

(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
2022 年 5 月 12 日 (12.05.2022)



(10) 国际公布号
WO 2022/095367 A1

(51) 国际专利分类号:
H04L 29/06 (2006.01) **H04L 12/24** (2006.01)

(21) 国际申请号: PCT/CN2021/090762

(22) 国际申请日: 2021 年 4 月 28 日 (28.04.2021)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
202011232429.5 2020 年 11 月 6 日 (06.11.2020) 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 518057 (CN)。

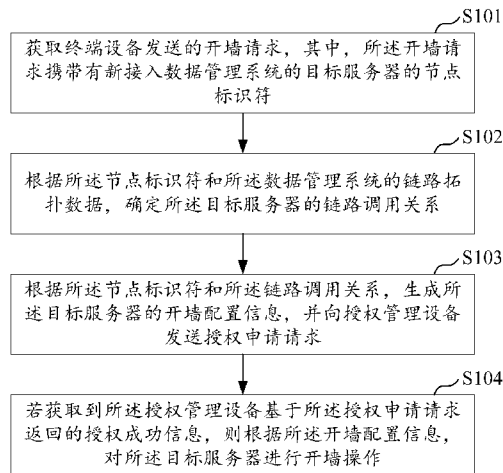
(72) 发明人: 曹晗 (CAO, Han); 中国广东省深圳市福田区福田街道福安社区益田路 5033 号平安金融中心 23 楼, Guangdong 518057 (CN)。

(74) 代理人: 深圳市力道知识产权代理事务所 (普通合伙) (SHENZHEN LIDAO INTELLECTUAL PROPERTY AGENCY (GENERAL PARTNERSHIP)); 中国广东省深圳市福田区园岭街道八卦一路 50 号鹏基商务时空大厦 1718, Guangdong 518000 (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, IT, 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,

(54) Title: FIREWALL OPENING PROCESSING METHOD AND APPARATUS, SERVER, SYSTEM AND READABLE STORAGE MEDIUM

(54) 发明名称: 开墙处理方法、装置、服务器、系统及可读存储介质



S101 Acquire a firewall opening request sent by a terminal device, wherein the firewall opening request carries a node identifier of a target server newly accessing a data management system

S102 According to the node identifier and link topology data of the data management system, determine a link calling relationship of the target server

S103 Generate, according to the node identifier and the link calling relationship, firewall opening configuration information of the target server, and send an authorization application request to an authorization management device

S104 If authorization success information returned by the authorization management device on the basis of the authorization application request is acquired, perform a firewall opening operation on the target server according to the firewall opening configuration information

图 2

(57) Abstract: The present application provides a firewall opening processing method and apparatus, a server, a system and a readable storage medium. Said method comprises: acquiring a firewall opening request sent by a terminal device, wherein the firewall opening request carries a node identifier of a target server newly accessing a data management system; according to the node identifier and link topology data of the data management system, determining a link calling relationship of the target server; generating, according to the node identifier and the link calling relationship, firewall opening configuration information of the target server, and sending an authorization application request to an authorization management device; and if authorization success information returned by the authorization management device on the basis of the authorization application request is acquired, performing a firewall opening operation on the target server according to the firewall opening configuration information. The present application increases the firewall-opening efficiency and accuracy. The present application also relates to the field of blockchains, and the described readable storage medium can store data created according to the use of blockchain nodes.

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, 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: 本申请提供一种开墙处理方法、装置、服务器、系统及可读存储介质, 该方法包括: 获取终端设备发送的开墙请求, 其中, 所述开墙请求携带有新接入数据管理系统的目标服务器的节点标识符; 根据所述节点标识符和所述数据管理系统的链路拓扑数据, 确定所述目标服务器的链路调用关系; 根据所述节点标识符和所述链路调用关系, 生成所述目标服务器的开墙配置信息, 并向授权管理设备发送授权申请请求; 若获取到所述授权管理设备基于所述授权申请请求返回的授权成功信息, 则根据所述开墙配置信息, 对所述目标服务器进行开墙操作。本申请提高了开墙效率和准确性。本申请还涉及区块链领域, 上述可读存储介质可存储根据区块链节点的使用所创建的数据。

开墙处理方法、装置、服务器、系统及可读存储介质

本申请要求于2020年11月6日提交中国专利局、申请号为2020112324295、发明名称为“开墙处理方法、装置、服务器、系统及可读存储介质”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

本申请涉及安全防护技术领域，尤其涉及一种开墙处理方法、装置、服务器、系统及可读存储介质。

背景技术

目前，越来越多的企业都使用服务器建立数据管理系统，方便企业管理数据，对于金融保险企业，数据管理系统所需的服务器和应用较多，同时由于金融保险数据的敏感性，对数据管理系统的安全性要求较高，对此按照需求需要在各服务器之间设置防火墙。对于新接入数据管理系统的服务器，需要对新接入的服务器进行开墙操作，即配置新接入的服务器的防火墙以及配置与新接入的服务器相关联的服务器的防火墙，由于数据管理系统涉及到的服务器较多，用户无法准确和快速地对新接入的服务器进行开墙操作，开墙效率较低。

发明内容

本申请实施例提供一种开墙处理方法、装置、服务器、系统及可读存储介质，旨在提高服务器的开墙效率和准确性。

第一方面，本申请实施例提供一种开墙处理方法，包括：

获取终端设备发送的开墙请求，其中，所述开墙请求携带有新接入数据管理系统的目标服务器的节点标识符；

根据所述节点标识符和所述数据管理系统的链路拓扑数据，确定所述目标服务器的链路调用关系；

根据所述节点标识符和所述链路调用关系，生成所述目标服务器的开墙配置信息，并向授权管理设备发送授权申请请求；

若获取到所述授权管理设备基于所述授权申请请求返回的授权成功信息，则根据所述开墙配置信息，对所述目标服务器进行开墙操作。

第二方面，本申请实施例还提供一种开墙处理装置，所述开墙处理装置包括：

获取模块，用于获取终端设备发送的开墙请求，其中，所述开墙请求携带有新接入数据管理系统的目标服务器的节点标识符；

确定模块，用于根据所述节点标识符和所述数据管理系统的链路拓扑数据，确定所述目标服务器的链路调用关系；

生成模块，用于根据所述节点标识符和所述链路调用关系，生成所述目标服务器的开墙配置信息；

发送模块，用于向授权管理设备发送授权申请请求；

开墙模块，用于若获取到所述授权管理设备基于所述授权申请请求返回的授权成功信息，则根据所述开墙配置信息对所述目标服务器进行开墙操作。

第三方面，本申请实施例还提供一种开墙处理系统，所述开墙处理系统包括终端设备、

开墙服务器和授权管理设备,所述终端设备与所述开墙服务器通信连接,所述开墙服务器与所述授权管理设备通信连接,其中:

所述终端设备,用于向开墙服务器发送开墙请求,其中,所述开墙请求携带有新接入数据管理系统的目标服务器的节点标识符;

5 所述开墙服务器,用于获取所述终端设备发送的开墙请求,并根据所述开墙请求中的节点标识符和所述数据管理系统的链路拓扑数据,确定所述目标服务器的链路调用关系;

所述开墙服务器还用于根据所述节点标识符和所述链路调用关系,生成所述目标服务器的开墙配置信息,并向授权管理设备发送授权申请请求;

10 所述授权管理设备用于根据所述授权申请请求,输出授权提示信息,以提示授权人员需要进行开墙授权;

所述授权管理设备还用于在检测到所述授权人员触发的授权确认指令时,根据所述授权确认指令向所述开墙服务器发送授权成功信息;

所述开墙服务器还用于在接收到所述授权管理设备发送的授权成功信息时,根据所述开墙配置信息,对所述目标服务器进行开墙操作。

15 第四方面,本申请实施例还提供一种开墙服务器,所述开墙服务器包括处理器、存储器、以及存储在所述存储器上并可被所述处理器执行的计算机程序,其中所述计算机程序被所述处理器执行时,实现如上所述的开墙处理方法的步骤。

20 第五方面,本申请实施例还提供一种计算机可读存储介质,所述计算机可读存储介质上存储有计算机程序,其中所述计算机程序被处理器执行时,实现如上所述的开墙处理方法的步骤。

本申请实施例提供一种开墙处理方法、装置、服务器、系统及可读存储介质,通过根据新接入数据管理系统的目标服务器的节点标识符和数据管理系统的链路拓扑数据,确定目标服务器的链路调用关系,然后根据该节点标识符和链路调用关系,生成目标服务器的开墙配置信息,并向授权管理设备发送授权申请请求,若获取到授权管理设备基于授权申请请求返回的授权成功信息,则根据开墙配置信息,对目标服务器进行开墙操作,使得开墙服务器能够准确快速的对目标服务器进行开墙操作,极大的提高了开墙效率和用户体验。

附图说明

30 为了更清楚地说明本申请实施例技术方案,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是本申请实施例提供的一种开墙处理系统的架构示意图;

图2是本申请实施例提供的一种开墙处理方法的流程示意图;

图3是本申请实施例提供的另一种开墙处理方法的流程示意图;

35 图4是本申请实施例提供的一种开墙处理装置的示意性框图;

图5是本申请实施例提供的另一种开墙处理装置的示意性框图;

图6是本申请实施例提供的一种开墙服务器的结构示意图。

本申请目的的实现、功能特点及优点将结合实施例,参阅附图做进一步说明。

40 具体实施方式

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,所描述的实施例是本申请一部分实施例,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,都属于本申请保护的范围。

