(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
2017 年 6 月 22 日 (22.06.2017)

WIPO | PCT

(10) 国际公布号
WO 2017/101627 A1

(51) 国际专利分类号:
H04L 29/06 (2006.01)

(21) 国际申请号: PCT/CN2016/105775

(22) 国际申请日: 2016 年 11 月 14 日 (14.11.2016)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201510954617.1 2015 年 12 月 17 日 (17.12.2015) CN

(71) 申请人: 电信科学技术研究院 (CHINA ACADEMY OF TELECOMMUNICATIONS TECHNOLOGY) [CN/CN]; 中国北京市海淀区学院路 40 号, Beijing 100191 (CN)。

(72) 发明人: 侯云静 (HOU, Yunjing); 中国北京市海淀区学院路 40 号, Beijing 100191 (CN)。 徐晖 (XU, Hui); 中国北京市海淀区学院路 40 号, Beijing 100191 (CN)。 王胡成 (WANG, Hucheng); 中国北京市海淀区学院路 40 号, Beijing 100191 (CN)。

(74) 代理人: 北京同达信恒知识产权代理有限公司 (TDIP & PARTNERS); 中国北京市海淀区知春路 7 号致真大厦 A1304-05 室, Beijing 100191 (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, JP, KE, KG, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) 指定国 (除另有指明，要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO,

[见续页]

(54) Title: CONTENT ACCESS CONTROL METHOD AND RELATED DEVICE

(54) 发明名称 : 一种内容访问控制方法及相关设备

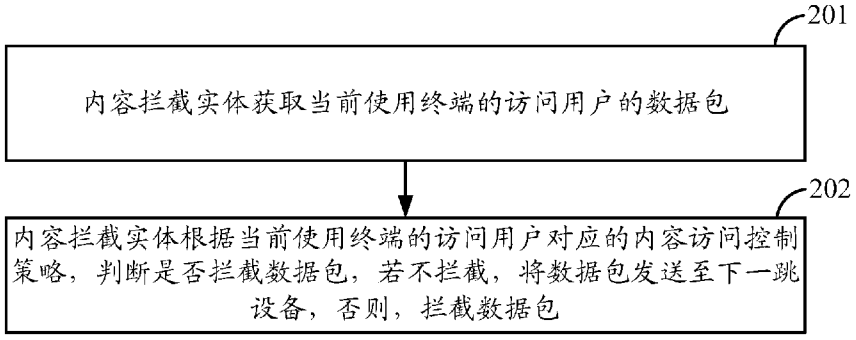

图 2

201 A content blocking entity acquiring a data packet of an access user of a current use terminal

202 The content blocking entity judging, according to a content access control policy corresponding to the access user of the current use terminal, whether to block the data packet, and if not, sending the data packet to a next hop device, and otherwise, blocking the data packet

(57) Abstract: Disclosed are a content access control method and a related device, which are used for distinctively controlling contents requested to be accessed by different users of the same terminal. The method comprises: a content blocking entity acquiring a data packet of an access user of a current use terminal; and the content blocking entity judging, according to a content access control policy corresponding to the access user of the current use terminal, whether to block the data packet, and if not, sending the data packet to a next hop device, and otherwise, blocking the data packet.

(57) 摘要: 本发明公开了一种内容访问控制方法及相关设备，用以对使用同一终端的不同用户所请求访问的内容进行区别控制。该方法为：内容拦截实体获取当前使用终端的访问用户的数据包；所述内容拦截实体根据所述当前使用终端的访问用户对应的内容访问控制策略，判断是否拦截所述数据包，若不拦截，将所述数据包发送至下一跳设备，否则，拦截所述数据包。

WO 2017/101627 A1

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))。

一种内容访问控制方法及相关设备

本申请要求在 2015 年 12 月 17 日提交中国专利局、申请号为 201510954617.1、发明名称为“一种内容访问控制方法及相关设备”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

本发明涉及通信技术领域，尤其涉及一种内容访问控制方法及相关设备。

背景技术

目前移动通信网络支持深度包检测机制，通过深度包检测机制可以检测用户当前使用的应用，深度包检测的具体架构如图 1 所示。

其中，策略和计费规则功能（Policy and Charging Rules Function，PCRF）实体制定应用检测控制策略，并将该应用检测控制策略发送给流量检测功能（Traffic Detection Function，TDF）实体。应用检测控制策略中包括应用标识、业务数据过滤器列表、优先级以及对流量执行的操作等信息，例如对流量执行上下行速率限制等操作。其中，应用标识和业务数据过滤器列表用于识别特定的应用或流量。

当 TDF 检测到与策略中的应用标识或业务数据流过滤器列表相匹配的流量时，TDF 根据策略中包括的操作处理该流量。

随着移动通信网络的发展，越来越多的儿童使用家长的智能手机上网，但是目前网络侧无法区分使用智能手机的用户是否为儿童，无法针对不同用户进行细粒度的网络内容控制，例如，儿童可通过家长的智能手机浏览不适合儿童观看的视频或网站，不利于儿童的健康成长。

鉴于此，需要提供一种能够对使用同一终端的不同用户请求访问的网络内容进行区别控制的方法。

发明内容

本发明实施例提供一种内容访问控制方法及相关设备，用以对使用同一终端的不同用户所请求访问的内容进行区别控制。

本发明实施例提供的具体技术方案如下：

本发明实施例提供了一种内容访问控制方法，包括：

内容拦截实体获取当前使用终端的访问用户的数据包；

所述内容拦截实体根据所述当前使用终端的访问用户对应的内容访问控制策略，判断是否拦截所述数据包，若不拦截，将所述数据包发送至下一跳设备，否则，拦截所述数据包。

可能的实施方式中，所述内容拦截实体获取当前使用终端的访问用户的数据包之前，所述方法还包括:

所述内容拦截实体获取所述终端配置的所述终端的两个以上访问用户各自对应的内容访问控制相关信息，分别根据所述两个以上访问用户各自对应的内容访问控制相关信息，获得所述两个以上访问用户各自对应的内容访问控制策略;

和/或，

所述内容拦截实体获取策略控制实体配置的所述终端的两个以上访问用户各自对应的内容访问控制策略。

可能的实施方式中，所述内容拦截实体获取当前使用终端的访问用户的数据包之前，所述方法还包括:

所述内容拦截实体获取策略控制实体配置的所述当前使用终端的访问用户的内容访问控制策略。

可能的实施方式中，所述内容拦截实体根据所述当前使用终端的访问用户对应的内容访问控制策略，判断是否拦截所述数据包，包括:

所述内容拦截实体获取所述终端发送的通知消息，所述通知消息中携带所述当前使用终端的访问用户的身份标识，根据所述身份标识确定所述当前使用终端的用户对应的内容访问控制策略；或者，

所述内容拦截实体获取身份管理服务器发送的通知消息，所述通知消息中携带所述当前使用终端的访问用户的身份标识，根据所述身份标识确定所述当前使用终端的用户对应的内容访问控制策略。

本发明实施例中，内容拦截实体根据当前使用终端的用户对应的内容访问控制策略拦截数据包，从而能够采用终端当前用户的内容访问控制策略进行内容访问控制。

本发明实施例还提供了一种内容访问控制方法，包括:

身份管理服务器获取终端的访问用户的内容访问控制相关信息;

所述身份管理服务器向策略控制实体发送所述访问用户的内容访问控制相关信息，由所述策略控制实体根据接收的所述访问用户的内容访问控制相关信息确定对应的内容访问控制策略，将确定的内容访问控制策略发送给内容拦截实体，由所述内容拦截实体根据接收的内容访问控制策略拦截数据包。

可能的实施方式中，所述身份管理服务器向策略控制实体发送所述访问用户的内容访问控制相关信息，包括:

所述身份管理服务器向策略控制实体发送当前使用所述终端的访问用户对应的内容访问控制相关信息;

或者,

所述身份管理服务器向策略控制实体发送所述终端的两个以上访问用户各自对应的内容访问控制相关信息。

可能的实施方式中，所述身份管理服务器获取终端的访问用户的内容访问控制相关信息，包括:

所述身份管理服务器获取所述终端配置的所述终端的至少一个访问用户各自对应的内容访问控制相关信息；和/或,

所述身份管理服务器获取第三方系统发送的所述终端的至少一个访问用户各自对应的内容访问控制相关信息。

可能的实施方式中，所述身份管理服务器向策略控制实体发送当前使用所述终端的访问用户对应的内容访问控制相关信息之前，所述方法还包括:

所述身份管理服务器接收所述终端发送的通知消息，所述通知消息中携带所述当前使用所述终端的访问用户的身份标识，根据所述身份标识确定所述当前使用所述终端的访问用户对应的内容访问控制相关信息。

本发明实施例中，身份管理服务器将终端的访问用户的内容访问控制相关信息发送给策略控制实体，以确定该访问用户的内容访问控制策略，由内容拦截实体根据访问用户对应的内容访问控制策略进行内容访问控制，从而可以实现对使用终端的访问用户所请求访问的内容进行控制。

本发明实施例还提供了一种内容访问控制方法，包括:

终端确定当前使用所述终端的访问用户;

所述终端通知内容拦截实体根据所述当前使用所述终端的访问用户对应的内容访问控制策略拦截数据包。

可能的实施方式中，所述方法还包括:

所述终端获取访问用户的内容访问控制相关信息;

所述终端根据所述访问用户的内容访问控制相关信息配置内容拦截实体，由所述内容拦截实体获取所述访问用户的内容访问控制相关信息对应的内容访问控制策略，所述访问用户为所述当前使用所述终端的访问用户或者为所述终端的两个以上的访问用户。

可能的实施方式中，所述终端根据所述访问用户的内容访问控制相关信息配置内容拦截实体，包括:

所述终端将所述访问用户的内容访问控制相关信息直接发送给所述内容拦截实体;

或者,

所述终端将所述访问用户的内容访问控制相关信息发送给身份管理服务器，由所述身份管理服务器向策略控制实体发送所述访问用户的内容访问控制相关信息，由所述策略控制实体根据所述访问用户的内容访问控制相关信息确定对应的内容访问控制策略，将确定的内容访问控制策略发送给所述内容拦截实体。

可能的实施方式中，所述终端通知内容拦截实体根据所述当前使用所述终端的访问用户对应的内容访问控制策略拦截数据包，包括:

所述终端向所述内容拦截实体发送通知消息，所述通知消息中携带所述当前使用所述终端的访问用户的身份标识，由所述内容拦截实体根据所述通知消息获取所述当前使用所述终端的访问用户对应的内容访问控制策略，并根据所述当前使用所述终端的访问用户对应的内容访问控制策略拦截数据包。

可能的实施方式中，所述方法还包括:

所述终端向所述身份管理服务器发送通知消息，所述通知消息中携带所述当前使用所述终端的访问用户的身份标识，由所述身份管理服务器根据所述通知消息向所述策略控制实体发送所述当前使用所述终端的访问用户对应的内容访问控制相关信息，由所述策略控制实体根据所述当前使用所述终端的访问用户的内容访问控制相关信息确定对应的内容访问控制策略，将所述当前使用所述终端的访问用户对应的内容访问控制策略发送给所述内容拦截实体。

