(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
2019 年 2 月 7 日 (07.02.2019)

WIPO | PCT

(10) 国际公布号
WO 2019/024880 A1

(51) 国际专利分类号:
H04L 12/911 (2013.01) *H04L 29/06* (2006.01)
H04L 12/741 (2013.01) *H04L 29/12* (2006.01)

(21) 国际申请号: PCT/CN2018/098212

(22) 国际申请日: 2018 年 8 月 2 日 (02.08.2018)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201710653308.X 2017年8月2日 (02.08.2017) CN

(71) 申请人: 华为技术有限公司 (HUAWEI TECHNOLOGIES CO., LTD.) [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(72) 发明人: **毛利铧(MAO, Lihua)**; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 **刘必振(LIU, Bizhen)**; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 **梅雪明(MEI, Xueming)**; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 **张玉磊(ZHANG, Yulei)**; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 **倪兵(NI, Bing)**; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (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,

(54) **Title:** MESSAGE SENDING METHOD AND NETWORK DEVICE

(54) **发明名称**: 发送报文的方法和网络设备

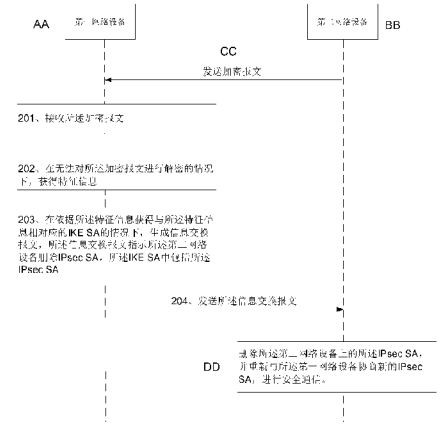


图 2

201 RECEIVE THE ENCRYPTED MESSAGE
202 OBTAIN CHARACTERISTIC INFORMATION IN A CASE WHERE THE ENCRYPTED MESSAGE CANNOT BE DECRYPTED
203 IN A CASE WHERE AN IKE SA CORRESPONDING TO THE CHARACTERISTIC INFORMATION IS OBTAINED ACCORDING TO THE CHARACTERISTIC INFORMATION, GENERATE AN INFORMATION EXCHANGE MESSAGE, WHICH INSTRUCTS THE SECOND NETWORK DEVICE TO DELETE THE IPSEC SA, THE IKE SA COMPRISING THE IPSEC SA
204 SEND THE INFORMATION EXCHANGE MESSAGE
AA FIRST NETWORK DEVICE
BB SECOND NETWORK DEVICE
CC SEND AN ENCRYPTED MESSAGE
DD DELETE THE IPSEC SA ON THE SECOND NETWORK DEVICE AND RE-NEGOTIATE A NEW IPSEC SA WITH THE FIRST NETWORK DEVICE FOR SECURE COMMUNICATION

(57) Abstract: The present application provides a message sending method and a network device, applicable to Internet security IPsec communications between a first network device and a second network device. The first network device has no IPsec security association (SA), and the second network device has a network scenario of the IPsec SA. The method comprises: the first network device receives an encrypted message received from the second network device; in a case where the first network device is unable to decrypt the encrypted message, the first network device obtains characteristic information; in a case where the first network device obtains, according to the characteristic information, an Internet key exchange (IKE) SA corresponding to the characteristic information, the first network device generates an information exchange message, which instructs the second network device to delete the IPsec SA on the second network device; and the first network device sends the information exchange message to the second network device. The present application can shorten service interruption time.

(57) 摘要: 本申请提供一种发送报文的方法和网络设备，应用于第一网络设备和第二网络设备之间进行互联网安全IPsec通信，且第一网络设备上没有IPsec安全联盟SA，第二网络设备上拥有IPsec SA的网络场景中，所述方法包括：第一网络设备接收来自第二网络设备的加密报文；在第一网络设备无法对所述加密报文进行解密的情况下，第一网络设备获得特征信息；在第一网络设备依据所述特征信息获得与所述特征信息相对应的互联网密钥交换IKE SA的情况下，第一网络设备生成信息交换报文，信息交换报文指示第二网络设备删除第二网络设备上的IPsec SA；第一网络设备向第二网络设备发送所述信息交换报文。有助于缩短业务中断时间。

WO 2019/024880 A1

[见续页]

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, 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))。

发送报文的方法和网络设备

本申请要求于2017年8月2日提交中国专利局、申请号为201710653308.X、申请名称为“发送报文的方法和网络设备”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，具体涉及一种用于发送报文的方法和网络设备。

背景技术

互联网协议安全（英文：Internet Protocol Security ，IPsec）使用中，会协商生成两个安全联盟（英文：Security Association ，SA）：一个是互联网密钥交换（英文：Internet Key Exchange，IKE） SA，它的作用是建立两个端点间信令协商的SA，所有信令（包括后续IPsec SA的协商）都在IKE SA保护下，加解密后收发；另一个是IPsec SA，它的作用是加解密网络上的用户数据流。

在IKE自动协商IPsec隧道的场景下，可能出现一种故障场景， IKE SA正常工作，但IPsec隧道一端存在IPsec SA，一端不存在IPsec SA的情况下，隧道转发流量会由于在缺失IPsec SA的设备上无法做正常的报文加密和报文解密导致流量中断。当IPsec SA的生存周期快到期时，IPsec隧道的两端通过IKE协商重新建立新的IPsec SA，此时数据流的转发恢复，继续进行通信。但考虑到性能等因素，生存周期通常设置的比较长，造成业务中断时间过长，降低了业务处理效率、进而也降低了用户的业务体验。

发明内容

本发明实施例提供的用于发送报文的方法和网络设备，解决了第一网络设备和第二网络设备之间进行互联网安全IPsec通信，当所述第一网络设备上没有IPsec 安全联盟SA，所述第二网络设备上拥有IPsec SA时业务中断时间过长的问题，提高了网络的可靠性和用户的业务体验。

为了解决上述问题，本发明实施例第一方面提供一种用于发送报文的方法，应用于第一网络设备和第二网络设备之间进行互联网安全IPsec通信，且所述第一网络设备上没有IPsec 安全联盟SA，所述第二网络设备上拥有IPsec SA的网络场景中，所述方法包括：所述第一网络设备接收来自第二网络设备的加密报文；在所述第一网络设备无法对所述加密报文进行解密的情况下，所述第一网络设备获得特征信息；在所述第一网络设备依据所述特征信息获得与所述特征信息相对应的互联网密钥交换IKE SA的情况下，所述第一网络设备生成信息交换报文，所述信息交换报文指示所述第二网络设备删除所述第二网络设备上的IPsec SA；所述第一网络设备向所述第二网络设备发送所述信息交换报文。

在一种可能的设计中，所述第一网络设备接收来自所述第二网络设备在删除所述

IPsec SA 之后发送的协商报文，并根据所述协商报文，生成新的 IPsec SA 对后续收到的加密报文进行解密。

通过所述第一网络设备在无法对所述加密报文进行解密的情况下获得特征信息，并且在依据所述特征信息获得对应的 IKE SA 的情况下向所述第二网络设备发送所述信息交换报文，触发所述第二网络设备重新发起与所述第一网络设备的新的 IPsec SA 的协商，而不用等到 IPsec SA 的生存周期快到期时进行新的 IPsec SA 协商，从而缩短了业务中断的时间、提高了业务处理效率、提升了用户的体验。

在一种可能的设计中，在所述第一网络设备依据所述特征信息无法获得与所述特征信息相对应的所述 IKE SA 的情况下，丢弃所述加密报文。

通过丢弃，避免了无用报文在设备里的堆积，节约了设备的存储空间。

在一种可能的设计中，所述特征信息包括 IPsec 安全参数索引 SPI；相应地，所述第一网络设备依据所述特征信息获得与所述特征信息相对应的 IKE SA 包括：所述第一网络设备依据所述 IPsec SPI 与所述 IKE SA 的映射关系，获得所述 IKE SA。

通过 IPsec SPI 来获得所述 IKE SA 的方法，使所述第一网络设备能及时、准确地发送信息交换报文，加快了业务恢复的速度。

在一种可能的设计中，所述特征信息包括源 IP 地址和目的 IP 地址；相应地，所述第一网络设备依据所述特征信息获得与所述特征信息相对应的 IKE SA 包括：所述第一网络设备依据所述源 IP 地址和所述目的 IP 地址与所述 IKE SA 的映射关系，获得所述 IKE SA。

通过源 IP 地址和目的 IP 地址来获得所述 IKE SA 信息的方法，在所述第一网络设备不能使用 IPsec SPI 精确命中 IKE SA 时，使所述第一网络设备能及时地发送信息交换报文，增强了设备的容错性。

在一种可能的设计中，所述特征信息还包括 IKE 标识；相应地，所述第一网络设备依据所述特征信息获得与所述特征信息相对应的 IKE SA 包括：所述第一网络设备依据所述源 IP 地址、所述目的 IP 地址和所述 IKE 标识与所述 IKE SA 的映射关系，获得所述 IKE SA。

通过源 IP 地址、目的 IP 地址和所述 IKE 标识来获得所述 IKE SA 信息的方法，在容错性的基础上，又一定程度提高了命中 IKE SA 的准确性。

在一种可能的设计中，所述特征信息还包括协议号；相应地，所述第一网络设备依据所述特征信息获得与所述特征信息相对应的 IKE SA 包括：所述第一网络设备依据所述源 IP 地址、所述目的 IP 地址和所述协议号与所述 IKE SA 的映射关系，获得所述 IKE SA。

