(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 103391274 A
(43)申请公布日 2013.11.13

(21)申请号 201210141396.2

(22)申请日 2012.05.08

(71)申请人 北京邮电大学
地址 100876 北京市海淀区西土城路 10 号

(72)发明人 张宏科 关建峰 许长桥 权伟
曹远龙 赵付涛 刘诗维 文新

(74)专利代理机构 北京三高永信知识产权代理有限责任公司 11138
代理人 王希刚

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 12/24(2006.01)

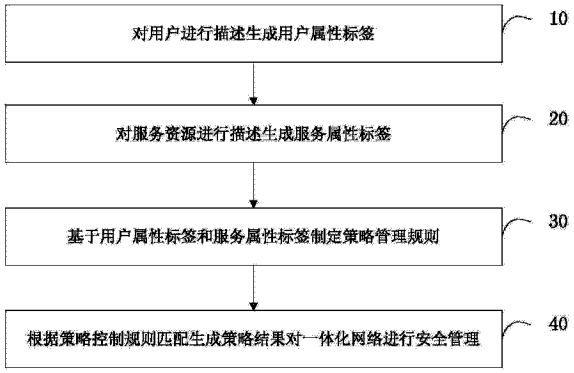
权利要求书1页 说明书7页 附图3页

(54)发明名称

一种一体化网络安全管理方法和装置

(57)摘要

本发明公开了一种一体化网络安全管理方法，属于计算机网络通信技术领域。所述方法包括：对用户属性进行描述生成用户属性标签；对服务属性进行描述生成服务属性标签；基于用户属性标签和服务属性标签制定策略管理规则；根据策略管理规则匹配生成策略结果，从而对一体化网络进行安全管理。本发明还公开了一种一体化网络安全管理装置。本发明通过引入用户属性标签和服务属性标签，其分别从多个维度对用户属性和服务服务属性进行描述，并按照一定的编码规则进行编码，同时建立基于属性标签的策略管理规则实现多样化、分级别的安全管理方法。



CN 103391274 A

1. 一种一体化网络安全管理方法，其特征在于，所述方法包括：

对用户属性进行描述生成用户属性标签；

对服务属性进行描述生成服务属性标签；

基于用户属性标签和服务属性标签制定策略管理规则；

根据策略管理规则匹配生成策略结果对一体化网络进行安全管理。

2. 如权利要求 1 所述的方法，其特征在于，所述对用户属性进行描述包括对用户的基本信息和行为信息进行多维描述，包括但不限于用户的身份、地域、年龄、工作性质、上网时间和用户可信度。

3. 如权利要求 1 所述的方法，其特征在于，所述对服务属性进行描述包括对服务的基本信息和行为信息进行多维描述，包括但不限于服务类别、服务提供商、服务 QoS、服务可信度和服务受欢迎度。

4. 如权利要求 1 所述的方法，其特征在于，所述用户属性标签和服务属性标签为字符串形式，利用同一设定的标签计算方法生成。

5. 如权利要求 1 所述的方法，其特征在于，所述策略结果为一个或多个元素的集合，包括但不限于拒绝访问、允许访问、提示警告、正向引导、多路访问、单路访问和内容推送。

6. 一种一体化网络安全管理装置，其特征在于，所述装置包括用户管理单元、服务管理单元、策略管理单元和策略匹配单元，其中，

所述用户管理单元，用于对用户属性进行描述生成用户属性标签；

所述服务管理单元，用于对服务属性进行描述生成服务属性标签；

所述策略管理单元，用于基于用户属性标签和服务属性标签制定策略管理规则；

所述策略匹配单元，用于根据策略管理规则匹配生成策略结果对一体化网络进行安全管理。

7. 如权利要求 6 所述的装置，其特征在于，所述用户管理单元进一步用于对用户进行注册、认证和管理，生成用户属性信息。

8. 如权利要求 6 所述的装置，其特征在于，所述资源管理单元进一步用于对服务资源进行注册和管理，生成服务属性信息。

9. 如权利要求 6 所述的装置，其特征在于，所述策略管理单元进一步用于对策略条目进行动态调整和聚合。

10. 如权利要求 6 所述的装置，其特征在于，所述策略匹配单元进一步用于对用户属性标签、服务属性标签以及策略结果生成多元组，并对所述多元组进行匹配来执行策略匹配操作。

一种一体化网络安全管理方法和装置

技术领域

[0001] 本发明涉及计算机网络通信技术领域，特别涉及一种一体化网络安全管理方法和装置。

背景技术

[0002] 随着互联网技术及其应用服务的飞速发展，人们对通信的需求日益增长，现有网络存在的问题也日益突出，当前的计算机网络已经不能满足人们的需求。由于现有的网络在设计之初就存在一些本质的问题，例如，IP 地址承担身份和位置双重角色，网络中服务资源存在冗余等。虽然人们一直在对现有网络进行优化和改进，但基本都是以一种打补丁的方式来完成，最后将导致网络架构越来越复杂。为了能够从根本上解决现有网络中的问题，新的网络体系架构的提出正逐步成为国内外信息网络研究的重要内容。

