



(12) 发明专利

(10) 授权公告号 CN 102577302 B

(45) 授权公告日 2015. 11. 25

(21) 申请号 201080021938. 1

(74) 专利代理机构 北京泛华伟业知识产权代理有限公司 11280

(22) 申请日 2010. 02. 24

代理人 王勇

(30) 优先权数据

61/161,918 2009. 03. 20 US

(51) Int. Cl.

H04L 29/06(2006. 01)

(85) PCT国际申请进入国家阶段日

2011. 11. 18

(56) 对比文件

CN 101069145 A, 2007. 11. 07,

(86) PCT国际申请的申请数据

US 2007277231 A1, 2007. 11. 29,

PCT/US2010/025227 2010. 02. 24

US 2008034410 A1, 2008. 02. 07,

(87) PCT国际申请的公布数据

审查员 闫飞燕

W02010/107558 EN 2010. 09. 23

(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 J·哈里斯 李瑞 A·库玛

R·塔库 P·阿加瓦 A·仇达瑞

P·古伯塔

权利要求书2页 说明书53页 附图19页

(54) 发明名称

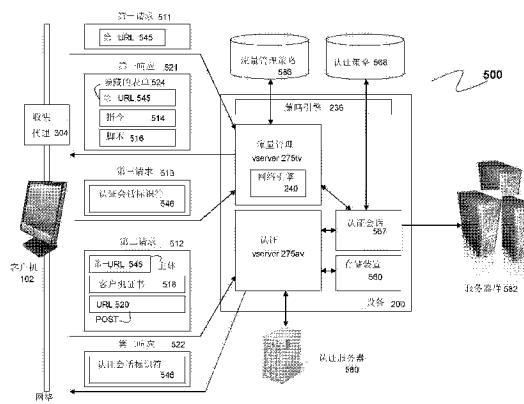
用于在具有流量管理的连接中使用端点审计的系统和方法

(57) 摘要

本发明提供了基于端点审计的结果管理经过中间设备的流量的系统和方法。中间设备的认证虚拟服务器确定对客户机的端点分析扫描的结果。响应于所述确定，流量管理虚拟服务器可从认证虚拟服务器获得该结果。此外，流量管理虚拟服务器可以将该结果应用于一个或多个流量管理策略以便管理经过中间设备的客户机的连接的网络流量。在一些实施例中，认证虚拟服务器可以接收由客户机求值的一个或多个表达式。所述一个或多个表达式标识客户机的一个或多个属性。流量管理虚拟服务器也可以基于对使用该结果的一个或多个流量管理策略的应用来确定用于该连接的压缩或加密类型。

B

CN



1. 一种基于端点分析的结果管理经过中间设备的流量的方法,所述方法包括 :

a) 由中间设备的认证虚拟服务器接收对客户机的端点分析扫描的结果,并且所述认证虚拟服务器在向中间设备的流量管理虚拟服务器转发所述结果之前根据一个或多个授权、认证和审计 / 记账策略来处理全部或部分结果,其中,所述端点分析扫描由所述客户机处的收集代理执行并且作为该认证虚拟服务器的一个或多个授权、认证和审计 / 记账动作的部分而被启动;

b) 由所述流量管理虚拟服务器从认证虚拟服务器获得所述结果;以及

c) 由流量管理虚拟服务器将所述结果应用于一个或多个流量管理策略以便管理经过中间设备的客户机的连接的网络流量,

其中,使用一个或多个策略引擎来识别用于所述认证虚拟服务器和所述流量管理虚拟服务器的一个或多个策略。

2. 根据权利要求 1 所述的方法,其中步骤 (a) 还包括由认证虚拟服务器从客户机接收表达式,所述表达式标识下列的其中一个在客户机上的存在:操作系统的版本、操作系统的服务包、正在运行的服务、正在运行的进程和文件。

3. 根据权利要求 1 所述的方法,其中步骤 (a) 还包括由认证虚拟服务器从客户机接收表达式,所述表达式标识下列的其中一个的存在或版本之一:反病毒软件、个人防火墙软件、反垃圾邮件软件和互联网安全软件。

4. 根据权利要求 1 所述的方法,其中步骤 (a) 还包括由认证虚拟服务器接收由客户机求值的一个或多个表达式,所述一个或多个表达式标识客户机的一个或多个属性。

5. 根据权利要求 1 所述的方法,其中步骤 (b) 还包括由认证虚拟服务器将对标识客户机的一个或多个属性的一个或多个表达式的求值提供为所述结果。

6. 根据权利要求 1 所述的方法,其中步骤 (b) 还包括由认证虚拟服务器将所述结果提供为对流量管理虚拟服务器的一个或多个流量管理策略的输入。

7. 根据权利要求 1 所述的方法,其中步骤 (c) 还包括由流量管理虚拟服务器基于对使用所述结果的一个或多个流量管理策略的应用来确定用于所述连接的压缩类型。

8. 根据权利要求 1 所述的方法,其中步骤 (c) 还包括由流量管理虚拟服务器基于对使用所述结果的一个或多个流量管理策略的应用来确定用于所述连接的加密类型。

9. 根据权利要求 1 所述的方法,其中步骤 (c) 还包括由流量管理虚拟服务器基于对使用所述结果的一个或多个流量管理策略的应用来确定用于所述连接的一个或多个文件类型关联。

10. 根据权利要求 1 所述的方法,其中步骤 (c) 还包括由流量管理虚拟服务器基于经由该一个或多个流量管理策略应用所述结果来确定对于所述连接使用或不使用单点登录。

11. 一种用于基于端点分析的结果管理经过中间设备的流量的中间设备,所述中间设备包括:

认证虚拟服务器,用于接收对客户机的端点分析扫描的结果,并且用于在向中间设备的流量管理虚拟服务器转发所述结果之前根据一个或多个授权、认证和审计 / 记账策略来处理全部或部分结果,其中,所述端点分析扫描由所述客户机处的收集代理执行并且作为该认证虚拟服务器的一个或多个授权、认证和审计 / 记账动作的部分而被启动;

流量管理虚拟服务器,用于从认证虚拟服务器获得所述结果,并将所述结果应用于一

个或多个流量管理策略以便管理经过中间设备的客户机的连接；以及

一个或多个策略引擎，用于识别用于所述认证虚拟服务器和所述流量管理虚拟服务器的一个或多个策略。

12. 根据权利要求 11 所述的中间设备，其中认证虚拟服务器从客户机接收表达式，所述表达式标识下列的其中一个在客户机上的存在：操作系统的版本、操作系统的服务包、正在运行的服务、正在运行的进程和文件。

13. 根据权利要求 11 所述的中间设备，其中认证虚拟服务器从客户机接收表达式，所述表达式标识下列的其中一个的存在或版本之一：反病毒软件、个人防火墙软件、反垃圾邮件软件和互联网安全软件。

14. 根据权利要求 11 所述的中间设备，其中认证虚拟服务器接收由客户机求值的一个或多个表达式，所述一个或多个表达式标识客户机的一个或多个属性。

15. 根据权利要求 11 所述的中间设备，其中认证虚拟服务器将对标识客户机的一个或多个属性的一个或多个表达式的求值提供为所述结果。

16. 根据权利要求 11 所述的中间设备，其中认证虚拟服务器将所述结果提供为对流量管理虚拟服务器的一个或多个流量管理策略的输入。

17. 根据权利要求 11 所述的中间设备，其中流量管理虚拟服务器基于对使用所述结果的一个或多个流量管理策略的应用来确定用于所述连接的压缩类型。

18. 根据权利要求 11 所述的中间设备，其中流量管理虚拟服务器基于对使用所述结果的一个或多个流量管理策略的应用来确定用于所述连接的加密类型。

19. 根据权利要求 11 所述的中间设备，其中流量管理虚拟服务器基于对使用所述结果的一个或多个流量管理策略的应用来确定用于所述连接的一个或多个文件类型关联。

20. 根据权利要求 11 所述的中间设备，其中流量管理虚拟服务器基于经由一个或多个流量管理策略应用所述结果来确定对于所述连接使用或不使用单点登录。

用于在具有流量管理的连接中使用端点审计的系统和方法

[0001] 本专利文件公开的一部分包括受版权保护的内容。版权所有者不反对任何人以专利商标局所公开的文件或记录的形式对专利文件或专利公开进行拓制，除此之外，保留所有版权。

[0002] 相关申请

[0003] 本申请要求在 2009 年 3 月 23 日提交的美国非临时申请 No. 12/409, 332 的优先权，该美国非临时申请要求在 2009 年 3 月 20 日提交的美国临时专利申请 No. 61/161, 918 的利益和优先权，该两个申请通过引用全部包含于此。

技术领域

[0004] 本申请总的涉及数据通信网络。具体而言，本申请涉及用于在具有流量管理的连接中有选择地认证、授权和审计的系统和方法。

背景技术

[0005] 公司或企业可跨越网络部署各种服务以便服务来自多个区域的用户。用户可以使用客户机来请求访问由企业提供的诸如 web 和应用服务器的服务。为了改善对该服务的访问，企业可以在多个不同地理位置动态地部署多个服务器以便改善流量管理，并且根据网络带宽、流量和其他因素来满足用户的需求。网络服务器或设备结合流量管理策略可提供流量管理服务。例如，企业可使用负载平衡器来管理或分布跨越这些服务器的网络流量。而且，为了确定是否对请求访问该服务的客户机准许访问，可以对操作客户机的用户进行认证。该认证过程可以是由网络中的认证服务器（例如 RADIUS 服务器）提供的，以及由访问请求发起的。也可以提供其他的授权、认证和审计 / 记账 (AAA) 服务以建立和监控每个客户机 - 服务器连接。这些 AAA 服务通常是由不同的网络模块提供的。而且，认证服务和流量管理服务通常是被分开实现和 / 或设计的。

发明内容

[0006] 本方案提供为流量管理提供授权、认证和审计 / 记账 (AAA) 支持的系统和方法，通过关联策略特征并扩展握手能力来提高了两个服务集合之间的集成度和互操作性。此外，在 AAA 和流量管理服务之间的关联可以是动态的和 / 或静态的，并且可以在多种配置中被实现。

[0007] 一方面，用于对由流量管理虚拟服务器管理的网络流量进行认证的方法包括由流量管理虚拟服务器从访问服务器的客户机请求确定该客户机还未被认证。该请求包括第一统一资源定位符 (URL)。响应于该请求，流量管理虚拟服务器可以向客户机传输响应。该响应包括第一 URL 和重定向到认证虚拟服务器的指令。认证虚拟服务器可以接收来自客户机的第二请求。第二请求标识第一 URL。认证虚拟服务器接着可以对从客户机收到的证书进行认证并为该客户机建立认证会话。该认证会话可以识别一个或多个策略。而且，认证虚拟服务器可以传输第二响应以便将客户机重定向到流量管理虚拟服务器。第二响应标识该

认证会话。流量管理虚拟服务器可以接收来自客户机的第三请求。第三请求包含认证会话的标识符。

[0008] 在一些实施例中，流量管理虚拟服务器可以确定该请求不包含认证会话的标识符。在一个实施例中，流量管理虚拟服务器可以通过隐藏的表单传输标识第一 URL 的响应。流量管理虚拟服务器也可以传输包括脚本的响应以触发向认证虚拟服务器的 POST 请求的传输。响应于传输该响应，认证虚拟服务器可接收包含到预定的 URL 的 POST 消息的第二请求。在一些实施例中，除了对从客户机接收的证书进行认证外，认证虚拟服务器将第一 URL 和流量管理虚拟服务器的域名与认证会话存在一起。

[0009] 在一些实施例中，响应于收到第三请求，流量管理虚拟服务器（虚拟服务器有时也称为“vServer”）可以验证由标识符识别的认证会话。流量管理 vServer 也可以使用该标识符识别认证会话的一个或多个策略。而且，流量管理 vServer 可以将认证会话的一个或多个策略的授权策略应用于第三请求。流量管理 vServer 也可以将认证会话的一个或多个策略的流量管理策略应用于第三请求。

[0010] 在又一个方面，提供对由流量管理虚拟服务器管理的网络流量的认证的系统包括流量管理虚拟服务器。流量管理虚拟服务器可以从访问服务器的客户机请求确定该客户机还没有被认证。该请求可包括第一统一资源定位符 (URL)。响应于该请求，流量管理虚拟服务器可以向客户机传输包括第一 URL 和重定向到用于认证的第二虚拟服务器的指令的响应。系统也可以包括接收来自客户机的第二请求的认证虚拟服务器。第二请求标识第一 URL。而且，认证虚拟服务器可以对从客户机收到的证书进行认证并为该客户机建立认证会话。该认证会话可以识别一个或多个策略。此外，认证虚拟服务器可以传输第二响应以便将客户机重定向到流量管理虚拟服务器。第二响应标识该认证会话。流量管理虚拟服务器可以接收来自客户机的第三请求。第三请求包含认证会话的标识符。

[0011] 在又一个方面，用于从多个认证虚拟服务器中动态地选择认证虚拟服务器的方法包括由流量管理虚拟服务器从自客户机接收的访问服务器的内容的请求来确定客户机还没有被认证。流量管理虚拟服务器可识别用于从多个认证虚拟服务器选择一个认证虚拟服务器的策略以便提供对客户机的认证。流量管理虚拟服务器可以通过该策略从多个认证虚拟服务器选择认证虚拟服务器以便认证客户机。响应于该请求，流量管理虚拟服务器可以向客户机传输响应。该响应包括重定向到所选择的认证虚拟服务器的指令。

[0012] 在一个实施例中，流量管理虚拟服务器确定该请求不包含会话 cookie。在又一个实施例中，流量管理虚拟服务器确定该请求不包含对有效的认证会话的索引。流量管理虚拟服务器可基于请求的用户来识别用于选择认证虚拟服务器的策略。流量管理虚拟服务器也可以基于所收集的关于在客户机上安装的软件的信息来识别用于选择认证虚拟服务器的策略。此外，流量管理虚拟服务器可以基于所收集的关于客户机上的操作系统的信息来识别用于选择认证虚拟服务器的策略。

[0013] 在一个实施例中，响应于该策略的识别，流量管理虚拟服务器从多种类型的认证虚拟服务器中选择认证虚拟服务器作为第一类型的认证虚拟服务器。在又一个实施例中，响应于该策略，流量管理虚拟服务器基于多种认证类型的一种认证类型来选择认证虚拟服务器。在又一个实施例中，流量管理虚拟服务器基于与客户机的对多种认证类型的一种认证类型的协商来选择认证虚拟服务器。在一些实施例中，流量管理虚拟服务器接收访问资

源的第二请求。第二请求可包括识别对认证虚拟服务器的认证会话的索引的会话 cookie。流量管理虚拟服务器也可以从由该索引识别的认证会话确定要应用于第二请求的一个或多个流量管理策略。

[0014] 在又一个方面,用于从多个认证虚拟服务器中动态地选择认证虚拟服务器的系统包括设备的流量管理虚拟服务器。流量管理虚拟服务器可从自客户机接收的访问服务器的内容的请求来确定客户机还没有被认证。流量管理虚拟服务器也可以识别用于从多个认证虚拟服务器选择认证虚拟服务器的策略以便提供对客户机的认证。该系统也可以包括策略引擎,其给流量管理虚拟服务器提供选择多个认证虚拟服务器的一个认证虚拟服务器的策略以便认证客户机。该系统也可包括流量管理虚拟服务器的网络引擎。网络引擎可向客户机传输对该请求的响应。该响应包括重定向到所选择的认证虚拟服务器的指令。

[0015] 在又一个方面,基于端点审计的结果管理经过中间设备的流量的方法包括由中间设备的认证虚拟服务器确定对客户机的端点分析扫描的结果。流量管理虚拟服务器从认证虚拟服务器获得该结果。此外,流量管理虚拟服务器可以将该结果应用于一个或多个流量管理策略以便管理经过中间设备的客户机的连接的网络流量。

[0016] 在一个实施例中,认证虚拟服务器从客户机接收表达式,所述表达式标识在客户机上的存在的下列的其中一个:操作系统的版本、操作系统的服务包、正在运行的服务、正在运行的进程和文件。认证虚拟服务器也可以接收表达式,所述表达式标识在客户机 102 上的存在的下列之一,或下列的版本:反病毒软件、个人防火墙软件、反垃圾邮件软件和互联网安全软件。在一些实施例中,认证虚拟服务器可以接收由客户机求值的一个或多个表达式。所述一个或多个表达式标识客户机的一个或多个属性。认证虚拟服务器可以将对标识客户机的一个或多个属性的一个或多个表达式的求值提供为结果。认证虚拟服务器也可以将所述结果提供为对流量管理虚拟服务器的一个或多个流量管理策略的输入。

[0017] 在一些实施例中,流量管理虚拟服务器基于对使用所述结果的一个或多个流量管理策略的应用来确定用于所述连接的压缩类型。流量管理虚拟服务器也可以基于对使用该结果的一个或多个流量管理策略的应用来确定用于该连接的加密类型。此外,流量管理虚拟服务器可以基于对使用该结果的一个或多个流量管理策略的应用来确定用于所述连接的一个或多个文件类型关联。流量管理虚拟服务器也可以基于经由一个或多个流量管理策略应用所述结果来确定对于所述连接使用或不使用单点登录。

[0018] 在又一个方面,用于基于端点审计的结果管理经过中间设备的流量的中间设备包括认证虚拟服务器。认证虚拟服务器可以确定对客户机的端点分析扫描的结果。中间设备也包括流量管理虚拟服务器,其从认证虚拟服务器获得该结果,并且将该结果应用于一个或多个流量管理策略以管理经过中间设备的客户机连接。

[0019] 在下面的附图和描述中详细阐述了本发明的各种实施例的细节。

附图说明

[0020] 本发明的前述和其它目的、方面、特征和优点,通过参考下述结合附图的描述将会更加明显并更易于理解,其中:

[0021] 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;

[0022] 图 1B 是从服务器经由设备传送计算环境到客户机的环境的实施例的框图;

- [0023] 图 1C 是从服务器经由网络传送计算环境到客户机的环境的实施例的框图；
[0024] 图 1E 到 1F 是计算装置的实施例的框图；
[0025] 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；
[0026] 图 2B 是用于优化、加速、负载平衡和路由客户机和服务器之间的通信的设备的又一个实施例的框图；
[0027] 图 3 是用于通过设备与服务器通信的客户机的实施例的框图；
[0028] 图 4A-4E 是在其中认证 vServer 可与流量管理 vServer 相关联的配置的实施例的框图；
[0029] 图 5 是为流量管理提供 AAA 支持的系统的实施例的框图；
[0030] 图 6A-6B 是用于为流量管理提供 AAA 支持的方法的步骤的实施例的流程图；
[0031] 图 7A-7B 是用于为流量管理提供 AAA 支持的方法的步骤的多个实施例的流程图；
[0032] 图 8 是基于端点审计的结果来管理经过中间设备的流量的方法的步骤的实施例的流程图。
[0033] 从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

- [0034] 为了阅读下述本发明的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：
[0035] -A 部分描述有益于本发明的实施例的网络环境和计算环境；
[0036] -B 部分描述用于向远程用户加速传送计算环境的系统和设备架构的实施例；
[0037] -C 部分描述用于加速客户机和服务器之间的通信的客户机代理的实施例；
[0038] -D 部分描述用于向流量管理提供认证、授权和审计支持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。在其它实施例中，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。在其它实施例中，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。在其它实施例中，设备 200 包括由位于华盛顿州西雅图的 F5 Networks 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。在其它实施例中，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 可与群 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 上所识别的应用的执行而产生的诸如显示数据的应用输出数据。

[0050] 现在参考图 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] 现在参考图 1C，描述了网络环境的另一个实施例，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。在其它实施例中，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。在其它实施例中，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。在其它实施例中，设备 205 包括由位于华盛顿州 Seattle 的 F5 Networks 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。在其它实施例中，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。在其它实施例中，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。在其它实施例中，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] 现在参考图 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。在其它实施例中，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 所应用的任一认证和授权策略，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 PresentationServer™），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。在其它实施例中，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 PresentationServer™），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 CitrixSystems 有限公司开发的 ICA 客户机。在其它实施例中，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 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] 仍然参看图 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。在其它实施例中, 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] 在其它实施例中, 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。在其它实施例中, 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。在其它实施例中, 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。在其它实施例中, 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 PresentationServer) 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 (activeserver)。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。在其它实施例中, 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] 在又一个实施例中, 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 使用和磁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。在其它实施例中, 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。在其它实施例中, 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,或者能够按照这里所说明的那样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、PC100 SDRAM、双数据速率 SDRAM(DDR SDRAM)、增强型 SRAM(ESDRAM)、同步链路 DRAM(SLDRAm)、直接 Rambus 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,或者能够像这里所说明的那样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背侧总线。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 130 进行通信,同时直接与 I/O 装置 130 进行通信。

[0079] 计算装置 100 可以支持任何适当的安装装置 116, 例如用于接收像 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、多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。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 分发获得。

[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。在其它实施例中, 计算装置 100 可以提供 USB 连接以接收手持 USB 存储装置, 例如由位于加利福尼亚州 Los Alamitos, 的 Twintech Industry 公司生产的设备的 USB 闪存驱动器线。

[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。在其它实施例中, 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。在其它实施例中, 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会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] 在进一步的实施例中, 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：WINDOWS 3.x、WINDOWS 95、WINDOWS 98、WINDOWS 2000、WINDOWS NT 3.51、WINDOWS NT 4.0、WINDOWS CE 和 WINDOWSXP，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，以及其他。

[0085] 在其它实施例中，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] B. 设备架构

[0087] 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。

[0088] 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'。在其它实施例中，处理器 262 或者 262' 包括多核处理器。

[0089] 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。

[0090] 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。

[0091] 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 202。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 Mac OS®、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。

[0092] 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 是操作系统的中心，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。

[0093] 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。

[0094] 如图 2 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。

[0095] 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,而在另一个实施例中,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。

[0096] 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。在其它实施例中,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。

[0097] 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 可作为程序、服务、进程或任务操作执行在内核空间 204 中,并且在其它实施例中,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)。

[0098] 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。在其它实施例中,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它实施例此处进一步描述。

[0099] 在一些实施例中,策略引擎 236 可以提供配置机制以允许用户识别、指定、定义或

配置指导包括但不限于图 2B 中描述的诸如 vServers 275、VPN 功能 280、内联网 IP 功能 282、交换功能 284、DNS 功能 286、加速功能 288、应用防火墙功能 290 和监控代理 197 的部件的设备的任何其它部件或功能的行为的策略。在其它实施例中，策略引擎 236 可以响应于任一配置的策略来进行检查、评价、实现或者以其他方式产生作用，并且还可以响应于策略来指导一个或多个设备功能的操作。

[0100] 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。在其它实施例中，加密引擎 234 包括运行在加密处理器 260 上的可执行指令。

[0101] 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 IP 上语音 (VoIP) 协议。在其它实施例中，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)。

[0102] 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 Microsoft 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。

[0103] 高速层 27 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。

[0104] 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 27 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，而在其它实施例中，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 27 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无效。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。

