

一种数据处理方法、装置及分布式防火墙系统

相关申请的交叉引用

本申请要求在2024年02月26日提交中国国家知识产权局、申请号为202410210863.5、申请名称为“一种数据处理的方法、装置及其他设备”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；
5 本申请要求在2024年03月29日提交中国国家知识产权局、申请号为202410387020.2、申请名称为“一种数据处理方法、装置及分布式防火墙系统”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

10 本申请涉及云计算技术领域，尤其涉及一种数据处理方法、装置及分布式防火墙系统。

背景技术

防火墙系统是一个由计算机硬件和软件组成的系统，部署于网络边界，是内部网络和外部网络之间的连接桥梁。防火墙系统可以将内部网络和外部网络分开，对网络边界的数据进行访问控制，防止非法访问、恶意入侵等，能够保障内部网络数据的安全。
15 防火墙系统可以由负载均衡节点和多个引擎节点组成。负载均衡节点主要负责多个引擎节点的流量均衡等，引擎节点主要根据安全策略控制报文的访问。目前，引擎节点主要是基于会话的相关信息（例如，会话列表）控制会话的访问。防火墙系统进行扩容、缩容、或引擎节点发生故障时，会导致部分会话重新分发到其他引擎节点，由于该其他引擎节点没有这部分会话的相关信息，这样就会导致该会话的中断，从而影响业务的正常传输。
20

发明内容

本申请实施例提供一种数据处理方法、装置及分布式防火墙系统，用于减少因防火墙系统进行扩容、缩容、或引擎节点发生故障对业务传输的影响。
25 第一方面，本申请提供一种数据处理方法，该方法可以由分布式防火墙系统中的第一引擎节点执行，或者也可以由包括第一引擎节点的设备执行，或者还可以由配置于第一引擎节点中的部件（如芯片系统、或芯片、或功能模块等）执行，不予限制。其中，分布式防火墙系统可以包括多个引擎节点，该第一引擎节点属于该多个引擎节点。
以第一引擎节点为执行主体为例，该方法包括：第一引擎节点为第二引擎节点创建第一位表文件，其中，第一位表文件用于指示第一引擎节点对第二引擎节点的至少一个消息（如记为M个消息，M为正整数）中的每个消息的接收情况，M个消息包括如下项或多项：第一会话表、或者与流重组相关的第一信息，第二引擎节点属于多个引擎节点；在第一位表文件指示M个消息中的N个消息未接收到的情况下，向第二引擎节点发送请求消息，其中，请求消息用于请求N个消息，N为小于或等于M的正整数；接收来自第二引擎节点发送的N个消息；以及，修改第一位表文件，修改后的第一位表文件
30 用于指示M个消息均已接收。
35 本申请上述实施例中，第一引擎节点可以获取第二引擎节点第一会话表（和/或流重组的第一信息），意味着分布式防火墙系统中的多个引擎节点之间可以共享会话表（和/或流重组的信息），这样当分布式防火墙系统缩容（即减少引擎节点的数量）或引擎节点发生故障后，由于其他引擎节点共享有该引擎节点的会话表（和/或流重组的信息），因此，该其他引擎节点可以继续为该引擎节点负责的会话（和/或数据流）提供服务，从而能够减少分布式防火墙系统进行缩容或引擎节点发生故障时对业务的影响。当分布式防火墙系统扩容（即有新的引擎节点加入分布式防火墙系统）时，该引擎节点可以通过本申请实施例获取分布式防火墙系统中其他引擎节点的历史数据（即会话表和/或流重组的信息），这样即便为该新加入的引擎节点分发其他引擎节点的业务任务该新加入的引擎节点也可以根据该历史数据继续为该业务提供服务，从而能够减少分布式防火墙系统进行扩容时对业务的影响。
40 在一种可能的实现方式中，第一引擎节点还可以将待发送的至少一个消息（如记为H个消息）进
45

行存储, H 个消息包括如下一项或多项: 第二会话表、或者与流重组相关的第二信息, H 为正整数; 向多个引擎节点中除了第一引擎节点之外的至少一个引擎节点发送 H 个消息。

通过上述实现方式, 第一引擎节点可以将待发送的消息存储一份在本地使用, 另外复制一份共享给分布式防火墙系统中的其他引擎节点, 实现分布式防火墙系统中多个引擎节点之间的数据同步(或共享), 有利于减少对业务传输的影响。

在一种可能的实现方式中, 第一引擎节点向多个引擎节点中除了第一引擎节点之外的至少一个引擎节点发送 H 个消息, 可以为: 第一引擎节点将 H 个消息写入缓冲区; 在满足第一条件的情况下, 向多个引擎节点中除了第一引擎节点之外的至少一个引擎节点发送该 H 个消息, 其中, 第一条件包括如下一项或多项: H 个消息的数据量大于或等于第一阈值、或者 H 个消息的缓存时间大于或等于第二阈值。

通过上述实现方式, 第一引擎节点可以将待发送的消息先存储到缓冲区, 待满足条件后再发送给分布式防火墙系统中的其他引擎节点。

在一种可能的实现方式中, 第一引擎节点还可以接收第一报文, 第一报文属于第一会话; 在第一会话为新建会话的情况下, 根据第一会话的连接方向和访问控制列表确定是否允许第一报文的访问。

通过上述实现方式, 如果第一报文所属的第一会话为新建会话, 那么第一引擎节点可以直接获得该第一会话的连接方向, 并基于该第一会话的连接方向查询访问控制列表。

在一种可能的实现方式中, 在第一会话表中不包括第一会话的标识, 或者第一会话表中包括第一会话的标识和第三信息, 该第三信息用于指示第一会话的连接方向不确定的情况下, 第一引擎节点还可以修改第一会话表, 其中, 修改后的第一会话表中包括第一会话的标识、第四信息以及第一会话的连接方向, 第四信息用于指示第一会话的连接方向确定; 向多个引擎节点中除了第一引擎节点之外的至少一个引擎节点发送修改后的第一会话表。

通过上述实现方式, 第一引擎节点还可以修改第一会话表, 以及将修改后的第一会话表同步给分布式防火墙系统中的其他引擎节点, 实现数据的同步, 有利于减少对业务传输的影响。

在一种可能的实现方式中, 第一引擎节点还可以接收第一报文, 第一报文属于第一会话; 在第一会话不是新建会话的情况下, 根据第一会话表确定第一会话的连接方向, 其中, 第一会话表中不包括第一会话的标识, 第一会话的连接方向为第一报文的发送方向; 根据第一会话的连接方向和访问控制列表确定是否允许第一报文的访问; 修改第一会话表, 其中, 修改后的第一会话表中包括第一会话的标识以及第三信息, 第三信息用于指示第一会话的连接方向不确定; 向多个引擎节点中除了第一引擎节点之外的至少一个引擎节点发送修改后的第一会话表。

通过上述实现方式, 第一会话不是新建会话, 第一引擎节点可以查询第一会话表, 根据查询结果确定第一会话的连接方向, 以及根据该第一会话的连接方向查询访问控制列表。在第一会话表不包括第一会话的情况下, 第一引擎节点还可以修改第一会话表, 以及将修改后的第一会话表同步给分布式防火墙系统中的其他引擎节点, 实现数据的同步, 有利于减少对业务传输的影响。

在一种可能的实现方式中, 第一引擎节点还可以接收第一报文, 第一报文属于第一会话; 在第一会话不是新建会话的情况下, 根据第一会话表确定第一会话的连接方向; 根据第一会话的连接方向和访问控制列表确定是否允许第一报文的访问; 其中, 第一会话表包括第一会话的标识、第四信息和第一会话的连接方向, 第四信息用于指示第一会话的连接方向确定; 或者, 第一会话表包括第一会话的标识和第三信息, 第三信息用于指示第一会话的连接方向不确定, 第一会话的连接方向包括第一报文的正反两个方向。其中, 第一报文的正反两个方向可以包括第一报文的发送方向和第一报文的发送方向的反(或逆)方向。

通过上述实现方式, 第一会话不是新建会话, 第一引擎节点可以查询第一会话表, 并根据查询结果确定第一会话的连接方向, 以及根据该第一会话的连接方向查询访问控制列表。

在一种可能的实现方式中, 第一引擎节点还可以接收第二报文, 第二报文属于第一数据流; 在第二报文为第一数据流中的第一个报文的情况下, 对第二报文进行流重组处理; 在第一数据流重组完成的情况下, 向多个引擎节点中除了第一引擎节点之外的至少一个引擎节点发送第五信息, 第五信息用于指示第一数据流重组完成; 或者, 在第一数据流未重组完成的情况下, 向多个引擎节点中除了第一引擎节点之外的至少一个引擎节点发送第六信息, 第六信息用于指示第一数据流未重组完成且第一数据流的主处理节点为第一引擎节点。

通过上述实现方式, 第一引擎节点是主处理节点, 可以对接收到的报文进行流重组处理, 以及将第

一数据流的重组的相关信息发送给分布式防火墙系统中的其他引擎节点,以便该其他引擎节点获得该第一数据流的重组的相关信息并进行相应的处理。例如,第一数据流重组完成,接收有该第一数据流的报文的其他引擎节点可以丢弃该报文,释放存储资源。又例如,第一数据流未重组完成且主处理节点为第一引擎节点,接收有该第一数据流的报文的其他引擎节点可以将该报文发送给第一引擎节点,以尽早完成该第一数据流的重组。

在一种可能的实现方式中,第一信息中不包括第一数据流的信息,第一引擎节点还可以接收第二报文,第二报文属于第一数据流;在第二报文不是第一数据流中的第一个报文的情况下,根据第一信息确定第一数据流未重组完成以及第一数据流的主处理节点不存在;缓存第二报文。

通过上述实现方式,第一引擎节点是主处理节点,可以缓存该第二报文,以便在缓存有效期内可以将该第二报文发送给主处理节点进行流重组。

在一种可能的实现方式中,第一引擎节点还可以接收第七信息,第七信息用于指示第一数据流未重组完成且第一数据流的主处理节点为第三引擎节点,第三引擎节点属于多个引擎节点;向第三引擎节点发送第二报文。

在另一种可能的实现方式中,第一引擎节点还可以接收第三报文,第三报文属于第一数据流;在第三报文是第一数据流中的第一个报文的情况下,对第二报文和第三报文进行流重组处理;在第一数据流重组完成的情况下,向多个引擎节点中除了第一引擎节点之外的至少一个引擎节点发送第五信息,第五信息用于指示第一数据流重组完成;或者,在第一数据流未重组完成的情况下,向多个引擎节点中除了第一引擎节点之外的至少一个引擎节点发送第六信息,第六信息用于指示第一数据流未重组完成且第一数据流的主处理节点为第一引擎节点。

通过上述两种实现方式中,在缓存有效期内,如果第一引擎节点确定主处理节点是其他引擎节点(即第三引擎节点),则第一引擎节点将第二报文发送给第三引擎节点;或者,如果第一引擎节点确定主处理节点是自身,则第一引擎节点对第三报文以及缓冲区内的报文进行流重组。

在一种可能的实现方式中,第一信息用于指示第一数据流未重组完成且第一数据流的主处理节点为第三引擎节点,第一引擎节点还可以接收第二报文,第二报文属于第一数据流;根据第一信息向第三引擎节点发送第二报文。

通过上述方式中,第一信息也可以指示主处理节点为第三引擎节点,这样第一引擎节点可以直接向该第三引擎节点发送第二报文。

第二方面,本申请提供一种数据处理方法,该方法可以由防火墙系统执行。该防火墙系统中包括多个引擎节点,该多个引擎节点中包括第一引擎节点和第二引擎节点。该方法可以包括:

第二引擎节点,将待发送的M个消息进行存储,以及向多个引擎节点中除了第二引擎节点之外的至少一个引擎节点发送M个消息;其中,M个消息包括如下一项或多项:第一会话表、或者与流重组相关的第一信息,M为正整数;

