新軟週報
http://www.nusoft.com.tw
Internet Security Fighter
2009/7/13- 2009/7/26 第96期

郵件伺服器 / ML 系列報導

技術淺談與應用 - 公司如何避免內對內信件傳送被誤判成垃圾郵件

在今日高度網路化的商業環境裡，公司企業無不依賴電子郵件傳遞或收發大量商業訊息以維持組織運作，除了對外的聯繫之外，為了在每項作業都能有個重要的記錄依據，於公司內部間的溝通也同樣的早已將電子郵件用來做為最主要的管道之一。

然而科技所帶來的影響，除了創造了不少的便利之外同樣也夾雜了不少的負面情況。垃圾郵件就是其中之一，現今垃圾郵件「污染」網路世界的情況到底多嚴重？這個問題相信在每個人心中都早已有了明確的答案。也正因為如此，企業紛紛的導入相關的資安防護設備，以維持正常運作。為解決擾人的垃圾郵件問題，新軟系統所推出的『郵件伺服器 - ML』，一直以來深受企業與公司的喜愛，正因為『郵件伺服器 - ML』擁有了強大的防護功能以防止擾人的垃圾郵件再度來襲。

但垃圾郵件的欺騙手法也同樣不斷的在更新，發送者為了將信件送達至收件者信箱，其中一項手法則是利用偽造信件中的郵件地址來欺騙該公司郵件伺服器中的過濾機制，讓郵件伺服器認為是公司裡內部對內部之間所相互傳送的信件而放行，因而造成公司內部人員不斷的收到煩人的垃圾郵件。所以網路管理人員若是將公司內對內的信件皆設為無條件通行的情況，將有可能會因此而再一次的飽受垃圾郵件所困擾。為了避免這類的情形發生，該如何去設定郵件伺服器上的阻擋規則，而最為重要的是又不會將內部所傳送的信件誤判為 SPAM 而遭阻擋才好呢？除此之外，於公司內，同事與同事間的信件傳送，通常會單純只以一個夾檔的方式來寄送，而這樣的方式和單純只以單一圖片之類的垃圾郵件寄送內容相似，以至於有可能會因此遭郵件伺服器所阻擋，管理人員又該如何去解決？

首先，管理人員先進入“郵件安全 > 郵件過濾 > 全體化規則”，同時新增 2 項規則。

全體化規則內容第 1 項：

1. 將規則分類設為“Ham（Non-Spam）”。
2. 組合方式設為“And”。
3. 新增一條項目為“Received”、條件為“Contains”、郵件特徵為“公司所設定的郵件伺服器 IP”的規則條件。
4. 新增一條項目為“From”、條件為“Contains”、郵件特徵為“公司所申請之 Domain name”的規則條件。

全體化規則設定範例圖片

全體化規則內容第 2 項：

1. 將規則分類設為“Ham(Non-Spam)”。
2. 組合方式設為“And”。
3. 新增一條項目為“Received”、條件為“Contains”、郵件特徵為“公司內部(LAN)的網段 IP”的規則條件。(此條件為預防公司內部寄件者將 Outlook 中 SMTP 部份直接填為郵件伺服器之 LAN 端 IP 位址，而非 Domain。因為若是直接填為郵件伺服器之 LAN 端 IP 位址，在內部傳送之信件所夾帶的 IP 會是使用者本身電腦中 LAN 端 IP。)

SMTP 所填內容為郵件伺服器之 LAN 端 IP

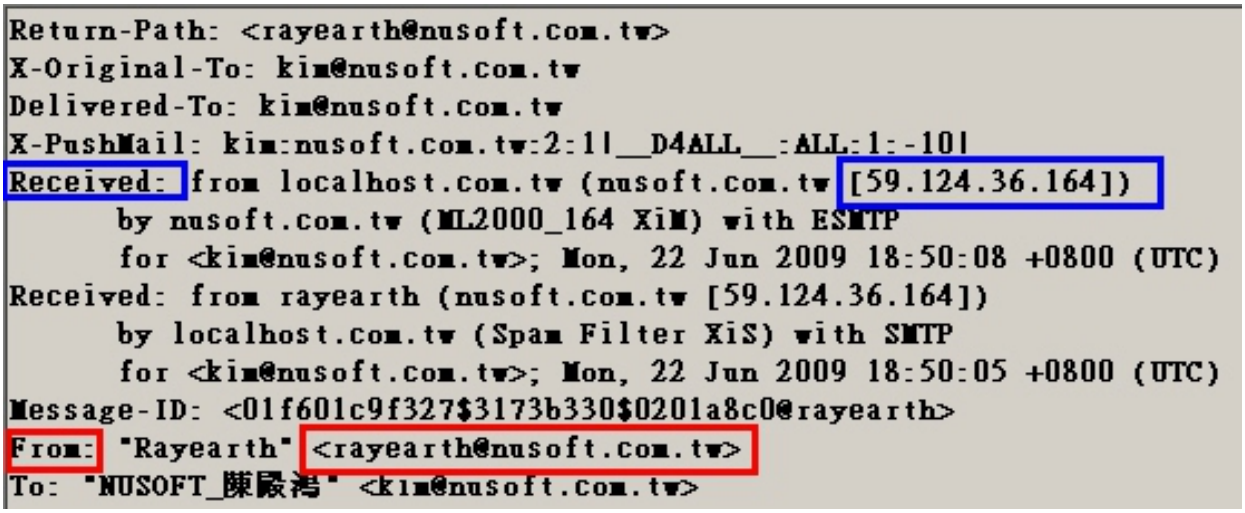
```
Return-Path: <kim@nusoft.com.tw>
X-Original-To: kim@nusoft.com.tw
Delivered-To: kim@nusoft.com.tw
X-PushMail: kim:nusoft.com.tw:2:1|__D4ALL__:ALL:1:-10|
Received: from localhost.com.tw (unknown [172.19.50.9])
      by nusoft.com.tw (ML2000_164 XiM) with ESMTP
      for <kim@nusoft.com.tw>; Thu,  2 Jul 2009 20:00:48 +0800 (UTC)
Received: from K (unknown [172.19.50.9])
      by localhost.com.tw (Spam Filter XiS) with SMTP
      for <kim@nusoft.com.tw>; Thu,  2 Jul 2009 20:00:58 +0800 (UTC)
```

