(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
2023 年 11 月 2 日 (02.11.2023)

WIPO | PCT

(10) 国际公布号
WO 2023/207547 A1

(51) 国际专利分类号:
H04L 9/40 (2022.01) *H04L 69/16* (2022.01)
H04L 47/10 (2022.01)

(21) 国际申请号: PCT/CN2023/086761

(22) 国际申请日: 2023 年 4 月 7 日 (07.04.2023)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
202210468297.9 2022年4月29日 (29.04.2022) CN

(71) 申请人: 北京火山引擎科技有限公司 (**BEIJING VOLCANO ENGINE TECHNOLOGY CO., LTD.**) [CN/CN]; 中国北京市海淀区紫金数码园4号楼13层1309, Beijing 100190 (CN)。

(72) 发明人: 张晨 (**ZHANG, Chen**); 中国北京市朝阳区七圣中街12号院融中心B1小邮局, Beijing 100028 (CN)。罗辉 (**LUO, Hui**); 中国北京市朝阳区七圣中街12号院融中心B1小邮局, Beijing 100028 (CN)。郭建新 (**GUO, Jianxin**); 中国北京市朝阳区七圣中街12号院融中心B1小邮局, Beijing 100028 (CN)。

(74) 代理人: 北京信远达知识产权代理有限公司 (**SINOTALEN ATTORNEYS AT LAW**); 中国北京市大兴区北京经济技术开发区科创十三街18号院10号楼301室, Beijing 100176 (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,

(54) **Title:** TRAFFIC TRANSMISSION CONTROL METHOD AND APPARATUS, AND DEVICE AND STORAGE MEDIUM

(54) 发明名称: 一种流量传输控制方法、装置、设备及存储介质

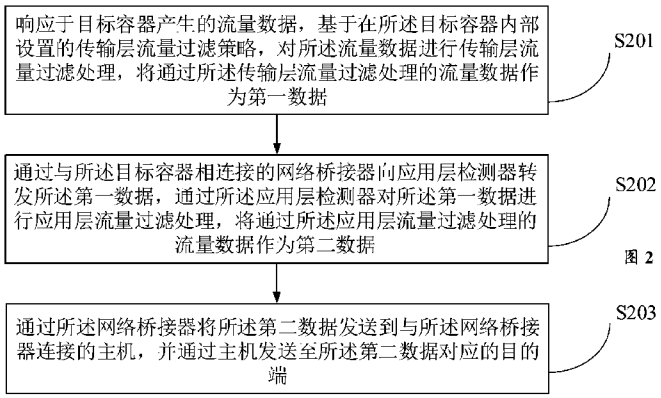

图 2

S201 In response to traffic data which is generated by a target container, perform transmission layer traffic filtering processing on the traffic data on the basis of a transmission layer traffic filtering strategy which is provided in the target container, and use, as first data, the traffic data which has been subjected to transmission layer traffic filtering processing

S202 Forward the first data to an application layer detector by means of a network bridge which is connected to the target container, perform application layer traffic filtering processing on the first data by means of the application layer detector, and use, as second data, the traffic data which has been subjected to application layer traffic filtering processing

S203 Send, by means of the network bridge, the second data to a host which is connected to the network bridge, and send, by means of the host, the second data to a destination end corresponding to the second data

(57) **Abstract:** Provided in the present disclosure are a traffic transmission control method and apparatus, and a device and a storage medium. A network bridge is configured between a target container and a host, and traffic data is forwarded to an application layer detector by means of the network bridge to perform application layer traffic filtering processing, so as to be compatible with target containers with various different service characteristics, thereby improving the stability of traffic transmission; and a transmission layer traffic filtering strategy is directly acted on in a container, and transmission layer traffic filtering processing is performed in the

WO 2023/207547 A1

[见续页]

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, 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))。

container, thereby avoiding the problem of a fault occurring in a container cluster due to an error or an anomaly of a network protection strategy, and realizing security detection and normal transmission of the traffic data in a container environment.

(57) 摘要: 本公开提供了一种流量传输控制方法、装置、设备及存储介质，通过在目标容器和主机之间配置网络桥接器，通过网络桥接器将流量数据转发到应用层检测器进行应用层流量过滤处理，可以兼容各种不同业务特性的目标容器，提升流量传输的稳定性；并且将传输层流量过滤策略直接作用于容器内部，在容器内部进行传输层流量过滤处理，防止由于网络防护策略的失误或异常导致容器集群出现故障问题，实现对容器环境下流量数据的安全检测和正常传输。

一种流量传输控制方法、装置、设备及存储介质

本公开要求于2022年04月29日提交中国专利局、申请号为202210468297.9、申请名称为“一种流量传输控制方法、装置、设备及存储介质”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

本公开涉及互联网技术领域，具体而言，涉及一种流量传输控制方法、装置、设备及存储介质。

背景技术

容器网络是一个开放的网络架构，一般的网络导流与阻断方案是使用容器网络接口（Container Network Interface，CNI）插件，CNI插件需要与容器网络匹配，才能获取流量数据并进行相应的安全扫描和网络策略阻断。这种控制方式主要是基于宿主机的网络的协议栈进行流量数据的过滤，达到网络隔离的目的，这种技术方案可以满足单一的容器网络环境的业务需求。

但是，随着容器技术的发展，出现了混合网络模式，很多容器的流量数据不再进入主机的协议栈，而是通过宿主机的物理网卡直接流向外部的虚拟交换机，如果仍然采用CNI插件，会由于无法获取到相关的流量数据而导致无效的安全扫描和网络策略阻断，进而可能出现无法对流量数据进行导流和传输的情况，影响流量数据传输的完整性，并且影响后续对流量数据进行流量检测的结果，降低容器环境的安全性和稳定性。

发明内容

本公开实施例至少提供一种流量传输控制方法、装置、设备及存储介质。

第一方面，本公开实施例提供了一种流量传输控制方法，所述方法包括：

响应于目标容器产生的流量数据，基于在所述目标容器内部设置的传输层流量过滤策略，对所述流量数据进行传输层流量过滤处理，将通过所述传输层流量过滤处理的流量数据作为第一数据；

通过与所述目标容器相连接的网络桥接器向应用层检测器转发所述第一数据，通过所述应用层检测器对所述第一数据进行应用层流量过滤处理，将通过所述应用层流量过滤处理的流量数据作为第二数据；

通过所述网络桥接器将所述第二数据发送到与所述网络桥接器连接的主机，并通过主机发送至所述第二数据对应的目的端。

一种可选的实施方式中，在基于在所述目标容器内部设置的传输层流量过滤策略，对所述流量数据进行传输层流量过滤处理之前，还包括：

获取网络策略器生成的与所述目标容器对应的传输层流量过滤策略，并将所述传输层流量过滤策略发送至所述网络桥接器；所述传输层流量过滤策略指示有符合传输要求的五元组信息和不符合传输要求的五元组信息；

通过所述网络桥接器将所述传输层流量过滤策略设置在所述目标容器的独立网络命名空间中；

所述基于在所述目标容器内部设置的传输层流量过滤策略，对所述流量数据进行传输层流量过滤处理，包括：

从所述独立网络命名空间中读取所述传输层流量过滤策略，基于所述流量数据携带的五元组信息，以及所述传输层流量过滤策略指示的符合传输要求的五元组信息和不符合传输要求的五元组信息，对所述流量数据进行传输层流量过滤处理。

一种可选的实施方式中，所述目标容器上设置有第一网络接口，所述主机上设置有第二网络接口；所述网络桥接器上设置有第三网络接口和第四网络接口；其中，所述第一网络接口和所述第三网络接口通信连接，所述第二网络接口和所述第四网络接口通信连接；

所述通过与所述目标容器相连接的网络桥接器向应用层检测器转发所述第一数据，包括：

通过与所述目标容器相连接的网络桥接器的第三网络接口接收所述目标容器的所述第一网络接口传输的所述第一数据，并调用所述网络桥接器的包转发功能将所述第一数据转发到应用层检测器；

所述通过所述网络桥接器将所述第二数据发送到与所述网络桥接器连接的主机，包括：

通过所述网络桥接器的所述第四网络接口将所述第二数据转发到与所述网络桥接器连接的主机的第二网络接口。

一种可选的实施方式中，通过所述应用层检测器对所述第一数据进行应用层流量过滤处理，包括：

通过所述应用层检测器从预先训练的流量过滤模型集中调用与所述目标容器关联的流量过滤模型；

基于调用的所述流量过滤模型，对所述第一数据进行应用层流量过滤处理。

第二方面，本公开实施例提供了一种流量传输控制方法，所述方法包括：

响应于主机接收的流量数据，通过与所述主机相连接的网络桥接器向应用层检测器转发所述流量数据，以通过所述应用层检测器对所述流量数据进行应用层流量过滤处理，将通过所述应用层流量过滤处理的流量数据作为第三数据；

通过所述网络桥接器将所述第三数据发送到与所述网络桥接器连接的目标容器，基于在所述目标容器内部设置的传输层流量过滤策略，对所述第三数据进行传输层流量过滤处理，将通过所述传输层流量过滤处理的流量数据作为第四数据；

在所述目标容器对所述第四数据进行处理。

一种可选的实施方式中，所述目标容器上设置有第一网络接口，所述主机上设置有第二网络接口；所述网络桥接器上设置有第三网络接口和第四网络接口；其中，所述第一网络接口和所述第三网络接口通信连接，所述第二网络接口和所述第四网络接口通信连接；

所述通过与所述主机相连接的网络桥接器向应用层检测器转发所述流量数据，包括：

通过与所述主机相连接的网络桥接器的第四网络接口接收所述主机的所述第二网络接口传输的所述流量数据，并调用所述网络桥接器的包转发功能将所述流量数据转发到应用层检测器；

所述通过所述网络桥接器将所述第三数据发送到与所述网络桥接器连接的目标容器，包括：

通过所述网络桥接器的所述第三网络接口将所述第三数据转发到与所述网络桥接器连接的目标容器的第一网络接口。

一种可选的实施方式中，通过所述应用层检测器对所述流量数据进行应用层流量过滤处理，包括：

通过所述应用层检测器从预先训练的流量过滤模型集中调用与所述目标容器关联的流量过滤模型；

基于调用的所述流量过滤模型，对所述流量数据进行应用层流量过滤处理。

一种可选的实施方式中，在基于在所述目标容器内部设置的传输层流量过滤策略，对所述第三数据进行传输层流量过滤处理之前，还包括：

获取网络策略器生成的与所述目标容器对应的传输层流量过滤策略，并将所述传输层流量过滤策略发送至所述网络桥接器；所述传输层流量过滤策略指示有符合传输要求的五元组信息和不符合传输要求的五元组信息；

通过所述网络桥接器将所述传输层流量过滤策略设置在所述目标容器的独立网络命名空间中；

所述基于在所述目标容器内部设置的传输层流量过滤策略，对所述第三数据进行传输层流量过滤处理，包括：

从所述独立网络命名空间中读取所述传输层流量过滤策略，基于所述第三数据携带的五元组信息，以及所述传输层流量过滤策略指示的符合传输要求的五元组信息和不符合传输要求的五元组信息，对所述第三数据进行传输层流量过滤处理。

第三方面，本公开实施例还提供一种流量传输控制装置，所述装置包括：

第一过滤模块，用于响应于目标容器产生的流量数据，基于在所述目标容器内部设置的传输层流量过滤策略，对所述流量数据进行传输层流量过滤处理，将通过所述传输层流量过滤处理的流量数据作为第一数据；

