

谈垃圾邮件防火墙在运营商环境中的应用 PDF转换可能丢失图片或格式，建议阅读原文

[https://www.100test.com/kao\\_ti2020/0/2021\\_2022\\_\\_E8\\_B0\\_88\\_E5\\_9E\\_83\\_E5\\_9C\\_BE\\_E9\\_c99\\_431.htm](https://www.100test.com/kao_ti2020/0/2021_2022__E8_B0_88_E5_9E_83_E5_9C_BE_E9_c99_431.htm) 在刚刚过去的2009年，虽然我国垃圾邮件治理工作取得了较大进展。经由我国发出的垃圾邮件占全球垃圾邮件总数的比例，从2008年底的23.0%降至2009年第三季度的4.0%，排名也从最高时的第2位降至第6位，总体呈下降趋势。但是我国反垃圾邮件的工作仍然任重而道远。通过最近一轮的调查发现，我国近来产生的垃圾邮件，很大一部分是由于垃圾邮件发送者假冒、伪造邮件地址，或者利用他人服务器转发大量垃圾邮件。对此，叫苦不迭的不只是邮箱拥有者，一些电信运营商和邮箱运营商更是垃圾邮件的直接受害者。

运营商反垃圾邮件困扰

1. 现有的防火墙和病毒防火墙只能阻断来自网络的普通攻击，不能有效防止Internet混合在垃圾邮件当中的病毒，蠕虫，URL等威胁，使得病毒能够躲避传统的防御方法，且将其代理文件植入到运营商邮件系统的网络中。
2. 现有垃圾邮件防护系统不能有效的过滤垃圾邮件，导致系统内存在着大量的垃圾邮件，占用了传输、存储和运算资源，不但造成网络资源浪费，降低了系统的使用率，还造成邮件服务器拥塞，降低了网络的运行效率，严重影响正常的邮件服务，对信息安全系统性能形成重大影响。
3. 由于垃圾邮件具有反复性、强制性、欺骗性、不健康性和传播速度快等特点，严重干扰了个人的正常生活，浪费了用户的时间、精力和金钱，使得很多的用户对运营商的服务产生了不满，极大的影响了用户满意度，导致用户对运营商投诉增加，甚至客户流失的严重后果。
- 4

· 大量的攻击测试，由于电信属于大用户，目标较大容易电信外部的邮件系统引起黑客兴趣，配置稍有不慎即成为黑客的攻击目标，甚至成为垃圾邮件的中转站，这样不但严重影响电信系统内部的正常邮件交流，而且很容易被国际反垃圾邮件组织列入黑名单，从而造成该邮件服务器无法向外界正常的发送邮件。

5. 电信邮箱的用户群体比较巨大，很多电信域的用户利用本域邮箱向外部其他邮箱发送垃圾邮件，很容易造成该域被其他的邮件服务器屏蔽，影响正常邮件发送，甚至有的邮件用户向其他用户发送反动邮件，从而产生一些政治事件，严重影响运营商形象。

某大型电信网络中，邮件服务器群架设在具有负载均衡功能交换设备后端，SMTP服务和POP服务在不同的服务器上实现，具备强大的负载均衡和抗攻击能力。

反垃圾邮件产品的安装模式以梭子鱼垃圾邮件防火墙为例，介绍一下运营商环境中的反垃圾邮件产品安装模式：

1. MX记录修改模式 这种模式针对大型网络中架设梭子鱼后能够给梭子鱼分配公网地址的情况。通过在DNS上修改本域的MX记录，使MX记录优先指向梭子鱼的公网IP地址，从而使邮件流优先流向梭子鱼，经由梭子鱼过滤病毒和垃圾邮件后再转发到邮件服务器。前面所述的运营商典型邮件系统环境一般都属于这种架设模式。
2. 端口转发模式 这种模式针对局域网络环境中，公网地址缺乏或者网络环境不允许修改MX记录的情况。通过将邮件域公网地址的SMTP端口指向梭子鱼（NAT或者PAT），其它端口不变，使邮件流先指向梭子鱼的私网地址，梭子鱼过滤完病毒和垃圾邮件后再转发到邮件服务器的私网地址。这种模式的优点是架设简单，不需要对网络架构做大的修改。运营商环境中的反垃圾

邮件防火墙性能要求 1 . 强大的邮件处理能力 对于运营商邮件系统而言，需要反垃圾邮件防火墙设备有强大的邮件处理能力，即支持上万个邮件帐号，每日处理邮件量要达到上千万封，我们可以看看梭子鱼高端型号设备的邮件处理能力。单台梭子鱼垃圾邮件防火墙支持超过100,000邮件帐户，日处理邮件数量达到200万封的项目案例，从上图中可以看到运营商的病毒邮件数量达到1.5%，而垃圾邮件数量则超过了90%。

2 . 针对邮件瞬间峰值的邮件接收处理能力 对于运营商而言，对垃圾邮件防火墙设备的瞬间高峰处理能力要求很高，这样也就要求垃圾邮件防火墙设备要有强大的接收处理能力，能在邮件高峰时间，把邮件“吃进肚子”，然后在慢慢消化。运营商垃圾邮件防火墙要求实现负载均衡、冗余及容错

1 . 通过DNS轮巡的方式实现负载均衡及冗余 通过DNS的轮寻机制，邮件在传输到某台梭子鱼前将经过一个随机挑选的过程，上图所示的5台梭子鱼，在轮寻机制下有相同的几率被选中，这将使进入的邮件平均的分配到所有的梭子鱼中，从而达到负载均衡的效果。

2 . 选择专业的负载均衡设备实现负载均衡功能 除了以上的DNS轮巡模式以外，还可以选择专业的负载均衡设备，采用加权最小连接数（WLC）、加权轮巡（WRR）及应用程序智能引擎(Adaptive Scheduling)等模式来进行负载均衡计算，把流量平均分配到几台梭子鱼垃圾邮件防火墙上。运营商环境需要不断提高垃圾邮件过滤技术

对于反滥发邮件措施,运营商的邮件管理者应该意识到：互联网上增加了大量垃圾邮件；身份欺诈的手段在不断变化；图片垃圾邮件的飙升。依据这些趋势精心策划邮件防护部署，才能够保护系统的安全。梭子鱼垃圾邮件防火墙根据国际垃

垃圾邮件的发展趋势而增加了许多新技术，专门针对不同的攻击类别，如图片扫描，意图分析，OCR技术，发件人特征识别等，紧密跟踪垃圾邮件事态，立即响应和动态升级服务被验证能够正确且有效的确保运营商邮件环境的安全。编辑特别推荐: #0000ff>安全硬件是否会被SaaS式安全取代 100Test 下载频道开通，各类考试题目直接下载。详细请访问 [www.100test.com](http://www.100test.com)