寄送之郵件所夾帶 IP 為使用者電腦內部 IP

4. 新增一條項目為“From”、條件為“Contains”、郵件特徵為“公司所申請之Domain name”的規則條件。

全體化規則設定範例圖片

其如此設定的用義為何呢？因為發件者在偽造郵件位置來欺騙郵件伺服器時，所能變動偽造的為『From』(下圖紅色框部份)，而『Received』來源位置(下圖藍框部份)是無法做更動的，所以當伺服器收到信件後，判斷條件須是利用『and』的方式，將『From』、『Received』兩組條件皆符合該公司所設定之內容才能讓該信件正常通過。



信件原始檔截圖

如此一來若是有心人士偽造郵件位址來欺騙郵件伺服器以達到垃圾郵件的散播，則會因為沒達到規則條件內容而無法順利通過；反之，而當遇到真的是內部對內部之信件傳送時，也不會因阻擋機制而遭『郵件伺服器 - ML』誤判為 SPAM，而錯失掉重要的信件訊息。

文 陳殿鴻 kim@nusoft.com.tw

市場行銷報導 - 新軟「硬體式 Mail server」與一般「軟體式 Mail server」的差異

一般企業生意往來大多透過 Email 來傳達所有的商業訊息，因此電子郵件對企業來說，其重要性自然不在話下。因此一間有規模、有制度的公司，必然得有一台可容易控管且功能強大的電子郵件伺服器。

目前市場上以軟體式 Mail Server 及硬體式 Mail Server 最為廣泛使用。然而，很多人第一印象便是“我自己來架設軟體式 Mail Server 應該會比較容易、省錢吧？”，其實不盡然。

《一般軟體式 Mail Server》：

一般軟體式郵件伺服器架設方式，無非是購入一台電腦硬體，然後安裝作業系統，接著安置 Mail Server 軟體、防毒軟體…等等，最後再做相關設定及一連串的測試然後再實機上線。

這樣的架設方式乍看之下難度似乎不高，其實並非如此。從技術層面來看：在系統建置時，首先就得面臨使用哪個作業系統(Windows 或 Linux，若使用 Windows 雖然安裝較容易，但是其版權成本極高且較耗系統資源，再加上容易成為駭客“照顧”的目標；若使用 Linux 雖然無需版權費用且安全性與穩定性較高，但是其安裝時得對於 Linux 操作有專業的技術)，接著面臨 Mail Server 軟體、防毒軟體…等等成本及技術上的考量，最後還得在後續維護成本上花不少的費用及時間和功夫，在種種問題解決後便將軟體式 Mail Server 架設完成。

然而，這只是最原始功能之 Mail Server 而已，此時系統就像是堆積木一樣地將各種所需元素堆積起來，若之後還需增加進階功能時就得大幅變動系統之架構設計，管理人員所耗的時間就會越來越多，不可掌控的變數也就越來越多了，甚至容易使得系統因此而變的更為脆弱。

《新軟硬體式 Mail Server》：

新軟系統所推出的硬體式郵件伺服器 - ML 系列，貫徹「輕鬆架設、功能完整、維護簡單」此設計理念。在硬體上以安全、穩定的嵌入式 Linux 系統為核心平台。在軟體上，以簡單、人性化的操作介面呈現於管理者面前，無須豐富的專業知識也可以輕鬆架設。

在相關郵件服務、稽核等功能上也一應俱全，另外擁有獨家帳號信件無痛移植功能，取代企業原有郵件伺服器，快速方便且可以與 LDAP 伺服器搭配結合做完整帳號整合。在防毒機制上也以 ClamAV 等兩種掃毒機制嚴陣以待。而針對變化性極大的 SPAM 垃圾信，新軟以包含獨家提供的「垃圾郵件特徵碼」在內的七道垃圾郵件過濾機制，徹底掃蕩垃圾郵件。在備援機制問題上，以獨家的 HA 雙主機備援方式用以確保系統內所有資料的備援完整性。其他包含業務部門較常用的「Push Mail」、「WebMail」等功能也都貼心地建構於其中。

最後令公司企業最為關心的就是「系統後續維護成本」，新軟對產品用戶提供了完善的售後服務，對於垃圾郵件特徵碼、ClamAV 掃毒引擎病毒碼等更新服務上，皆不收取任何的費用。

新軟系統所推出之硬體式郵件伺服器 - ML 系列不單單只是一台會收發信件的機器而已；更重要的是它帶來更多更強大功能、更方便之操作介面以及減少後續維護時所花費的精神、時間、成本。如此一來，Mail Server 才能真正達到現代企業的完整需求。

	新軟硬體式 Mail server - ML 系列	一般軟體式 Mail server
軟硬體成本	低	高
建構技術成本	低	高
人力花費成本	低	高
後續維護成本	低	高
防毒防駭安全性	高	低
多樣強大功能	高	低
完整售後服務	有	無

新軟硬體式郵件伺服器 - ML 系列與一般軟體式 Mail Server 差異表。

文 黃政銘 ming@nusoft.com.tw