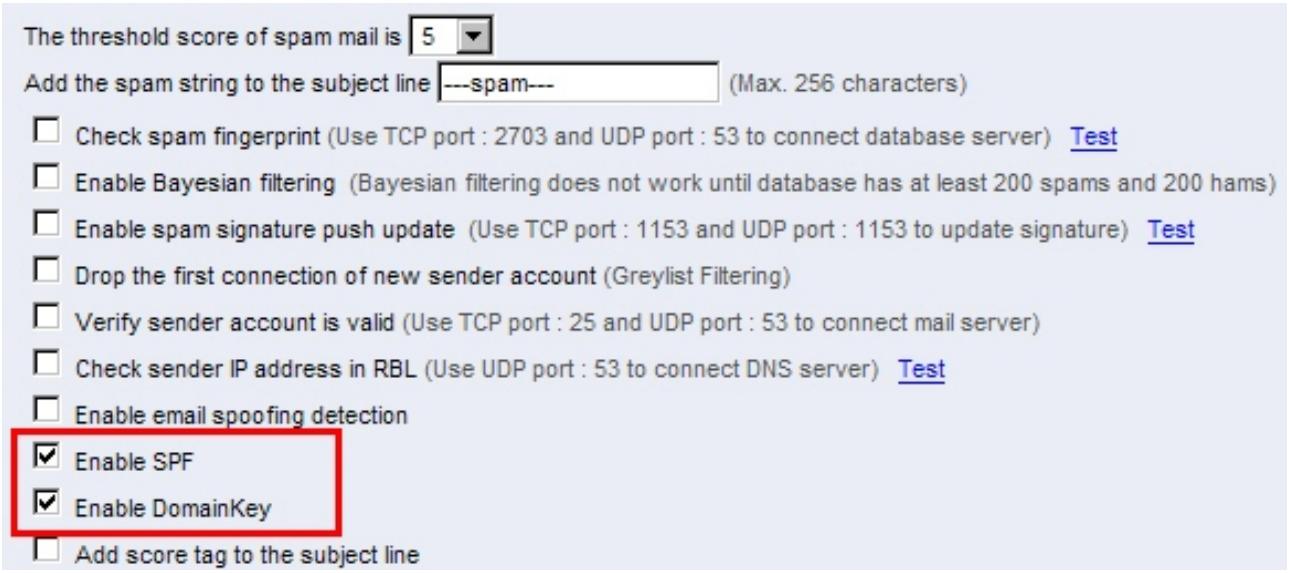
新软周报
http://www.nusoft.com.tw
Internet Security Fighter
2009/12/14- 2009/12/27 第107期

多功能 UTM / MS 系列报导

技术浅谈与应用 - SPF 与 DomainKey 的差异

网络电子邮件让彼此之间的沟通缩短了距离，同样却也因如此的便利性让使用者饱受有心人事的骚扰；垃圾邮件的影响，至今依然只能够仰赖防护机制来降低影响程度，随着垃圾邮件不断的创新入侵方式，防护机制也因此不断的在更新阻挡机制。

随着不断推出之新垃圾邮件防护机制，身为公司内部网络管理人员同样也必须先去了解，而后再加强公司内的防护系统，但在众多的防护机制下要一项一项熟悉也非一时三刻可做到的事情，甚至有让人搞混的情况发生。新软系统于多功能 UTM - MS 中 V5. 08 版新增了几项垃圾邮件过滤功能，其中有些许相似之处的为『SPF』、『DomainKey』两项过滤功能，此两项功能虽同为针对『伪造 Domain』这方向来做防护，但其运作原理实为不同，为了能让管理人员能清楚厘清两项功能，以下将分别一一做说明。

