

(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
2017年7月27日 (27.07.2017)



(10) 国际公布号
WO 2017/124837 A1

- (51) 国际专利分类号:
H04L 12/46 (2006.01)
- (21) 国际申请号: PCT/CN2016/107738
- (22) 国际申请日: 2016年11月29日 (29.11.2016)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201610034241.7 2016年1月19日 (19.01.2016) CN
- (71) 申请人: 深圳前海达闼云端智能科技有限公司 (CLOUDMINDS (SHENZHEN) ROBOTICS SYSTEMS CO., LTD.) [CN/CN]; 中国北京市朝阳区望京SOHO塔3A区23层, Beijing 100102 (CN)。
- (72) 发明人: 朱磊 (ZHU, Lei); 中国北京市朝阳区望京SOHO塔3A区23层, Beijing 100102 (CN)。
- (74) 代理人: 北京新知远方知识产权代理事务所 (普通合伙) (IPFUTURE INTELLECTUAL PROPERTY LAW OFFICE); 中国北京市海淀区花园东路10号高德大厦905徐烨, Beijing 100191 (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, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, 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, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, 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, KM, 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))。

(54) Title: PROXY METHOD, SERVER AND CLIENT FOR SSLVPN, AND PROCESSING METHOD THEREOF

(54) 发明名称: 一种SSLVPN的代理方法、服务器以及客户端及其处理方法

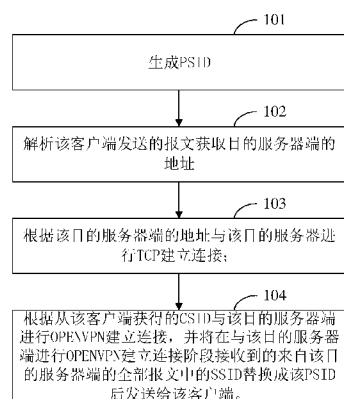


图4

- 101 Generate a PSID
- 102 Parse a message transmitted by a client to obtain a destination server-side address
- 103 Establish a TCP connection with the destination server according to the destination server-side address
- 104 Establish an OPENVPN connection with the destination server-side according to a CSID acquired from the client, and after SSIDs in all the messages received from the destination server-side at the establishment stage of the OPENVPN connection with the destination server-side are replaced with the PSID, transmit the messages to the client

(57) Abstract: An embodiment of the present application proposes a proxy method, a server and a client for an SSLVPN, and a processing method thereof, for reduction of IP resource consumption. In the present invention, a proxy server generates a PSID, and establishes an OPENVPN connection with a client according to the PSID; parses a message transmitted by the client to obtain a destination server-side address, wherein the message contains IP address information of the server; establishes a TCP connection with the destination server according to the destination server-side address; establishes an OPENVPN connection with the destination server-side according to a CSID acquired from the client, and, after SSIDs in all the messages received from the destination server-side at the establishment stage of the OPENVPN connection with the destination server-side are replaced with the PSID, transmits the messages to the client. By adding information processing at the establishment stage of the OPENVPN connection between the SSLVPN proxy server and client and the destination server-side, IP resource consumption is reduced.

(57) 摘要:

[见续页]



WO 2017/124837 A1



本申请实施例提出了一种 SSLVPN 的代理方法、服务器以及客户端及其处理方法，用于减少 IP 资源的消耗。本发明中，代理服务器生成 PSID，根据 PSID 与客户端进行 OPENVPN 建立连接；解析客户端发送的报文获取目的服务器端的地址，其中报文中包含服务器的 IP 地址信息；根据目的服务器端的地址与目的服务器进行 TCP 建立连接；根据从客户端获得的 CSID 与目的服务器端进行 OPENVPN 建立连接，并将在与目的服务器端进行 OPENVPN 建立连接阶段接收到的来自目的服务器端的全部报文中的 SSID 替换成 PSID 后发送给客户端。由于增加 SSLVPN 的代理服务器与客户端以及目的服务器端进行 OPENVPN 建立连接阶段的信息处理，从而减少了 IP 资源的消耗。

一种SSLVPN的代理方法、服务器以及客户端及其处理方法

技术领域

本申请涉及SSLVPN(Security Socket Layer Virtual Private Network, 安全套接层虚拟专用网络)技术领域, 尤其涉及一种SSLVPN的代理方法、服务器以及客户端及其处理方法。

背景技术

目前, 互联网及 ADN (Application Delivery Networking, 应用分发网络) 领域, 尤其在 SSLVPN 动态内容传输加速方面, 在 TCP (Transmission Control Protocol, 传输控制协议) 代理转发的方法中, 在使用通用服务端口 443 或者 1194 的情况下, 需要增加 IP (Internet Protocol, 因特网协议) 进行区分不同 SSLVPN 目的地址的问题, 提出了一种通用的 SSLVPN 协议解析目的地址识别的方法, 实现了基于 TCP 的通用的 SSLVPN 代理服务器。

在 ADN 领域中, 针对一个频道的 SSLVPN 请求, 通过 DNS (Domain Name System, 域名系统) 服务器将用户的访问引导到最近的 TCP 代理服务器上, TCP 代理服务器通过监听特定的套接字 (IP 地址+端口) 来接受来自用户的访问请求 (通常为 443 或者 1194 端口), 并使用预先配置好的源站的套接字与源站服务器建立连接, 将 SSLVPN 请求以 TCP 数据的形式发给源站服务器, 同时将来自源站服务器的响应转发给用户, 而在本地不做分析。

TCP 代理服务器的一个 IP 的 443 端口只能服务一个 SSLVPN 频道, 如果需要服务多个频道的话就会出现冲突。如果需要服务多个源站的时候就需要通过增加 IP 的方式进行解决, 即 IP1: 443 服务一个频道, IP2: 443 服务另外一个频道。

现有技术中无疑对 IP 资源的消耗非常严重。尽管可以做到多个 SSLVPN 频道的转发, 但是限制了 SSLVPN 服务频道个数。图 1 示出了传统 SSLVPN 代

理架构，如图所示，要区分两个不同的频道，需要使用两个不同的 IP，频道 1 解析到 IP1 上，频道 2 解析到 IP2 上。从而做到 SSLVPN 代理转发的功能。

现有技术中的 SSLVPN 代理基本都是位于 TCP 层或者 IP 层的。基本都是通过增加 IP 或者更换端口的方式进行区分。还未有基于一个 IP: PORT (端口) 的

5 通用的 SSLVPN 代理服务器。

发明内容

本申请实施例提出了一种 SSLVPN 的代理方法、服务器以及客户端及其处理方法，主要用于减少 IP 资源的消耗。

10 在一个方面，本申请实施例提供了一种 SSLVPN 的代理方法，包括：

生成代理会话标识，根据所述代理会话标识与客户端建立连接；

解析所述客户端发送的报文，获取目的服务器端的地址，其中所述客户端发送的报文中包含服务器的 IP 地址信息；

与所述 SSLVPN 目的服务器端建立连接，并将与所述目的服务器端建立连
15 接阶段接收到的来自所述目的服务器端的报文中的服务器会话标识，替换为所述代理会话标识后发送给所述客户端。

并提供了与上述代理方法对应的一种 SSLVPN 的代理服务器包括：

代理会话标识生成模块，用于生成代理会话标识信息；

解析模块，用于解析所述客户端发送的报文获取目的服务器端的地址；

20 客户端连接模块，用于根据所述代理会话标识信息与客户端建立连接；

服务器连接模块，用于与所述 SSLVPN 目的服务器端建立连接，并将与所述目的服务器端建立连接阶段接收到的来自所述目的服务器端的报文中的服务器会话标识，替换为所述代理会话标识后发送给所述客户端。

