(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 111095862 B
(45)授权公告日 2021.10.01

(21)申请号 201880058908.4
(22)申请日 2018.09.11
(65)同一申请的已公布的文献号
申请公布号 CN 111095862 A
(43)申请公布日 2020.05.01
(30)优先权数据
15/702,355 2017.09.12 US
(85)PCT国际申请进入国家阶段日
2020.03.11
(86)PCT国际申请的申请数据
PCT/US2018/050411 2018.09.11
(87)PCT国际申请的公布数据
WO2019/055391 EN 2019.03.21
(73)专利权人 新纳聚克斯集团
地址 美国康涅狄格州
专利权人 范控股有限公司 韦恩·泰勒
(72)发明人 西恩·万·范
(74)专利代理机构 中原信达知识产权代理有限责任公司 11219
代理人 韩峰 孙志湧
(51)Int.Cl.
H04L 9/32(2006.01)
H04L 12/26(2006.01)
H04L 29/02(2006.01)
(56)对比文件
US 2017126740 A1,2017.05.04
US 2005283536 A1,2005.12.22
US 2012215911 A1,2012.08.23
CN 106209799 A,2016.12.07
CN 106790161 A,2017.05.31
审查员 毛韵楠

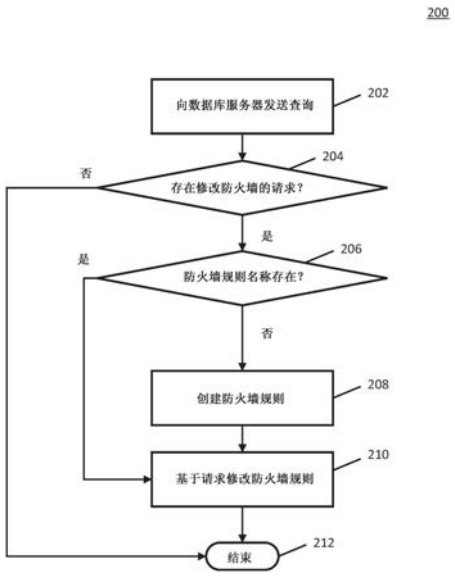
权利要求书3页 说明书10页 附图4页

(54)发明名称

基于动态IP地址修改防火墙的方法、系统和介质

(57)摘要

提供了用于基于动态互联网协议(IP)地址修改防火墙规则的方法、系统和介质。在一些实施例中,该方法包括:从数据库服务器接收修改保护远程计算机的防火墙的防火墙规则的请求,其中,该请求包括发起到远程计算机的连接的用户设备的IP地址,并且其中,防火墙规则指示被允许建立到远程计算机的连接的设备的IP地址;确定是否要将用户设备的IP地址添加到防火墙规则中;以及响应于确定要将用户设备的IP地址添加到防火墙规则中,将当前IP地址添加到防火墙规则中。



CN 111095862 B

1.一种用于基于动态互联网协议(IP)地址修改防火墙规则的方法,包括:

利用硬件处理器,识别用户设备的用户有权限与之建立远程连接的至少一个计算机;

使得所述至少一个计算机的指示被呈现给所述用户以供所述用户选择;

从所述用户接收对所述至少一个计算机中的计算机的名称的选择;

从数据库服务器接收用于修改保护所述计算机的防火墙的防火墙规则的请求,其中,所述请求包括所述用户设备的当前IP地址,并且其中,所述防火墙规则指示出被允许建立到所述计算机的连接的设备的IP地址;

确定所述用户设备是否正在使用特定类型的加密;

基于所述用户设备是否正在使用所述特定类型的加密,来确定是否要将所述用户设备的所述当前IP地址添加到所述防火墙规则中;以及

响应于确定要将所述用户设备的所述当前IP地址添加到所述防火墙规则中,将所述当前IP地址添加到所述防火墙规则中。

2.根据权利要求1所述的方法,进一步包括:

确定是否要从所述防火墙规则中移除所述用户设备的所述当前IP地址;以及

响应于确定要从所述防火墙规则中移除所述用户设备的所述当前IP地址,从所述防火墙规则中移除所述当前IP地址。

3.根据权利要求1所述的方法,进一步包括:

确定所述防火墙规则不存在;以及

响应于确定所述防火墙规则不存在,创建所述防火墙规则。

4.根据权利要求1所述的方法,其中,

所述请求包括指示出所述防火墙规则的防火墙规则名称。

5.根据权利要求1所述的方法,其中,

响应于被发送到所述服务器的查询,从所述服务器接收所述请求。

6.根据权利要求1所述的方法,其中,

确定是否要将所述用户设备的所述当前IP地址添加到所述防火墙规则也基于所述用户设备是否正在使用特定类型的认证。

7.根据权利要求6所述的方法,其中,

确定是否要将所述用户设备的所述当前IP地址添加到所述防火墙规则也基于所述用户设备是否正在使用特定类型的远程桌面协议。

8.一种用于基于动态互联网协议(IP)地址修改防火墙规则的系统,所述系统包括:

第一硬件处理器,所述第一硬件处理器被编程以:

识别用户设备的用户有权限与之建立远程连接的至少一个计算机;

使得所述至少一个计算机的指示被呈现给所述用户以供所述用户选择;

从所述用户接收对所述至少一个计算机中的计算机的名称的选择;以及

第二硬件处理器,所述第二硬件处理器被编程以:

从服务器接收用于修改保护所述计算机的防火墙的防火墙规则的请求,其中,所述请求包括所述用户设备的当前IP地址,并且其中,所述防火墙规则指示出被允许建立到所述计算机的连接的设备的IP地址;

确定所述用户设备是否正在使用特定类型的加密;

基于所述用户设备是否正在使用所述特定类型的加密,来确定是否要将所述用户设备的所述当前IP地址添加到所述防火墙规则中;以及

响应于确定要将所述用户设备的所述当前IP地址添加到所述防火墙规则中,将所述当前IP地址添加到所述防火墙规则中。

9.根据权利要求8所述的系统,其中,所述第二硬件处理器进一步被编程以:

确定是否要从所述防火墙规则中移除所述用户设备的所述当前IP地址;以及

响应于确定要从所述防火墙规则中移除所述用户设备的所述当前IP地址,从所述防火墙规则中移除所述当前IP地址。

10.根据权利要求8所述的系统,其中,所述第二硬件处理器进一步被编程以:

确定所述防火墙规则不存在;以及

响应于确定所述防火墙规则不存在,创建所述防火墙规则。

11.根据权利要求8所述的系统,其中,

所述请求包括指示出所述防火墙规则的防火墙规则名称。

12.根据权利要求8所述的系统,其中,

响应于被发送到所述服务器的查询,从所述服务器接收所述请求。

13.根据权利要求8所述的系统,其中,

确定是否要将所述用户设备的所述当前IP地址添加到所述防火墙规则也基于所述用户设备是否正在使用特定类型的认证。

14.根据权利要求13所述的系统,其中,

确定是否要将所述用户设备的所述当前IP地址添加到所述防火墙规则也基于所述用户设备是否正在使用特定类型的远程桌面协议。

15.一种包含计算机可执行指令的非暂时性计算机可读介质,所述计算机可执行指令在由多个处理器执行时使所述多个处理器执行用于基于动态互联网协议(IP)地址修改防火墙规则的方法,所述方法包括:

使用硬件处理器,识别用户设备的用户有权限与之建立远程连接的至少一个计算机;

使得所述至少一个计算机的指示被呈现给所述用户以供所述用户选择;

从所述用户接收对所述至少一个计算机中的计算机的名称的选择;

从数据库服务器接收用于修改保护所述计算机的防火墙的防火墙规则的请求,其中,所述请求包括所述用户设备的当前IP地址,并且其中,所述防火墙规则指示出被允许建立到所述计算机的连接的设备的IP地址;

确定所述用户设备是否正在使用特定类型的加密;

基于所述用户设备是否正在使用所述特定类型的加密,来确定是否要将所述用户设备的所述当前IP地址添加到所述防火墙规则中;以及

响应于确定要将所述用户设备的所述当前IP地址添加到所述防火墙规则中,将所述当前IP地址添加到所述防火墙规则中。

16.根据权利要求15所述的非暂时性计算机可读介质,其中,所述方法进一步包括:

确定是否要从所述防火墙规则中移除所述用户设备的所述当前IP地址;以及

响应于确定要从所述防火墙规则中移除所述用户设备的所述当前IP地址,从所述防火墙规则中移除所述当前IP地址。

17.根据权利要求15所述的非暂时性计算机可读介质,其中,所述方法进一步包括:

确定所述防火墙规则不存在;以及

响应于确定所述防火墙规则不存在,创建所述防火墙规则。

18.根据权利要求15所述的非暂时性计算机可读介质,其中,

所述请求包括指示出所述防火墙规则的防火墙规则名称。

19.根据权利要求15所述的非暂时性计算机可读介质,其中,

响应于被发送到所述服务器的查询,从所述服务器接收所述请求。

20.根据权利要求15所述的非暂时性计算机可读介质,其中,

确定是否要将所述用户设备的所述当前IP地址添加到所述防火墙规则也基于所述用户设备是否正在使用特定类型的认证。

21.根据权利要求20所述的非暂时性计算机可读介质,其中,

确定是否要将所述用户设备的所述当前IP地址添加到所述防火墙规则也基于所述用户设备是否正在使用特定类型的远程桌面协议。

基于动态IP地址修改防火墙的方法、系统和介质

[0001] 相关申请的交叉引用

[0002] 本申请要求2017年9月12日提交的美国专利申请No.15/702,355的权益，其通过引用其整体合并于此。

技术领域

[0003] 所公开的主题涉及用于基于动态IP地址修改防火墙的方法、系统和介质。

背景技术

[0004] 许多用户想要建立到远程计算机的远程桌面连接。例如，远离他或她的办公室的用户可能想经由公用网络连接使用膝上型计算机来建立到工作计算机的远程桌面连接。但是，在某些情况下，用户可能会被阻止建立远程桌面连接，因为防火墙会阻止未知地址访问远程计算机。另外，在某些情况下，即使可以将用户的IP地址编程到这样的防火墙中，但由于该IP地址是由用户的互联网服务提供商(ISP)动态分配的，因此该用户计算机的IP地址也可能是未知的。

[0005] 因此，期望提供用于基于动态IP地址修改防火墙的新方法、系统和介质。

发明内容

[0006] 提供用于基于动态IP地址修改防火墙的方法、系统和介质。根据所公开的主题的一些实施例，提供一种用于基于动态IP地址修改防火墙的方法，该方法包括：从数据库服务器接收修改保护远程计算机的防火墙的防火墙规则的请求，其中，该请求包括发起到远程计算机的连接的用户设备的IP地址，并且其中，防火墙规则指示出被允许建立到远程计算机的连接的设备的IP地址；确定是否要将用户设备的IP地址添加到防火墙规则中；以及响应于确定要将用户设备的IP地址添加到防火墙规则中，将当前IP地址添加到防火墙规则中。

[0007] 根据所公开的主题的一些实施例，提供一种用于基于动态IP地址修改防火墙的系统，该系统包括：硬件处理器，该硬件处理器被编程为：从数据库服务器接收修改保护远程计算机的防火墙的防火墙规则的请求，其中，该请求包括发起到远程计算机的连接的用户设备的IP地址，并且其中，防火墙规则指示出被允许建立到远程计算机的连接的设备的IP地址；确定是否要将用户设备的IP地址添加到防火墙规则中；以及响应于确定要将用户设备的IP地址添加到防火墙规则中，将当前IP地址添加到防火墙规则中。

[0008] 根据所公开的主题的一些实施例，提供包含计算机可执行指令的非暂时性计算机可读介质，该计算机可执行指令在由处理器执行时使处理器执行用于基于动态IP地址修改防火墙的方法。该方法包括：从数据库服务器接收修改保护远程计算机的防火墙的防火墙规则的请求，其中，该请求包括发起到远程计算机的连接的用户设备的IP地址，并且其中，防火墙规则指示出被允许建立到远程计算机的连接的设备的IP地址；确定是否要将用户设备的IP地址添加到防火墙规则中；以及响应于确定要将用户设备的IP地址添加到防火墙规

则中，将当前IP地址添加到防火墙规则中。

[0009] 根据所公开的主题的一些实施例，提供一种用于基于动态IP地址修改防火墙的系统，该系统包括：用于从服务器数据库接收修改保护远程计算机的防火墙的防火墙规则的请求的装置，其中，该请求包括发起到远程计算机的连接的用户设备的IP地址，并且其中，防火墙规则指示出被允许建立到远程计算机的连接的设备的IP地址；用于确定是否要将用户设备的IP地址添加到防火墙规则中的装置；以及响应于确定要将用户设备的IP地址添加到防火墙规则中，用于将当前IP地址添加到防火墙规则中的装置。

[0010] 在一些实施例中，系统进一步包括：用于确定是否将用户设备的IP地址从防火墙规则中移除的装置；以及响应于确定要从防火墙规则中移除用户设备的IP地址，用于从防火墙规则中移除当前IP地址的装置。