第二过滤模块，用于通过与所述目标容器相连接的网络桥接器向应用层检测器转发所述第一数据，通过所述应用层检测器对所述第一数据进行应用层流量过滤处理，将通过所述应用层流量过滤处理的流量数据作为第二数据；

第一处理模块，用于通过所述网络桥接器将所述第二数据发送到与所述网络桥接器连接的主机，并通过主机发送至所述第二数据对应的目的端。

第四方面，本公开实施例还提供一种流量传输控制装置，所述装置包括：

第三过滤模块，用于响应于主机接收的流量数据，通过与所述主机相连接的网络桥接器向应用层检测器转发所述流量数据，以通过所述应用层检测器对所述流量数据进行应用层流量过滤处理，将通过所述应用层流量过滤处理的流量数据作为第三数据；

第四过滤模块，用于通过所述网络桥接器将所述第三数据发送到与所述网络桥接器连接的目标容器，基于在所述目标容器内部设置的传输层流量过滤策略，对所述第三数据进行传输层流量过滤处理，将通过所述传输层流量过滤处理的流量数据作为第四数据；

第二处理模块，用于在所述目标容器对所述第四数据进行处理。

第五方面，本公开实施例还提供一种电子设备，包括：处理器、存储器和总线，所述存储器存储有所述处理器可执行的机器可读指令，当电子设备运行时，所述处理器与所述存储器之间通过总线通信，所述机器可读指令被所述处理器执行时执行上述第一方面，或第一方面中任一种可能的流量传输控制方法的步骤，或第二方面，或第二方面中任一种可

能的流量传输控制方法的步骤。

第六方面，本公开实施例还提供一种计算机可读存储介质，该计算机可读存储介质上存储有计算机程序，该计算机程序被处理器运行时执行上述第一方面，或第一方面中任一种可能的流量传输控制方法的步骤，或第二方面，或第二方面中任一种可能的流量传输控制方法的步骤。

关于上述的流量传输控制装置、电子设备、及计算机可读存储介质的效果描述参见上述流量传输控制方法的说明，这里不再赘述。

本公开实施例中，在流量数据从容器流出的场景下，将传输层流量过滤策略直接作用于容器内部，以对容器产生的流量数据在容器内部直接进行传输层流量过滤处理，可以降低对容器集群的影响，防止由于网络防护策略的失误或异常导致容器集群出现故障问题；另外，通过将网络桥接器配置在目标容器和主机之间，目标容器可以将通过传输层流量过滤处理的流量数据通过网络桥接器转发到应用层检测器进行应用层流量过滤处理后，将通过应用层流量过滤处理的流量数据发送到主机，由于网络桥接器可以兼容各种不同业务特性的容器的流量数据传输，具备良好的适应性、通用性、和鲁棒性，从而可以保障流量传输的稳定性和完整性，进而实现对容器环境下流量数据的安全检测和正常传输。

相应地，在流量数据流入容器的场景下，主机在接收到流量数据后，通过配置在主机与容器之间的网络桥接器将流量数据转发到应用层检测器进行应用层流量过滤处理，再将通过应用层流量过滤处理的流量数据转发到容器，通过容器内部设置的传输层流量过滤策略直接进行传输层流量过滤处理；一方面，通过在容器内部进行传输层流量过滤处理的机制，可以降低对容器集群的影响，防止由于网络防护策略的失误或异常导致容器集群出现故障问题；另一方面，由于配置在主机和容器之间的网络桥接器可以兼容各种不同业务特性的容器的流量数据传输，具备良好的适应性、通用性、和鲁棒性，从而可以保障流量传输的稳定性和完整性，进而实现对容器环境下流量数据的安全检测和正常传输。

为使本公开的上述目的、特征和优点能更明显易懂，下文特举较佳实施例，并配合所附附图，作详细说明如下。

附图说明

为了更清楚地说明本公开实施例的技术方案，下面将对实施例中所需要使用的附图作简单地介绍，此处的附图被并入说明书中并构成本说明书中的一部分，这些附图示出了符合本公开的实施例，并与说明书一起用于说明本公开的技术方案。应当理解，以下附图仅示出了本公开的某些实施例，因此不应被看作是对范围的限定，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相关的附图。

图 1 示出了本公开实施例所提供的一种应用场景示意图；

图 2 示出了本公开实施例所提供的一种流量传输控制方法的流程图；

图 3 示出了本公开实施例所提供的一种网络接口示意图；

图 4 示出了本公开实施例所提供的一种包转发过程示意图；

图 5 示出了本公开实施例所提供的又一种流量传输控制方法的流程图；

图 6 示出了本公开实施例所提供的另一种流量传输控制方法的流程图；

图 7 示出了本公开实施例所提供的又一种流量传输控制方法的流程图；

图 8 示出了本公开实施例所提供的一种流量传输控制装置的示意图之一；

图 9 示出了本公开实施例所提供的一种流量传输控制装置的示意图之二；

图 10 示出了本公开实施例所提供的另一种流量传输控制装置的示意图之一；

图 11 示出了本公开实施例所提供的另一种流量传输控制装置的示意图之二；

图 12 示出了本公开实施例所提供的一种电子设备的示意图。

具体实施方式

为使本公开实施例的目的、技术方案和优点更加清楚，下面将结合本公开实施例中附图，对本公开实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本公开一部分实施例，而不是全部的实施例。通常在此处附图中描述和示出的本公开实施例的组件可以以各种不同的配置来布置和设计。因此，以下对在附图中提供的本公开的实施例的详细描述并非旨在限制要求保护的本公开的范围，而是仅仅表示本公开的选定实施例。基于本公开的实施例，本领域技术人员在没有做出创造性劳动的前提下所获得的所有其他实施例，都属于本公开保护的范围。

应注意到：相似的标号和字母在下面的附图中表示类似项，因此，一旦某一项在一个附图中被定义，则在随后的附图中不需要对其进行进一步定义和解释。

本文中术语“和/或”，仅仅是描述一种关联关系，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，本文中术语“至少一种”表示多种中的任意一种或多种中的至少两种的任意组合，例如，包括 A、B、C 中的至少一种，可以表示包括从 A、B 和 C 构成的集合中选择的任意一个或多个元素。

经研究发现，一般的网络导流与阻断方案是使用容器网络接口（Container Network Interface，CNI）插件，即使用与容器网络匹配的 CNI 插件获取流量数据并进行相应的安全扫描和网络策略阻断，然而这无法适配容器环境中混合网络模式下的流量阻断与引流需求，并且 CNI 插件离容器较远，传输的流量数据存在完整性缺失的风险，导致获取到的流量数据失真，进而影响后续流量检测的结果，难以保证流量数据传输的完整性，影响容器环境的安全性和稳定性。

基于上述研究，本公开提供了一种流量传输控制方法，通过在目标容器和主机之间配置网络桥接器，通过网络桥接器将流量数据转发到应用层检测器进行应用层流量过滤处理，可以兼容各种不同业务特性的目标容器，提升流量传输的稳定性；并且将传输层流量过滤策略直接作用于容器内部，在容器内部进行传输层流量过滤处理，防止由于网络防护策略的失误或异常导致容器集群出现故障问题，实现对容器环境下流量数据的安全检测和正常传输。

为便于对本实施例进行理解，首先对本公开实施例所公开的一种流量传输控制方法进行详细介绍，本公开实施例所提供的流量传输控制方法的执行主体一般为具有一定计算能力的计算机设备，该计算机设备例如包括：终端设备或服务器或其它处理设备。在一些可能的实现方式中，该流量传输控制方法可以通过处理器调用存储器中存储的计算机可读指令的方式来实现。

下面对本公开实施例提供的流量传输控制方法加以说明。

请参阅图 1，图 1 为本公开实施例提供的一种应用场景示意图。如图 1 中所示，为了

对从目标容器传输至主机的流量数据、以及从主机传输至目标容器的流量数据进行流量的过滤处理和传输控制，可以利用网络桥接器，将网络桥接器配置在目标容器和主机之间，以通过网络桥接器进行目标容器和主机之间的数据传输，进而还可以利用网络桥接器的包转发功能将流量数据转发到应用层检测器进行应用层流量过滤处理，从而提升流量传输的稳定性，保障容器环境下流量传输的正常进行。

请参阅图 2，图 2 为本公开实施例提供的一种流量传输控制方法的流程图，该流量传输控制方法可以认为由网络流量管控器执行，该网络流量管控器可以部署在一个独立的计算机设备上或本公开实施例进行网络流量处理的主机上。如图 2 中所示，本公开实施例提供的流量传输控制方法包括步骤 S201~S203，其中：

S201：响应于目标容器产生的流量数据，基于在所述目标容器内部设置的传输层流量过滤策略，对所述流量数据进行传输层流量过滤处理，将通过所述传输层流量过滤处理的流量数据作为第一数据。

这里，流量数据是目标容器基于网络传输协议生成的、待发送给其他容器或主机的数据。该步骤中，在检测到目标容器产生的流量数据后，根据在目标容器内部设置的流量过滤策略，对所述流量数据进行传输层流量过滤处理，针对未通过所述传输层流量过滤处理的流量数据，对其进行拦截，针对通过所述传输层流量过滤处理的流量数据，将其确定为第一数据，对其进行放行。

其中，所述传输层流量过滤处理为四层流量过滤处理，四层流量过滤处理是指在开放式系统互联通信参考模型（Open System Interconnection Reference Model，OSI）的第四层传输层，基于五元组信息进行流量数据的过滤与防护。

这里，五元组信息包括源互联网协议（Internet Protocol Address，IP）地址、源端口、目的 IP 地址、目的端口和传输层协议。

可以理解，传输层流量过滤处理即为获取流量数据携带的五元组信息，并获取传输层流量过滤策略指示的符合传输要求的五元组信息和不符合传输要求的五元组信息，以检测该流量数据的五元组信息是否符合传输层流量过滤策略指示的传输要求。

这里，为了能够在目标容器内部对所述流量数据进行传输层流量过滤处理，需要预先在目标容器内部设置相应的传输层流量过滤策略。

相应地，在一些可能的实施方式中，在基于在所述目标容器内部设置的传输层流量过滤策略，对所述流量数据进行传输层流量过滤处理之前，还包括：

获取网络策略器生成的与所述目标容器对应的传输层流量过滤策略，并将所述传输层流量过滤策略发送至所述网络桥接器；所述传输层流量过滤策略指示有符合传输要求的五元组信息和不符合传输要求的五元组信息；

通过所述网络桥接器将所述传输层流量过滤策略设置在所述目标容器的独立网络命名空间中。

该步骤中，可以获取网络策略器生成的传输层流量过滤策略，这里，所述传输层流量过滤策略与所述目标容器对应，以便在后续按照所述传输层流量过滤策略对目标容器产生的流量数据进行传输层流量过滤处理，在获取到所述传输层流量过滤策略的情况下，可以将所述传输层流量过滤策略发送至所述网络桥接器，并通过所述网络桥接器将所述传输层

