(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 114268507 A
(43)申请公布日 2022.04.01

(21)申请号 202111645208.5

(22)申请日 2021.12.30

(71)申请人 天翼物联科技有限公司
地址 210000 江苏省南京市秦淮区中山南路501号1101室

(72)发明人 陈天 黄勇军 陈楠 吴斯栋 王雪艳 林睦楷

(74)专利代理机构 深圳市精英专利事务所 44242
代理人 武志峰

(51)Int.Cl.
H04L 9/40(2022.01)

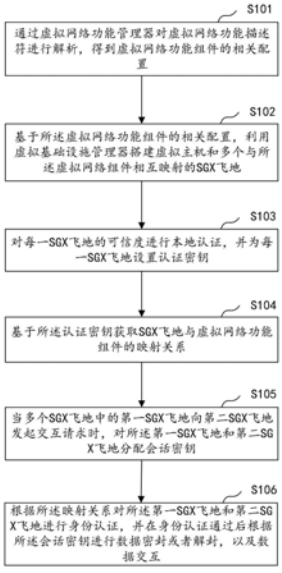
权利要求书2页 说明书7页 附图4页

(54)发明名称

一种基于SGX的网络云安全优化方法、系统及相关介质

(57)摘要

本发明公开了一种基于SGX的网络云安全优化方法、装置及相关介质，该方法包括：对虚拟网络功能描述符进行解析，得到虚拟网络功能组件的相关配置；搭建虚拟主机和多个与所述虚拟网络组件相互映射的SGX飞地；对每一SGX飞地的可信度进行本地认证，并为每一SGX飞地设置认证密钥；基于认证密钥获取SGX飞地与虚拟网络功能组件的映射关系；当多个SGX飞地中的第一SGX飞地向第二SGX飞地发起交互请求时，对第一SGX飞地和第二SGX飞地分配会话密钥；根据映射关系对所述第一SGX飞地和第二SGX飞地进行身份认证，并在身份认证通过后根据会话密钥进行数据交互。本发明可解决飞地单点故障和资源受限的问题，实现对大型网元的支持，以及对SGX进行优化以提高可靠性。



CN 114268507 A

1.一种基于SGX的网络云安全优化方法,其特征在于,包括:

通过虚拟网络功能管理器对虚拟网络功能描述符进行解析,得到虚拟网络功能组件的相关配置;

基于所述虚拟网络功能组件的相关配置,利用虚拟基础设施管理器搭建虚拟主机和多个与所述虚拟网络组件相互映射的SGX飞地;

对每一SGX飞地的可信度进行本地认证,并为每一SGX飞地设置认证密钥;

基于所述认证密钥获取SGX飞地与虚拟网络功能组件的映射关系;

当多个SGX飞地中的第一SGX飞地向第二SGX飞地发起交互请求时,对所述第一SGX飞地和第二SGX飞地分配会话密钥;

根据所述映射关系对所述第一SGX飞地和第二SGX飞地进行身份认证,并在身份认证通过后根据所述会话密钥进行数据密封或者解封,以及数据交互。

2.根据权利要求1所述的基于SGX的网络云安全优化方法,其特征在于,所述通过虚拟网络功能管理器对虚拟网络功能描述符进行解析,得到虚拟网络功能组件的相关配置,包括:

通过虚拟网络功能管理器对虚拟网络功能描述符进行解析,明确普通虚拟网络功能组件的相关配置和受保护虚拟网络功能组件的相关配置。

3.根据权利要求2所述的基于SGX的网络云安全优化方法,其特征在于,所述基于所述虚拟网络功能组件的相关配置,利用虚拟基础设施管理器搭建虚拟主机和多个与所述虚拟网络组件相互映射的SGX飞地,包括:

根据所述受保护虚拟网络功能组件的数量,利用虚拟基础设施管理器搭建数量相同的SGX飞地,并使所述受保护虚拟网络功能组件与所述SGX飞地相互之间一一映射。

4.根据权利要求3所述的基于SGX的网络云安全优化方法,其特征在于,所述基于所述认证密钥获取SGX飞地与虚拟网络功能组件的映射关系,包括:

基于所述认证密钥获取SGX飞地与受保护虚拟网络功能组件的映射关系。

5.根据权利要求1所述的基于SGX的网络云安全优化方法,其特征在于,所述根据所述映射关系对所述第一SGX飞地和第二SGX飞地进行身份认证,包括:

基于哈希算法对对所述第一SGX飞地和第二SGX飞地进行身份认证。

6.根据权利要求5所述的基于SGX的网络云安全优化方法,其特征在于,所述基于哈希算法对对所述第一SGX飞地和第二SGX飞地进行身份认证,包括:

分别对所述第一SGX飞地和第二SGX飞地进行哈希计算,得到所述第一SGX飞地的第一身份认证值和所述第二SGX飞地的第二身份认证值;

基于所述映射关系,分别获取所述第一SGX飞地和第二SGX飞地各自对应的第一虚拟网络功能组件和第二虚拟网络功能组件;

分别对所述第一虚拟网络功能组件和第二虚拟网络功能组件进行哈希计算,得到所述第一虚拟网络功能组件的第一映射身份认证值和所述第二虚拟网络功能组件的第二映射身份认证值。

