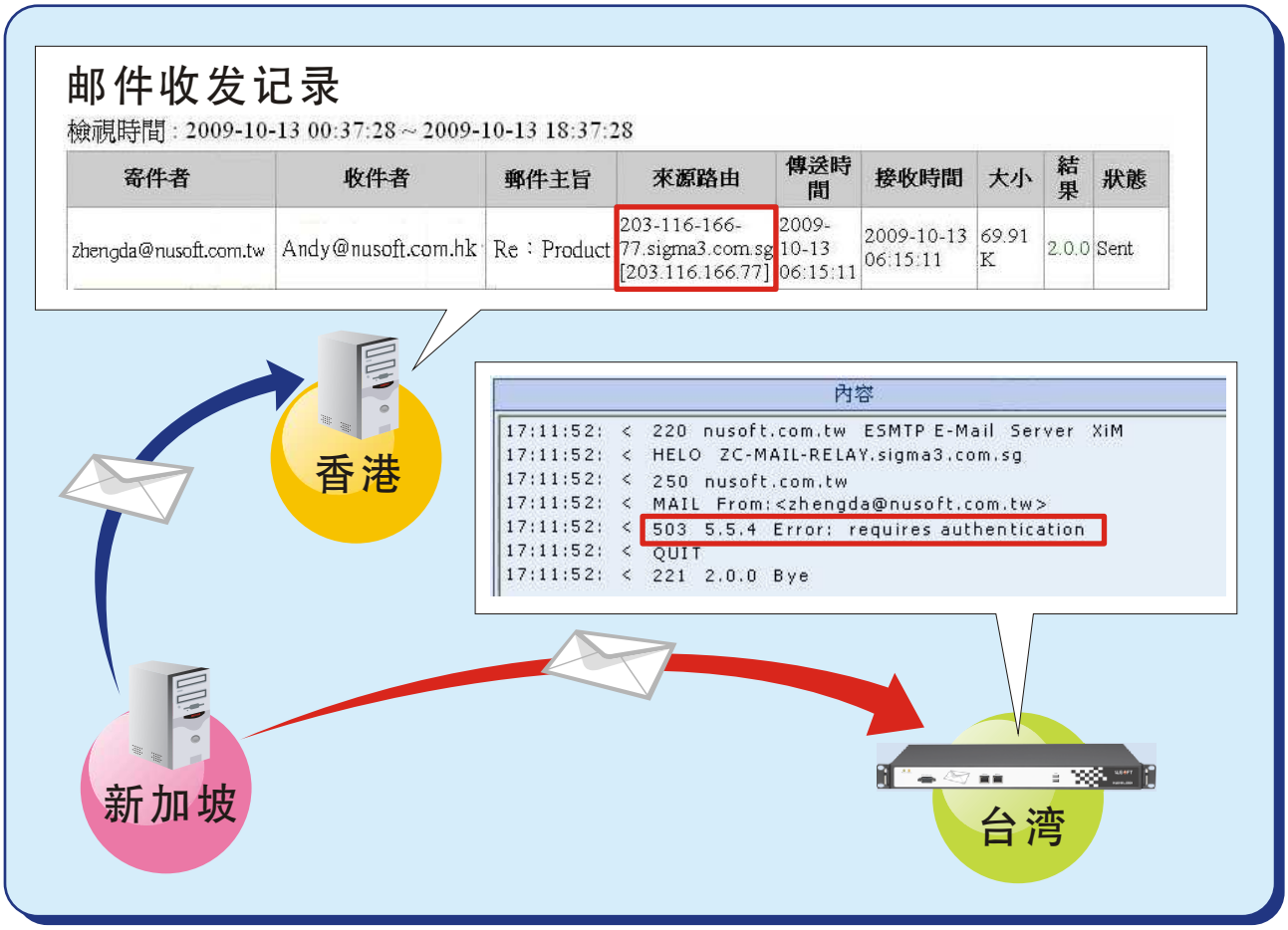
二. 不可与『Mail Management > Account Management > Settings』下的『自动新增(Automatically add)』功能同时启用，以免因账号自动新增的功能让有心人士藉由此方式来创立新账号发送垃圾邮件。

