(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 107360120 B
(45)授权公告日 2019.06.11

(21)申请号 201610304572.8

(22)申请日 2016.05.10

(65)同一申请的已公布的文献号
申请公布号 CN 107360120 A

(43)申请公布日 2017.11.17

(73)专利权人 华为技术有限公司
地址 518129 广东省深圳市龙岗区坂田华为总部办公楼

(72)发明人 张波 谢于明 黄志钢 汪洋 夏靓

(74)专利代理机构 北京同立钧成知识产权代理有限公司 11205
代理人 张洋 刘芳

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

(56)对比文件
US 2015288541 A1,2015.10.08,
US 8401982 B1,2013.03.19,

审查员 毛韵楠

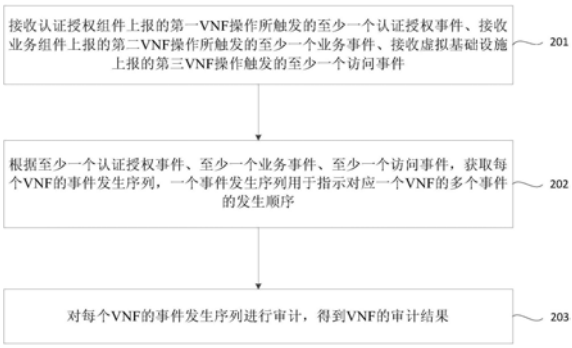
权利要求书3页 说明书14页 附图3页

(54)发明名称

虚拟网络功能的审计方法和装置

(57)摘要

本发明实施例提供一种虚拟网络功能的审计方法和装置，用于审计由包括认证授权组件、业务组件和虚拟基础设施的平台生成的虚拟网络功能，该方法包括：接收认证授权组件上报的事件、接收业务组件上报的事件、接收虚拟基础设施上报的事件；根据接收到的所有事件，获取每个VNF的事件发生序列；对每个VNF的事件发生序列进行审计，得到VNF的审计结果。该方法通过将分散在不同组件的事件，整合在一个事件发生序列中，可直观快速的检测出绕过某个组件而实现的恶意VNF，可以更全面的检测出恶意VNF，降低VNF操作审计的漏检率。



CN 107360120 B

1.一种虚拟网络功能的审计方法,用于审计由包括认证授权组件、业务组件和虚拟基础设施的平台生成的虚拟网络功能VNF,其特征在于,所述方法包括:

接收所述认证授权组件上报的第一VNF操作所触发的至少一个认证授权事件、接收所述业务组件上报的第二VNF操作所触发的至少一个业务事件、接收所述虚拟基础设施上报的第三VNF操作触发的至少一个访问事件;

根据所述至少一个认证授权事件、所述至少一个业务事件、所述至少一个访问事件,获取每个VNF的事件发生序列,一个事件发生序列用于指示对应一个VNF的多个事件的发生顺序;

对每个VNF的事件发生序列进行审计,得到所述VNF的审计结果;

所述第一VNF操作,第二VNF操作,第三VNF操作均包括一个或多个VNF操作。

2.根据权利要求1所述的方法,其特征在于,所述根据所述至少一个认证授权事件、所述至少一个业务事件、所述至少一个访问事件,获取每个VNF的事件发生序列,包括:

根据所述至少一个认证授权事件、所述至少一个业务事件、所述至少一个访问事件中每个事件对应的事件信息中的用户标识,对所述至少一个认证授权事件、所述至少一个业务事件、所述至少一个访问事件分类,得到每个用户标识所对应的所有事件;

根据每个用户标识所对应的所有事件中每个事件对应的事件信息所包含的VNF标识,分析所述同一用户标识所对应的所有事件,得到每个VNF标识对应的所有事件;

根据每个VNF标识对应的所有事件中每个事件对应的事件信息所包含的发生时间,对每个VNF标识对应的所有事件进行排序,以获取每个VNF标识对应的VNF的事件发生序列。

3.根据权利要求2所述的方法,其特征在于,

所述至少一个认证授权事件、所述至少一个业务事件、所述至少一个访问事件中每个事件对应的事件信息均包含所述事件对应的VNF操作调用的模块编号,

所述对每个VNF的事件发生序列进行审计,得到所述VNF的审计结果,包括:

对于每个VNF的事件发生序列,确定所述事件发生序列中的每个事件对应的事件信息所包含的VNF操作调用的模块编号所组成的模块序列;

判断所述模块序列是否符合预设模块序列;

如果所述模块序列不符合预设模块序列,则得到所述VNF为恶意VNF的审计结果。

4.根据权利要求2所述的方法,其特征在于,

所述至少一个认证授权事件、所述至少一个业务事件、所述至少一个访问事件中每个事件对应的事件信息均包含所述事件对应的VNF操作的发生时间,

所述对每个VNF的事件发生序列进行审计,得到所述VNF的审计结果,包括:

对于每个VNF的事件发生序列,根据所述事件发生序列中的每个事件对应的事件信息所包含的发生时间,确定所述事件发生序列中的每个事件的执行时长;

判断所述每个事件的执行时长是否均小于预设时长;

如果存在执行时长大于或等于所述预设时长的事件时,则得到所述VNF为恶意VNF的审计结果。

5.根据权利要求2所述的方法,其特征在于,

所述至少一个认证授权事件、所述至少一个业务事件、所述至少一个访问事件中每个事件对应的事件信息均包含所述事件对应的VNF操作的操作类型和用户类型;

所述对每个VNF的事件发生序列进行审计，得到所述VNF的审计结果，包括：

对于每个VNF的事件发生序列，确定所述事件发生序列中的每个事件对应的事件信息所包含的用户类型以及所述用户类型对应的操作类型集合；

判断所述事件发生序列中的每个事件对应的事件信息所包含的操作类型是否在所述事件信息所包含的用户类型对应的操作类型集合内；

当至少一个事件对应的事件信息所包含的操作类型不在所述事件信息所包含的用户类型对应的操作类型集合内时，得到所述VNF为恶意VNF的审计结果。

6.根据权利要求1至5任一项所述的方法，其特征在于，若所述审计结果为所述VNF为恶意VNF时，所述方法还包括：

输出警告信息。

7.一种虚拟网络功能的审计装置，用于审计由包括认证授权组件、业务组件和虚拟基础设施的平台生成的虚拟网络功能VNF，其特征在于，包括：

接收模块，用于接收所述认证授权组件上报的第一VNF操作所触发的至少一个认证授权事件、接收所述业务组件上报的第二VNF操作所触发的至少一个业务事件、接收所述虚拟基础设施上报的第三VNF操作触发的至少一个访问事件；

排序模块，用于根据所述至少一个认证授权事件、所述至少一个业务事件、所述至少一个访问事件，获取每个VNF的事件发生序列，一个事件发生序列用于指示对应一个VNF的多个事件的发生顺序；

审计模块，用于对每个VNF的事件发生序列进行审计，得到所述VNF的审计结果；

所述第一VNF操作，第二VNF操作，第三VNF操作均包括一个或多个VNF操作。

8.根据权利要求7所述的装置，其特征在于，所述排序模块，具体用于：

根据所述至少一个认证授权事件、所述至少一个业务事件、所述至少一个访问事件中每个事件对应的事件信息中的用户标识，对所述至少一个认证授权事件、所述至少一个业务事件、所述至少一个访问事件分类，得到每个用户标识所对应的所有事件；

