(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 104052736 A
(43)申请公布日 2014.09.17

(21)申请号 201410148406.4

(22)申请日 2014.03.15

(30)优先权数据
61/800405 2013.03.15 US
14/092528 2013.11.27 US

(71)申请人 弗里塞恩公司
地址 美国弗吉尼亚州

(72)发明人 D·布拉卡 R·潘德兰吉

(74)专利代理机构 中国专利代理(香港)有限公司 72001
代理人 申屠伟进 徐红燕

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 29/12(2006.01)
H04L 9/32(2006.01)

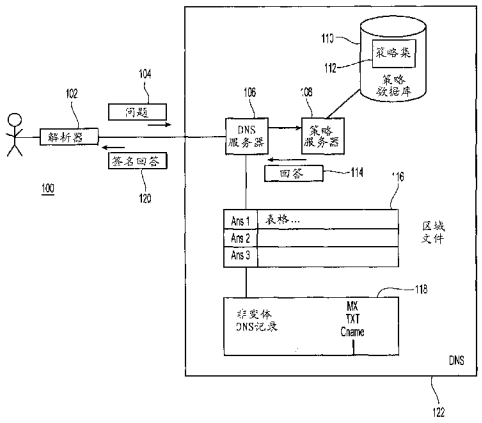
权利要求书1页 说明书6页 附图4页

(54)发明名称

用于预签名DNSSEC启用区域至记录集中的系统和方法

(57)摘要

本发明涉及用于预签名DNSSEC启用区域至记录集中的系统和方法。域名系统(DNS)可以接收和/或施加管理员或DNS运营商自身所希望的DNS策略集以管理用于网络域的具有安全性扩展的域名方案(DNSSEC)。DNS可以基于该策略集生成指向域的用户问题的回答集。基于策略规则而不同或变化的那些回答可以被存储为变体回答，并且可以用变体ID来标记。该变体回答可以被预签名并存储在DNS中。由于在DNS请求被接收之前生成和存储密钥数据和其它信息，所以请求的变体回答可以以更大的响应性和安全性返回。



CN 104052736 A

1. 一种管理域名系统操作的方法，包括：

使用具有安全性扩展的域名系统 (DNSSEC) 访问用于域名系统 (DNS) 操作的策略集；

基于该策略集，生成对与区域的域名集相关的问题的回答集；

根据该回答集和密钥数据集生成签名回答集；

将该签名回答集存储在区域文件中；

从解析器接收问题；以及

基于从解析器接收的问题以及该策略集取出签名回答以传输给解析器。

2. 如权利要求 1 所述的方法，其中访问该策略集包括从与该域名集相关的用户处接收策略集。

3. 如权利要求 1 所述的方法，其中访问该策略集包括施加由 DNS 生成的策略。

4. 如权利要求 1 所述的方法，其中访问该策略集包括安装默认策略集。

5. 如权利要求 1 所述的方法，其中生成签名回答集包括使用存储在密钥数据中的公和私密钥集生成该签名回答集。

6. 如权利要求 1 所述的方法，其中该策略集包括以下中的至少一个：

基于地理位置数据的策略，

基于负载均衡数据的策略，

基于日时信息的策略，

基于授权级别的策略，或

基于流量管理规则的策略。

7. 如权利要求 1 所述的方法，其中生成回答集包括基于与解析器和策略集相关的互联网协议 (IP) 地址生成回答集。

8. 如权利要求 1 所述的方法，其中该回答集包括下述中的至少一个：

与该域名集相关的互联网协议 (IP) 数据集，

与该域名集相关的所有权信息，

与该域名集相关的分类信息，

与该域名集相关的初始信息，或

与该域名集相关的过期信息。

9. 如权利要求 1 所述的方法，还包括升级该策略集。

10. 一种系统，包括：

至解析器的网络接口，传输与区域的域名集相关的问题，该域名在具有安全性扩展的域系统 (DNSSEC) 下操作；以及

处理器，经由该网络接口与该解析器通信，该处理器被配置为：

访问用于域名系统 (DNS) 操作的策略集，

基于该策略集，生成对与域名的区域集相关的问题的回答集，

根据该回答集和密钥数据集生成签名回答集，

将该签名回答集存储在区域文件中，

从解析器接收该问题，以及

基于该问题和该策略集取出签名回答以传输给解析器。

用于预签名 DNSSEC 启用区域至记录集中的系统和方法

[0001] 优先权

[0002] 要求 2013 年 3 月 15 日提交的、标题为“Systems and Methods for Pre-Signing of DNSSEC Enabled Zones into Record Sets”、序号 61 / 800,405 的美国临时专利申请的优先权，其内容通过引用被明确地合并到本文中。

技术领域

[0003] 本教导涉及用于预签名 DNSSEC 启用区域至记录集中的系统和方法，并且更具体地，涉及用于基于 DNS 系统策略管理从具有预签名的密钥签名数据的域名系统中生成回答的平台和技术。

