(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
2020 年 9 月 24 日 (24.09.2020)

WIPO | PCT

(10) 国际公布号
WO 2020/186694 A1

(51) 国际专利分类号:
H04L 12/46 (2006.01) *H04L 29/06* (2006.01)
H04L 29/08 (2006.01)

(21) 国际申请号: PCT/CN2019/102738

(22) 国际申请日: 2019 年 8 月 27 日 (27.08.2019)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201910196147.5 2019年3月15日 (15.03.2019) CN

(71) 申请人: 平安科技（深圳）有限公司 (PING AN TECHNOLOGY (SHENZHEN) CO., LTD.) [CN/CN]; 中国广东省深圳市福田区福田街道福安社区益田路5033号平安金融中心23楼, Guangdong 518000 (CN)。

(72) 发明人: 匡光彩 (KUANG, Guangcai); 中国广东省深圳市福田区福田街道福安社区益田路5033号平安金融中心23楼, Guangdong 518000 (CN)。

(74) 代理人: 广州三环专利商标代理有限公司 (SCIHEAD IP LAW FIRM); 中国广东省广州市越秀区先烈中路80号汇华商贸大厦1508室, Guangdong 510070 (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, JO, JP, KE, KG, KH, 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,

(54) **Title:** COMMUNICATION METHOD FOR VIRTUAL PRIVATE NETWORK, AND RELATED DEVICE

(54) **发明名称:** 一种虚拟专用网络的通信方法及相关装置

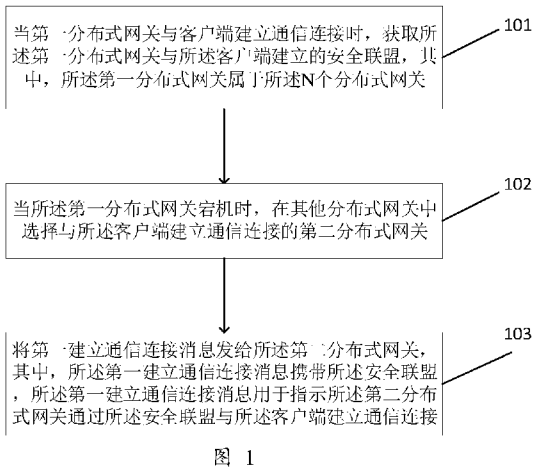

图 1

101 When a first distributed gateway establishes a communication connection with a client, acquire a security alliance established between the first distributed gateway and the client, wherein the first distributed gateway belongs to N distributed gateways

102 When the first distributed gateway crashes, select, from the other distributed gateways, a second distributed gateway, which establishes a communication connection with the client

103 Send a first communication connection establishment message to the second distributed gateway, wherein the first communication connection establishment message carries the security alliance, and the first communication connection establishment message is used for indicating that the second distributed gateway establishes a communication connection with the client by means of the security alliance

(57) **Abstract:** The present application relates to the field of cloud transmission. Provided are a communication method for a virtual private network, and a related apparatus. A communication method for a virtual private network comprises: when a first distributed gateway establishes a communication connection with a client, acquiring a security alliance established between the first distributed gateway and the client; when the first distributed gateway crashes, selecting, from other distributed gateways, a second distributed gateway, which establishes a communication connection with the client; and sending a first communication connection establishment message to the second distributed gateway, wherein the first communication connection establishment message carries the security alliance, and the first communication connection establishment message is used for indicating that the second distributed gateway establishes a communication connection with the client by means of the security alliance. The technical solutions in the embodiments of the present application realize efficient communication in a virtual private network.

WO 2020/186694 A1

[见续页]

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))。

(57) 摘要：本申请涉及云传输领域，提供一种虚拟专用网络的通信方法及相关装置。一种虚拟专用网络的通信方法包括：当第一分布式网关与客户端建立通信连接时，获取第一分布式网关与客户端建立的安全联盟；当第一分布式网关宕机时，在其他分布式网关中选择与客户端建立通信连接的第二分布式网关；将第一建立通信连接消息发给第二分布式网关，其中，第一建立通信连接消息携带安全联盟，第一建立通信连接消息用于指示第二分布式网关通过安全联盟与客户端建立通信连接。本申请实施例的技术方案，实现了在虚拟专用网络中高效的通信。

一种虚拟专用网络的通信方法及相关装置

本申请要求于2019年3月15日提交中国专利局、申请号为2019101961475、申请名称为“一种虚拟专用网络的通信方法及相关装置”的中国专利申请的优先权，其部分内容通过引用结合在本申请中。

技术领域

本申请涉及云传输领域，尤其涉及一种虚拟专用网络的通信方法及相关装置。

背景技术

虚拟专用网络的功能是在公用网络上建立专用网络，进行加密通讯，实现远程访问，在企业网络中有广泛应用。目前，云计算厂商使用的虚拟专用网络方案是主备的方式，主链路传输数据的时候备链路不参与，当主链路发生故障时，流量切回到备链路。

目前在虚拟专用网络中，利用加密技术在公网上封装出一个数据通讯隧道，通过 IPSec 协议在客户端与分布式网关之间提供安全通信，其中，安全联盟是客户端与分布式网关之间对通信要素的约定，例如，使用的协议、协议的封装模式、密码算法、特定数据流中保护数据的共享密钥以及密钥的生存周期等，在采用主备的方式的虚拟专用网络中，分为两种方式，一种是主链路和备链路不同步安全联盟，那么当主链路的分布式网关宕机时，已经建立的安全联盟会丢失，客户端与其他分布式网关需要重新建立安全联盟才能进行安全通信，另一种是主链路和备链路同步安全联盟，那么需要在所有的分布式网关之间定时的同步数据，这两种方式都不能实现在虚拟专用网络中高效的通信。

发明内容

本申请实施例提供一种虚拟专用网络的通信方法及相关装置，以实现在虚拟专用网络中高效的通信。

本申请第一方面提供一种虚拟专用网络的通信方法，所述虚拟专用网络包括 N 个分布式网关和集中控制器，其中，N 为正整数，包括：

当第一分布式网关与客户端建立通信连接时，获取所述第一分布式网关与所述客户端建立的安全联盟，其中，所述第一分布式网关属于所述 N 个分布式网关；

当所述第一分布式网关宕机时，在其他分布式网关中选择与所述客户端建立通信连接的第二分布式网关；

将第一建立通信连接消息发给所述第二分布式网关，其中，所述第一建立通信连接消息携带所述安全联盟，所述第一建立通信连接消息用于指示所述第二分布式网关通过所述安全联盟与所述客户端建立通信连接。

本申请第二方面提供了一种虚拟专用网络的通信装置，包括：

获取模块，用于当第一分布式网关与客户端建立通信连接时，获取所述第一分布式网关与所述客户端建立的安全联盟，其中，所述第一分布式网关属于所述 N 个分布式网关；

选择模块，用于当所述第一分布式网关宕机时，在其他分布式网关中选择与所述客户端建立通信连接的第二分布式网关；

发送模块，用于将第一建立通信连接消息发给所述第二分布式网关，其中，所述第一建立通信连接消息携带所述安全联盟，所述第一建立通信连接消息用于指示所述第二分布式网关通过所述安全联盟与所述客户端建立通信连接。

本申请第三方面提供了一种虚拟专用网络的电子设备，所述电子设备包括处理器、存储器、通信接口以及一个或多个程序，其中，所述一个或多个程序被存储在所述存储器中，并且被配置由所述处理器执行，所述程序包括用于执行本申请第一方面任一方法中的步骤的指令。

本申请第四方面提供了一种计算机可读存储介质，所述计算机可读存储介质存储有计算机程序，所述计算机程序被处理器执行以实现本申请第一方面任一方法中所描述的部分或全部步骤。

可以看到，上述技术方案中，不需要在第一分布式网关与第二分布式网关之间同步安全联盟，造成资源浪费，也不需要第二分布式网关与客户端重新建立安全联盟，实现了在虚拟专用网络中高效的通信。

附图说明

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

图 1 为本申请实施例提供的一种虚拟专用网络的通信方法的流程图；

图 2 为本申请实施例提供的另一种虚拟专用网络的通信方法的流程图；

图 3 为本申请实施例提供的另一种虚拟专用网络的通信方法的流程图；

图 4 为本申请实施例提供的第一环形哈希空间的示意图；

图 5 为本申请实施例提供的第二环形哈希空间的示意图；

图 6 为本申请实施例提供的一种虚拟专用网络的通信装置的示意图；

图 7 为本申请实施例涉及的硬件运行环境的电子设备结构示意图。

具体实施方式

本申请实施例提供的虚拟专用网络的通信方法及相关装置，以实现在虚拟专用网络中高效的通信。

为了使本技术领域的人员更好地理解本申请方案，下面将结合本申请实施例中的附图，对本申请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申请一部分的实施例，而不是全部的实施例。基于本申请中的实施例，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，都应当属于本申请保护的范围。

以下分别进行详细说明。

本申请的实施例中，虚拟专用网络包括 N 个分布式网关和集中控制器，其中，N 为正整数，集中控制器用于控制虚拟专用网络的运行。

首先参见图 1，图 1 为本申请的一个实施例提供的一种虚拟专用网络的通信方法的流程图。其中，如图 1 所示，本申请的一个实施例提供的一种虚拟专用网络的通信方法可以包括：

