新軟週報
http://www.nusoft.com.tw
Internet Security Fighter
2007/10/15- 2007/10/21 第46期

多功能 UTM / MS 系列報導

技術淺談與應用 - 淺談IDP入侵偵測防禦系統

隨著網際網路日益發達，絕大多數的企業也將其版圖擴張到這個領域，透過網際網路提昇企業競爭力。也因為企業網路對於企業來說重要度已經不可小覷，所以企業都會添購相關網路安全設備以確保企業網路安全無虞。

目前一般企業為保護其網路系統，採用防火牆作為企業網路進出的門戶，以確保企業網路之安全。防火牆雖可防止來自於網際網路之不明或惡意存取、攻擊行為，但也只能針對 OSI 模型 2~4 層的封包進行檢測來源、目的地、連接埠等欄位來對某個服務存取進行限制，並不能檢視所通過的封包是否有異常。因此對於企業網路來說，防火牆的保護已經日漸不敷使用。

為此，網路安全相關業者推出 IDS（Intrusion Detection System）入侵偵測系統以協助保護企業網路安全。IDS 的功能是針對 OSI 模型 5~7 層的封包進行檢測，可在偵測到問題時做相關記錄並及時發出警訊通報管理人員處理。 “IDS 可即時反應企業網路問題” 聽起來可以協助企業解決防火牆保護之不足，但實際上其僅能告知管理人員而無法自行阻擋，且常發生誤判的情況。在天天「狼來了！！」誤判警告下，網管人員只能疲於奔命的反覆查核該警告是否正確，而真正問題發生時，整個企業網路已經回天乏術。

IPS（Intrusion Prevention System）入侵防禦系統就是針對 IDS 僅能發現問題而無法解決問題之缺陷而發展出的新產品。IPS 能在偵測到入侵攻擊時，可立即阻斷該封包通過，以保護企業網路安全。IPS 遇到問題時能即時防禦，但如遇到誤判之狀況時，IPS 的防禦機制還是全面阻攔，明顯不具彈性。

為了徹底解決企業網路安全問題，新軟系統在其推出的新軟 UTM（MS 系列產品）中加入了最新一代的企業網路防禦利器 IDP（Intrusion Detection and Prevention）入侵偵測防禦系統。就如字面上的意思，IDP 結合了 IDS 的入侵偵測與 IPS 之入侵防禦功能，可以檢測出包藏在應用層裡的惡意攻擊碼（譬如：蠕蟲攻擊、緩衝溢位攻擊）並加以阻攔、警告。