[0105] 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。GUI 210 和 GLI 212 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。GUI 210 和 GLI 212 可包括运行在用户空间 202 或内核框架 204 中的代码。GUI 210 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。CLI 212 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，CLI 212 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 GLI 212。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 GUI 210 和 / 或 CLI 212 的与设备 200 或者操作系统的交互。

[0106] 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。

[0107] 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，而在其它实施例中，一个或多个守护服务 218 运行在内核空间。

[0108] 现在参考图 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 vServer 275、vS 275、VIP 服务器或者仅是 VIP 275a-275n（此处也称为 vServer 275）。vServer 275 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。

[0109] vServer 275 可以包括软件、硬件或者软件和硬件的任何组合。vServer 275 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。vServer 275 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 VPN 280、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，vServer 275 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 vServer 275 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。

[0110] 在一些实施例中，vServer 275 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 vServer 275 相关联。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 vServer 275a-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、分组中的首部或者字段、或者通信的上下文，诸如用户、用户组、vServer 275、传输层连接、和 / 或客户机 102 或者服务器 106 的标识或者属性。

[0111] 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 的认证和 / 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 的认证和 / 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 的认证和 / 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 的策略控制网络业务流量以及通信会话。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。

[0112] 在一些实施例中, vServer 275 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, vServer 275 监听和接收来自客户机 102 的通信。在其它实施例中, vServer 275 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, vServer 275 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, vServer 275 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, vServer 275 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。

[0113] 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。在其它实施例中, 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。

[0114] 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 IntranetIP 282 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 IntranetIP 282, 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, vServer 275 监听和响应到客户机 102 的 IntranetIP 282 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 IntranetIP 282 的查验。在又一个实施例中, 设备可以与请求和客户机 IntranetIP 282 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。

[0115] 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”。

[0116] 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）的情况下，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）的情况下，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。

[0117] 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 有效载荷或应用层请求数据来分配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 利用承载为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。

[0118] 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。

[0119] 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。在其它实施例中，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。在其它实施例中，应用防火墙 290 通过执行合法的 URL 来防御强制浏览。

[0120] 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。

[0121] 仍然参考图 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。在其它实施例中，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。

[0122] 在其它实施例中，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 vServers 275A 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。在其它实施例中，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。

[0123] C. 客户机代理

[0124] 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。

[0125] 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 IEEE 802.3 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 IEEE 802.11 和 / 或移动因特网协议。

[0126] 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 IP 语音 (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 IP 上 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。

[0127] 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。在其它实施例中, 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。

[0128] 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, 而在其它实施例中, 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。

[0129] 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, 而其它部分在用户模式 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。在其它实施例中, 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。

[0130] 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。在其它实施例中，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。在其它实施例中，拦截器 350 为用户模式应用或者程序，诸如应用。

[0131] 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。

[0132] 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。

[0133] 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）。在其它实施例中，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'。

[0134] 客户机代理 120 和 / 或拦截器 350 可以对网络堆栈 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。

[0135] 此外,客户机代理 120 和 / 或拦截器可以对任何应用、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。

[0136] 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 有限公司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。

[0137] 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。

[0138] 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。

[0139] 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。在其它实施例中，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客户机到网络 104 的连接的访问、认证和授权控制。

[0140] 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。

[0141] 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。在其它实施例中，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。

[0142] 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。在其它实施例中，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。

[0143] 在一些实施例中，仍参见图 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。

[0144] D. 对流量管理的认证、授权和审计 (AAA) 支持

[0145] 在流量管理系统的一些实施例中，客户机 102 传输访问由一个或多个服务器 106 提供的服务 270 的请求。该请求可以由提供流量管理功能的中间设备（例如设备 200）进行拦截和处理。通过举例且考虑到不同的流量管理和负载平衡产品，设备 200 可以是由 Citrix System 公司出品的被称为 NetScaler 的产品实施例、由 F5 网络公司出品的 BigIP 装置、由 Radware 有限责任公司出品的 AppDirector 设备，或者由 Cisco System 公司或 NortelNetwork 公司出品的设备中的任何一个。设备 200 可以具有一个或多个虚拟服务器 275A-275N，所述虚拟服务器 275A-275N 被配置、构建或设计为提供如上文结合图 2A 描述的各种网络通信功能。

[0146] 设备 200 可以包括一个或多个流量管理 vServer 275tv 或与其通信，所述流量管理 vServer 275tv 提供在一个或多个网络 104、104’ 上的客户机 102 与一个或多个服务器 106 之间的流量管理 (TM) 功能。在一些实施例中，设备 200 包括一个或多个认证 (AuthN) vServer 275av 或与其通信，所述认证 vServer 275av 提供用于控制客户机 102 对服务 270 的访问的认证服务。为了给流量管理特征提供 AAA 支持，流量管理 vServer 275tv 和认证 vServer 275av 可以通信以便处理客户机 - 服务器访问和流量的任意方面。流量管理 vServer 275tv 和认证 vServer 275av 的任何一个也可以驻留在一个或多个设备 200 或服务器 106 中并通过一个或多个网络 104、104’ 通信。此外，可以通过其各自的宿主服务器在结构上或者在逻辑上分层次地连接或布置任何数量的流量管理 vServer 275tv 和认证 vServer 275av，以便提供流量管理和认证服务。

[0147] 流量管理 vServer

[0148] 流量管理 vServer 275tv 可以是用于执行流量管理活动的任何类型的虚拟服务器，包括负载平衡 (LB)、内容交换 (CS) 和高速缓存重定向 (CR)。例如，在一些实施例中，高速缓存重定向 vServer 识别用于重定向到另一个服务器的可缓存的和不可缓存的消息，所述另一个服务器可以是 vServer（例如，LB vServer）、高速缓存服务器或源服务器。通过有选择地重定向流量，可以从高速缓存检索一些请求的内容，例如经常访问的内容。在这些实施例的一个中，高速缓存重定向识别对于 HTTP 事务的可缓存的和不可缓存的请求。高速缓存重定向可以通过解析每个请求的 HTTP 头部和 URL 识别对于 HTTP 事务的可缓存的和不可缓存的请求。另一方面，内容交换可包括各种操作技术，所述各种操作技术用于以可优化网络使用的方式使数据从一个或多个源到达端点。

[0149] 流量管理 vServer 275tv 可包括上文结合图 2B 所描述的 vServer275 的任意实施例，并提供任何类型的功能和特征。流量管理 vServer 275tv 可根据一个或多个 TM 策略的集合来操作。而且，TM vServer 275tv 可包括策略引擎 236 或用策略引擎 236 进行操作，所述策略引擎 236 例如上文结合图 2A 所描述的策略引擎 236 的任意实施例。在一些实施例中，可以将来自一个或多个 TM vServer 275tv 的一个或多个流量管理特征与一组或多组 TM 策略进行组合。在一个实施例中，可以在互相之间不冲突的范围内来组合一个或多个特征。举例说明，在一个实施例中，由 TM vServer 支持的特征和 / 或流量管理策略可包括，但不限于：

[0150] ○ 401 认证方法支持，例如基本认证 (Basic-Authentication)；

[0151] ○对非 HTTP 客户机的认证支持；

[0152] ○对在认证和流量管理 vServer 之间的任何类型或形式的复杂的和 / 或灵活的关

联的支持，

[0153] ■除了被关联到 LB vServer 之外, 认证 vServer 也可被关联到 CS 或 CR vServer ;

[0154] ■支持认证和流量管理 vServer 之间多对多的关系；

[0155] ■允许基于策略动态地选择认证 vServer ；

[0156] ■允许对使用哪种类型的认证的交互性决策。认证 vServer 可决定执行哪种类型的认证。也允许客户机与认证 vServer 就该客户机能选择的认证的类型进行协商。

[0157] ○会话同步 (Session Sync) 以支持在主动的 / 主动配置的设备 (例如 CITRIX Netscaler 设备) 之间的外部认证。这在一些实施例中可支持认证 vServer 驻留在一个设备 (其中可以定义或控制认证行为) 而流量管理 vServer 驻留在另一个设备上的需求, 也就是属于同一域的流量管理 vServer 为了负载分布的目的可散布在多个设备上但仍使用单点登录 (SSO) 认证。例如, 在一个实施例中, 在一个设备上认证的用户 (例如, 由于访问在该设备上的流量管理 vServer 并被重定向到用于认证服务的另一个设备) 可单点登录到属于同一域的任何其他设备上的任何流量管理 vServer。

[0158] ○支持对于端用户的可定制的会话管理门户网页；

[0159] ○支持与其他模块的集成：

[0160] ■应用防火墙 (AppFirewall), 包括 XML 支持

[0161] ■集成缓存

[0162] ■压缩

[0163] 网络引擎

[0164] 流量管理 vServer 275tv 可包括和 / 或操作网络引擎 240。网络引擎 240 可以是硬件和软件的组合。网络引擎 240 可包含来自上文结合图 2A 所描述的集成的分组引擎 240 的任意实施例的一个或多个特征。网络引擎 240 可包括用于接收和传输网络流量的收发器。在一些实施例中, 网络引擎 240 也可包含硬件接口, 例如来自设备 200, 以与网络 104 和其他网络组件连接。在一个实施例中, 网络引擎 240 与客户机 102 和 / 或认证 vServer 275av 相接口。网络引擎 240 可执行任何类型或形式的数据处理, 例如压缩、加密、加速、缓冲、检索、转换、重定向, 以及协议处理。此外, 网络引擎可访问和 / 或更新所存储的会话表, 例如 AAA-TM 会话表。网络引擎 240 可以包括策略引擎 236 或与策略引擎 236 通信并访问一个或多个策略。在一个实施例中, 网络引擎 240 可提供和 / 或应用所访问的一个或多个策略。在一些实施例中, 网络引擎 240 可提供流量管理 vServer 275tv 的一些或全部功能。

[0165] 认证 vServer

[0166] 认证 vServer 275av 可以是执行 AAA 服务的授权、认证和审计 / 记账特征的任意组合的虚拟服务器。在一些实施例中, 认证 vServer 275av 可包括上文结合图 2B 所描述的 vServer275 的任意实施例, 并提供任何数量和类型的功能和特征。而且, 认证 vServer 275av 可包括上文结合图 2A 所描述的策略引擎 236 的任意实施例或用其进行操作。在一些实施例中, 认证 vServer275av 可包括虚拟专用网 (VPN) vServer 的任意实施例和 / 或特征, 用于对访问 TM vServer 275tv 和 / 或服务 270 的用户进行认证。在这些实施例的一个中, VPN vServer 可以是轻量级的 vServer。

[0167] 在一些实施例中, 认证 vServer 275av 可以驻留于一个或多个认证服务器上或与其通信, 所述一个或多个认证服务器例如在一个或多个网络 104、104' 上聚集或分布的远

程访问远程认证拨入用户服务 (RADIUS) 服务器、防火墙、访问控制服务器以及认证、授权和审计 / 记账 (AAA) 服务器。

[0168] 认证 vServer 275av 可支持灵活的基于策略的规则。认证 vServer 275av 也可根据不同的访问请求方案提供任何 AAA 服务。认证 vServer 275av 可根据一个或多个认证策略 568 的集合来进行操作。认证策略 568 也可以包括至少一个授权策略和 / 或至少一个审计 / 记账 (此后总的称为“审计”) 策略。在一些实施例中,可以由在流量管理 vServer 275tv 上配置的授权策略执行授权。在这些实施例的一些中,认证 vServer 275av 仅提供认证相关的服务。进一步地,认证策略 568 可包括至少一个 VPN 策略。在一些实施例中,可以通过将现有的 VPN 特征 (例如 VPN 策略和数据结构) 与其他认证特征相组合来实现对流量管理的认证支持。在一些实施例中,可被包含到对流量管理的 AAA 支持中的 VPN 特征包括但不限于 :

- [0169] ■ 单点登录 (SSO) 服务
- [0170] ■ Cookie 代理
- [0171] ■ 动态的每用户 / 组感知的流量管理策略 (例如, 集成缓存、AppFirewall 等)
- [0172] ■ 基于表单的 SSO
- [0173] ■ 接受从 Microsoft ADFS 到来的 SSO 断言
- [0174] ■ 接受从 Netegrity 到来的 SSO 断言。例如, 基于安全和标记语言 (SAML) 的支持。
- [0175] ■ 接受从其他认证或互联网下载管理 (IDM) 供应商到来的 SSO 断言。
- [0176] ■ 对自定制的 / 自主开发的 / 一次性认证系统的可扩展的认证

[0177] 认证 vServer 275av 可支持任何数量、类型和形式的认证和 / 或授权服务器, 例如活动目录 (AD)、轻量级目录访问协议 (LDAP)、RADIUS、RSASecureID、终端访问控制器访问 - 控制 (TACACS) 和 TACACS+、WINDOWS NT LAN 管理器 (NTLM) 和智能卡登录。在一些实施例中, 多个认证 vServer 可支持两个或多个不同类型的认证。在这些实施例的一个中, 可以依据认证 vServer 275av 支持的认证类型 (例如, TACACS+) 来选择该认证 vServer 275av。通过认证 vServer 可用的认证类型可以被一个或多个认证和 / 或授权服务器支持。例如, 两个 RADIUS 服务器可以支持 RADIUS vServer。可基于一个或多个因素, 例如地理上的接近性、网络流量和每个服务器上的处理负载来将一个或两个 RADIUS 服务器 (例如, 静态地或动态地) 绑定到或分配给该认证 vServer。在一些实施例中, 基于一个或多个策略的应用将一个或多个认证服务器关联或分配或绑定到认证 vServer 275av。例如, 可以在结构上或逻辑上以级联的形式布置所述一个或多个认证服务器。

[0178] 可以基于上下文动态地或以其他方式支持和定制各种认证配置, 例如双因素认证 (T-FA) 或双重密码认证。认证 vServer 275av 也可支持基于证书的认证。在一些实施例中, 来自一个或多个认证 vServer 275av 的 AAA 特征可能会同一组或多组 AAA 或认证策略组合在一起。可以将认证 vServer 275av 关联到、或分配给或绑定到下面将要讨论的多个不同配置中的一个或多个 TMvServer 275tv。认证服务器 275av 可以通过预定义的绑定与 TM vServer 275tv 静态地关联, 或者基于一个或多个策略与 TM vServer 275tv 动态地关联。

[0179] 现参考图 4A, 描述了用于将认证 vServer 275av 关联到一个或多个 TMvServer 275tv 的系统的实施例。认证 vServer 275av 可以被静态地绑定到一个 TM vServer 或者由多个包括静态和 / 或非静态绑定的 TM vServer 共享。

[0180] 现参考图 4B, 描述了用于将认证 vServer 275av 关联到一个或多个 TMvServer 275tv 的系统的两个实施例。在一个实施例中, 第一认证 vServer 275av1 可以被关联到多个 TM vServer 275tv1、275tv2, 而第二认证 vServer 275av2 可以被关联到一个 TM vServer 275tv3。可以依赖于诸如流量管理域的大小、负载和诸如就近分组的地理上的考虑的因素来创建这样的分组或分配。

[0181] 在一些实施例中, 其中多个认证 vServer 275av 与 TM vServer 275tv 配置在一起, 跟踪和 / 或验证过程可确保一直在该 TM vServer 275tv 和所选择的认证 vServer 275av 之间处理客户机请求。例如, 该 TM vServer 275tv 可以验证: 重定向消息是从在该 TM vServer 275tv 收到初始的客户机请求时所选择的同一认证 vServer 275av 接收的。

[0182] 现参考图 4C, 描述了用于将一个或多个认证 vServer 275av 关联到 TMvServer 275tv 的系统的实施例。总的来说, 该系统包括一个或多个策略、多个认证 vServer 275av1-N, 和 TM vServer 275tv。可以基于一个或多个策略将认证 vServer 275av 动态地分配给 TM vServer 275tv。可以在运行时将一个或多个策略绑定到 TM vServer 275tv。而且, 可以在运行时经由一个或多个策略将一个或多个认证 vServer 275av 的任何一个或多个分配给该 TMvServer 275tv 以建立认证会话。

[0183] 在一些实施例中, 一个或多个策略可包括 AppFW 策略。AppFW 策略和与 AppFW 模块一起操作, 所述 AppFW 模块在由 Citrix Systems 公司出品的设备的环境中有时也被称为 AppSecure 模块。AppSecure 模块可包括用于执行任何类型和形式的内容重写 (例如, URL 重写) 的逻辑、功能或操作。在一些实施例中, AppSecure 模块可执行对在客户机和服务器之间的请求和 / 或响应的任何类型或形式的内容注入。AppSecure 模块可将诸如 JavaScript 的脚本注入到对客户机的响应中以执行任何类型和形式的期望的功能。在一个实施例中, AppFW 策略可以被设计和构造来重写请求和响应的 URL 以便重定向到特定的认证 vServer 275av 或以其他方式与其关联。例如, 可以由 TM vServer 对在认证会话期间所接收的消息中的链接 (例如, URL) 进行修改, 这样将该链接指向特定认证 vServer 275av。

[0184] 认证 vServer 275av 可以被关联到任何形式或类型的 TM vServer 275tv, 包括 CR、CS 和 LB vServer 的任意组合或分层布置。在该分层结构中可以将流量的单位 (例如消息或分组) 从第一 TM vServer 重定向到另一个 TMvServer。这个过程可以发生在该分层结构的多个层次上, 直到最终的 TMvServer 被指定为管理该流量为止。在一些实施例中, 其中将多个认证 vServer 275av 关联到 TM vServer 的分层结构。与最具体的 TM vServer 关联的认证 vServer 275av 优先提供 AAA 功能。然而, 在一些其他实施例中, 优先考虑与处于分层结构顶部的 TM vServer 275tv 关联的认证 vServer 275av。可以将管理响应于客户机请求的全部流量的 TM vServer 275tv 指定为分层结构的顶部。在其他实施例中, 可以通过一个或多个策略来确定任一认证 vServer 275av 的优先级, 该一个或多个策略例如与处于分层结构顶部的 TM vServer 275tv 关联的策略。

[0185] 现参考图 4D, 描述了用于给流量管理提供 AAA 支持的系统的实施例。总的来说, 该系统包括与多个认证 vServer 275av 关联的、并且以分层配置布置的多个 CR、CS 和 LB TM vServer。该系统可包括上文结合图 4A-4C 描述的配置的任意组合和实施例。在一些实施例中, 分层配置支持内容感知的流量管理和认证。例如, 在一个实施例中, 在 CR vServer 275crv 处收到的流量可以被分为可缓存的和不可缓存的流量。该流量可以

包括在一个或多个客户机 102、服务器 106 和中间设备之间的任何类型和形式的消息，包括请求和响应。在一些实施例中，可缓存的流量被定向到 CS vServer275csv2，而不可缓存的流量被定向到 CS vServer275csv1。CS vServer275csv1 可将不可缓存的流量分布到 LB vServer2751bv11、2751bv12 上，而 CS vServer275csv2 可在 LB vServer2751bv21、2751bv22 之间分布可缓存的流量。

[0186] 在图 4D 的进一步的细节中，举例说明分层配置的一个实施例，该配置包括在 LB vServer2751bv11、2751bv21 和 CS vServer275csv1 处动态地关联的认证 vServer；在 LB vServer2751bv12、CS vServer275csv2 和 CRvServer275crv 处静态地关联的认证 vServer；以及关联到 LBvServer2751bv22 的非认证 vServer。例如，如果 LB vServer2751bv12 被选择来执行流量管理，那么关联到 LB vServer2751bv12 的认证 vServer 可提供 AAA 特征。在另一个实施例中，如果未关联到任何认证 vServer 275av 的 TM vServer 被选择来执行流量管理，那么可通过与该 TM vServer 的父亲关联的认证 vServer 275av 来提供 AAA 特征。例如，如果选择了 LBvServer2751bv22，那么关联到 CS vServer275csv2 的认证 vServer 可提供 AAA 特征。如果在分层结构中 TM vServer 在同一层或不同层上有多个父亲，则例如，根据认证 vServer 的可用性、地理上或逻辑上的接近度，和 / 或一个或多个策略，多个父亲的其中一个可提供关联的认证 vServer 275av。

[0187] 现参考图 4E，描述了用于给流量管理提供 AAA 支持的系统的另一个实施例。在进一步的细节中，图 4E 示出了在其中可以由多个 TM vServer 共享一个认证 vServer 275av 的实施例。在一些实施例中，为系统配置了单个认证 vServer 275av，这样可以不要求跟踪和 / 或验证过程，和 / 或将该认证 vServer 275av 绑定到 TM vServer 275tv 的策略。在一些实施例中，父 TMvServer 可将所有流量管理责任定向到子 TM vServer 以便关联认证 vServer275av。例如，CS vServer275csv2 可以将所有的流量管理责任定向到 LBvServer2751b21 而不是 LB vServer2751bv22。在一些其他实施例中，可以在没有 AAA 支持的情况下管理被定向到不与任何认证 vServer 275av 关联的 TM vServer 的流量管理责任，或者可以将其重定向到与认证 vServer 275av 关联的另一个 TM vServer。

[0188] 现参考图 5，描述了用于为流量管理提供 AAA 支持的系统 500 的实施例。总的来说，系统 500 包括与一个或多个认证 vServer 275av（此后总的称为“认证 vServer”）关联的一个或多个 TM vServer 275tv（此后，总的称为“TM vServer”）。可以任何方式来布置这些 vServer，例如根据上文结合图 4A-E 描述的配置的任意实施例。TM vServer 根据一个或多个流量管理策略 586 在客户机 102 和服务器群 582 中的一个或多个服务器 106 之间提供流量管理服务。可以由认证 vServer 根据一个或多个认证策略 568 为任何客户机 - 服务器流量提供 AAA 服务。此外，收集代理 304 可以为 TM vServer 和认证 vServer 之一或全部获取来自客户机 102 的信息。尽管在图 5 所示的实施例中只描述了一个客户机 102、收集代理 304、应用服务器群 582 和存储装置 560，但应理解该系统可提供这些组件中任意个或每个的多个。

[0189] 收集代理

[0190] 收集代理 304 可包括上文结合图 3 描述的收集代理 304 和 / 或结合图 2B 描述的监控代理 197 的任何实施例或组件。可以从驻留在设备 200、存储装置 560 和 / 或网络 104 中的任何其他机器或存储装置中的任何脚本或程序来生成收集代理 304。在一些实施例中，

将脚本和 / 或程序传输到客户机 102 并生成收集代理 304。在一些其他实施例中，收集代理 304 执行于设备 200 或网络中的任何其他机器中并且远程地轮询、请求或收集来自客户机 102 的信息。收集代理 304、脚本和 / 或程序可以是用于收集诸如客户机 102 的端点装置的属性的端点审计 (EPA) 系统或解决方案的部分。

[0191] EPA 可以包含端点分析、端点扫描和端点检测的一个或多个。EPA 解决方案可在做出 AAA 和 / 或流量管理决策之前在客户机 102 上执行一系列安全、身份和装置完整性检查。例如，EPA 解决方案可以扫描客户机 102 的文件和注册表设置，并且检查没有引入未授权的、非法的或没有许可证的可执行代码（包括间谍软件、恶意软件和木马）。EPA 解决方案在用于系统 500 的实施例中时，也可以包含上文结合图 3 所描述的端点检测和扫描技术和 / 或组件的任何实施例的全部或部分。EPA 解决方案的一个实施例是 CITRIX 访问网关高级端点分析软件开发工具包（端点分析 SDK）。EPA 解决方案的其他实施例包括来自 EPA FACTORY 和 EXTENTRIX 的解决方案。

