(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 108574667 B
(45)授权公告日 2021.01.15

(21)申请号 201710138725.0
(22)申请日 2017.03.09
(65)同一申请的已公布的文献号
申请公布号 CN 108574667 A
(43)申请公布日 2018.09.25
(73)专利权人 华为技术有限公司
地址 518129 广东省深圳市龙岗区坂田华为总部办公楼
(72)发明人 银宇 戚彩霞
(74)专利代理机构 北京同达信恒知识产权代理有限公司 11291
代理人 冯艳莲
(51)Int.Cl.
H04L 29/06(2006.01)

(56)对比文件
CN 101355415 A,2009.01.28
CN 105847236 A,2016.08.10
US 2014233385 A1,2014.08.21
CN 1581803 A,2005.02.16
CN 105050140 A,2015.11.11

审查员 刘仪瑶

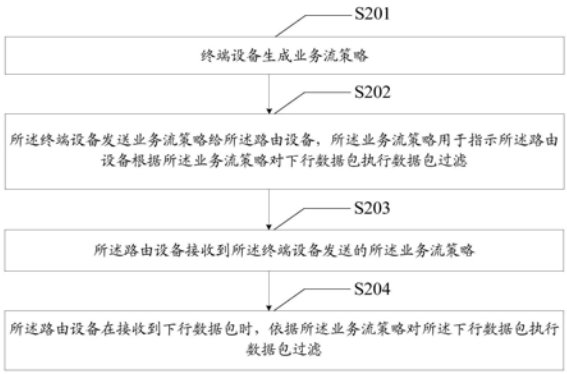
权利要求书3页 说明书15页 附图6页

(54)发明名称

一种业务流的控制方法及装置

(57)摘要

本申请公开了一种业务流的控制方法及装置，用以解决现有存在的安全性较差的问题。所述方法包括：终端设备生成业务流策略；所述终端设备发送业务流策略给所述路由设备，所述业务流策略用于指示所述路由设备根据所述业务流策略对下行数据包执行数据包过滤。



CN 108574667 B

1.一种业务流的控制方法,其特征在于,包括:

终端设备生成业务流策略;

所述终端设备发送所述业务流策略给路由设备,所述业务流策略用于指示所述路由设备根据所述业务流策略对下行数据包执行数据包过滤;

所述终端设备生成业务流策略,包括:

所述终端设备识别存在安全威胁的下行数据包,并基于识别的所述下行数据包生成所述业务流策略;或者,

所述终端设备识别存在安全威胁的下行数据包,基于经过用户确认的存在安全威胁的下行数据包生成所述业务流策略。

2.如权利要求1所述的方法,其特征在于,所述终端设备识别存在安全威胁的下行数据包,包括:

所述终端设备接收所述下行数据包;

若确认所述终端设备上没有监听所述下行数据包的端口,则所述终端设备识别所述下行数据包存在安全威胁。

3.如权利要求1或2所述的方法,其特征在于,所述终端设备发送业务流策略给所述路由设备,包括:

所述终端设备通过网络设备将所述业务流策略发送给所述路由设备;或者,

所述终端设备通过安全服务器将所述业务流策略发送给所述路由设备。

4.如权利要求3所述的方法,其特征在于,所述方法还包括:

所述终端设备注册到所述网络设备的过程中,所述终端设备接收所述网络设备发送的所述安全服务器的通信地址;

所述终端设备通过安全服务器将所述业务流策略发送给所述路由设备,包括:

所述终端设备基于所述安全服务器的通信地址将业务流策略发送给所述安全服务器。

5.如权利要求1或2所述的方法,其特征在于,所述业务流策略包括:至少一个数据包过滤规则以及每一个数据包过滤规则对应的操作信息。

6.如权利要求1或2所述的方法,其特征在于,所述路由设备为网关设备或者防火墙。

7.一种业务流的控制方法,其特征在于,包括:

网络设备获取业务流策略;

所述网络设备将所述业务流策略发送给路由设备,所述业务流策略用于指示所述路由设备根据所述业务流策略对下行数据包执行数据包过滤;

所述网络设备获取业务流策略,包括:

所述网络设备从运营商应用平台获取到所述业务流策略;

所述网络设备获取业务流策略之前,所述方法还包括:所述网络设备接收运营商应用平台发送的用户属性与业务流策略的对应关系;

终端设备注册到所述网络设备的过程中,所述网络设备获取所述终端设备的用户属性;

所述网络设备获取业务流策略,包括:

所述网络设备确定所述终端设备的用户属性对应的业务流策略。

8.如权利要求7所述的方法,其特征在于,所述业务流策略包括:至少一个数据包过滤

规则以及每一个数据包过滤规则对应的操作信息。

9.如权利要求7或8所述的方法,其特征在于,所述网络设备获取业务流策略,还包括:

所述网络设备接收由终端设备发来的业务流策略。

10.如权利要求7或8所述的方法,其特征在于,所述网络设备获取业务流策略之前,所述方法还包括:

终端设备注册到所述网络设备的过程中,所述网络设备获取所述终端设备的用户属性;

所述网络设备获取业务流策略,包括:

所述网络设备从所述运营商应用平台获取所述用户属性对应的业务流策略。

11.如权利要求7或8所述的方法,其特征在于,所述方法还包括:

终端设备注册到所述网络设备的过程中,所述网络设备将安全服务器的通信地址发送给终端设备,以便所述终端设备基于所述通信地址将所述业务流策略通过安全服务器发送给所述路由设备。

12.如权利要求7或8所述的方法,其特征在于,所述路由设备为网关设备或者防火墙。

13.一种业务流的控制装置,其特征在于,包括:

处理单元,用于生成业务流策略;

发送单元,用于发送所述处理单元生成业务流策略给路由设备,所述业务流策略用于指示所述路由设备根据所述业务流策略对下行数据包执行数据包过滤;

所述处理单元,具体用于:

识别存在安全威胁的下行数据包,并基于识别的所述下行数据包生成所述业务流策略;或者,

识别存在安全威胁的下行数据包,基于经过用户确认的存在安全威胁的下行数据包生成所述业务流策略。

14.如权利要求13所述的装置,其特征在于,所述装置还包括:

接收单元,用于接收所述下行数据包;

所述处理单元,在识别存在安全威胁的下行数据包时,具体用于:

若确认终端设备上没有监听所述下行数据包的端口,则识别所述下行数据包存在安全威胁。

15.如权利要求13至14任一项所述的装置,其特征在于,所述发送单元,具体用于:

通过网络设备将所述业务流策略发送给所述路由设备;或者,

通过安全服务器将所述业务流策略发送给所述路由设备。

16.如权利要求15所述的装置,其特征在于,所述装置还包括:

接收单元,用于在终端设备注册到所述网络设备的过程中,接收所述网络设备发送的所述安全服务器的通信地址;

所述发送单元,在通过安全服务器将所述业务流策略发送给所述路由设备时,具体用于:

基于所述安全服务器的通信地址将业务流策略发送给所述安全服务器。

17.如权利要求13或14所述的装置,其特征在于,所述业务流策略包括:至少一个数据包过滤规则以及每一个数据包过滤规则对应的操作信息。

18.如权利要求13或14所述的装置，其特征在于，所述路由设备为网关设备或者防火墙。

19.一种业务流的控制装置，其特征在于，包括：

获取单元，用于获取业务流策略；

发送单元，用于将所述业务流策略发送给路由设备，所述业务流策略用于指示所述路由设备根据所述业务流策略对下行数据包执行数据包过滤；

所述获取单元，具体用于：

从运营商应用平台获取到所述业务流策略；

接收单元，用于在所述获取单元获取业务流策略之前，接收运营商应用平台发送的用户属性与业务流策略的对应关系；

所述获取单元，具体用于在终端设备注册到网络设备的过程中，获取所述终端设备的用户属性，并确定所述终端设备的用户属性对应的业务流策略。

20.如权利要求19所述的装置，其特征在于，所述业务流策略包括：至少一个数据包过滤规则以及每一个数据包过滤规则对应的操作信息。

21.如权利要求19或20所述的装置，其特征在于，还包括：

接收单元，用于接收由终端设备发来的业务流策略。

22.如权利要求19或20所述的装置，其特征在于，所述获取单元，还用于在获取业务流策略之前，在终端设备注册到所述网络设备的过程中，获取所述终端设备的用户属性：

所述获取单元，在获取业务流策略时，具体用于从所述运营商应用平台获取所述用户属性对应的业务流策略。

23.如权利要求19或20所述的装置，其特征在于，所述发送单元，还用于：

在终端设备注册到所述网络设备的过程中，将安全服务器的通信地址发送给终端设备，以便所述终端设备基于所述通信地址将所述业务流策略通过安全服务器发送给所述路由设备。

24.如权利要求19或20所述的装置，其特征在于，所述路由设备为网关设备或者防火墙。

一种业务流的控制方法及装置

技术领域

[0001] 本申请涉及通信技术领域，尤其涉及一种业务流的控制方法及装置。

背景技术

[0002] 随着终端设备越来越多样性，如智能手机，平板电脑和车载电脑等，以及终端设备上应用的迅速增长，如视频通话，虚拟现实(英文:Virtual Reality，简称:VR)，移动购物等，移动通信网络在近几年来给人们的生活带来了翻天覆地的变化，影响着人们的生活、学习、工作和娱乐等方方面面。与此同时，终端设备也受到越来越多的网络安全威胁，比如网络内部分终端设备持续收到来自数据网络的下行数据包，或者挂马网站将木马病毒隐藏在用户访问的主页之中等等。

[0003] 网络安全威胁会对用户造成财产损失和隐私信息泄露的风险，比如导致终端设备的账号、密码等信息泄露，带来财产损失；又比如大量的下行数据包发送到终端设备会占用终端设备的流量，终端设备需要根据流量支付过多的通信费用，并且大量的下行数据包占用网络资源，可能导致网络拥塞等等。