流量过滤策略设置在所述目标容器的独立网络命名空间中。

可选地，所述传输层流量过滤策略可以是基于安全传输设定的网络访问接口规则生成的，所述传输层流量过滤策略指示目标容器可以访问的情况和不可以访问的情况，即指示符合传输要求的五元组信息和不符合传输要求的五元组信息。示例性的，针对目标容器 A 生成的、访问容器 B 的流量数据，传输层流量传输策略表征容器 A 不能访问容器 B 的 3306 端口，则容器 A 访问容器 B 的 3306 端口的访问过程对应的五元组信息即为传输层流量传输策略指示的不符合传输要求的五元组信息。

在将传输层流量过滤策略设置在所述目标容器的独立网络命名空间中后，就可以从所述独立网络命名空间中读取所述传输层流量过滤策略，按照所述传输层流量过滤策略对所述流量数据进行传输层流量过滤处理。

因此，在一些可能的实施方式中，所述基于在所述目标容器内部设置的传输层流量过滤策略，对所述流量数据进行传输层流量过滤处理，包括：

从所述独立网络命名空间中读取所述传输层流量过滤策略，基于所述流量数据携带的五元组信息，以及所述传输层流量过滤策略指示的符合传输要求的五元组信息和不符合传输要求的五元组信息，对所述流量数据进行传输层流量过滤处理。

可以理解，若所述流量数据携带的五元组信息与所述传输层流量过滤策略指示的符合传输要求的五元组信息匹配，可以确定所述流量数据通过传输层流量过滤处理，从而对所述流量数据进行放行；相反的，若所述流量数据携带的五元组信息与所述传输层流量过滤策略指示的不符合传输要求的五元组信息匹配，可以确定所述流量数据未通过传输层流量过滤处理，从而对所述流量数据进行拦截和过滤。

S202：通过与所述目标容器相连接的网络桥接器向应用层检测器转发所述第一数据，通过所述应用层检测器对所述第一数据进行应用层流量过滤处理，将通过所述应用层流量过滤处理的流量数据作为第二数据。

该步骤中，针对通过所述传输层流量过滤处理的第一数据，可以将所述第一数据从目标容器传输至网络桥接器，再通过网络桥接器转发到应用层检测器，以通过所述应用层检测器对所述第一数据进行应用层流量过滤处理，针对未通过所述应用层流量过滤处理的第一数据，对其进行拦截，针对通过所述应用层流量过滤处理的第一数据，将其确定为第二数据，对其进行放行。

其中，流量数据在虚拟网络设备之间的传输需要利用网络接口，网络接口均为成对出现，网络接口的一端连接着各自对应的虚拟网络设备，另一端彼此相连。

进而，在一些可能的实施方式中，所述目标容器上设置有第一网络接口，所述主机上设置有第二网络接口；所述网络桥接器上设置有第三网络接口和第四网络接口；其中，所述第一网络接口和所述第三网络接口通信连接，所述第二网络接口和所述第四网络接口通信连接。

请同时参阅图 3，图 3 为本公开实施例提供的一种网络接口示意图。如图 3 中所示，传统模式是生成一对网络接口，一个网络接口设置在目标容器上，另一个网络接口设置在主机上，如图 3 中所示即为目标容器上设置有第一网络接口，主机上设置有第二网络接口，第一网络接口和第二网络接口通信连接，目标容器产生的流量数据通过第一网络接口发送

到主机的第二网络接口。

而在本实施例中，在目标容器上设置有第一网络接口，主机上设置有第二网络接口的基础上，加入网络桥接器，网络桥接器上设置有第三网络接口和第四网络接口，第一网络接口和第三网络接口通信连接，第二网络接口和第四网络接口通信连接，从而使得目标容器产生的流量数据可以通过网络桥接器发送到主机。

相应地，在一些可能的实施方式中，所述通过与所述目标容器相连接的网络桥接器向应用层检测器转发所述第一数据，包括：

通过与所述目标容器相连接的网络桥接器的第三网络接口接收所述目标容器的所述第一网络接口传输的所述第一数据，并调用所述网络桥接器的包转发功能将所述第一数据转发到应用层检测器。

该步骤中，由于所述第一网络接口和所述第三网络接口通信连接，因此可以通过所述网络桥接器的第三网络接口接收所述目标容器的所述第一网络接口传输的所述第一数据，以将所述第一数据从目标容器传输至网络桥接器，进而调用所述网络桥接器的包转发功能将所述第一数据转发到应用层检测器，以通过所述应用层检测器对所述第一数据进行应用层流量过滤处理。

这里，所述应用层流量过滤处理为七层流量过滤处理，七层流量过滤处理是指在开放式系统互联通信参考模型（Open System Interconnection Reference Model，OSI）的第七层应用层，根据应用层的业务规则进行流量数据的识别与过滤。

具体的，在一些可能的实施方式中，通过所述应用层检测器对所述第一数据进行应用层流量过滤处理，包括：

通过所述应用层检测器从预先训练的流量过滤模型集中调用与所述目标容器关联的流量过滤模型；

基于调用的所述流量过滤模型，对所述第一数据进行应用层流量过滤处理。

针对预先训练的流量过滤模型集，所述流量过滤模型集中包括多个流量过滤模型，每个流量过滤模型存储有与其对应的业务容器，因此可以通过所述应用层检测器从流量过滤模型集中调用与所述目标容器关联的流量过滤模型，从而基于调用的所述流量过滤模型，对所述第一数据进行应用层流量过滤处理。

这里，基于所述网络桥接器的包转发功能，可以实现内核态和用户态之间的转换。

具体的，可以使用一种内存映射文件的方法（mmap），mmap 机制是一种双工通信机制，可用于操作内核态与用户态通信进程之间的数据传递共享，即双方都读写同一块内存空间的数据来完成通信。

请同时参阅图 4，图 4 为本公开实施例提供的一种包转发过程示意图。如图 4 中所示，传统模式是将网络策略器生成的传输层流量过滤策略（即为图中的四层过滤策略）直接发送到目标容器的宿主机上，通过宿主机的协议栈进行传输层流量过滤处理。而在本实施例中是将传输层流量过滤策略直接作用于目标容器内部，以对流量数据进行传输层流量过滤处理，从而降低对容器集群的影响，防止由于网络防护策略的失误或异常导致容器集群出现故障问题，同时还可以利用网络桥接器的包转发功能将流量数据转发到应用层检测器进行应用层流量过滤处理，如图 4 中所示即为将七层防护策略作用于用户态过滤引擎，以对

流量数据进行应用层流量过滤处理，网络桥接器可以兼容各种不同业务特性的目标容器，从而提升流量传输的稳定性，提高接收到的流量数据的完整性，实现对容器环境下流量数据的安全检测和正常传输。

具体的，通过所述网络桥接器的第三网络接口接收所述目标容器的所述第一网络接口传输的所述第一数据，此时所述第一数据处于内核态进程，此时可以基于 mmap 机制，将所述第一数据传递给用户态进程，在用户态进程进行应用层流量过滤处理，并生成检测结果信息，这里，所述检测结果信息并不包括数据信息，而是包括对于该第一数据是否通过应用层流量过滤处理的判定结果，此时可以基于 mmap 机制，将所述检测结果信息传递给内核态进程，在内核态进程做数据拦截或放行的处理，若该流量数据未通过应用层流量过滤处理，通过内核态过滤引擎将该流量数据过滤掉，即进行数据拦截处理，相反的，若该流量数据通过应用层流量过滤处理，进行数据放行处理。

S203：通过所述网络桥接器将所述第二数据发送到与所述网络桥接器连接的主机，并通过主机发送至所述第二数据对应的目的端。

该步骤中，在得到通过所述应用层流量过滤处理的第二数据后，可以同样利用网络接口，通过所述网络桥接器将所述第二数据发送到主机，这里，所述第二数据携带有发送的网络链路，通过主机按照所述第二数据携带的网络链路发送至所述第二数据对应的目的端。

通过上文内容可知，所述第二网络接口和所述第四网络接口通信连接，因此，在一些可能的实施方式中，所述通过所述网络桥接器将所述第二数据发送到与所述网络桥接器连接的主机，包括：

通过所述网络桥接器的所述第四网络接口将所述第二数据转发到与所述网络桥接器连接的主机的第二网络接口。

该步骤中，由于所述第二网络接口和所述第四网络接口通信连接，因此可以通过所述网络桥接器的所述第四网络接口将所述第二数据转发到所述主机的第二网络接口，以将通过所述应用层流量过滤处理的第二数据从网络桥接器传输至主机。

请参阅图 5，图 5 为本公开实施例提供的又一种流量传输控制方法的流程图。如图 5 中所示，在流量数据从容器流出的场景下，针对目标容器产生的流量数据，先根据在目标容器内部设置的传输层流量过滤策略，对流量数据进行传输层流量过滤处理，得到通过传输层流量过滤处理的第一数据，对第一数据进行放行，对未通过传输层流量过滤处理的流量数据进行拦截和过滤，然后将第一数据通过网络桥接器转发到应用层检测器进行应用层流量过滤处理，得到通过应用层流量过滤处理的第二数据，对第二数据进行放行，对未通过应用层流量过滤处理的第一数据进行拦截和过滤，进而将第二数据通过网络桥接器发送到主机，并通过主机发送至第二数据对应的目的端。

本公开实施例提供的流量传输控制方法，可以响应于目标容器产生的流量数据，基于在所述目标容器内部设置的传输层流量过滤策略，对所述流量数据进行传输层流量过滤处理，将通过所述传输层流量过滤处理的流量数据作为第一数据；通过与所述目标容器相连接的网络桥接器向应用层检测器转发所述第一数据，通过所述应用层检测器对所述第一数据进行应用层流量过滤处理，将通过所述应用层流量过滤处理的流量数据作为第二数据；通过所述网络桥接器将所述第二数据发送到与所述网络桥接器连接的主机，并通过主机发

送至所述第二数据对应的目的端。

这样，在流量数据从容器流出的场景下，将传输层流量过滤策略直接作用于容器内部，以对容器产生的流量数据在容器内部直接进行传输层流量过滤处理，可以降低对容器集群的影响，防止由于网络防护策略的失误或异常导致容器集群出现故障问题；另外，通过将网络桥接器配置在目标容器和主机之间，目标容器可以将通过传输层流量过滤处理的流量数据通过网络桥接器转发到应用层检测器进行应用层流量流量过滤处理后，将通过应用层流量过滤处理的流量数据发送到主机，由于网络桥接器可以兼容各种不同业务特性的容器的流量数据传输，具备良好的适应性、通用性、和鲁棒性，从而可以保障流量传输的稳定性和完整性，进而实现对容器环境下流量数据的安全检测和正常传输。

请参阅图 6，图 6 为本公开实施例提供的另一种流量传输控制方法的流程图，该流量传输控制方法可以认为由网络流量管控器执行，该网络流量管控器可以部署在一个独立的计算机设备上或本公开实施例进行网络流量处理的主机上。如图 6 中所示，本公开实施例提供的流量传输控制方法包括步骤 S601~S603，其中：

S601：响应于主机接收的流量数据，通过与所述主机相连接的网络桥接器向应用层检测器转发所述流量数据，以通过所述应用层检测器对所述流量数据进行应用层流量过滤处理，将通过所述应用层流量过滤处理的流量数据作为第三数据。

这里，所述流量数据表征主机接收到的、基于网络传输协议生成的、待发送给容器的流量数据。该步骤中，在检测到主机接收到流量数据后，对所述流量数据进行应用层流量过滤处理，具体的，先将流量数据从主机传输至网络桥接器，再通过网络桥接器将所述流量数据转发到应用层检测器以进行应用层流量过滤处理。