第一引擎节点,为第二引擎节点创建第一位表文件,在第一位表文件指示M个消息中的N个消息未接收到的情况下,向第二引擎节点发送请求消息;其中,第一位表文件用于指示第一引擎节点对M个消息中的每个消息的接收情况,请求消息用于请求N个消息,N为小于或等于M的正整数;

第二引擎节点,接收来自第一引擎节点的请求消息,以及向第一引擎节点发送N个消息;

第一引擎节点,接收来自第二引擎节点的N个消息,并修改第一位表文件,修改后的第一位表文件用于指示M个消息均已接收。

在一种可能的实现方式中,在向多个引擎节点中除了第二引擎节点之外的至少一个引擎节点发送M个消息时,第二引擎节点将该M个消息写入缓冲区;在满足第二条件的情况下,向多个引擎节点中除了第二引擎节点之外的至少一个引擎节点发送M个消息,其中,第二条件包括如下一项或多项:M个消息的数据量大于或等于第三阈值、或者M个消息的缓存时间大于或等于第四阈值。

在一种可能的实现方式中,第一引擎节点还可以将待发送的H个消息进行存储,H个消息包括如下一项或多项:第二会话表、或者与流重组相关的第二信息,H为正整数;向多个引擎节点中除了第一引擎节点之外的至少一个引擎节点发送H个消息。多个引擎节点中除了第一引擎节点之外的至少一个引擎节点还可以接收该H个消息。

在一种可能的实现方式中,第一引擎节点还可以将待发送的H个消息进行存储,H个消息包括如下一项或多项:第二会话表、或者与流重组相关的第二信息,H为正整数;向多个引擎节点中除了第一

引擎节点之外的至少一个引擎节点发送 H 个消息。

在一种可能的实现方式中,在向多个引擎节点中除了第一引擎节点之外的至少一个引擎节点发送 H 个消息时,第一引擎节点可以将 H 个消息写入缓冲区;在满足第一条件的情况下,向多个引擎节点中除了第一引擎节点之外的至少一个引擎节点发送 H 个消息,其中,第一条件包括如下一项或多项: H 个消息的数据量大于或等于第一阈值、或者 H 个消息的缓存时间大于或等于第二阈值。

在一种可能的实现方式中,第一引擎节点还可以接收第一报文,第一报文属于第一会话;在第一会话为新建会话的情况下,根据第一会话的连接方向和访问控制列表确定是否允许第一报文的访问。

在一种可能的实现方式中,在第一会话表中不包括第一会话的标识,或者第一会话表中包括第一会话的标识和第三信息,该第三信息用于指示第一会话的连接方向不确定的情况下,第一引擎节点还可以修改第一会话表,其中,修改后的第一会话表中包括第一会话的标识、第四信息以及第一会话的连接方向,第四信息用于指示第一会话的连接方向确定;向多个引擎节点中除了第一引擎节点之外的至少一个引擎节点发送修改后的第一会话表。多个引擎节点中除了第一引擎节点之外的至少一个引擎节点还可以接收该修改后的第一会话表。

在一种可能的实现方式中,第一引擎节点还可以接收第一报文,第一报文属于第一会话;在第一会话不是新建会话的情况下,根据第一会话表确定第一会话的连接方向,其中,第一会话表中不包括第一会话的标识,第一会话的连接方向为第一报文的发送方向;根据第一会话的连接方向和访问控制列表确定是否允许第一报文的访问;修改第一会话表,其中,修改后的第一会话表中包括第一会话的标识以及第三信息,第三信息用于指示第一会话的连接方向不确定;向多个引擎节点中除了第一引擎节点之外的至少一个引擎节点发送修改后的第一会话表。多个引擎节点中除了第一引擎节点之外的至少一个引擎节点还可以接收该修改后的第一会话表。

在一种可能的实现方式中,第一引擎节点还可以接收第一报文,第一报文属于第一会话;在第一会话不是新建会话的情况下,根据第一会话表确定第一会话的连接方向;根据第一会话的连接方向和访问控制列表确定是否允许第一报文的访问;其中,第一会话表包括第一会话的标识、第四信息和第一会话的连接方向,第四信息用于指示第一会话的连接方向确定;或者,第一会话表包括第一会话的标识和第三信息,第三信息用于指示第一会话的连接方向不确定,第一会话的连接方向包括第一报文的正反两个方向。其中,第一报文的正反两个方向可以包括第一报文的发送方向和第一报文的发送方向的反(或逆)方向。

在一种可能的实现方式中,第一引擎节点还可以接收第二报文,第二报文属于第一数据流;在第二报文为第一数据流中的第一个报文的情况下,对第二报文进行流重组处理;在第一数据流重组完成的情况下,向多个引擎节点中除了第一引擎节点之外的至少一个引擎节点发送第五信息,第五信息用于指示第一数据流重组完成;或者,在第一数据流未重组完成的情况下,向多个引擎节点中除了第一引擎节点之外的至少一个引擎节点发送第六信息,第六信息用于指示第一数据流未重组完成且第一数据流的主处理节点为第一引擎节点。该多个引擎节点中除了第一引擎节点之外的至少一个引擎节点还可以接收第五信息或第六信息。

在一种可能的实现方式中,第一信息中不包括第一数据流的信息,第一引擎节点还可以接收第二报文,第二报文属于第一数据流;在第二报文不是第一数据流中的第一个报文的情况下,根据第一信息确定第一数据流未重组完成以及第一数据流的主处理节点不存在;缓存第二报文。

在一种可能的实现方式中,该多个引擎节点还包括第三引擎节点,第三引擎节点可以向该多个引擎节点中除了第三引擎节点之外的至少一个引擎节点发送第七信息,第七信息用于指示第一数据流未重组完成且第一数据流的主处理节点为第三引擎节点;第一引擎节点接收第七信息;向第三引擎节点发送第二报文。第三引擎节点接收第二报文,对第二报文进行流重组。

在另一种可能的实现方式中,第一引擎节点还可以接收第三报文,第三报文属于第一数据流;在第三报文是第一数据流中的第一个报文的情况下,对第二报文和第三报文进行流重组处理;在第一数据流重组完成的情况下,向多个引擎节点中除了第一引擎节点之外的至少一个引擎节点发送第五信息,第五信息用于指示第一数据流重组完成;或者,在第一数据流未重组完成的情况下,向多个引擎节点中除了第一引擎节点之外的至少一个引擎节点发送第六信息,第六信息用于指示第一数据流未重组完成且第一数据流的主处理节点为第一引擎节点。该多个引擎节点中除了第一引擎节点之外的至少一个引擎节点还可以接收第五信息或第六信息。

在一种可能的实现方式中,该多个引擎节点还包括第三引擎节点,第一信息用于指示第一数据流未重组完成且第一数据流的主处理节点为第三引擎节点。第一引擎节点还可以接收第二报文,第二报文属于第一数据流;根据第一信息向第三引擎节点发送第二报文。第三引擎节点可以接收第二报文,对第二报文进行流重组。

- 5 第三方面,本申请提供一种数据处理装置,该数据处理装置应用于分布式防火墙系统中的第一引擎节点,该分布式防火墙系统包括多个引擎节点,该第一引擎节点属于该多个引擎节点。例如,该数据处理装置可以执行上述第一方面及其任一种可能的实现方式中所述的方法。该数据处理装置可以包括处理模块、发送模块和接收模块。其中,处理模块也可以称为处理单元、逻辑单元等。发送模块也可以称为发送单元。接收模块也可以称为接收单元。发送模块和接收模块也可以统称为收发模块(或收发单元)、通信模块(或通信单元)、或接口电路等。

其中,所述处理模块,用于为第二引擎节点创建第一位表文件,其中,所述第一位表文件用于指示所述第一引擎节点对所述第二引擎节点的M个消息中的每个消息的接收情况,所述M个消息包括如下

10 一项或多项:第一会话表、或者与流重组相关的第一信息,所述第二引擎节点属于所述多个引擎节点,所述M为正整数;

- 15 所述发送模块,用于在所述第一位表文件指示所述M个消息中的N个消息未接收到的情况下,向所述第二引擎节点发送请求消息,其中,所述请求消息用于请求所述N个消息,所述N为小于或等于所述M的正整数;

所述接收模块,用于接收来自所述第二引擎节点发送的所述N个消息;

- 20 所述处理模块,还用于修改所述第一位表文件,修改后的第一位表文件用于指示所述M个消息均已接收。

在一种可能的实现方式中,处理模块,还用于将待发送的H个消息进行存储,H个消息包括如下

25 一项或多项:第二会话表、或者与流重组相关的第二信息,H为正整数;发送模块,还用于向多个引擎节点中除了第一引擎节点之外的至少一个引擎节点发送H个消息。

- 在一种可能的实现方式中,在向多个引擎节点中除了第一引擎节点之外的至少一个引擎节点发送H个消息时,处理模块,用于将H个消息写入缓冲区;发送模块,用于在满足第一条件的情况下向多个引擎节点中除了第一引擎节点之外的至少一个引擎节点发送该H个消息,其中,第一条件包括如下
- 30 一项或多项:H个消息的数据量大于或等于第一阈值、或者H个消息的缓存时间大于或等于第二阈值。

在一种可能的实现方式中,接收模块,还用于接收第一报文,第一报文属于第一会话;处理模块,还用于在第一会话为新建会话的情况下,根据第一会话的连接方向和访问控制列表确定是否允许第一报文的访问。

- 35 在一种可能的实现方式中,处理模块,还用于在第一会话表中不包括第一会话的标识,或者第一会话表中包括第一会话的标识和第三信息,该第三信息用于指示第一会话的连接方向不确定的情况下,修改第一会话表,其中,修改后的第一会话表中包括第一会话的标识、第四信息以及第一会话的连接方向,第四信息用于指示第一会话的连接方向确定;发送模块,还用于向多个引擎节点中除了第一引擎节点之外的至少一个引擎节点发送修改后的第一会话表。

- 在一种可能的实现方式中,接收模块,还用于接收第一报文,第一报文属于第一会话;处理模块,还用于在第一会话不是新建会话的情况下,根据第一会话表确定第一会话的连接方向,其中,第一会话表中不包括第一会话的标识,第一会话的连接方向为第一报文的发送方向;根据第一会话的连接方向和访问控制列表确定是否允许第一报文的访问;以及,修改第一会话表,其中,修改后的第一会话表中
- 40 包括第一会话的标识以及第三信息,第三信息用于指示第一会话的连接方向不确定;发送模块,还用于向多个引擎节点中除了第一引擎节点之外的至少一个引擎节点发送修改后的第一会话表。

- 在一种可能的实现方式中,接收模块,还用于接收第一报文,第一报文属于第一会话;处理模块,还用于在第一会话不是新建会话的情况下,根据第一会话表确定第一会话的连接方向,以及根据第一会话的连接方向和访问控制列表确定是否允许第一报文的访问;其中,第一会话表包括第一会话的标识、第四信息和第一会话的连接方向,第四信息用于指示第一会话的连接方向确定;或者,第一会话表包括第一会话的标识和第三信息,第三信息用于指示第一会话的连接方向不确定,第一会话的连接方向包括第一报文的正反两个方向。其中,第一报文的正反两个方向可以包括第一报文的发送方向和第一报文的发送方向的反(或逆)方向。
- 45

在一种可能的实现方式中,接收模块,还用于接收第二报文,第二报文属于第一数据流;处理模块,还用于在第二报文为第一数据流中的第一个报文的情况下,对第二报文进行流重组处理;发送模块,还用于在第一数据流重组完成的情况下,向多个引擎节点中除了第一引擎节点之外的至少一个引擎节点发送第五信息,第五信息用于指示第一数据流重组完成;或者,发送模块,还用于在第一数据流未重组完成的情况下,向多个引擎节点中除了第一引擎节点之外的至少一个引擎节点发送第六信息,第六信息用于指示第一数据流未重组完成且第一数据流的主处理节点为第一引擎节点。

在一种可能的实现方式中,数据处理装置还可以包括存储模块,第一信息中不包括第一数据流的信息,接收模块,还用于接收第二报文,第二报文属于第一数据流;处理模块,还用于在第二报文不是第一数据流中的第一个报文的情况下,根据第一信息确定第一数据流未重组完成以及第一数据流的主处理节点不存在;存储模块,用于缓存第二报文。