[0004] 目前，运营商通常通过部署防火墙的方式，确保移动通信网络和外部数据网络的安全隔离，避免终端设备遭受外部的安全威胁。防火墙根据本地配置的过滤规则，比如数据包的五元组(源IP地址、目的IP地址、协议类型、源端口、目的端口)等数据包头信息，以及数据包传输方向等信息，来判断是否允许该数据包从外部数据网络通过防火墙进入移动通信网络，并发送给终端设备。

[0005] 目前由于网络安全威胁的方法演进变化较快，从而导致过滤规则也需要随着更新变化，因此仅仅通过本地配置的过滤规则针对下行数据包进行过滤的方法，导致防火墙出现漏洞的可能性增加，从而防火墙不能完全阻隔终端设备免受外部数据网络的安全威胁。

[0006] 另外，5G网络服务于更多的垂直行业，如车联网、物联网等等，垂直行业的用户可能只允许使用较少的应用，如电表终端，只需要与电力公司的应用服务器通信进行电子抄表等业务。目前防火墙本地配置过滤规则的机制难以支持基于垂直行业应用模式的差异化灵活控制。

发明内容

[0007] 本申请提供一种业务流的控制方法及装置，用以解决现有存在的安全性较差的问题。

[0008] 第一方面，本申请实施例提供了一种业务流的控制方法，包括：

[0009] 终端设备生成业务流策略；

[0010] 所述终端设备发送业务流策略给所述路由设备，所述业务流策略用于指示所述路由设备根据所述业务流策略对下行数据包执行数据包过滤。

[0011] 通过上述设计，由终端设备自己生成业务流策略发送给路由设备，从而路由设备根据终端设备的要求，丢弃存在安全威胁的数据包，通过安全的数据包，从而避免对终端设

备带来财产损失或者隐私信息泄露等安全风险。

[0012] 在一种可能的设计中，所述终端设备生成业务流策略，可以通过如下方式实现：

[0013] 所述终端设备基于业务流策略配置信息生成所述业务流策略；或者，

[0014] 所述终端设备基于用户输入的存在安全威胁的数据包信息生成所述业务流策略；或者，

[0015] 所述终端设备识别存在安全威胁的下行数据包，并基于识别的所述下行数据包生成所述业务流策略；或者，

[0016] 所述终端设备识别存在安全威胁的下行数据包，基于经过用户确认的存在安全威胁的下行数据包生成所述业务流策略。

[0017] 通过上述设计，由终端设备生成业务流策略，由于终端设备和终端设备上应用的多样化发展，从而保证路由设备接收到的业务流策略也随着更新变化，降低了路由设备出现漏洞的可能性，提高了终端设备的安全性。

[0018] 在一种可能的设计中，所述终端设备识别存在安全威胁的下行数据包，包括：

[0019] 所述终端设备接收所述下行数据包；

[0020] 若确认所述终端设备上没有监听所述下行数据包的端口，则所述终端设备识别所述下行数据包存在安全威胁。

[0021] 通过上述方式，在确认所述终端设备上没有监听所述下行数据包的端口时，所述终端设备识别所述下行数据包存在安全威胁，提高了监听存在安全威胁的数据包的准确性。

[0022] 在一种可能的设计中，所述终端设备发送业务流策略给所述路由设备，包括：

[0023] 所述终端设备通过网络设备将所述业务流策略发送给所述路由设备；或者，

[0024] 所述终端设备通过安全服务器将所述业务流策略发送给所述路由设备。

[0025] 在一种可能的设计中，所述方法还包括：

[0026] 所述终端设备注册到所述网络设备的过程中，所述终端设备接收所述网络设备发送的所述安全服务器的通信地址；

[0027] 所述终端设备通过安全服务器将所述业务流策略发送给所述路由设备，包括：

[0028] 所述终端设备基于所述安全服务器的通信地址将业务流策略发送给所述安全服务器。

[0029] 通过上述设计，在终端设备注册到所述网络设备的过程中，获取安全服务器的通信地址，从而保证终端设备将能够将业务流策略发送给安全服务器，由安全服务器转发给路由设备，由于安全服务器的安全性高，因此提高了业务流策略的安全性。

[0030] 在一种可能的设计中，所述业务流策略包括：至少一个数据包过滤规则以及每一个数据包过滤规则对应的操作信息。

[0031] 在一种可能的设计中，所述路由设备可以为网关设备或者防火墙，或者其他能够实现数据包过滤的设备。

[0032] 第二方面，本申请实施例中提供了一种业务流的控制方法，包括：

[0033] 网络设备获取业务流策略；

[0034] 所述网络设备将所述业务流策略发送给路由设备，所述业务流策略用于指示所述路由设备根据所述业务流策略对下行数据包执行数据包过滤。

[0035] 通过上述方式，由网络设备获取业务流策略，并发送给路由设备，并不是将业务流策略配置在路由设备中，使得路由设备获取到多个网络设备发送的业务流策略，从而使得路由设备获取到的业务流策略更多样化，使得过滤存在安全威胁的数据包更准确，提高了终端设备的安全性。

[0036] 在一种可能的设计中，所述业务流策略包括：至少一个数据包过滤规则以及每一个数据包过滤规则对应的操作信息。

[0037] 相比现有技术中采用针对所有数据包过滤规则均采用一种操作信息而言，使得针对数据包的处理更加多样化，使得过滤存在安全威胁的数据包更准确，提高了终端设备的安全性。

[0038] 在一种可能的设计中，所述网络设备获取业务流策略，包括：

[0039] 所述网络设备接收由终端设备发来的业务流策略。

[0040] 通过终端设备将自身的业务流策略发送给网络设备，从而由网络设备将业务流策略发送给路由设备，使得路由设备基于终端设备的要求执行业务流的控制，避免对终端设备带来财产损失或者隐私信息泄露等安全风险。

[0041] 在一种可能的设计中，所述网络设备获取业务流策略，包括：

[0042] 所述网络设备从运营商应用平台获取到所述业务流策略。

[0043] 在一种可能的设计中，所述网络设备获取业务流策略之前，所述方法还包括：

[0044] 所述网络设备接收所述运营商应用平台发送的用户属性与业务流策略的对应关系；

[0045] 终端设备注册到所述网络设备的过程中，所述网络设备获取所述终端设备的用户属性；

[0046] 所述网络设备获取业务流策略，包括：

[0047] 所述网络设备确定所述终端设备的用户属性对应的业务流策略。

[0048] 通过上述设计，针对不同的用户配置不同的业务流策略，从而在保证终端设备的安全性的基础上，实现了基于垂直行业应用模式的差异化灵活控制。

[0049] 在一种可能的设计中，所述网络设备获取业务流策略之前，所述方法还包括：

[0050] 终端设备注册到所述网络设备的过程中，所述网络设备获取所述终端设备的用户属性；

[0051] 所述网络设备获取业务流策略，包括：

[0052] 所述网络设备从所述运营商应用平台获取所述用户属性对应的业务流策略。

[0053] 通过上述设计，针对不同的用户配置不同的业务流策略，从而在保证终端设备的安全性的基础上，实现了基于垂直行业应用模式的差异化灵活控制。

[0054] 在一种可能的设计中，所述方法还包括：

[0055] 终端设备注册到所述网络设备的过程中，所述网络设备将安全服务器的通信地址发送给终端设备，以便所述终端设备基于所述通信地址将所述业务流策略通过安全服务器发送给所述路由设备。

[0056] 在一种可能的设计中，所述路由设备为网关设备或者防火墙。

[0057] 第三方面，本申请实施例还提供了一种业务流的控制方法，包括：

[0058] 路由设备获取业务流策略；

[0059] 所述路由设备接收到下行数据包时，依据所述业务流策略对所述下行数据包执行数据包过滤。

[0060] 在一种可能的设计中，所述路由设备接收业务流策略，包括：

[0061] 所述路由设备接收由终端设备发来的业务流策略；或者，

[0062] 所述路由设备接收由运营商应用平台发来的业务流策略。

[0063] 通过上述设计，不是将业务流策略配置在路由设备中，而是由路由设备接收终端设备或者运营商应用平台发送的业务流策略，从而保证了业务流策略的更新，提高了终端设备的安全性。

[0064] 在一种可能的设计中，所述业务流策略包括：至少一个数据包过滤规则以及每一个数据包过滤规则对应的执行操作；

[0065] 所述路由设备依据所述业务流策略对所述下行数据包执行数据包过滤，包括：

[0066] 所述路由设备确定所述下行数据包所匹配的数据包过滤规则，并对所述下行数据包执行所匹配的数据包过滤规则对应的执行操作。

[0067] 在一种可能的设计中，所述路由设备为网关设备或者防火墙。

[0068] 第四方面，本申请实施例提供了一种业务流的控制方法，包括：

[0069] 安全服务器接收终端设备发送的业务流策略；

[0070] 所述安全服务器将所述业务流策略发送给路由设备，所述业务流策略用于指示所述路由设备根据所述业务流策略对下行数据包执行数据包过滤。

[0071] 通过上述设计，由终端设备自己生成业务流策略发送给路由设备，从而路由设备根据终端设备的要求，丢弃存在安全威胁的数据包，通过安全的数据包，从而避免对终端设备带来财产损失或者隐私信息泄露等安全风险。另外，终端设备将业务流策略发送给安全服务器，由安全服务器转发给路由设备，由于安全服务器的安全性高，因此提高了业务流策略的安全性。