背景技术

[0004] 在用于在互联网和其它网络上定位网站和其它资源的域名系统 (DNS) 的发展中，安全性问题随时间占据增加的重要性。响应于发展安全性需要，行业中的组织已对基线 DNS 协议提出和开发了扩展以允许在 DNS 服务的传递中引进安全性措施。一般来说这些已知的标准被称为具有安全性扩展的 DNS，或 DNSSEC。

[0005] 具体来说，需求本身已呈现为允许用户运行网络浏览器或其它软件以保证当试图导航至已知的通用资源定位器 (URL) 时传递给它们的互联网协议 (IP) 地址是真的，并且表示它们正试图访问的网站。由于缓存中毒或对 DNS 服务器的其它攻击，伪 IP 地址可能被传递给不知情的用户，DNS 服务器用于取出和供应给定域名的 IP 地址或由 DNS 系统提供的其它回答。

[0006] 在网站布署方面，现在许多网站由许多分层区段或分区组成，其中每个都有不同的扩展域名。例如，涉及体育新闻的网站可以具有根等级诸如 SportsPage.com，并且此外许多区段或“区域”致力于单独的体育活动。那些标题可能反映在域（诸如 Golf.SportsPage.com、Soccer.SportsPage.com 等等）中。

[0007] 在 SportsPage.com 内导航的用户可以向支持网站的 DNS 系统提供一个或多个问题或请求，诸如 IP 地址，或其它信息。对用户问题的回答可以从网站内的各个区域内生成。为了确保用户收到一个有效的回答，DNSSEC 启用域要求用使用公 / 私密钥信息生成的签名来签名的一系列消息。尽管 DNSSEC 协议因此供应认证服务给通过网络属性导航的用户，但因为域的区域的深度和分层链接变得更加复杂，DNS 系统的处理和带宽资源上的负担变大。那个负担会即减小 DNS 响应性。

[0008] 此外，对于希望施加灵活的 DNS 策略同时使用 DNSSEC 布置的网站所有者，事情可能进一步复杂。也就是说，部署了具有许多区域的相对丰富的网站的运营商可能希望对个体请求者施加规则以便基于用户的位置、日时、服务器负载、和 / 或基于其它因素，它们的 DNS 查找或回答被指向不同的服务器、和 / 或域的区域。识别关于用户的信息，施加恰当的策略，并且然后生成将允许它们的具体回答被认证的必要签名，同样可能招致性能以及对系统响应性的用户感知方面的损失。

[0009] 可能需要提供用于预签名 DNSSEC 启用区域至记录集中的方法和系统，其中域名系统可以从域名所有者处接收任意策略集，将那些策略转换为预生成的签名回答集或其它区域文件，并基于所存储的资源记录将签名回答而不是必须按需生成和 / 或签名的回答传输至用户。

发明内容

[0010] 依照本发明的一个实施例，提供了管理域名系统操作的方法，该方法包括 ：

[0011] 使用具有安全性扩展的域名系统 (DNSSEC) 访问用于域名系统 (DNS) 操作的策略集 ；

[0012] 基于该策略集，生成对与区域的域名集相关的问题的回答集 ；

[0013] 根据该回答集和密钥数据集生成签名回答集 ；

[0014] 将该签名回答集存储在区域文件中 ；

[0015] 从解析器接收问题 ；以及

[0016] 基于从解析器接收的问题以及该策略集取出签名回答以传输给解析器。

[0017] 该方法还包括升级该策略集。

[0018] 该方法还包括基于该升级的策略集升级该回答集。

[0019] 依照本发明的另一个实施例，一种系统包括 ：

[0020] 至解析器的网络接口，传输与区域的域名集相关的问题，该域名在具有安全性扩展的域系统 (DNSSEC) 下操作 ；以及

[0021] 处理器，经由该网络接口与该解析器通信，该处理器被配置为 ：

[0022] 访问用于域名系统 (DNS) 操作的策略集，

[0023] 基于该策略集，生成对与域名的区域集相关的问题的回答集，

[0024] 根据该回答集和密钥数据集生成签名回答集，

[0025] 将该签名回答集存储在区域文件中，

[0026] 从解析器接收该问题，以及

[0027] 基于该问题和该策略集取出签名回答以传输给解析器。

[0028] 依照本发明的另一个实施例，访问该策略集包括从与该域名相关的用户处接收策略集。

[0029] 依照本发明的另一个实施例，访问该策略集包括施加由 DNS 生成的策略。

[0030] 依照本发明的另一个实施例，访问该策略集包括安装默认的策略集。

[0031] 依照本发明的另一个实施例，生成签名回答集包括使用存储在该密钥数据中的公密钥和私密钥集生成该签名回答集。

[0032] 依照本发明的另一个实施例，该策略集包括下述至少一个

[0033] 基于地理位置数据的策略，

[0034] 基于负载均衡数据的策略，

[0035] 基于日时信息的策略，

[0036] 基于授权级别的策略，或

[0037] 基于流量管理规则的策略 .

