(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 105939330 A
(43)申请公布日 2016.09.14

(21)申请号 201610079813.3

(22)申请日 2016.02.04

(71)申请人 杭州迪普科技有限公司
地址 310051 浙江省杭州市滨江区通和路68号中财大厦6层

(72)发明人 周守亚

(74)专利代理机构 北京博思佳知识产权代理有限公司 11415
代理人 林祥

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

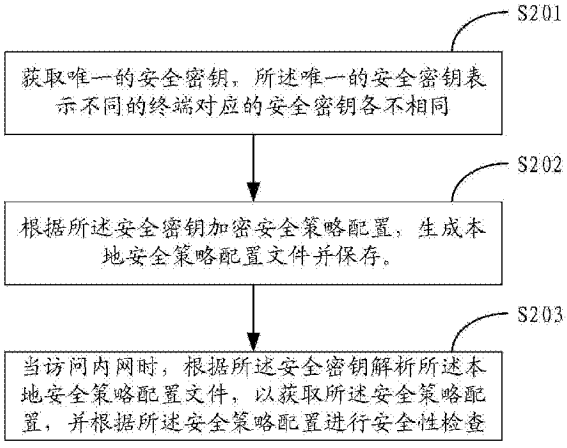
权利要求书2页 说明书9页 附图8页

(54)发明名称

处理本地安全策略配置的方法及装置

(57)摘要

本申请提供处理本地安全策略配置的方法及装置，所述方法包括：获取唯一的安全密钥，所述唯一的安全密钥表示不同的终端对应的安全密钥各不相同；根据所述安全密钥加密安全策略配置，生成本地安全策略配置文件并保存；当访问内网时，根据所述安全密钥解析所述本地安全策略配置文件，以获取所述安全策略配置，并根据所述安全策略配置进行安全性检查。应用本申请实施例，有效地避免了终端上的本地安全策略配置泄密，导致不安全的终端访问内网，对内网的安全造成威胁。



CN 105939330 A

1.一种处理本地安全策略配置的方法，其特征在于，所述方法应用在终端上，所述方法包括：

获取唯一的安全密钥，所述唯一的安全密钥表示不同的终端对应的安全密钥各不相同；

根据所述安全密钥加密安全策略配置，生成本地安全策略配置文件并保存；

当访问内网时，根据所述安全密钥解析所述本地安全策略配置文件，以获取所述安全策略配置，并根据所述安全策略配置进行安全性检查。

2.根据权利要求1所述的方法，其特征在于，所述获取唯一的安全密钥包括：

向生成所述安全策略配置的服务器请求获取安全密钥，以使服务器生成服务器安全密钥，且服务器根据不同终端生成的服务器安全密钥各不相同；

接收所述服务器返回的服务器安全密钥，并保存所述服务器安全密钥作为所述唯一的安全密钥。

3.根据权利要求1所述的方法，其特征在于，所述获取唯一的安全密钥包括：

向生成所述安全策略配置的服务器请求获取安全密钥，以使服务器生成服务器安全密钥；

接收所述服务器返回的服务器安全密钥；

根据所述终端的硬件属性标识，生成终端安全密钥；

按照预设的组合规则，根据所述终端安全密钥与所述服务器安全密钥生成新的安全密钥，将所述新的安全密钥作为所述唯一的安全密钥。

4.根据权利要求2所述的方法，其特征在于，所述根据所述安全密钥解析所述本地安全策略配置文件，包括：

获取所述服务器安全密钥；

根据所述服务器安全密钥解析所述本地安全策略配置文件。

5.根据权利要求3所述的方法，其特征在于，所述根据所述安全密钥解析所述本地安全策略配置文件，包括：

获取所述服务器安全密钥；

根据所述终端的硬件属性标识，生成终端安全密钥；

按照预设的组合规则，根据所述终端安全密钥与所述服务器安全密钥生成新的安全密钥；

根据所述新的安全密钥，解析所述本地安全策略配置文件。

6.一种处理本地安全策略配置的装置，其特征在于，所述装置应用在终端上，所述装置包括：

获取单元，用于获取唯一的安全密钥，所述唯一的安全密钥表示不同的终端对应的安全密钥各不相同；

加密单元，用于根据所述安全密钥加密安全策略配置，生成本地安全策略配置文件并保存；

解析单元，用于当访问内网时，根据所述安全密钥解析所述本地安全策略配置文件，以获取所述安全策略配置，并根据所述安全策略配置进行安全性检查。

7.根据权利要求6所述的装置，其特征在于，所述获取单元包括：

第一请求子单元，用于向生成所述安全策略配置的服务器请求获取安全密钥，以使服务器生成服务器安全密钥，且服务器根据不同终端生成的服务器安全密钥各不相同；

第一接收子单元，用于接收所述服务器返回的服务器安全密钥，并保存所述服务器安全密钥作为所述唯一的安全密钥。

8.根据权利要求6所述的装置，其特征在于，所述获取单元包括：

第二请求子单元，用于向生成所述安全策略配置的服务器请求获取安全密钥，以使服务器生成服务器安全密钥；

第二接收子单元，用于接收所述服务器返回的服务器安全密钥；

第一生成子单元，用于根据所述终端的硬件属性标识，生成终端安全密钥；

第一组合子单元，用于按照预设的组合规则，根据所述终端安全密钥与所述服务器安全密钥生成新的安全密钥，将所述新的安全密钥作为所述唯一的安全密钥。

9.根据权利要求7所述的装置，其特征在于，所述解析单元包括：

第一获取子单元，用于获取所述服务器安全密钥；

第一解析子单元，用于根据所述服务器安全密钥解析所述本地安全策略配置文件。

10.根据权利要求8所述的装置，其特征在于，所述解析单元包括：

第二获取子单元，用于获取所述服务器安全密钥；

第二生成子单元，用于根据所述终端的硬件属性标识，生成终端安全密钥；

第二组合子单元，用于按照预设的规则，根据所述终端安全密钥与所述服务器安全密钥生成新的安全密钥；

第二解析子单元，用于根据所述新的安全密钥，解析所述本地安全策略配置文件。

处理本地安全策略配置的方法及装置

技术领域

[0001] 本申请涉及网络通信技术领域，尤其涉及处理本地安全策略配置的方法及装置。

背景技术

[0002] TAC(Terminal Access Control，终端接入控制)解决方案通过对接入内网(例如，企业网)的终端强制实施终端安全策略配置，有效地加强了终端的自动防御能力，避免接入内网的终端不安全，对内网的安全造成威胁。现有技术中，终端接入内网，在通过身份认证后，可以向TAC服务器请求获取安全策略配置，并通过关键字密钥加密TAC服务器提供的安全策略配置，生成本地安全策略配置文件并保存。终端在对内网进行访问时，解析该本地安全策略配置文件，获取安全策略配置，根据该安全策略配置对自身安全状态进行检查，例如，自身的系统补丁是否已升级，病毒库是否更新为最新版本等等。检查结果为安全的终端可以对内网进行访问。

[0003] 然而，若终端上的本地安全策略配置文件被复制到其它终端上时，由于每个终端上预先设置有关键字密钥，且不同终端上的关键字密钥都相同，因此其他终端也可以通过自身的关键字密钥解析该终端上的本地安全策略配置文件，导致终端上的本地安全策略配置泄密，例如，攻击者篡改终端上的本地安全策略配置，使得终端无法根据本地安全策略配置准确检测自身的安全性，很有可能导致不安全的终端访问内网，对内网的安全造成威胁。