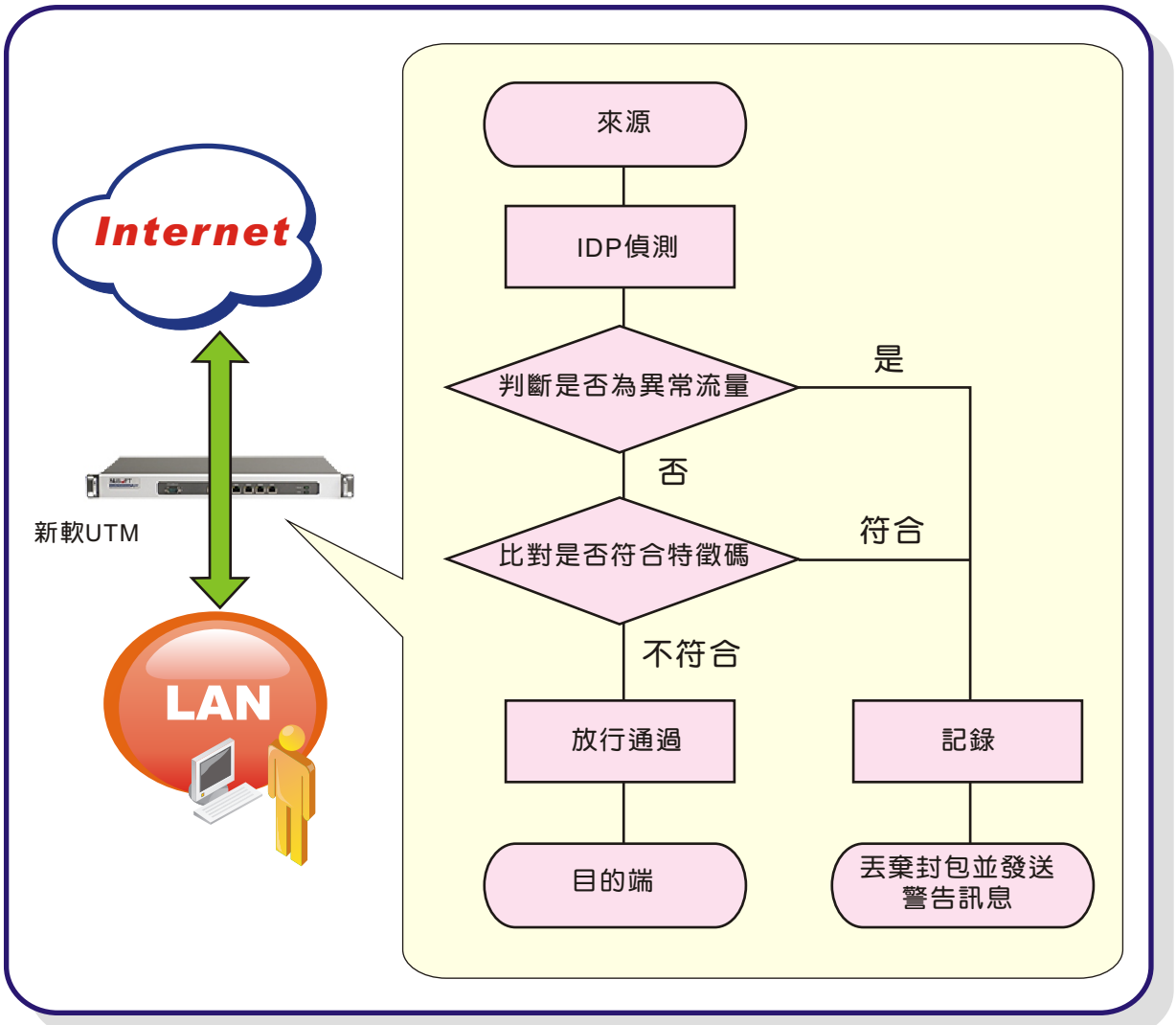
新軟 UTM 的 IDP 機制擁有兩種偵測功能－特徵比對偵測 與 異常偵測，來保護企業免於各種入侵或攻擊的危害：

特徵比對偵測機制－擁有一龐大的「IDP 特徵資料庫」，所有經過 IPD 掃描之封包只要與資料庫的特徵相符時，新軟 UTM 就會依照先前管理人員所訂定的處置方式處理該封包。

異常偵測機制－可針對各種網路攻擊模式防禦；當網路連線符合攻擊模式時，新軟 UTM 會將它視為網路攻擊，並依管理人員所訂定的處理方式處理該連線。

網路科技日新月異，當然各種入侵、攻擊手段也在進步。新軟 UTM 的 IDP 功能當然也要隨時更新，以迎接各項更加嚴峻的挑戰。因此，其內建的「IDP 特徵資料庫」會每兩小時自動上線檢查是否有新的特徵檔可下載，以維持資料庫在最新的狀態。另外，網管人員亦可以針對企業網路實際需求，自訂所要的特徵，讓新軟 UTM 的 IDP 防護更具彈性。

網路的普及帶給人們方便卻也蘊藏著許多的危機。“如何安全運用網路為企業帶來商機”已經成為企業重點工作之一。不安全的網路環境就如同企業根基埋藏著不定時炸彈，一但引爆將嚴重影響企業之運作。而防火牆對於目前嚴峻的網際網路環境已不堪負荷，擁有 IDP 的新軟 UTM 必然是企業最佳之選擇。



