Rich Firewall 反垃圾网关

产品白皮书

修订时间：2022/12

版本：V5.0.0

免责声明

本文档仅提供阶段性信息，所含内容可根据产品的实际情况随时更新，恕不另行通知。

文档更新

本文档于 2022 年 12 月最后修订。

A、 文档修改记录

版本	修改日期	修改人员	修改记录
V4.0.3	2016/10/31	王启铭	反垃圾网关产品 V4.0.3
V4.0.3	2019/06/18	孔祥立	更新文档说明以及图片替换
V5.0.0	2022/12/27	陈祥海	更新文档

B、 文档审核记录

版本	审核日期	审核人员	审核记录

目 录

1 产品概述

1.1 需求背景

随着互联网的蓬勃发展，电子邮件已经成为互联网上最普遍的通讯方式。中国是世界垃圾邮件大国之一，最新调查显示 2013 年第一季度垃圾邮件占比为 66.55%。作为因特网中最具有争议的副产品，垃圾邮件对于企业邮箱用户的影响首先就在于给日常办公和邮箱管理者带来额外负担。根据不完全统计，对于中国多数企业邮件应用仍处于低效率反垃圾环境的情况下，有 80%的用户每周需要耗费 100 分钟左右的时间处理垃圾邮件。

垃圾邮件的恶意投送，还会大量占用网络资源，使得邮件服务器 85%的系统资源在用于处理垃圾邮件的识别，不仅资源浪费极其严重，甚至可能导致网络阻塞瘫痪，影响企业正常业务邮件的沟通。更严重的垃圾邮件问题甚至不仅只是影响企业工作效率，甚至会祸及整个服务器。

针对这一现象，市场上很早就开始出现各种各样的反垃圾反病毒网关产品，但这些产品的产品力却并不能让企业级的用户满意。数据安全性差、垃圾邮件拦截率低、防病毒攻击能力弱、管理和协同不方便、操作界面繁琐不友好、无法与企业其他系统配合使用、无法为企业提供提升品牌形象的自定制化服务、售后、升级服务得不到及时响应造成损失等诸多方面，因而急需更专业的反垃圾反病毒网关产品来向企业级客户提供服务，帮助企业保护自身数据安全，免受病毒攻击；拦截垃圾邮件，进一步提高企业的内部沟通管理效率。

1.2 产品介绍

Rich firewall 反垃圾网关是目前市场上技术最成熟的反垃圾邮件解决方案，在安全性上，采用了二十多种世界领先的邮件安全技术，七层过滤机制，垃圾邮件过滤拦截率超过

99.7%，基于 139 邮箱 8.5 亿用户垃圾特征库实时向客户提供反垃圾服务，目前市场上反垃圾能力最强；在功能性上，Rich firewall 反垃圾网关为企业提供成熟的权限管理体系，平台采用全新的扁平化设计，简约大气的设计风格，极大的提高了用户的操作体验；在安装部署方面，采用一键安装、分布式部署，支持标准的开放 API 对接企业现有系统，同时提供企业自定制化服务。

Rich firewall 反垃圾网关目前服务的客户分布在政府、通信、金融、能源、集团型企业、教育科技等各个行业，典型的有深圳市电子政务资源中心、中国移动、南粤银行、南方电网、神华集团等，积累了丰富的针对各行各业的部署经验，拥有完善、成熟的行业化解决方案。

目前彩讯反垃圾邮件的产品形态为两种：Rich Firewall 独立网关与 Rich mail 邮箱系统附带网关。

2 产品定位

Rich firewall 反垃圾网关(Rich Firewall)是一款为企事业单位邮件系统提供最安全高效稳定的反垃圾、反病毒邮件技术的企业级安全管理软件平台。

2.1 应用价值

企业时刻都在产生大量的邮件往来，而除了正常邮件以外，也时刻遭受着垃圾邮件的侵扰。对于企业而言，垃圾邮件的泛滥有可能带来严重的损失，某一个员工收到病毒邮件而导致全公司的网络瘫痪，员工需要花费额外的精力来处理邮件，除了造成一些不必要的资源浪费，更有可能导致企业整个服务器的崩溃与机密数据的泄露。

- **恶意攻击**：邮件服务阻塞、不稳定，甚至宕机；
- **病毒邮件**：借垃圾邮件传播病毒、阻塞网络与邮件服务器；

- **垃圾邮件：**消耗系统资源，浪费用户的时间，进行网络诈骗；
- **政治邮件：**散布非法信息，如“金融危机”、“房产崩溃”等引起社会动乱敏感内容的邮件；

针对企业的上述问题，Rich firewall 反垃圾网关使用多项反垃圾邮件的新技术，包括 RBL、SPF、Bayes、图片 SVM 过滤、邮件指纹过滤、智能邮件特征评分机制、实时规则库更新等，经过多层次优化，来实现对垃圾、病毒邮件的高效拦截，对邮件系统的稳定防护。

2.2 目标行业和客户

对 Rich firewall 反垃圾网关(Rich Firewall)有强烈需求的客户主要集中在以下三大行业群：

- **海外贸易、进出口业**

代表：外贸公司、物流公司等

由于地理位置因素，电子邮件无疑是此类行业进行工作沟通的重要手段。而恰恰在跨区域、跨国际的环境中，最容易受到垃圾邮件的侵扰与病毒邮件的攻击，严重影响与客户之间的交流，所以需要网关系统来保证邮件系统的安全与流畅。

- **企事业单位**

代表：政府、国企

企事单位与民生息息相关，因此对于内部的邮件管理极为严格，对网关产品的安全性、稳定性有严格的标准

- **软件和信息技术服务业、广告业**

代表：软件开发公司、广告创意公司

此类公司在内部的收发邮件中包含大量关于公司核心产品的机密信息，如果收到攻击导致机密泄露或被偷取，将会为公司带来不可估量的损失。要求对病毒邮件有极高的防护性能。

3 产品系统架构介绍

3.1 技术架构

本产品通过采用模块化设计、分布式部署、分层式架构，保证了产品服务高安全性、高稳定性、高可用性。

- 过滤层： 实现邮件反垃圾过滤检查；
- 接口层：提供 SMTP 协议 API 接口、过滤保护及负载均衡；
- 管理层：实现运维管理、规则更新、用户控制等；
- 硬件配置：

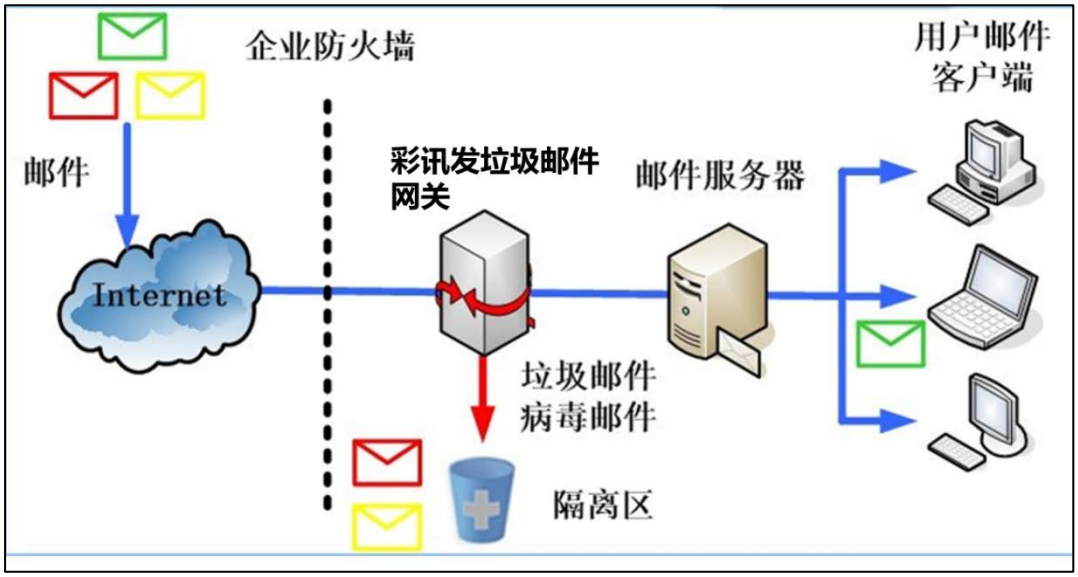
服务器名称	建议配置	部署软件说明
企业业务服务器	X86 系统/双路 8 核 CPU/16 G 内存/500G 硬盘	网盘管理中心 用户平台 认证中心
数据库服务器	X86 系统/四路 16 核 CPU/32 G 内存/500G 硬盘	Mysql 数据库
存储服务器	X86 系统/四路 16 核 CPU/64G 内存/1T SAS 10K 硬盘	分布式存储系统

