NAT 和防火墙穿越技术研究

韩可玉[1],王振涛[2],苏继斌[3]

(1.中国人民解放军 71352 部队司令部,河南 安阳 474500;2.中国人民解放军 71336 部队司令部,河南 安阳 474500;3.中国人民解放军 71391 部队司令部,河南 开封 475000)

摘 要:在研究分析常用的 NAT 和防火墙穿越技术优缺点的基础上,设计了“STUN+TURN”的 STR NAT 和防火墙穿越整体方案,同时对该方案涉及的相关问题进行了深入研究,形成了相得益彰、浑然一体、普适易用的 NAT 和防火墙穿越解决方案。

关键词:NAT 和防火墙穿越;STUN;TURN

中图分类号:TP309 **文献标识码**:A **文章编号**:1672-7800(2014)003-0134-03

0 引言

随着互联网的发展,IP 资源变得越来越紧张,为了解决 IP 资源匮乏的问题,出现了网络地址转换(NAT)方法。NAT 是将 IP 地址从一个编址域映射到另外一个编址域的方法[1],最典型的应用是把私有 IP 地址映射到互联网的公有 IP 地址上。NAT 在节省 IP 地址空间的同时,也破坏了 Internet 最基本的“端到端的透明性”的设计理念,增加了网络的复杂性,阻断了现有的很多 IP 应用。特别是像 SIP 这样的端到端软交换协议,由于需要协商多个端口并维护多个 UDP 或 TCP 数据流,无法自己穿越 NAT[2];另外,出于安全的考虑,绝大多数的企业都配置了专用的防火墙。和 NAT 一样,防火墙在增加安全性的同时,也使现存 IP 应用无法穿透。基于此,本文在研究常用 NAT 和防火墙穿越技术的基础上,提出了相应的解决方案,使具有 NAT 和防火墙问题的用户也可以像公有 IP 地址的用户一样,顺畅地使用各种网络服务。

1 常用 NAT 和防火墙穿越技术介绍

目前,常用的 NAT 和防火墙穿越技术主要有 STUN(Simple Traversal of UDP Through Network Address Translators,即 UDP 对 NAT 的简单穿透方式)和 TURN(Traversal Using Relay NAT,即通过转发的方式穿透 NAT)两种。

STUN 主要用于 UDP 传输,其基本思想如图 1 所示,STUN 客户端向 NAT 外的 STUN 服务器通过 UDP 发送请求 STUN 消息,STUN 服务器收到请求消息,产生响应消息,响应消息中携带 STUN 客户端在 NAT 上对应的外部端口,响应消息通过 NAT 发送给 STUN 客户端,STUN 客户端通过响应消息体中的内容得知其在 NAT 上对应的外部地址,并且将其填入以后呼叫协议的 UDP 负载中,告知被叫端(Peer)的 UDP 接收地址和端口号为 NAT 上映射的 IP 地址和端口号[3],这样,应用程序就可以收到被叫端发来的报文。STUN 的优点是处理简单,缺点是不支持 TCP,也不支持对称类型(同时限制 IP 和端口)的 NAT。

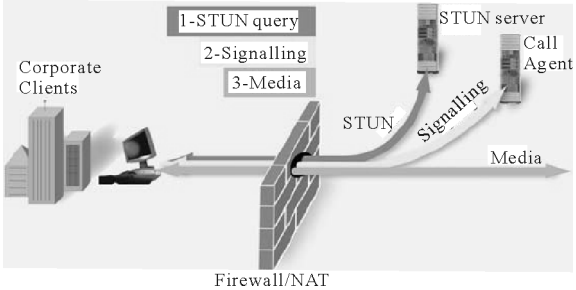

图 1 STUN 穿透 NAT 和防火墙示意图

TURN 的基本思想如图 2 所示,NAT 或防火墙内的 TURN 客户端通过向 TURN 服务器申请绑定,获得外部 IP 地址和端口(由 TURN 服务器分配),这样该用户就可以使用这个外部的 IP 地址和端口接收 NAT 和防火墙外的用户发送的报文[4]。TURN 的优点是可以穿越所有类型的 NAT 及防火墙,缺点在于所有报文都必须经过 TURN 服务器转发,增大了包的延迟和丢包的可能性,