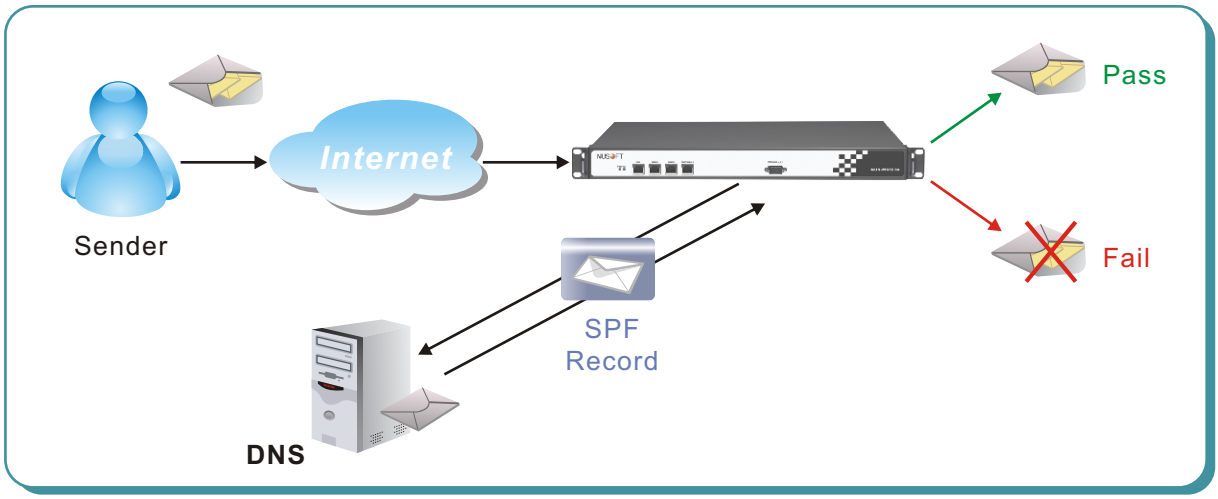


可于 Mail Security > Anti-Spam > Setting 下启动『SPF』、『DomainKey』两项过滤功能

SPF

由于同一个网域名称可能透过多台的 mail server 或是 ISP 寄信，所以只单靠反解的方式来做侦测，已不敷现在需求，因此有效的网域验证是目前防护机制中不可或缺之功能。

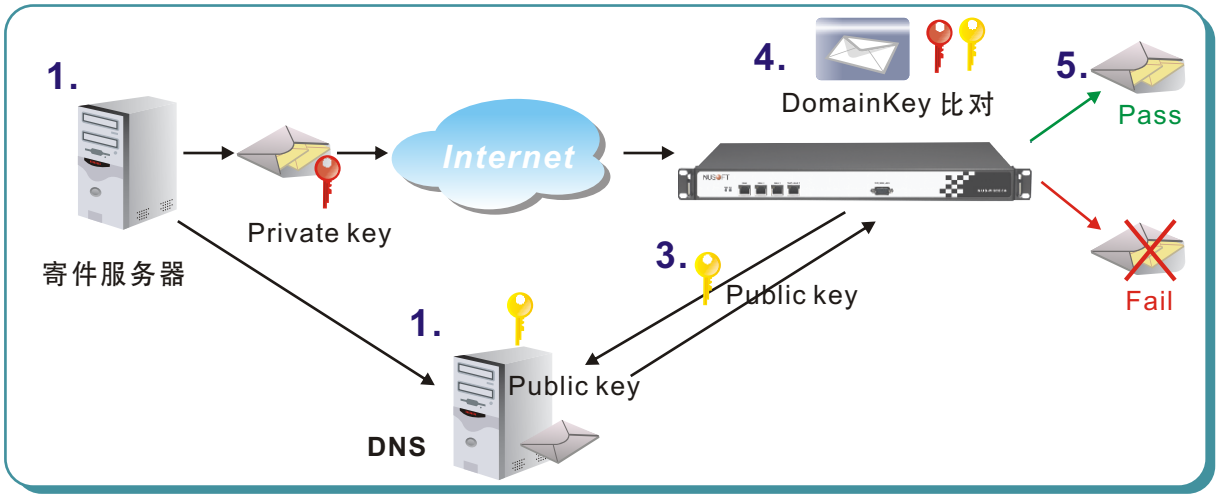
Sender Policy Framework 简称为 SPF，SPF 主要作为反伪造邮件的解决方案，SPF 过滤机制最主要是用来检查 SMTP Server 是否有伪造其它人的 Domain 或是虚设 Domain 之情况发生，SPF 会根据 Domain Name 的 SPF 记录确认连结的 IP 是否内含 SPF 记录，透过此方式来宣告这个网域名称的信件可能透过哪几个 IP 或网址寄出，其它的就是非法的，若该封信件是由正式 DNS 内的邮件服务器发出，那么即可避免有心人事利用假冒网域之方式来发送信件。



SPF 机制运作流程示意图

DomainKey

主要是在设计一套 Email 的认证方式，以增加在垃圾邮件的判读能更准确，虽然此机制与 SPF 机制一样都是针对网域来做验证，但 DomainKey 却比较仅慎且复杂些。该机制做法主要于 MTA 发送信件时同时产生『公开钥匙 (Public key)』、『非公开钥匙 (Private key)』两组 Key，并以自己的 Private key 对表头 (Mail Header) 加密计算，产生一组签章，而另一组 Public key 则在寄信的过程中存入『网域名称服务 (DNS)』中，当收信端的 MTA 在收到信件时，以 DNS 查询的方式取得发送端的 public key，并进行还原处理，处理后与发送端的签章进行比对是否一致。以此方式来更准确的判断该信件是否由他人所伪造寄送。



DomainKey 机制运作流程示意图

寄信服务器部份

(步骤 1)**设定钥匙**：网域在寄信时产生两组『Key』，公开钥匙 (Public key) 以及非公开钥匙 (Private key)。公开钥匙 (Private key) 将在寄信的过程中被存入『网域名称服务器 (DNS)』中，而非公开钥匙 (Private key) 将暂时存在寄信服务器中。

(步骤 2)**传送钥匙**：当网域经过认证后，此时系统会根据非公开钥匙 (Private key) 而自动产生一组数字认证签章，此签名档将会依附在寄出信件的标头中，并且传送至收件者端。

