(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 103119907 B
(45)授权公告日 2016.06.15

(21)申请号 201180045267.7

(22)申请日 2011.07.19

(30)优先权数据
12/840632 2010.07.21 US

(85)PCT国际申请进入国家阶段日
2013.03.20

(86)PCT国际申请的申请数据
PCT/US2011/044550 2011.07.19

(87)PCT国际申请的公布数据
WO2012/012438 EN 2012.01.26

(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 M·穆尔吉亚 P·拉菲克
J·卡妮娜 L·汤姆林 I·波尔

(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 29/06(2006.01)
H04L 12/24(2006.01)

(56)对比文件
WO 2010056843 A1,2010.05.20,
CN 101309279 A,2008.11.19,
CN 101764742 A,2010.06.30,

审查员 柴华

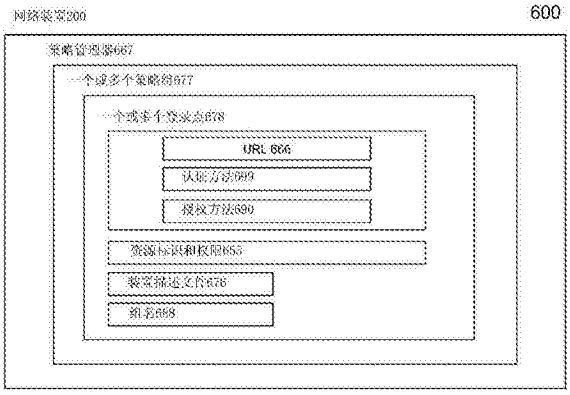
权利要求书2页 说明书56页 附图18页

(54)发明名称

提供用于访问控制的智能组的系统和方法

(57)摘要

本公开针对用于建立和应用策略组(677)以控制用户对所识别资源的访问的系统和方法。可经由策略管理器建立策略组,该策略组表示一个或多个访问配置的集合,用于用户访问一个或多个所识别资源。所述策略组可包括用于表示访问所识别资源的入口点的登录点组件(678)。可经由策略管理器将登录点配置用于为入口点(666)指定统一资源定位符。可为登录点组件选择一个或多个认证和授权方法(699),(690)。装置可接收访问统一资源定位符的请求。装置可初始化策略组用于评估。装置可发起由登录点组件指定的与用户的一个或多个认证和授权方法。



CN 103119907 B

1.一种用于建立策略组以集合访问配置从而控制用户对所识别资源的访问的方法，所述方法包括：

a)经由在多个客户机和一个或多个服务器中间的装置上执行的策略管理器来建立策略组，所述策略组表示一个或多个访问配置的集合，用于用户经由所述装置访问所述一个或多个服务器的一个或多个所识别资源，所述策略组包含用于表示访问所述一个或多个所识别资源的入口点的登录点组件；

b)经由所述策略管理器配置所述登录点组件，以为所述入口点指定统一资源定位符；

c)经由所述策略管理器为所述登录点组件选择一个或多个认证方法；以及

d)经由所述策略管理器，基于所述一个或多个认证方法为所述登录点组件识别一个或多个授权方法。

2.根据权利要求1所述的方法，其中步骤(a)还包括建立所述策略组以使其具有装置描述文件组件与所述登录点组件，所述装置描述文件组件识别要执行的端点分析，用于经由所述登录点组件的入口点进行访问。

3.根据权利要求1所述的方法，其中步骤(b)还包括为所述策略组建立第二登录点组件并且将第二统一资源定位符配置为入口点。

4.根据权利要求1所述的方法，其中步骤(c)还包括为所述登录点组件指定两个认证方法用于双重认证。

5.根据权利要求1所述的方法，其中步骤(d)还包括由所述策略管理器基于所述一个或多个认证方法的选择来限制所述授权方法的选择。

6.根据权利要求1所述的方法，还包括当禁用所述登录点组件时，所述策略组变为不可用。

7.根据权利要求1所述的方法，还包括为所述策略组指定一个或多个装置描述文件，所述一个或多个装置描述文件的每一个识别一种或多种类型的端点分析以在用户的装置上执行。

8.根据权利要求1所述的方法，还包括为所述策略组指定所述一个或多个所识别资源中的允许访问的一种资源。

9.根据权利要求1所述的方法，还包括为所述策略组指定所述一个或多个所识别资源中的拒绝访问的一种资源。

10.根据权利要求1所述的方法，还包括为所述登录点组件指定一个或多个参数，所述一个或多个参数优先于所述装置的相应参数。

11.一种用于应用策略组以控制用户对所识别资源的访问的方法，所述方法包括：

a)由在多个客户机和一个或多个服务器中间的装置来识别策略组，所述策略组表示一个或多个访问配置的集合，用于用户经由所述装置访问所述一个或多个服务器的一个或多个所识别资源，所述策略组包含用于表示访问所述一个或多个所识别资源的入口点的登录点组件；

b)由所述装置接收所述用户访问统一资源定位符的请求，所述统一资源定位符对应于由所述登录点组件指定的入口点；

c)由所述装置发起由所述登录点组件指定的与所述用户的一个或多个认证方法；以及

d)由所述装置基于所述一个或多个认证方法应用由所述登录点组件指定的一个或多

个授权方法来访问所述一个或多个所识别资源。

12.根据权利要求11所述的方法，其中步骤(a)还包括识别所述策略组的装置描述文件组件，所述装置描述文件组件指定一个或多个装置描述文件，用于经由所述登录点组件的入口点进行访问。

13.根据权利要求11所述的方法，其中步骤(b)还包括由所述装置接收统一资源定位符，所述统一资源定位符被识别为所述策略组的第二登录组件的入口点。

14.根据权利要求11所述的方法，其中步骤(c)还包括由所述装置发起由所述登录点组件指定的两个认证方法用于双重认证。

15.根据权利要求11所述的方法，其中所述授权方法的选择受限于所述一个或多个认证方法的指定。

16.根据权利要求11所述的方法，还包括由在所述用户的第二装置上的装置来执行由装置描述文件组件的一个或多个装置描述文件指定的一种或多种类型的端点分析。

17.根据权利要求11所述的方法，还包括由所述装置准许对所述一个或多个所识别资源的一种资源的访问。

18.根据权利要求11所述的方法，还包括由所述装置拒绝对所述一个或多个所识别资源的一种资源的访问。

19.根据权利要求11所述的方法，还包括：如由所述策略组指定的，由所述装置忽略所述装置的一个或多个参数。

20.一种用于提供策略组以集合访问配置从而控制特定用户对特定资源的访问的系统，所述系统包括：

在多个客户机和一个或多个服务器中间的装置；

所述装置的策略管理器，其建立策略组，所述策略组表示一个或多个访问配置的集合，用于用户经由所述装置访问所述一个或多个服务器的一个或多个所识别资源；

所述策略组的登录点组件，其表示访问所述一个或多个所识别资源的入口点，所述登录点组件为所述入口点指定统一资源定位符；以及

其中，经由所述策略管理器为所述登录点组件指定一个或多个认证方法；并且基于所述一个或多个认证方法为所述登录点组件识别一个或多个授权方法。

提供用于访问控制的智能组的系统和方法

[0001] 相关申请

[0002] 本申请要求2010年7月21日提交的、名称为“SYSTEMS AND METHODS FOR PROVIDING A SMART GROUP”的美国专利申请序列号12/840632的优先权，该申请通过引用被全部包含于此。

技术领域

[0003] 本申请总的涉及控制对与数据通信网络连接的资源的访问。本申请尤其涉及用于配置和应用用于做出访问控制决策的策略组的系统和方法。

背景技术

[0004] 通信和数据网络的激增已经显著提高了资源对于大量用户的可用性，该资源例如是文件、应用以及服务。为了有效地管理和保护这些资源，可以实施各种系统来限制或控制对这些资源的访问。可将对某些网络及其资源的访问限制到对这些网络具有访问权限的用户上。例如，可能需要对请求访问资源的用户进行认证。在一些实施例中，可基于资源的可用性和/或其他因素将有限的资源分配给用户。随着资源类型、网络、保护方案和分配方法的增加，网络资源的管理也变得日益复杂。例如，传统系统可能包括诸如访问网关、防火墙以及认证、授权和审计(AAA)服务器的网络组件，来提供各种功能。

发明内容

[0005] 本发明针对提供策略组用于控制对网络资源的访问的方法和系统。可将策略组配置为聚合与控制对网络资源的访问相关的一个或多个访问配置。可将策略组用于逻辑地管理一个或多个访问配置。策略组的访问配置可属于下列中一个或多个的任意组合：登录点(logon point)、资源的标识和该资源的可用权限、装置描述文件，以及组名。每个登录点可与至少一种认证方法和一种授权方法相关联。应用策略组的网络装置或访问网关可基于访问配置的评估来为所请求的资源授予特定的访问级别。客户机装置处的用户可尝试登录会话以访问资源。用户可经由登录点提供的统一资源定位符(URL)来访问登录接口。可认证用户并且可以评估用户的授权权限。基于认证和/或授权，可识别用户可应用的组名。系统可至少部分基于该组名识别一个或多个策略组。还可以根据与该策略组关联的装置描述文件来评估用户的客户机装置。基于所识别的组名、认证、授权和/或装置描述文件评估，所述策略组可准许用户对一个或多个资源的访问。

[0006] 在一个方面，本发明涉及用于建立策略组以集合访问配置从而控制用户对所识别资源的访问的方法。该方法包括经由在多个客户机和一个或多个服务器的中间的装置上执行的策略管理器，建立策略组，该策略组表示一个或多个访问配置的集合，用于用户经由该装置访问一个或多个服务器的一个或多个所标识资源。策略组可包括用于表示访问一个或多个所标识资源的入口点的登录点组件。该方法可包括经由策略管理器将所述登录点组件配置用于为入口点指定统一资源定位符。该方法可包括经由策略管理器为登录点组件选择

一个或多个认证方法。该方法可包括经由策略管理器，基于一个或多个认证方法为登录点组件识别一个或多个授权方法。

[0007] 在一些实施例中，该方法包括建立策略组以使其具有装置描述文件组件与登录点组件。装置描述文件组件可识别要执行的一个或多个端点分析用于经由登录点组件的入口点访问。该方法可包括为策略组建立第二登录点组件并且将第二统一资源定位符(URL)配置为入口点。方法可以包括为登录点组件指定两个认证方法用于双重认证。策略管理器可基于一个或多个认证方法的选择来限制授权方法的选择。在一个实施例中，该方法可包括禁用登录点组件，其中策略组可变为不可用。

[0008] 在一些实施例中，该方法包括为策略组指定一个或多个装置描述文件。该一个或多个装置描述文件的每一个可识别一种或多种类型的端点分析以在用户的装置上执行。该方法可包括为策略组指定一个或多个所识别资源的允许访问的一种资源。该方法可包括为策略组指定一个或多个所识别资源的拒绝访问的一种资源。该方法可包括为登录点组件指定一个或多个参数，该一个或多个参数优先于装置的相应参数。

[0009] 在另一个方面，本发明涉及用于应用策略组来控制用户对所识别资源的访问的方法。在多个客户机和一个或多个服务器中间的装置可识别策略组。所述策略组可表示一个或多个访问配置的集合，用于用户经由所述装置访问一个或多个服务器的一个或多个所识别资源。策略组可包括用于表示访问一个或多个所识别资源的入口点的登录点组件。所述装置可接收用户访问统一资源定位符的请求，该统一资源定位符对应于由登录点组件指定的入口点。装置可发起由登录点组件指定的与用户的一个或多个认证方法。为访问所述一个或多个所识别资源，装置可基于一个或多个认证方法应用由登录点组件指定的一个或多个授权方法。

[0010] 在一些实施例中，该方法包括识别策略组的装置描述文件组件。装置描述文件组件可指定一个或多个装置描述文件用于经由登录点组件的入口点进行访问。装置可接收统一资源定位符，该统一资源定位符被识别为策略组的第二登录组件的入口点。装置可发起由登录点组件指定的两个认证方法用于双重认证。在一些实施例中，一个或多个授权方法的选择受限于一个或多个认证方法的指定。在用户的第二装置上，装置可执行由装置描述文件组件的一个或多个装置描述文件指定的一种或多种类型的端点分析。装置可准许对一个或多个所识别资源的一种资源的访问。装置可拒绝对一个或多个所识别资源的一种资源的访问。如策略组所指定的，装置可忽略该装置的一个或多个参数。

[0011] 在另一个方面，本发明涉及用于提供策略组以集合访问配置从而控制特定用户对特定资源的访问的系统。该系统可包括在多个客户机和一个或多个服务器中间的装置。该装置的策略管理器可建立策略组。所述策略组可表示一个或多个访问配置的集合，用于用户经由所述装置访问一个或多个服务器的一个或多个所标识资源。策略组的登录点组件可表示访问一个或多个所识别资源的入口点。登录点组件可指定入口点的统一资源定位符。可经由策略管理器指定用于登录点组件的一个或多个认证方法。可经由策略管理器基于所述一个或多个认证方法为登录点组件识别一个或多个授权方法。

[0012] 在附图和下面的描述中将详细阐述本发明的各种实施例的细节。

附图说明

[0013] 通过参考下述结合附图的描述，本发明的前述及其它目的、方面、特征和优点将会更加明显并更易于理解，其中：

[0014] 图1A是客户机经由设备访问服务器的网络环境的实施例的框图；

[0015] 图1B是经由设备从服务器传送计算环境到客户机的环境的实施例的框图；

[0016] 图1C是经由设备从服务器传送计算环境到客户机的环境的另一个实施例的框图；

[0017] 图1D是经由设备从服务器传送计算环境到客户机的环境的又一个实施例的框图；

[0018] 图1E-1H是计算装置的实施例的框图；

[0019] 图2A是用于处理客户机和服务器之间的通信的设备的实施例的框图；

[0020] 图2B是用于优化、加速、负载平衡以及路由客户机和服务器之间的通信的设备的另一个实施例的框图；

[0021] 图3是用于经由设备与服务器通信的客户机的实施例的框图；

[0022] 图4A是虚拟化环境的实施例的框图；

[0023] 图4B是虚拟化环境的另一个实施例的框图；

[0024] 图4C是虚拟化设备的实施例的框图；

[0025] 图5A是在多核网络设备中实现并行的方法的实施例的框图；

[0026] 图5B是使用多核网络应用的系统的实施例的框图；

[0027] 图5C是多核网络设备的一个方面的实施例的框图；

[0028] 图6A是用于提供策略组的系统的实施例的框图；

[0029] 图6B是用于提供策略组的系统的另一个实施例的框图；以及

[0030] 图6C是用于提供策略组的方法的实施例的流程图。

[0031] 根据下面结合附图所阐述的详细描述，本发明的特征和优点将更明显，其中，同样的参考标记在全文中标识相应的元素。在附图中，同样的附图标记通常表示相同的、功能上相似的和/或结构上相似的元素。

具体实施方式

[0032] 为了阅读本发明下述各种具体实施例的描述，下述对于说明书的部分以及它们各自内容的描述是有用的：

[0033] —A部分描述有益于实施本文描述的实施例的网络环境和计算环境；

[0034] —B部分描述用于将计算环境传送到远程用户的系统和方法的实施例；

[0035] —C部分描述用于加速客户机和服务器之间通信的系统和方法的实施例；

[0036] —D部分描述用于对应用传送控制器进行虚拟化的系统和方法的实施例。

[0037] —E部分描述用于提供多核架构和环境的系统和方法的实施例；以及

[0038] —F部分描述用于提供策略组以控制对资源的访问的系统和方法的实施例。

[0039] A.网络和计算环境

[0040] 在讨论设备和/或客户机的系统和方法的实施例的细节之前，讨论可在其中部署这些实施例的网络和计算环境是有帮助的。现在参见图1A，描述了网络环境的实施例。概括来讲，网络环境包括经由一个或多个网络104、104'（总的称为网络104）与一个或多个服务器106a－106n（同样总的称为服务器106，或远程机器106）通信的一个或多个客户机102a－102n（同样总的称为本地机器102，或客户机102）。在一些实施例中，客户机102通过设备200

与服务器106通信。

[0041] 虽然图1A示出了在客户机102和服务器106之间的网络104和网络104’，客户机102和服务器106可以位于同一个的网络104上。网络104和104’可以是相同类型的网络或不同类型的网络。网络104和/或104’可为局域网(LAN)例如公司内网，城域网(MAN)，或者广域网(WAN)例如因特网或万维网。在一个实施例中，网络104可为专用网络并且网络104’可为公网。在一些实施例中，网络104可为专用网并且网络104’可为公网。在又一个实施例中，网络104和104’可都为专用网。在一些实施例中，客户机102可位于公司企业的分支机构中，通过网络104上的WAN连接与位于公司数据中心的服务器106通信。

[0042] 网络104和/或104’可以是任何类型和/或形式的网络，并且可包括任何下述网络：点对点网络，广播网络，广域网，局域网，电信网络，数据通信网络，计算机网络，ATM(异步传输模式)网络，SONET(同步光纤网络)网络，SDH(同步数字体系)网络，无线网络和有线网络。在一些实施例中，网络104可以包括无线链路，诸如红外信道或者卫星频带。网络104和/或104’的拓扑可为总线型、星型或环型网络拓扑。网络104和/或104’以及网络拓扑可以是对于本领域普通技术人员所熟知的、可以支持此处描述的操作的任何这样的网络或网络拓扑。

[0043] 如图1A所示，设备200被显示在网络104和104’之间，设备200也可被称为接口单元200或者网关200。在一些实施例中，设备200可位于网络104上。例如，公司的分支机构可在分支机构中部署设备200。在其他实施例中，设备200可以位于网络104’上。例如，设备200可位于公司的数据中心。在又一个实施例中，多个设备200可在网络104上部署。在一些实施例中，多个设备200可部署在网络104’上。在一个实施例中，第一设备200与第二设备200’通信。在其他实施例中，设备200可为位于与客户机102同一或不同网络104、104’的任一客户机102或服务器106的一部分。一个或多个设备200可位于客户机102和服务器106之间的网络或网络通信路径中的任一点。

[0044] 在一些实施例中，设备200包括由位于佛罗里达州Ft.Lauderdale的Citrix Systems公司制造的被称为Citrix NetScaler设备的任何网络设备。在其他实施例中，设备200包括由位于华盛顿州西雅图的F5Networks公司制造的被称为WebAccelerator和BigIP的任何一个产品实施例。在又一个实施例中，设备205包括由位于加利福尼亚州Sunnyvale的Juniper Networks公司制造的DX加速设备平台和/或诸如SA700、SA2000、SA4000和SA6000的SSL VPN系列设备中的任何一个。在又一个实施例中，设备200包括由位于加利福尼亚州San Jose的Cisco Systems公司制造的任何应用加速和/或安全相关的设备和/或软件，例如Cisco ACE应用控制引擎模块服务(Application Control Engine Module service)软件和网络模块以及Cisco AVS系列应用速度系统(Application Velocity System)。

[0045] 在一个实施例中，系统可包括多个逻辑分组的服务器106。在这些实施例中，服务器的逻辑分组可以被称为服务器群38。在其中一些实施例中，服务器106可为地理上分散的。在一些情况中，群38可以作为单个实体被管理。在其他实施例中，服务器群38包括多个服务器群38。在一个实施例中，服务器群代表一个或多个客户机102执行一个或多个应用程序。

[0046] 在每个群38中的服务器106可为不同种类。一个或多个服务器106可根据一种类型

的操作系统平台(例如,由华盛顿州Redmond的Microsoft公司制造的WINDOWS NT)操作,而一个或多个其它服务器106可根据另一类型的操作系统平台(例如,Unix或Linux)操作。每个群38的服务器106不需要与同一群38内的另一个服务器106物理上接近。因此,被逻辑分组为群38的服务器106组可使用广域网(WAN)连接或城域网(MAN)连接互联。例如,群38可包括物理上位于不同大陆或大陆的不同区域、国家、州、城市、校园或房间的服务器106。如果使用局域网(LAN)连接或一些直连形式来连接服务器106,则可增加群38中的服务器106间的数据传送速度。

[0047] 服务器106可指文件服务器、应用服务器、web服务器、代理服务器或者网关服务器。在一些实施例中,服务器106可以有作为应用服务器或者作为主应用服务器工作的能力。在一个实施例中,服务器106可包括活动目录。客户机102也可称为客户端节点或端点。在一些实施例中,客户机102可以有作为客户机节点寻求访问服务器上的应用的能力,也可以有作为应用服务器为其它客户机102a-102n提供对寄载的应用的访问的能力。

[0048] 在一些实施例中,客户机102与服务器106通信。在一个实施例中,客户机102与群38中的服务器106的其中一个直接通信。在又一个实施例中,客户机102执行程序邻近应用(program neighborhood application)以与群38内的服务器106通信。在又一个实施例中,服务器106提供主节点的功能。在一些实施例中,客户机102通过网络104与群38中的服务器106通信。通过网络104,客户机102例如可以请求执行群38中的服务器106a-106n寄载的各种应用,并接收应用执行结果的输出进行显示。在一些实施例中,只有主节点提供识别和提供与寄载所请求的应用的服务器106'相关的地址信息所需的功能。

[0049] 在一个实施例中,服务器106提供web服务器的功能。在又一个实施例中,服务器106a接收来自客户机102的请求,将该请求转发到第二服务器106b,并使用来自服务器106b对该请求的响应来对客户机102的请求进行响应。在又一个实施例中,服务器106获得客户机102可用的应用的列举以及与由该应用的列举所识别的应用的服务器106相关的地址信息。在又一个实施例中,服务器106使用web接口将对请求的响应提供给客户机102。在一个实施例中,客户机102直接与服务器106通信以访问所识别的应用。在又一个实施例中,客户机102接收由执行服务器106上所识别的应用而产生的诸如显示数据的应用输出数据。

[0050] 现参考图1B,描述了部署多个设备200的网络环境的实施例。第一设备200可以部署在第一网络104上,而第二设备200'部署在第二网络104'上。例如,公司可以在分支机构部署第一设备200,而在数据中心部署第二设备200'。在又一个实施例中,第一设备200和第二设备200'被部署在同一个网络104或网络104上。例如,第一设备200可以被部署用于第一服务器群38,而第二设备200可以被部署用于第二服务器群38'。在另一个实例中,第一设备200可以被部署在第一分支机构,而第二设备200'被部署在第二分支机构'。在一些实施例中,第一设备200和第二设备200'彼此协同或联合工作,以加速客户机和服务器之间的网络流量或应用和数据的传送。

[0051] 现参考图1C,描述了网络环境的又一个实施例,在该网络环境中,将设备200和一个或多个其它类型的设备部署在一起,例如,部署在一个或多个WAN优化设备205,205'之间。例如,第一WAN优化设备205显示在网络104和104'之间,而第二WAN优化设备205'可以部署在设备200和一个或多个服务器106之间。例如,公司可以在分支机构部署第一WAN优化设备205,而在数据中心部署第二WAN优化设备205'。在一些实施例中,设备205可以位于网络

104'上。在其他实施例中，设备205'可以位于网络104上。在一些实施例中，设备205'可以位于网络104'或网络104"上。在一个实施例中，设备205和205'在同一个网络上。在又一个实施例中，设备205和205'在不同的网络上。在另一个实例中，第一WAN优化设备205可以被部署用于第一服务器群38，而第二WAN优化设备205'可以被部署用于第二服务器群38'。

[0052] 在一个实施例中，设备205是用于加速、优化或者以其他方式改善任何类型和形式的网络流量(例如去往和/或来自WAN连接的流量)的性能、操作或服务质量的装置。在一些实施例中，设备205是一个性能增强代理。在其他实施例中，设备205是任何类型和形式的WAN优化或加速装置，有时也被称为WAN优化控制器。在一个实施例中，设备205是由位于佛罗里达州Ft.Lauderdale的Citrix Systems公司出品的被称为WANScaler的产品实施例中的任何一种。在其他实施例中，设备205包括由位于华盛顿州Seattle的F5Networks公司出品的被称为BIG-IP链路控制器和WANjet的产品实施例中的任何一种。在又一个实施例中，设备205包括由位于加利福尼亚州Sunnyvale的Juniper NetWorks公司出品的WX和WXC WAN加速装置平台中的任何一种。在一些实施例中，设备205包括由加利福尼亚州San Francisco的Riverbed Technology公司出品的虹鳟(steelhead)系列WAN优化设备中的任何一种。在其他实施例中，设备205包括由位于新泽西州Roseland的Expand Networks公司出品的WAN相关装置中的任何一种。在一个实施例中，设备205包括由位于加利福尼亚州Cupertino的Packeteer公司出品的任何一种WAN相关设备，例如由Packeteer提供的PacketShaper、iShared和SkyX产品实施例。在又一个实施例中，设备205包括由位于加利福尼亚州San Jose的Cisco Systems公司出品的任何WAN相关设备和/或软件，例如Cisco广域网应用服务软件和网络模块以及广域网引擎设备。

[0053] 在一个实施例中，设备205为分支机构或远程办公室提供应用和数据加速服务。在一个实施例中，设备205包括广域文件服务(WAFS)的优化。在又一个实施例中，设备205加速文件的传送，例如经由通用互联网文件系统(CIFS)协议。在其他实施例中，设备205在存储器和/或存储装置中提供高速缓存来加速应用和数据的传送。在一个实施例中，设备205在任何级别的网络堆栈或在任何的协议或网络层中提供网络流量的压缩。在又一个实施例中，设备205提供传输层协议优化、流量控制、性能增强或修改和/或管理，以加速WAN连接上的应用和数据的传送。例如，在一个实施例中，设备205提供传输控制协议(TCP)优化。在其他实施例中，设备205提供对于任何会话或应用层协议的优化、流量控制、性能增强或修改和/或管理。

[0054] 在又一个实施例中，设备205将任何类型和形式的数据或信息编码成网络分组的定制的或标准的TCP和/或IP的报头字段或可选字段，以将其存在、功能或能力通告给另一个设备205'。在又一个实施例中，设备205'可以使用在TCP和/或IP报头字段或选项中编码的数据来与另一个设备205'进行通信。例如，设备可以使用TCP选项或IP报头字段或选项来传达在执行诸如WAN加速的功能时或者为了彼此联合工作而由设备205，205'所使用的一个或多个参数。

[0055] 在一些实施例中，设备200保存在设备205和205'之间传达的TCP和/或IP报头和/或可选字段中编码的任何信息。例如，设备200可以终止经过设备200的传输层连接，例如经过设备205和205'的在客户机和服务器之间的一个传输层连接。在一个实施例中，设备200识别并保存由第一设备205通过第一传输层连接发送的传输层分组中的任何编码信息，并

经由第二传输层连接来将具有编码信息的传输层分组传达到第二设备205'。

[0056] 现参考图1D,描述了用于传送和/或操作客户机102上的计算环境的网络环境。在一些实施例中,服务器106包括用于向一个或多个客户机102传送计算环境或应用和/或数据文件的应用传送系统190。总的来说,客户机10通过网络104、104'和设备200与服务器106通信。例如,客户机102可驻留在公司的远程办公室里,例如分支机构,并且服务器106可驻留在公司数据中心。客户机102包括客户机代理120以及计算环境15。计算环境15可执行或操作用于访问、处理或使用数据文件的应用。可经由设备200和/或服务器106传送计算环境15、应用和/或数据文件。

[0057] 在一些实施例中,设备200加速计算环境15或者其任何部分到客户机102的传送。在一个实施例中,设备200通过应用传送系统190加速计算环境15的传送。例如,可使用此处描述的实施例来加速从公司中央数据中心到远程用户位置(例如公司的分支机构)的流应用(streaming application)及该应用可处理的数据文件的传送。在又一个实施例中,设备200加速客户机102和服务器106之间的传输层流量。设备200可以提供用于加速从服务器106到客户机102的任何传输层有效载荷的加速技术,例如:1)传输层连接池,2)传输层连接多路复用,3)传输控制协议缓冲,4)压缩和5)高速缓存。在一些实施例中,设备200响应于来自客户机102的请求提供服务器106的负载平衡。在其他实施例中,设备200充当代理或者访问服务器来提供对一个或者多个服务器106的访问。在又一个实施例中,设备200提供从客户机102的第一网络104到服务器106的第二网络104'的安全虚拟专用网络连接,诸如SSL VPN连接。在又一些实施例中,设备200提供客户机102和服务器106之间的连接和通信的应用防火墙安全、控制和管理。

[0058] 在一些实施例中,基于多个执行方法并且基于通过策略引擎195所应用的任一验证和授权策略,应用传送管理系统190提供将计算环境传送到远程的或者另外的用户的桌面的应用传送技术。使用这些技术,远程用户可以从任何网络连接装置100获取计算环境并且访问服务器所存储的应用和数据文件。在一个实施例中,应用传送系统190可驻留在服务器106上或在其上执行。在又一个实施例中,应用传送系统190可驻留在多个服务器106a-106n上或在其上执行。在一些实施例中,应用传送系统190可在服务器群38内执行。在一个实施例中,执行应用传送系统190的服务器106也可存储或提供应用和数据文件。在又一个实施例中,一个或多个服务器106的第一组可执行应用传送系统190,而不同的服务器106n可存储或提供应用和数据文件。在一些实施例中,应用传送系统190、应用和数据文件中的每一个可驻留或位于不同的服务器。在又一个实施例中,应用传送系统190的任何部分可驻留、执行、或被存储于或分发到设备200或多个设备。

[0059] 客户机102可包括用于执行使用或处理数据文件的应用的计算环境15。客户机102可通过网络104、104'和设备200请求来自服务器106的应用和数据文件。在一个实施例中,设备200可以将来自客户机102的请求转发到服务器106。例如,客户机102可能不具有本地存储或者本地可访问的应用和数据文件。响应于请求,应用传送系统190和/或服务器106可以传送应用和数据文件到客户机102。例如,在一个实施例中,服务器106可以把应用作为应用流来传输,以在客户机102上的计算环境15中操作。

[0060] 在一些实施例中,应用传送系统190包括Citrix Systems有限公司的Citrix Access Suite™的任一部分(例如MetaFrame或Citrix Presentation Server™),和/或微

软公司开发的Microsoft®Windows终端服务中的任何一个。在一个实施例中，应用传送系统190可以通过远程显示协议或者以其它方式通过基于远程计算或者基于服务器计算来传送一个或者多个应用到客户机102或者用户。在又一个实施例中，应用传送系统190可以通过应用流来传送一个或者多个应用到客户机或者用户。

[0061] 在一个实施例中，应用传送系统190包括策略引擎195，其用于控制和管理对应用的访问、应用执行方法的选择以及应用的传送。在一些实施例中，策略引擎195确定用户或者客户机102可以访问的一个或者多个应用。在又一个实施例中，策略引擎195确定应用应该如何被传送到用户或者客户机102，例如执行方法。在一些实施例中，应用传送系统190提供多个传送技术，从中选择应用执行的方法，例如基于服务器的计算、本地流式传输或传送应用给客户机120以用于本地执行。

[0062] 在一个实施例中，客户机102请求应用程序的执行并且包括服务器106的应用传送系统190选择执行应用程序的方法。在一些实施例中，服务器106从客户机102接收证书。在又一个实施例中，服务器106从客户机102接收对于可用应用的列举的请求。在一个实施例中，响应该请求或者证书的接收，应用传送系统190列举对于客户机102可用的多个应用程序。应用传送系统190接收执行所列举的应用的请求。应用传送系统190选择预定数量的方法之一来执行所列举的应用，例如响应策略引擎的策略。应用传送系统190可以选择执行应用的方法，使得客户机102接收通过执行服务器106上的应用程序所产生的应用输出数据。应用传送系统190可以选择执行应用的方法，使得本地机器10在检索包括应用的多个应用文件之后本地执行应用程序。在又一个实施例中，应用传送系统190可以选择执行应用的方法，以通过网络104流式传输应用到客户机102。

[0063] 客户机102可以执行、操作或者以其它方式提供应用，所述应用可为任何类型和/或形式的软件、程序或者可执行指令，例如任何类型和/或形式的web浏览器、基于web的客户机、客户机－服务器应用、瘦客户端计算客户机、ActiveX控件、或者Java程序、或者可以在客户机102上执行的任何其它类型和/或形式的可执行指令。在一些实施例中，应用可以是代表客户机102在服务器106上执行的基于服务器或者基于远程的应用。在一个实施例中，服务器106可以使用任何瘦-客户端或远程显示协议来显示输出到客户机102，所述瘦-客户端或远程显示协议例如由位于佛罗里达州Ft.Lauderdale的Citrix Systems公司出品的独立计算架构(ICA)协议或由位于华盛顿州Redmond的微软公司出品的远程桌面协议(RDP)。应用可使用任何类型的协议，并且它可为，例如，HTTP客户机、FTP客户机、Oscar客户机或Telnet客户机。在其他实施例中，应用包括和VoIP通信相关的任何类型的软件，例如软IP电话。在进一步的实施例中，应用包括涉及到实时数据通信的任一应用，例如用于流式传输视频和/或音频的应用。

