SPAM SQR

垃圾邮件管理专家

产品白皮书

版权信息

商标信息

SOFTNEXT， SPAM SQR，SSQR等标识及其组合是守内安信息科技（上海）有限公司拥有的商标，受商标法和有关国际公约的保护。

第三方信息

本文档中所涉及到的产品名称和商标，属于各自公司或组织所有。

守内安信息科技（上海）有限公司
网站： WWW.SOFTNEXT.COM.CN
地址：上海市长宁区天山路600弄2号新虹桥捷运大厦10楼E座
邮编： 200051
电话： +86-21-51036007
传真： +86-21-62741030
邮件： SNSERVICE@SOFTNEXT.COM.CN

目录

1 背景概述

1.1 垃圾邮件

垃圾邮件是INTERNET技术发展的产物，所谓垃圾邮件多指未经请求而发送的电子邮件，即一些批量发送的未征得收信人同意的电子邮件，从内容上看，主要是商业广告性质或是发财之道的邮件，另有少量政治，团体的宣传邮件，铺天盖地的宣传邮件不仅侵犯了用户的私人空间，干扰了正常使用电子邮件的功能，而且企业大量宝贵的网络带宽被无效的甚至有害的垃圾邮件所拥塞，当垃圾邮件或病毒邮件爆发时，经常用户无法连接互联网，浪费了使用者的时间，甚至许多企业用户的邮箱所收到的正常邮件占所有邮件的不到10%，也就是说有些企业用户处理垃圾邮件的90%以上的时间被浪费。随着现代技术的发达，垃圾邮件的外延也在扩展，包含了病毒、蠕虫、特洛伊木马的邮件也进入了垃圾邮件的范畴，垃圾邮件发送技术、病毒蠕虫的传染技术、各种入侵技术在相互配合、攻城略地。事实上，随着网络防范技术的提高，直接入侵系统已越来越困难，特洛伊木马成为机密泄露的主要原因，而垃圾邮件恰恰是这类恶意程序传播的一个重要渠道和帮凶，许多企业都蒙受金融损失，由此威胁所带来成本，就并非是人力工时成本所能计算的了，企业唯有正视，才能先期避免耗损更大的意外成本。

1.2 反垃圾邮件技术

随着现代技术的突飞猛进，目前市场上反垃圾邮件产品令人目不暇接。通过在自身邮件系统中设计反垃圾邮件功能来抵制垃圾邮件的做法在当前较为普遍，产品种类也非常繁多，但基本上都是建立在内容过滤、智能分拣、行为识别这几大类技术应用上的。内容过滤技术由于需要检查每封信的内容，效率低，而且一旦垃圾邮件的内容变换就无法做到准确拦截，因而是属于已快被淘汰的老技术了。智能分拣技术虽然对垃圾邮件的拦截率非常高，但前提是需要大量用户投票确定垃圾邮件定位成立，用户量、投票量越大，对垃圾邮件判断才能越准确。一定量的投票后才能拦截，不能提前预防。所以投票的邮件少或垃圾邮件内容变化，都会影响抵制垃圾邮件的效果。行为识别技术是一种分析邮件发送者特征来提高垃圾邮件分辨率的智能技术，如对发信者是否不断变换主题、是否不断变换发信人等异常行为来判定它是否是垃圾邮件，这样做可极大提高垃圾邮件的处理速度，并节省大量的系统资源和网络带宽。行为识别技术可谓是当前抵御垃圾邮件最经济、最有效的工具。

为了有效地拒绝来自恶意的垃圾邮件来源站点和或被利用的垃圾邮件来源站点所发来的垃圾邮件，最直接和有效的办法就拒绝该来源的连接，即在邮件服务器端直接将垃圾邮件屏蔽掉，这样不仅用户不会受到垃圾邮件的骚扰，而且服务器可以减少邮件的处理量，节约处理器资源和带宽大流量。