通过源 IP 地址、目的 IP 地址和所述协议号来获得所述 IKE SA 信息的方法，在容错性的基础上，又进一步提高了命中 IKE SA 的准确性。

在一种可能的设计中，所述特征信息还包括协议号；相应地，所述第一网络设备依据所述特征信息获得与所述特征信息相对应的 IKE SA 包括：所述第一网络设备依据所述源 IP 地址、所述目的 IP 地址、所述 IKE 标识和所述协议号与所述 IKE SA 的映射关系，获得所述 IKE SA。

通过源 IP 地址、目的 IP 地址、所述 IKE 标识和所述协议号来获得所述 IKE SA

信息的方法，在容错性的基础上，又更进一步提高了命中 IKE SA 的准确性。

在一种可能的设计中，所述第一网络设备无法对所述加密报文进行解密包括至少下述方式之一：根据所述加密报文中的IPsec安全参数索引SPI无法获得所述IPsec SA；根据所述加密报文中的源 IP 地址和目的 IP 地址无法获得所述 IPsec SA；以及根据所述加密报文中的所述源 IP 地址、所述目的 IP 地址和协议号无法获得所述 IPsec SA。

通过两次查找的方式能够增加判断是否能够解密的准确性，第二次查找是对第一次查找结果的校验，可以有效的避免误判。

在一种可能的设计中，所述第一网络设备根据所述目的 IP 地址与所述 IKE 标识的映射关系，获得所述 IKE 标识；所述第一网络设备根据所述目的 IP 地址和源 IP 地址与所述 IKE 标识的映射关系，获得所述 IKE 标识；所述第一网络设备根据所述目的 IP 地址、源 IP 地址和协议号与所述 IKE 标识的映射关系，获得所述 IKE 标识；或者所述第一网络设备根据所述目的 IP 地址、源 IP 地址、协议号、源端口号和目的端口号与所述 IKE 标识的映射关系，获得所述 IKE 标识。

第二方面，本发明提供一种第一网络设备，所述第一网络设备用于执行第一方面或第一方面的任意可能的实现方式中的方法。具体地，所述第一网络设备包括用于执行第一方面或第一方面的任意可能的实现方式中的方法的模块。

第三方面，本发明提供一种第一网络设备，所述第一网络设备包括：处理器、收发器、随机存取存储器、只读存储器以及总线。其中，处理器通过总线分别耦接发送器、随机存取存储器以及只读存储器。其中，当需要运行第一网络设备时，通过固化在只读存储器中的基本输入输出系统或者嵌入式系统中的 bootloader 引导系统进行启动，引导第一网络设备进入正常运行状态。在第一网络设备进入正常运行状态后，在随机存取存储器中运行应用程序和操作系统，使得该处理器执行第一方面或第一方面的任意可能的实现方式中的方法。

第四方面，提供一种第一网络设备，所述第一网络设备包括：中央处理器、转发表项存储器、物理接口网卡、网络转发处理器。所述第一网络设备用于执行第一方面任意可能的实现方式中的方法。具体地，所述第一网络设备包括用于执行第一方面或第一方面的任意可能的实现方式中的方法的模块。

第五方面，本发明提供一种计算机可读介质，包括指令，当其在计算机上运行时，使得计算机执行第一方面或第一方面的任意可能的实现方式中的方法。

附图说明

为了更清楚地说明本申请实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要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中记载的一些实施例，对于本领域普通技术人员来讲，还可以根据这些附图获得其它的附图。

图1a是本发明实施例一种发送报文的应用场景示意图；

图1b是本发明实施例又一种发送报文的应用场景示意图；

图2是本发明实施例中一种用于发送报文的方法的流程示意图；

图3是本发明实施例中一种IKE Header的字段格式示意图；

图4是本发明实施例中一种Delete Payload的字段格式示意图；

图5a是本发明实施例一种第一网络设备的结构示意图；

图5b是本发明实施例另一种第一网络设备的结构示意图；

图 5c 是本发明实施例又一种第一网络设备的结构示意图。

具体实施方式

为了使本技术领域的人员更好地理解本发明方案，下面结合附图和实施方式对本发明实施例作进一步的详细说明。显然，所描述的实施例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它实施例，都属于本发明保护的范围。

在介绍本发明实施例技术方案之前，先对本发明实施例相关的应用场景进行解释说明。本发明应用于在互联网协议（英文：Internet Protocol , IP）网络中通过 IPsec 进行安全通信的场景中。

IPSec 是由国际互联网工程任务组（Internet Engineering Task Force，IETF）制定的用来为支持互联网通信协议第 4 版（英文：Internet Protocol version 4， Ipv4）和支持互联网通信协议第 6 版（英文：Internet Protocol version 6， IPv6）提供可互操作的、高质量的、基于加密的安全服务的一套协议。

IPSec 提供的安全服务是在 IP 层提供的，是以标准的方式，对 IP 层和承载在 IP 层上的所有协议提供保护。使用 IPsec 可以保护两个端点之间的通信路径，例如，一对主机之间、一对安全网关之间、一个安全网关与一个主机之间的一条或多条路径。这样 IPSec 主要用来在互联网（英文：Internet）上构建三层隧道的方式来提供 IPSec 虚拟专用网（Virtual Private Network ，VPN）服务，广泛应用在主机、路由器以及安全网关等网络设备上。

IPSec 是一个协议族，主要由安全协议、安全协议使用的加密算法和验证算法、以及相关的密钥管理协议构成。IPSec 的安全协议有两个：认证头（英文：Authentication Header，AH）和封装安全载荷（英文：Encapsulating Security Payload，ESP），AH 和 ESP 都有两种封装模式：隧道模式和传输模式。密钥管理协议为因特网密钥交换（英文：Internet Key Exchange，IKE）协议。

IPSec 通过 AH 和 ESP 这两个安全协议来实现安全服务的目标。并且还可以通过 IKE 协议为 IPSec 提供自动协商交换密钥、建立和维护安全联盟的服务，以简化 IPSec 的使用和管理。

与 IPsec 相关的概念包括数据流、安全联盟（英文：Security Association，SA）、安全策略和隧道等，为了便于对本发明的理解，下面分别简要介绍。

1、数据流

数据流是指由具有相同报文特征值的一组报文构成的流，所述报文特征值包括但不限于： IP 报文头中包含的源 IP 地址、目的 IP 地址、协议号等；TCP/UDP 报文头中包含的源端口号、目的端口号等。该若干个特征值的组合也可以称为 N 元组（N 为大于等于 1 的正整数），N 元组用于标识一条数据流。例如，数据流可以用源 IP 地址、目的 IP 地址、协议号、源端口号、目的端口号构成的五元组来标识，也可以用源 IP

地址、目的 IP 地址、协议号构成的三元组来标识。IPSec 能够对不同的数据流施加不同的安全保护，例如对不同的数据流使用不同的安全协议、算法或密钥。

2、安全联盟（英文：Security Association，SA）

IPSec 在两个端点之间提供安全通信，这两个端点被称为 IPSec 对等体。安全联盟是 IPSec 对等体之间对某些要素的约定。例如，使用哪种协议（AH、ESP、还是两者结合使用）、协议的封装模式（传输模式和隧道模式）、安全参数索引（Security Parameter Index，SPI）、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。

安全联盟是单向的。如果有两个主机（A 和 B）使用 ESP 进行安全通信，主机 A 就需要两个 SA，一个 SA 处理外发数据包，另一个 SA 处理进入的数据包。同样，主机 B 也需要两个 SA。

安全联盟还与协议相关。如果主机 A 和主机 B 同时使用 AH 和 ESP 进行安全通信，对于主机 A 就需要四个 SA，AH 协议的两个 SA（出方向和入方向各一个）和 ESP 协议的两个 SA（出方向和入方向各一个）。同样，主机 B 也需要四个 SA。

安全联盟由一个三元组来唯一标识。这个三元组包括： SPI、目的 IP 地址、安全协议号（AH 协议号或 ESP 协议号）。SPI 用于标识具有相同 IP 地址和相同安全协议的不同 SA，是为唯一标识 SA 而生成的一个 32 比特的数值，它在 AH 和 ESP 头中传输。SPI 可以包括 IPsec SPI 和 IKE SPI，IPsec SPI 用于标识一个 IPsec SA，IKE SPI 用于标识一个 IKE SA。

安全联盟具有生存周期。生存周期的计算包括两种方式：

以时间为基准，每隔指定长度的时间就进行更新；

以流量为基准，每传输指定的数据量（字节）就进行更新。

无论哪一种类型的生存周期先到期，安全联盟都会失效。安全联盟快要失效前，IKE 将为 IPSec 协商建立新的安全联盟，这样在旧的安全联盟失效时新的安全联盟就已经准备好。

通常，安全联盟包括 IKE SA 和 IPsec SA。IKE SA 负责 IPSec SA 的建立和维护，起控制作用。IPSec SA 负责具体的数据流加密。

3、安全策略（英文：Security Policy）

安全策略是规定对什么样的数据流采用什么样的安全措施，通常由用户手工配置。通过在一个访问控制列表中配置多条规则来实现对数据流的定义，在安全策略中引用这个访问控制列表来确定需要进行保护的数据流。

IPSec 端点对于进入或外出的每一份数据报文（即数据包），都可能有三种处理：丢弃、绕过或应用 IPSec。第一种处理方式是指数据报文不被处理，只是简单地丢弃。第二种处理方式是指数据报文不需要 IPSec 保护，而在载荷内增添 IP 头，然后分发 IP 数据报文。第三种处理方式是指对数据报文提供 IPSec 保护，且安全策略必须说明提供的安全服务、应用的协议及使用的算法等。