[0064] 在一些实施例中，服务器106或服务器群38可运行一个或多个应用，例如提供瘦客户端计算或远程显示表示应用的应用。在一个实施例中，服务器106或服务器群38作为一个应用来执行Citrix Systems有限公司的Citrix Access Suite™的任一部分(例如MetaFrame或Citrix Presentation Server™)，和/或微软公司开发的Microsoft®Windows终端服务中的任何一个。在一个实施例中，该应用是位于佛罗里达州Fort Lauderdale的Citrix Systems有限公司开发的ICA客户机。在其他实施例中，该应用包括由位于华盛顿州Redmond的Microsoft公司开发的远程桌面(RDP)客户机。另外，服务器106可以运行一个应

用，例如，其可以是提供电子邮件服务的应用服务器，例如由位于华盛顿州Redmond的Microsoft公司制造的Microsoft Exchange，web或Internet服务器，或者桌面共享服务器，或者协作服务器。在一些实施例中，任一应用可以包括任一类型的所寄载的服务或产品，例如位于加利福尼亚州Santa Barbara的Citrix Online Division公司提供的GoToMeeting™，位于加利福尼亚州Santa Clara的WebEx有限公司提供的WebEx™，或者位于华盛顿州Redmond的Microsoft公司提供的Microsoft Office Live Meeting。

[0065] 仍参考图1D，网络环境的一个实施例可以包括监控服务器106A。监控服务器106A可以包括任何类型和形式的性能监控服务198。性能监控服务198可以包括监控、测量和/或管理软件和/或硬件，包括数据收集、集合、分析、管理和报告。在一个实施例中，性能监控服务198包括一个或多个监控代理197。监控代理197包括用于在诸如客户机102、服务器106或设备200和205的装置上执行监控、测量和数据收集活动的任何软件、硬件或其组合。在一些实施例中，监控代理197包括诸如Visual Basic脚本或Javascript任何类型和形式的脚本。在一个实施例中，监控代理197相对于装置的任何应用和/或用户透明地执行。在一些实施例中，监控代理197相对于应用或客户机不显眼地被安装和操作。在又一个实施例中，监控代理197的安装和操作不需要用于该应用或装置的任何设备。

[0066] 在一些实施例中，监控代理197以预定频率监控、测量和收集数据。在其他实施例中，监控代理197基于检测到任何类型和形式的事件来监控、测量和收集数据。例如，监控代理197可以在检测到对web页面的请求或收到HTTP响应时收集数据。在另一个实例中，监控代理197可以在检测到诸如鼠标点击的任一用户输入事件时收集数据。监控代理197可以报告或提供任何所监控、测量或收集的数据给监控服务198。在一个实施例中，监控代理197根据时间安排或预定频率来发送信息给监控服务198。在又一个实施例中，监控代理197在检测到事件时发送信息给监控服务198。

[0067] 在一些实施例中，监控服务198和/或监控代理197对诸如客户机、服务器、服务器群、设备200、设备205或网络连接的任何网络资源或网络基础结构元件的进行监控和性能测量。在一个实施例中，监控服务198和/或监控代理197执行诸如TCP或UDP连接的任何传输层连接的监控和性能测量。在又一个实施例中，监控服务198和/或监控代理197监控和测量网络等待时间。在又一个实施例中，监控服务198和/或监控代理197监控和测量带宽利用。

[0068] 在其他实施例中，监控服务198和/或监控代理197监控和测量终端用户响应时间。在一些实施例中，监控服务198执行应用的监控和性能测量。在又一个实施例中，监控服务198和/或监控代理197执行到应用的任何会话或连接的监控和性能测量。在一个实施例中，监控服务198和/或监控代理197监控和测量浏览器的性能。在又一个实施例中，监控服务198和/或监控代理197监控和测量基于HTTP的事务的性能。在一些实施例中，监控服务198和/或监控代理197监控和测量IP电话(VoIP)应用或会话的性能。在其他实施例中，监控服务198和/或监控代理197监控和测量诸如ICA客户机或RDP客户机的远程显示协议应用的性能。在又一个实施例中，监控服务198和/或监控代理197监控和测量任何类型和形式的流媒体的性能。在进一步的实施例中，监控服务198和/或监控代理197监控和测量所寄载的应用或软件即服务(Software-As-A-Service，SaaS)传送模型的性能。

[0069] 在一些实施例中，监控服务198和/或监控代理197执行与应用相关的一个或多个事务、请求或响应的监控和性能测量。在其他实施例中，监控服务198和/或监控代理197监

控和测量应用层堆栈的任何部分，例如任何.NET或J2EE调用。在一个实施例中，监控服务198和/或监控代理197监控和测量数据库或SQL事务。在又一个实施例中，监控服务198和/或监控代理197监控和测量任何方法、函数或应用编程接口(API)调用。

[0070] 在一个实施例中，监控服务198和/或监控代理197对经由诸如设备200和/或设备205的一个或多个设备从服务器到客户机的应用和/或数据的传送进行监控和性能测量。在一些实施例中，监控服务198和/或监控代理197监控和测量虚拟化应用的传送的性能。在其他实施例中，监控服务198和/或监控代理197监控和测量流式应用的传送的性能。在又一个实施例中，监控服务198和/或监控代理197监控和测量传送桌面应用到客户机和/或在客户机上执行桌面应用的性能。在又一个实施例中，监控服务198和/或监控代理197监控和测量客户机/服务器应用的性能。

[0071] 在一个实施例中，监控服务198和/或监控代理197被设计和构建成为应用传送系统190提供应用性能管理。例如，监控服务198和/或监控代理197可以监控、测量和管理经由Citrix表示服务器(Citrix Presentation Server)传送应用的性能。在该实例中，监控服务198和/或监控代理197监控单独的ICA会话。监控服务198和/或监控代理197可以测量总的以及每次的会话系统资源使用，以及应用和连网性能。监控服务198和/或监控代理197可以对于给定用户和/或用户会话来标识有效服务器(active server)。在一些实施例中，监控服务198和/或监控代理197监控在应用传送系统190和应用和/或数据库服务器之间的后端连接。监控服务198和/或监控代理197可以测量每个用户会话或ICA会话的网络等待时间、延迟和容量。

[0072] 在一些实施例中，监控服务198和/或监控代理197测量和监控对于应用传送系统190的诸如总的存储器使用、每个用户会话和/或每个进程的存储器使用。在其他实施例中，监控服务198和/或监控代理197测量和监控诸如总的CPU使用、每个用户会话和/或每个进程的应用传送系统190的CPU使用。在又一个实施例中，监控服务198和/或监控代理197测量和监控登录到诸如Citrix表示服务器的应用、服务器或应用传送系统所需的时间。在一个实施例中，监控服务198和/或监控代理197测量和监控用户登录应用、服务器或应用传送系统190的持续时间。在一些实施例中，监控服务198和/或监控代理197测量和监控应用、服务器或应用传送系统会话的有效和无效的会话计数。在又一个实施例中，监控服务198和/或监控代理197测量和监控用户会话等待时间。

[0073] 在另外的实施例中，监控服务198和/或监控代理197测量和监控任何类型和形式的服务器指标。在一个实施例中，监控服务198和/或监控代理197测量和监控与系统内存、CPU使用和盘存储器有关的指标。在又一个实施例中，监控服务198和/或监控代理197测量和监控和页错误有关的指标，诸如每秒页错误。在其他实施例中，监控服务198和/或监控代理197测量和监控往返时间的指标。在又一个实施例中，监控服务198和/或监控代理197测量和监控与应用崩溃、错误和/或中止相关的指标。

[0074] 在一些实施例中，监控服务198和监控代理198包括由位于佛罗里达州Ft.Lauderdale的Citrix Systems公司出品的被称为EdgeSight的任何一种产品实施例。在又一个实施例中，性能监控服务198和/或监控代理198包括由位于加利福尼亚州Palo Alto的Symphoniq公司出品的被称为TrueView产品套件的产品实施例的任一部分。在一个实施例中，性能监控服务198和/或监控代理198包括由位于加利福尼亚州San Francisco的

TeaLeaf技术公司出品的被称为TeaLeafCX产品套件的产品实施例的任何部分。在其他实施例中，性能监控服务198和/或监控代理198包括由位于德克萨斯州Houston的BMC软件公司出品的诸如BMC性能管理器和巡逻产品(BMC Performance Manager and Patrol products)的商业服务管理产品的任何部分。

[0075] 客户机102、服务器106和设备200可以被部署为和/或执行在任何类型和形式的计算装置上，诸如能够在任何类型和形式的网络上通信并执行此处描述的操作的计算机、网络装置或者设备。图1E和1F描述了可用于实施客户机102、服务器106或设备200的实施例的计算装置100的框图。如图1E和1F所示，每个计算装置100包括中央处理单元101和主存储器单元122。如图1E所示，计算装置100可以包括可视显示装置124、键盘126和/或诸如鼠标的指示装置127。每个计算装置100也可包括其它可选元件，例如一个或多个输入/输出装置130a－130b(总的使用附图标记130表示)，以及与中央处理单元101通信的高速缓存存储器140。

[0076] 中央处理单元101是响应并处理从主存储器单元122取出的指令的任何逻辑电路。在许多实施例中，中央处理单元由微处理器单元提供，例如：由加利福尼亚州Mountain View的Intel公司制造的微处理器单元；由伊利诺伊州Schaumburg的Motorola公司制造的微处理器单元；由加利福尼亚州Santa Clara的Transmeta公司制造的微处理器单元；由纽约州White Plains的International Business Machines公司制造的RS/6000处理器；或者由加利福尼亚州Sunnyvale的Advanced Micro Devices公司制造的微处理器单元。计算装置100可以基于这些处理器中的任何一种，或者能够如此处所述方式运行的任何其它处理器。

[0077] 主存储器单元122可以是能够存储数据并允许微处理器101直接访问任何存储位置的一个或多个存储器芯片，例如静态随机存取存储器(SRAM)、突发SRAM或同步突发SRAM(BSRAM)、动态随机存取存储器DRAM、快速页模式DRAM(FPM DRAM)、增强型DRAM(EDRAM)、扩展数据输出RAM(EDO RAM)、扩展数据输出DRAM(EDO DRAM)、突发式扩展数据输出DRAM(BEDO DRAM)、增强型DRAM(EDRAM)、同步DRAM(SDRAM)、JEDEC SRAM、PC100SDRAM、双数据速率SDRAM(DDR SDRAM)、增强型SRAM(ESDRAM)、同步链路DRAM(SLDRAM)、直接内存总线DRAM(DRDRAM)或铁电RAM(FRAM)。主存储器122可以基于上述存储芯片的任何一种，或者能够如此处所述方式运行的任何其它可用存储芯片。在图1E中所示的实施例中，处理器101通过系统总线150(在下面进行更详细的描述)与主存储器122进行通信。图1E描述了在其中处理器通过存储器端口103直接与主存储器122通信的计算装置100的实施例。例如，在图1F中，主存储器122可以是DRDRAM。

[0078] 图1F描述了在其中主处理器101通过第二总线与高速缓存存储器140直接通信的实施例，第二总线有时也称为后端总线。其他实施例中，主处理器101使用系统总线150和高速缓存存储器140通信。高速缓存存储器140通常有比主存储器122更快的响应时间，并且通常由SRAM、BSRAM或EDRAM提供。在图1F中所示的实施例中，处理器101通过本地系统总线150与多个I/O装置130进行通信。可以使用各种不同的总线将中央处理单元101连接到任何I/O装置130，所述总线包括VESA VL总线、ISA总线、EISA总线、微通道体系结构(MCA)总线、PCI总线、PCI-X总线、PCI-Express总线或NuBus。对于I/O装置是视频显示器124的实施例，处理器101可以使用高级图形端口(AGP)与显示器124通信。图1F说明了主处理器101通过超传输

(HyperTransport)、快速I/O或者InfiniBand直接与I/O装置130通信的计算机100的一个实施例。图1F还描述了在其中混合本地总线和直接通信的实施例:处理器101使用本地互连总线与I/O装置130b进行通信,同时直接与I/O装置130a进行通信。

[0079] 计算装置100可以支持任何适当的安装装置116,例如用于接纳诸如3.5英寸、5.25英寸磁盘或ZIP磁盘这样的软盘的软盘驱动器、CD-ROM驱动器、CD-R/RW驱动器、DVD-ROM驱动器、各种格式的磁带驱动器、USB装置、硬盘驱动器或适于安装像任何客户机代理120或其部分的软件和程序的任何其它装置。计算装置100还可以包括存储装置128,诸如一个或者多个硬盘驱动器或者独立磁盘冗余阵列,用于存储操作系统和其它相关软件,以及用于存储诸如涉及客户机代理120的任何程序的应用软件程序。或者,可以使用安装装置116的任何一种作为存储装置128。此外,操作系统和软件可从例如可引导CD的可引导介质运行,诸如KNOPPIX®,一种用于GNU/Linux的可引导CD,该可引导CD可自knoppix.net作为GNU/Linux一个分发版获得。

[0080] 此外,计算装置100可以包括通过多种连接接口到局域网(LAN)、广域网(WAN)或因特网的网络接口118,所述多种连接包括但不限于标准电话线路、LAN或WAN链路(例如802.11,T1,T3、56kb、X.25)、宽带连接(如ISDN、帧中继、ATM)、无线连接、或上述任何或所有连接的一些组合。网络接口118可以包括内置网络适配器、网络接口卡、PCMCIA网络卡、卡总线网络适配器、无线网络适配器、USB网络适配器、调制解调器或适用于将计算装置100接口到能够通信并执行这里所说明的操作的任何类型的网络的任何其它设备。

[0081] 计算装置100中可以包括各种I/O装置130a-130n。输入装置包括键盘、鼠标、触控板、轨迹球、麦克风和绘图板。输出装置包括视频显示器、扬声器、喷墨打印机、激光打印机和热升华打印机。如图1E所示,I/O装置130可以由I/O控制器123控制。I/O控制器可以控制一个或多个I/O装置,例如键盘126和指示装置127(如鼠标或光笔)。此外,I/O装置还可以为计算装置100提供存储装置128和/或安装介质116。在其他实施例中,计算装置100可以提供USB连接以接纳手持USB存储装置,例如由位于美国加利福尼亚州Los Alamitos的Twintech Industry有限公司生产的USB闪存驱动驱动系列装置。

[0082] 在一些实施例中,计算装置100可以包括多个显示装置124a-124n或与其相连,这些显示装置各自可以是相同或不同的类型和/或形式。因而,任何一种I/O装置130a-130n和/或I/O控制器123可以包括任一类型和/或形式的适当的硬件、软件或硬件和软件的组合,以支持、允许或提供通过计算装置100连接和使用多个显示装置124a-124n。例如,计算装置100可以包括任何类型和/或形式的视频适配器、视频卡、驱动器和/或库,以与显示装置124a-124n接口、通信、连接或以其他方式使用显示装置。在一个实施例中,视频适配器可以包括多个连接器以与多个显示装置124a-124n接口。在其他实施例中,计算装置100可以包括多个视频适配器,每个视频适配器与显示装置124a-124n中的一个或多个连接。在一些实施例中,计算装置100的操作系统的任一部分都可以被配置用于使用多个显示器124a-124n。在其他实施例中,显示装置124a-124n中的一个或多个可以由一个或多个其它计算装置提供,诸如例如通过网络与计算装置100连接的计算装置100a和100b。这些实施例可以包括被设计和构造为将另一个计算机的显示装置用作计算装置100的第二显示装置124a的任一类型的软件。本领域的普通技术人员应认识和理解可以将计算装置100配置成具有多个显示装置124a-124n的各种方法和实施例。

[0083] 在另外的实施例中，I/O装置130可以是系统总线150和外部通信总线之间的桥170，所述外部通信总线例如USB总线、Apple桌面总线、RS-232串行连接、SCSI总线、FireWire总线、FireWire800总线、以太网总线、AppleTalk总线、千兆位以太网总线、异步传输模式总线、HIPPI总线、超级HIPPI总线、SerialPlus总线、SCI/LAMP总线、光纤信道总线或串行SCSI总线。

[0084] 图1E和1F中描述的那类计算装置100通常在控制任务的调度和对系统资源的访问的操作系统的控制下操作。计算装置100可以运行任何操作系统，如Microsoft®Windows操作系统，不同发行版本的Unix和Linux操作系统，用于Macintosh计算机的任何版本的MAC OS®，任何嵌入式操作系统，任何实时操作系统，任何开源操作系统，任何专有操作系统，任何用于移动计算装置的操作系统，或者任何其它能够在计算装置上运行并完成这里所述操作的操作系统。典型的操作系统包括：WINDOWS3.x、WINDOWS95、WINDOWS98、WINDOWS2000、WINDOWS NT3.51、WINDOWS NT4.0、WINDOWS CE和WINDOWS XP，所有这些均由位于华盛顿州Redmond的微软公司出品；由位于加利福尼亚州Cupertino的苹果计算机出品的MacOS；由位于纽约州Armonk的国际商业机器公司出品的OS/2；以及由位于犹他州Salt Lake City的Caldera公司发布的可免费使用的Linux操作系统或者任何类型和/或形式的Unix操作系统，以及其它。

[0085] 在其他的实施例中，计算装置100可以有符合该装置的不同的处理器、操作系统和输入设备。例如，在一个实施例中，计算机100是由Palm公司出品的Treo180、270、1060、600或650智能电话。在该实施例中，Treo智能电话在PalmOS操作系统的控制下操作，并包括指示笔输入装置以及五向导航装置。此外，计算装置100可以是任何工作站、桌面计算机、膝上型或笔记本计算机、服务器、手持计算机、移动电话、任何其它计算机、或能够通信并有足够的处理器能力和存储容量以执行此处所述的操作的其它形式的计算或者电信装置。

[0086] 如图1G所示，计算装置100可以包括多个处理器，可以提供用于对不只一个数据片同时执行多个指令或者同时执行一个指令的功能。在一些实施例中，计算装置100可包括具有一个或多个核的并行处理器。在这些实施例的一个中，计算装置100是共享内存并行设备，具有多个处理器和/或多个处理器核，将所有可用内存作为一个全局地址空间进行访问。在这些实施例的又一个中，计算装置100是分布式存储器并行设备，具有多个处理器，每个处理器访问本地存储器。在这些实施例的又一个中，计算装置100既有共享的存储器又有仅由特定处理器或处理器子集访问的存储器。在这些实施例的又一个中，如多核微处理器的计算装置100将两个或多个独立处理器组合在一个封装中，通常在一个集成电路(IC)中。在这些实施例的又一个中，计算装置100包括具有单元宽带引擎(CELL BROADBAND ENGINE)架构的芯片，并包括高能处理器单元以及多个协同处理单元，高能处理器单元和多个协同处理单元通过内部高速总线连接在一起，可以将内部高速总线称为单元互连总线。

[0087] 在一些实施例中，处理器提供用于对多个数据片同时执行单个指令(SIMD)的功能。其他实施例中，处理器提供用于对多个数据片同时执行多个指令(MIMD)的功能。又一个实施例中，处理器可以在单个装置中使用SIMD和MIMD核的任意组合。

[0088] 在一些实施例中，计算装置100可包括图像处理单元。图1H所示的在这些实施例的一个中，计算装置100包括至少一个中央处理单元101和至少一个图像处理单元。在这些实施例的又一个中，计算装置100包括至少一个并行处理单元和至少一个图像处理单元。在这

些实施例的又一个中，计算装置100包括任意类型的多个处理单元，多个处理单元中的一个包括图像处理单元。

[0089] 一些实施例中，第一计算装置100a代表客户计算装置100b的用户执行应用。又一个实施例中，计算装置100执行虚拟机，其提供执行会话，在该会话中，代表客户计算装置100b的用户执行应用。在这些实施例的一个中，执行会话是寄载的桌面会话。在这些实施例的又一个中，计算装置100执行终端服务会话。终端服务会话可以提供寄载的桌面环境。在这些实施例的又一个中，执行会话提供对计算环境的访问，该计算环境可包括以下的一个或多个：应用、多个应用、桌面应用以及可执行一个或多个应用的桌面会话。

[0090] B.设备架构

[0091] 图2A示出设备200的一个示例实施例。提供图2A的设备200架构仅用于示例，并不意于作为限制性的架构。如图2所示，设备200包括硬件层206和被分为用户空间202和内核空间204的软件层。

[0092] 硬件层206提供硬件元件，在内核空间204和用户空间202中的程序和服务在该硬件元件上被执行。硬件层206也提供结构和元件，就设备200而言，这些结构和元件允许在内核空间204和用户空间202内的程序和服务既在内部进行数据通信又与外部进行数据通信。如图2所示，硬件层206包括用于执行软件程序和服务的处理单元262，用于存储软件和数据的存储器264，用于通过网络传输和接收数据的网络端口266，以及用于执行与安全套接字协议层相关的功能处理通过网络传输和接收的数据的加密处理器260。在一些实施例中，中央处理单元262可在单独的处理器中执行加密处理器260的功能。另外，硬件层206可包括用于每个处理单元262和加密处理器260的多处理器。处理器262可以包括以上结合图1E和1F所述的任一处理器101。例如，在一个实施例中，设备200包括第一处理器262和第二处理器262'。在其他实施例中，处理器262或者262'包括多核处理器。

[0093] 虽然示出的设备200的硬件层206通常带有加密处理器260，但是处理器260可为执行涉及任何加密协议的功能的处理器，例如安全套接字协议层(SSL)或者传输层安全(TLS)协议。在一些实施例中，处理器260可为通用处理器(GPP)，并且在进一步的实施例中，可为用于执行任何安全相关协议处理的可执行指令。

[0094] 虽然图2中设备200的硬件层206包括了某些元件，但是设备200的硬件部分或组件可包括计算装置的任何类型和形式的元件、硬件或软件，例如此处结合图1E和1F示出和讨论的计算装置100。在一些实施例中，设备200可包括服务器、网关、路由器、开关、桥接器或其它类型的计算或网络设备，并且拥有与此相关的任何硬件和/或软件元件。

[0095] 设备200的操作系统分配、管理或另外分离可用的系统存储器到内核空间204和用户空间204。在示例的软件架构200中，操作系统可以是任何类型和/或形式的Unix操作系统，尽管本发明并未这样限制。这样，设备200可以运行任何操作系统，如任何版本的Microsoft®Windows操作系统、不同版本的Unix和Linux操作系统、用于Macintosh计算机的任何版本的MacOS®、任何的嵌入式操作系统、任何的网络操作系统、任何的实时操作系统、任何的开放源操作系统、任何的专用操作系统、用于移动计算装置或网络装置的任何操作系统、或者能够运行在设备200上并执行此处所描述的操作的任何其它操作系统。

[0096] 保留内核空间204用于运行内核230，内核230包括任何设备驱动器，内核扩展或其他内核相关软件。就像本领域技术人员所知的，内核230是操作系统的核心，并提供对资源

以及设备104的相关硬件元件的访问、控制和管理。根据设备200的实施例，内核空间204也包括与高速缓存管理器232协同工作的多个网络服务或进程，高速缓存管理器232有时也称为集成的高速缓存，其益处此处将进一步详细描述。另外，内核230的实施例将依赖于通过设备200安装、配置或其他使用的操作系统的实施例。

[0097] 在一个实施例中，设备200包括一个网络堆栈267，例如基于TCP/IP的堆栈，用于与客户机102和/或服务器106通信。在一个实施例中，使用网络堆栈267与第一网络(例如网络108)以及第二网络110通信。在一些实施例中，设备200终止第一传输层连接，例如客户机102的TCP连接，并建立客户机102使用的到服务器106的第二传输层连接，例如，终止在设备200和服务器106的第二传输层连接。可通过单独的网络堆栈267建立第一和第二传输层连接。在其他实施例中，设备200可包括多个网络堆栈，例如267或267'，并且在一个网络堆栈267可建立或终止第一传输层连接，在第二网络堆栈267'上可建立或者终止第二传输层连接。例如，一个网络堆栈可用于在第一网络上接收和传输网络分组，并且另一个网络堆栈用于在第二网络上接收和传输网络分组。在一个实施例中，网络堆栈267包括用于为一个或多个网络分组进行排队的缓冲器243，其中网络分组由设备200传输。

[0098] 如图2A所示，内核空间204包括高速缓存管理器232、高速层2-7集成分组引擎240、加密引擎234、策略引擎236以及多协议压缩逻辑238。在内核空间204或内核模式而不是用户空间202中运行这些组件或进程232、240、234、236和238提高这些组件中的每个单独的和结合的性能。内核操作意味着这些组件或进程232、240、234、236和238在设备200的操作系统的核地址空间中运行。例如，在内核模式中运行加密引擎234通过移动加密和解密操作到内核可改进加密性能，从而可减少在内核模式中的存储空间或内核线程与在用户模式中的存储空间或线程之间的传输的数量。例如，在内核模式获得的数据可能不需要传输或拷贝到运行在用户模式的进程或线程，例如从内核级数据结构到用户级数据结构。在另一个方面，也可减少内核模式和用户模式之间的上下文切换的数量。另外，在任何组件或进程232、240、235、236和238间的同步和通信在内核空间204中可被执行的更有效率。

[0099] 在一些实施例中，组件232、240、234、236和238的任何部分可在内核空间204中运行或操作，而这些组件232、240、234、236和238的其它部分可在用户空间202中运行或操作。在一个实施例中，设备200使用内核级数据结构来提供对一个或多个网络分组的任何部分的访问，例如，包括来自客户机102的请求或者来自服务器106的响应的网络分组。在一些实施例中，可以由分组引擎240通过到网络堆栈267的传输层驱动器接口或过滤器获得内核级数据结构。内核级数据结构可包括通过与网络堆栈267相关的内核空间204可访问的任何接口和/或数据、由网络堆栈267接收或发送的网络流量或分组。在其他实施例中，任何组件或进程232、240、234、236和238可使用内核级数据结构来执行组件或进程的需要的操作。在一个实例中，当使用内核级数据结构时，组件232、240、234、236和238在内核模式204中运行，而在又一个实施例中，当使用内核级数据结构时，组件232、240、234、236和238在用户模式中运行。在一些实施例中，内核级数据结构可被拷贝或传递到第二内核级数据结构，或任何期望的用户级数据结构。

[0100] 高速缓存管理器232可包括软件、硬件或软件和硬件的任何组合，以提供对任何类型和形式的内容的高速缓存访问、控制和管理，例如对象或由源服务器106提供服务的动态产生的对象。由高速缓存管理器232处理和存储的数据、对象或内容可包括任何格式(例如

标记语言)的数据,或者通过任何协议的通信的任何类型的数据。在一些实施例中,高速缓存管理器232复制存储在其他地方的原始数据或先前计算、产生或传输的数据,其中相对于读高速缓存存储器元件,需要更长的访问时间以取得、计算或以其他方式得到原始数据。一旦数据被存储在高速缓存存储元件中,通过访问高速缓存的副本而不是重新获得或重新计算原始数据即可进行后续操作,因此而减少了访问时间。在一些实施例中,高速缓存元件可以包括设备200的存储器264中的数据对象。在其他实施例中,高速缓存存储元件可包括有比存储器264更快的存取时间的存储器。在又一个实施例中,高速缓存元件可以包括设备200的任一类型和形式的存储元件,诸如硬盘的一部分。在一些实施例中,处理单元262可提供被高速缓存管理器232使用的高速缓存存储器。在又一个实施例中,高速缓存管理器232可使用存储器、存储区或处理单元的任何部分和组合来高速缓存数据、对象或其它内容。

[0101] 另外,高速缓存管理器232包括用于执行此处描述的设备200的技术的任一实施例的任何逻辑、功能、规则或操作。例如,高速缓存管理器232包括基于无效时间周期的终止,或者从客户机102或服务器106接收无效命令使对象无效的逻辑或功能。在一些实施例中,高速缓存管理器232可作为在内核空间204中执行的程序、服务、进程或任务而操作,并且在其他实施例中,在用户空间202中执行。在一个实施例中,高速缓存管理器232的第一部分在用户空间202中执行,而第二部分在内核空间204中执行。在一些实施例中,高速缓存管理器232可包括任何类型的通用处理器(GPP),或任何其他类型的集成电路,例如现场可编程门阵列(FPGA),可编程逻辑设备(PLD),或者专用集成电路(ASIC)。

[0102] 策略引擎236可包括例如智能统计引擎或其它可编程应用。在一个实施例中,策略引擎236提供配置机制以允许用户识别、指定、定义或配置高速缓存策略。策略引擎236,在一些实施例中,也访问存储器以支持数据结构,例如备份表或hash表,以启用用户选择的高速缓存策略决定。在其他实施例中,除了对安全、网络流量、网络访问、压缩或其它任何由设备200执行的功能或操作的访问、控制和管理之外,策略引擎236可包括任何逻辑、规则、功能或操作以确定和提供对设备200所高速缓存的对象、数据、或内容的访问、控制和管理。特定高速缓存策略的其他实施例此处进一步描述。

[0103] 加密引擎234包括用于操控诸如SSL或TLS的任何安全相关协议或其中涉及的任何功能的处理的任何逻辑、商业规则、功能或操作。例如,加密引擎234加密并解密通过设备200传输的网络分组,或其任何部分。加密引擎234也可代表客户机102a-102n、服务器106a-106n或设备200来设置或建立SSL或TLS连接。因此,加密引擎234提供SSL处理的卸载和加速。在一个实施例中,加密引擎234使用隧道协议来提供在客户机102a-102n和服务器106a-106n间的虚拟专用网络。在一些实施例中,加密引擎234与加密处理器260通信。在其他实施例中,加密引擎234包括运行在加密处理器260上的可执行指令。

[0104] 多协议压缩引擎238包括用于压缩一个或多个网络分组协议(例如被设备200的网络堆栈267使用的任何协议)的任何逻辑、商业规则、功能或操作。在一个实施例中,多协议压缩引擎238双向压缩在客户机102a-102n和服务器106a-106n间任一基于TCP/IP的协议,包括消息应用编程接口(MAPI)(电子邮件)、文件传输协议(FTP)、超文本传输协议(HTTP)、通用互联网文件系统(CIFS)协议(文件传输)、独立计算架构(ICA)协议、远程桌面协议(RDP)、无线应用协议(WAP)、移动IP协议以及互联网协议电话(VoIP)协议。在其他实施例中,多协议压缩引擎238提供基于超文本标记语言(HTML)的协议的压缩,并且在一些实施例

中，提供任何标记语言的压缩，例如可扩展标记语言(XML)。在一个实施例中，多协议压缩引擎238提供任何高性能协议的压缩，例如设计用于设备200到设备200通信的任何协议。在又一个实施例中，多协议压缩引擎238使用修改的传输控制协议来压缩任何通信的任何载荷或任何通信，例如事务TCP(T/TCP)、带有选择确认的TCP(TCP-SACK)、带有大窗口的TCP(TCP-LW)、例如TCP-Vegas协议的拥塞预报协议以及TCP欺骗协议(TCP spoofing protocol)。

[0105] 同样的，多协议压缩引擎238为用户加速经由桌面客户机乃至移动客户机访问应用的性能，所述桌面客户机例如Micosoft Outlook和非web瘦客户机，诸如由像Oracle、SAP和Siebel的通用企业应用所启动的任何客户机，所述移动客户机例如掌上电脑。在一些实施例中，通过在内核模式204内部执行并与访问网络堆栈267的分组处理引擎240集成，多协议压缩引擎238可以压缩TCP/IP协议携带的任何协议，例如任何应用层协议。

[0106] 高速层2-7集成分组引擎240，通常也称为分组处理引擎，或分组引擎，负责设备200通过网络端口266接收和发送的分组的内核级处理的管理。高速层2-7集成分组引擎240可包括用于在例如接收网络分组和传输网络分组的处理期间排队一个或多个网络分组的缓冲器。另外，高速层2-7集成分组引擎240与一个或多个网络堆栈267通信以通过网络端口266发送和接收网络分组。高速层2-7集成分组引擎240与加密引擎234、高速缓存管理器232、策略引擎236和多协议压缩逻辑238协同工作。更具体地，配置加密引擎234以执行分组的SSL处理，配置策略引擎236以执行涉及流量管理的功能，例如请求级内容切换以及请求级高速缓存重定向，并配置多协议压缩逻辑238以执行涉及数据压缩和解压缩的功能。