[0072] 在一种可能的设计中，所述业务流策略是预配置在所述终端设备上的；或者，

[0073] 所述业务流策略是由所述终端设备基于用户输入的存在安全威胁的数据包信息生成的；或者，

[0074] 所述业务流策略是所述终端设备基于识别的存在安全威胁的下行数据包生成的；或者，

[0075] 所述业务流策略是所述终端设备基于识别的存在安全威胁的且经用户确认后的下行数据包生成的。

[0076] 在一种可能的设计中，所述路由设备为网关设备或者防火墙。

[0077] 第五方面，本申请实施例提供了一种业务流的控制方法，包括：

[0078] 运营商应用平台确定业务流策略；

[0079] 所述运营商应用平台将所述业务流策略发送给路由设备，所述业务流策略用于指示所述路由设备根据所述业务流策略对下行数据包执行数据包过滤。

[0080] 在一种可能的设计中，所述方法还包括：

[0081] 所述运营商平台接收网络设备发送的业务流策略请求消息，所述业务流策略请求消息携带终端设备的用户属性；

[0082] 所述运营商应用平台获取业务流策略，包括：

[0083] 所述运营商平台根据预配置用户属性与业务流策略的对应关系，确定所述终端设备的用户属性对应的业务流策略。

[0084] 通过上述设计，针对不同的用户配置不同的业务流策略，从而在保证终端设备的安全性的基础上，实现了基于垂直行业应用模式的差异化灵活控制。

[0085] 在一种可能的设计中，所述路由设备为网关设备或者防火墙。

[0086] 第五方面，本申请实施例提供了一种业务流的控制装置，包括：

[0087] 处理单元，用于生成业务流策略；

[0088] 发送单元，用于发送所述处理单元生成业务流策略给路由设备，所述业务流策略用于指示所述路由设备根据所述业务流策略对下行数据包执行数据包过滤。

[0089] 在一种可能的设计中，所述处理单元，具体用于：

[0090] 基于业务流策略配置信息生成所述业务流策略；或者，

[0091] 基于用户输入的存在安全威胁的数据包信息生成所述业务流策略；或者，

[0092] 识别存在安全威胁的下行数据包，并基于识别的所述下行数据包生成所述业务流策略；或者，

[0093] 识别存在安全威胁的下行数据包，基于经过用户确认的存在安全威胁的下行数据包生成所述业务流策略。

[0094] 在一种可能的设计中，所述装置还包括：

[0095] 接收单元，用于接收所述下行数据包；

[0096] 所述处理单元，在识别存在安全威胁的下行数据包时，具体用于：

[0097] 若确认所述终端设备上没有监听所述下行数据包的端口，则识别所述下行数据包存在安全威胁。

[0098] 在一种可能的设计中，所述发送单元，具体用于：

[0099] 通过网络设备将所述业务流策略发送给所述路由设备；或者，

[0100] 通过安全服务器将所述业务流策略发送给所述路由设备。

[0101] 在一种可能的设计中，所述装置还包括：

[0102] 接收单元，用于在所述终端设备注册到所述网络设备的过程中，接收所述网络设备发送的所述安全服务器的通信地址；

[0103] 所述发送单元，在通过安全服务器将所述业务流策略发送给所述路由设备时，具体用于：

[0104] 基于所述安全服务器的通信地址将业务流策略发送给所述安全服务器。

[0105] 在一种可能的设计中，所述业务流策略包括：至少一个数据包过滤规则以及每一个数据包过滤规则对应的操作信息。

[0106] 在一种可能的设计中，所述路由设备为网关设备或者防火墙。

[0107] 第六方面，本申请实施例提供了一种业务流的控制装置，包括：

[0108] 获取单元，用于获取业务流策略；

[0109] 发送单元，用于将所述业务流策略发送给路由设备，所述业务流策略用于指示所述路由设备根据所述业务流策略对下行数据包执行数据包过滤。

[0110] 在一种可能的设计中，所述业务流策略包括：至少一个数据包过滤规则以及每一个数据包过滤规则对应的操作信息。

[0111] 在一种可能的设计中，还包括：

[0112] 接收单元，用于接收由终端设备发来的业务流策略。

[0113] 在一种可能的设计中，所述获取单元，具体用于：

[0114] 从运营商应用平台获取到所述业务流策略。

[0115] 在一种可能的设计中，所述接收单元，还用于在所述获取单元获取业务流策略之前，接收所述运营商应用平台发送的用户属性与业务流策略的对应关系；

[0116] 所述获取单元，具体用于在终端设备注册到所述网络设备的过程中，获取所述终端设备的用户属性，并确定所述终端设备的用户属性对应的业务流策略。

[0117] 在一种可能的设计中，所述获取单元，还用于在获取业务流策略之前，在终端设备注册到所述网络设备的过程中，获取所述终端设备的用户属性：

[0118] 所述获取单元，在获取业务流策略时，具体用于从所述运营商应用平台获取所述用户属性对应的业务流策略。

[0119] 在一种可能的设计中，所述发送单元，还用于：

[0120] 在终端设备注册到所述网络设备的过程中，将安全服务器的通信地址发送给终端设备，以便所述终端设备基于所述通信地址将所述业务流策略通过安全服务器发送给所述路由设备。

[0121] 在一种可能的设计中，所述路由设备为网关设备或者防火墙。

[0122] 基于与方法实施例同样的发明构思，第七方面，本申请实施例还提供了一种应用于终端设备的业务流的控制装置，该装置包括：

[0123] 收发器，处理器以及存储器。

[0124] 存储器用于存储处理器所执行的程序代码。

[0125] 所述处理器通过收发器收发数据，具体用于执行存储器存储的程序代码，实现第一方面或第一方面的任一种设计所述的方法。

[0126] 基于与方法实施例同样的发明构思，第八方面，本申请实施例还提供了一种应用于网络设备的业务流的控制装置，该装置包括：

[0127] 通信接口，处理器以及存储器。

[0128] 存储器用于存储处理器所执行的程序代码。

[0129] 所述处理器通过通信接口收发数据，具体用于执行存储器存储的程序代码，实现第二方面或第二方面的任一种设计所述的方法。

[0130] 第九方面，本申请实施例中还提供一种计算机存储介质，该存储介质中存储软件程序，该软件程序在被一个或多个处理器读取并执行时可实现第一方面或上述第一方面的任意一种设计提供的方法，或者实现第二方面或者第二方面的任一种设计所提供的方法，或者实现第三方面或者第三方面的任一种设计所提供的方法，或者实现第四方面或者第四方面的任一种设计所提供的方法。

附图说明

[0131] 图1为本申请实施例提供的一种移动通信网络系统架构图；

[0132] 图2为本申请实施例提供的一种业务流的控制方法流程图；

[0133] 图3为本申请实施例提供的一种业务流的控制方法流程示意图；

[0134] 图4为本申请实施例提供的另一种移动通信网络系统架构图；

[0135] 图5为本申请实施例提供的另一种业务流的控制方法流程示意图；

[0136] 图6为本申请实施例提供的另一种业务流的控制方法流程图；

[0137] 图7为本申请实施例提供的又一种业务流的控制方法流程图；

[0138] 图8为本申请实施例提供的再一种业务流的控制方法流程图；

[0139] 图9为本申请实施例提供的一种应用于终端设备的业务流的控制装置示意图；

[0140] 图10为本申请实施例提供的另一种应用于终端设备的业务流的控制装置示意图；

[0141] 图11为本申请实施例提供的一种应用于网络设备的业务流的控制装置示意图；

[0142] 图12为本申请实施例提供的另一种应用于网络设备的业务流的控制装置示意图。

具体实施方式

[0143] 本申请实施例可以适用于2G(第二代移动通信系统)、3G(第三代移动通信系统)或者4G(第四代移动通信系统)，如长期演进(英文:Long Term Evolution，简称:LTE)系统，或者还可以为5G(第五代移动通信系统)，如5G系统架构(英文:5G System Architecture，简称:5GS)。

[0144] 参见图1所示，为本申请实施例提供的一种可能的移动通信网络系统逻辑架构图。应理解，本申请实施例并不限于图1所示的系统中。如图1所示，本申请实施例提供的移动通信网络系统包括:终端设备、基站、网络设备、网关设备、数据网络，还可以包括防火墙。针对下行数据包进行过滤的操作由网关设备或者防火墙执行，或者其他能够执行过滤功能的网络设备，本申请在此不作具体限定。

[0145] 网络设备可以是控制面功能网元(英文:Control Plane，简称:CP)、核心控制功能(英文:Core Control Function，简称:CCF)、GPRS服务支撑节点(Serving GPRS Support Node，SGSN)、移动性管理实体(英文Mobility Management Entity，简称MME)。其中，网络设备负责用户设备的设备注册、安全认证、移动性管理和位置管理等。控制面功能网元或者核心控制功能可以包括鉴权与移动性管理功能(英文:Authentication and Mobility Management Function，简称:AMF)、会话管理功能(英文:Session Management Function，简称:SMF)等功能。其中，AMF负责UE移动性管理、NAS消息路由和SMF选择等。SMF负责会话管理，如会话创建，修改，删除等，用户面功能(英文:User Plane Function，简称:UPF)选择，UE IP地址分配等。

[0146] 网关设备可以是用户面网元(英文:User Plane function，简称:UPF)、分组数据网(英文:packet data network，简称:PDN)网关(英文:Gate Way，简称:GW)、服务网关(英文:Serving Gate Way，简称:S-GW)、GPRS网关支撑节点(Gateway GPRS Support Node，GGSN)。网关设备用于转发用户设备和外部数据网络之间的数据包。

[0147] 基站还可以称为接入节点(英文:Access Node，简称:AN)，为终端设备提供无线接入服务。接入节点具体可以是全球移动通信(英文:Global System for Mobile communication，简称:GSM)系统或码分多址(英文:Code Division Multiple Access，简称:CDMA)系统中的基站(英文:Base Transceiver Station，简称:BTS)，也可以是宽带码分多址(英文:Wideband Code Division Multiple Access，简称:WCDMA)系统中的基站(NodeB)，还可以是LTE系统中的演进型基站(英文:Evolutional Node B，简称:eNB或

eNodeB)，或者是未来5G网络中的基站设备、小基站设备、无线访问节点(WiFi AP)、无线互通微波接入基站(英文:Worldwide Interoperability for Microwave Access Base Station，简称:WiMAX BS)等，本申请对此并不限定。

[0148] 终端设备，也可称为接入终端、用户设备(英文:User Equipment，简称:UE)，用户单元、用户站、移动站、移动台、远方站、远程终端、移动设备、用户终端、无线通信设备、用户代理或用户装置等。终端设备可以是蜂窝电话、无绳电话、会话启动协议(英文:Session Initiation Protocol，简称:SIP)电话、无线本地环路(英文:Wireless Local Loop，简称:WLL)站、个人数字处理(英文:Personal Digital Assistant，简称:PDA)、具有无线通信功能的手持设备、计算设备或连接到无线调制解调器的其它处理设备、车载设备、可穿戴设备、物联网终端设备，比如火灾检测传感器、智能水表/电表、工厂监控设备等等。

