



(12) 发明专利申请

(10) 申请公布号 CN 104333567 A

(43) 申请公布日 2015. 02. 04

(21) 申请号 201410347566. 1

H04L 29/06 (2006. 01)

(22) 申请日 2014. 07. 21

(30) 优先权数据

13/947, 498 2013. 07. 22 US

(71) 申请人 思科技术公司

地址 美国加利福尼亚州

(72) 发明人 瑞迪·蒂鲁玛勒什沃尔

帕蒂尔·普拉尚斯 内什·拉梅什  
温·丹尼尔 怀尔德·克里斯多夫

(74) 专利代理机构 北京东方亿思知识产权代理

有限责任公司 11258

代理人 李晓冬

(51) Int. Cl.

H04L 29/08 (2006. 01)

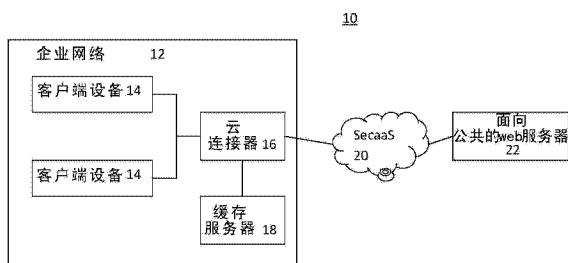
权利要求书3页 说明书12页 附图3页

(54) 发明名称

采用安全即服务的 web 缓存

(57) 摘要

本公开涉及采用安全即服务的 web 缓存。在一个实现方式中，将部署在企业场所中的 web 缓存和基于云的 SecaaS 相组合，以使得类似的基于身份的策略被实施在 SecaaS 和从 web 缓存递送的内容二者上。使用 SecaaS 在网络外部并且在网络内部针对 web 缓存的内容的基于身份的策略实现方式提供了一致的基于身份的安全，同时仍然高性能地将内容提供给最终用户。由 SecaaS 检查和 / 或修改的内容可以被缓存在企业场所中，以使得对来自原始服务器的内容的请求减少。流内容的本地缓存可以降低延时同时基于身份的策略的本地实现方式继续适当地限制流式传输内容。基于身份的策略的本地实现方式可以降低 SecaaS 上的负载。对于 web 内容，不使用由服务提供商提供的内容递送网络而使用企业内的缓存服务器。



1. 一种方法,包括:

在网络的云连接器设备处拦截来自用户的对内容的请求;

当所述内容未被缓存在所述网络中时:

将所述请求重定向至基于云的安全即服务服务器;

从所述基于云的安全即服务服务器接收所述内容;

将所述内容路由至缓存服务器;以及

在云连接器处从所述基于云的安全即服务服务器接收针对所述内容的基于身份的安全策略;

当所述内容被缓存在所述网络中时:

确定所述请求是否满足基于身份的安全策略;

当所述请求满足所述基于身份的安全策略时,将所述请求发送至缓存服务器;以及

当所述请求不满足所述基于身份的安全策略时,拒绝所述请求。

2. 如权利要求1所述的方法,其中,拦截包括:拦截在所述云连接器设备处接收到的、包括所述请求在内的所有请求,并且其中,包括被路由到所述缓存服务器的所述内容在内的所有缓存的内容在进行缓存之前由基于云的安全即服务服务器进行过滤。

3. 如权利要求1所述的方法,其中,在网络的云连接器设备处进行拦截包括:采用在企业网络的边界路由器处的透明代理进行拦截。

4. 如权利要求1所述的方法,还包括:存储可缓存的目标统一资源定位符列表,并且确定所述内容是否是从所述可缓存的目标统一资源定位符缓存来的。

5. 如权利要求1所述的方法,其中,重定向包括:重定向至所述网络外部的安全即服务服务器。

6. 如权利要求1所述的方法,其中,接收所述内容包括:在由基于云的安全即服务服务器对所述内容进行过滤之后接收所述内容。

7. 如权利要求1所述的方法,其中,路由所述内容包括:将所述内容路由至缓存服务器以进行缓存,并且由所述缓存服务器以所述内容对来自客户端而不是所述缓存服务器的请求做出响应。

8. 如权利要求1所述的方法,还包括:通知安全即服务服务器在所述网络中进行web缓存,其中,接收所述内容包括:接收与由内容服务器所提供的内容相比具有更改的缓存头部的内容。

9. 如权利要求8所述的方法,其中,接收所述具有更改的缓存头部的内容包括:接收具有不缓存指示的内容。

10. 如权利要求1所述的方法,其中,确定所述请求是否满足所述基于身份的安全策略包括:由用户、用户群组、设备群组、安全许可、来源的位置或他们的组合确定所述请求的来源的身份。

11. 如权利要求1所述的方法,还包括:从基于云的安全即服务服务器接收基于身份的安全策略,其中,确定所述请求是否满足所述基于身份的安全策略包括:采用与在所述安全即服务服务器处进行确定所采用的相同策略在所述云连接器设备处针对所述缓存的内容进行确定。

12. 如权利要求1所述的方法,其中,确定所述请求是否满足基于身份的安全策略包

括：确定对于所述内容的所述请求的来源的身份是否在白名单或黑名单中。

13. 如权利要求 12 所述的方法，其中，还包括：在所述身份不在所述白名单或所述黑名单中的情况下，向所述安全即服务服务器请求策略。

14. 一种编码在一个或多个非暂态计算机可读介质中的逻辑，所述逻辑包括用于运行的代码并且当所述代码由处理器运行时可操作以执行以下操作，所述操作包括：

在网络内从所述网络外部的安全即服务服务器接收基于身份的安全信息；

从识别出的来源接收对缓存在所述网络内的内容的请求；

采用所述基于身份的安全信息核实所述识别出的来源被允许访问缓存在所述网络内的所述内容；以及

将所述内容提供给所述识别出的来源。

15. 如权利要求 14 所述的编码在一个或多个非暂态计算机可读介质中的逻辑，其中，接收基于身份的安全信息包括：接收用户身份、用户群组身份、位置身份、设备身份或它们的组合以及由所述安全即服务服务器实现的相应的安全策略，并且其中，核实包括：将所述安全策略应用到对所缓存的内容的请求。

16. 如权利要求 14 所述的编码在一个或多个非暂态计算机可读介质中的逻辑还包括：确定所述内容被缓存在所述网络内，所缓存的内容包括由基于云的安全即服务过滤后的内容，其中，核实包括：对缓存在所述网络中的所述过滤后的内容实现基于身份的安全。

17. 如权利要求 14 所述的编码在一个或多个非暂态计算机可读介质中的逻辑还包括：

接收对未被缓存在所述网络中的内容的进一步请求；

将所述进一步请求重定向至安全即服务；

从所述安全即服务接收对所述进一步请求的响应；以及

提供所述响应以在所述网络中进行缓存。

18. 如权利要求 17 所述的编码在一个或多个非暂态计算机可读介质中的逻辑，其中，所述响应包括：响应于所述进一步请求的进一步内容，所述进一步内容包括：具有由安全即服务服务器调整的缓存寿命的安全过滤后的内容。