- 操作系统

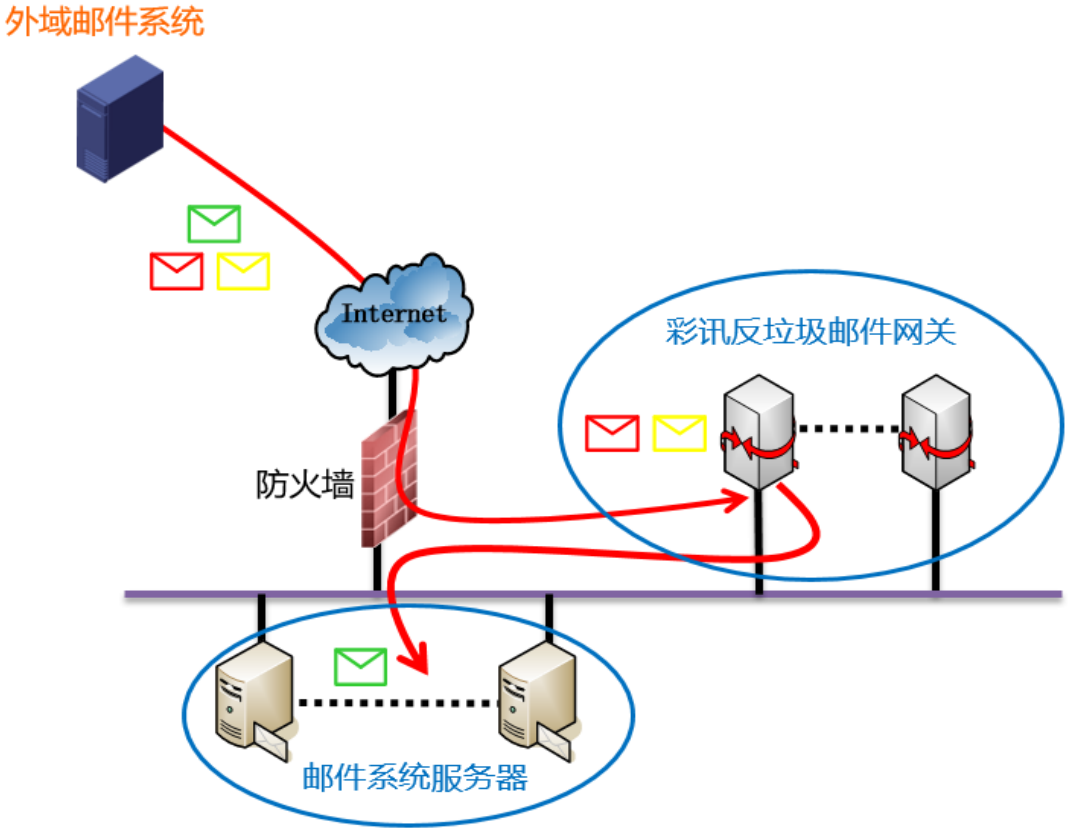
Redhat6.5 LINUX 6.5 企业版操作系统

- 产品部署图

中小企业（用户数量 5000 以内）：自动检查和隔离垃圾邮件和病毒邮件，根据关键字，自动检查和处理特定邮件。

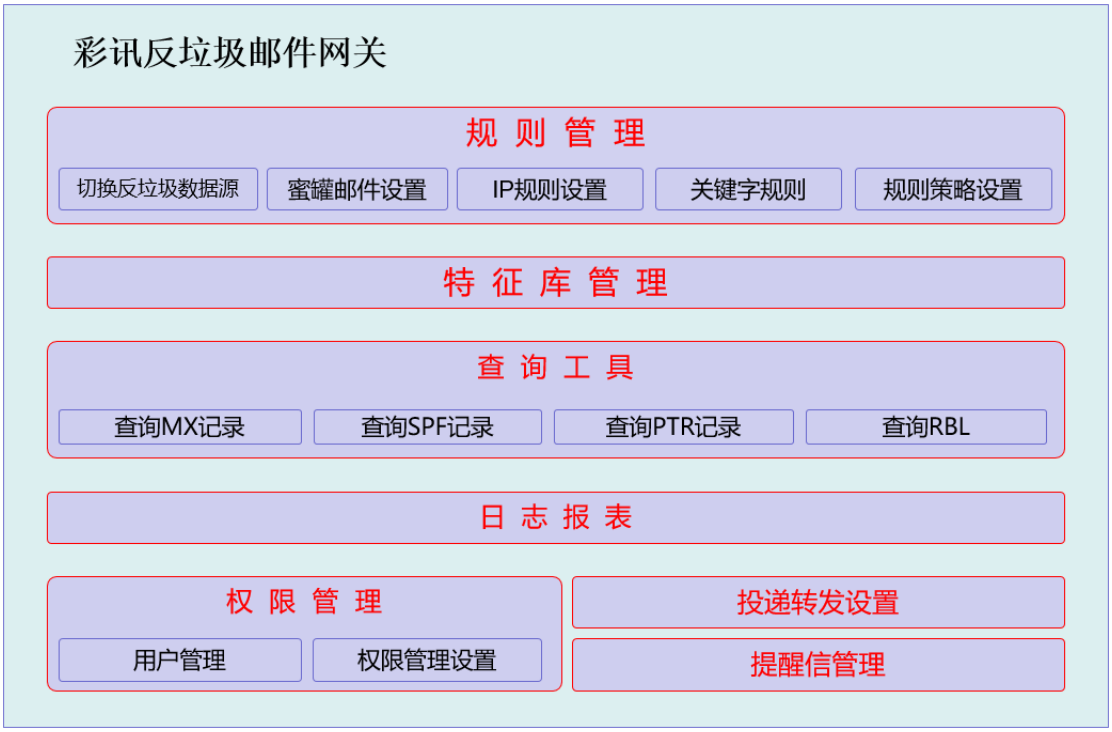


大中型企业（0.5 万~10 万）：采用多台反垃圾邮件网关设备进行双机热备与负载均衡，这种部署可以为邮件系统安全提供业务连续性保障，避免单点故障造成邮件系统瘫痪。



3.2 软件架构

Rich firewall 反垃圾网关（Rich Firewall）管理平台，功能架构如下：



- **Rich firewall 反垃圾网关**

Rich firewall 反垃圾网关的产品形态为：Rich Firewall 独立网关与 Rich mail 中的附带网关，同样使用 sophos 杀毒引擎，共享垃圾病毒库。而 Rich Firewall 独立网关除了更高的杀毒反垃圾性能外，增设了更多专业、个性化功能模块。