101、当第一分布式网关与客户端建立通信连接时，获取所述第一分布式网关与所述客户端建立的安全联盟，其中，所述第一分布式网关属于所述 N 个分布式网关。

第一分布式网关与客户端通过 IPSec 协议建立安全的通信连接，IPSec 协议是 IETF（Internet Engineering Task Force）制定的一系列协议，为 IP 数据报提供了高质量的安全性，保证了数据报在网络上传输时的私有性和完整性，其中，安全联盟是第一分布式网关与客户端之间对通信要素的约定，包括使用认证头协议（AH，Authentication Header）还是封装安全载荷协议（ESP，Encapsulating Security Payload）还是两者结合，协议的封装模式使用传输模式还是隧道模式，密码算法使用 DES 还是 3DES 还是其他密码算法，特定数据流中保护数据的共享密钥以及密钥的生存周期等。

可选的，集中控制器在获取第一分布式网关与客户端建立的安全联盟之前，还包括：

集中控制器获取客户端的客户端标识，对客户端标识通过哈希算法进行处理以得到客户端标识的哈希值，根据客户端标识的哈希值在 N 个分布式网关中选择与客户端建立通信连接的第一分布式网关。

可选的，集中控制器根据客户端标识的哈希值在 N 个分布式网关中选择与客户端建立通信连接的第一分布式网关包括：

集中控制器获取 N 个分布式网关的 N 个分布式网关标识，其中，N 个分布式网关与 N 个分布式网关标识一一对应，对 N 个分布式网关标识通过哈希算法进行处理以得到 N 个哈希值，其中，N 个分布式网关标识与 N 个哈希值一一对应，将 N 个哈希值映射到第一环形哈希空间中。

集中控制器将客户端标识的哈希值映射到第一环形哈希空间中，根据客户端标识的哈希值在第一环形哈希空间中的位置从 N 个哈希值中选择第一哈希值，确定与第一哈希值对应的分布式网关为第一分布式网关。

可选的，集中控制器根据客户端标识的哈希值在 N 个分布式网关中选择与客户端建立通信连接的第一分布式网关包括：

集中控制器获取 N 个分布式网关的 N 个分布式网关标识，其中，N 个分

布式网关与 N 个分布式网关标识一一对应，对 N 个分布式网关标识通过带权重的哈希算法进行处理以得到 N 个带权重的哈希值，其中，N 个分布式网关标识与 N 个带权重的哈希值一一对应，将 N 个带权重的哈希值映射到第二环形哈希空间中以得到 M 个虚拟节点，其中，M 为不小于 N 的正整数，带权重越大的哈希值对应的分布式网关在第二环形哈希空间中对应的虚拟节点越多。

集中控制器将客户端标识的哈希值映射到第二环形哈希空间中，根据客户端标识的哈希值在第二环形哈希空间中的位置从 M 个虚拟节点中选择第一虚拟节点，确定与第一虚拟节点对应的分布式网关为第一分布式网关。

基于上述示例，在一个可能的示例中，对 N 个分布式网关标识通过带权重的哈希算法进行处理以得到 N 个带权重的哈希值之前，还包括：

分别获取 N 个分布式网关的 N 个转发流量能力，N 个分布式网关与 N 个转发流量能力一一对应；根据 N 个转发流量能力确定 N 个分布式网关的权重，转发流量能力大的分布式网关的权重大于转发流量能力小的分布式网关的权重；根据 N 个分布式网关的权重设置 N 个分布式网关标识的权重。

具体的，不同分布式网关的转发流量能力不同，有些分布式网关的转发流量能力较强，有些分布式网关的转发流量能力较弱，客户端与转发流量能力较强的分布式网关建立连接时，可以提高客户端的数据传输速度，集中控制器分别获取 N 个分布式网关的 N 个转发流量能力，根据 N 个转发流量能力确定 N 个分布式网关的权重，其中，转发流量能力大的分布式网关的权重大于转发流量能力小的分布式网关的权重，即，转发流量能力越大的分布式网关的权重越大，转发流量能力越小的分布式网关的权重越小，然后根据分布式网关的权重设置分布式网关标识的权重，这样，集中控制器对 N 个分布式网关标识通过带权重的哈希算法进行处理以得到 N 个带权重的哈希值，分布式网关标识的权重越大，则通过哈希算法处理得到的哈希值的权重也越大，将 N 个带权重的哈希值映射到第二环形哈希空间中以得到 M 个虚拟节点，其中，M 为不小于 N 的正整数，带权重越大的哈希值对应的分布式网关在第二环形哈希空间中对应的虚拟节点越多，即，带权重越大的哈希值对应的分布式网关在第二环形哈希空间中的范围越大，因此将客户端映射到第二环形哈希空间后，选择带权重越大的哈希值对应的分布式网关的可能性更大，即选择转发流量能力较强的分布式网关的可能性越大，客户端与转发流量能力较强的分布式网关建立连接时，可以提高客户端的数据传输速度，实现单个分布式网关的高可用性。

进一步可选的，集中控制器获取了第一分布式网关与客户端建立的安全联盟后，将该安全联盟与该客户端标识关联存储在集中控制器中，同一个分布式网关可以与多个客户端建立连接，多个分布式网关与多个客户端建立连接，这样，集中控制器获取了多个其他分布式网关与其他客户端建立的安全联盟并存储通过存储安全联盟与客户端标识的关联关系，可以根据客户端标识对安全联盟做出区分。

102、当所述第一分布式网关宕机时，在其他分布式网关中选择与所述客户端建立通信连接的第二分布式网关。

在一个可能的示例中，当第一分布式网关宕机时，集中控制器在其他分布式网关中选择与客户端重新建立通信连接的第二分布式网关，包括：

集中控制器将第一哈希值从第一环形哈希空间中删除，根据客户端标识的哈希值在第一环形哈希空间中的位置从其他哈希值中选择第二哈希值，确定与第二哈希值对应的分布式网关为第二分布式网关。

具体的，第一分布式网关宕机时，客户端无法再与第一分布式网关建立通信连接，此时客户端需要与其他分布式网关建立通信连接，从而继续发送数据，集中控制器确定第一分布式网关对应的第一哈希值，将第一哈希值从第一环形哈希空间中删除，这样第一环形哈希空间中的其他哈希值对应的都是处于工作状态的分布式网关，然后根据客户端标识的哈希值在第一环形哈希空间中的位置从其他哈希值中选择第二哈希值，选择的方式可以是按照顺时针方向选择离客户端标识的哈希值最近位置的第二哈希值，确定第二哈希值对应的分布式网关，即为第二分布式网关。

基于上述示例，集中控制器在其他分布式网关中选择与客户端重新建立通信连接的第二分布式网关之后，包括：

集中控制器获取第二分布式网关的转发流量大小，若第二分布式网关的转发流量大小超过预设转发流量阈值，则将第二哈希值从第一环形哈希空间中删除。集中控制器根据客户端标识的哈希值在第一环形哈希空间中的位置从其他哈希值中选择第三哈希值，确定与第三哈希值对应的分布式网关为与客户端建立通信连接的第三分布式网关。集中控制器将第二建立通信连接消息发给第三分布式网关，其中，第二建立通信连接消息携带安全联盟，第二建立通信连接消息用于指示第三分布式网关通过安全联盟与客户端建立通信连接。

在一个可能的示例中，当第一分布式网关宕机时，集中控制器在其他分布式网关中选择与客户端重新建立通信连接的第二分布式网关，包括：

集中控制器确定第一分布式网关的第一分布式网关标识，确定第一分布式网关标识对应的带权重的哈希值，确定第一分布式网关标识对应的带权重的哈希值映射得到的至少一个虚拟节点；集中控制器将该至少一个虚拟节点从第二环形哈希空间中删除，根据客户端标识的哈希值在第二环形哈希空间中的位置从其他虚拟节点中选择第二虚拟节点；集中控制器确定与第二虚拟节点对应的分布式网关为第二分布式网关。

具体的，第一分布式网关宕机时，客户端无法再与第一分布式网关建立通信连接，此时客户端需要与其他分布式网关建立通信连接，从而继续发送数据，集中控制器确定第一分布式网关的第一分布式网关标识，确定第一分布式网关标识对应的带权重的哈希值，进一步确定第一分布式网关标识对应的带权重的哈希值映射得到的至少一个虚拟节点，其中，如果第一分布式网关的权重越大，

那么对应的虚拟节点也越多，将该至少一个虚拟节点从第二环形哈希空间中删除，这样第二环形哈希空间中的其他虚拟节点对应的都是处于工作状态的分布式网关，然后根据客户端标识的哈希值在第二环形哈希空间中的位置从其他虚拟节点中选择第二虚拟节点，选择的方式可以是按照顺时针方向选择离客户端标识的哈希值最近位置的第二虚拟节点，确定第二虚拟节点后，确定与第二虚拟节点对应的分布式网关，即为第二分布式网关。

基于上述示例，集中控制器在其他分布式网关中选择与客户端重新建立通信连接的第二分布式网关之后，包括：

集中控制器获取第二分布式网关的转发流量大小，若第二分布式网关的转发流量大小超过预设转发流量阈值，则确定第二分布式网关的第二分布式网关标识，确定第二分布式网关标识对应的带权重的哈希值，确定第二分布式网关标识对应的带权重的哈希值映射得到的至少一个虚拟节点；集中控制器将该至少一个虚拟节点从第二环形哈希空间中删除。集中控制器根据客户端标识的哈希值在第二环形哈希空间中的位置从其他虚拟节点中选择第三虚拟节点，确定与第三虚拟节点对应的分布式网关为与客户端建立通信连接的第三分布式网关。集中控制器将第二建立通信连接消息发给第三分布式网关，其中，第二建立通信连接消息携带安全联盟，第二建立通信连接消息用于指示第三分布式网关通过安全联盟与客户端建立通信连接。

103、将第一建立通信连接消息发给所述第二分布式网关，其中，所述第一建立通信连接消息携带所述安全联盟，所述第一建立通信连接消息用于指示所述第二分布式网关通过所述安全联盟与所述客户端建立通信连接。