7.根据权利要求6所述的基于SGX的网络云安全优化方法,其特征在于,所述基于哈希算法对对所述第一SGX飞地和第二SGX飞地进行身份认证,还包括:

当所述第一身份认证值和第一映射身份认证值相等且所述第二身份认证值和第二映

射身份认证值相等时,则判定身份认证通过;

当所述第一身份认证值和第一映射身份认证值不相等和/或所述第二身份认证值和第二映射身份认证值不相等时,则判定身份认证未通过;

将所述第一SGX飞地和第二SGX飞地各自对应的身份认证结果反馈至对方。

8.一种基于SGX的网络云安全优化装置,其特征在于,包括:

解析单元,用于通过虚拟网络功能管理器对虚拟网络功能描述符进行解析,得到虚拟网络功能组件的相关配置;

搭建单元,用于基于所述虚拟网络功能组件的相关配置,利用虚拟基础设施管理器搭建虚拟主机和多个与所述虚拟网络组件相互映射的SGX飞地;

认证密钥设置单元,用于对每一SGX飞地的可信度进行本地认证,并为每一SGX飞地设置认证密钥;

第一获取单元,用于基于所述认证密钥获取SGX飞地与虚拟网络功能组件的映射关系;

会话密钥分配单元,用于当多个SGX飞地中的第一SGX飞地向第二SGX飞地发起交互请求时,对所述第一SGX飞地和第二SGX飞地分配会话密钥;

身份认证单元,用于根据所述映射关系对所述第一SGX飞地和第二SGX飞地进行身份认证,并在身份认证通过后根据所述会话密钥进行数据密封或者解封,以及数据交互。

9.一种计算机设备,其特征在于,包括存储器、处理器及存储在所述存储器上并可在所述处理器上运行的计算机程序,所述处理器执行所述计算机程序时实现如权利要求1至7任一项所述的基于SGX的网络云安全优化方法。

10.一种计算机可读存储介质,其特征在于,所述计算机可读存储介质上存储有计算机程序,所述计算机程序被处理器执行时实现如权利要求1至7任一项所述的基于SGX的网络云安全优化方法。

一种基于SGX的网络云安全优化方法、系统及相关介质

技术领域

[0001] 本发明涉及云网融合技术领域，特别涉及一种基于SGX的网络云安全优化方法、系统及相关介质。

背景技术

[0002] SGX(Software Guard Extensions)是一种CPU架构扩展技术，其采用一套新的指令集和内存访问机制，在主机硬件之上部署完全独立于主机OS、安全可信的执行环境(SGX enclave，即SGX飞地)，支持抵御OS特权域攻击。SGX的特性天然适用于云计算场景，支持在虚拟化和资源共享的环境，提供独立于操作系统和虚拟化资源的硬件加密防护的安全区，用以最小化受攻击面，增强数据保护。

[0003] 在网络云化承载的过程中，虚拟化、容器等虚拟化层技术，增加了系统暴露面和受攻击面，同样带来了更多的安全问题。现有的网络云安全方案，一般实现主机操作系统层之上的安全防护，不能抵御来自主机操作系统特权域的安全威胁，需要深层次安全保障。

[0004] 目前，基于SGX的网络云安全方案仍处于探索阶段，一般仅简单的将VNF网元当作应用处理，分为可受保护的SGX部分和其他部分(如图3所示)。但云化网元的架构与IT应用不同，一般由接口组件、业务组件、数据组件、管理运维组件构成，且对云化的安全性、性能、可靠性等存在更高的要求。现有方案存在单点故障、侧信道攻击、仅适用于小型网元等潜在问题。

发明内容

[0005] 本发明实施例提供了一种基于SGX的网络云安全优化方法、装置、计算机设备及存储介质，旨在解决飞地单点故障和资源受限的问题，实现对大型网元的支持，以及对SGX进行优化以提高可靠性。

[0006] 第一方面，本发明实施例提供了一种基于SGX的网络云安全优化方法，包括：

[0007] 通过虚拟网络功能管理器对虚拟网络功能描述符进行解析，得到虚拟网络功能组件的相关配置；

[0008] 基于所述虚拟网络功能组件的相关配置，利用虚拟基础设施管理器搭建虚拟主机和多个与所述虚拟网络组件相互映射的SGX飞地；

[0009] 对每一SGX飞地的可信度进行本地认证，并为每一SGX飞地设置认证密钥；

[0010] 基于所述认证密钥获取SGX飞地与虚拟网络功能组件的映射关系；

[0011] 当多个SGX飞地中的第一SGX飞地向第二SGX飞地发起交互请求时，对所述第一SGX飞地和第二SGX飞地分配会话密钥；

[0012] 根据所述映射关系对所述第一SGX飞地和第二SGX飞地进行身份认证，并在身份认证通过后根据所述会话密钥进行数据密封或者解封，以及数据交互。

[0013] 第二方面，本发明实施例提供了一种基于SGX的网络云安全优化装置，包括：

[0014] 解析单元，用于通过虚拟网络功能管理器对虚拟网络功能描述符进行解析，得到

虚拟网络功能组件的相关配置；

[0015] 搭建单元，用于基于所述虚拟网络功能组件的相关配置，利用虚拟基础设施管理器搭建虚拟主机和多个与所述虚拟网络组件相互映射的SGX飞地；

[0016] 认证密钥设置单元，用于对每一SGX飞地的可信度进行本地认证，并为每一SGX飞地设置认证密钥；

[0017] 第一获取单元，用于基于所述认证密钥获取SGX飞地与虚拟网络功能组件的映射关系；

[0018] 会话密钥分配单元，用于当多个SGX飞地中的第一SGX飞地向第二SGX飞地发起交互请求时，对所述第一SGX飞地和第二SGX飞地分配会话密钥；

[0019] 身份认证单元，用于根据所述映射关系对所述第一SGX飞地和第二SGX飞地进行身份认证，并在身份认证通过后根据所述会话密钥进行数据密封或者解封，以及数据交互。

