张翔 李军怀 张景 吕林涛 (西安理工大学 计算机学院 710048)

Anti-Relay of Netscape Message Server 4.15 on Windows 2000

Windows 2000下 Netscape Message Server 4.15 对邮件转发的限制方法

摘要：本文介绍了垃圾邮件的危害，详细分析Netscape Message Server 4.15对付邮件转发的原理，结合工程实践阐述了利用UBE plug-in filter限制转发的设置。

关键词：垃圾邮件 转发 Netscape Message Server Windwos 2000

1 邮件服务器Netscape Messaging Server

Netscape Messaging Server是iPlanet电子商务解决方案公司（Sun与AOL Netscape建立的联盟公司）开发的基于开放标准，客户服务器结构邮件系统的第三代产品，提供高级的目录服务、可管理性、伸缩性、安全加密和远程连接等能力。

我们课题组在工程应用中，由于企业用户采用Windows 2000 Server平台，经过测试表明只有Netscape Messaging Server 4.15能在Windows 2000下正常运行。iPlanet™Messaging Server 5.x不能运行在Windows2k操作系统上，因为MTA的两个服务不能很好地启动。

经过短期的试运行，它的方便易用性，得到了用户的好评。但是好景不长，就发现服务器负荷很重，响应慢，磁盘空间急剧增长。经过仔细检查发现是由于没有限制邮件转发，给国内外不法分子提供可乘之机，使他们能通过该邮件服务器发送大量“垃圾”邮件，给系统造成很大压力。

2 垃圾邮件的危害

人们将向新闻组或他人电子信箱发送大量不恰当的以及无聊消息的行为和这些消息本身称为Spam(垃圾邮件)，从事此类活动的人员叫做Spammer(垃圾信制造者)，现在主要包括以下几类：① 商业广告；② 站点宣传；③ “病毒”谣言；④ 某些不请自来的网络杂志；⑤ 连环信的E－mail版；⑥ 反动、色情邮件；⑦ 法轮功反动宣传，这些邮件相当一部分发送地址都是不存在的，这些信件就“死”在队列中，影响系统运行效率和浪费介质空间，需要定时清理，才能提高运行效率，有时因“垃圾”邮件太多还会导致系统崩溃。

从全球范围来看，垃圾邮件成为互联网上的一大国际问题。垃圾邮件来势汹汹，不仅耽误了人们的时间，降低了工作效率，还经常阻塞网路的畅通，造成巨大的经济损失。去年欧盟的一项调查估计全球网民为收取垃圾邮件而支出的接入费用高达100亿欧元。我国电子邮件提供商目前面临的主要问题是邮件服务器自我管理不严，容易被非授权人员用于转发邮件，一旦转发的是垃圾邮件，则会带来不良影响。因此，从管理上国内电子邮件服务的提供者要建立完善的邮件管理规范，既要防止授权用户发送垃圾邮件问题，又要防范自身服务器被人利用，不要成为垃圾邮件的转发器。

3 邮件传送方式

电子邮件与普通邮件有类似的地方，发信者注明收件人的姓名与地址（即邮件地址），发送方服务器把邮件传到收件方服务器，收件方服务器再把邮件发到收件人的邮箱中。目前使用的SMTP协议是存储转发协议，意味着它允许邮件通过一系列的服务器发送到最终目的地。事实上，在80年代前，网络还不是很健全，机器之间很少能直接对话发送邮件，人们必须得找出一条有效的连接通路来，然后信件沿着通路一步一步传送到目的地。SMTP协议中就明确指出当邮件在不同的网络间传送时，需要借助中间服务器的RELAY。服务器在一个队列中存储到达的邮件，

等待发送到下一个目的地。下一个目的地可以是本地用户，或者是另一个邮件服务器。如果下游的服务器暂时不可用，MTA就暂时在队列中保存信件，并在以后尝试发送。现在网络四通八达，已经很少再使用中继，大多都是由发信服务器直接传递到收信服务器。邮件传送方式如图1所示。

目前，正常邮件转发已经不再必要，相反，无限制转发常常被发送垃圾邮件的人利用，来隐藏真实的邮件来源，让别人以为是从另外的ISP发出的信件；同时，也把大量的处理工作转移到别人机器上。如图1中的"垃圾邮件制造者"，就可以伪装成是甲公司的员工。

