(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 102047262 B
(45)授权公告日 2015.07.22

(21)申请号 200980120235.1
(22)申请日 2009.03.27
(30)优先权数据
12/127,803 2008.05.27 US
(85)PCT国际申请进入国家阶段日
2010.11.26
(86)PCT国际申请的申请数据
PCT/US2009/038673 2009.03.27
(87)PCT国际申请的公布数据
WO2009/151730 EN 2009.12.17
(73)专利权人 微软公司
地址 美国华盛顿州
(72)发明人 N·奈斯 O·阿纳尼耶夫
J·F·沃尔伏特 A·芬克尔斯坦
A·捷普里斯基
(74)专利代理机构 上海专利商标事务所有限公司 31100
代理人 陈斌 钱静芳
(51)Int.Cl.
G06F 21/31(2013.01)
G06F 21/60(2013.01)
(56)对比文件
US 2008/0052771 A1,2008.02.28,
US 2008/0052771 A1,2008.02.28,
US 2004/0073629 A1,2004.04.15,
US 2007/0208936 A1,2007.09.06,
US 2003/0041263 A1,2003.02.27,
CN 1516833 A,2004.07.28,
CN 1581771 A,2005.02.16,
US 2005/0160161 A1,2005.07.21,
审查员 吴琼

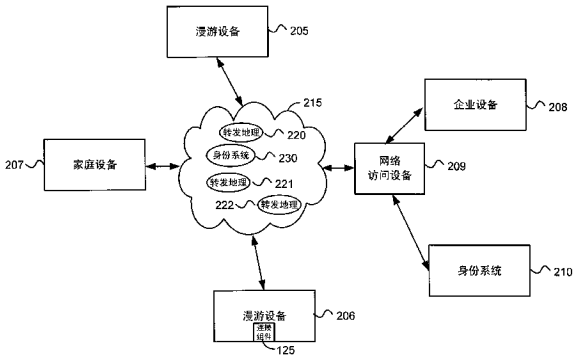
权利要求书3页 说明书10页 附图5页

(54)发明名称

用于分布式安全内容管理系统的认证

(57)摘要

此处所描述的主题的各方面涉及用于分布式安全内容管理系统的认证。在各方面,要访问可通过因特网获得的资源的请求被路由到安全组件。安全组件是分布在因特网各处的多个安全组件中的一个并负责认证与企业相关联的实体。安全组件确定要对实体使用的认证协议然后认证该实体。如果该实体被认证,则该实体被允许使用转发代理。



CN 102047262 B

1. 一种至少部分地由计算机实现的方法，所述方法包括：

由设备发送访问资源的请求；

将所述请求路由到与转发代理相关联的安全组件，所述转发代理在逻辑上处于所述设备和所述资源之间；

在所述安全组件处接收 (420) 从设备发送的消息；

经由所述安全组件认证 (430) 与所述设备相关联的实体；

由所述转发代理或所述安全组件生成 cookie 并将所述 cookie 发送 (435) 给所述设备，所述 cookie 指示所述实体先前是否已经由所述安全组件认证，所述设备随着要访问可经由所述转发代理访问的资源的后续请求来呈现所述 cookie，所述转发代理提供所述设备到所述资源的连接；以及

为所述 cookie 建立生存时间，所述 cookie 在超过所述生存时间之后对认证不再有用，其中所述 cookie 包括与所述实体相关联的策略信息，所述策略信息可用于实施用于所述后续请求的策略。

2. 如权利要求 1 所述的方法，其特征在于，所述转发代理至少作为 HTTP 代理来操作，且其中认证与所述设备相关联的实体包括在所述转发代理和所述设备之间建立安全连接。

3. 如权利要求 2 所述的方法，其特征在于，所述安全连接包括安全套接字层连接。

4. 如权利要求 2 所述的方法，其特征在于，所述安全连接包括传输层安全连接。

5. 如权利要求 1 所述的方法，其特征在于，所述转发代理至少作为 HTTP 代理来操作，且其中认证与所述设备相关联的实体包括使用客户机证书。

6. 如权利要求 1 所述的方法，其特征在于，所述 cookie 指示与所述实体相关联的身份，所述身份标识关联于与所述设备相关联的实体的企业实体所控制的网络上的实体。

7. 如权利要求 6 所述的方法，其特征在于，还包括存储所述设备发送的后续请求以及标识符的历史。

8. 如权利要求 1 所述的方法，其特征在于，还包括在位于所述转发代理本地的第一网络上的第一身份系统和所述第一网络外部的网络上的第二身份系统之间建立信任关系。

9. 如权利要求 8 所述的方法，其特征在于，建立信任关系包括在所述第一和第二身份系统之间同步凭证。

10. 一种计算机实现的方法，包括：

从与附连到第一网络的设备相关联的实体发送 (510) 要访问来自第二网络的资源的请求；

在主存在所述设备上的组件处接收 (515) 所述请求，所述组件监视所述设备和所述第二网络之间的通信；

在将所述请求发送到所述第二网络之前，通过所述组件与关联于附连到所述第二网络的转发代理的安全组件进行通信，来认证 (520) 所述实体，所述转发代理在逻辑上在所述设备和所述第二网络之间；

将所述请求发送 (525) 给所述转发代理；以及

从所述转发代理接收 cookie，所述 cookie 指示所述实体先前是否已经由所述安全组件认证。

11. 如权利要求 10 所述的计算机实现的方法，其特征在于，所述转发代理至少作为

HTTP 代理来操作，且其中认证与所述设备相关联的实体包括使用客户机证书。

12. 如权利要求 10 所述的计算机实现的方法，其特征在于，还包括处理所述 cookie，其中处理所述 cookie 包括存储所述 cookie 并在对于可经由所述第二网络访问的资源的后续请求中发送所述 cookie。

13. 如权利要求 10 所述的计算机实现的方法，其特征在于，所述实体包括设备和 / 或用户。

14. 一种处于计算环境的装置，包括 ：

可用于与关联于试图获得对可经由第一网络获得的资源的访问的实体的设备来协商认证协议的协议选择器 (315)，所述认证协议是结合对所述实体的认证来使用的 ；

可用于经由与所述实体相关联的所述设备、使用所述认证协议来认证所述实体的客户机组件 (320) ；以及

可用于从与第二身份系统具有信任关系的第一身份系统获得用于所述实体的标识符的身份确认器 (325)，所述第一身份系统驻留在所述第一网络上，所述第二身份系统驻留在第二网络上 ；

可用于向转发代理指示所述实体是否被认证的代理通知器 (330)，所述转发代理是分布在一个或多个网络上的多个转发代理中的一个，所述转发代理被构造成允许经认证的实体访问可经由所述一个或多个网络获得的资源 ；以及

可用于存储标识所述实体和所述实体访问的可经由所述第一网络获得的资源的信息的历史跟踪器。

15. 如权利要求 14 所述的装置，其特征在于，还包括可用于按标识所述实体和所访问的资源的形式来提供所述信息的报告组件。

16. 一种计算机实现的系统，包括 ：

用于从与附连到第一网络的设备相关联的实体发送要访问来自第二网络的资源的请求的装置 ；

用于在主存在所述设备上的组件处接收所述请求的装置，所述组件监视所述设备和所述第二网络之间的通信 ；

用于在将所述请求发送到所述第二网络之前，通过所述组件与关联于附连到所述第二网络的转发代理的安全组件进行通信，来认证所述实体的装置，所述转发代理在逻辑上在所述设备和所述第二网络之间 ；

