

MLS / 邮件服务器系列报导

技术浅谈与应用 - 不再担忧邮件服务器被列为黑名单

在多元化的网络时代，企业无不依赖电子邮件做为商业交流工具，带给企业许多便利与商机。但也因电子邮件的便利，不少有心人士利用企业邮件伺服器安全性之漏洞，成为病毒邮件或垃圾邮件的转送点，不仅将企业网络资源消耗殆尽，更严重导致邮件服务器被列为黑名单，影响企业形象。

邮件服务器被列为黑名单，常见的原因如下：

1.发送电子报或电子 DM：

未经收件人同意，直接发送大量广告信，收件人易心生反感，视为垃圾信件，并向 RBL 组织检举。

2.恶意程序 / 感染病虫：

藉由病毒、木马或恶意程序，在受感染的计算机内植入 Spam Relay 转信引擎，透过受害者计算机作为跳板，然后自动启用 SMTP 服务四处寄送病毒信，使计算机被列为广告信主机，因此被 RBL 盯上。

3.Open Relay：

开放式的转寄。管理人员没将 SMTP 设定需要为认证，或者限定某些 IP 才能 Relay 而造成的人为疏失。使得有心人士利用 Open Relay 来传送大量的讯息，以便伪装真实的邮件来源进而隐藏自己的身分，让无辜企业成为垃圾邮件的转送点。

4.先前 IP 承租者问题：

先前有些 ISP 线路用户的 IP 因发垃圾信被 ISP 停权，甚至列入实时黑名单，用户退租后，若无人处理，IP 仍名列 RBL，等到下一个用户使用，会发现寄出的邮件都被阻挡。

5.网络遭入侵盗用 / 不肖员工：

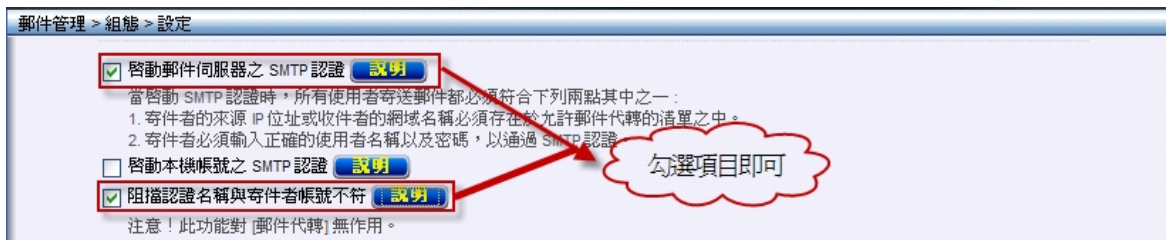
有些公司的邮件服务器遭黑客入侵，或者员工利用公司本身网络资源，转寄垃圾信，因此被 RBL 盯上。

为了避免上述之问题发生，新软系统邮件服务器 MLS / ML 系列产品，提供邮件寄送路由、邮件管制临界值、SMTP 认证等几种方式，解决企业邮件服务器被当跳板，发送大量的垃圾邮件与病毒邮件，因而被列入为黑名单。

1. 限制信件代转对象

当邮件服务器的代转方式采用 Open Relay 时，非常容易被作为发送垃圾邮件的跳板，因而被反垃圾邮件组织列入黑名单；成为其它邮件服务器的拒绝对象，影响正常的邮件联系。新软邮件服务器 (MLS / ML) 为了限制邮件代转功能采用「邮件代转设定」、「SMTP 认证」两种方式；信件如需新软邮件服务器 (MLS / ML) 代为转发，须满足上述两种条件之一。「邮件代转设定」是“寄件者的来源 IP”或是“收件者之网域名称”必须存在于允许邮件代转的清单之中，新软邮件服务器 (MLS / ML) 才会代为转发信件。「SMTP 认证」则是寄件者于寄信时必须通过 SMTP 认证，新软邮件服务器 (MLS / ML) 才会代为转发信件。

