(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 107209701 B
(45)授权公告日 2020.12.15

(21)申请号 201680006089.X

(22)申请日 2016.01.19

(65)同一申请的已公布的文献号
申请公布号 CN 107209701 A

(43)申请公布日 2017.09.26

(30)优先权数据
62/105,685 2015.01.20 US
14/857,775 2015.09.17 US

(85)PCT国际申请进入国家阶段日
2017.07.17

(86)PCT国际申请的申请数据
PCT/US2016/013944 2016.01.19

(87)PCT国际申请的公布数据
WO2016/118518 EN 2016.07.28

(73)专利权人 赛姆普蒂夫技术公司
地址 美国华盛顿州

(72)发明人 罗伯特·派克

(74)专利代理机构 北京集佳知识产权代理有限公司 11227
代理人 唐京桥 陈炜

(51)Int.Cl.
G06F 11/00(2006.01)
G06F 12/14(2006.01)

(56)对比文件
US 2014108775 A1,2014.04.17
US 2014108775 A1,2014.04.17
US 2012209977 A1,2012.08.16
US 2008046982 A1,2008.02.21
CN 104133730 A,2014.11.05

审查员 于炘成

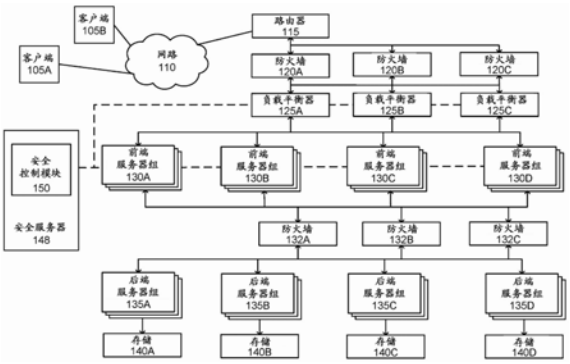
权利要求书3页 说明书11页 附图10页

(54)发明名称

滚动安全平台

(57)摘要

一种用于系统的滚动安全的方法，该系统包括多个服务器组，例如一个或多个服务器的第一服务器组以及一个或多个服务器的第二服务器组。该方法包括重复地启动一个或多个服务器的第一服务器组的重建。该方法还包括重复地启动一个或多个服务器的第二服务器组的重建。一个或多个服务器的第一服务器组的重建与一个或多个服务器的第二服务器组的重建在时间上交错。服务器可以是物理服务器或者虚拟服务器。滚动安全还可以应用于软件容器、数据中心内部的计算设备以及数据中心外部的计算设备。



CN 107209701 B

1.一种滚动安全系统,包括:

服务器的第一服务器组;

服务器的第二服务器组,所述第一服务器组和所述第二服务器组中的每个服务器包括软件,所述软件包括操作系统和支持用户会话的应用程序;以及

存储指令的非暂态计算机可读介质,当由至少一个处理器执行时,所述指令使所述至少一个处理器:

访问基于监测的在应用程序与客户端设备之间建立的先前用户会话的持续时间而生成的滚动时间信息,所述滚动时间信息指示所述第一服务器组的重建时间和所述第二服务器组的重建时间,所述第一服务器组的重建时间与所述第二服务器组的重建时间在时间上交错;

根据所述第一服务器组的重建时间周期性地启动服务器的第一服务器组中的每个服务器的软件的重建;以及

根据所述第二服务器组的第二重建时间周期性地启动服务器的第二服务器组中的每个服务器的软件的重建,服务器的第一服务器组的重建与服务器的第二服务器组的重建在时间上交错。

2.根据权利要求1所述的系统,其中,所述指令还使所述至少一个处理器:

监测所述先前用户会话的持续时间;以及

生成所述滚动时间信息。

3.一种非暂态计算机可读介质,其存储有用于实现系统的滚动安全的指令,所述系统包括服务器的第一服务器组和服务器的第二服务器组,所述第一服务器组和所述第二服务器组中的每个服务器包括软件,所述软件包括操作系统和支持用户会话的应用程序,当由至少一个处理器执行时,所述指令使所述至少一个处理器:

访问基于监测的在应用程序与客户端设备之间建立的先前用户会话的持续时间而生成的滚动时间信息,所述滚动时间信息指示用于重建所述第一服务器组的第一重建时间和用于重建所述第二服务器组的第二重建时间,所述第一重建时间与所述第二重建时间在时间上交错;

根据所述第一重建时间周期性地启动服务器的第一服务器组的重建;以及

根据所述第二重建时间周期性地启动服务器的第二服务器组的重建,服务器的第一服务器组的重建与服务器的第二服务器组的重建在时间上交错。

4.根据权利要求3所述的非暂态计算机可读介质,其中,

周期性地启动所述第一服务器组的重建包括启动所述第一服务器组中的每个服务器的软件的重建;以及

周期性地启动所述第二服务器组的重建包括启动所述第二服务器组中的每个服务器的软件的重建。

5.根据权利要求3所述的非暂态计算机可读介质,其中,

周期性地启动所述第一服务器组的重建包括启动所述第一服务器组中的每个服务器的固件的重建;以及

周期性地启动所述第二服务器组的重建包括启动所述第二服务器组中的每个服务器的固件的重建。

6.根据权利要求3所述的非暂态计算机可读介质,其中,所述指令能够被执行以:

当重建所述第一服务器组时,周期性地启动所述第一服务器组中的每个服务器的密码更改;以及

当重建所述第二服务器组时,周期性地启动所述第二服务器组中的每个服务器的密码更改。

7.根据权利要求3所述的非暂态计算机可读介质,所述指令还使所述至少一个处理器:

监测所述先前用户会话的持续时间;以及

生成所述滚动时间信息。

8.根据权利要求3所述的非暂态计算机可读介质,其中,被周期性地重建的所述第一服务器组和所述第二服务器组中的服务器是物理服务器。

9.根据权利要求3所述的非暂态计算机可读介质,其中,被周期性地重建的所述第一服务器组和所述第二服务器组中的服务器是虚拟机。

10.根据权利要求3所述的非暂态计算机可读介质,其中,所述系统还包括在所述第一服务器组和所述第二服务器组之间平衡网络流量的一个或多个负载平衡器,并且所述指令使所述至少一个处理器:

在所述第一服务器组的每次重建之前周期性地启动所述第一服务器组的关闭准备模式,所述负载平衡器防止当所述第一服务器组处于关闭准备模式时与所述第一服务器组的应用程序建立新的会话;以及

在所述第二服务器组的每次重建之前周期性地启动所述第二服务器组的关闭准备模式,所述负载平衡器防止当所述第二服务器组处于关闭准备模式时与所述第二服务器组的应用程序建立新的会话。

11.一种用于系统的滚动安全的计算机实现的方法,所述系统包括服务器的第一服务器组和服务器的第二服务器组,所述第一服务器组和所述第二服务器组中的每个服务器包括软件,所述软件包括操作系统和支持用户会话的应用程序,所述方法包括:

访问基于监测的在应用程序与客户端设备之间建立的先前用户会话的持续时间而生成的滚动时间信息,所述滚动时间信息指示用于重建所述第一服务器组的第一重建时间和用于重建所述第二服务器组的第二重建时间,所述第一重建时间与所述第二重建时间在时间上交错;

根据所述第一重建时间周期性地启动一个或多个服务器的第一服务器组的重建;以及

根据所述第二重建时间周期性地启动一个或多个服务器的第二服务器组的重建,所述第一服务器组的重建与所述第二服务器组的重建在时间上交错。

12.根据权利要求11所述的方法,其中,

周期性地启动所述第一服务器组的重建包括启动所述第一服务器组中的每个服务器的软件的重建;以及

周期性地启动所述第二服务器组的重建包括启动所述第二服务器组中的每个服务器的软件的重建。

13.根据权利要求11所述的方法,其中,

周期性地启动所述第一服务器组的重建包括启动所述第一服务器组中的每个服务器的固件的重建;以及

周期性地启动所述第二服务器组的重建包括启动所述第二服务器组中的每个服务器的固件的重建。

14.根据权利要求11所述的方法,还包括:

当重建所述第一服务器组时,周期性地启动所述第一服务器组中的每个服务器的密码更改;以及

当重建所述第二服务器组时,周期性地启动所述第二服务器组中的每个服务器的密码更改。

15.根据权利要求11所述的方法,还包括:

监测所述先前用户会话的持续时间;以及

生成所述滚动时间信息。

16.一种非暂态计算机可读介质,其存储有用于实现系统的滚动安全的指令,所述系统包括第一软件容器组和第二软件容器组,所述第一软件容器组和所述第二软件容器组中的每个软件容器包括软件,所述软件包括操作系统和支持用户会话的应用程序,当由至少一个处理器执行时,所述指令使所述至少一个处理器:

访问基于监测的在应用程序与客户端设备之间建立的先前用户会话的持续时间而生成的滚动时间信息,所述滚动时间信息指示用于重建所述第一软件容器组的第一重建时间和用于重建所述第二软件容器组的第二重建时间,所述第一重建时间与所述第二重建时间在时间上交错;

根据所述第一重建时间周期性地启动所述第一软件容器组的重建;以及

根据所述第二重建时间周期性地启动所述第二软件容器组的重建,所述第一软件容器组的重建与所述第二软件容器组的重建在时间上交错。

17.一种用于实现系统的滚动安全的方法,所述系统包括第一软件容器组和第二软件容器组,所述第一软件容器组和所述第二软件容器组中的每个软件容器包括软件,所述软件包括操作系统和支持用户会话的应用程序,所述方法包括:

访问基于监测的在应用程序与客户端设备之间建立的先前用户会话的持续时间而生成的滚动时间信息,所述滚动时间信息指示用于重建所述第一软件容器组的第一重建时间和用于重建所述第二软件容器组的第二重建时间的,所述第一重建时间与所述第二重建时间在时间上交错;

根据所述第一重建时间周期性地启动所述第一软件容器组的重建;以及

根据所述第二重建时间周期性地启动所述第二软件容器组的重建,所述第一软件容器组的重建与所述第二软件容器组的重建在时间上交错。

滚动安全平台

[0001] 相关领域的交叉引用

[0002] 本申请要求2015年1月20号提交的美国临时专利申请第62/105,685号以及2015年9月17号提交的美国专利申请第14/857,775的优先权,其全部内容通过引用被合并到本文中。

背景技术

1.技术领域

[0003] 本公开内容涉及防御对资源的未授权访问的计算机安全,并且更具体地涉及安全性增加的滚动安全平台。

[0004] 2.相关领域的描述

[0005] 在网络通信中,存在很多形式的软件安全和硬件安全,包括防火墙和入侵检测和防止系统。但他们都会在一个核心问题上出问题,即如果没有正确地应用规则,则他们会提供未授权访问的机会。现今操作系统和应用程序也具有很多缺陷,如果这些缺陷暴露于因特网,则可能允许远程访问托管这些应用程序的服务器。