以及一种 SLVPN 代理服务器，包括：

25 收发单元，用于数据收发；

存储介质，用于存储程序；

处理器，用于依照所述存储介质的程序执行上文所述的 SSLVPN 代理方法。

在另一个方面，本申请实施例提供了一种 SSLVPN 客户端处理方法，包括：
获得 SSLVPN 目的服务器端的信息；

将所述目的服务器端的信息写入 SSL/TLS 协议报文中，并将所述报文发送给 SSLVPN 代理服务器。

5 并提供了与上述客户端处理方法对应的 SSLVPN 客户端，包括：
信息获取模块，用于获得 SSLVPN 目的服务器端的信息；
发送模块，用于将所述目的服务器端的信息写入 SSL/TLS 协议报文中，
并将所述报文发送给 SSLVPN 代理服务器。

以及一种 SSLVPN 客户端，包括：

10 收发单元，用于数据收发；

存储介质，用于存储程序；

处理器，用于依照所述存储介质的程序执行上文所述的 SSLVPN 客户端处理方法。

有益效果如下：

15 在本发明实施例中，增加 SSLVPN 的代理服务器与客户端以及目的服务器端进行 OPENVPN 建立连接阶段的信息处理，这样对于多个源站对应的客户端，SSLVPN 的代理服务器可以使用同一 IP 地址与各个客户端建立连接，对于各个客户端接收到的报文，可以通过服务器地址进行区分，从而确定服务器发送至哪个服务器。这样就无需通过 IP 地址对不同源站的客户端进行区分。从而
20 避免了现有技术中 TCP 代理服务器一个 IP 的 443 端口只能服务一个 SSLVPN 频道，如果需要服务多个频道的话就会出现冲突，如果需要服务多个源站的时候就需要通过增加 IP 的方式进行解决的问题，从而减少了 IP 资源的消耗。

附图说明

25 下面将参照附图描述本申请的具体实施例，其中：

图 1 示出了传统 SSLVPN 代理架构示意图；

图 2 示出了在没有代理的情况下 SSLVPN 的处理流程示意图；

图 3 示出了本申请实施例中采用了通用的 SSLVPN 代理服务器的 SSLVPN 的处理流程示意图；

图 4 示出了本申请实施例中 SSLVPN 代理服务器的代理方法流程示意图；

图 5 示出了本申请实施例中 SSLVPN 客户端处理方法流程示意图；

5 图 6 示出了本申请实施例中的 SSLVPN 代理架构示意图；

图 7 示出了本申请实施例中的 SSLVPN 的代理服务器的结构示意图；

图 8 示出了本申请实施例中 SSLVPN 的客户端的结构示意图；

图9示出了本申请实施例中一个具体的SSLVPN的客户端的结构示意图；

图10示出了本申请实施例中一种SSLVPN代理服务器的结构示意图；

10 图11示出了本申请实施例中一种SSLVPN客户端的结构示意图。

具体实施方式

为了使本申请的技术方案及优点更加清楚明白，以下结合附图对本申请的示例性实施例进行进一步详细的说明，显然，所描述的实施例仅是本申请的一部分实施例，而不是所有实施例的穷举。并且在不冲突的情况下，本说明书中的实施例及实施例中的特征可以互相结合。

基于 TCP 的 SSLVPN 代理服务器的前提是无证书，所谓无证书指的是源站不将 SSL 的证书及私钥放在代理服务器上，这样代理服务器不具备对 SSL 协议解析的功能，即客户端的访问内容依然是加密的，安全性可以保证。代理服务器作为中间人的角色，从 TCP 的层面进行 TCP 包的转发。

在没有代理的情况下，如图 2 所示，根据 SSLVPN 的原理，SSLVPN Client（客户）端与 Server（服务器）端首先进行 TCP 建立连接，TCP 建立连接后进行 OPENVPN 建立连接，主要是客户端发送“P_CONTROL_HEAD_RESET_CLIENT_V2”，服务器端发送“P_CONTROL_HEAD_RESET_SERVER”。客户端与服务端各自生成 CSID(客户端会话标识)和 SSID(服务器会话标识)，即一个随机的会话号。OPENVPN 建立连接之后即进入 SSL 建立连接阶段。SSL 建立连接阶段遵循正常的 SSL/TLS

(Transport Layer Security Protocol, 安全传输层协议)流程。主要流程为客户端发送 Client Hello 与服务器端进行建立连接, 该字段为明文。服务器端接收到之后发送 Server Hello 及证书等流程。在验证证书及秘钥通过后即可协商一个加密通道 VPN(Virtual Private Network, 虚拟专用网络)。客户端与服务端的交互数据即可通过该加密通道进行传输。

但是由于 SSLVPN 位于公共互联网基础之上, 受到各种网络因素的影响, 稳定性及速度均受到影响。如果使用 ADN 加速网络的话, 可以明显的解决访问速度及稳定性的问题。但是现有的 TCP 代理的方式严重浪费 IP 资源(如前文所述), 故本发明用一个通用的 SSLVPN 代理服务器来解决以上问题。

为解决 IP 资源浪费的问题, 本发明主要需解决两个问题: 1、如何识别是来自不同的 VPN 客户端的目的地问题; 2、SSLVPN 客户端及服务器端如何信任 VPN 代理, 即解决 SID(会话标识)的问题。

1、针对问题 1, SSL/TLS 协议中 SNI(Server Name Indication, 服务器名称指示)扩展字段为通用的方式, 在通用的 HTTPS 协议中, 在 Client Hello 的明文包中即插入了访问的去向域名。例如 sslvpn.test.com. 不同的访问目的地址该 SNI 字段不同, 且为明文字段。但是在 SSLVPN 协议中均未利用该 SNI 字段。本发明利用这个 SNI 字段进行 SSLVPN 经过代理服务器时的目的地址选择的标识, 在客户端插入了 SNI 字段, 具体可以如下:

Secure Sockets Layer

TLSv1 Record Layer: Handshake Protocol: Client Hello

Content Type: Handshake (22)

Version: TLS 1.0 (0x0301)

Length: 287

Handshake Protocol: Client Hello

Handshake Type: Client Hello (1)

Length: 283

Version: TLS 1.2 (0x0303)

Random

Session ID Length: 0

Cipher Suites Length: 110

Cipher Suites (55 suites)

5 Compression Methods Length: 1

Compression Methods (1 method)

Extensions Length: 132

Extension: server_name

Type: server_name (0x0000)

10 Length: 23

Server Name Indication extension

Server Name list length: 21

Server Name Type: host_name (0)

Server Name length: 18

15 **Server Name: www.cloudminds.com**

但是，SSL/TLS 的建立连接阶段是位于 OPENVPN 建立连接之后的，即如果代理服务器不知道目的地址的话，OPENVPN 建立连接是不成功的。更无法进行后续的 SSL 建立连接。所以为了解决 OPENVPN 建立连接不通的问题，提出方法解决问题 2；

20 2、如图 3 所示，由于 OPENVPN 建立连接阶段，客户端与服务器端各自生成 CSID 与 SSID, 且 OPENVPN 进行三次握手的时候，VPNPROXY 代服务器端与客户端进行 OPENVPN 进行建立连接，生成一个 Proxy Session ID, 简称 PSID（代理会话标识），该 PSID 可随机生成，也可根据实际需要按不同算法生成，通过 PSID 代替 SSID 与客户端进行建立连接。在客户端与 VPN 代理建立 OPENVPN
25 连接之后，客户端会发送 Client Hello 的明文字段进行 SSL 建立连接，由于携带了 SNI 字段，代理服务器对 Client Hello 报文进行协议解析，解析出 SNI 字段，并对 SNI 进行 DNS 解析等操作，获取到目的 IP 地址。这样代理服务器就可以与真正的服务器端进行 TCP 建立连接，TCP 建立连接之后，VPN 代理再