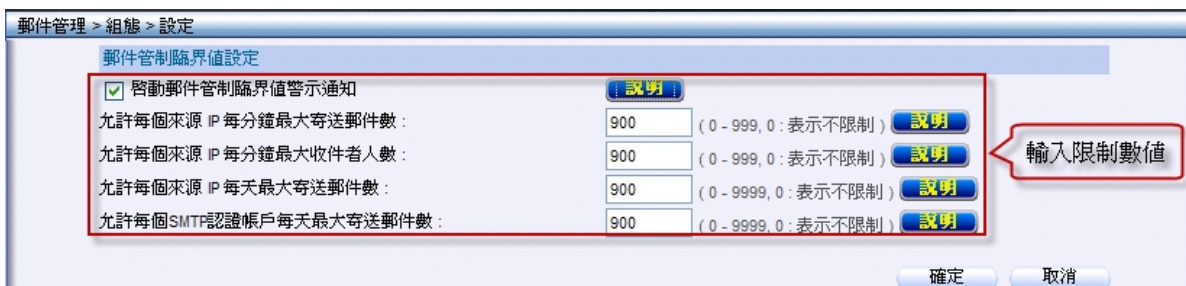
另外，需要注意的是当启用 SMTP 认证功能时，若使用者之密码过于简单则容易被垃圾邮件发送者所利用；反而成为垃圾邮件之跳板。因此，新软系统邮件服务器加入「阻挡认证名称与寄件者账号不符」功能，以阻挡上述情形之发生 (一般垃圾邮件会伪造寄件者账号，故认证名称与寄件者账号不同)。



图一

2. 邮件管制临界值

如因使用者人为操作疏失 (中毒、密码过于简单...) 导致企业开始寄送垃圾邮件时，新软邮件服务器亦提供了「邮件管制临界值」以避免事态扩大。本功能有「启动邮件管制临界值警示通知」、「允许每个来源 IP 每分钟最大寄送邮件数」、「允许每个来源 IP 每分钟最大收件者人数」、「允许每个来源 IP 每天最大寄送邮件数」、「允许每个核定账户每天最大寄送邮件数」几种设定。可限定来源 IP 限制寄送邮件数、收件者人数... 方式封锁滥寄垃圾邮件的发生。并若有异常事件发生时，系统将会寄送通知信给管理人员；管理人员可立即察觉出问题所在，避免企业被列为黑名单。



图二

3. 「由内对外」垃圾邮件过滤机制

若上述防堵机制尚有漏网之鱼时，新软邮件服务器亦内建了一般邮件服务器所没有的「由内对外垃圾邮件过滤」机制，可过滤从企业网络所发出的垃圾邮件。只要启用「扫描本机账号所寄出的信件」设定，即可将垃圾邮件以“直接删除”、“转送给收件者”、“储存在隔离区”…方式处理(由管理人员订定处理方式，建议采用“储存在隔离区”)。



图三

4. 邮件寄送路由

如果先前 IP 承租者发送垃圾信件，而被列入为黑名单，造成下一个 IP 用户者寄出邮件都被阻挡。新软邮件服务器「MLS/ML系列」提供「邮件寄送路由」功能。何谓邮件寄送路由？是将邮件服务器所有寄送之邮件，先行寄送至 ISP 业者之 MTA 上，再统一透过此 MTA 转送至目的邮件服务器。当目的端邮件服务器接收信件时，由于信件是由 ISP 之 MTA 所发送，所以信件之来源端位置将是「MTA 之 IP」而不是使用者所设置之「发信服务器 IP」，藉由此方式解决先前 IP 用户者不当，所造成的问题。



图四

另外，新软邮件服务器提供「电子报」功能，以便订户可自行「新增订阅」或「取消订阅」，防止订户因电子报寄送，心生反感并视为垃圾邮件，向 RBL 举发，因而被列为黑名单。

文  余光明 kongmeng@nusoft.com.tw

市场营销报导 - 完整之 Backup 机制，保存企业重要的电子邮件

原本以为云端很安全的 Gmail 用户，在美国时间 2 月 27 号，全球约 0.08% 用户的账户被清空，不论是信件、附件、分类的卷标或是聊天纪录、部落格，全都不见。甚至有些用户的 Gmail 还出现了新使用者才会有的「注册成功欢迎信」；更有用户在状况发生不久后，还被暂时停权，无法登入。经此事件，才让不少企业明白资料仍然需做备份，以免造成重要数据遗失，严重影响企业利益。

因此，新软邮件服务器 MLS / ML 系列产品中提供各种电子邮件相关机制(双扫毒引擎、多重垃圾邮件过滤机制、Push Mail...)，当然也包含完整之 Backup 机制 - 「高可用性(HA)」、「电子邮件归档保存(Mail Archive)」、「远程备份电子邮件(Remote Backup)」，来协助企业架构完整的电子邮件系统。

高可用性(High Availability)