发明内容

[0006] 本公开内容的实施方式包括提供防止黑客的在线安全的智能方法和系统。在一个实施方式中,公开了滚动安全系统。该系统包括服务器的第一服务器组和服务器的第二服务器组。第一服务器组和第二服务器组中的每个服务器包括软件,该软件包括操作系统和支持用户会话的应用程序。非暂态计算机可读介质存储指令,当由至少一个处理器执行时,所述指令使得至少一个处理器访问指示第一服务器组的重建计时和第二服务器组的重建计时的滚动计时信息。第一服务器的滚动计时与第二服务器组的滚动计时在时间上交错。所述指令还使处理器根据第一服务器组的重建计时周期性地启动服务器的第一服务器组中的每个服务器的软件的重建。所述指令还使处理器根据第二服务器组的第二重建计时周期性地启动服务器的第二服务器组中的每个服务器的软件的重建。服务器的第一服务器组的重建与服务器的第二服务器组的重建在时间上交错。

[0007] 在一个实施方式中,公开了用于包括多个服务器组的系统的滚动安全的方法。该方法包括重复地启动一个或多个服务器的第一服务器组的重建。该方法还包括重复地启动一个或多个服务器的第二服务器组的重建。一个或多个服务器的第一服务器组的重建与一个或多个服务器的第二服务器组的重建在时间上交错。

[0008] 在一个实施方式中,第一组和第二组中的每个服务器包括软件,所述软件重复地被重建,例如周期性地被重建。重建的软件可以包括操作系统、应用程序和其他软件。在一个实施方式中,第一服务器组和第二服务器中的每个服务器包括相应的固件。重复地启动第一服务器组的重建包括启动第一服务器组中的每个服务器的相应固件的重建。重复地启动第二服务器组的重建包括启动第二服务器组中的每个服务器的相应固件的重建。

[0009] 在一个实施方式中，第一服务器组和第二服务器组中的每个服务器包括相应的密码。该方法还包括：当重建第一服务器组时重复地启动第一服务器组中的每个服务器的密码更改；以及当重建第二服务器组时重复地启动第二服务器组中的每个服务器的密码更改。

[0010] 在一个实施方式中，该方法包括访问指示用于重建第一服务器组和第二服务器组的重建计时的滚动时间信息。第一服务器组和第二服务器组根据该滚动时间信息重复地被重建。另外，第一服务器组和第二服务器组中的每个服务器托管相应的应用程序并且支持应用程序的用户会话，并且该方法还包括监测相应的应用程序的用户会话的持续时间；以及基于监测的用户会话的持续时间生成指示第一服务器组和第二服务器组的重建时间的滚动时间信息。

[0011] 在一个实施方式中，被重复地重建的第一服务器组和第二服务器组中的服务器是物理服务器。在一个实施方式中，被重复地重建的第一服务器组和第二服务器组中的服务器是虚拟服务器。

[0012] 在一个实施方式中，该系统还包括用于在第一服务器组和第二服务器组之间平衡网络流量的一个或多个负载平衡器。该方法还包括：在第一服务器组的每次重建之前重复地启动第一服务器组的关闭准备模式，负载平衡器防止当第一服务器组处于关闭准备模式时与第一服务器组的应用程序建立新的会话。该方法还包括：在第二服务器组的每次重建之前重复地启动第二服务器组的关闭准备模式，负载平衡器防止当第二服务器组处于关闭准备模式时与第二服务器组的应用程序建立新的会话。

[0013] 其他实施方式包括存储指令的非暂态计算机可读介质。所述指令能够被至少一个处理器执行以使所述至少一个处理器执行用于滚动安全的方法。其他实施方式可以将滚动安全应用于软件容器。其他实施方式可以将滚动安全应用于数据中心内部的网络计算设备或者数据中心外部的计算设备。

附图说明

[0014] 图1A是根据一个实施方式的具有适合于滚动安全的安全数据中心的部件的网络通信系统的框图。

[0015] 图1B是根据另一个实施方式的具有适合于滚动安全的安全数据中心的部件的网络通信系统的框图。

[0016] 图1C是根据又一个实施方式的具有适合于滚动安全的安全数据中心的部件的网络通信系统的框图。

[0017] 图2A是根据一个实施方式的图1A的前端服务器的框图。

[0018] 图2B是根据一个实施方式的具有虚拟机的服务器的框图。

[0019] 图2C是根据一个实施方式的具有软件容器的服务器的框图。

[0020] 图3是根据一个实施方式的滚动服务器组的图。

[0021] 图4是根据一个实施方式的安全控制模块的框图。

[0022] 图5是根据一个实施方式的用于滚动安全的方法的流程图。

[0023] 图6示出了计算设备的硬件体系结构。

具体实施方式

[0024] 现在将详细地参照本公开内容的几个实施方式，在附图中示出了这些实施方式的示例。应当注意，在可行的情况下，可以在附图中使用类似或相似的附图标记，并且这些类似或相似的附图标记可以指示类似或相似的功能。仅出于说明的目的，附图描述了本公开内容的实施方式。本领域技术人员将从下面的描述中容易地认识到，在不偏离本文所描述的公开内容的原理或优点的情况下，可以采用本文所示出的结构和方法的替代实施方式。

[0025] 本公开内容涉及一种防止黑客获得对后端数据集的访问并防止对任何数据集的持续访问的系统平台。更具体地，本发明可以停止升级对未授权资源的访问，得到更高安全性的方案。

[0026] 在一个实施方式中，公开了一种数据中心的安全平台。安全平台根据具体的时间指标以滚动的方式不断重复重建自身。滚动安全将在短时间内自动替换服务器软件，以完全消除在操作系统或应用程序中发现的任何配置或漏洞，从而将对任何服务器的访问限于短时间。例如，这个时间可以短至10秒钟或长达几小时。在一个实施方式中，标准配置将在重建之间默认为10分钟。黑客将具有这样一个短暂的窗口，在该短暂的窗口中学习攻击、弄清后台的体系架构是什么、损害服务器、并尝试安装根工具包来进一步访问。因此，黑客尝试完成其攻击是毫无意义的，因为服务器的替换经常发生。当黑客发现密码或公共密钥基础设施(PKI)密钥时，操作系统(OS)连同新的密码和密钥被替换。

[0027] 系统可以但不限于在短时间内替换设备上的整个软件堆栈，包括OS、应用程序、内容、数据和缓存。该系统可以与网络中的多个设备(例如负载平衡器、防火墙等)完全集成，以无缝地管理真实用户和黑客用户两者。在其他实施方式中，可以使用会话计数、连接计数、唯一传感器触发器和其他安全指示来触发重建。在其他实施方式中，可以将会话动态地包含在隔离环境中，并且可以扩展会话的时间以在隔离环境中了解正在进行的攻击。

[0028] 系统可以动态地学习应用程序平均会话计数器和时间，并动态地调整重建时间或者进行手动配置以实现更严格的安全策略。系统限制了任何单个会话可以连接至前端应用程序和数据集的时间，以防止长期远程访问任何系统。

[0029] 图1A是根据一个实施方式的具有适合于滚动安全的安全数据中心的部件的网络通信系统的框图。该系统包括若干客户端设备105、网络110、路由器115、前端防火墙120A至120C、负载平衡器125A至125C、前端服务器组130A至130D、后端防火墙或负载平衡器132A至132C、后端服务器组135A至135D、存储系统140A至140D以及安全服务器148。路由器、防火墙120、负载平衡器125、前端服务器130、防火墙132、后端服务器135和存储系统140可以是数据中心的部件。在图1A中仅示出了有限数量的设备，但是在其他实施方式中，可以具有更多数量的设备(例如大于四个前端服务器组)。

[0030] 客户端设备105可以是计算设备，例如智能电话、平板电脑、笔记本电脑和台式计算机等。用户通过诸如触摸屏或鼠标和键盘的接口与客户端设备105的软件进行交互。客户端设备105由用户控制以建立与由前端服务器组130托管的各种应用程序的应用程序会话和连接。

[0031] 路由器115在网络110和数据中心的其余部件之间路由网络流量。前端防火墙120是基于硬件的防火墙设备，其使用所应用的规则集来控制输入(incoming)网络流量和输出(outgoing)网络流量。防火墙建立外部网络110与数据中心的内部网络之间的障碍。负载平

衡器125在大量前端服务器组130之间分配网络流量。负载平衡器通过减少任一个特定的前端服务器组130上的负载来增加应用程序的容量和可靠性。

[0032] 每个前端服务器组130包括若干物理前端服务器。服务器是可以包括一个或多个处理器并执行操作系统的服务器类计算设备。一台服务器托管若干软件应用程序。客户端105可以与由前端服务器托管的应用程序建立网络连接和应用程序会话。为了安全起见，每个服务器组可以在一段时间到期后滚动(即通过重建服务器组)，并且服务器组可以以交错方式滚动。相同应用程序的副本由多个服务器组130托管，使得即使服务器组滚动，应用程序仍然对客户端设备105可用。在一个实施方式中，共有九个前端服务器组130，并且每个前端服务器组130包括数千个前端服务器。

[0033] 后端防火墙132是基于硬件的防火墙设备或虚拟防火墙，其使用所应用的规则集来控制前端服务器组130和后端服务器组135之间的流量。每个后端服务器组135包括一个或多个后端服务器。后端服务器允许访问存储在存储系统140中的数据。后端服务器应由前端服务器组130托管的应用程序的请求，存储数据和取回来自存储系统140的数据。后端服务器的示例是提供对SQL数据库的访问的SQL服务器。

[0034] 安全服务器148包括协调前端服务器组130的滚动操作的安全控制模块150。具体地，安全控制模块150以周期性的和交错的间隔重复地启动前端服务器组130的重建。重建服务器可以包括通过用已知良好的替换镜像替换服务器的硬盘驱动器镜像来替换服务器的整个软件栈，包括操作系统(OS)、应用程序、内容、数据和缓存。重建服务器还可以包括替换服务器的固件。除了这些操作之外，重建还可以包括其他操作。重建之间的时间可以短至10秒或长达几小时。在其他实施方式中，标准的重建时间将默认为10分钟。

[0035] 周期性和频繁地重复重建服务器迫使黑客在短时间内(例如5秒以下)完成其攻击，这几乎不可能，因为响应时间和加载时间通常要求更大的时间量。例如，对于DNS服务器，可以使用新的OS和DNS数据库缓存每10秒重建DNS服务器。在这种情况下，黑客不会有时间破解(hack)协议并通过缓存欺骗加载虚假数据。黑客加载的任何恶意代码也将被删除。绑定到服务器的一切将被替换，从而不可能从外部远程访问OS。同时，标准的客户请求所需要的所有内容都可以正确地被提供。这完全解决了当今软件中发现的任何漏洞。