『本机帐号之 SMTP 认证』

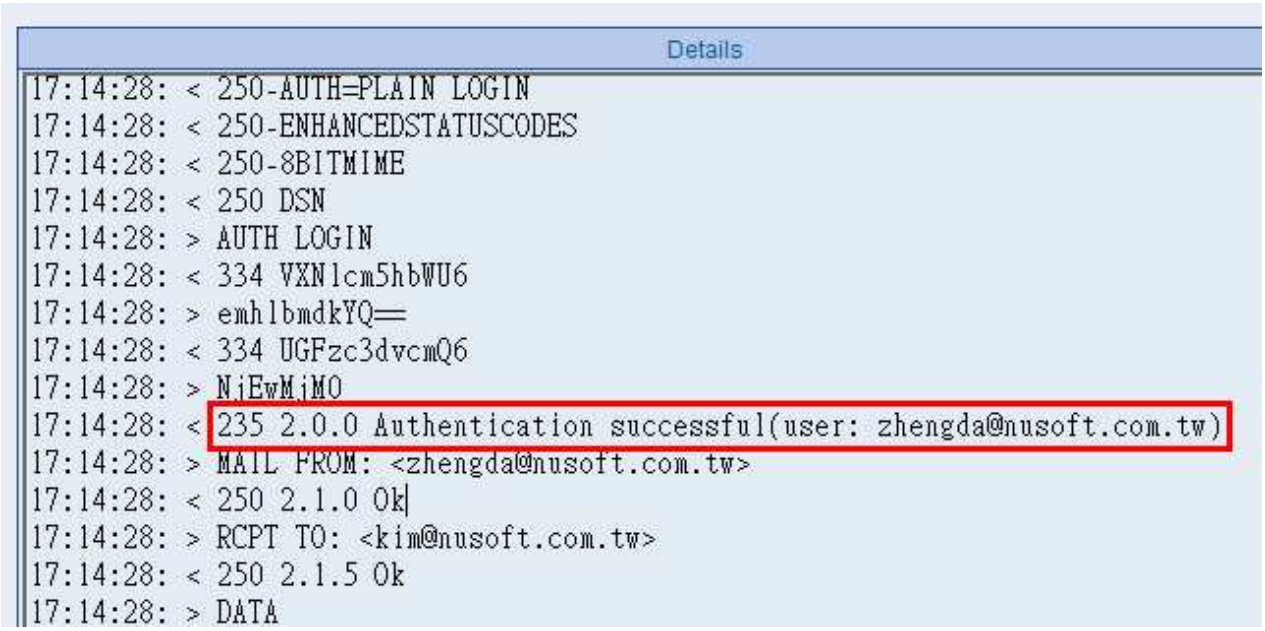
此种认证方式的运作方式为 ML 本机账号之使用者寄信至本机账号使用者时，需要进行认证。相信不少人都曾收到自己寄给自己的信件，但该封信件内容却又是自己不曾发送过的垃圾信，有心人士就是利用大多数邮件服务器会无条件让内部账号或 Domain 通过的漏洞，进而窜改信件的来源信息，以达到垃圾邮件能成功发送到收件者信箱之目的。而使用『本机账号之 SMTP 认证』功能，将 ML 本机账号寄给本机账号的此项动作进行认证，来防止外部有心人士利用窜改账号及 Domain 来将垃圾信件送达至本机账号使用者的事情发生。简单的说，此认证方式之定位方向为对内做 SMTP 认证动作。

勾选启用此种认证方式时，还必须注意到的情况则是，使用者于国外出差洽公所进住的饭店、旅馆于邮件寄发方面若设有邮件代送服务 (不管您邮件伺服设定为何，一率从该饭店设备寄送) 情况下，若使用 ML 中的邮件账号来寄送信件至内部账号使用者时，可能会被该认证机制所阻挡。

原因为该信件是从饭店设备直接寄出，而该设备与公司 ML 的 SMTP 联机，并不夹带认证所需要的账号与密码，导致信件传送到 ML 时所需检查的认证信息不符，因此会遭认证机制所阻挡。



邮件直接由饭店设备寄出导致认证信息不符



正确的『本机帐号之 SMTP 认证』成功邮件讯息

文 陈殿鸿 kim@nusoft.com.tw

市场营销报导 - 新软邮件服务器替您解决大容量信件寄送限制的窘境

日前，传出有公司企业的内部 FTP 服务器遭到有心人士入侵，并疑似遭窃取走许多相关公司机密，可能造成该公司高达数百万元商业损失。事后经由该公司相关信息人员指出其公司内外部防火墙、防毒墙、许多资安设备一应俱全，一般黑客较难以正面攻破；唯一可能发生安全漏洞的地方在于该公司员工使用 Outlook 寄信时，有时候因为客户端的信箱有收信容量大小之限制，造成若得夹带大容量的附件文件时，得将欲夹带之附件文件放置外部之 FTP 服务器上，再将 FTP 的账号密码夹带于信件里，由客户自行登入 FTP 下载大容量附件文件。

如此之状况，因为长时间累积下来的数据量加上又不定时整理 FTP 服务器的习惯，使得许多重要及非重要的文件通通混杂累积于暴露在外的 FTP 服务器里；此时又遇到有心人士进入 FTP 服务器入侵窃取其它数据，造成其公司许多重要商业机密外流，产生难以估计的商业损失。

现今许多公司企业之状况便是如此，但是碍于使用电子邮件与客户往来又是现代企业与企业间商业行为的必备条件，因此又不能禁止电子邮件夹带大容量数据，在如此两面为难的状况底下企业自身究竟该如何解决呢？

新软系统以使用者所可能产生的任何状况为产品设计方向，在所推出的邮件服务器 - ML 系列产品中，内建 “WebDisk 网络磁盘” 之功能，此功能一般除了可让使用者把网络硬盘当暂存数据碟来使用以外，还可以和新软的 WebMail 甚至其它的信件软件 (例如：Outlook Express、Thunderbird) 做结合；将欲夹带之数据上传至网络磁盘后将会产生一组超级链接，此组超级链接可夹带于信件中提供予客户透过 WebDisk 下载欲取得的大容量文件，藉此能满足工作上所需求的功能。

而一般最常发生在 FTP 服务器上的状况就是数据遭人窃取的问题，但是新软邮件服务器所内建的 “WebDisk 网络磁盘” 之安全性无须使用者担心！因为新软系统邮件服务器所提供之 WebDisk 功能是以账号区分硬盘空间，账号与账号之间的数据互不关联，而且文件与文件间也无法相连，因此让有心人士无法轻易推测到网络硬盘里的数据，进而使公司电子邮件往来安全无虞，顺利完成所有的商业往来交易。

	新软邮件服务器 - WebDisk	FTP
安全性	高 数据间无相连性亦无法推测其他文件的所在。	低 用户可透过帐号在 FTP server 里取得其他数据。
方便性	高 直接产生一组超连结，并可与新软 WebMail 甚至其他的信件软件 (例如：Outlook Express、Thunderbird) 搭配使用。	低 须另外提供帐号密码予以客户，由客户自行於 FTP server 里下载。

使用者使用新软邮件服务器 - WebDisk 及一般 FTP 服务器与信件结合之差异表

文 黄政铭 ming@nusoft.com.tw