高校电子邮件系统的优化管理①

罗辉琼, 李瑞维

(华南师范大学 网络中心, 广州 510631)

摘 要: 针对华南师范大学电子邮件系统的优化管理进行研究. 介绍了校内电子邮件系统的现状, 包括系统网络部署、收信和发信流程等. 对邮件系统目前存在的运维安全问题进行了全面分析, 包括校内邮箱与国外邮箱通信畅通性较差、发信机制存在安全漏洞等问题. 最后从注册反向域名及优化发信机制等方面给出了邮件系统的整体优化方案和实施步骤. 研究表明华南师范大学电子邮件系统的优化管理, 不仅解决了系统运维安全问题、增强了用户体验, 同时也给管理员的维护管理带来了便利. 这在高校电子邮件系统的管理应用中具有一定的参考意义.

关键词: 电子邮件; 优化管理; 部署; 方案; 实施

Optimization of University E-mail System Management

LUO Hui-Qiong, LI Rui-Wei

(Network Center, South China Normal University, Guangzhou 510631, China)

Abstract: The paper studies on the optimal management of South China Normal University E-mail system. The current campus E-mail system is introduced, including system and network deployment, reception and dispatch processes. The operation and security problems of E-mail system are analyzed, including the school mailbox and the mailbox communication abroad poor, signaling mechanism exists security vulnerabilities. Finally, from the aspects of registered reverse domain name and optimization of signaling mechanism, the overall optimization scheme and implementation steps of mail system are given. Studies have shown that optimal management of South China Normal University E-mail system, not only solved the problem of system operation and safety, enhance the user experience, but also brought convenience to administrators of maintenance and management. It has a certain reference value in college E-mail system management applications.

Key words: E-mail; optimal management; deployment; program; implementation

随着互联网的飞速发展, E-mail(电子邮件)已成为Internet 应用最为广泛的一项服务, 也是个人日常工作学习生活中的必备通讯工具. 对于高校而言, 电子邮件更是学校与师生、教师与学生进行互动的重要途径. 目前大部分高校都有属于自己高校的、自主建设的邮件系统. 自建邮件服务器具有明显特点:有助于提高办公效率、增强数据安全、提高单位形象;应用及管理灵活、可根据个人所需进行相应的调整和个性化的设置等. 但高校自主建设的邮件系统在维护管理方面可能都存在不可忽视的问题, 如:垃圾邮件泛滥、邮件遭到拦截和篡改、与国外邮件通信的不畅通性、邮件帐号经常被盗成为垃圾邮件中转站等. 高校电子邮件系统的管理维护关系到整个学校的形象、与师生的日常工作学习生活也息息相关. 如何更好地优化管理校内电子邮件系统已成为高校亟待解决及长期研究的课题. 本文正是针对华南师范大学电子邮件系统的优化管理展开研究.

1 校内邮件系统的现状

1.1 网络部署

华南师范大学电子邮件系统是基于 Microsoft Exchange Server 2007[1,2]平台建设, 主要包括 4 台服务

① 基金项目:自然科学基金(2013Y2－00062)
收稿时间:2014-08-23 ;收到修改稿时间:2014-10-08

器, 其中两台服务器作为邮箱角色, 另外两台服务器作为客户访问和集线传输角色. 具体网络拓扑结构如图 1 所示.

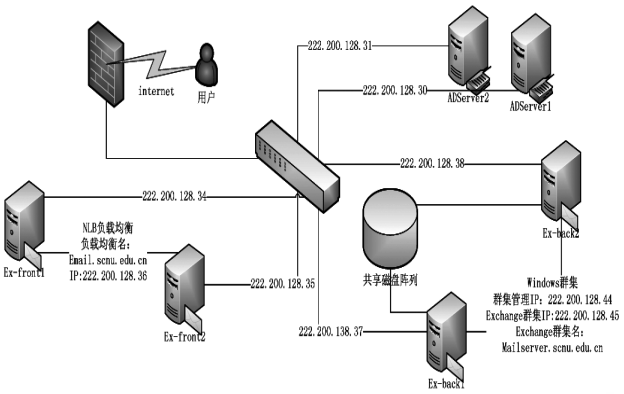

图 1 邮件系统网络拓扑图

Ex-back1 和 Ex-back2: 使用两台 HP 416653-B21 服务器 2CPU, 4G 内存;Ex-front1 和 Ex-front2:使用两台 HP 416653-B21 服务器 2CPU, 4G 内存. 四台服务器均安装 Windows Server 2003 64bit 操作系统.