[0036] 安全控制模块150还通过在时间上相对于其他前端服务器组(例如，130B)使每个前端服务器组(例如130A)的重建交错来滚动地启动重建。当服务器组130开始工作并开始服务于流量时，每个前端服务器组130将在不同时间开始服务于用户会话，从而创建一个交错的方法。会话开始和结束的过程全部发生在单个服务器或服务器组130内。这允许在组内进行简单的负载平衡，但也允许在组内发生会话的终止。服务器组130内的服务器将在其他服务器组130刚刚开始工作并服务于新的用户会话的同时替换其OS。重建服务器组130的时帧可以根据服务器组130中的应用程序的功能而变化。

[0037] 安全控制模块150还与负载平衡器125通信，使得负载平衡器125知道服务器组正在关闭以进行新的OS安装，从而允许负载平衡器125将网络流量仅分配给在线的服务器组130。安全控制模块150可以向负载平衡器125发送信息，以指示服务器组130何时开始准备关闭。作为响应，负载平衡器125使服务器组130脱机，并阻止与服务器组130建立新的连接。一旦服务器组130被重建，安全控制模块150可以向负载平衡器125发送指示服务器组130准备好接受新的连接的信息。作为响应，负载平衡器125使服务器组130重新在线，并允许与服

务器组130建立新的连接。

[0038] 当重建服务器组130时，安全控制模块150还可以更改服务器组130的密码。频繁的密码更改使得不可能对服务器进行密码攻击。

[0039] 安全控制模块150可以被实现为软件、硬件或硬件和软件的组合。在其他实施方式中，除了安全服务器148之外，安全控制模块150可以分布在数据中心的一个或多个部件之间。

[0040] 图1B是根据另一个实施方式的具有适合于滚动安全的安全数据中心的部件的网络通信系统的框图。除了现在包括前端虚拟机(VM)组160和管理程序(hypervisor)190之外，图1B类似于图1A。每个VM组160包括一个或多个VM。VM是对计算机系统的仿真，例如对计算机服务器的仿真。每个VM可以附接至其自己的虚拟磁盘。在本文中虚拟机可以被称为虚拟服务器。

[0041] 管理程序190创建和管理VM组160。每个管理程序190可以位于其自己的物理前端服务器159上，并且还控制位于同一物理前端服务器上的一组VM 160。例如，管理程序190A和VM组160A位于单个物理服务器159A上。

[0042] 在该实施方式中，安全控制模块150通过周期性地启动前端VM组160(即虚拟服务器组)的重建向网络通信系统提供滚动安全。同一应用程序的副本由多个VM组160托管，使得即使正在重建VM组160时应用程序也始终在线。重建VM可以包括将VM的状态恢复成原始已知的良好状态。将在下面进行更详细地说明重建。

[0043] 另外，安全控制模块150的操作与结合图1B描述的操作相同。在一个实施方式中，网络通信系统可以包括周期地和交错地重建的物理服务器组和虚拟服务器组。

[0044] 图1C是根据又一个实施方式的具有适合于滚动安全的安全数据中心的部件的网络通信系统的框图。除了现在包括位于服务器159上的容器组960和容器引擎990之外，图1C类似于图1B。

[0045] 每个容器组960包括用于OS级虚拟化的一个或多个软件容器。软件容器包括应用程序，其依赖关系、库和二进制文件捆绑在一个包中。软件容器与同一服务器159上的其他软件容器共享OS(未示出)。软件容器在操作系统的内核中被实例化并使应用程序的实例虚拟化。软件容器允许快速创建要放入一个资源块中的应用程序或服务。容器的部署很快，因为容器可以从核心OS共享核心库文件。软件容器由容器引擎990管理。在一个实施方式中，软件容器960是DOCKER容器或者符合开放容器项目标准。

[0046] 在该实施方式中，安全控制模块150通过滚动地、周期性地启动容器组960的重建来向网络通信系统提供滚动安全。同一应用程序的副本被包含在多个容器组960中，使得即使正在重建某些容器组960时应用程序也始终在线。可以通过将容器恢复成已知的良好状态来重建容器。将在下面更详细地说明重建。另外，安全控制模块150的操作与结合图1A和图1B描述的操作相同。在一个实施方式中，重建容器可以比重建物理服务器和虚拟机更有效。例如，可以在约30秒内恢复和部署容器。相比之下，重建服务器和虚拟机会的时间要长得多。虽然使容器滚动比使物理服务器和虚拟机滚动容易，但由于使用共享的核心OS文件，所以它们具有更高的风险。管理程序体系架构也有风险，但是由于OS专用于每个虚拟机，因此与容器平台相比降低了风险。当使物理服务器滚动时，由于黑客将需要具有对服务器的BIOS级控制来进行服务器劫持或者黑客将需要远程管理工具访问，风险就会再次降低。

[0047] 本文的描述主要关注物理服务器或虚拟机的滚动。然而，本文所描述的滚动安全的原理适用于物理服务器、虚拟机或容器的滚动。

[0048] 图2A是根据一个实施方式的前端服务器200的框图。前端服务器200可以表示来自图1A的前端服务器组130的前端服务器。前端服务器200包括若干软件应用程序250A至250C、OS 152、固件154和前端安全模块156。OS 152的示例包括LINUX和MICROSOFT WINDOWS等。应用程序250在OS 152的顶部执行。固件154包括存储在可编程存储器芯片中的软件。

[0049] 客户端设备105可以与应用程序250建立网络连接C1至C6。连接被用作在客户端设备105处和服务器200处的套接字之间的双向通信信道。连接使用握手过程在某个时间点建立，然后在稍后的时间点终止。连接可以包括由协议定义的几种状态。连接的示例是开放系统互连(OSI)模型的传输层的传输控制协议(TCP)连接。

[0050] 客户端设备105还通过连接C1-C6与应用程序250建立应用程序用户会话S1-S6。用户会话是给定应用程序的两个或多个通信实体之间的交互信息交换。用户会话在某个时间点建立，然后在稍后的时间点终止。在用户会话期间，可以通过已经为会话建立的连接在每个方向上发送一个或多个消息。在一个实施方式中，应用程序会话是位于传输层之上的OSI会话层的会话。

[0051] 在一个示例中，当用户在客户端设备105A处刷信用卡时，可以启动信用卡认证会话(例如，S1、S2)，并且客户端设备105A建立与信用卡支付应用程序250A的连接和会话。信用卡支付应用程序250A与客户端设备105A进行通信以从客户端设备105A取得信用卡号码和收费金额。然后，信用卡支付应用程序250经由后端服务器135访问数据库140以确定信用卡号码是否具有足够的信用来处理支付。然后，信用卡支付应用程序250向客户端设备105A提供是/否响应。然后在向客户端设备105A提供响应之后终止连接和会话。

[0052] 在另一示例中，当用户在客户端105B处将URL输入浏览器时，可以启动网页(web)表单会话(例如，S3、S4)。客户端设备105B与网站250B建立会话。客户端设备105B与网站250B建立会话。服务器200可以处理多个会话。服务器200每个会话启动一个时间计数器。用户在会话关闭前具有x量的时间填写表单。由于填写网页表单数据花费时间，所以不同的服务器会处理最初会话中的表单提交。

[0053] 在另一示例中，当用户在客户端设备105B处打开移动银行应用程序时，可以启动网上银行会话(例如，S5、S6)，并且客户端设备105B与网络银行应用程序250C建立连接和会话。网上银行应用程序250C与客户端设备105C进行通信以从客户端设备105C获得认证信息。一旦被认证，客户端设备105C可以请求帐户余额，加载存款支票的副本，以及进行其他银行请求。银行应用程序250C可以经由后端服务器135访问存储在数据库140中的帐户信息来处理这些请求。连接和会话最终在会话结束时终止。

[0054] 前端安全模块156可以与安全控制模块150通信以发送和接收安全信息以实现滚动安全。安全模块156可以接收命令以启动前端服务器200的重建。这些命令可以包括黄金镜像的名称，其是将被用作重建的模板的已知良好的主要软件镜像。然后，安全模块156根据这些命令来重建前端服务器200，例如通过替换OS 152、应用程序和/或固件154。可以通过用黄金镜像覆盖服务器200上的现有软件、删除服务器200上的现有软件、以及将新软件从黄金镜像复制到服务器200上来替换OS 152、应用程序154和/或固件154。黄金镜像可以本地存储在服务器200内的磁盘内或网络上的其他地方。

[0055] 可以使用具有变化的重建时间的不同重建技术。在一个实施方式中，可以使用单个黄金镜像来重建多个服务器200。可以将来自黄金镜像的数据复制到前端服务器200上，然后在每个前端服务器200上执行后处理配置以配置OS 152或应用程序154。例如，可以在每个前端服务器200上执行不同的脚本以建立该服务器的唯一名称和该服务器的IP地址。在一个实施方式中，可以存在对于每个前端服务器200而言特定且唯一的多个黄金镜像。来自黄金镜像的数据可以被复制到相应的服务器上，而不需要后处理配置，这减少了重建时间。

[0056] 在另一个实施方式中，使用数据差分技术来重建前端服务器200。具体地，前端服务器200的软件的数据块或文件可以与黄金镜像的数据块或文件进行比较。仅从黄金镜像恢复不同的数据块或文件。通过利用基于块或文件的差异，经由本地磁盘、远程SAN磁盘或NAS磁盘来快速部署预配置的操作系统和应用程序配置是可行的。应当注意，其他重建技术也是可行的，并且仍然落入本公开内容的范围内。

[0057] 在一个实施方式中，可以将各种散列或加密模型或块状态比较应用于重建的软件镜像，以验证重建是标准预期配置，并且状态是已知良好的配置。例如，重建软件可以被散列，然后与黄金镜像的散列进行比较，以验证重建是否按预期执行。

[0058] 在一个实施方式中，前端安全模块156在重建期间将前端服务器200置于锁定安全模式中以防止篡改。在重建期间，前端安全模块156可以将其内部防火墙访问控制列表(ACL)设置成具有阻止除与安全服务器148的安全控制模块150的通信之外的到特定端口的任何流量的权限。ACL可以是网络端口以及允许使用网络端口的特定实体的列表。也可以根据需要允许其他第三方应用程序访问以验证合规性的状态(state of compliance)。

[0059] 安全模块156还可以接收更改OS 152的密码的命令，然后根据该命令替换密码。在一个实施方式中，通过智能平台管理接口(IPMI)传送安全信息。

[0060] 图2B是根据一个实施方式的具有VM 204的前端服务器202的框图。前端服务器202可以表示来自图1B的前端服务器159。前端服务器202包括若干VM 204、管理程序208、OS 152和前端安全模块156。每个VM包括虚拟化OS 206和应用程序250。

