新软周报
http://www.nusoft.com.tw
Internet Security Fighter
2007/3/19 - 2007/3/25 第20期

多功能 UTM / MS 系列报导

技术浅谈与应用 - 利用灰名单过滤垃圾邮件

垃圾邮件的型态变化过于迅速，常常造成许多预防措施成效不彰，而各厂家陆续推出的解决方案，也大多是治标不治本的方法，有时或许能立竿见影，但长久下来已造成使用者信心动摇、不堪其扰的负面影响。

传统的邮件账号判断和黑名单(RBL)过滤机制，由于垃圾邮件寄送内容的篡改，和疏漏的回报系统，已经丧失对其判别的精确度，常常导致企业往来邮件无法递送的情形，许多交易因而停摆，无形中扼杀了企业的竞争力。

现在大多数的垃圾邮件，皆是透过大量发送邮件的软件做寄送的动作。而这种发送方式有一特点，就是以随机伪造的寄件者账号，针对所搜罗到的收件者做一次发信的动作。对于此情形，新软公司观察此类邮件发送模式，并研发出相应的解决技术，务求根治大多数的灾情，经数度改良后，独创一格的灰名单过滤机制终于问世，并将其导入 MS 系列产品之中。

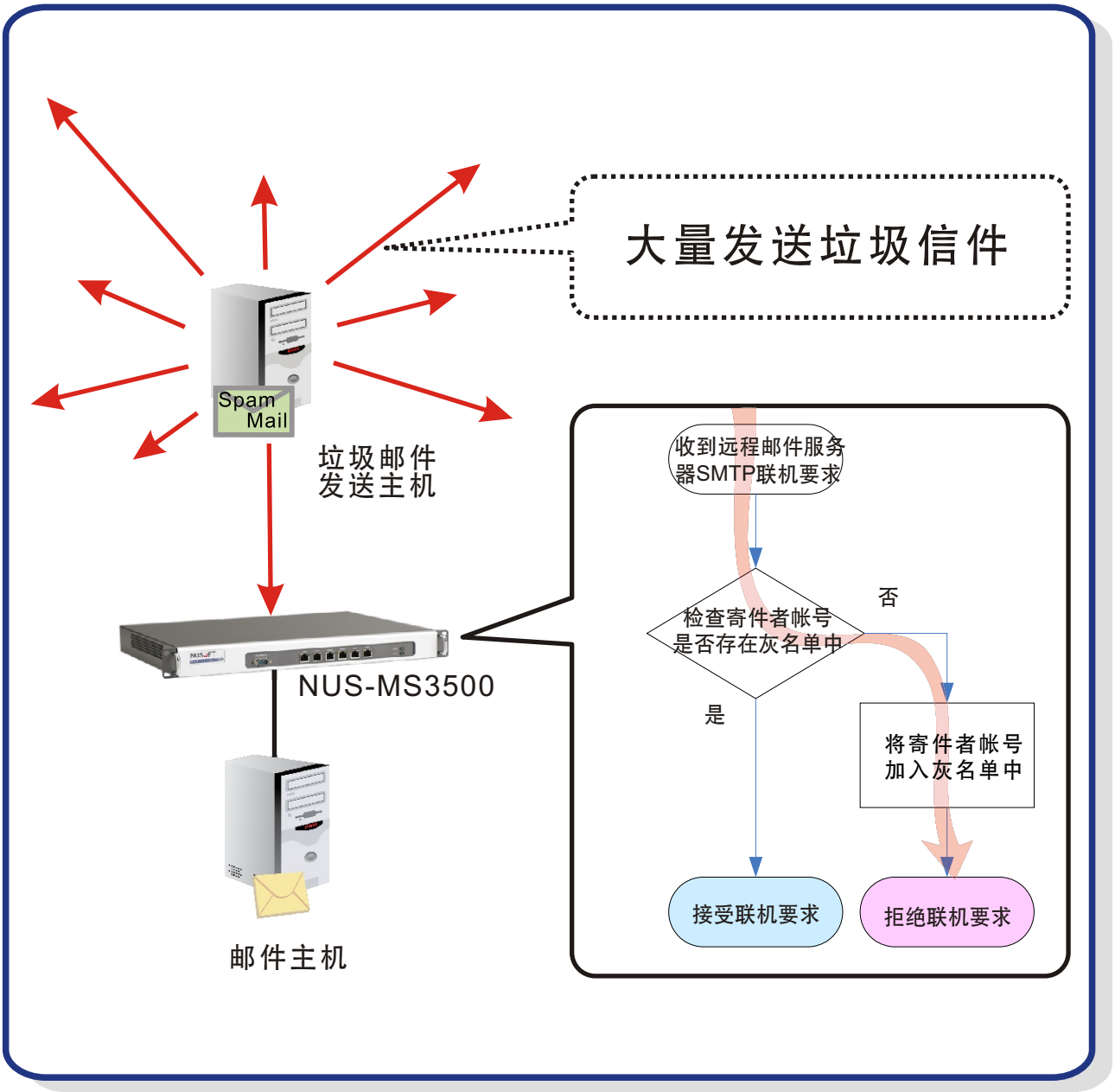
- 新软－灰名单过滤机制，以下列方式运作：

  1.无条件拒绝任何外部邮件服务器 “新寄件者账号” 的第一次 SMTP 联机要求。
  2.会将上述的“新寄件者账号”列入“灰名单”中。
  3.往后，灰名单过滤机制将不再拒绝列名于“灰名单”中的寄件者账号之 SMTP 联机要求，而将垃圾邮件过滤任务交由其它机制处理。

- 新软 MS 系列产品内建的灰名单过滤机制，和一般市售具有此功能设备的比较（如下表）：

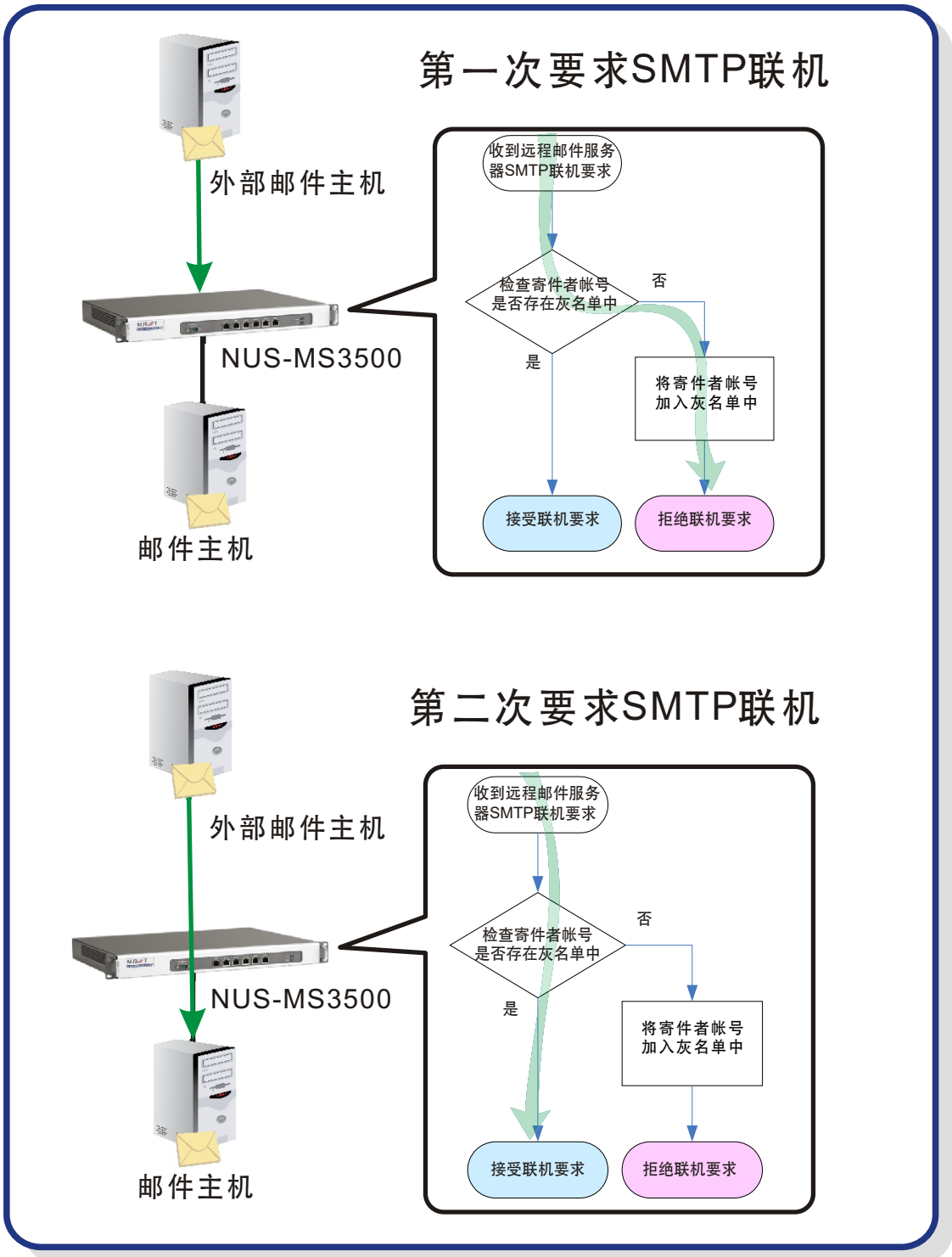
	新软公司灰名单过滤机制	一般市售产品灰名单过滤机制
差异	● 拥有灰名单数据库设计。 ● 列名于其中的寄件者帐号将不会再被灰名单过滤机制拒绝 SMTP 联机要求。信件传送快速。	● 没有灰名单数据库设计。 ● 每次信件的寄送，皆需要被拒绝一次后方能寄送成功。造成设备要花费较多的系统资源，来处理邮件。且容易造成邮件延後或无法寄达的情形。