在一种可能的实现方式中,接收模块,该用于接收第七信息,第七信息用于指示第一数据流未重组完成且第一数据流的主处理节点为第三引擎节点,第三引擎节点属于多个引擎节点;发送模块,还用于向第三引擎节点发送第二报文。

在另一种可能的实现方式中,接收模块,还用于接收第三报文,第三报文属于第一数据流;处理模块,还用于在第三报文是第一数据流中的第一个报文的情况下,对第二报文和第三报文进行流重组处理;发送模块,还用于在第一数据流重组完成的情况下,向多个引擎节点中除了第一引擎节点之外的至少一个引擎节点发送第五信息,第五信息用于指示第一数据流重组完成;或者,发送模块,还用于在第一数据流未重组完成的情况下,向多个引擎节点中除了第一引擎节点之外的至少一个引擎节点发送第六信息,第六信息用于指示第一数据流未重组完成且第一数据流的主处理节点为第一引擎节点。

在一种可能的实现方式中,第一信息用于指示第一数据流未重组完成且第一数据流的主处理节点为第三引擎节点,接收模块,还用于接收第二报文,第二报文属于第一数据流;发送模块,还用于根据第一信息向第三引擎节点发送第二报文。

第四方面,本申请提供一种分布式防火墙系统,该分布式防火墙系统中包括多个引擎节点,该多个引擎节点中包括第一引擎节点和第二引擎节点,其中:

第二引擎节点,用于将待发送的M个消息进行存储,以及向多个引擎节点中除了第二引擎节点之外的至少一个引擎节点发送M个消息;其中,M个消息包括如下一项或多项:第一会话表、或者与流重组相关的第一信息,M为正整数;

第一引擎节点,用于为第二引擎节点创建第一位表文件,在第一位表文件指示M个消息中的N个消息未接收到的情况下,向第二引擎节点发送请求消息;其中,第一位表文件用于指示第一引擎节点对M个消息中的每个消息的接收情况,请求消息用于请求N个消息,N为小于或等于M的正整数;

第二引擎节点,还用于接收来自第一引擎节点的请求消息,以及向第一引擎节点发送N个消息;

第一引擎节点,还用于接收来自第二引擎节点的N个消息,并修改第一位表文件,修改后的第一位表文件用于指示M个消息均已接收。

在一种可能的实现方式中,在向多个引擎节点中除了第二引擎节点之外的至少一个引擎节点发送M个消息时,第二引擎节点,用于将该M个消息写入缓冲区;在满足第二条件的情况下,向多个引擎节点中除了第二引擎节点之外的至少一个引擎节点发送M个消息,其中,第二条件包括如下一项或多项:M个消息的数据量大于或等于第三阈值、或者M个消息的缓存时间大于或等于第四阈值。

在一种可能的实现方式中,第一引擎节点,还用于将待发送的H个消息进行存储,H个消息包括如下一项或多项:第二会话表、或者与流重组相关的第二信息,H为正整数;向多个引擎节点中除了第一引擎节点之外的至少一个引擎节点发送H个消息。多个引擎节点中除了第一引擎节点之外的至少一个引擎节点,还用于接收该H个消息。

在一种可能的实现方式中,第一引擎节点,还用于将待发送的H个消息进行存储,H个消息包括如下一项或多项:第二会话表、或者与流重组相关的第二信息,H为正整数;向多个引擎节点中除了第一引擎节点之外的至少一个引擎节点发送H个消息。

在一种可能的实现方式中,在向多个引擎节点中除了第一引擎节点之外的至少一个引擎节点发送H个消息时,第一引擎节点,用于将H个消息写入缓冲区;在满足第一条件的情况下,向多个引擎节点中除了第一引擎节点之外的至少一个引擎节点发送H个消息,其中,第一条件包括如下一项或多项:H个消息的数据量大于或等于第一阈值、或者H个消息的缓存时间大于或等于第二阈值。

在一种可能的实现方式中，第一引擎节点，还用于接收第一报文，第一报文属于第一会话；在第一会话为新建会话的情况下，根据第一会话的连接方向和访问控制列表确定是否允许第一报文的访问。

在一种可能的实现方式中，在第一会话表中不包括第一会话的标识，或者第一会话表中包括第一会话的标识和第三信息，该第三信息用于指示第一会话的连接方向不确定的情况下，第一引擎节点，还用于修改第一会话表，其中，修改后的第一会话表中包括第一会话的标识、第四信息以及第一会话的连接方向，第四信息用于指示第一会话的连接方向确定；向多个引擎节点中除了第一引擎节点之外的至少一个引擎节点发送修改后的第一会话表。多个引擎节点中除了第一引擎节点之外的至少一个引擎节点，还用于接收该修改后的第一会话表。

在一种可能的实现方式中，第一引擎节点，还用于接收第一报文，第一报文属于第一会话；在第一会话不是新建会话的情况下，根据第一会话表确定第一会话的连接方向，其中，第一会话表中不包括第一会话的标识，第一会话的连接方向为第一报文的发送方向；根据第一会话的连接方向和访问控制列表确定是否允许第一报文的访问；修改第一会话表，其中，修改后的第一会话表中包括第一会话的标识以及第三信息，第三信息用于指示第一会话的连接方向不确定；向多个引擎节点中除了第一引擎节点之外的至少一个引擎节点发送修改后的第一会话表。多个引擎节点中除了第一引擎节点之外的至少一个引擎节点，还用于接收该修改后的第一会话表。

在一种可能的实现方式中，第一引擎节点，还用于接收第一报文，第一报文属于第一会话；在第一会话不是新建会话的情况下，根据第一会话表确定第一会话的连接方向；根据第一会话的连接方向和访问控制列表确定是否允许第一报文的访问；其中，第一会话表包括第一会话的标识、第四信息和第一会话的连接方向，第四信息用于指示第一会话的连接方向确定；或者，第一会话表包括第一会话的标识和第三信息，第三信息用于指示第一会话的连接方向不确定，第一会话的连接方向包括第一报文的正反两个方向。其中，第一报文的正反两个方向可以包括第一报文的发送方向和第一报文的发送方向的反（或逆）方向。

在一种可能的实现方式中，第一引擎节点，还用于接收第二报文，第二报文属于第一数据流；在第二报文为第一数据流中的第一个报文的情况下，对第二报文进行流重组处理；在第一数据流重组完成的情况下，向多个引擎节点中除了第一引擎节点之外的至少一个引擎节点发送第五信息，第五信息用于指示第一数据流重组完成；或者，在第一数据流未重组完成的情况下，向多个引擎节点中除了第一引擎节点之外的至少一个引擎节点发送第六信息，第六信息用于指示第一数据流未重组完成且第一数据流的主处理节点为第一引擎节点。该多个引擎节点中除了第一引擎节点之外的至少一个引擎节点，还用于接收第五信息或第六信息。

在一种可能的实现方式中，第一信息中不包括第一数据流的信息，第一引擎节点，还用于接收第二报文，第二报文属于第一数据流；在第二报文不是第一数据流中的第一个报文的情况下，根据第一信息确定第一数据流未重组完成以及第一数据流的主处理节点不存在；缓存第二报文。

在一种可能的实现方式中，该多个引擎节点还包括第三引擎节点，第三引擎节点，用于向该多个引擎节点中除了第三引擎节点之外的至少一个引擎节点发送第七信息，第七信息用于指示第一数据流未重组完成且第一数据流的主处理节点为第三引擎节点；第一引擎节点，还用于接收第七信息；向第三引擎节点发送第二报文。第三引擎节点，还用于接收第二报文，对第二报文进行流重组。

在另一种可能的实现方式中，第一引擎节点，还用于接收第三报文，第三报文属于第一数据流；在第三报文是第一数据流中的第一个报文的情况下，对第二报文和第三报文进行流重组处理；在第一数据流重组完成的情况下，向多个引擎节点中除了第一引擎节点之外的至少一个引擎节点发送第五信息，第五信息用于指示第一数据流重组完成；或者，在第一数据流未重组完成的情况下，向多个引擎节点中除了第一引擎节点之外的至少一个引擎节点发送第六信息，第六信息用于指示第一数据流未重组完成且第一数据流的主处理节点为第一引擎节点。该多个引擎节点中除了第一引擎节点之外的至少一个引擎节点，还用于接收第五信息或第六信息。

在一种可能的实现方式中，该多个引擎节点还包括第三引擎节点，第一信息用于指示第一数据流未重组完成且第一数据流的主处理节点为第三引擎节点。第一引擎节点，还用于接收第二报文，第二报文属于第一数据流；根据第一信息向第三引擎节点发送第二报文。第三引擎节点，还用于接收第二报文，对第二报文进行流重组。

第五方面，本申请提供一种数据处理装置，该数据处理装置包括处理器，所述处理器用于读取存储

器中存储的计算机程序或指令并执行,以使得该计算设备执行上述第一方面及其任一种可能的实现方式中所述的方法。可选地,该数据处理装置还可以包括该存储器,所述存储器存储有计算机程序或指令。

第六方面,本申请提供一种计算设备,该计算设备包括至少一个处理器和通信接口,所述至少一个处理器用于通过所述通信接口读取并执行指令,使得所述计算设备执行上述第一方面及其任一种可能的实现方式中所述的方法。

第七方面,本申请还提供一种计算设备集群,包括至少一个计算设备,每个计算设备包括处理器和存储器;所述至少一个计算设备的处理器用于执行所述至少一个计算设备的存储器中存储的指令,以使得所述计算设备集群执行上述第二方面及其任一种可能的实现方式中所述的方法。

第八方面,本申请还提供一种芯片系统,所述芯片系统包括至少一个处理器,用于执行所述存储器中的一个或多个计算机程序或指令,以实现上述第一方面或第二方面及其任一种可能的实现方式中所述的方法。可选地,所述至少一个处理器与存储器耦合。

第九方面,本申请还提供一种计算机程序产品,包含有计算机可执行指令,该计算机可执行指令用于使计算设备执行上述第一方面或第二方面及其任一种可能的实现方式中所述的方法。

第十方面,本申请还提供一种计算机可读存储介质,所述计算机可读存储介质内存储有计算机可执行指令,该计算机可执行指令用于使计算设备执行上述第一方面或第二方面及其任一种可能的实现方式中所述的方法。

上述第二方面至第十方面中任一方面及其任一种可能的实现方式可以达到的技术效果可以参照上述第一方面及其任一种可能的实现方式中有益效果的描述,此处不再重复赘述。

附图说明

- 图 1a 为本申请实施例提供的一种分布式防火墙系统的结构示意图;
- 图 1b 为本申请实施例提供的另一种分布式防火墙系统的结构示意图;
- 图 2 为本申请实施例提供的第一种数据处理方法的流程示意图;
- 图 3 为本申请实施例提供的一种数据共享的示意图;
- 图 4 为本申请实施例提供的第二种数据处理方法的流程示意图;
- 图 5 为本申请实施例提供的第三种数据处理方法的流程示意图;
- 图 6 为本申请实施例提供的一种数据处理装置的结构示意图;
- 图 7 为本申请实施例提供的一种计算设备的结构示意图;
- 图 8 为本申请实施例提供的一种计算设备集群的结构示意图;
- 图 9 为本申请实施例提供的另一种计算设备集群的结构示意图。

具体实施方式

本申请实施例将围绕包括多个设备、组件、模块等的系统来呈现。应当理解的是,该系统可以包括其它未提及的设备、组件、模块等,也可以仅包括实施例中提及的部分设备、组件、或模块等。

本申请实施例中“多个”可以是指两个或两个以上,鉴于此,本申请实施例中也可以将“多个”理解为“至少两个”。“至少一个”,可理解为一个或多个,例如理解为一个、两个或多个。例如,“包括至少一个”,是指包括一个、两个或多个,例如,包括 A、B 和 C 中的至少一个,那么包括的可以是 A、B、C、A 和 B、A 和 C、B 和 C、或 A、B 和 C。“和/或”,描述关联对象的关联关系,具体可以存在三种关系,例如, A 和/或 B,可以表示:单独存在 A,同时存在 A 和 B,单独存在 B 这三种情况。另外,字符“/”,如无特殊说明,一般表示前后关联对象是一种“或”的关系。

