新軟週報
http://www.nusoft.com.tw
Internet Security Fighter
2008/4/14-2008/4/27 第65期

多功能 UTM / MS 系列報導

技術淺談與應用 - SPF 機制簡述

SPF（Sender Policy Framework）是用來防止郵件偽造發信地址的一項驗證機制，以判斷發信者所寄出的郵件之網域名稱是否屬實，來過濾煩人的垃圾郵件郵件。

SPF 機制的運作

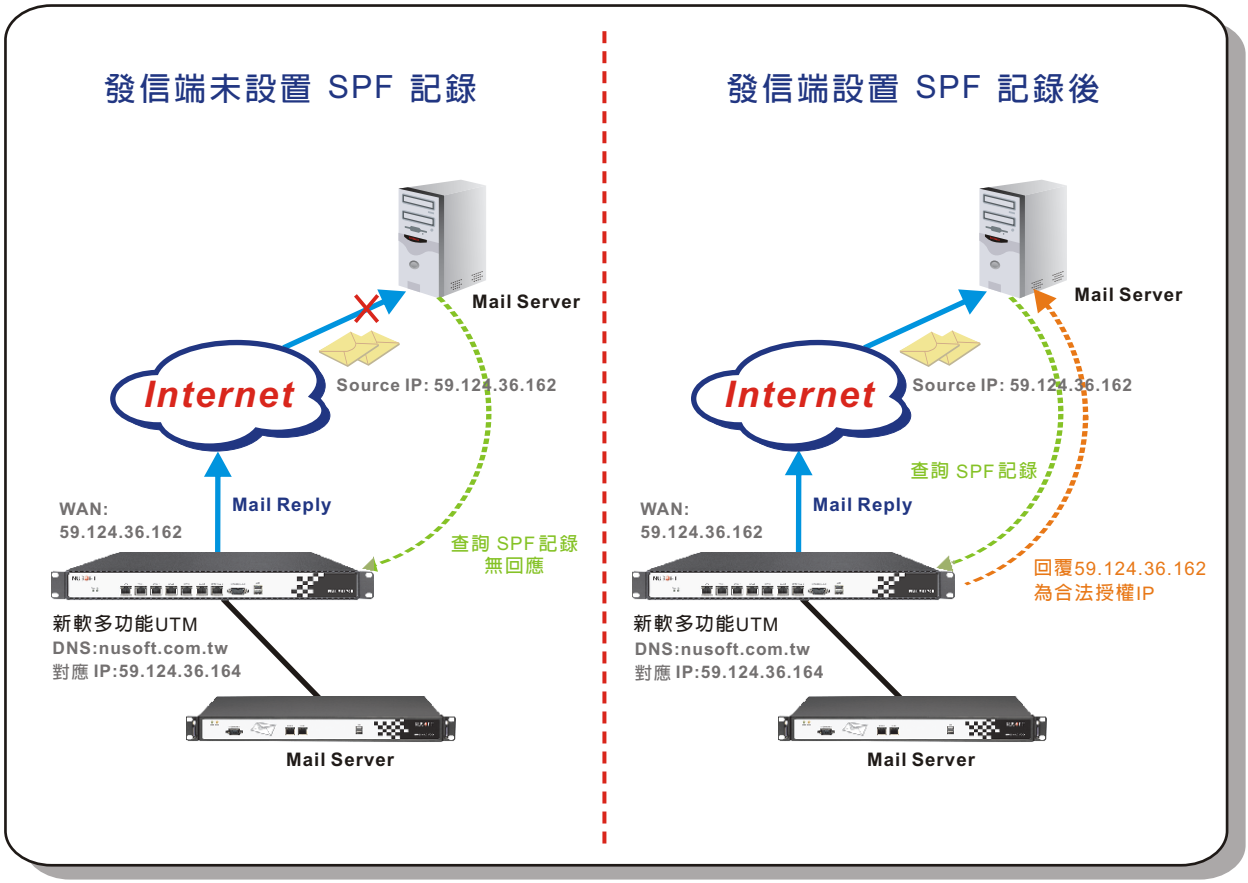
若想要實現 SPF 驗證機制，必須先做好兩項重要的配置在收發電子郵件的兩端，首先發信方必須在 DNS 伺服器裡添加一條 SPF 紀錄，而收信方的郵件伺服器必須開啟 SPF 驗證功能，才能達到郵件防偽的目的。

舉例來說，假設有一垃圾郵件發送者偽造來自 Nusoft 的郵件試著對你寄送垃圾郵件，當郵件到達配置有 SPF 驗證機制的收信端閘道，收信端便會依郵件的 Mail From 欄位中的郵件地址，向 Nusoft 詢問 SPF 記錄，確認寄送這封信的 IP 是否來自他們的網路，若 Nusoft 有提供 SPF 記錄反查，而這 SPF 記錄將可告訴收信端發送此信的 IP 是否有經授權以 Nusoft 的郵件地址寄信，如果 Nusoft 告訴收信端這 IP 經過 SPF 記錄反查得到，信件便能通過收信端的 SPF 驗證而傳送給收件者，換而言之，若信件無法通過 SPF 驗證則視為垃圾郵件，也就是說，就算信件真由 Nusoft 網路送出，但是在 Nusoft 沒有提供 SPF 記錄反查的情況下，無法通過收信端的 SPF 驗證還是會被視為垃圾郵件。

