防火墙中NNTP代理的设计与实现

王美珍　李之棠　杨红云（华中理工大学计算机科学与技术学院 430074）

摘要：本文针对目前防火墙产品中缺乏对NNTP的访问控制功能的状况，提出了NNTP代理的设计思想，并详细说明了各模块的实现方法。为了解决NNTP中新闻伪造的问题，还提出了用一次性口令对NNTP中使用特定命令的用户进行身份认证的解决方案。

关键词：NNTP　PROXY　FIREWALL　OTP

1　引言

随着Internet的高速发展，国家政治、军事、经济以及社会生活等各个方面中的网络安全问题日益突出，各种网络安全工具也应运而生，其中最受人注目的当属网络防火墙产品。几乎所有的防火墙都具备包过滤、网络地址转换和应用代理等功能，应用代理通常只包括HTTP、FTP和邮件协议的代理(如CheckPoint的Firewall-1)。随着电子新闻系统的迅猛发展，NNTP(Network News Transfer Protocol)也开始受到越来越严重的安全威胁。因此在防火墙中加入NNTP代理，实现对新闻组查看和发表权限的访问控制以及对使用特定命令的用户进行身份认证是十分必要的。

2　NNTP代理的设计

2.1　NNTP代理的基本原理

代理是客户与服务器之间的应用层转发器，并在其上加入各种检查、控制和审计。它由客户代理和服务器代理构成。客户代理代替客户与服务器会话，服务器代理代替服务器与客户会话。作为防火墙代理则还对客户发向服务器的请求进行访问控制，对外部服务器发向内部客户的应答进行内容检查。

代理分为不透明和透明代理两种。不透明代理需要客户显示设置代理服务器，而透明代理则不需要，使用者也无需知道防火墙的地址，使用上比传统的proxy机制更简便。本文描述的是透明代理，其基本原理是:当客户欲同服务器建立连接时，防火墙网络层地址转换模块将目的地址转换成防火墙的地址，这样该连接变成了客户与代理的连接，以后所有该连接的后续包都做相同的转换，实现了客户与代理的透明连接。然后代理根据服务器IP地址或其他标识服务器的地址，与真正的服务器建立连接，从服务器的角度看，服务器与代理在会话，从而屏蔽了内部网。

防火墙代理在实现上可以有两种基本的模式。第一，客户与代理的会话和代理与服务器的会话是并发的；第二，客户先与代理会话结束后，再由代理与服务器会话。前者主要用于实时性较强的应用，后者主要用于实时性较差，且对访问控制比较严格的应用。

NNTP代理是基于TCP的应用，因此在实现时采用两个并发连接的结构，即客户与代理建立连接，代理再与服务器建立连接，在客户与代理的连接中进行访问控制，在服务器与代理的连接中进行内容检查。代理将符合访问控制的请求转发给服务器，将服务器符合安全政策的应答转发给客户。

防火墙中代理与NAT、包过滤间的数据流图如图1所示：

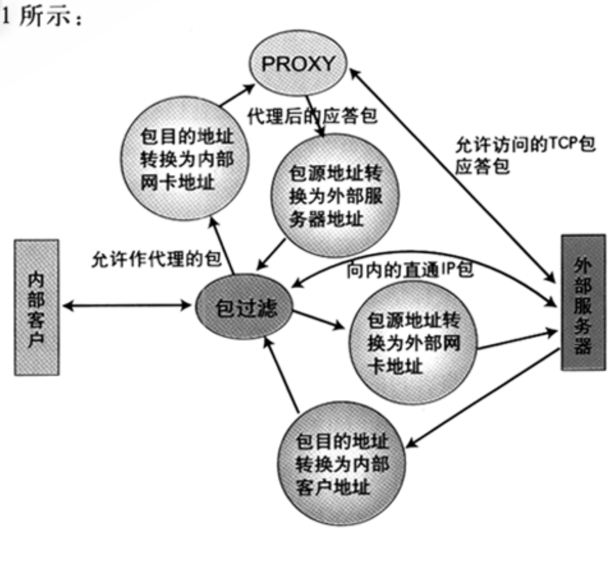

图1　防火墙中代理与NAT、包过滤的数据流图

2.2 NNTP 代理的结构设计

NNTP是一个Internet标准 [1]，它基于TCP的流式连接,该连接存在于网络中的客户和在磁盘上保存网络新闻的服务器主机之间。流式连接允许客户与服务器交互地协商几乎无延迟的数据传输,因而使得重复的数据数量很少。另外，还由于Internet的高传输速率，使得至今新闻的传输胜过原来的UUCP网络。NNTP安全的一个主要问题是它可能使伪造发送者说明的文章插入到新闻流中,称为伪造新闻（news faking）[1] [2] [3]。一个对NNTP的扩展是对特定命令要求用户身份验证。

