反垃圾邮件6大方案

6 Schemas to Against Garbage Mails

策划：周斌　　撰稿：周斌 稚晖

反垃圾邮件正在成为国内IT界的共同行动。2003年12月7日，旨在探讨中国互联网的发展趋势，以促进互联网在经济、社会、科教、文化等领域应用的创新和提高的第二界中国互联网大会在北京闭幕。在此次大会中，治理垃圾邮件成为最受关注的四大热点之一。

随着信息时代的飞速发展，无限沟通与信息共享成为可能。但是，人们在享受互联时代所带来的方便与快捷的同时，烦恼也随之而至。据中国互联网协会和CNNIC最新联合发布的《中国互联网发展报告》显示，我国网民在2003年7月份每周收到正常电子邮件为7.2封，垃圾邮件数却达到8.9封。垃圾邮件数量比2002年12月的8.3封又有增长。

垃圾邮件已经成为继病毒之后对互联网危害最大的杀手。它不仅对整个世界的现代经济造成了严重破坏，而且，它也开始动摇人们对电子邮件——这一最基本的网络通讯方式的信任。面对着垃圾邮件的泛滥成灾，反垃圾邮件的呼声一浪高过一浪，全世界都在采取相应措施应对这一危机。美国、日本、韩国、法国、澳大利亚以及欧盟都纷纷出台了针对垃圾邮件的相关法案。以法律的形式来遏制这一人为因素而导致的人类公害，是人类想要控制灾害时通用的世界性规则。

当然，事物的两重性在这场全球化的“瘟疫”中也突显出来。从另一个角度来看，反垃圾邮件战役也为相关商家提供了巨大的商机。在国内，众多反病毒厂商凭借着先天的优势开始跻身于这一广阔的市场之中。金山、赛门铁克、趋势科技、冠群金辰以及美国网络联盟等，都相继提供了针对垃圾邮件的产品和解决方案。与此同时，以263为首的众多国内邮件服务商也组织成立了国内第一个反垃圾邮件组织——“反垃圾邮件协调小组”，从另一侧面有效地推动了国内互联网行业的反垃圾邮件协作。

但是，所谓“魔高一尺，道高一丈”，在这场斗志斗勇又比拼耐力的无硝烟战场上，很难评定出谁将是真正意义上的胜利者。机遇永远会与挑战结伴而行，能够以慧眼把握先机、以实力奠定前提的人将注定在这场严峻的商战中成为最后的赢家。

本期所选出的“反垃圾邮件6大方案”，涉及了电子邮件服务商和国内外反病毒厂商的几款最新产品，其中263的“五重净化”极具特色，代表了国内外电子邮件服务商如新浪、搜狐、雅虎等在为客户服务方面的独特思想。另外，国内反病毒厂商金山公司也涉足该领域，显示了一定的市场眼光。

垃圾邮件横亘网中央

和往日一样，何先生进入办公室的第一件事情就是打开电脑进入自己的电子邮箱。作为部门主管，浏览和处理电子邮件成为何先生每日必须完成的第一件工作。

与客户沟通、公司内部交流……电子邮件成为何先生对外联系的一个不可或缺的方式。然而，很长一段时间以来，一个越来越麻烦的问题开始日日困扰着他，那就是：每天打开邮箱后，他不得不花费大量的时间来处理一些与工作和生活毫不相干的垃圾邮件。促销广告、致富信息、理财宝典、黄色网页……最可怕的是有些垃圾邮件还带着致命的病毒，一旦打开，后果不堪设想。怎么办呢？何先生也想了不少的办法，但最后都收效甚微。

互联网让这个世界变得越来越小。南半球的故事传到北半球所经历的不过是区区几分钟而已。然而积极的一面总会与消极的一面共生共存。互联网在打破地域和时空界限的同时，也将如瘟疫一般的负面浪潮无视种族、国家、性别的障碍而肆无忌惮的呈现于全人类的面前，正如垃圾邮件。

1972年，当第一封Email 诞生之后，电子邮件这种快捷方便的通讯方式就像雨后春笋般，在全世界范围内迅速成长并得到普及。现在，人们的日常工作、生活都与这种现代的通讯方式密不可分。但是，时至今日，铺天盖地的垃圾邮件已经让Email——这条通讯的“高速公路”越来越难行了。

触目惊心的损害

现在，垃圾邮件已经成为何先生最为头痛的一件事。如果有一天，这些讨厌的垃圾邮件能够从邮箱中彻底消失，互联网的方便快捷和无限沟通才有可能得到真正实现。

事实上，垃圾邮件带来的困扰不仅仅是何先生个人的问题。目前，几乎所有使用电子邮件的人都曾受到过而且正在经受垃圾邮件的骚扰。垃圾邮件已经成为继电脑病毒之后危害互联网的第二大杀手。它所造成的损失与危害已经触目惊心。