[0003] 国家 973 项目“一体化可信网络与普适服务体系基础研究”提出了一种新的网络体系架构，以下简称一体化网络。一体化网络架构由两层组成 :服务层和网通层。服务层可分为虚拟服务模块和虚拟连接模块 ;网通层可分为虚拟接入模块和虚拟骨干模块。服务层定义了服务标识和连接标识，并引入从服务到连接的服务标识解析映射，完成了各种服务的统一描述和管理，从而实现服务的普适化。网通层定义了接入标识和路由标识，并引入从连接到路由的接入标识解析映射，支持现有各种子网和终端的接入，为多元化的网络接入提供了平台，为数据、语音、视频服务提供了一体化网络的网络通信平台，从而有效地支持普适服务。其中，服务标识是一种统一的服务描述形式，每一个服务有唯一的服务标识 ;连接标识用于为服务建立连接与传输数据 ;路由标识用在网通层进行选路和路由 ;接入标识是用于客户端接入的身份标识。一体化网络通过解析映射来完成四个标签的转化过程。

[0004] 基于此，现有技术提出了一种用户身份认证和消息认证的方案，从而实现一体网络中移动与固定节点的安全接入。该方案主要是设计接入交换路由器、认证中心以及终端这三个功能实体之间的通信协议，通过认证消息的查询和处理等过程，来实现一体化网络基于标识的终端接入方法，提高网络的安全性。

[0005] 现有的一体化网络体系包括了对用户的注册和认证过程以及服务的注册过程，但并没有一种方法来安全管理控制用户对资源的访问。随着网络服务的不断发展，对网络资源访问的安全管理需求日益增加。例如，如何管控不同用户访问不同资源，如何提供用户的个性化服务等问题日益突出。在一体化网络中，接入标识和服务标识分别代表用户身份和服务身份，如何利用用户身份和服务身份进行网络安全管理成为了一个重要的研究内容，也对当前的网络安全管理具有重要的意义。

[0006] 现有技术提出了一种基于一体化网络安全服务架构的综合安全防护方法，采用网络承载信息的分类隔离安全防护技术，将业务、控制和管理等信息相互隔离 ;采用用户的安全接入防护技术，对终端设备进行接入认证 ;采用节点的安全互连防护技术，对互连节点的合法性进行认证 ;采用业务的准入控制技术，对用户身份和业务权限进行认证。该发明的积极效果是 :将网络通信与安全保密有机融合，构建多层次、全方位的综合安全保密体系，解

决了通用 IP 网络中存在的信令、管理、业务平面不分，网络地址与用户地址不分，网络资源使用范围和时间不受控等问题，有效地避免了叠加式安全保密机制的效率低、防护不全，不能提供面向流的快速安全传输等缺陷。

[0007] 该技术采用业务的准入控制技术，对用户身份和业务权限进行认证。随着网络安全要求的提高，对信息内容安全管理力度逐步加大。现有的技术只侧重于用户的安全接入和认证，以及业务的认证，并没有提出一种针对用户和服务交互的安全管理方法。

[0008] 另一现有技术公开了一种基于一体化网络安全服务架构的信息分类隔离方法，将网络中的业务、控制和管理信息分类隔离，各类数据在网络中进行独立的路由交换和传输，具有独立的带宽资源和相应的 QoS 保证措施，各类数据各行其道，互不干扰。该发明的积极效果是：由于信令系统和网管系统在网络中相对独立的运行，不受业务流量和异常报文的影响，即使在网络业务严重拥塞时也能对系统实施有效控制。同时，也避免了系统消息抢占业务带宽，影响业务的服务质量。

[0009] 该技术方法具体提出了一种将信息分类隔离的方法，各类数据在网络中进行独立的路由交换和传输，减少各类数据之间的干扰。其侧重点在网络传输层的安全，并没有提出一种针对用户和服务的分类隔离方法。随着网络的发展，网络业务的安全性至关重要，该技术只是在传输层对各类数据进行分离，无法对用户和服务进行分类隔离，从而无法对用户和服务进行分类的操作管理。

[0010] 现有技术中提出了一种广告策略的验证方案，该方案包括：测试终端接收输入的与广告策略相匹配的用户属性和行为；向服务器发送携带有所述用户属性和行为的广告模拟请求；接收并显示所述服务器发送的广告列表，广告列表为服务器将用户属性和行为与广告策略进行匹配得出。服务器从数据库中提取用户配置的广告策略；将用户属性和行为与用户配置的广告策略进行匹配；如果匹配，则将与用户属性和行为匹配的广告策略对应的广告列表发送给所述第一测试终端，如果不匹配，则不返回广告列表。

[0011] 该方案中，利用用户属性和行为跟广告策略进行匹配，可以降低广告策略验证的复杂度，提高广告策略验证的效率。但是，其对象主要是针对广告推送业务，并没有针对网络服务资源进行属性描述，也就没有形成网络安全管理体系。