[0061] 前端安全模块156A类似于前端模块156，但是现在响应于重建VM 204的命令来重建虚拟机。虚拟机204的重建类似于关于图2A所描述的重建，并且还可以利用VM 204的黄金镜像来生成VM 204、利用数据差分、和/或在重建VM 204之后执行重建验证。

[0062] 图2C是根据一个实施方式的具有容器292的前端服务器290的框图。前端服务器290可以表示来自图1C的前端服务器159。前端服务器290包括若干容器292、容器引擎294、OS 152和前端安全模块156B。每个容器包括虚拟化应用程序250。

[0063] 前端安全模块156B类似于前端模块156，但是现在响应于重建容器292的命令滚动地重建容器292。容器292的重建类似于关于图2A所描述的重建，并且还可以利用容器292的黄金镜像来生成容器292、利用数据差分、和/或在重建容器292之后执行重建验证。

[0064] 图3是根据一个实施方式的使服务器组滚动的图。在图3中示出了四个服务器组130A-130D的滚动操作。在其他实施方式中，图3所示的滚动操作也适用于VM组160和软件容器组960的滚动。

[0065] 每个服务器组130以不同的滚动安全模式操作：(1)正常操作模式、(2)关闭准备模式和(3)重建模式。在正常操作模式期间，服务器组130接受和服务新的用户会话和连接。在

关闭准备模式期间，服务器组130不接受新的会话和连接。允许现有会话和连接完成。在一个实施方式中，负载平衡器125可以被通知特定服务器组130正被置于关闭准备模式并且不接受新的会话和连接。负载平衡器125通过从能够向其创建新的会话和连接的可能的服务器组130移除服务器组130来响应。在重建模式期间，服务器组130从服务中被移除，并通过替换服务器组130的软件被重建。这些模式周期性地例如每60秒重复。

[0066] 服务器组130以滚动方式操作，使得不同服务器组的重建在不同时间启动。例如，在1:00:50重建服务器组130A，在1:01:00重建服务器组130B，在1:01:10重建服务器组130C，而在1:01:20重建服务器组130D。重建时间相互交错十秒。重建时间的交错确保始终存在至少一个服务器组130处于服务中，并可用于接受由服务器组130托管的应用程序的新的连接和用户会话。换句话说，总是存在处于正常运行模式下的至少一个服务器组130。

[0067] 在一个实施方式中，如果指示存在黑客的安全条件被触发，则对于服务器组130，可以延迟关闭准备模式。例如，如果会话与可疑IP相关联或已将会话打开太久，则会触发安全条件。在这种情况下，安全控制模块150可以实现会话、会话的容量和会话的记录的深度分析以更好地理解黑客的动作。可替代地，如果安全条件被触发，则安全模块150可以从服务器组130中除去在其上检测到被攻击的会话的被攻击的服务器。然后，将新的服务器热交换代替被攻击的服务器，使得滚动的服务器组130不被中断。

[0068] 图4是根据一个实施方式的安全控制模块150的框图。安全控制模块130包括通信模块405、滚动时间模块410、滚动控制模块415和密码更改模块420。在其他实施方式中，安全控制模块130可以具有图4中未示出的附加模块。

[0069] 滚动时间模块410保存滚动时间信息，该滚动时间信息指示有关物理服务器组130、VM组160或容器组960(在本文中统称为“滚动实体组”)应当何时进入不同模式(例如，正常运行模式、关闭准备模式和重建模式)的交错时间。时间信息可以是包括滚动实体组和每个滚动实体组应当何时进入不同模式的特定时间的列表的时间表的形式。下面的表格是时间表的一个例子。

[0070]

服务器组	模式：正常操作	模式：关闭准备模式	模式：重建
1	1:00:00 1:01:00 …	1:00:30 1:01:30 …	1:00:50 1:01:50 …
2	1:00:10 1:01:10 …	1:00:40 1:01:40 …	1:01:00 1:02:00 …
3	1:00:20 1:01:20 …	1:00:50 1:01:50 …	1:01:10 1:02:10 …
4	1:00:30 1:01:30 …	1:01:00 1:02:00 …	1:01:20 1:02:20 …

[0071] 表格的第一列标识服务器组。第二列标识服务器组应当何时进入正常操作模式的开始时间。第三列标识服务器组应当何时进入关闭准备模式。第四列标识重建过程应当何时开始。

[0072] 在其他实施方式中，时间信息可以是最大时限的形式，而不是时间表。例如，时间信息可以包括滚动实体组的最大正常运行时间、正常操作模式的最大持续时间、关闭准备模式的最大持续时间和/或重建模式的最大持续时间。时间信息还可以包括描述滚动实体组之间的交错延迟量的信息。

[0073] 滚动模式的滚动时间信息可以由用户手动设置。在另一个实施方式中，时间信息可以通过监测服务器上的先前应用程序会话或连接的持续时间并生成包括所监测的持续时间的应用程序配置文件而由机器学习。持续时间(例如平均持续时间、最大持续时间)的统计测量可以根据所监测的持续时间来确定。然后将统计测量乘以乘数(例如8x、10x)以确定每个滚动模式的最大持续时间。因此，在重建滚动实体组之前，重建之间的时间足以使新用户会话和连接建立并完成。例如，如果用户会话长达6秒，则该值可以乘以8x，以产生48秒的周期性重建之间的持续时间，这比会话持续时间大得多。

[0074] 滚动控制模块415根据滚动时间信息(例如，滚动时间表或上述最大时限)控制滚动实体组的滚动操作。滚动控制模块415使用滚动时间信息来确定服务器组应当处于的滚动模式。然后，滚动控制模块415经由通信模块405向负载平衡器125和滚动实体组发送控制命令，这导致滚动实体组以如图3所示的滚动方式操作。每个滚动实体组的命令会相对于其他滚动实体组的命令在时间上交错，以确保滚动实体组以受控和交错的时间滚动。

[0075] 为了启动正常操作模式，滚动控制模块415可以向负载平衡器125发送正常操作启动命令。该命令识别特定的滚动实体组，并且还指示对于该滚动实体组要开始的正常操作模式。负载平衡器125通过允许与所识别的滚动实体组建立会话和连接来响应该命令。在一个实施方式中，正常操作启动命令也可以被发送至对于其正在启动正常操作的适当的滚动实体组。

[0076] 为了启动关闭准备模式，滚动控制模块415可以向负载平衡器125发送关闭准备启动命令。该命令识别特定的滚动实体组，并且还指示对于该滚动实体组要开始的关闭准备启动模式。负载平衡器125通过阻止与所识别的滚动实体组建立任何新的会话和连接来响应该命令。允许滚动实体组的现有会话和连接完成。在一个实施方式中，关闭准备启动命令也可以被发送至滚动实体组的适当的服务器。

[0077] 为了启动重建，滚动控制模块145可以将重建启动命令发送至与要重建的滚动实体组相关联的适当的前端服务器。该命令可以包括要用于重建的已知良好的软件镜像的名称。作为响应，滚动实体组可以被利用已知良好的软件镜像重建。一旦重建完成，则滚动控制模块145还可以从适当的前端服务器接收重建确认信息。

[0078] 另外，在重建之前，滚动控制模块145可以将来自滚动实体组的数据复制到单独的存储驱动器。机器学习可以用于监测数据的变化，并对变化进行在线分析以用于其他服务器之间的整体比较的。这允许了解当实体在线时黑客对操作系统、应用程序或文件所做的所有更改。机器学习重建状态和时间是重要的，但是在被攻击的情况下延迟重建状态以实现更高级的学习也是经由滚动控制模块145管理的系统控制的一部分。滚动控制模块145还可以与本地服务器组、路由器115和防火墙120通信以继续服务于黑客，目的是学习和收集更多数据以学习黑客能力并关于新攻击了解更多。

[0079] 密码更改模块420启动服务器组130的密码更改。密码可以是OS、数据库或应用程序密码等。密码可以随由滚动时间信息指示的每次重建而更改，或者可以在特定的时间戳(即，以一定的间隔)被重建。密码更改的频率可以与滚动实体组重建的频率相同或不同。在一个实施方式中，密码更改模块420可以通过生成新密码并将密码发送至服务器来启动密码更改。在另一个实施方式中，密码更改模块420可以通过向服务器发送密码更改命令来启动密码更改。然后，服务器会响应于该命令生成新密码。可以使用很多算法中的任一种算法来生成密码。在一个实施方式中，时间戳是用于生成密码的要素中之一。

[0080] 通信模块405与网络通信系统中的服务器、负载平衡器125和其他设备进行通信。通信模块305可以发送滚动安全命令，其使滚动实体组以滚动和交错的方式进行操作。通信模块305可以发送在滚动实体组处启动密码更改的命令。通信模块305还可以从网络通信系统中的设备接收其他类型的信息。

[0081] 图5是根据一个实施方式的用于滚动安全的方法的流程图。在步骤505中，监测由滚动实体组托管的应用程序的先前连接或用户会话。持续时间存储在应用程序配置文件中。一旦收集了足够的信息，就使用先前连接和用户会话的持续时间来生成滚动时间信息，该滚动时间信息描述滚动实体组的不同滚动安全模式的交错时间，例如有关不同的滚动实体组应该何时被重建的交错时间。

[0082] 在步骤510中，安全控制模块150在由滚动时间信息指定的时间处启动第一滚动实体组的正常操作。在步骤512中，安全控制模块150在由滚动时间信息指定的时间处启动滚

动实体组的关闭准备模式。在步骤514中，安全控制模块150在由滚动时间信息指定的时间处启动第一滚动实体组的重建。此外，安全控制模块150同时启动第一滚动实体组的密码更改。步骤510-514连续重复，例如，以周期性的间隔重复。

[0083] 在步骤520中，安全控制模块150在由滚动时间信息指定的时间处启动第二滚动实体组的正常操作。在步骤522中，安全控制模块150在由滚动时间信息指定的时间处启动第二滚动体组的关闭准备模式。在步骤524中，安全控制模块150在由滚动时间信息指定的时间处启动第二滚动实体组的重建。此外，安全控制模块150同时启动第一滚动实体组的密码更改。步骤520-524连续例如以周期性的间隔重复。

[0084] 也可以以与步骤510-514和520-524类似的方式来控制其他滚动实体组。另外，对于每个滚动实体组，重建、正常操作模式和关闭准备模式的启动相对于其他滚动实体组在时间上交错。安全模式的交错产生图1所示的滚动安全。

