新软周报
http://www.nusoft.com.tw
Internet Security Fighter
2007/10/15- 2007/10/21 第46期

## 多功能 UTM / MS 系列报导

### 技术浅谈与应用 - 浅谈 IDP 入侵侦测防御系统

随着因特网日益发达，绝大多数的企业也将其版图扩张到这个领域，透过因特网提升企业竞争力。也因为企业网络对于企业来说重要度已经不可小觑，所以企业都会添购相关网络安全设备以确保企业网络安全无虞。

目前一般企业为保护其网络系统，采用防火墙作为企业网络进出的门户，以确保企业网络之安全。防火墙虽可防止来自于因特网之不明或恶意存取、攻击行为，但也只能针对 OSI 模型 2~4 层的封包进行检测来源、目的地、连接埠等字段来对某个服务存取进行限制，并不能检视所通过的封包是否有异常。因此对于企业网络来说，防火墙的保护已经日渐不敷使用。

为此，网络安全相关业者推出 IDS（Intrusion Detection System）入侵侦测系统以协助保护企业网络安全。IDS 的功能是针对 OSI 模型 5~7 层的封包进行检测，可在侦测到问题时做相关记录并及时发出警讯通报管理人员处理。“IDS 可实时反应企业网络问题”听起来可以协助企业解决防火墙保护之不足，但实际上其仅能告知管理人员而无法自行阻挡，且常发生误判的情况。在天天「狼来了！！」误判警告下，网管人员只能疲于奔命的反复查核该警告是否正确，而真正问题发生时，整个企业网络已经回天乏术。

IPS（Intrusion Prevention System）入侵防御系统就是针对 IDS 仅能发现问题而无法解决问题之缺陷而发展出的新产品。IPS 能在侦测到入侵攻击时，可立即阻断该封包通过，以保护企业网络安全。IPS 遇到问题时能实时防御，但如遇到误判之状况时，IPS 的防御机制还是全面阻拦，明显不具弹性。

为了彻底解决企业网络安全问题，新软系统在其推出的新软 UTM（MS 系列产品）中加入了最新一代的企业网络防御利器 IDP（Intrusion Detection and Prevention）入侵侦测防御系统。就如字面上的意思，IDP 结合了IDS 的入侵侦测与 IPS 之入侵防御功能，可以检测出包藏在应用层里的恶意攻击码（譬如：蠕虫攻击、缓冲溢位攻击）并加以阻拦、警告。

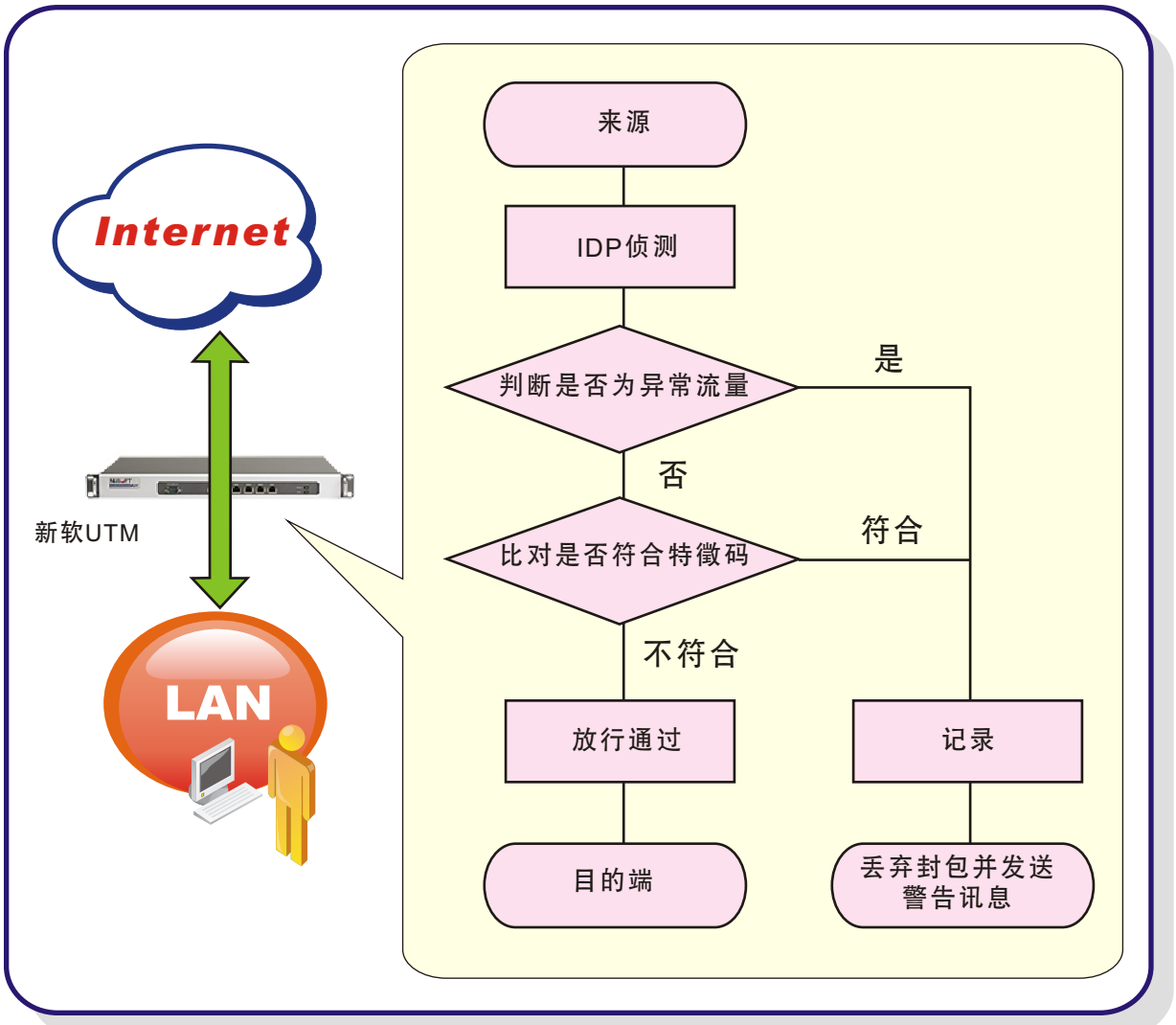
新软 UTM 的 IDP 机制拥有两种侦测功能－特征比对侦测 与 异常侦测，来保护企业免于各种入侵或攻击的危害：