附图中所示的流程图仅是示例说明，不是必须包括所有的内容和操作/步骤，也不是必须按所描述的顺序执行。例如，有的操作/步骤还可以分解、组合或部分合并，因此实际执行的顺序有可能根据实际情况改变。

下面结合附图，对本申请的一些实施方式作详细说明。在不冲突的情况下，下述的实施例及实施例中的特征可以相互组合。

目前，越来越多的企业都使用服务器建立数据管理系统，方便企业管理数据，对于金融保险企业，数据管理系统所需的服务器和应用较多，同时由于金融保险数据的敏感性，对数据管理系统的安全性要求较高，对此按照需求需要在各服务器之间设置防火墙。对于新接入数据管理系统的服务器，需要对新接入的服务器进行开墙操作，即配置新接入的服务器的防火墙以及配置与新接入的服务器相关联的服务器的防火墙，由于数据管理系统涉及到的服务器较多，用户无法准确和快速地对新接入的服务器进行开墙操作，开墙效率较低。

本申请实施例提供一种开墙处理方法、装置、服务器、系统及可读存储介质，通过根据新接入数据管理系统的目标服务器的节点标识符和数据管理系统的链路拓扑数据，确定目标服务器的链路调用关系，然后根据该节点标识符和链路调用关系，生成目标服务器的开墙配置信息，并向授权管理设备发送授权申请请求，若获取到授权管理设备基于授权申请请求返回的授权成功信息，则根据开墙配置信息，对目标服务器进行开墙操作，使得开墙服务器能够准确快速的对目标服务器进行开墙操作，极大的提高了开墙效率和用户体验。

请参阅图 1，图 1 是本申请实施例提供的一种开墙处理系统的架构示意图。

如图 1 所示，如图 1 所示，开墙处理系统包括终端设备 110、开墙服务器 120 和授权管理设备 130，终端设备 110 与开墙服务器 120 通信连接，开墙服务器 120 与授权管理设备 130 连接，其中：

所述终端设备 110，用于向开墙服务器 120 发送开墙请求，其中，开墙请求携带有新接入数据管理系统的目标服务器的节点标识符；

所述开墙服务器 120，用于获取终端设备 110 发送的开墙请求，并根据开墙请求中的节点标识符和数据管理系统的链路拓扑数据，确定目标服务器的链路调用关系；

所述开墙服务器 120 还用于根据节点标识符和链路调用关系，生成目标服务器的开墙配置信息，并向授权管理设备 130 发送授权申请请求；

所述授权管理设备 130 用于根据授权申请请求，输出授权提示信息，以提示授权人员需要进行开墙授权；

所述授权管理设备 130 还用于在检测到授权人员触发的授权确认指令时，根据授权确认指令向开墙服务器 120 发送授权成功信息；

所述开墙服务器 120 还用于在接收到授权管理设备 130 发送的授权成功信息时，根据开墙配置信息，对目标服务器进行开墙操作。

其中，该终端设备 110 可以手机、平板电脑、笔记本电脑、台式电脑、个人数字助理和穿戴式设备等，授权管理设备 130 可以为手机、平板电脑、笔记本电脑和台式电脑等，开墙服务器 120 可以为单台的服务器，也可以为由多台服务器组成的集群。

在数据管理系统中新接入服务器后，需要对新接入的服务器进行开墙操作，即配置新接入的服务器的防火墙以及配置与新接入的服务器相关联的服务器的防火墙，使得新接入的服务器能够与数据管理系统中的服务器进行数据交互，为此，终端设备 110 还用于：显示开墙配置页面，并获取用户在该开墙配置页面输入的新接入数据管理系统的目标服务器的节点标识符，然后向开墙服务器 120 发送携带有节点标识符的开墙请求，开墙服务器 120 获取终端设备发送的开墙请求，并提取该开墙请求中的新接入数据管理系统的目标服务器的节点标识符以及获取数据管理系统的最新的链路拓扑数据。

其中，该开墙配置页面包括节点标识符的输入框和开墙确认图标，当检测到用户对该开墙确认图标的触控操作时，终端设备 110 可以确定用户想要获取目标服务器的上下游链路调用关系，因此，终端设备 110 确定该输入框中是否存在用户输入的新接入数据管理系统的目标服务器的节点标识符，若该输入框中存在用户输入的新接入数据管理系统的目标服务器的节点标识符，则终端设备 110 生成携带有该节点标识符的开墙请求，并向开墙服务器 120 发送该开墙请求。

进一步地，终端设备 110 还用于获取用户在该输入框中输入的节点标识符，并获取数据管理系统的节点标识符库；确定用户在该输入框中输入的节点标识符是否位于数据管理系统的新增节点标识符库内，如果用户在该输入框中输入的节点标识符位于新增节点标识符库内，则确定输入的节点标识符为新接入数据管理系统的目标服务器的节点标识符，如果输入的节点标识符不位于新增节点标识符库内，则输出提示信息，以提示用户输入新接入数据管理系统的目标服务器的节点标识符。通过对用户输入的节点标识符进行校验，能够在用户输入的节点标识符不为新接入数据管理系统的目标服务器的节点标识符时，输出提示信息以提示用户重新输入节点标识符，提高用户体验。

在一实施例中，开墙服务器 120 还用于：根据节点标识符和链路拓扑数据，确定与目标服务器相连的上游服务器和/或下游服务器；从链路拓扑数据中获取上游服务器的第一节点标识符和/或下游服务器的第二节点标识符；根据第一节点标识符和第二节点标识符中的至少一项和节点标识符，确定目标服务器的链路调用关系。

在一实施例中，所述链路调用关系包括上游链路调用关系和下游链路调用关系中的至少一项，所述开墙配置信息包括上游开墙配置信息和下游开墙配置信息中的至少一项，开墙服务器 120 还用于：从上游链路调用关系获取所述目标服务器的上游服务器的第一节点标识符；获取目标服务器的节点标识符对应的 IP 地址和端口信息，获取第一节点标识符对应的第一 IP 地址和第一端口信息；根据节点标识符对应的 IP 地址和端口信息以及第一 IP 地址和第一端口信息，生成目标服务器的上游开墙配置信息；和/或从下游链路调用关系获取目标服务器的下游服务器的第二节点标识符；获取目标服务器的节点标识符对应的 IP 地址和端口信息，获取第二节点标识符对应的第二 IP 地址和第二端口信息；根据节点标识符对应的 IP 地址和端口信息以及第二 IP 地址和第二端口信息，生成目标服务器的下游开墙配置信息。

在一实施例中，开墙服务器 120 还用于：从上游开墙配置信息中获取目标服务器的上游服务器的第一 IP 地址和第一端口信息以及目标服务器的 IP 地址和端口信息；根据目标服务器的 IP 地址和端口信息，将第一 IP 地址和第一端口信息添加到目标服务器与上游服务器之间的第一防火墙的白名单内；和/或从下游开墙配置信息中获取目标服务器的下游服务器的第二 IP 地址和第二端口信息以及目标服务器的 IP 地址和端口信息；根据第二 IP 地址和第二端口信息，将 IP 地址和端口信息添加到目标服务器与下游服务器之间的第二防火墙的白名单内。

在一实施例中，在对目标服务器进行开墙操作之后，开墙服务器 120 还用于：对目标服务器的关联服务器与目标服务器之间的通信链路进行开墙验证，得到开墙验证结果；将开墙验证结果发送至终端设备，以供终端设备显示开墙验证结果。其中，目标服务器的关联服务器包括目标服务器的上游服务器和下游服务器中的至少一项。

在一实施例中，开墙服务器 120 还用于：控制上游服务器，向目标服务器发送第一 telnet 命令；在目标服务器执行所述第一 telnet 命令后，获取第一 telnet 命令对应的第一日志；根据第一日志，确定上游服务器与目标服务器之间的第一开墙验证结果；和/或控制所述目标服务器，向所述下游服务器发送第二 telnet 命令；在下游服务器执行第二 telnet 命令后，获取第二 telnet 命令对应的第二日志；根据第二日志，确定下游服务器与目标服务器之间的

第二开墙验证结果。

请参阅图 2，图 2 是本申请实施例提供的一种开墙处理方法的流程示意图。

如图 2 所示，该开墙处理方法包括步骤 S101 至步骤 S104。

5 步骤 S101、获取终端设备发送的开墙请求，其中，所述开墙请求携带有新接入数据管理系统的目标服务器的节点标识符。

其中，终端设备与开墙服务器通信连接，开墙服务器与授权管理设备通信连接。

10 在数据管理系统中新接入服务器后，需要对新接入的服务器进行开墙操作，即配置新接入的服务器的防火墙以及配置与新接入的服务器相关联的服务器的防火墙，使得新接入的服务器能够与数据管理系统中的服务器进行数据交互，为此，终端设备显示开墙配置页面，并获取用户在该开墙配置页面输入的新接入数据管理系统的目标服务器的节点标识符，然后向开墙服务器发送携带有节点标识符的开墙请求，开墙服务器获取终端设备发送的开墙请求，并提取该开墙请求中的新接入数据管理系统的目标服务器的节点标识符，且获取数据管理系统的最新的链路拓扑数据。

15 其中，该开墙配置页面包括节点标识符的输入框和开墙确认图标，当检测到用户对该开墙确认图标的触控操作时，终端设备可以确定用户想要获取目标服务器的上下游链路调用关系，因此，确定该输入框中是否存在用户输入的新接入数据管理系统的目标服务器的节点标识符，若该输入框中存在用户输入的新接入数据管理系统的目标服务器的节点标识符，则生成携带有该节点标识符的开墙请求，并向开墙服务器发送该开墙请求。