本发明实施例中，终端通知内容拦截实体根据当前使用该终端的访问用户对应的内容访问控制策略拦截数据包，从而可以实现对当前使用终端的访问用户所请求访问的内容进行控制。

本发明实施例还提供了一种内容访问控制系统，包括:

终端，用于确定当前使用所述终端的访问用户，并通知内容拦截实体根据所述当前使用所述终端的访问用户对应的内容访问控制策略拦截数据包;

内容拦截实体，用于获取所述当前使用所述终端的访问用户的数据包，根据所述当前使用所述终端的访问用户对应的内容访问控制策略判断是否拦截所述数据包，若不拦截，将所述数据包发送至下一跳设备，否则，拦截所述数据包。

可能的实施方式中，所述终端还用于:

获取访问用户的内容访问控制相关信息，根据所述访问用户的内容访问控制相关信息配置内容拦截实体，其中，所述访问用户为所述当前使用所述终端的访问用户或者为所述终端的两个以上的访问用户;

所述内容拦截实体还用于:

获取所述访问用户的内容访问控制相关信息对应的内容访问控制策略。

可能的实施方式中，还包括身份管理服务器和策略控制实体;

所述终端具体用于:

将所述访问用户的内容访问控制相关信息发送给所述身份管理服务器;

所述身份管理服务器用于:

接收所述终端发送的所述访问用户的内容访问控制相关信息，向所述策略控制实体发送所述访问用户的内容访问控制相关信息;

所述策略控制实体用于:

根据所述身份管理服务器发送的所述访问用户的内容访问控制相关信息，确定对应的内容访问控制策略，将确定的内容访问控制策略发送给所述内容拦截实体。

本发明实施例还提供了一种内容拦截实体，包括:

获取模块，用于获取当前使用终端的访问用户的数据包;

拦截模块，用于根据所述当前使用终端的访问用户对应的内容访问控制策略，判断是否拦截所述数据包，若不拦截，将所述数据包发送至下一跳设备，否则，拦截所述数据包。

可能的实施方式中，所述获取模块还用于:

获取当前使用终端的访问用户的数据包之前，

获取所述终端配置的所述终端的两个以上访问用户各自对应的内容访问控制相关信息，分别根据所述两个以上访问用户各自对应的内容访问控制相关信息，获得所述两个以上访问用户各自对应的内容访问控制策略;

和/或，

获取策略控制实体配置的所述终端的两个以上访问用户各自对应的内容访问控制策略。

可能的实施方式中，所述获取模块还用于:

获取当前使用终端的访问用户的数据包之前，获取策略控制实体配置的所述当前使用终端的访问用户的内容访问控制策略。

可能的实施方式中，所述拦截模块具体用于:

获取所述终端发送的通知消息，所述通知消息中携带所述当前使用终端的访问用户的身份标识，根据所述身份标识确定所述当前使用终端的用户对应的内容访问控制策略;或者，

获取身份管理服务器发送的通知消息，所述通知消息中携带所述当前使用终端的访问用户的身份标识，根据所述身份标识确定所述当前使用终端的用户对应的内容访问控制策略。

本发明实施例还提供一种身份管理服务器，包括:

获取模块，用于获取终端的访问用户的内容访问控制相关信息;

发送模块，用于向策略控制实体发送所述访问用户的内容访问控制相关信息，由所述

策略控制实体根据接收的所述访问用户的内容访问控制相关信息确定对应的内容访问控制策略，将确定的内容访问控制策略发送给内容拦截实体，由所述内容拦截实体根据接收的内容访问控制策略拦截数据包。

可能的实施方式中，所述发送模块具体用于:

向策略控制实体发送当前使用所述终端的访问用户对应的内容访问控制相关信息;

或者，

向策略控制实体发送所述终端的两个以上访问用户各自对应的内容访问控制相关信息。

可能的实施方式中，所述获取模块具体用于:

获取所述终端配置的所述终端的至少一个访问用户各自对应的内容访问控制相关信息; 和/或，

获取第三方系统发送的所述终端的至少一个访问用户各自对应的内容访问控制相关信息。

可能的实施方式中，还包括接收模块，用于:

在所述发送模块向策略控制实体发送当前使用所述终端的访问用户对应的内容访问控制相关信息之前，接收所述终端发送的通知消息，所述通知消息中携带所述当前使用所述终端的访问用户的身份标识，根据所述身份标识确定当前使用所述终端的访问用户对应的内容访问控制相关信息。

本发明实施例还提供了一种终端，包括:

确定模块，用于确定当前使用所述终端的访问用户;

通知模块，用于通知内容拦截实体根据所述当前使用所述终端的访问用户对应的内容访问控制策略拦截数据包。

可能的实施方式中，还包括获取模块，用于获取访问用户的内容访问控制相关信息;

配置模块，用于根据所述访问用户的内容访问控制相关信息配置内容拦截实体，由所述内容拦截实体获取所述访问用户的内容访问控制相关信息对应的内容访问控制策略，所述访问用户为所述当前使用所述终端的访问用户或者为所述终端的两个以上的访问用户。

可能的实施方式中，所述配置模块具体用于:

将所述访问用户的内容访问控制相关信息直接发送给所述内容拦截实体;

或者，

将所述访问用户的内容访问控制相关信息发送给身份管理服务器，由所述身份管理服务器向策略控制实体发送所述访问用户的内容访问控制相关信息，由所述策略控制实体根据所述访问用户的内容访问控制相关信息确定对应的内容访问控制策略，将确定的内容访问控制策略发送给所述内容拦截实体。

可能的实施方式中，所述通知模块具体用于:

向所述内容拦截实体发送通知消息，所述通知消息中携带所述当前使用所述终端的访问用户的身份标识，由所述内容拦截实体根据所述通知消息获取所述当前使用所述终端的访问用户对应的内容访问控制策略，并根据所述当前使用所述终端的访问用户对应的内容访问控制策略拦截数据包。

可能的实施方式中，所述通知模块还用于:

向所述身份管理服务器发送通知消息，所述通知消息中携带所述当前使用所述终端的访问用户的身份标识，由所述身份管理服务器根据所述通知消息向所述策略控制实体发送所述当前使用所述终端的访问用户对应的内容访问控制相关信息，由所述策略控制实体根据所述当前使用所述终端的访问用户的内容访问控制相关信息确定对应的内容访问控制策略，将所述当前使用所述终端的访问用户对应的内容访问控制策略发送给所述内容拦截实体。

本发明实施例提供了另一种内容拦截实体，该内容拦截实体主要包括处理器、存储器和收发机，其中，收发机用于在处理器的控制下接收和发送数据，存储器中保存有预设的程序，处理器用于读取存储器中保存的程序，按照该程序执行以下过程:

通过收发机获取当前使用终端的访问用户的数据包;

根据所述当前使用终端的访问用户对应的内容访问控制策略，判断是否拦截所述数据包，若不拦截，通过收发机将所述数据包发送至下一跳设备，否则，拦截所述数据包。

可能的实施方式中，处理器通过收发机获取当前使用终端的访问用户的数据包之前，通过收发机获取所述终端配置的所述终端的两个以上访问用户各自对应的内容访问控制相关信息，分别根据所述两个以上访问用户各自对应的内容访问控制相关信息，获得所述两个以上访问用户各自对应的内容访问控制策略;

和/或，

通过收发机获取策略控制实体配置的所述终端的两个以上访问用户各自对应的内容访问控制策略。

可能的实施方式中，处理器通过收发机获取当前使用终端的访问用户的数据包之前，通过收发机获取策略控制实体配置的所述当前使用终端的访问用户的内容访问控制策略。

可能的实施方式中，处理器通过收发机获取所述终端发送的通知消息，所述通知消息中携带所述当前使用终端的访问用户的身份标识，根据所述身份标识确定所述当前使用终端的用户对应的内容访问控制策略; 或者，

通过收发机获取身份管理服务器发送的通知消息，所述通知消息中携带所述当前使用终端的访问用户的身份标识，根据所述身份标识确定所述当前使用终端的用户对应的内容访问控制策略。

本发明实施例中还提供了另一种身份管理服务器，该身份管理服务器主要包括处理器、存储器和收发机，其中，收发机用于在处理器的控制下接收和发送数据，存储器中保存有预设的程序，处理器用于读取存储器中保存的程序，按照该程序执行以下过程：

通过收发机获取终端的访问用户的内容访问控制相关信息；

通过收发机向策略控制实体发送所述访问用户的内容访问控制相关信息，由所述策略控制实体根据接收的所述访问用户的内容访问控制相关信息确定对应的内容访问控制策略，将确定的内容访问控制策略发送给内容拦截实体，由所述内容拦截实体根据接收的内容访问控制策略拦截数据包。

可能的实施方式中，处理器通过收发机向策略控制实体发送当前使用所述终端的访问用户对应的内容访问控制相关信息；

或者，

处理器通过收发机向策略控制实体发送所述终端的两个以上访问用户各自对应的内容访问控制相关信息。

可能的实施方式中，处理器在通过收发机获取所述终端配置的所述终端的至少一个访问用户各自对应的内容访问控制相关信息；和/或，

通过收发机获取第三方系统发送的所述终端的至少一个访问用户各自对应的内容访问控制相关信息。

可能的实施方式中，处理器通过收发机接收所述终端发送的通知消息，所述通知消息中携带所述当前使用所述终端的访问用户的身份标识，根据所述身份标识确定所述当前使用所述终端的访问用户对应的内容访问控制相关信息。

本发明实施例中还提供了另一种终端，该终端主要包括处理器、存储器和收发机，其中，收发机用于在处理器的控制下接收和发送数据，存储器中保存有预设的程序，处理器用于读取存储器中保存的程序，按照该程序执行以下过程：

确定当前使用所述终端的访问用户；

通过收发机通知内容拦截实体根据所述当前使用所述终端的访问用户对应的内容访问控制策略拦截数据包。

可能的实施方式中，处理器通过收发机获取访问用户的内容访问控制相关信息；

根据所述访问用户的内容访问控制相关信息配置内容拦截实体，由所述内容拦截实体获取所述访问用户的内容访问控制相关信息对应的内容访问控制策略，所述访问用户为所述当前使用所述终端的访问用户或者为所述终端的两个以上的访问用户。

可能的实施方式中，处理器通过收发机将所述访问用户的内容访问控制相关信息直接发送给所述内容拦截实体；

或者，

通过收发机将所述访问用户的内容访问控制相关信息发送给身份管理服务器，由所述身份管理服务器向策略控制实体发送所述访问用户的内容访问控制相关信息，由所述策略控制实体根据所述访问用户的内容访问控制相关信息确定对应的内容访问控制策略，将确定的内容访问控制策略发送给所述内容拦截实体。

可能的实施方式中，处理器通过收发机向所述内容拦截实体发送通知消息，所述通知消息中携带所述当前使用所述终端的访问用户的身份标识，由所述内容拦截实体根据所述通知消息获取所述当前使用所述终端的访问用户对应的内容访问控制策略，并根据所述当前使用所述终端的访问用户对应的内容访问控制策略拦截数据包。

