(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2012 年 2 月 23 日 (23.02.2012)

PCT

(10) 国际公布号
WO 2012/022145 A1

(51) 国际专利分类号:
H04L 12/46 (2006.01)

(21) 国际申请号: PCT/CN2011/071659

(22) 国际申请日: 2011 年 3 月 10 日 (10.03.2011)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201010264191.4 2010 年 8 月 20 日 (20.08.2010) CN

(71) 申请人 (对除美国外的所有指定国): **成都市华为赛门铁克科技有限公司 (CHENGDU HUAWEI SYMANTEC TECHNOLOGIES CO., LTD.)** [CN/CN]; 中国四川省成都高新西区清水河片区电子科大高新科技园天辰路 88 号, Sichuan 611731 (CN)。

(72) 发明人; 及

(75) 发明人/申请人 (仅对美国): **陈爱平 (CHEN, Aiping)** [CN/CN]; 中国四川省成都市高新西区清水河片区电子科大高新科技园天辰路 88 号, Sichuan 611731 (CN)。 **聂成蛟 (NIE, Chengjiao)** [CN/CN]; 中国四川省成都市高新西区清水河片区电子科大高新科技园天辰路 88 号, Sichuan 611731 (CN)。 **张战兵 (ZHANG, Zhanbing)** [CN/CN]; 中国四川省成都市高新西区清水河片区电子科大高新科技园天辰路 88 号, Sichuan 611731 (CN)。

(81) 指定国 (除另有指明，要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) 指定国 (除另有指明，要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)。

本国际公布:

— 包括国际检索报告(条约第 21 条(3))。

[见续页]

(54) **Title**: METHOD, EQUIPMENT AND NETWORK SYSTEM FOR TERMINAL COMMUNICATING WITH IP MULTIMEDIA SUBSYSTEM(IMS) CORE NETWORK SERVER BY TRAVERSING PRIVATE NETWORK

(54) **发明名称** : 终端穿越私网与 IMS 核心网中服务器通信的方法、装置及网络系统

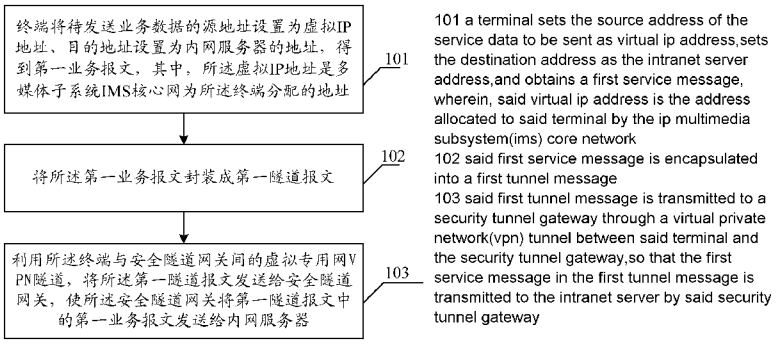

图 1A / **Fig. 1A**

(57) **Abstract**: A method, equipment and network system for a terminal communicating with an IP Multimedia Subsystem(IMS) core network server by traversing private network are provided by the embodiments of the present invention, wherein, the method for the terminal communicating with the IMS core network server by traversing private network includes: the terminal sets the source address of the service data to be sent as virtual IP address,sets the destination address as the intranet server address,and obtains a first service message, wherein, the virtual IP address is the address allocated to the terminal by the IMS core network; the first service message is encapsulated to a first tunnel message, and the first tunnel message is transmitted to a security tunnel gateway through a Virtual Private Network(VPN) tunnel between the terminal and the security tunnel gateway, so that the first service message in the first tunnel message is transmitted to the intranet server by the security tunnel gateway. By using the technical solution of the embodiments of the present invention, the terminal can communicate with the server in the IMS core network by traversing private network, with no need of altering the enterprise network.

[见续页]

WO 2012/022145 A1

(57) **摘要**:

本发明实施例提供一种终端穿越私网与 IMS 核心网中服务器通信的方法、装置及网络系统，其中，终端穿越私网与 IMS 核心网中服务器通信的方法包括：终端将待发送业务数据的源地址设置为虚拟 IP 地址、目的地址设置为内网服务器的地址，得到第一业务报文，其中，虚拟 IP 地址是多媒体子系统 IMS 核心网为所述终端分配的地址；将第一业务报文封装成第一隧道报文，利用所述终端与安全隧道网关间的虚拟专用网 VPN 隧道，将所述第一隧道报文发送给安全隧道网关，使所述安全隧道网关将第一隧道报文中的第一业务报文发送给内网服务器。使用本发明实施例提供的技术方案，不需要改动企业网络，终端就可以穿越私网，与 IMS 核心网中的服务器进行通信。

终端穿越私网与IMS核心网中服务器通信的方法、装置及网络系统

本申请要求于 2010 年 8 月 20 日提交中国专利局、申请号为201010264191.4、发明名称为“终端穿越私网与 IMS 核心网中服务器通信的方法、装置及网络系统”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

本发明涉及通信技术领域，特别涉及一种终端穿越私网与 IMS 核心网中服务器通信的方法、装置及网络系统。

背景技术

互联网协议多媒体子系统（Internet Protocol Media Subsystem， IMS）是一个基于IP技术的、与接入无关的网络架构，它是能被移动网络与固定网络共用的融合核心网，即能够为使用2.5G、3G、WLAN和固定宽带等不同接入手段的用户提供融合的业务，被业界认为是下一代网络的基础。

终端要接入IMS核心网，需要穿越私网（比如终端所接入的企业网络），具体的，由于企业网络内部使用私网IP地址，企业网络边缘部署NAT设备，终端需要穿越NAT设备接入IMS核心网的服务器，或者，如果企业网络边缘部署应用层代理服务器，则终端需要穿越应用层代理服务器接入IMS核心网的服务器。

现有技术提供一种穿越私网的方法，具体的，在企业网络和IMS网络中分别部署IPSec VPN（互联网协议安全虚拟专用，Internet Protocol Security VPN）网关，以便通过所部属的IPSec VPN网关在企业网络和IMS网络间建立IPSec VPN隧道，并将企业网络中的终端的路由聚合到企业网络中的IPSec VPN网关，由其执行业务数据的封装/解封装等操作。具体的，当终端向IMS核心网

发送业务数据时，修改终端所发送的业务数据的路由，将该业务数据先路由到企业网络中的IPSec VPN网关，IPSec VPN网关对业务数据进行封装，然后通过IPSec VPN隧道传送到IMS核心网中的IPSec VPN网关，核心网中的IPSec VPN网关对业务数据进行解封装后发送给IMS核心网中的服务器。

现有技术需要在企业侧网络中部署IPSec VPN网关，并且需要修改终端的数据路由，对企业网络的改动很大。

发明内容

本发明实施例提供一种终端穿越私网与 IMS 核心网中服务器通信的方法、装置及网络系统，不需要改动企业网络，终端就可以穿越私网，与公网（即 IMS 核心网）中服务器进行通信。

有鉴于此，本发明实施例提供:

一种终端穿越私网与 IMS 核心网中服务器通信的方法，包括:

终端将待发送业务数据的源地址设置为虚拟 IP 地址、目的地址设置为内网服务器的地址，得到第一业务报文，其中，所述虚拟 IP 地址是多媒体子系统 IMS 核心网为所述终端分配的地址;

将所述第一业务报文封装成第一隧道报文，其中所述第一隧道报文的源 IP 地址为终端的 IP 地址、目的 IP 地址为安全隧道网关的 IP 地址;

利用所述终端与安全隧道网关间的虚拟专用网 VPN 隧道，将所述第一隧道报文发送给安全隧道网关，使所述安全隧道网关将第一隧道报文中的第一业务报文发送给内网服务器。

一种终端穿越私网与 IMS 核心网中服务器通信的方法，包括:

安全隧道网关通过安全隧道网关与终端间的隧道接收第一隧道报文; 其中，所述第一隧道报文的源 IP 地址为终端的 IP 地址、目的 IP 地址为安全隧道网关的 IP 地址;

对所述第一隧道报文进行解封装，得到第一业务报文，所述第一业务报文的源地址为虚拟 IP 地址、目的地址为内网服务器地址; 将所述第一业务报

文向内网服务器发送。

一种终端，包括：通信能力组件，所述通信能力组件包括：

第一数据汇聚模块，用于将待发送业务数据的源地址设置为虚拟 IP 地址、目的地址设置为内网服务器的地址，得到第一业务报文；其中，所述虚拟 IP 地址是多媒体子系统 IMS 核心网为所述终端分配的地址；

第一隧道传输模块，用于将所述第一业务报文封装成第一隧道报文，其中所述第一隧道报文的源 IP 地址为终端的 IP 地址、目的 IP 地址为安全隧道网关的 IP 地址；利用所述终端与安全隧道网关间的虚拟专用网 VPN 隧道，将所述第一隧道报文发送给安全隧道网关，使所述安全隧道网关将第一隧道报文中的第一业务报文发送给内网服务器。

一种安全隧道网关，包括：

第一接收模块，用于通过安全隧道网关与终端间的隧道接收第一隧道报文；其中，所述第一隧道报文的源 IP 地址为终端的 IP 地址、目的 IP 地址为安全隧道网关的 IP 地址；解封装模块，用于对所述第一隧道报文进行解封装；

第一发送模块，用于将解封装模块解封装后得到的第一业务报文向内网服务器发送，其中，所述第一业务报文的源地址为虚拟 IP 地址、目的地址为内网服务器地址。

一种网络系统，包括：安全隧道网关和内网服务器，安全隧道网关，用于通过安全隧道网关与终端间的隧道接收第一隧道报文；其中，所述第一隧道报文的源 IP 地址为终端的 IP 地址、目的 IP 地址为安全隧道网关的 IP 地址；对所述第一隧道报文进行解封装，得到第一业务报文，所述第一业务报文的源地址为虚拟 IP 地址、目的地址为内网服务器地址；将所述第一业务报文向内网服务器发送；接收内网服务器发送的第二业务报文，所述第二业务报文的源地址为内网服务器的地址、目的地址为虚拟 IP 地址；将所述第二业务报文封装成第二隧道报文，其中，第二隧道报文的源 IP 地址为安全隧道网关的 IP 地址、目的 IP 地址为终端的 IP 地址；通过安全隧道网关与终端间的隧道向所述终端发送第二隧道报文；

内网服务器，用于接收安全隧道网关发送的第一业务报文，向安全隧道网关发送第二业务报文。

本发明实施例中终端将 IMS 核心网分配的虚拟 IP 地址作为终端与内网服务器的通信地址，将待发送业务数据的源地址设置为虚拟 IP 地址、目的地址设置为内网服务器的地址，并封装成隧道报文后通过终端与安全隧道网关间的隧道传输到安全隧道网关，使安全隧道网关能够将源地址为虚拟 IP 地址、目的地址为内网服务器地址的业务报文发送给内网服务器，这样，就能够实现通过安全隧道网关传输内网服务器与终端间的业务数据，不需要改动终端所在的企业网络，就可以使终端穿越私网，与公网中的服务器进行通信。

