新软周报
http://www.nusoft.com.tw
Internet Security Fighter
2009/4/6- 2009/4/19 第89期

多功能 UTM / MS 系列报导

技术浅谈与应用 - 贝氏过滤的两种学习方式

虽然对抗垃圾信件的技术不断在更新，但在众多的过滤方式中仍然以“贝氏过滤法（Bayesian Filtering）”最为被广泛所使用。其运作之基础是采用贝氏定理 -『以过往所累积之数据来预测事件发生机率』的方式来判断垃圾邮件。此种方式会将信件切分成多数单词(Token)，并利用算法作统计，进而推算出该封信件为垃圾信的机率，并配合其“贝氏过滤数据库”，及透过不断学习来提升垃圾邮件辨识准确率。

而“贝氏过滤数据库”学习的来源分为『垃圾邮件数据库』与『非垃圾邮件数据库』两种，系统会将数据库中的所有信件内容切成单词，并给予每个单词不同的比率。当下次新信件寄来时，一样会把信件分解成单词，同时比对学习过的「贝氏过滤法数据库」单词，分析过往的经验来评判此封为垃圾信件的机率。因此，要让贝氏过滤能准确运作，垃圾邮件数据库与非垃圾邮件数据库必须越庞大越好。

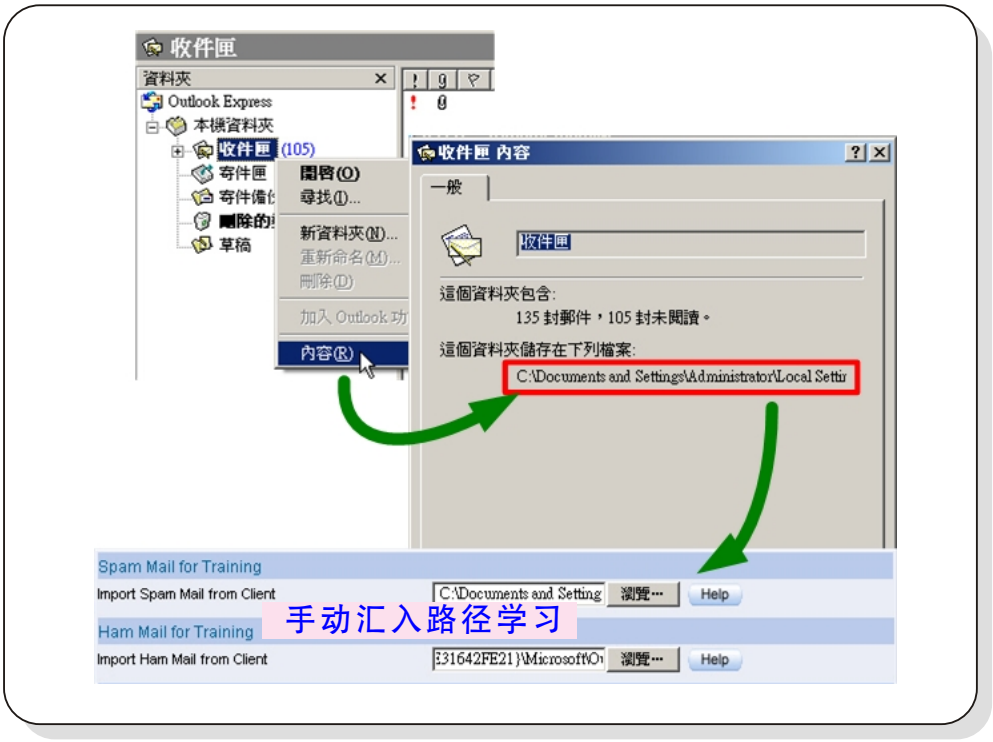
但是，新软多功能 UTM 的贝氏数据库在出厂时却不包含任何数据。这不是与上述之运作原理有所矛盾吗？其实，新软多功能 UTM 的贝氏数据库在出厂时特意不包含任何数据，原因是因为新软多功能 UTM 并无客户公司所认定之正常信件，若只有“垃圾邮件数据库”而无“非垃圾邮件数据库”，则相当容易造成信件的误判。