可能的实施方式中，处理器通过收发机向所述身份管理服务器发送通知消息，所述通知消息中携带所述当前使用所述终端的访问用户的身份标识，由所述身份管理服务器根据所述通知消息向所述策略控制实体发送所述当前使用所述终端的访问用户对应的内容访问控制相关信息，由所述策略控制实体根据所述当前使用所述终端的访问用户的内容访问控制相关信息确定对应的内容访问控制策略，将所述当前使用所述终端的访问用户对应的内容访问控制策略发送给所述内容拦截实体。

附图说明

图 1 为深度包检测的具体架构示意图；

图 2 为本发明第一实施例中内容拦截实体进行内容访问控制的方法流程示意图；

图 3 为本发明第二实施例中身份管理服务器进行内容访问控制的方法流程示意图；

图 4 为本发明第三实施例中终端进行内容访问控制的方法流程示意图；

图 5 为本发明第四实施例中内容访问控制系统架构示意图；

图 6 为本发明第四实施例中另一内容访问控制系统架构示意图；

图 7 为本发明第五实施例中内容拦截实体的结构示意图；

图 8 为本发明第六实施例中身份管理服务器的结构示意图；

图 9 为本发明第七实施例中终端结构示意图；

图 10 为本发明第八实施例中内容拦截实体的结构示意图；

图 11 为本发明第九实施例中身份管理服务器的结构示意图；

图 12 为本发明第十实施例中终端结构示意图。

具体实施方式

为使本发明实施例的目的、技术方案和优点更加清楚，下面将结合本发明实施例中的附图，对本发明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

发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

应理解，本发明的技术方案可以应用于各种通信系统，例如：全球移动通讯（Global System of Mobile communication，GSM）系统、码分多址（Code Division Multiple Access，CDMA）系统、宽带码分多址（Wideband Code Division Multiple Access，WCDMA）系统、通用分组无线业务（General Packet Radio Service，GPRS）、长期演进（Long Term Evolution，LTE）系统、先进的长期演进（Advanced long term evolution，LTE-A）系统、通用移动通信系统（Universal Mobile Telecommunication System，UMTS）等。

还应理解，在本发明实施例中，用户设备（User Equipment，UE）包括但不限于移动台（Mobile Station，MS）、移动终端（Mobile Terminal）、移动电话（Mobile Telephone）、手机（handset）及便携设备（portable equipment）等，该用户设备可以经无线接入网（Radio Access Network，RAN）与一个或多个核心网进行通信，例如，用户设备可以是移动电话（或称为“蜂窝”电话）、具有无线通信功能的计算机等，用户设备还可以是便携式、袖珍式、手持式、计算机内置的或者车载的移动装置。

在本发明实施例中，基站（例如，接入点）可以是指接入网中在空中接口上通过一个或多个扇区与无线终端通信的设备。基站可用于将收到的空中帧与 IP 分组进行相互转换，作为无线终端与接入网的其余部分之间的路由器，其中接入网的其余部分可包括网际协议（IP）网络。基站还可协调对空中接口的属性管理。例如，基站可以是 GSM 或 CDMA 中的基站（Base Transceiver Station，BTS），也可以是 WCDMA 中的基站（NodeB），还可以是 LTE 中的演进型基站（NodeB 或 eNB 或 e-NodeB，evolutional Node B），本发明并不限定。

为了使本发明的目的、技术方案和优点更加清楚，下面将结合附图对本发明作进一步地详细描述，显然，所描述的实施例仅仅是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其它实施例，都属于本发明保护的范围。

以下各实施例中，内容拦截实体可以部署在 TDF 或 PGW 上，也可以作为一种业务功能部署在（S）Gi-局域网（Local Area Network，LAN）中，其中，（S）Gi 为位于 PGW 与业务网络之间的接口的名称。

以下各实施例中，策略控制实体可以是 PCRF 实体。

如图 2 所示，本发明第一实施例中，内容拦截实体进行内容访问控制的详细方法流程如下：

步骤 201：内容拦截实体获取当前使用终端的访问用户的数据包。

实施中，内容拦截实体在获取当前使用终端的访问用户的数据包之前，需要获取当前使用终端的访问用户对应的内容访问控制策略，获取方式可以是以下所列举的两种实现方式中的任意一种或者组合:

第一，内容拦截实体获取终端配置的该终端的两个以上访问用户各自对应的内容访问控制相关信息，分别根据该两个以上访问用户各自对应的内容访问控制相关信息，获得该两个以上访问用户各自对应的内容访问控制策略，其中，该两个以上访问用户中包括当前使用终端的访问用户。

第二，内容拦截实体获取策略控制实体配置的终端的两个以上访问用户各自对应的内容访问控制策略，其中，该两个以上访问用户中包括当前使用终端的访问用户。

其中，所谓以上两种获取方式的组合是指将内容拦截实体可以将终端以及策略控制实体分别配置的终端同一访问用户的内容访问控制策略进行组合。

对应于以上两种内容访问控制策略的获取方式中的任意一种或组合，内容访问控制实体需要从保存的终端的多个用户的内容访问控制策略中选择当前使用终端的用户对应的内容访问控制策略。

实施中，内容拦截实体确定当前使用终端的访问用户对应的内容访问控制策略，包括但不限于以下两种实现方式:

第一，内容拦截实体获取终端发送的通知消息，该通知消息中携带当前使用终端的访问用户的身份标识，根据该身份标识确定当前使用该终端的用户对应的内容访问控制策略;

第二，内容拦截实体获取身份管理服务器发送的通知消息，通知消息中携带当前使用终端的访问用户的身份标识，根据该身份标识确定当前使用该终端的用户对应的内容访问控制策略。

具体地，身份标识为访问用户登录终端所使用的密码和/或用户名。

具体应用中，用户在终端上安装内容控制软件，用户通过该内容控制软件提供的人机交互界面设置多个登录终端所使用的用户名和/或密码。终端在解锁屏幕时需要用户输入设置的用户名和/或密码，并且终端在每次解锁屏幕后发送通知消息，该通知消息中携带解锁屏幕过程中获得的用户名和/或密码。可选择地，用户通过内容控制软件设置登录终端所使用的用户名和/或密码时，还可以设置于该用户名和/或密码对应的内容访问控制相关信息。

具体地，终端通过安装的内容控制软件获取为使用该终端的访问用户设置的用户名、密码以及内容访问控制相关信息，在获取提交指示后，向身份管理服务器（或内容拦截实体）发送消息，该消息中携带设置的每个用户名、密码以及内容访问控制相关信息之间的

对应关系，由身份管理服务器（或内容拦截实体）保存该对应关系。

实施中，内容拦截实体可以获取策略控制实体配置的当前使用终端的访问用户的内容访问控制策略，该实施方式内容拦截实体仅保存当前使用终端的访问用户的内容访问控制策略，内容拦截实体不需要获知当前使用终端的访问用户是哪个用户，直接根据保存的内容访问控制策略进行拦截即可。

步骤 202：内容拦截实体根据当前使用终端的访问用户对应的内容访问控制策略，判断是否拦截数据包，若不拦截，将数据包发送至下一跳设备，否则，拦截数据包。

其中，内容访问控制策略用于限定访问用户能够访问的内容，或者用于限定访问用户不能访问的内容。例如，手机的儿童用户对应的内容访问控制策略中规定，儿童用户不能访问视频，或者，儿童仅能够访问军事网站。

具体地，根据具体应用场景的不同，下一跳设备可以是路由器，也可以是运营商部署的运行增值业务的设备。

第一实施例中，内容拦截实体根据当前使用终端的访问用户对应的内容访问控制策略拦截数据包，从而能够采用当前使用终端的访问用户的内容访问控制策略进行内容访问控制。

如图 3 所示，本发明第二实施例中，身份管理服务器进行内容访问控制的详细方法流程如下：

步骤 301：身份管理服务器获取终端的访问用户的内容访问控制相关信息。

实施中，身份管理服务器获取终端的访问用户的内容访问控制相关信息，可以采用以下两种实现方式中的任意一种或组合：

第一，身份管理服务器获取终端配置的该终端的至少一个访问用户各自对应的内容访问控制相关信息；

第二，身份管理服务器获取第三方系统发送的该终端的至少一个访问用户各自对应的内容访问控制相关信息。

例如，第三方系统可以是银行系统或者运营商的计费系统，当访问用户在银行的信用等级下降时，银行服务器主动向身份管理服务器提供该访问用户的信用等级，身份管理服务器将该访问用户的信用等级发送给策略控制实体，策略控制实体根据访问用户的信用等级制定能够禁止该访问用户访问与该信用等级不相符的内容的内容访问控制策略。当运营商计费系统发现访问用户欠费时，主动向身份管理服务器提供该访问用户的欠费信息，身份管理服务器将该访问用户的欠费信息发送给策略控制实体，策略控制实体根据该访问用户的欠费信息制定能够禁止该访问用户在欠费状态下访问的内容的内容访问控制策略。

步骤 302：身份管理服务器向策略控制实体发送所述访问用户的内容访问控制相关信息。

其中，策略控制实体根据接收的访问用户的内容访问控制相关信息确定对应的内容访问控制策略，将确定的内容访问控制策略发送给内容拦截实体，由内容拦截实体根据接收的内容访问控制策略拦截数据包。

实施中，身份管理服务器向策略控制实体发送访问用户的内容访问控制相关信息，包括但不限于以下两种实现方式：

第一，身份管理服务器向策略控制实体发送当前使用终端的访问用户对应的内容访问控制相关信息。

实施中，策略控制实体根据当前使用终端的访问用户的内容访问控制相关信息确定内容访问控制策略，并由策略控制实体将当前使用终端的访问用户的内容访问控制策略发送给内容拦截实体，由内容拦截实体根据当前使用终端的访问用户的内容访问控制策略拦截数据包。

该第一实现方式中，身份管理服务器需要确定当前使用该终端的访问用户，具体地，身份管理服务器接收终端发送的通知消息，该通知消息中携带当前使用该终端的访问用户的身份标识。

该第一实现方式中，身份管理服务器根据通知消息中携带的身份标识确定当前使用终端的访问用户对应的内容访问控制相关信息，将当前使用终端的访问用户对应的内容访问控制相关信息发送给策略控制实体，由策略控制实体确定接收的该内容访问控制相关信息对应的内容访问控制策略，将该内容访问控制策略发送给内容拦截实体，由内容拦截实体根据该内容访问控制策略拦截数据包。该实施方式中，内容拦截实体仅保存当前使用终端的访问用户对应的内容访问控制策略，无需获知当前使用终端的为哪个访问用户，直接按照所保存的内容访问控制策略拦截数据包即可。

该第一实现方式中，身份管理服务器获取终端每次切换访问用户后发送的通知消息，该通知消息中携带当前使用该终端的访问用户的身份标识。身份管理服务器根据通知消息确定当前使用终端的访问用户并将该当前使用终端的访问用户的内容访问控制相关信息发送给策略控制实体。