发明内容

[0004] 有鉴于此，本申请提供一种处理本地安全策略配置的方法及装置，以实现有效地避免终端上的本地安全策略配置泄密，导致不安全的终端访问内网，对内网的安全造成威胁。

[0005] 具体地，本申请是通过如下技术方案实现的：

[0006] 根据本申请实施例的第一方面，提供处理本地安全策略配置的方法，该方法应用在终端上，包括：

[0007] 获取唯一的安全密钥，所述唯一的安全密钥表示不同的终端对应的安全密钥各不相同；

[0008] 根据所述安全密钥加密安全策略配置，生成本地安全策略配置文件并保存；

[0009] 当访问内网时，根据所述安全密钥解析所述本地安全策略配置文件，以获取所述安全策略配置，并根据所述安全策略配置进行安全性检查。

[0010] 在一个实施例中，所述获取唯一的安全密钥包括：

[0011] 向生成所述安全策略配置的服务器请求获取安全密钥，以使服务器生成服务器安全密钥，且服务器根据不同终端生成的服务器安全密钥各不相同；

[0012] 接收所述服务器返回的服务器安全密钥，并保存所述服务器安全密钥作为所述唯一的安全密钥。

[0013] 在另一个实施例中，所述获取唯一的安全密钥包括：

[0014] 向生成所述安全策略配置的服务器请求获取安全密钥，以使服务器生成服务器安全密钥；

[0015] 接收所述服务器返回的服务器安全密钥；

[0016] 根据所述终端的硬件属性标识，生成终端安全密钥；

[0017] 按照预设的组合规则，根据所述终端安全密钥与所述服务器安全密钥生成新的安全密钥，将所述新的安全密钥作为所述唯一的安全密钥。

[0018] 在另一个实施例中，所述根据所述安全密钥解析所述本地安全策略配置文件，包括：

[0019] 获取所述服务器安全密钥；

[0020] 根据所述服务器安全密钥解析所述本地安全策略配置文件。

[0021] 在另一个实施例中，所述根据所述安全密钥解析所述本地安全策略配置文件，包括：

[0022] 获取所述服务器安全密钥；

[0023] 根据所述终端的硬件属性标识，生成终端安全密钥；

[0024] 按照预设的组合规则，根据所述终端安全密钥与所述服务器安全密钥生成新的安全密钥；

[0025] 根据所述新的安全密钥，解析所述本地安全策略配置文件。

[0026] 根据本申请实施例的第二方面，提供处理本地安全策略配置的装置，该装置应用在终端上，包括：

[0027] 获取单元，用于获取唯一的安全密钥，所述唯一的安全密钥表示不同的终端对应的安全密钥各不相同；

[0028] 加密单元，用于根据所述安全密钥加密安全策略配置，生成本地安全策略配置文件并保存；

[0029] 解析单元，用于当访问内网时，根据所述安全密钥解析所述本地安全策略配置文件，以获取所述安全策略配置，并根据所述安全策略配置进行安全性检查。

[0030] 在一个实施例中，所述获取单元包括：

[0031] 第一请求子单元，用于向生成所述安全策略配置的服务器请求获取安全密钥，以使服务器生成服务器安全密钥，且服务器根据不同终端生成的服务器安全密钥各不相同；

[0032] 第一接收子单元，用于接收所述服务器返回的服务器安全密钥，并保存所述服务器安全密钥作为所述唯一的安全密钥。

[0033] 在另一个实施例中，所述获取单元包括：

[0034] 第二请求子单元，用于向生成所述安全策略配置的服务器请求获取安全密钥，以使服务器生成服务器安全密钥；

[0035] 第二接收子单元，用于接收所述服务器返回的服务器安全密钥；

[0036] 第一生成子单元，用于根据所述终端的硬件属性标识，生成终端安全密钥；

[0037] 第一组合子单元，用于按照预设的组合规则，根据所述终端安全密钥与所述服务器安全密钥生成新的安全密钥，将所述新的安全密钥作为所述唯一的安全密钥。

[0038] 在另一个实施例中，所述解析单元包括：

[0039] 第一获取子单元，用于获取所述服务器安全密钥；

[0040] 第一解析子单元，用于根据所述服务器安全密钥解析所述本地安全策略配置文件。

[0041] 在另一个实施例中，所述解析单元包括：

[0042] 第二获取子单元，用于获取所述服务器安全密钥；

[0043] 第二生成子单元，用于根据所述终端的硬件属性标识，生成终端安全密钥；

[0044] 第二组合子单元，用于按照预设的规则，根据所述终端安全密钥与所述服务器安全密钥生成新的安全密钥；

[0045] 第二解析子单元，用于根据所述新的安全密钥，解析所述本地安全策略配置文件。

[0046] 本实施例处理本地安全策略配置的方法，通过获取一个唯一的安全密钥，该唯一的安全密钥表示不同终端获取到的安全密钥各不相同，使用该唯一的安全密钥加密安全策略配置，生成本地安全策略配置文件并保存。由于不同终端的安全密钥各不相同，即使该终端上的本地安全策略配置文件被复制到了其它终端上，其它终端也无法使用自身的安全密钥解析该本地安全策略配置文件，从而避免了安全策略配置泄密，导致不安全的终端访问内网，有效地保证了内网的安全。

附图说明

[0047] 图1示例了本申请实施例实现处理本地安全策略配置的方法的应用场景示意图。

[0048] 图2示例了本申请处理本地安全策略配置的方法的一个实施例流程图。

[0049] 图3示例了本申请处理本地安全策略配置中保存本地安全策略配置的方法的一个实施例流程图。

[0050] 图4示例了本申请处理本地安全策略配置中解析本地安全策略配置的方法的一个实施例流程图。

[0051] 图5示例了本申请处理本地安全策略配置中保存本地安全策略配置的方法的另一个实施例流程图。

[0052] 图6示例了本申请处理本地安全策略配置中解析本地安全策略配置的方法的另一个实施例流程图。

[0053] 图7为本申请处理本地安全策略配置的装置所在终端的一种硬件结构图。

[0054] 图8示例了本申请处理本地安全策略配置的装置的一个实施例框图。

[0055] 图9示例了本申请处理本地安全策略配置的装置的另一个实施例框图。

[0056] 图10示例了本申请处理本地安全策略配置的装置的另一个实施例框图。

具体实施方式

[0057] 这里将详细地对示例性实施例进行说明，其示例表示在附图中。下面的描述涉及附图时，除非另有表示，不同附图中的相同数字表示相同或相似的要素。以下示例性实施例中所描述的实施方式并不代表与本申请相一致的所有实施方式。相反，它们仅是与如所附权利要求书中所详述的、本申请的一些方面相一致的装置和方法的例子。

[0058] 在本申请使用的术语是仅仅出于描述特定实施例的目的，而非旨在限制本申请。在本申请和所附权利要求书中所使用的单数形式的“一种”、“所述”和“该”也旨在包括多数形式，除非上下文清楚地表示其他含义。还应当理解，本文中使用的术语“和/或”是指并包

含一个或多个相关联的列出项目的任何或所有可能组合。

[0059] 应当理解，尽管在本申请可能采用术语第一、第二、第三等来描述各种信息，但这些信息不应限于这些术语。这些术语仅用来将同一类型的信息彼此区分开。例如，在不脱离本申请范围的情况下，第一信息也可以被称为第二信息，类似地，第二信息也可以被称为第一信息。取决于语境，如在此所使用的词语“如果”可以被解释成为“在……时”或“当……时”或“响应于确定”。