[0192] 在图 5 的进一步的细节中，设备 200 可操作或执行 TM vServer 和认证 vServer 的其中一个、二者、或二者都不操作或执行。在一些实施例中，认证 vServer 在第一设备或第一组设备 200a 上执行，而 TM vServer 在第二设备或第二组设备 200b 上执行。在一个实施例中，设备 200 被配置、设计和构造来使用私有的或定制的协议和 / 或通信模型。在又一个实施例中，设备 200 可以支持一个或多个协议和 / 或通信模型。设备 200 可包括一个或多个策略引擎 236 或与其通信。在一些实施例中，流量管理和 / 或认证服务各自操作或执行于一个或多个设备 200 的用户空间 202 和内核空间 204 的其中一个或者用户空间 202 和内核空间 204 的组合。如结合图 4A-E 所讨论的，TMvServer 和认证 vServer 可驻留于网络 104 上的一个或多个服务器 106 和 / 或中间设备 200。TM vServer 和 / 或认证 vServer 可包括一个或多个策略引擎 236 或与其通信。

[0193] 策略引擎

[0194] 一个或多个策略引擎 236 可各自驻留于系统 500 的任意组件上。所述一个或多个策略引擎 236 的每一个可以是上文结合图 2A 所描述的策略引擎 236 的任意实施例。而且，每个策略引擎 236 可被静态地或动态地绑定到一个或多个策略或者策略的集合，例如流量管理策略 586 和认证策略 568。此外，一个或多个策略引擎 236 可以识别用于 TM vServer 和认证 vServer 的一个或多个策略。在一些实施例中，一个或多个策略引擎 236 应用一个或多个策略用于 TM vServer 或认证 vServer 并且将该应用的一个或多个结果发送到 TM vServer 或认证 vServer。在其他实施例中，一个或多个策略引擎 236 可以将一个或多个所识别的策略发送到 TM vServer 和 / 或认证 vServer。

[0195] 存储装置

[0196] 设备 200 可包括存储装置 560。存储装置 560 可以是上文结合图 1E 所描述的存储装置、上文结合图 1F 所描述的主存储器 122 或高速缓存 140，以及上文结合图 2A 所描述的存储器 264 的任意实施例。存储装置 560 可存储任何类型或形式的信息，包括持续性信息（例如，在认证会话期间持续的客户机信息）和临时信息（在运行期间生成的中间数据）。在一些实施例中，存储装置 560 可存储一个或多个 URL，例如与客户机请求关联的 URL。存储装置 560 也可以存储机器或 vServer 275 的域名、地址、定位符、索引或其他标识符，例如 TM vServer 的域名。存储装置 560 也可以存储一个或多个策略，例如流量管理策略 586 和

认证策略 568。而且，存储装置 560 可存储跟踪 AAA 和流量管理事务或记录 AAA 和流量管理事务日志的 AAA-TM 会话表。

[0197] 策略

[0198] 流量管理策略 586、认证策略 568 和一个或多个策略引擎 236（此后总称为“策略”或“策略引擎 236”）可包括响应于一组输入和 / 或条件而被应用和 / 或输出的任何形式和类型的策略、规则、程序、要求、指令、指南和建议。一些流量管理策略 586 和 / 或认证策略 568 可以例如在连接会话或认证会话期间无限期地持续或在固定时间段内持续。一些流量管理策略 586 和 / 或认证策略 568 可以是持续的，直到事件发生为止。一些流量管理策略 586 和认证策略 568 可以是静态的，其是由管理员预定义的或由机器生成的。一些流量管理策略 586 和认证策略 568 可以是动态的，例如，根据包括网络、流量模式、服务器负载、访问频率和访问历史的条件的任意组合的条件而适应性改变或调整。而且，可以由其他策略修改和 / 或生成这些策略的一些。

[0199] 流量管理策略 586 和认证策略 568 可驻留于网络 104 的任何地方的一个或多个存储装置中。这样的存储装置可以是结合图 1E 所描述的存储、结合图 1F 所描述的主存储器 122 或高速缓存 140，结合图 2A 所描述的存储器 264、以及结合图 5 所描述的存储装置 560 的任意实施例。在一些实施例中，流量管理策略 586 和认证策略 568 可一起驻留在例如设备 200 和 / 或存储装置 560 中。在其他实施例中，这些策略可包括地理上或逻辑上分开的策略组，例如根据上文结合图 4A-4E 所描述的配置而分布的策略。

[0200] 流量管理策略 586 可包括直接或间接影响流量管理活动和 / 或决策的任何策略。例如，流量管理策略 586 可包括与非流量管理策略（例如，认证策略 568）联合应用的策略以做出流量管理决策。而且，流量管理策略 586 可包括与下列内容相关的任何策略：1) 流量路由、重定向、寻址、分布，2) 服务器、服务器群、网关、客户机、vServer、设备或其他网络组件的选择和分配，3) 流量数据加密、压缩、加速、缓冲和其他类型的处理，4) 流量溢出支持，5) 网络或网络组件失效支持，6) 流量数据收集、分析、报告，以及 7) 服务水平的管理。

[0201] 认证策略 568 可包括直接或间接影响 AAA 活动和 / 或决策的任何策略。例如，认证策略 568 可包括与非 AAA 策略（例如，流量管理策略 586）联合应用的策略以做出 AAA 决策。在一些实施例中，认证策略 568 可包括与安全和访问控制特征关联的任何策略，所述安全和访问特征例如安全套接字层 (SSL)、虚拟专用网 (VPN)、防火墙、加密、水印、安全密钥、用户或客户注册、上下文的访问级别，以及 EPA。认证策略 568 可支持由认证 vServer 和所关联的认证服务器 580 所支持的特征的全部或任意子集。

[0202] 在一些实施例中，将授权和 / 或审计 / 记账策略与认证策略分开组织，逻辑上分区或物理上存储于不同的存储装置中。一个或多个认证、授权和 / 或审计 / 记账策略可以在这些策略的另一个之前、之后被使用或与这些策略的另一个联合使用。在特定的条件发生或满足时，或者被另一策略调用时，可以使用这些 AAA 策略的任何一个。而且，这些 AAA 策略的任何一个可以与 AAA 或认证 vServer 相关联或者绑定到 AAA 或认证 vServer。此外，例如，根据上文结合图 4A-4E 描述的配置的任意实施例，这些 AAA 策略的任何一个可以经由 AAA 或认证 vServer 与 TM vServer 相关联或者绑定到 TM vServer。

[0203] 可以响应于来自客户机 102 的请求来使用与 TM vServer 相关联的或绑定到 TM vServer 的授权策略。在一些实施例中，可以在客户机 102 已被认证后使用授权策略。在

这些实施例的一个中,可以在客户机 102 已被认证后将绑定到 TM vServer 的授权策略应用于相关的流量。授权策略可以被关联或绑定到用户、组、vServer 或全局级别。在一些实施例中,可以支持或优选绑定到某些级别的授权策略。例如,在一个实施例中,由于所有流量被定向到 TM vServer,所以可以容易地支持在 TM vServer 级别对授权策略的支持。由于冲突、冗余、协同或其他,第一级授权策略的存在或缺席也可以影响对第二级授权策略的支持。例如,如果已经支持诸如内容过滤策略的组级别的策略,这可能与 vServer 级别的策略相冲突或优于 vServer 级别的策略。例如,在一些实施例中,可以从关于各种流量管理特征的已有的或替代的全局授权策略的角度来评估支持组级别的策略的决策,例如用于 VPN 特征的默认授权组。

[0204] 在一些实施例中,认证、授权和审计特征是分开的和 / 或由不同的 vServer 提供的。例如,在一个实施例中,认证策略可以被绑定到认证 vServer 并且在认证会话建立期间被应用于验证用户证书。在会话建立之后,该会话可与认证策略解除关联,同时可以引入被绑定到给定的用户或组的授权策略。接着可以在运行时评估这些授权策略以对照每个给定的请求来做出决定。因此,在一些实施例中,在认证和授权策略之间可能没有重叠。

[0205] 审计策略可以具有大体上类似于认证或授权策略的属性或特性。审计策略可以被绑定到一个或多个 TM vServer、认证会话、和流量管理会话。审计策略可以支持由任何形式或类型的 AAA 或认证 vServer 和服务器提供的特征。所支持的审计特征可包括,但不限于对下列内容的支持:

[0206] ■ 对在包括 TCP、UDP 和 HTTP 的多个协议中的流量管理端用户的全面的或定制的审计跟踪;

[0207] ■ 对系统管理员和流量管理端用户的完整的或定制的审计跟踪,例如记录命令和跟踪基于角色的管理;

[0208] ■ SYSLOG 和 / 或高性能 TCP 记录;

[0209] ■ 记录系统事件;

[0210] ■ 支持丰富的细节;

[0211] ■ 可脚本化的或可定制的记录格式;

[0212] ■ 不同粒度的基于策略的审计;以及

[0213] ■ 专用于 TM 的 AAA 的审计。

[0214] 可以以用户、组、vServer、全局或其他级别设置策略,或者为多个级别设置策略。在本发明的各种实施例中,可以支持特定级别或特定的级别组。在一些实施例中,可以将用于策略级别的任何现有的框架(例如,认证策略的框架)扩展到不同的策略集合(例如,流量管理策略)。例如,在一个实施例中,用于支持流量管理的新的认证策略可以通过继承相关的用户或组的定义和数据库来对现有的用于审计策略的用户框架或组框架产生影响。可以分层顺序或扁平化(flat)来指定策略间的优先级。在一些实施例中,有用于策略的扁平的优先级空间。对于诸如流量管理策略的某些策略,可以在配置时确定将要被评估的策略的顺序。例如,可以在确定后维护这样的策略的有序列表,并将其应用于多个认证会话。可以在运行时确定一些其他策略的优先级顺序。策略所属的策略级别可以确定是在运行时还是在配置期间确定优先级顺序。

[0215] 在图 5 的进一步的细节中,上文所讨论的策略和 vServer 可作用于处理访问服务

器 106 的客户机请求。在涉及客户机 102、TM vServer 和认证 vServer 之间的多个请求和响应的多个事务上处理该请求。请求和响应可以是任意通信协议（私有的或其他的）中的任何类型或形式的消息。在一些实施例中，该消息可以是 HTTP、HTTPS 或类似协议的形式。这些消息可包括任何类型或形式的信息，例如与客户机 102、所请求的资源、设备 200，以及认证会话 567 相关联的信息。

[0216] 请求 511

[0217] 在一些实施例中，客户机 102 发起请求 511，所述请求被拦截或路由到 TM vServer。该请求 511 可包括 URL 545。URL 545 可以是指向将要连接的服务器 106 的资源或标识符的指针。在一些实施例中，请求 511 中可以不包括 URL 545。请求 511 也可包括诸如中间设备或设备 200 的地址的信息，以及识别要使用的策略和 / 或认证服务器的信息。此外，请求 511 可包括指示客户机 102 是否已被认证和 / 或是否需要已认证的访问的信息。例如，在一些实施例中，请求 511 中可以包括域会话 cookie。如果域会话 cookie 是有效的，则这可以指示已经对发送请求 511 的客户机 102 和 / 或用户进行了认证。如果域会话 cookie 是无效的，或者如果与域会话 cookie 相关联的关联的认证会话已过期，则可以执行认证或者重新认证。

[0218] 域会话 cookie

[0219] 域会话 cookie 可以给有效的认证会话提供认证会话信息，例如索引或标识符 546。域会话 cookie 可用于跟踪经过流量管理 vServer 的已认证的流量的状态信息。在一个实施例中，如果在流量管理 vServer 收到的请求 511 包括有效的域会话 cookie，那么关联的认证会话 567 将会被“刷新”或者在另一个预定时间段内处于活动状态。在一个实施例中，域会话 cookie 包括一个或多个下列信息：

[0220] ● Cookie 名

[0221] ● Cookie 值 :< 认证会话索引 >

[0222] ● 域 :< 流量管理 vServer 域 >

[0223] ● 路径

[0224] ● 到期时间 :< 值 / 未设置 / 默认 >

[0225] 在一些实施例中，可以在认证之前创建认证会话 567。在这些实施例的一个中，域会话 cookie 的暴露会引起某些安全问题，并且由流量管理 vServer 接收的流量将必须被安全地保护。在这些实施例的另一个中，域会话 cookie 的暴露不引起安全问题。在其他实施例中，认证会话是在认证时或认证后被创建的。例如，在这些实施例的一个中，认证会话是响应于认证而被创建的。

[0226] 响应 521

[0227] 再参考图 5，在进一步的细节中，TM vServer 可响应于请求 511 而发出响应 521。在一些实施例中，响应 521 是 200 OK HTTP 响应。响应 521 可包括用于在客户机 102 处显示的页面或表单。响应 521 也可包括任何数目、类型和形式的字段、按钮和用于显示和 / 或用户交互的其他部件。响应 521 可包括 URL 545。在一些实施例中，其中请求 511 不包括任何 URL，响应 521 可包括可能由 TM vServer 生成的 URL 545。该 URL 545 可以是至少部分地从请求 511 中所包含的信息和 / 或一个或多个流量管理策略 545 的应用中生成的。URL 545 可以以隐藏的表单或隐藏的字段的方式被包含在响应 521 中。在一些实施例中，将这样

的隐藏的字段或表单的输入类型指定为“HIDDEN”。与隐藏的表单或字段关联的文档（例如 Html 文档）在其被显示在浏览器中时可能不显示该隐藏的表单或字段，也不显示该隐藏的表单或字段的值或内容。在一些实施例中，面对该文档的用户不会与该隐藏的表单或字段交互。响应 521 也可包括加载时提交事件句柄。加载时提交事件句柄可以包括在预定事件出现时发起或触发消息的命令的任何集合，或者任何形式或类型的脚本或程序。例如，当用户点击“提交”按钮时，可以触发提交隐藏的表单或字段的消息。

[0228] 响应 521 可包括将请求 511 重定向到认证服务器的指令 514。指令 514 可以是由 TM vServer 生成的、至少部分地从请求 511 中所包含的信息和 / 或一个或多个流量管理策略 545 的应用而生成的。指令 514 可包括任何类型或形式的命令（例如 HTTP 命令），或者任何类型或形式的程序代码。此外，可以根据客户机 102 的类型或能力来定制指令 514。在一些实施例中，指令 514 可包含脚本 516 或者被包含在脚本 516 中。客户机 102 可执行脚本 516，或者在客户机 102 处收到脚本 516 时，该脚本 516 可自动执行。脚本可以是事件句柄。在其他实施例中，脚本 516 可独立于指令和 / 或服务于不同的目的。脚本 516 可触发、生成或以其他方式由客户机 102 发起第二或另外的请求 512。

[0229] 请求 512

[0230] 在一些实施例中，请求 512 用于将 URL 545 和 / 或其他信息传递或重定向到诸如认证 vServer 的目的地。在其他实施例中，在将 URL 545 和 / 或其他信息传递到目的地的过程中，302 响应可代替响应 521。请求 512 可包括重定向位置头部。该重定向位置头部可包括任何类型或形式的信息，例如用于检索登录页面的信息。在一个实施例中，重定向位置头部可具有下面的格式：

[0231] 位置 :<http|https>://<vpn_vServer>:<port>/vpn/index.html

[0232] 在一些实施例中，请求 512 是由用户动作触发的，例如与客户机 102 处收到的响应 521 关联的在提交按钮上的鼠标点击。在其他实施例中，当客户机 102 处收到响应 521 时，请求 512 自动地触发。在一个实施例中，脚本 516 可将请求 512 生成为 POST（发布）消息。在一些实施例中，例如与 302 重定向消息可在其 HTTP 头部包含的内容相比，POST 消息能够包含更多的内容，例如，诸如较长的 URL。POST 消息可包括 URL520。请求 512 的 URL520 可是指向任何类型或形式的脚本、可执行文件、程序或资源的指针。在一些实施例中，URL520 可指向脚本或可执行文件的目录、目录树或者脚本或可执行文件的位置。在这些实施例的一个中，URL520 是指向 CGI 可执行文件的指针。URL520 可指向包含 CGI 可执行文件的 CGI 二进制目录或目录树。URL520 可包含字符串，例如“/cgi/tm”。该字符串可指示响应 521 是来自 TM vServer 的重定向消息。在一些实施例中，诸如“/cgi/tm”的 URL 字符串可以是硬编码的、预定的或动态生成的。URL520 也可以是不同于 URL 的一些其他类型或形式的指针或指示器。

[0233] 请求 512 可包括任何类型或形式的信息，例如与客户机 102、任何所请求的资源、设备 200，认证会话 567 和请求 511 相关联的信息。该请求 512 也可包含 URL 545。在一些实施例中，请求 512 可在该请求 512 的主体中包含 URL 545。请求 512 也可包含客户机和 / 或用户证书 518。在一些实施例中，证书 518 用于认证客户机 102 和 / 或用户。在各种实施例中，证书 518、URL 545 和 URL520 的一个或多个可以是可选的或者必须的。这些证书 518、URL 545 和 URL520 的一个或多个可以驻留在请求 512 的主体中、请求 512 的 POST 请求行

中、请求 512 的头部或其他部分中。在一个实施例中，请求 512 包括但不限于下列属性的任何一个或多个：

- [0234] ● 请求行 :POST/cgi/tm
- [0235] ● 主机 :< 认证 vServer 标识符或定位符 >
- [0236] ● 主体 :url = <URL 545>
- [0237] 请求 512 可包括任何类型或形式的标记或 cookie，例如 AAA cookie。AAA cookie 是由 TM vServer、客户机 102 或系统 500 的任何其他模块生成的，和 / 或依据一个或多个策略 586/568 生成的。AAA cookie 可用于在认证过程中执行对任何类型和形式的状态和 / 或数据的跟踪。AAA cookie 可包括一个或多个属性，并且每个属性可包括任何类型或形式的信息，例如关于认证 vServer 和关联的认证会话 567 的信息。可以在认证期间重复利用 AAA cookie。当认证会话 567 到期时，AAA cookie 会到期。在一些实施例中，AAA cookie 是仅对认证 vServer 275av 的域有效，并且可能在发送到 TM vServer 的请求中是不可用的。在一个实施例中，AAA cookie 包括但不限于下列属性：

- [0238] ● Cookie 名
- [0239] ● Cookie 值
- [0240] ● 域 :< 认证 vServer >
- [0241] ● 路径
- [0242] ● 到期时间
- [0243] 认证会话
- [0244] 在一些实施例中，认证会话 567 可以是响应于请求 512 而被创建的。当进行连接或资源请求时，以及在一些实施例中在认证会话已过期之后，认证 vServer 275av 可建立认证会话来认证客户机 102 和 / 或用户。认证会话 567 可表示任何类型或形式的连接、通道、会话、集合或事务单元。此外，认证会话 567 可支持任何会话层服务和协议。认证会话也可以大体上类似于任何现有类型的安全的、认证的和 / 或加密的会话、通道或连接或者包含其特征。

[0245] 在一些实施例中，认证会话 567 是 VPN 会话。如果认证会话 567 是由 VPNvServer 或服务器创建的，则其可以是 VPN 会话。在一些实施例中，认证会话 567 基本上类似于 VPN 会话和 / 或包含 VPN 会话的特征。例如，在一个实施例中，可以通过集成轻量级的 VPN 框架来提供认证，这样可以包含未来的 VPN 增强，例如安全保证标记语言 (SAML) 和活动目录联合服务 (ADFS)。在又一个实施例中，认证会话 567 包括另外的字段，例如存储所关联的 TMvServer 的域名和 URL 545 的字段。

[0246] 可以在认证 vServer 275av 收到从 TM vServer 重定向的第一客户机请求之后马上创建认证会话。在一些实施例中，该会话的创建可以发生在认证之前。然而，VPN vServer 可以在完成认证后创建 VPN 会话。这个区别的原因在于在认证之前创建认证会话以存储 TM vServer 的域名和由客户机向 TMvServer 发起的初始请求的 URL 的其中一个或者全部。在一些实施例中，可能需要或提供防止拒绝服务 (DOS) 攻击的对认证会话的保护，例如防止发送填满 AAA-TM 会话表的消息的黑客，防止拒绝合法用户的访问。

[0247] 在一些实施例中，认证会话可能被刷新，或在另一个指定的时间段内被激活。在这些实施例的一个中，如果在流量管理 vServer 处收到的请求 511 中发现有效的域会话

cookie，则认证会话可以在另一指定时间段内处于活动状态。如果认证会话没有被刷新，则其可能超时，并且客户机 102 可能必须被重新认证（例如，重新登录）。会话超时有时也可以被称为被动超时。认证会话 567 可以通过用户的明确的退出（例如，点击退出按钮或链接）而终止或者当该会话超时时终止。在一些实施例中，一旦用户退出，认证会话（例如，在诸如 CITIRX Netscaler 设备的设备 200 上的认证会话）就变为无效的。用户可能必须要被重新认证以进入有效的认证会话。在一个实施例中，可以支持对用户退出的 CGI 支持。例如，可以在“/cgi/logout”路径中找到处理该退出的可执行文件，并将其链接到例如退出按钮。在又一个实施例中，可以支持包括退出功能的完整的会话管理页面，并在客户机 102 处显示该页面。也可以定制该完整的会话管理页面。可以从存储装置中检索该完整的会话管理页面并且 / 或者在到客户机 102 的消息中包含该页面。

[0248] 在一些实施例中，对流量管理的 AAA 支持可提高认证登录速率和 / 或增加并发会话的数量。例如，这些认证登录速率和并发会话的数量可能比典型的 VPN 应用高。这也可能增加存储器消耗。为了抵消这样的增加，管理员可设置较小的会话超时值，例如用于认证会话 567 的较小的默认超时值。

[0249] 认证会话 567 可以与或者不与流量管理会话（未示出）共存和 / 或互操作。在一个实施例中，在认证会话之后开始流量管理会话。在又一个实施例中，流量管理会话启动一个或多个认证会话和 / 或与其交互。例如，为了在流量流过期间审计 / 记账的目的，流量管理会话也可以与认证会话互操作、访问 AAA 反馈和 / 或作出或更新流量管理决策。在一些实施例中，用于认证和 / 或支持流量管理的 VPN 的安全模型可能使会话建立和认证令牌收集发生在安全通道（SSL）上，但可能不要求流量管理内容是安全的。认证和 / 或 VPN 支持可以保护流量管理 vServer 而不管穿过该流量管理 vServer 的流量。

[0250] 响应 522

[0251] 例如如果客户机 102 的认证是成功的，则生成对客户机 102 的第二响应 522，以使得认证会话 567 是可利用的。第二响应 522 可标识到客户机 102 的认证会话 567。认证 vServer 可生成第二响应 522 并且将该响应 522 传输到客户机 102。第二响应 522 可以在第二响应 522 的主体中、第二响应 522 的 POST 消息结构中、在域会话 cookie、头部或第二响应 522 的任何其他部分中包含认证会话标识符 546 或信息。在一些实施例中，认证会话标识符 546 可以被称为认证会话索引 546。认证索引 546 可以用于标识有效的认证会话。

