

会话访问控制方法、装置、设备、介质及程序产品

5 相关申请的交叉引用

本申请要求享有于 2024 年 6 月 25 日提交的名称为“会话访问控制方法、装置、设备、介质及程序产品”的中国专利申请 202410833758.7 的优先权，该申请的全部内容通过引用并入本文中。

10 技术领域

本申请属于数据通信领域，尤其涉及一种会话访问控制方法、装置、设备、介质及程序产品。

背景技术

15 传输控制协议（Transmission Control Protocol，TCP）是一种面向连接的、可靠的传输层通信协议。在客户端访问服务端，服务端为客户端提供服务的场景下，可在客户端与服务端之间建立 TCP 通信会话，从而传输数据包。为了提高网络安全，会设置防火墙，由防火墙基于规则对客户端与服务端之间的数据包进行检测以及对不满足规则的数据包进行阻断，以实
20 现会话访问控制。但基于数据包检测的防火墙无法判断数据包的 TCP 会话方向，在一些场景，如允许网络协议（Internet Protocol Address，IP）地址 A1 的设备访问 IP 地址 A2 的设备，但不允许 IP 地址 A2 的设备访问 IP 地址 A1 的设备的场景中，无法配置符合该场景的访问控制规则，使得防火墙的会话访问控制无法满足实际的场景需求，适用性较差。

25

发明内容

本申请实施例提供一种会话访问控制方法、装置、设备、介质及程序产品，能够提高防火墙的适用性。

第一方面，本申请实施例提供一种会话访问控制方法，包括：接收第

一数据包，第一数据包包括建立传输控制协议 TCP 通信会话后传输的数据包；基于第一数据包中的网络协议 IP 地址和端口、服务端口集合以及注册 IP 地址集合，将预设的第一访问控制表 ACL 和/或预设的第二 ACL 确定为目标 ACL，服务端口集合包括注册且作为服务端的通信设备的 IP 地址和端口，或，包括未注册且作为服务端的通信设备的 IP 地址和端口，服务端为 TCP 通信会话的接收方，注册 IP 地址集合包括注册的通信设备的 IP 地址，第一 ACL 与注册的通信设备的第一会话方向对应，第二 ACL 与注册的通信设备的第二会话方向对应；按照目标 ACL，执行访问控制操作。

第二方面，本申请实施例提供一种会话访问控制装置，包括：接收模块，用于接收第一数据包，第一数据包包括建立传输控制协议 TCP 通信会话后传输的数据包；访问控制表确定模块，用于基于第一数据包中的网络协议 IP 地址和端口、服务端口集合以及注册 IP 地址集合，将预设的第一访问控制表 ACL 和/或预设的第二 ACL 确定为目标 ACL，服务端口集合包括注册且作为服务端的通信设备的 IP 地址和端口，或，包括未注册且作为服务端的通信设备的 IP 地址和端口，服务端为 TCP 通信会话的接收方，注册 IP 地址集合包括注册的通信设备的 IP 地址，第一 ACL 与注册的通信设备的第一会话方向对应，第二 ACL 与注册的通信设备的第二会话方向对应；访问控制模块，用于按照目标 ACL，执行访问控制操作。

第三方面，本申请实施例提供一种防火墙设备，包括：处理器以及存储有计算机程序指令的存储器；处理器执行计算机程序指令时实现第一方面的会话访问控制方法。

第四方面，本申请实施例提供一种计算机可读存储介质，计算机可读存储介质上存储有计算机程序指令，计算机程序指令被处理器执行时实现第一方面的会话访问控制方法。

第五方面，本申请实施例提供一种计算机程序产品，包括计算机程序，计算机程序被处理器执行时实现第一方面的会话访问控制方法。

本申请实施例提供一种会话访问控制方法、装置、设备、介质及程序产品，可针对 TCP 通信会话的不同的会话方向设置对应的 ACL，防火墙设备可接收建立 TCP 通信会话后传输来的数据包，根据记录作为服务端即

TCP 通信会话的接收方的通信设备的 IP 地址和端口的服务端口集合，确定该数据包所属的 TCP 通信会话的会话方向，从而确定与会话方案对应的 ACL，并按照与会话方向对应的 ACL 执行访问控制操作。通过服务端口集合和注册 IP 地址集合，使得基于数据包检测的防火墙设备也可识别 TCP 通信会话的会话方向，能够为不同的会话方向配置各自的 ACL，从而配置符合各种场景的访问控制规则，使得防火墙的会话访问控制能够满足实际的场景需求，提高防火墙的适用性。

附图说明

10 为了更清楚地说明本申请实施例的技术方案，下面将对本申请实施例中所需要使用的附图作简单的介绍，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

图 1 为本申请实施例提供的会话访问控制方法的应用场景的一示例的架构示意图；

15 图 2 为本申请实施例提供的会话访问控制方法的应用场景的另一示例的架构示意图；

图 3 为本申请一实施例提供的会话访问控制方法的流程图；

图 4 为本申请另一实施例提供的会话访问控制方法的流程图；

图 5 为本申请又一实施例提供的会话访问控制方法的流程图；

20 图 6 为本申请实施例提供的云防火墙的一示例的架构示意图；

图 7 为本申请一实施例提供的会话访问控制装置的结构示意图；

图 8 为本申请一实施例提供的防火墙设备的结构示意图。

具体实施方式

25 下面将详细描述本申请的各个方面的特征和示例性实施例，为了使本申请的目的、技术方案及优点更加清楚明白，以下结合附图及具体实施例，对本申请进行进一步详细描述。应理解，此处所描述的具体实施例仅意在解释本申请，而不是限定本申请。对于本领域技术人员来说，本申请可以在不需要这些具体细节中的一些细节的情况下实施。下面对实施例的

描述仅仅是为了通过示出本申请的示例来提供对本申请更好的理解。需要说明的是，本申请实施例中对信息、数据的获取、存储、使用、处理等均得到用户或相关机构的授权，符合国家法律法规的相关规定。

TCP 是一种面向连接的、可靠的传输层通信协议。在客户端访问服务端，服务端为客户端提供服务的场景下，可在客户端与服务端之间建立 TCP 通信会话，从而传输数据包。为了提高网络安全，会设置防火墙，由防火墙基于规则对客户端与服务端之间的数据包进行检测以及对不满足规则的数据包进行阻断，以实现会话访问控制。但基于数据包检测的防火墙无法判断数据包的 TCP 会话方向，从而无法配置满足某些场景要求的访问控制规则，使得防火墙的会话访问控制无法满足实际的场景需求。例如，对于允许 IP 地址 A1 的设备访问 IP 地址 A2 的设备，但不允许 IP 地址 A2 的设备访问 IP 地址 A1 的设备的场景而言，无法配置符合该场景的访问控制规则，使得防火墙的会话访问控制无法满足实际的场景需求，适用性较差。

为了提高防火墙的会话访问控制的适应性，可采用状态检测防火墙来进行会话访问控制，状态检测防火墙会通过会话表来记录 TCP 通信会话，将通信双方之间交互的属于同一连接的所有报文都作为整体的数据流来看待，从而识别会话方向。但会话表需要占用非常大的存储空间，当会话表中记录的会话数量达到一定量级如 20 万条会话后，会话表的查询和维护时间将会大幅度增加，会降低会话访问控制的性能。且，TCP 通信会话是长连接，会话之间的数据交互间隔时间可以较长，网络攻击者可通过不断与目的服务器建立 TCP 通信会话，但不释放对应的 TCP 通信连接，使得状态检测防火墙维护的会话表中会话数量能够轻易达到上限，使得状态检测防火墙容易被恶意攻击破坏。

本申请提供一种会话访问控制方法、装置、设备、介质及程序产品，可在基于数据包检测的防火墙基础上，针对不同的会话方向设置对应的访问控制表（Access Control List，ACL），根据记录作为服务端即 TCP 通信会话的接收方的通信设备的 IP 地址和端口的服务端端口集合，确定数据包所属的 TCP 通信会话的会话方向，从而确定与会话方向对应的 ACL，并按照

与会话方向对应的 ACL 执行访问控制操作。会话方向的识别使得能够针对不同的会话方向分别设置 ACL，从而能够配置符合各种场景的访问控制规则，使得防火墙的会话访问控制能够满足实际的场景需求，提高防火墙适用性。而且，基于数据包检测的防火墙不需建立会话表，服务端口集合与
5 会话表相比，占用存储空间非常小，且网络攻击者即使不断地与目标服务器建立 TCP 通信连接，由于目标服务器的 IP 地址和端口不会发生变化，在服务端口表中也不会将每次建立的 TCP 通信连接都按照不同的 IP 地址和端口进行记录，服务端口集合中的记录数量始终保持在一个较低的状态，能够保证通信性能并避免防火墙被恶意攻击破坏。

10 为了便于理解，这里先对本申请实施例提供的会话访问控制方法的应用场景进行简单的说明。图 1 为本申请实施例提供的会话访问控制方法的应用场景的一示例的架构示意图，如图 1 所示，通信设备 11 通过防火墙设备 12 与通信设备 13 进行通信，防火墙设备 12 为串联在通信设备 11 与通信设备 13 之间的防火墙设备，防火墙设备 12 可执行本申请实施例中的会
15 话访问控制方法。

