(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
2022 年 5 月 19 日 (19.05.2022)

WIPO | PCT

(10) 国际公布号
WO 2022/100001 A1

(51) 国际专利分类号:
H04L 29/06 (2006.01)

(21) 国际申请号: PCT/CN2021/088488

(22) 国际申请日: 2021 年 4 月 20 日 (20.04.2021)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
202011248794.5 2020年11月10日 (10.11.2020) CN

(71) 申请人: 华 为 技 术 有 限 公 司 (**HUAWEI TECHNOLOGIES CO., LTD.**) [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(72) 发明人: 何 新 乾 (**HE, Xinqian**); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 周 侃 (**ZHOU, Kan**); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(74) 代理人: 北京三高永信知识产权代理有限责任公司 (**BEIJING SAN GAO YONG XIN INTELLECTUAL PROPERTY AGENCY CO., LTD.**); 中国北京市海淀区学院路蓟门里和景园A座1单元102室, Beijing 100088 (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,

(54) **Title:** NETWORK SECURITY PROTECTION METHOD AND PROTECTION DEVICE

(54) **发明名称**: 网络安全防护方法以及防护设备

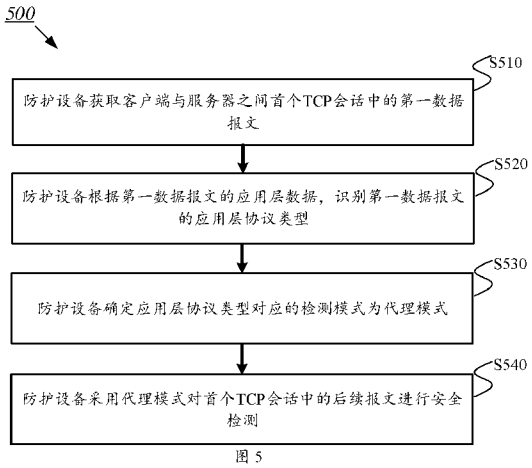


图 5

S510 A protection device acquires a first data message in a first TCP session between a client and a server
S520 The protection device identifies an application layer protocol type of the first data message according to application layer data of the first data message
S530 The protection device determines that a testing mode corresponding to the application layer protocol type is a proxy mode
S540 The protection device uses the proxy mode to perform security testing on a subsequent message in the first TCP session

(57) **Abstract:** The present application belongs to the technical field of communications, and provides a network security protection method and a protection device. The method comprises: when a message of a first session is exchanged between a client and a server, a protection device identifying an application layer protocol type according to application layer data in the message of the first session; determining, according to the application layer protocol type, that a testing mode is a proxy mode; and then using the proxy mode to perform security testing on a subsequent message of the first TCP session. Therefore, the technical bottleneck that the message of the first TCP session can only be tested using a flow mode is broken through, and it is ensured that the message of the first TCP session can also be tested using the proxy mode, thereby avoiding attack missed detection caused by the message of the first TCP session being limited to the flow mode.

(57) **摘要**: 本申请提供了一种网络安全防护方法以及防护设备，属于通信技术领域。在客户端与服务器之间交互首个会话的报文时，防护设备通过根据首个会话的报文中的应用层数据，识别应用层协议类型，根据应用层协议类型确定检测模式为代理模式，则采用代理模式对首个TCP会话的后续报文进行安全检测，从而突破首个TCP会话的报文只能采用流模式检测的技术瓶颈，保证首个TCP会话的报文也能通过代理模式检测，避免首个TCP会话的报文局限于流模式造成攻击漏检。

WO 2022/100001 A1

[见续页]

GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, JO, JP, KE, KG, KH, 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, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, 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, 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))。

网络安全防护方法以及防护设备

本申请要求于 2020 年 11 月 10 日提交的申请号为 202011248794.5、发明名称为“网络安全防护方法以及防护设备”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

本申请涉及通信技术领域，特别涉及一种网络安全防护方法以及防护设备。

背景技术

现代网络安全防护方案的基本原理是在客户端与受保护的服务器之间部署防护设备（如防火墙），由防护设备对客户端与服务器之间交互的报文进行检测。

代理模式是防护设备的重要检测模式。代理模式的原理是防护设备代替服务器发送确认报文给客户端，并且防护设备代替客户端发送确认报文给服务器。在代理模式下，防护设备需要使用传输控制协议/互联网协议（transmission control protocol/internet protocol，TCP/IP）协议栈负责报文的可靠发送。代理模式有助于检测出复杂的网络攻击，更能满足安全防护的需求，然而代理模式防护设备需要对大量数据报文进行缓存重组、以及支持完整的协议栈，因此需要消耗大量资源。

相关技术中，在客户端和服务器数量较大时，由于处理性能的限制，防护设备难以对每个客户端和服务器之间所有会话中交互的报文都采用代理模式进行检测。通常的做法是防护设备在客户端和服务器之间建立首个会话的过程中进行识别，并记录首个会话的 IP 地址、目的端口号、以及协议类型等信息，以确定是否需要以代理模式对同一客户端与同一服务器上的同一端口之间建立的后续会话进行检测。这种方案，防护设备实际上未对客户端和服务器之间建立首个会话中的报文进行安全检测，在这种方案中，如果客户端与服务器之间交互的首个会话中的报文存在攻击行为，则防护设备就会出现漏检问题。

发明内容

本申请实施例提供了一种网络安全防护方法以及防护设备，有助于避免首个会话中的报文存在攻击行为时出现漏检。所述技术方案如下。

第一方面，提供了一种网络安全防护方法，在该方法中，防护设备获取客户端设备与服务器之间首个 TCP 会话中的第一数据报文，所述首个 TCP 会话为客户端设备与服务器之间建立的第一个会话，所述防护设备部署于所述客户端设备与所述服务器之间；所述防护设备根据所述第一数据报文的应用层数据，识别所述第一数据报文的应用层协议类型；所述防护设备确定所述应用层协议类型对应的检测模式为代理模式；所述防护设备采用所述代理模式对所述首个 TCP 会话中的后续报文进行安全检测。

第一方面提供了能够快速切换至代理模式的方案。在客户端与服务器之间交互首个会话的报文时，防护设备通过根据首个会话的报文中的应用层数据，识别应用层协议类型，根据应用层协议类型确定检测模式为代理模式，则采用代理模式对首个 TCP 会话的后续报文进行

安全检测，从而突破首个 TCP 会话的报文只能采用流模式检测的技术瓶颈，保证首个 TCP 会话的报文也能通过代理模式检测，避免首个 TCP 会话的报文局限于流模式造成攻击漏检。

可选地，所述防护设备获取客户端设备与服务器之间首个 TCP 会话中的第一数据报文之前，所述方法还包括：所述防护设备获取所述客户端设备与所述服务器之间传输的第一握手报文，所述第一握手报文用于创建所述首个 TCP 会话，所述第一握手报文包括第一选项以及第二选项，所述第一选项为所述防护设备支持的选项，所述第二选项为所述防护设备不支持的选项；所述防护设备从所述第一握手报文删除所述第二选项，从而得到第二握手报文；所述防护设备向所述第一握手报文的目的设备发送所述第二握手报文。

通过上述可选方式，避免因客户端设备和服务器设备使用防护设备不支持的选项进行通信而造成的防护设备针对首条流切换到代理模式后，由于难以解析客户端或者服务器使用的选项造成报文传输失败，提高模式切换流程的可靠性和成功率。

可选地，所述首个 TCP 会话中的后续报文包括第二数据报文，所述防护设备采用所述代理模式对所述首个 TCP 会话中的后续报文进行安全检测，包括：所述防护设备接收并缓存所述第二数据报文；所述防护设备根据所述第一选项生成针对所述第二数据报文的确认报文；所述防护设备向所述第二数据报文的源设备发送所述针对第二数据报文的确认报文，所述第二数据报文的源设备为所述客户端设备或者所述服务器。

通过上述可选方式，提供之前在流模式下已缓存数据报文的复杂情况下如何模式切换的实现方式，提升方案的可用性。

可选地，所述首个 TCP 会话中的后续报文包括第三数据报文，所述防护设备采用所述代理模式对所述首个 TCP 会话中的后续报文进行安全检测，包括：所述防护设备发送并缓存所述第三数据报文；如果所述第三数据报文满足重传条件，所述防护设备根据所述第一选项向所述第三数据报文的目的设备重新发送所述第三数据报文，所述第三数据报文的目的设备为所述客户端设备或者所述服务器。

通过上述可选方式，提供之前在流模式下已发送数据报文的复杂情况下如何模式切换的实现方式，提升方案的可用性。

可选地，所述重传条件包括：所述防护设备未接收到针对数据报文的确认报文；或者，所述第一选项为选择性确认（selective acknowledgement，SACK）选项，所述重传条件包括：所述防护设备根据来自于数据报文的目的设备的 SACK 选项中的信息，确定数据报文发生丢包。

通过上述可选方式，有助于防护设备在代理模式下保证报文的传输可靠性。

可选地，所述第一握手报文为来自于所述客户端设备的同步序列编号（synchronize sequence numbers，SYN）报文，所述第一握手报文的目的设备为所述服务器；或者，所述第一握手报文为来自于所述服务器的同步序列编号确认（synchronize sequence numbers acknowledgement，SYN ACK）报文，所述第一握手报文的目的设备为所述客户端设备。

可选地，所述安全检测为防病毒（anti virus，AV）检测，所述防护设备采用所述代理模式对所述首个 TCP 会话中的后续报文进行安全检测，包括：所述防护设备采用所述代理模式对所述首个 TCP 会话中的第四数据报文进行 AV 检测，所述第四数据报文为所述首个 TCP 会话中在所述第一数据报文之后传输的报文；所述方法还包括：如果所述防护设备对所述首个 TCP 会话中的第四数据报文进行 AV 检测的结果为不包含病毒，所述防护设备切换为流模式，

并采用所述流模式针对所述首个TCP会话中所述第四数据报文之后传输的后续报文继续进行安全检测。

通过上述可选方式，由于防护设备通过 AV 检测结果发现客户端设备与服务器在首个会话交互的数据报文不包含病毒时，从代理模式切换为流模式，从而利用流模式加速针对首个会话后续的处理流程，降低设备的资源占用量，有助于提升检测性能。

可选地，所述防护设备采用所述代理模式对所述首个TCP会话中的后续报文进行安全检测，包括：所述防护设备采用所述代理模式对所述首个TCP会话中的第五数据报文进行检测，所述第五数据报文为所述首个TCP会话中在所述第一数据报文之后传输的报文；所述方法还包括：如果所述第五数据报文的应用层数据指示所述客户端设备与所述服务器将要在所述TCP会话中进行加密通信，所述防护设备切换为流模式，并采用所述流模式针对所述首个TCP会话中所述第五数据报文之后传输的后续报文继续进行安全检测。

通过上述可选方式，由于防护设备发现客户端设备与服务器后续将要在首个会话加密通信时，从代理模式切换为流模式，有助于在防护设备不支持加解密功能导致无法利用代理模式对加密数据检测的场景下，及时切换回流模式，从而利用流模式加速首个会话后续的处理流程，降低设备的资源占用量，有助于提升检测性能。

第二方面，提供了一种防护设备，该防护设备具有实现上述第一方面或第一方面任一种可选方式的功能。该防护设备包括至少一个单元，至少一个单元用于实现上述第一方面或第一方面任一种可选方式所提供的方法。

在一些实施例中，防护设备中的单元通过软件实现，防护设备中的单元是程序模块。在另一些实施例中，防护设备中的单元通过硬件或固件实现。第二方面提供的防护设备的具体细节可参见上述第一方面或第一方面任一种可选方式，此处不再赘述。

第三方面，提供了一种防护设备，该防护设备包括处理器和通信接口，该处理器用于执行指令，使得该防护设备执行上述第一方面或第一方面任一种可选方式所提供的方法，所述通信接口用于接收或发送报文。第三方面提供的防护设备的具体细节可参见上述第一方面或第一方面任一种可选方式，此处不再赘述。

第四方面，提供了一种计算机可读存储介质，该存储介质中存储有至少一条指令，该指令由处理器读取以使防护设备执行上述第一方面或第一方面任一种可选方式所提供的方法。

第五方面，提供了一种计算机程序产品，该计算机程序产品包括一个或多个计算机指令，当所述计算机程序指令被计算机加载并执行时，使得所述计算机执行上述第一方面或第一方面任一种可选方式所提供的方法。

第六方面，提供了一种芯片，当该芯片在防护设备上运行时，使得防护设备执行上述第一方面或第一方面任一种可选方式所提供的方法。

第七方面，提供了一种网络系统，该网络系统包括防护设备、客户端设备以及服务器，该防护设备用于执行上述第一方面或第一方面任一种可选方式所述的方法。

附图说明

图 1 是本申请实施例提供的一种流模式下报文交互的流程图；

图 2 是本申请实施例提供的一种代理模式下报文交互的流程图；

图 3 是本申请实施例提供的一种典型应用场景的示意图；
图 4 是本申请实施例提供的一种防护设备的结构示意图；
图 5 是本申请实施例提供的一种网络安全防护方法的流程图；
图 6 是本申请实施例提供的一种客户端与服务器之间三次握手的流程图；
图 7 是本申请实施例提供的一种防护设备在三次握手阶段的处理流程图；
图 8 是本申请实施例提供的一种防护设备的系统架构图；
图 9 是本申请实施例提供的一种防护设备的系统架构图；
图 10 是本申请实施例提供的一种防护设备的结构示意图。

具体实施方式

为使本申请的目的、技术方案和优点更加清楚，下面将结合附图对本申请实施方式作进一步地详细描述。

最早的防火墙，是在传统的路由器的基础上，增加访问控制列表（access control lists，ACL）对转发的数据包进行过滤实现的，称为包过滤防火墙。包过滤的基本原理是，对需要转发的数据包，防火墙先获取数据包的包头信息。包头信息例如互联网协议（internet protocol，IP）地址、源端口、目的端口等网络层信息。然后，防火墙用包头信息和设定的规则（ACL 中的表项）进行比较，防火墙根据比较的结果对数据包进行转发或者丢弃。

流模式（flow mode）在上述包过滤方式的基础上进一步结合了会话状态信息。参见附图 1，附图 1 示出了流模式下报文交互的流程。在流模式下，防火墙对客户端和服务器发出的原始报文进行包过滤匹配，决定是丢弃报文还是转发报文。在流模式下，防火墙虽然会维护会话状态信息，但很少对报文进行修改，也很少主动生成报文发送给客户端和服务器。报文传输的可靠性，依赖客户端和服务器自身部署的传输控制协议（transmission control protocol，TCP）/IP 协议栈保证。比如，客户端发送的数据报文，经过防火墙检测后，如果在发送给服务器的过程中意外丢失，则依赖客户端上 TCP 协议的重传机制，由客户端负责重新发送丢失的报文。

随着网络、应用的复杂性增长，简单的网络层信息检查的包过滤技术已经不能满足安全防范的需要。以 AV 检测场景为例，防病毒功能要求获得完整传输的文件，才能检测出一些高级的病毒。而 TCP 传输机制要求，在客户端发送一定的数据后（部分文件），需要服务器产生应答，客户端收到应答之后才会继续发送后续数据。而服务器只有收到来自客户端的数据，服务器才会进行应答。因此，防火墙采用流模式时，只能将数据报文发送出去。服务器收到防火墙发来的数据报文并产生应答后，客户端才会发送后续数据报文。等到数据报文发送完，防火墙才能开始对提取的文件（防火墙进行缓存拷贝）进行病毒检查。此时，即使防火墙发现有病毒，也不能进行阻断。因为，几乎所有数据报文已经发送到服务器，病毒的实际有效部分已经发送，攻击已经形成，显然对服务器的防护效果不佳。为了实现阻断病毒的目的，一些研究引入了代理模式（proxy mode）。

参见附图 2，附图 2 示出了代理模式下报文交互的流程。代理模式下，防火墙扮演模拟服务器的角色，由防火墙代替服务器和客户端进行交互。并且，防火墙扮演模拟客户端的角色，由防火墙代替客户端和服务器交互。例如，在病毒检测场景中，防火墙代替服务器发送确认（acknowledgement，ACK）报文给客户端，使客户端在确认报文的触发下继续发送后续

