新軟週報
http://www.nusoft.com.tw
Internet Security Fighter
2007/3/19 - 2007/3/25 第20期

多功能 UTM / MS 系列報導

技術淺談與應用 - 利用灰名單過濾垃圾郵件

垃圾郵件的型態變化過於迅速，常常造成許多預防措施成效不彰，而各廠家陸續推出的解決方案，也大多是治標不治本的方法，有時或許能立竿見影，但長久下來已造成使用者信心動搖、不堪其擾的負面影響。

傳統的郵件帳號判斷和黑名單(RBL)過濾機制，由於垃圾郵件寄送內容的篡改，和疏漏的回報系統，已經喪失對其判別的精確度，常常導致企業往來郵件無法遞送的情形，許多交易因而停擺，無形中扼殺了企業的競爭力。

現在大多數的垃圾郵件，皆是透過大量發送郵件的軟體做寄送的動作。而這種發送方式有一特點，就是以隨機偽造的寄件者帳號，針對所蒐羅到的收件者做一次發信的動作。對於此情形，新軟公司觀察此類郵件發送模式，並研發出相應的解決技術，務求根治大多數的災情，經數度改良後，獨創一格的**灰名單過濾機制**終於問世，並將其導入 MS 系列產品之中。

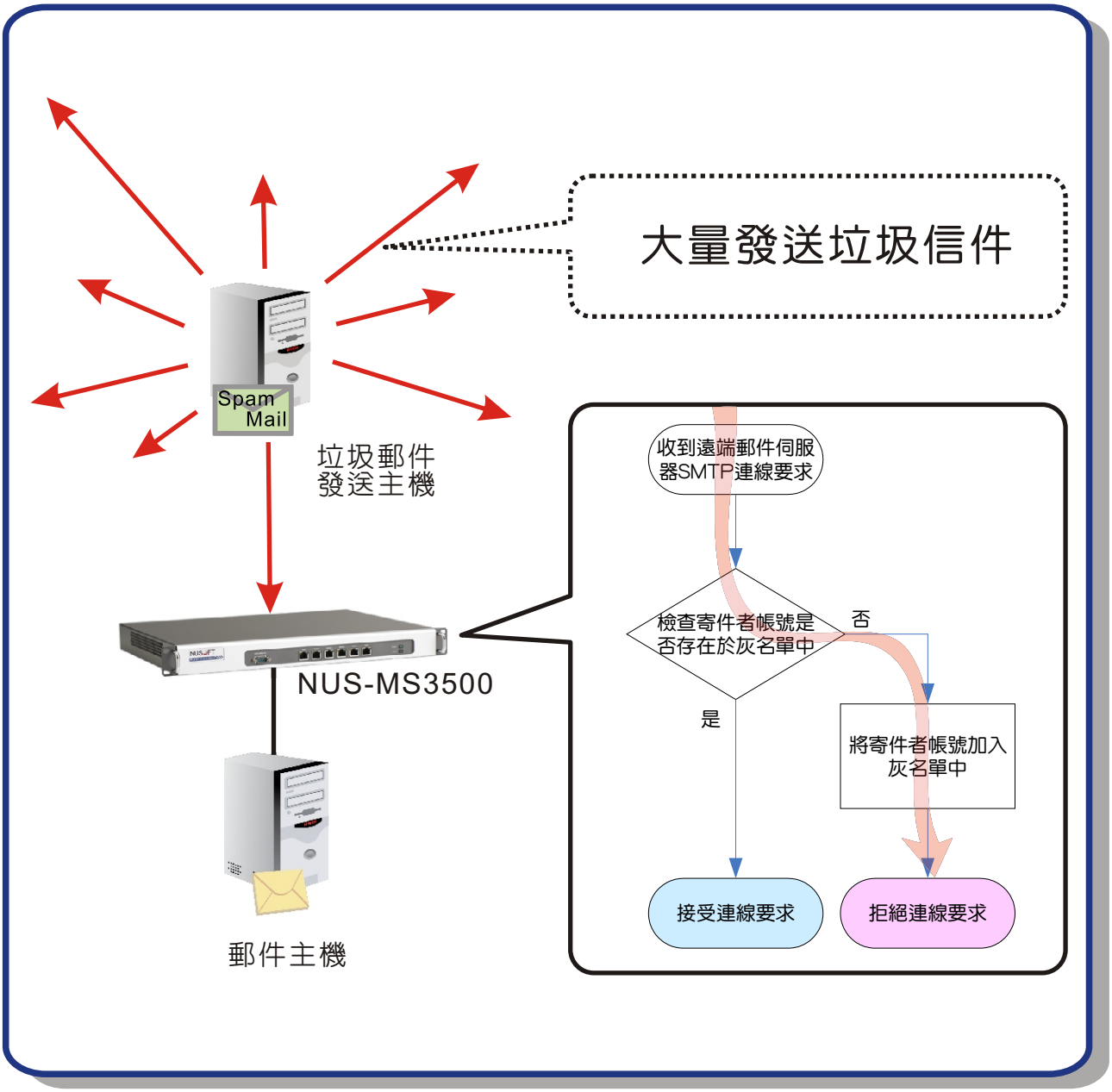
- 新軟－**灰名單過濾機制**，以下列方式運作：

  1.無條件拒絕任何外部郵件伺服器 “新寄件者帳號” 的第一次 SMTP 連線要求。
  2.會將上述的 “新寄件者帳號” 列入 “灰名單” 中。
  3.往後，**灰名單過濾機制**將不再拒絕列名於 “灰名單” 中的寄件者帳號之SMTP 連線要求，而將垃圾郵件過濾任務交由其他機制處理。

- 新軟 MS 系列產品內建的灰名單過濾機制，和一般市售具有此功能設備的比較（如下表）：

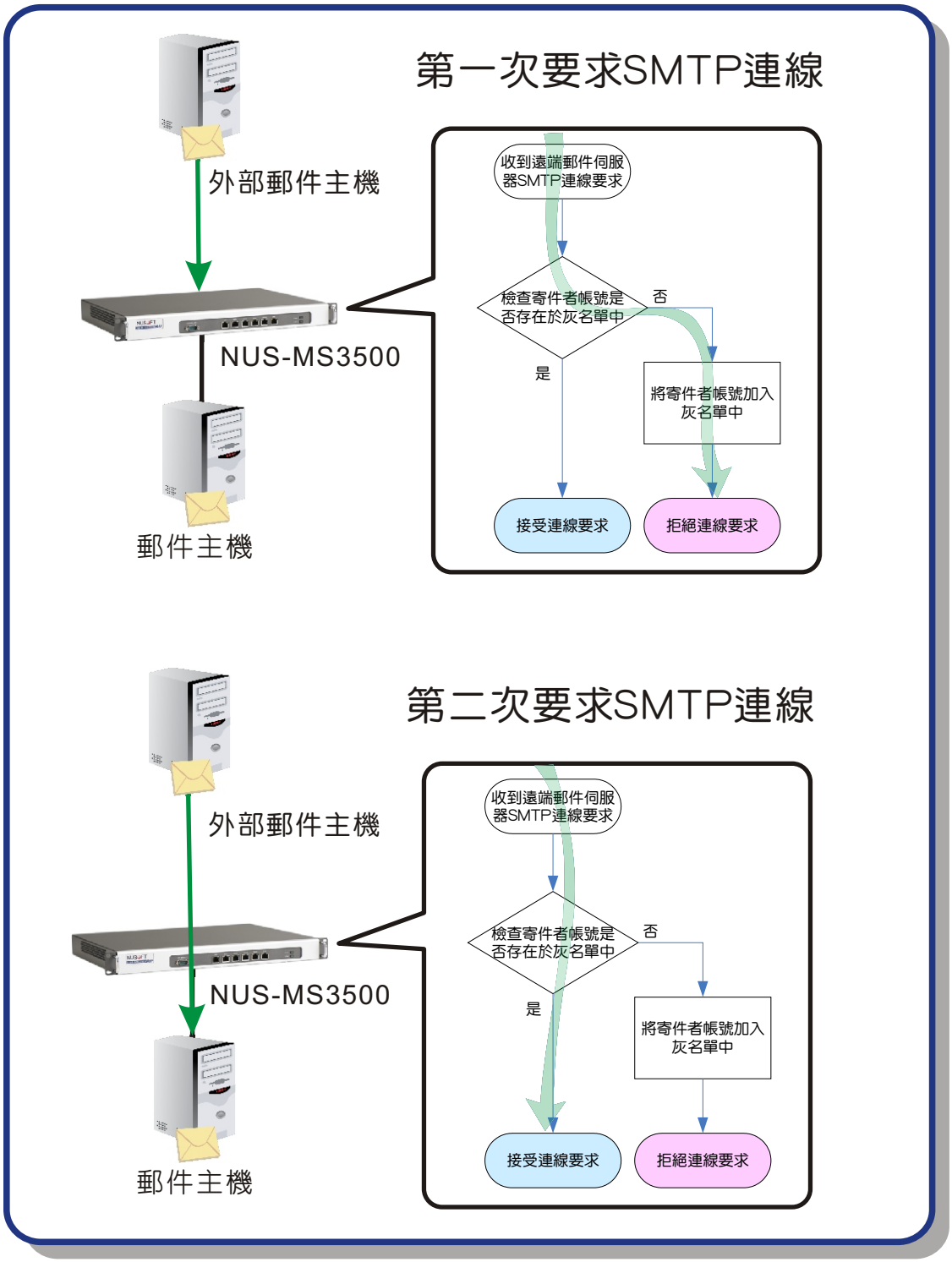
	新軟公司灰名單過濾機制	一般市售產品灰名單過濾機制
差異	● 擁有灰名單資料庫設計。 ● 列名於其中的寄件者帳號將不會再被灰名單過濾機制拒絕 SMTP 連線要求。信件傳送快速。	● 沒有灰名單資料庫設計。 ● 每次信件的寄送，皆需要被拒絕一次後方能寄送成功。造成設備要花費較多的系統資源，來處理郵件。且容易造成郵件延後或無法寄達的情形。