目前最流行和最有前景的是实时黑白单（REALTIME BLACKHOLE LISTS,简称RBL），通

常该技术通过DNS方式实现，通过查询方式来查找一个IP 地址的A 记录是否存在判断其是否列入了该实时黑名单中。故该名单的权威性和可靠性就依赖于该提供者。通常多数的提供者是比较有国际信誉的组织，故对于该名单来说还是可以信任的。但只通过这种技术并不能完全解决垃圾邮件的问题，在反垃圾邮件产品中还有极为重要的技术是邮件过滤技术（MAIL FILTER），邮件过滤按照邮件系统的角色结构可以分为3类：MTA（邮件传输代理）、MDA（邮件递交代理）和MUA（邮件用户代理），MTA过滤是指在会话过程中对会话的数据进行检查，对于符合过滤条件的邮件进行过滤处理；MDA过滤是指在本地或远程进行递交时进行检查，对于符合条件的邮件进行过滤处理。MTA和MDA过滤都是邮件服务器端的过滤，而MUA过滤是邮件用户的客户端的过滤。邮件过滤作为一个有效的对抗垃圾邮件的手段，就如同杀毒软件对病毒的查杀一样，也是需要不断根据情况更新邮件过滤规则的，通常需根据垃圾邮件监测情况来更新过滤规则。

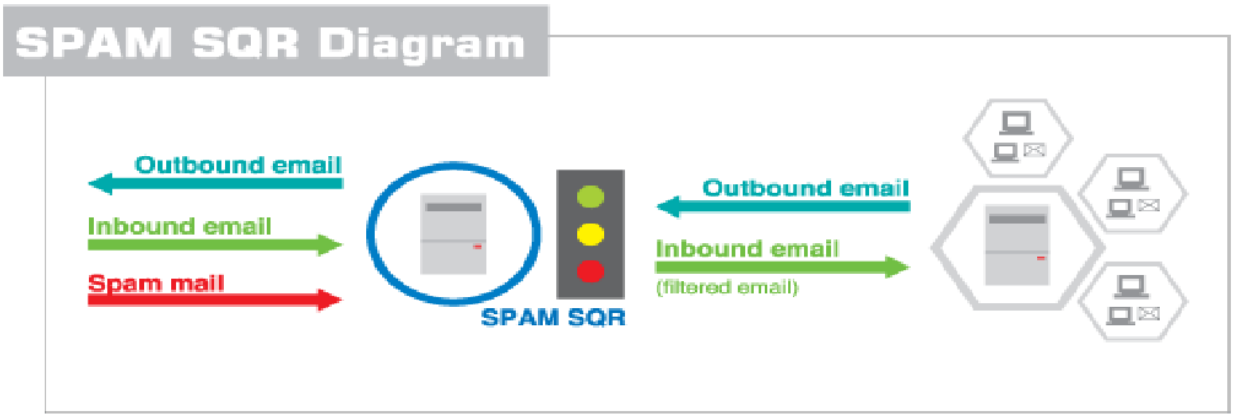
2 SSQR 产品介绍

2.1 产品概述

SPAM SQR 是一款强大的垃圾邮件阻绝系统，与 ASRC 垃圾讯息研究中心技术合作，透过 ASRC 回馈新型垃圾信特征，主采用 N-TIER 层过滤技术对垃圾邮件进行侦测过滤机制，可有效减轻企业邮件服务器负担，提供 27 类垃圾邮件关键词过滤字库，并搭配 SPAM SQR 自动学习过滤引擎，以及独特的垃圾邮件特征加权比对，能精准防堵各类垃圾邮件，可有效提升企业阻挡垃圾信的成效，亦可根据不同群组设置不同邮件过滤策略，提供 MYSPAM 个人化服务，使用者可自行过滤类别调整，以及个人黑白名单管理，方便企业各类人员的使用。