数据报文。在防火墙和客户端交互数据报文的过程中，数据报文并没有被发送给服务器；等到防火墙从客户端获得所有的数据报文，从而获得完整的文件内容，防火墙开始进行病毒检查。如果防火墙发现病毒，则防火墙将含病毒文件完整删除，确保病毒不会发送到服务器；或者，防火墙不删除附件，而是通过增加提示信息的方式告知用户，附件存在病毒；对于没有发现病毒的文件，则由防火墙代替客户端发送给服务器。

从代理模式的原理可见，由于代理模式下防火墙通过主动向数据报文的源端（如客户端）回复确认报文，使得源端在确认报文的触发下继续发送后续的数据报文，因此，防火墙能够收到更多的数据报文，从而获得更多的数据进行检测。显然，代理模式有助于检测出复杂的网络攻击，提高安全检测的精确性。此外，由于代理模式下，防火墙对完整的文件内容检测，确认文件安全后，才会将文件转发给数据报文的目的端（如服务器），避免虽然检测出文件包含病毒、但包含病毒的文件已经被转发给目的端的情况，显然更能阻断病毒的传播，提升安全防护的有效性。

在代理模式下，防护设备需要对大量数据报文进行缓存重组、以及支持完整的协议栈，因此需要消耗大量资源。由于硬件资源限制、性能等方面的考虑，防火墙难以对所有会话都默认采用代理模式处理。考虑到实际应用场景下现网流量的复杂性（非标准端口）以及用户配置的灵活性（基于应用层的配置），防火墙根据首个会话中的 SYN 报文无法判定是否需要采用代理模式，而是需要在进行一定数据报文交互后，才能确定是否需要使用代理模式处理。因此以防火墙为例的防护设备会采用流模式对首个会话中的报文进行协议识别，根据识别结果判断是否需要采用代理模式。如果需要采用代理模式进行检测，则服务器根据 SYN 报文记录服务器的 IP 地址、端口号等以形成识别表。当该客户端后续尝试与该服务器的同一端口号再次建立会话时，如果服务器的 IP 地址、端口号存在于识别表中，则防护设备再采用代理模式对后续建立的会话中的报文进行检测。

在研究过程中发现，采用上述方案存在诸多缺陷。由于首个会话中的流（如服务器向客户端传输的首条流以及客户端向服务器传输的首条流）没有采用代理模式处理，对于依赖代理模式检测的复杂业务，如加密套接字（security socket layer，SSL）解密等特性，如果首个会话中的流（如服务器向客户端传输的首条流以及客户端向服务器传输的首条流）中存在攻击行为，防火墙将无法检测出攻击行为，从而导致攻击漏过，严重影响网络安全性。

有鉴于此，本申请实施例提供了能够快速切换至代理模式的方案。防火墙或者其他防护设备通过实施本技术方案，能够根据应用层对安全检测的需求，采用代理模式检测首条流，从而突破首条流只能采用流模式检测的技术瓶颈，避免首条流局限于流模式造成攻击漏检。

相对于首条流默认采用流模式的方案而言，本技术方案能确保所有流量，即使是非标准端口的首条流，也获得充分的安全检测，不漏过威胁，充分提升安全防护效果。相对于默认采用代理模式的方案而言，本技术方案极大减少了代理类会话的数量，降低了设备的资源消耗，提升了设备的整体处理能力。

下面，从系统运行环境、硬件装置、软件装置、方法流程等多个角度，对本技术方案进行详细介绍。

以下结合附图 3 介绍本申请实施例提供的系统运行环境。

请参考图 3，图 3 是本申请实施例提供的一种典型应用场景 10 的示意图。应用场景 10

包括客户端设备 11、服务器 12 以及防护设备 13。下面对客户端设备 11、服务器 12 以及防护设备 13 分别进行描述。

（1）客户端设备 11

客户端设备 11 为 TCP 会话中发起访问的设备。客户端设备 11 包括但不限于个人计算机、移动电话、服务器 12、笔记本电脑、IP 电话、摄像头、平板电脑、可穿戴设备等。例如，客户端设备 11 为企业内部员工的办公设备。

在一些实施例中，客户端设备 11 安装了邮箱客户端、文件传输客户端等应用程序，客户端设备 11 通过应用程序产生应用层数据，基于应用层协议与服务器 12 交互应用层数据，从而触发下述方法实施例。在一个示例性场景中，客户端设备 11 在运行邮箱客户端的过程中，基于 SMTP 协议与服务器 12 传输邮件。在另一个示例性场景中，客户端设备 11 在运行文件传输客户端的过程中，基于文件传输协议（file transfer protocol，FTP）协议与服务器 12 传输文件。

在一些实施例中，系统架构 10 中包含大量客户端设备 11，为了简明起见，图 3 以一个客户端设备 11 的情况为例进行说明。

（2）服务器 12

服务器 12 为 TCP 会话中提供服务的设备。例如，服务器 12 为邮件服务器 12，邮件服务器 12 基于 SMTP 协议为客户端提供邮件传输服务。又如，服务器 12 为文件服务器 12，文件服务器 12 基于 FTP 协议为客户端提供文件传输服务。又如，服务器 12 为网站服务器。

上述客户端设备 11 和服务器 12 之间的文件传输可能是双向的，既可能是客户端设备 11 向服务器 12 发送文件，也可能是服务器 12 向客户端设备 11 发送文件。

（3）防护设备 13

防护设备 13 部署于客户端设备 11 与服务器 12 之间。防护设备 13 与客户端设备 11 与服务器 12 分别通过网络相连。防护设备 13 用于对网络中传输的报文进行安全检测，安全检测包括而不限于 IPS 检测、AV 检测等。防护设备 13 包括而不限于防火墙、入侵检测系统（intrusion detection system，IDS）类设备、IPS 类设备。防护设备 13 例如为网络中直路部署的网络检测设备。

防护设备 13 支持的多种检测模式构成了检测模式集合。检测模式集合包括至少一种检测模式。例如，检测模式集合中包括包过滤模式、流模式或代理模式等等。

以下，以防护设备 13 支持的检测模式集合包括流模式以及代理模式为例，对防护设备 13 内部的逻辑功能架构进行介绍。

请参考附图 3，防护设备 13 包括上层业务模块 130、流模式处理模块 131、代理模式处理模块 132 以及 TCP/IP 协议栈模块 133。

（a）上层业务模块 130

上层业务模块 130 例如通过防护设备 13 的应用程序实现。上层业务模块 130 用于处理应用层的业务。在本申请的一些实施例中，上层业务模块 130 用于根据应用层数据进行协议识别，以便根据识别出的协议类型确定采用哪种检测模式检测报文。

（b）流模式处理模块 131

流模式处理模块 131 负责流模式下对 TCP 会话中报文的处理任务。例如，流模式处理模

块 131 用于在流模式下接收来自客户端设备 11 或者服务器 12 的数据报文、缓存收到的数据报文、向客户端设备 11 或者服务器 12 转发数据报文、接收来自客户端设备 11 或者服务器 12 的确认报文、向客户端设备 11 或者服务器 12 转发确认报文。流模式处理模块 131 内部的具体构成可参考附图 8 相关的介绍。

（c）代理模式处理模块 132

代理模式处理模块 132 负责代理模式下对 TCP 会话中报文的处理任务。在一些实施例中，代理模式处理模块 132 和 TCP/IP 协议栈模块 133 分离设置。图 3 以代理模式处理模块 132 与 TCP/IP 协议栈模块 133 分离设置为例进行说明。在另一些实施例中，代理模式处理模块 132 和 TCP/IP 协议栈模块 133 集成为同一个模块。

（d）TCP/IP 协议栈模块 133

TCP/IP 协议栈模块 133 用于基于 TCP/IP 协议传输报文，从而确保报文的传输可靠性。TCP/IP 协议栈模块 133 内部的具体构成可参考附图 8 或附图 9 相关的介绍。在一些实施例中，TCP/IP 协议栈模块 133 采用软件实现。在另一些实施例中，TCP/IP 协议栈模块 133 采用硬件实现，或者采用软件硬件相结合的方式实现。例如，防护设备 13 配置有加速器，加速器为专用于处理 TCP/IP 协议栈相关处理步骤的硬件，TCP/IP 协议栈模块 133 通过加速器实现，从而将 TCP/IP 协议栈卸载至加速器上，减少中央处理器（central processing unit，CPU）的负载。

TCP/IP 协议栈模块 133 确保传输可靠性主要通过回复确认以及重传机制实现。具体地，TCP/IP 协议栈模块 133 在接收数据报文后，TCP/IP 协议栈模块 133 会向数据报文的源端返回确认报文。TCP/IP 协议栈模块 133 在发送数据报文后，如果数据报文满足重传条件，TCP/IP 协议栈模块 133 会向数据报文的目的端重新发送数据报文。

在一些实施例中，重传条件包括未接收到针对数据报文的确认报文。比如，TCP/IP 协议栈模块 133 将数据报文发送给对端后，如果超过预设时长未收到数据报文对应的确认报文，则满足重传条件，TCP/IP 协议栈模块 133 会自动重传数据报文。

在另一些实施例中，重传条件包括根据对端（客户端设备 11 或者服务器 12）发来的确认报文中选择性确认（selective acknowledgement，SACK）选项中的信息，确定数据报文发生丢包。这种重传条件适用于 TCP/IP 协议栈模块 133 支持 SACK 选项的情况。具体地，TCP/IP 协议栈模块 133 向对端发出数据报文后，TCP/IP 协议栈模块 133 接收来自对端的确认报文，TCP/IP 协议栈模块 133 根据确认报文中 SACK 选项中的范围以及记录的最大序列号（sequence number，Seq）号，确定数据报文丢失，则 TCP/IP 协议栈模块 133 重传数据报文。例如，防护设备 13 发送了 Seq 号分别为 1，2，3，4 的四个报文。由于网络原因造成 Seq 号为 1 的报文丢包，Seq 号分别为 2，3，4 的三个报文成功传输到对端。当对端收到 Seq 号分别为 2，3，4 的三个报文时，对端在确认报文中通过 SACK 选项通知防护设备 13，Seq 号分别为 2，3，4 的三个报文都收到了，只有 Seq 号为 1 的报文没收到，则 Seq 号为 1 的报文满足重传条件，防护设备 13 重传 Seq 号为 1 的报文。

附图 4 是本申请实施例提供的防护设备的结构示意图。可选地，具有附图 4 所示结构的防护设备是附图 3、附图 8 或附图 9 中的防护设备 13。

防护设备 200 包括至少一个处理器 201、通信总线 202、存储器 203 以及至少一个通信接口 204。

处理器 201 例如是通用中央处理器（central processing unit，CPU）、网络处理器（network processer，NP）、图形处理器（graphics processing unit，GPU）、神经网络处理器（neural-network processing units，NPU）、数据处理单元（data processing unit，DPU）、微处理器或者一个或多个用于实现本申请方案的集成电路。例如，处理器 201 包括专用集成电路（application-specific integrated circuit，ASIC），可编程逻辑器件（programmable logic device，PLD）或其组合。PLD 例如是复杂可编程逻辑器件（complex programmable logic device，CPLD）、现场可编程逻辑门阵列（field-programmable gate array，FPGA）、通用阵列逻辑（generic array logic，GAL）或其任意组合。

在一些实施例中，处理器 201 用于支持防护设备 200 执行附图 5 所示方法 500 中 S520、S530 以及 S540。在一些实施例中，处理器 201 还用于支持防护设备 200 执行附图 7 所示方法 700 中 S720 以及 S750。

通信总线 202 用于在上述组件之间传送信息。通信总线 202 可以分为地址总线、数据总线、控制总线等。为便于表示，附图 4 中仅用一条粗线表示，但并不表示仅有一根总线或一种类型的总线。

存储器 203 例如是只读存储器（read-only memory，ROM）或可存储静态信息和指令的其它类型的静态存储设备，又如是随机存取存储器（random access memory，RAM）或者可存储信息和指令的其它类型的动态存储设备，又如是电可擦可编程只读存储器（electrically erasable programmable read-only memory，EEPROM）、只读光盘（compact disc read-only memory，CD-ROM）或其它光盘存储、光碟存储（包括压缩光碟、激光碟、光碟、数字通用光碟、蓝光光碟等）、磁盘存储介质或者其它磁存储设备，或者是能够用于携带或存储具有指令或数据结构形式的期望的程序代码并能够由计算机存取的任何其它介质，但不限于此。存储器 203 例如是独立存在，并通过通信总线 202 与处理器 201 相连接。存储器 203 也可以和处理器 201 集成在一起。

在一些实施例中，存储器 203 用于支持防护设备 200 缓存收到的报文、缓存已发送的报文。例如，结合附图 8 或附图 9 来看，存储器 203 包括接收报文队列 13111、接收报文队列 13121、发送报文队列 13312 或者发送报文队列 13322 中的至少一项。

通信接口 204 使用任何收发器一类的装置，用于与其它设备或通信网络通信。例如，结合附图 3 所示的部署场景来看，通信接口 204 用于与客户端设备 11 或者服务器 12 通信。通信接口 204 包括有线通信接口，还可以包括无线通信接口。其中，有线通信接口例如可以为以太网接口。以太网接口可以是光接口，电接口或其组合。无线通信接口可以为无线局域网（wireless local area networks，WLAN）接口，蜂窝网络通信接口或其组合等。

在一些实施例中，通信接口 204 用于支持防护设备 200 执行附图 5 所示方法 500 中 S510。在一些实施例中，通信接口 204 还用于支持防护设备 200 执行附图 7 所示方法 700 中 S730 以及 S780。

在具体实现中，作为一种实施例，处理器 201 可以包括一个或多个 CPU，如附图 4 中所示的 CPU0 和 CPU1。

在具体实现中，作为一种实施例，防护设备 200 可以包括多个处理器，如附图 4 中所示的处理器 201 和处理器 205。这些处理器中的每一个可以是一个单核处理器（single-CPU），也可以是一个多核处理器（multi-CPU）。这里的处理器可以指一个或多个设备、电路、和/或

用于处理数据（如计算机程序指令）的处理核。

在具体实现中，作为一种实施例，防护设备 200 还可以包括输出设备和输入设备。输出设备和处理器 201 通信，可以以多种方式来显示信息。例如，输出设备可以是液晶显示器（liquid crystal display，LCD）、发光二级管（light emitting diode，LED）显示设备、阴极射线管（cathode ray tube，CRT）显示设备或投影仪（projector）等。输入设备和处理器 201 通信，可以以多种方式接收用户的输入。例如，输入设备可以是鼠标、键盘、触摸屏设备或传感设备等。

在一些实施例中，存储器 203 用于存储执行本申请方案的程序代码 210，处理器 201 可以执行存储器 203 中存储的程序代码 210。也即是，防护设备 200 可以通过处理器 201 以及存储器 203 中的程序代码 210，来实现附图 5 所示方法 500 或附图 7 所示方法 700。

本申请实施例的防护设备 200 可对应于附图 5 所示方法 500 或附图 7 所示方法 700 中的防护设备，并且，该防护设备 200 中的处理器 201、通信接口 204 等可以实现附图 5 所示方法 500 或附图 7 所示方法 700 中的防护设备所具有的功能和/或所实施的各种步骤和方法。为了简洁，在此不再赘述。

下面结合附图 5 对本申请实施例提供的网络安全防护方法进行介绍。

附图 5 是本申请实施例提供的网络安全防护方法 500 的流程图。方法 500 包括步骤 S510 至步骤 S540。

可选地，方法 500 中涉及的客户端设备、服务器以及防护设备的网络部署场景如附图 3 所示。方法 500 中涉及的客户端设备为附图 3 中的客户端设备 11，方法 500 中服务器为系统架构 10 中的服务器 12，方法 500 中防护设备为附图 3 中的防护设备 13。

可选地，方法 500 中防护设备具备附图 4 所示的结构。

步骤 S510、防护设备获取客户端与服务器之间首个 TCP 会话中的第一数据报文。

首个会话为客户端与服务器之间建立的第一个会话。在一些实施例中，首个会话为预定时间段内客户端与服务器之间建立的第一个会话。其中，预定时间段的起始时间点为防火墙的上线时间点。在一些实施例中，首个会话是指防护设备上线后经过防护设备访问特定服务器上特定服务的第一个会话。首条流是指首个会话的报文流。例如，首条流为首个会话中客户端向服务器发送的流，又如，首条流为首个会话中服务器向客户端发送的流。在一个示例性场景中，防火墙开机后，第一次经过防火墙访问 IP 地址为 10.10.10.10、端口 80 的流为首条流；第一次经过防火墙访问 IP 地址为 10.10.10.10、端口 8080 的流为首条流；第一次经过防火墙访问 IP 地址为 20.20.20.20、端口 80 的流为首条流。