使用 CSID 与服务器端进行 OPENVPN 建立连接。注意此时真正的服务器会发送真正的 SSID 给 VPN 代理服务器，如果直接将 SSID 发给客户端的话会导致客户端的验证失败，导致连接断开。所以 VPN 代理服务器的另外一个重要的功能就是需要将来自服务器的 OPENVPN 的建立连接阶段的所有报文的 SSID 替换成为 PSID 后再发给客户端。后续 VPN 代理服务器将继续做 TCP 数据报文的转发，而无需解密数据包。这样便解决了通用的 SSLVPN 代理服务器的问题。

从 SSLVPN 代理服务器的角度，其代理方法如图 4 所示，包括：

步骤 101，生成 PSID，根据该 PSID 与客户端进行 OPENVPN 建立连接；

步骤 102，解析该客户端发送的报文获取目的服务器端的地址；

10 步骤 103，根据该目的服务器端的地址与该目的服务器进行 TCP 建立连接；

步骤 104，根据从该客户端获得的 CSID 与该目的服务器端进行 OPENVPN 建立连接，并将在与该目的服务器端进行 OPENVPN 建立连接阶段接收到的来自该目的服务器端的全部报文中的 SSID 替换成该 PSID 后发送给该客户端。

15 上述流程中步骤 102 解析所述客户端发送的报文获取目的服务器端的地址包括：

从该客户端发送的 hello 报文中解析出 SNI，该 SNI 携该目的服务器端的信息；

根据该 SNI 携带的该目的服务器端的信息获取所述目的服务器端的地址。

从 SSLVPN 客户端的角度，其客户端处理方法如图 5 所示，包括：

20 步骤 201，获得目的服务器端的信息；

步骤 202，将所述目的服务器端的信息写入 SSL/TLS 协议报文中，并将所述报文发送给 SSLVPN 代理服务器。

具体地，该步骤 202 中将所述目的服务器端的信息发送给代理服务器包括：将该目的服务器端的信息写入客户端 hello 报文中的 SNI 字段并发送给该代理服务器。

25

本申请实施例中的 SSLVPN 代理架构如图 6 所示。

其中的流程编号简述如下

编号 1、SSLVPN 客户端 1 访问 SSLVPN 代理服务器，并在 Client Hello 包中携带 SNI；

编号 2、SSLVPN 代理服务器识别并解析 SNI，获取 SSLVPN server 域名，
5 并查询本地 DNS 服务器；

编号 3、本地 DNS 服务器返回 SSLVPN 服务器的 IP 地址；

编号 4、SSLVPN 代理服务器使用该 IP 地址与 SSLVPN 服务器建立连接，并完成通信。

基于同一发明构思，本申请实施例中还提供了一种 SSLVPN 的代理服务器，
10 由于这些设备解决问题的原理与一种 SSLVPN 的代理方法相似，因此这些设备的实施可以参见方法的实施，重复之处不再赘述。

如图 7 所示，本申请实施例中的 SSLVPN 的代理服务器包括：

解析模块，用于解析所述客户端发送的报文获取目的服务器端的地址；

客户端连接模块，用于根据所述代理会话标识信息与客户端建立连接；

15 服务器连接模块，用于与所述 SSLVPN 目的服务器端建立连接，并将与所述目的服务器端建立连接阶段接收到的来自所述目的服务器端的报文中的服务器会话标识转换后发送给所述客户端。

作为一个实施例，代理服务器可以包括下述模块：

代理会话标识生成模块 701，用于生成代理会话标识 PSID；

20 第一 OPENVPN 模块 702，用于根据所述 PSID 与客户端进行 OPENVPN 建立连接；

解析模块 703，用于解析所述客户端发送的报文获取目的服务器端的地址；

TCP 模块 704，用于根据所述目的服务器端的地址与所述目的服务器进行
25 传输控制协议 TCP 建立连接；

第二 OPENVPN 模块 705，用于根据从所述客户端获得的客户端会话标识

CSID 与所述目的服务器端进行 OPENVPN 建立连接，并将在与所述目的服务器端进行 OPENVPN 建立连接阶段接收到的来自所述目的服务器端的全部报文中的服务器会话标识 SSID 替换成所述 PSID 后发送给所述客户端。

进一步地，解析模块 703 解析所述客户端发送的报文获取目的服务器端的地址包括：

从所述客户端发送的 hello 报文中解析出服务器名称指示 SNI，所述 SNI 携带所述目的服务器端的信息；

根据所述 SNI 携带的所述目的服务器端的信息获取所述目的服务器端的地址。

并且，代理会话标识生成模块 701 可以用于随机生成所述 PSID。

基于同一发明构思，本申请实施例中还提供了一种 SSLVPN 的客户端，由于这些设备解决问题的原理与一种 SSLVPN 的客户端处理方法相似，因此这些设备的实施可以参见方法的实施，重复之处不再赘述。

如图 8 所示，本申请实施例中的 SSLVPN 的客户端，包括：

信息获取模块 801，用于获得目的服务器端的信息；

发送模块 802，用于将所述目的服务器端的信息写入 SSL/TLS 协议报文中，并将所述报文发送给 SSLVPN 代理服务器。

具体地，本申请实施例中的 SSLVPN 的客户端如图 9 所示，所述发送模块 802 包括：

信息写入单元 901，用于将所述目的服务器端的信息写入 hello 报文中的服务器名称指示 SNI 字段；

发送单元 902，用于将所述客户端 hello 报文发送给 SSLVPN 代理服务器。

本领域内的技术人员应明白，本申请的实施例可提供为方法、装置、系统、或计算机程序产品。因此，本申请可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本申请可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质（包括但不限于磁盘

存储器、CD-ROM、光学存储器等)上实施的计算机程序产品的形式。

基于同一发明构思,本申请实施例中还提供了一种 SSLVPN 代理服务器 1000,如图 10 所示,包括:收发单元 1001,用于数据收发;存储介质 1003,用于存储程序;处理器 1005,用于依照存储介质 1003 的程序执行上文所述的
5 SSLVPN 代理方法。

此外,本申请实施例还提供一种 SSLVPN 客户端 1100,如图 11 所示,包括:收发单元 1101,用于数据收发;存储介质 1103,用于存储程序;处理器 1105,用于依照存储介质 1103 的程序执行上文所述的 SSLVPN 客户端处理方法。

10 本申请是参照根据本申请实施例的方法、设备(系统)、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器,使得通
15 过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中,使得存储在该计算机可读存储器
20 中的指令产生包括指令装置的制造品,该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上,使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理,从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图
25 一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

尽管已描述了本申请的优选实施例，但本领域内的技术人员一旦得知了基本创造性概念，则可对这些实施例作出另外的变更和修改。所以，所附权利要求意欲解释为包括优选实施例以及落入本申请范围的所有变更和修改。

权 利 要 求 书

1. 一种 SSLVPN 代理方法，其特征在于，包括：

生成代理会话标识，根据所述代理会话标识与客户端建立连接；

5 解析所述客户端发送的报文，获取目的服务器端的 IP 地址；其中，所述客户端发送的报文中包含服务器的 IP 地址信息；

与所述 SSLVPN 目的服务器端建立连接，并将与所述目的服务器端建立连接阶段接收到的来自所述目的服务器端的报文中的服务器会话标识，替换为所述代理会话标识后发送给所述客户端。