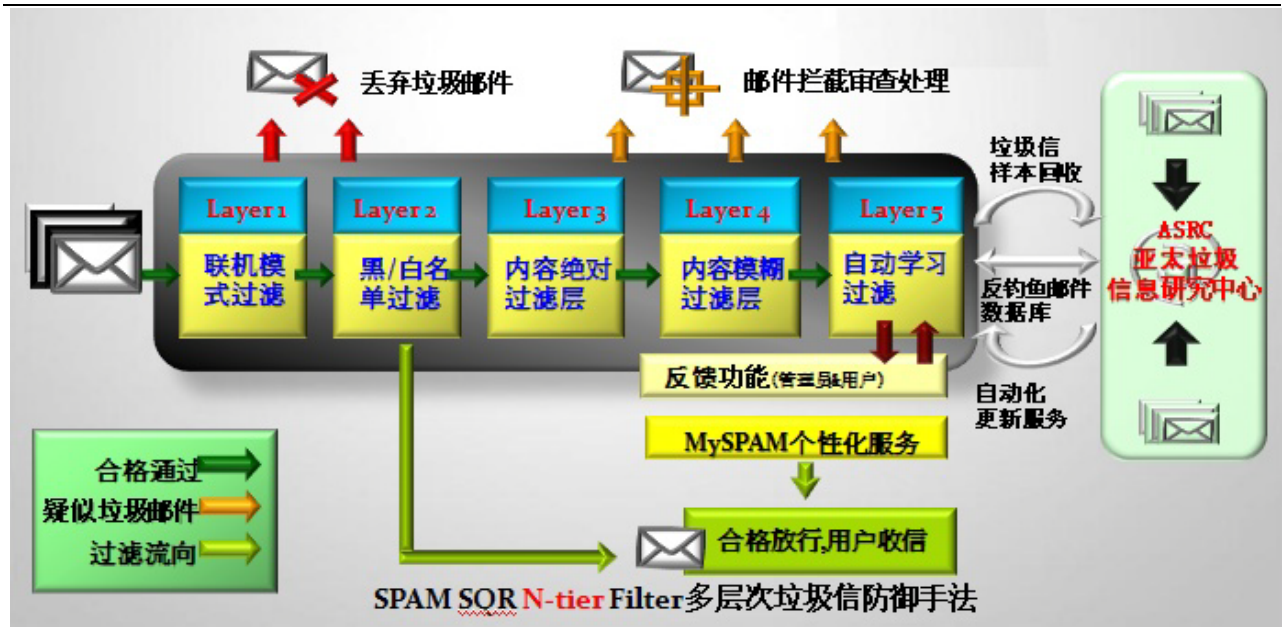
2.2 系统架构与产品特色

2.2.1 系统架构



在企业邮件服务器收邮件前，SPAM SQR运用N-TIER多层过滤技术，多元拦截服务模式，搭配MYSPAM个人化服务，高效率阻挡垃圾邮件。可有效协助企业减少垃圾信件对于频宽、邮件服务器及MIS人员的负担，是系统管理员及使用者双赢管理的最佳ANTI-SPAM系统。

2.2.2 产品特色



全效性N-TIER过滤技术，垃圾邮件一网打尽

SPAM SQR进行邮件过滤可支持多种编码(UNICODE)，并提供简体中文、繁体中文、英文、日文..等多种常用语系的操作界面。SPAM SQR所采用的N-TIER过滤技术包含联机模式过滤、黑/白名单过滤、内容绝对过滤、内容模糊过滤…等严密侦测，其中运用数十万笔特征比对规则，依垃圾邮件行为特征提供绝对黑特征(伪造发件人检查、异常邮件标题、主题夹带乱码检查、纯图片连结无内容检查)及模糊灰特征(超级链接侦测分析、拨接式浮动IP地址)..等侦测过滤机制，并能进行智能型调整误判率。搭配SPAM SQR独特的垃圾邮件的内容过滤比对数据库，及自动学习过滤引擎，大大提升企业阻挡垃圾邮件的成效。

- 多元化拦截服务模式，满足企业管理需求

SPAM SQR 提供分级标记传送模式、垃圾邮件拦截模式..等多元化服务，企业若偏好无痛式导入经验，可采用分级标记传送模式。企业若采用垃圾邮件拦截模式，可明显免除垃圾邮件的骚扰，被过滤的垃圾邮件会被暂存在拦截区，搭配定时发送的MYSPAM拦截明细通知，可检视邮件内容以进行删除、复原重送或加入个人黑白名单。另外，还提供弹性化指定明细派送服务，弹性管理更方便。

- 群组到个人的参与式策略管理，兼顾垃圾邮件管理差异认识

提供全公司各群组或部门的账号及邮件过滤条件设置，可以快速浏览或调整过滤类别，利于实施部门差异化的垃圾邮件过滤管理策略，还能弹性设置群组人员使用MYSPAM个人化服务的功能，可满足部门到个人对垃圾邮件的认知差异，落实邮件自主管理。

- MYSPAM个人化服务，落实个人邮件自主管理，安全分级管理有效率

从使用权限管理、MYSPAM拦截明细通知、到MYSPAM个人化服务 (WEB界面)，SPAM SQR提供一系列个人化的贴心服务机制，包含使用者自选浏览语系、风险分级拦截明细列表、个人

黑白名单管理、过滤类别调整设置、简易个人邮件备份及复原..等服务。使用者可自行切换浏览界面的语系(提供简体中文、繁体中文、英文、日文..等)，浏览个人的邮件拦截记录时，MYSPAM会贴心地会依照低、中、高的风险指数，来分级显示拦截明细，还能显示被黑名单封锁的邮件，使用者可以进行重寄邮件，或依个人需要将发件人加入黑、白名单。MYSPAM可为使用者创造弹性及服务加值的管理成效。遇有个人计算机硬盘毁损导致电子邮件遗失时，MYSPAM更可提供个人邮件备份还原的贴心功能。