本实施例中为了区分不同的数据报文，用“第一数据报文”、“第二数据报文”描述不同的数据报文。

第一数据报文是防护设备在第一模式下接收并缓存的报文。第一数据报文包括客户端设备与服务器之间交互的内容。在一些实施例中，第一数据报文的源设备是客户端设备，第一数据报文的目的设备是服务器。例如，第一数据报文是客户端设备根据来自于服务器的数据报文生成的报文，第一数据报文包括客户端设备需要反馈给服务器的应答内容。在另一些实施例中，第一数据报文的源设备是服务器，第一数据报文的目的设备是客户端设备。例如，第一数据报文是服务器根据来自于客户端设备的数据报文生成的报文，第一数据报文包括服务器需要反馈给客户端设备的应答内容。

步骤 S520、防护设备根据第一数据报文的应用层数据，识别第一数据报文的应用层协议类型。

应用层协议为客户端设备上的应用与服务器上的应用相互传递报文时使用的协议。应用层协议的类型包括很多种。例如，应用层协议为电子邮件传输协议。比如说，应用层协议为 SMTP 协议、邮局协议版本 3（post office protocol 3，POP3）、交互式数据消息访问协议第四个版本（internet message access protocol 4，IMAP4）协议等。又如，应用层协议为文件传输协议。比如说，应用层协议为 FTP 协议。当然，应用层协议可选地为隶属于 TCP/IP 协议簇的其他协议，本实施例对应用层协议的具体类型不做限定。

在一些实施例中，防护设备根据应用层数据以及应用层协议对应的关键字，识别应用层协议类型。

应用层协议对应的关键字例如为应用层协议规定的数据报文所需包含的关键字。应用层协议对应的关键字例如通过应用层协议相关的标准或草案指定。在一些实施例中，应用层协议对应的关键字为应用层协议中登录命令携带的关键字。登录命令用于请求登录至服务器。下面，结合 SMTP 协议以及 FTP 协议这两类协议，对关键字以及利用关键字识别应用层协议类型的方式举例说明。

例如，应用层协议为 SMTP 协议，SMTP 协议中登录命令包括 HELO（hello，问候）命令。SMTP 协议对应的关键字例如为 HELO 命令携带的关键字。HELO 命令携带的关键字为 HELO。其中，HELO 命令的格式可简化表示为“HELO xxxx”。“HELO xxxx”中“xxxx”是 HELO 命令包含的参数，该参数的含义通常是 SMTP 客户端的域名。那么，如果防护设备收到的应用层数据包括 HELO，防护设备即可识别出应用层协议的类型是 SMTP 协议。当然，HELO 命令仅是对 SMTP 协议中登录命令的举例说明，HELO 仅是对 SMTP 协议对应的关键字的举例说明，HELO 命令可替代为 SMTP 协议中其他登录命令，如 EHLO（extended hello）命令等，SMTP 协议对应的关键字可替代为其他登录命令中的关键字，本实施例对识别 SMTP 协议时采用的关键字不做限定。

又如，应用层协议为 FTP 协议，FTP 协议中登录命令包括 USER 命令。FTP 协议对应的关键字例如为 USER 命令携带的关键字。具体地，USER 命令携带的关键字为 USER。USER 命令可简化表示为“USER xxx”。“USER xxx”中“xxxx”是 USER 命令包含的参数，该参数的含义通常是用户名。那么，如果防护设备收到的应用层数据包括 USER，防护设备即可识别出应用层协议的类型是 FTP 协议。当然，USER 命令仅是对 FTP 协议中登录命令的举例说明，USER 仅是对 FTP 协议对应的关键字的举例说明，USER 命令可替代为 FTP 协议中其他登录命令，如 pass 命令、pavs 命令等，FTP 协议对应的关键字可替代为其他登录命令中的关键字，如 pass、pavs 等，本实施例对识别 FTP 协议时采用的关键字不做限定。

步骤 S530、防护设备确定应用层协议类型对应的检测模式为代理模式。

在一些实施例中，防护设备保存应用层协议类型与检测模式之间的对应关系。防护设备根据应用层协议类型与检测模式之间的对应关系，确定第一数据报文的应用层协议类型对应的检测模式为代理模式。

例如，应用层协议类型与检测模式之间的对应关系包括 SMTP 协议与代理模式之间的对应关系。防护设备识别出应用层协议类型为 SMTP 协议后，防护设备根据 SMTP 协议与代理

模式之间的对应关系，确定第一数据报文的应用层协议类型对应代理模式，则防护设备切换为代理模式，采用代理模式对首个 TCP 会话中基于 SMTP 协议传输的邮件进行防病毒检测。

又如，应用层协议类型与检测模式之间的对应关系包括 FTP 协议与流模式之间的对应关系。防护设备识别出应用层协议类型为 FTP 协议后，防护设备根据 FTP 协议与流模式之间的对应关系，确定第一数据报文的应用层协议类型对应流模式，则防护设备继续使用流模式对首个 TCP 会话后续报文进行安全检测。

步骤 S540、防护设备采用代理模式对首个 TCP 会话中的后续报文进行安全检测。

本实施例提供的方法，在客户端与服务器之间交互首个会话的报文时，防护设备通过根据首个会话的报文中的应用层数据，识别应用层协议类型。如果根据应用层协议类型确定检测模式为代理模式，则防护设备采用代理模式对首个 TCP 会话的后续报文进行安全检测。从而能够在首个 TCP 会话处理过程中快速切换至代理模式，突破了首个 TCP 会话的报文只能采用流模式检测的技术瓶颈，保证首个 TCP 会话的报文也能通过代理模式检测，避免首个 TCP 会话的报文局限于流模式造成攻击漏检，因此提升了防护效果。

下面通过实例一和实例二这两个实例，对步骤 S520 中防护设备如何利用协议对应的关键字识别协议类型举例说明。

实例一、客户端与服务器基于 SMTP 协议交互。

客户端设备与服务器建立首个 TCP 会话后，服务器向客户端设备发送欢迎信息。防护设备接收到来自于服务器的欢迎信息后，防护设备将欢迎信息转发到客户端设备。客户端设备收到欢迎信息后，发送的应用层数据包括“HELO xxxx”。防护设备收到应用层数据之后，发现应用层数据包括“HELO”，则识别出首个 TCP 会话运行了 SMTP 协议。

例如，客户端发送的应用层数据如以下所示。

220 dshnayder. fscinternet. com ESMTP postfix
HELO localhost
MAIL FROM: <test>
RCPT TO: <test@dshnayder. fscinternet. com>
data
From: "test" <ttest>
To: <test@dshnayder. fscinternet. com>
Subject: open object tag-exploit. html
Content-Type: text/html; charset="iso-8859-1

其中，“220 dshnayder. fscinternet. com ESMTP postfix”为欢迎信息，“HELO localhost”为 HELO 命令。

实例二、客户端与服务器基于 FTP 协议交互。

客户端设备与服务器建立首个 TCP 会话后，服务器向客户端设备发送欢迎信息。防护设备接收到来自于服务器的欢迎信息后，防护设备将欢迎信息转发到客户端设备。客户端设备收到欢迎信息后，发送的应用层数据包括“USER xxx”。防护设备收到应用层数据之后，发现应用层数据包括“USER”，则识别出首个 TCP 会话运行了 FTP 协议。

例如，客户端发送的应用层数据如以下所示。

220 redhat_52. test FTP server （Version wu-2.4.2-academ[BETA-18]（1）Mon Aug 3 19: 17: 20 EDT 1998）ready.

USER anonymous

331 Guest login ok，send your complete e-mail address as password.

PASS hi@blahblah. net

230 Guest login ok，access restrictions apply.

MKD /incoming

550 /incoming: Permission denied.

CND /incoming

250 CWD command successful.

其中，“220 redhat_52. test FTP server （Version wu-2.4.2-academ[BETA-18]（1）Mon Aug 3 19: 17: 20 EDT 1998）ready”为欢迎信息，“USER anonymous”为 USER 命令。这一 USER 命令表示匿名登录 FTP 服务器。

以上实例一和实例二以 SMTP 协议、FTP 协议这两种应用层协议为例进行说明。本实施例的应用范围并不仅限于这几种协议。本实施例能够应用于各种基于协议类型、应用层数据等需要若干报文交互后才能确定是否需要采用代理模式检测的流量的处理场景。

防护设备如何获得应用层协议类型与检测模式之间的对应关系包括多种实现方式。在一些实施例中，防护设备根据用户的配置操作，确定应用层协议类型与检测模式之间的对应关系。例如，用户配置了对基于 SMTP 协议传输的流量进行 AV 检测。由于 AV 检测通常情况下要求使用代理模式，则防护设备确定 SMTP 协议与代理模式对应。

在一些实施例中，防护设备在检测首个会话中的流量的过程中，用户对配置进行修改，使得应用层协议类型与检测模式之间的对应关系发生更新。在这一场景下，防护设备根据更新后的应用层协议类型与检测模式之间的对应关系，确定首个会话的应用层协议类型对应的检测模式为代理模式，则防护设备针对首个会话切换为代理模式，从而实现用户配置的实时生效，保障首条流及时地采用代理模式检测。例如，用户通过对配置进行修改，将原来配置为使用流模式检测的流量修改为需要使用代理模式检测。防护设备在检测首个会话的报文的过程中，当检测到配置修改后，将针对首个会话的报文的检测模式切换为代理模式。

在一些实施例中，防护设备针对首个会话从流模式切换至代理模式之后，防护设备还针对首个会话从代理模式切换回流模式，从而在首个 TCP 会话中多次切换检测模式。例如，按照时间先后顺序的角度描述，在首个 TCP 会话建立之后，防护设备首先采用流模式检测首个 TCP 会话中的数据报文。之后，防护设备通过执行步骤 S510 至步骤 S530，从流模式切换为代理模式，采用代理模式检测首个 TCP 会话中后续的数据报文。之后，防护设备在一些场景下从代理模式重新切换为流模式，采用流模式检测首个 TCP 会话中后续的数据报文，直至首个 TCP 会话结束。下面，针对首个会话采用流模式→代理模式→流模式的一些实现方式进行举例说明，具体参见以下实现方式一和实现方式二。

实现方式一、防护设备根据 AV 检测结果，确定从代理模式重新切换回流模式。

例如，防护设备在采用代理模式对首个 TCP 会话中的报文进行安全检测的过程中，防护设备接收到了第四数据报文。防护设备采用代理模式对第四数据报文的应用层数据进行 AV

检测，从而得到 AV 检测结果。如果 AV 检测结果为不包含病毒，防护设备切换为流模式，并采用流模式针对首个 TCP 会话中第四数据报文之后传输的后续报文继续进行安全检测。其中，第四数据报文为首个 TCP 会话中在第一数据报文之后传输的报文。例如，在客户端与服务器首个会话中基于 SMTP 协议交互的场景下，防护设备在转发客户端与服务器之间的邮件时，防护设备采用代理模式对邮件的内容（包含邮件附件）进行 AV 检测，如果邮件的 AV 检测结果为邮件不包含病毒，或者说邮件是安全的，则防护设备从代理模式切换为流模式。

实现方式二、防护设备通过识别出客户端和服务器要开始加密通信，确定从代理模式重新切换回流模式。

例如，防护设备在采用代理模式对首个 TCP 会话中的报文进行检测的过程中，防护设备接收到了第五数据报文。防护设备采用代理模式对第五数据报文进行安全检测。如果第五数据报文的应用层数据指示客户端设备与服务器将要在 TCP 会话中进行加密通信，防护设备切换为流模式，并采用流模式针对首个 TCP 会话中第五数据报文之后传输的后续报文继续进行安全检测。其中，第五数据报文为首个 TCP 会话中在第一数据报文之后传输的报文。在一些实施例中，防护设备预先保存加密通信命令的关键字，如果第五数据报文的应用层数据包括加密通信命令的关键字，则确定客户端设备与服务器将要加密通信。其中，加密通信命令例如为 starttls 命令。

在一个示例性应用场景中，防护设备采用上述方法 500 对基于 SMTP 协议的邮件进行安全检测，服务器具体为邮箱服务器，客户端设备安装有 SMTP 客户端。在 SMTP 客户端与邮箱服务器建立会话后，防护设备首先采用流模式检测会话中的数据报文。之后，在 SMTP 客户端与邮箱服务器在会话中交互的过程中，防护设备通过 SMTP 客户端与邮箱服务器之间交互的数据报文，发现会话对应的应用层协议是 SMTP 协议，则防护设备从流模式切换为代理模式。防护设备采用代理模式检测 SMTP 客户端与邮箱服务器在会话中后续交互的数据报文。具体地，SMTP 客户端发送的邮件数据，均由防护设备进行 ACK，使得 SMTP 客户端将整个邮件（包括附件）完整发送到防护设备上。防护设备对邮件数据进行防病毒检测，防护设备确认邮件数据不包括病毒，则通过自身 TCP/IP 协议栈代替 SMTP 客户端将邮件数据发送给服务器。防护设备通过在代理模式下进行一次或多次检测，确定 SMTP 客户端与服务器之间传输的邮件安全，则防护设备再从代理模式切换为流模式，从而加速后续的处理流程。

以上提供的方法中，防护设备通过基于数据报文交互结果，在首个会话中的数据报文交互阶段进行不同检测模式之间的自适应切换，能够实现按需进行模式选择，避免单一采用流模式造成威胁漏过，并避免单一采用代理模式造成大量不必要的资源占用，因此提升了防护效果。

下面介绍防护设备在三次握手阶段的处理流程。

为了便于理解，下面先对 TCP 协议中三次握手的原理进行介绍。

参见附图 6，附图 6 是客户端与服务器之间三次握手的流程图。在附图 6 所示的流程中，客户端为 TCP 会话的发起方，服务器为 TCP 会话的接受方。客户端与服务器的交互主要包括会话建立、数据传输以及会话关闭这三个阶段。附图 6 未示出数据传输的具体流程。

会话建立是通过三次握手（three-way handshake）实现的。当客户端与服务器需要使用 TCP 协议传输数据时，客户端使用 SYN 报文发起 TCP 会话来建立协商，称为三次握手。三

次握手涉及 SYN 报文、同步序列编号确认（synchronize sequence numbers acknowledgement，SYN ACK）报文以及 ACK 报文这三种报文的交互过程。具体地，三次握手包括以下步骤一至步骤三。

步骤一、客户端向服务器发送 SYN 报文。SYN 报文包括建立 TCP 会话需要用到的选项。选项例如为最大报文段长度（maximum segment size，MSS）、SACK、数据缓冲区大小（TCP 窗口）等。

其中，SYN 报文中的 Seq 号为客户端初始序列号（inital sequence number，ISN）。SYN 报文中的 ISN 为客户端随机产生的一个值。SYN 报文中的 ISN 可简化表示为 ISN（c）。ISN（c）中“c”的含义是客户端（client）。

步骤二、服务器接收 SYN 报文，服务器向客户端发送 SYN ACK 报文。SYN ACK 报文包括服务器支持的选项。服务器通过发送 SYN ACK 报文，从而通知客户端已经收到了客户端的 SYN 报文，并将支持的选项告诉给客户端。

其中，SYN ACK 报文中的 Seq 号为 ISN。SYN ACK 报文中的 ISN 为服务器随机产生的一个值。SYN ACK 报文中的 ISN 可简化表示为 ISN(s)。ISN(c)中“s”的含义是服务器(server)。SYN ACK 报文中的 ACK 号为 ISN（c）+1。

步骤三、客户端接收 SYN ACK 报文，客户端向服务器发送 ACK 报文，从而完成三次握手。其中，ACK 报文中的 Seq 号为 ISN（c）+1。ACK 报文中的 ACK 号为 ISN（s）+1。

