(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 103036984 B
(45)授权公告日 2015.07.08

(21)申请号 201210546318.0
(22)申请日 2012.12.17
(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 薛智慧 蒋武 李世光
(74)专利代理机构 深圳中一专利商标事务所 44237
代理人 张全文
(51)Int.Cl.
H04L 29/08(2006.01)
H04L 29/06(2006.01)
H04L 12/803(2013.01)

(56)对比文件
CN 101795277 A,2010.08.04,
US 2007127388 A1,2007.06.07,

审查员 陈希元

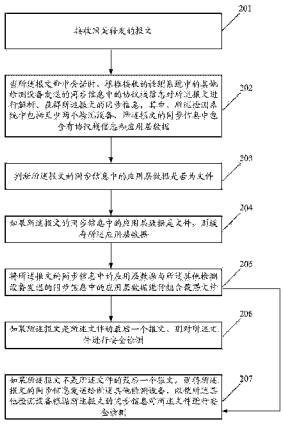
权利要求书2页 说明书10页 附图5页

(54)发明名称

一种单向流量的检测方法及网络设备

(57)摘要

本发明实施例公开一种单向流量的检测方法及网络设备，通过根据接收的检测系统中其他网络设备发送的同步信息中的协议栈信息对报文进行解析，并将所述报文的同步信息中的应用层数据与所述其他网络设备发送的同步信息中的应用层数据进行组合获得文件，如果所述报文是所述文件的最后一个报文时，则对所述文件进行安全检测，如果所述报文不是所述文件的最后一个报文时，则将所述报文的同步信息发送给其他网络设备，以使得所述其他网络设备根据所述报文的同步信息对所述文件进行检测从而实现对单向流量基于代理技术的安全检测。



CN 103036984 B

1. 一种单向流量的检测方法，其特征在于，所述方法包括：

接收网关转发的报文；

当所述报文命中会话时，根据接收的检测系统中的其他网络设备发送的同步信息中的协议栈信息对所述报文进行解析，获得所述报文的同步信息，其中，所述检测系统中包括至少两个网络设备，所述至少两个网络设备用于实现网络流量的负载均衡，所述报文的同步信息中包含有协议栈信息和应用层数据；

判断所述报文的同步信息中的应用层数据是否为文件；

如果所述报文的同步信息中的应用层数据是文件，则缓存所述应用层数据；

将所述报文的同步信息中的应用层数据与所述其他网络设备发送的同步信息中的应用层数据进行组合获得文件；

如果所述报文是所述文件的最后一个报文，则对所述文件进行安全检测；

如果所述报文不是所述文件的最后一个报文，则将所述报文的同步信息发送给所述其他网络设备，以使所述其他网络设备根据所述报文的同步信息对所述文件进行安全检测。

2. 根据权利要求 1 所述的单向流量的检测方法，其特征在于，所述根据接收的检测系统中的其他网络设备发送的同步信息中的协议栈信息对所述报文进行解析包括：

接收所述其他网络设备发送的封装的同步信息，其中所述其他网络设备发送的同步信息中包含有所述其他网络设备接收的文件的其他报文的协议栈信息以及应用层数据信息；

对所述其他网络设备发送的封装的同步信息进行解封装；

根据解封装后的所述其他网络设备发送的同步信息中的协议栈信息对所述报文进行解析。

3. 根据权利要求 1 所述的单向流量的检测方法，其特征在于，所述将所述报文的同步信息发送给所述其他网络设备包括：

将所述报文的同步信息进行封装；

将封装后的所述报文的同步信息发送给所述其他网络设备。

4. 根据权利要求 1-3 任意一项所述的方法，其特征在于：

所述同步信息中还包括五元组信息，

所述方法还包括：

根据接收的所述其他网络设备发送的同步信息中的五元组信息建立会话。

5. 根据权利要求 4 所述的方法，其特征在于，还包括：

如果所述报文的同步信息中的应用层数据不是文件，则根据所述五元组信息将所述报文通过所述网关设备进行转发。

6. 一种网络设备，其特征在于，所述网络设备包括：

接收单元，用于接收网关转发的报文；

解析单元，用于当所述报文命中会话时，根据所述接收单元接收的检测系统中的其他检测设备发送的同步信息中的协议栈信息对所述报文进行解析，获得所述报文的同步信息，其中，所述检测系统中包括至少两个检测设备，所述报文的同步信息中包含有协议栈信息和应用层数据；

判断单元，用于判断所述解析单元获得的所述报文的同步信息中的应用层数据是否为

文件；

缓存单元，用于如果所述报文的同步信息中的应用层数据是文件，则缓存所述应用层数据；

组合单元，用于将所述报文的同步信息中的应用层数据与所述其他检测设备发送的同步信息中的应用层数据进行组合获得文件；

安全检测单元，用于如果所述报文是所述文件的最后一个报文，则对所述文件进行安全检测；

发送单元，用于如果所述报文不是所述文件的最后一个报文，则将所述报文的同步信息发送给所述其他检测设备，以使所述其他检测设备根据所述报文的同步信息对所述文件进行安全检测。

7. 根据权利要求 6 所述的网络设备，其特征在于，所述解析单元，包括：

第一接收子单元，用于接收所述其他检测设备发送的封装的同步信息，其中所述其他检测设备发送的同步信息中包含有所述其他检测设备接收的文件的其他报文的协议栈信息以及应用层数据信息；

解封装子单元，用于对所述第一接收子单元接收的所述其他检测设备发送的封装的同步信息进行解封装；

解析子单元，用于根据所述解封装子单元解封装后的所述其他检测设备发送的同步信息中的协议栈信息对所述报文进行解析。

8. 根据权利要求 6 所述的网络设备，其特征在于，所述发送单元，包括：

封装子单元，用于将所述报文的同步信息进行封装；

发送子单元，用于将所述封装子单元封装后的所述报文的同步信息发送给所述其他检测设备。

9. 根据权利要求 6-8 任意一项所述的网络设备，其特征在于，所述同步信息还包括五元组信息，

所述网络设备还包括：

会话建立单元，用于根据接收的所述其他检测设备发送的同步信息中的五元组信息建立会话。

10. 根据权利要求 9 所述的网络设备，其特征在于，所述网络设备还包括：

转发单元，用于如果所述报文的同步信息中的应用层数据不是文件，则根据所述五元组信息将所述报文通过所述网关设备进行转发。

11. 一种单向流量的检测系统，其特征在于，所述检测系统包括至少两个如权利要求 6-10 任意一项所述的网络设备，所述至少两个网络设备用于实现网络流量的负载均衡。

一种单向流量的检测方法及网络设备

技术领域

[0001] 本发明属于安全检测领域，尤其涉及一种单向流量的检测方法及网络设备。

背景技术

[0002] 当前，在硬件安全市场中，反病毒(Anti-Virus，AV)或者数据泄露防护(DataLoss，DLP)等实现内容安全检测的功能，已经成为UTM或者其他网络安全设备必备的安全功能。由于AV或者DLP等特性本身主要都是对文件进行操作，如果每次都是对文件的部分内容进行操作，而不是整个文件的话，特性的检测率就会受到很大影响。在此基础上，出现了代理技术。