图 2 为本申请实施例提供的会话访问控制方法的应用场景的另一示例的架构示意图，如图 2 所示，通信设备 11 和通信设备 13 进行通信，防火墙设备 14 为通信设备 11 和通信设备 13 的旁路防火墙设备，防火墙设备 14 可执行本申请实施例中的会话访问控制方法。图 1 中的通信设备 11 和通信
20 设备 13 只是示例，在实际应用场景中还可包括更多的通信设备，在此并不限定。

下面对本申请提供的会话访问控制方法、装置、设备、介质及程序产品分别进行说明。

本申请第一方面提供一种会话访问控制方法，可应用于防火墙的会话
25 访问控制场景或其他场景，该会话访问控制方法可由会话访问控制装置、设备等执行，会话访问控制装置可实现为防火墙设备、防火墙系统等，在此并不限定。图 3 为本申请一实施例提供的会话访问控制方法的流程图，如图 3 所示，该会话访问控制方法可包括步骤 S201 至步骤 S203。

在步骤 S201 中，接收第一数据包。

第一数据包包括建立 TCP 通信会话后传输的数据包，即，建立 TCP 通信会话后两个通信设备之间传输的数据包可称为第一数据包。

在步骤 S202 中，基于第一数据包中的网络协议 IP 地址和端口、服务端口集合以及注册 IP 地址集合，将预设的第一访问控制表 ACL 和/或预设的第二 ACL 确定为目标 ACL。

第一数据包中可包括 IP 地址和端口，具体地，第一数据包中包括源 IP 地址、源端口、目的 IP 地址和目的端口。源 IP 地址和源端口为第一数据包的发送方的 IP 地址和端口，目的 IP 地址和目的端口为第一数据包的接收方的 IP 地址和端口。仅凭第一数据包，可以得知第一数据包的传输方向，但无法确定第一数据包所属的 TCP 通信会话的会话方向，在 TCP 通信会话中，TCP 通信会话的发起方可作为第一数据包的发送方，也可作为第一数据包的接收方，同理，TCP 通信会话的接收方可作为第一数据包的发送方，也可作为第一数据包的接收方。

为了便于说明，本申请实施例中将 TCP 通信会话的接收方称为服务端，将 TCP 通信会话的发起方称为客户端。需要说明的是，一个通信设备在不同的 TCP 通信会话中的身份可以会不同，如，一个通信设备在一个 TCP 通信会话中为服务端，该通信设备在另一个 TCP 通信会话中可为客户端。服务端口集合是一个动态变化的集合，可实现为表的形式，如，服务端口集合采用服务端口表的形式实现。服务端口集合可包括注册且作为服务端的通信设备的 IP 地址和端口。或者，服务端口集合可包括未注册且作为服务端的通信设备的 IP 地址和端口。注册 IP 地址集合包括注册的通信设备的 IP 地址。注册的通信设备为在防火墙注册的通信设备，即，注册的通信设备为受防火墙保护的通信设备。

在本申请实施例中，ACL 包括第一 ACL 和第二 ACL，第一 ACL 与注册的通信设备的第一会话方向对应，第二 ACL 与注册的通信设备的第二会话方向对应。第一 ACL 包括为注册的通信设备的第一会话方向配置的访问控制规则。第二 ACL 包括为注册的通信设备的第二会话方向配置的访问控制规则。第一会话方向与第二会话方向相反，例如，对于一个注册的通信设备而言，该注册的通信设备在 TCP 通信会话中作为服务端的会话方向为

第一会话方向，该注册的通信设备在 TCP 通信会话中作为客户端的会话方向为第二会话方向。通过第一 ACL 和第二 ACL 的设置，能够满足各种实际的场景需求。例如，上文中提到的相关技术中无法配置的允许 IP 地址 A1 的通信设备访问 IP 地址 A2 的通信设备，但不允许 IP 地址 A2 的通信设备访问 IP 地址 A1 的通信设备的场景，在本申请实施例

5 中，可在第一 ACL 中配置允许 IP 地址 A1 的通信设备访问 IP 地址 A2 的通信设备的访问控制规则，在第二 ACL 中配置禁止 IP 地址 A2 的通信设备访问 IP 地址 A1 的通信设备的访问控制规则，满足该场景的配置需求。

可通过第一数据包中的 IP 地址和端口是否记录在服务端口集合，以及

10 第一数据包中的 IP 地址是否记录在注册 IP 地址集合，来确定第一数据包的发送方通信设备和接收方通信设备是作为服务端还是客户端，以及，第一数据包的发送方通信设备和接收方通信设备是否为注册的通信设备，从而确定注册的通信设备的会话方向，实现基于数据包检测的防火墙设备对 TCP 通信会话的会话方向识别。确定本次 TCP 通信会话的会话方向，即可

15 将本次 TCP 通信会话的会话方向对应的第一 ACL 或第二 ACL 确定为目标 ACL。

在步骤 S203 中，按照目标 ACL，执行访问控制操作。

在确定目标 ACL 后，可按照目标 ACL 中的访问控制规则来执行访问控制操作。目标 ACL 包括第一 ACL 和/或第二 ACL。目标 ACL 属于 ACL，

20 ACL 可包括禁止访问规则和/或允许访问规则，禁止访问规则可包括表征禁止访问的通信规则，允许访问规则可包括表征允许访问的规则。例如，第一 ACL 的规则如下表一所示：

表一

序号	源 IP 地址	源端口	目的 IP 地址	目的端口	动作
2	Cloud_IP_A	ANY	Cloud_IP_B	80	禁止通过
0	ANY	ANY	Cloud_IP_B	80	允许通过

其中，序号为 2 的访问控制规则为禁止访问规则，表征禁止 IP 地址为 Cloud_IP_A 的通信设备通过任意一个端口访问 IP 地址为 Cloud_IP_B 的通信设备的 80 端口；序号为 0 的访问控制规则为允许访问规则，表征允许任

25

意一个 IP 地址的通信设备通过任意一个端口访问 IP 地址为 Cloud_IP_B 的通信设备的 80 端口。

在 ACL 包括禁止访问规则的情况下，若第一数据包符合任意一项禁止访问规则，则阻断数据包所属的 TCP 通信会话。若第一数据包符合任意一项禁止访问规则，表示该第一数据包所属的 TCP 通信会话是禁止的，应阻止该 TCP 通信会话。在 ACL 包括允许访问规则的情况下，若第一数据包不符合任意一项允许访问规则，则阻断数据包所属的 TCP 通信会话。若第一数据包符合允许访问规则，表示该第一数据包所属的 TCP 通信会话是允许的，可继续该 TCP 通信会话。若第一数据包不符合任意一项允许访问规则，表示该第一数据包所属的 TCP 通信会话是禁止的，应阻止该 TCP 通信会话。具体地，阻断第一数据包所属的 TCP 通信会话可具体实现为但不限于防火墙设备分别向第一数据包所属的 TCP 通信会话的发起方通信设备和接收方通信设备发送结束会话数据包，结束第一数据包所属的 TCP 通信会话，从而实现 TCP 通信会话的阻断。

在本申请实施例中，可针对 TCP 通信会话的不同的会话方向设置对应的 ACL，防火墙设备可接收建立 TCP 通信会话后传输来的数据包，根据记录作为服务端即 TCP 通信会话的接收方的通信设备的 IP 地址和端口的服务端口集合，确定该数据包所属的 TCP 通信会话的会话方向，从而确定与会话方案对应的 ACL，并按照与会话方向对应的 ACL 执行访问控制操作。通过服务端口集合和注册 IP 地址集合，使得基于数据包检测的防火墙设备也可识别 TCP 通信会话的会话方向，能够为不同的会话方向配置各自的 ACL，从而配置符合各种场景的访问控制规则，使得防火墙的会话访问控制能够满足实际的场景需求，提高防火墙的适用性。而且，基于数据包检测的防火墙所设置的服务端口集合占用存储空间非常小，维护时间和查询时间都非常短，可保障会话访问控制的性能。即使网络攻击者通过不断建立 TCP 通信会话的方式进行网络攻击，服务端口集合中记录的 IP 地址和端口的数量始终保持在一个较低的状态，能够适应并发高的场景以及避免防火墙被恶意攻击破坏，提高会话访问控制的安全性。

在一些实施例中，可先确定 TCP 通信会话中注册的通信设备的会话方

向，根据会话方向确定目标 ACL。上述步骤 S202 可具体细化为：根据服务端集合是否包括第一数据包中的 IP 地址和端口，以及，注册 IP 地址集合是否包括第一数据包中的 IP 地址，确定 TCP 通信会话中注册的通信设备的会话方向；根据 TCP 通信会话中注册的通信设备的会话方向，将第一

5 ACL 和/或第二 ACL 确定为目标 ACL。

根据服务端集合是否包括第一数据包中的 IP 地址和端口以及注册 IP 地址集合是否包括第一数据包中的 IP 地址，可确定注册的通信设备在本次 TCP 通信会话中是服务端还是接收端，进而确定 TCP 通信会话中注册的通信设备的会话方向，TCP 通信会话中注册的通信设备的会话方向即可视为