4、IPsec 隧道（英文：tunnel）

IPSec 隧道是为了保证 IP 通信安全，通过在 IPsec 对等体（或端点）之间建立安全联盟、配置相同的策略，从而建立的一个安全的 IP 数据包传输的通道，实现了在本

端对 IP 报文加密，在对端解密。

在 IKE 自动协商 IPsec 隧道进行通信的场景下，可能出现一种故障场景，例如图 1a 所示，A 端和 B 端之间建立了 IPsec 隧道进行正常通信，但此时由于各种原因，引起所述 IPsec 隧道两端的 IKE SA 正常工作，所述 IPsec 隧道一端（如 A 端）存在 IPsec SA，另一端（如 B 端）不存在 IPsec SA。在这种情况下，由于在缺失 IPsec SA 的 B 端无法做正常的报文加密和报文解密，会导致所述 IPsec 隧道无法转发数据流、造成业务中断。引起所述 B 端原来有 IPsec SA，而后来 IPsec SA 丢失的原因各种各样，例如，对 B 端网络设备的误操作。

还例如，IPsec 隧道使用双机保护的场景。在主设备发生故障的时候，通过虚拟路由冗余协议（英文：Virtual Router Redundancy Protocol， VRRP）实现自动切换，数据流通过备设备转发，保障业务不中断。IPsec SA 在主设备协商完成，但对应的 IPsec SA 协商信息还没有备份到备设备的时候出现主备设备倒换，此时备设备上没有 IPsec SA。但倒换前的主设备已经与对端设备完成 IPsec 隧道协商，而所述对端设备上与主设备之间已经协商完成的 IPsec SA 是存在的。 这样就造成了当网络中的主设备故障时，所述对端设备有 IPsec SA，备设备上没有 IPSEC SA，没有 IPSEC SA 的备设备无法完成数据流的加密和解密，导致业务中断。如图 1b 所示，第一网络设备和第三网络设备之间通过运行 VRRP 协议形成一个虚拟网络设备（即 VRRP 备份组，拥有一个虚拟网络 IP 地址），第一网络设备为备用设备，第三网络设备为主用设备。A 端（第二网络设备）和 B 端（虚拟网络设备）之间建立了 IPsec 隧道，传送 IP 数据流，进行安全的通信。在 B 端的主用设备（第三网络设备）发生故障的时候，通过 VRRP 协议实现自动切换，数据流通过备用设备转发，从而保障数据流转发不中断。然而，在建立 IPsec 隧道时，IPsec SA 在第二网络设备和主用设备（第三网络设备）上协商完成，当主用设备上的 IKE SA 信息已经备份到备用设备（第一网络设备）上，而 IPsec SA 信息还没有备份到备用设备（第一网络设备）上的时候出现主备设备倒换，此时备用设备上还没有 IPsec SA。这样就造成了当网络中的主用设备故障时，A 端的所述第二网络设备有 IPsec SA，备用设备（第一网络设备）上没有 IPsec SA（也可以说所述虚拟网络设备上没有 IPsec SA），没有 IPsec SA 的备用设备无法完成数据流的加密和解密，导致所述 IPsec 隧道无法转发数据流、造成业务中断。

当 IPsec SA 的生存周期到期前，所述第二网络设备和备用设备之间通过 IKE 协商重新建立新的 IPsec SA，此时数据流的转发恢复，继续通过备用设备进行通信。但这种方式业务的恢复快慢取决于设置的生存周期的长短。因为正常情况下，生存周期设置的太短，会造成频繁的密钥协商，占用设备大量的 CPU 资源，降低设备的处理性能，所以通常生存周期设置的较长。然而生存周期设置的较长，又会导致业务中断后恢复的时间过长，业务中断时间过长降低了业务处理的效率、也降低了用户的业务体验。

上面描述了本发明涉及的可能的应用场景，下面将基于此对本发明实施例进一步详细说明。

图 2 为本发明实施例提供的一种发送报文的方法流程示意图。该方法应用于第一

网络设备和第二网络设备之间进行互联网安全 IPsec 通信，且所述第一网络设备上没有 IPsec SA，所述第二网络设备上拥有 IPsec SA 的网络场景中。

在一个示例中，如图 1a 所示，所述 IPsec 隧道从 A 端到 B 端，B 端的第一网络设备上的 IPsec SA 信息由于误操作等原因丢失，造成所述第一网络设备上没有 IPsec SA。

在又一个实例中，如图 1b 所示，所述 IPsec 隧道从 A 端到 B 端，B 端是一个虚拟网络设备，例如通过运行 VRRP 协议实现对主用设备（第三网络设备）的可靠性保护。当主用设备故障时，如果主用设备上的 IPsec SA 信息还没有备份到备用设备（所述第一网络设备）上，也会造成所述第一网络设备上没有 IPsec SA。

本发明实施例提供的方案包括 201、202、203 和 204 部分，下面分别说明。

在 201 部分，所述第一网络设备接收来自所述第二网络设备的加密报文，对所述加密报文解密。

在一个具体的实施方式中，所述第一网络设备根据所述加密报文中携带的 IPsec SPI 查找对应 IPsec 隧道的解密信息，例如，IPsec SA，当查找不到时，则无法进行解密。

在另一个具体的实施方式中，所述第一网络设备根据所述加密报文中携带的源 IP 地址、目的 IP 地址、协议号查找对应的 IPsec 隧道的解密信息，例如，IPsec SA，当查找不到时，则无法进行解密。

在又一个具体的实施方式中，所述第一网络设备首先根据所述加密报文中携带的 IPsec SPI 查找（第一次查找）对应 IPsec 隧道的解密信息，例如，IPsec SA；当查找不到时，再继续根据所述加密报文中携带的源 IP 地址、目的 IP 地址、协议号查找（第二次查找）对应的 IPsec 隧道的解密信息；此时，当仍然查找不到时，则确认无法进行解密，当然，如果此时查找到了 IPsec 隧道的解密信息，则确认可以进行解密。这种两次查找的方式能够增加判断是否能够解密的准确性，第二次查找是对第一次查找结果的校验，可以有效的避免误判。

在 202 部分，在所述第一网络设备无法对所述加密报文进行解密的情况下，所述第一网络设备获得特征信息。

因为所述第一网络设备上没有 IPsec SA （可能的原因参见上文图 1a 和图 1b 部分的描述），所以无法对来自第二网络设备的所述加密报文进行相应的 IPsec 解密。此时，所述第一网络设备根据所述加密报文中携带的信息获取特征信息，所述特征信息与 IKE SA 有关联关系，用于指示一个 IPsec SA，所述第一网络设备根据所述特征信息可以查找到所述特征信息指示的所述 IPsec SA 所属的 IKE SA。所述特征信息可以是 IPsec SPI；也可以是源 IP 地址和目的 IP 地址，并且进一步包括协议号和/或 IKE 标识。其中，所述 IKE 标识用于标识一个网络设备接收 IPsec 加密报文的入口信息，所述入口信息可以是逻辑接口信息、物理接口信息或者 VPN 信息。例如，所述 IKE 标识可以是物理端口标识、逻辑接口的标识、物理接口的接口索引（英文：IFindex）、逻辑接口的接口索引、虚拟专用网（Virtual Private Network ，VPN）标识、VPN 索引（英文：index）、虚拟路由转发（英文：Virtual Routing Forwarding，VRF）标识（ 英文：Identifier，ID）等。其中，IKE 标识的获取可以有以下几种方式：

1）所述第一网络设备根据所述目的 IP 地址，查找所述目的 IP 地址与所述 IKE

标识的映射关系得到。

2）所述第一网络设备根据所述目的 IP 地址和源 IP 地址，查找所述目的 IP 地址和源 IP 地址与所述 IKE 标识的映射关系得到。

3）所述第一网络设备根据所述目的 IP 地址、源 IP 地址和协议号，查找所述目的 IP 地址、源 IP 地址和协议号与所述 IKE 标识的映射关系得到。

4）所述第一网络设备根据所述目的 IP 地址、源 IP 地址、协议号、源端口号和目的端口号，查找所述目的 IP 地址、源 IP 地址、协议号、源端口号和目的端口号与所述 IKE 标识的映射关系得到。

需要说明的是，在一个具体的实施例中，上述处理都是在所述第一网络设备的转发面（例如，网络设备的接口板卡或转发板卡，执行数据报文的转发相关的功能）进行的。接着，所述第一网络设备的转发面将所述特征信息上送到所述第一网络设备的控制面（例如，网络设备的控制板卡，执行信令协议等控制相关的功能）处理。

所述第一网络设备的控制面针对收到的所述特征信息查找到与之对应的 IKE SA 信息，所述 IKE SA 信息包含以下信息中的至少一项： IKE SPI 信息、生存周期时间、对应的失效对端检测（英文：Dead Peer Detection ,DPD）的探测策略（用于确认对端的 IKE SA 是否存在的策略）、交换（英文：exchange）密钥信息（即上次交换时存储的秘钥）等。

在一个具体的实施方式中，所述特征信息为 IPsec SPI，所述第一网络设备依据所述 IPsec SPI 与所述 IKE SA 信息的映射关系（如表 1 所示），获得所述 IKE SA 信息。因为 IPsec SPI 可以精确的代表 IPsec 隧道，所以用 IPsec SPI 来获得所述 IKE SA 信息的方法比较精确，使所述第一网络设备能及时、准确地发送信息交换报文，加快了业务恢复的速度。