Exchange Server 2007 的系统采用 Windows Server 2003 64 位操作系统, 并安装了 IIS 服务器端程序. 同时将服务器加进域并设置 DNS 地址为域控制器地址, 活动目录(Active Directory)域功能级别被设置为 2003 的纯模式. 在确保服务器可以正常访问 Internet 的情况下, 依次在服务器上安装 Microsoft.Net Framework 2.0、MMC 控制台、Microsoft Command Shell、Microsoft Exchange.

2.2 收信流程

邮件系统采用两台 EQManager 邮件安全网关[3](mg1 和 mg2)作为收信的反垃圾邮件过滤网关. 邮件 MX 记录分别指向 mg1 和 mg2, mg2 优先级高于 mg1.

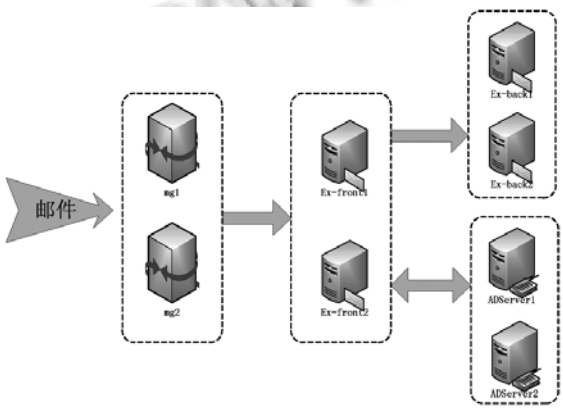

图 2 邮件系统收信流程图

目前邮件接收流程为:外来邮件首先到达邮件网关(mg1 和 mg2), 由邮件网关过滤后再发往邮件服务器前端(Ex-front1 和 Ex-front2), 然后再到达邮件后端存储(Ex-back1 和 Ex-back2), 用户信息由 AD 域服务器(AD1 和 AD2)提供. 其中客户端收信服务器为:mail.scnu.edu.cn/pop.scnu.edu.cn, 两个域名都同时指向了邮箱前端 Ex-front1 和 Ex-front2 的 IP. 具体的收信流程如图 2 所示.

2.3 发信流程

现有发信方式有两种, 分别是 web 发信方式和客户端发信方式. web 发信方式:直接从邮件服务器前端(Ex-front1 和 Ex-front2)发出, 不经过邮件网关. 客户端(outlook、foxmail 等)发信方式:可以任选邮件服务器前端(Ex-front1 和 Ex-front2)进行发信, 不经过邮件网关, 也没有对邮件服务器前端的 25 端口进行限制. 具体发信流程如图 3 所示.

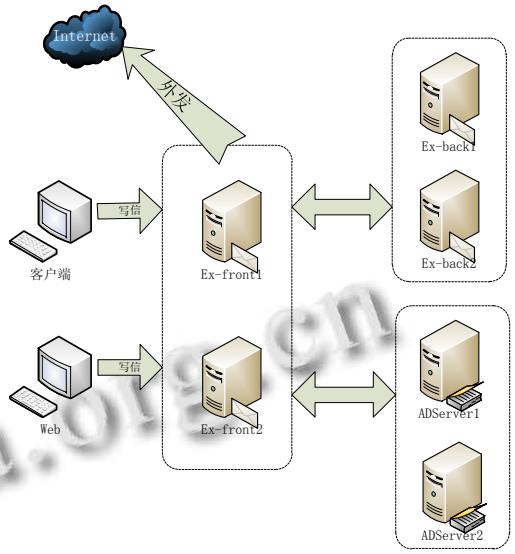

图 3 邮件系统原发信流程图

2.4 存在的问题与分析

校内自建邮件系统虽然具有明显的优势, 例如:增强了内部敏感数据的安全性、提升了学校的身份和形象、方便灵活管理及个性化设置等. 但高校自建的邮件系统普遍存在垃圾邮件泛滥、与国外通信的不畅通性等问题. 目前华师校内邮件系统同样也存在两个比较突出的问题:

一是与国外通信的畅通度较差, 校内发往国外的邮件经常出现无故丢失的现象.