19. 一种装置，包括：

连接至网络的客户端设备，所述客户端设备被配置来请求内容；以及

所述网络的网关设备，所述网关设备被配置来响应于所述请求，根据基于云的安全即服务的基于身份的安全策略，约束对所述网络内缓存的内容的供应。

20. 如权利要求 19 所述的装置，还包括存储所述缓存的内容的缓存服务器，所述缓存的内容的寿命由安全即服务设置为与所述内容的来源的设置不同。

21. 一种方法，包括：

在安全服务处理器处从企业网络中的主机接收对内容的请求；

从 web 服务器请求所述内容；

响应于所述请求，从所述 web 服务器接收所述内容；

由所述安全服务处理器过滤从所述 web 服务器接收到的内容；

调整所述内容的新鲜度设置，所述新鲜度设置与缓存相对应；以及

将具有调整的新鲜度设置的所述内容传送至所述企业网络作为对所述请求的响应。

22. 如权利要求 21 所述的方法，还包括：

将基于身份的安全策略传送至所述企业网络中的云连接器,以使用所述基于身份的安全策略从所述网络内的缓存提供所述内容。

## 采用安全即服务的 web 缓存

### 技术领域

[0001] 本公开总体涉及计算机网络领域,更具体地涉及采用基于云的安全即服务(security as a service)的web缓存。

### 背景技术

[0002] 企业网络可以缓存 web 内容。web 缓存通过缓存受欢迎的内容增强了内容的端到端传输。需求量最大的内容缓存在网络内的服务器上以将这些内容高可靠性且高性能地供应给终端用户。企业部署 web 内容的缓存来降低带宽需求、降低服务器负载、并且改善对存储在缓存中的内容的客户端响应时间。

[0003] 作为安全措施,内容被过滤。企业部署执行应用协议检测 / 解密、深度分组检查、启发式方法和 / 或网络内的其他功能以检测恶意软件、利用脚本、防止数据泄漏或以其他方式保护网络的安全装置。可能将这些基于网络的安全处理应用到缓存的内容。另一种用于企业网络的安全是基于云的“安全即服务”(SecaaS)。SecaaS 提供可扩展的安全。使用 SecaaS,企业受益于市场主导的 web 安全,在节省带宽、资金和资源的同时快速且容易地保护网络免受基于 web 的威胁。然而, SecaaS 被提供于网络外部,因此可能无法实现针对网络内缓存的内容的基于身份的安全策略。

### 发明内容

[0004] 本公开一方面提供了一种方法,包括:在网络的云连接器设备处拦截来自用户的对内容的请求;当内容未被缓存在网络中时:将该请求重定向至基于云的安全即服务服务器;从基于云的安全即服务服务器接收内容;将该内容路由至缓存服务器;以及在云连接器处从基于云的安全即服务服务器接收针对该内容的基于身份的安全策略;当内容被缓存在网络中时:确定请求是否满足基于身份的安全策略;当请求满足基于身份的安全策略时,将请求发送至缓存服务器;以及当请求不满足所述基于身份的安全策略时,拒绝该请求。

[0005] 本公开另一方面提供了一种编码在一个或多个非暂态计算机可读介质中的逻辑,该逻辑包括用于运行的代码并且当这些代码由处理器运行时可操作以执行以下操作:在网络内从网络外部的安全即服务服务器接收基于身份的安全信息;从识别出的来源接收对缓存在网络内的内容的请求;采用基于身份的安全信息核实识别出的来源被允许访问缓存在网络内的内容;以及将内容提供给识别出的来源。

[0006] 本公开另一方面提供了一种装置,包括:连接至网络的客户端设备,该客户端设备被配置来请求内容;以及网络的网关设备,该网关设备被配置来响应于请求,根据基于云的安全即服务的基于身份的安全策略,约束对网络内缓存的内容的供应。

[0007] 本公开还提供了一种方法,包括:在安全服务处理器处从企业网络中的主机接收对内容的请求;从 web 服务器请求内容;响应于请求,从 web 服务器接收内容;由安全服务处理器过滤从 web 服务器接收到的内容;调整内容的新鲜度设置,该新鲜度设置与缓存相

对应；以及将具有调整的新鲜度设置的内容传送至企业网络作为对请求的响应。

## 附图说明

- [0008] 为提供对本公开以及其特征和优点更加完整的理解，结合附图，参照以下说明，其中，相同的参考序号表示相同的部分，其中：
- [0009] 图 1 是用于采用安全即服务的 web 缓存的示例网络的简化框图；
- [0010] 图 2 是用于获得安全信息的方法的一个实施例的流程图；
- [0011] 图 3 是从云连接器的角度的、用于采用安全即服务的 web 缓存的方法的一个实施例的流程图；
- [0012] 图 4 是采用安全即服务的 web 缓存的示例的通信示意图；
- [0013] 图 5 是从安全即服务服务器的角度的、用于采用安全即服务的 web 缓存的方法的一个实施例的流程图；
- [0014] 图 6 是根据一个实施例，用于采用安全即服务的 web 缓存的网络设备的框图。

## 具体实施方式

[0015] 缓存的内容由 SecaaS 过滤。然而，请求者的身份可能改变，因此，对缓存的内容来说，基于身份的安全是在安全方面的缺口。当缓存中内容不可用时，云连接器能够从 web 缓存获取或将流量重定向至 SecaaS。为安全，云连接器将 HTTP 流量重定向至 SecaaS。它还收集用户身份，以便 SecaaS 能够在云上提供基于身份的安全。这隐含着云连接器不知道云上的策略。另一方面，随着 web 缓存的出现，从 web 缓存而不是从内容服务器获得缓存的内容。不将流量重定向至 SecaaS。

[0016] 将 web 缓存和 SecaaS 组合起来，以使得在 SecaaS 和从 web 缓存递送来的内容二者上实施类似的基于身份的策略。在使用 SecaaS 的企业网络外且在用于 web 缓存的内容的网络内的基于身份的策略实现方式在高性能地将内容提供给终端用户的同时还提供了一致的基于身份的安全。可以将由 SecaaS 检查的和 / 或修改的内容缓存在企业场所中，以使得对来自源服务器的内容的请求减少，从而释放互联网带宽并降低访问时间。对流内容的本地缓存可以降低延时，同时基于身份的策略的本地实现方式适当地持续限制内容的递送。基于身份的策略的本地实现可以降低 SecaaS 上的负载。虽然 CDN（内容递送网络）是由互联网服务提供商（ISP）提供的，但是这对于附连到企业网络的最终用户将不是高效的，因为内容请求将由云连接器重定向至基于云的 SecaaS。因此，企业将要在企业本身中部署 web 缓存。

[0017] 在一方面，提供了一种方法。在网络的云连接器设备处拦截来自用户的对内容的请求。当该内容没被缓存在该网络中时，该请求由云连接器重定向至基于云的安全即服务，从基于云的安全即服务接收该内容，并且该内容由云连接器路由至缓存服务器。当该内容被缓存在该网络中时，处理器确定该请求是否满足基于身份的安全策略。当该请求满足基于身份的安全策略时，将该请求发送至缓存服务器，而当该请求不满足基于身份的安全策略时，拒绝该请求。

[0018] 在另一方面，将逻辑编码到一个或多个非暂态的计算机可读介质中。该逻辑包括用于运行并且当由处理器运行可操作以执行各种操作的代码。基于身份的安全信息从网络

外的基于云的安全即服务接收到该网络内。从识别的来源接收对缓存在网络内的内容的请求。基于身份的安全信息被用来核实该识别的来源被允许访问缓存在该网络内的内容。将该内容提供给该识别的来源。

[0019] 还有在另一个方面,客户端设备连接到企业网络。该客户端设备被配置来请求内容。该网络的网关设备被配置来响应于该请求,基于从基于云的安全即服务接收到的基于身份的安全策略,约束对该网络内缓存的内容的供应。

[0020] 在其他方面,基于云的安全即服务接收来自企业网络的对内容的请求。从 web 服务器请求该内容。响应于该请求,从 web 服务器接收该内容。基于云的安全即服务过滤从 web 服务器接收到的内容,并且调整该内容的新鲜度设置。新鲜度设置与缓存相对应。作为对该请求的响应,将具有调整的新鲜度设置的内容传送至企业网络。