表 1

特征信息	IKE SA 信息
IPsec SPI	IKE SA

在另一个具体的实施方式中，所述特征信息包括源 IP 地址和目的 IP 地址，所述第一网络设备依据所述源 IP 地址和所述目的 IP 地址与所述 IKE SA 信息的映射关系（如表 2 所示），获得所述 IKE SA 信息。源 IP 地址和目的 IP 地址不能唯一代表 IPsec 隧道，但当无法使用 IPsec SPI 获得所述 IKE SA 信息时，可以用源 IP 地址和目的 IP 地址来获得所述 IKE SA 信息，增强了设备的容错性。

表 2

特征信息	IKE SA 信息
源 IP 地址，目的 IP 地址	IKE SA

在又一个具体的实施方式中，所述特征信息包括源 IP 地址、目的 IP 地址和 IKE 标识，所述第一网络设备依据所述源 IP 地址、所述目的 IP 地址和所述 IKE 标识与所述 IKE SA 信息的映射关系（如表 3 所示），获得所述 IKE SA 信息。这种方式，通过引入所述 IKE 标识，在容错性的基础上，又一定程度提高了准确性。

表 3

特征信息	IKE SA 信息
源 IP 地址，目的 IP 地址，IKE 标识	IKE SA

在又一个具体的实施方式中，所述特征信息包括源 IP 地址、目的 IP 地址和协议号，所述第一网络设备依据所述源 IP 地址、所述目的 IP 地址和所述协议号与所述 IKE SA 信息的映射关系（如表 4 所示），获得所述 IKE SA 信息。这种方式，通过引入所述协议号，在容错性的基础上，又一定程度提高了准确性。

表 4

特征信息	IKE SA 信息
源 IP 地址，目的 IP 地址，协议号	IKE SA

在又一个具体的实施方式中，所述特征信息包括源 IP 地址、目的 IP 地址、IKE 标识和协议号，所述第一网络设备依据所述源 IP 地址、所述目的 IP 地址、所述 IKE 标识和所述协议号与所述 IKE SA 信息的映射关系（如表 5 所示），获得所述 IKE SA 信息。这种方式，通过引入所述协议号和所述 IKE 标识，在容错性的基础上，又进一步提高了准确性。

表 5

特征信息	IKE SA 信息
源 IP 地址，目的 IP 地址，协议号，IKE 标识	IKE SA

需要说明的是，上述表 1 至 5 所述的任意一项映射关系可以以映射表的形式保存在所述第一网络设备上，可以通过人工的配置建立、运行 IKE 等协议自动计算生成、或者从其它设备获取，而且该映射关系可以根据实际情况进行更新。

在又一个具体的实施方式中，在所述第一网络设备依据所述特征信息无法获得与所述特征信息相对应的互联网密钥交换 IKE SA 信息的情况下，丢弃所述加密报文。通过丢弃，避免了无用报文在设备里的堆积，节约了对设备存储空间的占用。

在 203 部分，在所述第一网络设备依据所述特征信息获得与所述特征信息相对应的 IKE SA 信息的情况下，所述第一网络设备的控制面根据所述 IPsec SPI（携带在上述 201 部分描述的所述加密报文中）生成信息交换（英文：informational exchange）报文，所述信息交换报文指示所述第二网络设备删除所述 IPsec SA。

在一个具体实施方式中，所述信息交换报文包含一个标志位和所述 IPsec SPI，该标志位用于指示接收到所述信息交换报文的网络设备删除该该网络设备上所述 IPsec SPI 所对应的 IPsec SA。在另一个具体实施方式中，获得了 IKE SA 信息后，说明 IKE 协商可以正常工作。在 IKE SA 协商操作的过程中，IPsec 对等体之间需要传递一些特定情况下的错误或通告之类的控制消息，为此，IKE 定义了所述信息交换报文。IKE

定义的的IKE报文头（英文： IKE Header）格式如图3所示，包括IKE 发起端的SPI（英文：IKE SA Initiator's SPI）字段、 IKE 响应端的SPI（英文：IKE SA Responder's SPI）字段、下一个载荷（英文：Next Payload）字段、主要版本（英文：Major Version，MjVer）字段、少数版本（英文：Minor Version，MnVer）、交换类型（英文：Exchange Type）字段、标志（英文：Flags）字段、消息标识（英文：Message ID）字段、长度（英文：Length）字段。

其中，例如，所述第一网络设备将所述Exchange Type字段的值设置为37，代表此报文为信息交换报文，并将所述Next Payload字段的值设置为42，代表在IKE Header后面携带的是一个删除载荷（英文：Delete Payload）。

该Delete Payload字段的格式如图4所示，包括：Next Payload字段、C字段、 保留（英文：RESERVED）字段、 载荷长度（英文： Payload Length）字段、协议标识（英文：Protocol ID）字段、SPI尺寸（英文:Size）字段、SPI数量（英文：Num of SPIs）字段和SPI(es)字段。所述SPI(es)字段携带上述IPsec SPI。所述信息交换报文用于通告所述第二网络设备将与所述IPsec SPI相对应的IPsec SA删除。

需要说明的是，本发明中有关信息交换报文的细节，请参考国际互联网工程任务组（Internet Engineering Task Force，IETF）发布的征求意见（英文：Request For Comments，RFC）7296，该文档与此相关部分的内容好像整体复制一般以引入的方式并入本文本中，此处为了简洁，不再赘述。

还需要说明的是，IPsec SA和IPsec SA信息在本发明的各个实施例中是同一个意思，可以互相使用。同理，IKE SA和IKE SA信息也可以互相使用。本发明说明书中所述的第一网络设备中的“第一”、第二网络设备中的“第二”和第三网络设备中的“第三”仅仅用于区分不同的网络设备。在本发明的实施例举例中，第二网络设备作为IPsec加密报文的发送端，第一网络设备和第二网络设备作为IPsec加密报文的接收端。

在204部分，所述第一网络设备向所述第二网络设备发送所述信息交换报文。

在一个具体的实施例中，发送所述信息交换报文的可参考上面203部分以及IETF定义的IKE SA协商过程，为了简洁，此处不再赘述。

所述第二网络设备收到所述信息交换报文后，根据所述信息交换报文中携带的所述IPsec SPI找到与所述IPsec SPI相对应的IPsec SA，并将其删除。所述第二网络设备没有了IPsec SA，则会发起新一轮的IPsec SA的协商。所述第二网络设备向所述第一网络设备发送协商报文，所述协商报文用于协商所述新的IPsec SA。

所述第二网络设备接收来自所述第二网络设备在删除所述IPsec SA之后发送的协商报文，并根据所述协商报文，生成所述新的IPsec SA，用所述新的IPsec SA对后续收到的加密报文进行解密。

通过及时、自动地触发所述第二网络设备重新发起与所述第一网络设备的新的IPsec SA的协商，从而缩短了业务中断的时间、提高了业务处理效率、提升了用户的体验。

图 5a 示出了上述实施例中所涉及的第一网络设备的一种可能的结构示意图。第一网络设备 500A 包括：中央处理器 510、转发表项存储器 511、物理接口网卡 513、网络转发处理器 512 和加解密处理器 514。控制面执行信令协议等控制相关的功能，转发面执行数据报文的转发相关的功能。在多板卡的设备结构下，控制面是指一块独立的主控板卡，该主控板卡上包括所述中央处理器 510；转发面是指一块独立的转发板卡或接口板卡，该转发板卡上包括转发表项存储器 511、物理接口网卡 513、网络转发处理器 512 和加解密处理器 514。在单板卡的设备结构下，转发面和控制面集成在一块板卡上，包括执行控制管理功能的中央处理器 510 和执行转发面功能的转发表项存储器 511、物理接口网卡 513、网络转发处理器 512 和加解密处理器 514。

当第一网络设备 500A 从物理接口网卡 513 收到所述第二网络设备发来的加密报文，物理接口网卡 513 将所述加密报文送到网络转发处理器 512，网络转发处理器 512 根据所述加密报文中的特征信息（与上文图 2 部分的有关特征信息的相关描述一致，请参考，此处不再赘述）从转发表项存储器 511 中找不到对应的 IPsec SA 时（即为无法解密），网络转发处理器 512 将所述加密报文上送控制面的中央处理器 510，中央处理器 510 根据协商信息构造信息交换报文（携带所述 IPsec SPI），并发送给所述第二网络设备，通知所述第二网络设备删除所述 IPsec SPI 对应的 IPsec SA，并重新发起协商创建新的 IPsec SA。中央处理器 510 具体执行上面图 2 中 203 部分的功能步骤，网络转发处理器 512 具体执行上述图 2 中 201、202、204 部分的功能步骤，可参考上面相关描述，此处不再赘述。

当第一网络设备 500A 从物理接口网卡 513 收到所述第二网络设备发来的新的加密报文，物理接口网卡 513 将所述新的加密报文送到网络转发处理器 512，网络转发处理器 512 根据所述新的加密报文的特征信息从转发表项存储器 511 中找到对应的 IPsecSA 时，网络转发处理器 512 将所述新的加密报文发送到加解密处理器 514 进行解密处理，解密后发送到网络转发处理器 512，网络转发处理器 512 根据所述解密后的报文的目的 IP 查找转发表项存储器 511 中的转发表进行转发。

本实施例的第一网络设备 500A 可对应于上述图 1a 至图 4 所对应的实施例中的第一网络设备，该第一网络设备 500A 中的中央处理器 510、转发表项存储器 511、物理接口网卡 513、网络转发处理器 512 等可以实现图 1a 至图 4 所对应的实施例中的第一网络设备所具有的功能和/或所实施的各种步骤，中央处理器 510 具体执行上面图 2 中 203 部分的功能步骤，网络转发处理器 512、转发表项存储器 511、物理接口网卡 513 具体执行上述图 2 中 201、202、204 部分的功能步骤。详细内容可参考上面相关描述，为了简洁，在此不再赘述。