作者简介:韩可玉(1972—),男,硕士,中国人民解放军 71352 部队司令部高级工程师,研究方向为计算机网络与信息安全;王振涛(1976—),男,中国人民解放军 71336 部队司令部工程师,研究方向为计算机网络与指挥自动化;苏继斌(1975—),男,硕士,中国人民解放军 71391 部队司令部工程师,研究方向为网络管理与网络安全。

同于也增加了 TURN 服务器的负载，容易造成网络瓶颈。

2　NAT 和防火墙穿越整体解决方案

为了解决 NAT 类型的复杂性，使具有 NAT 和防火墙问题的用户也可以像公有 IP 地址的用户一样，顺畅地使用各种网络服务，根据 NAT 和防火墙穿越原理和常用方法的特点，设计提出了“STUN＋TURN”的 NAT 和防火墙穿越的综合解决方案(以下简称“STR NAT 穿越方案”)。

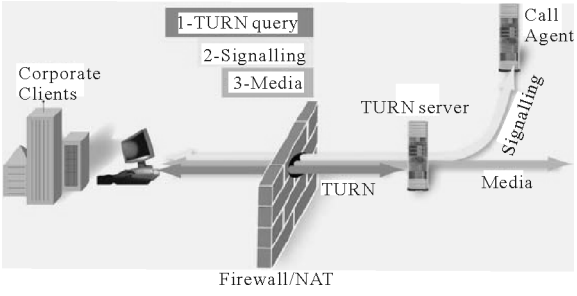

图 2　TURN 穿透 NAT 和防火墙示意图

STR NAT 穿越方案将 STUN 和 TURN 两种 NAT 和防火墙传输层穿越解决方案相结合，并在客户端和服务器端进行编程处理，使它们互相补充，相得益彰，形成一个整体。其主要思想是：如果传输协议是 TCP 协议，直接用 TURN 的方法穿越 NAT 及防火墙；如果传输协议是 UDP 协议，则首先检测 NAT 和防火墙类型，若为对称型 NAT 则用 TURN 的方法穿越，否则用 STUN 方法穿越。该方案不仅可以充分发挥两种穿越技术的优点，还避免了各自的缺点，形成一个比较完整的 NAT 穿越解决方案。

STR NAT 穿越方案在程序设计和实现上采用 C/S 结构，分为服务器端和客户端两部分，其结构分别如图 3 和图 4 所示。

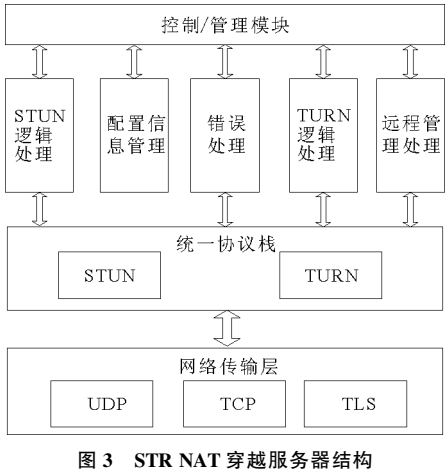

图 3　STR NAT 穿越服务器结构

STR NAT 穿越方案要达到 STUN 和 TURN 两种 NAT 和防火墙穿越技术相得益彰、对用户提供统一的用户应用模式的目的，需要解决好以下几方面的问题。

2.1　统一协议栈

STR NAT 穿越方案是 STUN 和 TURN 两种方法的结合，要使它们形成一个整体穿越方案，对用户表现出一致性，就不能简单地将两种方法进行叠加，需要提供两种穿越消息的一致处理。

