新软周报
http://www.nusoft.com.tw
Internet Security Fighter
2009/11/30- 2009/12/13 第106期

邮件服务器 / ML系列报导

技术浅谈与应用 - 自动化白名单

数字e化的时代，垃圾邮件问题，长久以来一直是所有人的困扰，在目前无法完全治本的情况下，只能靠治标的方向来解决，利用科技来围堵垃圾信将是企业自保首要之道。因此反垃圾邮件技术不断翻新，在众多防护机制中，比对式垃圾邮件过滤方式又是最为基本不可缺的一项。比对过滤技术大概可分两种类型，传统也是大多企业使用的是『名单比对』(如黑、白名单)。其中黑名单是拦阻垃圾邮件最常用之过滤方式，基本上利用人工键入方式来判断是否为垃圾邮件来源，邮件服务器再依据黑、白名单上所键入之清单来判断处理。

“黑名单”是指一个事先的邮件筛检方式。虽然被最广泛地用以对抗垃圾邮件的解决方案，但有时它不但不能够有效阻止垃圾邮件，而且还可能会导致了一些合法并重要的电子邮件永远都不能到达目的地。相对和黑名单基于排除的做法不同，“白名单”是致力于确认合法之电子邮件来源，这样就不会有黑名单排除失误之情况，但却有可能因为垃圾邮件利用伪造寄件来源的方式，而出现漏洞。

为弥补垃圾邮件黑、白名单防护机制旧有的不足之处，同时还可再配合其它邮件过滤机制，新软系统推出了新式防护机制『自动化白名单』，来有效减轻管理人员对于垃圾邮件阻挡上的负担。何谓『自动化白名单』？其运作方式又为何？以下将一一说明。