10 2、如权利要求 1 所述的方法，其特征在于，根据所述代理会话标识信息与客户端建立连接，包括：

所述生成代理会话标识为 PSID，根据所述 PSID 与客户端进行 OPENVPN 建立连接。

3、如权利要求 1 所述的方法，其特征在于，所述解析所述客户端发送的
15 报文，获取目的服务器端的地址，包括：

从所述客户端发送的 hello 报文中解析出服务器名称指示 SNI，所述 SNI 携带所述目的服务器端的信息；

根据所述 SNI 携带的所述目的服务器端的信息获取所述目的服务器端的地址。

20 4、如权利要求 1 或 3 所述的方法，其特征在于，所述与所述目的服务器端建立连接，包括：

根据所述目的服务器端的地址与所述目的服务器进行传输控制协议 TCP 建立连接；

25 根据从所述客户端获得的客户端会话标识 CSID 与所述目的服务器端进行 OPENVPN 建立连接。

5、如权利要求 2 所述的方法，其特征在于，将与所述目的服务器端建立连接阶段接收到的来自所述目的服务器端的报文中的服务器会话标识，替换为所述代理会话标识后发送给所述客户端，包括：

5 将与所述目的服务器端进行 OPENVPN 建立连接阶段，接收到的来自所述目的服务器端的全部报文中的服务器会话标识 SSID 替换成所述 PSID 后发送给所述客户端。

6、如权利要求 2 所述的方法，其特征在于，所述生成 PSID 包括：

随机生成 PSID, 或根据算法生成 PSID。

7、一种 SSLVPN 客户端处理方法，其特征在于，包括：

10 获得目的服务器端的地址信息；

将所述目的服务器端的信息写入 SSL/TLS 协议报文中，并将所述报文发送给 SSLVPN 代理服务器。

8、如权利要求 7 所述的方法，其特征在于，所述将所述目的服务器端的地址信息写入 SSL/TLS 协议报文中，包括：

15 将所述目的服务器端的信息写入 hello 报文中的服务器名称指示 SNI 字段。

9、一种 SSLVPN 代理服务器，其特征在于，包括：

代理会话标识生成模块，用于生成代理会话标识信息；

20 解析模块，用于解析所述客户端发送的报文获取目的服务器端的地址，其中，所述客户端发送的报文中包含服务器的 IP 地址信息；

客户端连接模块，用于根据所述代理会话标识信息与客户端建立连接；

服务器连接模块，用于与所述 SSLVPN 目的服务器端建立连接，并将与所述目的服务器端建立连接阶段接收到的来自所述目的服务器端的报文中的服务器会话标识，替换为所述代理会话标识后发送给所述客户端。

10、如权利要求 9 所述的服务器，其特征在于，所述代理会话标识生成

模块, 生成的代理会话标识信息, 包括: PSID。

11、如权利要求 10 所述的服务器, 其特征在于, 所述客户端连接模块, 包括:

第一 OPENVPN 模块, 用于根据所述 PSID 与客户端进行 OPENVPN 建立连接。

5 12、如权利要求 9 所述的服务器, 其特征在于, 所述解析模块, 解析所述客户端发送的报文获取目的服务器端的地址, 包括:

从所述客户端发送的 hello 报文中解析出服务器名称指示 SNI, 所述 SNI 携带所述目的服务器端的信息;

10 根据所述 SNI 携带的所述目的服务器端的信息获取所述目的服务器端的地址。

13、如权利要求 9 所述的服务器, 其特征在于, 所述服务器连接模块, 包括:

TCP 模块, 用于根据所述目的服务器端的地址与所述目的服务器进行传输控制协议 TCP 建立连接;

15 第二 OPENVPN 模块, 用于根据从所述客户端获得的客户端会话标识 CSID 与所述目的服务器端进行 OPENVPN 建立连接。

14、如权利要求 13 所述的服务器, 其特征在于, 所述第二 OPENVPN 模块, 还用于:

20 将与所述目的服务器端进行 OPENVPN 建立连接阶段, 接收到的来自所述目的服务器端的全部报文中的服务器会话标识 SSID 替换成所述 PSID 后发送给所述客户端。

15、如权利要求 9 所述的代理服务器, 其特征在于, 所述代理会话标识生成模块生成代理会话标识信息, 包括: 随机生成所述 PSID, 或根据算法生成 PSID。

25 16、一种 SSLVPN 客户端, 其特征在于, 包括:

信息获取模块, 用于获得 SSLVPN 目的服务器端的信息;

发送模块，用于将所述目的服务器端的信息写入 SSL/TLS 协议报文中，并将所述报文发送给 SSLVPN 代理服务器。

17、如权利要求 16 所述的客户端，其特征在于，所述发送模块包括：

5 信息写入单元，用于将所述目的服务器端的信息写入 hello 报文中的服务器名称指示 SNI 字段；发送单元，用于将所述客户端 hello 报文发送给所述代理服务器。

