(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
2025 年 1 月 30 日 (30.01.2025)

WIPO | PCT

(10) 国际公布号
WO 2025/020437 A1

(51) 国际专利分类号:
H04L 9/40 (2022.01)

(21) 国际申请号: PCT/CN2023/140207

(22) 国际申请日: 2023 年 12 月 20 日 (20.12.2023)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
202310913190.5 2023年7月25日 (25.07.2023) CN

(71) 申请人:中国电信股份有限公司(**CHINA TELECOM CORPORATION LIMITED**) [CN/CN]; 中国北京市西城区金融大街31号, Beijing 100033 (CN)。

(72) 发明人:陈文华 (**CHEN, Wenhua**); 中国北京市西城区金融大街31号, Beijing 100033 (CN)。 陈鸿杰 (**CHEN, Hongjie**); 中国北京市西城区金融大街31号, Beijing 100033 (CN)。 王爱宝 (**WANG, Aibao**); 中国北京市西城区金融大街31号, Beijing 100033 (CN)。 蒋春元 (**JIANG, Chunyuan**); 中国北京市西城区金融大街31号, Beijing 100033 (CN)。 李澄宇 (**LI, Chengyu**); 中国北京市西城区金融大街31号, Beijing 100033 (CN)。

(74) 代理人: 华进联合专利商标代理有限公司 (**ADVANCE CHINA IP LAW OFFICE**); 中国广东省广州市天河区珠江东路6号4501房（部位：自编01-03和08-12单元）（仅限办公用途）, Guangdong 510623 (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, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, MG, MK, MN, MU, 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, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, 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, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, 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, ME, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF,

(54) **Title:** DATA TRANSMISSION METHOD AND APPARATUS, AND COMPUTER DEVICE, STORAGE MEDIUM AND PROGRAM PRODUCT

(54) 发明名称: 数据传输方法、装置、计算机设备、存储介质和程序产品

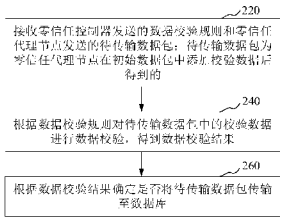

图 2

220 Receive a data checking rule, which is sent by a zero-trust controller, and a data packet to be transmitted, which is sent by a zero-trust proxy node, wherein said data packet is obtained after the zero-trust proxy node adds check data into an initial data packet

240 Perform data checking on the check data in said data packet according to the data checking rule, so as to obtain a data check result

260 According to the data checking result, determine whether to transmit said data packet to a database

(57) **Abstract:** The present application relates to a data transmission method and apparatus, and a computer device, a storage medium and a program product. The method comprises: receiving a data checking rule, which is sent by a zero-trust controller, and a data packet to be transmitted, which is sent by a zero-trust proxy node, wherein said data packet is obtained after the zero-trust proxy node adds check data into an initial data packet; performing data checking on the check data in said data packet according to the data checking rule, so as to obtain a data check result; and according to the data checking result, determining whether to transmit said data packet to a database.

(57) 摘要: 本申请涉及一种数据传输方法、装置、计算机设备、存储介质和程序产品。上述方法包括：接收零信任控制器发送的数据校验规则和零信任代理节点发送的待传输数据包；待传输数据包为零信任代理节点在初始数据包中添加校验数据后得到的；根据数据校验规则对待传输数据包中的校验数据进行数据校验，得到数据校验结果；根据数据校验结果确定是否将待传输数据包传输至数据库。

WO 2025/020437 A1

[见续页]

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))。

数据传输方法、装置、计算机设备、存储介质和程序产品

相关申请

本申请要求 2023 年 7 月 25 日申请的，申请号为 2023109131905，名称为“数据传输方法、装置、计算机设备、存储介质和程序产品”的中国专利申请的优先权，在此将其全文引入作为参考。

技术领域

本申请涉及信息安全技术领域，特别是涉及一种数据传输方法、装置、计算机设备、存储介质和程序产品。

背景技术

随着计算机技术的发展，出现了零信任网络。零信任网络是指用户之间没有信任，通过匿名的方式来进行数据传输的网络。

传统技术，可以在零信任网络中基于 TCP/IP 协议（Transmission Control Protocol/Internet Protocol，传输控制协议/网际协议）进行 IP 数据包的传输，从而实现数据的传输。

数据传输过程中的安全问题至关重要。

发明内容

第一方面，本申请提供了一种数据传输方法。应用于零信任通信网络中的零信任网关中，所述方法包括：

接收零信任控制器发送的数据校验规则和零信任代理节点发送的待传输数据包；所述待传输数据包为所述零信任代理节点在初始数据包中添加校验数据后得到的；

根据所述数据校验规则对所述待传输数据包中的校验数据进行数据校验，得到数据校验结果；

根据所述数据校验结果确定是否将所述待传输数据包传输至数据库。

在其中一个实施例中，所述校验数据包括用户会话信息和用户签名信息，所述用户会话信息用于指示与所述零信任代理节点建立会话连接过程中生成的地址信息和会话计数信息，所述用户签名信息用于指示发送所述初始数据包的用户的身份参数，所述数据校验规则包括用户会话信息校验规则及数据签名校验规则；所述根据所述数据校验规则对所述待传输数据包中的校验数据进行数据校验，得到数据校验结果，包括：

根据所述用户会话信息校验规则对所述待传输数据包中的用户会话信息进行数据校验，生成第一数据校验结果；

根据所述数据签名校验规则对所述待传输数据包中的用户签名信息进行数据校验，生成第二数据校验结果；

根据所述第一数据校验结果及所述第二数据校验结果，生成所述数据校验结果。

在其中一个实施例中，所述根据所述用户会话信息校验规则对所述待传输数据包中的用户会话信息进行数据校验，生成第一数据校验结果，包括：

根据所述地址信息确定所述待传输数据包的网络地址类型；所述网络地址类型包括公网地址类型及私网地址类型；

根据所述待传输数据包的网络地址类型，确定是否需要对所述待传输数据包中的源网络地址进行更新，生成中间数据包；

根据所述用户会话信息校验规则对所述中间数据包中的会话计数信息进行数据校验，生成所述第一数据校验结果。

在其中一个实施例中，所述根据所述待传输数据包的网络地址类型，确定是否需要对所述待传输数据包中的源网络地址进行更新，生成中间数据包，包括：

若所述待传输数据包的网络地址类型为所述私网地址类型，则将所述待传输数据包作为所述中间数据包；

若所述待传输数据包的网络地址类型为所述公网地址类型，则将所述待传输数据包中的源网络地址更新为所述待传输数据包对应的公网地址，生成所述中间数据包。

在其中一个实施例中，所述根据所述数据签名校验规则对所述待传输数据包中的用户签名信息进行数据校验，生成第二数据校验结果，包括：

根据所述数据签名校验规则对所述中间数据包中的用户签名信息进行数据校验，生成所述第二数据校验结果。

在其中一个实施例中，所述方法还包括：

从所述待传输数据包中确定校验未通过的数据包，根据所述校验未通过的数据包生成异常会话信息；

将所述异常会话信息发送至零信任控制器；所述异常会话信息用于指示所述零信任控制器对所述异常会话信息进行分析及向所述零信任代理节点发送会话终止指令。

在其中一个实施例中，所述数据校验规则是根据用户标准签名信息和用户标准会话信息生成的，其中，所述用户标准签名信息包括用户公钥信息以及用户身份标准信息。

在其中一个实施例中，所述用户标准签名信息是在用户证书验证通过的情况下，从所述用户证书中获取的。

第二方面，本申请还提供了一种数据传输方法。应用于零信任通信网络中的零信任控制器中，所述方法包括：

接收零信任代理节点发送的用户证书和用户标准会话信息；

根据所述用户证书和用户标准会话信息，生成数据校验规则；

向零信任网关发送所述数据校验规则；所述数据校验规则用于指示所述零信任网关根据所述数据校验规则对待传输数据包中的校验数据进行数据校验，得到数据校验结果；根据所述数据校验结果确定是否将所述待传输数据包传输至数据库。

在其中一个实施例中，所述根据所述用户证书和所述用户标准会话信息，生成所述数据校验规则，包括：

对所述用户证书进行验证，生成证书验证结果；

在证书验证结果为证书验证通过的情况下，从所述用户证书中获取用户标准签名信息，其中，所述用户标准签名信息包括用户公钥信息以及用户标准身份信息；以及

根据所述用户标准签名信息和所述用户标准会话信息，生成所述数据校验规则。

第三方面，本申请还提供了一种数据传输方法。应用于零信任通信网络中的零信任代理节点中，所述方法包括：

获取用户证书、用户标准会话信息和初始数据包；

将所述用户证书及所述用户标准会话信息发送至零信任控制器，以使所述零信任控制器基于所述用户证书及所述用户标准会话信息，生成数据校验规则，向零信任网关发送所述数据校验规则；

向所述初始数据包中添加校验数据，生成待传输数据包，并将所述待传输数据包发送至所述零信任网关；所述待传输数据包用于指示所述零信任网关根据所述数据校验规则对所述待传输数据包中的校验数据进行数据校验，得到数据校验结果；根据所述数据校验结果确定是否将所述待传输数据包传输至数据库。

在其中一个实施例中，所述用户证书在验证通过的情况下，使得所述零信任控制器从所述用户证书中获取用户标准签名信息并基于所述标准签名信息和所述用户标准会话信息生成数据校验规则，其中，所述用户标准签名信息包括用户公钥信息以及用户身份标准信息。

第四方面，本申请还提供了一种数据传输装置。应用于零信任通信网络中的零信任网关中，所述装置包括：

待传输数据包接收模块，用于接收零信任控制器发送的数据校验规则和零信任代理节点发送的待传输数据包；所述待传输数据包为所述零信任代理节点在初始数据包中添加校验数据后得到的；

数据校验模块，用于根据所述数据校验规则对所述待传输数据包中的校验数据进行数据校验，得到数据校验结果；

数据传输模块，用于根据所述数据校验结果确定是否将所述待传输数据包传输至数据库。

第五方面，本申请还提供了一种数据传输装置。应用于零信任通信网络中的零信任控制器中，所述装置包括：

信息接收模块，用于接收零信任代理节点发送的用户证书和用户标准会话信息；

数据校验规则生成模块，用于根据所述用户证书和用户标准会话信息，生成数据校验规则；

数据校验规则发送模块，用于向零信任网关发送所述数据校验规则；所述数据校验规则用于指示所述零信任网关根据所述数据校验规则对待传输数据包中的校验数据进行数据校验，得到数据校验结果；根据所述数据校验结果确定是否将所述待传输数据包传输至数据库。

第六方面，本申请还提供了一种数据传输装置。应用于零信任通信网络中的零信任代理节点中，所述装置包括：

信息获取模块，用于获取用户证书、用户标准会话信息和初始数据包；

信息发送数据校验模块，用于将所述用户证书及所述用户标准会话信息发送至零信任控制器，以使

所述零信任控制器基于所述用户证书及所述用户标准会话信息，生成数据校验规则，向零信任网关发送所述数据校验规则；

待传输数据包生成模块，用于向所述初始数据包中添加校验数据，生成待传输数据包，并将所述待传输数据包发送至所述零信任网关；所述待传输数据包用于指示所述零信任网关根据所述数据校验规则对所述待传输数据包中的校验数据进行数据校验，得到数据校验结果；根据所述数据校验结果确定是否将所述待传输数据包传输至数据库。

第七方面，本申请还提供了一种零信任网关，包括收发器、处理器和存储器，所述存储器存储有计算机程序，所述处理器执行所述计算机程序，用于执行上述第一方面中任一项实施例中的方法的步骤。

第八方面，本申请还提供了一种零信任控制器，包括收发器、处理器和存储器，所述存储器存储有计算机程序，所述处理器执行所述计算机程序，用于控制所述收发器接收零信任代理节点发送的用户证书和用户标准会话信息；

用于控制所述处理器根据所述用户证书和用户标准会话信息，生成数据校验规则；

用于控制所述收发器向零信任网关发送所述数据校验规则；所述数据校验规则用于指示所述零信任网关根据所述数据校验规则对待传输数据包中的校验数据进行数据校验，得到数据校验结果；根据所述数据校验结果确定是否将所述待传输数据包传输至数据库。

第九方面，本申请还提供了一种零信任代理节点，包括收发器、处理器和存储器，所述存储器存储有计算机程序，所述处理器执行所述计算机程序，用于控制所述收发器获取用户证书、用户标准会话信息和初始数据包；

用于控制所述收发器将所述用户证书及所述用户标准会话信息发送至零信任控制器，以使所述零信任控制器基于所述用户证书及所述用户标准会话信息，生成数据校验规则，向零信任网关发送所述数据校验规则；

用于控制所述处理器和所述收发器向所述初始数据包中添加校验数据，生成待传输数据包，并将所述待传输数据包发送至所述零信任网关；所述待传输数据包用于指示所述零信任网关根据所述数据校验规则对所述待传输数据包中的校验数据进行数据校验，得到数据校验结果；根据所述数据校验结果确定是否将所述待传输数据包传输至数据库。

第十方面，本申请还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，其上存储有计算机程序，所述计算机程序被处理器执行时实现上述第一方面至第三方面中任一项实施例中的方法的步骤。

第十一方面，本申请还提供了一种计算机程序产品。所述计算机程序产品，包括计算机程序，该计算机程序被处理器执行时实现上述第一方面至第三方面中任一项实施例中的方法的步骤。

第十二方面，本申请还提供了一种装置，被配置为执行上述第一方面至第三方面任一项实施例中的方法步骤。

本申请的一个或多个实施例的细节在下面的附图和描述中提出。本申请的其他特征、目的和优点将从说明书、附图以及权利要求书变得明显。

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的实施例，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，还可以根据公开的附图获得其他的附图。