[0021] 将网络内的 web 缓存和 SecaaS 结合以在能将内容高性能地提供给最终用户的同时还提供安全。一套机制确保这两种方案按照要求工作。为提供一致的安全,云连接器实现基于身份的安全策略。缓存的内容已经由 SecaaS 过滤。甚至对从 web 缓存检索到的内容,企业可以实施身份策略。SecaaS 通过提供可以是由云连接器使用的白名单或黑名单的优化的 URL 列表来优化 web 缓存方案。

[0022] 图 1 显示了用于采用基于云的安全即服务的 web 缓存的示例网络 10。网络 10 或其一部分是用于采用安全即服务的 web 缓存的装置。对于非缓存的内容,基于身份的策略由 SecaaS 来实现,并且,对于缓存的内容,基于身份的策略在企业网络 12 中实现。旨在将相同的基于身份的安全策略用于内容和 / 或位置两种类型。

[0023] 网络 10 包括连接到其他服务器和 / 或网络(比如,SecaaS 网络或服务器 20 和面向公共 web 服务器 22)的企业网络 12。企业网络 12、SecaaS 服务器 20 和 web 服务器 22 包括各种网络设备,包括一个或多个客户端设备 14、网关或云连接器 16、缓存服务器 18、安全即服务服务器 20 以及面向公共 web 服务器 22。企业网络 12 与更广的网络 10 相连接或是更广的网络 10 的一部分。采用安全即服务的 web 缓存在企业网络 12 和 / 或 SecaaS 服务器 20 上进行操作。企业网络 12 通过线路或无线地与诸如互联网之类的其他网络相连接。SecaaS 服务器 20 和面向公共 web 服务器 22 是一个或多个其他网络的一部分或可通过一个或多个其他网络进行访问。SecaaS 服务器 20 由企业网络 12 外部的一个或多个服务器来实现。类似地,web 服务器 22 由企业网络 12 外部的一个或多个服务器来实现。可以使用任意现在所知的或之后开发的 SecaaS 服务器 20 和 / 或 web 服务器 22。

[0024] 可以提供附加的、不同的或更少的部件。例如,提供附加的客户端设备 14。如另一个示例,可以提供附加的云连接器 16 和 / 或缓存服务器 18。可以使用任意数目的用于提供安全即服务、缓存和 / 或 web 服务的服务器。

[0025] 企业网络 12 显示为框,但可以是连接到局域网、广域网、内联网、虚拟局域网、互联网或网络的组合的许多不同设备。可以提供任意形式的网络,例如,传输网络、数据中心或其他有线的或无线的网络。网络 12 可以跨平台适用、可扩展和 / 或通过连接性的链路协商(link-negotiation)适应于专用平台和 / 或技术要求。

[0026] 企业网络 12 的网络设备 14、16、18 处于相同的房间、建筑物、设施或校园。在其他的实施例中,企业网络 12 由分布在整个地区(例如,多个州和 / 或国家)的设备形成。企业网络 12 是由或为给定实体所有、操作和 / 或运行的网络(例如,针对企业操作的 Cisco

网络)。

[0027] 网络设备通过端口经由链路连接。可以使用任意数目的端口和链路。这些端口和链路可以使用相同或不同的介质来通信。可以使用无线网、有线网、以太网、数字用户线路(DSL)、电话线、T1 线、T3 线、卫星、光纤、电缆和 / 或其他链路。提供相应的接口作为端口。

[0028] 可以提供任意数目的客户端设备 14。客户端设备 14 是计算机、平板电脑、蜂窝电话、支持 wifi 的设备、膝上计算机、主机或通过企业网络 12 访问内容的其他用户设备。客户端设备 14 通过诸如以太网电缆之类的线路或使用诸如 wifi 之类的无线地连接到企业网络 12。连接可以相对固定,例如,对于通过线路连接至交换机的个人计算机。连接可以是暂时的,例如,与按照需要或当在范围中时访问企业网络 12 的移动设备相关联的连接。

[0029] 客户端设备 14 被配置来请求 web 内容。例如,在客户端设备 14 之一上操作的浏览器根据 TCP/IP 来请求 web 内容。如另一个例,根据企业网络 12 中用于通信的任意标准,应用请求更新或其他信息。

[0030] 所请求的内容位于 web 服务器 22 上。为更快的响应,所请求的内容可以已经被缓存在网络内。一个或多个缓存服务器 18 将先前所请求和所获得的内容存储在企业网络 12 内。缓存服务器 18 可以预获取并存储预期将被请求的内容。

[0031] 缓存服务器 18 是诸如服务器卡和 / 或数据库之类的服务器。可以使用其他网络设备,例如,路由器、网关或网桥。缓存服务器 18 是处理设备。由缓存服务器 18 来处理数据,例如,响应于客户端请求和 / 或基于编程来提供缓存的内容。当所请求的内容没有被存储和 / 或到期时,缓存服务器 18 可以被配置来获得原始内容。

[0032] 可以使用任意内容缓存。在一个实施例中,缓存操作依赖于随内容提供的头部信息。头部可以指示适合于该内容的寿命、新鲜度或期限。例如,相对静态的内容可以指示可允许缓存数小时或数天。只要该内容在可缓存的周期内通过请求被获得,该缓存的内容就可以被使用。如果该内容到期,那么该内容不从缓存中供应。

[0033] 云连接器 16 是企业网络 12 的网关设备。云连接器 16 是网络接口卡、边界路由器、其他路由器、防火墙或其他网络设备。作为网关设备,云连接器 16 将企业网络 12 与诸如互联网中的 SecaaS 服务器 20 之类的其他网络相接合。云连接器 16 是用于与缓存服务器 18、客户端设备 14 和 / 或基于云的 SecaaS 20 进行通信的处理设备。还可以提供与其他网络设备的通信。

[0034] 云连接器 16 由软件和 / 或硬件配置来对缓存的内容实现基于身份的策略。响应于客户端请求而对网络内缓存内容的进行供应被约束。该约束基于 SecaaS 20 的基于身份的安全策略。一致的身份策略由云连接器 16 和 SecaaS 服务器 20 来实施。在可替代的实施例中,不同的基于身份的策略可以用于缓存的内容与非缓存的内容。

[0035] 即使对于缓存的内容,其他安全过滤由 SecaaS 服务器 20 提供。任何缓存的内容都是从 SecaaS 服务器 20 接收的,因此,在缓存之前已经被安全过滤。由于缓存内容的请求者的身份可以与原始请求者的身份不同,因此,针对每个请求实现基于身份的安全。

[0036] 网络 10 的各个部件由硬件和 / 或软件配置以提供缓存、SecaaS、供应内容或其他操作。逻辑被编码在一个或多个非暂态的计算机可读介质中,以操作云连接器 16、缓存服务器 18 和 / 或 SecaaS 服务器 20。该介质是存储器。可以使用企业网络 12 内部或外部的存储器。该逻辑包括用于由诸如云连接器 16 的处理器之类的一个或多个处理器运行的代码。

当由处理器运行时,该代码用来执行用于缓存、供应缓存的内容和基于身份的安全的操作。该逻辑代码配置设备以执行操作。

[0037] 图 2 和图 3 显示了从云连接器 16 的角度的、用于采用基于云的安全即服务 (SecaaS) 的 web 缓存的方法的实施例。图 2 针对用于获得基于身份的安全策略的初始化、更新或周期性操作。该操作在不考虑任何客户端请求的情况下出现,并且 / 或者该操作被作为对内容的请求的响应的过程的一部分来触发。

[0038] 图 3 针对响应于来自网络内的客户端对内容的请求。采用基于云的安全即服务的 web 缓存的组合被实现为程序,例如,由 WebSocket 创建的程序。可以创建协议来定义操作,或者程序不需要专用协议定义进行操作。