需要说明的是，在一种可能的设计中，应用于基于控制转发分离的软件定义网络（英文：Software Defined Network，SDN）架构中。所述第一网络设备 500A 控制面的功能与转发面的功能分离到两个独立的网络设备中，例如，控制器和转发设备。所述控制器包括中央处理器 510，所述转发设备包括转发表项存储器 511、物理接口网卡 513、网络转发处理器 512 和加解密处理器 514 等。相应地，上述各器件（中央处理器 510、转发表项存储器 511、物理接口网卡 513、网络转发处理器 512 和加解密处理器 514）分别执行上面图 5a 中相应各器件所执行的功能和作用，详细内容可参考上面相

关描述，为了简洁，在此不再赘述。

图 5b 示出了上述实施例中所涉及的第一网络设备的又一种可能的结构示意图。第一网络设备 500B 应用于所述第一网络设备和第二网络设备之间进行互联网安全 IPsec 通信，且所述第一网络设备上没有 IPsec 安全联盟 SA，所述第二网络设备上拥有 IPsec SA 的网络场景中，所述第一网络设备包括：处理单元 504B、接收单元 502B 和发送单元 506B。

接收单元 502B 用于接收来自第二网络设备的加密报文。

处理单元 504B 用于在所述处理单元 504B 无法对所述加密报文进行解密的情况下，获得特征信息。

其中，所述处理单元 504B 无法对所述加密报文进行解密包括以下几种情况：

1)所述处理单元 504B 根据所述加密报文中的 IPsec SPI 无法获得所述 IPsec SA；

2）所述处理单元 504B 根据所述加密报文中的源 IP 地址和目的 IP 地址无法获得所述 IPsec SA；

3）所述处理单元 504B 根据所述加密报文中的所述源 IP 地址、所述目的 IP 地址和协议号无法获得所述 IPsec SA；或

4）所述处理单元 504B 根据所述加密报文中的所述 IPsec SPI 无法获得所述 IPsec SA，并且根据所述加密报文中的所述源 IP 地址、所述目的 IP 地址和所述协议号也无法获得所述 IPsec SA。

在所述处理单元 504B 依据所述特征信息获得与所述特征信息相对应的 IKE SA 的情况下，所述处理单元 504B 还用于生成信息交换报文，所述信息交换报文指示所述第二网络设备删除所述第二网络设备上的 IPsec SA。发送单元 506B 用于向所述第二网络设备发送所述信息交换报文。

在所述处理单元 504B 依据所述特征信息无法获得与所述特征信息相对应的所述 IKE SA 的情况下，所述处理单元 504B 还用于丢弃所述加密报文。

其中，所述处理单元 504B 依据所述特征信息获得与所述特征信息相对应的 IKE SA 可以包括以下几种可能的实现方式：

1)所述特征信息包括 IPsec 安全参数索引 SPI。所述处理单元 504B 依据所述 IPsec SPI 与所述 IKE SA 的映射关系，获得所述 IKE SA。

2）所述特征信息包括源 IP 地址和目的 IP 地址。所述处理单元 504B 依据所述源 IP 地址和所述目的 IP 地址与所述 IKE SA 的映射关系，获得所述 IKE SA。

3）所述特征信息包括源 IP 地址、目的 IP 地址和 IKE 标识。所述处理单元 504B 依据所述源 IP 地址、所述目的 IP 地址和所述 IKE 标识与所述 IKE SA 的映射关系，获得所述 IKE SA。

4）所述特征信息包括源 IP 地址、目的 IP 地址和协议号。所述处理单元 504B 依据所述源 IP 地址、所述目的 IP 地址和所述协议号与所述 IKE SA 的映射关系，获得所述 IKE SA。

5）所述特征信息包括源 IP 地址、目的 IP 地址、IKE 标识和协议号。所述处理单元 504B 依据所述源 IP 地址、所述目的 IP 地址、IKE 标识和所述协议号与所述 IKE SA

的映射关系，获得所述 IKE SA。

其中，所述处理单元 504B 还用于根据所述目的 IP 地址与所述 IKE 标识的映射关系，获得所述 IKE 标识。

所述接收单元 502B，还用于接收来自所述第二网络设备在删除所述 IPsec SA 之后发送的协商报文。

所述处理单元 504B，还用于根据所述协商报文，生成新的 IPsec SA 对后续收到的加密报文进行解密。

本发明实施例的第一网络设备 500B 可对应于上述发送报文的方法实施例中的第一网络设备，并且，该第一网络设备 500B 中的各模块和上述其他操作和/或功能分别为了实现图 1a 至图 4 所对应的实施例中的第一网络设备所实施的各种步骤和方法，所述处理单元 504B 具体执行上面图 2 中 202、203 部分的功能步骤，接收单元 502B 具体执行上述图 2 中 201 部分的功能步骤，发送单元 506B 具体执行上述图 2 中 204 部分的功能步骤。详细内容可参考上面相关描述，为了简洁，在此不再赘述。

图 5c 示出了上述实施例中所涉及的第一网络设备的再一种可能的结构示意图。第一网络设备 500C 包括：收发器 510C、处理器 520C、随机存取存储器 540 C、只读存储器 550 C 以及总线 560 C。其中，处理器 520 C 通过总线 560 C 分别耦接收发器 510 C、随机存取存储器 540C 以及只读存储器 550C。其中，当需要运行第一网络设备 500C 时，通过固化在只读存储器 550C 中的基本输入输出系统或者嵌入式系统中的 bootloader 引导系统进行启动，引导第一网络设备 500 C 进入正常运行状态。在第一网络设备 500C 进入正常运行状态后，在随机存取存储器 540 C 中运行应用程序和操作系统，使得：

收发器 510C 用于接收来自第二网络设备的加密报文。处理器 520C 用于在所述处理器 520C 无法对所述加密报文进行解密的情况下，获得特征信息。在所述处理器 520C 依据所述特征信息获得与所述特征信息相对应的 IKE SA 的情况下，所述处理器 520C 还用于生成信息交换报文，所述信息交换报文指示所述第二网络设备删除所述第二网络设备上的 IPsec SA。收发器 510C 还用于向所述第二网络设备发送所述信息交换报文。

在所述处理器 520C 依据所述特征信息无法获得与所述特征信息相对应的所述 IKE SA 的情况下，所述处理器 520C 还用于丢弃所述加密报文。

所述收发器 510C，还用于接收来自所述第二网络设备在删除所述 IPsec SA 之后发送的协商报文。

所述处理器 520C，还用于根据所述协商报文，生成新的 IPsec SA 对后续收到的加密报文进行解密。

本发明实施例的第一网络设备 500C 可对应于上述图 1a 至图 4 所对应的实施例中的第一网络设备，并且，该第一网络设备 500C 中的处理器 520C、收发器 510C 等可以实现图 1a 至图 4 所对应的实施例中的第一网络设备所具有的功能和/或所实施的各种步骤和方法。所述处理器 520C 用于执行图 5b 所述第一网络设备的处理单元 504B 的所有操作，所述收发器 510C 用于执行图 5b 所述第一网络设备的接收单元 502B 和发送单元 506B 的所有操作。所述处理器 520C 具体执行上面图 2 中 202、203 部分的

功能步骤，收发器 510C 具体执行上述图 2 中 201 和 204 部分的功能步骤。详细内容可参考上面相关描述，为了简洁，在此不再赘述。

需要说明的是，本实施例也可以基于通用的物理服务器结合网络功能虚拟化（英文：Network Function Virtualization，NFV）技术实现的第一网络设备，所述第一网络设备为虚拟第一网络设备（如，虚拟路由器或虚拟交换机）。所述虚拟第一网络设备可以是运行有用于发送报文功能的程序的虚拟机（英文：Virtual Machine，VM），所述虚拟机部署在硬件设备上（例如，物理服务器）。虚拟机指通过软件模拟的具有完整硬件系统功能的、运行在一个完全隔离环境中的完整计算机系统。本领域技术人员通过阅读本申请即可结合 NFV 技术在通用物理服务器上虚拟出具有上述功能的多个第一网络设备。此处不再赘述。

应理解，本领域技术人员在阅读本申请文件的基础上，可以针对本申请实施例中所描述的可选的特征、步骤或方法进行不需要付出创造性的组合，都属于本申请公开的实施例，只是由于描述或行文的简单没有重复赘述不同组合。

应理解，本领域技术人员在阅读本申请文件的基础上，可以针对本申请实施例中所描述的可选的特征、步骤或方法进行不需要付出创造性的组合，都属于本申请公开的实施例，只是由于描述或行文的简单没有重复赘述不同组合。

应理解，本文中术语“和/或”，仅仅是一种描述关联对象的关联关系，表示可以存在三种关系，例如，A 和/或 B，可以表示：单独存在 A，同时存在 A 和 B，单独存在 B 这三种情况。另外，本文中字符“/”，一般表示前后关联对象是一种“或”的关系。

应理解，在本发明的各种实施例中，上述各过程的序号的大小并不意味着执行顺序的先后，各过程的执行顺序应以其功能和内在逻辑确定，而不应对本发明实施例的实施过程构成任何限定。