在代理的实现中，一个关键的问题就是如何实现对同时与服务器和客户建立控制连接和数据连接的支持[5]。控制连接的建立比较简单，它在客户欲与服务器建立连接的时候,代理与客户建立连接,随后代理与服务器建立控制连接。在本系统处理过程中,代理成为客户的代理服务器，同时是服务器的代理客户。此外，代理将客户的命令转发给服务器,这样只有代理主动向服务器建立连接,避免了外部主机向防火墙建立连接的情况出现,提高了防火墙自身的安全，同时简化了防火墙的设计。

此外,本系统在实现上采用线程机制,在一定程度上降低了系统的负载，提高了系统的运行效率。

其主要框图如图2所示：

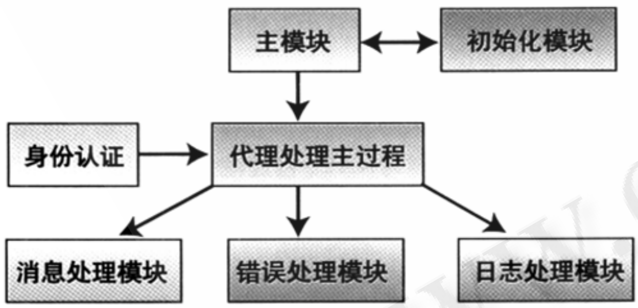

图 2　NNTP 代理的结构框图

主模块主要完成进程的守护，从防火墙系统中读入配置，初始化全程信息变量和信号。然后守候一个新连接,新连接到来后,创建一个线程,获取客户端的地址和用户信息，并将客户的IP和端口变为代理服务器的源IP和端口。然后调用NAT的系统调用，取得服务器的地址和访问控制信息，并将代理服务器的目的IP和端口变为服务器的IP和端口，建立与服务器的连接，读取访问控制信息，进入代理处理主过程。

代理处理主过程对收到的客户端的命令请求，与访问控制规则匹配，如果匹配成功，则转发该命令给服务器,否则不转发并返回应答信息给客户端;对收到的服务器应答，进行检查，并做出相应的处理。

消息处理模块主要完成对消息MESSAGE的处理。MESSAGE是用于不定长字符串缓冲区管理的数据结构。缓冲区由连续的若干块构成,它可在需要时扩展,直至允许的最大块数。

错误处理模块主要处理程序中出现的错误，建立统一的错误日志，以便管理员查看出错原因。

日志记录模块记录用户访问的时间、源IP地址、源端口、目的地址、目的端口、使用的协议、访问的新闻组以及使用的命令。

身份认证模块用来对使用特殊命令(POST和IHAVE)的用户进行身份认证。

3　NNTP 代理的实现

3.1 主模块

主模块的流程如图3所示：

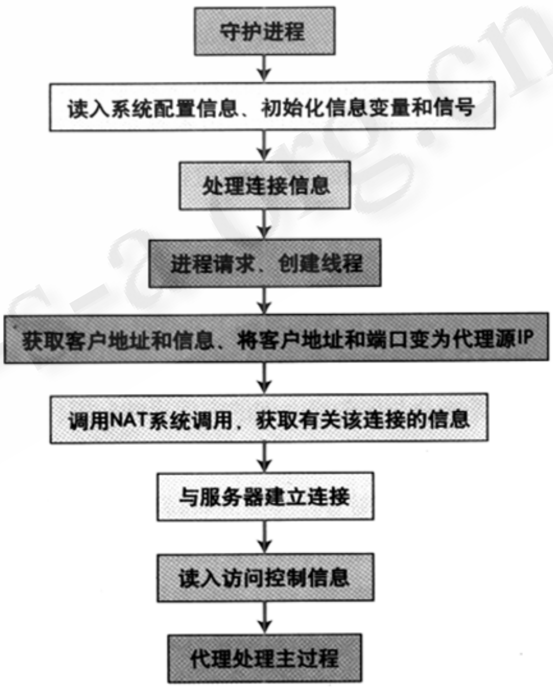

图 3　NNTP 代理主模块的结构图

由于本代理采用透明模式，因此客户访问服务器时，在正常情况下是在客户与服务器间建立连接，但为了将请求定向到代理上，需将服务器的地址转换为防火墙的地址，防火墙收到连接请求后，它请求NAT模块告知其真正的服务器地址和有关的访问控制信息，