[0252] 在一些实施例中，第二响应 522 可以是 HTTP 302 消息，或任何其他类型或形式的重定向消息。在一些实施例中，第二响应 522 可以在认证后将客户机请求重定向回到 TM vServer。在一个实施例中，第二响应包括但不限于下列信息和 / 或结构的任何一个或多个：

[0253] ■位置头部格式：

[0254] ●位置 :< 协议 >://<traffic_management_vServer>[:< 端口 >]/<url>

[0255] < 协议 > 和 < 端口 >：可取决于流量管理 vServer IP 和服务端口；

[0256] <traffic_management_vServer>：可以从认证会话中复制，并且可能最初来自于域 cookie；

[0257] <url>：可以从认证会话中复制，并且可能源自于对流量管理 vServer 的初始请求。

[0258] ■域会话 cookie :

[0259] ● Cookie 名

[0260] ● Cookie 值 :< 认证会话索引 >

[0261] ●域 :< 流量管理 vServer 域 >

[0262] ●路径

[0263] ●到期时间 :< 值 / 未设置 / 默认 >

[0264] 请求 513

[0265] 请求 513 可以是由客户机 102 向 TM vServer 发送的。在一个实施例中,请求 513 可以是重定向的第二响应 522,带有或不带有对第二响应 522 的任何改变。在又一个实施例中,请求 513 大体上类似于请求 511。例如,请求 513 可包含来自请求 511 的信息以及认证信息。请求 513 可标识认证会话 567。在一些实施例中,请求 513 标识有效的认证会话 567。请求 513 可以在请求 513 的主体中、请求 513 的 POST 消息结构中、或者在请求 513 的头部或其他部分中包含认证会话标识符 546 或信息。

[0266] 先前的消息(请求或响应)之后的响应 521、522 和请求 512、513 的任何一个中可以包含在任意先前的消息中包含的任何信息。例如,响应 521 可包含在请求 511 中包含的全部或一些信息。在一些实施例中,任一随后的消息可以是任意先前的消息的修改或更新。例如,可以通过封装请求 512、修改请求 512 的头部或地址,和 / 或在请求 512 中添加新的信息来生成响应 522。而且,可以根据一个或多个流量管理、认证或其他策略从另一个消息生成和 / 或修改这些消息的每一个。

[0267] 系统 500 可以提供诸如 web 接口的接口。该接口可包括来自上文结合图 2A 所讨论的 GUI210、CLI212、壳服务 214 的任意实施例的特征。流量管理系统的管理员可以利用多个命令来安装和配置在本公开中所讨论的系统和方法。可以通过命令行接口来输入命令,例如上文结合图 2A 所描述的 CLI212。举例说明,在一些实施例中,对于各种功能,可以使用下列命令的一些或全部:

[0268] (a) 添加认证虚拟服务器:

[0269] add authentication vServer<vServer name>

[0270] <serviceType><IPAddress>[<port>]

[0271] ● <vServer name> : 认证虚拟服务器的名称。

[0272] ● <serviceType> : 服务的类型,例如,SSL。

[0273] ● <port> : 端口号,例如,443。

[0274] (b) 设置 / 注销 CR/CS/LB 虚拟服务器:

[0275] set/unset cr|cs|lb vServer<vServer name>

[0276] -authentication[on|off]

[0277] -authenticationURL< 认证 vServer 的 FQDN>[<port>]

[0278] ● <vServer name> : 认证虚拟服务器的名称。

[0279] ● -authentication[on|off] : 该开关能启用或禁用对于流量管理 vServer 的认证功能。

[0280] ● < 认证 vServer 的 FQDN> : 认证 vServer 的域名或 IP 地址。

[0281] ● <port> : 监听认证 vServer 的服务端口,其应该是与在认证 vServer 上指定的

端口相同的。端口号,例如,443。

- [0282] (c) 将策略绑定到认证虚拟服务器
- [0283] bind authentication vServer<vServer name>
- [0284] -policy<authNpolicy>|<sessionPolicy>
- [0285] (d) 将策略绑定到 CR/CS/LB 虚拟 vServer
- [0286] bind cr|cs|lb vServer<vServer name>
- [0287] -policy<auditPolicy>|<authorizationPolicy>...
- [0288] (e) 设置参数
- [0289] set tm sessionParameter
- [0290] set vpn parameter
- [0291] add/rm/set tm sessionPolicy/sessionAction
- [0292] add/rm/set vpn sessionPolicy/sessionAction
- [0293] set tm session parameter
 - [–sessTimeout<mins>]
 - [–defaultAuthorizationAction(ALLOW|DENY)]
 - [–authorization Group<string>]
 - [–homePage<URL>]
 - [–clientSecurity<expression>]
 - [–clientSecurityGroup<string>]
 - [–clientSecurityMessage<string>]]
 - [ssoCredential(PRIMARY|SECONDARY)]
 - [–loginScript<input_filename>][–logoutScript<input_filename>]
 - [–ntDomain<string>]
 - [–(pre)authenticationPolicy/(pre)authenticationActions<string>]
- [0305] set aaa param
 - [–sessTimeout<mins>]
 - [–defaultAuthorizationAction(ALLOW|DENY)]
 - [–authorization Group<string>]
 - [–homePage<URL>]
 - [–clientSecurity<expression>]
 - [–clientSecurityGroup<string>]
 - [–clientSecurityMessage<string>]]
 - [–ssoCredential(PRIMARY|SECONDARY)]
 - [–loginScript<input_filename>][–logoutScript<input_filename>]
 - [–ntDomain<string>]
 - [–(pre)authenticationPolicy/(pre)authenticationActions<string>]
- [0317] set aaa sessionparams
 - [–sessTimeout<mins>]
 - [–defaultAuthorizationAction(ALLOW|DENY)]

```
[0320]      [-authorization Group<string>]
[0321]      [-homePage<URL>]
[0322]      [-clientSecurity<expression>
[0323]      [-clientSecurityGroup<string>]
[0324]      [-clientSecurityMessage<string>]]
[0325]      [-ssoCredential (PRIMARY|SECONDARY)]
[0326]      [-loginScript<input_filename>][-logoutScript<input_filename>]
[0327]      [-ntDomain<string>]
[0328]          [- (pre) authenticationPolicy / (pre)
authenticationActions<string>]
[0329] { 定义 TM 会话的会话行为 }
[0330] set vpn param
[0331]      [-sessTimeout<mins>]
[0332]      [-defaultAuthorizationAction (ALLOW|DENY)]
[0333]      [-authorization Group<string>]
[0334]      [-homePage<URL>]
[0335]      [-clientSecurity<expression>]
[0336]      [-clientSecurityGroup<string>]
[0337]      [-clientSecurityMessage<string>]]
[0338]      [-ssoCredential (PRIMARY|SECONDARY)]
[0339]      [-loginScript<input_filename>][-logoutScript<input_filename>]
[0340]      [-ntDomain<string>]
[0341]          [- (pre) authenticationPolicy / (pre)
authenticationActions<string>]
[0342] { 定义 VPN 会话的会话行为 }
[0343] (f) 显示统计 :
[0344] show aaa session
[0345] { 显示会话和它们的统计,包括 VPN、流量管理和 / 或系统 }
[0346] 现参考图 6A 和 6B,显示了描述对由流量管理虚拟 vServer 管理的网络流量进行认证的方法的步骤的实施例的流程图 600。总的来说,在步骤 601,流量管理 vServer 接收来自客户机 102 的与服务器 106 建立连接的请求 511。请求 511 包括第一统一资源定位符 (URL) 545。在步骤 603,流量管理虚拟服务器确定客户机 102 是否已经被认证。在步骤 605,流量管理虚拟服务器识别用于从多个认证虚拟服务器 275av 中选择一个认证虚拟服务器 275av 的策略以便提供对客户机 102 的认证。在步骤 607,流量管理虚拟服务器通过该策略从多个认证虚拟服务器 275av 中选择一个认证虚拟服务器 275av。在步骤 609,流量管理虚拟服务器向客户机 102 传输对请求 511 的响应 521。响应 521 包括 URL 545 和重定向到认证虚拟服务器 275av 的指令 514。在步骤 611,响应 521 触发来自客户机 102 的、到认证虚拟服务器 275av 的请求 512。在步骤 613,认证虚拟服务器接收来自客户机 102 的请求 512。第二请求识别 URL 545 并指示从流量管理虚拟服务器的重定向。在步骤 615,认证虚拟服
```

务器为客户机 102 建立认证会话 567。该认证会话 567 识别一个或多个策略 568。在步骤 617, 认证虚拟服务器将 URL 545 和流量管理虚拟服务器 275tv 的域名与认证会话 567 存在一起。在步骤 619, 认证虚拟服务器对从客户机 102 接收的证书进行认证。在步骤 621, 流量管理虚拟服务器将认证会话 567 的一个或多个策略 568 应用到请求 511。在步骤 623, 认证虚拟服务器向客户机 102 传输响应 522 以将客户机 102 重定向到流量管理虚拟服务器。该响应 522 标识认证会话 567。在步骤 625, 流量管理虚拟服务器接收来自客户机 102 的请求 513。请求 513 包含认证会话 567 的标识符 546。在步骤 627, 流量管理虚拟服务器验证由该标识符 546 识别的认证会话 567。在步骤 629, 流量管理虚拟服务器将认证会话 567 的一个或多个策略 568 应用到请求 513。在步骤 631, 流量管理虚拟服务器将由一个或多个策略 568 授权的流量从客户机 102 转发到服务器 106。

[0347] 在步骤 601 的进一步的细节中, 流量管理 vServer 从客户机 102 接收与服务器 106 建立连接的请求 511。请求 511 可包括统一资源定位符 (URL) 545。在一些实施例中, 请求 511 是访问资源的请求。请求 511 可以是来自客户机的多个请求中的最初的请求 511, 并且可能包含或不包含 URL 545。流量管理 vServer 可通过在客户机 102 和服务器 106 或服务器群 582 之间的另一个中间设备 (例如设备 200) 接收请求 511。请求 511 可以被拦截和 / 或重定向到流量管理 vServer。请求 511 也可以被重定向和 / 或编址到执行流量管理 vServer 的设备 200 或服务器 106。在一些实施例中, 请求 511 中可以不编制到流量管理 vServer。可以根据一个或多个策略 (诸如来自流量管理策略 586 的策略) 将请求 511 定向到流量管理 vServer。此外, 可以经由上文结合图 4A-4E 描述的配置的任意实施例将请求 511 从一个或多个流量管理 vServer275tmv 输送、路由、重定向或委派到流量管理 vServer 275tv。

[0348] 在步骤 603 的进一步的细节中, 流量管理虚拟服务器确定客户机 102 是否已经被认证。流量管理 vServer 可以通过应用一个或多个策略, 例如来自与流量管理虚拟服务器关联的流量管理策略和 / 或认证策略 568 的策略, 来确定客户机 102 和 / 或用户是否已经被认证。在一些实施例中, 请求 511 可包含指示客户机 102 和 / 或用户是否是已认证的信息。特定信息的缺席也可能指示客户机 102 和 / 或用户是否是已认证的。流量管理 vServer 可确定该请求不包含诸如域会话 cookie 的会话 cookie。在一些实施例中, 流量管理 vServer 可确定该请求不包含对有效的认证会话的标识符或索引 546。在一个实施例中, 因为请求 511 不包含域会话 cookie 和 / 或对有效的认证会话的索引, 流量管理 vServer 可确定客户机 102 和 / 或用户没有被认证。请求 511 中的有效的域会话 cookie 和 / 或对有效的认证会话的索引可指示客户机 102 和 / 或用户是已认证的。在一个实施例中, 流量管理 vServer 检查请求 511 中所识别的或者通过会话域 cookie 所识别的认证会话是有效的或未过期的。在一些实施例中, 如果请求 511 包含有效的域会话 cookie 并且所关联的认证会话是有效的且未到期, 那么流量管理 vServer 确定客户机 102 和 / 或用户是已认证的。

[0349] 流量管理 vServer 也向客户机 102 请求信息。所请求的信息可用于确定客户机 102 和 / 或用户是否是已认证的。例如, 流量管理 vServer 可启动客户机 102 的端点分析扫描。在一些实施例中, 流量管理 vServer 可以向客户机 102 传输脚本和 / 或程序以收集信息, 或者执行脚本和 / 或程序以向客户机 102 轮询或请求信息。在一些实施例中, 流量管理 vServer 可传输和 / 或激活在客户机 102 中的收集代理 304 来为流量管理 vServer 收集信息。所收集的信息可以是上文结合收集代理 304 以及图 3A 和图 5 所讨论的任何类型或形

式的信息。流量管理 vServer 接着可以响应于接收和 / 或分析所收集的信息来确定客户机 102 是否已被认证。

[0350] 在一些实施例中，流量管理 vServer 可能不能够确定客户机 102 是否已经被认证。在这些实施例的一个中，流量管理 vServer 可以将客户机 102 看作是已认证的。在这些实施例的另一个中，流量管理 vServer 可以将客户机 102 看作是未被认证的。流量管理 vServer 可以通过应用诸如流量管理策略 586 和认证策略 568 的一个或多个策略来将客户机 102 看作是已认证的或未被认证的。取决于客户机 102 是否已经被认证，流量管理 vServer 可执行相同或不同的动作。可以通过应用一个或多个策略来确定动作。在一个实施例中，如果客户机 102 是已认证的，则该方法可转到步骤 621，在流量管理操作之前应用一个或多个认证策略 568。在又一个实施例中，如果客户机 102 是未被认证的，该方法转到步骤 605 以发起认证。

[0351] 在步骤 605，流量管理虚拟服务器识别用于从多个认证虚拟服务器选择一个认证虚拟服务器的策略以便执行对客户机 102 的认证。在选择认证 vServer 中可以选择和应用一个或多个策略，例如流量管理策略 586。在一些实施例中，可能仅有一个认证虚拟服务器是可用的，或者仅支持一个认证虚拟服务器，并且可能不要求识别该认证服务器的策略。在一个实施例中，请求 511 包含用于选择认证虚拟服务器的策略的信息。在又一个实施例中，请求 511 提供用于选择认证虚拟服务器的策略。在又一个实施例中，流量管理虚拟服务器部分地基于从客户机 102 收集的信息来识别该策略。而且，可以从流量管理策略 586、认证策略 568 或任何其他策略来识别该策略。通过策略引擎可以应用任意策略，所述策略引擎例如上文结合图 2A 所讨论的策略引擎 236 的任意实施例。

[0352] 在一个实施例中，流量管理虚拟服务器基于与请求关联的用户来识别选择认证 vServer 的策略。在又一个实施例中，流量管理虚拟服务器基于从客户机 102 收集的信息来识别选择认证 vServer 的策略。流量管理虚拟服务器可基于从客户机 102 收集的任何类型或形式的信息来识别策略。流量管理虚拟服务器可启动 EPA 来从客户机 102 收集用于识别策略的信息。流量管理虚拟服务器可以通过发送收集代理 304 到客户机 102 或者与位于客户机 102 的收集代理 304 通信来从客户机 102 接收用于识别策略的信息。在一个实施例中，流量管理虚拟服务器基于所收集的关于在客户机 102 上安装的软件的信息来识别用于选择认证 vServer 的策略。在又一个实施例中，流量管理虚拟服务器基于所收集的关于在客户机 102 上的操作系统的信息来识别用于选择认证 vServer 的策略。

[0353] 在一些实施例中，流量管理 vServer 可以经由所关联的策略引擎 236 来对与策略相关的任意动作进行操作。例如，在流量管理 vServer 中的或者与流量管理 vServer 通信的策略引擎 236 可以代表流量管理 vServer 来识别用于选择认证 vServer 的策略。

[0354] 在步骤 607 的进一步的细节中，流量管理 vServer 通过该策略选择多个认证 vServer 的一个认证 vServer 以认证客户机。响应于策略的识别，流量管理 vServer 选择认证 vServer。在一个实施例中，流量管理 vServer 从与该流量管理 vServer 关联的多个 vServer 中选择认证 vServer。在又一个实施例中，流量管理 vServer 从多个 vServer 中选择认证 vServer 作为第一类型的认证 vServer。流量管理 vServer 可基于由该认证 vServer 支持的认证类型来选择认证 vServer。例如，认证类型可包括活动目录 (AD)、轻量级目录访问协议 (LDAP)、RADIUS 和 RSA SecureID。流量管理 vServer 也可以基于由认证 vServer 提

供的认证类型所支持的特征（例如，SSO）和 / 或选项来选择认证 vServer。可以为由策略识别的特定的认证类型选择认证 vServer。流量管理 vServer 也可以基于与客户机 102 就任何类型的需求和 / 或选项的协商来选择认证 vServer。在一个实施例中，流量管理 vServer 基于与客户机 102 的对认证类型的协商来选择认证 vServer。可以从多个认证类型来协商认证类型。在一些实施例中，流量管理 vServer 基于由客户机支持的认证类型来选择认证 vServer。

[0355] 在一些实施例中，流量管理 vServer 可不应用任何策略就选择认证虚拟服务器。例如，流量管理 vServer 可以与上文结合图 4A 和 4B 所描述的认证 vServer 静态地相关联。在一个实施例中，请求 511 提供识别或选择认证 vServer 的信息。在又一个实施例中，流量管理 vServer 使用从客户机 102 收集的信息来识别或选择认证虚拟服务器。流量管理 vServer 选择一个或多个认证 vServer 来认证客户机 102 和 / 或用户。此外，一个或多个认证服务器 580 可以与每个所选择的认证 vServer 静态地或动态地相关联以便对客户机 102 和 / 或用户进行认证。在一些实施例中，通过应用例如来自认证策略 568 的一个或多个策略，可以进行动态的关联。

[0356] 在步骤 609 的进一步的细节中，流量管理虚拟服务器向客户机 102 传输对请求 511 的响应 521。流量管理虚拟服务器可以将包括 URL 545 和 / 或重定向到认证虚拟服务器的指令 514 的响应 521 传输到客户机 102。在一些实施例中，流量管理 vServer 可以经由隐藏的表单或字段来传输标识 URL 545 的响应 521。流量管理 vServer 也可以传输包括加载时提交事件句柄和 / 或用于在客户机 102 上显示和 / 或用户交互的页面或表单的响应 521。如果客户机 102 和 / 或用户未被认证或者如果不能确定客户机 102 和 / 或用户是已认证的，则流量管理 vServer 可传输响应 521。

[0357] 在一些实施例中，流量管理 vServer 通过任何类型或形式的修改、变换和 / 或转换将请求 511 转变为响应 521。在其他实施例中，流量管理 vServer 部分地基于请求 511 的内容来生成响应 521。也可以通过除了流量管理 vServer 之外的模块，例如设备 200 的组件，来生成和 / 或修改响应 521。此外，可以通过应用诸如来自流量管理策略和 / 或认证策略 568 的策略的一个或多个策略来生成和 / 或修改响应 521。在一些实施例中，响应 521 包括脚本 516，所述脚本 516 触发从客户机 102 向认证虚拟服务器传输请求 521。

[0358] 在一些实施例中，流量管理 vServer 可以通过网络引擎 240 来操作或执行任何动作。流量管理 vServer 也可以就任何这样的动作来指导网络引擎 240。例如，网络引擎 240 可生成和 / 或向客户机 102 传输响应 521 以重定向到所选择的认证 vServer。网络引擎 240 可以代表流量管理 vServer 生成包括客户机 102 重定向到所选择的认证 vServer 的指令的响应 521。

[0359] 在步骤 611，响应于响应 521 的接收，响应 521 触发从客户机 102 到认证虚拟服务器的请求 512。在一个实施例中，请求 512 是响应于收到响应 521 而被触发的。在又一个实施例中，请求 512 是由用户动作触发的，例如在客户机 102 上显示的提交按钮上的点击。客户机 102 可以接收被包含在触发请求 512 的响应 521 中的一个或多个命令、脚本和 / 或程序。客户机 102 也可以具有响应于响应 521 的接收来触发请求 512 的一个或多个脚本和 / 或程序。在一些实施例中，由客户机 102 接收的或在客户机 102 处可利用的一个或多个脚本和 / 或程序触发向认证虚拟服务器的 POST 请求 512 的传输。客户机 102 和 / 或一

个或多个脚本和 / 或程序也可以生成用于包含在请求 512 中的指针或 URL520。例如,在请求 512 是 POST 请求的情况下,指针或 URL520 可被包含在请求 512 的 POST 字段中。在一些实施例中,指针或 URL 指示到 CG I 可执行文件的路径。客户机 102 和 / 或一个或多个脚本和 / 或程序可以生成对用于包含在请求 512 中的 CGI 可执行脚本的一个或多个输入或值。请求 512 也可包含一个或多个命令、脚本和 / 或程序。在一些实施例中,客户机 102 将请求 512 传输到认证 vServer。请求 512 也可以例如通过设备 200 和 / 或流量管理 vServer 被路由或重定向到认证 vServer。

[0360] 在步骤 613 的进一步的细节中,认证虚拟服务器接收来自客户机 102 的请求 512,该请求 512 识别 URL 545 并指示从流量管理 vServer 的重定向。在一些实施例中,认证 vServer 接收到预定的 URL 和 / 或 URL 545 的、包括 POST 消息的请求 512。响应于收到请求 512,认证 vServer 可以从该请求 512 中提取指针或 URL520。认证 vServer 可以根据所提取的指针或 URL520 来检索或请求可执行文件。此外,认证 vServer 可以执行该可执行文件,无论有没有被包含在请求 512 中的输入或值。在又一个实施例中,认证 vServer 可以执行一个或多个命令、脚本和 / 或程序。所述一个或多个命令、脚本和 / 或程序可以被包含在请求 512 中或者认证 vServer 275av 中、从存储装置 560 中进行检索,或者是根据一个或多个认证策略 568 而生成的。而且,认证 vServer 可以根据一个或多个认证策略 568 来选择用于执行的一个或多个命令、脚本、程序和 / 或可执行文件。

[0361] 在一些实施例中,认证 vServer 在请求 512 中寻找 AAA cookie。如果 AAA cookie 是可利用的并且是有效的,那么认证 vServer 可转到步骤 615 或任何其他认证步骤。如果 AAA cookie 是不可用的或者是无效的,那么认证 vServer 可以确定请求 512 是否是属于特定类型的消息并且是有效的。在一些实施例中,认证 vServer 可确定请求 512 是否是 POST 消息。如果该消息是有效的,那么认证 vServer 可以依照步骤 615 进行处理。在一些实施例中,如果该消息是 POST 消息,则其是有效的。在这些实施例的一个中,如果认证 vServer 确定 POST 消息包含预定的 URL,例如“/cgi/tm”,则该消息是有效的。或者,如果该消息被确定为是无效的和 / 或不是 POST 消息,则认证 vServer 可以拒绝客户机请求。认证 vServer 可以通过发送任何类型和形式的消息来拒绝客户机请求。在一些实施例中,认证 vServer 通过 HTTP403 禁止消息或 503 服务不可用消息来拒绝客户机请求。在各种实施例中,认证 vServer 可以执行生成拒绝客户机请求的消息、将该消息发送到客户机 102 和关闭到客户机 102 的连接中的一个或多个步骤。