[0038] 依照本发明的另一个实施例，生成回答集包括基于与该解析器和该策略集相关的

互联网协议（IP）地址生成回答集。

[0039] 依照本发明的另一个实施例，该回答集包括下述至少一个

[0040] 与该域名集相关的互联网协议（IP）数据集，

[0041] 与该域名集相关的所有权信息，

[0042] 与该域名集相关的分类信息，

[0043] 与该域名集相关的初始信息，或

[0044] 与该域名集相关的过期信息。

[0045] 依照本发明的另一个实施例，该处理器还被配置成升级该策略集。

[0046] 依照本发明的另一个实施例，该处理器还被配置成基于该升级的策略集升级该回答集。

附图说明

[0047] 被合并到本说明书中并构成本说明书的部分的附图图示了本教导的实施方式并且与描述一起，用于解释本教导的原理。在图中：

[0048] 图 1 图示了依照各个实施方式，可以在用于预签名 DNSSEC 启用区域至记录集中的系统和方法中使用的整体域名环境；

[0049] 图 2 图示了依照各个实施方式，可以在用于预签名 DNSSEC 启用区域至记录集中的系统和方法中使用的区域文件的数据结构；

[0050] 图 3 图示了依照各个实施方式，可以在用于预签名 DNSSEC 启用区域至记录集中的系统和方法中使用的策略验证、签名数据生成、以及其它处理的流程图；以及

[0051] 图 4 图示了依照各种实施方式，可以在用于预签名 DNSSEC 启用区域至记录集中使用的示例性硬件、软件、和其它资源。

具体实施方式

[0052] 本教导的实施方式涉及用于预签名 DNSSEC 启用区域至记录集中的系统和方法。更具体地，实施方式涉及用于管理采用 DNSSEC 安全性的 DNS 实施方式的平台和技术。在那个环境中，依照本教导的平台和技术可以接收用于 DNS 操作的任意策略集，通过其可以执行回答问题的请求，诸如将域名解析到有效 IP 地址或其它中的请求。

[0053] DNS 系统可以从域名所有者或运营商处接收策略集、对照 DNS 系统本身的内部操作策略验证那些策略，并且合并可被用以生成有效回答的策略。该策略集还能或替代地包括由 DNS 系统本身的运营商供应的规则或策略，例如，向 DNS 底层结构施加负载均衡或其它逻辑。基于策略变量将变化或不同的回答可以被生成且存储在区域文件的资源记录集中，由变体标识符索引。可以用公 / 私密钥对预签名变体回答，使得当新问题到达 DNS 系统时，已经被签名的有效回答可以从区域文件表或其它记录中取出，并且传输至请求者。

[0054] 因此新的域名解析请求可以被更有效地解析，因为签名的数据不是运行中生成的。也可以更安全地执行那些操作，因为公 / 私密钥数据不必分配给支持 DNS 平台的各种服务器。可以实现其它的优点和益处。

[0055] 现在将详细参考在附图中图示的本教导的示例性实施方式。其中可能相同的参考数字在整个附图中将被用于指代相同或类似部分。

[0056] 图 1 图示了依照各方面的整体 DNS 环境 100，其中用于预签名 DNSSEC 启用区域至记录集中的系统和方法可以操作。在如所示的方面中，该 DNS 环境可包括与域名系统 (DNS) 122 通信的解析器 102 用于传送问题 104 以及接收签名回答 120。如本文中所用的，该签名回答 120 可以指代包含签名 DNS 记录的回答。DNS122 可以是或包括服务器、分布式服务器集、集群、基于云的服务、应用和 / 或其它硬件、资源、平台、或元件。

[0057] 问题 104 可以是或包括各种查询中的任何一种，诸如，举例来说，对关于给定域名、区域、和 / 或其它地点或位置的互联网协议 (IP) 地址的请求。该 IP 地址可以是 IPv4(32 位)、IPv6(128 位)、和 / 或其它格式。问题 104 还可以或替代地是对来自 DNS122 的其它信息的请求，诸如位置信息、证书信息、授权信息、服务器信息、网络信息、和 / 或其它结果或信息。解析器 102 可以经由互联网和 / 或其它公或私网络或信道与 DNS122 进行通信。解析器 102 可以由多方操作，包括例如域名的所有者或运营商、用于那些实体的系统管理员、或其它。

[0058] DNS122 可被配置成接收问题 104 以及生成与具有安全性扩展的 DNS(DNSSEC) 标准一致的签名回答 120，如由互联网工程任务组 (IETF) 和 / 或其它相关标准实体指定。一般来说，DNSSEC 的使用包括在支持给定域的服务器、与域相关的区域、和 / 或 DNS 网络中的其它元件之间对签名消息或数据的交换的使用。给 DNS 查询提供回答的服务器可以使用私密钥签名它们的回答，传输给信任链中的下一个服务器以认证提供的信息。签名回答或其它数据的接收者可以使用始发服务器的公密钥检验对该数据的认证。