10 TCP 通信会话的会话方向。第一数据包包括两组 IP 地址和端口，一组 IP 地址和端口为源 IP 地址和源端口，另一组 IP 地址和端口为目的 IP 地址和目的端口。

在一些示例中，服务端集合包括注册且作为服务端的通信设备的 IP 地址和端口，即，服务端集合记录的是被防火墙设备保护且作为服务端的通信设备的 IP 地址和端口。若服务端集合包括第一数据包中一组 IP 地址和端口，且注册 IP 地址集合包括一组 IP 地址和端口中的 IP 地址的情况下，确定 TCP 通信会话中注册的通信设备的会话方向包括第一会话方向。服务端集合包括第一数据包中一组 IP 地址和端口，可实现为服务端集合包括第一数据包中的源 IP 地址和源端口或服务端口集合包括第一数据包中的目的 IP 地址和目的端口。服务端集合包括第一数据包中一组 IP 地址和端口，且注册 IP 地址集合也包括这一组 IP 地址和端口中的 IP 地址，表示该 TCP 通信会话中注册的通信设备为服务端，该 TCP 通信会话中未注册的通信设备为客户端，在该情况下可认为是未注册的通信设备向注册的通信设备发起 TCP 通信会话，即，注册的通信设备作为服务端的 TCP 通信

15 会话的会话方向为第一会话方向。若服务端集合不包括第一数据包中任意一组 IP 地址和端口，且注册 IP 地址集合包括第一数据包中一组 IP 地址和端口中的 IP 地址的情况下，确定 TCP 通信会话中注册的通信设备的会话方向包括第二会话方向。服务端集合不包括第一数据包中任意一组 IP 地址和端口，即，服务端集合既不包括第一数据包中的源 IP 地址和源端口，

20

25

- 也不包括第一数据包中的目的 IP 地址和源端口。服务端口集合不包括第一数据包中任意一组 IP 地址和端口，且注册 IP 地址集合包括第一数据包中一组 IP 地址和端口中的 IP 地址，表示该 TCP 通信会话中注册的通信设备为客户端，该 TCP 通信会话中未注册的通信设备为服务端，在该情况下可
- 5 认为是注册的通信设备向未注册的通信设备发起 TCP 通信会话，即，注册的通信设备作为客户端的 TCP 通信会话的会话方向为第二会话方向。若服务端口集合包括第一数据包中一组 IP 地址和端口，且注册 IP 地址集合包括第一数据包中两组 IP 地址和端口中的 IP 地址的情况下，确定 TCP 通信会话中注册的通信设备的会话方向包括第一会话方向和第二会话方向。服务
- 10 端口集合包括第一数据包中一组 IP 地址和端口，可实现为服务端口集合包括第一数据包中的源 IP 地址和源端口或服务端口集合包括第一数据包中的目的 IP 地址和目的端口。服务端口集合包括第一数据包中一组 IP 地址和端口，且注册 IP 地址集合包括第一数据包中两组 IP 地址和端口中的 IP 地址，表示该 TCP 通信会话中涉及的两个通信设备均为注册的通信设备，
- 15 该 TCP 通信会话中一个注册的通信设备为服务端，该 TCP 通信会话中另一个注册的通信设备为客户端，在该情况下可认为是注册的通信设备向注册的通信设备发起 TCP 通信会话，对于作为服务端的注册的通信设备而言 TCP 通信会话的会话方向为第一会话方向，对于作为客户端的注册的通信设备而言 TCP 通信会话的会话方向为第二会话方向，因此，对于这两个注
- 20 册的通信设备的 TCP 通信会话的会话方向为第一会话方向和第二会话方向。

- 在一些示例中，服务端口集合包括未注册且作为服务端的通信设备的 IP 地址和端口，即，服务端口集合记录的是未被防火墙设备保护且作为服务端的通信设备的 IP 地址和端口。若服务端口集合包括第一数据包中一组 IP 地址和端口，且注册 IP 地址集合不包括这一组 IP 地址和端口中的 IP 地
- 25 址的情况下，确定 TCP 通信会话中注册的通信设备的会话方向包括第二会话方向。服务端口集合包括第一数据包中一组 IP 地址和端口，可实现为服务端口集合包括第一数据包中的源 IP 地址和源端口或服务端口集合包括第一数据包中的目的 IP 地址和目的端口。服务端口集合包括第一数据包中一组 IP 地址和端口，且注册 IP 地址集合不包括这一组 IP 地址和端口中的 IP

地址，表示该 TCP 通信会话中未注册的通信设备为服务端，该 TCP 通信会话中注册的通信设备为客户端，在该情况下可认为是注册的通信设备向未注册的通信设备发起 TCP 通信会话，即，注册的通信设备作为客户端的 TCP 通信会话的会话方向为第二会话方向。若服务端口集合不包括第一数据包中任意一组 IP 地址和端口，且注册 IP 地址集合包括第一数据包中一组 IP 地址和端口中的 IP 地址的情况下，确定 TCP 通信会话中注册的通信设备的会话方向包括第一会话方向。服务端口集合不包括第一数据包中任意一组 IP 地址和端口，即，服务端口集合既不包括第一数据包中的源 IP 地址和源端口，也不包括第一数据包中的目的 IP 地址和源端口。服务端口集合不包括第一数据包中任意一组 IP 地址和端口，且注册 IP 地址集合包括第一数据包中一组 IP 地址和端口中的 IP 地址，表示该 TCP 通信会话中注册的通信设备为服务端，该 TCP 通信会话中未注册的通信设备为客户端，在该情况下可认为是未注册的通信设备向注册的通信设备发起 TCP 通信会话，即，注册的通信设备作为服务端的 TCP 通信会话的会话方向为第一会话方向。若服务端口集合不包括第一数据包中任意一组 IP 地址和端口，且注册 IP 地址集合包括第一数据包中两组 IP 地址和端口中的 IP 地址的情况下，确定 TCP 通信会话中注册的通信设备的会话方向包括第一会话方向和第二会话方向。服务端口集合不包括第一数据包中任意一组 IP 地址和端口，即，服务端口集合既不包括第一数据包中的源 IP 地址和源端口，也不包括第一数据包中的目的 IP 地址和源端口。服务端口集合不包括第一数据包中任意一组 IP 地址和端口，且注册 IP 地址集合包括第一数据包中两组 IP 地址和端口中的 IP 地址，表示该 TCP 通信会话中涉及的两个通信设备均为注册的通信设备，该 TCP 通信会话中一个注册的通信设备为服务端，该 TCP 通信会话中另一个注册的通信设备为客户端，在该情况下可认为是注册的通信设备向注册的通信设备发起 TCP 通信会话，对于作为服务端的注册的通信设备而言 TCP 通信会话的会话方向为第一会话方向，对于作为客户端的注册的通信设备而言 TCP 通信会话的会话方向为第二会话方向，因此，对于这两个注册的通信设备的 TCP 通信会话的会话方向为第一会话方向和第二会话方向。

在 TCP 通信会话中注册的通信设备的会话方向包括第一会话方向的情况下，将第一 ACL 确定为目标 ACL。在 TCP 通信会话中注册的通信设备的会话方向包括第二会话方向的情况下，将第二 ACL 确定为目标 ACL。在 TCP 通信会话中注册的通信设备的会话方向包括第一会话方向和第二会话方向的情况下，将第一 ACL 和第二 ACL 确定为目标 ACL。

在一些实施例中，两个通信设备需要先进行三次握手，以建立 TCP 通信会话。在建立 TCP 通信会话的过程中，防火墙设备依然可对建立 TCP 通信会话过程中传输的数据包进行检测，实现会话访问控制。下面分别以服务端口集合包括注册且作为服务端的通信设备的 IP 地址和端口、服务端口集合包括未注册且作为服务端的通信设备的 IP 地址和端口为例对建立 TCP 通信会话过程中的会话访问控制进行说明。

图 4 为本申请另一实施例提供的会话访问控制方法的流程图，图 4 所示的是服务端口集合包括注册且作为服务端的通信设备的 IP 地址和端口情况下的会话访问控制方法，图 4 与图 3 的不同之处在于，图 4 所示的会话访问控制方法还可包括步骤 S204 至步骤 S209。

在步骤 S204 中，接收第三数据包。

第三数据包为建立 TCP 通信会话过程中第一次握手传输的数据包。第三数据包具有请求标识，通过该请求标识可识别出数据包为第三数据包，第三数据包也可称为 synchronize 包，简称为 SYN 数据包，请求标识可包括 SYN 标识。第三数据包包括源 IP 地址和源端口以及目的 IP 地址和目的端口。由于第三数据包为建立 TCP 通信会话过程中第一次握手传输的数据包，第三数据包的发送方通信设备为该 TCP 通信会话的客户端，第三数据包的接收方通信设备为该 TCP 通信会话的服务端。对应地，第三数据包中的源 IP 和源端口为该 TCP 通信会话的客户端的 IP 地址和端口，第三数据包中的目的 IP 地址和目的端口为该 TCP 通信会话的服务端的 IP 地址和端口。

在步骤 S205 中，若注册 IP 地址集合包括第三数据包中的目的 IP 地址，则按照第一 ACL，执行访问控制操作。

注册 IP 地址集合包括第三数据包中的目的 IP 地址，表示注册的通信

设备为该 TCP 通信会话的服务端，TCP 通信会话中注册的通信设备的会话方向包括第一会话方向，按照与第一会话方向对应的第一 ACL 执行访问控制操作。

- 5 在步骤 S206 中，若注册 IP 地址集合包括第二数据包中的源 IP 地址，则按照第二 ACL，执行访问控制操作。

注册 IP 地址集合包括第三数据包中的源 IP 地址，表示注册的通信设备为该 TCP 通信会话的客户端，TCP 通信会话中注册的通信设备的会话方向包括第二会话方向，按照与第二会话方向对应的第二 ACL 执行访问控制操作。

