(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 112805982 B
(45)授权公告日 2022.04.08

(21)申请号 201980066643.7
(22)申请日 2019.09.10
(65)同一申请的已公布的文献号
申请公布号 CN 112805982 A
(43)申请公布日 2021.05.14
(30)优先权数据
16/128424 2018.09.11 US
(85)PCT国际申请进入国家阶段日
2021.04.09
(86)PCT国际申请的申请数据
PCT/US2019/050386 2019.09.10
(87)PCT国际申请的公布数据
WO2020/055847 EN 2020.03.19
(73)专利权人 思杰系统有限公司
地址 美国佛罗里达州
(72)发明人 A·乔汉
(74)专利代理机构 北京泛华伟业知识产权代理有限公司 11280
代理人 王勇
(51)Int.Cl.
H04L 9/40(2022.01)
H04L 67/141(2022.01)
H04W 12/086(2021.01)
(56)对比文件
CN 105556928 A,2016.05.04
US 2009138937 A1,2009.05.28
CN 107924318 A,2018.04.17
审查员 侯艳兰

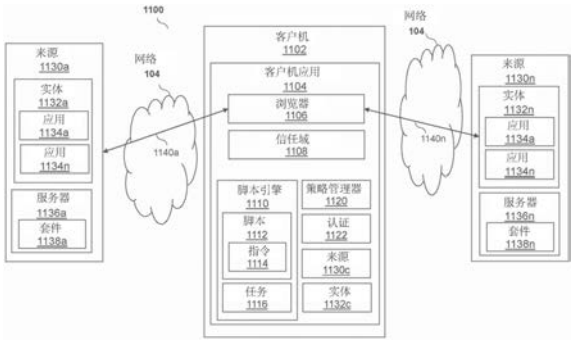
权利要求书3页 说明书38页 附图13页

(54)发明名称

用于跨域应用的应用脚本

(57)摘要

所描述的实施例包括用于在嵌入式浏览器中执行用于不同来源的网络应用的应用脚本的系统和方法。客户机应用可以经由客户机应用内的嵌入式浏览器与第一来源处的第一实体的第一网络应用建立第一会话,并经由客户机应用内的嵌入式浏览器与第二来源处的第二实体的第二网络应用建立第二会话。第三来源处的用户的客户机装置的客户机应用内的脚本引擎可以识别具有与第一网络应用和第二网络应用进行交互的指令的应用脚本,并且可以执行指令以跨第一来源处的第一实体的第一网络应用和第二来源处的第二实体的第二网络应用执行任务。



CN 112805982 B

1.一种用于在嵌入式浏览器中执行用于不同来源的网络应用的应用脚本的方法,所述方法包括:

(a)由客户机应用经由所述客户机应用内的嵌入式浏览器与第一来源处的第一实体的一个或多个第一网络应用建立一个或多个第一会话;

(b)由所述客户机应用经由所述客户机应用内的嵌入式浏览器与第二来源处的第二实体的一个或多个第二网络应用建立一个或多个第二会话;

(c)由第三来源处的用户的客户机装置的客户机应用内的脚本引擎识别应用脚本,所述应用脚本包括各自与所述第一来源处的第一实体的一个或多个第一网络应用以及所述第二来源处的第二实体的一个或多个第二网络应用进行交互的指令;以及

(d)由所述脚本引擎执行所述应用脚本的指令,以使用所述第一来源处的第一实体的一个或多个第一网络应用的第一网络应用执行任务的第一部分以及使用所述第二来源处的第二实体的一个或多个第二网络应用的第二网络应用执行所述任务的第二部分。

2.根据权利要求1所述的方法,其中,所述一个或多个第一网络应用包括源自所述第一来源处的一个或多个第一服务器或由所述第一来源处的一个或多个第一服务器托管的应用的套件。

3.根据权利要求1所述的方法,其中,所述一个或多个第二网络应用包括源自所述第二来源处的一个或多个第二服务器或由所述第二来源处的一个或多个第二服务器托管的应用的套件。

4.根据权利要求1所述的方法,其中,所述第一来源和所述第二来源是使相同来源策略失败的不同来源。

5.根据权利要求1所述的方法,还包括由所述客户机应用在所述第一来源处的所述第一实体的所述一个或多个第一网络应用与所述第二来源处的所述第二实体的所述一个或多个第二网络应用之间建立信任域。

6.根据权利要求5所述的方法,其中,经由与所述第三来源相对应的用户的第三实体的客户机装置上的客户机应用响应于同一用户对所述一个或多个第一网络应用和所述一个或多个第二网络应用的认证来建立所述信任域。

7.根据权利要求1所述的方法,还包括由所述一个或多个第一网络应用或所述一个或多个第二网络应用中的一者启动所述应用脚本的执行。

8.根据权利要求1所述的方法,其中,(d)还包括由所述客户机应用响应于策略来允许所述应用脚本跨所述第一来源和所述第二来源进行交互。

9.根据权利要求8所述的方法,其中,所述策略指定所述第一来源和所述第二来源是经由所述客户机应用的所述嵌入式浏览器进行交互跨越的受信任的来源。

10.一种用于在嵌入式浏览器中跨不同来源的网络应用进行协作的方法,所述方法包括:

(a)由客户机应用经由所述客户机应用内的嵌入式浏览器与第一来源处的第一实体的一个或多个第一网络应用建立一个或多个第一会话;

(b)由所述客户机应用经由所述客户机应用内的嵌入式浏览器与第二来源处的第二实体的一个或多个第二网络应用建立一个或多个第二会话;

(c)由所述客户机应用响应于策略来确定所述第一来源和所述第二来源是被信任以经

由所述嵌入式浏览器进行交互跨越的来源;以及

(d)由所述客户机应用响应于确定所述第一来源和所述第二来源是被信任以经由所述嵌入式浏览器进行交互跨越的来源,来允许所述第一来源处的第一实体的一个或多个第一网络应用的第一网络应用经由所述嵌入式浏览器与所述第二来源处的第二实体的一个或多个第二网络应用的第二网络应用进行交互,以用于所述第一网络应用执行任务的第一部分以及所述第二网络应用执行所述任务的第二部分。

11.根据权利要求10所述的方法,其中,所述第一来源和所述第二来源使相同来源策略失败。

12.根据权利要求10所述的方法,其中,所述策略指定要信任的多个不同来源,所述多个不同来源包括所述第一来源和所述第二来源。

13.根据权利要求10所述的方法,还包括由所述客户机应用的脚本引擎执行脚本,以经由所述嵌入式浏览器在所述第一来源处的第一实体的一个或多个第一网络应用与所述第二来源处的第二实体的一个或多个第二网络应用之间进行交互。

14.根据权利要求10所述的方法,其中,(d)还包括响应于同一用户对所述一个或多个第一网络应用和所述一个或多个第二网络应用中的每一个的认证来允许进行交互。

15.一种用于在嵌入式浏览器中跨不同来源的网络应用进行协作的系统,所述系统包括:

客户机应用,能够在客户机装置的一个或多个处理器上执行并被配置为:

经由所述客户机应用内的嵌入式浏览器与第一来源处的第一实体的一个或多个第一网络应用建立一个或多个第一会话,以及经由所述客户机应用内的嵌入式浏览器与第二来源处的第二实体的一个或多个第二网络应用建立一个或多个第二会话;

响应于策略来确定所述第一来源和所述第二来源是被信任以经由所述嵌入式浏览器进行交互跨越的来源;以及

响应于确定所述第一来源和所述第二来源是被信任以经由所述嵌入式浏览器进行交互跨越的来源,来允许所述第一来源处的第一实体的一个或多个第一网络应用的第一网络应用经由所述嵌入式浏览器与所述第二来源处的第二实体的一个或多个第二网络应用的第二网络应用进行交互,以用于所述第一网络应用执行任务的第一部分以及所述第二网络应用执行所述任务的第二部分。

16.根据权利要求15所述的系统,其中,所述第一来源和所述第二来源是使相同来源策略失败的不同来源。

17.根据权利要求15所述的系统,其中,所述策略指定了要信任的多个不同来源,所述多个不同来源包括所述第一来源和所述第二来源。

18.根据权利要求15所述的系统,还包括脚本引擎,所述脚本引擎被配置为执行脚本的指令,以经由所述嵌入式浏览器来跨所述第一来源处的第一实体的一个或多个第一网络应用和所述第二来源处的第二实体的一个或多个第二网络应用执行任务。

19.根据权利要求15所述的系统,其中,所述一个或多个第一网络应用包括源自所述第一来源处的一个或多个第一服务器或由所述第一来源处的一个或多个第一服务器托管的应用的套件。

20.根据权利要求15所述的系统,其中,所述客户机应用被配置为响应于同一用户对所

述一个或多个第一网络应用和所述一个或多个第二网络应用中的每一个的认证来允许进行交互。

用于跨域应用的应用脚本

[0001] 相关申请的交叉引用

[0002] 本申请要求于2018年9月11日提交的名称为“SYSTEMS AND METHODS FOR APPLICATION SCRIPTS FOR CROSS-DOMAIN APPLICATIONS”的美国专利申请No.16/128,424的优先权和利益,其内容出于所有目的通过引用全部合并于此。

技术领域

[0003] 本申请总地涉及应用的管理,包括但不限于用于使用嵌入式浏览器来管理和监测web和软件即服务(SaaS)应用的系统和方法。

背景技术

[0004] 随着企业的劳动力变得更有移动性和在各种条件下工作,个人可以使用一个或多个客户机装置(包括个人装置)以访问网络资源,例如web应用。由于客户机装置和网络资源可以被访问的方式之间的不同,给企业在管理访问网络资源和监测资源的潜在滥用提出显著的挑战。

发明内容

[0005] 本公开涉及用于在嵌入式浏览器中执行用于不同来源的网络应用的应用脚本的系统和方法。例如,客户机应用可以经由嵌入式浏览器在客户机装置上执行。客户机应用可以经由嵌入式浏览器建立或提供到一个或多个网络应用的一个或多个会话。客户机应用可以在客户机装置与来自一个或多个不同实体和/或不同来源的一个或多个网络应用之间建立信任域。信任域可以为客户机装置的用户提供执行任务(例如但不限于跨来自不同实体和/或不同来源的网络应用传输数据)的平台。例如,客户机应用可以包括或以其他方式提供生成一个或多个应用脚本的脚本引擎。应用脚本可以包括指令,以跨来自不同实体和/或不同来源的网络应用执行一个或多个任务。客户机应用可以使用应用脚本在来自不同实体和/或不同来源的网络应用上实现客户机装置的用户特有的策略,并因此覆盖或替代相应网络应用的策略,例如但不限于相同来源策略,以允许在客户机应用的嵌入式浏览器内进行跨应用协作。

[0006] 与客户机应用的嵌入式浏览器耦合或在其中执行的网络应用可以利用信任域进行跨应用协作。例如,网络应用可以包括源自或由不同来源处的不同服务器托管的应用的套件或由其提供。套件可以包括相同来源安全策略,该策略限制或防止来自不同套件、不同服务器和/或不同来源的网络应用之间的协作或集成。本文所述的系统和方法可以建立信任域,该信任域形成用于在来自不同套件、不同服务器和/或不同来源的网络应用之间进行协作或集成的平台。例如,客户机装置的用户可以使用由客户机应用的脚本引擎生成的应用脚本,跨信任域内的不同网络应用执行一个或多个任务。

[0007] 应用脚本可以跨多供应商网络应用工作,以为客户机装置的用户执行各种任务。例如,可以生成应用脚本,以使得它们满足来自不同套件、不同服务器、不同实体和/或不同

来源的网络应用的相应安全策略。因此，客户机应用可以作为客户机装置的脚本主机操作，以跨来自不同套件、不同服务器、不同实体和/或不同来源的不同应用经由脚本引擎并在信任域内执行脚本。例如，客户机应用的脚本引擎可以编写应用脚本和/或自动化任务，例如但不限于从第一来源处的第一实体的第一网络应用提取数据并将数据传输到第二来源处的第二实体的第二网络应用。

[0008] 在至少一个方面，提供了一种用于在嵌入式浏览器中执行用于不同来源的网络应用的应用脚本的方法。该方法包括由客户机应用经由客户机应用内的嵌入式浏览器与第一来源处的第一实体的第一一个或多个网络应用建立第一一个或多个会话。该方法包括由客户机应用经由客户机应用内的嵌入式浏览器与第二来源处的第二实体的第二一个或多个网络应用建立第二一个或多个会话。该方法包括由第三来源处的用户的客户机装置的客户机应用内的脚本引擎识别应用脚本，应用脚本包括各自与第一来源处的第一实体的第一一个或多个网络应用以及第二来源处的第二实体的第二一个或多个网络应用进行交互的指令。该方法包括由脚本引擎执行应用脚本的指令，以跨第一来源处的第一实体的第一一个或多个网络应用以及第二来源处的第二实体的第二一个或多个网络应用执行任务。

[0009] 第一一个或多个网络应用可以包括源自第一来源处的第一一个或多个服务器或由其托管的应用的套件。第二一个或多个网络应用可以包括源自第二来源处的第二一个或多个服务器或由其托管的应用的套件。第一来源和所述第二来源可以是使相同来源策略失败的不同来源。

[0010] 在一些实施例中，该方法可以包括由客户机应用在第一来源处的第一实体的第一一个或多个网络应用与第二来源处的第二实体的第二一个或多个网络应用之间建立信任域。可以经由与第三来源相对应的用户的第三实体的客户机装置上的客户机应用响应于同一用户对第一一个或多个网络应用和第二一个或多个网络应用的认证来建立信任域。该方法可以包括由第一一个或多个网络应用或第二一个或多个网络应用中的一者启动应用脚本的执行。

[0011] 该方法可以包括由所述客户机应用响应于策略来允许应用脚本跨第一来源和第二来源进行交互。该策略可以指定第一来源和第二来源是经由客户机应用的嵌入式浏览器进行交互跨越的受信任的来源。

[0012] 在至少一个方面，提供了一种用于在嵌入式浏览器中跨不同来源的网络应用进行协作的方法。该方法可以包括由客户机应用经由客户机应用内的嵌入式浏览器与第一来源处的第一实体的第一一个或多个网络应用建立第一一个或多个会话。该方法可以包括由客户机应用经由客户机应用内的嵌入式浏览器与第二来源处的第二实体的第二一个或多个网络应用建立第二一个或多个会话。该方法可以包括由客户机应用响应于策略来确定第一来源和第二来源是被信任以经由嵌入式浏览器进行交互跨越的来源。该方法可以包括由客户机应用响应于所述确定来允许第一来源处的第一实体的第一一个或多个网络应用经由嵌入式浏览器与第二来源处的第二实体的第二一个或多个网络应用进行交互。

[0013] 第一来源和第二来源可以使相同来源策略失败。策略可以指定要信任的多个不同来源，所述多个不同来源包括第一来源和第二来源。该方法可以包括由所述客户机应用的脚本引擎执行脚本，以经由嵌入式浏览器在第一来源处的第一实体的第一一个或多个网络应用与第二来源处的第二实体的第二一个或多个网络应用之间进行交互。在一些实施例

中，该方法可以包括响应于同一用户对第一一个或多个网络应用和第二一个或多个网络应用中的每一个的认证来允许进行交互。

[0014] 在至少一个方面，提供了一种用于在嵌入式浏览器中跨不同来源的网络应用进行协作的系统。该系统可以包括能够在客户机装置的一个或多个处理器上执行的客户机应用。客户机应用可以被配置为经由客户机应用内的嵌入式浏览器与第一来源处的第一实体的第一一个或多个网络应用建立第一一个或多个会话，以及经由客户机应用内的嵌入式浏览器与第二来源处的第二实体的第二一个或多个网络应用建立第二一个或多个会话。客户机应用可以被配置为响应于策略来确定第一来源和第二来源是被信任以经由嵌入式浏览器进行交互跨越的来源。客户机应用可以被配置为响应于所述确定来允许第一来源处的第一实体的第一一个或多个网络应用经由嵌入式浏览器与第二来源处的第二实体的第二一个或多个网络应用进行交互。

[0015] 第一来源和第二来源可以是使相同来源策略失败的不同来源。策略可以指定要信任的多个不同来源，所述多个不同来源包括第一来源和第二来源。

[0016] 在一些实施例中，该系统还可以包括脚本引擎，所述脚本引擎被配置成执行脚本的指令，以经由嵌入式浏览器跨第一来源处的第一实体的第一一个或多个网络应用和第二来源处的第二实体的第二一个或多个网络应用执行任务。第一一个或多个网络应用可以包括源自第一来源处的第一一个或多个服务器或由其托管的应用的套件。客户机应用可以被配置为响应于同一用户对第一一个或多个网络应用和第二一个或多个网络应用中的每一个的认证来允许进行交互。

附图说明

[0017] 通过参考以下结合附图的描述，本解决方案的前述和其他目的、方面、特征和优点将变得更加明显和更好理解，其中：

[0018] 图1是计算装置的实施例的框图；

[0019] 图2是用于访问资源的云服务的说明性实施例的框图；

[0020] 图3是企业移动性管理系统的示例实施例的框图；

[0021] 图4是嵌入式浏览器的系统400的框图；

[0022] 图5是用于使用安全浏览器的系统的示例实施例的框图；

[0023] 图6是用于使用安全浏览器插件的浏览器重定向的实施方式的示例表示；

[0024] 图7是使用安全浏览器的系统的示例实施例的框图；

[0025] 图8是用于使用本地嵌入式浏览器和托管安全浏览器的系统的示例实施例的框图；

[0026] 图9是用于使用本地嵌入式浏览器和托管安全浏览器的示例处理流程；

[0027] 图10是用于管理用户对网页的访问的系统的示例实施例；

[0028] 图11是用于在嵌入式浏览器中跨不同来源的网络应用进行协作的系统的示例实施例的框图；

[0029] 图12是用于在嵌入式浏览器中执行用于不同来源的网络应用的应用脚本的方法的示例实施例的流程图；以及

[0030] 图13是用于在嵌入式浏览器中跨不同来源的网络应用进行协作的方法的示例实

施例的流程图。

[0031] 根据下文结合附图时阐述的详细描述，本解决方案的特征和优点将变得更加明显，在附图中，相似的附图标记始终标识相应的元件。在附图中，相似的附图标记通常表示相同、功能相似和/或结构相似的元件。

具体实施方式

[0032] 为了阅读以下各个实施例的描述，本说明书各部分的以下描述及其各自的内容可能是有帮助的：

[0033] A部分描述了一种计算环境，该计算环境可用于实践本文描述的实施例；

[0034] B部分描述了用于嵌入式浏览器的系统和方法。

[0035] C部分描述了用于在嵌入式浏览器中执行用于不同来源的网络应用的应用脚本的系统和方法。

[0036] A.计算环境

[0037] 在讨论本文B部分中详细的系统和方法的实施例的细节之前，讨论这样的实施例可以被部署的计算环境可能是有帮助的。

[0038] 如图1所示，计算机101可以包括一个或多个处理器103、易失性存储器122(例如，随机存取存储器(RAM))、非易失性存储器128(例如，一个或多个硬盘驱动器(HDD)或其他磁性或光学存储介质、一个或多个固态驱动器(SSD)(例如闪存驱动器或其他固态存储介质)、一个或多个混合磁性和固态驱动器、和/或一个或多个虚拟存储卷(例如云存储)、或这种物理存储卷和虚拟存储卷或其阵列的组合)、用户界面(UI)123、一个或多个通信接口118和通信总线150。用户界面123可包括图形用户界面(GUI)124(例如，触摸屏、显示器等)和一个或多个输入/输出(I/O)装置126(例如，鼠标、键盘、麦克风、一个或多个扬声器、一个或多个照相机、一个或多个生物特征扫描仪、一个或多个环境传感器、一个或多个加速度计等)。非易失性存储器128存储操作系统115、一个或多个应用116和数据117，从而例如由处理器103从易失性存储器122中执行操作系统115和/或应用116的计算机指令。在一些实施例中，易失性存储器122可以包括一种或多种类型的RAM和/或高速缓冲存储器，其可以提供比主存储器更快的响应时间。可以使用GUI 124的输入装置来输入数据，或者可以从I/O装置126接收数据。计算机101的各种元件可以经由一条或多条通信总线(显示为通信总线150)进行通信。

[0039] 图1所示的计算机101仅作为示例示出，因为可以通过任何计算或处理环境，以及利用可以具有能够如本文所述操作的合适的硬件和/或软件的任何类型的机器或机器组，来实现客户机、服务器、中间装置和其他网络装置。处理器103可以由执行一个或多个可执行指令(诸如计算机程序)的一个或多个可编程处理器来实现，用以执行系统的功能。如本文所使用的，术语“处理器”描述了执行功能、操作或操作序列的电路。功能、操作或操作序列可以被硬编码到电路中，或者通过存储在存储器装置中的指令被软编码和被电路执行。“处理器”可以使用数字值和/或使用模拟信号执行功能、操作或操作序列。在一些实施例中，“处理器”可以以一个或多个专用集成电路(ASIC)、微处理器、数字信号处理器(DSP)、图形处理单元(GPU)、微控制器、现场可编程门阵列(FPGA)、可编程逻辑阵列(PLA)、多核处理器、或具有关联存储器的通用计算机来实现。“处理器”可以是模拟、数字或混合信号。在一

些实施例中，“处理器”可以是一个或多个物理处理器或一个或多个“虚拟”(例如，位于远程的或“云”)处理器。包括多个处理器核和/或多个处理器的处理器可以提供用于并行、同时执行多个指令或用于并行、同时执行多于一段数据上的一个指令的功能。

[0040] 通信接口118可以包括一个或多个接口，以使计算机101能够通过各种有线和/或无线或蜂窝连接来访问诸如局域网(LAN)、广域网(WAN)、个人局域网(PAN)或互联网的计算机网络。

[0041] 在所描述的实施例中，计算装置101可以代表客户机计算装置的用户执行应用。例如，计算装置101可以执行虚拟机，该虚拟机提供执行会话，应用在该执行会话(例如托管的桌面会话)内代表用户或客户机计算装置执行。计算装置101还可以执行终端服务会话以提供托管的桌面环境。计算装置101可以提供对包括以下中的一个或多个的计算环境的访问：一个或多个应用、一个或多个桌面应用以及可以在其中执行一个或多个应用的一个或多个桌面会话。

[0042] 网络环境、计算机101以及客户机和服务器计算机的实施和操作的其他细节，可以参见2017年1月3日授予佛罗里达州劳德代尔堡的Citrix Systems，Inc.的美国专利No.9,538,345中的描述，其教导通过引用合并于此。

[0043] B.用于嵌入式浏览器的系统和方法

[0044] 本公开涉及嵌入式浏览器的系统和方法。在客户机装置上执行的客户机应用可以允许用户访问从一个或多个服务器被服务和/或在一个或多个服务器上被托管的应用(app)，诸如web应用和软件即服务(SaaS)应用(以下称有时通常称为网络应用)。嵌入或集成到客户机应用中的浏览器可以向用户呈现经由客户机应用访问或请求的网络应用，并且可以启用用户与网络应用之间的交互性。该浏览器有时被称为嵌入式浏览器，而具有嵌入式浏览器的客户机应用(CEB)有时被称为工作空间应用。客户机应用可以建立到一个或多个服务器的安全连接，以提供应用会话，以便用户使用客户机装置和嵌入式浏览器访问网络应用。嵌入式浏览器可以与客户机应用集成，以确保与网络应用相关的流量通过客户机应用路由和/或在客户机应用中处理，这可以为客户机应用提供流量的实时可见性(例如，当通过客户机应用进行解密时)、以及用户交互和行为。当经由用户界面(由客户机应用和嵌入式浏览器共享)请求网络应用，以及通过嵌入式浏览器在同一用户界面内呈现时，嵌入式浏览器可以为用户提供无缝体验。

[0045] 客户机应用可以终止与网络应用的服务器建立的安全连接(诸如安全套接字层(SSL)虚拟专用网络(VPN)连接)的一端。客户机应用可以从网络应用接收加密的流量，并且可以在进一步处理(例如，由嵌入式浏览器呈现)之前对流量进行解密。客户机应用可以监测接收到的流量(例如，以加密分组的形式)，并且还可以对解密的数据流和/或SSL协议栈的内部具有完全可见性。这种可见性可以允许客户机应用执行或促进基于策略的管理(例如，包括数据丢失防护(DLP)能力)、应用控制(例如，提高性能、服务水平)以及分析的收集和产生。例如，本地CEB可以为信息技术(IT)管理员提供用于通过CEB部署Web和SaaS应用的受控系统，并允许IT管理员经由CEB设置策略或配置，以执行上述任何活动。