当客户端与服务器握手完成后，客户端与服务器在数据传输阶段交互数据报文时，客户端与服务器会使用握手协商出的报文序列号（Seq）、MSS，按序分段发送数据。其中，客户端与服务器每次发送的数据量的最大值为对方通告的窗口大小。接收方通过 ACK 报文确认收到的数据报文，同时更新自己可以接收到的最大数据长度。此外，TCP 协议还需要使用一系列定时器、拥塞算法，来处理网络中的异常丢包，以及发送过快造成的丢包。

以上介绍了三次握手的基本原理。可选地，由于版本限制或者性能限制等因素，在有些情况下防护设备的协议栈可能只能支持部分选项，而不能支持所有选项。如果客户端设备和服务器恰好使用防护设备协议栈不支持的选项进行会话协商，则可能会造成防护设备采用代理模式进行检测时出现检测失败。在这种情况下，本申请实施例提供了一种改进的报文处理方式，防护设备在三次握手阶段对交互报文进行处理，从而避免因协议栈不支持因素引入的检测故障。下面对本申请实施例提供的防护设备在三次握手阶段的处理流程进行介绍。

防护设备在三次握手阶段的处理流程包括以下步骤 S501 至步骤 S503。

以下介绍的步骤 S501 至步骤 S503，和上述步骤 S510 至步骤 S540 之间的关系是，步骤 S501 至步骤 S503、步骤 S510 至步骤 S540 分别针对同一个 TCP 会话的不同阶段。步骤 S501 至步骤 S503 应用在触发 TCP 会话建立的三次握手阶段。步骤 S510 至步骤 S540 应用在 TCP 会话建立之后的数据传输阶段。从时间先后顺序的角度而言，防护设备先在三次握手阶段执行步骤 S501 至步骤 S503。当 TCP 会话建立，客户端设备与服务器交互数据报文的过程中，防护设备执行上述步骤 S510 至步骤 S540。

步骤 S501、防护设备获取客户端设备与服务器之间传输的第一握手报文。

第一握手报文用于创建 TCP 会话。第一握手报文为 TCP 协议中的三次握手报文。具体地，第一握手报文为 SYN 报文或者 SYN ACK 报文中的至少一种。第一握手报文包括 TCP

头，TCP 头包括长度可变的选项（option）字段。选项字段的内容为选项的具体信息。选项包括而不限于 SACK 选项、MSS 选项、窗口扩大选项、时间戳选项等。

在第一握手报文为 SYN 报文的情况下，第一握手报文的源设备为客户端设备。步骤 S501 包括：防护设备接收来自于客户端设备的 SYN 报文。

在第一握手报文为 SYN ACK 报文的情况下，第一握手报文的源设备为服务器。步骤 S501 包括：防护设备接收来自于服务器的 SYN ACK 报文。

步骤 S502、防护设备从第一握手报文删除第二选项，从而得到第二握手报文。

以第一握手报文包括第一选项和第二选项为例，防护设备分别判断第一选项和第二选项是否是防护设备的 TCP/IP 协议栈支持的选项；防护设备确定第一选项是防护设备的 TCP/IP 协议栈支持的选项，则防护设备保留第一选项。防护设备确定第二选项是防护设备的 TCP/IP 协议栈不支持的选项，则防护设备删除第二选项。防护设备处理得到的第二握手报文包括第一选项且不包括第二选项。

步骤 S503、防护设备向第一握手报文的目的设备发送第二握手报文。

在第一握手报文为 SYN 报文的情况下，第一握手报文的目的设备为服务器。第二握手报文为删除选项后的 SYN 报文。步骤 S503 包括：防护设备向服务器发送删除选项后的 SYN 报文。

在第一握手报文为 SYN ACK 报文的情况下，第一握手报文的目的设备为客户端设备。第二握手报文为删除选项后的 SYN ACK 报文。步骤 S503 包括：防护设备向客户端设备发送删除选项后的 SYN ACK 报文。

以上通过步骤 S501 至步骤 S503 介绍了防护设备在三次握手阶段删除选项相关的流程，以下介绍基于上述删除选项的流程进行三次握手的完整流程。

请参考附图 7，本申请实施例在三次握手阶段包括附图 7 所示的流程 700。流程 700 包括以下步骤 S710 至步骤 S780。其中，步骤 S710 和步骤 S720 中的 SYN 报文、步骤 S740 和步骤 S750 中的 SYN ACK 报文均是对第一握手报文的举例说明，步骤 S720 和步骤 S730 中删除选项后的 SYN 报文、步骤 S750 和步骤 S760 中删除选项后的 SYN ACK 报文均是对第二握手报文的举例说明。

步骤 S710、客户端设备生成并发送 SYN 报文。

步骤 S720、防护设备接收来自客户端的 SYN 报文。防护设备解析 SYN 报文，从 SYN 报文中提取客户端的 MSS、窗口、时间戳、SACK 等选项。防护设备根据防护设备本地的 TCP/IP 协议栈支持的选项，从 SYN 报文中删除本地的 TCP/IP 协议栈不支持的选项，保留 SYN 报文中本地的 TCP/IP 协议栈支持的选项，得到删除选项后的 SYN 报文。

步骤 S730、防护设备向服务器发送删除选项后的 SYN 报文。

步骤 S740、服务器接收删除选项后的 SYN 报文，生成并发送 SYNACK 报文。

步骤 S750、防护设备接收来自服务器的 SYN ACK 报文。与步骤 S720 同理地，防护设备解析 SYN ACK 报文，从 SYN ACK 报文提取服务器的 MSS、窗口、时间戳、SACK 等选项。防护设备根据防护设备本地的 TCP/IP 协议栈支持的选项，从 SYN ACK 报文中删除不支持的选项，保留 SYN ACK 报文中本地的 TCP/IP 协议栈支持的选项，得到删除选项后的 SYN ACK 报文。

步骤 S760、防护设备向客户端发送删除选项后的 SYN ACK 报文。

步骤 S770、客户端接收删除选项后的 SYN ACK 报文，生成并发送 ACK 报文。

步骤 S780、防护设备接收来自于客户端的 ACK 报文，防护设备将客户端的 ACK 报文转发给服务器，从而完成客户端和服务器会话建立。

以上介绍了本实施例提供的三次握手流程，以下介绍基于该三次握手流程切换至代理模式的流程。

以下介绍的模式切换的流程是对上述方法 500 中步骤 S540 的举例说明。以上介绍的三次握手流程与以下介绍的模式切换流程之间的主要关联在于，由于三次握手流程中防护设备删除了不支持的选项，能够确保采用代理模式检测首条流的过程中报文交互涉及的选项是防护设备自身的 TCP/IP 协议栈支持的选项，避免针对首条流切换至代理模式后由于防护设备难以解析客户端或者服务器使用的选项造成报文传输失败，提高针对首条流检测的可靠性和成功率。下面，对达到这种效果的原理进行介绍。

在 TCP 协议中，TCP 会话中使用哪些选项来传输数据报文是通过三次握手报文进行协商的。具体而言，收发两端（客户端和服务器）在三次握手阶段中，会在三次握手报文中添加自身支持的选项，将三次握手报文发给对端，从而通知对端自身支持哪些选项。收发两端收到对端发来的三次握手报文后，如果三次握手报文中携带某个选项，而且自身也支持这个选项，收发两端会将该选项作为协商出的选项。当会话建立后时，收发两端会启动协商出的选项传输数据。

而通过本实施例提供的三次握手流程，由于防护设备从三次握手报文中删除了不支持的选项，将删除选项后的三次握手报文转发给客户端设备或者服务器，因此，传递到客户端设备以及服务器上的三次握手报文中不包括防护设备不支持的选项。换句话说，传递到客户端设备以及服务器上的三次握手报文中的选项都是防护设备支持的选项。因此，客户端设备和服务器协商出的每个选项都会是防护设备支持的选项，避免出现客户端设备和服务器协商出的选项包含防护设备不支持的选项的情况。那么，当首个会话建立后，客户端和服务器在首个会话中交互的报文中的选项都是防护设备支持的选项。

因此，在本实施例提供的针对首个会话进行检测的流程中，在客户端和服务器交互首个会话的报文的过程中，如果防护设备决定要切换针对首个会话的检测模式，由于防护设备切换为代理模式后继续收到的首个会话中的报文中的选项是防护设备支持的选项，因此防护设备能够通过自身支持的选项采用切换后的模式处理首个会话中继续收到的报文，确保在首个会话过程中成功地进入代理模式，使得首个会话中后续报文能通过代理模式检测。

具体地，防护设备通过在初始的三次握手阶段，根据防护设备的 TCP/IP 协议栈的能力，对客户端设备和服务器的握手进行干涉，确保客户端设备和服务器协商出的选项防护设备本地 TCP/IP 协议栈都可以支持。因此，后续一旦在首个会话中切换为代理模式，客户端设备和服务器使用协商的选项进行报文交互时，防护设备自身的 TCP/IP 协议栈能够利用支持的选项代替服务器与客户端设备交互，防护设备自身的 TCP/IP 协议栈能够利用支持的选项代替客户端设备与服务器交互，从而成功执行采用代理模式进行检测的任务，而不会出现错误。比如，如果防护设备上的 TCP/IP 协议栈不支持 SACK 选项，而客户端设备和服务器支持 SACK 选项，如果客户端设备和服务器在三次握手阶段协商使用 SACK 选项，当防护设备在首个会话

中切换为代理模式后，防护设备会因为难以解析SACK选项，造成首个会话中的报文传输故障，导致业务不通。而防护设备通过删除握手报文中的SACK选项，使得客户端设备和服务器在三次握手阶段不会协商使用SACK选项，因此防护设备在首个会话中切换为代理模式后继续收到的报文不包括SACK选项,避免由于防护设备难以解析SACK选项造成的传输故障。

下面，以防护设备在流模式与代理模式之间进行模式切换为例，对防护设备在首个会话中进行模式切换的具体过程举例说明，详见下述场景一和场景二。

场景一、流模式切换为代理模式

在场景一下，防护设备之前在流模式下可能已经缓存了首个会话中的一些数据报文。比如，防护设备在流模式下，为了进行流重组而缓存一个窗口内接收的数据报文。又如，防护设备在流模式下缓存了一些已经转发给对端，而对端尚未返回确认报文的数据报文。对于这些之前已经缓存的数据报文，防护设备通过执行以下介绍的方案，从而在达到删除选项带来的效果的基础上，进一步加速模式切换的处理过程，减少模式切换的处理时延。

以下，通过方面（1）和方面（2）这两个方面，描述场景一涉及的具体实现方式。

方面（1）防护设备如何处理之前在流模式下缓存的已接收的数据报文。

防护设备在针对首个TCP会话从流模式切换为代理模式的过程中，对于之前在流模式下缓存的已接收的数据报文，防护设备会通过自身TCP/IP协议栈进行ACK处理。具体而言，针对之前在流模式下缓存的客户端设备发来的数据报文，防护设备会通过TCP/IP协议栈主动生成确认报文发送给客户端设备，从而扮演模拟的服务器的角色来应答客户端设备；针对之前在流模式下缓存的服务器发来的数据报文，防护设备会通过TCP/IP协议栈主动生成确认报文发送给服务器，从而扮演模拟的客户端设备的角色来应答服务器。

例如，防护设备在三次握手阶段保留了第一选项（防护设备支持的选项），删除了第二选项（防护设备不支持的选项）。以上方法500中，防护设备在流模式下接收并缓存了首个TCP会话中的第二数据报文。防护设备确定将要切换为代理模式以检测首个TCP会话之后，防护设备根据第一选项生成针对首个TCP会话中的第二数据报文的确认报文；防护设备向第二数据报文的源设备发送针对第二数据报文的确认报文。

在一些实施例中，第二数据报文是客户端发往服务器的报文。具体地，防护设备在采用流模式检测首个TCP会话的数据报文的过程中，客户端发送第二数据报文；防护设备接收并缓存来自于客户端的第二数据报文；防护设备确定将要切换为代理模式以检测首个TCP会话之后，防护设备向客户端发送针对第二数据报文的确认报文。

在另一些实施例中，第二数据报文是服务器发往客户端的报文。具体地，防护设备在采用流模式检测首个TCP会话的数据报文的过程中，服务器发送第二数据报文；防护设备接收并缓存来自于服务器的第二数据报文；防护设备确定将要切换为代理模式以检测首个TCP会话之后，防护设备向服务器发送针对第二数据报文的确认报文。

方面（2）防护设备如何处理之前在流模式下已经转发给对端、而没有收到对端的确认报文的数据报文。

防护设备在针对首个TCP会话从流模式切换为代理模式的过程中，对于之前在流模式下已经转发给对端，而没有收到对端的确认报文的数据报文，防护设备会通过自身TCP/IP协议栈负责这些数据报文的传输可靠性。具体地，针对之前在流模式下已经转发给服务器、且还

没有收到确认报文的数据报文，防护设备会扮演模拟客户端的角色，当发生丢包时向服务器重传数据报文，从而确保数据报文抵达服务器；针对之前在流模式下已经转发给客户端、且还没有收到确认报文的数据报文，防护设备会扮演模拟服务器的角色，当发生丢包时向客户端重传数据报文，从而确保数据报文抵达客户端。

例如，防护设备在三次握手阶段保留了第一选项（防护设备支持的选项），删除了第二选项（防护设备不支持的选项），以上方法 500 中，防护设备在流模式下发送了首个 TCP 会话中的第三数据报文，并缓存第三数据报文。防护设备确定将要切换为代理模式之后，如果第三数据报文满足重传条件，防护设备根据第一选项向第三数据报文的目的设备重新发送第三数据报文。

在一些实施例中，第三数据报文是客户端发往服务器的报文。具体地，防护设备在采用流模式检测首个 TCP 会话的数据报文的过程中，客户端发送第三数据报文；防护设备接收第三数据报文，对第三数据报文进行安全检测后，向服务器转发第三数据报文；防护设备确定将要切换为代理模式之后，如果第三数据报文满足重传条件，防护设备向服务器重新发送第三数据报文。

在一些实施例中，第三数据报文是服务器发往客户端的报文。具体地，防护设备在采用流模式检测首个 TCP 会话的数据报文的过程中，服务器发送第三数据报文；防护设备接收第三数据报文，对第三数据报文进行安全检测后，向客户端转发第三数据报文；防护设备确定将要切换为代理模式之后，如果第三数据报文满足重传条件，防护设备向客户端重新发送第三数据报文。

从以上方面（1）和方面（2）可见，在流模式切换为代理模式的场景下，防护设备根据握手阶段协商出的选项（第一选项），对之前在流模式下缓存的报文进行 ACK 处理以及负责可靠性传输，使得防护设备之前在流模式下缓存的首个会话中数据报文也能够快速走代理模式处理，从而缩短了流模式切换到代理模式所需耗费的时间。

请参考附图 8，防护设备通过提供附图 8 中的功能模块来支持上述处理流程。

防护设备的 TCP 控制层中包括流模式处理模块 1311、TCP/IP 协议栈模块 1331、流模式处理模块 1312 以及 TCP/IP 协议栈模块 1332。其中，附图 3 中的流模式处理模块 131 包括附图 8 中的流模式处理模块 1311 以及流模式处理模块 1312。附图 3 中的 TCP/IP 协议栈模块 133 包括附图 8 中的 TCP/IP 协议栈模块 1331 以及 TCP/IP 协议栈模块 1332。

流模式处理模块 1311 用于处理流模式下与客户端设备 11 的交互。流模式处理模块 1311 包括接收报文队列 13111 以及已发送报文队列 13112。接收报文队列 13111 用于缓存流模式下接收到的来自客户端设备 11 的数据报文。在一些实施例中，接收报文队列 13111 具体用于缓存一个窗口内收到的客户端设备 11 的数据报文。接收报文队列 13111 缓存的数据报文用于进行 TCP 层的流重组。已发送报文队列 13112 用于缓存流模式下已经向客户端设备 11 发送的数据报文。在一些实施例中，已发送报文队列 13112 具体用于缓存已发送、且仍未收到客户端设备 11 的确认报文的数据报文。

流模式处理模块 1312 用于处理流模式下与服务器 12 的交互。流模式处理模块 1312 包括接收报文队列 13121 以及已发送报文队列 13122。接收报文队列 13121 用于缓存流模式下接收到的来自服务器 12 的数据报文。在一些实施例中，接收报文队列 13121 具体用于缓存一个