SPF 機制的缺點

由於 SPF 的驗證機制需要寄信端設置 SPF 記錄提供反查，才能正常往來信件，也就是說這個驗證機制若越多人使用越是能表現其功用，而目前有設置 SPF 記錄可提供反查的企業並不多，在不普及的情況收信端設置 SPF 機制過濾垃圾郵件反而使得寄信端非常困擾。

為了解決少數機率可能發生被收信端的 SPF 機制誤擋的情形，新軟在多功能 UTM 及負載平衡器（MS1500、MS2800、MS3700 及 MH1500、MH2400G）增加了提供 SPF 記錄反查的功能，讓使用者輕鬆設置 SPF 記錄，不論信件是經由平衡負載或是信件代轉所寄出而改變了原本郵件地址所對應的 IP，也能通過收信端的 SPF 驗證機制，將信件順利送達。



文 黃智傑 alex@nusoft.com.tw

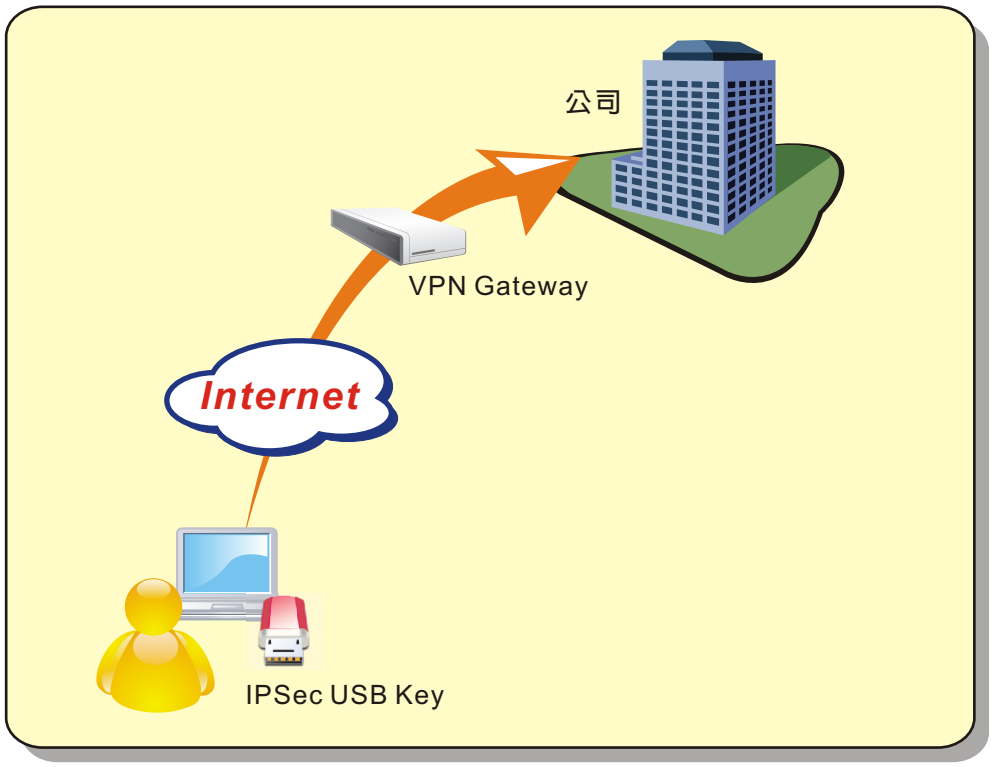
市場行銷報導 - SSL VPN硬體認證vs. IPSec USB Key

隨著無線網路與筆記型電腦發展迅速，越來越多的員工得以透過網際網路進行遠端辦公，無論出差或加班，隨時隨地都能進入企業內部網路存取資料，真正實現不在辦公室，也能辦公事，而這一切均必須建立於安全的連線上，絕大多數的企業乃採用VPN技術作為解決安全連線的需求。

目前VPN技術以SSL VPN與IPSec VPN為主流，不過SSL VPN建置容易，透過Web即可建立與IPsec VPN幾乎一樣強大的安全連線，深受遠端辦公一族的喜愛，而IPSec VPN仍然多被應用在辦公室與辦公室等固定網路間的安全連線。

