Http隧道在穿越NAT/防火墙技术中的应用

韩 凤,施 寅
(北京交通大学 计算机系,北京 100044)

摘 要:要让私有IP地址的用户通过SIP等协议进行会话,就必须使SIP信令和媒体流穿越NAT/防火墙。STUN,ICE等现有协议只能应用于UDP,不能用在有防火墙限制以及只能TCP连接的环境下。文中在研究了http协议中一些常用的方法,如:Post,然后借鉴并结合了TURN协议的一些控制方法,提出了SIP phone中用http隧道穿越NAT/防火墙的方案,并且详细叙述了SIP phone注册、呼叫过程。该方法在防火墙受限制端口或者UDP连接的网络环境下,使用户仍然可以进行正常通信,弥补了在现实环境中STUN,ICE协议的不足。

关键词:防火墙;http协议;SIP;中继;NAT
中图分类号:TN915 **文献标识码**:A **文章编号**:1673-629X(2006)05-0163-03

Application of Http Tunnel in Traversal NAT/Firewall

HAN Feng, SHI Yin
(Dept. of Computer and Information Technology, Beijing Jiaotong University, Beijing 100044, China)

Abstract: Only when the control and media flow traverse firewall/NAT, can people use private IP address to make sessions with SIP protocol. STUN, ICE protocol can only be used in UDP, but doesn't effect in the firewall restriction or only TCP connection environment. The paper studies some methods of http protocol, consults the TURN protocol then describes using the http tunnel in the traverse firewall/NAT. A detail instance is also presented in order to explain how to use http tunnel in register and call flow. This way can make user communicate when this is a firewall restrict the port or UDP connection, meanwhile it makes up the shortcoming of the STUN and ICE.

Key words: firewall; http protocol; SIP; relay; NAT

0 引 言

目前NGN网络逐步从试验走向商用[1],大量的企业网和驻地网基本上都采用私有IP地址通过出口的NAT/FW接入到公网。而在企业网和驻地网上,要求承载语音、多媒体和视频等业务越来越普遍。如果终端用户处在NAT之后,由于NAT仅对IP包的地址及端口号进行转换,而SIP[2]协议真正的媒体连接信息是放在SDP(即IP包的负载)中传递的,这部分私网地址无法被NAT映射成公网地址传到对方用户,所以媒体流是无法真正建立起来的,并且NAT如何保持记录的会话地址转换直到通话结束才被删除,这都是目前这一领域有待解决的问题。

另外在许多企业组网的过程中都要设置防火墙,提高网络安全。这些防火墙不仅具有NAT的功能,还可以限制内网外出端口,使得防火墙之后的用户利用SIP协议建立通信过程中也产生一定的困难。

现有穿越NAT的方法,如STUN[3],虽然能穿透大部分的NAT,但是如果一个NAT是对称性的,STUN协议就无能为力。ICE[4]方法采用动态穿越方法,根据不同的网络环境决定最后的穿越方法,虽然大多数NAT都可以穿越,但是如果网络中存在一个防火墙,该防火墙限制外出端口或者只开放http 80端口。上述方法都存在困难。

文中提出了在这种网络环境中一种实现穿越NAT/防火墙新方法——http隧道。这种方法可以让用户在防火墙限制端口或者只开放http端口的情况下利用SIP建立语音通信,同时也可以适用一般的网络情况。

1 http隧道的原理

现有的防火墙大多具有NAT功能,在过滤数据包的时候,不仅仅只检查TCP或者UDP数据包中的端口信息,甚至还要对应用层的数据进行检查。例如如果防火墙只开放80端口,那么所有外出的数据包必须是访问外部的TCP 80端口,还要检查应用层的数据是否符合http包头。

因此防火墙后用户将通信的数据包按照http格式进行封装,发给外网服务器,然后由服务器解析数据包,通过服务器实现信令、媒体的中继(SIP、media relay)。最终实现防火墙后的用户与其他用户通信。

