TurboGate
邮件网关

产品解决方案书

广州拓波软件科技有限公司
地址：广州市天河区天河路242号丰兴广场B座2502
邮编：510620
传真：8620-38921969
电话：8620-85509396 38395469 38394823
技术支持热线：400-6688-629
网址：www.turbogate.net

目录

公司简介

广州拓波软件科技有限公司的前身拓波工作室成立于 2002 年，是专业研发电子邮件系统、邮件网关系统、企业即时通讯和短信平台的组织机构。经过三年的研发，在 2005 年，拓波工作室正式发布 1.0.2 版本 TurboMail® 邮件服务器软件，并成为国内最大的邮件服务器软件 OEM 开发商，为国内知名的邮件系统供应商提供产品。2007 年拓波工作室正式转为实体公司，正式开展自主品牌 Turbo 系列邮件系统、邮件网关、即时通讯产品、飞邮手机客户端的销售。凭借着卓越的产品性能与功能，Turbo 品牌企业通信产品签约了超过 3000 家各级别企事业单位客户，跃居国产邮件通信产品第一品牌。

广州拓波软件科技有限公司的创始团队来自华南理工大学，依托华南理工大学的优势，聚集了一群软件开发高级人才专注于企业通信相关软件产品的研发。公司视产品性能，功能和服务为自己的生命，秉承“行胜于言”的所训以及“技术服务社会”企业理念，以 100%客户满意度为产品合格标准，坚持实施自主创新战略、品牌战略和产学研一体化战略，实现企业的可持续发展，为打造一流的科技企业而努力。广州拓波软件科技有限公司是国家双软企业、高新技术企业、广东软件协会成员。

客户的需求是拓波的发展动力，拓波始终以客户的需求为根本出发点，用扎实的技术实力解决企业客户有关邮件的一切问题和达成企业用户对邮件方面的各种功能需求。TurboGate®以开放的技术架构，在国内整合了几十家二次开发伙伴，为各行各业客户提供个性化需求。

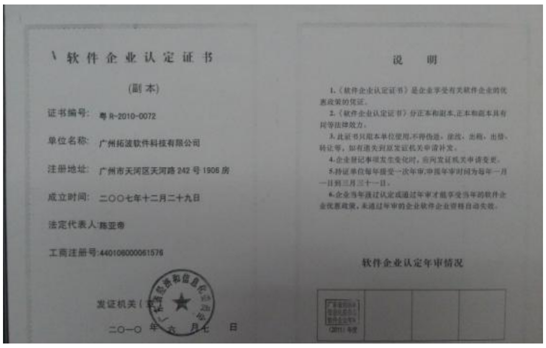
邮件是一个古老而又永恒的互联网基本功能，拓波已积累了丰富的邮件网关系统架设经验，能为客户未雨绸缪的处理许多潜在问题，解除用户未知的烦恼，使得邮件网关系统成为企业拦截垃圾和病毒邮件的前锋，是企业控制内部邮件服务器邮件收发的最佳助手。

拓波理念：　　坚实　　创新　　服务　　真诚

拓波产品方针：　　领先产品+专业服务=长期信赖的伙伴

资质证书

电话：8620-85509396　38395469　38394823
地址：广东省广州市天河区天河路242号丰兴广场B座2501-2502号


软件企业认定证书
(副本)
证书编号：粤R-2010-0072
单位名称：广州拓波软件科技有限公司
成立时间：二〇〇七年十二月二十八日
说 明
软件企业认定年审情况


计算机信息系统集成
资 质 证 书


设计、施工、维修资格证
说明
年检记录


新办高新技术企业证书
（副 本）


中华人民共和国国家版权局
计算机软件著作权登记证书
软 件 名 称：TurboGate邮件网关软件
[简称：TurboGate]
V4.3.0
著 作 权 人：广州拓波软件科技有限公司
开发完成日期：2011年03月11日
首次发表日期：2011年03月20日
权利取得方式：原始取得
权 利 范 围：全部权利
登 记 号：2011SR059142
根据《计算机软件保护条例》和《计算机软件著作权登记办法》的规定，经中国版权保护中心审核，对以上事项予以登记。
No. 00028592


软件产品登记证书
经审核，拓波 TurboGate 邮件网关软件 V4.3.0符合《鼓励软件产业和集成电路产业发展的若干政策》和《软件产品管理办法》的有关规定，准予登记，特发此证。
申请企业：广州拓波软件科技有限公司
证书编号：粤 DGY-2011-1299
有 效 期：五年 至：2016 年 11 月 10 日
发证机关：
二〇一一 年 十一月 十一日

一、 邮件系统面临的安全威胁

众所周知，随着 Internet 的普及，电子邮件作为现代通信手段逐渐占据了互联网主流应用的地位。由于电子邮件的方便、快捷、经济等特点，人们对电子邮件的依赖程度日益增强。然而在全国乃至全世界，都在大力推进政府信息化、企业信息化、电子商务活动的形势下，电子邮件系统面临着十分严峻的安全威胁：既要防止黑客的攻击，又要防范邮件系统病毒邮件蔓延；既要防止垃圾邮件泛滥，又要堤防内部敏感资料的泄漏。

在国内，垃圾邮件的猖獗现象更是不容忽视。据赛门铁克 2011 年最新发布的全球互联网安全统计报告指出，中国垃圾邮件比率高达 84.6%。大量垃圾邮件的存在占用了大量的网络带宽资源，服务器存储资源以及邮件用户的时间；日益增加的垃圾邮件有淹没正常邮件的趋势，严重干扰了正常信息的传递与流动，为了保障正常信息的有效，稳定，高效传递，邮件系统的安全加固方案越来越受到各单位信息部门的重视。

电子邮件系统面临的威胁：

- **反垃圾**

这三种罪大恶极的恶意代码可以作为电子邮件附件诱使用户打开或运行，它们就可以破坏一台主机系统的数据，将计算机变成可被远程控制的网络僵尸，甚至可以导致收件人经济上的巨大损失。举个例子来说，有一种特洛伊木马称为键盘记录器，它可以秘密地记录系统活动，可以导致外部的恶意用户访问公司的银行账户、企业的内部网站及其它的私密资源。

- **网络钓鱼**

钓鱼攻击可以利用社交网络工程窃取个人的信息和财务金融数据。这种攻击主要依赖“伪造”邮件将收件人指引到欺诈性站点，诱骗用户输入机密的金融数据，如信用卡号、账户名、口令等。钓鱼活动的诈骗者典型情况下通过假冒的身段来隐藏自己，这些身份是通过从银行、在线交易商、信用卡公司等窃取的。

- **垃圾邮件**

垃圾邮件虽然不像病毒感染一样是一种明显的威胁，垃圾邮件可以极快地淹没用户的收件箱，这就使得用户难于查看合法的电子邮件。垃圾邮件问题已经相当严重，以至于用户会放弃某个由垃圾邮件摧毁的电子邮件账户。垃圾邮件还是钓鱼者和病毒制造者喜欢的传播媒介。

- **邮件泄密**

随着企业电子文挡资料的日益丰富，许多企业内部不法员工也经常会选择利用电子邮件将机密资料快速转移，以达到他们的非法目的。很多企业对电子邮件系统的使用，缺乏安全审计管理的措施，给管理层带来诸多麻烦。

二、垃圾邮件泛滥原因

垃圾邮件的产生可以追溯到最开始的连锁信，随着邮件技术的发展，垃圾邮件技术也在逐步发展，但要想找到彻底解决垃圾邮件问题的技术，必须从邮件传输的原理人手。目前邮件传递的主要协议是 SMTP 协议，该协议没有任何认证手段，因此缺省的 SMTP 邮件服务器是所谓的 OpenRelay(开放转发器)，无论邮件来自哪里或发到哪里，邮件服务器都会予以发送。最常见的邮件发送过程是，邮件的客户端使用 SMTP 协议将邮件发送给一台 SMTP 发送服务器，然后 SMTP 发送服务器根据邮件的目的地址，使用 SMTP 协议将该邮件转发给目标 SMTP 服务器(接收服务器)，接收服务器收到邮件后放入接收人的邮箱(Mailbox 或 Maildir，可，能是单独的服务器，也可能是同一台机器上)，最后另一个邮件客户端(接收方)使用 POP3 或 IMAP 协议从邮箱服务器上接收自己的邮件。整个过程中，发送方与发送服务 QS、发送服务器与接收服务器之间都不做认证，因此发送方可以使用互联网上任意一台 SMTP 服务器来发送邮件，这就是 OpenRelay。

近年来由于垃圾邮件的泛滥，大部分邮件服务器关闭了 OpenRelay，在发送方与发送服务器间需要认证，来保证发送服务器发送邮件的主机的合法性，这就是增强的 ESMTP 协议。但这并没有解决第二个环节：发送邮件器和接收邮件服务器间的合法性认证。因为不可能要求接收邮件服务器上保存所有发送邮件服务器的合法用户信息，因此发送邮件服务器无法向接收邮件服务器做认证。

目前的邮件服务器的处理方式是：如果目的地址是本邮件服务器的用户，则无需认证予以接收;如果目的地址不是本邮件服务器的用户，需要用本邮件服务器的合法用户的用户名和口令来认证(该用户可以不是该邮件的发件人)。这样，就给自动垃圾邮件发送程序提供了可能：只要给邮件服务器发的邮件是该邮件服务器的用户，即可发送进去。我们知道，可以随处得到一个数百万甚至上千万的 Email 列表，使用程序自动按照邮件服务器域名发送相应的用户是很容易的，这就导致了垃圾邮件的泛滥。

三、TurboGate 简介

针对国内大量泛滥的垃圾邮件形势，拓波研发出 TurboGate 邮件网关系统。TurboGate 邮件网关系统放置在公网与内部邮件系统之间，起到拦截作用。邮件网关服务器作为公网和内部邮件服务器数据沟通的唯一途径，可控性极高，网络只能前进到邮件网关服务器，无法入侵内部邮件服务器。若网关服务器因病毒等原因出现故障，管理员可快速中断内外部之间的通讯，有效保护邮件系统的正常运营，而且所有的数据信息仍保存在内部邮件服务器上，不会因为邮件网关的任何故障而损害或影响用户的各种数据信息，有效的保证零数据丢失。

作为邮件网关，TurboGate 实现了如下 7 大功能。

- **反垃圾**

TurboGate 内嵌反垃圾功能模块，把外网发送过来的垃圾邮件全部都拦截在 TurboGate 邮件网关系统上，既减轻了内网邮件系统的负担，又不会干涉到内网的正常收发。若出现误判，或者需要处理垃圾邮件时（垃圾邮件存放在 TurboGate 系统上），只要登陆 TurboGate 邮件网关系统进行处理即可，不必通过内网的邮件系统进行处理，极大减轻内网邮件系统的压力。

针对近年来企业内部频繁出现的内部账号被盗用外发垃圾邮件的问题，TurboGate 采取一系列的措施有效的预防和制止此行为，例如：防止 SMTP 盗号、外发垃圾邮件扫描、锁定盗号账户、限制 SMTP 访问频率等，全方位的保护企业内部邮件服务器安全。

■ **反病毒**

实现反病毒功能。TurboGate 邮件网关系统支持多种杀毒引擎，并且内置著名的开源杀毒引擎 ClamAV，对邮件类病毒具有 99.9%的杀灭能力，同时支持嵌入式杀毒和网关杀毒自动定时更新病毒特征库。

■ **邮件中继**

TurboGate 邮件网关提供高级中继服务，通过 TurboGate 在国外设置的中继服务器，系统会自动把企业发往国外失败的邮件，转由中继服务器投送出去。全球通邮的百分百收发成功率，是企业发展强大的保障和后盾，为海外业务的拓展打下了通讯的奠基石。

■ **邮件监控**

对经过邮件网关的所有邮件进行灵活监控。

邮件监控的邮箱账号有两种选择：

① 可在 TurboGate 邮件网关系统上建立一邮箱账号，所有的被监控邮件都会发送到该账号上。

② 可用外部邮箱账号作为监控邮箱，所有的被监控邮件都会发送到该外部邮箱账号上。

■ **邮件审核**

经过邮件网关时，对符合邮件审核规则的邮件进行审核。只有通过审核的邮件才能进行收发。该操作对于用户是透明操作的，邮件审核规则也灵活多变,且支持多级审核。

■ **邮件过滤**

实现邮件过滤，只有符合过滤规则的邮件才能发送到内网邮件系统或者发送到外部互联网上。灵活的规则设置，可以有效的控制用户收发权限。

■ **邮件归档**

在邮件网关中实现邮件归档功能，所有经过 TurboGate 邮件网关系统收发的邮件都将进行同步备份，即使内部邮件系统彻底删除某些邮件，由于邮件已被备份，仍能在 TurboGate 网关邮件系统上轻松检索调出，邮件备份功能就像是一个持续运作的复印机，来往所有邮件全部被复印留底。归档功能只能在 TurboGate 邮件网关系统上实现和管理，无法在内部邮件系统上实现，但同时也释放了内网邮件服务器，不用承受日积月累的邮件数量的压力。