然后它与服务器建立连接，在两个连接构成的通道上进行转发和访问控制。

此接口是一个系统调用，其定义如下：

```
_syscall2(int,get_connect_info,struct st_connect_info *,info,int,len)
```

其中 struct st_connect_info 定义如下：

```
struct st_connect_info {
  __u32 saddr ; /* 源 IP 地址 */
  __u16   sport ; /* 源端口 */
  __u32   daddr ; /* 目标 IP 地址 */
  __u16   dport ;/* 目的端口 */
  int protocol ; /* 协议 TCP/UDP */
  int offset ;  /* 访问控制信息的偏移 */
  int number ; /* 访问控制信息的块数，*/
  char    action ; /* */
};
```

3.2 代理主过程

对收到的客户端命令进行分析，如果客户端发出的为POST或IHAVE命令，代理服务器检查该用户是否通过身份认证，如果通过，代理服务器将请求转发给服务器，否则丢弃该请求包。如果服务器客户端继续传送数据，代理服务器客户端传送的数据头进行检查，获得新闻组名，并与访问控制规则进行匹配，如果匹配成功，则将所有数据（包括头和正文）转发给服务器，否则不转发给请求，并给客户端返回该服务被禁止的应答；如果客户端发出的为GROUP命令，代理服务器将此新闻组与访问控制规则进行匹配，如果匹配成功，则将请求转发给服务器，否则不转发该请求，并给客户端返回该服务被禁止的应答。

3.3 一次性口令认证(OTP)[5] [6]

NNTP中，允许所有的新闻都保存在一个中央主机上，以便让网络上的所有用户（假定都是本地的）使用基于NNTP的客户程序进行新闻的阅读和投递，这就不可避免地会出现伪造新闻的现象。因此，本系统采用对特定命令(POST、IHAVE)进行用户身份认证的方法来解决这个问题。为了避免在网络上明文传输用户私有口令，来防止用户口令被窃听盗用，故采用一次性口令来进行身份认证。一次性口令认证的基本思想是客户端每次使用一个不同的口令。其基本方法是，客户（用户）每次请求认证时，服务器都会向该客户提出一个不同的挑战(迭代值和种子)，客户根据自己拥有的私有口令和挑战计算出一个响应，提交给服务器，服务器与客户做同样的计算，检验客户的响应是否正确，从而决定客户是否通过认证。这一基本认证过程如图4所示。

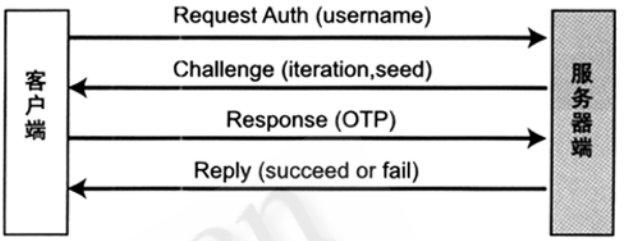

图 4 一次性口令认证过程

其中，OTP = MD5 (n)(MD5(strcat(seed, private password)))。

4 结论

本系统已经在我们开发的防火墙产品FW3000中得到了应用，已通过许多管理部门的测试和大量用户的使用，证明本系统对NNTP的访问控制和避免新闻伪造的设计与实现是成功的。■

参考文献

1 Brian Kanto, Phil Lapsley ,Network News Transfer Protocol, RFC 977, Feb. 1986

2 The Network Administrators' Guide , Olaf Kirch , Mar. 1996

3 M.Horton, R.Adams. Standard for Interchange of USENET Messages, RFC 1036, Dec.1987

4 RiszSalz. Inter Net News: Usenet transport for Internet sites, In USENIX Summer Conference—SanAntonio, TX. ,Summer 92

5 Chris Hare Karanjit Siyanz著 刘成男等译. Internet防火墙与网络安全，机械工业出版社，1998年2月

6 [美] Garfinkel S著，王启智、申功迈等译．实用UNIX和INTERNET安全技术，电子工业出版社