(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 104967589 B
(45)授权公告日 2019.02.05

(21)申请号 201410227945.7

(22)申请日 2014.05.27

(65)同一申请的已公布的文献号
申请公布号 CN 104967589 A

(43)申请公布日 2015.10.07

(73)专利权人 腾讯科技(深圳)有限公司
地址 518000 广东省深圳市福田区振兴路赛格科技园2栋东403室

(72)发明人 罗喜军 陈曦

(74)专利代理机构 深圳市深佳知识产权代理事务所(普通合伙) 44285
代理人 王仲凯

(51)Int.Cl.
H04L 29/06(2006.01)

(56)对比文件
CN 101459548 A,2009.06.17,
CN 101459548 A,2009.06.17,
CN 103051617 A,2013.04.17,
CN 101902456 A,2010.12.01,
EP 1960867 A2,2008.08.27,
US 2006064598 A1,2006.03.23,
CN 101572700 A,2009.11.04,

审查员 肖敬伟

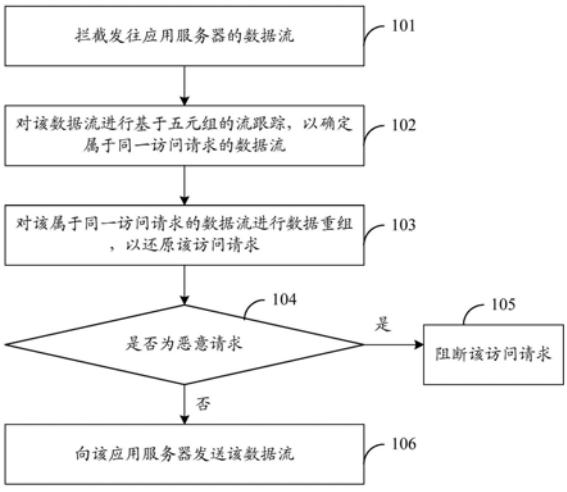
权利要求书1页 说明书11页 附图5页

(54)发明名称

一种安全性检测方法、装置和系统

(57)摘要

本发明实施例公开了一种安全性检测方法、装置和系统，本发明实施例采用拦截发往应用服务器的数据流，对该数据流进行基于五元组的流跟踪，以确定属于同一访问请求的数据流，然后对属于该同一访问请求的数据流进行数据重组，以还原该访问请求，并对该访问请求进行检测，若为恶意请求，则阻断该访问请求，否则，则向该应用服务器发送该数据流，从而实现防止漏洞攻击的恶意请求的目的。该方案可以减低开发和运维成本，而且，无需占用应用服务器的资源，有利于提高服务器性能。



CN 104967589 B

1.一种安全性检测方法,其特征在于,包括:

向应用服务器对应的核心层路由设备发送动态牵引指令;

接收所述核心层路由设备根据所述动态牵引指令所牵引的数据流;

对所述数据流进行基于五元组的流跟踪,对该数据流中数据包的包头进行解析,提取源地址和目的地址,将具有同一源地址和目的地址的所有数据包作为属于同一访问请求的数据流;

基于传输控制协议对所述属于同一访问请求的数据流进行数据重组,以还原所述访问请求;

根据所述访问请求查询病毒库,若所述访问请求中存在与所述病毒库匹配的字段,则确定所述访问请求为恶意请求;若所述访问请求中不存在与所述病毒库匹配的字段,则确定所述访问请求不是恶意请求;

在确定所述访问请求是恶意请求时,则阻断所述访问请求;

在确定所述访问请求不是恶意请求时,则向所述应用服务器发送所述数据流。

2.根据权利要求1所述的方法,其特征在于,所述基于传输控制协议对所述属于同一访问请求的数据流进行数据重组,以还原所述访问请求之后,还包括:

缓存属于同一访问请求的数据流中的至少一个数据包,并将所述属于同一访问请求的数据流中的其他数据包发送给所述应用服务器。

3.根据权利要求1或2所述的方法,其特征在于,所述阻断所述访问请求之后,还包括:

向所述服务器发送指示访问请求已被阻断的通知。

4.一种安全性检测装置,其特征在于,包括:

拦截单元,用于向应用服务器对应的核心层路由设备发送动态牵引指令,接收所述核心层路由设备根据所述动态牵引指令所牵引的数据流;

流跟踪单元,用于对所述数据流进行基于五元组的流跟踪,对该数据流中数据包的包头进行解析,提取源地址和目的地址,将具有同一源地址和目的地址的所有数据包作为属于同一访问请求的数据流;

重组单元,用于基于传输控制协议对所述属于同一访问请求的数据流进行数据重组,以还原所述访问请求;

检测单元,用于根据所述访问请求查询病毒库,若所述访问请求中存在与所述病毒库匹配的字段,则确定所述访问请求为恶意请求;若所述访问请求中不存在与所述病毒库匹配的字段,则确定所述访问请求不是恶意请求;

阻断单元,用于在检测单元确定所述访问请求为恶意请求时,阻断所述访问请求;

发送单元,用于在检测单元确定所述访问请求不是恶意请求时,向所述应用服务器发送所述数据流。

5.根据权利要求4所述的安全性检测装置,其特征在于,还包括缓存单元;

缓存单元,用于缓存属于同一访问请求的数据流中的至少一个数据包,并将所述属于同一访问请求的数据流中的其他数据包发送给所述应用服务器;

所述发送单元,用于在检测单元确定所述访问请求不是恶意请求时,将缓存的数据包发送给所述应用服务器。

6.一种通信系统,其特征在于,包括权利要求4或5所述的安全性检测装置。

一种安全性检测方法、装置和系统

技术领域

[0001] 本发明涉及通信技术领域，具体涉及一种安全性检测方法、装置和系统。

背景技术

[0002] 随着通信技术的发展，各种网络应用服务也日益繁多起来，与此同时，提供服务的应用服务器所面临的威胁也日益增加，而如何保证服务器的安全性，对于整个网络的健康发展而言，也极为重要。

[0003] 对漏洞进行防护是保障服务器安全性的一项重要内容。针对网页(Web)漏洞的防护，传统方法是基于主机层实现，比如，通常可以通过在应用服务器上设置相应的安全接口/模块，来达到对用户请求的检测分析和恶意拦截防护，等等，其中，针对不同的应用服务器特性，需要分别设置相应的安全接口/模块，比如，如果是apache(一种应用服务器软件)，则需要针对apache专门设置对应安全接口/模块，如果是nginx(一种应用服务器软件)，则需要针对nginx专门设置对应安全接口/模块，以此类推，等等，然后，当应用服务器接收到用户的访问请求，比如超文本传输协议(Http，Hypertext transfer protocol)请求后，调用该安全接口/模块对接收到的访问请求进行解析，以进行安全性检测，如果确定该访问行为为恶意，则进行阻断。

[0004] 在对现有技术的研究和实践过程中，本发明的发明人发现，由于应用服务器特性种类繁多，而安全接口/模块均需要根据不同的特性进行定制，因此，开发和运维成本较高，而且，安全接口/模块的安装较为繁琐复杂，工作时也需要占用应用服务器一定的资源，所以，对应用服务器本身的性能也具有一定影响，不利于提高应用服务器的性能。