2003年，全球企业因垃圾邮件引起的损失已超过205亿美元。著名网络安全研究机构GADICATIGROUP强调，情况如得不到控制，到2007年时，这个损失将暴涨到1980亿美元，到那时候，垃圾邮件将占总邮件比例的70%。

互联网研究机构Jupiter则估计，如果垃圾邮件泛滥的局面继续下去，到2006年，全球个人消费者将收到总计为2060亿个的垃圾邮件，平均每人1400件垃圾邮件，其造成的损失将是难以估量。据相关调查，全球每年有逾50万件线上身份证和信用卡盗用案例是透过垃圾邮件达成的，而网民平均每天需花费6.5分钟来处理无用的邮件，单是下载垃圾邮件所花费的上网费与电话费，每年就要花掉全球网民94亿美元。

在中国，根据中国互联网协会公布的数据，截至2003年11月底，向中国服务器发出的垃圾邮件约有1500亿封，占中国互联网用户收到的电子邮件总数的30%，垃圾邮件耗费了中国GDP超过48亿元。

垃圾邮件已经成为摆在人们面前的一道棘手难题。

高调立法用处不大

垃圾邮件的出现给所有与网络有关联的人们带来了无穷无尽的烦恼。如果说数年前电子邮件所带来的新颖的营销方式还使人们津津乐道的话，那么现在无孔不入的强迫性的接受方式却成为电子邮件使用者心口永久的痛。垃圾邮件的治理已经迫在眉睫。

事实上，反垃圾邮件成为互联网业界刻不容缓的事情早已是定论。世界各国均对此采取了相应的措施。立法，而后依法行事，高额的处罚款项对垃圾邮件的发送者至少产生了一定的约束力。从意识层面上讲，对反垃圾邮件，全球已经达成了共识。而只有全球统一起来，反垃圾邮件才有可能是真正意义上的开始。

在美国，2003年12月，美国总统布什签署通过了Can-Spam垃圾邮件管制法案，并于2004年1月1日起开始生效。而早在同年9月，美国加州就通过了全美最为严格的反垃圾邮件法案，该法案禁止加州营销人员主动提供商业电子邮件，并禁止营销人员向加州居民发送此类邮件。

在欧洲，2003年年初，法国国民议会表决通过一项议案，禁止向个人发送商业广告性质的电子邮件，除非事先征得收件人同意。鉴于许多垃圾邮件是"境外来客"，10月31日欧盟正式实施了与法国类似的法案，在欧洲范围内全面禁止跨国滥发电子邮件的行为。

在澳大利亚，联邦政府2003年12月19日宣布，澳大利亚的反垃圾邮件法案在获得王室同意书120天之后将在2004年4月11日成为法律。从4月11日起，坚持滥发垃圾邮件的企业每天最多可罚款110万澳元（约81.1万美元）。

从国内的情况来看，2000年8月，中国电信出台垃圾邮件处理的具体办法，但并未出台如何认定垃圾邮件的具体细则。2002年11月，中国"反垃圾邮件协调小组"成立。尽管协调小组先后三次针对发送垃圾邮件的若干个国内外服务器的IP地址进行了封杀，但是作为行业组织的自律行为，其权威性必定受到质疑，而其更无法与法律相提并论。

2003年12月，第二届中国互联网大会召开，反垃圾邮件成为本次会议四大热点之一。尽管大会人所共识“要真正解决垃圾邮件的问题非立法不可”，但是，垃圾邮件的模糊界定，法律自身存在的漏洞以及垃圾邮件层出不穷的花样翻新，都为立法设置了重重障碍。国内的立法似乎依然有一段长路要走。

虽然立法反垃圾邮件的呼声已经响遍全球，但是这种没有国界限制的垃圾邮件如果不是全球的统一行动，想要彻底根除它的可能性微乎其微。同时，立法也就真的是万全之策吗？就如同垃圾邮件的出现是网络技术漏洞产生出的附加产品一样，任何法律的漏洞都可以作为垃圾邮件制造成长的新温床。

事实上，立法应该仅仅是反垃圾邮件战役的重要组成部分之一。因为对于这样一个全球性的行动来讲，并不是一个企业或者一个组织能够实现的，它需要全社会包括政府、组织、普通用户、各种网络服务商在内的群体的支持和协作，实行立法、组织和技术的综合治理。