图 1 为一个实施例中数据传输方法的应用环境图；

图 2 为一个实施例中零信任网关对应的数据传输方法的流程示意图；

图 3 为一个实施例中数据校验步骤的流程示意图；

图 4 为一个实施例中第一数据校验结果生成步骤的流程示意图；

图 5 为一个实施例中异常会话信息发送步骤的流程示意图；

图 6 为另一个实施例中零信任控制器对应的数据传输方法的流程示意图；

图 7 为另一个实施例中零信任代理节点对应的数据传输方法的流程示意图；

图 8 为一个实施例中待传输数据包的结构示意图；

图 9 为一个可选的实施例中零信任网关对应的数据传输方法的流程示意图；

图 10 为一个实施例中零信任通信网络对应的通信系统的结构示意图；

图 11 为一个实施例中在零信任通信网络中进行数据校验及数据传输的流程示意图；

图 12 为一个实施例中零信任网关对应的数据传输装置的结构框图；

图 13 为一个实施例中零信任控制器对应的数据传输装置的结构框图；

图 14 为一个实施例中零信任代理节点对应的数据传输装置的结构框图；

图 15 为一个实施例中零信任网关的内部结构示意图；

图 16 为另一个实施例中零信任控制器的内部结构示意图；

图 17 为又一个实施例中零信任代理节点的内部结构示意图。

具体实施方式

为了使本申请的目的、技术方案及优点更加清楚明白，以下结合附图及实施例，对本申请进行进一步详细说明。应当理解，此处描述的具体实施例仅仅用以解释本申请，并不用于限定本申请。

随着计算机技术的发展，出现了零信任网络。零信任网络是指用户之间没有信任，通过匿名的方式来进行数据传输的网络。

传统技术，可以在零信任网络中基于 TCP/IP 协议（Transmission Control Protocol/Internet Protocol，传输控制协议/网际协议）进行 IP 数据包的传输，从而实现数据的传输。

然而，在传统的数据传输过程中，数据存在被伪冒、被篡改、出现重放攻击等安全问题。因此，传统的数据传输方法，存在安全性较低的问题。

本申请实施例提供的数据传输方法，可以应用于如图 1 所示的应用环境中。其中，零信任通信网络（即零信任网络）对应的通信系统 100 中包括零信任代理节点 102、零信任控制器 104、零信任网关 106 和数据库。零信任代理节点 102 可以从用户终端处获取数据，且零信任代理节点 102 可以通过通信网络向零信任网关 106 发送数据，零信任代理节点 102 还可以向零信任控制器 104 发送数据。其中，通信网络包括公网和局域网。零信任控制器 104 可以向零信任网关 106 发送数据。零信任网关 106 可以将数据传输至数据库，或者，零信任网关 106 也可以将数据传输至零信任控制器 104。在本申请实施例中，零信任网关 106 接收零信任控制器 104 发送的数据校验规则和零信任代理节点 102 发送的待传输数据包；待传输数据包为零信任代理节点 102 在初始数据包中添加校验数据后得到的；零信任网关 106 根据数据校验规则对待传输数据包中的校验数据进行数据校验，得到数据校验结果；零信任网关 106 根据数据校验结果确定是否将待传输数据包传输至数据库。

其中，用户终端可以但不限于是各种个人计算机、笔记本电脑、智能手机、平板电脑、物联网设备和便携式可穿戴设备，物联网设备可为智能音箱、智能电视、智能空调、智能车载设备等。便携式可穿戴设备可为智能手表、智能手环、头戴设备等。零信任代理节点 102、零信任控制器 104、零信任网关 106 均可以用独立的服务器或者是多个服务器组成的服务器集群来实现。

在一个实施例中，如图 2 所示，提供了一种数据传输方法，以该方法应用于图 1 中的零信任通信网络中的零信任网关 106 为例进行说明，包括以下步骤：

S220，接收零信任控制器发送的数据校验规则和零信任代理节点发送的待传输数据包；待传输数据包为零信任代理节点在初始数据包中添加校验数据后得到的。

其中，零信任通信网络即零信任网络，零信任网络是指用户之间没有信任，通过匿名的方式来进行数据传输的网络。零信任通信网络对应的通信系统中包括零信任代理节点、零信任控制器、零信任网关和数据库。数据校验规则是由零信任代理节点生成的规则，数据校验规则用于对待传输数据包中的数据进行数据校验。待传输数据包是指需要先进行数据校验、且只有在数据校验通过之后才能进行传输的数据包。待传输数据包为零信任代理节点在初始数据包中添加校验数据后得到的数据包。初始数据包是指从用户终端处获取的数据包。校验数据是指待传输数据包中用于进行数据校验的数据。

在一些实施方式中，由于零信任通信网络对应的通信系统 100 中包括零信任代理节点 102、零信任控制器 104、零信任网关 106 和数据库，且零信任代理节点 102 和零信任控制器 104 均可以向零信任网关 106 发送数据。因此，可选地，零信任网关 106 可以同时接收零信任控制器 104 发送的数据校验规则和零信任代理节点 102 发送的待传输数据包；或者，零信任网关 106 也可以先接收零信任控制器 104 发送的数据校验规则，再接收零信任代理节点 102 发送的待传输数据包；或者，零信任网关 106 还可以先接收零信任代理节点 102 发送的待传输数据包，再接收零信任控制器 104 发送的数据校验规则。需要说明的是，在本申请实施例中，对于零信任网关 106 接收数据校验规则和接收待传输数据包的时间顺序不做限定。

S240，根据数据校验规则对待传输数据包中的校验数据进行数据校验，得到数据校验结果。

一些实施方式中，零信任网关 106 可以根据数据校验规则对待传输数据包中的校验数据进行数据校验，得到数据校验结果。示例性的，假设数据校验规则中包括校验数据阈值，且数据校验规则为：若校验数据小于或者等于校验数据阈值，则表示数据校验通过。那么，零信任网关 106 可以将校验数据阈值与待传输数据包中的校验数据进行比较，从而生成数据校验结果。其中，数据校验规则和校验数据阈值可以是根据数据包进行设置的，本申请实施例对此不做限定。数据校验结果包括数据校验通过以及数

据校验未通过。

S260，根据数据校验结果确定是否将待传输数据包传输至数据库。

一些实施方式中，零信任网关 106 可以根据数据校验结果确定是否将待传输数据包传输至数据库。示例性的，若数据校验结果为数据校验通过，则零信任网关 106 可以将待传输数据包传输至数据库。若数据校验结果为数据校验未通过，则零信任网关 106 可以丢弃待传输数据包。

上述数据传输方法中，接收零信任控制器发送的数据校验规则和零信任代理节点发送的待传输数据包；待传输数据包为零信任代理节点在初始数据包中添加校验数据后得到的；根据数据校验规则对待传输数据包中的校验数据进行数据校验，得到数据校验结果；根据数据校验结果确定是否将待传输数据包传输至数据库。本申请实施例中的零信任代理节点能够在初始数据包中添加校验数据，得到重新封装的待传输数据包。从而，零信任网关能够接收零信任控制器发送的数据校验规则以及零信任代理节点发送的、重新封装的待传输数据包，并根据数据校验规则对重新封装的待传输数据包中的校验数据进行数据校验，得到较准确的数据校验结果。进而，能够根据较准确的数据校验结果，确定是否将待传输数据包传输至数据库。由于本申请需要先根据数据校验规则对重新封装的待传输数据包中的校验数据进行数据校验，且本申请只能对数据校验通过的待传输数据包进行传输，因此，能够提高数据传输过程的安全性。

在上面的实施例中，涉及到了根据数据校验规则对待传输数据包中的校验数据进行数据校验，得到数据校验结果，下面对其具体方法进行介绍。在一个实施例中，校验数据包括用户会话信息和用户签名信息，用户会话信息用于指示与零信任代理节点建立会话连接过程中生成的地址信息和会话计数信息，用户签名信息用于指示发送初始数据包的用户的身份参数，数据校验规则包括用户会话信息校验规则及数据签名校验规则；如图 3 所示，S240 包括：

S320，根据用户会话信息校验规则对待传输数据包中的用户会话信息进行数据校验，生成第一数据校验结果。

其中，校验数据可以包括但不局限于用户会话信息和用户签名信息，用户会话信息用于指示与零信任代理节点建立会话连接过程中生成的地址信息和会话计数信息。地址信息包括源网络地址、目的网络地址以及发送待传输数据包的网络地址等信息。会话计数信息是指会话信息的数量。用户签名信息用于指示发送初始数据包的用户的身份参数。身份参数可以包括但不局限于用户名称、用户的身份认证标识等。从而，零信任网关 106 可以接收地址信息、会话计数信息及用户的身份参数等校验数据。数据校验规则包括用户会话信息校验规则及数据签名校验规则。用户会话信息校验规则是指对地址信息、会话计数信息等用户会话信息进行数据校验的规则，数据签名校验规则是指对用户签名信息进行数据校验的规则。

一些实施方式中，零信任网关 106 可以根据用户会话信息校验规则对待传输数据包中的用户会话信息进行数据校验，生成第一数据校验结果。示例性的，假设用户会话信息校验规则中包括会话信息阈值，且用户会话信息校验规则为：若用户会话信息小于或者等于会话信息阈值，则表示会话信息校验通过。那么，零信任网关 106 可以将会话信息阈值与待传输数据包中的用户会话信息进行比较，从而生成第一数据校验结果。其中，用户会话信息校验规则和会话信息阈值可以是根据数据包进行设置的，本申请实施例对此不做限定。第一数据校验结果包括会话信息校验通过以及会话信息校验未通过。

S340，根据数据签名校验规则对待传输数据包中的用户签名信息进行数据校验，生成第二数据校验结果。

一些实施方式中，零信任网关 106 可以根据数据签名校验规则对待传输数据包中的用户签名信息进行数据校验，生成第二数据校验结果。示例性的，假设数据签名校验规则中包括数据签名阈值，且数据签名校验规则为：若用户签名信息小于或者等于数据签名阈值，则表示数据签名校验通过。那么，零信任网关 106 可以将数据签名阈值与待传输数据包中的用户签名信息进行比较，从而生成第二数据校验结果。其中，数据签名校验规则和数据签名阈值可以是根据数据包进行设置的，本申请实施例对此不做限定。第二数据校验结果包括数据签名校验通过以及数据签名校验未通过。

S360，根据第一数据校验结果及第二数据校验结果，生成数据校验结果。

一些实施方式中，零信任网关 106 可以根据第一数据校验结果及第二数据校验结果，确定会话信息校验是否通过以及数据签名校验是否通过。若第一数据校验结果为会话信息校验通过，且第二数据校验结果为数据签名校验通过，即会话信息校验和数据签名校验均通过，则确定数据校验结果为数据校验通过。若第一数据校验结果为会话信息校验未通过，和/或，第二数据校验结果为数据签名校验未通过，即会话信息校验和数据签名校验中存在至少一次校验未通过，则确定数据校验结果为数据校验未通过。

本实施例中，由于校验数据包括用户会话信息和用户签名信息，且数据校验规则包括用户会话信息校验规则及数据签名校验规则。因此，根据用户会话信息校验规则对待传输数据包中的用户会话信息进

行数据校验，能够较准确地生成第一数据校验结果；根据数据签名校验规则对待传输数据包中的用户签名信息进行数据校验，能够较准确地生成第二数据校验结果。从而，能够根据较准确的第一数据校验结果及较准确的第二数据校验结果，生成较准确的数据校验结果。

在上面的实施例中，涉及到了根据用户会话信息校验规则对待传输数据包中的用户会话信息进行数据校验，生成第一数据校验结果，下面对其具体方法进行介绍。在一个实施例中，如图 4 所示，S320 包括：

S420，根据地址信息确定待传输数据包的网络地址类型；网络地址类型包括公网地址类型及私网地址类型。

一些实施方式中，零信任网关 106 可以从待传输数据包地址信息中获取发送待传输数据包的网络地址，并根据该发送待传输数据包的网络地址，确定待传输数据包的网络地址类型。其中，网络地址类型包括公网地址类型及私网地址类型。公网地址是指在因特网上可以直接进行访问的地址。私网地址是指在私网上可以直接进行访问的地址。私网即为局域网，局域网是在局部地区形成的一个区域网络，只有特定区域内的计算机设备可以访问私网。示例性的，若发送待传输数据包的网络地址为私网地址，则零信任网关 106 可以确定待传输数据包的网络地址类型为私网地址类型；若发送待传输数据包的网络地址为公网地址，则零信任网关 106 可以确定待传输数据包的网络地址类型为公网地址类型。

S440，根据待传输数据包的网络地址类型，确定是否需要对待传输数据包中的源网络地址进行更新，生成中间数据包。

一些实施方式中，零信任网关 106 可以根据待传输数据包的网络地址类型，确定发送待传输数据包的网络地址是公网地址还是私网地址，从而确定是否需要对待传输数据包中的源网络地址进行更新，进而生成中间数据包。其中，中间数据包为基于待传输数据包的网络地址类型所生成的数据包。

在其中一个实施例中，S440 包括：

若待传输数据包的网络地址类型为私网地址类型，则将待传输数据包作为中间数据包。

若待传输数据包的网络地址类型为公网地址类型，则将待传输数据包中的源网络地址更新为待传输数据包对应的公网地址，生成中间数据包。

若待传输数据包的网络地址类型为私网地址类型，即发送待传输数据包的网络地址是私网地址，则说明未对待传输数据包进行网络地址转换（Network Address Translation，NAT）。此时，待传输数据包中的源网络地址与私网地址相同，因此，零信任网关 106 可以对待传输数据包不做更新处理，直接将待传输数据包作为中间数据包。

若待传输数据包的网络地址类型为公网地址类型，即发送待传输数据包的网络地址是公网地址，则说明对待传输数据包进行了网络地址转换（Network Address Translation，NAT）。此时，待传输数据包中的源网络地址仍为私网地址，但是，待传输数据包的真实网络地址为公网地址，即待传输数据包中的源网络地址与真实网络地址（即公网地址）不相同，因此，零信任网关 106 可以将待传输数据包中的源网络地址更新为待传输数据包对应的公网地址，从而生成中间数据包。