[0012] 在实现本发明的过程中，发明人发现现有技术尚没有一种能够有效地实现一体化网络整体安全控制方案，无法支持多样性的安全管理策略。

发明内容

[0013] 为了解决现有技术中一体化网络无法支持多样性安全管理策略的问题，本发明实施例提供了一种一体化网络安全管理方法和装置。所述技术方案如下：

[0014] 一种一体化网络安全管理方法，所述方法包括：

[0015] 对用户属性进行描述生成用户属性标签；

[0016] 对服务属性进行描述生成服务属性标签；

[0017] 基于用户属性标签和服务属性标签制定策略管理规则；

[0018] 根据策略管理规则匹配生成策略结果对一体化网络进行安全管理。

[0019] 所述对用户属性进行描述包括对用户的基本信息和行为信息进行多维描述，包括但不限于用户的身份、地域、年龄、工作性质、上网时间和用户可信度。

[0020] 所述对服务属性进行描述包括对服务的基本信息和行为信息进行多维描述，包括但不限于服务类别、服务提供商、服务 QoS、服务可信度和服务受欢迎度。

[0021] 所述用户属性标签和服务属性标签为字符串形式，利用设定的标签计算方法生成。

[0022] 所述策略结果为一个或多个元素的集合，包括但不限于拒绝访问、允许访问、提示警告、业务引导、多路访问、单路访问和内容推送。

[0023] 一种一体化网络安全管理装置，所述装置包括用户管理单元、服务管理单元、策略管理单元和策略匹配单元，其中，

[0024] 所述用户管理单元，用于对用户属性进行描述生成用户属性标签；

[0025] 所述服务管理单元，用于对服务属性进行描述生成服务属性标签；

[0026] 所述策略管理单元，用于基于用户属性标签和服务属性标签制定策略管理规则；

[0027] 所述策略匹配单元，用于根据策略管理规则匹配生成策略结果对一体化网络进行安全管理。

[0028] 所述用户管理单元进一步用于对用户进行注册、认证和管理，生成用户属性信息。

[0029] 所述资源管理单元进一步用于对服务资源进行注册和管理，生成服务属性信息。

[0030] 所述策略管理单元进一步用于对策略条目进行动态调整和聚合。

[0031] 所述策略匹配单元进一步用于对用户属性标签、服务属性标签以及策略结果生成多元组，并对所述多元组进行匹配来执行策略匹配操作。

[0032] 本发明实施例提供的技术方案带来的有益效果是：

[0033] 通过对用户属性进行描述生成用户属性标签，对服务属性进行描述生成服务属性标签，并且基于用户属性标签和服务属性标签制定策略管理规则，通过策略匹配生成策略结果来进行安全管理。本发明实施例提供的方案，在一体化网络的用户身份标识之上引入了用户属性标签，可以多维地从各个角度对用户进行描述；在一体化网络的服务标识之上引入了服务属性标签，可以多维地从各个角度对服务资源进行描述；为多样化的安全管理策略提供支持。同时，本发明实施例提出了基于用户属性标识和服务属性标识的安全管理策略，比现有技术中的路由安全管理策略更为高级，引申到了应用层。安全管理策略支持多维的，具有很好的可扩展性，扩展不受限于结构，用户可以根据需求随时的更改管理策略。安全管理策略是可聚合的，可以基于多维属性的描述，对部分具有很高耦合性的策略条目进行聚合，从而减少安全策略的数量。安全管理方法具有很好的灵活性，可以根据需求设定不同的管理机制，最大限度满足不同情况的安全管理需求。

附图说明

[0034] 为了更清楚地说明本发明实施例中的技术方案，下面将对实施例描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

[0035] 图 1 是本发明实施例提供的安全管理方案示意图；

[0036] 图 2 是本发明实施例 1 提供的一体化网络安全管理方法原理流程图；

[0037] 图 3 是本发明实施例 1 提供的一种用户属性标签的生成过程示意图；

[0038] 图 4 是本发明实施例 1 提供的一种用户属性标签的格式示例图；

[0039] 图 5 是本发明实施例 1 提供的一种服务属性标签的生成过程示意图；

[0040] 图 6 是本发明实施例 1 提供的一种服务属性标签的格式示例图；

[0041] 图 7 是本发明实施例 1 提供的一体化网络安全管理方法实现过程示意图；

[0042] 图 8 是本发明实施例 2 提供的一体化网络安全管理装置结构示意图。

具体实施方式

[0043] 为使本发明的目的、技术方案和优点更加清楚，下面将结合附图对本发明实施方式作进一步地详细描述。

[0044] 本发明实施例针对一体化网络引入用户属性标签、服务属性标签，通过一系列基于属性标签的策略规则，生成策略结果来进行网络的安全管理，提出一种一体化网络安全管理方法。并提出一种一体化网络安全管理装置。