根据每个用户标识所对应的所有事件中每个事件对应的事件信息所包含的VNF标识，分析所述同一用户标识所对应的所有事件，得到每个VNF标识对应的所有事件；

根据每个VNF标识对应的所有事件中每个事件对应的事件信息所包含的发生时间，对每个VNF标识对应的所有事件进行排序，以获取每个VNF标识对应的VNF的事件发生序列。

9.根据权利要求8所述的装置，其特征在于，所述至少一个认证授权事件、所述至少一个业务事件、所述至少一个访问事件中每个事件对应的事件信息均包含所述事件对应的VNF操作调用的模块编号，所述审计模块具体用于：

对于每个VNF的事件发生序列，确定所述事件发生序列中的每个事件对应的事件信息所包含的VNF操作调用的模块编号所组成的模块序列；

判断所述模块序列是否符合预设模块序列；

如果所述模块序列不符合预设模块序列，则得到所述VNF为恶意VNF的审计结果。

10.根据权利要求8所述的装置，其特征在于，所述至少一个认证授权事件、所述至少一个业务事件、所述至少一个访问事件中每个事件对应的事件信息均包含所述事件对应的VNF操作的发生时间，所述审计模块具体用于：

对于每个VNF的事件发生序列，根据所述事件发生序列中的每个事件对应的事件信息

所包含的发生时间，确定所述事件发生序列中的每个事件的执行时长；

判断所述每个事件的执行时长是否均小于预设时长；

如果存在执行时长大于或等于所述预设时长的事件时，则得到所述VNF为恶意VNF的审计结果。

11.根据权利要求8所述的装置，其特征在于，所述至少一个认证授权事件、所述至少一个业务事件、所述至少一个访问事件中每个事件对应的事件信息均包含所述事件对应的VNF操作的操作类型和用户类型，所述审计模块具体用于：

对于每个VNF的事件发生序列，确定所述事件发生序列中的每个事件对应的事件信息所包含的用户类型以及所述用户类型对应的操作类型集合；

判断所述事件发生序列中的每个事件对应的事件信息所包含的操作类型是否在所述事件信息所包含的用户类型对应的操作类型集合内；

当至少一个事件对应的事件信息所包含的操作类型不在所述事件信息所包含的用户类型对应的操作类型集合内时，得到所述VNF为恶意VNF的审计结果。

12.根据权利要求7至11任一项所述的装置，其特征在于，若所述审计结果为VNF为恶意VNF时，所述审计模块还用于：

输出警告信息。

13.一种存储介质，其特征在于，所述存储介质存储有一个或多个程序，所述一个或多个程序包括指令，当所述指令被主机中的处理器调用时，使所述主机执行权利要求1至6中任一项所述的方法。

虚拟网络功能的审计方法和装置

技术领域

[0001] 本发明涉及虚拟网络领域，尤其涉及一种虚拟网络功能(virtual network function，简称VNF)的审计方法和装置。

背景技术

[0002] 传统的网络设备例如路由器、交换机、防火墙等一般都是基于该设备包含的硬件所具有的功能，而具有固定网络功能，例如对各种协议的支持、负载均衡、速率控制等，该类网络设备难以升级和扩容。现有技术通常采用网络功能虚拟化来解决上述问题，网络功能虚拟化技术通过在任意网络设备中创建虚拟机来实现VNF，VNF可以灵活的根据需求来创建，不存在升级和扩容的问题。

[0003] 但是与传统的网络设备相比，VNF的这种灵活性导致网络安全管理的复杂度增大。在实现VNF时，通常在已有的平台(如OpenStack云平台)中建立虚拟机，然后通过虚拟机建立VNF。示例性的，现有的OpenStack云平台包括认证授权组件、业务组件和虚拟基础设施，在建立VNF时，合法用户需向认证授权组件申请令牌，通过虚拟基础设施控制业务组件验证令牌权限并完成VNF的建立。

[0004] 其中平台的业务组件可能存在漏洞，恶意用户能够利用业务组件的漏洞创建恶意VNF，恶意VNF攻击其他合法的VNF或者宿主机，以获取到通信双方的数据，从而造成用户数据泄露。现有技术中，通常由技术人员对各组件在建立VNF过程中生成的事件记录日志逐个进行分析，以发现恶意VNF。该方法不仅对技术人员的技术水平要求较高，而且效率低下；同时，当恶意VNF的建立过程绕过平台的任一组件时，该组件不会产生任何日志，技术人员一次只检查一个组件的事件记录日志更难以发现恶意VNF，导致现有恶意VNF的审计方法检测不够全面、漏检率高。

发明内容

[0005] 本发明实施例提供一种虚拟网络功能的审计方法和装置，以解决现有VNF的审计方法检测不够全面、漏检率高的问题。

[0006] 第一方面，本发明实施例提供一种虚拟网络功能的审计方法，用于审计由包括认证授权组件、业务组件和虚拟基础设施的平台生成的虚拟网络功能VNF，该方法包括：

[0007] 接收认证授权组件上报的第一VNF操作所触发的至少一个认证授权事件、接收业务组件上报的第二VNF操作所触发的至少一个业务事件、接收虚拟基础设施上报的第三VNF操作触发的至少一个访问事件；根据至少一个认证授权事件、至少一个业务事件、至少一个访问事件，获取每个VNF的事件发生序列，一个事件发生序列用于指示对应一个VNF的多个事件的发生顺序；对每个VNF的事件发生序列进行审计，得到VNF的审计结果。

[0008] 上述方法通过接收认证授权组件、业务组件和虚拟基础设施上报的事件，并将根据接收到的所有事件获取能够指示每个VNF的事件的发生顺序的事件发生序列，最后对每个VNF的事件发生序列进行审计，以得到审计结果。通过将分散在不同组件的对应于一个

VNF的事件，整合在一个事件发生序列中，可直观快速的检测出绕过某个组件而实现的恶意VNF，可以更全面的检测出恶意VNF，降低VNF操作审计的漏检率。

[0009] 结合第一方面，在第一方面的第一种可能的实现方式中，获取事件发生序列的过程具体包括：

[0010] 根据至少一个认证授权事件、至少一个业务事件、至少一个访问事件中每个事件对应的事件信息中的用户标识，对至少一个认证授权事件、至少一个业务事件、至少一个访问事件分类，得到每个用户标识所对应的所有事件；根据每个用户标识所对应的所有事件中每个事件对应的事件信息所包含的VNF标识，对同一用户标识所对应的所有事件进行分析，得到每个VNF标识对应的所有事件；根据同一VNF标识对应的所有事件中每个事件对应的事件信息所包含的发生时间，对同一VNF标识对应的所有事件进行排序，以获取每个VNF标识对应的VNF的事件发生序列。

[0011] 上述方法中通过根据事件的用户标识、VNF标识、发生时间的不同，将所有的事件进行整理，得到相互间关系更明显的事件发生序列，可提高审计速度。

[0012] 结合第一方面的第一种可能的实现方式，在第一方面的第二种可能的实现方式中，至少一个认证授权事件、至少一个业务事件、至少一个访问事件中每个事件对应的事件信息均包含事件对应的VNF操作调用的模块编号，审计过程具体包括：