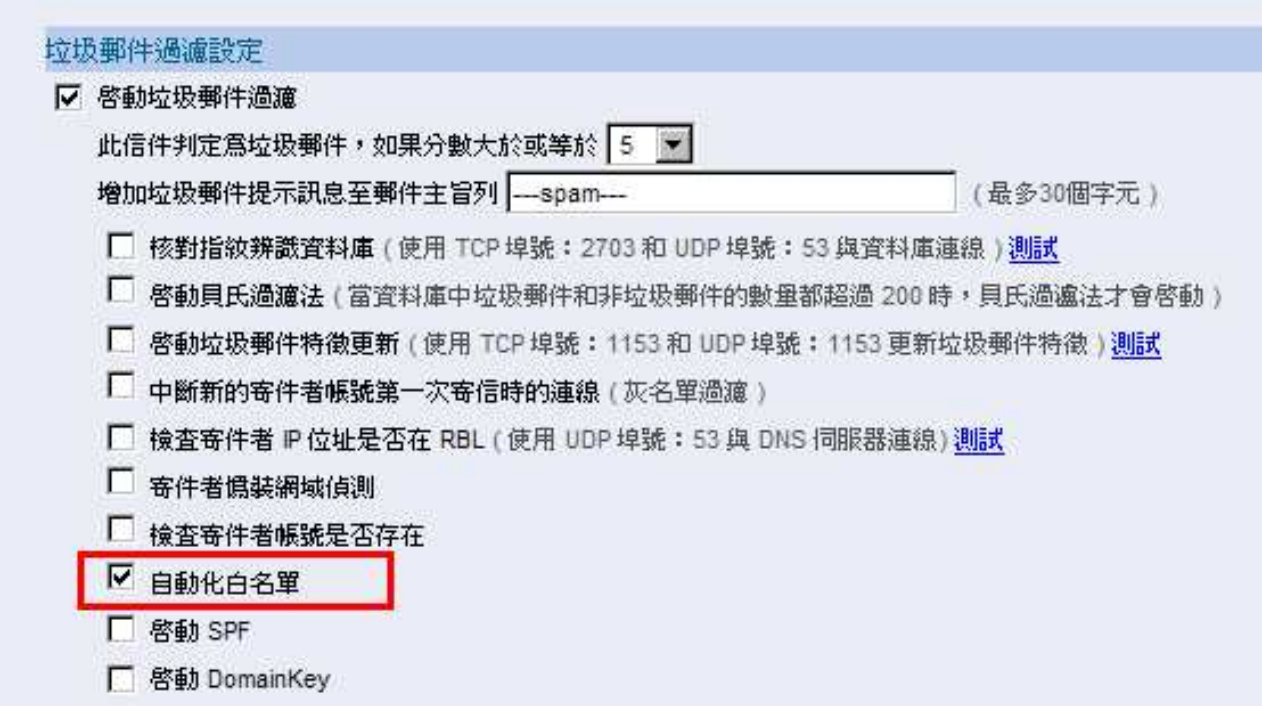
一、何谓自动化白名单：

简单的说，自动化白名单是依照该寄件来源以往的记录，进而来计算新信件是否为垃圾邮件之机率。当寄件者寄出一封信件到邮件服务器-ML时，会先经由其它过滤机制过滤评分，最后再由『自动化白名单』机制计算这封信的评等，分数若越高，则代表该封信件之内容越符合垃圾邮件的定义。有别于平常一般所使用的黑、白名单之处在于管理人员可不必费心思去自行设定黑、白名单中的来源清单，即可藉由自动化白名单机制来达到有效的黑、白名单防护机制功能，同时还可大幅降低一般黑、白名单所易产生之信件误判情形发生。

但管理人员必须要注意到，若于ML里黑、白名单上有键入之名单，系统则会先行依照黑、白名单来做阻挡及放行，该些名单并不会再由『自动化白名单』机制来进行处理判断与计算。

二、如何启用自动化白名单：

管理人员可在 ML 系统中『邮件安全 > 邮件过滤 > 设定』下，于『垃圾邮件过滤设定』中勾选『自动化白名单』后，即可启用。



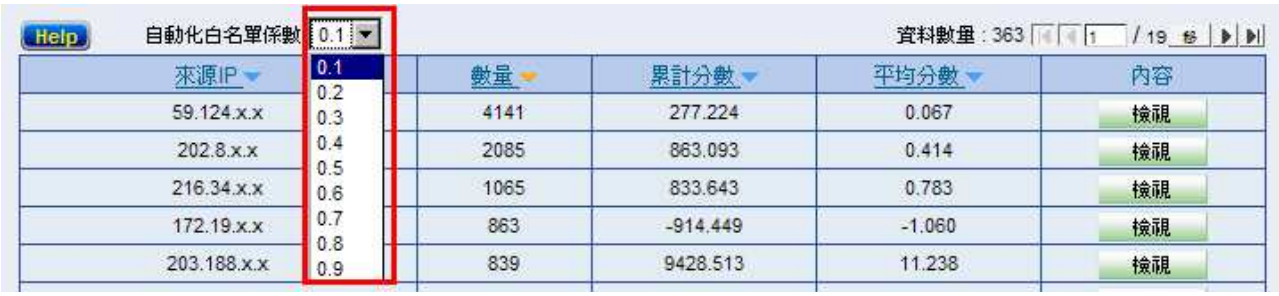
开启自动化白名单机制

三、自动化白名单中的来源判断方式：

『自动化白名单』机制会记录所有寄件者的 e-mail 和 class B 的 IP 地址，每当有新信件时，则系统会去比对这两个字段，若两个字段信息皆相同系统才会将该信件视为同一个寄件来源。之后再依据来源做分数的计算与累计，这样定义方法，可以避免垃圾邮件随机假冒他人之 e-mail 账号或者 IP 发出垃圾邮件，而造成该账号或网域被误列为黑名单。

四、自动化白名单上的『系数』用意：

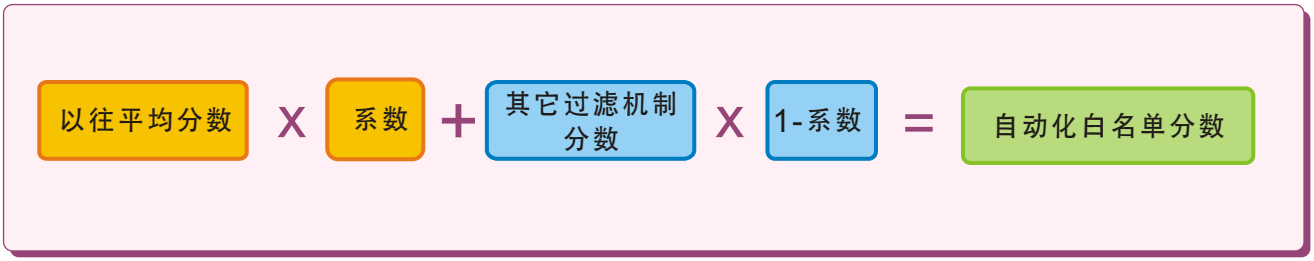
每有新信件送达时，自动化白名单机制就会将该封信件来源于机制里以往所算出之平均分数 (累计分数/累计信件数) 和新信件的分数 (其它过滤机制所算出)，依自动化白名单系数做权重分析。而当管理人员所设定之系数数值越高，则表示该来源之前于此机制中所计算出之平均分数占有的权重越高，也就是说越重视该邮件来源先前所算出的分数结果。所以自动化白名单上的系数 0.1~0.9，也可以说成每次在做分数上的计算时，先前所算出之结果于该次分数运算中所占的权重比例为 10%~90%。



