基于 MIDCOM 协议的 VoIP 防火墙实现

田 辉 王伟明 何 茜

(北京化工大学信息学院 北京 100029) (北京 IDES 科技有限公司)

摘要：本文介绍了一种新的 VoIP 防火墙的实现方案，该方案是由 MIDCOM 协议设计的。使用该协议，能够解决以前特定的 VoIP 防火墙存在的许多技术难题，因而目前在 VoIP 服务网的架构中得到广泛的采用。

关键词：MIDCOM middlebox VoIP 防火墙

1 引言

经过几年的发展，基于 IP 的语音服务在世界范围得到了全面的展开应用。该技术由最初的 PC 初级产品和限定在 IP 网络范围内发展到具有多业务、高可靠性、较好服务的含语音、传真、数据传输的电信业务。为了提供稳定、安全的 IP 电话体系，就需要为 VoIP 服务网设计一种安全、高效、可靠的防火墙。以前的 VoIP 防火墙大多数采用根据某个特定的 VoIP 实现协议设计特定的防火墙。这种防火墙在实际的使用过程中，特别是在需要提供越来越丰富服务的情况下，其运行的复杂性、不稳定性突出地表现出来。对此，IETF 提出了一种将 VoIP 服务和防火墙功能相互独立的 middlebox 结构，在 VoIP 服务和防火墙功能间采用 MIDCOM 协议。本文讨论了用 MIDCOM 协议在 middlebox 上实现 VoIP 防火墙的设计方案。

2 VoIP 协议防火墙

实现 VoIP 服务有三种主要的媒体传输协议，它们为 H.323 协议、会话初始化协议 SIP、S/MGCP 协议。我国目前采用 H.323 协议。为了加强电信网络安全，通常采用的防火墙为基于包过滤的技术和代理服务的应用级网关或混合网关构成。然而以往的 VoIP 防火墙存在如下的问题：

(1) H.323 协议中如何实现地址转换，即如何进行私人 IP 和公共 IP 间的转换问题。

(2) 由于在 H.323 使用 UDP 进行媒体流的传输控制，UDP、RPC 为不安全协议，因而大多数防火墙不允许 UDP 包通过。同时，H.323 在通话建立过程中要动态地建立 TCP 的端口，对防火墙来说，打开所有的 TCP 端口是不可能的，因此需要制定针对 H.323 的防火墙协议。

(3) 连接过程中需要 H.225 和 H.245 协议的 IP 地址不存在包头中，NAT 服务无法进行转换。

(4) IPSEC 不通过 NAT（IPSEC 为 IPv4 的可选段，而对 IPv6 不需要进行 NAT），防火

本文于 2002－09－05 收到，2002－11－29 收到修改稿。

墙不打开 IPSEC，从而无法知道需要打开的端口。

(5) 在 TCP 信令连接完成之后，NAT 将关闭该端口，通话无法正常进行下去。

(6) NAT 不支持广播。

(7) 对于实现 H.323、SIP 协议的防火墙，如果通过套接字 SOCKS 连接方式，需要为这些特定的应用协议设计不同的代理程序。

(8) 应用防火墙会造成时延，造成语音信号质量的损失，而简单电路级防火墙，虽然具有快速的优点，但不能在协议上执行严格的检查。

为了克服防火墙以上的缺点，VoIP 架构者往往需要修改协议或采用特殊手段，而新的 MIDCOM 协议则克服了这些缺点。

3 MIDCOM 通信结构和框架

MIDCOM 是一种 VoIP 安全服务协议，该协议讨论了媒体传输的应用策略。例如包过滤、区分质量服务、管道、入侵检测、安全。它将功能服务从 middlebox 独立到 MIDCOM 服务代理中，使 middlebox 的设计与具体应用无关，专门提供像防火墙和 NAT 等服务。具体来说这些服务就是网络中间传输中的自动推测行为，包括：包过滤策略、网络地址转换、入侵探测、负载平衡、管道策略、IPSEC 等。

MIDCOM 协议允许 MIDCOM 代理访问 middlebox 的资源，允许 middlebox 取消 MIDCOM 代理的程序应用。middlebox 在MIDCOM 代理的帮助下实现具体应用功能，而不需把该功能放在 middlebox 中。通过该协议，middlebox 能够无缝地使用第三方提供的程序。

在 MIDCOM 协议中，middlebox 各个服务间共享资源，这些资源被 middlebox 的各个功能共同管理。共享资源通过 MIDCOM 协议协助 middlebox 实现特定的功能。见图 1 所示。