[0013] 对于每个VNF的事件发生序列，确定事件发生序列中的每个事件对应的事件信息所包含的VNF操作调用的模块编号所组成的模块序列；判断模块序列是否符合预设模块序列；如果模块序列不符合预设模块序列，则得到VNF为恶意VNF的审计结果。

[0014] 结合第一方面的第一种可能的实现方式，在第一方面的第三种可能的实现方式中，至少一个认证授权事件、至少一个业务事件、至少一个访问事件中每个事件对应的事件信息均包含事件对应的VNF操作的发生时间，审计过程具体包括：

[0015] 对于每个VNF的事件发生序列，根据事件发生序列中的每个事件对应的事件信息所包含的发生时间，确定事件发生序列中的每个事件的执行时长；判断每个事件的执行时长是否均小于预设时长；如果存在执行时长大于或等于预设时长的事件时，则得到VNF为恶意VNF的审计结果。

[0016] 结合第一方面的第一种可能的实现方式，在第一方面的第四种可能的实现方式中，至少一个认证授权事件、至少一个业务事件、至少一个访问事件中每个事件对应的事件信息均包含事件对应的VNF操作的操作类型和用户类型，审计过程具体包括：

[0017] 对于每个VNF的事件发生序列，确定事件发生序列中的每个事件对应的事件信息所包含的用户类型以及用户类型对应的操作类型集合；判断事件发生序列中的每个事件对应的事件信息所包含的操作类型是否在事件信息所包含的用户类型对应的操作类型集合内；当至少一个事件对应的事件信息所包含的操作类型不在事件信息所包含的用户类型对应的操作类型集合内时，得到VNF为恶意VNF的审计结果。

[0018] 结合第一方面、第一方面的第一种至第四种中任一种可行的实现方式，在第一方面的第五种可能的实现方式中，若审计结果为VNF为恶意VNF时，该方法还包括：输出警告信息。

[0019] 结合第一方面、第一方面的第一种至第五种中任一种可行的实现方式，在第一方面的第六种可能的实现方式中，认证授权事件、业务事件和访问事件对应的事件信息中均

包括如下中的至少一种:VNF操作调用的模块编号、用户标识、用户类型、操作类型、VNF标识、发生时间、操作结果、镜像文件类型。

[0020] 下面介绍本发明实施例提供的一种虚拟网络功能的审计装置,该装置与方法一一对应,用以实现上述实施例中的VNF的审计方法,具有相同的技术特征和技术效果,本发明实施例对此不再赘述。

[0021] 第二方面,本发明实施例提供一种虚拟网络功能的审计装置,用于审计由包括认证授权组件、业务组件和虚拟基础设施的平台生成的虚拟网络功能VNF,该装置包括:

[0022] 接收模块,用于接收认证授权组件上报的第一VNF操作所触发的至少一个认证授权事件、接收业务组件上报的第二VNF操作所触发的至少一个业务事件、接收虚拟基础设施上报的第三VNF操作触发的至少一个访问事件;

[0023] 排序模块,用于根据至少一个认证授权事件、至少一个业务事件、至少一个访问事件,获取每个VNF的事件发生序列,一个事件发生序列用于指示对应一个VNF的多个事件的发生顺序;

[0024] 审计模块,用于对每个VNF的事件发生序列进行审计,得到VNF的审计结果。

[0025] 结合第二方面,在第二方面的第一种可能的实现方式中,排序模块具体用于:

[0026] 根据至少一个认证授权事件、至少一个业务事件、至少一个访问事件中每个事件对应的事件信息中的用户标识,对至少一个认证授权事件、至少一个业务事件、至少一个访问事件分类,得到每个用户标识所对应的所有事件;

[0027] 根据每个用户标识所对应的所有事件中每个事件对应的事件信息所包含的VNF标识,分析同一用户标识所对应的所有事件,得到每个VNF标识对应的所有事件;

[0028] 根据每个VNF标识对应的所有事件中每个事件对应的事件信息所包含的发生时间,对每个VNF标识对应的所有事件进行排序,以获取每个VNF标识对应的VNF的事件发生序列。

[0029] 结合第二方面的第一种可能的实现方式,在第二方面的第二种可能的实现方式中,至少一个认证授权事件、至少一个业务事件、至少一个访问事件中每个事件对应的事件信息均包含事件对应的VNF操作调用的模块编号,审计模块具体用于:

[0030] 对于每个VNF的事件发生序列,确定事件发生序列中的每个事件对应的事件信息所包含的VNF操作调用的模块编号所组成的模块序列;判断模块序列是否符合预设模块序列;如果模块序列不符合预设模块序列,则得到VNF为恶意VNF的审计结果。

[0031] 结合第一方面的第一种可能的实现方式,在第一方面的第三种可能的实现方式中,至少一个认证授权事件、至少一个业务事件、至少一个访问事件中每个事件对应的事件信息均包含事件对应的VNF操作的发生时间,审计模块具体用于:

[0032] 对于每个VNF的事件发生序列,根据事件发生序列中的每个事件对应的事件信息所包含的发生时间,确定事件发生序列中的每个事件的执行时长;判断每个事件的执行时长是否均小于预设时长;如果存在执行时长大于或等于预设时长的事件时,则得到VNF为恶意VNF的审计结果。

[0033] 结合第二方面的第一种可能的实现方式,在第二方面的第四种可能的实现方式中,至少一个认证授权事件、至少一个业务事件、至少一个访问事件中每个事件对应的事件信息均包含事件对应的VNF操作的操作类型和用户类型,审计模块具体用于:

[0034] 对于每个VNF的事件发生序列，确定事件发生序列中的每个事件对应的事件信息所包含的用户类型以及用户类型对应的操作类型集合；判断事件发生序列中的每个事件对应的事件信息所包含的操作类型是否在事件信息所包含的用户类型对应的操作类型集合内；当至少一个事件对应的事件信息所包含的操作类型不在事件信息所包含的用户类型对应的操作类型集合内时，得到VNF为恶意VNF的审计结果。

[0035] 结合第二方面、第二方面的第一种至第四种中任一种可行的实现方式，在第二方面的第五种可能的实现方式中，若审计结果为VNF为恶意VNF时，审计模块还用于：输出警告信息。

[0036] 结合第二方面、第二方面的第一种至第五种中任一种可行的实现方式，在第二方面的第六种可能的实现方式中，认证授权事件、业务事件和访问事件对应的事件信息中均包括如下中的至少一种：VNF操作调用的模块编号、用户标识、用户类型、操作类型、VNF标识、时间、操作结果、镜像文件类型。

[0037] 第三方面，本发明实施例提供一种存储介质，该存储介质为存储有一个或多个程序，一个或多个程序包括指令，当指令被主机中的处理器调用时，使主机执行如上述第一方面、第一方面的第一种至第六种中任一种可行的实现方式中的VNF的审计方法。