Rich firewall 反垃圾网关主要分为：规则管理、特征库管理、日志报表、投递转发设置、提醒信管理、权限管理（独立网关特有）、查询工具（独立网关特有）这七大主要功能模块。

其中：

规则管理包含：

数据源管理（独立网关提供 smtp/out 双数据源切换，收、发邮件双规则管理，反垃圾、反病毒性能极大提高）

蜜罐邮件(独立网关开发全功能,用户可自行添加蜜罐邮箱,收集垃圾、病毒邮件数据,自行提高网关反垃圾、反病毒效率)

IP 规则管理、关键字规则、规则策略管理(独立网关开放全功能全操作,附带网关仅可进行查找、启用、禁用,不可自行添加规则策略。附带网关由彩讯公司运维人员进行日常维护,能够保证基本的反垃圾、反病毒防护效果,但相比独立网关,附带网关用户不能自行添加、修改规则,缺乏一定的个性化与处理特殊性问题的能力)

日志报表包含:

登录日志、操作日志、邮件日志信息、连接日志信息(附带网关为单管理员机制,独立网关用户可以设置多用户、多权限管理。为了便于独立网关用户的日常管理,此四模块为独立网关单独开发)

拦截日志、系统统计信息(独立网关会保存被拦截邮件,用户可以在拦截日志中直接对被拦截邮件原文进行查看、转发等操作,而附带网关不会保存,仅仅提供被拦截邮件列表,用户只能查看到被拦截邮件名称、被拦截原因等;独立网关开发全功能、附带网关仅支持“查找”与“导出 excel”;系统统计信息为独立、附带网关均享有功能模块)

特征库更新管理包含:

历史更新记录、特征库版本信息(独立、附带网关均享有功能模块)

提醒信管理包含:

全局配置、新增收件人(全局配置为独立、附带网关均享有功能模块;附带网关为单管理员管理,故无“新增收件人”功能模块)

投递转发设置包含:

邮件代理设置、海外转发设置、海外转发统计（独立、附带网关均享有功能模块）

查询工具包含：查询 RBL、查询 PTR 记录、查询 MX 记录、查询 SPF 记录

管理权限包含：权限管理设置、用户管理

对于系统基本设置，因为附带网关的单管理员管理设置，在某些功能的操作选择上有所不同。

3.3 反垃圾有效性

3.3.1 算法优势

自主创新的邮件指纹算法：

该算法根据发件 IP 所在地、Received、Message-ID、X-Mailer、Content-Type、helo、发件人、邮件大小、html 源码、URL、正文内容等等多种特征生成 hash 值。该算法可对任意邮件生成指纹，不管邮件如何变化，人工认为相似的邮件均可生成相似的指纹，进而拦截自动变化的垃圾邮件。打个比方，在没使用该算法前，对于只带一个图片的发票类垃圾邮件，反垃圾系统只能根据图片过滤算法来过滤，但图片变化后即无法过滤，而使用该指纹算法对于所有这些发票垃圾邮件均生成相似的指纹，进而有效拦截

特征聚类算法：

反垃圾系统对于每封邮件的任意一个特征值都会生成相应的规则，聚类算法根据每封邮件生成的规则聚合生成一个聚类 ID，再根据历史上该聚类 ID 在垃圾

邮件/正常邮件出现的情况自动生成该聚类 ID 的信誉。对于新入的一封邮件生成聚类 ID 后，检查该聚类 ID 的信誉进而生成评分规则。

3.3.2 设计优势

反垃圾网关系统由 smtp 网关、反垃圾引擎、数据缓存服务器、管理平台等多个模块组成。在设计中使用了一些技巧：

1. 将反垃圾引擎和数据缓存服务器分开，反垃圾引擎根据 hash 定位到数据缓存服务器，一份数据在整个系统中只保存一份

2. 反垃圾引擎和数据缓存服务器分离，当数据缓存服务器发生故障时，不影响用户发信

3. 当某台数据缓存服务器出现故障时，反垃圾引擎根据一致性 hash 算法会 hash 到另一台缓存服务器上，避免某台数据缓存服务器出现故障时查询不到数据

4. 反垃圾系统需要分析保存海量的规则库，当所有规则库都保存到内存时对内存使用量要求较高，而小企业一般只用一台服务器来部署整个邮件系统，鉴于这种情况数据缓存服务器可支持数据保存在 mysql 数据库或保存在内存，根据配置指定

3.3.3 数据优势

专业运维人员实时分析 139 邮件系统海量的往来邮件，生成垃圾邮件规则库，并同步到企业客户反垃圾系统中。经统计，139 每天处理的邮件大约为 1000 万，过滤率为 99%以上，误判率在万分之 1 以下。

海量的反垃圾规则库包括：

- 发件人信誉文件有约 4000 万条记录

- RBL 有 4000 万条记录
- IP 信誉有 1000 万条记录

总之，139 有专业的分析程序 24 小时在不停的分析，分析出结果后再经过人工审核即可同步到企业反垃圾系统中

3.3.4 世界领先的过滤技术

囊括了二十多种世界领先的邮件安全技术，通过多因素关联分析判别方法，精确识别处理垃圾邮件，大幅降低“非黑即白”所造成的误判和漏判。

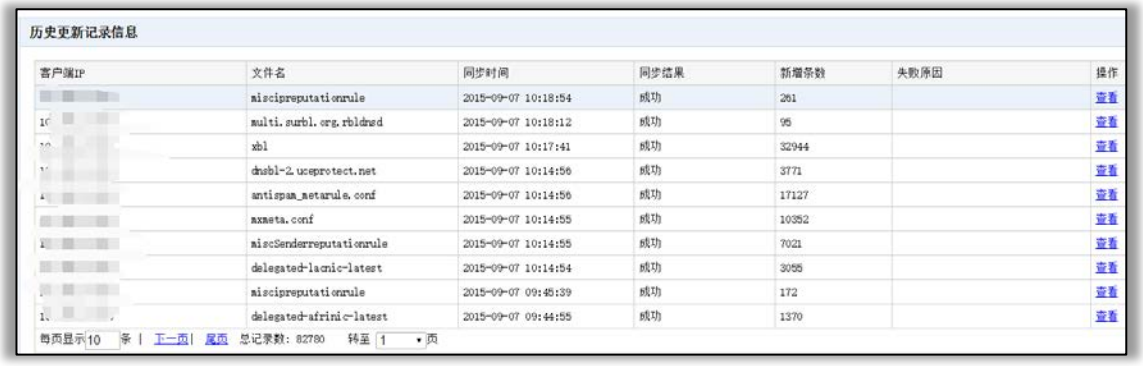
3.4 防病毒准确性

3.4.1 强大防病毒功能

使用全球优秀的企业级杀毒引擎 Sophos，使防病毒技术服务和产品升级的连续性能够得到有效保障。

3.4.2 规则库实时更新

根据预定义的更新频率与策略，可通过 Internet 自动更新病毒特征码、垃圾邮件规则库。可实现系统内核的在线升级。



3.4.3 丰富的 API 接口

针对邮件特征增加了对 IP、发件人、邮件标题、邮件正文、邮件正文指纹、URL、附件名、附件名指纹、信头发件人姓名 等十几种数据操作的接口，便于运维实时学习垃圾邮件样本后实时添加规则。