本发明实施例中的安全隧道网关作为中间设备，将来自终端的隧道报文解封装后发送给内网服务器，以便终端与 IMS 核心网中的服务器间传输业务数据，这样不需要改动终端所在的企业网络，就可以使终端穿越私网，与公网中的服务器进行通信了。

附图说明

图1A是本发明实施例提供的一种终端穿越私网与IMS核心网中服务器通信的方法流程图;

图1B为本发明实施例提供的又一种终端穿越私网与IMS核心网中服务器通信的方法流程图;

图2A是本发明实施例提供的另一种终端穿越私网与IMS核心网中服务器通信的方法流程图;

图2B是本发明实施例提供的再一种终端穿越私网与IMS核心网中服务器通信的方法流程图;

图3为本发明实施例提供的VPN隧道建立流程图;

图4为本发明实施例提供的终端身份认证流程图;

图5为本发明实施例提供的一种IMS业务数据安全穿越流程图;

图6为本发明实施例提供的另一种IMS业务数据安全穿越流程图;

图7为本发明实施例提供的终端结构图;

图8为本发明实施例提供的安全隧道网关结构图;

图9为本发明实施例提供的网络系统结构图。

具体实施方式

参阅图 1A，本发明实施例提供一种终端穿越私网与 IMS 核心网中服务器通信的方法，该方法从终端侧描述本发明实施例提供的技术方案，该方法包括:

101、终端将待发送业务数据的源地址设置为虚拟 IP 地址、目的地址设置为内网服务器的地址，得到第一业务报文，其中，所述虚拟 IP 地址是多媒体子系统 IMS 核心网为所述终端分配的地址。

其中，终端具体获得第一业务报文的过程包括：将待发送业务数据的源地址设置为虚拟 IP 地址、目的地址设置为内网服务器的地址，将待发送业务数据的源端口设置为终端的业务端口，将待发送数据的目的端口设置为内网服务器的业务端口。

本发明实施例及后续各实施例可适用于如下环境，终端位于私网中，比如企业网络中，终端想与 IMS 核心网中的服务器进行通信，则终端需要穿越私网与 IMS 核心网中的内网服务器进行通信。

其中，所述虚拟 IP 地址是由安全隧道网关（Security Tunnel Gateway STG）分配的，该安全隧道网关位于 IMS 核心网的边缘。所述安全隧道网关（Security Tunnel Gateway STG）可以是后续各实施例中描述的 VPN 网关。终端与安全隧道网关间的隧道可以是用户数据报协议（User Datagram Protocol，UDP）VPN 隧道，安全套接层（Security Socket Layer，SSL）VPN 隧道或者超文本传输协议（Hyper Text Transfer Protocol ，HTTP）VPN 隧道。

其中，所述虚拟 IP 地址也可以是由 IMS 核心网的动态主机设置协议(Dynamic Host Configuration Protocol, DHCP)服务器分配的。

所述 UDP VPN 隧道包含数据报传输层安全协议（Datagram Transport

Layer Security, DTLS）VPN 隧道。

102、将所述第一业务报文封装成第一隧道报文，其中所述第一隧道报文的源 IP 地址为终端的 IP 地址、目的 IP 地址为安全隧道网关的 IP 地址。

其中，具体的封装第一隧道报文的过程包括：设置第一业务报文的源 IP 地址为终端的 IP 地址，这个 IP 地址为终端真实的 IP 地址，设置第一业务报文的目的 IP 地址为安全隧道网关的 IP 地址，设置第一业务报文的源端口为终端的隧道端口，设置第一业务报文的目的端口为安全隧道网关的隧道端口。

103、利用所述终端与安全隧道网关间的虚拟专用网 VPN 隧道，将所述第一隧道报文发送给安全隧道网关，使所述安全隧道网关将第一隧道报文中的第一业务报文发送给内网服务器。

图 1B 为本发明实施例提供的又一种终端穿越私网与 IMS 核心网中服务器通信的方法流程图，图 1B 所述实施例描述了当终端需要接收内网服务器的业务数据时，穿越私网接收 IMS 核心网中服务器发送的业务数据的方法，如图 1B 所示，该方法包括：

104、终端通过所述隧道接收第二隧道报文，其中，第二隧道报文的源 IP 地址为安全隧道网关的 IP 地址、目的 IP 地址为终端的 IP 地址；

105、对所述第二隧道报文进行解封装得到第二业务报文；其中，所述第二业务报文的源地址为内网服务器的地址、目的地址为虚拟 IP 地址；

106、获得所述第二业务报文中的业务数据。

实际应用中，图 1A 与图 1B 所示的实施例终端穿越私网与 IMS 核心网中服务器通信的方法可以结合使用。图 1A 所示的实施例描述了终端穿越私网向 IMS 核心网中的服务器发送业务数据的过程，图 1B 所示的实施例描述了终端穿越私网接收 IMS 核心网中的服务器发送的业务数据的过程。

当终端与安全隧道网关间的 VPN 隧道同时存在 UDP VPN 隧道和 SSL VPN 隧道时，则通过 UDP VPN 隧道传输业务数据，通过 SSL VPN 隧道传输业务控制信息，具体的，该方法还包括：终端利用所述 SSL VPN 隧道向所述安全隧道网关发送第一业务控制信息，比如，向安全网关发送请求分配虚拟

IP 地址的信息，或者，当终端需要释放 VPN 隧道时，可以通过 SSL VPN 隧道向安全隧道网关发送释放 VPN 隧道的指示信息；或者，所述终端利用所述 SSL VPN 隧道接收所述安全隧道网关发送的第二业务控制信息。比如，在安全隧道网关为终端分配虚拟 IP 地址后，终端通过 SSL VPN 隧道接收安全隧道网关分配的虚拟 IP 地址。

本发明实施例中终端将 IMS 核心网分配的虚拟 IP 地址作为终端与内网服务器的通信地址，将待发送业务数据的源地址设置为虚拟 IP 地址、目的地址设置为内网服务器的地址，并封装成隧道报文后通过终端与安全隧道网关间的隧道传输到安全隧道网关，使安全隧道网关能够将源地址为虚拟 IP 地址、目的地址为内网服务器地址的业务报文发送给内网服务器；当需要接收内网服务器的业务数据时，将接收的隧道报文进行解封装，得到源地址为内网服务器的地址、目的地址为虚拟 IP 地址的业务报文，这样，就能够实现通过安全隧道网关传输内网服务器与终端间的业务数据，不需要改动终端所在的企业网络，就可以使终端穿越私网，与公网中的服务器进行通信。

参阅图 2A，本发明实施例提供一种终端穿越私网与 IMS 核心网中服务器通信的方法，该方法从安全隧道网关侧描述本发明实施例提供的技术方案，描述包括：

201、安全隧道网关通过安全隧道网关与终端间的隧道接收第一隧道报文；其中，所述第一隧道报文的源 IP 地址为终端的 IP 地址、目的 IP 地址为安全隧道网关的 IP 地址。

其中，所述虚拟 IP 地址是由安全隧道网关分配的，安全隧道网关与终端间的隧道可以是用户数据报协议（User Datagram Protocol ，UDP）隧道， 安全套接层（Security Socket Layer，SSL）隧道或者超文本传输协议（Hyper Text Transfer Protocol ，HTTP）隧道。

202、安全隧道网关对所述第一隧道报文进行解封装，得到第一业务报文，所述第一业务报文的源地址为虚拟 IP 地址、目的地址为内网服务器地址。

203、安全隧道网关将所述第一业务报文向内网服务器发送。

图 2B 是本发明实施例提供的再一种终端穿越私网与 IMS 核心网中服务器通信的方法流程图，图 2B 所述的实施例从安全隧道网关侧描述了将内网服务器发送的业务报文通过 VPN 隧道传输给终端的方法，如图 2B 所示，该方法包括:

204、安全隧道网关接收内网服务器发送的第二业务报文，所述第二业务报文的源地址为内网服务器的地址、目的地址为虚拟 IP 地址;

205、将所述第二业务报文封装成第二隧道报文，其中，第二隧道报文的源 IP 地址为安全隧道网关的 IP 地址、目的 IP 地址为终端的 IP 地址;

206、通过安全隧道网关与终端间的隧道向所述终端发送第二隧道报文。

图 2A 与图 2B 所示的实施例均从安全隧道网关侧描述了终端穿越私网与 IMS 核心网中服务器通信的方法，图 2A 所示的实施例从安全隧道网关侧描述了将终端通过 VPN 隧道发送的业务报文传输给 IMS 核心网中的服务器的过程，图 2B 所示的实施例从安全隧道网关侧描述了将 IMS 核心网中的服务器发送的业务报文通过 VPN 隧道传输给终端的过程，实际应用中，图 2A 与图 2B 所示的实施例所述方法可以结合使用。

当终端与安全隧道网关间的 VPN 隧道同时存在 UDP VPN 隧道和 SSL VPN 隧道时，则通过 UDP VPN 隧道传输业务数据，通过 SSL VPN 隧道传输业务控制信息，具体的，该方法还包括：安全隧道网关利用所述 SSL VPN 隧道向所述终端发送第二业务控制信息；比如，在安全隧道网关为终端分配虚拟 IP 地址后，安全隧道网关通过 SSL VPN 隧道向终端发送虚拟 IP 地址。或者，安全隧道网关利用所述 SSL VPN 隧道接收终端发送的第一业务控制信息，比如，当终端需要释放 VPN 隧道时，可以通过 SSL VPN 隧道向安全隧道网关发送释放 VPN 隧道的指示信息。

本发明实施例中的安全隧道网关作为中间设备，将来自终端的隧道报文解封装后发送给内网服务器，将来自内网服务器的业务报文封装成隧道报文后发送给终端，以便终端与 IMS 核心网中的服务器间传输业务数据，这样不需要改动终端所在的企业网络，就可以使终端穿越私网，与公网中的服务器

进行通信了。

如下对本发明实施例提供的技术方案进行详细介绍:

图 3 示出了本发明实施例提供的 VPN 隧道建立流程图，VPN 隧道建立过程具体包括:

301、终端判断是否配置了应用层代理服务器相关信息，如果是，则向应用层代理服务器发送建立代理连接请求消息，如果否，则执行 303。

具体的，终端的业务模块调用终端中通信能力组件中的隧道传输模块的接口，触发隧道传输模块判断是否配置了应用层代理服务器相关信息，并在判断结果为是时发送建立代理连接请求消息，在判断结果为否时直接向 VPN 安全隧道网关发送建立 VPN 隧道的请求。本发明各实施例中的通信能力组件包括三个模块，隧道传输模块、加解密模块和数据汇聚模块。该步骤具体是由隧道传输模块执行的。

其中，应用层代理服务器相关信息包括应用层代理服务器类型、IP 地址和端口；应用层代理服务器类型包括 HTTP 代理服务器、HTTPS 代理服务器、SOCKS 代理服务器等。在该步骤之前，是由用户根据企业网络到 VPN 网关（即安全隧道网关）之间的网络情况决定是否需要经过应用层代理服务器，如果需要经过应用层代理服务器连接到 VPN 网关，则需要在终端上配置应用层代理服务器的类型、IP 地址、端口。