20 进一步地，终端设备获取用户在该输入框中输入的节点标识符，并获取数据管理系统的节点标识符库；确定用户在该输入框中输入的节点标识符是否位于数据管理系统的新增节点标识符库内，如果用户在该输入框中输入的节点标识符位于新增节点标识符库内，则确定输入的节点标识符为新接入数据管理系统的目标服务器的节点标识符，如果输入的节点标识符不位于新增节点标识符库内，则输出提示信息，以提示用户输入新接入数据管理系统的目标服务器的节点标识符。通过对用户输入的节点标识符进行校验，能够在用户输入的节点标识符不为新接入数据管理系统的目标服务器的节点标识符时，输出提示信息以提示用户重新输入节点标识符，提高用户体验。

25 步骤 S102、根据所述节点标识符和所述数据管理系统的链路拓扑数据，确定所述目标服务器的链路调用关系。

30 其中，该链路拓扑数据包括数据管理系统涉及到的各个服务器的节点标识符和链路调用关系，数据管理系统涉及到的服务器包括负载均衡服务器(F5)、代理服务器(nginx)、应用服务器和数据库服务器等，不同的服务器对应不同的节点标识符，该节点标识符用于唯一标识服务器，例如，该节点标识符为服务器的名称，通过名称来区分服务器，便于用户记忆。

35 在一实施例中，根据节点标识符和数据管理系统的链路拓扑数据，确定目标服务器的链路调用关系的方式可以为：根据节点标识符和链路拓扑数据，确定与目标服务器相连的上游服务器和/或下游服务器；从链路拓扑数据中获取上游服务器的第一节点标识符和/或下游服务器的第二节点标识符；根据第一节点标识符和第二节点标识符中的至少一项和节点标识符，确定目标服务器的链路调用关系。

40 步骤 S103、根据所述节点标识符和所述链路调用关系，生成所述目标服务器的开墙配置信息，并向授权管理设备发送授权申请请求。

其中，目标服务器的链路调用关系包括目标服务器的上游链路调用关系和下游链路调用关系中的至少一项，所述开墙配置信息包括上游开墙配置信息和下游开墙配置信息中的至少一项，上游链路调用关系包括目标服务器的节点标识符和该目标服务器的上游服务器的第一节点标识符，下游链路调用关系包括目标服务器的节点标识符和该目标服务器的下

游服务器的第二节点标识符。

在一实施例中，根据节点标识符和链路调用关系，生成目标服务器的开墙配置信息的方式可以为：从上游链路调用关系获取所述目标服务器的上游服务器的第一节点标识符；获取目标服务器的节点标识符对应的 IP 地址和端口信息，获取第一节点标识符对应的第一 IP 地址和第一端口信息；根据节点标识符对应的 IP 地址和端口信息以及第一 IP 地址和第一端口信息，生成目标服务器的上游开墙配置信息；和/或从下游链路调用关系获取目标服务器的下游服务器的第二节点标识符；获取目标服务器的节点标识符对应的 IP 地址和端口信息，获取第二节点标识符对应的第二 IP 地址和第二端口信息；根据节点标识符对应的 IP 地址和端口信息以及第二 IP 地址和第二端口信息，生成目标服务器的下游开墙配置信息。

在一实施例中，在生成目标服务器的开墙配置信息后，开墙服务器向授权管理设备发送授权申请请求；授权管理设备在接收到该授权申请请求后，输出授权提示信息，以提示授权人员需要进行开墙授权；当检测到授权人员触发的授权确认指令时，向开墙服务器发送授权成功信息，而当检测到授权人员触发的授权拒绝指令时，向开墙服务器发送授权失败信息。

在一实施例中，授权管理设备响应于授权人员对该授权提示信息的触控操作，显示授权登录页面；获取授权人员在该授权登录页面输入的登录信息，并对该登录信息进行身份验证；当该登录信息通过身份验证时，显示开墙授权页面，其中，该开墙授权页面包括授权确认图标和授权拒绝图标；当检测到授权人员对该授权确认图标的触控操作时，生成授权确认指令，而当检测到授权人员对该授权拒绝图标的触控操作时，生成授权拒绝指令。通过对授权人员输入的登录信息进行验证，并在验证后，显示开墙授权页面，可以提高授权的安全性。

步骤 S104、若获取到所述授权管理设备基于所述授权申请请求返回的授权成功信息，则根据所述开墙配置信息，对所述目标服务器进行开墙操作。

若获取到授权管理设备基于授权申请请求返回的授权失败信息，向终端设备发送授权失败信息，终端设备在接收到授权失败信息时，输出授权失败提示信息，以提示用户开墙申请失败；若获取到墙授权设备基于授权申请请求返回的授权成功信息，则根据该开墙配置信息，对目标服务器进行开墙操作。

在一实施例中，根据开墙配置信息，对目标服务器进行开墙操作的方式可以为：从上游开墙配置信息中获取目标服务器的上游服务器的第一 IP 地址和第一端口信息以及所述目标服务器的 IP 地址和端口信息；根据目标服务器的 IP 地址和端口信息，将第一 IP 地址和第一端口信息添加到目标服务器与上游服务器之间的第一防火墙的白名单内，使得上游服务器能够通过第一防火墙访问目标服务器；和/或从下游开墙配置信息中获取目标服务器的下游服务器的第二 IP 地址和第二端口信息以及目标服务器的 IP 地址和端口信息；根据第二 IP 地址和所述第二端口信息，将 IP 地址和端口信息添加到目标服务器与下游服务器之间的第二防火墙的白名单内，使得目标服务器能够通过第二防火墙访问下游服务器。

上述实施例提供的开墙处理方法，通过根据新接入数据管理系统的目标服务器的节点标识符和数据管理系统的链路拓扑数据，确定目标服务器的链路调用关系，然后根据该节点标识符和链路调用关系，生成目标服务器的开墙配置信息，并向授权管理设备发送授权申请请求，若获取到授权管理设备基于授权申请请求返回的授权成功信息，则根据开墙配置信息，对目标服务器进行开墙操作，使得开墙服务器能够准确快速的对目标服务器进行开墙操作，极大的提高了开墙效率和用户体验。

请参阅图 3，图 3 是本申请实施例提供的另一种开墙处理方法的流程示意图。

如图 3 所示，该开墙处理方法包括步骤 S201 至 S206。

步骤 S201、获取终端设备发送的开墙请求，其中，所述开墙请求携带有新接入数据管

理系统的目标服务器的节点标识符。

终端设备显示开墙配置页面，并获取用户在该开墙配置页面输入的新接入数据管理系统的目标服务器的节点标识符，然后向开墙服务器发送携带有节点标识符的开墙请求，开墙服务器获取终端设备发送的开墙请求，并提取该开墙请求中的新接入数据管理系统的目标服务器的节点标识符，且获取数据管理系统的最新的链路拓扑数据。

步骤 S202、根据所述节点标识符和所述数据管理系统的链路拓扑数据，确定所述目标服务器的链路调用关系。

示例性的，根据节点标识符和链路拓扑数据，确定与目标服务器相连的上游服务器和/或下游服务器；从链路拓扑数据中获取上游服务器的第一节点标识符和/或下游服务器的第二节点标识符；根据第一节点标识符和第二节点标识符中的至少一项和节点标识符，确定目标服务器的链路调用关系。

步骤 S203、根据所述节点标识符和所述链路调用关系，生成所述目标服务器的开墙配置信息，并向授权管理设备发送授权申请请求。

其中，目标服务器的链路调用关系包括目标服务器的上游链路调用关系和下游链路调用关系中的至少一项，所述开墙配置信息包括上游开墙配置信息和下游开墙配置信息中的至少一项。

示例性的，在生成目标服务器的开墙配置信息后，开墙服务器向授权管理设备发送授权申请请求；授权管理设备在接收到该授权申请请求后，输出授权提示消息，以提示授权人员需要进行开墙授权；当检测到授权人员触发的授权确认指令时，向开墙服务器发送授权成功信息，而当检测到授权人员触发的授权拒绝指令时，向开墙服务器发送授权失败信息。

步骤 S204、若获取到所述授权管理设备基于所述授权申请请求返回的授权成功信息，则根据所述开墙配置信息，对所述目标服务器进行开墙操作。

若获取到授权管理设备基于授权申请请求返回的授权失败信息，向终端设备发送授权失败信息，终端设备在接收到授权失败信息时，输出授权失败提示信息，以提示用户开墙申请失败；若获取到墙授权设备基于授权申请请求返回的授权成功信息，则根据该开墙配置信息，对目标服务器进行开墙操作。

步骤 S205、对所述目标服务器的关联服务器与所述目标服务器之间的通信链路进行开墙验证，得到开墙验证结果。

示例性的，控制目标服务器的上游服务器，向目标服务器发送第一 telnet 命令；在目标服务器执行所述第一 telnet 命令后，获取所述第一 telnet 命令对应的第一日志；根据第一日志，确定目标服务器的上游服务器与目标服务器之间的第一开墙验证结果；和/或控制目标服务器，向目标服务器的下游服务器发送第二 telnet 命令；在下游服务器执行第二 telnet 命令后，获取第二 telnet 命令对应的第二日志；根据第二日志，确定目标服务器的下游服务器与目标服务器之间的第二开墙验证结果。