由於這些垃圾郵件發送軟體，其目的僅是在極短之時間內大量發送郵件，因此不會確認信件是否有寄送成功，而只是一昧的在做寄送的動作。所以，一但阻絕其寄送的連線，它也不會做嘗試重寄的動作。由此，新軟 MS 系列產品可排除大量可疑的信件，不僅解決收件者的困擾，也可降低系統郵件處理的負荷量。(如圖一)



圖一 灰名單過濾 V.S.垃圾郵件發送主機

至於正常郵件伺服器在傳送“新寄件者帳號”之信件時，灰名單過濾機制一樣會拒絕其第一次 SMTP 連線要求。而與垃圾郵件發送軟體不同的是，當連線失敗後，正常郵件伺服器會嘗試再次連線。這時，灰名單過濾機制將不再阻擋，信件也就傳送成功。（如圖二）



圖二 灰名單過濾 V.S. 正常郵件伺服器

文 程智偉 rayearth@nusoft.com.tw

市場行銷報導 - 高精準度垃圾郵件過濾機制

垃圾郵件的氾濫已不再只是一件麻煩事而已，對企業資訊部門而言，它的存在勢必成為將來法律責任問題以及枯竭企業生產力的主要隱憂。不僅嚴重消耗員工的生產力與浪費珍貴的 IT 資源（例如：磁碟儲存空間與網路頻寬），同時也因為夾雜未知病毒程式，而使得企業網路遭受不明的攻擊以致網路癱瘓，或公司重要敏感資訊外流等情況發生。為因應此趨勢，新軟公司將多項垃圾郵件過濾機制導入 MS 系列產品之中，其中包括：指紋辨識過濾、貝氏學習過濾、垃圾郵件特徵過濾、灰名單過濾等，使得垃圾郵件辨識率可達 99%，藉此協助企業避免上述問題的發生（如 圖一）。