发明内容

[0005] 本发明实施例提供一种安全性检测方法、装置和系统，不仅可以减低开发和运维成本，而且，无需占用应用服务器的资源，有利于提高服务器性能。

[0006] 一种安全性检测方法，其特征在于，包括：

[0007] 拦截发往应用服务器的数据流；

[0008] 对所述数据流进行基于五元组的流跟踪，以确定属于同一访问请求的数据流；

[0009] 对所述属于同一访问请求的数据流进行数据重组，以还原所述访问请求；

[0010] 对所述访问请求进行检测，以确定所述访问请求是否为恶意请求；

[0011] 若是，则阻断所述访问请求；

[0012] 若否，则向所述应用服务器发送所述数据流。

[0013] 一种安全性检测装置，包括：

[0014] 拦截单元，用于拦截发往应用服务器的数据流；

[0015] 流跟踪单元，用于对所述数据流进行基于五元组的流跟踪，以确定属于同一访问请求的数据流；

[0016] 重组单元，用于对所述属于同一访问请求的数据流进行数据重组，以还原所述访

问请求；

[0017] 检测单元，用于对所述访问请求进行检测，以确定所述访问请求是否为恶意请求；

[0018] 阻断单元，用于在检测单元确定所述访问请求为恶意请求时，阻断所述访问请求；

[0019] 发送单元，用于在检测单元确定所述访问请求不是恶意请求时，向所述应用服务器发送所述数据流。

[0020] 一种通信系统，包括本发明实施例提供的任一种安全性检测装置。

[0021] 本发明实施例采用拦截发往应用服务器的数据流，对该数据流进行基于五元组的流跟踪，以确定属于同一访问请求的数据流，然后对属于该同一访问请求的数据流进行数据重组，以还原该访问请求，并对该访问请求进行检测，以确定该访问请求是否为恶意请求，若为恶意请求，则阻断该访问请求，否则，若不是恶意请求，则向该应用服务器发送该数据流，从而实现防止漏洞攻击的恶意请求的目的。由于在该方案中，采用的是在数据流进入应用服务器之前，由专用的安全性检测装置对该数据流进行安全性检测，因此，并不受制于应用服务器服务软件的特性，相对于现有技术中需要根据不同的特性在应用服务器内设置不同的安全接口/模块而言，大大可以减低开发和运维成本，而且，无需占用应用服务器的资源，有利于提高服务器性能。

附图说明

[0022] 为了更清楚地说明本发明实施例中的技术方案，下面将对实施例描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

[0023] 图1是本发明实施例提供的安全性检测方法的流程图；

[0024] 图2a是本发明实施例提供的安全性检测方法的网络框图；

[0025] 图2b是本发明实施例提供的安全性检测方法的场景示意图；

[0026] 图2c是本发明实施例提供的安全性检测方法的另一流程图；

[0027] 图3是本发明实施例提供的安全性检测装置的结构示意图；

[0028] 图4是本发明实施例提供的网络安全防护设备的结构示意图。

具体实施方式

[0029] 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。

[0030] 本发明实施例提供一种安全性检测方法、装置和系统。以下分别进行详细说明。

[0031] 实施例一、

[0032] 本实施例将从安全性检测装置的角度进行描述，该安全性检测装置可以作为独立的实体来实现，也可以集成在网关等其他的设备中。

[0033] 一种安全性检测方法，包括：拦截发往应用服务器的数据流，对该数据流进行基于五元组的流跟踪，以确定属于同一访问请求的数据流；对该属于同一访问请求的数据流进

行数据重组，以还原该访问请求；对该访问请求进行检测，以确定该访问请求是否为恶意请求，若是，则阻断该访问请求；若否，则向该应用服务器发送该数据流。

[0034] 如图1所示，该安全性检测方法，具体流程可以如下：

[0035] 101、拦截发往应用服务器的数据流，例如，具体可以如下：

[0036] 向该应用服务器对应的核心层路由设备发送动态牵引指令，接收该核心层路由设备根据该动态牵引指令所牵引的数据流。

[0037] 当然，也可以采用其他可以对数据流进行牵引的指令，或者，还可以采用其他的拦截技术，在此不再赘述。

[0038] 102、对该数据流进行基于五元组的流跟踪，以确定属于同一访问请求的数据流。例如，具有可以如下：

[0039] 对该数据流中数据包的包头进行解析，提取源地址和目的地址，将具有同一源地址和目的地址的所有数据包作为属于同一访问请求的数据流。

[0040] 103、对该属于同一访问请求的数据流进行数据重组，以还原该访问请求。

[0041] 基于传输控制协议(TCP，Transmission Control Protocol)对所述属于同一访问请求的数据流进行数据重组，以还原所述访问请求。

[0042] 104、对该访问请求进行检测，以确定该访问请求是否为恶意请求，若为恶意请求，则执行步骤105，若不是恶意请求，则执行步骤106。

[0043] 其中，检测的技术可以有多种，例如，可以预先设置病毒库，通过将访问请求与该病毒库进行字段匹配，来确定该访问请求中是否存在有对应用服务器造成威胁的字段，从而判断该访问请求是否为恶意请求；即步骤“对该访问请求进行检测，以确定该访问请求是否为恶意请求”具体可以如下：

[0044] 根据该访问请求查询病毒库，若该访问请求中存在与所述病毒库匹配的字段，则确定该访问请求为恶意请求；若该访问请求中不存在与该病毒库匹配的字段，则确定该访问请求不是恶意请求。

[0045] 其中，该病毒库可以根据实际应用的需求进行设置，主要用于收集并记录各种可能会对应用服务器造成威胁的访问请求所携带的字段，在此不再赘述。

[0046] 105、在确定该访问请求为恶意请求时，阻断该访问请求，以避免该访问请求对应用服务器造成威胁。

[0047] 可选的，在阻断该访问请求之后，还可以将访问请求的阻断情况通知给应用服务器，即在步骤“阻断该访问请求”之后，该安全性检测方法还可以包括：

[0048] 向该服务器发送指示访问请求已被阻断的通知。

[0049] 106、在确定该访问请求不是恶意请求时，向该应用服务器发送该数据流，即对原拦截到的数据流进行回注。

[0050] 例如，具体可以向核心路由设备发送该数据流，以便该核心路由设备将该数据流发送给应用服务器。

[0051] 需说明的是，为了避免恶意请求完全被透传到应用服务器，在对该访问请求进行检测之前，可以对属于同一访问请求的数据流进行缓存，然后再确定该访问请求不是恶意请求时，才将这些数据流传送给应用服务器。但是，为了减轻负载，提高传输效率，在缓存这些需要进行数据重组的数据流时，也可以只缓存一部分，另一部分则直接转发给应用服务

器，如果后续确定该访问请求为恶意请求，则无需将缓存的数据流发送给应用服务器，而如果后续确定该访问请求不是恶意请求，则将缓存的数据流发送给应用服务器，从而使得应用服务器可以接收到关于该访问请求的完整的数据流。即，在步骤“对该属于同一访问请求的数据流进行数据重组，以还原该访问请求(步骤103)”之后，还可以

[0052] 缓存属于同一访问请求的数据流中的至少一个数据包，并将该属于同一访问请求的数据流中的其他数据包(即除缓存了的数据包之外的其他数据包)发送给所述应用服务器。

[0053] 则此时，步骤“在确定该访问请求不是恶意请求时，向该应用服务器发送所述数据流”可以包括：

[0054] 将缓存的数据包发送给该应用服务器。

[0055] 其中，缓存的数据包的数量和位置可以根据实际应用的需求进行设置，比如，可以缓存某个数据流中最后一个数据包(也称为分片包)、最后两个数据包、前三个数据包、或中间的一个数据包，还可以缓存所有数据包，等等，在此不再赘述。