18、一种 SSLVPN 代理服务器，其特征在于，包括：

收发单元，用于数据收发；

存储介质，用于存储程序；

10 处理器，用于依照所述存储介质的程序执行如权利要求 1 至 6 任意一项所述的 SSLVPN 代理方法。

19、一种 SSLVPN 客户端，其特征在于，包括：

收发单元，用于数据收发；

存储介质，用于存储程序；

15 处理器，用于依照所述存储介质的程序执行如权利要求 7 或 8 所述的 SSLVPN 客户端处理方法。

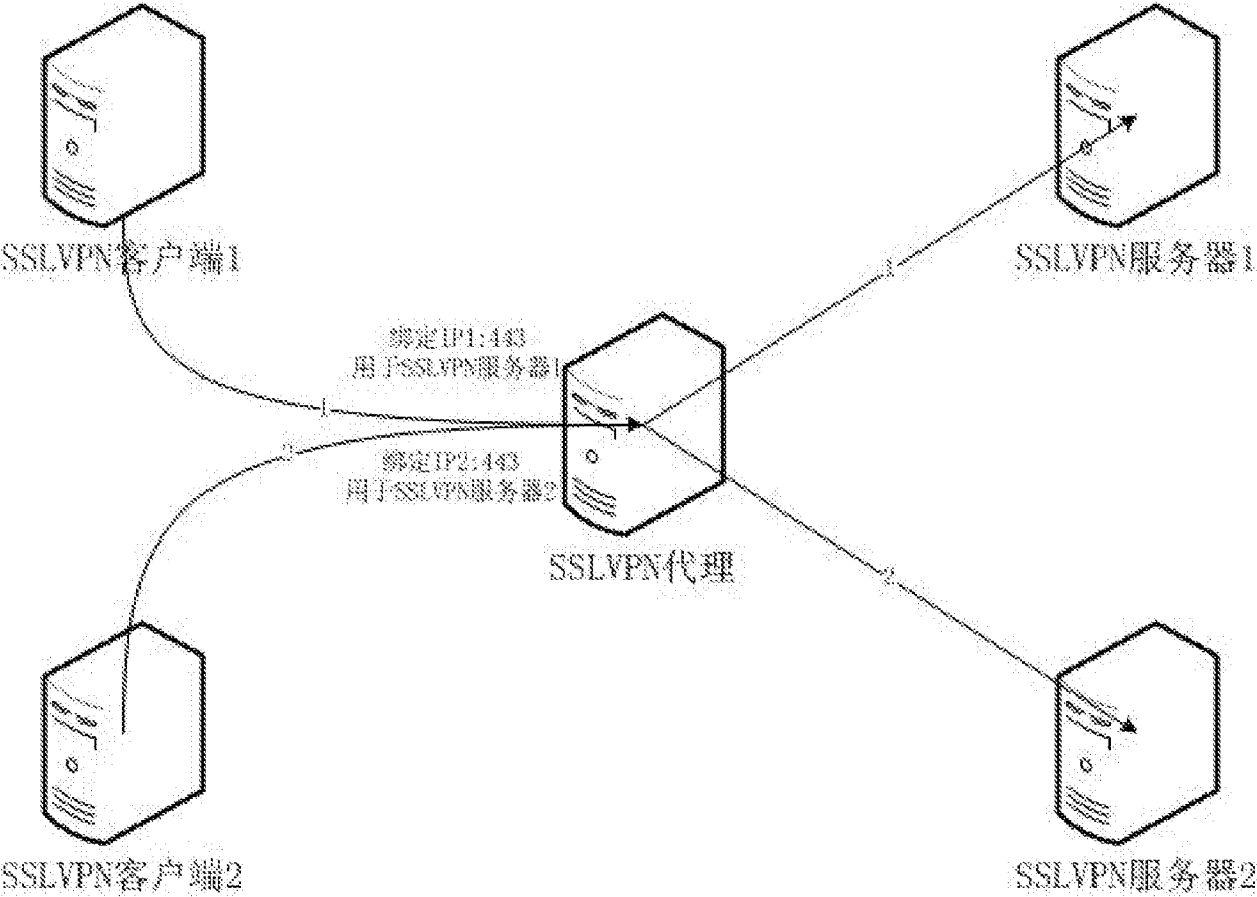


图 1

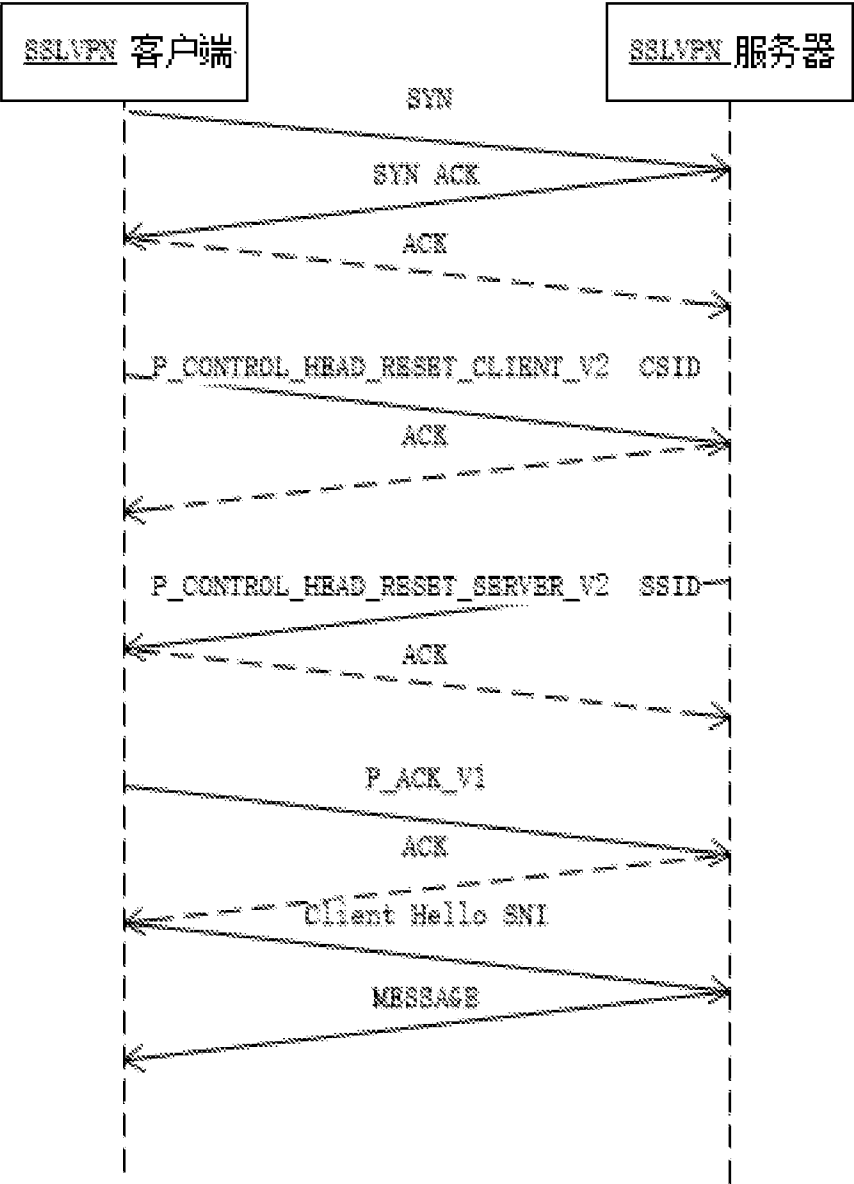


图 2

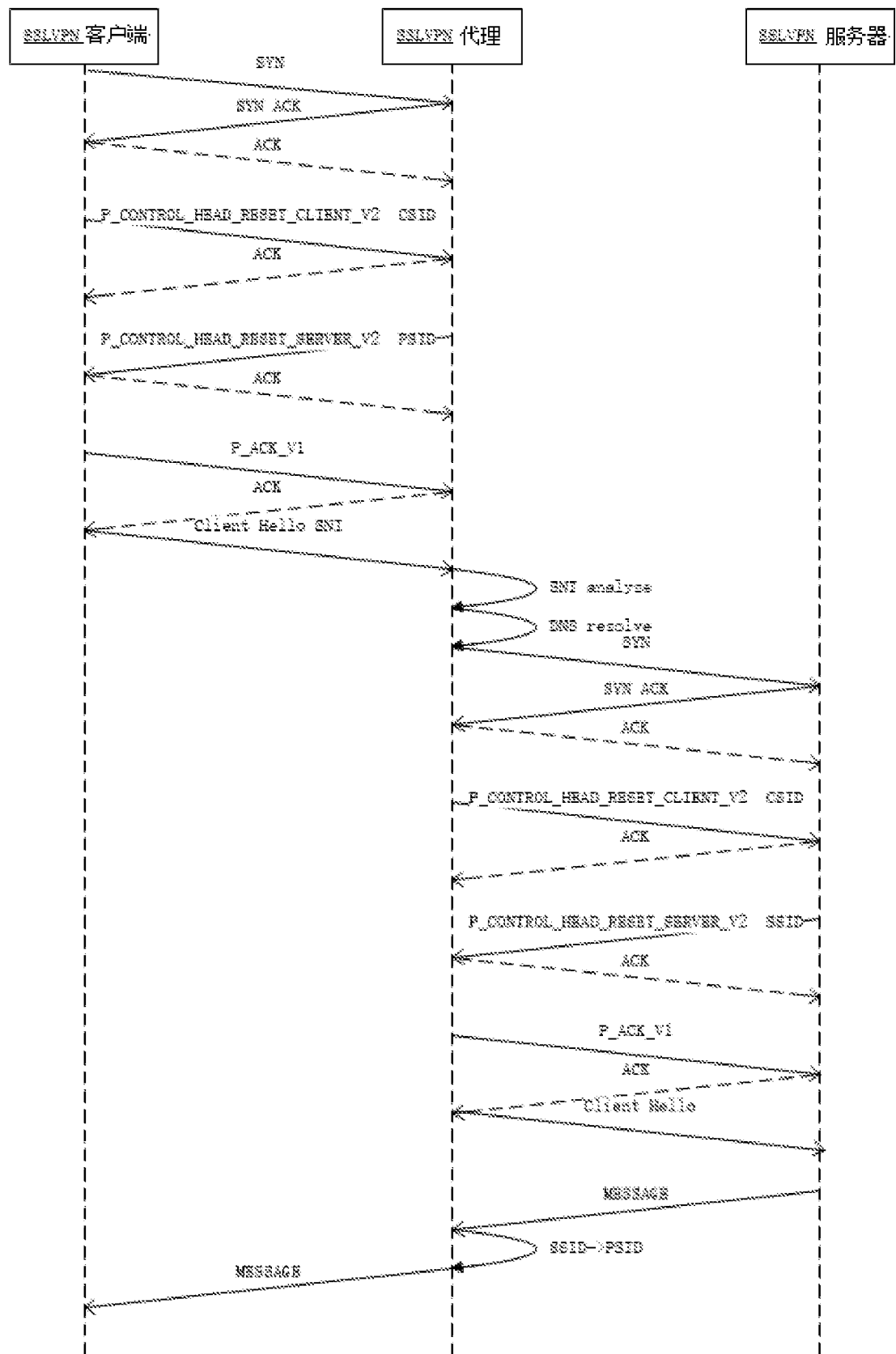


图 3

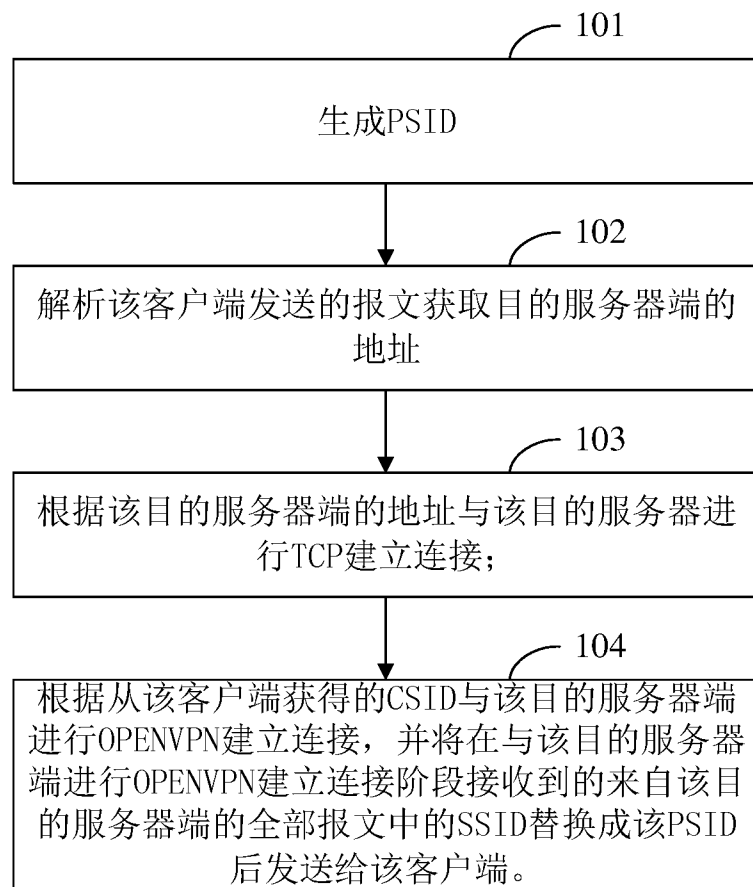


图 4

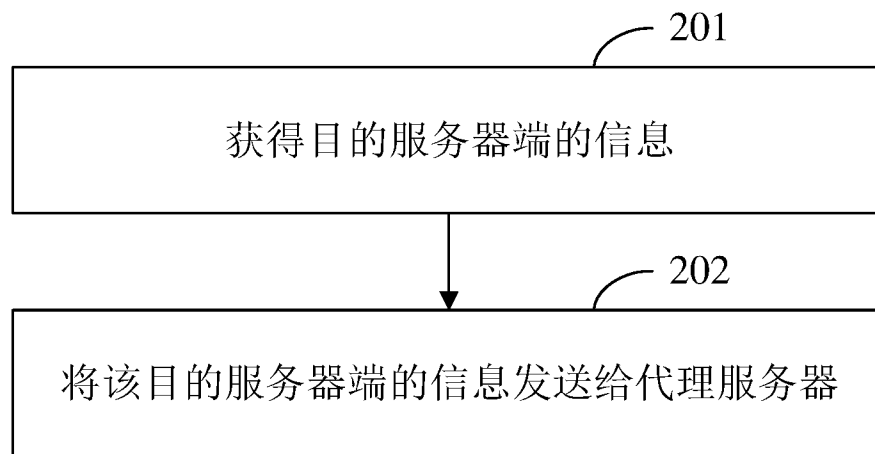


图 5

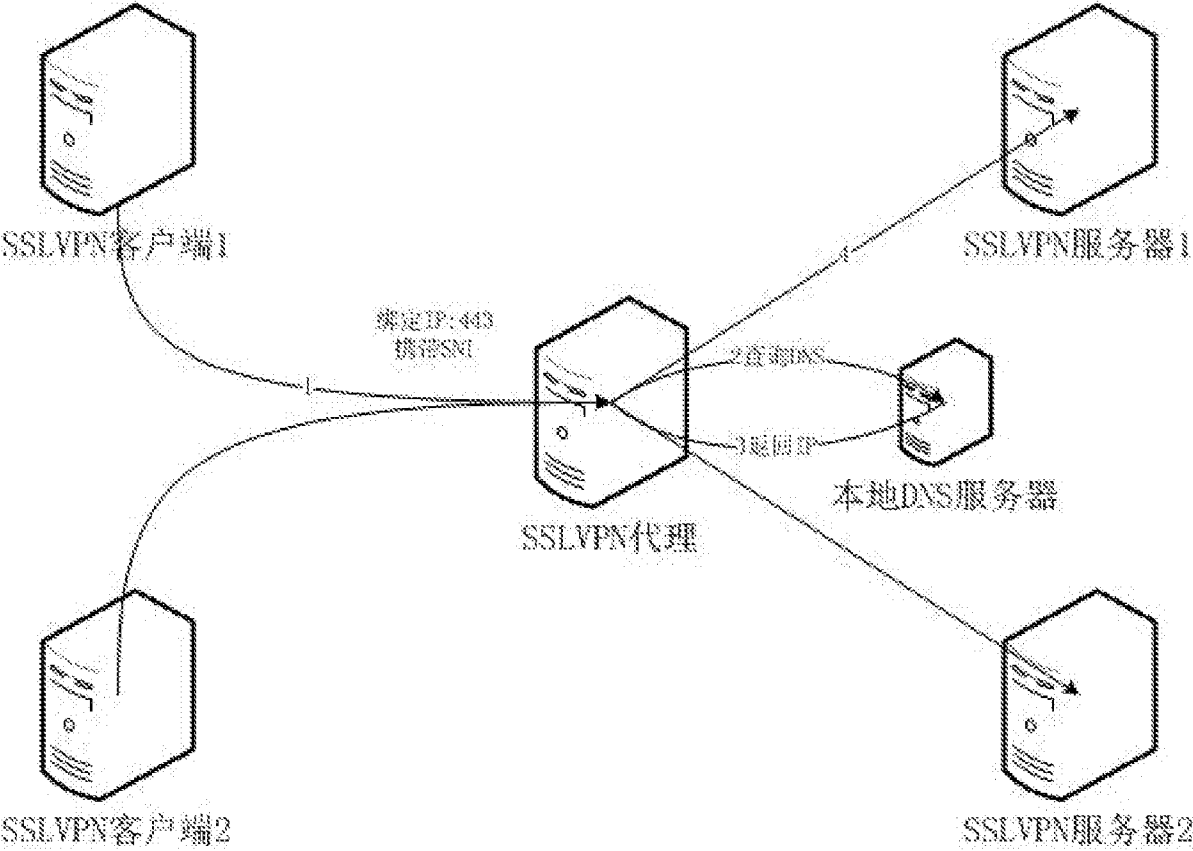


图 6

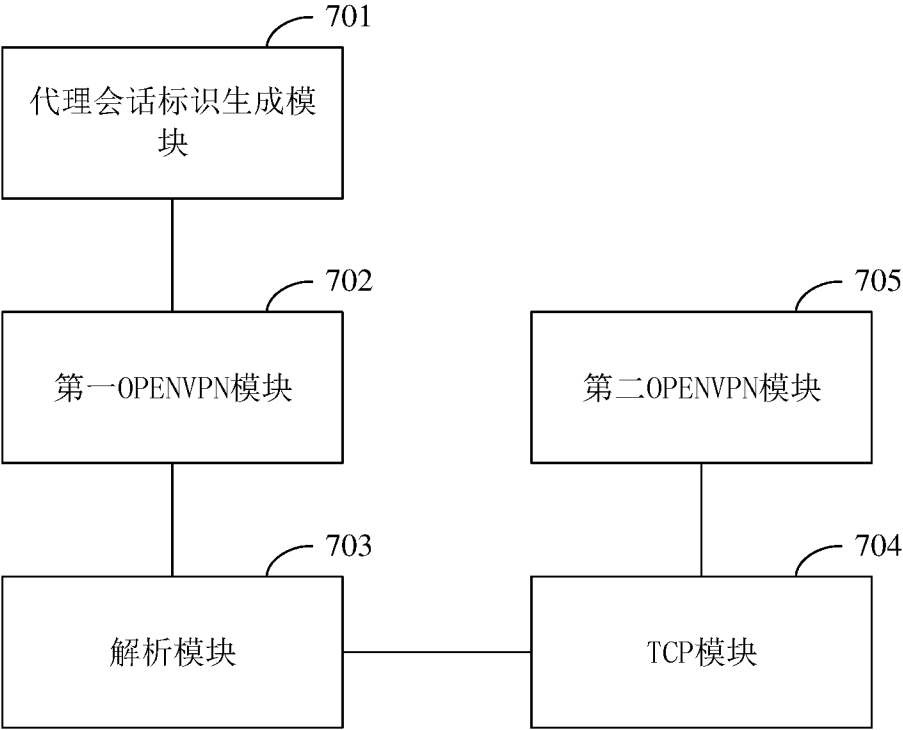


图 7

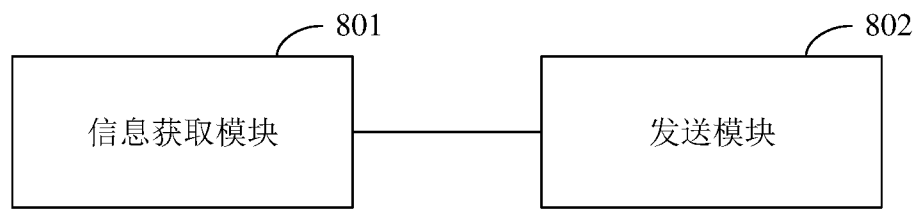


图 8

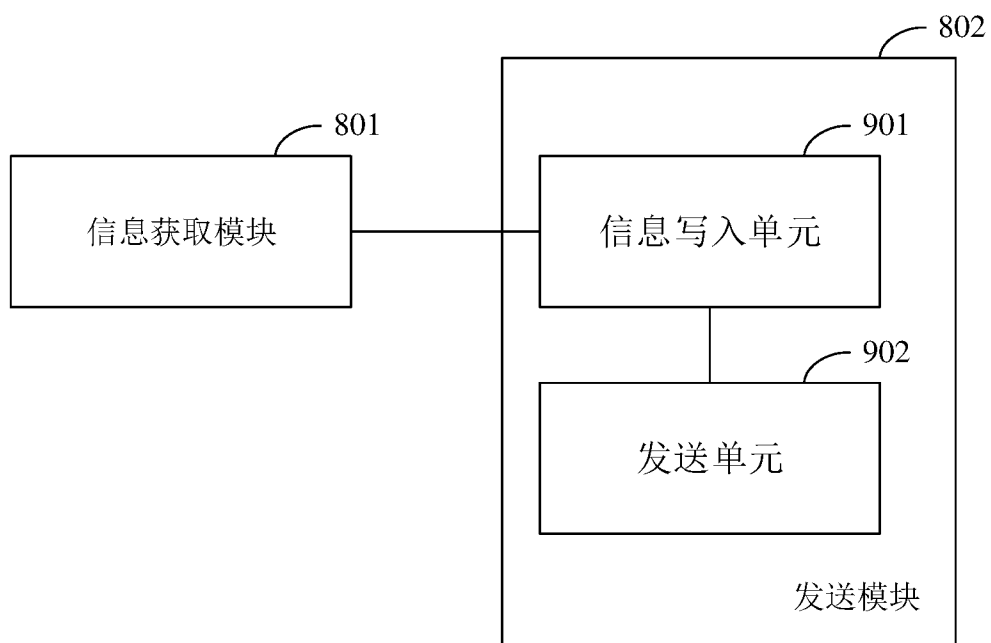


图 9

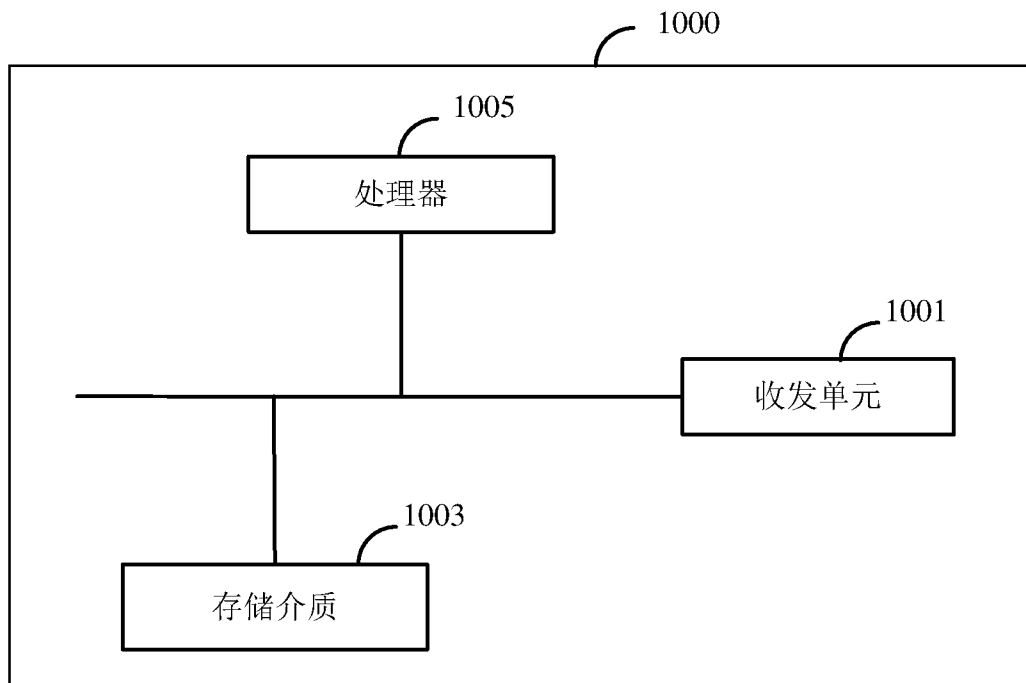


图 10

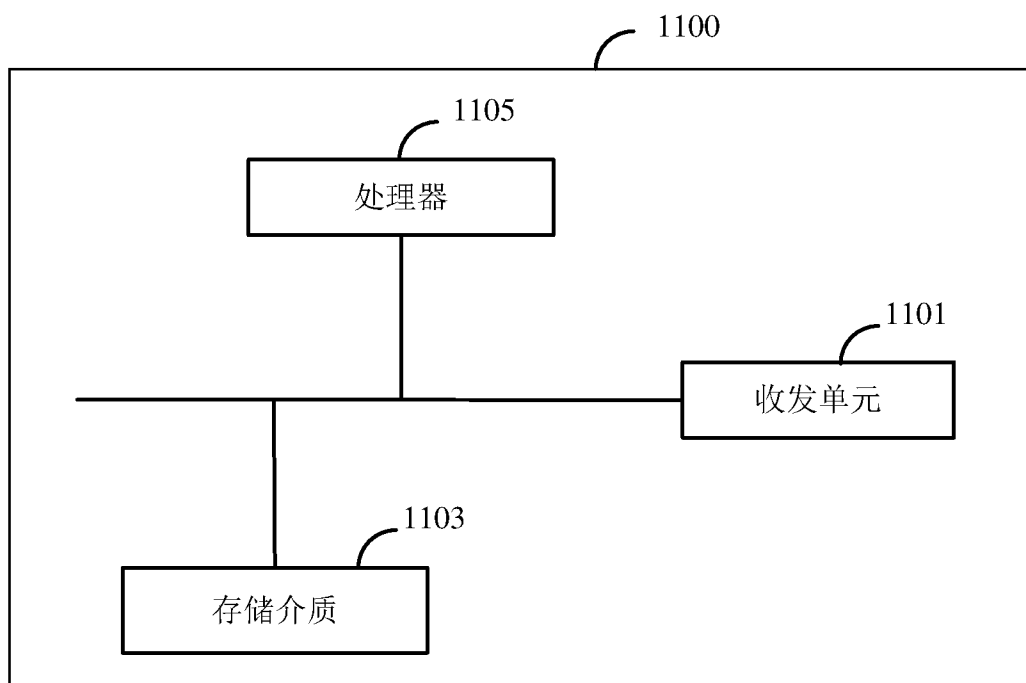


图 11

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2016/107738

A. CLASSIFICATION OF SUBJECT MATTER

H04L 12/46 (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)

H04L

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)

CNABS, CNTXT, VEN, CNKI: ssl, security socket layer, VPN, virtual private network, IP, address, proxy, reduc+, sav+, SNI, server
name indication

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 105634904 A (CLOUDMINDS INC.) 01 June 2016 (01.06.2016) description, paragraphs [0006]-[0086]	1-19