[0059] 图示的 DNS122 可以主持或管理用于各种实体的 DNS 平台或服务。例如，DNS122 可以为希望使其 DNS 操作由外部资源提供的第三方订户提供 DNS 服务。同样可以采用 DNS122 来支持用于实体自身网络的 DNS 服务，或可以支持其它布置下的 DNS 服务。

[0060] DNS122 一般可合并许多元件或资源以执行启用 DNSSEC 的 DNS 操作，同时使用策略集 112 来确定对进入的问题的回答或者可能涉及域名和 / 或与该域名相关的区域集或与域名和 / 或与该域名相关的区域集相关的请求。DNS122 可以合并 DNS 服务器 106(或多个服务器)，其与策略服务器 108 通信以生成或取出对问题 104 的回答 114。可以如指出的那样基于该策略集 112 生成或取出回答 114，该策略集可存储在策略数据库 110 和 / 或在 DNS122 中被主持或与 DNS122 相关的其它数据存储中。依照各方面，该策略集 112 可被施加到问题 104 和 / 或回答 114 以响应于问题 104 而创建信息的预生成集。该预生成的信息可被分割成依赖于在该策略集 112 中指定的变量和策略而不同或变化的信息，以及不依赖于在该策略集 112 中指定的变量和策略而不同或变化的信息。

[0061] 该策略集 112 可以是或包括脚本或其它逻辑、程序设计、条件、或者规则集，它们确定对解析器问题 104 的回答 114 在其下被生成和供应给请求用户的条件。该策略集 112 可包括地理位置规则，例如指定以特定地理区域作出请求的用户的 IP 地址可被指向与 DNS122 相关的特定服务器。也可以施加基于日时的规则，诸如当接收问题 104 时。该策略集 112 可以进一步包括基于负载均衡准则的规则以平衡掉与 DNS122 相关的服务器上的负载。该策略集 112 同样可以包括其它规则、测试、试探、或策略。例如，该策略集 112 可以包括诸如由 Daniel James 和 Arunabho Das 在 2013 年 3 月 15 日提交的、序号 __、标题为 “High Performance DNS Traffic Management”、代理人案号第 11569.0210、并且被转让给或在转让的义务下给与本申请相同的实体的、共同未决美国申请中所描述那些的规则和逻

辑，该申请通过引用以其整体被合并。

[0062] 在各情况中，该策略集 112 可以被由 DNS122 支持的域名的所有者或运营商提供。该策略集 112 还可以或替代地由 DNS122 的所有者或运营商本身和 / 或由其它用户或资源指定。

[0063] 在接收和安装该策略集 112 后，在实施方式中，DNS122 可以比照 DNS122 的内部规则或策略检验或验证那些策略，以确保由解析器 102 和 / 或其它用户提供的策略不与 DNS122 的内部操作冲突。依照进一步的实施方式，在解析器 102 和 / 或其它用户不能供应必要策略全集的情况下，DNS122 可以对相关域名的操作施加默认的规则或策略。

[0064] 在该策略集 112 被安装后，DNS122 可以使用那个规则或逻辑集生成与域名和 / 或其相关区域相关的回答。依照各方面，以及如在图 1 中所示，回答可以编码在区域文件 116 中。该区域文件 116 可以以表格的形式存储，由针对每个可能回答的标识符（例如，如所示的回答 1、回答 2、回答 3...）基于该策略集 112 索引。在实施方式中，给定的该策略集 112 以及域的相关域名记录，则生成或知道问题 104 的所有可能回答可以是可能的。在实例中，例如，回答的总数目可能相对小，例如 5、10、或另外数目的可能回答。较小数目的回答可以有助于更大的系统响应性，但是将理解的是还可以生成和存储更大集合的回答。

[0065] 如所示的，由 DNS122 发展的回答可以被分割成两个整体组：基于该策略集 112 和 / 或其它因素将会不同或变化的一个集，和将不会不同或变化的另一个集。当接收到要求那些动态选择的回答之一的问题 104 时，如上所述，变化的回答可以作为“变体答案”被存储在区域文件 116 中供取出。那些变体回答可基于变体 ID 被索引或键控，并且当接收到相应的问题 104 时被取出以发送至解析器 102。变体回答数据可以例如包括针对不同服务位置的不同 IP 地址值，和 / 或包括不同别名 (CNAME)，以及其它信息。不变化的回答可以存储在非变体 DNS 记录 118 中。例如，该非变体 DNS 记录集在域名的给定示例中可以是或包括：与邮件交换 (MX) 数据相关的数据、文本 (TXT) 数据、别名 (CNAME) 数据、或其它类型数据。但是将明白的是，在其它的实施方式中，数据的所述类型 (MX 等）可以合并入存储在区域文件 116 中的变体回答信息中，和 / 或其它信息可以存储在非变体 DNS 记录 118 中的。