窗口内收到的服务器 12 的数据报文。接收报文队列 13121 缓存的数据报文用于进行 TCP 层的流重组。已发送报文队列 13122 用于缓存流模式下已经向服务器 12 发送的数据报文。在一些实施例中，已发送报文队列 13122 具体用于缓存已发送、且仍未收到服务器 12 的确认报文的数据报文。

TCP/IP 协议栈模块 1331 为用于与客户端设备 11 交互的 TCP/IP 协议栈模块。

TCP/IP 协议栈模块 1331 包括接收报文队列 13311 以及发送报文队列 13312。接收报文队列 13311 用于缓存代理模式下接收到的来自客户端设备 11 的数据报文。发送报文队列 13312 用于缓存代理模式下向客户端设备 11 发送的数据报文。在一些实施例中，发送报文队列 13312 具体用于缓存代理模式下已经向客户端设备 11 发送、且仍未收到确认报文的数据报文。

TCP/IP 协议栈模块 1332 为与服务器 12 交互的 TCP/IP 协议栈模块。TCP/IP 协议栈模块 1332 包括接收报文队列 13321 以及发送报文队列 13322。接收报文队列 13321 用于缓存代理模式下接收到的来自服务器 12 的数据报文。发送报文队列 13322 用于缓存代理模式下向服务器 12 发送的数据报文。在一些实施例中，发送报文队列 13322 具体用于缓存代理模式下已经向服务器 12 发送、且仍未收到确认报文的数据报文。

下面介绍防护设备如何通过图 3 或者图 8 示出的各个模块实现从流模式切换为代理模式的处理流程。

请参考图 3 和图 8，上层业务模块 130 判断需要进入代理模式处理，则上层业务模块 130 向 TCP 控制层下发指令从而通知 TCP 控制层要转换为代理模式。TCP 控制层接收到上层业务模块 130 发来的指令后，执行以下步骤 S530a 至步骤 S530d。

步骤 S530a、TCP 控制层根据流模式处理模块 131 记录的 TCP 三次握手协商信息，通过 TCP/IP 协议栈模块 133 快速建立会话对。其中，会话对包括代理服务器会话以及代理客户端会话。代理服务器会话负责和真实的客户端交互。代理客户端会话负责和真实的服务器交互。其中，协商信息包括三次握手处理时协商出的选项（如第一选项）。

步骤 S530b、TCP 控制层将从流模式处理模块 131 缓存的数据报文送入 TCP/IP 协议栈模块 133。TCP/IP 协议栈模块 133 对从流模式处理模块 131 送入的报文进行 ACK 处理，从而应答真实客户端或者真实服务器。

具体地，请参考图 8，流模式处理模块 1311 中的接收报文队列 13111 缓存了来自客户端设备 11 的数据报文。TCP 控制层将接收报文队列 13111 缓存的数据报文送入 TCP/IP 协议栈模块 1331 的接收报文队列 13311。TCP/IP 协议栈模块 1331 针对流模式处理模块 1311 送入的报文进行 ACK 处理，从而应答客户端设备 11。

流模式处理模块 1312 中的接收报文队列 13121 缓存了来自服务器 12 的数据报文。TCP 控制层将接收报文队列 13121 缓存的数据报文送入 TCP/IP 协议栈模块 1332 的接收报文队列 13321。TCP/IP 协议栈模块 1332 针对流模式处理模块 1312 送入的报文进行 ACK 处理，从而应答服务器 12。

步骤 S530c、TCP 控制层将流模式处理模块 131 已经转发，尚未收到 ACK 的报文加入 TCP/IP 协议栈模块/代理模式处理模块中的发送报文队列。具体地，流模式处理模块 1311 以及 TCP/IP 协议栈模块 1331 都负责处理和客户端设备 11 的交互，流模式处理模块 1312 以及 TCP/IP 协议栈模块 1332 都负责处理和服务器 12 的交互。在流模式切换为代理模式的过程中，

TCP 控制层会将流模式处理模块 1311 中已发送报文队列 13112 中缓存的报文加入 TCP/IP 协议栈模块 1331 中发送报文队列 13312。TCP 控制层会将流模式处理模块 1312 中已发送报文队列 13122 中缓存的报文加入 TCP/IP 协议栈模块 1332 中发送报文队列 13322。

比如，上层业务模块 130 根据客户端设备 11 发送的数据报文判定需要采用代理模式，TCP 控制层将客户端设备 11 后续发来的数据报文送入 TCP/IP 协议栈模块 1331 之后，TCP 控制层需要将流模式处理模块 1311 已经转发给客户端设备 11 的数据报文，送入 TCP/IP 协议栈模块 1331，通过 TCP/IP 协议栈模块 1331 实现代理客户端的功能，由 TCP/IP 协议栈模块 1331 负责丢包、超时引起的重传操作。

步骤 S530d、TCP 控制层清理流模式使用的资源，进入代理模式处理 TCP 会话后续报文。

例如，TCP 控制层释放流模式处理模块 1311 中接收报文队列 13111 以及已发送报文队列 13112、流模式处理模块 1312 中接收报文队列 13121 以及已发送报文队列 13122 占用的缓存空间。

以上提供的系统架构中，通过定制化的 TCP/IP 协议栈，不仅实现基于数据报文交互结果，在数据报文交互阶段从流模式自适应地切换到代理模式，还支持已经在流模式下缓存数据报文的复杂情况，提升方案的可用性。

场景二、代理模式切换为流模式

防护设备在采用代理模式处理的过程中，防护设备的 TCP/IP 协议栈模块内部、防护设备的上层业务模块都会缓存有一定数量的数据报文。代理模式切换为流模式理想的时间点是防护设备的 TCP/IP 协议栈模块内部以及上层业务模块都没有任何缓存数据报文。在这种理想的时间点进行模式切换时，防护设备建立流模式处理相关的资源、状态等，释放 TCP/IP 协议栈相关资源，即可完成模式切换。但是，通常情况下，并不能满足这一理想状态；这是由于，TCP/IP 协议栈模块中的两种缓存（接收报文队列以及发送报文队列）通常是非空的。比如，当防护设备决定要切换到代理模式时，TCP/IP 协议栈模块中的发送报文队列可能已经缓存了一些已经发送、等待对端确认的报文，TCP/IP 协议栈模块中的接收报文队列可能已经缓存了一些 TCP/IP 协议栈模块已经确认、等待上层业务处理的报文。对于这些之前在代理模式下缓存的数据报文，防护设备通过执行以下介绍的方案，从而在达到删除选项带来的效果的基础上，进一步保证这些数据报文的传输可靠性。

以下，通过方面（a）和方面（b）这两个方面，描述场景二涉及的具体实现方式。以下描述的实现方式能够应用在防护设备针对首个会话，从流模式切换为代理模式之后再重新切换回流模式的场景。

方面（a）防护设备如何处理之前在代理模式下缓存的已发送的数据报文。

防护设备在针对首个 TCP 会话从代理模式切换为流模式的过程中，对于之前在代理模式下已发送的首个 TCP 会话的数据报文，防护设备会通过自身 TCP/IP 协议栈负责这些数据报文的传输可靠性。具体地，防护设备会继续等待对端对这些数据报文的确认报文。当防护设备收到对端针对这些数据报文的确认报文之后，防护设备再从缓存中删除这些数据报文。如果防护设备通过超时未收到确认报文、SACK 选项或者其他方式，发现这些数据报文丢包，则防护设备执行重传。

例如，防护设备在三次握手阶段保留了第一选项（防护设备支持的选项），删除了第二选项（防护设备不支持的选项），以上方法 500 中，防护设备在代理模式下已发送首个 TCP 会

话中的第六数据报文。防护设备确定针对首个TCP会话切换回流模式之后，如果第六数据报文满足重传条件，防护设备根据第一选项向第六数据报文的目的设备重新发送第六数据报文。

在一些实施例中，第六数据报文是首个 TCP 会话中客户端发往服务器的报文。具体地，防护设备在采用代理模式检测首个TCP会话的数据报文的过程中，客户端发送第六数据报文；防护设备接收第六数据报文，防护设备对第六数据报文根据第一选项执行解析后，向客户端设备发送确认报文，此外，防护设备对第六数据报文进行安全检测。如果第六数据报文检测通过，防护设备向服务器发送第六数据报文。防护设备确定将要切换为流模式之后，如果第六数据报文满足重传条件，防护设备根据第一选项向服务器重新发送第六数据报文。

在另一些实施例中，第六数据报文是首个TCP会话中服务器发往客户端的报文。具体地，防护设备在采用代理模式检测首个TCP会话的数据报文的过程中，服务器发送第六数据报文；防护设备接收第六数据报文，防护设备对第六数据报文根据第一选项执行解析后，向服务器发送确认报文，此外，防护设备对第六数据报文进行安全检测。如果第六数据报文检测通过，防护设备向客户端发送第六数据报文。防护设备确定将要切换为流模式之后，如果第六数据报文满足重传条件，防护设备根据第一选项向客户端重新发送第六数据报文。

方面（b）防护设备如何处理之前在代理模式下缓存的已接收的数据报文。

防护设备在针对首个 TCP 会话从代理模式切换为流模式的过程中，对于之前在代理模式下已接收并回复确认的首个TCP会话中数据报文，防护设备会先根据这些数据报文安全检测，再通过自身 TCP/IP 协议栈模块将检测处理后的数据报文进行可靠性发送。其中，可靠性发送是指 TCP/IP 协议栈基于 TCP 重传机制向 TCP 会话的对端（客户端或者服务器）发送数据报文。

例如，防护设备在三次握手阶段保留了第一选项（防护设备支持的选项），删除了第二选项（防护设备不支持的选项）。以上方法 500 中，防护设备在代理模式下已接收首个 TCP 会话中的第七数据报文，并且防护设备已对第七数据报文根据第一选项执行解析后向第七数据报文的源设备发送针对第七数据报文的确认报文。防护设备确定将要切换为流模式之后，防护设备对第七数据报文执行检测处理，得到第八数据报文；防护设备根据第一选项向第七数据报文的目的设备发送第八数据报文。

在一些实施例中，第七数据报文是首个 TCP 会话中客户端发往服务器的报文。具体地，防护设备在采用代理模式检测首个TCP会话的数据报文的过程中，客户端发送第七数据报文；防护设备接收第七数据报文，防护设备对第七数据报文根据第一选项执行解析后，向客户端设备发送针对第七数据报文的确认报文。防护设备确定将要切换为流模式之后，防护设备对第七数据报文执行检测处理，得到第八数据报文；防护设备根据第一选项向服务器发送第八数据报文。此外，如果第八数据报文满足重传条件，防护设备根据第一选项向服务器重新发送第八数据报文。

在另一些实施例中，第七数据报文是首个TCP会话中服务器发往客户端的报文。具体地，防护设备在采用代理模式检测首个TCP会话的数据报文的过程中，服务器发送第七数据报文；防护设备接收第七数据报文，防护设备对第七数据报文根据第一选项执行解析后，向服务器发送针对第七数据报文的确认报文。防护设备确定将要切换为流模式之后，防护设备对第七数据报文执行检测处理，得到第八数据报文；防护设备根据第一选项向客户端发送第八数据报文。此外，如果第八数据报文满足重传条件，防护设备根据第一选项向客户端重新发送第

八数据报文。

下面结合附图 9，介绍防护设备如何通过附图 9 所示的各个模块实现代理模式切换至流模式的处理流程。

请参考附图 9，防护设备从代理模式切换为流模式的步骤包括以下步骤 S530a'至步骤 S530i'。

步骤 S530a'、TCP 控制层停止新报文的入协议栈操作。具体地，上层业务模块 130 确定切换为流模式之后，如果 TCP 控制层新接收到来自客户端设备 11 的数据报文，TCP 控制层停止将数据报文添加至 TCP/IP 协议栈模块 1331 的接收报文队列 13111；如果 TCP 控制层新接收到来自服务器 12 的数据报文，TCP 控制层停止将数据报文添加至 TCP/IP 协议栈模块 1332 的接收报文队列 13321。

步骤 S530b'、TCP 控制层丢弃 TCP/IP 协议栈模块 1331 的接收报文队列 13111 中乱序的数据报文，以及 TCP/IP 协议栈模块 1332 的接收报文队列 13321 中乱序的数据报文。

具体地，由于 TCP/IP 协议栈模块不会对乱序的数据报文回复确认报文，因此乱序的数据报文是能够安全丢弃的。其中，乱序的数据报文是指数据报文的 Seq 号不连续。例如，TCP/IP 协议栈模块 1331 的接收报文队列 13111 缓存有 Seq 号分别是 1-5 的数据报文以及 Seq 号分别是 8-10 的数据报文，但是 TCP/IP 协议栈模块 1331 的接收报文队列 13111 中没有 Seq 号分别是 6-7 的数据报文，那么 Seq 号分别是 8-10 的数据报文即为乱序的数据报文，TCP 控制层在执行步骤 S530b 时，丢弃 Seq 号分别是 8-10 的数据报文。

步骤 S530c'、TCP 控制层将 TCP/IP 协议栈模块 1331 的接收报文队列 13111 中的数据报文以及 TCP/IP 协议栈模块 1332 的接收报文队列 13321 中的数据报文提交给上层业务模块 130 处理，并清空 TCP/IP 协议栈模块 1331 的接收报文队列 13111 以及 TCP/IP 协议栈模块 1332 的接收报文队列 13321。

步骤 S530d'、上层业务模块 130 将处理后的数据报文发给 TCP 控制层，之后上层业务模块 130 清空缓存。TCP 控制层将处理后的数据报文交给对端 TCP/IP 协议栈模块中的发送报文队列。

具体地，如果数据报文来自于 TCP/IP 协议栈模块 1331 的接收报文队列 13111，TCP 控制层会将数据报文发送给 TCP/IP 协议栈模块 1332 中的发送报文队列 13322，由 TCP/IP 协议栈模块 1332 中的发送报文队列 13322 向服务器 12 发送数据报文。如果数据报文来自于 TCP/IP 协议栈模块 1332 的接收报文队列 13321，TCP 控制层会将数据报文发送给 TCP/IP 协议栈模块 1331 中的发送报文队列 13312，由 TCP/IP 协议栈模块 1331 中的发送报文队列 13312 向客户端发送数据报文。

步骤 S530e'、针对处于发送报文队列的数据报文，防护设备通过 TCP/IP 协议栈模块对数据报文进行可靠性发送，并记录 TCP/IP 协议栈模块已发送的数据报文的最大 Seq 号。其中，已发送的数据报文的最大 Seq 号例如是初始序列号（ISN）的基础上按照已发送的数据长度进行递增得到的值。例如，客户端的初始序列号，即 ISN（c）是 1000，防护设备已经为客户端转发了 2000 字节的数据，那么最大 Seq 号就是 3001，其中 SYN 报文占 1 字节。

步骤 S530f'、防护设备接收到来自客户端或者服务器的后续数据报文后，按照流模式处理后续数据报文。

防护设备接收到来自客户端或者服务器的确认报文时，对确认报文的处理步骤包括以下步骤 S530g'或步骤 S530h'。具体地，如果防护设备不支持 SACK 选项，防护设备在三次握手阶段从握手报文中删除 SACK 选项，并按照以下步骤 S530g'处理确认报文。如果防护设备支持 SACK 选项，防护设备在三次握手阶段保留握手报文中的 SACK 选项，并按照以下步骤 S530h'处理确认报文。

步骤 S530g'、如果防护设备不支持 SACK 选项，对于确认报文，防护设备判断确认报文的 ACK 号。如果确认报文的 ACK 号小于或等于记录的最大 Seq 号，防护设备将确认报文送 TCP/IP 协议栈模块。如果确认报文的 ACK 号大于记录的最大 Seq 号，防护设备跳转至步骤 S530i，按照流模式处理确认报文。

其中，将确认报文送 TCP/IP 协议栈模块与按照流模式处理确认报文是两种不同的动作。

如果防护设备按照流模式处理确认报文，防护设备会将确认报文转发给对端。例如，如果确认报文来自于服务器，防护设备会将确认报文转发给客户端。如果确认报文来自于客户端，防护设备会将确认报文转发给服务器。