3.4.4 报表分析功能

提供丰富的病毒邮件、垃圾邮件综合统计分析报告，支持多网关报表数据合并，可保留非法信息传递记录。报表分析系统独立工作，可保障反垃圾邮件网关处理效率。

3.5 运维管理易用性

3.5.1 灵活多样的处理策略

当发现邮件病毒或垃圾邮件时，提供多达十种的邮件处理策略，包括：接收、标记、复制、添加声明、清除病毒、剥离附件、拒收、转发、弹回、隔离等。

3.5.2 简单美观的管理界面

通过 web 管理系统的系统管理功能，直观展示反垃圾系统的工作状态，如资源使用、队列状态、邮件进出情况等。通过规则管理功能，方便添加蜜罐、IP、发件人、关键字等规则。同时提供了查询反垃圾过滤率、统计报表、拦截记录和发送记录等功能。

3.5.3 灵活的部署方式

仅用一台设备即可实现由外到内、内到外、内到内的三向邮件传递保护，保障邮件安全管理策略的一致性，节约投资。一键安装，可适应用户各种复杂网络环境要求。

3.5.4 系统实时监控

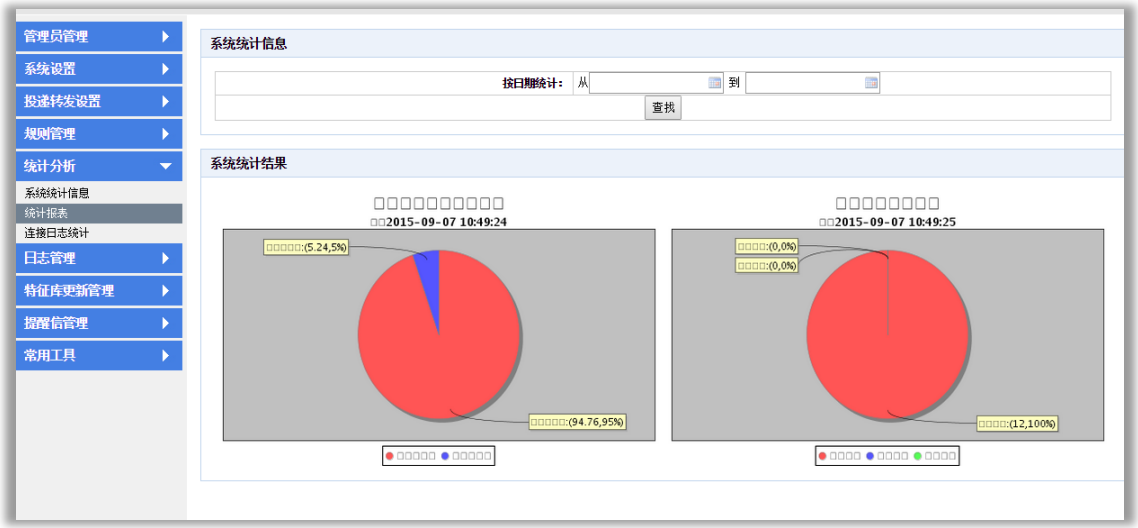
针对反垃圾系统中的各个模块实现了丰富的监控程序，当机器负载、网络通讯、邮件互通异常时，可及时告警、及时解决。

3.5.5 邮件监控与审核

对于某类型的用户，如果符合某些条件，就把邮件转发给指定的邮箱，便于管理员对特定邮件做监控和审核。

4 产品功能介绍

4.1 反垃圾防病毒



4.1.1 过滤病毒邮件

全面过滤外来电子邮件病毒的入侵破坏，保障内部网络环境安全；防止内部邮件病毒向外或在内部扩散，保证发送邮件的安全性和信誉。

4.1.2 过滤垃圾邮件

可全面、智能、高效识别和拦截各种垃圾邮件，防止内部邮件系统和网络带宽被大量占用从而保障资源合理应用，避免个人邮箱被侵占空间从而保障正常邮件接收，预防收件人通过不明邮件上当受骗或引入安全隐患，节约员工处理垃圾邮件时间从而保证工作效率。通过拦截大量垃圾邮件，提高邮件系统和网络资源正常工作效率，防止邮件服务器被利用向外发送大量垃圾邮件，避免被列入黑名单导致不能使用的风险。

4.2 欺诈防御

4.2.1 抵御邮件攻击和欺诈

可根据邮件行为特征，抵御 DHA 攻击、字典攻击、DoS 攻击、邮件假冒（spoofing）、网络钓鱼（phishing）等，保障邮件系统安全可靠工作。

4.2.2 邮件监控与审核

可防范政治敏感信息、违法信息、内部机密信息转播扩散，并可对重点邮件账户进行关键字过滤和内容监管。

4.2.3 邮件真实性校验

通过邮件身份认证、地址绑定、Relay 转发控制、DNS 反查、改进黑名单、邮件结构一致性检查等手段，防范和清除伪装邮件群发和匿名欺骗。

4.3 安全评分规则

4.3.1 网络控制层安全管理

4.3.1.1 TCP/IP 连接管理

连接管理过程不需要多长时间,但对于邮件处理过程的优化相当重要，对于一般规模的中小型企业，一半以上的邮件数量仅仅通过连接管理就将被阻断。绝大多数的 ISP 和小型 WEB 主机在遭受攻击时，可以观察到超过 99%的邮件在连接管理层被阻断。这是一个庞大的数字，如果没有连接管理，海量邮件将会耗费邮件服务器以及邮件防火墙的大量资源。对于频繁的 TCP/IP 连接做必要的限制，有效控制明显的垃圾邮件发送行为。

4.3.1.2 防止 DOS 攻击

在一个极短的时间里，向一个邮件服务器发送大量的邮件，占用邮件服务器的资源使邮件服务器不能正常地提供邮件服务，这就是针对于邮件系统的拒绝式服务攻击。将邮件系统在一定时间内处理的邮件数量限制在一个相对合适的范围，就可以有效地防止拒绝式服务攻击，这里建议邮件系统每分钟可以处理 30 封信件。 通过灵活设计限制每个 IP 同时连接数、每个连接最多发送的命令数量、最近 1 小时发送命令失败比例、最近 1 小时密码校验失败次数等发送策略，可有效防止拒绝式服务攻击。

另外，还可以启用安全操作系统的部分防火墙功能，并采取行为控制措施，对明显的非邮件服务请求予以阻断，防止 DOS 攻击；采用专用安全 OS 与硬件平台有效抵御攻击。

4.3.1.3 发信速率控制

自动垃圾邮件软件可以向一个邮件服务器发送大量垃圾邮件。为了保护邮件服务器免受这些攻击，反垃圾网关对从来自一个特定 IP 地址的连接进行计数，并在这个连接超出阀值时断开连接，以规避大量的通过客户端软件发送垃圾的行为。通过已知服务器或与已知合作伙伴交流频繁的公司应该将这些合法的 IP 地址和合法的邮件服务器加入速率控制的例外名单。

4.3.2 人工智能识别

4.3.2.1 意图分析技术

意图分析包括鉴别历史记录里的错误邮件发送基点、它们目前的行为和意图。许多防御策略用来鉴别垃圾邮件，而意图是随时间而改变的特殊类别。

大部分垃圾邮件背后的动机是使接受某物，例如登陆某个站点，拨打某个电话，或者买某只股票。这些动机被称为邮件“意图”，观察邮件的这些特点叫做“意图分析”。目前为止，大部分垃圾邮件的意图都是让用户点击一个网页或链接。

即使邮件发送者试图通过新 IP 地址掩盖他们的不良记录，他们最终还是需要驱使用户去特定的网站。通过对发信 IP、发件人、邮件正文等多指标，多因素关联分析。以模式而不是算式的方式建立模型，包含特征，特征间关系，以及模型匹配的方法。

