(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
2009 年 11 月 5 日 (05.11.2009)

PCT

(10) 国际公布号
WO 2009/132594 A1

(51) 国际专利分类号:
H04L 12/56 (2006.01)

(21) 国际申请号: PCT/CN2009/071586

(22) 国际申请日: 2009 年 4 月 30 日 (30.04.2009)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
200810094439.X 2008 年 4 月 30 日 (30.04.2008) 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]; 中国四川省成都市高新区西部园区清水河片区, Sichuan 611731 (CN)。

(72) 发明人; 及

(75) 发明人/申请人 (仅对美国): **刘利锋 (LIU, Lifeng)** [CN/CN]; 中国广东省深圳市龙岗区坂田华为基地总部办公楼, Guangdong 518129 (CN)。 **黄敏 (HUANG, Min)** [CN/CN]; 中国广东省深圳市龙岗区坂田华为基地总部办公楼, Guangdong 518129 (CN)。 **万适 (WAN, Shi)** [CN/CN]; 中国广东省深圳市龙岗区坂田华为基地总部办公楼, Guangdong 518129 (CN)。

(74) 代理人: **北京中博世达专利商标代理有限公司 (BEIJING ZBSD PATENT & TRADEMARK AGENT LTD.)**; 中国北京市海淀区大柳树路 17 号富海大厦 B 座 501 室, Beijing 100081 (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, 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, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

[见续页]

(54) Title: METHOD AND SYSTEM FOR FORWARDING DATA AMONG PRIVATE NETWORKS

(54) 发明名称: 实现私网之间转发数据的方法和系统

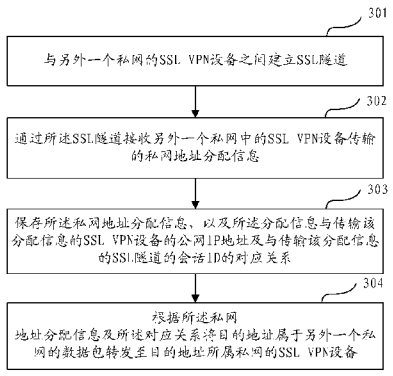

图 3 / FIG. 3

301 SSL CHANNEL IS ESTABLISHED WITH A SSL VPN DEVICE OF ANOTHER PRIVATE NETWORK
302 A PRIVATE ADDRESS ALLOCATING INFORMATION OF THE ANOTHER PRIVATE NETWORK IS RECEIVED VIA THE SSL CHANNEL
303 THE PRIVATE ADDRESS ALLOCATING INFORMATION AND THE CORRESPONDING RELATIONSHIP AMONG THE ADDRESS ALLOCATING INFORMATION, THE PUBLIC NETWORK IP ADDRESS OF THE SSL VPN DEVICE TRANSMITTING THE ALLOCATING INFORMATION AND THE SESSION ID OF THE SSL CHANNEL TRANSMITTING THE ALLOCATING INFORMATION ARE STORED
304 THE DATA PACKAGES WHOSE TARGET ADDRESSES BELONG TO ANOTHER PRIVATE NETWORK ARE FORWARDED TO A SSL VPN DEVICE OF THE PRIVATE NETWORK WHICH THE TARGET ADDRESS BELONGS TO ACCORDING TO THE ADDRESS ALLOCATING INFORMATION AND THE CORRESPONDING RELATIONSHIP

(57) Abstract: A method and system for forwarding data among private networks. The method includes the following steps: a SSL channel is established with a SSL VPN device of another private network; an address allocating information of the another private network is received via the SSL channel; the address allocating information and the corresponding relationship among the address allocating information, the public network IP address of the SSL VPN device transmitting the allocating information and the session ID of the SSL channel transmitting the allocating information are stored; and the data packages whose target addresses belong to another private network are forwarded to a SSL VPN device of the private network which the target address belongs to according to the address allocating information and the corresponding relationship. The method can be used by the SSL VPN device to analyze the private network address of another private network.

[见续页]

WO 2009/132594 A1

(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, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), 欧洲 (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, SE, SI, SK, 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))。

(57) **摘要**:

一种实现私网之间转发数据的方法和系统。方法包括以下步骤：与另外一个私网的 SSL VPN 设备之间建立 SSL 隧道；通过 SSL 隧道接收另外一个私网的地址分配信息；保存所述地址分配信息，以及所述地址分配信息与传输该分配信息的 SSL VPN 设备的公网 IP 地址以及与传输该分配信息的 SSL 隧道的会话 ID 的对应关系；根据所述地址分配信息及所述对应关系将目的地址属于另外一个私网的数据包转发至目的地址所属私网的 SSL VPN 设备。该方法可用于 SSL VPN 设备对其他私网的私网地址的解析。

实现私网之间转发数据的方法和系统

本申请要求了 2008 年 4 月 30 日提交的、申请号为 200810094439.X、发明名称为“实现私网之间转发数据的方法和系统”的中国申请的优先权，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，具体而言是涉及一种共享私网地址分配信息的方法和装置以及实现私网之间转发数据的方法和系统。

背景技术

在全球化的商业环境中，一个大型的跨国企业可能在全世界都有其子公司或是分支机构，如何安全快速的远程访问企业内部资源具有重要意义。基于安全套接层（Secure Socket Layer， SSL)技术的虚拟专用网（Virtual Private Network，VPN）可通过 SSL 来保证用户远程接入网络的安全性，以达到像专用网络一样的数据的安全传输。SSL VPN 技术帮助用户通过标准的 Web 浏览器就可以访问重要的企业应用，使得部门员工出差时不必再携带自己的笔记本电脑，仅仅通过一台接入了 Internet 的计算机就能访问企业资源，这为企业提高效率带来了方便，同时也可以很好的解决安全性问题。

目前很多机构通过公共网络（例如互联网），使用 SSL VPN 设备连接地理或逻辑上分离的分支机构网络，SSL VPN 设备部署在分支机构网络与公共网络边缘，SSL VPN 设备具有可以在公网路由的公网 IP 地址，每个分支机构网络使用私网地址，所有私网地址统一分配，则整个机构的任一分支网络中的 IP 地址与其它分支网络中的 IP 地址是不相同的，这使得所有属于该机构的每个分支机构网络的内部终端“融合”成为一个总体的网络。

对于这样的机构网络，要实现各分支机构私网之间的通信，即要实现分支机构内部终端使用分配的私网地址与其他分支机构网络内部的终端之间转

发数据，由于当前每个分支机构的SSL VPN设备无法解析其他分支机构网络的私网地址，因此无法将待转发的数据封装到相应的SSL隧道，发送至目的地址为其他分支机构网络的SSL VPN设备。要传输私网之间的通信数据，当前采用的方案是向运营商租用专用线路，即专用网（Private Network）。由于专用网仅供租用者使用，因此数据的安全和网络带宽可以得到充分的保证。