其中，所述应用层流量过滤处理为七层流量过滤处理，七层流量过滤处理是指在开放式系统互联通信参考模型（Open System Interconnection Reference Model，OSI）的第七层应用层，根据应用层的业务规则进行流量数据的识别与过滤。

可以理解，所述应用层流量过滤处理为根据应用层的业务规则，检测所述流量数据携带的业务信息是否符合传输要求，这里，所述流量数据携带的业务信息可以包括统一资源定位符（Uniform Resource Locator，URL）地址、请求体（Body）参数信息等。

这里，通过上文内容可知，流量数据在虚拟网络设备之间的传输需要利用网络接口，网络接口均为成对出现，网络接口的一端连接着各自对应的虚拟网络设备，另一端彼此相连。

进而，在一些可能的实施方式中，所述目标容器上设置有第一网络接口，所述主机上设置有第二网络接口；所述网络桥接器上设置有第三网络接口和第四网络接口；其中，所述第一网络接口和所述第三网络接口通信连接，所述第二网络接口和所述第四网络接口通信连接。

具体可参见图 3，图 3 为本公开实施例提供的一种网络接口示意图。如图 3 中所示，传统模式是生成一对网络接口，一个网络接口设置在目标容器上，另一个网络接口设置在主机上，如图中所示即为目标容器上设置有第一网络接口，主机上设置有第二网络接口，第一网络接口和第二网络接口通信连接，主机接收到的流量数据通过第二网络接口发送到目标容器的第一网络接口。

而在本实施例中，在目标容器上设置有第一网络接口，主机上设置有第二网络接口的基础上，加入网络桥接器，网络桥接器上设置有第三网络接口和第四网络接口，第一网络接口和第三网络接口通信连接，第二网络接口和第四网络接口通信连接，从而使得主机接收到的流量数据可以通过网络桥接器发送到目标容器。

相应地，在一些可能的实施方式中，所述通过与所述主机相连接的网络桥接器向应用层检测器转发所述流量数据，包括：

通过与所述主机相连接的网络桥接器的第四网络接口接收所述主机的所述第二网络接口传输的所述流量数据，并调用所述网络桥接器的包转发功能将所述流量数据转发到应用层检测器。

该步骤中，由于所述第二网络接口和所述第四网络接口通信连接，因此可以通过所述网络桥接器的所述第四网络接口接收所述主机的所述第二网络接口传输的所述流量数据，以将所述流量数据从主机传输至网络桥接器，在所述网络桥接器接收到所述流量数据的情况下，可以调用所述网络桥接器的包转发功能将所述流量数据转发到应用层检测器，以通过所述应用层检测器对所述流量数据进行应用层流量过滤处理。

具体的，在一些可能的实施方式中，通过所述应用层检测器对所述流量数据进行应用层流量过滤处理，包括：

通过所述应用层检测器从预先训练的流量过滤模型集中调用与所述目标容器关联的流量过滤模型；

基于调用的所述流量过滤模型，对所述流量数据进行应用层流量过滤处理。

针对预先训练的流量过滤模型集，所述流量过滤模型集中包括多个流量过滤模型，每个流量过滤模型存储有与其对应的业务容器，因此可以通过所述应用层检测器从流量过滤模型集中调用与所述目标容器关联的流量过滤模型，从而基于调用的所述流量过滤模型，对所述流量数据进行应用层流量过滤处理。

这里，基于所述网络桥接器的包转发功能，可以实现内核态和用户态之间的转换。

具体的，可以使用一种内存映射文件的方法（mmap），mmap 机制是一种双工通信机制，可用于操作内核态与用户态通信进程之间的数据传递共享，即双方都读写同一块内存空间的数据来完成通信。

具体可参见图 4，图 4 为本公开实施例提供的一种包转发过程示意图。如图 4 中所示，传统模式是将网络策略器生成的传输层流量过滤策略（即为图中的四层过滤策略）直接发送到目标容器的宿主机上，通过宿主机的协议栈进行传输层流量过滤处理。而在本实施例中是将传输层流量过滤策略直接作用于目标容器内部，以对流量数据进行传输层流量过滤处理，从而降低对容器集群的影响，防止由于网络防护策略的失误或异常导致容器集群出现故障问题，同时还可以利用网络桥接器的包转发功能将流量数据转发到应用层检测器进行应用层流量过滤处理，如图 4 中所示即为将七层防护策略作用于用户态过滤引擎，以对流量数据进行应用层流量过滤处理，网络桥接器可以兼容各种不同业务特性的目标容器，从而提升流量传输的稳定性，提高接收到的流量数据的完整性，实现对容器环境下流量数据的安全检测和正常传输。

具体的，通过所述网络桥接器的第四网络接口接收所述主机的所述第二网络接口传输

的流量数据，此时流量数据处于内核态进程，可以基于 mmap 机制，将流量数据传递给用户态进程，在用户态进程进行应用层流量过滤处理，并生成检测结果信息，这里，所述检测结果信息并不包括数据信息，而是包括对于该流量数据是否通过应用层流量过滤处理的判定结果，此时可以基于 mmap 机制，将所述检测结果信息传递给内核态进程，在内核态进程做数据拦截或放行的处理，若该流量数据未通过应用层流量过滤处理，通过内核态过滤引擎将该流量数据过滤掉，即进行数据拦截处理，相反的，若该流量数据通过应用层流量过滤处理，进行数据放行处理。

S602：通过所述网络桥接器将所述第三数据发送到与所述网络桥接器连接的目标容器，基于在所述目标容器内部设置的传输层流量过滤策略，对所述第三数据进行传输层流量过滤处理，将通过所述传输层流量过滤处理的流量数据作为第四数据。

该步骤中，在得到通过应用层流量过滤处理的第三数据后，可以同样利用网络接口，通过所述网络桥接器将所述第三数据发送到目标容器，从而根据在所述目标容器内部设置的传输层流量过滤策略，对所述第三数据进行传输层流量过滤处理，针对未通过所述传输层流量过滤处理的第三数据，对其进行拦截，针对通过所述传输层流量过滤处理的第三数据，将其确定为第四数据，对其进行放行。

其中，所述传输层流量过滤处理为四层流量过滤处理，四层流量过滤处理是指在开放式系统互联通信参考模型（Open System Interconnection Reference Model，OSI）的第四层传输层，基于五元组信息进行流量数据的过滤与防护。

这里，五元组信息包括源互联网协议（Internet Protocol Address，IP）地址、源端口、目的 IP 地址、目的端口和传输层协议。

可以理解，传输层流量过滤处理即为获取第三数据携带的五元组信息，并获取传输层流量过滤策略指示的符合传输要求的五元组信息和不符合传输要求的五元组信息，以检测该第三数据的五元组信息是否符合传输层流量过滤策略指示的传输要求。

通过上文内容可知，所述第一网络接口和所述第三网络接口通信连接，因此，在一些可能的实施方式中，所述通过所述网络桥接器将所述第三数据发送到与所述网络桥接器连接的目标容器，包括：

通过所述网络桥接器的所述第三网络接口将所述第三数据转发到与所述网络桥接器连接的目标容器的第一网络接口。

该步骤中，由于所述第一网络接口和所述第三网络接口通信连接，因此可以通过所述网络桥接器的所述第三网络接口，将所述第三数据转发到所述目标容器的第一网络接口，进而基于在所述目标容器内部设置的传输层流量过滤策略，对所述第三数据进行传输层流量过滤处理。

可以理解，为了能够在目标容器内部对所述第三数据进行传输层流量过滤处理，需要预先在目标容器内部设置相应的传输层流量过滤策略。

相应地，在一些可能的实施方式中，在基于在所述目标容器内部设置的传输层流量过滤策略，对所述第三数据进行传输层流量过滤处理之前，还包括：

获取网络策略器生成的与所述目标容器对应的传输层流量过滤策略，并将所述传输层流量过滤策略发送至所述网络桥接器；所述传输层流量过滤策略指示有符合传输要求的五

元组信息和不符合传输要求的五元组信息；

通过所述网络桥接器将所述传输层流量过滤策略设置在所述目标容器的独立网络命名空间中。

该步骤中，可以获取网络策略器生成的传输层流量过滤策略，这里，所述传输层流量过滤策略与所述目标容器对应，以便在后续按照所述传输层流量过滤策略对目标容器接收的流量数据进行传输层流量过滤处理，在获取到所述传输层流量过滤策略的情况下，可以将所述传输层流量过滤策略发送至所述网络桥接器，并通过所述网络桥接器将所述传输层流量过滤策略设置在所述目标容器的独立网络命名空间中。

在将传输层流量过滤策略设置在所述目标容器的独立网络命名空间中后，就可以从所述独立网络命名空间中读取所述传输层流量过滤策略，按照所述传输层流量过滤策略对所述流量数据进行传输层流量过滤处理。

因此，在一些可能的实施方式中，所述基于在所述目标容器内部设置的传输层流量过滤策略，对所述第三数据进行传输层流量过滤处理，包括：

从所述独立网络命名空间中读取所述传输层流量过滤策略，基于所述第三数据携带的五元组信息，以及所述传输层流量过滤策略指示的符合传输要求的五元组信息和不符合传输要求的五元组信息，对所述第三数据进行传输层流量过滤处理。

可以理解，若所述第三数据携带的五元组信息与所述传输层流量过滤策略指示的符合传输要求的五元组信息匹配，可以确定所述第三数据通过传输层流量过滤处理，从而对所述第三数据进行放行；相反的，若所述第三数据携带的五元组信息与所述传输层流量过滤策略指示的不符合传输要求的五元组信息匹配，可以确定所述第三数据未通过传输层流量过滤处理，从而对所述第三数据进行拦截和过滤。

S603：在所述目标容器对所述第四数据进行处理。

该步骤中，在确定通过所述传输层流量过滤处理的第四数据后，可以在目标容器相应的服务进程中，对目标容器接收到的所述第四数据进行处理。

请参阅图 7，图 7 为本公开实施例提供的又一种流量传输控制方法的流程图。如图 7 中所示，在流量数据流入容器的场景下，针对主机接收到的流量数据，先将流量数据通过网络桥接器转发到应用层检测器进行应用层流量过滤处理，得到通过应用层流量过滤处理的第三数据，对第三数据进行放行，对未通过应用层流量过滤处理的流量数据进行拦截和过滤，然后将第三数据通过网络桥接器发送到目标容器，根据在目标容器内部设置的传输层流量过滤策略，对第三数据进行传输层流量过滤处理，得到通过传输层流量过滤处理的第四数据，对第四数据进行放行，对未通过传输层流量过滤处理的第三数据进行拦截和过滤，进而在目标容器对第四数据进行处理。

本公开实施例提供的流量传输控制方法，可以响应于主机接收的流量数据，通过与所述主机相连接的网络桥接器向应用层检测器转发所述流量数据，以通过所述应用层检测器对所述流量数据进行应用层流量过滤处理，将通过所述应用层流量过滤处理的流量数据作为第三数据；通过所述网络桥接器将所述第三数据发送到与所述网络桥接器连接的目标容器，基于在所述目标容器内部设置的传输层流量过滤策略，对所述第三数据进行传输层流量过滤处理，将通过所述传输层流量过滤处理的流量数据作为第四数据；在所述目标容器