[0060] 随着企业信息化办公越来越普及，接入内网(例如，企业网)的终端数量在不断增加，并且终端应用日益复杂化。为了保障内网安全，需对终端进行接入控制和访问管理。TAC解决方案通过对接入内网(例如，企业网)的终端强制实施终端安全策略配置，有效地加强了终端的自动防御能力，避免接入内网的终端不安全，对内网的安全造成威胁。

[0061] 为了更好的实现上述功能，本申请提供了处理本地安全策略配置的方法。如图1所示，示例了本申请实施例实现处理本地安全策略配置的方法的应用场景示意图。

[0062] 图1中，包括TAC服务器11、多个终端(如图1中所示的终端12至终端1n)，其中，每个终端在接入内网，通过身份认证后，均可以向TAC服务器请求获取安全策略配置。当终端接收到TAC服务器返回的安全策略配置后，为了避免安全策略配置泄密，例如，安全策略配置被恶意篡改，终端可以获取一个唯一的安全密钥，即不同终端获取到的安全密钥各不相同，使用该安全密钥对获取到的安全策略配置进行加密，生成本地安全策略配置文件并保存。当终端对内网进行访问时，可以通过该唯一的安全密钥解析所述保存的本地安全策略配置文件，获得安全策略配置，并根据该安全策略配置对自身的安全状态进行检查，例如，检查自身的系统补丁是否已升级、病毒库是否已更新为最新版本等等。当检查结果为安全时，该终端才可以访问内网，从而有效地保障了内网的安全。

[0063] 由于终端获取到安全策略配置后，通过唯一的安全密钥将安全策略配置加密，解析本地安全策略配置文件时，也需要使用该唯一的安全密钥解析，从而有效地避免了终端的安全策略配置泄密，避免了终端的安全策略配置被恶意篡改，使得终端无法根据安全策略配置准确检查自身安全性，导致不安全的终端可以访问内网，对内网的安全造成威胁。

[0064] 为了详细的说明终端是如何处理获取到的安全策略配置的，结合图1所示的应用场景示意图，如下图2，示例了本申请处理本地安全策略配置的方法的一个实施例流程图，以其中的一台终端，例如，终端12，执行该方法为例，包括以下步骤：

[0065] 步骤S201：获取唯一的安全密钥，所述唯一的安全密钥表示不同的终端对应的安全密钥各不相同。

[0066] 通过上述描述可知，为了避免终端上的本地安全策略配置泄密，终端12可以对本地安全策略配置加密。为了实现加密，终端可以获取一个安全密钥，且该安全密钥为唯一的安全密钥，即不同终端获取到的安全密钥各不相同。

[0067] 步骤S202：根据所述安全密钥加密安全策略配置，生成本地安全策略配置文件并保存。

[0068] 终端12根据所述安全密钥加密接收到的安全策略配置，生成本地安全策略配置文件并保存的过程可以参见现有技术，本申请对此不再详细赘述。

[0069] 步骤S203：当访问内网时，根据所述安全密钥解析所述本地安全策略配置文件，以获取所述安全策略配置，并根据所述安全策略配置进行安全性检查。

[0070] 由于终端已通过安全密钥将本地安全策略配置加密，当终端需要获取本地安全策略配置时，可以使用该安全密钥解析所述本地安全策略配置文件，从而获取本地安全策略配置，根据该本地安全策略配置对自身进行安全性检查，例如，检查自身的系统补丁是否已升级、病毒库是否已更新为最新版本等等。当检查结果为安全时，该终端才可以访问内网，从而有效地保障了内网的安全。

[0071] 本实施例处理本地安全策略配置的方法，通过获取一个唯一的安全密钥，该唯一的安全密钥表示不同终端获取到的安全密钥各不相同，使用该唯一的安全密钥加密安全策略配置，生成本地安全策略配置文件并保存。由于不同终端的安全密钥各不相同，即使该终端上的本地安全策略配置文件被复制到了其它终端上，其它终端也无法使用自身的安全密钥解析该本地安全策略配置文件，从而避免了安全策略配置泄密，导致不安全的终端访问内网，有效地保证了内网的安全。

[0072] 通过图2所描述的实施例，可以得出，处理本地安全策略配置可以分为两个过程：保存本地安全策略配置和解析本地安全策略配置。为了更详细地说明本申请是如何处理本地安全策略配置的，下面分别就保存本地安全策略配置和解析本地安全策略配置的过程分别进行详细描述。

[0073] 如下的图3，示例了本申请处理本地安全策略配置中保存本地安全策略配置的方法的一个实施例流程图，如下的图4，示例了本申请处理本地安全策略配置中解析本地安全策略配置的方法的一个实施例流程图。该图3和图4均以图2所示实施例为基础。其中，图3包括：

[0074] 步骤S301：向生成安全策略配置的服务器请求获取安全密钥，以使服务器生成服务器安全密钥，且服务器根据不同终端生成的服务器安全密钥各不相同。

[0075] 本实施例中，终端可以向生成安全策略配置的服务器(例如，TAC服务器)请求获取安全密钥，当该服务器接收到请求后，可以生成一个服务器安全密钥，且该服务器针对不同终端的请求所生成的服务器安全密钥各不相同。

[0076] 例如，该服务器接收到终端的请求后，可以按照预先定义的规格，例如，预先定义所述服务器安全密钥为8位，其中需同时包含字母和数字，并且字母区分大小写，不得出现其他符号，则服务器可以按照该规格随机生成服务器安全密钥，例如，生成的服务器安全密钥为1a2B3c4D。由于服务器安全密钥是由服务器随机生成的，因此，服务器为不同终端生成的服务器安全密钥各不相同。

[0077] 步骤S302：接收所述服务器返回的服务器安全密钥，并保存所述服务器安全密钥作为所述唯一的安全密钥。

[0078] 终端接收到服务器返回的服务器安全密钥后，可以保存该服务器安全密钥，例如，保存在本地配置中。由于服务器为不同终端生成的服务器安全密钥并不相同，因此，终端可以将接收到的服务器安全密钥作为唯一的安全密钥。

[0079] 步骤S303：根据所述安全密钥加密安全策略配置，生成本地安全策略配置文件并保存。

[0080] 终端根据所述安全密钥加密接收到的安全策略配置，生成本地安全策略配置文件并保存的过程可以参见现有技术，本申请对此不再详细赘述。

[0081] 图4包括：

[0082] 步骤S401：当访问内网时，获取所述保存的服务器安全密钥。

[0083] 由步骤S302可知，终端将服务器安全密钥进行了保存，则终端可以获取该服务器安全密钥。

[0084] 步骤S402：根据所述服务器安全密钥解析所述本地安全策略配置文件，以获取所述安全策略配置，并根据所述安全策略配置进行安全性检查。

[0085] 终端根据所述安全密钥解析本地安全策略配置文件，并根据解析得到的安全策略配置对自身进行安全性检查的过程可以参见现有技术，本申请对此不再详细赘述。

[0086] 本实施例处理本地安全策略配置的方法，通过向生成安全策略配置的服务器获取安全密钥，该服务器可以为不同终端生成不同的服务器安全密钥，使得终端获取一个唯一的安全密钥，并使用该唯一的安全密钥加密安全策略配置，生成本地安全策略配置文件并保存。由于不同终端的安全密钥各不相同，即使该终端上的本地安全策略配置文件被复制到了其它终端上，其它终端也无法使用自身的安全密钥解析该本地安全策略配置文件，从而避免了安全策略配置泄密，导致不安全的终端访问内网，有效地保证了内网的安全。