[0039] 图 5 针对 SecaaS 的操作。SecaaS 与企业网络进行交互来为内容提供安全和 / 或提供基于身份的策略以由企业网络来实现。

[0040] 图 2、图 3 和图 5 的方法由图 1 的网络、由云连接器 (图 3)、由 SecaaS 服务器 (图 5)、由其他企业网络设备、或由其他网络或软件来实现。各种设备和相应应用的任意一种可以实现这些方法的全部或者一部分。可以提供附加的、不同的或更少的动作。例如,这些方法针对为给定的请求服务。对于其他请求,重复这些动作的一些或者全部。以所示顺序或不同的顺序执行这些动作。

[0041] 参照图 2,在动作 30 中,将网络中的 web 缓存通知给基于云的安全即服务。该网络将在缓存的内容上执行基于身份的安全。为了提供一致的基于身份的策略,安全即服务被通知来同步策略。云连接器 16 或其他企业网络设备请求基于身份的安全策略或其他信息。可替代地,实现不同的策略,并且不执行图 2 的动作。在另一个选项中,在动作 32 中通过推送来提供策略,因此,不需要来自网络的通知或请求。而在另一个选项中,通过人工或半自动的配置,管理员确保在两个位置实现相同的策略。

[0042] 通知作为建立缓存时的初始动作出现。可替代地或附加地,通知周期地出现,例如更新策略信息。在其他实施例中,通知可以响应于触发而出现。

[0043] 在动作 32 中,从 SecaaS 接收基于身份的安全策略。响应于请求,从 SecaaS 提供与身份相关联的安全策略。SecaaS 是企业网络外、用于安全策略的集中的资源,因此,提供策略以由云连接器 16 使用。在其他实施例中,从其他资源提供策略,例如,从网络内广播或分发的资源。策略可以起源于企业网络内部或外部。

[0044] 策略与安全有关,例如,限制访问。限制可以出于威胁或攻击原因,或者可以出于其他原因。例如,对企业网络的雇员限制内容,例如,不允许赌博相关内容。客人可以被允许赌博内容。如另一示例,与可能的网络威胁相关联的内容被限制到只有具有处理这样威胁的技能 (training) 的雇员。策略可以是以规则陈述、一个或多个列表、至资源的链路或该策略的其他指示的形式。

[0045] 在一个实施例中,将基于身份的安全策略作为一个或多个列表来提供,例如,一个或多个白名单和一个或多个黑名单。白名单指示被允许访问各类内容的用户群组。黑名单指示不被允许访问各类内容的用户群组。其他因素可以用于包含在或不包含在给定的列表中,例如,基于 URL 而不是内容类型的列表。可以为不同类型的内容和 / 或具体的内容提供分开的列表。可替代地,列表包括通过不同类型的内容进行不同分组的指示。可以使用考虑允许或不允许通过身份访问内容的任意格式和因素。提供针对不同身份的安全策略。

[0046] 可以使用任意身份分类。在一个实施例中，身份是用户。在上述示例中，用户可以是客人或雇员。可以提供其他分组，例如，承包人或不是承包人。可以使用其他标识。例如，用户的位置为标识，例如，位于公共空间的用户与位于私有或约束空间的用户。另一标识可以是客户端设备的类型。例如，内容约束对于私有客户端设备与公共客户端设备可以是不同的。如另一个示例，内容约束对于蜂窝电话或移动电话可以不同于个人计算机或固定设备。可以提供这些不同类型的基于身份的群组的组合。

[0047] 可以从 SecaaS 提供其他信息。例如，SecaaS 提供将被缓存的内容。因此，SecaaS 可以记载或记录缓存的信息的列表和该缓存的内容的相关联的寿命。在其他实施例中，云连接器和 / 或缓存服务器记载或记录缓存的内容的列表。该列表可以由统一资源定位符 (URL) 标识，但可以使用其他标识。在可替代的实施例中，SecaaS 提供内容类型的指示（例如，可缓存的目标 URL）和由该类型使用的相应的寿命。

[0048] 参照图 3，显示了云连接器 16 的操作。其他企业网络设备可以执行这些动作中的一个或多个动作，例如，缓存服务器 18 执行这些动作的子集或全部。在此将参照图 4 的示例对图 3 的动作进行描述。图 4 显示了包括客户端、云连接器、缓存服务器、SecaaS 和内容提供商的通信和相应动作的示例通信示意图。也可能是其他示例。

[0049] 诸如客人“bob”之类的客户端生成对内容的请求。在该示例中，该内容与赌博相关联或涉及赌博。将该请求提供给云连接器。该请求被提交 (address) 至内容提供商以供应所请求的内容。

[0050] 在动作 40 中，云连接器拦截来自用户的请求。该请求可能不可被提交到云连接器，但是云连接器沿着针对该请求的传送或路由的路径，从而对该请求进行检查。在其他实施例中，该请求被定向到云连接器，因此，云连接器通过接收进行拦截。由于该请求是针对不由云连接器供应的内容的，因此，该请求被拦截。

[0051] 云连接器作为透明代理 (transparent proxy) 进行操作。任何对于内容的请求通过云连接器进行路由，因此，所有的请求都可被拦截。在提供多个云连接器的情况下，每个给定的云连接器拦截通过给定云连接器进行路由或在给定云连接器处被接收的所有对于内容的请求。针对任何给定请求，透明代理允许客户端设备、缓存服务器以及 SecaaS 进行操作就像云连接器不是 web 缓存和 SecaaS 操作的一部分。适合于请求和对内容的请求的响应的寻址和路由对于缓存和 / 或 SecaaS 是相同的。

[0052] 请求是针对被缓存的内容或没被缓存的内容。一些请求可以针对缓存的内容。其他请求可以针对未缓存的内容。客户端可能不知道该内容是否被缓存。缓存操作根据任意缓存方法发生。对于缓存的内容，云连接器将对内容的请求从网络外的 web 服务器重新路由到该网络内的缓存服务器，对于未缓存的任意内容，云连接器将请求转发到 web 服务器。可替代地，云连接器将所有请求定向到缓存服务器。缓存服务器提供缓存的内容或者将请求转发回云连接器以从 web 服务器获得内容。

[0053] 在动作 42 中，确定请求的来源的身份。解析请求。请求的头部包括标识信息，例如，客户端设备的类型，设备的位置，与该设备相关联的用户，登录信息，传输连接，或者客户端、客户端设备或用户的其他标识特点。连接器可以使用多种机制中的任意一种机制来得知用户身份。可以从诸如活动目录 (Active Directory) /AAA 服务器之类的会话目录或者通过诸如 web 认证、NTLM 或 Kerberos 之类的认证机制来得知身份。

[0054] 针对请求确定该请求的来源（即，客户端）。来自请求自身的身份信息被用作标识。在其他实施例中，来自请求的信息被用来确定进一步的身份信息。例如，客户端设备地址的指示被用来查找登录到该设备的当前用户或者当前的连接类型或该设备的位置。该查找可以通过对另一个设备的请求、对客户端设备的请求和 / 或由云连接器进行的本地查找进行。可以使用用于 SecaaS 或其他策略实现方式的任意身份确定或处理。

[0055] 从所标识的来源接收对缓存的内容或非缓存的内容的请求。该标识由云连接器针对缓存的内容并且由 SecaaS 针对非缓存的内容用于基于身份的安全策略。

[0056] 在动作 44 中，云连接器确定所请求的内容是否被缓存在网络内。例如并如图 4 中所示，云连接器将请求转发至缓存服务器。缓存实现方式可以首先从缓存中寻找内容。如果缓存服务器响应该内容没有被缓存，那么云连接器确定没有缓存。如果缓存服务器以缓存的内容做出响应，那么云连接器确定缓存。缓存服务器维护针对缓存的内容的统一资源定位符的列表。可替代地，云连接器维护该列表，并且在不需要转发给缓存服务器的情况下进行确定。