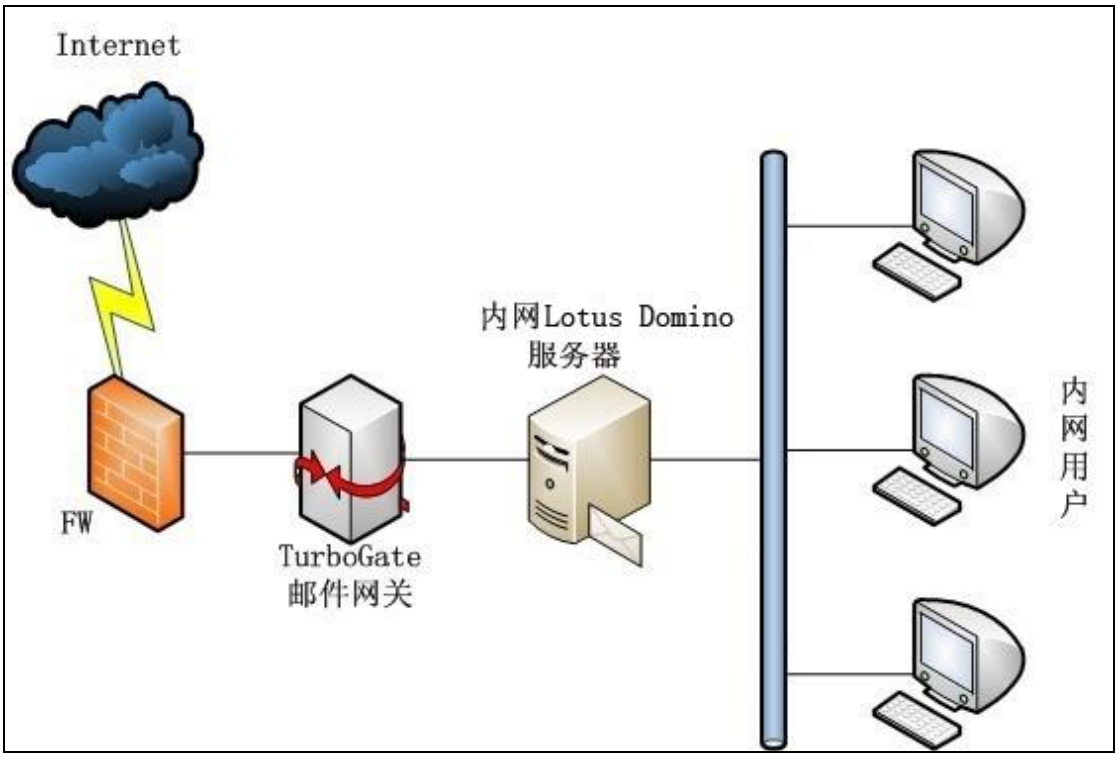
一、硬件配置

服务器数量：1 台，功能指标：

网络层功能	1. 网络地址阻断：控制特定的地址、端口 2. 最大连接数控制 3. 最大连接频率控制 4. 邮件路由控制
协议层功能	1. 支持协议：SMTP、ESMTP、http 2. 邮件发送数量控制 3. 指定邮件监控 4. 邮件转发控制（smtp relay）
应用层功能	1. 同步频率设置 2. 邮件备份 3. 多域同步 4. 信头重写 5. 公共邮箱 6. 邮件过滤插件
操作系统	windows2000/2003/2008,linux,, freebsd,Solaris,Aix,HP-UX
硬件配置	CPU：一个英特尔至强四核处理器 内存：2G 硬盘：200GB【500 网关用户标配】 网卡：2 块千兆网卡
应用软件	TurboGate V4.3.0

二、系统部署

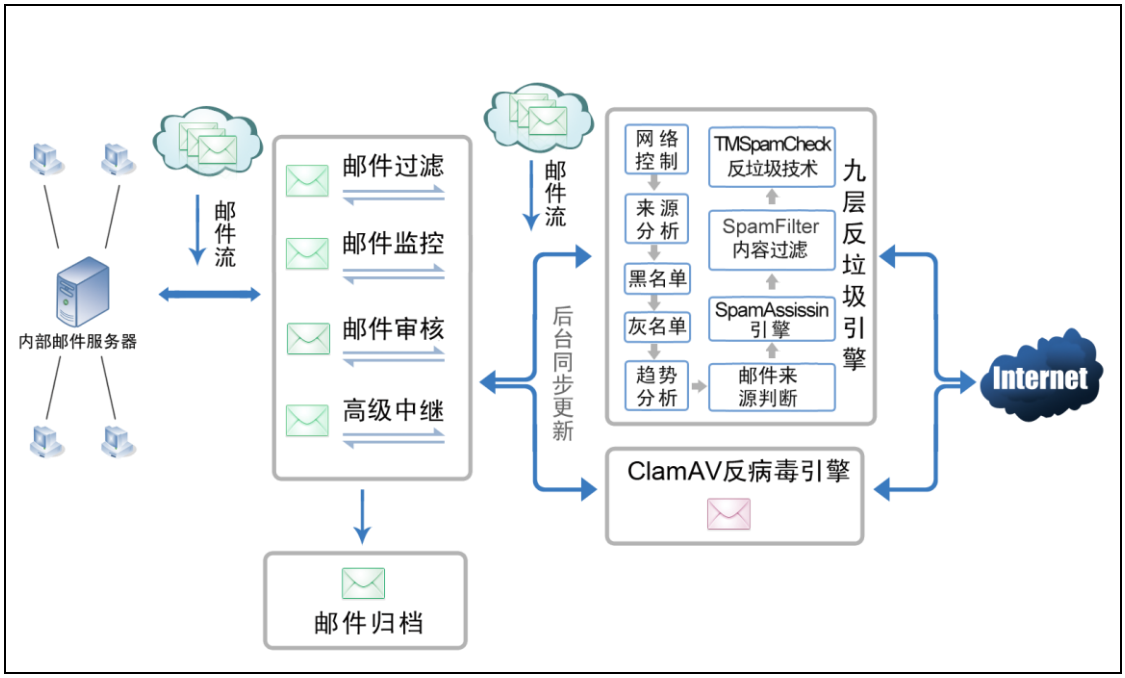
（一） 网络拓扑图



【内部用 lotus 邮件服务器示例】

内部邮件服务器和电子邮件网关系统可部署到同一台服务器上，也可分开部署在不同服务器上。邮件服务存储邮件数据、提供电子邮件收发请求的入口，电子邮件收到用户的请求后，自动将请求转发给电子邮件网关系统处理。实现内外网隔离，一方面加强了内网的安全性，一方面实现了对内网邮件的轻松管理。

（二） 工作原理图



（三） 安装方式

■ **准备条件：**

① 直接部署在邮件服务器上（cpu 要求 PIII 以上，512M 内存，硬盘在 40G 以上），也可安装在独立服务器上。

② IP 地址（使用现有 IP 地址）

③ 独立域名（使用现有的独立域名）

④ TurboGate 邮件网关系统

■ **部署过程：**

① 直接在邮件服务器或者独立服务器上安装 TurboGate 邮件网关系统，并给网关系统分配一个合法的固定 IP 地址或者使用花生壳绑定动态 IP 地址，并重新分配一个内网 IP 给邮件服务器。

② 把原来指向电子邮件系统的 MX 记录，重定向到 TurboGate 邮件网关。

③ 在 TurboGate 邮件网关配置 SMTP 路由，投递到电子邮件服务器。

部署完成后，外界无论是正常邮件、恶意攻击还是垃圾邮件，均由 TurboGate 邮件网关进行过滤，然后再从邮件安全网关将正常邮件投递到内部电子邮件系统。这样，TurboGate 邮件网关就成为了外界电子邮件通向内部邮件系统的唯一通道，为内部邮件系统提供了可靠的安全屏障。

三、设计架构

TurboGate 电子邮件网关结构图如下。

面对国内巨大的用户群体，邮件系统的高可用性、高可扩展性是极其重要的。Java 在跨平台、开放性、扩展性方面具有先天优势，因此，基于 J2EE 构建大容量的邮件应用系统也就成为很好的技术选择

邮件系统在当今社会，作为一种基础通讯平台，已经不单纯是简单收发邮件，而是成为互联网各种应用的核心，承载越来越重要的应用。中国人口众多，上网人数逐年剧增，使用邮件也日益频繁。邮件系统从建成的那一天起，就面临升级的压力。如何设计一个结构良好的大容量邮件系统，对于系统稳定性、可靠性，对于日后的升级维护有着至关重要的作用。

TurboGate 作为一个在邮件领域不断成长的产品，最终希望打造一个坚固的、高度可扩展的、容易管理维护的大容量分布式邮件系统。为保证系统的稳定可靠，需要在硬件、操作系统、核心 MTA、应用层在内的每一个环节都稳定可靠才行。硬件通常选取知名品牌服务器，稳定性、可靠性都有保障，差别不大。

操作系统选择 windows,Linux, 针对邮件系统的特点，内核需要特殊调整：如打开文件数（open files）、stack size 、max user processes 等。除了操作系统核心外，系统只加载必须的软件，屏蔽一切不要的服务端口。

服务层选择严谨高效的 C/C++语言进行开发，保证效率同时也确保了安全性。

四、TurboGate 系统安全

（一） 电子邮件网关系统核心安全设计

广州拓波软件汲取超过 3000 家企业客户的实际应用需求，应用邮件系统行业从业十年的行业经验，基于先进的 TurboMail 邮件内核推出的 TurboGate 邮件网关产品，全面支持所有的邮件服务器品牌，它有效地补充了内网邮件系统的不足，并进一步为企业提供了更多增值管理功能。

TurboGate 邮件网关内核采用自主研发、自主知识产权的 MTA。TurboGate 的 MTA 采用 C/C++开发，和操作系统紧密结合，在稳定性和效率方面，取得最佳平衡点。同时，邮件网关系统的核心技术自主研发，促进产品的持续改进和完善，给邮件应用层不断提供澎湃的动力，确保邮件通讯系统的安全和稳定运行。

1. 智能化防范 SMTP 攻击

- ✓ SMTP 智能化反垃圾，根据发送垃圾邮件的特征，TurboGate 自动将发送频率较高的 ip 地址加入智能化反垃圾列表，防止垃圾邮件的蔓延。
- ✓ 具有 SMTP 超时限定，防止 SMTP 半连接攻击，具有较好的防 DDos 攻击能力。
- ✓ 可以控制用户发送邮件的频率和 SMTP 登录情况。
- ✓ 具有 SMTP 防盗号功能，根据盗号的行为特征，如果有盗号嫌疑就立即锁定账户，防止盗号的发送。
- ✓ 用户身份验证采用高强度加密算法，支持 MD5 不可逆加密。
- ✓ 拒绝口令探测，垃圾/病毒邮件攻击者为了获得用户的口令，以达到获取商业信息或登录服务器或获取中继转发的权限的目的，常采用字典攻击的方法连接服务器，TurboGate 可以设置用户验证尝试次数，超过登录验证次数后自动锁定账号。
- ✓ 拒绝恶意攻击，采用巨量空邮件、大邮件轰炸等恶意针对邮件服务器的攻击。TurboGate 可设置邮件最大体积，超过指定体积后拒绝接收，也可以通过过滤规则直接拒绝恶意攻击邮件。

2. 邮件管理安全

- ✓ 邮件审计：使用智能邮件过滤器，根据核心关键字对进行邮件布控。
- ✓ 邮件归档：内嵌专业邮件归档模块和全文检索模块，实现安全管理历史邮件，也可以进行灾难性恢复。
- ✓ 邮件审核：通过邮件的各种条件设置规则，邮件在发送或接收前就进行审核，只有审核通过的邮件才能正常收发，从而最大程度的保证邮件内容的安全性和邮件传输的可控制性。 此外，还支持多级审核。

✓ 邮件监控：根据条件对指定用户收发的所有邮件做监控，将邮件发送到指定邮箱中。

3. 数字签名和传输数据加密

基于先进 PKI-CA 的安全机制，采用标准的 SMTP/SSL、S/MIME 协议，满足企业、军队、企业、个人在 Internet 上安全收发电子邮件的需求，保证信息传递的安全。TurboGate 邮件网关的加密安全性能特点。

✓ 数据加密功能

对邮件进行高强度的加密和解密以实现数据的保密。

✓ 抗抵赖功能

邮件的数字签名（鉴别）实现发件人认证和不可抵赖；

返回带数字签名的回执实现收件人不可抵赖。

✓ 防篡改功能

完整性校验功能防止信息传输过程中被篡改。

✓ 访问控制功能

通过安全邮件代理和证书来实现对用户强身份认证，给用户划分不同权限规则检验功能。通过安全邮件代理对邮件进行过滤。

✓ 日志和审计功能

通过分级日志系统来记录系统日志，并进行审计。

✓ 证书管理功能

提供用户管理、更新联系人和证书功能。

✓ 用 RSA 密钥算法，支持标准 PKI－CA 系统

支持国密办批准认可的加密算法。

✓ 支持多种硬件密码平台

采用公开密钥和对称密钥相结合的密钥体系。

（二） 防止用户被盗号外发垃圾邮件功能

为什么单位的邮件系统收发突然变得这么慢？

为什么无法收发了？

为什么在我没有发邮件的情况下却收到了大量的退信？

……

当系统发生这样的情况时，请注意：您的邮件服务器系统可能是被垃圾邮件发送者劫持来大量群发广告邮件了，用户无法收发邮件、网络带宽被大量堵塞、服务器 IP 被列入垃圾邮件黑名单。