302、应用层代理服务器向终端返回建立代理连接响应消息。

该步骤具体可以是应用层代理服务器向终端中的隧道传输模块返回建立代理连接响应消息。

终端与不同类型的应用层代理服务器之间建立代理连接的过程不一样，并且需要进行交互的次数也可能会不同，但是建立代理连接时对 NAT 设备没有任何特殊要求，因此建立代理连接请求消息和响应消息可以穿越所有正常的 NAT 设备。

303、终端向 VPN 网关发送建立 VPN 隧道的请求消息。

具体的，终端中的隧道传输模块向 VPN 网关发送建立 VPN 隧道的请求

消息。

304、 VPN 网关向终端返回建立 VPN 隧道的响应消息。

该实施例中的 VPN 隧道可以包括 SSL VPN、HTTP VPN、UDP VPN 三种隧道类型。具体的，VPN 网关向终端中的隧道传输模块返回建立 VPN 隧道的响应消息。

当终端需要通过应用层代理服务器连接到 VPN 网关时，则步骤 303 需要通过应用层代理服务器向 VPN 网关发送建立 VPN 隧道的请求消息，相应的，在步骤 304 中 VPN 网关通过应用层代理服务器向终端发送建立 VPN 隧道的响应消息。

305、VPN 隧道建立成功后，终端利用 VPN 隧道向 VPN 网关发起请求配置信息的报文。

具体的，终端中的隧道传输模块向 VPN 网关发起请求配置信息的报文。

306、VPN 网关利用 VPN 隧道向终端返回配置信息。

其中，配置信息包括：内网服务器的 IP 地址/掩码、VPN 网关分配给终端的虚拟 IP 地址/掩码。内网服务器的 IP 地址可以是某些具体的 IP 地址，也可以是多个 IP 地址段，此时该内网服务器在多个网段内。

具体的，VPN 网关向终端中的隧道传输模块返回配置信息，隧道传输模块解析配置信息，并将配置信息发送给数据汇聚模块，数据汇聚模块根据配置信息配置终端地址为虚拟 IP 地址/掩码，并配置与终端通信的内网服务器的地址/掩码，然后通知隧道传输模块设置完成；隧道传输模块向终端中的业务模块发送指示隧道建立完成的指示信息。

步骤 303-304 可以具体采用如下方式实现：

1、终端首先尝试建立 UDP 隧道：终端向 VPN 网关发送建立 UDP 隧道的请求，并可以在请求消息中携带身份信息，VPN 网关可以通过与认证服务器进行信息交互来校验身份的合法性，向终端返回校验结果；如果终端身份合法且企业网络防火墙开放了特定的 UDP 端口，则 UDP 隧道建立成功，否则，UDP 隧道建立失败。本节所述的 UDP 隧道，包含 UDP 明文隧道、UDP

加密隧道和基于 UDP 的 DTLS（Datagram Transport Layer Security）隧道。可以理解的是，在 SOCKS V5 代理服务器、HTTP 代理服务器、HTTPS 代理服务器同时存在时，如果需要通过应用层代理服务器建立 UDP 隧道，要求经过 SOCK5 VS 代理服务器建立 UDP 隧道，相对于其他 HTTP 隧道、SSL 隧道来说，UDP 隧道能提高语音质量。

2、终端尝试建立 SSL 隧道：终端向 VPN 网关发送建立 SSL 隧道的请求，并可以在请求消息中携带身份信息，VPNVPN 网关可以通过与认证服务器进行信息交互来校验身份的合法性，向终端返回校验结果；如果终端身份合法且企业网络防火墙开放了特定的 SSL 端口，则 SSL 隧道建立成功，否则，SSL 隧道建立失败。在 SSL 隧道建立成功之后，可以进一步建立 UDP 隧道，具体的，可以先发送 UDP 连接建立请求以便探测终端到 VPN 网关间的路径是否已通，如果路径已通，则 IMS 通过 SSL 隧道与 VPN 网关协商 UDP 隧道密钥，以便建立 UDP 隧道。本节所述的 UDP 隧道，包含 UDP 明文隧道、UDP 加密隧道和基于 UDP 的 DTLS（Datagram Transport Layer Security）隧道。可以理解的是，如果需要通过应用层代理服务器建立 SSL 隧道，则要求通过 HTTPS 代理服务器建立 SSL 隧道。

3、终端尝试建立 HTTP 隧道：终端向 VPN 网关发送建立 HTTP 隧道的请求，并可以在请求消息中携带身份信息，VPN 网关可以通过与认证服务器进行信息交互来校验身份的合法性，向终端返回校验结果；如果终端身份合法且企业网络防火墙开放了 HTTP 端口，则 HTTP 隧道建立成功。在隧道建立成功之后，再通过 HTTP 隧道与 VPN 网关协商 SSL 隧道密钥，以便后续利用 SSL 隧道密钥对 HTTP 隧道中传输的业务数据进行加密。可以理解的是，如果需要通过应用层代理服务器建立 HTTP 隧道，则要求通过 HTTP 代理服务器建立 HTTP 隧道。

需要说明的是，如果当前需要进行的业务的安全性较低但性能要求高，则可以选择建立 UDP 隧道，如果当前需要进行的业务的安全性较高，则可以选择建立 SSL 隧道。

可选的，终端可以首先尝试采用现有的方式直接与 IMS 核心网中的内网服务器建立业务连接，由于 IMS 业务要求在企业网络和 IMS 网络中部署的防火墙上面开放较多的 UDP 端口，如果防火墙的端口开发不满足 IMS 业务的需求，则会导致终端直接和内网服务器之间建立业务连接的尝试失败，在建立业务连接失败之后，再采用本发明实施例提供的上述方式请求建立 UDP VPN 隧道、SSL VPN 隧道或者 HTTP VPN 隧道；或者，也可以直接采用本发明实施例提供的上述方式请求建立 UDP VPN 隧道、SSL VPN 隧道或者 HTTP VPN 隧道。

图 4 示出了本发明实施例提供的通过 VPN 隧道进行身份认证的流程图，其中，通过 VPN 隧道进行身份认证的过程包括:

401、终端通过 VPN 隧道向 VPN 网关发送终端标识码。

402、VPN 网关通过本地或外部的签约记录和终端标识码，确定是否允许该终端建立 VPN 隧道，并向终端返回认证结果，即标识终端是否可以建立 VPN 隧道的结果。

403、当允许该终端建立 VPN 隧道时，终端通过 VPN 隧道向 VPN 网关发送用户身份信息。

其中，用户身份信息包括：用户名和密码。

404、VPN 网关根据用户身份信息，对用户的身份进行校验，并返回校验结果。

具体的，可以根据本地存储的签约用户信息或者外部服务器的签约用户信息，对用户的身份进行校验。

其中，终端也通过 VPN 隧道发送消息请求 VPN 网关对组件调用者进行认证，即请求 VPN 网关校验该终端是否可以使用通信能力组件，执行通信能力组件的功能，即该终端是否可以建立 VPN 和进行数据汇聚。

其中，图 4 所示的各步骤的执行主体为终端中的隧道传输模块。

图 5 示出了本发明实施例提供的 IMS 业务数据安全穿越流程图，该方法中终端主动与 IMS 核心网中的内网服务器进行通信，具体的，IMS 业务数据

安全穿越过程包括:

501-502、终端将待发送业务数据的源地址设置为虚拟 IP 地址、目的地址设置为内网服务器的地址，将待发送业务数据的源端口设置为终端的业务端口、目的端口设置为内网服务器的业务端口，得到第一业务报文，对第一业务报文进行加密，设置加密后的报文的源 IP 地址为终端的真实 IP 地址、目的 IP 地址为 VPN 网关的 IP 地址、源端口为终端的隧道端口，目的端口为 VPN 网关的隧道端口，得到第一隧道报文，然后利用终端与 VPN 网关间的隧道向 VPN 网关发送第一隧道报文。

如前所述，终端中包括通信能力组件，通信能力组件中包括三大模块，数据汇聚模块，加解密模块和隧道传输模块，具体的，数据汇聚模块包括：第一数据汇聚模块和第二数据汇聚模块，加解密模块包括加密模块和解密模块，隧道传输模块包括：第一隧道传输模块和第二隧道传输模块。

终端获得第一业务报文具体可以有两种实现方式：第一种方式为：终端的业务模块通过调用终端中的第一数据汇聚模块提供的接口，触发所述第一数据汇聚模块将待发送业务数据的源地址设置为虚拟 IP 地址，目的地址设置为内网服务器的地址，将待发送业务数据的源端口设置为终端的业务端口、目的端口设置为内网服务器的业务端口；第二种方式为：所述终端中的第一数据汇聚模块在操作系统提供的通信接口捕获所述待发送业务数据，将所述待发送业务数据的源地址设置为虚拟 IP 地址，目的地址设置为内网服务器的地址，源端口设置为终端的业务端口、目的端口设置为内网服务器的业务端口。其中，操作系统提供的通信接口可以是虚拟网卡驱动口或传输层驱动接口（Transport Driver Interface，TDI）。

然后终端中的加密模块对第一业务报文进行加密，终端中的第一隧道传输模块设置加密后的报文的源 IP 地址为终端的真实 IP 地址，目的 IP 地址为 VPN 网关的 IP 地址，源端口为终端的隧道端口，目的端口为 VPN 网关的隧道端口，得到第一隧道报文，然后利用终端与 VPN 网关间的隧道向 VPN 网关发送第一隧道报文。具体的，如果采用的 VPN 隧道为 HTTP VPN 隧道，则

该步骤中终端中的加密模块采用 SSL 隧道密钥，对第一业务报文进行加密。

503-504、VPN 网关收到第一隧道报文后，对第一隧道报文进行解封装、解密，得到源地址为虚拟 IP 地址、目的地址为内网服务器的 IP 地址的第一业务报文，向内网服务器发送第一业务报文。

其中，如果采用 HTTP 隧道，则该步骤中 VPN 网关采用 SSL 隧道密钥对第一隧道报文进行解密。

505、内网服务器收到第一业务报文后，如果需要向终端回复响应报文，则向 VPN 网关发送源地址为内网服务器的 IP 地址、目的地址为虚拟 IP 地址、源端口为内网服务器的业务端口，目的端口为终端的业务端口的第二业务报文。

具体的，内网服务器广播携带该虚拟 IP 地址的地址解析协议（Adress resolution protocol，ARP）消息，以便查询该虚拟 IP 地址属于哪个 VPN 网关，曾分配过这个虚拟 IP 地址的 VPN 网关向内网服务器发送 ARP 应答消息，在 ARP 应答消息中携带该 VPN 网关的 MAC 地址，内网服务器根据该 MAC 地址，向 VPN 网关发送第二业务报文。

506-507、VPN 网关对所接收的第二业务报文进行加密、封装成第二隧道报文，利用 VPN 网关与终端间的隧道向终端发送第二隧道报文。

其中，如果采用 HTTP 隧道，则该步骤中 VPN 网关采用 SSL 隧道密钥对第二业务报文进行加密。

508、终端接收到 VPN 网关发送的第二隧道报文之后，对所接收的第二隧道报文进行解封装、解密得到第二业务报文，从第二业务报文中提取业务数据。

具体的，终端中的第二隧道传输模块接收到 VPN 网关发送的第二隧道报文，对第二隧道报文进行解封装，去除第二隧道报文中的源 IP 地址（VPN 网关的 IP 地址）和目的 IP 地址（终端的真实 IP 地址），源端口（VPN 网关的隧道端口），目的端口（终端的隧道端口）。然后终端中的解密模块对解封装后的报文进行解密得到第二业务报文，第二数据汇聚模块去除解密后的第二