步骤 S206、将所述开墙验证结果发送至所述终端设备，以供所述终端设备显示所述开墙验证结果。

在获取到目标服务器的开墙验证结果后，将该开墙验证结果发送至终端设备，以供终端设备显示开墙验证结果，使得运维任务可以知晓目标服务器的开墙情况。

上述实施例提供的开墙处理方法，通过在对目标服务器进行开墙操作后，对目标服务器的关联服务器与目标服务器之间的通信链路进行开墙验证，得到开墙验证结果，并将该开墙验证结果发送至终端设备，以供终端设备显示开墙验证结果，可以实现目标服务器的开墙操作和开墙验证的自动化，极大的提高了开墙验证的效率。

请参阅图 4，图 4 是本申请实施例提供的一种开墙处理装置的示意性框图。

如图 4 所示, 该开墙处理装置 300, 包括: 获取模块 310、确定模块 320、生成模块 330、发送模块 340 和开墙模块 350, 其中:

所述获取模块 310, 用于获取终端设备发送的开墙请求, 其中, 所述开墙请求携带有新接入数据管理系统的目标服务器的节点标识符;

5 所述确定模块 320, 用于根据所述节点标识符和所述数据管理系统的链路拓扑数据, 确定所述目标服务器的链路调用关系;

所述生成模块 330, 用于根据所述节点标识符和所述链路调用关系, 生成所述目标服务器的开墙配置信息;

所述发送模块 340, 用于向授权管理设备发送授权申请请求;

10 所述开墙模块 350, 用于若获取到所述授权管理设备基于所述授权申请请求返回的授权成功信息, 则根据所述开墙配置信息对所述目标服务器进行开墙操作。

在一实施例中, 所述确定模块 320 还用于:

根据所述节点标识符和所述链路拓扑数据, 确定与所述目标服务器相连的上游服务器和/或下游服务器;

15 从所述链路拓扑数据中获取所述上游服务器的第一节点标识符和/或所述下游服务器的第二节点标识符;

根据所述第一节点标识符和所述第二节点标识符中的至少一项和所述节点标识符, 确定所述目标服务器的链路调用关系。

20 在一实施例中, 所述链路调用关系包括上游链路调用关系和下游链路调用关系中的至少一项, 所述开墙配置信息包括上游开墙配置信息和下游开墙配置信息中的至少一项, 所述生成模块 330 还用于:

从所述上游链路调用关系获取所述目标服务器的上游服务器的第一节点标识符;

获取所述目标服务器的节点标识符对应的 IP 地址和端口信息, 获取所述第一节点标识符对应的第一 IP 地址和第一端口信息;

25 根据所述节点标识符对应的 IP 地址和端口信息以及所述第一 IP 地址和所述第一端口信息, 生成所述目标服务器的上游开墙配置信息;

和/或

从所述下游链路调用关系获取所述目标服务器的下游服务器的第二节点标识符;

30 获取所述目标服务器的节点标识符对应的 IP 地址和端口信息, 获取所述第二节点标识符对应的第二 IP 地址和第二端口信息;

根据所述节点标识符对应的 IP 地址和端口信息以及所述第二 IP 地址和所述第二端口信息, 生成所述目标服务器的下游开墙配置信息。

在一实施例中, 所述开墙模块 350 还用于:

35 从所述上游开墙配置信息中获取所述目标服务器的上游服务器的第一 IP 地址和第一端口信息以及所述目标服务器的 IP 地址和端口信息;

根据所述目标服务器的 IP 地址和端口信息, 将所述第一 IP 地址和所述第一端口信息添加到所述目标服务器与所述上游服务器之间的第一防火墙的白名单内;

和/或

40 从所述下游开墙配置信息中获取所述目标服务器的下游服务器的第二 IP 地址和第二端口信息以及所述目标服务器的 IP 地址和端口信息;

根据所述第二 IP 地址和所述第二端口信息, 将所述 IP 地址和所述端口信息添加到所述目标服务器与所述下游服务器之间的第二防火墙的白名单内。

请参阅图 5, 图 5 是本申请实施例提供的另一种开墙处理装置的示意性框图。

如图 5 所示, 该开墙处理装置 400, 包括: 获取模块 410、确定模块 420、生成模块

430、发送模块 440、开墙模块 450 和验证模块 460，其中：

所述获取模块 410，用于获取终端设备发送的开墙请求，其中，所述开墙请求携带有新接入数据管理系统的目标服务器的节点标识符；

5 所述确定模块 420，用于根据所述节点标识符和所述数据管理系统的链路拓扑数据，确定所述目标服务器的链路调用关系；

所述生成模块 430，用于根据所述节点标识符和所述链路调用关系，生成所述目标服务器的开墙配置信息；

所述发送模块 440，用于向授权管理设备发送授权申请请求；

10 所述开墙模块 450，用于若获取到所述授权管理设备基于所述授权申请请求返回的授权成功信息，则根据所述开墙配置信息对所述目标服务器进行开墙操作；

所述验证模块 460，用于对所述目标服务器的关联服务器与所述目标服务器之间的通信链路进行开墙验证，得到开墙验证结果；

所述发送模块 440，还用于将所述开墙验证结果发送至所述终端设备，以供所述终端设备显示所述开墙验证结果。

15 在一实施例中，所述关联服务器包括目标服务器的上游服务器和下游服务器中的至少一项，所述验证模块 460 还用于：

控制所述上游服务器，向所述目标服务器发送第一 telnet 命令；

在所述目标服务器执行所述第一 telnet 命令后，获取所述第一 telnet 命令对应的第一日志；

20 根据所述第一日志，确定所述上游服务器与所述目标服务器之间的第一开墙验证结果；和/或

控制所述目标服务器，向所述下游服务器发送第二 telnet 命令；

在所述下游服务器执行所述第二 telnet 命令后，获取所述第二 telnet 命令对应的第二日志；

25 根据所述第二日志，确定所述下游服务器与所述目标服务器之间的第二开墙验证结果。

需要说明的是，所属领域的技术人员可以清楚地了解到，为了描述的方便和简洁，上述描述的装置和各模块及单元的具体工作过程，可以参考前述开墙处理方法实施例中的对应过程，在此不再赘述。

30 上述实施例提供的装置可以实现为一种计算机程序的形式，该计算机程序可以在如图 6 所示的开墙服务器上运行。

请参阅图 6，图 6 是本申请实施例提供的一种开墙服务器的结构示意图。

如图 6 所示，该开墙服务器包括通过系统总线连接的处理器、存储器和网络接口，其中，存储器可以包括存储介质和内存储器。

35 存储介质可存储操作系统和计算机程序。该计算机程序包括程序指令，该程序指令被执行时，可使得处理器执行任意一种开墙处理方法。

处理器用于提供计算和控制能力，支撑整个开墙服务器的运行。

内存储器为存储介质中的计算机程序的运行提供环境，该计算机程序被处理器执行时，可使得处理器执行任意一种开墙处理方法。

40 该网络接口用于进行网络通信，如发送分配的任务等。本领域技术人员可以理解，图 6 中示出的结构，仅仅是与本申请方案相关的部分结构的框图，并不构成对本申请方案所应用于其上的开墙服务器的限定，具体的开墙服务器可以包括比图中所示更多或更少的部件，或者组合某些部件，或者具有不同的部件布置。

应当理解的是，处理器可以是中央处理单元 (Central Processing Unit, CPU)，该处理器还可以是其他通用处理器、数字信号处理器 (Digital Signal Processor, DSP)、专用集成

电路 (Application Specific Integrated Circuit, ASIC)、现场可编程门阵列 (Field-Programmable Gate Array, FPGA) 或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件等。其中, 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。

5 本领域技术人员可以理解, 图 6 中示出的结构, 仅仅是与本申请方案相关的部分结构的框图, 并不构成对本申请方案所应用于其上的开墙服务器的限定, 具体的开墙服务器可以包括比图中所示更多或更少的部件, 或者组合某些部件, 或者具有不同的部件布置。

应当理解的是, 处理器可以是中央处理单元 (Central Processing Unit, CPU), 该处理器还可以是其他通用处理器、数字信号处理器 (Digital Signal Processor, DSP)、专用集成
10 电路 (Application Specific Integrated Circuit, ASIC)、现场可编程门阵列 (Field-Programmable Gate Array, FPGA) 或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件等。其中, 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。

其中, 在一实施例中, 所述处理器用于运行存储在存储器中的计算机程序, 以实现如下
15 步骤:

获取终端设备发送的开墙请求, 其中, 所述开墙请求携带有新接入数据管理系统的目标服务器的节点标识符;

根据所述节点标识符和所述数据管理系统的链路拓扑数据, 确定所述目标服务器的链路调用关系;

20 根据所述节点标识符和所述链路调用关系, 生成所述目标服务器的开墙配置信息, 并向授权管理设备发送授权申请请求;

若获取到所述授权管理设备基于所述授权申请请求返回的授权成功信息, 则根据所述开墙配置信息, 对所述目标服务器进行开墙操作。

在一实施例中, 所述处理器在实现根据所述开墙请求中的所述节点标识符和所述数据
25 管理系统的链路拓扑数据, 确定所述目标服务器的链路调用关系时, 用于实现:

根据所述节点标识符和所述链路拓扑数据, 确定与所述目标服务器相连的上游服务器和/或下游服务器;

从所述链路拓扑数据中获取所述上游服务器的第一节点标识符和/或所述下游服务器的第二节点标识符;