[0149] 另外系统架构中还可以包括数据网络(英文:Data Network，简称:DN)，为用户提供数据传输服务，可以是PDN网络，如因特网(Internet)、IP多媒体业务(英文:IP Multi-media Service，简称:IMS)等。

[0150] 需要说明的是，本申请中涉及的多个，是指两个或两个以上。“和/或”，描述关联对象的关联关系，表示可以存在三种关系，例如，A和/或B，可以表示:单独存在A，同时存在A和B，单独存在B这三种情况。字符“/”一般表示前后关联对象是一种“或”的关系。同时，应当理解，尽管在本申请实施例中可能采用术语第一、第二等来描述各种消息，但这些消息不应限于这些术语。这些术语仅用来将消息彼此区分开。

[0151] 另外，本申请实施例中涉及的业务流策略可以包括数据包过滤规则。针对满足数据包过滤规则的数据包执行预配置的操作。业务流策略还可以包括多种数据包过滤规则以及每一种数据包过滤规则对应的操作信息，针对满足某一种数据包过滤规则的数据包执行该某一种数据包过滤规则对应的操作。数据包过滤规则中可以包括:源网际互连协议(英文:Internet Protocol，简称:IP)地址、目的IP地址、协议类型、源端口、目的端口等数据包的包头信息。预配置的操作，或者业务流策略中包括的操作信息可以为丢弃(block)/屏蔽(screen)/通过(pass)等。

[0152] 本申请提供一种业务流的控制方法及装置，用以解决现有存在的安全性差的问题。其中，方法和装置是基于同一发明构思的，由于方法及装置解决问题的原理相似，因此装置与方法的实施可以相互参见，重复之处不再赘述。

[0153] 下面结合附图对本申请实施例作具体说明。

[0154] 一种可能的应用场景中，由终端设备生成业务流策略并发送给用于执行数据包过滤的路由设备，另一种可能的应用场景中，运营商应用平台中配置业务流策略，从而由运营商应用平台将业务流策略发送给用于执行数据包过滤的路由设备。

[0155] 下面针对由终端设备生成业务流策略并发送给用于执行数据包过滤的路由设备的场景进行描述:

[0156] 参见图2所示，为本申请实施例提供的一种业务流的控制方法，所述方法的流程如下:

[0157] S201，终端设备生成业务流策略。

[0158] S202，所述终端设备发送业务流策略给所述路由设备，所述业务流策略用于指示所述路由设备根据所述业务流策略对下行数据包执行数据包过滤。

[0159] S203,所述路由设备接收到所述终端设备发送的所述业务流策略。

[0160] S204,所述路由设备接收到下行数据包时,依据所述业务流策略对所述下行数据包执行数据包过滤。

[0161] 在上述应用场景中,一种可能的实现方式中,所述业务流策略由终端设备发送且由网络设备转发。具体的,参见图3所示,图3中,以上述路由设备为网关设备或者防火墙为例进行说明。

[0162] S301,终端设备附着到网络设备上,并建立到网关设备的数据连接。终端设备附着到网络设备的过程也可以认为是终端设备注册到网络侧过程,具体的附着过程可以参见现有技术提供的方案,本申请实施例在此不再赘述。

[0163] S302,终端设备生成业务流策略,并将生成的业务流策略发送给网络设备。

[0164] 所述业务流策略可以包括多个数据包过滤规则和以及每个数据包过滤规则对应的操作信息。每个数据包过滤规则包含源IP地址、目的IP地址、协议类型、源端口、目的端口等信息。每个数据包过滤规则对应的操作信息,即对匹配该数据包过滤规则的数据包执行相应的操作,操作可以为丢弃(block)/屏蔽(screen)/通过(pass)等。

[0165] 具体的,终端设备可以通过如下的方式生成业务流策略:

[0166] 第一种实现方式:

[0167] 业务流策略预先配置在终端设备中,则终端设备基于预配置的业务流策略生成所述业务流策略。

[0168] 第二种实现方式:

[0169] 所述终端设备识别存在安全威胁的下行数据包,并基于识别到的所述下行数据包生成所述业务流策略。具体的,所述终端设备收到可能存在安全威胁的下行数据包后,获取该下行数据包中的源IP地址、目的IP地址、协议类型、源端口、目的端口等信息,从而生成业务流策略。

[0170] 其中,识别存在安全威胁的下行数据包的规则可以预先配置在终端设备上,如终端设备收到某个下行数据包后,确定没有监听该下行数据包的端口,则终端设备识别该下行数据包存在安全威胁。

[0171] 第三种实现方式:

[0172] 所述终端设备识别存在安全威胁的下行数据包,基于经过用户确认的存在安全威胁的下行数据包生成所述业务流策略。

[0173] 具体的,当终端设备识别收到可能存在安全威胁的下行数据包后,提供界面由用户确认。然后基于用户确认的存在安全威胁的数据包生成业务流策略。

[0174] 第四种实现方式:

[0175] 所述终端设备识别用户的输入信息得到所述业务流策略。

[0176] 具体的,可以由持有所述终端设备的用户,通过终端设备提供的界面输入业务流策略。

[0177] 在上述第二种实现方式以及第三种实现方式中,终端设备识别存在安全威胁的下行数据包,并根据下行数据包生成业务流策略后,可以不马上将业务流策略通知给路由设备,而是存储该业务流策略,然后一定的周期后通知,如1分钟后将存储的一个或者多个业务流策略通知给路由设备。终端设备还可以每次识别到存在安全威胁的下行数据包后,则

基于该存在安全威胁的数据包生成业务流策略，并实时得将该业务流策略通知给路由设备。

[0178] S303，所述网络设备在接收到终端设备发送的业务流策略后，所述网络设备将业务流策略发送给网关设备/防火墙。

[0179] S304，网关设备/防火墙收到来自数据网络的下行数据包。

[0180] S305，所述网关设备/防火墙确定所述下行数据包所匹配的数据包过滤规则，并针对所述下行数据执行所匹配的数据包过滤规则对应的操作。比如丢弃该下行数据包，或者将该下行数据包发送给终端设备。

[0181] 可选地，S306，所述网关设备/防火墙确定针对下行数据包执行的操作为通过时，则将下行数据包发送给终端设备。

[0182] 通过上述方案，网关设备或者防火墙根据终端设备发来的业务流策略，即网关设备或者防火墙基于终端设备的要求，丢弃存在安全威胁的数据包，通过安全的数据包，从而避免对终端设备带来财产损失或者隐私信息泄露等安全风险。

[0183] 在上述应用场景中，另一种可能的实现方式中，可以在移动通信网络系统中配置一个新的功能实体，即负责终端设备的业务流策略管理的安全服务器，从而终端设备发送给网关设备或者防火墙的业务流策略由该安全服务器转发。参见图4所示为增加安全服务器的移动通信网络系统逻辑架构图。

[0184] 具体的，业务流的控制方法流程参见图5所示。

[0185] S501，终端设备附着到网络设备上，并建立到网关设备的数据连接。

[0186] 在步骤S501中，终端设备与注册到网络设备的过程中，网络设备将安全服务器的通信地址(比如，IP地址)通知给终端设备，所述安全服务器的通信地址可以预先配置在网络设备上。网络设备的通信地址也可以通过操作维护中心(英文：Operation and maintenance，简称：O&M)，或者其他网络获取。

[0187] S502，终端设备生成业务流策略，并将生成的业务流策略发送给安全服务器。

[0188] 所述业务流策略可以包括多个数据包过滤规则和以及每个数据包过滤规则对应的操作信息。每个数据包过滤规则包含源IP地址、目的IP地址、协议类型、源端口、目的端口等信息。每个数据包过滤规则对应的操作信息，即对匹配该数据包过滤规则的数据包执行相应的操作，操作可以为丢弃(block)/屏蔽(screen)/通过(pass)等。

[0189] 具体的，终端设备生成业务流策略的方式可以参见图3所对应的实施例中描述的方式，本申请实施例在此不再赘述。

[0190] S503，安全服务器在接收到所述终端设备发送的业务流策略后，将业务流策略信息发送给网关设备/防火墙；

[0191] S504，网关设备/防火墙收到来自数据网络的下行数据包。

[0192] S505，所述网关设备/防火墙确定所述下行数据包所匹配的数据包过滤规则，并针对所述下行数据执行所匹配的数据包过滤规则对应的操作。比如丢弃该下行数据包，或者将该下行数据包发送给终端设备。

[0193] 可选地，S506，所述网关设备/防火墙确定针对下行数据包执行的操作为通过时，则将下行数据包发送给终端设备。

[0194] 通过上述方案，网关设备或者防火墙通过安全服务器来接收终端设备发来的业务

流策略，从而网关设备或者防火墙根据终端设备发来的业务流策略，即终端设备的要求，丢弃存在安全威胁的数据包，通过安全的数据包，由于安全服务器的安全性比较高，从而保证业务流策略的安全性，从而避免对终端设备带来财产损失或者隐私信息泄露等安全风险。

[0195] 下面针对运营商应用平台中配置业务流策略场景进行具体描述。运营商应用平台为应用平台管理网络内的设备，安全性比较高。

[0196] 参见图6所示，为本申请实施例中提供的业务流的控制方法流程图，所述方法包括：

[0197] S601，运营商应用平台确定业务流策略。

[0198] S602，运营商应用平台将所述业务流策略发送给路由设备，所述业务流策略用于指示所述路由设备根据所述业务流策略对下行数据包执行数据包过滤。

[0199] S603，所述路由设备接收到所述运营商应用平台发送的所述业务流策略。

[0200] S604，所述路由设备在接收下行数据包时，依据所述业务流策略对所述下行数据包执行数据包过滤。

[0201] 在上述应用场景中，运营商应用平台通过网络设备将所述业务流策略发送给路由设备。具体的，参见图7所示，图7中，以上述路由设备为网关设备或者防火墙为例进行说明。

