文章编号:1008-0570(2006)05-3-0067-03

基于 MIDCOM 协议的 SIP 穿越 NAT/FW

SIP traverse NAT/FW based on MIDCOM protocol

(华中科技大学电子与信息工程系)旷志荣 王芙蓉
Kuang,Zhirong Wang,Furong

摘要:本文介绍利用 MIDCOM 协议,将程序智能从 NAT/FW 转移到第三方,从而解决在 SIP 网的大规模部署中,NAT/FW 性能成为整个 SIP 网的瓶颈这一难题。基于 MIDCOM 协议构架的 SIP 穿越 NAT/FW 解决方案在组网方面具有很强的扩展性,一旦 NAT/FW 设备支持 MIDCOM 协议,通过 MIDCOM 代理对 SIP 应用协议作相应的处理,便可一劳永逸的解决 SIP 业务的 NAT/FW 穿越问题。

关键词:中间盒通信;会话初始化协议;网络地址转换;防火墙
中图分类号:TP393.08 **文献标识码**:A

Abstract:In large scale SIP net, the performance of NAT/FW is the whole net's bottleneck. This paper introduces a way using MIDCOM protocol, transferring application intelligence to the third party (MIDCOM agent) to solve this problem. When construct SIP network, this way has strong extensibility. While NAT/FW devices support MIDCOM protocol, it can solve the problem entirely through MIDCON agent extending SIP.

Keywords: MIDCOM;SIP; NAT;firewall

技术创新

1 引言

基于 SIP 的 VoIP 应用越来越广,已经有很多企业在其内部部署了 SIP 网,在一些国家也已经有了 SIP 公网。由于网络地址资源缺乏和安全原因,大量企业和驻地网采用了私有网络通过 NAT (Network Address Translation,网络地址转换) / FW(Firewall,防火墙) 出口来

接入公共网络的解决方案[1,2]。SIP 协议[3]是基于 UDP/TCP 之上的应用层控制协议,SIP 包头中含有很多关于路由、接续 SIP 信令和建立呼叫连接的必不可少的地址信息,而且真正的媒体连接信息是放在 SDP 中动态配置传送的,这部分私网地址在穿越 NAT 时不能被转换,因而造成 SIP 信令寻址不成功或媒体通道不能建立。所以 SIP 穿越 NAT/FW 要求 NAT/FW 具有应用程序智能,现有的解决方法大都是把应用程序智能嵌入 NAT/FW。随着 SIP 网的大规模部署,NAT/FW 将要处理大量的 UDP/TCP 通信,大大增强了 NAT/FW 的复杂性,难于维护,成为 SIP 大规模部署的瓶颈。本文讨论通过利用 IETF 的 MIDCOM 协议实现 SIP 穿越 NAT/FW,使应用程序智能转移到第三方的方法来解决这个问题。

2 MIDCOM 协议介绍

MIDCOM(middlebox communication)协议[4]是一个与应用无关,中间盒专注于服务(如防火墙、NAT),而应用程序智能通过 MIDCOM 协议转移到可信赖的第三方(MIDCOM 代理)上的协议。

2.1 MIDCOM 代理

MIDCOM 代理是指执行应用层网关功能、逻辑上在中间盒外的实体。MIDCOM 代理同时认知应用程序和中间盒功能。这种能力让代理能够使应用程序数据包轻松穿越中间盒。有两类 MIDCOM 代理:线内(in-path) MIDCOM 代理、线外 (out of path) MIDCOM 代理。这里所说的线内或线外指的是代理是否位于应用的通信线路中的实体上。有单独的控制和数据会话的包会话应用程序,比如 H.323、SIP 和 RTSP,他们的会话会取不同的路径。这种情况下的线内 MIDCOM 代理是指位于控制会话通路上的代理。代理协助中间盒完成其服务。中间盒的某一功能或特定应用穿越中间盒可能要求不只一个 MIDCOM 代理的介入,每一个代理对应应用程序的一个子会话。