[0085] 图6示出了根据一个实施方式的诸如防火墙115、路由器120、负载平衡器125、客户端设备105、前端服务器130或159、后端服务器135或安全服务器148的计算设备的硬件体系结构。在一个实施方式中，计算设备是包括诸如通过总线601彼此交换数据和控制信号的处理器602、存储器603、存储模块604、输入模块(例如，键盘、鼠标等)606、显示模块607和通信接口605的计算机。存储模块604被实现为一个或多个非暂态计算机可读存储介质(例如，硬盘或固态驱动器)，并且存储软件指令640(例如模块)，所述软件指令640由处理器602结合存储器603执行以实现本文所描述的滚动安全特征。操作系统软件和其他应用程序软件也可以存储在存储模块604中以在处理器602上运行。

[0086] 本文所描述的滚动安全不仅限于前端服务器130、虚拟机160和容器960。在其他实施方式中，滚动安全可以用于周期性地重建数据中心内的计算系统的其他组，例如防火墙120、负载平衡器126、交换机、后端服务器135和后端存储装置140。此外，本文所描述的模块的功能可以被组合成单个模块或被分配在附加模块之间。

[0087] 在其他实施方式中，本文所描述的滚动安全可以应用于提供公共软件功能的数据中心外部的计算系统的其他组。计算系统可以是台式机、笔记本电脑、ipad、iphone、和车辆(汽车、火车、飞机)中的计算系统以及发电厂、发电机等中的计算系统。在飞机的示例中，飞机可以包括几个并行的飞行控制系统，其中每个都可以为飞机提供飞行控制。使飞行控制系统以交错方式滚动可以保护飞行控制系统不被攻击，同时确保至少一个飞行控制系统总是在线。

[0088] 在阅读本公开内容后，本领域技术人员可以理解有关滚动安全的另外的替选设计。因此，虽然已经示出和描述了本公开内容的特定实施方式和应用，但是应当理解，本公开内容不限于本文所公开的精确构造和部件。在不偏离所附权利要求中限定的公开内容的精神和范围的情况下，可以在本公开内容的方法和装置的布置、操作和细节中进行对本领域技术人员而言显见的各种修改、变化和变形。

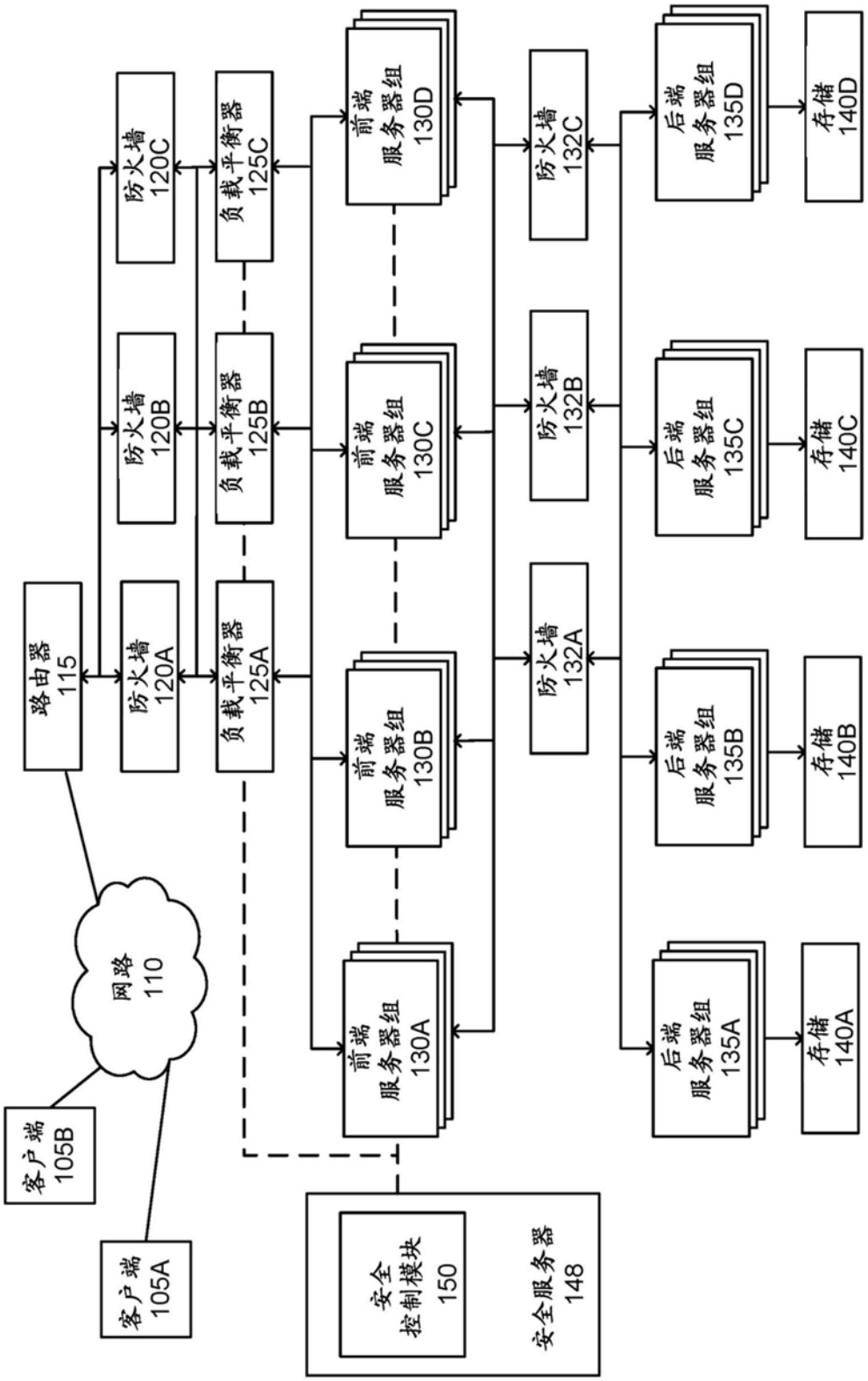

路由器
115
防火墙
120A
防火墙
120B
防火墙
120C
负载平衡器
125A
负载平衡器
125B
负载平衡器
125C
前端
服务器组
130A
前端
服务器组
130B
前端
服务器组
130C
前端
服务器组
130D
防火墙
132A
防火墙
132B
防火墙
132C
后端
服务器组
135A
后端
服务器组
135B
后端
服务器组
135C
后端
服务器组
135D
存储
140A
存储
140B
存储
140C
存储
140D
网路
110
客户端
105A
客户端
105B
安全
控制模块
150
安全服务器
148

图1A

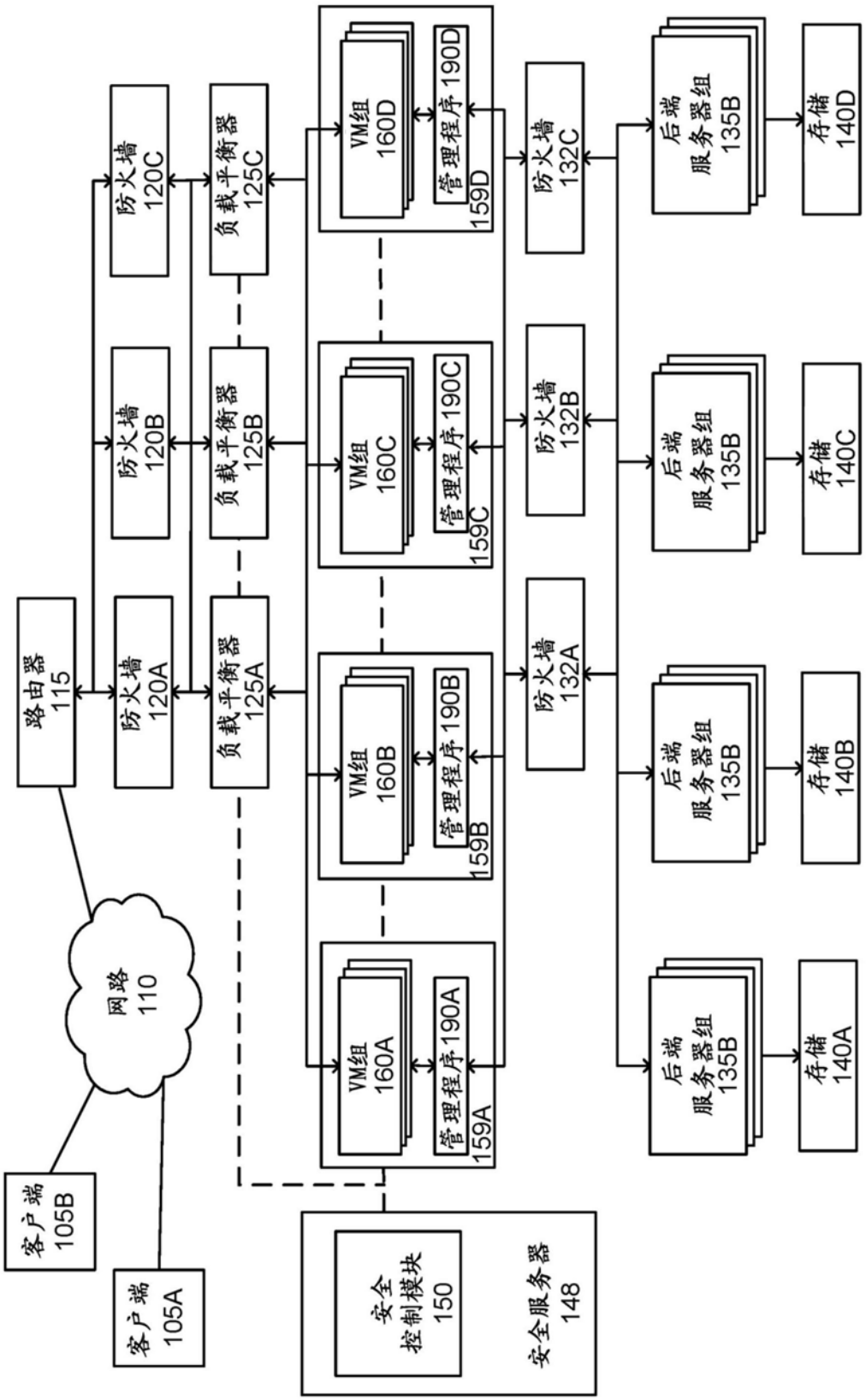

路由器
115
防火墙
120A
防火墙
120B
防火墙
120C
负载平衡器
125A
负载平衡器
125B
负载平衡器
125C
VM组
160A
管理程序190A
159A
VM组
160B
管理程序190B
159B
VM组
160C
管理程序190C
159C
VM组
160D
管理程序190D
159D
防火墙
132A
防火墙
132B
防火墙
132C
后端
服务器组
135B
后端
服务器组
135B
后端
服务器组
135B
后端
服务器组
135B
存储
140A
存储
140B
存储
140C
存储
140D
网路
110
客户端
105A
客户端
105B
安全
控制模块
150
安全服务器
148