[0087] 在图3所描述的实施例中，当终端获取到服务器安全密钥后，可以将其保存。由于该服务器安全密钥保存在终端上，则有可能会被恶意获取到并篡改，仍存在本地安全策略泄密的风险。为了更有效地避免本地安全策略泄密，本申请中可以获取更为安全的唯一的安全密钥，如下的图5，示例了本申请处理本地安全策略配置中保存本地安全策略配置的方法的另一个实施例流程图，如下的图6，示例了本申请处理本地安全策略配置中解析本地安全策略配置的方法的另一个实施例流程图。其中，图5包括：

[0088] 步骤S501：向生成安全策略配置的服务器请求获取安全密钥，以使服务器生成服务器安全密钥。

[0089] 本步骤的详细描述可以参见步骤S301中的描述，在此不再详细赘述。

[0090] 步骤S502：接收所述服务器返回的服务器安全密钥，并保存所述服务器安全密钥。

[0091] 步骤S503：根据所述终端的硬件属性标识，生成终端安全密钥。

[0092] 本实施例中，终端根据自身的硬件属性标识，例如处理器标识，即CPU序列号，按照预设的生成终端安全密钥规则，例如，取硬件属性标识的前八位，生成终端安全密钥。举例来说，假设终端11的CPU序列号为BFEBFBFF000306C3，取该CPU序列号的前八位1a2B3c4D作为终端安全密钥。

[0093] 可以理解的是，上述仅仅为终端生成终端安全密钥的示例，在实际实施中，终端可以根据其它硬件属性标识，按照预先设置的规则，生成终端安全密钥。

[0094] 由于不同的终端具有不同的硬件属性标识，因此不同的终端所生成的终端安全密钥也各不相同。

[0095] 步骤S504：按照预设的组合规则，根据所述终端安全密钥与所述服务器安全密钥生成新的安全密钥，将所述新的安全秘钥作为唯一的安全密钥。

[0096] 当执行完步骤S501和步骤S502，终端可以按照预设的组合规则，根据所述终端安全密钥与所述服务器安全密钥生成一个新的安全密钥。例如，假设服务器安全密钥为1a2B3c4D，终端安全密钥为1a2B3c4D，预设的组合规则为，取终端安全密钥的前四位与服务器安全密钥的后四位进行组合，则生成的新的安全密钥为BFEB3c4D。

[0097] 可以理解的是，上述仅仅为终端生成新的安全密钥的示例，在实际实施中，终端生

成新的安全密钥的组合规则可以更复杂，本申请对此不做限制。

[0098] 通过上述描述可知，不同终端获取到的服务器安全密钥各不相同，而且不同终端生成的终端安全密钥也各不相同，则不同终端按照上述描述的过程所生成的新的安全密钥也各不相同，则终端可以将该新的安全密钥作为唯一的安全密钥。

[0099] 步骤S505：根据所述安全密钥加密安全策略配置，生成本地安全策略配置文件并保存。

[0100] 终端根据所述安全密钥加密接收到的安全策略配置，生成本地安全策略配置文件并保存的过程可以参见现有技术，本申请对此不再详细赘述。

[0101] 图6包括：

[0102] 步骤S601：当访问内网时，获取所述保存的服务器安全密钥。

[0103] 本步骤的详细描述可以参见上述步骤S401中的相关描述，在此不再详细赘述。

[0104] 步骤S602：根据所述终端的硬件属性标识，生成终端安全密钥。

[0105] 本步骤中，终端可以按照步骤S502中的描述，采取与步骤S502中相同的规则，按照相同的硬件属性标识，生成终端安全密钥。

[0106] 步骤S603：按照预设的组合规则，根据所述终端安全密钥与所述服务器安全密钥生成新的安全密钥。

[0107] 本步骤中，终端可以按照步骤S503中的描述，采取与步骤S503中相同的组合规则，将服务器安全密钥与终端安全密钥进行组合，生成新的安全密钥。

[0108] 由于该新的安全密钥是由终端安全密钥与服务器安全密钥组合生成，即使服务器安全密钥有可能会被恶意获取并篡改，但终端安全密钥是根据终端自身的硬件属性标识生成，攻击者很难确定终端安全密钥是根据哪个硬件属性标识生成，从而攻击者很难获取到终端安全密钥，从而很难获取到最终生成的唯一的安全密钥。

[0109] 步骤S604：根据所述新的安全密钥解析所述本地安全策略配置文件，以获取所述安全策略配置，并根据所述安全策略配置进行安全性检查。

[0110] 终端根据所述安全密钥解析本地安全策略配置文件，并根据解析得到的安全策略配置对自身进行安全性检查的过程可以参见现有技术，本申请对此不再详细赘述。

[0111] 本实施例处理本地安全策略配置的方法，通过使用获取到的服务器安全密钥与自身的终端安全密钥生成最终唯一的安全密钥，并使用该唯一的安全密钥加密安全策略配置，生成本地安全策略配置文件并保存。当解析该本地安全策略配置时，仍需获取保存的服务器安全密钥，并生成终端安全密钥，根据该两者最终生成新的安全密钥，使用该新的安全密钥才可以解析本地安全策略配置文件，获取到安全策略配置。即使服务器安全密钥可能被攻击者恶意获取到，攻击者也很难获取到终端安全密钥，从而很难获取到最终的唯一的安全密钥，从而有效地避免了安全策略配置泄密，导致不安全的终端访问内网，有效地保证了内网的安全。

[0112] 此外，本实施例中，服务器向不同终端返回的服务器安全密钥也可以相同，由于不同终端自身生成的终端安全密钥并不相同，即使服务器安全密钥相同，将服务器安全密钥与终端安全密钥进行组合后，所生成的新的安全密钥也会各不相同。

[0113] 与前述处理本地安全策略配置的方法的实施例相对应，本申请还提供了处理本地安全策略配置的装置的实施例。

[0114] 本申请处理本地安全策略配置的装置的实施例可以应用在终端上。装置实施例可以通过软件实现，也可以通过硬件或者软硬件结合的方式实现。以软件实现为例，作为一个逻辑意义上的装置，是通过其所在终端的处理器将非易失性存储器中对应的计算机程序指令读取到内存中运行形成的。从硬件层面而言，如图7所示，为本申请处理本地安全策略配置的装置所在终端的一种硬件结构图，除了图7所示的处理器71、内存72、网络接口73、以及非易失性存储器74之外，实施例中装置所在的终端通常根据该终端的实际功能，还可以包括其他硬件，对此不再赘述。

[0115] 请参考图8，示例了本申请处理本地安全策略配置的装置的一个实施例框图，所述装置可以包括：获取单元81、加密单元82、解析单元83。

[0116] 其中，所述获取单元81，可以用于获取唯一的安全密钥，所述唯一的安全密钥表示不同的终端对应的安全密钥各不相同；

[0117] 所述加密单元82，可以用于根据所述安全密钥加密安全策略配置，生成本地安全策略配置文件并保存；

[0118] 所述解析单元83，可以用于当访问内网时，根据所述安全密钥解析所述本地安全策略配置文件，以获取所述安全策略配置，并根据所述安全策略配置进行安全性检查。

[0119] 请参考图9，示例了本申请处理本地安全策略配置的装置的另一个实施例框图，该图9所示的装置在上述图8所示装置的基础上，所述获取单元81，可以包括：第一请求子单元811、第一接收子单元812。