4.3.2.2 Bayes 算法

Bayes 分析是一种语言算法，目的是对邮件中的语言进行分析，为了判定一封新邮件是垃圾邮件还是正常邮件，Bayes 分析首先使用常规的分词手段和程序将一段文字或内容切词（tokenize）成一些单词字符串（token 串），并进行评分设置，用于对比待检验可以达到 99.7%的垃圾邮件识别率，同时误判率极低，是目前最有效的反垃圾邮件技术。系统采用 Bayes 自动学习算法，事先对大批量人工分类的正常邮件和垃圾邮件进行学习，统计出邮件每个词条在正常邮件和垃圾邮件中出现的几率。在处理邮件的时候，可基于这些事先统计好的数据，评估出一封邮件是垃圾邮件的几率。在邮件评分的统一架构下，Bayes 评估结果作为邮件评分的一个因子，反映 Bayes 算法对邮件是否垃圾邮件的评定。

1)Bayes 过滤技术对邮件的所有内容进行分析，不仅仅是其中的某个关键词，而且他能判别邮件是垃圾邮件还是正常邮件。例如：包含“free” “cash” “发票”字样的邮件不一定是垃圾邮件，如果采用关键字过滤技术，显然难以达到理想的效果。而 Bayes 呢，即考虑了这些词在垃圾邮件中出现的概率又考虑了它在正常邮件中的概率，综合考虑这些因素才做出判断。可以说，Bayes 具有一定的智能，它对邮件中的关键词汇能综合的进行评判，可以把握“好”与“坏”之间的平衡。显然，这种技术远远高于非 1 即 0 的静态过滤技术。

2) Bayes 过滤技术具备自适应功能—通过学习新的垃圾邮件及正常邮件样本，Bayes 将能对抗最新的垃圾邮件。并且对变体字有奇效。比如，垃圾邮件发送者开始使用"f-r-e-e"来代替“free”这样能够绕过关键字检查，除非"f-r-e-e"被加到新的关键字中。对 Bayes 而言，当它发现邮件中含有"f-r-e-e"时，由于正常邮件中从来没有发现这个词，因此他是垃圾邮件的可能性将急剧增加，"f-r-e-e"这个新词无疑成了垃圾邮件的指示器。在比如，垃圾邮件中用 5ex 代替 sex，Bayes 也推算出他是垃圾邮件的可能性也急剧增加。

3) Bayes 过滤技术更加个性化。他能学习并理解用户对邮件的偏好。如前所述，‘mortgage’抵押一词对软件公司而言意味者垃圾，但对金融类公司则意味着好邮件。Bayes 能根据用户的这种偏好进行处理。

4)Bayes 过滤技术支持多语种或者说与编码无关。对于 Bayes 而言，他分析的是字串，无论他是字、词、符号、还是别的什么，当然更与语言无关。

5)Bayes 过滤器很难被欺骗。垃圾邮件发送高手通常通过减少垃圾词汇（如 free、viagra、发票）或者在信中多掺一些好的词汇（如合同、文件）来绕过检

查一般的邮件内容检查，但由于 Bayes 具有的个性化色彩，要想成功的绕过 Bayes 的检查，他就不得不对每个收件人的偏好进行研究，这简直是“不可能完成的任务”。垃圾邮件发送者无法容忍的。若采用变化字，则如前所述 Bayes 判断其为垃圾邮件的可能性反而增加。

4.3.2.3 图片 SVM 过滤技术

基于图片特征和相关文本特征，采用 SVM 技术分类垃圾图片和正常图片。首先通过人工标注，建立正常图片集合和垃圾图片集合。然后自动提取每张图片和相关邮件文本的特征，使用 SVM 根据两类特征数据进行训练，得到图片分类模型。在线上处理邮件时，使用分类模型，计算得到一张图片是否垃圾图片的概率。

4.3.2.4 举报垃圾邮件及智能学习

与邮件系统结合，当用户举报垃圾邮件时，后台程序分析提取邮件特征，再通过 API 接口发送给反垃圾系统。反垃圾系统通过收到的邮件特征，与新收到的邮件匹配进而有效拦截后来发送进来的垃圾邮件。

4.3.2.5 邮件指纹技术

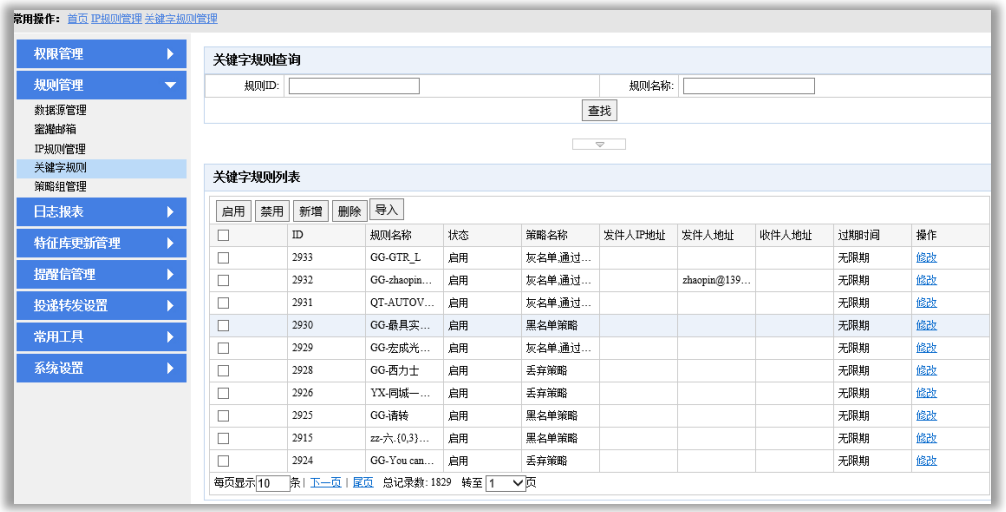
指纹分析是基于许多常见的垃圾邮件组成部分（比如图片）。当前已爆发的垃圾邮件被定义后，生成指纹，以阻止进一步扩散，这是一种有效的阻断机制。但需要技术支持团队做 24 小时的跟踪监测。 将垃圾邮件抽样提取标本，形成小的特征文件，我们称之为指纹，再利用这些指纹来判定一封邮件究竟是不是垃

圾邮件。再通过反垃圾数据同步机制，将数据中心 24 小时监控收集到的数据实时同步到反垃圾网关使用，进而实时有效拦截垃圾邮件。

传统的文件比较方法，会将有微少区别的邮件判断为两封邮件。实际上垃圾邮件发送者往往改变邮件信体部分的内容，例如只是改变信件的称呼，或者改变信件内容的排版，发送大量事实上内容相同的垃圾邮件。邮件指纹算法可判断两封邮件的相似度，进而有效拦截垃圾邮件。

4.3.2.6 关键字规则

当管理员发现某些使用现有技术无法有效拦截的垃圾邮件时，可通过管理界面添加关键字规则，进而让系统马上拦截此类垃圾邮件。可以和发信 IP、发件人等多维度的信息结合，有效降低误判率。