[0056] 由上可知，本实施例采用拦截发往应用服务器的数据流，对该数据流进行基于五元组的流跟踪，以确定属于同一访问请求的数据流，然后对属于该同一访问请求的数据流进行数据重组，以还原该访问请求，并对该访问请求进行检测，以确定该访问请求是否为恶意请求，若为恶意请求，则阻断该访问请求，否则，若不是恶意请求，则向该应用服务器发送该数据流，从而实现防止漏洞攻击的恶意请求的目的。由于在该方案中，采用的是在数据流进入应用服务器之前，由专用的安全性检测装置对该数据流进行安全性检测，因此，并不受制于应用服务器服务软件的特性，相对于现有技术中需要根据不同的特性在应用服务器内设置不同的安全接口/模块而言，大大可以减低开发和运维成本，而且，无需占用应用服务器的资源，有利于提高服务器性能。

[0057] 实施例二、

[0058] 根据实施例一所描述的方法，以下将举例作进一步详细说明。

[0059] 在本实施例中，将以该安全性检测装置作为独立的实体为例进行说明。为了描述方案，在本发明实施例中，将该实体称为Web应用防火墙(WAF，Web Application Firewall)防护设备。

[0060] 参见图2a和图2b，其中，图2a为本发明实施例提供的安全性检测方法的网络框图，图2b为本发明实施例提供的安全性检测方法的场景示意图，在该场景中，核心路由设备在接收到用户发往应用服务器的访问请求后，可以将该访问请求所对应的数据流牵引到WAF防护设备中，由WAF防护设备对该访问请求的安全性进行检测，如果安全(即不是恶意请求)，才将该访问请求所对应的数据流回注给核心层路由设备，以发送给应用服务器，否则，如果确定该访问请求为恶意请求，则对该访问请求进行阻断。当然，核心层路由设备在将数据流发送给应用服务器时，还需经过一些中间设备或进行一些出来，比如对数据进行接入层交换，等等，在此不再赘述。

[0061] 此外，需说明的是，各个应用服务器的特性可以是相同的，也可以是不同，比如，应用服务器1可以为安装apache服务软件，应用服务器可以按照nginx服务软件，应用服务器3可以按照tomcat服务软件，等等。

[0062] 基于上述应用场景，以下将对该安全性检测方法进行详细说明，如图2c所示，具体

流程可以如下：

[0063] 201、WAF防护设备向核心层路由设备发送动态牵引指令。

[0064] 202、核心层路由设备接收到该动态牵引指令之后，根据该动态牵引指令将发往应用服务器的数据流牵引至WAF防护设备。

[0065] 例如，以该核心层路由设备接收到用户发往服务器1的访问请求K为例，则该核心层路由设备可以根据该动态牵引指令将该访问请求K的数据流牵引至WAF防护设备，即暂时不发送给服务器1，而是发送给WAF防护设备。

[0066] 其中，该访问请求可以是超文本传输协议(HTTP，Hypertext transfer protocol)访问请求或文件传输协议(FTP，File Transfer Protocol)访问请求等。

[0067] 203、WAF防护设备接收到该数据流后，对该数据流进行基于五元组的流跟踪，以确定属于同一访问请求的数据流。

[0068] 例如，具体可以对该数据流中数据包的包头进行解析，提取源地址和目的地址，将具有同一源地址和目的地址的所有数据包作为属于同一访问请求的数据流。

[0069] 需说明的是，由于一个访问请求可能需要多个数据包进行传输，因此，仅仅只依靠解析一个数据包并不足以得到该访问请求完整的信息，因此，需要对这些数据流进行流跟踪，以确定属于同一访问请求的数据流，以便后续可以还原该访问请求。

[0070] 204、WAF防护设备基于TCP协议对该属于同一访问请求的数据流进行数据重组，以还原该访问请求。

[0071] 205、WAF防护设备对该访问请求进行检测，以确定该访问请求是否为恶意请求，若为恶意请求，则执行步骤206，若不是恶意请求，则执行步骤207。

[0072] 例如，可以根据该访问请求查询病毒库，若该访问请求中存在与该病毒库匹配的字段，则确定该访问请求为恶意请求；若该访问请求中不存在与该病毒库匹配的字段，则确定该访问请求不是恶意请求。

[0073] 其中，该病毒库可以根据实际应用的需求进行设置，主要用于收集并记录各种可能会对应用服务器造成威胁的访问请求所携带的字段，在此不再赘述。

[0074] 206、在确定该访问请求为恶意请求时，WAF防护设备阻断该访问请求，以避免该访问请求对应用服务器造成威胁。

[0075] 此时，WAF防护设备还可以向该服务器发送指示访问请求已被阻断的通知，以便应用服务器获知访问请求的阻断情况。

[0076] 207、在确定该访问请求不是恶意请求时，WAF防护设备向该核心路由设备发送该数据流，即对原拦截到的数据流进行回注，然后执行步骤208。

[0077] 208、核心路由设备向应用服务器发送该WAF防护设备回注的数据流。

[0078] 例如，还是以该访问请求为发往服务器1的访问请求K为例，则此时，核心路由设备向应用服务器1发送该访问请求K的数据流。

[0079] 需说明的是，为了避免恶意请求完全被透传到应用服务器，在对该访问请求进行检测之前，可以对属于同一访问请求的数据流进行缓存，然后再确定该访问请求不是恶意请求时，才将这些数据流传送给应用服务器。但是，为了减轻负载，提高传输效率，在缓存这些需要进行数据重组的数据流时，也可以只缓存一部分，另一部分则直接转发给应用服务器，如果后续确定该访问请求为恶意请求，则无需将缓存的数据流发送给应用服务器，而如

果后续确定该访问请求不是恶意请求，则将缓存的数据流发送给应用服务器，从而使得应用服务器可以接收到关于该访问请求的完整的数据流。具体可参见实施例一，在此不再赘述。

[0080] 由上可知，本实施例采用拦截发往应用服务器的数据流，对该数据流进行基于五元组的流跟踪，以确定属于同一访问请求的数据流，然后对属于该同一访问请求的数据流进行数据重组，以还原该访问请求，并对该访问请求进行检测，以确定该访问请求是否为恶意请求，若为恶意请求，则阻断该访问请求，否则，若不是恶意请求，则向该应用服务器发送该数据流，从而实现防止漏洞攻击的恶意请求的目的。由于在该方案中，采用的是在数据流进入应用服务器之前，由专用的安全性检测装置对该数据流进行安全性检测，因此，并不受制于应用服务器服务软件的特性，相对于现有技术中需要根据不同的特性在应用服务器内设置不同的安全接口/模块而言，大大可以减低开发和运维成本，而且，无需占用应用服务器的资源，有利于提高服务器性能。

[0081] 实施例三、

[0082] 为了更好地实施以上方法，本发明实施例还提供一种安全性检测装置，如图3所示，该安全性检测装置包括拦截单元301、流跟踪单元302、重组单元303、检测单元304、阻断单元305和发送单元306，如下：

