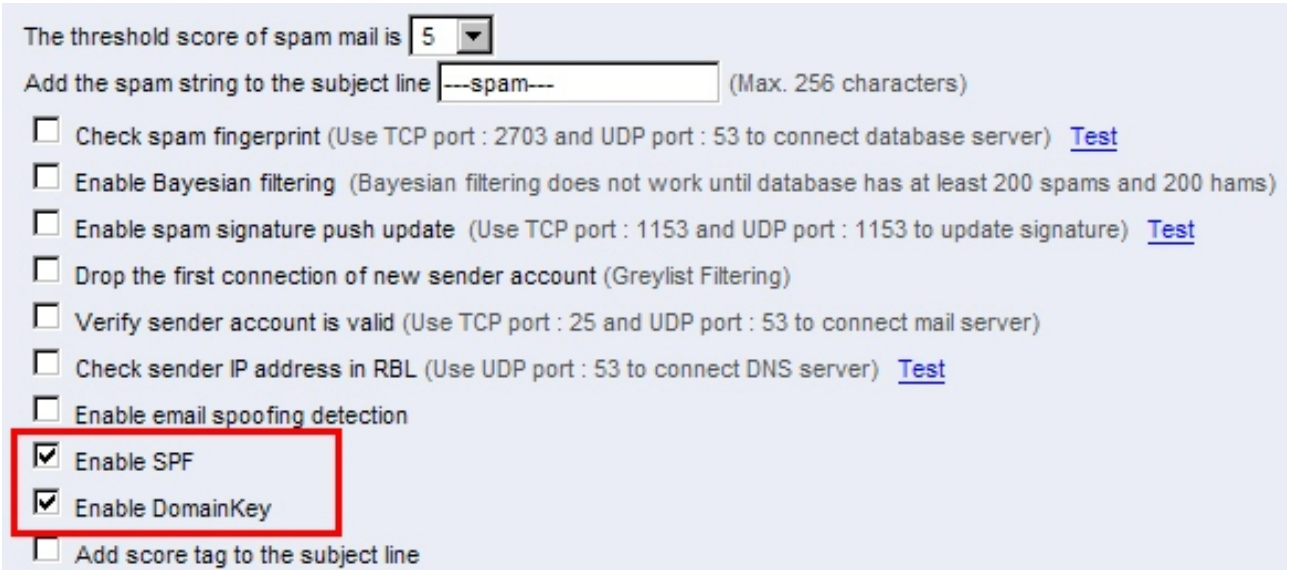
新軟週報
http://www.nusoft.com.tw
Internet Security Fighter
2009/12/14- 2009/12/27 第107期

## 多功能 UTM / MS 系列報導

# 技術淺談與應用 – SPF 與 DomainKey 的差異

網路電子郵件讓彼此之間的溝通縮短了距離，同樣卻也因如此的便利性讓使用者飽受有心人事的騷擾；垃圾郵件的影響，至今依然只能夠仰賴防護機制來降低影響程度，隨著垃圾郵件不斷的創新入侵方式，防護機制也因此不斷的在更新阻擋機制。

隨著不斷推出之新垃圾郵件防護機制，身為公司內部網路管理人員同樣也必須先去瞭解，而後再加強公司內的防護系統，但在眾多的防護機制下要一項一項熟悉也非一時三刻可做到的事情，甚至有讓人搞混的情況發生。新軟系統於多功能 UTM - MS 中 V5.08 版新增了幾項垃圾郵件過濾功能，其中有些許相似之處的為『SPF』、『DomainKey』兩項過濾功能，此兩項功能雖同為針對『偽造 Domain』這方向來做防護，但其運作原理實為不同，為了能讓管理人員能清楚釐清兩項功能，以下將分別一一做說明。