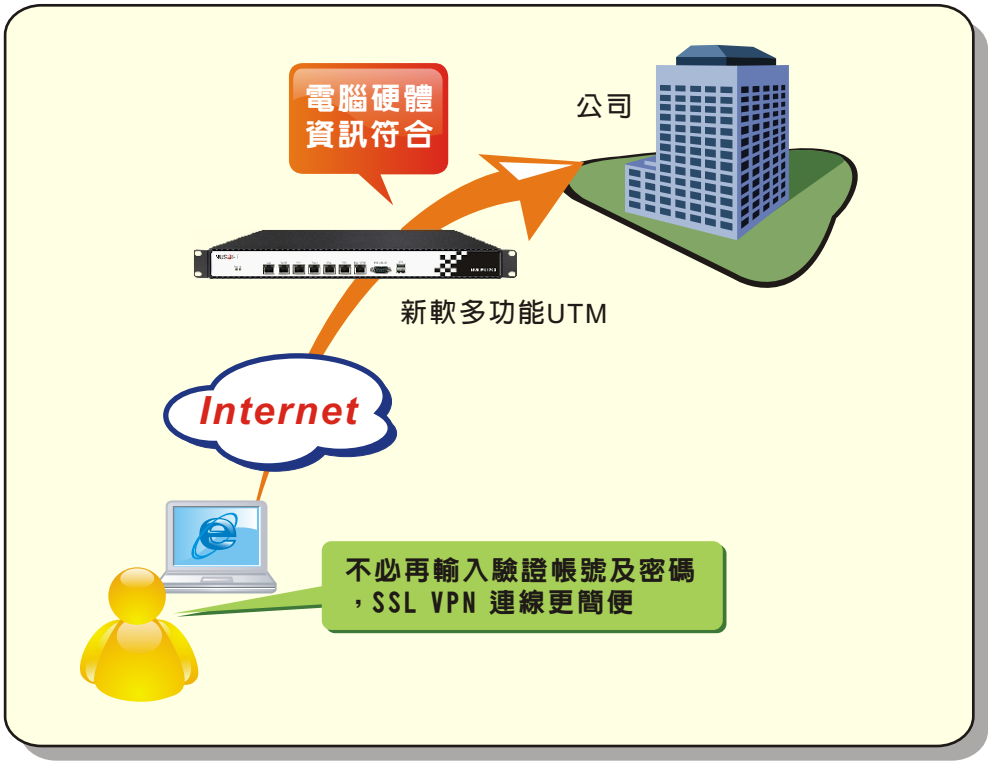
IPSec USB Key

為了使得IPSec VPN Client用戶設定方便，市面上某些資安設備廠商則搭配產品推出IPSec USB Key，將建立VPN所需要的設定參數全部存放在USB Key裡，使用者只需將USB Key插在電腦的USB Port，不需輸入任何密碼或設定參數便可與遠端建立起VPN，以此方式簡化IPSec VPN Client端的設定，並利用USB隨插即用的特性，試著得到更多外勤工作人員及遠端辦公人員的青睞。不過就安全性而論，由於任何人只要插上USB Key便可透過VPN存取企業內部資源，萬一USB Key遺失被有心人士拾得，那將造成企業莫大的危害，於是乎USB Key進而結合密碼以防止盜用，使用者必須先得輸入密碼後才可使用USB Key建立VPN連線，雖然防盜的設計使得資訊安全多了一道防線，不過也因此失去了USB Key隨插即用不必輸入驗證密碼的優點。



SSL VPN 硬體認證

近來新軟系統即將在多功能 UTM 及多功能負載平衡器的 SSL VPN 功能中，增加硬體認證機制。由於外勤工作人員大多利用個人的筆記型電腦與公司建立 VPN，而時常透過 VPN 進行遠端辦公的人員也大都使用特定的電腦，為了讓這些使用者在建立 SSL VPN 時的程序更為簡便，新軟設計將通過硬體認證的電腦，不必再輸入任何驗證帳號及密碼，便可直接進行 SSL VPN 的連線，對於經常使用同一部電腦建立 SSL VPN 的用戶來說十分方便。一般來說使用者只需透過 Web 輸入驗證的帳號密碼便可建立 SSL VPN 連線，已經十分方便，而硬體認證機制更是簡略了輸入驗證帳號及密碼的步驟，使用者只需在第一次連線時利用驗證帳號及密碼建立連線，系統管理員再將其硬體認證設為通過，往後使用者利用這台電腦使用 SSL VPN 便不必再輸入帳號密碼。就安全性來說，透過 SSL VPN 傳輸資料的安全性是無庸置疑的，而硬體認證機制是以電腦各種裝置（CPU、硬碟、光碟機…等）的資訊作為判別，有心人士必須得將整台電腦偷走才可能盜用 SSL VPN 偷取企業資料，況且大多數的使用者會在電腦設置系統登入密碼，相對於較易遺失的 USB Key 來說，安全性更勝一籌。



	SSL VPN 硬體認證	IPSec USB Key
功能	只需系統管理員將使用者的電腦硬體資訊設為通過，之後以此電腦連接 SSL VPN 便可不必再輸入驗證帳號及密碼。	只需插上 USB Key，不必做任何設定便能建立 IPSec VPN。
供給使用數量	使用者只需透過網頁瀏覽器即可進行連線，建置容易且硬體認證可供上百台電腦同時使用。	USB Key 裝置的成本較高，數量有限無法同時提供多人同時使用。
盜連風險	風險較低	遭盜用風險較高

文 黃智傑 alex@nusoft.com.tw