2.2 MIDCOM PDP

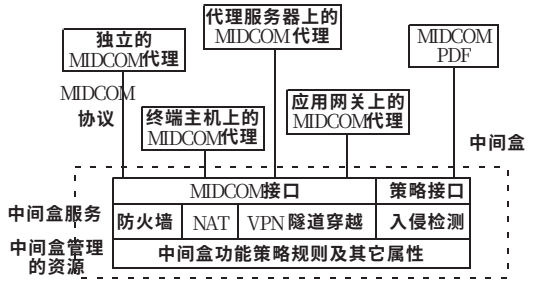

图 1 MIDCOM 代理、中间盒与 MIDCOM PDP 的关系

旷志荣:研究生
基金资助:湖北省青年杰出人才 编号:2005ABB006

MIDCOM PDP 是指物理上位于中间盒上或中间盒以外的结点上的逻辑实体,负责中间盒授权和有关策略规则服务。对于中间盒来说,MIDCOM PDP 扮演一个顾问的身份,批准或终止代理连接中间盒的授权。为了得到调用中间盒服务的授权,代理要向 MIDCOM PDP 注册。

MIDCOM 代理、中间盒与 MIDCOM PDP 之间的接口关系如图 1 所示。

2.3 MIDCOM 协议交互

MIDCOM 协议交互是通过事件 (transaction)[5]来描述的。协议中使用两类基本事件 请求事件和异步事件。一个请求事件由以下几部分组成:请求消息从代理到中间盒的传输,中间盒对请求信息的处理,应答消息从中间盒到代理的传输和可选的从中间盒到代理的通知信息传输组成。而不仅仅指请求消息的传输。请求事件可能引起中间盒状态转移。请求事件还可以细分为配置事件和监控事件。配置事件是包含要求中间盒状态改变的一种请求事件,如果接受了就会引起中间盒状态改变。监控事件是包含查询中间盒状态信息的一种请求事件,不会引起中间盒状态信息。异步事件不是由代理触发,没有任何代理参与中间盒会话也可能发生。异步事件潜在地包括从中间盒到参与开放会话的所有代理的通知信息传递。通知信息被发给需要知道此异步事件的各个代理。这个消息表明中间盒发生了状态转移。

协议交互涉及中间盒管理、策略规则管理和代理与中间盒之间的通信。中间盒状态涉及到中间盒的功能,得具体问题具体分析。策略规则管理由状态机来描述。用于策略规则管理的事件主要有:

保存策略规则(PRR- Policy Reserve Rule)

使能策略规则(PER Policy Enable Rule)

生存期变化策略规则 (RLC: Policy Rule Lifetime Change)

策略规则列表(PRL: Policy Rule List)

策略规则状态(PRS: Policy Rule Status)

异步策略规则事件 (ARE: Asynchronous Policy Rule Event)。其中 PRL、PRS、ARE 不会引起策略规则的状态变化。

MIDCOM 代理与中间盒之间的通信由会话来描述。用于控制会话的事件有:

会话建立(SE: Session Establishment)

会话结束(ST: Session Termination)

异步会话结束 (AST: Asynchronous Session Termination.)

3 应用 MIDCOM 协议的 SIP 穿越 NAT/FW

如图 2 所示,左边是一个典型的 SIP 呼叫流程,右边的就是使用了 MIDCOM 协议后穿越 NAT/FW 的流程。对于一个 SIP 电话呼叫,可以分为两部分:一部分是信令,也就是建立呼叫的协议消息;别一部分是实际的媒体流。图中虚线代表内部专有通信网与外网的分界线,也是 NAT/FW 所处的位置。我们作如下的假定:用户代理 A 和 SIP Proxy 在内部专有通信网,而用户代理 B 在外网上;图中直接穿越 NAT/FW 的线表示使用已有规则穿越 NAT/FW;在应用 MIDCOM 协议之后,NAT/FW 是中间盒的服务,我们使用线内 MIDCOM 代理并且 MIDCOM 代理位于 SIP Proxy 上;使用 SIP 注册服务器作为 MIDCOM PDP,由它来决定是否允许一个内外网之间的通信。