但是在实现本发明的过程中，发明人发现现有技术中至少存在如下问题：专用网的部署比较复杂，对现有网络设备和结构的改动较大，因而不能成为一个实用的解决方案。

发明内容

一方面，本发明实施例提供了一种共享私网地址分配信息的方法和装置，能够解决一个私网的SSL VPN设备对其他私网的私网地址进行解析的问题。

本发明实施例提供的一种共享私网地址分配信息的方法，包括：

通过SSL隧道接收另外一个私网的地址分配信息；保存所述地址分配信息，所述地址分配信息用于在接收到数据包时判断所述数据包的目的地址是否属于所述另外一个私网。

本发明实施例提供的一种共享私网地址分配信息的装置，包括：

地址分配信息接收单元，用于通过SSL隧道接收另外一个私网的地址分配信息；地址分配信息保存单元，用于保存所述地址分配信息接收单元接收的地址分配信息，所述地址分配信息用于在接收到数据包时判断所述数据包的目的地址是否属于所述另外一个私网。

由以上技术方案可知，通过SSL隧道接收由另外一个私网中的SSL VPN设备传输的另外一个私网的地址分配信息，并保存所述地址分配信息，使得一个私网的SSL VPN设备获知了另外一个私网私有地址的分配信息，这样在接收到数据包时能够根据该地址分配信息判断该数据包的目的地址是否属于所述另外一个私网，因此能够实现一个私网的SSL VPN设备对其他私网的私网地址的解析。

另一方面，本发明实施例提供了一种实现私网之间转发数据的方法和系统，能够解决不同私网内的终端使用私网地址进行安全通信的问题。

本发明实施例提供的一种实现私网之间转发数据的方法，包括:

与另外一个私网的SSL VPN设备之间建立SSL隧道；通过所述SSL隧道接收另外一个私网的地址分配信息，所述地址分配信息由所述另外一个私网中的SSL VPN设备通过所述SSL隧道传输；保存所述地址分配信息，以及所述地址分配信息与传输该分配信息的SSL VPN设备的公网IP地址及与传输该分配信息的SSL隧道的会话ID的对应关系；根据所述地址分配信息及所述对应关系将目的地址属于另外一个私网的数据包转发至目的地址所属私网的SSL VPN设备。

本发明实施例提供的一种实现私网之间转发数据的系统，包括两个或两个以上私网，所述每个私网分别通过分配有公网IP地址的SSL VPN设备接入到公网，所述每个SSL VPN设备包括：SSL隧道建立单元，用于与另外一个私网的SSL VPN设备之间建立SSL隧道；地址分配信息接收单元，用于通过所述SSL隧道建立单元建立的SSL隧道接收另外一个私网的地址分配信息，所述地址分配信息由所述另外一个私网中的SSL VPN设备通过所述SSL隧道传输；保存单元，用于保存所述地址分配信息接收单元接收的地址分配信息，以及所述地址分配信息与传输该分配信息的SSL VPN设备的公网IP地址及与传输该分配信息的SSL隧道的会话ID的对应关系；数据包转发单元，用于根据所述保存单元保存的所述地址分配信息及所述对应关系，将目的地址属于另外一个私网的数据包转发至目的地址所属私网的SSL VPN设备。

由以上技术方案可知，通过与另外一个私网的SSL VPN设备建立SSL隧道，接收另外一个私网中的SSL VPN设备通过所述SSL隧道传输的所述另外一个私网的地址分配信息，并保存所述地址分配信息，使得一个私网的SSL VPN设备拥有了另外一个私网私有地址的分配信息；通过保存所述地址分配信息与传输该分配信息的SSL VPN设备的公网IP地址及与传输该分配信息的SSL

隧道的会话ID的对应关系，对于一个源地址为私网地址，目的地址为另一个私网的私有IP地址的数据包，通过所述地址分配信息查询该对应关系，得到与公网IP地址对应的SSL VPN设备以及与会话ID对应的SSL隧道，从而能够将该数据包转发至查询到的SSL VPN设备，因此解决了不同私网内的终端使用私网地址进行安全通信的问题。

附图说明

为了更清楚地说明本发明实施例的技术方案，下面将对实施例中所需要使用的附图作一简单地介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动性的前提下，还可以根据这些附图获得其他的附图。

图 1 为本发明实施例一提供的共享私网地址分配信息的方法的流程图；

图 2 为本发明实施例二提供的共享私网地址分配信息的装置的结构图；

图 3 为本发明实施例三提供的实现私网之间转发数据的方法的流程图；

图 4 为本发明实施例三中由 SSL VPN 设备转发数据操作的流程图；

图 5 为本发明实施例三中确定与会话 ID 对应的 SSL 隧道操作的流程图；

图 6 为本发明实施例四提供的实现私网之间转发数据的系统中每个 SSL VPN 设备的结构图；

图 7 为本发明实施例四中数据包转发单元的结构图；

图 8 为本发明实施例五提供的一个具体实施例的网络示意图。

具体实施方式

下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

实施例一

参见图 1，本发明实施例一提供的共享私网地址分配信息的方法，包括:

步骤 101，一个私网的 SSL VPN 设备通过 SSL 隧道接收另外一个私网的地址分配信息;

所述地址分配信息由另外一个私网的 SSL VPN 设备通过所述 SSL 隧道传输。

步骤 102，保存所述地址分配信息，所述地址分配信息用于在接收到数据包时判断所述数据包的目的地址是否属于所述另外一个私网。

步骤 103，保存所述地址分配信息与传输该地址分配信息的 SSL VPN 设备的公网 IP 地址及与传输该地址分配信息的 SSL 隧道的会话 ID 的对应关系。

实施例二

在本发明实施例一提供的方法基础上，本发明实施例二提供了一种共享私网地址分配信息的装置，如图 2 所示，包括:

地址分配信息接收单元 201，用于一个私网的 SSL VPN 设备通过 SSL 隧道接收另外一个私网的地址分配信息；所述地址分配信息由所述另外一个私网中的 SSL VPN 设备通过所述 SSL 隧道传输。

地址分配信息保存单元 202，用于保存所述地址分配信息，所述地址分配信息用于在该 SSL VPN 接收到数据包时判断所述数据包的目的地址是否属于所述另外一个私网。

对应关系保存单元 203，用于保存所述地址分配信息与传输该地址分配信息的 SSL VPN 设备的公网 IP 地址及与传输该地址分配信息的 SSL 隧道的会话 ID 的对应关系。

所述装置可以部署在现有的 SSL VPN 设备上，使得 SSL VPN 设备拥有其它私网逻辑拓扑的能力，即拥有可以解析其它私网的私网地址的能力。

由以上实施例可知，一个私网的 SSL VPN 设备通过 SSL 隧道接收由另外一个私网中的 SSL VPN 设备传输的另外一个私网的地址分配信息，并保存所述地址分配信息，使得该私网的 SSL VPN 设备拥有了另外一个私网的私有地