[0003] 代理可以使得网络设备充当中间人的角色，将报文中的文件内容全部缓存下来，待到整个文件全部还原后再进行安全检测，可以明显提高检测率。

[0004] 现有代理技术依赖于宿主操作系统提供的内核态协议栈功能，报文要到达应用程序，需要经过多次的报文拷贝，这在性能上是一个巨大的开销。同时，由操作系统内核来完全维护链接需要的所有信息，应用程序无法做到任何干预。

[0005] 由操作系统内核来维护链接信息所带来的缺点是：所有报文必须全部经过操作系统内核，才能实现链接信息的正常维护以形成完整的文件内容。而如果在单向流量场景下，报文会根据当前网络负载情况选择不同的链路进行转发。如果文件中有一个报文从其他路径转发而并没有经过内核进行处理，则此时该文件就会由于链接信息的不一致导致丢包，最终导致该文件的链接中断，无法形成完整的文件内容。因此，现有代理技术都不支持单向流量检测。

发明内容

[0006] 本发明实施例的目的在于提供一种检测单向流量的方法。所述方法在具有统一网关出口的负载均衡场景下，基于代理技术实现对单向流量的安全检测。

[0007] 第一方面，一种单向流量的检测方法，其特征在于，所述方法包括：

[0008] 接收网关转发的报文；

[0009] 当所述报文命中会话时，根据接收的检测系统中的其他网络设备发送的同步信息中的协议栈信息对所述报文进行解析，获得所述报文的同步信息，其中，所述检测系统中包括至少两个网络设备，所述报文的同步信息中包含有协议栈信息和应用层数据；

[0010] 判断所述报文的同步信息中的应用层数据是否为文件；

[0011] 如果所述报文的同步信息中的应用层数据是文件，则缓存所述应用层数据；

[0012] 将所述报文的同步信息中的应用层数据与所述其他网络设备发送的同步信息中的应用层数据进行组合获得文件；

[0013] 如果所述报文是所述文件的最后一个报文，则对所述文件进行安全检测；

[0014] 如果所述报文不是所述文件的最后一个报文，则将所述报文的同步信息发送给所述其他网络设备，以使所述其他网络设备根据所述报文的同步信息对所述文件进行安全检

测。

[0015] 结合第一方面，在第一方面的第一种可能的实现方式中，所述根据接收的检测系统中的其他网络设备发送的同步信息中的协议栈信息对所述报文进行解析包括：

[0016] 接收所述其他网络设备发送的封装的同步信息，其中所述其他网络设备发送的同步信息中包含有所述其他网络设备接收的文件的其他报文的协议栈信息以及应用层数据信息；

[0017] 对所述其他网络设备发送的封装的同步信息进行解封装；

[0018] 根据解封装后的所述其他网络设备发送的同步信息中的协议栈信息对所述报文进行解析。

[0019] 结合第一方面，在第一方面的第二种可能的实现方式中，所述将所述报文的同步信息发送给所述其他网络设备包括：

[0020] 将所述报文的同步信息进行封装；

[0021] 将封装后的所述报文的同步信息发送给所述其他网络设备。

[0022] 结合第一方面或者第一方面的第一种可能的实现方式或者第一方面的第二种可能的实现方式，在第一方面的第三种可能的实现方式中，所述同步信息中还包括五元组信息，所述方法还包括：

[0023] 根据接收的所述其他网络设备发送的同步信息中的五元组信息建立会话。

[0024] 结合第一方面的第三种可能的实现方式，在第一方面的第四种可能的实现方式中，还包括：

[0025] 如果所述报文的同步信息中的应用层数据不是文件，则根据所述五元组信息将所述报文通过所述网关设备进行转发。

[0026] 第二方面，一种网络设备，所述网络设备包括：

[0027] 接收单元，用于接收网关转发的报文；

[0028] 解析单元，用于当所述报文命中会话时，根据接收的检测系统中的其他检测设备发送的同步信息中的协议栈信息对所述报文进行解析，获得所述报文的同步信息，其中，所述检测系统中包括至少两个检测设备，所述报文的同步信息中包含有协议栈信息和应用层数据；

[0029] 判断单元，用于判断所述报文的同步信息中的应用层数据是否为文件；

[0030] 缓存单元，用于如果所述报文的同步信息中的应用层数据是文件，则缓存所述应用层数据；

[0031] 组合单元，用于将所述报文的同步信息中的应用层数据与所述其他检测设备发送的同步信息中的应用层数据进行组合获得文件；

[0032] 安全检测单元，用于如果所述报文是所述文件的最后一个报文，则对所述文件进行安全检测；

[0033] 发送单元，用于如果所述报文不是所述文件的最后一个报文，则将所述报文的同步信息发送给所述其他检测设备，以使所述其他检测设备根据所述报文的同步信息对所述文件进行安全检测。

[0034] 结合第二方面，在第二方面的第一种可能的实现方式中，所述解析单元，包括：

[0035] 第一接收子单元，用于接收所述其他检测设备发送的封装的同步信息，其中所述

其他检测设备发送的同步信息中包含有所述其他检测设备接收的文件的其他报文的协议栈信息以及应用层数据信息；

[0036] 解封装子单元，用于对所述其他检测设备发送的封装的同步信息进行解封装；

[0037] 解析子单元，用于根据解封装后的所述其他检测设备发送的同步信息中的协议栈信息对所述报文进行解析。

[0038] 结合第二方面，在第二方面的第二种可能的实现方式中，所述发送单元，包括：

[0039] 封装子单元，用于将所述报文的同步信息进行封装；

[0040] 发送子单元，用于将封装后的所述报文的同步信息发送给所述其他检测设备。

[0041] 结合第二方面或者第二方面的第一种可能的实现方式或者第二方面的第二种可能的实现方式，在第二方面的第三种可能的实现方式中，所述同步信息还包括五元组信息，

[0042] 所述网络设备还包括：

[0043] 会话建立单元，用于根据接收的所述其他检测设备发送的同步信息中的五元组信息建立会话。

[0044] 结合第二方面的第三种可能的实现方式，在第二方面的第四种可能的实现方式中，所述网络设备还包括：

[0045] 转发单元，用于如果所述报文的同步信息中的应用层数据不是文件，则根据所述五元组信息将所述报文通过所述网关设备进行转发。

[0046] 第三方面，一种系统，所述系统包括至少两个上述网络设备，所述至少两个网络设备用于实现网络流量的负载均衡。

[0047] 本发明实施例提供的一种单向流量的检测方法，通过根据接收检测系统中其他网络设备发送的同步信息中的协议栈信息对报文进行解析，并将所述报文的同步信息中的应用层数据与所述其他网络设备发送的同步信息中的应用层数据进行组合获得文件，如果所述报文是所述文件的最后一个报文时，则对所述文件进行安全检测，如果所述报文不是所述文件的最后一个报文时，则将所述报文的同步信息发送给其他网络设备，以使得所述其他网络设备根据所述报文的同步信息对所述文件进行检测，从而能够在利用多个网络设备接收文件的报文的情形下基于代理技术实现对单向流量的安全检测。

附图说明

[0048] 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，对于本领域普通技术人员来讲，在不付出创造性劳动性的前提下，还可以根据这些附图获得其他的附图。