对所述第四数据进行处理。

这样，主机在接收到流量数据后，通过配置在主机与容器之间的网络桥接器将流量数据转发到应用层检测器进行应用层流量过滤处理，再将通过应用层流量过滤处理的流量数据转发到容器，通过容器内部设置的传输层流量过滤策略直接进行传输层流量过滤处理；一方面，通过在容器内部进行传输层流量过滤处理的机制，可以降低对容器集群的影响，防止由于网络防护策略的失误或异常导致容器集群出现故障问题；另一方面，由于配置在主机和容器之间的网络桥接器可以兼容各种不同业务特性的容器的流量数据传输，具备良好的适应性、通用性、和鲁棒性，从而可以保障流量传输的稳定性和完整性，进而实现对容器环境下流量数据的安全检测和正常传输。

本领域技术人员可以理解，在具体实施方式的上述方法中，各步骤的撰写顺序并不意味着严格的执行顺序而对实施过程构成任何限定，各步骤的具体执行顺序应当以其功能和可能的内在逻辑确定。

基于同一发明构思，本公开实施例中还提供了与流量传输控制方法对应的流量传输控制装置，由于本公开实施例中的装置解决问题的原理与本公开实施例上述流量传输控制方法相似，因此装置的实施可以参见方法的实施，重复之处不再赘述。

请参阅图 8 和图 9，图 8 为本公开实施例提供的一种流量传输控制装置的示意图之一，图 9 为本公开实施例提供的一种流量传输控制装置的示意图之二。如图 8 中所示，本公开实施例提供的流量传输控制装置 800 包括：

第一过滤模块 801，用于响应于目标容器产生的流量数据，基于在所述目标容器内部设置的传输层流量过滤策略，对所述流量数据进行传输层流量过滤处理，将通过所述传输层流量过滤处理的流量数据作为第一数据；

第二过滤模块 802，用于通过与所述目标容器相连接的网络桥接器向应用层检测器转发所述第一数据，通过所述应用层检测器对所述第一数据进行应用层流量过滤处理，将通过所述应用层流量过滤处理的流量数据作为第二数据；

第一处理模块 803，用于通过所述网络桥接器将所述第二数据发送到与所述网络桥接器连接的主机，并通过主机发送至所述第二数据对应的目的端。

一种可选的实施方式中，如图 9 中所示，所述流量传输控制装置 800 还包括第一设置模块 804，所述第一设置模块 804 用于：

获取网络策略器生成的与所述目标容器对应的传输层流量过滤策略，并将所述传输层流量过滤策略发送至所述网络桥接器；所述传输层流量过滤策略指示有符合传输要求的五元组信息和不符合传输要求的五元组信息；

通过所述网络桥接器将所述传输层流量过滤策略设置在所述目标容器的独立网络命名空间中；

所述第一过滤模块 801 在用于基于在所述目标容器内部设置的传输层流量过滤策略，对所述流量数据进行传输层流量过滤处理时，具体用于：

从所述独立网络命名空间中读取所述传输层流量过滤策略，基于所述流量数据携带的五元组信息，以及所述传输层流量过滤策略指示的符合传输要求的五元组信息和不符合传输要求的五元组信息，对所述流量数据进行传输层流量过滤处理。

一种可选的实施方式中，所述目标容器上设置有第一网络接口，所述主机上设置有第二网络接口；所述网络桥接器上设置有第三网络接口和第四网络接口；其中，所述第一网络接口和所述第三网络接口通信连接，所述第二网络接口和所述第四网络接口通信连接；

所述第二过滤模块 802 在用于通过与所述目标容器相连接的网络桥接器向应用层检测器转发所述第一数据时，具体用于：

通过与所述目标容器相连接的网络桥接器的第三网络接口接收所述目标容器的所述第一网络接口传输的所述第一数据，并调用所述网络桥接器的包转发功能将所述第一数据转发到应用层检测器；

所述第一处理模块 803 在用于通过所述网络桥接器将所述第二数据发送到与所述网络桥接器连接的主机时，具体用于：

通过所述网络桥接器的所述第四网络接口将所述第二数据转发到与所述网络桥接器连接的主机的第二网络接口。

一种可选的实施方式中，所述第二过滤模块 802 在用于通过所述应用层检测器对所述第一数据进行应用层流量过滤处理时，具体用于：

通过所述应用层检测器从预先训练的流量过滤模型集中调用与所述目标容器关联的流量过滤模型；

请参阅图 10 和图 11，图 10 为本公开实施例提供的另一种流量传输控制装置的示意图之一，图 11 为本公开实施例提供的另一种流量传输控制装置的示意图之二。如图 10 中所示，本公开实施例提供的流量传输控制装置 1000 包括：

第三过滤模块 1001，用于响应于主机接收的流量数据，通过与所述主机相连接的网络桥接器向应用层检测器转发所述流量数据，以通过所述应用层检测器对所述流量数据进行应用层流量过滤处理，将通过所述应用层流量过滤处理的流量数据作为第三数据；

第四过滤模块 1002，用于通过所述网络桥接器将所述第三数据发送到与所述网络桥接器连接的目标容器，基于在所述目标容器内部设置的传输层流量过滤策略，对所述第三数据进行传输层流量过滤处理，将通过所述传输层流量过滤处理的流量数据作为第四数据；

第二处理模块 1003，用于在所述目标容器对所述第四数据进行处理。

一种可选的实施方式中，所述目标容器上设置有第一网络接口，所述主机上设置有第二网络接口；所述网络桥接器上设置有第三网络接口和第四网络接口；其中，所述第一网络接口和所述第三网络接口通信连接，所述第二网络接口和所述第四网络接口通信连接；

所述第三过滤模块 1001 在用于通过与所述主机相连接的网络桥接器向应用层检测器转发所述流量数据时，具体用于：

通过与所述主机相连接的网络桥接器的第四网络接口接收所述主机的所述第二网络接口传输的所述流量数据，并调用所述网络桥接器的包转发功能将所述流量数据转发到应用层检测器；

所述第四过滤模块 1002 在用于将通过所述网络桥接器将所述第三数据发送到与所述网络桥接器连接的目标容器时，具体用于：

通过所述网络桥接器的所述第三网络接口将所述第三数据转发到与所述网络桥接器连接的目标容器的第一网络接口。

一种可选的实施方式中，所述第四过滤模块 1002 在用于通过所述应用层检测器对所述流量数据进行应用层流量过滤处理时，具体用于：

通过所述应用层检测器从预先训练的流量过滤模型集中调用与所述目标容器关联的流量过滤模型；

基于调用的所述流量过滤模型，对所述流量数据进行应用层流量过滤处理。

一种可选的实施方式中，如图 11 中所示，所述流量传输控制装置 1000 还包括第二设置模块 1004，所述第二设置模块 1004 用于：

获取网络策略器生成的与所述目标容器对应的传输层流量过滤策略，并将所述传输层流量过滤策略发送至所述网络桥接器；所述传输层流量过滤策略指示有符合传输要求的五元组信息和不符合传输要求的五元组信息；

通过所述网络桥接器将所述传输层流量过滤策略设置在所述目标容器的独立网络命名空间中；

所述第四过滤模块 1002 在用于基于在所述目标容器内部设置的传输层流量过滤策略，对所述第三数据进行传输层流量过滤处理时，具体用于：

从所述独立网络命名空间中读取所述传输层流量过滤策略，基于所述第三数据携带的五元组信息，以及所述传输层流量过滤策略指示的符合传输要求的五元组信息和不符合传输要求的五元组信息，对所述第三数据进行传输层流量过滤处理。

关于装置中的各模块的处理流程、以及各模块之间的交互流程的描述可以参照上述方法实施例中的相关说明，这里不再详述。

基于同一技术构思，本公开实施例还提供了一种电子设备。参照图 12 所示，为本公开实施例提供的电子设备 1200 结构示意图，包括：

处理器 1210、存储器 1220、和总线 1230；存储器 1220 用于存储执行指令，包括内存 1221 和外部存储器 1222；这里的内存 1221 也称内存储器，用于暂时存放处理器 1210 中的运算数据，以及与硬盘等外部存储器 1222 交换的数据，处理器 1210 通过内存 1221 与外部存储器 1222 进行数据交换，当所述电子设备 1200 运行时，所述处理器 1210 与所述存储器 1220 之间通过总线 1230 通信，使得所述处理器 1210 可以执行上述的流量传输控制方法实施例中所提及的执行指令。

本公开实施例还提供一种计算机可读存储介质，该计算机可读存储介质上存储有计算机程序，该计算机程序被处理器运行时执行上述方法实施例中所述的流量传输控制方法的步骤。其中，该存储介质可以是易失性或非易失的计算机可读取存储介质。

本公开实施例还提供一种计算机程序产品，该计算机程序产品包括有计算机指令，所述计算机指令被处理器执行时可以执行上述方法实施例中所述的流量传输控制方法的步骤，具体可参见上述方法实施例，在此不再赘述。

其中，上述计算机程序产品可以具体通过硬件、软件或其结合的方式实现。在一个可选实施例中，所述计算机程序产品具体体现为计算机存储介质，在另一个可选实施例中，计算机程序产品具体体现为软件产品，例如软件开发包（Software Development Kit，SDK）等等。

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，上述描述的设备和装置的具体工作过程，可以参考前述方法实施例中的对应过程，在此不再赘述。在本公开所提供的几个实施例中，应该理解到，所揭露的设备、装置和方法，可以通过其它的方式实现。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，又例如，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通信接口，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，在本公开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，可以存储在一个处理器可执行的非易失的计算机可读取存储介质中。基于这样的理解，本公开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）执行本公开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（Read-Only Memory，ROM）、随机存取存储器（Random Access Memory，RAM）、磁碟或者光盘等各种可以存储程序代码的介质。

最后应说明的是：以上所述实施例，仅为本公开的具体实施方式，用以说明本公开的技术方案，而非对其限制，本公开的保护范围并不局限于此，尽管参照前述实施例对本公开进行了详细的说明，本领域的普通技术人员应当理解：任何熟悉本技术领域的技术人员在本公开揭露的技术范围内，其依然可以对前述实施例所记载的技术方案进行修改或可轻易想到变化，或者对其中部分技术特征进行等同替换；而这些修改、变化或者替换，并不使相应技术方案的本质脱离本公开实施例技术方案的精神和范围，都应涵盖在本公开的保护范围之内。因此，本公开的保护范围应所述以权利要求的保护范围为准。

权 利 要 求

1、一种流量传输控制方法，所述方法包括：

响应于目标容器产生的流量数据，基于在所述目标容器内部设置的传输层流量过滤策略，对所述流量数据进行传输层流量过滤处理，将通过所述传输层流量过滤处理的流量数据作为第一数据；

通过与所述目标容器相连接的网络桥接器向应用层检测器转发所述第一数据，通过所述应用层检测器对所述第一数据进行应用层流量过滤处理，将通过所述应用层流量过滤处理的流量数据作为第二数据；

通过所述网络桥接器将所述第二数据发送到与所述网络桥接器连接的主机，并通过主机发送至所述第二数据对应的目的端。

2、根据权利要求 1 所述的方法，其中，在基于在所述目标容器内部设置的传输层流量过滤策略，对所述流量数据进行传输层流量过滤处理之前，还包括：

获取网络策略器生成的与所述目标容器对应的传输层流量过滤策略，并将所述传输层流量过滤策略发送至所述网络桥接器；所述传输层流量过滤策略指示有符合传输要求的五元组信息和不符合传输要求的五元组信息；