[0107] 高速层2-7集成分组引擎240包括分组处理定时器242。在一个实施例中，分组处理定时器242提供一个或多个时间间隔以触发输入处理，例如，接收或者输出(即传输)网络分组。在一些实施例中，高速层2-7集成分组引擎240响应于定时器242处理网络分组。分组处理定时器242向分组引擎240提供任何类型和形式的信号以通知、触发或传输时间相关的事件、间隔或发生。在许多实施例中，分组处理定时器242以毫秒级操作，例如100ms、50ms、或25ms。例如，在一些实例中，分组处理定时器242提供时间间隔或者以其它方式使得由高速层2-7集成分组引擎240以10ms时间间隔处理网络分组，而在其他实施例中，使高速层2-7集成分组引擎240以5ms时间间隔处理网络分组，并且在进一步的实施例中，短到3、2或1ms时间间隔。高速层2-7集成分组引擎240在操作期间可与加密引擎234、高速缓存管理器232、策略引擎236以及多协议压缩引擎238连接、集成或通信。因此，响应于分组处理定时器242和/或分组引擎240，可执行加密引擎234、高速缓存管理器232、策略引擎236以及多协议压缩引擎238的任何逻辑、功能或操作。因此，在由分组处理定时器242提供的时间间隔粒度，可执行加密引擎234、高速缓存管理器232、策略引擎236以及多协议压缩引擎238的任何逻辑、功能或操作，例如，时间间隔少于或等于10ms。例如，在一个实施例中，高速缓存管理器232可响应于高速层2-7集成分组引擎240和/或分组处理定时器242来执行任何高速缓存的对象的终止。在又一个实施例中，高速缓存的对象的终止或无效时间被设定为与分组处理定时器242的时间间隔相同的粒度级，例如每10ms。

[0108] 与内核空间204不同，用户空间202是被用户模式应用或在用户模式运行的程序所使用的操作系统的存储区域或部分。用户模式应用不能直接访问内核空间204而使用服务调用以访问内核服务。如图2所示，设备200的用户空间202包括图形用户接口(GUI)210、命

令行接口(CLI)212、壳服务(shell service)214、健康监控程序216以及守护(daemon)服务218。GUI210和CLI212提供系统管理员或其他用户可与之交互并控制设备200操作的装置，例如通过设备200的操作系统。GUI210和CLI212可包括运行在用户空间202或内核框架204中的代码。GUI210可以是任何类型或形式的图形用户接口，可以通过文本、图形或其他形式由任何类型的程序或应用(如浏览器)来呈现。CLI212可为任何类型和形式的命令行或基于文本的接口，例如通过操作系统提供的命令行。例如，CLI212可包括壳，该壳是使用户与操作系统相互作用的工具。在一些实施例中，可通过bash、csh、tcsh或者ksh类型的壳提供CLI212。壳服务214包括程序、服务、任务、进程或可执行指令以支持由用户通过GUI210和/或CLI212的与设备200或者操作系统的交互

[0109] 健康监控程序216用于监控、检查、报告并确保网络系统正常运行，以及用户正通过网络接收请求的内容。健康监控程序216包括一个或多个程序、服务、任务、进程或可执行指令，为监控设备200的任何行为提供逻辑、规则、功能或操作。在一些实施例中，健康监控程序216拦截并检查通过设备200传递的任何网络流量。在其他实施例中，健康监控程序216通过任何合适的方法和/或机制与一个或多个下述设备连接：加密引擎234，高速缓存管理器232，策略引擎236，多协议压缩逻辑238，分组引擎240，守护服务218以及壳服务214。因此，健康监控程序216可调用任何应用编程接口(API)以确定设备200的任何部分的状态、情况或健康。例如，健康监控程序216可周期性地查验(ping)或发送状态查询以检查程序、进程、服务或任务是否活动并当前正在运行。在又一个实施例中，健康监控程序216可检查由任何程序、进程、服务或任务提供的任何状态、错误或历史日志以确定设备200任何部分的任何状况、状态或错误。

[0110] 守护服务218是连续运行或在背景中运行的程序，并且处理设备200接收的周期性服务请求。在一些实施例中，守护服务可向其他程序或进程(例如合适的另一个守护服务218)转发请求。如本领域技术人员所公知的，守护服务218可无人监护的运行，以执行连续的或周期性的系统范围功能，例如网络控制，或者执行任何需要的任务。在一些实施例中，一个或多个守护服务218运行在用户空间202中，而在其他实施例中，一个或多个守护服务218运行在内核空间。

[0111] 现参考图2B，描述了设备200的又一个实施例。总的来说，设备200提供下列服务、功能或操作中的一个或多个：用于一个或多个客户机102以及一个或多个服务器106之间的通信的SSL VPN连通280、交换/负载平衡284、域名服务解析286、加速288和应用防火墙290。服务器106的每一个可以提供一个或者多个网络相关服务270a-270n(称为服务270)。例如，服务器106可以提供http服务270。设备200包括一个或者多个虚拟服务器或者虚拟互联网协议服务器，称为vServer275、vS275、VIP服务器或者仅是VIP275a-275n(此处也称为vServer275)。vServer275根据设备200的配置和操作来接收、拦截或者以其它方式处理客户机102和服务器106之间的通信。

[0112] vServer275可以包括软件、硬件或者软件和硬件的任何组合。vServer275可包括在设备200中的用户模式202、内核模式204或者其任何组合中运行的任何类型和形式的程序、服务、任务、进程或者可执行指令。vServer275包括任何逻辑、功能、规则或者操作，以执行此处所述技术的任何实施例，诸如SSL VPN280、转换/负载平衡284、域名服务解析286、加速288和应用防火墙290。在一些实施例中，vServer275建立到服务器106的服务270的连接。

服务275可以包括能够连接到设备200、客户机102或者vServer275并与之通信的任何程序、应用、进程、任务或者可执行指令集。例如，服务275可以包括web服务器、http服务器、ftp、电子邮件或者数据库服务器。在一些实施例中，服务270是守护进程或者网络驱动器，用于监听、接收和/或发送应用的通信，诸如电子邮件、数据库或者企业应用。在一些实施例中，服务270可以在特定的IP地址、或者IP地址和端口上通信。

[0113] 在一些实施例中，vServer275应用策略引擎236的一个或者多个策略到客户机102和服务器106之间的网络通信。在一个实施例中，该策略与vServer275相关。在又一个实施例中，该策略基于用户或者用户组。在又一个实施例中，策略为通用的并且应用到一个或者多个vServer275a-275n，和通过设备200通信的任何用户或者用户组。在一些实施例中，策略引擎的策略具有基于通信的任何内容应用该策略的条件，通信的内容诸如互联网协议地址、端口、协议类型、分组中的头部或者字段、或者通信的上下文，诸如用户、用户组、vServer275、传输层连接、和/或客户机102或者服务器106的标识或者属性。

[0114] 在其他实施例中，设备200与策略引擎236通信或接口，以便确定远程用户或远程客户机102的验证和/或授权，以访问来自服务器106的计算环境15、应用和/或数据文件。在又一个实施例中，设备200与策略引擎236通信或交互，以便确定远程用户或远程客户机102的验证和/或授权，使得应用传送系统190传送一个或多个计算环境15、应用和/或数据文件。在又一个实施例中，设备200基于策略引擎236对远程用户或远程客户机102的验证和/或授权建立VPN或SSL VPN连接。一个实施例中，设备200基于策略引擎236的策略控制网络流量以及通信会话。例如，基于策略引擎236，设备200可控制对计算环境15、应用或数据文件的访问。

[0115] 在一些实施例中，vServer275与客户机102经客户机代理120建立传输层连接，诸如TCP或者UDP连接。在一个实施例中，vServer275监听和接收来自客户机102的通信。在其他实施例中，vServer275与客户机服务器106建立传输层连接，诸如TCP或者UDP连接。在一个实施例中，vServer275建立到运行在服务器106上的服务器270的互联网协议地址和端口的传输层连接。在又一个实施例中，vServer275将到客户机102的第一传输层连接与到服务器106的第二传输层连接相关联。在一些实施例中，vServer275建立到服务器106的传输层连接池并经由所述池化(pooled)的传输层连接多路复用客户机的请求。

[0116] 在一些实施例中，设备200提供客户机102和服务器106之间的SSL VPN连接280。例如，第一网络102上的客户机102请求建立到第二网络104'上的服务器106的连接。在一些实施例中，第二网络104'是不能从第一网络104路由的。在其他实施例中，客户机102位于公用网络104上，并且服务器106位于专用网络104'上，例如企业网。在一个实施例中，客户机代理120拦截第一网络104上的客户机102的通信，加密该通信，并且经第一传输层连接发送该通信到设备200。设备200将第一网络104上的第一传输层连接与到第二网络104上的服务器106的第二传输层连接相关联。设备200接收来自客户机代理102的所拦截的通信，解密该通信，并且经第二传输层连接发送该通信到第二网络104上的服务器106。第二传输层连接可以是池化的传输层连接。同样的，设备200为两个网络104、104'之间的客户机102提供端到端安全传输层连接。

[0117] 在一个实施例中，设备200寄载虚拟专用网络104上的客户机102的内部网互联网协议或者IntranetIP282地址。客户机102具有本地网络标识符，诸如第一网络104上的互联

网协议(IP)地址和/或主机名称。当经设备200连接到第二网络104'时,设备200在第二网络104'上为客户机102建立、分配或者以其它方式提供IntranetIP,其是诸如IP地址和/或主机名称的网络标识符。使用为客户机的所建立的IntranetIP282,设备200在第二或专用网104'上监听并接收指向该客户机102的任何通信。在一个实施例中,设备200在第二专用网络104上用作或者代表客户机102。例如,在又一个实施例中,vServer275监听和响应到客户机102的IntranetIP282的通信。在一些实施例中,如果第二网络104'上的计算装置100发送请求,设备200如同客户机102一样来处理该请求。例如,设备200可以响应对客户机IntranetIP282的查验。在又一个实施例中,设备可以与请求和客户机IntranetIP282连接的第二网络104上的计算装置100建立连接,诸如TCP或者UDP连接。

[0118] 在一些实施例中,设备200为客户机102和服务器106之间的通信提供下列一个或多个加速技术288:1)压缩;2)解压缩;3)传输控制协议池;4)传输控制协议多路复用;5)传输控制协议缓冲;以及6)高速缓存。在一个实施例中,设备200通过开启与每一服务器106的一个或者多个传输层连接并且维持这些连接以允许由客户机经因特网的重复数据访问,来为服务器106缓解由重复开启和关闭到客户机102的传输层连接所造成的大量处理负载。该技术此处称为"连接池"。

[0119] 在一些实施例中,为了经池化的传输层连接无缝拼接从客户机102到服务器106的通信,设备200通过在传输层协议级修改序列号和确认号来转换或多路复用通信。这被称为"连接多路复用"。在一些实施例中,不需要应用层协议相互作用。例如,在到来分组(即,自客户机102接收的分组)的情况中,所述分组的源网络地址被改变为设备200的输出端口的网络地址,而目的网络地址被改为目的服务器的网络地址。在发出分组(即,自服务器106接收的一个分组)的情况中,源网络地址被从服务器106的网络地址改变为设备200的输出端口的网络地址,而目的地址被从设备200的网络地址改变为请求的客户机102的网络地址。分组的序列号和确认号也被转换为到客户机102的设备200的传输层连接上的客户机102所期待的序列号和确认。在一些实施例中,传输层协议的分组校验和被重新计算以计及这些转换。

[0120] 在又一个实施例中,设备200为客户机102和服务器106之间的通信提供交换或负载平衡功能284。在一些实施例中,设备200根据层4或应用层请求数据来分布流量并将客户机请求定向到服务器106。在一个实施例中,尽管网络分组的网络层或者层2识别目的服务器106,但设备200通过承载为传输层分组的有效载荷的数据和应用信息来确定服务器106以便分发网络分组。在一个实施例中,设备200的健康监控程序216监控服务器的健康来确定分发客户机请求到哪个服务器106。在一些实施例中,如果设备200探测到某个服务器106不可用或者具有超过预定阈值的负载,设备200可以将客户机请求指向或者分发到另一个服务器106。

[0121] 在一些实施例中,设备200用作域名服务(DNS)解析器或者以其它方式为来自客户机102的DNS请求提供解析。在一些实施例中,设备拦截由客户机102发送的DNS请求。在一个实施例中,设备200以设备200的IP地址或其所寄载的IP地址来响应客户机的DNS请求。在此实施例中,客户机102把用于域名的网络通信发送到设备200。在又一个实施例中,设备200以第二设备200'的或其所寄载的IP地址来响应客户机的DNS请求。在一些实施例中,设备200使用由设备200确定的服务器106的IP地址来响应客户机的DNS请求。

[0122] 在又一个实施例中，设备200为客户机102和服务器106之间的通信提供应用防火墙功能290。在一个实施例中，策略引擎236提供用于探测和阻断非法请求的规则。在一些实施例中，应用防火墙290防御拒绝服务(DoS)攻击。在其他实施例中，设备检查所拦截的请求的内容，以识别和阻断基于应用的攻击。在一些实施例中，规则/策略引擎236包括用于提供对多个种类和类型的基于web或因特网的脆弱点的保护的一个或多个应用防火墙或安全控制策略，例如下列的一个或多个脆弱点：1)缓冲区泄出，2)CGI-BIN参数操纵，3)表单/隐藏字段操纵，4)强制浏览，5)cookie或会话中毒，6)被破坏的访问控制列表(ACLs)或弱密码，7)跨站脚本处理(XSS)，8)命令注入，9)SQL注入，10)错误触发敏感信息泄露，11)对加密的不安全使用，12)服务器错误配置，13)后门和调试选项，14)网站涂改，15)平台或操作系统弱点，和16)零天攻击。在一个实施例中，对下列情况的一种或多种，应用防火墙290以检查或分析网络通信的形式来提供HTML格式字段的保护：1)返回所需的字段，2)不允许附加字段，3)只读和隐藏字段强制(enforcement)，4)下拉列表和单选按钮字段的一致，以及5)格式字段最大长度强制。在一些实施例中，应用防火墙290确保cookie不被修改。在其他实施例中，应用防火墙290通过执行合法的URL来防御强制浏览。

[0123] 在其他实施例中，应用防火墙290保护在网络通信中包含的任何机密信息。应用防火墙290可以根据引擎236的规则或策略来检查或分析任一网络通信以识别在网络分组的任一字段中的任一机密信息。在一些实施例中，应用防火墙290在网络通信中识别信用卡号、口令、社会保险号、姓名、病人代码、联系信息和年龄的一次或多次出现。网络通信的编码部分可以包括这些出现或机密信息。基于这些出现，在一个实施例中，应用防火墙290可以对网络通信采取策略行动，诸如阻止发送网络通信。在又一个实施例中，应用防火墙290可以重写、移动或者以其它方式掩盖该所识别的出现或者机密信息。

[0124] 仍参考图2B，设备200可以包括如上面结合图1D所讨论的性能监控代理197。在一个实施例中，设备200从如图1D中所描述的监控服务198或监控服务器106中接收监控代理197。在一些实施例中，设备200在诸如磁盘的存储装置中保存监控代理197，以用于传送给与设备200通信的任何客户机或服务器。例如，在一个实施例中，设备200在接收到建立传输层连接的请求时发送监控代理197给客户机。在其他实施例中，设备200在建立与客户机102的传输层连接时发送监控代理197。在又一个实施例中，设备200在拦截或检测对web页面的请求时发送监控代理197给客户机。在又一个实施例中，设备200响应于监控服务器198的请求来发送监控代理197到客户机或服务器。在一个实施例中，设备200发送监控代理197到第二设备200'或设备205。

[0125] 在其他实施例中，设备200执行监控代理197。在一个实施例中，监控代理197测量和监控在设备200上执行的任何应用、程序、进程、服务、任务或线程的性能。例如，监控代理197可以监控和测量vServers275A-275N的性能与操作。在又一个实施例中，监控代理197测量和监控设备200的任何传输层连接的性能。在一些实施例中，监控代理197测量和监控通过设备200的任何用户会话的性能。在一个实施例中，监控代理197测量和监控通过设备200的诸如SSL VPN会话的任何虚拟专用网连接和/或会话的性能。在进一步的实施例中，监控代理197测量和监控设备200的内存、CPU和磁盘使用以及性能。在又一个实施例中，监控代理197测量和监控诸如SSL卸载、连接池和多路复用、高速缓存以及压缩的由设备200执行的任何加速技术288的性能。在一些实施例中，监控代理197测量和监控由设备200执行的任一

负载平衡和/或内容交换284的性能。在其他实施例中，监控代理197测量和监控由设备200执行的应用防火墙290保护和处理的性能。

[0126] C.客户机代理

[0127] 现参考图3，描述客户机代理120的实施例。客户机102包括客户机代理120，用于经由网络104与设备200和/或服务器106来建立和交换通信。总的来说，客户机102在计算装置100上操作，该计算装置100拥有带有内核模式302以及用户模式303的操作系统，以及带有一个或多个层310a-310b的网络堆栈310。客户机102可以已经安装和/或执行一个或多个应用。在一些实施例中，一个或多个应用可通过网络堆栈310与网络104通信。所述应用之一，诸如web浏览器，也可包括第一程序322。例如，可在一些实施例中使用第一程序322来安装和/或执行客户机代理120，或其中任何部分。客户机代理120包括拦截机制或者拦截器350，用于从网络堆栈310拦截来自一个或者多个应用的网络通信。

[0128] 客户机102的网络堆栈310可包括任何类型和形式的软件、或硬件或其组合，用于提供与网络的连接和通信。在一个实施例中，网络堆栈310包括用于网络协议组的软件实现。网络堆栈310可包括一个或多个网络层，例如为本领域技术人员所公认和了解的开放式系统互联(OSI)通信模型的任何网络层。这样，网络堆栈310可包括用于任何以下OSI模型层的任何类型和形式的协议：1)物理链路层；2)数据链路层；3)网络层；4)传输层；5)会话层)；6)表示层，以及7)应用层。在一个实施例中，网络堆栈310可包括在因特网协议(IP)的网络层协议上的传输控制协议(TCP)，通常称为TCP/IP。在一些实施例中，可在以太网协议上承载TCP/IP协议，以太网协议可包括IEEE广域网(WAN)或局域网(LAN)协议的任何族，例如被IEEE802.3覆盖的这些协议。在一些实施例中，网络堆栈310包括任何类型和形式的无线协议，例如IEEE802.11和/或移动因特网协议。

[0129] 考虑基于TCP/IP的网络，可使用任何基于TCP/IP的协议，包括消息应用编程接口(MAPI)(email)、文件传输协议(FTP)、超文本传输协议(HTTP)、通用因特网文件系统(CIFS)协议(文件传输)、独立计算架构(ICA)协议、远程桌面协议(RDP)、无线应用协议(WAP)、移动IP协议，以及互联网协议电话(VoIP)协议。在又一个实施例中，网络堆栈310包括任何类型和形式的传输控制协议，诸如修改的传输控制协议，例如事务TCP(T/TCP)，带有选择确认的TCP(TCP-SACK)，带有大窗口的TCP(TCP-LW)，例如TCP-Vegas协议的拥塞预测协议，以及TCP欺骗协议。在其他实施例中，网络堆栈310可使用诸如基于IP的UDP的任何类型和形式的用户数据报协议(UDP)，例如用于语音通信或实时数据通信。

[0130] 另外，网络堆栈310可包括支持一个或多个层的一个或多个网络驱动器，例如TCP驱动器或网络层驱动器。网络层驱动器可作为计算装置100的操作系统的一部分或者作为计算装置100的任何网络接口卡或其它网络访问组件的一部分被包括。在一些实施例中，网络堆栈310的任何网络驱动器可被定制、修改或调整以提供网络堆栈310的定制或修改部分，用来支持此处描述的任何技术。在其他实施例中，设计并构建加速程序302以与网络堆栈310协同操作或工作，上述网络堆栈310由客户机102的操作系统安装或以其它方式提供。

[0131] 网络堆栈310包括任何类型和形式的接口，用于接收、获得、提供或以其它方式访问涉及客户机102的网络通信的任何信息和数据。在一个实施例中，与网络堆栈310的接口包括应用编程接口(API)。接口也可包括任何函数调用、钩子或过滤机制，事件或回调机制、或任何类型的接口技术。网络堆栈310通过接口可接收或提供与网络堆栈310的功能或操作

相关的任何类型和形式的数据结构，例如对象。例如，数据结构可以包括与网络分组相关的信息和数据或者一个或多个网络分组。在一些实施例中，数据结构包括在网络堆栈310的协议层处理的网络分组的一部分，例如传输层的网络分组。在一些实施例中，数据结构325包括内核级别数据结构，而在其他实施例中，数据结构325包括用户模式数据结构。内核级数据结构可以包括获得的或与在内核模式302中操作的网络堆栈310的一部分相关的数据结构、或者运行在内核模式302中的网络驱动程序或其它软件、或者由运行或操作在操作系统的内核模式的服务、进程、任务、线程或其它可执行指令获得或收到的任何数据结构。

[0132] 此外，网络堆栈310的一些部分可在内核模式302执行或操作，例如，数据链路或网络层，而其他部分在用户模式303执行或操作，例如网络堆栈310的应用层。例如，网络堆栈的第一部分310a可以给应用提供对网络堆栈310的用户模式访问，而网络堆栈310的第二部分310a提供对网络的访问。在一些实施例中，网络堆栈的第一部分310a可包括网络堆栈310的一个或多个更上层，例如层5-7的任何层。在其他实施例中，网络堆栈310的第二部分310b包括一个或多个较低的层，例如层1-4的任何层。网络堆栈310的每个第一部分310a和第二部分310b可包括网络堆栈310的任何部分，位于任何一个或多个网络层，处于用户模式203、内核模式202，或其组合，或在网络层的任何部分或者到网络层的接口点，或用户模式203和内核模式202的任何部分或到用户模式203和内核模式202的接口点。

[0133] 拦截器350可以包括软件、硬件、或者软件和硬件的任何组合。在一个实施例中，拦截器350在网络堆栈310的任一点拦截网络通信，并且重定向或者发送网络通信到由拦截器350或者客户机代理120所期望的、管理的或者控制的目的地。例如，拦截器350可以拦截第一网络的网络堆栈310的网络通信并且发送该网络通信到设备200，用于在第二网络104上发送。在一些实施例中，拦截器350包括含有诸如被构建和设计来与网络堆栈310对接并一同工作的网络驱动器的驱动器的任一类型的拦截器350。在一些实施例中，客户机代理120和/或拦截器350操作在网络堆栈310的一个或者多个层，诸如在传输层。在一个实施例中，拦截器350包括过滤器驱动器、钩子机制、或者连接到网络堆栈的传输层的任一形式和类型的合适网络驱动器接口，诸如通过传输驱动器接口(TDI)。在一些实施例中，拦截器350连接到诸如传输层的第一协议层和诸如传输协议层之上的任何层的另一个协议层，例如，应用协议层。在一个实施例中，拦截器350可以包括遵守网络驱动器接口规范(NDIS)的驱动器，或者NDIS驱动器。在又一个实施例中，拦截器350可以包括微型过滤器或者微端口驱动器。在一个实施例中，拦截器350或其部分在内核模式202中操作。在又一个实施例中，拦截器350或其部分在用户模式203中操作。在一些实施例中，拦截器350的一部分在内核模式202中操作，而拦截器350的另一部分在用户模式203中操作。在其他实施例中，客户机代理120在用户模式203操作，但通过拦截器350连接到内核模式驱动器、进程、服务、任务或者操作系统的部分，诸如以获取内核级数据结构225。在其他实施例中，拦截器350为用户模式应用或者程序，诸如应用。

[0134] 在一个实施例中，拦截器350拦截任何的传输层连接请求。在这些实施例中，拦截器350执行传输层应用编程接口(API)调用以设置目的地信息，诸如到期望位置的目的地IP地址和/或端口用于定位。以此方式，拦截器350拦截并重定向传输层连接到由拦截器350或客户机代理120控制或管理的IP地址和端口。在一个实施例中，拦截器350把连接的目的地信息设置为客户机代理120监听的客户机102的本地IP地址和端口。例如，客户机代理120可

以包括为重定向的传输层通信监听本地IP地址和端口的代理服务。在一些实施例中，客户机代理120随后将重定向的传输层通信传送到设备200。

[0135] 在一些实施例中，拦截器350拦截域名服务(DNS)请求。在一个实施例中，客户机代理120和/或拦截器350解析DNS请求。在又一个实施例中，拦截器发送所拦截的DNS请求到设备200以进行DNS解析。在一个实施例中，设备200解析DNS请求并且将DNS响应传送到客户机代理120。在一些实施例中，设备200经另一个设备200'或者DNS服务器106来解析DNS请求。

[0136] 在又一个实施例中，客户机代理120可以包括两个代理120和120'。在一个实施例中，第一代理120可以包括在网络堆栈310的网络层操作的拦截器350。在一些实施例中，第一代理120拦截网络层请求，诸如因特网控制消息协议(ICMP)请求(例如，查验和跟踪路由)。在其他实施例中，第二代理120'可以在传输层操作并且拦截传输层通信。在一些实施例中，第一代理120在网络堆栈210的一层拦截通信并且与第二代理120'连接或者将所拦截的通信传送到第二代理120'。

[0137] 客户机代理120和/或拦截器350可以以对网络堆栈310的任何其它协议层透明的方式在协议层操作或与之对接。例如，在一个实施例中，拦截器350可以以对诸如网络层的传输层之下的任何协议层和诸如会话、表示或应用层协议的传输层之上的任何协议层透明的方式在网络堆栈310的传输层操作或与之对接。这允许网络堆栈310的其它协议层如所期望的进行操作并无需修改以使用拦截器350。这样，客户机代理120和/或拦截器350可以与传输层连接以安全、优化、加速、路由或者负载平衡经由传输层承载的任一协议提供的任一通信，诸如TCP/IP上的任一应用层协议。

[0138] 此外，客户机代理120和/或拦截器可以以对任何应用、客户机102的用户和与客户机102通信的诸如服务器的任何其它计算装置透明的方式在网络堆栈310上操作或与之对接。客户机代理120和/或拦截器350可以以无需修改应用的方式被安装和/或执行在客户机102上。在一些实施例中，客户机102的用户或者与客户机102通信的计算装置未意识到客户机代理120和/或拦截器350的存在、执行或者操作。同样，在一些实施例中，相对于应用、客户机102的用户、诸如服务器的另一个计算装置、或者在由拦截器350连接的协议层之上和/或之下的任何协议层透明地来安装、执行和/或操作客户机代理120和/或拦截器350。

[0139] 客户机代理120包括加速程序302、流客户机306、收集代理304和/或监控代理197。在一个实施例中，客户机代理120包括由佛罗里达州Fort Lauderdale的Citrix Systems Inc.开发的独立计算架构(ICA)客户机或其任一部分，并且也指ICA客户机。在一些实施例中，客户机代理120包括应用流客户机306，用于从服务器106流式传输应用到客户机102。在一些实施例中，客户机代理120包括加速程序302，用于加速客户机102和服务器106之间的通信。在又一个实施例中，客户机代理120包括收集代理304，用于执行端点检测/扫描并且用于为设备200和/或服务器106收集端点信息。

[0140] 在一些实施例中，加速程序302包括用于执行一个或多个加速技术的客户机侧加速程序，以加速、增强或者以其他方式改善客户机与服务器106的通信和/或对服务器106的访问，诸如访问由服务器106提供的应用。加速程序302的可执行指令的逻辑、函数和/或操作可以执行一个或多个下列加速技术：1)多协议压缩，2)传输控制协议池，3)传输控制协议多路复用，4)传输控制协议缓冲，以及5)通过高速缓存管理器的高速缓存。另外，加速程序302可执行由客户机102接收和/或发送的任何通信的加密和/或解密。在一些实施例中，加

速程序302以集成的方式或者格式执行一个或者多个加速技术。另外，加速程序302可以对作为传输层协议的网络分组的有效载荷所承载的任一协议或者多协议执行压缩。

[0141] 流客户机306包括应用、程序、进程、服务、任务或者可执行指令，所述应用、程序、进程、服务、任务或者可执行指令用于接收和执行从服务器106所流式传输的应用。服务器106可以流式传输一个或者多个应用数据文件到流客户机306，用于播放、执行或者以其它方式引起客户机102上的应用被执行。在一些实施例中，服务器106发送一组压缩或者打包的应用数据文件到流客户机306。在一些实施例中，多个应用文件被压缩并存储在文件服务器上档案文件中，例如CAB、ZIP、SIT、TAR、JAR或其它档案文件。在一个实施例中，服务器106解压缩、解包或者解档应用文件并且将该文件发送到客户机102。在又一个实施例中，客户机102解压缩、解包或者解档应用文件。流客户机306动态安装应用或其部分，并且执行该应用。在一个实施例中，流客户机306可以为可执行程序。在一些实施例中，流客户机306可以能够启动另一个可执行程序。

[0142] 收集代理304包括应用、程序、进程、服务、任务或者可执行指令，用于识别、获取和/或收集关于客户机102的信息。在一些实施例中，设备200发送收集代理304到客户机102或者客户机代理120。可以根据设备的策略引擎236的一个或多个策略来配置收集代理304。在其他实施例中，收集代理304发送在客户机102上收集的信息到设备200。在一个实施例中，设备200的策略引擎236使用所收集的信息来确定和提供到网络104的客户机连接的访问、验证和授权控制。

[0143] 在一个实施例中，收集代理304包括端点检测和扫描机制，其识别并且确定客户机的一个或者多个属性或者特征。例如，收集代理304可以识别和确定任何一个或多个以下的客户机侧属性：1)操作系统和/或操作系统的版本，2)操作系统的服务包，3)运行的服务，4)运行的进程，和5)文件。收集代理304还可以识别并确定客户机上任何一个或多个以下软件的存在或版本：1)防病毒软件；2)个人防火墙软件；3)防垃圾邮件软件，和4)互联网安全软件。策略引擎236可以具有基于客户机或客户机侧属性的任何一个或多个属性或特性的一个或多个策略。

[0144] 在一些实施例中，客户机代理120包括如结合图1D和2B所讨论的监控代理197。监控代理197可以是诸如Visual Basic或Java脚本的任何类型和形式的脚本。在一个实施例中，监控代理197监控和测量客户机代理120的任何部分的性能。例如，在一些实施例中，监控代理197监控和测量加速程序302的性能。在又一个实施例中，监控代理197监控和测量流客户机306的性能。在其他实施例中，监控代理197监控和测量收集代理304的性能。在又一个实施例中，监控代理197监控和测量拦截器350的性能。在一些实施例中，监控代理197监控和测量客户机102的诸如存储器、CPU和磁盘的任何资源。

[0145] 监控代理197可以监控和测量客户机的任何应用的性能。在一个实施例中，监控代理197监控和测量客户机102上的浏览器的性能。在一些实施例中，监控代理197监控和测量经由客户机代理120传送的任何应用的性能。在其他实施例中，监控代理197测量和监控应用的最终用户响应时间，例如基于web的响应时间或HTTP响应时间。监控代理197可以监控和测量ICA或RDP客户机的性能。在又一个实施例中，监控代理197测量和监控用户会话或应用会话的指标。在一些实施例中，监控代理197测量和监控ICA或RDP会话。在一个实施例中，监控代理197测量和监控设备200在加速传送应用和/或数据到客户机102的过程中的性能。

[0146] 在一些实施例中，仍参考图3，第一程序322可以用于自动地、静默地、透明地或者以其它方式安装和/或执行客户机代理120或其部分，诸如拦截器350。在一个实施例中，第一程序322包括插件组件，例如ActiveX控件或Java控件或脚本，其加载到应用并由应用执行。例如，第一程序包括由web浏览器应用载入和运行的ActiveX控件，例如在存储器空间或应用的上下文中。在又一个实施例中，第一程序322包括可执行指令组，该可执行指令组被例如浏览器的应用载入并执行。在一个实施例中，第一程序322包括被设计和构造的程序以安装客户机代理120。在一些实施例中，第一程序322通过网络从另一个计算装置获得、下载、或接收客户机代理120。在又一个实施例中，第一程序322是用于在客户机102的操作系统上安装如网络驱动的程序的安装程序或即插即用管理器。

[0147] D.用于提供虚拟化应用传送控制器的系统和方法

[0148] 现参考图4A，该框图描述虚拟化环境400的一个实施例。总体而言，计算装置100包括管理程序层、虚拟化层和硬件层。管理程序层包括管理程序401(也称为虚拟化管理器)，其通过在虚拟化层中执行的至少一个虚拟机来分配和管理对硬件层中的多个物理资源(例如处理器421和盘428)的访问。虚拟化层包括至少一个操作系统410和分配给至少一个操作系统410的多个虚拟资源。虚拟资源可包括而不限于多个虚拟处理器432a、432b、432c(总称为432)和虚拟盘442a、442b、442c(总称为442)，以及如虚拟存储器和虚拟网络接口的虚拟资源。可将多个虚拟资源和操作系统称为虚拟机406。虚拟机406可包括控制操作系统405，该控制操作系统405与管理程序401通信，并用于执行应用以管理并配置计算装置100上的其他虚拟机。