服务商在行动

垃圾邮件的存在对于计算机系统及网络安全的威胁不言自明。因此在美国，反垃圾邮件的市场份额一点都不比反病毒市场小，而且许多反病毒厂商本身就扮演着反垃圾邮件的角色。

在国内，与政府行动迟缓相对照的，是国内一些反病毒厂商的积极行动。对于敏感的商家而言，反垃圾邮件这块巨大的奶酪正在日益散发出诱人的清香。

2003年12月18日，金山率先推出国内首款反垃圾邮件的杀毒软件“金山网镖6”，“防毒防黑反垃圾，三防一体化”。新概念催发了新的市场。金山先声夺人拔得这一市场的头筹，相信对此眼红的商家亦不在少数。目前，除金山之外，国内一些反病毒厂商如冠群金辰、赛门铁克、美国网络联盟、趋势科技等都纷纷开始针对这一领域推出了相应的产品及解决方案，以期夺得这一空白市场。

在反垃圾邮件行动中表现踊跃的还有邮件服务商们。2003年12月6日，国内专业电子邮件服务商263网络集团，宣布针对邮件用户推出全新的超级反垃圾邮件解决方案。其“五重净化”功能扬言将终结“信骚扰”时代。263在反垃圾邮件领域一直不遗余力，2002年其与中国互联网协会共同发起了“反垃圾邮件协调小组”。2003年，该小组先后三次牵头，在电信级运营商提供的支持下，开展了“封杀垃圾邮件服务器”的行动。

但是，巨大的市场是否真的能够带来巨大的收益？反垃圾邮件市场若干年后是否会步杀毒软件市场的后尘？这个疑问是许多企业进军反垃圾邮件领域后心中的一个结。但是我们又不得不承认，后病毒时代为低迷的IT业创造了又一个产业的崛起。那些因垃圾邮件或生存或灭亡的企业，将注定在这个网络时代设置一个几年内尚无法预知无法推测的悬念。

难说再见

尽管垃圾邮件已经到了过街老鼠人人喊打的地步，但要想要对它们彻底说再见，却绝不是一件轻而易举的事！毕竟，治理垃圾邮件不是一朝一夕的事情。

垃圾邮件产生的原因是多方面的，除了用户的意识薄弱是造成垃圾邮件泛滥的主要原因之外，利益的趋动也是诸多垃圾邮件制造者趋之若鹜的根本动力。所谓“魔高一尺道高一丈”，在反垃圾邮件厂商们正在为这一空白市场沾沾自喜的时候，垃圾邮件的制造者们也正在把握时机，从软件与服务中寻找新的漏洞，来制造更大的机会获取更为诱人的利益。向垃圾邮件说再见，绝不仅仅是挥挥手那么容易。

垃圾邮件令政府和企业都开始行动起来，然而，由于最终的邮件使用者是反垃圾邮件最大的收益者，他们也应该在这个全球范围的行动中担当起主要角色，他们是这个战役中最重要的一个组成部分。263网络集团总裁黄明生就曾指出：“就像打击街头小广告一样，抵制垃圾邮件应成为全社会共同关注的问题，信息共享、共同防范是反垃圾邮件的首要任务。反垃圾邮件不只需要厂商行动起来，也需要用户的大力配合和积极参与。”反垃圾邮件，应该是全民动员与参与的又一个集体行动。

背 景：

什么是垃圾邮件？

2003年11月1日，中国互联网协会、263网络集团、新浪网共同发起“反垃圾邮件协调小组”，在成立仪式上，中国互联网协会公布了对“垃圾邮件”的正式定义：

- 收件人事先没有提出要求或者同意接收的广告、电子刊物、各种形式的宣传品等宣传性质的电子邮件；
- 收件人无法拒收的电子邮件；
- 隐藏发件人身份、地址、标题等信息的电子邮件；
- 含有虚假的信息源、发件人、路由等信息的电子邮件。

垃圾邮件的起源？

1994年4月12日，两名来自亚力桑那专门从事移民生意的律师，通过互联网大量发送他们移民顾问服务的电子邮件，从那时起，这一对当时默默无闻的夫妻搭档为互联网创造了"垃圾邮件"。