S460，根据用户会话信息校验规则对中间数据包中的会话计数信息进行数据校验，生成第一数据校验结果。

一些实施方式中，零信任网关 106 可以根据用户会话信息校验规则对中间数据包中的会话计数信息进行数据校验，生成第一数据校验结果。示例性的，假设用户会话信息校验规则中包括标准会话计数，且用户会话信息校验规则包括：若中间数据包中的会话计数信息小于或者等于标准会话计数，则表示会话信息校验通过。那么，零信任网关 106 可以将标准会话计数与中间数据包中的会话计数信息进行比较，从而生成第一数据校验结果。其中，用户会话信息校验规则和标准会话计数可以是根据数据包进行设置的，本申请实施例对此不做限定。需要说明的是，根据会话计数信息的校验过程，零信任网关 106 可以确定是否接收到多余的会话信息，若接收到多余的会话信息，则说明出现重放攻击的现象，此时，第一数据校验结果为会话信息校验未通过，从而能够有效地避免出现重放攻击的现象。

本实施例中，根据地址信息确定待传输数据包的网络地址类型，能够较准确地确定出网络地址类型为公网地址类型还是私网地址类型。从而，能够根据待传输数据包的网络地址类型，较准确地确定是否需要对待传输数据包中的源网络地址进行更新，从而生成包含准确的源网络地址的中间数据包。进而，根据用户会话信息校验规则对包含准确的源网络地址的中间数据包中的会话计数信息进行数据校验，就能够较准确地生成第一数据校验结果。

在上面的实施例中，涉及到了根据数据签名校验规则对待传输数据包中的用户签名信息进行数据校验，生成第二数据校验结果，下面对其具体方法进行介绍。在一个实施例中，S340 包括：

根据数据签名校验规则对中间数据包中的用户签名信息进行数据校验，生成第二数据校验结果。

一些实施方式中，零信任网关 106 可以根据数据签名校验规则对中间数据包中的用户签名信息进

行数据校验，生成第二数据校验结果。示例性的，假设用户会话信息校验规则中包括用户标准签名，且用户会话信息校验规则包括：若中间数据包中的用户签名信息等于用户标准签名，则表示会话信息校验通过。那么，零信任网关 106 可以将用户标准签名与中间数据包中的用户签名信息进行比较，从而生成第二数据校验结果。其中，用户会话信息校验规则和用户标准签名可以是根据数据包进行设置的，本申请实施例对此不做限定。

本实施例中，根据数据签名校验规则对包含准确的源网络地址的中间数据包中的用户签名信息进行数据校验，能够较准确地生成第二数据校验结果。

在上面的实施例中，涉及到了根据数据校验结果确定是否将待传输数据包传输至数据库，下面对另一个实施例中的具体方法进行介绍。在一个实施例中，如图 5 所示，上述数据传输方法还包括：

S520，从待传输数据包中确定校验未通过的数据包，根据校验未通过的数据包生成异常会话信息。

一些实施方式中，若待传输数据包的数据校验结果为数据校验未通过，即会话信息校验和数据签名校验中存在至少一次校验未通过，则零信任网关 106 可以确定该待传输数据包是校验未通过的数据包。基于此，零信任网关 106 可以从待传输数据包中确定校验未通过的数据包，并根据校验未通过的数据包生成该校验未通过的数据包对应的异常会话信息。之后，零信任网关 106 还可以丢弃该校验未通过的数据包。

S540，将异常会话信息发送至零信任控制器；异常会话信息用于指示零信任控制器对异常会话信息进行分析及向零信任代理节点发送会话终止指令。

一些实施方式中，零信任网关 106 可以将异常会话信息发送至零信任控制器 104。其中，异常会话信息表示的是该待传输数据包对应的会话信息存在异常，异常会话信息用于指示零信任控制器 104 对异常会话信息进行分析及向零信任代理节点 102 发送会话终止指令。会话终止指令用于指示将异常的会话信息对应的会话进行终止。

本实施例中，从待传输数据包中确定校验未通过的数据包，并根据校验未通过的数据包较准确地生成异常会话信息。之后，将较准确的异常会话信息发送至零信任控制器，以使零信任控制器对异常会话信息进行分析，并向零信任代理节点发送会话终止指令，从而能够根据异常会话信息终止异常会话。

在一个实施例中，如图 6 所示，还提供了一种数据传输方法，以该方法应用于图 1 中的零信任通信网络中的零信任控制器 104 为例进行说明，包括以下步骤：

S620，接收零信任代理节点发送的用户证书和用户标准会话信息。

一些实施方式中，零信任控制器 104 可以接收零信任代理节点 102 发送的用户证书和用户标准会话信息。其中，用户证书是由证书颁发机构（Certificate Authority，CA）签发给用户的证书。用户标准会话信息可以包括但不局限于用户真实的五元组信息。五元组信息通常可以包括源网络地址、源端口、目的网络地址、目的端口和传输层协议。

S640，根据用户证书和用户标准会话信息，生成数据校验规则。

一些实施方式中，零信任控制器 104 可以对用户证书进行证书验证，生成证书验证结果。在证书验证结果为证书验证通过的情况下，零信任控制器 104 可以从用户证书中获取用户标准签名信息。从而，零信任控制器 104 可以根据用户标准签名信息和用户标准会话信息，生成数据校验规则。其中，用户标准签名信息包括用户公钥信息以及用户标准身份信息。用户公钥信息用于对用户标准身份信息进行加密。用户标准身份信息可以包括用户真实的身份参数。数据校验规则中包括用户标准签名信息对应的校验规则和用户标准会话信息对应的校验规则。

S660，向零信任网关发送数据校验规则；数据校验规则用于指示零信任网关根据数据校验规则对待传输数据包中的校验数据进行数据校验，得到数据校验结果；根据数据校验结果确定是否将待传输数据包传输至数据库。

一些实施方式中，零信任控制器 104 可以向零信任网关 106 发送数据校验规则，以使零信任网关 106 根据数据校验规则对待传输数据包中的校验数据进行数据校验，得到数据校验结果；从而，以使零信任网关 106 根据数据校验结果确定是否将待传输数据包传输至数据库。其中，零信任网关 106 进行数据校验及数据传输的步骤详见上述实施例，在此不做赘述。

上述数据传输方法中，接收零信任代理节点发送的用户证书和用户标准会话信息，能够获取较准确的用户证书和用户标准会话信息。从而，能够根据较准确的用户证书和用户标准会话信息，较准确地生成数据校验规则，并能够向零信任网关发送较准确的数据校验规则。其中，较准确的数据校验规则用于指示零信任网关根据数据校验规则对待传输数据包中的校验数据进行数据校验，得到数据校验结果；根据数据校验结果确定是否将待传输数据包传输至数据库。

在一个实施例中，如图 7 所示，还提供了一种数据传输方法，以该方法应用于图 1 中的零信任通信网络中的零信任代理节点 102 为例进行说明，包括以下步骤：

S720，获取用户证书、用户标准会话信息和初始数据包。

一些实施方式中，零信任代理节点 102 可以从用户终端处获取用户证书。零信任代理节点 102 还可以与零信任网关 106 建立会话连接，生成用户标准会话信息。零信任代理节点 102 还可以从用户终端处获取初始数据包。其中，初始数据包是指未添加校验数据的数据包。

S740，将用户证书及用户标准会话信息发送至零信任控制器，以使零信任控制器基于用户证书及用户标准会话信息，生成数据校验规则，向零信任网关发送数据校验规则。

一些实施方式中，零信任代理节点 102 可以向零信任控制器 104 进行用户注册，以将用户证书发送至零信任控制器 104。此外，由于零信任代理节点 102 可以与零信任网关 106 建立会话连接，因此，零信任代理节点 102 可以通过零信任网关 106 对用户标准会话信息进行标准会话信息校验，生成标准会话信息校验结果。在标准会话信息校验结果为标准会话信息校验通过的情况下，零信任代理节点 102 可以通过零信任网关 106 将校验通过的标准会话信息发送至零信任控制器 104，以使零信任控制器 104 基于用户证书及用户标准会话信息，生成数据校验规则，并向零信任网关 106 发送数据校验规则。

S760，向初始数据包中添加校验数据，生成待传输数据包，并将待传输数据包发送至零信任网关；待传输数据包用于指示零信任网关根据数据校验规则对待传输数据包中的校验数据进行数据校验，得到数据校验结果，及根据数据校验结果确定是否将待传输数据包传输至数据库。

图 8 为一个实施例中待传输数据包的结构示意图。初始数据包中包括初始数据包的版本（一般为 4 位）、头部长度（一般为 4 位）、服务类型（一般为 8 位）、总长度（一般为 16 位）、标识符（一般为 16 位）、标志（一般为 3 位）、偏移量（一般为 13 位）、生存时间 TTL（Time To Live，用于指示初始数据包被丢弃之前允许通过的最大网段数量，一般为 8 位）、协议（一般为 8 位）、校验位（一般为 16 位）、源网络地址（一般为 32 位）、目的网络地址（一般为 32 位）、选项、数据等。零信任代理节点 102 可以在初始数据包的末端中添加校验数据，生成待传输数据包。其中，校验数据包括用户会话信息和用户签名信息。示例性的，用户会话信息可以包括会话计数器字段，会话计数器字段用于对会话信息的数量进行计数。用户签名信息可以包括数据签名信息字段，数据签名信息字段通常可以是 32 位的字段。此外，还需要将初始数据包的总长度更新为添加校验数据之后的数据包的总长度。

之后，零信任代理节点 102 可以将待传输数据包发送至零信任网关 106。待传输数据包用于指示零信任网关 106 根据数据校验规则对待传输数据包中的校验数据进行数据校验，得到数据校验结果；零信任网关 106 根据数据校验结果确定是否将待传输数据包传输至数据库。其中，零信任网关 106 进行数据校验及数据传输的步骤详见上述实施例，在此不做赘述。

上述数据传输方法中，能够获取较准确的用户证书、用户标准会话信息和初始数据包；将较准确的用户证书及用户标准会话信息发送至零信任控制器，以使零信任控制器基于较准确的用户证书及用户标准会话信息，生成数据校验规则，向零信任网关发送数据校验规则。还能够向初始数据包中添加较准确的校验数据，生成较准确的待传输数据包，并将较准确的待传输数据包发送至零信任网关。其中，较准确的待传输数据包用于指示零信任网关根据数据校验规则对待传输数据包中的校验数据进行数据校验，得到数据校验结果；根据数据校验结果确定是否将待传输数据包传输至数据库。

在一个可选的实施例中，如图 9 所示，提供了一种数据传输方法，应用于零信任通信网络中的零信任网关 106，上述数据传输方法包括：

S902，接收零信任控制器发送的数据校验规则和零信任代理节点发送的待传输数据包；待传输数据包为零信任代理节点在初始数据包中添加校验数据后得到的；

S904，根据地址信息确定待传输数据包的网络地址类型；网络地址类型包括公网地址类型及私网地址类型；

S906，若待传输数据包的网络地址类型为私网地址类型，则将待传输数据包作为中间数据包；

S908，若待传输数据包的网络地址类型为公网地址类型，则将待传输数据包中的源网络地址更新为待传输数据包对应的公网地址，生成中间数据包；

S910，根据用户会话信息校验规则对中间数据包中的会话计数信息进行数据校验，生成第一数据校验结果；

S912，根据数据签名校验规则对中间数据包中的用户签名信息进行数据校验，生成第二数据校验结果；

S914，根据第一数据校验结果及第二数据校验结果，生成数据校验结果；

S916，根据数据校验结果确定是否将待传输数据包传输至数据库；

S918，从待传输数据包中确定校验未通过的数据包，根据校验未通过的数据包生成异常会话信息；

S920，将异常会话信息发送至零信任控制器；异常会话信息用于指示零信任控制器对异常会话信息进行分析及向零信任代理节点发送会话终止指令。

图 10 为一个实施例中零信任通信网络对应的通信系统的结构示意图。零信任通信网络（即零信任网络）对应的通信系统 100 中包括零信任代理节点 102、零信任控制器 104、零信任网关 106 和数据库。其中，可以在零信任代理节点 102 和零信任网关 106 之间通过通信网络传输控制流消息数据或者业务流消息数据；可以在零信任控制器 104 和零信任网关 106 之间传输控制流消息数据；可以在零信任网关 106 和数据库之间传输业务流消息数据。控制流消息数据是指包含一定顺序的消息，业务流消息数据是指包含一定动作或事务的消息。零信任代理节点 102 可以对初始数据包进行数据签名（即添加校验信息），生成待传输数据包，且可以将待传输数据包发送至零信任网关 106。其中，数据签名的过程可以包括 PKI（公钥基础设施，Public Key Infrastructure）数字签名过程。零信任网关 106 可以对待传输数据包进行数据校验，生成数据校验结果。

图 11 为一个实施例中在零信任通信网络中进行数据校验及数据传输的流程示意图。S1102，零信任代理节点 102 可以获取用户证书，并可以向零信任控制器 104 进行用户注册，以将用户证书发送至零信任控制器 104。S1104，零信任控制器 104 可以接收零信任代理节点 102 发送的用户证书，并对用户证书进行证书验证，生成证书验证结果。在证书验证结果为证书验证通过的情况下，零信任控制器 104 可以从用户证书中获取用户标准签名信息。S1106，零信任代理节点 102 还可以与零信任网关 106 建立会话连接，生成用户标准会话信息。之后，零信任代理节点 102 可以通过零信任网关 106 对用户标准会话信息进行标准会话信息校验，生成标准会话信息校验结果。S1108，在标准会话信息校验结果为标准会话信息校验通过的情况下，零信任代理节点 102 可以通过零信任网关 106 将校验通过的标准会话信息发送至零信任控制器 104。S1110，零信任控制器 104 可以根据用户标准签名信息和用户标准会话信息，生成数据校验规则。S1112，零信任控制器 104 可以向零信任网关 106 发送数据校验规则。

结合图 11 所示，S1114，零信任代理节点 102 还可以从用户终端处获取初始数据包，并可以在初始数据包的末端中添加校验数据，生成待传输数据包。之后，S1116，零信任代理节点 102 可以将待传输数据包发送至零信任网关 106。零信任网关 106 接收零信任控制器 104 发送的数据校验规则和零信任代理节点 102 发送的待传输数据包，并根据校验数据中的地址信息确定待传输数据包的网络地址类型；网络地址类型包括公网地址类型及私网地址类型。S1118，若待传输数据包的网络地址类型为私网地址类型，则将待传输数据包作为中间数据包，并根据用户会话信息校验规则对中间数据包中的会话计数信息进行数据校验，生成第一数据校验结果；根据数据签名校验规则对中间数据包中的用户签名信息进行数据校验，生成第二数据校验结果；根据第一数据校验结果及第二数据校验结果，生成数据校验结果。