二是邮件帐号经常被黑客盗用成为垃圾邮件中转

站对外发送垃圾邮件，严重影响学校的形象，而且还造成学校的邮件服务器IP地址被反垃圾邮件组织列入黑名单，从而导致发往校外的邮件经常被拒收的现象.

针对问题一，通过抓包对日志进行分析，可知大部分是由于反向 DNS 没做好，所以被拒收. 日志分析如图 4 所示.

图 4　往国外发信的日志分析图

使用校内 DNS 对邮件服务器的 IP 进行 PTR(邮件发送过程的反向地址解释)解释时显示正常，但使用校外 DNS 进行 PTR 解释时却显示失败. 通过 Trace 跟踪发现我们校内的 DNS 上对邮箱服务器的 PTR 记录完整正确，但上级 DNS 没有注册我们校内邮件服务器所在的 IP 段: 222.200.128.，即是没有把 128.200.222.in-addr.arpa.授权至我们的 DNS.

针对问题二，通过系统的检查和分析发现我们的发信流程存在安全漏洞. 邮件服务器前端(Ex-front1 和 Ex-front2)的 25 端口是对外开放的，垃圾邮件组织可以直接用 smtp 方式往邮件前端发信，无需经过网关，大量垃圾邮件过滤不了. 另外邮件服务器前端(Ex-front1 和 Ex-front2)安装的是 Exchange server 2007，该版本不能做发信频率限制等安全设置.

3　优化方案及具体实施

拟对校内邮件系统存在的问题进行整体优化调整. 优化调整的内容主要分为两大块:一个是解决校内与国外通信畅通性较差的问题;二是解决校内邮件系统在发信机制上存在的安全漏洞问题.

3.1 反向域名注册申请

调研发现校内局域网邮箱与国外通信出现经常丢失或拒收的问题也是众多高校存在的普遍问题，究其原因都是未提供 PTR(反向地址解释)记录[4,5]，从而导致国内邮件发到国外被封锁. PTR (Pointer Recore)，指针记录，是电子邮件系统中的一种数据类型，被互联网标准文件 RFC1035 所定义. 与其相对应的是 A 记录、地址记录. 二者组成邮件交换记录. A 记录解析名字到地址，而 PTR 记录解析地址到名字. PTR 记录被用于电子邮件发送过程中的反向地址解析. 当正向域名解析完成后，还应当向线路接入商(ISP)申请做反向地址解析，以减少被国外机构退信的可能性.

因此解决的办法是向上级 DNS(或者 IP 供应商)申请对我们的服务器 IP 段进行反向解释的授权. 我们的 IP 是由教育网 CERNET 分配的，可直接到 CERNET 网络信息中心(http://nic.edu.cn/)上提交 PTR 记录的申请. CERNET 网络信息中心提供了 “IN-ADDR.ARPA Template [CERNIC-021-HTML]”即 CERNIC IPv4 反向域名注册表，我们只需要根据注册表填写自己所在院校的 IP 段及域名等资料，填写好后提交申请，等待申请通过后反向域名解释生效即可.

3.2 优化发信机制

针对发信流程上存在的安全漏洞，拟对邮件系统的发信机制进行全面优化.

优化方案为:充分利用邮件网关的反垃圾邮件过滤功能[6,7]，将邮件网关加进发信机制中. 在邮件前端 Exchange 上设置外发路由到邮件网关，向外发信时首先经过邮件网关过滤，网关过滤后再向外投递. 同时限制邮件前端服务器的相关端口，禁止垃圾邮件组织直接往邮件前端发送. 由于 Exchange server 自身的特点，只能指向一台网关作外发路由. 考虑到收信过滤网关设置是 mg2 优先级高于 mg1，为均衡负载，在发信过滤网关上选择 mg1 为外发路由. 发信路由转发虽然没有实现群集，但若某台发生故障时，可以通过对 DNS 和 Exchange server 的简单设置，随时进行调整，实现快速功能转移.