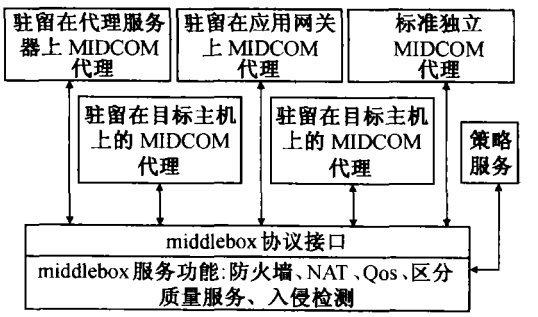

图 1 middlebox 和 MIDCOM 代理的关系

4 MIDCOM 代理的分类

(1) In－Path 代理 (IP)

IP 提供本地的服务，它们的功能与 MIDCOM 是独立的，IP 代理出现在数据流的通路上。例如 H.323，SIP 和 RTSP，它们都有单独的数据和控制任务 (见图 2)。程序代理和网关是典型的 IP 代理。IP 代理处理自己的功能外，还可以加上附加的本地服务，例如限制已知的病毒，非法的授权用户。对于像语音这样的实时流传送，可以只对控制信号进行处理。

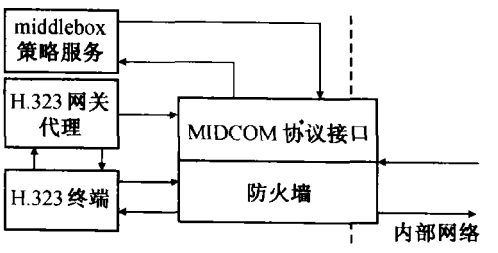

图 2 In－Path 代理通信框架

SIP 代理和 H.323 网关可以作为 MIDCOM 代理的功能，协助 middlebox 实现防火墙和 NAT 的功能。使用 IP 代理可以把服务功能独立出来，通过 MIDCOM 协议实现它们之间的控制。

(2) Out－of－path 代理 (OOP)

OOP 不属于传输路径上的实体，它不在传输路径之中，但也具有实现应用的传输功能。它的优点为 OOP 代理实现与应用的独立性，它不同于 IP 代理，与应用的拓扑没有联系，可以把多个具体的功能划归在相同的节点之中。采用 OOP 代理，middlebox 需要对数据流进行重定向，因此 OOP 代理要对数据进行监测并对它们的流向进行控制（见图 3)。

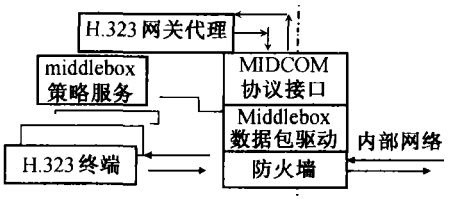

图 3　Out－of－Path 代理通信结构

OOP 代理适用于那些需要重定向的服务，例如对于 SIP 服务，通常简单的把它们发送到代理服务，但是在代理同时管理 NAT 功能时，代理需要更改 SIP 消息，定向到控制通路上。

如果支持 OOP 代理，middlebox 需要附加的“数据流分路”功能，它的执行如下：

① middlebox 接收到数据流时，middlebox 将它转发到对应的 middlebox 服务代理。如果该数据流已被规定为到支路，middlebox 通过 RPC 调用把数据流分到支路上特殊的负载实体进行处理。

② 负载实体接收到数据流，进行转换，有选择地进行修改后，可采用两种方式：从原路将数据包返回给 middlebox；或者 OOP 代理具有路由能力，将数据流直接发到目标实体。

③ 在 middlebox 接收到数据包后，简单地转发到恰当的目标。

5　协议安全策略

安全策略由策略服务来实现和控制。具体细分为主机身份证明、独立消息证明、完全性验证、确信性身份验证。在实现时，由 MIDCOM 代理在访问 middlebox 资源前，进行登记，结束时解除登记。

6　基于 MIDCOM 协议的 VoIP 网关代理的实现

H.323 的拓扑基本网络单元由终端、GK、MCU、GW 共同构成。其呼叫过程分为 5 个阶段① 呼叫初始化(阶段 A)；② 端点间的初始通信和端点容量交换(阶段 B)；③ 建立端点之间的音频/视频通信(阶段 C)；④ 呼叫服务请求和协商(阶段 D)；⑤ 呼叫终止(阶段 E)。

