(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 107241294 B
(45)授权公告日 2020.09.15

(21)申请号 201610183552.X

(22)申请日 2016.03.28

(65)同一申请的已公布的文献号
申请公布号 CN 107241294 A

(43)申请公布日 2017.10.10

(73)专利权人 阿里巴巴集团控股有限公司
地址 英属开曼群岛大开曼资本大厦一座四层847号邮箱

(72)发明人 胡闽 贾炯

(74)专利代理机构 北京博思佳知识产权代理有限公司 11415
代理人 陈蕾

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 12/46(2006.01)

(56)对比文件
CN 104158803 A,2014.11.19
CN 101924764 A,2010.12.22
CN 104967588 A,2015.10.07
US 2016080411 A1,2016.03.17

审查员 许婵

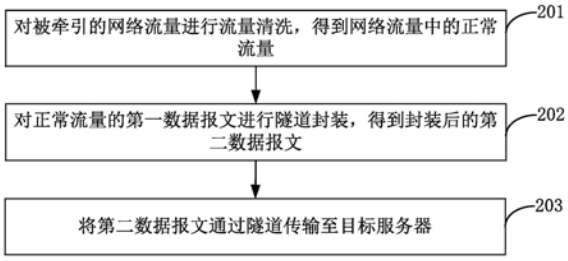
权利要求书3页 说明书8页 附图8页

(54)发明名称

网络流量的处理方法及装置、清洗设备、网络设备

(57)摘要

本申请提供一种网络流量的处理方法及装置、清洗设备、网络设备，该方法包括：对被牵引的网络流量进行流量清洗，得到所述网络流量中的正常流量；对所述正常流量的第一数据报文进行隧道封装，得到封装后的第二数据报文；将所述第二数据报文通过隧道传输至目标服务器。在本申请的技术方案可以避免正常流量被目的端的清洗设备重复清洗，继而避免对目的端的清洗设备的计算资源造成浪费，并且还能避免目的端的清洗设备对正常流量的误清洗。



CN 107241294 B

1.一种网络流量的处理方法,应用在网络流量的源端,其特征在于,所述方法包括:

对被牵引的网络流量进行流量清洗,得到所述网络流量中的正常流量;

对所述正常流量的第一数据报文进行隧道封装,得到封装后的第二数据报文;

将所述第二数据报文通过隧道传输至目标服务器。

2.根据权利要求1所述的方法,其特征在于,所述对所述正常流量的第一数据报文进行隧道封装,包括:

确定隧道协议的类型;

根据与所述隧道协议的类型相对应的报文格式对所述正常流量的第一数据报文进行封装。

3.根据权利要求2所述的方法,其特征在于,所述根据与所述隧道协议的类型相对应的报文格式对所述正常流量的第一数据报文进行封装,包括:

确定所述隧道对应的终结设备的IP地址;

根据与所述隧道协议的类型相对应的报文格式将所述正常流量的第一数据报文封装在内层IP头和负荷对应的字段,将所述终结设备的IP地址封装在外层IP头对应的字段。

4.一种网络流量的处理方法,应用在网络流量的目的端,其特征在于,所述方法包括:

接收网络流量的数据报文;

当所述网络流量的数据报文为封装后的第二数据报文时,对所述第二数据报文进行解封装,得到所述网络流量的第一数据报文以及所述第一数据报文的目的IP地址;其中,所述封装后的第二数据报文是由网络流量的源端对正常流量的第一数据报文进行隧道封装得到的,所述正常流量是由网络流量的源端对被牵引的网络流量进行流量清洗得到的;

根据所述第一数据报文的目的IP地址将所述第一数据报文转发至目标服务器。

5.根据权利要求4所述的方法,其特征在于,所述对所述第二数据报文进行解封装,包括:

确定所述第二数据报文在进行隧道封装时采用的隧道协议的类型;

根据与所述隧道协议的类型相对应的报文格式对所述第二数据报文进行解封装。

6.根据权利要求4所述的方法,其特征在于,所述方法还包括:

检测网络流量的第二数据报文是否为封装后的数据报文;

当所述第二数据报文为封装后的数据报文时,执行所述对所述第二数据报文进行解封装的步骤。

7.一种网络流量的处理装置,应用在网络流量的源端,其特征在于,所述装置包括:

流量清洗模块,用于对被牵引的网络流量进行流量清洗,得到所述网络流量中的正常流量;

封装模块,用于对所述流量清洗模块清洗得到的所述正常流量的第一数据报文进行隧道封装,得到封装后的第二数据报文;

发送模块,用于将所述封装模块封装后的所述第二数据报文通过隧道传输至目标服务器。

8.根据权利要求7所述的装置,其特征在于,所述封装模块包括:

第一确定单元,用于确定隧道协议的类型;

封装单元,用于根据与所述第一确定单元确定的所述隧道协议的类型相对应的报文格

式对所述正常流量的第一数据报文进行封装。

9.根据权利要求8所述的装置,其特征在于,所述封装单元包括:

确定子单元,用于确定所述隧道对应的终结设备的IP地址;

封装子单元,用于根据与所述隧道协议的类型相对应的报文格式将所述正常流量的第一数据报文封装在内层IP头和负荷对应的字段,将所述确定子单元确定的所述终结设备的IP地址封装在外层IP头对应的字段。

10.一种网络流量的处理装置,应用在网络流量的目的端,其特征在于,所述装置包括:

接收模块,用于接收网络流量的数据报文;

解封装模块,用于当所述接收模块接收到的所述网络流量数据报文为封装后的第二数据报文时,对所述第二数据报文进行解封装,得到所述网络流量的第一数据报文以及所述第一数据报文的目的IP地址;其中,所述封装后的第二数据报文是由网络流量的源端对正常流量的第一数据报文进行隧道封装得到的,所述正常流量是由网络流量的源端对被牵引的网络流量进行流量清洗得到的;

转发模块,用于根据所述解封装模块解封装得到的所述第一数据报文的目的IP地址将所述第一数据报文转发至目标服务器。

11.根据权利要求10所述的装置,其特征在于,所述解封装模块包括:

第二确定单元,用于确定所述第二数据报文在进行隧道封装时采用的隧道协议的类型;

解封装单元,用于根据与所述第二确定单元确定的所述隧道协议的类型相对应的报文格式对所述第二数据报文进行解封装。

12.根据权利要求10所述的装置,其特征在于,所述装置还包括:

检测模块,用于检测所述接收模块接收到的所述网络流量的第二数据报文是否为封装后的数据报文;

当所述检测模块检测到所述第二数据报文为封装后的数据报文时,所述解封装模块执行所述对所述第二数据报文进行解封装的步骤。

13.一种清洗设备,其特征在于,所述清洗设备包括:

第一处理器;用于存储所述第一处理器可执行程序的第一存储器;第一网络接口;

其中,所述第一处理器,用于对被牵引的网络流量进行流量清洗,得到所述网络流量中的正常流量;对所述正常流量的第一数据报文进行隧道封装,得到封装后的第二数据报文;

所述第一网络接口,用于将所述第一处理器得到的所述第二数据报文通过隧道传输至目标服务器。

14.一种网络设备,其特征在于,所述网络设备包括:

第二处理器;用于存储所述第二处理器可执行程序的第二存储器;第二网络接口;

所述第二网络接口,用于接收网络流量的数据报文;

所述第二处理器,用于当所述第二网络接口接收到的所述网络流量的数据报文为封装后的第二数据报文时,对所述第二数据报文进行解封装,得到所述网络流量的第一数据报文以及所述第一数据报文的目的IP地址;其中,所述封装后的第二数据报文是由网络流量的源端对正常流量的第一数据报文进行隧道封装得到的,所述正常流量是由网络流量的源端对被牵引的网络流量进行流量清洗得到的;根据所述第一数据报文的目的IP地址将所述

第一数据报文转发至目标服务器。

网络流量的处理方法及装置、清洗设备、网络设备

技术领域

[0001] 本申请涉及网络技术领域，尤其涉及一种网络流量的处理方法及装置、清洗设备、网络设备。

背景技术

[0002] 随着网络的发展，攻击流量越来越大，通过与运营商合作，在用户的出口处进行安全防护，将攻击分散的消灭在源端，从而减少攻击时服务器机房的带宽压力。现有技术中与运营商进行合作部署的近源端分布式拒绝服务(Distributed Denial of Service，简称为DDoS)防护系统，有些地区因为各种原因无法部署，这时候一般采用两级DDoS防护策略，即：一级为部分的和运营商合作的近源端防护系统，一级为云服务提供商(或IDC机房)部署在机房入口的近目的端防护系统。当攻击目标被攻击时，近源端防护系统和近目的端防护系统联动工作，同时对攻击流量进行流量清洗，丢弃攻击流量，放行正常流量。

