ISSN 1009-3044
Computer Knowledge and Technology 电脑知识与技术
Vol.13, No.23, August 2017

E-mail: jslt@dnzs.net.cn
http://www.dnzs.net.cn
Tel:+86-551-65690963 65690964

# Postfix反垃圾邮件过滤技术分析及应用

陈昀[1],杨戈[2]

(1.深圳技师学院 电子信息技术系,广东 深圳 518116;2.深圳市智联信息技术有限公司,广东 深圳 518057)

**摘要:**该文介绍了开源免费的Postfix邮件服务器软件及其邮件过滤技术,通过分析其过滤规则将其应用到反垃圾邮件中。

**关键词:**Postfix;邮件过滤;反垃圾邮件

**中图分类号:TP311 文献标识码:A 文章编号:1009-3044(2017)23-0049-02**

DOI:10.14004/j.cnki.ckt.2017.2386

电子邮件作为历史悠久的互联网应用,因为其当初设计的宗旨就是开放、互联,只要有互联网接入就可以实现电子邮件的收发,其发送成本非常的低廉。其设计的开放性就在机制上允许了任何人向任何人发送电子邮件,现在一些个人或企业出于商业推广等目的在未经用户许可的情况下强行发送与用户无关的内容到用户的邮箱中,这样就造成了垃圾邮件的肆虐。垃圾邮件也称为SPAM、UBE(Unsolicited Bulk Email)或UCE(Unsolicited Commercial Email),垃圾邮件不仅占用了网络带宽、存储空间,更主要的是侵犯了用户隐私、给用户造成了骚扰。

在全球互联网环境下,反垃圾邮件是个国际性话题,源头上各个国家或地区需要制定相关的法律法规,技术层面上需要从电子邮件的发送源头、传输途径和达到目标上进行监控、识别和过滤。本文以电子邮件传输的目的地邮件服务器为角色中心,通过Postfix过滤技术对进入到本地服务器的电子邮件进行分析、排查,对垃圾邮件进行处理。

## 1 Postfix简介

Postfix是一个免费并开源的邮件传输代理(MTA),用于电子邮件的路由、传送和接收,其目的是替代老旧、安全问题频出的Sendmail邮件传输代理。Postfix以前的名字有叫过VMailer和IBM Secure Mailer。最早是IBM于1997年进行了初始开发,1998年时正式对外发布,直到现在其开发团队仍然非常活跃,以持续其新特性和新功能的开发。

Postfix以其高效性、安全性,在互联网邮件服务器领域中占据了广泛的市场。Postfix可以运行于AIX、BSD、HP-UX、Linux、OS X、Solaris等类Unix系统中,它也是OS X、NetBSD和Ubuntu Linux系统的默认邮件传输代理程序。

Postfix作为邮件传输代理主要担当SMTP服务器和SMTP客户端的角色。作为SMTP服务器,Postfix可以从网络层到应用层对进入服务器的连接和邮件进行过滤处理。除了其本身的过滤处理机制,Postfix还可以联动其他第三方的反垃圾邮件过滤或病毒扫描,例如Amavisd-new或Dovecot,以及更复杂的应用层SMTP协议访问策略,例如postfwd、policyd-weight或greylisting。

## 2 Postfix过滤机制分析及应用

Postfix作为SMTP服务器时,处于被动监听状态,对外界开放25/TCP端口,接受来自网络SMTP客户端的连接请求,连接建立后双方在应用层通过SMTP协议进行会话,若判断为垃圾邮件则对其进行拦截,否则邮件正常进入到系统的用户邮箱,其反垃圾邮件过滤流程如图1所示。

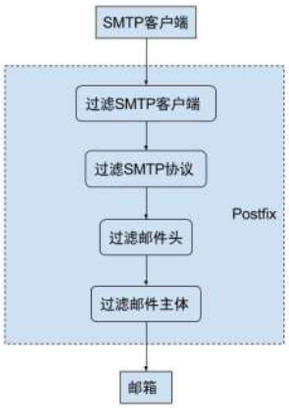


**图1 Postfix反垃圾邮件过滤流程**

### 2.1 过滤SMTP客户端

对于SMTP客户端的过滤,通过Postfix主配置文件main.cf中的smtpd_client_restrictions进行控制。smtpd_client_restrictions可以基于客户端IP地址、客户端网络地址或客户端主机名对其进行过滤;匹配上规则后,其动作可以是允许邮件过程或拒绝邮件。

在main.cf中配置过滤SMTP客户端:

```
smtpd_client_restrictions =
check_client_access  hash:/etc/postfix/maps/access_client,
permit
```

access_client内容如下(因该文件会被编译为带索引的数据库,故其规则是顺序无关的):

```
1.2.3 REJECT        #拒绝1.2.3.0/24网络段的客户端连接
1.2.3.4 OK          #允许1.2.3.4这个IP地址的客户端连接
mail.f.cn  REJECT       #拒绝来自mail.f.cn客户端的连接
mail.g.cn  OK           #允许来自mail.g.cn.客户端的连接
```