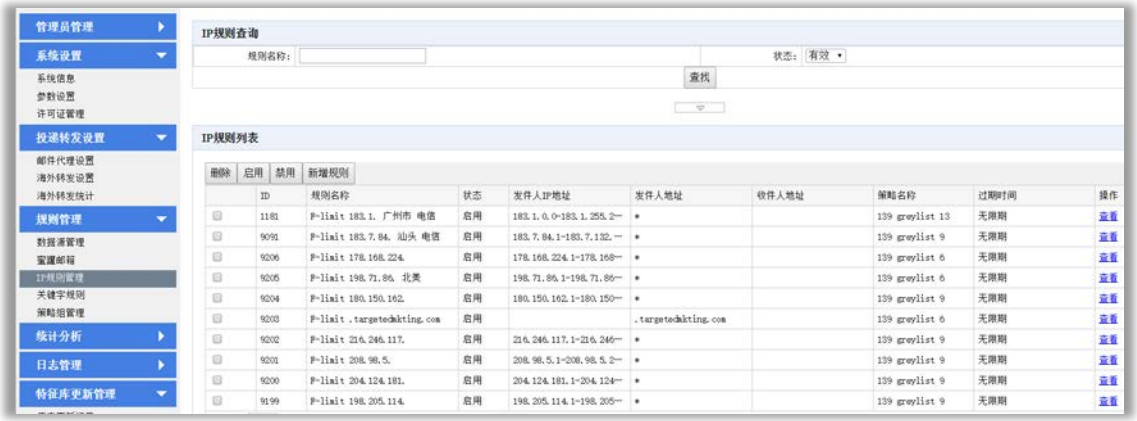


4.3.2.7 邮件规则评分

系统使用多条评判垃圾邮件的规则，对邮件的发信 IP，发信人地址，信件内容所有特征都生成规则，并对规则进行评分。使用邮件评分技术使得反垃圾邮件

系统可以更灵活地组合各种过滤规则，系统管理员可以设定划分垃圾邮件的系统过滤阈值参数，从而动态调整系统对垃圾邮件的过滤强度。

4.3.3 IP 评分



4.3.3.1 IP RBL 过滤

这种技术类似于前面所提到 IP 黑名单的方法，区别在于实时黑名单列表是借助于第三方机构，他们为用户提供，垃圾邮件的判断工作也是在 INTERNET 上进行的，不需要用户进行干涉和手动添加。通常该技术是通过 DNS 方式（查询和区域传输）实现的。

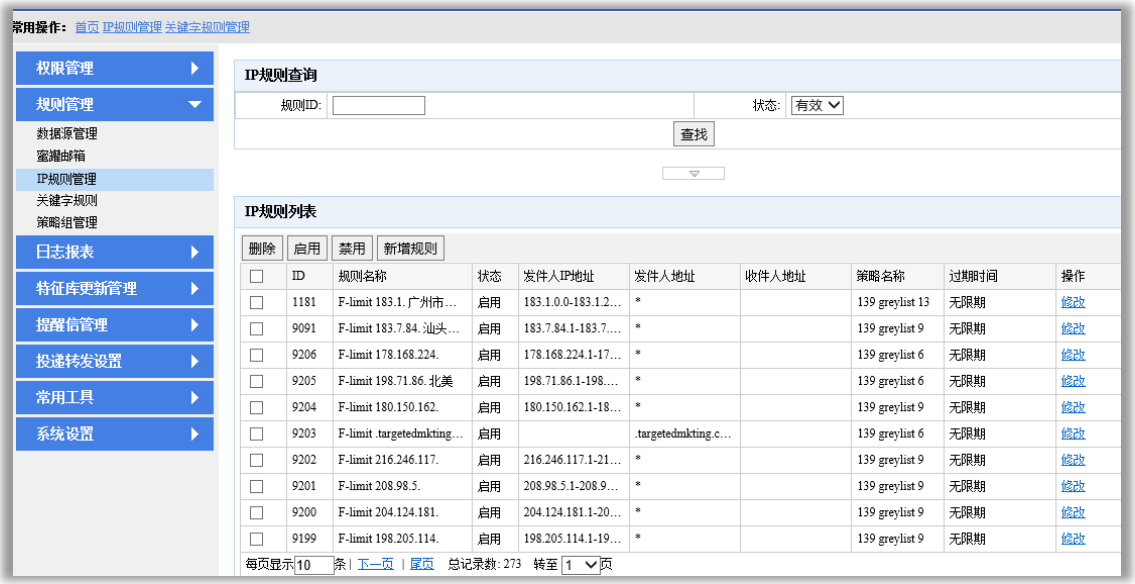
实时黑名单实际上是一个可供查询的 IP 地址列表，通过 DNS 的查询方式来查找一个 IP 地址的 A 记录是否存在来判断其是否被列入了该实时黑名单中。举例来说，如果要判断一个地址 61.138.111.227 是否被列入了黑名单，那么使用黑名单服务的软件会发出一个 DNS 查询到黑名单服务器（如 zen.spamhaus.org），该查询是这样的： 227.111.138.61.zen.spamhaus.org 是否存在 A 记录？如果该地址被列入了黑名单，那么服务器会返回一个有效地址的答案，按照惯例，这个地址是 127.0.0.2 (之所以使用这个地址是因为 127/8

这个地址段被保留用于打环测试，除了 127.0.0.1 用于打环地址，其它的地址都可以被用来做这个使用，比如有时候还用 127.0.0.3 等。）。如果没有列入黑名单，那么查询会得到一个否定回答。 有时候，由于邮件服务器非常繁忙，而且这个查询结果是不缓存的，那么对黑名单服务器的查询会非常多，导致查询响应迟缓。在这种情况下，可以使用 DNS 的区域传输，将黑名单服务器的数据传输到本地的 DNS 服务器，然后对本地的 DNS 服务器进行查询即可。

RBL 服务器的 DNS 查询和区域传输，并不是都可以随意使用的。有些服务器可供任何人查询和区域传输，而有些只对特定的用户开放。我们根据国内外 Spamhaus 等多个著名的 RBL 组织提供的数据对发信 IP 进行检查，速度非常快。同时由专业的运维团队维护数据，保证高过滤率了的前提下零误判率。

优点：减少用户的工作量和设置难度，降低一定的误报率。

缺点：有的 RBL 提供方提供的 RBLS 过于强硬。



4.3.3.2 SPF 过滤

SPF 是发送方策略框架（Sender Policy Framework）的缩写，一种以IP(互联网协定）地址认证电子邮件寄件人身份的技术，是非常高效的垃圾邮件解决方案，旨在应对垃圾邮件中的一个特别问题——发送方假冒问题。当用户定义了他的域名 SPF 记录之后，接收邮件方会根据该用户的 SPF 记录来确定连接过来的 IP 地址是否被包含在 SPF 记录里面，如果在，则认为是一封正确的邮件，否则则认为是一封伪造的邮件。因此，那些发信人伪造域名的垃圾邮件在 SPF 的火眼金睛下再也无法隐藏，企业邮箱就可以有效地避免此类垃圾邮件。SPF 正在逐步成为一个防伪标准，来防止伪造邮件地址。您的域管理员或托管公司仅需在域名系统（DNS）中发布 SPF 记录。这些简单的文本记录标识了经过授权的电子邮件发送服务器（通过列出这些服务器的 IP 地址）。电子邮件接收系统会检查邮件是否来自经过正确授权的电子邮件发送服务器，防止假冒信誉较好的域名发信。

4.3.3.3 发信 IP 反向解析

在发邮件的时候，随意编造一个域名是非常容易的，如果采用阻断非法域名的方式来防止垃圾邮件的话，那么用户可以说是被动到极点了，而且根本没有办法防止，因为那些域名都是根本不存在的。DNS 反向查找技术就是在收到邮件时对发件人的地址的真实性进行核查，防止 DNS 欺骗，发现冒充的虚假发件人地址。