集中控制器在将第一建立通信连接消息发给第二分布式网关之前，查找与客户端的客户端标识关联存储的安全联盟。集中控制器将第一建立通信连接消息发给第二分布式网关，其中，该第一建立通信连接消息携带该安全联盟。第二分布式网关接收该第一建立通信连接消息时，通过该安全联盟与客户端建立通信连接。

可选的，当第二分布式网关与客户端完成通信时，第二分布式网关向集中控制器发送通信结束消息，通信结束消息携带客户端的客户端标识，集中控制器接收到通信结束消息时，根据客户端标识查找与客户端标识关联存储的安全联盟，然后集中控制器将该安全联盟从安全联盟数据库中删除。这样，可以避免无效的安全联盟存储在集中控制器中，造成集中控制器的存储资源浪费。

进一步可选的，在第二分布式网关与客户端进行通信的过程中，集中控制器按照预设周期获取第一分布式网关的状态，当第一分布式网关的状态为工作时，将第一哈希值添加到所述第一环形空间中。集中控制器将切断通信连接指令发给第二分布式网关，其中，该切断通信连接指令用于指示第二分布式网关与所述客户端切断通信连接。集中控制器将第三建立通信连接消息发给第一分布式网关，其中，该第三建立通信连接消息携带安全联盟，该第三建立通信连

接消息用于指示第一分布式网关通过该安全联盟与客户端重新建立通信连接。

参见图 2，图 2 为本申请的另一个实施例提供的另一种虚拟专用网络的通信方法的流程图。其中，如图 2 所示，本申请的另一个实施例提供的另一种虚拟专用网络的通信方法可以包括：

201、集中控制器获取客户端的客户端标识，对客户端标识通过哈希算法进行处理以得到客户端标识的哈希值。

202、集中控制器根据客户端标识的哈希值在 N 个分布式网关中选择与客户端建立通信连接的第一分布式网关。

可选的，集中控制器根据客户端标识的哈希值在 N 个分布式网关中选择与客户端建立通信连接的第一分布式网关包括：

集中控制器获取 N 个分布式网关的 N 个分布式网关标识，其中，N 个分布式网关与 N 个分布式网关标识一一对应，分布式网关标识包括分布式网关的 IP 地址或者主机名。

对 N 个分布式网关标识通过一致性哈希算法进行处理以得到 N 个哈希值，其中，N 个分布式网关标识与 N 个哈希值一一对应，将 N 个哈希值映射到第一环形哈希空间中，第一环形哈希空间是一个虚拟的圆环，按顺时针方向组织。

集中控制器将客户端标识的哈希值映射到第一环形哈希空间中，根据客户端标识的哈希值在第一环形哈希空间中的位置从 N 个哈希值中选择第一哈希值，具体为，根据客户端标识的哈希值在第一环形哈希空间中的位置沿环顺时针方向寻找到的第一个哈希值，即为第一哈希值，确定与第一哈希值对应的分布式网关为第一分布式网关。

203、当第一分布式网关与客户端建立通信连接时，获取第一分布式网关与所述客户端建立的安全联盟。

第一分布式网关与客户端通过 IPSec 协议建立安全的通信连接，IPSec 协议是 IETF（Internet Engineering Task Force）制定的一系列协议，为 IP 数据报提供了高质量的安全性，保证了数据报在网络上传输时的私有性和完整性，其中，安全联盟是第一分布式网关与客户端之间对通信要素的约定，包括使用认证头协议（AH，Authentication Header）还是封装安全载荷协议（ESP，Encapsulating Security Payload）还是两者结合，协议的封装模式使用传输模式还是隧道模式，密码算法使用 DES 还是 3DES 还是其他密码算法，特定数据流中保护数据的共享密钥以及密钥的生存周期等。

204、集中控制器存储该安全联盟。

集中控制器获取了第一分布式网关与客户端建立的安全联盟后，将该安全联盟与该客户端标识关联存储在集中控制器中，这样，当集中控制器获取了多个其他分布式网关与其他客户端建立的安全联盟时，可以根据客户端标识对安全联盟做出区分，通过客户端标识可以获得与客户端标识关联存储的安全联盟。

205、当第一分布式网关宕机时，集中控制器将第一哈希值从第一环形哈

希空间中删除。

集中控制器获取第一分布式网关的第一分布式网关标识，对第一分布式网关标识通过哈希算法进行处理以得到第一哈希值，将第一哈希值从第一环形哈希空间中删除。

206、集中控制器从（N-1）个分布式网关中选择与客户端建立通信连接的第二分布式网关。

集中控制器根据客户端标识的哈希值在第一环形哈希空间中的位置从（N-1）个哈希值中选择第二哈希值，确定与第二哈希值对应的分布式网关为第二分布式网关。

具体的，第一分布式网关宕机时，客户端无法再与第一分布式网关建立通信连接，此时客户端需要与其他分布式网关建立通信连接，从而继续发送数据，集中控制器确定第一分布式网关对应的第一哈希值，将第一哈希值从第一环形哈希空间中删除，这样第一环形哈希空间中的其他哈希值对应的都是处于工作状态的分布式网关，然后根据客户端标识的哈希值在第一环形哈希空间中的位置从其他哈希值中选择第二哈希值，选择的方式可以是按照顺时针方向选择离客户端标识的哈希值最近位置的第二哈希值，确定第二哈希值对应的分布式网关，即为第二分布式网关。

207、集中控制器获取该安全联盟。

可选的，由于集中控制器中存储有多个安全联盟，所以集中控制器查找是否存在与客户端标识匹配的第一客户端标识，若有，则集中控制器获取与第一客户端标识关联存储的安全联盟，即为原先第一分布式网关与客户端建立的安全联盟，若没有，则第二分布式网关需要重新与客户端建立安全联盟，才能进行安全通信。

208、集中控制器将第一建立通信连接消息发给第二分布式网关，其中，第一建立通信连接消息携带该安全联盟。

209、第二分布式网关通过安全联盟与客户端建立通信连接。

可选的，当第二分布式网关与客户端完成通信时，第二分布式网关向集中控制器发送通信结束消息，通信结束消息携带客户端的客户端标识，集中控制器接收到通信结束消息时，根据客户端标识查找与客户端标识关联存储的安全联盟，然后集中控制器将该安全联盟从安全联盟数据库中删除。这样，可以避免无效的安全联盟存储在集中控制器中，造成集中控制器的存储资源浪费。

可选的，在第二分布式网关与客户端进行通信的过程中，集中控制器按照预设周期获取第一分布式网关的状态，该预设周期可以是 10 分钟、30 分钟、60 分钟等。

当第一分布式网关的状态仍然为宕机时，第二分布式网关保持与客户端的通信连接。当第一分布式网关的状态为工作时，将第一哈希值添加到所述第一环形空间中。

集中控制器将切断通信连接指令发给第二分布式网关，其中，该切断通信连接指令用于指示第二分布式网关与所述客户端切断通信连接。

集中控制器将第三建立通信连接消息发给第一分布式网关，其中，该第三建立通信连接消息携带安全联盟，该第三建立通信连接消息用于指示第一分布式网关通过该安全联盟与客户端建立通信连接。

参见图 3，图 3 为本申请的另一个实施例提供的另一种虚拟专用网络的通信方法的流程图。其中，如图 3 所示，本申请的另一个实施例提供的另一种虚拟专用网络的通信方法可以包括：

301、集中控制器获取客户端的客户端标识，对客户端标识通过哈希算法进行处理以得到客户端标识的哈希值。

302、集中控制器根据客户端标识的哈希值在 N 个分布式网关中选择与客户端建立通信连接的第一分布式网关。

可选的，集中控制器根据客户端标识的哈希值在 N 个分布式网关中选择与客户端建立通信连接的第一分布式网关包括：

集中控制器获取 N 个分布式网关的 N 个分布式网关标识，其中，N 个分布式网关与 N 个分布式网关标识一一对应，分布式网关标识包括分布式网关的 IP 地址或者主机名。对 N 个分布式网关标识通过一致性哈希算法进行处理以得到 N 个哈希值，其中，N 个分布式网关标识与 N 个哈希值一一对应，将 N 个哈希值映射到第一环形哈希空间中，第一环形哈希空间是一个虚拟的圆环，按顺时针方向组织。集中控制器将客户端标识的哈希值映射到第一环形哈希空间中，根据客户端标识的哈希值在第一环形哈希空间中的位置从 N 个哈希值中选择第一哈希值，具体为，根据客户端标识的哈希值在第一环形哈希空间中的位置沿环顺时针方向寻找到的第一个哈希值，即为第一哈希值，确定与第一哈希值对应的分布式网关为第一分布式网关。

可选的，集中控制器根据客户端标识的哈希值在 N 个分布式网关中选择与客户端建立通信连接的第一分布式网关包括：

集中控制器获取 N 个分布式网关的 N 个分布式网关标识，其中，N 个分布式网关与 N 个分布式网关标识一一对应，分布式网关标识包括分布式网关的 IP 地址或者主机名。对 N 个分布式网关标识通过带权重的哈希算法进行处理以得到 N 个带权重的哈希值，其中，N 个分布式网关标识与 N 个带权重的哈希值一一对应，将 N 个带权重的哈希值映射到第二环形哈希空间中以得到 M 个虚拟节点，其中，M 为不小于 N 的正整数，第二环形哈希空间是一个虚拟的圆环，按顺时针方向组织，转发能力越强的分布式网关带的权重越大，由于带权重越大的哈希值对应的分布式网关在第二环形哈希空间中对应的虚拟节点越多，所以客户端映射到带权重越大的哈希值对应的分布式网关的几率越大，即客户端与转发能力较强的分布式网关建立通信连接的几率较大。集中控制器将客户端标识的哈希值映射到第二环形哈希空间中，根据客户端标识的哈