[0038] 该存储介质用于存储能够执行上述第一方面的各方法实施方式的指令，与第一方面的方法具有相同的技术特征和技术效果，本发明对此不再赘述。

附图说明

[0039] 为了更清楚地说明本发明实施例的技术方案，下面将对实施例描述中所需要使用的附图作简单地介绍。

[0040] 图1为本发明实施例提供的审计系统的架构示意图；

[0041] 图2为本发明实施例提供的一种虚拟网络功能的审计方法的流程示意图；

[0042] 图3为图2提供的方法中获取每个VNF的事件发生序列的过程示意图；

[0043] 图4为本发明实施例提供的一种虚拟网络功能的审计装置的结构示意图。

具体实施方式

[0044] 为使本发明实施例的目的、技术方案和优点更加清楚，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描述。

[0045] 本发明实施例提供一种虚拟网络功能的审计方法和装置，用于审计由包括认证授权组件、业务组件和虚拟基础设施的平台生成的VNF，根据平台的所有组件上报的事件，生成每个VNF的事件发生序列，并根据预设策略对每个VNF的事件发生序列进行审计，可快速准确的检测出恶意VNF。下面对本发明实施例提供的审计系统的架构进行详细说明。

[0046] 图1为本发明实施例提供的审计系统的架构示意图。如图1所示，该系统包括审计装置1和平台2，平台2包括认证授权组件21、业务组件22和虚拟基础设施23，其中认证授权组件21用于认证用户、生成用户令牌；业务组件22用于控制虚拟基础设施23创建虚拟机并实现VNF，并监测虚拟机和VNF的整个生命周期；虚拟基础设施23用于创建虚拟机并实现VNF。当用户向业务组件22发送VNF操作请求时，业务组件22根据VNF操作请求，检测该VNF操作请求中是否携带有令牌，若不含有令牌则要求用户向认证授权组件21进行认证并获取令

牌，若该VNF操作请求中携带有令牌，则业务组件22根据VNF操作请求中的令牌验证该用户是否具有创建虚拟机的权限，当用户具有创建虚拟机的权限时，业务组件22控制虚拟基础设施23创建虚拟机并实现VNF操作请求中指定的VNF功能。

[0047] 示例性的，平台2具体可以为OpenStack云平台，认证授权组件21可以为keystone组件或moon组件，业务组件22包括nova组件、glance组件等，虚拟基础设施203可以为kvm组件。当善意用户创建VNF时，认证授权组件21、业务组件22、虚拟基础设施23均会向审计装置1上报因执行VNF操作触发的事件，审计装置1还可进一步将上报的所有事件存储在数据库中。VNF操作可以为VNF创建、删除、启动、停止、暂停、恢复等。各上报事件对应的事件信息至少包括如下信息中的一个：VNF操作调用的模块编号、用户标识、用户类型、操作类型、VNF标识、镜像文件类型、发生时间、操作结果等。当恶意用户向业务组件22发送VNF操作请求或存在恶意VNF操作时，通常利用平台漏洞，绕过(即不经过)平台2中的某一组件完成虚拟机建立和实现VNF操作，例如绕过认证授权组件21，或绕过虚拟基础设施23。此时，认证授权组件21或虚拟基础设施23将不会上报事件。本申请的审计装置1可以通过汇总所有事件，来发现绕过某个组件的VNF事件，从而发现恶意VNF。

[0048] 下面采用具体实施例对本发明实施例提供的VNF审计方法进行详细说明。

[0049] 图2为本发明实施例提供的一种虚拟网络功能的审计方法的流程示意图。该方法应用于如图1所示的审计装置中，该审计装置可以通过软件或硬件实现。如图2所示，该方法包括：

[0050] 步骤201、接收认证授权组件上报的第一VNF操作所触发的至少一个认证授权事件、接收业务组件上报的第二VNF操作所触发的至少一个业务事件、接收虚拟基础设施上报的第三VNF操作触发的至少一个访问事件。

[0051] 其中，所述第一VNF操作，第二VNF操作，第三VNF操作均可以包括一个或多个VNF操作。

[0052] 步骤202、根据至少一个认证授权事件、至少一个业务事件、至少一个访问事件，获取每个VNF的事件发生序列，一个事件发生序列用于指示对应一个VNF的多个事件的发生顺序。

[0053] 步骤203、对每个VNF的事件发生序列进行审计，得到VNF的审计结果。

[0054] 具体的，在步骤201中，审计装置接收认证授权组件、业务组件和虚拟基础设施上报的事件，并存储各事件对应的事件信息。用户发起的VNF操作可以为一个或多个，因此每个组件上报的事件可以为一个或多个。当所有组件均未上报事件，则说明没有VNF操作。示例性的，本发明实施例中将认证授权组件中因VNF操作触发的事件记为第一VNF操作所触发的认证授权事件，将业务组件中因VNF操作触发的事件记为第二VNF操作所触发的业务事件，将虚拟基础设施中因VNF操作触发的事件记为第三VNF操作触发的访问事件，此处第一VNF操作、第二VNF操作和第三VNF操作可以为同一VNF操作在不同组件中操作时的不同名称，也可为不同的VNF操作。

[0055] 示例性的，认证授权组件、业务组件或者虚拟基础设施向审计装置报告的事件对应的事件信息均包括如下中的至少一种：VNF操作调用的模块编号、用户标识、用户类型、操作类型、VNF标识、发生时间、操作结果、镜像文件类型。其中，不同的用户类型对应不同的用户权限，可执行的操作类型不同，对应不同的操作类型集合。其中，用户标识用于识别发起

VNF操作的用户;用户类型用于指示发起VNF操作的用户的级别或权限,根据用户类型可确定发起VNF操作的用户能够执行的操作类型;操作类型用于指示用户发起的VNF操作的类型;VNF标识用于指示VNF操作涉及的VNF;发生时间用于指示VNF操作发生的时刻;操作结果用于指示VNF操作是否成功;镜像文件类型用于指示创建VNF时使用的镜像文件的类型,镜像文件可以按照网络功能进行分类。

[0056] 下面以认证授权组件为例,对事件信息进行详细说明。认证授权组件上报的事件对应的事件信息可以如下所示:

[0057] {模块编号:1;用户标识:admin1;用户类型:admin;操作类型:创建;VNF标识:vRouter;时间:2015-12-20 15:10:27;}。

[0058] 该事件信息表示用户类型为admin的用户admin1在2015年12月20日15点10分27时创建了一个虚拟路由器(Virtual Router)。

[0059] 具体的,在步骤202中,根据步骤201中接收到的所有事件,获取每个VNF的事件发生序列,一个事件发生序列用于指示对应一个VNF的多个事件的发生顺序,具体在获取事件发生序列时,可根据各事件发生的时间先后顺序将审计装置接收到的对应同一个VNF的所有事件进行排序。事件发生序列将每一组件中发生的对应同一个VNF的事件按照时间先后进行排序,方便了技术人员查看同一个VNF操作请求在各组件所分别引发的事件,当该VNF操作为恶意事件,例如故意绕过某个组件时,技术人员可直接发现。可选的,还可进一步在按照时间先后将事件进行排序后,根据VNF操作的用户标识或VNF标识等参数,对所有上报的事件进行整理,得到一个或多个事件发生序列,进一步方便了技术人员进行审计。

[0060] 具体的,在步骤203中,对步骤202中得到的每个VNF的事件发生序列进行审计,得到审计结果。具体的审计策略可以为,依据预设规则对每个VNF对应的事件发生序列中各事件对应的事件信息进行审计,当一个VNF的事件信息中存在不符合预设规则的信息时,审计结果为该VNF为恶意VNF。