本领域普通技术人员可以意识到，结合本文中所公开的实施例描述的各示例的单元及算法步骤，能够以电子硬件、或者计算机软件和电子硬件的结合来实现。这些功能究竟以硬件还是软件方式来执行，取决于技术方案的特定应用和设计约束条件。专业技术人员可以对每个特定的应用来使用不同方法来实现所描述的功能，但是这种实现不应认为超出本发明的范围。

所属领域的技术人员可以清楚地了解到，为描述的方便和简洁，上述描述的系统、装置和单元的具体工作过程，可以参考前述方法实施例中的对应过程，在此不再赘述。

在本申请所提供的几个实施例中，应该理解到，所揭露的系统、装置和方法，可以通过其它的方式实现。例如，以上所描述的装置实施例仅仅是示意性的，例如，所述单元的划分，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式，例如多个单元或组件可以结合或者可以集成到另一个系统，或一些特征可以忽略，或不执行。另一点，所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些接口，装置或单元的间接耦合或通信连接，可以是电性，机械或其它的形式。

所述作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本实施例

方案的目的。

另外，在本发明各个实施例中的各功能单元可以集成在一个处理单元中，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单元中。

所述功能如果以软件功能单元的形式实现并作为独立的产品销售或使用时，可以存储在一个计算机可读取存储介质中。基于这样的理解，本发明的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质中，包括若干指令用以使得一台计算机设备（可以是个人计算机，服务器，或者网络设备等）执行本发明各个实施例所述方法的全部或部分步骤。而前述的存储介质包括：U 盘、移动硬盘、只读存储器（ROM，Read-Only Memory）、随机存取存储器（RAM，Random Access Memory）、磁碟或者光盘等各种可以存储程序代码的介质。

以上所述，仅为本发明的具体实施方式，但本发明的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本发明揭露的技术范围内，可轻易想到变化或替换，都应涵盖在本发明的保护范围之内。因此，本发明的保护范围应以所述权利要求的保护范围为准。

权 利 要 求 书

1、一种发送报文的方法，其特征在于，应用于第一网络设备和第二网络设备之间进行互联网安全 IPsec 通信，且所述第一网络设备上没有 IPsec 安全联盟 SA，所述第二网络设备上拥有 IPsec SA 的网络场景中，所述方法包括：

所述第一网络设备接收来自第二网络设备的加密报文；

在所述第一网络设备无法对所述加密报文进行解密的情况下，所述第一网络设备获得特征信息；

在所述第一网络设备依据所述特征信息获得与所述特征信息相对应的互联网密钥交换 IKE SA 的情况下，所述第一网络设备生成信息交换报文，所述信息交换报文指示所述第二网络设备删除所述第二网络设备上的 IPsec SA；

所述第一网络设备向所述第二网络设备发送所述信息交换报文。

2、根据权利要求 1 所述的方法，其特征在于，还包括：

所述第一网络设备接收来自所述第二网络设备在删除所述 IPsec SA 之后发送的协商报文，并根据所述协商报文，生成新的 IPsec SA 对后续收到的加密报文进行解密。

3、根据权利要求 1 或 2 所述的方法，其特征在于，还包括：

在所述第一网络设备依据所述特征信息无法获得与所述特征信息相对应的所述 IKE SA 的情况下，丢弃所述加密报文。

4、根据权利要求 1 至 3 任一所述的方法，其特征在于，所述特征信息包括 IPsec 安全参数索引 SPI；

相应地，所述第一网络设备依据所述特征信息获得与所述特征信息相对应的 IKE SA 包括：

所述第一网络设备依据所述 IPsec SPI 与所述 IKE SA 的映射关系，获得所述 IKE SA。

5、根据权利要求 1 至 3 任一所述的方法，其特征在于，所述特征信息包括源 IP 地址和目的 IP 地址；

相应地，所述第一网络设备依据所述特征信息获得与所述特征信息相对应的 IKE SA 包括：

所述第一网络设备依据所述源 IP 地址和所述目的 IP 地址与所述 IKE SA 的映射关系，获得所述 IKE SA。

6、根据权利要求 5 所述的方法，其特征在于，所述特征信息还包括 IKE 标识；

相应地，所述第一网络设备依据所述特征信息获得与所述特征信息相对应的 IKE SA 包括：

所述第一网络设备依据所述源 IP 地址、所述目的 IP 地址和所述 IKE 标识与所述 IKE SA 的映射关系，获得所述 IKE SA。

7、根据权利要求 5 所述的方法，其特征在于，所述特征信息还包括协议号；

相应地，所述第一网络设备依据所述特征信息获得与所述特征信息相对应的 IKE SA 包括：

所述第一网络设备依据所述源 IP 地址、所述目的 IP 地址和所述协议号与所述 IKE

SA 的映射关系，获得所述 IKE SA。

8、根据权利要求 6 所述的方法，其特征在于，所述特征信息还包括协议号；

相应地，所述第一网络设备依据所述特征信息获得与所述特征信息相对应的 IKE SA 包括：

所述第一网络设备依据所述源 IP 地址、所述目的 IP 地址、所述 IKE 标识和所述协议号与所述 IKE SA 的映射关系，获得所述 IKE SA。

9、根据权利要求 1 至 3 任一所述的方法，其特征在于，所述第一网络设备无法对所述加密报文进行解密包括至少下述方式之一：

根据所述加密报文中的 IPsec 安全参数索引 SPI 无法获得所述 IPsec SA；

根据所述加密报文中的源 IP 地址和目的 IP 地址无法获得所述 IPsec SA；以及

根据所述加密报文中的所述源 IP 地址、所述目的 IP 地址和协议号无法获得所述 IPsec SA。

10、一种网络设备，用作第一网络设备，其特征在于，应用于所述第一网络设备和第二网络设备之间进行互联网安全 IPsec 通信，且所述第一网络设备上没有 IPsec 安全联盟 SA，所述第二网络设备上拥有 IPsec SA 的网络场景中，所述第一网络设备包括：

接收单元，用于接收来自第二网络设备的加密报文；

处理单元，用于在所述处理单元无法对所述加密报文进行解密的情况下，获得特征信息；

所述处理单元，还用于在所述处理单元依据所述特征信息获得与所述特征信息相对应的互联网密钥交换 IKE SA 的情况下，生成信息交换报文，所述信息交换报文指示所述第二网络设备删除所述第二网络设备上的 IPsec SA；

发送单元，用于向所述第二网络设备发送所述信息交换报文。

11、根据权利要求 9 所述的第一网络设备，其特征在于，

所述接收单元，还用于接收来自所述第二网络设备在删除所述 IPsec SA 之后发送的协商报文；

所述处理单元，还用于根据所述协商报文，生成新的 IPsec SA 对后续收到的加密报文进行解密。

12、根据权利要求 9 或 10 所述的第一网络设备，其特征在于，

所述处理单元，还用于在所述处理单元依据所述特征信息无法获得与所述特征信息相对应的所述 IKE SA 的情况下，丢弃所述加密报文。

13、根据权利要求 10 至 12 任一所述的第一网络设备，其特征在于，所述特征信息包括 IPsec 安全参数索引 SPI；

相应地，所述处理单元依据所述特征信息获得与所述特征信息相对应的 IKE SA 包括：

所述处理单元依据所述 IPsec SPI 与所述 IKE SA 的映射关系，获得所述 IKE SA。

14、根据权利要求 10 至 12 任一所述的第一网络设备，其特征在于，所述特征信息包括源 IP 地址和目的 IP 地址；

相应地，所述处理单元依据所述特征信息获得与所述特征信息相对应的 IKE SA

包括：

所述处理单元依据所述源IP地址和所述目的IP地址与所述IKE SA的映射关系，获得所述IKE SA。

15、根据权利要求14所述的第一网络设备，其特征在于，所述特征信息还包括IKE标识；

相应地，所述处理单元依据所述特征信息获得与所述特征信息相对应的IKE SA包括：

所述处理单元依据所述源IP地址、所述目的IP地址和所述IKE标识与所述IKE SA的映射关系，获得所述IKE SA。

16、根据权利要求14所述的第一网络设备，其特征在于，所述特征信息还包括协议号；

相应地，所述处理单元依据所述特征信息获得与所述特征信息相对应的IKE SA包括：

所述处理单元依据所述源IP地址、所述目的IP地址和所述协议号与所述IKE SA的映射关系，获得所述IKE SA。

17、根据权利要求15所述的第一网络设备，其特征在于，所述特征信息还包括协议号；

相应地，所述处理单元依据所述特征信息获得与所述特征信息相对应的IKE SA包括：

所述处理单元依据所述源IP地址、所述目的IP地址、所述IKE标识和所述协议号与所述IKE SA的映射关系，获得所述IKE SA。

18、根据权利要求10所述的第一网络设备，其特征在于，所述处理单元无法对所述加密报文进行解密包括至少下述方式之一：

所述处理单元根据所述加密报文中的IPsec安全参数索引SPI无法获得所述IPsec SA；

所述处理单元根据所述加密报文中的源IP地址和目的IP地址无法获得所述IPsec SA；以及

所述处理单元根据所述加密报文中的所述源IP地址、所述目的IP地址和协议号无法获得所述IPsec SA。

19、一种网络设备，用作第一网络设备，其特征在于，应用于所述第一网络设备和第二网络设备之间进行互联网安全IPsec通信，且所述第一网络设备上没有IPsec安全联盟SA，所述第二网络设备上拥有IPsec SA的网络场景中，所述第一网络设备包括：

收发器，用于接收来自第二网络设备的加密报文；

处理器，用于在所述处理器无法对所述加密报文进行解密的情况下，获得特征信息；

所述处理器，还用于在所述处理器依据所述特征信息获得与所述特征信息相对应的互联网密钥交换IKE SA的情况下，生成信息交换报文，所述信息交换报文指示所述第二网络设备删除所述第二网络设备上的IPsec SA；