业务报文的源 IP 地址(内网服务器的 IP 地址)和目的 IP 地址(虚拟 IP 地址),源端口(内网服务器的业务端口),目的端口(终端的业务端口),提取第二业务报文中的业务数据。

其中,如果位于终端上层的业务模块想获取第二业务报文中的业务数据,可以有如下两种实现方式:第一种方式为:终端的业务模块从终端中的第二数据汇聚模块获得第二业务报文中的业务数据;第二种方式为:终端的第二数据汇聚模块将所提取的业务数据植入操作系统提供的通信接口,终端中的业务模块从所述操作系统提供的通信接口中获取第二业务报文中的业务数据。

本发明实施例中业务数据的传输都是通过 VPN 隧道(比如前述 UDP VPN 隧道、SSL VPN 隧道和 HTTP VPN 隧道)传输的,这些隧道都能够穿过具备 NAT 功能的路由器、防火墙、交换机等 NAT 设备,因此可以防止这些 NAT 设备对业务数据进行访问控制、地址修改等操作,这样可以避免由于 NAT 设备的操作导致的终端与内网服务器之间的通信失败。并且,UDP VPN 隧道可以穿越 SOCKS V5 代理服务器,SSL VPN 隧道能够穿越 HTTPS 代理服务器,HTTP VPN 隧道能够穿越 HTTP 代理服务器,所以在终端与内网服务器通信时,可以防止相应的应用层代理服务器对业务数据进行访问控制、地址修改等操作,这样可以避免由于应用层代理服务器操作导致的终端与内网服务器之间的通信失败。而且该实施例将虚拟 IP 地址作为终端与内网服务器通信的地址,通过 VPN 网关与内网服务器进行通信,无需企业网络做额外的路由转换,不需要改动企业网络。

图 6 示出了本发明实施例提供的 IMS 业务数据安全穿越流程图,该方法中 IMS 核心网中的内网服务器主动与终端进行通信,具体的,IMS 业务数据安全穿越过程包括:

601、内网服务器向 VPN 网关发送源地址为内网服务器的 IP 地址、目的地址为虚拟 IP 地址、源端口为内网服务器的业务端口、目的地址为终端的业务端口的业务报文。

具体的，内网服务器需要向某个虚拟 IP 地址对应的终端发送业务数据时，该内网服务器广播携带该虚拟 IP 地址的 ARP 消息，以便查询该虚拟 IP 地址属于哪个 VPN 网关，曾分配这个虚拟 IP 地址的 VPN 网关向内网服务器发送 ARP 应答消息，在 ARP 应答消息中携带该 VPN 网关的 IP 地址，内网服务器根据该 IP 地址，向 VPN 网关发送源地址为内网服务器的 IP 地址、目的地址为虚拟 IP 地址的业务报文。

602-603、VPN 网关对所接收的业务报文进行加密、封装后得到隧道报文，利用已建立的隧道向终端发送隧道报文。

该步骤的具体实现方式参见上述步骤 506-507 的相应描述，在此不再赘述。

604、终端接收到 VPN 网关发送的隧道报文后，进行解封装、解密，得到业务报文，并获取业务报文中的业务数据。

该步骤的具体实现方式参见上述步骤 508 的相应描述，在此不再赘述.

本发明实施例中业务数据的传输都是通过 VPN 隧道(比如前述 UDP VPN 隧道、SSL VPN 隧道和 HTTP VPN 隧道）传输的，这些隧道都能够穿过具备 NAT 功能的路由器、防火墙、交换机等 NAT 设备，因此可以防止这些 NAT 设备对业务数据进行访问控制、地址修改等操作，这样可以避免由于 NAT 设备的操作导致的终端与内网服务器之间的通信失败。并且，UDP VPN 隧道可以穿越 SOCKS V5 代理服务器，SSL VPN 隧道能够穿越 HTTPS 代理服务器，HTTP VPN 隧道能够穿越 HTTP 代理服务器，所以在终端与内网服务器通信时，可以防止相应的应用层代理服务器对业务数据进行访问控制、地址修改等操作，这样可以避免由于应用层代理服务器操作导致的终端与内网服务器之间的通信失败。而且该实施例将虚拟 IP 地址作为终端与内网服务器通信的地址，通过 VPN 网关与内网服务器进行通信，无需企业网络做额外的路由转换，不需要改动企业网络。

需要说明的，在上述实施例建立 UDP VPN 隧道、SSL VPN 隧道或者 HTTP VPN 隧道之后，终端会定期向 VPN 网关发送保活报文，或按照设定的时间向

VPN 网关发送保活报文，以便维持已建立的隧道。

需要说明的，当终端与 VPN 网关间存在两个 VPN 隧道，即 UDP VPN 隧道和 SSL VPN 隧道时，可以通过 UDP VPN 隧道传输业务数据，具体传输方式如上述实施例所述，终端还可以通过 SSL VPN 隧道传输业务控制信息，具体的终端将待发送的第一业务控制信息进行加密后，设置加密后的控制信息的源 IP 地址为终端的真实 IP 地址，目的 IP 地址为 VPN 网关的 IP 地址，然后向 VPN 网关发送；VPN 网关收到后进行解封装，解密，得到第一控制信息。同理，VPN 网关可以利用 SSL VPN 隧道向终端发送第二控制信息。这样，可以实现通过安全性较低的 UDP VPN 隧道传输业务数据，通过安全性较高的 SSL VPN 隧道传输业务控制信息。

参阅图 7，本发明实施例提供一种终端，其包括：

第一数据汇聚模块 701，用于将待发送业务数据的源地址设置为虚拟 IP 地址、目的地址设置为内网服务器的地址，得到第一业务报文；其中，所述虚拟 IP 地址是多媒体子系统 IMS 核心网为所述终端分配的地址；

第一隧道传输模块 702，用于将所述第一业务报文封装成第一隧道报文，其中所述第一隧道报文的源 IP 地址为终端的 IP 地址、目的 IP 地址为安全隧道网关的 IP 地址；利用所述终端与安全隧道网关间的虚拟专用网 VPN 隧道，将所述第一隧道报文发送给安全隧道网关，使所述安全隧道网关将第一隧道报文中的第一业务报文发送给内网服务器。

进一步的，在本发明另一个实施例中，为了接收内网服务器发送的业务数据，该终端还可以包括：

第二隧道传输模块 703，用于当终端需要接收内网服务器的业务数据时，通过所述隧道接收第二隧道报文，对所述第二隧道报文进行解封装；其中，第二隧道报文的源 IP 地址为安全隧道网关的 IP 地址、目的 IP 地址为终端的 IP 地址。

第二数据汇聚模块 704，用于从第二隧道传输模块解封装得到的第二业务

报文中获取业务数据，其中，所述第二业务报文的源地址为内网服务器的地址、目的地址为虚拟 IP 地址。

进一步的，在本发明另一个实施例中，该终端还可以包括:

业务模块 705，具体用于当终端需要发送业务数据时，通过调用第一数据汇聚模块提供的接口，触发所述第一数据汇聚模块将待发送业务数据的源地址设置为虚拟 IP 地址，目的地址设置为内网服务器的地址；当终端需要接收内网服务器的业务数据时，从第二数据汇聚模块获得第二业务报文中的业务数据。

具体的，第一数据汇聚模块 701，用于当终端需要发送业务数据时，在操作系统提供的通信接口捕获所述待发送业务数据，将所述待发送业务数据的源地址设置为虚拟 IP 地址，目的地址设置为内网服务器的地址；其中，待发送业务数据是由业务模块 705 发送到操作系统提供的通信接口的。采用这种方式，使业务模块与通信能力组件不需要紧密耦合。

所述第二数据汇聚模块 704，用于当终端需要接收内网服务器的业务数据时，提取第二业务报文中的业务数据，将所提取的业务数据植入操作系统提供的通信接口，使终端中的业务模块能够从所述操作系统提供的通信接口中获取所述第二业务报文中的业务数据。

在本发明另一个实施例中，为了保证 VPN 隧道上传输的报文的安全性，该终端还可以包括:

加密模块 706，用于在终端与安全隧道网关间的 VPN 隧道为 HTTP VPN 隧道时，利用 SSL 隧道密钥对第一业务报文进行加密;

解密模块 707，用于在终端与安全隧道网关间的 VPN 隧道为 HTTP VPN 隧道时，利用 SSL 隧道密钥对第二隧道传输模块解封装得到的报文进行解密。

其中，所述 SSL 隧道密钥是所述终端预先通过所述 HTTP 隧道与安全隧道网关协商得到的。此时，第一隧道传输模块 701 具体用于将加密模块 706 加密后的第一业务报文封装成第一隧道报文，利用所述终端与安全隧道网关间的 VPN 隧道，将所述第一隧道报文发送给安全隧道网关。第二数据汇聚模

块 704 具体用于从解密模块 707 解密得到的报文中获取业务数据。

当终端与安全隧道网关间存在两条 VPN 隧道，比如 UDP VPN 隧道和 SSL VPN 隧道时，在本发明又一个实施例中，终端可以采用第一数据汇聚模块 701、第一隧道传输模块 702、第二隧道传输模块 703 和第二数据汇聚模块 704 处理和传输业务数据，此外，还可以采用第三隧道传输模块 708 和/或第四隧道传输模块 709 处理和传输业务控制信息，其中：

第三隧道传输模块 708，用于利用所述 SSL VPN 隧道向所述业务安全隧道网关发送第一业务控制信息；和/或，

第四隧道传输模块 709，用于利用所述 SSL VPN 隧道接收所述业务安全隧道网关发送的第二业务控制信息。

为了建立上述两条 VPN 隧道，在本发明又一个实施例中，还包括：

第一隧道建立单元 710，用于建立 UDP VPN 隧道；

第二隧道建立单元 711，用于通过已建立的 SSL 隧道与所述安全隧道网关协商 UDP 隧道密钥，以便建立 UDP 隧道。

本发明实施例中终端将 IMS 核心网分配的虚拟 IP 地址作为终端与内网服务器的通信地址，将待发送业务数据的源地址设置为虚拟 IP 地址、目的地址设置为内网服务器的地址，并封装成隧道报文后通过终端与安全隧道网关间的隧道传输到安全隧道网关，使安全隧道网关能够将源地址为虚拟 IP 地址、目的地址为内网服务器地址的业务报文发送给内网服务器；当需要接收内网服务器的业务数据时，将接收的隧道报文进行解封装，得到源地址为内网服务器的地址、目的地址为虚拟 IP 地址的业务报文，这样，就能够实现通过安全隧道网关传输内网服务器与终端间的业务数据，不需要改动终端所在的企业网络，就可以使终端穿越私网，与公网中的服务器进行通信。

参阅图 8，本发明实施例提供一种安全隧道网关，其包括：隧道传输模块一 80，隧道传输模块一 80 包括：第一接收模块 801，解封装模块 802，和第一发送模块 803，