垃圾邮件的蔓延态势

- 2002年垃圾邮件大约占所有邮件信息量的25%，据估计在2003年将有76亿不需要的商业性邮件信息在互联网上传播。
- 垃圾邮件现在正呈现不断增多的趋势，据美国Brightmail公司统计，在过去的6个月里垃圾邮件的数量翻了不止一倍。Jupiter曾估计，到2006年消费者将收到2060亿个垃圾邮件，平均每人1400件，而2003年的统计数据是每人700件。
- 仅商业性垃圾信件一项，每封垃圾邮件所抵消的生产力成本就在1美元左右。以此计算，2060亿个垃圾邮件造成的损失让人痛心。
- 欧盟的一项调查估计全球网民为收取垃圾邮件而支出的接入费用高达100亿欧元。
- 单是下载垃圾邮件所花费的上网费与电话费，每年就要花掉全球网民94亿美元。
- 在企业网络中，36%的邮件为垃圾邮件。

最新一份数据显示，根据英国的一份调查，互联网上所有垃圾邮件的“幕后黑手”全世界大约共有150人，而90%的垃圾邮件都来自其中的一个核心组织。在英国每8封电子邮件中就有一封是垃圾邮件，3/4的私人账户每天都会受到垃圾邮件的骚扰。

“反垃圾邮件六大方案之一”

263“五重净化”

在所有的互联网服务中，电子邮件服务是一项最基本的服务，而各大电子邮件服务商在“反垃圾邮件”上的探索和尝试更是由来已久。263网络集团提供的方案入选六大方案之首，即基于此原因，其提供的电子邮件服务在国内家喻户晓。

2003年12月6日，263宣布针对邮件用户推出全新的超级反垃圾邮件解决方案，该解决方案具备从系统端到用户端“五重净化”功能，向用户提供了独特的“不明邮件夹”和“超级地址簿”，用户可以依据自身需求方便地分级设置反垃圾系统，最终实现彻底排除垃圾邮件干扰，同时，也能有效防止正常邮件被误屏蔽的现象。

其实，邮件过滤早已是众多电子邮件服务提供商的一项基本服务项目。263的反垃圾邮件系统将其继续深化，设置了“系统端屏蔽”、“系统端过滤”、“用户端屏蔽”、“用户端过滤”“超级地址簿”五重过滤屏障，同时添加了“不明邮件夹”，为邮件过滤上了“全险”。

一重过滤：系统级屏蔽

系统通过“垃圾邮件黑名单”在邮件系统的外部直接屏蔽垃圾邮件，被称作263反垃圾邮件解决方案的第一道屏障。“垃圾邮件黑名单”内置于系统内部，来自业界已公布的垃圾邮件地址以及投诉系统反馈的垃圾邮件地址的邮件，将会直接被屏蔽。此外还有一些符合系统默认规则的邮件，也同时被屏蔽，如发件人过多的邮件，主题明显符合垃圾邮件特征的邮件等，通过屏蔽，邮件用户将无法看到这些垃圾邮件。

二重过滤：用户级屏蔽

对于那些用户很明确不愿意接收的邮件，但又不是系统默认的垃圾邮件，比如，不想再接触某个人，或不想再接收自己曾经定制的某些新闻邮件等等，用户可以通过拒收的方式，从此屏蔽掉这些邮件，这被称为“用户级屏蔽”。这种操作非常简便，用户只需选中该邮件，并点击功能选项中的“拒收”按钮，即可将该地址加入拒收名单中，以后来自该地址的邮件将被直接屏蔽掉，不再进入用户的视线。

三重过滤：用户级过滤

用户还能够自行制定一些过滤规则，比如主题中包含“get money”、“注册”等的邮件，不希望被收进收件箱中，但其中有可能是有用邮件，263超级反垃圾系统的突破就是为用户提供了“不明邮件夹”，符合此类条件的邮件可以暂时存放到“不明邮件夹”中，用户还可以根据自己的需求设定过滤规则和相应的文件夹用来存放某一类邮件，称为“用户级过滤”。“不明邮件夹”只存在于web邮箱中，并且不占用用户的使用容量，由用户自由决定是否接收、查阅或移动这些邮件，这样用户便可以更合理地管理邮件。

四重过滤：系统级过滤

对于那些系统不能完全确定是垃圾邮件、用户也未经设定的不明邮件，可以通过“系统级过滤”来进行第四重检测。系统设定一些较为常见或模糊的分辨规则，如，主题中包含“hi”、“Do you want……”、等，通过“系统级过滤”，这些邮件将被过滤暂存到“不明邮件夹”中，用户可以选择性查阅，这样有效地避免了系统将正常邮件误屏蔽的现象。