[0362] 在步骤 615 的进一步的细节中,认证虚拟服务器为客户机 102 建立认证会话 567。认证会话 567 可以识别一个或多个策略 568。由认证 vServer 建立的认证会话可以是 VPN 会话。在一些实施例中,认证 vServer 在认证客户机 102 和 / 或用户之前建立认证会话 567。在其他实施例中,认证 vServer 在对客户机 102 和 / 或用户进行认证时或者认证之后建立认证会话 567。认证 vServer 可以使用任何类型或形式的数据结构、对象或应用处理接口 (API) 来创建或建立认证会话 567。例如,认证 vServer 可以建立或创建会话表,例如在存储装置 560 中的 AAA-TM 会话表。认证 vServer 也可以创建和 / 或存储会话 cookie(例如 AAA 会话 cookie) 和 / 或与认证会话 567 关联的其他信息。在一些实施例中,认证 vServer 与服务器 106 或其他机器 102 通信或进行握手以便建立认证会话 567。可以由流量管理 vServer 基于客户机请求来识别服务器 106 或其他机器 102。在一些其他实施例中,认证 vServer 建

立认证会话 567 从而为连接到已被流量管理 vServer 识别的服务器 106 或其他机器 102 做准备。认证 vServer 也可以建立认证会话 567 从而为认证客户机 102 和 / 或用户做准备。

[0363] 在一些实施例中,可以通过执行由指针或 URL520 指示的可执行文件来建立认证会话 567。请求 512 可将诸如输入和值的信息传递到认证 vServer275av 以建立认证会话 567。通过执行在请求 512 中接收的、驻留在认证 vServer 275av 中的、从存储装置 560 中检索的,或者根据一个或多个认证策略 568 而生成的一个或多个命令、脚本和 / 或程序也可以建立认证会话 567。

[0364] 在步骤 617,认证虚拟服务器将 URL 545 和流量管理虚拟服务器 275tv 的域名与认证会话 567 存在一起。认证 vServer 可以存储 URL 545 和与认证会话 567 关联的流量管理虚拟服务器的域名的其中一个或两者。此外,认证 vServer 可存储来自请求 512 或其他的、与认证会话 567 关联的任何类型或形式的信息。认证 vServer 275av 可以响应于收到请求 512 来存储这些信息的任何内容。认证 vServer 275av 可以响应于应用一个或多个策略(例如来自认证策略 568 的策略)来存储这些信息的任何内容。此外,认证 vServer275av 可以通过执行由指针或 URL520 指示的可执行文件来存储这些信息的任何内容。认证会话 567 也可以通过执行在请求 512 中包含的、驻留在认证 vServer 275av 中的、从存储装置 560 中检索的,或者根据一个或多个认证策略 568 而生成的一个或多个命令、脚本和 / 或程序来存储这些信息中的任何内容。

[0365] 认证 vServer 可存储与客户机请求、客户机 102、用户和 / 或上文结合图 5 所描述的系统 500 的任何其他组件相关联的任何信息。可将这些信息存储在存储装置 560 中,或者网络 104 上的一个或多个存储装置之间。在一些实施例中,认证会话 567 将这些信息的一些或全部存储在会话表中,例如 AAA-TM 会话表。认证 vServer 275av 可以向任何存储装置传输或传送这些信息以用于存储。

[0366] 在步骤 619 的进一步的细节中,认证虚拟服务器认证从客户机 102 接收的证书。认证 vServer 可以根据由认证 vServer 使用或配置的认证类型(例如,LDAP、RADIUS)来进行认证。认证 vServer 也可以与任何类型或形式的服务器或系统通信来执行该类型的认证。例如,在一些实施例中,认证 vServer 可以执行由绑定到或分配给认证 vServer 的一个或多个认证和 / 或授权服务器 580 支持的类型的认证。此外,认证 vServer 可根据由流量管理 vServer 和 / 或一个或多个策略识别的认证类型来进行认证。认证 vServer 也可以使用任何常规的、私有的和 / 或定制的认证技术和过程来执行客户机 102 和 / 或用户的认证。认证 vServer 可以响应于收到请求 512 来执行认证。认证 vServer 也可以响应于应用一个或多个策略(例如来自认证策略 568 的策略)来执行认证。此外,认证 vServer 可以通过执行由指针或 URL520 识别的可执行文件来进行认证。认证会话 567 也可以通过执行在请求 512 中包含的、在认证 vServer 中的、从存储装置 560 中检索的,或者根据一个或多个认证策略 568 而生成的一个或多个命令、脚本和 / 或程序来进行认证。

[0367] 认证 vServer 可识别或提取客户机证书 518 和 / 或来自请求 512 的任何类型或形式的信息。而且,认证 vServer 275av 可以从客户机 102 和 / 或用户请求和 / 或收集任何类型或形式的认证和 / 或授权信息。该信息可包括用户标识、密码、对质问问题的回答、认证密钥、会话表索引和会话 cookie 中的一个或多个。可以在与客户机上的密码管理器、会话表和 / 或数据库(例如,在存储装置 560 和 / 或 RADIUS 服务器中维护的)和用户输入中的

一个或多个的通信中来收集该信息。认证 vServer 可启动客户机 102 的端点分析或扫描。在一些实施例中,认证 vServer 可以向客户机 102 传输脚本和 / 或程序以收集信息,或者可执行脚本和 / 或程序以向客户机 102 轮询或请求信息。在一个实施例中,收集代理 304 为认证 vServer 收集信息。认证 vServer 也可以执行任何类型或形式的预认证动作。在一些实施例中,可以根据一个或多个认证策略 568 来进行预认证动作。

[0368] 在一些实施例中,认证 vServer 将客户机 102 或客户机请求重定向到登录页面或其他网页。可以使用 HTTP 302 消息或任何其他类型的消息来发起该重定向。在一些实施例中,认证 vServer 生成重定向消息并将其传输到客户机 102。在一个实施例中,认证 vServer 275av 通过指针或 URL(例如,“/vpn/index.html”)将客户机 102 或客户机请求重定向到页面。在一些实施例中,可以通过访问页面来执行一些或全部的预认证动作。该页面可以驻留在认证 vServer、存储装置 560 或上文结合图 5 所描述的系统 500 的任何其他组件中,或者可以由认证 vServer、存储装置 560 或上文结合图 5 所描述的系统 500 的任何其他组件来提供该页面。在其他实施例中,认证 vServer 给客户机 102 发送或提供页面或消息以发起认证。

[0369] 响应于收到重定向消息,客户机 102 可以向认证服务器发送重定向请求。在一个实施例中,客户机发送包括“GET/vpn/index.html”命令的重定向请求。响应于该重定向请求,认证服务器可以发送包括页面(例如登录页面)的响应。客户机 102 可以将证书和 / 或其他信息输入到该页面并通过该页面向认证服务器发送登录请求。认证 vServer 可接收并处理该登录请求。在一些实施例中,认证 vServer 275av 尝试本地或者远程地对客户机 102 和 / 或用户进行认证。例如,在一个实施例中,认证 vServer 275av 通过应用一个或多个认证策略和 / 或使用在存储装置 560 中存储的认证信息来本地执行认证。在又一个实施例中,认证 vServer 通过将客户机和 / 或用户信息传输到一个或多个远程认证服务器 580 来执行认证。可以部分地基于认证配置的类型或形式、和 / 或一个或多个认证策略 568 的应用来选择远程认证和 / 或本地认证。

[0370] 如果认证不成功,例如,如果认证步骤(615、617 和 619)的任何一个不成功,则客户机请求将被拒绝、忽略,或者重新执行认证,其中重新执行认证可以有或没有另外的步骤。认证 vServer 可以通过向客户机 102 发送任何类型和形式的消息来拒绝客户机请求。在一些实施例中,认证 vServer 通过 HTTP403 消息来拒绝客户机请求。在一些实施例中,如果在诸如步骤 615、617 和 619 的认证步骤的任何一个中的认证不成功,则认证 vServer 可以执行生成拒绝客户机请求的消息、将该消息发送到客户机 102 和关闭到客户机 102 的连接中的一个或多个步骤。认证 vServer 可终止认证会话 567,如果有的话。此外,认证 vServer 275av 可从存储装置中删除所存储的流量管理 vServer 275tv 的域名和 / 或 URL 545。

[0371] 如果认证是成功的,则认证 vServer 可为该流量管理会话设置域会话 cookie。在一些实施例中,一旦成功认证,该方法可转到步骤 623 或 621。

[0372] 在步骤 621 的进一步的细节中,流量管理虚拟服务器或认证虚拟服务器将认证会话 567 的一个或多个策略应用于请求。在一些实施例中,该步骤在流量管理 vServer 已经确定客户机 102 和 / 或用户已经被认证之后发生。也可以在由认证 vServer 成功认证客户机 102 和 / 或用户后进行该步骤。在一些实施例中,流量管理 vServer 将客户机请求传输

或者重定向到认证 vServer。流量管理 vServer 或认证虚拟 vServer 可以将一个或多个策略（例如来自认证策略 568 的策略）应用于客户机请求。流量管理 vServer 或认证虚拟 vServer 可以在诸如请求 511 的客户机消息上，或者在（例如，来自存储装置 560 的）所存储的与客户机请求相关联的信息上应用一个或多个策略。流量管理 vServer 或认证虚拟服务器可以识别与已认证的客户机 102 和 / 或用户相关联的认证会话 567。此外，可以由与流量管理 vServer 相关联的认证 vServer 来识别认证会话 567 和 / 或一个或多个策略。

[0373] 在步骤 623，认证虚拟服务器向客户机 102 传输响应以便将客户机 102 重定向到流量管理虚拟服务器。在一些实施例中，认证 vServer 用上文结合图 5 所描述的响应 522 来生成并传输响应。认证 vServer 可以将流量管理会话的会话 cookie 插入到响应 522 中。而且，认证 vServer 可以将关于认证会话 567 的标识符 546 或信息插入到响应 522 中。认证 vServer 可将关于认证会话 567 的标识符 546 或信息插入到在响应中所包含的会话 cookie（例如，域会话 cookie）。认证 vServer 可以将标识认证会话 567 的响应 522 发送到客户机 102。在一些实施例中，认证 vServer 将响应 522 作为重定向消息（例如，HTTP 302 消息）传输到客户机 102 以将客户机请求重定向到流量管理 vServer。此外，认证 vServer 可以在发送响应 522 后终止它与客户机 102 的连接。

[0374] 在步骤 625 的进一步的细节中，流量管理虚拟服务器接收来自客户机 102 的另一个请求 513。请求 513 可包含认证会话 567 的标识符或索引 546。客户机 102 可以响应于收到响应 522 来生成请求 513。客户机 102 可从响应 522 中提取标识符 546 或关于认证会话 567 的信息，并将标识符 546 或关于认证会话 567 的信息插入到请求 513 中。在一些实施例中，客户机 102 将响应 522 进行修改或以其他方式处理到请求 513 中。客户机 102 可以将请求 513 直接传输到流量管理 vServer，或者直接传输到用于重定向到流量管理 vServer 的设备 200。在一些实施例中，客户机 102 可以通过在客户机 102 上执行的或代表客户机 102 执行的一个或多个应用来执行任何动作，诸如处理响应和生成请求。这些动作中的任何动作的执行可以是自动化的和 / 或包括用户交互。由客户机发送的请求可以是用于例如经由应用的使用来访问服务器的任何类型的请求。

[0375] 在步骤 627 的进一步的细节中，流量管理虚拟服务器验证由索引或标识符 546 识别的认证会话 567。流量管理 vServer 可以从请求 513 中提取或识别索引 546 或关于认证会话 567 的信息。在一些实施例中，流量管理 vServer 使用该索引 546 或信息来识别认证会话 567。此外，流量管理 vServer 可以验证该认证会话标识符 546 或信息。在一些实施例中，流量管理 vServer 使用该标识符 546 或信息识别认证会话的一个或多个策略。流量管理 vServer 可以通过使用在存储装置 560 中存储的信息、从客户机 102 收集的信息，以及 / 或者应用来自所关联的流量管理策略 586 和 / 或认证策略 568 的一个或多个策略来执行该验证。流量管理 vServer 可以验证认证会话 567 仍是活动的和 / 或就客户机 102 和 / 或用户而言是已认证的。

[0376] 在一些实施例中，流量管理 vServer 不验证认证会话 567。响应于验证认证会话 567 的失败，流量管理或认证 vServer 可以通过向客户机 102 发送任何类型和形式的消息来拒绝客户机请求。在一些实施例中，流量管理或认证 vServer 通过 HTTP403 消息来拒绝客户机请求。流量管理或认证 vServer 可以执行生成拒绝客户机请求的消息、将该消息发送到客户机 102 和关闭到客户机 102 的连接中的一个或多个步骤。流量管理或认证 vServer

可以终止认证会话 567。此外，流量管理或认证 vServer 可以从存储装置 560 中删除所存储的流量管理 vServer 的域名和 / 或 URL 545。流量管理或认证 vServer 也可以（例如从存储装置 560）更新和 / 或删除一个或多个会话表，例如 AAA-TM 会话表。

[0377] 在一些实施例中，流量管理 vServer 可以使用经过验证的认证会话 567 来执行 EPA 和 / 或获得客户机 102 和 / 或用户信息。例如，在认证时，流量管理 vServer 可使用认证会话 567 来自动地和 / 或安全地收集客户机 102 和 / 或用户信息。在一些实施例中，流量管理 vServer 使用认证会话 567 来识别一个或多个策略 586、568。对于经过流量管理 vServer 的任何通信，流量管理 vServer 可以使用关于客户机或从认证 vServer 可用的会话的任何信息，例如任何收集的端点信息。在一些实施例中，可以从经由认证 vServer（例如经由已认证的会话）可用的任何数据、值或信息中获得或导出策略表达式的任一部分的值。在一些实施例中，对策略的条件、动作或规则的输入可以是来自由认证 vServer 所存储的端点收集的信息的值。

[0378] 这样，流量管理 vServer 可使用端点或认证会话信息来为任一请求定向流量。例如，在经过流量管理 vServer 的应用流量的通信中，流量管理 vServer 可使用端点或已认证的会话信息来基于请求做出流量控制决策。例如，如果客户机有或没有软件，那么流量管理 vServer 可做出特定的流量管理决策。如果客户机是由特定类型的认证而不是另一类型的认证所认证的，则流量管理 vServer 也可做出特定的流量管理决策。

[0379] 在步骤 629，流量管理虚拟服务器将认证会话 567 的一个或多个策略 586、568 应用于请求 513。流量管理 vServer 可以应用一个或多个策略 586、568，例如来验证 URL 545、将 URL 545 与认证会话 567 相关联，或者为客户机 102 确定资源或服务器 106。在一些实施例中，流量管理 vServer 可以将认证会话的一个或多个策略的授权策略应用于请求 513。流量管理 vServer 可以应用授权策略来识别来自自己认证的客户机 102 的授权的流量。在一些其他实施例中，流量管理 vServer 可以将认证会话的一个或多个策略的流量管理策略应用于请求 513。流量管理策略可以确定与授权的客户机 102 相关联的流量是加密的和 / 或压缩的。

[0380] 流量管理 vServer 可以为客户机 102 应用一个或多个策略 586、568 来将 URL 545 验证为指向资源或服务器 106 的指针。流量管理 vServer 也可以将一个或多个策略 586、568 应用于来自自己认证的客户机 102 和 / 或用户的至少一些随后的请求以验证这些请求。一旦经过一个或多个策略 586、568 的验证，这些请求就成为授权的流量的部分。

[0381] 在步骤 631，流量管理虚拟服务器将由一个或多个策略 586、568 授权的流量从客户机 102 转发到服务器 106。可以由 URL 545、由流量管理 vServer，或者通过应用一个或多个策略 586、568 来识别服务器 106。在一些实施例中，流量管理 vServer 将由一个或多个策略 568 验证的请求从客户机 102 转发到服务器 106。在一个实施例中，流量管理 vServer 可以将授权的流量或经验证的请求转发到服务 270 或服务器 106。在又一个实施例中，流量管理 vServer 可以经由一个或多个流量管理会话来转发授权的流量或经验证的请求。在一些实施例中，认证会话可以持续到流量管理会话被终止为止。在其他实施例中，在流量管理会话期间可以创建和 / 或终止多个认证会话，例如以便验证或授权部分流量。

[0382] 在各种实施例中，一个或多个步骤可以是可选的、必须的和 / 或被重排序，而不限于所描述的方法。

[0383] 在一个实施例中,方法 600 包括流量管理虚拟服务器,其从访问服务器的客户机请求确定客户机 102 尚未被认证,所述请求包括 URL 545(步骤 603),向客户机 102 传输对请求 511 的响应 521,所述响应 521 包括 URL 545 和重定向到认证虚拟服务器的指令(步骤 609),由认证虚拟服务器接收来自客户机 102 的请求 512,该第二请求识别 URL 545(步骤 613),对从客户机收到的证书进行认证,为客户机建立认证会话,所述认证会话识别一个或多个策略(步骤 619),向客户机 102 传输响应 522 以便将客户机 102 经由 URL 545 重定向到流量管理虚拟服务器,所述响应 522 识别认证会话 567(步骤 623),以及由流量管理虚拟服务器 275tv 接收来自客户机 102 的请求 513,请求 513 包括认证会话 567 的标识符 546(步骤 625)。

[0384] 在又一个实施例中,方法 600 包括由流量管理虚拟服务器从自客户机 102 的接收的访问服务器 106 的内容的请求 511 确定客户机 102 尚未被认证(步骤 603),识别用于从多个认证虚拟服务器选择一个认证虚拟服务器的策略以提供对客户机 102 的认证(步骤 605),通过该策略选择多个认证虚拟服务器的一个认证虚拟服务器以认证客户机 102(步骤 607),以及向客户机 102 传输对请求 511 的响应,所述响应 521 包括重定向到所选择的认证虚拟服务器 275av 的指令(步骤 609)。

[0385] 在又一个实施例中,方法 600 包括流量管理虚拟服务器,其从客户机 102 接收与服务器 106 建立连接的请求 511(步骤 601),确定客户机 102 已被认证(步骤 603),将该请求转发到认证 vServer 以便将认证会话 567 的一个或多个策略应用于请求 511(步骤 621),认证 vServer 向客户机 102 传输响应 522 以便将客户机 102 重定向到流量管理虚拟服务器(步骤 623),流量管理虚拟服务器接收来自客户机 102 的请求 513(步骤 625),验证由标识符 546 识别的认证会话 567(步骤 627),将该认证会话 567 的一个或多个策略 568 应用于请求 513(步骤 629),以及经由认证会话 567 将由一个或多个策略 568 授权的流量从客户机 102 转发到由 URL 545 识别的服务器(步骤 631)。

[0386] 现参考图 7A,描述了给流量管理提供 AAA 支持的方法的又一个实施例。在进一步的细节中,图 7A 示出了其中是在与一个或多个认证 vServer 通信的流量管理 vServer 处对流量进行处理的实施例。图 7A 的步骤可代表方法 600 的步骤的一部分。简而言之,流量管理虚拟服务器接收来自客户机 102 的、与服务器 106 建立连接的请求 511(步骤 601),在请求 511 中寻找会话 cookie 以确定客户机 102 是否已经被认证(步骤 603),如果该 cookie 以及其识别的认证会话都是有效的,则将该请求转发到认证 vServer 以应用认证策略(步骤 621),由认证 vServer 重定向回到流量管理虚拟服务器(步骤 623)。如果 cookie 和 / 或其识别的认证会话是无效的,则流量管理 vServer 识别认证 vServer 以认证该客户机并将客户机请求重定向到该认证 vServer(步骤 605),上文结合图 6A 和 6B 讨论了每个步骤的细节。

[0387] 现参考图 7B,仍描述了给流量管理提供 AAA 支持的方法的又一个实施例。在进一步的细节中,图 7B 示出了其中客户机请求是在与流量管理 vServer 关联的认证 vServer 处进行处理的。图 7A 的步骤可代表方法 600 的步骤的一部分。上文结合图 6A 和 6B 描述了每个步骤的细节。简而言之,认证 vServer 接收来自客户机 102 的请求 512 并且在该请求 512 中寻找 AAAcookie(步骤 613)。如果该 cookie 是可用的并且是有效的,则认证 vServer 对客户机 102 执行认证(步骤 615-619)。如果认证成功,则认证 vServer 将客户机请求重

定向回到流量管理虚拟服务器（步骤 623）。如果认证失败，客户机请求被拒绝。另一方面，如果该 cookie 是不可用的或无效的，则认证 vServer 确定请求 512 是否是有效的 POST 消息（步骤 613）。如果请求 512 是有效的 POST 消息，则建立认证会话 567 并执行认证（步骤 615–619）。如果请求 512 不是有效的 POST 消息，则客户机请求被拒绝。上文结合图 6A 和 6B 描述了每个步骤的细节。

[0388] 现参考图 8，示出了将端点审计用于流量管理的方法的步骤的实施例的流程图 800。简而言之，在步骤 801，中间设备 200 的认证虚拟服务器确定对客户机 102 的端点分析扫描的结果。在步骤 803，流量管理虚拟服务器从认证虚拟服务器获得该结果。在步骤 805，流量管理虚拟服务器将该结果应用于一个或多个流量管理策略 586 以管理经过该中间设备 200 的客户机 102 连接的网络流量。

[0389] 在步骤 801 的进一步的细节中，中间设备 200 的认证虚拟服务器确定对客户机 102 的端点分析扫描的结果。分配给或绑定到认证 vServer 的一个或多个认证和 / 或授权服务器 580 可代表认证 vServer 来确定端点分析扫描的结果。在一些实施例中，认证 vServer 响应于事件来启动对客户机 102 的端点分析扫描。该事件可以是任何类型和形式的事件，例如收到客户机请求或客户机流量、客户机 102 的属性的改变、服务水平的改变或网络中断。该事件也可以是来自流量管理 vServer 或不同的 AAA vServer（例如审计 vServer）的请求。在一些其他实施例中，认证 vServer 基于预定频率来启动端点分析扫描。用于启动端点分析扫描的预定频率可以根据调度表来运行。可以基于过去的历史，例如网络流量和 / 或客户机请求的过去的历史，来预先确定该频率。也可以通过例如在过去的历史上应用一个或多个策略和 / 或公式来预先确定该频率。此外，可基于审计 / 记账需要来预先确定该频率。在一些实施例中，该频率是在数据库和 / 或会话表中进行存储和 / 或维护的。数据库和 / 或会话表驻留于网络 104 中的一个或多个存储装置（例如，存储装置 560）中。

