第33卷 第17期 计 算 机 工 程 2007年9月
Vol.33 No.17 Computer Engineering September 2007
·安全技术· 文章编号：1000—3428(2007)17—0184—03 文献标识码：A 中图分类号：TP309

面向安全检测的SMTP透明代理服务器

曾新洲，王勇军，陈三龙
(国防科学技术大学计算机学院，长沙 410073)

摘 要：通过对SMTP协议和SMTP代理服务器原理的分析，在Linux环境下开发了面向安全检测的SMTP透明代理，设计并实现了一些关键技术，包括端口重定向、并发邮件服务、获取邮件服务器的地址和端口号、处理附件等。测试表明，该系统实现了用户透明功能，可以代理多种邮件服务，有效地防止了病毒入侵和内容泄露。

关键词：Linux；SMTP；代理服务器；透明代理；安全检测

SMTP Transparent Proxy Server for Security Detection

ZENG Xin-zhou, WANG Yong-jun, CHEN San-long
(School of Computer, National University of Defense Technology, Changsha 410073)

【Abstract】 On the basis of the analysis of SMTP protocol and SMTP proxy server principle, a SMTP transparent proxy for security detection is developed under Linux environment. Some key techniques are designed and implemented, such as redirecting port, concurrent mail service, getting the address and port of the server, handling annex. System test shows that the SMTP proxy is transparent to users, and can deputize for multiple e-mail services, prevent virus intrusion and leakage of internal content efficiently.

【Key words】 Linux; SMTP; proxy server; transparent proxy; security detection

随着电子邮件的广泛应用，公司、企业内部网络通过SMTP 代理服务器与外界进行邮件交流，人们在享受益处的同时，也要面对安全方面的挑战，如何有效地防止病毒入侵和机密泄露，引起了人们的重视，迫切需要建立一种安全可靠的机制来保障内部邮件系统的安全运行，这就要求 SMTP代理服务器不再局限于代理服务，它还必须具有内容过滤、安全审计、病毒查杀等功能，以保证内部网络资源的安全和对外网络访问的控制。例如对邮件用户进行过滤、拒绝某些用户使用邮件服务，以防止机密信息泄露；禁止发送含有机密信息的邮件；对邮件附件进行病毒检查等。

1 基于Linux的SMTP透明代理服务器

1.1 SMTP协议

简单邮件传输协议(simple mail transfer protocol, SMTP)，发送方SMTP与接收方SMTP建立一个双向的传输通道，接收方SMTP或者是一个最终的目的地或者是一个中间媒介。发送方SMTP产生SMTP命令并发送给接收方SMTP，接收方SMTP响应该命令。SMTP服务主要由以下3步构成：

(1)一旦建立好传输通道，发送方SMTP发送MAIL命令指明邮件的发送者，如果接收方SMTP能接收邮件，便响应一个OK。

(2)发送方SMTP发送RCPT命令指明邮件的接收者，如果接收方SMTP能为那个接收者接收邮件，则响应一个OK，如果不能，响应一个拒绝。

(3)发送方SMTP发送邮件数据，以字符序列“<CRLF>.<CRLF>”结束，如果接收方SMTP能成功处理邮件数据，则响应一个OK。

1.2 SMTP透明代理工作原理

代理服务器接收邮件客户端的连接请求，与邮件服务器建立连接，并把邮件服务器的service ready响应返回给邮件客户端，代理服务器接收邮件客户端的命令请求，转发该请求到邮件服务器，接收邮件服务器的命令响应，并返回给邮件客户端，直到邮件发送完毕。在此过程中，代理服务器既可以作为服务器，又可以作为客户端而存在；对于邮件客户端，代理服务器作为服务器而存在；对于邮件服务器，代理服务器却是作为客户端而存在的。

2 Linux下实现SMTP代理服务器

2.1 SMTP代理服务器框架结构

SMTP代理服务器由以下5个部分构成：守护进程，代理服务模块，用户过滤模块，内容过滤模块和病毒检查模块。如图1所示。

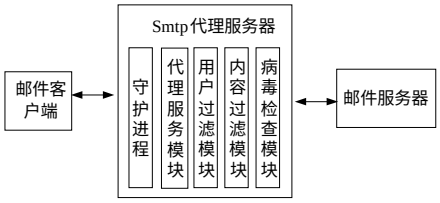

图1 SMTP代理服务器框架结构

2.2 守护进程的实现

守护进程负责SMTP代理服务器的初始化、监听客户端连接、接收客户端的连接请求、创建线程池等。流程如下：

(1)创建线程池、建立socket套接字、设置套接字属性、绑定代理服务器地址、监听客户端连接。

(2)创建一个while循环，把socket套接字添加到可读套接字集合中，调用select函数判断socket套接字上是否有数据需要接收，如果有，则调用accept函数接受客户端的连接。