五重过滤：超级地址簿过滤

当用户选择使用超级地址簿过滤时，邮件在经过前四重过滤后，只有用户地址簿中的地址发来的邮件，才能到达用户的收件箱，其余邮件均被过滤到“不明邮件夹”中，达到“真空环保”的效果，这对于对通信的保密程度具有高要求的用户来说非常合适，因此，这种方式被称作“绿色通道”，意指可以完全保证用户收件箱的清洁度。值得一提的是，所谓的“超级地址簿”具有很便捷的“自动导入”和“智能添加”的功能——可以将用户OUTLOOK中的地址簿自动导入到263的Web邮箱的地址簿中，成为“超级地址簿”；并且此后用户在第一次向“超级地址簿”中尚未收录的邮件地址发送邮件时，该地址将会被自动添加到“超级地址簿”中。

263超级反垃圾邮件解决方案的五重过滤是可选择的，用户可以按照自身需求设置合适的过滤方式。263将用户端设置分为高、中、低三档选择，用户如果选择为“高级过滤”，则邮件将完成全部的五重过滤，直到彻底清洁；用户选择为“中级过滤”，邮件完成前四重过滤后就直接进入收件箱中。而当用户选择“低级过滤”时，邮件完成前三重过滤后，便进入收件箱。

“反垃圾邮件六大方案之二”

趋势科技 SPS 2.0

目前拦阻垃圾邮件的方法有两种：数据库比对和智能型判断。

数据库比对也可以称作是被动式的垃圾邮件拦阻方式，利用建立垃圾邮件的黑名单数据库，根据来源的IP地址、网域，寄件人的E-mail 地址或是内容、标头所含的关键词等作为数据库的基础。再将寄达的E-mail与这已知的垃圾邮件数据库比对，藉以判别是否为垃圾邮件然后再来做拦阻的动作。

智能型判断也就是主动式的拦阻方式，则是根据邮件的多项特征，包括内容、标头、格式等来判断这封E-mail会不会是封垃圾邮件。再来针对这封E-mail做处理。所以智能型判断的方式可以用来辨识和监测现有与新型的垃圾邮件。

趋势科技最新版的IMSS 5.5（InterScan Messaging Security Suite），整合了垃圾邮件防治服务SPS2.0（Spam Prevention Solution）。IMSS5.5通过网关端整合反垃圾邮件的智能型启发式垃圾邮件扫描引擎、网关邮件防毒以及内容管理三大关键安全要素，拥有防毒、防范垃圾邮件和内容侦测等多项强大功能，同时可减少45%的安全部署整体成本。

同时，IMSS 5.5也具备了数据库比对和智能型判断两种方式，而SPS针对E-mail的多项特征值进行交叉计算得出一组机率值，作为判定这封E-mail是否为垃圾邮件的依据。IMSS的特色就是可以群组化和层次化的弹性设定安全管理策略，可以针对公司内的个人或是群组甚至是不同的网域来分别设定适当的邮件处理原则。当IMSS 5.5整合了SPS 2.0之后，和eManager 过滤器一样，SPS 2.0就如同IMSS 5.5的一个过滤器，所以可以弹性的加入原本的安全管理策略之中。

SPS的运作流程

SPS的核心技术就是一组详细计算架构出的演算式，依据E-mail的标头、内容、格式等特征去进行计算与判断。当一封E-mail通过SPS的启发式引擎时，会有许多组演算式同时被激活进行运算。然后得出一组垃圾邮件机率值。如果这封E-mail的垃圾邮件机率值分数超过了使用者设定的界线，那么就会被视为垃圾邮件加以处理。当E-mail经过SPS的垃圾邮件引擎（Anti-Spam Engine）时，会经过六个步骤，完成运算、判断及处理动作。

1. 首先检查E-mail是否属于黑名单或是例外清单之中。如果列在黑名单中则加以拦截，属于例外清单的寄件者则允许通过不需要再经过垃圾邮件引擎。
2. 接着检查E-mail的标头及内文是否符合特别例外清单内的条件式。符合特别例外清单条件的E-mail可以直接寄送。
3. 除了列在上述特别名单中的E-mail以外，第三步骤则是经过SPS的垃圾邮件引擎来帮经过的E-mail打分数。给定垃圾邮件机率值。主要有两种分数，即Baseline（基准线），是根据邮件的各项特征来判断是否为垃圾邮件；另外就是进一步判断可能的广告类型，如商业广告、赚钱广告、色情广告、种族歧视广告等。
4. 当有了垃圾邮件引擎所计算出来的垃圾邮件机率值和四种广告类型的可能机率值之后，再根据使用者的侦测率及敏感度设定来标示这封信件是否为垃圾邮件。
5. 接下来便是根据SPS的分数和判断结果，在E-mail中加入SPS的标头讯息。
6. 因为IMSS可以弹性的设定过滤器处理动作，所以可以针对这些E-mail经过垃圾邮件引擎处理过后的结果加以执行不同的动作。