[0066] 随着问题 104 在 106 被接收，数据从 116 中取出并且 108 用于使用策略服务器 108 选择从区域文件 116 中取出的回答 114 或回答 114 的组成部分。数据可以替代地或额外地从 118 中取出。从 116 和 / 或 118 取出的数据可以被组合和编码在签名回答 120 中，签名回答 120 被返回至解析器 102。

[0067] 图 2 图示了可以在区域文件 116 中使用的示例性数据结构。在所示的实施方式中，区域文件 116 可以编码或存储各种信息，包括变体 ID124，其可以作为密钥或索引用到存储在区域文件 116 中的表中。其它信息（诸如所有者名、分类、类型、记录数据 (rdata)、初始、和过期）可以记录在区域文件 116 中。区域文件 116 还可以包括基于与由变体 ID124 标识的每个变体回答相关的密钥数据的签名 126。签名 126 可以由解析器 102 或其它用户使用公密钥信息检查以确保签名的回答 120 是可信的并且能被依赖。因此该签名的回答 120 可以在自发或运行中基础上被取出并且传输至解析器 102 而无需生成回答本身，或针对回答的签名 126。

[0068] 依照各方面，图 3 图示了可以在用于预签名 DNSSEC 启用区域至记录集中的系统和方法中执行的策略调节、签名数据通路生成、以及其它处理的流程图。在 302 中，处理可以

开始。在 304 中，对于给定的或主题区域，DNS122 可以标识将基于该策略集 112 而变化或不同的策略依赖的记录。在 306 中，DNS122 可以为由该策略集 112 的应用产生的每个变体记录集限定或生成所有可能的值。在 308 中，DNS122 可以标识用于从该策略集 112 中选择每个变体回答的一个或多个策略。

[0069] 在 310 中，DNS122 可以单独签名区域文件 116，该区域文件 116 包括由该策略集 112 产生的每个变体回答。对区域文件 116 的签名可以通过使用脱机访问的密钥数据而被执行，密钥数据存储在分离的系统中，该单独系统包括专用密钥数据存储系统，或其它存储或主机。在 312 中，DNS122 可以从解析器 102 接收问题 104，诸如对 IP 地址的请求和 / 或其它查询或请求。在 314 中，如果问题 104 被 DNS122 确定为请求变体资源记录集（而不是非变体 DNS 记录 118），则 DNS122 可以调用该策略集 112 中的一个或多个相关策略以挑选或选择签名回答 120。在 316 中，DNS122 可以基于所选择的一个或多个策略而将签名回答 120 返回至解析器 102。在 318 中，处理可以重复，返回至之前的处理点，跳转至进一步处理点，或结束。

[0070] 图 4 图示了依照各实施方式的、可以被合并在 DNS122 中的各种硬件、软件、和其它资源。在所示的实施方式中，DNS122 可以包含平台，该平台包括与存储器 142（诸如电随机访问存储器）通信的处理器 140，在操作系统 146 控制下或连同操作系统 146 一起进行操作。实施方式中的处理器 140 可以被合并在一个或多个服务器、集群、和 / 或其它计算机或硬件资源中，和 / 或可以使用基于云的资源来实施。操作系统 146 可以是例如分布式 Linux™ 操作系统、Unix™ 操作系统、或其它开源或专有的操作系统或平台。处理器 140 可以与数据存储 148（诸如存储在本地硬驱动器或驱动器阵列上的数据库）通信，以访问或存储一个或多个区域文件 116、其它 DNS 记录、和 / 或其选择的子集，以及其它内容、媒介、或其它数据。处理器 140 还可以与网络接口 150（诸如以太网或无线数据连接）通信，网络接口 150 进而与一个或多个网络 152（诸如互联网或其它公共或私有网络）通信。一般来说，处理器 140 可以编程或配置为在 DNS122 的控制下执行控制逻辑以及控制各种处理操作，包括处理问题 104、策略集 112、IP 地址信息、和 / 或涉及 DNS 操作的其它数据或信息。在各方面中，解析器 102 以及在主题域中的任何区域服务器可以是或包括类似于 DNS122 中的那些的资源，和 / 或可包括额外的或不同的硬件、软件、和 / 或其它资源。DNS122、解析器 102、相关网络相连、以及其它硬件、软件、和服务资源的其它配置是可能的。

[0071] 前面的描述是说明性的，并且对本领域技术人员来说，可以发生配置和实施方式中的变化。例如，尽管已经描述了在其中一个 DNS122 平台或元件支持给定域的实施方式，但是在各实施方式中，可以应用两个或多个域名系统 (DNS) 来支持域。被描述为单个或集成的其它资源在实施方式中可以是复数个或分布式的，并且被描述为多个或分布式的资源在实施方式中可以被组合。因此本教导的范围意图仅仅由所附权利要求来限定。