如果防护设备将确认报文送 TCP/IP 协议栈模块，防护设备不会将确认报文转发给对端，而是通过 TCP/IP 协议栈模块处理确认报文。比如，如果确认报文来自于服务器，防护设备不会将确认报文转发给客户端，而是通过 TCP/IP 协议栈模块充当模拟的服务器处理确认报文。

步骤 S530h'、如果防护设备支持 SACK 选项，防护设备根据 SACK 选项中的范围以及记录的最大 Seq 号按 TCP 协议进行处理。如果确认报文是针对 TCP/IP 协议栈发送的数据报文的确认报文，则防护设备将确认报文送 TCP/IP 协议栈处理；如果确认报文是针对流模式下转发的数据报文的确认报文，则防护设备按照流模式处理确认报文，从而交给对端设备处理确认报文。进一步地，如果 SACK 选项同时确认了 TCP/IP 协议栈发送的数据和流模式下转发的数据，防护设备拆分确认报文分别送 TCP/IP 协议栈处理以及按照流模式处理。

例如，源端先后依次发送了 7 个报文，分别是报文 1、报文 2、报文 3、报文 4、报文 5、报文 6 和报文 7。其中，报文 4 丢失，报文 1、报文 2、报文 3、报文 5、报文 6 以及报文 7 成功传输到了目的端。如果源端和目的端在三次握手时协商使用 SACK 选项，目的端能够利用 SACK 选项指明丢失的报文是报文 4。具体地，目的端返回的确认报文包括 ACK 号以及 SACK 选项。ACK 号用于指示报文 1、报文 2 至报文 3 已经收到，SACK 选项中的序号用于指示报文 5、报文 6 至报文 7 已经收到。因此，发送方根据 ACK 号以及 SACK 选项中的序号，能够知道报文 4 丢了。结合防护设备从代理模式切换为流模式的场景，例如，防护设备在代理模式下接收到报文 1、报文 2、报文 3、报文 4 以及报文 5，防护设备通过自身的 TCP/IP 协议栈发送报文 1、报文 2、报文 3、报文 4 以及报文 5。防护设备确定要切换到流模式之后，后续接收到了报文 6 和报文 7。防护设备按照流模式转发了报文 6 和报文 7。如果防护设备、客户端、服务器均使用 SACK 选项，防护设备接收到确认报文时会对确认报文拆分，针对确认报文中报文 1、报文 2、报文 3、报文 4 以及报文 5 对应的内容，防护设备会通过自身的 TCP/IP 协议栈处理，比如如果报文 4 丢失了，防护设备会通过自身的 TCP/IP 协议栈重传报文 4。针对确认报文中报文 6 以及报文 7 对应的内容，防护设备会通过流模式通知源端处理。

步骤 S530i'、如果 TCP/IP 协议栈模块中针对当前 TCP 会话的发送报文队列缓存的数据报文都已经发送完毕，且防护设备已经接收到这些数据报文的确认报文，防护设备删除 TCP/IP 协议栈模块相关资源。对于 TCP 会话后续的所有报文，防护设备会按照流模式处理。

以上提供的系统架构中，通过定制化的TCP/IP协议栈，不仅实现基于数据报文交互结果，在数据报文交互阶段从代理模式自适应地切换为流模式，还支持已经在代理模式下缓存数据报文的复杂情况，提升方案的可用性。

附图10示出了防护设备的一种可能的结构示意图。

附图10所示的防护设备800例如实现附图5所示方法500中防护设备的功能。在一些实施例中，附图10所示的防护设备800还用于实现附图7所示方法700中防护设备的功能。

在一些实施例中，附图10所示的防护设备800为附图3、附图8或附图9中的防护设备13。例如，附图10所示的防护设备800中的处理单元802通过附图8或附图9中的流模式处理模块1311、TCP/IP协议栈模块1331、流模式处理模块1312、TCP/IP协议栈模块1332中的至少一项实现。

请参考附图10，防护设备800包括获取单元801和处理单元802。可选地，防护设备800还包括发送单元和存储单元。防护设备800中的各个单元全部或部分地通过软件、硬件、固件或者其任意组合来实现。防护设备800中的各个单元分别用于执行上述方法500或方法700中防护设备的相应功能。具体地，获取单元801用于支持防护设备800执行S510。处理单元802用于支持防护设备800执行S520、S530以及S540。在一些实施例中，处理单元802还用于支持防护设备800执行S720以及S750。发送单元用于支持防护设备800执行S730以及S780。存储单元用于支持防护设备800缓存数据报文。

本申请实施例中对单元的划分是示意性的，仅仅为一种逻辑功能划分，实际实现时可选地有另外的划分方式。

在一些实施例中，防护设备800中各个单元集成在一个单元中。例如，防护设备800中各个单元集成在同一个芯片上。该芯片包括处理电路和与该处理电路内部连接通信的输入接口以及输出接口。处理单元802通过芯片中的处理电路实现。获取单元801通过芯片中的输入接口实现。发送单元通过芯片中的输出接口实现。例如，该芯片通过一个或多个现场可编程门阵列（field—programmable gate array，FPGA）、可编程逻辑器件(programmable logic device，PLD)、控制器、状态机、门逻辑、分立硬件部件、任何其它适合的电路、或者能够执行本申请通篇所描述的各种功能的电路的任意组合实现。

在另一些实施例中，防护设备800各个单元单独物理存在。在另一些实施例中，防护设备800一部分单元单独物理存在，另一部分单元集成在一个单元中。例如，在一些实施例中，防护设备800中获取单元801和发送单元集成为同一个硬件（如通信接口）。在一些实施例中，不同单元的集成采用硬件的形式实现，即，不同单元对应于同一个硬件。又如，不同单元的集成采用软件单元的形式实现。

在防护设备800中通过硬件实现的情况下，防护设备800中处理单元802例如通过附图4所示的防护设备200中的处理器201实现。防护设备800中获取单元801、发送单元例如通过附图4所示的防护设备200中的通信接口204实现。防护设备800中存储单元例如通过附图4所示的防护设备200中的存储器203实现。

在防护设备800中通过软件实现的情况下，防护设备800中各个单元例如为防护设备200中的处理器201读取存储器203中存储的程序代码210后生成的软件。例如，防护设备800为虚拟化设备。虚拟化设备包括而不限于虚拟机、容器、Pod中的至少一种。在一些实施例

中，防护设备 800 以虚拟机的形式，部署在硬件设备(如物理服务器)上。例如，基于通用的物理服务器结合网络功能虚拟化（network functions virtualization，NFV）技术来实现防护设备 800。采用虚拟机的方式实现时，防护设备 800 例如为虚拟主机、虚拟路由器或虚拟交换机。本领域技术人员通过阅读本申请即可结合 NFV 技术在通用物理服务器上虚拟出防护设备 800。在另一些实施例中，防护设备 800 以容器（例如 docker 容器）的形式，部署在硬件设备上。例如，防护设备 800 执行上述方法实施例的流程被封装在镜像文件中，硬件设备通过运行镜像文件来创建防护设备 800。在另一些实施例中，防护设备 800 以 Pod 的形式，部署在硬件设备上。Pod 包括多个容器，每个容器用于实现防护设备 800 中的一个或多个单元。

本领域普通技术人员可以意识到，结合本文中所公开的实施例中描述的各方法步骤和单元，能够以电子硬件、计算机软件或者二者的结合来实现，为了清楚地说明硬件和软件的可互换性，在上述说明中已经按照功能一般性地描述了各实施例的步骤及组成。这些功能究竟以硬件还是软件方式来执行，取决于技术方案的特定应用和设计约束条件。本领域普通技术人员可以对每个特定的应用来使用不同方法来实现所描述的功能，但是这种实现不应认为超出本申请的范围。

所属领域的技术人员可以清楚地了解到，为了描述的方便和简洁，上述描述的系统、装置和单元的具体工作过程，可以参见前述方法实施例中的对应过程，在此不再赘述。

本申请中术语“第一”、“第二”等字样用于对作用和功能基本相同的相同项或相似项进行区分，应理解，“第一”、“第二”之间不具有逻辑或时序上的依赖关系，也不对数量和执行顺序进行限定。例如，在不脱离各种示例的范围的情况下，第一数据报文可以被称为第二数据报文，并且类似地，第二数据报文可以被称为第一数据报文。第一数据报文和第二数据报文都可以是数据报文，并且在某些情况下，可以是单独且不同的数据报文。

本申请中术语“至少一个”的含义是指一个或多个。

在上述实施例中，可以全部或部分地通过软件、硬件、固件或者其任意组合来实现。当使用软件实现时，可以全部或部分地以计算机程序产品的形式实现。该计算机程序产品包括一个或多个计算机程序指令。在计算机上加载和执行该计算机程序指令时，全部或部分地产生按照本申请实施例中的流程或功能。该计算机可以是通用计算机、专用计算机、计算机网络、或者其他可编程装置。

该计算机指令可以存储在计算机可读存储介质中，或者从一个计算机可读存储介质向另一个计算机可读存储介质传输，例如，该计算机程序指令可以从一个网站站点、计算机、服务器或数据中心通过有线或无线方式向另一个网站站点、计算机、服务器或数据中心进行传输。该计算机可读存储介质可以是计算机能够存取的任何可用介质或者是包含一个或多个可用介质集成的服务器、数据中心等数据存储设备。该可用介质可以是磁性介质 (例如软盘、硬盘、磁带)、光介质(例如，数字视频光盘（digital video disc，DVD)、或者半导体介质（例如固态硬盘）等。前述的存储介质包括：U 盘、移动硬盘、只读存储器（read-only memory，ROM)、随机存取存储器（random access memory，RAM)、磁碟或者光盘等各种可以存储程序代码的介质。

以上实施例仅用以说明本申请的技术方案，而非对其限制；尽管参照前述实施例对本申请进行了详细的说明，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申请各实施例技术方案的范围。

权利要求书

1.一种网络安全防护方法，其特征在于，所述方法包括：

防护设备获取客户端设备与服务器之间首个传输控制协议 TCP 会话中的第一数据报文，所述首个 TCP 会话为客户端设备与服务器之间建立的第一个会话，所述防护设备部署于所述客户端设备与所述服务器之间；

所述防护设备根据所述第一数据报文的应用层数据，识别所述第一数据报文的应用层协议类型；

所述防护设备确定所述应用层协议类型对应的检测模式为代理模式；

所述防护设备采用所述代理模式对所述首个 TCP 会话中的后续报文进行安全检测。

2.根据权利要求 1 所述的方法，其特征在于，所述防护设备获取客户端设备与服务器之间首个传输控制协议 TCP 会话中的第一数据报文之前，所述方法还包括：

所述防护设备获取所述客户端设备与所述服务器之间传输的第一握手报文，所述第一握手报文用于创建所述首个 TCP 会话，所述第一握手报文包括第一选项以及第二选项，所述第一选项为所述防护设备支持的选项，所述第二选项为所述防护设备不支持的选项；

所述防护设备从所述第一握手报文删除所述第二选项，从而得到第二握手报文；

所述防护设备向所述第一握手报文的目的设备发送所述第二握手报文。

3.根据权利要求 2 所述的方法，其特征在于，所述首个 TCP 会话中的后续报文包括第二数据报文，所述防护设备采用所述代理模式对所述首个 TCP 会话中的后续报文进行安全检测，包括：

所述防护设备接收并缓存所述第二数据报文；

所述防护设备根据所述第一选项生成针对所述第二数据报文的确认报文；

所述防护设备向所述第二数据报文的源设备发送所述针对第二数据报文的确认报文，所述第二数据报文的源设备为所述客户端设备或者所述服务器。

4.根据权利要求 2 所述的方法，其特征在于，所述首个 TCP 会话中的后续报文包括第三数据报文，所述防护设备采用所述代理模式对所述首个 TCP 会话中的后续报文进行安全检测，包括：

所述防护设备发送并缓存所述第三数据报文；

如果所述第三数据报文满足重传条件，所述防护设备根据所述第一选项向所述第三数据报文的目的设备重新发送所述第三数据报文，所述第三数据报文的目的设备为所述客户端设备或者所述服务器。

5.根据权利要求 4 所述的方法，其特征在于，所述重传条件包括：所述防护设备未接收到针对数据报文的确认报文；或者，

所述第一选项为选择性确认 SACK 选项，所述重传条件包括：所述防护设备根据来自于

数据报文的目的设备的 SACK 选项中的信息，确定数据报文发生丢包。

6.根据权利要求 2 至 5 中任一项所述的方法，其特征在于，所述第一握手报文为来自于所述客户端设备的同步序列编号 SYN 报文，所述第一握手报文的目的设备为所述服务器；或者，

所述第一握手报文为来自于所述服务器的同步序列编号确认 SYN ACK 报文，所述第一握手报文的目的设备为所述客户端设备。

7.根据权利要求 1 所述的方法，其特征在于，所述安全检测为防病毒 AV 检测，所述防护设备采用所述代理模式对所述首个 TCP 会话中的后续报文进行安全检测，包括：

所述防护设备采用所述代理模式对所述首个 TCP 会话中的第四数据报文进行 AV 检测，所述第四数据报文为所述首个 TCP 会话中在所述第一数据报文之后传输的报文；

所述方法还包括：

如果所述防护设备对所述首个 TCP 会话中的第四数据报文进行 AV 检测的结果为不包含病毒，所述防护设备切换为流模式，并采用所述流模式针对所述首个 TCP 会话中所述第四数据报文之后传输的后续报文继续进行安全检测。

8.根据权利要求 1 所述的方法，其特征在于，所述防护设备采用所述代理模式对所述首个 TCP 会话中的后续报文进行安全检测，包括：

所述防护设备采用所述代理模式对所述首个 TCP 会话中的第五数据报文进行检测，所述第五数据报文为所述首个 TCP 会话中在所述第一数据报文之后传输的报文；

所述方法还包括：

如果所述第五数据报文的应用层数据指示所述客户端设备与所述服务器将要在所述 TCP 会话中进行加密通信，所述防护设备切换为流模式，并采用所述流模式针对所述首个 TCP 会话中所述第五数据报文之后传输的后续报文继续进行安全检测。

9.一种防护设备，其特征在于，所述防护设备包括：

获取单元，用于获取客户端设备与服务器之间首个传输控制协议 TCP 会话中的第一数据报文，所述首个 TCP 会话为客户端设备与服务器之间建立的第一个的会话，所述防护设备部署于所述客户端设备与所述服务器之间；

处理单元，用于根据所述第一数据报文的应用层数据，识别所述第一数据报文的应用层协议类型；

所述处理单元，还用于确定所述应用层协议类型对应的检测模式为代理模式；

所述处理单元，还用于采用所述代理模式对所述首个 TCP 会话中的后续报文进行安全检测。

10.根据权利要求 9 所述的防护设备，其特征在于，

所述获取单元，还用于获取所述客户端设备与所述服务器之间传输的第一握手报文，所述第一握手报文用于创建所述首个 TCP 会话，所述第一握手报文包括第一选项以及第二选项，

所述第一选项为所述防护设备支持的选项，所述第二选项为所述防护设备不支持的选项；

所述处理单元，还用于从所述第一握手报文删除所述第二选项，从而得到第二握手报文；

所述防护设备还包括发送单元，所述发送单元用于向所述第一握手报文的目的设备发送所述第二握手报文。

11.根据权利要求 10 所述的防护设备，其特征在于，所述首个 TCP 会话中的后续报文包括第二数据报文；

所述防护设备还包括接收单元和存储单元，所述接收单元用于接收所述第二数据报文，所述存储单元用于缓存所述第二数据报文；

所述处理单元，用于根据所述第一选项生成针对所述第二数据报文的确认报文；

所述发送单元，用于向所述第二数据报文的源设备发送所述针对第二数据报文的确认报文，所述第二数据报文的源设备为所述客户端设备或者所述服务器。

12.根据权利要求 10 所述的防护设备，其特征在于，所述首个 TCP 会话中的后续报文包括第三数据报文，所述发送单元，用于发送所述第三数据报文；

所述防护设备还包括存储单元，所述存储单元，用于缓存所述第三数据报文；

所述发送单元，还用于如果所述第三数据报文满足重传条件，根据所述第一选项向所述第三数据报文的目的设备重新发送所述第三数据报文，所述第三数据报文的目的设备为所述客户端设备或者所述服务器。