用于将所述请求发送给所述转发代理的装置 ；以及

用于从所述转发代理接收 cookie 的装置，所述 cookie 指示所述实体先前是否已经由所述安全组件认证。

17. 如权利要求 16 所述的计算机实现的系统，其特征在于，所述转发代理至少作为 HTTP 代理来操作，且其中用于认证与所述设备相关联的实体的装置包括用于使用客户机证书的装置。

18. 如权利要求 16 所述的计算机实现的系统，其特征在于，还包括用于处理所述 cookie 的装置，其中用于处理所述 cookie 的装置包括用于存储所述 cookie 并在对于可经由所述第二网络访问的资源的后续请求中发送所述 cookie 的装置。

19. 如权利要求 16 所述的计算机实现的系统，其特征在于，所述实体包括设备和 / 或用

户。

用于分布式安全内容管理系统的认证

[0001] 背景

[0002] 通常，企业采用包括在各种安全产品和设备中的功能来保护公司信息技术资产。这些功能可包括，例如，过滤进入和离开企业的网络通信的诸如恶意软件等恶意代码、限制对不适当的外部内容的访问、阻止对企业网络的攻击和其他入侵等。

[0003] 随着移动、家庭和其他计算设备的广泛的使用，员工将工作带到公司网络以外的地方。为了获得同等级的保护和实施企业网络上提供的策略，某些企业要求这些员工登录或以其他方式访问企业网络并通过企业网络来访问企业网络以外的资源。出于各种原因，当漫游用户不靠近企业网络时，这成为非最优的。

[0004] 在此要求保护的主题不限于解决任何缺点或仅在诸如上述环境中操作的各个实施例。相反，提供该背景仅用以示出在其中可实践在此描述的部分实施例的一个示例性技术领域。

[0005] 概述

[0006] 简言之，此处所描述的主题的各方面涉及用于分布式安全内容管理系统的认证。在各方面，访问可通过因特网获得的资源的请求被路由到安全组件。安全组件是分布在因特网各处的多个安全组件中的一个并负责认证与企业相关联的实体。安全组件确定要对实体使用的认证协议然后认证该实体。如果该实体被认证，则该实体被允许使用转发代理。

[0007] 提供本概述是为了简要地标识在以下详细描述中进一步描述的主题的一些方面。本概述并不旨在标识出所要求保护的主题的关键特征或必要特征，也不旨在用于限制所要求保护的主题的范围。

[0008] 除非上下文清楚地指出，否则短语“此处所描述的主题”指的是详细描述中所描述的主题。术语“方面”被当作“至少一个方面”。标识详细描述中所描述的主题的各方面不旨在标识所要求保护的主题的关键特征或必要特征。

[0009] 上述各方面和此处所描述的主题的其它方面是借助于示例说明的，并且不受附图限制，附图中相同的标号指出相似的元素。

[0010] 附图简述

[0011] 图 1 是表示其中可结合此处所描述的主题的各方面的示例性通用计算环境的框图；

[0012] 图 2 是概括地表示此处所描述的主题的各方面可以在其中实现的示例性环境的框图；

[0013] 图 3 是表示根据此处所描述的主题的各方面的用安全组件配置的示例性装置的框图；以及

[0014] 图 4-5 是概括地表示根据此处所描述的主题的各方面的可结合认证发生的动作的流程图。

[0015] 详细描述

[0016] 示例性操作环境

[0017] 图 1 示出可在其上实现此处所描述的主题的各方面的合适的计算系统环境 100 的

示例。计算系统环境 100 仅为合适的计算环境的一个示例，并非旨在对此处所描述的主题的各方面的使用范围或功能提出任何限制。也不应该将计算环境 100 解释为对示例性操作环境 100 中示出的任一组件或其组合有任何依赖性或要求。

[0018] 此处所描述的主题的各方面可与众多其他通用或专用计算系统环境或配置一起操作。适用于此处所描述的主题的各方面的公知的计算系统、环境和 / 或配置的示例包括，但不限于，个人计算机、服务器计算机、手持式或膝上型设备、多处理器系统、基于微处理器的系统、机顶盒、可编程消费电子产品、网络 PC、小型计算机、大型计算机、包括上述系统或设备中的任一个的分布式计算环境等。

[0019] 此处所描述的主题的各方面可在由计算机执行的诸如程序模块等计算机可执行指令的一般上下文中描述。一般而言，程序模块包括执行特定任务或实现特定抽象数据类型的例程、程序、对象、组件、数据结构等等。此处所描述的主题的各方面也可以在其中任务由通过通信网络链接的远程处理设备执行的分布式计算环境中实现。在分布式计算环境中，程序模块可以位于包括存储器存储设备在内的本地和远程计算机存储介质中。

[0020] 参考图 1，用于实现此处所描述的主题的各方面的示例性系统包括计算机 110 形式的通用计算设备。计算机 110 的组件可以包括但不限于 ：处理单元 120、系统存储器 130 和将包括系统存储器在内的各种系统组件耦合至处理单元 120 的系统总线 121。系统总线 121 可以是几种类型的总线结构中的任何一种，包括存储器总线或存储控制器、外围总线、以及使用各种总线体系结构中的任一种的局部总线。作为示例，而非限制，这样的体系结构包括工业标准体系结构 (ISA) 总线、微通道体系结构 (MCA) 总线、增强型 ISA(EISA) 总线、视频电子技术标准协会 (VESA) 局部总线、也称为夹层 (Mezzanine) 总线的外围部件互连 (PCI) 总线、扩展外围部件互连 (PCI-X) 总线、高级图形端口 (AGP)、以及快速 PCI(PCIe)。

[0021] 计算机 110 通常包括各种计算机可读介质。计算机可读介质可以是能由计算机 110 访问的任何可用介质，并包含易失性和非易失性介质以及可移动、不可移动介质。作为示例而非限制，计算机可读介质可以包括计算机存储介质和通信介质。

[0022] 计算机存储介质包括以用于存储诸如计算机可读指令、数据结构、程序模块或其它数据等信息的任何方法或技术实现的易失性和非易失性、可移动和不可移动介质。计算机存储介质包括但不限于，RAM、ROM、EEPROM、闪存或其它存储器技术、CD-ROM、数字多功能盘 (DVD) 或其它光盘存储、磁盒、磁带、磁盘存储或其它磁存储设备、或可以用来储存所期望的信息并可由计算机 110 访问的任一其它介质。

[0023] 通信介质通常以诸如载波或其他传输机制等已调制数据信号来体现计算机可读指令、数据结构、程序模块或其他数据，并包括任何信息传送介质。术语“已调制数据信号”指的是其一个或多个特征以在信号中编码信息的方式被设定或更改的信号。作为示例而非限制，通信介质包括有线介质，如有线网络或直接线连接，以及诸如声学、RF、红外线及其他无线介质之类的无线介质。上述的任意组合也应包含在计算机可读介质的范围内。

[0024] 系统存储器 130 包括易失性和 / 或非易失性存储器形式的计算机存储介质，如只读存储器 (ROM)131 和随机存取存储器 (RAM)132。基本输入 / 输出系统 133(BIOS) 包括如在启动时帮助在计算机 110 内的元件之间传输信息的基本例程，它通常储存在 ROM 131 中。RAM 132 通常包含处理单元 120 可以立即访问和 / 或目前正在操作的数据和 / 或程序模块。作为示例而非限制，图 1 示出了操作系统 134、应用程序 135、其它程序模块 136 和程序数据