[0390] 在一些实施例中，认证 vServer 可以向客户机 102 传输脚本和 / 或程序以执行端点分析扫描，或者执行脚本和 / 或程序以向客户机 102 轮询或请求信息。在一个实施例中，收集代理 304 为认证 vServer 收集信息。认证 vServer 和 / 或流量管理 vServer 可将收集代理 304 发送到客户机 304 以便执行端点分析扫描。端点分析扫描可作为认证 vServer 的一个或多个 AAA 动作的部分（例如，预先认证动作）而被启动。端点分析扫描也可以作为流量管理 vServer 的一个或多个流量管理动作的部分而被启动。此外，流量管理 vServer 或认证 vServer 可响应于一个或多个策略 586、568 的应用来启动端点分析扫描。

[0391] 认证 vServer 接收端点分析扫描的结果，其可包括任何类型或形式的客户机信息。在一些实施例中，该结果包括表达式，该表达式可包括任何类型或形式的字符串、等式、列表或命令。认证 vServer 可接收由客户机 102 求值的一个或多个表达式。所接收的一个或多个表达式可识别客户机 102 的一个或多个属性。该结果可识别下列的一个或多个在客户机 102 上的存在：操作系统的版本、操作系统的服务包、正在运行的服务、正在运行的进程、和文件。该结果也可识别下列的存在或版本的一个或多个在客户机 102 上的存在：反病毒软件、个人防火墙软件、反垃圾邮件软件和互联网安全软件。

[0392] 在一些实施例中，收集代理 304 可将结果传输到认证 vServer 和 / 或流量管理 vServer。在一些其他实施例中，传输到客户机 102 的脚本和 / 或程序可以在客户机 102 上执行并将结果传输到认证 vServer 和 / 或流量管理 vServer。客户机 102、所接收的脚本或

所接收的程序可以将包含所收集的结果的收集代理 304 传输回到认证 vServer。在其他实施例中，客户机 102 将结果传输到认证 vServer 和 / 或流量管理 vServer。客户机 102 也可以将结果发送到设备 200 或中间设备 200，以便被重定向到认证 vServer 和 / 或流量管理 vServer。可以根据客户机 102 的通信协议或者在从客户机 102 发出之前，对结果进行加密、压缩、格式化和 / 或以其他方式进行处理。在认证 vServer 和 / 或流量管理 vServer 处收到这些结果后，可以对这些结果进行处理以提取任何需要的信息。此外，认证 vServer 可根据一个或多个 AAA 或认证策略 586 来处理和 / 或评价这些结果。

[0393] 在步骤 803 的进一步的细节中，流量管理虚拟服务器从认证虚拟服务器获得该结果。流量管理 vServer 可根据另一个预定的频率来接收该结果。该频率可大体上类似于、或包括上文结合步骤 801 所描述的频率的任何实施例。在一些实施例中，该频率是由认证 vServer 和 / 或一个或多个认证策略来预先确定的。在一个实施例中，认证 vServer 将全部或部分结果转发到流量管理 vServer。认证 vServer 可在向流量管理 vServer 转发之前处理全部或部分结果。在一些实施例中，认证 vServer 向流量管理 vServer 提供对标识客户机 102 的一个或多个属性的一个或多个表达式的求值。认证 vServer 可根据一个或多个 AAA 或认证策略 586 来转发全部或部分结果。认证 vServer 也可以将全部或部分结果提供为对流量管理 vServer 的一个或多个流量管理策略 586 的输入。

[0394] 在步骤 805 的进一步的细节中，流量管理虚拟服务器将该结果应用于一个或多个流量管理策略 586 以管理经过中间设备 200 的客户机 102 的连接的网络流量。流量管理 vServer 可根据另一个预定的频率来应用该结果。该频率可大体上类似于、或包括上文结合步骤 803 所描述的频率的任何实施例。流量管理 vServer 可以将来自认证 vServer 的全部或部分结果应用于一个或多个流量管理策略 586。流量管理 vServer 也可以在应用策略 586 之前对来自认证 vServer 的全部或部分结果进行进一步的处理。

[0395] 流量管理 vServer 可基于对使用该结果的一个或多个流量管理策略 586 的应用来确定对于连接的压缩类型。而且，流量管理 vServer 可基于对使用该结果的一个或多个流量管理策略 586 的应用来确定对于连接的加密类型。流量管理 vServer 也可以基于对使用该结果的一个或多个流量管理策略 586 的应用来确定对于连接的一个或多个文件类型关联。此外，流量管理 vServer 可以基于通过一个或多个流量管理策略应用该结果来确定对于连接是否使用单点登录。基于所述确定，流量管理 vServer 可作出一个或多个流量管理和 / 或 AAA 决策以管理来自客户机 102 的经过中间设备 200 的流量。

[0396] 在一些实施例中，方法 800 可以与图 6A 和 6B 的方法 600 联合运用。例如，方法 800 的实施例可以作为方法 600 的步骤 607 或 629 的部分而被实现。

[0397] 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或可执行指令而被提供。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。软件程序或可执行指令可以作为目标代码被存储在一件或多件产品上或其中。