- 10 需要说明的是，若注册 IP 地址集合包括第二数据包中的源 IP 地址和目的 IP 地址，表示该 TCP 通信会话中一个注册的通信设备作为服务端，另一个注册的通信设备作为客户端，TCP 通信会话中这一个注册的通信设备的会话方向为第一会话方向，另一个注册的通信设备的会话方向为第二会话方向，即，TCP 通信会话中注册的通信设备的会话方向包括第一会话方向
15 和第二会话方向，按照第一 ACL 和第二 ACL 执行访问控制操作。

通过第三数据包与注册 IP 地址集合，可确定 TCP 通信会话的会话方向，进而进行访问控制操作，保障建立 TCP 通信会话过程中会话访问控制的安全性。

在步骤 S207 中，接收第二数据包。

- 20 第二数据包为建立 TCP 通信会话过程中第二次握手传输的数据包。第二数据包具有请求及确认标识，通过该请求及确认标识可识别出数据包为第二数据包，第二数据包也可称为 SYN/ACK 数据包或 SYN+ACK 数据包。请求及确认标识可包括 SYN/ACK 标识。第二数据包包括源 IP 地址和源端口以及目的 IP 地址和目的端口。由于第二数据包为建立 TCP 通信会话过程
25 中第二次握手传输的数据包，第二数据包的发送方通信设备为该 TCP 通信会话的服务端，第二数据包的接收方通信设备为该 TCP 通信会话的客户端。对应地，第二数据包中的源 IP 和源端口为该 TCP 通信会话的服务端的 IP 地址和端口，第二数据包中的目的 IP 地址和目的端口为该 TCP 通信会话的客户端的 IP 地址和端口。

在步骤 S208 中，若注册 IP 地址集合包括第二数据包中的源 IP 地址，则将第二数据包中的源 IP 地址和源端口写入服务端口集合，按照第一 ACL，执行访问控制操作。

注册 IP 地址集合包括第二数据包中的源 IP 地址，表示第二数据包中源 IP 地址对应的通信设备为注册的通信设备，且该注册的通信设备在该 TCP 通信会话中为服务端，因此将第二数据包中的源 IP 地址和源端口写入服务端口集合，保证服务端口集合中记录有所有注册且作为服务端的通信设备的 IP 地址和端口，以便在建立 TCP 通信会话后使用该服务端口集合来确定后续的第一数据包所属的 TCP 通信会话的会话方向。该注册的通信设备在该 TCP 通信会话中为服务端，TCP 通信会话中注册的通信设备的会话方向包括第一会话方向，按照与第一会话方向对应的第一 ACL 执行访问控制操作。

在步骤 S209 中，若注册 IP 地址集合包括第二数据包中的目的 IP 地址，则按照第二 ACL，执行访问控制操作。

注册 IP 地址集合包括第二数据包中的目的 IP 地址，表示第二数据包中目的 IP 地址对应的通信设备为注册的通信设备，且该注册的通信设备在该 TCP 通信会话中为客户端，不需将第二数据包中的源 IP 地址和源端口写入服务端口集合。该注册的通信设备在该 TCP 通信会话中作为客户端，TCP 通信会话中注册的通信设备的会话方向包括第二会话方向，按照与第二会话方向对应的第二 ACL 执行访问控制操作。

在一些示例中，若注册 IP 地址集合包括第二数据包中的目的 IP 地址但不包括源 IP 地址，且服务端口集合包括第二数据包中的目的 IP 地址和目的端口，则从服务端口集合中删除第二数据包中的目的 IP 地址和目的端口。注册 IP 地址集合包括第二数据包中的目的 IP 地址但不包括源 IP 地址，表示注册的通信设备为该 TCP 通信会话中的客户端，若此时服务端口集合包括第二数据包中的目的 IP 地址和目的端口，可能是之前建立的 TCP 通信会话中该注册的通信设备为服务端，为了避免之前建立的 TCP 通信会话影响本次 TCP 通信会话，从服务端口集合中删除第二数据包中的目的 IP 地址和目的端口，避免该注册的通信设备在本次 TCP 通信会话中被认为是服务

端。

需要说明的是，若注册 IP 地址集合包括第二数据包中的源 IP 地址和目的 IP 地址，表示该 TCP 通信会话中一个注册的通信设备作为服务端，另一个注册的通信设备作为客户端，TCP 通信会话中这一个注册的通信设备的会话方向为第一会话方向，另一个注册的通信设备的会话方向为第二会话方向，即，TCP 通信会话中注册的通信设备的会话方向包括第一会话方向和第二会话方向，按照第一 ACL 和第二 ACL 执行访问控制操作。

在建立 TCP 通信会话的第二次握手的过程中，可动态更新服务端口集合，以便后续准确地判断传输的第一数据包所属的 TCP 通信会话的会话方向，选用正确的 ACL，提高会话访问控制的安全性。

图 5 为本申请又一实施例提供的会话访问控制方法的流程图，图 5 所示的是服务端口集合包括未注册且作为服务端的通信设备的 IP 地址和端口情况下的会话访问控制方法，图 5 与图 3 的不同之处在于，图 4 所示的会话访问控制方法还可包括步骤 S210 至步骤 S216。

在步骤 S210 中，接收第三数据包。

在步骤 S211 中，若注册 IP 地址集合包括第三数据包中的目的 IP 地址，则按照第一 ACL，执行访问控制操作。

在步骤 S212 中，若注册 IP 地址集合包括第二数据包中的源 IP 地址，则按照第二 ACL，执行访问控制操作。

在步骤 S213 中，接收第二数据包。

第二数据包具有请求及确认标识。第二数据包包括源 IP 地址和源端口以及目的 IP 地址和目的端口。

步骤 S210 至步骤 S213 的具体内容与上述实施例中步骤 S204 至步骤 S207 的具体内容基本相同，可参见上文中的相关说明，在此不再赘述。

在步骤 S214 中，若注册 IP 地址集合包括第二数据包中的目的 IP 地址但不包括源 IP 地址，则将第二数据包中的源 IP 地址和源端口写入服务端口集合，按照第二 ACL，执行访问控制操作。

注册 IP 地址集合包括第二数据包中的目的 IP 地址但不包括源 IP 地址，表示第二数据包中目的 IP 地址对应的通信设备为注册的通信设备，第二数

据包中源 IP 地址对应的通信设备为未注册的通信设备，且注册的通信设备在该 TCP 通信会话中为客户端，未注册的通信设备在该 TCP 通信会话中为服务端，因此将第二数据包中的源 IP 地址和源端口写入服务端口集合，保证服务端口集合中记录有所有未注册且作为服务端的通信设备的 IP 地址和端口，以便在建立 TCP 通信会话后使用该服务端口集合来确定后续的第一数据包所属的 TCP 通信会话的会话方向。该注册的通信设备在该 TCP 通信会话中作为客户端，TCP 通信会话中注册的通信设备的会话方向包括第二会话方向，按照与第二会话方向对应的第二 ACL 执行访问控制操作。

在步骤 S215 中，若注册 IP 地址集合包括第二数据包中的源 IP 地址但不包括目的 IP 地址，则按照第一 ACL，执行访问控制操作。

注册 IP 地址集合包括第二数据包中的源 IP 地址但不包括目的 IP 地址，表示第二数据包中源 IP 地址对应的通信设备为注册的通信设备，第二数据包中目的 IP 地址对应的通信设备为未注册的通信设备，该注册的通信设备在该 TCP 通信会话中为服务端，该未注册的通信设备在该 TCP 通信会话中为客户端，不需将第二数据包中目的 IP 地址和目的端口写入服务端口集合。该注册的通信设备在该 TCP 通信会话中为服务端，TCP 通信会话中注册的通信设备的会话方向包括第一会话方向，按照与第一会话方向对应的第一 ACL 执行访问控制操作。

在一些示例中，若注册 IP 地址集合包括第二数据包中的源 IP 地址但不包括目的 IP 地址，且服务端口集合包括第二数据包中的目的 IP 地址和目的端口，则从服务端口集合中删除第二数据包中的目的 IP 地址和目的端口。注册 IP 地址集合包括第二数据包中的源 IP 地址但不包括目的 IP 地址，表示未注册的通信设备为该 TCP 通信会话中的客户端，若此时服务端口集合包括第二数据包中的目的 IP 地址和目的端口，可能是之前建立的 TCP 通信会话中该未注册的通信设备为服务端，为了避免之前建立的 TCP 通信会话影响本次 TCP 通信会话，从服务端口集合中删除第二数据包中的目的 IP 地址和目的端口，避免该注册的通信设备在本次 TCP 通信会话中被认为是服务端。

在步骤 S216 中，若注册 IP 地址集合包括第二数据包中的源 IP 地址和

目的 IP 地址，则按照第一 ACL 和第二 ACL，执行访问控制操作。

注册 IP 地址集合包括第二数据包中的源 IP 地址和目的 IP 地址，表示该 TCP 通信会话中一个注册的通信设备作为服务端，另一个注册的通信设备作为客户端，TCP 通信会话中这一个注册的通信设备的会话方向为第一
5 会话方向，另一个注册的通信设备的会话方向为第二会话方向，即，TCP 通信会话中注册的通信设备的会话方向包括第一会话方向和第二会话方向，按照第一 ACL 和第二 ACL 执行访问控制操作。