[0083] 拦截单元301，用于拦截发往应用服务器的数据流。

[0084] 流跟踪单元302，用于对所述数据流进行基于五元组的流跟踪，以确定属于同一访问请求的数据流；

[0085] 重组单元303，用于对所述属于同一访问请求的数据流进行数据重组，以还原该访问请求。

[0086] 例如，具体可以基于TCP协议对该属于同一访问请求的数据流进行数据重组，以还原所述访问请求。

[0087] 检测单元304，用于对该访问请求进行检测，以确定该访问请求是否为恶意请求；

[0088] 阻断单元305，用于在检测单元确定该访问请求为恶意请求时，阻断该访问请求；

[0089] 发送单元306，用于在检测单元确定该访问请求不是恶意请求时，向该应用服务器发送该数据流。

[0090] 其中，检测的技术可以有多种，例如，可以预先设置病毒库，通过将访问请求与该病毒库进行字段匹配，来确定该访问请求中是否存在有对应用服务器造成威胁的字段，从而判断该访问请求是否为恶意请求，即：

[0091] 检测单元305，具体可以用于根据该访问请求查询病毒库，若该访问请求中存在与所述病毒库匹配的字段，则确定该访问请求为恶意请求；若该访问请求中不存在与所述病毒库匹配的字段，则确定该访问请求不是恶意请求。

[0092] 其中，该病毒库可以根据实际应用的需求进行设置，主要用于收集并记录各种可能会对应用服务器造成威胁的访问请求所携带的字段，在此不再赘述。

[0093] 此外，在对发往应用服务器的数据流进行拦截时，具体也可以采用多种方式，比如，可以向该应用服务器对应的核心层路由设备发送动态牵引指令，使得该核心层路由设备根据该动态牵引指令将发往应用服务器的数据流牵引至该安全性检测装置，即：

[0094] 拦截单元301，具体可以用于向该应用服务器对应的核心层路由设备发送动态牵

引指令，接收该核心层路由设备根据该动态牵引指令所牵引的数据流。

[0095] 可选的，在阻断该访问请求之后，还可以将访问请求的阻断情况通知给应用服务器，即：

[0096] 发送单元306，还可以用于向该服务器发送指示访问请求已被阻断的通知。

[0097] 需说明的是，为了避免恶意请求完全被透传到应用服务器，在对该访问请求进行检测之前，可以对属于同一访问请求的数据流进行缓存，然后再确定该访问请求不是恶意请求时，才将这些数据流传送给应用服务器。但是，为了减轻负载，提高传输效率，在缓存这些需要进行数据重组的数据流时，也可以只缓存一部分，另一部分则直接转发给应用服务器，如果后续确定该访问请求为恶意请求，则无需将缓存的数据流发送给应用服务器，而如果后续确定该访问请求不是恶意请求，则将缓存的数据流发送给应用服务器，从而使得应用服务器可以接收到关于该访问请求的完整的数据流。即该安全性检测装置还可以包括缓存单元，如下：

[0098] 缓存单元，用于缓存属于同一访问请求的数据流中的至少一个数据包，并将该属于同一访问请求的数据流中的其他数据包发送给所述应用服务器。

[0099] 则此时，发送单元306，可以用于在检测单元305确定该访问请求不是恶意请求时，将缓存的数据包发送给所述应用服务器。

[0100] 其中，缓存的数据包的数量和位置可以根据实际应用的需求进行设置，比如，可以缓存某个数据流中最后一个数据包(也称为分片包)、最后两个数据包、前三个数据包、或中间的一个数据包，还可以缓存所有数据包，等等，在此不再赘述。

[0101] 具体实施时，以上各个单元可以作为独立的实体来实现，也可以进行任意组合，作为同一或若干个实体来实现，以上各个单元的具体实施可参见前面的方法实施例，在此不再赘述。

[0102] 由上可知，本实施例的安全性检测装置的拦截单元301拦截发往应用服务器的数据流，由流跟踪单元302对该数据流进行基于五元组的流跟踪，以确定属于同一访问请求的数据流，然后由重组单元303对属于该同一访问请求的数据流进行数据重组，以还原该访问请求，并由检测单元304对该访问请求进行检测，以确定该访问请求是否为恶意请求，若为恶意请求，则由阻断单元305阻断该访问请求，否则，若不是恶意请求，则由发送单元306向该应用服务器发送该数据流，从而实现防止漏洞攻击的恶意请求的目的。由于在该方案中，采用的是在数据流进入应用服务器之前，由专用的安全性检测装置对该数据流进行安全性检测，因此，并不受制于应用服务器服务软件的特性，相对于现有技术中需要根据不同的特性在应用服务器内设置不同的安全接口/模块而言，大大可以减低开发和运维成本，而且，无需占用应用服务器的资源，有利于提高服务器性能。

[0103] 实施例四、

[0104] 相应的，本发明实施例还提供一种通信系统，包括本发明实施例提供的任一种安全性检测装置，例如，具体可以如下：

[0105] 安全性检测装置，用于拦截发往应用服务器的数据流，对该数据流进行基于五元组的流跟踪，以确定属于同一访问请求的数据流；对该属于同一访问请求的数据流进行数据重组，以还原该访问请求；对该访问请求进行检测，以确定该访问请求是否为恶意请求，若是，则阻断该访问请求；若否，则向该应用服务器发送该数据流。

[0106] 其中，检测的技术可以有多种，例如，可以预先设置病毒库，通过将访问请求与该病毒库进行字段匹配，来确定该访问请求中是否存在有对应用服务器造成威胁的字段，从而判断该访问请求是否为恶意请求，即：

[0107] 安全性检测装置，具体可以用于根据该访问请求查询病毒库，若该访问请求中存在与所述病毒库匹配的字段，则确定该访问请求为恶意请求；若该访问请求中不存在与所述病毒库匹配的字段，则确定该访问请求不是恶意请求。

[0108] 其中，该病毒库可以根据实际应用的需求进行设置，主要用于收集并记录各种可能会对应用服务器造成威胁的访问请求所携带的字段，在此不再赘述。

[0109] 此外，在对发往应用服务器的数据流进行拦截时，具体也可以采用多种方式，比如，可以向该应用服务器对应的核心层路由设备发送动态牵引指令，使得该核心层路由设备根据该动态牵引指令将发往应用服务器的数据流牵引至该安全性检测装置，即：

[0110] 安全性检测装置，具体可以用于向该应用服务器对应的核心层路由设备发送动态牵引指令，接收该核心层路由设备根据该动态牵引指令所牵引的数据流。

[0111] 可选的，在阻断该访问请求之后，还可以将访问请求的阻断情况通知给应用服务器，即：

[0112] 安全性检测装置，还可以用于向该服务器发送指示访问请求已被阻断的通知。

[0113] 该安全性检测装置的具体实施可参见前面的实施例，在此不再赘述。

[0114] 由上可知，本实施例的通信系统中的安全性检测装置可以拦截发往应用服务器的数据流，对该数据流进行基于五元组的流跟踪，以确定属于同一访问请求的数据流，然后对属于该同一访问请求的数据流进行数据重组，以还原该访问请求，并对该访问请求进行检测，以确定该访问请求是否为恶意请求，若为恶意请求，则阻断该访问请求，否则，若不是恶意请求，则向该应用服务器发送该数据流，从而实现防止漏洞攻击的恶意请求的目的。由于在该方案中，采用的是在数据流进入应用服务器之前，由专用的安全性检测装置对该数据流进行安全性检测，因此，并不受制于应用服务器服务软件的特性，相对于现有技术中需要根据不同的特性在应用服务器内设置不同的安全接口/模块而言，大大可以减低开发和运维成本，而且，无需占用应用服务器的资源，有利于提高服务器性能。