采用基于 IP 代理的 middlebox 结构的通信实现过程，为了清晰的表达主要的连接流程，这里略去了一些实现过程中次要状态，但在实际的设计中也是需要考虑的。

阶段 A，位于防火墙外的呼叫方 A 向防火墙内一个主机 B 发起呼叫，假设 A 已经知道 B 的地址。第一个交换为在呼叫双方 TSAP 间打开 TCP 连接。TSAP 是 H.323 传输层服务接入点，即 TCP 端口 1720。被叫方返回应答消息 TCP－ACK，表示连接已经建立，呼叫信令就可以开始了。在新的 TCP 连接上发送的第一条消息是 H.225.0 的建立连接消息（Set-up)。如果在该网络不存在终端，呼叫端的 Setup 计时器会超时，呼叫尝试被中断。如果该终端忙于另一呼叫，它将返回一条 ReleaseComplete（释放完成）消息，并说明拒绝呼叫理由。如果该终端处于空闲状态，信令过程以一个或多个请求登记状态消息（RAS）交换开始。该阶段如果该终端还没有向一个网守（GK）注册，进行 RAS 注册。GK 可能拒绝接受登记请求消息，发出登记拒绝消息（RRJ)。在这种情况下，该终端必须找另外一个 GK 注

册。假定 GK 接受注册，接收终端会发送一条 RAS，接收请求到 GK。请求进入网络，为呼叫分配带宽和建立信令模型，建立直接或通过 GK 的路由。不可靠数据传输协议 UDP 端口 1719 是 RAS 传输地址。如果 GK 并不允许该请求，终端会用 H.225.0 消息 ReleaseComplete 释放该呼叫。如果 GK 批准了该请求，被叫端发送 H.225.0 振铃消息（Alerting），指示呼叫端正在振铃。最后，如果被叫方接受该呼叫将发送连续消息，该消息携带用于初始化 H.245 的介质通道的动态端口号的重要消息。

阶段 B 是终端之间的初始通信和容量交换。这时，再次需要在呼叫方和协议 H.225.0 连接消息中提供的被叫方的 TCP 传输地址之间建立新的 TCP 连接。在两个端点之间需要建立主/从关系。主机用来解决所出现的任何和通信所需资源有关的冲突，或者其他次要的类型冲突。在呼叫期间，具有最高端点类型的端点确定为主机。一旦容量交换完成，主从关系确定后，阶段 B 完成。

阶段 C 为任何一方发送 H.245 打开逻辑信道消息，H.245 的逻辑信道为半双工的双向通信，它必须在每个方向打开一条信道。利用事先交换所得到的端点容量集的性质，同时建立一个或多个逻辑信道。

阶段 D 中，接受端点和 GK 做出带宽请求 RAS 交换。如果 GK 允许请求，那么返回一条带宽确认消息，不过造成带宽差别的逻辑信道需要关闭，再用新的多路复用参数打开。如果在阶段 C 不存在带宽差别，则不需要激活阶段 D。在打开逻辑信道消息交换以后，介质会流入这些消息选定的端口。阶段 D 呼叫服务还包括状态更新、特定的会议从 MC 点对点会议扩散到点到多点、附加服务、多点级联和第三方重新路由。

阶段 E 实现呼叫的终止。任何一方发送 H.245 关闭逻辑信道命令，关闭视频、音频和数据通道。然后发送终止会话连接命令。此后，端点不再发送任何 H.245 信令消息。接受方也会发送一条关闭逻辑信道命令以关闭另外一方逻辑信道，一旦各自的关闭逻辑信道应答消息被交换，正在断开的端点发送一条 H.225.0 的释放完成命令，呼叫终止。

7 结束语

在 VoIP 试验网关开发环境中，我们采用了基于 MIDCOM 协议的设计方法，H.323 协议以 OpenH.323 的源码为参考进行设计和实验。通过采用 MIDCOM 协议来解决 VoIP 防火墙实现的问题，实现系统灵活的框架配置，解决以往采用独立防火墙占用主机资源大，语音服务不稳定等问题，为丰富的 VoIP 特性功能提供了一种很好的解决方案和可行性。

参 考 文 献

1 Bill Douskalis, 潇湘工作室译. IP 电话技术——稳定的 VOIP 服务集成. 北京：机械工业出版社, 2000.

2 Srisuresh Kuthan, Molitor Rayhan. Draft - ietf - midcom - framework - 01. INTERNET DRAFT: Aravox Technologies, 2001.

3 Huitema. Draft - ietf - midcom - scenarios - 01. INTERNET: DRAFT Microsoft, 2001.

4 Swale Mart. Sijben. Draft - ietf - midcom - requirements - 00. INTERNET DRAFT: Lucent Technologies, 2001.