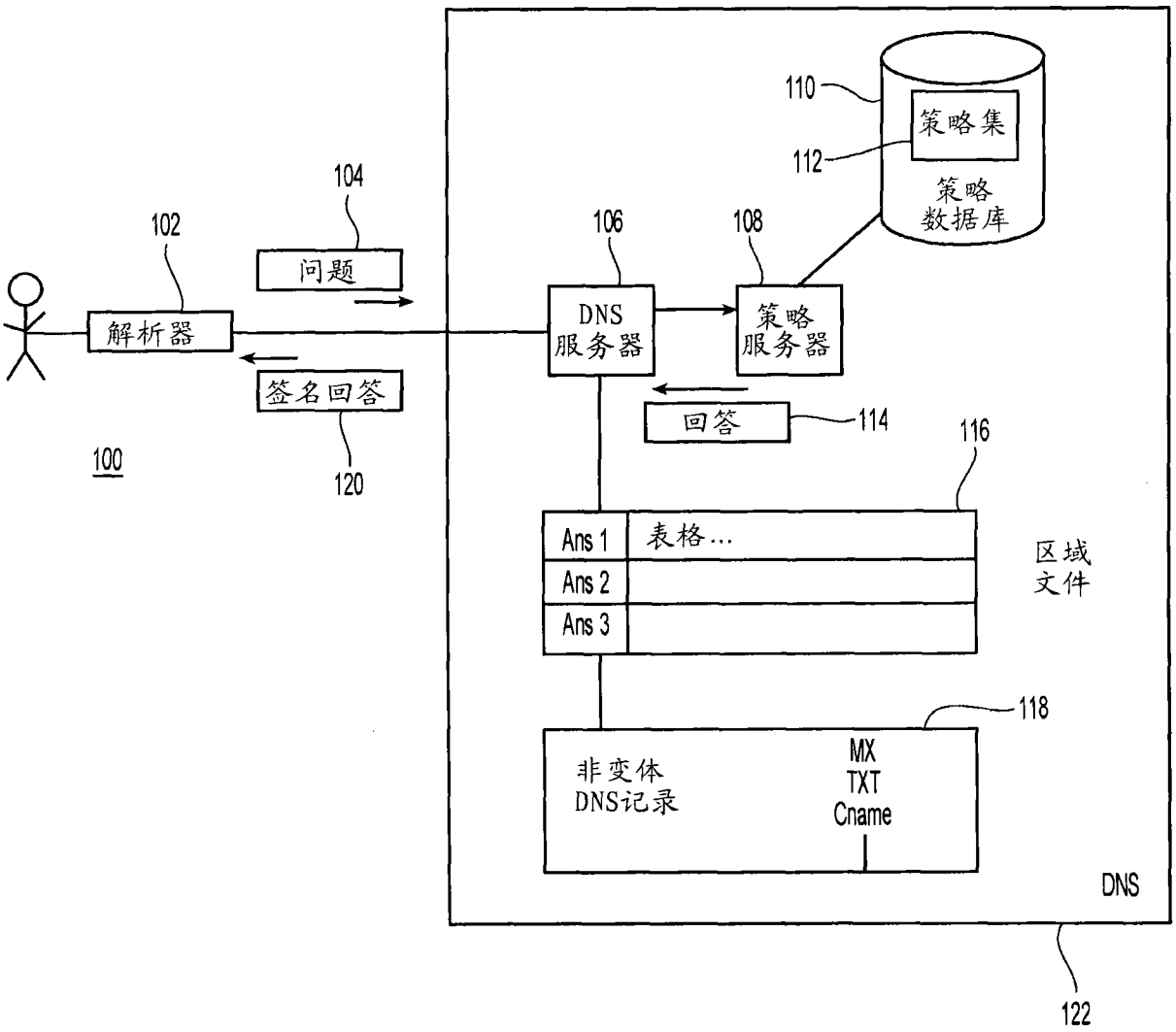

110
策略集
112
策略
数据库
104
102
106
108
问题
DNS
服务器
策略
服务器
解析器
签名回答
回答
114
116
100
120
Ans 1
表格...
Ans 2
Ans 3
区域
文件
118
非变体
DNS记录
MX
TXT
Cname
DNS
122