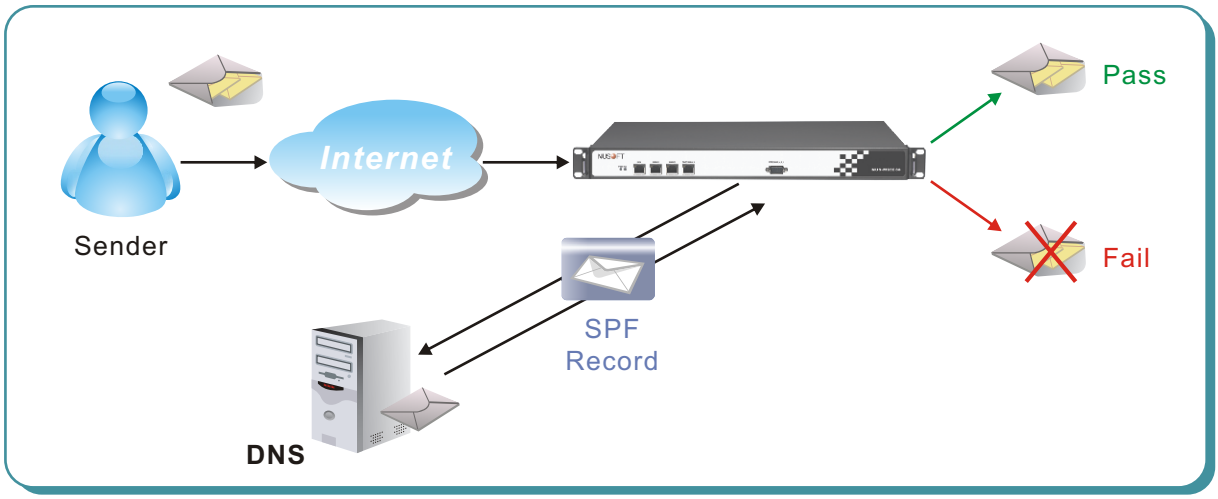



可於 Mail Security > Anti-Spam > Setting 下啟動『SPF』、『DomainKey』兩項過濾功能

**SPF**

由於同一個網域名稱可能透過多台的 mail server 或是 ISP 寄信，所以只單靠反解的方式來做偵測，已不敷現在需求，因此有效的網域驗證是目前防護機制中不可或缺之功能。

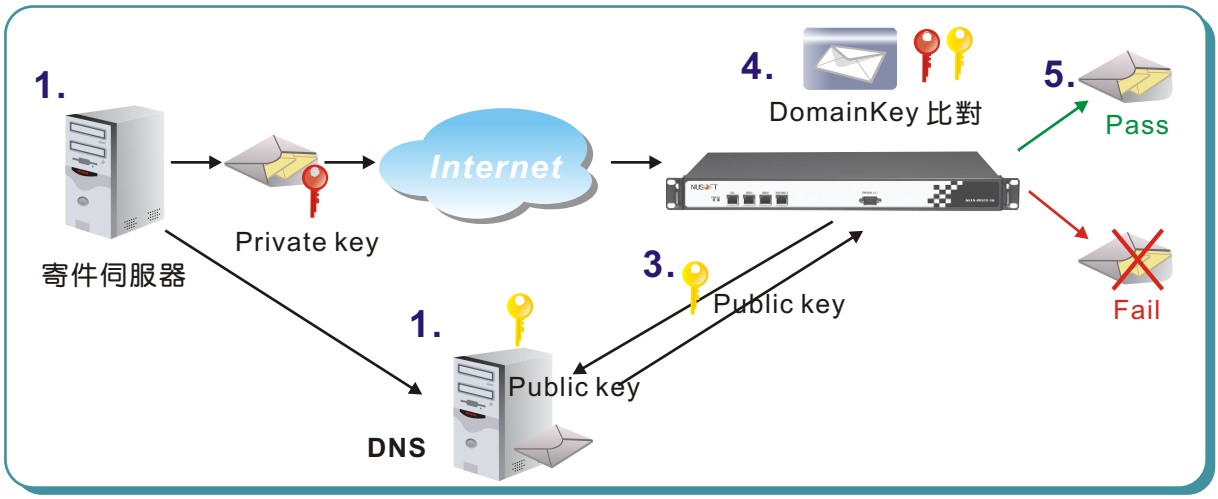
Sender Policy Framework 簡稱為 SPF，SPF 主要作為反偽造郵件的解決方案，SPF 過濾機制最主要是用來檢查 SMTP Server 是否有偽造其它人的 Domain 或是虛設 Domain 之情況發生，SPF 會根據 Domain Name 的 SPF 記錄確認連結的 IP 是否內含 SPF 記錄，透過此方式來宣告這個網域名稱的信件可能透過哪幾個 IP 或網址寄出，其他的就是非法的，若該封信件是由正式 DNS 內的郵件伺服器發出，那麼即可避免有心人事利用假冒網域之方式來發送信件。