- 邮件管理透明化，有助于系统管理体检

进入SPAM SQR系统首页时，会显示实时流量统计图及系统状态报告； SPAM SQR内建邮件系统

体检的相关功能，如邮件记录的数据显示、联机错误统计、查询传送纪录、邮件队列、丢弃纪录、使用纪录…等，MIS人员利用这些服务工具，就能检测邮件系统运作状况，提高邮件服务的稳定性及安全度。

.

- 多元化统计报表，ANTI-SPAM及EMAIL管理成效一览无遗

SPAM SQR提供各项统计信息，如统计报表、拦截比例统计、邮件分类统计、人员排名、发件人来源统计、IP来源统计、重寄邮件统计、阻挡统计、联机错误统计..等多类报表，同时提供报表导出及打印的功能，让MIS人员及经营者能掌握邮件管理的成效。

- 支持扩充性高，持续进化的专业ANTI-SPAM系统

随着垃圾邮件的进化，SPAM SQR的防御机制也具备高扩充性，可支持ANTI-SPAM新技术(DOMAINKEYS、SPF..等)。针对集团性或跨国性企业庞大电子邮件管理，SOFTNEXT推出SPAM SQR的MULTI-WAY整合服务，透过分流过滤、异地备援、账号／数据同步传输、及分布式系统分工及运作架构模式，协助集团或跨国企业能兼顾系统最佳效能，并有效防御大量垃圾邮件。

2.3 功能描述

- 多层次垃圾信过滤系统
- 定时自动寄发拦截明细功能
- 可根据不同群组设定不同邮件过滤策略
- 完整的邮件纪录、拦截邮件查询功能
- 垃圾信拦截自动分类、自动学习功能
- 交互式回报功能
- 完整的统计图表
- 垃圾邮件自动学习引擎

2.3.1主要功能

2.3.1.1联机模式过滤层

- DOS防御：
  - 可针对大量邮件攻击及大量联机数攻击进行安全防御，可限制某一IP来源瞬间联机的连机次数，自动的将大量发送的邮件来源断绝，以避免遭受垃圾邮件发送商或黑客以大量邮件联机进行攻击，DOS防御也可设定排除该信任IP。
- 不当网域阻绝
  - 可锁定不当发信的来源IP，并将该网域寄来的邮件进行丢弃，以节省邮件服务器收垃圾邮件所浪费的频宽。

2.3.1.2 黑/白名单过滤层

- 黑白名单过滤
  - 支持实时RBL名单过滤数据库，并提供管理者设置寄件人或IP的黑名单，后续会丢弃黑名单邮件。
  - 允许建立白名单(经防伪检测)，以允许接收合作厂商或可信赖的寄件人的来信，有利提升收信效率。
  - 并提供陷阱EMAIL，有效防御字典档攻击。若邮件发送至陷阱EMAIL，系统会自动将该邮件的寄件人、主题、IP加入过滤条件中，以让后续相同特征的邮件被拦截。

2.3.1.3 内容绝对过滤层

- 过滤条件：
  - 用于阻挡已知明显待征的垃圾信，或是用以特定的规则，筛选出特定的信件。
  - 可按各群组的角度设置此过滤条件，以进行不同群组过滤条件过滤。
- 垃圾邮件行为待征过滤
  - 依垃圾邮件行为特征提供绝对黑特征(伪造发件人检查、异常邮件标题、主题夹带乱码检查、纯图片连结无内容检查)及模糊灰特征(超级链接侦测分析、拨接式浮动IP地址)..等侦测过滤机制，并能进行智能型调整误判率。

- ASRC垃圾信息研究中心
  - ASRC垃圾信息研究中心为一专门研究垃圾邮件动态的单位，该中心定时释出垃圾邮件相关特征及过滤数据库，以供SPAM SQR实时更新其内部判断机制，实时防堵多变的垃圾邮件。另透过长期搜集的资料、语意仿真、陷阱账号所收集的样本，产生更新的数据库以强化SPAM SQR的反钓鱼诈骗的功能。

2.3.1.4 内容模糊过滤层

- 自动学习引擎过滤
  - 依自动学习过滤引擎进行垃圾邮件及正常邮件的大量训练，并可配合样本邮件的投寄，新增到自动学习引擎，以进行持续性修正训练，有利于分辨过滤垃圾邮件及正常邮件。