结合图 11 所示，S1120，若待传输数据包的网络地址类型为公网地址类型，则将待传输数据包中的源网络地址更新为待传输数据包对应的公网地址，生成中间数据包；并根据用户会话信息校验规则对中间数据包中的会话计数信息进行数据校验，生成第一数据校验结果；根据数据签名校验规则对中间数据包中的用户签名信息进行数据校验，生成第二数据校验结果；根据第一数据校验结果及第二数据校验结果，生成数据校验结果。S1122，在数据校验结果为校验通过的情况下，零信任网关 106 可以将校验通过的待传输数据包传输至数据库。S1124，在数据校验结果为校验未通过的情况下，零信任网关 106 可以从待传输数据包中确定校验未通过的数据包，根据校验未通过的数据包生成异常会话信息，并将异常会话信息发送至零信任控制器 104。零信任网关 106 还可以将校验未通过的数据包进行丢弃。S1126，零信任控制器 104 可以对异常会话信息进行分析，并向零信任代理节点 102 发送会话终止指令，以使零信任代理节点 102 根据会话终止指令终止会话。

上述数据传输方法中，本申请实施例中的零信任代理节点能够对初始数据包进行数据签名，即能够在初始数据包中添加用户会话信息和用户签名信息，得到重新封装的待传输数据包。且本申请实施例中的零信任控制器能够生成较准确的数据校验规则。从而，零信任网关能够接收零信任控制器发送的较准确的数据校验规则以及零信任代理节点发送的、重新封装的待传输数据包，并根据较准确的数据校验规则对重新封装的待传输数据包中的用户会话信息和用户签名信息进行数据校验，得到较准确的数据校验结果。进而，能够根据较准确的数据校验结果，确定是否将待传输数据包传输至数据库。由于本申请需要先根据较准确的数据校验规则对重新封装的待传输数据包中的校验数据进行数据校验，且本申请只能对数据校验通过的待传输数据包进行传输，因此，能够提高数据传输过程的安全性。

应该理解的是，虽然如上的各实施例所涉及的流程图中的各个步骤按照箭头的指示依次显示，但是这些步骤并不是必然按照箭头指示的顺序依次执行。除非本文中有明确的说明，这些步骤的执行并没有严格的顺序限制，这些步骤可以以其它的顺序执行。而且，如上的各实施例所涉及的流程图中的至少一部分步骤可以包括多个步骤或者多个阶段，这些步骤或者阶段并不必然是在同一时刻执行完成，而是可以在不同的时刻执行，这些步骤或者阶段的执行顺序也不必然是依次进行，而是可以与其它步骤或者其它步骤中的步骤或者阶段的至少一部分轮流或者交替地执行。

基于同样的发明构思，本申请实施例还提供了一种用于实现上述所涉及的数据传输方法的数据传

输装置。该装置所提供的解决问题的实现方案与上述方法中所记载的实现方案相似，故下面所提供的一个或多个数据传输装置实施例中的具体限定可以参见上文中对于数据传输方法的限定，在此不再赘述。

在一个实施例中，如图 12 所示，提供了一种数据传输装置 1200，应用于零信任通信网络中的零信任网关中，包括：待传输数据包接收模块 1220、数据校验模块 1240 和数据传输模块 1260，其中：

待传输数据包接收模块 1220，用于接收零信任控制器发送的数据校验规则和零信任代理节点发送的待传输数据包；待传输数据包为零信任代理节点在初始数据包中添加校验数据后得到的。

数据校验模块 1240，用于根据数据校验规则对待传输数据包中的校验数据进行数据校验，得到数据校验结果。

数据传输模块 1260，用于根据数据校验结果确定是否将待传输数据包传输至数据库。

在其中一个实施例中，校验数据包括用户会话信息和用户签名信息，用户会话信息用于指示与零信任代理节点建立会话连接过程中生成的地址信息和会话计数信息，用户签名信息用于指示发送初始数据包的用户的身份参数，数据校验规则包括用户会话信息校验规则及数据签名校验规则；数据校验模块 1240 包括：

第一数据校验结果生成单元，用于根据用户会话信息校验规则对待传输数据包中的用户会话信息进行数据校验，生成第一数据校验结果；

第二数据校验结果生成单元，用于根据数据签名校验规则对待传输数据包中的用户签名信息进行数据校验，生成第二数据校验结果；

数据校验单元，用于根据第一数据校验结果及第二数据校验结果，生成数据校验结果。

在其中一个实施例中，第一数据校验结果生成单元包括：

网络地址类型确定子单元，用于根据地址信息确定待传输数据包的网络地址类型；网络地址类型包括公网地址类型及私网地址类型；

中间数据包生成子单元，用于根据待传输数据包的网络地址类型，确定是否需要对待传输数据包中的源网络地址进行更新，生成中间数据包；

第一数据校验结果生成子单元，用于根据用户会话信息校验规则对中间数据包中的会话计数信息进行数据校验，生成第一数据校验结果。

在其中一个实施例中，中间数据包生成子单元包括：

第一中间数据包生成子单元，用于在待传输数据包的网络地址类型为私网地址类型的情况下，将待传输数据包作为中间数据包；

第二中间数据包生成子单元，用于在待传输数据包的网络地址类型为公网地址类型的情况下，将待传输数据包中的源网络地址更新为待传输数据包对应的公网地址，生成中间数据包。

在其中一个实施例中，第二数据校验结果生成单元包括：

第二数据校验结果生成子单元，用于根据数据签名校验规则对中间数据包中的用户签名信息进行数据校验，生成第二数据校验结果。

在其中一个实施例中，数据传输装置 1200 还包括：

异常会话信息生成模块，用于从待传输数据包中确定校验未通过的数据包，根据校验未通过的数据包生成异常会话信息；

异常会话信息发送模块，用于将异常会话信息发送至零信任控制器；异常会话信息用于指示零信任控制器对异常会话信息进行分析及向零信任代理节点发送会话终止指令。

在一个实施例中，如图 13 所示，还提供了一种数据传输装置 1300，应用于零信任通信网络中的零信任控制器中，包括：信息接收模块 1320、数据校验规则生成模块 1340 和数据校验规则发送模块 1360，其中：

信息接收模块 1320，用于接收零信任代理节点发送的用户证书和用户标准会话信息。

数据校验规则生成模块 1340，用于根据用户证书和用户标准会话信息，生成数据校验规则。

数据校验规则发送模块 1360，用于向零信任网关发送数据校验规则；数据校验规则用于指示零信任网关根据数据校验规则对待传输数据包中的校验数据进行数据校验，得到数据校验结果；根据数据校验结果确定是否将待传输数据包传输至数据库。

在一个实施例中，如图 14 所示，还提供了一种数据传输装置 1400，应用于零信任通信网络中的零信任代理节点中，包括：信息获取模块 1420、信息发送数据校验模块 1440 和待传输数据包生成模块 1460，其中：

信息获取模块，用于获取用户证书、用户标准会话信息和初始数据包。

信息发送数据校验模块，用于将用户证书及用户标准会话信息发送至零信任控制器，以使零信任控制器基于用户证书及用户标准会话信息，生成数据校验规则，向零信任网关发送数据校验规则。

待传输数据包生成模块，用于向初始数据包中添加校验数据，生成待传输数据包，并将待传输数据包发送至零信任网关；待传输数据包用于指示零信任网关根据数据校验规则对待传输数据包中的校验数据进行数据校验，得到数据校验结果；根据数据校验结果确定是否将待传输数据包传输至数据库。

上述数据传输装置中的各个模块可全部或部分通过软件、硬件及其组合来实现。上述各模块可以硬件形式内嵌于或独立于计算机设备中的处理器中，也可以以软件形式存储于计算机设备中的存储器中，以便于处理器调用执行以上各个模块对应的操作。

图 15 是本发明实施例提供的零信任网关的结构示意图。图 15 所示的零信任网关 1500 包括：至少一个处理器 1501、存储器 1502、至少一个网络接口 1504。零信任网关 1500 中的各个组件通过总线系统 1505 耦合在一起。可理解，总线系统 1505 用于实现这些组件之间的连接通信。总线系统 1505 除包括数据总线之外，还包括电源总线、控制总线和状态信号总线。但是为了清楚说明起见，在图 15 中将各种总线都标为总线系统 1505。另外，本发明实施例中，零信任网关 1500 还包括收发器 1506，收发器可以是多个元件，即包括发送器和接收器，提供用于在传输介质上与各种其他装置通信的单元。

可以理解，本发明实施例中的存储器 1502 可以是易失性存储器或非易失性存储器，或可包括易失性和非易失性存储器两者。其中，非易失性存储器可以是只读存储器(Read-OnlyMemory，ROM)、可编程只读存储器 (ProgrammableROM，PROM)、可擦除可编程只读存储器(ErasablePROM，EPROM)、电可擦除可编程只读存储器(ElectricallyEPROM，EEPROM)或闪存。易失性存储器可以是随机存取存储器(RandomAccessMemory，RAM)，其用作外部高速缓存。通过示例性但不是限制性说明，许多形式的 RAM 可用，例如静态随机存取存储器(StaticRAM，SRAM)、动态随机存取存储器 (DynamicRAM，DRAM)、同步动态随机存取存储器(SynchronousDRAM，SDRAM)、双倍数据速率同步动态随机存取存储器(DoubleDataRate SDRAM，DDRSDRAM)、增强型同步动态随机存取存储器(Enhanced SDRAM，ESDRAM)、同步连接动态随机存取存储器(SynchlinkDRAM，SLDRAM)和直接内存总线随机存取存储器(DirectRambusRAM，DRRAM)。本发明实施例描述的系统和方法的存储器 1502 旨在包括但不限于这些和任意其它适合类型的存储器。

在一些实施方式中，存储器 1502 存储了如下的元素，可执行模块或者数据结构，或者他们的子集，或者他们的扩展集：操作系统 1502a。其中，操作系统 1502a，包含各种系统程序，例如框架层、核心库层、驱动层等，用于实现各种基础业务以及处理基于硬件的任务。

在本发明实施例中，通过调用存储器 1502 存储的程序或指令，使得接收器，用于接收零信任控制器发送的数据校验规则和零信任代理节点发送的待传输数据包；待传输数据包为零信任代理节点在初始数据包中添加校验数据后得到的；处理器 1501，用于根据数据校验规则对待传输数据包中的校验数据进行数据校验，得到数据校验结果；发送器，用于根据数据校验结果确定是否将待传输数据包传输至数据库。

上述本发明实施例揭示的部分或者全部方法还可以应用于处理器 1501 中，或者由处理器 1501 实现，或者由处理器 1501 与其他元件（例如收发器）配合实现。处理器 1501 可能是一种集成电路芯片，具有信号的处理能力。在实现过程中，上述方法的各步骤可以通过处理器 1501 中的硬件的集成逻辑电路或者软件形式的指令完成。上述的处理器 1501 可以是通用处理器、数字信号处理器(DigitalSignalProcessor，DSP)、专用集成电路(ApplicationSpecific IntegratedCircuit，ASIC)、现成可编程门阵列(FieldProgrammableGateArray，FPGA)或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件。可以实现或者执行本发明实施例中的公开的各方法、步骤及逻辑框图。通用处理器可以是微处理器或者该处理器也可以是任何常规的处理器等。结合本发明实施例所公开的方法的步骤可以直接体现为硬件译码处理器执行完成，或者用译码处理器中的硬件及软件模块组合执行完成。软件模块可以位于随机存储器，闪存、只读存储器，可编程只读存储器或者电可擦写可编程存储器、寄存器等本领域成熟的存储介质中。该存储介质位于存储器 1502，处理器 1501 读取存储器 1502 中的信息，结合其硬件完成上述方法的步骤。

可以理解的是，本发明实施例描述的这些实施例可以用硬件、软件、固件、中间件、微码或其组合来实现。对于硬件实现，处理单元可以实现在一个或多个专用集成电路(ApplicationSpecificIntegratedCircuits，ASIC)、数字信号处 理器(DigitalSignalProcessing，DSP)、数字信号处理设备(DSPDevice，DSPD)、可编程逻辑设备(ProgrammableLogicDevice，PLD)、现场可编程门阵列(Field-ProgrammableGateArray，FPGA)、通用处理器、控制器、微控制器、微处理器、用于执行本申请功能的其它电子单元或其组合中。

对于软件实现，可通过执行本发明实施例功能的模块(例如过程、函数等)来实现本发明实施例的技术。软件代码可存储在存储器中并通过处理器 1501 执行。存储器可以在处理器 1501 中或在处理器 1501 外部实现。

在一个实施例中，校验数据包括用户会话信息和用户签名信息，用户会话信息用于指示与零信任代理节点建立会话连接过程中生成的地址信息和会话计数信息，用户签名信息用于指示发送初始数据包的用户的身份参数，数据校验规则包括用户会话信息校验规则及数据签名校验规则；处理器，具体用于根据用户会话信息校验规则对待传输数据包中的用户会话信息进行数据校验，生成第一数据校验结果；根据数据签名校验规则对待传输数据包中的用户签名信息进行数据校验，生成第二数据校验结果；根据第一数据校验结果及第二数据校验结果，生成数据校验结果。

在一个实施例中，处理器，还用于根据地址信息确定待传输数据包的网络地址类型；网络地址类型包括公网地址类型及私网地址类型；根据待传输数据包的网络地址类型，确定是否需要对待传输数据包中的源网络地址进行更新，生成中间数据包；根据用户会话信息校验规则对中间数据包中的会话计数信息进行数据校验，生成第一数据校验结果。

在一个实施例中，处理器，还用于若待传输数据包的网络地址类型为私网地址类型，则将待传输数据包作为中间数据包；若待传输数据包的网络地址类型为公网地址类型，则将待传输数据包中的源网络地址更新为待传输数据包对应的公网地址，生成中间数据包。