[0045] 现有网络安全管理策略是基于 IP 地址或 URL 的，根据源地址和目的地址或访问 URL 进行路由策略管理。在一体化网络中用户注册生成唯一的 UID(User Identification，用户标识)，同时服务在网络中注册生成唯一的 SID(Service Identification，服务标识)。用户每一次操作都是用户向服务的一次请求，也就是 UID 和 SID 的一个配对操作。UID 和 SID 可以唯一地确定用户和服务，但是由于 UID 和 SID 含有的信息量极少，单纯地依靠 UID 和 SID 来进行策略管理，往往只是一些没有含义的数字组合，无法支持一些高级别的策略管理和安全管理。例如，如何为拥有不同爱好的用户提供不同类别的服务，如何管理不同服务级别的资源，如何管理不同年龄段的用户上网行为等等。为此，本发明提出两个属性标签来分别体现用户和服务的一些属性特性。通过对 UID 属性进行描述生成一个 UTAG (User Tag，用户属性标签)，两者之间绑定生成一个二元组(UID，UTAG)；对 SID 属性进行描述生成一个 STAG (Service Tag，服务属性标签)，两者之间绑定生成一个二元组(SID，STAG)。UTAG 和 STAG 是对所选属性的描述，具有丰富的含义。基于 UTAG 和 STAG 设定 RULES (策略规则)。用户每次访问资源会分别查询获取请求服务中 UID 和 SID 对应的 UTAG 和 STAG，再通过查询相关的 RULES 得到策略结果，从而实现安全管理。如图 1 所示，为本发明实施例提供的安全管理方案示意图。

[0046] 实施例 1

[0047] 如图 2 所示，为本发明提供的一体化网络安全管理方法原理流程图，其中，

[0048] 步骤 10，对用户属性进行描述生成用户属性标签。

[0049] 这里的用户属性标签用于描述用户的基本信息和行为信息，支持从多个角度多维度去描述用户(具体可以从身份，地域，年龄，工作性质，上网时间，用户可信度等角度进行描述，但不局限于此)。标签的具体表现形式为字符串格式，利用统一设定的标签计算方法来生成标签。该计算方法支持多种多样。例如，可以对用户属性进行标准化编码，由每个属性编码组合成用户属性便签。如图 3 所示，为用户属性标签的生成过程示意图。

[0050] 如图 4 所示，为本发明实施例提供的一种用户属性标签的格式示例图。本示例中用户属性标签可以利用多个维度来标记，如地域、语言习惯等。

[0051] 步骤 20，对服务属性进行描述生成服务属性标签。

[0052] 服务属性标签用于描述服务资源的基本信息和行为信息，支持从多个角度和多维

去描述服务资源(具体可以从服务类别,服务提供商,服务 QoS,服务可信度,服务受欢迎度等角度进行描述,但不局限于此)。标签的具体表现形式为字符串格式,利用统一设定的标签计算方法来生成标签。该计算方法支持多种多样。例如,可以对选定的服务属性进行标准化编码,由每个属性编码项组合成服务属性标签。图 5 为服务属性标签的生成过程示意图。

[0053] 图 6 为一种服务属性标签的格式的示例图,其属性包括资源性质、服务类别等。

[0054] 为了进一步说明用户属性标签和服务属性标签的生成,如图 7 所示,为本实施例提供的一体化网络安全管理方法实现过程示意图,其中,

[0055] 用户通过注册,将用户的基本信息(其主要包括 :用户 ID,用户年龄,性别,用户身份,用户工作领域等)注册到用户认证中心数据库。服务通过注册,将服务的基本描述信息(其主要包括 :服务 ID,服务资源大小,服务类别,服务 QoS)记录到服务管理中心数据库。

[0056] 行为分析服务器对用户和服务的行为信息(其主要包括 :用户可信度,用户流量消耗,用户活跃度等,服务优良度,服务受欢迎度等)进行分析、汇总、反馈。分别记录到用户认证中心和服务管理中心。行为分析服务器保持动态的对用户和服务的行为信息进行更改。

[0057] 这里,通过用户基本信息和用户行为信息,进行标准化之后,生成用户属性标签。用户属性标签在用户请求服务之后,进一步的用户行为信息会反馈给用户信息数据库,生成新的用户行为信息。同样,服务提供后,通过采集服务基本信息,将服务分类,并通过获取服务行为信息,经过标准化之后,生成服务属性信息。服务属性信息在提供服务的过程中,经过行为分析,进一步将服务行为信息反馈给服务信息数据库,从而生成新的服务行为信息。

[0058] 步骤 30,基于用户属性标签和服务属性标签制定策略管理规则。

[0059] 这里的策略管理规则是基于用户属性标签和服务属性标签制定的,支持用户属性和服务属性多维的匹配规则,支持可扩展。具有可聚合性,针对某些共有特性可以进行提取,聚合策略条目,大大减少条目的数量,从而减少查询、匹配时间。同时又不损失匹配策略完备性,可以尽最大努力满足策略匹配需求和原则。举例来说,根据用户属性标签可以设定用户可以访问哪些服务,基于该服务的服务属性标签,可以设定用户访问服务的方式和规定的路由,这些设定的方式和规定的路由就是策略管理规则。这样的策略管理规则是基于用户属性标签和服务属性标签制定的,可以是人工制定,也可以通过模型训练等方式设定。