30 根据所述第一节点标识符和所述第二节点标识符中的至少一项和所述节点标识符, 确定所述目标服务器的链路调用关系。

在一实施例中, 所述链路调用关系包括上游链路调用关系和下游链路调用关系中的至少一项, 所述开墙配置信息包括上游开墙配置信息和下游开墙配置信息中的至少一项, 所述处理器在实现根据所述节点标识符和所述链路调用关系, 生成所述目标服务器的开墙配置
35 信息时, 用于实现:

从所述上游链路调用关系获取所述目标服务器的上游服务器的第一节点标识符;

获取所述目标服务器的节点标识符对应的 IP 地址和端口信息, 获取所述第一节点标识符对应的第一 IP 地址和第一端口信息;

40 根据所述节点标识符对应的 IP 地址和端口信息以及所述第一 IP 地址和所述第一端口信息, 生成所述目标服务器的上游开墙配置信息;

和/或

从所述下游链路调用关系获取所述目标服务器的下游服务器的第二节点标识符;

获取所述目标服务器的节点标识符对应的 IP 地址和端口信息, 获取所述第二节点标识符对应的第二 IP 地址和第二端口信息;

根据所述节点标识符对应的 IP 地址和端口信息以及所述第二 IP 地址和所述第二端口信息，生成所述目标服务器的下游开墙配置信息。

在一实施例中，所述处理器在实现根据所述开墙配置信息，对所述目标服务器进行开墙操作时，用于实现：

- 5 从所述上游开墙配置信息中获取所述目标服务器的上游服务器的第一 IP 地址和第一端口信息以及所述目标服务器的 IP 地址和端口信息；

根据所述目标服务器的 IP 地址和端口信息，将所述第一 IP 地址和所述第一端口信息添加到所述目标服务器与所述上游服务器之间的第一防火墙的白名单内；

和/或

- 10 从所述下游开墙配置信息中获取所述目标服务器的下游服务器的第二 IP 地址和第二端口信息以及所述目标服务器的 IP 地址和端口信息；

根据所述第二 IP 地址和所述第二端口信息，将所述 IP 地址和所述端口信息添加到所述目标服务器与所述下游服务器之间的第二防火墙的白名单内。

- 15 其中，在另一实施例中，所述处理器用于运行存储在存储器中的计算机程序，以实现如下步骤：

获取终端设备发送的开墙请求，其中，所述开墙请求携带有新接入数据管理系统的目标服务器的节点标识符；

根据所述节点标识符和所述数据管理系统的链路拓扑数据，确定所述目标服务器的链路调用关系；

- 20 根据所述节点标识符和所述链路调用关系，生成所述目标服务器的开墙配置信息，并向授权管理设备发送授权申请请求；

若获取到所述授权管理设备基于所述授权申请请求返回的授权成功信息，则根据所述开墙配置信息，对所述目标服务器进行开墙操作；

- 25 对所述目标服务器的关联服务器与所述目标服务器之间的通信链路进行开墙验证，得到开墙验证结果；

将所述开墙验证结果发送至所述终端设备，以供所述终端设备显示所述开墙验证结果。

在一实施例中，所述关联服务器包括目标服务器的上游服务器和下游服务器中的至少一项，所述处理器在实现所述目标服务器的关联服务器与所述目标服务器之间的通信链路进行开墙验证，得到开墙验证结果时，用于实现：

- 30 控制所述上游服务器，向所述目标服务器发送第一 telnet 命令；

在所述目标服务器执行所述第一 telnet 命令后，获取所述第一 telnet 命令对应的第一日志；

根据所述第一日志，确定所述上游服务器与所述目标服务器之间的第一开墙验证结果；

和/或

- 35 控制所述目标服务器，向所述下游服务器发送第二 telnet 命令；

在所述下游服务器执行所述第二 telnet 命令后，获取所述第二 telnet 命令对应的第二日志；

根据所述第二日志，确定所述下游服务器与所述目标服务器之间的第二开墙验证结果。

- 40 需要说明的是，所属领域的技术人员可以清楚地了解到，为了描述的方便和简洁，上述描述的开墙服务器的具体工作过程，可以参考前述开墙处理方法实施例中的对应过程，在此不再赘述。

通过以上的实施方式的描述可知，本领域的技术人员可以清楚地了解到本申请可借助软件加必需的通用硬件平台的方式来实现。基于这样的理解，本申请的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来，该计算机软件产品可以

存储在存储介质中，如ROM/RAM、磁碟、光盘等，包括若干指令用以使得一台开墙服务器（可以是个人计算机，服务器，或者网络设备）执行本申请各个实施例或者实施例的某些部分所述的方法。

5 本申请实施例还提供一种计算机可读存储介质，所述计算机可读存储介质上存储有计算机程序，所述计算机程序被处理器执行时，实现以下步骤：

获取终端设备发送的开墙请求，其中，所述开墙请求携带有新接入数据管理系统的目标服务器的节点标识符；

根据所述节点标识符和所述数据管理系统的链路拓扑数据，确定所述目标服务器的链路调用关系；

10 根据所述节点标识符和所述链路调用关系，生成所述目标服务器的开墙配置信息，并向授权管理设备发送授权申请请求；

若获取到所述授权管理设备基于所述授权申请请求返回的授权成功信息，则根据所述开墙配置信息，对所述目标服务器进行开墙操作。

15 需要说明的是，所属领域的技术人员可以清楚地了解到，为了描述的方便和简洁，上述描述的计算机可读存储介质的具体工作过程，可以参考前述开墙处理方法的各个实施例。

其中，所述计算机可读存储介质可以是易失性的，也可以是非易失性的。所述计算机可读存储介质可以是前述实施例所述的开墙服务器的内部存储单元，例如所述开墙服务器的硬盘或内存。所述计算机可读存储介质也可以是所述开墙服务器的外部存储设备，例如所述开墙服务器上配备的插接式硬盘，智能存储卡(Smart Media Card, SMC)，安全数字(Secure Digital, SD)卡，闪存卡(Flash Card)等。

进一步地，所述计算机可读存储介质可主要包括存储程序区和存储数据区，其中，存储程序区可存储操作系统、至少一个功能所需的应用程序等；存储数据区可存储根据区块链节点的使用所创建的数据等。

25 本申请所指区块链是分布式数据存储、点对点传输、共识机制、加密算法等计算机技术的新型应用模式。区块链(Blockchain)，本质上是一个去中心化的数据库，是一串使用密码学方法相关联产生的数据块，每一个数据块中包含了一批次网络交易的信息，用于验证其信息的有效性(防伪)和生成下一个区块。区块链可以包括区块链底层平台、平台产品服务层以及应用服务层等。

30 应当理解，在此本申请说明书中所使用的术语仅仅是出于描述特定实施例的目的而并不意在限制本申请。如在本申请说明书和所附权利要求书中所使用的那样，除非上下文清楚地指明其它情况，否则单数形式的“一”、“一个”及“该”意在包括复数形式。

还应当理解，在本申请说明书和所附权利要求书中使用的术语“和/或”是指相关联列出的项中的一个或多个的任何组合以及所有可能组合，并且包括这些组合。需要说明的是，在本文中，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得35 包括一系列要素的过程、方法、物品或者系统不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、物品或者系统所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括该要素的过程、方法、物品或者系统中还存在另外的相同要素。

40 上述本申请实施例序号仅仅为了描述，不代表实施例的优劣。以上所述，仅为本申请的具体实施方式，但本申请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申请揭露的技术范围内，可轻易想到各种等效的修改或替换，这些修改或替换都应涵盖在本申请的保护范围之内。因此，本申请的保护范围应以权利要求的保护范围为准。

权 利 要 求 书

1、一种开墙处理方法，其中，包括：

获取终端设备发送的开墙请求，其中，所述开墙请求携带有新接入数据管理系统的目
5 标服务器的节点标识符；

根据所述节点标识符和所述数据管理系统的链路拓扑数据，确定所述目标服务器的链路调用关系；

根据所述节点标识符和所述链路调用关系，生成所述目标服务器的开墙配置信息，并向授权管理设备发送授权申请请求；

10 若获取到所述授权管理设备基于所述授权申请请求返回的授权成功信息，则根据所述开墙配置信息，对所述目标服务器进行开墙操作。

2、根据权利要求1所述的开墙处理方法，其中，所述根据所述开墙请求中的所述节点标识符和所述数据管理系统的链路拓扑数据，确定所述目标服务器的链路调用关系，包括：

15 根据所述节点标识符和所述链路拓扑数据，确定与所述目标服务器相连的上游服务器和/或下游服务器；

从所述链路拓扑数据中获取所述上游服务器的第一节点标识符和/或所述下游服务器的第二节点标识符；

20 根据所述第一节点标识符和所述第二节点标识符中的至少一项和所述节点标识符，确定所述目标服务器的链路调用关系。

3、根据权利要求1所述的开墙处理方法，其中，所述链路调用关系包括上游链路调用关系和下游链路调用关系中的至少一项，所述开墙配置信息包括上游开墙配置信息和下游开墙配置信息中的至少一项，所述根据所述节点标识符和所述链路调用关系，生成所述目标服务器的开墙配置信息，包括：