[0046] 许多Web和SaaS输送的应用从Web服务器连接到用户的通用浏览器(例如Internet Explorer、Firefox等)。一旦通过认证，便会加密此类网络应用的整个会话。然而，在这种情况下，管理员可能不具有对从用户的数字工作空间进入网络应用的内容、或离开网络应用

并进入用户的数字工作空间的内容的可见性、分析、或控制。此外，在通用浏览器中查看的网络应用的内容可以被复制或下载(例如，由用户或程序)到潜在地任意应用或装置，从而导致可能违反数据安全性。

[0047] 本系统和方法可以确保与网络应用相关联的流量是被引导通过CEB的。通过图示的方式，例如，当用户访问具有启用的安全断言标记语言(SAML)的SaaS web服务时，相应的访问请求可以被转发到一个指定的网关服务，该服务确定、检查或者验证CEB是否被用于提出该访问请求。响应于确定CEB被用于提出访问请求，网关服务可以执行或提供认证和单点登录(SSO)，并且可以允许CEB直接连接到SaaS web服务。加密(例如标准加密)可用于CEB与SaaS web服务之间的应用会话。当来自web服务的内容在CEB中未加密以经由嵌入式浏览器查看时，和/或当输入经由CEB输入时，CEB可以提供用于例如控制和分析的选择性应用相关的信息上的附加服务。例如，分析代理或应用编程接口(API)可以被嵌入在CEB中以提供或执行附加服务。

[0048] CEB(有时被称为工作空间应用或接收器)可以与一个或多个网关服务、中间装置和/或网络服务器(有时统称为云服务或思杰云(Citrix Cloud))进行交互操作，以提供对网络应用的访问。与云服务的实施例的操作相关的环境的特征和元件如下所述。

[0049] 图2示出了用于在访问包括网络应用的资源中使用的云服务的实施例。云服务可以包括企业移动性技术架构200，在一个说明性实施例中，其可以包括访问网关260。例如，该架构可以用于自携装置(BYOD)的环境中。该架构可以使客户机装置202(例如，手机或其它装置)的用户能够从客户机装置202访问企业或个人资源，并且使用客户机装置202以供个人使用。用户可以经由在客户机装置202上执行的客户机应用来访问这种企业资源204或企业服务208。用户可以使用由用户购买的客户机装置202或由企业提供给用户的客户机装置202来访问这种企业资源204或企业服务208。用户可以将客户机装置202仅用于商业用途或用于商业和个人用途。客户机装置可运行iOS操作系统和Android操作系统等。企业可以选择实施策略来管理客户机装置202。可以通过防火墙或网关来植入策略，使得客户机装置可以被识别、保护或安全验证，为客户机装置提供对企业资源的选择性或完全访问权限。这些策略可以是客户机装置管理策略、移动应用管理策略、移动数据管理策略或客户机装置、应用和数据管理策略的一些组合。通过施加客户机装置管理策略管理的客户机装置202可以被称为注册装置。该客户机装置管理策略可经由例如客户机应用施加。

[0050] 在一些实施例中，客户机装置的操作系统可以被分成受管理分区210和未管理分区212。受管理分区210可以被施加策略以保护在受管理分区中运行的应用和存储在其中的数据。在受管理分区上运行的应用可以是安全应用。在其他实施例中，所有应用可以根据与该应用分开接收的一个或多个策略文件的集合来执行，并且该策略文件定义一个或多个安全参数、特征、资源限制和/或由客户机装置管理系统在应用在装置上执行时实施的其他访问控制。通过根据它们各自的策略文件进行操作，可以允许或限制每个应用与一个或多个其他应用和/或资源的通信，从而创建虚拟分区。因此，如本文所使用的，分区可以指存储器的物理分区部分(物理分区)、存储器的逻辑分区部分(逻辑分区)和/或如本文所述由于实施一个或多个策略和/或跨多个app的策略文件而创建的虚拟分区(虚拟分区)。换句话说，通过在受管理app上实施策略，那些app可能会被限制为只能与其他受管理app和受信任的企业资源进行通信，从而创建虚拟分区，未管理app和装置无法访问该虚拟分区。

[0051] 安全应用可以是电子邮件(email)应用、web浏览应用、软件即服务(SaaS)访问应用、Windows应用访问应用等。客户机应用可包括安全应用启动器218。安全应用可以是安全本机应用214、由安全应用启动器218执行的安全远程应用222、由安全应用启动器218执行的虚拟化应用226,等等。安全本机应用214可以由安全应用包装器220包装。当在装置上执行安全本机应用时,安全应用包装器220可以包括在客户机装置202上执行的集成策略。安全应用包装器220可以包括元数据,该元数据将在客户机装置202上运行的安全本机应用214指向安全本机应用214可能需要的以完成安全本机应用214执行要求的任务的托管在企业的资源。由安全应用启动器218执行的安全远程应用222可以在安全应用启动器应用218内执行。由安全应用启动器218执行的虚拟化应用226可以利用客户机装置202上、企业资源204处等的资源。由安全应用启动器218执行的虚拟化应用226在客户机装置202上使用的资源可以包括用户交互资源、处理资源等。用户交互资源可以用于收集和传输键盘输入、鼠标输入、照相机输入、触觉输入、音频输入、视觉输入、手势输入等。处理资源可以用于呈现用户界面,处理从企业资源204接收的数据等。由安全应用启动器218执行的虚拟化应用226在企业资源204处使用的资源可以包括用户界面生成资源、处理资源等。用户界面生成资源可以被用于组装用户界面、修改用户界面、刷新用户界面,等等。处理资源可以用于创建信息、读取信息、更新信息、删除信息等。例如,虚拟化应用可以记录与图形用户界面(GUI)相关联的用户交互,并将它们传达给服务器应用,其中服务器应用可以使用用户交互数据作为在服务器上运行的应用的输入。在该布置中,企业可以选择在服务器侧维护应用以及与应用相关联的数据、文件等。虽然企业可以根据此处通过确保一些应用在客户机装置上的部署(例如,通过客户机应用)的安全的原则来选择“移动化”它们,但也可以为特定应用选择该布置。例如,尽管可以确保一些应用在客户机装置上使用的安全性,但是其他应用可能没有准备好或不适合在客户机装置上部署,因此企业可以选择通过虚拟化技术为移动用户提供对未准备好的应用的访问。作为另一个示例,企业可能具有带有大型和复杂数据集的大型复杂应用(例如,物质资源计划应用),在这种情况下很难或不希望为客户机装置定制应用,因此企业可以选择通过虚拟化技术提供对应用的访问。作为又一个示例,企业可以具有维护高度安全数据(例如,人力资源数据、客户数据、工程数据)的应用,该应用可能被企业认为甚至对于安全的移动环境也太敏感,因此企业可以选择使用虚拟化技术允许移动访问这些应用和数据。企业可以选择在客户机装置上提供完全安全和功能完整的应用。企业可以使用客户机应用(可以包括虚拟化应用)来允许访问被认为更适合在服务器侧操作的应用。在一个实施例中,虚拟化的应用可以在安全存储位置中的一个中在移动电话上存储一些数据、文件等。例如,企业可以选择允许特定信息存储在电话中,而不允许其他信息。

[0052] 结合本文中所描述的虚拟化应用,客户机装置可以具有被设计为呈现GUI并且然后记录用户与GUI的交互的虚拟化应用。该虚拟化应用可以将用户交互传送到服务器侧,以被服务器侧的应用作为用户与该应用的交互使用。作为响应,服务器侧的应用可以将新的GUI发送回客户机装置。例如,新的GUI可以是静态页面、动态页面、动画等,从而提供对远程资源的访问。

[0053] 安全应用可以访问存储在客户机装置的受管理分区210中的安全数据容器228中的数据。安全包装应用214、由安全应用启动器执行的应用222,由安全应用启动器218执行的虚拟化应用226等可以访问在安全数据容器中保护的数据。存储在安全数据容器228中的

数据可以包括文件、数据库等。存储在安全数据容器228中的数据可以包括限于特定的安全应用230，在安全应用232之间共享的数据等。限于安全应用的数据可以包括安全通用数据234和高度安全数据238。安全通用数据可以使用诸如高级加密标准(AES)128位加密之类的强加密形式，而高度安全数据238可以使用诸如AES 256位加密之类的非常强加密形式。当从装置管理器224接收到命令时，可以从装置中删除存储在安全数据容器228中的数据。安全应用可以具有双模式选项240。双模式选项240可以向用户呈现在非安全或非管理模式下操作安全应用的选项。在非安全或非管理模式下，安全应用可以访问存储在客户机装置202的非管理分区212上的非安全数据容器242中的数据。存储在非安全数据容器中的数据可以是个人数据244。存储在非安全数据容器242中的数据还可以由在客户机装置202的未管理分区212上运行的非安全应用248访问。当存储在安全数据容器228中的数据被从客户机装置202删除时，存储在非安全数据容器242中的数据可以保持在客户机装置202中。企业可能希望从客户机装置中删除由企业拥有、许可或控制的所选择的或所有的数据、文件和/或应用(企业数据)，同时留下或以其它方式保留由用户拥有、许可或控制的个人数据、文件和/或应用(个人数据)。该操作可以称为选择性擦除。利用根据本文所述方面布置的企业和个人数据，企业可以执行选择性擦除。

[0054] 客户机装置202可以连接到企业处的企业资源204和企业服务208，连接到公共互联网248等。该客户机装置可以通过虚拟专用网络连接来连接到企业资源204和企业服务208。虚拟专用网络连接(也称为微VPN或应用特定的VPN)可以特定于特定应用(例如，如微VPN 250所示)、特定装置、客户机装置上的特定安全区域(例如，如O/S VPN 252所示)等。例如，电话的安全区域中的每个包装应用都可以通过应用特定的VPN访问企业资源，从而可以基于与该应用相关联的属性(可能结合用户或装置属性信息)来授予对VPN的访问权限。虚拟专用网络连接可以承载Microsoft Exchange流量、Microsoft Active Directory流量、超文本传输协议(HTTP)流量、安全超文本传输协议(HTTPS)流量、应用管理流量等。虚拟专用网络连接可以支持并启用单点登录认证过程254。单点登录过程可以允许用户提供一组认证凭证，然后由认证服务258对其进行验证。然后，认证服务258可以向用户授予对多个企业资源204的访问权限，而无需用户向每个单独的企业资源204提供认证凭证。

[0055] 虚拟专用网络连接可以由访问网关260建立和管理。访问网关260可以包括管理、加速和改善企业资源204到客户机装置202的输送的性能增强特征。访问网关还可以将流量从客户机装置202重新路由到公共互联网248，从而使客户机装置202能够访问在公共互联网248上运行的公共可用和非安全的应用。该客户机装置可以经由传输网络262连接到访问网关。传输网络262可以使用一种或多种传输协议，并且可以是有线网络、无线网络、云网络、局域网、城域网、广域网、公共网络、专用网络等。

[0056] 企业资源204可以包括电子邮件服务器、文件共享服务器、SaaS/Web应用、Web应用服务器、Windows应用服务器等。电子邮件服务器可以包括Exchange服务器、Lotus Notes服务器等。文件共享服务器可以包括ShareFile服务器等。SaaS应用可以包括Salesforce等。Windows应用服务器可以包括为提供旨在在本地Windows操作系统上运行的应用等而构建的任何应用服务器。企业资源204可以是基于本地的资源、基于云的资源等。企业资源204可由客户机装置202直接访问或通过访问网关260访问。客户机装置202可以经由传输网络262访问企业资源204。传输网络262可以是有线网络、无线网络、云网络、局域网、城域网、广域

网、公共网络、专用网络等。

[0057] 云服务可以包括访问网关260和/或企业服务208。企业服务208可以包括认证服务258、威胁检测服务264、装置管理器服务224、文件共享服务268、策略管理器服务270、社交整合服务272、应用控制器服务274等。认证服务258可以包括用户认证服务、装置认证服务、应用认证服务、数据认证服务等。认证服务258可以使用凭证。凭证可以通过企业资源204等存储在客户机装置202上。存储在客户机装置202上的凭证可以被存储在客户机装置上的加密位置，凭证可以被临时存储在客户机装置202上以在认证等时使用。威胁检测服务264可以包括入侵检测服务、未授权访问尝试检测服务等。未授权访问尝试检测服务可以包括访问装置、应用、数据等的未授权的尝试。装置管理服务224可以包括配置、供应、安全、支持、监测、报告和报废服务。文件共享服务268可以包括文件管理服务、文件存储服务、文件协作服务等。策略管理器服务270可以包括装置策略管理器服务、应用策略管理器服务、数据策略管理器服务等。社交整合服务272可以包括联系人整合服务、协作服务、与诸如Facebook、Twitter和LinkedIn等的社交网络的整合。应用控制器服务274可以包括管理服务、供应服务、部署服务、分配服务、撤销服务、包装服务等。

[0058] 企业移动性技术架构200可以包括应用商店278。应用商店278可以包括未包装应用280、预包装应用282等。可以从应用控制器274将应用填充在应用商店278中。客户机装置202可以通过访问网关260、通过公共互联网248等来访问应用商店278。可以提供具有直观且易于使用的用户界面的应用商店。

[0059] 软件开发工具包284可以通过在应用周围提供安全包装为用户提供保护用户选择的应用的能力。然后，可以通过使用应用控制器274将已使用软件开发工具包284包装的应用填充到应用商店278中，使其对客户机装置202可用。

[0060] 企业移动性技术架构200可以包括管理和分析能力。管理和分析能力可以提供与如何使用资源、使用资源的频率等有关的信息。资源可以包括装置、应用、数据等。如何使用资源可以包括哪些装置下载哪些应用、哪些应用访问哪些数据等。使用资源的频率可以包括应用的下载频率、应用访问特定数据集的次数等。

[0061] 图3描绘了企业移动性管理系统300的说明性实施例。为了简单起见，已省略了以上参考图2已描述的移动性管理系统200的一些组件。图3中描绘的系统300的架构在许多方面与上面参考图2描述的系统200的架构相似，并且可以包括上面未提及的附加特征。

[0062] 在这种情况下，左侧代表具有客户机代理304的注册客户机装置302，其与网关服务器306交互以访问各种企业资源308和服务309，例如Web或SaaS应用、Exchange、Sharepoint、公钥基础设施(PKI)资源、Kerberos资源、凭证发行服务，如右上方所示。网关服务器306可以包括云服务的特征和功能的实施例，例如访问网关260和应用控制器功能。尽管未具体示出，客户机代理304可以是客户机应用的一部分和/或与客户机应用交互，该客户机应用可以作为企业应用商店(店面)操作以选择和/或下载网络应用。

[0063] 客户机代理304可以充当托管在企业数据中心中的Windows app/桌面的UI(用户界面)中间装置，其使用高清晰度用户体验(HDX)或独立计算架构(ICA)显示远程协议来访问。客户机代理304还可支持客户机装置302上的本机应用(例如本机iOS或Android应用)的安装和管理。例如，上图中所示的受管理应用310(邮件、浏览器、包装的应用)是在装置上本地执行的本机应用。该架构的客户机代理304和应用管理框架用于向企业资源/服务308提

供策略驱动的管理能力和特征，诸如连接性和SSO(单点登录)。客户机代理304利用至其它网关服务器组件的SSO来处理向企业(例如向访问网关(AG))的主要用户认证。客户机代理304从网关服务器306获得策略以控制客户机装置302上的受管理应用310的行为。

[0064] 本机应用310与客户机代理304之间的安全进程间通信(IPC)链路312代表管理通道，该管理通道允许客户机代理提供由应用管理框架314“包装”每个应用实施的策略。IPC通道312还允许客户机代理304提供使到企业资源308的连接性和SSO成为可能的凭证和认证信息。最终，IPC通道312允许应用管理框架314调用由客户机代理304实现的用户界面功能，例如在线和离线认证。

[0065] 客户机代理304与网关服务器306之间的通信本质上是来自应用管理框架314的管理通道的扩展，该应用管理框架314包装了每个本机受管理的应用310。应用管理框架314从客户机代理304请求策略信息，客户机代理304又从网关服务器306请求策略信息。应用管理框架314请求认证，以及客户机代理304登录到网关服务器306(也被称为NetScaler访问网关)的网关服务部分。客户机代理304还可在网关服务器306上调用支持服务，其可产生输入材料以导出用于本地数据仓库316的加密密钥，或提供客户机凭证，该客户机凭证可使得能够对PKI保护的资源进行直接认证，如下文更充分地解释的。

[0066] 更详细地，应用管理框架314“包装”每个受管理的应用310。这可以经由显式的构建步骤，或经由后构建处理步骤来合并。在首次启动应用310时，应用管理框架314可以与客户机代理304“配对”，以初始化安全IPC通道并获取该应用的策略。应用管理框架314可以实施在本地应用的策略的相关部分，例如客户机代理登录依赖性和一些包含策略，其限制了本地OS服务可以如何被使用，或者它们如何与应用310交互。

[0067] 应用管理框架314可以使用客户机代理304通过安全IPC通道312提供的服务来促进认证和内部网络访问。专用和共享数据仓库316(容器)的密钥管理也可以通过受管理的应用310和客户机代理304之间的适当交互来管理。仓库316仅在在线认证之后才可用，或者，如果策略允许，可在离线认证后使其可用。仓库316的首次使用可能需要在线认证，并且在需要再次在线认证之前，离线访问最多可以限制为策略刷新期。

[0068] 可直接从单个受管理的应用310通过访问网关306网络访问内部资源。应用管理框架314负责代表每个应用310协调网络访问。客户机代理304可以通过提供在在线认证之后获得的合适的时间有限的辅助凭证来促进这些网络连接。可以使用多种模式的网络连接，例如反向web代理连接和端到端VPN样式的隧道318。

[0069] 邮件和浏览器管理的应用310可以具有特殊状态，并且可以利用对于任意包装的应用通常可能不可用的设施。例如，邮件应用可以使用特殊的后台网络访问机制，该机制允许它在延长的时间内访问Exchange，而无需完整的AG登录。浏览器应用可以使用多个专用数据仓库来隔离不同种类的数据。

[0070] 该架构可以支持各种其他安全特征的合并。例如，在某些情况下，网关服务器306(包括其网关服务)可能不需要验证活动目录(AD)密码。企业可以自行决定是否将AD密码用作某些用户在某些情况下的认证因素。如果用户在线或离线(即，已连接或未连接到网络)，则可以使用不同的认证方法。

[0071] 逐步认证是一种特征，其中网关服务器306可以识别使用强认证来被允许访问更多敏感数据的受管理的本机应用310，并确保仅在执行适当的认证之后才允许访问这些应

用,即使这意味着在先前较弱级别的登录之后,要求用户重新认证。

[0072] 该解决方案的另一安全特征是对客户机装置302上的数据仓库316(容器)的加密。仓库316可以被加密,使得包括剪贴板/缓存数据、文件、数据库和配置在内的所有装置上的数据都受到保护。对于在线仓库,密钥可以存储在服务器(网关服务器306)上,对于离线仓库,密钥的本地副本可以通过用户密码或生物特征验证来保护。当数据被本地存储在装置302上的安全容器316中时,优选地,利用最低限度的AES 256加密算法。

[0073] 还可以实现其他安全容器特征。例如,可以包括日志记录特征,其中记录在应用310内部发生的所有安全事件的日志并将其报告给后端。可以支持数据擦除,例如如果应用310检测到篡改,则可以用随机数据覆盖相关联的加密密钥,而不留下在文件系统上用户数据被破坏的提示。屏幕截图保护是另一个特征,应用可能会阻止任何数据存储在屏幕截图中。例如,可以将关键窗口的隐藏属性设置为YES。这可能会使得屏幕上当前显示的任何内容都被隐藏,从而产生空白屏幕截图,通常任何内容都将驻留在该屏幕截图上。

[0074] 诸如通过防止任何数据在应用容器之外本地传输(例如通过将数据复制或发送至外部应用),可以防止本地数据传输。键盘高速缓存特征可操作来禁用敏感文本字段的自动更正功能。SSL凭证验证可能是可操作的,因此应用专门验证服务器SSL凭证,而不是将其存储在密钥链中。可以使用加密密钥生成特征,以便使用用户提供的密码或生物特征数据生成用于在装置上加密数据的密钥(如果需要离线访问)。如果不需要离线访问,可以将它与另一个随机生成的密钥进行异或并存储在服务器侧。密钥导出功能可以操作,使得从用户密码生成的密钥使用KDF(密钥导出功能,尤其是基于密码的密钥导出功能2(PBKDF2)),而不是为其创建密码散列。后者使密钥容易受到暴力破解或字典攻击。

[0075] 此外,可以在加密方法中使用一个或多个初始化向量。初始化向量可以使得同一加密数据的多个副本产生不同的密文输出,从而防止重放和密码分析攻击。这也可以防止攻击者即使使用被盗的加密密钥也无法解密任何数据。此外,可以使用认证然后解密,其中仅在用户已经在应用内进行认证之后才对应用数据进行解密。另一个特征可以涉及在存储器中的敏感数据,仅当需要它时,它可以被保持在存储器中(而不是在磁盘上)。例如,登录凭证可能会在登录后从存储器中擦除,并且Objective-C实例变量中的加密密钥和其他数据不会被存储,因为它们很容易被引用。而是可以为这些手动分配存储器。

[0076] 可以经由CEB实现非活动超时,其中,在策略定义的非活动时间段之后,终止用户会话。

[0077] 可以以其他方式防止来自应用管理框架314的数据泄漏。例如,当将应用310置于后台时,可以在预定的(可配置的)时间段之后清除存储器。当置于后台时,可以对应用的最后显示的屏幕获取截图以加快前台操作进程。屏幕截图可能包含机密数据,因此应被清除。

[0078] 另一安全特征涉及不使用用于访问一个或多个应用的AD(活动目录)322密码而使用OTP(一次性密码)320。在某些情况下,某些用户不知道(或不被允许知道)其AD密码,因此这些用户可以使用OTP 320进行认证,例如通过使用像SecurID这样的硬件OTP系统(OTP也可以由不同的供应商提供,例如Entrust或Gemalto)。在某些情况下,在用户使用用户ID进行认证之后,带有OTP 320的文本将被发送给用户。在某些情况下,只能将其实现为在线使用,提示是单个字段。

[0079] 对于那些经由企业策略允许离线使用的应用310,可以实现离线密码以用于离线

认证。例如,企业可能希望店面以这种方式被访问。在这种情况下,客户机代理304可以要求用户设置定制的离线密码并且不使用AD密码。网关服务器306可以提供策略来控制和执行有关密码的最小长度、字符类型组成和密码年龄的密码标准,例如标准Windows Server密码复杂性要求所描述的,尽管可以修改这些要求。

[0080] 另一个特征涉及针对特定应用310的客户机侧凭证作为辅助凭证的启用(目的是经由应用管理框架微VPN特征访问PKI保护的web资源)。例如,应用可以利用这样的凭证。在这种情况下,可以支持使用ActiveSync协议的基于凭证的认证,其中来自客户机代理304的凭证可以由网关服务器306检索并在密钥链中使用。每个受管理应用可以具有一个关联的客户机凭证,该凭证由网关服务器306中定义的标签标识。

[0081] 网关服务器306可以与企业专用web服务进行交互以支持客户机凭证的发行,以允许相关的受管理应用向内部PKI保护的资源进行认证。

[0082] 客户机代理304和应用管理框架314可以被增强以支持获得和使用客户机凭证以向内部PKI保护的网络资源进行认证。可以支持多于一个凭证,例如以匹配各种级别的安全性和/或分离要求。凭证可由邮件和浏览器管理的应用使用,并最终由任意包装的应用使用(前提是那些应用使用web服务样式的通信模式,其中应用管理框架可以合理地居中调解https请求)。

[0083] iOS上的应用管理客户机凭证支持可能依赖于在每个使用时间段的每个受管理应用中的iOS密钥链中导入公钥加密标准(PKCS)12BLOB(二进制大对象)。应用管理框架客户机凭证支持可以使用具有私有内存密钥存储的HTTPS实施方式。客户机凭证可能永远不会存在于iOS密钥链中,也可能不会持久保留,除非可能存在于受到严格保护的“仅在线”数据值中。

[0084] 也可以通过要求将客户机装置302向企业认证以提供附加的安全性实现相互SSL或TLS,反之亦然。也可以实现用于向网关服务器306进行认证的虚拟智能卡。

[0085] 有限和完全的Kerberos支持都可以是附加特征。完全支持特征涉及使用AD密码或受信任的客户机凭证对活动目录(AD)322进行完全Kerberos登录,并获得Kerberos服务票证以响应HTTP协商认证挑战的能力。有限的支持特征涉及Citrix访问网关企业版(AGEE)中的约束委派,其中AGEE支持调用Kerberos协议转换,以便它可以响应于HTTP协商认证挑战,而获得和使用Kerberos服务票证(经受约束委派)。该机制在反向web代理(也称为公司虚拟专用网络(CVPN))模式中,以及在VPN和微VPN模式中http(但不是https)连接被代理时起作用。