SPS的部署模式

通常而言，SPS会与IMSS集成为一体，部署在企业内部网与外部Internet之间的网关位置。由于IMSS即包括了邮件病毒过滤、邮件内容过滤功能，再加上SPS的垃圾邮件过滤，实现了“三合一”的功能组合，有效地在网关建立起一套完善的邮件防护体系，杜绝了各种非法或可疑邮件进入内部网络进而造成破坏事件发生。

IMSS与SPS都是软件产品，部署在服务器上作为邮件过滤网关，在提供高性能的过滤能力的同时，也提供了良好的升级、更新等功能，更具备了为系统管理员而安全策略定制的灵活性。作为网关型产品，IMSS+SPS的组合，支持大型企业级网络的大数据量邮件的过滤。

“反垃圾邮件六大方案之三”

冠群金辰 KShield Gateway

冠群金辰软件公司的反垃圾邮件系统KShield Gateway是一个针对E-MAIL系统的SMTP（简单邮件传输协议）进行过滤的产品。因此KShield Gateway的应用只与是否使用SMTP协议有关，而与具体的邮件系统无关。KShield Gateway包括邮件病毒过滤、垃圾邮件过滤、敏感信息过滤等引擎，根据用户需要可进行功能扩展。在对SMTP协议的支持上，当前KShield Gateway支持标准的SMTP和SMTP的扩展协议ESMTP。

工作原理

对于发进来的邮件，KShield Gateway主要是利用邮件路由协议的特点进行工作，出于容错和扩展方面的考虑，SMTP在设计时引入了邮件路由的思想，邮件总是首先试图传递给优先级值相对较高的MX邮件服务器，失败后才试图传递给优先级值稍大的MX邮件服务器；同时邮件总是在试遍了同一优先级的MX邮件服务器都失败后，才试图传递给优先级稍低的MX邮件服务器。

因此，一封具有一个收件人地址的E-mail可以有多个MX邮件服务器目标，每台MX邮件服务器可以设置成不同的优先级，高优先级的邮件服务器将先进行处理，如果高优先级的邮件服务器出现意外，邮件会自动发向第二优先服务器，依次直到最低优先级服务器。在使用中，我们赋予KShield Gateway最高的优先级，KShield Gateway具有完整的MTA服务功能，这样所有的邮件将先发到KShield Gateway，进行处理，再由KShield Gateway通过SMTP协议传给MX邮件服务器。

对于发出去的邮件，可以在DNS中修改RELAY服务器的IP指向，或者用户直接修改自己所用的邮件客户端软件的RELAY服务器以指向KShield Gateway 就可以了。

从垃圾邮件过滤引擎的原理来看，可以看到KShield Gateway的垃圾邮件过滤引擎从各个方面进行检查，切断垃圾邮件的源头，可有效防止未授权的邮件进入或发出，阻挡垃圾邮件、禁止邮件转发和防止电子邮件炸弹。它通过消除不需要的邮件，有效降低网络资源浪费，与KShield Gateway的病毒过滤引擎一起，确保企业邮件服务器不受垃圾、病毒邮件的干扰。

多重反垃圾邮件技术

首先，采用了SMTP转发认证。如果用户的RELAY邮件服务器要求MUA进行认证，在引入了KShield Gateway之后，SMTP认证的过程将由KShield Gateway来进行。KShield Gateway会将这一认证过程的数据流重新定向给用户的RELAY邮件服务器，并根据认证的结果来决定是否接收MUA的发信请求。认证的过程完全遵循ESMTP的认证协议标准。

如果用户的RELAY邮件服务器不支持SMTP认证，可以使用KShield Gateway的SMTP认证扩展模块，KShield Gateway有POP3用户和Windows域用户的SMTP认证扩展模块，可以将SMTP认证协议转变为对POP3用户或对Windows域用户的认证协议，这样用户就可以使用KShield Gateway进行发信认证了。增加了SMTP认证功能后可确保只有授权用户才可以使用企业的邮件服务器，大大减少了垃圾邮件的来源。

其次，自定义了垃圾邮件过滤策略。KShield Gateway的垃圾邮件过滤引擎。

冠群金辰 KShield Gateway

支持用户根据邮件的下述信息过滤相关邮件：可以针对信件的主题、信件地址和信件正文、附件名称、收发件人等进行关键字过滤。如信件中包含“促销”、“法轮功”等字样；可以拒收来自某个IP或者网段、域的邮件；可以限制系统总的收信进程数；可以限制对任意IP的连接数；可以限制一封信总的收件人的数目；可以限制每封信的大小；可以自定义垃圾邮件列表，阻塞来自列表中地址发来的邮件。