25 从所述上游链路调用关系获取所述目标服务器的上游服务器的第一节点标识符；

获取所述目标服务器的节点标识符对应的IP地址和端口信息，获取所述第一节点标识符对应的第一IP地址和第一端口信息；

根据所述节点标识符对应的IP地址和端口信息以及所述第一IP地址和所述第一端口信息，生成所述目标服务器的上游开墙配置信息；

30 和/或

从所述下游链路调用关系获取所述目标服务器的下游服务器的第二节点标识符；

获取所述目标服务器的节点标识符对应的IP地址和端口信息，获取所述第二节点标识符对应的第二IP地址和第二端口信息；

35 根据所述节点标识符对应的IP地址和端口信息以及所述第二IP地址和所述第二端口信息，生成所述目标服务器的下游开墙配置信息。

4、根据权利要求3所述的开墙处理方法，其中，所述根据所述开墙配置信息，对所述目标服务器进行开墙操作，包括：

从所述上游开墙配置信息中获取所述目标服务器的上游服务器的第一IP地址和第一端口信息以及所述目标服务器的IP地址和端口信息；

40 根据所述目标服务器的IP地址和端口信息，将所述第一IP地址和所述第一端口信息添加到所述目标服务器与所述上游服务器之间的第一防火墙的白名单内；

和/或

从所述下游开墙配置信息中获取所述目标服务器的下游服务器的第二IP地址和第二端口信息以及所述目标服务器的IP地址和端口信息；

根据所述第二 IP 地址和所述第二端口信息,将所述 IP 地址和所述端口信息添加到所述目标服务器与所述下游服务器之间的第二防火墙的白名单内。

5、根据权利要求 1-4 中任一项所述的开墙处理方法,其中,所述根据所述开墙配置信息,对所述目标服务器进行开墙操作之后,包括:

5 对所述目标服务器的关联服务器与所述目标服务器之间的通信链路进行开墙验证,得到开墙验证结果;

将所述开墙验证结果发送至所述终端设备,以供所述终端设备显示所述开墙验证结果。

6、根据权利要求 5 所述的开墙处理方法,其中,所述关联服务器包括目标服务器的上游服务器和下游服务器中的至少一项,所述对所述目标服务器的关联服务器与所述目标服务器之间的通信链路进行开墙验证,得到开墙验证结果,包括:

控制所述上游服务器,向所述目标服务器发送第一 telnet 命令;

在所述目标服务器执行所述第一 telnet 命令后,获取所述第一 telnet 命令对应的第一日志;

15 根据所述第一日志,确定所述上游服务器与所述目标服务器之间的第一开墙验证结果;和/或

控制所述目标服务器,向所述下游服务器发送第二 telnet 命令;

在所述下游服务器执行所述第二 telnet 命令后,获取所述第二 telnet 命令对应的第二日志;

20 根据所述第二日志,确定所述下游服务器与所述目标服务器之间的第二开墙验证结果。

7、一种开墙处理装置,其中,所述开墙处理装置包括:

获取模块,用于获取终端设备发送的开墙请求,其中,所述开墙请求携带有新接入数据管理系统的目标服务器的节点标识符;

确定模块,用于根据所述节点标识符和所述数据管理系统的链路拓扑数据,确定所述目标服务器的链路调用关系;

25 生成模块,用于根据所述节点标识符和所述链路调用关系,生成所述目标服务器的开墙配置信息;

发送模块,用于向授权管理设备发送授权申请请求;

开墙模块,用于若获取到所述授权管理设备基于所述授权申请请求返回的授权成功信息,则根据所述开墙配置信息对所述目标服务器进行开墙操作。

30 8、一种开墙处理系统,其中,所述开墙处理系统包括终端设备、开墙服务器和授权管理设备,所述终端设备与所述开墙服务器通信连接,所述开墙服务器与所述授权管理设备通信连接,其中:

所述终端设备,用于向开墙服务器发送开墙请求,其中,所述开墙请求携带有新接入数据管理系统的目标服务器的节点标识符;

35 所述开墙服务器,用于获取所述终端设备发送的开墙请求,并根据所述开墙请求中的节点标识符和所述数据管理系统的链路拓扑数据,确定所述目标服务器的链路调用关系;

所述开墙服务器还用于根据所述节点标识符和所述链路调用关系,生成所述目标服务器的开墙配置信息,并向授权管理设备发送授权申请请求;

40 所述授权管理设备用于根据所述授权申请请求,输出授权提示信息,以提示授权人员需要进行开墙授权;

所述授权管理设备还用于在检测到所述授权人员触发的授权确认指令时,根据所述授权确认指令向所述开墙服务器发送授权成功信息;

所述开墙服务器还用于在接收到所述授权管理设备发送的授权成功信息时,根据所述开墙配置信息,对所述目标服务器进行开墙操作。

9、一种开墙服务器，其中，所述开墙服务器包括处理器、存储器、以及存储在所述存储器上并可被所述处理器执行的计算机程序，其中所述计算机程序被所述处理器执行时，实现以下步骤：

获取终端设备发送的开墙请求，其中，所述开墙请求携带有新接入数据管理系统的目标服务器的节点标识符；

根据所述节点标识符和所述数据管理系统的链路拓扑数据，确定所述目标服务器的链路调用关系；

根据所述节点标识符和所述链路调用关系，生成所述目标服务器的开墙配置信息，并向授权管理设备发送授权申请请求；

若获取到所述授权管理设备基于所述授权申请请求返回的授权成功信息，则根据所述开墙配置信息，对所述目标服务器进行开墙操作。

10、根据权利要求9所述的开墙服务器，其中，所述处理器在实现根据所述开墙请求中的所述节点标识符和所述数据管理系统的链路拓扑数据，确定所述目标服务器的链路调用关系时，用于实现：

根据所述节点标识符和所述链路拓扑数据，确定与所述目标服务器相连的上游服务器和/或下游服务器；

从所述链路拓扑数据中获取所述上游服务器的第一节点标识符和/或所述下游服务器的第二节点标识符；

根据所述第一节点标识符和所述第二节点标识符中的至少一项和所述节点标识符，确定所述目标服务器的链路调用关系。

11、根据权利要求9所述的开墙服务器，其中，所述链路调用关系包括上游链路调用关系和下游链路调用关系中的至少一项，所述开墙配置信息包括上游开墙配置信息和下游开墙配置信息中的至少一项，所述处理器在实现根据所述节点标识符和所述链路调用关系，生成所述目标服务器的开墙配置信息时，用于实现：

从所述上游链路调用关系获取所述目标服务器的上游服务器的第一节点标识符；

获取所述目标服务器的节点标识符对应的IP地址和端口信息，获取所述第一节点标识符对应的第一IP地址和第一端口信息；

根据所述节点标识符对应的IP地址和端口信息以及所述第一IP地址和所述第一端口信息，生成所述目标服务器的上游开墙配置信息；

和/或

从所述下游链路调用关系获取所述目标服务器的下游服务器的第二节点标识符；

获取所述目标服务器的节点标识符对应的IP地址和端口信息，获取所述第二节点标识符对应的第二IP地址和第二端口信息；

根据所述节点标识符对应的IP地址和端口信息以及所述第二IP地址和所述第二端口信息，生成所述目标服务器的下游开墙配置信息。

12、根据权利要求11所述的开墙服务器，其中，所述处理器在实现根据所述开墙配置信息，对所述目标服务器进行开墙操作时，用于实现：

从所述上游开墙配置信息中获取所述目标服务器的上游服务器的第一IP地址和第一端口信息以及所述目标服务器的IP地址和端口信息；

根据所述目标服务器的IP地址和端口信息，将所述第一IP地址和所述第一端口信息添加到所述目标服务器与所述上游服务器之间的第一防火墙的白名单内；

和/或

从所述下游开墙配置信息中获取所述目标服务器的下游服务器的第二IP地址和第二端口信息以及所述目标服务器的IP地址和端口信息；

根据所述第二 IP 地址和所述第二端口信息,将所述 IP 地址和所述端口信息添加到所述目标服务器与所述下游服务器之间的第二防火墙的白名单内。

13、根据权利要求 9-12 中任一项所述的开墙服务器,其中,所述处理器在实现根据所述开墙配置信息,对所述目标服务器进行开墙操作之后,还用于实现:

5 对所述目标服务器的关联服务器与所述目标服务器之间的通信链路进行开墙验证,得到开墙验证结果;

将所述开墙验证结果发送至所述终端设备,以供所述终端设备显示所述开墙验证结果。

14、根据权利要求 13 所述的开墙服务器,其中,所述关联服务器包括目标服务器的上游服务器和下游服务器中的至少一项,所述处理器在实现所述目标服务器的关联服务器与
10 所述目标服务器之间的通信链路进行开墙验证,得到开墙验证结果时,用于实现:

控制所述上游服务器,向所述目标服务器发送第一 telnet 命令;

在所述目标服务器执行所述第一 telnet 命令后,获取所述第一 telnet 命令对应的第一日志;

15 根据所述第一日志,确定所述上游服务器与所述目标服务器之间的第一开墙验证结果;和/或

控制所述目标服务器,向所述下游服务器发送第二 telnet 命令;

在所述下游服务器执行所述第二 telnet 命令后,获取所述第二 telnet 命令对应的第二日志;

根据所述第二日志,确定所述下游服务器与所述目标服务器之间的第二开墙验证结果。

20 15、一种计算机可读存储介质,其中,所述计算机可读存储介质上存储有计算机程序,其中所述计算机程序被处理器执行时,实现以下步骤:

获取终端设备发送的开墙请求,其中,所述开墙请求携带有新接入数据管理系统的目标服务器的节点标识符;

25 根据所述节点标识符和所述数据管理系统的链路拓扑数据,确定所述目标服务器的链路调用关系;

根据所述节点标识符和所述链路调用关系,生成所述目标服务器的开墙配置信息,并向授权管理设备发送授权申请请求;