在一个实施例中，处理器，还用于根据数据签名校验规则对中间数据包中的用户签名信息进行数据校验，生成第二数据校验结果。

在一个实施例中，处理器，还用于从待传输数据包中确定校验未通过的数据包，根据校验未通过的数据包生成异常会话信息；发送器，还用于将异常会话信息发送至零信任控制器；异常会话信息用于指示零信任控制器对异常会话信息进行分析及向零信任代理节点发送会话终止指令。

图 16 是本发明实施例提供的零信任控制器的结构示意图。图 16 所示的零信任控制器 1600 包括：至少一个处理器 1601、存储器 1602、至少一个网络接口 1604。零信任控制器 1600 中的各个组件通过总线系统 1605 耦合在一起。可理解，总线系统 1605 用于实现这些组件之间的连接通信。总线系统 1605 除包括数据总线之外，还包括电源总线、控制总线和状态信号总线。但是为了清楚说明起见，在图 16 中将各种总线都标为总线系统 1605。另外，本发明实施例中，还包括收发器 1606，收发器可以是多个元件，即包括发送器和接收器，提供用于在传输介质上与各种其他装置通信的单元。

可以理解，本发明实施例中的存储器 1602 可以是易失性存储器或非易失性存储器，或可包括易失性和非易失性存储器两者。其中，非易失性存储器可以是只读存储器(Read-OnlyMemory，ROM)、可编程只读存储器 (ProgrammableROM，PROM)、可擦除可编程只读存储器(ErasablePROM，EPROM)、电可擦除可编程只读存储器(ElectricallyEPROM，EEPROM)或闪存。易失性存储器可以是随机存取存储器(RandomAccessMemory，RAM)，其用作外部高速缓存。通过示例性但不是限制性说明，许多形式的 RAM 可用，例如静态随机存取存储器(StaticRAM，SRAM)、动态随机存取存储器 (DynamicRAM，DRAM)、同步动态随机存取存储器(SynchronousDRAM，SDRAM)、双倍数据速率同步动态随机存取存储器(DoubleDataRate SDRAM，DDRSDRAM)、增强型同步动态随机存取存储器(Enhanced SDRAM，ESDRAM)、同步连接动态随机存取存储器(SynchlinkDRAM，SLDRAM)和直接内存总线随机存取存储器(DirectRambusRAM，DRRAM)。 本发明实施例描述的系统和方法的存储器 1602 旨在包括但不限于这些和任意其它适合类型的存储器。

在一些实施方式中，存储器 1602 存储了如下的元素，可执行模块或者数据结构，或者他们的子集，或者他们的扩展集：操作系统 1602a。其中，操作系统 1602a，包含各种系统程序，例如框架层、核心库层、驱动层等，用于实现各种基础业务以及处理基于硬件的任务。

在本发明实施例中，通过调用存储器 1602 存储的程序或指令，使得接收器，用于接收零信任代理节点发送的用户证书和用户标准会话信息；处理器 1601，用于根据用户证书和用户标准会话信息，生成数据校验规则；发送器，用于向零信任网关发送数据校验规则；数据校验规则用于指示零信任网关根据数据校验规则对待传输数据包中的校验数据进行数据校验，得到数据校验结果；根据数据校验结果确定是否将待传输数据包传输至数据库。

上述本发明实施例揭示的部分或者全部方法还可以应用于处理器 1601 中，或者由处理器 1601 实现，或者由处理器 1601 与其他元件（例如收发器）配合实现。处理器 1601 可能是一种集成电路芯片，具有信号的处理能力。在实现过程中，上述方法的各步骤可以通过处理器 1601 中的硬件的集成逻辑电路或者软件形式的指令完成。上述的处理器 1601 可以是通用处理器、数字信号处理器(DigitalSignalProcessor，DSP)、专用集成电路(ApplicationSpecific IntegratedCircuit，ASIC)、现成可编程门阵列(FieldProgrammableGateArray，FPGA)或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件。可以实现或者执行本发明实施例中的公开的各方法、步骤及逻辑框图。通用处理器可以是微处理器或者该处理器也可以是任何常规的处理器等。结合本发明实施例所公开的方法的步骤可以直接体现为硬件译码处理器执行完成，或者用译码处理器中的硬件及软件模块组合执行完成。软件模块

可以位于随机存储器，闪存、只读存储器，可编程只读存储器或者电可擦写可编程存储器、寄存器等本领域成熟的存储介质中。该存储介质位于存储器 1602，处理器 1601 读取存储器 1602 中的信息，结合其硬件完成上述方法的步骤。

可以理解的是，本发明实施例描述的这些实施例可以用硬件、软件、固件、中间件、微码或其组合来实现。对于硬件实现，处理单元可以实现在一个或多个专用集成电路(ApplicationSpecificIntegratedCircuits，ASIC)、数字信号处 理器(DigitalSignalProcessing，DSP)、数字信号处理设备(DSPDevice，DSPD)、可编程逻辑设备(ProgrammableLogicDevice，PLD)、现场可编程门阵列(Field-ProgrammableGateArray，FPGA)、通用处理器、控制器、微控制器、微处理器、用于执行本申请功能的其它电子单元或其组合中。

对于软件实现，可通过执行本发明实施例功能的模块(例如过程、函数等)来实现本发明实施例的技术。软件代码可存储在存储器中并通过处理器 1601 执行。存储器可以在处理器 1601 中或在处理器 1601 外部实现。

图 17 是本发明实施例提供的零信任代理节点的结构示意图。图 17 所示的零信任代理节点 1700 包括：至少一个处理器 1701、存储器 1702、至少一个网络接口 1704。零信任代理节点 1700 中的各个组件通过总线系统 1705 耦合在一起。可理解，总线系统 1705 用于实现这些组件之间的连接通信。总线系统 1705 除包括数据总线之外，还包括电源总线、控制总线和状态信号总线。但是为了清楚说明起见，在图 17 中将各种总线都标为总线系统 1705。另外，本发明实施例中，还包括收发器 1706，收发器可以是多个元件，即包括发送器和接收器，提供用于在传输介质上与各种其他装置通信的单元。

可以理解，本发明实施例中的存储器 1702 可以是易失性存储器或非易失性存储器，或可包括易失性和非易失性存储器两者。其中，非易失性存储器可以是只读存储器(Read-OnlyMemory，ROM)、可编程只读存储器 (ProgrammableROM，PROM)、可擦除可编程只读存储器(ErasablePROM，EPROM)、电可擦除可编程只读存储器(ElectricallyEPROM，EEPROM)或闪存。易失性存储器可以是随机存取存储器(RandomAccessMemory，RAM)，其用作外部高速缓存。通过示例性但不是限制性说明，许多形式的 RAM 可用，例如静态随机存取存储器(StaticRAM，SRAM)、动态随机存取存储器 (DynamicRAM，DRAM)、同步动态随机存取存储器(SynchronousDRAM，SDRAM)、双倍数据速率同步动态随机存取存储器(DoubleDataRate SDRAM，DDRSDRAM)、增强型同步动态随机存取存储器(Enhanced SDRAM，ESDRAM)、同步连接动态随机存取存储器(SynchlinkDRAM，SLDRAM)和直接内存总线随机存取存储器(DirectRambusRAM，DRRAM)。本发明实施例描述的系统和方法的存储器 1702 旨在包括但不限于这些和任意其它适合类型的存储器。

在一些实施方式中，存储器 1702 存储了如下的元素，可执行模块或者数据结构，或者他们的子集，或者他们的扩展集：操作系统 1702a。其中，操作系统 1702a，包含各种系统程序，例如框架层、核心库层、驱动层等，用于实现各种基础业务以及处理基于硬件的任务。

在本发明实施例中，通过调用存储器 1702 存储的程序或指令，使得接收器，用于获取用户证书、用户标准会话信息和初始数据包；发送器，用于将用户证书及用户标准会话信息发送至零信任控制器，以使零信任控制器基于用户证书及用户标准会话信息，生成数据校验规则，向零信任网关发送数据校验规则；处理器 1701 和发送器，用于向初始数据包中添加校验数据，生成待传输数据包，并将待传输数据包发送至零信任网关；待传输数据包用于指示零信任网关根据数据校验规则对待传输数据包中的校验数据进行数据校验，得到数据校验结果；根据数据校验结果确定是否将待传输数据包传输至数据库。

上述本发明实施例揭示的部分或者全部方法还可以应用于处理器 1701 中，或者由处理器 1701 实现，或者由处理器 1701 与其他元件（例如收发器）配合实现。处理器 1701 可能是一种集成电路芯片，具有信号的处理能力。在实现过程中，上述方法的各步骤可以通过处理器 1701 中的硬件的集成逻辑电路或者软件形式的指令完成。上述的处理器 1701 可以是通用处理器、数字信号处理器(DigitalSignalProcessor，DSP)、专用集成电路(ApplicationSpecific IntegratedCircuit，ASIC)、现成可编程门阵列(FieldProgrammableGateArray，FPGA)或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件。可以实现或者执行本发明实施例中的公开的各方法、步骤及逻辑框图。通用处理器可以是微处理器或者该处理器也可以是任何常规的处理器等。结合本发明实施例所公开的方法的步骤可以直接体现为硬件译码处理器执行完成，或者用译码处理器中的硬件及软件模块组合执行完成。软件模块可以位于随机存储器，闪存、只读存储器，可编程只读存储器或者电可擦写可编程存储器、寄存器等本领域成熟的存储介质中。该存储介质位于存储器 1702，处理器 1701 读取存储器 1702 中的信息，结合其硬件完成上述方法的步骤。

可以理解的是，本发明实施例描述的这些实施例可以用硬件、软件、固件、中间件、微码或其组合来实现。对于硬件实现，处理单元可以实现在一个或多个专用集成电路

(ApplicationSpecificIntegratedCircuits，ASIC)、数字信号处 理器(DigitalSignalProcessing，DSP)、数字信号处理设备(DSPDevice，DSPD)、可编程逻辑设备(ProgrammableLogicDevice，PLD)、现场可编程门阵列(Field-ProgrammableGateArray，FPGA)、通用处理器、控制器、微控制器、微处理器、用于执行本申请功能的其它电子单元或其组合中。

对于软件实现，可通过执行本发明实施例功能的模块(例如过程、函数等)来实现本发明实施例的技术。软件代码可存储在存储器中并通过处理器 1701 执行。存储器可以在处理器 1701 中或在处理器 1701 外部实现。

在一个实施例中，提供了一种计算机可读存储介质，其上存储有计算机程序，该计算机程序被处理器执行时实现上述各方法实施例中的步骤。

在一个实施例中，提供了一种计算机程序产品，包括计算机程序，该计算机程序被处理器执行时实现上述各方法实施例中的步骤。

需要说明的是，本申请所涉及的用户信息（包括但不限于用户设备信息、用户个人信息等）和数据（包括但不限于用于分析的数据、存储的数据、展示的数据等），均为经用户授权或者经过各方充分授权的信息和数据，且相关数据的收集、使用和处理需要遵守相关国家和地区的相关法律法规和标准。

本领域普通技术人员可以理解实现上述实施例方法中的全部或部分流程，是可以通过计算机程序来指令相关的硬件来完成的，计算机程序可存储于一非易失性计算机可读取存储介质中，该计算机程序在执行时，可包括如上述各方法的实施例的流程。其中，本申请所提供的各实施例中所使用的对存储器、数据库或其它介质的任何引用，均可包括非易失性和易失性存储器中的至少一种。非易失性存储器可包括只读存储器（Read-Only Memory，ROM）、磁带、软盘、闪存、光存储器、高密度嵌入式非易失性存储器、阻变存储器（ReRAM）、磁变存储器（Magnetoresistive Random Access Memory，MRAM）、铁电存储器（Ferroelectric Random Access Memory，FRAM）、相变存储器（Phase Change Memory，PCM）、石墨烯存储器等。易失性存储器可包括随机存取存储器（Random Access Memory，RAM）或外部高速缓冲存储器等。作为说明而非局限，RAM 可以是多种形式，比如静态随机存取存储器（Static Random Access Memory，SRAM）或动态随机存取存储器（Dynamic Random Access Memory，DRAM）等。本申请所提供的各实施例中所涉及的数据库可包括关系型数据库和非关系型数据库中至少一种。非关系型数据库可包括基于区块链的分布式数据库等，不限于此。本申请所提供的各实施例中所涉及的处理器可为通用处理器、中央处理器、图形处理器、数字信号处理器、可编程逻辑器、基于量子计算的数据处理逻辑器等，不限于此。

上述数据传输方法、装置、计算机设备、存储介质和程序产品，接收零信任控制器发送的数据校验规则和零信任代理节点发送的待传输数据包；待传输数据包为零信任代理节点在初始数据包中添加校验数据后得到的；根据数据校验规则对待传输数据包中的校验数据进行数据校验，得到数据校验结果；根据数据校验结果确定是否将待传输数据包传输至数据库。本申请实施例中的零信任代理节点能够在初始数据包中添加校验数据，得到重新封装的待传输数据包。从而，零信任网关能够接收零信任控制器发送的数据校验规则以及零信任代理节点发送的、重新封装的待传输数据包，并根据数据校验规则对重新封装的待传输数据包中的校验数据进行数据校验，得到较准确的数据校验结果。进而，能够根据较准确的数据校验结果，确定是否将待传输数据包传输至数据库。由于本申请需要先根据数据校验规则对重新封装的待传输数据包中的校验数据进行数据校验，且本申请只能对数据校验通过的待传输数据包进行传输，因此，能够提高数据传输过程的安全性。

以上实施例的各技术特征可以进行任意的组合，为使描述简洁，未对上述实施例中的各个技术特征所有可能的组合都进行描述，然而，只要这些技术特征的组合不存在矛盾，都应当认为是本说明书记载的范围。

以上实施例仅表达了本申请的几种实施方式，其描述较为具体和详细，但并不能因此而理解为对本申请专利范围的限制。应当指出的是，对于本领域的普通技术人员来说，在不脱离本申请构思的前提下，还可以做出若干变形和改进，这些都属于本申请的保护范围。因此，本申请的保护范围应以所附权利要求为准。