第一接收模块 801，用于通过安全隧道网关与终端间的隧道接收第一隧道

报文；其中，所述第一隧道报文的源 IP 地址为终端的 IP 地址、目的 IP 地址为安全隧道网关的 IP 地址；

解封装模块 802，用于对所述第一隧道报文进行解封装；

第一发送模块 803，用于将解封装模块解封装后得到的第一业务报文向内网服务器发送，其中，所述第一业务报文的源地址为虚拟 IP 地址、目的地址为内网服务器地址。

进一步，在本发明另一个实施例中，为了向终端传输内网服务器的发送的业务报文，还包括：隧道传输模块一 90，其中，隧道传输模块一 90 具体包括：

第二接收模块 804，用于接收内网服务器发送的第二业务报文，所述第二业务报文的源地址为内网服务器的地址、目的地址为虚拟 IP 地址；

封装模块 805，用于将所述第二业务报文封装成第二隧道报文，其中，第二隧道报文的源 IP 地址为安全隧道网关的 IP 地址、目的 IP 地址为终端的 IP 地址；

第二发送单元 806，用于通过安全隧道网关与终端间的隧道向所述终端发送第二隧道报文。

在本发明另一个实施例中，为了保证 VPN 隧道上传输的报文的安全性，该终端还可以包括：

加密模块 807，用于在所述终端与安全隧道网关间的 VPN 隧道为 HTTP VPN 隧道时，利用 SSL 隧道密钥对所述第二业务报文进行加密；

解密模块 808，用于在所述终端与安全隧道网关间的 VPN 隧道为 HTTP VPN 隧道时，利用 SSL 隧道密钥对解封装模块解封装所得到的报文进行解密，得到第一业务报文。

其中，所述 SSL 隧道密钥是所述终端预先通过所述 HTTP 隧道与安全隧道网关协商得到的；封装模块 805 具体用于将加密后的第二业务报文封装成第二隧道报文；第一发送模块 803 具体用于将解密模块 808 解密后得到的第一业务报文向内网服务器发送。

当终端与安全隧道网关间存在两条VPN隧道，比如UDP VPN隧道和SSL VPN隧道时，终端可以利用UDP VPN隧道初始业务报文，利用SSL VPN隧道传输业务控制信息，则在本发明又一个实施例中，还包括:

第三发送模块809，还用于利用所述SSL VPN隧道向所述终端发送第二业务控制信息；和，第四接收模块810，还用于利用所述SSL VPN隧道接收所述终端发送的第一业务控制信息。

其中，为了建立上述两条隧道，在本发明又一个实施例中，还包括:

第一隧道建立模块811，用于与终端间建立SSL隧道;

第二隧道建立模块812，用于通过已建立的SSL隧道与所述终端协商UDP隧道密钥，以便建立UDP隧道。

本发明实施例中的安全隧道网关作为中间设备，将来自终端的隧道报文解封装后发送给内网服务器，将来自内网服务器的业务报文封装成隧道报文后发送给终端，以便终端与IMS核心网中的服务器间传输业务数据，这样不需要改动终端所在的企业网络，就可以使终端穿越私网，与公网中的服务器进行通信了。

参阅图9，本发明实施例提供一种网络系统，其主要包括上述实施例中的安全隧道网关901和内网服务器902，其中安全隧道网关的功能和结构与上述实施例中的描述相似，在此不再赘述。

本发明实施例提供的网络系统利用安全隧道网关作为中间设备，将来自终端的隧道报文解封装后发送给内网服务器，将来自内网服务器的业务报文封装成隧道报文后发送给终端，以便终端与IMS核心网中的服务器间传输业务数据，这样不需要改动终端所在的企业网络，就可以使终端穿越私网，与公网中的服务器进行通信了。

需要说明的是，对于前述的各方法实施例，为了简单描述，故将其都表述为一系列的动作组合，但是本领域技术人员应该知悉，本发明并不受所描述的动作顺序的限制，因为依据本发明，某些步骤可以采用其他顺序或者同时进行。其次，本领域技术人员也应该知悉，说明书中所描述的实施例均属

于优选实施例，所涉及的动作和模块并不一定是本发明所必须的。

在上述实施例中，对各个实施例的描述都各有侧重，某个实施例中没有详述的部分，可以参见其他实施例的相关描述。

本领域普通技术人员可以理解实现上述实施例方法中的全部或部分流程，是可以通过计算机程序来指令相关的硬件来完成，所述的程序可存储于计算机可读取存储介质中，该程序在执行时，可包括如上述各方法的实施例的流程。其中，所述的存储介质可为磁碟、光盘、只读存储记忆体（Read-Only Memory，ROM）或随机存储记忆体（Random Access Memory，RAM）等。

以上对本发明所提供的一种终端穿越私网与 IMS 核心网中服务器通信的方法、装置及网络系统进行了详细介绍，对于本领域的一般技术人员，依据本发明实施例的思想，在具体实施方式及应用范围上均会有改变之处，综上所述，本说明书内容不应理解为对本发明的限制。

权 利 要 求

1、一种终端穿越私网与 IMS 核心网中服务器通信的方法，其特征在于，包括:

终端将待发送业务数据的源地址设置为虚拟 IP 地址、目的地址设置为内网服务器的地址，得到第一业务报文，其中，所述虚拟 IP 地址是多媒体子系统 IMS 核心网为所述终端分配的地址;

将所述第一业务报文封装成第一隧道报文，其中所述第一隧道报文的源 IP 地址为终端的 IP 地址、目的 IP 地址为安全隧道网关的 IP 地址;

利用所述终端与安全隧道网关间的虚拟专用网 VPN 隧道，将所述第一隧道报文发送给安全隧道网关，使所述安全隧道网关将第一隧道报文中的第一业务报文发送给内网服务器。

2、根据权利要求 1 所述的方法，其特征在于，

所述将待发送业务数据的源地址设置为虚拟 IP 地址、目的地址设置为内网服务器的地址包括:

终端的业务模块通过调用终端中的第一数据汇聚模块提供的接口，触发所述第一数据汇聚模块将待发送业务数据的源地址设置为虚拟 IP 地址，目的地址设置为内网服务器的地址;

或者，

所述终端中的第一数据汇聚模块在操作系统提供的通信接口捕获所述待发送业务数据，将所述待发送业务数据的源地址设置为虚拟 IP 地址，目的地址设置为内网服务器的地址。

3、根据权利要求 1 所述的方法，其特征在于，

所述终端与安全隧道网关间的 VPN 隧道为超文本传输协议 HTTP VPN 隧道;

在将所述第一业务报文封装成第一隧道报文之前，该方法还包括:

利用 SSL 隧道密钥对第一业务报文进行加密；其中，所述 SSL 隧道密钥

是所述终端预先通过所述 HTTP 隧道与安全隧道网关协商得到的;

将所述第一业务报文封装成第一隧道报文具体为:

将加密后的第一业务报文封装成第一隧道报文。

4、根据权利要求 1 所述的方法，其特征在于，该方法还包括:

当终端需要接收内网服务器的业务数据时，终端通过所述隧道接收第二隧道报文，其中，第二隧道报文的源 IP 地址为安全隧道网关的 IP 地址、目的 IP 地址为终端的 IP 地址;

对所述第二隧道报文进行解封装得到第二业务报文；其中，所述第二业务报文的源地址为内网服务器的地址、目的地址为虚拟 IP 地址;

获得所述第二业务报文中的业务数据。

5、根据权利要求 4 所述的方法，其特征在于，

所述终端与安全隧道网关间的 VPN 隧道为 HTTP VPN 隧道;

在对所述第二隧道报文进行解封装之后，该方法还包括:

利用 SSL 隧道密钥对解封装得到的报文进行解密；其中，所述 SSL 隧道密钥是所述终端预先通过所述 HTTP 隧道与安全隧道网关协商得到的;

所述第二业务报文为解密后得到的报文。

6、根据权利要求 1 所述的方法，其特征在于，

所述终端与安全隧道网关间的 VPN 隧道为用户数据报协议 UDP VPN 隧道;

当所述终端与安全隧道网关间还存在安全套接层 SSL VPN 隧道时，该方法还包括:

所述终端利用所述 SSL VPN 隧道向所述安全隧道网关发送第一业务控制信息;

或者，

所述终端利用所述 SSL VPN 隧道接收所述安全隧道网关发送的第二业务控制信息。

7、根据权利要求 6 所述的方法，其特征在于，

该方法还包括：所述终端与安全隧道网关间先建立 SSL 隧道，通过已建立的 SSL 隧道与所述安全隧道网关协商 UDP 隧道密钥，以便建立 UDP 隧道。

8、一种终端穿越私网与 IMS 核心网中服务器通信的方法，其特征在于，包括:

安全隧道网关通过安全隧道网关与终端间的隧道接收第一隧道报文；其中，所述第一隧道报文的源 IP 地址为终端的 IP 地址、目的 IP 地址为安全隧道网关的 IP 地址;

对所述第一隧道报文进行解封装，得到第一业务报文，所述第一业务报文的源地址为虚拟 IP 地址、目的地址为内网服务器地址;

将所述第一业务报文向内网服务器发送。

9、根据权利要求 8 所述的方法，其特征在于，

所述终端与安全隧道网关间的 VPN 隧道为 HTTP VPN 隧道;

在对所述第一隧道报文进行解封装之后，还包括:

利用 SSL 隧道密钥对解封装后的报文进行解密，其中，所述 SSL 隧道密钥是所述终端预先通过所述 HTTP 隧道与安全隧道网关协商得到的;

所述第一业务报文为解密得到的报文。

10、根据权利要求 8 所述的方法，其特征在于，还包括:

安全隧道网关接收内网服务器发送的第二业务报文，所述第二业务报文的源地址为内网服务器的地址、目的地址为虚拟 IP 地址;

将所述第二业务报文封装成第二隧道报文，其中，第二隧道报文的源 IP 地址为安全隧道网关的 IP 地址、目的 IP 地址为终端的 IP 地址;

通过安全隧道网关与终端间的隧道向所述终端发送第二隧道报文。

11、根据权利要求 10 所述的方法，其特征在于，

所述终端与安全隧道网关间的 VPN 隧道为 HTTP VPN 隧道;

在将所述第二业务报文封装成第二隧道报文之前，该方法还包括:

利用 SSL 隧道密钥对所述第二业务报文进行加密;

所述将所述第二业务报文封装成第二隧道报文具体:

将加密后的报文封装成第二隧道报文。

12、根据权利要求 10 所述的方法，其特征在于，

所述终端与安全隧道网关间的 VPN 隧道为 UDP VPN 隧道;

当所述终端与安全隧道网关间还存在 SSL VPN 隧道时，该方法还包括:

所述安全隧道网关利用所述 SSL VPN 隧道向所述终端发送第二业务控制信息;

或者，

所述安全隧道网关利用所述 SSL VPN 隧道接收所述终端发送的第一业务控制信息。

13、一种终端，其特征在于，包括：通信能力组件，所述通信能力组件包括:

第一数据汇聚模块,用于将待发送业务数据的源地址设置为虚拟 IP 地址、目的地址设置为内网服务器的地址，得到第一业务报文；其中，所述虚拟 IP 地址是多媒体子系统 IMS 核心网为所述终端分配的地址;