[0057] 在其他实施例中，在动作 52 中请求所寻找的内容是否违反基于身份的策略的判定，在不需要对该内容是否被缓存进行确定或在此之前被执行。云连接器可以执行基于身份的策略验证，而不考虑该内容是否被缓存，避免 SecaaS 不得不执行基于身份的核实。

[0058] 动作 46、48 和 50 与当内容没被缓存在网络中时所采取的行动相对应。当最终用户或客户端从缓存服务器请求内容时，云连接器已经意识到该内容在使用列表（例如，针对可从该站点（标称为 WCache）访问的内容的可缓存的目标 URI 和目标寿命）的缓存中不可得，并且将该请求转发至缓存服务器。在缓存的一种实现方式中，缓存服务器被配置来从内容提供商请求未缓存的内容。

[0059] 在动作 46 中，云连接器将对内容提供商的请求重定向至基于云的安全即服务。由于新的内容正被寻找，因此，该内容将通过安全即服务进行路由，并且由安全即服务进行处理。改变寻址，以使得网络外的安全即服务接收该请求。该过程针对与未缓存的内容相关联的任意请求来执行。云连接器将针对原始内容提供商的流量重定向至 SecaaS。SecaaS 实施 web 过滤策略，因此，该请求被路由至 SecaaS，以使得响应的内容也经过 SecaaS 进行过滤。

[0060] 参照图 4，SecaaS 接收对内容的请求。SecaaS 检查请求或流量，并且获取响应。该检查是针对 URL，以确保 URL 满足安全策略。这可以是基于身份、基于内容和 / 或其他策略。如果满足，那么响应于该请求，从内容提供商接收内容。

[0061] SecaaS 过滤任何所接收到的内容。可以使用任意策略。例如，该内容可以针对多种“粉色”或肤色进行检查。如另一个示例，可以执行字搜索来识别不被允许的具体的字或字串。SecaaS 使流量经受深度分组检查、行为分析、启发式方法、应用识别或其他处理。可以使用任意 SecaaS 处理。

[0062] 在其他实施例中，内容被提供给云连接器，而不需要特别对于响应的内容通过 SecaaS 进行路由。内容和 / 或身份策略由 SecaaS 通过检查请求和相应的 URL 而不是响应的内容本身来实现。

[0063] 在动作 48 中，从 SecaaS 服务器和 / 或 web 服务器来接收内容。响应于对没有被缓存的内容的请求，接收该内容。在企业网络的操作期间，响应于相应的请求，可以接收许

多这样的响应和相应的内容。

[0064] 接收到的内容是安全的。由 SecaaS 实现的过滤和策略被满足,因为 SecaaS 被包括在请求响应回路内。如果满足 SecaaS 策略,则在由 SecaaS 服务器过滤之后接收内容。SecaaS 实施基于身份的 web 过滤策略。

[0065] 将响应从 SecaaS 通过云连接器发送至缓存服务器。实现缓存,除了将非缓存的内容提供给客户端或作为将该内容提供给客户端的一部分,将非缓存的内容提供给缓存服务器。

[0066] 对于缓存,将一个或多个设置或参数包括在内容中。内容提供商指示该内容是否可以被缓存以及持续多久。例如,寿命或新鲜度设置被包括在该内容内。可以使用有效性和无效性设置。可以提供任意缓存设置。

[0067] SecaaS 可以更改缓存设置的一个或多个值。例如,更改寿命。由云连接器从 SecaaS 接收到的内容已经更改了缓存设置。在另一个实施例中,从内容提供商接收内容,并且云连接器根据从 SecaaS 提供的策略更改缓存设置。缓存头部包括与由内容提供商提供的不同的值。内容的寿命通常由原始获得该内容的 web 服务器来指示。可以更改寿命。例如,SecaaS 可以将寿命调整为不同。寿命可以被增加或减少。由于 SecaaS 已经被通知企业网络正在使用 web 缓存,因此 SecaaS 知道修改响应来影响内容的缓存。可替代地,SecaaS 进行修改,而不考虑知道缓存是否被执行。

[0068] 可以为任何目的而修改寿命。例如,SecaaS 适当地改变到期头部来影响将被缓存的时间内容和 / 或改变缓存控制头部,以使得内容可以是可缓存的或不是可缓存的。在对于 SecaaS 来说内容可以是未知的或者不完整的启发式方法是可用的情况下,为了收集启发式方法可以设置缓存控制来阻止任意缓存。如另一个示例,可以减少期限以使得缓存更早到期,在这种情况下,该内容可能遭受包括不想要的内容的风险。如果所获取的内容不具有信誉得分并且经受蜜罐 (Honey-pot) 方式的测试以监控所获取内容的活动 (在 OS 级别和虚拟网络两者处以检测任意恶意内容),那么基于云的 SecaaS 改变 HTTP 响应中的头部以指示“不储存”,以使得 web 缓存不缓存该内容。

[0069] 在动作 50 中,内容被提供以缓存在网络中。该内容被路由至缓存服务器。基于缓存头部,缓存服务器进行缓存或不进行缓存。缓存有效的时间段是基于寿命设置的。通过将内容路由至缓存服务器,缓存服务器可以进行缓存。基于响应中的 HTTP 头部,缓存服务器缓存该内容。

[0070] 作为缓存操作的一部分,缓存服务器还可以将内容发送至客户端。在其他实施例中,云连接器将内容提供给缓存服务器和客户端二者。缓存服务器不转发该内容。无论哪种方法,只要该内容清除 SecaaS,客户端就接收所请求的内容。

[0071] 作为从企业网络外部获得内容的处理的一部分,缓存的内容由 SecaaS 清除。在缓存之前,所有缓存的内容由 SecaaS 过滤。

[0072] 可以缓存附加的内容。例如,缓存实现方式可以预测将被请求的下一个内容。缓存服务器预获取或预请求可能被客户端请求的内容。该预获取作为对来自企业网络外部内容的任意请求由云连接器重定向至 SecaaS。因此,缓存服务器仅仅存储由 SecaaS 检查的内容。

[0073] 云连接器和 / 或缓存服务器存储可缓存的目标统一资源定位符的列表。该列表是

关于已经被缓存的内容的 URL 的。该列表用来确定后续所请求的内容是否可从缓存中得到。缓存服务器为客户端请求服务，并且该缓存随着时间而受欢迎。可以减少对来自原始服务器的内容的请求，以释放互联网带宽。

[0074] 回到动作 44，内容可能已经被缓存。缓存的内容被对请求做出响应。在图 4 的示例中，雇员请求赌博内容。如上述对图 2 所讨论的，在某个较早点（如图 4 中所示的在缓存之后且客人请求之前），将基于身份的策略从 SecaaS 提供给云连接器。在该示例中，基于身份的策略为不允许雇员访问赌博内容而允许客人访问。这些适合于缓存的内容的策略可以被提供有用于与内容的类型相关联的缓存的原始内容，或者提供一套综合的基于身份的策略。

[0075] 如果所请求的内容先前被缓存并且到期，那么处理按照上面所讨论的动作 46、48 和 50 进行。将请求提供给缓存服务器，缓存服务器检查期限。如果该内容不是新鲜的，那么缓存服务器通过云连接器从 web 服务器请求原始内容。该请求通过 SecaaS 被重定向。