[0020] 第三方面，本发明实施例提供了一种计算机设备，包括存储器、处理器及存储在所述存储器上并可在所述处理器上运行的计算机程序，所述处理器执行所述计算机程序时实现如第一方面所述的基于SGX的网络云安全优化方法。

[0021] 第四方面，本发明实施例提供了一种计算机可读存储介质，所述计算机可读存储介质上存储有计算机程序，所述计算机程序被处理器执行时实现如第一方面所述的基于SGX的网络云安全优化方法。

[0022] 本发明实施例提供了一种基于SGX的网络云安全优化方法、装置、计算机设备及存储介质，该方法包括：通过虚拟网络功能管理器对虚拟网络功能描述符进行解析，得到虚拟网络功能组件的相关配置；基于所述虚拟网络功能组件的相关配置，利用虚拟基础设施管理器搭建虚拟主机和多个与所述虚拟网络组件相互映射的SGX飞地；对每一SGX飞地的可信度进行本地认证，并为每一SGX飞地设置认证密钥；基于所述认证密钥获取SGX飞地与虚拟网络功能组件的映射关系；当多个SGX飞地中的第一SGX飞地向第二SGX飞地发起交互请求时，对所述第一SGX飞地和第二SGX飞地分配会话密钥；根据所述映射关系对所述第一SGX飞地和第二SGX飞地进行身份认证，并在身份认证通过后根据所述会话密钥进行数据密封或者解封，以及数据交互。本发明实施例通过将多飞地与多虚拟网络功能组件一对一部署防护，将防护颗粒度细化到虚拟网络功能组件层面，将虚拟网络功能组件按需放入单独的SGX飞地安全空间，形成对虚拟网络功能的分布式防护体系，如此可解决飞地单点故障和资源受限的问题，实现对大型网元的支持；同时通过本地认证和身份认证，对存在交互需求的飞地新增进行双向的身份认证，并结合后续的数据密封/解封，实现二次认证，从而实现对SGX技术的优化，进一步提高可靠性。

附图说明

[0023] 为了更清楚地说明本发明实施例技术方案，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。

[0024] 图1为本发明实施例提供的一种基于SGX的网络云安全优化方法的流程示意图；

[0025] 图2为本发明实施例提供的一种基于SGX的网络云安全优化方法的子流程示意图；

[0026] 图3为现有方案对比示意图；

[0027] 图4为本发明实施例提供的一种基于SGX的网络云安全优化方法的网络示意图；

[0028] 图5为本发明实施例提供的一种基于SGX的网络云安全优化方法的示例示意图；

[0029] 图6为本发明实施例提供的一种基于SGX的网络云安全优化装置的示意性框图；

[0030] 图7为本发明实施例提供的一种基于SGX的网络云安全优化装置的子示意性框图。

具体实施方式

[0031] 下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

[0032] 应当理解，当在本说明书和所附权利要求书中使用时，术语“包括”和“包含”指示所描述特征、整体、步骤、操作、元素和/或组件的存在，但并不排除一个或多个其它特征、整体、步骤、操作、元素、组件和/或其集合的存在或添加。

[0033] 还应当理解，在此本发明说明书中所使用的术语仅仅是出于描述特定实施例的目的而并不意在限制本发明。如在本发明说明书和所附权利要求书中所使用的那样，除非上下文清楚地指明其它情况，否则单数形式的“一”、“一个”及“该”意在包括复数形式。

[0034] 还应当进一步理解，在本发明说明书和所附权利要求书中使用的术语“和/或”是指相关联列出的项中的一个或多个的任何组合以及所有可能组合，并且包括这些组合。

[0035] 下面请参见图1，图1为本发明实施例提供的一种基于SGX的网络云安全优化方法的流程示意图，具体包括：步骤S101～S106。

[0036] S101、通过虚拟网络功能管理器对虚拟网络功能描述符进行解析，得到虚拟网络功能组件的相关配置；

[0037] S102、基于所述虚拟网络功能组件的相关配置，利用虚拟基础设施管理器搭建虚拟主机和多个与所述虚拟网络组件相互映射的SGX飞地；

[0038] S103、对每一SGX飞地的可信度进行本地认证，并为每一SGX飞地设置认证密钥；

[0039] S104、基于所述认证密钥获取SGX飞地与虚拟网络功能组件的映射关系；

[0040] S105、当多个SGX飞地中的第一SGX飞地向第二SGX飞地发起交互请求时，对所述第一SGX飞地和第二SGX飞地分配会话密钥；

[0041] S106、根据所述映射关系对所述第一SGX飞地和第二SGX飞地进行身份认证，并在身份认证通过后根据所述会话密钥进行数据密封或者解封，以及数据交互。

[0042] 本实施例中，首先利用虚拟网络功能管理器(VNF)对虚拟网络功能描述符(VNFD)进行解析，以获取虚拟网络功能(VNF)中的各虚拟网络功能组件(VNFC)对应的配置，再利用虚拟基础设施管理器(VIF)搭建起相应的SGX飞地以及虚拟主机。对搭建的所有SGX飞地进行本地认证，以及将SGX飞地与VNFC一一对应。当SGX飞地之间需要进行交互时，对交互的SGX飞地进行二次认证，即身份认证。并只有在交互的双方均通过身份认证时，才会进行数据密封或者解封，使交互的SGX飞地可以进行数据交互。