[0003] 但是上述防护方法存在如下问题：目的端防护系统流量清洗边界网关协议(Border Gateway Protocol，简称为BGP)由于在牵引流量时无法区分攻击流量和正常流量，会将全部到达攻击目标的访问流量牵引到清洗设备上进行流量清洗，会使一些通过近源端防护系统清洗后的正常流量到达云服务提供商的IDC机房时仍然会被近目的端防护系统牵引到清洗设备上进行清洗，从而浪费目的端防护系统的清洗设备的计算资源以及正常流量的误清洗。

发明内容

[0004] 有鉴于此，本申请提供一种新的技术方案，可以避免正常流量到达云服务提供商的IDC机房时不会被近目的端防护系统牵引到清洗设备上进行清洗，降低目的端防护系统的清洗设备的计算资源，避免正常流量的误清洗。

[0005] 为实现上述目的，本申请提供技术方案如下：

[0006] 根据本申请的第一方面，提出了一种网络流量的处理方法，应用在网络流量的源端，包括：

[0007] 对被牵引的网络流量进行流量清洗，得到所述网络流量中的正常流量；

[0008] 对所述正常流量的第一数据报文进行隧道封装，得到封装后的第二数据报文；

[0009] 将所述第二数据报文通过隧道传输至目标服务器。

[0010] 根据本申请的第二方面，提出了一种网络流量的处理方法，应用在网络流量的目的端，包括：

[0011] 接收网络流量的数据报文；

[0012] 当所述网络流量的数据报文为封装后的第二数据报文时，对所述第二数据报文进行解封装，得到所述网络流量的第一数据报文以及所述第一数据报文的目的IP地址；

[0013] 根据所述第一数据报文的目的IP地址将所述第一数据报文转发至目标服务器。

[0014] 根据本申请的第三方面，提出了一种网络流量的处理装置，应用在网络流量的源

端，包括：

[0015] 流量清洗模块，用于对被牵引的网络流量进行流量清洗，得到所述网络流量中的正常流量；

[0016] 封装模块，用于对所述流量清洗模块清洗得到的所述正常流量的第一数据报文进行隧道封装，得到封装后的第二数据报文；

[0017] 发送模块，用于将所述封装模块封装后的所述第二数据报文通过隧道传输至目标服务器。

[0018] 根据本申请的第四方面，提出了一种网络流量的处理装置，应用在网络流量的目的端，包括：

[0019] 接收模块，用于接收网络流量的数据报文；

[0020] 解封装模块，用于当所述接收模块接收到的所述网络流量数据报文为封装后的第二数据报文时，对所述第二数据报文进行解封装，得到所述网络流量的第一数据报文以及所述第一数据报文的目的IP地址；

[0021] 转发模块，用于根据所述解封装模块解封装得到的所述第一数据报文的目的IP地址将所述第一数据报文转发至目标服务器。

[0022] 根据本申请的第五方面，提出了一种流量清洗设备，所述清洗设备包括：

[0023] 第一处理器；用于存储所述第一处理器可执行指令的第一存储器；第一网络接口；

[0024] 其中，所述第一处理器，用于对被牵引的网络流量进行流量清洗，得到所述网络流量中的正常流量；对所述正常流量的第一数据报文进行隧道封装，得到封装后的第二数据报文；

[0025] 所述第一网络接口，用于将所述第一处理器得到的所述第二数据报文通过隧道传输至目标服务器。

[0026] 根据本申请的第六方面，提出了一种网络设备，所述网络设备包括：

[0027] 第二处理器；用于存储所述第二处理器可执行指令的第二存储器；第二网络接口；

[0028] 所述第二网络接口，用于接收网络流量的数据报文；

[0029] 所述第二处理器，用于当所述第二网络接口接收到的所述网络流量的数据报文为封装后的第二数据报文时，对所述第二数据报文进行解封装，得到所述网络流量的第一数据报文以及所述第一数据报文的目的IP地址；根据所述第一数据报文的目的IP地址将所述第一数据报文转发至目标服务器。

[0030] 由以上技术方案可见，本申请通过对正常流量的第一数据报文进行隧道封装，得到封装后的第二数据报文，将第二数据报文通过隧道传输至目标服务器，可以避免正常流量被目的端的清洗设备重复清洗，继而避免对目的端的清洗设备的计算资源造成浪费，并且还能避免目的端的清洗设备对正常流量的误清洗。

附图说明

[0031] 图1A示出了本发明的示例性实施例所适用的网络架构图之一；

[0032] 图1B示出了本发明的示例性实施例所适用的网络架构图之二；

[0033] 图2A示出了根据本发明的示例性实施例一的网络流量的处理方法的流程示意图；

[0034] 图2B示出了根据本发明的示例性实施例一的GRE隧道封装的报文格式的示意图；

[0035] 图3示出了根据本发明的示例性实施例二的网络流量的处理方法的流程示意图；

[0036] 图4示出了根据本发明的示例性实施例三的网络流量的处理方法的流程示意图；

[0037] 图5示出了根据本发明的示例性实施例四的网络流量的处理方法的流程示意图；

[0038] 图6示出了根据本发明的示例性实施例五的网络流量的处理方法的流程示意图；

[0039] 图7示出了根据本发明的一示例性实施例的清洗设备的结构示意图；

[0040] 图8示出了根据本发明的一示例性实施例的网络设备的结构示意图；

[0041] 图9示出了根据本发明的示例性实施例一的网络流量的处理装置的结构示意图；

[0042] 图10示出了根据本发明的示例性实施例二的网络流量的处理装置的结构示意图；

[0043] 图11示出了根据本发明的示例性实施例三的网络流量的处理装置的结构示意图；

[0044] 图12示出了根据本发明的示例性实施例四的网络流量的处理装置的结构示意图。

具体实施方式

[0045] 这里将详细地对示例性实施例进行说明，其示例表示在附图中。下面的描述涉及附图时，除非另有表示，不同附图中的相同数字表示相同或相似的要素。以下示例性实施例中所描述的实施方式并不代表与本申请相一致的所有实施方式。相反，它们仅是与如所附权利要求书中所详述的、本申请的一些方面相一致的装置和方法的例子。

[0046] 在本申请使用的术语是仅仅出于描述特定实施例的目的，而非旨在限制本申请。在本申请和所附权利要求书中所使用的单数形式的“一种”、“所述”和“该”也旨在包括多数形式，除非上下文清楚地表示其他含义。还应当理解，本文中使用的术语“和/或”是指并包含一个或多个相关联的列出项目的任何或所有可能组合。

[0047] 应当理解，尽管在本申请可能采用术语第一、第二、第三等来描述各种信息，但这些信息不应限于这些术语。这些术语仅用来将同一类型的信息彼此区分开。例如，在不脱离本申请范围的情况下，第一信息也可以被称为第二信息，类似地，第二信息也可以被称为第一信息。取决于语境，如在此所使用的词语“如果”可以被解释成为“在……时”或“当……时”或“响应于确定”。

[0048] 图1A示出了本发明的示例性实施例所适用的网络架构图之一；以M地区部署有源端防护系统以及N地区未部署源端防护系统为例进行示例性说明，如图1A所示，M地区源端防护系统在发现攻击流量后，第一路由器111将攻击流量牵引到源端防护系统的第一清洗设备121中进行流量清洗，通过下述图2A或图3所示实施例将攻击流量中的第一正常流量进行隧道封装后，得到封装后的第二数据报文，将第二数据报文回注到第一路由器111上，其中，隧道封装后的第二正常流量被封装起来，封装后的第二正常流量的外层的目的IP地址修改为隧道的终结网关13的IP地址，该封装后的第一正常流量被转发至目的机房的第二路由器112后，由于封装后的第二数据报文的目的IP地址为隧道终点的网关设备13的IP地址，因此封装后的第二数据报文不会被目的防护系统牵引到第二清洗设备122上，而是通过第二路由器112转发到隧道终点的网关设备13，网关设备13对封装后的第二数据报文通过下述图4-图6任一所示实施例的方法流程进行解封装，得到第一数据报文，将第一数据报文转发到目标服务器14。N地区的攻击流量直接转发至目的机房的第二路由器112后，目的端防护系统检测到攻击后将攻击流量牵引到第二清洗设备122上进行流量清洗，并将清洗后的第二正常流量回注给第二路由器112，第二路由器112将第二正常流量转发给目标服务器

14。

[0049] 图1B示出了本发明的示例性实施例所适用的网络架构图之二;以M地区部署有源端防护系统以及N地区未部署源端防护系统为例进行示例性说明,如图1B所示,M地区对攻击流量进行清洗以及正常流量封装的方式参见图1A的相关描述,在此不再详述,当封装后的第二数据报文通过目的端防护系统牵引到第二清洗设备122后,第二清洗设备122检测到牵引流量为封装后的第二数据报文后,第二清洗设备122对封装后的第二数据报文通过下述图4-图6任一所示实施例的方法流程进行解封装,得到原始的第一数据报文,将解封装后的第一数据报文转发到目标服务器14。N地区的攻击流量的处理方式参见上述图1A的相关描述,在此不再详述。