[0061] 示例性的,预设规则可依据如下信息中的至少一种进行设置:用户标识、用户类型、操作类型、VNF标识、镜像文件类型、VNF操作调用的模块编号、发生时间。

[0062] 当依据用户标识或用户类型设置预设规则时,预设规则可以为:确定事件发生序列中各事件对应的事件信息中的用户标识或者该用户类型不在黑名单中。即当曾经被列入到黑名单中的操作用户执行VNF操作时,可直接认为该VNF操作不符合预设规则,则输出警告信息。

[0063] 操作类型表示操作VNF的动作,可能是创建、删除、启动、停止、暂停、恢复等。不同操作用户或不同角色可向业务组件发送的VNF操作请求不同,当用户角色为管理员时,其VNF操作请求可以包括创建、删除、启动、停止、暂停、恢复等,当用户角色为VNF拥有者时,其VNF操作请求可仅为启动、停止、暂停和恢复。

[0064] VNF标识可以表示具有某些属性的VNF集合,同样的,用户类型不同,其可操作的VNF对象也不同。VNF操作调用的模块编号表示执行VNF操作必须经过的模块的编号,在依据模块编号设置预设规则时,可按照执行VNF操作必须经过的模块的顺序设置预设规则,即一个事件发生序列中的各事件依次对应的模块的编号。根据发生时间可确定事件发生序列中的每个事件的执行时长,可根据各事件可持续的最长时长设置预设规则。

[0065] 具体在审计时,可以为技术人员依照上述预设规则进行审计,也可以为依据预设

的一个或多个预设规则进行自动审计，审计结果包括存在恶意VNF或不存在恶意VNF。该审计过程可以在审计装置接收上报事件后实时进行，或间隔预设时间段执行。

[0066] 可选的，在步骤203之后，本发明实施例提供的审计方法还包括：

[0067] 若审计结果为VNF为恶意VNF时，则输出警告信息。

[0068] 当对每个VNF的事件发生序列进行审计，发现多个VNF为恶意VNF时，可以输出包括多个恶意VNF的警告信息，或分别针对每个恶意VNF分别发送警告信息。

[0069] 警告信息可具体包括不符合预设规则的事件对应的事件信息，还可包括判断为恶意VNF所不符合的预设规则，以方便技术人员快速发现恶意VNF并解决。具体的警告信息输出方式可以为弹出警告信息窗、可以为将恶意VNF对应的事件高亮显示、也可为发出警报声。

[0070] 本发明实施例提供的审计方法中，审计装置接收认证授权组件、业务组件和虚拟基础设施上报的事件，并根据接收到的所有事件获取能够指示每个VNF的事件的发生顺序的事件发生序列，最后对每个VNF的事件发生序列进行审计，以得到审计结果。通过将分散在不同组件的对应于一个VNF的事件，整合在一个事件发生序列中，可直观快速的检测出绕过某个组件而实现的恶意VNF，可以更全面的检测出恶意VNF，降低VNF操作审计的漏检率。

[0071] 下面结合图3，采用具体的实施例，对步骤202中的获取每个VNF的事件发生序列的过程进行详细说明。图3为图2提供的方法中获取每个VNF的事件发生序列的过程示意图，如图3所示，该过程包括：

[0072] 步骤301、根据至少一个认证授权事件、至少一个业务事件、至少一个访问事件用户标识中每个事件对应的事件信息中的用户标识，对至少一个认证授权事件、至少一个业务事件、至少一个访问事件分类，得到每个用户标识所对应的所有事件；

[0073] 步骤302、根据每个用户标识所对应的所有事件中每个事件对应的事件信息所包含的VNF标识，分析同一用户标识所对应的所有事件，得到每个VNF标识对应的所有事件；

[0074] 步骤303、根据每个VNF标识对应的所有事件中每个事件对应的事件信息所包含的发生时间，对每个VNF标识对应的所有事件进行排序，以获取每个VNF标识对应的VNF的事件发生序列。

[0075] 在本实施例中，首先根据各上报事件各自对应的事件信息中包含的用户标识将审计装置接收到的所有事件按照用户标识的不同，划分为不同类，同一类事件对应同一个操作用户；然后，针对同一个操作用户的所有事件，再按照VNF标识的不同，进行分析，得到每个VNF标识对应的所有事件，每个VNF标识对应的所有事件具有相同的操作用户和相同的操作对象；最后，对于具有相同的操作用户和相同的操作对象的事件，按照时间的先后进行排序，即可得到每个VNF的事件发生序列，每个事件发生序列代表了一个操作用户针对一个VNF，按照时间顺序进行了哪些操作。通过对所有上报的事件进行汇总和分类，可方便用户设定更具有针对性的VNF的预设策略，并方便后续根据预设策略进行审计，提高审计效率。

[0076] 下面举一个具体实施例来说明上述事件发生序列的获取方式。

[0077] 审计装置接收到认证授权组件上报的3个认证授权事件，业务组件上报的4个业务事件，虚拟基础设施上报的4个访问事件。

[0078] 其中，3个认证授权事件A1、A2、A4各自对应的事件信息可分别简单记为：

[0079] A1{user1,file1,2015-12-20 15:10:27}；

[0080] A2{user2,file2,2015-12-20 16:10:27}；

[0081] A4{user1,file4,2015-12-20 20:10:27}。

[0082] 四个业务事件B1、B2、B3、B4各自对应的事件信息可分别简单记为：

[0083] B1{user1,file1,2015-12-20 15:20:27}；

[0084] B2{user2,file2,2015-12-20 16:20:27}；

[0085] B3{user3,file3,2015-12-20 17:20:27}；

[0086] B4{user1,file4,2015-12-20 20:20:27}。

[0087] 四个访问事件C1、C2、C3、C4各自对应的事件信息可分别简单记为：

[0088] C1{user1,file1,2015-12-20 15:30:27}；

[0089] C2{user2,file2,2015-12-20 16:30:27}；

[0090] C3{user3,file3,2015-12-20 17:30:27}；

[0091] C4{user1,file4,2015-12-20 20:30:27}。

[0092] 审计装置首先按照所有事件A1、A2、A4、B1、B2、B3、B4、C1、C2、C3、C4(共11个)各自对应的事件信息中的用户标识的不同，可发现共有3类：user1、user2、user3，将11个事件划分为3类：

[0093] 第一类：操作用户为user1的所有事件，共6个，A1、A4、B1、B4、C1、C4；

[0094] 第二类：操作用户为user2的所有事件，共3个，A2、B2、C2；

[0095] 第三类：操作用户为user3的所有事件，共2个，B3、C3。

[0096] 然后审计装置将每一类的所有事件按照每个事件对应的事件信息中的VNF标识的不同，对具有相同VNF标识的事件进行分析。

[0097] 在第一类中：可得到对应同一VNF标识的事件A1、B1和C1，即A1、B1和C1均为操作用户user1对file1进行操作而引发上报的事件，以及对应另一个VNF标识的事件A4、B4和C4；即A4、B4和C4均为操作用户user1对file4进行操作而引发上报的事件；