[0043] 本发明通过将多飞地与多虚拟网络功能组件一对一部署防护，将防护颗粒度细化到虚拟网络功能组件层面，将虚拟网络功能组件按需放入单独的SGX飞地安全空间，形成对虚拟网络功能的分布式防护体系，如此可解决飞地单点故障和资源受限的问题，实现对大

型网元的支持;同时通过本地认证和身份认证,对存在交互需求的飞地新增进行双向的身份认证,并结合后续的数据密封/解封,实现二次认证,从而实现对SGX技术的优化,进一步提高可靠性。

[0044] 具体来说,VNF(即所述虚拟网络功能)网元由多个VNFC(即所述虚拟网络功能组件)构成,具体包括接口组件、业务组件、数据组件、管理组件等。针对单个SGX飞地资源有限的特点,本实施例提出了多飞地与多VNFC一对一部署防护的方法,将防护颗粒度细化到VNFC层面,将VNFC按需放入单独的SGX飞地安全空间,形成对VNF的分布式防护体系,解决飞地单点故障和资源受限的问题,实现对大型网元的支持。

[0045] 另外,在SGX现有方法中,同一应用的多个SGX飞地进行本地认证后,可基于事先协商的同一个会话密钥或者基于密钥管理模块临时分配的会话密钥,透明地对其他飞地的数据进行密封和解封,但存在潜在的侧信道攻击和数据泄露风险。本实施例则提出了本地认证飞地之间数据交互的二次认证方法,在通过本地认证之后,以及在数据交互之前,对存在交互需求的飞地新增双向的身份认证,并结合后续的数据密封/解封,实现二次认证,从而实现对SGX技术的优化,进一步提高了可靠性。

[0046] 在一实施例中,所述步骤S101包括:

[0047] 通过虚拟网络功能管理器对虚拟网络功能描述符进行解析,明确普通虚拟网络功能组件的相关配置和受保护虚拟网络功能组件的相关配置。

[0048] 本实施例中,所述虚拟网络功能组件具体包括普通虚拟网络功能组件和受保护虚拟网络功能组件,通过对虚拟网络功能描述符进行解析,可以获得二者各自对应的相关配置,以便于在后续步骤使受保护虚拟网络功能组件与SGX飞地之间进行映射。

[0049] 在一实施例中,所述步骤S102包括:

[0050] 根据所述受保护虚拟网络功能组件的数量,利用虚拟基础设施管理器搭建数量相同的SGX飞地,并使所述受保护虚拟网络功能组件与所述SGX飞地相互之间一一映射。

[0051] 本实施例中,结合图4,根据解析得到的受保护VNFC的相关配置,将所述VNFC ID与所述SGX飞地相互之间一一映射,从而可以得到一SGX飞地与VNFC ID之间的映射表。

[0052] 在一实施例中,所述步骤S104包括:

[0053] 基于所述认证密钥获取SGX飞地与受保护虚拟网络功能组件的映射关系。

[0054] 本实施例中,对于已经完成身份认证的SGX飞地,根据SGX飞地配置的认证密钥可以在映射表中找到与该SGX飞地映射的VNFC ID,从而在后续步骤对SGX飞地和映射的VNFC ID进行哈希计算。

[0055] 在一实施例中,所述步骤S106包括:

[0056] 基于哈希算法对对所述第一SGX飞地和第二SGX飞地进行身份认证。

[0057] 本实施例中,对于SGX飞地之间的双向身份认证,采用基于哈希算法的VNFC ID认证,进一步保证身份认证的可靠性。

[0058] 具体的,在一实施例中,如图2所示,所述基于哈希算法对对所述第一SGX飞地和第二SGX飞地进行身份认证,包括:步骤S201～S203。

[0059] S201、分别对所述第一SGX飞地和第二SGX飞地进行哈希计算,得到所述第一SGX飞地的第一身份认证值和所述第二SGX飞地的第二身份认证值;

[0060] S202、基于所述映射关系,分别获取所述第一SGX飞地和第二SGX飞地各自对应的

第一虚拟网络功能组件和第二虚拟网络功能组件；

[0061] S203、分别对所述第一虚拟网络功能组件和第二虚拟网络功能组件进行哈希计算，得到所述第一虚拟网络功能组件的第一映射身份认证值和所述第二虚拟网络功能组件的第二映射身份认证值。