第三，采用了第三方垃圾邮件列表。KShield Gateway支持全球最大的反垃圾邮件组织MAPS（Mail Abuse Prevention System）提供的anti-Spam数据库，包括RBL（Real Time Black-hole list）、DUL、RSS以及RBL+等，有助于减少对网关的大量邮件的恶意攻击。

“反垃圾邮件六大方案之四”

美国网络联盟 McAfee SpamKiller

McAfee SpamKiller是美国网络联盟于2003年上半年收购反垃圾邮件应用软件供应商Deersoft公司后推出的第一款产品。收购Deersoft公司是美国网络联盟在垃圾邮件和内容过滤技术方面所做众多投资的第一项。

该软件专用于用于微软Exchange Small Business，也是NAI推出的第一款全方位反击垃圾邮件的产品，它可以帮助中小企业用户降低网络风险。它使用预先设置的几百个规则扫描每一个进入服务器的邮件，可主动检测并隔离垃圾邮件。据测试，该产品的误报率小于0.05%。

McAfee SpamKiller使用预先设置的几百个规则扫描每一个进入服务器的邮件进，可主动检测并隔离垃圾邮件，企业员工不必再浪费时间来判断收到的邮件是有效邮件还是垃圾邮件。不适当的内容进入员工收件箱的可能性大大减小，因此企业可以大大减少人力资源、财务和法律方面的责任。

SpamKiller技术使用的是一套非常准确的评分系统，用来判断一个特定的电子邮件是否为垃圾邮件。利用SpamKiller所使用的众多规则，每一个邮件都会得到一个是或否的评定，以确定它是否为垃圾邮件。一旦检测到垃圾邮件，这些邮件就会被发送到终端用户的收件箱、个人垃圾邮件文件夹或系统垃圾邮件文件夹。

McAfee SpamKiller通过使用五种不同的检测方法，McAfee Security为IT管理人员提供了一套主动、全面的解决方案，用来抗击垃圾邮件。

首先是整体分析：检查收到的每一个邮件的标题、布局和结构，并运用数以千计的算法来判断此邮件是否为垃圾邮件。

其次，启发式检测：通过使用一套基于已知垃圾邮件特性的自动规则，SpamKiller可主动出击，确保网络不受垃圾邮件的侵犯。

第三，内容过滤：管理员可设置词和词组，以进一步识别不想要的邮件和不恰当的内容。

第四，个性化的黑白名单：管理员和用户可使用黑白名单来设定一套标准，以判断可接受的邮件发送人和不想要的及不能接受的邮件发送人。

第五，自我调整：由SpamAssassin驱动的SpamKiller可记住桌面机收到邮件的特性，对已知发件人发来的邮件进行总体垃圾邮件评分调整。

也许某人认为是垃圾邮件的邮件可能会对另一个人有用，而这对于SpamKiller也并不是难事，SpamKiller允许终端用户在桌面机上对他们的垃圾邮件设置进行设定和个性化处理，为企业提供一套真正全面的工具，可极大减少垃圾邮件的数量，能够使网络管理员从垃圾邮件的烦恼中解放出来，转而去关心更加重要的IT问题。

“反垃圾邮件六大方案之五”

诺顿特警2004

赛门铁克公司最新推出的诺顿网络安全特警2004（Norton Internet Security 2004）具备较好的垃圾邮件过滤功能。

NIS2004无缝集成防病毒、防火墙、入侵检测、隐私保护、垃圾邮件过滤以及父母控制等多项功能，而具备垃圾邮件过滤功能的就是NIS2004的新成员——Norton AntiSpam 2004，它可以与任何标准POP3电子邮件程序一起工作，并且自动与最新版本的Microsoft Outlook、Outlook Express和Eudora集成，直接从用户的电子邮件收件箱过滤和消除接收的垃圾邮件。

NIS2004通过在邮件的标题前加“Spam”来标识垃圾邮件，这样用户就可以选择删除这些邮件或者自动将这些邮件放到一个指定的文件夹下留待以后处理。这一功能提供了几项设置，首先有一个移动滑块，可以根据

情况调整垃圾邮件的检测级别。它有高、中、低三个档，NIS2004的智能垃圾邮件过滤引擎通过分析往来邮件提高辨别垃圾邮件的能力，降低辨别的错误率，选择越高的级别，那么对邮件的审查也越严格，也就可以更彻底地杜绝垃圾邮件，但是也同时存在将个人邮件当成垃圾清除的可能。