[0049] 图 1 是本发明实施例提供的一种检测单向流量的方法应用场景图；

[0050] 图 2 是本发明实施例提供的一种单向流量检测的方法流程图；

[0051] 图 3 是本发明实施例提供的一种网络设备的装置结构图；

[0052] 图 4 是本发明实施例提供的一种网络设备中解析单元的装置结构图；

[0053] 图 5 是本发明实施例提供的一种网络设备中发送单元的装置结构图；

[0054] 图 6 是本发明实施例提供的又一种网络设备的装置结构图；

[0055] 图 7 是本发明实施例提供的又一种网络设备的装置结构图；

[0056] 图 8 是本发明实施例提供的一种系统结构图。

具体实施方式

[0057] 为了使本发明的目的、技术方案及优点更加清楚明白，以下结合附图及实施例，对本发明进行进一步详细说明。应当理解，此处所描述的具体实施例仅仅用以解释本发明，并不用于限定本发明。

[0058] 以上所述仅为本发明的较佳实施例而已，并不用以限制本发明，凡在本发明的精神和原则之内所作的任何修改、等同替换和改进等，均应包含在本发明的保护范围之内。

[0059] 参考图 1，图 1 是本发明实施例提供的一种单向流量的检测方法应用场景图。

[0060] 如图 1 所示，内网具有统一的网关出口，在内网中部署有至少两台的网络设备，图 1 中以两台网络设备（网络设备 A 和网络设备 B）为例进行说明，其中，网络设备和内网用户的个人电脑（Personal Computer，PC）全部连接在办公网络上，网络设备 A 和网络设备 B 具有同一的网关出口，即通过同一个网关设备 C 实现内网 PC 与外网设备的通信流量的转发，网络设备 A 和网络设备 B 构成的网络系统可以对至少一个 PC 的流量进行转发，因此，网络设备 A 和网络设备 B 需要对内网的至少一个 PC 与外部设备的流量进行处理、检测和转发，并能实现流量过滤的功能，且网络设备 A 和网络设备 B 能够实现流量的负载均衡。

[0061] 需要说明的是，本发明实施例中的多个网络设备包括网络设备及具有流量检测功能的其他网络设备，同样的，该多个网络设备构成的网络系统包括由多个网络设备构成的检测系统以及具有流量检测功能的网络系统。为了描述方便，下面的实施例中，将该多个网络设备构成的网络系统称为检测系统。

[0062] 参考图 2，图 2 是本发明实施例提供的一种单向流量的检测方法流程图。该方法可以由图 1 中的网络设备 A 或网络设备 B 来执行，如图 2 所示，该方法包括以下步骤：

[0063] 步骤 201，接收网关转发的报文；

[0064] 步骤 202，当所述报文命中会话时，根据接收的检测系统中的其他网络设备发送的同步信息中的协议栈信息对所述报文进行解析，获得所述报文的同步信息，其中，所述检测系统中包括至少两个网络设备，所述至少两个网络设备用于实现网络流量的负载均衡，所述报文的同步信息中包含有协议栈信息和应用层数据；

[0065] 其中，所述协议栈信息包括但不限于序列号、确认（Acknowledgement，ACK）号、头部长度、标记位、选项。

[0066] 可实现的，所述根据接收的检测系统中的其他网络设备发送的同步信息中的协议栈信息对所述报文进行解析包括：

[0067] 接收所述其他网络设备发送的封装的同步信息，其中所述其他网络设备发送的同步信息中包含有所述其他网络设备接收的文件的其他报文的协议栈信息以及应用层数据信息；

[0068] 对所述其他网络设备发送的封装的同步信息进行解封装；

[0069] 根据解封装后的所述其他网络设备发送的同步信息中的协议栈信息对所述报文进行解析。

[0070] 具体的，网络设备 B 接收网络设备 A 发送的封装的同步信息，所述网络设备将网络设备 A 发送的封装的同步信息进行解封装，并根据解封装后的同步信息中的协议栈信息对

所述网络设备 B 接收的第二报文进行解析。

[0071] 步骤 203，判断所述报文的同步信息中的应用层数据是否为文件；

[0072] 具体的，如果报文以 HTTP 协议传输，则当解码后应用层数据中出现 Content-Disposition 字段，就认为后面的数据的应用层数据是在传文件；如果报文以 FTP 协议传输，则当出现命令 RETR，会新建一个链接，则认为此链接是在传输文件。

[0073] 步骤 204，如果所述报文的同步信息中的应用层数据是文件，则缓存所述应用层数据；

[0074] 具体的，当网络设备 A 接收第一报文的同步信息中应用层数据是文件时，则所述网络设备 A 缓存所述应用层数据；当网络设备 B 接收第二报文的同步信息中的应用层数据是文件时，则所述网络设备 B 缓存所述应用层数据。

[0075] 步骤 205，将所述报文的同步信息中的应用层数据与所述其他网络设备发送的同步信息中的应用层数据进行组合获得文件；

[0076] 本领域人员可以知道，同一时间一个会话只能传输一个文件，因此，当通过多个设备进行负载均衡的情况下，在同一时间，同一文件的多个报文可以经过多个网络设备进行传输。由于同一个会话中的五元组信息(包括：源 IP、目的 IP、源端口、目的端口及协议类型)相同，而 ACK 号不同，因此，可以根据报文的五元组信息确定不同的报文是否属于同一个会话，从而可以根据报文的五元组信息来确定不同的报文是否属于同一个文件。并根据报文的 ACK 号将属于同一个文件的多个报文的应用层数据内容进行拼接以形成完整的文件内容。

[0077] 步骤 206，如果所述报文是所述文件的最后一个报文，则对所述文件进行安全检测；

[0078] 本领域人员可以知道，在进行文件传输时，会在该文件的最后一个数据包中打上传输结束的标识以表明该数据包为某个文件的最后一个数据包，因此，在本发明实施例中，可以根据报文中的结束标识来确定接收的报文是否为文件的最后一个报文，例如：如果在报文中出现 FIN 或 RST 标记，则表示该报文为文件的最后一个报文。

[0079] 步骤 207，如果所述报文不是所述文件的最后一个报文，则将所述报文的同步信息发送给所述其他网络设备，以使所述其他网络设备根据所述报文的同步信息对所述文件进行安全检测。

[0080] 可实现的，在步骤 207 中，为了保证文件链接的正确性和完整性，所述将所述报文的同步信息发送给所述其他网络设备可以包括：

[0081] 将所述报文的同步信息进行封装；

[0082] 将封装后的所述报文的同步信息发送给所述其他网络设备。

[0083] 具体的，当网络设备 A 判断接收的第一个报文不是文件的最后一个报文时，则所述网络设备 A 将第一报文的同步信息进行封装，发送到网络设备 B，使得所述网络设备 B 根据解封装后得到的第一报文的同步信息对第二报文进行解析。

[0084] 作为一种可选的实施例，所述方法还包括：

[0085] 如果所述报文的同步信息中的应用层数据不是文件，则根据所述五元组信息将所述报文通过所述网关设备进行转发。

[0086] 其中，所述五元组信息包括源 IP、目的 IP、源端口、目的端口、传输层协议。当网络

设备 A 判断所述报文的同步信息中的应用层数据不是文件时，则可以根据该报文的五元组信息将该报文通过网络设备 C 进行转发。

[0087] 本发明实施例提供的一种单向流量的检测方法，通过根据接收的检测系统中其他网络设备发送的同步信息中的协议栈信息对报文进行解析，并将所述报文的同步信息中的应用层数据与所述其他网络设备发送的同步信息中的应用层数据进行组合获得文件，如果所述报文是所述文件的最后一个报文时，则对所述文件进行安全检测，如果所述报文不是所述文件的最后一个报文时，则将所述报文的同步信息发送给其他网络设备，以使得所述其他网络设备根据所述报文的同步信息对所述文件进行检测从而实现对单向流量基于代理技术的安全检测。