[0062] 本实施例中，通过哈希计算得到所述第一SGX飞地和第二SGX飞地各自对应的第一身份认证值和第二身份认证值，同时基于SGX飞地和虚拟网络功能组件之间的映射关系，对所述第一SGX飞地和第二SGX飞地各自对应的第一虚拟网络功能组件和第二虚拟网络功能组件进行哈希计算，得到二者各自对应的第一映射身份认证值和第二映射身份认证值。

[0063] 进一步的，在一实施例中，所述基于哈希算法对对所述第一SGX飞地和第二SGX飞地进行身份认证，还包括：

[0064] 当所述第一身份认证值和第一映射身份认证值相等且所述第二身份认证值和第二映射身份认证值相等时，则判定身份认证通过；

[0065] 当所述第一身份认证值和第一映射身份认证值不相等和/或所述第二身份认证值和第二映射身份认证值不相等时，则判定身份认证未通过；

[0066] 将所述第一SGX飞地和第二SGX飞地各自对应的身份认证结果反馈至对方。

[0067] 本实施例中，对由哈希计算得到的第一身份认证值和第一映射身份认证值进行比较，如果二者相等，则判定认证通过，如果二者不相等，则判认证不通过。同样的，对第二身份认证值和第二映射身份认证值进行比较，如果二者相等，则判定认证通过。同时，将第一SGX飞地和第二SGX飞地各自的身份认证结果互相发送至对方。

[0068] 在一具体实施例中，如图5所示，其为NFV网络云体系框架，包括基础设施层、网络功能层、运营支撑层等三大层次，用于实现基于虚拟化的网元云化部署和运营管理。与现有技术相比，本实施例在NFV网络云系统中新增了SGX功能模块，用于提供SGX解决方案能力，具体介绍如下所示：

[0069] (1)支持SGX的服务器：支持拉起SGX飞地安全空间。

[0070] (2)VIM(虚拟基础设施管理器)新增SGX资源管理模块：支持对服务器中SGX飞地的全生命周期管理。

[0071] (3)VNFM(虚拟网络功能管理器)新增SGX管理模块：提供SGX认证和密钥管理等功能，具体如前面专利方案中所述。

[0072] (4)VNF(虚拟网络功能)新增基于SGX飞地部署的VNFC(虚拟网络功能组件)：本案例中将数据VNFC和运维VNFC部署在encalve(飞地)中，实现对其中用户和运维信息等关键数据的深度安全防护。

[0073] (5)OSS/BSS业务运营管理中新增SGX业务管理模块：支持接收并下达SGX相关业务需求，并通过NFVO维护的NSD实现需求映射。

[0074] 图6为本发明实施例提供的一种基于SGX的网络云安全优化装置600的示意性框图，该装置600包括：

[0075] 解析单元601，用于通过虚拟网络功能管理器对虚拟网络功能描述符进行解析，得到虚拟网络功能组件的相关配置；

[0076] 搭建单元602，用于基于所述虚拟网络功能组件的相关配置，利用虚拟基础设施管理器搭建虚拟主机和多个与所述虚拟网络组件相互映射的SGX飞地；

[0077] 认证密钥设置单元603,用于对每一SGX飞地的可信度进行本地认证,并为每一SGX飞地设置认证密钥;

[0078] 第一获取单元604,用于基于所述认证密钥获取SGX飞地与虚拟网络功能组件的映射关系;

[0079] 会话密钥分配单元605,用于当多个SGX飞地中的第一SGX飞地向第二SGX飞地发起交互请求时,对所述第一SGX飞地和第二SGX飞地分配会话密钥;

[0080] 身份认证单元606,用于根据所述映射关系对所述第一SGX飞地和第二SGX飞地进行身份认证,并在身份认证通过后根据所述会话密钥进行数据密封或者解封,以及数据交互。

[0081] 在一实施例中,所述解析单元601包括:

[0082] 组件明确单元,用于通过虚拟网络功能管理器对虚拟网络功能描述符进行解析,明确普通虚拟网络功能组件的相关配置和受保护虚拟网络功能组件的相关配置。

[0083] 在一实施例中,所述搭建单元602包括:

[0084] 映射单元,用于根据所述受保护虚拟网络功能组件的数量,利用虚拟基础设施管理器搭建数量相同的SGX飞地,并使所述受保护虚拟网络功能组件与所述SGX飞地相互之间一一映射。

[0085] 在一实施例中,所述第一获取单元604包括:

[0086] 第二获取单元,用于基于所述认证密钥获取SGX飞地与受保护虚拟网络功能组件的映射关系。

[0087] 在一实施例中,所述身份认证单元606包括:

[0088] 哈希计算单元,用于基于哈希算法对对所述第一SGX飞地和第二SGX飞地进行身份认证。

[0089] 在一实施例中,如图7所示,所述哈希计算单元包括:

[0090] 第一计算单元701,用于分别对所述第一SGX飞地和第二SGX飞地进行哈希计算,得到所述第一SGX飞地的第一身份认证值和所述第二SGX飞地的第二身份认证值;

[0091] 组件获取单元702,用于基于所述映射关系,分别获取所述第一SGX飞地和第二SGX飞地各自对应的第一虚拟网络功能组件和第二虚拟网络功能组件;

[0092] 第二计算单元703,用于分别对所述第一虚拟网络功能组件和第二虚拟网络功能组件进行哈希计算,得到所述第一虚拟网络功能组件的第一映射身份认证值和所述第二虚拟网络功能组件的第二映射身份认证值。