通过所述网络桥接器将所述传输层流量过滤策略设置在所述目标容器的独立网络命名空间中；

所述基于在所述目标容器内部设置的传输层流量过滤策略，对所述流量数据进行传输层流量过滤处理，包括：

从所述独立网络命名空间中读取所述传输层流量过滤策略，基于所述流量数据携带的五元组信息，以及所述传输层流量过滤策略指示的符合传输要求的五元组信息和不符合传输要求的五元组信息，对所述流量数据进行传输层流量过滤处理。

3、根据权利要求 1 所述的方法，其中，所述目标容器上设置有第一网络接口，所述主机上设置有第二网络接口；所述网络桥接器上设置有第三网络接口和第四网络接口；其中，所述第一网络接口和所述第三网络接口通信连接，所述第二网络接口和所述第四网络接口通信连接；

所述通过与所述目标容器相连接的网络桥接器向应用层检测器转发所述第一数据，包括：

通过与所述目标容器相连接的网络桥接器的第三网络接口接收所述目标容器的所述第一网络接口传输的所述第一数据，并调用所述网络桥接器的包转发功能将所述第一数据转发到应用层检测器；

所述通过所述网络桥接器将所述第二数据发送到与所述网络桥接器连接的主机，包括：

通过所述网络桥接器的所述第四网络接口将所述第二数据转发到与所述网络桥接器连接的主机的第二网络接口。

4、根据权利要求 1 所述的方法，其中，所述通过所述应用层检测器对所述第一数据进行应用层流量过滤处理，包括：

通过所述应用层检测器从预先训练的流量过滤模型集中调用与所述目标容器关联的流量过滤模型；

基于调用的所述流量过滤模型，对所述第一数据进行应用层流量过滤处理。

5、一种流量传输控制方法，所述方法包括：

响应于主机接收的流量数据，通过与所述主机相连接的网络桥接器向应用层检测器转发所述流量数据，以通过所述应用层检测器对所述流量数据进行应用层流量过滤处理，将通过所述应用层流量过滤处理的流量数据作为第三数据；

通过所述网络桥接器将所述第三数据发送到与所述网络桥接器连接的目标容器，基于在所述目标容器内部设置的传输层流量过滤策略，对所述第三数据进行传输层流量过滤处理，将通过所述传输层流量过滤处理的流量数据作为第四数据；

在所述目标容器对所述第四数据进行处理。

6、根据权利要求 5 所述的方法，其中，所述目标容器上设置有第一网络接口，所述主机上设置有第二网络接口；所述网络桥接器上设置有第三网络接口和第四网络接口；其中，所述第一网络接口和所述第三网络接口通信连接，所述第二网络接口和所述第四网络接口通信连接；

所述通过与所述主机相连接的网络桥接器向应用层检测器转发所述流量数据，包括：

通过与所述主机相连接的网络桥接器的第四网络接口接收所述主机的所述第二网络接口传输的所述流量数据，并调用所述网络桥接器的包转发功能将所述流量数据转发到应用层检测器；

所述通过所述网络桥接器将所述第三数据发送到与所述网络桥接器连接的目标容器，包括：

通过所述网络桥接器的所述第三网络接口将所述第三数据转发到与所述网络桥接器连接的目标容器的第一网络接口。

7、根据权利要求 5 所述的方法，其中，所述通过所述应用层检测器对所述流量数据进行应用层流量过滤处理，包括：

通过所述应用层检测器从预先训练的流量过滤模型集中调用与所述目标容器关联的流量过滤模型；

基于调用的所述流量过滤模型，对所述流量数据进行应用层流量过滤处理。

8、根据权利要求 5 所述的方法，其中，在基于在所述目标容器内部设置的传输层流量过滤策略，对所述第三流量数据进行传输层流量过滤处理之前，还包括：

获取网络策略器生成的与所述目标容器对应的传输层流量过滤策略，并将所述传输层流量过滤策略发送至所述网络桥接器；所述传输层流量过滤策略指示有符合传输要求的五元组信息和不符合传输要求的五元组信息；

通过所述网络桥接器将所述传输层流量过滤策略设置在所述目标容器的独立网络命名空间中；

所述基于在所述目标容器内部设置的传输层流量过滤策略，对所述第三数据进行传输层流量过滤处理，包括：

从所述独立网络命名空间中读取所述传输层流量过滤策略，基于所述第三数据携带的五元组信息，以及所述传输层流量过滤策略指示的符合传输要求的五元组信息和不符合传输要求的五元组信息，对所述第三数据进行传输层流量过滤处理。

9、一种流量传输控制装置，所述装置包括：

第一过滤模块，用于响应于目标容器产生的流量数据，基于在所述目标容器内部设置的传输层流量过滤策略，对所述流量数据进行传输层流量过滤处理，将通过所述传输层流量过滤处理的流量数据作为第一数据；

第二过滤模块，用于通过与所述目标容器相连接的网络桥接器向应用层检测器转发所述第一数据，通过所述应用层检测器对所述第一数据进行应用层流量过滤处理，将通过所述应用层流量过滤处理的流量数据作为第二数据；

第一处理模块，用于通过所述网络桥接器将所述第二数据发送到与所述网络桥接器连接的主机，并通过主机发送至所述第二数据对应的目的端。

10、一种流量传输控制装置，所述装置包括：

第三过滤模块，用于响应于主机接收的流量数据，通过与所述主机相连接的网络桥接器向应用层检测器转发所述流量数据，以通过所述应用层检测器对所述流量数据进行应用层流量过滤处理，将通过所述应用层流量过滤处理的流量数据作为第三数据；

第四过滤模块，用于通过所述网络桥接器将所述第三数据发送到与所述网络桥接器连接的目标容器，基于在所述目标容器内部设置的传输层流量过滤策略，对所述第三数据进行传输层流量过滤处理，将通过所述传输层流量过滤处理的流量数据作为第四数据；

第二处理模块，用于在所述目标容器对所述第四数据进行处理。

11、一种电子设备，包括：处理器、存储器和总线，所述存储器存储有所述处理器可执行的机器可读指令，当电子设备运行时，所述处理器与所述存储器之间通过总线通信，所述机器可读指令被所述处理器执行时执行如权利要求 1 至 4 或者权利要求 5 至 8 中任一项所述的流量传输控制方法的步骤。

12、一种计算机可读存储介质，该计算机可读存储介质上存储有计算机程序，该计算机程序被处理器运行时执行如权利要求 1 至 4 或者权利要求 5 至 8 中任一项所述的流量传输控制方法的步骤。

13、一种计算机程序产品，所述计算机程序产品在设备上运行时，使得所述设备执行如权利要求 1 至 4 或者权利要求 5 至 8 中任一项所述的流量传输控制方法的步骤。

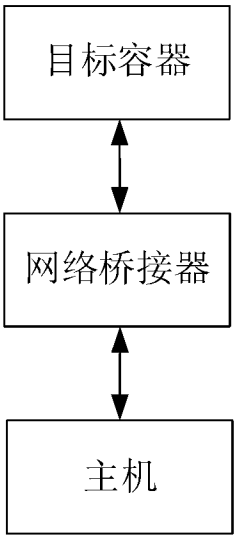
目标容器
网络桥接器
主机

图 1

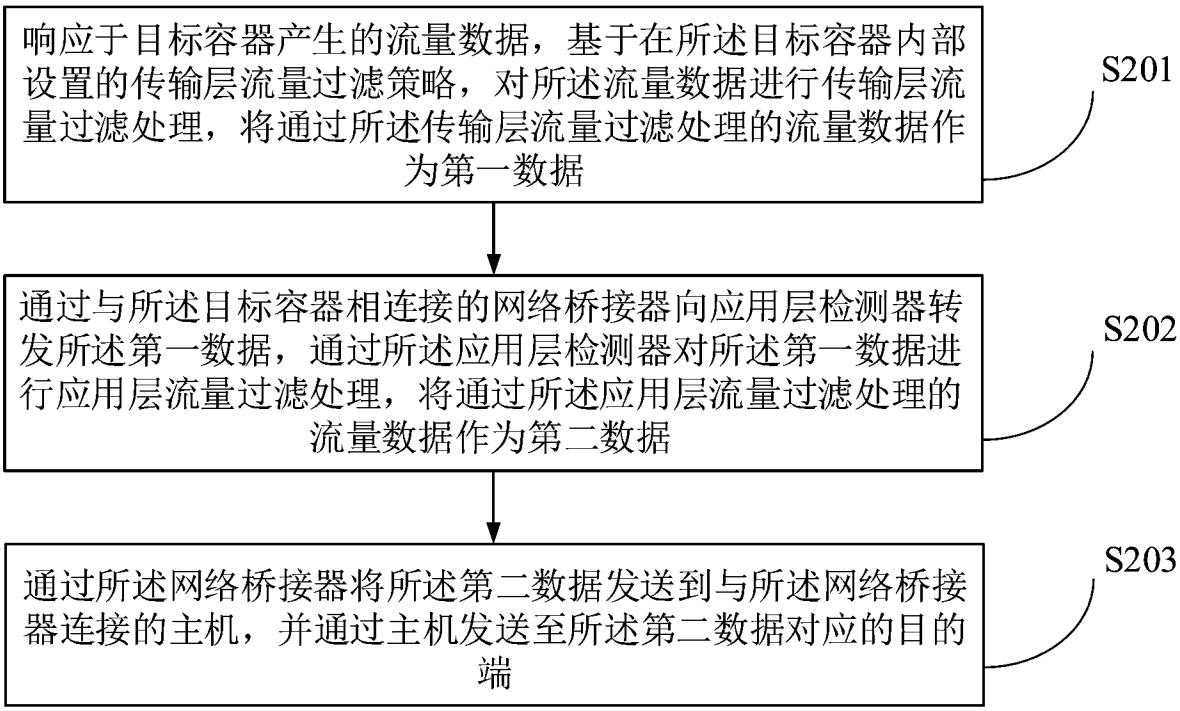
响应于目标容器产生的流量数据，基于在所述目标容器内部设置的传输层流量过滤策略，对所述流量数据进行传输层流量过滤处理，将通过所述传输层流量过滤处理的流量数据作为第一数据
S201
通过与所述目标容器相连接的网络桥接器向应用层检测器转发所述第一数据，通过所述应用层检测器对所述第一数据进行应用层流量过滤处理，将通过所述应用层流量过滤处理的流量数据作为第二数据
S202
通过所述网络桥接器将所述第二数据发送到与所述网络桥接器连接的主机，并通过主机发送至所述第二数据对应的目的端
S203