[0050] 为对本申请进行进一步说明,提供下列实施例:

[0051] 图2A示出了根据本发明的示例性实施例一的网络流量的处理方法的流程示意图,图2B示出了根据本发明的示例性实施例一的GRE隧道封装的报文格式的示意图;本实施例可以在上述图1A或图1B所示的第一清洗设备121上实现,如图2A所示,包括如下步骤:

[0052] 步骤201,对被牵引的网络流量进行流量清洗,得到网络流量中的正常流量。

[0053] 步骤202,对正常流量的第一数据报文进行隧道封装,得到封装后的第二数据报文。

[0054] 步骤203,将第二数据报文通过隧道传输至目标服务器。

[0055] 上述步骤201中对网络流量进行流量清洗的方式可以参见现有技术中的相关描述,在此不再详述。上述步骤203中通过隧道传输至目标服务器的方式可以参见现有技术中的相关描述,在此不再详述。

[0056] 上述步骤202中,隧道封装的方式可以为GRE隧道封装,还也可以为VXLAN隧道封装等;以GRE封装为例进行示例性说明,如图2B所示,上述对正常流量的第一数据报文进行GRE隧道封装的处理的过程例如为:按照GRE的报文格式将第一数据报文内层IP头(inner IP Header)设置第一数据报文的目标服务器的IP地址,负荷(payload)为第一数据报文,外层IP头(outer IP header)和GRE头(GRE header)为GRE隧道封装添加的报文,其中,外层IP头中的目的IP地址(dst ip)为GRE隧道的终结网关的IP地址或者目标服务器的IP地址。VXLAN隧道封装的方式可以参见上述GRE隧道封装的描述,在此不再详述。

[0057] 由上述描述可知,本发明实施例通过对正常流量的第一数据报文进行隧道封装,得到封装后的第二数据报文,将第二数据报文通过隧道传输至目标服务器,可以避免正常流量被目的端的清洗设备重复清洗,继而避免对目的端的清洗设备的计算资源造成浪费,并且还能避免目的端的清洗设备对正常流量的误清洗。

[0058] 图3示出了根据本发明的示例性实施例二的网络流量的处理方法的流程示意图;本实施例结合图1A进行示例性说明,如图3所示,包括如下步骤:

[0059] 步骤301,对被牵引的网络流量进行流量清洗,得到网络流量中的正常流量。

[0060] 步骤302,确定隧道协议的类型。

[0061] 步骤303,根据与隧道协议的类型相对应的报文格式对正常流量的第一数据报文进行封装,得到封装后的第二数据报文。

[0062] 步骤304,将第二数据报文通过隧道传输至目标服务器。

[0063] 上述步骤301中对网络流量进行流量清洗的方式可以参见现有技术中的相关描

述，在此不再详述。上述步骤304中通过隧道传输至目标服务器的方式可以参见现有技术中的相关描述，在此不再详述。

[0064] 上述步骤302中，隧道协议的类型可以为GRE协议，还也可以为VXLAN协议。在部署源端和目的端的DDoS防护系统时，源端和目的端的DDoS防护系统可以约定双方所采用的隧道协议的类型。

[0065] 上述步骤303中，在一实施例中，可以确定隧道对应的终结设备的IP地址，根据与隧道协议的类型相对应的报文格式将正常流量的第一数据报文封装在内层IP头和负荷对应的字段，将终结设备的IP地址封装在外层IP头对应的字段，例如，通过GRE协议的GRE隧道封装可以参见上述图2A的相关描述，在此不再详述。在一实施例中，终结设备可以为目标服务器，在另一实施例中，终结设备也可以为隧道的网关设备，可以视第二数据报文的外层的目的IP地址而定，当第二数据报文的外层的目的IP地址为目标服务器时，则终结设备为目标是服务器，当第二数据报文的外层的目的IP地址为隧道的网关设备时，终结设备为目标是服务器。

[0066] 本实施例在具有上述实施例的有益技术效果的基础上，根据与隧道协议的类型相对应的报文格式对正常流量的第一数据报文进行封装，提高了源端的清洗设备在封装第一数据报文时的灵活性。

[0067] 图4示出了根据本发明的示例性实施例三的网络流量的处理方法的流程示意图；应用在网络流量的目的端，如图4所示，包括如下步骤：

[0068] 步骤401，接收网络流量的数据报文。

[0069] 步骤402，当网络流量的数据报文为封装后的第二数据报文时，对第二数据报文进行解封装，得到网络流量的第一数据报文以及第一数据报文的目的IP地址。

[0070] 步骤403，根据第一数据报文的目的IP地址将第一数据报文转发至目标服务器。

[0071] 上述步骤401以及步骤403的描述可以参见现有技术中的相关描述，在此不再详述。

[0072] 上述步骤402中，以第二数据报文通过GRE协议封装得到为例进行示例性说明，与上述图2A所示实施例中关于封装相反过程，当第二数据报文到达图1A所示的网关设备13或者清洗设备122后，网关设备13或者清洗设备122可以对第二数据报文进行解封装，解封装的动作为：去除图2B所示的报文格式中的外层IP头和GRE头，第二数据报文的内层IP头和负荷(inner IP header和payload)即为源端的清洗设备121进行流量清晰后放行的第一正常流量，该第一数据报文可以被网关设备13或者清洗设备122转发给目标服务器14。

[0073] 由上述描述可知，本发明实施例当第二数据报文为封装后的数据报文时，对第二数据报文进行解封装，得到网络流量的第一数据报文以及第一数据报文的目的IP地址，根据第一数据报文的目的IP地址将第一数据报文转发至目标服务器，从而可以避免正常流量被目的端的清洗设备重复清洗，继而避免对目的端的清洗设备的计算资源造成浪费，并且还能避免目的端的清洗设备对正常流量的误清洗。

[0074] 图5示出了根据本发明的示例性实施例四的网络流量的处理方法的流程示意图；本实施例以在图1A所示的网关设备13上实现解封装为例进行示例性说明，如图5所示，包括如下步骤：

[0075] 步骤501，接收网络流量的数据报文。

[0076] 步骤502，当网络流量的数据报文为封装后的第二数据报文时，确定第二数据报文在进行隧道封装时采用的隧道协议的类型。

[0077] 步骤503，根据与隧道协议的类型相对应的报文格式对第二数据报文进行解封装，得到网络流量的第一数据报文以及第一数据报文的目的IP地址。

[0078] 步骤504，根据第一数据报文的目的IP地址将第一数据报文转发至目标服务器。

[0079] 上述步骤501以及步骤504的描述可以参见现有技术中的相关描述，在此不再详述。

[0080] 上述步骤502中，在一实施例中，可以通过解析第二数据报文，得到第二数据报文的外层IP地址，将该外层IP地址分别与目标服务器14的IP地址、隧道终结的网关设备13的IP地址进行比较来确定是否为封装后的第二数据报文，例如，当检测到外层IP地址与网关设备13的IP地址相同时，则可以确定该网络流量为需要转发至网关设备13的数据报文，当检测到外层IP地址与目标服务器14的IP地址相同时，则可以确定该网络流量为需要转发至第二清洗设备122的数据报文。

[0081] 上述步骤503中的解封装的描述可以参见上述图4所示实施例的相关描述，在此不再详述。

[0082] 本实施例在具有上述实施例的有益技术效果的基础上，通过将对第二数据报文进行解封装的流程在网关设备上实现，既可以缓解目的端的清洗设备的流量清洗的压力，还可以缩短正常流量达到目标服务器的时间，提升了用户体验。

[0083] 图6示出了根据本发明的示例性实施例五的网络流量的处理方法的流程示意图；本实施例以在图1B所示的第二流量清洗设备122上实现解封装为例进行示例性说明，如图6所示，包括如下步骤：

[0084] 步骤601，接收网络流量的数据报文。

[0085] 步骤602，检测网络流量的数据报文是否为封装后的第二数据报文，当网络流量的数据报文为封装后的第二数据报文时，执行步骤603，当网络流量的数据报文为攻击流量时，对网络流量进行流量清洗。

[0086] 步骤603，当第二数据报文为封装后的数据报文时，确定第二数据报文在进行隧道封装时采用的隧道协议的类型。

[0087] 步骤604，根据与隧道协议的类型相对应的报文格式对第二数据报文进行解封装，得到网络流量的第一数据报文以及第一数据报文的目的IP地址。

[0088] 步骤605，根据第一数据报文的目的IP地址将第一数据报文转发至目标服务器。

[0089] 上述步骤601以及步骤606的描述可以参见现有技术中的相关描述，在此不再详述。上述步骤603和步骤604的相关描述可以参见上述图5所示实施例的描述，在此不再详述。