[0088] 参考图 3，图 3 是本发明实施例提供的一种网络设备的装置结构图。所述装置包括如下单元：

[0089] 接收单元 301，用于接收网关转发的报文；

[0090] 解析单元 302，用于当所述报文命中会话时，根据所述接收单元接收的检测系统中的其他检测设备发送的同步信息中的协议栈信息对所述报文进行解析，获得所述报文的同步信息，其中，所述检测系统中包括至少两个检测设备，所述报文的同步信息中包含有协议栈信息和应用层数据；

[0091] 其中，所述协议栈信息包括但不限于序列号、确认（Acknowledgement，ACK）号、头部长度、标记位、选项。

[0092] 可实现的，所述解析单元 302，包括：

[0093] 第一接收子单元 401，用于接收所述其他检测设备发送的封装的同步信息，其中所述其他检测设备发送的同步信息中包含有所述其他检测设备接收的文件的其他报文的协议栈信息以及应用层数据信息；

[0094] 解封装子单元 402，用于对所述第一接收子单元接收的所述其他检测设备发送的封装的同步信息进行解封装；

[0095] 解析子单元 403，用于根据所述解封装子单元解封装后的所述其他检测设备发送的同步信息中的协议栈信息对所述报文进行解析。

[0096] 判断单元 303，用于判断所述解析单元获得的所述报文的同步信息中的应用层数据是否为文件；

[0097] 具体的，如果报文以 HTTP 协议传输，则当解码后应用层数据中出现 Content-Disposition 字段，就认为后面的数据的应用层数据是在传文件；如果报文以 FTP 协议传输，则当出现命令 RETR，会新建一个链接，则认为此链接是在传输文件。

[0098] 缓存单元 304，用于如果所述报文的同步信息中的应用层数据是文件，则缓存所述应用层数据；

[0099] 具体的，当网络设备 A 接收第一报文的同步信息中应用层数据是文件时，则所述网络设备 A 缓存所述应用层数据；当网络设备 B 接收第二报文的同步信息中的应用层数据是文件时，则所述网络设备 B 缓存所述应用层数据。

[0100] 组合单元 305，用于将所述报文的同步信息中的应用层数据与所述其他检测设备发送的同步信息中的应用层数据进行组合获得文件；

[0101] 本领域人员可以知道，同一时间一个会话只能传输一个文件，因此，当通过多个设

备进行负载均衡的情况下，在同一时间，同一文件的多个报文可以经过多个网络设备进行传输。由于同一个会话中的五元组信息(包括：源 IP、目的 IP、源端口、目的端口及协议类型)相同，而 ACK 号不同，因此，可以根据报文的五元组信息确定不同的报文是否属于同一个会话，从而可以根据报文的五元组信息来确定不同的报文是否属于同一个文件。并根据报文的 ACK 号将属于同一个文件的多个报文的应用层数据内容进行拼接以形成完整的文件内容。

[0102] 安全检测单元 306，用于如果所述报文是所述文件的最后一个报文，则对所述文件进行安全检测；

[0103] 发送单元 307，用于如果所述报文不是所述文件的最后一个报文，则将所述报文的同步信息发送给所述其他检测设备，以使所述其他检测设备根据所述报文的同步信息对所述文件进行安全检测。

[0104] 可实现的，所述发送单元 307，包括：

[0105] 封装子单元 501，用于将所述报文的同步信息进行封装；

[0106] 发送子单元 502，用于将所述封装子单元封装后的所述报文的同步信息发送给所述其他检测设备。

[0107] 本领域人员可以知道，在进行文件传输时，会在该文件的最后一个数据包中打上传输结束的标识以表明该数据包为某个文件的最后一个数据包，因此，在本发明实施例中，可以根据报文中的结束标识来确定接收的报文是否为文件的最后一个报文。

[0108] 具体的，当网络设备 A 判断接收的第一个报文不是文件的最后一个报文时，则所述网络设备 A 将第一报文的同步信息进行封装，发送到网络设备 B，使得所述网络设备 B 根据解封装后得到的第一报文的同步信息对第二报文进行解析。

[0109] 其中，所述五元组信息包括源 IP、目的 IP、源端口、目的端口、传输层协议。当网络设备 A 判断所述报文的同步信息中的应用层数据不是文件时，则可以根据该报文的五元组信息将该报文通过网络设备 C 进行转发。

[0110] 作为一种可选的实施例，所述同步信息还包括五元组信息，

[0111] 所述网络设备还包括：

[0112] 会话建立单元，用于根据接收的所述其他网络设备发送的同步信息中的五元组信息建立会话。

[0113] 图 6 本发明实施例提供的图 1 中所示网络设备的又一种装置结构示意图。如图 6 所示，其中会话管理模块可以包括图 3 所示实施例中的接收单元 201，用户态协议栈处理模块可以包括图 3 所示实施例中的解析单元 202、判断单元 203，应用层处理模块可以包括图 3 所示实施例中的缓存单元 204、组合单元 205、安全检测单元 206，消息处理模块可以包括图 3 所示实施例中的发送单元 207。

[0114] 假设外网发送文件分为第一报文和第二报文。当网络设备 A 接收到来自于外网的第一报文时，当所述第一报文是会话报文时，所述网络设备 A 的会话管理模块提取第一报文中的会话信息；所述网络设备 A 的用户态协议栈处理模块获取的第一报文中的同步信息，存储第一报文同步信息中的协议栈信息，将第一报文同步信息中的应用层数据发送到网络设备 A 的应用层代理模块，并将第一报文的同步信息发送给消息处理模块进行同步信息的封装，发给网络设备 B。

[0115] 网络设备 B 和网络设备 A 根据预先设置的 IP 地址列表是联网的，网络设备 B 将接收到网络设备 A 发送的封装的同步信息，所述网络设备 B 解封装所述封装的同步信息，将第一报文中的会话信息存储在网络设备 B 的会话管理模块，将第一报文中的同步信息存储在网络设备 B 的用户态协议栈，将第一报文中的应用层数据存储在网络设备 B 的应用层代理模块。

[0116] 当网络设备 B 接收到来自外网发送的同一个文件的第二报文时，所述网络设备 B 的会话管理模块根据网络设备 A 同步的同步信息中的协议栈信息对第二报文进行解析，提取第二报文中的会话信息；所述网络设备 B 的用户态协议栈处理模块提取第二报文中的同步信息，存储第二报文同步信息中的协议栈信息，将第二报文同步信息中的应用层数据发送到网络设备 B 的应用层代理模块。网络设备 B 的应用层代理模块将之前存储的第一报文的应用层数据和现在解析的第二报文的应用层数据进行组合获得文件。