权利要求

1、一种数据传输方法，应用于零信任通信网络中的零信任网关中，所述方法包括：

接收零信任控制器发送的数据校验规则和零信任代理节点发送的待传输数据包；所述待传输数据包为所述零信任代理节点在初始数据包中添加校验数据后得到的；

根据所述数据校验规则对所述待传输数据包中的校验数据进行数据校验，得到数据校验结果；以及

根据所述数据校验结果确定是否将所述待传输数据包传输至数据库。

2、根据权利要求 1 所述的方法，其中，所述校验数据包括用户会话信息和用户签名信息，所述用户会话信息用于指示与所述零信任代理节点建立会话连接过程中生成的地址信息和会话计数信息，所述用户签名信息用于指示发送所述初始数据包的用户的身份参数，所述数据校验规则包括用户会话信息校验规则及数据签名校验规则；所述根据所述数据校验规则对所述待传输数据包中的校验数据进行数据校验，得到数据校验结果，包括：

根据所述用户会话信息校验规则对所述待传输数据包中的用户会话信息进行数据校验，生成第一数据校验结果；

根据所述数据签名校验规则对所述待传输数据包中的用户签名信息进行数据校验，生成第二数据校验结果；以及

根据所述第一数据校验结果及所述第二数据校验结果，生成所述数据校验结果。

3、根据权利要求 2 所述的方法，其中，所述根据所述用户会话信息校验规则对所述待传输数据包中的用户会话信息进行数据校验，生成第一数据校验结果，包括：

根据所述地址信息确定所述待传输数据包的网络地址类型；所述网络地址类型包括公网地址类型及私网地址类型；

根据所述待传输数据包的网络地址类型，确定是否需要对所述待传输数据包中的源网络地址进行更新，生成中间数据包；以及

根据所述用户会话信息校验规则对所述中间数据包中的会话计数信息进行数据校验，生成所述第一数据校验结果。

4、根据权利要求 3 所述的方法，其中，所述根据所述待传输数据包的网络地址类型，确定是否需要对所述待传输数据包中的源网络地址进行更新，生成中间数据包，包括：

若所述待传输数据包的网络地址类型为所述私网地址类型，则将所述待传输数据包作为所述中间数据包；以及

若所述待传输数据包的网络地址类型为所述公网地址类型，则将所述待传输数据包中的源网络地址更新为所述待传输数据包对应的公网地址，生成所述中间数据包。

5、根据权利要求 3 或 4 所述的方法，其中，所述根据所述数据签名校验规则对所述待传输数据包中的用户签名信息进行数据校验，生成第二数据校验结果，包括：

根据所述数据签名校验规则对所述中间数据包中的用户签名信息进行数据校验，生成所述第二数据校验结果。

6、根据权利要求 1-5 任一项所述的方法，其中，所述方法还包括：

从所述待传输数据包中确定校验未通过的数据包，根据所述校验未通过的数据包生成异常会话信息；

将所述异常会话信息发送至所述零信任控制器；所述异常会话信息用于指示所述零信任控制器对所述异常会话信息进行分析及向所述零信任代理节点发送会话终止指令。

7、根据权利要求 1-5 任一项所述的方法，其中，所述数据校验规则是根据用户标准签名信息和用户标准会话信息生成的，其中，所述用户标准签名信息包括用户公钥信息以及用户身份标准信息。

8、根据权利要求 7 所述的方法，其中，所述用户标准签名信息是在用户证书验证通过的情况下，从所述用户证书中获取的。

9、一种数据传输方法，应用于零信任通信网络中的零信任控制器中，所述方法包括：

接收零信任代理节点发送的用户证书和用户标准会话信息；

根据所述用户证书和用户标准会话信息，生成数据校验规则；以及

向零信任网关发送所述数据校验规则；所述数据校验规则用于指示所述零信任网关根据所述数据校验规则对待传输数据包中的校验数据进行数据校验，得到数据校验结果，并根据所述数据校验结果确定是否将所述待传输数据包传输至数据库。

10、根据权利要求 9 所述的方法，其中，所述根据所述用户证书和所述用户标准会话信息，生成所述数据校验规则，包括：

对所述用户证书进行验证，生成证书验证结果；

在证书验证结果为证书验证通过的情况下，从所述用户证书中获取用户标准签名信息，其中，所述用户标准签名信息包括用户公钥信息以及用户标准身份信息；以及

根据所述用户标准签名信息和所述用户标准会话信息，生成所述数据校验规则。

11、一种数据传输方法，应用于零信任通信网络中的零信任代理节点中，所述方法包括：

获取用户证书、用户标准会话信息和初始数据包；

将所述用户证书及所述用户标准会话信息发送至零信任控制器，以使所述零信任控制器基于所述用户证书及所述用户标准会话信息，生成数据校验规则，向零信任网关发送所述数据校验规则；以及

向所述初始数据包中添加校验数据，生成待传输数据包，并将所述待传输数据包发送至所述零信任网关；所述待传输数据包用于指示所述零信任网关根据所述数据校验规则对所述待传输数据包中的校验数据进行数据校验，得到数据校验结果，并根据所述数据校验结果确定是否将所述待传输数据包传输至数据库。

12、根据权利要求 11 所述的数据传输方法，其中，所述用户证书在验证通过的情况下，使得所述零信任控制器从所述用户证书中获取用户标准签名信息并基于所述标准签名信息和所述用户标准会话信息生成数据校验规则，其中，所述用户标准签名信息包括用户公钥信息以及用户身份标准信息。

13、一种数据传输装置，应用于零信任通信网络中的零信任网关中，所述装置包括：

待传输数据包接收模块，用于接收零信任控制器发送的数据校验规则和零信任代理节点发送的待传输数据包；所述待传输数据包为所述零信任代理节点在初始数据包中添加校验数据后得到的；

数据校验模块，用于根据所述数据校验规则对所述待传输数据包中的校验数据进行数据校验，得到数据校验结果；

数据传输模块，用于根据所述数据校验结果确定是否将所述待传输数据包传输至数据库。

14、一种数据传输装置，应用于零信任通信网络中的零信任控制器中，所述装置包括：

信息接收模块，用于接收零信任代理节点发送的用户证书和用户标准会话信息；

数据校验规则生成模块，用于根据所述用户证书和用户标准会话信息，生成数据校验规则；

数据校验规则发送模块，用于向零信任网关发送所述数据校验规则；所述数据校验规则用于指示所述零信任网关根据所述数据校验规则对待传输数据包中的校验数据进行数据校验，得到数据校验结果；根据所述数据校验结果确定是否将所述待传输数据包传输至数据库。

15、一种数据传输装置，应用于零信任通信网络中的零信任代理节点中，所述装置包括：

信息获取模块，用于获取用户证书、用户标准会话信息和初始数据包；

信息发送数据校验模块，用于将所述用户证书及所述用户标准会话信息发送至零信任控制器，以使所述零信任控制器基于所述用户证书及所述用户标准会话信息，生成数据校验规则，向零信任网关发送所述数据校验规则；

待传输数据包生成模块，用于向所述初始数据包中添加校验数据，生成待传输数据包，并将所述待传输数据包发送至所述零信任网关；所述待传输数据包用于指示所述零信任网关根据所述数据校验规则对所述待传输数据包中的校验数据进行数据校验，得到数据校验结果；根据所述数据校验结果确定是否将所述待传输数据包传输至数据库。

16、一种零信任网关，包括收发器、处理器和存储器，所述存储器存储有计算机程序，所述处理器执行所述计算机程序，用于执行如权利要求 1 至 8 中任一项所述的方法的步骤。

17、一种零信任控制器，包括收发器、处理器和存储器，所述存储器存储有计算机程序，所述处理器执行所述计算机程序，用于控制所述收发器接收零信任代理节点发送的用户证书和用户标准会话信息；

用于控制所述处理器根据所述用户证书和用户标准会话信息，生成数据校验规则；

用于控制所述收发器向零信任网关发送所述数据校验规则；所述数据校验规则用于指示所述零信任网关根据所述数据校验规则对待传输数据包中的校验数据进行数据校验，得到数据校验结果；根据所述数据校验结果确定是否将所述待传输数据包传输至数据库。

18、一种零信任代理节点，包括收发器、处理器和存储器，所述存储器存储有计算机程序，所述处理器执行所述计算机程序，用于控制所述收发器获取用户证书、用户标准会话信息和初始数据包；

用于控制所述收发器将所述用户证书及所述用户标准会话信息发送至零信任控制器，以使所述零信任控制器基于所述用户证书及所述用户标准会话信息，生成数据校验规则，向零信任网关发送所述数据校验规则；

用于控制所述处理器和所述收发器向所述初始数据包中添加校验数据，生成待传输数据包，并将所述待传输数据包发送至所述零信任网关；所述待传输数据包用于指示所述零信任网关根据所述数据校

验规则对所述待传输数据包中的校验数据进行数据校验，得到数据校验结果；根据所述数据校验结果确定是否将所述待传输数据包传输至数据库。

19、一种计算机可读存储介质，其上存储有计算机程序，所述计算机程序被处理器执行时实现权利要求 1 至 12 中任一项所述的方法的步骤。

20、一种计算机程序产品，包括计算机程序，该计算机程序被处理器执行时实现权利要求 1 至 12 中任一项所述的方法的步骤。

21、一种装置，被配置为执行权利要求 1 至 12 任一项的方法。

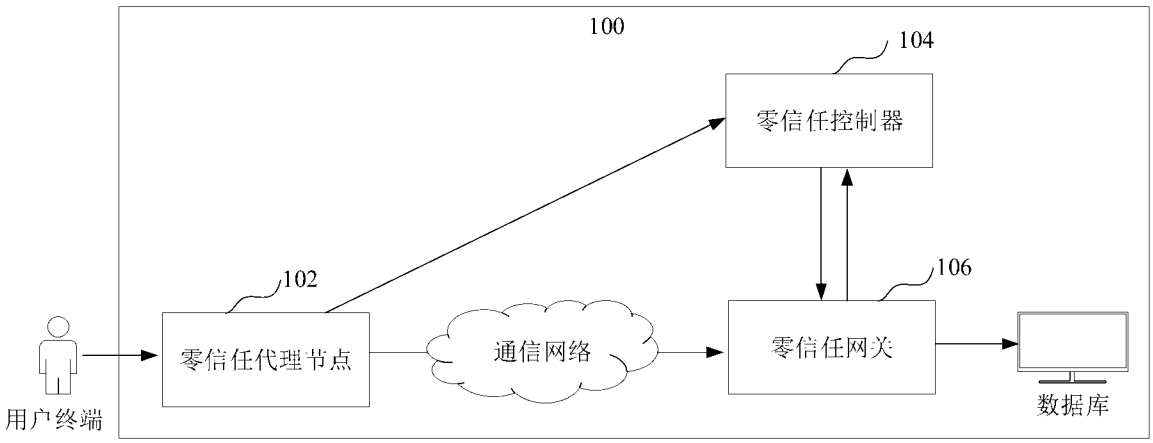
100
104
零信任控制器
102
106
零信任代理节点
通信网络
零信任网关
用户终端
数据库

图 1

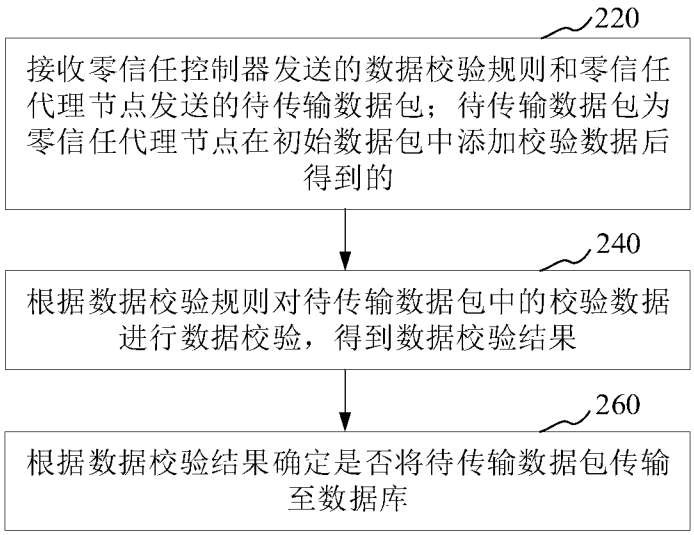
220
接收零信任控制器发送的数据校验规则和零信任代理节点发送的待传输数据包；待传输数据包为零信任代理节点在初始数据包中添加校验数据后得到的
240
根据数据校验规则对待传输数据包中的校验数据进行数据校验，得到数据校验结果
260
根据数据校验结果确定是否将待传输数据包传输至数据库

图 2

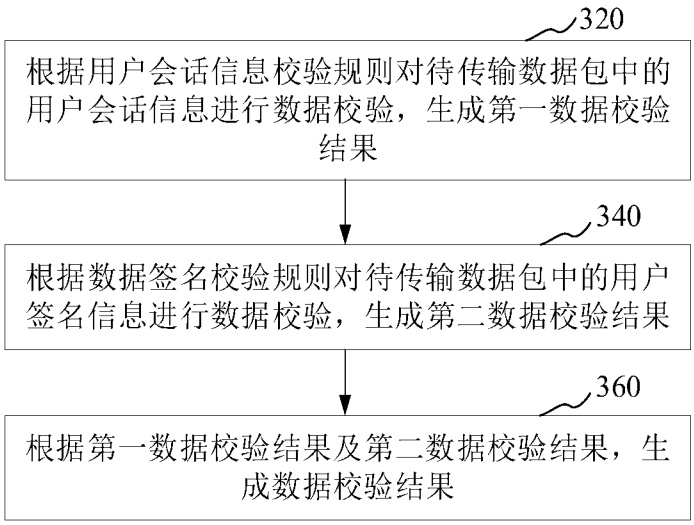
320
根据用户会话信息校验规则对待传输数据包中的用户会话信息进行数据校验，生成第一数据校验结果
340
根据数据签名校验规则对待传输数据包中的用户签名信息进行数据校验，生成第二数据校验结果
360
根据第一数据校验结果及第二数据校验结果，生成数据校验结果