[0202] S701，运营商应用平台将用户属性与业务流策略的对应关系发送给网络设备。

[0203] 其中，运营商应用平台的安全性较高。运营商可以在运营商应用平台上配置用户属性与业务流策略的对应关系。所述用户属性可以为用户的标识，或者用户类型，所述用户标识可以为国际移动用户识别码(英文：International Mobile Subscriber Identification Number，简称：IMSI)，国际移动设备身份码(英文：International Mobile Equipment Identity，简称：IMEI)或者移动台识别号码(英文：Mobile Subscriber International ISDN/PSTN number，简称：MSISDN)等，所述用户类型可以为移动宽带(英文：Mobile Broadband，简称：MBB)用户，车联网用户，物联网用户等。运营商应用平台上可以配置某类用户与业务流策略的对应关系，如只允许车联网用户使用某一些车辆网相关的应用。

[0204] S702，终端设备附着到网络设备上，并建立到网关设备的数据连接。在终端设备附着到网络设备的过程中，即终端设备与注册到网络设备的过程中，所述网络设备获取所述终端设备的用户属性。

[0205] S703，网络设备获取终端设备的用户属性后，确定所述用户属性对应的业务流策略。从而网络设备获取到所述终端设备对应的业务流策略。

[0206] S704，网络设备将业务流策略发送给网关设备/防火墙。

[0207] S705，网关设备/防火墙收到来自数据网络的下行数据包。

[0208] S706，所述网关设备/防火墙确定所述下行数据包所匹配的数据包过滤规则，并对所述下行数据执行所匹配的数据包过滤规则对应的操作。比如丢弃该下行数据包，或者将该下行数据包发送给终端设备。

[0209] 可选地，S707，所述网关设备/防火墙确定对下行数据包执行的操作为通过时，则将下行数据包发送给终端设备。

[0210] 需要说明的是，在图7对应的实施例中，由运营商应用平台将用户属性与业务流策略的对应关系推送给网络设备。具体实施时，也可以在终端设备附着到网络后，网络设备向

应用平台获取该终端设备对应的业务流策略，具体参见图8所示。

[0211] S801，终端设备附着到网络设备上，并建立到网关设备的数据连接。在终端设备附着到网络设备的过程中，即终端设备注册到网络设备的过程中，所述网络设备获取所述终端设备的用户属性。

[0212] S802，网络设备获取终端设备的用户属性后，向所述运营商应用平台获取所述用户属性对应的业务流策略。

[0213] 其中，运营商应用平台上配置有用户属性与业务流策略的对应关系。

[0214] S803，网络设备将业务流策略发送给网关设备/防火墙。

[0215] S804，网关设备/防火墙收到来自数据网络的下行数据包。

[0216] S805，所述网关设备/防火墙确定所述下行数据包所匹配的数据包过滤规则，并对所述下行数据执行所匹配的数据包过滤规则对应的操作。比如丢弃该下行数据包，或者将该下行数据包发送给终端设备。

[0217] 可选地，S806，所述网关设备/防火墙确定对下行数据包执行的操作为通过时，则将下行数据包发送给终端设备。

[0218] 通过上述方案，在运营商应用平台配置不同的用户属性与业务流策略的对应关系，从而针对不同的用户采用不同的业务流策略，比如针对一些特殊要求用户配置该用户适用的业务流策略，例如车联网用户，仅针对车联网相关的数据包才能通过、发送给该车联网用户的终端设备，针对其它的数据包均丢弃，从而保证用户的安全性，避免对用户带来财产损失或者隐私信息泄露等安全风险。另外，上述方案能够实现支持基于垂直行业应用模式的差异化灵活控制。

[0219] 基于与方法实施例同样的发明构思，本申请实施例提供了一种业务流的控制装置，所述装置应用于终端设备，参见图9所示，所述装置包括：

[0220] 处理单元901，用于生成业务流策略；

[0221] 发送单元902，用于发送所述处理单元901生成业务流策略给路由设备，所述业务流策略用于指示所述路由设备根据所述业务流策略对下行数据包执行数据包过滤。

[0222] 在一种可能的设计中，所述处理单元901，具体用于：

[0223] 基于业务流策略配置信息生成所述业务流策略；或者，

[0224] 基于用户输入的存在安全威胁的数据包信息生成所述业务流策略；或者，

[0225] 识别存在安全威胁的下行数据包，并基于识别的所述下行数据包生成所述业务流策略；或者，

[0226] 识别存在安全威胁的下行数据包，基于经过用户确认的存在安全威胁的下行数据包生成所述业务流策略。

[0227] 在一种可能的设计中，所述装置还包括：

[0228] 接收单元903，用于接收所述下行数据包；

[0229] 所述处理单元901，在识别存在安全威胁的下行数据包时，具体用于：

[0230] 若确认所述终端设备上没有监听所述下行数据包的端口，则识别所述下行数据包存在安全威胁。

[0231] 在一种可能的设计中，所述发送单元902，具体用于：

[0232] 通过网络设备将所述业务流策略发送给所述路由设备；或者，

[0233] 通过安全服务器将所述业务流策略发送给所述路由设备。

[0234] 在一种可能的设计中，所述装置还包括：

[0235] 接收单元903，用于在所述终端设备注册到所述网络设备的过程中，接收所述网络设备发送的所述安全服务器的通信地址；

[0236] 所述发送单元902，在通过安全服务器将所述业务流策略发送给所述路由设备时，具体用于：

[0237] 基于所述安全服务器的通信地址将业务流策略发送给所述安全服务器。

[0238] 在一种可能的设计中，所述业务流策略包括：至少一个数据包过滤规则以及每一个数据包过滤规则对应的操作信息。

[0239] 在一种可能的设计中，所述路由设备为网关设备或者防火墙。

[0240] 本申请实施例中对单元的划分是示意性的，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，另外，在本申请各个实施例中的各功能单元可以集成在一个处理器中，也可以是单独物理存在，也可以两个或两个以上单元集成在一个单元中。上述集成的单元既可以采用硬件的形式实现，也可以采用软件功能单元的形式实现。

[0241] 如图10所示，应用于终端设备的业务流的控制装置可以包括收发器1010、处理器1020以及存储器1030。上述图9所示的单元对应的实体的硬件可以为处理器1020。处理器1020通过收发器1010收发数据，并用于实现图2、图3、图5～图8中所述的终端设备所执行的方法。在实现过程中，处理流程的各步骤可以通过处理器1020中的硬件的集成逻辑电路或者软件形式的指令完成。处理器1020可以是通用处理器、数字信号处理器、专用集成电路、现场可编程门阵列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申请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任何常规的处理器等。结合本申请实施例所公开的方法的步骤可以直接体现为硬件处理器执行完成，或者用处理器中的硬件及软件单元组合执行完成。处理器1020用于实现上述方法所执行的程序代码可以存储在存储器1030中。存储器1030可以是非易失性存储器，比如硬盘(英文：hard disk drive，缩写：HDD)或固态硬盘(英文：solid-state drive，缩写：SSD)等，还可以是易失性存储器(英文：volatile memory)，例如随机存取存储器(英文：random-access memory，缩写：RAM)。存储器1030是能够用于携带或存储具有指令或数据结构形式的期望的程序代码并能够由计算机存取的任何其他介质，但不限于此。

[0242] 本申请实施例中不限定上述收发器1010、处理器1020以及存储器1030之间的具体连接介质。本申请实施例在图10中以存储器1030、处理器1020以及收发器1010之间通过总线1040连接，总线在图10中以粗线表示，其它部件之间的连接方式，仅是进行示意性说明，并不引以为限。所述总线可以分为地址总线、数据总线、控制总线等。为便于表示，图10中仅用一条粗线表示，但并不表示仅有一根总线或一种类型的总线。

[0243] 本申请实施例提供了一种业务流的控制装置，所述装置应用于网络设备，所述网络设备可以是图1或者图4中所示的网络设备，所述装置包括，参见图11所示：

[0244] 获取单元1101，用于获取业务流策略；

[0245] 发送单元1102，用于将所述业务流策略发送给路由设备，所述业务流策略用于指示所述路由设备根据所述业务流策略对下行数据包执行数据包过滤。

[0246] 在一种可能的设计中，所述业务流策略包括：至少一个数据包过滤规则以及每一

个数据包过滤规则对应的操作信息。

[0247] 在一种可能的设计中，还包括：

[0248] 接收单元1103，用于接收由终端设备发来的业务流策略。

[0249] 在一种可能的设计中，所述获取单元1101，具体用于：

[0250] 从运营商应用平台获取到所述业务流策略。

[0251] 在一种可能的设计中，所述接收单元1103，还用于在所述获取单元1101获取业务流策略之前，接收所述运营商应用平台发送的用户属性与业务流策略的对应关系；

[0252] 所述获取单元1101，具体用于在终端设备注册到所述网络设备的过程中，获取所述终端设备的用户属性，并确定所述终端设备的用户属性对应的业务流策略。

[0253] 在一种可能的设计中，所述获取单元1101，还用于在获取业务流策略之前，在终端设备注册到所述网络设备的过程中，获取所述终端设备的用户属性：

[0254] 所述获取单元1101，在获取业务流策略时，具体用于从所述运营商应用平台获取所述用户属性对应的业务流策略。

[0255] 在一种可能的设计中，所述发送单元1102，还用于：

[0256] 在终端设备注册到所述网络设备的过程中，将安全服务器的通信地址发送给终端设备，以便所述终端设备基于所述通信地址将所述业务流策略通过安全服务器发送给所述路由设备。

[0257] 在一种可能的设计中，所述路由设备为网关设备或者防火墙。

[0258] 本申请实施例中对单元的划分是示意性的，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，另外，在本申请各个实施例中的各功能单元可以集成在一个处理器中，也可以是单独物理存在，也可以两个或两个以上单元集成在一个单元中。上述集成的单元既可以采用硬件的形式实现，也可以采用软件功能单元的形式实现。