13.根据权利要求 9 所述的防护设备，其特征在于，所述安全检测为防病毒 AV 检测，所述处理单元，用于采用所述代理模式对所述首个 TCP 会话中的第四数据报文进行 AV 检测，所述第四数据报文为所述首个 TCP 会话中在所述第一数据报文之后传输的报文；

所述处理单元，还用于如果对所述首个 TCP 会话中的第四数据报文进行 AV 检测的结果为不包含病毒，切换为流模式，并采用所述流模式针对所述首个 TCP 会话中所述第四数据报文之后传输的后续报文继续进行安全检测。

14.根据权利要求 9 所述的防护设备，其特征在于，

所述处理单元，用于采用所述代理模式对所述首个 TCP 会话中的第五数据报文进行检测，所述第五数据报文为所述首个 TCP 会话中在所述第一数据报文之后传输的报文；

所述处理单元，还用于如果所述第五数据报文的应用层数据指示所述客户端设备与所述服务器将要在所述 TCP 会话中进行加密通信，切换为流模式，并采用所述流模式针对所述首个 TCP 会话中所述第五数据报文之后传输的后续报文继续进行安全检测。

15.一种防护设备，其特征在于，所述防护设备包括处理器和通信接口，所述处理器用于执行程序代码，使得所述防护设备执行如权利要求 1 至权利要求 8 中任一项所述的方法，所述通信接口用于接收或发送报文。

16.一种计算机程序产品，其特征在于，所述计算机程序产品包括一个或多个计算机程序

指令，当所述计算机程序指令被计算机加载并执行时，使得所述计算机执行权利要求 1 至 8 中任意一项所述的网络安全防护方法。

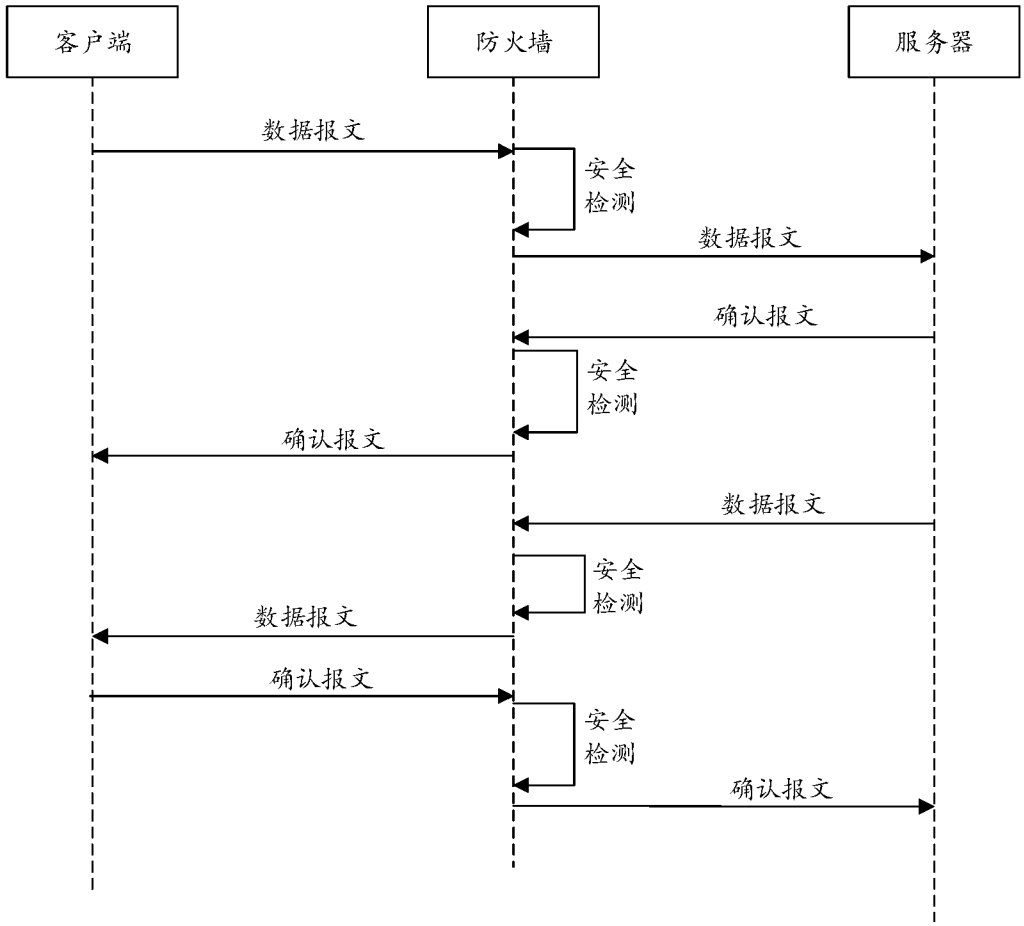

客户端
防火墙
服务器
数据报文
安全检测
数据报文
确认报文
安全检测
确认报文
数据报文
安全检测
数据报文
确认报文
安全检测
确认报文

图 1

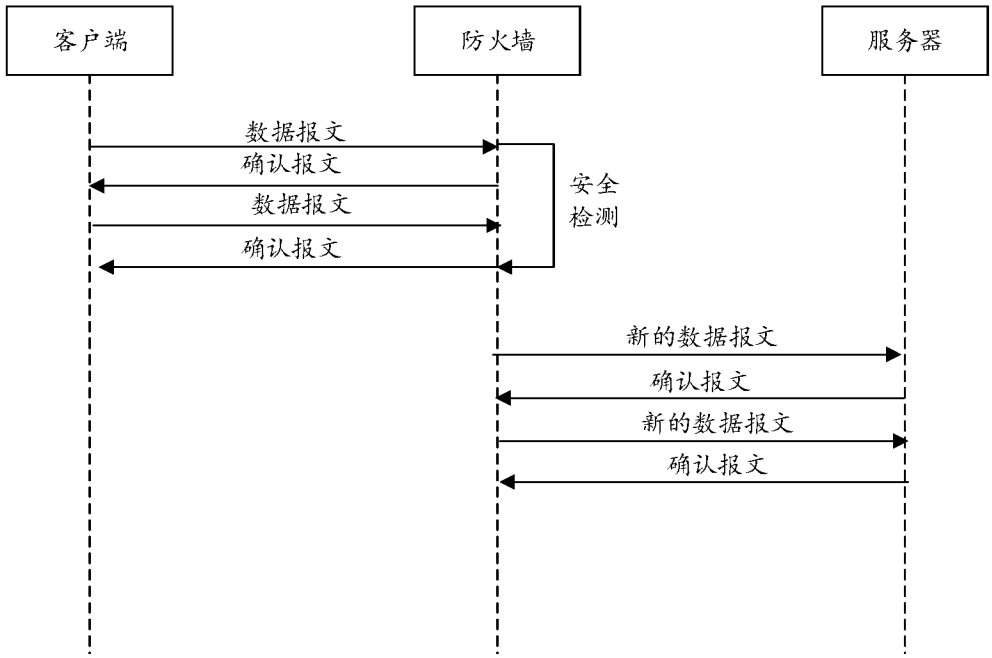

客户端
防火墙
服务器
数据报文
确认报文
数据报文
确认报文
安全检测
新的数据报文
确认报文
新的数据报文
确认报文

图 2

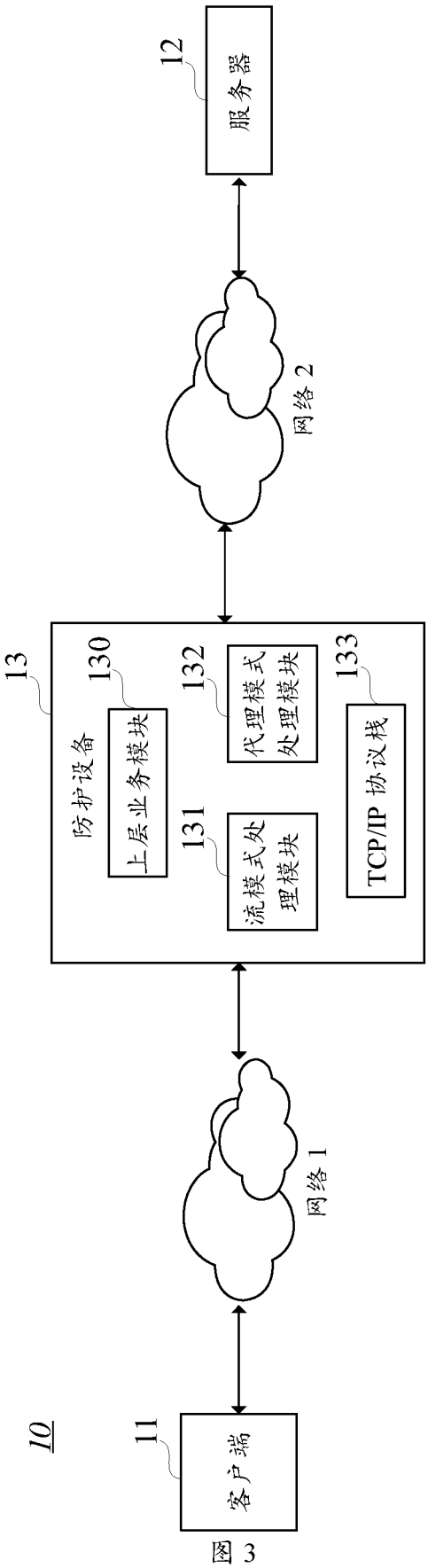

10
11
客户端
网络 1
13
防护设备
130
上层业务模块
131
流模式处理模块
132
代理模式处理模块
133
TCP/IP 协议栈
网络 2
12
服务器

图 3

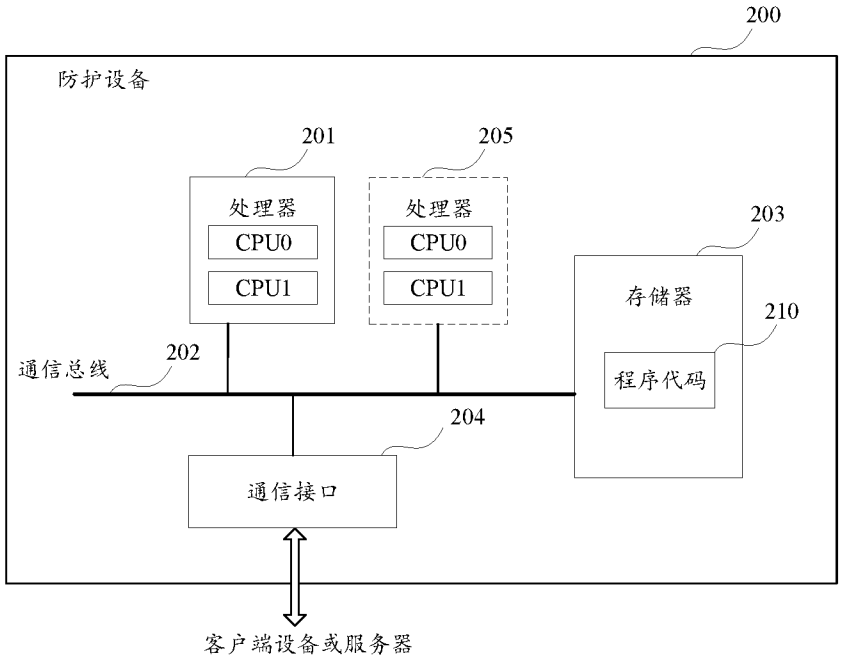

200
防护设备
201
205
处理器
CPU0
CPU1
处理器
CPU0
CPU1
203
存储器
210
程序代码
通信总线
202
204
通信接口
客户端设备或服务器

图 4

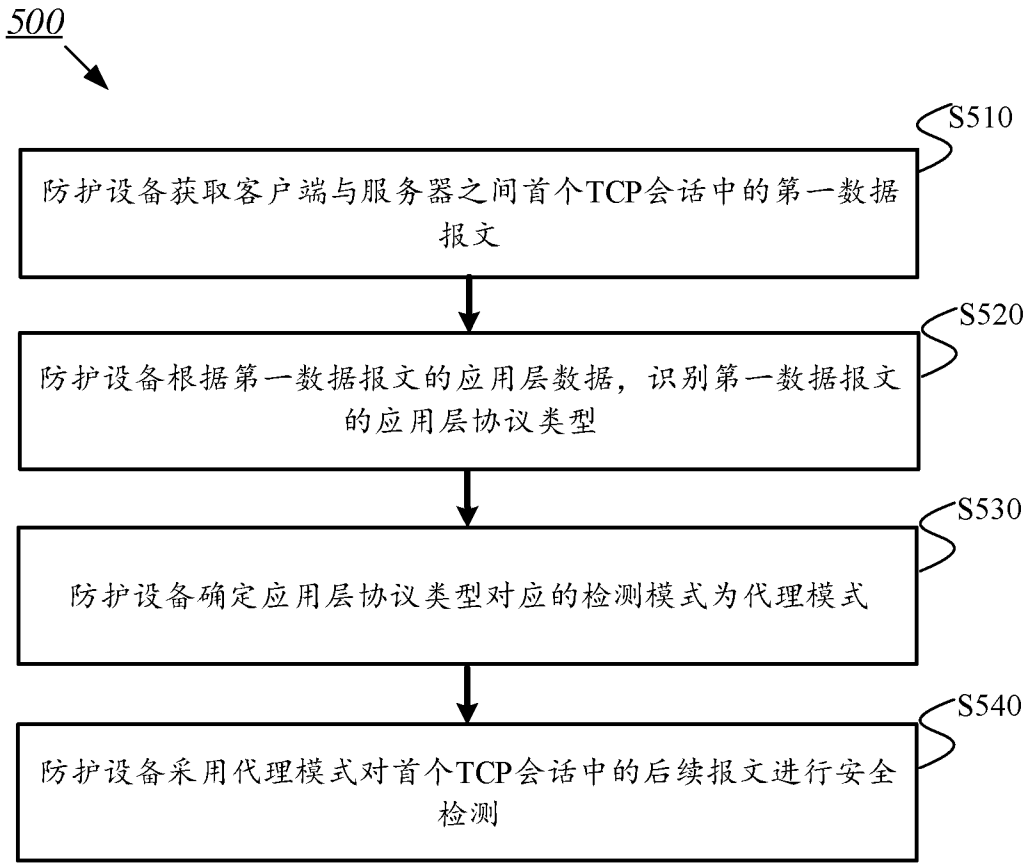

500
S510
防护设备获取客户端与服务器之间首个TCP会话中的第一数据报文
S520
防护设备根据第一数据报文的应用层数据，识别第一数据报文的应用层协议类型
S530
防护设备确定应用层协议类型对应的检测模式为代理模式
S540
防护设备采用代理模式对首个TCP会话中的后续报文进行安全检测