[0098] 在第二类中：可得到对应同一VNF标识的事件A2、B2和C2，即A2、B2和C2均为操作用户user2对file2进行操作而引发上报的事件；

[0099] 在第三类中：可得到对应同一VNF标识的事件B3和C3，即B3和C3均为操作用户user3对file3进行操作而引发上报的事件。

[0100] 最后，对每组事件，即A1、B1和C1；A4、B4和C4；A2、B2和C2；B3和C3分别按照发生时间进行排序，得到4个事件发生序列，即A1、B1和C1；A4、B4和C4；A2、B2和C2；B3和C3。

[0101] 在得到4个事件发生序列后，可直观的发现B3和C3所组成的事件发生序列中缺少认证授权组件所上报的事件，即表明user3对file3进行操作没有经过认证授权，可认为file3为恶意VNF。通过根据事件的操作用户、操作对象、发生时间的不同，将所有的事件进行整理，得到每个VNF的更明显更直观的事件发生序列，可提高审计速度。因此，通过获取事件发生序列可直观快速的检测出恶意VNF并降低漏检率。

[0102] 下面在图3实施例的基础上，结合不同的预设规则，对事件发生序列的具体审计方式进行详细说明。

[0103] 示例性的，针对不同预设规则的审计过程包括如下可行的实现方式：

[0104] 可行的实现方式一：

[0105] 至少一个认证授权事件、至少一个业务事件、至少一个访问事件中每个事件对应

的事件信息均包含事件对应的VNF操作调用的模块编号,VNF的审计过程具体包括:

[0106] 对于每个VNF的事件发生序列,确定事件发生序列中的每个事件对应的事件信息所包含的VNF操作调用的模块编号所组成的模块序列;

[0107] 判断模块序列是否符合预设模块序列;

[0108] 如果模块序列符合预设模块序列,则得到VNF为合法VNF的审计结果;如果模块序列不符合预设模块序列,则得到VNF为恶意VNF的审计结果。

[0109] 具体的,可根据善意用户创建VNF时所触发的事件发生序列中的每个事件对应的事件信息所包含的VNF操作调用的模块编号所组成的模块序列,确定预设模块序列,该预设模块序列限定了善意的VNF操作需按时间顺序依次调用的模块,当发现事件发生序列中的模块调用情况与预设模块序列指示的模块调用情况不符时,可确定事件发生序列所对应的VNF为恶意VNF,故输出警告信息。

[0110] 例如,当审计装置接收到认证授权组件上报的1个认证授权事件A1,业务组件上报的1个业务事件B1,虚拟基础设施上报的1个访问事件C1;其中,A1、B1、C1各自对应的事件信息可分别简单记为:

[0111] A1{user1,file1,1,2015-12-20 15:10:27};

[0112] B1{user1,file1,2、3,2015-12-20 15:20:27};

[0113] C1{user1,file1,4,2015-12-20 15:30:27}。

[0114] 首先根据图3所示实施例即可得到事件发生序列A1、B1、C1。根据事件发生序列中的每个事件对应的事件信息所包含的VNF操作调用的模块编号1、2、3和4,即可组成该事件发生序列对应的模块序列{1、2、3、4}。然后将该模块序列与预设模块序列进行比较,判断二者是否相符。示例性的,当预设模块序列为{1、2、3、4}时,可得到该事件发生序列对应的VNF为合法VNF的审计结果;当预设模块序列为{1、2、3、4、5}时,可发现当前事件发生序列对应的模块序列与预设模块序列不符,可得到该事件发生序列对应的VNF为恶意VNF的审计结果,并发出警报信息。

[0115] 可行的实现方式二:

[0116] 至少一个认证授权事件、至少一个业务事件、至少一个访问事件中每个事件对应的事件信息均包含事件对应的VNF操作的发生时间,VNF的审计过程具体包括:

[0117] 对于每个VNF的事件发生序列,根据事件发生序列中的每个事件对应的事件信息所包含的发生时间,确定事件发生序列中的每个事件的执行时长;

[0118] 判断每个事件的执行时长是否均小于预设时长;

[0119] 如果存在执行时长大于或等于预设时长的事件时,则得到VNF为恶意VNF的审计结果;如果每个事件的执行时长均小于预设时长,则得到VNF为合法VNF的审计结果。

[0120] 具体的,可根据善意用户创建VNF时所触发的事件发生序列中的各事件对应的事件信息所包含的发生时间,确定善意VNF的事件发生序列中每个事件的执行时长,根据该执行时长可设定预设时长,该预设时长限定了善意用户创建的VNF对应的事件发生序列中每个事件的最长间隔时间,当发现事件发生序列所指示的所有事件的执行时长中存在至少一个执行时长超过了预设时长时,可得到该事件发生序列对应的VNF为恶意VNF的审计结果,故输出警告信息。

[0121] 示例性的,参考可行的实现方式一中的具体示例,当事件发生序列A1、B1、C1各自

对应的事件信息为如下所示时：

[0122] A1{user1,file1,1,2015-12-20 15:10:27}；

[0123] B1{user1,file1,2、3,2015-12-20 16:10:27}；

[0124] C1{user1,file1,4,2015-12-20 16:30:27}。

[0125] 根据事件A1和B1的发生时间，可知用户user1在认证授权组件中花费了1小时，然后才在业务组件中开始事件B1，考虑到通常认证授权过程10分钟即可结束，可将预设时长设置为10分钟，该事件发生序列中的1小时明显超出了预设时长，可得到该事件发生序列对应的VNF为恶意VNF的审计结果。

[0126] 示例性的，事件C1的执行时长可进一步根据用户user1针对file1所做的后续操作确定，也可不为事件C1设定预设时长。进一步的，还可针对不同组件上报的事件设定不同的预设时长。

[0127] 可行的实现方式三：

[0128] 至少一个认证授权事件、至少一个业务事件、至少一个访问事件中每个事件对应的事件信息均包含事件对应的VNF操作的操作类型和用户类型，VNF的审计过程具体包括：

[0129] 对于每个VNF的事件发生序列，确定事件发生序列中的每个事件对应的事件信息所包含的用户类型以及用户类型对应的操作类型集合；

[0130] 判断事件发生序列中的每个事件对应的事件信息所包含的操作类型是否在事件信息所包含的用户类型对应的操作类型集合内；

[0131] 当至少一个事件对应的事件信息所包含的操作类型不在事件信息所包含的用户类型对应的操作类型集合内时，得到VNF为恶意VNF的审计结果；如果每个事件对应的事件息所包含的操作类型均在事件信息所包含的用户类型对应的操作类型集合内时，得到VNF为合法VNF的审计结果。

[0132] 具体的，不同的用户类型对应不同的用户权限，可执行的操作类型不同，对应不同的操作类型集合。根据事件发生序列中每个事件对应的事件信息包含的用户类型，以及该用户类型对应的操作类型集合，可确定该事件发生序列对应的操作类型范围，审计过程具体为检测出事件发生序列中的每个事件的操作类型是否在该事件发生序列的操作类型集合内，当超出集合范围时，得到当前事件发生序列对应的VNF为恶意VNF的审计结果，故输出警告信息。