自动化白名单的系数选单

五、自动化白名单的分数计算：

在自动化白名单机制中，新进信件的分数计算方式为『(先前平均分数 x 系数) +〔新进信件分数 x (1-系数)〕』，若是该来源无先前平均分数则会将其它过滤机制分数直接列入。如此计算器制有什么好处呢？在这样的机制下，当纪录里一个不曾寄送垃圾邮件之来源，新寄出的信件在垃圾邮件分析后分数若出现偏高时，机制会因为之前平均分数的良好纪录，自动调降信件在垃圾邮件定义下之分数，以防止不当的误判发生。例如当管理人员将自动化白名单上之系数设定为 0.4 时，某平均分数为 -5 分的良好来源，新寄出了一封分数为 10 分的信件时，先前良好的平均纪录会乘上 0.4，而新信件的分数则会占去另外的 0.6，[(-5) x 0.4] + (10 x 0.6)=4，分数则会被降低为 4 分。



信件计算示意图

相反地，当一个常常寄出垃圾邮件的来源，就算本次寄出的信件在垃圾邮件的评等中分数偏低时，也会因为先前的不良纪录而使得最后计算出之分数变高，藉此来提升该信成为垃圾邮件的可能，以防止不正常之信件因此而流入内部。例如当管理人员将自动化白名单上之系数同样设定为 0.4 时，平均分数为 20 分的不良来源寄出一封分数 2 分的新信件时，在 (20 × 0.4) + (2 × 0.6) 计算后，分数则会被提升为 9.2 分。

此外，自动化白名单中的分数表达方式为小数点以下第 4 位，四舍五入。

文 陈殿鸿 kim@nusoft.com.tw

市场营销报导 - 新增功能「自动化白名单」，给您更聪明的邮件过滤机制

在现代这个数字化的时代，网络改变了人们的生活方式，随之而来的便是e化之方便生活方式；但是从相反面来看，许多现实生活中让人烦恼不已之行为也随着生活e化而衍生出来；最为明显行为莫过于“企业最为倚重之电子邮件”的垃圾邮件问题。

电子邮件是企业与企业之间最为倚重之商业往来工具，然而有利必有弊，其强大方便的功能性也被不肖份子所看中，被人拿来利用成为广告垃圾信件的最佳途径，导致现今广告信件肆虐，常常让人在一堆广告信件里找不到真正那封自己想要的浏览的信件，间接造成企业营运资源多余浪费、公司生产效率降低…。基于以上多项企业间困扰的问题所在，使得市面上出现许多拥有垃圾邮件过滤机制的邮件服务器。

但是目前市面上许多的邮件服务器所提供之垃圾过滤机制大多都不够完善、不够人性化，最常见的方式是采用黑、白名单、RBL黑名单、贝式过滤…等几种垃圾邮件过滤机制，然而单单就只依靠此几类判别机制容易造成信件漏挡，甚至是信件误判…等问题；因此新软系统邮件服务器-ML系列则提供使用者以独家七道垃圾邮件过滤机制来严格把关，但是网络世界、一日千里，垃圾邮件也随之变化多端。所以为了因应如此变化巨大的垃圾邮件类型，新软系统邮件服务器-ML系列又推出了“自动化白名单”此项聪明人性化之设计，藉以尽滤所有的垃圾邮件。

※自动化白名单

将以往之信件(来源与寄件者账号)作为参考依据，再依所设定的系数做权重分析，以阻拦伪造寄件者之垃圾邮件(寄件人为自己的垃圾邮件)，并可避免经常往来之寄件者的来信被误判为垃圾信。(详细计算方式，请参阅本期技术篇)

新软系统藉提供此功能让使用者在白名单使用上更为轻松方便，也让垃圾邮件在新软系统邮件服务器7+1的八道垃圾邮件过滤机制里更加无所遁形，让企业资安处理能力更为完善、企业营运更具实力。

	使用时机
黑名单	不请自来的电子报。 (固定寄件者帐号之垃圾信件)
白名单	信件往来的厂商、客户。 (不建议将企业网域整个加入白名单，此种设定会造成无法阻挡伪装成内部寄件者之垃圾信件)
自动化白名单	1.伪造成内部寄件者之垃圾信件 2.企业内部往来之正常信件被误判时。

新软邮件服务器黑名单、白名单与自动化白名单使用时机

文 黄政铭 ming@nusoft.com.tw