[0120] 所述第一请求子单元811，可以用于向生成所述安全策略配置的服务器请求获取安全密钥，以使服务器生成服务器安全密钥，且服务器根据不同终端生成的服务器安全密钥各不相同；

[0121] 所述第一接收子单元812，可以用于接收所述服务器返回的服务器安全密钥，并保存所述服务器安全密钥作为所述唯一的安全密钥。

[0122] 所述解析单元83，可以包括：第一获取子单元831、第一解析子单元832。

[0123] 其中，所述第一获取子单元831，可以用于获取所述服务器安全密钥；

[0124] 所述第一解析子单元832，可以用于根据所述服务器安全密钥解析所述本地安全策略配置文件。

[0125] 请参考图10，示例了本申请处理本地安全策略配置的装置的另一个实施例框图，该图9所示的装置在上述图7所示装置的基础上，所述获取单元81，可以包括：第二请求子单元813、第二接收子单元814、第一生成子单元815、第一组合子单元816。

[0126] 其中，所述第二请求子单元813，可以用于向生成所述安全策略配置的服务器请求获取安全密钥，以使服务器生成服务器安全密钥；

[0127] 所述第二接收子单元814，可以用于接收所述服务器返回的服务器安全密钥；

[0128] 所述第一生成子单元815，可以用于根据所述终端的硬件属性标识，生成终端安全密钥；

[0129] 所述第一组合子单元816，可以用于按照预设的组合规则，根据所述终端安全密钥与所述服务器安全密钥生成新的安全密钥，将所述新的安全秘钥作为所述唯一的安全秘钥。

[0130] 所述解析单元83，可以包括：第二获取子单元833、第二生成子单元834、第二组合

子单元835、第二解析子单元836。

[0131] 其中，所述第二获取子单元833，可以用于获取所述服务器安全密钥；

[0132] 所述第二生成子单元834，可以用于根据所述终端的硬件属性标识，生成终端安全密钥；

[0133] 所述第二组合子单元835，可以用于按照预设的规则，根据所述终端安全密钥与所述服务器安全密钥生成新的安全密钥；

[0134] 所述第二解析子单元836，可以用于根据所述新的安全密钥，解析所述本地安全策略配置文件。

[0135] 上述装置中各个单元的功能和作用的实现过程具体详见上述方法中对应步骤的实现过程，在此不再赘述。

[0136] 对于装置实施例而言，由于其基本对应于方法实施例，所以相关之处参见方法实施例的部分说明即可。以上所描述的装置实施例仅仅是示意性的，其中所述作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部模块来实现本申请方案的目的。本领域普通技术人员在不付出创造性劳动的情况下，即可以理解并实施。

[0137] 以上所述仅为本申请的较佳实施例而已，并不用以限制本申请，凡在本申请的精神和原则之内，所做的任何修改、等同替换、改进等，均应包含在本申请保护的范围之内。