TURN(Traversal Using Relay NAT)协议详细描述了如何用中继方式穿越NAT,但是TURN协议并不能穿越

收稿日期:2005-08-08
作者简介:韩 凤(1981-),男,上海人,硕士研究生,研究方向为IP通讯、软交换;施 寅,教授,硕士生导师,硕士,研究方向为计算机图形学。

防火墙,http 隧道采用 TURN 的方法去控制 http 隧道的建立。

1.1 http 协议

http[5]协议是 request/response 的协议。http 的消息分成两大类:Request 和 Response,其基本结构是:

generic - message = start - line
* message - header
CRLF
[message - body]

其中消息体(message - body)是可以选择的,如果一个 http 消息中包含消息体,它的消息头必须包含 Content - Length 域,给出消息体的长度。协议中规定用户的程序如果收到一个无效的长度必须通知用户。http 协议采用请求/响应的模式,请求的双方分别为客户端(Client)和服务器端(Server),Client 发出的请求方法有 GET, HEAD, POST, PUT 和 DELETE 等,常用的有 GET 和 POST。Server 端用 Response 消息回应用户的请求,并带上应答的状态信息和用户请求数据。

http 隧道建立过程主要用到了 POST 和 GET 方法。

1.2 TURN 协议

TURN[6]的全称为 Traversal Using Relay NAT,即通过 Relay 方式穿越 NAT。TURN 穿越 NAT 问题的设计思路是:对于私网接入用户来说,它们可以通过某种机制预先得到其私有地址对应在公网的地址(STUN 方式得到的地址为出口 NAT 上的地址,TURN 方式得到地址为 TURN Server 上的地址),然后将报文负载中描述的地址信息直接填写为公网 TURN Server 上的地址。这样报文负载中的内容在经过 NAT 时就无需被修改了,只需按普通 NAT 流程转换报文头的 IP 地址即可,负载中的 IP 地址信息和报文头地址信息又是一致的,TURN Server 对后续的报文根据分配的地址和端口信息作地址变换后 Relay 转发。

TURN 协议是通过在服务器上的绑定(binding)记录来进行数据中继的,绑定格式如表 1。

表 1 服务器记录格式

本地五元组					远端五元组				
Source IP	Source Port	Dest IP	Dest Port	Proto	Source IP	Source Port	Dest IP	Dest Port	Proto

协议中五元组指:通讯双方的 IP、端口以及协议(TCP 或 UDP)。

本地五元组用来记录防火墙后的用户的通讯记录,远端五元组用来记录通讯另一方的地址。NAT 后的用户把通信数据发送给服务器,服务器中转数据时首先根据数据的源地址查找绑定记录,找到相符合的本地五元组,然后将源地址变成远端五元组的源 IP, port 发往相应的目的地址。目的地址接收到数据以后,返回数据给远端五元组的源 IP, port,即 TURN 分配的地址。服务器收到以后,根据绑定记录的本地五元组将数据再发送给 NAT 后用户。

1.3 http 隧道

http 隧道也是由客户端和服务器端组成。客户端是由隧道控制(tunnel control)功能和 http Client 功能组成。其中隧道控制完成和 Turn Server 命令交互,建立隧道;http Client 完成本地的端口映射,并且将收到的数据封装成 http 的格式发往服务器。

服务器端也就是 Tunnel Server,由隧道控制和 http Server 组成。http Server 负责对近来的数据包进行解包,把返回的响应封包发送。隧道控制 确定防火墙后的用户和其他某个用户通信的一一对应的关系(TURN 控制功能)。

防火墙后的用户要建立 http 隧道,首先用 http GET 和 POST 的方法连接在公网的服务器[7],GET 建立的连接用于服务器向用户返回数据,POST 建立的连接用于客户向服务器发送命令或者数据。服务器通过绑定过记录进行数据中继。例如:用户 A 通过 POST 的连接发送控制命令给服务器。服务器接接收数据以后,解析 http 包,然后建立新的绑定记录,如表 1。表中的远端五元组中的目的地址 Dest IP 和 port 是通讯的对方 B,其地址由用户 A 发命令给服务器。服务器生成记录以后,http 隧道建立完毕。用户 A 可以把数据通过 http 的 POST 数据发送给服务器,服务器根据表中所记录地址将数据发送给 B。B 返回的数据发给服务器,服务器再通过 http 的 GET 建立的连接返回数据给 A。