和没有使用 MIDCOM 协议相比较来看,这个流程多了三个 MIDCOM 通信过过程,也正是由于这三个通信过程的存在,使应用程序智能从中间盒转移到 MIDCOM 代理上,从而简化中间盒的结构和维护。

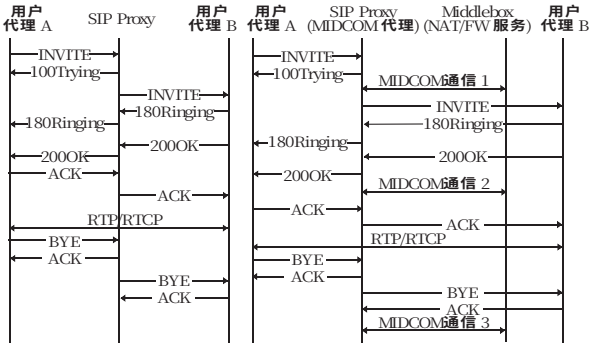

图 2

3.1 MIDCOM 通信过程 1

由于在 MIDCOM 通过过程中使用的是 MIDCOM 代理、中间盒和 MIDCOM PDP。所以在下面的描述中将使用这几个术语,其实他们对应 SIP 通信系统中的 SIP Proxy、NAP/FW 和注册服务器。通信过程 1 的流程如图 3:

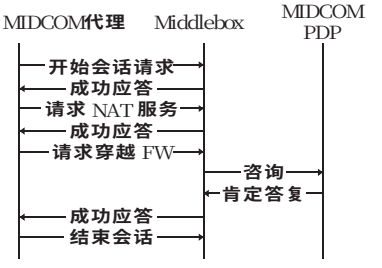

图 3

1MIDCOM 代理向中间盒发出一个建立会话的请求

2 在相互鉴权后,中间盒返回一个成功消息,MIDCOM 代理和中间盒之间的会话就建立起来了。

3MIDCOM 向中间盒请求 NAT 服务。

4 中间盒触发 PER 事件,把用户代理 A 的内网地址和 5060 绑定到中间盒的外网地址和某一端口。

5 返回成功消息到 MIDCOM 代理。

6MIDCOM 代理再请求穿越防火墙。

7 中间盒在接到请求后,咨询 MIDCOM PDP 是否允

许此穿越。

8MIDCOM PDP返回肯定答复

9中间盒触发PER事件,允许用户代理A到用户代理B的UDP通信穿越防火墙。同时中间盒触发另一PER事件,使到用户A的某一端口的RTP/RTCP通信穿越防火墙。(从INVITE的SDP提取参数)

10中间盒向MIDCOM代理发成功消息。

11MIDCOM代理发送中止会话的消息,完成会话。

从以上的过程可以看出,在第一次通信过程后,用户代理A和用户代理B之间的信令通信已经完成对NAT/FW的穿越。并且从用户代理B到用户代理A的RTP/RTCP通信也已经完成穿越。

3.2 MIDCOM通信过程2:

通信过程2的会话建立和过程1一样,只是建立的规则不同,建立的是允许从用户代理B到用户代理A的RTP/RTCP通信穿越防火墙的规则(从SIP的200OK消息中提取参数)。

3.3 MIDCOMC通信过程3

当用户代理A和B之间的通信结束之后,中间盒触发异步事件,取消通信过程1、2建立的所有规则并通知MIDCOM代理。

由上述可以看出,在穿越NAT/FW过程中,由于使用了MIDCOM协议,中间盒只在信令通信期间和MIDCOM代理进行了简单的通信来建立规则,而不需要复杂的程序智能;对于后面的媒体通信只要应用规则就可以了,这样大大减轻了中间盒的负担。而对于智能终端,还可以将MIDCOM代理放到终端上,这样没有SIP Proxy的参与就可以完成穿越。