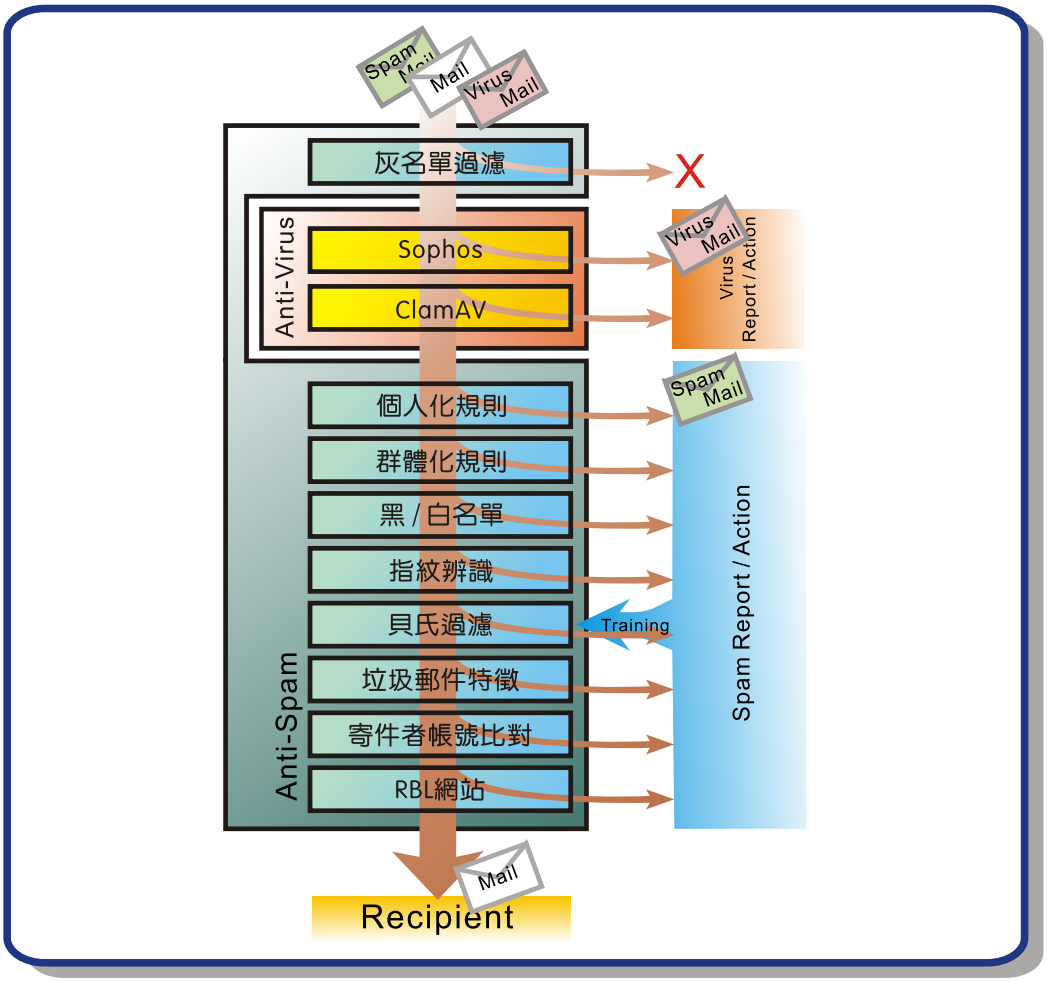


圖 一 新軟公司垃圾郵件過濾流程示意圖

灰名單過濾：

利用垃圾郵件發送主機使用偽造的寄件者帳號大量發送信件，卻不檢查信件發送是否成功的特性。拒絕所有“新寄件者帳號”的第一次 SMTP 連線，以達到防堵垃圾郵件之目的。

個人 / 群體化規則：

使用者可自行訂定個人的黑白名單，管理人員也可訂定企業的郵件規則。個人與群體化規則的優先權可由管理人員自行訂定。

黑 / 白名單：
管理人員可將企業往來之客戶訂定為白名單，將不請自來的“電子報”訂定為黑名單。

指紋辨識（DNA辨識）：
將信件以特殊方式換算為一指紋碼，在與網路上的指紋庫做比對，符合者即為垃圾郵件。指紋庫是由成千上萬的使用者協力構成；當一封信被大多數的使用者認為是垃圾信件時，指紋庫會收錄將該信件之指紋碼。

貝氏過濾：
貝氏過濾法是將信件之內文以貝氏資料庫之規則來評分，分數越高者其越有可能是垃圾信件。貝氏資料庫擁有自動學習之功能，可針對企業之收信狀況調整為最適合之過濾條件。

垃圾郵件特徵：
將信件與新軟特製的垃圾郵件特徵碼比對，檢查信件各項特徵是否符合垃圾信件特徵。垃圾郵件特徵資料庫會隨時針對各種新型垃圾郵件而做出更新。

寄件者帳號比對：
一般垃圾郵件的寄件者帳號皆為偽造，利用比對寄件者帳號是否存在之方式檢查信件是否為垃圾信件。

RBL 網站：
比對信件的來源 IP 是否與網路上的 RBL 網站之垃圾郵件黑名單相同。

市面上充斥著許多自稱可精準判別垃圾郵件的網路設備，但實際上卻都以簡易的功能濫竽充數，使得企業的垃圾郵件問題並不能因此得到改善。有鑑於此，新軟公司則針對一直推陳出新的垃圾郵件運作手法，做相關的研究和分析，並適時調整應對的機制，導入設備中，以有效嚇阻此情形。

	新軟公司郵件過濾機制	一般市售郵件過濾機制
掃毒引擎	內建雙掃毒引擎 ClamAV Sohpos	內建單一掃毒引擎
垃圾郵件特徵過濾	○	×
指紋辨識過濾	○	大多只具備郵件帳號判斷過濾，和來源 IP 黑名單過濾的辨識能力
貝氏學習過濾	○	
灰名單	○	
郵件帳號判斷過濾	○	
來源 IP 黑名單過濾	○	

文 程智偉 rayearth@nusoft.com.tw