[0117] 同时，所述网络设备 B 判断所述第二报文已经是所述文件的最后一个报文时，则所述网络设备 B 通过应用层代理模块对所述文件进行安全检测。

[0118] 本发明实施例提供的一种网络设备，通过根据接收的检测系统中其他网络设备发送的同步信息中的协议栈信息对报文进行解析，并将所述报文的同步信息中的应用层数据与所述其他网络设备发送的同步信息中的应用层数据进行组合获得文件，如果所述报文是所述文件的最后一个报文时，则对所述文件进行安全检测，如果所述报文不是所述文件的最后一个报文时，则将所述报文的同步信息发送给其他网络设备，以使得所述其他网络设备根据所述报文的同步信息对所述文件进行检测从而实现对单向流量基于代理技术的安全检测。

[0119] 参考图 7，图 7 是本发明实施例提供的一种网络设备的装置结构图。参考图 7，图 7 是本发明实施例提供的一种网络设备 700，本发明具体实施例并不对所述设备的具体实现做限定。所述网络设备 700 包括：

[0120] 处理器 (processor)701，通信接口 (Communications Interface)702，存储器 (memory)703，总线 704。

[0121] 处理器 701，通信接口 702，存储器 703 通过总线 704 完成相互间的通信。

[0122] 通信接口 702，用于与其他网络设备进行通信；

[0123] 处理器 701，用于执行程序。

[0124] 具体地，程序可以包括程序代码，所述程序代码包括计算机操作指令。

[0125] 处理器 701 可能是一个中央处理器 CPU，或者是特定集成电路 ASIC（Application Specific Integrated Circuit），或者是被配置成实施本发明实施例的一个或多个集成电路。

[0126] 存储器 703，用于存放程序 7031。存储器 803 可能包含高速 RAM 存储器，也可能还包括非易失性存储器（non-volatile memory）。

[0127] 程序 7031 具体可以包括：

[0128] 接收网关转发的报文；

[0129] 当所述报文命中会话时，根据接收的检测系统中的其他网络设备发送的同步信息中的协议栈信息对所述报文进行解析，获得所述报文的同步信息，其中，所述检测系统中包括至少两个网络设备，所述报文的同步信息中包含有协议栈信息和应用层数据；

[0130] 判断所述报文的同步信息中的应用层数据是否为文件；

[0131] 如果所述报文的同步信息中的应用层数据是文件，则缓存所述应用层数据；

[0132] 将所述报文的同步信息中的应用层数据与所述其他网络设备发送的同步信息中的应用层数据进行组合获得文件；

[0133] 如果所述报文是所述文件的最后一个报文，则对所述文件进行安全检测；

[0134] 如果所述报文不是所述文件的最后一个报文，则将所述报文的同步信息发送给所述其他网络设备，以使所述其他网络设备根据所述报文的同步信息对所述文件进行安全检测。

[0135] 程序 7031 中各功能模块的具体实现可以参见上述图 4- 图 6 所示实施例中的相应模块，在此不再赘述。

[0136] 参考图 8，图 8 是本发明实施例提供的一种检测系统结构图。如图 8 所示，为了描述方便，图 8 以检测系统中包括 3 个网络设备（网络设备 1、网络设备 2，网络设备 3）为例进行描述，实际应用中，所述系统可以包括至少两个网络设备，所述至少两个网络设备用于实现网络流量的负载均衡；

[0137] 所述网络设备，用于接收网关转发的报文；当所述报文命中会话时，根据接收的检测系统中的其他网络设备发送的同步信息中的协议栈信息对所述报文进行解析，获得所述报文的同步信息，所述报文的同步信息中包含有协议栈信息和应用层数据；判断所述报文的同步信息中的应用层数据是否为文件；如果所述报文的同步信息中的应用层数据是文件，则缓存所述应用层数据；将所述报文的同步信息中的应用层数据与所述其他网络设备发送的同步信息中的应用层数据进行组合获得文件；如果所述报文是所述文件的最后一个报文，则对所述文件进行安全检测；如果所述报文不是所述文件的最后一个报文，则将所述报文的同步信息发送给所述其他网络设备，以使所述其他网络设备根据所述报文的同步信息对所述文件进行安全检测。

[0138] 图 8 以检测系统中包括 3 个网络设备（网络设备 1、网络设备 2，网络设备 3）为例进行描述，假设外网发送文件分为第一报文和第二报文至第 N 报文，其中 N 等于或大于 2，当网络设备 1 接收到来自于外网的第一报文时，当所述第一报文是会话报文时，所述网络设备 1 的会话管理模块提取第一报文中的会话信息；所述网络设备 1 的用户态协议栈处理模块获取的第一报文中的同步信息，存储第一报文同步信息中的协议栈信息，将第一报文同步信息中的应用层数据发送到网络设备 1 的应用层代理模块，并将第一报文的同步信息发送给消息处理模块进行同步信息的封装，同步发给网络设备 2。

[0139] 网络设备 2 和网络设备 1 根据预先设置的 IP 地址列表是联网的，网络设备 2 将接收到网络设备 1 发送的封装的同步信息，所述网络设备 2 解封装所述封装的同步信息，将第一报文中的会话信息存储在网络设备 2 的会话管理模块，将第一报文中的同步信息存储在网络设备 2 的用户态协议栈处理模块，将第一报文中的应用层数据存储在网络设备 2 的应用层代理模块。

[0140] 当网络设备 2 接收到来自外网发送的同一个文件的第二报文时，所述网络设备 2 的用户态协议栈处理模块提取第二报文中的同步信息，存储第二报文同步信息中的协议栈信息，将第二报文同步信息中的应用层数据发送到网络设备 2 的应用层代理模块。网络设备 2 的应用层代理模块将之前存储的第一报文的应用层数据和现在解析的第二报文的应

用层数据进行组合获得文件。

[0141] 同时，所述网络设备 2 判断所述第二报文不是所述文件的最后一个报文时，则所述网络设备 2 通过消息处理模块将第二报文的同步信息进行封装，发送给系统中的其他网络设备，所述其他网络设备为除 2 以外的系统中的所有网络设备，例如网络设备 1。

[0142] 当所述网络设备 3 接收到来自外网发送的同一个文件的第 N 报文时，所述网络设备 3 的会话管理模块根据网络设备 3 同步的同步信息中的协议栈信息对第 N 报文进行解析，提取第 N 报文中的会话信息；所述网络设备 3 的用户态协议栈提取第 N 报文中的同步信息，存储第 N 报文同步信息中的协议栈信息，将第 N 报文同步信息中的应用层数据发送到网络设备 3 的应用层代理模块。网络设备 3 的应用层代理模块将之前存储的第一报文的应用层数据，第二报文的应用层数据及第 N-1 报文的应用层数据和现在解析的第 N 报文的应用层数据进行组合获得文件。

[0143] 同时，所述网络设备 3 判断所述第 N 报文已经是所述文件的最后一个报文时，则所述网络设备 3 通过应用层代理模块对所述文件进行安全检测。

[0144] 所属领域的技术人员可以清楚地了解到，为描述的方便和简洁，上述描述的设备和模块的具体工作过程，可以参考前述方法实施例中的对应过程描述，在此不再赘述。

[0145] 在本申请所提供的几个实施例中，应该理解到，所揭露的设备和方法，可以通过其它的方式实现。例如，以上所描述的装置实施例仅仅是示意性的，例如，所述模块的划分，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式，例如多个模块或组件可以结合或者可以集成到另一个设备中，或一些特征可以忽略，或不执行。另一点，所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些通信接口，装置或模块的间接耦合或通信连接，可以是电性，机械或其它的形式。