图 3

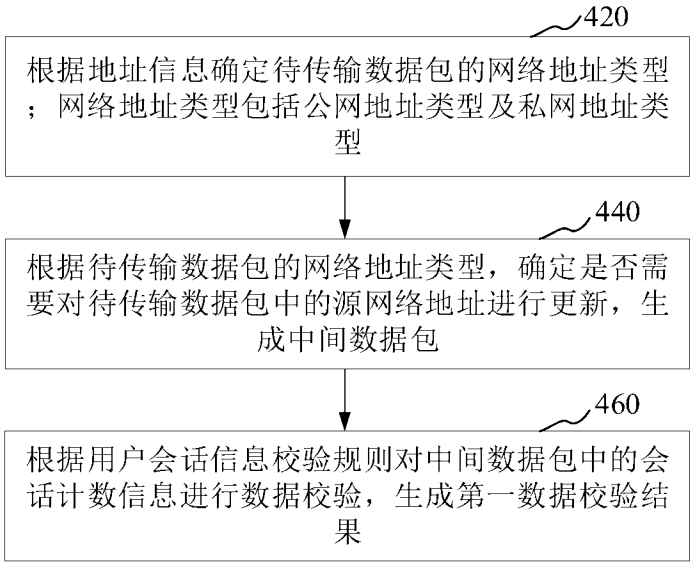
420
根据地址信息确定待传输数据包的网络地址类型；网络地址类型包括公网地址类型及私网地址类型
440
根据待传输数据包的网络地址类型，确定是否需要对待传输数据包中的源网络地址进行更新，生成中间数据包
460
根据用户会话信息校验规则对中间数据包中的会话计数信息进行数据校验，生成第一数据校验结果

图 4

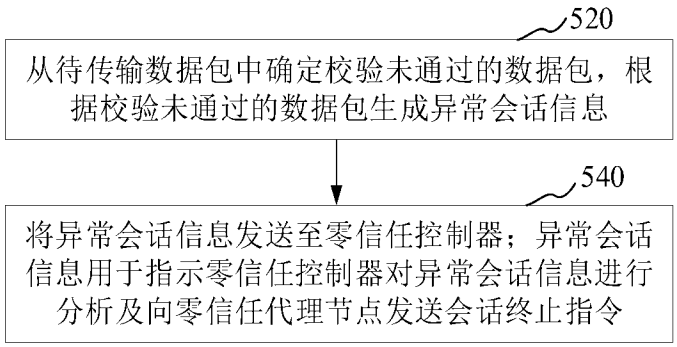
520
从待传输数据包中确定校验未通过的数据包，根据校验未通过的数据包生成异常会话信息
540
将异常会话信息发送至零信任控制器；异常会话信息用于指示零信任控制器对异常会话信息进行分析及向零信任代理节点发送会话终止指令

图 5

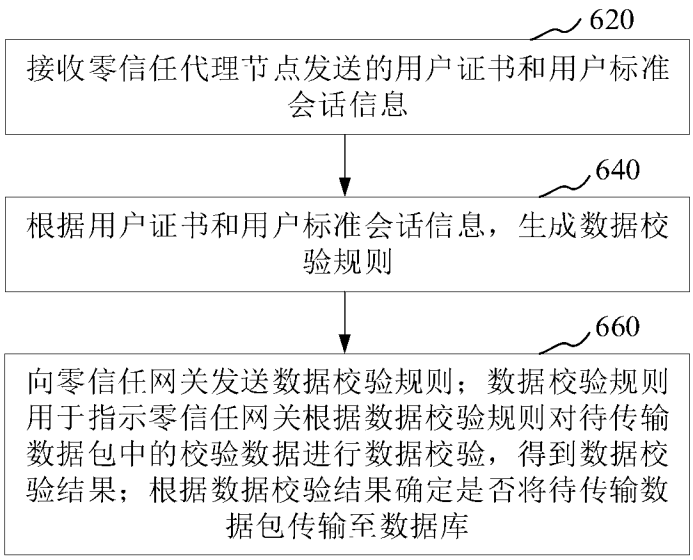
620
接收零信任代理节点发送的用户证书和用户标准会话信息
640
根据用户证书和用户标准会话信息，生成数据校验规则
660
向零信任网关发送数据校验规则；数据校验规则用于指示零信任网关根据数据校验规则对待传输数据包中的校验数据进行数据校验，得到数据校验结果；根据数据校验结果确定是否将待传输数据包传输至数据库

图 6

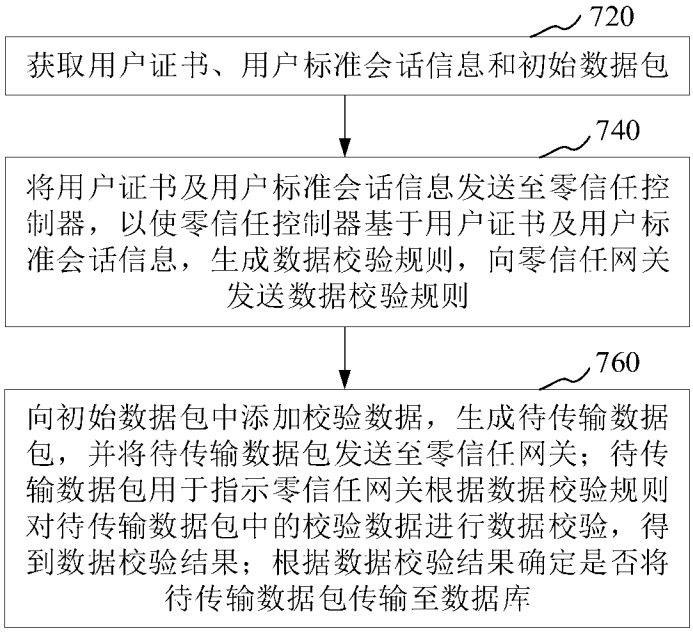

图 7

版本	头部长度	服务类型	总长度	
标识符			标志	偏移量
生存时间		协议	校验位	
源网络地址				
目的网络地址				
选项				
数据				
会话计数器字段	数据签名信息字段			

图 8

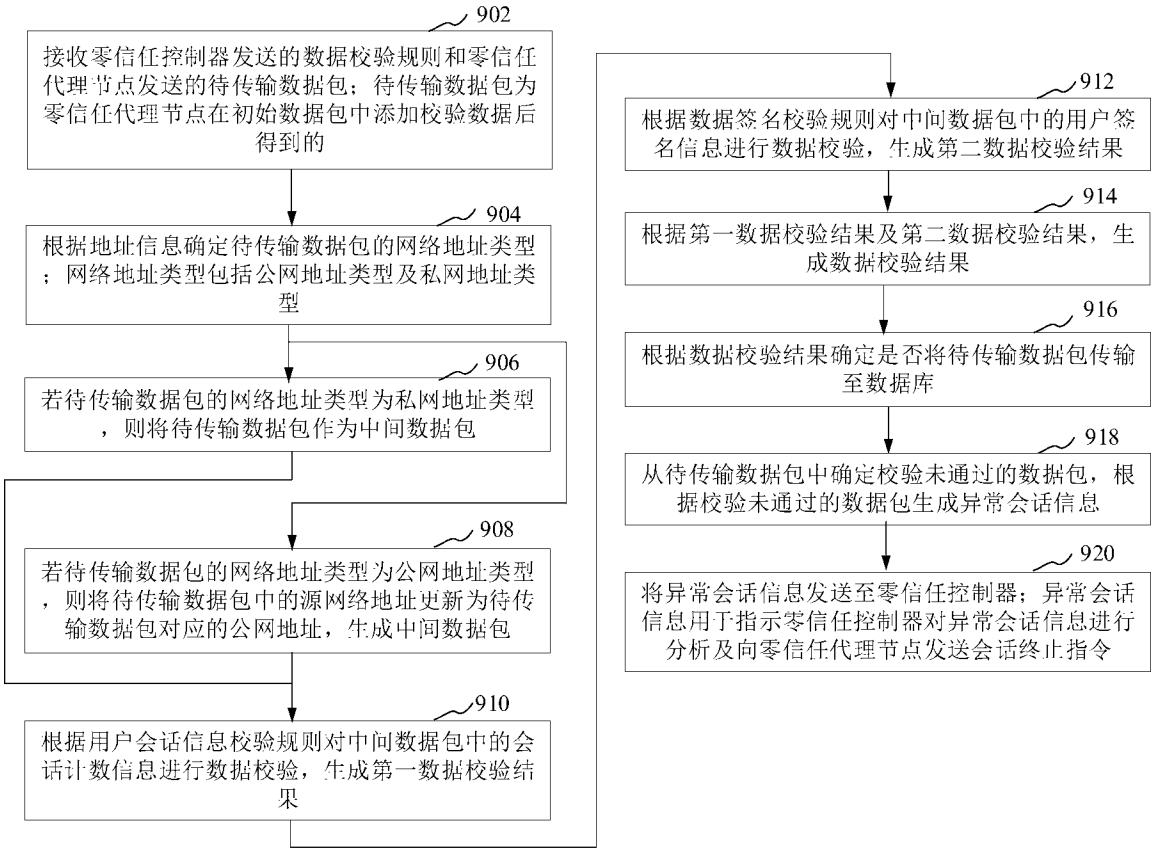
902
接收零信任控制器发送的数据校验规则和零信任代理节点发送的待传输数据包；待传输数据包为零信任代理节点在初始数据包中添加校验数据后得到的
904
根据地址信息确定待传输数据包的网络地址类型；网络地址类型包括公网地址类型及私网地址类型
906
若待传输数据包的网络地址类型为私网地址类型，则将待传输数据包作为中间数据包
908
若待传输数据包的网络地址类型为公网地址类型，则将待传输数据包中的源网络地址更新为待传输数据包对应的公网地址，生成中间数据包
910
根据用户会话信息校验规则对中间数据包中的会话计数信息进行数据校验，生成第一数据校验结果
912
根据数据签名校验规则对中间数据包中的用户签名信息进行数据校验，生成第二数据校验结果
914
根据第一数据校验结果及第二数据校验结果，生成数据校验结果
916
根据数据校验结果确定是否将待传输数据包传输至数据库
918
从待传输数据包中确定校验未通过的数据包，根据校验未通过的数据包生成异常会话信息
920
将异常会话信息发送至零信任控制器；异常会话信息用于指示零信任控制器对异常会话信息进行分析及向零信任代理节点发送会话终止指令

图 9

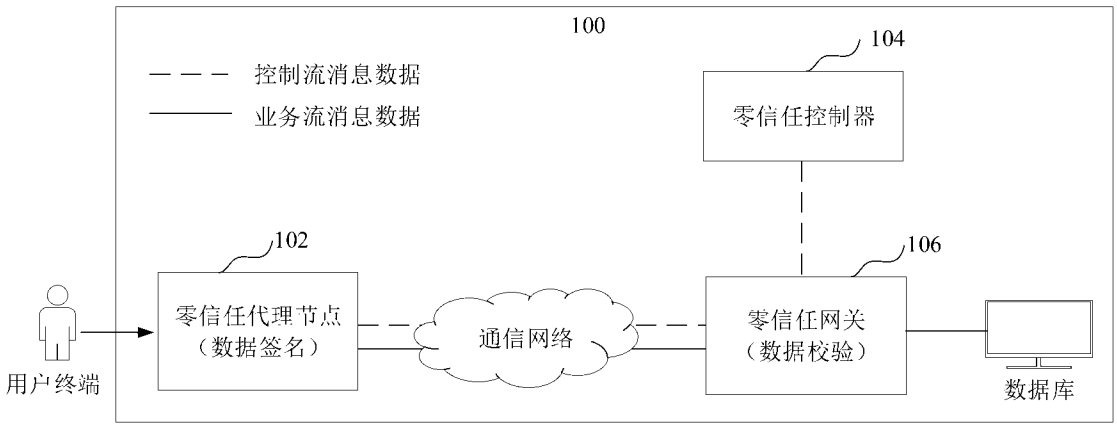
100
控制流消息数据
业务流消息数据
104
零信任控制器
102
零信任代理节点
（数据签名）
通信网络
106
零信任网关
（数据校验）
用户终端
数据库