STR NAT 穿越方案根据 STUN 和 TURN 的消息格式及属性相同的特点，设计了统一的协议栈，使得 STUN 和 TURN 对用户表现为一个整体。如图 5 所示，统一协议栈主要由接收/发送消息、消息判断、消息分析、消息分类、消息处理、应答消息生成、错误处理、消息池以及协议栈的接口几部分组成。其中最主要的是“接收/发送消息”和“消息池”两个部分。接收/发送消息是对网络传输层的封装，其主要作用一是为上层提供一个易用的网络传输层接口，二是隔离上层逻辑和网络传输层，屏蔽不同操作系统对网络传输要求的差异，增强系统的可移置性。“消息池”是数据交换的中心，它把 STUN 和 TURN 协议中对消息的串行处理变成并行处理，从而提高处理效率。

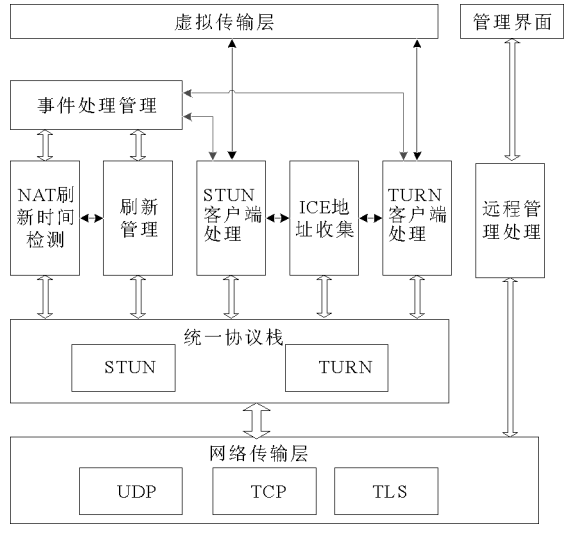

图 4　STR NAT 穿越客户端结构

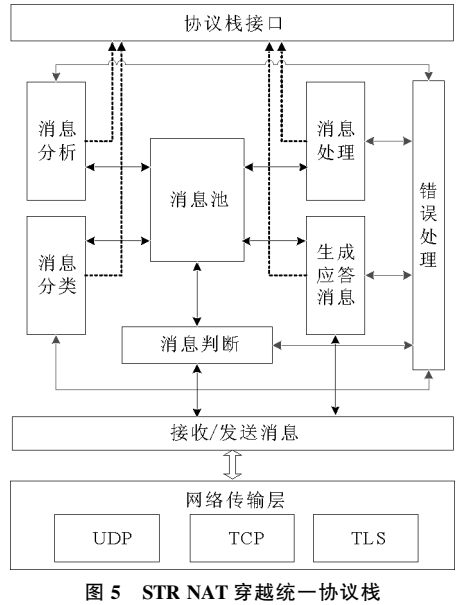

图 5　STR NAT 穿越统一协议栈

统一协议栈按照同一方式和流程处理 STUN 和 TURN 消息,为系统提供统一的消息处理机制,并且减少了冗余,降低了使用难度,为上层提供统一的逻辑处理奠定了坚实的基础。

2.2 虚拟传输层

为了屏蔽 NAT 及防火墙穿越的复杂性,提供与传统传输层编程相一致的编程接口,STR NAT 穿越方案对传统传输层和 NAT 穿越处理进行了封装,我们称为“虚拟传输层”。“虚拟传输层”屏蔽 NAT 及防火墙问题,提供与传统传输层一致的编程方法。对一般编程用户来说,不需要了解和处理 NAT 问题,可以按照传统传输层的编程习惯,不用考虑 NAT 和防火墙的存在。

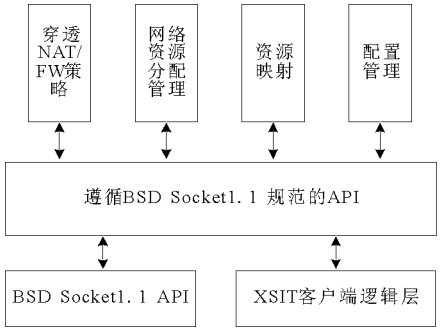

图 6 STR NAT 穿越虚拟传输层框架

如图 6 所示,虚拟传输层对外提供的是遵循 BSD Socket1.1 规范的 API。为了区别传统的传输层 API,虚拟传输层 API 的命名规则为在 BSD Socket1.1 API 函数名的前面加一个 X,例如对于函数 socket(int domin, int type, int protocol),我们把它封装成 Xsocket(int domin, int type, int protocol)。