第一隧道传输模块，用于将所述第一业务报文封装成第一隧道报文，其中所述第一隧道报文的源 IP 地址为终端的 IP 地址、目的 IP 地址为安全隧道网关的 IP 地址; 利用所述终端与安全隧道网关间的虚拟专用网 VPN 隧道，将所述第一隧道报文发送给安全隧道网关，使所述安全隧道网关将第一隧道报文中的第一业务报文发送给内网服务器。

14、根据权利要求 13 所述的终端，其特征在于，

第二隧道传输模块，用于当终端需要接收内网服务器的业务数据时，通过所述隧道接收第二隧道报文，对所述第二隧道报文进行解封装；其中，第二隧道报文的源 IP 地址为安全隧道网关的 IP 地址、目的 IP 地址为终端的 IP 地址;

第二数据汇聚模块，用于从第二隧道传输模块解封装得到的第二业务报文中获取业务数据，其中，所述第二业务报文的源地址为内网服务器的地址、目的地址为虚拟 IP 地址，或者

用于当终端需要接收内网服务器的业务数据时，提取第二业务报文中的业务数据，将所提取的业务数据植入操作系统提供的通信接口，使终端中的业务模块能够从所述操作系统提供的通信接口中获取所述第二业务报文中的业务数据。

15、根据权利要求 13 所述的终端，其特征在于，

所述终端与安全隧道网关间的 VPN 隧道为 UDP VPN 隧道；当所述终端与安全隧道网关间还存在 SSL VPN 隧道时，还包括：

第三隧道传输模块，用于利用所述 SSL VPN 隧道向所述业务安全隧道网关发送第一业务控制信息；

或者，

第四隧道传输模块，用于利用所述 SSL VPN 隧道接收所述业务安全隧道网关发送的第二业务控制信息。

16、根据权利要求 15 所述的终端，其特征在于，还包括：

第一隧道建立单元，用于建立 UDP VPN 隧道；

第二隧道建立单元，用于通过已建立的 SSL 隧道与所述安全隧道网关协商 UDP 隧道密钥，以便建立 UDP 隧道。

17、一种安全隧道网关，其特征在于，包括：

第一接收模块，用于通过安全隧道网关与终端间的隧道接收第一隧道报文；其中，所述第一隧道报文的源 IP 地址为终端的 IP 地址、目的 IP 地址为安全隧道网关的 IP 地址；

解封装模块，用于对所述第一隧道报文进行解封装；

第一发送模块，用于将解封装模块解封装后得到的第一业务报文向内网服务器发送，其中，所述第一业务报文的源地址为虚拟 IP 地址、目的地址为内网服务器地址。

18、根据权利要求 17 所述的安全隧道网关，其特征在于，还包括：

第二接收模块，用于接收内网服务器发送的第二业务报文，所述第二业务报文的源地址为内网服务器的地址、目的地址为虚拟 IP 地址；

封装模块，用于将所述第二业务报文封装成第二隧道报文，其中，第二隧道报文的源 IP 地址为安全隧道网关的 IP 地址、目的 IP 地址为终端的 IP 地址；

第二发送单元，用于通过安全隧道网关与终端间的隧道向所述终端发送第二隧道报文。

19、根据权利要求 17 所述的安全隧道网关，其特征在于，

所述终端与安全隧道网关间的 VPN 隧道为 UDP VPN 隧道；当所述终端与安全隧道网关间还存在 SSL VPN 隧道时，还包括：

第三发送模块，还用于利用所述 SSL VPN 隧道向所述终端发送第二业务控制信息；

第四接收模块，还用于利用所述 SSL VPN 隧道接收所述终端发送的第一业务控制信息。

20、一种网络系统，其特征在于，包括：安全隧道网关和内网服务器，

安全隧道网关，用于通过安全隧道网关与终端间的隧道接收第一隧道报文；其中，所述第一隧道报文的源 IP 地址为终端的 IP 地址、目的 IP 地址为安全隧道网关的 IP 地址；对所述第一隧道报文进行解封装，得到第一业务报文，所述第一业务报文的源地址为虚拟 IP 地址、目的地址为内网服务器地址；将所述第一业务报文向内网服务器发送；接收内网服务器发送的第二业务报文，所述第二业务报文的源地址为内网服务器的地址、目的地址为虚拟 IP 地址；将所述第二业务报文封装成第二隧道报文，其中，第二隧道报文的源 IP 地址为安全隧道网关的 IP 地址、目的 IP 地址为终端的 IP 地址；通过安全隧道网关与终端间的隧道向所述终端发送第二隧道报文；

内网服务器，用于接收安全隧道网关发送的第一业务报文，向安全隧道网关发送第二业务报文。

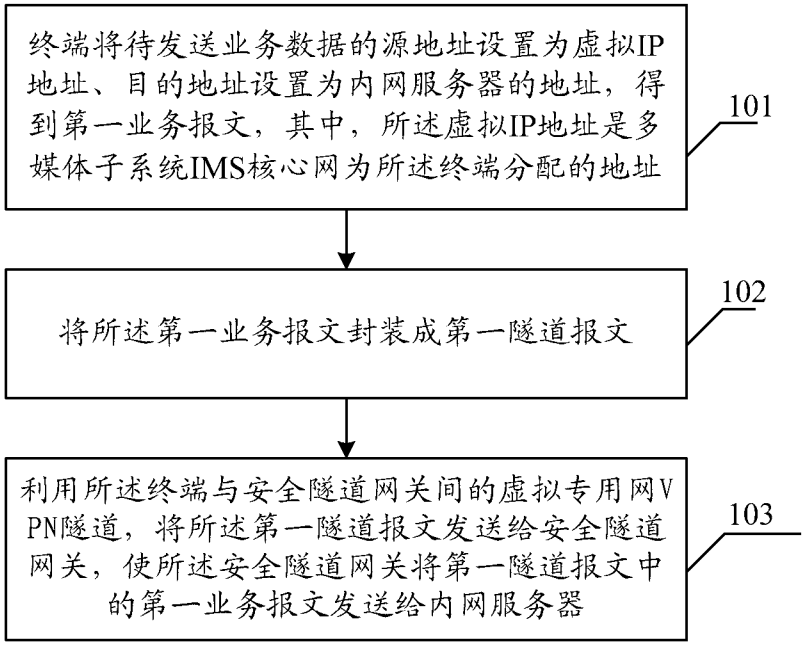
终端将待发送业务数据的源地址设置为虚拟IP地址、目的地址设置为内网服务器的地址，得到第一业务报文，其中，所述虚拟IP地址是多媒体子系统IMS核心网为所述终端分配的地址
101
将所述第一业务报文封装成第一隧道报文
102
利用所述终端与安全隧道网关间的虚拟专用网VPN隧道，将所述第一隧道报文发送给安全隧道网关，使所述安全隧道网关将第一隧道报文中的第一业务报文发送给内网服务器
103

图 1A

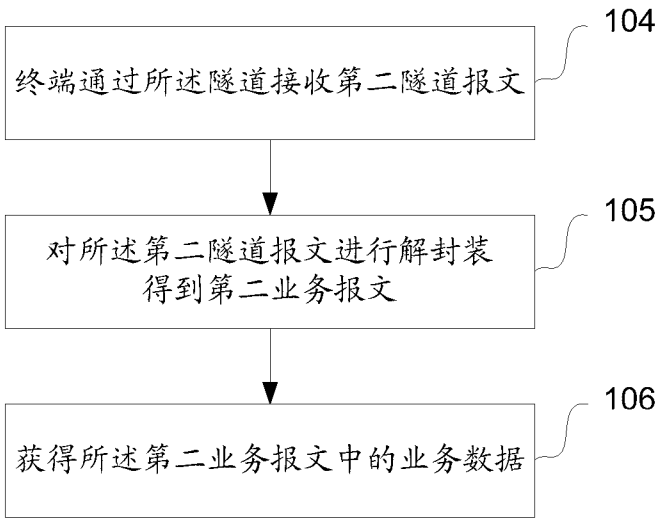
终端通过所述隧道接收第二隧道报文
104
对所述第二隧道报文进行解封装得到第二业务报文
105
获得所述第二业务报文中的业务数据
106

图 1B

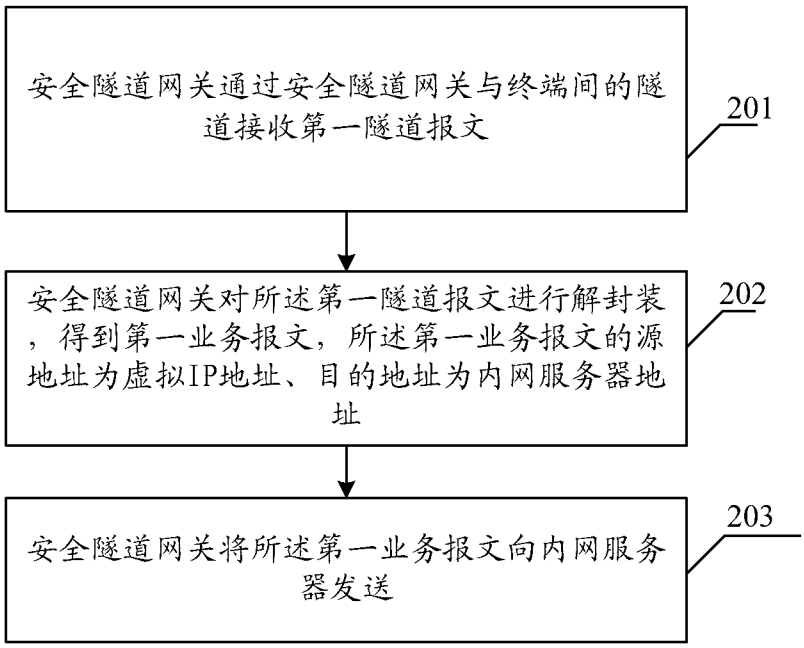
安全隧道网关通过安全隧道网关与终端间的隧道接收第一隧道报文
201
安全隧道网关对所述第一隧道报文进行解封装，得到第一业务报文，所述第一业务报文的源地址为虚拟IP地址、目的地址为内网服务器地址
202
安全隧道网关将所述第一业务报文向内网服务器发送
203

图 2A

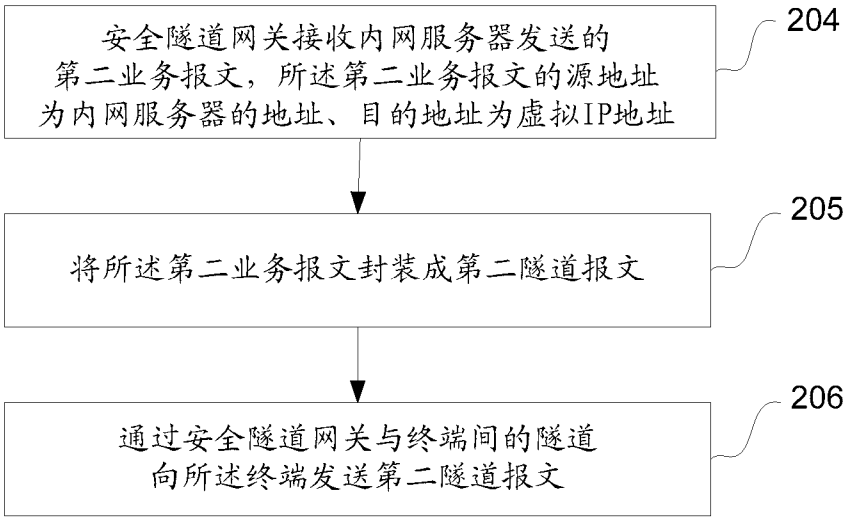
安全隧道网关接收内网服务器发送的第二业务报文，所述第二业务报文的源地址为内网服务器的地址、目的地址为虚拟IP地址
204
将所述第二业务报文封装成第二隧道报文
205
通过安全隧道网关与终端间的隧道向所述终端发送第二隧道报文
206