在建立 TCP 通信会话的第二次握手的过程中，可动态更新服务端口集合，以便后续准确地判断传输的第一数据包所属的 TCP 通信会话的会话方
10 向，选用正确的 ACL，提高会话访问控制的安全性。

在上述实施例中，在 ACL 包括禁止访问规则的情况下，若第二数据包符合任意一项所述禁止访问规则，则阻断第二数据包所属的 TCP 通信会话；在 ACL 包括允许访问规则的情况下，若第二数据包不符合任意一项所述允许访问规则，则阻断第二数据包所属的 TCP 通信会话。在 ACL 包括禁止
15 访问规则的情况下，若第三数据包符合任意一项所述禁止访问规则，则阻断第三数据包所属的 TCP 通信会话；在 ACL 包括允许访问规则的情况下，若第三数据包不符合任意一项所述允许访问规则，则阻断第三数据包所属的 TCP 通信会话。具体内容可参考上文中阻断第一数据包所属的 TCP 通信会话的相关说明，在此不再赘述。

20 需要说明的是，本申请实施例中提到的 TCP 通信会话中注册的通信设备的会话方向可具体包括 TCP 通信会话中注册的通信设备的端口的会话方向。

在一些实施例中，可能会出现一个通信设备的某个端口同时作为客户端和服务端，即，注册的通信设备的会话方向同时包括第一会话方向和第二
25 会话方向的情况，在该情况下，可执行预定的访问控制策略。预定访问控制策略可包括：按照所述第一 ACL，执行访问控制操作；或者，按照所述第二 ACL，执行访问控制操作；或者，按照所述第一 ACL 和所述第二 ACL，执行访问控制操作。预定访问控制策略可包括按照所述第一 ACL 执行访问控制操作，表示将同时作为客户端和服务端的通信设备的端口强制

标记为服务端。预定访问控制策略可包括按照所述第二 ACL 执行访问控制操作，表示将同时作为客户端和服务端的通信设备的端口强制标记为客户端。预定访问控制策略可包括按照第一 ACL 和第二 ACL 执行访问控制操作，表示将同时作为客户端和服务端的通信设备的端口强制标记为客户端和服务端。该强制标记行为可预先进行，也可在检测到通信设备的某个端口同时作为客户端和服务端的情况下进行，在此并不限定。预定访问控制策略也可根据场景、需求等进行调整、更新。

本申请实施例中的防火墙可实现为云防火墙，图 6 为本申请实施例提供的云防火墙的一示例的架构示意图，如图 6 所示，云防火墙 30 包括防火墙单元 31、网络流量分析（Network Traffic Analysis, NTA）单元 32、安全管理单元 33、同步单元 34 和 ACL 管理单元 35。安全管理单元 33 可具有阻断模式功能和封禁管理功能，这两个功能可通过同步单元 34 同步来的 ACL 管理单元 35 中的入方向 ACL 管理和出方向 ACL 管理触发和执行。入方向为上述实施例中的第一会话方向，出方向为上述实施例中的第二会话方向。云防火墙 30 可与用户的通信设备 40 通信交互，传输至通信设备 40 的数据流量可通过镜像流量方式传输给防火墙单元 31 以及 NTA 单元 32。防火墙单元 31 通过安全管理单元 33 中封禁管理功能进行阻断指令的查询与管理，通过安全管理单元 33 中的阻断模式功能向防火墙单元 31 下发阻断指令，以使防火墙单元 31 执行阻断动作。NTA 单元 32 也可能向安全管理单元 33 提供阻断建议。

为了便于理解，下面以服务端口集合包括注册且作为服务端的服务器的 IP 地址和端口情况下的三个具体场景来对上述实施例中的会话访问控制方法进行举例说明。

场景一：用户 A 的注册的通信设备的 IP 地址为 Cloud_IP_A，用户 A 所在公司的一个出口 IP 地址为 OA_OUT_IP_A，对该注册的通信设备的会话访问控制希望能够满足以下要求：（1）所有通信设备端口都能访问该注册的通信设备的 IP 地址 Cloud_IP_A 的 443 端口和 80 端口发布的网站服务；（2）只允许在公司登录该注册的通信设备的 IP 地址 Cloud_IP_A 进行运维操作，即，仅允许使用 IP 地址 OA_OUT_IP_A 访问 IP 地址 Cloud_IP_A

的 22 端口；（3）由于 IP 地址 Cloud_IP_A 所对应的注册的通信设备需要不受限的访问外部服务，以调用外部应用程序编程接口（Application Programming Interface，API）API 服务、进行漏洞审计等。针对上述要求，可配置得到如下表二所示的第一 ACL 和如下表三所示的第二 ACL：

5

表二

第一 ACL	序号	源 IP 地址	源端口	目的 IP 地址	目的端口	动作
	1	ANY	ANY	Cloud_IP_A	80, 443	允许通过
	2	OA_OUT_IP_A	ANY	Cloud_IP_A	22	允许通过

表三

第二 ACL	序号	源 IP 地址	源端口	目的 IP 地址	目的端口	动作
	3	Cloud_IP_A	ANY	ANY	ANY	允许通过

其中，IP 地址中的 ANY 表示任意一个 IP 地址，端口中的 ANY 表示任意一个端口；序号 1 对应上述要求（1），序号 2 对应上述要求（2），序号 3 对应上述要求（3）。

10

场景一的访问请求是：一个不属于 OA_OUT_IP_A 的 IP 地址 IP_B 尝试访问 Cloud_IP_A 的 22 端口。对应地，TCP 通信会话的访问控制流程可包括步骤 a1 至步骤 a3。

15

在步骤 a1 中，IP_B 通过一个随机端口 random_b 向 Cloud_IP_A 的 22 端口发送一个 SYN 数据包，根据 SYN 数据包可直接确定会话方向为第一会话方向，因此防火墙在检测到该 SYN 数据包时，结合 Cloud_IP_A 为注册的通信设备的 IP 地址，查询第一 ACL，确定该访问请求不符合第一 ACL 中的任意一条允许访问规则，该访问请求应被拒绝，从而执行阻断措施。

若由于其他各种原因导致步骤 a1 的阻断失效。在步骤 a2 中可再次判断会话方向，查找对应的 ACL，以执行阻断措施。

20

在步骤 a2 中，Cloud_IP_A 的 22 端口向 IP_B 的一个随机端口 random_b 发送一个 SYN+ACK 数据包，防火墙检测到该数据包后，由于 Cloud_IP_A 为注册的通信设备的 IP 地址且作为服务端，将 Cloud_IP_A 和 22 端口登记为服务端写入服务端集合。检测到 SYN+ACK 数据包，结合 Cloud_IP_A 为注册的通信设备的 IP 地址，查询第一 ACL，确定该访问请

求不符合第一 ACL 中的任意一条允许访问规则，该访问请求应被拒绝，从而执行阻断措施。

若由于其他各种原因导致步骤 a2 的阻断失效。在步骤 a3 中可再次判断会话方向，查找对应的 ACL，以执行阻断措施。

- 5 在步骤 a3 中，TCP 通信会话已经建立，防火墙对 Cloud_IP_A 的 22 端口与 IP_B 的一个随机端口 random_b 之间传输的每个第一数据包进行检测，第一数据包中的 Cloud_IP_A 的 22 端口在服务端口集合中，且 Cloud_IP_A 在注册 IP 地址集合中，确定会话方向为第一会话方向，查询第一 ACL，确定该访问请求不符合第一 ACL 中的任意一条允许访问规则，该访问请求应
- 10 被拒绝，从而执行阻断措施。

场景二：场景二中配置的第一 ACL 和第二 ACL 与场景一相同，不同的是，场景二的访问请求是：Cloud_IP_A 访问 IP_C 的 80 端口的服务，IP_C 是未注册的通信设备的 IP 地址。对应地，TCP 通信会话的访问控制流程可包括步骤 b1 至步骤 b3。

- 15 在步骤 b1 中，Cloud_IP_A 通过一个随机端口 random_a 向 IP_C 的 80 端口发送一个 SYN 数据包，根据 SYN 数据包可直接确定会话方向为第二会话方向，因此防火墙在检测到该 SYN 数据包时，结合 Cloud_IP_A 为注册的通信设备的 IP 地址，查询第二 ACL，确定该访问请求符合第二 ACL 中的允许访问规则，该访问请求应被接受，从而放行该访问请求。
- 20 在步骤 b2 中，IP_C 的 80 端口会向 Cloud_IP_A 的随机端口 random_a 发送一个 SYN+ACK 数据包，IP_C 对应的通信设备为 TCP 通信会话的服务端，且 IP_C 对应的通信设备为未注册的通信设备，不会将 IP_C 的 80 端口写入服务端口集合，同时因为 Cloud_IP_A 对应的通信设备为 TCP 通信会话的客户端，确定会话方向为第二会话方向，查询第二 ACL，确定该访问
- 25 请求符合第二 ACL 中的允许访问规则，该访问请求应被接受，从而放行该访问请求。

在步骤 b3 中，TCP 通信会话已经建立，防火墙对 IP_C 的 80 端口与 Cloud_IP_A 的随机端口 random_a 之间传输的每个第一数据包进行检测，第一数据包中的 Cloud_IP_A 的随机端口 random_a 和 IP_C 的 80 端口均不