[0398] 尽管已经参考特定的实施例具体地显示和描述了本发明，但本领域技术人员应理

解在不脱离由如下的权利要求限定的本发明的精神和范围的情况下,可以进行形式和细节上的各种变化。

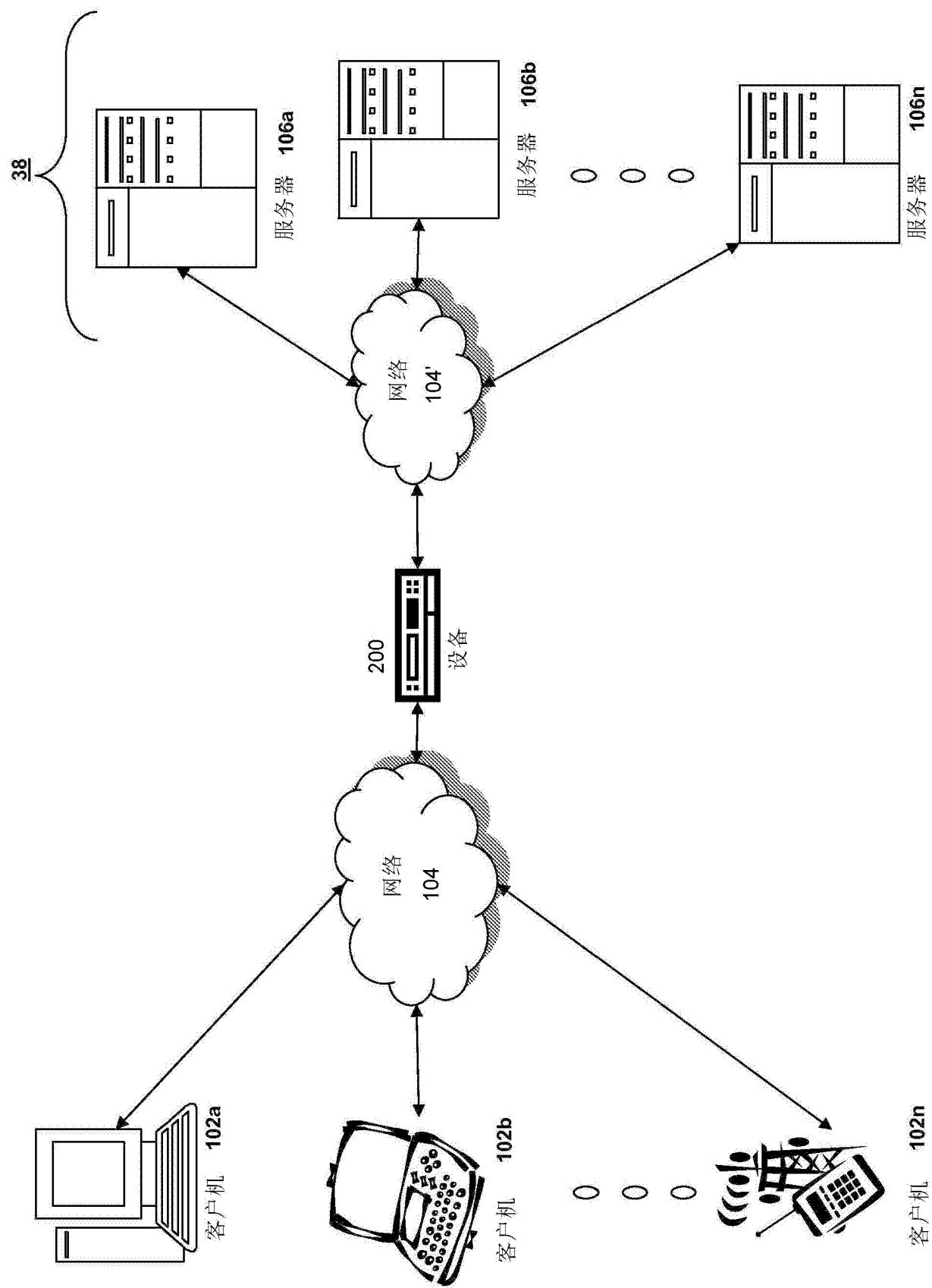


图 1A

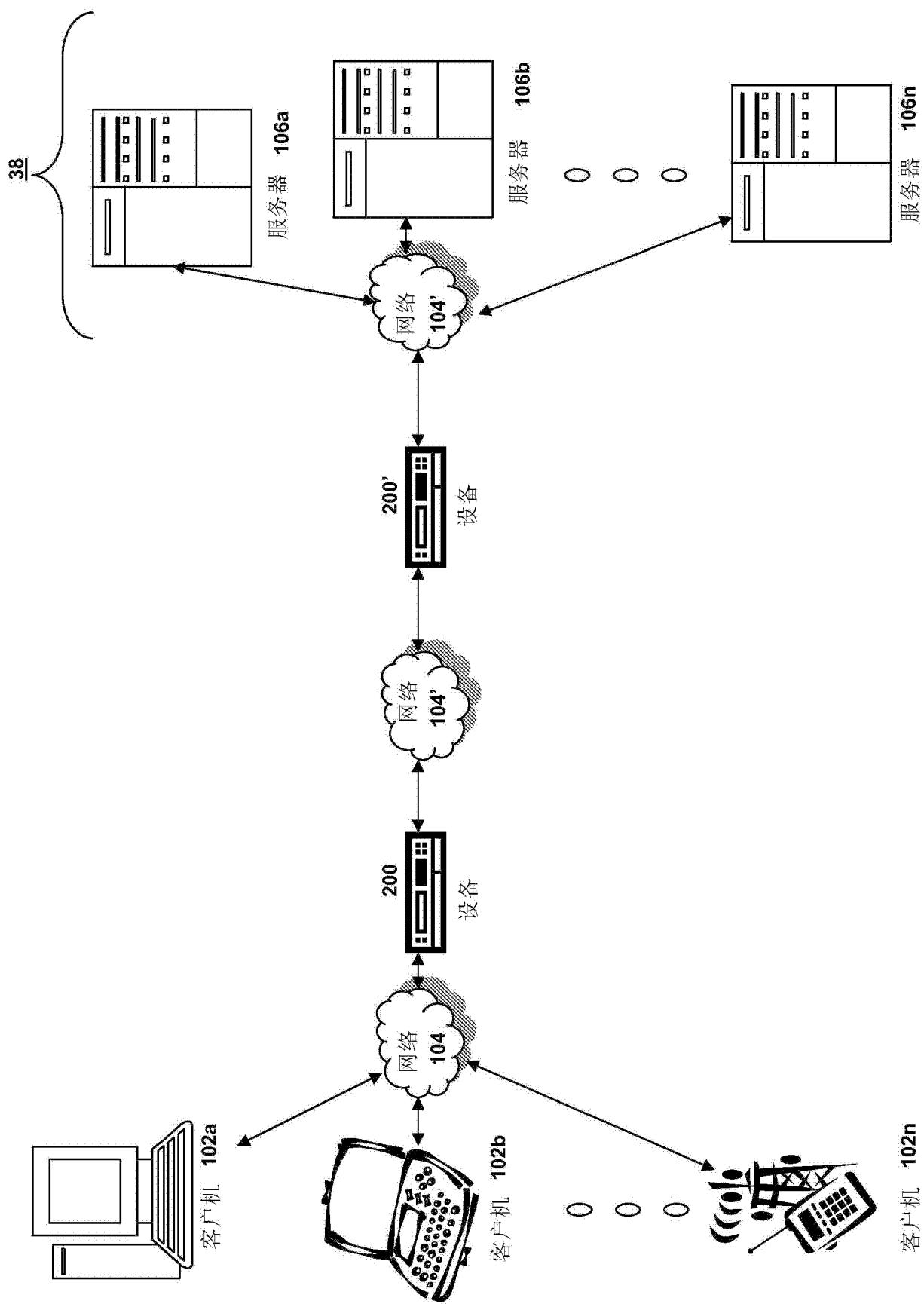


图 1B

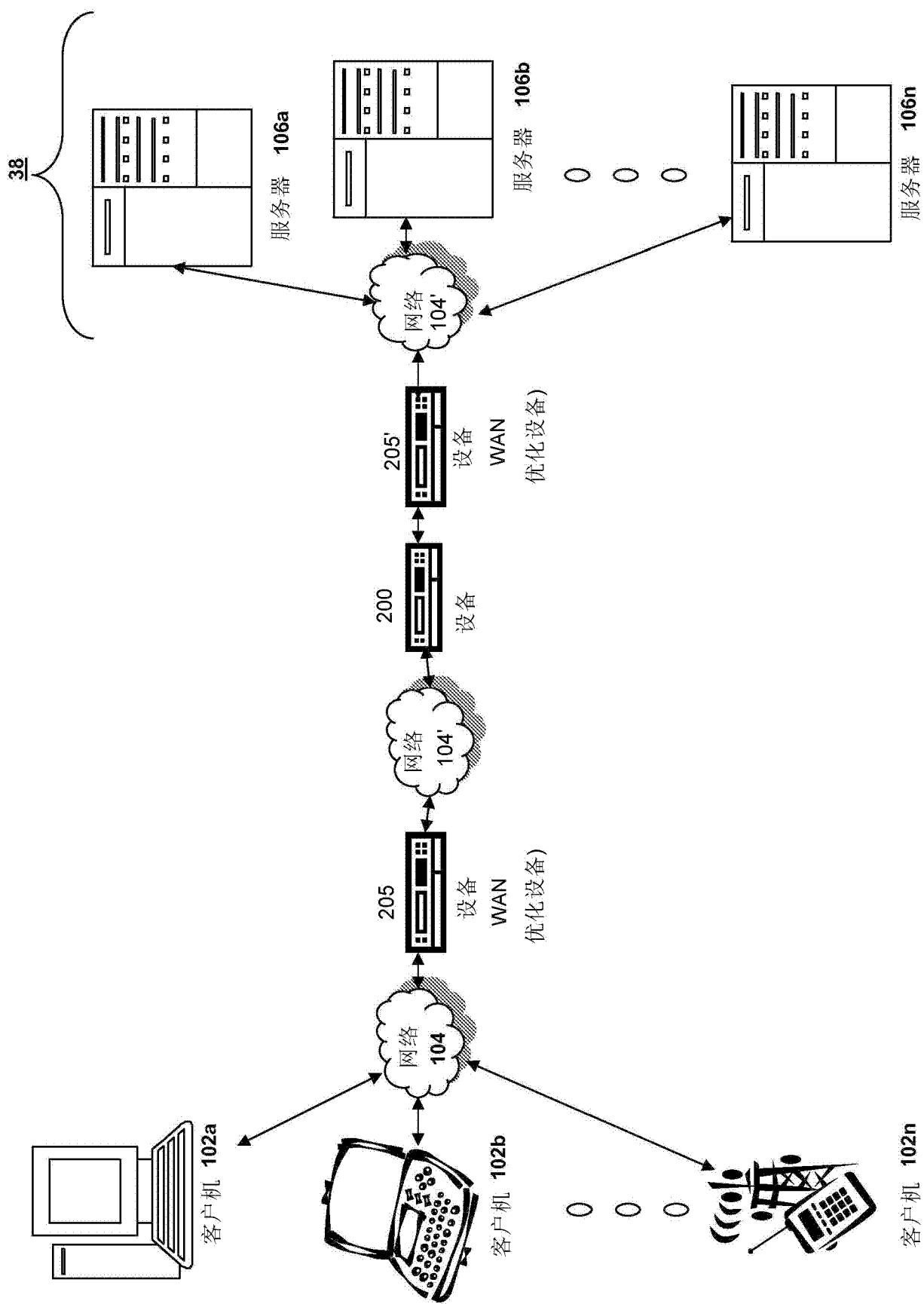


图 1C

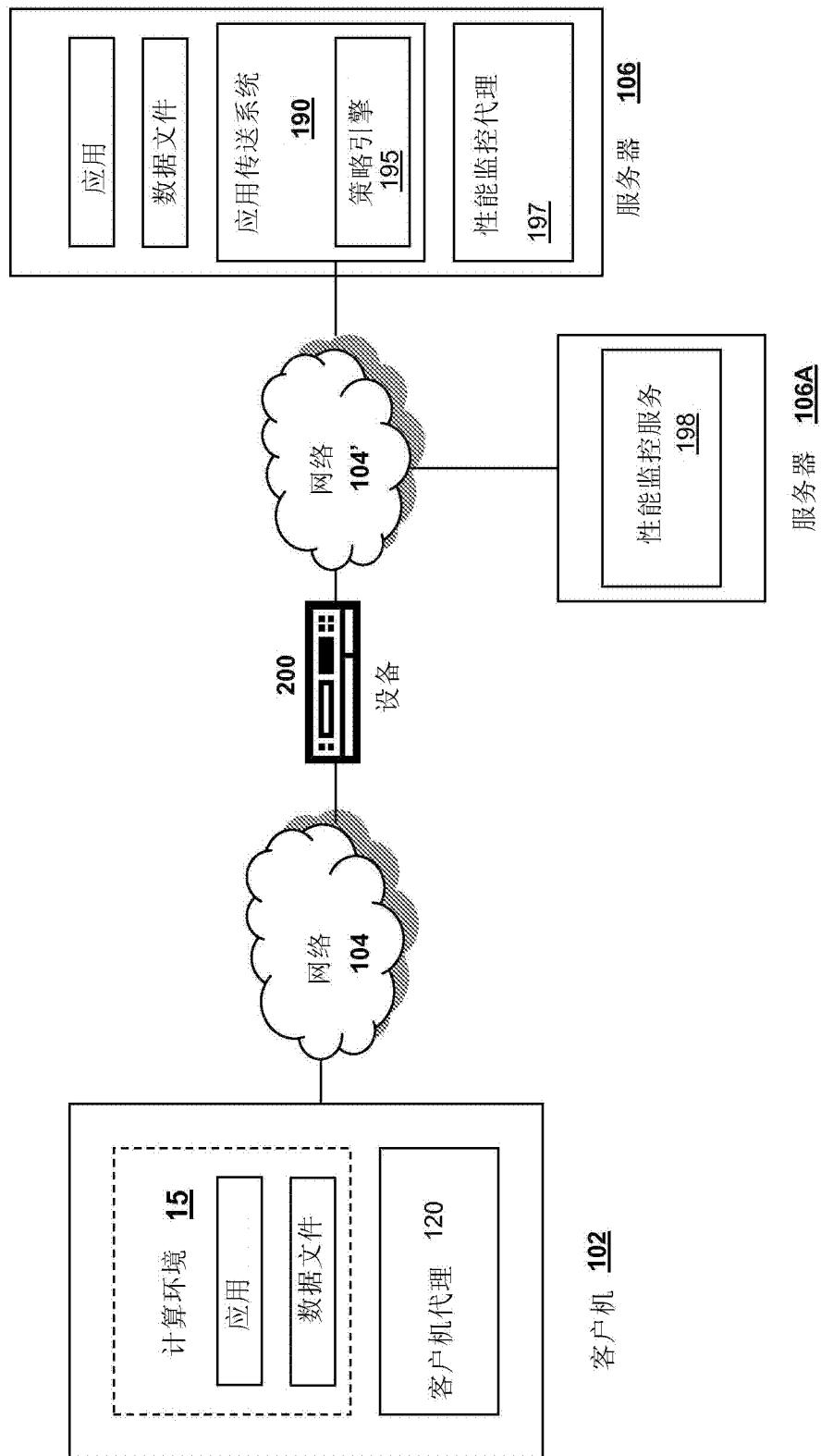


图 1D

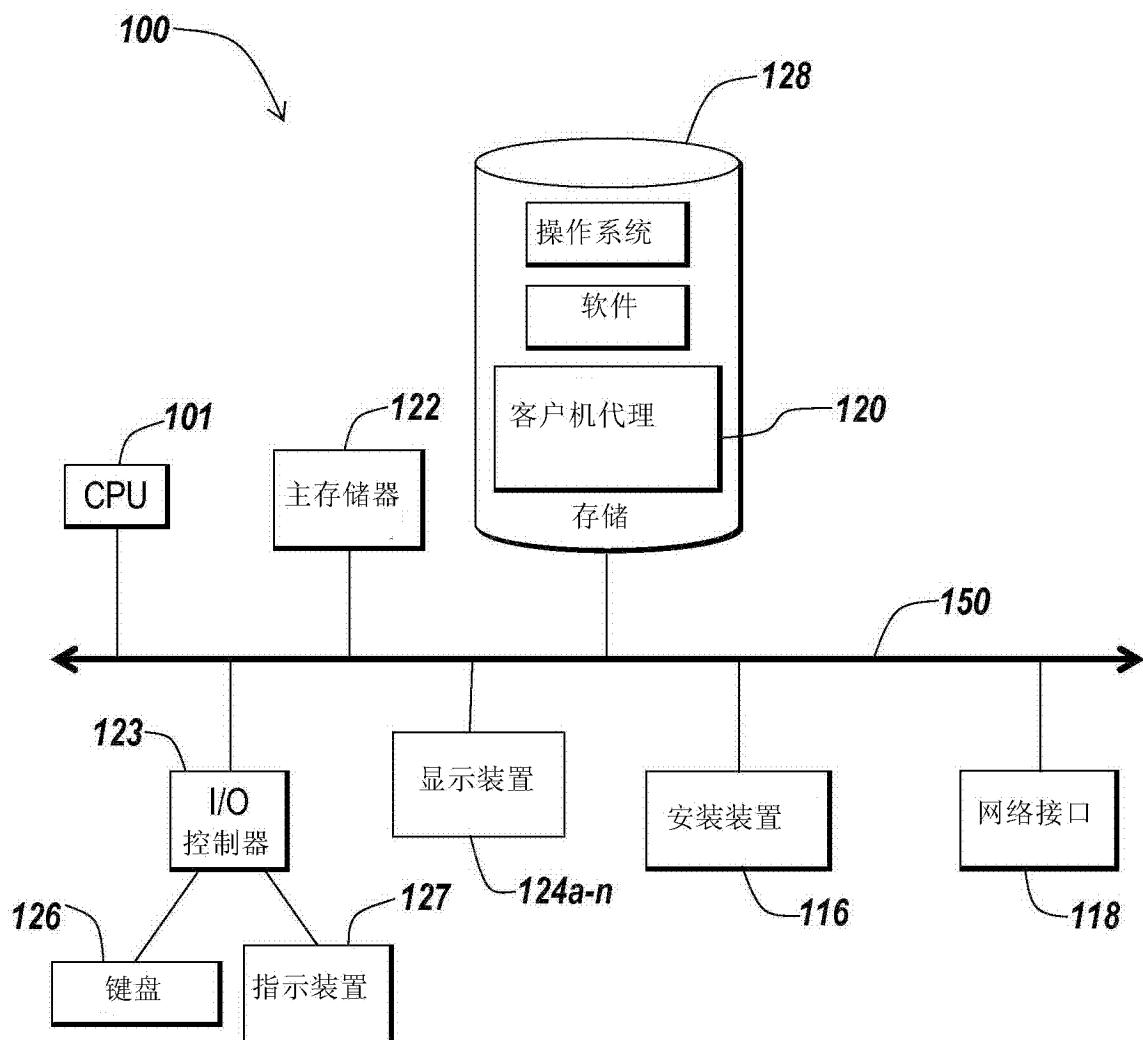


图 1E

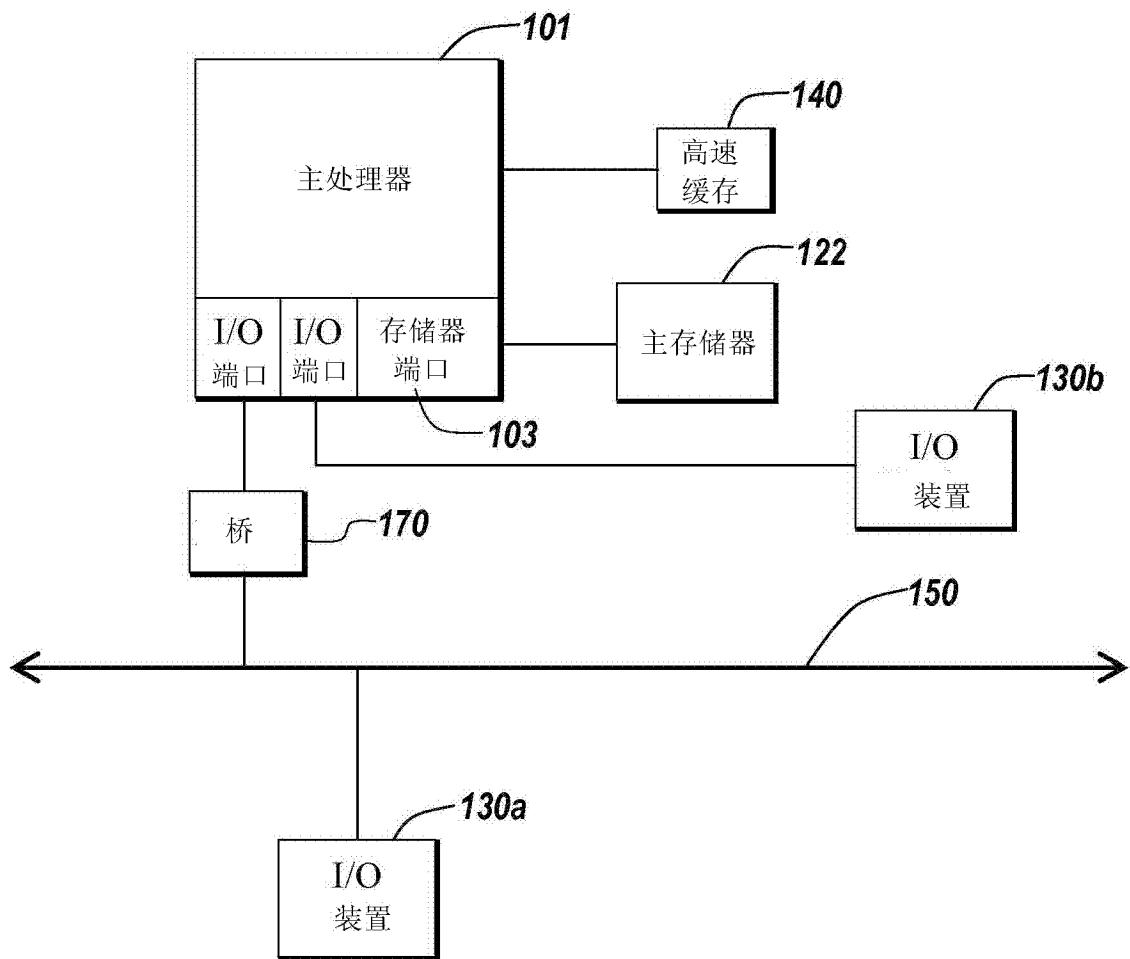


图 1F

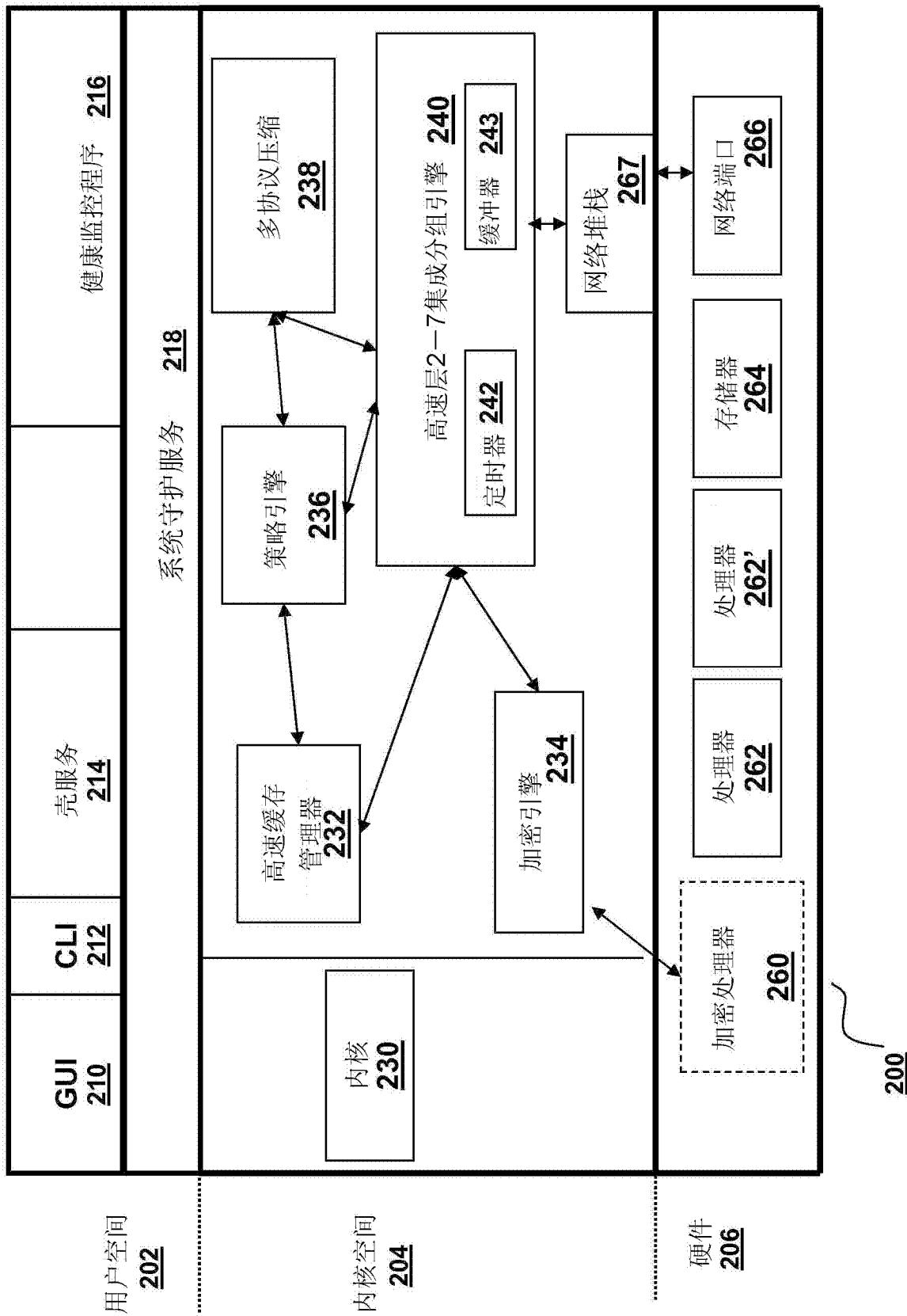


图 2A

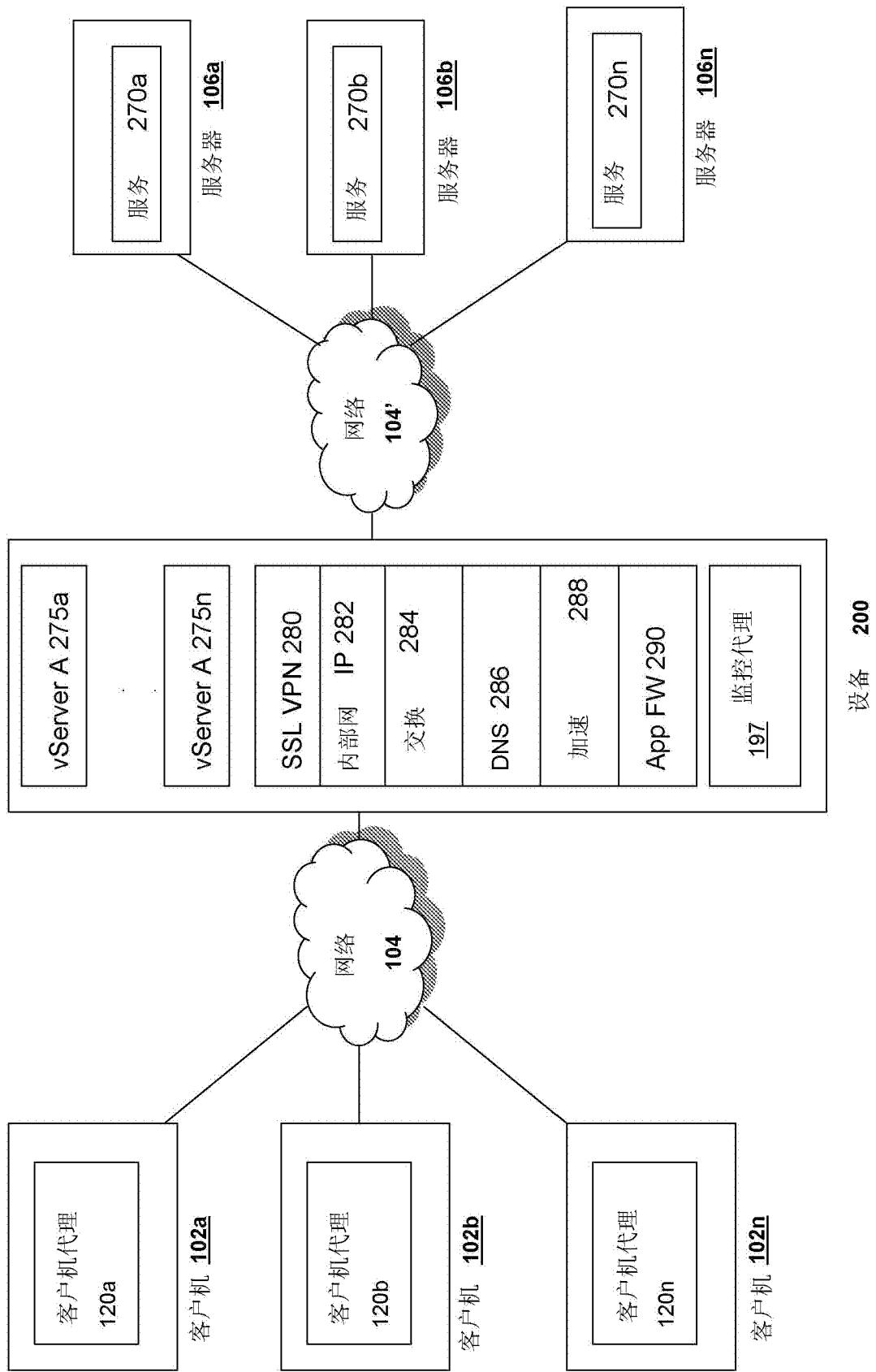


图 2B

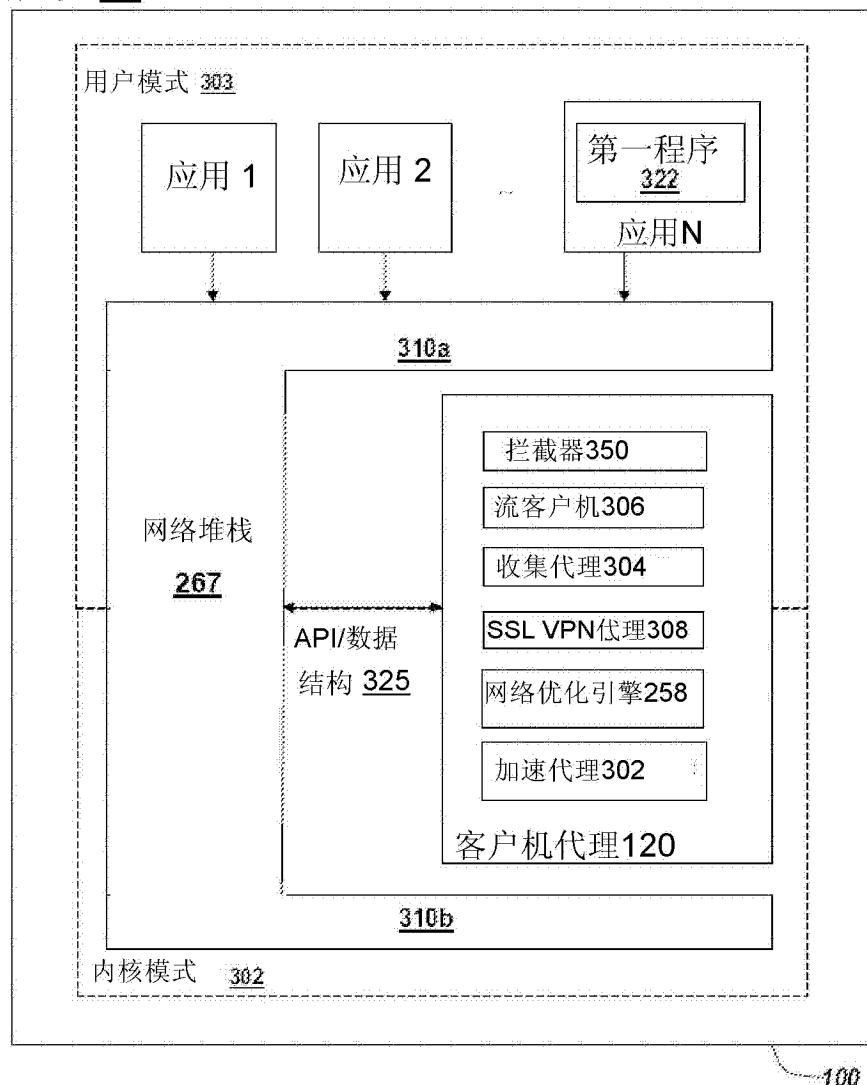
客户机 102

图 3