本申请实施例提及的“第一”、“第二”等序数词通常用于对不同对象进行区分,不用于限定多个对象的顺序、时序、优先级或者重要程度等。例如,本申请实施例涉及的第一引擎节点和第二引擎节点用于对不同的引擎节点进行区别,不用于限定这两个引擎节点的顺序、时序、优先级或者重要程度等。

本申请实施例可以应用于防火墙系统。防火墙系统可以由负载均衡节点和多个引擎节点组成。负载均衡节点主要负责多个引擎节点的流量均衡等,引擎节点主要根据安全策略控制报文的访问。目前,防火墙系统包括引擎节点主要是基于会话的相关信息(例如,会话列表)控制会话的访问。防火墙系统进行扩容、缩容、或引擎节点发生故障时,会导致部分会话重新分发到其他引擎节点,由于该其他引擎节

点没有这部分会话的相关信息,这样就会导致该会话的中断,从而影响业务的正常传输。

鉴于此,本申请实施例提供一种数据处理方法、装置及分布式防火墙系统,用以减少防火墙系统进行扩容、缩容或引擎节点发生故障时对业务的影响。其中,本申请所述方法和装置基于同一技术构思,由于方法及装置解决问题的原理相似,因此装置与方法的实施可以相互参见,重复之处不再赘述。

5 在介绍本申请实施例提供的数据处理方法之前,下面先介绍本申请实施例提供的分布式防火墙系统。

图 1a 和图 1b 示出了本申请实施例提供的分布式防火墙系统(也可以简称为防火墙系统、或防火墙)的架构示意图。如图 1a 或图 1b 所示,分布式防火墙系统部署于网络边界,是内部网络和外部网络(例如,因特网(internet)等)之间的连接桥梁。分布式防火墙系统可以将内部网络和外部网络分开,对网络边界的数据进行访问控制,防止非法访问、恶意入侵等,能够保障内部网络数据的安全。如图 1a 或图 1b 所示,分布式防火墙系统可以包括多个引擎节点。该多个引擎节点之间可以进行通信。本申请实施例对分布式防火墙系统中所包括的引擎节点的数量不做限定。图 1a 或图 1b 中以第一引擎节点、第二引擎节点以及第三引擎节点为例示出。

引擎节点,也可以称为端节点、节点等,本申请实施例对引擎节点的命名不做限定。引擎节点主要根据安全策略(例如,会话列表、访问控制列表(access control list, ACL)等)控制报文的访问。例如,引擎节点可以根据安全策略确定是否允许报文的访问;如果引擎节点根据安全策略确定允许该报文的访问,则引擎节点转发该报文;如果引擎节点根据安全策略确定不允许该报文的访问,则引擎节点丢弃该报文。该引擎节点的功能可以由计算机设备、服务器、云服务器、物理机或虚拟机等实现。本申请实施例对引擎节点的功能以及实现形式不做限定。

20 可选地,该分布式防火墙系统还可以包括负载均衡节点,图 1a 和图 1b 中以虚线表示。该负载均衡节点可以与该多个引擎节点进行通信。

负载均衡节点,也可以称为负载均衡设备,本申请实施例对负载均衡节点的命名不做限定。负载均衡节点主要负责业务数据分发、以及多个引擎节点间的流量均衡等。该负载均衡节点的功能可以由计算机设备、服务器、云服务器、物理机或虚拟机等实现。本申请实施例对负载均衡节点的功能以及实现形式不做限定。

25 可选地,该分布式防火墙系统还可以包括控制节点,图 1a 和图 1b 中未示出。该控制节点可以与多个引擎节点之间进行通信。该控制节点还可以与负载均衡节点进行通信。控制节点,也可以称为控制中心等,本申请实施例对控制节点的命名不做限定。控制节点主要负责对多个引擎节点和/或负载均衡节点下发配置信息,例如,配置访问控制列表(access control list, ACL)、负载均衡策略等。该控制节点的功能可以由计算机设备、服务器、云服务器、物理机或虚拟机等实现。本申请实施例对控制节点的功能以及实现形式不做限定。

30 其中,报文,是网络中用于交换和传输数据的单元,即站点一次性要发送的数据块。本申请实施例中的报文可以是基于传输控制协议/网际互连协议(transmission control protocol/internet protocol, TCP/IP)的报文。例如,报文可以为 TCP 报文,也可以为 IP 报文,还可以为因特网控制消息协议(internet control message protocol, ICMP)报文等,不予限制。当需要传输的数据较大时,报文分段技术可以将该数据切分成多个较小的数据段进行传输,以提高传输效率。数据切分行为发生在使用 TCP 的传输层中可以称为 TCP 分段或分段。数据切分行为发生在使用 IP 的网络 IP 层中可以称为 IP 分片或分片。TCP 分段和 IP 分片皆可以通过流重组处理获得完整的数据流。流重组,是指把同一条 TCP 或 IP 流的报文按照顺序进行组合,解析出应用层的数据流。

40 会话,是指一次网络连接的开始和结束之间的时间段,包括了从会话发起端发起连接请求到会话响应端响应请求的整个过程。一个会话包括由双向流组成的多个报文。以 TCP 报文为例,交换五元组中的源和目的之后具有相同的五元组的多个报文属于同一个会话。五元组包括源 IP、目的 IP、源端口、目的端口和协议号。会话方向,也可以称为会话的连接方向、或报文的连接方向等,不予限制。该会话的连接方向可以指从会话发起端到会话响应端的方向。

45 图 1b 所示的分布式防火墙系统相较于图 1a 所示的分布式防火墙系统,区别在于:分布式防火墙系统中的每个引擎节点中可以包括消息广播模块、会话处理模块和流重组模块。其中:

消息广播模块可以用于实现引擎节点的发送动作和/或接收动作,协助会话处理模块实现引擎节点对报文的访问控制,以及协助流重组模块实现引擎节点对报文分段或报文分片进行流重组处理。例如,消息广播模块可以向分布式防火墙系统中的其他引擎节点发送会话表,意味着分布式防火墙系统中的多

个引擎节点之间可以共享会话表,这样该消息广播模块所在的引擎节点负责的会话也可以由其他节点提供服务。例如,消息广播模块可以向分布式防火墙系统中的其他引擎节点发送与流重组相关的信息,意味着分布式防火墙系统中的多个引擎节点之间可以与流重组相关的信息,这样该消息广播模块所在的引擎节点负责的一条数据流可以由多个引擎节点协同处理。

会话处理模块,也可以称为会话表模块,可以用于实现引擎节点对报文的访问控制。例如,会话处理模块可以根据会话表(该会话表可以是自身维护的,或者也可以是通过消息广播模块来自其他引擎节点的,不予限制)对接收到的报文进行访问控制。

流重组模块,可以用于实现引擎节点对报文分段或报文分片进行流重组处理。例如,流重组模块可以根据与流重组相关的信息(该与流重组相关的信息可以是自身维护的,或者也可以是通过消息广播模块来自其他引擎节点的,不予限制),对接收到的报文分段(或报文分片)进行流重组处理,或者将接收到的报文分段(或报文分片)通过消息广播模块发送给其他引擎节点进行流重组处理。

需要指出的是,上述多个功能模块可以基于软件、硬件或软件和硬件的结合实现,且多个功能模块可以基于具体实现进行任意组合或分割。另外,本申请实施例提供的分布式防火墙系统还可以包括其他节点,本申请实施例对其实现形式不做限定。

本申请实施例提供的分布式防火墙系统中多个引擎节点之间可以共享会话表和/或与流重组相关的信息等,以减少因分布式防火墙系统进行扩容、缩容、或引擎节点发生故障对业务传输的影响。下面结合图 2 至图 5,以第一引擎节点与第二引擎节点交换的角度以及第一引擎节点的角度对本申请实施例提供的数据处理方法进行介绍。

图 2 示出了本申请实施例提供的第一种数据处理方法的流程示意图。该方法可以应用于图 1a 或图 1b 所示的分布式防火墙系统。如图 2 所示,该方法可以包括如下步骤。

S201: 第二引擎节点将待发送的至少一个消息进行存储。

第二引擎节点可以将待发送的至少一个消息写入文件(或数据文件)。其中,写入文件可以理解为进行存储、或写入硬盘(或磁盘、或内存等)。为了便于理解,后文中将第二引擎节点待发送的至少一个消息记为 M 个消息,M 为正整数为例进行描述。图 2 中以第二引擎节点将待发送的 M 个消息进行存储为例示出。该 M 个消息可以理解为第二引擎节点共享给分布式防火墙系统中的其他引擎节点的消息。该消息可以理解为如下一项或多项:信息、表格、文本或数据等。

本申请实施例中,该 M 个消息可以包括第一会话表,或者包括与流重组相关的第一信息,或者包括第一会话表和与流重组相关的第一信息。其中,该第一会话表可以包括至少一个会话的信息。该至少一个会话的信息可以包括:至少一个会话的标识和用于指示该至少一个会话表中的每个会话的连接方向是否确定的指示信息。进一步地,如果指示信息指示会话的连接方向是确定的,该至少一个会话的信息中还可以包括该会话的连接方向,如表 1 所示。表 1 中以第一会话表包括三个会话为例示出。应理解的是,至少一个会话的信息还可以包括其他内容,本申请实施例对此不做限定。

表 1

会话的标识	会话的连接方向是否确定	会话的连接方向
会话 1	不确定	
会话 2	确定	A 到 B
会话 3	不确定	

与流重组相关的第一信息可以包括至少一个数据流的标识以及用于指示该至少一个数据流中的每个数据流是否处理完成的指示信息。可选地,该第一信息还可以包括数据流的主处理节点的标识,如表 2 所示。表 2 中以三个数据流为例示出。应理解的是,第一信息还可以包括其他内容,本申请实施例对此不做限定。

表 2

数据流的标识	是否处理完成	主处理节点
数据流 1	完成	
数据流 2	未完成	引擎节点 1
数据流 3	未完成	

需要指出的是，该 M 个消息也可以包括第一会话表的部分内容，和/或包括第一信息的部分内容。为了便于理解，本申请实施例以 M 个消息包括第一会话表和/或第一信息为例进行描述。

5 S202: 第二引擎节点发送 M 个消息。例如，第二引擎节点可以向分布式防火墙系统中除了第二引擎节点之外的至少一个引擎节点发送 M 个消息。例如，第二引擎节点中的消息广播模块发送该 M 个消息。

10 示例性地，第二引擎节点可以将 M 个消息写入文件，并复制一份发送给分布式防火墙系统中除了第二引擎节点之外的至少一个引擎节点。一种实施方式中，第二引擎节点可以将该 M 个消息进行缓冲（或缓存）；或者，第二引擎节点可以将该 M 个消息写入缓冲区（或缓存区）。即，第二引擎节点将 M 个消息写入文件和缓冲区。进一步地，在满足第二条件的情况下，第二引擎节点可以向分布式防火墙系统中除了第二引擎节点之外的至少一个引擎节点发送该 M 个消息。第二条件可以包括 M 个消息的数据量大于或等于第三阈值，或者包括 M 个消息的缓存时长大于或等于第四阈值，或者包括 M 个消息的数据量大于或等于第三阈值和 M 个消息的缓存时长大于或等于第四阈值。其中，第三阈值和第四阈值均
15 可以是预先设定的，不予限制。例如，第三阈值可以为 1.3 KB，不予限制。例如，第四阈值可以为 100 微秒，不予限制。

一种实施方式中，第二引擎节点可以确定该 M 个消息的序号。例如，第二引擎节点可以根据 M 个消息写入文件的时间（或时间戳）和该 M 个消息写入文件的偏移确定该 M 个消息的序号。其中，该 M 个消息写入文件的时间可以记为第一时间，或第一时间戳。