SPF 機制運作流程示意圖

**DomainKey**

主要是在設計一套 Email 的認證方式，以增加在垃圾郵件的判讀能更準確，雖然此機制與 SPF 機制一樣都是針對網域來做驗證，但 DomainKey 卻比較僅慎且複雜些。該機制做法主要於 MTA 發送信件時同時產生『公開鑰匙（Public key）』、『非公開鑰匙（Private key）』兩組 Key，並以自己的 Private key 對表頭（Mail Header）加密計算，產生一組簽章，而另一組 Public key 則在寄信的過程中存入「網域名稱伺服器（DNS）」中，當收信端的 MTA 在收到信件時，以 DNS 查詢的方式取得發送端的 public key，並進行還原處理，處理後與發送端的簽章進行比對是否一致。以此方式來更準確的判斷該信件是否由他人所偽造寄送。




DomainKey 機制運作流程示意圖

寄信伺服器部份

（步驟 1）**設定鑰匙：**網域在寄信時產生兩組「Key」，公開鑰匙（Public key）以及非公開鑰匙（Private key）。公開鑰匙（Private key）將在寄信的過程中被存入「網域名稱伺服器（DNS）」中，而非公開鑰匙（Private key）將暫時存在寄信伺服器中。

（步驟 2）**傳送鑰匙：**當網域經過認證後，此時系統會根據非公開鑰匙（Private key）而自動產生一組數位認證簽章，此簽名檔將會依附在寄出信件的標頭中，並且傳送至收件者端。

多功能 UTM 部份

（步驟 3）**蒐集鑰匙：**在 DomainKey 機制運作下，收信伺服器將收到夾帶在寄出信件裡的非公開鑰匙（Private key)以及自動擷取「網域名稱伺服器（DNS）」裡的公開鑰匙（Public key）。

（步驟 4）**比對鑰匙：**系統將開始比對兩組鑰匙，比對信件的寄件者名稱是否符合此網域，一旦發現兩組鑰匙不相符，代表著這封信是偽造他人網域而寄出信件，很有可能就是垃圾信或是詐騙信。

（步驟 5）**確定傳送：**在比對結束後，比對成功的信件將被順利地 Pass，而比對失敗的信件將會被系統阻擋、或是被系統隔離。

文 陳殿鴻 kim@nusoft.com.tw

## 市場行銷報導 - 新軟多功能 UTM 替企業有效「管制 IM 通訊軟體、防範電腦病毒散播」

自從 www（全球資訊網）在 1995 年如雨後春筍般的漫延擴散到世界各個角落開始，就註定網路將徹底改變全世界人類之生活型態；及至現今，人類許多行為、習慣也隨之 e 化，就連最單純「人與人」之間的溝通也產生 e 化方式，例如：現在最為當紅的社交工具 MSN、即時通、Skype…等等，最為清楚明顯。而在一般公司企業商業往來時，也會使用此類 IM 通訊軟體作為彼此之間的溝通社交工具；久而久之，IM 即時通訊軟體逐漸成為企業營運不可缺少的重要工具之一。