137。

[0025] 计算机 110 也可以包括其他可移动 / 不可移动、易失性 / 非易失性计算机存储介质。仅作为示例，图 1 示出了从不可移动、非易失性磁介质中读取或向其写入的硬盘驱动器 141，从可移动、非易失性磁盘 152 中读取或向其写入的磁盘驱动器 151，以及从诸如 CD ROM 或其它光学介质等可移动、非易失性光盘 156 中读取或向其写入的光盘驱动器 155。可以在该示例性操作环境中使用的其他可移动 / 不可移动、易失性 / 非易失性计算机存储介质包括但不限于，磁带盒、闪存卡、数字多功能盘、其他光盘、数字录像带、固态 RAM、固态 ROM 等等。硬盘驱动器 141 通常通过诸如接口 140 等不可移动存储器接口连接到系统总线 121，而磁盘驱动器 151 和光盘驱动器 155 则通常由诸如接口 150 等可移动存储器接口连接至系统总线 121。

[0026] 以上描述并在图 1 中示出的驱动器及其相关联的计算机存储介质为计算机 110 提供了对计算机可读指令、数据结构、程序模块和其它数据的存储。例如，在图 1 中，硬盘驱动器 141 被示为存储操作系统 144、应用程序 145、其它程序模块 146 和程序数据 147。注意，这些组件可以与操作系统 134、应用程序 135、其他程序模块 136 和程序数据 137 相同，也可以与它们不同。操作系统 144、应用程序 145、其他程序模块 146 和程序数据 147 在这里被标注了不同的附图标记是为了说明至少它们是不同的副本。用户可以通过输入设备，如键盘 162 和定点设备 161（通常被称为鼠标、跟踪球或触摸板）向计算机 20 输入命令和信息。其它输入设备（未示出）可包括话筒、操纵杆、游戏手柄、圆盘式卫星天线、扫描仪、触敏屏、写字板等。这些和其他输入设备通常由耦合至系统总线的用户输入接口 160 连接至处理单元 120，但也可以由其他接口和总线结构，诸如并行端口、游戏端口或通用串行总线 (USB) 连接。监视器 191 或其他类型的显示设备也经由接口，诸如视频接口 190 连接至系统总线 121。除监视器以外，计算机还可以包括其他外围输出设备，诸如扬声器 197 和打印机 196，它们可以通过输出外围接口 190 连接。

[0027] 计算机 110 可使用至一个或多个远程计算机，如远程计算机 180 的逻辑连接在网络化环境中操作。远程计算机 180 可以是个人计算机、服务器、路由器、网络 PC、对等设备或其它常见网络节点，且通常包括上文相对于计算机 110 描述的许多或所有元件，尽管在图 1 中只示出存储器存储设备 181。图 1 中所示的逻辑连接包括局域网 (LAN)171 和广域网 (WAN)173，但也可以包括其它网络。这样的联网环境常见于办公室、企业范围计算机网络、内联网和因特网中。

[0028] 当在 LAN 联网环境中使用时，计算机 110 通过网络接口或适配器 170 连接至 LAN 171。当在 WAN 联网环境中使用时，计算机 110 可包括调制解调器 172 或用于通过诸如因特网等的 WAN 173 来建立通信的其它装置。可为内置或可为外置的调制解调器 172 可以经由用户输入接口 160 或其他合适的机制连接至系统总线 121。在网络化环境中，关于计算机 110 所描述的程序模块或其部分可被储存在远程存储器存储设备中。作为示例而非限制，图 1 示出了远程应用程序 185 驻留在存储器设备 181 上。可以理解，所示的网络连接是示例性的，且可以使用在计算机之间建立通信链路的其他手段。

[0029] 认证

[0030] 如前所述，员工常常在公司网络以外工作。然而，同时，企业希望能够提供同等级的保护、提供基于用户活动的报告、并应用与当用户使用企业网络来访问远程网络资源时

所应用的相同的策略。

[0031] 根据此处所描述的主题的各方面，提供了位于云中的一个或多个转发代理。在逻辑上，转发代理位于客户机和该客户机试图访问的网络资源之间。转发代理从客户机接收请求、向客户机提供到所请求的资源的连接、并可在适当时向这些请求提供上文标识的其他功能。转发代理可与认证实体并记录与其相关联的活动的一个或多个安全组件相关联。这些组件可使用各种认证协议来认证实体，并可与位于企业站点的身份系统进行通信来执行该认证。这些组件还可获得要在记录实体活动时使用的标识符。

[0032] 与安全组件相关联意味着转发代理可包括安全组件的全部或部分，或者安全组件的全部或部分可位于转发代理之外。

[0033] 图 2 是概括地表示此处所描述的主题的各方面可以在其中实现的示例性环境的框图。图 2 中示出的环境可包括漫游设备 205-206、家庭设备 207、企业设备 208、网络访问设备 209 和身份系统 210（在下文中有时被共同称为实体），并可包括其他实体（未示出）。各种实体可以经由各种网络进行通信，这些网络包括办公室内和办公室间网络以及网络 215。

[0034] 在一实施例中，网络 215 可包括因特网。在一实施例中，网络 215 可包括一个或多个局域网、广域网、直接连接、以上的某种组合等。

[0035] 设备 205-208 可包括一个或多个通用或专用计算设备。这些设备可包括，例如，个人计算机、服务器计算机、手持式或膝上型设备、多处理器系统、基于微控制器的系统、机顶盒、可编程消费电子产品、网络 PC、小型计算机、大型计算机、个人数字助理 (PDA)、游戏设备、打印机、包括机顶盒、媒体中心或其他电器在内的电器、汽车嵌入式或附连的计算设备、其他移动设备、包括以上系统或设备中的任一种的分布式计算环境等。可被配置成用作设备 205-208 中的一个或多个的示例性设备包括图 1 的计算机 110。

[0036] 漫游设备 205-206 可包括在各位置之间携带的计算设备。例如，员工可在出差时携带笔记本计算机。作为另一示例，员工可带着蜂窝电话、PDA 或员工几乎可以在任何地方使用的某种其他手持式设备来旅行。

[0037] 家庭设备 207 可包括，例如，个人计算机或位于员工的家的其他电子设备。

[0038] 企业设备 208 可包括位于一个或多个企业站点并连接到企业网络的设备。例如，企业设备 208 可包括工作站、服务器、路由器、移动设备、或上述的其他通用或专用计算设备。

[0039] 网络访问设备 209 可包括被配置成允许、拒绝、代理、发送、缓存计算机通信或对其执行其他动作的一个或多个设备和 / 或软件组件。在被配置为防火墙的情况下，网络访问设备 209 可用于提供对连接在网络访问设备 209 后的企业设备 208 和身份系统 210 以及其他设备（如果存在）的保护。网络访问设备 209 可被配置为到虚拟专用网络的端点。在这种配置中，网络访问设备 209 可向转发代理 220-222 中的一个或多个以及诸如本地身份系统 230 等的附连到网络 215 的其他组件提供安全通信信道。与本地身份系统 230 之间的安全通信信道可用于在身份系统 210 和本地身份系统 230 之间建立单向或双向信任关系。在一个实施例中，网络访问设备 209 可包括，例如，用适当的硬件和软件来配置的图 1 的计算机 110。在另一实施例中，网络访问设备 209 可包括专用设备。