[0133] 示例性的，仍参考可行的实现方式一中的具体示例，当事件发生序列A1、B1、C1各自对应的事件信息为如下所示时：

[0134] A1{user1,file1,creat,1,2015-12-20 15:10:27}；

[0135] B1{user1,file1,creat,2、3,2015-12-20 16:10:27}；

[0136] C1{user1,file1,creat,4,2015-12-20 16:30:27}。

[0137] 根据事件发生序列的用户标识user1，确定当前操作用户user1所属的用户类型为普通用户user，进而可确定当前操作用户对应的操作类型集合{delete、pause}，即当前操作用户user1只能执行删除和暂停操作，不能执行创建操作，即事件发生序列中的每个事件对应的事件信息中的操作类型不在该事件发生序列的用户类型对应的操作类型集合内，当前操作用户user1进行了超出其权限的操作，可得到当前事件发生序列对应的VNF为恶意VNF的审计结果。

[0138] 示例性的，当事件发生序列中只要有一个事件对应的事件信息中包含有VNF操作的操作类型时，即可采用该可行的实现方式进行VNF审核。

[0139] 本发明实施例另一方面提供一种VNF的审计装置，用于审计由包括认证授权组件、业务组件和虚拟基础设施的平台生成的虚拟网络功能VNF，该装置可以执行上述任一实施例中的VNF的审计方法，其实现原理和技术效果类似，在此不再赘述。图4为本发明实施例提供的一种虚拟网络功能的审计装置的结构示意图。如图4所示，该装置包括：

[0140] 接收模块401，用于接收认证授权组件上报的第一VNF操作所触发的至少一个认证授权事件、接收业务组件上报的第二VNF操作所触发的至少一个业务事件、接收虚拟基础设施上报的第三VNF操作触发的至少一个访问事件；

[0141] 排序模块402，用于根据至少一个认证授权事件、至少一个业务事件、至少一个访问事件，获取每个VNF的事件发生序列，一个事件发生序列用于指示对应一个VNF的多个事件的发生顺序；

[0142] 审计模块403，用于对每个VNF的事件发生序列进行审计，得到VNF的审计结果。

[0143] 可选的，在图4所述实施例的基础上，对排序模块进行详细说明。排序模块402具体用于：

[0144] 根据至少一个认证授权事件、至少一个业务事件、至少一个访问事件中每个事件对应的事件信息中的用户标识，对至少一个认证授权事件、至少一个业务事件、至少一个访问事件分类，得到每个用户标识所对应的所有事件；

[0145] 根据每个用户标识所对应的所有事件中每个事件对应的事件信息所包含的VNF标识，分析同一用户标识所对应的所有事件，得到每个VNF标识对应的所有事件；

[0146] 根据每个VNF标识对应的所有事件中每个事件对应的事件信息所包含的发生时间，对每个VNF标识对应的所有事件进行排序，以获取每个VNF标识对应的VNF的事件发生序列。

[0147] 可选的，至少一个认证授权事件、至少一个业务事件、至少一个访问事件中每个事件对应的事件信息均包含事件对应的VNF操作调用的模块编号，审计模块403具体用于：

[0148] 对于每个VNF的事件发生序列，确定事件发生序列中的每个事件对应的事件信息所包含的VNF操作调用的模块编号所组成的模块序列；判断模块序列是否符合预设模块序列；如果模块序列不符合预设模块序列，则得到VNF为恶意VNF的审计结果。

[0149] 可选的，至少一个认证授权事件、至少一个业务事件、至少一个访问事件中每个事件对应的事件信息均包含事件对应的VNF操作的发生时间，审计模块403具体用于：

[0150] 对于每个VNF的事件发生序列，根据事件发生序列中的每个事件对应的事件信息所包含的发生时间，确定事件发生序列中的每个事件的执行时长；判断每个事件的执行时长是否均小于预设时长；如果存在执行时长大于或等于预设时长的事件时，则得到VNF为恶意VNF的审计结果。

[0151] 可选的，至少一个认证授权事件、至少一个业务事件、至少一个访问事件中每个事件对应的事件信息均包含事件对应的VNF操作的操作类型和用户类型，审计模块403具体用于：

[0152] 对于每个VNF的事件发生序列，确定事件发生序列中的每个事件对应的事件信息所包含的用户类型以及用户类型对应的操作类型集合；判断事件发生序列中的每个事件对

应的事件信息所包含的操作类型是否在事件信息所包含的用户类型对应的操作类型集合内;当至少一个事件对应的事件信息所包含的操作类型不在事件信息所包含的用户类型对应的操作类型集合内时,得到VNF为恶意VNF的审计结果。

[0153] 可选的,若审计结果为VNF为恶意VNF时,审计模块403还用于:输出警告信息。

[0154] 本发明实施例又一方面提供一种虚拟网络功能的审计装置,用于审计由包括认证授权组件、业务组件和虚拟基础设施的平台生成的虚拟网络功能VNF,该装置可以执行上述任一实施例中的VNF的审计方法,其实现原理和技术效果类似,在此不再赘述。该装置包括:

[0155] 接收器,用于接收认证授权组件上报的第一VNF操作所触发的至少一个认证授权事件、接收业务组件上报的第二VNF操作所触发的至少一个业务事件、接收虚拟基础设施上报的第三VNF操作触发的至少一个访问事件;

[0156] 处理器,用于根据接收器接收到的至少一个认证授权事件、至少一个业务事件、至少一个访问事件,获取每个VNF的事件发生序列,一个事件发生序列用于指示对应一个VNF的多个事件的发生顺序;对每个VNF的事件发生序列进行审计,得到VNF的审计结果。

[0157] 可选的,该装置还包括存储器,用于存储接收器接收到的所有事件,处理器根据存储器中存储的所有事件进行后续的审计过程。

[0158] 可选的,处理器具体用于:

[0159] 根据至少一个认证授权事件、至少一个业务事件、至少一个访问事件中每个事件对应的事件信息中的用户标识,对至少一个认证授权事件、至少一个业务事件、至少一个访问事件分类,得到每个用户标识所对应的所有事件;

[0160] 根据每个用户标识所对应的所有事件中每个事件对应的事件信息所包含的VNF标识,分析同一用户标识所对应的所有事件,得到每个VNF标识对应的所有事件;

[0161] 根据每个VNF标识对应的所有事件中每个事件对应的事件信息所包含的发生时间,对每个VNF标识对应的所有事件进行排序,以获取每个VNF标识对应的VNF的事件发生序列;

[0162] 对每个VNF的事件发生序列进行审计,得到VNF的审计结果。

[0163] 可选的,至少一个认证授权事件、至少一个业务事件、至少一个访问事件中每个事件对应的事件信息均包含事件对应的VNF操作调用的模块编号,处理器具体用于:

[0164] 对于每个VNF的事件发生序列,确定事件发生序列中的每个事件对应的事件信息所包含的VNF操作调用的模块编号所组成的模块序列;判断模块序列是否符合预设模块序列;如果模块序列不符合预设模块序列,则得到VNF为恶意VNF的审计结果。

[0165] 可选的,至少一个认证授权事件、至少一个业务事件、至少一个访问事件中每个事件对应的事件信息均包含事件对应的VNF操作的发生时间,处理器具体用于:

[0166] 对于每个VNF的事件发生序列,根据事件发生序列中的每个事件对应的事件信息所包含的发生时间,确定事件发生序列中的每个事件的执行时长;判断每个事件的执行时长是否均小于预设时长;如果存在执行时长大于或等于预设时长的事件时,则得到VNF为恶意VNF的审计结果。