[0259] 如图12所示，应用于网络设备的业务流的控制装置可以包括通信接口1210、处理器1220以及存储器1230。上述图11所示的单元对应的实体的硬件可以为处理器1220。处理器1220通过通信接口1210收发数据，并用于实现图2、图3、图5～图8中中所述的网络设备所执行的方法。在实现过程中，处理流程的各步骤可以通过处理器1220中的硬件的集成逻辑电路或者软件形式的指令完成。处理器1220可以是通用处理器、数字信号处理器、专用集成电路、现场可编程门阵列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申请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任何常规的处理器等。结合本申请实施例所公开的方法的步骤可以直接体现为硬件处理器执行完成，或者用处理器中的硬件及软件单元组合执行完成。处理器1220用于实现上述方法所执行的程序代码可以存储在存储器1230中。存储器1230可以是非易失性存储器，比如HDD或SSD等，还可以是易失性存储器，例如RAM。存储器1230是能够用于携带或存储具有指令或数据结构形式的期望的程序代码并能够由计算机存取的任何其他介质，但不限于此。

[0260] 本申请实施例中不限定上述通信接口1210、处理器1220以及存储器1230之间的具体连接介质。本申请实施例在图12中以存储器1230、处理器1220以及通信接口1210之间通过总线1240连接，总线在图12中以粗线表示，其它部件之间的连接方式，仅是进行示意性说明，并不引以为限。所述总线可以分为地址总线、数据总线、控制总线等。为便于表示，图12

中仅用一条粗线表示，但并不表示仅有一根总线或一种类型的总线。

[0261] 本领域内的技术人员应明白，本申请的实施例可提供为方法、系统、或计算机程序产品。因此，本申请可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本申请可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质(包括但不限于磁盘存储器、CD-ROM、光学存储器等)上实施的计算机程序产品的形式。

[0262] 本申请是参照根据本申请的方法、设备(系统)、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

[0263] 这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

[0264] 这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

[0265] 显然，本领域的技术人员可以对本申请进行各种改动和变型而不脱离本申请的精神和范围。这样，倘若本申请的这些修改和变型属于本申请权利要求及其等同技术的范围之内，则本申请也意图包含这些改动和变型在内。

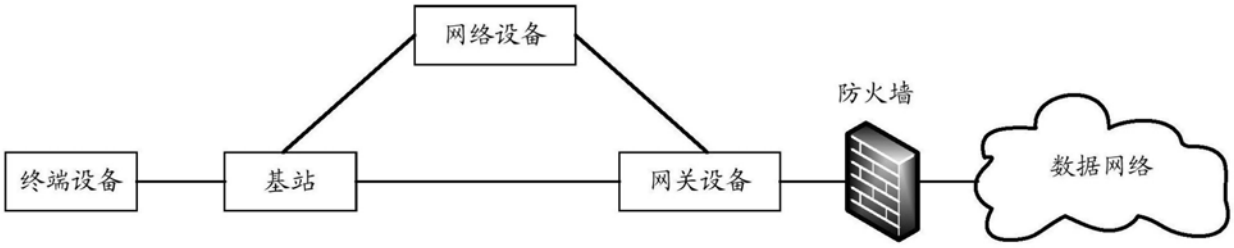

网络设备
防火墙
终端设备
基站
网关设备
数据网络

图1

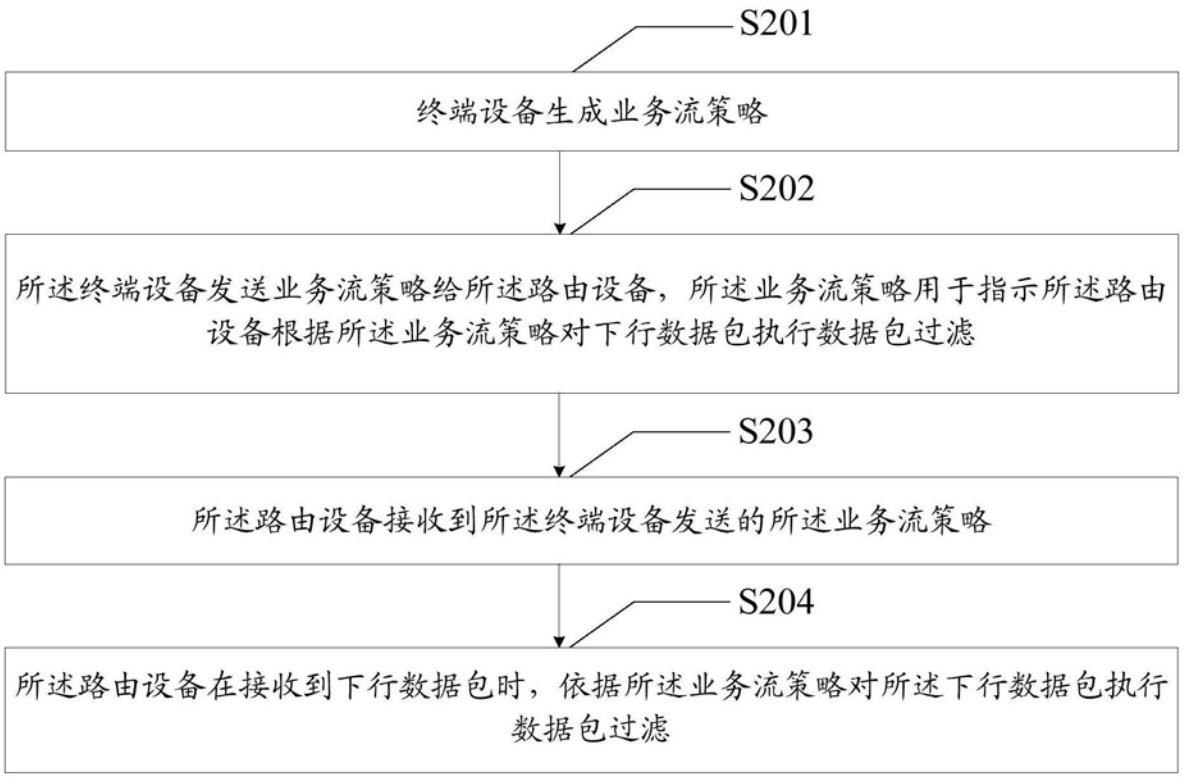

S201
终端设备生成业务流策略
S202
所述终端设备发送业务流策略给所述路由设备，所述业务流策略用于指示所述路由设备根据所述业务流策略对下行数据包执行数据包过滤
S203
所述路由设备接收到所述终端设备发送的所述业务流策略
S204
所述路由设备在接收到下行数据包时，依据所述业务流策略对所述下行数据包执行数据包过滤

图2

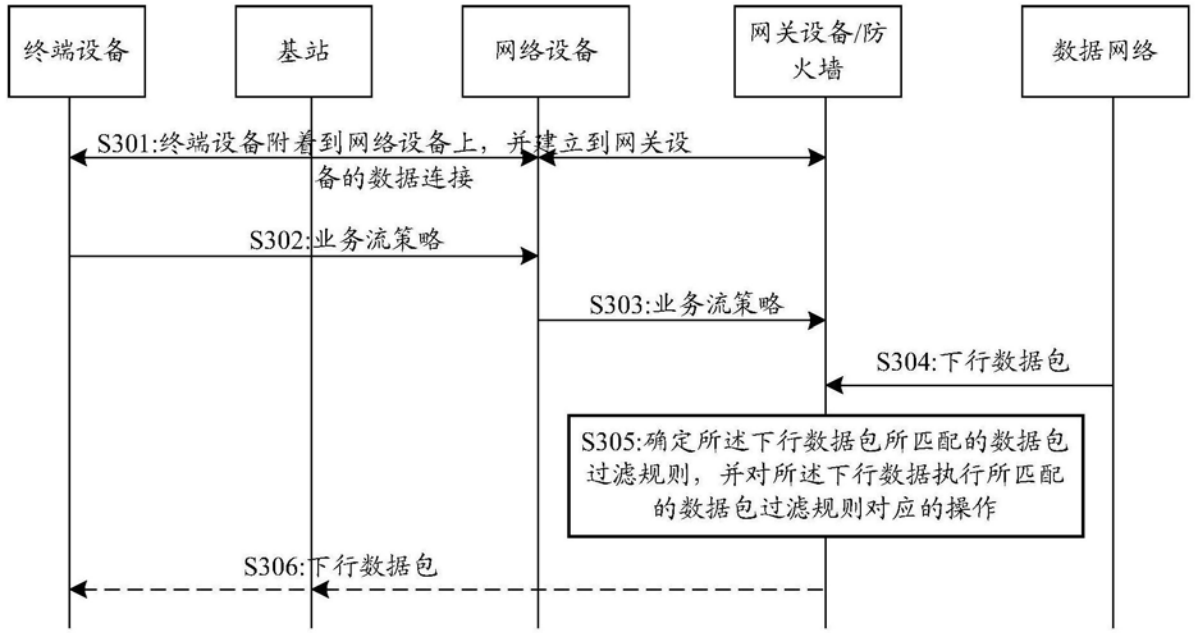

终端设备
基站
网络设备
网关设备/防火墙
数据网络
S301:终端设备附着到网络设备上，并建立到网关设备的数据连接
S302:业务流策略
S303:业务流策略
S304:下行数据包
S305:确定所述下行数据包所匹配的数据包过滤规则，并对所述下行数据执行所匹配的数据包过滤规则对应的操作
S306:下行数据包