[0086] 另一特征涉及应用容器锁定和擦除,其可以在检测到越狱或获取超级权限时自动进行,并且作为来自管理控制台的推送命令而进行,并且即使在应用310未运行时也可以包括远程擦除功能。

[0087] 可以支持企业应用商店的多站点架构或配置以及应用控制器,其允许用户在发生故障的情况下从多个不同位置之一进行服务。

[0088] 在某些情况下,可以允许受管理应用310经由API(示例OpenSSL)访问凭证和私钥。可以允许企业的受信任的受管理应用310使用应用的客户机凭证和私钥来执行特定的公钥操作。例如,当应用的行为类似于浏览器并且不使用凭证访问时,当应用读取“我是谁”的凭证时,当应用使用凭证来建立安全会话令牌时,以及当应用使用私钥以进行重要数据(例

如,事务日志)的数字签名或临时数据加密时,可以相应地识别和处理各种用例。

[0089] 现在参考图4,描绘了嵌入式浏览器的系统400的框图。在简要概述中,该系统400可以包括具有用于用户的数字工作空间的客户机装置402、客户机应用404、在至少一个网络装置上432上操作的云服务408、以及从一个或多个服务器430服务的和/或托管在一个或多个服务器430上的网络应用406。客户机应用404可以例如包括以下中至少之一:嵌入式浏览器410、网络代理412、云服务代理414、远程会话代理416或安全容器418。云服务408可以例如包括在以下中至少之一:安全浏览器420、访问网关422(或CIS,例如,用于登记和/或认证客户机应用和/或用户)、或分析服务424(或CAS,例如,用于从客户机应用接收信息以进行分析)。网络应用406可以包括批准的应用426和未批准的应用428。

[0090] 在一个或多个实施例中,上述元件或实体中的每一个以硬件、或硬件和软件的组合实现。系统400的每个组件可以使用以上结合图1详细描述的硬件或硬件或软件的组合来实现。例如,这些元件或实体的每一个可以包括任何应用、程序、库、脚本、任务、服务、进程或在客户机装置402、至少一个网络装置432和/或在一个或多个服务器430的硬件上执行的任何类型和形式的可执行指令。在一个或多个实施例中,硬件包括诸如一个或多个处理器的电路。例如,至少一个网络装置432和/或一个或多个服务器430可以包括以上结合至少例如图1描述的计算装置的任何元件。

[0091] 客户机装置402可以包括以上结合至少例如图1描述的计算装置的任何实施例。客户机装置402可以包括任何用户装置,诸如台式计算机、膝上型计算机、平板装置、智能电话、或任何其他移动或个人装置。客户机装置402可以包括用户的数字工作空间,该用户的数字工作空间可以包括文件系统、高速缓存或存储器(例如,包括电子剪贴板)、容器、应用和/或客户机装置402上的其他资源。数字工作空间可以包括或扩展到客户机装置402可访问的一个或多个网络,诸如内联网和互联网,包括可经由一个或多个网络访问的文件系统和/或其他资源。例如,可以通过使用具有嵌入式浏览器410(CEB)的客户机应用404来保护数字工作空间的一部分。数字工作空间的安全部分可以包括例如文件系统、高速缓存或内存(例如,包括电子剪贴板)、应用、容器和/或分配给CEB、和/或由CEB分配给经由CEB访问的网络应用406的其他资源。数字工作空间的安全部分还可以包括由CEB(经由一个或多个策略)指定的用于包括在数字工作空间的安全部分的资源(例如,特定的本地应用可以经由策略被指定允许接收从网络应用获得的数据)。

[0092] 客户机应用404可以包括一个或多个组件,诸如嵌入式浏览器410、网络代理412、云服务代理414(有时称为管理代理)、远程会话代理416(有时称为HDX引擎)和/或安全容器418(有时称为安全高速缓存容器)。例如,一个或多个组件可以作为客户机应用404或CEB的软件构建或发布的一部分进行安装,也可以单独获取或下载并安装/集成到客户机应用404或CEB的现有安装中。例如,客户机装置可以从网络装置432下载或以其他方式接收客户机应用404(或任何组件)。在一些实施例中,客户机装置可以将对客户机应用404的请求发送到网络装置432。例如,客户机装置的用户可以发起客户机应用的请求、下载和/或安装。网络装置432继而可发送客户机应用到客户机装置。在一些实施例中,网络装置432可以将用于客户机应用的设置或安装应用发送到客户机装置。在接收到时,客户机装置可以安装该客户机应用到客户机装置的硬盘上。在一些实施例中,客户机装置可以运行设置应用以打开或解压缩客户机应用的包。在一些实施例中,客户机应用可以是对安装在客户机装置上

的另一个应用(例如,网络代理412)的扩展(例如,附加组件(add-on)、内插式附件(add-in)、小应用或插件(plug-in))。客户机装置可以安装客户机应用以与预安装的应用接口或互操作。在一些实施例中,客户机应用可以是独立应用。客户机装置可以安装客户机应用以作为单独的进程执行。

[0093] 嵌入式浏览器410可以包括web浏览器应用或引擎的元件和功能。嵌入式浏览器410可以本地呈现网络应用作为客户机应用的组件或扩展。例如,嵌入式浏览器410可以在CEB内呈现SaaS/Web应用,这可以向CEB提供应用会话的完全的可视性和控制。嵌入式浏览器可以经由任何方式嵌入或合并到客户机应用中,例如直接集成(例如,编程语言或脚本插入)到客户机应用的可执行代码中,或经由插件安装。例如,嵌入式浏览器可以包括基于Chromium的浏览器引擎或其他类型的浏览器引擎,例如,可以使用Chromium嵌入式框架(CEF)将其嵌入到客户机应用中。嵌入式浏览器可以包括基于HTML5的布局图形用户界面(GUI)。嵌入式浏览器可以为合并了各种编程语言的客户机应用提供HTML渲染和JavaScript支持。例如,嵌入式浏览器的元件可以绑定到合并了C、C++、Delphi、Go、Java、.NET/Mono、Visual Basic 6.0和/或Python的客户机应用。

[0094] 在一些实施例中,嵌入式浏览器包括安装在客户机应用上的插件。例如,插件可以包括一个或多个组件。一个这样的组件可以是ActiveX控件或Java控件,或者是能够加载到客户机应用中并在其中执行的任何其他类型和/或形式的可执行指令。例如,客户机应用可以加载和运行嵌入式浏览器的Active X控件,例如在客户机应用的存储空间或上下文中。在一些实施例中,嵌入式浏览器可以作为扩展安装在客户机应用上,并且用户可以选择启用或禁用插件或扩展。嵌入式浏览器(例如,经由插件或扩展)可以形成或操作为安全浏览器,用于保护、使用和/或访问数字工作空间的安全部分内的资源。

[0095] 嵌入式浏览器可以合并超出标准或典型浏览器中的可用或可能的代码和功能。例如,嵌入式浏览器可以与安全容器418绑定或被分配给安全容器418,以定义用户数字工作空间的安全部分的至少一部分。嵌入式浏览器可以与客户机装置的高速缓存的一部分绑定或被分配给客户机装置的高速缓存的一部分,以形成安全剪贴板(例如,客户机装置本地或可扩展到其他装置),该剪贴板可以是安全容器418的至少一部分。嵌入式浏览器可以与客户机应用集成,以确保与网络应用相关的流量通过客户机应用路由和/或在客户机应用中进行处理,这可以为客户机应用提供流量的实时可见性(例如,当通过客户机应用解密时)。对流量的这种可见性可以允许客户机应用执行或促进基于策略的管理(例如,包括数据丢失防护(DLP)能力)、应用控制、以及分析的收集和产生。

[0096] 在一些实施例中,嵌入式浏览器合并了客户机应用404的一个或多个其他组件,诸如云服务代理414、远程会话代理416和/或安全容器418。例如,用户可以使用嵌入式浏览器的云服务代理414与访问网关422(有时称为CIS)互操作以访问网络应用。例如,云服务代理414可以在嵌入式浏览器内执行,并且可以从嵌入式浏览器接收导航命令并将其发送到托管网络应用。云服务代理可以使用远程呈现协议将由网络应用生成的输出显示到嵌入式浏览器。例如,云服务代理414可以包括HTML5 Web客户机,其允许最终用户访问嵌入式浏览器上的远程桌面和/或应用。

[0097] 客户机应用404和CEB在客户机装置的操作(OSI)栈的应用层上操作。客户机应用404可以包括和/或执行与云服务408互操作的一个或多个代理。客户机应用404可以接收、

获得、检索或以其他方式访问各种策略(例如,企业的定制、指定或内部策略或规则)和/或数据(例如,来自云服务408的访问网关422和/或网络装置、或可以由企业管理的其他服务器)。客户机应用可以访问策略和/或数据以控制和/或管理网络应用(例如,SaaS、web或远程托管的应用)。网络应用的控制和/或管理可以包括网络应用的各个方面的控制和/或管理,例如访问控制、会话输送、可用特征或功能、服务级别、流量管理和监测等等。网络应用可以来自企业的提供者或供应商(例如,salesforce.com、SAP、Microsoft Office 365),来自企业本身或来自另一个实体(例如,Dropbox或Gmail服务)。

[0098] 例如,云服务代理414可以提供与网络应用的使用和/或访问有关的策略驱动的管理能力和特征。例如,云服务代理414可以包括策略引擎,以应用(例如,从云服务接收到的)一个或多个策略来确定对诸如网络应用的资源的访问控制和/或连接性。例如,当在客户机应用和提供SaaS应用的服务器430之间建立会话时,云服务代理414可以应用一个或多个策略来控制会话的流量级别和/或流量类型(或其他方面),例如来管理SaaS应用的服务级别。可以控制或管理的应用流量的其他方面可以包括:应用于流量的加密级别和/或加密类型、对于用户所允许的交互级别、对网络应用的某些功能(例如打印屏幕、保存、编辑或复制功能)的受限访问、对使用或传输从网络应用获得的数据的限制、限制对两个或更多个网络应用的并发访问、限制对某些文件存储库或其他资源的访问等等。

[0099] 云服务代理414可传达或馈送信息至云服务408的分析服务424,例如对CEB可见的有关SaaS交互事件的信息。使用CEB的这种配置可以监测或捕获信息以进行分析,而无需在客户机装置和服务器430之间放置内联装置或代理,也无需使用SaaS API网关“带外”方法。在一些实施例中,云服务代理414不在嵌入式浏览器内执行。在这些实施例中,用户可以类似地使用云服务代理414来与访问网关(或CIS)422互操作以访问网络应用。例如,云服务代理414可以向访问网关(或CIS)422注册和/或认证,并且可以从访问网关(或CIS)422获得网络应用的列表。云服务代理414可以包括和/或作为应用商店(或店面)进行操作,以供用户选择和/或下载网络应用。当登录以访问网络应用时,云服务代理414可以从嵌入式浏览器拦截和传送导航命令到网络应用。云服务代理可以使用远程呈现协议将由网络应用生成的输出显示到嵌入式浏览器。例如,云服务代理414可以包括HTML5 web客户机,其允许最终用户访问嵌入式浏览器上的远程桌面和/或应用。

[0100] 在一些实施例中,云服务代理414为用户和/或客户机装置提供单点登录(SSO)能力以访问多个网络应用。云服务代理414可以例如通过与访问网关422通信,来执行用户认证以访问网络应用以及其他网络资源和服务。例如,云服务代理414可以认证或向访问网关422注册,以访问云服务408和/或网络应用406的其他组件。响应于认证或注册,访问网关422可以为(或代表)用户和/或客户机应用向网络应用执行认证和/或SSO。

[0101] 客户机应用404可以包括网络代理412。网络代理412有时被称为软件定义的广域网(SD-WAN)代理、mVPN代理或微VPN代理。该网络代理412可以建立或促进建立客户机应用和一个或多个资源(例如,服务于网络应用的服务器430)之间的网络连接。网络代理412可以为来自客户机应用的请求的连接执行握手,以访问网络应用,并且可以建立请求的连接(例如,安全或加密的连接)。网络代理412可以例如经由虚拟专用网络(VPN)连接到企业资源(包括服务)。例如,网络代理412可以建立客户机应用和提供网络应用406的服务器430之间的安全套接字层(SSL)VPN。VPN连接,有时也被称为微VPN或应用专用VPN,可能特定于特

定的网络应用、特定的装置、客户机装置上的特定的安全区域等，例如上面结合图3所讨论的。作为某些示例，这样的VPN连接可以承载Microsoft Exchange流量、Microsoft Active Directory流量、超文本传输协议(HTTP)流量、安全超文本传输协议(HTTPS)流量。

[0102] 远程会话代理416(有时被称为HDX引擎)可包括上文结合图2所讨论的客户机代理304的特征，例如，以支持显示远程协议(例如，HDX或ICA)。在一些实施例中，远程会话代理416可以根据诸如远程桌面协议(RDP)、设备链接协议(ALP)、远程帧缓冲器(RFB)协议和ICA协议的任何各种协议建立远程桌面会话和/或远程应用会话。例如，远程会话代理416可以为客户机装置的用户建立远程应用会话以访问企业网络应用。远程会话代理416可以例如在由网络代理412建立的安全连接(例如，VPN)之内或之上建立远程应用会话。

[0103] 客户机应用或CEB可以包括安全容器418或与安全容器418相关联。安全容器可以包括在客户机装置内的可访问和/或由客户机装置可访问的一种或多种类型的资源的逻辑或虚拟描述。例如，安全容器418可以指数字工作空间的整个安全部分，或安全部分的特定方面。在一些实施例中，安全容器418对应于安全高速缓存(例如，电子或虚拟剪贴板)，并且可以动态地合并用户的每个客户机装置的本地高速缓存的一部分，和/或受保护或安全(例如，加密)的用户的基于云的高速缓存。安全容器可以定义文件系统的一部分，和/或描绘分配给CEB和/或经由CEB访问的网络应用的资源。安全容器可以包括例如以上结合图2讨论的安全数据容器228的元件。CEB可以被配置为(例如，经由策略)限制、禁止或禁用识别为在安全容器内的资源和/或数据上的某些动作或活动。安全容器可以被定义以指定安全容器内的资源和/或数据对于误用、滥用和/或泄漏进行监测。

[0104] 在某些实施例中，安全容器与实现各种企业安全特征的安全浏览器(例如，嵌入式浏览器410或安全浏览器420)的使用有关或涉及其使用。被配置为在安全浏览器内运行的网络应用(或由安全浏览器访问的网页)可以有效地继承由安全浏览器实现的安全机制。这些网络应用可以被视为包含在安全容器内。使用这种安全浏览器可以使企业实施内容过滤策略，例如，其中员工被阻止从其客户机装置访问特定网站。例如，可以使用安全浏览器来使客户机装置用户无需VPN即可访问公司内部网络。

[0105] 在一些实施例中，安全容器可以支持用于保护企业资源的各种类型的补救措施。一种这样的补救措施是锁住客户机装置、或客户机装置上存储要保护的数据的安全容器，以使得客户机装置或安全容器只能用例如管理员提供的有效密码来解锁。在一些实施例中，这些和其他类型的补救措施可以基于在客户机装置上检测到的条件而自动调用(例如，经由策略的应用)，或者可以由管理员远程启动。

[0106] 在一些实施例中，安全容器可以包括用于文档的安全文档容器。文档可以包括任何计算机可读文件，其包括文本、音频、视频和/或其他类型的信息或媒体。文档可以包括这些媒体类型中的任何单独一个或组合。如本文所解释的，安全容器可以帮助防止企业信息向客户机装置的不同应用和组件以及向其他装置传播。企业系统(可以部分或全部在云网络内)可以将文档传输到各种装置，这些装置可以被存储在安全容器中。安全容器可以防止客户机装置的未授权的应用和其他组件访问安全容器内的信息。对于允许用户使用自己的客户机装置访问、存储和使用企业数据的企业，在客户机装置上提供安全容器有助于保护企业数据。例如，在客户机装置上提供安全容器可以在每个客户机装置上的一个位置集中企业数据，并且可以促进在需要时，从每个客户机装置对企业数据的选择性的或完全的删

除。

[0107] 安全容器可以包括实现存储文档和/或其他类型的文件的文件系统的应用。文件系统可以包括客户机装置的计算机可读存储器的一部分。文件系统可以在逻辑上与客户机装置的计算机可读存储器的其他部分分离。以这种方式，例如，企业数据可以被存储在安全容器中，并且私有数据可以被存储在客户机装置的计算机可读存储器的单独部分中。该安全容器可以允许CEB、经由CEB访问的网络应用、本地安装的应用和/或客户机装置的其他组件从文件系统中读取、写入和/或删除信息(如果被授权这样做)。从安全容器删除数据可以包括：删除存储在安全容器中的实际数据，删除指向存储在安全容器中的数据的指针，删除用于解密存储在安全容器中的数据的加密密钥，等等。该安全容器可以由例如客户机应用、管理员或客户机装置制造商安装。安全容器可以使得删除存储在文件系统中的部分或全部企业数据，而无需修改存储在安全容器外部的客户机装置上的私有数据。文件系统可以促进从文件系统中选择性或完全地删除数据。例如，企业系统的授权组件可以基于例如编码规则从文件系统中删除数据。在一些实施例中，客户机应用可以响应于从企业系统接收删除命令，从文件系统中删除数据。

[0108] 安全容器可以包括访问管理器，该访问管理器管理客户机装置的应用和其他组件对文件系统的访问。可以基于在文档和/或在文件系统中由客户机应用维护的文档访问策略(例如，编码规则)，管理对文件系统的访问。文档访问策略可以基于以下限制对文件系统的访问：(1)客户机装置的哪个应用或其他组件正在请求访问，(2)正在请求哪些文档，(3)时间或日期，(4)客户机装置的地理位置，(5)请求的应用或其他组件是否提供了正确的证书或凭证，(6)客户机装置的用户是否提供正确的凭证，(7)其他条件，或它们的任何组合。用户的凭证可以包括例如密码、安全性问题(例如，您的高中的吉祥物是什么?)的一个或多个答案、生物特征信息(例如，指纹扫描、眼球扫描)等。因此，通过使用访问管理器，可以将安全容器配置为仅由被授权访问安全容器的应用访问。作为一个示例，访问管理器可以使安装在客户机装置上的企业应用能够访问存储在安全容器中的数据，并防止非企业应用访问存储在安全容器中的数据。

[0109] 对文档访问的时间和地理限制可能是有用的。例如，管理员可以部署文档访问策略，该文档访问策略将文档(存储在安全容器中)的可用性限制到指定的时间窗口和/或客户机装置在其中必须驻留才能访问文档的地理区域(例如，由GPS芯片确定)。此外，文档访问策略可以指示安全容器或客户机应用从安全容器中删除文档，或者在指定的时间段到期时或在客户机装置被带到定义的地理区域之外的情况下，使文档不可用。

[0110] 一些文档可以具有禁止该文档在安全容器内被保存的访问策略。在这样的实施例中，仅当用户例如经由云服务登录或认证时，文档才可用于在客户机装置上查看。

[0111] 访问管理器还可以被配置为在远程装置(例如，企业资源或其他企业服务器)和安全容器之间实施某些连接模式。例如，访问管理器可以要求由安全容器从远程装置接收的文档和/或从安全容器发送到远程装置的文档例如通过安全隧道/连接进行传输。访问管理器可以要求对发送到安全容器和从安全容器发送的所有文档进行加密。该客户机应用或访问管理器可以被配置为加密从安全容器发送的文档以及解密发送到安全容器的文档。安全容器中的文档也可以加密形式存储。

[0112] 安全容器可以被配置为防止客户机装置或其他装置的未授权应用或组件使用文

档或文档包括的数据或安全容器。例如，可以对有权从安全容器访问文档的客户机装置应用进行编程，以防止用户复制文档数据并将其粘贴到另一个文件或应用界面中，或者在本地在安全容器之外将文档或文档数据保存为新文件。类似地，安全容器可以包括文档查看器和/或编辑器，其不允许这样的复制/粘贴和本地保存操作。此外，可以将访问管理器配置为防止这种复制/粘贴和本地保存操作。此外，安全容器和被编程并授权从安全容器访问文档的应用可以被配置为防止用户将这种文档附加到电子邮件或其他形式的通信中。

[0113] 一个或多个应用(例如，安装在客户机装置上的应用，和/或经由CEB访问的网络应用)可以被编程或控制(例如，经由基于策略的实施)以将企业相关的数据仅写入安全容器中。例如，可以为应用的源代码提供安全容器的资源名称。类似地，远程应用(例如，在除客户机装置以外的装置上执行)可以被配置为将数据或文档仅发送到安全容器(而不是客户机装置的其他组件或存储器位置)。将数据存储到安全容器可以自动地进行，例如，在应用、客户机应用、和/或安全浏览器的控制下。可以对客户机应用进行编程，以对存储在安全容器中或将要存储在安全容器中的文档进行加密或解密。在某些实施例中，安全容器只能由这种应用(在客户机装置或远程装置上)使用：被编程为识别和使用安全容器的应用，并且该应用具有授权这样做。

[0114] 网络应用406可以包括批准的网络应用426和未批准的网络应用428。通过非限制性示例的方式，批准的网络应用426可以包括来自Workday、Salesforce、Office 365、SAP等的网络应用，而未批准的网络应用426可以包括来自Dropbox、Gmail等的网络应用。例如，图4示出了经由CEB访问批准的应用426的情况。在操作(1)中，安装在客户机装置402上的客户机应用404的用户实例可以向云服务408的访问网关422注册或认证。例如，用户可以向客户机装置402认证该用户，并登录到客户机装置402。客户机应用可以自动执行或由用户激活。在一些实施例中，用户可以在客户机应用签到(例如，通过向客户机应用认证用户)。响应于登录或签到，客户机应用可以向访问网关422注册或认证用户和/或客户机应用。

[0115] 在操作(2)中，响应于注册或认证，访问网关422可以识别或检索可用的或预分配给用户的列举的网络应用的列表，并且可以将该列表提供给客户机应用。例如，响应于注册或认证，访问网关可以识别用户和/或检索用户的用户简档。根据身份和/或用户简档，访问网关可以确定列表(例如，检索与用户简档和/或用户身份匹配的网络应用的存储的列表)。该列表可以对应于为用户批准的网络应用的列表。访问网关可以将列表发送到客户机应用或嵌入式浏览器，该列表可以经由客户机应用或嵌入式浏览器呈现给用户(例如，在店面用户界面中)以供选择。

[0116] 在操作(3)中，用户可以通过从呈现给用户的网络应用列表中进行选择，来启动与批准的网络应用(例如SaaS应用)的连接。例如，用户可以点击经由客户机应用或者嵌入式浏览器显示的批准的网络应用的图标或其他表示。该用户动作可以触发CEB向配置网络应用的服务器发送连接或访问请求。该请求可以包括对服务器(例如，SaaS提供者)的请求，以与访问网关进行通信以认证用户。例如，服务器可以向访问网关发送请求以认证用户。

[0117] 在操作(4)中，访问网关可以与服务器执行SSO，以认证用户。例如，响应于服务器对用户进行认证的请求，访问网关可以向用于SSO的服务器430提供用户的凭证，以访问所选择的网络应用和/或其他批准的网络应用。在操作(5)中，用户可以基于SSO(例如，使用凭证)登录到所选择的网络应用。客户机应用(例如，网络代理412和/或远程会话代理416)可

以与服务器430建立安全连接和会话以访问所选择的网络应用。CEB可以解密经由安全连接接收到的应用流量。CEB可以监测经由CEB和到服务器430的安全连接发送的流量。

[0118] 在操作(6)中，客户机应用可以将信息提供给云服务408的分析服务424，以进行分析处理。例如，客户机应用404的云服务代理414可以监测或捕获与所选择的网络应用的用户交互事件。云服务代理414可以将用户交互事件传达到分析服务424，以进行处理以产生分析。

[0119] 图5描绘了用于使用安全浏览器的系统的示例实施例。在简要概述中，该系统包括云服务408、网络应用406和客户机装置402。在一些实施例中，系统的各种元件类似于以上针对图4所描述的元件，但是客户机应用(具有嵌入式浏览器)在客户机装置402中不可用。标准或典型的浏览器在客户机装置上可能是可用的，例如，用户可以从该浏览器发起访问批准的网络应用的请求。可以经由可由管理员设置或自动设置的策略(例如，经由人工智能)将网络应用指定为批准的或未批准的。