[0011] 在一些实施例中，系统进一步包括：用于确定防火墙规则不存在的装置；以及响应于确定防火墙规则不存在，用于创建防火墙规则的装置。

[0012] 在一些实施例中，请求包括指示出防火墙规则的防火墙规则名称。

[0013] 在一些实施例中，响应于发送到数据库服务器的查询，从数据库服务器接收请求。

附图说明

[0014] 当结合以下附图考虑时，参考对所公开主题的以下详细描述，可以更充分地理解所公开主题的各种目的、特征和优点，其中，相似的附图标记标识相似的元素。

[0015] 图1示出根据所公开的主题的一些实施例的用于生成向防火墙添加IP地址的请求的过程的示例。

[0016] 图2示出根据所公开的主题的一些实施例的用于基于检索到的请求来修改防火墙的过程的示例。

[0017] 图3示出根据所公开的主题的一些实施例的适用于基于动态IP地址来修改防火墙的说明性系统的示意图。

[0018] 图4示出根据所公开的主题的一些实施例的可以在图3的服务器和/或用户设备中使用的硬件的详细示例。

具体实施方式

[0019] 根据各种实施例，提供用于基于动态IP地址修改防火墙的机制(其可以包括方法、系统和介质)。

[0020] 在一些实施例中，本文描述的机制可以动态地和远程地将IP地址添加到防火墙的未阻止的IP地址的列表中，以便例如用户能够建立到受防火墙保护的远程计算机的远程桌面连接。在一些实施例中，用户设备可以具有动态互联网协议(IP)地址。在一些这样的实施例中，用户设备可以向数据库服务器发送消息，该消息包括与用户设备相关联的当前IP地址以及向与远程计算机相关联的防火墙规则添加IP地址的请求。在一些实施例中，远程计算机可以向数据库服务器查询发送查询以检索当前的IP地址，并且然后可以更新与远程计算机相关联的防火墙规则以包括当前的IP地址。

[0021] 转向图1，示出根据所公开的主题的一些实施例的用于请求将与用户设备相关联的IP地址添加到防火墙的过程的示例100。在一些实施例中，过程100的框可以由任何合适

的设备执行，诸如，寻求访问由防火墙保护的远程计算机(例如，以建立与远程计算机的远程桌面连接)的用户设备。更具体地，在一些实施例中，过程100的框可以由在设备上执行的程序(例如，web应用，独立应用和/或任何其他合适的程序)执行。

[0022] 过程100可以通过向数据库服务器(例如，如在图3中所示并结合图3在下面所描述的数据库服务器302)认证执行过程100的用户设备在102处开始。例如，在一些实施例中，用户设备的用户可以使用任何合适的技术或技术组合来登录到与数据库服务器相关联的帐户。作为更具体的示例，在一些实施例中，用户可以经由用户界面输入与帐户相关联的用户名和密码。作为另一个更具体的示例，在一些实施例中，可以使用与用户相关联的生物特征信息向该帐户认证用户。在一些实施例中，可以使用任何其他合适的认证技术向数据库服务器认证用户设备。

[0023] 过程100可以在104处识别与向保护远程计算机的防火墙添加IP地址的请求有关的信息。例如，在一些实施例中，过程100可以确定用户设备将要连接到的远程计算机的标识符。在一些实施例中，过程100可以使用任何合适的技术来确定远程计算机的标识符。例如，在一些实施例中，过程100可以通过经由用户界面接收标识远程计算机的名称的选择来确定远程计算机的标识符。作为另一示例，在一些实施例中，过程100可以识别用户设备的用户可以有权限与之建立远程连接的一个或多个远程计算机。作为更具体的示例，在一些实施例中，过程100可以识别与用户的名称相关联的特定远程计算机。作为另一个更具体的示例，在一些实施例中，过程100可以基于与用户相关联的用户类型(例如，该用户在每个远程计算机上具有管理员特权和/或任何其他合适的用户类型)来识别多台远程计算机。在一些这样的实施例中，过程100可以使被标识的远程计算机的指示出被呈现给用户(例如，经由用户界面)以供用户选择。

[0024] 作为另一个示例，在一些实施例中，过程100可以确定与用户设备相关联的信息。作为更具体的示例，在一些实施例中，过程100可以确定与用户设备相关联的当前IP地址。作为另一个更具体的示例，在一些实施例中，过程100可以确定用户设备的地理位置(例如，与用户设备的当前位置相关联的纬度和/或经度、指示出用户设备当前不在用户办公室的信息和/或任何其他合适的地理位置)。

[0025] 作为又一示例，在一些实施例中，过程100可以确定与请求(诸如，将当前IP地址添加到与远程计算机相关联的防火墙规则的列表中，或者将当前IP地址从与远程计算机关联的防火墙规则的列表中移除)相关联的动作。作为更具体的示例，在过程100确定用户设备将要建立到远程计算机的新连接的情况下，过程100可以确定当前IP地址将被添加到防火墙规则的列表中。作为另一个更具体的示例，在过程100确定要终止到远程计算机的连接(例如，基于来自用户设备的用户的显式输入，基于用户设备上在没有活动的情况下流逝的持续时间，和/或基于任何其他合适的信息)的情况下，过程100可以确定当前IP地址将被从防火墙规则的列表中移除。

[0026] 在一些实施例中，过程100可以确定与修改防火墙规则的请求相对应的任何合适的标准。例如，在请求是将IP地址添加到防火墙规则的列表的情况下，过程100可以确定要被包括在该请求中的任何合适的定时信息。作为更具体的示例，在一些实施例中，过程100可以确定请求有效的持续时间(例如，一个小时，两个小时，一天，一个月和/或任何其他合适的持续时间)、要从防火墙规则中移除IP地址的日期和/或时间、要将IP地址包括在防火

墙规则中的时间窗口(例如,在特定日期的下午1点至下午3点之间,一周中的特定几天,一天中的特定几个小时,和/或任何其他合适的时间窗口)和/或任何其他合适的定时信息。作为另一个更具体的示例,在一些实施例中,过程100可以确定针对其请求有效的用户设备与远程计算机之间的连接的类型。作为特定示例,在一些实施例中,如果用户设备正在使用特定级别的加密和/或加密协议,使用特定认证技术(例如,多因素认证和/或任何其他合适的技术)和/或任何其他合适的标准来实现特定的远程桌面连接技术,则过程100可以确定请求是有效的。

[0027] 在106处,过程100可以基于所识别的信息来生成修改保护远程计算机的防火墙的请求。例如,在一些实施例中,请求可以包括远程计算机的标识符。作为另一个示例,在一些实施例中,请求可以包括与用户设备相关联的当前IP地址。作为又一个示例,在一些实施例中,请求可以包括动作值参数,该动作值参数指示:是否要将当前IP地址添加到防火墙规则的列表中,该防火墙规则指示被允许建立到远程计算机的连接的设备的IP地址;是否要将当前IP地址从防火墙规则的列表中移除;和/或任何其他合适的动作。作为又一示例,在一些实施例中,请求可以包括与日期和/或时间相关联的任何合适的定时信息,该日期和/或时间是与用户设备相关联的IP地址将被包括在防火墙规则中的日期和/或时间,该防火墙规则指示出被允许建立到远程计算机的连接的设备的IP地址。作为更具体的示例,如上所述,请求中包括的定时信息可以指示出要在下述的定时将IP地址添加到防火墙规则中,所述定时包括:在特定的持续时间(例如,一小时、两小时、一天、一小时、一个月,和/或任何其他合适的持续时间)、直到特定日期和/或时间、在特定时间范围内(例如,下午1点至5点之间、特定日期的下午1点直到另一个日期的下午1点之间和/或任何其他合适的时间范围)、在一周的特定几天(例如,星期一、工作日、周末和/或任何其他合适的日期)、在一天的特定几个小时(例如,晚上9点之后、上午9点至下午5点之间和/或任何其他合适的小时)和/或任何其他合适的定时信息或定时信息的组合。作为又一个具体示例,如上所述,如果IP地址要被包括在指示被允许建立到远程计算机的连接的设备的IP地址的防火墙规则中,则请求可以包括要满足的标准。作为更具体的示例,如上所述,标准可以包括要使用特定类型的连接协议(例如,必须使用特定的远程桌面连接技术和/或任何其他合适的协议)、要使用特定类型或级别的加密、要使用特定类型的认证(例如,多因素认证和/或任何其他合适类型的认证)和/或任何其他合适的标准。