那么，如何将公司的正常信件与垃圾信件加入“贝氏数据库”以供学习呢？为了方便各公司的邮件使用习惯，新软系统多功能 UTM 提供了两种学习方式来让贝氏过滤数据库进行更新与学习。

方法一：手动汇入学习方式

此种方式是以手动的方法将垃圾信件另存于数据匣中，再将其数据匣连结输入于多功能 UTM 连结栏中，系统则会立即依据所填入之连结位置更新其贝氏过滤数据库。

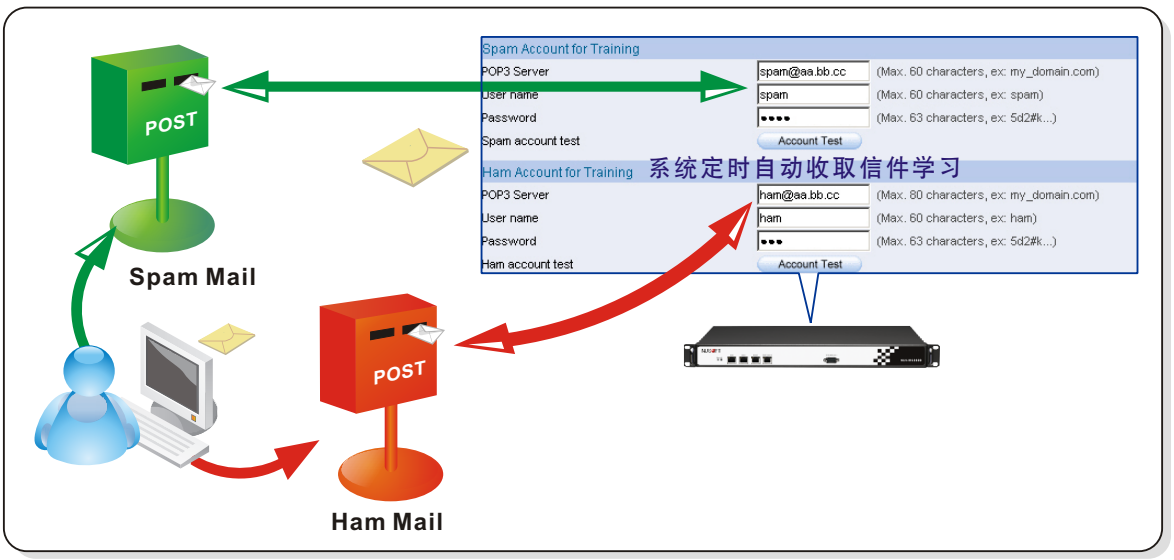
由于多功能 UTM 系统接口通常是资安管理人员才能够进入，所以信件的汇入相对也只有管理人员才能执行，如此的操作方式较为安全，比较不会有遭到其它使用者搞错或乱汇入之情形发生。然而也因此种操作方式完全必须透过管理人员才能执行，所以在数据库更新方面会稍显缓慢。



利用信件匣的储存连结，即可手动进行信件汇入贝氏过滤数据库

方法二：系统自动学习方式

另一种学习方式则是利用另外建立两组信箱账号，让系统来自动更新学习。管理人员可利用公司的邮件信箱，另外设立两组账号，分别为『正常信件用』及『垃圾信件用』，让公司内部人员将自己所遭到误判之信件分别传至此两种信箱内。而管理人员只需将此两组信箱账号分别填入多功能 UTM 系统中即可，系统会于每三十分钟自动向该两组信箱收取信件来进行数据库更新。



管理人员只需分别填入所设立之正常及垃圾邮件信箱即可让系统自动学习

利用自动学习方式需要注意的是，在分别寄送信件至所指定之信箱时，必需以转寄且用附加文件的方式来寄送，以保存该封信件的原始内容完整性，让贝氏过滤数据库于学习时能够更准确的学习到判断之条件。