[0060] 如图 7 中所示,可以设定策略管理库的 RULES,其格式为三元组,形如 :(UTAG STAGOperator),其中 UTAG 为用户属性标签,UTAG 形如 ($utag_1$,$utag_2$,$utag_3$,$utag_4$,$utag_5$,…),由多维属性组合而成,$utag_i$ (i>=1)表示用户在每一维上的属性。STAG 为服务属性标签,STAG 形如 ($stag_1$,$stag_2$,$stag_3$,$stag_4$,$stag_5$,…),同样由多维属性组合而成,$stag_j$(j>=1)表示服务资源在每一维上的属性,Operator 表示策略匹配对应的操作。管理策略规则还可以设定模糊管理策略,形如(Sub-UTAG Sub-STAG Operator),其中 Sub-UTAG 为子用户属性标签,由 UTAG 的子集组成,Sub-STAG 为子服务属性标签,由 STAG 的子集组成。这里的策略管理库可以通过多种方式设定,例如,可以通过 WEB 接口来设定策略管理库。

[0061] 策略管理库用于基于用户属性标签和服务属性标签制定和管理策略管理规则,这些策略管理规则就保存在策略管理库中。进一步的,这些策略管理规则可以通过人工设定、需求场景和模型训练得到。这些策略管理规则可以互相匹配得到策略结果,这些策略结果

直接对一体化网络进行安全管理。

[0062] 步骤 40，根据策略管理规则匹配生成策略结果对一体化网络进行安全管理。

[0063] 为了达到网络安全管理，本发明对策略结果进行描述，来实现用户访问服务资源的管理。当用户访问服务的时候，根据设定的策略管理规则进行匹配，确定用户访问服务的结果，就是策略结果。策略结果针对策略匹配规则得出的具体网络操作结果，可以是一个或多个元素的集合。具体可以是 :拒绝访问，允许访问，提示警告，业务引导，多路访问，单路访问，内容推送等。

[0064] 如图 7 所示，当用户 A 请求服务 B 时，通过用户认证中心查询，可以利用标准化编码表生成用户 A 的用户属性标签 UTAG_A，通过服务管理中心查询生成服务 B 的服务属性标签 STAG_B，网络管理单元分别对用户属性标签和服务属性标签进行匹配，找到合适的 Operator。Operator 可以支持多种，特别的，可以表示为 :0- 拒绝访问 ;1- 允许访问 ;2- 警告提示 ;3- 业务引导。

[0065] 根据 Operator 指示的操作进行连接标识的映射，若为 0 则直接返回不可达的 CID (Connection Identification，连接标识);若为 1 则寻找正确的 CID 返回至用户 ;若为 2 则直接返回对应警告提示的 CID 地址 ;若为 3 则返回对应资源类似的引导资源的 CID 地址。

[0066] 完成用户访问资源的一次过程。行为分析服务器记录用户的行为信息以及服务资源的行为信息，作为数据资源为分析用户和服务的行为属性提供素材。

[0067] 实施例 2

[0068] 如图 8 所示，为本发明实施例 2 提供的一体化网络安全管理装置结构示意图，该装置包括用户管理单元 100、服务管理单元 200、策略管理单元 300 和策略匹配单元 400，其中，

[0069] 用户管理单元 100，用于对用户属性进行描述生成用户属性标签。

[0070] 进一步地，用户管理单元 100 还用于对用户进行注册、认证和管理，生成用户属性信息。用户属性通过用户的注册信息和网络行为信息进行多维的评估描述。对用户在网络上操作产生的一些动态信息描述，可以包括用户上网时间，用户可信度，操作合法性等。

[0071] 服务管理单元 200，用于对服务属性进行描述生成服务属性标签。

[0072] 进一步地，服务管理单元 200 还用于对服务资源进行注册和管理，生成服务属性信息。服务属性通过服务资源的基本属性和服务行为属性进行多维的评估描述。对服务通过用户操作产生的一些动态变化的信息描述。可以包括服务可信度，服务访问量，服务合法性等。

[0073] 策略管理单元 300，用于基于用户属性标签和服务属性标签制定策略管理规则。

[0074] 策略管理单元 300 进一步用于对策略条目进行动态调整和聚合，针对不同的用户组和服务组设定不同策略结果。策略规则可以是用户属性标签、服务属性标签以及策略结果组成的三元组。

[0075] 策略匹配单元 400，用于根据策略管理规则匹配生成策略结果对一体化网络进行安全管理。还用于对用户属性标签、服务属性标签以及策略结果生成二元组，并将二元组与策略规则中的前两元进行匹配。通过对用户属性标签和服务属性标签二元组进行匹配，获得对应的策略结果来执行操作，完成策略管控。当然，这里对用户属性标签、服务属性标签以及策略结果生成的可以不仅仅是二元组，而是三元组或者多元组。