1. 原因调查

帐户被盗用发垃圾邮件主要情况有以下几种：

① 帐户密码设置过于简单，很多邮件用户由于疏忽，设置了一个简单的帐户密码，这种密码很容易被基于字典的破解技术破解。

② 用户使用 Outlook ，foxmail 等邮件客户端收发邮件，如果用户的客户端没有安装杀毒软件，一旦用户的操作系统中了盗取邮件帐户的木马病毒，邮件帐户密码就很容易被盗取。

③ 用户在其他网站使用帐户加常用密码注册帐户，如果这些网站的资料泄露，就会导致邮件帐户密码的泄露。

以上几种情况是常见的帐户密码泄露情况，但是一旦帐户密码泄露，影响的不只是一个帐户，而是整个邮件服务器的正常运作。

2. 如何预防

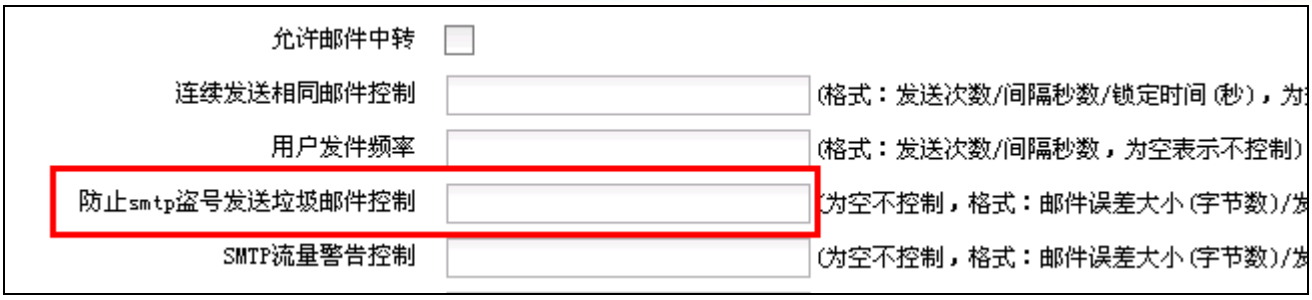
无论系统采用如何先进的防盗号技术，最重要的还是要加强用户的安全意识，从根本上杜绝此现象，例如采用复杂度高的密码，避免使用包含用户名或者纪念日之类的数字作为密码，定期修改邮箱密码等等措施。TurboGate 邮件网关系统在防盗号上，做了诸多预防措施和设置，从源头上防止垃圾邮件发送者的侵袭。

① 防止 SMTP 盗号

用户邮箱被利用发送垃圾邮件，总是会依据一定的时间频率频繁发送差不多大小的垃圾邮件，根据垃圾邮件发送的特点，TurboGate 邮件网关系统会自动扫描用户发邮件状况，在检测到用户有可能频繁发送垃圾邮件时，能自动锁定账号，及时堵截垃圾邮件的发送，保证其他用户邮件的正常收发。

系统设置

系统管理员 postmaster 登录后台管理→系统设置→SMTP 服务



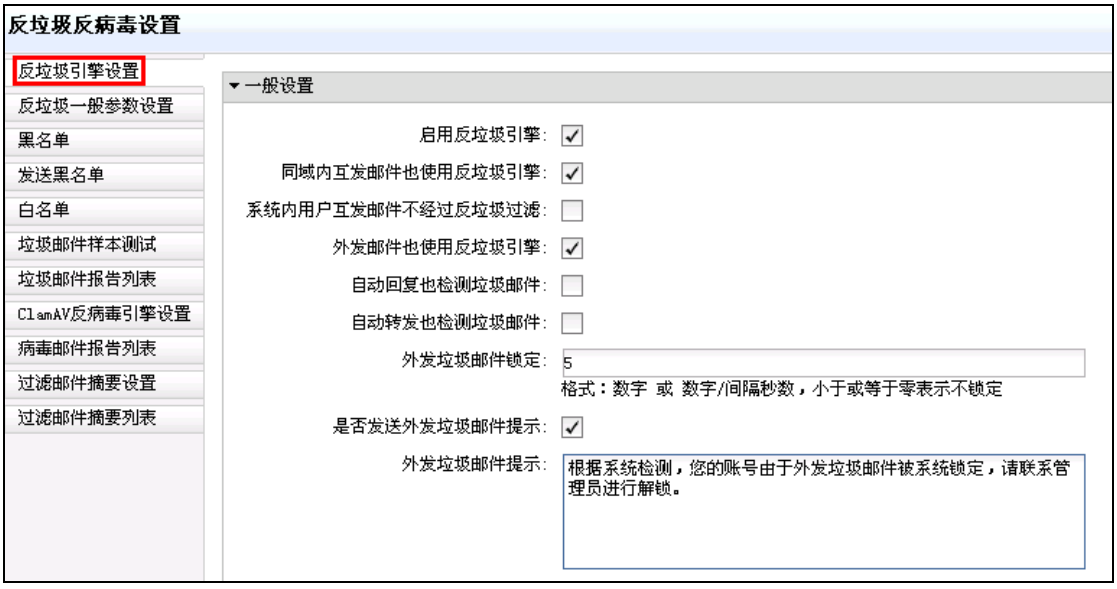
系统管理员可以根据自己企业的实际情况，通过检测用户定期发送邮件的频率和邮件大小的情况，来判定用户账号是否已被利用来发送垃圾邮件。一旦判定用户已被利用发送大量垃圾邮件，该用户账号将被锁定。该用户需要向管理员申请解锁并修改邮箱密码。

② 外发邮件使用反垃圾引擎

通过 TurboGate 邮件网关系统反垃圾引擎，判断系统用户外发的邮件是否为垃圾邮件。若判断为垃圾邮件，可通过邮件网关系统发送“外发垃圾邮件提示”给该用户，及时提醒用户邮箱的使用情况。另外，若外发垃圾邮件达到一定的次数，将自动锁定该用户邮箱账号，避免继续外发垃圾邮件。

系统设置

系统管理员 postmaster 登录后台管理→反垃圾/反病毒→反垃圾引擎设置



锁定例子

网关系统管理员 postmaster 登录后台管理→系统监控→SMTP 盗号发送垃圾邮件帐号列表

一旦用户邮件账户被锁定，该用户将不能在邮件客户端如 outlook、foxmail 等使用该邮件账户发送邮件。此时邮件客户端会提示：

系统管理员可根据实际情况，设置“外发垃圾邮件锁定数”，以及外发垃圾邮件提醒邮件的内容。用户被锁定后，需要向管理员申请解锁并修改邮箱密码。

3. *如何解决*

如果预防措施失败，内部邮件服务器已经被垃圾邮件发送者入侵，并被转发大量垃圾邮件，这时候系统管理员可以采取一些操作解决问题。

企业邮件服务器被利用发垃圾邮件，一般是因为两种情况：

- 邮箱用户密码被盗，垃圾邮件发送者利用被盗账户去发送垃圾邮件；
- 邮件系统设置了允许中转功能。

针对这两种情况，首先系统管理员必须确定是哪种，再对症下药。

① 如果邮箱用户密码被盗，可以登录 TurboGate 邮件网关系统后台管理，查看服务器队列。

登录后台→系统监控→服务器队列查看

通过查看服务器队列，如果发现队列不正常，例如队列里排列着几千封甚至几万封邮件，并且大部分邮件的发件人都是来自同一个账号，那可以肯定该账号的密码已经被盗，并被利用。正常的服务器队列，只有几十封，最多几百封邮件。

解决方法：找出被盗的账户名称，修改账户密码，尽量提高密码的复杂度，防止再次被破解密码，删除该账户在服务器队列里的所有邮件，就可以解决问题。

② **允许中转：系统管理员通过查看服务器队列，发现队列里存在大量的邮件，并且都不是来自同一个账户，那就是被利用中转发送垃圾邮件了。**

登录后台→系统设置→SMTP 服务

解决方法：把“允许邮件中转”的勾取消，再删除服务器队列里的所有邮件，禁止垃圾邮件发送者再利用邮件服务器转发垃圾邮件。

企业如何防止邮件服务器账号被利用来发垃圾邮件，应先从加强用户安全意识做起，注重密码安全和防 SMTP 盗号，方方面面，防的滴水不漏，让垃圾邮件发送者无洞可钻。

(三) TCP/IP 网络层安全防范机制

很多其他品牌邮件网关系统由于 TCP/IP 网络层安全防范机制导致系统运行不稳定，攻击者通过垃圾邮件字典攻击瞬间发送大量的垃圾邮件可以使网关系统崩溃。

TurboGate 的解决方案：

- ✓ 具有连接速率控制，在业务峰值时仍保有良好效率，不发生拥堵、宕机。
- ✓ 具有 SMTP/POP3/IMAP 来自同一 IP 访问频率和最大同时访问数控制，有效防止连接攻击。
- ✓ 具有 SMTP/POP3/IMAP 超时限定，防止 SMTP 半连接攻击，优秀的防 DDos 攻击能力。
- ✓ 具有完善的系统运行监控功能，可实时监控 webmail 在线用户、队列、 SMTP 、POP3、IMAP 会话、web 服务器信息、系统信息，可随时掌控系统运行状况。

(四) 系统监控

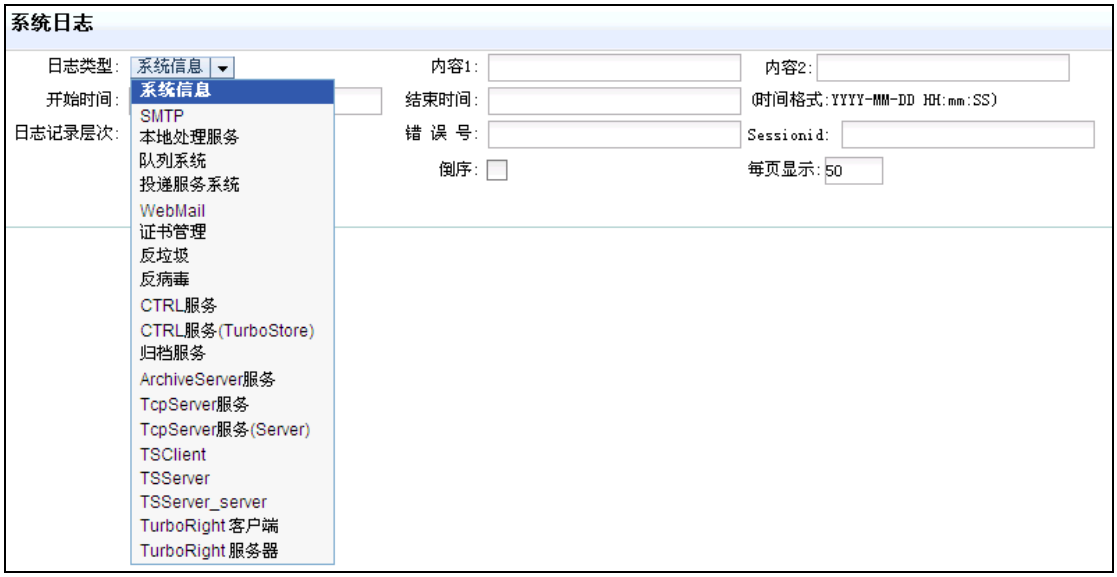
TurboGate 拥有优秀的系统监控功能,可以让管理员实时地直观地观察系统运行的各项指标，从各项指标中监控系统的运行情况，发现异常时及时处理问题。

TurboGate 的系统监控功能是纯 Web 图形化监控模式，包含以下内容：

（五） 日志查看

良好的日志查看功能是网关系统维护的必备条件，它可以在事后还原系统的使用过程，尤其是产生故障时可以迅速地定位故障发生的过程。与别的邮件网关产品的简单的系统日志功能（非对系统运行记录全面日志）相比，TurboGate 的日志查看功能非常强大，它分层级记录日志，在每个层级里又按照不同的属性进行分类记录。

系统日志详细地根据各类型服务进行分类，方便管理员查询日志。



作为网关，TurboGate 可以实现 8 大功能。

✓ 反垃圾邮件	✓ 邮件监控
✓ 反病毒邮件	✓ 邮件审核
✓ 邮件中继	✓ 邮件归档
✓ 邮件过滤	✓ 统计分析

一、反垃圾

（一） 垃圾邮件的恶劣影响

由于电子邮件能够方便快捷地传递信息，并且成本极低，所以常被滥用于传播各种信息，例如广告，色情，政治敏感信息等；许多非法信息邮件，如法轮功邮件等，往往更常见的发送对象是企业集团、政府、高校及科研院所等机构。大量的垃圾邮件给用户带来极大麻烦，甚至有可能产生不良的影响。

① 占用网络带宽。造成邮件服务器拥塞，进而降低整个网络的运行效率。

② 增加破坏机械设备的可能。垃圾邮件通常都可能携带危险的病毒、蠕虫，对电脑硬盘造成威胁。

③ 侵犯收件人及收件人所在公司的隐私权，侵占收件人及收件人所在公司的信箱空间，对有用电子邮件的抵消。

④ 耗费公司员工的时间、精力和金钱。一般来说，人们需要至少 10 秒钟来判断收到的邮件是否为垃圾邮件。如果每天收到几十份垃圾邮件，就得花大约 10 分钟的时间来处理它们。