- 关键字设置
  - SPAM SQR 提供了独创的27类垃圾信内容关键过滤字库，以关键词比对的技术来判定该邮件是否为 垃圾邮件。扫描垃圾邮件主旨与内容，并比对关键词的权值计分，以判定垃圾邮件的类别进行隔离， 亦提供企业自定过滤的类别及建立关键词。

2.3.2多元化，安全分级管理

- 群组设置
  - 提供企业内群组人员的账号设置，将企业内部的邮件账号依照需求进行分群，以配合其它功能设置不同群组的不同垃圾邮件处理策略，并能依群组内成员的管理需要，进行开关个人化服务设置，以弹性代替单一策略僵化E-MAIL的应用。

- 策略管理
  - 提供群组或部门的过滤条件设置一览表，可快速浏览并调整过滤设置。使用MYSPAM 个人化服务时，使用者可自行开启过滤类别及调整敏感度。

- MYSPAM个人化服务
  - 提供个人化服务（含拦截明细通知、接收正常邮件信箱，个人化过滤策略管理、个人化黑白名单），使用者可自行切换浏览接口的语系（提供简体中文、繁体中文、

英文、日文……），浏览个人的邮件拦截记录时，MYSPAM可依照低、中、高的风险批数，来分级显示拦截明细，还可显示被黑名单封锁的邮件，使用者可进行重寄邮件，或依个人需要将发件人加入黑、白名单。

2.3.3透明化的邮件管理

- 邮件记录
  - 可针对所有往来的邮件进行记录（记录寄件人，收件人，主题，联机IP，处理状态……），以方便管理员查看，可显示邮件的详细数据，以辅助侦测异常邮件流。提供近期邮件备份机制，预设支持大型数据库切割管理，以确保执行及查询效能，亦可复原之用。同进可进行自动学习引擎的样本投寄，转寄新型垃圾邮件给ASRC进行特征研究。

- 邮件拦截
  - 流进的邮件若符合过滤条件及超出验证值的邮件分开放置在各拦截区，邮件拦截区提供分群组显示拦截的邮件，管理员可根据自己的需要进行邮件查询，以便进行重送、转发、删除等，被置于拦截区的邮件，亦可搭配MYSPAM拦截明细通知服务，以加速处理拦截邮件。

- 用户反馈
  - 用户回报功能可回报SPAM SQR漏拦或误拦的邮件，并提供全自动将回报自动训练功能，管理员可自行分别决定是否启用垃圾信或正常信的自动训练功能，方便了管理员针对使用者的回报能做快速的反应及处理，亦搭配个人化使用回报SPAM和NOT SPAM，以利速修证引擎。

- 邮件回收
  - 可将未被拦截的垃圾邮件寄回SPAM SQR，管理员依照这些邮件进行测试，并参考测试结果，进行关键字的调整设置。

2.3.4 统计功能

- 统计报表
  - 可依日、周、月指定时间区间检视群组及个人的流量大小、邮件封数等统计数据。
  - 可依日、周、月指定时间区间检视群组及个人的一般邮件、拦截邮件、总流量等统计数据。并可提供所有人员或单一群组内人员的排名。
  - 可依日、周、月指定时间区间进行分类过滤字库、寄信来源、重寄邮件、DOS联机次数等统计数据。
  - 全体报表皆有完整打印、汇出、寄送功能，并可新增多笔排程自动寄送报表。

2.3.5 VIRUS SQR防毒模块（选购功能）

- 病毒隔离
  - 整合防毒功能，并可和其防毒系统的病毒拦截功能，可对病毒邮件进行彻底拦截，可有效防堵病毒、蠕虫……等恶意程序。
  - 提供防毒资讯及设定、病毒隔离、病毒统计报告……等功能。
  - 可发出病毒拦截通知给系统管理员、收件人、寄件人。
  - 对放至隔离区的病毒邮件可进行删除后寄出，直接删除亦或清除病毒后自动送出……等功能。
  - 可自动将含有病毒邮件的备份档清除。

2.3.6标准LDAP账号整合

- **LDAP**同步账号
  - 整合标准LDAP同步账号EMAIL群组账号资料,减轻管理员的负担,可方便进行分组管理,亦可进行SMTP认证,并搭配SPAM SQR可有效防堵以字典攻击防御效果。