希值在第二环形哈希空间中的位置从 M 个虚拟节点中选择第一虚拟节点，确定与第一虚拟节点对应的分布式网关为第一分布式网关。

303、当第一分布式网关与客户端建立通信连接时，获取第一分布式网关与所述客户端建立的安全联盟。

第一分布式网关与客户端通过 IPSec 协议建立安全的通信连接，IPSec 协议是 IETF（Internet Engineering Task Force）制定的一系列协议，为 IP 数据报提供了高质量的安全性，保证了数据报在网络上传输时的私有性和完整性，其中，安全联盟是第一分布式网关与客户端之间对通信要素的约定，包括使用认证头协议（AH，Authentication Header）还是封装安全载荷协议（ESP，Encapsulating Security Payload）还是两者结合，协议的封装模式使用传输模式还是隧道模式，密码算法使用 DES 还是 3DES 还是其他密码算法，特定数据流中保护数据的共享密钥以及密钥的生存周期等。

304、集中控制器存储该安全联盟。

集中控制器获取了第一分布式网关与客户端建立的安全联盟后，将该安全联盟与该客户端标识关联存储在集中控制器中，这样，当集中控制器获取了多个其他分布式网关与其他客户端建立的安全联盟时，可以根据客户端标识对安全联盟做出区分，通过客户端标识可以获得与客户端标识关联存储的安全联盟。

305、当第一分布式网关宕机时，集中控制器从（N-1）个分布式网关中选择与客户端建立通信连接的第二分布式网关。

在一个可能的示例中，当第一分布式网关宕机时，集中控制器获取第一分布式网关的第一分布式网关标识，对第一分布式网关标识通过哈希算法进行处理以得到第一哈希值，将第一哈希值从第一环形哈希空间中删除。

集中控制器根据客户端标识的哈希值在第一环形哈希空间中的位置从（N-1）个哈希值中选择第二哈希值，确定与第二哈希值对应的分布式网关为第二分布式网关。

在一个可能的示例中，当第一分布式网关宕机时，集中控制器在其他分布式网关中选择与客户端重新建立通信连接的第二分布式网关，包括：

集中控制器确定第一分布式网关的第一分布式网关标识，确定第一分布式网关标识对应的带权重的哈希值，确定第一分布式网关标识对应的带权重的哈希值映射得到的至少一个虚拟节点；集中控制器将该至少一个虚拟节点从第二环形哈希空间中删除，根据客户端标识的哈希值在第二环形哈希空间中的位置从其他虚拟节点中选择第二虚拟节点；集中控制器确定与第二虚拟节点对应的分布式网关为第二分布式网关。

306、集中控制器获取第二分布式网关的转发流量大小。

307、若第二分布式网关的转发流量大小超过预设转发流量阈值，则集中控制器从（N-2）个分布式网关中选择与客户端建立通信连接的第三分布式网关。

若第二分布式网关的转发流量大小超过预设转发流量阈值，如果第二分布式网关与客户端建立通信连接，会造成网络拥塞，影响第二分布式网关的流量转发效率，并且也会造成该客户端的流量不能及时转发出去，网络延时太大，所以集中控制器需要从（N-2）个分布式网关中选择与客户端建立通信连接的第三分布式网关。

在一个可能的示例中，集中控制器从（N-2）个分布式网关中选择与客户端建立通信连接的第三分布式网关的方法可以是：

获取第二分布式网关的第二分布式网关标识，对第二分布式网关标识通过哈希算法进行处理以得到第二哈希值，将第二哈希值从第一环形哈希空间中删除，集中控制器根据客户端标识的哈希值在第一环形哈希空间中的位置从（N-2）个哈希值中选择第三哈希值，确定与第三哈希值对应的分布式网关为与客户端建立通信连接的第三分布式网关。

308、集中控制器获取该安全联盟。

309、集中控制器将第二建立通信连接消息发给第三分布式网关，其中，第二建立通信连接消息携带安全联盟。

310、第三分布式网关通过安全联盟与客户端建立通信连接。

可选的，当第三分布式网关与客户端完成通信时，第三分布式网关向集中控制器发送通信结束消息，通信结束消息携带客户端的客户端标识，集中控制器接收到通信结束消息时，根据客户端标识查找与客户端标识关联存储的安全联盟，然后集中控制器将该安全联盟从安全联盟数据库中删除。这样，可以避免无效的安全联盟存储在集中控制器中，造成集中控制器的存储资源浪费。

可选的，在第三分布式网关与客户端进行通信的过程中，集中控制器按照预设周期获取第一分布式网关的状态，该预设周期可以是 10 分钟、30 分钟、60 分钟等。

当第一分布式网关的状态仍然为宕机时，第三分布式网关保持与客户端的通信连接。当第一分布式网关的状态为工作时，将第一哈希值添加到所述第一环形空间中。

集中控制器将切断通信连接指令发给第三分布式网关，其中，该切断通信连接指令用于指示第三分布式网关与所述客户端切断通信连接。集中控制器将第三建立通信连接消息发给第一分布式网关，其中，该第三建立通信连接消息携带安全联盟，该第三建立通信连接消息用于指示第一分布式网关通过该安全联盟与客户端建立通信连接。

参见图 4，图 4 为本申请的一个实施例提供的一种第一环形哈希空间的示意图。其中，如图 4 所示，将 N 个分布式网关和客户端映射到第一环形哈希空间中，N 个分布式网关分别为分布式网关 1、分布式网关 2、分布式网关 N 等，按照顺时针方向，距离客户端最近位置的分布式网关为第一分布式网关，即可以确定客户端与第一分布式网关建立通信连接。

参见图 5，图 5 为本申请的一个实施例提供的一种第二环形哈希空间的示意图。其中，如图 5 所示，将 N 个分布式网关和客户端映射到第二环形哈希空间中，得到 M 个虚拟节点和客户端在第二环形哈希空间中的位置，M 个虚拟节点分别为虚拟节点 1、虚拟节点 2、虚拟节点 3、虚拟节点 4、虚拟节点 M 等，按照顺时针方向，距离客户端最近位置的为第一虚拟节点，即可以确定客户端与第一虚拟节点对应的分布式网关建立通信连接。

参见图 6，图 6 为本申请的另一个实施例提供的一种虚拟专用网络的通信装置的示意图。其中，如图 6 所示，本申请的另一个实施例提供的一种虚拟专用网络的通信装置可以包括：

获取模块 601，用于当第一分布式网关与客户端建立通信连接时，获取所述第一分布式网关与所述客户端建立的安全联盟，其中，所述第一分布式网关属于所述 N 个分布式网关。

选择模块 602，用于当所述第一分布式网关宕机时，在其他分布式网关中选择与所述客户端建立通信连接的第二分布式网关。

发送模块 603，用于将第一建立通信连接消息发给所述第二分布式网关，其中，所述第一建立通信连接消息携带所述安全联盟，所述第一建立通信连接消息用于指示所述第二分布式网关通过所述安全联盟与所述客户端建立通信连接。

本申请虚拟专用网络的通信装置的具体实施可参见上述虚拟专用网络的通信方法的各实施例，在此不做赘述。

参见图 7，图 7 为本申请的实施例涉及的硬件运行环境的电子设备结构示意图。其中，如图 7 所示，本申请的实施例涉及的硬件运行环境的电子设备可以包括：

处理器 701，例如 CPU。

存储器 702，可选的，存储器可以为高速 RAM 存储器，也可以是稳定的存储器，例如磁盘存储器。

通信接口 703，用于实现处理器 701 和存储器 702 之间的连接通信。

本领域技术人员可以理解，图 7 中示出的虚拟专用网络的通信电子设备的结构并不构成对虚拟专用网络的通信电子设备的限定，可以包括比图示更多或更少的部件，或者组合某些部件，或者不同的部件布置。

如图 7 所示，存储器 702 中可以包括操作系统、网络通信模块以及虚拟专用网络的通信程序。操作系统是管理和控制虚拟专用网络的通信电子设备硬件和软件资源的程序，支持虚拟专用网络的通信程序以及其他软件或程序的运行。网络通信模块用于实现存储器 702 内部各组件之间的通信，以及与虚拟专用网络的通信电子设备中其他硬件和软件之间通信。

在图 7 所示的虚拟专用网络的通信电子设备中，处理器 701 用于执行存储器 702 中存储的虚拟专用网络的通信程序，实现以下步骤：

当第一分布式网关与客户端建立通信连接时，获取所述第一分布式网关与所述客户端建立的安全联盟，其中，所述第一分布式网关属于所述 N 个分布式网关。

当所述第一分布式网关宕机时，在其他分布式网关中选择与所述客户端建立通信连接的第二分布式网关。

将第一建立通信连接消息发给所述第二分布式网关，其中，所述第一建立通信连接消息携带所述安全联盟，所述第一建立通信连接消息用于指示所述第二分布式网关通过所述安全联盟与所述客户端建立通信连接。

本申请虚拟专用网络的通信电子设备的具体实施可参见上述虚拟专用网络的通信方法的各实施例，在此不做赘述。

本申请的另一个实施例提供了一种计算机可读存储介质，计算机可读存储介质存储有计算机程序，计算机程序被处理器执行以实现以下步骤：

当第一分布式网关与客户端建立通信连接时，获取所述第一分布式网关与所述客户端建立的安全联盟，其中，所述第一分布式网关属于所述 N 个分布式网关。

当所述第一分布式网关宕机时，在其他分布式网关中选择与所述客户端建立通信连接的第二分布式网关。

将第一建立通信连接消息发给所述第二分布式网关，其中，所述第一建立通信连接消息携带所述安全联盟，所述第一建立通信连接消息用于指示所述第二分布式网关通过所述安全联盟与所述客户端建立通信连接。