该第一实现方式中，身份管理服务器在获取终端的任一访问用户更新后的内容访问控制相关信息后，对本地保存的该访问用户的内容访问控制相关信息进行更新。

第二，身份管理服务器向策略控制实体发送终端的两个以上访问用户各自对应的内容访问控制相关信息。

该第二实现方式中，身份管理服务器需要确定当前使用该终端的访问用户，具体地，身份管理服务器接收终端发送的通知消息，该通知消息中携带当前使用该终端的访问用户的身份标识。

该第二实现方式中，身份管理服务器通知内容拦截实体根据该身份标识从保存的该终端的多个用户各自对应的内容访问控制策略中，选择当前使用该终端的访问用户对应的内容访问控制策略，根据该当前使用该终端的访问用户对应的内容访问控制策略拦截数据包。

该第二实现方式中，身份管理服务器获取终端每次切换访问用户后发送的通知消息，该通知消息中携带当前使用该终端的访问用户的身份标识。

该第二实现方式中，身份管理服务器在获取终端的任一访问用户更新后的内容访问控制相关信息后，对本地保存的该访问用户的内容访问控制相关信息进行更新，并将发生更新的访问用户的内容访问控制相关信息发送给策略控制实体，由策略控制实体分别确定发生更新的访问用户的内容访问控制信息对应的内容访问控制策略，并将更新的访问用户的内容访问控制策略发送给内容拦截实体。

以上两种实现方式中，身份管理服务器可以是主动将终端的访问用户的内容访问控制相关信息发送给策略控制实体，也可以是在策略控制实体的请求下将终端的访问用户的内容访问控制相关信息发送给策略控制实体。

本发明第二实施例中，身份管理服务器将终端的访问用户的内容访问控制相关信息发送给策略控制实体，以确定访问用户对应的内容访问控制策略，由内容拦截实体根据访问用户对应的内容访问控制策略进行内容访问控制，从而可以实现对使用终端的访问用户进行内容访问控制。

如图 4 所示，本发明第三实施例中，终端进行内容访问控制的详细方法流程如下：

步骤 401：终端确定当前使用终端的访问用户。

步骤 402：终端通知内容拦截实体根据当前使用该终端的访问用户对应的内容访问控制策略拦截数据包。

实施中，终端获取访问用户的内容访问控制相关信息，根据访问用户的内容访问控制相关信息配置内容拦截实体，由内容拦截实体获取访问用户的内容访问控制相关信息对应的内容访问控制策略。

其中，访问用户为当前使用该终端的访问用户，或者为该终端的两个以上的访问用户。

具体地，终端通过人机交互界面（例如客户端软件）获取终端的特权用户输入的其它一个或多个访问用户各自对应的内容访问控制相关信息；或者，终端根据运营商网络提供

的签约信息获取至少一个访问用户各自对应的内容访问控制相关信息。

第一实施方式中，终端将访问用户的内容访问控制相关信息直接发送给内容拦截实体，由内容拦截实体根据该访问用户的内容访问控制相关信息，获得该访问用户对应的内容访问控制策略；

具体地，内容拦截实体将访问用户对应的内容访问控制相关信息作为该访问用户对应的内容访问控制策略，在确定当前使用该终端的访问用户后，按照该访问用户对应的内容访问控制策略拦截数据包。

该第一实施方式中，终端需要向内容拦截实体发送通知消息，通知消息中携带当前使用终端的访问用户的身份标识，由内容拦截实体根据通知消息获取当前使用终端的访问用户对应的内容访问控制策略，并根据当前使用终端的访问用户对应的内容访问控制策略拦截数据包。或者，终端向身份管理服务器发送通知消息，该通知消息中携带当前使用终端的访问用户的身份标识，由身份管理服务器根据该通知消息通知内容拦截实体选择当前使用终端的访问用户对应的内容访问控制策略。

实施中，终端在确定终端的任一访问用户的内容访问控制相关信息发生更新时，将更新后的内容访问控制相关信息发送给内容拦截实体。

第二实施方式中，终端将访问用户的内容访问控制相关信息发送给身份管理服务器，由身份管理服务器向策略控制实体发送该访问用户的内容访问控制相关信息；由策略控制实体根据接收的访问用户的内容访问控制相关信息确定对应的内容访问控制策略，将确定的内容访问控制策略发送给内容拦截实体。

该第二实施方式中，终端需要向内容拦截实体发送通知消息，通知消息中携带当前使用终端的访问用户的身份标识，由内容拦截实体根据通知消息获取当前使用终端的访问用户对应的内容访问控制策略，并根据当前使用终端的访问用户对应的内容访问控制策略拦截数据包。

或者，

终端向身份管理服务器发送通知消息，通知消息中携带当前使用终端的访问用户的身份标识，由身份管理服务器根据通知消息向策略控制实体发送当前使用终端的访问用户对应的内容访问控制相关信息，由策略控制实体根据当前使用终端的访问用户的内容访问控制相关信息确定对应的内容访问控制策略，将当前使用终端的访问用户对应的内容访问控制策略发送给内容拦截实体。

该第二实施方式中，身份管理服务器保存终端的多个访问用户各自对应的内容访问控制相关信息。

第一种实现方式中，身份管理服务器向策略控制实体发送当前使用终端的访问用户对应的内容访问控制相关信息。策略控制实体根据接收的内容访问控制相关信息确定内容访问控制策略，将确定的内容访问控制策略发送给内容拦截实体。内容拦截实体根据接收的内容访问控制策略拦截数据包。

该具体实施中，身份管理服务器向策略控制实体发送当前使用终端的访问用户对应的内容访问控制相关信息之前，向身份管理服务器发送通知消息，该通知消息中携带当前使用终端的访问用户的身份标识。身份管理服务器根据该通知消息确定当前使用该终端的访问用户对应的内容访问控制相关信息。

第二种实现方式中，身份管理服务器向策略控制实体发送多个访问用户各自对应的内容访问控制相关信息。策略控制实体根据接收的每个访问用户的内容访问控制相关信息确定每个访问用户各自对应的内容访问控制策略，将确定的内容访问控制策略发送给内容拦截实体。内容拦截实体根据接收的内容访问控制策略拦截数据包。

该具体实施中，终端向身份管理服务器发送通知消息，该通知消息中携带当前使用终端的访问用户的身份标识。身份管理服务器通知内容拦截实体选择当前使用终端的访问用户对应的内容访问控制策略拦截数据包。

如图 5 所示，本发明第四实施例中，内容访问控制系统包括终端 501 和内容拦截实体 502，具体地:

终端 501，用于确定当前使用所述终端的访问用户，并通知内容拦截实体 502 根据所述当前使用所述终端的访问用户对应的内容访问控制策略拦截数据包;

内容拦截实体 502，用于获取当前使用终端的访问用户的数据包，根据所述当前使用所述终端的访问用户对应的内容访问控制策略判断是否拦截所述数据包，若不拦截，将所述数据包发送至下一跳设备，否则，拦截所述数据包。

实施中，终端还用于:

获取访问用户的内容访问控制相关信息，根据所述访问用户的内容访问控制相关信息配置内容拦截实体，其中，所述访问用户为所述当前使用所述终端的访问用户或者为所述终端的两个以上的访问用户;

所述内容拦截实体还用于:

获取所述访问用户的内容访问控制相关信息对应的内容访问控制策略。

具体实施中，如图 6 所示，内容访问控制系统还包括身份管理服务器 503 和策略控制实体 504，具体地:

所述终端 501 具体用于:

将所述访问用户的内容访问控制相关信息发送给所述身份管理服务器;

所述身份管理服务器 503 用于:

接收所述终端发送的所述访问用户的内容访问控制相关信息，向所述策略控制实体发送所述访问用户的内容访问控制相关信息;

所述策略控制实体 504 用于:

根据所述身份管理服务器发送的所述访问用户的内容访问控制相关信息，确定对应的内容访问控制策略，将确定的内容访问控制策略发送给所述内容拦截实体 502。

第一具体实施方式中，身份管理服务器 503，用于获取终端的至少一个访问用户各自对应的内容访问控制相关信息，将终端的至少一个访问用户各自对应的内容访问控制相关信息发送给策略控制实体 504;

策略控制实体 504，用于接收身份管理服务器 503 发送的终端的至少一个访问用户各自对应的内容访问控制相关信息，分别根据该终端的至少一个访问用户各自对应的内容访问控制相关信息确定该至少一个访问用户各自对应的内容访问控制策略，并将该终端的至少一个访问用户各自对应的内容访问控制策略发送给内容拦截实体 502;

内容拦截实体 502，用于接收策略控制实体 504 发送的该终端的至少一个访问用户各自对应的内容访问控制策略，根据该终端的至少一个访问用户各自对应的内容访问控制策略拦截数据包。

实施中，身份管理服务器获取终端配置的该终端的至少一个访问用户各自对应的内容访问控制相关信息; 和/或，获取第三方系统发送的该终端的至少一个访问用户各自对应的内容访问控制相关信息。

实施中，身份管理服务器接收终端发送的通知消息，通知消息中携带当前使用终端的访问用户的身份标识。具体地，身份管理服务器根据该通知消息通知内容拦截实体选择当前使用终端的访问用户对应的内容访问控制策略，根据当前使用终端的访问用户对应的内容访问控制策略拦截数据包。

第二具体实施方式中，身份管理服务器获取终端的至少一个访问用户各自对应的内容访问控制相关信息，确定当前使用该终端的访问用户，将当前使用终端的访问用户对应的内容访问控制相关信息发送给策略控制实体;

策略控制实体接收身份管理服务器发送的当前使用终端的访问用户对应的内容访问控制相关信息，根据当前使用终端的访问用户的内容访问控制相关信息确定内容访问控制策略，将当前使用终端的访问用户的内容访问控制策略发送给内容拦截实体;

内容拦截实体接收策略控制实体发送的当前使用终端的访问用户的内容访问控制策

略，根据该内容访问控制策略拦截数据包。

实施中，身份管理服务器接收终端发送的通知消息，通知消息中携带当前使用终端的访问用户的身份标识，根据该身份标识确定当前使用终端的访问用户对应的内容访问控制相关信息。

以下通过三个具体例子对内容访问控制的过程进行举例说明。

第一具体实施例

家长在手机上预设儿童账户，当前儿童通过输入儿童账户的用户名和密码解锁手机；

手机发现儿童账户登录，向身份管理服务器发送儿童账户的用户名以及家长为该儿童账户设置的内容访问控制相关信息，例如不能浏览游戏网站；如果儿童账户为第一次登录或者家长设置的内容访问控制相关信息发生变化，手机需要将儿童账户最新的内容访问控制相关信息发送给身份管理服务器；