所述收发器，还用于向所述第二网络设备发送所述信息交换报文。

20、一种计算机可读介质，包括指令，当其在计算机上运行时，使得计算机执行如权利要求 1 至 9 任意一项所述的方法。

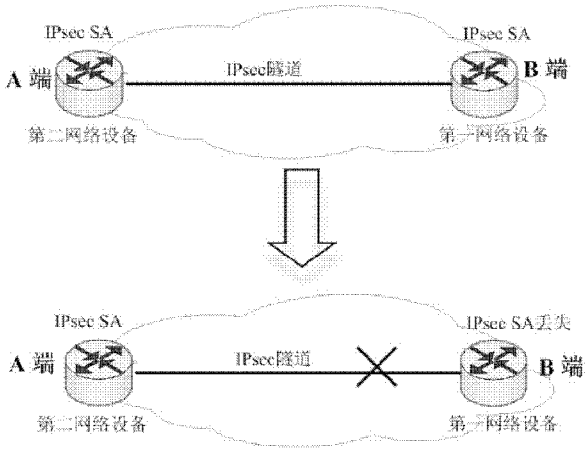

IPsec SA
IPsec SA
A 端
IPsec隧道
B 端
第二网络设备
第一网络设备
IPsec SA
IPsec SA丢失
A 端
IPsec隧道
B 端
第二网络设备
第一网络设备

图 1a

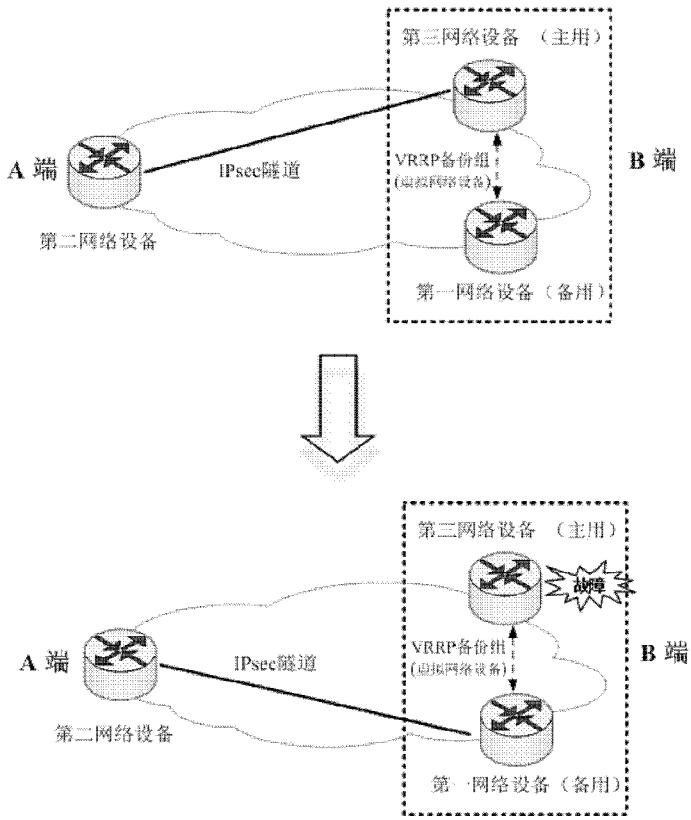

第二网络设备（主用）
A 端
IPsec隧道
VRRP备份组
B 端
第二网络设备
第一网络设备（备用）
第二网络设备（主用）
故障
A 端
IPsec隧道
VRRP备份组
B 端
第二网络设备
第一网络设备（备用）

图 1b

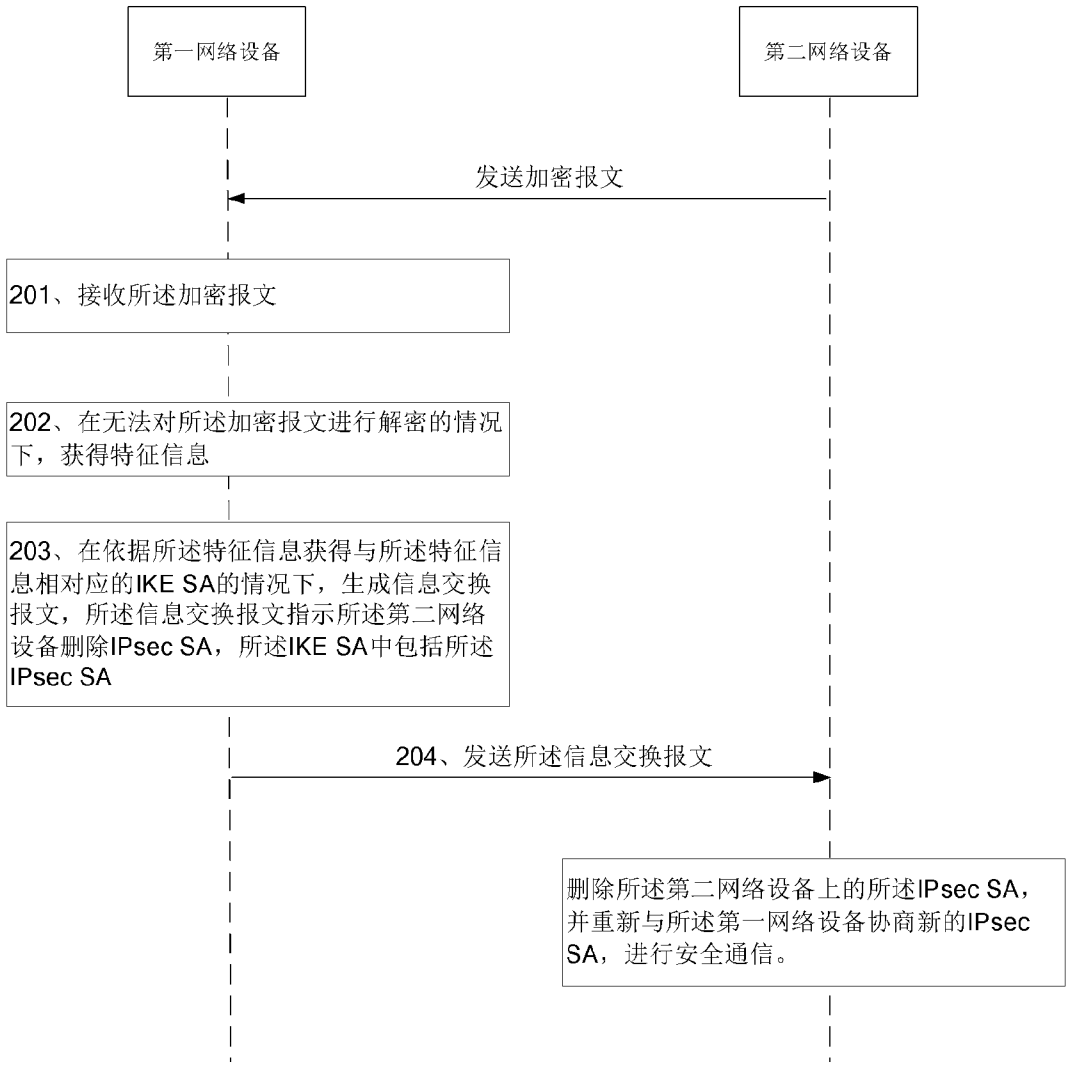

第一网络设备
第二网络设备
发送加密报文
201、接收所述加密报文
202、在无法对所述加密报文进行解密的情况下，获得特征信息
203、在依据所述特征信息获得与所述特征信息相对应的IKE SA的情况下，生成信息交换报文，所述信息交换报文指示所述第二网络设备删除IPsec SA，所述IKE SA中包括所述IPsec SA
204、发送所述信息交换报文
删除所述第二网络设备上的所述IPsec SA，并重新与所述第一网络设备协商新的IPsec SA，进行安全通信。

图 2

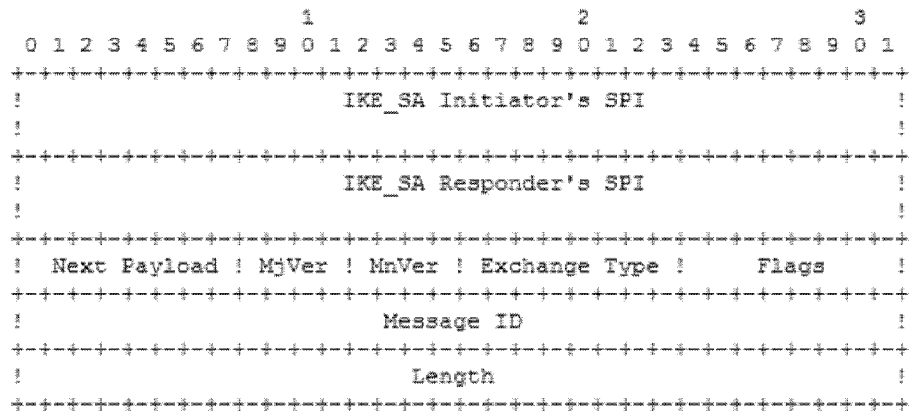

1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
IKE_SA Initiator's SPI
IKE_SA Responder's SPI
Next Payload
MjVer
MnVer
Exchange Type
Flags
Message ID
Length