[0090] 上述步骤602中，可以在封装后的第二数据报文中设置一个比特位，通过该比特位来表示第二数据报文为已封装的数据报文，例如，当该比特位为1时，确定第二数据报文为已封装的数据报文。

[0091] 本实施例在具有上述实施例的有益技术效果的基础上，通过将对第二数据报文进行解封装的流程在目的端的清洗设备上实现，避免了在目的端增加一个专用的隧道终结的网络设备，节省用户在网络部署时的硬件成本。

[0092] 对应于上述的网络流量的处理方法，本申请还提出了图7所示的根据本申请的一示例性实施例的清洗设备的示意结构图。请参考图7，在硬件层面，该清洗设备包括第一处理器、内部总线、第一网络接口、内存以及非易失性存储器，当然还可能包括其他业务所需要的硬件。第一处理器从非易失性存储器中读取对应的计算机程序到内存中然后运行，在逻辑层面上形成网络流量的处理装置。当然，除了软件实现方式之外，本申请并不排除其他实现方式，比如逻辑器件抑或软硬件结合的方式等等，也就是说以下处理流程的执行主体并不限定于各个逻辑单元，也可以是硬件或逻辑器件。

[0093] 其中，第一处理器，用于对被牵引的网络流量进行流量清洗，得到网络流量中的正常流量；对正常流量的第一数据报文进行隧道封装，得到封装后的第二数据报文；

[0094] 第一网络接口，用于将第一处理器得到的第二数据报文通过隧道传输至目标服务器。

[0095] 对应于上述的网络流量的处理方法，本申请还提出了图8所示的根据本申请的一示例性实施例的网络设备的示意结构图。请参考图8，在硬件层面，该网络设备包括第二处理器、内部总线、第二网络接口、内存以及非易失性存储器，当然还可能包括其他业务所需要的硬件。第二处理器从非易失性存储器中读取对应的计算机程序到内存中然后运行，在逻辑层面上形成网络流量的处理装置。当然，除了软件实现方式之外，本申请并不排除其他实现方式，比如逻辑器件抑或软硬件结合的方式等等，也就是说以下处理流程的执行主体并不限定于各个逻辑单元，也可以是硬件或逻辑器件。

[0096] 其中，第二网络接口，用于接收网络流量的数据报文；

[0097] 第二处理器，用于当第二网络接口接收到的网络流量的数据报文为封装后的第二数据报文时，对第二数据报文进行解封装，得到网络流量的第一数据报文以及第一数据报文的目的IP地址；根据第一数据报文的目的IP地址将第一数据报文转发至目标服务器。

[0098] 图9示出了根据本发明的示例性实施例一的网络流量的处理装置的结构示意图；如图9所示，该网络流量的处理装置可以应用在网络流量的源端，包括：流量清洗模块91、封装模块92、发送模块93。其中：

[0099] 流量清洗模块91，用于对被牵引的网络流量进行流量清洗，得到网络流量中的正常流量；

[0100] 封装模块92，用于对流量清洗模块91清洗得到的正常流量的第一数据报文进行隧道封装，得到封装后的第二数据报文；

[0101] 发送模块93，用于将封装模块92封装后的第二数据报文通过隧道传输至目标服务器。

[0102] 图10示出了根据本发明的示例性实施例二的网络流量的处理装置的结构示意图；如图10所示，在上述图9所示实施例的基础上，在一实施例中，封装模块92可包括：

[0103] 第一确定单元921，用于确定隧道协议的类型；

[0104] 封装单元922，用于根据与第一确定单元确定的隧道协议的类型相对应的报文格式对正常流量的第一数据报文进行封装。

[0105] 在一实施例中，封装单元922可包括：

[0106] 确定子单元9221，用于确定隧道对应的终结设备的IP地址；

[0107] 封装子单元9222，用于根据与隧道协议的类型相对应的报文格式将正常流量的第

一数据报文封装在内层IP头和负荷对应的字段，将确定子单元9221确定的终结设备的IP地址封装在外层IP头对应的字段。

[0108] 图11示出了根据本发明的示例性实施例三的网络流量的处理装置的结构示意图；如图11所示，该网络流量的处理装置可以应用在网络流量的目的端，包括：接收模块11、解封装模块12、转发模块13。其中：

[0109] 接收模块11，用于接收网络流量的数据报文；

[0110] 解封装模块12，用于当接收模块11接收到的网络流量数据报文为封装后的第二数据报文时，对第二数据报文进行解封装，得到网络流量的第一数据报文以及第一数据报文的目的IP地址；

[0111] 转发模块13，用于根据解封装模块12解封装得到的第一数据报文的目的IP地址将第一数据报文转发至目标服务器。

[0112] 图12示出了根据本发明的示例性实施例四的网络流量的处理装置的结构示意图；如图12所示，在上述图11所示实施例的基础上，在一实施例中，解封装模块12可包括：

[0113] 第二确定单元1201，用于确定第二数据报文在进行隧道封装时采用的隧道协议的类型；

[0114] 解封装单元1202，用于根据与第二确定单元1201确定的隧道协议的类型相对应的报文格式对第二数据报文进行解封装。

[0115] 在一实施例中，装置还可包括：

[0116] 检测模块14，用于检测接收模块11接收到的网络流量的第二数据报文是否为封装后的数据报文；

[0117] 当检测模块14检测到第二数据报文为封装后的数据报文时，解封装模块12执行对第二数据报文进行解封装的步骤。

[0118] 上述实施例可见，本申请通过对正常流量的第一数据报文进行隧道封装，得到封装后的第二数据报文，将第二数据报文通过隧道传输至目标服务器，可以避免正常流量被目的端的清洗设备重复清洗，继而避免对目的端的清洗设备的计算资源造成浪费，并且还能避免目的端的清洗设备对正常流量的误清洗。

[0119] 本领域技术人员在考虑说明书及实践这里公开的发明后，将容易想到本申请的其它实施方案。本申请旨在涵盖本申请的任何变型、用途或者适应性变化，这些变型、用途或者适应性变化遵循本申请的一般性原理并包括本申请未公开的本技术领域中的公知常识或惯用技术手段。说明书和实施例仅被视为示例性的，本申请的真正范围和精神由下面的权利要求指出。

[0120] 还需要说明的是，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、商品或者设备不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、商品或者设备所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括所述要素的过程、方法、商品或者设备中还存在另外的相同要素。

[0121] 以上所述仅为本申请的较佳实施例而已，并不用以限制本申请，凡在本申请的精神和原则之内，所做的任何修改、等同替换、改进等，均应包含在本申请保护的范围之内。