图 10

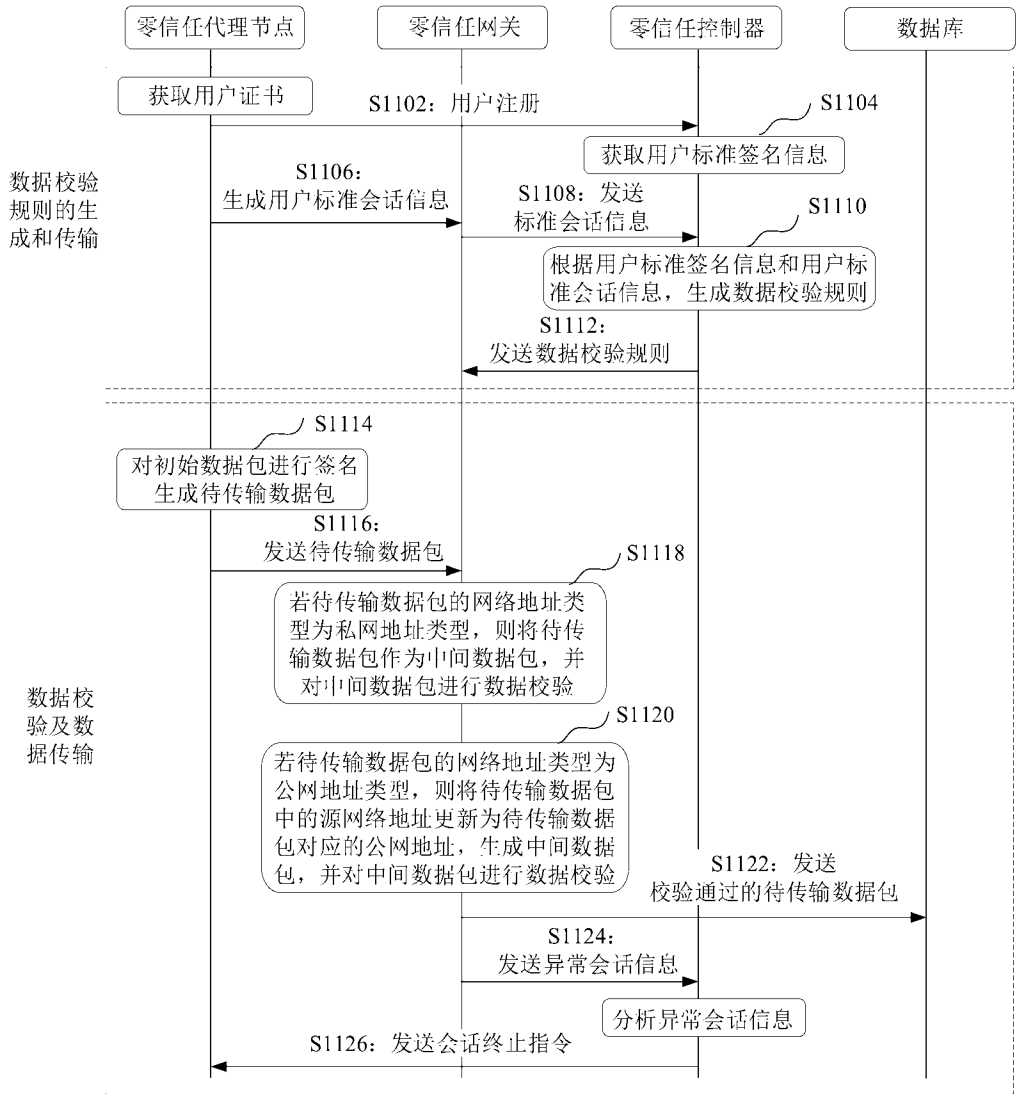
零信任代理节点
零信任网关
零信任控制器
数据库
获取用户证书
S1102：用户注册
S1104
获取用户标准签名信息
数据校验规则的生成和传输
S1106：生成用户标准会话信息
S1108：发送标准会话信息
S1110
根据用户标准签名信息和用户标准会话信息，生成数据校验规则
S1112：发送数据校验规则
S1114
对初始数据包进行签名生成待传输数据包
S1116：发送待传输数据包
S1118
若待传输数据包的网络地址类型为私网地址类型，则将待传输数据包作为中间数据包，并对中间数据包进行数据校验
数据校验及数据传输
S1120
若待传输数据包的网络地址类型为公网地址类型，则将待传输数据包中的源网络地址更新为待传输数据包对应的公网地址，生成中间数据包，并对中间数据包进行数据校验
S1122：发送校验通过的待传输数据包
S1124：发送异常会话信息
分析异常会话信息
S1126：发送会话终止指令

图 11

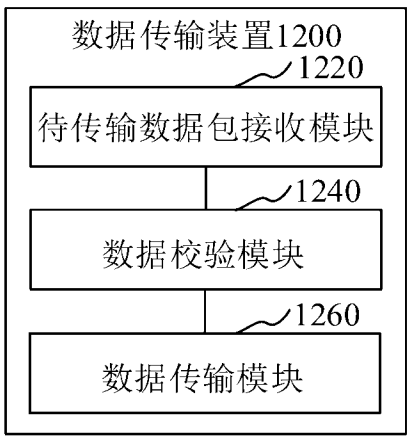
数据传输装置1200
1220
待传输数据包接收模块
1240
数据校验模块
1260
数据传输模块

图 12

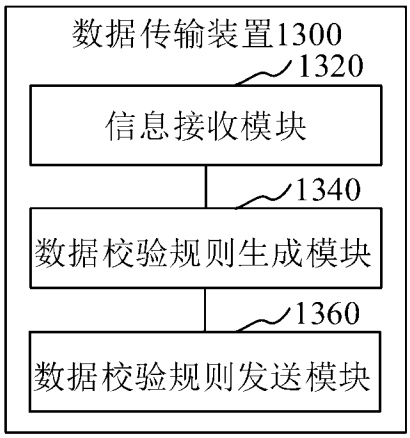
数据传输装置1300
1320
信息接收模块
1340
数据校验规则生成模块
1360
数据校验规则发送模块

图 13

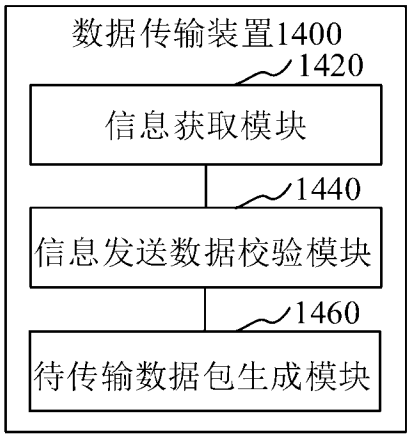
数据传输装置1400
1420
信息获取模块
1440
信息发送数据校验模块
1460
待传输数据包生成模块

图 14

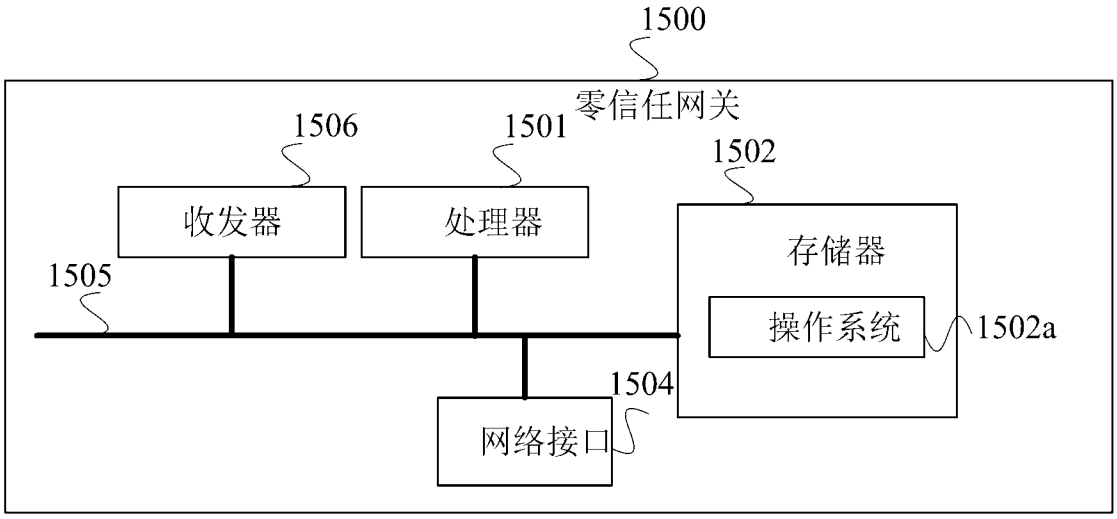
1500
零信任网关
1506
1501
1502
收发器
处理器
存储器
1505
操作系统
1502a
1504
网络接口

图 15

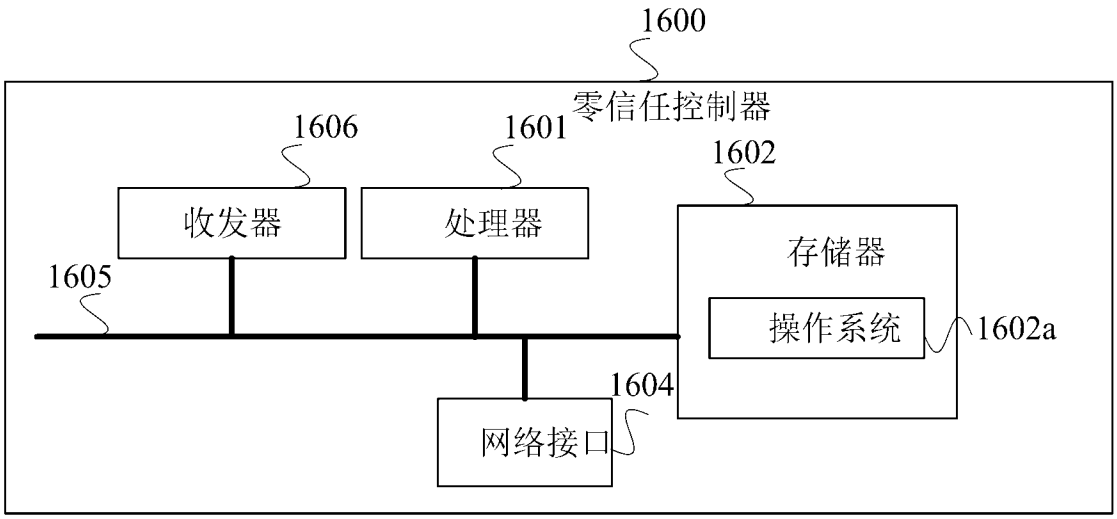
1600
零信任控制器
1606
1601
1602
收发器
处理器
存储器
1605
操作系统
1602a
1604
网络接口

图 16

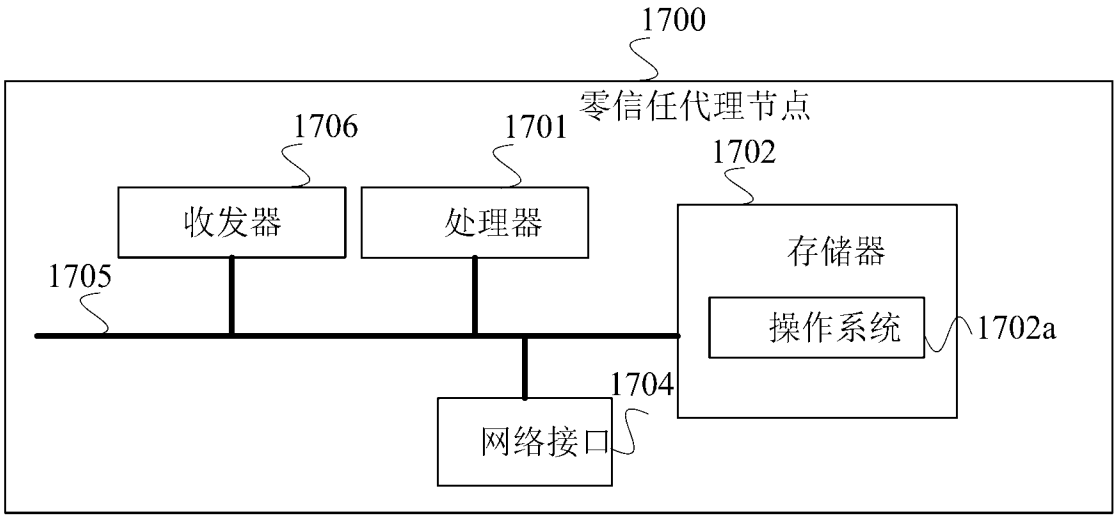
1700
零信任代理节点
1706
1701
1702
收发器
处理器
存储器
1705
操作系统
1702a
1704
网络接口

图 17

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2023/140207

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/40(2022.01)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)

CNTXT; CNKI; WPABS; ENTXT: 零信任, 校验, 验证, 认证, 规则, 策略, 证书, 身份, 签名, 会话, 网关, 代理, zero trust, verify, authenticate, rule, policy, certificate, identity, signature, session, gateway, agent

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 116633698 A (CHINA TELECOM CORP., LTD.) 22 August 2023 (2023-08-22) claims 1-16, and description, paragraph 68	1-21
X	CN 114553568 A (CHONGQING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS) 27 May 2022 (2022-05-27) description, paragraphs [0032]-[0051], and figure 2	1-21
X	CN 113051602 A (SOUTHEAST UNIVERSITY et al.) 29 June 2021 (2021-06-29) description, paragraphs [0058]-[0066]	1-21
A	CN 114679293 A (TENCENT CLOUD COMPUTING (BEIJING) CO., LTD.) 28 June 2022 (2022-06-28) entire document	1-21
A	CN 113992402 A (BEIJING FANGJIANGHU TECHNOLOGY CO., LTD.) 28 January 2022 (2022-01-28) entire document	1-21
A	KR 102333553 B1 (PRIBIT TECHNOLOGY INC.) 01 December 2021 (2021-12-01) entire document	1-21

☐ 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
"D" document cited by the applicant in the international application
"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
21 March 2024	**29 March 2024**

Name and mailing address of the ISA/CN	Authorized officer
China National Intellectual Property Administration (ISA/CN) **China No. 6, Xitucheng Road, Jimenqiao, Haidian District, Beijing 100088**	Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2023/140207

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 116633698 A	22 August 2023	None	
CN 114553568 A	27 May 2022	None	
CN 113051602 A	29 June 2021	None	
CN 114679293 A	28 June 2022	None	
CN 113992402 A	28 January 2022	None	
KR 102333553 B1	01 December 2021	None	

国际检索报告

国际申请号
PCT/CN2023/140207

A. 主题的分类

H04L 9/40(2022.01)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）)

CNTXT;CNKI;WPABS;ENTXT：零信任，校验，验证，认证，规则，策略，证书，身份，签名，会话，网关，代理，zero trust, verify, authenticate, rule, policy, certificate, identity, signature, session, gateway, agent

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 116633698 A (中国电信股份有限公司) 2023年8月22日 (2023 - 08 - 22) 权利要求1-16，说明书第68段	1-21
X	CN 114553568 A (重庆邮电大学) 2022年5月27日 (2022 - 05 - 27) 说明书第[0032]-[0051]段，附图2	1-21
X	CN 113051602 A (东南大学等) 2021年6月29日 (2021 - 06 - 29) 说明书第[0058]-[0066]段	1-21
A	CN 114679293 A (腾讯云计算（北京）有限责任公司) 2022年6月28日 (2022 - 06 - 28) 全文	1-21
A	CN 113992402 A (北京房江湖科技有限公司) 2022年1月28日 (2022 - 01 - 28) 全文	1-21
A	KR 102333553 B1 (PRIBIT TECH INC) 2021年12月1日 (2021 - 12 - 01) 全文	1-21

☐ 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

“D” 申请人在国际申请中引证的文件

“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
2024年3月21日	2024年3月29日
ISA/CN的名称和邮寄地址 中国国家知识产权局 中国北京市海淀区蓟门桥西土城路6号 100088	受权官员 曹玉华 电话号码 (+86) 010-62412272

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2023/140207

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 116633698 A	2023年8月22日	无	
CN 114553568 A	2022年5月27日	无	
CN 113051602 A	2021年6月29日	无	
CN 114679293 A	2022年6月28日	无	
CN 113992402 A	2022年1月28日	无	
KR 102333553 B1	2021年12月1日	无	