[0093] 在一实施例中,所述哈希计算单元还包括:

[0094] 第一判定单元,用于当所述第一身份认证值和第一映射身份认证值相等且所述第二身份认证值和第二映射身份认证值相等时,则判定身份认证通过;

[0095] 第二判定单元,用于当所述第一身份认证值和第一映射身份认证值不相等和/或所述第二身份认证值和第二映射身份认证值不相等时,则判定身份认证未通过;

[0096] 结果反馈单元,用于将所述第一SGX飞地和第二SGX飞地各自对应的身份认证结果反馈至对方。

[0097] 由于装置部分的实施例与方法部分的实施例相互对应,因此装置部分的实施例请参见方法部分的实施例的描述,这里暂不赘述。

[0098] 本发明实施例还提供了一种计算机可读存储介质，其上存有计算机程序，该计算机程序被执行时可以实现上述实施例所提供的步骤。该存储介质可以包括：U盘、移动硬盘、只读存储器(Read-Only Memory，ROM)、随机存取存储器(RandomAccess Memory，RAM)、磁碟或者光盘等各种可以存储程序代码的介质。

[0099] 本发明实施例还提供了一种计算机设备，可以包括存储器和处理器，存储器中存有计算机程序，处理器调用存储器中的计算机程序时，可以实现上述实施例所提供的步骤。当然计算机设备还可以包括各种网络接口，电源等组件。

[0100] 说明书中各个实施例采用递进的方式描述，每个实施例重点说明的都是与其他实施例的不同之处，各个实施例之间相同相似部分互相参见即可。对于实施例公开的系统而言，由于其与实施例公开的方法相对应，所以描述的比较简单，相关之处参见方法部分说明即可。应当指出，对于本技术领域的普通技术人员来说，在不脱离本申请原理的前提下，还可以对本申请进行若干改进和修饰，这些改进和修饰也落入本申请权利要求的保护范围内。

[0101] 还需要说明的是，在本说明书中，诸如第一和第二等之类的关系术语仅仅用来将一个实体或者操作与另一个实体或操作区分开来，而不一定要求或者暗示这些实体或操作之间存在任何这种实际的关系或者顺序。而且，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、物品或者设备不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、物品或者设备所固有的要素。在没有更多限制的状况下，由语句“包括一个……”限定的要素，并不排除在包括所述要素的过程、方法、物品或者设备中还存在另外的相同要素。