[0120] 例如，在操作(1)中，用户可以使用标准浏览器登录到网络应用。为了访问批准的网络应用，用户可以经由标准浏览器访问预定义URL和/或配置网络应用的服务器的相应网页，以发起访问网络应用的请求。在一些实施例中，请求可以被转发到指定的网关服务或被指定的网关服务拦截(例如，在该请求的数据路径中)。例如，网关服务可以驻留在客户机装置上(例如，作为可执行程序)，或者可以驻留在例如云服务408的网络装置432上。在一些实施例中，访问网关可以对应于或包括网关服务。网关服务可以确定所请求的网络应用是否为批准的网络应用。网关服务可以确定CEB是否发起了请求。该网关服务可以检测或以其他方式确定该请求是从在客户机装置中的非CEB的源发起的(例如，通过标准的浏览器发起的)。在一些实施例中，不需要指定的网关服务来检测或确定该请求是否从CEB发起，例如如果所请求的网络应用是批准的，该用户正在通过标准浏览器发起该请求，和/或被访问的是预定义的URL和/或相应网页。

[0121] 在操作(2)中，服务器可以经由云服务408的访问网关对用户进行认证。服务器可以响应于请求，与访问网关进行通信以对用户进行认证。例如，该请求可以包括服务器与访问网关进行通信以认证用户的指示。在一些实施例中，服务器被预配置为与访问网关通信以认证用户，用于访问批准的网络应用的请求。服务器可以向访问网关发送请求以认证用户。响应于服务器认证用户的请求，访问网关可以将用户的凭证提供给服务器430。

[0122] 在操作(3)中，网关服务和/或服务器可以定向(或重定向)所有流量到安全浏览器420，其提供安全浏览服务。这可以响应于以下中至少之一：确定所请求的网络应用是批准的网络应用，确定从非CEB的源发起该请求，确定所请求的网络应用是批准的，确定用户正在经由标准浏览器发起请求，和/或确定访问预定义的URL和/或相应的网页。

[0123] 可以将用户的URL会话重定向到安全浏览器。例如，服务器、网关服务和/或访问网关可以响应于该确定，生成和/或发送URL重定向消息至标准浏览器。标准浏览器的安全浏览器插件可以接收URL重定向消息，并且可以例如向安全浏览器420发送访问未批准的网络应用的请求。安全浏览器420可以将请求定向到未批准的网络应用的服务器。URL重定向消息可以指示标准浏览器(和/或安全浏览器插件)将来自标准浏览器的流量(例如，发往网络应用)定向至托管在网络装置上的安全浏览器420。这可以经由动态路由通过安全浏览器服务提供无客户机访问和控制。在一些实施例中，在与服务器(例如，使用SSO)执行用户的认

证之前,所有流量至安全浏览器420的重定向被启动或被配置。

[0124] 在一些实施例中,网关服务可以定向或请求所请求的网络应用的服务器与安全浏览器420通信。例如,网关服务可以定向服务器和/或安全浏览器在服务器和安全浏览器之间建立安全连接,以建立用于网络应用的应用会话。

[0125] 在一些实施例中,安全浏览器420包括托管在云服务408的网络装置432上的浏览器。安全浏览器420可以包括以上至少结合例如图4描述的安全浏览器420的一个或多个特征。所托管的浏览器可以包括CEB的嵌入式浏览器,其在网络装置432上托管,而不是在客户机装置上。所托管的浏览器可以包括托管在网络装置432上的CEB的托管虚拟化版本的嵌入式浏览器。与安装在客户机装置上的CEB类似,流量通过网络装置上托管的CEB路由,这允许管理员具有对通过CEB的流量的可视性,并保留对安全策略控制、分析和/或性能管理的控制。

[0126] 图6示出了用于使用安全浏览器插件的浏览器重定向的示例实现。在简要概述中,该实施方式包括具有在客户机装置上操作的安全浏览器插件516的web浏览器512、以及驻留在网络装置上的托管的web浏览器(或安全浏览器)522。web浏览器512可以对应于标准浏览器,而不是如上面结合例如图4所讨论的嵌入式浏览器。安全浏览器插件516可在第一网络510内执行并访问在第二网络530中的服务器430。第一网络510和第二网络530是出于说明的目的,并且可以用更少或更多的计算机网络代替。安全浏览器插件516可以安装在标准浏览器512上。插件可以包括一个或多个组件。一个这样的组件可以包括ActiveX控件或Java控件或能够加载到标准浏览器中并在其中执行的任何其他类型和/或形式的可执行指令。例如,标准浏览器可以在标准浏览器的存储空间或上下文中,加载并运行安全浏览器插件516的Active X控件。在一些实施例中,安全浏览器插件可以作为扩展安装在标准浏览器上,并且用户可以选择启用或禁用该插件或扩展。安全浏览器插件可以进行与安全浏览器420通信和/或操作,以保护、使用和/或访问数字工作空间的安全部分内的资源。

[0127] 通过使用在标准浏览器512内操作的安全浏览器插件516,经由标准浏览器512访问的网络应用可以被重定向到托管的安全浏览器。例如,安全浏览器插件516可以被实现和/或设计为检测网络应用正在经由标准浏览器访问,并且可以定向/重定向与网络应用相关联的来自客户机装置的流量至托管的安全浏览器。托管的安全浏览器可以将从网络应用接收的流量定向到安全浏览器插件516和/或客户机代理514,以例如进行呈现和/或显示。客户机代理514可以在web浏览器512和/或安全浏览器插件内执行,并且可以包括以上结合至少例如图4讨论的客户机应用404的特定元件或特征。例如,客户机代理514可以包括用于在web浏览器512处呈现网络应用的远程会话代理416。在一些实施例中,在托管的安全浏览器处呈现网络应用,并且所呈现的数据被传送或镜像到安全浏览器插件516和/或客户机代理514以进行处理和/或显示。

[0128] 通过示例的方式,用户可能正在远程工作并且可能想要访问网络应用,该网络应用是在安全的企业网络的内部,而用户正在连接到不安全网络的计算装置上工作。在这种情况下,用户可以利用在第一网络510中执行的标准浏览器512,其中第一网络510可以包括不安全的网络。用户想要访问的服务器430可能在第二网络530上,其中第二网络530包含例如安全的企业网络。用户可能无法通过点击安全网站532的内部统一记录定位符(URL)从不安全的第一网络510访问服务器430。即,用户在从外部不安全网络510执行标准浏览器512

时,可能需要利用不同的URL(例如,外部URL)。外部URL可以被定向到,或者可以寻址被配置成在第二网络530(例如,安全网络)内访问服务器430的一个或多个托管的web浏览器522。为了保持安全访问,安全浏览器插件516可以将内部URL重定向到托管的安全浏览器的外部URL。

[0129] 安全浏览器插件516能够实现网络检测,以便识别是否将内部URL重定向到外部URL。标准浏览器512可以接收包括在安全网络内执行的网站的内部URL的请求。例如,标准浏览器512可以接收响应于用户在标准浏览器中输入web网址(例如,用于安全网站532)的请求。安全浏览器插件516可以将用户web浏览器应用512从内部的URL重定向到托管的web浏览器应用的外部的URL。例如,安全浏览器插件516可以用在安全网络530内执行的托管的web浏览器应用522的外部URL替换内部URL。

[0130] 安全浏览器插件516可以允许将客户机代理514连接到托管的web浏览器应用522。客户机代理514可以包括插件组件,例如ActiveX控件或Java控件或能够加载到标准浏览器512中并在其中执行的任何其他类型和/或形式的可执行指令。例如,客户机代理514可以包括由标准浏览器512加载和运行的ActiveX控件,诸如在用户web浏览器应用512的存储空间或上下文中。客户机代理514可以被预配置为在用户web浏览器应用512内呈现托管的web浏览器应用522的内容。

[0131] 客户机代理514可以连接到服务器或云/托管的web浏览器服务520,其使用瘦客户机或远程显示协议来呈现由在服务520上执行的托管的web浏览器应用522生成的显示输出。瘦客户机或远程显示协议可以是以下协议的非穷举列表中的任何一个:由佛罗里达州劳德代尔的思杰系统公司开发的独立计算架构(ICA)协议;或由华盛顿州雷德蒙德的微软公司制造的远程桌面协议(RDP)。

[0132] 托管的web浏览器应用522可以在全屏模式中导航到所请求的网络应用,并且可以呈现所请求的网络应用。客户机代理514可以例如基于正在以全屏模式显示的内容以无缝和透明的方式呈现web浏览器应用512上的网络应用的内容或重现,使得看起来该内容正被标准浏览器512显示。换句话说,可以给用户的印象是网站内容是由用户web浏览器应用512而不是由托管的web浏览器应用522显示的。客户机代理514可以使用瘦客户机或远程显示协议,将由用户web浏览器应用512生成的导航命令发送到托管的web浏览器应用522。由于导航命令对托管的web浏览器应用522的显示输出的改变,可以由客户机代理514反映在用户web浏览器应用512中,从而给用户印象:导航命令是由用户web浏览器应用512执行的。

[0133] 再次参考图5,在操作(4)中,可以在标准浏览器上打开新的浏览器选项卡,以呈现或显示安全浏览器会话。例如,可以通过安全浏览器插件建立或打开新的浏览器选项卡。安全浏览器插件和/或客户机代理可以从安全浏览器会话接收数据,并且可以如以上结合例如图6所讨论的那样在新的浏览器选项卡内呈现网络应用。

[0134] 在操作(5)中,安全浏览器可以将经由网络应用的所有用户交互事件馈送回分析服务以进行处理。安全的浏览器插件可以在浏览器选项卡内监测并拦截定向到网络应用的重现的任何用户交互事件。因此,用户可以使用本机(或标准)的浏览器访问网络应用,同时经由云服务和安全浏览器的互操作(在没有客户机应用的情况下),允许对网络应用的流量的可见性。

[0135] 图7描绘了使用安全浏览器的系统的另一个示例性实施例。在简要概述中,该系统

包括云服务408、网络应用406和客户机装置402。在一些实施例中，系统的各种元件与以上针对图5描述的元件相似。在客户机装置402中，具有嵌入式浏览器的客户机应用不可用。在客户机装置上，标准的或典型的(例如，HTML5)浏览器是可用的，用户可以从其发起访问未批准的网络应用的请求。可以经由可由管理员设置或自动设置的策略(例如，经由人工智能)将网络应用指定为批准的或未批准的。

[0136] 在操作(1)中，用户可以尝试使用标准浏览器登录到未批准的网络应用。用户可以尝试访问配置该网络应用的服务器的网页，并发起访问该网络应用的请求。在一些实施例中，请求可以被转发到指定的网关服务或被指定的网关服务拦截(例如，在请求的数据路径中)。例如，网关服务(有时称为SWG)可以驻留在客户机装置上(例如，作为可执行程序)，或者可以驻留在例如云服务408的网络装置432上。网关服务可以检测或以其他方式确定所请求的网络应用是否为批准的网络应用。网关服务可以确定CEB是否发起了请求。网关服务可以检测或以其他方式确定该请求是从客户机装置中除CEB之外的源发起的(例如，由标准浏览器发起的)。

[0137] 在操作(2)中，网关服务检测到所请求的网络应用是未批准的网络应用。网关服务可以例如从请求中提取信息(例如，目的地址、所请求的网络应用的名称)，并将该信息与来自批准和/或未批准的网络应用的数据库的信息进行比较。网关服务可以基于比较确定所请求的网络应用是未批准的网络应用。

[0138] 在操作(3)中，响应于该确定，网关服务可以阻止对所请求的网络应用的访问，例如通过阻止请求。响应于该确定，网关服务可以生成和/或发送URL重定向消息至标准浏览器。URL重定向消息可以类似于图5中操作(3)中从服务器发送到标准浏览器的URL重定向消息。标准浏览器的安全浏览器插件可接收URL重定向消息，并且可以例如向安全浏览器420发送访问未批准的网络应用的请求。安全浏览器420可以将请求定向到未批准的网络应用的服务器。

[0139] 未批准的网络应用的服务器可以例如响应于从安全浏览器接收到请求，经由云服务408的访问网关来认证用户。响应于该请求，服务器可以与访问网关通信以认证用户。服务器可以向访问网关发送认证用户的请求。响应于服务器对用户进行认证的请求，访问网关可以向服务器430提供用户的凭证。在认证时，安全浏览器(或相应的CEB)可以与服务器建立安全连接和应用会话。

[0140] 在操作(4)中，可以在标准浏览器上打开新的浏览器选项卡，以呈现或显示安全浏览器的应用会话。例如，可以由安全浏览器插件建立或打开新的浏览器选项卡。安全浏览器插件和/或客户机代理可以从安全浏览器会话接收数据，并且可以在新的浏览器选项卡内呈现网络应用，如以上结合例如图5-6所讨论的。

[0141] 在操作(5)中，安全浏览器可以经由网络应用将所有用户交互事件馈送回分析服务以进行处理。安全浏览器插件可以在浏览器选项卡内监测并拦截任何涉及网络应用重现的用户交互事件。因此，用户可以使用本机(或标准)浏览器访问网络应用，同时允许经由云服务和安全浏览器(在没有客户机应用的情况下)的互操作的对于网络应用的流量的可见性。

[0142] 在某些实施例中，在CEB在客户机装置上不存在或不可用的情况下，执行浏览器重定向，使得经由用于处理的相应的托管安全浏览器(或托管CEB)访问每个请求的网络应用，

而不是将所有流量重定向通过单个托管的安全浏览器(或托管的CEB)。每个专用的安全浏览器都可以提供分区功能并提高安全性。

[0143] CEB的使用,无论是托管的还是客户机装置本地的,都可以允许应用流量的端到端可见性以进行分析、服务水平协议(SLA)、资源利用、审计等。除了这种可见性,CEB可以配置有用于管理和控制任何这些方面以及其他方面的策略。例如,可以支持DLP特征以控制"复制和粘贴"活动、文件下载、文件共享以及例如实施水印。作为另一个示例,CEB可以配置有用于管理和控制对本地驱动器和/或装置资源(例如外围装置)的访问的策略。

[0144] 现在参考图8,描绘了用于使用本地嵌入式浏览器和托管安全浏览器的系统的示例实施例。示出了环境,其中可以使用不同类型的客户机装置402A、402B(例如,在BYOD环境中),使得一个客户机装置可以在本地配备有合适的CEB,而另一客户机装置可能没有安装合适的本地CEB。在这样的环境中,可以使用图4、5和7中描述的系统,以基于本地安装的合适CEB的可用性支持客户机装置中的每一个。

[0145] 图9描绘了用于使用本地嵌入式浏览器和托管安全浏览器的示例处理流程。该处理流程可以在以上图8中描述的环境中使用,以确定对于每个客户机装置访问网络应用应使用嵌入式浏览器还是托管的安全浏览器。例如,在操作901中,HTTP客户机可以尝试访问web服务(例如,网络应用的服务器)。在操作903中,web服务可以将HTTP客户机重定向到网关服务以进行认证。在操作905中,网关服务可以确定HTTP客户机是否为CEB。如果是这样,则在操作909中,网关服务可以确定CEB是否是合适的CEB,例如能够执行所定义的应用策略。如果是这样,则在操作911中,允许CEB访问web服务,并且可以执行所定义的策略。

[0146] 如果网关服务确定该HTTP客户机不是CEB,则在操作907中,网关服务可使CEB的虚拟化版本被初始化并被托管在远程服务器(例如,云服务408的网络装置432)上。在一些实施例中,这样的托管CEB在网络装置432上可能已经可用,并且可以被选择使用。例如,在操作911中,CEB被允许访问web服务,并且可以执行所定义的策略。

[0147] 如果网关服务确定HTTP客户机是CEB,但是该CEB不是合适的CEB,则在操作907中,网关服务可以使CEB的虚拟化版本被初始化并被托管在远程服务器(例如,云服务408的网络装置432)上。在一些实施例中,这样的托管CEB可能已经在网络装置432上可用,并且可以被选择使用。例如,在操作911中,CEB被允许访问web服务,并且可以执行所定义的策略。

[0148] 在一些实施例中,如果用户正在请求访问位于公司数据中心中的web应用,则网关服务(在云服务中或在内部)可以在检测到具有CEB的客户机应用时允许访问。否则,可以将请求路由到具有CEB的托管虚拟化版本的服务,然后对访问进行认证和授权。

[0149] 例如,在操作905和/或操作909中,关于HTTP客户机是否是CEB以及它是否是合适的CEB的决定可以由许多因素来确定。例如,为了确定HTTP客户机是否是CEB,该网关服务可以考虑例如包括以下中至少之一的因素:用户身份和认证的强度、客户机位置、客户机IP地址、用户身份被信任程度、客户机位置、客户机IP、客户机装置的越狱状态、反恶意软件状态、对客户机装置的企业策略的遵从、和/或客户机软件的完整性的远程证明或其他证据。

[0150] 为了确定CEB能够兑现或支持所有定义的应用策略(这可以由于客户机版本、客户机OS平台和其他因素而变化),客户机装置的软件和网关服务可以执行能力协商和/或交换版本信息。在一些实施例中,网关服务可以查询或检查CEB的版本号或标识符,以确定CEB是否是要使用的合适的CEB。

[0151] 驱动所有流量通过CEB,然后允许对访问基于SaaS和Web的系统的内容进行附加控制。SaaS和Web流量的数据丢失防护(DLP)可以通过CEB app来应用,其特征包括将对其他CEB访问应用或IT管理的装置的复制和粘贴控制。通过使内容只能在IT控制下下载到指定的文件服务器或服务,也可以执行DLP。

[0152] 现在参考图10,描绘了用于管理用户对网页的访问的系统的示例实施例。某些网页(或网站)被认为是安全的,而另一些网页则可能是可疑的。用户可以通过标准浏览器经由相应的URL访问网页。例如,用户可以点击与URL相对应的链接,该链接可以包括在使用邮件应用正在查看的电子邮件中。访问网关(SWG)可以拦截通过点击链接而生成的访问请求,并且可以确定相应的URL是安全的还是可疑的。如果URL被认为是安全的,则访问网关可以允许请求继续进行至相应的网站或web服务器。如果该URL是可疑的,则访问网关可以重定向请求经由托管的安全浏览器处理。安全浏览器可以请求访问和访问网页(代表标准浏览器),并且可以允许将网页信息传送到标准浏览器,类似于经由浏览器重定向对网络应用的处理,如结合至少图7和5所讨论的。

[0153] C.用于在嵌入式浏览器中执行用于不同来源的网络应用的应用脚本的系统和方法

[0154] 本公开涉及用于在嵌入式浏览器中执行用于不同来源的网络应用的应用脚本的系统和方法。客户机应用可以经由嵌入式浏览器在客户机装置上执行。客户机应用可以经由嵌入式浏览器建立一个或多个会话或向一个或多个网络应用提供一个或多个会话。客户机应用可以建立策略并执行脚本来控制嵌入式浏览器的操作和功能。例如,可以在客户机应用的嵌入式浏览器内将网络应用提供给客户机装置的用户。客户机应用可以经由脚本引擎建立策略并执行脚本,以控制在嵌入式浏览器内执行的不同网络应用的操作。

[0155] 客户机应用可以生成和应用对嵌入式浏览器内执行的网络应用特有的策略,而不是覆盖、防止或以其他方式修改网络应用所源自的实体和/或来源的策略。在一些实施例中,客户机应用可以生成和应用策略以覆盖在客户机应用的嵌入式浏览器内执行的一个或多个网络应用的相同来源策略。客户机应用通过嵌入式浏览器可以在客户机应用的嵌入式浏览器内执行的不同网络应用之间提供跨应用协作,以使得网络应用可以利用嵌入式浏览器内执行的其他网络应用的功能,即使其他网络应用是不同的实体和/或不同的来源。例如,客户机应用的脚本引擎可以执行应用脚本,以使用不同实体和/或不同来源的网络应用执行任务。在一些实施例中,第一实体和/或第一来源的第一一个或多个网络应用可以协作或以其他方式共享、传输和/或接收来自第二不同实体和/或第二不同来源的第二一个或多个网络应用的数据来完成相应的任务。

[0156] 客户机应用可以在客户机装置与来自一个或多个不同实体和/或不同来源的一个或多个网络应用之间建立信任域。信任域可以形成供客户机装置的用户执行任务(例如但不限于跨来自不同实体和/或不同来源的网络应用传输数据)的平台。信任域可以在客户机应用的嵌入式浏览器内执行。信任域可以为受信任的来源的网络应用提供受信任的环境以在网络应用之间共享数据,和/或使用多个不同网络应用的功能为客户机装置的用户执行各种任务。客户机应用可以包括或以其他方式提供生成一个或多个应用脚本的脚本引擎。应用脚本可以包括指令,以跨来自不同实体和/或不同来源的网络应用执行一个或多个任务。

[0157] 与客户机应用的嵌入式浏览器耦合或在客户机应用的嵌入式浏览器内执行的网络应用可以利用信任域进行跨应用协作。例如,网络应用可以包括源自或由不同来源处的不同服务器托管的应用套件或由其提供。套件可以包括相同来源安全策略,该策略限制或防止来自不同套件、不同服务器和/或不同来源的网络应用之间的协作或集成。本文所述的系统和方法可以建立信任域,该信任域形成用于在来自不同套件、不同服务器和/或不同来源的网络应用之间进行协作或集成的平台。例如,客户机装置的用户可以使用由客户机应用的脚本引擎生成的应用脚本,跨信任域内的不同网络应用执行一个或多个任务。

[0158] 应用脚本可以跨多供应商网络应用工作,以为客户机装置的用户执行各种任务。例如,可以生成应用脚本,使得它们满足来自不同套件、不同服务器、不同实体和/或不同来源的网络应用的相应安全策略。因此,客户机应用可以作为客户机装置的脚本主机操作,以跨来自不同套件、不同服务器、不同实体和/或不同来源的不同应用经由脚本引擎并在信任域内执行脚本。例如,客户机应用的脚本引擎可以编写应用脚本和/或自动化任务,例如但不限于从第一来源处的第一实体的第一网络应用提取数据并将数据传输到第二来源处的第二实体的第二网络应用。

[0159] 参考图11,描绘了用于在嵌入式浏览器中跨不同来源的网络应用进行协作的系统1100的框图。系统1100可以包括在客户机装置1102上执行的客户机应用1104的一个实施例。客户机应用1104可以在一个或多个不同来源1130处的一个或多个不同实体1132的一个或多个网络应用1134之间建立信任域1108。例如,客户机应用1104可以包括脚本引擎1110,以针对客户机装置1102的用户跨一个或多个不同来源1130处的一个或多个不同实体1132的一个或多个网络应用1134执行一个或多个应用脚本1112。

[0160] 客户机应用1104包括嵌入式浏览器1106、信任域1108、脚本引擎1110、策略管理器1120和认证服务器1122。客户机应用1104可以由来源1130c(例如,第三来源)托管或源于来源1130c,并由实体1132c(例如,第三实体)提供。客户机应用1104可以使用脚本引擎1110的应用脚本1112建立到一个或多个网络应用1134a-1134n的一个或多个会话1140a-1140n,以跨网络应用1134a-1134n执行一个或多个任务1116。客户机应用1104可以是本文描述的任何客户机应用的实例。例如,客户机应用1104可以与图4的客户机应用404相同或基本相似。

[0161] 客户机应用1104可以包括集成到客户机应用1104内的嵌入式浏览器1106,以访问多个网络应用1134a-1134n中的一个或多个网络应用1134。具有嵌入式浏览器1106的客户机应用1104(CEB)可以包括如本文所述的CEB的任何元件。例如,嵌入式浏览器1106可以与以上关于图4描述的嵌入式浏览器410相同或基本相似。嵌入式浏览器1106可以包括web浏览器应用或引擎的元件和功能。嵌入式浏览器1106可以本地呈现网络应用1134a-1134n中的一个或多个作为客户机应用1104的组件或扩展。例如,嵌入式浏览器1106可以呈现CEB内部的SaaS/Web应用,该应用可以向CEB提供应用会话的完全可见性和控制。

[0162] 客户机应用1104可以通过嵌入式浏览器1106为客户机装置1102建立到网络应用1134a-1134n中的一个或多个的会话1140a-1140n中的一个或多个。会话1140a-1140n可以包括如本文所述的任何类型或形式的会话。例如,会话1140a-1140n可以包括但不限于应用会话、执行会话、桌面会话、托管桌面会话、终端服务会话、浏览器会话、远程桌面会话和远程应用会话。会话1140a-1140n可以包括在网络应用1134a-1134n与客户机装置1102之间建立的加密和/或安全会话。