特征比对侦测机制－拥有一庞大的「IDP 特征数据库」，所有经过 IPD 扫描之封包只要与数据库的特征相符时，新软 UTM 就会依照先前管理人员所订定的处置方式处理该封包。

异常侦测机制－可针对各种网络攻击模式防御；当网络联机符合攻击模式时，新软 UTM 会将它视为网络攻击，并依管理人员所订定的处理方式处理该联机。

网络科技日新月异，当然各种入侵、攻击手段也在进步。新软 UTM 的 IDP 功能当然也要随时更新，以迎接各项更加严峻的挑战。因此，其内建的「IDP 特征数据库」会每两小时自动上线检查是否有新的特征文件可下载，以维持数据库在最新的状态。另外，网管人员亦可以针对企业网络实际需求，自订所要的特征，让新软 UTM 的 IDP 防护更具弹性。

网络的普及带给人们方便却也蕴藏着许多的危机。“如何安全运用网络为企业带来商机”已经成为企业重点工作之一。不安全的网络环境就如同企业根基埋藏着不定时炸弹，一但引爆将严重影响企业之运作。而防火墙对于目前严峻的因特网环境已不堪负荷，拥有 IDP 的新软 UTM 必然是企业最佳之选择。




文 黄智杰 alex@nusoft.com.tw

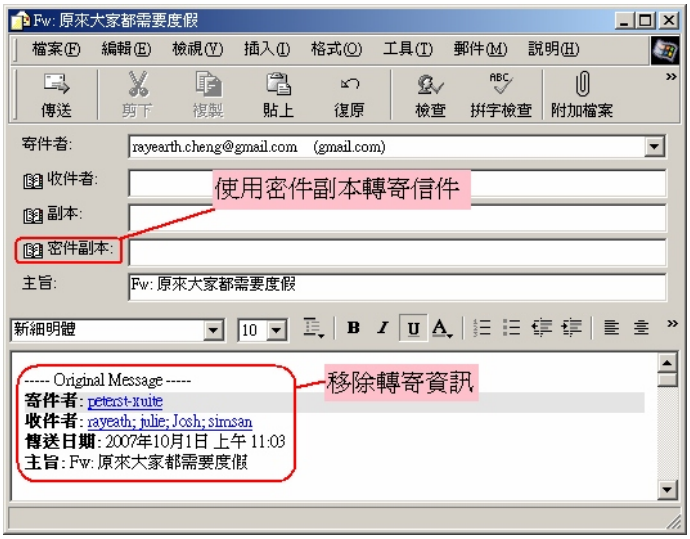
# 市场营销报导 - 要如何减少恼人的垃圾邮件

**垃圾邮件满坑满谷实在讨人厌，要如何减少垃圾邮件呢？**

想要减少垃圾邮件，就必须从垃圾虫（Spammer，指滥发垃圾邮件者）如何收集邮寄名单谈起。一般垃圾虫所用的邮寄名单采取了下列做法收集：

善意的转寄信件－当您收到一封由朋友转寄而来之信件，且觉得其内容真的很不错时，是否会将该信件再转寄给其它亲朋好友，将它分享出去呢？如果您常做上述这个动作可能就要小心了，因为您可能正在“协助”垃圾虫收集名单！！

这些转寄信件中常常富含着众多电子邮件账号（在转寄信息中），因此在转寄信件时没有使用「密件副本」或是将「转寄信息」移除时，很容易让有心人士收集邮件名单。




图一 转寄信件时的必须动作

字典式尝试法－此种方法较常使用于名气大的邮件服务提供商，像是 Hotmail、Yahoo、Hinet、163...。垃圾虫会用「字典」（包含常见的人名、字符串、数字...）来排列组合猜测使用者的邮件账号。因为邮件服务器会将寄给无效邮件账号之信件退回给寄件者，垃圾虫可藉此判断该邮件账号是否有效。