图 5

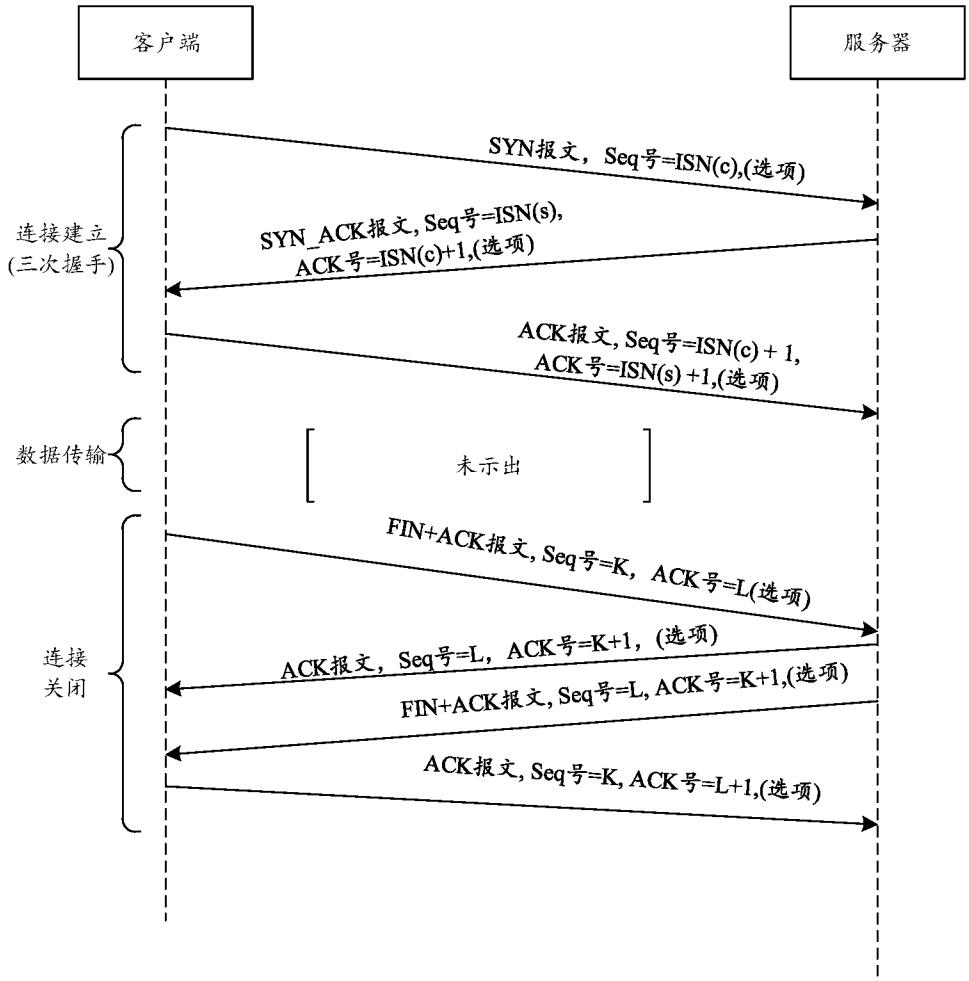

客户端
服务器
SYN报文，Seq号=ISN(c),(选项)
连接建立
(三次握手)
SYN_ACK报文, Seq号=ISN(s),
ACK号=ISN(c)+1,(选项)
ACK报文, Seq号=ISN(c) + 1,
ACK号=ISN(s) +1,(选项)
数据传输
未示出
FIN+ACK报文, Seq号=K，ACK号=L(选项)
连接
关闭
ACK报文，Seq号=L，ACK号=K+1，(选项)
FIN+ACK报文, Seq号=L, ACK号=K+1,(选项)
ACK报文, Seq号=K, ACK号=L+1,(选项)

图 6

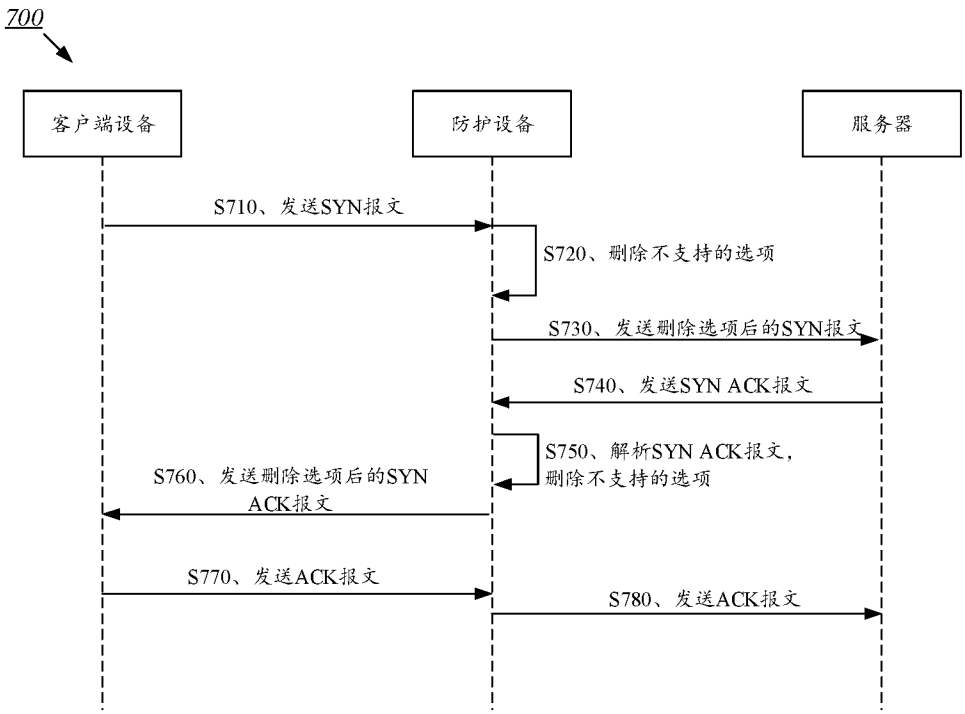

700
客户端设备
防护设备
服务器
S710、发送SYN报文
S720、删除不支持的选项
S730、发送删除选项后的SYN报文
S740、发送SYN ACK报文
S750、解析SYN ACK报文，
删除不支持的选项
S760、发送删除选项后的SYN
ACK报文
S770、发送ACK报文
S780、发送ACK报文

图 7

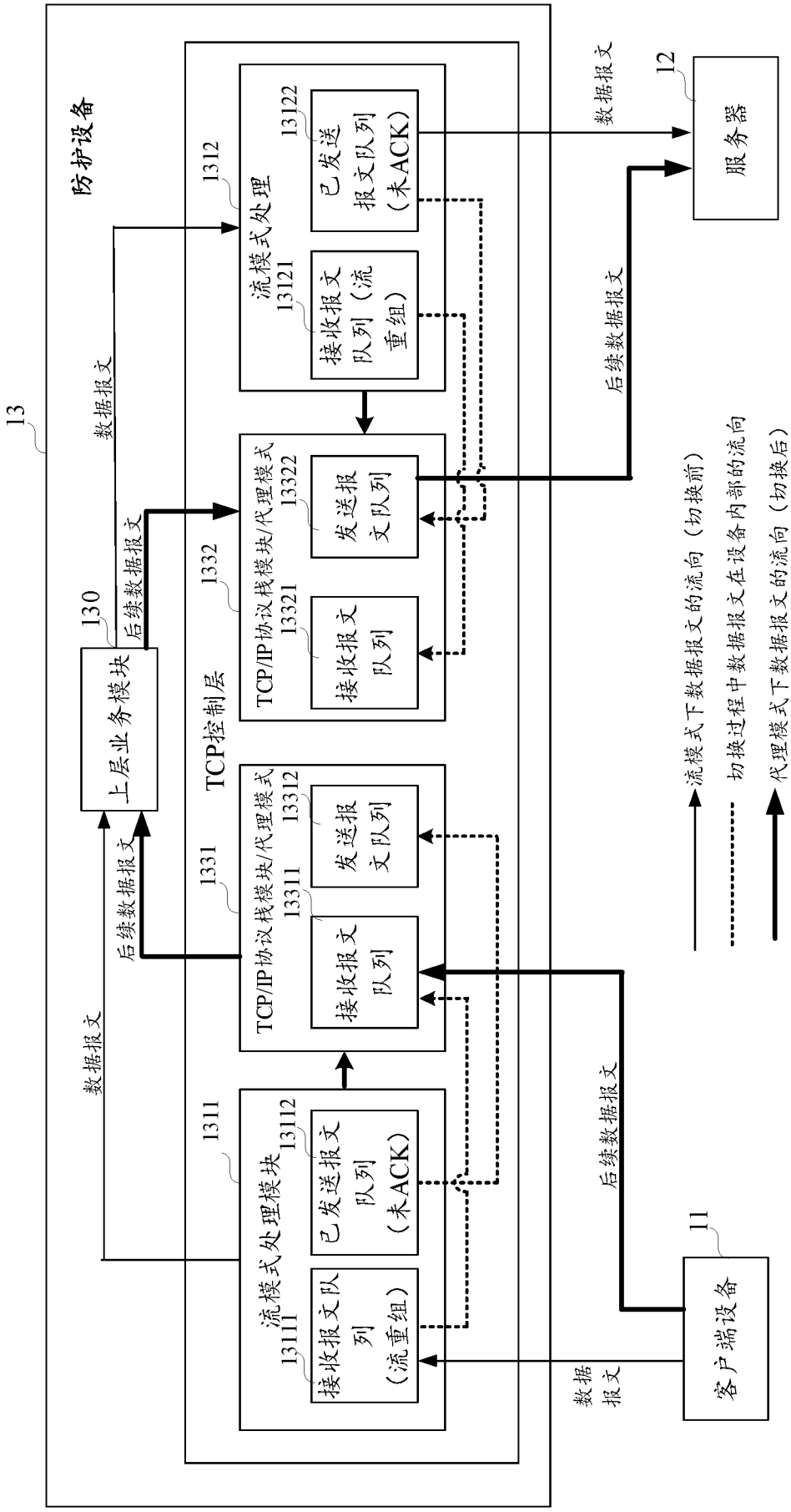

13
防护设备
130
上层业务模块
TCP控制层
1312
流模式处理
13121
接收报文队列（流重组）
13122
已发送报文队列（未ACK）
TCP/IP协议栈模块/代理模式
1332
13321
接收报文队列
13322
发送报文队列
1331
13311
接收报文队列
13312
发送报文队列
流模式处理模块
1311
13111
接收报文队列（流重组）
13112
已发送报文队列（未ACK）
数据报文
后续数据报文
12
服务器
11
客户端设备
流模式下数据报文的流向（切换前）
切换过程中数据报文在设备内部的流向
代理模式下数据报文的流向（切换后）

图 8

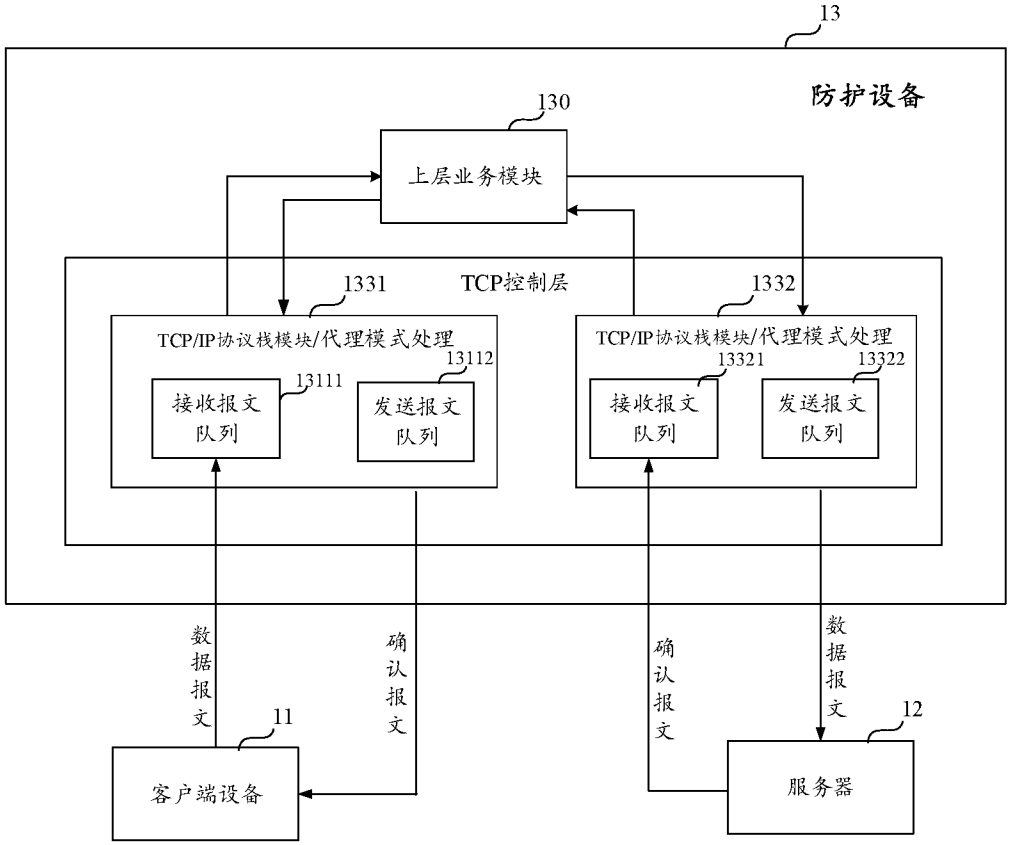

13
防护设备
130
上层业务模块
1331
TCP控制层
1332
TCP/IP协议栈模块/代理模式处理
13112
13111
接收报文队列
发送报文队列
TCP/IP协议栈模块/代理模式处理
13321
13322
接收报文队列
发送报文队列
数据报文
确认报文
确认报文
数据报文
11
12
客户端设备
服务器

图 9

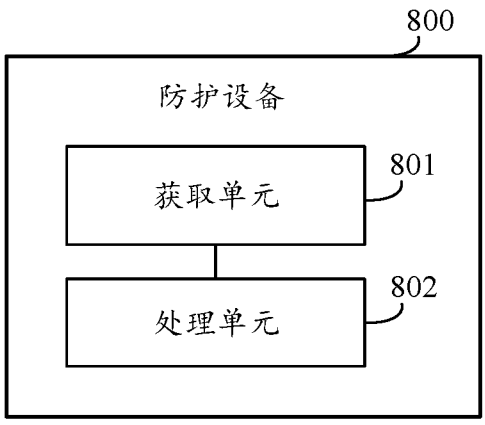

800
防护设备
801
获取单元
802
处理单元

图 10

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2021/088488

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)

CNABS; CNTXT; CNKI; VEN; USTXT; USTXT; WOTXT; IEEE: 防火墙, 防护设备, 网桥, 网关, 路由器, 流模式, 漏检, 攻击, 网络安全, 代理模式, 透明模式, 应用层, 协议, 识别, 检测, 确定, 首个, 第一个, 会话, 数据报, 数据包, network, firewall, bridge, gate, router, flow, attack, safety, proxy, transparent, application layer, protocol, identify, detect, determine, first, session, data packet

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 109698831 A (CEC INTELLIGENT TECHNOLOGY CO., LTD.) 30 April 2019 (2019-04-30) entire document	1-16
A	CN 107370715 A (SANGFOR NETWORK TECHNOLOGY (SHENZHEN) CO., LTD. et al.) 21 November 2017 (2017-11-21) entire document	1-16
A	CN 110138722 A (XI'AN JIAOTONG JUMP NETWORK TECHNOLOGY CO., LTD.) 16 August 2019 (2019-08-16) entire document	1-16
A	US 2019238513 A1 (GENERAL ELECTRIC COMPANY) 01 August 2019 (2019-08-01) entire document	1-16

☐ 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
23 July 2021	**29 July 2021**
Name and mailing address of the ISA/CN **China National Intellectual Property Administration (ISA/CN)** **No. 6, Xitucheng Road, Jimenqiao, Haidian District, Beijing 100088, China** Facsimile No. **(86-10)62019451**	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2021/088488

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 109698831 A	30 April 2019	None	
CN 107370715 A	21 November 2017	CN 107370715 B	18 September 2020
CN 110138722 A	16 August 2019	None	
US 2019238513 A1	01 August 2019	None	

国际检索报告

国际申请号
PCT/CN2021/088488

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））

CNABS;CNTXT;CNKI;VEN;USTXT;USTXT;WOTXT;IEEE:防火墙，防护设备，网桥，网关，路由器，流模式，漏检，攻击，网络安全，代理模式，透明模式，应用层，协议，识别，检测，确定，首个，第一个，会话，数据报，数据包，network，firewall，bridge，gate，router，flow，attack，safety，proxy，transparent，application layer，protocol，identify，detect，determine，first，session，data packet

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
A	CN 109698831 A (中电智能科技有限公司) 2019年 4月 30日 (2019-04-30) 全文	1-16
A	CN 107370715 A (深信服科技股份有限公司等) 2017年 11月 21日 (2017-11-21) 全文	1-16
A	CN 110138722 A (西安交大捷普网络科技有限公司) 2019年 8月 16日 (2019-08-16) 全文	1-16
A	US 2019238513 A1 (GEN ELECTRIC) 2019年 8月 1日 (2019-08-01) 全文	1-16

☐ 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
2021年 7月 23日	2021年 7月 29日

ISA/CN的名称和邮寄地址	受权官员
中国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088	朱秀玲
传真号 (86-10)62019451	电话号码 86-(010)-62089127

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2021/088488

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 109698831 A	2019年 4月 30日	无	
CN 107370715 A	2017年 11月 21日	CN 107370715 B	2020年 9月 18日
CN 110138722 A	2019年 8月 16日	无	
US 2019238513 A1	2019年 8月 1日	无	