[0163] 网络应用1134a-1134n可以包括本文详细描述的任何类型或形式的网络应用。例如,网络应用1134a-1134n可以与以上关于图4描述的网络应用406相同或基本相似。网络应用1134a-1134n可以包括由一个或多个服务器(例如,第三方服务器)服务和/或托管在一个或多个服务器(例如,第三方服务器)上的应用(app)。网络应用1134a-1134n可以包括托管在由客户机装置1102经由网络104访问的至少一个服务器上的应用。网络应用1134a-1134n可以包括但不限于web应用、桌面应用、远程托管的应用、虚拟应用、软件即服务(SaaS)应用、移动应用、HDX应用、本地应用、本机应用(例如,客户机装置的本机)和/或与客户机装置1102耦合的装置。网络应用1134a-1134n可以包括或执行一个或多个网页。例如,网络应用1134a-1134n中的每一个可以包括多个网页。网页可以包括网站和/或与至少一个网络应用1134相关联的web服务器。网页可以提供与至少网络应用1134相对应的内容。

[0164] 网络应用1134a-1134n中的每一个都可以源于至少一个来源1130。来源1130a-1130n可以指的是网页或网络应用1134的来源。来源1130a-1130n包括域名或URI方案、主机名和端口号的组合。例如,来源1130可以指URL的协议、主机和端口的组合。在一些实施例中,具有相同来源1130的两个或更多个URL可以具有相同的协议、主机和端口。例如,如果用于它们各自URL的协议、主机和端口相同,则两个或更多个网页或网络应用1134可以具有相同的来源1130。

[0165] 网络应用1134a-1134n中的每一个可以由至少一个实体1132提供。实体1132a-1132n可以包括一个或多个网络应用1134a-1134n的供应商或提供者。例如,实体1132a-1132n可以生成并提供一个或多个网络应用1134a-1134n。实体1132a-1132n可以包括在一个或多个第三方服务器1136上执行的第三方供应商。实体1132a-1132n可以将多个网络应用1134a-1134n一起分组或以其他方式提供在一个或多个套件1138(或应用套件)中。套件1138可以包括被组合并一起提供给一个或多个客户机装置1102的多个网络应用1134a-1134n。例如,套件1138可以包括在单个可执行和/或可安装文件内输送的两个或更多个网络应用1134a-1134n(例如,软件程序)。套件1138可以包括来自相同或公共实体1132的多个网络应用1134a-1134n。套件1138可以包括来自相同或公共来源1130的多个网络应用1134a-1134n。

[0166] 网络应用1134a-1134n可以分别由服务器1136a-1136n(例如,第三方服务器)托管。网络应用1134a-1134n可以包括托管在由客户机装置1102经由网络104访问的至少一个服务器1136上的应用。服务器1136a-1136n可以与托管客户机应用1104的服务器分离。来源1130a-1130n中的每一个可以包括或对应于至少一个服务器1136。在一些实施例中,来源1130可以包括或对应于多个服务器1136。例如,应用的套件1137可以源自或由来源1130的服务器1138托管。例如,第一一个或多个网络应用1134a-1134n可以包括应用的第一套件1138a,其源自第一来源1130a处的第一一个或多个服务器1136a或由其托管。第二一个或多个网络应用1134a-1134n可以包括应用的第二套件1138b,其源自第二来源1130b处的第二一个或多个服务器1136b或由其托管。服务器1136a-1136n可以与图4的服务器430相同或基本相似。

[0167] 客户机应用1104可以建立、提供或包括信任域1108。信任域1108可以包括不同网络应用1134a-1134n之间的平台或一个或多个连接。连接可以包括在不同网络应用1134a-1134n之间建立的一个或多个信任关系。在一些实施例中,信任域1108可以包括或形成为多

个网络应用1134a-1134n之间的安全平台或连接。信任域1108通过安全平台连接两个或更多个网络应用1134a-1134n,以使得不同实体1132a-1132n和/或不同来源1130a-1130n的网络应用1134a-1134n可以从彼此共享、交换、传输和/或接收数据或信息。在一些实施例中,可以使用本文描述的加密技术来对信任域1108和多个应用1134a-1134n之间的信任关系进行加密。信任域1108可以与网络104或多个网络104耦合(例如,耦合多个网络104),以允许不同网络应用1134a-1134n之间的通信、信息交换和协作。

[0168] 客户机应用1104可以建立单个信任域1108或多个信任域1108。例如,客户机应用1104可以建立单个信任域1108,其包括客户机装置访问或请求访问的每个网络应用1134。客户机应用1104可以建立多个信任域1108,其中每个信任域1108具有两个或更多个网络应用1134a-1134n。可以部分地基于它们各自的来源和/或实体,将网络应用1134a-1134n分组在公共的信任域1108内。在一些实施例中,网络应用1134a-1134n可以部分地基于它们执行的功能、它们执行或可以执行的任务1116、各自的网络应用的类型和/或各自的网络应用的属性,被分组在公共的信任域1108内。客户机应用1104可以为网络应用1134a-1134n的不同套件1138a-1138n建立多个信任域1108。

[0169] 客户机应用1104可以包括脚本引擎1110。脚本引擎1110可以以一种或多种不同的脚本语言生成并执行脚本,以允许客户机装置1102的用户在客户机应用1104的嵌入式浏览器1106内在不同实体1132a-1132n和/或不同来源1130a-1130n的不同网络应用1134内进行交互。例如,脚本引擎1110可以为来自不同实体1132a-1132n和/或不同来源1130a-1130b的网络应用1134生成并执行应用脚本1112。因此,客户机应用1104可以使用来自不同实体1132a-1132n和/或不同来源1130a-1130b的网络应用1134为客户机装置1102的用户执行任务1116,以便在嵌入式浏览器1106中跨不同实体1132a-1132n和/或不同来源1130a-1130b的各自的网络应用1134进行协作。脚本引擎1110可以包括一个或多个处理器,以执行一个或多个应用脚本。脚本引擎1110可以包括一个或多个软件程序以执行一个或多个应用脚本。

[0170] 应用脚本1112可以包括在一个或多个网络应用1134a-1134n上支持和/或执行的计算机语言或编程语言。应用脚本1112可以在可被执行的文件内包括一个或多个指令1114或一系列命令。指令1114可以包括一系列命令或代码,以执行处理器的一个或多个操作。应用脚本1112可以支持不同实体1132a-1132n和/或不同来源1130a-1130b的网络应用1134a-1134n,并且在不同实体1132a-1132n和/或不同来源1130a-1130b的网络应用1134a-1134n上执行。例如,应用脚本1112可以在第一实体1132和/或第一来源1130的第一网络应用1134上,在其内或以其他方式使用第一网络应用1134来支持和/或执行一个或多个任务1116,并且在第二不同实体1132和/或第二不同来源1130的第二不同网络应用1134上,在其内或以其他方式使用第二不同网络应用1134来支持和/或执行一个或多个任务1116。

[0171] 任务1116可以包括要在客户机装置1102上或经由客户机装置1102进行或执行的动作。任务1116可以包括要使用至少一个网络应用1134在客户机装置1102上或经由客户机装置1102进行或执行的动作。任务1116可以包括在至少一个客户机装置1102和/或网络应用1134上或经由至少一个客户机装置1102和/或网络应用1134进行或执行的编程单元、执行单元、工作或处理单元。例如,任务1116可以包括但不限于发送电子邮件,起草word文档,将数据从第一网络应用1134传输到第二不同的网络应用1134,或包括例如经由客户机应用

1104和嵌入式浏览器1106与耦合至客户机装置1102或在客户机装置1102上执行的任何网络应用1134、程序、文件和/或装置进行交互的任何动作。任务1116可以包括但不限于打印功能、在特定位置中(例如,在客户机装置上、在网络服务器上)存储数据或文件、下载功能、上传功能、摄像机功能、查看装置功能、拍照功能、获得签名功能和/或数字签名功能。此处提供的任务1116出于说明目的而列出,无论如何不旨在进行限制。

[0172] 客户机应用可以包括策略管理器1120。策略管理器1120可以生成用于认证客户机装置1102的用户和/或客户机装置1102的一个或多个策略。策略管理器1120生成用于建立一个或多个网络应用1134a-1134n、一个或多个来源1130a-1130n和/或一个或多个实体1132a-1132n的信任级别的一个或多个策略。策略管理器1120生成用于在一个或多个网络应用1134a-1134n、一个或多个来源1130a-1130n和/或一个或多个实体1132a-1132n之间建立信任关系的一个或多个策略。例如,信任级别可以对应于访问特权,例如但不限于对客户机装置的不同装置或系统的访问、安全特权、嵌入式浏览器内的各自的网络应用的功能和/或各自的网络应用或装置可以在嵌入式浏览器内执行的任务。在一些实施例中,响应于被分配了特定的信任级别,网络应用可以被允许但不限于将数据传输到客户机应用的嵌入式浏览器内的不同实体和/或不同来源的第二网络应用。策略管理器1120可以确定一个或多个网络应用1134a-1134n、一个或多个来源1130a-1130n和/或一个或多个实体1132a-1132n中的哪一个可以被信任并包括在一个或多个信任域1108内或与之耦合。

[0173] 在一些实施例中,策略管理器1120应用或以其他方式提供用于管理网络应用1134a-1134n与客户机装置1102之间的会话1140a-1140n的策略。策略管理器1120可以应用或以其他方式提供用于管理或建立网络应用1134a-1134n与客户机装置1102之间的会话1140a-1140n的策略。例如,策略管理器1120可以为网络应用1134a-1134n与客户机装置1102之间的会话1140a-1140n建立信任级别。策略管理器1120可以生成和/或存储用于会话1140a-1140n的多个策略。策略可以用于控制网络应用1134a-1134n与客户机装置1102之间的通信和信息交换。例如,策略可以包括访问策略和/或安全策略。客户机应用1104可以通过策略管理器1120将一个或多个策略应用于会话1140,以保护网络应用1134和客户机装置1102之间的相应的会话1140。策略可以用于通过不同的会话1140a-1140n控制流量级别和/或流量类型。策略可用于管理一个或多个会话1140a-1140n的服务级别。策略管理器1120可以应用策略以加密或以其他方式保护一个或多个会话1140a-1140n。可以向网络应用1134a-1134n、客户机装置1102和/或客户机装置1102或网络应用1134a-1134n的用户中的每一个分配策略。策略可用于控制和/或增强在网络应用1134a-1134n与客户机装置1102之间建立的一个或多个会话1140a-1140n的使用。

[0174] 客户机应用可以包括认证管理器1122。认证管理器1122可以认证客户机装置1102的一个或多个用户、一个或多个客户机装置1102、一个或多个网络应用1134a-1134n、一个或多个来源1130a-1130n、和/或一个或多个实体1132a-1132n。例如,认证可以认证接收到的认证凭证,并将接收到的认证凭证与存储的认证凭证进行比较,以认证客户机装置1102的一个或多个用户、一个或多个客户机装置1102、一个或多个网络应用1134a-1134n、一个或多个来源1130a-1130n、和/或一个或多个实体1132a-1132n。认证管理器1122可以存储用于客户机装置1102的一个或多个用户、一个或多个客户机装置1102、一个或多个网络应用1134a-1134n、一个或多个来源1130a-1130n、和/或一个或多个实体1132a-1132n的认证凭

证。在一些实施例中，认证管理器1122可以与在第三方服务器1136上执行的认证服务器耦合，以检索、存储和/或接收用于客户机装置1102的一个或多个用户、一个或多个客户机装置1102、一个或多个网络应用1134a-1134n、一个或多个来源1130a-1130n、和/或一个或多个实体1132a-1132n的认证凭证。

[0175] 客户机装置1102可以是本文描述的任何客户机装置的实例。例如，客户机装置1102可以与以上关于图2描述的客户机装置202、204、以上关于图3描述的客户机装置302、和/或以上关于图4描述的客户机装置402a相同或基本相似。客户机装置1102可以包括但不限于计算装置、台式计算装置和/或移动计算装置。客户机装置1102可以包括或存储用于客户机装置1102的一个或多个用户的上下文1112。用户的上下文1112可以包括用户和/或客户机装置1102的属性或特征。例如，用户的上下文1112可以包括但不限于：用户的身份、用户简档、用户的家庭位置、与该用户相关联的一个或多个客户机装置1102的位置、关于执行客户机应用1104的客户机装置1102的信息、关于一个或多个网络应用1140a-1140n的信息和/或关于与用户相关联的实体的信息。

[0176] 网络104可以是公共网络，例如广域网(WAN)或互联网。在一些实施例中，网络104可以是诸如局域网(LAN)或公司内联网的专用网络。网络104可以采用一种或多种类型的物理网络和/或网络拓扑，例如有线和/或无线网络，并且可以采用一种或多种通信传输协议，例如传输控制协议(TCP)、互联网协议(IP)、用户数据报协议(UDP)或其他类似协议。

[0177] 在一个或多个实施例中，以硬件或硬件和软件的组合来实现上述元件或实体中的每一个。客户机应用1104的每个组件可以使用以上结合图1详细描述的硬件或硬件或软件的组合来实现。例如，这些元件或实体中的每一个可以包括在客户机装置1102的硬件上执行的任何应用、程序、库、脚本、任务、服务、进程或任何类型和形式的可执行指令(例如，客户机应用404)。在一个或多个实施例中，硬件包括诸如一个或多个处理器的电路。

[0178] 参考图12，其描绘了用于在嵌入式浏览器中执行用于不同来源的网络应用的应用脚本的方法1200的一个实施例的流程图。该方法的功能可以使用在此结合图1-11详细描述的组件来实现或由其执行。简要概述，可以由客户机应用建立到第一网络应用的第一会话(1205)。可以由客户机应用建立到第二网络应用的第二会话(1210)。可以为一个或多个网络应用识别应用脚本(1215)。可以执行应用脚本(1220)。

[0179] 现在参考操作(1205)，并且在一些实施例中，客户机应用可以建立到第一网络应用的第一会话。客户机应用可以经由客户机应用内的嵌入式浏览器与第一来源处的第一实体的第一实体的第一一个或多个网络应用建立第一一个或多个会话。客户机应用可以通过嵌入式浏览器在客户机装置上执行。客户机装置可以与用户相关联。客户机应用可以包括嵌入式浏览器，以为客户机装置的用户提供对一个或多个网络应用的访问。客户机应用可以经由客户机应用内的嵌入式浏览器为客户机装置的用户建立与一个或多个网络应用的一个或多个会话。客户机应用可以通过嵌入式浏览器在客户机装置上执行。客户机装置可以与用户相关联。会话可以包括如本文所述的任何类型或形式的会话。例如，会话可以包括但不限于应用会话、执行会话、桌面会话、托管的桌面会话、终端服务会话、浏览器会话、远程桌面会话和远程应用会话。会话可以包括在网络应用和用户的客户机装置之间建立的加密和/或安全会话。

[0180] 网络应用可以包括托管在由客户机装置经由网络访问的服务器(例如，第三方服

务器)上的应用。网络应用可以包括但不限于Web应用、桌面应用、虚拟应用、软件即服务(SaaS)应用、移动应用、HDX应用、本地应用、本机应用(例如,客户机装置的本机)和/或与客户机装置耦合的装置。网络应用可以包括从一个或多个服务器提供服务和/或托管在一个或多个服务器上的应用(app)。例如,网络应用中的每一个可以包括可以提供与各自的网络应用相关联的内容的一个或多个位置或一个或多个存在点。在一些实施例中,网络应用可以包括托管在由用户的客户机装置经由一个或多个网络访问的服务器上的应用。网络应用可以包括或执行一个或多个网页。客户机应用可以提供对本地文件或本机文件(例如,在客户机装置上执行的文件)的访问。

[0181] 现在参考操作(1210),并且在一些实施例中,客户机应用可以建立到第二网络应用的第二会话。例如,客户机应用可以经由客户机应用内的嵌入式浏览器与第二来源处的第二实体的第二一个或多个网络应用建立第二一个或多个会话。可以从一个或多个不同实体和/或一个或多个不同来源提供网络应用。例如,每个网络应用可以由至少一个实体托管或以其他方式由至少一个实体提供。实体可以包括各自的网络应用的供应商或提供者或与该网络应用相对应的网页。每个实体可以包括一个或多个服务器,这些服务器在一个或多个不同的来源处托管一个或多个网络应用。来源可以指各自的网络应用或与网络应用1134相对应的网页的来源。来源可以包括域名或URI方案、主机名和端口号的组合。例如,来源可以指URL的协议、主机和端口的组合。

[0182] 实体和/或来源可以将策略分配给它们各自的网络应用中的每一个,以控制各自的网络应用的访问和/或操作。该策略可以包括访问策略和/或来源策略(例如,相同来源策略)。例如,策略(例如,相同来源策略)可以指示特定网络应用可以与哪些其他网络应用进行交互或协作,例如但不限于,用于在各个网络应用之间共享和/或传输数据。在一些实施例中,来自相同来源的网络应用可以共享一个或多个策略(例如,访问策略,来源策略)。该策略可以指示各自的网络应用的来源的信任级别。

[0183] 在一些实施例中,第一来源和第二来源可以是使相同来源策略失败的不同来源。例如,第一来源可以指与第二来源不同的来源。每个相应的来源都可以具有来源策略,例如但不限于相同来源策略。在相同来源策略下,第一网络应用可以被限制为与与第一网络应用相同来源的第二不同网络应用协作,从第二不同网络应用访问数据和/或将数据传输到第二不同网络应用。例如,第一来源的第一网络应用可以与第一来源的第二不同网络应用进行协作,从第一来源的第二不同网络应用访问数据和/或将数据传输到第一来源的第二不同网络应用,但是可以防止、阻止或限制第一来源的第一网络应用与第二来源的第三不同网络应用协作,从第三不同网络应用访问数据和/或将数据传输到第三不同网络应用。因此,不同的来源可能会使相同来源策略失败,因为它们源自不同的来源。相同的来源可以通过相同来源策略。在一些实施例中,来自相同实体的网络应用可以共享一个或多个策略(例如,访问策略、来源策略)。因此,来自相同来源的网络应用可以通过相同来源策略。来自不同来源的网络应用可能会使相同来源策略失败。在一些实施例中,来自相同实体的网络应用可以具有一个或多个不同的策略(例如,访问策略、来源策略)。

[0184] 可以将网络应用分组为具有多个网络应用的套件(例如,应用套件)。提供相应网络应用的实体或托管相应网络应用的来源和/或服务器可以将多个网络应用分组为应用的套件。例如,第一一个或多个网络应用可以包括源自第一来源处的第一一个或多个服务器

或由其托管的应用的套件。第二一个或多个网络应用可包括源自第二来源处的第二一个或多个服务器或由其托管的应用的套件。套件可以包括不同但相关的网络应用。例如，套件可以包括相同来源和/或相同实体的网络应用。公共或相同套件中的每个网络应用都可以执行一个或多个公共功能任务和/或一个或多个不同功能或任务。在一些实施例中，套件可以包括以单个可执行格式或文件提供的两个或更多个网络应用。

[0185] 在一些实施例中，可以在不同的网络应用之间建立信任域。例如，可以在客户机应用的嵌入式浏览器内执行的不同网络应用之间建立信任域。客户机应用可以在第一域处的第一实体的第一一个或多个网络应用与第二域处的第二实体的第二一个或多个网络应用之间建立信任域。信任域可以包括和/或提供公共平台，以在不同网络应用之间共享信息。例如，客户机应用可以在多个网络应用之间建立信任关系(例如，会话、连接)。例如，与一个或多个第二不同网络应用具有信任关系的第一一个或多个网络应用可以被包括在公共信任域内。公共或相同信任域内的网络应用可以具有在各个网络应用之间建立的一个或多个信任关系。例如，响应于一个或多个应用脚本，公共或相同信任域内的网络应用可以彼此协作、共享、访问、接收和/或传输数据。信任域可以提供安全的环境或安全的连接，以允许各种应用之间进行通信和信息交换。

[0186] 在一些实施例中，信任域可以包括或形成为多个不同网络应用之间的安全平台或连接。例如，信任域通过安全平台连接两个或更多个网络应用，以使得不同实体和/或不同来源的网络应用可以彼此共享、交换、传输和/或接收数据或信息。在一些实施例中，可以使用如本文所述的加密技术来对多个应用之间的信任域和信任关系进行加密。信任域可以允许不同网络应用之间的通信、信息交换和协作。

[0187] 客户机应用可以为信任域建立一个或多个策略。策略可以包括但不限于访问策略、分组策略和/或来源策略。策略可以指示对于客户机装置的用户和/或客户机装置，可以将哪些网络应用分组到彼此信任的公共域中。策略可以指示特定的第一一个或多个网络应用可能需要与第二一个或多个不同网络应用一起被分组到公共信任域的属性。例如，可以在客户机应用的嵌入式浏览器内将网络应用提供给客户机装置的用户。客户机应用可以为在客户机应用的嵌入式浏览器内执行的第一一个或多个网络应用生成并分配一个或多个策略，以控制访问，例如但不限于由第二不同的一个或多个网络应用通过信任域的访问。在一些实施例中，策略可以用于覆盖托管各自的网络应用的来源和/或服务器的相同来源策略。因此，客户机应用通过嵌入式浏览器可以生成和/或控制用于和应用于每个网络应用的策略和脚本。因此，客户机应用通过嵌入式浏览器可以提供在客户机应用的嵌入式浏览器内执行的不同网络应用之间的跨应用协作。例如，客户机应用的脚本引擎可以执行应用脚本，以使用不同实体和/或不同来源的网络应用执行任务。例如，第一实体和/或第一来源的第一一个或多个网络应用可以协作或以其他方式共享、传输和/或接收来自第二不同实体和/或第二不同来源的第二一个或多个网络应用的数据，以完成相应的任务。

[0188] 客户机应用可以建立策略来控制客户机装置的用户可以对一个或多个网络应用所具有的访问级别。例如，客户机应用可以部分地基于用户的凭证并响应于用户的认证，为用户分配对一个或多个不同的网络应用的不同策略和/或不同访问级别。访问级别可以指示客户机装置的用户可以与哪些网络应用进行交互。访问级别可以指示允许用户访问一个或多个网络应用的程度。例如，访问级别可以指示用户可以利用网络应用的哪些功能和/或

用户可以利用网络应用执行哪个或哪些任务。访问级别可以指示特定用户和/或特定客户机装置可以与哪些其他用户和/或其他客户机装置进行交互。客户机装置的用户可以与之交互的应用。访问级别可以指示不同网络应用之间的通信级别。

[0189] 在一些实施例中，客户机应用可以为客户机装置的用户建立一个或多个信任域。客户机应用可以部分地基于特定用户先前已经访问和/或请求访问的网络应用，在网络应用之间分组或建立信任关系。客户机应用可以部分地基于特定用户先前已经经由客户机装置执行的一个或多个任务以及与该任务相对应的网络应用和/或可以进行或执行相应任务的网络应用，在网络应用之间进行分组或建立信任关系。

[0190] 在一些实施例中，客户机应用可以为客户机装置建立一个或多个信任域。客户机应用可以部分地基于特定客户机装置先前已交互或访问和/或请求访问的网络应用，在网络应用之间分组或建立信任关系。客户机应用可以部分地基于特定客户机装置先前已经进行或执行的一个或多个任务以及与任务相对应的网络应用和/或可以进行或执行相应任务的网络应用，在网络应用之间分组或建立信任关系。

[0191] 在一些实施例中，客户机应用可以为一组用户(例如，办公场所、家庭住户)建立一个或多个信任域。客户机应用可以部分地基于特定用户组先前已访问和/或请求访问的网络应用，在网络应用之间分组或建立信任关系。客户机应用可以部分地基于特定用户组先前已经经由一个或多个客户机装置或计算装置执行的一个或多个任务以及与该任务相对应的网络应用和/或可以进行或执行相应的任务的网络应用，在网络应用之间分组或建立信任关系。

[0192] 在一些实施例中，客户机应用可以为多个客户机装置或计算装置(例如，办公场所、家庭住户)建立一个或多个信任域。客户机应用可以部分地基于特定的多个客户机装置或计算装置先前已经交互或访问和/或请求访问的网络应用，在网络应用之间分组或建立信任关系。客户机应用可以部分地基于特定的多个客户机装置或计算装置先前已经进行或执行的一个或多个任务以及与该任务相对应的网络应用和/或可以进行或执行相应的任务的网络应用，在网络应用之间分组或建立信任关系。

[0193] 在一些实施例中，可以响应于相同用户针对第一一个或多个网络应用和第二一个或多个网络应用的认证，经由与第三来源相对应的用户的第三实体的客户机装置上的客户机应用建立信任域。例如，客户机应用可以认证客户机装置的用户。认证可以包括针对一个或多个网络应用认证用户。客户机应用可以响应于用户的认证而与一个或多个网络应用建立一个或多个会话。例如，客户机应用可以接收用户的认证凭证，并识别该用户访问或有权与之交互的网络应用。客户机应用可以与用户访问或有权与之交互的网络应用建立会话。客户机应用可以为用户访问或有权与之交互的网络应用建立一个或多个信任域。网络应用可以包括不同实体和/或不同来源的多个网络应用。客户机应用可以使用信任域在不同实体和/或不同来源的网络应用之间建立信任关系。客户机应用可以为信任域建立访问策略。例如，在一些实施例中，对于客户机装置的用户的用于访问信任域的访问策略。