[0076] 如果所请求的内容被缓存并且依然新鲜，那么该缓存的内容对于给定的客户端（例如，个人、设备、位置、连接类型或其他客户端身份）来说可能适用或者可能不适用。当最终用户请求内容时，云连接器已经意识到该内容可在使用列表（例如，WCache）的缓存服务器中得到。为实施基于身份的安全策略，云连接器在客户端和缓存服务器之间的路径中作为 SecaaS。云连接器根据基于身份的策略采用合适的行动。

[0077] 在动作 52 中，云连接器确定对内容的请求是否满足基于身份的安全策略。其他设备可以进行该确定，比如缓存服务器。

[0078] 为确定满足策略，识别合适的策略。具有或不具有其他设置的内容的类型被用来选择策略。在图 4 的示例中，关于赌博的策略被选择。针对不同的身份分组可以提供不同的策略，因此可以选择不止一种策略。其他标准可以被用于选择一个或多个合适的策略。

[0079] 所选择的一个或多个基于身份的策略被用来核实允许所识别的来源访问缓存的内容。适合于所选择的策略的身份信息被用来将安全策略应用到该请求。在图 4 的示例中，客户端的身份是该客户端是该网络上的雇员。使用赌博策略，允许客人访问赌博内容而不允许雇员访问赌博内容。将具有或不具有其他设置的客户端的身份和内容的类型与白名单和 / 或黑名单或表格进行比较以确定依从性。这些列表用于具体情况，合适的列表被获得，并且身份用来确定满足或不满足。缓存的内容先前由 SecaaS 进行过滤，因此，由云连接器实现基于身份的安全提供了综合安全策略实现方式。

[0080] 在基于身份的策略是从 SecaaS 提供的或者与 SecaaS 相同的情况下，基于身份的策略的满足条件对于云连接器与对于 SecaaS 是相同的。因此，安全实现方式在原始内容和缓存的内容之间是一致的，尽管缓存的内容不被重路到网络外至 SecaaS。

[0081] 在动作 54 中，将内容供应给客户端，在该情况下，请求满足基于身份的安全策略。如果匹配“白名单 SecaaS”策略规则，那么云连接器将该请求发送至缓存服务器来为客户端请求服务。缓存服务器以该内容进行回复。将内容提供给客户端。所提供的内容经过或不经过云连接器。

[0082] 在动作 56 中，该请求不满足基于身份的安全策略。在图 4 的示例中，雇员请求缓存的赌博内容。云连接器和 / 或缓存服务器确定不允许雇员或该身份群组访问赌博内容。例如，该请求可能在黑名单上。对赌博内容的列表指示不允许雇员访问，因此，云连接器拒

绝该请求。将错误或其他没有内容的响应发送给客户端。

[0083] 如果身份、内容的类型或其他值不落入可用列表或基于身份的策略内,那么动作 52 是不确定的。缓存的内容可用,但是不能确定对内容的请求是否应该被准许。云连接器通常可以请求策略更新或请求具体针对该情况的策略。该附加的信息可以包括处理该情况的策略规则(例如,新用户群组许可)。云连接器然后可以允许对缓存的内容进行检索或在适当的情况下拒绝。可替代地,将请求路由至 SecaaS 以如获得原始内容一样进行处置。

[0084] 图 5 显示了一种对图 1 的网络或其他网络由 SecaaS 表示行动的方法。尽管下面描述为给定 SecaaS 服务器的行动,但是这些行动可以由分布式服务器执行。类似地,其他 SecaaS 服务器可以针对其他请求重复这些行动。

[0085] 在动作 80 中,接收对内容的请求,比如,上面针对动作 46 所讨论的请求。诸如服务器之类的安全服务处理器从诸如企业网络之类的网络接收对内容的请求。

[0086] 在动作 82 中,从 web 服务器请求内容。安全服务器更改头部,以使得 web 服务器将该内容提供给安全服务器,而不是企业网络或原始客户端。将请求发送至 web 服务器。在动作 84 中,web 服务器做出响应,因此,安全服务器从 web 服务器接收该内容。

[0087] 在动作 86 中,安全服务器过滤从 web 服务器接收到的内容。过滤可以基于 URL、内容分析、请求者的身份和 / 或其他信息。该过滤实现了 SecaaS 的策略或者实现了由或对企业网络进行配置的策略。尽管显示了在接收内容之后进行过滤,但是一些过滤可以在从 web 服务器请求内容之前发生。例如,基于 URL 的过滤和 / 或基于身份的过滤基于请求而不是所接收到的内容而发生。从请求或先前的发掘能够得知内容的性质。例如,URL 可以被用来指示内容的类型。使用内容的类型,客户端的身份被用来确定是否应该提供该内容的类型。

[0088] 在可选的动作 88 中,安全服务器调整该内容的新鲜度或其他缓存设置。web 服务器向该内容提供缓存设置。这些缓存设置可以根据安全策略进行更改。例如,缓存的能力或没有缓存的能力从允许缓存改变为不允许缓存,比如,正在为 SecaaS 收集启发式方法的情况。如另一示例,缩短寿命来确保新鲜度,而不管对该内容的原始缓存设置。在另一示例中,可能无法获得充足的安全信息,因此,将缓存改为更有限或不被允许的。

[0089] 在动作 90 中,在过滤之后,将该内容作为对来自客户端的请求的响应进行传送。该内容可以与从 web 服务器接收到的内容相同或从其进行更改。缓存头部可以与从 web 服务器接收的头部相同或从其进行更改。将过滤的内容传送至企业网络。在其他示例中,该内容不传递安全策略,因此,错误消息或其他消息而不是该内容被传送。

[0090] 在动作 92 中,将一个或多个基于身份的安全策略传送至企业网络,比如,传送至云连接器。传送黑名单、白名单、以规则、代码形式或其他形式的策略和 / 或其他策略信息。可替代地,传送用来配置基于身份的安全策略的一个或多个设置。

[0091] 该传送响应于来自企业网络的通知。该通知指示正在执行缓存。在其他实施例中,该传送响应于另一触发而发生,例如,企业网络指示策略不足以确定是否基于身份供应缓存的信息。可替代地或附加地,该传送是周期性的。

[0092] 图 6 是诸如图 1 的客户端设备 14、云连接器 16、缓存服务器 18 或 SecaaS 服务器 20 之类的示例网络设备的简化框图。在图 6 中,示例网络装置或设备 70 与可以被部署在网络 12 或网络 10 中的网络元件或计算设备相对应。网络设备 70 包括软件和 / 或硬件以执

行用于通过安全即服务进行缓存的活动或操作中的任意一个或多个。

[0093] 网络设备 70 包括处理器 72、主存储器 73、次级存储设备 74、无线网络接口 75、有线网络接口 76、用户接口 77 和包括计算机可读介质 79 的可移除介质驱动 78。诸如系统总线和存储器总线之类的总线 71 可以提供处理器 72 与网络设备 70 的其他部件、存储器、驱动和接口之间的电子通信。

[0094] 可以提供附加的、不同的或更少的部件。这些部件旨在用于说明性的目的，并且不意味着隐含对网络设备 12、14 的架构限制。例如，网络设备 70 可以包括另一个处理器和 / 或不包括次级存储设备 74 或可移除介质驱动 78。每个网络设备 12、14 可以包括比其他网络设备 14 更多或更少的部件。

[0095] 处理器 72(还可以称为中央处理单元 (CPU)) 是能够运行机器可读指令并按照由这些机器可读指令所指示的来对数据执行操作的通用或专用处理器。主存储器 73 对处理器 72 访问机器指令来说是可以直接进行访问的，并且主存储器 73 可以是随机存取存储器 (RAM) 或任意类型的动态存储设备 (例如，动态随机存取存储器 (DRAM))。次级存储设备 74 可以是诸如硬盘之类的能够存储包括可执行软件文件的电子数据的任意非易失性存储器。可以将外部存储的电子数据通过一个或多个可移除介质驱动 78 提供给计算机 70，可移除介质驱动 78 可以被配置来接收任意类型的外部介质 79，例如，光盘 (CD)、数字视频盘 (DVD)、闪速驱动、外部硬驱或任意其他外部介质。