20 一种实施方式中，分布式防火墙系统（或者说第二引擎节点）可以具备过期机制。例如，当 M 个消息中的任一个消息的存储时长超过设定阈值，则第二引擎节点可以删除存储时长超过设定阈值的至少一个消息。例如，第一引擎节点可以从文件和/或缓冲区内删除该至少一个消息，以减少存储资源的浪费。

25 可选地，第二引擎节点可以通过用户数据报协议（user datagram protocol，UDP）向至少一个引擎节点发送该 M 个消息，这样可以保证数据传输的实时性。在分布式防火墙系统包括三个或三个以上的引擎节点的情况下，第二引擎节点可以通过 UDP 组播的方式向分布式防火墙系统中除了第二引擎节点之外的多个引擎节点发送该 M 个消息，以节省网络传输资源；或者，第二引擎节点也可以通过 UDP 单播的方式逐一向分布式防火墙系统中除了第二引擎节点之外的多个引擎节点发送该 M 个消息，以适应不支持 UDP 组播的网络环境。

30 通过上述 S201 和 S202，分布式防火墙系统中的多个引擎节点间可以实现数据共享（或数据同步）。一种实施方式中，分布式防火墙系统中的多个引擎节点可以共享同一个关键字键值（key value，KV）结构，具备本地内存级的读写速度，且任意引擎节点写入的数据全局皆可以读取。该 KV 结构例如可以为哈希（hash）表，但并不限于此。例如，引擎节点更新（或修改）hash 表，该引擎节点可以将更新内容或更新后的 hash 表发送给其他引擎节点。举例而言，如图 3 所示，引擎节点 1 的数据 1 先写入文件（图 3 中未示出）和本地缓冲区 1 中，再发送给引擎节点 2 和引擎节点 3；引擎节点 2 的数据 2 先写入文件（图 3 中未示出）和本地缓冲区 1 中，再发送给引擎节点 1 和引擎节点 3；引擎节点 3 的数据 3 先写入文件（图 3 中未示出）和本地缓冲区 1 中，再发送给引擎节点 1 和引擎节点 2；这样，引擎节点 1、引擎节点 2 和引擎节点 3 均可以使用数据 1、数据 2 和数据 3。可以理解的是，引擎节点的本地缓冲区可以部署在该引擎节点外部，也可以部署在该引擎节点内部，不予限制。图 3 中以引擎节点 1、引擎
35 节点 2 以及引擎节点 3 三者通过总线（图 3 中以黑粗线标识）相互通信为例示出。
40 需要指出的是，第二引擎节点可以向分布式防火墙系统中除了第二引擎节点之外的至少一个引擎节点

点发送 M 个消息，该至少一个引擎节点可以包括第一引擎节点，或者也可以不包括第一引擎节点。例如，第一引擎节点可以是在 S202 之后以及 S203 之前新加入该分布式防火墙系统的引擎节点。

S203: 第一引擎节点为第二引擎节点创建（或构建、或确定、或建立）第一位表文件。

5 第一引擎节点可以为分布式防火墙系统中的除了第一引擎节点之外的至少一个引擎节点中的每个引擎节点创建至少一个位表文件。该分布式防火墙系统中除了第一引擎节点之外的至少一个引擎节点中包括第二引擎节点。第一引擎节点为第二引擎节点创建的至少一个位表文件中包括第一位表文件。该第一引擎节点为第二引擎节点创建的至少一个位表文件可以用于对第二引擎节点发送给第一引擎节点的多个消息进行去重，以及快速确定哪些消息还未接收到。为了便于理解，下文以第一位表文件为例进行介绍，其余位表文件均可以参考第一位表文件的描述。

10 示例性地，第一引擎节点可以响应于接收到来自第二引擎节点的第一个消息，该第一个消息属于该 M 个消息，创建该第一位表文件。或者，第一引擎节点也可以根据其他信息创建该第一位表文件。如果第一引擎节点为新加入的引擎节点，该第一位置文件可以理解为空文件，或者该第一位置文件也可以理解为一个全范围的文件；或者第一引擎节点也可以根据控制节点的配置信息等创建该第一位表文件；或者，第一引擎节点新加入分布式防火墙系统后，可以向分布式防火墙系统中除了第一引擎节点之外的至少一个引擎节点（包括第二引擎节点）发送获取共享信息的请求，在收到相应的消息之后再为至少一个引擎节点创建至少一个位表文件。本申请实施例对第一引擎节点创建第一位表文件的触发条件不做限定。

第一位表文件可以用于指示第一引擎节点对第二引擎节点的 M 个消息中的每个消息的接收情况。可选地，该第一位表文件可以是以第一时间（或第一时间戳）命名的，以表示第一引擎节点在该第一时间内的每个序号所指示的消息的接收情况。其中，第一时间（或第一时间戳）是第二引擎节点将该 M 个消息写入文件的时间。示例性地，该第一位表文件可以包括 M 个消息的序号和用于指示该 M 个消息中的每个消息是否接收到的指示信息，如表 3 所示。表 3 中以三个消息为例示出。

表 3

消息的序号	是否接收到
序号 1	未接收到
序号 2	已接收
序号 3	未接收到

25 在 S202 中，第二引擎节点发送 M 个消息。第一引擎节点每接收到一个消息，可以根据第一位表文件确定该消息是否有接收到。以 M 个消息中的消息 1 为例，如果第一位表文件指示该消息 1 已接收，则第一引擎节点丢弃该消息 1；如果第一位表文件指示该消息 1 未接收到，则第一引擎节点更新该第一位表文件，更新后的第一位表文件指示该消息 1 已接收，以及将消息 1 传递给上层应用处理（如写入会话表，和/或用于流重组等）。第一引擎节点对每接收到的一个消息均按照消息 1 的处理方式进行处理，直至处理完第一引擎节点接收到的最后一个消息。进一步地，第一引擎节点可以周期性地或非周期性地检测第一位表文件，确定该 M 个消息是否都已接收。如果第一位表文件指示该 M 个消息都已接收，则流程结束。如果第一位表文件指示该 M 个消息中的 N 个消息未接收到，则第一引擎节点执行 S204。该 N 为小于或等于 M 的正整数。例如，如果第一引擎节点为新加入的节点，则 N 可以等于 M。本申请实施例以 M 个消息中存在 N 个消息未接收为例进行描述。图 2 的 S202 中用“X”表示该 M 个消息中的 N 个消息未接收到。

30 S204: 在第一位表文件指示 M 个消息中的 N 个消息未接收到的情况下，第一引擎节点向第二引擎节点发送请求消息。相应地，第二引擎节点接收来自第一引擎节点的请求消息。

该请求消息可以用于请求该 N 个消息，或者说，该请求消息可以用于请求该 N 个消息的重传，或者说，该请求消息可以用于获取该 N 个消息。可选地，该请求消息中包括该 N 个消息的序号。例如，40 第一引擎节点可以通过 TCP 协议向第二引擎节点发送该请求消息，不予限制。

S205: 第二引擎节点向第一引擎节点发送 N 个消息。

例如,第二引擎节点接收到请求消息后,根据该请求消息可以向第一引擎节点发送该 N 个消息。第一引擎节点对每接收的一个消息可以按照前述的消息 1 处理。如果该 N 个消息中的部分或全部未接收到,则第一引擎节点执行 S203,直至 N 个消息皆接收到为止。图 2 中以第一引擎节点接收该 N 个消息为例示出。

5 S206: 第一引擎节点修改第一位表文件。

第一引擎节点修改(或更新)第一位表文件。例如,第一引擎节点根据 N 个消息的接收情况修改(或更新)第一位表文件,请参考前述消息 1 的处理方式。修改后的第一位表文件用于指示该 M 个消息均已接收。

图 2 以第一引擎节点作为消息接收方为例进行描述。可选地,第一引擎节点也可以作为消息发送方。一种可能的实现方式中,第一引擎节点可以将待发送的至少一个消息进行存储(或写入文件),以及向分布式防火墙系统中除了第一引擎节点之外的至少一个引擎节点发送该至少一个消息。为了简洁,后文中以第一引擎节点待发送的至少一个消息记为 H 个消息,H 为正整数为例进行描述。其中,H 个消息可以包括第二会话表,或者包括与流重组相关的第二信息,或者包括第二会话表和与流重组相关的第二信息。该 H 个消息请对照参考 M 个消息的描述,该第二会话表请对照参考第一会话表的描述,第二信息请对照参考第一信息的描述,不再赘述。

10 示例性地,第一引擎节点向分布式防火墙系统中除了第一引擎节点之外的至少一个引擎节点发送该 H 个消息可以为:第一引擎节点将该 H 个消息写入缓冲区,并在满足第一条件的情况下向分布式防火墙系统中除了第一引擎节点之外的至少一个引擎节点发送该 H 个消息。其中,第一条件可以包括 H 个消息的数据量大于或等于第一阈值,或者包括 H 个消息的缓存时间大于或等于第二阈值,或者包括 H 个消息的数据量大于或等于第一阈值和包括 H 个消息的缓存时间大于或等于第二阈值。H 为正整数。第一阈值和第二阈值可以预定义的,不予限制。

可选地,第一引擎节点还可以确定该 H 个消息的序号,其实现过程请对照参考第二引擎节点确定 M 个消息的序号的描述,不再赘述。

需要指出的是,图 2 中各个步骤的执行顺序为一种示例,并不限于此。例如,第一引擎节点接收 N 个消息和第一引擎节点修改第一位表文件可以同步进行。

在上述第一种数据处理方法中,分布式防火墙系统中的多个引擎节点可以共享会话表(和/或流重组的信息),这样当分布式防火墙系统扩容(即减少引擎节点的数量)或引擎节点发生故障后,由于其他引擎节点共享有该引擎节点的会话表(和/或流重组的信息),因此,该其他引擎节点可以继续为该引擎节点负责的会话(和/或数据流)提供服务,从而能够减少分布式防火墙系统进行扩容或引擎节点发生故障时对业务的影响。当分布式防火墙系统扩容(即有新的引擎节点加入分布式防火墙系统)时,该引擎节点可以通过上述第一种数据处理方法获取分布式防火墙系统中其他引擎节点的历史数据(即会话表和/或流重组的信息),这样即便为该引擎节点分发其他引擎节点的业务任务该引擎节点也可以根据该历史数据继续为该业务提供服务,从而能够减少分布式防火墙系统进行扩容时对业务的影响。

30 单条会话由一个引擎节点处理,当这条会话的流量较大时,这个引擎节点可能会遭遇大象流攻击,存在单个引擎节点被打爆而导致无法提供服务的风险。本申请上述实施例中,分布式防火墙系统中的多个引擎节点可以共享会话表和/或流重组的信息,意味着一条会话可以分布给多个引擎节点处理,这样可以减少因单条会话流较大而导致单个节点被打爆的风险,使得分布式防火墙系统能够支持更大的单条会话流,从而提高分布式防火墙系统的稳定性。

40 前述提到,分布式防火墙系统中的多个引擎节点之间可以共享会话表,该会话表主要用于控制报文的访问。接下来结合图 4 对其进行介绍。

图 4 示出了本申请实施例提供的第二种数据处理方法的流程示意图。该方法可以应用于图 1a 或图 1b 所示的分布式防火墙系统。如图 4 所示,该方法可以包括如下步骤。

S401: 第一引擎节点接收第一报文。

45 该第一报文属于第一会话。该第一报文可以来自内部网络,或者也可以来自外部网络,不予限制。示例性地,第一引擎节点加入分布式防火墙系统时可以加载配置并构建 ACL 等,并通过上述第一种数据处理方法获取分布式防火墙系统的历史数据得到第一会话表。可选地,第一引擎节点还可以获得第一信息。之后,第一引擎节点启动报文收发流程,接收该第一报文。