[0040] 身份系统 210 可包括主存在诸如以上描述的设备等的一个或多个设备上的一个或多个进程。可利用身份系统 210 来标识用户和 / 或设备，如以下将更详细地描述的。在

一个实施例中，身份系统 210 可包括华盛顿州雷蒙德市微软公司生产的现用目录 (Active Directory)。身份系统的其他示例包括基于 RADIUS 的 ID 系统、基于 LDAP 的 ID 系统、通用数据库 ID 系统等。

[0041] 如图 2 所示，在一个实施例中，身份系统 210 驻留在可通过网络访问设备 209 访问的企业网络上。在另一实施例中，身份系统 210 可驻留在企业网络外部的网络上。例如，身份系统 210 可驻留或分布在网络 215 中的各个位置处。在一个实施例中，身份系统 210 可以是附连到网络 215 的服务器所主存的服务。

[0042] 转发代理 220-222 位于可经由网络访问的各个位置处。这些转发代理可提供有时由企业网络中的设备所提供的各种功能，如连接、反病毒、间谍软件和网络钓鱼保护、URL 过滤、防火墙、入侵检测、信息泄漏保护 (ILP) 等。转发代理 220-222 还可向连接到网络 215 的漫游设备提供集中式管理。转发代理 220-220 还可向各种设备提供其他功能，诸如用于移动设备的呈现、对网页和其他内容的缓存、和企业可能期望的任何其他连接和 / 或安全功能。

[0043] 当设备试图访问连接到网络 215 的资源时，进入和离开该设备的通信可被路由到转发代理来提供例如上述的一个或多个功能。然而，在向设备提供这些功能之前，与转发代理相关联的安全组件认证该设备和 / 或使用该设备的用户。在认证的上下文中，此处使用的术语实体有时指示设备和 / 或使用该设备的用户。

[0044] 可出于各种原因来认证实体。例如，可能期望只允许已注册的实体使用转发代理。为了确保出现这种情况，可执行认证。作为另一示例，认证实体可用作标识来了解向被路由至和自该设备的通信应用什么策略。作为又一示例，认证实体可用于报告、审计、和以其他方式跟踪实体的活动。

[0045] 以上所述的认证实体的示例原因不旨在是包括一切的或限制性的。其也不旨在限制此处所描述的主题的各方面和涉及上述示例的一个或多个的实现。事实上，基于此处的教学，本领域技术人员可认识到，可以应用此处呈现的各概念中的许多其他场景而不背离此处所描述的主题的方面的精神或范围。

[0046] 在基于企业凭证来认证实体时，来自身份系统 210 的信息可被发送到试图认证实体的安全组件。在一个实施例中，安全组件可以不为被授权使用转发代理的实体维护其自身的凭证数据库。相反，凭证可被存储在企业控制的位置处，如可经由身份系统 210 访问的凭证数据库上。这可以出于各种原因来完成。例如，在云中没有凭证数据库的情况下，系统可避免维护并同步存储在云中的凭证数据库和存储在企业网络上的凭证数据库。同样，因为云凭证数据库可由除企业之外的一方控制，所以将凭证数据库存储在企业网络上可引起较少的安全风险。作为另一好处，企业网络上最近创建的新的实体可立即访问转发代理，因为这些实体不需要等待同步。另外，不再被允许访问转发代理的实体可通过将其凭证从凭证数据库中移除来立即拒绝对转发代理的访问。此外，关于实体的网络活动所生成的报告可跟踪实体，无论该实体从什么位置访问转发代理。

[0047] 在该实施例中，为认证实体，安全组件可在需要时与身份系统 210 进行通信来获得足够的信息以认证该实体。该信息可包括，例如，实体凭证、质询 / 响应数据、证书相关的信息、或可用于认证该实体的任何其他信息。

[0048] 在另一实施例中，安全组件可访问使用单向或双向信任关系与身份系统 210 同步

的本地身份系统 230。在单向信任关系中，使用同步到本地身份系统 230 的企业凭证来认证的实体被允许经由转发代理来访问资源。

[0049] 安全组件和身份系统 210 和 230 之间的通信可按各种方式完成，包括例如，虚拟专用网络 (VPN)、多协议标签转换 (MPLS)、因特网协议安全 (IPSec)、因特网协议版本 6(IPv6) 全局寻址、其他通信协议等。

[0050] 在一个实施例中，只有特定通信协议所需的端口可在身份系统和安全组件之间的虚拟专用网络中涉及。换言之，可转发到在通信协议中涉及的端口的消息，而不转发到不在通信协议中涉及的端口的消息。这可有助于维护企业网络的安全，因为大大降低了攻击表面（例如，转发的端口数量）。

[0051] 转发代理和身份系统可被配置成经由 IPv6 来进行通信。结合 IPsec 和所配置的策略，这可用于保证只有指定的转发代理被允许与身份系统进行通信。

[0052] 为了认证实体，与转发代理相关联的安全组件可使用许多不同的机制中的一个或多个。例如，可以在安全组件和设备之间建立虚拟专用网络 (VPN)。在这种配置中，成功地建立 VPN 可用于认证实体。作为其他示例，可以使用集成Windows®认证、IPSec、基于表单的认证、RADIUS、MPLS、基本访问认证、Kerberos、基于客户机证书的认证、或某些其他认证协议等来认证实体。在一个实施例中，认证可作为 HTTP 代理认证的一部分来发起。

[0053] 认证协议的类型可在安全组件和设备之间协商。例如，如果设备支持第一组认证协议而安全组件支持第二组认证协议，则可以选择设备和安全组件两者都支持的认证协议来认证该实体。作为另一示例，如果设备支持允许设备来认证自身和 / 或用户而无需用户交互的认证协议（例如，诸如集成Windows®认证），则可以选择该协议。

[0054] 有许多方式来认证实体。例如，为了认证实体，安全组件可要求实体凭证（例如，用户名和口令或与该实体相关联的其他凭证）。使用这些凭证，安全组件可与身份系统 210 进行通信来验证这些凭证。为此，实体可使用例如 Basic、表单、RADIUS 或某种其他认证协议。

[0055] 如果凭证有效，则身份系统 210 可将此指示给安全组件并将与该实体相关联的标识符发送给安全组件。该标识符可包括该实体的企业身份。该标识符可在记录该实体的后续活动时使用。

[0056] 作为认证实体的另一示例，安全组件可在不接收凭证的情况下认证凭证。例如，安全组件可向实体提供质询并可使用对该质询的响应来认证实体。安全组件可将身份系统 210 涉及到确定质询和 / 或验证对质询的响应中。

[0057] 作为另一示例，安全组件可关联于使用单向或双向信任关系来与身份系统 210 同步的本地身份系统 230。安全组件可利用本地身份系统 230 来认证实体。

[0058] 作为另一示例，可向在 HTTP 协议中定义的代理能力添加安全套接字层 (SSL) 和 / 或传输层安全 (TLS) 能力。用于 HTTP 代理的当前 HTTP 协议不提供在 HTTP 代理中使用 SSL 或 TLS。当与客户机进行通信时，可增强 HTTP 代理来使用 SSL 和 / 或 TLS。SSL/TLS 也可用于互认证。作为建立连接的一部分，客户机可经由 SSL 或 TLS 来认证。在该认证方法中，安全组件可例如通过验证可信证书授权机构所签署的客户机证书来认证客户机。向 HTTP 代理添加 SSL/TLS 还能够实现端点和转发代理之间的安全（例如，加密）通信。