此外新软系统多功能 UTM 还拥有学习时间的设计，让系统在更新贝氏过滤数据库后，系统可以在管理人员所设定之时间下才进行贝氏数据库的学习，这样的设计有何好处？由于贝氏过滤数据库在学习信件时多少都会消耗掉系统些许资源，而一般于正常上班时间系统还必须处理其它相关动作，为了能避免掉不必要的系统资源消耗及浪费，让系统于正常上班时间能全力处理当下所需处理之事宜，管理人员可将学习时间设定于下班后或是半夜、凌晨…等空闲时间，再让已更新过的贝氏数据库进行学习动作。

可自由调配及设定数据库学习之时间

	手动汇入方式	自动学习方式
优点	经过管理人员一一审核，所汇入之邮件较不容易出错，且较为安全。	数据库更新速度较快。
注意	数据库更新速度较为缓慢。	1. 需另外设立两组邮件信箱以分别提供『Ham Mail』、『Spam Mail』使用。 2. 信件寄送至指定信箱时，需使用附件转寄方式，保留原信件之完整内容。
备注	贝氏过滤数据库学习时间，建议设为下班後或是半夜、凌晨…等空闲时间。	

贝氏过滤两种学习方式

文 陈殿鸿 kim@nusoft.com.tw

市场营销报导 - 您也可轻松解决复杂的带宽管理需求

拜现今科技日新月异以及网络普及化所赐，网络已成为大多数现代人不可或缺之重要工具。但是使用网络时最在乎的就是联机顺畅度，而影响网络联机顺畅度最直接之因素就是「带宽」。一般来说，向 ISP 业者所申请之带宽一般都是有固定制量，所以在同一个网络环境里的所有人皆得同用一条对外线路，而每个人使用网络之目的皆不相同；有人只是纯粹浏览网页、有人用来看网络电视、有人用来下载文件、有人用来玩在线游戏…等等，所以在同时间内，若有使用者占用大量带宽时，势必会压缩到其它人的带宽，导致联机不顺畅（俗称 LAG）或者甚至有断线问题产生。所以妥善分配带宽规划是必须的。

而一般市售「带宽管理器」所提供之「QoS 带宽管理功能」，大多都只有最大带宽和优先权之设计；单纯的限制使用者带宽而无法确保重要网络服务运行所需之带宽。且如要细部管控整个企业带宽，需要特别为每台计算机都订定个别之带宽管理条例，运作起来相当死板、不方便。对网络架构简单之环境可能还好，但对于那些动则数十台、上百台甚至是上千台的网络环境则明显招架不住。

就以网吧为例－
A 网吧业者推出新消费政策，将店内计算机规划出 VIP 上网包厢区，需重新调整带宽规划，而店内网络环境如下：
计算机总数量：300 台
VIP 上网区计算机数量：60 台（开放使用 P2P 软件与在线影音软件）
一般上网区计算机数量：240 台（管制使用 P2P 软件与在线影音软件）
因应公司政策需求，将店内对外线路带宽划分一半，分别给 VIP 上网区及一般上网区之计算机使用。

如使用一般市售「带宽管理器」来管理网吧之带宽，则必须“针对这 300 台计算机一一定订带宽管理规则”、“个别限定 VIP 上网区计算机的最大联机数（P2P 软件之联机数也是造成网络堵塞的元凶之一）”、“另购管理机制禁止一般上网区之计算机使用 P2P 软件与在线影音”...。完成这庞大的建置工程后，才能达到网吧业者之规划需求。

但是！！
如果往后网吧因扩增而网络有所变动时（增加对外带宽、增设计算机数量...），这些变更都会牵一发而动全身，造成先前努力付诸流水；300 条的带宽管理政策、60 条之最大联机数设定...再也无法适用，必需重新来过。