X	CN 104270379 A (BEIJING CHINA CACHE COMMUNICATION TECHNOLOGY CO.,LTD.) 07 January 2015 (07.01.2015) description, paragraphs [0029]-[0089]	7, 8, 16, 17, 19
A	CN 104270379 A (BEIJING CHINA CACHE COMMUNICATION TECHNOLOGY CO.,LTD.) 07 January 2015 (07.01.2015) the whole document	1-6, 9-15, 18
A	CN 102948131 A (CITRIX SYSTEMS INC.) 27 February 2013 (27.02.2013) the whole document	1-19
A	CN 103139185 A (ZHONGKE INFORMATION SECURITY COMMON TECHNOLOGY NATIONAL ENGINEERING RESEARCH CENTER CO., LTD.) 05 June 2013 (05.06.2013) the whole document	1-19

☒ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:	“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
“A” document defining the general state of the art which is not considered to be of particular relevance	“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
“E” earlier application or patent but published on or after the international filing date	“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
“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)	“&” document member of the same patent family
“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	

Date of the actual completion of the international search 13 February 2017	Date of mailing of the international search report 02 March 2017
Name and mailing address of the ISA State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No. (86-10) 62019451	Authorized officer BAI, Jingxin Telephone No. (86-10) 62089447

INTERNATIONAL SEARCH REPORTInternational application No.
PCT/CN2016/107738

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 8572721 B2 (KUMAR ARKESH et al.) 29 October 2013 (29.10.2013) the whole document	1-19

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2016/107738

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 105634904 A	01 June 2016	None	
CN 104270379 A	07 January 2015	None	
CN 102948131 A	27 February 2013	EP 2561639 A2	27 February 2013
		US 2014122865 A1	01 May 2014
		EP 2561639 A4	22 June 2016
		WO 2011133422 A3	12 January 2012
		US 8543805 B2	24 September 2013
		WO 2011133422 A2	27 October 2011
		US 2011264905 A1	27 October 2011
		CN 102948131 B	15 July 2015
		US 8949591 B2	03 February 2015
CN 103139185 A	05 June 2013	None	
US 8572721 B2	29 October 2013	US 9246878 B2	26 January 2016
		US 2014041014 A1	06 February 2014
		US 2008034416 A1	07 February 2008

国际检索报告

国际申请号

PCT/CN2016/107738

A. 主题的分类

H04L 12/46(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)

H04L

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))

CNABS, CNTXT, VEN, CNKI:安全套接层, 虚拟专用网, 地址, 代理服务器, 减少, 节省, 服务器名称指示, ssl, security socket layer, VPN, virtual private network, IP, address, proxy, reduc+, sav+, SNI, server name indication

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