⑤ 有的垃圾邮件还盗用他人的电子邮件地址做发信地址，严重损害了该人和其所在公司的信誉。

⑥ 错失正常邮件。正常邮件容易被大量的垃圾邮件所淹没，用户在处理过程中容易漏掉正常邮件，从而对业务产生影响，甚至丢失项目。

⑦ 妖言惑众，骗人钱财，传播色情等内容的垃圾邮件，已经对现实社会造成了危害。

（二） 垃圾邮件特征

① 从目前收集到垃圾邮件发送特点来看，主要有以下几点：

② 密集发送，大批量向同一域名不同用户发送垃圾邮件，这样会节省发送时间。

③ 伪装来源。

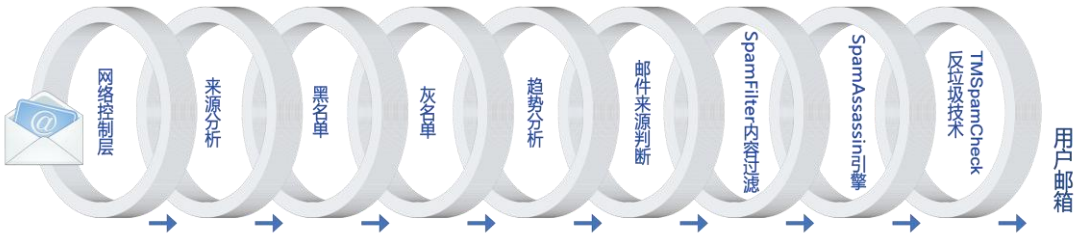
④ 内容大部分涉及非正常渠道销售的产品，如：假发票，性药品，各类培训课程等等。。

⑤ 邮件内容采用混淆技术，以躲过反垃圾系统。

⑥ 把发送时间设为未来时间，使得垃圾邮件显示在邮件列表开头。

（三） TurboGate 九层反垃圾引擎

TurboGate 系统内嵌九层反垃圾邮件引擎，反垃圾/反病毒模块都能自动升级和更新，内嵌反垃圾邮件模块，一方面可以提高邮件数据的传输效率，另外一方面，对于判定为垃圾邮件的邮件，TurboGate 系统自动投递到普通用户的垃圾邮件箱，同时存放到管理员的垃圾邮件列表，供管理员进一步处理。TurboGate 邮件网关系统的反垃圾引擎包含了多种现今流行的反垃圾技术，例如黑名单、白名单、灰名单、规则过滤等，但不同于其他邮件系统， TurboGate 采用九层反垃圾过滤技术，根据不同垃圾邮件特点采用不同技术，综合分析垃圾邮件，同时为每种特征打上垃圾分值，根据综合评分判断是否为垃圾邮件，真正做到准确率高，误杀率低。



TurboGate 系统同时支持发信认证(smtp-auth)、黑名单和系统级垃圾邮件过滤功能，为用户邮箱提供三重保护功能。用户可以随时从国内反垃圾邮件组织获得黑名单列表文件，导入邮件网关系统。从而使网关管理员从被动变为主动。TurboGate 系统黑名单功能支持模糊匹配，可以屏蔽一个域如@usa.com ，也可以只屏蔽域内的一个用户如 spam@usa.com 。提供多种方式的垃圾邮件过滤功能，避免邮件服务器成为垃圾邮件中转站。

第一层：网络控制层

经验分析，发送垃圾邮件的服务器一般都会同时大批量的向某些域的多个帐号发送垃圾邮件，对于这些发送垃圾邮件方式，可通过设定一定网络访问频率控制进行有效的阻隔，TurboGate 提供了两种设置方式对付这种攻击，并可自动把发送垃圾邮件的 IP 归为垃圾 IP（SpamIP）列表。

通过 smtp 服务层把明显的发送垃圾邮件的 smtp 连接拒绝，大大减轻后台投递系统和反垃圾引擎的负载。

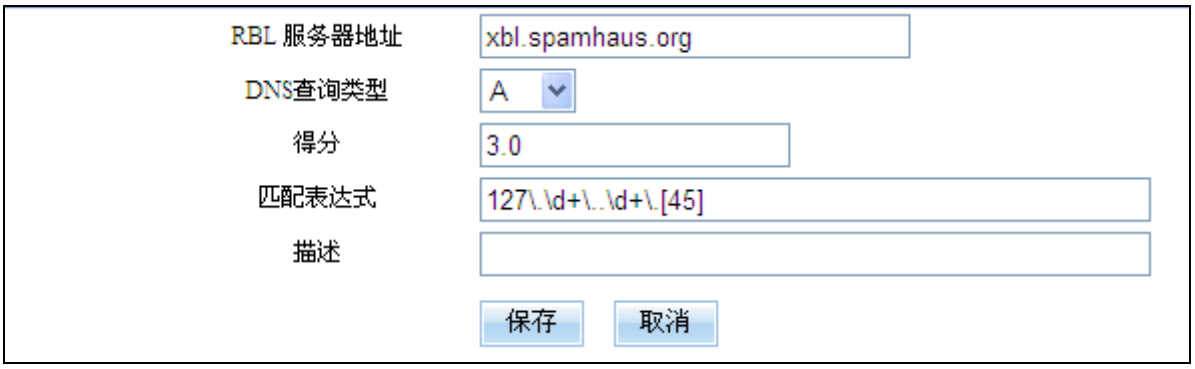
第二层：来源分析

根据垃圾邮件发送者 IP 的地理位置，与 APNIC 的 IP 信息库核对结果，看来源是否真实，如果真实则通过，否则可能为可疑邮件，由于 IP 来源无法伪装，所以这个反垃圾策略比较有效。

第三层：黑名单

通过黑名单，TurboGate 系统设置屏蔽任何一个 IP,一个网段；也可以屏蔽任何一个发信人，一个域。

实时黑名单(RBL)主要通过利用互联网公开的 rbl 资源判断垃圾邮件的可能性。目前 RBL 一般都通过 DNS 查询的方式提供对某个 IP 或域名是否是垃圾邮件发送源的判断。另外，由于国外大多数 rbl 都对来自中国的 ip 有“歧视”，所以我们并不能完全依靠 rbl 来判断一封邮件是否是垃圾邮件，只能根据 rbl 查询结果判断邮件是否垃圾邮件的可能性。可设置以下参数定制 rbl:



- RBL 服务器，指定 RBL 查询域名后缀。
- DNS 查询类型，根据具体的 RBL 要求指定 DNS 查询记录类型。
- 匹配表达式，指定 RBL 查询结果的匹配模式，表达式格式采用 perl 正则表达式，如果为空，则表示如果可查到 RBL 结果，就表示符合条件。

目前所知比较有效的 RBL 服务器为：

- xbl.spamhaus.org
- bl.spamcop.net
- cbl.anti-spam.org.cn
- cdl.anti-spam.org.cn

第四层：灰名单

灰名单技术源于：http://www.greylisting.org/ 。

灰名单技术其基本假设是：病毒和垃圾邮件，通常都是一次性的，如果遇到错误，不会重试。

一些发垃圾邮件的软件，这些软件基本上都不会对邮件服务器返回的错误做出任何重试，而只是简单的在日志里记录发送失败而已。而病毒引发的邮件风暴则更加不会识别邮件服务器返回的错误，因为这些病毒仅仅是简单的发送邮件，发送时根本不理会服务器的状态。

Greylist 的设计大体上是基于一种重试的原则，即第一次看到某个 IP 要想给某个收件人发信，那么它将简单的返回一个临时错误（4xx），并拒绝此请求，正常的邮件服务器都会在一段时间内（如半小时）重发一次邮件。 greylist 发现还是刚才同样的 ip 地址和收件人，认为此 ip 是来自合法服务器的，予以放行。如果是非正常的邮件，那么或者将永远也不再进行重试，或者会疯狂重试，但由于间隔太近，而遭拒绝。因此，greylist 只要设置一个合适的放行间隔，就可以在很大程度上对这类垃圾邮件有着良好的免疫能力。greylist 的一大特点就是不会丢信，正规的邮件服务器认为 4xx 错误只是临时性、软性的错误，会隔一段时间重试，因此邮件还是可以投递成功。但 greylist 的一大缺点即使延迟（delay），延迟从几分钟到几个小时不等。对于一些对邮件及时性很强的客户， greylist 可能不是一个很好的选择。

第五层：趋势分析

趋势分析原理为，所有垃圾邮件都有目标指向，比如：卖药广告邮件都会在邮件内容里指定卖药的电话、邮件或网站，如果不指定这些信息，发送垃圾邮件也就没有意义了。趋势分析法就是通过分析邮件里的电话、邮件或网站链接内容，通过匹配判断他的指向从而判断邮件是否是垃圾邮件。

第六层：邮件来源判断

主要通过分析邮件的来源，如：发件人 ip ，发件人，发件域，等内容，来判断垃圾邮件的可能行。

第七层：SpamFilter 内容过滤

通过邮件内容关键字分析，可为符合内容分析结果的邮件打上相应的垃圾邮件评分。这类规则的判断条件类似系统的过滤规则。可参考过滤规则设定来设定过滤评分内容，同时我们也会通过收集客户反馈的垃圾邮件特点整理成规则内容，定期通知客户更新。

第八层：SpamAssassin 引擎

SpamAssassin 是一个由 Apache 开发的一个著名的反垃圾引擎，TurboGate 邮件网关系统完整的集成了 SpamAssassin 反垃圾引擎。邮件网关系统提供了一个名为 SA-Server 的 SpamAssassin 反垃圾服务器，邮件网关系统通过把需要进行反垃圾分析的邮件提交给 SA-Server 进行分析。

SA-Server 在 Windows 平台上可通过 SA_Server 服务启动，在 Unix/Linux 平台上可通过 sa/sa_server.sh 脚本启动。SA-Server 默认端口为 8700，可通过直接修改 sa/sa_server.pl 修改这个端口。

可通过网关系统中的，反垃圾\反病毒－》反垃圾引擎设置 中的 SpamAssassin 中的相关设置进行 SA-Server 的服务配置。

其中：

- 启用 SpamAssassin ， 指定是否启动 SpamAssassin 反垃圾检查
- SpamAssassin 服务器地址，指定 SA-Server 服务器地址，默认为本机。
- SpamAssassin 服务端口，指定 SA-Server 服务器端口，默认为 8700.
- 最大 SpamAssassin 检查线程数，指定最大的连接 SA-Server 服务数，可根据系统的复杂进行适当调整。

第九层：TMspamcheck 引擎

垃圾广告商总是在想方设法的绕开上述拦截与屏蔽方式，“作案”手段不时更改，TurboGate 通过定期巡查以及与客户建立沟通制度，广泛搜集现行的各类垃圾邮件，并逐个分析，将垃圾邮件源列入 TMchecklist，所有的正式客户都将得到同步更新的服务，再度查杀漏网之“邮”。

具体设置如下：

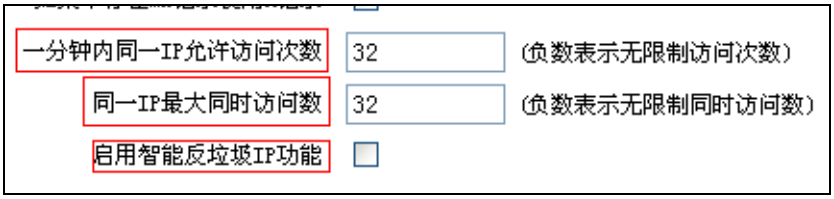
通过控制同一 IP 连接频率控制大批量发来的垃圾邮件。

通过统计分析，我们发现很多发送垃圾邮件的 smtp 连接具有以下特点。

- 同一 IP 同时的 SMTP 连接数非常大。
- 同一 IP 在一段时间，SMTP 连接频率非常大。

一般出现这两种情况，都表示源发件人非常有可能发送垃圾邮件。通过设置以下这两个参数可控制这类型的 SMTP 连接，从而截断发送垃圾邮件的源头：

进入管理员=>系统设置=>SMTP 服务中有如下所示：



设置同一个 IP 每分钟内访问次数，同时启用“启用智能反垃圾 IP 功能”，把符合以上两个条件的 IP 地址自动加入系统的智能反垃圾 IP 列表（SmartSpamIP），当以后系统碰到这些 IP 的连接的时候，直接拒绝。