[0059] 在一个实施例中，在客户机和安全组件之间的第一认证之后，可向客户机提供

cookie 以便与后续请求一起使用。当前 HTTP 协议允许目标服务器向客户机提供 cookie 但不允许 HTTP 代理独立地生成 cookie 并将其供应给客户机。此外，在当前 HTTP 协议中，客户机只有在与向该客户机发送 cookie 的目标服务器进行通信时才提供 cookie。

[0060] 当转发代理用作 HTTP 代理时，转发代理（或与其相关联的安全组件）可生成 cookie 并在客户机被认证之后将其发送给客户机。在后续请求中，客户机随后可将该 cookie 发送给向该客户机提供该 cookie 的转发代理（或与其相关联的安全组件）或另一转发代理。客户机甚至还可在该客户机试图访问不同目标服务器上的资源时发送该 cookie。

[0061] 当客户机在后续请求中发送该 cookie 时，转发代理（或与其相关联的安全组件）可检查该 cookie 来判定该客户机是否已经被认证。这可避免与重新认证从客户机接收的每一请求相关联的开销。可用生存时间参数来配置 cookie 从而使得其在一设定时间后超时。

[0062] 此处使用的 cookie 包括可用于验证一实体已经被认证的任何数据。例如，cookie 可包括安全组件可用来访问数据库的记录的标识符。该记录可指示该实体是否已经被认证。作为另一示例，cookie 可包括安全组件能够解密来判定该实体是否已经被认证的加密信息。

[0063] cookie 还可包括关于实体的其他数据。例如，cookie 可包括与该实体相关联的标识符。该标识符可与该实体例如在访问企业网络时使用的标识符相对应。该标识符可在记录实体活动时使用。作为另一示例，cookie 可包括与该实体相关联的策略信息。例如，cookie 可包括指示该实体被允许访问什么站点的信息。

[0064] 可用于认证实体的另一机制是经由连接组件（例如，连接组件 125）。连接组件是驻留在设备上并监视来自设备的连接的组件。例如，连接组件可监视发送至和自设备的 TCP 通信。当连接组件看到要被路由到转发代理的连接请求时，连接组件可用与该转发代理相关联的安全组件来认证并加密该连接。这可以按照对使用设备的用户透明的方式来完成。当用户输入需要通过转发代理来路由的请求（例如，URL 请求）时，连接组件可用与该转发代理相关联的安全组件来认证该请求，然后通过安全信道将该请求转发给转发代理。

[0065] 在一个实施例中，当 cookie 被提供给实体以便在后续请求中的认证中使用时，连接组件可处理该 cookie 并在后续请求中提供该 cookie。在另一实施例中，当 cookie 被提供给实体以便在后续请求中的认证中使用时，连接组件可允许实体来处理该 cookie 并在后续请求中提供该 cookie。

[0066] 虽然上文提供了用于认证实体的某些机制的示例，但这些示例不旨在是包括一切的或限制性的。事实上，此处所描述的主题的各方面不限于该认证方法，因为基本上可以采用任何认证方法（现有的或要开发的）而不背离此处所描述的主题的各方面的精神或范围。

[0067] 作为认证过程的结果，可以获得随后可用于记录、审计、应用策略等的标识符。该标识符可由身份系统 210、本地身份系统 230、或某一其他组件来提供而不背离此处所描述的主题的各方面。该标识符可以是与用于向与实体相关联的企业网络标识该实体的标识符相同的标识符。

[0068] 虽然上述环境包括不同数量的实体中的每一个和相关基础结构，但可以理解，可

以采用更多、更少的这些实体和其他实体或这些实体和其他实体的不同组合而不背离此处所描述的主题的各方面的精神或范围。此外，该环境中包括的各实体和通信网络可以用本领域技术人员所理解的各种方式来配置而不背离此处所描述的主题的各方面的精神或范围。

[0069] 图 3 是表示根据此处所描述的主题的各方面的用安全组件来配置的示例性装置的框图。图 3 中示出的组件是示例性的且不意味着包括一切的可能需要或包括的组件。在其他实施例中，结合图 3 描述的组件或功能可被包括在其他组件中或者被放置在子组件中而不背离此处所描述的主题的各方面的精神或范围。在某些实施例中，结合图 3 描述的组件或功能可分布在装置 305 可访问的多个设备上。

[0070] 转向图 3，装置 305 可包括安全组件 310、存储 340 和通信机制 345。安全组件 310 可包括协议选择器 315、客户机组件 320、身份确认器 325、代理通知器 330、历史跟踪器 335 和报告组件 337。安全组件 310 可与结合图 1 描述的转发代理相关联。与上下文相关联意味着被包括在相同的设备上、位于不主存转发代理但可与转发代理通信的一个或多个设备上等等。

[0071] 通信机制 345 允许装置 305 与图 2 中示出的其他实体进行通信。通信机制 345 可以是结合图 1 描述的网络接口或适配器 170、调制解调器 172 或用于建立通信的任何其它机制。

[0072] 存储 340 是能够存储关于实体所参与的活动的历史信息的任何存储介质。存储 340 可包括文件系统、数据库、诸如 RAM 等易失性存储器、其它存储、以上的某种组合等，并可以分布在多个设备中。存储 340 可以在装置 305 的外部或内部。

[0073] 协议选择器 315 可用于确定要结合认证试图获取对可经由第一网络获得的资源的访问的实体来使用的认证协议。例如，参考图 2，协议选择器可确定要用于在设备 205-208 中的一个试图访问可经由网络 215 访问的资源时认证这些设备的认证协议。

[0074] 客户机组件 320 可用于使用协议选择器 315 所确定的认证协议来认证实体。实体可包括使用设备的用户和 / 或设备。例如，参考图 2，客户机组件可使用互 TLS 协议来认证使用漫游设备 205 的用户。

[0075] 身份确认器 325 可用于从身份系统获得与实体相关联的标识符。身份系统可位于本地网络上或如前所指示的客户机组件 320 外部的网络上。身份系统可访问包括用于与控制客户机组件 320 外部的网络（例如，企业网络）的企业相关联的实体的标识符的数据库。例如，参考图 2，身份确认器可与身份系统 210 通信来获得该标识符。

[0076] 代理通知器 330 可用于基于从客户机组件 320 获得的结果向转发代理指示实体是否被认证。例如，参考图 2，代理通知器可向转发代理 220-222 中的一个指示实体被认证来使用该转发代理所提供的安全功能。

[0077] 历史跟踪器 335 可用于存储标识实体和该实体访问的资源的信息。例如，参考图 2，历史跟踪器可随着使用漫游设备 205 的用户向转发代理 220 发送的每一 URL 来存储用户名。历史跟踪器 335 可利用存储 340 来存储历史信息。

[0078] 报告组件 337 可用于按标识实体和该实体访问的资源（例如，URL、网络地址等）的形式来提供历史信息。该形式可包括用户名或其他标识符，连同资源标识符。因为该信息包含足够的信息来标识企业上的实体，所以如果设备变为感染的（例如，经由恶意软件），