身份管理服务器向策略控制实体发送消息，该消息中携带手机的标识、儿童账户的用户名以及儿童账户对应的内容访问控制相关信息；

策略控制实体根据儿童账户对应的内容访问控制相关信息制定内容访问控制策略，该内容访问控制策略使得在儿童账户登录该手机时对游戏相关的流量进行拦截处理；

策略控制实体将手机标识、儿童账户以及儿童账户对应的内容访问控制策略发送给内容拦截实体；

内容拦截实体在儿童账户登录该手机时根据该内容访问控制策略拦截游戏相关的流量。

第二具体实施例

手机的签约用户在银行系统的信用等级下降，银行服务器向身份管理服务器发送手机的签约用户的标识以及信用等级下降信息；

身份管理服务器向策略控制实体发送消息，该消息中包括手机的签约用户的标识以及信用等级下降信息；

策略控制实体根据接收的消息制定该签约用户的内容访问控制策略，使得该签约用户无法使用特定的应用，例如网页浏览应用，并将该内容访问控制策略发送给内容拦截实体；

内容拦截实体在手机的签约账户登录手机时根据该内容访问控制策略拦截网页浏览应用相关的流量。

第三具体实施例

计费系统发现用户欠费超过预设金额，向身份管理服务器发送用户标识（如 IMSI）以及欠费信息；

身份管理服务器向策略控制实体发送消息，该消息中携带用户标识和欠费信息；

策略控制实体根据接收的消息制定该签约用户的内容访问控制策略，使得该签约用户无法使用特定的应用，例如网页浏览应用，并将该内容访问控制策略发送给内容拦截实体；

内容拦截实体在手机的签约账户登录手机时根据该内容访问控制策略拦截网页浏览应用相关的流量。

如图 7 所示，本发明第五实施例中提供了一种内容拦截实体，该内容拦截实体的具体实施可参见上述方法部分的描述，重复之处不再赘述，该内容拦截实体主要包括：

获取模块 701，用于获取当前使用终端的访问用户的数据包；

拦截模块 702，用于根据所述当前使用终端的访问用户对应的内容访问控制策略，判断是否拦截所述数据包，若不拦截，将所述数据包发送至下一跳设备，否则，拦截所述数据包。

实施中，所述获取模块还用于：

获取当前使用终端的访问用户的数据包之前，

获取所述终端配置的所述终端的两个以上访问用户各自对应的内容访问控制相关信息，分别根据所述两个以上访问用户各自对应的内容访问控制相关信息，获得所述两个以上访问用户各自对应的内容访问控制策略；

和/或，

获取策略控制实体配置的所述终端的两个以上访问用户各自对应的内容访问控制策略。

实施中，所述获取模块还用于：

获取当前使用终端的访问用户的数据包之前，获取策略控制实体配置的所述当前使用终端的访问用户的内容访问控制策略。

实施中，所述拦截模块具体用于：

获取所述终端发送的通知消息，所述通知消息中携带所述当前使用终端的访问用户的身份标识，根据所述身份标识确定所述当前使用终端的用户对应的内容访问控制策略；或者，

获取身份管理服务器发送的通知消息，所述通知消息中携带所述当前使用终端的访问用户的身份标识，根据所述身份标识确定所述当前使用终端的用户对应的内容访问控制策略。

如图 8 所示，本发明第六实施例中提供了一种身份管理服务器，该身份管理服务器的具体实施可参见上述方法实施例部分的描述，重复之处不再赘述，该身份管理服务器主要

包括:

获取模块 801，用于获取终端的访问用户的内容访问控制相关信息;

发送模块 802，用于向策略控制实体发送所述访问用户的内容访问控制相关信息，由所述策略控制实体根据接收的所述访问用户的内容访问控制相关信息确定对应的内容访问控制策略，将确定的内容访问控制策略发送给内容拦截实体，由所述内容拦截实体根据接收的内容访问控制策略拦截数据包。

实施中，所述发送模块具体用于:

向策略控制实体发送当前使用所述终端的访问用户对应的内容访问控制相关信息;

或者，

向策略控制实体发送所述终端的两个以上访问用户各自对应的内容访问控制相关信息。

实施中，所述获取模块具体用于:

获取所述终端配置的所述终端的至少一个访问用户各自对应的内容访问控制相关信息; 和/或，

获取第三方系统发送的所述终端的至少一个访问用户各自对应的内容访问控制相关信息。

实施中，还包括接收模块 803，用于:

在所述发送模块向策略控制实体发送当前使用所述终端的访问用户对应的内容访问控制相关信息之前，接收所述终端发送的通知消息，所述通知消息中携带所述当前使用所述终端的访问用户的身份标识，根据所述身份标识确定当前使用所述终端的访问用户对应的内容访问控制相关信息。

如图 9 所示，本发明第七实施例中提供了一种终端，该终端的具体实施可参见上述方法实施例部分的描述，重复之处不再赘述，该终端主要包括:

确定模块 901，用于确定当前使用所述终端的访问用户;

通知模块 902，用于通知内容拦截实体根据所述当前使用所述终端的访问用户对应的内容访问控制策略拦截数据包。

实施中，还包括获取模块 903，用于获取访问用户的内容访问控制相关信息;

配置模块 904，用于根据所述访问用户的内容访问控制相关信息配置内容拦截实体，由所述内容拦截实体获取所述访问用户的内容访问控制相关信息对应的内容访问控制策略，所述访问用户为所述当前使用所述终端的访问用户或者为所述终端的两个以上的访问用户。

实施中，所述配置模块具体用于:

将所述访问用户的内容访问控制相关信息直接发送给所述内容拦截实体;

或者，

将所述访问用户的内容访问控制相关信息发送给身份管理服务器，由所述身份管理服务器向策略控制实体发送所述访问用户的内容访问控制相关信息，由所述策略控制实体根据所述访问用户的内容访问控制相关信息确定对应的内容访问控制策略，将确定的内容访问控制策略发送给所述内容拦截实体。

实施中，所述通知模块具体用于:

向所述内容拦截实体发送通知消息，所述通知消息中携带所述当前使用所述终端的访问用户的身份标识，由所述内容拦截实体根据所述通知消息获取所述当前使用所述终端的访问用户对应的内容访问控制策略，并根据所述当前使用所述终端的访问用户对应的内容访问控制策略拦截数据包。

实施中，所述通知模块还用于:

向所述身份管理服务器发送通知消息，所述通知消息中携带所述当前使用所述终端的访问用户的身份标识，由所述身份管理服务器根据所述通知消息向所述策略控制实体发送所述当前使用所述终端的访问用户对应的内容访问控制相关信息，由所述策略控制实体根据所述当前使用所述终端的访问用户的内容访问控制相关信息确定对应的内容访问控制策略，将所述当前使用所述终端的访问用户对应的内容访问控制策略发送给所述内容拦截实体。

如图 10 所示，本发明第八实施例中，提供了另一种内容拦截实体，该内容拦截实体可以是一个独立的设备，也可以为集成在一个网络设备中，该内容拦截实体主要包括处理器 1001、存储器 1002 和收发机 1003，其中，收发机用于在处理器的控制下接收和发送数据，存储器中保存有预设的程序，处理器用于读取存储器中保存的程序，按照该程序执行以下过程:

通过收发机获取当前使用终端的访问用户的数据包;

根据所述当前使用终端的访问用户对应的内容访问控制策略，判断是否拦截所述数据包，若不拦截，通过收发机将所述数据包发送至下一跳设备，否则，拦截所述数据包。

可能的实施方式中，处理器通过收发机获取当前使用终端的访问用户的数据包之前，通过收发机获取所述终端配置的所述终端的两个以上访问用户各自对应的内容访问控制相关信息，分别根据所述两个以上访问用户各自对应的内容访问控制相关信息，获得所述两个以上访问用户各自对应的内容访问控制策略;

和/或，

通过收发机获取策略控制实体配置的所述终端的两个以上访问用户各自对应的内容访问控制策略。

可能的实施方式中，处理器通过收发机获取当前使用终端的访问用户的数据包之前，通过收发机获取策略控制实体配置的所述当前使用终端的访问用户的内容访问控制策略。

可能的实施方式中，处理器通过收发机获取所述终端发送的通知消息，所述通知消息中携带所述当前使用终端的访问用户的身份标识，根据所述身份标识确定所述当前使用终端的用户对应的内容访问控制策略；或者，

通过收发机获取身份管理服务器发送的通知消息，所述通知消息中携带所述当前使用终端的访问用户的身份标识，根据所述身份标识确定所述当前使用终端的用户对应的内容访问控制策略。

如图 11 所示，本发明第九实施例中，提供了另一种身份管理服务器，该身份管理服务器主要包括处理器 1101、存储器 1102 和收发机 1103，其中，收发机 1103 用于在处理器 1101 的控制下接收和发送数据，存储器 1102 中保存有预设的程序，处理器 1101 用于读取存储器 1102 中保存的程序，按照该程序执行以下过程：

通过收发机获取终端的访问用户的内容访问控制相关信息；

通过收发机向策略控制实体发送所述访问用户的内容访问控制相关信息，由所述策略控制实体根据接收的所述访问用户的内容访问控制相关信息确定对应的内容访问控制策略，将确定的内容访问控制策略发送给内容拦截实体，由所述内容拦截实体根据接收的内容访问控制策略拦截数据包。

可能的实施方式中，处理器通过收发机向策略控制实体发送当前使用所述终端的访问用户对应的内容访问控制相关信息；

或者，

处理器通过收发机向策略控制实体发送所述终端的两个以上访问用户各自对应的内容访问控制相关信息。

可能的实施方式中，处理器在通过收发机获取所述终端配置的所述终端的至少一个访问用户各自对应的内容访问控制相关信息；和/或，

通过收发机获取第三方系统发送的所述终端的至少一个访问用户各自对应的内容访问控制相关信息。

可能的实施方式中，处理器通过收发机接收所述终端发送的通知消息，所述通知消息中携带所述当前使用所述终端的访问用户的身份标识，根据所述身份标识确定所述当前使

用所述终端的访问用户对应的内容访问控制相关信息。

如图 12 所示，本发明第十实施例中，提供了一种终端，该终端主要包括处理器 1201、存储器 1202 和收发机 1203，其中，收发机 1203 用于在处理器 1201 的控制下接收和发送数据，存储器 1202 中保存有预设的程序，处理器 1201 用于读取存储器 1202 中保存的程序，按照该程序执行以下过程:

确定当前使用所述终端的访问用户;

通过收发机通知内容拦截实体根据所述当前使用所述终端的访问用户对应的内容访问控制策略拦截数据包。

可能的实施方式中，处理器通过收发机获取访问用户的内容访问控制相关信息;

根据所述访问用户的内容访问控制相关信息配置内容拦截实体，由所述内容拦截实体获取所述访问用户的内容访问控制相关信息对应的内容访问控制策略，所述访问用户为所述当前使用所述终端的访问用户或者为所述终端的两个以上的访问用户。

可能的实施方式中，处理器通过收发机将所述访问用户的内容访问控制相关信息直接发送给所述内容拦截实体;

或者，

通过收发机将所述访问用户的内容访问控制相关信息发送给身份管理服务器，由所述身份管理服务器向策略控制实体发送所述访问用户的内容访问控制相关信息，由所述策略控制实体根据所述访问用户的内容访问控制相关信息确定对应的内容访问控制策略，将确定的内容访问控制策略发送给所述内容拦截实体。

可能的实施方式中，处理器通过收发机向所述内容拦截实体发送通知消息，所述通知消息中携带所述当前使用所述终端的访问用户的身份标识，由所述内容拦截实体根据所述通知消息获取所述当前使用所述终端的访问用户对应的内容访问控制策略，并根据所述当前使用所述终端的访问用户对应的内容访问控制策略拦截数据包。