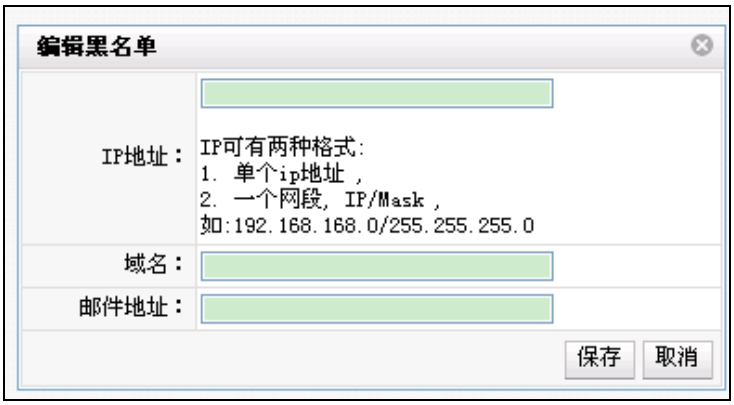
可通过：

系统监控=>智能反垃圾 IP 列表

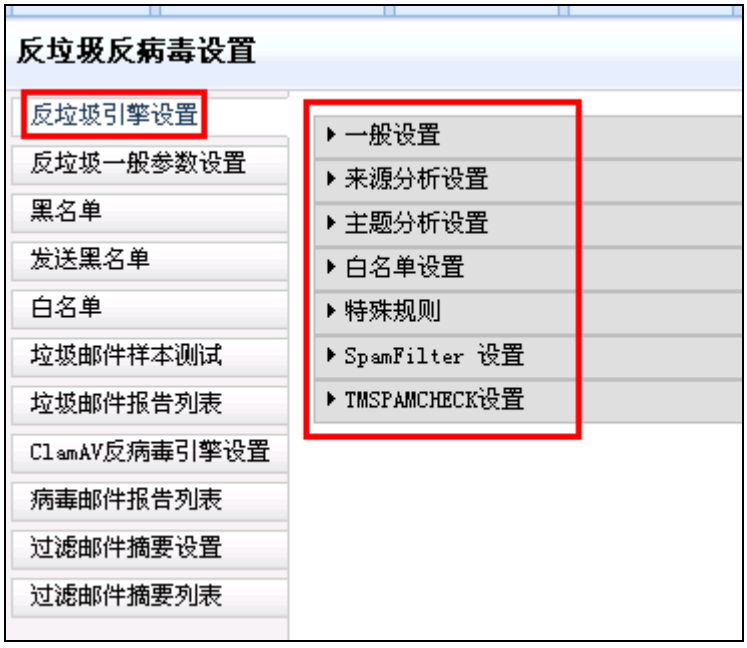
查看系统目前智能反垃圾 IP 列表。

① 如果确认某些 IP、域名或者发送者确实为垃圾邮件来源，可以在把这些来源地址直接加入系统黑名单，这样来自这些地址的垃圾邮件就直接被拒绝了。

可通过“反垃圾\反病毒设置”=>“黑名单”



② 对于广泛的垃圾邮件可通过对反垃圾、反病毒设置，管理员=>反垃圾\反病毒=>反垃圾引擎设置如下图所示：



更多有关反垃圾反病毒详细的设置，请联系拓波技术人员进行安装网关系统试用。

注：垃圾邮件内容评分规则可以在后台自动更新。

二、反病毒

在日常的网络应用中，电子邮件成了我们常用的工具，其发信速度和加载附件的功能为我们提供了很大的便利。但是正因为电子邮件的便利，使得它成为了病毒传播的一种搭载形式。

（一） 邮件病毒特征

“邮件病毒”其实和普通的电脑病毒一样，只不过由于它们的传播途径主要是通过电子邮件，所以才被称为“邮件病毒”。“邮件病毒”主要是为了让用户的计算机感染病毒，或者是成为黑客手中的肉鸡。“邮件病毒”除了具备普通病毒可传播性、可执行性、破坏性、可触发性特征之外，还有如下几个特点：

① 感染速度快：在单机环境下，病毒只能通过 U 盘或光盘等介质，从一台计算机传染到另一台，而在网络中、则可以通过诸如电子邮件这样的网络通讯机制进行迅速扩散。根据测定，针对一台典型的 PC 网络在正常使用情况，只要有一台工作站有病毒，就可在几十分钟内将网上的数百台计算机全部感染。

② 扩散面广：由于企业邮箱的邮件不仅仅在单个企业内部传播，这直接致使“邮件病毒”的扩散不仅快，而且扩散范围很大，不但能迅速传染局域网内所有计算机，还能通过将病毒在一瞬间传播到千里之外。

③ 清除病毒困难：单机上的计算机病毒有时可通过删除带毒文件，格式化硬盘等措施将病毒彻底清除。而企业中的计算机一旦感染了病毒，清除病毒变得非常困难，刚刚完成清除工作的计算机就有可能被网络中另一台带毒工作站所感染，使得邮件病毒变得非常困难了。

④ 破坏性大：网络中的计算机感染了邮件病毒之后，将直接影响网络的工作，轻则降低速度，影响工作效率，重则使网络及计算机崩溃，资料丢失。

⑤ 隐蔽性：邮件病毒与其他病毒相比，更隐蔽。一般来说，邮件病毒通常是隐蔽在邮件的附件中，或者是邮件的信纸中，这一定程度上会加速病毒的泛滥，也增加了查杀病毒的难度。

（二） TurboGate 反病毒引擎

TurboGate 邮件网关系统内置著名的开源杀毒引擎 ClamAV，对邮件类病毒具有 99.9%的杀灭能力，同时支持嵌入式杀毒和网关杀毒自动定时更新病毒特征库。同时，TurboGate 也支持多种杀毒引擎，将所有的邮件病毒都拦截在邮件网关系统上，不会影响到内部邮件系统的使用，极大减轻内部邮件系统的压力。

1. ClamAV 杀毒引擎简介

Clam AntiVirus 是一款 UNIX 下开源的 (GPL) 反病毒工具包，专为邮件网关上的电子邮件扫描而设计。该工具包提供了包含灵活且可伸缩的监控程序、命令行扫描程序以及用于自动更新数据库的高级工具在内的大量实用程序。该工具包的核心在于可用于各类场合的反病毒引擎共享库。

2. 主要特征

- ✓ 命令行扫描程序
- ✓ 快速、支持按访问扫描的多线程监控程序
- ✓ 支持 Sendmail 的 Milter 接口
- ✓ 支持脚本更新和数字特征库的高级数据库更新程序
- ✓ 支持病毒扫描程序 C 语言库
- ✓ 支持按访问扫描 (Linux® 和 FreeBSD®)
- ✓ 每天多次更新病毒库 (特征库总数请参阅主页)
- ✓ 内置了对包含 Zip、RAR、Tar、Gzip、Bzip2、OLE2、Cabinet、CHM、BinHex、SIS 及其它格式在内的多种压缩包格式的支持
- ✓ 内置了对绝大多数邮件文件格式的支持
- ✓ 内置了对使用 UPX、FSG、Petite、NsPack、wwpack32、MEW、Upack 压缩以及用 SUE、YOda Cryptor 和其它程序模糊处理的 ELF 可执行文件和便携式可执行文件的支持
- ✓ 内置了对包括 MS Office 和 MacOffice 文件，HTML、RTF 和 PDF 在内的主流文档格式的支持

注：TurboGate 支持反病毒库永久免费升级，保证系统病毒库处于最新状态。

三、海外邮件发送

（一） 海外中继服务

邮件的顺利快速收发是一个邮件系统最基本和最重要的功能，邮件收发不顺严重影响着使用者的工作效率，是否保证全球通邮，是判断一套邮件系统是否可用的基本条件。

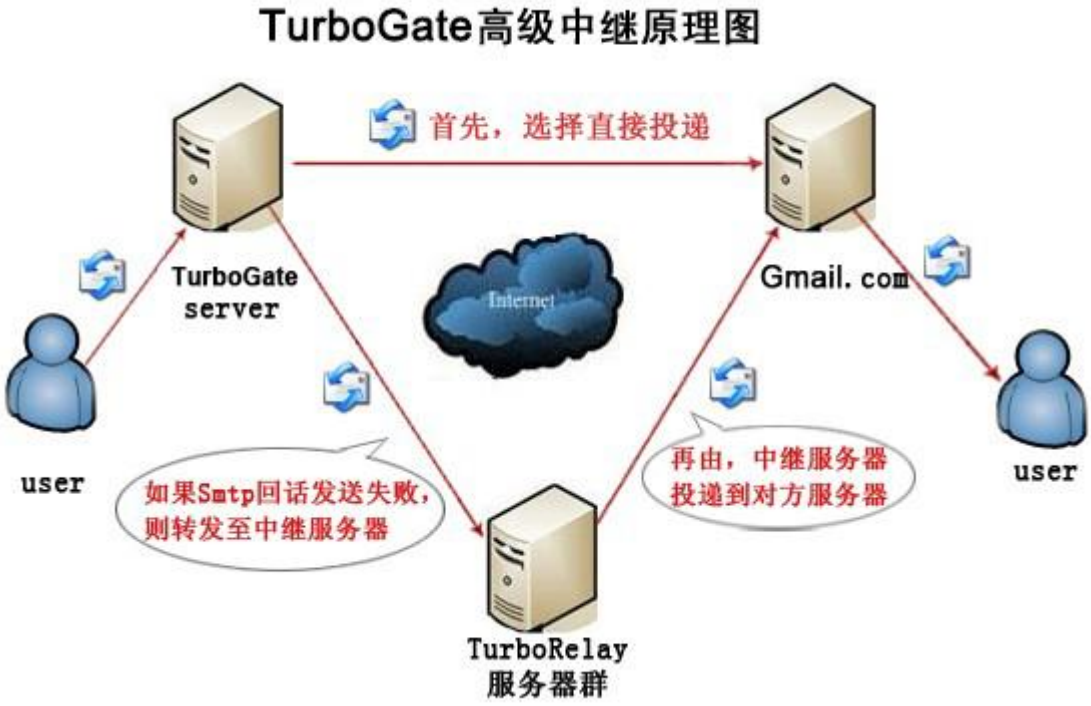
近年来，广大用户对邮件系统的反馈，出现最多的抱怨就是与大型的邮件服务提供商，特别是国外的，例如 hotmail、yahoo、sina 之间的通信障碍，经常无法将正常邮件发送出去给这些邮箱。甚至在中国国内，都经常会发生邮件投递失败的情况。究其原因主要是因为中国的垃圾邮件过度泛滥，中国国内 IP 信誉度不高，大量的 IP 和邮箱域名进入了国际邮件组织的黑名单（如 Spamhaushuo 或 FortiGuard 等），中国用户发出的邮件被当成垃圾邮件被自动屏蔽。

TurboGate 邮件网关系统在企业原有内部邮件系统的基础上，为客户提供邮件中继功能，并采取 DKIM 技术，大大提高用户发往海外邮箱的成功率，多方面保障了企业邮件的全球通邮。

1. TurboGate 中继网络

TurboGate 拆耗巨资在亚洲（香港）、欧洲（法国）、大洋洲（澳大利亚）、美洲（美国）分别设立了中转服务器，形成了一个高级的邮件中转网络。广州拓波软件科技有限公司在国际服务器设备的投入，以及国际邮件市场的战略定位，保证了企业内部邮件服务器的国际邮件收发。

2. 中继工作原理



① 邮件第一次正常发送不成功，拓波网关会自动利用中继进行再次发送，提高中继使用效率和非国外邮件投递的效率。

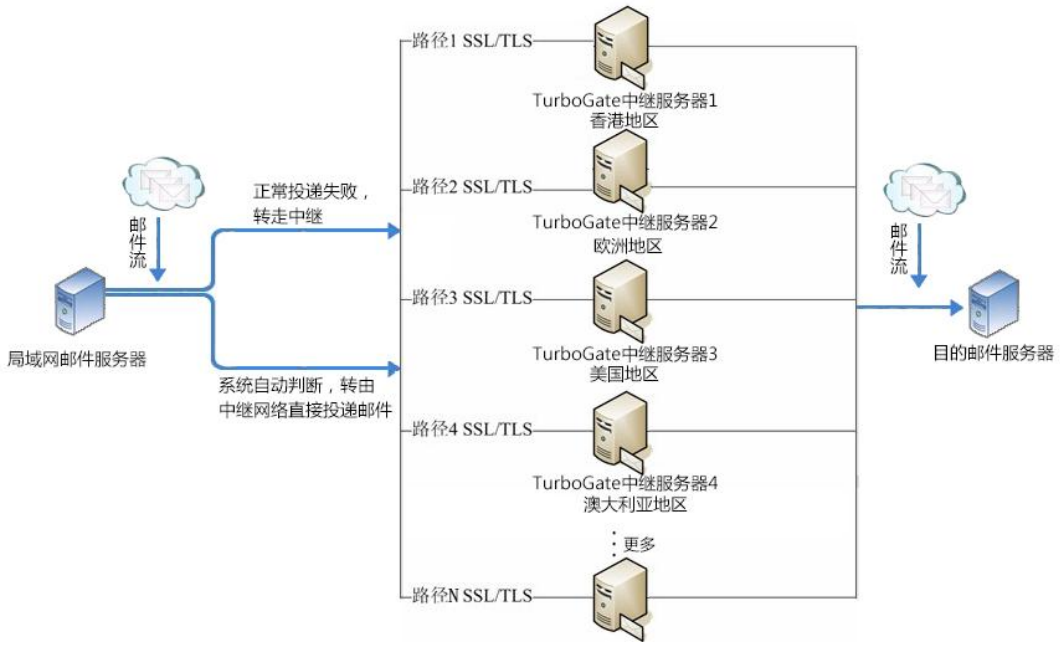
② 拓波网关可以设定发送失败判断条件，指定某些暂时发送失败的邮件直接通过中继发送。

③ 拓波网关可以指定收件域、收件箱、收件 ip、发件箱、发件域、发件 ip 第一次发送直接使用中继发送，此方法可提高海外邮件直投效率。

④ 拓波网关对所有中继邮箱进行排序，当使用第一个中继邮箱仍然无法成功投递后，系统自动转用下一个中继邮箱进行投递。全球网状的服务器布局，保证用户顺利的发送邮件。

高级中继体现在邮路选择上的灵活。其他产品一旦使用中继功能后，因技术上的原因使得所有邮件都无法从本地服务器收发，全部通过中转服务器，大大加重了系统负担，造成延时、阻塞、退信等等现象。而 TurboGate 可以根据实际情况灵活处理，不同邮件区别对待。