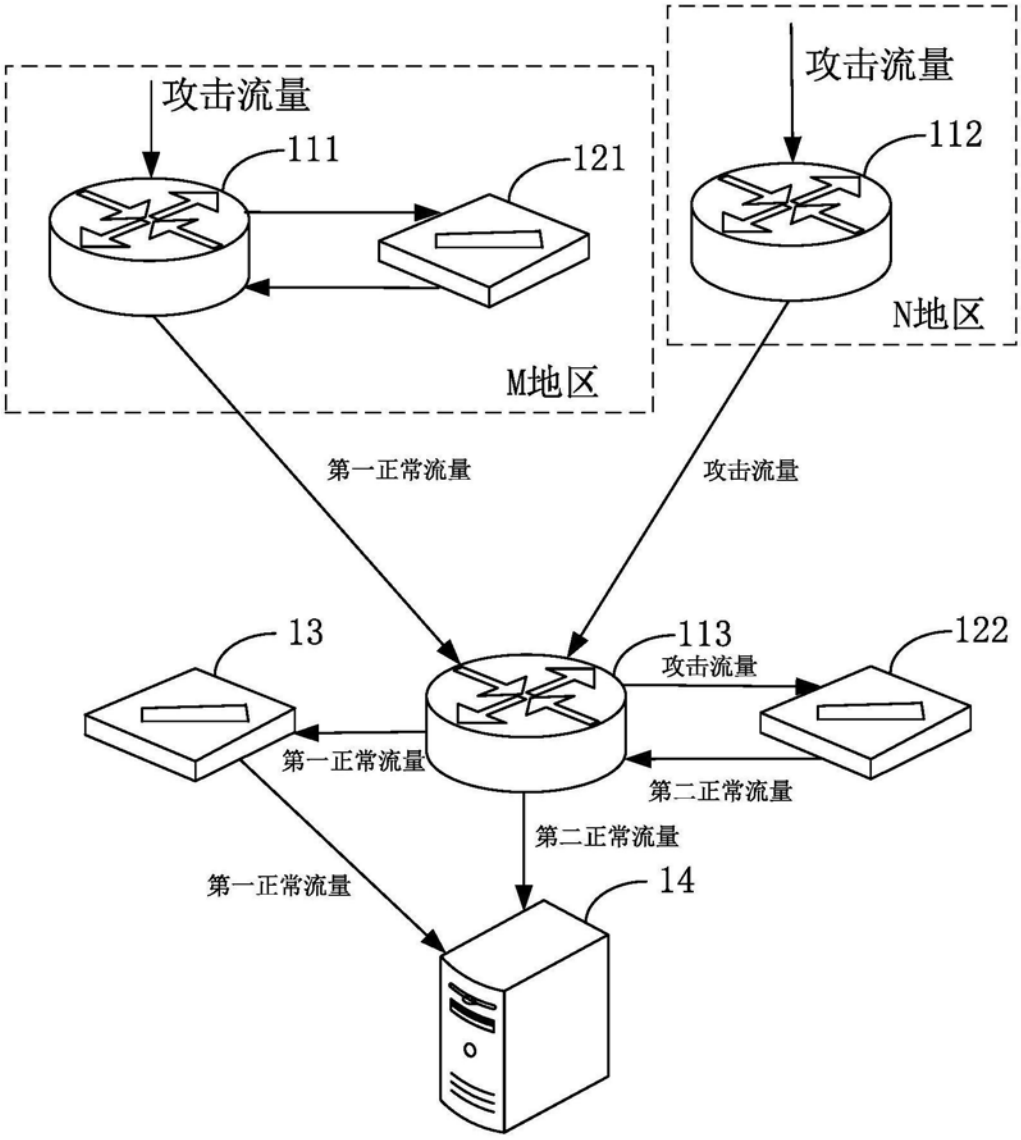

攻击流量
111
121
M地区
攻击流量
112
N地区
第一正常流量
攻击流量
13
113
攻击流量
122
第一正常流量
第二正常流量
第二正常流量
第一正常流量
14

图1A

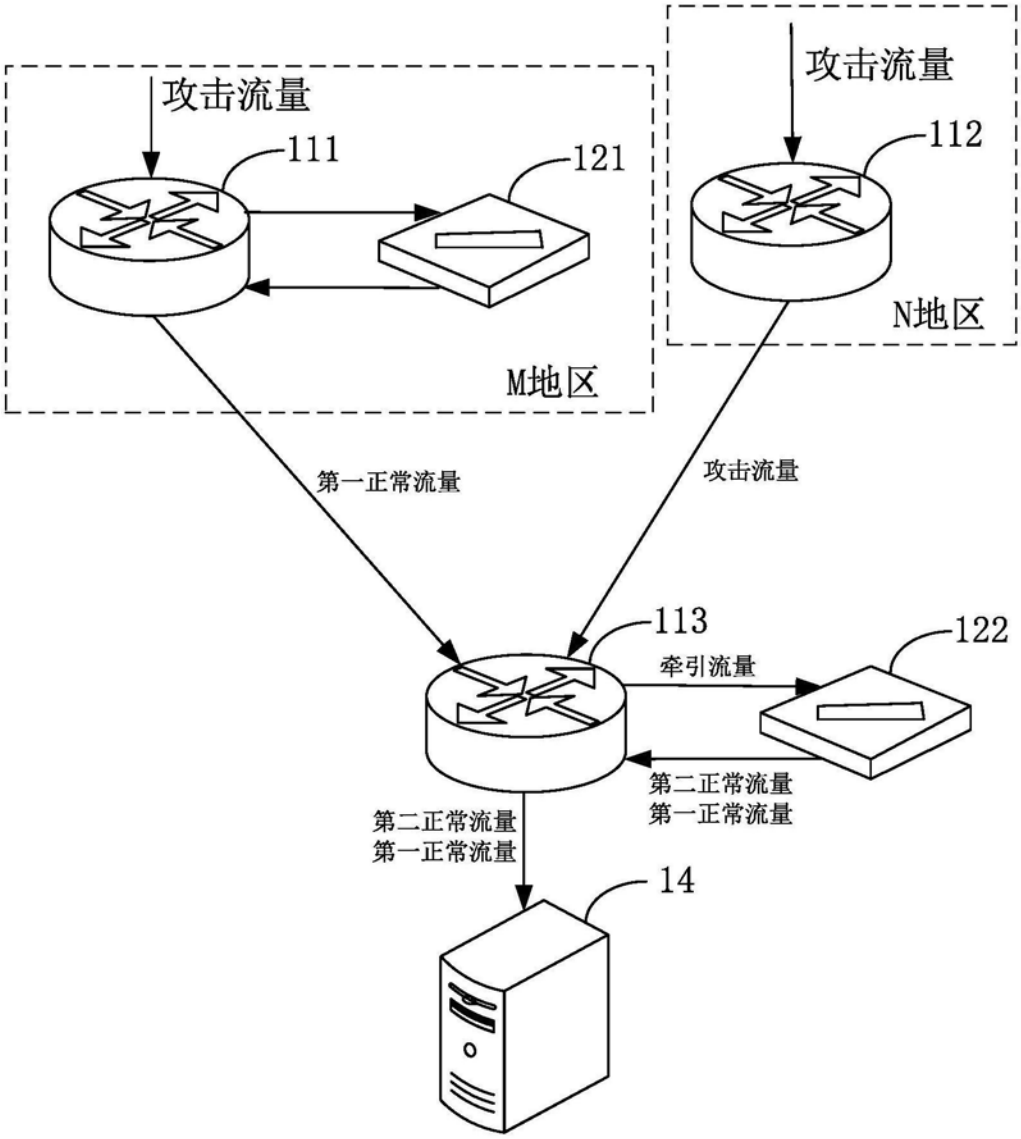

攻击流量
111
121
M地区
攻击流量
112
N地区
第一正常流量
攻击流量
113
牵引流量
122
第二正常流量
第一正常流量
第二正常流量
第一正常流量
14

图1B

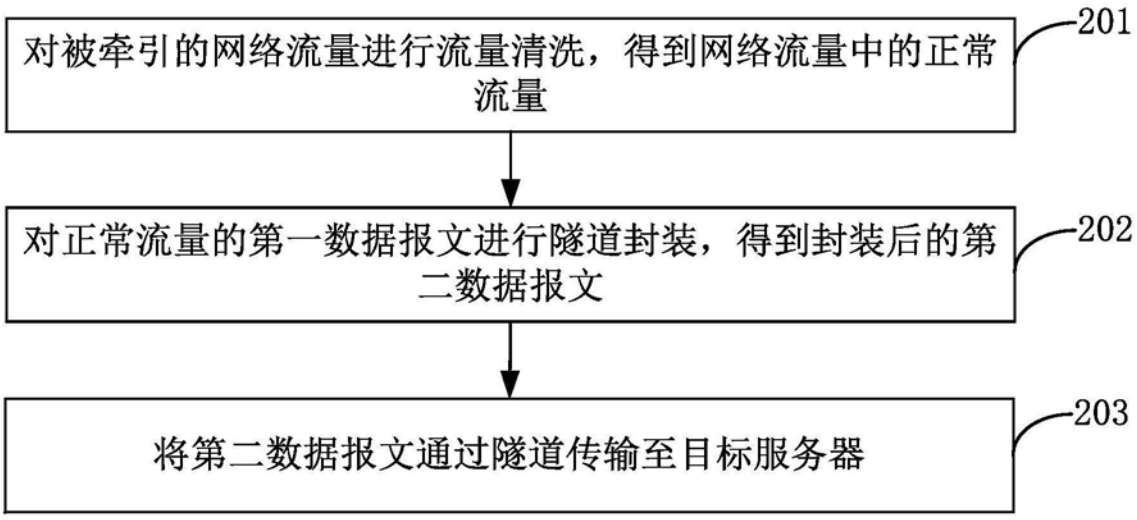

对被牵引的网络流量进行流量清洗，得到网络流量中的正常流量
201
对正常流量的第一数据报文进行隧道封装，得到封装后的第二数据报文
202
将第二数据报文通过隧道传输至目标服务器
203