[0115] 实施例五、

[0116] 本发明实施例还提供一种网络安全防护设备，如图4所示，其示出了本发明实施例所涉及的网络安全防护设备的结构示意图，具体来讲：

[0117] 该网络安全防护设备可以包括一个或者一个以上处理核心的处理器401、一个或一个以上计算机可读存储介质的存储器402、射频(Radio Frequency，RF)电路403、无线通信模块如蓝牙模块和/或无线保真(WiFi，Wireless Fidelity)模块404等(图4中以WIFI模块404为例)、电源405、传感器406、输入单元407、以及显示单元408等部件。本领域技术人员可以理解，图4中示出的网络安全防护设备结构并不构成对网络安全防护设备的限定，可以包括比图示更多或更少的部件，或者组合某些部件，或者不同的部件布置。其中：

[0118] 处理器401是该网络安全防护设备的控制中心，利用各种接口和线路连接整个网络安全防护设备的各个部分，通过运行或执行存储在存储器402内的软件程序和/或模块，以及调用存储在存储器402内的数据，执行网络安全防护设备的各种功能和处理数据，从而对网络安全防护设备进行整体监控。可选的，处理器401可包括一个或多个处理核心；优选

的，处理器401可集成应用处理器和调制解调处理器，其中，应用处理器主要处理操作系统、用户界面和应用程序等，调制解调处理器主要处理无线通信。可以理解的是，上述调制解调处理器也可以不集成到处理器401中。

[0119] 存储器402可用于存储软件程序以及模块，处理器401通过运行存储在存储器402的软件程序以及模块，从而执行各种功能应用以及数据处理。存储器402可主要包括存储程序区和存储数据区，其中，存储程序区可存储操作系统、至少一个功能所需的应用程序(比如声音播放功能、图像播放功能等)等；存储数据区可存储根据网络安全防护设备的使用所创建的数据等。此外，存储器402可以包括高速随机存取存储器，还可以包括非易失性存储器，例如至少一个磁盘存储器件、闪存器件、或其他易失性固态存储器件。相应地，存储器402还可以包括存储器控制器，以提供处理器401对存储器402的访问。

[0120] RF电路403可用于收发信息过程中，信号的接收和发送，特别地，将基站的下行信息接收后，交由一个或者一个以上处理器401处理；另外，将涉及上行的数据发送给基站。通常，RF电路403包括但不限于天线、至少一个放大器、调谐器、一个或多个振荡器、用户身份模块(SIM)卡、收发信机、耦合器、低噪声放大器(LNA，Low Noise Amplifier)、双工器等。此外，RF电路403还可以通过无线通信与网络和其他设备通信。所述无线通信可以使用任一通信标准或协议，包括但不限于全球移动通讯系统(GSM，Global System of Mobile communication)、通用分组无线服务(GPRS，General Packet Radio Service)、码分多址(CDMA，Code Division Multiple Access)、宽带码分多址(WCDMA，Wideband Code Division Multiple Access)、长期演进(LTE，Long Term Evolution)、电子邮件、短消息服务(SMS，Short Messaging Service)等。

[0121] WiFi属于短距离无线传输技术，网络安全防护设备通过WiFi模块404收发电子邮件和访问流式媒体等，它可以提供无线的宽带互联网访问。虽然图4示出了WiFi模块404，但是可以理解的是，其并不属于网络安全防护设备的必须构成，完全可以根据需要在不改变发明的本质的范围内而省略。

[0122] 网络安全防护设备还包括给各个部件供电的电源405(比如电池)，优选的，电源可以通过电源管理系统与处理器401逻辑相连，从而通过电源管理系统实现管理充电、放电、以及功耗管理等功能。电源405还可以包括一个或一个以上的直流或交流电源、再充电系统、电源故障检测电路、电源转换器或者逆变器、电源状态指示器等任意组件。

[0123] 该网络安全防护设备还可包括至少一种传感器406，比如光传感器、运动传感器以及其他传感器。该网络安全防护设备还可配置的陀螺仪、气压计、湿度计、温度计、红外线传感器等其他传感器，在此不再赘述。

[0124] 该网络安全防护设备还可包括输入单元407，该输入单元407可用于接收输入的数字或字符信息，以及产生与用户设置以及功能控制有关的键盘、鼠标、操作杆、光学或者轨迹球信号输入。具体地，在一个具体的实施例中，输入单元407可包括触敏表面以及其他输入设备。触敏表面，也称为触摸显示屏或者触控板，可收集用户在其上或附近的触摸操作(比如用户使用手指、触笔等任何适合的物体或附件在触敏表面上或在触敏表面附近的操作)，并根据预先设定的程式驱动相应的连接装置。可选的，触敏表面可包括触摸检测装置和触摸控制器两个部分。其中，触摸检测装置检测用户的触摸方位，并检测触摸操作带来的信号，将信号传送给触摸控制器；触摸控制器从触摸检测装置上接收触摸信息，并将它转换

成触点坐标，再送给处理器401，并能接收处理器401发来的命令并加以执行。此外，可以采用电阻式、电容式、红外线以及表面声波等多种类型实现触敏表面。除了触敏表面，输入单元407还可以包括其他输入设备。具体地，其他输入设备可以包括但不限于物理键盘、功能键(比如音量控制按键、开关按键等)、轨迹球、鼠标、操作杆等中的一种或多种。

[0125] 该网络安全防护设备还可包括显示单元408，该显示单元408可用于显示由用户输入的信息或提供给用户的信息以及网络安全防护设备的各种图形用户接口，这些图形用户接口可以由图形、文本、图标、视频和其任意组合来构成。显示单元408可包括显示面板，可选的，可以采用液晶显示器(LCD，Liquid Crystal Display)、有机发光二极管(OLED，Organic Light-Emitting Diode)等形式来配置显示面板。进一步的，触敏表面可覆盖显示面板，当触敏表面检测到在其上或附近的触摸操作后，传送给处理器401以确定触摸事件的类型，随后处理器401根据触摸事件的类型在显示面板上提供相应的视觉输出。虽然在图4中，触敏表面与显示面板是作为两个独立的部件来实现输入和输入功能，但是在某些实施例中，可以将触敏表面与显示面板集成而实现输入和输出功能。

[0126] 尽管未示出，网络安全防护设备还可以包括摄像头、蓝牙模块等，在此不再赘述。具体在本实施例中，网络安全防护设备中的处理器401会按照如下的指令，将一个或一个以上的应用程序的进程对应的可执行文件加载到存储器402中，并由处理器401来运行存储在存储器402中的应用程序，从而实现各种功能，如下：

[0127] 拦截发往应用服务器的数据流，对该数据流进行基于五元组的流跟踪，以确定属于同一访问请求的数据流；对该属于同一访问请求的数据流进行数据重组，以还原该访问请求；对该访问请求进行检测，以确定该访问请求是否为恶意请求，若是，则阻断该访问请求；若否，则向该应用服务器发送该数据流。

[0128] 其中，检测的技术可以有多种，例如，可以预先设置病毒库，通过将访问请求与该病毒库进行字段匹配，来确定该访问请求中是否存在有对应用服务器造成威胁的字段，从而判断该访问请求是否为恶意请求，即操作“对该访问请求进行检测，以确定该访问请求是否为恶意请求”具体可以如下：