本申请计算机可读存储介质的具体实施可参见上述虚拟专用网络的通信方法的各实施例，在此不做赘述。

还需要说明的是，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，本申请并不受所描述的动作顺序的限制，因为依据本申请，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申请所必须的。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。

以上所述，以上实施例仅用以说明本申请的技术方案，而非对其限制；尽管参照前述实施例对本申请进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分技术特征进行等同替换；而这些修改或者替换，并不使相应技术方案的本质脱离本申请各实施例技术方案的范围。

权 利 要 求

1、一种虚拟专用网络的通信方法，其特征在于，所述虚拟专用网络包括 N 个分布式网关和集中控制器，其中，N 为正整数，包括：

当第一分布式网关与客户端建立通信连接时，获取所述第一分布式网关与所述客户端建立的安全联盟，其中，所述第一分布式网关属于所述 N 个分布式网关；

当所述第一分布式网关宕机时，在其他分布式网关中选择与所述客户端建立通信连接的第二分布式网关；

将第一建立通信连接消息发给所述第二分布式网关，其中，所述第一建立通信连接消息携带所述安全联盟，所述第一建立通信连接消息用于指示所述第二分布式网关通过所述安全联盟与所述客户端建立通信连接。

2、根据权利要求 1 所述的方法，其特征在于，所述获取所述第一分布式网关与所述客户端建立的安全联盟之前，所述方法还包括：

获取所述客户端的客户端标识；

对所述客户端标识通过哈希算法进行处理以得到所述客户端标识的哈希值；

根据所述客户端标识的哈希值在所述 N 个分布式网关中选择与所述客户端建立通信连接的所述第一分布式网关。

3、根据权利要求 2 所述的方法，其特征在于，所述根据所述客户端标识的哈希值在所述 N 个分布式网关中选择与所述客户端建立通信连接的所述第一分布式网关，包括：

获取所述 N 个分布式网关的 N 个分布式网关标识，其中，所述 N 个分布式网关与所述 N 个分布式网关标识一一对应；

对所述 N 个分布式网关标识通过哈希算法进行处理以得到 N 个哈希值，其中，所述 N 个分布式网关标识与所述 N 个哈希值一一对应；

将所述 N 个哈希值映射到第一环形哈希空间中；

将所述客户端标识的哈希值映射到所述第一环形哈希空间中；

根据所述客户端标识的哈希值在所述第一环形哈希空间中的位置从所述 N 个哈希值中选择第一哈希值；

确定与所述第一哈希值对应的分布式网关为所述第一分布式网关。

4、根据权利要求 2 所述的方法，其特征在于，所述根据所述客户端标识的哈希值在所述 N 个分布式网关中选择与所述客户端建立通信连接的所述第一分布式网关，包括：

获取所述 N 个分布式网关的 N 个分布式网关标识，其中，所述 N 个分布式网关与所述 N 个分布式网关标识一一对应；

对所述 N 个分布式网关标识通过带权重的哈希算法进行处理以得到 N 个带权重的哈希值，其中，所述 N 个分布式网关标识与所述 N 个带权重的哈希

值一一对应；

将所述 N 个带权重的哈希值映射到第二环形哈希空间中以得到 M 个虚拟节点，其中，M 为不小于 N 的正整数；

将所述客户端标识的哈希值映射到所述第二环形哈希空间中；

根据所述客户端标识的哈希值在所述第二环形哈希空间中的位置从所述 M 个虚拟节点中选择第一虚拟节点；

确定与所述第一虚拟节点对应的分布式网关为所述第一分布式网关。

5、根据权利要求 4 所述的方法，其特征在于，所述对所述 N 个分布式网关标识通过带权重的哈希算法进行处理以得到 N 个带权重的哈希值之前，所述方法还包括：

分别获取所述 N 个分布式网关的 N 个转发流量能力，所述 N 个分布式网关与所述 N 个转发流量能力一一对应；

根据所述 N 个转发流量能力确定所述 N 个分布式网关的权重，转发流量能力大的分布式网关的权重大于转发流量能力小的分布式网关的权重；

根据所述 N 个分布式网关的权重设置所述 N 个分布式网关标识的权重。

6、根据权利要求 3 所述的方法，其特征在于，所述在其他分布式网关中选择与所述客户端建立通信连接的第二分布式网关包括：

将所述第一哈希值从所述第一环形哈希空间中删除；

根据所述客户端标识的哈希值在所述第一环形哈希空间中的位置从其他哈希值中选择第二哈希值；

确定与所述第二哈希值对应的分布式网关为所述第二分布式网关。

7、根据权利要求 4 所述的方法，其特征在于，所述在其他分布式网关中选择与所述客户端建立通信连接的第二分布式网关包括：

确定所述第一分布式网关的第一分布式网关标识；

确定所述第一分布式网关标识对应的带权重的哈希值；

确定所述第一分布式网关标识对应的带权重的哈希值映射得到的至少一个虚拟节点；

将所述至少一个虚拟节点从所述第二环形哈希空间中删除；

根据所述客户端标识的哈希值在所述第二环形哈希空间中的位置从其他虚拟节点中选择第二虚拟节点；

确定与所述第二虚拟节点对应的分布式网关为所述第二分布式网关。

8、根据权利要求 6 所述的方法，其特征在于，所述在其他分布式网关中选择与所述客户端建立通信连接的第二分布式网关之后，所述方法还包括：

获取所述第二分布式网关的转发流量大小；

若所述第二分布式网关的转发流量大小超过预设转发流量阈值，则将所述第二哈希值从所述第一环形哈希空间中删除；

根据所述客户端标识的哈希值在所述第一环形哈希空间中的位置从其他

哈希值中选择第三哈希值；

确定与所述第三哈希值对应的分布式网关为与所述客户端建立通信连接的第三分布式网关；

将第二建立通信连接消息发给所述第三分布式网关，其中，所述第二建立通信连接消息携带所述安全联盟，所述第二建立通信连接消息用于指示所述第三分布式网关通过所述安全联盟与所述客户端建立通信连接。

9、根据权利要求 6 所述的方法，其特征在于，所述方法还包括：

按照预设周期获取所述第一分布式网关的状态；

当所述第一分布式网关的状态为工作时，将所述第一哈希值添加到所述第一环形空间中；

将切断通信连接指令发给所述第二分布式网关，其中，所述切断通信连接指令用于指示所述第二分布式网关与所述客户端切断通信连接；

将第三建立通信连接消息发给所述第一分布式网关，其中，所述第三建立通信连接消息携带所述安全联盟，所述第三建立通信连接消息用于指示所述第一分布式网关通过所述安全联盟与所述客户端建立通信连接。

10、一种虚拟专用网络的通信装置，其特征在于，所述装置包括：

获取模块，用于当第一分布式网关与客户端建立通信连接时，获取所述第一分布式网关与所述客户端建立的安全联盟，其中，所述第一分布式网关属于所述 N 个分布式网关；

第一选择模块，用于当所述第一分布式网关宕机时，在其他分布式网关中选择与所述客户端建立通信连接的第二分布式网关；

发送模块，用于将第一建立通信连接消息发给所述第二分布式网关，其中，所述第一建立通信连接消息携带所述安全联盟，所述第一建立通信连接消息用于指示所述第二分布式网关通过所述安全联盟与所述客户端建立通信连接。

11、根据权利要求 10 所述的装置，其特征在于，所述装置还包括第二选择模块，所述第二选择模块用于：

获取所述客户端的客户端标识；

对所述客户端标识通过哈希算法进行处理以得到所述客户端标识的哈希值；

根据所述客户端标识的哈希值在所述 N 个分布式网关中选择与所述客户端建立通信连接的所述第一分布式网关。

12、根据权利要求 11 所述的装置，其特征在于，在所述根据所述客户端标识的哈希值在所述 N 个分布式网关中选择与所述客户端建立通信连接的所述第一分布式网关方面，所述第二选择模块具体用于：

获取所述 N 个分布式网关的 N 个分布式网关标识，其中，所述 N 个分布式网关与所述 N 个分布式网关标识一一对应；

对所述 N 个分布式网关标识通过哈希算法进行处理以得到 N 个哈希值，

其中，所述 N 个分布式网关标识与所述 N 个哈希值一一对应；

将所述 N 个哈希值映射到第一环形哈希空间中；

将所述客户端标识的哈希值映射到所述第一环形哈希空间中；

根据所述客户端标识的哈希值在所述第一环形哈希空间中的位置从所述 N 个哈希值中选择第一哈希值；

确定与所述第一哈希值对应的分布式网关为所述第一分布式网关。

13、根据权利要求 11 所述的装置，其特征在于，在所述根据所述客户端标识的哈希值在所述 N 个分布式网关中选择与所述客户端建立通信连接的所述第一分布式网关方面，所述第二选择模块具体用于：