图 2B

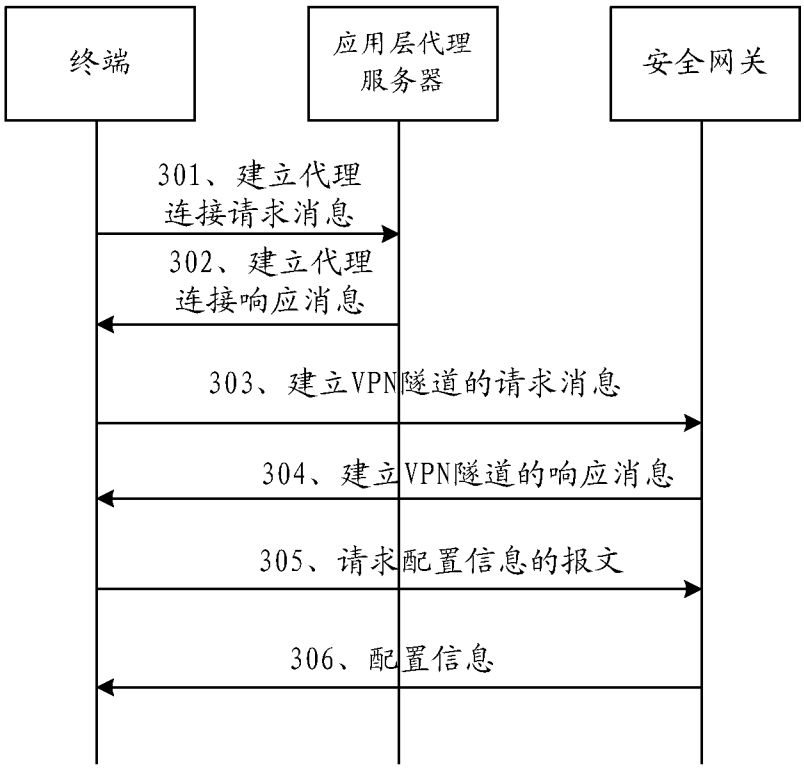
终端
应用层代理服务器
安全网关
301、建立代理连接请求消息
302、建立代理连接响应消息
303、建立VPN隧道的请求消息
304、建立VPN隧道的响应消息
305、请求配置信息的报文
306、配置信息

图 3

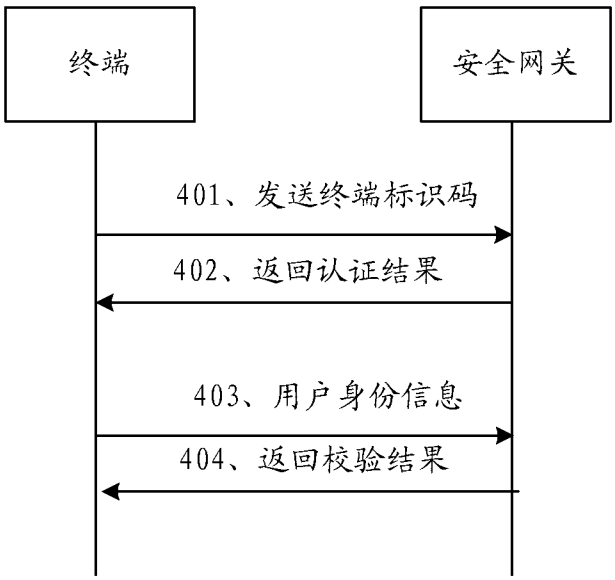
终端
安全网关
401、发送终端标识码
402、返回认证结果
403、用户身份信息
404、返回校验结果

图 4

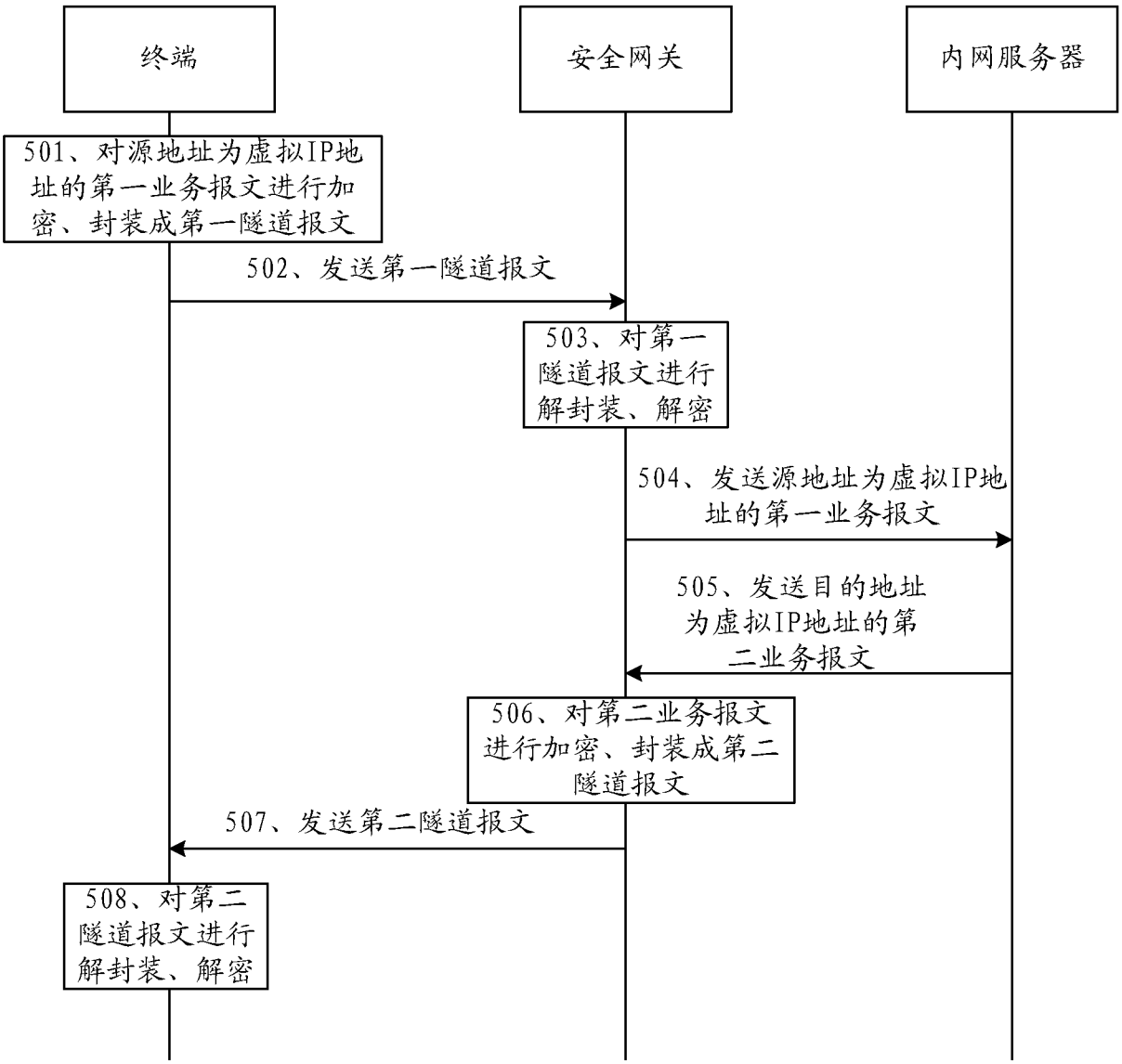
终端
安全网关
内网服务器
501、对源地址为虚拟IP地址的第一业务报文进行加密、封装成第一隧道报文
502、发送第一隧道报文
503、对第一隧道报文进行解封装、解密
504、发送源地址为虚拟IP地址的第一业务报文
505、发送目的地址为虚拟IP地址的第二业务报文
506、对第二业务报文进行加密、封装成第二隧道报文
507、发送第二隧道报文
508、对第二隧道报文进行解封装、解密

图 5

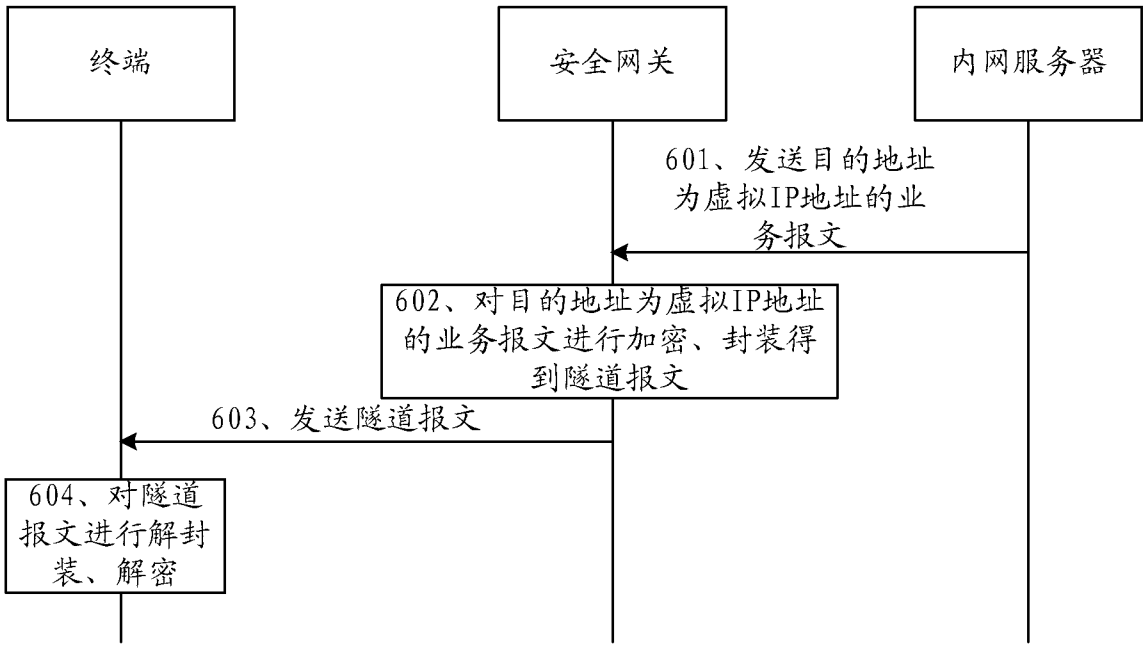
终端
安全网关
内网服务器
601、发送目的地址为虚拟IP地址的业务报文
602、对目的地址为虚拟IP地址的业务报文进行加密、封装得到隧道报文
603、发送隧道报文
604、对隧道报文进行解封装、解密

