新软周报
http://www.nusoft.com.tw
Internet Security Fighter
2008/4/14-2008/4/27 第65期

多功能UTM / MS系列报导

技术浅谈与应用 - SPF机制简述

SPF（Sender Policy Framework）是用来防止邮件伪造发信地址的一项验证机制，以判断发信者所寄出的邮件之网域名称是否属实，来过滤烦人的垃圾邮件邮件。

SPF机制的运作

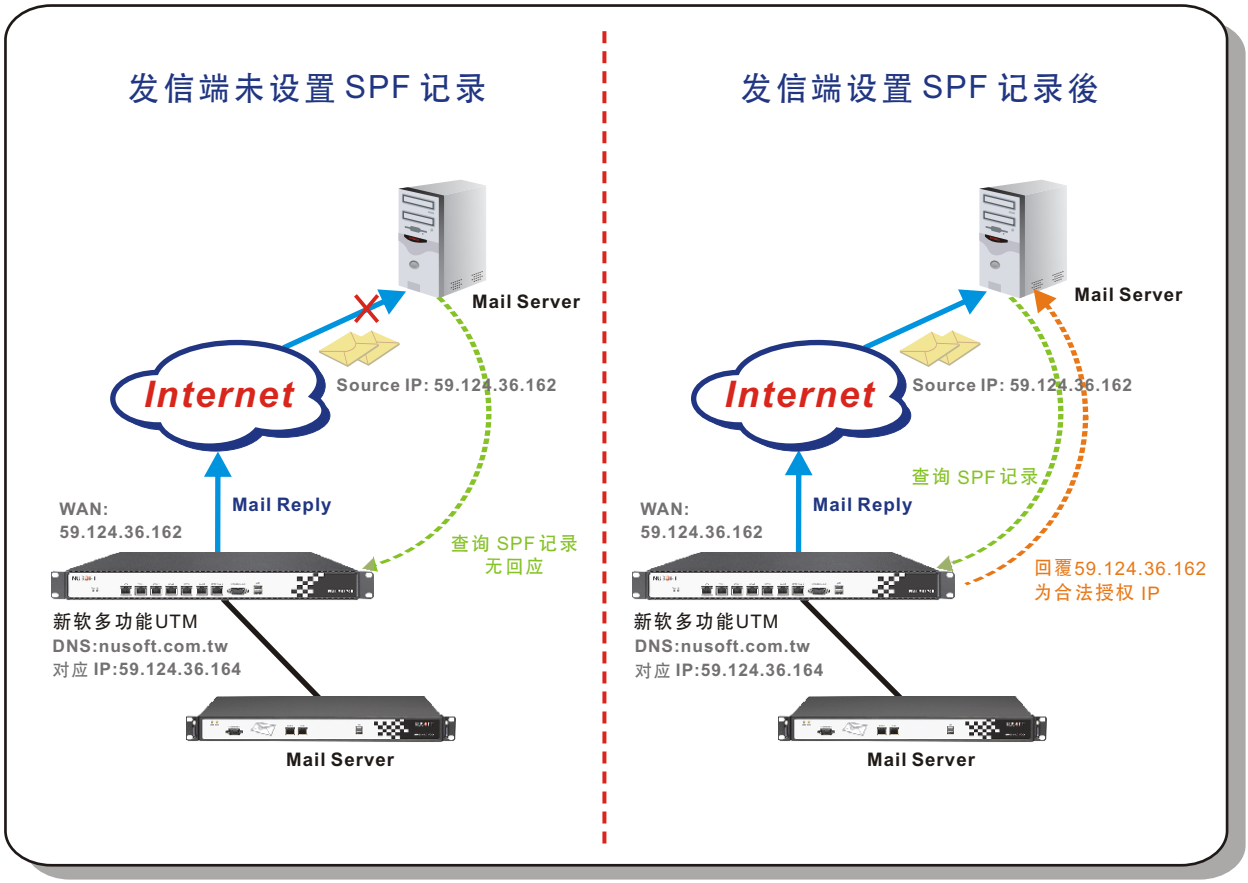
若想要实现SPF验证机制，必须先做好两项重要的配置在收发电子邮件的两端，首先发信方必须在DNS服务器里添加一条SPF纪录，而收信方的邮件服务器必须开启SPF验证功能，才能达到邮件防伪的目的。

举例来说，设有一垃圾邮件发送者伪造来自Nusoft的邮件试着对你寄送垃圾邮件，当邮件到达配置有SPF验证机制的收信端网关，收信端便会依邮件的Mail From字段中的邮件地址，向Nusoft询问SPF记录，确认寄送这封信的IP是否来自他们的网络，若Nusoft有提供SPF记录反查，而这SPF记录将可告诉收信端发送此信的IP是否有经授权以Nusoft的邮件地址寄信，如果Nusoft告诉收信端这IP经过SPF记录反查得到，信件便能通过收信端的SPF验证而传送给收件者，换而言之，若信件无法通过SPF验证则视为垃圾邮件，也就是说，就算信件真由Nusoft网络送出，但是在Nusoft没有提供SPF记录反查的情况下，无法通过收信端的SPF验证还是会被视为垃圾邮件。