[0028] 在一些实施例中,请求可以包括防火墙规则名称。例如,在一些实施例中,防火墙名称可以指示出请求与关联于防火墙的入站规则、与防火墙相关联的出站规则和/或任何其他合适的规则有关。作为另一个示例,在一些实施例中,防火墙名称可以指示出请求与在远程计算机上执行特定活动(诸如,建立远程桌面连接,文件传输,远程打印和/或任何其他合适的活动)有关。作为更具体的示例,在一些实施例中,防火墙名称可以指示出请求与关联于用户设备和远程计算机之间的连接的特定端口有关。

[0029] 在108处,过程100可以将请求发送到数据库服务器(例如,如在图3中所示和结合图3在下面所描述的数据库服务器302),以供数据库服务器存储。在一些实施例中,过程100可以使用任何合适的技术将请求发送到数据库服务器。例如,在一些实施例中,如在图3中所示和结合图3在下面更详细描述的,过程100可以经由连接到设备的网络路由器发送请求,该网络路由器经由通信网络将设备连接到数据库服务器。

[0030] 在一些实施例中，过程100可以在任何合适的时间循环回到框104。例如，在一些实施例中，过程100可以循环回到框104，并且响应于确定已经过去了一定量的时间、与设备相关联的IP地址已更改，和/或在任何其他合适的时间点，识别用于生成对远程计算机的更新与该远程计算机相关联的防火墙规则的请求的信息。在一些实施例中，在当用户设备连接到远程计算机时过程100循环回到框104的情况下，过程100可以确定任何合适的信息子集。例如，在一些实施例中，过程100可以循环回到框104，并且可以确定更新的定时信息、更新的连接标准和/或任何其他合适的更新的信息。

[0031] 转向图2，示出根据所公开的主题的一些实施例的用于修改用于保护远程计算机的防火墙的防火墙规则的过程的示例200。在一些实施例中，过程200的框可以在保护远程计算机的防火墙设备(例如，如在图3中所示和结合图3在下面所描述的防火墙314)上和/或在使用防火墙的远程计算机设备上执行。

[0032] 过程200可以通过查询数据库服务器(例如，如在图3中所示和结合图3在下面所描述的数据库服务器302)以确定修改与远程计算机相关联的防火墙的请求是否可用而在202处开始。例如，在一些实施例中，数据库服务器可以是接收并存储对防火墙的修改的请求的数据库服务器。作为更具体的示例，在一些实施例中，数据库服务器可以从用户设备接收修改防火墙规则以包括用户设备的IP地址的请求，如以上结合图1所描述的。在一些实施例中，过程200可以在向数据库服务器发送的查询中包括任何合适的信息。例如，在一些实施例中，过程200可以包括远程计算机的标识符，数据库服务器可以使用该标识符来识别针对远程计算机的请求。

[0033] 在204处，过程200可以确定是否存在指向远程计算机的修改保护远程计算机的防火墙的可用请求。过程200可以基于任何合适的信息来确定是否存在可用请求。例如，在一些实施例中，过程200可以基于对从数据库服务器接收到的查询的响应来确定是否存在可用请求。作为更具体的示例，在一些实施例中，在没有可用请求的情况下，过程200可以从数据库服务器接收指示出未发现与远程计算机相对应的请求的响应。作为另一个更具体的示例，在一些实施例中，在存在可用请求的情况下，过程200可以从数据库服务器接收包括与该请求相对应的信息的响应。

[0034] 在过程200从数据库服务器接收到指示出从特定用户设备接收到的修改防火墙规则的请求可用的响应的情况下，该响应可以包括与该请求相对应的任何合适的信息。例如，在一些实施例中，信息可以包括与用户设备相关联的当前IP地址。作为另一个示例，在一些实施例中，该信息可以包括指示出将修改特定防火墙规则的方式的动作值。作为更具体的示例，在一些实施例中，动作值可以指示出与用户设备相关联的IP地址将被添加到特定防火墙规则，该特定防火墙规则指示出被允许建立到远程计算机的连接的设备的IP地址。在一些这样的实施例中，动作值和/或包括在请求中的信息可以附加地包括定时信息，该定时信息指示出在其间IP地址将被包括在防火墙规则中的时间段，如结合图1的框104和106在上面更详细地描述的。作为另一个更具体的示例，在一些实施例中，动作值可以指示出与用户设备相关联的IP地址将从特定防火墙规则中移除，该特定防火墙规则指示出被允许建立到远程计算机的连接的设备的IP地址。作为又一个示例，在一些实施例中，信息可以包括一个或多个防火墙规则名称。作为更具体的示例，在一些实施例中，防火墙规则名称可以指示出请求对应于入站规则和/或出站规则。作为另一个更具体的示例，在一些实施例中，防火

墙规则名称可以指示出请求对应于特定的活动，诸如，建立远程桌面连接、打印、文件传输和/或任何其他合适的活动。

[0035] 注意，在一些实施例中，过程200可以直接从数据库服务器接收与请求相对应的信息，而不向数据库服务器发送查询。例如，在一些实施例中，数据库服务器可以在一旦从用户设备接收到请求时将从用户设备接收到的请求推送到其指向的远程计算机或保护远程计算机的防火墙。作为更具体的示例，在一些实施例中，数据库服务器可以维持到远程计算机和/或保护远程计算机的防火墙的连接(例如，虚拟专用网络和/或任何其他合适类型的连接)，并且可以使用该连接来发送与请求相对应的信息。在一些这样的实施例中，框202和204可以被省略。

[0036] 如果在204处，过程200确定不存在可用请求(在204处为“否”)，则过程200可以在212处结束。

[0037] 如果在204处，过程200确定存在可用请求(在204处为“是”)，则在206处，过程200可以确定与该请求相对应的防火墙规则名称是否已存在。注意，防火墙规则名称可以是与防火墙规则的任何合适集合相关联的名称，诸如，入站规则、出站规则、与特定活动相对应的规则和/或任何其他合适的规则。过程200可以以任何合适的方式确定防火墙规则名称是否存在。例如，在一些实施例中，过程200可以确定防火墙规则名称是否被包括在存储在防火墙设备的存储器和/或远程计算机的存储器(例如，防火墙314的存储器404和/或远程计算机304的存储器404，如在图3和图4中所示和结合图3和图4在下面所描述的)的防火墙规则名称的列表中。注意，在请求包括多个防火墙规则名称(例如，对应于入站规则的第一防火墙规则、对应于出站规则的第二防火墙规则名称和/或任何其他合适的防火墙规则名称)的情况下，过程200可以确定多个防火墙规则名称中的每一个是否已经存在。