可能的实施方式中，处理器通过收发机向所述身份管理服务器发送通知消息，所述通知消息中携带所述当前使用所述终端的访问用户的身份标识，由所述身份管理服务器根据所述通知消息向所述策略控制实体发送所述当前使用所述终端的访问用户对应的内容访问控制相关信息，由所述策略控制实体根据所述当前使用所述终端的访问用户的内容访问控制相关信息确定对应的内容访问控制策略，将所述当前使用所述终端的访问用户对应的内容访问控制策略发送给所述内容拦截实体。

其中，第八至第十实施例中，处理器、存储器与收发机之间通过总线连接，总线架构可以包括任意数量的互联的总线和桥，具体由处理器代表的一个或多个处理器和存储器代

表的存储器的各种电路链接在一起。总线架构还可以将诸如外围设备、稳压器和功率管理电路等之类的各种其他电路链接在一起，这些都是本领域所公知的，因此，本文不再对其进行进一步描述。总线接口提供接口。收发机可以是多个元件，即包括发送机和收发机，提供用于在传输介质上与各种其他装置通信的单元。处理器负责管理总线架构和通常的处理，存储器可以存储处理器在执行操作时所使用的数据。

本领域内的技术人员应明白，本发明的实施例可提供为方法、系统、或计算机程序产品。因此，本发明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，本发明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。

本发明是参照根据本发明实施例的方法、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。

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。

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。

尽管已描述了本发明的优选实施例，但本领域内的技术人员一旦得知了基本创造性概念，则可对这些实施例作出另外的变更和修改。所以，所附权利要求意欲解释为包括优选实施例以及落入本发明范围的所有变更和修改。

显然，本领域的技术人员可以对本发明实施例进行各种改动和变型而不脱离本发明实施例的精神和范围。这样，倘若本发明实施例的这些修改和变型属于本发明权利要求及其等同技术的范围之内，则本发明也意图包含这些改动和变型在内。

权 利 要 求

1、一种内容访问控制方法，其特征在于，包括:

内容拦截实体获取当前使用终端的访问用户的数据包;

所述内容拦截实体根据所述当前使用终端的访问用户对应的内容访问控制策略，判断是否拦截所述数据包，若不拦截，将所述数据包发送至下一跳设备，否则，拦截所述数据包。

2、如权利要求 1 所述的方法，其特征在于，所述内容拦截实体获取当前使用终端的访问用户的数据包之前，所述方法还包括:

所述内容拦截实体获取所述终端配置的所述终端的两个以上访问用户各自对应的内容访问控制相关信息，分别根据所述两个以上访问用户各自对应的内容访问控制相关信息，获得所述两个以上访问用户各自对应的内容访问控制策略;

和/或，

所述内容拦截实体获取策略控制实体配置的所述终端的两个以上访问用户各自对应的内容访问控制策略。

3、如权利要求 1 所述的方法，其特征在于，所述内容拦截实体获取当前使用终端的访问用户的数据包之前，所述方法还包括:

所述内容拦截实体获取策略控制实体配置的所述当前使用终端的访问用户的内容访问控制策略。

4、如权利要求 2 所述的方法，其特征在于，所述内容拦截实体根据所述当前使用终端的访问用户对应的内容访问控制策略，判断是否拦截所述数据包，包括:

所述内容拦截实体获取所述终端发送的通知消息，所述通知消息中携带所述当前使用终端的访问用户的身份标识，根据所述身份标识确定所述当前使用终端的用户对应的内容访问控制策略; 或者，

所述内容拦截实体获取身份管理服务器发送的通知消息，所述通知消息中携带所述当前使用终端的访问用户的身份标识，根据所述身份标识确定所述当前使用终端的用户对应的内容访问控制策略。

5、一种内容访问控制方法，其特征在于，包括:

身份管理服务器获取终端的访问用户的内容访问控制相关信息;

所述身份管理服务器向策略控制实体发送所述访问用户的内容访问控制相关信息，由所述策略控制实体根据接收的所述访问用户的内容访问控制相关信息确定对应的内容访问控制策略，将确定的内容访问控制策略发送给内容拦截实体，由所述内容拦截实体根据接收的内容访问控制策略拦截数据包。

6、如权利要求 5 所述的方法，其特征在于，所述身份管理服务器向策略控制实体发

送所述访问用户的内容访问控制相关信息，包括:

所述身份管理服务器向策略控制实体发送当前使用所述终端的访问用户对应的内容访问控制相关信息;

或者，

所述身份管理服务器向策略控制实体发送所述终端的两个以上访问用户各自对应的内容访问控制相关信息。

7、如权利要求 5 所述的方法，其特征在于，所述身份管理服务器获取终端的访问用户的内容访问控制相关信息，包括:

所述身份管理服务器获取所述终端配置的所述终端的至少一个访问用户各自对应的内容访问控制相关信息; 和/或，

所述身份管理服务器获取第三方系统发送的所述终端的至少一个访问用户各自对应的内容访问控制相关信息。

8、如权利要求 6 所述的方法，其特征在于，所述身份管理服务器向策略控制实体发送当前使用所述终端的访问用户对应的内容访问控制相关信息之前，所述方法还包括:

所述身份管理服务器接收所述终端发送的通知消息，所述通知消息中携带所述当前使用所述终端的访问用户的身份标识，根据所述身份标识确定所述当前使用所述终端的访问用户对应的内容访问控制相关信息。

9、一种内容访问控制方法，其特征在于，包括:

终端确定当前使用所述终端的访问用户;

所述终端通知内容拦截实体根据所述当前使用所述终端的访问用户对应的内容访问控制策略拦截数据包。

10、如权利要求 9 所述的方法，其特征在于，所述方法还包括:

所述终端获取访问用户的内容访问控制相关信息;

所述终端根据所述访问用户的内容访问控制相关信息配置内容拦截实体，由所述内容拦截实体获取所述访问用户的内容访问控制相关信息对应的内容访问控制策略，所述访问用户为所述当前使用所述终端的访问用户或者为所述终端的两个以上的访问用户。

11、如权利要求 10 所述的方法，其特征在于，所述终端根据所述访问用户的内容访问控制相关信息配置内容拦截实体，包括:

所述终端将所述访问用户的内容访问控制相关信息直接发送给所述内容拦截实体;

或者，

所述终端将所述访问用户的内容访问控制相关信息发送给身份管理服务器，由所述身份管理服务器向策略控制实体发送所述访问用户的内容访问控制相关信息，由所述策略控制实体根据所述访问用户的内容访问控制相关信息确定对应的内容访问控制策略，将确定

的内容访问控制策略发送给所述内容拦截实体。

12、如权利要求 9、10 或 11 所述的方法，其特征在于，所述终端通知内容拦截实体根据所述当前使用所述终端的访问用户对应的内容访问控制策略拦截数据包，包括:

所述终端向所述内容拦截实体发送通知消息，所述通知消息中携带所述当前使用所述终端的访问用户的身份标识，由所述内容拦截实体根据所述通知消息获取所述当前使用所述终端的访问用户对应的内容访问控制策略，并根据所述当前使用所述终端的访问用户对应的内容访问控制策略拦截数据包。

13、如权利要求 11 所述的方法，其特征在于，所述方法还包括:

所述终端向所述身份管理服务器发送通知消息，所述通知消息中携带所述当前使用所述终端的访问用户的身份标识，由所述身份管理服务器根据所述通知消息向所述策略控制实体发送所述当前使用所述终端的访问用户对应的内容访问控制相关信息，由所述策略控制实体根据所述当前使用所述终端的访问用户的内容访问控制相关信息确定对应的内容访问控制策略，将所述当前使用所述终端的访问用户对应的内容访问控制策略发送给所述内容拦截实体。

14、一种内容访问控制系统，其特征在于，包括:

终端，用于确定当前使用所述终端的访问用户，并通知内容拦截实体根据所述当前使用所述终端的访问用户对应的内容访问控制策略拦截数据包;

内容拦截实体，用于获取所述当前使用所述终端的访问用户的数据包，根据所述当前使用所述终端的访问用户对应的内容访问控制策略判断是否拦截所述数据包，若不拦截，将所述数据包发送至下一跳设备，否则，拦截所述数据包。

15、如权利要求 14 所述的系统，其特征在于，所述终端还用于:

获取访问用户的内容访问控制相关信息，根据所述访问用户的内容访问控制相关信息配置内容拦截实体，其中，所述访问用户为所述当前使用所述终端的访问用户或者为所述终端的两个以上的访问用户;

所述内容拦截实体还用于:

获取所述访问用户的内容访问控制相关信息对应的内容访问控制策略。

16、如权利要求 15 所述的系统，其特征在于，还包括身份管理服务器和策略控制实体;

所述终端具体用于:

将所述访问用户的内容访问控制相关信息发送给所述身份管理服务器;

所述身份管理服务器用于:

接收所述终端发送的所述访问用户的内容访问控制相关信息，向所述策略控制实体发送所述访问用户的内容访问控制相关信息;

所述策略控制实体用于:

根据所述身份管理服务器发送的所述访问用户的内容访问控制相关信息，确定对应的内容访问控制策略，将确定的内容访问控制策略发送给所述内容拦截实体。

17、一种内容拦截实体，其特征在于，包括:

获取模块，用于获取当前使用终端的访问用户的数据包;

拦截模块，用于根据所述当前使用终端的访问用户对应的内容访问控制策略，判断是否拦截所述数据包，若不拦截，将所述数据包发送至下一跳设备，否则，拦截所述数据包。

18、如权利要求 17 所述的内容拦截实体，其特征在于，所述获取模块还用于:

获取当前使用终端的访问用户的数据包之前，

获取所述终端配置的所述终端的两个以上访问用户各自对应的内容访问控制相关信息，分别根据所述两个以上访问用户各自对应的内容访问控制相关信息，获得所述两个以上访问用户各自对应的内容访问控制策略;

和/或，

获取策略控制实体配置的所述终端的两个以上访问用户各自对应的内容访问控制策略。

19、如权利要求 17 所述的内容拦截实体，其特征在于，所述获取模块还用于:

获取当前使用终端的访问用户的数据包之前，获取策略控制实体配置的所述当前使用终端的访问用户的内容访问控制策略。

20、如权利要求 18 所述的内容拦截实体，其特征在于，所述拦截模块具体用于:

获取所述终端发送的通知消息，所述通知消息中携带所述当前使用终端的访问用户的身份标识，根据所述身份标识确定所述当前使用终端的用户对应的内容访问控制策略；或者，

获取身份管理服务器发送的通知消息，所述通知消息中携带所述当前使用终端的访问用户的身份标识，根据所述身份标识确定所述当前使用终端的用户对应的内容访问控制策略。

21、一种身份管理服务器，其特征在于，包括:

获取模块，用于获取终端的访问用户的内容访问控制相关信息;

发送模块，用于向策略控制实体发送所述访问用户的内容访问控制相关信息，由所述策略控制实体根据接收的所述访问用户的内容访问控制相关信息确定对应的内容访问控制策略，将确定的内容访问控制策略发送给内容拦截实体，由所述内容拦截实体根据接收的内容访问控制策略拦截数据包。