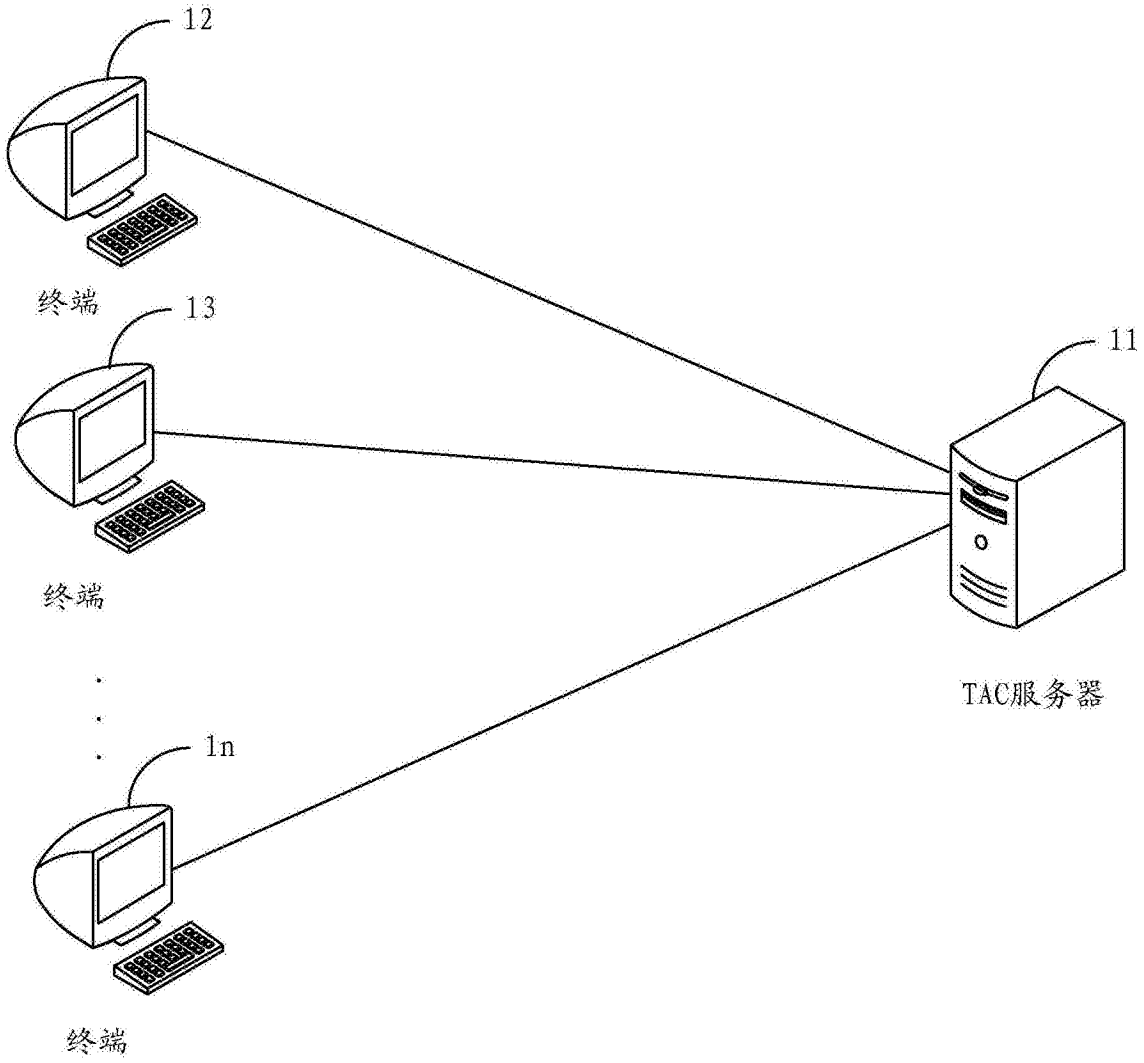


图1

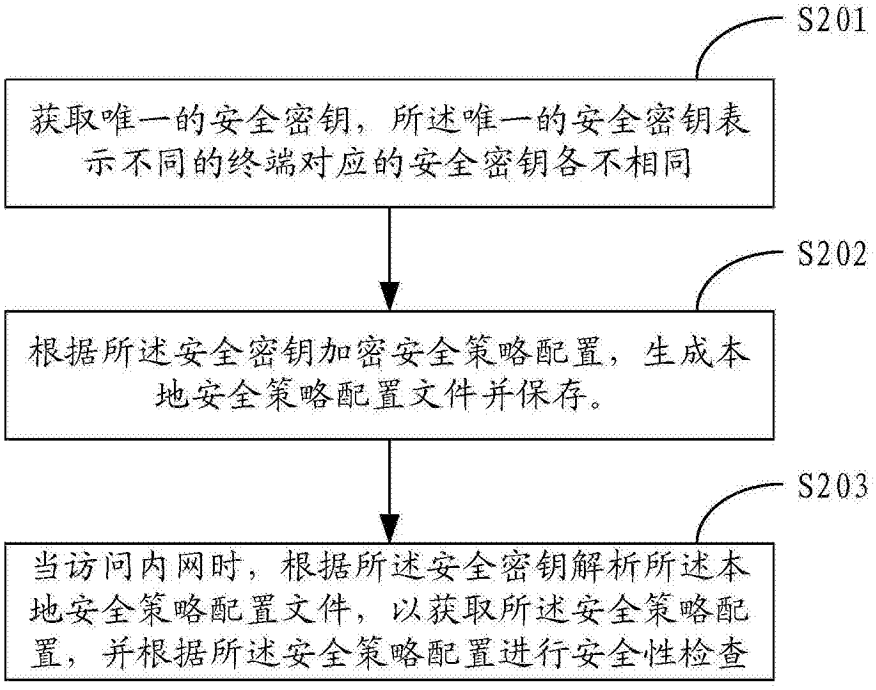

S201
获取唯一的安全密钥，所述唯一的安全密钥表示不同的终端对应的安全密钥各不相同
S202
根据所述安全密钥加密安全策略配置，生成本地安全策略配置文件并保存。
S203
当访问内网时，根据所述安全密钥解析所述本地安全策略配置文件，以获取所述安全策略配置，并根据所述安全策略配置进行安全性检查

图2

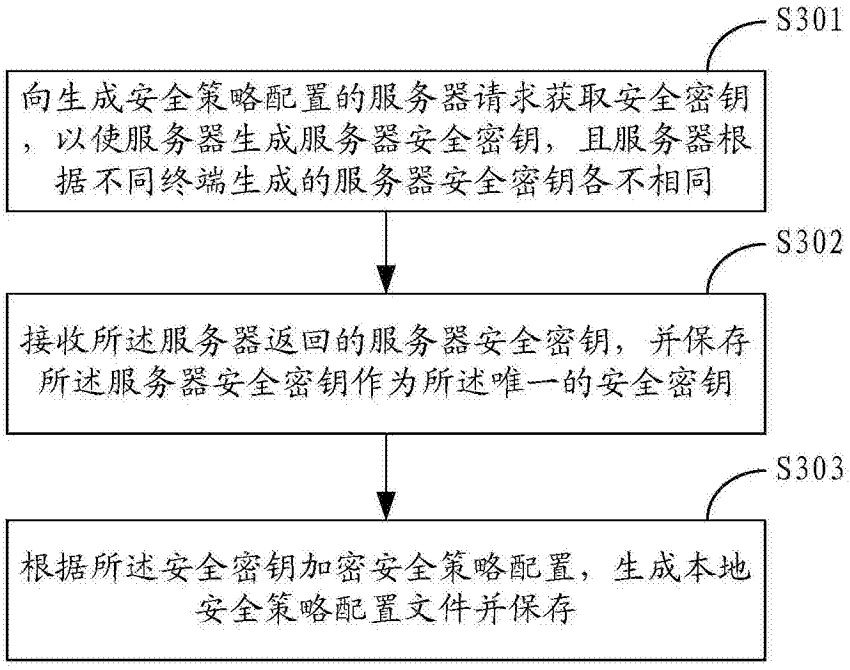

S301
向生成安全策略配置的服务器请求获取安全密钥，以使服务器生成服务器安全密钥，且服务器根据不同终端生成的服务器安全密钥各不相同
S302
接收所述服务器返回的服务器安全密钥，并保存所述服务器安全密钥作为所述唯一的安全密钥
S303
根据所述安全密钥加密安全策略配置，生成本地安全策略配置文件并保存

图3

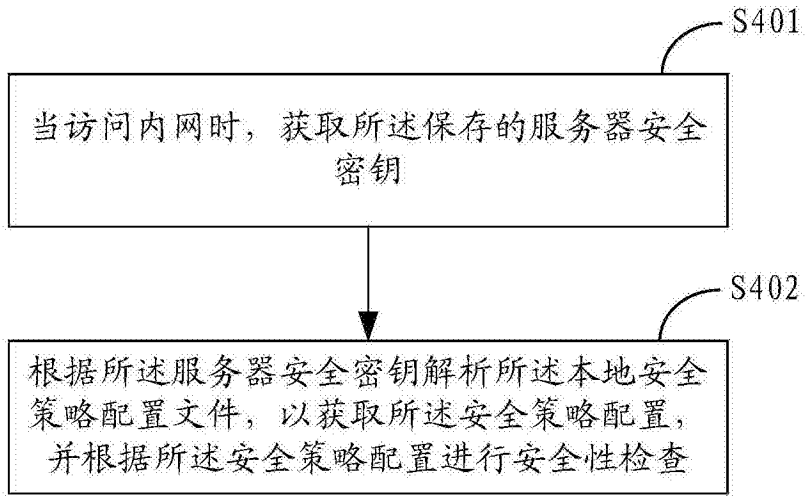

S401
当访问内网时，获取所述保存的服务器安全密钥
S402
根据所述服务器安全密钥解析所述本地安全策略配置文件，以获取所述安全策略配置，并根据所述安全策略配置进行安全性检查