针对上述问题，新软系统所推出之「多功能 UTM（MS 系列）」、「负载均衡器（MH 系列）」特别提供了各种管理机制，协助企业解决带宽管理之各种问题。

以多功能 UTM 為例：

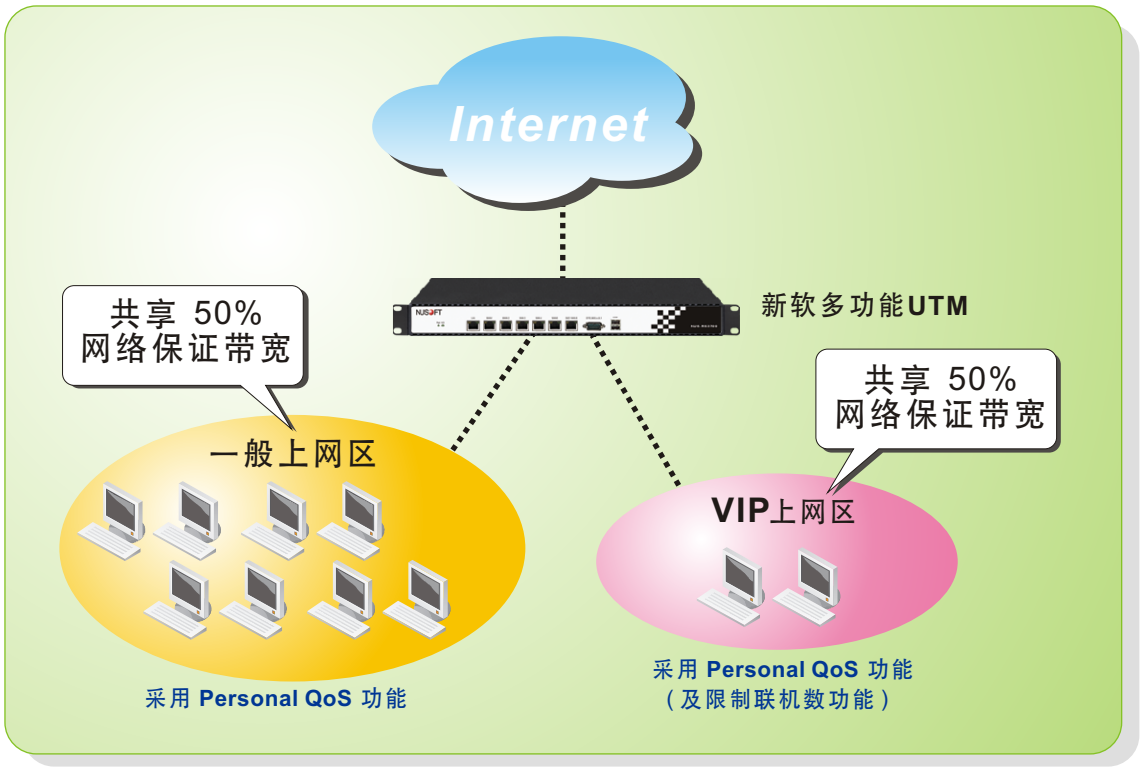


图 网咖业者希望不同上网计算机采用不同管制方式

一般上网区：采用多功能 UTM 的「带宽管理」功能将 50% 带宽划分给“一般上网”使用，再透过「个人化带宽管理」机制将这些带宽均分给一般上网区的计算机。最后再以「应用程序管制」功能封锁一般上网区“P2P 软件与在线影音软件”之使用权限。仅要一条管制条例，即可达成“一般上网区”的带宽管理需求。

VIP 上网区：一样使用「带宽管理」与「个人化带宽管理」功能将网吧 50% 之带宽均分给 VIP 上网区的计算机，再透过「个人化最大联机数」机制限定每台计算机的最大联机数。一样仅需要一条管制条例，就可轻松管理“VIP 上网区”之带宽使用。

如此一来，既可保证所有使用者之上网联机带宽，又可让 VIP 上网区之 VIP 使用者享受到网上奔驰快感。往后，如因扩增而需变动网络时，就只要调整这“两”建条管制条例，轻松、简单！！

	新软多功能UTM、负载均衡器	一般市售带宽管理器
管理规则	优，可搭配两种以上不同的带宽管理规则。	差，只能设定最大带宽限制规则。
管理方式	优，依照管理政策分别对不同群组进行的带宽规划。	差，无法做到「依政策做到弹性的带宽规划」。
其　　他	可在同机上使用相关应用管制规则(如:P2P 管制)。	无，需另外花费添购其他网络管理设备。

表 新软多功能UTM、负载平衡器与其他市售产品比较表

文 黄政铭 ming@nusoft.com.tw