图1B

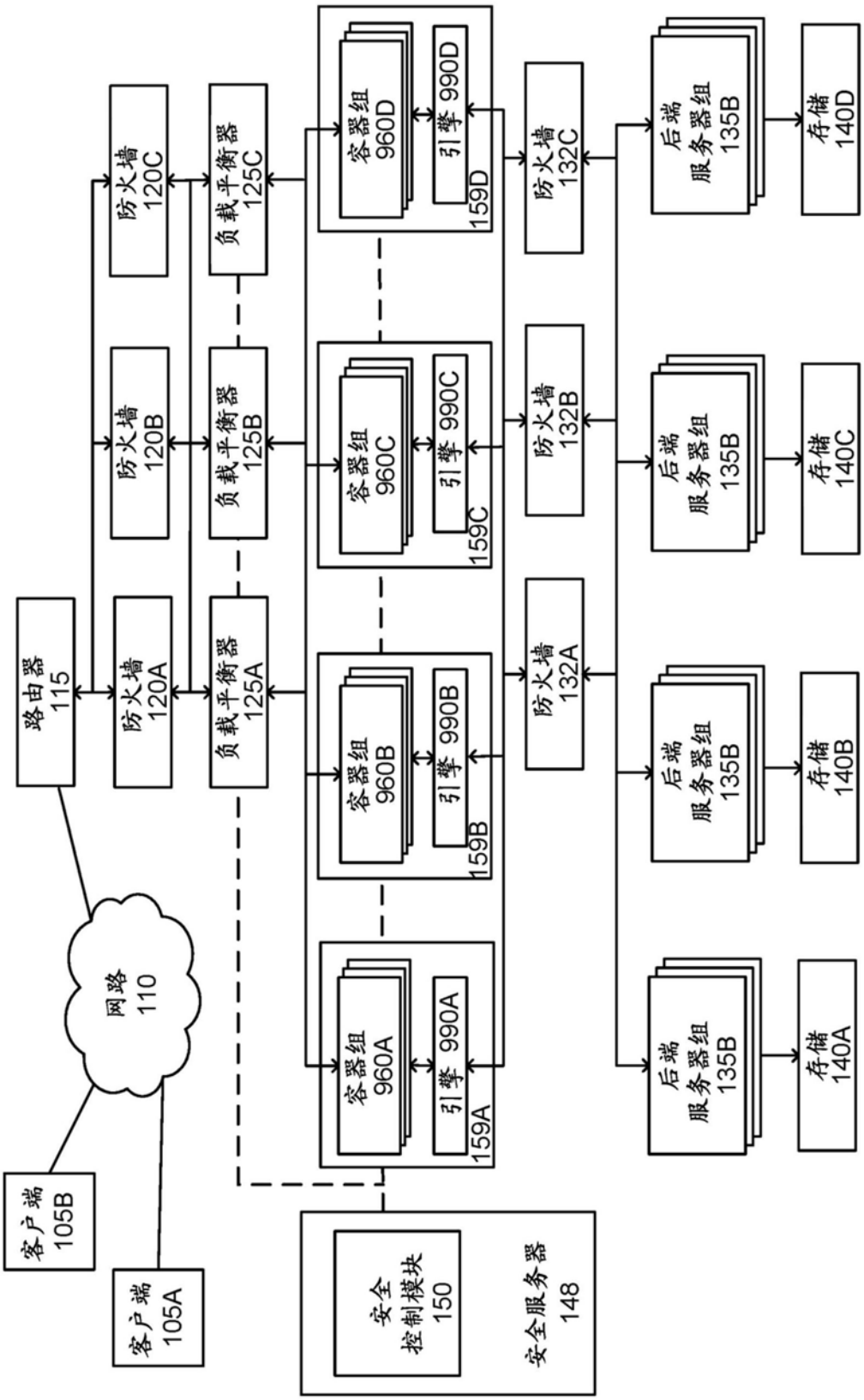

路由器
115
防火墙
120A
防火墙
120B
防火墙
120C
负载平衡器
125A
负载平衡器
125B
负载平衡器
125C
容器组
960A
引擎 990A
159A
容器组
960B
引擎 990B
159B
容器组
960C
引擎 990C
159C
容器组
960D
引擎 990D
159D
防火墙
132A
防火墙
132B
防火墙
132C
后端
服务器组
135B
后端
服务器组
135B
后端
服务器组
135B
后端
服务器组
135B
存储
140A
存储
140B
存储
140C
存储
140D
网路
110
客户端
105A
客户端
105B
安全
控制模块
150
安全服务器
148

图1C

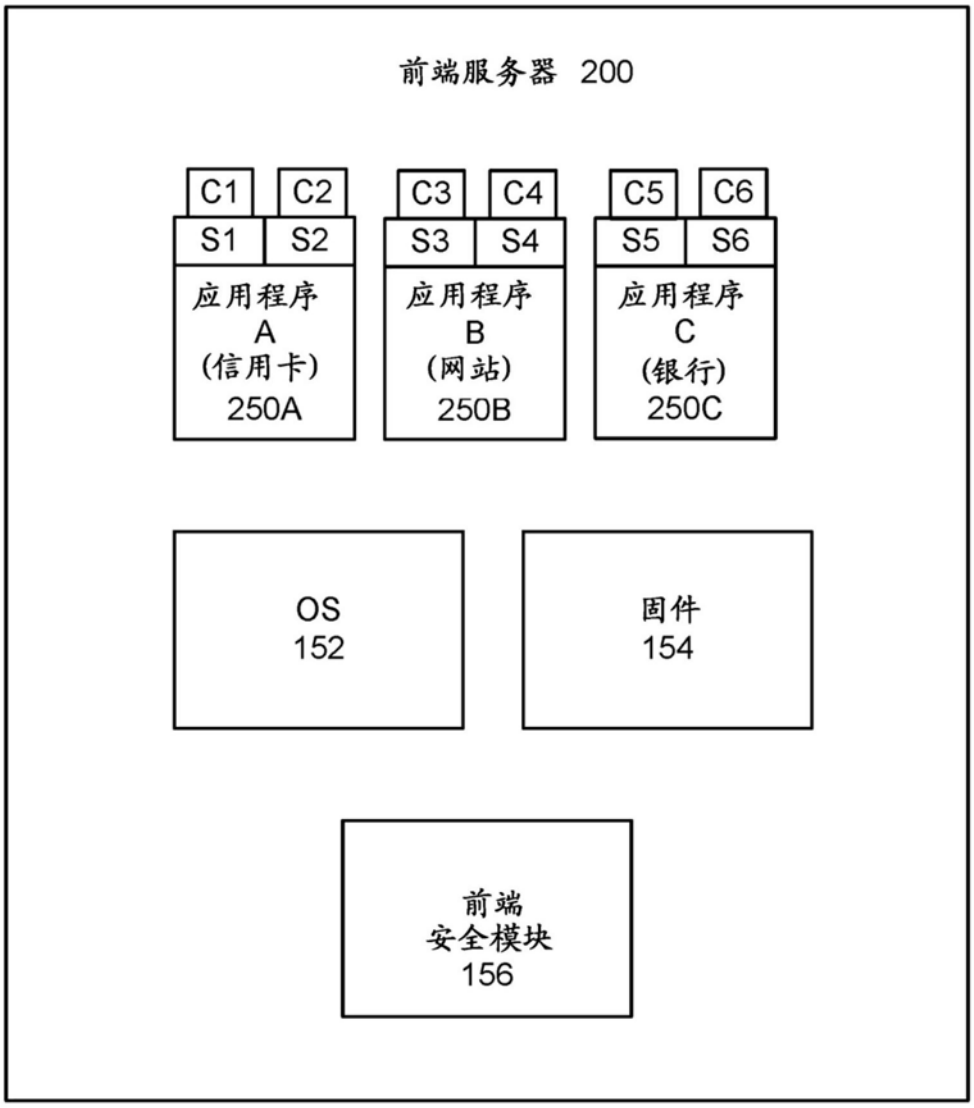

前端服务器 200
C1
C2
S1
S2
应用程序
A
(信用卡)
250A
C3
C4
S3
S4
应用程序
B
(网站)
250B
C5
C6
S5
S6
应用程序
C
(银行)
250C
OS
152
固件
154
前端
安全模块
156