由于前面提到的历史原因，最初的绝大多数邮件服务器都允许OPEN RELAY的。现在大部分邮件服务器升级版本已经提供了关闭open relay的方法，或者在缺省设置中关闭了OPEN RELAY，但由于很多服务器管理员的疏忽而没能及时的修补这些安全漏洞，就会被利用来转发垃圾邮件。

4 邮件服务器转发(RELAY)的确认

垃圾信件制造者通常使用专门的扫描软件，一次自动扫描多个网段的主机，来发现可以用来执行转发信件的邮件服务器，我们手工输入一些SMPT指令，来模拟这种扫描。假设要测试的服务器是http://mail.mydomain.com，按下面的指令序列进行测试：

(1) 远程连接服务器：

c:\>telnet mail.mydomain.com 25

220 mail.mydomain.com ESMTP service (Netscape Messaging Server 4.15 Patch 3 (built Sep 28 2000)) //服务器回复信息，指明邮电服务器域名及类型

(2) 发件方问候收件方，后面是发件人的服务器地址或标识：

helo mail.otherdomain.com

250 mail.mydomain.com //收件方标识自己的身份，表明两台机器可以进行通信

(3) 告知发信人的地址：

mail from:nobody@otherdomain.com

250 Sender <nobody@ otherdomain.com> Ok //服务器回复允许

(4) 告知转发地址

rcpt to:nobody@third-domain.com

！！！关键就在于这次服务器回复内容：

如果是 250 Recipient <nobody@third-domain.com> Ok，则说明该服务器没有限制转发；

如果是：554<nobody@third-domain.com>... Relay operation rejected，则说明已经设置好限制转发。

(5) 知服务器，要输入信件内容了。(可以忽略)

data

354 Enter mail, end with "." on a line by itself //服务器提示表示信件结束的方式

(6) 输入信件内容，结束输入时按一个回车，一个英文句号，再一个回车：(可以忽略)

This is a test

.(表示结束)

250 Message received: H19CE400.V00 服务器回复信息的存储编号

(7) SMTP要求接收方必须回答OK，然后中断传输中断连接。

quit

221 mail.mydomain.com ESMTP server closing connection //服务器同意中断

(8) 发件方收到答复，中断本次连接。

屏幕显示：遗失对主机的连接。

C:\>

通过上述八条指令，我们就知道邮件服务器是否安全的限制了转发功能。如果发现没有设置就应该赶快设置好，以免给不法分子造成可乘之机。

5 网络拓扑结构

从邮件服务器安全角度出发，有两种拓扑，一种使用两台服务器，一种使用一台服务器。

5.1 利用两台服务器处理所有进出邮件

此种方法在防火墙外放置一台独立的机器，它的功能就是检查电子邮件的域名，而在防火墙内的另一台服务器用来处理所有进出邮件的发送与接受。防火墙外的服务器也是一台邮件服务器，它先行处理所有进入的邮件，不论是来自internet还是来自内部用户，如图2所示。

我们允许User1和User2可以发送电子邮件到任何地方，但X1和X2仅仅只允许给内部邮电服务器发邮电。我们不需要在内部服务器作任何设置，因为有了防火墙，只有内部用户才可以连接到这台服务器，而我们允许内部用户可以接受和发送邮件到任何地方的。