则当用户将设备带至企业网络时，报告可指示该设备已经被感染并需要在被允许访问企业网络之前清除。

[0079] 图 4-5 是概括地表示根据此处所描述的主题的各方面的可结合认证发生的动作的流程图。为解释简明起见，结合图 4-5 描述的方法被描绘和描述为一系列动作。可以理解和明白，此处所描述的主题的各方面不受所示出的动作和 / 或动作次序的限制。在一个实施例中，动作以如下描述的次序发生。然而，在其它实施例中，动作可以并行地发生，以另一次序发生，和 / 或与此处未呈现和描述的其它动作一起发生。此外，并非所有示出的动作都是实现根据此处所描述的主题的各方面的方法所必需的。另外，本领域的技术人员将了解和明白，方法也可以替代地经由状态图或作为事件表示为一系列相互相关联的状态。

[0080] 转向图 4，在框 405 处，动作开始。在框 407，可以建立信任关系。例如，参考图 2，本地身份系统 230 可建立与企业身份系统 210 之间的信任关系。在框 410 处，设备试图访问该设备外部的网络（例如，因特网）上的资源。例如，参考图 2，漫游设备 206 试图访问可经由网络 215 获得的资源（例如，网页）。

[0081] 在框 415 处，请求被路由到与转发代理相关联的安全组件。例如，参考图 2，连接组件 125 将请求路由到与转发代理 222 相关联的安全组件。

[0082] 在框 420 处，安全组件从设备接收消息。例如，参考图 3，安全组件 310 接收请求。

[0083] 在框 425 处，确定要用于认证与设备相关联的实体的认证协议。例如，参考图 310，协议选择器 315 确定要在认证与图 2 的漫游设备 206 相关联的用户时使用的认证协议。

[0084] 在框 430 处，安全组件认证与设备相关联的实体。例如，参考图 2 和 3，客户机组件 320 认证与漫游设备 206 相关联的用户。

[0085] 在框 435 处，当使用 cookie 时，将 cookie 发送给设备以便在后续请求中使用。例如，参考图 2，与转发代理 222 相关联的安全组件将 cookie 发送给漫游设备 206。

[0086] 在框 440 处，设备在后续请求中发送 cookie。例如，参考图 2，漫游设备 206 在对于可经由网络 215 访问的资源的后续请求中发送其接收的 cookie。

[0087] 在框 445 处，可以发生其他动作（如果存在）。例如，可以周期性地重新认证实体。

[0088] 转向图 5，在框 505 处，动作开始。在框 510 处，从与附连到第一网络的设备相关联的实体发送要访问第二网络上的资源的请求。例如，参考图 2，从与设备 206 相关联的实体发送要访问可经由网络 215 访问的资源的请求。

[0089] 在框 515 处，在通信组件处接收请求。例如，参考图 2，通信组件 125 接收请求。

[0090] 在框 520 处，经由通信组件来认证实体。例如，参考图 2，通信组件 125 与关联于转发代理 222 的安全组件通信来认证使用设备 206 的用户。

[0091] 在框 525 处，将请求发送到转发代理。例如，参考图 2，将请求从设备 206 发送到转发代理 222。

[0092] 在框 530 处，可在设备处接收 cookie。该 cookie 指示该实体先前是否已经由安全组件认证。例如，可出现这种情况来加速后续认证。

[0093] 在框 535 处，在后续请求中发送 cookie。例如，参考图 2，通信组件 125 可在对资源的后续请求中发送 cookie。

[0094] 在框 540 处，可以发生其他动作（如果存在）。

[0095] 如从上述详细描述中可以看见，已经描述了关于在分布式安全内容管理系统中的

认证的各方面。尽管此处所描述的主题的各方面易于作出各种修改和替换构造，但其某些说明性实施例在附图中示出并在上面被详细地描述。然而，应当理解，并不旨在将所要求保护主题的各方面限制于所公开的具体形式，而是相反地，目的是要覆盖落入此处所描述的主题的各方面的精神和范围之内的所有修改、替换构造和等效方案。

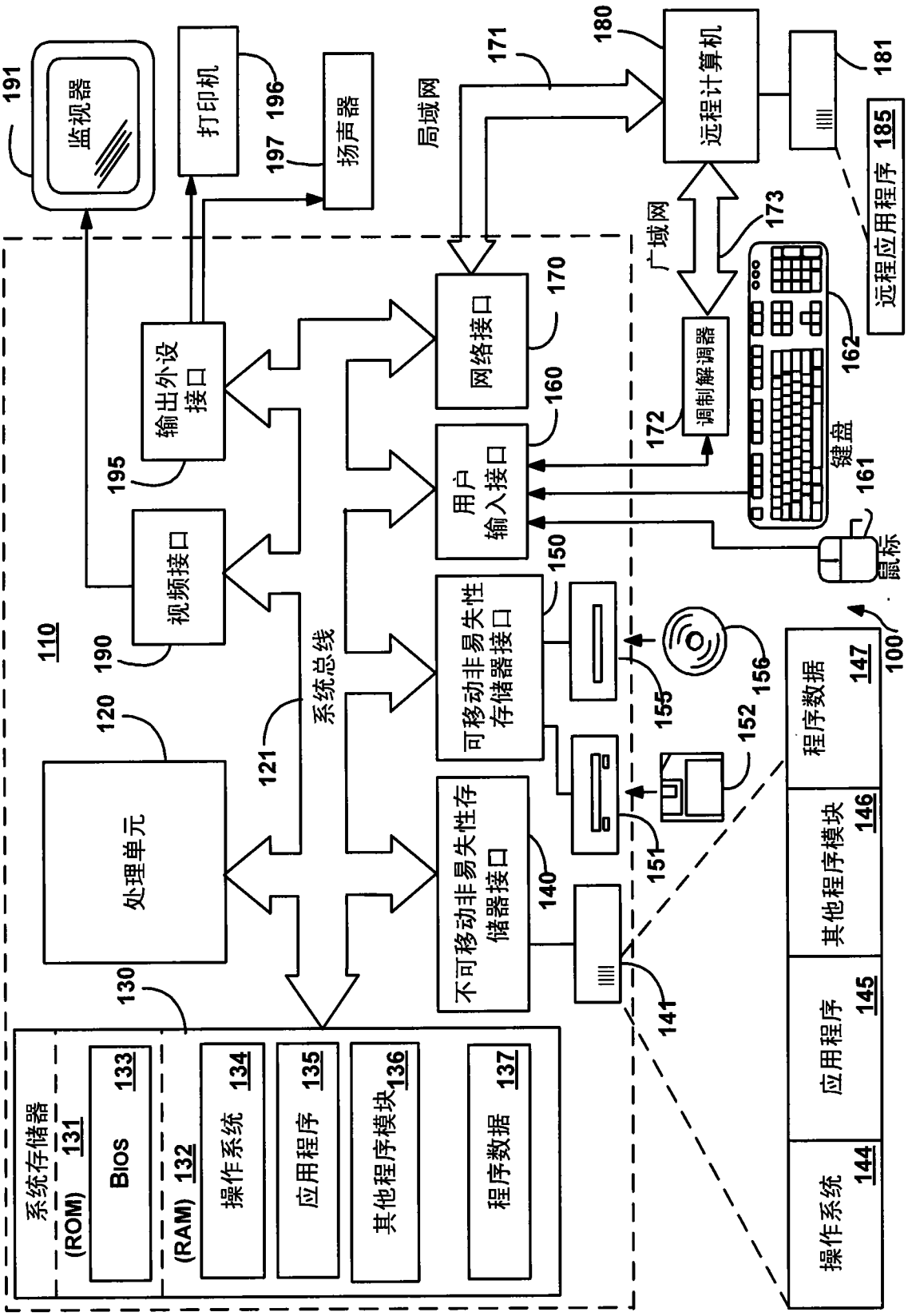

191
监视器
打印机
196
197
扬声器
局域网
171
180
远程计算机
181
远程应用程序 185
广域网
173
输出外设接口
网络接口
170
160
调制解调器
172
162
键盘
161
鼠标
195
用户输入接口
150
视频接口
190
110
120
处理单元
121
系统总线
可移动非易失性存储器接口
155
156
152
151
140
不可移动非易失性存储器接口
141
130
系统存储器
(ROM) 131
Bios 133
(RAM) 132
操作系统 134
应用程序 135
其他程序模块 136
程序数据 137
程序数据 147
100
其他程序模块 146
应用程序 145
操作系统 144