图2A

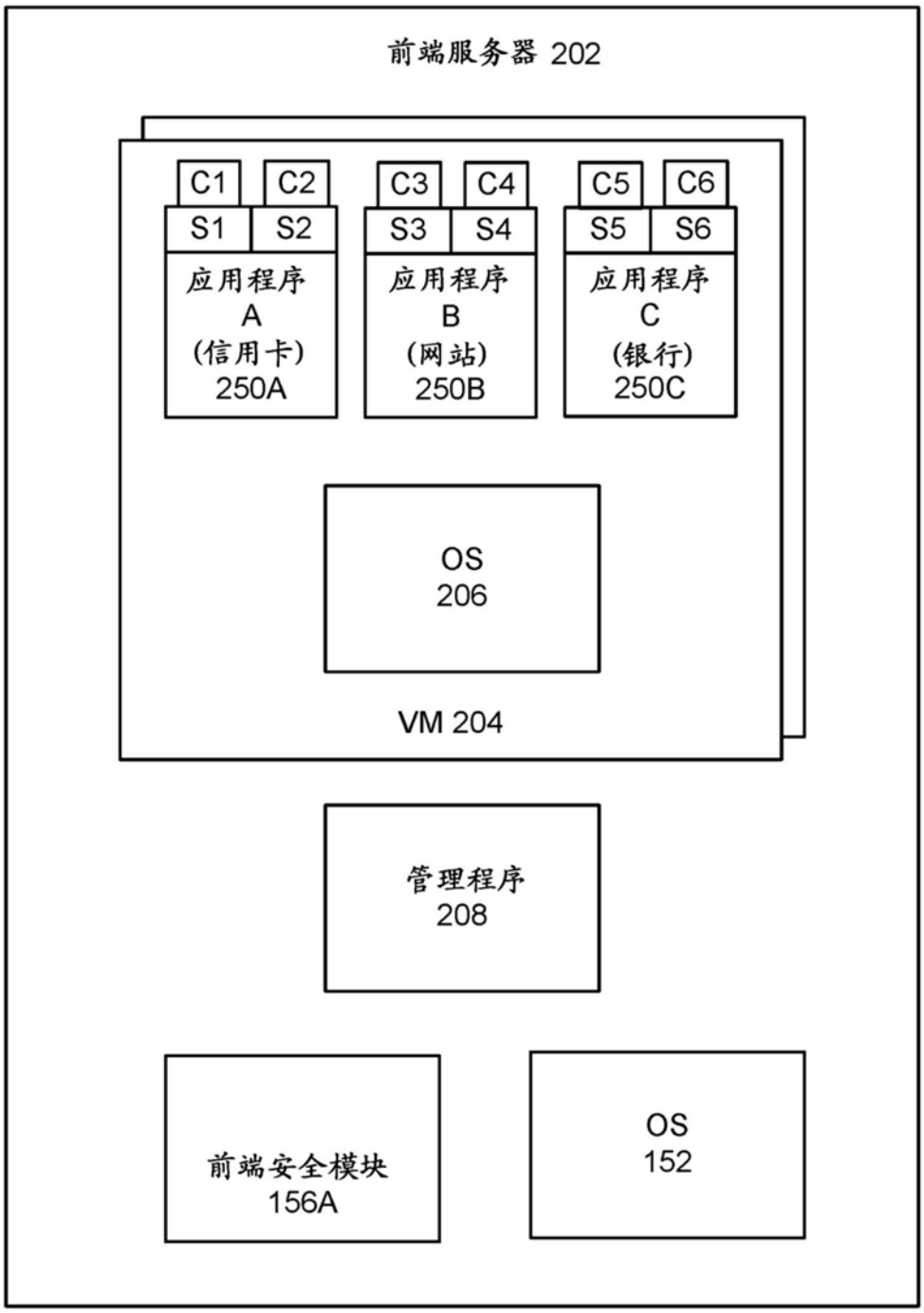

前端服务器 202
C1
C2
S1
S2
应用程序
A
(信用卡)
250A
C3
C4
S3
S4
应用程序
B
(网站)
250B
C5
C6
S5
S6
应用程序
C
(银行)
250C
OS
206
VM 204
管理程序
208
前端安全模块
156A
OS
152

图2B

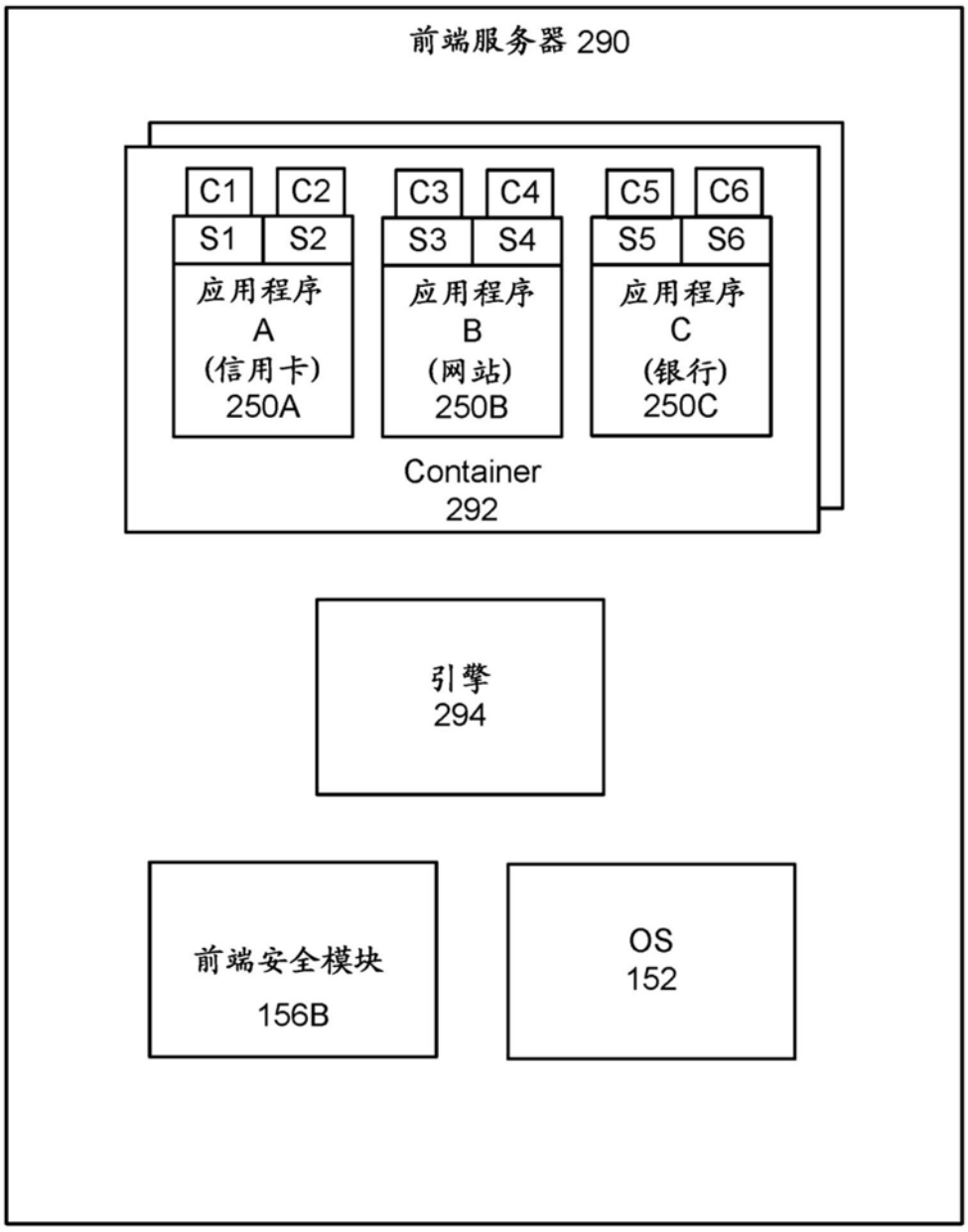

前端服务器 290
C1
C2
S1
S2
应用程序
A
(信用卡)
250A
C3
C4
S3
S4
应用程序
B
(网站)
250B
C5
C6
S5
S6
应用程序
C
(银行)
250C
Container
292
引擎
294
前端安全模块
156B
OS
152

图2C

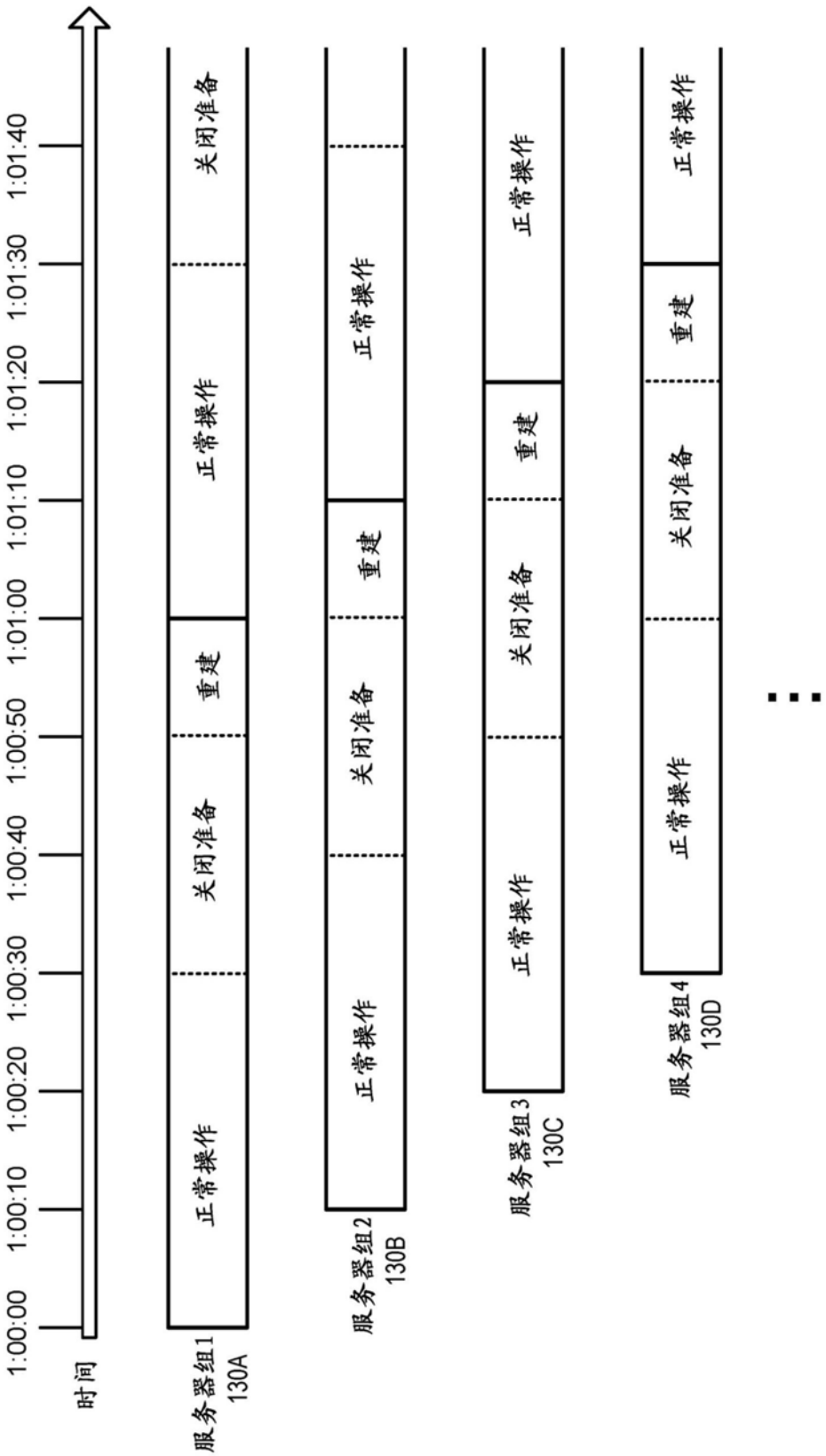

时间
1:00:00
1:00:10
1:00:20
1:00:30
1:00:40
1:00:50
1:01:00
1:01:10
1:01:20
1:01:30
1:01:40
服务器组1
130A
正常操作
关闭准备
重建
正常操作
关闭准备
服务器组2
130B
正常操作
关闭准备
重建
正常操作
服务器组3
130C
正常操作
关闭准备
重建
正常操作
服务器组4
130D
正常操作
关闭准备
重建
正常操作