图4

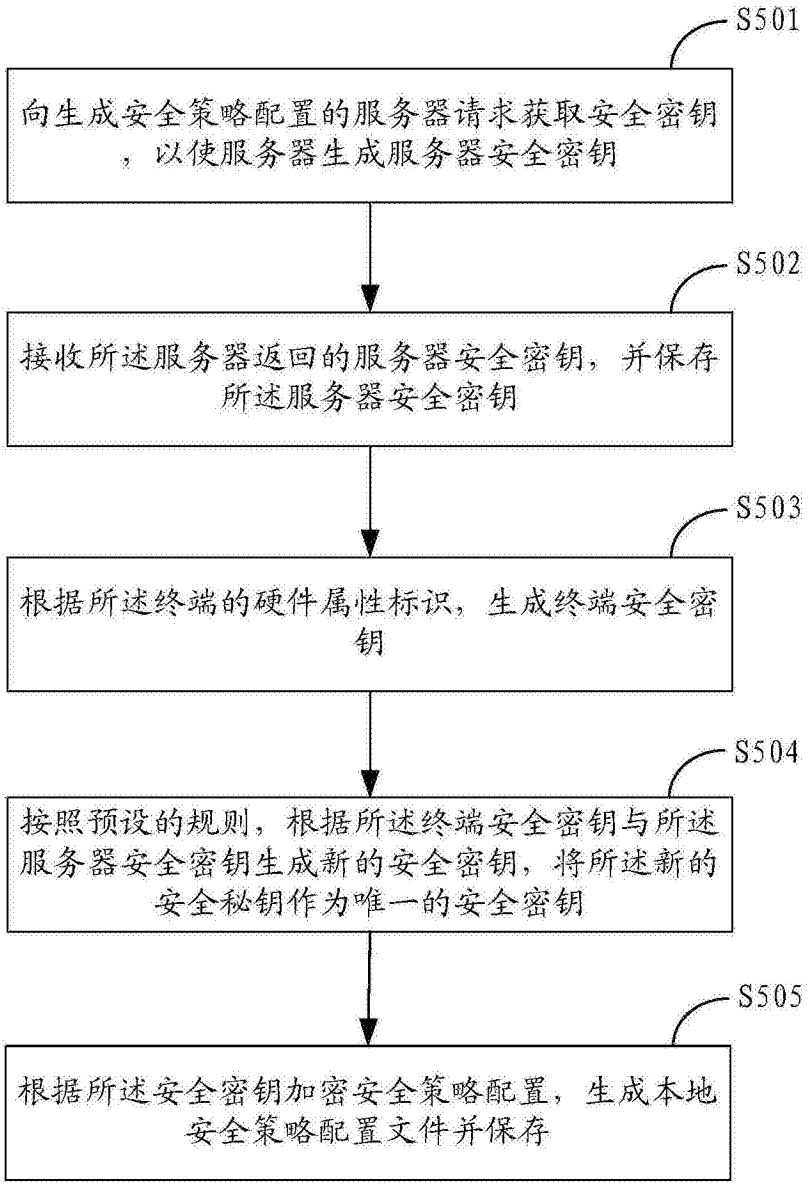

S501
向生成安全策略配置的服务器请求获取安全密钥，以使服务器生成服务器安全密钥
S502
接收所述服务器返回的服务器安全密钥，并保存所述服务器安全密钥
S503
根据所述终端的硬件属性标识，生成终端安全密钥
S504
按照预设的规则，根据所述终端安全密钥与所述服务器安全密钥生成新的安全密钥，将所述新的安全秘钥作为唯一的安全密钥
S505
根据所述安全密钥加密安全策略配置，生成本地安全策略配置文件并保存

图5

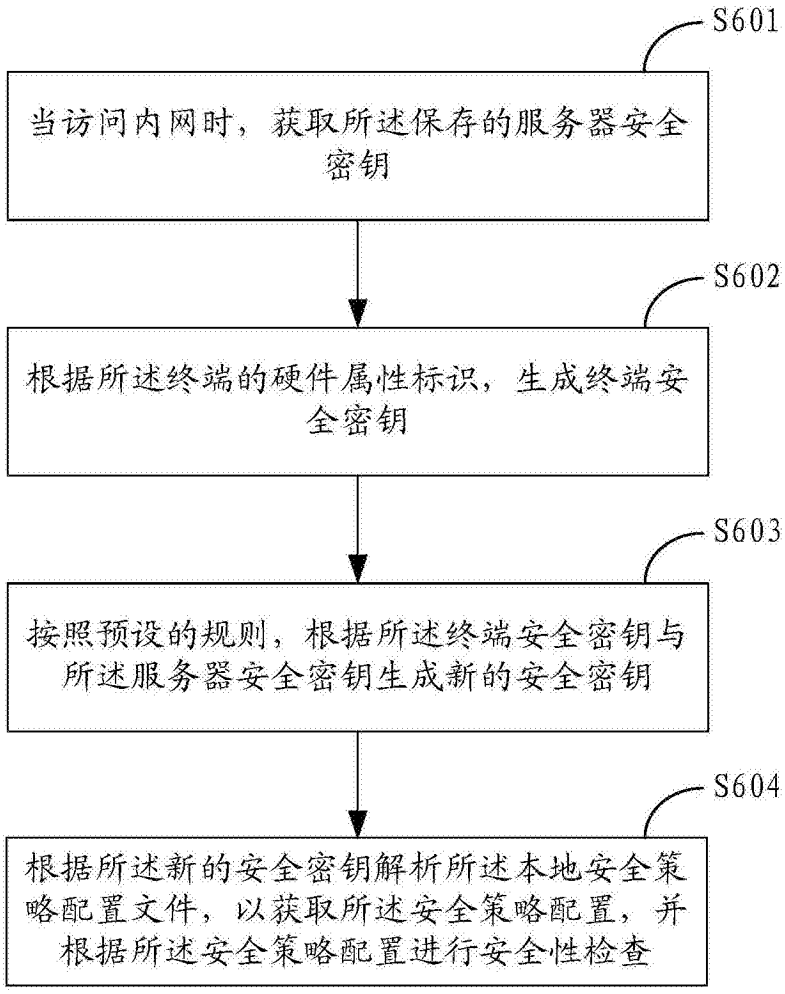

S601
当访问内网时，获取所述保存的服务器安全密钥
S602
根据所述终端的硬件属性标识，生成终端安全密钥
S603
按照预设的规则，根据所述终端安全密钥与所述服务器安全密钥生成新的安全密钥
S604
根据所述新的安全密钥解析所述本地安全策略配置文件，以获取所述安全策略配置，并根据所述安全策略配置进行安全性检查