若获取到所述授权管理设备基于所述授权申请请求返回的授权成功信息,则根据所述开墙配置信息,对所述目标服务器进行开墙操作。

30 16、根据权利要求 15 所述的计算机可读存储介质,其中,所述处理器在实现根据所述开墙请求中的所述节点标识符和所述数据管理系统的链路拓扑数据,确定所述目标服务器的链路调用关系时,用于实现:

根据所述节点标识符和所述链路拓扑数据,确定与所述目标服务器相连的上游服务器和/或下游服务器;

35 从所述链路拓扑数据中获取所述上游服务器的第一节点标识符和/或所述下游服务器的第二节点标识符;

根据所述第一节点标识符和所述第二节点标识符中的至少一项和所述节点标识符,确定所述目标服务器的链路调用关系。

40 17、根据权利要求 15 所述的计算机可读存储介质,其中,所述链路调用关系包括上游链路调用关系和下游链路调用关系中的至少一项,所述开墙配置信息包括上游开墙配置信息和下游开墙配置信息中的至少一项,所述处理器在实现根据所述节点标识符和所述链路调用关系,生成所述目标服务器的开墙配置信息时,用于实现:

从所述上游链路调用关系获取所述目标服务器的上游服务器的第一节点标识符;

获取所述目标服务器的节点标识符对应的 IP 地址和端口信息,获取所述第一节点标

识符对应的第一 IP 地址和第一端口信息；

根据所述节点标识符对应的 IP 地址和端口信息以及所述第一 IP 地址和所述第一端口信息，生成所述目标服务器的上游开墙配置信息；

和/或

5 从所述下游链路调用关系获取所述目标服务器的下游服务器的第二节点标识符；

获取所述目标服务器的节点标识符对应的 IP 地址和端口信息，获取所述第二节点标识符对应的第二 IP 地址和第二端口信息；

根据所述节点标识符对应的 IP 地址和端口信息以及所述第二 IP 地址和所述第二端口信息，生成所述目标服务器的下游开墙配置信息。

10 18、根据权利要求 17 所述的计算机可读存储介质，其中，所述处理器在实现根据所述开墙配置信息，对所述目标服务器进行开墙操作时，用于实现：

从所述上游开墙配置信息中获取所述目标服务器的上游服务器的第一 IP 地址和第一端口信息以及所述目标服务器的 IP 地址和端口信息；

15 根据所述目标服务器的 IP 地址和端口信息，将所述第一 IP 地址和所述第一端口信息添加到所述目标服务器与所述上游服务器之间的第一防火墙的白名单内；

和/或

从所述下游开墙配置信息中获取所述目标服务器的下游服务器的第二 IP 地址和第二端口信息以及所述目标服务器的 IP 地址和端口信息；

20 根据所述第二 IP 地址和所述第二端口信息，将所述 IP 地址和所述端口信息添加到所述目标服务器与所述下游服务器之间的第二防火墙的白名单内。

19、根据权利要求 15-18 中任一项所述的计算机可读存储介质，其中，所述处理器在实现根据所述开墙配置信息，对所述目标服务器进行开墙操作之后，还用于实现：

对所述目标服务器的关联服务器与所述目标服务器之间的通信链路进行开墙验证，得到开墙验证结果；

25 将所述开墙验证结果发送至所述终端设备，以供所述终端设备显示所述开墙验证结果。

20、根据权利要求 19 所述的计算机可读存储介质，其中，所述关联服务器包括目标服务器的上游服务器和下游服务器中的至少一项，所述处理器在实现所述目标服务器的关联服务器与所述目标服务器之间的通信链路进行开墙验证，得到开墙验证结果时，用于实现：