图2A

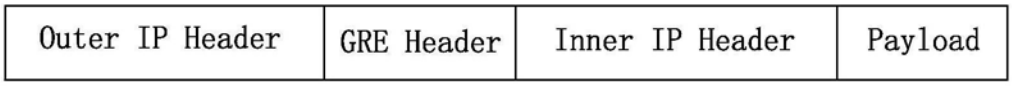

Outer IP Header
GRE Header
Inner IP Header
Payload

图2B

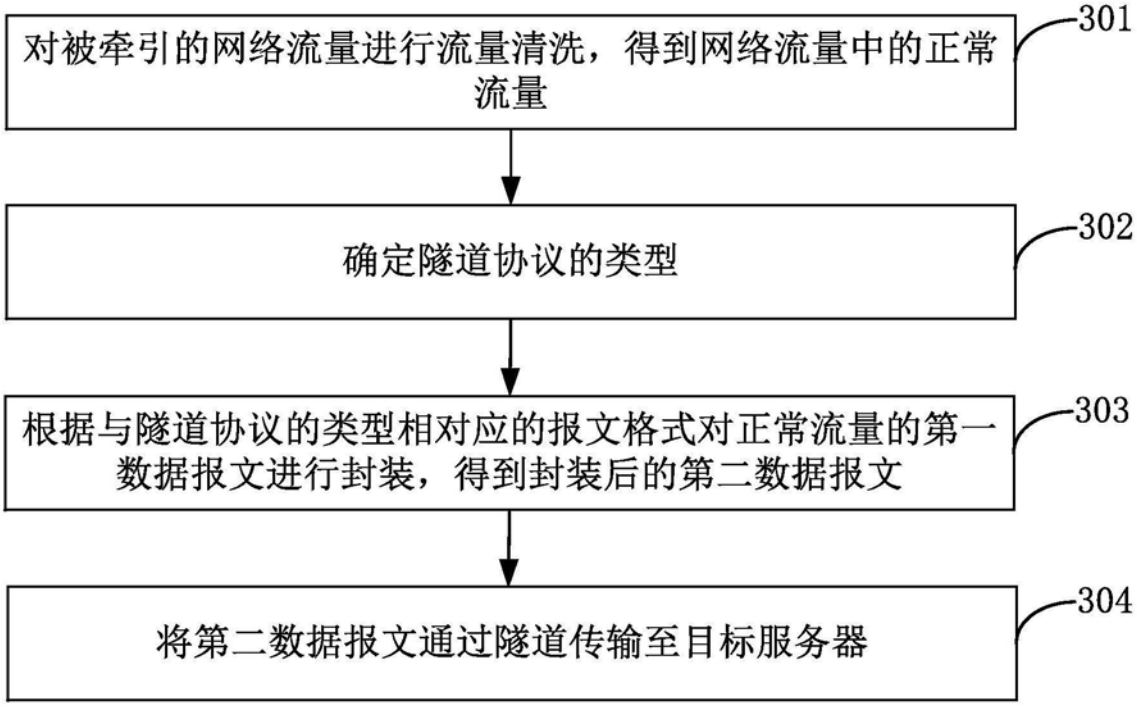

对被牵引的网络流量进行流量清洗，得到网络流量中的正常流量
301
确定隧道协议的类型
302
根据与隧道协议的类型相对应的报文格式对正常流量的第一数据报文进行封装，得到封装后的第二数据报文
303
将第二数据报文通过隧道传输至目标服务器
304

图3

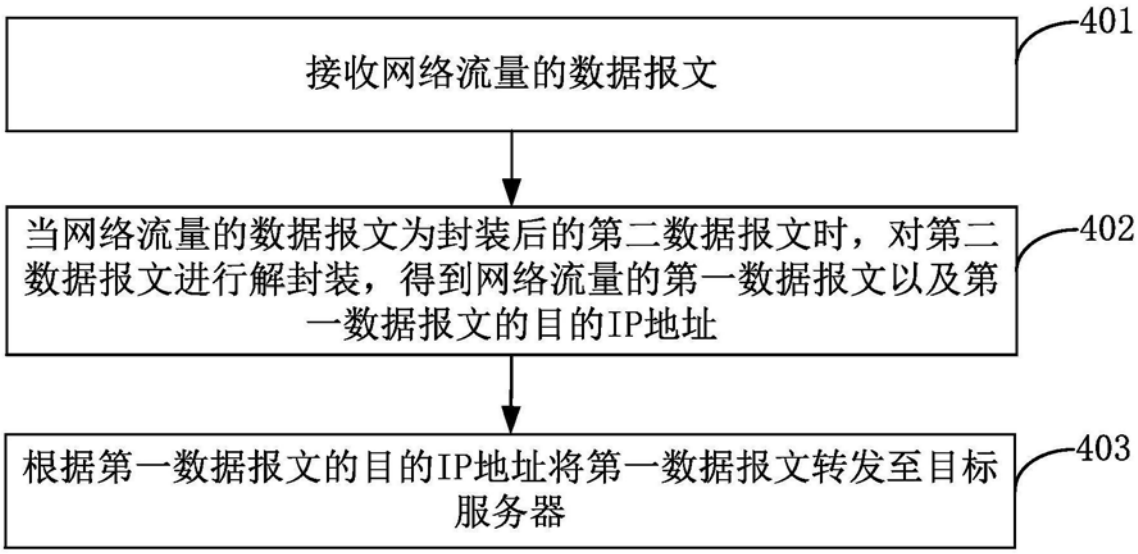

接收网络流量的数据报文
401
当网络流量的数据报文为封装后的第二数据报文时，对第二数据报文进行解封装，得到网络流量的第一数据报文以及第一数据报文的目的IP地址
402
根据第一数据报文的目的IP地址将第一数据报文转发至目标服务器
403

图4

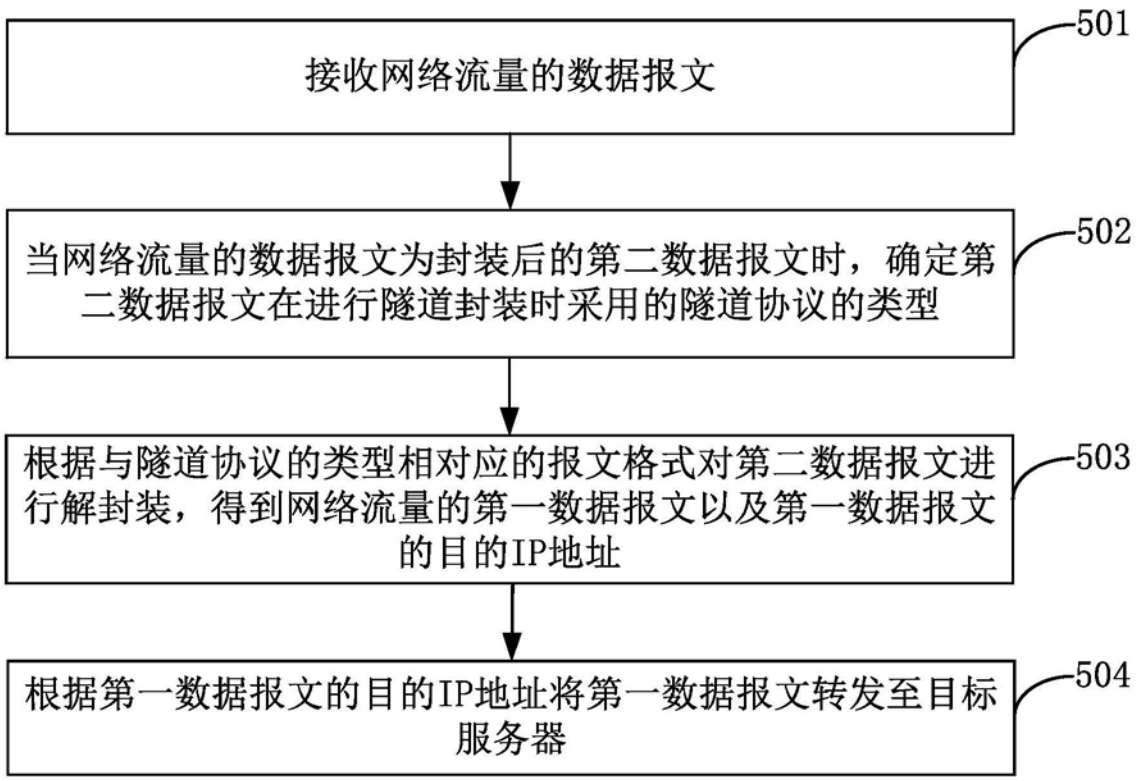

接收网络流量的数据报文
501
当网络流量的数据报文为封装后的第二数据报文时，确定第二数据报文在进行隧道封装时采用的隧道协议的类型
502
根据与隧道协议的类型相对应的报文格式对第二数据报文进行解封装，得到网络流量的第一数据报文以及第一数据报文的目的IP地址
503
根据第一数据报文的目的IP地址将第一数据报文转发至目标服务器
504