在服务端口集合，确定会话方向为第二方向，查询第二 ACL，确定该访问请求符合第二 ACL 中的允许访问规则，该访问请求应被接受，从而放行该访问请求。

场景三：用户 A 的注册的通信设备的 IP 地址为 Cloud_IP_A，用户 B 的注册的通信设备的 IP 地址为 Cloud_IP_B，对这两个注册的通信设备的会话访问控制希望能够满足以下要求：（1）Cloud_IP_B 对外开放 80 端口的 Web 服务；（2）Cloud_IP_A 放通自己访问 Cloud_IP_B 的 80 端口的服务；（3）但 Cloud_IP_B 禁止 Cloud_IP_A 对 Cloud_IP_B 的 80 端口的访问。针对上述要求，可配置得到如下表四所示的第一 ACL 和如下表五所示的第二 ACL：

表四

第一 ACL	序号	源 IP 地址	源端口	目的 IP 地址	目的端口	动作
	3	Cloud_IP_A	ANY	Cloud_IP_B	80	禁止通过
	1	ANY	ANY	Cloud_IP_B	80	允许通过

表五

第二 ACL	序号	源 IP 地址	源端口	目的 IP 地址	目的端口	动作
	2	Cloud_IP_A	ANY	Cloud_IP_B	80	允许通过

其中，IP 地址中的 ANY 表示任意一个 IP 地址，端口中的 ANY 表示任意一个端口；序号 1 对应上述要求（1），序号 2 对应上述要求（2），序号 3 对应上述要求（3）。

场景三的申请请求是：Cloud_IP_A 通过一个随机端口 random_a 访问 Cloud_IP_B 的 80 端口。对应地，TCP 通信会话的申请控制流程可包括步骤 c1 至步骤 c3。

在步骤 c1 中，Cloud_IP_A 将通过一个随机端口 random_a 向 Cloud_IP_B:80 发送一个 SYN 数据包，根据 SYN 数据包确定会话方向为 Cloud_IP_A 到 Cloud_IP_B，Cloud_IP_A 对应的通信设备和 Cloud_IP_B 对应的通信设备均为注册的通信设备，因此会话方向包括第一会话方向和第二会话方向，查询第一 ACL 和第二 ACL，确定该访问请求符合第一 ACL 和第二 ACL 中的禁止访问规则，该访问请求应被拒绝，从而执行阻断措施。

若由于其他各种原因导致步骤 c1 的阻断失效。在步骤 c2 中可再次判断会话方向，查找对应的 ACL，以执行阻断措施。

在步骤 c2 中，Cloud_IP_B 的 80 端口向 Cloud_IP_A 的随机端口 random_a 发送一个 SYN+ACK 数据包，根据 SYN+ACK 数据包确定会话方向为 Cloud_IP_A 到 Cloud_IP_B，Cloud_IP_B 为 TCP 通信会话中的服务端，将 Cloud_IP_B 的 80 端口写入服务端口集合。Cloud_IP_A 对应的通信设备和 Cloud_IP_B 对应的通信设备均为注册的通信设备，因此会话方向包括第一会话方向和第二会话方向，查询第一 ACL 和第二 ACL，确定该访问请求符合第一 ACL 和第二 ACL 中的禁止访问规则，该访问请求应被拒绝，从而执行阻断措施。

若由于其他各种原因导致步骤 c2 的阻断失效。在步骤 c3 中可再次判断会话方向，查找对应的 ACL，以执行阻断措施。

在步骤 c3 中，TCP 通信会话已经建立，防火墙对 Cloud_IP_B 的 80 端口与 Cloud_IP_A 的随机端口 random_a 之间传输的每个第一数据包进行检测，第一数据包中的 Cloud_IP_B 的 80 端口在服务端口集合中，且 Cloud_IP_A 对应的通信设备和 Cloud_IP_B 对应的通信设备均为注册的通信设备，因此会话方向包括第一会话方向和第二会话方向，查询第一 ACL 和第二 ACL，确定该访问请求符合第一 ACL 和第二 ACL 中的禁止访问规则，该访问请求应被拒绝，从而执行阻断措施。

通过上述场景举例可得，采用本申请实施例提供的会话访问控制方法，能够配置符合各种场景的访问控制规则，如，可实现 IP 地址 A1 的通信设备访问 IP 地址 A2 的通信设备，但不允许 IP 地址 A2 的通信设备访问 IP 地址 A1 的通信设备的场景的访问控制规则的配置，使得防火墙的访问控制能够满足实际的场景需求，提高防火墙的会话访问控制的适用性和准确性，保障会话访问控制的安全性。

本申请第二方面提供一种会话访问控制装置。图 7 为本申请一实施例提供的会话访问控制装置的结构示意图，如图 7 所示，该会话访问控制装置 500 可包括接收模块 501、访问控制表确定模块 502 和访问控制模块 503。

接收模块 501 可用于接收第一数据包。

第一数据包包括建立传输控制协议 TCP 通信会话后传输的数据包。

访问控制表确定模块 502 可用于基于第一数据包中的网络协议 IP 地址和端口、服务端口集合以及注册 IP 地址集合，将预设的第一访问控制表 ACL 和/或预设的第二 ACL 确定为目标 ACL。

5 服务端口集合包括注册且作为服务端的通信设备的 IP 地址和端口，或，包括未注册且作为服务端的通信设备的 IP 地址和端口。服务端为 TCP 通信会话的接收方。注册 IP 地址集合包括注册的通信设备的 IP 地址。第一 ACL 与注册的通信设备的第一会话方向对应，第二 ACL 与注册的通信设备的第二会话方向对应。

10 访问控制模块 503 可用于按照目标 ACL，执行访问控制操作。

 在一些实施例中，访问控制表确定模块 502 可具体用于：根据服务端口集合是否包括第一数据包中的 IP 地址和端口，以及，注册 IP 地址集合是否包括第一数据包中的 IP 地址，确定 TCP 通信会话中注册的通信设备的会话方向；根据 TCP 通信会话中注册的通信设备的会话方向，将第一 ACL
15 和/或第二 ACL 确定为目标 ACL。

 在一些示例中，第一数据包包括两组 IP 地址和端口，服务端口集合包括注册且作为服务端的通信设备的 IP 地址和端口。访问控制表确定模块 502 可具体用于：若服务端口集合包括第一数据包中一组 IP 地址和端口，且注册 IP 地址集合包括一组 IP 地址和端口中的 IP 地址的情况下，确定
20 TCP 通信会话中注册的通信设备的会话方向包括第一会话方向；若服务端口集合不包括第一数据包中任意一组 IP 地址和端口，且注册 IP 地址集合包括第一数据包中一组 IP 地址和端口中的 IP 地址的情况下，确定 TCP 通信会话中注册的通信设备的会话方向包括第二会话方向；若服务端口集合包括第一数据包中一组 IP 地址和端口，且注册 IP 地址集合包括第一数据
25 包中两组 IP 地址和端口中的 IP 地址的情况下，确定 TCP 通信会话中注册的通信设备的会话方向包括第一会话方向和第二会话方向。

 在一些示例中，第一数据包包括两组 IP 地址和端口，服务端口集合包括未注册且作为服务端的通信设备的 IP 地址和端口。访问控制表确定模块 502 可具体用于：若服务端口集合包括第一数据包中一组 IP 地址和端口，

- 且注册 IP 地址集合不包括一组 IP 地址和端口中的 IP 地址的情况下，确定 TCP 通信会话中注册的通信设备的会话方向包括第二会话方向；若服务端口集合不包括第一数据包中任意一组 IP 地址和端口，且注册 IP 地址集合包括第一数据包中一组 IP 地址和端口中的 IP 地址的情况下，确定 TCP 通信会话中注册的通信设备的会话方向包括第一会话方向；若服务端口集合不包括第一数据包中任意一组 IP 地址和端口，且注册 IP 地址集合包括第一数据包中两组 IP 地址和端口中的 IP 地址的情况下，确定 TCP 通信会话中注册的通信设备的会话方向包括第一会话方向和第二会话方向。

- 10 在一些示例中，访问控制表确定模块 502 可具体用于：在 TCP 通信会话中注册的通信设备的会话方向包括第一会话方向的情况下，将第一 ACL 确定为目标 ACL；在 TCP 通信会话中注册的通信设备的会话方向包括第二会话方向的情况下，将第二 ACL 确定为目标 ACL；在 TCP 通信会话中注册的通信设备的会话方向包括第一会话方向和第二会话方向的情况下，将第一 ACL 和第二 ACL 确定为目标 ACL。

- 15 在一些实施例中，服务端口集合包括注册且作为服务端的通信设备的 IP 地址和端口。

接收模块 501 还可用于：在接收第一数据包之前，接收第二数据包，第二数据包具有请求及确认标识，第二数据包包括源 IP 地址和源端口以及目的 IP 地址和目的端口。

- 20 访问控制模块 503 还可用于：若注册 IP 地址集合包括第二数据包中的源 IP 地址，则将第二数据包中的源 IP 地址和源端口写入服务端口集合，按照第一 ACL，执行访问控制操作；若注册 IP 地址集合包括第二数据包中的目的 IP 地址，则按照第二 ACL，执行访问控制操作。

- 25 在一些示例中，访问控制模块 503 还可用于：若注册 IP 地址集合包括第二数据包中的目的 IP 地址但不包括源 IP 地址，且服务端口集合包括第二数据包中的目的 IP 地址和目的端口，则从服务端口集合中删除第二数据包中的目的 IP 地址和目的端口。