图3

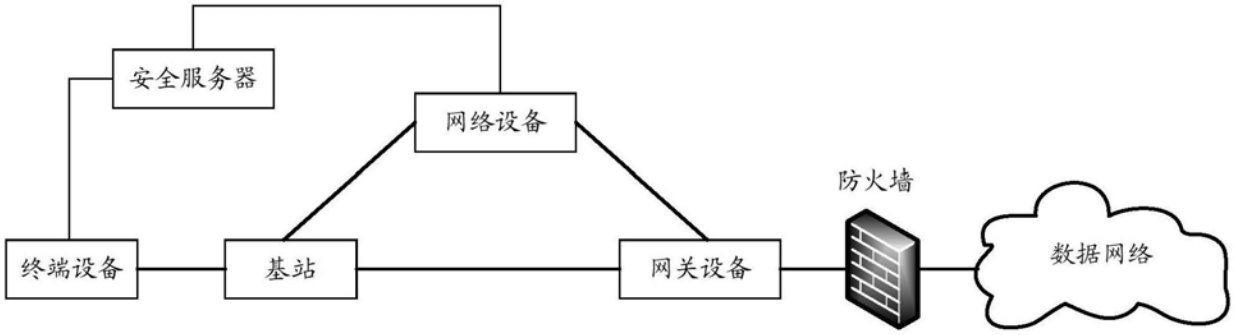

安全服务器
网络设备
防火墙
终端设备
基站
网关设备
数据网络

图4

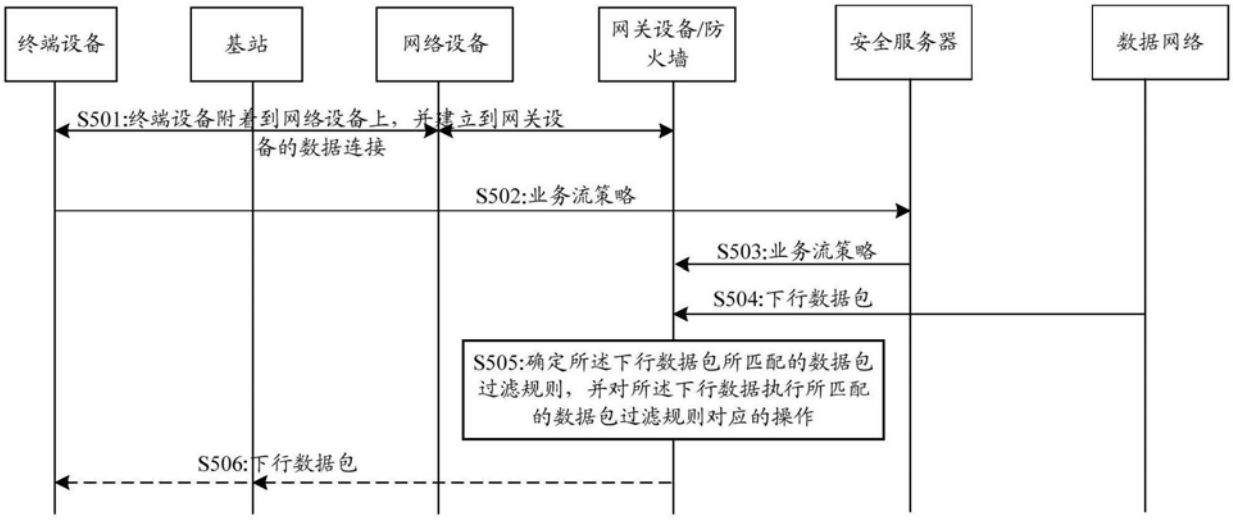

终端设备
基站
网络设备
网关设备/防火墙
安全服务器
数据网络
S501:终端设备附着到网络设备上，并建立到网关设备的数据连接
S502:业务流策略
S503:业务流策略
S504:下行数据包
S505:确定所述下行数据包所匹配的数据包过滤规则，并对所述下行数据执行所匹配的数据包过滤规则对应的操作
S506:下行数据包

图5

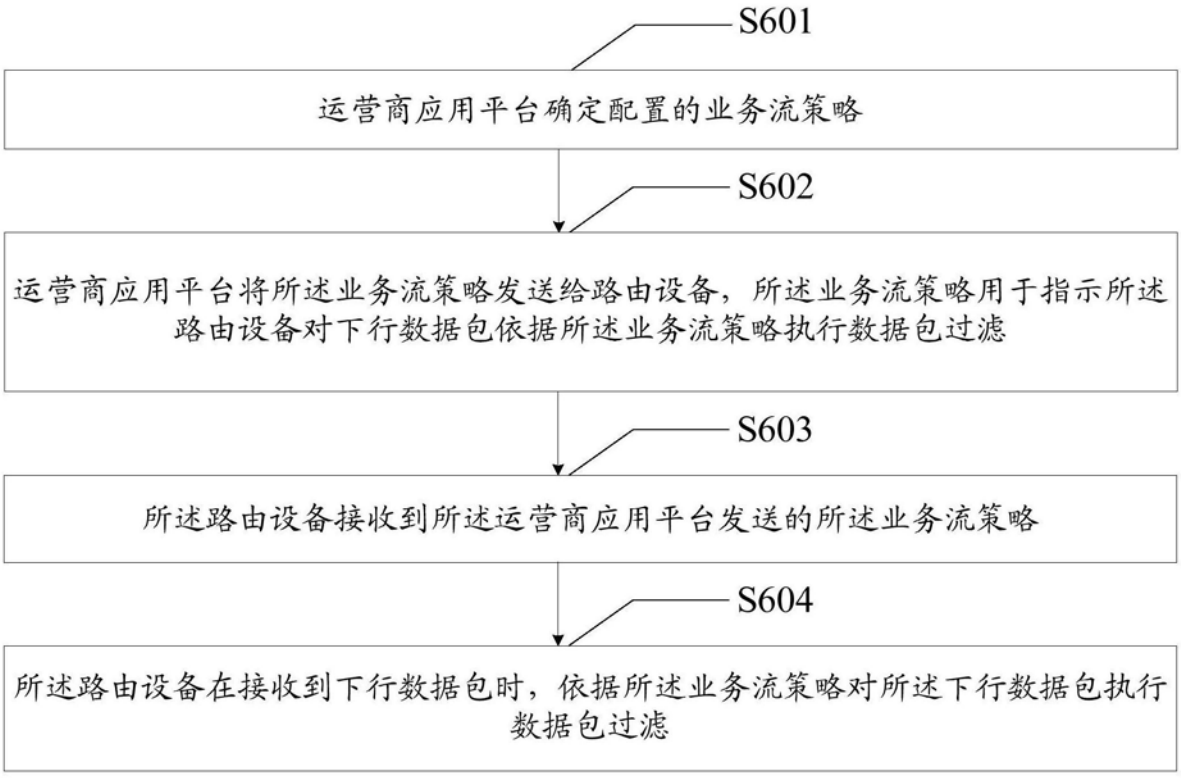

S601
运营商应用平台确定配置的业务流策略
S602
运营商应用平台将所述业务流策略发送给路由设备，所述业务流策略用于指示所述路由设备对下行数据包依据所述业务流策略执行数据包过滤
S603
所述路由设备接收到所述运营商应用平台发送的所述业务流策略
S604
所述路由设备在接收到下行数据包时，依据所述业务流策略对所述下行数据包执行数据包过滤

图6

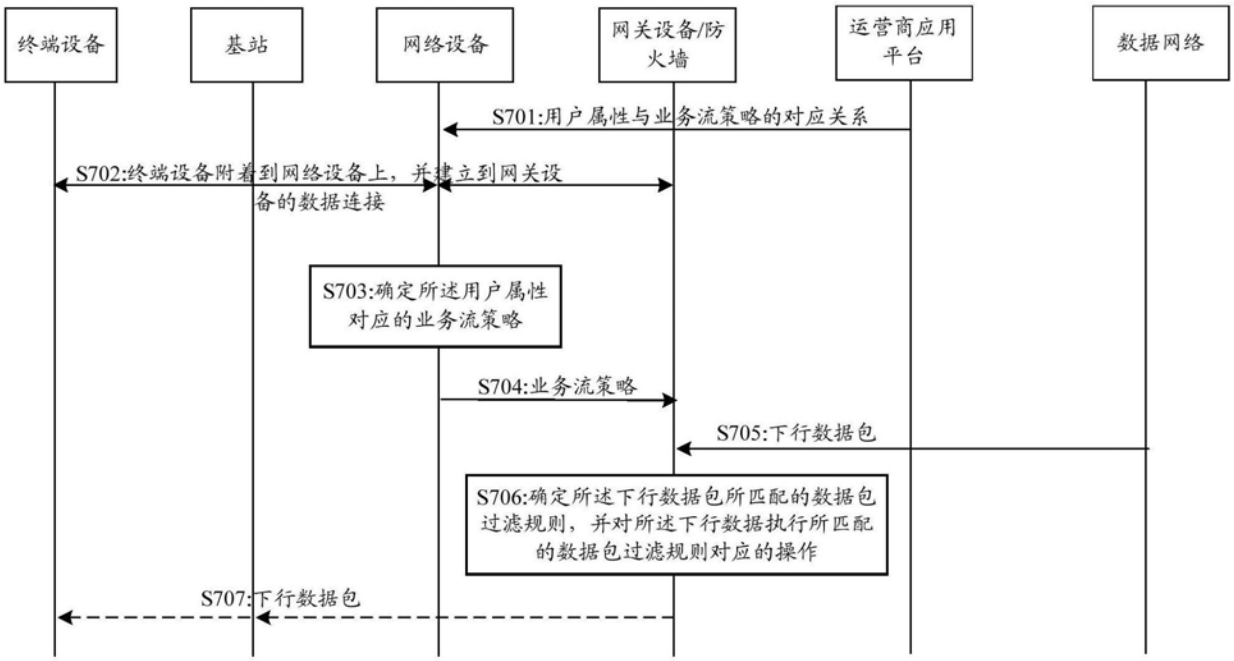

终端设备
基站
网络设备
网关设备/防火墙
运营商应用平台
数据网络
S701:用户属性与业务流策略的对应关系
S702:终端设备附着到网络设备上，并建立到网关设备的数据连接
S703:确定所述用户属性对应的业务流策略
S704:业务流策略
S705:下行数据包
S706:确定所述下行数据包所匹配的数据包过滤规则，并对所述下行数据执行所匹配的数据包过滤规则对应的操作
S707:下行数据包