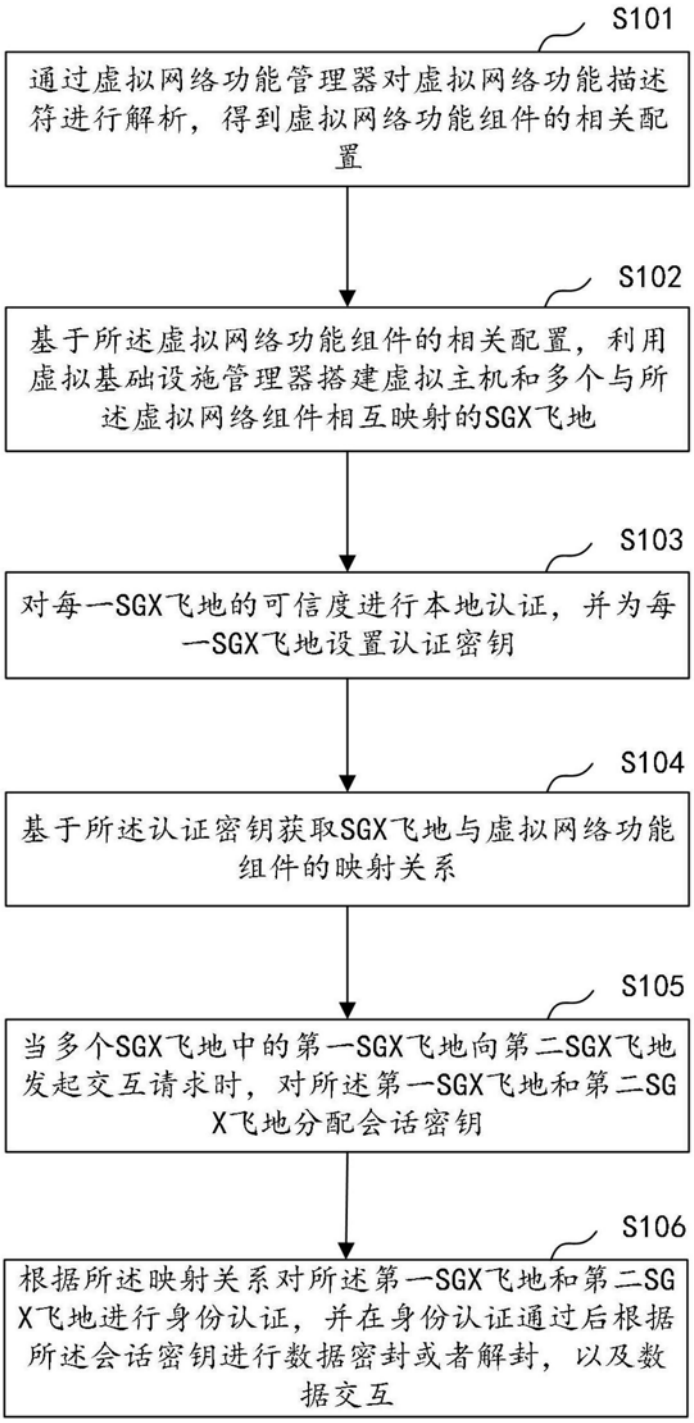

S101
通过虚拟网络功能管理器对虚拟网络功能描述符进行解析，得到虚拟网络功能组件的相关配置
S102
基于所述虚拟网络功能组件的相关配置，利用虚拟基础设施管理器搭建虚拟主机和多个与所述虚拟网络组件相互映射的SGX飞地
S103
对每一SGX飞地的可信度进行本地认证，并为每一SGX飞地设置认证密钥
S104
基于所述认证密钥获取SGX飞地与虚拟网络功能组件的映射关系
S105
当多个SGX飞地中的第一SGX飞地向第二SGX飞地发起交互请求时，对所述第一SGX飞地和第二SGX飞地分配会话密钥
S106
根据所述映射关系对所述第一SGX飞地和第二SGX飞地进行身份认证，并在身份认证通过后根据所述会话密钥进行数据密封或者解封，以及数据交互

图1

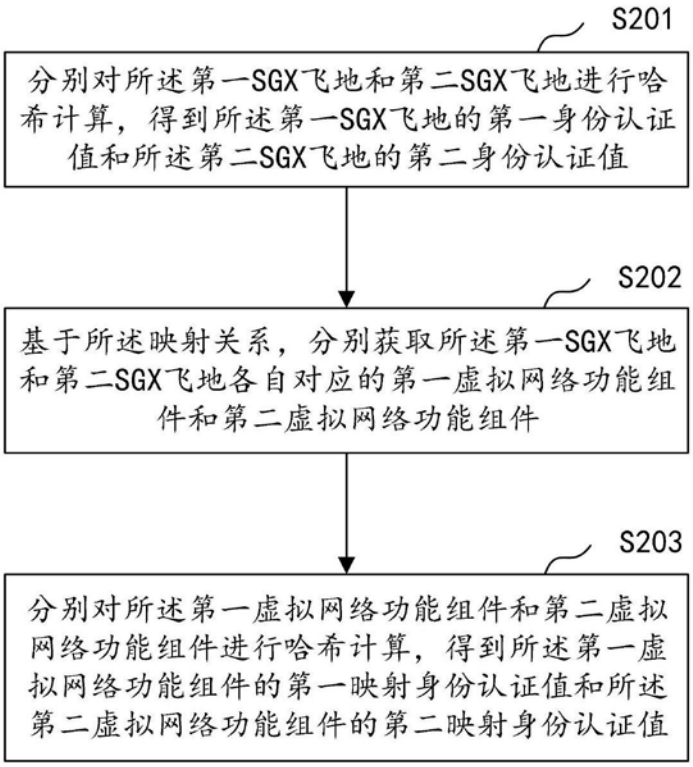

S201
分别对所述第一SGX飞地和第二SGX飞地进行哈希计算，得到所述第一SGX飞地的第一身份认证值和所述第二SGX飞地的第二身份认证值
S202
基于所述映射关系，分别获取所述第一SGX飞地和第二SGX飞地各自对应的第一虚拟网络功能组件和第二虚拟网络功能组件
S203
分别对所述第一虚拟网络功能组件和第二虚拟网络功能组件进行哈希计算，得到所述第一虚拟网络功能组件的第一映射身份认证值和所述第二虚拟网络功能组件的第二映射身份认证值

图2

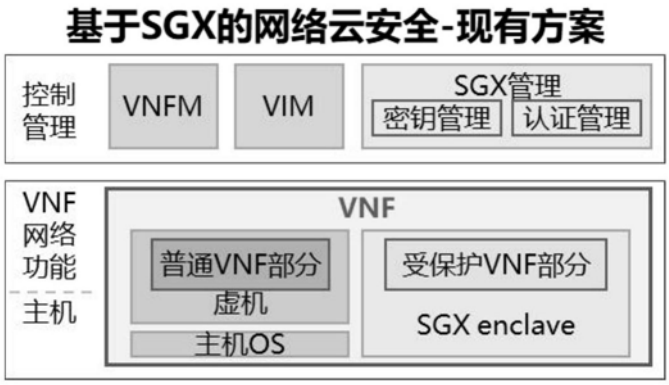

基于SGX的网络云安全-现有方案
控制管理
VNFM
VIM
SGX管理
密钥管理
认证管理
VNF网络功能
主机
VNF
普通VNF部分
虚机
主机OS
受保护VNF部分
SGX enclave