在一些实施例中，服务端口集合包括未注册且作为服务端的通信设备的 IP 地址和端口。

接收模块 501 还可用于：在接收第一数据包之前，接收第二数据包，第二数据包具有请求及确认标识，第二数据包包括源 IP 地址和源端口以及目的 IP 地址和目的端口。

访问控制表确定模块 502 还可用于：若注册 IP 地址集合包括第二数据包中的目的 IP 地址但不包括源 IP 地址，则将第二数据包中的源 IP 地址和源端口写入服务端口集合，按照第二 ACL，执行访问控制操作；若注册 IP 地址集合包括第二数据包中的源 IP 地址但不包括目的 IP 地址，则按照第一 ACL，执行访问控制操作；若注册 IP 地址集合包括第二数据包中的源 IP 地址和目的 IP 地址，则按照第一 ACL 和第二 ACL，执行访问控制操作。

在一些示例中，访问控制表确定模块 502 还可用于：若注册 IP 地址集合包括第二数据包中的源 IP 地址但不包括目的 IP 地址，且服务端口集合包括第二数据包中的目的 IP 地址和目的端口，则从服务端口集合中删除第二数据包中的目的 IP 地址和目的端口。

在一些实施例中，接收模块 501 还可用于：在接收第一数据包之前，接收第三数据包，第三数据包具有请求标识，第三数据包包括源 IP 地址和源端口以及目的 IP 地址和目的端口。

访问控制表确定模块 502 还可用于：若注册 IP 地址集合包括第三数据包中的目的 IP 地址，则按照第一 ACL，执行访问控制操作；若注册 IP 地址集合包括第二数据包中的源 IP 地址，则按照第二 ACL，执行访问控制操作。

在一些实施例中，访问控制表确定模块 502 还可用于：在一个注册的通信设备的会话方向同时包括第一会话方向和第二会话方向的情况下，执行预定访问控制策略。

预定访问控制策略包括：按照第一 ACL，执行访问控制操作；或者，按照第二 ACL，执行访问控制操作；或者，按照第一 ACL 和第二 ACL，执行访问控制操作。

在一些实施例中，ACL 包括第一 ACL 和/或第二 ACL。访问控制表确定模块 502 还可用于：在 ACL 包括禁止访问规则的情况下，若数据包符合任意一项禁止访问规则，则阻断数据包所属的 TCP 通信会话；在 ACL 包

括允许访问规则的情况下，若数据包不符合任意一项允许访问规则，则阻断数据包所属的 TCP 通信会话。数据包包括第一数据包、第二数据包、第三数据包中的至少一者。

需要说明的是，该会话访问控制装置 500 是与上述会话访问控制方法
5 对应的装置，上述方法实施例中所有实现方式均适用于该装置的实施例中，也能达到相同的技术效果。

本申请第三方面还提供了一种防火墙设备。图 8 为本申请一实施例提供的防火墙设备的结构示意图，如图 8 所示，防火墙设备 600 包括存储器 601、处理器 602 及存储在存储器 601 上并可在处理器 602 上运行的计算机
10 程序。

在一些示例中，上述处理器 602 可以包括中央处理器（CPU），或者特定集成电路（Application Specific Integrated Circuit，ASIC），或者可以被配置成实施本申请实施例的一个或多个集成电路。

存储器 601 可包括只读存储器（Read-Only Memory，ROM），随机存取存储器（Random Access Memory，RAM），磁盘存储介质设备，光存储介质设备，闪存设备，电气、光学或其他物理/有形的存储器存储设备。因此，通常，存储器包括一个或多个编码有包括计算机可执行指令的软件的有形（非暂态）计算机可读存储介质（例如，存储器设备），并且当该软件被执行（例如，由一个或多个处理器）时，其可操作来执行参考根据
15 本申请实施例中会话访问控制方法所描述的操作。

处理器 602 通过读取存储器 601 中存储的可执行程序代码来运行与可执行程序代码对应的计算机程序，以用于实现上述实施例中会话访问控制方法。

在一些示例中，防火墙设备 600 还可包括通信接口 603 和总线 604。
25 其中，如图 8 所示，存储器 601、处理器 602、通信接口 603 通过总线 604 连接并完成相互间的通信。

通信接口 603，主要用于实现本申请实施例中各模块、装置、单元和/或设备之间的通信。也可通过通信接口 603 接入输入设备和/或输出设备。

总线 604 包括硬件、软件或两者，将防火墙设备 600 的部件彼此耦接

在一起。举例来说而非限制，总线 604 可包括加速图形端口（Accelerated Graphics Port, AGP）或其他图形总线、增强工业标准架构（Enhanced Industry Standard Architecture, EISA）总线、前端总线（Front Side Bus, FSB）、超传输（Hyper Transport, HT）互连、工业标准架构（Industry Standard Architecture, ISA）总线、无限带宽互连、低引脚数（Low pin count, LPC）总线、存储器总线、微信道架构（Micro Channel Architecture, MCA）总线、外围组件互连（Peripheral Component Interconnect, PCI）总线、PCI-Express（PCI-E）总线、串行高级技术附件（Serial Advanced Technology Attachment, SATA）总线、视频电子标准协会局部（Video Electronics Standards Association Local Bus, VLB）总线或其他合适的总线或者两个或更多个以上这些的组合。在合适的情况下，总线 604 可包括一个或多个总线。尽管本申请实施例描述和示出了特定的总线，但本申请考虑任何合适的总线或互连。

本申请第四方面提供一种计算机可读存储介质，该计算机可读存储介质上存储有计算机程序指令，该计算机程序指令被处理器执行时可实现上述实施例中的会话访问控制方法，且能达到相同的技术效果，为避免重复，这里不再赘述。其中，上述计算机可读存储介质可包括非暂态计算机可读存储介质，如只读存储器（Read-Only Memory, 简称 ROM）、随机存取存储器（Random Access Memory, 简称 RAM）、磁碟或者光盘等，在此并不限定。

本申请第五方面提供一种计算机程序产品，该计算机程序产品包括计算机程序，该计算机程序被处理器执行时实现上述实施例中的会话访问控制方法，且能达到相同的技术效果，为避免重复，这里不再赘述。

需要明确的是，本说明书中的各个实施例均采用递进的方式描述，各个实施例之间相同或相似的部分互相参见即可，每个实施例重点说明的都是与其他实施例的不同之处。对于装置实施例、设备实施例、计算机可读存储介质实施例、计算机程序产品实施例而言，相关之处可以参见方法实施例的说明部分。本申请并不局限于上文所描述并在图中示出的特定步骤和结构。本领域的技术人员可以在领会本申请的精神之后，作出各种改变、

修改和添加，或者改变步骤之间的顺序。并且，为了简明起见，这里省略对已知方法技术的详细描述。

上面参考根据本申请的实施例的方法、装置（系统）和计算机程序产品的流程图和/或框图描述了本申请的各方面。应当理解，流程图和/或框图中的每个方框以及流程图和/或框图中各方框的组合可以由计算机程序指令实现。这些计算机程序指令可被提供给通用计算机、专用计算机、或其它可编程数据处理装置的处理器，以产生一种机器，使得经由计算机或其它可编程数据处理装置的处理器执行的这些指令使能对流程图和/或框图的一个或多个方框中指定的功能/动作的实现。这种处理器可以是但不限于是通用处理器、专用处理器、特殊应用处理器或者现场可编程逻辑电路。还可理解，框图和/或流程图中的每个方框以及框图和/或流程图中的方框的组合，也可以由执行指定的功能或动作的专用硬件来实现，或可由专用硬件和计算机指令的组合来实现。

本领域技术人员应能理解，上述实施例均是示例性而非限制性的。在不同实施例中出现的不同技术特征可以进行组合，以取得有益效果。本领域技术人员在研究附图、说明书及权利要求书的基础上，应能理解并实现所揭示的实施例的其他变化的实施例。在权利要求书中，术语“包括”并不排除其他装置或步骤；数量词“一个”不排除多个；术语“第一”、“第二”用于标示名称而非用于表示任何特定的顺序。权利要求中的任何附图标记均不应被理解为对保护范围的限制。权利要求中出现的多个部分的功能可以由一个单独的硬件或软件模块来实现。某些技术特征出现在不同的从属权利要求中并不意味着不能将这些技术特征进行组合以取得有益效果。

权 利 要 求 书

1. 一种云访问控制方法，包括：

5 接收第一数据包，所述第一数据包包括建立传输控制协议 TCP 通信会话后传输的数据包；

基于所述第一数据包中的网络协议 IP 地址和端口、服务端口集合以及注册 IP 地址集合，将预设的第一访问控制表 ACL 和/或预设的第二 ACL 确定为目标 ACL，所述服务端口集合包括注册且作为服务端的通信设备的 IP 地址和端口，或，包括未注册且作为服务端的通信设备的 IP 地址和端口，
10 服务端为 TCP 通信会话的接收方，所述注册 IP 地址集合包括注册的通信设备的 IP 地址，所述第一 ACL 与注册的通信设备的第一会话方向对应，所述第二 ACL 与注册的通信设备的第二会话方向对应；