[0129] 根据该访问请求查询病毒库，若该访问请求中存在与所述病毒库匹配的字段，则确定该访问请求为恶意请求；若该访问请求中不存在与所述病毒库匹配的字段，则确定该访问请求不是恶意请求。

[0130] 其中，该病毒库可以根据实际应用的需求进行设置，主要用于收集并记录各种可能会对应用服务器造成威胁的访问请求所携带的字段，在此不再赘述。

[0131] 此外，在对发往应用服务器的数据流进行拦截时，具体也可以采用多种方式，比如，可以向该应用服务器对应的核心层路由设备发送动态牵引指令，使得该核心层路由设备根据该动态牵引指令将发往应用服务器的数据流牵引至该网络安全防护设备，即操作“拦截发往应用服务器的数据流”具体可以如下：

[0132] 向该应用服务器对应的核心层路由设备发送动态牵引指令，接收该核心层路由设备根据该动态牵引指令所牵引的数据流。

[0133] 可选的，在阻断该访问请求之后，还可以将访问请求的阻断情况通知给应用服务器，即在阻断该访问请求之后，还可以执行如下指令：

[0134] 向该服务器发送指示访问请求已被阻断的通知。

[0135] 以上各个操作具体实施可参见前面的实施例，在此不再赘述。

[0136] 由上可知，本实施例的网络安全防护设备可以拦截发往应用服务器的数据流，对该数据流进行基于五元组的流跟踪，以确定属于同一访问请求的数据流，然后对属于该同一访问请求的数据流进行数据重组，以还原该访问请求，并对该访问请求进行检测，以确定该访问请求是否为恶意请求，若为恶意请求，则阻断该访问请求，否则，若不是恶意请求，则向该应用服务器发送该数据流，从而实现防止漏洞攻击的恶意请求的目的。由于在该方案中，采用的是在数据流进入应用服务器之前，由专用的安全性检测装置对该数据流进行安全性检测，因此，并不受制于应用服务器服务软件的特性，相对于现有技术中需要根据不同的特性在应用服务器内设置不同的安全接口/模块而言，大大可以减低开发和运维成本，而且，无需占用应用服务器的资源，有利于提高服务器性能。

[0137] 本领域普通技术人员可以理解上述实施例的各种方法中的全部或部分步骤是可以通过程序来指令相关的硬件来完成，该程序可以存储于一计算机可读存储介质中，存储介质可以包括：只读存储器(ROM，Read Only Memory)、随机存取记忆体(RAM，Random Access Memory)、磁盘或光盘等。

[0138] 以上对本发明实施例所提供的一种安全性检测方法、装置和系统进行了详细介绍，本文中应用了具体个例对本发明的原理及实施方式进行了阐述，以上实施例的说明只是用于帮助理解本发明的方法及其核心思想；同时，对于本领域的技术人员，依据本发明的思想，在具体实施方式及应用范围上均会有改变之处，综上所述，本说明书内容不应理解为对本发明的限制。

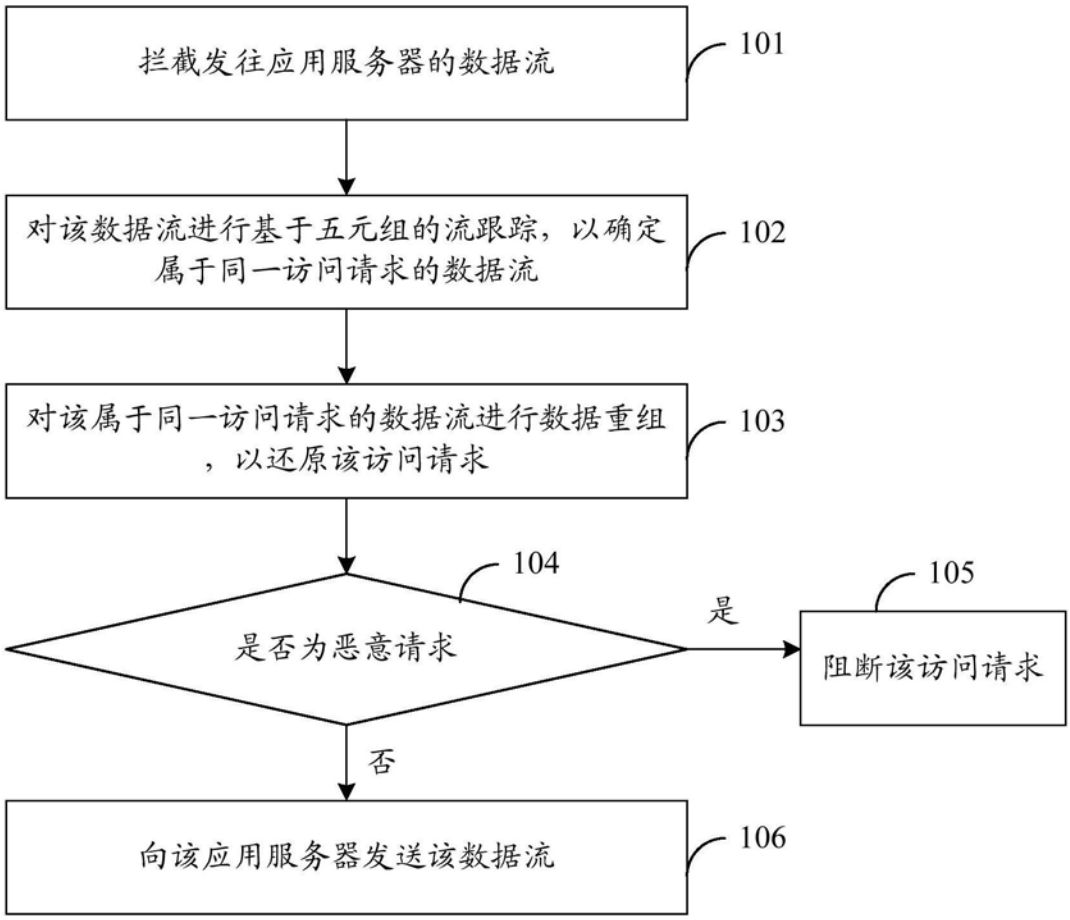

拦截发往应用服务器的数据流
101
对该数据流进行基于五元组的流跟踪，以确定属于同一访问请求的数据流
102
对该属于同一访问请求的数据流进行数据重组，以还原该访问请求
103
104
是否为恶意请求
是
105
阻断该访问请求
否
向该应用服务器发送该数据流
106