文 黃智傑 alex@nusoft.com.tw

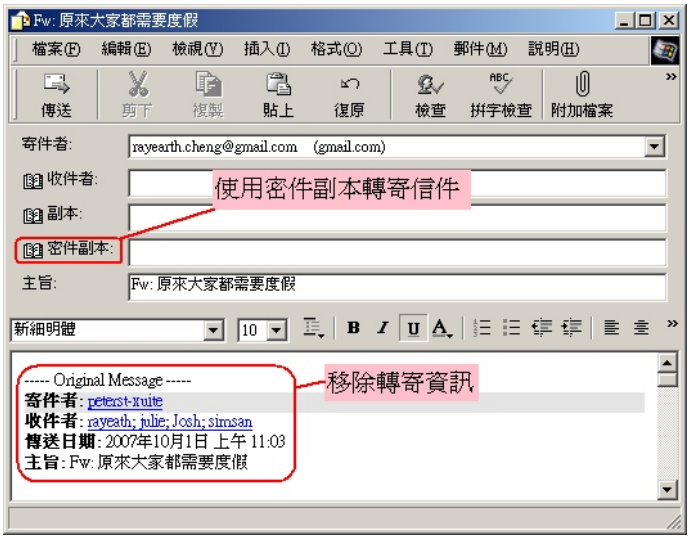
市場行銷報導 - 要如何減少惱人的垃圾郵件

垃圾郵件滿坑滿谷實在討人厭，要如何減少垃圾郵件呢？

想要減少垃圾郵件，就必須從垃圾蟲（Spammer，指濫發垃圾郵件者）如何收集郵寄名單談起。一般垃圾蟲所用的郵寄名單採取了下列做法收集：

善意的轉寄信件－當您收到一封由朋友轉寄而來之信件，且覺得其內容真的很不錯時，是否會將該信件再轉寄給其他親朋好友，將它分享出去呢？如果您常做上述這個動作可能就要小心了，因為您可能正在“協助”垃圾蟲收集名單！！

這些轉寄信件中常常富含著眾多電子郵件帳號（在轉寄資訊中），因此在轉寄信件時沒有使用「密件副本」或是將「轉寄資訊」移除時，很容易讓有心人士收集郵件名單。



圖一 轉寄信件時的必須動作

字典式嘗試法－此種方法較常使用於名氣大的郵件服務提供商，像是 Hotmail、Yahoo、Hinet、163...。垃圾蟲會用「字典」（包含常見的人名、字串、數字...）來排列組合猜測使用者的郵件帳號。因為郵件伺服器會將寄給無效郵件帳號之信件退回給寄件者，垃圾蟲可藉此判斷該郵件帳號是否有效。

一般會員網站－在註冊一些會員制網站時，通常註冊資料都會要求使用者提供郵件帳號。而這些郵件帳號常會因網站為了貪圖獲利、網站系統被駭客竊取資料...原因，被販賣給垃圾蟲作為垃圾郵件郵寄名單。

討論區、留言版－垃圾蟲常在各大討論區、留言板、BBS 站...中，利用搜尋程式搜集各篇文章作者所留下的郵件帳號。因此，在這些討論區、留言板中越活躍的作者，越容易收到垃圾郵件。

郵件代轉－近期內因中國大陸地區開始運行「網路防火牆長城（GFW）」，使得在中國大陸的使用者利用境外之郵件伺服器會發生傳輸上的問題。因此，使用者開始透過各種方式試圖避開此困擾，其中的一種方式就是利用境外沒有被封鎖的 Mail Relay Server 轉信。

使用免費的 Mail Relay Server 轉信雖然可以成功將信件寄出，但是有心人士可以從 Mail Relay Server 的記錄檔中輕易收集郵件地址。從今以後，不管是收件者還是寄件者將會被大量垃圾郵件侵擾。