SPF机制的缺点

由于SPF的验证机制需要寄信端设置SPF记录提供反查，才能正常往来信件，也就是说这个验证机制若越多人使用越是能表现其功用，而目前有设置SPF记录可提供反查的企业并不多，在不普及的情况收信端设置SPF机制过滤垃圾邮件反而使得寄信端非常困扰。

为了解决少数机率可能发生被收信端的SPF机制误挡的情形，新软在多功能UTM及负载平衡器（MS1500、MS2800、MS3700及MH1500、MH2400G）增加了提供SPF记录反查的功能，让使用者轻松设置SPF记录，不论信件是经由平衡负载或是信件代转所寄出而改变了原本邮件地址所对应的IP，也能通过收信端的SPF验证机制，将信件顺利送达。



文 黄智杰 alex@nusoft.com.tw

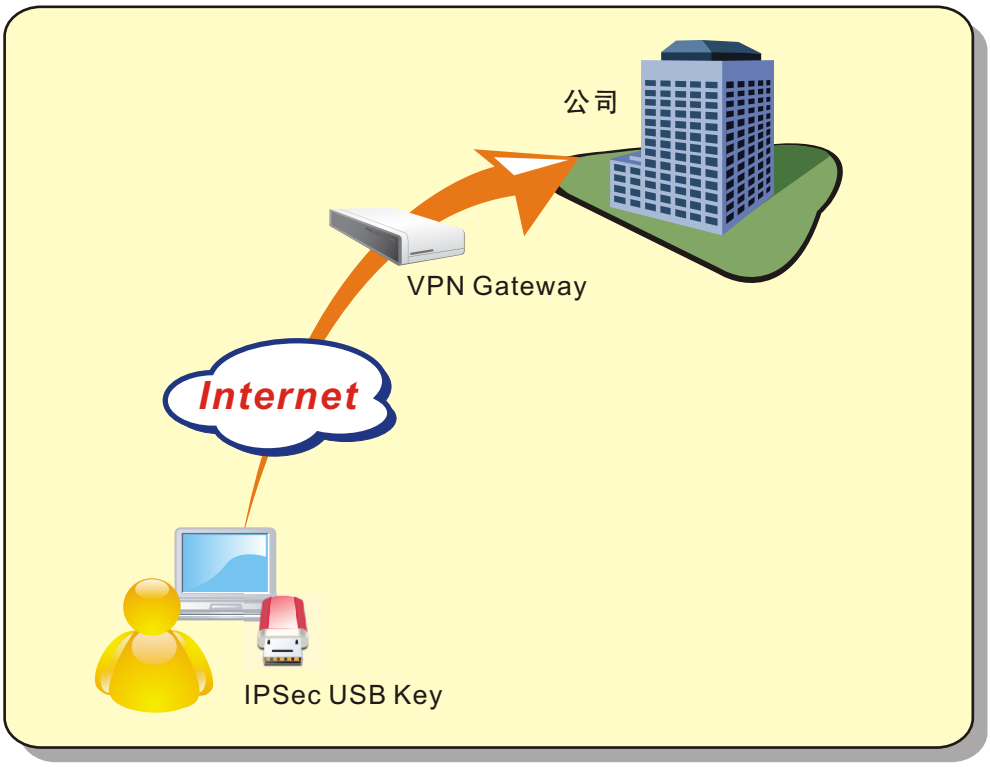
市场营销报导 - SSL VPN 硬件认证 vs. IPSec USB Key

随着无线网络与笔记本电脑发展迅速，越来越多的员工得以透过因特网进行远程办公，无论出差或加班，随时随地都能进入企业内部网络存取数据，真正实现不在办公室，也能办公事，而这一切均必须建立于安全的联机上，绝大多数的企业乃采用 VPN 技术作为解决安全联机的需求。

目前 VPN 技术以 SSL VPN 与 IPSec VPN 为主流，不过 SSL VPN 建置容易，透过 Web 即可建立与 IPsec VPN 几乎一样强大的安全联机，深受远程办公一族的喜爱，而 IPSec VPN 仍然多被应用在办公室与办公室等固定网络间的安全联机。