在 http 隧道建立的同时,在 NAT/防火墙之后用户也要建立本机通讯端口和 http 隧道一一对应的关系。例如:用户 A 的 SIP 通信端口,对应着 TCP 的 2 个端口。这 2 个 TCP 端口是由 POST,GET 方法建立的。

http 隧道建立以后,由防火墙后的用户去维持隧道,否则 NAT/防火墙会认为这个连接超时,从而断掉隧道的 TCP 连接。隧道销毁时,由 NAT/防火墙后用户完成。当用户关闭与服务器之间的 TCP 连接时,服务器收到关闭命令以后,自动将相应的绑定记录从服务器中删除。

http 隧道方法提出了一个比较完善、安全的解决方案。这种方案不仅适用于 NAT/防火墙限制内网外出的端口(只开 http 端口)的特殊情况,也可以应用于一般的网络情况,如网络中存在对称性 NAT。

2 实现方案

假设通信一方处于限制端口的 NAT/防火墙之后。终端 A 要向 Register Server 进行注册,然后与 B 进行通信。

A 所在的内部地址是 192.168.1.5,NAT/防火墙地址是 61.233.23.200;Tunnel Server 的地址是 61.233.23.201;终端 B 的地址是 219.242.249.22,注册服务器的地址是 202.112.147.177,如图 1 所示。

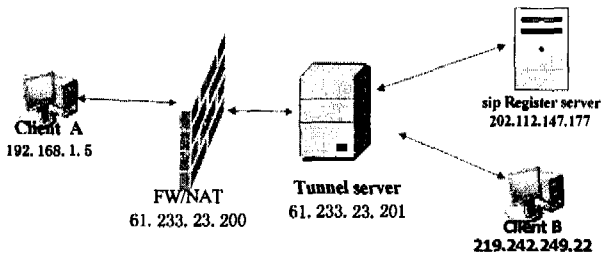

图 1　FW/NAT 网络拓扑图

2.1　注　册

假设用户 A 所有接受、发送 SIP 消息都是用同一个本地端口 5060。首先用户 A 为 SIP 消息端口(UDP)分配 2 个 TCP 连接,分别用 http 的 post 和 get 方法建立 2 个 TCP 连接,同时确定本地中继端口 D(UDP)。分配完成后,所有 SIP 消息端口发出的消息送到本地的中继端口 D,http Client 从 D 接收数据然后再利用建立的 POST 连接发送出去(如表 2)。

表 2　本机绑定记录

UA (UDP 端口)	TCP 端口	Method	TCP 端口	Method	Relay Port
5060	40000	POST	40001	GET	D

表中的 40000、40001 是指 TCP 连接对应的端口,Method 表明每个 TCP 连接的作用以及建立 http 协议的方法。

服务器接收到 post 和 get 的连接后,也会建立 2 个映射,同样也要进行标记,如表 3。

服务器解析 http 的包头,根据 http 的方法,以及数据包的源、目的确定本地五元组。其中本地五元组的 Source IP、Source Port 是指 A 用户的 NAT 以后 TCP 源地址,Dest IP、Dest port 指服务器监听的地址,Method 是建立 TCP 的方法。远端五元组的 Source IP、Source port 是由服务器分配给用户的有效(公网)的地址。服务器生成这个记录以后,将分配的地址(61.233.23.201:12301)信息返回给用户 A。

用户 A 收到该信息以后,将注册服务器的信息以 send 命令的形式发往服务器。其中 send 命令包含了数据最终要发送的目的地,以及要发送的数据。也就是说,用户发送的 send 命令中包含了注册服务器的地址以及注册的 register 消息。