[0146] 所述作为分离部件说明的模块可以是或者也可以不是物理上分开的，作为模块显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部，模块来实现本实施例方案的目的。

[0147] 另外，在本发明各个实施例中的各功能模块可以集成在一个处理模块中，也可以是各个模块单独物理存在，也可以两个或两个以上模块集成在一个模块中。

[0148] 最后应说明的是：以上各实施例仅用以说明本发明的技术方案，而非对其限制；尽管参照前述各实施例对本发明进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分或者全部技术特征进行等同替换；而这些修改或者替换，并不使相应技术方案的本质脱离本发明各实施例技术方案的范围。

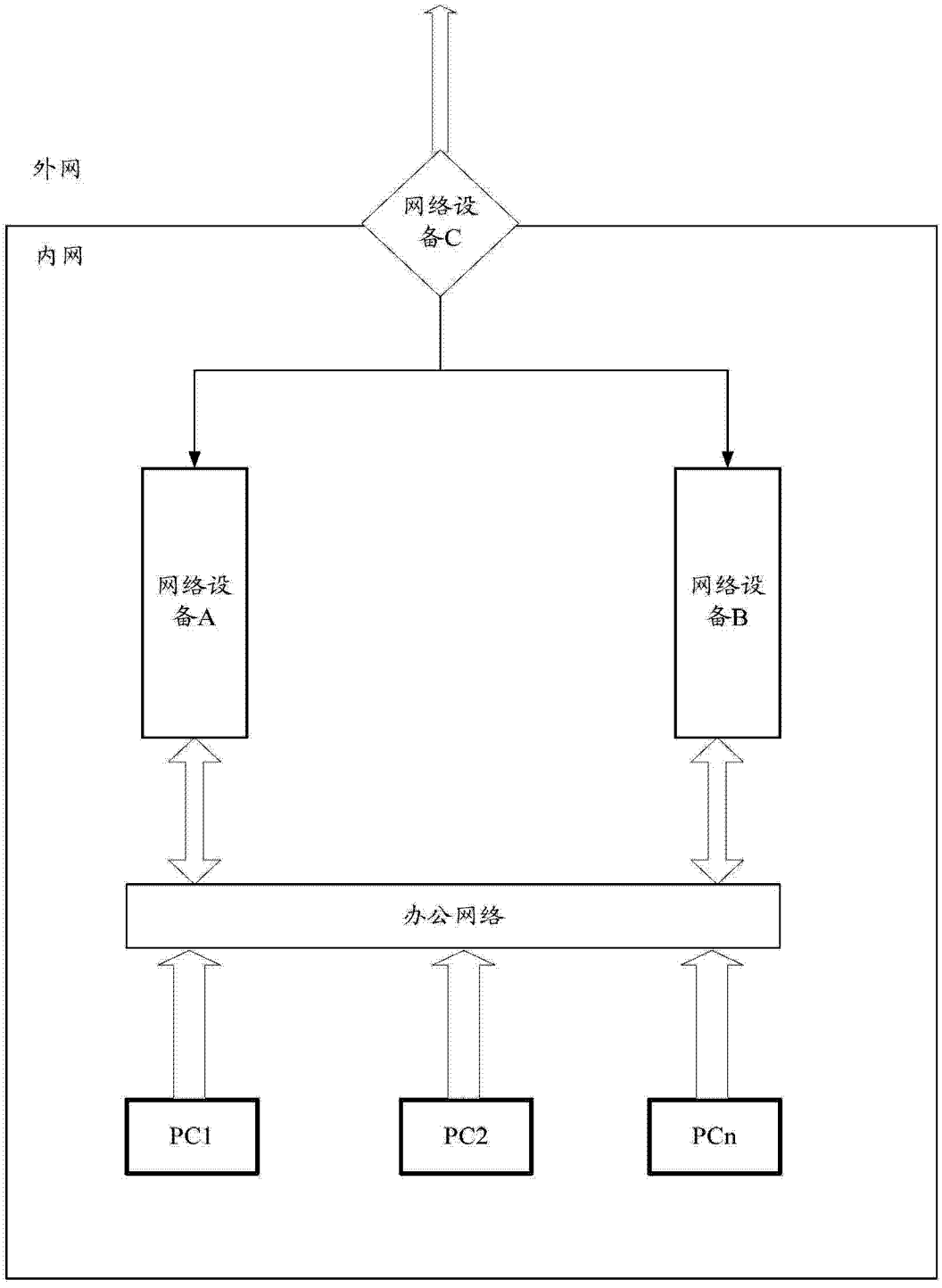


图 1

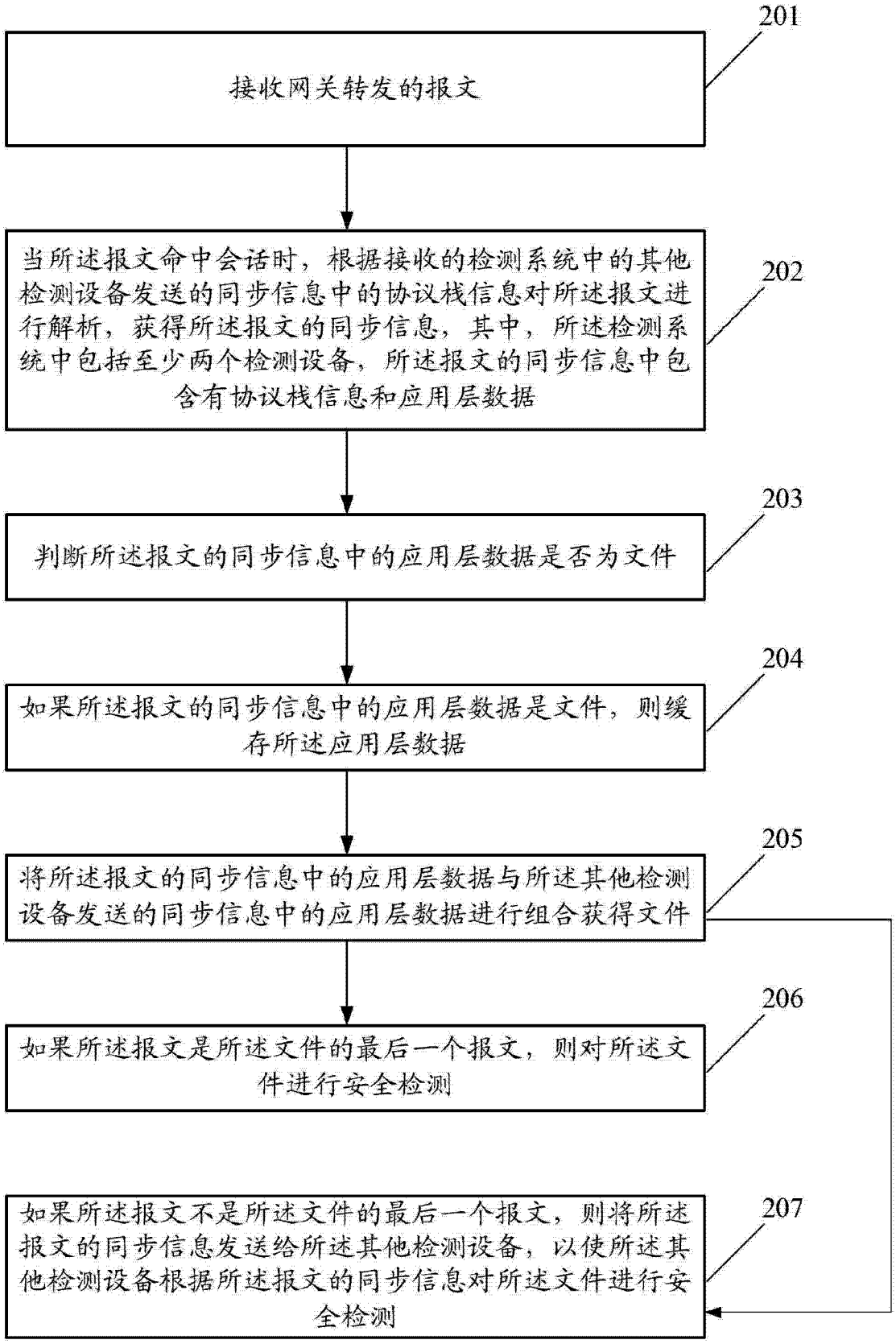

201
接收网关转发的报文
202
当所述报文命中会话时，根据接收的检测系统中的其他检测设备发送的同步信息中的协议栈信息对所述报文进行解析，获得所述报文的同步信息，其中，所述检测系统中包括至少两个检测设备，所述报文的同步信息中包含有协议栈信息和应用层数据
203
判断所述报文的同步信息中的应用层数据是否为文件
204
如果所述报文的同步信息中的应用层数据是文件，则缓存所述应用层数据
205
将所述报文的同步信息中的应用层数据与所述其他检测设备发送的同步信息中的应用层数据进行组合获得文件
206
如果所述报文是所述文件的最后一个报文，则对所述文件进行安全检测
207
如果所述报文不是所述文件的最后一个报文，则将所述报文的同步信息发送给所述其他检测设备，以使所述其他检测设备根据所述报文的同步信息对所述文件进行安全检测