[0194] 在一些实施例中，认证可以包括向用户提供对一个或多个网络应用的访问级别。访问级别可以对应和/或指示用户可以使用各自的网络应用执行哪些任务、功能或操作。例如，可以向客户机装置的用户提供或分配对第一网络应用的第一访问级别和对第二网络应用的第二访问级别。第一访问级别和第二访问级别可以不同。客户机装置的用户可以对分

组在公共信任域中的每个网络应用具有相同的访问级别。客户机装置的用户可以对分组在公共信任域中的一个或多个不同网络应用具有一个或多个不同的访问级别。

[0195] 现在参考操作(1215),并且在一些实施例中,可以为一个或多个网络应用识别应用脚本。例如,在第三来源处的用户的客户机装置的客户机应用内的脚本引擎可以识别应用脚本。客户机应用和/或客户机装置可以位于与第一来源和第二来源不同的第三来源处或由第三来源托管。例如,第三来源可以由与托管第一来源的一个或多个服务器和/或托管第二来源的一个或多个服务器不同的服务器托管。客户机应用和/或客户机装置可以由与第三来源相对应的第三实体提供。第三实体可以不同于第一实体和/或第二实体。应用脚本可以包括各自与第一来源处的第一实体的第一一个或多个网络应用以及第二来源处的第二实体的第二一个或多个网络应用交互的指令。

[0196] 脚本引擎可以在客户机应用的嵌入式浏览器内在客户机装置上执行。脚本引擎可以生成一个或多个应用脚本以与一个或多个网络应用进行交互,客户机应用为客户机装置的用户建立与该一个或多个网络应用的会话。在一些实施例中,脚本引擎可以将一个或多个应用脚本例如但不限于存储在客户机应用的数据库内。应用脚本可以对应于一个或多个任务、操作或功能。应用脚本可以对应于一个或多个网络应用。应用脚本可以对应于将使用一个或多个网络应用执行的一个或多个任务、操作或功能。在一些实施例中,可以响应于至少一个应用脚本,使用不同实体和/或不同来源的两个或更多个网络应用来执行任务、操作和/或功能。脚本引擎可以以一种或多种不同的脚本语言生成和执行脚本,以允许客户机装置的用户在客户机应用的嵌入式浏览器内的不同实体和/或不同来源的不同网络应用内进行交互。客户机应用可以使用应用脚本为客户机装置的用户执行任务,以与来自不同实体和/或不同来源的不同网络应用进行交互并跨来自不同实体和/或不同来源的不同网络应用进行交互。

[0197] 应用脚本可以包括支持一个或多个网络应用和/或在一个或多个网络应用上执行的计算机语言或编程语言。在一些实施例中,脚本引擎可以从一个或多个第三方服务器检索应用脚本。例如,脚本引擎可以从托管或提供一个或多个网络应用的一个或多个第三方服务器检索应用脚本。检索到的应用脚本可以对应于相应服务器托管或提供的网络应用。应用脚本可以在例如可以由客户机应用的嵌入式浏览器内的一个或多个网络应用执行的文件内包括一个或多个指令或一系列命令。应用脚本可以在不同实体和/或不同来源的网络应用上执行或跨不同实体和/或不同来源的网络应用执行。例如,应用脚本可以在第一实体和/或第一来源的第一网络应用上、第一实体和/或第一来源的第一网络应用内或以其他方式使用第一实体和/或第一来源的第一网络应用来支持和/或执行一个或多个任务,并且在第二不同实体和/或第二不同来源的第二不同网络应用上、第二不同实体和/或第二不同来源的第二不同网络应用内或以其他方式使用第二不同实体和/或第二不同来源的第二不同网络应用来支持和/或执行一个或多个任务。应用脚本可以被执行以覆盖一个或多个网络应用的相同来源策略,以使得不同实体和/或不同来源的网络应用可以彼此协作,以为客户机装置的用户在客户机应用的嵌入式浏览器内执行各种任务。

[0198] 脚本引擎可以响应于执行任务的请求来生成或识别应用脚本。例如,客户机应用可以接收在嵌入式浏览器内执行任务的请求。客户机应用可以将任务请求传输到脚本引擎。脚本引擎可以识别执行所请求的任务所需的一个或多个网络应用。脚本引擎可以生成

或识别与执行所请求的任务所需的一个或多个网络应用相对应的一个或多个应用脚本。客户机应用可以响应于访问网络应用的请求来生成或识别应用脚本。例如，客户机应用可以在嵌入式浏览器内接收对网络应用的请求。客户机应用可以将网络应用请求传输到脚本引擎。脚本引擎可以生成或识别与执行所请求的任务所需的一个或多个网络应用相对应的一个或多个应用脚本。

[0199] 现在参考操作(1220)，并且在一些实施例中，可以执行应用脚本。例如，脚本引擎可以执行应用脚本的指令，以跨第一来源处的第一实体的第一一个或多个网络应用和第二来源处的第二实体的第二一个或多个网络应用执行任务。应用脚本可以包括在可被执行的文件内一个或多个指令或一系列命令。指令可以包括例如由客户机应用的脚本引擎执行的一系列命令或代码。指令可以包括将被执行以进行一个或多个任务的一系列命令或代码。指令可以包括或识别要执行的任务、执行相应任务的一个或多个网络应用、相应的一个或多个网络应用的实体、相应的一个或多个网络应用的来源以及与相应的网络应用、实体和/或来源相对应的策略。任务可以包括但不限于要在客户机装置上或经由客户机装置进行或执行的动作。例如，任务可以包括要使用至少一个网络应用在客户机装置上或经由客户机装置进行或执行的动作。任务可以包括在至少一个客户机装置和/或网络应用上或经由至少一个客户机装置和/或网络应用进行或执行的编程单元、执行单元、工作或处理单元。任务可以包括但不限于打印功能、在特定位置中(例如，在客户机装置上、在网络服务器上)存储数据或文件、下载功能、上传功能、摄像机功能、查看装置功能、拍照功能、获得签名功能和/或数字签名功能。例如，任务可以包括但不限于经由客户机应用和嵌入式浏览器将数据从第一来源的第一实体的第一网络应用传输到第二不同来源的第二不同实体的第二不同网络应用。

[0200] 在一些实施例中，脚本引擎可以通过第一一个或多个网络应用或第二一个或多个网络应用之一来启动应用脚本的执行。一个或多个网络应用可以在客户机应用的嵌入式浏览器内执行。脚本引擎可以将应用脚本提供给被识别为执行客户机装置的用户所请求的任务的网络应用或将其应用到被识别为执行客户机装置的用户所请求的任务的网络应用。例如，可以在客户机应用的嵌入式浏览器内执行第一实体和第一来源的第一一个或多个网络应用以及第二来源的第二实体的第二一个或多个网络应用。脚本引擎可以将应用脚本提供或应用到第一一个或多个网络应用以及第二一个或多个网络应用。脚本引擎可以利用第一一个或多个网络应用和/或第二一个或多个网络应用启动一个或多个应用脚本的执行。一个或多个应用脚本的执行顺序可以被包括在各个应用脚本的指令内和/或部分地基于要执行的任务。在一些实施例中，脚本引擎可以利用第一一个或多个网络应用启动一个或多个应用脚本的执行，并同时利用第二一个或多个网络应用启动一个或多个应用脚本的执行。脚本引擎可以在利用第二一个或多个网络应用启动一个或多个应用脚本的执行之前，利用第一一个或多个网络应用启动一个或多个应用脚本的执行。脚本引擎可以在利用第二一个或多个网络应用启动一个或多个应用脚本的执行之后，利用第一一个或多个网络应用启动一个或多个应用脚本的执行。应用脚本可以使相应的一个或多个网络应用执行至少一个任务。

[0201] 在一些实施例中，所请求的任务可以包括多个任务或不同组的任务。脚本引擎可以将应用脚本提供给第一一个或多个网络应用，并且响应于该应用脚本，第一一个或多个

网络应用可以执行所请求的任务的第一组任务。脚本引擎可以将应用脚本提供给第二一个或多个网络应用，并且响应于该应用脚本，第二一个或多个网络应用可以执行所请求的任务的第二组任务。在一些实施例中，在完成第一组任务之后，第一一个或多个网络应用可以通过信任域将与第一组任务相对应的数据传输至第二一个或多个网络应用。第二一个或多个网络应用可以接收与第一组任务相对应的数据。第二一个或多个网络应用可以使用与第一组任务相对应的数据来完成或以其他方式执行第二组任务。因此，第一一个或多个网络应用和第二一个或多个网络应用可以使用客户机应用的嵌入式浏览器内的信任域来共享数据并协作，以执行一个或多个任务。客户机应用经由信任域可以使用不同实体和/或不同来源的不同网络应用提供访问的便利性和用于执行任务的功能。信任域可以提供系统和方法，用于不同实体和/或不同来源的不同网络应用经由客户机应用和嵌入式浏览器彼此交互，以共享和交换信息。

[0202] 在一些实施例中，客户机应用可以响应于策略而允许应用脚本跨第一来源和第二来源进行交互。客户机应用可以生成和/或分配策略，以指定应将哪些网络应用或网络应用的哪些属性识别为受信任的并连接或包括在信任域内。在一些实施例中，策略可以指定源自特定来源和/或特定实体的网络应用可以是受信任的或不受信任的。例如，策略可以指定源自第一来源和/或第一实体的网络应用可以是受信任的并且被包括在客户机装置的用户的信任域内。该策略可以指定源自第二来源和/或第二实体的网络应用可能不被信任，并且因此可以被阻止或防止在客户机装置的用户的信任域内执行。在一些实施例中，策略可以指定源自第一来源的网络应用可以被信任以与源自信任域内的第二不同来源的网络应用进行交互和协作。例如，策略可以指示或指定第一来源和第二来源是经由客户机应用的嵌入式浏览器进行交互跨越的受信任的来源。策略可以指示或指定第一实体和第二实体是经由客户机应用的嵌入式浏览器进行交互跨越的受信任的实体。

[0203] 参考图13，其描绘了用于在嵌入式浏览器中跨不同来源的网络应用进行协作的方法1300的一个实施例的流程图。该方法的功能可以使用在此结合图1-11详细描述的组件来实现或由其执行。简要概述，可以由客户机应用建立到第一网络应用的第一会话(1305)。可以由客户机应用建立到第二网络应用的第二会话(1310)。可以确定网络应用的信任级别(1315)。可以允许网络应用之间的交互(1320)。

[0204] 现在参考操作(1305)，并且在一些实施例中，客户机应用可以建立到第一网络应用的第一会话。客户机应用可以经由客户机应用内的嵌入式浏览器与第一来源处的第一实体的第一一个或多个网络应用建立第一一个或多个会话。现在参考操作(1310)，并且在一些实施例中，客户机应用可以建立到第二网络应用的第二会话。客户机应用可以经由客户机应用内的嵌入式浏览器与第二来源处的第二实体的第二一个或多个网络应用建立第二一个或多个会话。

[0205] 客户机应用可以通过嵌入式浏览器在客户机装置上执行。客户机装置可以与用户相关联。客户机应用可以包括嵌入式浏览器，以为客户机装置的用户提供对一个或多个网络应用的访问。客户机应用可以经由客户机应用内的嵌入式浏览器为客户机装置的用户建立与一个或多个网络应用的一个或多个会话。客户机应用可以通过嵌入式浏览器在客户机装置上执行。客户机装置可以与用户相关联。会话可以包括如本文所述的任何类型或形式的会话。例如，会话可以包括但不限于应用会话、执行会话、桌面会话、托管的桌面会话、终

端服务会话、浏览器会话、远程桌面会话和远程应用会话。会话可以包括在网络应用和用户的客户机装置之间建立的加密和/或安全会话。

[0206] 网络应用可以包括托管在由客户机装置经由网络访问的服务器(例如,第三方服务器)上的应用。网络应用可以包括但不限于web应用、桌面应用、虚拟应用、软件即服务(SaaS)应用、移动应用、HDX应用、本地应用、本机应用(例如,客户机装置的本机)和/或与客户机装置耦合的装置。网络应用可以包括从一个或多个服务器提供服务和/或托管在一个或多个服务器上的应用(app)。例如,网络应用中的每一个可以包括可以提供与各自的网络应用相关联的内容的一个或多个位置或一个或多个存在点。在一些实施例中,网络应用可以包括托管在由用户的客户机装置经由一个或多个网络访问的服务器上的应用。网络应用可以包括或执行一个或多个网页。客户机应用可以提供对本地文件或本机文件(例如,在客户机装置上执行的文件)的访问。

[0207] 现在参考操作(1315),并且在一些实施例中,客户机应用可以确定网络应用的信任级别。例如,客户机应用可以响应于策略而确定第一来源和第二来源是被信任以经由嵌入式浏览器进行交互跨越的来源。来自不同实体和/或不同来源的网络应用可以在客户机应用的嵌入式浏览器内执行。客户机应用可以确定在客户机应用的嵌入式浏览器内执行的网络应用中的每一个的信任级别。可以为网络分配相同的信任级别。可以为一个或多个网络应用分配一个或多个不同的信任级别。信任级别可以对应于用于网络应用和/或客户机装置的用户与网络应用中的相应一个进行交互的访问特权。例如,信任级别可以对应于访问特权,例如但不限于对客户机装置的不同装置或系统的访问、安全特权、嵌入式浏览器内的相应网络应用的功能和/或相应网络应用或装置可以在嵌入式浏览器内执行的任务。在一些实施例中,响应于被分配了特定的信任级别,网络应用可以被允许但不限于将数据传输到客户机应用的嵌入式浏览器内的不同实体和/或不同来源的第二网络应用。

[0208] 客户机应用可以将一个或多个策略应用于一个或多个网络应用的属性,以确定相应网络应用的信任级别。例如,可以部分地基于提供特定网络应用的实体、特定网络应用的来源或两者的组合来分配信任级别。例如,可以部分地基于网络应用源自的来源来选择网络应用的信任级别。可以为不同来源和/或不同实体的网络应用分配相同的信任级别。在一些实施例中,可以为不同来源和/或不同实体的网络应用分配一个或多个不同的信任级别。

[0209] 策略可以指定要信任的多个不同的来源。例如,多个不同的来源可以包括第一来源和第二来源。策略可以指示来自特定来源和/或实体的网络应用可以与来自一个或多个不同来源和/或不同实体的一个或多个网络应用进行交互并与之协作。客户机应用可以将策略应用于一个或多个网络应用,以部分地基于它们的来源来确定特定网络应用可以与嵌入式浏览器内执行的哪些其他网络应用进行交互。例如,客户机应用可以响应于策略来确定第一来源和第二来源是被信任以经由嵌入式浏览器进行交互跨越的来源。因此,响应于该策略,可以允许来自第一来源的网络应用与来自第二来源的网络应用进行协作并交互。

[0210] 在一些实施例中,第一来源和第二来源使得相同来源策略失败。例如,当在相应来源的浏览器内执行时,网络应用的来源可以包括相同来源策略或将相同来源策略应用于它们托管或提供的网络应用。相同来源策略可以指示网络应用只能与来自相同来源的网络应用进行交互。因此,与第二来源不同的第一来源可能会使相同来源策略失败。但是,客户机应用可以经由嵌入式浏览器应用一个或多个策略,以覆盖或以其他方式忽略在客户机应用

的嵌入式浏览器内执行的网络应用的来源的相同来源策略。例如，当每个网络应用在客户机应用的嵌入式浏览器内执行时，客户机应用可以为客户机装置的用户生成并应用策略以控制相应网络应用的操作和/或功能。因此，第一来源和第二来源可能会使相同来源策略失败，但是，在客户机应用的嵌入式浏览器内，第一。

[0211] 现在参考操作(1320)，并且在一些实施例中，客户机应用可以允许网络应用之间的交互。例如，响应于确定，客户机应用可以允许第一来源处的第一实体的第一一个或多个网络应用经由嵌入式浏览器与第二来源处的第二实体的第二一个或多个网络应用进行交互。交互可以包括使用在客户机应用的嵌入式浏览器内执行的一个或多个网络应用来执行一个或多个任务。任务可以包括但不限于打印功能、在特定位置中(例如，在客户机装置上、在网络服务器上)存储数据或文件、下载功能、上传功能、摄像机功能、查看装置功能、拍照功能、获得签名功能和/或数字签名功能。例如，响应于确定，客户机应用可以允许第一来源的第一实体的第一网络应用经由客户机应用和嵌入式浏览器传输来自第二不同来源的第二不同实体的第二不同网络应用的数据。不同来源和/或不同实体的不同网络应用可以彼此协作并交互，从而为客户机装置的用户执行一个或多个任务。

[0212] 在一些实施例中，客户机应用的脚本引擎可以执行脚本以经由嵌入式浏览器在第一来源处的第一实体的第一一个或多个网络应用与第二来源处的第二实体的第二一个或多个网络应用之间进行交互。脚本引擎可以识别或生成应用脚本以执行客户机装置的用户所请求的任务。应用脚本可以对应于要执行的任务和/或执行所请求的任务的网络应用。应用脚本可以包括一个或多个指令或一系列命令。指令可以包括将被执行以进行一个或多个任务的一系列命令或代码。指令可以包括或识别要执行的任务、执行相应任务的一个或多个网络应用、相应的一个或多个网络应用的实体、相应的一个或多个网络应用的来源以及与该相应的网络应用、实体和/或来源相对应的策略。

[0213] 脚本引擎可以将应用脚本提供或应用到被识别为执行客户机装置的用户所请求的任务的网络应用。可以在客户机应用的嵌入式浏览器内执行第一实体和第一来源的第一一个或多个网络应用以及第二来源的第二实体的第二一个或多个网络应用。脚本引擎可以将应用脚本提供或应用到第一一个或多个网络应用以及第二一个或多个网络应用。脚本引擎可以利用第一一个或多个网络应用和/或第二一个或多个网络应用启动一个或多个应用脚本的执行。一个或多个应用脚本的执行顺序可以被包括在各个应用脚本的指令内和/或部分地基于要执行的任务。

[0214] 在一些实施例中，客户机应用可以响应于相同用户对第一一个或多个网络应用和第二一个或多个网络应用中的每一个的认证来允许进行交互。客户机应用可以认证客户机装置的用户。认证可以包括针对在客户机应用的嵌入式浏览器内执行的一个或多个网络应用来认证用户。客户机应用可以响应于用户的认证而与一个或多个网络应用建立一个或多个会话。客户机应用可以响应于客户机应用的嵌入式浏览器内的客户机装置的用户的认证来提供对与一个或多个网络应用的一个或多个会话的访问。可以响应于接收到客户机装置的用户的认证凭证来执行认证。客户机应用可以为用户访问或有权交互的网络应用建立一个或多个信任域。响应于建立信任域，客户机应用可以通过一个或多个信任域与用户访问或有权交互的网络应用建立会话。网络应用可以包括不同实体和/或不同来源的多个网络应用。客户机应用可以使用信任域在不同实体和/或不同来源的网络应用之间建立信任关

系。客户机应用可以为信任域建立访问策略。例如，在一些实施例中，对于客户机装置的用户用于访问信任域的访问策略。客户机应用可以使用信任域为客户机装置的用户执行一个或多个任务。例如，脚本引擎可以通过信任域内的第一一个或多个网络应用或第二一个或多个网络应用中的一个来启动应用脚本的执行。

[0215] 应当理解，上述系统可以提供那些组件中的任一个或每一个的多个组件，并且这些组件可以在独立的机器上或者在一些实施例中在分布式系统中的多个机器上提供。可以通过使用编程和/或工程技术来生产软件、固件、硬件或其任何组合，将上述系统和方法实现为方法、设备或制造产品。另外，可以将上述系统和方法作为嵌入在一个或多个制造产品之上或之中的一个或多个计算机可读程序来提供。本文所使用的术语“制造产品”旨在包括可从一个或多个计算机可读装置可访问的或嵌入其中的代码或逻辑、固件、可编程逻辑、存储装置(例如EEPROM、ROM、PROM、RAM、SRAM等)、硬件(例如集成电路芯片、现场可编程门阵列(FPGA)、专用集成电路(ASIC)等)、电子装置、计算机可读非易失性存储单元(例如CD-ROM、USB闪存、硬盘驱动器等)。可以从文件服务器访问该制造产品，该文件服务器经由网络传输线、无线传输介质、在空间传播的信号、无线电波、红外信号等提供对计算机可读程序的访问。该制造产品可以是闪存卡或磁带。该制造产品包括硬件逻辑以及嵌入在计算机可读介质中的由处理器执行的软件或可编程代码。通常，计算机可读程序可以以任何编程语言(例如LISP、PERL、C、C++、C#、PROLOG)或任何字节代码语言(例如JAVA)实现。软件程序可以作为目标代码存储在一个或多个制造产品之上或之中。

[0216] 尽管已经描述了方法和系统的各种实施例，但是这些实施例是示意性的，并且绝不限制所描述的方法或系统的范围。相关领域的技术人员可以在不脱离所描述的方法和系统的最广泛范围的情况下，对所描述的方法和系统的形式和细节进行改变。因此，本文描述的方法和系统的范围不应受到任何示意性实施例的限制，而应根据所附权利要求及其等同物来定义。

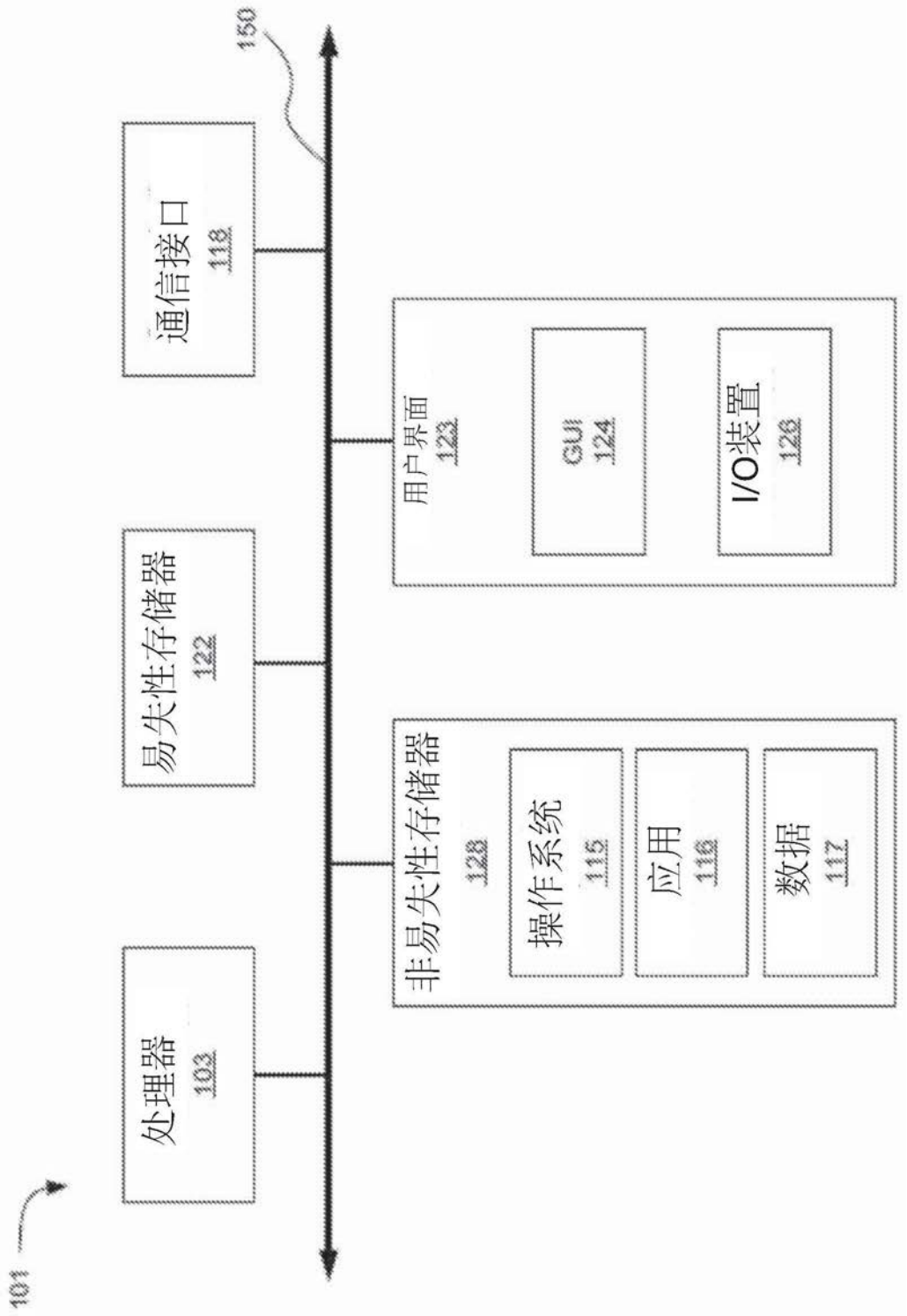

101
处理器
103
易失性存储器
122
通信接口
118
150
非易失性存储器
128
操作系统
115
应用
116
数据
117
用户界面
123
GUI
124
I/O装置
126