图 2

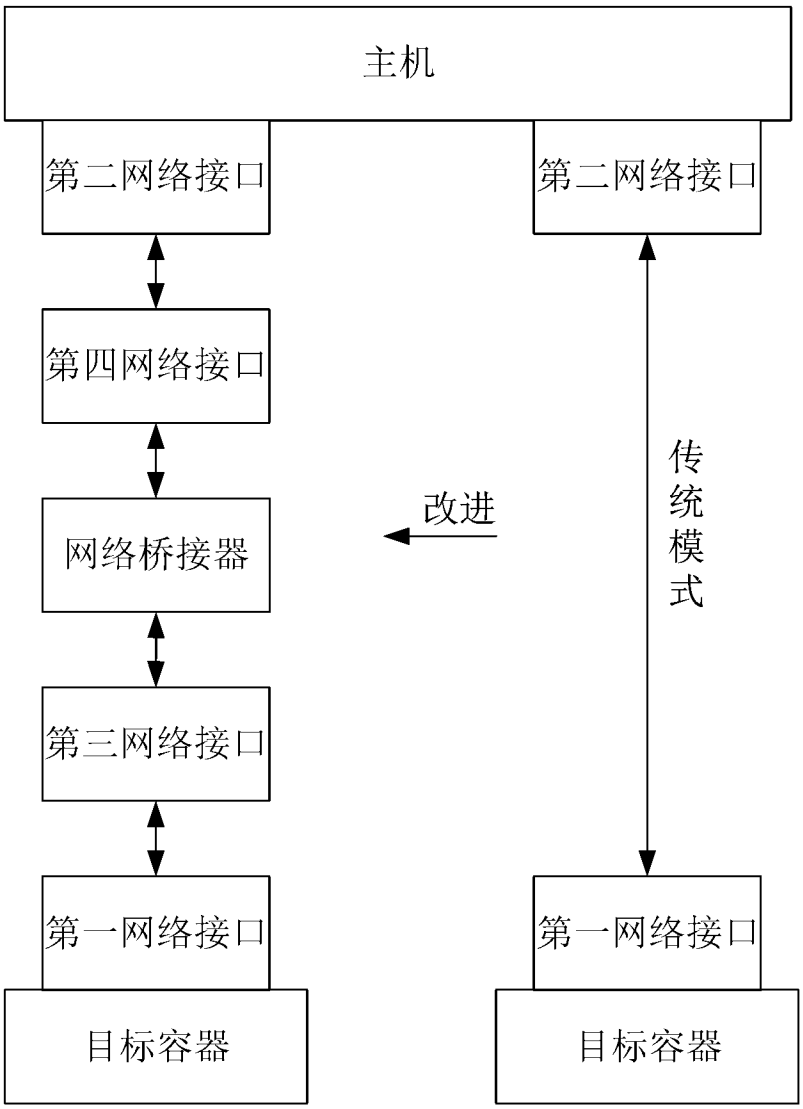
主机
第二网络接口
第二网络接口
第四网络接口
网络桥接器
改进
传统模式
第三网络接口
第一网络接口
第一网络接口
目标容器
目标容器

图 3

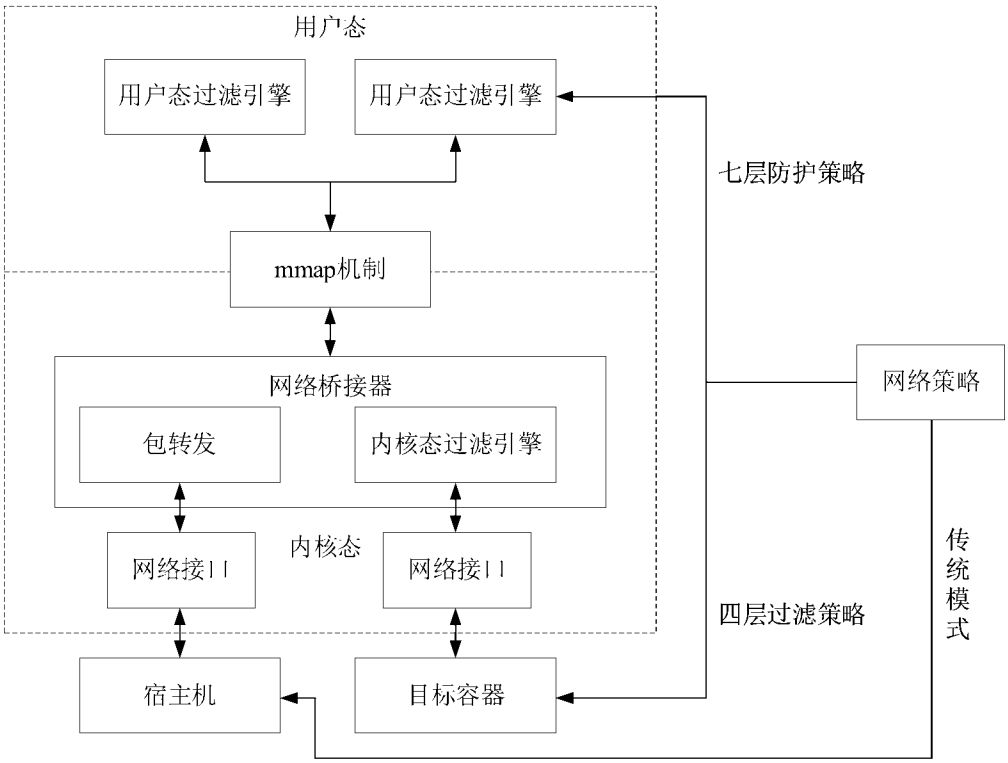
用户态
用户态过滤引擎
用户态过滤引擎
七层防护策略
mmap机制
网络桥接器
网络策略
包转发
内核态过滤引擎
内核态
网络接口
网络接口
传统模式
四层过滤策略
宿主机
目标容器

图 4

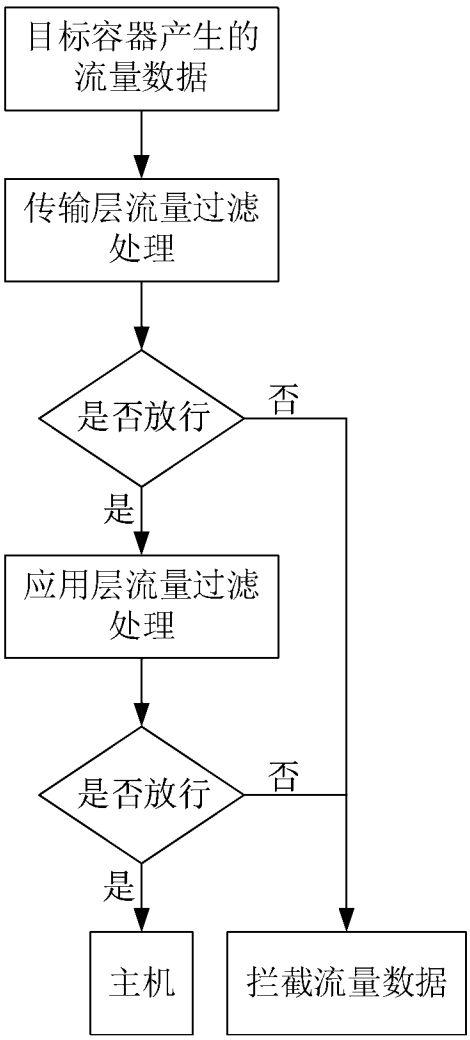
目标容器产生的流量数据
传输层流量过滤处理
是否放行
否
是
应用层流量过滤处理
是否放行
否
是
主机
拦截流量数据

图 5

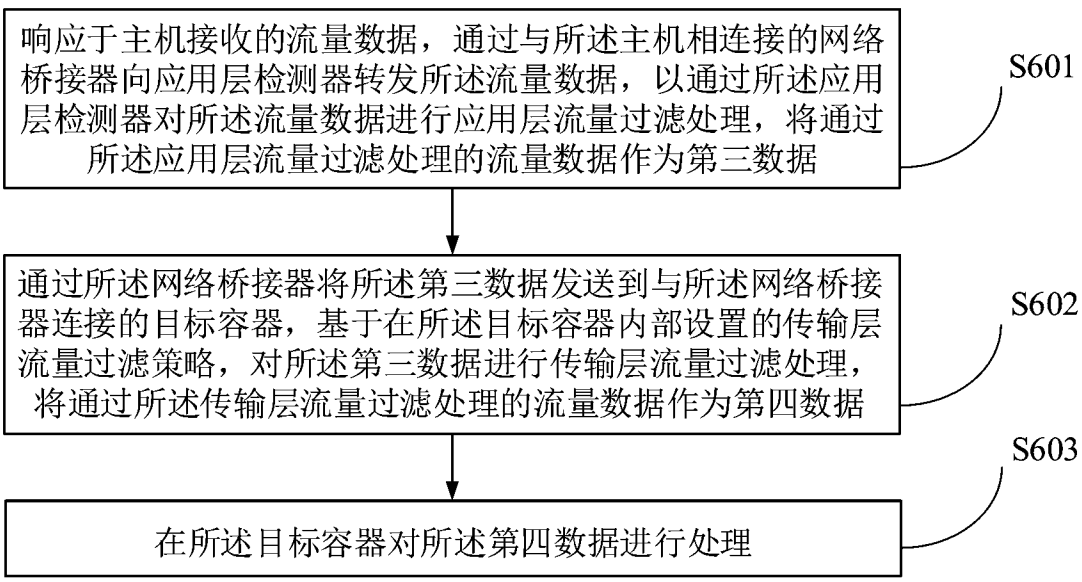
响应于主机接收的流量数据，通过与所述主机相连接的网络桥接器向应用层检测器转发所述流量数据，以通过所述应用层检测器对所述流量数据进行应用层流量过滤处理，将通过所述应用层流量过滤处理的流量数据作为第三数据
S601
通过所述网络桥接器将所述第三数据发送到与所述网络桥接器连接的目标容器，基于在所述目标容器内部设置的传输层流量过滤策略，对所述第三数据进行传输层流量过滤处理，将通过所述传输层流量过滤处理的流量数据作为第四数据
S602
在所述目标容器对所述第四数据进行处理
S603

图 6

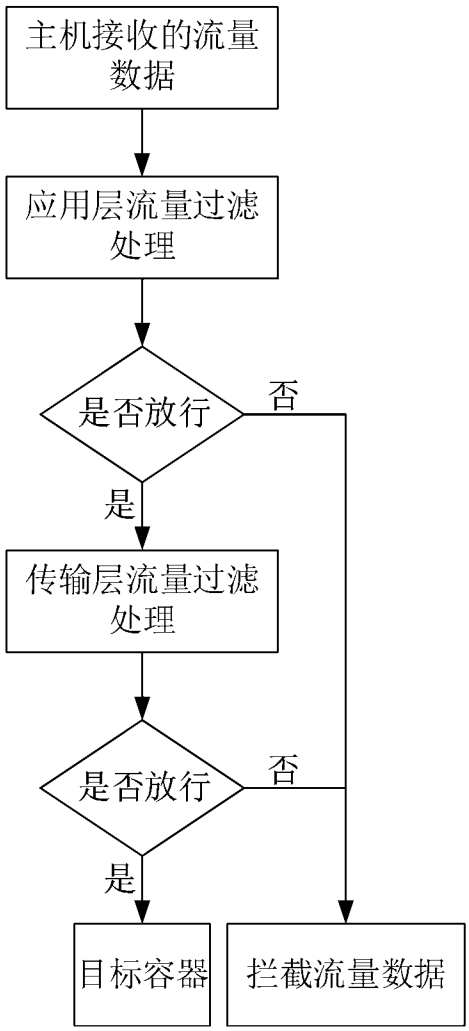

图 7

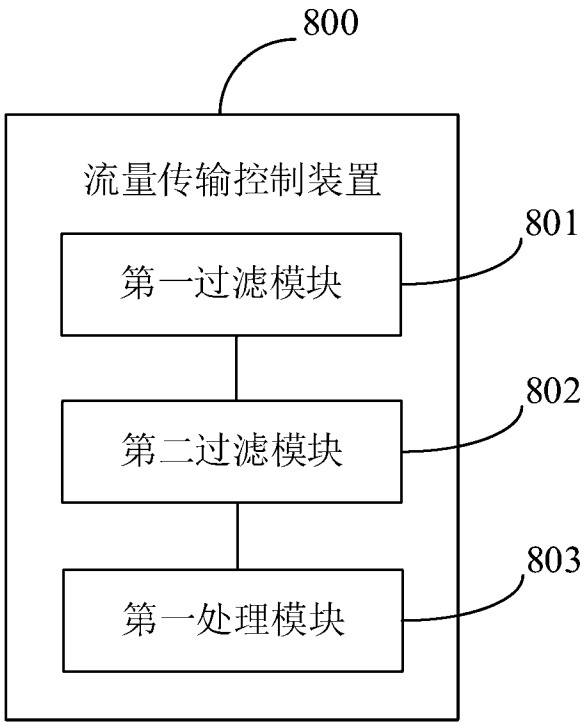
800
流量传输控制装置
801
第一过滤模块
802
第二过滤模块
803
第一处理模块