[0076] 策略结果是支持一个或多个。可以是拒绝访问，允许访问，警告处理，正向引导，反

向引导等。

[0077] 综上所述，本发明各个实施例通过对用户属性进行描述生成用户属性标签，对服务属性进行描述生成服务属性标签，并且基于用户属性标签和服务属性标签制定策略管理规则，通过策略匹配生成策略结果来进行安全管理。本发明实施例提供的方案，在原有的用户身份标识之前引入了用户属性标签，可以多维地从各个角度对用户进行描述；在原有的服务标识之前引入了服务属性标签，可以多维地从各个角度对服务资源进行描述；为多样化的安全管理策略提供支持。同时，本发明实施例提出了基于用户属性标识和服务属性标识的安全管理策略，比现有技术中的路由安全管理策略更为高级，引申到了应用层。安全管理策略支持多维的，具有很好的可扩展性，扩展不受限于结构，用户可以根据需求随时的更改管理策略。安全管理策略是可聚合的，可以基于多维属性的描述，对部分具有很高耦合性的策略条目进行聚合，从而减少安全策略的数量。安全管理方法具有很好的灵活性，可以根据需求设定不同的管理机制，最大限度满足不同情况的安全管理需求。

[0078] 本领域普通技术人员可以理解实现上述实施例的全部或部分步骤，可以通过硬件来完成，也可以通过程序来指令相关的硬件完成，所述的程序可以存储于一种计算机可读存储介质中，上述提到的存储介质可以是只读存储器，磁盘或光盘等。

[0079] 以上所述仅为本发明的较佳实施例，并不用以限制本发明，凡在本发明的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