S402: 第一引擎节点确定第一会话是否为新建会话。例如,第一引擎节点中的会话处理模块可以

确定第一会话是否为新建会话。

示例性地，第一引擎节点解析第一报文头可以确定第一会话是否为新建会话。例如，第一报文为 TCP 的 syn 报文，则第一引擎节点确定第一会话为新建会话，且确定第一会话的连接方向为第一报文的发送方向。又例如，第一报文为 TCP 的 syn-ack 报文，则第一引擎节点确定第一会话为新建会话，且确定第一会话的连接方向为第一报文的发送方向的反方向。又例如，第一报文为 ICMP 的 ping request 报文，则第一引擎节点确定第一会话为新建会话，且确定第一会话的连接方向为第一报文的发送方向。再例如，第一报文为 ICMP 的 ping response 报文，则第一引擎节点确定第一会话为新建会话，且确定第一会话的连接方向为第一报文的发送方向的反方向。本申请实施例对第一引擎节点确定第一会话是否为新建会话的实现过程不做限定。

10 如果第一引擎节点确定第一会话为新建会话，则执行 S403 和 S404；或者，如果第一引擎节点确定第一会话不是新建会话，则执行 S406。

S403：第一引擎节点根据第一会话的连接方向和 ACL 确定是否允许第一报文的访问。例如，第一引擎节点中的会话处理模块可以根据第一会话的连接方向和 ACL 确定是否允许第一报文的访问。

15 第一会话是新建会话，第一引擎节点可以直接获得该第一会话的连接方向，并根据该第一会话的连接方向和 ACL 确定是否允许第一报文的访问。例如，第一引擎节点根据第一会话的连接方向查询 ACL。进一步地，如果查询结果指示允许放通，则第一引擎节点转发该第一报文（例如，向第一报文的目的地发送该第一报文）；或者，如果查询结果指示不允许放通，则第一引擎节点丢弃该第一报文。

S404：第一引擎节点修改第一会话表。例如，第一引擎节点中的会话处理模块可以修改第一会话表。

20 S404 和 S405 为可选步骤，图 4 中以虚线表示。第一引擎节点可以根据第一会话表确定是否修改该第一会话表。例如，如果第一会话表中包括第一会话的标识、第四信息和第一会话的连接方向，则第一引擎节点确定不修改第一会话表；或者，如果第一会话表不包括第一会话的标识，或第一会话表中包括第一会话的标识和第三信息，该第三信息用于指示第一会话的连接方向不确定，则第一引擎节点可以修改第一会话表修改后。修改后的第一会话表中包括第一会话的标识、第四信息和第一会话的连接方向。

25 S405：第一引擎节点向至少一个引擎节点发送修改后的第一会话表。例如，第一引擎节点中的消息广播模块可以向至少一个引擎节点发送修改后的第一会话表。

该至少一个引擎节点为分布式防火墙系统中除了第一引擎节点之外的引擎节点。S405 的实现过程请参考 S201 和 S202 的实现过程，不再赘述。例如，第一引擎节点将修改后的第一会话表写入文件和缓冲区，以及发送该缓冲区中的该修改后的第一会话表。

30 需要指出的是，第一引擎节点可以向至少一个引擎节点发送修改后的第一会话表，或者也可以向至少一个引擎节点发送该第一会话表的修改内容，本申请实施例对此不做限定。

S406：第一引擎节点确定第一会话表中是否包括第一会话的标识。例如，第一引擎节点中的会话处理模块可以确定第一会话表中是否包括第一会话的标识。

35 在第一会话不是新建会话的情况下，第一引擎节点可以根据第一会话表确定第一会话的连接方向。例如，第一引擎节点可以确定第一会话表中是否包括第一会话的标识；或者说，第一引擎节点确定第一会话是否命中第一会话表；或者说，第一引擎节点确定第一会话是否与第一会话表匹配；或者，第一引擎节点可以确定第一会话表中是否包括第一会话的信息。

如果第一引擎节点确定第一会话表中不包括第一会话的标识，则执行 S407 至 S409；或者，如果第一引擎节点确定第一会话表中包括第一会话的标识，则执行 S410。

40 S407：第一引擎节点根据第一会话的连接方向和 ACL 确定是否允许第一报文的访问。例如，第一引擎节点中的会话处理模块可以根据第一会话的连接方向和 ACL 确定是否允许第一报文的访问。

其中，第一会话的连接方向为第一报文的发送方向。即，第一引擎节点将第一报文的发送方向作为第一会话的连接方向，并根据该第一会话的连接方向和 ACL 确定是否允许第一报文的访问。例如，第一引擎节点根据第一报文的发送方向查询 ACL。进一步地，如果查询结果指示允许放通，则第一引擎节点转发该第一报文（例如，向第一报文的目的地发送该第一报文）；或者，如果查询结果指示不允许放通，则第一引擎节点丢弃该第一报文。

45 S408：第一引擎节点修改第一会话表。例如，第一引擎节点中的会话处理模块修改第一会话表。修改后的第一会话表中包括第一会话的标识和第三信息。该第三信息用于指示第一会话的连接方向

不确定。

S409: 第一引擎节点向至少一个引擎节点发送修改后的第一会话表。例如, 第一引擎节点中的消息广播模块可以向至少一个引擎节点发送修改后的第一会话表。

该至少一个引擎节点为分布式防火墙系统中除了第一引擎节点之外的引擎节点。S409 的实现过程请参考 S405 的实现过程, 不再赘述。

S410: 第一引擎节点确定第一会话的连接方向是否是确定的。例如, 第一引擎节点中的会话处理模块可以确定第一会话的连接方向是否是确定的。

第一引擎节点可以根据第一会话表确定第一会话的连接方向是否是确定的。例如, 如果第一会话表中包括第一会话的标识、第四信息和第一会话的连接方向, 则第一引擎节点确定第一会话的连接方向是确定的, 并执行 S411 的内容; 或者, 如果第一会话表中包括第一会话的标识和第三信息, 则第一引擎节点确定第一会话的连接方向是不确定的, 并执行 S412。

S411: 第一引擎节点根据第一会话的连接方向和 ACL 确定是否允许第一报文的访问。例如, 第一引擎节点中的会话处理模块可以根据第一会话的连接方向和 ACL 确定是否允许第一报文的访问。

第一引擎节点从第一会话表中获取第一会话的连接方向, 并根据第一会话的连接方向和 ACL 确定是否允许第一报文的访问。进一步地, 如果查询结果指示正反方向中的任一方向允许放通, 则第一引擎节点转发该第一报文 (例如, 向第一报文的目的地发送该第一报文); 或者, 如果查询结果指示正反方向均不允许放通, 则第一引擎节点丢弃该第一报文。

S412: 第一引擎节点根据第一会话的连接方向和 ACL 确定是否允许第一报文的访问。例如, 第一引擎节点中的会话处理模块可以根据第一会话的连接方向和 ACL 确定是否允许第一报文的访问。

其中, 第一会话的连接方向包括第一报文的正反方向。即, 第一引擎节点将第一报文的正反方向作为第一会话的连接方向, 并根据第一会话的连接方向和 ACL 确定是否允许第一报文的访问。例如, 第一引擎节点根据第一报文的正反方向查询 ACL。进一步地, 如果查询结果指示正反方向中的任一方向允许放通, 则第一引擎节点转发该第一报文 (例如, 向第一报文的目的地发送该第一报文); 或者, 如果查询结果指示正反方向均不允许放通, 则第一引擎节点丢弃该第一报文。其中, 第一报文的正反方向是指第一报文的发送方向以及该第一报文的发送方向的反方向。

在上述第二种数据处理方法中, 第一引擎节点可以根据分布式防火墙系统共享的会话表实现对第一报文的访问控制。分布式防火墙系统中的多个引擎节点之间共享会话表, 确保任意一个引擎节点负责的会话也可以由其他引擎节点提供服务, 使得防火墙能够适应弹性扩容、扩容的应用场景。

前述提到, 分布式防火墙系统中的多个引擎节点之间可以共享与流重组相关的信息, 该与流重组相关的信息主要用于对报文分段或报文分片进行流重组处理。接下来结合图 5 对其进行介绍。

图 5 为本申请实施例提供第三种处理方法的流程示意图。该方法可以应用于图 1a 或图 1b 所示的分布式防火墙系统。如图 5 所示, 该方法可以包括如下步骤。

S501: 第一引擎节点接收第二报文。

该第二报文属于第一数据流。该第二报文可以来自内部网络, 或者也可以来自外部网络, 不予限制。示例性地, 第一引擎节点加入分布式防火墙系统时可以加载配置并构建 ACL 等, 并通过上述第一种数据处理方法获取分布式防火墙系统的历史数据得到与流重组相关的第一信息。可选地, 第一引擎节点还可以获得第一会话表。之后, 第一引擎节点启动报文收发流程, 接收该第二报文。

S502: 第一引擎节点确定第二报文是否是第一数据流中的第一个报文。例如, 第一引擎节点中的流重组模块可以确定第二报文是否是第一数据流中的第一个报文。

示例性地, 第一引擎节点解析第二报文的报文头, 可以确定该第二报文是否是第一数据流中的第一个报文。如果第一引擎节点确定第二报文是第一数据流中的第一个报文, 则执行 S503 和 S504; 或者, 如果第一引擎节点确定第二报文不是第一数据流中的第一个报文, 则执行 S507。

S503: 第一引擎节点对第二报文进行流重组处理。例如, 第一引擎节点中的流重组模块可以对第二报文进行流重组处理。

可选地, 如果第一引擎节点的缓冲区中包括第一数据流的报文 (如记为第四报文), 第一引擎节点可以对第二报文和第四报文进行流重组处理。

S504: 第一引擎节点确定第一数据流是否流重组完成。例如, 第一引擎节点中的流重组模块可以确定第一数据流是否流重组完成。

如果第一引擎节点确定第一数据流重组完成,则执行 S505;或者,如果第一引擎节点确定第一数据流未重组完成,则执行 S506。

S505: 第一引擎节点向至少一个引擎节点发送第五信息。例如,第一引擎节点中的消息广播模块可以向至少一个引擎节点发送第五信息。

- 5 该至少一个引擎节点为分布式防火墙系统中除了第一引擎节点之外的引擎节点。该第五信息可以用于指示第一数据流重组完成,以使其他引擎节点删除缓冲区中该第一数据流的报文,节省存储资源。S505 的实现过程请参考 S201 和 S202 的实现过程,不再赘述。

S506: 第一引擎节点向至少一个引擎节点发送第六信息。例如,第一引擎节点中的消息广播模块可以向至少一个引擎节点发送第六信息。

- 10 该至少一个引擎节点为分布式防火墙系统中除了第一引擎节点之外的引擎节点。该第六信息可以用于指示第一数据流重组未完成以及该第一数据流的主处理节点为第一引擎节点,以使其他引擎节点将缓冲区中缓冲的该第一数据流的报文发送给第一引擎节点。S506 的实现过程请参考 S201 和 S202 的实现过程,不再赘述。

- 15 S507: 第一引擎节点根据第一信息确定第一数据流是否重组完成。例如,第一引擎节点中的流重组模块可以根据第一信息确定第一数据流是否重组完成。

如果第一信息为第五信息,则第一引擎节点确定第一数据流重组完成,丢弃第二报文,流程结束;或者如果第一信息不包括第一数据流的信息,则执行 S508 和 S509;或者,如果第一信息用于指示第一数据流未重组完成且主处理节点为第三引擎节点,则执行 S510。

S508: 第一引擎节点缓存第二报文。

- 20 例如,第一引擎节点将第二报文写入缓冲区。

S509: 第一引擎节点确定主处理节点是否是第一引擎节点。例如,第一引擎节点中的流重组模块可以确定主处理节点是否是第一引擎节点。

- 25 如果第一引擎节点在 S502 中确定第二报文不是第一数据流的第一个报文,之后接收到第一数据流的第一个报文(如记为第三报文)(例如,在 S502 之后且在 S507 之前接收该第三报文),则第一引擎节点确定自身为主处理节点,并执行 S503。例如,第一引擎节点接收第三报文(图 5 中未示出),并在第三报文是第一数据流中的第一个报文的情况下,对第二报文和第三报文进行流重组处理。