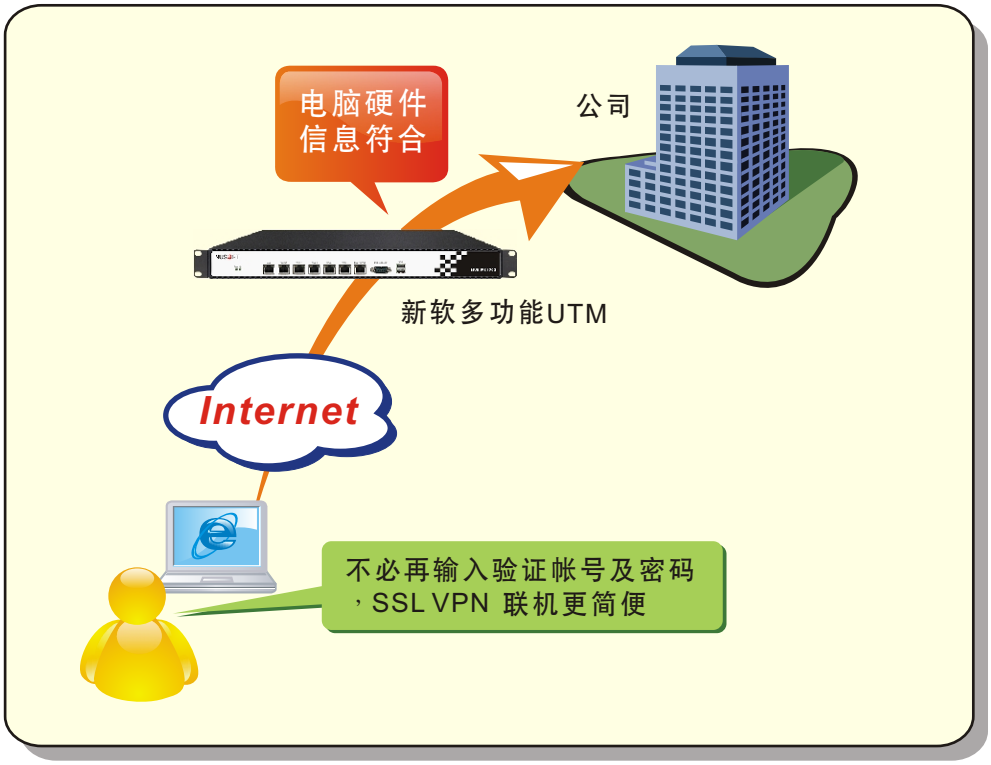
IPSec USB Key

为了使得 IPSec VPN Client 用户设定方便，市面上某些资安设备厂商则搭配产品推出 IPSec USB Key，将建立 VPN 所需要的设定参数全部存放在 USB Key 里，使用者只需将 USB Key 插在电脑的 USB Port，不需输入任何密码或设定参数便可与远程建立起 VPN，以此方式简化 IPSec VPN Client 端的设定，并利用 USB 随插即用的特性，试着得到更多外勤工作人员及远程办公人员的青睐。不过就安全性而论，由于任何人只要插上 USB Key 便可透过 VPN 存取企业内部资源，万一 USB Key 遗失被有心人士拾得，那将造成企业莫大的危害，于是乎 USB Key 进而结合密码以防止盗用，使用者必须先得输入密码后才可使用 USB Key 建立 VPN 联机，虽然防盗的设计使得信息安全多了一道防线，不过也因此失去了 USB Key 随插即用不必输入验证密码的优点。



SSL VPN 硬件认证

近来新软系统即将在多功能 UTM 及多功能负载平衡器的 SSL VPN 功能中，增加硬件认证机制。由于外勤工作人员大多利用个人的笔记本电脑与公司建立 VPN，而时常透过 VPN 进行远程办公的人员也大都使用特定的电脑，为了让这些使用者在建立 SSL VPN 时的程序更为简便，新软设计将通过硬件认证的电脑，不必再输入任何验证账号及密码，便可直接进行 SSL VPN 的联机，对于经常使用同一部电脑建立 SSL VPN 的用户来说十分方便。一般来说使用者只需透过 Web 输入验证的账号密码便可建立 SSL VPN 联机，已经十分方便，而硬件认证机制更是简略了输入验证账号及密码的步骤，使用者只需在第一次联机时利用验证账号及密码建立联机，系统管理员再将其硬件认证设为通过，往后使用者利用这台电脑使用 SSL VPN 便不必再输入账号密码。就安全性来说，透过 SSL VPN 传输数据的安全性是无庸置疑的，而硬件认证机制是以电脑各种装置（CPU、硬盘、光驱…等）的信息作为判别，有心人士必须得将整台电脑偷走才可能盗用 SSL VPN 偷取企业数据，况且大多数的使用者会在电脑设置系统登入密码，相对于较易遗失的 USB Key 来说，安全性更胜一筹。



	SSL VPN 硬件认证	IPSec USB Key
功能	只需系统管理员将使用者的电脑硬件信息设为通过，之後以此电脑连接 SSL VPN 便可不必再输入验证帐号及密码。	只需插上 USB Key，不必做任何设定便能建立 IPSec VPN。
供给使用数量	使用者只需透过网页浏览器即可进行联机，建置容易且硬件认证可供上百台电脑同时使用。	USB Key 装置的成本较高，数量有限无法同时提供多人同时使用。
盗连风险	风险较低	遭盗用风险较高

文 黄智杰 alex@nusoft.com.tw