(3)从连接中获得原始的目的IP地址和端口号，从线程池中获取一个空闲线程与客户端通信，并把accept后的套接字描述符、客户端IP地址和端口号、原始的目的IP地址和端口号传递给该线程。

作者简介：曾新洲(1978－)，男，硕士，主研方向：网络安全；王勇军，博士、副研究员；陈三龙，学士

收稿日期：2006-09-09 **E-mail：**pioneer211@126.com

(4)通信结束，将该线程置为空闲。

2.3 代理服务模块的实现

代理服务器模块主要负责与邮件客户端和邮件服务器的通信。其实现流程如下：

(1)与邮件服务器建立连接。

(2)接收并解析出邮件客户端的命令请求，如果是 HELO、EHLO、QUIT、TURN、RSET、NOOP、VRFY、EXPN 命令，则把该消息转发给邮件服务器；如果是 MAIL、SEND、SOML、SAML 命令，则从该消息中分离出发送邮件用户，进入用户过滤模块处理；如果是 RCPT 命令，则从该消息中获得接收邮件用户，进入用户过滤模块处理；如果是 DATA 消息，则创建一个与邮件用户名对应的文件名，把该消息存放到文件中，并判断 DATA 消息是否结束，如果已经结束，则还原出原始邮件内容，进入内容过滤模块和病毒检查模块处理；如果符合安全要求，则把从客户端接收到的数据转发给服务器，否则，丢弃邮件数据，断开与邮件客户端的连接。

(3)接收邮件服务器返回数据，并把数据返回给客户端。

2.4 用户过滤模块的实现

用户过滤模块主要负责对邮件用户进行过滤处理。代理服务器从邮件客户端的命令请求中解析出发送邮件用户或接收邮件用户后，查找用户过滤规则和用户黑名单，对于符合过滤规则的邮件用户或黑名单中存在该邮件用户，直接断开与该用户的连接，对于其他邮件用户，继续提供服务。

2.5 内容过滤模块的实现

内容过滤模块主要负责对邮件内容的过滤处理，代理服务器还原出邮件原始内容后，对邮件内容进行关键字匹配，如果邮件内容中存在与内容过滤关键字匹配的项，则禁止发送该邮件；如果邮件内容中包含有泄密内容，则把该邮件用户添加到邮件用户黑名单中。