图 1

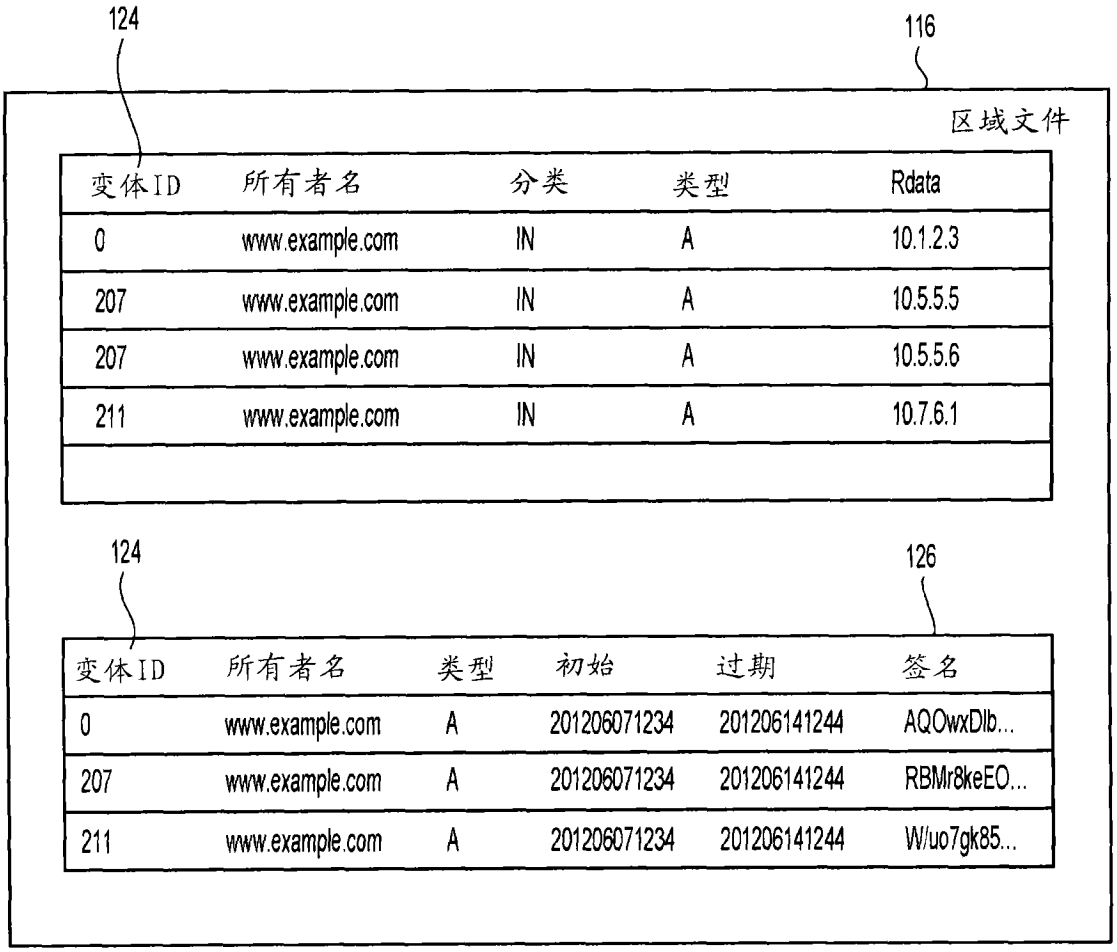

124
116
区域文件
变体ID 所有者名 分类 类型 Rdata
0 www.example.com IN A 10.1.2.3
207 www.example.com IN A 10.5.5.5
207 www.example.com IN A 10.5.5.6
211 www.example.com IN A 10.7.6.1
124
126
变体ID 所有者名 类型 初始 过期 签名
0 www.example.com A 201206071234 201206141244 AQOwxDlb...
207 www.example.com A 201206071234 201206141244 RBMr8keEO...
211 www.example.com A 201206071234 201206141244 W/uo7gk85...