虚拟传输层最上层为“穿透 NAT/FW 策略”、“网络资源分配管理”、“资源映射”和“配置管理”等。穿透 NAT/FW 策略是对采用穿透 NAT 和防火墙的策略进行设置和管理,这里的策略包括 4 种:①不使用 TURN 服务器,只使用 STUN 方式;②只使用 TURN 方式;③由系统决定;④不需要穿透 NAT 和防火墙。当为第 3 种时,系统先测试 NAT 和防火墙的类型,如果是对称型 NAT,使用 TURN 方式,否则使用 STUN 方式进行穿透。

网络资源分配管理是对网络资源进行管理。STR NAT 穿越方案在实现遵循 BSD Socket1.1 规范的 API 时,返回给用户的可能是虚拟资源。例如,用户调用 gethostbyname()函数返回本地 IP 地址时,根据“穿透 NAT/FW 策略”可能得到一个 NAT 地址或一个 TURN 绑定地址。因此,必须对这些 API 所使用的网络资源进行管理。

资源映射是管理真实资源和虚拟资源的映射。对于上面提到的情况,虚拟网络资源最终要体现在对真实网络资源的操作上,这就需要维持真实资源和虚拟资源的映射。

图 6 中间层是“遵循 BSD Socket1.1 规范的 API”的实现。这个模块是“虚拟传输层”的核心,STR NAT 穿越方案对大多数常用的 BSD Socket1.1 API 进行了封装,这使用户可以不用了解穿透 NAT 和防火墙的知识,直接根据 BSD Socket 编程习惯进行编程,就可透明穿透 NAT。

图 6 下层是“BSD Socket1.1 API”和“客户端逻辑层”,为程序开发人员提供具有 NAT 穿越能力编程接口。

2.3 连续端口申请

对于像 RTP 和 RTCP 这样的协议(组),要求使用两个或者更多的连续端口进行通信,而 TURN 的原有协议并没有考虑到这些要求。为此,STR NAT 穿越方案通过增加 TURN 的消息类型,实现了多个连续端口的绑定和申请。

2.4 代理绑定

为了使 TURN 服务器可以和 SIP Proxy 服务器配合使用,帮助 SIP 用户透明地穿透 NAT 和防火墙,STR NAT 穿越方案通过提供代理绑定接口,使得 TURN 服务器信任的第三方服务器(或客户端)可以帮助用户申请绑定。

2.5 统一刷新管理

对于具有 NAT 问题的用户,在进行通信时,NAT 的映射或绑定地址及端口在长时间不发消息时会出现超时中断,这需要在超时之前及时进行地址映射刷新。STR NAT 穿越方案首先用二分法找到 NAT 的超时时间,然后根据用户的使用情况进行定时的 NAT 地址刷新。

3 结语

本文在分析现有 NAT 和防火墙穿越技术的基础上,提出了“STUN+TURN”的 NAT 和防火墙整体穿越方案设计,并对该方案涉及的相关问题进行了深入的探讨,使得现有的 STUN 和 TURN 两种 NAT 和防火墙穿越技术相得益彰,浑然一体,为用户屏蔽 NAT 和防火墙穿越的复杂性提供了统一的用户应用模式。

参考文献:

[1] SRISURESH P, M HOLDREGE. IP network address translator (NAT) terminology and considerations[J]. RFC 2663, August 1999.

[2] ROSENBERG J, SCHULZRINNE H, CAMARILLO G, et al. SIP: session initiation protocol[J]. RFC 3261, June 2002.

[3] ROSENBERG J, MAHY R, MATTHEWS P, et al. Session traversal utilities for NAT (STUN)[J]. RFC 5389, October 2008.

[4] MAHY R, MATTHEWS P, ROSENBERG J. Traversal using relays around NAT (TURN): relay extensions to session traversal utilities for NAT (STUN)[J]. RFC 5766, April 2010.

(责任编辑:杜能钢)