多功能 UTM 部份

(步骤 3)**搜集钥匙**：在 DomainKey 机制运作下，收信服务器将收到夹带在寄出信件里的非公开钥匙 (Private key) 以及自动剪辑『网域名称服务器 (DNS)』里的公开钥匙 (Public key)。

(步骤 4)**比对钥匙**：系统将开始比对两组钥匙，比对信件的寄件者名称是否符合此网域，一旦发现两组钥匙不相符，代表着这封信是伪造他人网域而寄出信件，很有可能就是垃圾信或是诈骗信。

(步骤 5)**确定传送**：在比对结束后，比对成功的信件将被顺利地 Pass，而比对失败的信件将会被系统阻挡、或是被系统隔离。

文 陈殿鸿 kim@nusoft.com.tw

市场营销报导 - 新软多功能 UTM 替企业有效「管制 IM 通讯软件、防范计算机病毒散播」

自从 www（全球信息网）在 1995 年如雨后春笋般的漫延扩散到世界各个角落开始，就注定网络将彻底改变全世界人类之生活型态；及至现今，人类许多行为、习惯也随之 e 化，就连最单纯『人与人』之间的沟通也产生 e 化方式，例如：现在最为当红的社交工具 MSN、实时通、Skype…等等，最为清楚明显。而在一般公司企业商业往来时，也会使用此类 IM 通讯软件作为彼此之间的沟通社交工具；久而久之，IM 实时通讯软件逐渐成为企业营运不可缺少的重要工具之一。

『有正就有负、有黑就有白』，这些 e 化之社交工具所带来方便好用之余，背后所挟带而来的就是令人厌恶的恶意攻击及网络钓鱼。不久之前，网络上传出经常横行于各大网站上之计算机病毒『KOOBFACE』遭有心人士使用于 IM 实时通讯软件上，藉窃取账号后再利用账号间彼此信任的关系传送恶意文件，让不知情之被害者点选下载开启，于此被害者即在不自觉中感染 KOOBFACE 变种病毒；使得有心人士便可以透过病毒下载木马程序，进而窃取被害者 IM 账号所属的用户登入数据、通讯簿、联络人电话号码、所在地与其它相关信息。除此之外，KOOBFACE 变种病毒还会透过 IM 实时通讯软件自动散发恶意文件给所有通讯簿里成员点选下载，藉此一传十、十传百、百传千…，构成所谓的『殭尸网络(Botnet)』，造成不可预期之计算机灾情。

现代有些公司为了提高公司生产效率和保护公司商业财产安全的情形下，会进而限制公司员工不能使用 IM 通讯软件，然而为了维持公司营运顺畅又不得不使用 IM 实时通讯软件和客户沟通进行商业往来；在这相互矛盾的情况底下，究竟企业本身该如何拿捏分寸呢？

新软系统多功能 UTM 之产品定义之一便是『捍卫企业信息安全』，因此诸如此类之资安问题新软多功能 UTM 都能替企业把关，于此以新软多功能 UTM 内建之功能提出三项安全防护方案：

※禁止使用 IM

假如公司营运政策为保护企业信息安全而**禁止所有员工或禁止特定部门**（如：开发部、会计部...等等）使用 IM 实时通讯软件的话，新软多功能 UTM 即有提供完整的 IM 实时通讯软件管制机制（如：MSN、Yahoo 实时通、Skype...等等），让管理人员能够轻松管制公司员工使用 IM 通讯软件。

※允许使用 IM（Anti-Virus 防护）

倘若公司营运政策**开放特定部门**（如：业务部、客服部...等等）使用 IM 通讯软件进行商业行为，且又有与客户端互相传送文件之必要性存在的话，可以搭配使用多功能

UTM 内建的 Anti-Virus 扫描过滤机制；只要经由 IM 通讯软件传送之任何文件都必须受到多功能 UTM 所内建的扫毒引擎彻底过滤，藉此达到妥善安全的防护。

※允许使用 IM（ 无法传送文件 ）

假使企业营运政策为开放员工使用 IM 通讯软件进行商业交流，但是又怕遭受令人讨厌的恶意攻击及网络钓鱼攻击，而禁止员工使用 IM 通讯软件传送文件的话，也可以使用另一项开放性管制机制（**开放登入，但是禁止传送文件**），让员工能够正常使用 IM 实时通讯，但是却无法使用任何传文件功能。藉此就能够在安全无虞的情况下妥善满足企业营运的需求。

服务机制	管制对象
禁止使用 IM	MSN、YahooMessage、Skype、QQ、Google Talk、ICQ/AIM、Gadu-Gadu、Rediff、AliSoft、Fetion、WebIM
允许使用 IM（Anti-Virus 防护）	MSN、YahooMessage、Skype、QQ、Google Talk、ICQ/AIM、Gadu-Gadu、Rediff、AliSoft、Fetion、WebIM
允许使用 IM（无法传送文件）	MSN、YahooMessage、QQ、Google Talk、ICQ/AIM、Gadu-Gadu

新软多功能 UTM 提供弹性且有效之管制机制，藉以维护企业信息安全

文 黄政铭 ming@nusoft.com.tw