[0038] 如果在206处，过程200确定防火墙规则名称已经存在(在206处为“是”)，则过程200可以进行到框210。在请求中包括多个防火墙规则名称的情况下，过程200可以响应于确定所有防火墙规则名称已经存在而进行到框210。

[0039] 如果在206处，过程200确定防火墙规则名称尚不存在(在206处为“否”)，则过程200可以在208处创建与防火墙规则名称相对应的防火墙规则。例如，在一些实施例中，进程200可以创建与防火墙规则名称相对应的新列表。

[0040] 在210处，过程200可以基于请求来修改与防火墙规则名称相对应的防火墙规则。在一些实施例中，过程200可以基于请求中包括的任何合适的信息(诸如，指示出将要修改防火墙规则的方式的动作参数值、定时信息、标准信息和/或任何其他合适的信息)来修改防火墙规则。例如，在过程200确定要从防火墙规则中移除用户设备的IP地址的情况下，过程200可以从指示出被允许建立到远程计算机的连接的用户设备的IP地址的列表中删除该IP地址。在一些实施例中，过程200可以使用任何合适的技术或技术组合来确定是否要从防火墙规则中移除用户设备的IP地址。例如，在一些实施例中，请求可以包括从防火墙规则中移除IP地址(例如，基于动作参数值)的显式指令。作为另一示例，在一些实施例中，过程200可以基于请求中包括的定时信息或标准信息来确定要从防火墙规则中移除用户设备的IP地址。作为更具体的示例，在请求指示与IP地址将被包括在防火墙规则中的时间相对应的定时信息的情况下，过程200可以确定当前时间是否在IP地址将被包括在防火墙规则中的时间之外。作为特定示例，在定时信息指示IP地址将被包括在防火墙规则中直到特定日期

的特定时间的情况下，过程200可以确定当前时间是否在特定时间和特定日期之后。作为另一个更具体的示例，在标准信息指示必须使用特定类型的连接协议、认证协议和/或加密协议的情况下，过程200可以响应于确定在当前时间不满足标准而确定用户设备的IP地址将被移除。

[0041] 作为另一个示例，在过程200确定将修改防火墙规则以包括用户设备的IP地址的情况下，过程200可以将IP地址添加到与防火墙规则名称相对应的防火墙规则中。在一些实施例中，在将用户设备的IP地址添加到防火墙规则之前，过程200可以确定是否满足任何合适的标准。例如，在一些实施例中，过程200可以确定当前时间是否在请求中包括的定时信息所指示的时间范围内(该定时信息指定了IP地址将被包括在防火墙规则中的时间)，并且可以响应于确定当前时间包括在时间范围内而修改防火墙规则以包括IP地址。作为另一示例，在一些实施例中，过程200可以确定是否满足关联于与用户设备的连接的标准。作为更具体的示例，在一些实施例中，过程200可以确定用户设备是否正在使用特定类型或级别的加密、特定类型或级别的认证、特定类型的远程桌面协议和/或任何其他合适的标准，并且可以响应于确定满足标准而将用户设备的IP地址添加到防火墙规则中。作为另一个更具体的示例，在一些实施例中，过程200可以确定用户设备的位置是否满足特定地理信息(例如，用户设备当前是否位于特定地理区域内，用户设备当前是否不在该地理区域内和/或任何其他合适的地理信息)。作为具体示例，在一些实施例中，过程200可以响应于确定指示用户设备的位置的地理信息指示用户设备当前位于特定位置或位置组中(例如，在特定国家组中和/或在任何其他合适的位置组中)，确定用户设备的IP地址将被添加到防火墙规则中。

[0042] 注意，在一些实施例中，可以由数据库服务器执行确定在修改防火墙规则之前是否满足任何合适的标准。例如，在一些实施例中，数据库服务器可以确定是否满足与定时信息、连接信息、地理信息和/或任何其他合适信息有关的标准，并且，如果不满足标准，则数据库服务器可以删除所述请求，而不将请求发送到防火墙设备和/或远程计算机。

[0043] 过程200可以在212处结束。另外或可替选地，在一些实施例中，过程200可以循环回到框202，并且可以查询数据库服务器以确定是否已经接收到修改防火墙规则的附加或更新请求。

[0044] 转向图3，示出根据所公开的主题的一些实施例可以使用的用于修改防火墙规则的硬件的示例300。如图所示，硬件300可以包括数据库服务器302、远程计算机304、通信网络306、一个或多个用户设备308(诸如，用户设备310和312)和/或防火墙314。

[0045] 数据库服务器302可以是用于存储用于修改保护远程计算机304的防火墙的信息的任何合适的服务器。例如，在一些实施例中，数据库服务器302可以从尝试建立到远程计算机304的远程连接的用户设备308接收请求，如上面结合图1所描述的。作为另一示例，在一些实施例中，数据库服务器302可以将存储的请求和/或与存储的请求相对应的信息发送到远程计算机304，如上面结合图2所描述的。

[0046] 远程计算机304可以是接收来自用户设备308的访问请求的任何合适的设备。例如，在一些实施例中，用户设备308可以建立与远程计算机304的远程桌面连接。在一些实施例中，远程计算机304可以由防火墙314保护，如上面结合图2所描述的。

[0047] 在一些实施例中，通信网络306可以是一个或多个有线和/或无线网络的任何合适的组合。例如，通信网络306可以包括互联网、内部网、广域网(WAN)、局域网(LAN)、无线网

络,数字用户线(DSL)网络、帧中继网络、异步传输模式(ATM)网络、虚拟专用网(VPN)和/或任何其他合适的通信网络中的任何一个或多个。用户设备308可以通过一个或多个通信链路连接到通信网络306,该通信网络306可以经由一个或多个通信链路链接到数据库服务器302和远程计算机304。通信链路可以是适合于在用户设备308、数据库服务器302和远程计算机304之间传送数据的任何通信链路,诸如,网络链路、拨号链路、无线链路、硬连线链路、任何其他合适的通信链路或这些链路的任何合适组合。在一些实施例中,经由通信网络306的通信可以是通过与任何合适类型的通信协议(诸如,传输控制协议(TCP)、用户数据报协议(UDP)和/或任何其他合适协议)相对应的发送的网络分组。

[0048] 用户设备308可以包括适合于与数据库服务器302和/或远程计算机304通信的任何一个或多个用户设备(诸如,用户设备310和/或312)。例如,在一些实施例中,用户设备308可以包括移动设备,诸如,手机、平板电脑、可穿戴计算机、膝上型计算机、交通工具(例如,汽车、船只、飞机或任何其他合适的交通工具)信息和/或娱乐系统、和/或任何其他合适的移动设备。作为另一示例,在一些实施例中,用户设备308可以包括非移动设备,诸如,电视、投影仪设备、游戏控制台、台式计算机和/或任何其他合适的非移动设备。在一些实施例中,用户设备308可以建立与远程计算机304的远程桌面连接。