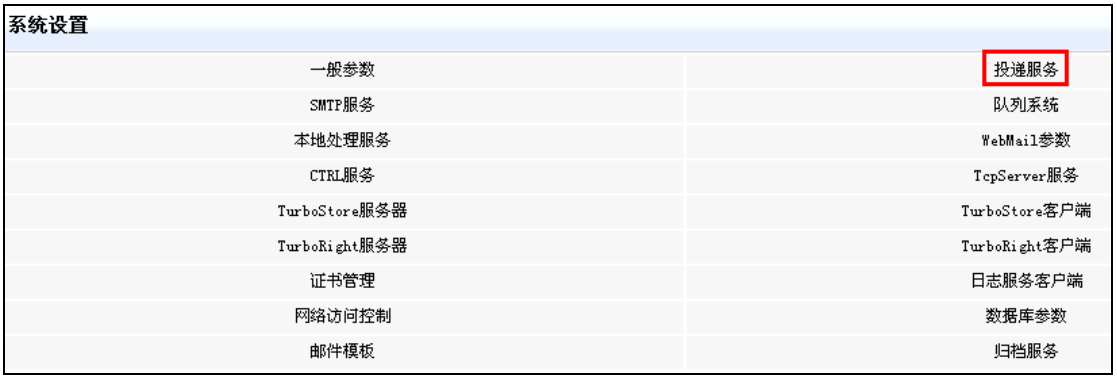
3. 拓波全球中继分布图



4. 中继操作设置

TurboGate 设置邮件中继方法

① 使用 web 登录管理员帐户，点击“系统设置”进入系统设置界面如图：

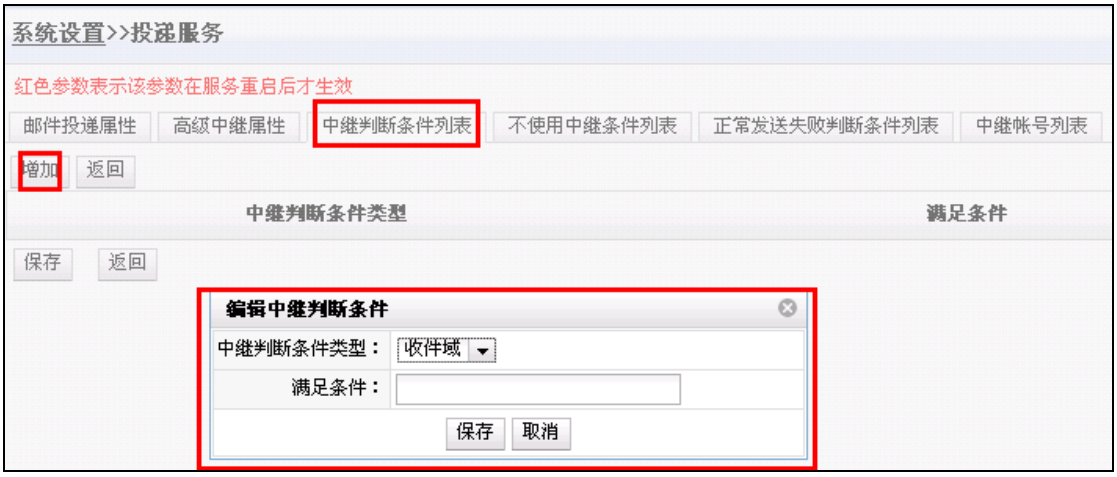


② 点击“投递服务”编辑中继功能设置。

- ✓ 中继使用方式：选中“当正常发送失败后，使用中继”；
- ✓ 根据判断条件使用中继：选中；
- ✓ 中继最大投递尝试次数：一般不设置用默认值，邮件量很大时可以根据情况调值；
- ✓ 中继最大同时投递数：一般使用默认值，邮件量很大时可以根据情况调值；

③ 编辑中继帐户列表(这里使用 foxmail 邮箱来做说明，如 quest@foxmail.com)，点击“中继帐号列表”进入中继帐号列表点击“增加”如下图：

④ 点击“中继判断条件列表”后进入下一页面点击“增加”编辑收件域：



✓ 中继判断条件类型：选中收件域；

✓ 满足条件：输入发送邮件失败的的域名；

⑤ 点击“正常发送失败判断条件列表”进入后点“增加”：

这里是根据发送失败，日志返回错误原因，一般填入“IP”、“blacklist”就可以了，有特殊情况可及时联系拓波。

（二） DKIM 技术——进一步提高海外邮件发送成功率

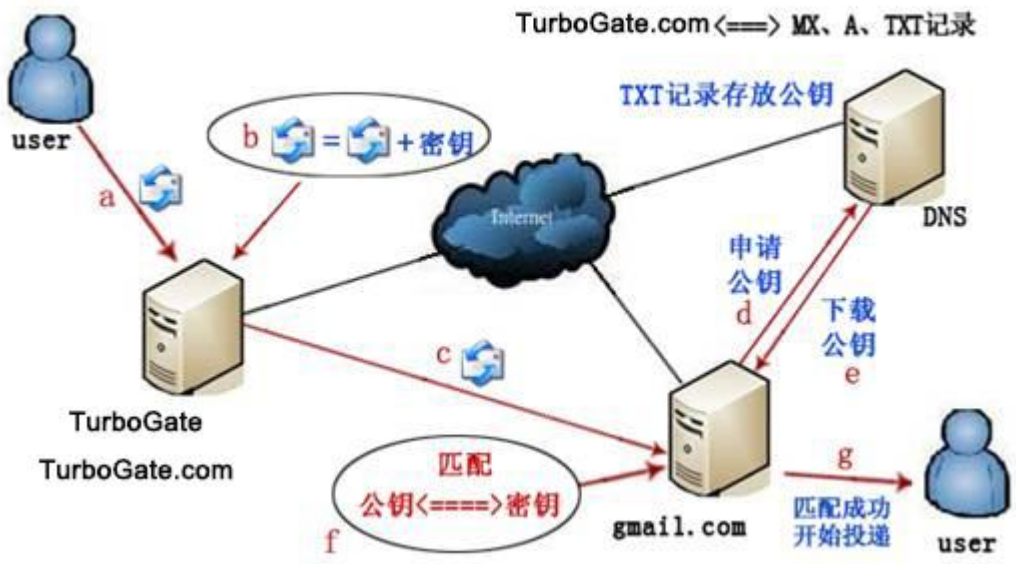
DKIM 是电子邮件验证标准：域名密钥识别邮件标准 DomainKeys Identified Mail 的缩写。

DKIM 由互联网工程任务组（IETF）开发而成；针对的目标是互联网最严重的威胁之一：电子邮件欺诈。 使用该技术后，发送方会在电子邮件的标头插入私钥，而接收方则透过 DNS 查询得到公钥後进行验证。

TurboGate 邮件网关系统提供 DKIM 功能，客户配置使用该功能后，发送邮件时在每封电子邮件上增加加密的数字标志，以支持接收方与合法的互联网地址数据库中的记录进行比较。由于 GMAIL、YAHOO、SINA、QQ 等大型邮箱系统会对收件进行 DKIM 验证，因此配置此功能后，能大大提高客户们发邮件至这些大型邮箱系统的成功率。

工作原理介绍：

DKIM 的基本工作原理同样是基于传统的密钥认证方式，他会产生两组钥匙，公钥(public key)和私钥(private key)，公钥将会存放在 DNS 中，而私钥会存放在寄信服务器中。私钥会自动产生，并依附在邮件头中，发送到寄信者的服务器里。公钥则放在 DNS 服务器上，供自动获得。收信的服务器，将会收到夹带在邮件头中的私钥和在 DNS 上自己获取公钥，然后进行比对，比较寄信者的域名是否合法，如果不合法，则判定为垃圾邮件。由于数字签名是无法仿造的，因此这项技术对于垃圾邮件制造者将是一次致命的打击，他们很难再像过去一样，通过盗用发件人姓名、改变附件属性等小伎俩达到目的。在此之前，垃圾邮件制造者通过把文本转换为图像等方式逃避邮件过滤，并且使得一度逐渐下降的垃圾邮件数目再度抬头。



四、邮件监控

邮件监控就是指监控指定用户发送或接收的所有邮件，将监控用户发送或接受的邮件邮件密送到指定邮箱，登录监控邮箱即可查看到被监控人的邮件列表。

（一） 应用背景

① 业务员离职，邮件被删除，业务也被随之带走。

② 担心公司业务客户资料和核心机密通过企业电子邮件外流，无法对员工邮件实施监控。

③ 业务员和客户沟通没有抄送邮件给主管，造成信息延迟。

（二） 邮件监控优点

为了保护公司机密信息的安全，对员工邮件收发行为进行规范化，TurboGate 网关系统对进出网关的所有邮件都能实现邮件监控功能，并可针对多种过滤条件进行特殊邮件的监控。

① 检查邮件进出，防止机密外泄。

② 监督用户邮件收发，了解邮件内容，以及时调整管理措施。

（三） 操作设置

TurboGate 网关系统的邮件监控的邮箱账号有两种选择：

① 可在 TurboGate 邮件网关系统上建立监控邮箱账号，所有的被监控邮件都会发送到该账号上。

② 可用外部邮箱账号作为监控邮箱，所有的被监控邮件都会发送到该外部邮箱账号上。

具体设置如下：

① 登录管理员进入管理员界面点击“邮件监控”。

② 点击“接收邮件监控”进入接收邮件监控设置列表。

③ 点击“增加”设置 abc@domain1.com 帐户监控 domain.com 域下帐户所接收的所有邮件，设置如下：

被监控收件人：输入被监控的收件人的邮箱（可输入多个账号，以分号分隔）如需监控某个域下面所有用户的邮件，可以输入@域名，如：@domain.com 表示监控整个 domain.com 域的邮件。

接收监控邮件邮箱：输入监控人邮箱，监控到的邮件会发送到监控邮箱的收件箱内。可以是 TurboGate 用户，如果设置了 TurboGate 用户，登录 TurboGate 用户后,在功能列表区的“监控邮件列表”可以查看到被监控人的邮件发送/接收邮件列表；也可以是邮件系统用户邮箱或其他外部邮箱。

注：发送邮件监控同上。

五、邮件审核

（一） 应用背景

TurboGate 网关系统通过多种关键字和属性的条件设置过滤规则，将符合规则的邮件邮件在发送或接收前做审核操作，只有审核通过的邮件才能进行正常收发，从而最大程度的保证邮件内容的安全性和邮件传输的可控制性。通过邮件审核功能，帮助企业打造一个更安全的 IT 环境，免除数据外泄的风险。此外，审核规则可根据多种条件进行设置，灵活多变，方便企业对一些敏感内容和数据的邮件进行控制和审核。

（二） 操作设置

邮件审核的账号，只能使用 TurboGate 邮件网关系统的账户作为审核人，因为邮件审核是在 TurboGate 系统内部执行的。审核人可以通过网页登陆 TurboGate 邮件网关系统进行邮件审核。