[0149] 具体而言，管理程序401可以以模拟可访问物理设备的操作系统的任何方式向操作系统提供虚拟资源。管理程序401可以向任何数量的客户操作系统410a、410b(总称为410)提供虚拟资源。一些实施例中，计算装置100执行一种或多种管理程序。这些实施例中，管理程序可用于模拟虚拟硬件、划分物理硬件、虚拟化物理硬件并执行提供对计算环境的访问的虚拟机。管理程序可包括由位于美国加州的Palo Alto的VMWare制造的这些程序；XEN管理程序(一种开源产品，其开发由开源Xen.org协会监管)；由微软公司提供的HyperV、VirtualServer或虚拟PC管理程序，或其他。一些实施例中，计算装置100执行创建客户操作系统可在其上执行虚拟机平台的管理程序，该计算装置100被称为宿主服务器。在这些实施例的一个中，例如，计算装置100是由位于美国佛罗里达州Fort Lauderdale的Citrix Systems有限公司提供的XEN SERVER。

[0150] 一些实施例中，管理程序401在计算装置上执行的操作系统之内执行。在这些实施例的一个中，执行操作系统和管理程序401的计算装置可被视为具有宿主操作系统(执行在计算装置上的操作系统)，和客户操作系统(在由管理程序401提供的计算资源分区内执行的操作系统)。其他实施例中，管理程序401和计算装置上的硬件直接交互而不是在宿主操作系统上执行。在这些实施例的一个中，管理程序401可被视为在“裸金属(bare metal)”上执行，所述“裸金属”指包括计算装置的硬件。

[0151] 一些实施例中，管理程序401可以产生操作系统410在其中执行的虚拟机406a-c(总称为406)。在这些实施例的一个中，管理程序401加载虚拟机映像以创建虚拟机406。在这些实施例的又一个中，管理程序401在虚拟机406内执行操作系统410。仍在这些实施例的又一个中，虚拟机406执行操作系统410。

[0152] 一些实施例中，管理程序401控制在计算装置100上执行的虚拟机406的处理器调度和内存划分。在这些实施例的一个中，管理程序401控制至少一个虚拟机406的执行。在这些实施例的又一个中，管理程序401向至少一个虚拟机406呈现由计算装置100提供的至少一个硬件资源的抽象。其他实施例中，管理程序401控制是否以及如何将物理处理器能力呈现给虚拟机406。

[0153] 控制操作系统405可以执行用于管理和配置客户操作系统的至少一个应用。一个实施例中，控制操作系统405可以执行管理应用，如包括如下用户接口的应用，该用户接口为管理员提供对用于管理虚拟机执行的功能的访问，这些功能包括用于执行虚拟机、中止虚拟机执行或者识别要分配给虚拟机的物理资源类型的功能。又一个实施例中，管理程序401在由管理程序401创建的虚拟机406内执行控制操作系统405。又一个实施例中，控制操作系统405在被授权直接访问计算装置100上的物理资源的虚拟机406上执行。一些实施例中，计算装置100a上的控制操作系统405a可以通过管理程序401a和管理程序401b之间的通信与计算装置100b上的控制操作系统405b交换数据。这样，一个或多个计算装置100可以和一个或多个其他计算装置100交换有关处理器或资源池中可用的其他物理资源的数据。在这些实施例的一个中，这种功能允许管理程序管理分布在多个物理计算装置上的资源池。在这些实施例的又一个中，多个管理程序管理在一个计算装置100上执行的一个或多个客户操作系统。

[0154] 一个实施例中，控制操作系统405在被授权与至少一个客户操作系统410交互的虚拟机406上执行。又一个实施例中，客户操作系统410通过管理程序401和控制操作系统405通信，以请求访问盘或网络。仍在又一个实施例中，客户操作系统410和控制操作系统405可通过由管理程序401建立的通信信道通信，例如，通过由管理程序401提供的多个共享存储器页面。

[0155] 一些实施例中，控制操作系统405包括用于直接与由计算装置100提供的网络硬件通信的网络后端驱动器。在这些实施例的一个中，网络后端驱动器处理来自至少一个客户操作系统110的至少一个虚拟机请求。其他实施例中，控制操作系统405包括用于与计算装置100上的存储元件通信的块后端驱动器。在这些实施例的一个中，块后端驱动器基于从客户操作系统410接收的至少一个请求从存储元件读写数据。

[0156] 一个实施例，控制操作系统405包括工具堆栈404。其他实施例中，工具堆栈404提供如下功能：和管理程序401交互、和其他控制操作系统405(例如位于第二计算装置100b上)通信，或者管理计算装置100上的虚拟机406b、406c。又一个实施例中，工具堆栈404包括自定义应用，其用于向虚拟机群的管理员提供改进的管理功能。一些实施例中，工具堆栈404和控制操作系统405中的至少一个包括管理API，其提供用于远程配置并控制计算装置100上运行的虚拟机406的接口。其他实施例中，控制操作系统405通过工具堆栈404和管理程序401通信。

[0157] 一个实施例中，管理程序401在由管理程序401创建的虚拟机406内执行客户操作系统410。又一个实施例中，客户操作系统410为计算装置100的用户提供对计算环境中的资源的访问。又一个实施例中，资源包括程序、应用、文档、文件、多个应用、多个文件、可执行程序文件、桌面环境、计算环境或对计算装置100的用户可用的其他资源。又一个实施例中，可通过多个访问方法将资源传送给计算装置100，这些方法包括但不限于：常规的直接在计

算装置100上安装、通过应用流的方法传送给计算装置100、将由在第二计算装置100'上执行资源产生的并通过表示层协议传送给计算装置100的输出数据传送给计算装置100、将通过在第二计算装置100'上执行的虚拟机执行资源所产生的输出数据传送给计算装置100、或者从连接到计算装置100的移动存储装置(例如USB设备)执行或者通过在计算装置100上执行的虚拟机执行并且产生输出数据。一些实施例中,计算装置100将执行资源所产生的输出数据传输给另一个计算装置100'。

[0158] 一个实施例中,客户操作系统410和该客户操作系统410在其上执行的虚拟机结合形成完全虚拟化虚拟机,该完全虚拟化虚拟机并不知道自己是虚拟机,这样的机器可称为"Domain U HVM(硬件虚拟机)虚拟机"。又一个实施例中,完全虚拟化机包括模拟基本输入/输出系统(BIOS)的软件以便在完全虚拟化机中执行操作系统。在又一个实施例中,完全虚拟化机可包括驱动器,其通过和管理程序401通信提供功能。这样的实施例中,驱动器可意识到自己在虚拟化环境中执行。又一个实施例中,客户操作系统410和该客户操作系统410在其上执行的虚拟机结合形成超虚拟化(paravirtualized)虚拟机,该超虚拟化虚拟机意识到自己是虚拟机,这样的机器可称为"Domain U PV虚拟机"。又一个实施例中,超虚拟化机包括完全虚拟化机不包括的额外驱动器。又一个实施例中,超虚拟化机包括如上所述的被包含在控制操作系统405中的网络后端驱动器和块后端驱动器。

[0159] 现参考图4B,框图描述了系统中的多个联网计算装置的一个实施例,其中,至少一个物理主机执行虚拟机。总体而言,系统包括管理组件404和管理程序401。系统包括多个计算装置100、多个虚拟机406、多个管理程序401、多个管理组件(又称为工具堆栈404或者管理组件404)以及物理资源421、428。多个物理机器100的每一个可被提供为如上结合图1E-1H和图4A描述的计算装置100。

[0160] 具体而言,物理盘428由计算装置100提供,存储至少一部分虚拟盘442。一些实施例中,虚拟盘442和多个物理盘428相关联。在这些实施例的一个中,一个或多个计算装置100可以与一个或多个其他计算装置100交换有关处理器或资源池中可用的其他物理资源的数据,允许管理程序管理分布在多个物理计算装置上的资源池。一些实施例中,将虚拟机406在其上执行的计算装置100称为物理主机100或主机100。

[0161] 管理程序在计算装置100上的处理器上执行。管理程序将对物理盘的访问量分配给虚拟盘。一个实施例中,管理程序401分配物理盘上的空间量。又一个实施例中,管理程序401分配物理盘上的多个页面。一些实施例中,管理程序提供虚拟盘442作为初始化和执行虚拟机450进程的一部分。

[0162] 一个实施例中,将管理组件404a称为池管理组件404a。又一个实施例中,可以称为控制管理系统405a的管理操作系统405a包括管理组件。一些实施例中,将管理组件称为工具堆栈。在这些实施例的一个中,管理组件是上文结合图4A描述的工具堆栈404。其他实施例中,管理组件404提供用户接口,用于从如管理员的用户接收要供应和/或执行的虚拟机406的标识。仍在其他实施例中,管理组件404提供用户接口,用于从如管理员的用户接收将虚拟机406b从一个物理机器100迁移到另一物理机器的请求。在进一步的实施例中,管理组件404a识别在其上执行所请求的虚拟机406d的计算装置100b并指示所识别的计算装置100b上的管理程序401b执行所识别的虚拟机,这样,可将管理组件称为池管理组件。

[0163] 现参考图4C,描述了虚拟应用传送控制器或虚拟设备450的实施例。总体而言,上

文结合图2A和2B描述的设备200的任何功能和/或实施例(例如应用传送控制器)可以部署在上文结合图4A和4B描述的虚拟化环境的任何实施例中。应用传送控制器的功能不是以设备200的形式部署,而是将该功能部署在诸如客户机102、服务器106或设备200的任何计算装置100上的虚拟化环境400中。

[0164] 现在参考图4C,描述了在服务器106的管理程序401上操作的虚拟设备450的实施例的框图。如图2A和2B的设备200一样,虚拟机450可以提供可用性、性能、卸载和安全的功能。对于可用性,虚拟设备可以执行网络第4层和第7层之间的负载平衡并执行智能服务健康监控。对于通过网络流量加速实现的性能增加,虚拟设备可以执行缓存和压缩。对于任何服务器的卸载处理,虚拟设备可以执行连接复用和连接池和/或SSL处理。对于安全,虚拟设备可以执行设备200的任何应用防火墙功能和SSL VPN功能。

[0165] 结合附图2A描述的设备200的任何模块可以虚拟化设备传送控制器450的形式被打包、组合、设计或构造,虚拟化设备传送控制器450可部署成在诸如流行的服务器这样的任何服务器上的虚拟化环境300或非虚拟化环境中执行的软件模块或组件。例如,可以安装在计算装置上的安装包的形式提供虚拟设备。参考图2A,可以将高速缓存管理器232、策略引擎236、压缩238、加密引擎234、分组引擎240、GUI210、CLI212、壳服务214中的任一个设计和构成在计算装置和/或虚拟化环境300的任何操作系统上运行的组件或模块。虚拟化设备400不使用设备200的加密处理器260、处理器262、存储器264和网络堆栈267,而是可使用虚拟化环境400提供的任何这些资源或者服务器106上以其他方式可用的这些资源。

[0166] 仍参考图4C,简言之,任何一个或多个vServer275A-275N可以操作或执行在任意类型的计算装置100(如服务器106)的虚拟化环境400中。结合附图2B描述的设备200的任何模块和功能可以设计和构造成在服务器的虚拟化或非虚拟化环境中操作。可以将vServer275、SSL VPN280、内网UP282、交换装置284、DNS286、加速装置288、APP FW280和监控代理中的任一个打包、组合、设计或构造成应用传送控制器450的形式,应用传送控制器450可部署成在装置和/或虚拟化环境400中执行的一个或多个软件模块或组件。

[0167] 一些实施例中,服务器可以在虚拟化环境中执行多个虚拟机406a-406b,每个虚拟机运行虚拟应用传送控制器450的相同或不同实施例。一些实施例中,服务器可以在多核处理系统的一个核上执行一个或多个虚拟机上的一个或多个虚拟设备450。一些实施例中,服务器可以在多处理器装置的每个处理器上执行一个或多个虚拟机上的一个或多个虚拟设备450。

[0168] E.提供多核架构的系统和方法

[0169] 根据摩尔定律,每两年集成电路上可安装的晶体管的数量会基本翻倍。然而,CPU速度增加会达到一个稳定的水平(plateaus),例如,2005年以来,CPU速度在约3.5-4GHz的范围内。一些情况下,CPU制造商可能不依靠CPU速度增加来获得额外的性能。一些CPU制造商会给处理器增加附加核以提供额外的性能。依靠CPU获得性能改善的如软件和网络供应商的产品可以通过利用这些多核CPU来改进他们的性能。可以重新设计和/或编写为单CPU设计和构造的软件以利用多线程、并行架构或多核架构。

[0170] 一些实施例中,称为nCore或多核技术的设备200的多核架构允许设备打破单核性能障碍并利用多核CPU的能力。前文结合图2A描述的架构中,运行单个网络或分组引擎。nCore技术和架构的多核允许同时和/或并行地运行多个分组引擎。通过在每个核上运行分

组引擎，设备架构利用附加核的处理能力。一些实施例中，这提供了高达七倍的性能改善和扩展性。

[0171] 图5A示出根据一类并行机制或并行计算方案(如功能并行机制、数据并行机制或基于流的数据并行机制)在一个或多个处理器核上分布的工作、任务、负载或网络流量的一些实施例。总体而言，图5A示出如具有n个核的设备200'的多核系统的实施例，n个核编号为1到N。一个实施例中，工作、负载或网络流量可以分布在第一核505A、第二核505B、第三核505C、第四核505D、第五核505E、第六核505F、第七核505G等上，这样，分布位于所有n个核505N(此后统称为核505)或n个核中的两个或多个上。可以有多个VIP275，每个运行在多个核中的相应的核上。可以有多个分组引擎240，每个运行在多个核的相应的核。所使用任何方法可产生多个核中任一核上的不同的、变化的或类似的工作负载或性能级别515。对于功能并行方法，每个核运行由分组引擎、VIP275或设备200提供的多个功能的不同功能。在数据并行方法中，数据可基于接收数据的网络接口卡(NIC)或VIP275并行或分布在核上。又一个数据并行方法中，可通过将数据流分布在每个核上而将处理分布在核上。

[0172] 图5A的进一步的细节中，一些实施例中，可以根据功能并行机制500将负载、工作或网络流量在多个核505间分布。功能并行机制可基于执行一个或多个相应功能的每个核。一些实施例中，第一核可执行第一功能，同时第二核执行第二功能。功能并行方法中，根据功能性将多核系统要执行的功能划分并分布到每个核。一些实施例中，可将功能并行机制称为任务并行机制，并且可在每个处理器或核对同一数据或不同数据执行不同进程或功能时实现。核或处理器可执行相同或不同的代码。一些情况下，不同的执行线程或代码可在工作时相互通信。可以进行通信以将数据作为工作流的一部分从一个线程传递给下一线程。

[0173] 一些实施例中，根据功能并行机制500将工作分布在核505上，可以包括根据特定功能分布网络流量，所述特定功能例如为网络输入/输出管理(NW I/O)510A、安全套接层(SSL)加密和解密510B和传输控制协议(TCP)功能510C。这会产生基于所使用的功能量或功能级别的工作、性能或者计算负载515。一些实施例中，根据数据并行机制540将工作分布在核505上可包括基于与特定的硬件或软件组件相关联的分布数据来分布工作量515。一些实施例中，根据基于流的数据并行机制520将工作分布在核505上可包括基于上下文或流来分布数据，从而使得每个核上的工作量515A-N可以类似、基本相等或者相对平均分布。

[0174] 在功能并行方法的情况下，可以配置每个核来运行由设备的分组引擎或VIP提供的多个功能中的一个或多个功能。例如，核1可执行设备200'的网络I/O处理，同时核2执行设备的TCP连接管理。类似地，核3可执行SSL卸载，同时核4可执行第7层或应用层处理和流量管理。每个核可执行相同或不同的功能。每个核可执行不只一个功能。任一核可运行结合附图2A和2B识别和/或描述的功能或其一部分。该方法中，核上的工作可以粗粒度或细粒度方式按功能划分。一些情况下，如图5A所示，按功能划分会使得不同核运行在不同的性能或负载级别515。

[0175] 在功能并行方法的情况下，可以配置每个核来运行由设备的分组引擎提供的多个功能中的一个或多个功能。例如，核1可执行设备200'的网络I/O处理，同时核2执行设备的TCP连接管理。类似地，核3可执行SSL卸载，同时核4可执行第7层或应用层处理和流量管理。每个核可执行相同或不同的功能。每个核可执行不只一个功能。任何核可运行结合附图2A和2B识别和/或描述的功能或其一部分。该方法中，核上的工作可以粗粒度或细粒度方式按

功能划分。一些情况下，如图5A所示，按功能划分会使得不同核运行在不同的性能或负载级别。

[0176] 可以用任何结构或方案来分布功能或任务。例如，图5B示出用于处理与网络I/O功能510A相关联的应用和进程的第一核Core1505A。一些实施例中，与网络I/O相关联的网络流量可以和特定的端口号相关联。因而，将具有与NW I/O510A相关联的端口目的地的发出和到来的分组导引给Core1505A，该Core1505A专用于处理与NW I/O端口相关联的所有网络流量。类似的，Core2505B专用于处理与SSL处理相关联的功能，Core4505D可专用于处理所有TCP级处理和功能。

[0177] 虽然图5A示出如网络I/O、SSL和TCP的功能，也可将其他功能分配给核。这些其他功能可包括此处描述的任一或多个功能或操作。例如，结合图2A和2B描述的任何功能可基于功能基础分布在核上。一些情况下，第一VIP275A可运行在第一核上，同时，具有不同配置的第二VIP275B可运行在第二核上。一些实施例中，每个核505可处理特定功能，这样每个核505可处理与该特定功能相关联的处理。例如，Core2505B可处理SSL卸载，同时Core4505D可处理应用层处理和流量管理。

[0178] 其他实施例中，可根据任何类型或形式的数据并行机制540将工作、负载或网络流量分布在核505上。一些实施例中，可由每个核对分布式数据的不同片执行相同任务或功能来实现多核系统中的数据并行机制。一些实施例中，单个执行线程或代码控制对所有数据片的操作。其他实施例中，不同线程或指令控制操作，但是可执行相同代码。一些实施例中，从分组引擎、vServer(VIP)275A-C、网络接口卡(NIC)542D-E和/或设备200上包括的或者与设备200相关联的任何其他网络硬件或软件的角度实现数据并行机制。例如，每个核可运行同样的分组引擎或VIP代码或配置但是在不同的分布式数据集上进行操作。每个网络硬件或软件结构可接收不同的、变化的或者基本相同量的数据，因而可以具有变化的、不同的或相对相同量的负载515。

[0179] 在数据并行方法的情况下，可以基于VIP、NIC和/或VIP或NIC的数据流来划分和分布工作。在这些的方法的一个中，可通过使每个VIP在分布的数据集上工作来将多核系统的工作划分或者分布在VIP中。例如，可配置每个核运行一个或多个VIP。网络流量可分布在处理流量的每个VIP的核上。在这些方法的又一个中，可基于哪个NIC接收网络流量来将设备的工作划分或分布在核上。例如，第一NIC的网络流量可被分布到第一核，同时第二NIC的网络流量可被分布给第二核。一些情况下，核可处理来自多个NIC的数据。

[0180] 虽然图5A示出了与单个核505相关联的单个vServer，正如VIP1275A、VIP2275B和VIP3275C的情况。但是，一些实施例中，单个vServer可以与一个或者多个核505相关联。相反，一个或多个vServer可以与单个核505相关联。将vServer与核505关联可包括该核505处理与该特定vServer关联的所有功能。一些实施例中，每个核执行具有相同代码和配置的VIP。其他实施例中，每个核执行具有相同代码但配置不同的VIP。一些实施例中，每个核执行具有不同代码和相同或不同配置的VIP。

[0181] 和vServer类似，NIC也可以和特定的核505关联。许多实施例中，NIC可以连接到一个或多个核505，这样，当NIC接收或传输数据分组时，特定的核505处理涉及接收和传输数据分组的处理。一个实施例中，单个NIC可以与单个核505相关联，正如NIC1542D和NIC2542E的情况。其他实施例中，一个或多个NIC可以与单个核505相关联。但其他实施例中，单个NIC

可以与一个或者多个核505相关联。这些实施例中，负载可以分布在一个或多个核505上，使得每个核505基本上处理类似的负载量。与NIC关联的核505可以处理与该特定NIC关联的所有功能和/或数据。

[0182] 虽然根据VIP或NIC的数据将工作分布在核上具有某种程度的独立性，但是，一些实施例中，这会造成如图5A的变化负载515所示的核的不平衡的使用。

[0183] 一些实施例中，可根据任何类型或形式的数据流将负载、工作或网络流量分布在核505上。在这些方法的又一个中，可基于数据流将工作划分或分布在多个核上。例如，客户机或服务器之间的经过设备的网络流量可以被分布到多个核中的一个核并且由其处理。一些情况下，最初建立会话或连接的核可以是该会话或连接的网络流量所分布的核。一些实施例中，数据流基于网络流量的任何单元或部分，如事务、请求/响应通信或来自客户机上的应用的流量。这样，一些实施例中，客户机和服务器之间的经过设备200'的数据流可以比其他方式分布的更均衡。

[0184] 在基于流的数据并行机制520中，数据分布和任何类型的数据流相关，例如请求/响应对、事务、会话、连接或应用通信。例如，客户机或服务器之间的经过设备的网络流量可以被分布到多个核中的一个核并且由其处理。一些情况下，最初建立会话或连接的核可以是该会话或连接的网络流量所分布的核。数据流的分布可以使得每个核505运行基本相等或相对均匀分布的负载量、数据量或网络流量。

[0185] 一些实施例中，数据流基于网络流量的任何单元或部分，如事务、请求/响应通信或源自客户机上的应用的流量。这样，一些实施例中，客户机和服务器之间的经过设备200'的数据流可以比其他方式分布的更均衡。一个实施例中，可以基于事务或一系列事务分布数据量。一些实施例中，该事务可以是客户机和服务器之间的，其特征可以是IP地址或其他分组标识符。例如，核1505A可专用于特定客户机和特定服务器之间的事务，因此，核1505A上的负载515A可包括与特定客户机和服务器之间的事务相关联的网络流量。可通过将源自特定客户机或服务器的所有数据分组路由到核1505A来将网络流量分配给核1505A。

[0186] 虽然可部分地基于事务将工作或负载分布到核，但是，其他实施例中，可基于每个分组的基础分配负载或工作。这些实施例中，设备200可拦截数据分组并将数据分组分配给负载量最小的核505。例如，由于核1上的负载515A小于其他核505B-N上的负载515B-N，所以设备200可将第一到来的数据分组分配给核1505A。将第一数据分组分配给核1505A后，核1505A上的负载量515A与处理第一数据分组所需的处理资源量成比例增加。设备200拦截到第二数据分组时，设备200会将负载分配给核4505D，这是由于核4505D具有第二少的负载量。一些实施例中，将数据分组分配给负载量最小的核可确保分布到每个核505的负载515A-N保持基本相等。

[0187] 其他实施例中，将一部分网络流量分配给特定核505的情况下，可以每单元为基础分配负载。上述示例说明以每分组为基础进行负载平衡。其他实施例中，可以基于分组数目分配负载，例如，将每10个、100个或1000个分组分配给流量最少的核505。分配给核505的分组数量可以是由应用、用户或管理员确定的数目，而且可以为大于零的任何数。仍在其他实施例中，基于时间指标分配负载，使得在预定时间段将分组分布到特定核505。这些实施例中，可以在5毫秒内或者由用户、程序、系统、管理器或其他方式确定的任何时间段将分组分布到特定核505。预定时间段过去后，在预定时间段内将时间分组传输给不同的核505。

[0188] 用于将工作、负载或网络流量分布在一个或多个核505上的基于流的数据并行方法可包括上述实施例的任意组合。这些方法可以由设备200的任何部分执行，由在核505上执行的应用或者一组可执行指令执行，例如分组引擎，或者由在与设备200通信的计算装置上执行的任何应用、程序或代理执行。

[0189] 图5A所示的功能和数据并行机制计算方案可以任何方式组合，以产生混合并行机制或分布式处理方案，其包括功能并行机制500、数据并行机制540、基于流的数据并行机制520或者其任何部分。一些情况下，多核系统可使用任何类型或形式的负载平衡方案来将负载分布在一个或多个核505上。负载平衡方案可以和任何功能和数据平行方案或其组合结合使用。

[0190] 图5B示出多核系统545的实施例，该系统可以是任何类型或形式的一个或多个系统、设备、装置或组件。一些实施例中，该系统545可被包括在具有一个或多个处理核505A-N的设备200内。系统545还可包括与存储器总线556通信的一个或多个分组引擎(PE)或分组处理引擎(PPE)548A-N。存储器总线可用于与一个或多个处理核505A-N通信。系统545还可包括一个或多个网络接口卡(NIC)552和流分布器550，流分布器还可与一个或多个处理核505A-N通信。流分布器550可包括接收侧调整器(Receiver Side Scaler-RSS)或接收侧调整(Receiver Side Scaling-RSS)模块560。

[0191] 进一步参考图5B，具体而言，一个实施例中，分组引擎548A-N可包括此处所述的设备200的任何部分，例如图2A和2B所述设备的任何部分。一些实施例中，分组引擎548A-N可包括任何下列的元件：分组引擎240、网络堆栈267、高速缓存管理器232、策略引擎236、压缩引擎238、加密引擎234、GUI210、CLI212、壳服务214、监控程序216以及能够从数据总线556或一个或多个核505A-N中的任一个接收数据分组的其他任何软件和硬件元件。一些实施例中，分组引擎548A-N可包括一个或多个vServer275A-N或其任何部分。其他实施例中，分组引擎548A-N可提供以下功能的任意组合：SSL VPN280、内部网IP282、交换284、DNS286、分组加速288、APPFW280、如由监控代理197提供的监控、和作为TCP堆栈关联的功能、负载平衡、SSL卸载和处理、内容交换、策略评估、高速缓存、压缩、编码、解压缩、解码、应用防火墙功能、XML处理和加速以及SSL VPN连接。

[0192] 一些实施例中，分组引擎548A-N可以与特定服务器、用户、客户或网络关联。分组引擎548与特定实体关联时，分组引擎548可处理与该实体关联的数据分组。例如，如果分组引擎548与第一用户关联，那么该分组引擎548将对由第一用户产生的分组或者目的地址与第一用户关联的分组进行处理和操作。类似地，分组引擎548可选择不与特定实体关联，使得分组引擎548可对不是由该实体产生的或目的是该实体的任何数据分组进行处理和以其他方式进行操作。

[0193] 一些实例中，可将分组引擎548A-N配置为执行图5A所示的任何功能和/或数据并行方案。这些实例中，分组引擎548A-N可将功能或数据分布在多个核505A-N上，从而使得分布是根据并行机制或分布方案的。一些实施例中，单个分组引擎548A-N执行负载平衡方案，其他实施例中，一个或多个分组引擎548A-N执行负载平衡方案。一个实施例中，每个核505A-N可以与特定分组引擎548关联，使得可以由分组引擎执行负载平衡。在该实施例中，负载平衡可要求与核505关联的每个分组引擎548A-N和与核关联的其他分组引擎通信，使得分组引擎548A-N可共同决定将负载分布在何处。该过程的一个实施例可包括从每个分组

引擎接收对于负载的投票的仲裁器。仲裁器可部分地基于引擎投票的持续时间将负载分配给每个分组引擎548A-N，一些情况下，还可基于与在引擎关联的核505上的当前负载量相关联的优先级值来将负载分配给每个分组引擎548A-N。

[0194] 核上运行的任何分组引擎可以运行于用户模式、内核模式或其任意组合。一些实施例中，分组引擎作为在用户空间或应用空间中运行的应用或程序来操作。这些实施例中，分组引擎可使用任何类型或形式的接口来访问内核提供的任何功能。一些实施例中，分组引擎操作于内核模式中或作为内核的一部分来操作。一些实施例中，分组引擎的第一部分操作于用户模式中，分组引擎的第二部分操作于内核模式中。一些实施例中，第一核上的第一分组引擎执行于内核模式中，同时，第二核上的第二分组引擎执行于用户模式中。一些实施例中，分组引擎或其任何部分对NIC或其任何驱动器进行操作或者与其联合操作。

[0195] 一些实施例中，存储器总线556可以是任何类型或形式的存储器或计算机总线。虽然在图5B中描述了单个存储器总线556，但是系统545可包括任意数量的存储器总线556。一个实施例中，每个分组引擎548可以和一个或者多个单独的存储器总线556相关联。

[0196] 一些实施例中，NIC552可以是此处所述的任何网络接口卡或机制。NIC552可具有任意数量的端口。NIC可设计并构造成连接到任何类型和形式的网络104。虽然示出单个NIC552，但是，系统545可包括任意数量的NIC552。一些实施例中，每个核505A-N可以与一个或多个单个NIC552关联。因而，每个核505可以与专用于特定核505的单个NIC552关联。

[0197] 核505A-N可包括此处所述的任何处理器。此外，可根据此处所述的任何核505配置来配置核505A-N。另外，核505A-N可具有此处所述的任何核505功能。虽然图5B示出七个核505A-G，但是系统545可包括任意数量的核505。具体而言，系统545可包括N个核，其中N是大于零的整数。

[0198] 核可具有或使用被分配或指派用于该核的存储器。可将存储器视为该核的专有或本地存储器并且仅有该核可访问该存储器。核可具有或使用共享的或指派给多个核的存储器。该存储器可被视为由不只一个核可访问的公共或共享存储器。核可使用专有或公共存储器的任何组合。通过每个核的单独的地址空间，消除了使用同一地址空间的情况下的一些协调级别。利用单独的地址空间，核可以对核自己的地址空间中的信息和数据进行工作，而不用担心与其他核冲突。每个分组引擎可以具有用于TCP和/或SSL连接的单独存储器池。

[0199] 仍参考图5B，上文结合图5A描述的核505的任何功能和/或实施例可以部署在上文结合图4A和4B描述的虚拟化环境的任何实施例中。不是以物理处理器505的形式部署核505的功能，而是将这些功能部署在诸如客户机102、服务器106或设备200的任何计算装置100的虚拟化环境400内。其他实施例中，不是以设备或一个装置的形式部署核505的功能，而是将该功能部署在任何布置的多个装置上。例如，一个装置可包括两个或多个核，另一个装置可包括两个或多个核。例如，多核系统可包括计算装置的集群、服务器群或计算装置的网络。一些实施例中，不是以核的形式部署核505的功能，而是将该功能部署在多个处理器上，例如部署多个单核处理器上。

[0200] 一个实施例中，核505可以为任何形式或类型的处理器。一些实施例中，核的功能可以基本类似此处所述的任何处理器或中央处理单元。一些实施例中，核505可包括此处所述的任何处理器的任何部分。虽然图5A示出7个核，但是，设备200内可以有任意N个核，其中N是大于1的整数。一些实施例中，核505可以安装在公用设备200内，其他实施例中，核505可

以安装在彼此通信连接的一个或多个设备200内。一些实施例中，核505包括图形处理软件，而其他实施例中，核505提供通用处理能力。核505可彼此物理靠近地安装和/或可彼此通信连接。可以用以物理方式和/或通信方式耦合到核的任何类型和形式的总线或子系统连接核，用于向核、从核和/或在核之间传输数据。

[0201] 尽管每个核505可包括用于与其他核通信的软件，一些实施例中，核管理器(未示出)可有助于每个核505之间的通信。一些实施例中，内核可提供核管理。核可以使用各种接口机制彼此接口或通信。一些实施例中，可以使用核到核的消息传送来在核之间通信，比如，第一核通过连接到核的总线或子系统向第二核发送消息或数据。一些实施例中，核可通过任何种类或形式的共享存储器接口通信。一个实施例中，可以存在在所有核中共享的一个或多个存储器单元。一些实施例中，每个核可以具有和每个其他核共享的单独存储器单元。例如，第一核可具有与第二核的第一共享存储器，以及与第三核的第二共享存储器。一些实施例中，核可通过任何类型的编程或API(如通过内核的函数调用)来通信。一些实施例中，操作系统可识别并支持多核装置，并提供用于核间通信的接口和API。

[0202] 流分布器550可以是任何应用、程序、库、脚本、任务、服务、进程或在任何类型或形式的硬件上执行的任何类型和形式的可执行指令。一些实施例中，流分布器550可以是用于执行此处所述任何操作和功能的任何电路设计或结构。一些实施例中，流分布器分布、转发、路由、控制和/或管理多个核505上的数据和/或在核上运行的分组引擎或VIP的分布。一些实施例中，可将流分布器550称为接口主装置(interface master)。一个实施例中，流分布器550包括在设备200的核或处理器上执行的一组可执行指令。又一个实施例中，流分布器550包括在与设备200通信的计算机器上执行的一组可执行指令。一些实施例中，流分布器550包括在如固件的NIC上执行的一组可执行指令。其他实施例，流分布器550包括用于将数据分组分布在核或处理器上的软件和硬件的任何组合。一个实施例中，流分布器550在至少一个核505A-N上执行，而在其他实施例中，分配给每个核505A-N的单独的流分布器550在相关联的核505A-N上执行。流分布器可使用任何类型和形式的统计或概率算法或决策来平衡多个核上的流。可以将如NIC的设备硬件或内核设计或构造成支持NIC和/或核上的顺序操作。