[0049] 在一些实施例中,防火墙314可以是用于保护远程计算机304的任何合适的设备。例如,在一些实施例中,防火墙314可以是存储和维护与用户设备相关联的IP地址的列表的设备,该用户设备被允许建立与远程计算机304的连接和/或被阻止建立与远程计算机304的连接。注意,尽管防火墙314被示出为与远程计算机304分离的设备,但在某些实施例中,防火墙314可以与远程计算机304结合。

[0050] 在一些实施例中,尽管数据库服务器302和远程计算机304被示为两个设备,但是数据库服务器302和/或远程计算机304执行的功能可以使用任何合适数量(包括仅一个)的设备来执行。例如,在一些实施例中,可以使用一个、三个或更多设备来实现由数据库服务器302和/或远程计算机304执行的功能。

[0051] 尽管在图3中示出两个用户设备310和312以避免使附图过于复杂,但在一些实施例中可以使用任何合适数量的用户设备(包括仅一个)和/或任何合适类型的用户设备。

[0052] 在一些实施例中,可以使用任何合适的硬件来实现数据库服务器302、远程计算机304和用户设备308。例如,在一些实施例中,可以使用任何合适的通用计算机或专用计算机来实现设备302、304和/或308。例如,可以使用专用计算机来实现移动电话。任何这样的通用计算机或专用计算机可以包括任何合适的硬件。例如,如在图4的示例硬件400中所图示的,这样的硬件可以包括硬件处理器402、存储器和/或存储装置404、输入设备控制器406、输入设备408、显示/音频驱动器410、显示和音频输出电路412、通信接口414、天线416和总线418。

[0053] 在一些实施例中,硬件处理器402可以包括任何合适的硬件处理器,诸如,微处理器、微控制器、数字信号处理器、专用逻辑和/或用于控制通用计算机或专用计算机的运行的任何其他合适的电路。在一些实施例中,硬件处理器402可以由存储在用户设备308的存储器和/或存储装置404中的计算机程序控制。例如,在一些实施例中,计算机程序可以使硬件处理器402执行如上面结合图1描述的过程(或其部分)。在一些实施例中,硬件处理器402可以由存储在防火墙314和/或远程计算机304的存储器和/或存储装置404中的计算机程序

控制。例如,在一些实施例中,计算机程序可以使硬件处理器402执行如上面结合图2描述的过程(或其部分)。

[0054] 在一些实施例中,存储器和/或存储装置404可以是用于存储程序、数据、媒体内容和/或任何其他合适的信息的任何合适的存储器和/或存储装置。例如,存储器和/或存储器404可以包括随机存取存储器、只读存储器、闪存、硬盘存储器、光学介质和/或任何其他合适的存储器。

[0055] 在一些实施例中,输入设备控制器406可以是用于控制和接收来自一个或多个输入设备408的输入的任何合适的电路。例如,输入设备控制器406可以是用于接收来自触摸屏、键盘、鼠标、一个或多个按钮、语音识别电路、麦克风、相机、光学传感器、加速度计、温度传感器、近场传感器和/或任何其他类型的输入设备的输入的电路。

[0056] 在一些实施例中,显示/音频驱动器410可以是用于控制和驱动到一个或多个显示/音频输出设备412的输出的任何合适的电路。例如,显示/音频驱动器410可以是用于驱动触摸屏、平板显示器、阴极射线管显示器、投影仪、一个或多个扬声器和/或任何其他合适的显示和/或呈现设备的电路。

[0057] 通信接口414可以是用于与一个或多个通信网络(诸如如图3所示的网络306)接口的任何合适的电路。例如,接口414可以包括网络接口卡电路、无线通信电路和/或任何其他合适类型的通信网络电路。

[0058] 在一些实施例中,天线416可以是用于与通信网络(例如,通信网络306)无线通信的任何合适的一个或多个天线。在一些实施例中,可以省略天线416。

[0059] 在一些实施例中,总线418可以是用于在两个或更多个组件402、404、406、410和414之间通信的任何合适的机制。

[0060] 根据一些实施例,任何其他合适的组件可以被包括在硬件400中。

[0061] 在一些实施例中,图1和图2的过程的上述方框中的至少一些可以以任何次序或顺序(不限于在附图示出和结合附图描述的次序和顺序)来执行或进行。同样,图1和图2的上述方框中的一些可以在适当时基本上同时地或并行地执行或进行,以减少时延和处理时间。附加地或可替选地,图1和图2的过程的上述方框中的一些可以省略。

[0062] 在一些实施例中,任何合适的计算机可读介质可以用于存储用于执行本文的功能和/或过程的指令。例如,在一些实施例中,计算机可读介质可以是暂时的或非暂时的。例如,非暂时性计算机可读介质可以包括下述介质,诸如,非暂时性形式的磁性介质(诸如,硬盘、软盘和/或任何其他合适的磁性介质)、非暂时性形式的光学介质(诸如,光盘、数字视频光盘、蓝光光盘和/或其他任何合适的光学介质)、非暂时性形式的半导体介质(诸如,闪存、电可编程只读存储器(EPROM)、电可擦除可编程只读存储器(EEPROM)和/或任何其他合适的半导体介质)、在传输过程中不是转瞬即逝型的或者缺乏永久性表象的任何合适介质和/或任何合适的非暂时性有形介质。作为另一示例,暂时性计算机可读介质可以包括网络上的信号,在电线、导体、光纤、电路、在传输期间是转瞬即逝型的或者缺乏任何永久性表象的任何合适的介质、和/或任何合适的无形介质上的信号。

[0063] 因此,提供了用于基于动态IP地址修改防火墙规则的方法、系统和介质。

[0064] 尽管已经在前述说明性实施例中描述和说明了本发明,但是应该理解,本公开仅是通过示例的方式进行的,并且可以在不脱离本发明的精神和范围的情况下对本发明的实