- SMTP代理认证
  - 可使邮件服务器不直接暴露在外部，以避免绕信攻击及遭受垃圾邮件的轰炸，而且不影响内部人员在外部发信。

2.3.7 备份机制

- 邮件备份设置
  - 可支持本机备份邮件，亦支持远程备份，即将本机的邮件备份至远程主机，以便日后查看，复原。
- MULTI-WAY异地备援（选购功能）
  - 以标准架构增加一台异地过滤器，可达到异地备援的效果。配合使用单位异地备援的第二建置点设立，增加一台FILTER作为主建置点的备援机制。第二建置点的数据亦会同步汇整至REPORT & STORAGE SERVER。
  - 标准的二层式架构，将负载均衡分散。适用于多收信DOMAIN或流量大须分流管理的使用单位，以两台SPAM SQR作为分流备援架构，将资料同步汇整至统计报表主机。若需从简架构，亦可将报表主机与SPAM SQR 1并为一台主机，以SPAM SQR 1作为邮件主要接收网关，SPAM SQR 2作为分流备援，而将数据集中存放在SPAM SQR1，以便统一管理。

3 典型应用

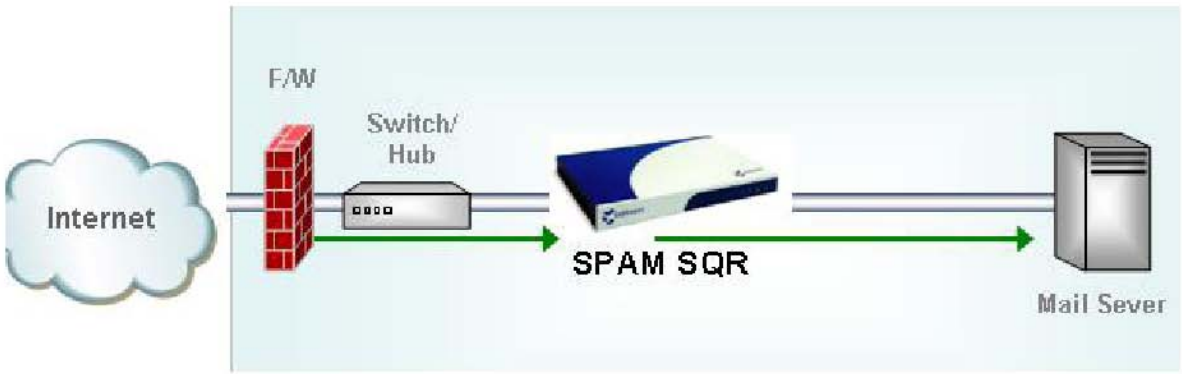
3.1 政府金融应用

◆ 概述

透过电子邮件传播的病毒在现今社会已不在陌生了，除了大量发送造成邮件服务器瘫痪外，这类不必要的病毒邮件也被视为垃圾邮件的一种。至于PHSHING（网络钓鱼）的运作模式，多半是透过一封不请自来的伪造电子邮件，同时搭配一个假冒的网页（多半是金融服务的相关网页），以骗取受害人的账号、密码等敏感信息；或是利用电子邮件以高效投资、灾难、疾病等理由，骗取资金或捐款等。这样的诈骗模式由来已久，但近两年来有暴增的趋势，光是2003 年美国就有200 万成人曾遭到这样的诈骗，不仅是收到PHISHING 诈骗邮件的人遭受损失，许多被假冒的企业也必须担负起赔偿受害人的责任，就因为无论个人或企业都蒙受金融损失. 通过使用这套系统可以有效的防范和消除这些威胁，降低信息安全风险、有效利用网络频宽资源,大大减少金融损失。

◆ 部署

通过使用SSQR的标准模式部署，部署拓扑见下图。所有邮件均通过SSQR进行层层过滤后转发，从而可有效阻挡不当垃圾邮件及病毒邮件。



◆ 效果

- 可有效避免遭受垃圾邮件发送商或大量黑客的联机攻击。
- 可对大量不法联机数攻击进行安全防御。
- 可有效减轻内部邮件服务器的负担。
- 可有效防堵病毒、蠕虫……等恶意程序攻击。