2.6 病毒检查模块的实现

病毒检查模块主要负责对邮件附件的病毒检查，代理服务器还原出原始的邮件数据后，如果邮件中存在附件，则调用杀毒程序对邮件附件进行杀毒处理。

SMTP 透明代理的工作流程见图 2。

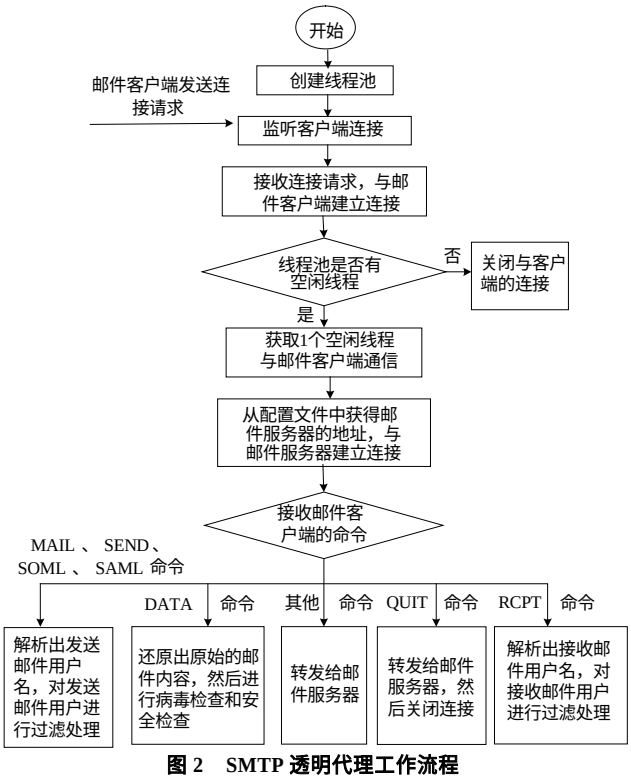

图 2 SMTP 透明代理工作流程

3 实现关键技术

3.1 端口重定向

邮件客户端设置的发送邮件地址为邮件服务器的地址而不是代理服务器的地址，端口号为标准的端口号 25，邮件数据到达代理服务器所在设备时，代理服务器为了获得这些数据，可以采用端口重定向技术。端口重定向是指将用户请求的服务重定向到代理服务器对应服务的监听端口，从而由代理服务器来代理用户发起请求和接收响应。假设 SMTP 代理监听端口为 5000，只需要在运行代理服务器之前，执行相应的重定向规则，即

```
iptables -t nat -A PREROUTING -p tcp -m tcp --dport 25 -j REDIRECT --to-ports 5000
```

执行该规则的目的是为了将目的端口为 25 的 TCP 数据重定向到代理服务器的监听端口 5000，并进行处理。

3.2 并发邮件服务

多个邮件客户端同时发送邮件时，为了不混淆多个客户端的通信数据，可采用多进程、多线程、线程池技术，由于在多进程实现中，存在着派生子进程昂贵、派生子进程后需要用进程间通信在父子进程之间传递信息等问题，而采用多线程有助于问题的解决，因此采用多线程技术。但是，当很多客户端在并发访问代理服务器时，频繁地创建和销毁线程，这会耗费大量的系统资源，极大地降低了系统性能，笔者采用了一种有效的解决方法即线程池技术，在主进程中创建一定数量的线程，并将其保存在线程池中，代理服务器在接收客户端连接后，从线程池中获取一个空闲线程与客户端通信，通信完毕，该线程置为空闲。

3.3 获取邮件服务器的地址和端口号

netfilter 给所有的 TCP 套接字一个新的选项 SO_ORIGINAL_DST(该选项的定义在 linux/netfilter_ipv4.h 中)，用来获得原始的目的 IP 和端口号，代理服务器在接收客户端连接后，通过调用 getsockopt 函数可获得服务器的 IP 地址和端口号。

3.4 处理附件

代理服务器在接收邮件数据时，由于数据部分可能带有附件，不可能一次接收完，此时邮件数据会分多次发送到代理服务器，第一个邮件数据包含有 DATA 命令，除最后一个邮件数据包含结束标识外，其他的邮件数据没有任何标识。可以在接收到 DATA 命令后，循环地接收邮件客户端的数据，并把接收到的数据存入文件中，直到接收到数据结束标志，然后还原出邮件原始内容，调用杀毒软件对附件进行杀毒处理，并对邮件内容进行内容审计，只有通过内容审计的无病毒邮件才可以转发给邮件服务器。

4 系统测试

为了评价本系统的性能，笔者基于 Linux 邮件服务器实现了一个测试平台，测试内容包括：(1)代理服务器监听端口对邮件客户端的影响；(2)代理服务器 IP 地址对邮件客户端的影响；(3)并发邮件服务；(4)泄密内容检查；(5)病毒检查。

测试平台由邮件客户端、代理服务器、Sendmail 邮件服务器 3 个部分构成，如图 3 所示，所有邮件客户端配置为：Pentium 4 CPU 2.66GHz，512MB 内存，IDE 硬盘，100Mb/s 网卡，代理服务器配置为：Pentium 4 CPU 2.66GHz，1GB 内存，IDE 硬盘，两块 100Mb/s 网卡，Sendmail 邮件服务器配置为：Pentium 4 CPU 2.66GHz，1GB 内存，IDE 硬盘，100Mb/s

网卡。SMTP 代理服务器、邮件服务器、所有的邮件客户端都安装了 Redhat Linux9.0 系统，所有的邮件客户端与网关直连，在网关设备上安装 SMTP 代理服务器，代理服务器与邮件服务器直连，代理服务器监听端口为 5000，各设备之间的连接情况及 IP 地址如图 3 所示。

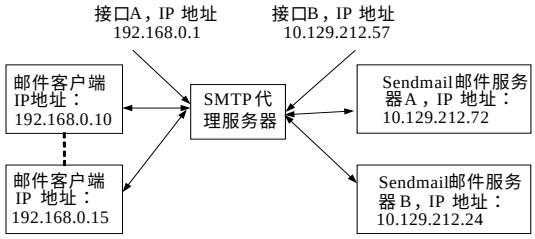

图 3　系统测试平台

根据测试内容，可以测试以下案例：

(1)把 SMTP 代理服务器的监听端口号改为 5003，邮件客户端感觉不到任何变化，可正常发送邮件；

(2)代理服务器原 IP 地址为 192.168.0.1，更改代理服务器的 IP 地址为 192.168.0.2，同步修改客户端的默认网关地址为 192.168.0.2，邮件即可正常发送，不需要修改其他配置；