4 结束语

MIDCOM协议通过将应用程序智能由中间盒上转移到相对独立的第三方MIDCOM代理上,从而简化中间盒的设计和维护。但是由于引入了第三方,增加了额外的通信,当系统很少时,比如仅仅一两百个终端这样的系统,这种方法并不能带来什么好处。在大规模的SIP部署中就有用武之地了。同时,基于MIDCOM协议构架的SIP穿越NAT/FW解决方案在组网方面具有很强的扩展性,一旦NAT/FW设备支持MIDCOM协议,通过MIDCOM代理逻辑功能实体对SIP应用协议作相应的处理,便可一劳永逸的解决SIP业务的NAT/FW穿越问题[6]。同时,由于软交换自身对用户呼叫协议的解析与处理同样能动态下发呼叫的QoS和安全信息,中间盒(NAT/FW)设备可根据这些信息采取必要的保证措施,因此这种方案又具有很好的安全性和实用性.由于软交换设备上已经实现了对SIP协议的解析与处理,因此只需在软交换和NAT/FW设备上增加MIDCOM协议即可,而且以后新的应用业务识别将支持软交换所支持的一切功能。这种方案是一种比较有前途的解决方案,但现有的NAT/FW设备需升级以支持MIDCOM协议。

参考文献:

[1]IETF RFC1631,IP Network Address Translator(NAT).
[2]IETF RFC2663,IP Network Address Translator(NAT) Terminology and Considerations.
[3]IETF RFC3261,SIP: Session Initiation Protocol
[4]IEFT RFC3303,Middlebox communication architecture and framework
[5]IEFT RFC3989,Middlebox Communications (MIDCOM) Protocol Semantics
[6]叶德谦,张树国,孟庆吉.状态服务在SIP协议中的应用研究[J].微计算机信息,2005,12-3:136-138

作者简介:旷志荣(1974.07-),男,汉族,研究生.专业:信息处理,主要方向:下一代通信网络和智能业务;王芙蓉(1966.07-),女,汉族,博士,教授。主要研究方向:移到通信网,下一代通信网络和智能业务、通信软件、多媒体信息处理。当前研究方向:移到通信网、智能业务

Author brief introduction:KUANG zhi-rong (07/1974-), male, Graduate Student.Major:information process.Research: Next Generation Telecommunication Networks and Intelligence Service.E-mail:hawkuang@sina.com

通讯地址:

(430074 湖北武汉华中科技大学西七舍240室)

(投稿日期:2005.9.2) (修稿日期:2005.10.15)

(接303页)[4]Tadeusz Pankowski. An XML Query Language Based on SQL and Path Table[M]. XML-SQL. A.B. Chaudhri et al.(Eds.): EDBT 2002 Workshops, LNCS 2490,2002,pp:184-209.
[5]陈旭春,赵明生.分布式多搜索引擎系统的研究与实现[J]微计算机信息,2005,10:37-39
[6]Qinghua Zou,Shaorong Liu,Wesley W.Chu. Ctree: A Compact Tree for Indexing XML Data.WIDM' 04, November 12-13, 2004, Washington, DC, USA. pp:39-46.
[7] James Cheng,Wilfred Ng. XQzip: Querying Compressed XML Using Structural Indexing. E. Bertino et al. (Eds.): EDBT 2004, LNCS 2992, pp:219－236.

作者简介:陈丽冰,(1969-),女,广东汕尾市人,工程师,本科,主要研究方向:数据库

(510275 广东省广州市 中山大学计算机系)陈丽冰 吉永杰 邓楚燕

(510260 广东广州 广东经济管理学院) 陈丽冰

(Computer Science department of Sun Yat-sen University, Guangzhou,510275;China) Chen,Libing Ji,Yongjie Deng, Chuyan

(Guangdong Institute of Business Administration,Guangzhou, 510260,China) Chen,Libing

通讯地址:

(510275 广东省广州市海珠区滨江东路嘉裕街6号2606) 陈丽冰

(投稿日期:2005.9.6) (修稿日期:2005.10.16)

技术创新