網站自行公佈－一般企業網站為了服務客戶，通常會在網站中公佈聯絡用的郵件帳號（通常是業務、服務人員之郵件帳號）。也導致這些郵件帳號每天都會有收不完的垃圾信件，嚴重拖慢業務處理速度。

怎麼樣，瞭解這些垃圾郵件名單的收集方式之後，是不是發現自己常常犯了這些錯誤呢？為了避免垃圾郵件的侵擾，有下列幾種方式可供參考：

1. 轉寄信件時使用「密件副本」並將「轉寄資訊」移除
就如先前所提及的，要轉寄好文章給親朋好友時，務必使用「密件副本」並將「轉寄資訊」移除，也最好在信中提醒收件者採取相同步驟。

2. 不要購買垃圾郵件所廣告的商品
當您採買了利用垃圾郵件廣告的商品時，也會向垃圾蟲透露了一個重要訊息「這個郵件帳號是有效的！！」。往後您將會有收不完的垃圾信件。

3. 使用兩個以上的郵件帳號
除了主要的郵件帳號外，您可再申請數個郵件帳號作為“申請會員”、“線上購物”、“抽獎”...之用。盡量分類電子郵件信箱，不要任意透露主要的郵件帳號給不相干的人士，以防郵件帳號流入垃圾蟲之手中。

4. 封鎖電子郵件的圖片檔
目前有許多垃圾郵件是採用圖片方式來傳遞廣告訊息。此種方式除了比較容易躲避一般垃圾郵件過濾系統的查緝外，該信件之圖片在下載時亦可傳遞收件者資訊給垃圾蟲；垃圾蟲可藉此了解「該郵件帳號尚有人會閱覽信件」。因此，最好可禁止收信軟體主動下載圖片。

這也就是為甚麼新軟 UTM（MS 系列產品）、郵件伺服器（ML 系列產品）、網路記錄器（IR 系列產品）在顯示其所記錄、備份的信件中，不會主動顯示圖片之原因。

5. 審慎查核網站之同意書
當您在註冊網站會員時，千萬要細讀網站的“會員同意書”－部份網站會詢問“是否願意收到「合作夥伴」的電子郵件”。當您完全沒有閱讀“會員同意書”一路按下【下一步】時，您已將自己的郵件帳號賣給了垃圾蟲。

6. 千萬不要回覆垃圾郵件的「取消訂閱」
   垃圾郵件的「取消訂閱」按鈕通常是個幌子，點選後只會告訴垃圾蟲「這個郵件帳號是有效的！！」，往後您會有更多的垃圾信件。

7. 取個較複雜的“郵件帳號”
   字典式嘗試法的郵件帳號收集方式只會用「字典檔」中的字串去做嘗試，如果您的郵件帳號超過「字典檔」的範疇，垃圾蟲將無法試出您的郵件帳號。

8. 透過加密方式連線境外郵件伺服器（中國大陸地區）
   不要透過 Mail Relay Server 傳送信件，新軟郵件服器提供了 SMTPS、POP3S 這兩種加密服務可供使用者選用，完全可避開 GFW 所造成的無法寄信之問題。

企業可依上述方式教育旗下員工如何使用電子郵件之外，建議企業還是必須建構一垃圾郵件過濾系統，來濾除垃圾郵件。畢竟，企業窗口所使用之電子郵件帳號必須公諸於世，當然會詳記於垃圾蟲的「工商名錄」中。

新軟系統所推出的多功能 UTM（MS 系列產品）與 郵件伺服器（ML 系列產品）就含有為企業量身打造的垃圾郵件過濾系統。該系統內建了多層垃圾郵件過濾機制，以層層把關方式將垃圾郵件一一濾出，封鎖在其內建的隔離區中，還給企業一個乾淨的電子郵件環境。因此，企業窗口再也不用擔心被垃圾郵件所掩埋，無需費心如何找到那重要的「客戶信件」！！

文 程智偉 rayearth@nusoft.com.tw