施方式的细节进行许多改变,其仅由所附权利要求书限定。所公开的实施例的特征可以以各种方式组合和重新布置。

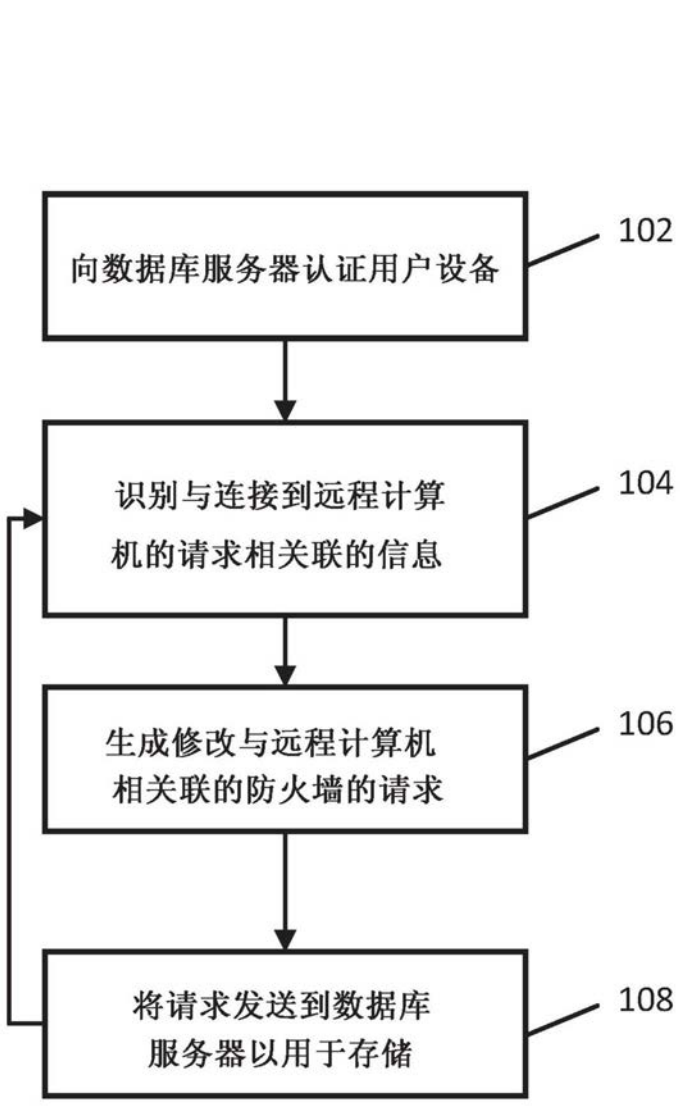

100
向数据库服务器认证用户设备
102
识别与连接到远程计算机的请求相关联的信息
104
生成修改与远程计算机相关联的防火墙的请求
106
将请求发送到数据库服务器以用于存储
108

图1

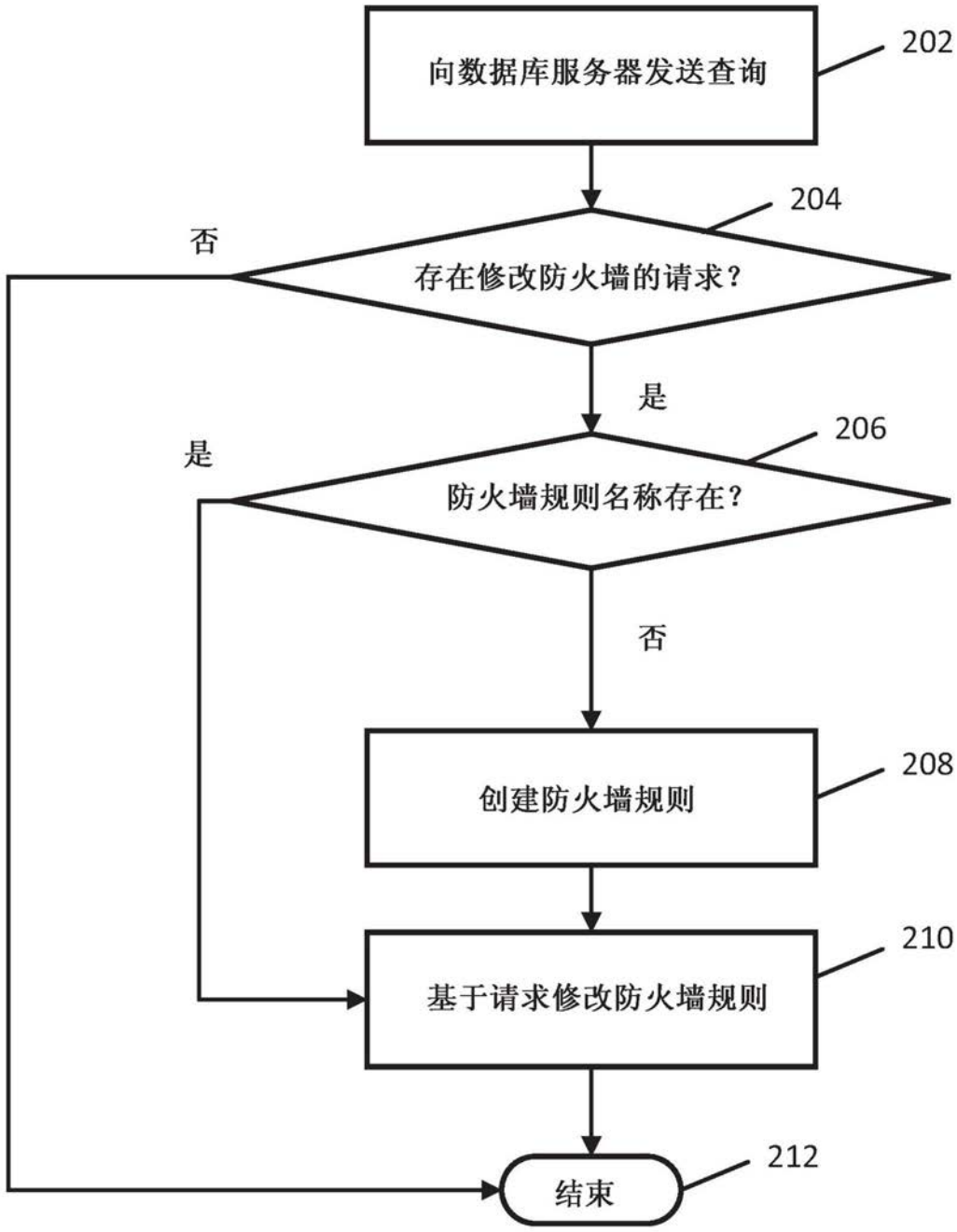

200
向数据库服务器发送查询
202
204
否
存在修改防火墙的请求？
是
206
是
防火墙规则名称存在？
否
创建防火墙规则
208
210
基于请求修改防火墙规则
212
结束