获取所述 N 个分布式网关的 N 个分布式网关标识，其中，所述 N 个分布式网关与所述 N 个分布式网关标识一一对应；

对所述 N 个分布式网关标识通过带权重的哈希算法进行处理以得到 N 个带权重的哈希值，其中，所述 N 个分布式网关标识与所述 N 个带权重的哈希值一一对应；

将所述 N 个带权重的哈希值映射到第二环形哈希空间中以得到 M 个虚拟节点，其中，M 为不小于 N 的正整数；

将所述客户端标识的哈希值映射到所述第二环形哈希空间中；

根据所述客户端标识的哈希值在所述第二环形哈希空间中的位置从所述 M 个虚拟节点中选择第一虚拟节点；

确定与所述第一虚拟节点对应的分布式网关为所述第一分布式网关。

14、根据权利要求 13 所述的装置，其特征在于，所述装置还包括设置模块，所述设置模块用于：

分别获取所述 N 个分布式网关的 N 个转发流量能力，所述 N 个分布式网关与所述 N 个转发流量能力一一对应；

根据所述 N 个转发流量能力确定所述 N 个分布式网关的权重，转发流量能力大的分布式网关的权重大于转发流量能力小的分布式网关的权重；

根据所述 N 个分布式网关的权重设置所述 N 个分布式网关标识的权重。

15、根据权利要求 12 所述的装置，其特征在于，所述第一选择模块具体用于：

将所述第一哈希值从所述第一环形哈希空间中删除；

根据所述客户端标识的哈希值在所述第一环形哈希空间中的位置从其他哈希值中选择第二哈希值；

确定与所述第二哈希值对应的分布式网关为所述第二分布式网关。

16、根据权利要求 13 所述的装置，其特征在于，所述第一选择模块具体用于：

确定所述第一分布式网关的第一分布式网关标识；

确定所述第一分布式网关标识对应的带权重的哈希值；

确定所述第一分布式网关标识对应的带权重的哈希值映射得到的至少一个虚拟节点；

将所述至少一个虚拟节点从所述第二环形哈希空间中删除；

根据所述客户端标识的哈希值在所述第二环形哈希空间中的位置从其他虚拟节点中选择第二虚拟节点；

确定与所述第二虚拟节点对应的分布式网关为所述第二分布式网关。

17、根据权利要求 15 所述的装置，其特征在于，所述装置还包括第一处理模块，所述第一处理模块用于：

获取所述第二分布式网关的转发流量大小；

若所述第二分布式网关的转发流量大小超过预设转发流量阈值，则将所述第二哈希值从所述第一环形哈希空间中删除；

根据所述客户端标识的哈希值在所述第一环形哈希空间中的位置从其他哈希值中选择第三哈希值；

确定与所述第三哈希值对应的分布式网关为与所述客户端建立通信连接的第三分布式网关；

将第二建立通信连接消息发给所述第三分布式网关，其中，所述第二建立通信连接消息携带所述安全联盟，所述第二建立通信连接消息用于指示所述第三分布式网关通过所述安全联盟与所述客户端建立通信连接。

18、根据权利要求 15 所述的装置，其特征在于，所述装置还包括第二处理模块，所述第二处理模块用于：

按照预设周期获取所述第一分布式网关的状态；

当所述第一分布式网关的状态为工作时，将所述第一哈希值添加到所述第一环形空间中；

将切断通信连接指令发给所述第二分布式网关，其中，所述切断通信连接指令用于指示所述第二分布式网关与所述客户端切断通信连接；

将第三建立通信连接消息发给所述第一分布式网关，其中，所述第三建立通信连接消息携带所述安全联盟，所述第三建立通信连接消息用于指示所述第一分布式网关通过所述安全联盟与所述客户端建立通信连接。

19、一种虚拟专用网络的通信电子设备，其特征在于，所述电子设备包括处理器、存储器、通信接口以及一个或多个程序，其中，所述一个或多个程序被存储在所述存储器中，并且被配置由所述处理器执行，所述程序包括用于执行权利要求 1 至 9 任一项方法中的步骤的指令。

20、一种计算机可读存储介质，其特征在于，所述计算机可读存储介质存储有计算机程序，所述计算机程序被处理器执行以实现权利要求 1 至 7 任意一项所述的方法。

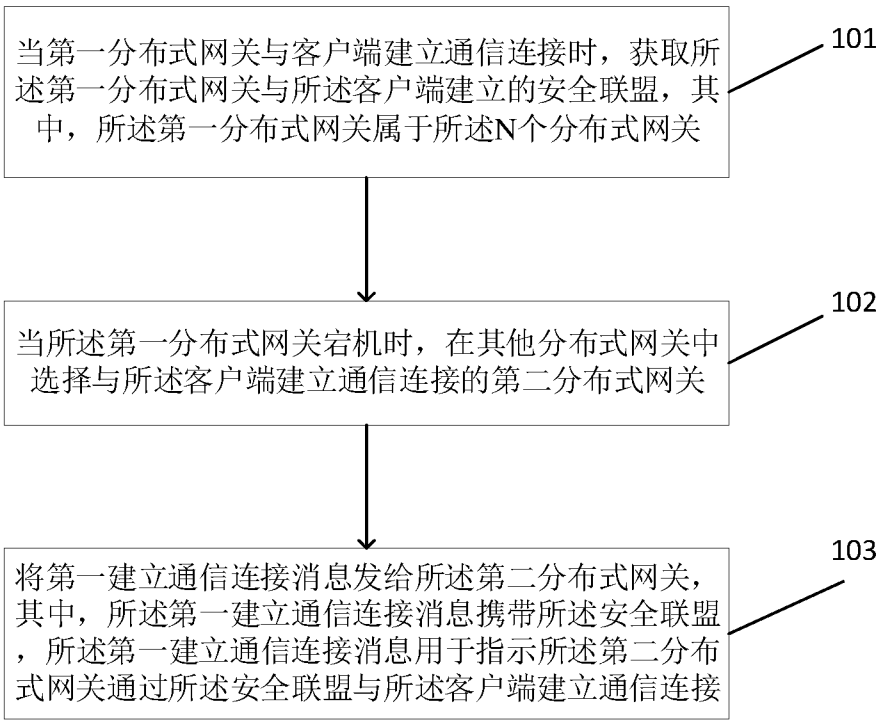
当第一分布式网关与客户端建立通信连接时，获取所述第一分布式网关与所述客户端建立的安全联盟，其中，所述第一分布式网关属于所述N个分布式网关
101
当所述第一分布式网关宕机时，在其他分布式网关中选择与所述客户端建立通信连接的第二分布式网关
102
将第一建立通信连接消息发给所述第二分布式网关，其中，所述第一建立通信连接消息携带所述安全联盟，所述第一建立通信连接消息用于指示所述第二分布式网关通过所述安全联盟与所述客户端建立通信连接
103

图 1

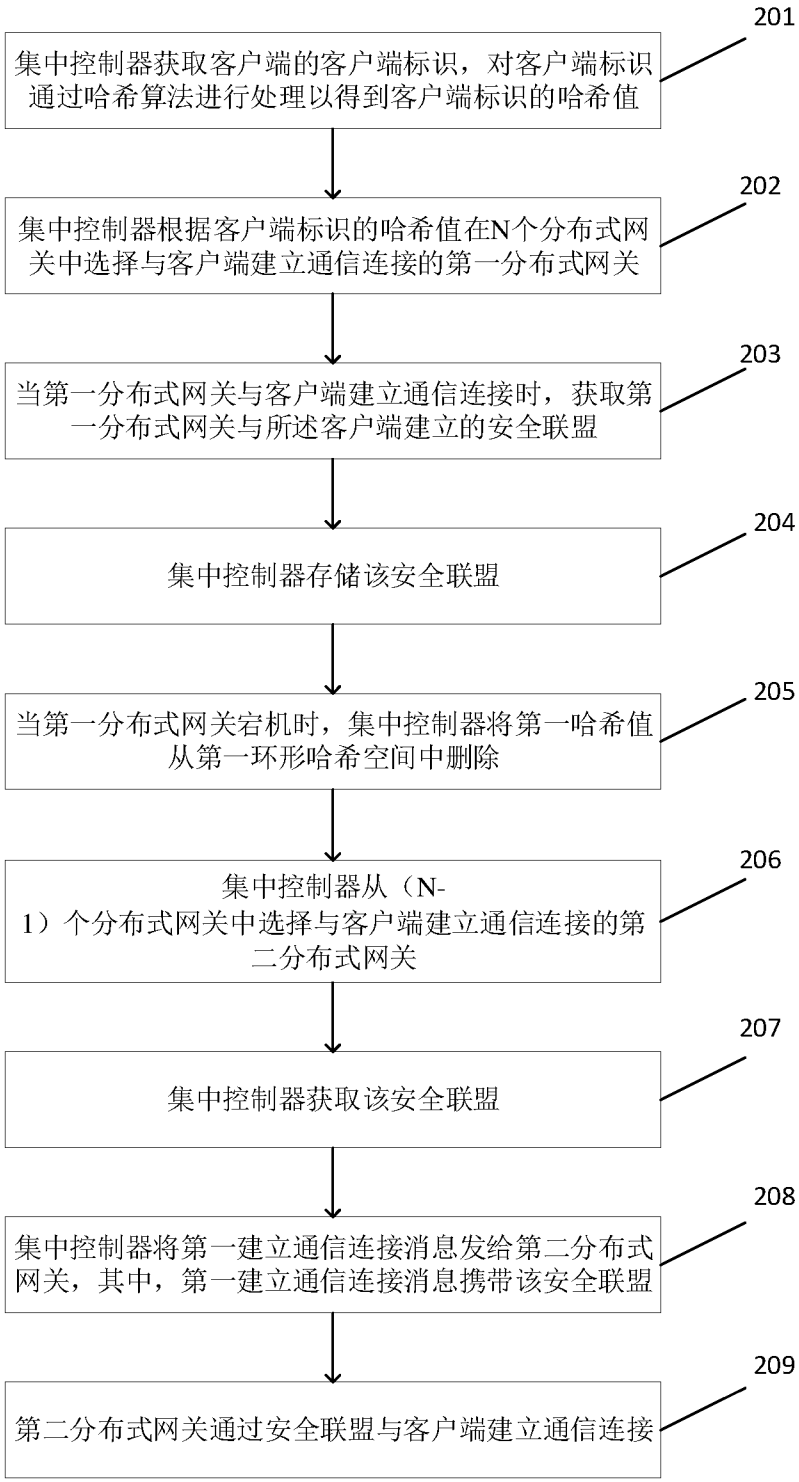
201
集中控制器获取客户端的客户端标识，对客户端标识通过哈希算法进行处理以得到客户端标识的哈希值
202
集中控制器根据客户端标识的哈希值在N个分布式网关中选择与客户端建立通信连接的第一分布式网关
203
当第一分布式网关与客户端建立通信连接时，获取第一分布式网关与所述客户端建立的安全联盟
204
集中控制器存储该安全联盟
205
当第一分布式网关宕机时，集中控制器将第一哈希值从第一环形哈希空间中删除
206
集中控制器从（N-1）个分布式网关中选择与客户端建立通信连接的第二分布式网关
207
集中控制器获取该安全联盟
208
集中控制器将第一建立通信连接消息发给第二分布式网关，其中，第一建立通信连接消息携带该安全联盟
209
第二分布式网关通过安全联盟与客户端建立通信连接