- 可有效防御字典档攻击。
- 提供过滤条件设置及关键字设置，有效阻挡各类垃圾邮件。

3.2 企业应用

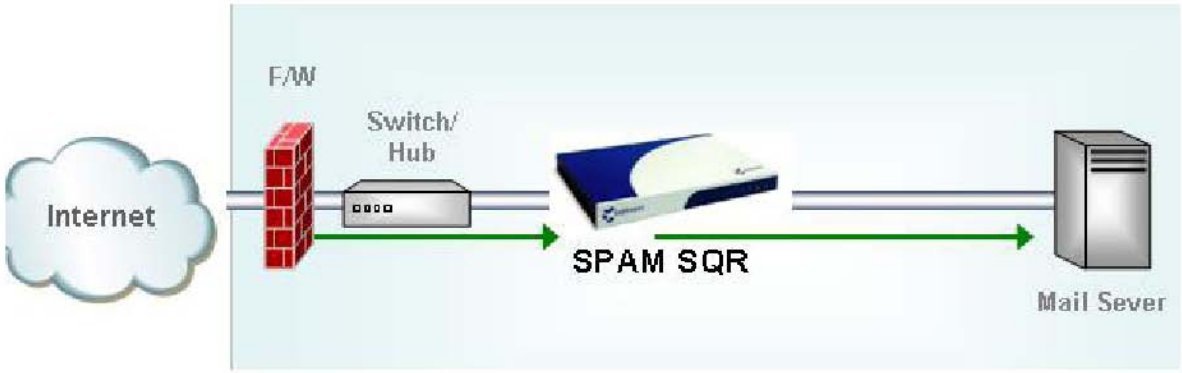
3.2.1 中小型企业应用

◆ . 概述

垃圾邮件对现在网络知识分子来说，已经不再是陌生的名词，据联合国组织机构国际电信联盟指出，全世界80%的电子邮件是垃圾邮件，几乎每一位电子邮件的使用者都曾遭受过垃圾邮件的骚扰。垃圾邮件的日益泛滥，不仅造成困扰、时间成本的浪费，对多数企业来说，影响所及就不只是觉得麻烦或讨厌，这些垃圾邮件对企业是会造成具体的损失。THE RADICATI GROUP 在2003 年的一份报告中指出，未来四年内垃圾邮件将带给欧洲企业850 亿欧元的损失，并且更进一步预测，垃圾邮件若不进行有效管束到了2007 年，全球企业因垃圾邮件所造成的损失将暴增至1980 亿美元。为此，如何防范垃圾邮件所带来的困扰，提高生产时速，是企业首当考虑的问题。

◆ 部署

通过使用SSQR的标准模式部署，部署拓扑见下图。所有邮件均通过SSQR进行层层过滤后转发，从而可有效阻挡不当垃圾邮件。



◆ . 效果

- 通过N-TIER层过滤技术，能精准防堵各类垃圾邮件。
- . 提供27类垃圾邮件关键字过滤字库，各类垃圾邮件一拦无遗。
- 独特的垃圾邮件特征加权比对，漏拦邮件微乎其微。
- . 提供自动学习过滤引擎，提升企业阻挡垃圾邮件的成效，使垃圾邮件无处遁形。
- 可针对企业收信的内容，设置特定条件的过滤规则，可有效阻挡垃圾邮件。