(3)从 IP 地址为 192.168.0.10~192.168.0.15 的 6 个邮件客户端同时向邮件服务器 A、B 发送邮件，代理服务器能正常处理；

(4)设过滤策略为“不包含某确定关键字，但发送包含该字段”的邮件，系统阻断，无法完成发送；

(5)发送带 ExploreZip.worm.pak 病毒的邮件，系统阻断，无法完成发送。

测试结果表明本系统已达到了以下设计目标：

(1)用户透明，易于使用，对代理服务器 IP 地址和端口号的修改，不影响邮件客户端的操作。

(2)功能完善，SMTP 透明代理可以为任何邮件服务器提供服务。

(3)有效检测，防止病毒入侵。

(4)有效检查，防止机密泄露。

5　结束语

本文分析了面向安全检测的 SMTP 透明代理服务器的设计方法，对邮件用户进行了过滤处理，并对邮件内容进行安全检查，提高了内部网络邮件系统的安全性。

参考文献

1 Simple Mail Transfer Protocol[S]. RFC 821, 1982-08.

2 Stevens W R, Fenner B, Rudoff A M. Unix Network Programming——The Sockets Networking API[M]. Massachusetts, USA: Addison-Wesley, 2004.

3 胡居成, 李侠林, 黄　皓. 一种 HTTP 代理服务器的设计与实现[J]. 计算机工程与设计, 2004, 11(25).

4 郑　琪, 方思行. 通用多线程服务器的设计与实现[J]. 计算机工程与应用, 2003, 39(16).

5 唐　寅, 王蔚然. Internet 防火墙透明代理技术的研究与实现[J]. 计算机科学, 2002, 29(4).

（上接第 180 页）

4　结论

以分布式数据库系统提供的服务作为入侵检测的对象，采取面向服务的入侵检测机制，通过检测当服务被攻陷后表现出来的可观测的现象来检测入侵的发生。通过在入侵攻击图上，跟踪每一个入侵攻击实例的攻击路径，既简化了整个检测过程，又提高了并发程度，有利于系统同时处理多个并发的入侵攻击行为，提高了效率。在处理检测到的入侵攻击时，改进了传统的基于校验点方法，提出了一种基于破坏隔离与围堵的安全恢复策略。在破坏隔离阶段，可疑受损对象被迅速隔离，不允许和其他事务、对象进行通信，可以防止破坏的传播。在释放被错误隔离的数据时，以日志中记录的更新为依据，以破坏检测阶段检测到的恶意事务为源头，把破坏的传播以及被污染的数据在图上直观地反映出来，避免了复杂推理过程，对被破坏和污染的数据进行准确定位、处理、恢复，不必将整个系统进行回退，最大限度地保证数据库中其他服务的正常运行，保证系统向合法用户提供连续的服务，从而达到了容忍入侵的目的。由于在破坏围堵阶段的破坏隔离是在更新(比事务粒度小)上进行的，因此可以增加执行的并发程度，提高数据的利用率，有利于系统向用户提供连续的服务，可用于构建提供关键性业务且对实时性要求较强的分布式数据库服务安全保护系统。

参考文献

1 Barbara D, Goel R, Jajodia S. Using Checksums to Detect Data Corruption[C]//Proceedings of the 2000 International Conference on Extending Data Base Technology. 2000.

2 Jaynarayan H L. Organically Assured and Survivable Information Systems[EB/OL]. (2003-05). http:www.darpa..mil/ipto/programs/oasis.

3 Pal P, Webber F, Schantz R, et al. Intrusion Tolerant Systems[C]//Proc. of IEEE Information Survivability Workshop. 2000.

4 Ammann P, Jajodia S, Liu P. Recovery from Malicious Transactions[C]//Proc. of IEEE Transactions on Knowledge and Data Engineering. 2002-09.

5 Carver C, Pooch U. An Intrusion Response Taxonomy and Its Role in Automatic Intrusion Response[C]//Proceedings of IEEE Workshop on Information Assurance and Security. 2000.

6 Ammann P, Jajodia S, McCollum C D, et al. Surviving Information Warfare Attacks on Databases[C]//Proc. of the IEEE Symposium on Security and Privacy. 1997: 164-174.

7 Jajodia S, McCollum C D, Ammann P. Trusted Recovery[J]. Communications of the ACM, 1999, 42(7): 71-75.