① 网关系统管理员任意设立审核人。

② 可根据发件人、收件人、主题、附件名、内容、邮件大小、邮件时间、是否含附件等条件做设定过滤条件，设置需要审核的邮件。

③ 可以选择对进出网关的接收邮件或者发出邮件进行审批。

④ 可以对部门邮件和组织邮件进行群体审批。

⑤ 审核人能收到待办审核的提醒，及时处理相关事项。

⑥ 审核功能能与短信提醒和手机邮箱配合使用，保证紧急事情能够得到及时处理，降低隐性风险和损失。

⑦ 支持多人审核，并支持审核提醒，对逾期还未审核的邮件，系统可设置发送审核提醒给审核人邮箱。

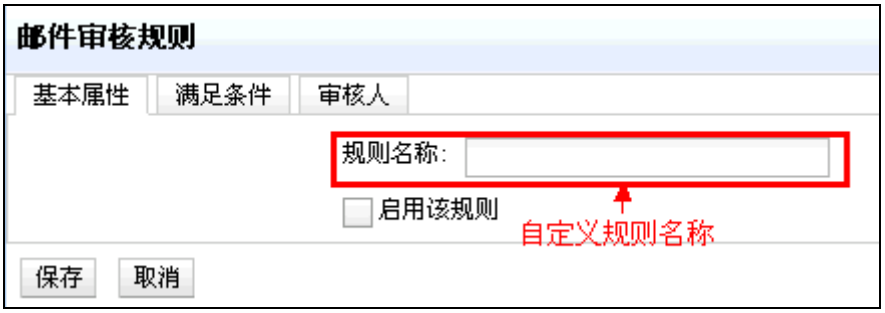
具体设置：

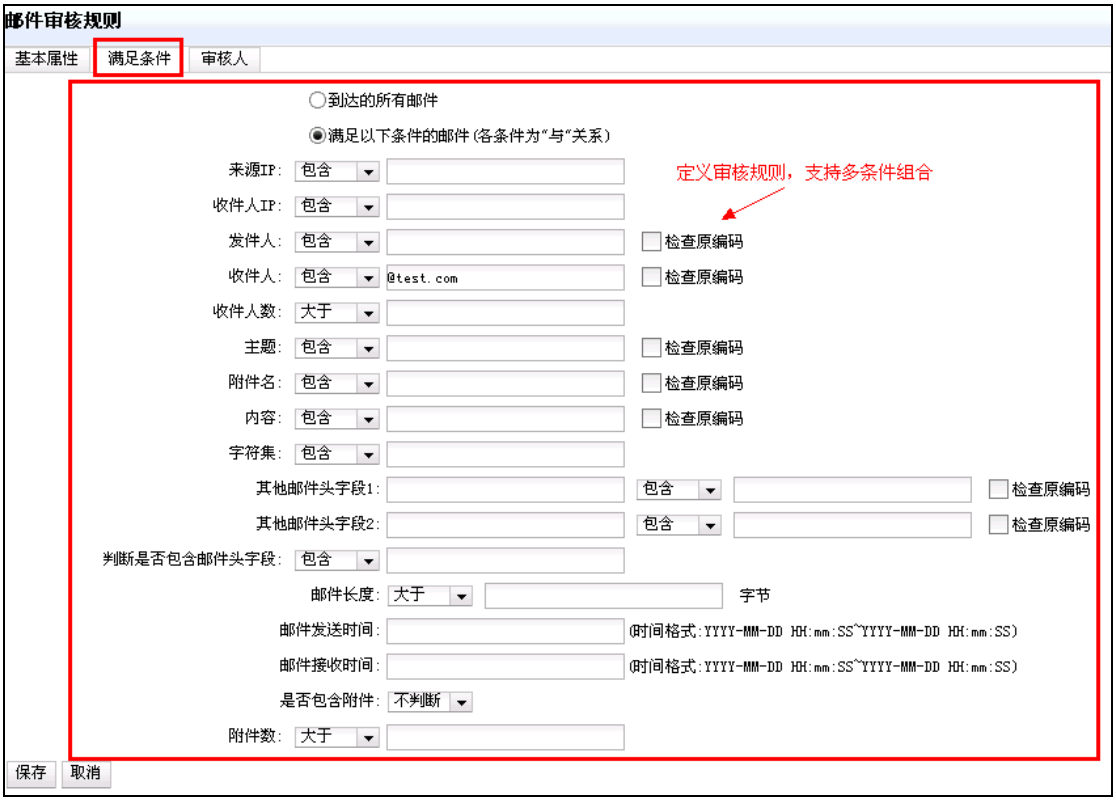
邮件审核必须是在 TurboGate 邮件网关系统下面建立一个单域如 turbogate.org.cn，再建立一个 admin@turbogate.org.cn 用户。

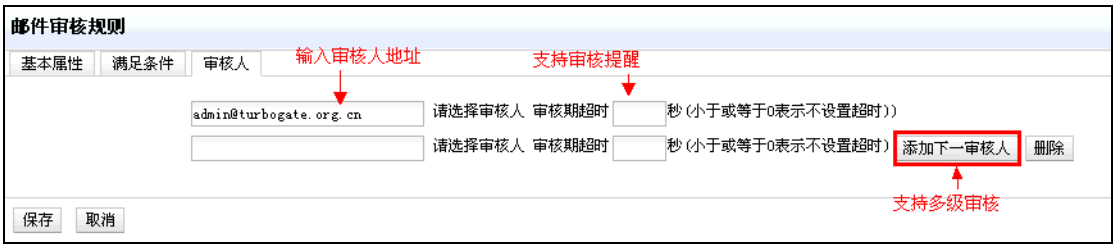
① 登录管理员进入管理员界面点击“邮件审核”。

② 点击“邮件审核规则列表”。

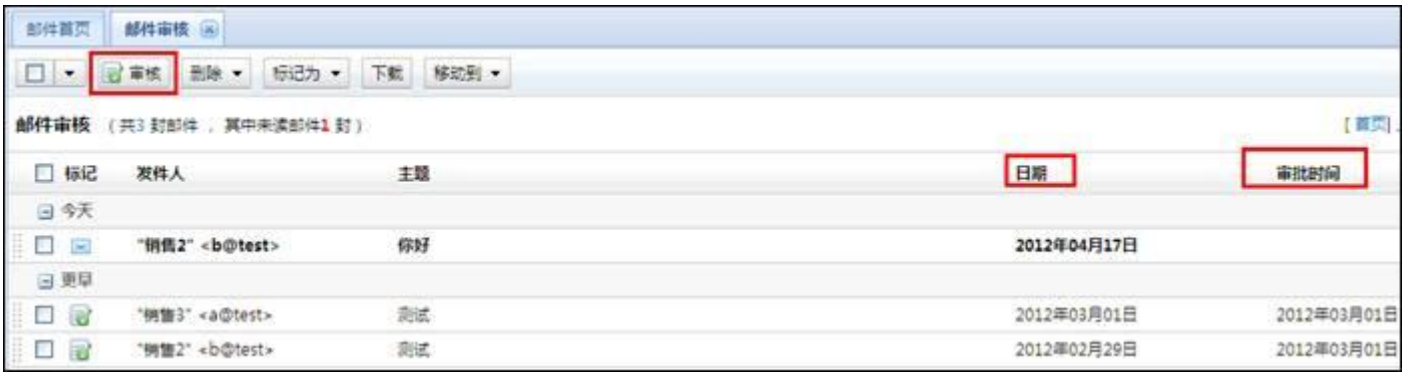
③ 点击“增加”添加审核规则名称、定义审核规则和审核人地址。







④ 审核规则建好后，被审核人发送或接收邮件时，登录审核人邮箱，左边多出“待审批邮件”此功能。



⑤ 点击主题进入内容查看内容是否通过，通过就击“审批”即可。

六、 邮件过滤

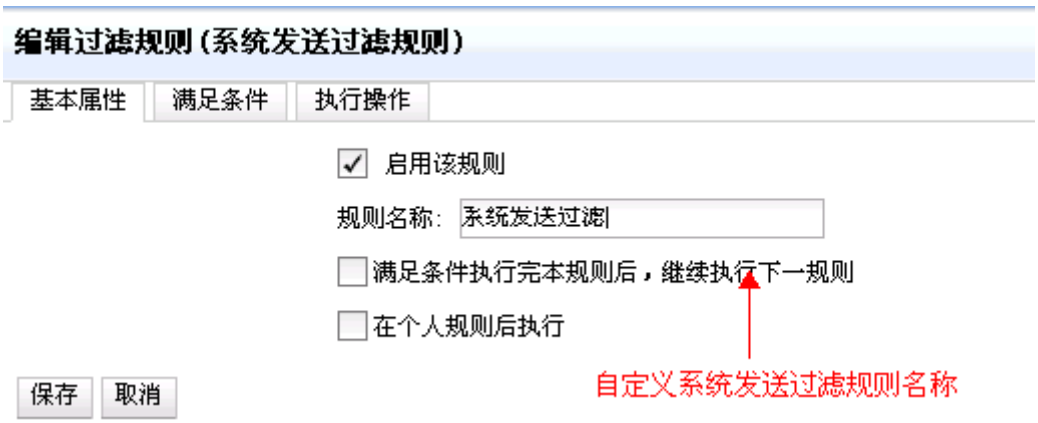
（一） 应用背景

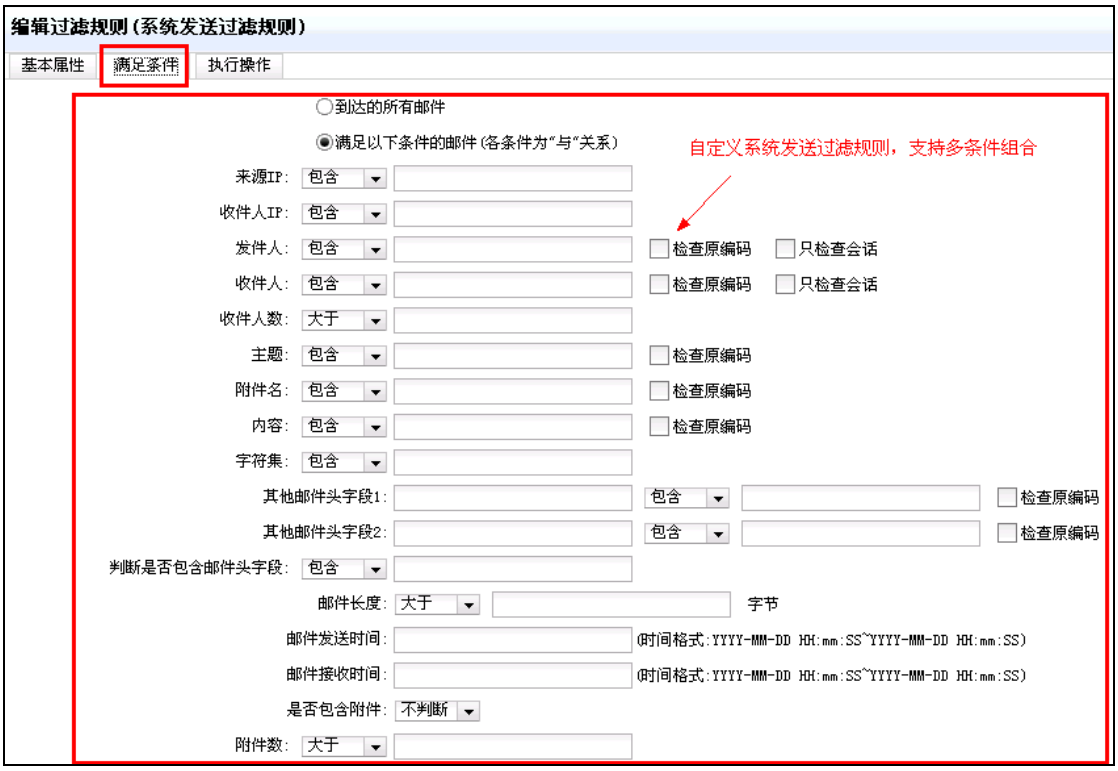
TurboGate 邮件网关可对所有进出网关系统的邮件进行过滤，可以对符合过滤规则的邮件执行指定操作。一方面，企业通过网关过滤功能杜绝掉企业不需要的骚扰邮件或者本行业内的敏感邮件等；另一方面，防止企业内部员工通过内部邮箱泄露公司机密信息或者超出权限发送违规邮件等。

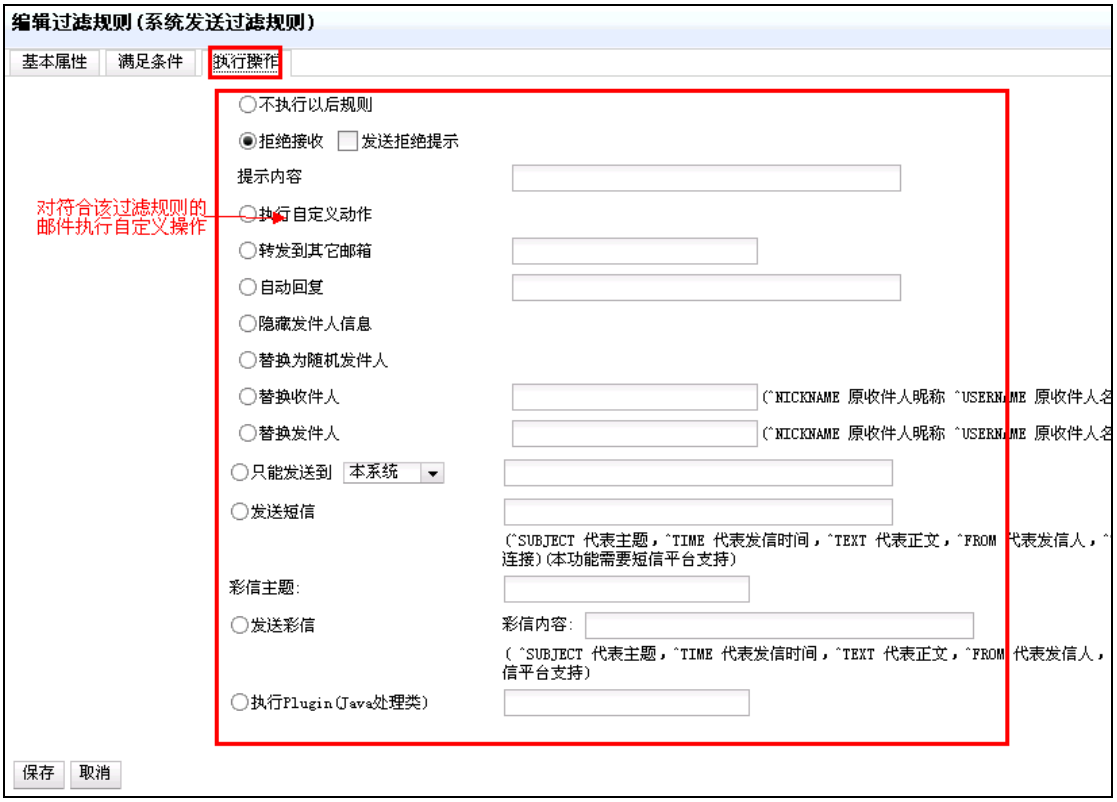
（二） 操作设置

过滤规则可通过各种条件来执行不同操作，可根据自己情况而定，操作如下：

过滤规则可分为系统发送过滤规则和系统接收过滤规则，以下为设置系统发送过滤规则的例子：



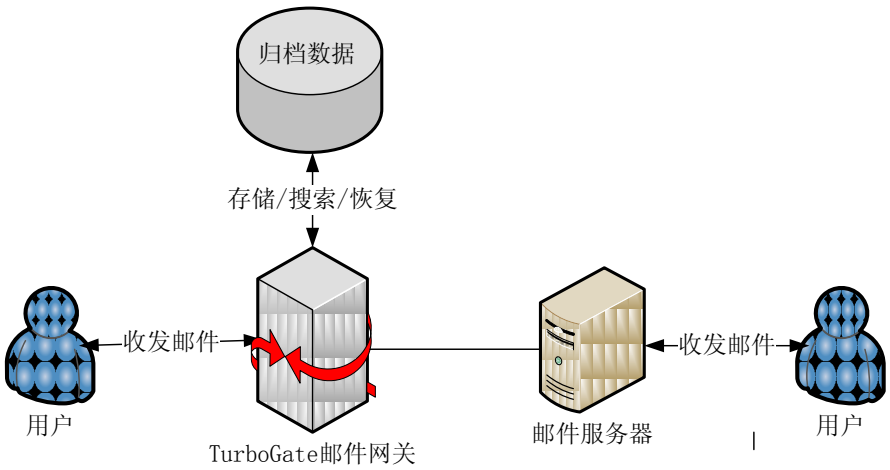




对符合过滤规则的邮件，管理员可以自定义不同的执行操作：拒绝接收（可选择是否发送拒绝提示）、转发到其他邮箱、自动回复、隐藏发件人信息、替换为随机发件人、替换收件人、替换发件人、限定只能发送到范围（本系统、域、邮件地址或指定 IP 范围）、短信或彩信通知等。