- 30 或者,如果第一引擎节点根据第一信息或第七信息确定主处理节点不是自身,则执行 S510。例如,第一信息用于指示第一数据流未重组完成且主处理节点为第三引擎节点,第一引擎节点根据该第一信息确定主处理节点不是自身,并执行 S510。又例如,第一引擎节点接收第七信息(例如,在 S507 之后且在 S509 接收来自第三引擎节点的第七信息),该第七信息用于指示第一数据流未重组完成且主处理节点为第三引擎节点,第一引擎节点根据该第七信息确定主处理节点不是自身,并执行 S510。

S510: 第一引擎节点向第三引擎节点发送第二报文。

- 35 相应地,第三引擎节点接收该第二报文,并对该第二报文进行流重组。例如,第一信息用于指示所述第一数据流未重组完成且所述第一数据流的主处理节点为第三引擎节点,第三引擎节点根据该第一信息向第三引擎节点发送第二报文。又例如,第一信息用于指示第一数据流未重组完成以及所述第一数据流的主处理节点不存在,第一引擎节点可以接收第七信息,并根据该第七信息向第三引擎节点发送第二报文。

- 40 在上述第三种数据处理方法中,第一引擎节点可以根据分布式防火墙系统共享的与流重组相关的信息实现对报文分段或报文分片的重组处理。分布式防火墙系统中的多个引擎节点之间共享与流重组相关的信息,这样同一个数据流的报文分段或报文分片可以分发到任意的引擎节点上,通过上述第三种数据处理方法主处理节点可以实现对该报文分段或报文分片的重组,获得完整的数据流。

- 45 本申请提供的实施例,从第一引擎节点的角度对本申请实施例提供的方法进行了介绍。其中,第一引擎节点执行的步骤可以由组成第一引擎节点的不同功能实体来实现。第一引擎节点可以包括硬件结构和/或软件模块,以硬件结构、软件模块、或硬件结构加软件模块的形式来实现上述各功能。上述各功能中的某个功能以硬件结构、软件模块、还是硬件结构加软件模块的方式来执行,取决于技术方案的特定应用和设计约束条件。

下面结合附图介绍本申请实施例中用来实现上述方法的数据处理装置。因此,上文中的内容均可以用于后续实施例中,重复的内容不再赘述。

图 6 示出了本申请实施例提供的一种数据处理装置的结构示意图。该数据处理装置 600 可以实现上述各个方法实施例中第一引擎节点的功能。如图 6 所示, 数据处理装置 600 包括处理模块 601、发送模块 602 和接收模块 603。其中, 处理模块 601 也可以称为处理单元、逻辑单元等。发送模块 602 也可以称为发送单元。接收模块 603 也可以称为接收单元。发送模块 602 和接收模块 603 也可以统称为收发模块 (或收发单元)、通信模块 (或通信单元)、或接口电路等。

可选地, 数据处理装置 600 还可以包括存储模块 604, 图 6 中以虚线表示。该存储模块 604 也可以称为存储单元、存储器等。

其中, 处理模块 601、发送模块 602、接收模块 603 和存储模块 604 均可以该通过软件实现, 或者也可以通过硬件实现, 或者还可以由软件和硬件结合实现。示例性的, 接下来以处理模块 601 为例, 介绍处理模块 601 的实现方式。类似的, 发送模块 602、接收模块 603 和存储模块 604 的实现方式可以对照参考处理模块 601 的实现方式。

模块作为软件功能单元的一种举例, 处理模块 601 可以包括运行在计算实例上的代码。其中, 计算实例可以包括物理主机 (计算设备)、虚拟机、容器中的至少一种。进一步地, 上述计算实例可以是一台或者多台。例如, 处理模块 601 可以包括运行在多个主机/虚拟机/容器上的代码。需要说明的是, 用于运行该代码的多个主机/虚拟机/容器可以分布在相同的区域 (region) 中, 也可以分布在不同的 region 中。进一步地, 用于运行该代码的多个主机/虚拟机/容器可以分布在相同的可用区 (availability zone, AZ) 中, 也可以分布在不同的 AZ 中, 每个 AZ 包括一个数据中心或多个地理位置相近的数据中心。其中, 通常一个 region 可以包括多个 AZ。

同样, 用于运行该代码的多个主机/虚拟机/容器可以分布在同一个虚拟私有云 (virtual private cloud, VPC) 中, 也可以分布在多个 VPC 中。其中, 通常一个 VPC 设置在一个 region 内, 同一 region 内两个 VPC 之间, 以及不同 region 的 VPC 之间跨区通信需在每个 VPC 内设置通信网关, 经通信网关实现 VPC 之间的互连。

模块作为硬件功能单元的一种举例, 处理模块 601 可以包括至少一个计算设备, 如服务器等。或者, 处理模块 601 也可以是利用专用集成电路 (application-specific integrated circuit, ASIC) 实现、或可编程逻辑器件 (programmable logic device, PLD) 实现的设备等。其中, 上述 PLD 可以是复杂程序逻辑器件 (complex programmable logical device, CPLD)、现场可编程门阵列 (field-programmable gate array, FPGA)、通用阵列逻辑 (generic array logic, GAL) 或其任意组合实现。

处理模块 601 包括的多个计算设备可以分布在相同的 region 中, 也可以分布在不同的 region 中。处理模块 601 包括的多个计算设备可以分布在相同的 AZ 中, 也可以分布在不同的 AZ 中。同样, 处理模块 601 包括的多个计算设备可以分布在同一个 VPC 中, 也可以分布在多个 VPC 中。其中, 所述多个计算设备可以是服务器、ASIC、PLD、CPLD、FPGA 和 GAL 等计算设备的任意组合。

示例性地, 处理模块 601 可以用于执行图 2 所示的方法实施例中的 S203、S206, 执行图 4 所示的方法实施例中的 S402 至 S404、S406 至 S407、S410 至 S411, 以及执行图 5 所示的方法实施例中的 S502 至 S504、S507 和 S509 等。发送模块 602 可以用于执行图 2 所述的方法实施例中的 S204, 执行图 4 所示的方法实施例中的 S405 和 S409, 以及执行图 5 所示的方法实施例中的 S505、S506 和 S510 等。接收模块 603 可以用于执行图 2 所述的方法实施例中的 S201 和 S205, 执行图 4 所示的方法实施例中的 S401, 以及执行图 5 所示的方法实施例中的 S501 等。存储模块 604 可以用于执行图 5 所示的方法实施例中的 S508 等。具体实现过程请参考前述各个方法实施例, 这里不再赘述。

本申请还提供一种计算设备 700。如图 7 所示, 计算设备 700 包括: 总线 701、处理器 702、存储器 703 和通信接口 704。处理器 702、存储器 703 和通信接口 704 之间通过总线 702 通信。计算设备 700 可以是服务器, 用于实现第一引擎节点的功能。应理解, 本申请不限定计算设备 700 中的处理器、存储器的个数。

总线 701 可以是外设部件互连标准 (peripheral component interconnect, PCI) 总线或扩展工业标准结构 (extended industry standard architecture, EISA) 总线等。总线可以分为地址总线、数据总线、控制总线等。为便于表示, 图 7 中仅用一条线表示, 但并不表示仅有一根总线或一种类型

的总线。总线 701 可包括在计算设备 700 各个部件（例如，存储器 703、处理器 702、通信接口 704）之间传送信息的通路。

处理器 702 可以包括中央处理器(central processing unit, CPU)、图形处理器(graphics processing unit, GPU)、微处理器（micro processor, MP）或者数字信号处理器（digital signal processor, DSP）等处理器中的任意一种或多种。

存储器 703 可以包括易失性存储器(volatile memory)，例如随机存取存储器(random access memory, RAM)。处理器 702 还可以包括非易失性存储器(non-volatile memory)，例如只读存储器(read-only memory, ROM)、快闪存储器、机械硬盘（hard disk drive, HDD）或固态硬盘（solid state drive, SSD）。

存储器 703 中存储有可执行的程序代码，处理器 702 执行该可执行的程序代码以分别实现前述处理模块 601、发送模块 602、接收模块 603 和存储模块 604 的功能，从而实现前述各个方法实施例。也即，存储器 703 上存有用于执行前述各个方法实施例的指令。

或者，存储器 703 中存储有可执行的代码，处理器 702 执行该可执行的代码以实现前述处理模块 601、发送模块 602、接收模块 603 和存储模块 604 的功能，从而实现前述各个方法实施例。也即，存储器 703 上存有用于执行前述各个方法实施例的指令。

通信接口 704 使用例如但不限于网络接口卡、收发器一类的收发模块，来实现计算设备 700 与其他设备或通信网络之间的通信。例如，通信接口 704 可以实现发送模块 602 和接收模块 603 的功能。

本申请实施例还提供了一种计算设备集群。该计算设备集群包括至少一台计算设备。该计算设备可以是服务器，例如是中心服务器、边缘服务器，或者是本地数据中心中的本地服务器。在一些实施例中，计算设备也可以是台式机、笔记本电脑或者智能手机等终端设备。

如图 8 所示，所述计算设备集群包括至少一个计算设备 700。计算设备集群中的一个或多个计算设备 700 中的存储器 703 中可以存有相同的用于执行前述各个方法实施例的指令。

在一些可能的实现方式中，该计算设备集群中的一个或多个计算设备 700 的存储器 703 中也可以分别存有用于执行前述各个方法实施例的部分指令。换言之，一个或多个计算设备 700 的组合可以共同执行用于执行前述各个方法实施例的指令。

需要说明的是，计算设备集群中的不同的计算设备 700 中的存储器 703 可以存储不同的指令，分别用于执行数据处理装置 600 的部分功能。也即，不同的计算设备 700 中的存储器 703 存储的指令可以实现处理模块 601、发送模块 602、接收模块 603 和存储模块 604 中的一个或多个模块的功能。

在一些可能的实现方式中，计算设备集群中的一个或多个计算设备可以通过网络连接。其中，所述网络可以是广域网或局域网等等。图 9 示出了一种可能的实现方式。如图 9 所示，两个计算设备 700A 和 700B 之间通过网络进行连接。具体地，通过各个计算设备中的通信接口与所述网络进行连接。在这一类可能的实现方式中，计算设备 700A 中的存储器 703 中存有执行处理模块 601 和存储模块 604 的功能的指令。同时，计算设备 700B 中的存储器 703 中存有执行发送模块 602 和接收模块 603 的功能的指令。

图 9 所示的计算设备集群之间的连接方式可以是考虑到本申请提供的前述方法实施例中需要执行接收动作和发送动作，因此考虑将发送模块 602 和接收模块 603 实现的功能交由计算设备 700B 执行。

应理解，图 9 中示出的计算设备 700A 的功能也可以由多个计算设备 700 完成。同样，计算设备 700B 的功能也可以由多个计算设备 700 完成。

本申请实施例还提供了另一种计算设备集群。该计算设备集群中各计算设备之间的连接关系可以类似的参考图 8 和图 9 所述计算设备集群的连接方式。不同的是，该计算设备集群中的一个或多个计算设备 700 中的存储器 703 中可以存有相同的用于执行前述方法实施例的指令。

在一些可能的实现方式中，该计算设备集群中的一个或多个计算设备 700 的存储器 703 中也可以分别存有用于执行前述方法实施例的部分指令。换言之，一个或多个计算设备 700 的组合可以共同执行用于执行前述方法实施例的指令。

需要说明的是，计算设备集群中的不同的计算设备 700 中的存储器 703 可以存储不同的指令，

用于执行分布式防火墙系统的部分功能。也即，不同的计算设备 700 中的存储器 703 存储的指令可以实现第一引擎节点、第二引擎节点和第三引擎节点中的一个或多个节点的功能。

5 本申请实施例还提供一种包含指令的计算机程序产品。所述计算机程序产品可以是包含指令的，能够运行在计算设备上或被储存在任何可用介质中的软件或程序产品。当所述计算机程序产品在至少一个计算设备上运行时，使得至少一个计算设备执行前述的各个方法实施例。