4.3.3.4 IP 信誉评估

通过统计运营商的海量过滤数据分析，计算所有曾经连接过这些运营商的 IP 信誉数据。历史发信记录好的 IP 信誉较高，对于历史上发送较多垃圾邮件的 IP

则信誉较低。根据信誉高低来判定发送垃圾邮件的概率，在规则评分系统中体现出来。

4.3.3.5 源 IR 信誉评估

通过分析提取邮件中特定信头字段，如 X-Originating-IP: 8.8.8.8，得到终端用户的真正 ip。再通过统计运海量过滤数据，计算得到这些 IP 的信誉。这样可有效拦截通过运营商发送的垃圾邮件。

4.3.3.6 发件人信誉评估

通过统计运营商的海量过滤数据分析，计算所有发信用户信誉数据。对于只有发信记录，没有收信记录的用户；或者历史上没有发信记录，最近突然有大量的发信记录的用户评估信誉较低。对于历史发信记录好的用户信誉较高，对于历史上发送较多垃圾邮件的用户则信誉较低。根据信誉高低来判定发送垃圾邮件的概率，在规则评分系统中体现出来。

4.3.3.7 URL RBL 过滤

数据更新系统会实时更新 Spam URL Realtime BlackList 数据，反垃圾邮件引擎自动提取分析邮件的 url 是不是符合 Spam URL RBL，若符合则将过滤该邮件。

4.3.4 智能钓鱼识别

4.3.4.1 蜜罐邮件

首先在系统内定义一批邮箱地址为蜜罐邮箱地址，通过论坛、网页等途径公开发布到互联网上。发垃圾邮件的程序通过爬虫技术抓取到这些邮箱地址，再往

这些邮箱发送垃圾邮件。反垃圾系统收到蜜罐邮箱的邮件后，通过自动学习邮件样本提取邮件特征和发送意图，进而有效的拦截同类垃圾邮件。

4.3.4.2 DKIM/DMARC 反钓鱼邮件技术

DKIM（DomainKeys Identified Mail）技术基于雅虎的 DomainKeys 验证技术和思科的 Internet Identified Mail。雅虎的 DomainKeys 利用公共密钥密码术验证电子邮件发件人。发送系统生成一个签名并把签名插入电子邮件信头，而接收系统利用 DNS 发布的一个公共密钥验证这个签名。思科的验证技术也利用密码术，但它把签名和电子邮件消息本身关联。发送服务器为电子邮件消息签名并把签名和用于生成签名的公共密钥插入一个新标题。而接收系统验证这个用于为电子邮件消息签名的公共密钥是授权给这个发件地址使用的。DKIM 将把这两个验证系统整合起来。它将以和 DomainKeys 相同的方式用 DNS 发布的公

共密钥验证签名，它也将利用思科的标题签名技术确保一致性。DKIM 给邮件提供一种机制来同时验证每个域邮件发送者和消息的完整性。一旦域能被验证，就用来同邮件中的发送者地址作比较检测伪造。如果是伪造，那么可能是 spam 或者是欺骗邮件，就可以被丢弃。如果不是伪造的，并且域是已知的，可为其建立起良好的声誉，并绑定到反垃圾邮件策略系统中，也可以在服务提供商之间共享，甚至直接提供给用户。对于知名公司来说，通常需要发送各种业务邮件给客户、银行等，这样，邮件的确认就显得很重要。可以保护避免受到 phishing 攻击。

DomainKeys 的实现过程：

发送服务器经过两步：

1、建立。域所有者需要产生一对公/私钥用于标记所有发出的邮件（允许多对密钥），公钥在 DNS 中公开，私钥在使用 DomainKey 的邮件服务器上。

2、签名。当每个用户发送邮件的时候，邮件系统自动使用存储的私钥来产生签名。签名作为邮件头的一部分，然后邮件被传递到接收服务器上。

接收服务器通过三步来验证签名邮件：

1、准备。接收服务器从邮件头提取出签名和发送域（From:）然后从 DNS 获得相应的公钥。

2、验证。接收服务器用从 DNS 获得的公钥来验证用私钥产生的签名。这保证邮件真实发送并且没有被修改过。

3、传递。接收服务器使用本地策略来作出最后结果，如果域被验证了，而且其他的反垃圾邮件测试也没有决定，那么邮件就被传递到用户的收件箱中，否则，

邮件可以被抛弃、隔离等，有效拦截识别并拦截钓鱼邮件，从而确保用户的个人信息安全。

4.3.5 黑白灰名单

4.3.5.1 黑白名单

较早的一种反垃圾邮件的技术，将经常向你发垃圾邮件的 IP 地址添加到 IP 黑名单中，当再从同样的 IP 地址发来信件都被判定为垃圾邮件。如果 IP 地址被加入到白名单中，则认为从那里来的任何邮件都不是垃圾邮件。后来出现的拒绝发件人、拒绝的域也都是类似的技术。

优点：技术比较容易实现，判断速度快。

缺点：误判率 LS 过于强硬。

4.3.5.2 自动白名单

系统能够自动监控本站用户外发的邮件，从外发邮件中自动搜集邮件的收件人地址，把收件人地址加入到发件人白名单里，这样当收件人给原发件人回复邮件时，就可以匹配自动白名单，降低系统误判率。

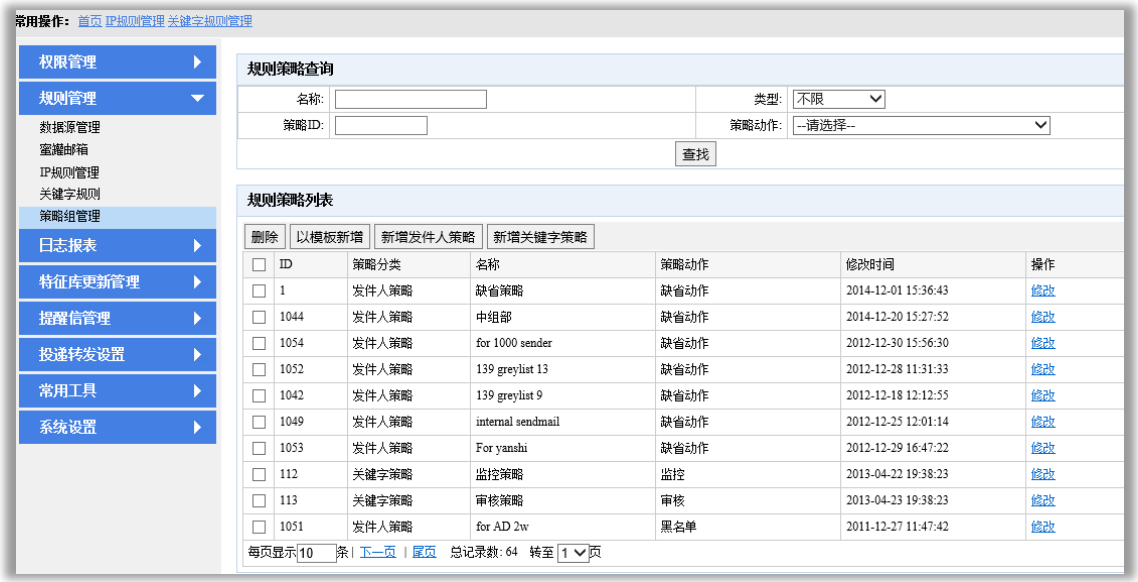
4.3.5.3 灰名单技术

根据协议，灰名单技术会返回 450 数字信号，告诉对方服务器暂时不能发信，请稍候尝试重新投递。如果对方服务器再次发送信件，证明发信方使用带有队列的正常邮件系统，而垃圾邮件发送程序要发送大量的邮件，一般很少重试灰名单的邮件。在重试的间隔内，网关产品通过实时的学习功能，在邮件重新投递时可准确判定邮件是正常邮件还是垃圾邮件，进一步提高过滤率，降低误判率。