22、如权利要求 21 所述的身份管理服务器，其特征在于，所述发送模块具体用于:

向策略控制实体发送当前使用所述终端的访问用户对应的内容访问控制相关信息;

或者，

向策略控制实体发送所述终端的两个以上访问用户各自对应的内容访问控制相关信息。

23、如权利要求 21 所述的身份管理服务器，其特征在于，所述获取模块具体用于：

获取所述终端配置的所述终端的至少一个访问用户各自对应的内容访问控制相关信息；和/或，

获取第三方系统发送的所述终端的至少一个访问用户各自对应的内容访问控制相关信息。

24、如权利要求 22 所述的身份管理服务器，其特征在于，还包括接收模块，用于：

在所述发送模块向策略控制实体发送当前使用所述终端的访问用户对应的内容访问控制相关信息之前，接收所述终端发送的通知消息，所述通知消息中携带所述当前使用所述终端的访问用户的身份标识，根据所述身份标识确定当前使用所述终端的访问用户对应的内容访问控制相关信息。

25、一种终端，其特征在于，包括：

确定模块，用于确定当前使用所述终端的访问用户；

通知模块，用于通知内容拦截实体根据所述当前使用所述终端的访问用户对应的内容访问控制策略拦截数据包。

26、如权利要求 25 所述的终端，其特征在于，还包括获取模块，用于获取访问用户的内容访问控制相关信息；

配置模块，用于根据所述访问用户的内容访问控制相关信息配置内容拦截实体，由所述内容拦截实体获取所述访问用户的内容访问控制相关信息对应的内容访问控制策略，所述访问用户为所述当前使用所述终端的访问用户或者为所述终端的两个以上的访问用户。

27、如权利要求 26 所述的终端，其特征在于，所述配置模块具体用于：

将所述访问用户的内容访问控制相关信息直接发送给所述内容拦截实体；

或者，

将所述访问用户的内容访问控制相关信息发送给身份管理服务器，由所述身份管理服务器向策略控制实体发送所述访问用户的内容访问控制相关信息，由所述策略控制实体根据所述访问用户的内容访问控制相关信息确定对应的内容访问控制策略，将确定的内容访问控制策略发送给所述内容拦截实体。

28、如权利要求 25、26 或 27 所述的终端，其特征在于，所述通知模块具体用于：

向所述内容拦截实体发送通知消息，所述通知消息中携带所述当前使用所述终端的访问用户的身份标识，由所述内容拦截实体根据所述通知消息获取所述当前使用所述终端的访问用户对应的内容访问控制策略，并根据所述当前使用所述终端的访问用户对应的内容

访问控制策略拦截数据包。

29、如权利要求 27 所述的终端，其特征在于，所述通知模块还用于:

向所述身份管理服务器发送通知消息，所述通知消息中携带所述当前使用所述终端的访问用户的身份标识，由所述身份管理服务器根据所述通知消息向所述策略控制实体发送所述当前使用所述终端的访问用户对应的内容访问控制相关信息，由所述策略控制实体根据所述当前使用所述终端的访问用户的内容访问控制相关信息确定对应的内容访问控制策略，将所述当前使用所述终端的访问用户对应的内容访问控制策略发送给所述内容拦截实体。

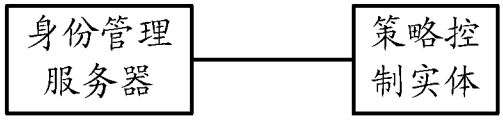
身份管理
服务器
策略控
制实体

图 1

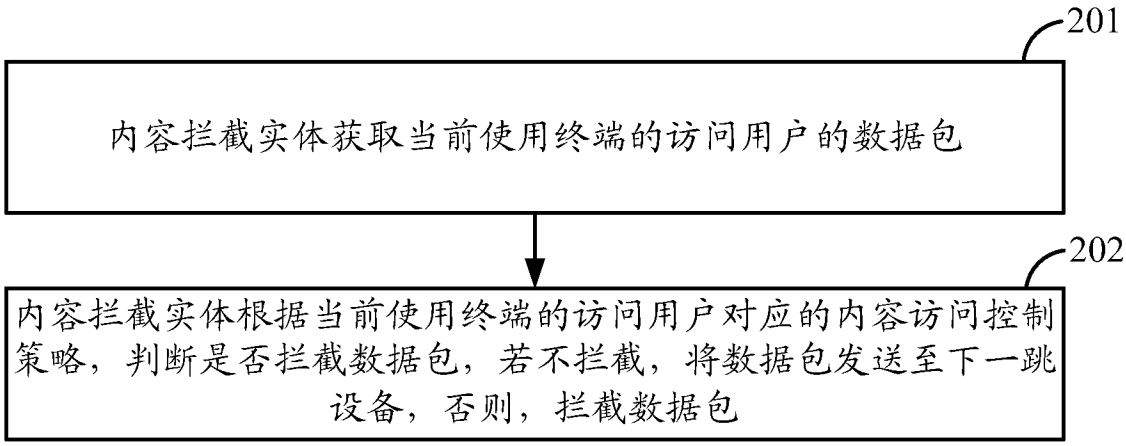
201
内容拦截实体获取当前使用终端的访问用户的数据包
202
内容拦截实体根据当前使用终端的访问用户对应的内容访问控制策略，判断是否拦截数据包，若不拦截，将数据包发送至下一跳设备，否则，拦截数据包

图 2

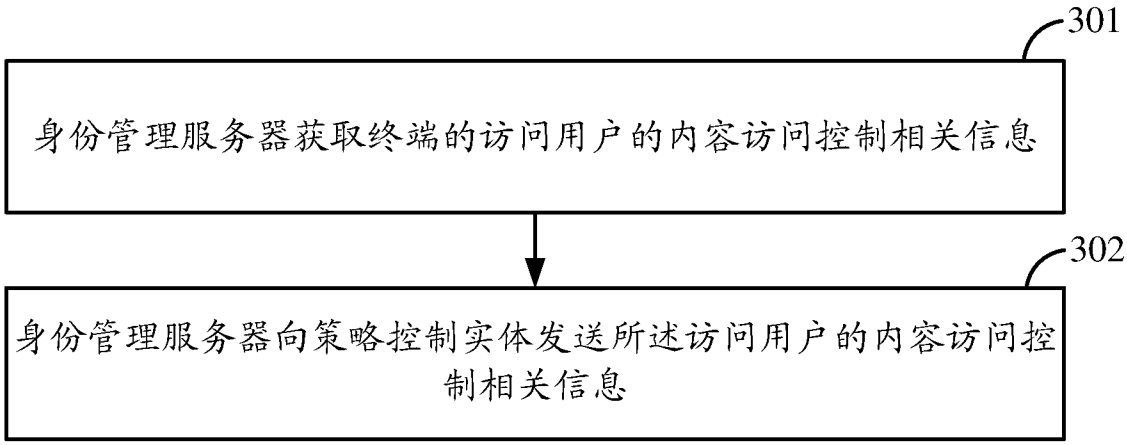
301
身份管理服务器获取终端的访问用户的内容访问控制相关信息
302
身份管理服务器向策略控制实体发送所述访问用户的内容访问控制相关信息

图 3

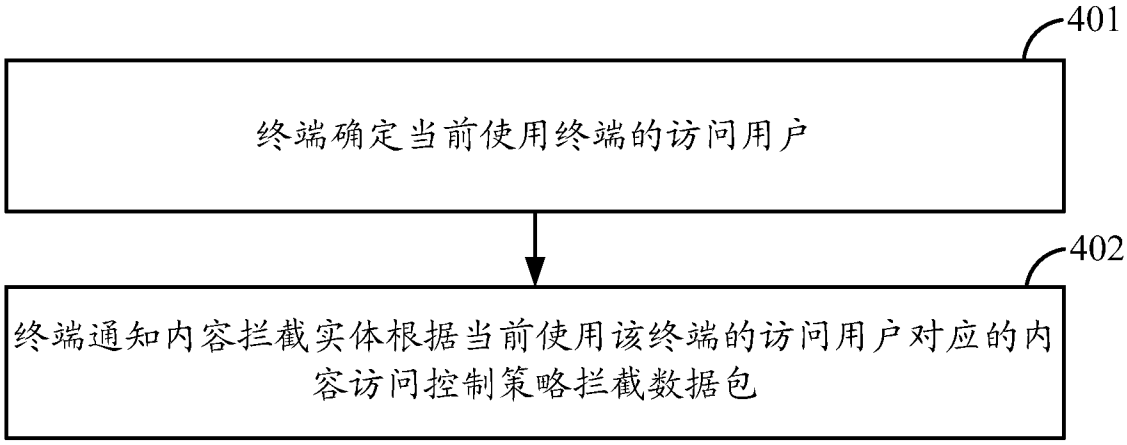
401
终端确定当前使用终端的访问用户
402
终端通知内容拦截实体根据当前使用该终端的访问用户对应的内容访问控制策略拦截数据包