[0096] 可以提供无线网络接口和有线网络接口 75 和 76 来使得网络设备 70 和其他网络设备 12、14 间能够通过一个或多个网络进行电子通信。在一个示例中，无线网络接口 75 包括具有合适的发射和接收部件 (比如，收发器) 的无线网络控制器 (WNIC)，用于在网络 10 内进行无线通信。有线网络接口 76 可以使得网络设备 70 能够通过诸如以太网电缆之类的线路物理地连接到网络 10。无线网络接口和有线网络接口 75 和 76 二者都可以被配置来使用合适的通信协议 (比如，互联网协议组 (TCP/IP)) 促进通信。

[0097] 仅为说明性的目的，网络设备 70 显示有无线网络接口和有线网络接口 75 和 76 二者。尽管无线接口和硬连线接口中的一者或二者可以被提供在网络设备 70 中，或者可以从外部连接到网络设备 70，但是只需要一个连接选项来使得网络设备 70 连接到网络 10。网络设备 70 可以包括使用任意类型连接选项的任意数目的端口。

[0098] 可以将用户接口 77 不提供在机器中、提供在一些机器中或提供在所有的机器中以允许用户与网络设备 70 进行交互。用户接口 77 包括显示设备 (例如，等离子显示板 (PDP)、液晶显示器 (LCD) 或阴极射线管 (CRT))。此外，还可以包括诸如键盘、触摸屏、鼠标、轨迹球、麦克风 (例如，用于声音识别的输入)、按钮和 / 或触摸板之类的任意合适的输入设备。

[0099] 可以将体现本申请所描述的活动或功能的指令存储在一个或多个外部计算机可读介质 79 上、在主存储器 73 中、在次级存储设备 74 中或在网络设备 70 的处理器 72 的缓存存储器中。网络设备 70 的这些存储器元件是非暂态计算机可读介质。将用于实现本申请所讨论的这些处理、方法和 / 或技术的逻辑提供在非暂态计算机可读存储介质或存储器上，比如，缓存、缓冲器、RAM、可移除介质、硬驱或其他计算机可读存储介质。计算机可读存储介质包括各种类型的易失性和非易失性存储介质。因此，“计算机可读介质”意味着包括能够存储指令的任意介质，网络设备 70 运行这些指令以使得机器执行本申请所公开的活

动中的任意一个或多个活动。

[0100] 作为逻辑存储在存储器上的指令可以由处理器 72 来运行。响应于存储在计算机可读存储介质中或上的指令中的一组或多组指令，执行附图中所示出的或本申请所描述的功能、动作或任务。这些功能、动作或任务独立于特定类型的指令集、存储介质、处理器或处理策略，并且这些功能、动作或任务可以由单独地或组合地进行操作的软件、硬件、集成电路、固件、微代码等来执行。同样，处理策略可以包括多处理、多任务、并行处理等。

[0101] 可以将附加的硬件耦合于网络设备 70 的处理器 72。例如，存储器管理单元 (MMU)、附加的对称多处理 (SMP) 元件、物理存储器、外部部件互联 (PCI) 总线和相应网桥或小型计算机系统接口 (SCSI) / 集成驱动电子 (IDE) 元件。网络设备 70 可以包括促进操作的任何附加的合适的硬件、软件、部件、模块、接口或对象。这可以包括允许对数据的有效保护和通信的合适的算法和通信协议。而且，任意合适的操作系统被配置在网络设备 70 中，以恰当地管理其硬件部件的操作。

[0102] 存储器 73、74、79 或另一个存储器中的一个或多个存储器存储缓存的内容、缓存设置或头部、黑名单、白名单、基于身份的策略、错误消息、请求、响应和 / 或一个或多个来源身份。处理器 72 被配置来应用基于身份的规则以供应缓存的信息并重定向对原始内容的请求。作为安全服务器，处理器 72 可以作为安全即服务的一部分更改缓存头部。

[0103] 尽管本发明上面已经通过参照各个实施例进行了描述，但是应当理解的是，可以在不背离本发明的范围的情况下做出许多改变和修改。因此，前面的详细描述可以被看作是说明性的而不是限制性的，并且应当理解所附权利要求包括所有等同物旨在限定本发明的精神和范围。