图1

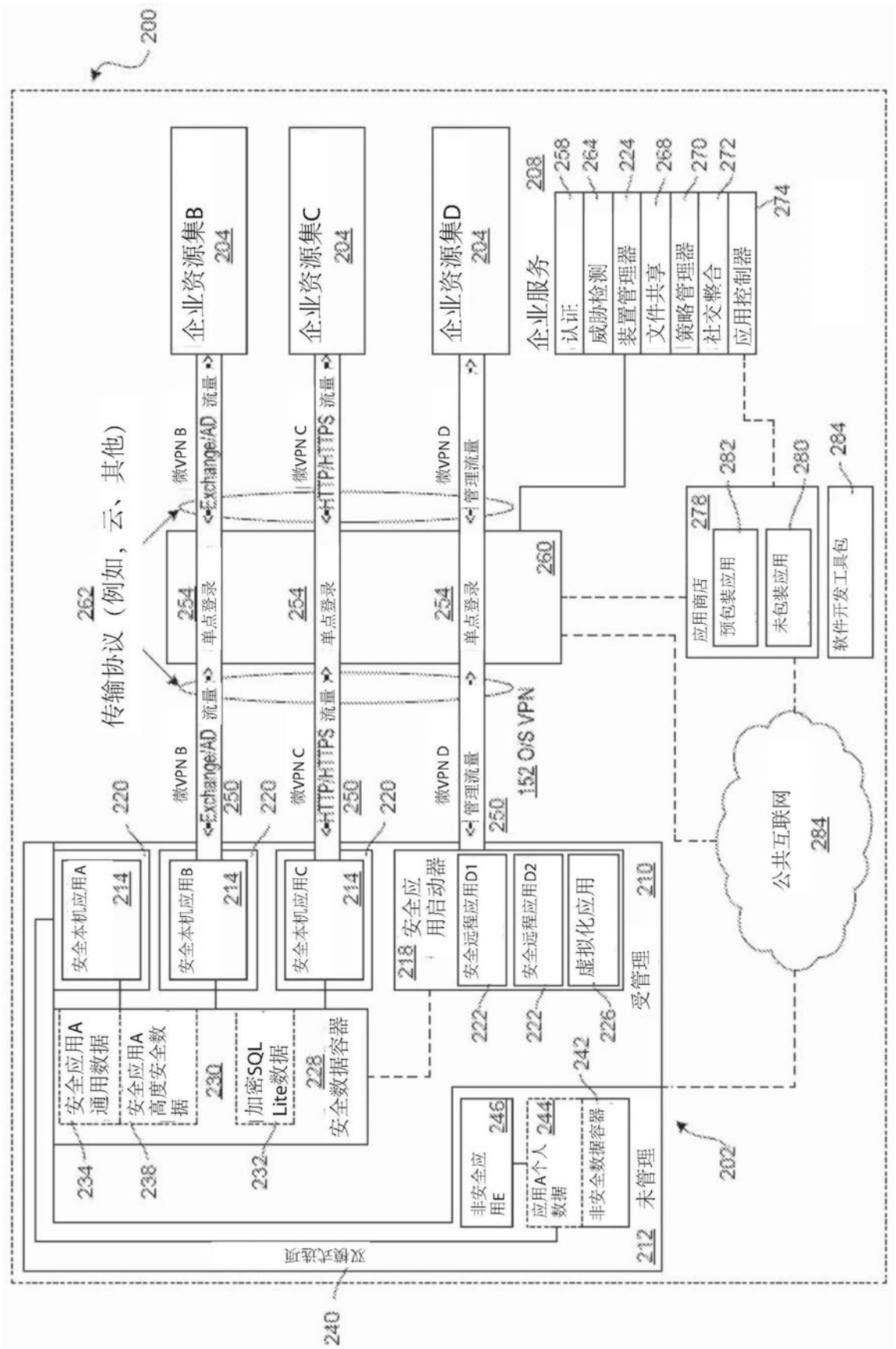

200
企业资源集B 204
企业资源集C 204
企业资源集D 204
企业服务 208
258 认证
264 威胁检测
224 装置管理器
268 文件共享
270 策略管理器
272 社交整合
274 应用控制器
262 传输协议（例如，云、其他）
微VPN B
微VPN C
微VPN D
Exchange/AD 流量
HTTP/HTTPS 流量
管理流量
254 单点登录
260
152 O/S VPN
250
220
应用商店 278
282 预包装应用
280 未包装应用
284 软件开发工具包
公共互联网 284
安全本机应用A 214
安全本机应用B 214
安全本机应用C 214
218 安全应用启动器
安全远程应用D1
安全远程应用D2
虚拟化应用
222
226
受管理 210
安全应用A通用数据 234
安全应用A高度安全数据 238
加密SQL Lite数据 232
230
228 安全数据容器
242
非安全应用E 246
应用A个人数据 244
非安全数据容器
未管理 212
202
高安全区域 240

图2

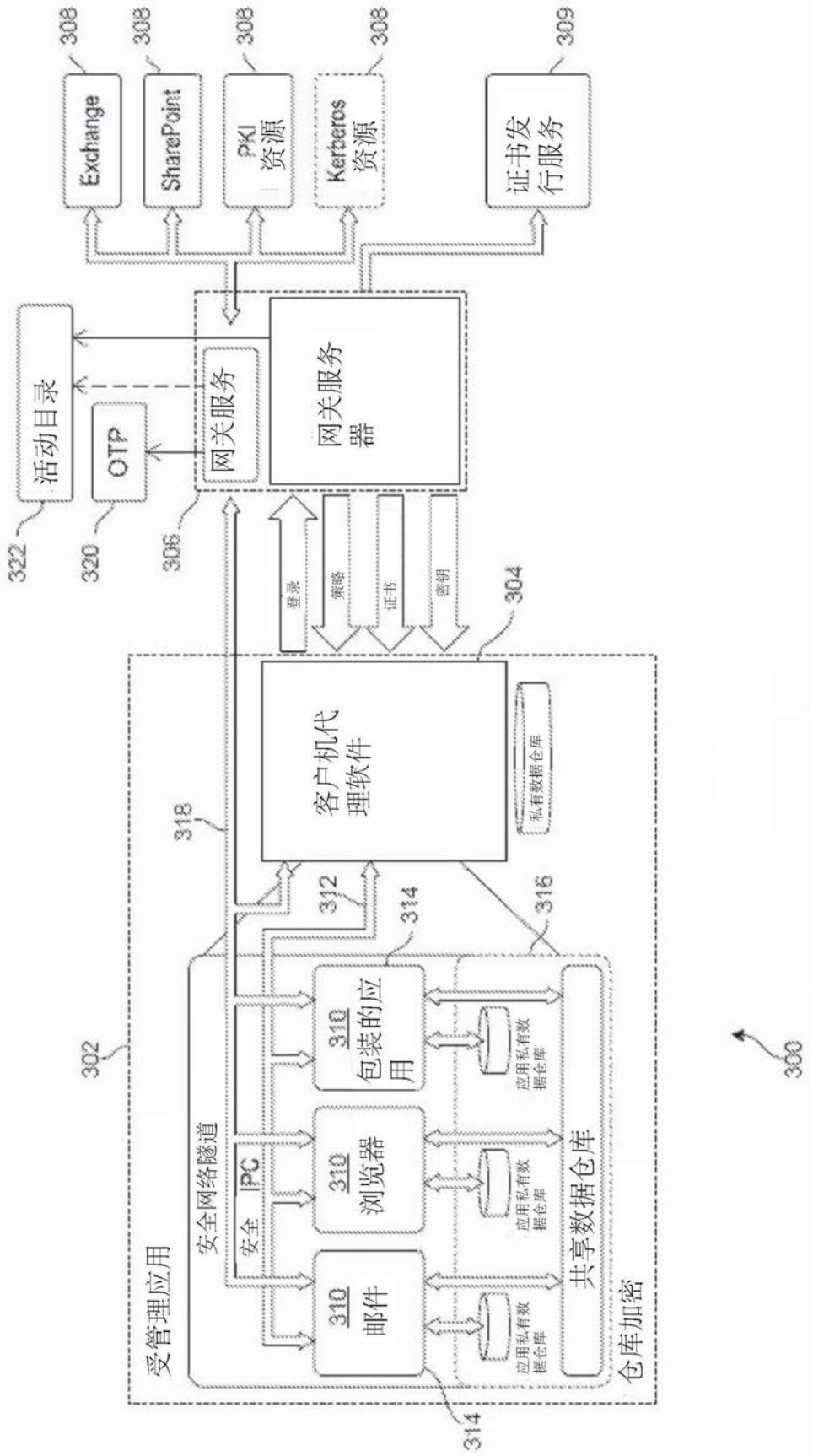

308
Exchange
308
SharePoint
308
PKI 资源
308
Kerberos 资源
309
证书发行服务
活动目录
OTP
网关服务
网关服务器
322
320
306
登录
策略
证书
密钥
304
客户机代理软件
私有数据仓库
318
312
314
316
302
安全网络隧道
安全
IPC
310 包装的应用
310 浏览器
310 邮件
应用私有数据仓库
共享数据仓库
仓库加密
314
300

图3

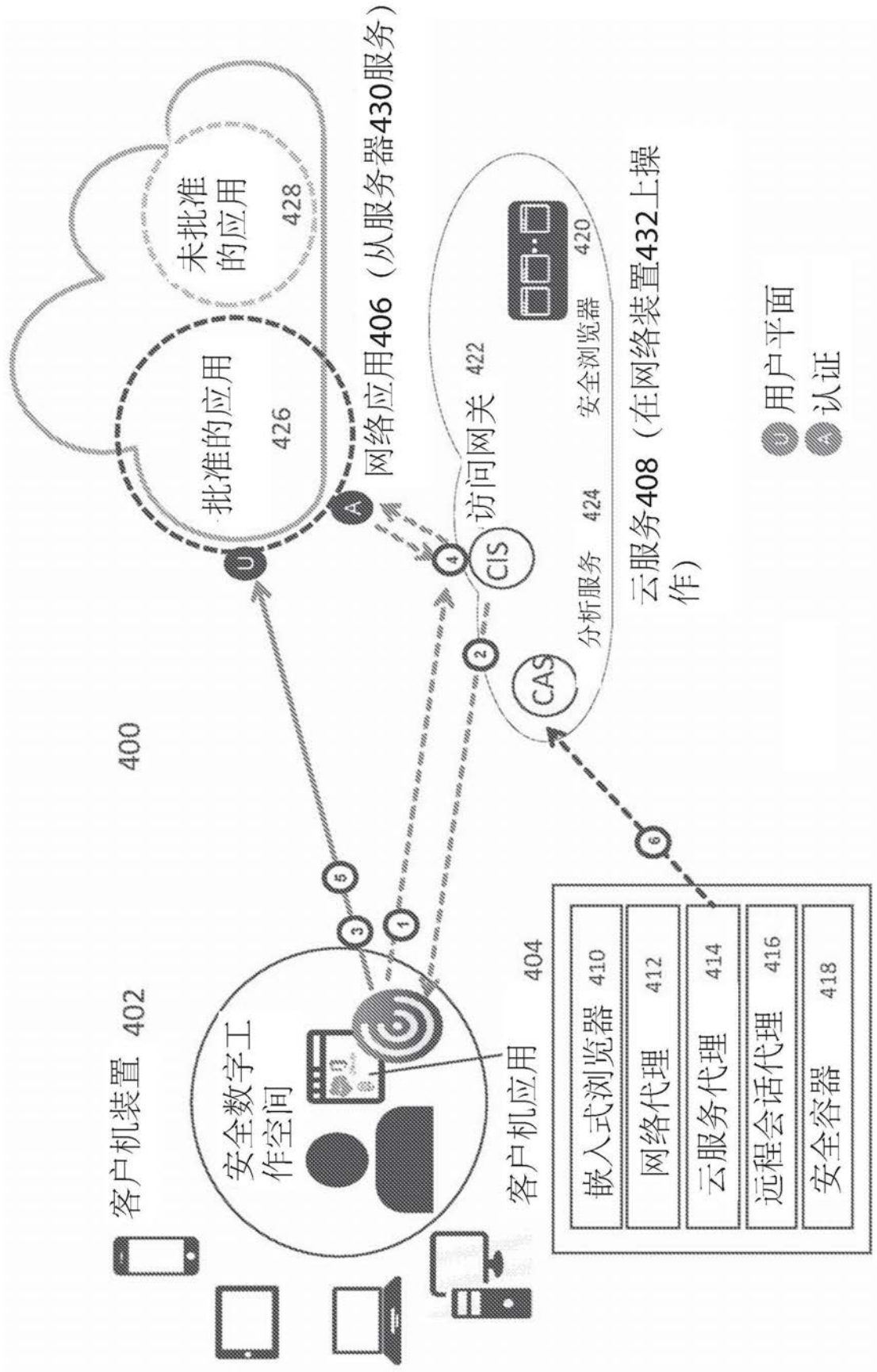

400
客户机装置 402
安全数字工作空间
客户机应用 404
嵌入式浏览器 410
网络代理 412
云服务代理 414
远程会话代理 416
安全容器 418
网络应用406（从服务器430服务）
批准的应用 426
未批准的应用 428
访问网关 422
CIS
CAS
分析服务 424
安全浏览器 420
云服务408（在网络装置432上操作）
用户平面
认证

图4

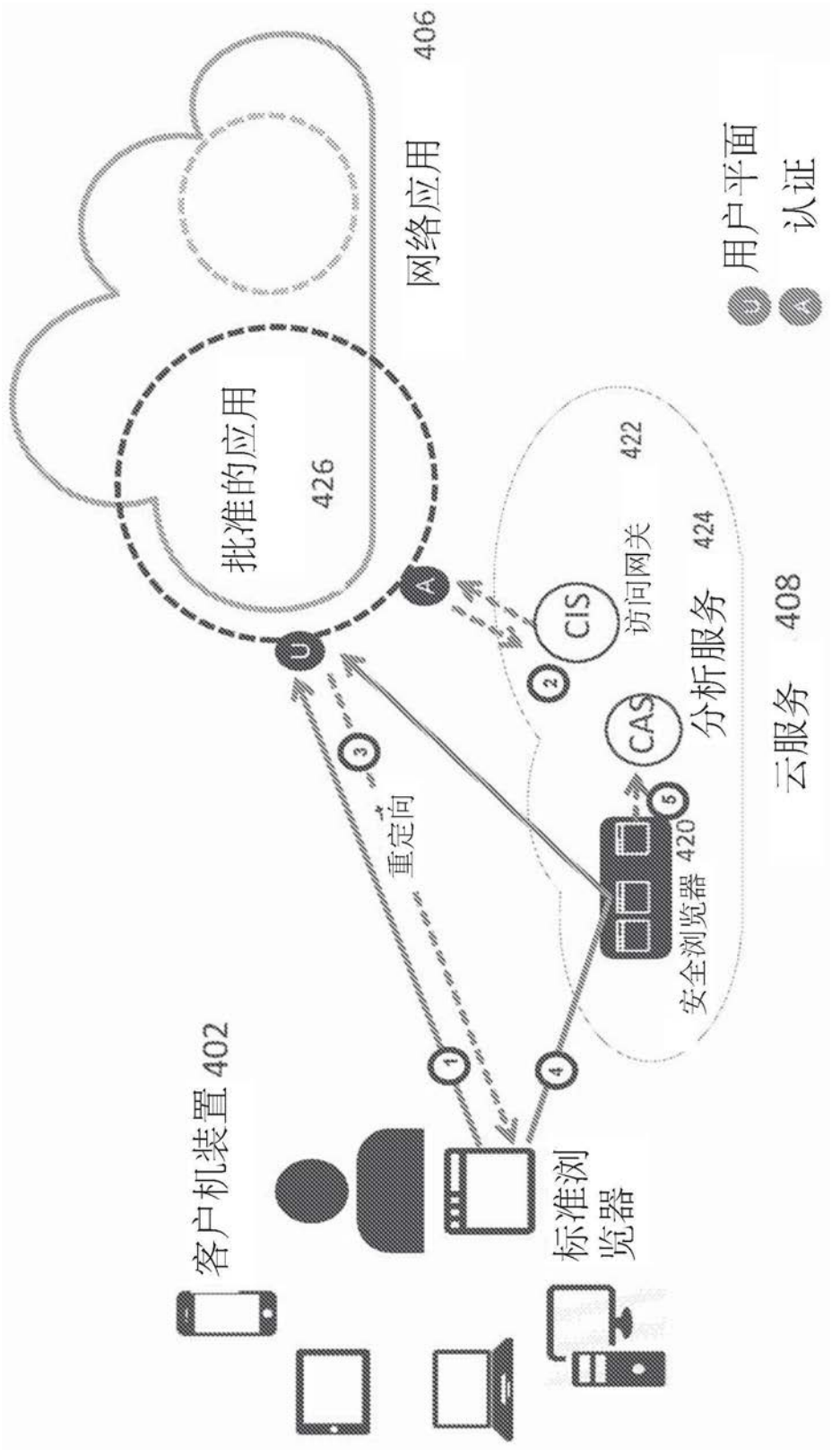

406
网络应用
用户平面
认证
批准的应用
426
422
CIS
访问网关
424
分析服务
CAS
重定向
安全浏览器 420
云服务 408
客户机装置 402
标准浏览器

图5

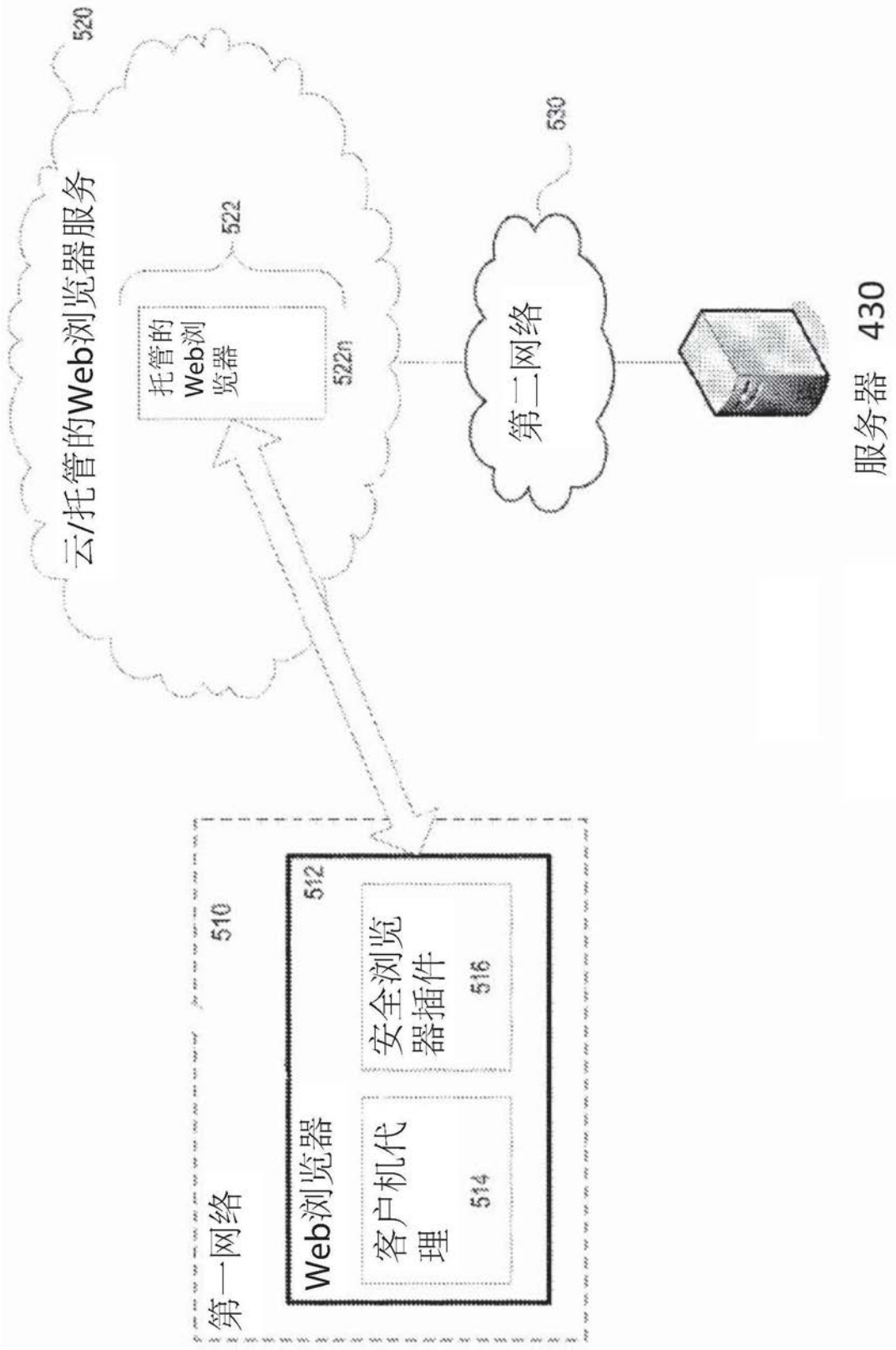

520
云/托管的Web浏览器服务
522
托管的Web浏览器
522n
530
第二网络
服务器 430
510
第一网络
512
Web浏览器
客户机代理
514
安全浏览器插件
516

图6

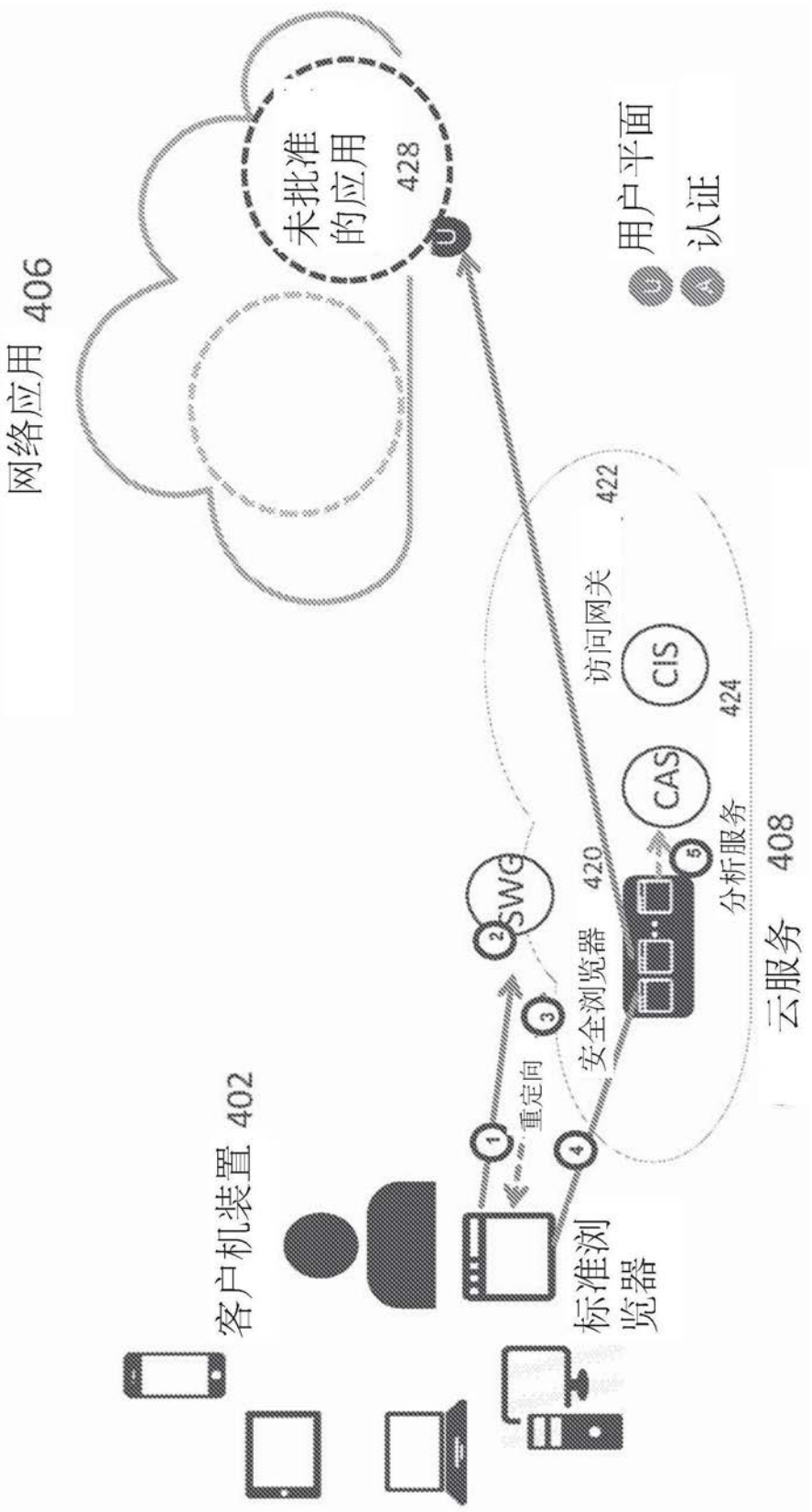

网络应用 406
未批准的应用 428
用户平面
认证
访问网关 422
CIS
CAS
分析服务 424
SWG
安全浏览器 420
重定向
客户机装置 402
标准浏览器
云服务 408