图 1

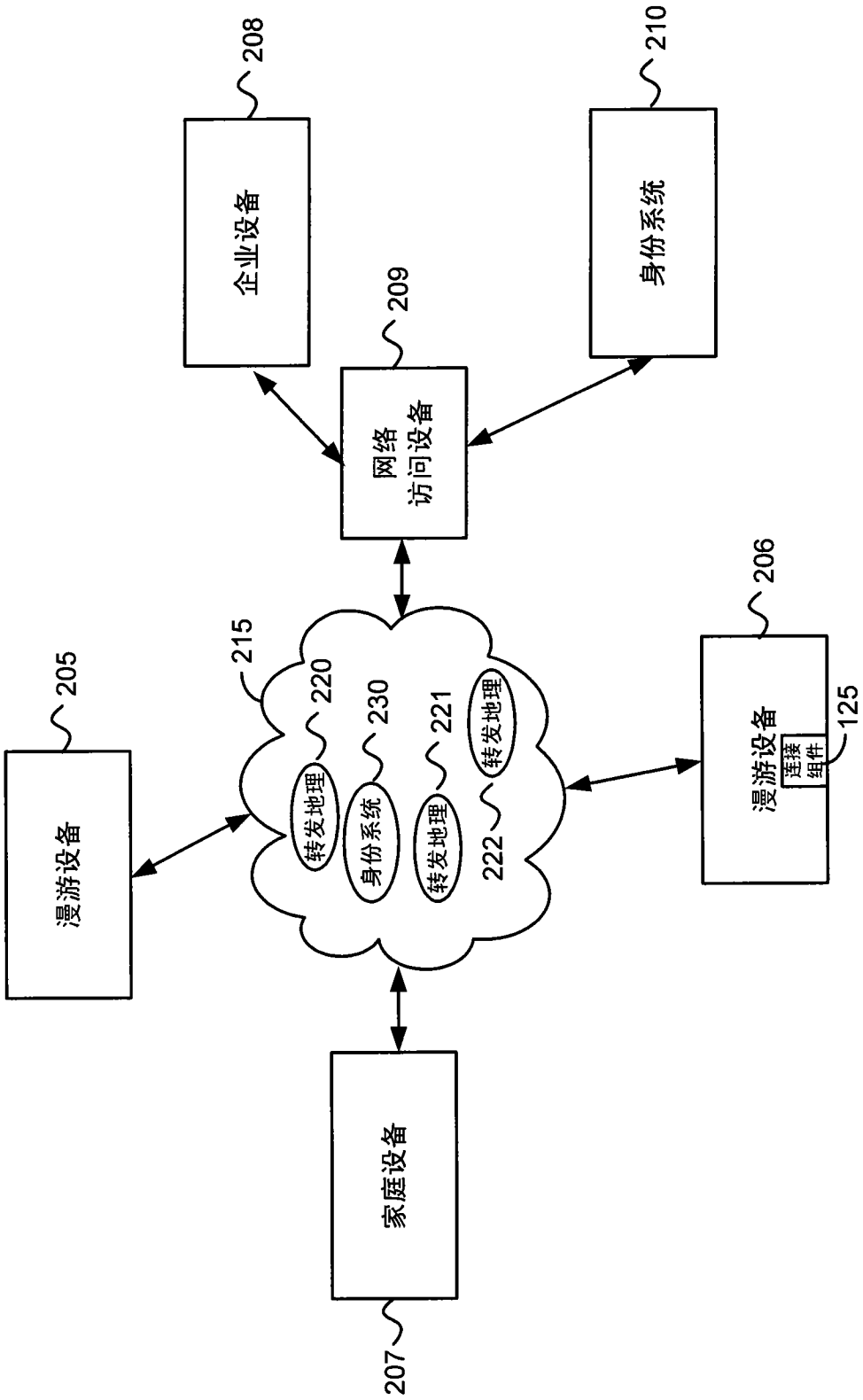

208
企业设备
210
身份系统
209
网络
访问设备
215
220
转发地理
230
身份系统
221
转发地理
222
转发地理
205
漫游设备
206
漫游设备
连接
组件
125
家庭设备
207