「有正就有負、有黑就有白」，這些 e 化之社交工具所帶來方便好用之餘，背後所挾帶而來的就是令人厭惡的惡意攻擊及網路釣魚。不久之前，網路上傳出經常橫行於各大網站上之電腦病毒「KOOBFACE」遭有心人士使用於 IM 即時通訊軟體上，藉竊取帳號後再利用帳號間彼此信任的關係傳送惡意檔案，讓不知情之被害者點選下載開啟，於此被害者即在不自覺中感染 KOOBFACE 變種病毒；使得有心人士便可以透過病毒下載木馬程式，進而竊取被害者 IM 帳號所屬的用戶登入資料、通訊錄、聯絡人電話號碼、所在地與其他相關資訊。除此之外，KOOBFACE 變種病毒還會透過 IM 即時通訊軟體自動散發惡意檔案給所有通訊錄裡成員點選下載，藉此一傳十、十傳百、百傳千…，構成所謂的「殭屍網路（Botnet）」，造成不可預期之電腦災情。

現代有些公司為了提高公司生產效率和保護公司商業財產安全的情形下，會進而限制公司員工不能使用 IM 通訊軟體，然而為了維持公司營運順暢又不得不使用 IM 即時通訊軟體和客戶溝通進行商業往來；在這相互矛盾的情況底下，究竟企業本身該如何拿捏分寸呢？

新軟系統多功能 UTM 之產品定義之一便是「捍衛企業資訊安全」，因此諸如此類之資安問題新軟多功能 UTM 都能替企業把關，於此以新軟多功能 UTM 內建之功能提出三項安全防護方案：

**※禁止使用 IM**

假如公司營運政策為保護企業資訊安全而**禁止所有員工或禁止特定部門**（如：開發部、會計部…等等）使用 IM 即時通訊軟體的話，新軟多功能 UTM 即有提供完整的 IM 即時通訊軟體管制機制（如：MSN、Yahoo 即時通、Skype…等等），讓管理人員能夠輕鬆管制公司員工使用 IM 通訊軟體。

**※允許使用 IM（Anti-Virus 防護）**

倘若公司營運政策**開放特定部門**（如：業務部、客服部…等等）使用 IM 通訊軟體進行商業行為，且又有與客戶端互相傳送檔案之必要性存在的話，可以搭配使用多功能 UTM 內建的 Anti-Virus 掃描過濾機制；只要經由 IM 通訊軟體傳送之任何檔案都必須受到多功能 UTM 所內建的掃毒引擎徹底過濾，藉此達到妥善安全的防護。

※允許使用 IM ( 無法傳送檔案 )

假使企業營運政策為開放員工使用 IM 通訊軟體進行商業交流，但是又怕遭受令人討厭的惡意攻擊及網路釣魚攻擊，而禁止員工使用 IM 通訊軟體傳送檔案的話，也可以使用另一項開放性管制機制（**開放登入，但是禁止傳送檔案**），讓員工能夠正常使用 IM 即時通訊，但是卻無法使用任何傳檔功能。藉此就能夠在安全無虞的情況下妥善滿足企業營運的需求。

| 服務機制 | 管制對象 |
| --- | --- |
| 禁止使用 IM | MSN、YahooMessage、Skype、QQ、Google Talk、ICQ/AIM、Gadu-Gadu、Rediff、AliSoft、Fetion、WebIM |
| 允許使用 IM ( Anti-Virus 防護 ) | MSN、YahooMessage、Skype、QQ、Google Talk、ICQ/AIM、Gadu-Gadu、Rediff、AliSoft、Fetion、WebIM |
| 允許使用 IM ( 無法傳送檔案 ) | MSN、YahooMessage、QQ、Google Talk、ICQ/AIM、Gadu-Gadu |

新軟多功能 UTM 提供彈性且有效之管制機制，藉以維護企業資訊安全

文 黃政銘 ming@nusoft.com.tw