[0203] 系统545包括一个或多个流分布器550的实施例中，每个流分布器550可以与处理器505或分组引擎548关联。流分布器550可包括允许每个流分布器550和在系统545内执行的其他流分布器550通信的接口机制。一个实例中，一个或多个流分布器550可通过彼此通信确定如何平衡负载。该过程的操作可以基本与上述过程类似，即将投票提交给仲裁器，然后仲裁器确定哪个流分布器550应该接收负载。其他实施例中，第一流分布器550'可识别所关联的核上的负载并基于任何下列标准确定是否将第一数据分组转发到所关联的核：所关联的核上的负载大于预定阈值；所关联的核上的负载小于预定阈值；所关联的核上的负载小于其他核上的负载；或者可以用于部分基于处理器上的负载量来确定将数据分组转发到何处的任何其他指标。

[0204] 流分布器550可以根据如此处所述的分布、计算或负载平衡方法而将网络流量分布在核505上。一个实施例中，流分布器可基于功能并行机制分布方案550、数据并行机制负载分布方案540、基于流的数据并行机制分布方案520或这些分布方案的任意组合或用于将负载分布在多个处理器上的任何负载平衡方案来分布网络流量。因而，流分布器550可通过

接收数据分组并根据操作的负载平衡或分布方案将数据分组分布在处理器上而充当负载分布器。一个实施例中，流分布器550可包括用于确定如何相应地分布分组、工作或负载的一个或多个操作、函数或逻辑。又一个实施例中，流分布器550可包括可识别与数据分组关联的源地址和目的地址并相应地分布分组的一个或多个子操作、函数或逻辑。

[0205] 一些实施例中，流分布器550可包括接收侧调整(RSS)网络驱动器模块560或将数据分组分布在一个或多个核505上的任何类型和形式的可执行指令。RSS模块560可以包括硬件和软件的任意组合。一些实施例中，RSS模块560和流分布器550协同工作以将数据分组分布在核505A-N或多处理器网络中的多个处理器上。一些实施例中，RSS模块560可在NIC552中执行，其他实施例中，可在核505的任何一个上执行。

[0206] 一些实施例中，RSS模块560使用微软接收侧调整(RSS)方法。一个实施例中，RSS是微软可扩展网络主动技术(Microsoft Scalable Networking initative technology)，其使得系统中的多个处理器上的接收处理是平衡的，同时保持数据的顺序传送。RSS可使用任何类型或形式的哈希方案来确定用于处理网络分组的核或处理器。

[0207] RSS模块560可应用任何类型或形式的哈希函数，如Toeplitz哈希函数。哈希函数可应用到哈希类型值或者任何值序列。哈希函数可以是任意安全级别的安全哈希或者是以其他方式加密。哈希函数可使用哈希关键字(hash key)。关键字的大小取决于哈希函数。对于Toeplitz哈希，用于IPv6的哈希关键字大小为40字节，用于IPv4的哈希关键字大小为16字节。

[0208] 可以基于任何一个或多个标准或设计目标设计或构造哈希函数。一些实施例中，可使用为不同的哈希输入和不同哈希类型提供均匀分布的哈希结果的哈希函数，所述不同哈希输入和不同哈希类型包括TCP/IPv4、TCP/IPv6、IPv4和IPv6头部。一些实施例中，可使用存在少量桶时(例如2个或4个)提供均匀分布的哈希结果的哈希函数。一些实施例中，可使用存在大量桶时(例如64个桶)提供随机分布的哈希结果的哈希函数。在一些实施例中，基于计算或资源使用水平来确定哈希函数。在一些实施例中，基于在硬件中实现哈希的难易度来确定哈希函数。在一些实施例中，基于用恶意的远程主机发送将全部哈希到同一桶中的分组的难易度来确定哈希函数。

[0209] RSS可从任意类型和形式的输入来产生哈希，例如值序列。该值序列可包括网络分组的任何部分，如网络分组的任何头部、域或载荷或其一部分。一些实施例中，可将哈希输入称为哈希类型，哈希输入可包括与网络分组或数据流关联的任何信息元组，例如下面的类型：包括至少两个IP地址和两个端口的四元组、包括任意四组值的四元组、六元组、二元组和/或任何其他数字或值序列。以下是可由RSS使用的哈希类型示例：

[0210] -源TCP端口、源IP版本4(IPv4)地址、目的TCP端口和目的IPv4地址的四元组。

[0211] -源TCP端口、源IP版本6(IPv6)地址、目的TCP端口和目的IPv6地址的四元组。

[0212] -源IPv4地址和目的IPv4地址的二元组。

[0213] -源IPv6地址和目的IPv6地址的二元组。

[0214] -源IPv6地址和目的IPv6地址的二元组，包括对解析IPv6扩展头部的支持。

[0215] 哈希结果或其任何部分可用于识别用于分布网络分组的核或实体，如分组引擎或VIP。一些实施例中，可向哈希结果应用一个或者多个哈希位或掩码。哈希位或掩码可以是任何位数或字节数。NIC可支持任意位，例如7位。网络堆栈可在初始化时设定要使用的实际

位数。位数介于1和7之间，包括端值。

[0216] 可通过任意类型和形式的表用哈希结果来识别核或实体，例如通过桶表(bucket table)或间接表(indrection table)。一些实施例中，用哈希结果的位数来索引表。哈希掩码的范围可有效地限定间接表的大小。哈希结果的任何部分或哈希结果自身可用于索引间接表。表中的值可标识任何核或处理器，例如通过核或处理器标识符来标识。一些实施例中，表中标识多核系统的所有核。其他实施例中，表中标识多核系统的一部分核。间接表可包括任意多个桶，例如2到128个桶，可以用哈希掩码索引这些桶。每个桶可包括标识核或处理器的索引值范围。一些实施例中，流控制器和/或RSS模块可通过改变间接表来重新平衡网络负载。

[0217] 一些实施例中，多核系统575不包括RSS驱动器或RSS模块560。在这些实施例的一些中，软件操控模块(未示出)或系统内RSS模块的软件实施例可以和流分布器550共同操作或者作为流分布器550的一部分操作，以将分组引导到多核系统575中的核505。

[0218] 一些实施例中，流分布器550在设备200上的任何模块或程序中执行，或者在多核系统575中包括的任何一个核505和任一装置或组件上执行。一些实施例中，流分布器550'可在第一核505A上执行，而在其他实施例中，流分布器550"可在NIC552上执行。其他实施例中，流分布器550'的实例可在多核系统575中包括的每个核505上执行。该实施例中，流分布器550'的每个实例可和流分布器550'的其他实例通信以在核505之间来回转发分组。存在这样的状况，其中，对请求分组的响应不是由同一核处理的，即第一核处理请求，而第二核处理响应。这些情况下，流分布器550'的实例可以拦截分组并将分组转发到期望的或正确的核505，即流分布器550'可将响应转发到第一核。流分布器550'的多个实例可以在任意数量的核505或核505的任何组合上执行。

[0219] 流分布器可以响应于任一个或多个规则或策略而操作。规则可识别接收网络分组、数据或数据流的核或分组处理引擎。规则可识别和网络分组有关的任何类型和形式的元组信息，例如源和目的IP地址以及源和目的端口的四元组。基于所接收的匹配规则所指定的元组的分组，流分布器可将分组转发到核或分组引擎。一些实施例中，通过共享存储器和/或核到核的消息传输将分组转发到核。

[0220] 虽然图5B示出了在多核系统575中执行的流分布器550，但是，一些实施例中，流分布器550可执行在位于远离多核系统575的计算装置或设备上。这样的实施例中，流分布器550可以和多核系统575通信以接收数据分组并将分组分布在一个或多个核505上。一个实施例中，流分布器550接收以设备200为目的地的数据分组，向所接收的数据分组应用分布方案并将数据分组分布到多核系统575的一个或多个核505。一个实施例中，流分布器550可以被包括在路由器或其他设备中，这样路由器可以通过改变与每个分组关联的元数据而以特定核505为目的地，从而每个分组以多核系统575的子节点为目的地。这样的实施例中，可用CISCO的vn-tag机制来改变或标记具有适当元数据的每个分组。

[0221] 图5C示出包括一个或多个处理核505A-N的多核系统575的实施例。简言之，核505中的一个可被指定为控制核505A并可用作其他核505的控制平面570。其他核可以是次级核，其工作于数据平面，而控制核提供控制平面。核505A-N共享全局高速缓存580。控制核提供控制平面，多核系统中的其他核形成或提供数据平面。这些核对网络流量执行数据处理功能，而控制核提供对多核系统的初始化、配置和控制。

[0222] 仍参考图5C，具体而言，核505A-N以及控制核505A可以是此处所述的任何处理器。此外，核505A-N和控制核505A可以是能在图5C所述系统中工作的任何处理器。另外，核505A-N可以是此处所述的任何核或核组。控制核可以是与其他核不同类型的核或处理器。一些实施例中，控制核可操作不同的分组引擎或者具有与其他核的分组引擎配置不同的分组引擎。

[0223] 每个核的存储器的任何部分可以被分配给或者用作核共享的全局高速缓存。简而言之，每个核的每个存储器的预定百分比或预定量可用作全局高速缓存。例如，每个核的每个存储器的50%可用作或分配给共享全局高速缓存。也就是说，所示实施例中，除了控制平面核或核1以外的每个核的2GB可用于形成28GB的共享全局高速缓存。例如通过配置服务而配置控制平面可确定用于共享全局高速缓存的存储量(the amount of memory)。一些实施例中，每个核可提供不同的存储量供全局高速缓存使用。其他实施例中，任一核可以不提供任何存储器或不使用全局高速缓存。一些实施例中，任何核也可具有未分配给全局共享存储器的存储器中的本地高速缓存。每个核可将网络流量的任意部分存储在全局共享高速缓存中。每个核可检查高速缓存来查找要在请求或响应中使用的任何内容。任何核可从全局共享高速缓存获得内容以在数据流、请求或响应中使用。

[0224] 全局高速缓存580可以是任意类型或形式的存储器或存储元件，例如此处所述的任何存储器或存储元件。一些实施例中，核505可访问预定的存储量(即32GB或者与系统575相当的任何其他存储量)。全局高速缓存580可以从预定的存储量分配而来，同时，其余的可用存储器可在核505之间分配。其他实施例中，每个核505可具有预定的存储量。全局高速缓存580可包括分配给每个核505的存储量。该存储量可以字节为单位来测量，或者可用分配给每个核505的存储器百分比来测量。因而，全局高速缓存580可包括来自与每个核505关联的存储器的1GB存储器，或者可包括和每个核505关联的存储器的20%或一半。一些实施例，只有一部分核505提供存储器给全局高速缓存580，而在其他实施例，全局高速缓存580可包括未分配给核505的存储器。

[0225] 每个核505可使用全局高速缓存580来存储网络流量或缓存数据。一些实施例中，核的分组引擎使用全局高速缓存来缓存并使用由多个分组引擎所存储的数据。例如，图2A的高速缓存管理器和图2B的高速缓存功能可使用全局高速缓存来共享数据以用于加速。例如，每个分组引擎可在全局高速缓存中存储例如HTML数据的响应。操作于核上的任何高速缓存管理器可访问全局高速缓存来将高速缓存响应提供给客户请求。

[0226] 一些实施例中，核505可使用全局高速缓存580来存储端口分配表，其可用于部分基于端口确定数据流。其他实施例中，核505可使用全局高速缓存580来存储地址查询表或任何其他表或列表，流分布器可使用这些表来确定将到来的数据分组和发出的数据分组导向何处。一些实施例中，核505可以读写高速缓存580，而其他实施例中，核505仅从高速缓存读或者仅向高速缓存写。核可使用全局高速缓存来执行核到核通信。

[0227] 可以将全局高速缓存580划分成各个存储器部分，其中每个部分可专用于特定核505。一个实施例中，控制核505A可接收大量的可用高速缓存，而其他核505可接收对全局高速缓存580的变化的访问量。

[0228] 一些实施例中，系统575可包括控制核505A。虽然图5C将核1505A示为控制核，但是，控制核可以是设备200或多核系统中的任何一个核。此外，虽然仅描述了单个控制核，但

是，系统575可包括一个或多个控制核，每个控制核对系统有某种程度的控制。一些实施例中，一个或多个控制核可以各自控制系统575的特定方面。例如，一个核可控制决定使用哪种分布方案，而另一个核可确定全局高速缓存580的大小。

[0229] 多核系统的控制平面可以是将一个核指定并配置成专用的管理核或者作为主核。控制平面核可对多核系统中的多个核的操作和功能提供控制、管理和协调。控制平面核可对多核系统中的多个核上存储器系统的分配和使用提供控制、管理和协调，这包括初始化和配置存储器系统。一些实施例中，控制平面包括流分布器，用于基于数据流控制数据流到核的分配以及网络分组到核的分配。一些实施例中，控制平面核运行分组引擎，其他实施例中，控制平面核专用于系统的其他核的控制和管理。

[0230] 控制核505A可对其他核505进行某种级别的控制，例如，确定将多少存储器分配给每个核505，或者确定应该指派哪个核来处理特定功能或硬件/软件实体。一些实施例中，控制核505A可以对控制平面570中的这些核505进行控制。因而，控制平面570之外可存在不受控制核505A控制的处理器。确定控制平面570的边界可包括由控制核505A或系统575中执行的代理维护由控制核505A控制的核的列表。控制核505A可控制以下的任一个：核初始化、确定核何时不可用、一个核出故障时将负载重新分配给其他核505、决定实现哪个分布方案、决定哪个核应该接收网络流量、决定应该给每个核分配多少高速缓存、确定是否将特定功能或元件分布到特定核、确定是否允许核彼此通信、确定全局高速缓存580的大小以及对系统575内的核的功能、配置或操作的任何其他确定。

[0231] F.用于提供策略组的系统和方法

[0232] 通信和数据网络向用户提供对网络资源的访问，该网络资源例如是文件、应用以及服务。为了有效地管理和保护网络资源，需要系统和方法来控制对受保护的和/或有限资源的访问。随着资源类型、网络、活动、通信协议和用户类别的增加，访问控制方案已变得越来越复杂。例如，访问控制方案可包括下列的任一个或者多个：认证、授权、证书验证、访问控制列表(ACL)、访问规则和/或策略、防火墙、负载和/或功率平衡、有限资源的分配、建立安全连接(例如SSL VPN)、会话重用、用户和/或用户组权限，以及密钥加密。由于各种访问控制方案可能需要相互协调运行来管理资源，因而出于访问控制的目的，将多种访问配置聚合到一个策略组中十分有利。诸如访问网关、防火墙以及认证、授权和审计(AAA)服务器的网络组件可以响应于对资源的请求来访问和/或应用这样的策略组。

[0233] 在一些实施例中，可以将访问配置的智能配置称作策略组。也可以将策略组称作访问配置组或智能组。策略组可以被设计为、建立为和/或配置为智能地和逻辑地聚合多个访问配置。出于访问控制的目的，策略组可聚合访问配置的补充集合和/或复合集合。策略组能够根据访问配置类型逻辑地组织、安排或关联多个访问配置。策略组可基于逻辑安排或者关联系统性地应用和/或评估多个访问配置。例如，在一些实施例中，应用不同类型的访问配置获得的结果可以逻辑地“与”(AND)在一起。

[0234] 策略组可包括一个或多个级别的访问配置。策略组可基于功能、优先极等将多个访问配置安排为不同级别。在一些实施例中，在最高级别策略组包括两个或更多组件，如标准和资源。例如，标准组件可包括登录点(login point)、装置描述文件和组访问配置。在一些实施例中，策略组可具有一种或多种访问配置类型和/或省略或者漏掉的级别。策略组可包括默认动作和/或任何访问配置类型的性质和/或省略或者漏掉的级别。策略组可提供访

问配置之间的冲突解决方案。

[0235] 在各个实施例中，可将策略组用作单个模块，该单个模块包括来自多个访问配置的策略、参数、性质和设置。在一些实施例中，可基于为用户识别和/或评估的一个或多个访问配置来为该用户确定(identify)一个或多个策略组。一旦确定，可以应用和/或评估来自这些策略组中每一个的另外的关联访问配置。例如，可基于初始访问控制活动和结果动态地确定策略组。可基于由策略组要求的对访问配置的评估来聚集或达成最终的访问控制决策。在一些实施例中，策略组可生成更加全面、优化或合适的访问控制决策。策略组可基于对策略组中各种级别和类型的访问配置进行互操作来生成这种访问控制决策。策略组可基于策略组中访问配置的广度、综合性以及协作交互来生成这种访问控制决策。

[0236] 现参考图6A，示出了提供策略组677用于控制对网络资源的访问的系统600的一个实施例。简要概括，该系统包括一网络装置，该网络装置包括策略管理器667。策略管理器667包括、提供和/或应用一个或多个策略组。策略组677可包括一个或多个访问配置。例如，可以为登录点、资源标识和可用权限、装置描述文件676和/或组名688定义访问配置。每个登录点可与至少一种认证方法和授权方法相关联。

[0237] 在图6A的进一步细节中，网络装置200可以是、或者包括与网络或网络节点关联的任何类型或形式的组件。举例来说，在一个实施例中，该网络装置可包括来自在上文中结合图1A-1D、2A、2B、4A、4C和5A描述的网络设备或中间装置200的任何实施例的特征。在各个实施例中，网络装置200可以是独立的装置、网络组件的附件，或者网络组件的模块。网络装置200可被设计为、建立为和/或配置为提供或控制对网络资源的访问。可将网络装置200设计为、建立为和/或配置为允许用户配置或者重新配置访问配置或策略组677用以控制对网络资源的访问。网络装置200可以为用户或应用提供任何类型或形式的接口来请求访问资源。网络装置200可以为用户或应用提供任何类型或形式的接口来配置或重新配置访问配置或策略组677。所提供的接口可包括在上文中结合了图1E、1F和2A描述的接口126、127、130、210、212、214的任何实施例的一个或多个特征。

[0238] 网络装置200可包括一个或多个策略管理器。每个策略管理器可以作为该网络装置上的虚拟服务器来实现，如在上文中结合图2B和4A-4C描述的虚拟服务器275和406。每个策略管理器667可以在如上文结合图5A-5C描述的多核系统的一个处理器上执行。在一些实施例中，策略管理器667包括在上文中结合图1D和2A描述的策略引擎195和236的任何实施例的一个或多个特征。在某些实施例中，策略管理器667提供替换或补充策略引擎的功能。策略管理器667可包括硬件或者软件和硬件的任意组合。策略管理器667可包括应用、程序、库、脚本、进程、任务、线程或在硬件上执行的任何类型和形式的指令，该硬件例如网络装置的处理器。策略管理器667可包括一个或多个存储装置或与一个或多个存储装置通信，该存储装置用于存储和/或检索策略组和/或访问配置。每个存储装置可包括来自在上文中结合图1D、1E、2A、4A、5B和5C描述的存储装置128、122、140、232、264、442、556、580的任何实施例的特征。在一些实施例中，可将该一个或多个存储装置联网，例如，作为存储区域网络(SAN)来实现。

[0239] 可将策略管理器667设计和构造为存储、提供、服务、执行、管理、生成和/或配置策略组677和/或访问配置。举例说明，在一个实施例中，管理员经由策略管理器667的接口来配置策略组677。在一些实施例中，策略管理器667可包括用于组织和检索可用的策略组677

的数据库管理和/或检索系统。策略管理器667可响应于对资源的请求来生成、识别、检索和/或应用一个或多个可应用的策略组。例如，在一个实施例中，策略管理器667可响应于访问网络文件的用户请求来识别和应用策略组677。在另一个实施例中，对于接收访问请求的访问网关或另一装置的申请，策略管理器667可向该访问网关或另一装置识别和提供策略组677。

[0240] 在某些实施例中，策略管理器667根据策略组677来协调和/或管理由各种网络模块或服务(例如，下列中的一个或多个的任意组合：AAA服务器、访问服务器、登录页面web服务器、资源和/或策略的存储装置，和/或用于收集关于客户机装置的计算环境的信息的收集代理)提供的功能。在一些实施例中，策略管理器667与这些网络模块或服务的一个或多个通信和/或收集来自这些网络模块或服务的一个或多个的信息，从而结合策略组677做出策略决策用于访问控制。可用一个或多个策略组(例如，基础或默认策略组)来预先配置或者预先构建系统600和/或策略管理器667用于部署。可以重新配置和/或组合这些策略组用于部署。

[0241] 如上文所述，策略组677可包括一个或多个访问配置。在一些实施例中，可将策略组677称作智能组(Smart Group)。访问配置可包括、描述和/或指定一个或多个访问控制方案的特征、需求、规则和/或策略，例如用于认证、授权、证书验证、访问控制表(ACL)操作、管理应用需求、防火墙操作、负载和/或功率平衡、有限资源分配、建立安全连接(如SSL VPN)、管理用户和/或用户组权限、管理装置需求、会话重用和密钥加密。在一些实施例中，访问配置可识别提供用于访问控制的特征、需求、信息、规则和/或策略的网络模块或服务。每个访问配置可能属于多种访问配置类型中的一种，例如登录点类型、装置描述文件类型、资源类型、IP地址池类型或者组名类型。策略组677可包括特定类型的一个或多个访问配置。如果没有用访问配置或特定类型的访问配置来配置策略组677，则策略管理器667可提供默认的动作、访问配置和/或策略来代替缺少的访问配置。

[0242] 在一些实施例中，可以将策略组677的访问配置分配、划分、分组或分类为策略组677的一个或多个组件。例如在一个实施例中，一个组件可包括与规则或标准相关的访问配置，例如，登录点678、装置描述文件676和组688(或组名)。另一组件可包括与资源和这些资源的访问权限(例如，允许、拒绝、不同的访问级别)相关的一个或多个访问配置。策略组677可以不包括与标准相关或与资源相关的访问配置，或者包括与标准相关或与资源相关的访问配置中的一个或多个。

[0243] 每个策略组677可以逻辑地组合、区分优先级和/或管理例如相同类型或不同类型的一个或多个访问配置。策略组677可以为相同类型(例如，装置描述文件676)的访问配置来定义或实现“或”(OR)逻辑操作或者组合。举例说明，在一个实施例中，将具有便携式装置描述文件676和移动装置描述文件的策略组677应用到是便携式计算机的客户机装置可产生该客户机装置满足这两种描述文件的OS需求的确定。因此，策略组677可基于满足这些描述文件中的任何一个来授予对所请求资源的访问级别。在另一个实施例中，向是PDA电话的客户机装置应用同一策略组677可产生该客户机装置仅满足移动装置描述文件的OS需求的确定。策略组677可根据满足装置描述文件676之一，例如移动装置描述文件，来授予对所请求资源的相同访问级别。

[0244] 策略组677可以为不同类型的访问配置(例如，装置描述文件访问配置676和组名

访问配置688之间)来定义或实现“与”(AND)逻辑操作或者组合。例如在一个实施例中,如果676访问配置和组名访问配置688两者均满足,策略组677可授予对资源的访问权限。举例说明,如果应用了具有两个登录点678(lp1,lp2)和一个装置描述文件676(dp1)的策略组677,则用于访问控制决策的规则语句可以逻辑地表示为:

[0245] IF(lp1OR lp2)AND dp1THEN…

[0246] 在另一个示例和实施例中,如果应用了具有两个登录点678(lp1,lp2)和两个装置描述文件676(dp1,dp2)的策略组677,则用于访问控制决策的规则语句可以逻辑地表示为:

[0247] IF(lp1OR lp2)AND(dp1OR dp2)THEN…

[0248] 在一些实施例中,策略组677包括一个或多个登录点访问配置(后文有时总称为“登录点”)。登录点678可以表示系统600、会话和/或连接的入口点,例如用于访问网络资源。登录点678可包括登录页或者任何类型或形式的接口(例如,包括在上文中结合图1E、1F和2A描述的接口126、127、130、210、212、214的任何实施例的一个或多个特征)。用户可经由URL或者任何类型或形式的web链接、桌面小程序或者图标来访问登录点678。可通过URL或任何类型或形式的web链接、桌面小程序或图标来标识或表示登录点678。例如在一个实施例中,可通过选择或点击URL来选择登录点678。可识别与所选登录点678关联的一个或多个策略组以用于评估。在一些实施例中,响应于经由登录点应用的一种或多种认证和/或授权方法690来选择该一个或多个识别的策略组的子集以用于评估。在其他实施例中,响应于经由登录点应用的一个或多个认证和/或授权方法690来识别一个或多个策略组用于评估。

[0249] 在一些实施例中,策略组677可要求为该策略组677定义或配置至少一个登录点678。在其他实施例中,可以为没有定义或配置的登录点的策略组677分配默认登录点678。在又一个实施例中,可基于用户访问的任何登录点678(例如基于所选登录点的相关的认证和/或授权结果)来选择没有定义或配置的登录点678的策略组677。为所选登录点678定义的性质可优先于(override)全局性质。例如在一个实施例中,所选登录点678可要求双重认证来代替由全局规则要求的单一类型的认证。策略组677的性质可优先于登录点678和/或全局性质。

[0250] 可以用一种或多种认证和/或授权方法690来配置登录点678。举例说明,在一些实施例中,登录点678可具有与其关联的两种认证方法699,有时称作双重验证。登录点678(例如经由认证和/或授权)可请求用户信息或者用户响应,例如用户标识(用户ID)、密码、验证问题的答案、RSA(Rivest,Shamir and Adleman)securID和/或生物信息。可基于识别如来自可信来源、现有安全会话和/或来自安全网络内部的访问请求来删减、绕过或跳过一个或多个认证方法699和/或授权方法690。在一些实施例中,可基于(例如由用户)选择的认证方法699来调用或选择一个或多个授权方法690。表F1示出了基于所选认证方法的授权方法选择过程的一个实施例。例如,如果所选认证方法是RSA,则所选授权方法690可以包括RSA、轻量级目录访问协议(LDAP)和活动目录(AD)中的一个或多个。如果所选认证方法是远程认证拨号用户服务(RADIUS),所选授权方法690则可以包括RADIUS、LDAP、AD中的一个或多个。

[0251] 表F1:授权方法选择

[0252]

认证	授权
RSA	RSA,LDAP,AD

RADIUS	RADIUS,LDAP,AD
AD	LDAP,AD

[0253] 在一些实施例中，可以(例如，由管理员或根据计划表)禁用登录点678。禁用登录点678可改变与该登录点关联的策略组677的行为。例如在一个实施例中，如果禁用了策略组677中的唯一登录点678，则该策略组677可能变为不可用。如果调用或评估该策略组677，则可能返回空集。在一个实施例中，这种策略组677可丧失其授予访问资源或拒绝访问资源的能力。如果策略组677中存在至少另一未被禁用的登录点678，则可基于该至少另一未被禁用的活动登录点678来评估策略组677。在其他实施例中，如果禁用了策略组677中的所有登录点678，则可以例如通过合并全局或默认登录点678来启用一登录点678。

[0254] 在一些实施例中，登录点678可能具有配置到或附属于该登录点的一个或多个可见性装置描述文件。登录点678可具有配置到或附属于该一个或多个可见性装置描述文件的评估属性。该评估属性可被配置为在两个或更多可见性装置描述文件之间应用“与”或者“或”逻辑函数。例如在一个实施例中，如果评估属性被设置为“与”，如果根据请求客户机装置成功地评估了所有可见性装置描述文件或者所有可见性装置描述文件成功匹配请求客户机装置，则可使登录点678变为可见(例如，可用、启动或有效)。例如在另一个实施例中，如果评估属性被设置为“与”，如果根据请求客户机装置未成功评估任何一个或多个可见性装置描述文件或者任何一个或多个可见性装置描述文件未成功匹配请求客户机装置，则可使登录点678变为不可见(例如，不可用、禁用或无效)。

[0255] 系统600可以经由策略管理器667或收集代理来执行对客户机装置的扫描或端点分析从而收集信息(例如计算环境特征)。可根据一个或多个可见性装置描述文件来评估装置信息从而确定登录点的可见性。装置信息可包括、但不限于：装置类型、OS类型和OS路径信息、软件应用(例如web浏览器)和路径信息、防病毒软件版本和更新、防火墙信息、处理器类型和处理能力、总线速度和带宽、存储器或存储信息、客户机装置是否是可信装置、客户机装置的机器ID、客户机节点的MAC或其他地址、安装的网卡和其他硬件、与客户机装置关联的数字水印、活动目录中的成员、网络连接信息、客户机装置证书和授权证书。例如在一些实施例中，客户机装置的数字水印可包括数据嵌入。水印可包括插入到文件中的数据形式以便提供关于该文件的来源或版权信息。水印可包括数字哈希文件以便提供篡改检测。在一些实施例中，网络连接信息涉及带宽能力。在其他实施例中，网络连接信息涉及或者包括互联网协议(IP)地址。

[0256] 在某些实施例中，如果中断、取消或提前终止装置扫描(或者端点分析)，则可将对应的装置描述文件评估确定为不成功的或不完全的。在一些实施例中可发出错误并且可发起重新扫描。在一些实施例中，可将为了可见性的目的而配置的装置描述文件676用于与策略组677关联的扫描后的评估。可见性装置描述文件可指定和/或请求一个或多个客户机装置属性。这些客户机属性可能覆盖由装置扫描所收集的装置信息的任何方面，例如在上文中描述的那些。可基于任何访问控制事件来发起装置扫描，例如当系统接收访问请求时、当选择登录点678时，或者当识别了策略组677时。网络装置可将收集代理传输到客户机节点以收集客户机信息。网络装置可与客户机装置通信以收集关于该客户机装置的信息。在一些实施例中，比起评估可见性装置描述文件所需的信息，装置扫描可收集更多的信息。装置扫描可根据要收集的指定或标准数据列表来收集信息。装置扫描可基于一个或多个策略的

应用来收集信息。

[0257] 在一些实施例中，策略组677包括一个或多个装置描述文件访问配置。在这些实施例的一些中，可将这些访问配置称作装置描述文件676用于扫描后的评估。这些访问配置可以与在上文中描述的可见性装置描述文件相同或改编自在上文中描述的可见性装置描述文件。在一些实施例中，扫描后装置描述文件676可能与可见性装置描述文件有区别。可根据正从装置扫描收集的信息和/或根据已经从装置扫描收集的信息来评估扫描后装置描述文件676。装置描述文件676可指定和/或请求一个或多个客户机装置属性。这种客户机属性可覆盖由装置扫描收集的装置信息的任何方面。装置描述文件676可(例如经由策略)指定和/或要求客户机节点中的某些操作能力和/或安全特征。

[0258] 可以将扫描后装置描述文件676用作策略组677的一部分以确定客户机装置的访问权限。在一些实施例中，策略组677可能不与任何装置描述文件访问配置相关联。在某些实施例中，如果没有为所选择的策略组677配置任何装置描述文件676，则可以简单地将装置描述文件676从对应的访问控制决策中排除。在其他实施例，可将默认和/或全局装置描述文件与没有配置任何装置描述文件676的所选择的策略组677一起应用。

[0259] 可基于所应用的认证和/或授权方法690将用户用一个或多个组来识别。基于该识别，可以将与该一个或多个组关联的一个或多个策略组677用于做出该用户的访问控制策略确定。在一些实施例中，策略组677可与一个或多个组相关联。该一个或多个组688中每个可由一个组名来识别。组名可包括任何字母数字和/或特殊字符。在一些实施例中，组名可以是不分大小写的。在某些实施例中，系统可从策略组677的名称中提取一个或多个组名688。在其他实施例中，系统不应使用策略组677的名称来推断或提取与该策略组677关联的组名688。

[0260] 组688可包括或者识别一个或多个用户。组688可识别用户的一个或多个属性。具有一个或多个识别的属性的用户可与该组关联或被分配到该组。如果请求访问资源的用户被关联到在策略组677中识别的组688，则可以应用该策略组677来确定该用户的访问控制。如果组688与多个策略组相关联，则可应用这些策略组的全部或一些以确定该用户的访问控制。例如在一个实施例中，如果多个策略组配置有与用户关联的组688，并且配置有与由该用户操作的客户机装置匹配的装置描述文件676，则系统可应用所有这些策略组来确定该用户的访问控制。

[0261] 在一些实施例中，策略组677与至少一个组或组名688相关联。在某些实施例中，如果没有为策略组677定义或配置组688(或组名)，则策略组677可能例如由于没有激活与组相关的策略而无意中允许访问。在这些实施例的一些中，系统可禁用策略组677，或者重新配置策略组677以返回一个空集(例如，而不是做出潜在地无效访问控制决策)。这样可以防止意外的安全漏洞(security breach)。因而，例如，如果为策略组677配置管理组名并且管理员意外地将该管理组名从策略组677移除，则系统可以禁用策略组677从避免使用户自动获得关于这个策略组677的权限。在一些实施例中，如果没有为策略组677配置至少一个组688，可将默认组附属到该策略组677，例如直到为该策略组677配置组688。