服务器收到以后,根据 send 命令中的目的地信息,填充远端五元组的 Dest IP、port,然后发送 register 消息。注册服务器的响应消息也发回给 61.233.23.201:13201,最终返回给用户 A 的监听 SIP 消息的端口。整个过程如图 2 所示。

表 3　服务器绑定记录

本地五元组					远端五元组				
23.200	5000	23.201	80	POST	23.201	12301			SIP
23.200	5001	23.201	80	GET	23.201	12301			SIP

2.2　呼　叫

用户 A 要呼叫公网上的用户 B。A 通过上述方式在发送 invite 消息之前要确定自己的 RTP 发送和接收端口。A 首先为 RTP 的收发端口建立 TCP 连接,并且向服务器发送隧道建立命令,服务器返回给用户 A 分配的 IP 地址和端口。

用户 A 构建 invite 消息,将服务器返回的 IP 地址和端口写在该 invite 消息的 SDP 中,发送给用户 B。

用户 A 接收到 200 OK 的消息以后,解析 B 的 RTP 的端口,接着再封装成 send 命令告诉服务器用户 A 要通讯的对端的 IP 地址。

最后用户 A 可以和 B 进行通讯。

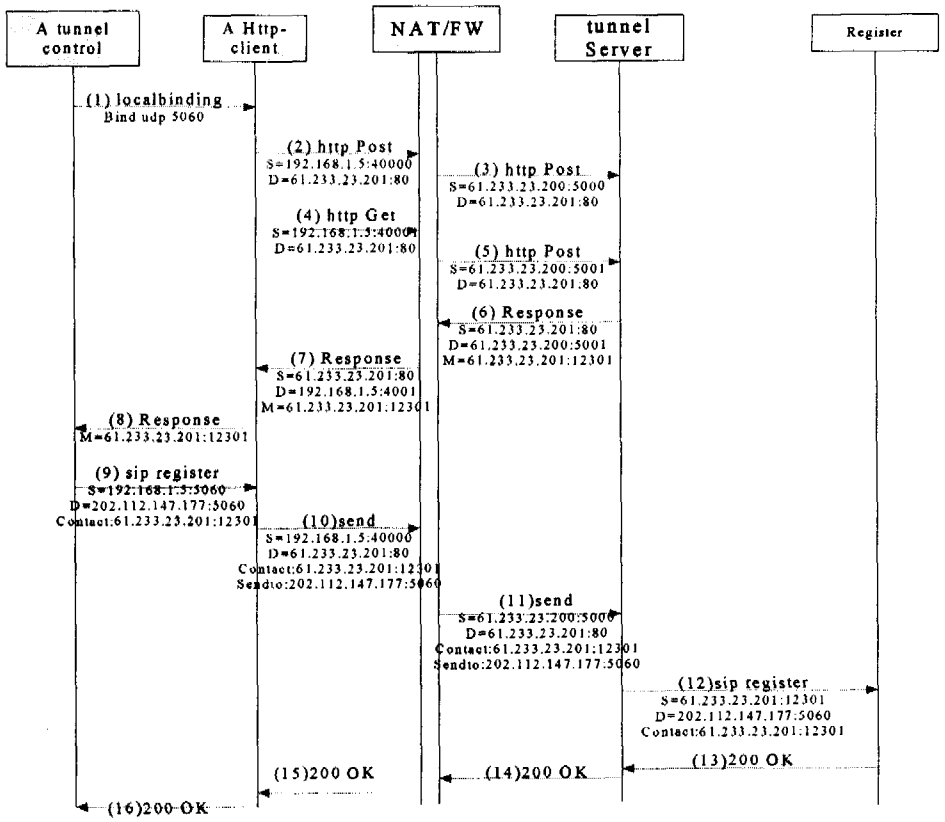

图 2　注册时序图

3　结束语

提出通过客户和服务器建立的 TCP 连接,并对 SIP 信令以及媒体流的中转,使处于私网内外的终端发出的用

(下转第 169 页)

```
(cmd);
BufferedReader in = new BufferedReader(new InputStreamReader
(ps.getInputStream()));
String createdon = in.readLine();
String author = in.readLine();
String type = in.readLine();
String comment = "";
String tmp;
while(tmp = in.readLine()! = null)
    comment + = tmp;
ps.destroy();
/* 代码示例 */
```