图6

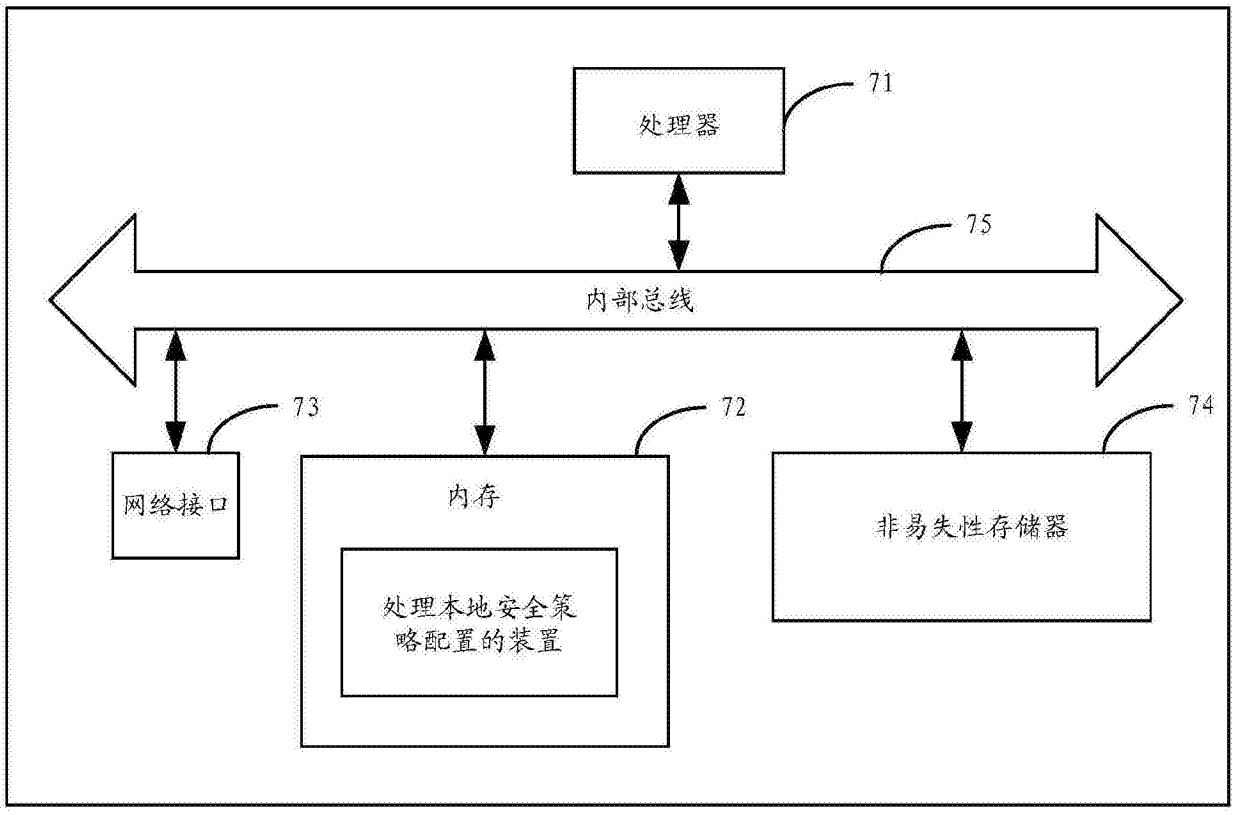

处理器
71
75
内部总线
73
72
74
网络接口
内存
处理本地安全策略配置的装置
非易失性存储器

图7

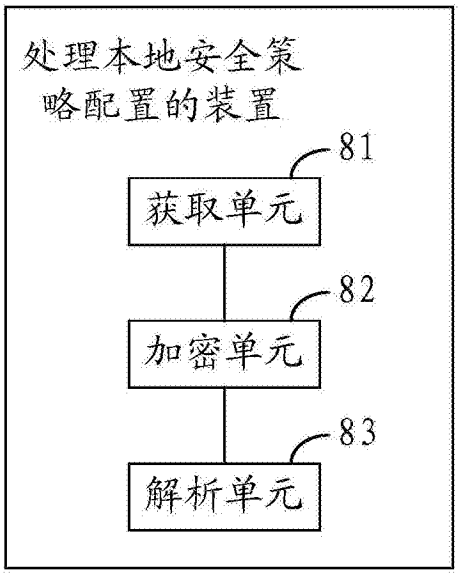

处理本地安全策略配置的装置
81
获取单元
82
加密单元
83
解析单元

图8

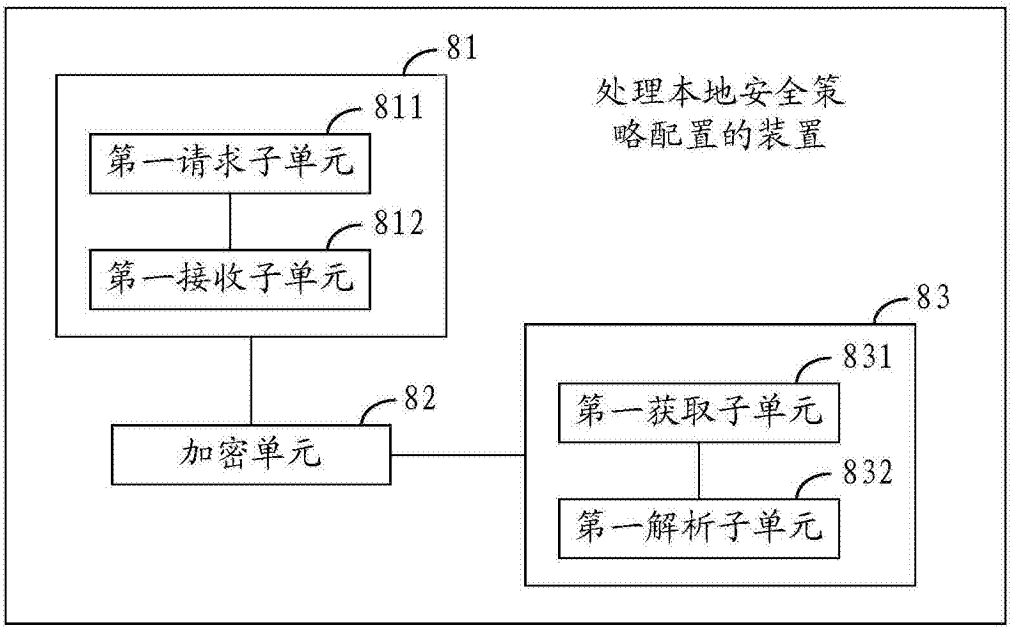

81
处理本地安全策略配置的装置
811
第一请求子单元
812
第一接收子单元
82
加密单元
83
831
第一获取子单元
832
第一解析子单元

图9

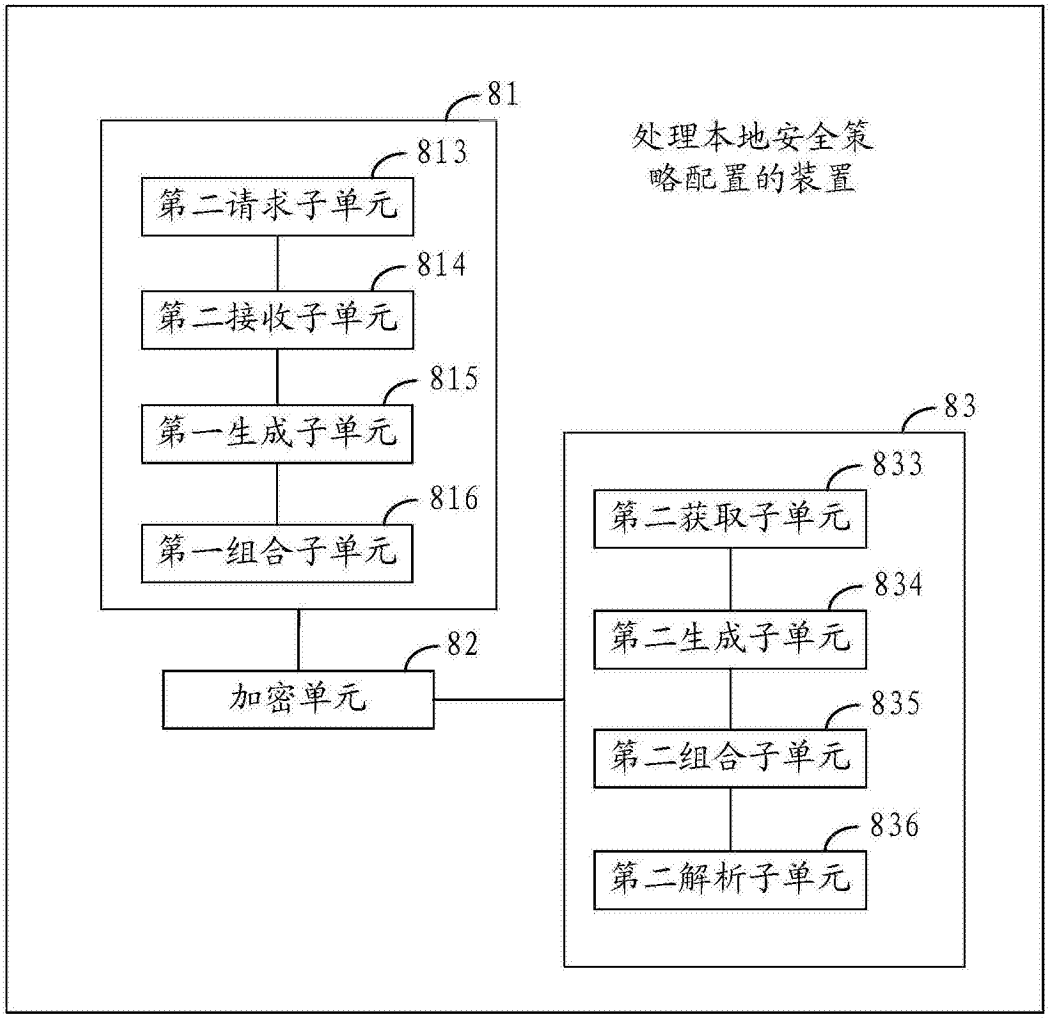

处理本地安全策略配置的装置
81
813
第二请求子单元
814
第二接收子单元
815
第一生成子单元
816
第一组合子单元
82
加密单元
83
833
第二获取子单元
834
第二生成子单元
835
第二组合子单元
836
第二解析子单元

图10