图 2

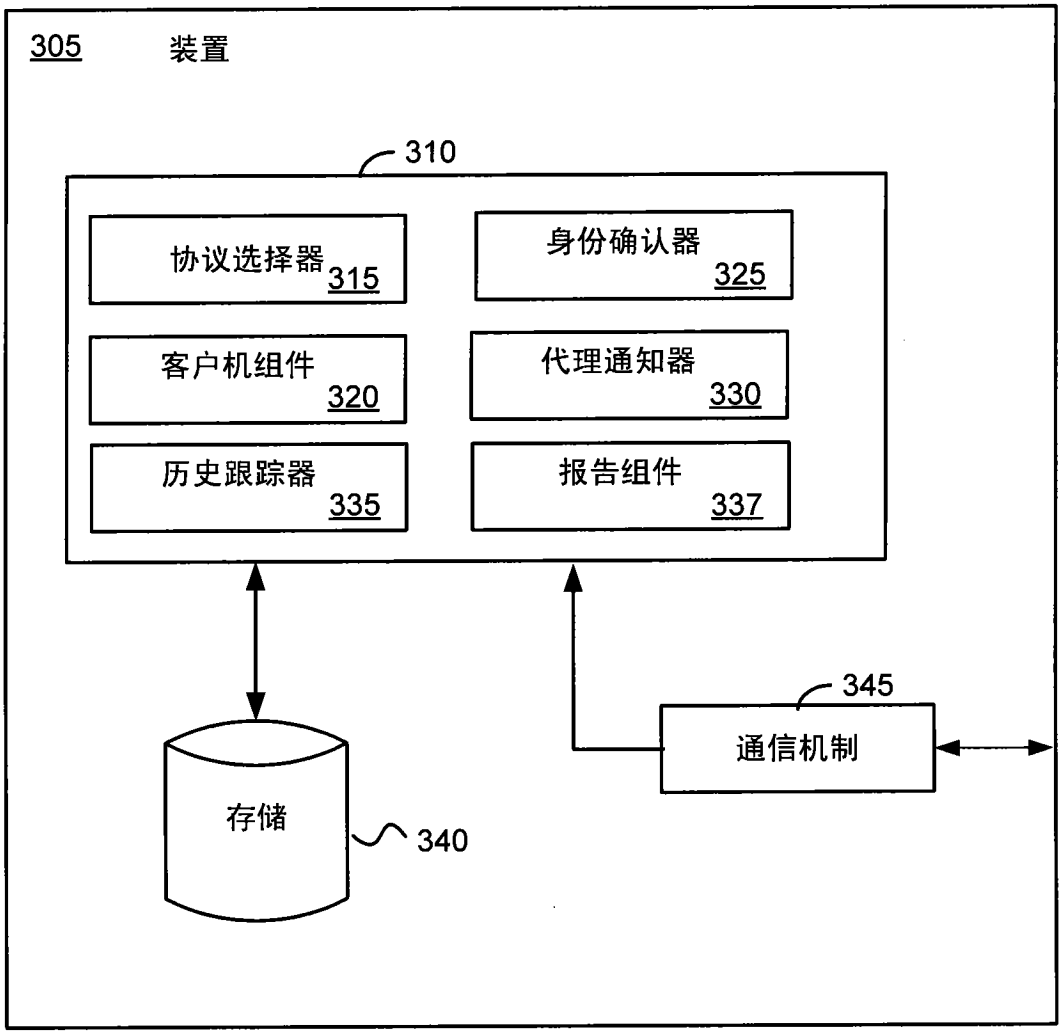

305
装置
310
协议选择器
315
身份确认器
325
客户机组件
320
代理通知器
330
历史跟踪器
335
报告组件
337
345
通信机制
存储
340

图 3

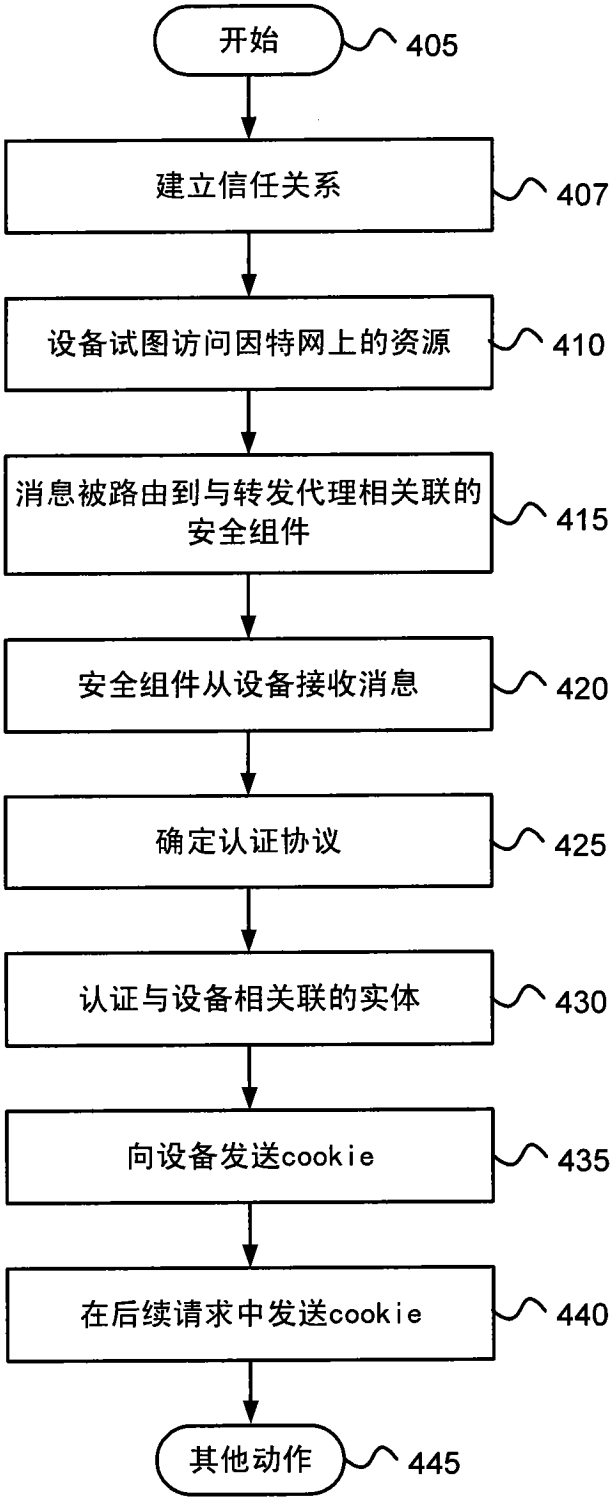

开始
405
建立信任关系
407
设备试图访问因特网上的资源
410
消息被路由到与转发代理相关联的安全组件
415
安全组件从设备接收消息
420
确定认证协议
425
认证与设备相关联的实体
430
向设备发送cookie
435
在后续请求中发送cookie
440
其他动作
445

图 4

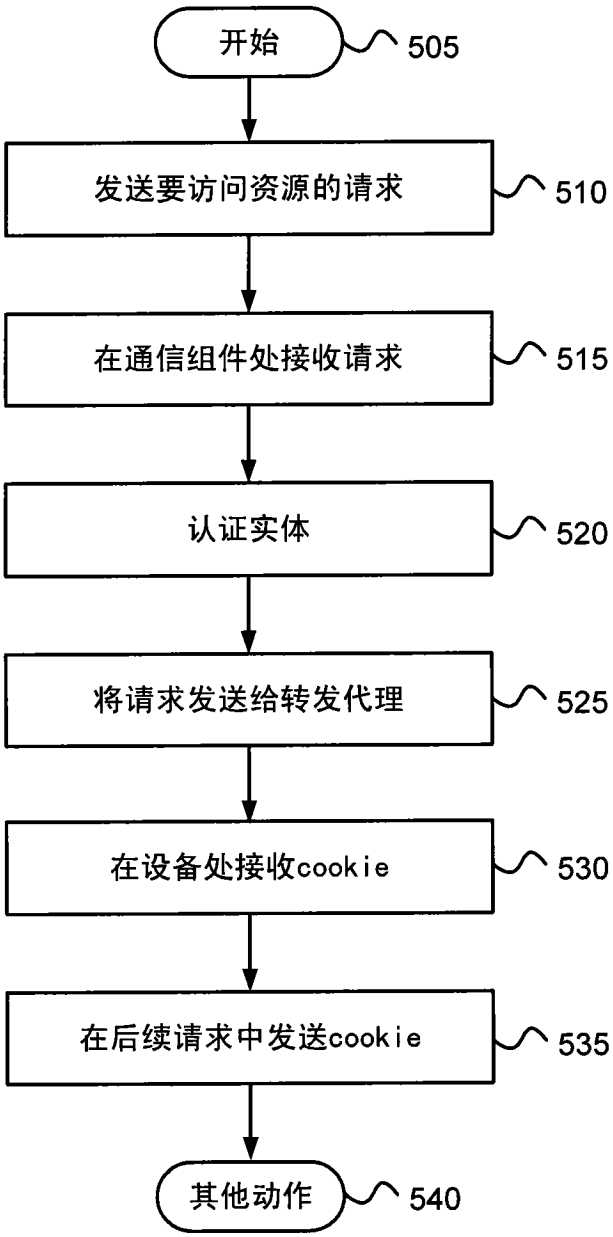

开始
505
发送要访问资源的请求
510
在通信组件处接收请求
515
认证实体
520
将请求发送给转发代理
525
在设备处接收cookie
530
在后续请求中发送cookie
535
其他动作
540

图 5