图3

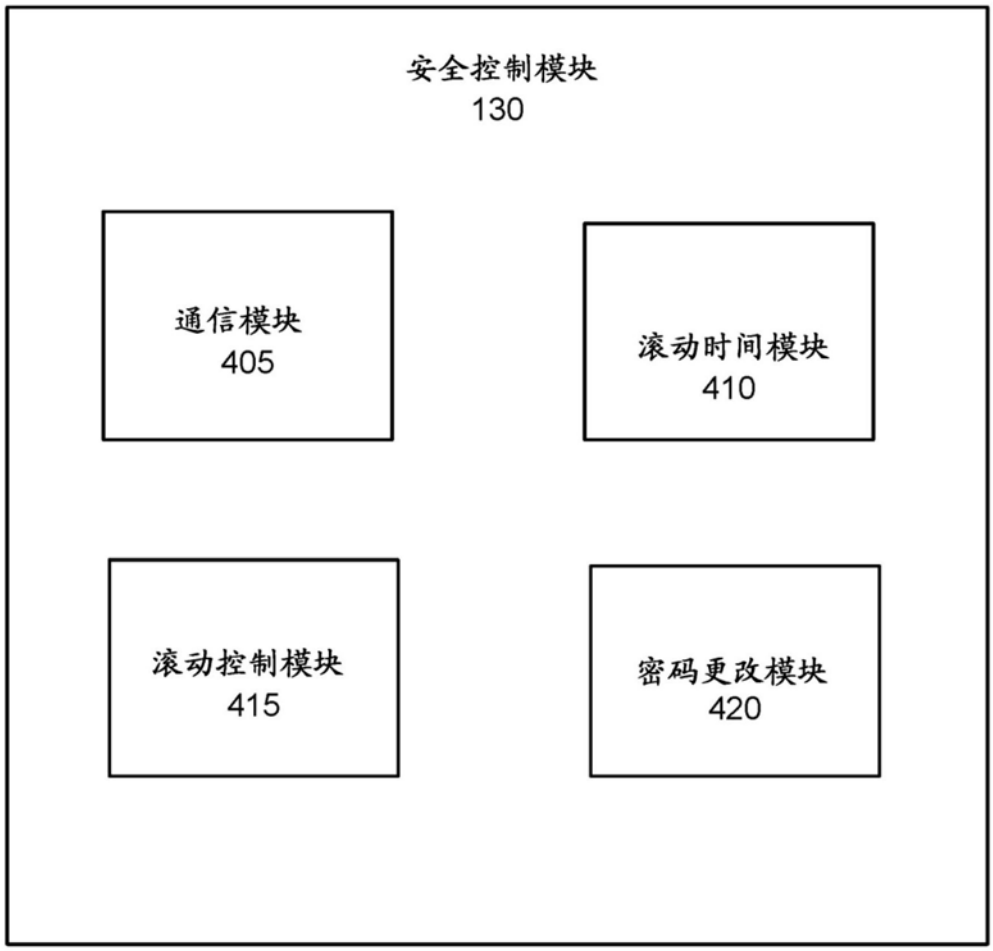


图4

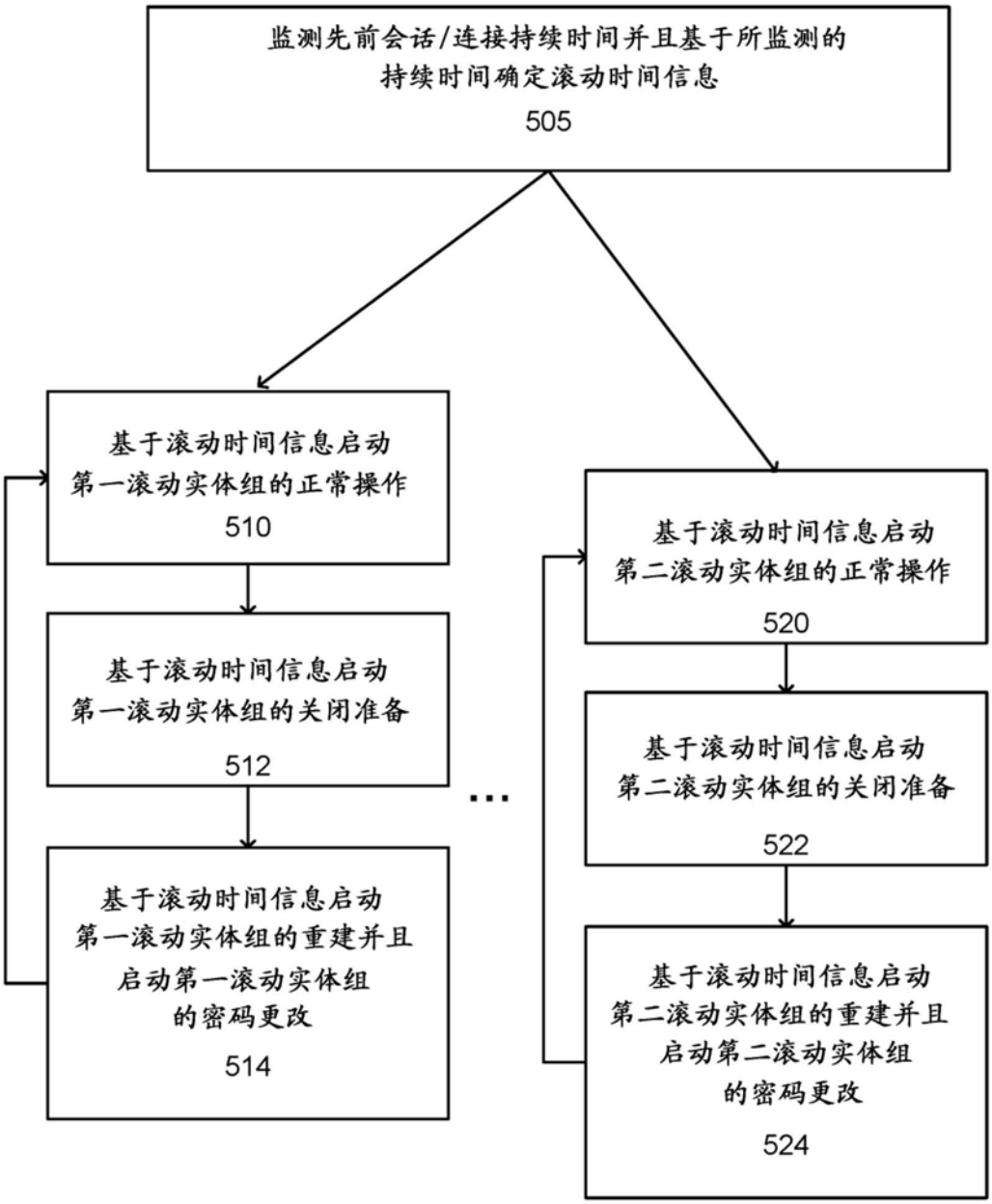

监测先前会话/连接持续时间并且基于所监测的持续时间确定滚动时间信息
505
基于滚动时间信息启动第一滚动实体组的正常操作
510
基于滚动时间信息启动第一滚动实体组的关闭准备
512
基于滚动时间信息启动第一滚动实体组的重建并且启动第一滚动实体组的密码更改
514
...
基于滚动时间信息启动第二滚动实体组的正常操作
520
基于滚动时间信息启动第二滚动实体组的关闭准备
522
基于滚动时间信息启动第二滚动实体组的重建并且启动第二滚动实体组的密码更改
524

图5

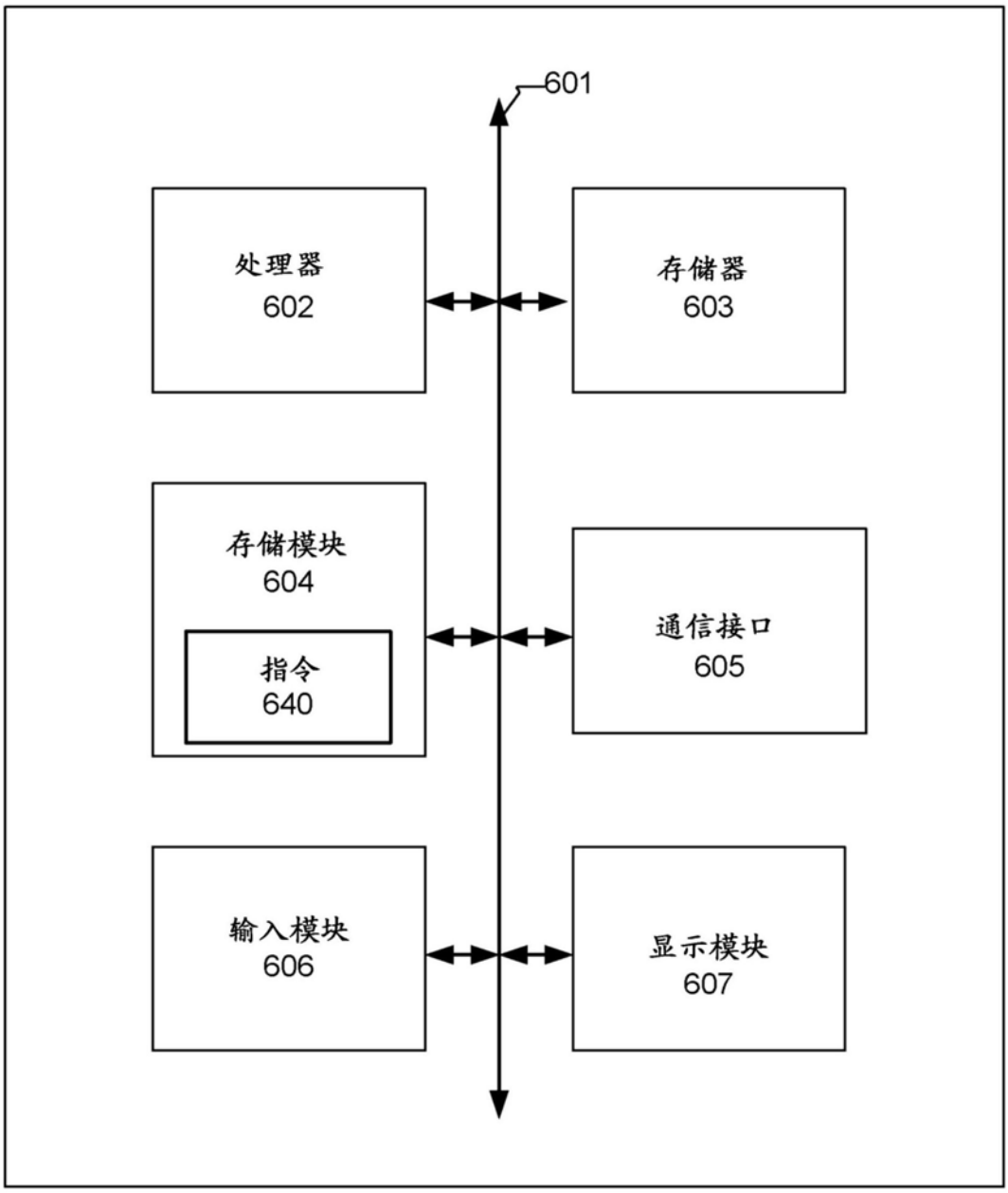


图6