按照所述目标 ACL，执行访问控制操作。

2. 根据权利要求 1 所述的方法，其中，所述基于所述第一数据包中的
15 网络协议 IP 地址和端口、服务端口集合以及注册 IP 地址集合，将预设的第一访问控制表 ACL 和/或预设的第二 ACL 确定为目标 ACL，包括：

根据所述服务端口集合是否包括所述第一数据包中的 IP 地址和端口，以及，所述注册 IP 地址集合是否包括第一数据包中的 IP 地址，确定 TCP 通信会话中注册的通信设备的会话方向；

20 根据 TCP 通信会话中注册的通信设备的会话方向，将所述第一 ACL 和/或所述第二 ACL 确定为所述目标 ACL。

3. 根据权利要求 2 所述的方法，其中，所述第一数据包包括两组 IP 地址和端口，所述服务端口集合包括注册且作为服务端的通信设备的 IP 地址和端口；

25 所述根据所述服务端口集合是否包括所述第一数据包中的 IP 地址和端口，以及，所述注册 IP 地址集合是否包括第一数据包中的 IP 地址，确定 TCP 通信会话中注册的通信设备的会话方向，包括：

若所述服务端口集合包括所述第一数据包中一组 IP 地址和端口，且所述注册 IP 地址集合包括所述一组 IP 地址和端口中的 IP 地址的情况下，确

定 TCP 通信会话中注册的通信设备的会话方向包括所述第一会话方向；

若所述服务端口集合不包括所述第一数据包中任意一组 IP 地址和端口，且所述注册 IP 地址集合包括所述第一数据包中一组 IP 地址和端口中的 IP 地址的情况下，确定 TCP 通信会话中注册的通信设备的会话方向包括所述

5 第二会话方向；

若所述服务端口集合包括所述第一数据包中一组 IP 地址和端口，且所述注册 IP 地址集合包括所述第一数据包中两组 IP 地址和端口中的 IP 地址的情况下，确定 TCP 通信会话中注册的通信设备的会话方向包括所述第一会话方向和所述第二会话方向。

10 4. 根据权利要求 2 所述的方法，其中，所述第一数据包包括两组 IP 地址和端口，所述服务端口集合包括未注册且作为服务端的通信设备的 IP 地址和端口；

所述根据所述服务端口集合是否包括所述第一数据包中的 IP 地址和端口，以及，所述注册 IP 地址集合是否包括第一数据包中的 IP 地址，确定

15 TCP 通信会话中注册的通信设备的会话方向，包括：

若所述服务端口集合包括所述第一数据包中一组 IP 地址和端口，且所述注册 IP 地址集合不包括所述一组 IP 地址和端口中的 IP 地址的情况下，确定 TCP 通信会话中注册的通信设备的会话方向包括所述第二会话方向；

若所述服务端口集合不包括所述第一数据包中任意一组 IP 地址和端口，且所述注册 IP 地址集合包括所述第一数据包中一组 IP 地址和端口中的 IP 地址的情况下，确定 TCP 通信会话中注册的通信设备的会话方向包括所述

20 第一会话方向；
若所述服务端口集合不包括所述第一数据包中任意一组 IP 地址和端口，且所述注册 IP 地址集合包括所述第一数据包中两组 IP 地址和端口中的 IP 地址的情况下，确定 TCP 通信会话中注册的通信设备的会话方向包括所述

25 第一会话方向和所述第二会话方向。
5. 根据权利要求 2 所述的方法，其中，所述根据 TCP 通信会话中注册的通信设备的会话方向，将所述第一 ACL 和/或所述第二 ACL 确定为所述目标 ACL，包括：

在 TCP 通信会话中注册的通信设备的会话方向包括所述第一会话方向的情况下，将所述第一 ACL 确定为所述目标 ACL；

在 TCP 通信会话中注册的通信设备的会话方向包括所述第二会话方向的情况下，将所述第二 ACL 确定为所述目标 ACL；

- 5 在 TCP 通信会话中注册的通信设备的会话方向包括所述第一会话方向和所述第二会话方向的情况下，将所述第一 ACL 和所述第二 ACL 确定为所述目标 ACL。

6. 根据权利要求 1 所述的方法，其中，所述服务端口集合包括注册且作为服务端的通信设备的 IP 地址和端口；

- 10 在所述接收第一数据包之前，还包括：

接收第二数据包，所述第二数据包具有请求及确认标识，所述第二数据包包括源 IP 地址和源端口以及目的 IP 地址和目的端口；

- 若所述注册 IP 地址集合包括所述第二数据包中的源 IP 地址，则将所述第二数据包中的源 IP 地址和源端口写入所述服务端口集合，按照所述第一 ACL，执行访问控制操作；
- 15 一 ACL，执行访问控制操作；

 若所述注册 IP 地址集合包括所述第二数据包中的目的 IP 地址，则按照所述第二 ACL，执行访问控制操作。

7. 根据权利要求 6 所述的方法，还包括：

- 若所述注册 IP 地址集合包括所述第二数据包中的目的 IP 地址但不包
- 20 括源 IP 地址，且所述服务端口集合包括所述第二数据包中的目的 IP 地址和目的端口，则从所述服务端口集合中删除所述第二数据包中的目的 IP 地址和目的端口。

8. 根据权利要求 1 所述的方法，其中，所述服务端口集合包括未注册且作为服务端的通信设备的 IP 地址和端口；

- 25 在所述接收第一数据包之前，还包括：

接收第二数据包，所述第二数据包具有请求及确认标识，所述第二数据包包括源 IP 地址和源端口以及目的 IP 地址和目的端口；

 若所述注册 IP 地址集合包括所述第二数据包中的目的 IP 地址但不包

括源 IP 地址，则将所述第二数据包中的源 IP 地址和源端口写入所述服务

端口集合，按照所述第二 ACL，执行访问控制操作；

若所述注册 IP 地址集合包括所述第二数据包中的源 IP 地址但不包括目的 IP 地址，则按照所述第一 ACL，执行访问控制操作；

若所述注册 IP 地址集合包括所述第二数据包中的源 IP 地址和目的 IP 地址，

5 则按照所述第一 ACL 和第二 ACL，执行访问控制操作。

9. 根据权利要求 8 所述的方法，还包括：

若所述注册 IP 地址集合包括所述第二数据包中的源 IP 地址但不包括目的 IP 地址，且所述服务端口集合包括所述第二数据包中的目的 IP 地址和目的端口，则从所述服务端口集合中删除所述第二数据包中的目的 IP 地址和目的端口。

10

10. 根据权利要求 1 所述的方法，在所述接收第一数据包之前，还包括：

接收第三数据包，所述第三数据包具有请求标识，所述第三数据包包括源 IP 地址和源端口以及目的 IP 地址和目的端口；

15

若所述注册 IP 地址集合包括所述第三数据包中的目的 IP 地址，则按照所述第一 ACL，执行访问控制操作；

若所述注册 IP 地址集合包括第二数据包中的源 IP 地址，则按照所述第二 ACL，执行访问控制操作。

11. 根据权利要求 1 所述的方法，还包括：

20

在一个注册的通信设备的会话方向同时包括所述第一会话方向和所述第二会话方向的情况下，执行预定访问控制策略；

其中，所述预定访问控制策略包括：

按照所述第一 ACL，执行访问控制操作；

或者，按照所述第二 ACL，执行访问控制操作；

25

或者，按照所述第一 ACL 和所述第二 ACL，执行访问控制操作。

12. 根据权利要求 1 至 11 中任意一项所述的方法，其中，ACL 包括所述所述第一 ACL 和/或所述第二 ACL，

按照 ACL，执行访问控制操作，包括：

在 ACL 包括禁止访问规则的情况下，若数据包符合任意一项所述禁止

访问规则，则阻断数据包所属的 TCP 通信会话；

在 ACL 包括允许访问规则的情况下，若数据包不符合任意一项所述允许访问规则，则阻断数据包所属的 TCP 通信会话；

数据包包括所述第一数据包、第二数据包、第三数据包中的至少一者。

5 13. 一种会话访问控制装置，包括：

接收模块，用于接收第一数据包，所述第一数据包包括建立传输控制协议 TCP 通信会话后传输的数据包；

访问控制表确定模块，用于基于所述第一数据包中的网络协议 IP 地址和端口、服务端口集合以及注册 IP 地址集合，将预设的第一访问控制表
10 ACL 和/或预设的第二 ACL 确定为目标 ACL，所述服务端口集合包括注册且作为服务端的通信设备的 IP 地址和端口，或，包括未注册且作为服务端的通信设备的 IP 地址和端口，服务端为 TCP 通信会话的接收方，所述注册 IP 地址集合包括注册的通信设备的 IP 地址，所述第一 ACL 与注册的通信设备的第一会话方向对应，所述第二 ACL 与注册的通信设备的第二会话方向对应；
15 向对应；

访问控制模块，用于按照所述目标 ACL，执行访问控制操作。

14. 一种防火墙设备，包括：处理器以及存储有计算机程序指令的存储器；

所述处理器执行所述计算机程序指令时实现如权利要求 1 至 12 中任意
20 一项所述的会话访问控制方法。

15. 一种计算机可读存储介质，所述计算机可读存储介质上存储有计算机程序指令，所述计算机程序指令被处理器执行时实现如权利要求 1 至 12 中任意一项所述的会话访问控制方法。

16. 一种计算机程序产品，包括计算机程序，所述计算机程序被处理器
25 器执行时实现权利要求 1 至 12 中任意一项所述的会话访问控制方法。