图 8

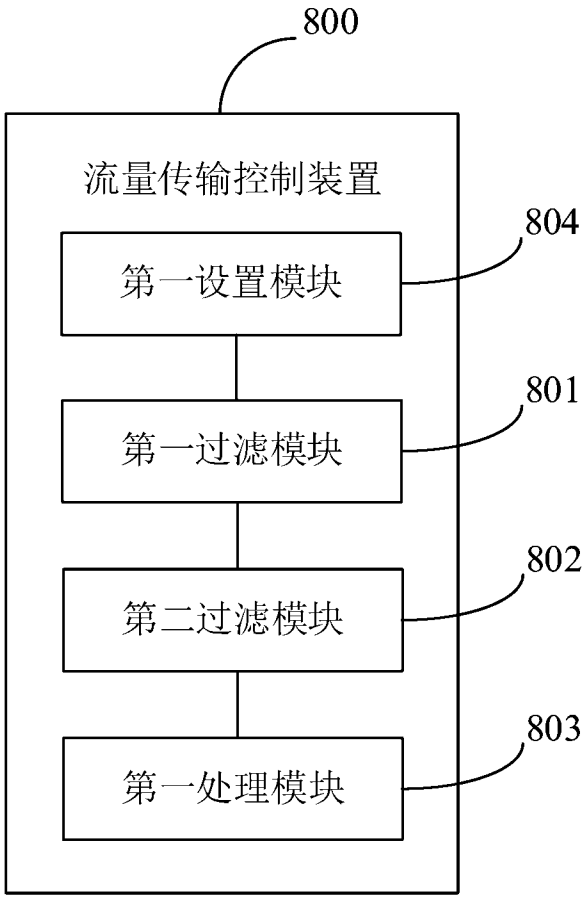
800
流量传输控制装置
804
第一设置模块
801
第一过滤模块
802
第二过滤模块
803
第一处理模块

图 9

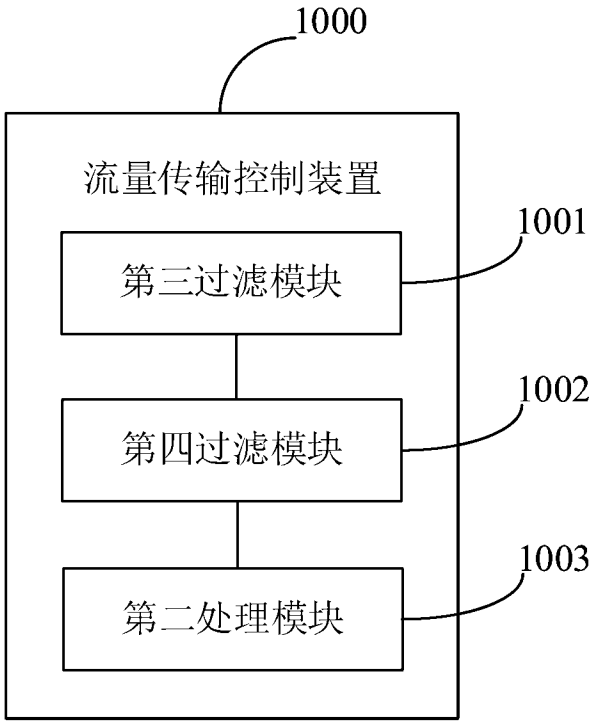

图 10

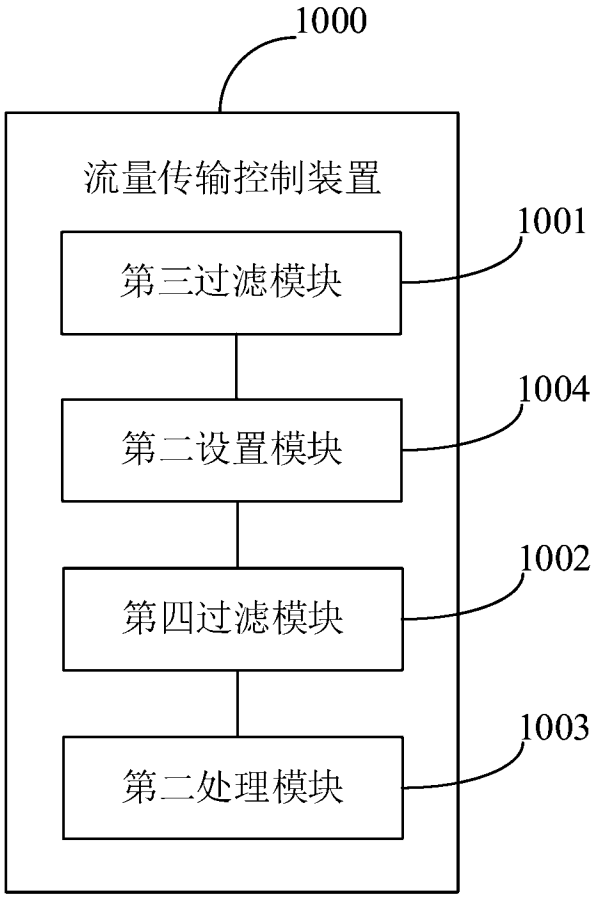
1000
流量传输控制装置
1001
第三过滤模块
1004
第二设置模块
1002
第四过滤模块
1003
第二处理模块

图 11

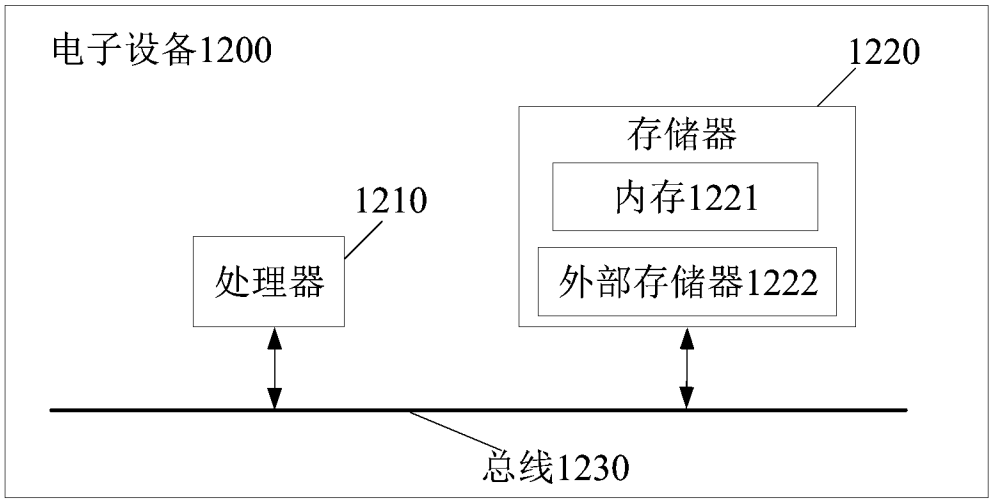
电子设备1200
1220
存储器
内存1221
外部存储器1222
1210
处理器
总线1230

图 12

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2023/086761

A. CLASSIFICATION OF SUBJECT MATTER

H04L9/40(2022.01)i;H04L47/10(2022.01)i;H04L69/16(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)

IPC: 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, USTXT, WOTXT, EPTXT, CNKI, IEEE Xplore, BAIDU: 容器, 传输层, 应用层, 主机, 宿主机, 网桥, 网络桥接, 拦截, 过滤, 规则, 策略, 检测, 检查, docker, container, bridge, host, transport layer, filter, head off, intercept, rule, policy, strategy, detect

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 114978610 A (BEIJING VOLCANO ENGINE TECHNOLOGY CO., LTD.) 30 August 2022 (2022-08-30) description, paragraphs [0072]-[0201]	1-13
A	US 2019058722 A1 (TWISTLOCK LTD.) 21 February 2019 (2019-02-21) description, paragraphs [0033]-[0102], and figures 1, 3-5, and 8	1-13
A	US 2018278639 A1 (TWISTLOCK LTD.) 27 September 2018 (2018-09-27) entire document	1-13
A	US 2021067538 A1 (ILLUMIO INC.) 04 March 2021 (2021-03-04) entire document	1-13
A	US 2009328210 A1 (MICROSOFT CORP.) 31 December 2009 (2009-12-31) entire document	1-13

☐ 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
11 May 2023	**22 May 2023**

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/CN2023/086761

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 114978610 A	30 August 2022	None	
US 2019058722 A1	21 February 2019	US 10693899 B2	23 June 2020
US 2018278639 A1	27 September 2018	US 10567411 B2	18 February 2020
US 2021067538 A1	04 March 2021	US 11516242 B2	29 November 2022
US 2009328210 A1	31 December 2009	None	

国际检索报告

国际申请号
PCT/CN2023/086761

A. 主题的分类

H04L9/40(2022.01)i;H04L47/10(2022.01)i;H04L69/16(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)

IPC：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, USTXT,WOTXT,EPTXT,CNKI,IEEE Xplore,BAIDU:容器,传输层, 应用层,主机,宿主机,网桥,网络桥接，拦截,过滤,规则,策略,检测,检查,docker,container, bridge,host,transport layer,filter,head off,intercept,rule,policy,strategy, detect

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 114978610 A (北京火山引擎科技有限公司) 2022年8月30日 (2022-08-30) 说明书第[0072]-[0201]段	1-13
A	US 2019058722 A1 (TWISTLOCK LTD) 2019年2月21日 (2019-02-21) 说明书[0033]-[0102]段，附图1、3-5、8	1-13
A	US 2018278639 A1 (TWISTLOCK LTD) 2018年9月27日 (2018-09-27) 全文	1-13
A	US 2021067538 A1 (ILLUMIO INC) 2021年3月4日 (2021-03-04) 全文	1-13
A	US 2009328210 A1 (MICROSOFT CORP) 2009年12月31日 (2009-12-31) 全文	1-13

☐ 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
2023年5月11日	2023年5月22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 匡仁炳 电话号码 (+86) 020-28950886

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2023/086761

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	114978610	A	2022年8月30日		无		
US	2019058722	A1	2019年2月21日	US	10693899	B2	2020年6月23日
US	2018278639	A1	2018年9月27日	US	10567411	B2	2020年2月18日
US	2021067538	A1	2021年3月4日	US	11516242	B2	2022年11月29日
US	2009328210	A1	2009年12月31日		无		