图7

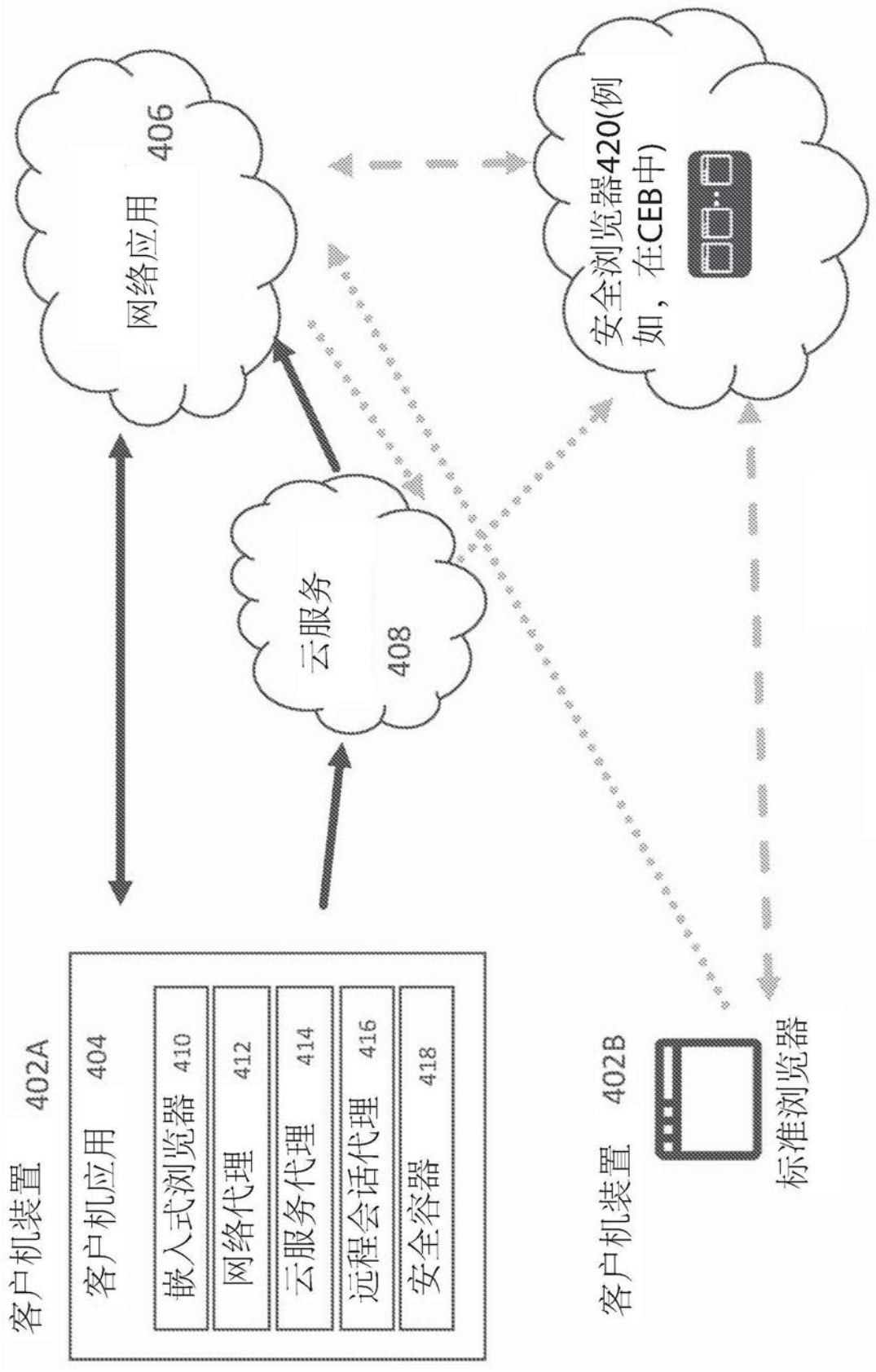

网络应用 406
安全浏览器420(例如，在CEB中)
云服务 408
客户机装置 402A
客户机应用 404
嵌入式浏览器 410
网络代理 412
云服务代理 414
远程会话代理 416
安全容器 418
客户机装置 402B
标准浏览器

图8

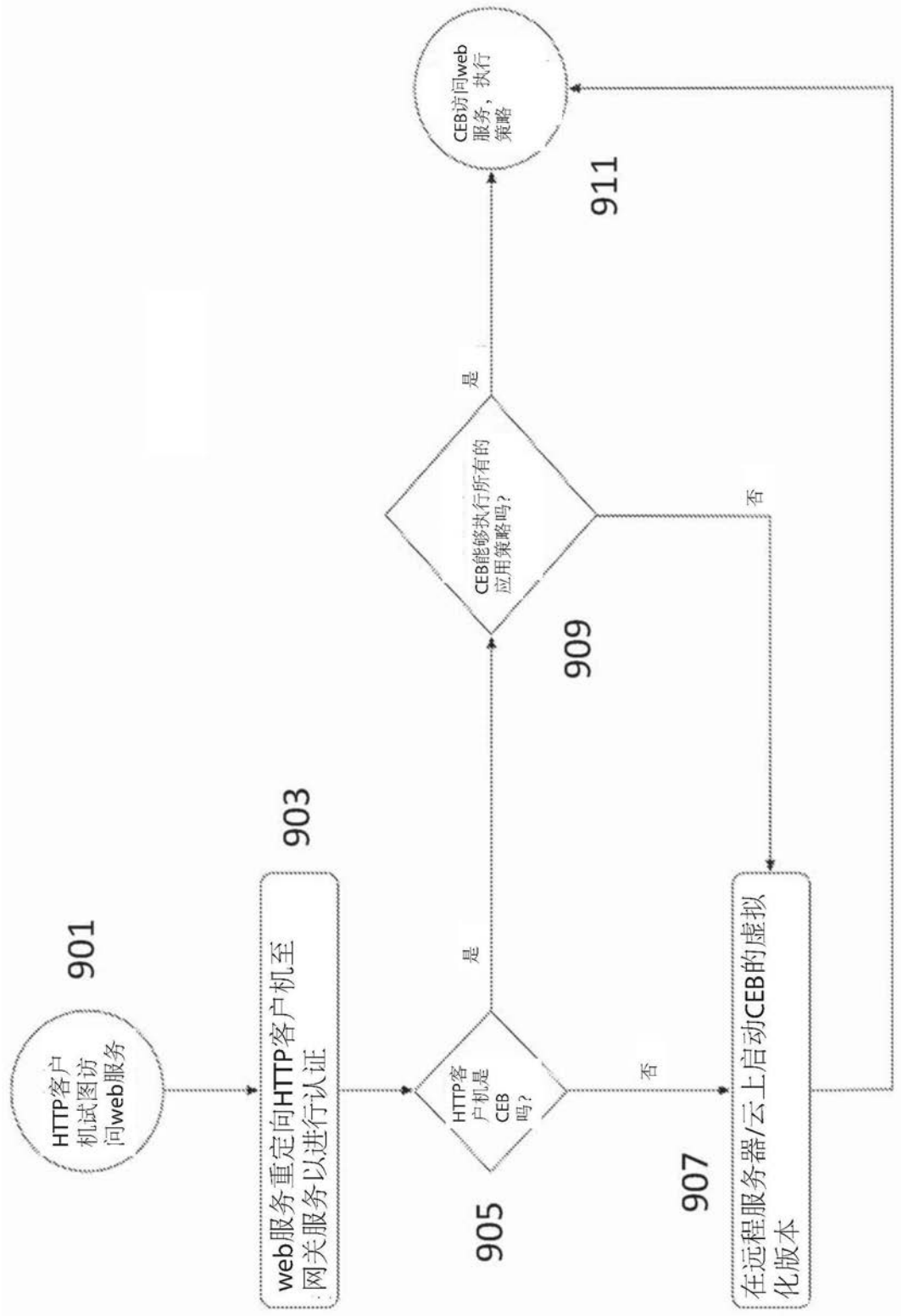

HTTP客户机试图访问web服务
901
web服务重定向HTTP客户机至网关服务以进行认证
903
HTTP客户机是CEB吗？
905
是
否
CEB能够执行所有的应用策略吗？
909
是
否
CEB访问web服务，执行策略
911
在远程服务器/云上启动CEB的虚拟化版本
907

图9

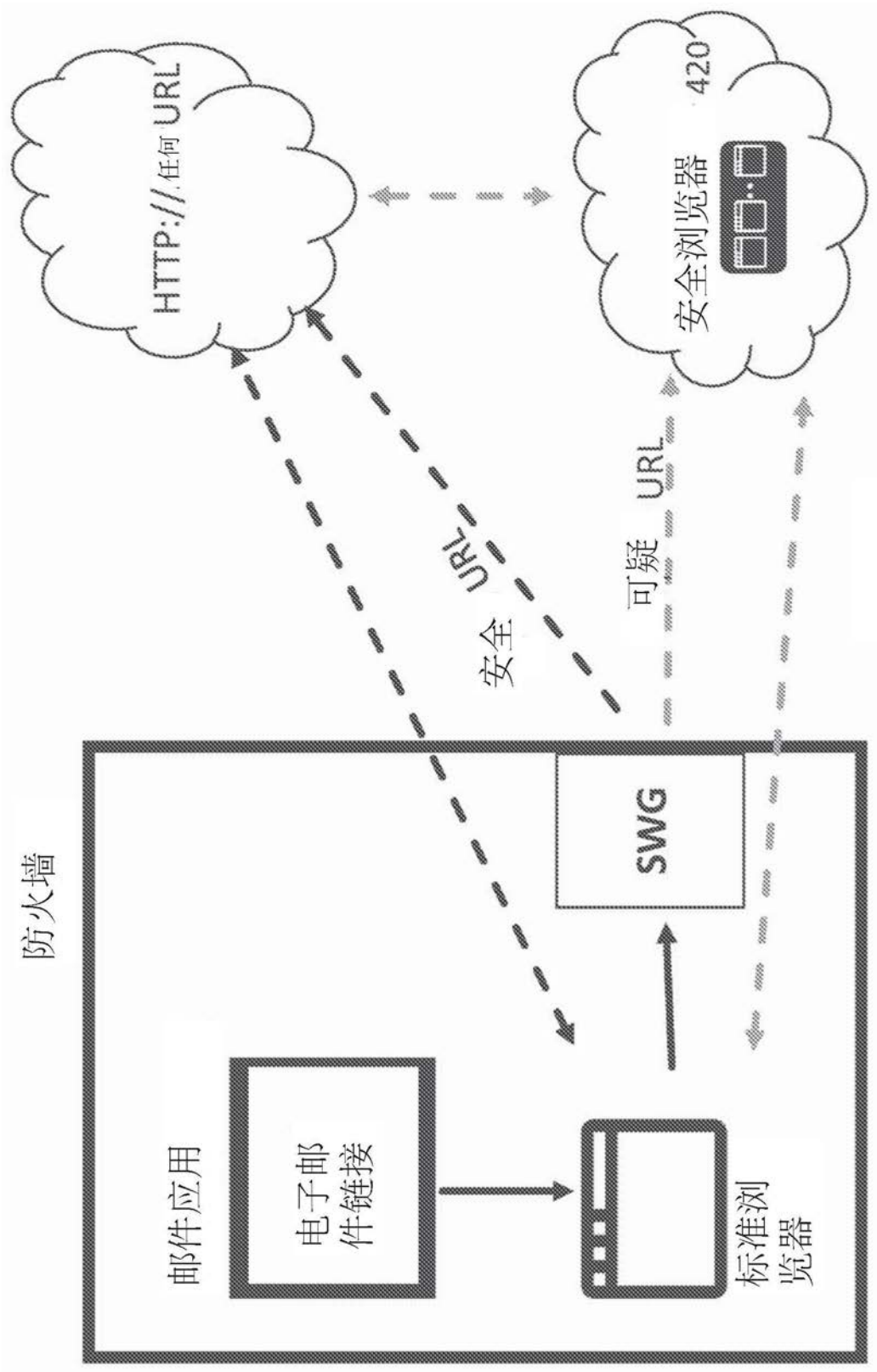


图10

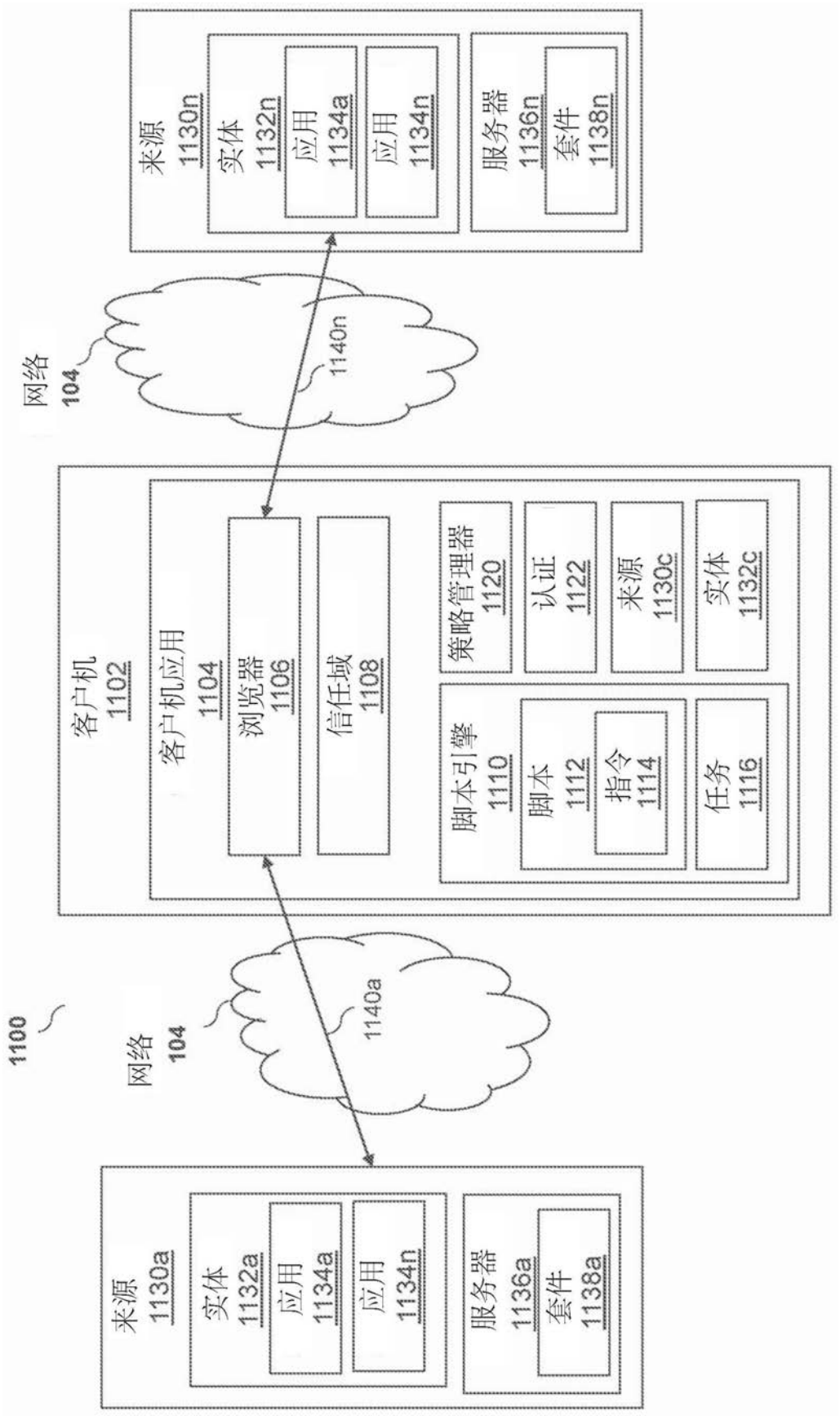

1100
网络
104
1140a
客户机
1102
客户机应用
1104
浏览器
1106
信任域
1108
脚本引擎
1110
脚本
1112
指令
1114
任务
1116
策略管理器
1120
认证
1122
来源
1130c
实体
1132c
来源
1130a
实体
1132a
应用
1134a
应用
1134n
服务器
1136a
套件
1138a
网络
104
1140n
来源
1130n
实体
1132n
应用
1134a
应用
1134n
服务器
1136n
套件
1138n

图11

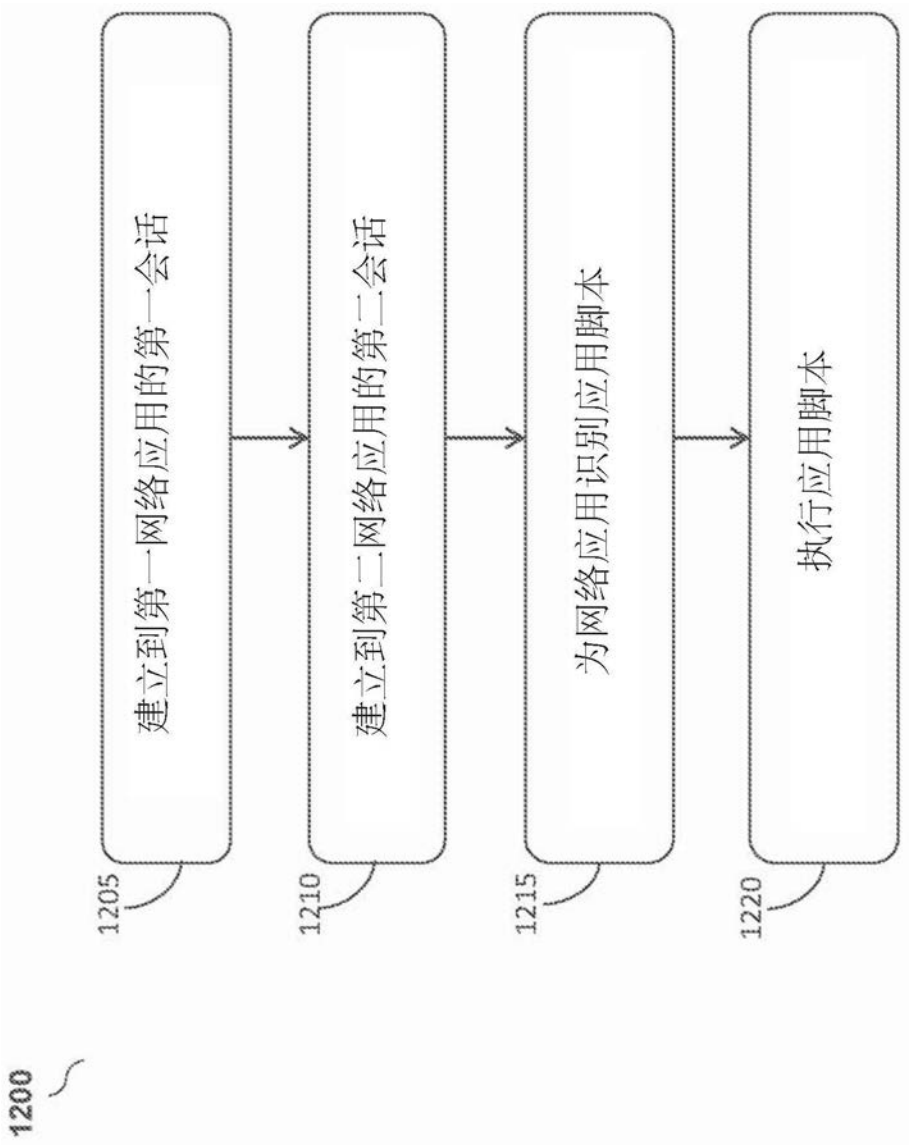

1200
1205
建立到第一网络应用的第一会话
1210
建立到第二网络应用的第二会话
1215
为网络应用识别应用脚本
1220
执行应用脚本

图12

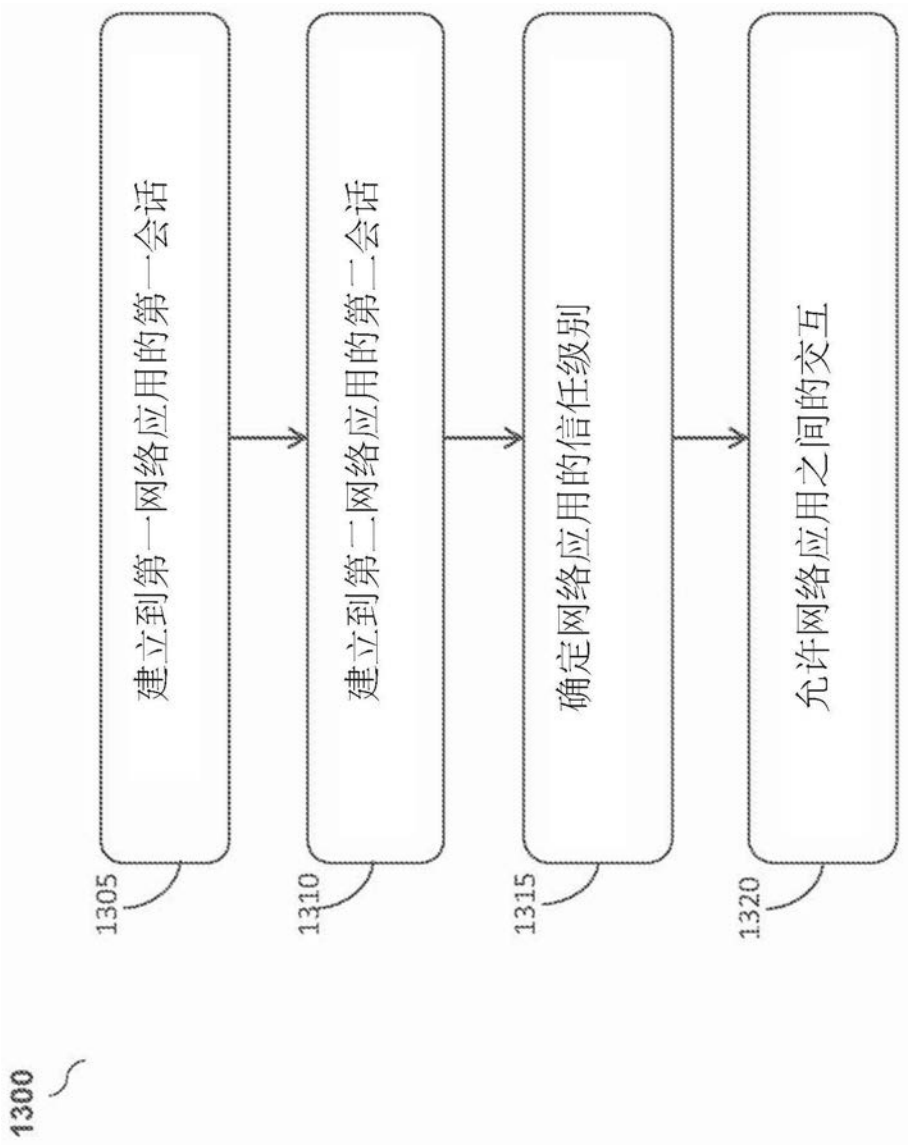

1300
1305
建立到第一网络应用的第一会话
1310
建立到第二网络应用的第二会话
1315
确定网络应用的信任级别
1320
允许网络应用之间的交互

图13