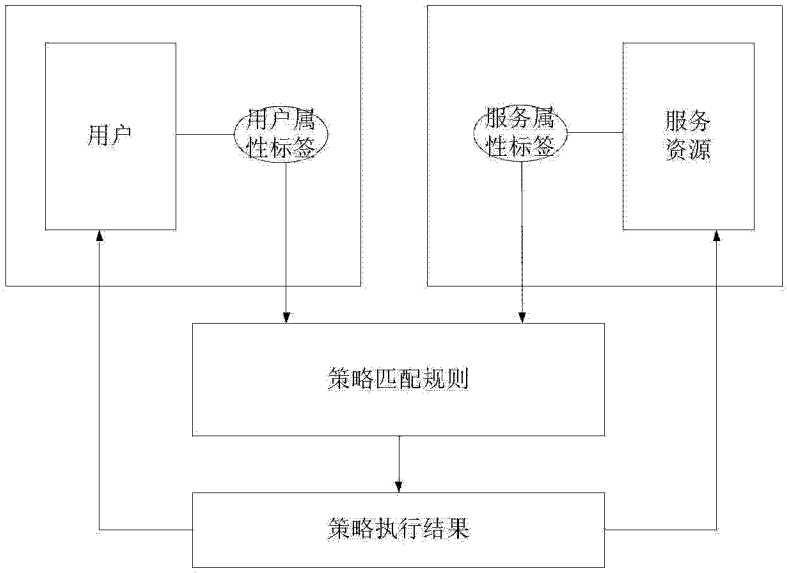

用户
用户属性标签
服务属性标签
服务资源
策略匹配规则
策略执行结果

图 1

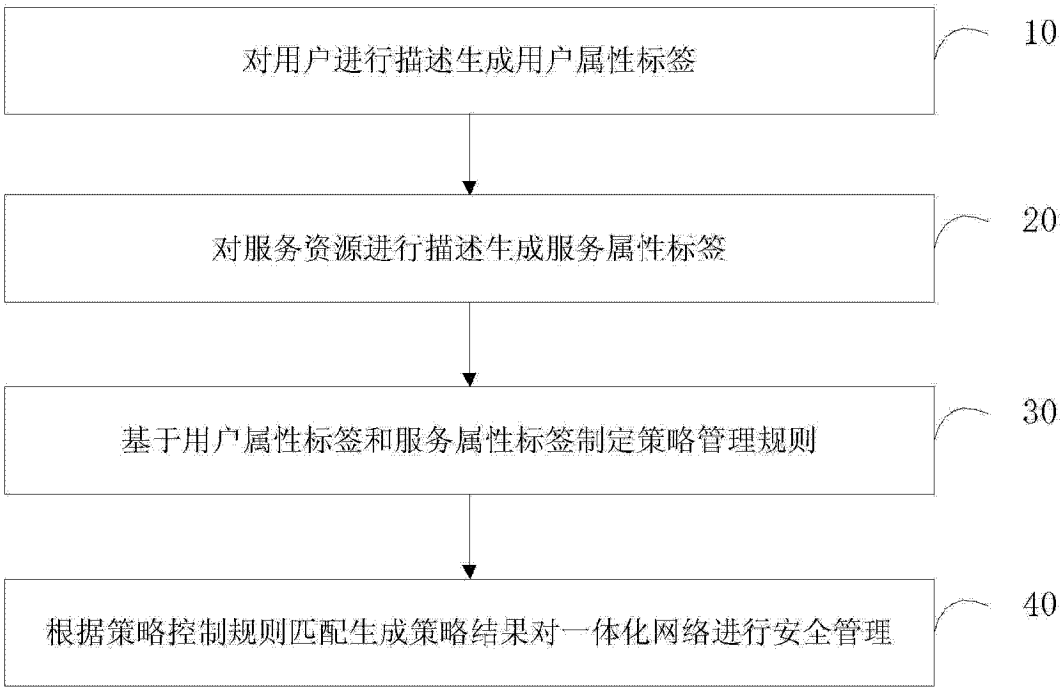

对用户进行描述生成用户属性标签
10
对服务资源进行描述生成服务属性标签
20
基于用户属性标签和服务属性标签制定策略管理规则
30
根据策略控制规则匹配生成策略结果对一体化网络进行安全管理
40