4.3.6 策略组

4.3.6.1 反病毒过滤

使用全球优秀的企业级杀毒引擎 Sophos，使防病毒技术服务和产品升级的连续性能够得到有效保障。当发现邮件病毒时，提供标记、复制、添加声明、清除病毒、剥离附件、拒收、转发、弹回、隔离等。



4.3.6.2 灵活的反垃圾策略组

管理员可以选择定义自己的策略，策略可基于主题，信头，信体，和附件类型的内容过滤。策略用于指定对应的限制，可以形成多条规则的组合，系统管理员可根据需要灵活更改策略的限制。采用过滤规则策略组的设计，可创建多条精确而且灵活的过滤规则组织形式，例如系统管理员可以对某个 IP 段内的主机，限制该区域用户每次连接可以发送的邮件数量、同一封邮件最大收件人数量、邮件大小限制、同一个发信人每 15 分钟、每天可以发送的邮件数量和收件人数量、

使用启用 RBL、SPF、邮件指纹、关键字过滤限制，设定灰名单、保存到垃圾箱、拦截评分阀值等多个策略选项，建立企业所需要的过滤策略。

4.3.6.3 子规则组合过滤

反垃圾系统对于所有特征都生成一条对应的规则，因为垃圾邮件总是在变化，单用某条规则难以有效拦截垃圾邮件时，管理员可针对邮件的特征，从 n 种特征中提取 m 种特征，当同时匹配这 m 种特征时则可判定更高的权重，进而有效拦截垃圾邮件。另外，还可判定当在 n 中特征中匹配任意 m 种特征时，则判定更高权重，进而有效拦截垃圾邮件。

4.4 系统管理

4.4.1 智能管理系统

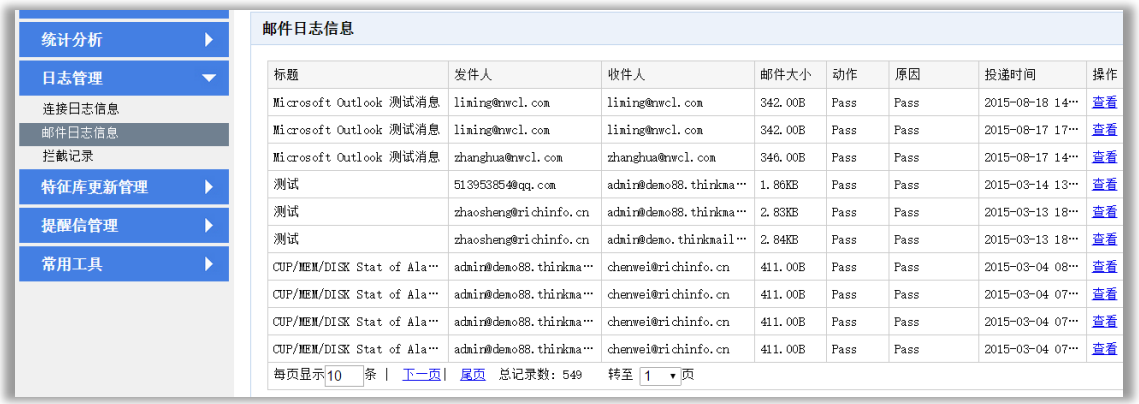
投递日志跟踪：系统保留垃圾邮件过滤的处理信息，即系统的日志。邮件日志跟踪的时候可以点击进去看更详细的投递信息。管理员可以根据系统的日志信息，回溯查找到具体的邮件处理过程，从而准确地判断邮件无法接收或者投递的原因。

4.4.2 统计报表

对各类特征和规则起到的反垃圾效率进行周期性统计，同时对各企业的反垃圾信息进行统计并以报表的形式展示给企业管理员查看。

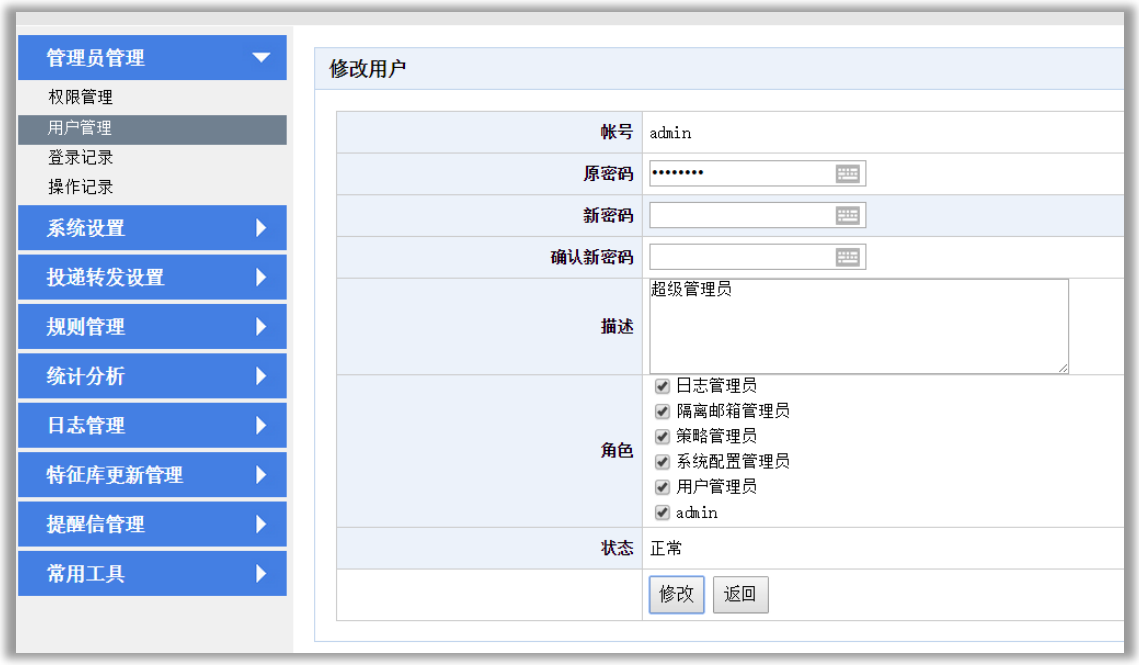
4.4.2.1 日志管理

主要是反垃圾产品的日志，我们会提供相应的日志规范文档，同时也会提供详细的日志查询界面，供管理员查询和定位日常问题。



4.4.2.2 用户控制

主要是针对用户进行分权分域管理，该功能在用户升级病毒库、垃圾规则库、以及产品使用权限等方面会得到体现。



4.4.2.3 规则更新

我们在提供反垃圾产品的同时，还提供了反垃圾产品更新能力，包括病毒库更新能力、垃圾规则更新能力，更新系统也随着反垃圾网关产品同步建设完成。

5 服务与支持

彩讯科技股份有限公司设有专门的运维与售后服务机构——运维部和客服中心，在深圳、广州、北京、上海等全国二十多个城市均具有优秀的技术人员和雄厚的技术力量，并且为本项目指定了专职运维与客服经理，负责运维及售后服务的统一协调工作。

深圳总部地址：深圳南山区高新南区科苑南路 3176 号彩讯科创中心 32 层

服务电话：4008-303-123

营销 QQ：4008303123

微信公众号：


彩讯
RICHINFO