10 本申请实施例还提供一种计算机可读存储介质。所述计算机可读存储介质可以是计算设备能够存储的任何可用介质或者是包含一个或多个可用介质的数据中心等数据存储设备。所述可用介质可以是磁性介质，（例如，软盘、硬盘、磁带）、光介质（例如，DVD）、或者半导体介质（例如固态硬盘）等。该计算机可读存储介质包括指令，所述指令指示计算设备执行前述的各个方法实施例，或指示计算设备执行前述的各个方法实施例。

最后应说明的是：以上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保护范围。

15

权利要求

- 1.一种数据处理方法，其特征在于，分布式防火墙系统包括多个引擎节点，所述方法包括：
第一引擎节点为第二引擎节点创建第一位表文件，其中，所述第一位表文件用于指示所述第一引擎节点对所述第二引擎节点的至少一个消息中的每个消息的接收情况，所述至少一个消息包括如下一项或多项：第一会话表、或者与流重组相关的第一信息，所述第一引擎节点和所述第二引擎节点属于所述多个引擎节点；
所述第一位表文件指示所述至少一个消息中的 N 个消息未接收到的情况下，向所述第二引擎节点发送请求消息，其中，所述请求消息用于请求所述 N 个消息，所述 N 为正整数；
所述第一位表文件接收来自所述第二引擎节点发送的所述 N 个消息；
所述第一位表文件修改所述第一位表文件，修改后的第一位表文件用于指示所述至少一个消息均已接收。
- 2.根据权利要求 1 所述的方法，其特征在于，所述方法还包括：
所述第一位表文件将待发送的 H 个消息进行存储，所述 H 个消息包括如下一项或多项：第二会话表、或者与流重组相关的第二信息，所述 H 为正整数；
所述第一位表文件向所述多个引擎节点中除了所述第一引擎节点之外的至少一个引擎节点发送所述 H 个消息。
- 3.根据权利要求 2 所述的方法，其特征在于，所述向所述多个引擎节点中除了所述第一引擎节点之外的至少一个引擎节点发送所述 H 个消息，包括：
所述第一位表文件将所述 H 个消息写入缓冲区；
在满足第一条件的情况下，所述第一位表文件向所述多个引擎节点中除了所述第一引擎节点之外的至少一个引擎节点发送所述 H 个消息，其中，所述第一条件包括如下一项或多项：所述 H 个消息的数据量大于或等于第一阈值、或者所述 H 个消息的缓存时间大于或等于第二阈值。
- 4.根据权利要求 1 至 3 中任一项所述的方法，其特征在于，所述方法还包括：
所述第一位表文件接收第一报文，所述第一报文属于第一会话；
在所述第一会话为新建会话的情况下，所述第一引擎节点根据所述第一会话的连接方向和访问控制列表确定是否允许所述第一报文的访问。
- 5.根据权利要求 4 所述的方法，其特征在于，所述至少一个消息包括所述第一会话表，所述方法还包括：
在所述第一会话表中不包括所述第一会话的标识，或者所述第一会话表中包括所述第一会话的标识和第三信息，该第三信息用于指示所述第一会话的连接方向不确定的情况下，所述第一引擎节点修改所述第一会话表，其中，修改后的第一会话表中包括所述第一会话的标识、第四信息以及所述第一会话的连接方向，所述第四信息用于指示所述第一会话的连接方向确定；
所述第一位表文件向所述多个引擎节点中除了所述第一引擎节点之外的至少一个引擎节点发送所述修改后的第一会话表。
- 6.根据权利要求 1 至 3 中任一项所述的方法，其特征在于，所述至少一个消息包括所述第一会话表，所述方法还包括：
所述第一位表文件接收第一报文，所述第一报文属于第一会话；
在所述第一会话不是新建会话的情况下，所述第一引擎节点根据所述第一会话表确定所述第一会话的连接方向，其中，所述第一会话表中不包括所述第一会话的标识，所述第一会话的连接方向为所述第一报文的发送方向；
所述第一位表文件根据所述第一会话的连接方向和访问控制列表确定是否允许所述第一报文的访问；
所述第一位表文件修改所述第一会话表，其中，修改后的第一会话表中包括所述第一会话的标识以及第三信息，所述第三信息用于指示所述第一会话的连接方向不确定；
所述第一位表文件向所述多个引擎节点中除了所述第一引擎节点之外的至少一个引擎节点发送所述修改后的第一会话表。
- 7.根据权利要求 1 至 3 中任一项所述的方法，其特征在于，所述至少一个消息包括所述第一会话表，

所述方法还包括:

所述第一引擎节点接收第一报文, 所述第一报文属于第一会话;

在所述第一会话不是新建会话的情况下, 所述第一引擎节点根据所述第一会话表确定所述第一会话的连接方向;

- 5 所述第一引擎节点根据所述第一会话的连接方向和访问控制列表确定是否允许所述第一报文的访问;

其中, 所述第一会话表包括所述第一会话的标识、第四信息和所述第一会话的连接方向, 所述第四信息用于指示所述第一会话的连接方向确定; 或者, 所述第一会话表包括所述第一会话的标识和第三信息, 所述第三信息用于指示所述第一会话的连接方向不确定, 所述第一会话的连接方向包括所述第一报文的正反两个方向。

10

8.根据权利要求1至7中任一项所述的方法, 其特征在于, 所述方法还包括:

所述第一引擎节点接收第二报文, 所述第二报文属于第一数据流;

在所述第二报文为所述第一数据流中的第一个报文的情况下, 所述第一引擎节点对所述第二报文进行流重组处理;

15

在所述第一数据流重组完成的情况下, 所述第一引擎节点向所述多个引擎节点中除了所述第一引擎节点之外的至少一个引擎节点发送第五信息, 所述第五信息用于指示所述第一数据流重组完成; 或者, 在所述第一数据流未重组完成的情况下, 所述第一引擎节点向所述多个引擎节点中除了所述第一引擎节点之外的至少一个引擎节点发送第六信息, 所述第六信息用于指示所述第一数据流未重组完成且所述第一数据流的主处理节点为所述第一引擎节点。

20

9.根据权利要求1至7中任一项所述的方法, 其特征在于, 所述至少一个消息包括所述第一信息, 所述第一信息中不包括第一数据流的信息, 所述方法还包括:

所述第一引擎节点接收第二报文, 所述第二报文属于第一数据流;

在所述第二报文不是所述第一数据流中的第一个报文的情况下, 所述第一引擎节点根据所述第一信息确定所述第一数据流未重组完成以及所述第一数据流的主处理节点不存在;

25

所述第一引擎节点缓存所述第二报文。

10.根据权利要求9所述的方法, 其特征在于, 所述方法还包括:

所述第一引擎节点接收第七信息, 所述第七信息用于指示所述第一数据流未重组完成且所述第一数据流的主处理节点为第三引擎节点, 所述第三引擎节点属于所述多个引擎节点;

所述第一引擎节点向所述第三引擎节点发送所述第二报文。

30

11.根据权利要求9所述的方法, 其特征在于, 所述方法还包括:

所述第一引擎节点接收第三报文, 所述第三报文属于所述第一数据流;

在所述第三报文是所述第一数据流中的第一个报文的情况下, 所述第一引擎节点对所述第二报文和所述第三报文进行流重组处理;

在所述第一数据流重组完成的情况下, 所述第一引擎节点向所述多个引擎节点中除了所述第一引擎节点之外的至少一个引擎节点发送第五信息, 所述第五信息用于指示所述第一数据流重组完成; 或者, 在所述第一数据流未重组完成的情况下, 所述第一引擎节点向所述多个引擎节点中除了所述第一引擎节点之外的至少一个引擎节点发送第六信息, 所述第六信息用于指示所述第一数据流未重组完成且所述第一数据流的主处理节点为所述第一引擎节点。

35

12.根据权利要求1至7中任一项所述的方法, 其特征在于, 所述至少一个消息包括所述第一信息,

40

所述第一信息用于指示所述第一数据流未重组完成且所述第一数据流的主处理节点为第三引擎节点, 所述方法还包括:

所述第一引擎节点接收第二报文, 所述第二报文属于第一数据流;

所述第一引擎节点根据所述第一信息向所述第三引擎节点发送所述第二报文。

13.一种数据处理方法, 其特征在于, 应用于分布式防火墙系统, 所述分布式防火墙系统包括多个引擎节点, 所述多个引擎节点中包括第一引擎节点和第二引擎节点, 所述方法包括:

45

所述第二引擎节点, 将待发送的至少一个消息进行存储, 以及向所述多个引擎节点中除了所述第二引擎节点之外的至少一个引擎节点发送所述至少一个消息; 其中, 所述至少一个消息包括如下项或多项: 第一会话表、或者与流重组相关的第一信息;

所述第一引擎节点,为所述第二引擎节点创建第一位表文件,在所述第一位表文件指示所述至少一个消息中的 N 个消息未接收到的情况下,向所述第二引擎节点发送请求消息;其中,所述第一位表文件用于指示所述第一引擎节点对所述至少一个消息中的每个消息的接收情况,所述请求消息用于请求所述 N 个消息,所述 N 为正整数;

- 5 所述第二引擎节点,接收来自所述第一引擎节点的请求消息,以及向所述第一引擎节点发送 N 个消息;

所述第一引擎节点,接收来自所述第二引擎节点发送的所述 N 个消息,并修改所述第一位表文件,修改后的第一位表文件用于指示所述至少一个消息均已接收。

- 10 14.一种数据处理装置,其特征在于,所述装置应用于分布式防火墙系统中的第一引擎节点,所述分布式防火墙系统包括多个引擎节点,所述第一引擎节点属于所述多个引擎节点,所述装置包括处理模块、发送模块和接收模块,其中:

所述处理模块,用于为第二引擎节点创建第一位表文件,其中,所述第一位表文件用于指示所述第一引擎节点对所述第二引擎节点的至少一个消息中的每个消息的接收情况,所述至少一个消息包括如下

- 15 所述发送模块,用于在所述第一位表文件指示所述至少一个消息中的 N 个消息未接收到的情况下,向所述第二引擎节点发送请求消息,其中,所述请求消息用于请求所述 N 个消息,所述 N 为正整数;

所述接收模块,用于接收来自所述第二引擎节点发送的所述 N 个消息;

所述处理模块,还用于修改所述第一位表文件,修改后的第一位表文件用于指示所述至少一个消息均已接收。

- 20 15.一种分布式防火墙系统,其特征在于,所述分布式防火墙系统包括多个引擎节点,所述多个引擎节点中包括第一引擎节点和第二引擎节点,其中:

所述第二引擎节点,用于将待发送的至少一个消息进行存储,以及向所述多个引擎节点中除了所述第二引擎节点之外的至少一个引擎节点发送所述至少一个消息;其中,所述至少一个消息包括如下

- 25 所述第一引擎节点,用于为所述第二引擎节点创建第一位表文件,在所述第一位表文件指示所述至少一个消息中的 N 个消息未接收到的情况下,向所述第二引擎节点发送请求消息;其中,所述第一位表文件用于指示所述第一引擎节点对所述至少一个消息中的每个消息的接收情况,所述请求消息用于请求所述 N 个消息,所述 N 为正整数;

- 30 所述第二引擎节点,还用于接收来自所述第一引擎节点的请求消息,以及向所述第一引擎节点发送 N 个消息;

所述第一引擎节点,还用于接收来自所述第二引擎节点发送的所述 N 个消息,并修改所述第一位表文件,修改后的第一位表文件用于指示所述至少一个消息均已接收。

- 35 16.一种计算设备集群,其特征在于,包括至少一个计算设备,每个计算设备包括处理器和存储器;所述至少一个计算设备的处理器用于执行所述至少一个计算设备的存储器中存储的指令,以使得所述计算设备集群执行如权利要求 1 至 12 或权利要求 13 中任一项所述的方法。

17.一种计算机可读存储介质,其特征在于,包括计算机程序指令,当所述计算机程序指令由计算设备集群执行时,所述计算设备集群执行如权利要求 1 至 12 或权利要求 13 中任一项所述的方法。

18.一种包含指令的计算机程序产品,其特征在于,所述指令被计算设备集群执行时,使得所述计算设备集群执行如权利要求 1 至 12 或权利要求 13 中任一项所述的方法。

40