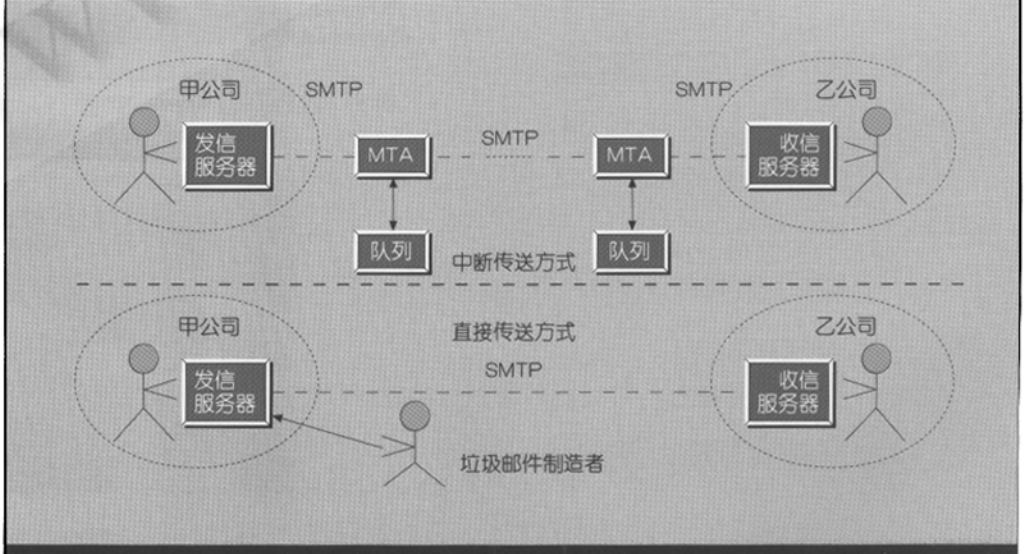

图1 邮件传送方式

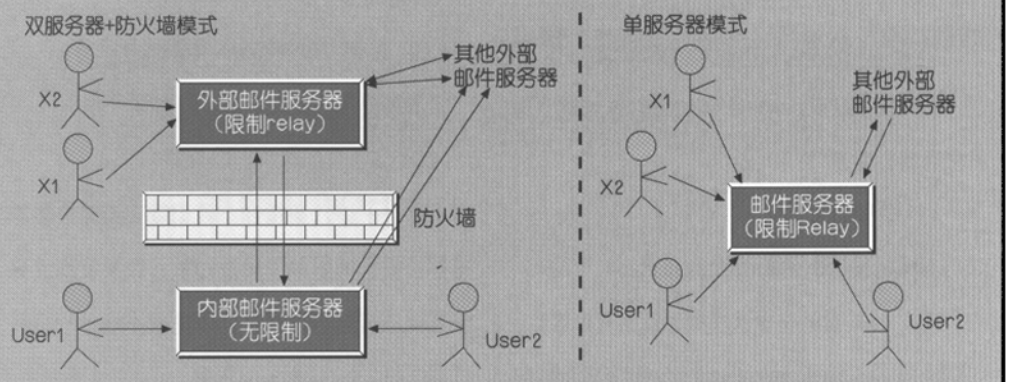

图2 网络拓扑图

5.2 利用单一服务器处理所有进出邮件

在此方案中，使用一台服务器处理和所有进出邮件连接。我们允许所有的本地用户可以不加限制收发邮件，但同样的权限不付给外部用户。这种策略安全性较第一种差，因为它使得邮件服务器处于一个可以被外部攻击的位置。如果有防火墙，那么也可以把邮件服务器放置在防火墙以内，做部分防护。我们允许User1、User2可以向任何地方收发邮件，但只允许X1和X2向本域发邮件，如图2所示。

从国内目前企业信息化的实际来看，第二种拓扑结构尽管安全性较差，但基本能满足一般企业的需求，费用低，实施简单，管理方便，所以采用的较多。

6 Netscape Messaging Server转发限制的方法

Netscape Messaging Server 有两种方法可以用来控制 open relay，一种是创建 UBE plug-in filter来实现 Anti-relay Filter；另一种是位于协议层的 Anti-relay Plug-In。后者的功能更强大些，但只支持4.x以上版本；早期版本只能使用前一种方法。

6.1 UBE plug-in filter

UBE是Unsolicited Bulk Email的缩写，与垃圾邮件意思相同。UBE plug-in filter是一个Netscape Messaging Server自带的用于控制SMTP工作的插件，在所有接收到的邮件进入用户邮箱或转发到其他服务器之前，根据配置文件中的过滤规则对信件进行处理，工作机制见图3。通过它可以在服务器上设置过滤机制，中止外部域名所转发的UBE信件；也可以设置成为某一服务器的中转服务器，通过中转隐藏发信人的真实身份。

UBE过滤规则就是UBE filter配置文件中的一条记录，该文件缺省文件名是：UBEfilter.cfg。配置过滤规则时有两种方法：一是通过Netscape Messaging Server控制台的图形界面，如图4所示。二是直接修改UBEfilter.cfg，例如与图4等价的规则就是：：AllowInternal Channel-To "domain1.com" EXIT。这两种方法效果是一致的。