图2

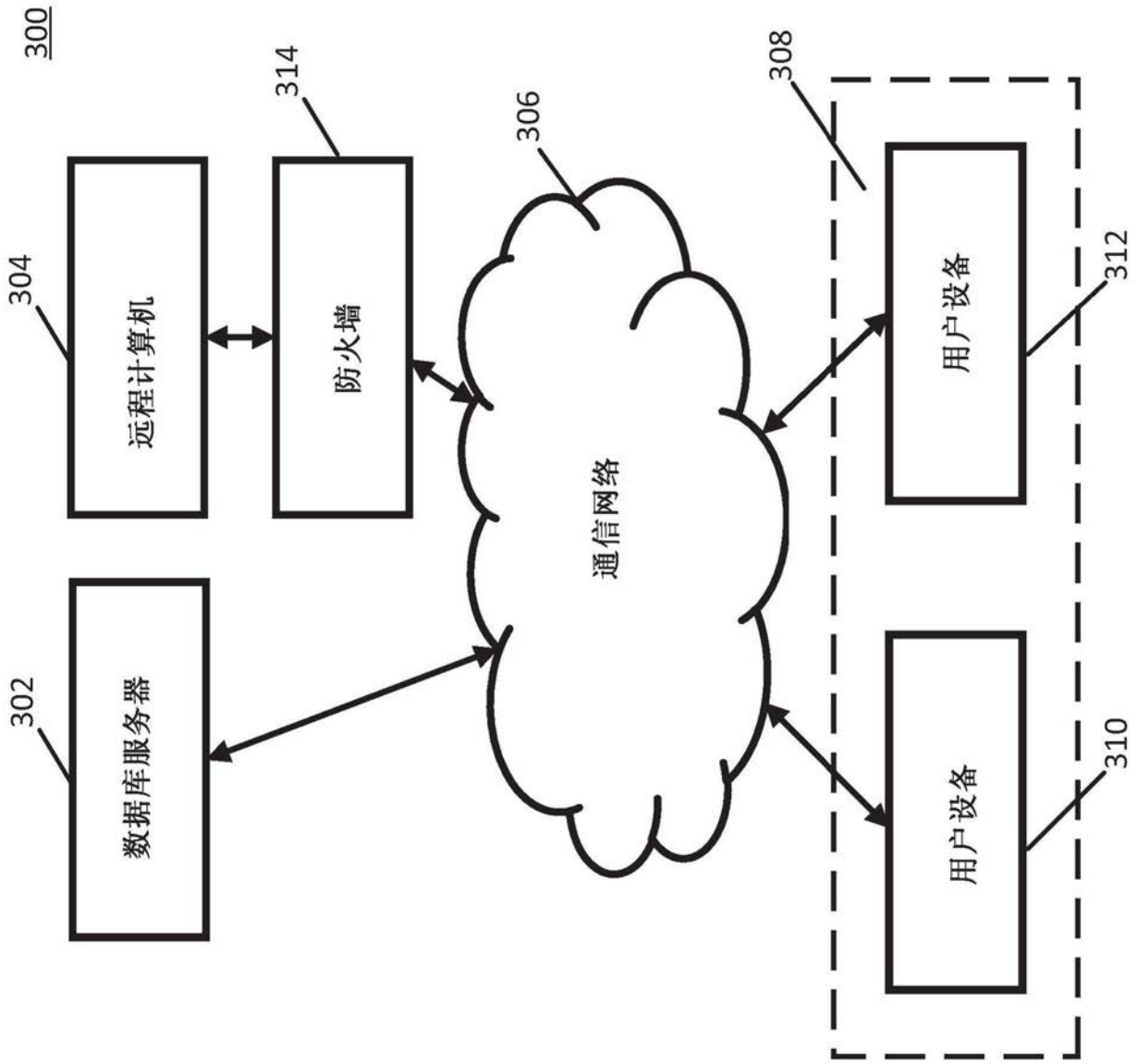

300
314
306
308
304
远程计算机
防火墙
通信网络
用户设备
312
302
数据库服务器
用户设备
310

图3

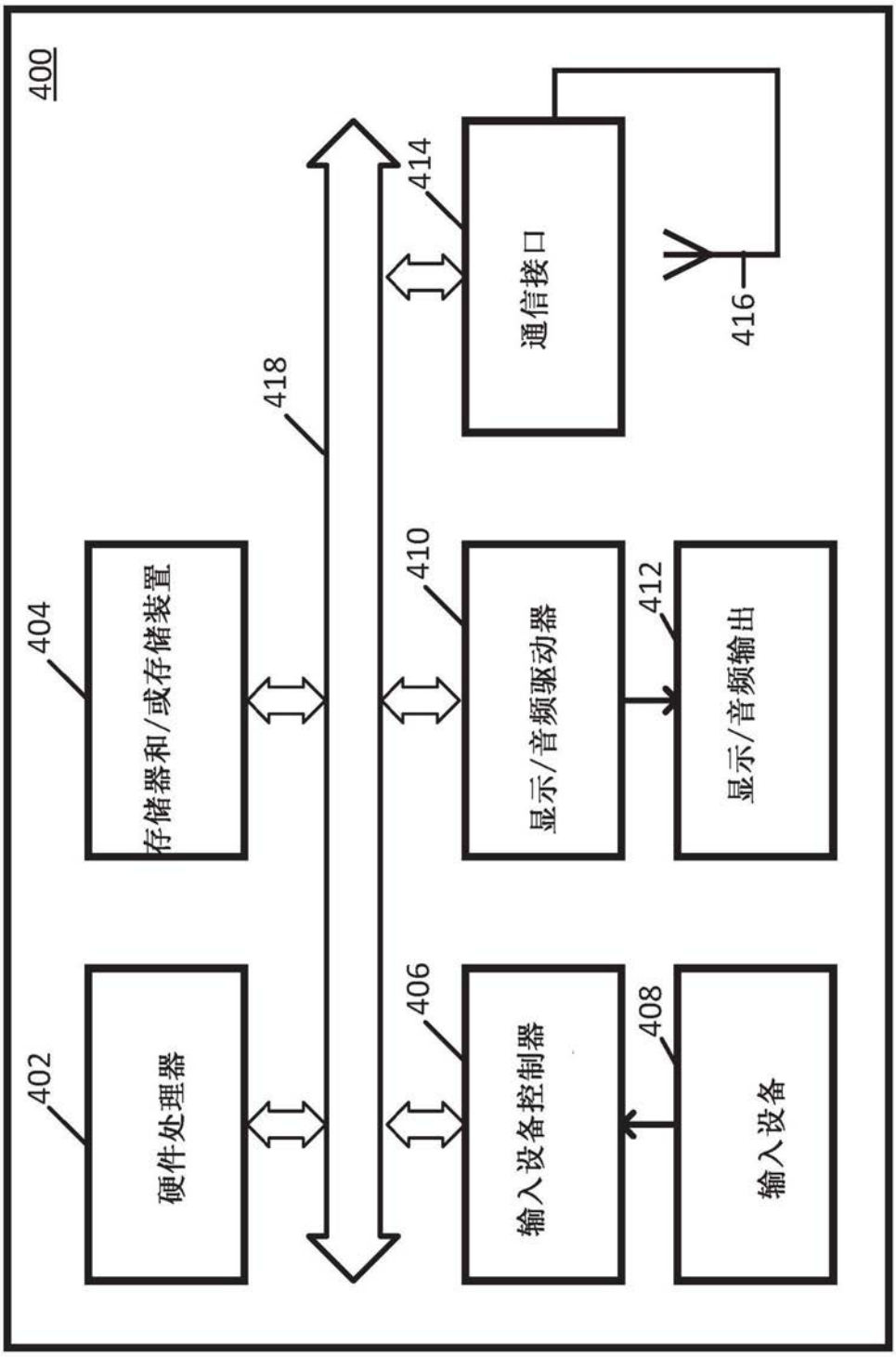

400
402
硬件处理器
404
存储器和/或存储装置
406
输入设备控制器
408
输入设备
410
显示/音频驱动器
412
显示/音频输出
414
通信接口
416
418

图4