由于这些垃圾邮件发送软件，其目的仅是在极短之时间内大量发送邮件，因此不会确认信件是否有寄送成功，而只是一味的在做寄送的动作。所以，一但阻绝其寄送的联机，它也不会做尝试重寄的动作。由此，新软 MS 系列产品可排除大量可疑的信件，不仅解决收件者的困扰，也可降低系统邮件处理的负荷量。(如图一)



图一 灰名单过滤 V.S. 垃圾邮件发送主机

至于正常邮件服务器在传送“新寄件者账号”之信件时，灰名单过滤机制一样会拒绝其第一次 SMTP 联机要求。而与垃圾邮件发送软件不同的是，当联机失败后，正常邮件服务器会尝试再次联机。这时，灰名单过滤机制将不再阻挡，信件也就传送成功。（如图二）



图二 灰名单过滤 V.S. 正常邮件服务器

文 程智伟 rayearth@nusoft.com.tw

市场营销报导 - 高精准度垃圾邮件过滤机制

垃圾邮件的泛滥已不再只是一件麻烦事而已，对企业信息部门而言，它的存在势必成为将来法律责任问题以及枯竭企业生产力的主要隐忧。不仅严重消耗员工的生产力与浪费珍贵的 IT 资源（例如：磁盘储存空间与网络带宽），同时也因为夹杂未知病毒程序，而使得企业网络遭受不明的攻击以致网络瘫痪，或公司重要敏感信息外流等情况发生。为因应此趋势，新软公司将多项垃圾邮件过滤机制导入 MS 系列产品之中，其中包括：指纹辨识过滤、贝氏学习过滤、垃圾邮件特征过滤、灰名单过滤等，使得垃圾邮件辨识率可达 99%，藉此协助企业避免上述问题的发生（如 图一）。