址分配信息，这样在接收到数据包时就能够根据该地址分配信息判断该数据包的目的地址是否属于所述另外一个私网，因此实现了一个私网的 SSL VPN 设备对其他私网的私网地址的解析。

实施例三

如图 3 所示，本发明实施例三提供的实现私网之间转发数据的方法，包括:

步骤 301，一个私网的 SSL VPN 设备与另外一个私网的 SSL VPN 设备之间建立 SSL 隧道;

在本步骤中，建立的 SSL 隧道对应一个会话 ID，所述会话 ID 用于唯一标识建立的 SSL 连接。在 SSL VPN 设备可能存在多个 SSL 连接、建立多个 SSL 隧道的情况下，会话 ID 用以确定 SSL VPN 设备间通过公网转发数据时使用哪个 SSL 隧道传输。

步骤 302，通过所述 SSL 隧道接收另外一个私网的地址分配信息，所述地址分配信息由所述另外一个私网中的 SSL VPN 设备通过所述 SSL 隧道传输;

在本步骤中，还包括通过所述 SSL 隧道请求另外一个私网的地址分配信息的步骤。

步骤 303，保存所述地址分配信息，以及所述地址分配信息与传输该分配信息的 SSL VPN 设备的公网 IP 地址的及与传输该分配信息的 SSL 隧道的会话 ID 对应关系。

步骤 304，根据所述地址分配信息及所述对应关系，将目的地址属于另外一个私网的数据包转发至目的地址所属私网的 SSL VPN 设备。

如图 4 所示，本步骤具体包括:

步骤 401，接收目的地址为另外一个私网终端的 IP 数据包。

由于目的地址为另外一个私网终端，因此该 IP 数据包将首先发往本私网的 SSL VPN 设备。

步骤 402，根据该 IP 数据包的目的地址所属网段确定另外一个私网对应的地址分配信息。

本私网的 SSL VNP 设备在接收到该 IP 数据包后，对目的地址所属的网段进行判断，从而确定该 IP 数据包应发往的私网对应的地址分配信息。

步骤 403，根据所述地址分配信息查询所述对应关系，确定与公网 IP 地址对应的传输该地址分配信息的 SSL VPN 设备，以及与会话 ID 对应的 SSL 隧道。

通过查询对应关系中，所述地址分配信息与传输该地址分配信息的 SSL VPN 设备的公网 IP 地址的对应关系及所述地址分配信息与传输该地址分配信息的 SSL 隧道的会话 ID 的对应关系，确定该 IP 数据包要发往的 SSL VPN 设备及要通过的 SSL 隧道。

在确定与会话 ID 对应的 SSL 隧道步骤中，如图 5 所示，具体包括:

步骤 501，根据会话 ID 查询 SSL 隧道的状态;

步骤 502，判断 SSL 隧道是否失效?

步骤 503，如果 SSL 隧道可用，则确定该 SSL 隧道为与会话 ID 对应的 SSL 隧道;

步骤 504，如果 SSL 隧道失效，则根据会话 ID 向所述确定的 SSL VPN 设备请求恢复该 SSL 隧道;

步骤 505，判断 SSL 隧道是否恢复成功?

步骤 506，如果恢复成功，确定该恢复的 SSL 隧道为与会话 ID 对应的 SSL 隧道;

步骤 507，如果恢复失败，则由本私网的 SSL VPN 设备向所述确定的 SSL VPN 设备请求建立新隧道，并用一个新的会话 ID 唯一标识新建立的 SSL 隧道，替换保存的会话 ID，由新的会话 ID 确定新建立的 SSL 隧道。

通过以上步骤，能够确保查询得到一条有效的 SSL 隧道，然后封装所述 IP 数据包后通过以上步骤确定的所述 SSL 隧道转发至所述 SSL VPN 设备，实

现 SSL VPN 设备之间的数据转发。

SSL VPN 设备之间通过在公网中建立 SSL 隧道进行数据传输时，为保证数据传输的安全性，需要对 IP 数据包进行封装和解封装。这个过程具体包括：认证用户和服务器，以确保数据发送到正确的客户机和服务器；加密数据以防止数据中途被窃取；维护数据的完整性，确保数据在传输过程中不被改变。

在目的地址所属私网的 SSL VPN 设备通过 SSL 隧道接收到由其他私网的 SSL VPN 设备转发的数据包后，解封装得到 IP 数据包；判断该 IP 数据包的目的地址所属的网段与本私网的网段是否属于同一网段，如果是，则重新封装该 IP 数据包二层报头后向内网中的该目的地址转发该数据包；如果否，则再由本私网的 SSL VPN 设备查找保存的其他私网的地址分配信息及对应关系，并将目的地址属于另外一个私网的数据包转发至目的地址所属私网的 SSL VPN 设备。

对于目的地址终端响应源地址终端的数据包，则以源终端的地址为目的地址，本目的地址作为源地址，其数据转发过程同于步骤 304。

对于存在多个私网和多个 SSL VPN 设备的情况，每两个私网内的终端使用私网地址进行通信的步骤都同于步骤 304。

实施例四

在本发明实施例三提供的实现私网之间转发数据的方法的基础上，如图 6 所示，本发明实施例四提供了一种实现私网之间转发数据的系统，包括两个或两个以上私网，所述每个私网分别通过分配有公网 IP 地址的 SSL VPN 设备接入到公网，所述每个 SSL VPN 设备包括：

SSL 隧道建立单元 601，用于与另外一个私网的 SSL VPN 设备之间建立 SSL 隧道；

所述 SSL 隧道对应一个会话 ID，会话 ID 用于唯一标识建立的 SSL 连接。在 SSL VPN 设备可能存在多个 SSL 连接、建立多个 SSL 隧道的情况下，会话 ID 用以确定 SSL VPN 设备间通过公网转发数据时使用哪个 SSL 隧道传输。

地址分配信息接收单元 602，用于通过所述 SSL 隧道接收另外一个私网的地址分配信息，所述地址分配信息由所述另外一个私网中的 SSL VPN 设备通过所述 SSL 隧道传输。

保存单元 603，用于保存所述地址分配信息，以及所述地址分配信息与传输该分配信息的 SSL VPN 设备的公网 IP 地址及与传输该分配信息的 SSL 隧道的会话 ID 的对应关系。

数据包转发单元 604，用于根据所述地址分配信息及所述对应关系，将目的地址属于另外一个私网的数据包转发至目的地址所属私网的 SSL VPN 设备。

其中，如图 7 所示，所述数据包转发单元 604 具体包括:

数据包接收模块 701，用于接收目的地址为另外一个私网终端的 IP 数据包;

地址分配信息确定模块 702，用于根据该 IP 数据包的目的地址所属网段确定另外一个私网对应的地址分配信息;

对应关系确定模块 703，用于根据所述地址分配信息查询所述对应关系，确定与公网 IP 地址对应的传输该地址分配信息的 SSL VPN 设备，以及与会话 ID 对应的 SSL 隧道。

所述对应关系确定模块 703，具体包括:

SSL VPN 设备确定子模块 7032，用于根据所述地址分配信息查询所述对应关系，确定与公网 IP 地址对应的传输该地址分配信息的 SSL VPN 设备;

SSL 隧道确定子模块 7034，用于根据所述地址分配信息查询所述对应关系，确定与会话 ID 对应的 SSL 隧道，该子模块 7034 首先根据会话 ID 查询 SSL 隧道的状态，如果 SSL 隧道可用，则确定该 SSL 隧道为与会话 ID 对应的 SSL 隧道；如果 SSL 隧道失效，则根据会话 ID 向所述确定的 SSL VPN 设备请求恢复该 SSL 隧道，确定该恢复的 SSL 隧道为与会话 ID 对应的 SSL 隧道；如果恢复失败，则由本私网的 SSL VPN 设备向所述确定的 SSL VPN 设备

请求建立新隧道，并用一个新的会话 ID 唯一标识新建立的 SSL 隧道，替换保存的会话 ID，由新的会话 ID 确定新建立的 SSL 隧道。

SSL 隧道确定子模块 7034 能够确保查询得到一条有效的 SSL 隧道，然后封装所述 IP 数据包后通过以上步骤确定的所述 SSL 隧道转发至所述 SSL VPN 设备，实现 SSL VPN 设备之间的数据转发。

数据包发送模块 704，用于封装所述 IP 数据包后通过所述 SSL 隧道发送至所述 SSL VPN 设备。

由以上技术方案可知，通过与另外一个私网的 SSL VPN 设备建立 SSL 隧道接收另外一个私网的地址分配信息，并保存所述地址分配信息，使得一个私网的 SSL VPN 设备拥有了另外一个私网私有地址的分配信息；通过保存所述地址分配信息与传输该分配信息的 SSL VPN 设备的公网 IP 地址及与传输该分配信息的 SSL 隧道的会话 ID 的对应关系，对于一个使用私网地址发往另外一个私网终端的数据包，通过所述地址分配信息查询该对应关系，得到与公网 IP 地址对应的 SSL VPN 设备以及与会话 ID 对应的 SSL 隧道，从而能够将该数据包转发至查询到的 SSL VPN 设备，从而解决了不同私网内的终端使用私网地址进行安全通信的问题。

实施例五

下面以一个具体的实施例对本发明的技术方案进行说明，如图 8 所示，为本发明实施例五提供的一种实现私网之间通信的网络示意图：

在本实施例中，整个机构网络内部使用 10.0.0.0/8 的私网地址，私网地址统一分配，包括三个分支机构网络：A 分支机构网络（简称 A 网络），分配的 IP 地址段为 10.1.0.0/16；B 分支机构网络（简称 B 网络），分配的 IP 地址段为 10.2.0.0/16； C 分支机构网络（简称 C 网络），分配的地址段为 10.3.0.0/16。各个分支机构网络与公共网络的边缘分别部署 SSL VPN 设备，设备具有可以在公网路由的公网 IP 地址：A 网络中的 SSL VPN 设备（简称 A 设备），公网 IP 地址为 20.1.1.10；B 网络中的 SSL VPN 设备（简称 B 设备），公网 IP 地址

为 30.1.1.10; 和 C 网络中的 SSL VPN 设备（简称 C 设备），公网 IP 地址为 40.1.1.10。各 SSL VPN 设备之间建立 SSL 隧道，用于传输分支机构网络之间的通信数据。

对于 A 网络中一台 IP 地址为 10.1.0.2/16 的终端（简称 A 终端）需要和 B 网络中一台 IP 地址为 10.2.0.2/16 的终端（简称 B 终端）通信，需要经过以下通信步骤:

1、A 网络中的 SSL VPN 设备（A 设备）和 B 网络中的 SSL VPN 设备（B 设备）建立 SSL 的点对点（site-to-site）隧道，并且该隧道唯一对应一个会话 ID;

2、A 设备通过 SSL 隧道接收 B 设备发送的 B 网络的地址分配信息，即 10.2.0.0/16，A 设备记录该地址分配信息，并与该传输该分配信息的源地址（即 B 设备的公网 IP 地址 30.1.1.10）以及传输该信息的 SSL 隧道的会话 ID 绑定，保存 B 网络的地址分配信息与 B 设备的公网 IP 地址及会话 ID 的对应关系;

3、B 设备通过 SSL 隧道接收 A 设备发送的 A 网络的地址分配信息，即 10.1.0.0/16，B 设备记录该地址分配信息，并与该传输该分配信息的源地址（即 A 设备的公网 IP 地址 20.1.1.10）以及传输该信息的 SSL 隧道的会话 ID 绑定，保存 A 网络的地址分配信息与 A 设备的公网 IP 地址及会话 ID 的对应关系;

其中步骤 2 与步骤 3 可以同时进行。

4、A 终端与 B 终端通信，由 A 终端发出一个目的地址为 B 终端地址（10.2.0.2/16）、源地址为 A 终端地址（10.1.0.2/16）的 IP 数据包。由于目的地址不属于 A 网络，因此，该数据包会发往 A 设备;

5、A 设备得到该 IP 数据包后，判断目的地址 10.2.0.2/16 发现该目的地址属于 10.2.0.0/16 网段，通过查询步骤 2 保存的对应关系，得知该网段对应公网 IP 地址为 30.1.1.10 的 B 设备，并根据保存的对应关系中的会话 ID 确定 A 设备与 B 设备进行通信的 SSL 隧道，因此 A 设备将该 IP 数据包作为负载进行封装后，通过 A 设备和 B 设备之间的 SSL 隧道传输至 B 设备;

在根据保存的对应关系中的会话ID确定A设备与B设备进行通信的SSL隧道中，首先根据会话ID查询SSL隧道的状态，如果SSL隧道可用，则确定该SSL隧道；如果SSL隧道失效，则根据会话ID向B设备请求恢复该SSL隧道；如果恢复失败，则由A设备向B设备请求建立新隧道，并用一个新的会话ID唯一标识新建立的SSL隧道，替换保存的会话ID，由新的会话ID确定新建立的SSL隧道。

6、B设备从SSL连接中接收A设备传输的数据包，解封装得到IP数据包，判断目的地址20.1.0.2所属的网段与本设备所连接的分支机构的网段属于同一网段，则重新封装该IP数据包的二层报头后向内网转发数据包；