6.2 邮件的组成结构

UBE过滤规则每一条都是针对邮件的信头或者信封的记录来进行判断的。邮件在传输过程中，服务器要把它打包成一个数据对象，包括信件和一个信封。邮件的投递是依靠信封上的地址或信封（envelop address 或 envelop header），而不是信件上的地址。邮件的信头是用户写好信，发送出去时，就自动生成的，比较容易利用一些工具篡改信头记录，而信封纪录是信件在发送过程中，又经过的服务器添加上的，不容易修改，所以UBE过滤规则缺省是仅仅检验信封纪录。常用的记录字段有：To, From, Sender, Reply-To，一些邮件还有cc, bcc等。具体E-mail的格式参见RFC821。

图3 Plug-in结构

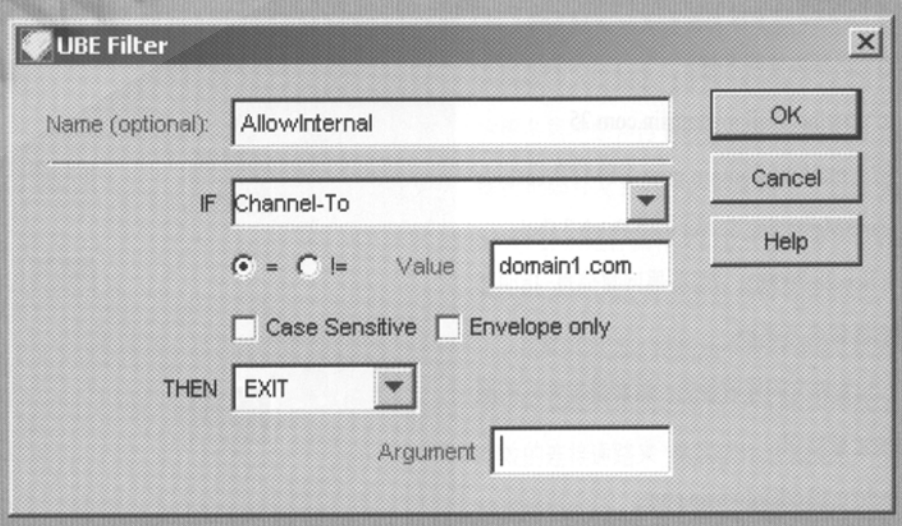

图4 UBE过滤规则

（文章尚未完，转第42页）

(接第38页)

6.3 UBE过滤规则设置

以使用单一服务器的拓扑结构为例，我们可以在邮件服务器上结合IP地址和域名创建过滤规则，允许自己的用户自由出入，拒绝所有外部的用户。我们自己的用户，它大多时候都有固定的IP地址，比如192.168.1.100,因此可以从地址加以检查。如果IP地址非内部，那一定来自internet。接着如果邮件收件人项和本地邮件相匹配，则继续执行，假如本地域名为mydomain.com，则设定如下：

判断来自内部的用户，如果连接来自内部，退出过滤检测继续执行。

Host-From "192.168.1.100" EXIT

Host-From "192.168.1.101." EXIT

如果不是来自内部的连接，用域名判断

Channel-To "mydomain.com" EXIT

拒绝其他任意项

$ANY ".*" REJECT "Relay operation rejected!"

符合条件，继续发送，否则的话立即拒绝。EXIT指退出过滤继续执行，$any即匹配所有的head项，".*"则匹配任何形式的文本。上面的三条使的这台服务器只能接收发往mydomain.com的信件。

7 结语

垃圾邮件（Spam）日益泛滥的危害，用三两句话是说不完的。在邮件服务器上限制邮件转发，只是在技术上减少垃圾邮件现象，要想彻底根绝垃圾邮件，最终还得靠制定相应的法律。希望通过全社会的共同努力，早日杜绝垃圾邮件。

参考文献

1 （美）Richard Blum著，杜鹏译，开放源码邮件系统安全，人民邮电出版社，2002.4。

2 段小华，E-mail服务器配置和管理，清华大学出版社，2002.3。

3 Netscape Corp，Netscape Messaging Server4.15 Administrator's Guide，Netscape Communications Corp，1999。

4 唐明湘、庄锦山、秦臻，Exchange Server 2000应用开发指南，清华大学出版社，2002.7。