[0262] 策略组677可在资源访问配置655中指定一个或多个可应用资源或资源类型。每个资源或资源类型可具有与其相关的多个访问级别或者访问权限。在一些实施例中，系统可支持包括至少“允许”或“拒绝”的访问权限。在其他实施例中，如果访问被允许，则可基于策

略组评估来授予多个访问级别中的一个。系统可审计或记录资源或资源类型的可用性。系统可根据该资源或资源类型的可用性来修改资源访问配置655。可指定关于资源或资源类型的默认或全局访问权限。具有资源访问配置655的策略组677可以忽略该默认或全局访问权限。

[0263] 资源访问配置655可支持类型为“任何”的资源，该“任何”可表示用于任意资源的通配符。例如，在一些实施例中，管理员可使用该资源访问配置655来建立适用于任何资源的基础策略组。在一些实施例中，在策略组677中缺少任一配置的资源访问配置655的情况下，应用于该策略组677的隐式默认或全局性质可以拒绝所有资源请求。这种隐式默认或全局性质可被称作“拒绝所有”性质或策略。在策略组677的评估期间，例如可以相对于定义的的资源访问配置655为“拒绝所有”性质或策略分配较低的优先级。在一些实施例中，如果策略组677未配置任何识别的资源或资源类型，则策略组677隐式地拒绝对所有请求资源或一些请求资源的访问。在其他实施例中，如果策略组677未配置任何识别的资源或资源类型，则策略组677可基于全局、默认或者登录点678级别策略或参数设置而允许对一些资源或资源类型的访问。

[0264] 现参考图6B，描述了策略组677的数据模型的一个实施例。策略组677可包括由网络装置配置和存储的一个或多个数据结构。该一个或多个数据结构可以由管理员和/或由应用动态地进行重新配置。在一些实施例中，其中一个数据结构经由任何类型或形式的存储器或数据库链接和/或指针与一个或多个其他数据结构相关联。例如在一个实施例中，策略组677可具有与资源631、组638、装置描述文件635、登录点633和/或IP地址池640的访问配置数据结构关联的智能组数据结构630。IP地址池可以是任何类型或形式的IP地址的集合，例如分配给用户和/或由用户操作的装置的内联网或虚拟IP地址(IIP)。例如，可在用户会话或访问资源的会话期间将IP地址池中的IP地址分配给用户和/或装置。这些IP地址可以例如在会话终止时重用。

[0265] 在一些实施例中，登录点可与一个或多个装置描述文件676关联。例如，这可以如同在图6B中由登录点678的数据结构633和装置描述文件的数据结构635的关联所描述的那样。在一个实施例中，可基于一种或多种装置类型或装置描述文件676(例如，可见性装置描述文件)使得特定的登录点676(例如web界面)可用。在另一个实施例中，例如，登录点678可以为了使认证和/或授权成功而请求特定的装置类型或装置描述文件676。在又一个实施例中，在认证用户时，如果该用户正在使用具有或满足识别的装置描述文件的装置，则登录点678可以授权给该用户。在某些实施例中，认证时可以根据用户识别一个或多个组。例如，这可以是在图6B中由认证方法的数据结构639和组数据结构638的关联所描述的那样。

[0266] 举例来说，且不以限制为目的，处于客户机装置的用户可能尝试登录到系统400和/或会话以访问资源。用户可经由统一资源定位符(URL)来选择和/或访问登录接口。URL可与登录点相关联。登录点可与一个或多个策略组相关联。一个或多个认证和/或授权方法690可与所选择的登录点相关联或附属于所选择的登录点。可基于所选登录点的一个或多个认证方法699来认证用户。可由所选登录点的一个或多个授权方法690来评估和/或确定用户的授权权利。基于认证和/或授权，用户可被识别为属于一个或多个组或者与一个或多个组相关联。可为每个组分配组名。基于所识别的组、组名、所请求的资源和/或登录点，系统可识别一个或多个策略组用于控制对所请求资源的用户访问。可根据由每个识别的策略

组描述或识别的一个或多个装置描述文件676来评估用户操作的客户机装置。策略组677可基于认证、授权、识别的组、装置描述文件评估和/或所请求的资源授予用户对该资源的访问权限。

[0267] 在一些实施例中，可使用策略组更有效地管理访问控制。与单独策略和/或决策树中的策略节点相比，使用策略组可以更有效地管理访问控制。每个访问配置可包括如上文描述的一个或多个相关的策略和/或访问控制方案的元素。可以模块化构造和管理每个访问配置。每个访问配置可与多个策略组关联或包括在多个策略组中。可使用一个或多个访问配置来组合或配置一个或多个策略组。还可以经由一个或多个共享的访问配置来重新配置或更新多个策略组。

[0268] 在一些实施例中，在认证和/或授权用户时，可为每个用户识别一个或多个可应用的策略组。管理员可为策略组677定义一个或多个性质。这些性质可包括动作(例如，基于策略组677的评估来拒绝、授予完全访问权限，或者授予访问级别)、相对于其他策略组的优先级、对于其中激活策略组677的时间段的识别等。所定义的策略组677的性质可优先于在全局和/或登录点级别所定义的性质。在缺少可应用的或合适的策略组677的情况下，可应用默认全局访问配置、登录点策略或策略组中的一个或多个。此外，可以通过逻辑地组合策略组677中的各种访问配置来应用精细(fine-grained)访问配置。对于每个资源，每个策略组677可以基于访问配置的聚合集合为用户授予多种访问级别中的一种。策略组677的每个访问配置可提供相对于策略组677的其他访问配置的不同访问控制特征和/或补充访问控制特征。例如，在一些实施例中，可在两个或更多访问配置中实现多个认证方法699。

[0269] 此外，一个策略组677可具有比另一策略组677更高的优先权。在这些实施例的一些中，可基于更高的优先权或更高级别的策略组677向与多个策略组关联的用户授予访问权限。因此，在配置、管理和应用策略组的过程中，有各种益处和灵活性。

[0270] 在一些实施例中，为策略组677建立初始配置包括(例如通过管理员经由策略组677接口)向登录点678(例如默认登录点)附加或关联认证方法。管理员可创建新的策略组677(例如，经由策略管理器667的智能组数据机构)。管理员可以向策略组677添加登录点678作为访问配置。在配置资源访问配置655的过程中，管理员可定义类型为“任何”的资源。管理员可为该资源将访问权限设置为“允许”和/或指定对这些资源可用的多个访问级别。管理员可例如经由策略管理器667保存策略组677的这个初始配置。

[0271] 在一些实施例中，并且举例说明，管理员可能想要配置策略组677用于控制对网段(例如，网段10.20.30.0/24)的访问。管理员可要求认证对该网段的访问。管理员可向默认登录点添加或关联一个或多个认证方法。管理员可基于例如OS类型、浏览器类型等来创建或配置新的装置描述文件676。管理员可为指向网段10.20.30.0/24的网段资源创建或配置访问配置。管理员可创建新的策略组677(例如，经由策略管理器667的智能组数据结构)。管理员可向策略组677添加登录点678作为另一访问配置。管理员可向策略组677添加装置描述文件676作为又一访问配置。管理员可向策略组677添加网段资源的访问配置。管理员可将这些配置保存在新的策略组677的数据结构中。

[0272] 如上文所述，系统可支持一个或多个全局配置。每个全局配置可与提供或管理对网络资源的访问的网络装置群关联。在一些实施例中，每个全局配置可与网关、设备或者经由一个或多个策略组677管理对资源的访问的任何其他网络节点的群关联。每个全局配置

可包括一个或多个与访问相关的性质、参数或属性(后文中总的称作“参数”)。这些参数或属性可当做例如在缺少由策略组677和/或登录点678提供的访问配置的情况下的默认配置。表F2示出了在全局、策略组677和/或登录点级别可用的参数的一个实施例。在一些实施例中,如果策略组级别的参数可用或者被支持,则该参数优先于在全局和/或登录点级别的相应的参数。如果在登录点级别的参数可用或被支持,则该参数可优先于在全局级别的相应的参数。表F3示出了在全局和策略组级别可用的参数的另一个实施例。系统可预先确定在多个可用策略组和全局参数之间的优先级。在一些实施例中(其中可应用多于一个策略组),最高优先级的策略组677可优先于其他策略组677的相应的参数值。在某些实施例中,系统可预先确定与策略组关联的多个(用户)组之间的优先级。当可以应用多于一个策略组时,具有最高优先级组的策略组677可优先于其他策略组的相应的参数值。

[0273] 表F2:支持的参数(与访问相关)的一个实施例

[0274]

属性/参数	全局	策略组	登录点	注释
分离隧道	X	X		
允许早期的访问网关插件	X			
关闭连接	X	X		
要求安全客户机证书	X			
验证内部安全证书	X			例如，从访问网关接入内部网。
客户机连接加密	X			
启用内部故障恢复	X			
禁用登录页面认证			X	例如，用于策略组模式
在网络中断后认证	X	X		
在系统恢复时认证	X	X		
用窗口启用单点登录（SSO）	X	X		
用户会话超时	X	X	X	指示用户可被连接到安全网络的时间（例如，数分钟内）。
网络闲置超时	X	X	X	如果在指定时间内（例如，数分钟内）没有来自客户机的分组，则访问网关可断开连接。
空闲会话超时	X	X	X	例如，如果没有鼠标、键盘和/或其他活动，则用户会话可能超时。
分离域名服务（DNS）	X	X		
登陆页面		X	X	

[0275] 表F3:考虑策略组参数的全局参数的实施例

[0276]

特征/参数名称	全局	策略组优先	注释

[0277]

启用分离隧道	X	X	在值冲突的情况下，可禁用分离隧道，除非另有组优先级提供。访问控制列表可从该项移除。
允许早期的访问网关插件	X		
web 会话超时	X	X	可选择两个超时值之间较小的，除非另有组优先级提供。可请求来自组优先级和/或默认值的支持。
启用不正确的密码缓存	X		管理员可能不可配置。
没有访问控制列表拒绝访问			可硬编码为 TRUE。管理员可能不可配置。
关闭连接	X	X	可链接到分离隧道。该特征与从访问网关接入内部网相关联。
要求安全客户机证书	X		
验证内部安全证书	X		可在逐个资源的基础上应用该设置。
客户机连接加密类型(RC4|AES|3DES)	X		默认可设置为 RC4。
启用内部故障恢复	X		
启用应用加速	X		可设置为 true。管理员可能不可配置。
启用登录页面认证	X		可为每个登录点配置该设置
网络中断后认证	X	X	在组级别可能是有利的
在系统恢复（休眠）时认证	X	X	
用窗口启用单点登	X	X	可添加至管理接口

[0278]

录			
运行登录脚本	X	X	
用户会话超时	X	X	
网络闲置超时	X	X	
空闲会话超时	X	X	
没有策略拒绝应用	X	X	默认设置可以是“禁用”。
启用分离 DNS	X	X	
启用 IP 池	X	X	可请求来自组优先级和/或默认值的支持。
终止连接	X	X	该特征可与“关闭连接”相同或类似。管理员可能不可配置。
使用定制门户页面	X	X	如果在组级别实现，该特征可请求指定优先级。管理员可能不可配置。
重定向到 web 接口	X	X	如果在组级别实现，该特征可请求指定优先级。可请求来自组优先级和/或默认值的支持。
使用多登录选择页面	X	X	

[0279] 现参考图6C，该流程图描述了用于建立和/或提供策略组677以控制用户对资源的访问的方法650中所采取步骤的实施例。该方法包括经由在多个客户机和一个或多个服务器中间的装置上执行的策略管理器667，建立策略组677，该策略组677表示用于用户经由该装置访问一个或多个服务器的一个或多个识别的资源的一个或多个访问配置的集合(601)。策略组677包括登录点组件，其表示访问该一个或多个识别的资源的入口点。该方法包括，经由策略管理器667配置登录点组件从而为入口点指定统一资源定位符(603)。该方法包括，经由策略管理器667选择登录点组件的一个或多个认证方法699(605)。该方法包括，经由策略管理器667基于一个或多个认证方法699识别登录点组件的一个或多个授权方法690(607)。该方法包括，经由策略管理器667为策略组677指定一个或多个装置描述文件676(609)。该一个或多个装置描述文件676中的每一个可识别一个或多个类型的端点分析以在用户装置上执行。该方法包括，经由策略管理器667为策略组677指定一个或多个识别的资源中的允许或拒绝访问的一种资源(611)。该装置接收来自用户的、访问与由登录点组件指定的入口点对应的统一资源定位符的请求(613)。该装置为用户发起由登录点组件指定的一个或多个认证方法699(615)。该装置基于发起的一个或多个认证方法699，应用由登

录点组件指定的一个或多个授权方法690来访问一个或多个识别的资源(617)。

[0280] 在(601)的进一步的细节中,用户或应用(后文为了说明目的有时总称为“用户”)可建立策略组677,该策略组677表示用于用户经由装置访问(例如一个或多个服务器的)一个或多个识别的资源的一个或多个访问配置的集合。用户可经由在多个客户机和一个或多个服务器中间的装置上执行的策略管理器667来建立该策略组677。用户可经由策略管理器667的接口来建立该策略组677。策略组677可包括表示访问一个或多个识别的资源的入口点的登录点组件。在一些实施例中,用户根据另一预先配置的策略组677来建立策略组677。用户可根据策略组677模板、一个或多个访问配置,和/或根据策略组677的初始配置来建立策略组677。

[0281] 在一些实施例中,用户通过建立一个或多个访问配置(例如类型资源、装置描述文件、组、登录点等)来建立策略组677。用户可通过向策略组677中合并、汇集或添加一个或多个访问配置来建立策略组677。在一些实施例中,可独立于任何策略组创建或配置访问配置(例如,即使该访问配置之后被添加到策略组677)。用户可在将策略组677建立为包含一个或多个访问配置之前先配置该一个或多个访问配置。用户可通过使用一个或多个全局参数和/或策略来建立策略组677。用户可通过使用一个或多个默认性质、参数和/或策略来建立策略组677。用户可响应于资源或资源类型的创建、定义或可用性来建立策略组677。系统可响应于对资源或资源类型的一个或多个访问请求来建立关于该资源或资源类型的策略组677。用户可响应于创建新的组或用户组来建立策略组677。用户可建立一个或多个策略组以启用该装置处理或者做出关于资源的访问控制决策。

[0282] 在(603)的进一步细节中,用户可经由策略管理器667配置登录点组件从而为入口点指定统一资源定位符(URL)。在一些实施例中,在建立策略组677之前(例如独立于任何识别的策略组)配置登录点。用户可指定或选择URL以表示、识别和/或访问该登录点。用户可指定或选择web链接、图标或应用小程序来表示、识别和/或访问该登录点。用户可以为策略组677选择或改写一个或多个预先配置的登录点678。用户可为策略组677关联或配置一个或多个登录点678。用户可经由策略管理器667的接口来选择、创建和/或配置登录点678。用户可为策略组677建立第二登录点组件。用户可将第二统一资源定位符配置为第二登录点的入口点。

[0283] 在一些实施例中,用户为登录点组件关联或配置装置描述文件组件676。用户可将策略组677建立为具有与登录点组件相关的装置描述文件组件676。装置描述文件组件676可识别在客户机装置上执行的端点分析以确定(例如经由登录点组件的入口点)访问。例如在一个实施例中,可将装置描述文件676配置为要求某些信息从请求访问资源的客户机节点收集,例如客户机节点的计算环境特征。在一些实施例中,用户基于为登录点关联或配置的装置描述文件676来为登录点选择一个或多个认证和/或授权方法690。

[0284] 在一些实施例中,用户可以为登录点指定一个或多个参数,该参数优先于装置或策略组677的一个或多个对应的性质(例如,设置、参数、规则和/或策略)。例如在一些实施例中,用户可为登录点指定一个或多个性质,该性质优先于装置的默认或全局性质。在某些实施例中,用户可以禁用登录点。在这些实施例的一些中,例如当策略组677中没有其他启用的登录点678时,策略组677可响应于禁用登录点而变为不可用。在一些实施例中,策略组677可以在禁用策略组677的登录点组件后保持启用。例如在一个实施例中,可响应于禁用

策略组677的登录点为策略组677分配默认或全局登录点678。

[0285] 参考(605),用户可经由策略管理器667为登录点组件选择一个或多个认证方法699。用户可选择认证方法用于控制对资源的访问。举例说明,并且在一个实施例中,用户可识别认证方法以控制对资源的用户访问。用户可选择认证方法以建立请求访问资源的用户的身份。用户可例如经由策略管理器667的接口来选择、创建、改写和/或配置登录点的一个或多个认证方法699。

[0286] 在一些实施例中,用户可基于与登录点关联的装置描述文件676来选择认证方法。用户可基于登录点或策略组677要求的安全等级或其他要求选择认证方法。用户可基于与配置的登录点或建立的策略组677关联的一个或多个授权方法690来选择认证方法。在一些实施例中,用户可以为登录点组件指定两种认证方法699,如双重认证。

[0287] 在(607)进一步的细节中,用户可经由策略管理器667、基于一个或多个认证方法699为登录点组件识别一个或多个授权方法690。用户可识别授权方法以提供对于资源请求的基于策略的评估。在一些实施例中,用户可识别授权方法以确定对资源的访问条件或要求。用户可以例如经由策略管理器667的接口来为登录点选择、识别、创建、改写和/或配置一个或多个授权方法690。用户可基于与登录点关联的装置描述文件676选择授权方法。用户可基于登录点或策略组677要求的安全等级或其他要求来选择授权方法。

[0288] 用户可基于与配置的登录点或建立的策略组677关联的一个或多个认证方法699来选择授权方法。在一些实施例中,用户可根据在上文中讨论的表F1来指定一个或多个授权方法690。策略管理器667可基于对一个或多个认证方法699的选择来限制授权方法690的选择。策略管理器667可基于所支持的或所选择的端点分析的类型来限制授权方法690的选择。策略管理器667可基于根据用户识别的一个或多个组来限制授权方法690的选择。

[0289] 在(609)进一步的细节中,用户可经由策略管理器667为策略组677指定一个或多个装置描述文件676。用户可经由策略管理器667的接口指定、选择和/或配置装置描述文件676。用户可基于配置的登录点来指定装置描述文件676。在一些实施例中,用户可从多个可用的装置描述文件676中选择一个或多个装置描述文件676。用户可从装置描述文件676的默认或基础集合中配置一个或多个装置描述文件676。用户可基于策略组677的一个或多个访问配置来指定装置描述文件676。例如在一个实施例中,用户可基于为策略组677配置的登录点678来指定装置描述文件676。

[0290] 一个或多个装置描述文件676中的每一个可识别在用户的装置上执行的一种或多种类型的端点分析或扫描。一个或多个装置描述文件676中的每一个可识别要从请求访问资源的用户的客户机装置收集的信息。装置描述文件676可识别要与客户机装置和/或该客户机装置的计算环境进行比较的信息。用户可基于支持的或选择的端点分析或扫描的类型来指定装置描述文件676。在一些实施例中,用户可基于根据用户识别的一个或多个组来指定装置描述文件676。用户可基于与配置的登录点或建立的策略组677关联的一个或多个认证和/或授权方法690来指定装置描述文件676。

[0291] 在一些实施例中,用户可指定可见性装置描述文件676来确定是否启用登录点。用户可指定装置描述文件676来确定请求的客户机节点的安全特征和/或其他功能。用户可指定装置描述文件676来提供对于访问资源的请求的基于策略的评估。用户可识别装置描述文件676以确定资源的访问条件或要求。在某些实施例中,用户可指定装置描述文件676来

确定或识别请求客户机的匹配装置类型。

[0292] 参考(611),用户可经由策略管理器667为策略组677指定一个或多个识别的资源中的允许或拒绝访问的一种资源。用户可指定和/或配置资源访问配置655用于一个或多个策略组中。用户可识别资源和/或资源类型用于访问控制。用户可经由策略管理器667的接口识别资源和/或资源类型。在一些实施例中,用户可基于一个或多个资源的功能、特征和/或特性来识别资源类型或类别。用户可识别全局资源类型或类别,例如"任何"(Any)表示任何资源或者资源类型。在某些实施例中,用户可指定或配置对资源和/或资源类型可用或可分配的访问权限(例如,允许、拒绝、访问级别)。例如在一个实施例中,用户可基于为登录点678和/或策略组677配置的一个或多个装置描述文件676来指定或配置访问权限。

[0293] 用户可经由策略管理器667的接口来指定、选择和/或配置资源访问配置655。用户可基于配置的登录点来指定资源访问配置655。用户可以从多个资源访问配置中选择一个或多个资源访问配置655。在一些实施例中,用户可从资源访问配置的默认或基础集合中配置一个或多个资源访问配置655。用户可基于策略组677的另一访问配置来指定资源访问配置655。例如,且在一个实施例中,用户可基于为策略组677配置的装置描述文件676来指定资源访问配置655。

[0294] 在(613)进一步的细节中,装置可接收来自用户的、访问统一资源定位符的请求,该统一资源定位符对应于由登录点组件指定的入口点。装置可接收或拦截来自该装置的网络的分组或消息。装置可接收或拦截来自连接到该装置的网络节点的分组或消息,该网络结点诸如是访问服务器或防火墙。装置可接收或拦截来自用户的客户机装置的请求。装置可经由策略管理器667的接口接收来自用户或应用的请求。装置(例如,经由策略管理器667)可识别策略组677,该策略组677包括登录点组件,该登录点组件表示访问一个或多个识别的资源的入口点。装置可以(例如响应于请求)为用户提供一个或多个可选择的URL、web链接和/或桌面小程序来选择登录点。用户可基于该一个或多个URL、web链接和/或桌面小程序来选择登录点678。

[0295] 在一些实施例中,可以例如响应于接收请求在用户的客户机装置上发起端点分析。可根据一个或多个可见性装置描述文件来评估从端点分析收集的信息。可以评估从端点分析收集的信息以识别为用户启用的一个或多个登录点678。可以缓存或存储从端点分析收集的信息用于根据一个或多个装置描述文件676进行评估,该一个或多个装置描述文件676例如结合一个或多个可应用的策略组被识别。可由为用户选择的一个或多个认证和/或授权方法690使用该从端点分析收集的信息。

[0296] 在一些实施例中,装置可基于请求识别一个或多个策略组。例如在一个实施例中,装置可选择在请求中识别的策略组677。该装置可基于在请求上应用策略来识别策略组677。在一些实施例中,装置可基于所请求的资源来识别策略组677。装置可接收或提取URL,该URL被识别为策略组677的登录组件的入口点。装置可基于在请求中接收的URL来识别策略组677和/或登录点。在某些实施例中,装置可接收或提取URL,该URL被识别为策略组677的第二或随后的登录组件的入口点。

[0297] 装置可基于在请求中识别的入口点和/或登录点678来识别策略组677。装置可基于默认(或全局)策略和/或设置来识别策略组677。在一些实施例中,该装置可将请求指向多个策略管理器中的一个,例如,每个可在上文中结合图5A-5C讨论的那些多核系统的处理

器上执行。装置可经由该装置的流分布器、分组引擎和/或负载平衡模块将请求指向一个或多个策略管理器。

[0298] 在一些实施例中，装备可推迟识别策略组677，直到已经应用或评估一个或多个访问配置。例如在一些实施例中，可进行认证和/或授权从而为用户识别组。可至少部分基于该用户的识别的组来确定策略组677。在一些实施例中，可基于所选择的登录点来评估装置描述文件676。可至少部分基于为请求所选择、评估和/或识别的一个或多个访问配置来识别策略组677。可响应于请求来初始识别多个策略组，但是可至少部分基于根据该请求所选择、评估和/或标识的一个或多个访问配置从评估中排除该多个策略组中的一些。在某些实施例中，如果没有识别可应用的预先确定策略组，则可以识别默认策略组677以处理访问请求。

[0299] 在(615)进一步的细节中，装置可以为用户发起由登录点组件指定的一个或多个认证方法699。装置可基于策略的应用(例如使用策略管理器667或策略引擎)来发起一个或多个认证方法699。装置可基于所选择的或提供的登录点678来为用户发起一个或多个认证方法699。在一些实施例中，装置可发起由登录点组件指定的两种认证方法699用于双重认证。装置可基于第一认证方法的评估来发起一个或多个认证方法699，例如用于额外的安全性。一个或多个认证方法699可能包含用户ID、密码、RSA securID、证书、其他用户信息和/或生物数据的某种组合。在应用一个或多个认证方法699的过程中，策略管理器667可与访问服务器或AAA服务器通信和/或互操作。

[0300] 参考(617)，装置可基于发起的一个或多个认证方法699来应用由登录点组件指定的一个或多个授权方法690从而访问一个或多个识别的资源。装置可基于策略的应用(例如使用策略管理器667或策略引擎)选择和/或发起一个或多个授权方法690。在一些实施例中，装置可基于所选择的或提供的登录点678来为用户发起一个或多个授权方法690。如上文中结合表F1所讨论的，装置可基于所选的一个或多个认证方法699发起一个或多个授权方法690。装置可以为用户发起双重认证。一个或多个授权方法690可评估端点分析期间收集的信息。可将该一个或多个授权方法690应用在访问请求中包含的信息上。在应用一个或多个授权方法690的过程中，策略管理器667可与访问服务器或AAA服务器通信和/或互操作。

[0301] 在一些实施例中，一个或多个授权方法690的选择受限于一个或多个认证方法699的指定。一个或多个认证方法699的选择可受限于一个或多个授权方法690的指定。选择一个或多个授权方法690可与所选择的一个或多个认证方法699协同作用或者适合于所选择的一个或多个认证方法699。在一些另外的实施例中，选择一个或多个授权方法690不限于一个或多个认证方法699的指定。在一些实施例中，选择一个或多个认证方法699可以不限于一个或多个授权方法690的选择。

[0302] 在一些实施例中，可以基于所选择的一个或多个认证和/或授权方法690来识别一个或多个装置描述文件676。策略管理器667可识别策略组677的装置描述文件组件。该装置描述文件组件676可包括或指定一个或多个装置描述文件676用于经由登录点组件的入口点进行访问。可由该一个或多个装置描述文件676识别或指定一种或多种类型的端点分析或扫描。可由该一个或多个装置描述文件676发起一种或多种类型的端点分析或扫描。在用户的客户机或第二装置上，该装置可执行由装置描述文件组件的一个或多个装置描述文件

676指定的一种或多种类型的端点分析或扫描。在某些实施例中，可基于所应用的一个或多个认证和/或授权方法690来为用户进一步识别一个或多个组。可以例如基于登录点678、装置描述文件676和所识别的组中的任何一个或多个来为用户识别一个或多个策略组。

[0303] 在一些实施例中，如由策略组677所指定的，装置忽略该装置的一个或多个参数。例如在一个实施例中，策略组677可忽略分配给装置或装置的群的一个或多个全局或默认性质、参数、策略、设置和/或特征。例如，如果没有被任何可应用的策略组677指定或覆盖，装置和/或策略管理器667可基于该全局或默认设置来识别和评估一个或多个策略。装置和/或策略管理器667可评估一个或多个策略组和/或全局或默认设置来确定是否可授予一些访问权限。

[0304] 装置和/或策略管理器667可授予对在请求中识别的一个或多个资源的访问权限，例如基于一个或多个策略组的评估。装置和/或策略管理器667可授予对一个或多个识别的资源的一种资源的访问权限。装置和/或策略管理器667可授予对所识别的资源或一种资源的多种访问级别中的一种。在一些实施例中，装置和/或策略管理器667可授予对所识别的资源的多种访问级别中的一种并且授予对另一所识别的资源的多种访问的另一种。在某些实施例或情况中，装置和/或策略管理器667可拒绝对所识别的资源的访问。该装置和/或策略管理器667可拒绝对一个或多个所识别的资源的一种资源的访问。

[0305] 在一些实施例中，策略组677可授予对所请求的资源的访问权限而另一策略组677拒绝对该资源的访问或授予对该资源的不同访问权限。装置可基于由较高优先级的策略组677授予的访问权限来提供对资源的访问。在一些实施例中，如果由不同的策略组授予的访问权限互相之间不一致，策略管理器667可提供对该资源的访问权限。如果策略组中的任一拒绝对该资源的访问，则策略管理器667可决定拒绝对该资源的访问。

[0306] 举例说明，策略组677可要求当客户机装置的应用软件匹配装置描述文件的一些或全部属性时，客户机节点才可接收所请求文件的内容的转换版本。客户机节点可接收启用到转换服务器的连接的可执行文件，该可执行文件可以采用对于客户机装置类型可访问的格式来表示文件的内容。在一些实施例中，例如，如果客户机装置不是可信装置、不包含合适的应用软件，和/或来自诸如互联网亭(kiosk)的不安全网络，则策略组677可以禁止向该客户机节点下载所请求的文件。在该实施例中，策略组677可要求装置向客户机节点传送可执行文件，用以启用到应用服务器的连接以呈现文件内容。指定的访问权限可以使客户机节点能够查看文件的内容，而不会由于不合适的散播而危及该文件的专有内容。在另一个实施例中，策略组677可要求客户机装置建立安全连接以访问所请求的资源。在一些实施例中，策略组677可要求用户的客户机装置重用或者访问现有的或之前分配的会话来访问资源。

[0307] 应该理解，此处描述的系统可提供多个组件或每个组件并且这些组件可以在单独机器上提供，或者在一些实施例中，可在分布式系统的多个机器上提供。此外，上述系统和方法可作为一件或多件产品上所体现的或在其中的一个或多个计算机可读程序而被提供。所述产品可以是软盘、硬盘、CD-ROM，闪存卡、PROM、RAM、ROM或磁带。通常，计算机可读程序可以任何编程语言来实现，如LISP、PERL、C、C++、C#、PROLOG，或者诸如JAVA的任何字节码语言。软件程序可以作为目标代码被存储在一件或多件产品上或其中。