一般会员网站－在注册一些会员制网站时，通常注册数据都会要求使用者提供邮件账号。而这些邮件账号常会因网站为了贪图获利、网站系统被黑客窃取数据...原因，被贩卖给垃圾虫作为垃圾邮件邮寄名单。

讨论区、留言版－垃圾虫常在各大讨论区、留言板、BBS 站...中，利用搜寻程序搜集各篇文章作者所留下的邮件账号。因此，在这些讨论区、留言板中越活跃的作者，越容易收到垃圾邮件。

邮件代转－近期内因中国大陆地区开始运行「网络防火墙长城（GFW）」，使得在中国大陆的使用者利用境外之邮件服务器会发生传输上的问题。因此，使用者开始透过各种方式试图避开此困扰，其中的一种方式就是利用境外没有被封锁的 Mail Relay Server 转信。

使用免费的 Mail Relay Server 转信虽然可以成功将信件寄出，但是有心人士可以从 Mail Relay Server 的记录文件中轻易收集邮件地址。从今以后，不管是收件者还是寄件者将会被大量垃圾邮件侵扰。

网站自行公布－一般企业网站为了服务客户，通常会在网站中公布联络用的邮件账号（通常是业务、服务人员之邮件账号）。也导致这些邮件账号每天都会有收不完的垃圾信件，严重拖慢业务处理速度。

怎么样，了解这些垃圾邮件名单的收集方式之后，是不是发现自己常常犯了这些错误呢？为了避免垃圾邮件的侵扰，有下列几种方式可供参考：

1. 转寄信件时使用「密件副本」并将「转寄信息」移除－
就如先前所提及的，要转寄好文章给亲朋好友时，务必使用「密件副本」并将「转寄信息」移除，也最好在信中提醒收件者采取相同步骤。

2. 不要购买垃圾邮件所广告的商品－
当您采买了利用垃圾邮件广告的商品时，也会向垃圾虫透露了一个重要讯息「这个邮件账号是有效的！！」。往后您将会有收不完的垃圾信件。

3. 使用两个以上的邮件账号－
除了主要的邮件账号外，您可再申请数个邮件账号作为“申请会员”、“在线购物”、“抽奖”...之用。尽量分类电子邮件信箱，不要任意透露主要的邮件账号给不相干的人士，以防邮件账号流入垃圾虫之手中。

4. 封锁电子邮件的图片文件－
目前有许多垃圾邮件是采用图片方式来传递广告讯息。此种方式除了比较容易躲避一般垃圾邮件过滤系统的查缉外，该信件之图片在下载时亦可传递收件者信息给垃圾虫；垃圾虫可藉此了解「该邮件账号尚有人会阅览信件」。因此，最好可禁止收信软件主动下载图片。

这也就是为甚么新软 UTM（MS 系列产品）、邮件服务器（ML 系列产品）、网络记录器（IR 系列产品）在显示其所记录、备份的信件中，不会主动显示图片之原因。

5. 审慎查核网站之同意书
当您在注册网站会员时，千万要细读网站的“会员同意书”－部份网站会询问“是否愿意收到「合作伙伴」的电子邮件”。当您完全没有阅读“会员同意书”一路按下【下一步】时，您已将自己的邮件账号卖给了垃圾虫。

6. 千万不要回复垃圾邮件的「取消订阅」
垃圾邮件的「取消订阅」按钮通常是个幌子，点选后只会告诉垃圾虫「这个邮件账号是有效的！！」，往后您会有更多的垃圾信件。

7. 取个较复杂的“邮件账号”
字典式尝试法的邮件账号收集方式只会用「字典文件」中的字符串去做尝试，如果您的邮件账号超过「字典文件」的范畴，垃圾虫将无法试出您的邮件账号。

8. 透过加密方式联机境外邮件服务器（中国大陆地区）
不要透过 Mail Relay Server 传送信件，新软邮件服器提供了 SMTPS、POP3S 这两种加密服务可供使用者选用，完全可避开 GFW 所造成的无法寄信之问题。

企业可依上述方式教育旗下员工如何使用电子邮件之外，建议企业还是必须建构一垃圾邮件过滤系统，来滤除垃圾邮件。毕竟，企业窗口所使用之电子邮件账号必须公诸于世，当然会详记于垃圾虫的「工商名录」中。

新软系统所推出的多功能 UTM（MS 系列产品）与邮件服务器（ML 系列产品）就含有为企业量身打造的垃圾邮件过滤系统。该系统内建了多层垃圾邮件过滤机制，以层层把关方式将垃圾邮件一一滤出，封锁在其内建的隔离区中，还给企业一个干净的电子邮件环境。因此，企业窗口再也不用担心被垃圾邮件所掩埋，无需费心如何找到那重要的「客户信件」！！

文 程智伟 rayearth@nusoft.com.tw