何谓高可用性？就是双主机备援机制，实时由备援设备取而代之。可避免发生不可预期的问题，导致相关工作顿时停摆时，有效减少邮件服务器停止运作时间以维持电子邮件系统运作正常。一般邮件服务器之硬件备援功能中，同步的数据包括「设定数据」、「使用者账号与密码」与「邮件」，其中以「邮件」数据最需要实时同步。因为在两次数据同步的间隔期间，邮件服务器发生问题而必须切换至备份主机时，尚未同步的邮件会从此消失了，而这些消失信件中有客户订单，或重要之电子文件，后果不堪设想。

新软系统高可用性功能与一般市用的高可用性不尽相同，因为新软系统特别推出全新的硬件备援概念 - 「实时硬件备援(Real Time HA)」，就是随时随地同步双方所有数据；正常运作的邮件服务器所收到之信件，也让备援主机同样的时间内收到，完全没有时间差的问题，在邮件服务器发生问题时，电子邮件系统仍能正常运作。虽然双主机备援需多买一台邮件服务器，但高可用性功能有其必要性，它的作用就像是保险一样为了以防万一，不会因为邮件服务器发生不可预期之问题，引发重要信件无法送达，进而造成信件遗失问题，损及企业商机。

电子邮件归档保存(Mail Archive)

企业要保存往来之电子邮件，除了以手动方式备份外，就只有建构「邮件备份服务器」方能达到备份邮件之目的。虽然手动方式可以依使用者的需求，备份所需之信件，但也可能因人为疏忽而导致有些重要信件遗漏备份，且麻烦无比。「邮件备份服务器」则简单多了，会自动处理，完全没有手动备份的麻烦。但是，企业需要额外增加电子邮件系统的建构成本，而且绝大部分的「邮件备份服务器」并没有筛选机制，因此正常邮件、垃圾邮件、病毒邮件...全部备份，真正有用的信件少之又少。

新软系统为了协助企业节省备份邮件之建构成本，在其推出的邮件服务器中加入了「邮件归档」功能，可自动将企业往来信件归档存查，完全不需使用者手动备份或是额外添购「邮件备份服务器」。除此之外，「邮件归档」功能亦可依照管理人员所设



定之条件规则选择所需要的信件备份，让企业能更灵活备份其电子邮件。

远程备份电子邮件(Remote Backup)

现在不少国家政府立法要求企业电子邮件需要保存五至七年，以便日后发生纠纷亦可此为证，因此电子邮件要长久保存五至七年，容易造成邮件服务器内建硬盘饱和问题，以及因天灾/人祸或其它事故，导致原有邮件服务器中断服务，严重影响公司营运正常运转。

为了上述之问题发生，新软系统邮件服务器提供了「远程备份」功能，可将「邮件归档」的信件备份至 NAS、File Server、拥有网络芳邻的计算机…方式。此种方式，除了备份空间大、全自动备份、使用磁盘阵列确保数据不损毁…外，在数据读取查阅上也有着随时随地、方便、快速…的特性。另外，与其它邮件备份服务器不同的是，新软邮件服务器的「远程备份」加入「信箱灾难复原机制」之功能，倘若内建硬盘损毁时，新软邮件服务器(MLS/ML系列产品)在更换新的硬盘后，即会自动启用「信箱灾难复原机制」之功能，系统会依照设定值迅速将信件数据备份回所更换之新硬盘里，包含：信件、通讯簿、WebDisk 里的数据，通通会原封不动地回到每个使用者的信箱当中。

	Gmail	新软邮件服务器
建构方式	软件安装。	无。
备份机制	软件备份。	远端 NAS 备份机制。
适用储存媒介	帐户者本机计算机。	NAS、File Server、拥有网络芳邻的计算机。
自动 / 人工备份	使用「桌面端邮件软件」、「Gmail Backup 软件」备份信件，需人在旁操作软件。	全自动备份，无须专人在旁操作。
备份信件浏览 / 找寻方式	在本机计算机数据夹中一封一封找寻所需之信件，花费时间长。	直接於管理接口浏览 / 搜寻信件，花费时间短。
浏览地点、时间	只能在本机计算机浏览信件。	在任何地点、时间，只需远程联机至新软邮件服务器之控制接口，即可浏览信件。
信件保存时间	可永久保存，但出现人为疏失或者，导致数据将无法全部复原。	利用磁盘阵列不怕信件遗失。
复原机制	无。	只要启动「信箱灾难复原机制」及设定备份服务器之地址，即可将整个信箱完整复原，成本相当低。

表1 - 比较备份机制的不同

文  余光明 kongmeng@nusoft.com.tw