将access_client文件编译为数据库文件:

```
postmap  /etc/postfix/maps/access_client
```

收稿日期:2017-07-03

### 2.2 过滤SMTP协议

SMTP客户端与服务端建立网络层和传输层连接后，就会通过应用层进行SMTP协议会话。客户端依次向服务端发送如下SMTP协议指令：HELO/EHLO、MAIL FROM、RCPT TO、DATA、QUIT。

#### 2.2.1 过滤HELO/EHLO

客户端会首先发送HELO或EHLO，用于标识自己的身份，很多垃圾邮件会伪造或跳过这个步骤。Postfix通过主配置文件main.cf中的smtpd_helo_required开关和smtpd_helo_restrictions对HELO/EHLO进行控制。

在main.cf中配置过滤HELO/EHLO：

```
smtpd_helo_required = yes                    #强制HELO或EHLO，若无则拒绝。
smtpd_helo_restrictions =
reject_unknown_helo_hostname,        #拒绝无DNS A记录或MX记录的客户端
permit                                       #默认为允许通过
```

#### 2.2.2 过滤MAIL FROM

客户端发送MAIL FROM指令用于标识邮件的发送者地址，垃圾邮件也会伪造该内容。Postfix通过主配置文件main.cf中的smtpd_sender_restrictions对MAIL FROM进行控制。

在main.cf中配置过滤MAIL FROM：

```
smtpd_sender_restrictions =
reject_non_fqdn_sender,  #拒绝非FQDN地址域名
reject_unknown_sender_domain,  #拒绝不存在的地址域名
check_sender_access  hash:/etc/postfix/maps/access_sender
permit
```

access_sender内容如下：

```
admin@sit.local          REJECT   #拒绝来自该地址的邮件
bugsreport@sit.net.cn    OK   #允许来自该地址的邮件
helloit.info             OK   #允许来由helloit.info的所有邮件
```

将access_sender文件编译为数据库文件：

```
postmap  /etc/postfix/maps/access_sender
```

#### 2.2.3 过滤RCPT TO

客户端发送RCPT TO指令用于标识邮件的接收者地址，垃圾邮件会尽量利用此内容向各个不同用户群发邮件。Postfix通过主配置文件main.cf中的smtpd_recipient_restrictions对RCPT TO进行控制。

在main.cf中配置过滤RCPT TO：

```
smtpd_recipient_restrictions =
reject_non_fqdn_recipient, #拒绝非FQDN地址域名
reject_unknown_recipient_domain, #拒绝不存在的地址域名
reject_unauth_pipelining, #拒绝未授权流水线操作(快速发送)
reject_unauth_destination, #拒绝未授权的接收者地址
reject_rbl_client  zen.spamhaus.org, #检索并拒绝第三方的实时黑名单
reject_rbl_client  dnsbl.sorbs.net,
reject_rbl_client  bl.spamcop.net,
reject_rbl_client  cbl.abuseat.org,
permit
```

### 2.3 过滤邮件头

邮件头包含与邮件相关的许多信息，对邮件头中的主题内容过滤是邮件头中垃圾邮件过滤的重要内容，Postfix通过主配置文件main.cf中的header_checks对邮件头进行过滤。

在main.cf中配置过滤邮件头：

```
header_checks = regexp:/etc/postfix/header_checks
```

header_checks内容如下：

```
/^Subject:.*AD/    REJECT      #拒绝主题中包含“AD”的邮件
/^Subject:.*广告/  REJECT      #拒绝主题中包含“广告”的邮件
/^Content-(Disposition|Type).*name\s*    =\s*"?([^;]*(\.|    =2E)(bat|com|exe)/
REJECT       #拒绝含有.bat、.com、或.exe附件的邮件
```

### 2.4 过滤邮件主体

Postfix也可以对邮件主体内容进行判断，通过检测邮件主体中的关键词或关键内容进行过滤。Postfix通过主配置文件main.cf中的body_checks对邮件主体进行控制。

在main.cf中配置过滤邮件主体：

```
body_checks = regexp:/etc/postfix/body_checks
```

body_checks内容如下：

```
/行用卡套现/REJECT #拒绝主体中包含“信用卡套现”的邮件
/Make Money Fast/REJECT   #拒绝主体中包含“Make Money Fast”的邮件
/<iframe/REJECT   #拒绝主体中包含“<iframe”的邮件
```

## 3 结论

Postfix的反垃圾邮件过滤技术是将垃圾邮件在到达用户邮箱之前就进行拦截，大大降低垃圾邮件对用户的骚扰。通过Postfix在邮件服务器的实际运作中，综合利用上其对SMTP客户端、SMTP协议、邮件头和邮件主体的过滤技术，可以达到较好的垃圾邮件过滤效果，大大降低进入到用户邮箱中的垃圾邮件。

## 参考文献：


[1] Postfix Configuration Parameters [EB/OL]. http://www.postfix.org/postconf.5.html, 2016-12-04/2016-12-18

[2] Postfix manual - access(5) [EB/OL]. http://www.postfix.org/access.5.html, 2016-02-28/2016-12-18

[3] Postfix manual - header_checks(5) [EB/OL]. http://www.postfix.org/header_checks.5.html, 2016-10-08/2016-12-18

[4] Comparison of DNS blacklists [EB/OL]. https://en.wikipedia.org/wiki/Comparison_of_DNS_blacklists, 2016-12-14/2016-12-18