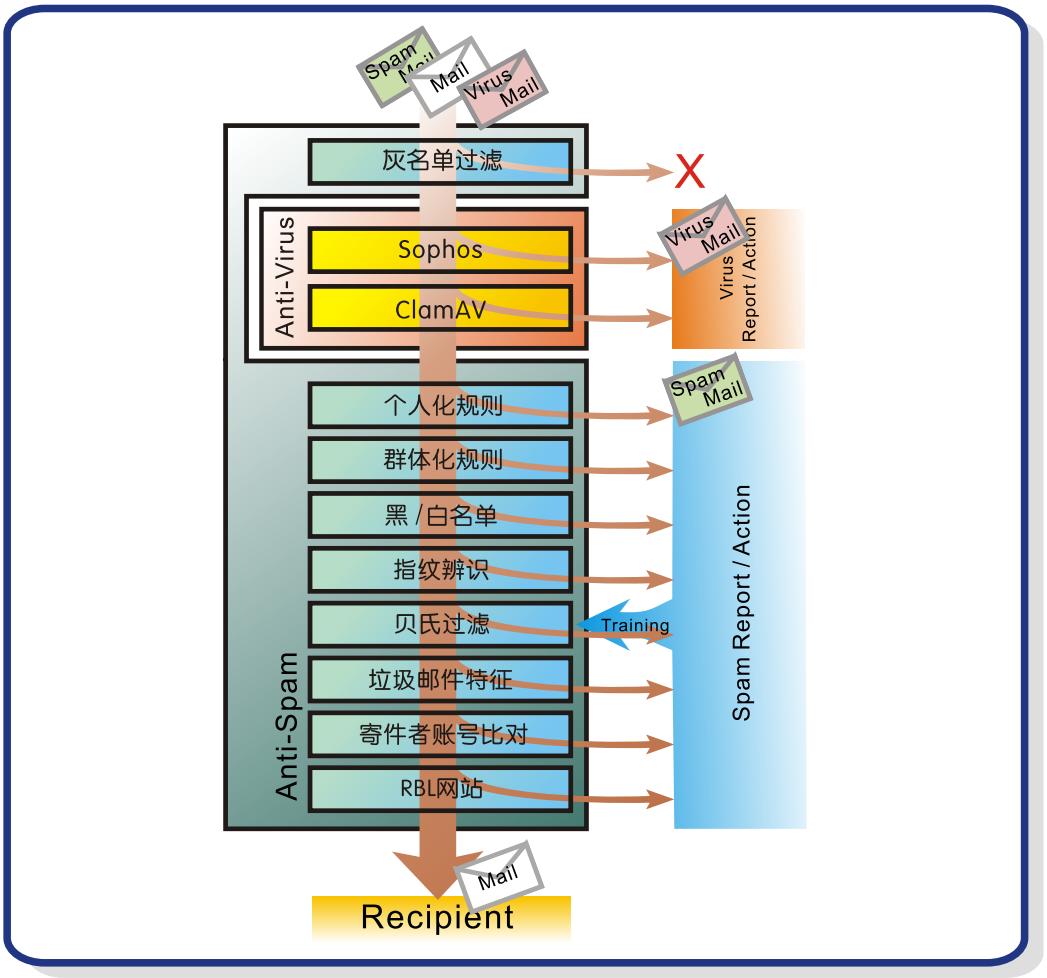


图 一 新软公司垃圾邮件过滤流程示意图

灰名单过滤：
利用垃圾邮件发送主机使用伪造的寄件者账号大量发送信件，却不检查信件发送是否成功的特性。拒绝所有“新寄件者账号”的第一次 SMTP 联机，以达到防堵垃圾邮件之目的。

个人 / 群体化规则：
使用者可自行订定个人的黑白名单，管理人员也可订定企业的邮件规则。个人与群体化规则的优先权可由管理人员自行订定。

黑 / 白名单：
管理人员可将企业往来之客户订定为白名单，将不请自来的“电子报”订定为黑名单。

指纹辨识（DNA 辨识）：
将信件以特殊方式换算为一指纹码，在与网络上的指纹库做比对，符合者即为垃圾邮件。指纹库是由成千上万的使用者协力构成；当一封信被大多数的使用者认为是垃圾信件时，指纹库会收录将该信件之指纹码。

贝氏过滤：
贝氏过滤法是将信件之内文以贝氏数据库之规则来评分，分数越高者其越有可能是垃圾信件。贝氏数据库拥有自动学习之功能，可针对企业之收信状况调整为最适合之过滤条件。

垃圾邮件特征：
将信件与新软特制的垃圾邮件特征码比对，检查信件各项特征是否符合垃圾信件特征。垃圾邮件特征数据库会随时针对各种新型垃圾邮件而做出更新。

寄件者帐号比对：
一般垃圾邮件的寄件者账号皆为伪造，利用比对寄件者账号是否存在之方式检查信件是否为垃圾信件。

RBL 网站：
比对信件的来源 IP 是否与网络上的 RBL 网站之垃圾邮件黑名单相同。

市面上充斥着许多自称可精准判别垃圾邮件的网络设备，但实际上却都以简易的功能滥竽充数，使得企业的垃圾邮件问题并不能因此得到改善。有鉴于此，新软公司则针对一直推陈出新的垃圾邮件运作手法，做相关的研究和分析，并适时调整应对的机制，导入设备中，以有效吓阻此情形。

	新软公司邮件过滤机制	一般市售邮件过滤机制
扫毒引擎	内建双扫毒引擎 ClamAV Sohpos	内建单一扫毒引擎
垃圾邮件特征过滤	○	×
指纹辨识过滤	○	大多只具备邮件帐号判断过滤，和来源 IP 黑名单过滤的辨识能力
贝氏学习过滤	○	
灰名单	○	
邮件帐号判断过滤	○	
来源 IP 黑名单过滤	○	

文 程智伟 rayearth@nusoft.com.tw