7、 B终端响应A终端的数据包是以A终端的地址（10.1.0.2）为目的地址，B 终端的地址（10.2.0.2）为源地址，因此响应数据包的传输过程与上述步骤4、5、6类似。

另外A网和C网、B网和C网内终端之间的通信步骤也和上述步骤一致。

可以理解的是，以上对本发明所提供的一种共享私网地址分配信息的方法和装置以及实现私网之间转发数据的方法和系统进行了详细介绍，可广泛应用在由地理或逻辑上隔离的多个分支机构网络组成、各个分支机构的网络使用统一分配的私网地址通过公共网络互连的整个机构网络中，使得每个分支机构内部终端使用分配的私网地址即可与其它分支机构网络内的终端进行安全方便的通信。

最后需要说明的是，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一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（ROM）或随机存储记忆体（RAM）等。

本发明实施例中的各功能单元可以集成在一个处理模块中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个模块中。上述

集成的模块既可以采用硬件的形式实现，也可以采用软件功能模块的形式实现。所述集成的模块如果以软件功能模块的形式实现并作为独立的产品销售或使用时，也可以存储在一个计算机可读取存储介质中。上述提到的存储介质可以是只读存储器，磁盘或光盘等。

上述具体实施例并不用以限制本发明，对于本技术领域的普通技术人员来说，凡在不脱离本发明原理的前提下，所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

权 利 要 求 书

1、一种共享私网地址分配信息的方法，包括以下步骤:

通过 SSL 隧道接收另外一个私网的地址分配信息;

保存所述地址分配信息，所述地址分配信息用于在接收到数据包时判断所述数据包的目的地址是否属于所述另外一个私网。

2、根据权利要求 1 所述的共享私网地址分配信息的方法，其特征在于，所述方法还包括步骤:

保存所述地址分配信息与传输该地址分配信息的 SSL VPN 设备的公网 IP 地址及与传输该地址分配信息的 SSL 隧道的会话 ID 的对应关系。

3、一种共享私网地址分配信息的装置，其特征在于，包括:

地址分配信息接收单元，用于通过 SSL 隧道接收另外一个私网的地址分配信息;

地址分配信息保存单元，用于保存所述地址分配信息接收单元接收的地址分配信息，所述地址分配信息用于在接收到数据包时判断所述数据包的目的地址是否属于所述另外一个私网。

4、根据权利要求 3 所述的共享私网地址分配信息的装置，其特征在于，所述装置还包括:

对应关系保存单元，用于保存所述地址分配信息与传输该地址分配信息的 SSL VPN 设备的公网 IP 地址及与传输该地址分配信息的 SSL 隧道的会话 ID 的对应关系。

5、一种实现私网之间转发数据的方法，包括以下步骤:

与另外一个私网的 SSL VPN 设备之间建立 SSL 隧道;

通过所述 SSL 隧道接收另外一个私网的地址分配信息，所述地址分配信息由所述另外一个私网中的 SSL VPN 设备通过所述 SSL 隧道传输;

保存所述地址分配信息，以及所述地址分配信息与传输该分配信息的 SSL VPN 设备的公网 IP 地址及与传输该分配信息的 SSL 隧道的会话 ID 的对应关系;

根据所述地址分配信息及所述对应关系将目的地址属于另外一个私网的数据包转发至目的地址所属私网的 SSL VPN 设备。

6、根据权利要求 5 所述的实现私网之间转发数据的方法，其特征在于，根据所述地址分配信息及所述对应关系将目的地址属于另外一个私网的数据包转发至目的地址所属私网的 SSL VPN 设备的步骤具体为:

接收目的地址为另外一个私网终端的 IP 数据包;

根据该 IP 数据包的目的地址所属网段确定另外一个私网对应的地址分配信息;

根据所述地址分配信息查询所述对应关系，确定与公网 IP 地址对应的传输该地址分配信息的 SSL VPN 设备，以及与会话 ID 对应的 SSL 隧道;

通过所述确定的 SSL 隧道将所述 IP 数据包封装后转发至所述确定的 SSL VPN 设备。

7、根据权利要求 6 所述的实现私网之间转发数据的方法，其特征在于，所述确定与会话 ID 对应的 SSL 隧道的步骤具体为:

根据会话 ID 查询 SSL 隧道的状态;

如果 SSL 隧道可用，则确定该 SSL 隧道为与会话 ID 对应的 SSL 隧道;

如果 SSL 隧道失效，则根据会话 ID 向所述确定的 SSL VPN 设备请求恢复该 SSL 隧道，确定该恢复的 SSL 隧道为与会话 ID 对应的 SSL 隧道;

如果恢复失败，则由本私网的 SSL VPN 设备向所述确定的 SSL VPN 设备请求建立新隧道，并用一个新的会话 ID 唯一标识新建立的 SSL 隧道，替换保存的会话 ID，由新的会话 ID 确定新建立的 SSL 隧道。

8、一种实现私网之间转发数据的系统，其特征在于，包括两个或两个以上私网，所述每个私网分别通过分配有公网 IP 地址的 SSL VPN 设备接入到公网，所述每个 SSL VPN 设备包括:

SSL 隧道建立单元，用于与另外一个私网的 SSL VPN 设备之间建立 SSL 隧道;

地址分配信息接收单元，用于通过所述 SSL 隧道建立单元建立的 SSL 隧道接收另外一个私网的地址分配信息，所述地址分配信息由所述另外一个私网中的 SSL VPN 设备通过所述 SSL 隧道传输;

保存单元，用于保存所述地址分配信息接收单元接收的地址分配信息，以及所述地址分配信息与传输该分配信息的 SSL VPN 设备的公网 IP 地址及与传输该分配信息的 SSL 隧道的会话 ID 的对应关系;

数据包转发单元，用于根据所述保存单元保存的地址分配信息及所述对应关系将目的地址属于另外一个私网的数据包转发至目的地址所属私网的 SSL VPN 设备。

9、根据权利要求 8 所述的实现私网之间转发数据的系统，其特征在于，所述数据包转发单元具体包括:

数据包接收模块，用于接收目的地址为另外一个私网终端的 IP 数据包;

地址分配信息确定模块，用于根据该 IP 数据包的目的地址所属网段确定另外一个私网对应的地址分配信息;

对应关系确定模块，用于根据所述地址分配信息查询所述对应关系，确定与公网 IP 地址对应的传输该地址分配信息的 SSL VPN 设备，以及与会话 ID 对应的 SSL 隧道;

数据包发送模块，用于通过所述确定的 SSL 隧道将所述 IP 数据包封装后转发至所述确定的 SSL VPN 设备。

10、根据权利要求 9 所述的实现私网之间转发数据的系统，其特征在于，所述对应关系确定模块进一步包括:

SSL VPN 设备确定子模块，用于根据所述地址分配信息查询所述对应关系，确定与公网 IP 地址对应的传输该地址分配信息的 SSL VPN 设备;

SSL 隧道确定子模块，用于根据所述地址分配信息查询所述对应关系，确定与会话 ID 对应的 SSL 隧道，所述 SSL 隧道确定子模块首先根据会话 ID 查询 SSL 隧道的状态，如果 SSL 隧道可用，则确定该 SSL 隧道为与会话 ID 对应的

SSL 隧道；如果 SSL 隧道失效，则根据会话 ID 向所述确定的 SSL VPN 设备请求恢复该 SSL 隧道，确定该恢复的 SSL 隧道为与会话 ID 对应的 SSL 隧道；如果恢复失败，则由本私网的 SSL VPN 设备向所述确定的 SSL VPN 设备请求建立新隧道，并用一个新的会话 ID 唯一标识新建立的 SSL 隧道，替换保存的会话 ID，由新的会话 ID 确定新建立的 SSL 隧道。

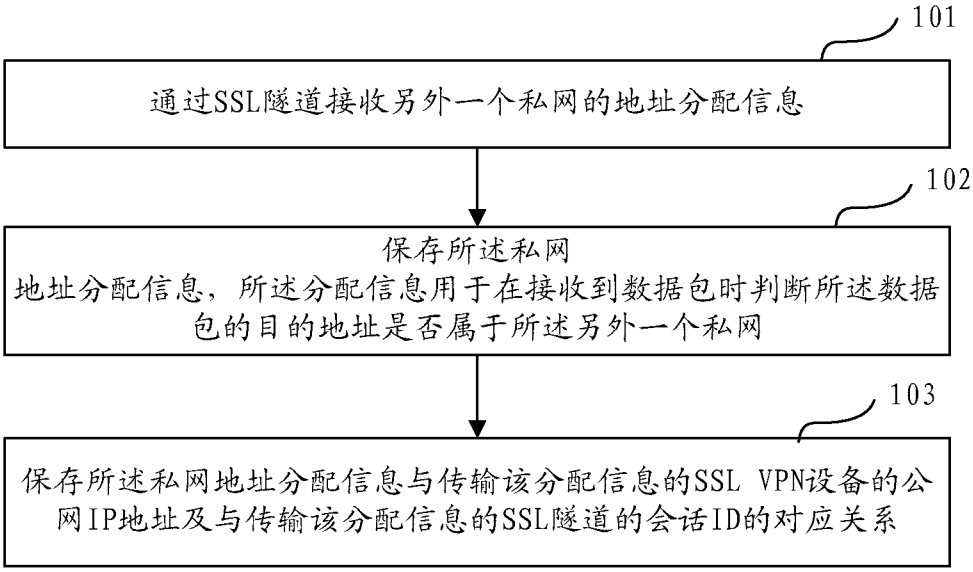
101
通过SSL隧道接收另外一个私网的地址分配信息
102
保存所述私网
地址分配信息，所述分配信息用于在接收到数据包时判断所述数据包的目的地址是否属于所述另外一个私网
103
保存所述私网地址分配信息与传输该分配信息的SSL VPN设备的公网IP地址及与传输该分配信息的SSL隧道的会话ID的对应关系

图 1

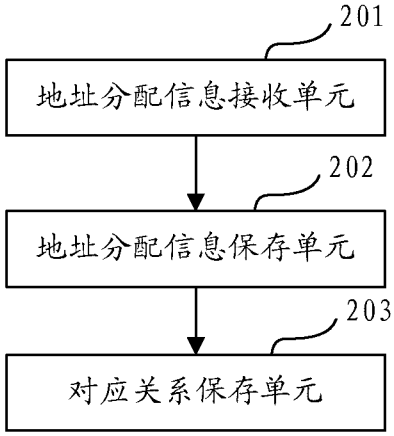
201
地址分配信息接收单元
202
地址分配信息保存单元
203
对应关系保存单元

图 2

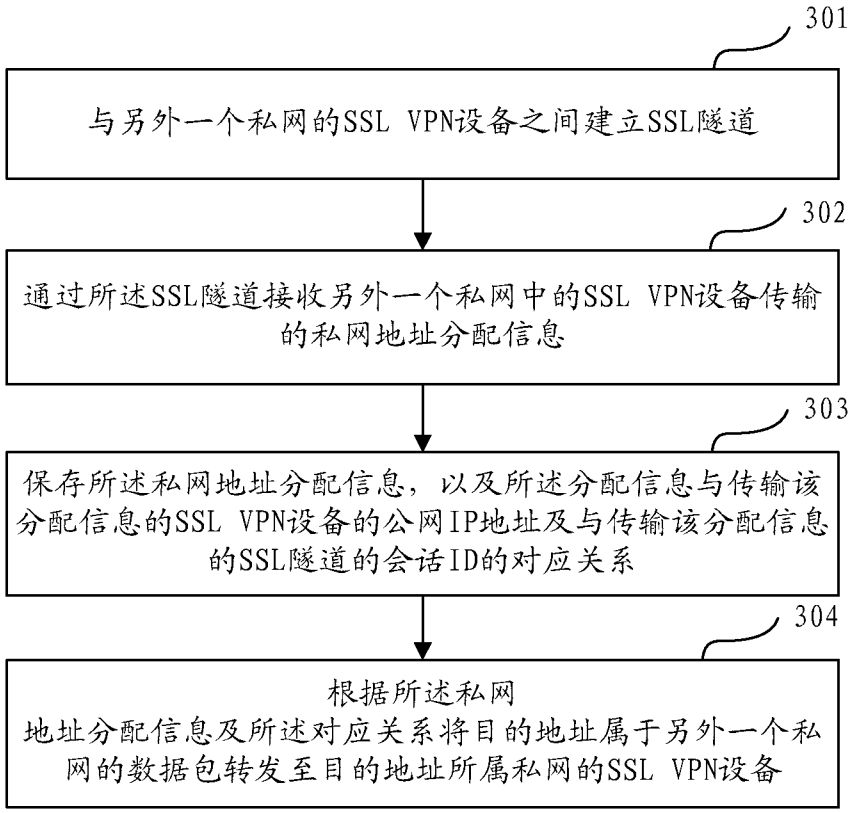
301
与另外一个私网的SSL VPN设备之间建立SSL隧道
302
通过所述SSL隧道接收另外一个私网中的SSL VPN设备传输的私网地址分配信息
303
保存所述私网地址分配信息，以及所述分配信息与传输该分配信息的SSL VPN设备的公网IP地址及与传输该分配信息的SSL隧道的会话ID的对应关系
304
根据所述私网
地址分配信息及所述对应关系将目的地址属于另外一个私网的数据包转发至目的地址所属私网的SSL VPN设备

