Linux中防御垃圾邮件的方法Linux认证考试 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/619/2021_2022_Linux_E4_B8_AD_E9_98_c103_619605.htm 相信大部分使用电子邮件的人每天都会收到大量垃圾邮件。作为单位网管，笔者每天收到垃圾邮件的数量更在数百封以上，预防垃圾邮件已到了刻不容缓的地步。 一、环境说明 单位的服务器使用RedHat Linux 9.0，邮件服务器使用Sendmail 8.12.8.这台服务器放在内网，通过一台Win2000的服务器作网关，连到Internet.网关软件使用的是WinRoute Pro 4.2.5。 二、主要修改措施 1.关闭Sendmail的Relay功能 所谓Relay就是指别人能用这台SMTP邮件服务器，给任何人发信，这样别有用心的垃圾发送者可以使用笔者单位的这台邮件服务器大量发送垃圾邮件，而最后别人投诉的不是垃圾发送者，而是单位的服务器。所以必须关闭Open Relay，其方法就是到Linux服务器的/etc/mail目录，编辑access文件，去掉“ *relay ”之类的设置，一般只留“ localhost relay ”和“ 127.0.0.1 relay ”两条即可。 注意：修改access文件后还要用命令makemap hash access.db 2.打开Sendmail的SMTP认证功能 关掉了Relay功能，单位的老师就不能使用OE之类的软件发信了不要紧，只要对Sendmail配置好SMTP认证功能，再在OE中打开SMTP认证，就可以在任何地方使用单位的SMTP服务器了。 在RedHat Linux 9.0中配置SMTP认证非常方便，首先用命令rpm -qa|grep sasl检查有没有安装cyrus-sasl软件包(一般默认安装已经包括了)。如果没有安装的话，用命令rpm -ivh cyrus-sasl.rpm安装所有软件包，接着打开/etc/mail/sendmail.mc文件，把如下三行： dnl

TRUST_AUTH_MECH(`DIGEST-MD5 CRAM-MD5 LOGIN PLAIN)dnldnl define(`confAUTH_MECHANISMS , `DIGEST-MD5 CRAM-MD5 LOGIN PLAIN)dnlDAEMON_OPTIONS(`Port=smtp，Addr=127.0.0.1，Name=MTA) 改为TRUST_AUTH_MECH(`DIGEST-MD5 CRAM-MD5 LOGIN PLAIN)dnldefine(`confAUTH_MECHANISMS，`DIGEST-MD5 CRAM-MD5 LOGIN PLAIN)dnlDAEMON_OPTIONS(`Port=smtp，Addr=0.0.0.0，Name=MTA) 3.在Sendmail中添加RBL功能 RBL(Realtime Blackhole List)是实时黑名单。国外有一些机构提供RBL服务，它们把收集到的专发垃圾邮件的IP地址加入他们的黑名单，我们只要在Sendmail中加入 RBL认证功能，就会使我们的邮件服务器在每次收信时都自动到RBL服务器上去查实，如果信件来源于黑名单，则Sendmail会拒收邮件，从而使单位的用户少受垃圾邮件之苦。 国外比较有名的RBL是http//www.ordb.org，他们的RBL可免费使用，去年国内的http//anti-spam.org.cn也提供类似的服务，但它必须先注册才能使用免费。 在Sendmail中添加RBL认证，只要对sendmail.mc添加以下几句话(第一句表示加入了ORDB.ORG的RBL服务，第二句表示加入了ANTI-SPAM的RBL 服务，注意第二条必须先去该网站注册后才能使用。如果还想加入其它的RBL认证，则将这样的话再多加几句即可，一般加入两个RBL认证也够了)： ①FEATURE(`dnsbl，`relays.ordb.org，` ″ Email blocked using ORDB.org - see ″ ) ②FEATURE(`dnsbl，`cblplus.anti-spam.org.cn，` ，` ″ 451 Temporary lookup failurefor

" $gt.sendmail.cf和service sendmail restart两条命令，使有关Sendmail的修改生效。 4.关闭Open Proxy 单位的网关使用WinRoute软件，为了提高访问Internet的网速，开放了WinRoute的Proxy服务，但想不到的是大部分 Proxy都是默认允许以HTTP Connect Method连接任意一个TCP端口，这样一来，当Proxy没有对使用者及相应的TCP端口做相应的限制时，很容易给垃圾邮件发送者可乘之机。他们只需要利用单位的Proxy来连接另外一台邮件服务器的25端口，并发送特定的SMTP指令就可以发送大量的垃圾邮件。 不查不知道，一查吓一跳。单位服务器早在去年12月就由于Open Proxy而在国外的黑名单上了。更可气的是，由于开放了代理，我们的网关机CPU利用率一直在50%左右，原来笔者单位的网关一直在为别人义务干坏事。 在WinRoute中关闭Open Proxy的方法也很简单，只要把连接外网网卡的Proxy端口关闭即可。 具体操作如下：单击“ Settings→Advanced→Packet Filter ”，选择Incoming面板，找到接外网的网卡，单击Add按钮，会显示Add Item对话框，把Protocol选为TCP，Destination中的Port选=3128，Action中选Deny。 5.关闭外部的25端口 笔者查看Sendmail的LOG，结果没发现从单位中发出很多垃圾邮件，正在郁闷时，突然想起这段时间正在大闹Internet的网络天空“ NetSky ”和唯诺格“ MyDoom ”病毒，这两种病毒都会自动发出很多垃圾邮件，特别是网络天空，它自带SMTP服务功能。不需要利用单位的Sendmail，就直接可以发信。单位的Sendmail的LOG中当然也不会有记录了，于是马上到网关机WinRoute中对连接内网的网卡加上不能向外连接25号端号的限制。 注意：这个设置是加在内网网卡上的，而上面关

闭Open Proxy的设置则是加在外网网卡上的。 6.从黑名单上除名 前段时间，由于自已的疏忽，使我单位的IP已经上了国外RBL的黑名单了。查询和删除RBL中的IP地址可以到 http：//openrbl.org/ 和http：//ordb.org，另外国内的http：//anti-spam.org.cn/cbl_minus/query.html也可查询。 