图 2

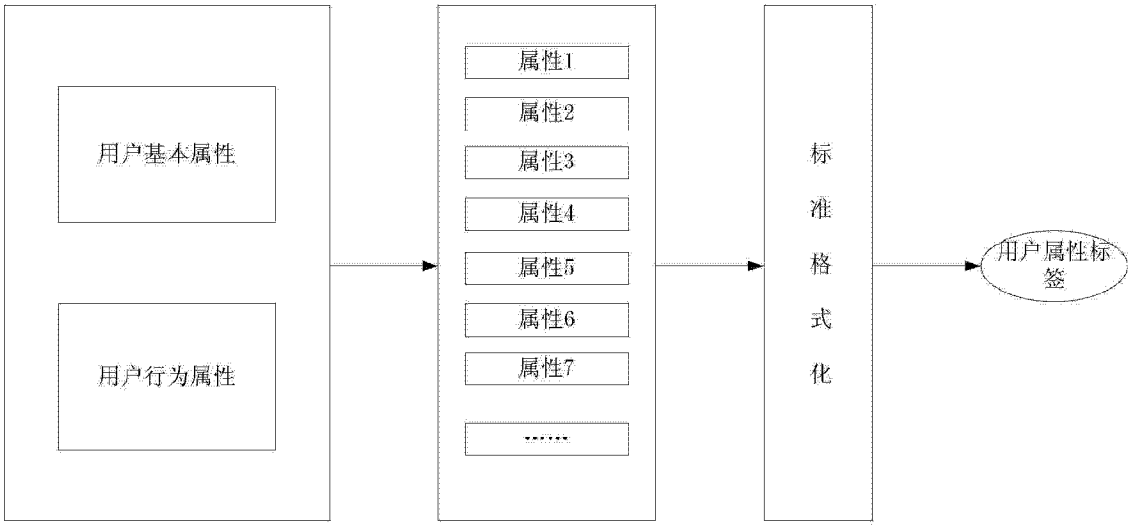

用户基本属性
用户行为属性
属性1
属性2
属性3
属性4
属性5
属性6
属性7
……
标准格式化
用户属性标签

图 3

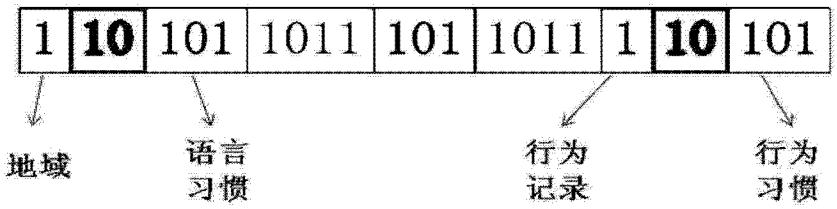

1 10 101 1011 101 1011 1 10 101
地域
语言习惯
行为记录
行为习惯

图 4

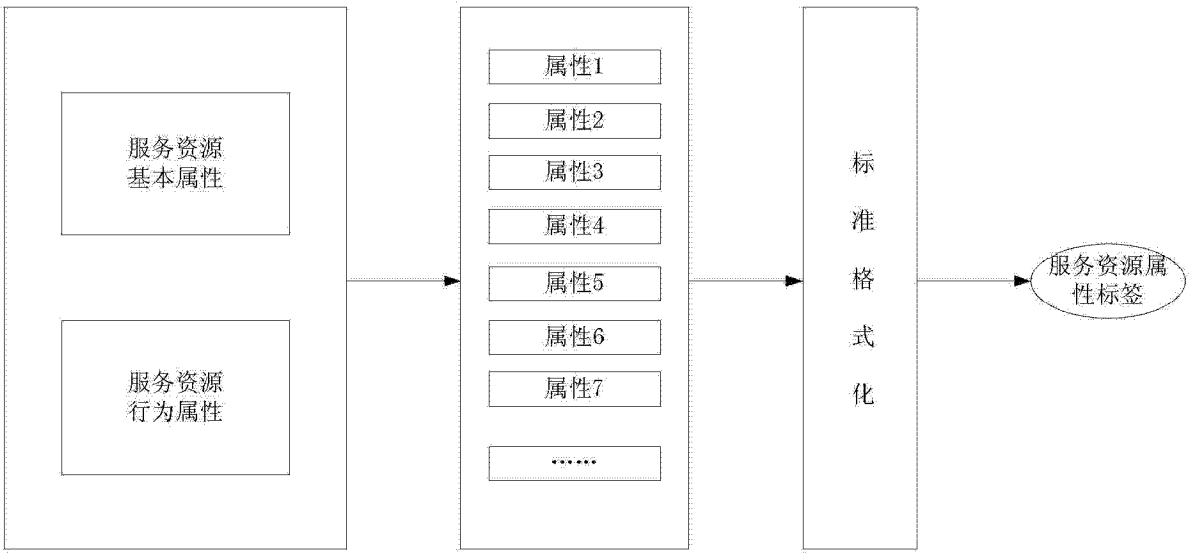

服务资源基本属性
服务资源行为属性
属性1
属性2
属性3
属性4
属性5
属性6
属性7
……
标准格式化
服务资源属性标签

图 5

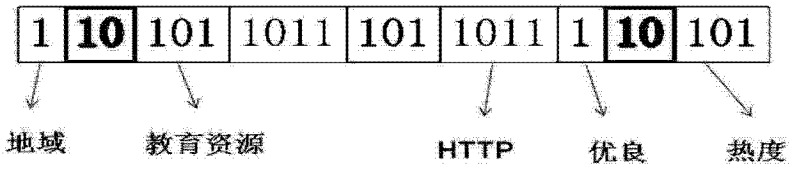

1 10 101 1011 101 1011 1 10 101
地域
教育资源
HTTP
优良
热度

图 6

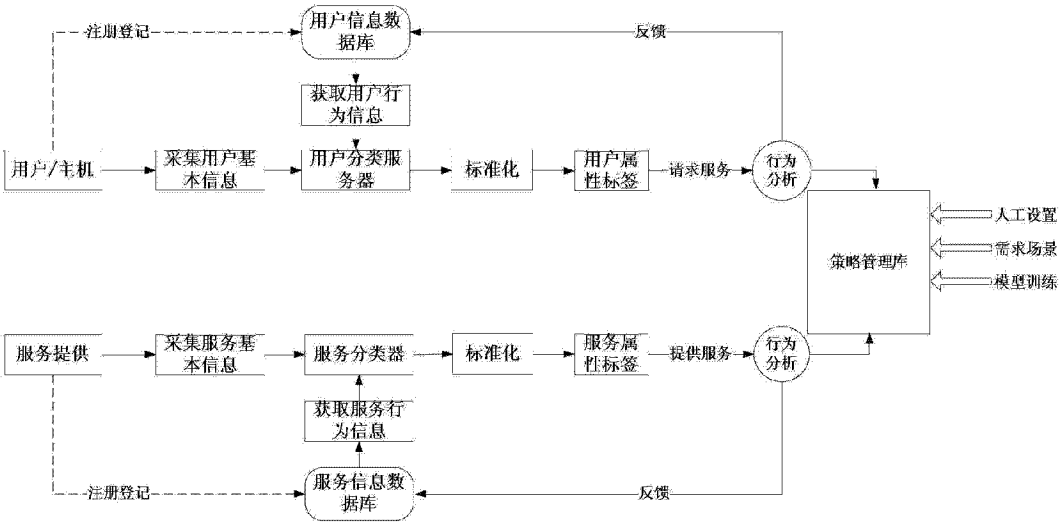

注册登记
用户信息数据库
反馈
获取用户行为信息
用户/主机
采集用户基本信息
用户分类服务器
标准化
用户属性标签
请求服务
行为分析
策略管理库
人工设置
需求场景
模型训练
服务提供
采集服务基本信息
服务分类器
标准化
服务属性标签
提供服务
行为分析
获取服务行为信息
注册登记
服务信息数据库
反馈

图 7

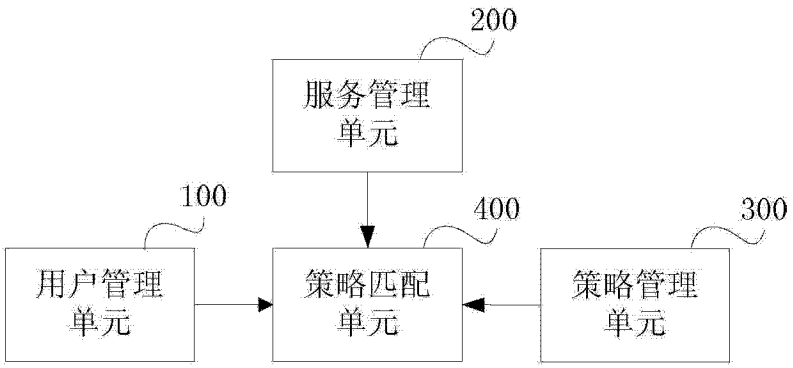

200
服务管理单元
100
400
300
用户管理单元
策略匹配单元
策略管理单元

图 8