图1

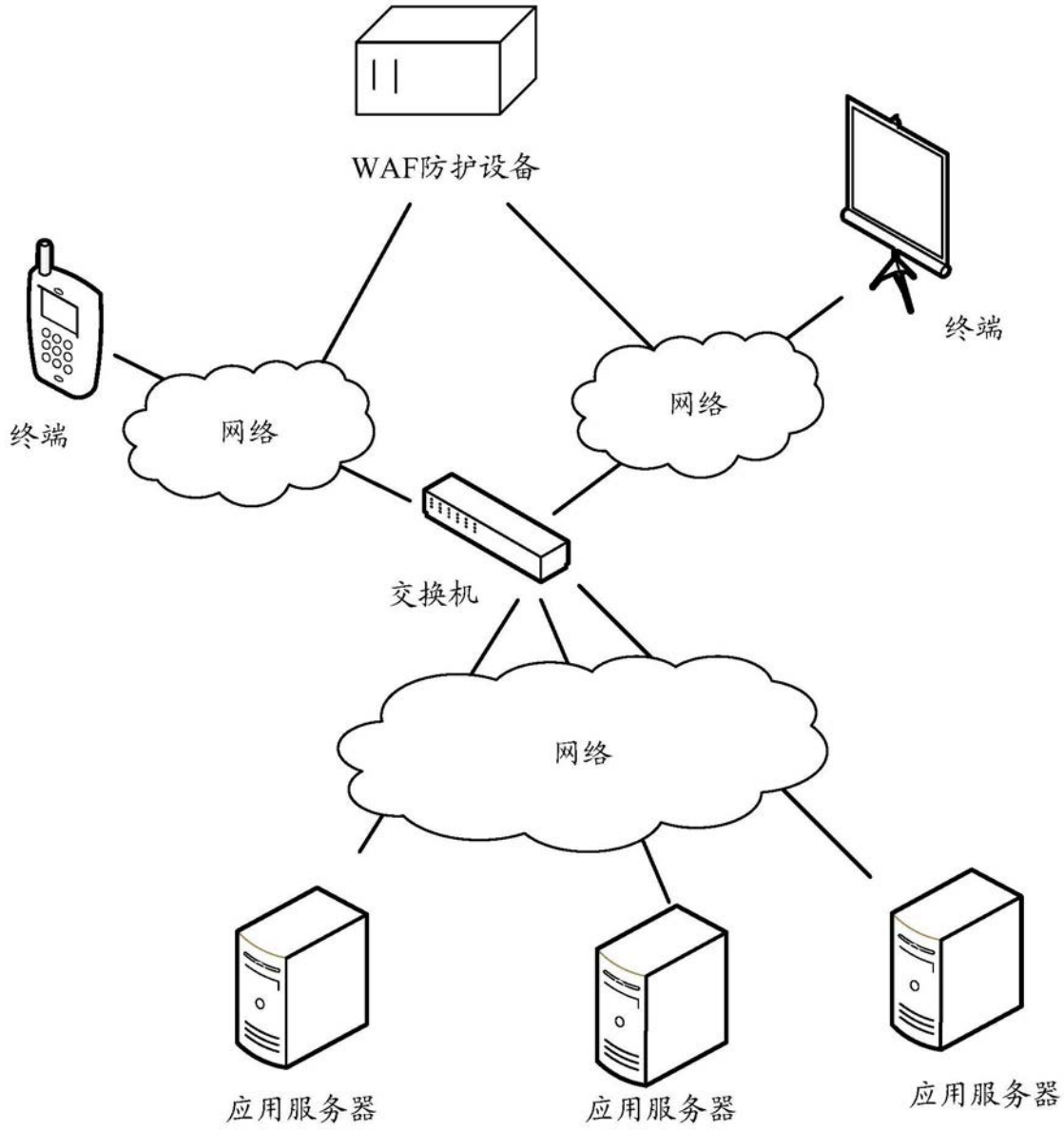


图2a

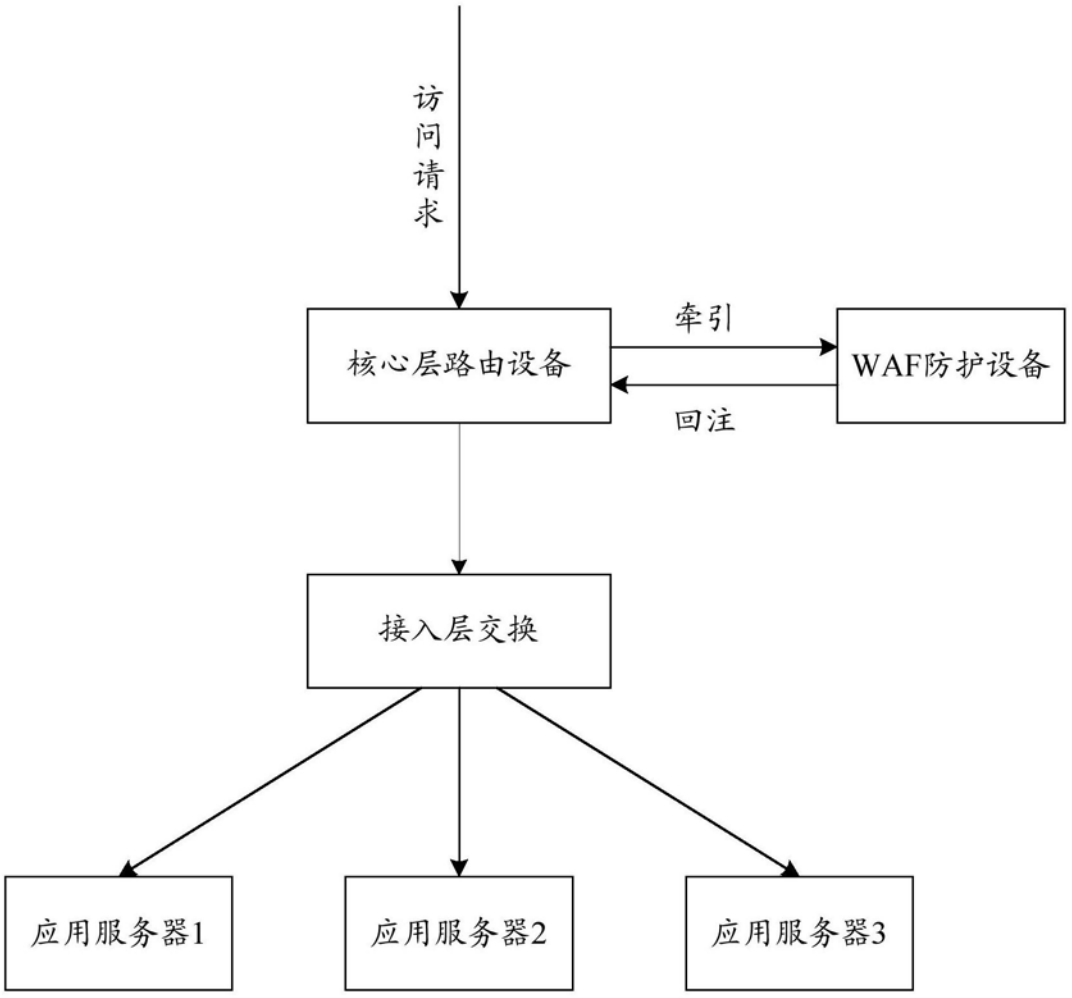


图2b

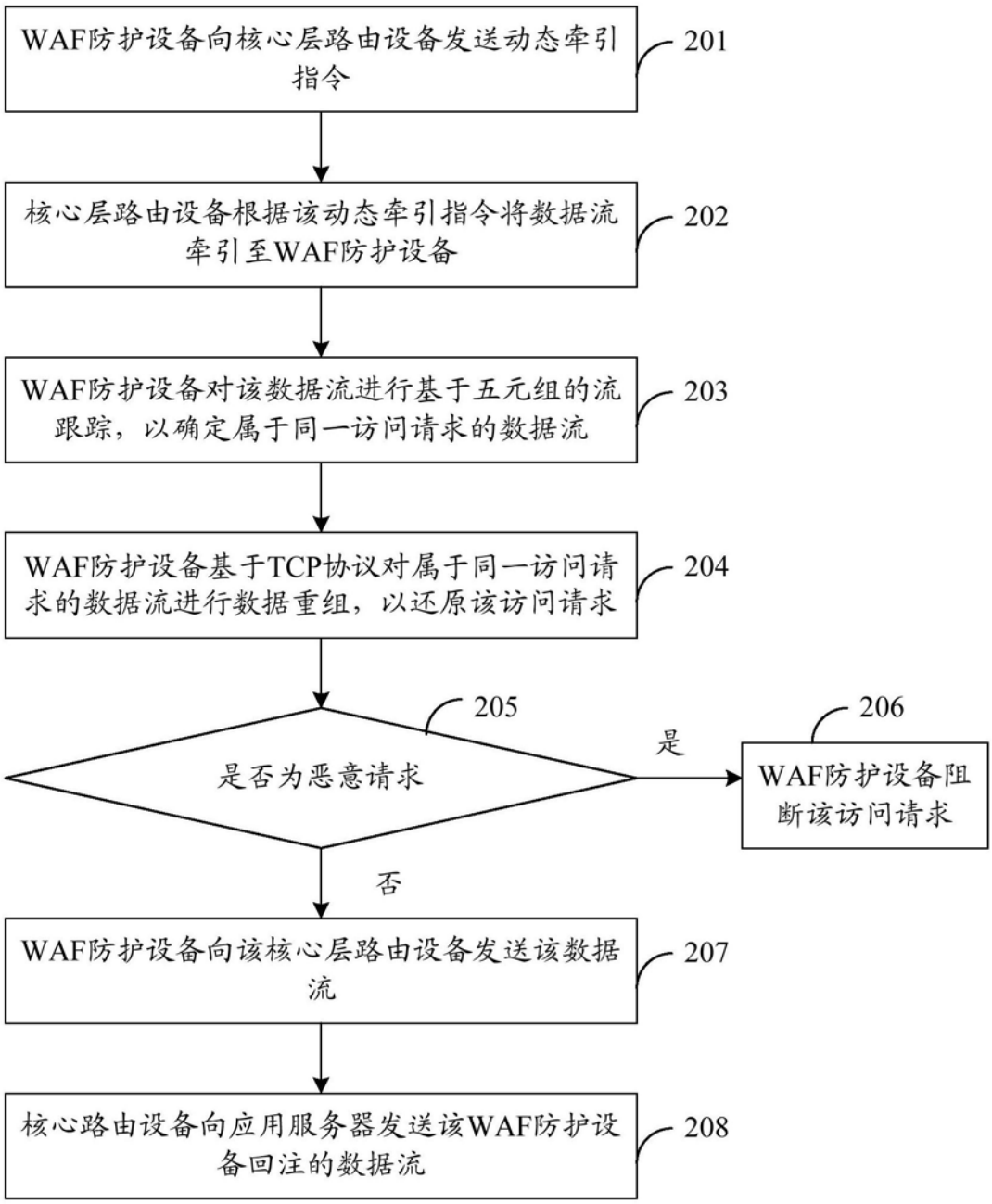

WAF防护设备向核心层路由设备发送动态牵引指令
201
核心层路由设备根据该动态牵引指令将数据流牵引至WAF防护设备
202
WAF防护设备对该数据流进行基于五元组的流跟踪，以确定属于同一访问请求的数据流
203
WAF防护设备基于TCP协议对属于同一访问请求的数据流进行数据重组，以还原该访问请求
204
205
是否为恶意请求