图 2

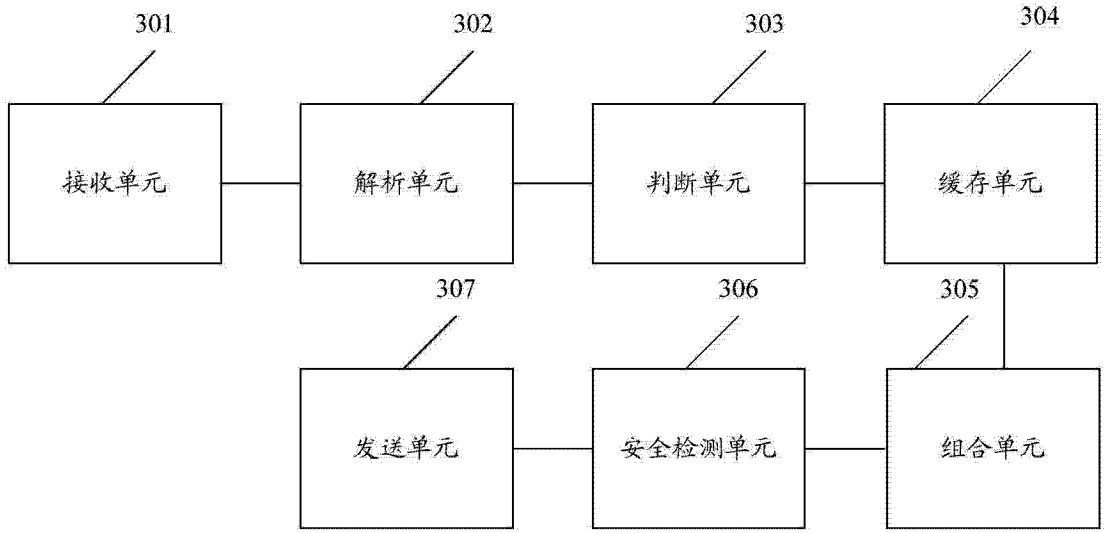

301
302
303
304
接收单元
解析单元
判断单元
缓存单元
307
306
305
发送单元
安全检测单元
组合单元

图 3

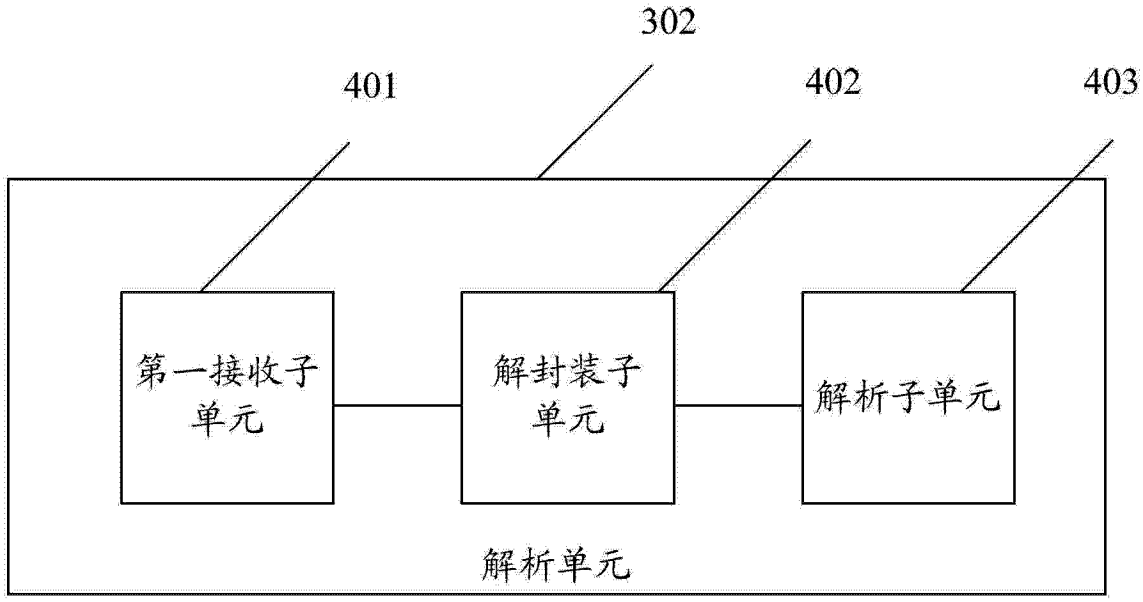

302
401
402
403
第一接收子单元
解封装子单元
解析子单元
解析单元

图 4

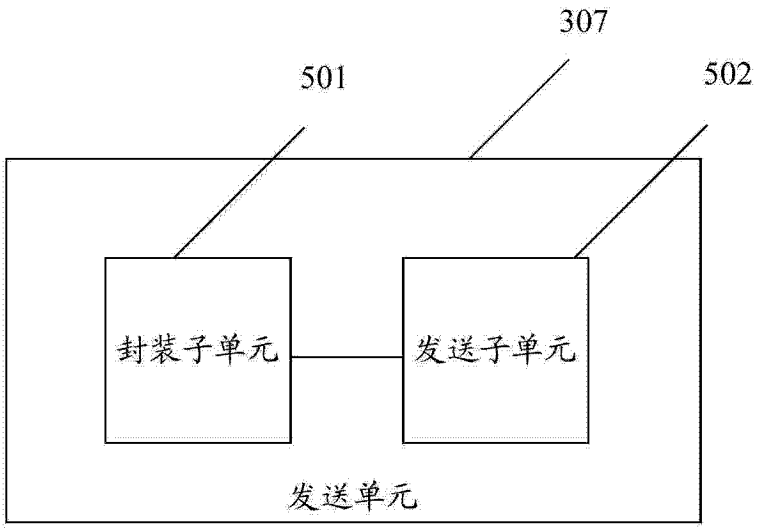

307