图7

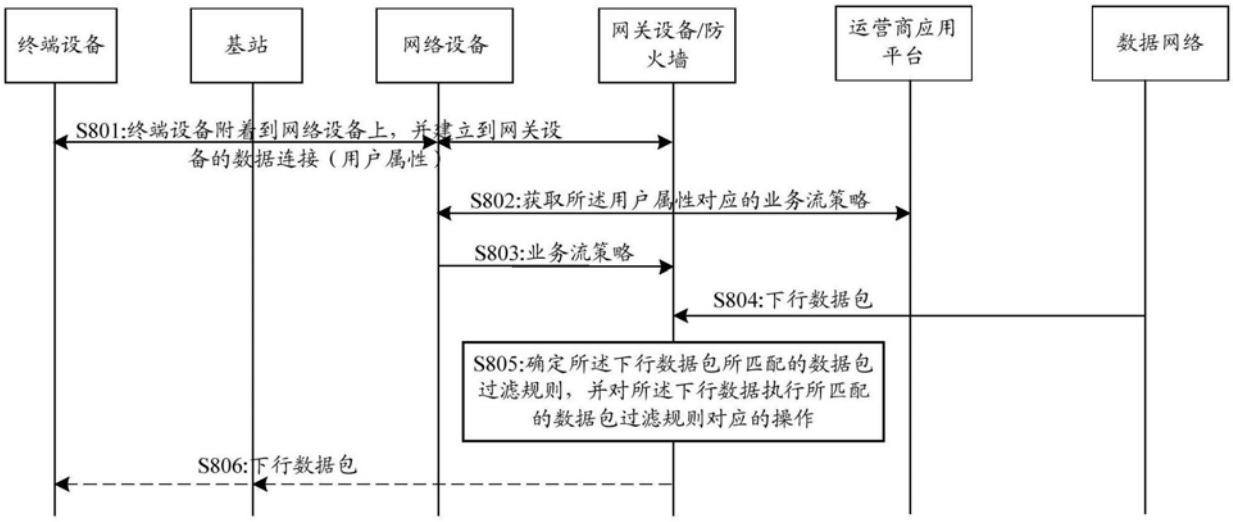

终端设备
基站
网络设备
网关设备/防火墙
运营商应用平台
数据网络
S801:终端设备附着到网络设备上，并建立到网关设备的数据连接（用户属性）
S802:获取所述用户属性对应的业务流策略
S803:业务流策略
S804:下行数据包
S805:确定所述下行数据包所匹配的数据包过滤规则，并对所述下行数据执行所匹配的数据包过滤规则对应的操作
S806:下行数据包

图8

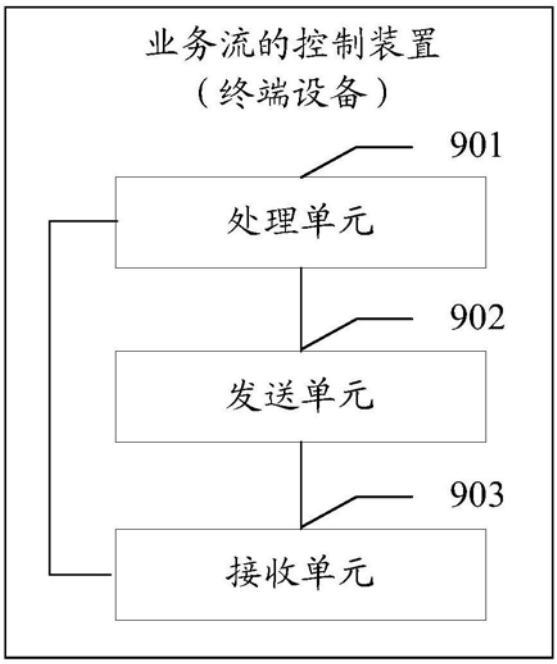

业务流的控制装置
（终端设备）
901
处理单元
902
发送单元
903
接收单元

图9

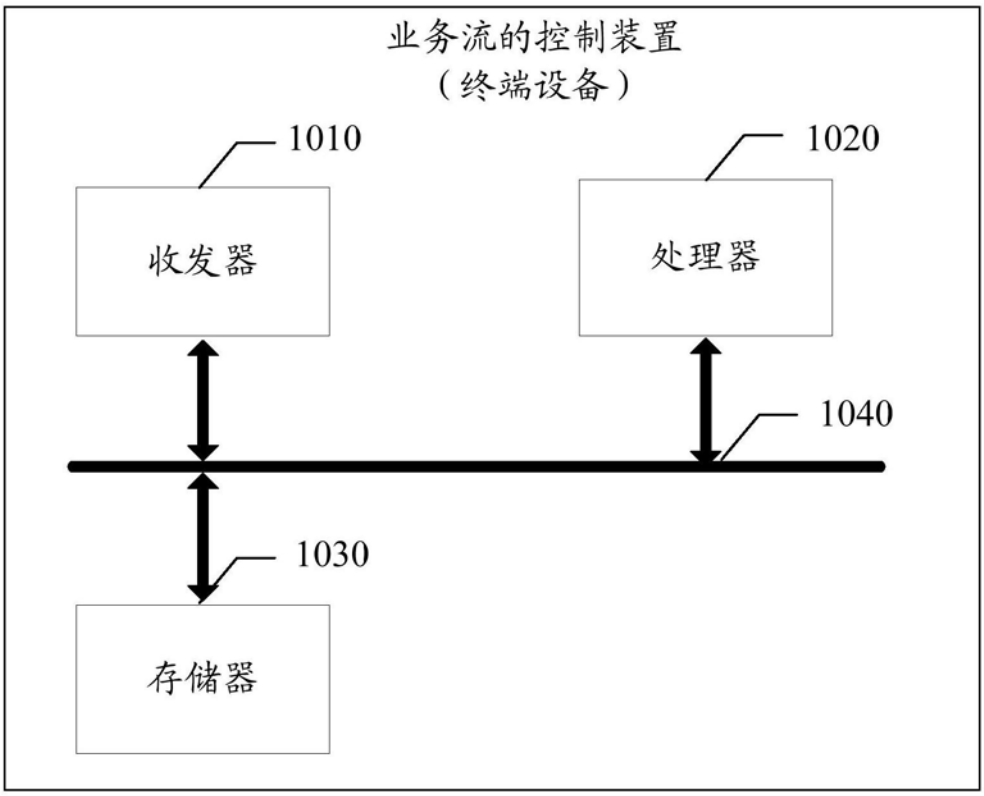

业务流的控制装置
（终端设备）
1010
收发器
1020
处理器
1040
1030
存储器

图10

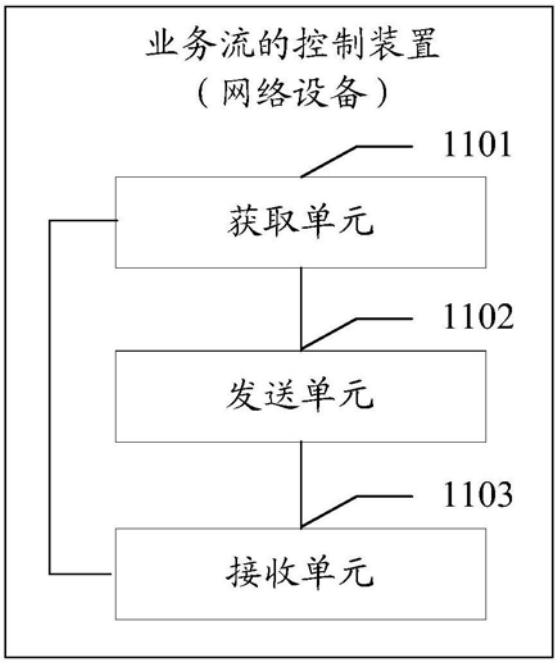

业务流的控制装置
（网络设备）
1101
获取单元
1102
发送单元
1103
接收单元

图11

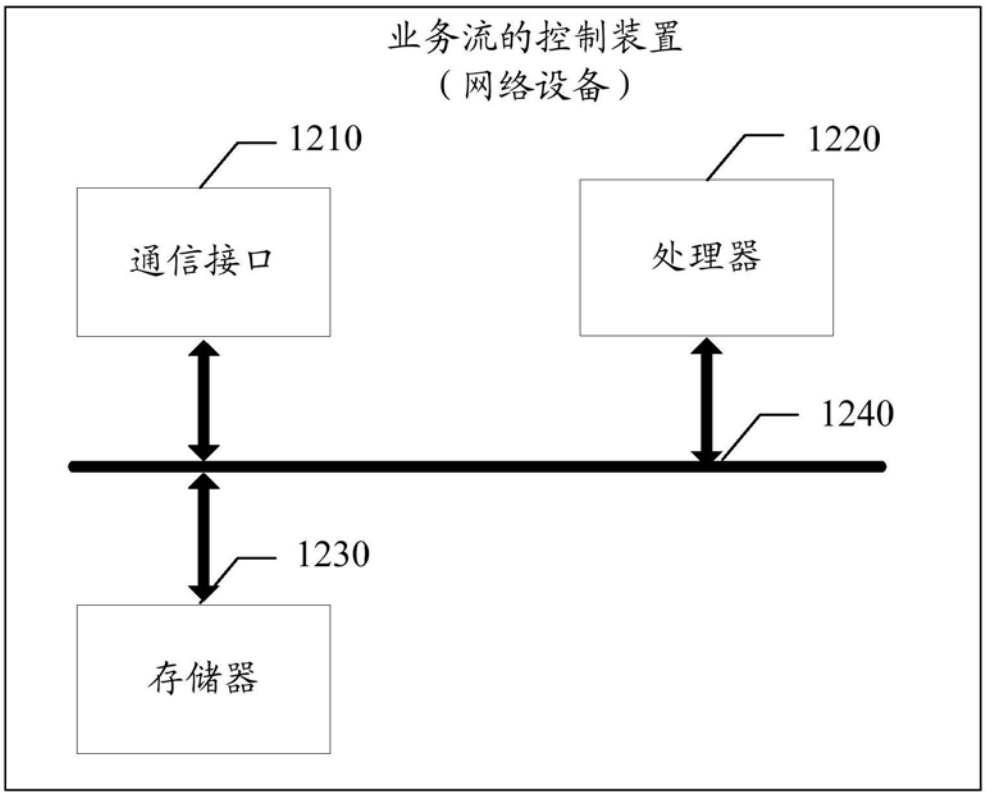

业务流的控制装置
（网络设备）
1210
通信接口
1220
处理器
1240
1230
存储器

图12