30 控制所述上游服务器，向所述目标服务器发送第一 telnet 命令；

在所述目标服务器执行所述第一 telnet 命令后，获取所述第一 telnet 命令对应的第一日志；

根据所述第一日志，确定所述上游服务器与所述目标服务器之间的第一开墙验证结果；

和/或

35 控制所述目标服务器，向所述下游服务器发送第二 telnet 命令；

在所述下游服务器执行所述第二 telnet 命令后，获取所述第二 telnet 命令对应的第二日志；

根据所述第二日志，确定所述下游服务器与所述目标服务器之间的第二开墙验证结果。

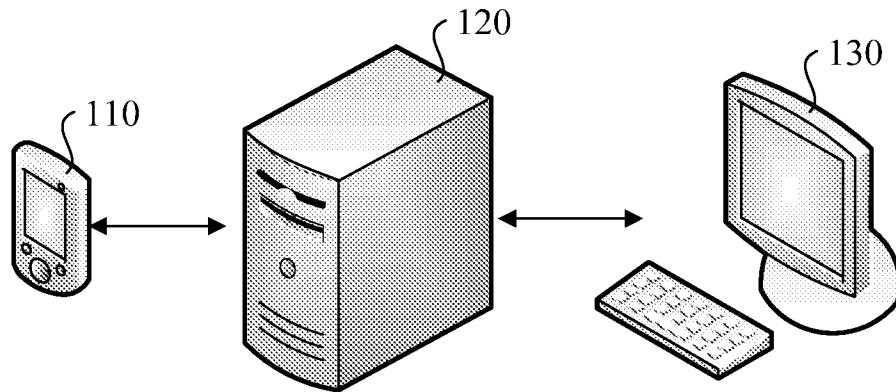


图 1

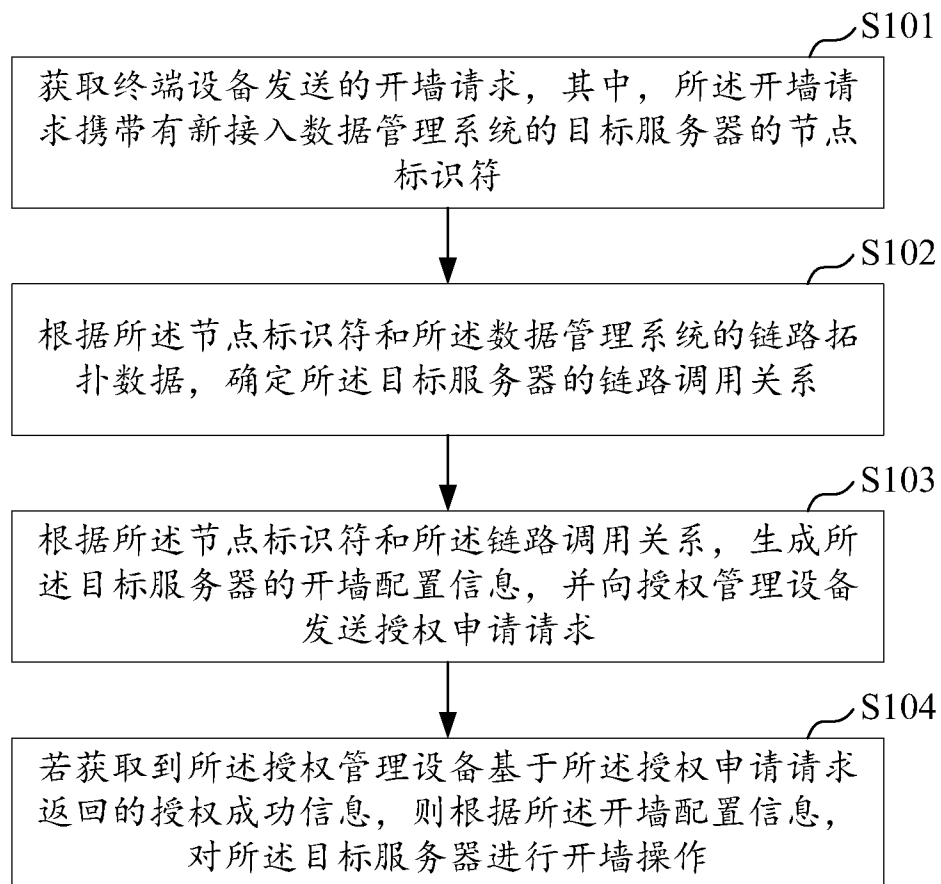


图 2

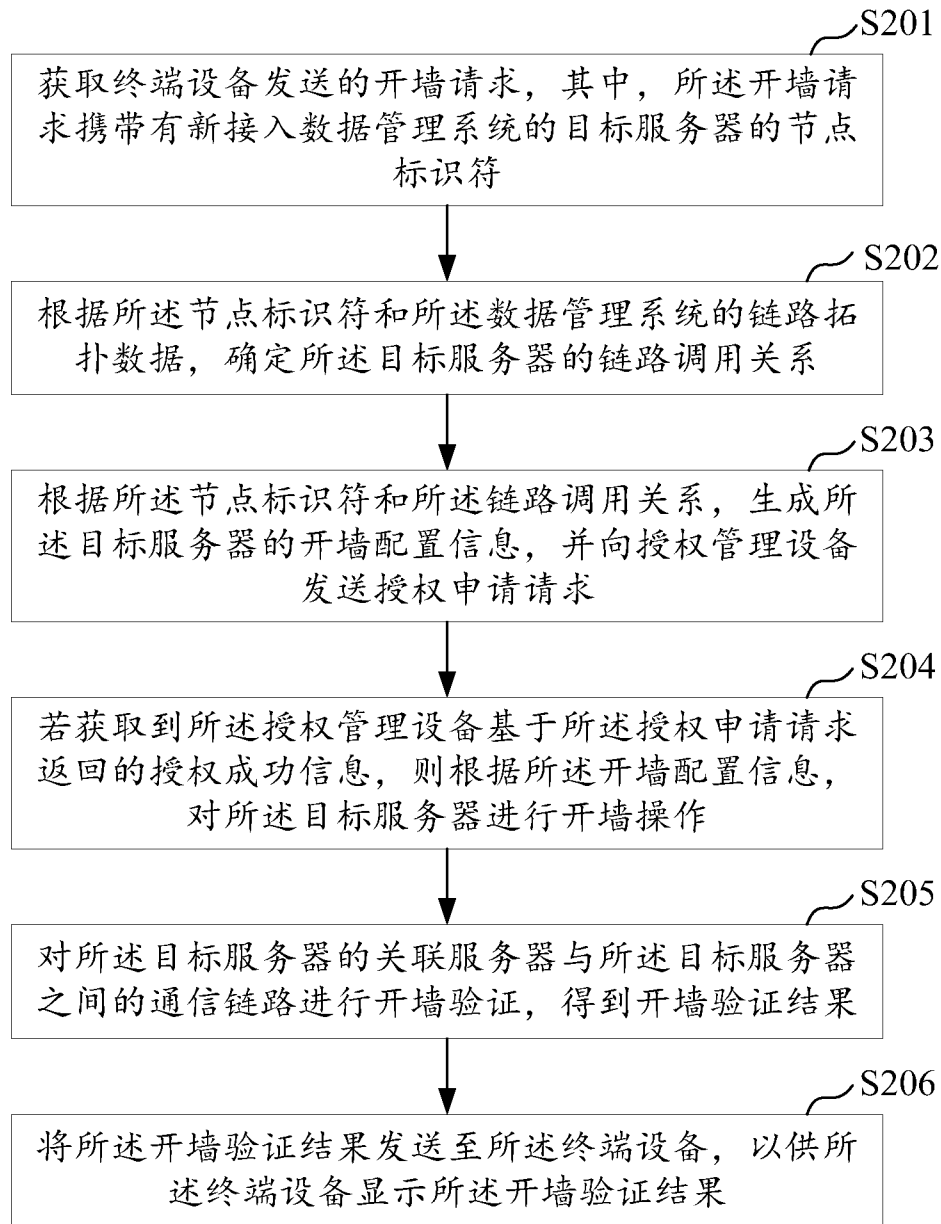


图 3

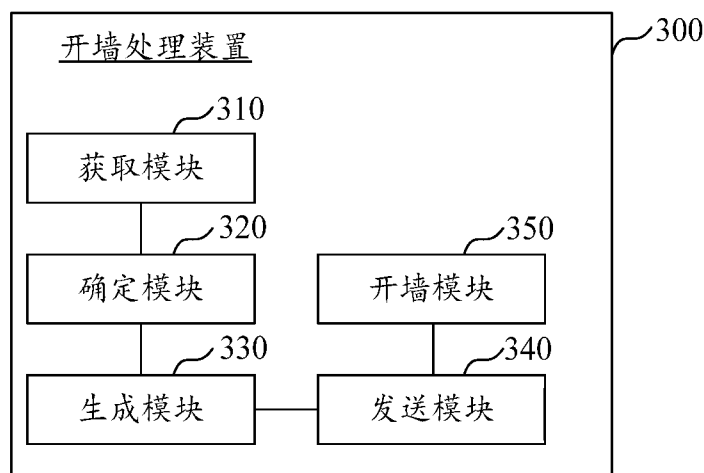


图 4

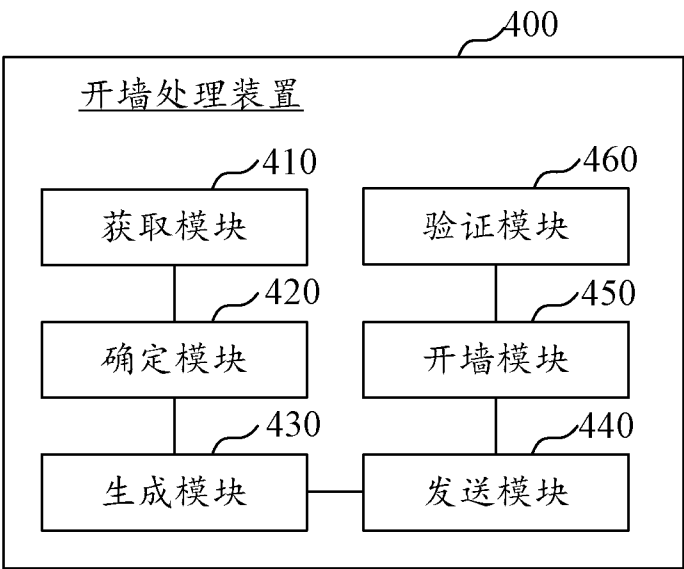


图 5

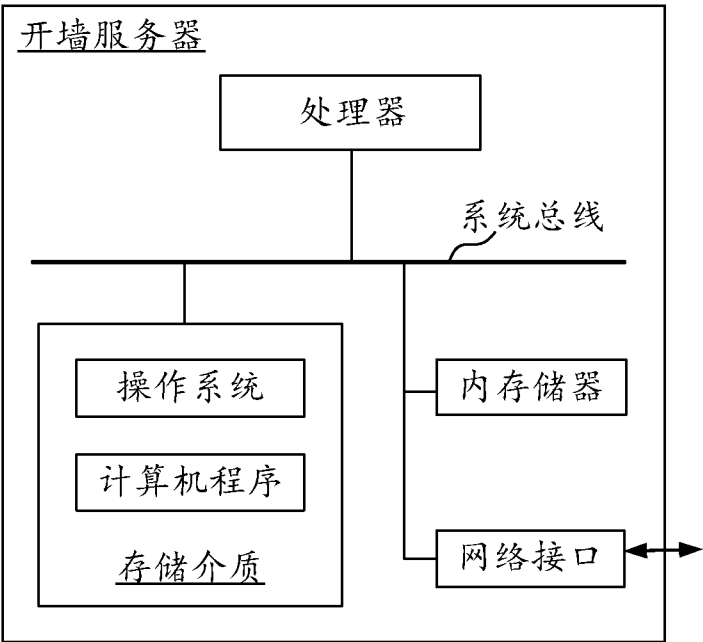


图 6

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2021/090762

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06(2006.01)i; H04L 12/24(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNABS; CNTXT; VEN; WOTXT; EPTXT; USTXT; CNKI: 开墙, 开启, 启动, 配置, 防火墙, 自动, 目标, 拓扑, 结构, 调用, 路径, 路由, 授权, 验证, start, firewall, configuration, auto, target, topology, structure, call, path, route, authorization, validate

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 112350868 A (PING AN TECHNOLOGY (SHENZHEN) CO., LTD.) 09 February 2021 (2021-02-09) claims 1-10	1-20
X	CN 111711635 A (PING AN BANK CO., LTD.) 25 September 2020 (2020-09-25) claims 1-10	1-20
A	CN 111586022 A (SHENZHEN ONECONNECT TECHNOLOGY CO., LTD.) 25 August 2020 (2020-08-25) entire document	1-20
A	CN 110677383 A (PING AN TECHNOLOGY (SHENZHEN) CO., LTD.) 10 January 2020 (2020-01-10) entire document	1-20
A	US 2008289026 A1 (MICROSOFT CORP.) 20 November 2008 (2008-11-20) 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

16 June 2021

Date of mailing of the international search report

30 June 2021

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/CN2021/090762

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	112350868	A	09 February 2021	None			
CN	111711635	A	25 September 2020	None			
CN	111586022	A	25 August 2020	None			
CN	110677383	A	10 January 2020	None			
US	2008289026	A1	20 November 2008	US	8266685	B2	11 September 2012

国际检索报告

国际申请号

PCT/CN2021/090762

A. 主题的分类

H04L 29/06 (2006.01) i; H04L 12/24 (2006.01) i

按照国际专利分类 (IPC) 或者同时按照国家分类和 IPC 两种分类

B. 检索领域

检索的最低限度文献 (标明分类系统和分类号)

H04L

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库 (数据库的名称, 和使用的检索词 (如使用))

CNABS; CNTXT; VEN; WOTXT; EPTXT; USTXT; CNKI; 开墙, 开启, 启动, 配置, 防火墙, 自动, 目标, 拓扑, 结构, 调用, 路径, 路由, 授权, 验证, start, firewall, configuration, auto, target, topology, structure, call, path, route, authorization, validate

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 112350868 A (平安科技深圳有限公司) 2021年 2月 9日 (2021 - 02 - 09) 权利要求1-10	1-20
X	CN 111711635 A (平安银行股份有限公司) 2020年 9月 25日 (2020 - 09 - 25) 权利要求1-10	1-20
A	CN 111586022 A (深圳壹账通智能科技有限公司) 2020年 8月 25日 (2020 - 08 - 25) 全文	1-20
A	CN 110677383 A (平安科技深圳有限公司) 2020年 1月 10日 (2020 - 01 - 10) 全文	1-20
A	US 2008289026 A1 (MICROSOFT CORP) 2008年 11月 20日 (2008 - 11 - 20) 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

2021年 6月 16日

国际检索报告邮寄日期

2021年 6月 30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

邓璐

电话号码 86-(010)-62089138

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2021/090762

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	112350868	A	2021年 2月 9日	无	
CN	111711635	A	2020年 9月 25日	无	
CN	111586022	A	2020年 8月 25日	无	
CN	110677383	A	2020年 1月 10日	无	
US	2008289026	A1	2008年 11月 20日	US 8266685 B2	2012年 9月 11日