图 3

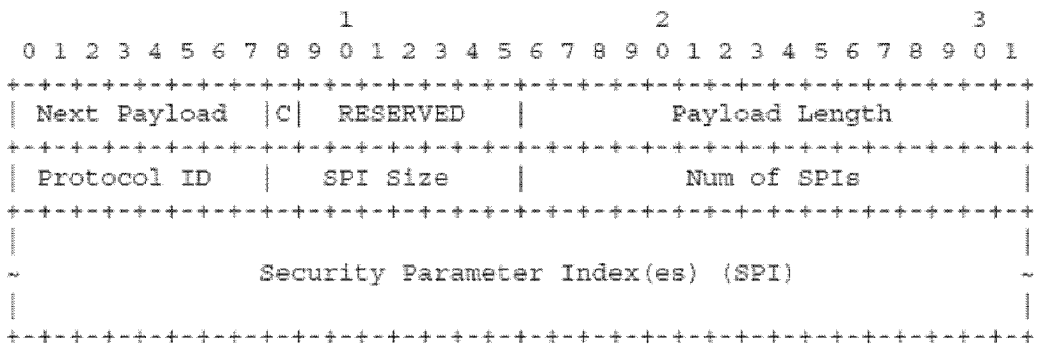

1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
Next Payload
C
RESERVED
Payload Length
Protocol ID
SPI Size
Num of SPIs
Security Parameter Index(es) (SPI)

图 4

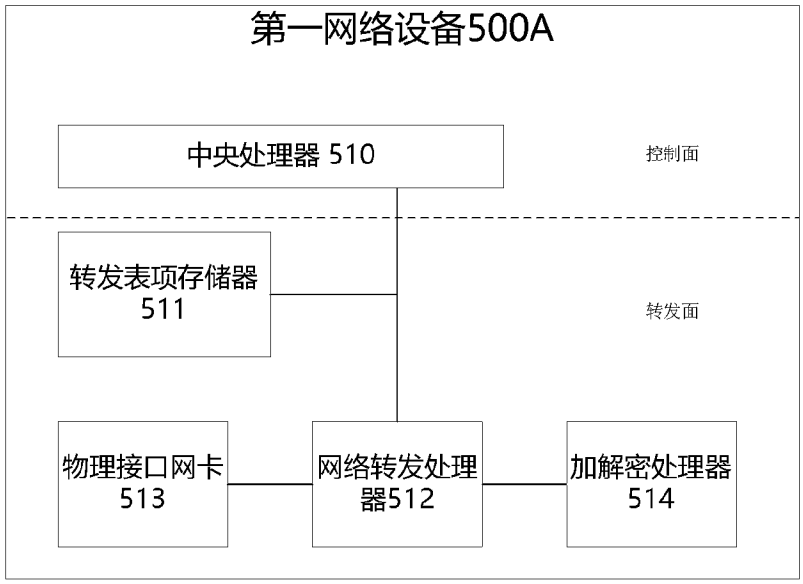

第一网络设备500A
中央处理器 510
控制面
转发表项存储器
511
转发面
物理接口网卡
513
网络转发处理
器512
加解密处理器
514

图 5a

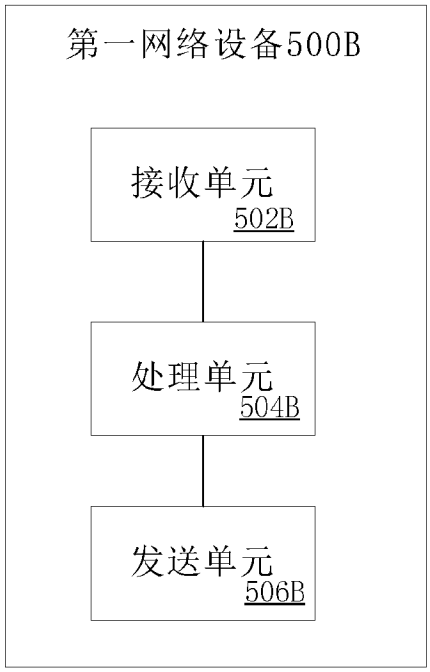

第一网络设备500B
接收单元
502B
处理单元
504B
发送单元
506B

图 5b

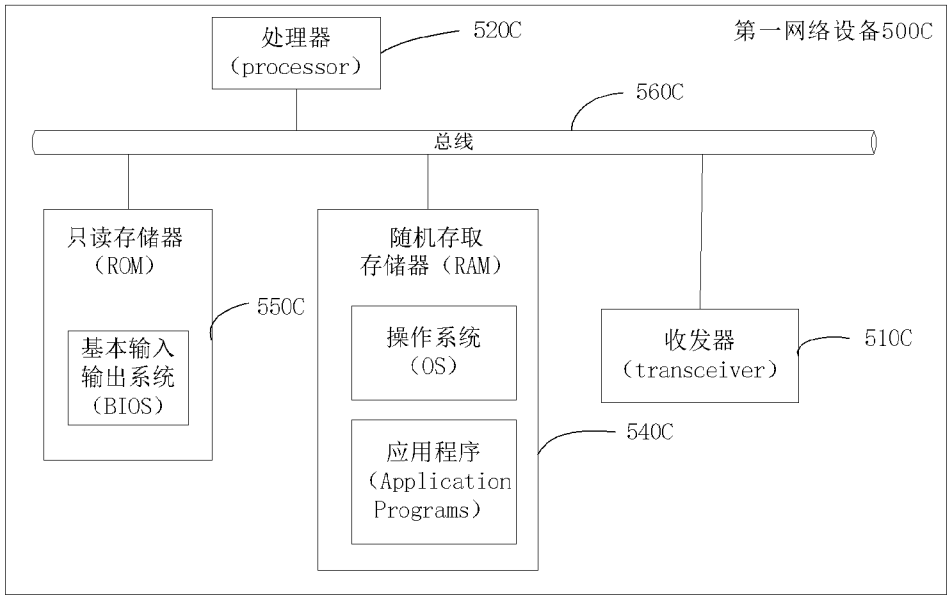

处理器
(processor)
520C
第一网络设备500C
560C
总线
只读存储器
(ROM)
基本输入
输出系统
(BIOS)
550C
随机存取
存储器(RAM)
操作系统
(OS)
应用程序
(Application
Programs)
540C
收发器
(transceiver)
510C

图 5c

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2018/098212

A. CLASSIFICATION OF SUBJECT MATTER

H04L 12/911(2013.01)i; H04L 12/741(2013.01)n; H04L 29/06(2006.01)n; H04L 29/12(2006.01)n

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)

VEN; SIPOABS; CNTXT; CNABS; CNKI; EPTXT; WOTXT; USTXT: 互联网安全, 安全联盟, IPsec, SA,加密, 删除, 刷新, 更新, 错误, 异常, 差错, 失效, 无效, encrypt+, delet+, refresh+, update+, error, fail+, invalid CPC: H04L67/104, H04L63/164

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 107682284 A (HUAWEI TECHNOLOGIES CO., LTD.) 09 February 2018 (2018-02-09) claims 1-20	1-20
X	CN 102148810 A (CHENGDU HUAWEI SYMANTEC TECHNOLOGIES CO., LTD.) 10 August 2011 (2011-08-10) paragraphs 62-181	1-20
A	CN 106487802 A (HANGZHOU DPTECH TECHNOLOGIES CO., LTD.) 08 March 2017 (2017-03-08) entire document	1-20
A	US 2015263866 A1 (NEC CORP.) 17 September 2015 (2015-09-17) 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
17 October 2018	**26 October 2018**

Name and mailing address of the ISA/CN	Authorized officer
State Intellectual Property Office of the P. R. China **No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing** **100088** **China**	
Facsimile No. **(86-10)62019451**	Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2018/098212

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	107682284	A	09 February 2018	None			
CN	102148810	A	10 August 2011	CN	102148810	B	12 March 2014
				WO	2011095097	A1	11 August 2011
CN	106487802	A	08 March 2017	None			
US	2015263866	A1	17 September 2015	JP	2015177430	A	05 October 2015
				US	9680663	B2	13 June 2017

国际检索报告

国际申请号
PCT/CN2018/098212

A. 主题的分类

H04L 12/911(2013.01)i; H04L 12/741(2013.01)n; H04L 29/06(2006.01)n; H04L 29/12(2006.01)n

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）)

VEN;SIPOABS;CNTXT;CNABS;CNKI;EPTXT;WOTXT;USTXT:互联网安全，安全联盟，IPsec，SA,加密，删除，刷新，更新，错误，异常，差错，失效，无效，encrypt+, delet+, refresh+, update+, error, fail+, invalid CPC: H04L67/104, H04L63/164

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 107682284 A (华为技术有限公司) 2018年 2月 9日 (2018-02-09) 权利要求1-20	1-20
X	CN 102148810 A (成都市华为赛门铁克科技有限公司) 2011年 8月 10日 (2011-08-10) 第62-181段	1-20
A	CN 106487802 A (杭州迪普科技股份有限公司) 2017年 3月 8日 (2017-03-08) 全文	1-20
A	US 2015263866 A1 (NEC CORP.) 2015年 9月 17日 (2015-09-17) 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
2018年 10月 17日	2018年 10月 26日

ISA/CN的名称和邮寄地址	受权官员
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	蔡茹辛
传真号 (86-10)62019451	电话号码 86-(010)-62089151

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2018/098212

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	107682284	A	2018年 2月 9日		无		
CN	102148810	A	2011年 8月 10日	CN	102148810	B	2014年 3月 12日
				WO	2011095097	A1	2011年 8月 11日
CN	106487802	A	2017年 3月 8日		无		
US	2015263866	A1	2015年 9月 17日	JP	2015177430	A	2015年 10月 5日
				US	9680663	B2	2017年 6月 13日