图 2

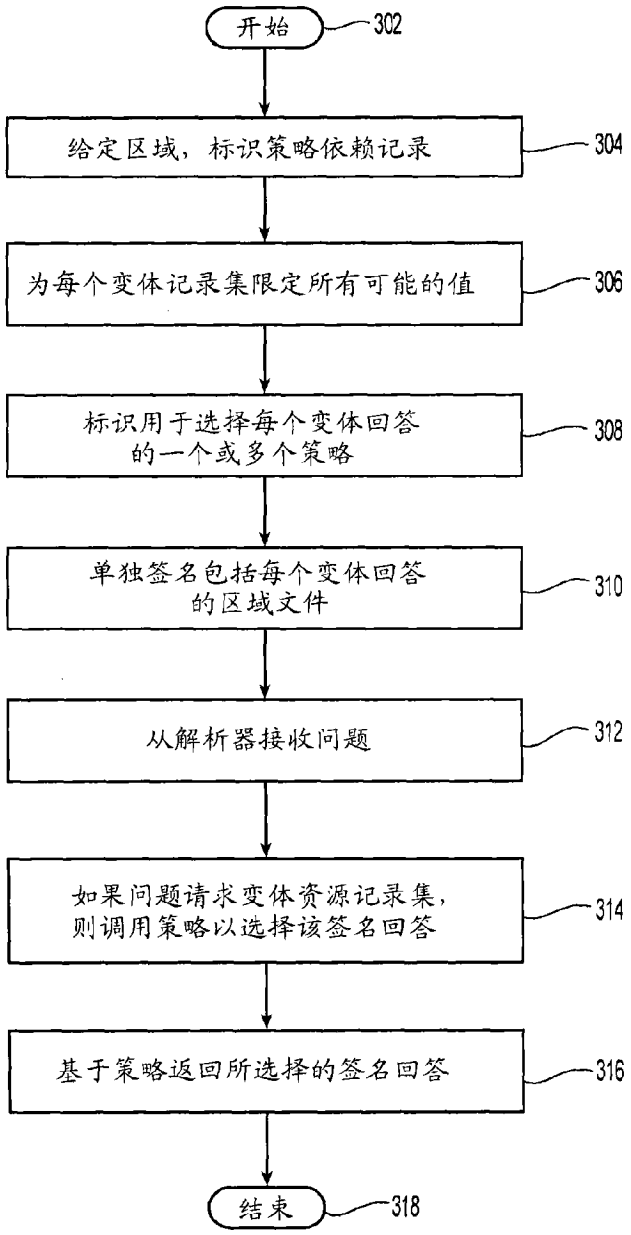

开始
302
给定区域，标识策略依赖记录
304
为每个变体记录集限定所有可能的值
306
标识用于选择每个变体回答的一个或多个策略
308
单独签名包括每个变体回答的区域文件
310
从解析器接收问题
312
如果问题请求变体资源记录集，则调用策略以选择该签名回答
314
基于策略返回所选择的签名回答
316
结束
318

图 3

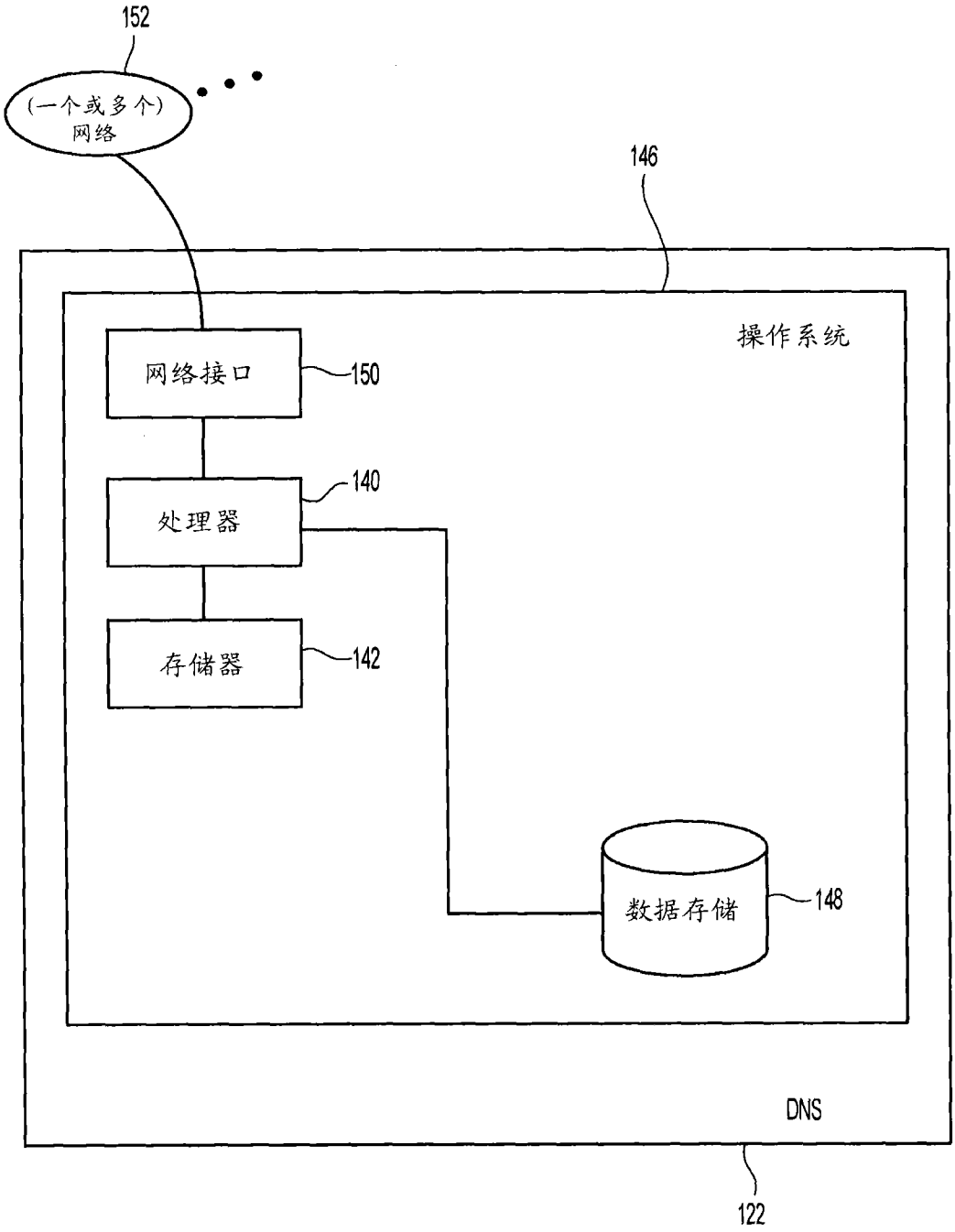


图 4