图3

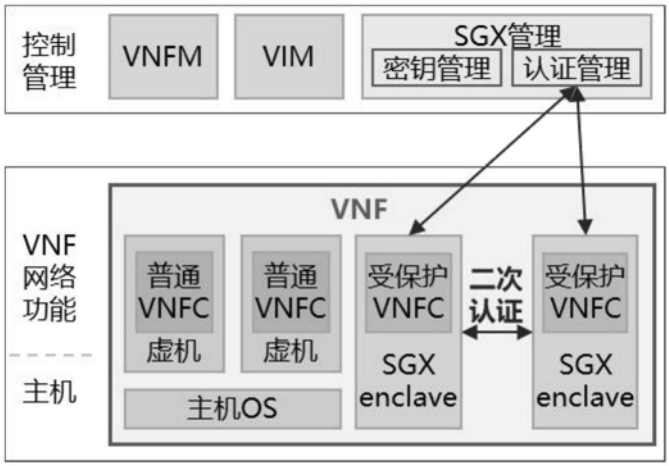

控制管理
VNFM
VIM
SGX管理
密钥管理
认证管理
VNF
VNF网络功能
主机
普通VNFC
虚机
普通VNFC
虚机
受保护VNFC
SGX enclave
二次认证
受保护VNFC
SGX enclave
主机OS

图4

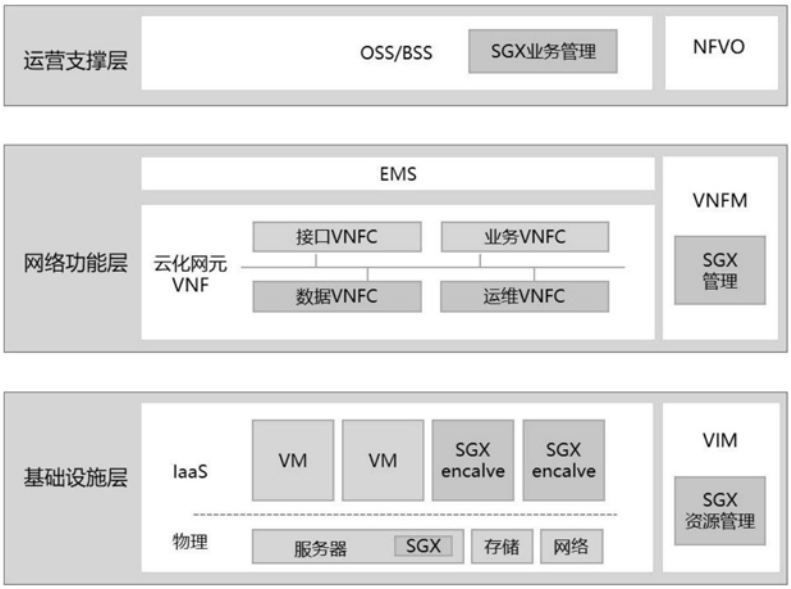

运营支撑层
OSS/BSS
SGX业务管理
NFVO
网络功能层
EMS
云化网元VNF
接口VNFC
业务VNFC
数据VNFC
运维VNFC
VNFM
SGX管理
基础设施层
IaaS
VM
VM
SGX encalve
SGX encalve
物理
服务器
SGX
存储
网络
VIM
SGX资源管理

图5

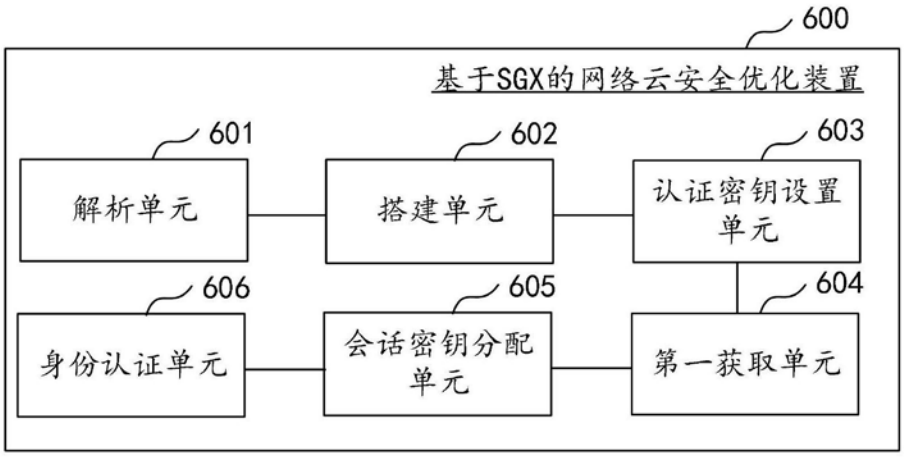

600
基于SGX的网络云安全优化装置
601
解析单元
602
搭建单元
603
认证密钥设置单元
606
身份认证单元
605
会话密钥分配单元
604
第一获取单元

图6

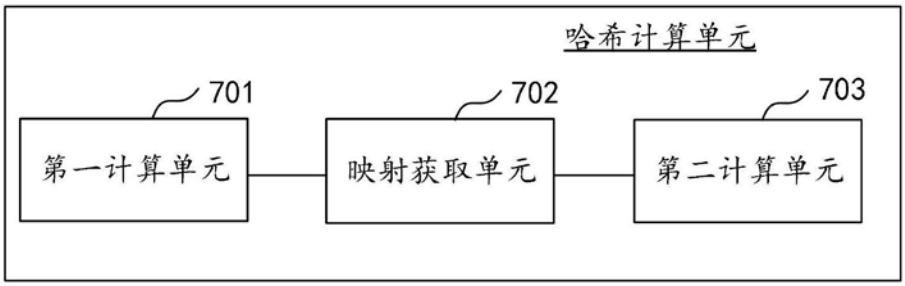

哈希计算单元
701
第一计算单元
702
映射获取单元
703
第二计算单元

图7