

# 中小企業商務應用 應用範例

## ■ 如何阻擋假借本機帳號傳送垃圾郵件

### 描述

相信很多企業爲了阻擋垃圾郵件的攻擊，設定了重重的關卡來防範。包含貝氏過濾法、個人化規則、黑白名單、垃圾郵件自動學習機制等，但是垃圾郵件傳遞者總是能輕易突破封鎖，藉由假借企業網域名稱選用一個不存在的帳號來做攻擊，透過僵屍電腦發送大量的垃圾郵件，因爲該收件人的帳號是不存在，所以郵件主機會退信給偽裝的寄件者，造成被偽裝的企業郵件主機收到大量的郵件退信通知，不僅造成郵件主機運作緩慢無法收信，甚至容易讓企業列入爲垃圾郵件黑名單的成員。

往常遇到這樣攻擊方式大多束手無策，如果不接收退信，則網域內正常的帳號無法接受到信件，造成管理者在郵件伺服器上維護的困擾。眾至資訊在郵件伺服器(MS系列)與UTM設備(AW系列)，提供企業阻擋偽裝企業網域不存在帳號垃圾郵件攻擊解決方案。

### 眾至解決方案

#### 解決方案一：郵件伺服器(MS系列)

寄件者偽造網域名稱與本機網域相同，但本機內卻無該帳號，因爲一般郵件伺服器處理內部對內部的信件通常比較寬鬆，不會被判斷成垃圾信件，這也是廣告信業者常用的發信方法。只要在Sharetech郵件伺服器設備上，將「寄件者偽造本機網域」勾選，即可阻擋非本機帳號的垃圾郵件攻擊。

## 中小企業商務應用 應用範例

|   |                                     |   |
|---|-------------------------------------|---|
| 過濾器名稱   | 寄件者偽造本機網域                           |   |
| 啟動  | <input checked="" type="checkbox"/> |   |
| 備註  |                                     |   |
| 過濾器條件 <span style="float: right;">操作說明</span> |                                     |   |
| 條件組合方式  | 只要其中任何一個欄位符合即可(OR)                  |   |
| * 寄件者包含                                       | <input type="text"/>                | <input type="checkbox"/> 反向             |
| 寄件者偽造本機網域                                     | <input checked="" type="checkbox"/> | <span style="float: right;">操作說明</span> |
| * 收件者包含                                       | <input type="text"/>                | <input type="checkbox"/> 反向             |
| * 寄件來源IP包含                                    | <input type="text"/>                | <input type="checkbox"/> 反向             |
| 郵件表頭包含  | <input type="text"/>                | <input type="checkbox"/> 反向             |
| 郵件主旨包含  | <input type="text"/>                | <input type="checkbox"/> 反向             |
| * 郵件內容包含                                      | <input type="text"/>                | <input type="checkbox"/> 反向             |
| 郵件容量大於  | <input type="text"/> K bytes        |   |
| * 郵件附件檔名包含                                    | <input type="text"/>                | <input type="checkbox"/> 反向             |

### 解決方案二：UTM設備(AW系列)

ShareTech UTM設備系統管理員可利用【郵件帳號】的【自動新增帳號至掃描帳號中並阻擋不掃描 / 不存在帳號中的郵件帳號】功能來防範，而當外部寄信給內部郵件伺服器的收件者，被內部郵件伺服器判別為合法帳號，並將此訊息回應給眾至UTM設備(AW-5150G、AW-5250G、AW-5350G)，則設備即會把此帳號列入【郵件帳號】的【掃描帳號】清單中。