图 2

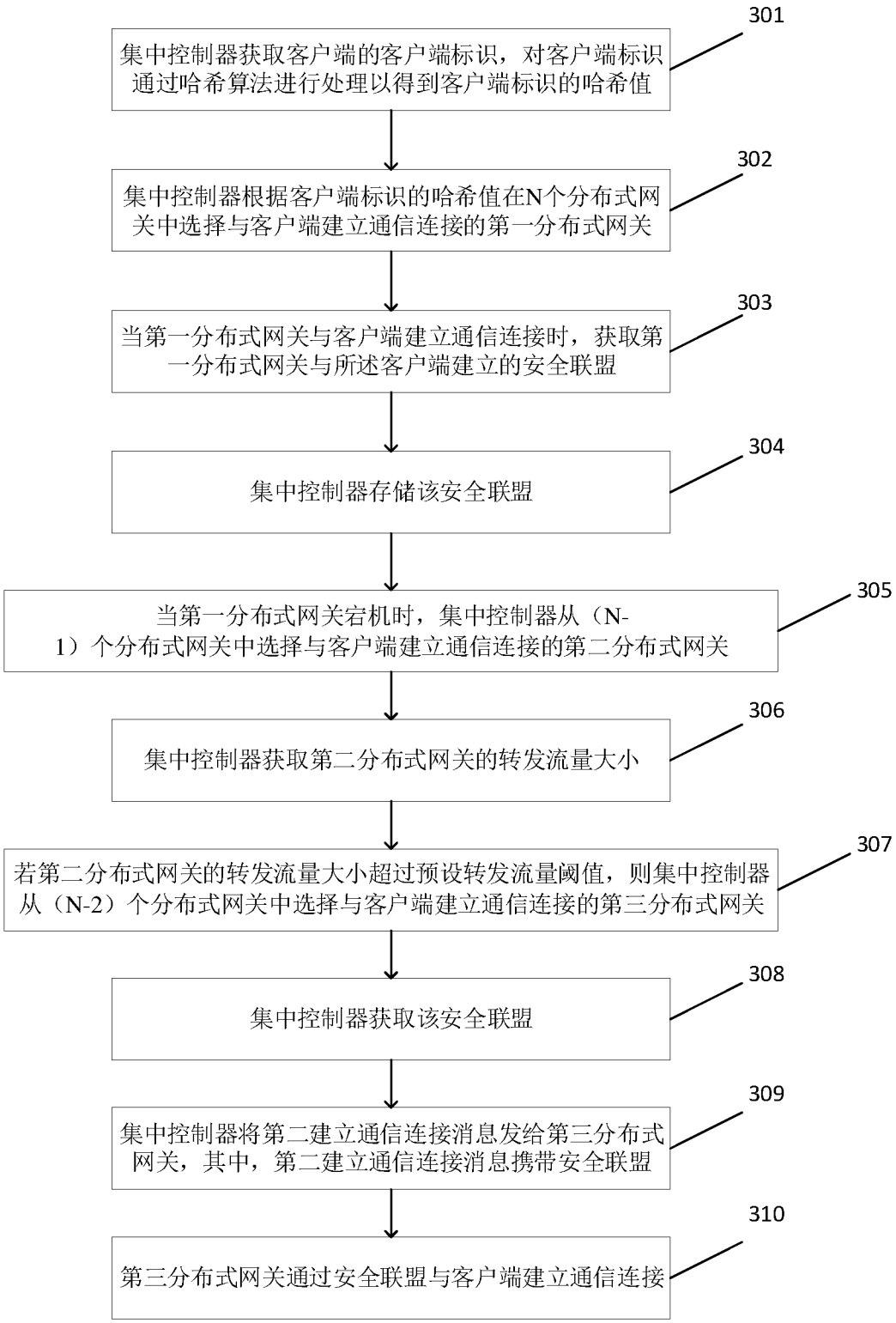
301
集中控制器获取客户端的客户端标识，对客户端标识通过哈希算法进行处理以得到客户端标识的哈希值
302
集中控制器根据客户端标识的哈希值在N个分布式网关中选择与客户端建立通信连接的第一分布式网关
303
当第一分布式网关与客户端建立通信连接时，获取第一分布式网关与所述客户端建立的安全联盟
304
集中控制器存储该安全联盟
305
当第一分布式网关宕机时，集中控制器从（N-1）个分布式网关中选择与客户端建立通信连接的第二分布式网关
306
集中控制器获取第二分布式网关的转发流量大小
307
若第二分布式网关的转发流量大小超过预设转发流量阈值，则集中控制器从（N-2）个分布式网关中选择与客户端建立通信连接的第三分布式网关
308
集中控制器获取该安全联盟
309
集中控制器将第二建立通信连接消息发给第三分布式网关，其中，第二建立通信连接消息携带安全联盟
310
第三分布式网关通过安全联盟与客户端建立通信连接

图 3

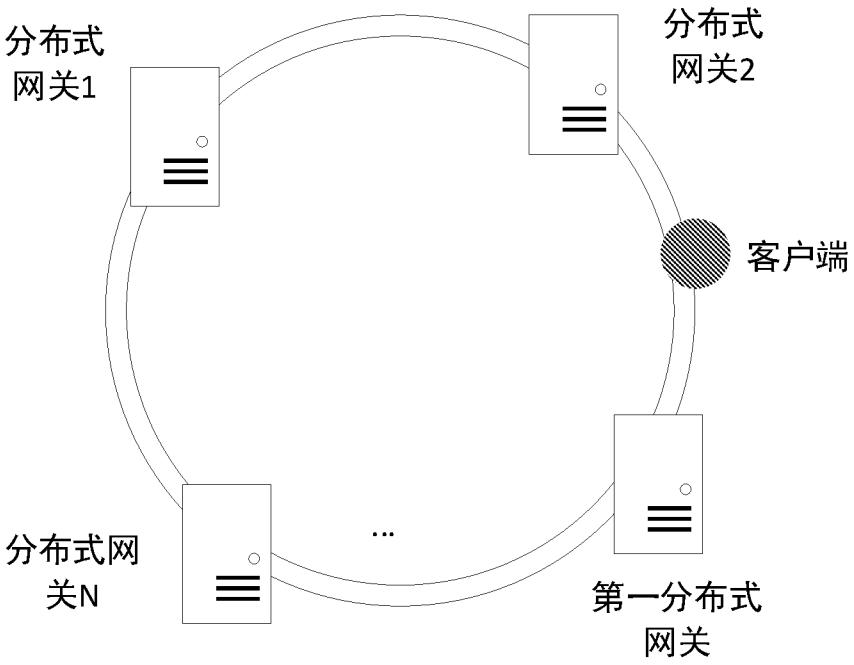
分布式
网关1
分布式
网关2
客户端
分布式网
关N
...
第一分布式
网关

图 4

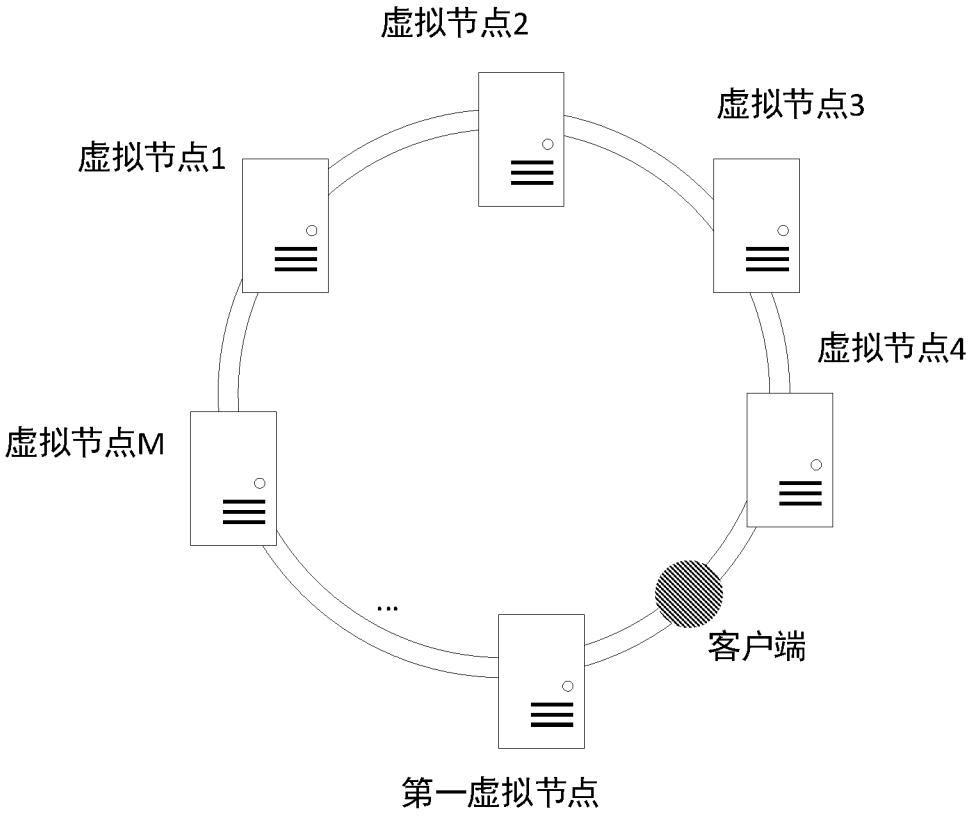
虚拟节点2
虚拟节点3
虚拟节点1
虚拟节点4
虚拟节点M
...
客户端
第一虚拟节点