是
206
WAF防护设备阻断该访问请求
否
WAF防护设备向该核心层路由设备发送该数据流
207
核心路由设备向应用服务器发送该WAF防护设备回注的数据流
208

图2c

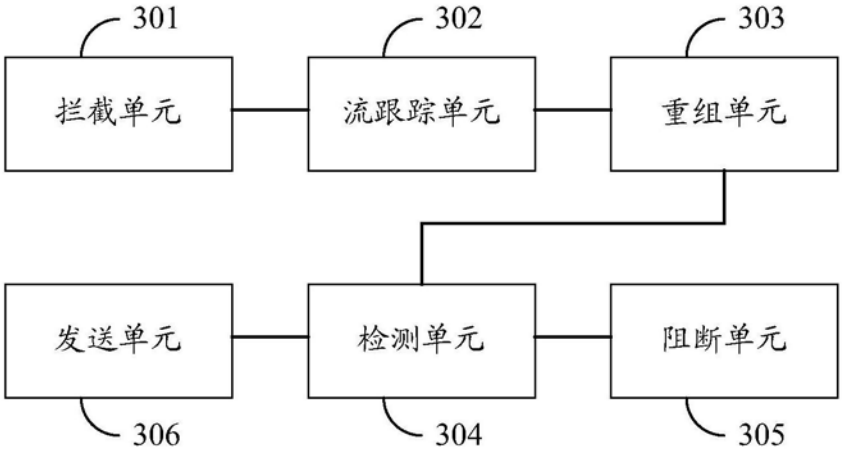

301
302
303
拦截单元
流跟踪单元
重组单元
发送单元
检测单元
阻断单元
306
304
305

图3

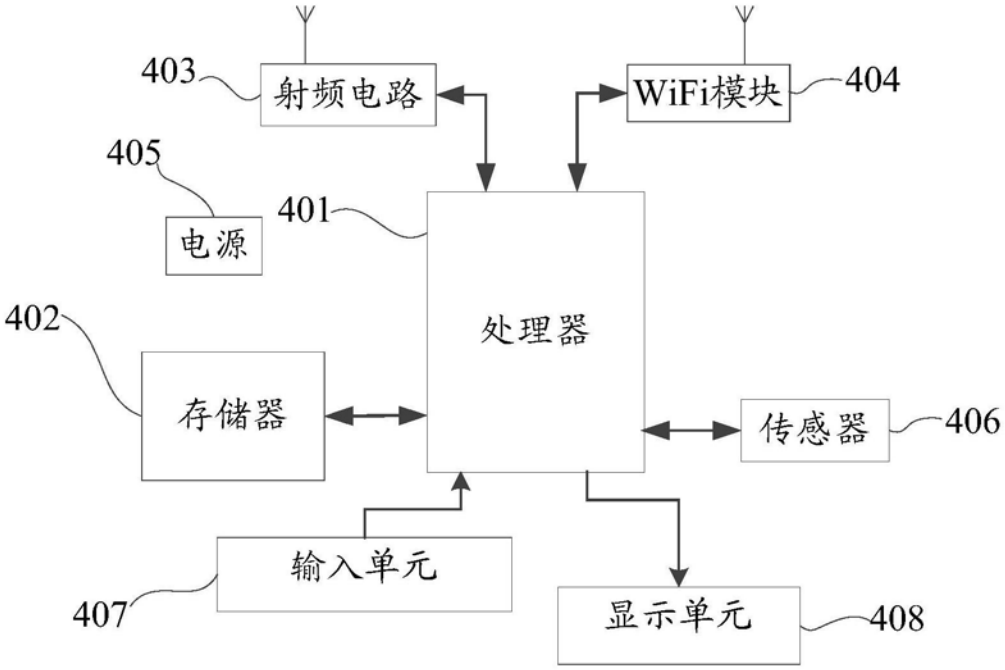

403
射频电路
WiFi模块
404
405
电源
401
处理器
402
存储器
传感器
406
输入单元
407
显示单元
408

图4