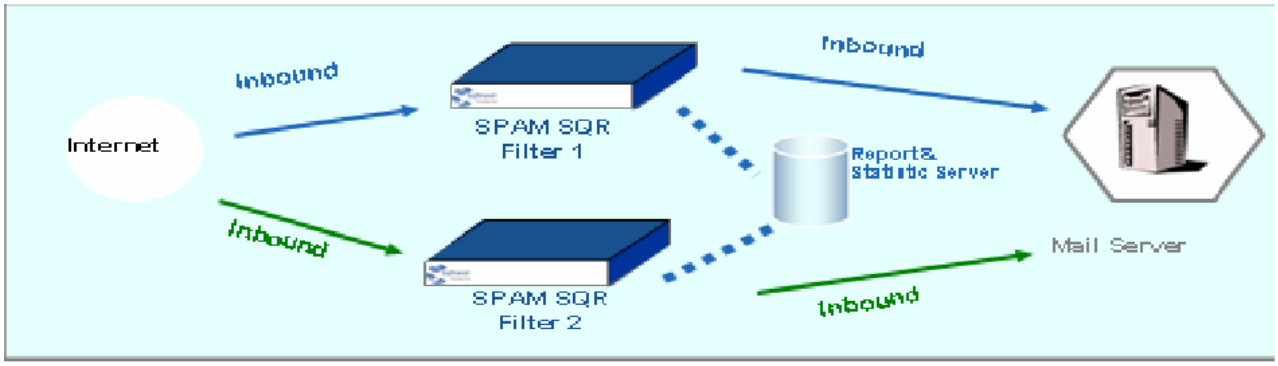
3.2.2 大型企业应用

◆ 概述

随着企业规模的不断成长，除了如何有效地防堵各类垃圾邮件外，许多企业的电子邮件往来都面临了大流量的问题，单一邮件服务器处理庞大的信件流可能导致效能的低落及漫长的处理时间，而且当发生问题时还可能导致电子邮件系统瘫痪，面对如此大的信件流，如何提升系统的运算效能；面对如此大的信件量，如何有效地分散因意外或天灾造成资料遗失的风险，亦是企业首当考虑的问题。

◆ 部署

通过采用SPAM SQR的MULTI-WAY整合服务，部署如下图。透过分流过滤、异地备援、账号/资料同步传输、及分布式系统分工及运作架构模式，协助集团或跨国企业能兼顾系统最佳效能，并有效防御大量垃圾邮件。



◆ 效果

- 分流过滤，提高邮件高速的处理能力，宿短时间，减轻邮件服务器的负担。
- 多服务器同步工作，提高效能，可避免资料分散及停机的风险。
- 良好的异地备份功能。
- 可将账号/资料采用同步功能，提升系统远算效能，亦降低MIS人员的管理负担。
- 通过N-TIER层过滤技术，能精准防堵各类垃圾邮件。

4 服务承诺及服务体系

SSQR垃圾邮件过滤管理专家产品提供如下服务：

1、整机一年有限保修

自购买之日（以正式购货发票日期为准）起，产品和附件免费保修一年，具体内容如下表。

部 件 名 称	保修期限	服 务 方 式
SPAM SQR 垃圾邮件过滤管理专家	一年	报修后 0.5 小时内响应，8 小时给出解决方案，上门服务
电源线、数据线等随机附件	一年	自购买日期起一年内，凭故障原件更换，提供寄送服务，不提供上门服务
用户手册，随机光盘	三个月	自购买日期起三个月内，凭故障原件更换，提供寄送服务，不提供上门服务

2、维护时间

维护时间为星期一至星期五上午九时至下午六时工作时间（不含法定节假日）。

3、联络窗口

我方指定固定的联络窗口，包括人员电话和 EMAIL

4、 服务范围

1) 我方提供电话咨询以及在取得用户同意下进行系统远程登录维护。
2) 我方提供非因硬件毁损或用户操作不当或自行修改系统功能或其它外力因素导致系统瘫痪的维护服务。
3) 若无法以远程登录维护方式进行问题排除，用户得向我方提请到场服务需求，我方应于接到用户请求后于八个工作小时内指派专人到场维护。我方并应于八个工作小时内修护完成；如我方无法于规定时间内修护完成者，我方应提供紧急旁路操作处理，使用户能正常作业。如因用户要求于服务时间外维护，则安装一般收费标准收取费用。

A) 到场服务原则为：

ⅰ. 用户因正常操作而产生系统故障。

ⅱ. 非用户自行以系统管理账号登录系统修改产品功能导致故障。

iii. 非用户产品安装环境因素，包括：电源供应、空调、搬移产品而导致故障。

iv. 非遇地震、火灾、水灾等天灾或不可抗力的因素导致故障。

v . 非我方或用户之第三者侵入系统且责任归属于我方系统功能所导致系统故障。

vi. 因用户系统软件功能无法运作并且无法以远程的方式进行维护。

B) 我方可应用户要求，提供架设备份机的旁路紧急处理方式，但需由用户提供硬设；我方仅提供后备系统架设，不包含原系统已载有的数据库或系统设置数据移转到后备机，亦不在原系统恢复正常运行后将后备机数据库移转至原系统。

C) 需求确认单的人员签名须为已规范的用户联络人员，如签名资料不符，请加盖公司章；如不符信息安全流程，我方可拒绝用户请求。

4) 由我方提供版本PATCH更新。

5) 如有更改系统设置或修正，经用户向我方提出需求确认单后，我方才可以依据用户的请求作设置修正。该需求确认单的人员签名须为已规范的用户联络人员，如签名资料不符，请加盖公司章；如不符信息安全流程，我方可拒绝用户请求。

6) 系统维护保修期一年年满后，用户可以向我方提出签订维护合约需求。维护价格以产品购买价格的15%为限，具体价格以签定维护合约时再议（如系统维护到期后不购买后续维护，我方将不提供版本升级及产品维护等）。