图 3

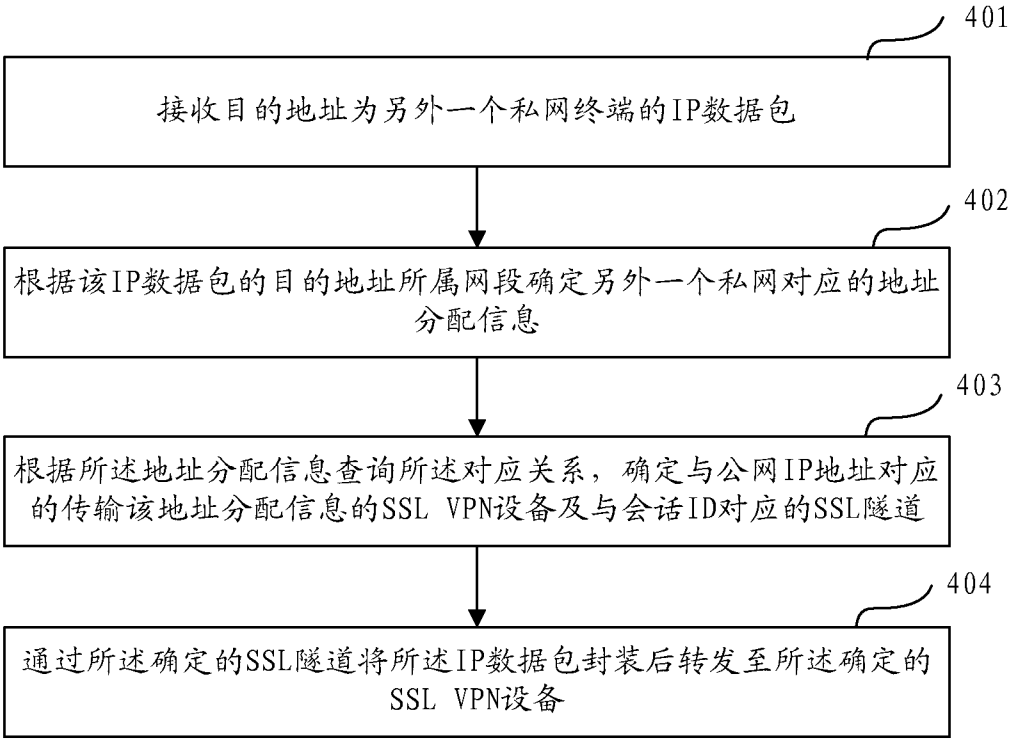
401
接收目的地址为另外一个私网终端的IP数据包
402
根据该IP数据包的目的地址所属网段确定另外一个私网对应的地址分配信息
403
根据所述地址分配信息查询所述对应关系，确定与公网IP地址对应的传输该地址分配信息的SSL VPN设备及与会话ID对应的SSL隧道
404
通过所述确定的SSL隧道将所述IP数据包封装后转发至所述确定的SSL VPN设备

图 4

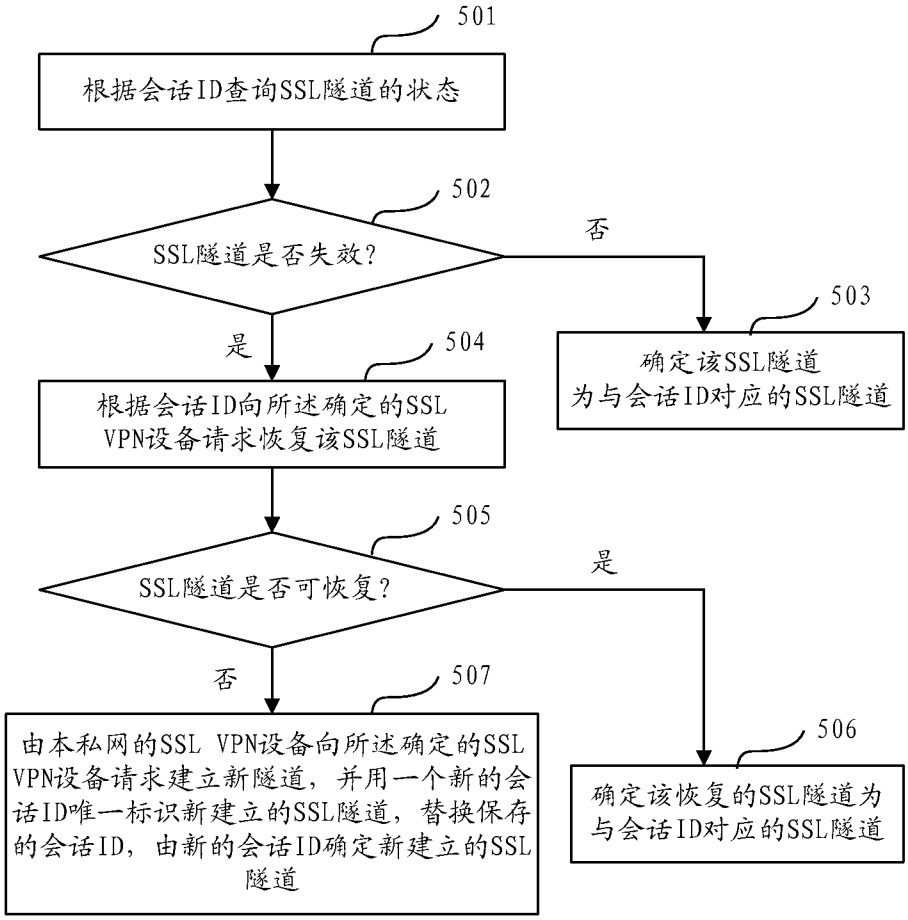
501
根据会话ID查询SSL隧道的状态
502
SSL隧道是否失效?
否
503
确定该SSL隧道
为与会话ID对应的SSL隧道
是
504
根据会话ID向所述确定的SSL
VPN设备请求恢复该SSL隧道
505
SSL隧道是否可恢复?
是
否
507
由本私网的SSL VPN设备向所述确定的SSL
VPN设备请求建立新隧道，并用一个新的会
话ID唯一标识新建立的SSL隧道，替换保存
的会话ID，由新的会话ID确定新建立的SSL
隧道
506
确定该恢复的SSL隧道为
与会话ID对应的SSL隧道