图 4

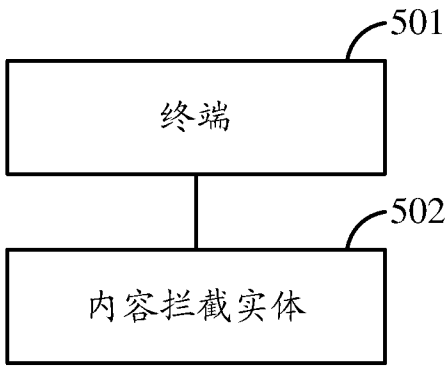

图 5

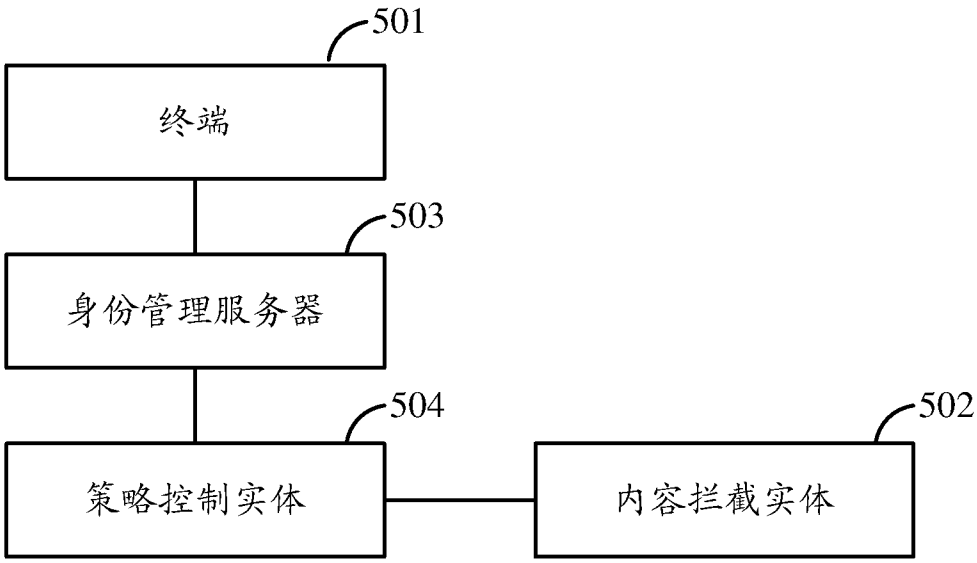

图 6

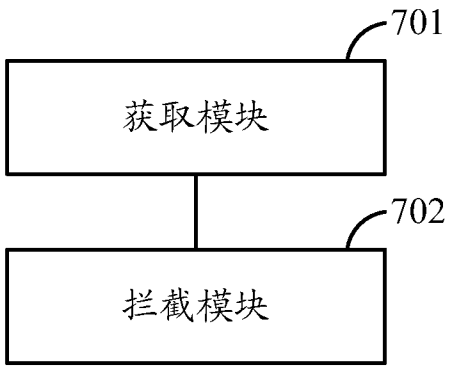

图 7

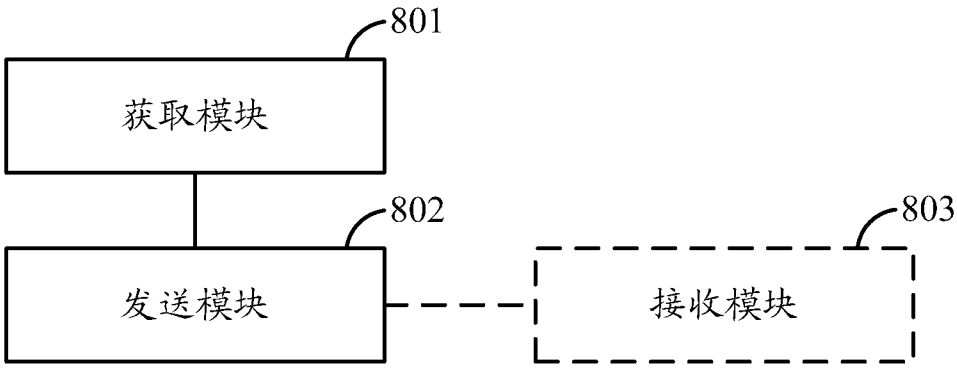

图 8

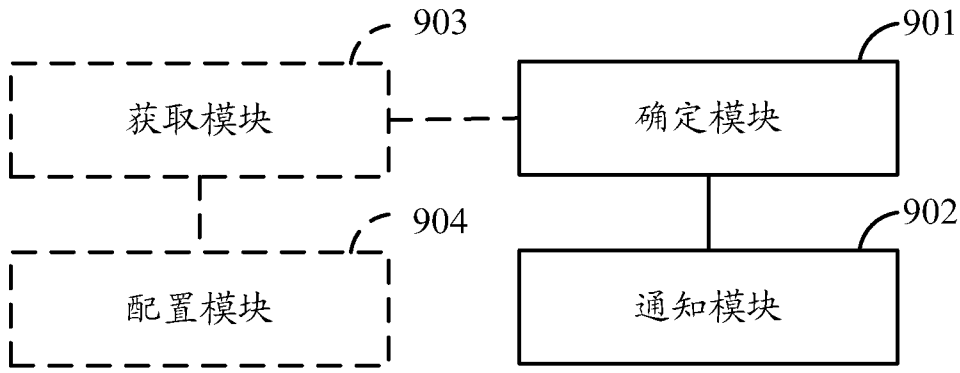
903
901
获取模块
确定模块
904
902
配置模块
通知模块

图 9

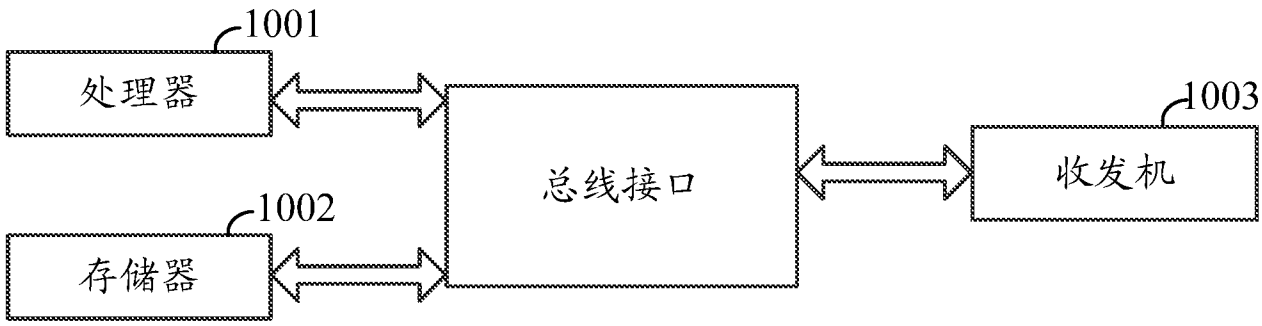
1001
处理器
1003
总线接口
收发机
1002
存储器

图 10

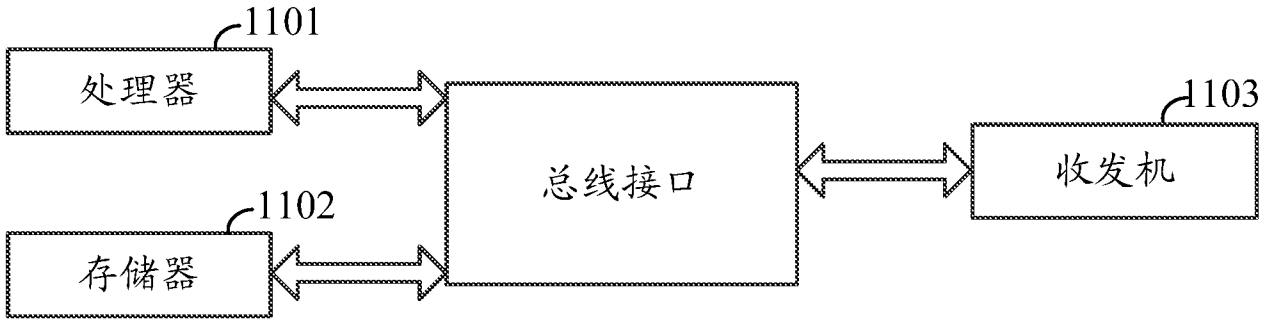
1101
处理器
1102
存储器
总线接口
1103
收发机

图 11

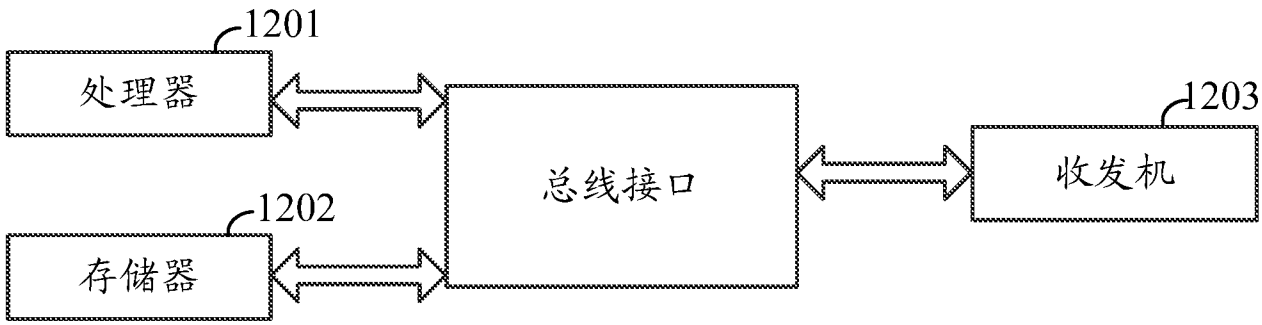
1201
处理器
1202
存储器
总线接口
1203
收发机

图 12

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2016/105775

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06 (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)

CNKI, CNPAT, WPI, EPODOC: multi+, user, different, same, terminal, pc, parent, child+, right, access, control, ACL, policy, strategy, use

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 103404093 A (NEC CORP.) 20 November 2013 (20.11.2013) description, paragraphs [0013]-[0023] and [0039]-[0090]	1-29
X	CN 104284027 A (DONGGUAN YULONG COMMUNICATION TECHNOLOGY CO., LTD.) 14 January 2015 (14.01.2015) description, paragraphs [0031]-[0064]	1-29
A	CN 101056343 A (HUAWEI TECHNOLOGIES CO., LTD.) 17 October 2007 (17.10.2007) the whole document	1-29
A	CN 1984402 A (HUAWEI TECHNOLOGIES CO., LTD.) 20 June 2007 (20.06.2007) the whole document	1-29
A	WO 2014135047 A1 (ZTE CORPORATION) 12 September 2014 (12.09.2014) the whole document	1-29

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
15 January 2017	25 January 2017
Name and mailing address of the ISA State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No. (86-10) 62019451	Authorized officer LI, Xiaoli Telephone No. (86-10) 62414494

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2016/105775

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 103404093 A	20 November 2013	RU 2013143020 A	27 March 2015
		JP 5811171 B2	11 November 2015
		WO 2012115058 A1	30 August 2012
		US 2013329738 A1	12 December 2013
		EP 2680506 A1	01 January 2014
CN 104284027 A	14 January 2015	None	
CN 101056343 A	17 October 2007	None	
CN 1984402 A	20 June 2007	None	
WO 2014135047 A1	12 September 2014	CN 104349370 A	11 February 2015

国际检索报告

国际申请号
PCT/CN2016/105775

A. 主题的分类

H04L 29/06(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））

CNKI，CNPAT，WPI，EPODOC：多用户，多个用户，不同用户，同一，终端，子女，儿童，孩子，父母，使用，权限，访问控制策略，访问控制，策略，multi+，user，different，same，terminal，pc，parent，child+，right，access，control，ACL，policy，strategy

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
X	CN 103404093 A (日本电气株式会社) 2013年 11月 20日 (2013-11-20) 说明书第[0013]-[0023]、[0039]-[0090]段	1-29
X	CN 104284027 A (东莞宇龙通信科技有限公司) 2015年 1月 14日 (2015-01-14) 说明书第[0031]-[0064]段	1-29
A	CN 101056343 A (华为技术有限公司) 2007年 10月 17日 (2007-10-17) 全文	1-29
A	CN 1984402 A (华为技术有限公司) 2007年 6月 20日 (2007-06-20) 全文	1-29
A	WO 2014135047 A1 (中兴通讯股份有限公司) 2014年 9月 12日 (2014-09-12) 全文	1-29

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2017年 1月 15日	2017年 1月 25日
ISA/CN的名称和邮寄地址 中华人民共和国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10)62019451	受权官员 李晓利 电话号码 (86-10)62414494

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2016/105775

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	103404093	A	2013年 11月 20日	RU	2013143020	A	2015年 3月 27日
				JP	5811171	B2	2015年 11月 11日
				WO	2012115058	A1	2012年 8月 30日
				US	2013329738	A1	2013年 12月 12日
				EP	2680506	A1	2014年 1月 1日
CN	104284027	A	2015年 1月 14日		无		
CN	101056343	A	2007年 10月 17日		无		
CN	1984402	A	2007年 6月 20日		无		
WO	2014135047	A1	2014年 9月 12日	CN	104349370	A	2015年 2月 11日