其中"cleartool"是 ClearCase 的命令行工具(区别于一些图形化的工具),基本命令都以其为开始。"describe"用于输出指定对象的描述信息,其可选项"-fmt"可用于指定输出格式。该选项的参数中"%Sd"为输出创建日期,"%Fu"为输出作者,"%[type]p"为输出文件类型,"%c"为输出该文件的描述信息,"\n"为换行符。也就是说执行该命令后的输出可能如下:

```
2004-05-21
Fred
Text
"a.java is created to test if 'javac' could compile .java files"
```

"Runtime.getRuntime().exec(cmd)"方法是用来输出命令到操作系统级执行,因为平时执行 ClearCase 命令就是在命令提示符中输入并执行的。并且该方法还会返回执行命令的进程的句柄,即 Process 对象。通过 Process 类的 getInputStream()方法,可以得到执行该命令后的输出(对我们的程序来说是输入流)。分析输入流(在这里每一行分别代表一个元数据,当然最后的 comment 元数据可能由多行组成),就可以得到想要的上述四个元数据了。

3 结　论

在功能点分析时,人为的数据收集较多。利用该方法可以减少人为的行为,让部分数据的收集自动化。更可以使数据来源可靠、及时,这对基于功能点方法对软件进行测量来说是非常重要和有用的。

参考文献:

[1] Kusumoto S. Function point measurement from Java programs [A]. International Conference on Software Engineering[C]. [s.l.]:[s.n.],2002.576-582.

[2] Al-Hajri M A. Modification of standard function point complexity weights system[J]. Journal of Systems and Software, 2005,74(2):195-206.

[3] IFPUG. Function Point Analysis Nears Approval As First International Standard For Software Functional Size[EB/OL]. http://www.ifpug.org/about/ISOPress.htm,2002.

[4] Longstreet D. Function Point counting practices. Manual release 4.1[Z]. IFPUG. 2001.

[5] IBM Rational ClearCase. User Manual[Z]. 1999.

[6] Q/P Management Group, INC. Solutions for improving quality and productivity[EB/OL]. http://www.qpmg.com/index2.htm, 2003.

(上接第 165 页)

UDP 承载的 SIP 消息和媒体流穿越大多数的防火墙和 NAT。这种方案的优点就是不需要对现有的防火墙做任何处理,利用 http 协议本身的机制去穿越。并且结合 TURN 的控制方法,使这种方式更加合理。而且用 http 隧道穿越方法比较简便,因为需要服务器去做信令、媒体流的中转,当与公网交互的终端数或出入私网的媒体流数据量较大时,可能成为瓶颈。如果将这种方案应用在 P2P 网络,可以很好地解决这一问题。

参考文献:

[1] 李鸿彬,杨雪华,雷为民 .TURN 服务器原型系统的设计与实现[J].计算机应用,2005,25(7):1688-1691.

[2] Rosenberg J. SIP: Session Initiation Protocol[S]. RFC3261, IETF,2002-06.

[3] Rosenberg J, Weinberger J, Huitema C, et al. STUN-Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)[S]. RFC 3489,2003-03.

[4] Rosenberg J. Interactive Connectivity Establishment(ICE):A Methodology for Network Address Translator (NAT) Traversal for the Session Initiation Protocol(SIP)[S]. draft-ietf-mmusic-ice-05,2005-07-17.

[5] UC Irvine J, Gettys J. Mogul HTTP-Hypertext Transfer Protocol[S]. RFC 2068,1997-01.

[6] Rosenberg J. Traversal Using Relay NAT(TURN)[S]. draft-rosenberg-midcom-turn-07 (work in progress), 2005-02-21.

[7] 黄伟峰. http tunnel 技术在 VOIP 系统中的实现[J].微型电脑应用,2004,20(2):44-47.