优化后发信流程如图 5 所示.

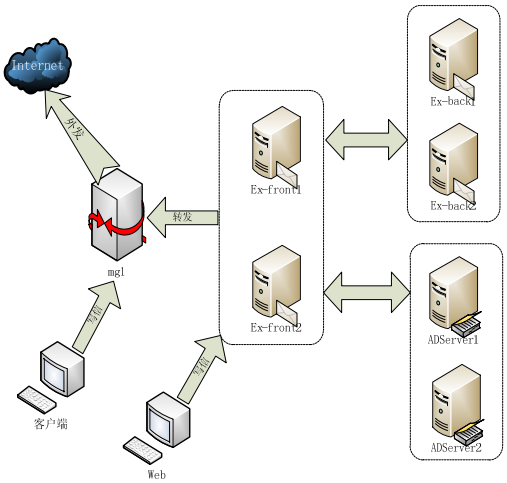

图 5　邮件系统优化后发信流程

具体实施:

①首先在邮件网关上设置邮件服务器前端的IP为无条件信任状态. 即在邮件网关 mg1 的系统配置中→抗攻击配置→非受限 IP 里分别添加邮件服务器前端 Ex-front1 和 Ex-front2 的 IP, 在 mg1 的策略配置中→IP 控制列表→允许转发列表中添加 Ex-front1 和 Ex-front2 的 IP.

②其次设置 Exchange server 的转发路由. 在 Exchange 管理控制台的集线器传输里选择发送连接器, 在发送连接器的“Internet 属性”的“网络”设置中, 有一个“通过以下智能主机路由邮件”的选项, 把邮件网关 mg1 的 IP 添加到该选项中. 这样可保证用户在用 Web 方式发信时都经由邮件网关 mg1 来过滤.

③接下来修改 DNS 设置. 这次优化调整拟统一规范客户端设置, 原客户端设置收发服务器均为 mail.scnu.edu.cn, 而且该域名直接指向 Ex-front1 和 Ex-front2 的 IP(存在垃圾邮件组织用 smtp 方式直接往邮件前端发信的漏洞). 现将发信服务器域名更改为 smtp.scnu.edu.cn, 该域名直接指向邮件网关 mg1 的 IP(由网关过滤和作发信频率限制);发信服务器域名更改为 pop.scnu.edu.cn, 该域名分别指向邮件服务器前端 Ex-front1 和 Ex-front2 的 IP. MX 记录维持原样不变, 即同时指向 mg1 和 mg2, 但 mg2 优先级高于 mg1. 以此确保收发邮件都经过邮件网关过滤, 发信过滤由 mg1 负责, 收信过滤则主要由 mg2 承担.

④最后是更改端口设置. 一是防火墙对外开放邮件网关(mg1 和 mg2)的部分端口, 包括 25、587、465、995 等. 二是更改邮件服务器前端(Ex-front1 和 Ex-front2)的系统防火墙设置, 设置邮件服务器前端发送端口(25)仅能与邮件网关通讯, 禁止外来邮件直接使用它们作为发信端口. 由此限制垃圾邮件组织直接往邮件服务器前端滥发垃圾邮件.

4 应用效果与分析

华师校内邮件系统经过优化调整后, 校内邮箱与国外通信不畅的问题得到了很大改善. 用户跟踪测试发现, 以前发往国外的邮件经常被拒收, 诊断信息诸如“Unfortunately, messages from 222.200.128.35 weren't sent. Please contact your Internet service provider since part of their network is on our block list.”; 自学校反向域名(PTR)注册申请通过后, 像此类因为反向 DNS 没做好被国外邮件系统拒收的情况均未再出现过, 与国外收发邮件都趋于正常状态.