图5

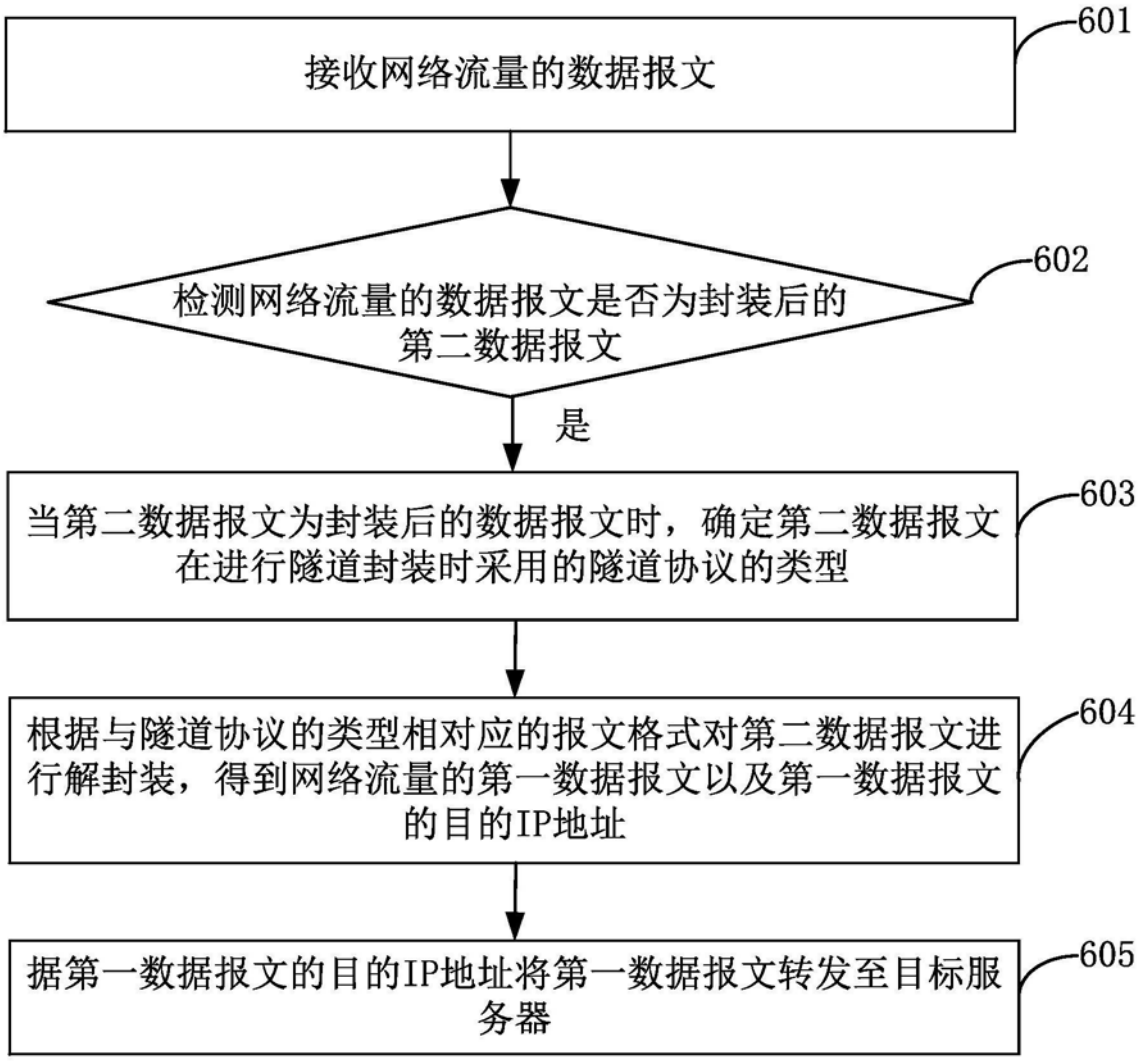

601
接收网络流量的数据报文
602
检测网络流量的数据报文是否为封装后的第二数据报文
是
603
当第二数据报文为封装后的数据报文时，确定第二数据报文在进行隧道封装时采用的隧道协议的类型
604
根据与隧道协议的类型相对应的报文格式对第二数据报文进行解封装，得到网络流量的第一数据报文以及第一数据报文的目的IP地址
605
据第一数据报文的目的IP地址将第一数据报文转发至目标服务器