PX	CN 105634904 A (深圳前海达闼云端智能科技有限公司) 2016年 6月 1日 (2016 - 06 - 01) 说明书第[0006]-[0086]段	1-19
X	CN 104270379 A (北京蓝汛通信技术有限公司) 2015年 1月 7日 (2015 - 01 - 07) 说明书第[0029]-[0089]段	7-8、16-17、19
A	CN 104270379 A (北京蓝汛通信技术有限公司) 2015年 1月 7日 (2015 - 01 - 07) 全文	1-6、9-15、18
A	CN 102948131 A (思杰系统有限公司) 2013年 2月 27日 (2013 - 02 - 27) 全文	1-19
A	CN 103139185 A (中科信息安全共性技术国家工程研究中心有限公司) 2013年 6月 5日 (2013 - 06 - 05) 全文	1-19
A	US 8572721 B2 (KUMAR ARKESH等) 2013年 10月 29日 (2013 - 10 - 29) 全文	1-19

☐ 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

2017年 2月 13日

国际检索报告邮寄日期

2017年 3月 2日

ISA/CN的名称和邮寄地址

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

白晶心

电话号码 (86-10)62089447

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2016/107738

检索报告引用的专利文件			公布日 (年/月/日)	同族专利			公布日 (年/月/日)
CN	105634904	A	2016年 6月 1日	无			
CN	104270379	A	2015年 1月 7日	无			
CN	102948131	A	2013年 2月 27日	EP	2561639	A2	2013年 2月 27日
				US	2014122865	A1	2014年 5月 1日
				EP	2561639	A4	2016年 6月 22日
				WO	2011133422	A3	2012年 1月 12日
				US	8543805	B2	2013年 9月 24日
				WO	2011133422	A2	2011年 10月 27日
				US	2011264905	A1	2011年 10月 27日
				CN	102948131	B	2015年 7月 15日
				US	8949591	B2	2015年 2月 3日
CN	103139185	A	2013年 6月 5日	无			
US	8572721	B2	2013年 10月 29日	US	9246878	B2	2016年 1月 26日
				US	2014041014	A1	2014年 2月 6日
				US	2008034416	A1	2008年 2月 7日

表 PCT/ISA/210 (同族专利附件) (2009年7月)