图 5

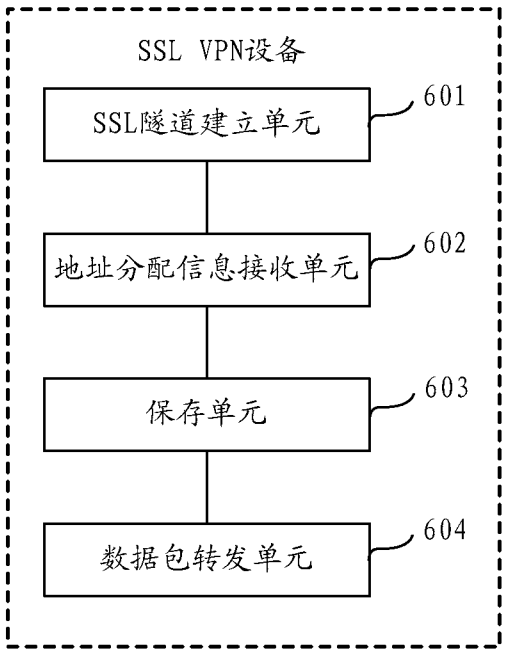
SSL VPN设备
SSL隧道建立单元
601
地址分配信息接收单元
602
保存单元
603
数据包转发单元
604

图 6

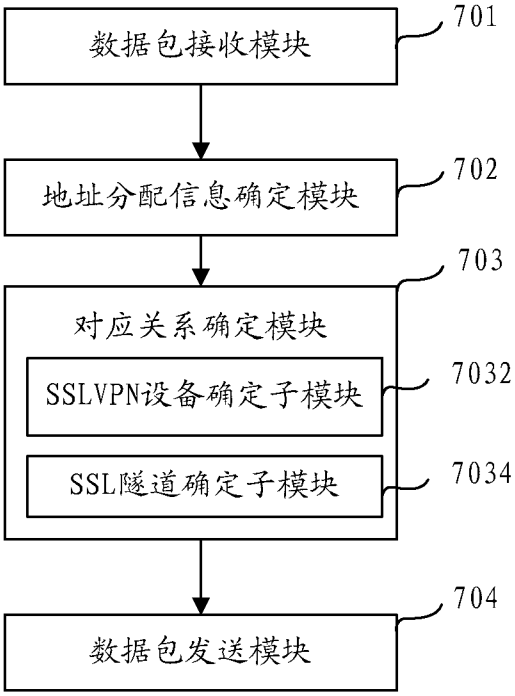
数据包接收模块
701
地址分配信息确定模块
702
对应关系确定模块
703
SSLVPN设备确定子模块
7032
SSL隧道确定子模块
7034
数据包发送模块
704

图 7

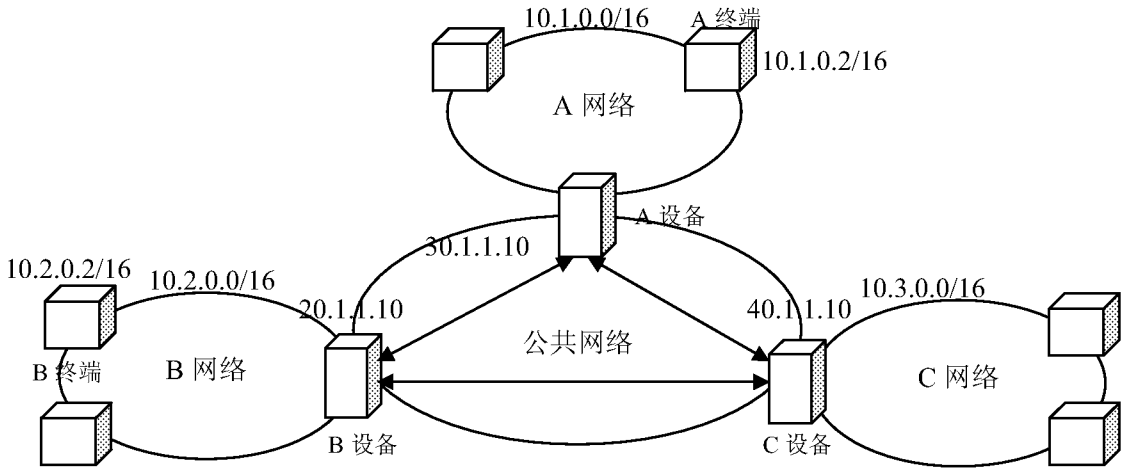
10.1.0.0/16
A 终端
10.1.0.2/16
A 网络
A 设备
30.1.1.10
10.2.0.2/16
10.2.0.0/16
20.1.1.10
40.1.1.10
10.3.0.0/16
公共网络
B 终端
B 网络
C 网络
B 设备
C 设备

图 8

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2009/071586

A. CLASSIFICATION OF SUBJECT MATTER

H04L 12/56(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 H04L12/-

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)

EPODOC WPI PAJ CNPAT CNKI

secure socket layer, SSL, virtual private network, VPN, IP, address, channel, private network

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN1838638A(HANGZHOU HUAWEI 3COM TECH [CN]) 27 Sept. 2006(27.09.2006) page 5 line 13 to page 6 line 19 in the description	1，3
A		2，4-10
A	US20080043749A1 (SUGANTHI ET AL) 21 Feb. 2008(21.02.2008) the whole document	1-10
A	CN101132420A (H3C TECHNOLOGIES CO LTD [CN]) 27 Feb. 2008(27.02.2008) the whole document	1-10

☐ 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
28 Jul. 2009(28.07.2009)	**13 Aug. 2009 (13.08.2009)**
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 CUI,Liyan Telephone No. (86-10)62411682

Form PCT/ISA/210 (second sheet) (April 2007)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2009/071586

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN1838638A	27.09.2006	none	
US20080043749A1	21.02.2008	none	
CN101132420A	27.02.2008	none	

国际检索报告

国际申请号
PCT/CN2009/071586

A. 主题的分类

H04L 12/56（2006.01）i

按照国际专利分类表(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 H04L12/-

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）)

EPODOC WPI PAJ CNPAT CNKI

secure socket layer, SSL, virtual private network, VPN, IP, address, channel, private network

安全套接层，虚拟专用网，地址，信道，隧道，通道，专用网，私网

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
X	CN1838638A（杭州华为三康技术有限公司） 27.9 月 2006（27.09.2006）说明书第 5 页第 13 行—第 6 页第 19 行	1，3
A		2，4-10
A	US20080043749A1 （SUGANTHI ET AL）21.2 月 2008（21.02.2008）全文	1-10
A	CN101132420A（杭州华三通信技术有限公司）27.2 月 2008（27.02.2008）全文	1-10

☐ 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

"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
28.7 月 2009（28.07.2009）	**13.8 月 2009 (13.08.2009)**
中华人民共和国国家知识产权局(ISA/CN) 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 崔丽艳 电话号码：(86-10) **62411682**

国际检索报告

关于同族专利的信息

国际申请号
PCT/CN2009/071586

检索报告中引用的专利文件	公布日期	同族专利	公布日期
CN1838638A	27.09.2006	无	
US20080043749A1	21.02.2008	无	
CN101132420A	27.02.2008	无	