图 5

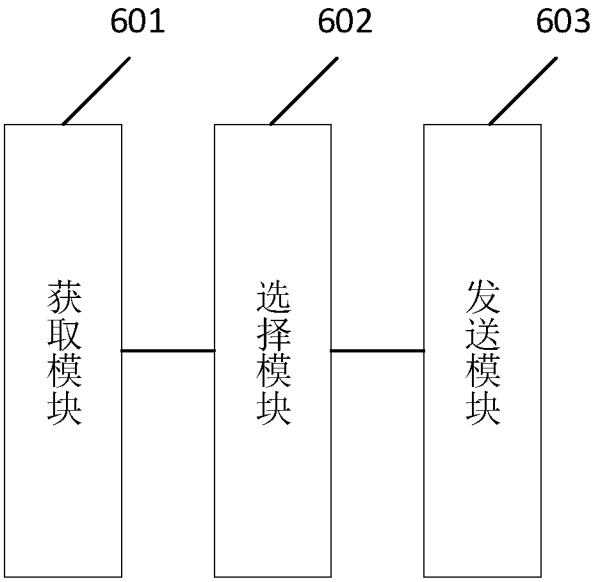
601
602
603
获取模块
选择模块
发送模块

图 6

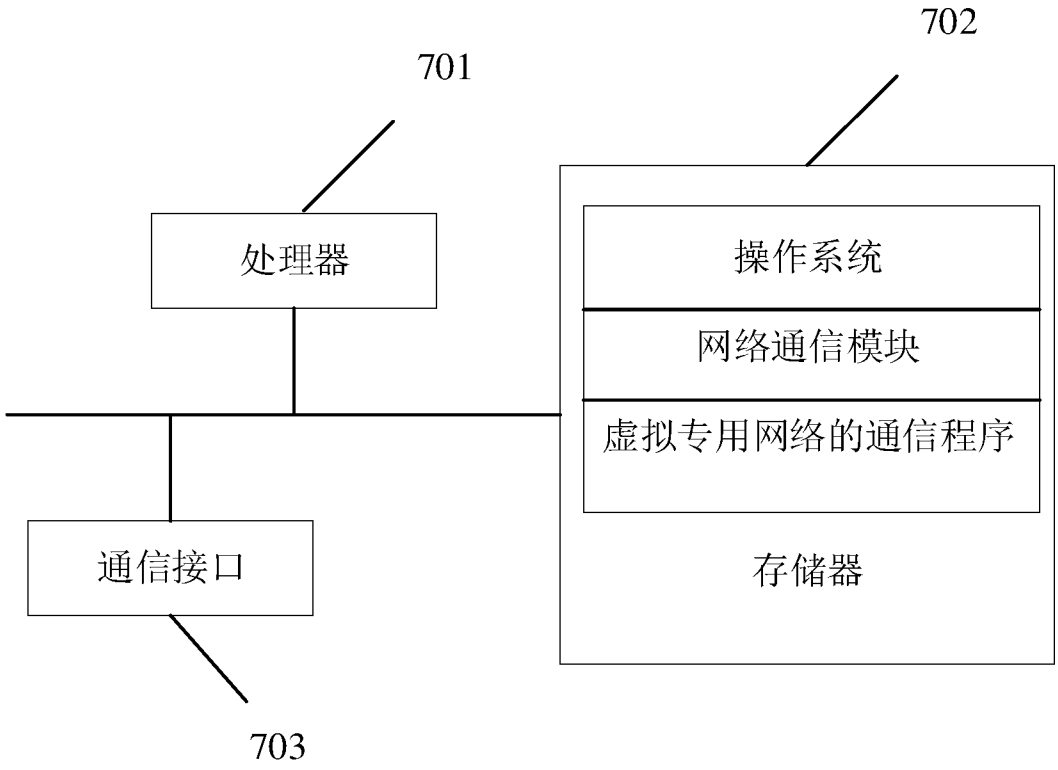
702
701
处理器
操作系统
网络通信模块
虚拟专用网络的通信程序
通信接口
存储器
703

图 7

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2019/102738

A. CLASSIFICATION OF SUBJECT MATTER

H04L 12/46(2006.01)i; H04L 29/08(2006.01)i; H04L 29/06(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; 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)

CNPAT, CNKI, WPI, EPODOC: 互联网协议安全性, Internet Protocol Security, IPSec, 虚拟专用网络, Virtual Private Network, VPN, 安全联盟, 安全关联, Security Association, SA, 网关, gateway, GW, 宕机, 故障, fault, failure, breakdown, 切换, switch, handover, 主, master, primary, first, 备, 辅, assistant, standby, redundancy, second, backup, 链路, 隧道, link, tunnel, 哈希, hash, IKE, Internet Key Exchange

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 110011892 A (PING AN TECHNOLOGY (SHENZHEN) CO., LTD.) 12 July 2019 (2019-07-12) claims 1-10, and description, paragraphs [0027]-[0135]	1-20
X	CN 103023741 A (OPZOON TECHNOLOGY CO., LTD.) 03 April 2013 (2013-04-03) description, paragraphs [0021]-[0032]	1, 10, 19, 20
Y	CN 103023741 A (OPZOON TECHNOLOGY CO., LTD.) 03 April 2013 (2013-04-03) description, paragraphs [0021]-[0032]	2-9, 11-18
Y	CN 106559349 A (ALIBABA GROUP HOLDING LIMITED) 05 April 2017 (2017-04-05) description, paragraphs [0090]-[0111]	2-9, 11-18
A	CN 103491088 A (CHENGDU WESTONE INFORMATION INDUSTRY INC.) 01 January 2014 (2014-01-01) entire document	1-20
A	US 2013182712 A1 (AGUAYO, Dan et al.) 18 July 2013 (2013-07-18) entire 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
18 November 2019	**28 November 2019**
Name and mailing address of the ISA/CN **China National Intellectual Property Administration (ISA/CN)** **No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088** **China** Facsimile No. **(86-10)62019451**	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2019/102738

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	110011892	A	12 July 2019	None			
CN	103023741	A	03 April 2013	None			
CN	106559349	A	05 April 2017	JP	2018534830	A	22 November 2018
				WO	2017050166	A1	30 March 2017
				US	2018212892	A1	26 July 2018
				EP	3355538	A1	01 August 2018
				KR	20180059448	A	04 June 2018
CN	103491088	A	01 January 2014	None			
US	2013182712	A1	18 July 2013	US	2015092603	A1	02 April 2015
				US	2019238418	A1	01 August 2019

国际检索报告

国际申请号 PCT/CN2019/102738

A. 主题的分类

H04L 12/46(2006.01)i; H04L 29/08(2006.01)i; H04L 29/06(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; 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））

CNPAT, CNKI, WPI, EPODOC: 互联网协议安全性, Internet Protocol Security, IPSec, 虚拟专用网络, Virtual Private Network, VPN, 安全联盟, 安全关联, Security Association, SA, 网关, gateway, GW, 宕机, 故障, fault, failure, breakdown, 切换, switch, handover, 主, master, primary, first, 备, 辅, assistant, standby, redundancy, second, backup, 链路, 隧道, link, tunnel, 哈希, hash, IKE, Internet Key Exchange

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 110011892 A (平安科技深圳有限公司) 2019年 7月 12日 (2019-07-12) 权利要求1-10，说明书第27-135段	1-20
X	CN 103023741 A (汉柏科技有限公司) 2013年 4月 3日 (2013-04-03) 说明书第21-32段	1，10，19-20
Y	CN 103023741 A (汉柏科技有限公司) 2013年 4月 3日 (2013-04-03) 说明书第21-32段	2-9，11-18
Y	CN 106559349 A (阿里巴巴集团控股有限公司) 2017年 4月 5日 (2017-04-05) 说明书第90-111段	2-9，11-18
A	CN 103491088 A (成都卫士通信息产业股份有限公司) 2014年 1月 1日 (2014-01-01) 全文	1-20
A	US 2013182712 A1 (AGUAYO, DAN 等) 2013年 7月 18日 (2013-07-18) 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
2019年 11月 18日	2019年 11月 28日
ISA/CN的名称和邮寄地址 中国国家知识产权局(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 李普昕 电话号码 86-(10)-53961653

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2019/102738

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	110011892	A	2019年 7月 12日	无			
CN	103023741	A	2013年 4月 3日	无			
CN	106559349	A	2017年 4月 5日	JP	2018534830	A	2018年 11月 22日
				WO	2017050166	A1	2017年 3月 30日
				US	2018212892	A1	2018年 7月 26日
				EP	3355538	A1	2018年 8月 1日
				KR	20180059448	A	2018年 6月 4日
CN	103491088	A	2014年 1月 1日	无			
US	2013182712	A1	2013年 7月 18日	US	2015092603	A1	2015年 4月 2日
				US	2019238418	A1	2019年 8月 1日