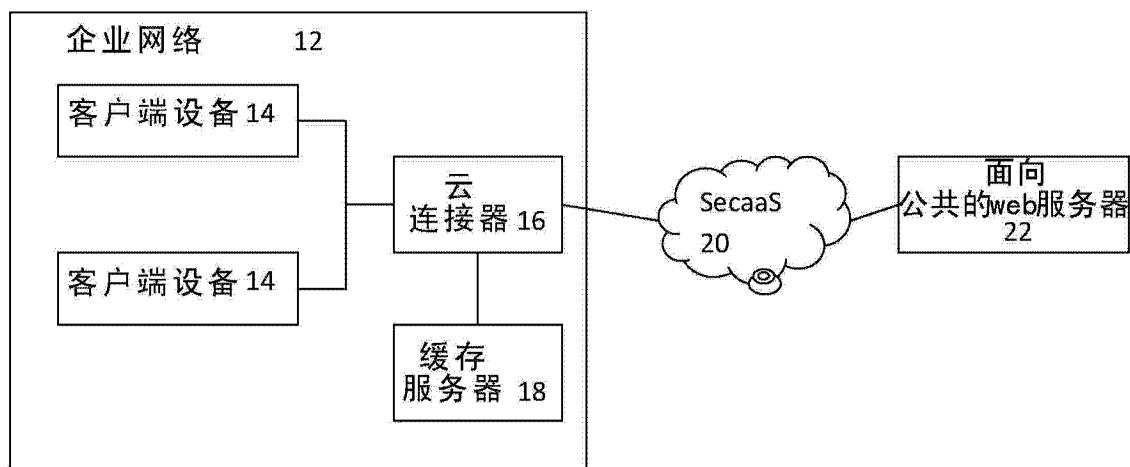
10

图 1

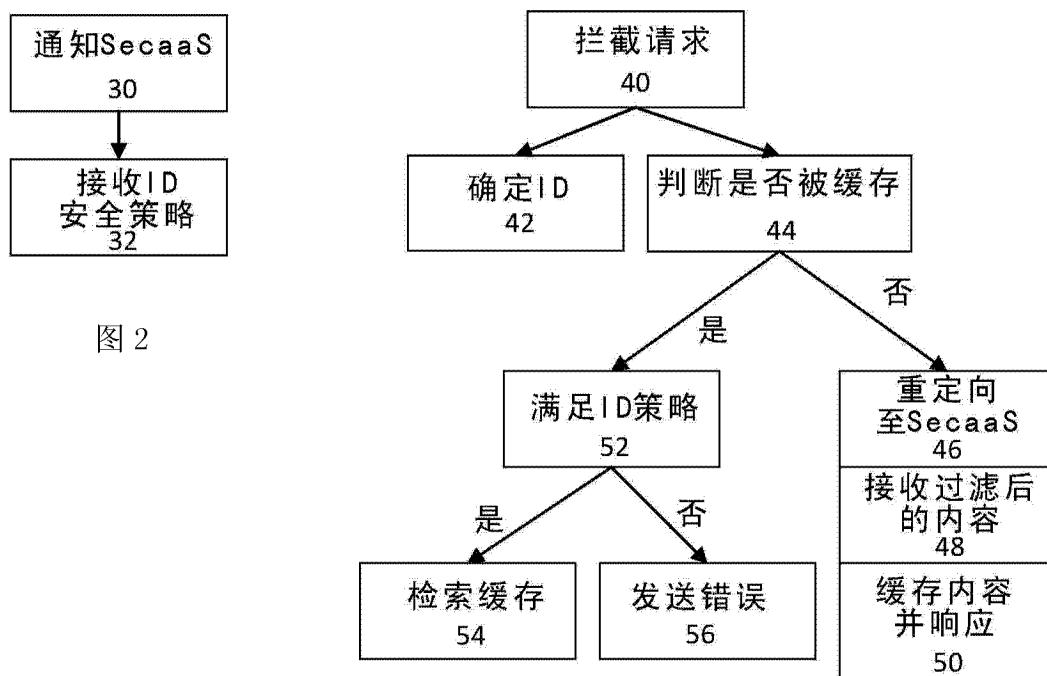


图 2

图 3

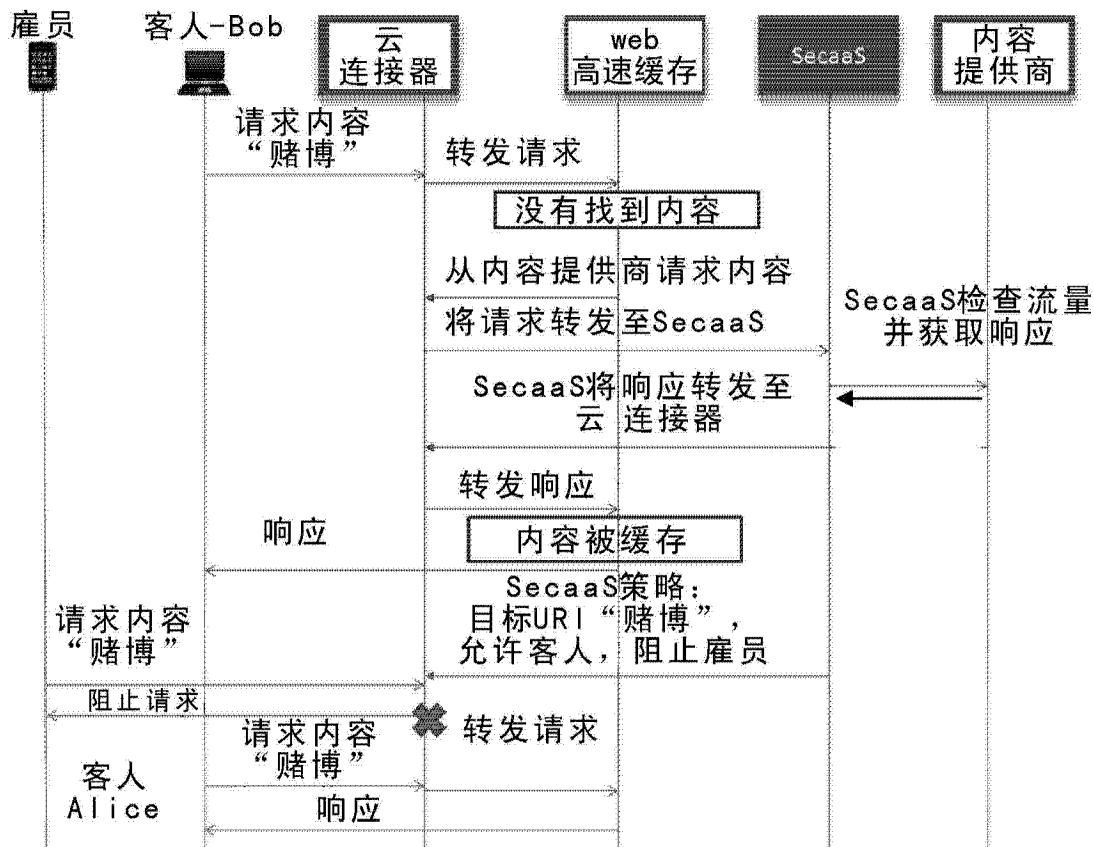


图 4

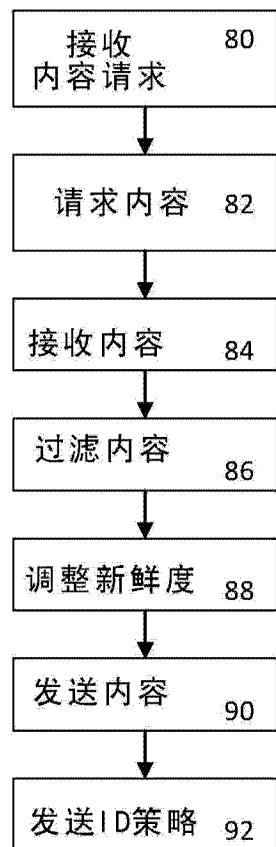


图 5

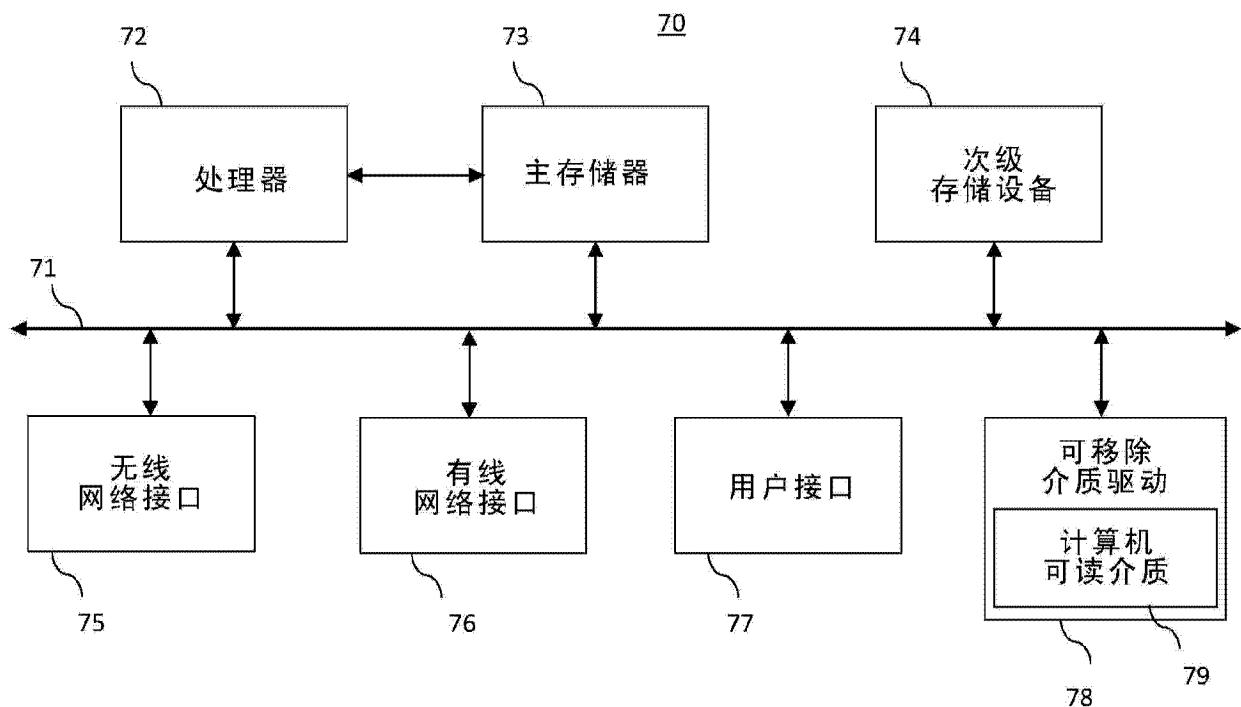


图 6