501
502
封装子单元
发送子单元
发送单元

图 5

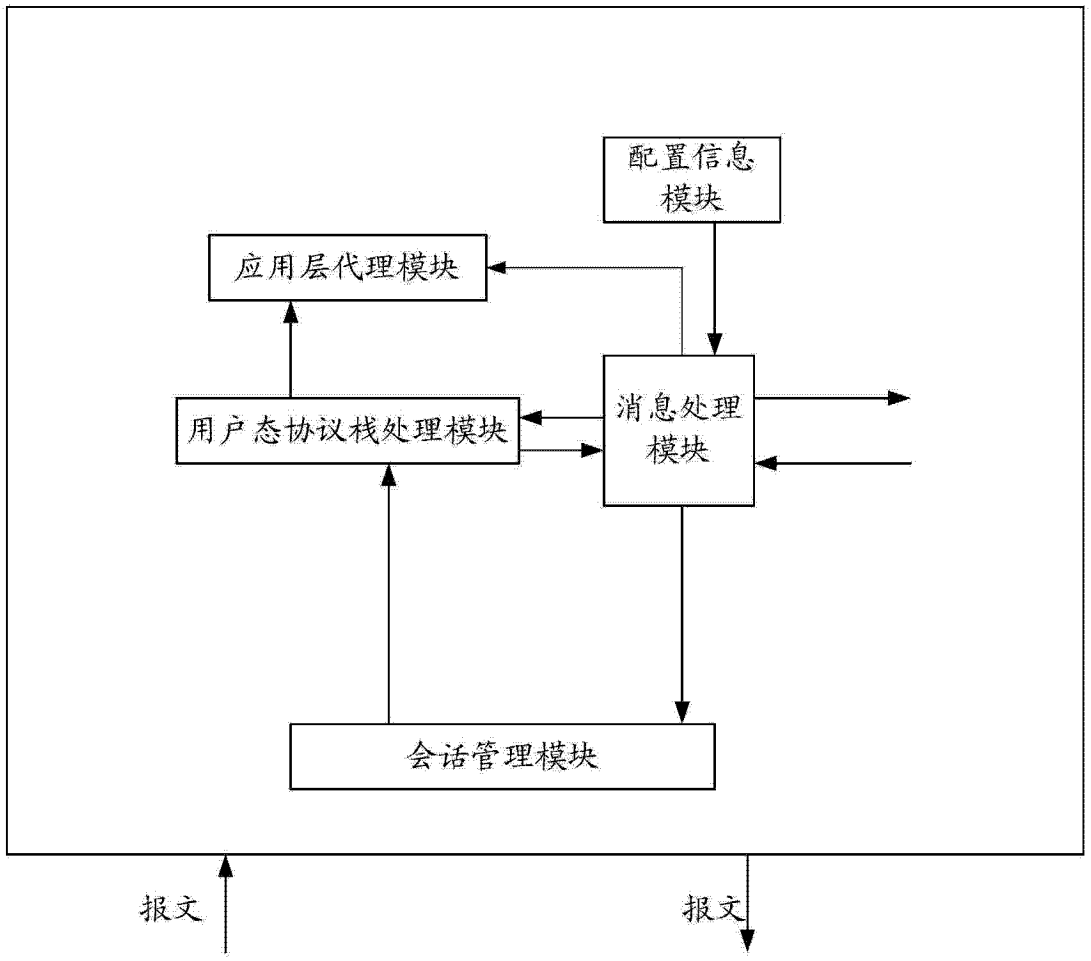

配置信息模块
应用层代理模块
用户态协议栈处理模块
消息处理模块
会话管理模块
报文
报文

图 6

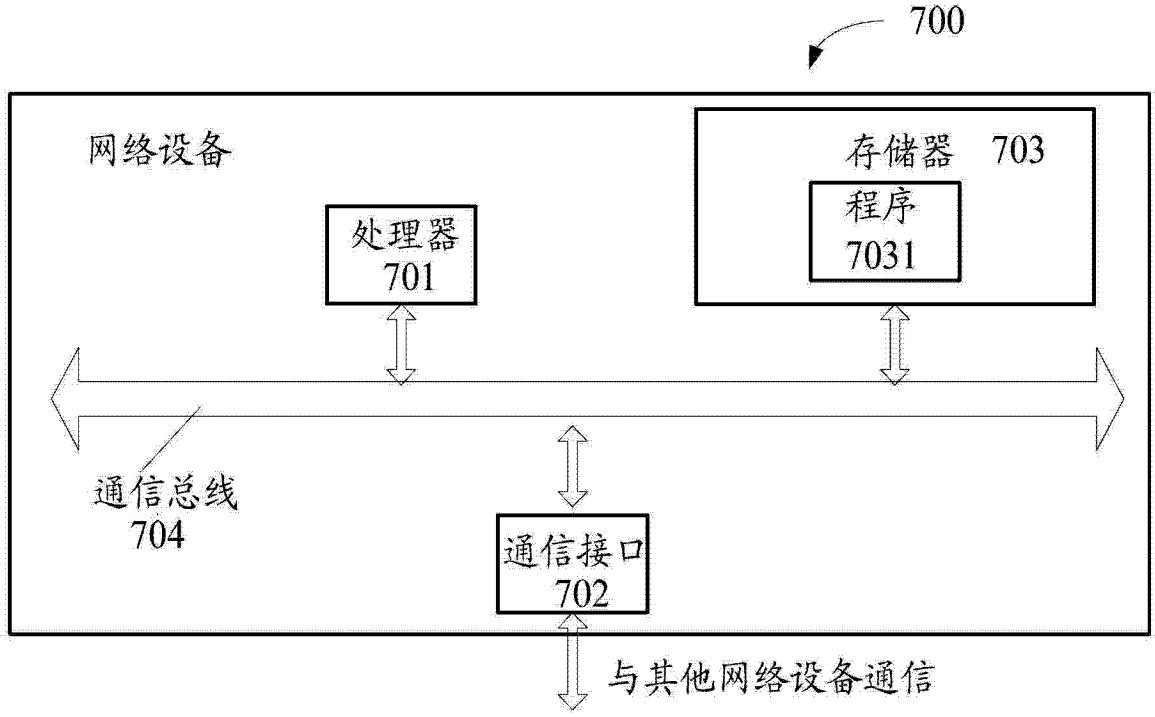

700
网络设备
存储器 703
程序
7031
处理器
701
通信总线
704
通信接口
702
与其他网络设备通信

图 7


网络设备1
网络设备2
网络设备3

图 8