对校内邮箱发信机制的调整, 也解决了邮件系统之前存在的安全隐患问题. 发信机制优化前, 校内邮件发送至校内或校外均未作过滤, 以致无法对用户滥发邮件作限制处理;发信机制优化后, 校内邮件发送经由网关过滤, 由网关的统计报表中的 “发信人统计”中可以看到:主题为(null)以及校外邮箱利用校内邮箱来发信的, 几乎全部被过滤, 加上基于其它原因被过滤的垃圾邮件每天都有几千或上万封, 这很好地限制了校内垃圾邮件的滥发, 并减轻了邮件服务器的负荷.

对外关闭邮件前端服务器的 25 端口, 可以有效地限制黑客盗用校内邮箱帐号作为垃圾邮件中转站对外滥发. 25 端口关闭前, 时常会出现用户被盗号并以每秒上百封地外发垃圾邮件;25 端口关闭后, 即使用户被盗号也无法用 smtp 方式连接 25 端口来批量发信, 而 web 方式有网关作发信频率限制. 因此从根本上解决了垃圾邮件滥发的问题, 这也减少了校内邮件服务器 IP 被其它反垃圾邮件组织列入黑名单的机率, 从而很好地维护了学校的声誉, 保障了校内外邮箱通信的畅通性.

将邮件网关引入发信机制中, 对邮件系统的日常监控、管理维护也提供了很大便利. 发信机制引入邮件网关前, 用户发信情况及故障日志都只能通过逐台邮件服务器排查, 且无 web 界面, 查找费时费力;发信机制引入邮件网关后, 可直接通过登陆网关的 web 应用界面进行排查, 方便快捷. EQManager 邮件网关[8]自带的“系统监控”功能, 可以让管理员及时监控资源的使用情况、SMTP 连接数等; “邮件队列”模块提供了包括正常、可疑、过滤三种队列的查询、放行等功能; “系统配置”和“策略配置”模块可供管理员随时调整过滤规则、策略设置、实时黑名单及抗攻击配置等;而 “日志浏览”和“日志查询”模块可以及时查询用户的发信状态及投递情况. 这不仅给管理员的日常维护工作带来便利, 也大大提高了工作效率.

因此, 校内邮件系统的优化调整, 不仅给校内邮箱用户带来了良好的用户体验, 而且给邮件系统管理员提供了更好的监控、查询、诊断等管理维护功能.

5 结语

华南师范大学电子邮件系统的优化管理调整, 不

仅解决了校内邮箱与国外通信难的问题, 而且修复了原来发信流程中存在的安全漏洞, 保证了校内邮箱与校外邮箱的收发通畅, 同时也提升了学校的声誉与形象. 因此, 华师校内邮件系统的优化管理, 不仅解决了系统运维安全问题, 增强了用户体验, 同时也给管理员的日常维护管理带来很大便利, 这在高校电子邮件系统的管理应用中具有一定的参考价值和意义.

参考文献

1 Gerber B, McBee, J. 王庆梅,陈宗斌译.Microsoft Exchange Server 2007 技术大全.北京:人民邮电出版社,2008.

2 罗辉琼,廖春盛.Exchange Server 2007 管理研究.计算机工程与设计,2010,31(6):1247–1254.

3 EQManager 邮件安全网关.http://www.eqmail.com/eqmanager. html.[2014-07-04].

4 PTR 记录.http://baike.baidu.com/link?url=jOoGI0s7Z2SxkpglUDLyo77XetYWLz5b74jAlgAUTGfbyqI3ttZrfVIM7PHxjXH7z1bGEWIGyI16DFBVD7Yzv_.[2014-07-04].

5 Pro DNS and BIND. http://www.zytrax.com/books/dns/ch8/ptr.html. [2014-07-04].

6 曾小宁.垃圾邮件过滤系统的探究与实现.计算机工程与设计,2009,30(15):3522–3530.

7 Zhou JY, Chin WY, Rodrigo R, et al. Aneffective multi-layered defense framework against spam. Information Security Technical Report, 2007, 12(3): 179–185.

8 EQManager 邮件网关管理系统管理员使用手册.北京敏讯科技有限公司,2006,5:1–5.