七、 邮件归档

邮件归档是指对邮件数据进行在线归档、分类管理、长期保留并允许实时搜索和访问，主要是针对海量数据的应用，是对数据进行有效的迁移和管理,其结构图如下所示



(一) 应用背景

从企业内部管理而言，邮件归档是实现同步邮件备份，通过把邮件数据存储到独立的存储硬件上，可以对邮件数据进行更安全的管理。当需要查询历史邮件时，可以快速地获得所需邮件，从而达到邮件管理的目的，也可实现灾难恢复。

从外部要求来看，数据安全存档成为必然的趋势。随着利用电子邮件作为法庭证据的趋势日益明确，美国和欧洲一些国家相继制订了一系列法规。美国和欧洲的众多政府法规（例如《Sarbanes_Oxley_Act_of_2002》法案）已经明确提出公司内电子邮件的电子发现和法规遵从方面的规定，要求上市公司保留所有业务记录，包括电子记录和邮件在内，不少于 5 年。这意味着企业必须很好地管理和保留企业所有的电子邮件，以应付未来的电子邮件查询需求，不然很可能给企业带来风险。

无论是从内部还是外部环境看，建立邮件归档系统，都是企业未来必然发展趋势，越来越多的企业逐步关注到这一领域。

(二) TurboGate 邮件归档

在邮件网关中实现邮件归档功能，所有经过 TurboGate 邮件网关系统收发的邮件都将进行同步备份，并建立即时全文索引，即使邮箱用户彻底删除了某些邮件，由于邮件已被备份，仍能在 TurboGate 邮件网关系统上轻松检索调出，邮件归档功能就像是一个持续运作的复印机，来往所有邮件全部被复印留底。

归档功能在 TurboGate 邮件网关系统上实现和管理，释放了内网邮件服务器，不用承受日积月累的邮件数量的压力。

① 遵从 Sarbanes-Oxley 法案，美国证监会 SEC 及其他的相关规定，满足法律上对电子文档的访问和保存及诉讼证据搜索的要求。

② 支持管理员、个人或者设置特定用户快速搜索并查看归档邮件。

③ 支持模糊搜索。

④ 支持高级搜索，可以通过发件账号、收件账号、主题、发件人、收件人、内容、附件名、日期、归档类型等子条件，快速全文搜索到自己所需的目标邮件。

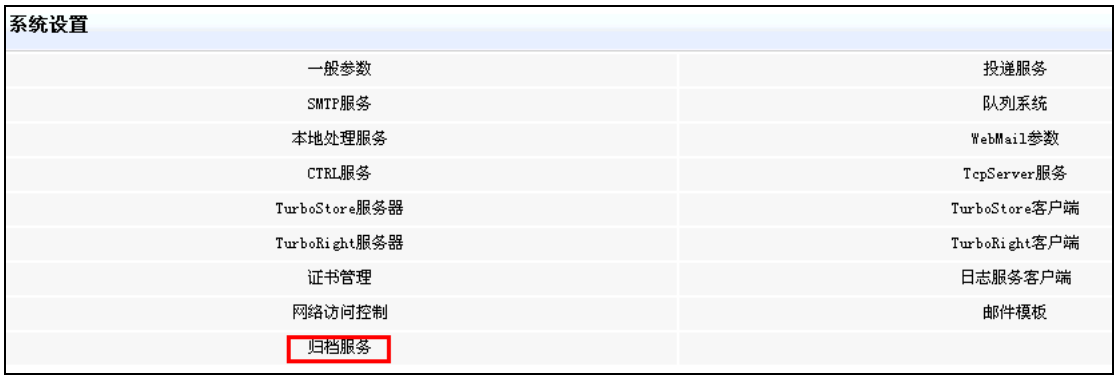
⑤ 同步备份归档邮件，相同一文件只归档一份，可达到 75%的压缩比例，大量节约存储空间。

⑥ 管理员可对网关系统内普通用户开启归档查看功能。用户在登陆自己的邮箱后，左侧邮件服务栏会出现“邮件归档”这个功能选项，可查看过去的历史邮件，并对有需要的邮件执行恢复操作。

（三） 操作设置

归档服务设置及使用

① 开启归档服务。登录管理员进入“系统设置”。



→点击“归档服务”进入开启设置页面

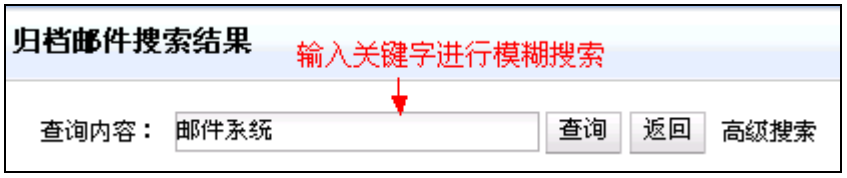
→按上图设置后点击“保存”。

② 归档使用

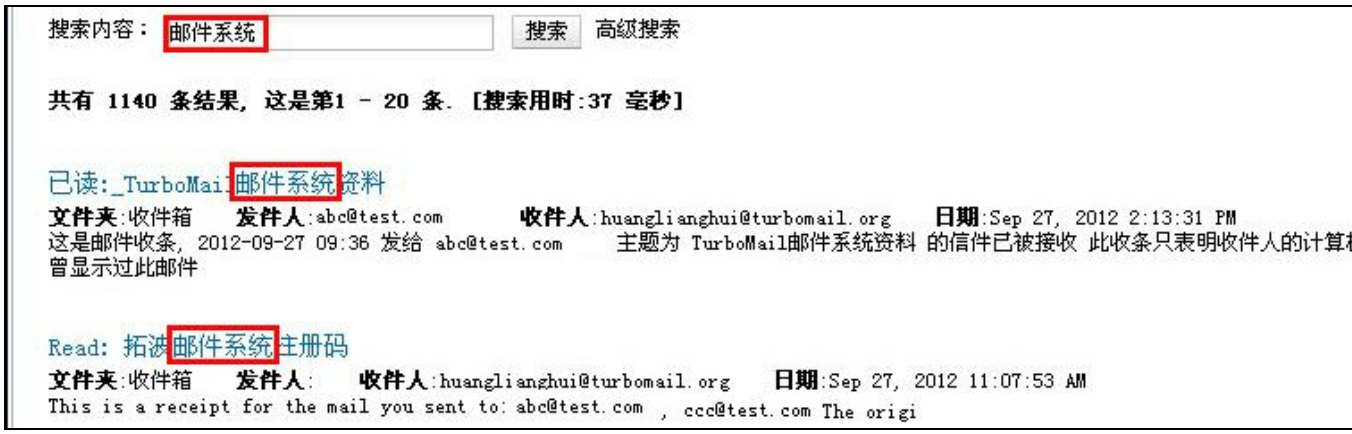
返回管理员界面，点击“归档服务”如下图

→点击“归档邮件搜索”，支持两种搜索模式：模糊搜索和高级搜索：

① 模糊搜索：



→点击“搜索”



② 高级搜索：

→点击“搜索”

对查找到的邮件，点击主题，可以直接打开此封邮件，可选择直接恢复此封邮件到用户收件箱。归档邮件恢复，可进行单个用户批量邮件查找并恢复，也可对查找到的邮件执行导出操作。

八、统计分析

统计分析模块进一步将系统的邮件进出进行汇总统计，便于管理员做各时间段之间流量的分析，它对这几个方面的提供统计报告：邮件收发情况统计、邮件日流量明细、邮件流量统计图、执行每日邮件统计。

（一） 邮件收发情况统计

（二） 邮件日流量明细

域	用户名	外发邮件数	外发邮件大小	接收邮件数	接收邮件大小	IMAP发件数	IMAP发件数大小	IMAP收件	IMAP收件大小	pop3收件	pop3收件大小	smtp发件数	smtp发件大小	被bl邮件数	被bl邮件大小	病毒邮件数	病毒邮件大小	spam邮件数	spam邮件大小	失败邮件	失败邮件大小
[illegible]	[illegible]	0	0	1	874K	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
[illegible]	[illegible]	0	0	1	874K	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
[illegible]	[illegible]	0	0	1	874K	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
[illegible]	[illegible]	0	0	1	874K	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
[illegible]	[illegible]	5	228K	3	1M	0	0	0	0	0	0	2	102K	0	0	0	0	2	59K	0	0
[illegible]	[illegible]	1	7K	2	1M	0	0	0	0	0	0	1	6K	0	0	0	0	0	0	0	0
[illegible]	[illegible]	0	0	0	0	0	0	0	0	0	0	1	1K	0	0	0	0	0	0	0	0
[illegible]	[illegible]	0	0	2	2M	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
[illegible]	[illegible]	11	1M	13	1M	0	0	0	0	0	0	4	357K	0	0	0	0	0	0	0	0
[illegible]	[illegible]	0	0	1	874K	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
[illegible]	[illegible]	0	0	1	874K	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
[illegible]	[illegible]	4	334K	0	0	0	0	0	0	0	0	9	6M	0	0	0	0	0	0	0	0

[首页 | 上一页 | 下一页 | 末页 第 1/213 页 共 10644 条记录]

（三） 邮件流量统计图

电话：8620-85509396 38395469 38394823
地址：广东省广州市天河区天河路242号丰兴广场B座2501-2502号

（四） 执行每日邮件统计

售后服务

（一） 服务承诺

针对 TurboGate 产品，我们公司一年内免费为客户升级并提供技术维护服务，一年后，如果继续需要技术服务则收取邮件网关系统造价的 20%。

服务期内容：

- 邮件网关系统首页定制
- 服务期内反垃圾规则库免费升级
- 反病毒库永久免费升级
- 邮件网关系统核心永久免费升级
- 服务期内高级中继服务免费开放

技术支持服务是指保障 TurboGate 邮件网关系统稳定运行所必要的技术服务，包括系统漏洞修补、邮件收发屏蔽解决、系统重装、数据迁移等，服务方式为远程服务和现场服务。在远程技术手段（如 SSH、远程桌面、QQ 远程协助）解决不了的情况下，拓波工程师需根据故障等级的响应时限，提供现场服务。技术支持热线 7x24 小时值班。

（二） 服务支持体系的构成

1. 电话支持中心

提供 7*24 小时热线电话（020-38921969,13928708886），并建立大客户档案，工程师在线提供技术问题咨询和故障诊断。远程在线诊断和故障排除。

对于电话咨询解决不了的问题，经用户授权我们可通过电话或 Internet 远程登录到用户网络系统进行的故障诊断和故障排除。

2. 定期巡查服务

提供的全方位网络技术服务，包括对用户的定期寻查制度，即定期远程诊断，采用先进的网络检测与分析工具对系统进行诊断，提出系统优化建议与措施。专人进行客户支持。

【注】定期巡查工作由拓波公司协助完成。巡查时间为一年一次。

（三） 故障等级设定

严格按照故障等级划分标准，将邮件网关系统的故障划为四级

- 一级故障：现有的网络停机，或对最终用户的业务运作有重大影响
- 二级故障：现有网络的的操作性能严重降级，或由于网络性能失常严重影响用户业务运作。
- 三级故障：网络的操作性能受损，但大部分业务运作仍可正常工作。
- 四级故障：在产品功能、安装或配置方面需要信息或支持，对用户的业务运作几乎没有影响。

优先级的划分及处理

- 一级优先权:拓波公司将全天候调集所有必要的资源来排除故障,在 4 小时内提供解决方案或替代方法。
- 二级优先权：拓波公司将全天候调集所有必要的资源来排除故障，在 12 小时内提供解决方案或替代方法。
- 三级优先权:拓波公司将全天候调集所有必要的资源来排除故障，一般在 5 天内提供解决方案或替代方法。
- 四级优先权:拓波公司将全天候调集所有必要的资源来排除故障，一般在 7 天内提供解决方案或替代方法。