[0308] 尽管已经参考具体实施例对本发明进行了详细的显示和描述，但对本领域技术人

员应该理解可以在其中进行形式和细节上的各种变化而不脱离由下列权利要求定义的精神和范围。

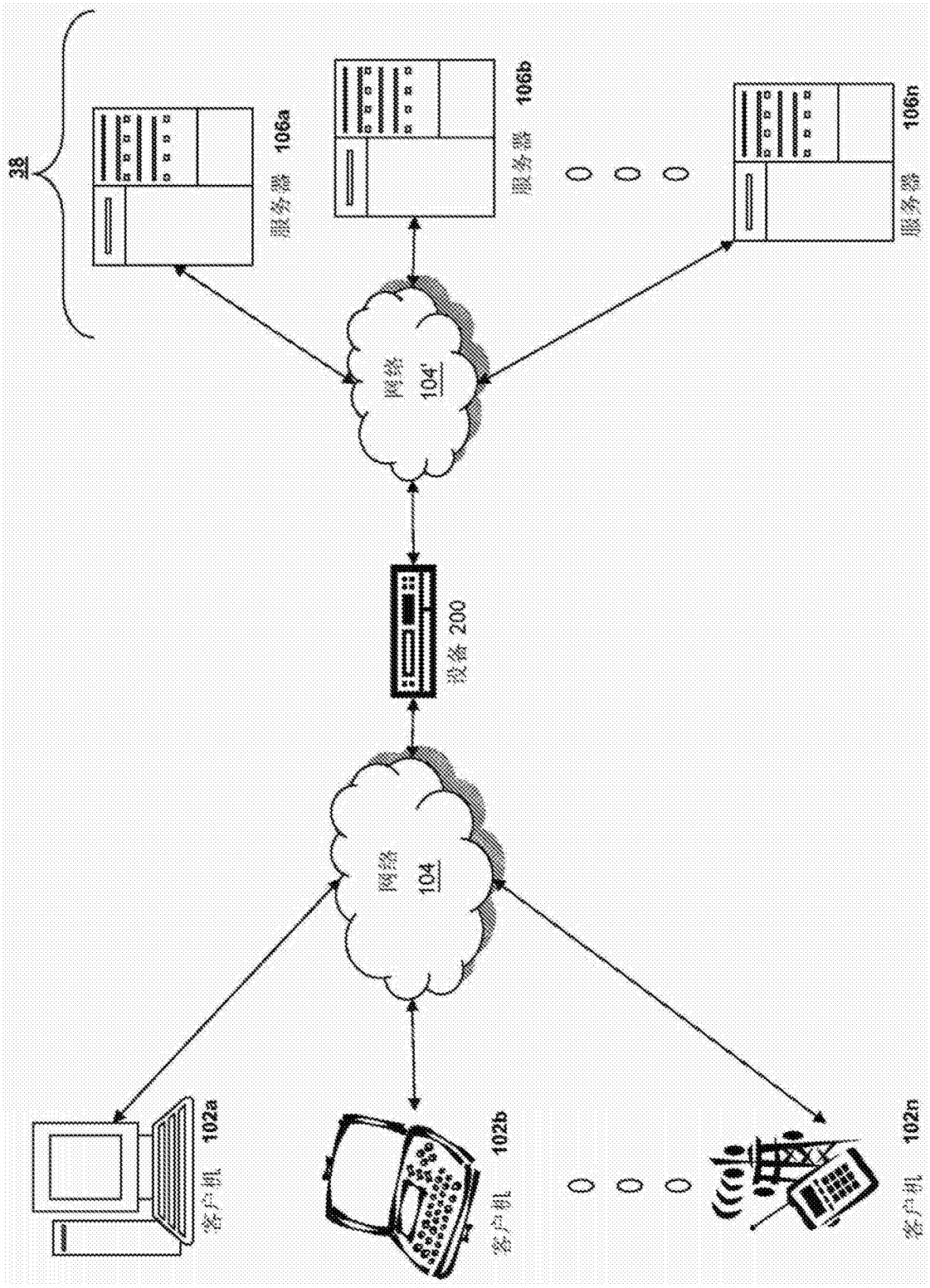

38
服务器 106a
服务器 106b
服务器 106n
网络 104'
设备 200
网络 104
客户机 102a
客户机 102b
客户机 102n

图1A

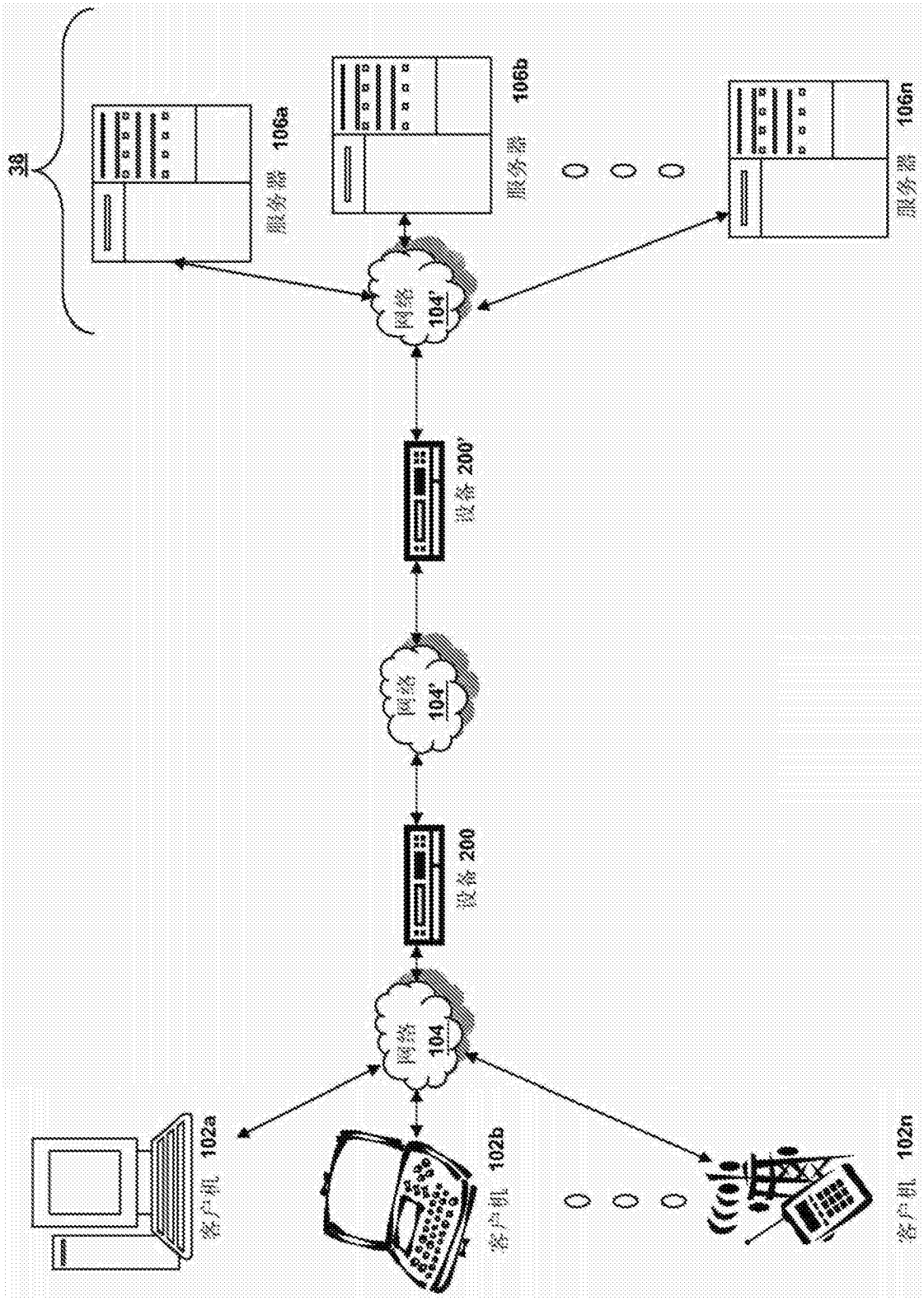

38
服务器 106a
服务器 106b
服务器 106n
网络 104'
设备 200'
网络 104'
设备 200
网络 104
客户机 102a
客户机 102b
客户机 102n

图1B

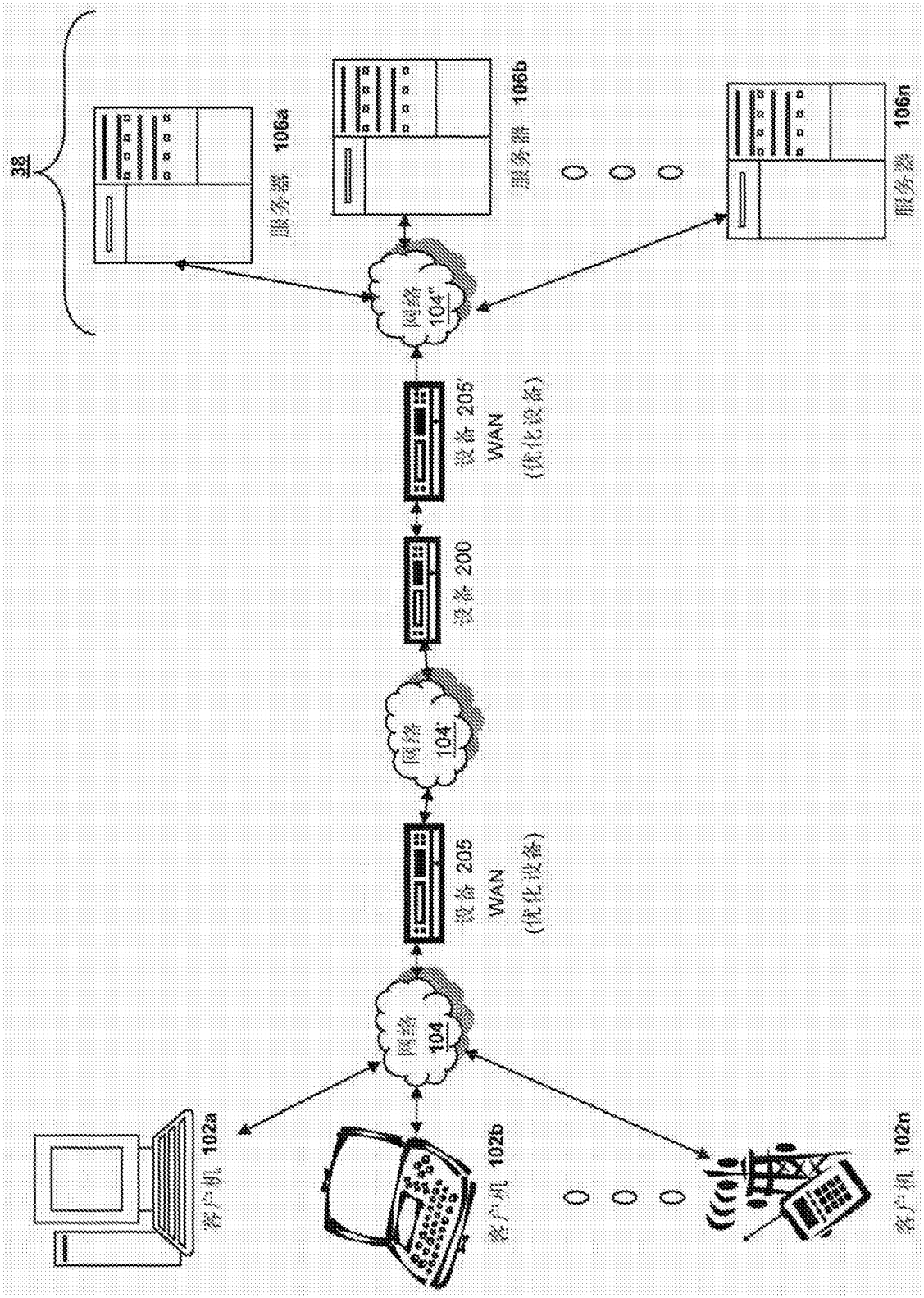

38
服务器 106a
服务器 106b
服务器 106n
网络 104"
设备 205' WAN (优化设备)
设备 200
网络 104'
设备 205 WAN (优化设备)
网络 104
客户机 102a
客户机 102b
客户机 102n

图1C

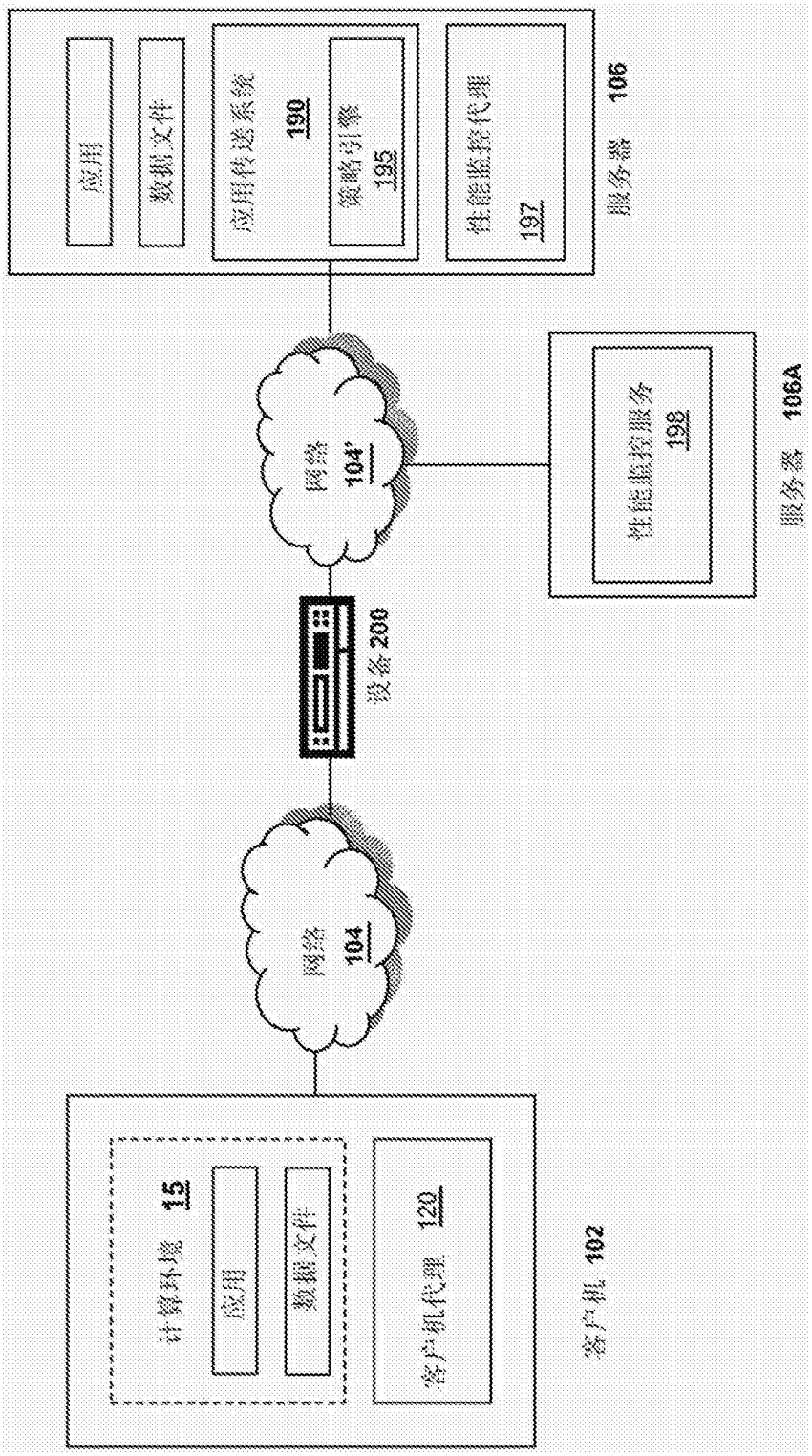

应用
数据文件
应用传送系统 190
策略引擎 195
性能监控代理 197
服务器 106
网络 104'
性能监控服务 198
服务器 106A
设备 200
网络 104
计算环境 15
应用
数据文件
客户机代理 120
客户机 102

图1D

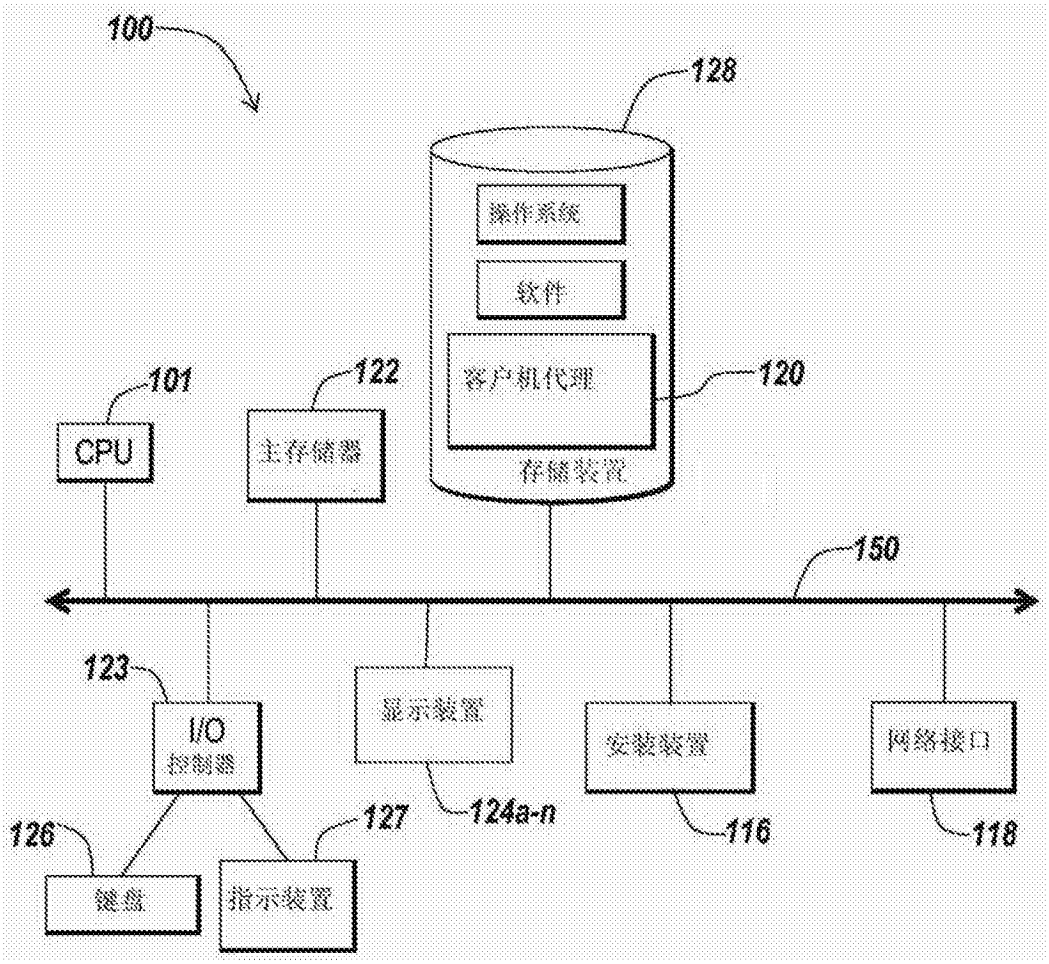

100
128
操作系统
软件
客户机代理
120
存储装置
101
CPU
122
主存储器
150
123
I/O
控制器
显示装置
124a-n
安装装置
116
网络接口
118
126
键盘
127
指示装置

图1E

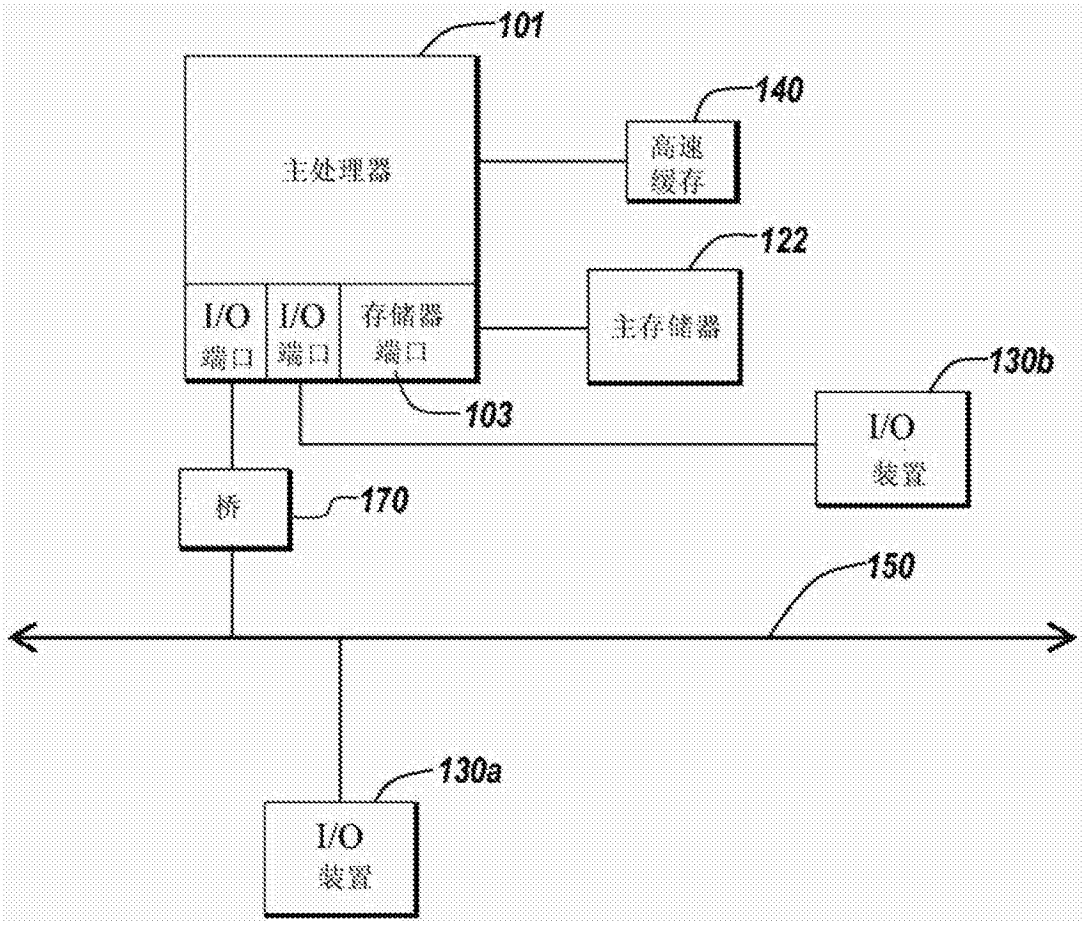

101
主处理器
140
高速缓存
122
I/O 端口
I/O 端口
存储器端口
主存储器
130b
103
I/O 装置
桥
170
150
130a
I/O 装置

图1F

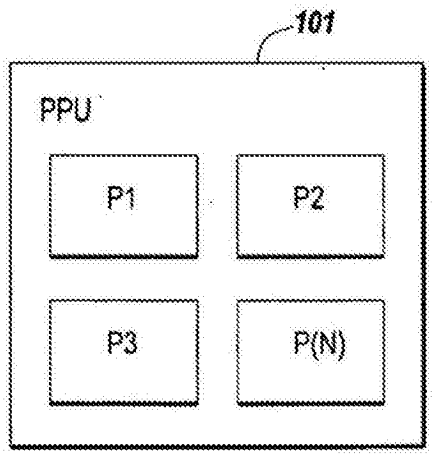

101
PPU
P1
P2
P3
P(N)

图1G

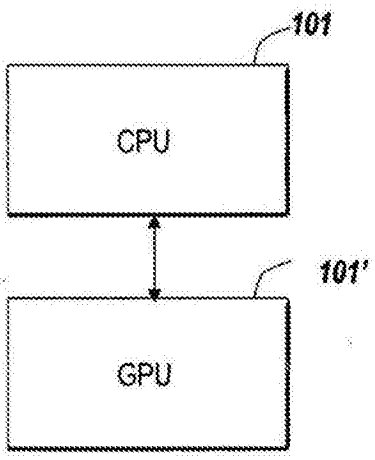

101
CPU
101'
GPU

图1H

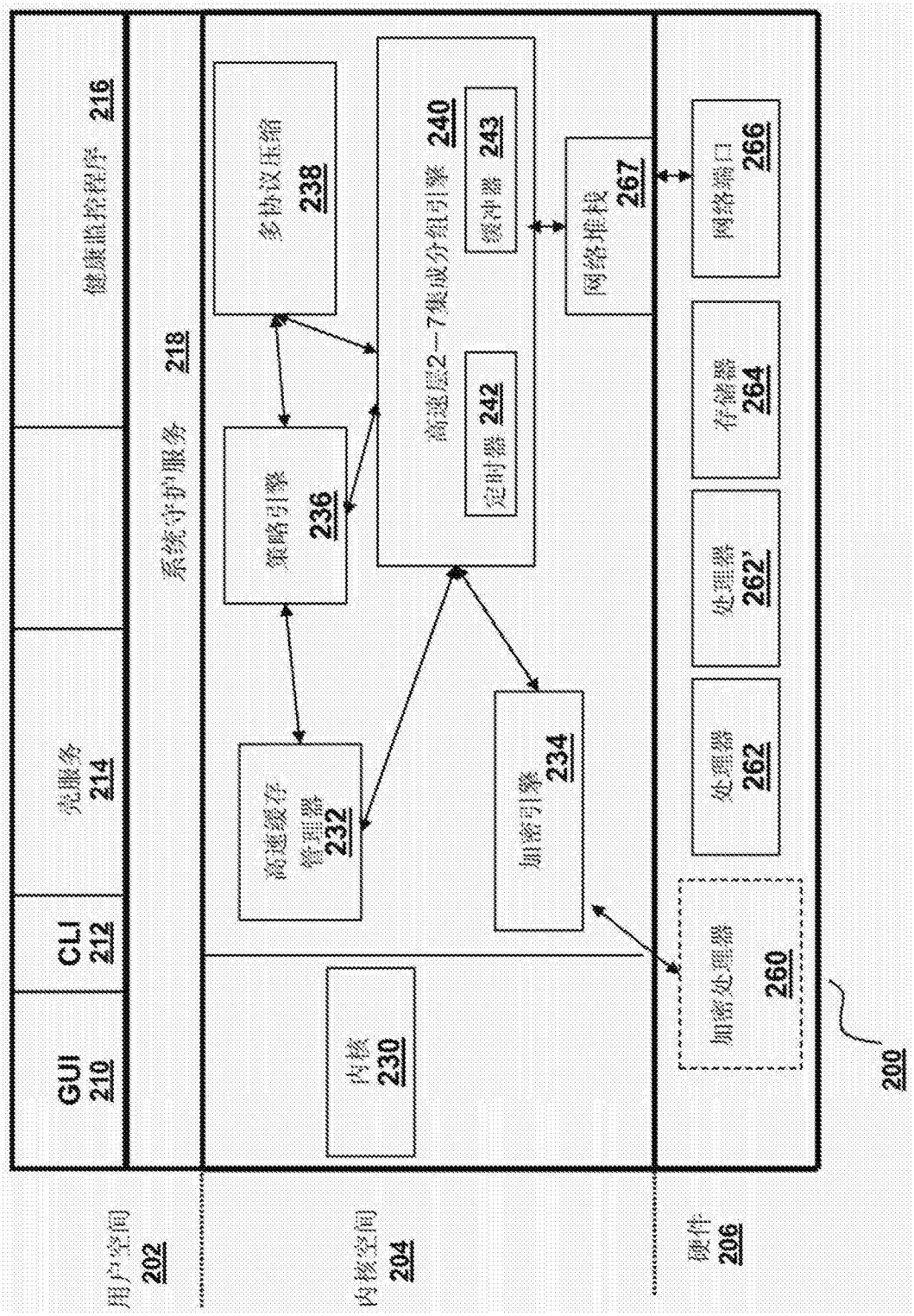

健康监控程序 216
壳服务 214
CLI 212
GUI 210
系统守护服务 218
多协议压缩 238
策略引擎 236
高速缓存管理器 232
内核 230
高速层2—7集成分组引擎 240
缓冲器 243
定时器 242
加密引擎 234
网络堆栈 267
网络端口 266
存储器 264
处理器 262'
处理器 262
加密处理器 260
200
用户空间 202
内核空间 204
硬件 206

图2A

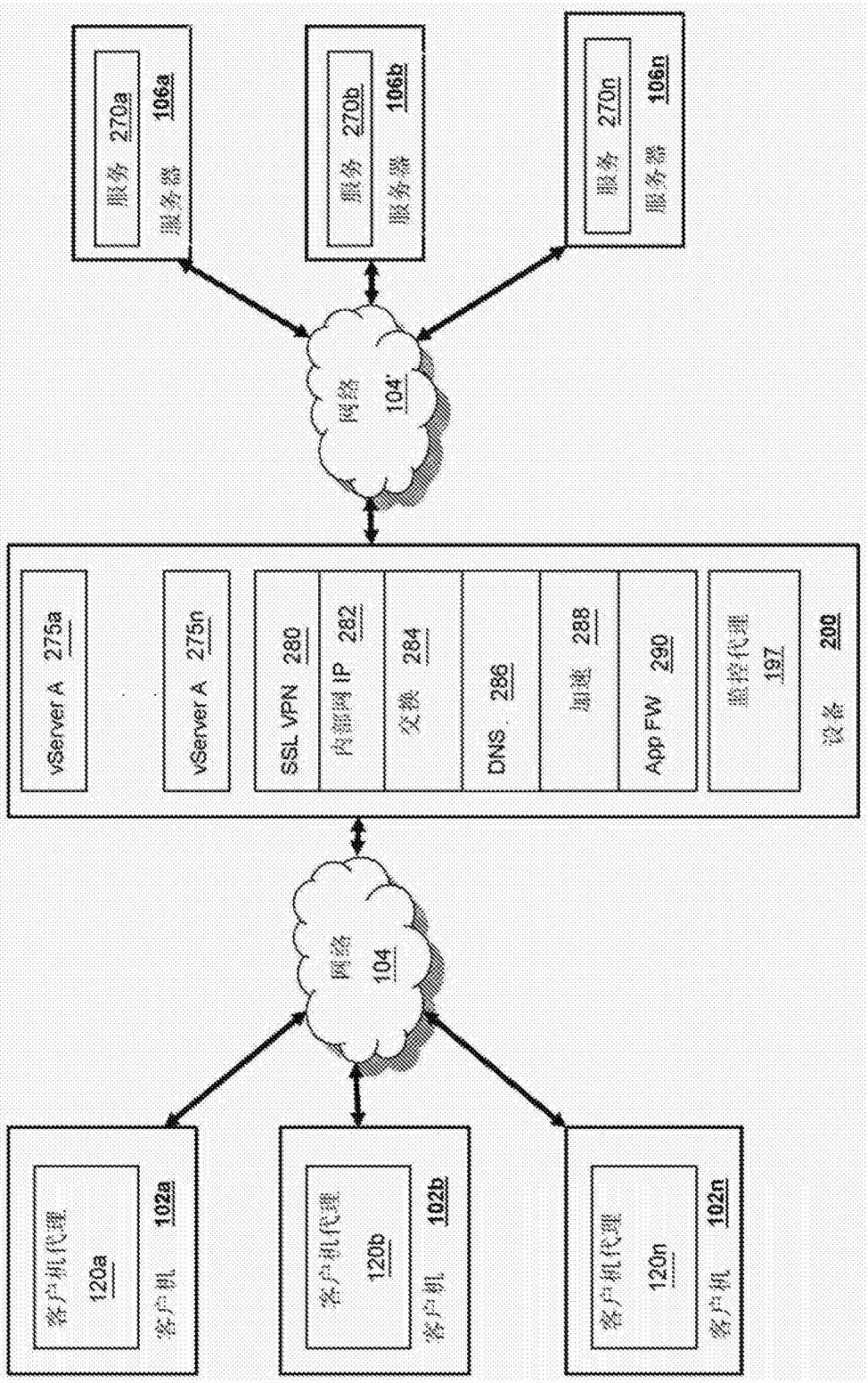

服务 270a
服务器 106a
服务 270b
服务器 106b
服务 270n
服务器 106n
网络 104'
vServer A 275a
vServer A 275n
SSL VPN 280
内部网 IP 282
交换 284
DNS 286
加速 288
App FW 290
监控代理 197
设备 200
网络 104
客户机代理 120a
客户机 102a
客户机代理 120b
客户机 102b
客户机代理 120n
客户机 102n

图2B

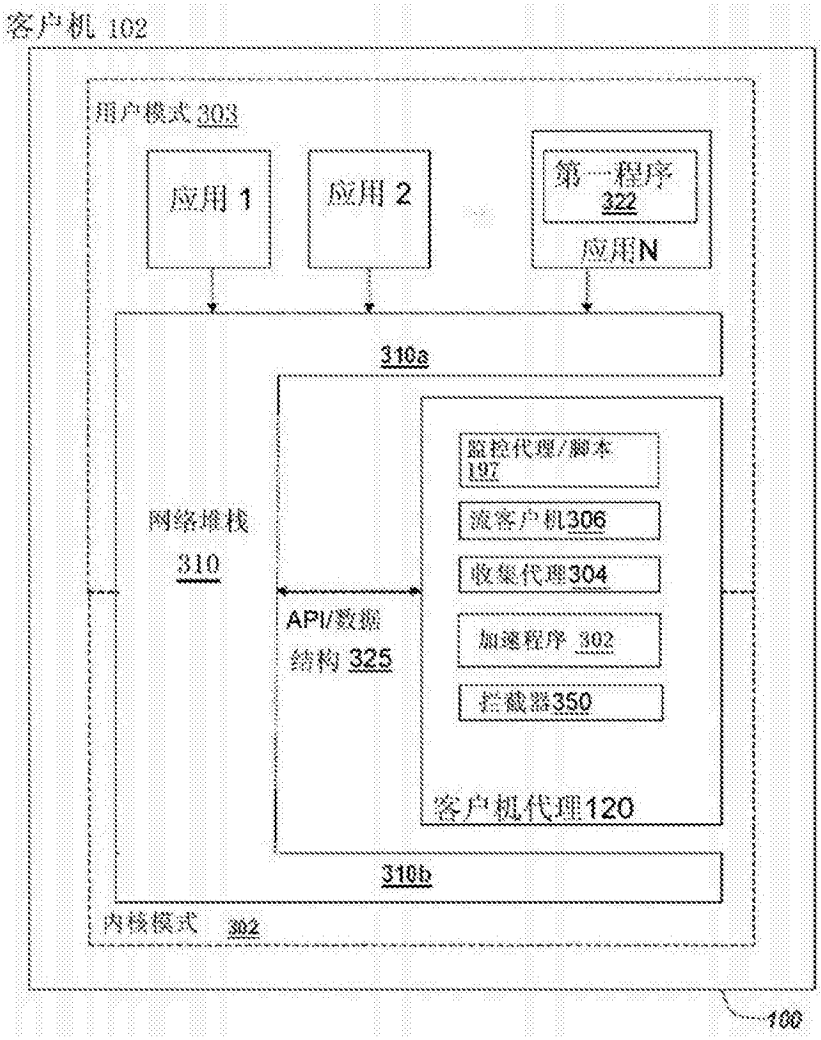

客户机 102
用户模式 303
应用 1
应用 2
第一程序 322
应用N
310a
监控代理/脚本 197
流客户机306
收集代理304
加速程序 302
拦截器350
网络堆栈 310
API/数据结构 325
客户机代理120
310b
内核模式 302
100