图6

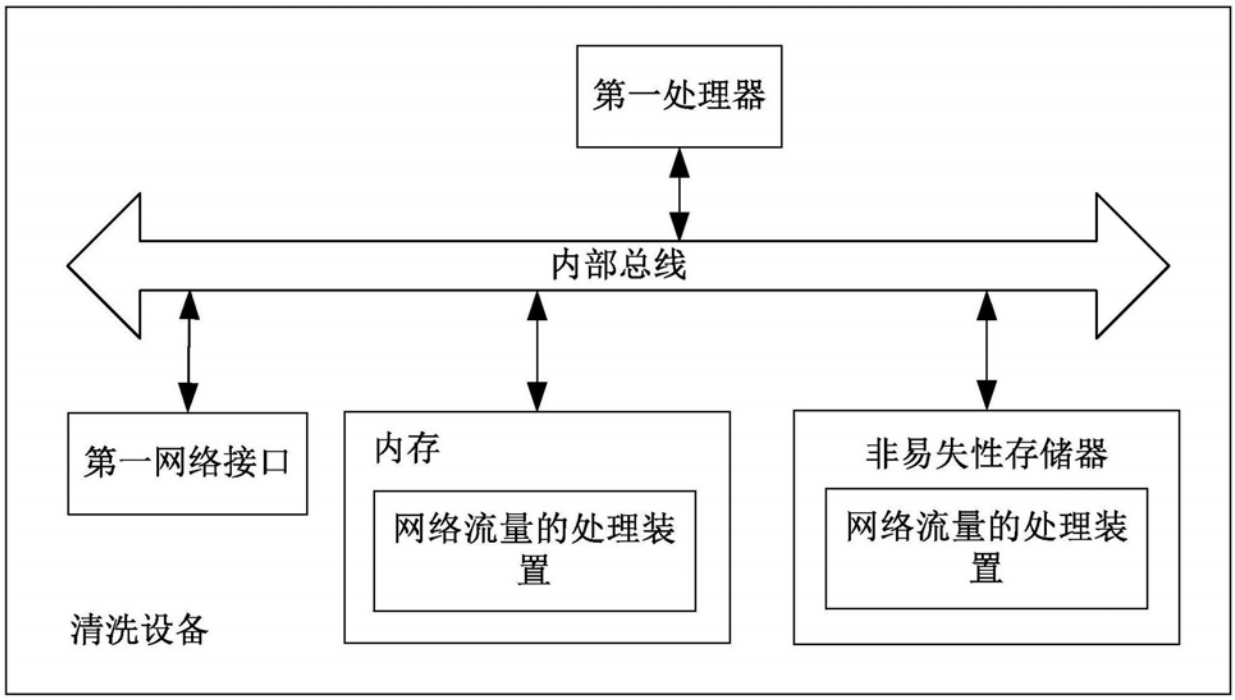

第一处理器
内部总线
第一网络接口
内存
网络流量的处理装置
非易失性存储器
网络流量的处理装置
清洗设备

图7

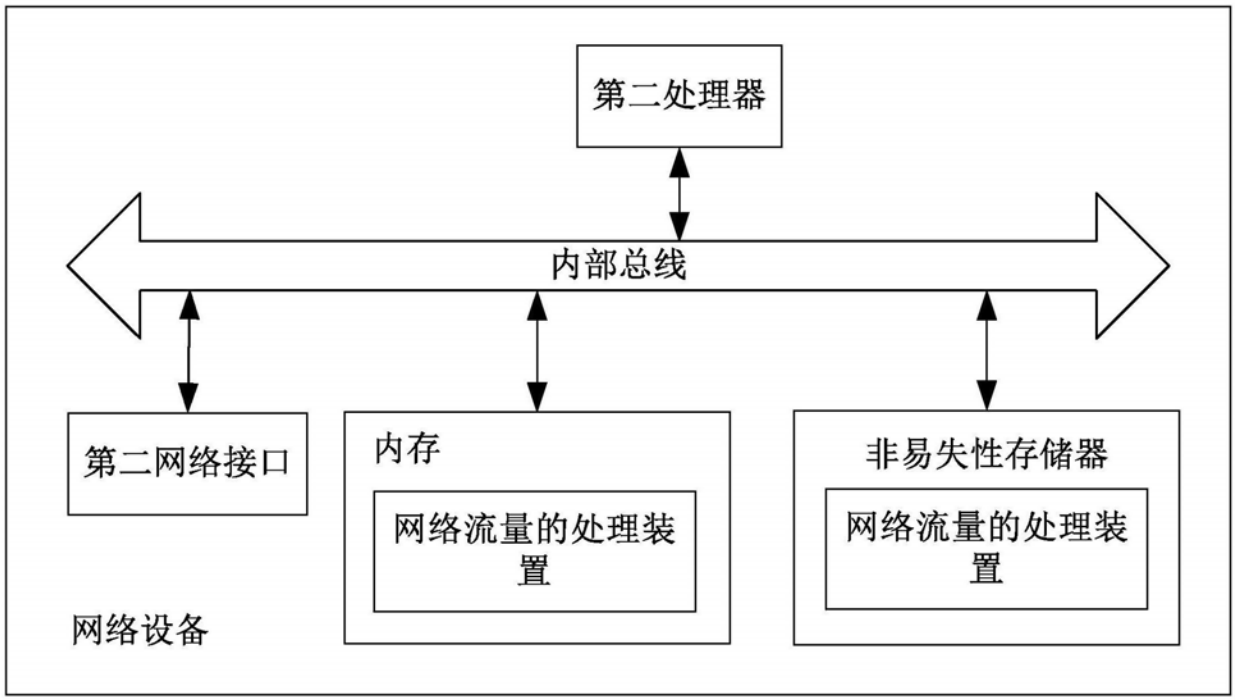

第二处理器
内部总线
第二网络接口
内存
网络流量的处理装置
非易失性存储器
网络流量的处理装置
网络设备

图8

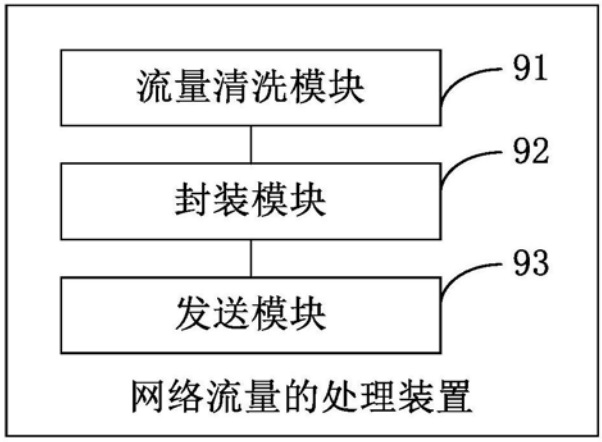

流量清洗模块
91
封装模块
92
发送模块
93
网络流量的处理装置

图9

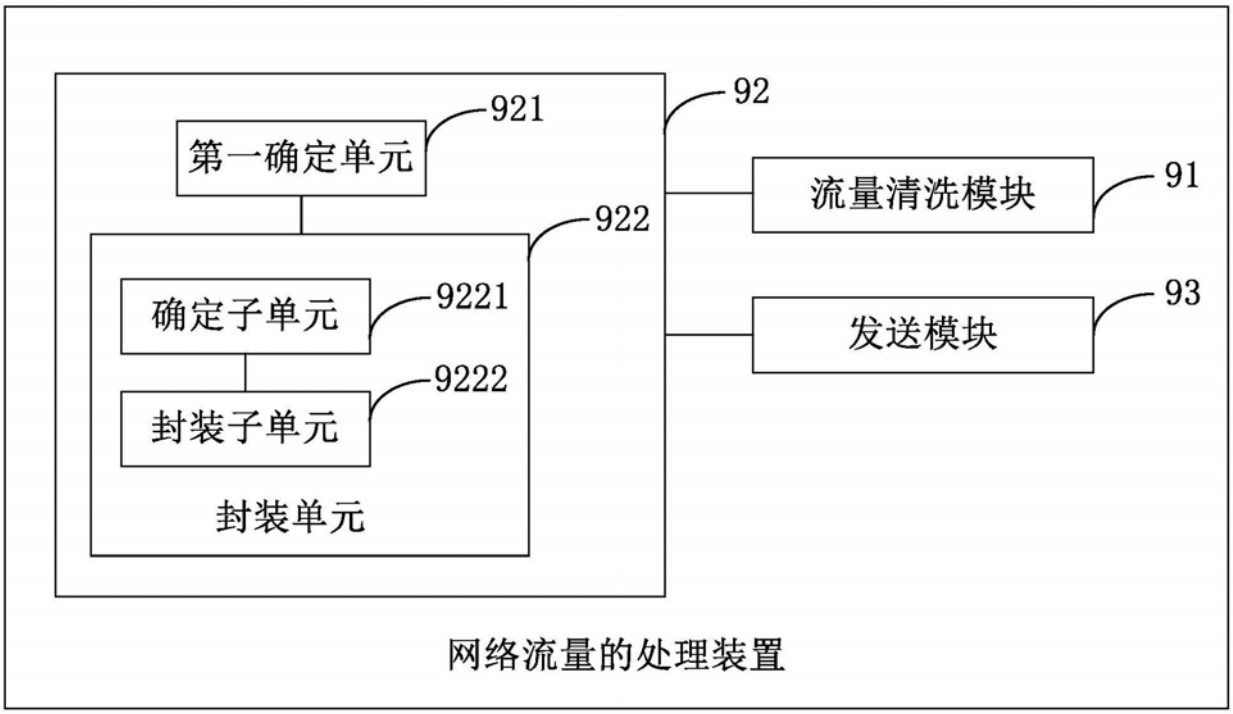

921
第一确定单元
92
922
确定子单元
9221
9222
封装子单元
封装单元
流量清洗模块
91
发送模块
93
网络流量的处理装置

图10

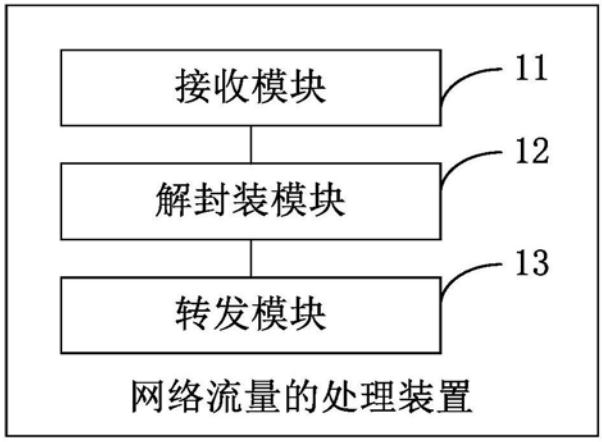

接收模块
11
解封装模块
12
转发模块
13
网络流量的处理装置

图11

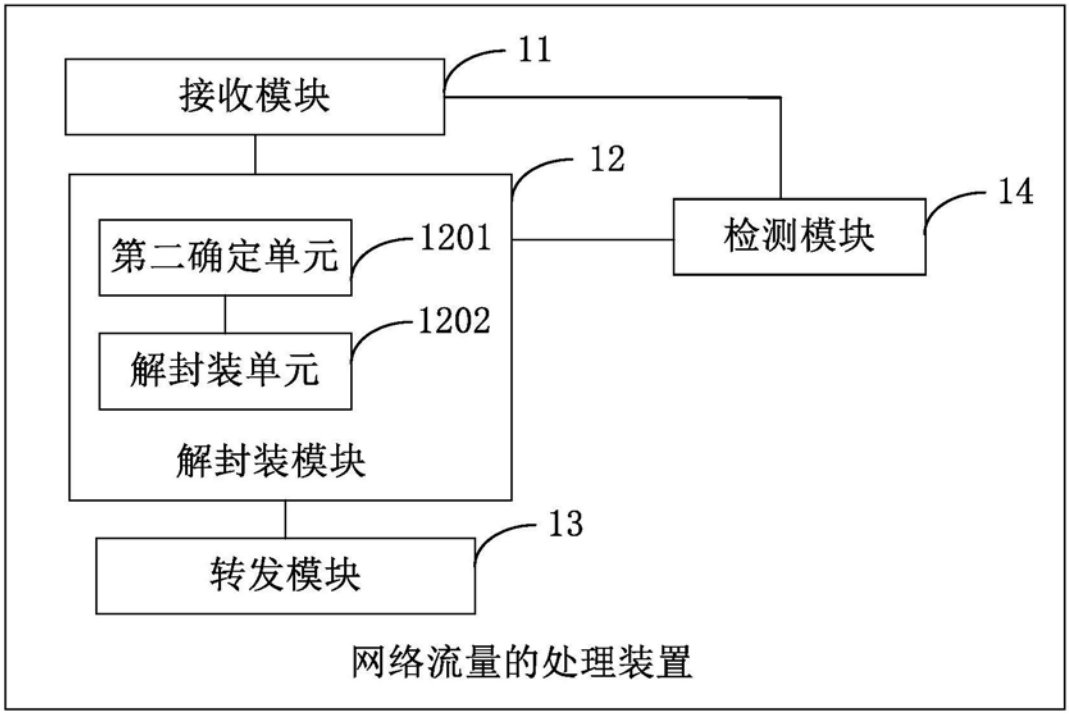

11
接收模块
12
第二确定单元
1201
检测模块
14
1202
解封装单元
解封装模块
13
转发模块
网络流量的处理装置

图12