图 6

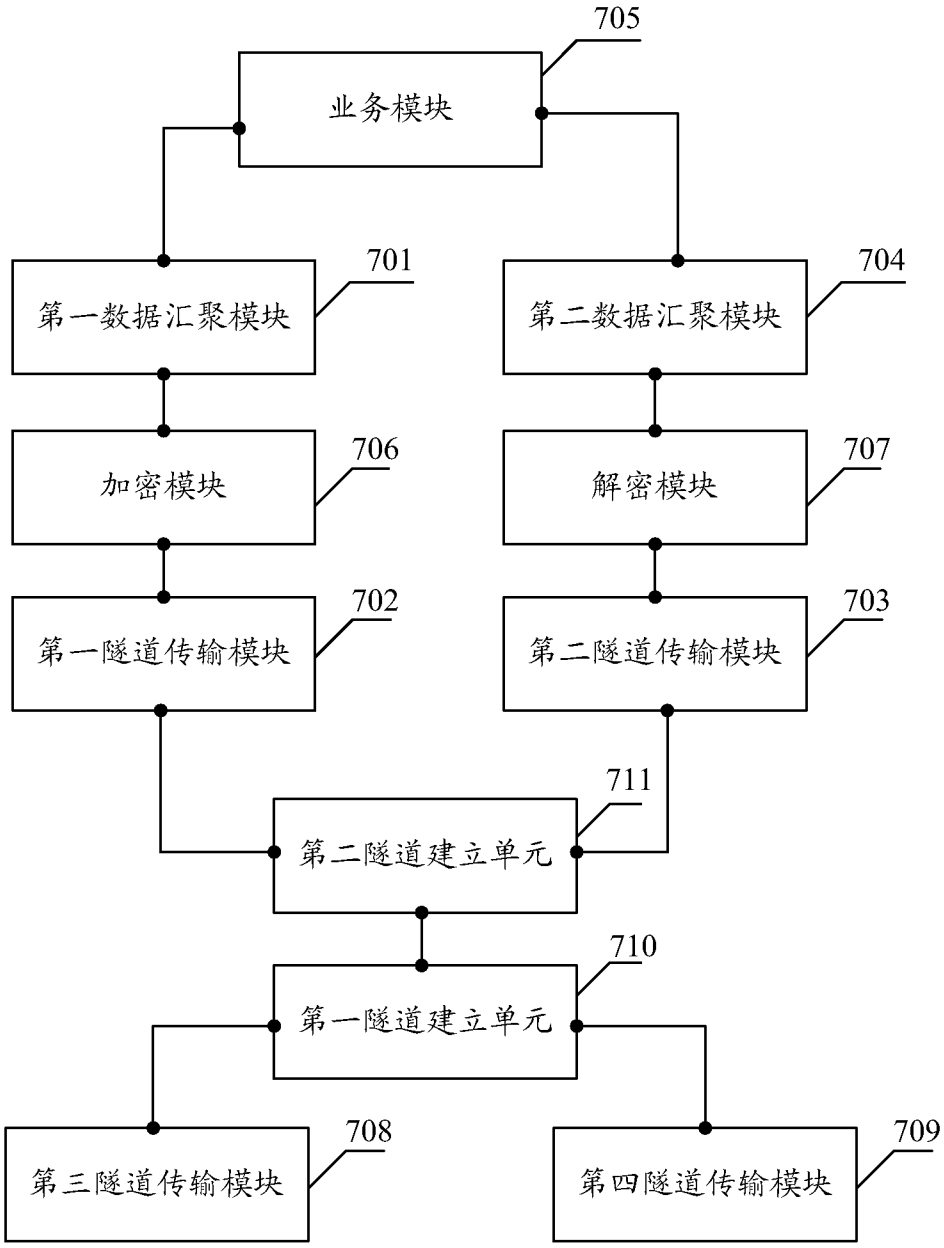
705
业务模块
701
第一数据汇聚模块
704
第二数据汇聚模块
706
加密模块
707
解密模块
702
第一隧道传输模块
703
第二隧道传输模块
711
第二隧道建立单元
710
第一隧道建立单元
708
第三隧道传输模块
709
第四隧道传输模块

图 7

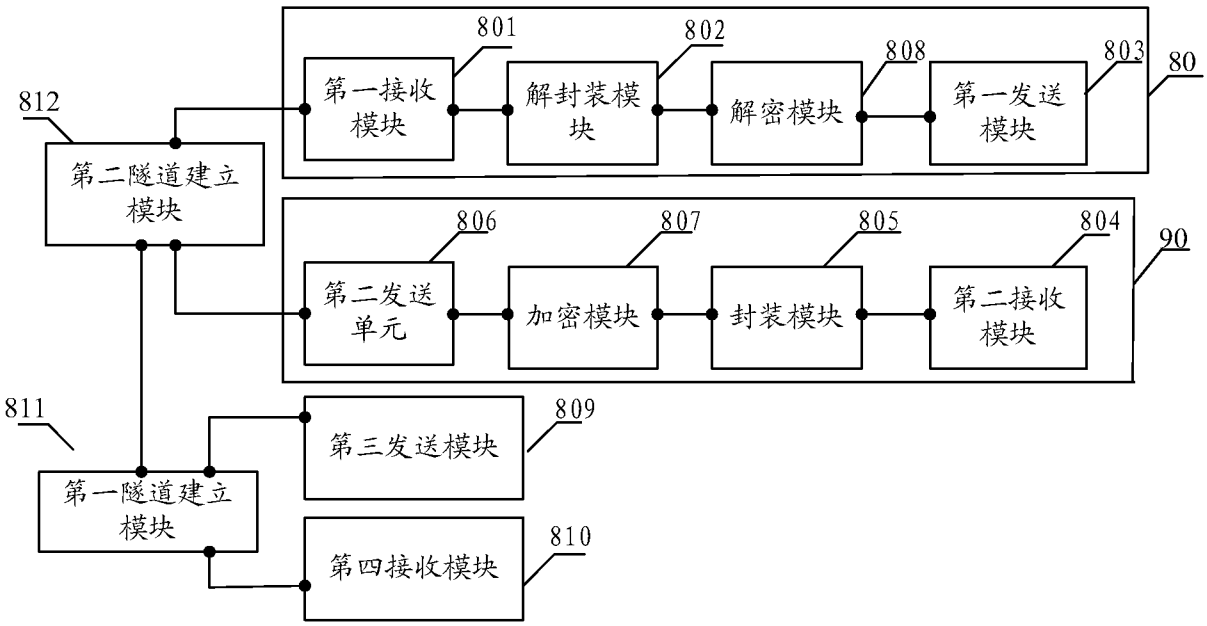
801
802
808
803
80
812
第一接收模块
解封装模块
解密模块
第一发送模块
第二隧道建立模块
806
807
805
804
90
第二发送单元
加密模块
封装模块
第二接收模块
811
809
第三发送模块
第一隧道建立模块
810
第四接收模块

图 8

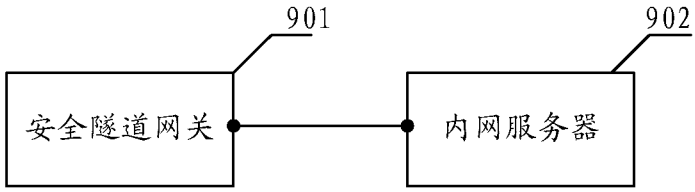
901
902
安全隧道网关
内网服务器

图 9

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2011/071659

A. CLASSIFICATION OF SUBJECT MATTER

H04L12/46(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC:H04L,H04W

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

WPI;EPODOC;CNKI;CNPAT: private network,internal network,IMS,ip multimedia subsystem,source IP,destination IP,source address,destination address,tunnel,traverse,gateway,GW,NAT,address translate,VPN,virtual private network, virtual address

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN101159657A(HUAWEI TECHNOLOGIES CO., LTD.) 09 Apr. 2008（09.04.2008） the whole document	1-20
A	CN101778045A（CHENGDU HUAWEI SYMANTEC TECHNOLOGIES CO., LTD.）14 Jul. 2010（14.07.2010）the whole document	1-20
A	US2003/0108041A1（NORTELL NETWORKS LIMITED）12 Jun. 2003（12.06.2003） the whole document	1-20

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim (S) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&"document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
03 May 2011（03.05.2011）	**23 Jun. 2011 (23.06.2011)**
Name and mailing address of the ISA/CN The State Intellectual Property Office, the P.R.China 6 Xitucheng Rd., Jimen Bridge, Haidian District, Beijing, China 100088 Facsimile No. 86-10-62019451	Authorized officer HE,Xijia Telephone No. (86-10)62413754

Form PCT/ISA /210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2011/071659

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN101159657A	09.04.2008	none	
CN101778045A	14.07.2010	none	
US2003/0108041A1	12.06.2003	CA2412916A1	07.06.2003

国际检索报告

国际申请号
PCT/CN2011/071659

A. 主题的分类

H04L12/46(2006.01)i

按照国际专利分类(IPC)或者同时按照国家分类和 IPC 两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

IPC:H04L,H04W

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用）)

WPI;EPODOC;CNKI;CNPAT:私网，内网，IP 多媒体子系统，源 IP，目的 IP，源地址，目的地址，隧道，穿越，网关，地址转换，虚拟专用网，虚拟地址，private network, internal network, IMS, ip multimedia subsystem, source IP, destination IP, source address, destination address, tunnel, traverse, gateway, GW, NAT, address translate, VPN, virtual private network, virtual address

C. 相关文件

类　型*	引用文件，必要时，指明相关段落	相关的权利要求
A	CN101159657A(华为技术有限公司) 09.4 月 2008（09.04.2008）全文	1-20
A	CN101778045A（成都市华为赛门铁克科技有限公司）14.7 月 2010（14.07.2010）全文	1-20
A	US2003/0108041A1（NORTELL NETWORKS LIMITED）12.6 月 2003（12.06.2003）全文	1-20

☐ 其余文件在 C 栏的续页中列出。　　☒ 见同族专利附件。

* 引用文件的具体类型：

"A" 认为不特别相关的表示了现有技术一般状态的文件

"E" 在国际申请日的当天或之后公布的在先申请或专利

"L" 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

"O" 涉及口头公开、使用、展览或其他方式公开的文件

"P" 公布日先于国际申请日但迟于所要求的优先权日的文件

"T" 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

"X" 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

"Y" 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

"&" 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
03.5 月 2011（03.05.2011）	**23.6 月 2011 (23.06.2011)**
ISA/CN 的名称和邮寄地址： 中华人民共和国国家知识产权局 中国北京市海淀区蓟门桥西土城路 6 号 100088 传真号：　(86-10)62019451	受权官员 贺希佳 电话号码：(86-10) **62413754**

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2011/071659

检索报告中引用的专利文件	公布日期	同族专利	公布日期
CN101159657A	09.04.2008	无	
CN101778045A	14.07.2010	无	
US2003/0108041A1	12.06.2003	CA2412916A1	07.06.2003