图3

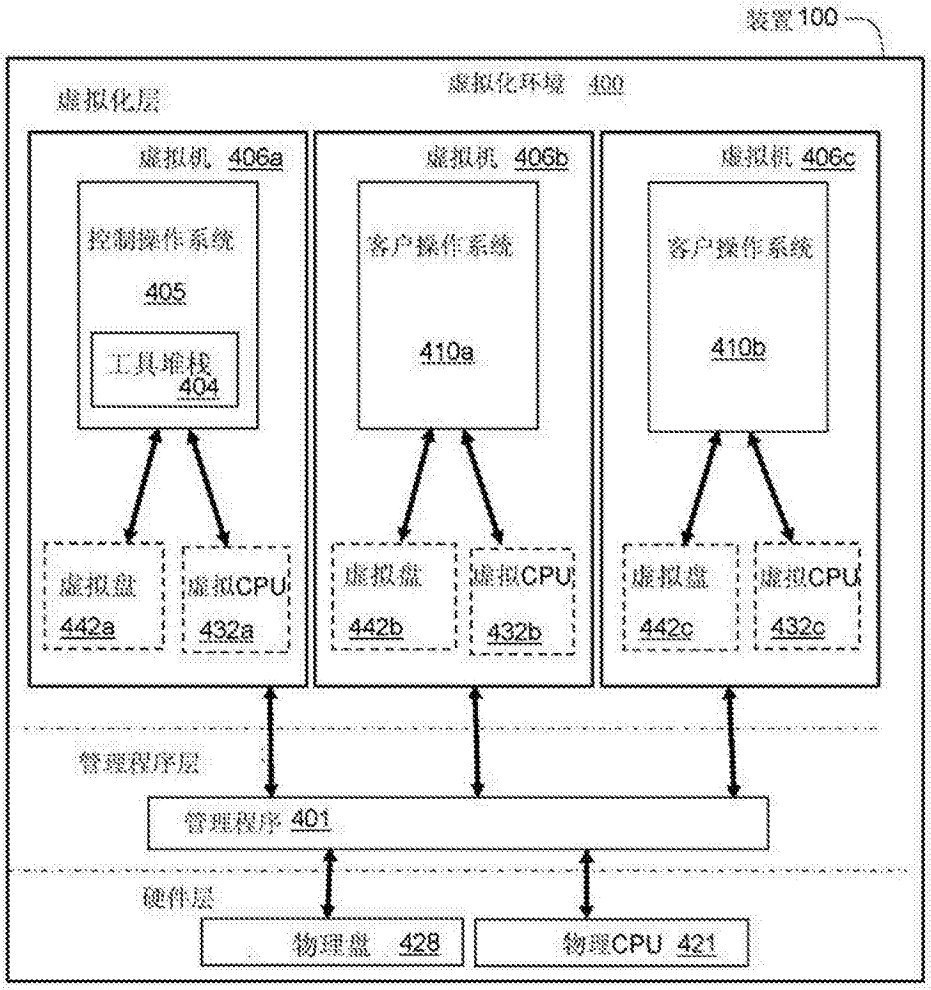

装置 100
虚拟化环境 400
虚拟化层
虚拟机 406a
虚拟机 406b
虚拟机 406c
控制操作系统
405
工具堆栈
404
客户操作系统
410a
客户操作系统
410b
虚拟盘
442a
虚拟CPU
432a
虚拟盘
442b
虚拟CPU
432b
虚拟盘
442c
虚拟CPU
432c
管理程序层
管理程序 401
硬件层
物理盘 428
物理CPU 421

图4A

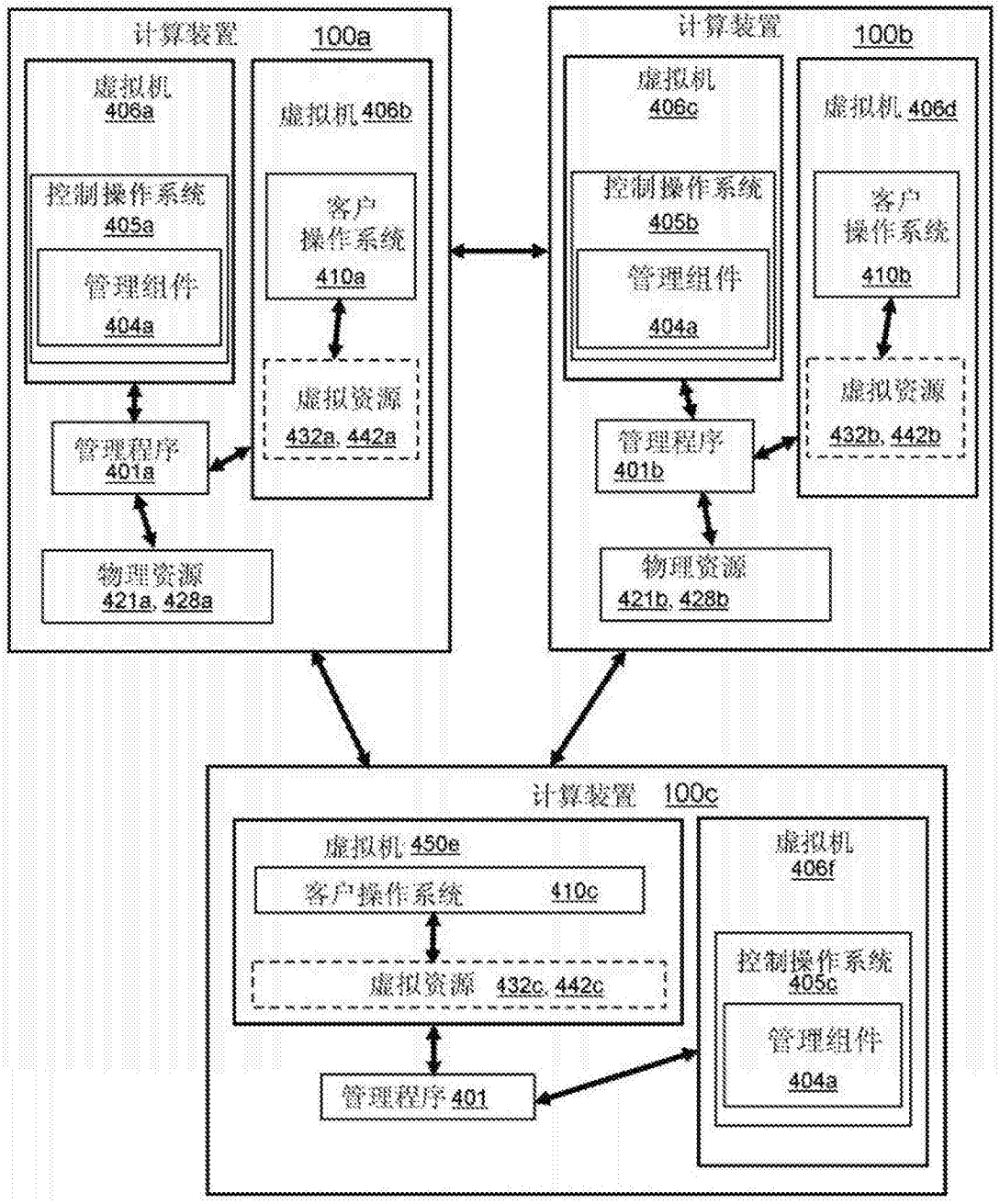

计算装置 100a
虚拟机 406a
控制操作系统 405a
管理组件 404a
虚拟机 406b
客户操作系统 410a
虚拟资源 432a, 442a
管理程序 401a
物理资源 421a, 428a
计算装置 100b
虚拟机 406c
控制操作系统 405b
管理组件 404a
虚拟机 406d
客户操作系统 410b
虚拟资源 432b, 442b
管理程序 401b
物理资源 421b, 428b
计算装置 100c
虚拟机 450e
客户操作系统 410c
虚拟资源 432c, 442c
管理程序 401
虚拟机 406f
控制操作系统 405c
管理组件 404a

图4B

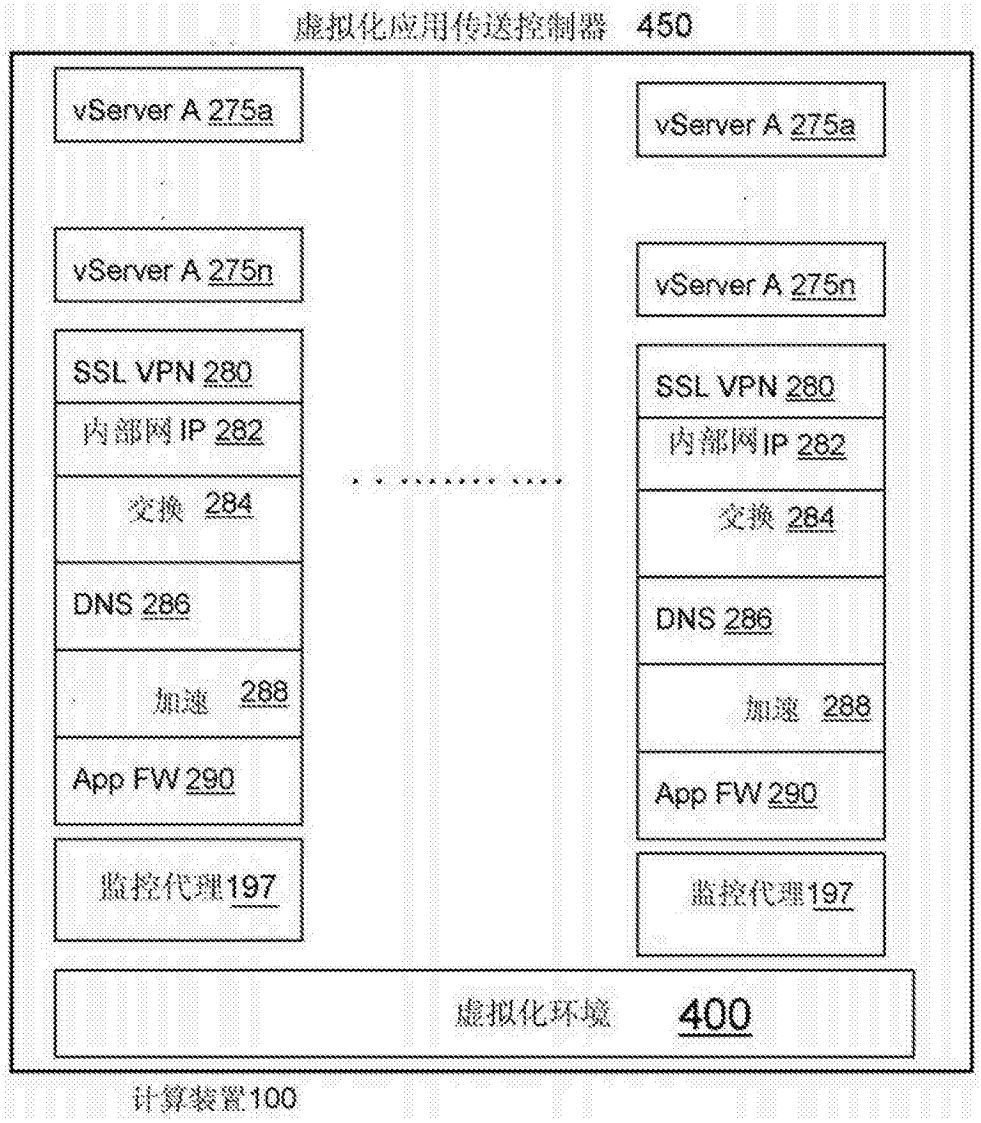

虚拟化应用传送控制器 450
vServer A 275a
vServer A 275n
SSL VPN 280
内部网IP 282
交换 284
DNS 286
加速 288
App FW 290
监控代理197
vServer A 275a
vServer A 275n
SSL VPN 280
内部网IP 282
交换 284
DNS 286
加速 288
App FW 290
监控代理197
虚拟化环境 400
计算装置100

图4C

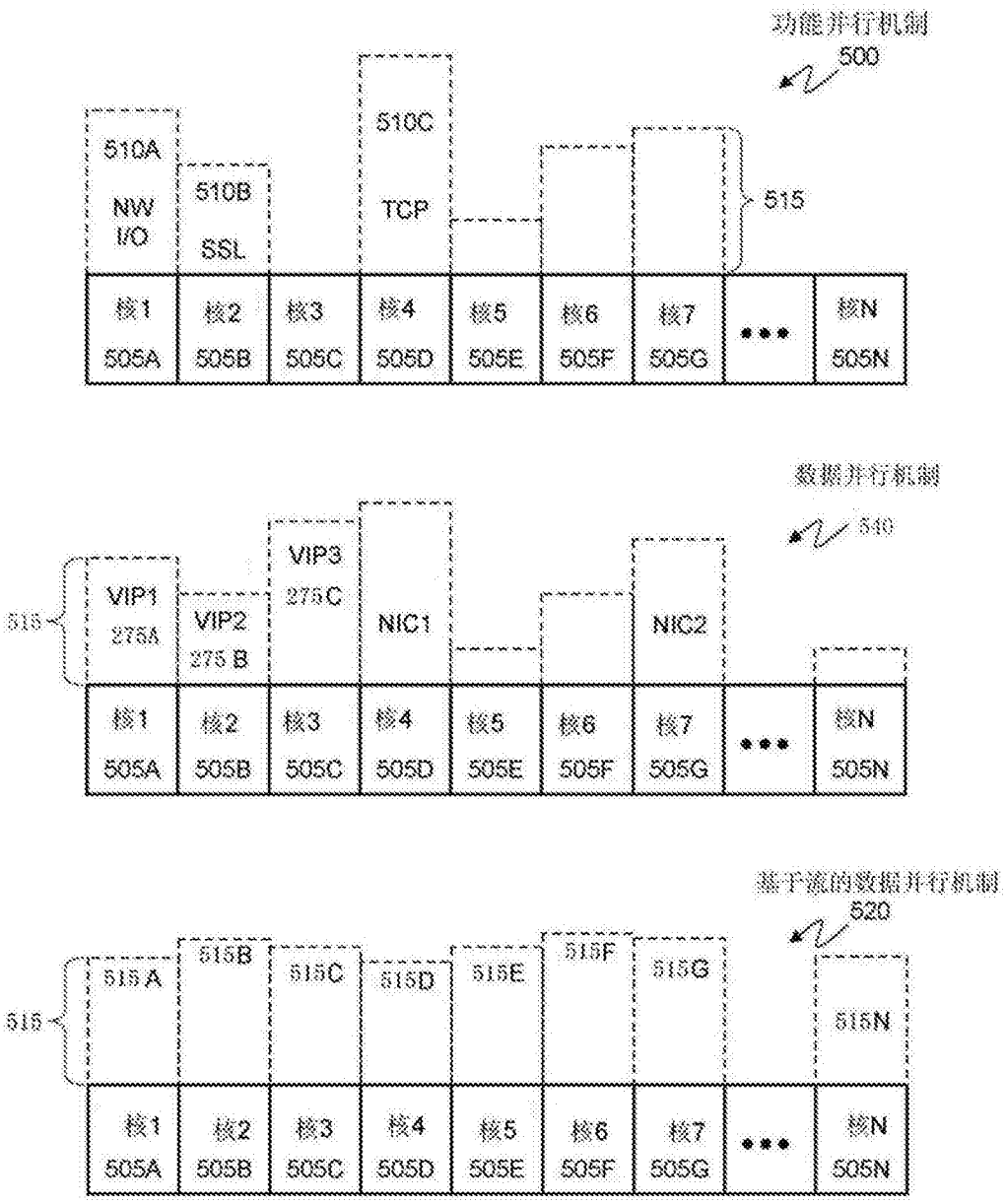

功能并行机制
500
510A
NW I/O
510B
SSL
510C
TCP
515
核1 505A
核2 505B
核3 505C
核4 505D
核5 505E
核6 505F
核7 505G
核N 505N
数据并行机制
540
515
VIP1 275A
VIP2 275 B
VIP3 275C
NIC1
NIC2
基于流的数据并行机制
520
515A
515B
515C
515D
515E
515F
515G
515N

图5A

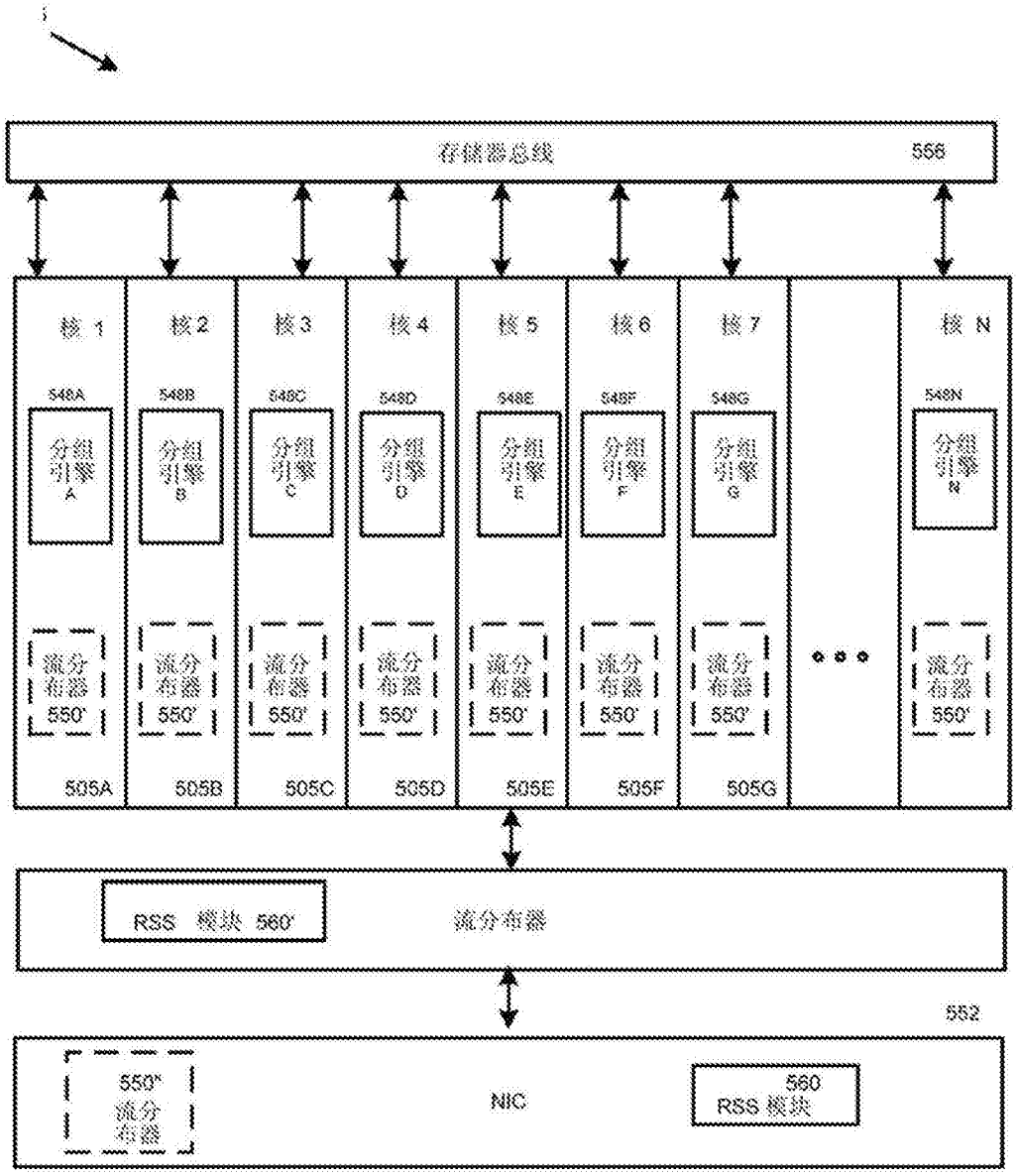

5
存储器总线
556
核 1
核 2
核 3
核 4
核 5
核 6
核 7
核 N
548A
548B
548C
548D
548E
548F
548G
548N
分组引擎 A
分组引擎 B
分组引擎 C
分组引擎 D
分组引擎 E
分组引擎 F
分组引擎 G
分组引擎 N
流分布器 550'
505A
505B
505C
505D
505E
505F
505G
RSS 模块 560'
流分布器
552
550"
流分布器
NIC
560
RSS 模块

图5B

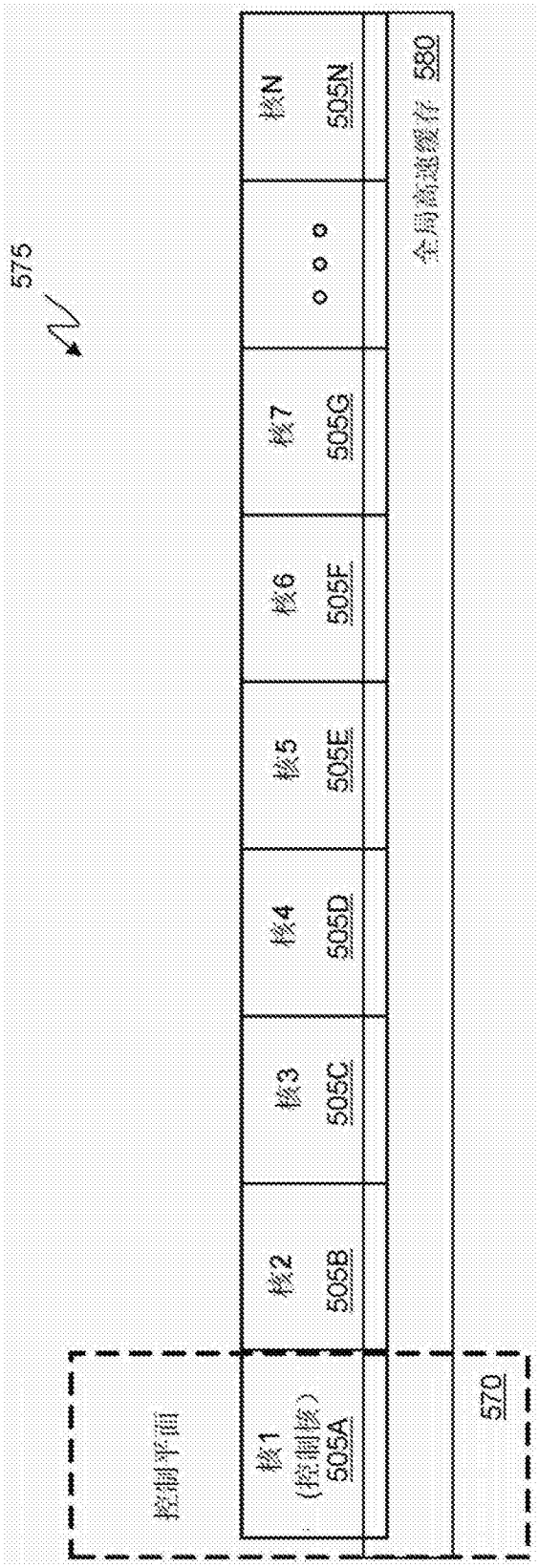

575
核1
(控制核)
505A
核2
505B
核3
505C
核4
505D
核5
505E
核6
505F
核7
505G
核N
505N
570
控制平面
全局高速缓存 580

图5C

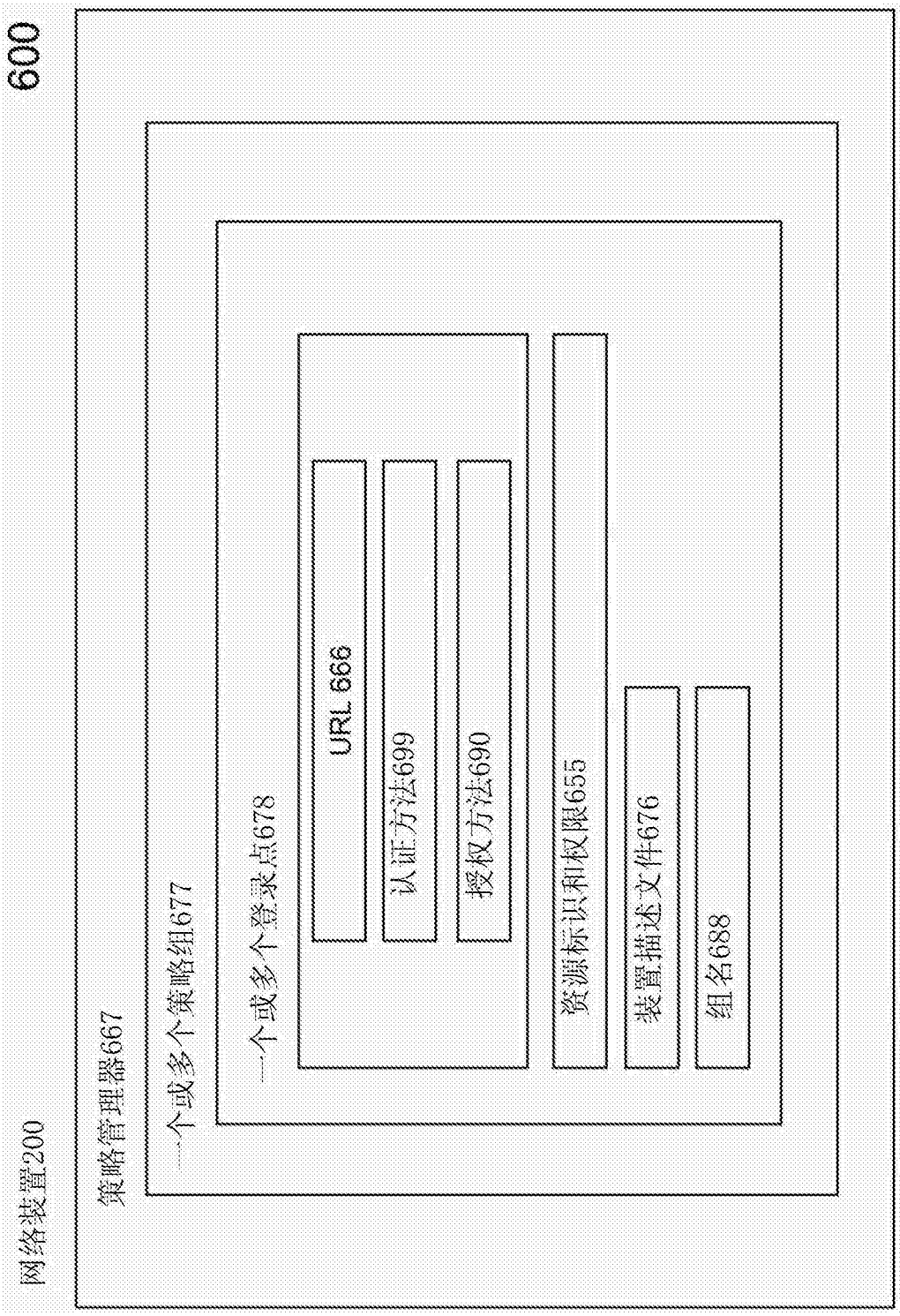

600
网络装置200
策略管理器667
一个或多个策略组677
一个或多个登录点678
URL 666
认证方法699
授权方法690
资源标识和权限655
装置描述文件676
组名688

图6A

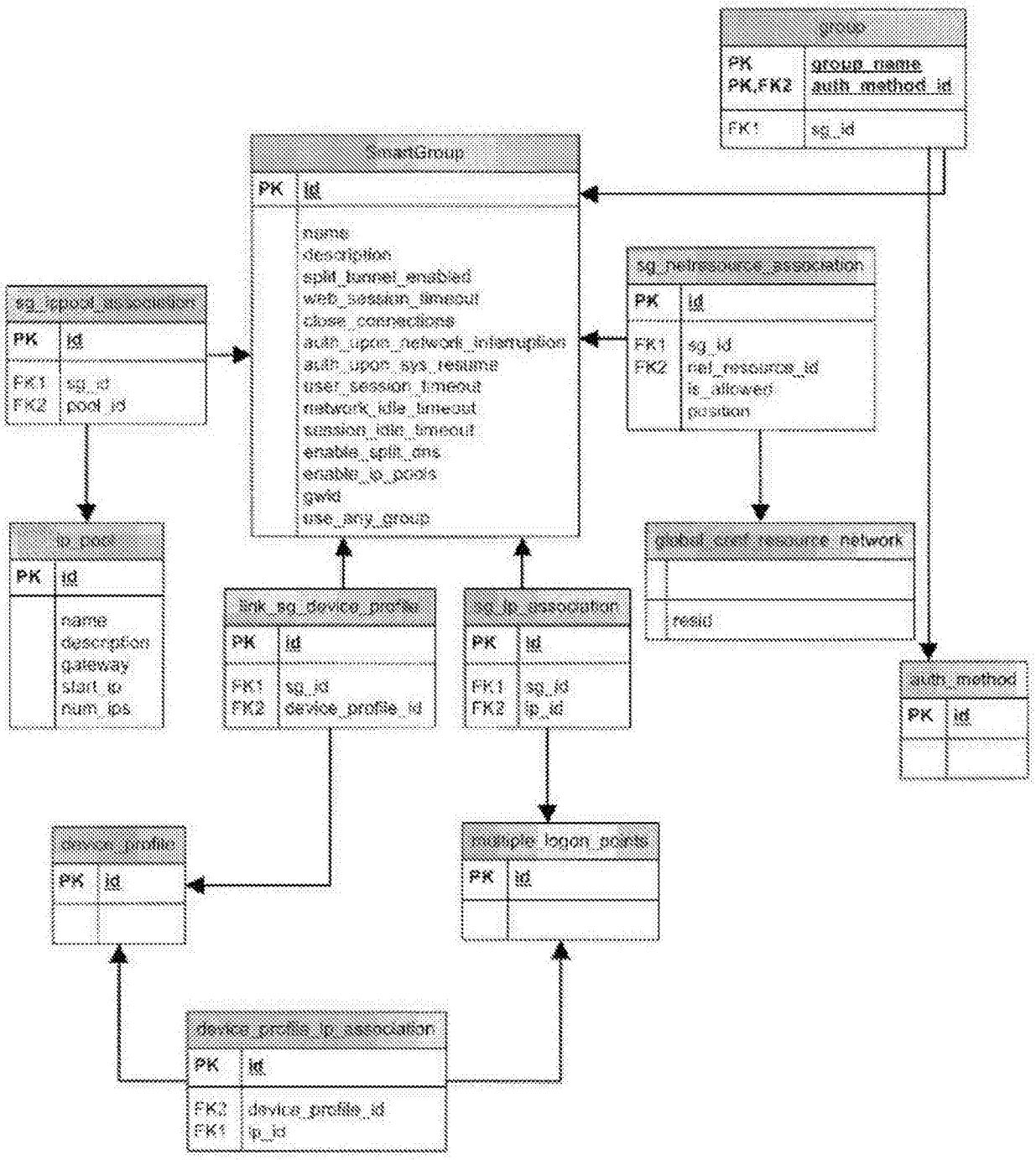

group
PK group_name
PK,FK2 auth_method_id
FK1 sg_id
SmartGroup
PK id
name
description
split_tunnel_enabled
web_session_timeout
close_connections
auth_upon_network_interruption
auth_upon_sys_resume
user_session_timeout
network_idle_timeout
session_idle_timeout
enable_split_dns
enable_ip_pools
gwid
use_any_group
sg_network_resource_association
PK id
FK1 sg_id
FK2 net_resource_id
is_allowed
position
sg_ippool_association
PK id
FK1 sg_id
FK2 pool_id
ip_pool
PK id
name
description
gateway
start_ip
num_ips
link_sg_device_profile
PK id
FK1 sg_id
FK2 device_profile_id
sg_ip_association
PK id
FK1 sg_id
FK2 ip_id
global_conf_resource_network
resid
auth_method
PK id
device_profile
PK id
multiple_logon_points
PK id
device_profile_ip_association
PK id
FK2 device_profile_id
FK1 ip_id

图6B


650
步骤 601
经由在多个客户机和一个或多个服务器中间的装置上执行的策略管理器来建立策略组，该策略组表示一个或多个访问配置的集合，用于用户经由该装置访问一个或多个服务器的一个或多个所识别资源，策略组包括登录点组件，该登录点组件表示访问一个或多个所识别资源的入口点。
步骤 603
经由策略管理器配置登录点组件以指定入口点的统一资源定位符。
步骤 605
经由策略管理器配置为登录点组件选择一个或多个认证方法。
步骤 607
经由策略管理器，基于所述一个或多个认证方法识别登录点组件的一个或多个授权方法。
步骤 609
经由策略管理器，为策略组指定一个或多个装置描述文件，该一个或多个装置描述文件的每一个识别一种或多种类型的端点分析以在用户的装置上执行。
步骤 611
经由策略管理器，为策略组指定一个或多个所识别资源的允许或拒绝访问的一种资源。
步骤 613
由装置接收来自用户的、访问统一资源定位符的请求，该统一资源定位符对应于由登录点组件指定的入口点。
步骤 615
由装置为用户发起由登录点组件指定的一个或多个认证方法。
步骤 617
由装置基于发起的一个或多个认证方法来应用由登录点组件指定的一个或多个授权方法，以访问一个或多个所识别资源。

图6C