在这种情况下用户就可以配合另一项设置一起保护邮件系统，那就是“允许邮件列表”和“禁止邮件列表”设置，将一些常用的邮件地址添加到允许邮件列表，这样就可以防止邮件被标志为Spam垃圾邮件。接下来就是可以自定义过滤垃圾邮件的规则，例如，包含哪些文字的邮件应该被过滤掉，或不应该被过滤掉，当邮件系统收到包含这些文字信息的邮件后就可以做相应的处理。

此外，诺顿个人防火墙也是NIS2004的重要成员，它不但能够全面防止黑客入侵，使黑客无法在网上看到用户，而且可以检测到隐藏在网络连接中的入侵行为，并根据入侵行为的特征自动采取保护措施，更重要的是它具备在不同的网络接入环境下自动切换安全设置的功能，能够提供随时随地提供防护。

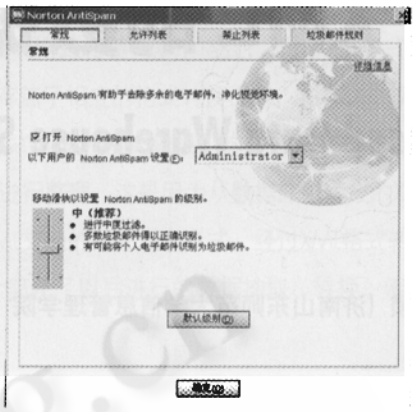

图 诺顿安全特警2004操作界面

“反垃圾邮件六大方案之六”

金山毒霸6“三防一体化”

金山毒霸6是六大方案中唯一没有外资背景反病毒厂商的产品，其提供的反病毒产品在国内个人用户中占有较高的市场份额。2003年12月18日，金山推出国内第一款具有反垃圾邮件功能的杀毒软件“金山毒霸6”，具备防黑、防毒、反垃圾“三防一体化”功能。该产品已于2003年12月20日上架销售，市场建议零售价198元。

在国际上，许多反病毒厂商本身就扮演着反垃圾邮件的角色。但在国内，这一领域还没有杀毒厂商提出成型的解决方案。新推出的金山毒霸6是国内首次提供专业反垃圾邮件功能的商业软件，其模块“邮件清道夫”便是专门对付垃圾邮件的。通过该软件，用户可以轻易设置“邮件规则编辑器”，对自己经常收到的垃圾邮件进行特征提取，比如“发件人”、“邮件标题”、“邮件正文”等。当以后再收到具有该特征的邮件时，毒霸便会将其过滤，或者智能提醒用户该邮件为垃圾邮件。同时，金山毒霸6独有的“a++”算法，使其查杀病毒的速度也非常高。

实际上金山毒霸系列产品一直具有自动过滤垃圾邮件的功能，这次毒霸6则首次加入了对付垃圾邮件的工具——“邮件规则编辑器”。用户可以根据自己经常接收的垃圾邮件的特征，自己编辑制定要过滤的垃圾邮件的规则。如下图：

金山毒霸6同时改良了邮件防毒的功能。除继承了毒霸V的双向快速过滤、严格监控各个通道外加入新的算法，可以快速准确的查杀任何格式的邮件正文以及附件。在表现形式上邮件防火墙加入智能提示的功能，如果通过客户端收取邮件，用户可一目了然的看到收发的邮件的安全程度以及是否为垃圾邮件，并可随时停止监控。

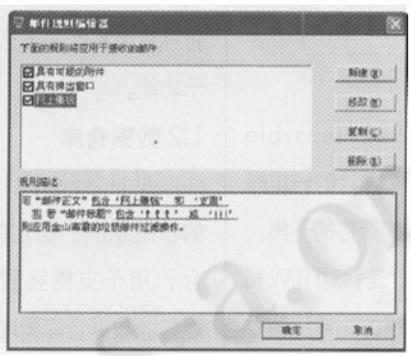

图1 邮件规则编辑器

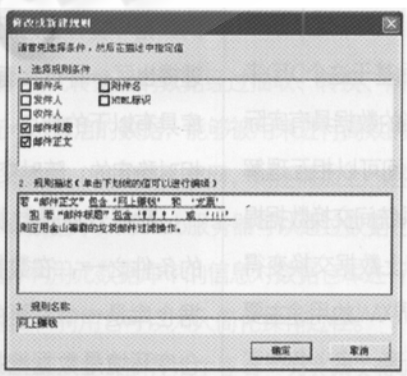

图2 修改或新建规则

图3 随时监控邮件收取