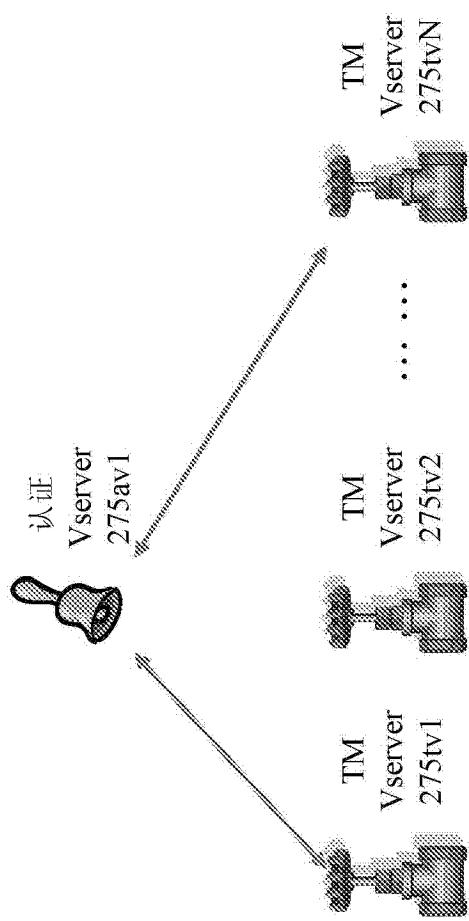


图 4A

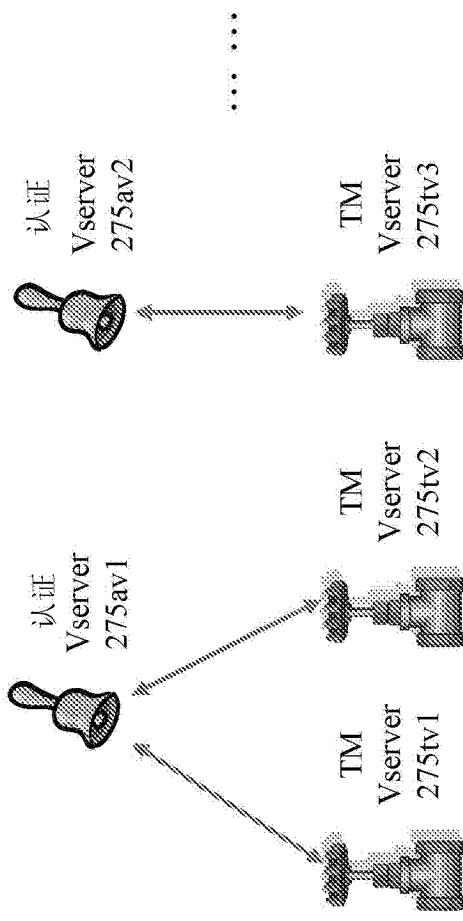


图 4B

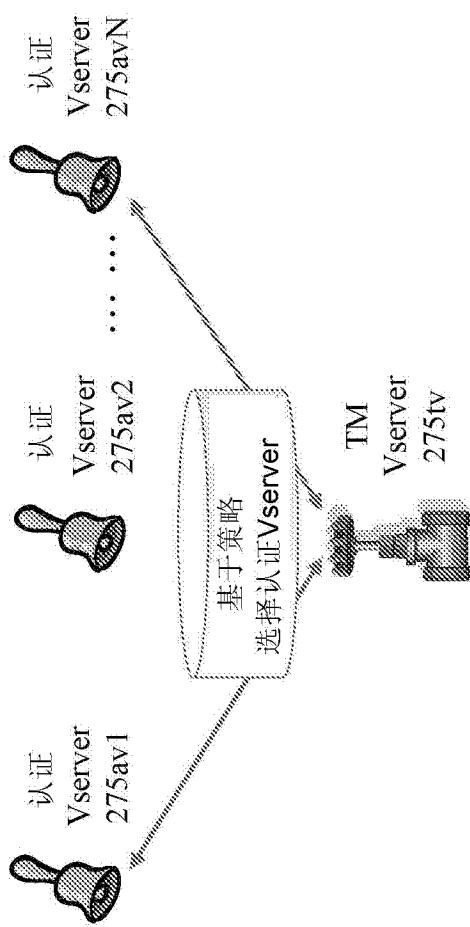


图 4C

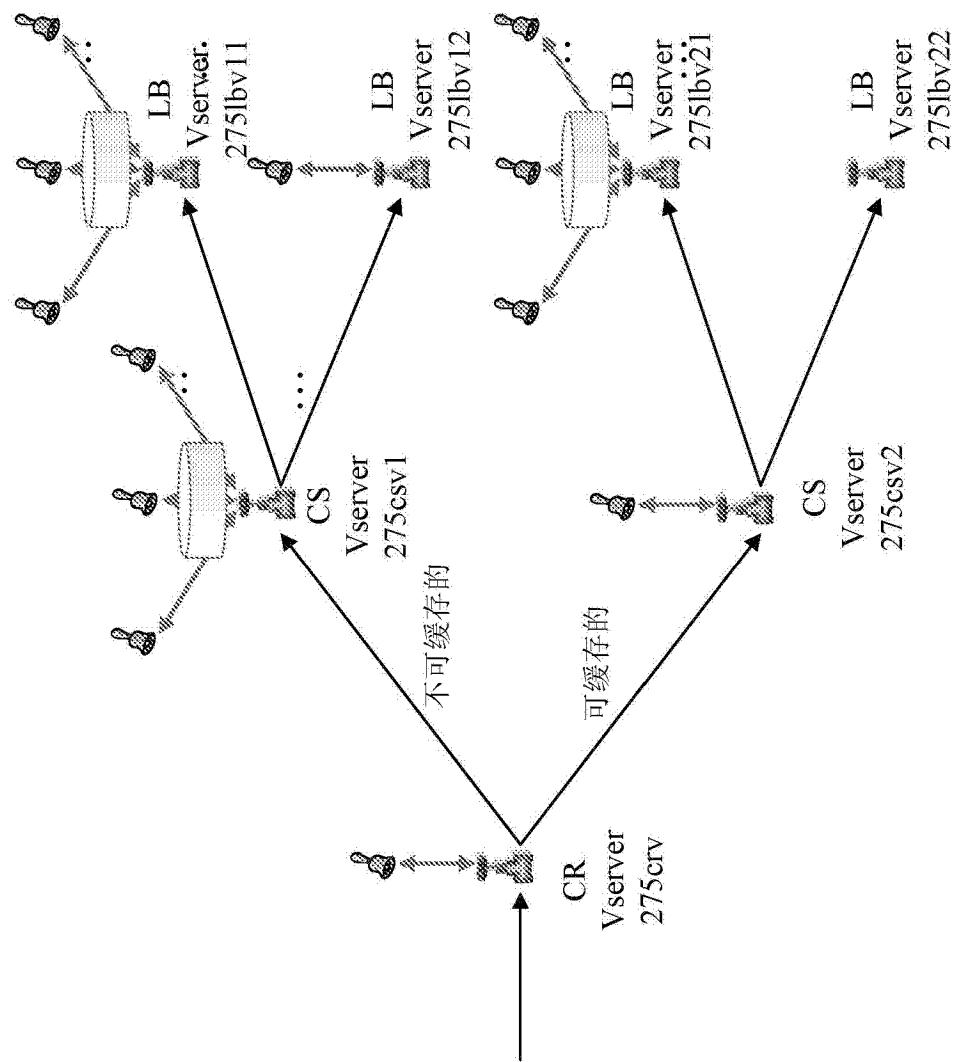


图 4D

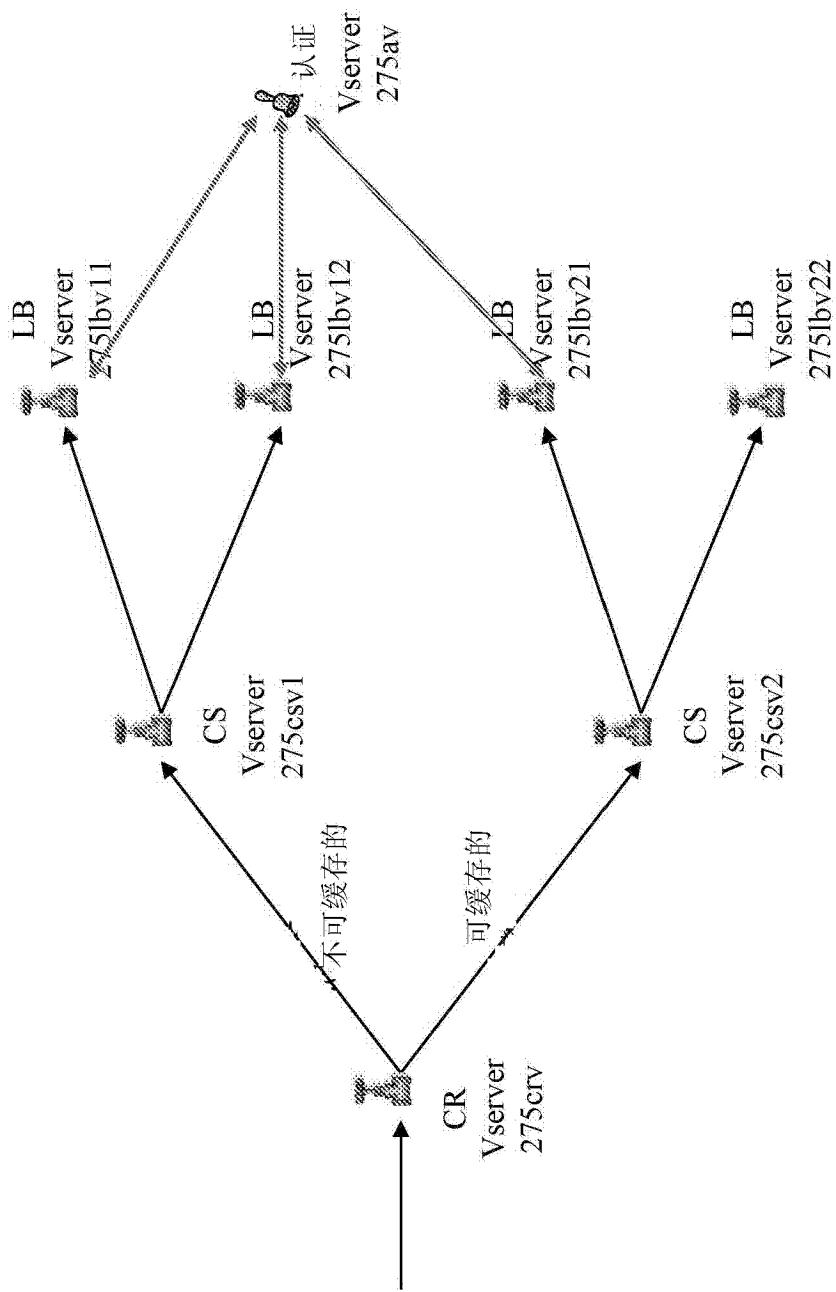
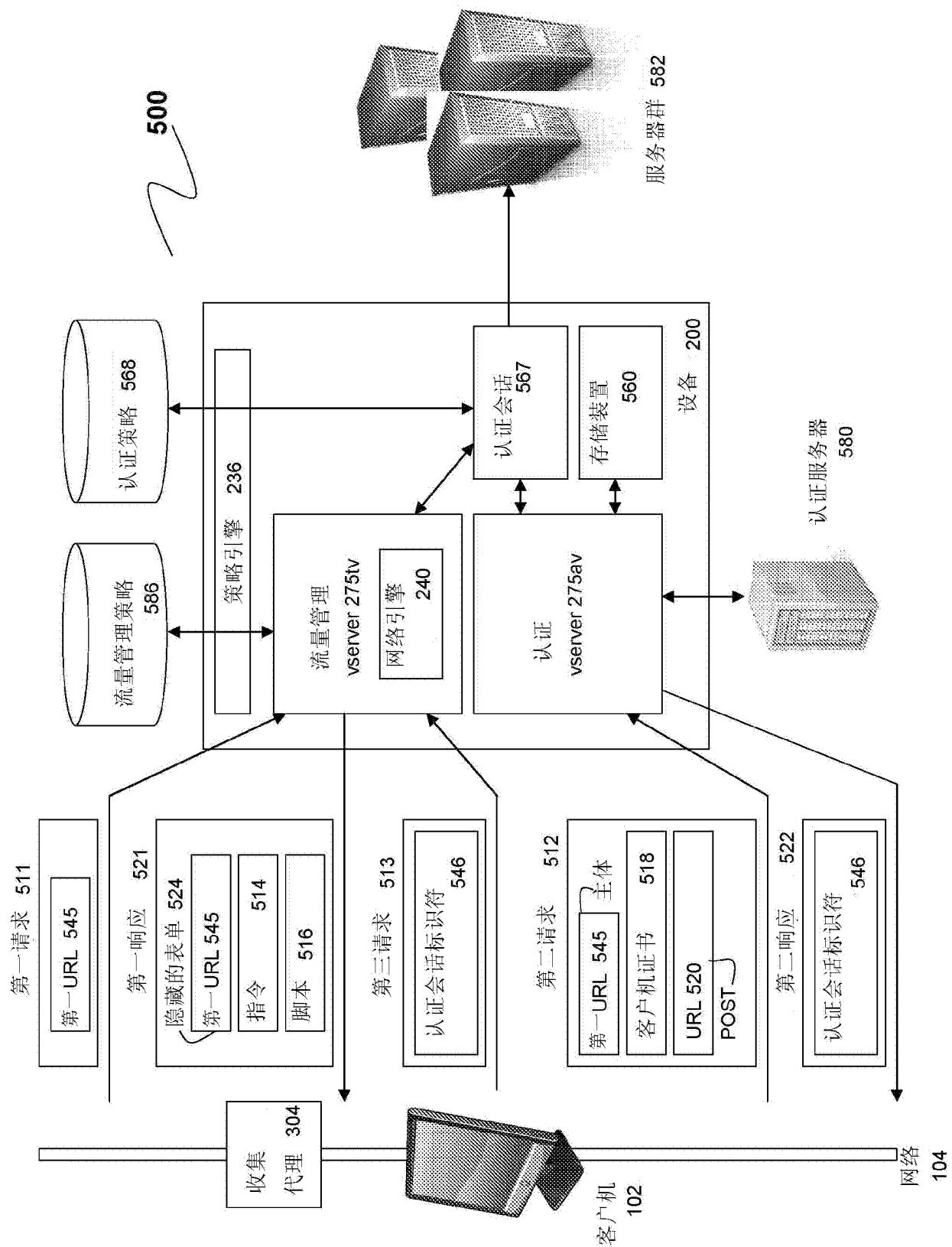


图 4E



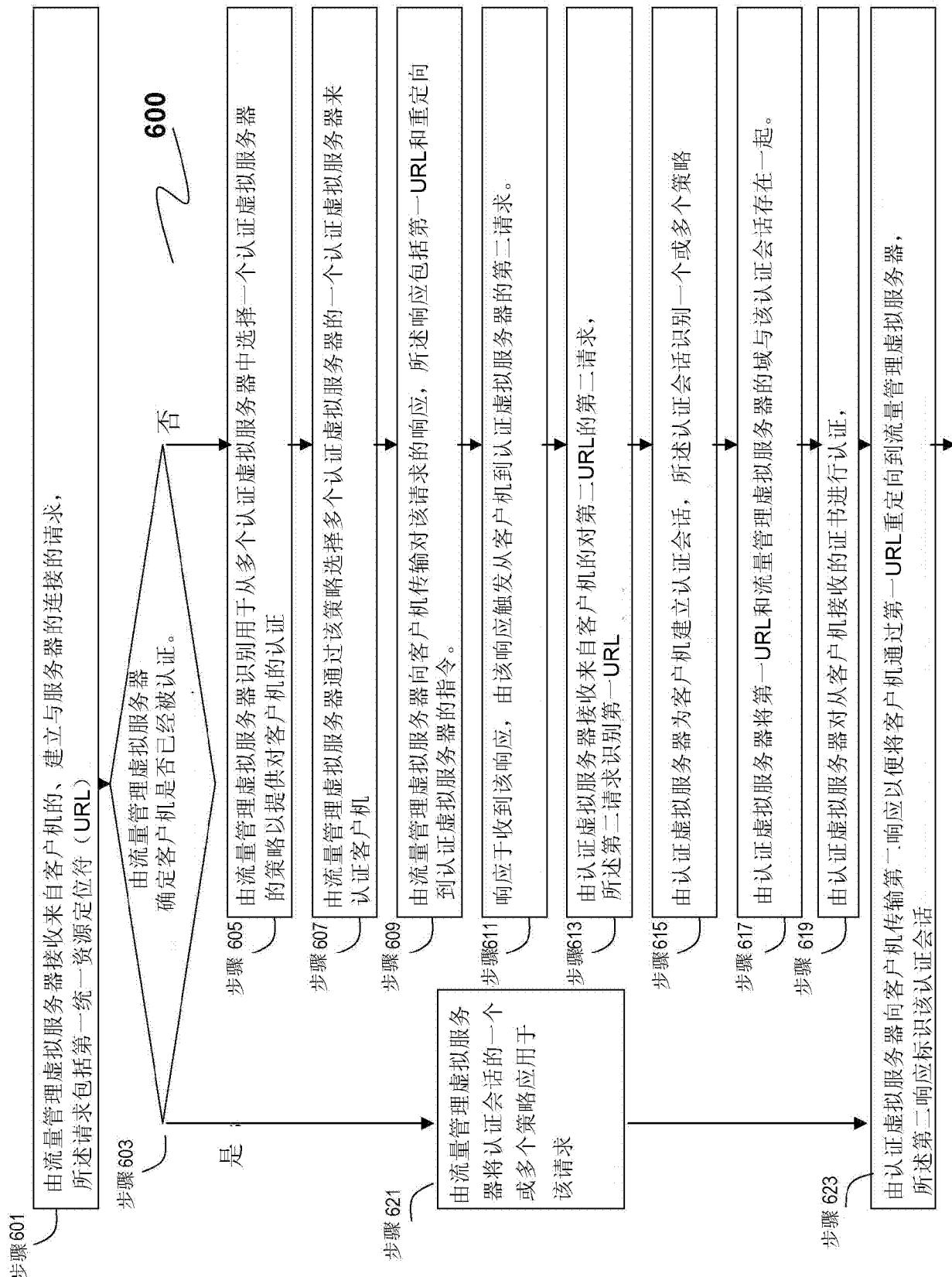


图 6A

600

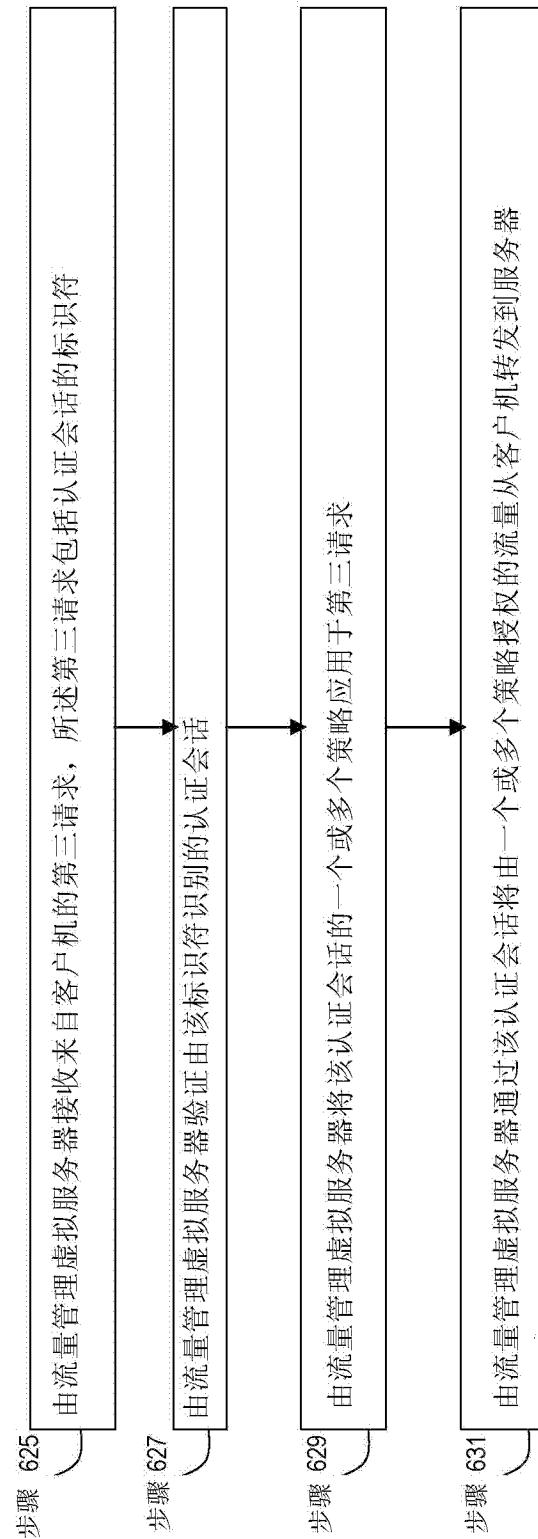


图 6B

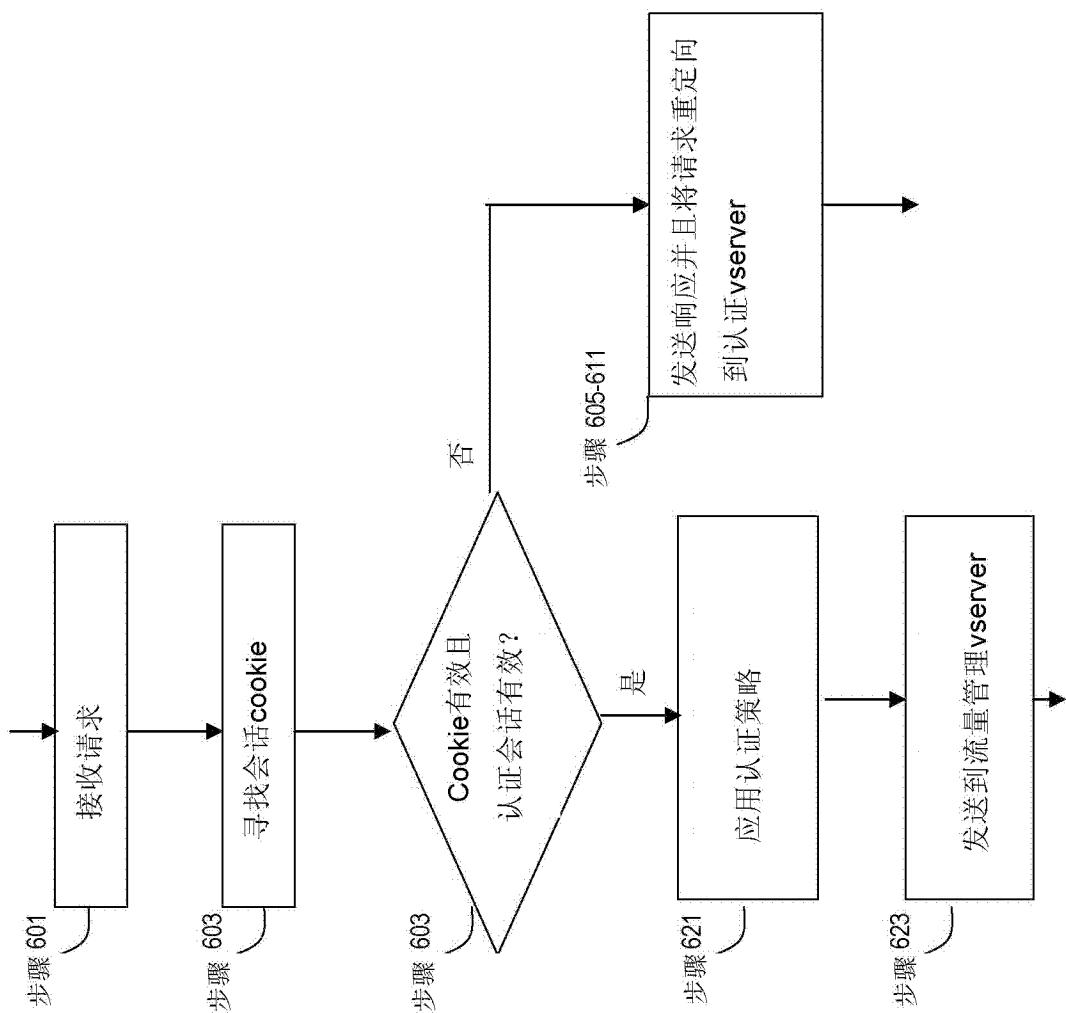


图 7A

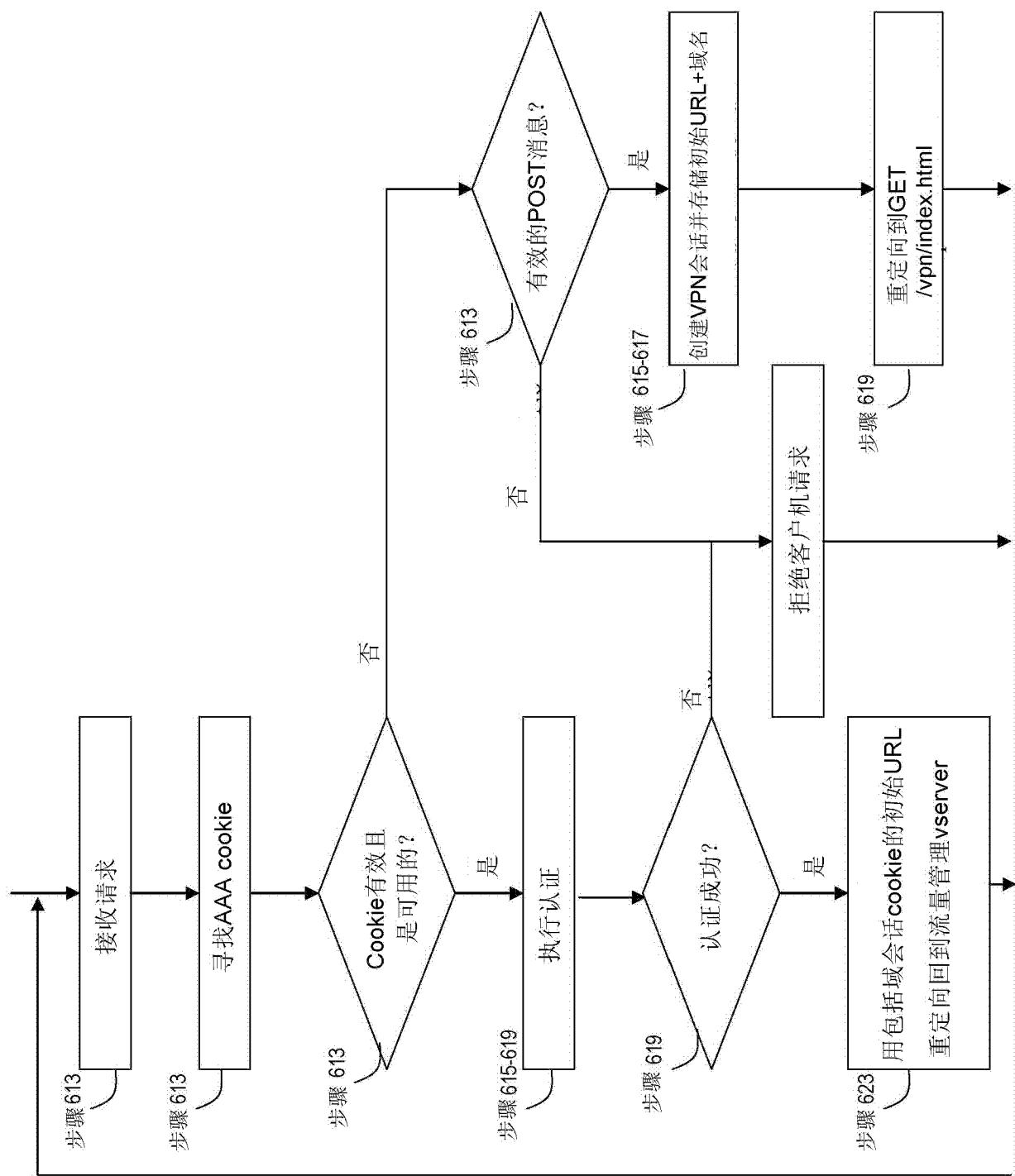


图 7B

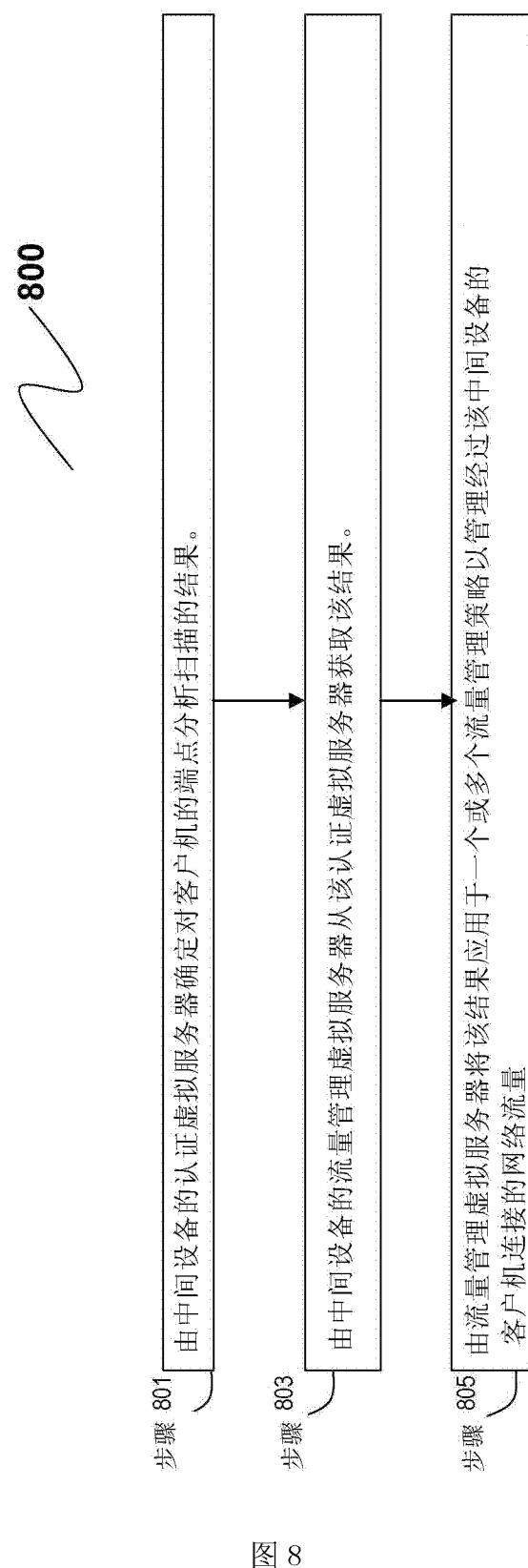


图 8