[0167] 可选的,至少一个认证授权事件、至少一个业务事件、至少一个访问事件中每个事件对应的事件信息均包含事件对应的VNF操作的操作类型和用户类型,处理器具体用于:

[0168] 对于每个VNF的事件发生序列,确定事件发生序列中的每个事件对应的事件信息

所包含的用户类型以及用户类型对应的操作类型集合;判断事件发生序列中的每个事件对应的事件信息所包含的操作类型是否在事件信息所包含的用户类型对应的操作类型集合内;当至少一个事件对应的事件信息所包含的操作类型不在事件信息所包含的用户类型对应的操作类型集合内时,得到VNF为恶意VNF的审计结果。

[0169] 可选的,该装置还包括发送器,用于在审计结果为VNF为恶意VNF时,输出警告信息。

[0170] 本发明实施例再一方面提供一种存储介质,该存储介质存储有一个或多个程序,一个或多个程序包括指令,当指令被主机中的处理器调用时,可以控制主机执行上述任一方法实施例中的VNF的审计方法。

[0171] 前述的存储介质包括:U盘、移动硬盘、只读存储器(read-only memory,简称ROM)、随机存取存储器(random access memory,简称RAM)、磁碟或者光盘等各种可以存储程序代码的介质。

[0172] 本领域普通技术人员可以意识到,结合本文中所公开的实施例描述的各示例的单元及算法步骤,能够以电子硬件、或者计算机软件和电子硬件的结合来实现。这些功能究竟以硬件还是软件方式来执行,取决于技术方案的特定应用和设计约束条件。专业技术人员可以对每个特定的应用来使用不同方法来实现所描述的功能,但是这种实现不应认为超出本发明的范围。

[0173] 所属领域的技术人员可以清楚地了解到,为描述的方便和简洁,上述描述的系统、装置和单元的具体工作过程,可以参考前述方法实施例中的对应过程,在此不再赘述。

[0174] 在本申请所提供的几个实施例中,应该理解到,所揭露的系统、装置和方法,可以通过其它的方式实现。例如,以上所描述的装置实施例仅仅是示意性的,例如,所述单元的划分,仅仅为一种逻辑功能划分,实际实现时可以有另外的划分方式,例如多个单元或组件可以结合或者可以集成到另一个系统,或一些特征可以忽略,或不执行。另一点,所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些接口,装置或单元的间接耦合或通信连接,可以是电性,机械或其它的形式。

[0175] 本发明的说明书和权利要求书及上述附图中的术语“第一”、“第二”、“第三”“第四”等(如果存在)是用于区别类似的对象,而不必用于描述特定的顺序或先后次序。应该理解这样使用的数据在适当情况下可以互换,以便这里描述的本发明的实施例例如能够以除了在这里图示或描述的那些以外的顺序实施。此外,术语“包括”和“具有”以及他们的任何变形,意图在于覆盖不排他的包含,例如,包含了一系列步骤或单元的过程、方法、系统、产品或设备不必限于清楚地列出的那些步骤或单元,而是可包括没有清楚地列出的或对于这些过程、方法、产品或设备固有的其它步骤或单元。

[0176] 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单元来实现本实施例方案的目的。

[0177] 另外,在本发明各个实施例中的各功能单元可以集成在一个处理单元中,也可以是各个单元单独物理存在,也可以两个或两个以上单元集成在一个单元中。

[0178] 最后应说明的是:以上各实施例仅用以说明本发明的技术方案,而非对其限制;尽

管参照前述各实施例对本发明进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分或者全部技术特征进行等同替换；而这些修改或者替换，并不使相应技术方案的本质脱离本发明各实施例技术方案的范围。

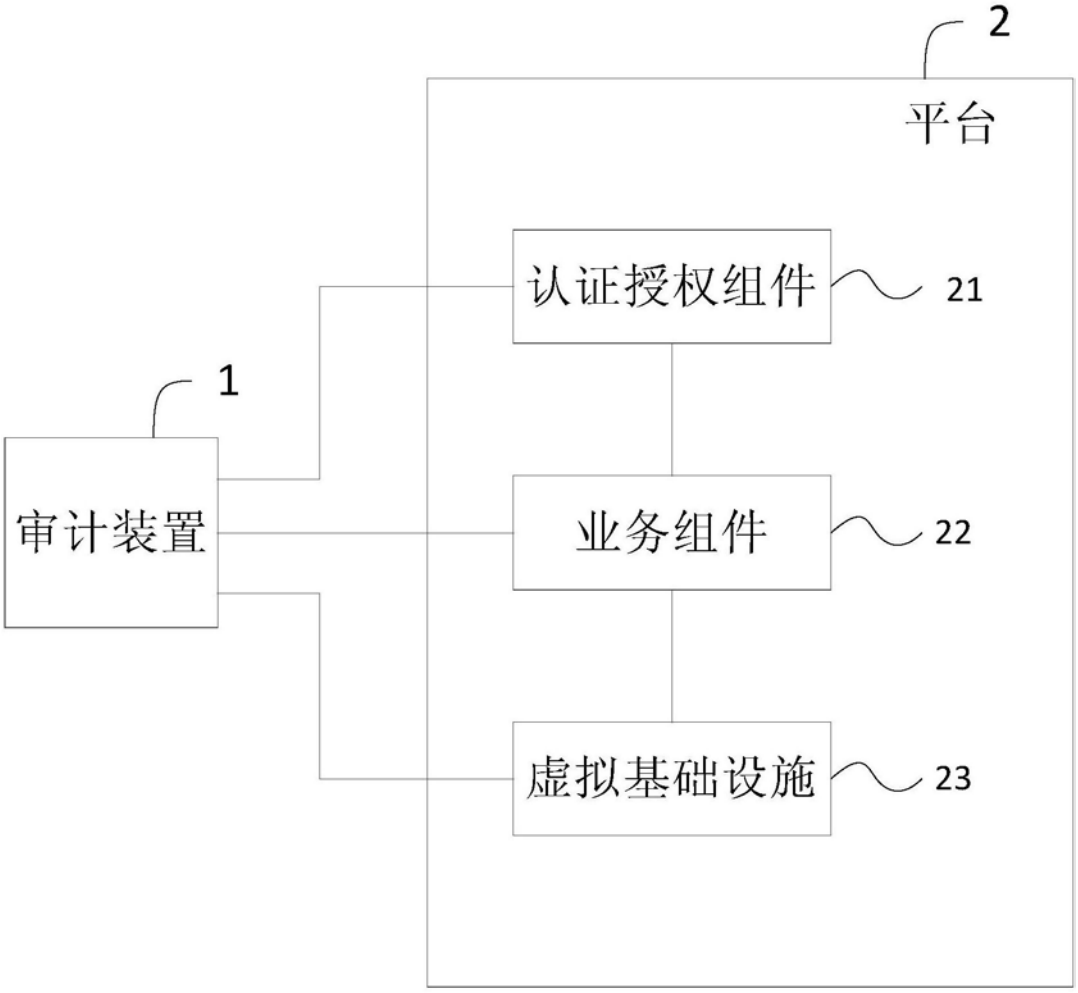


图1

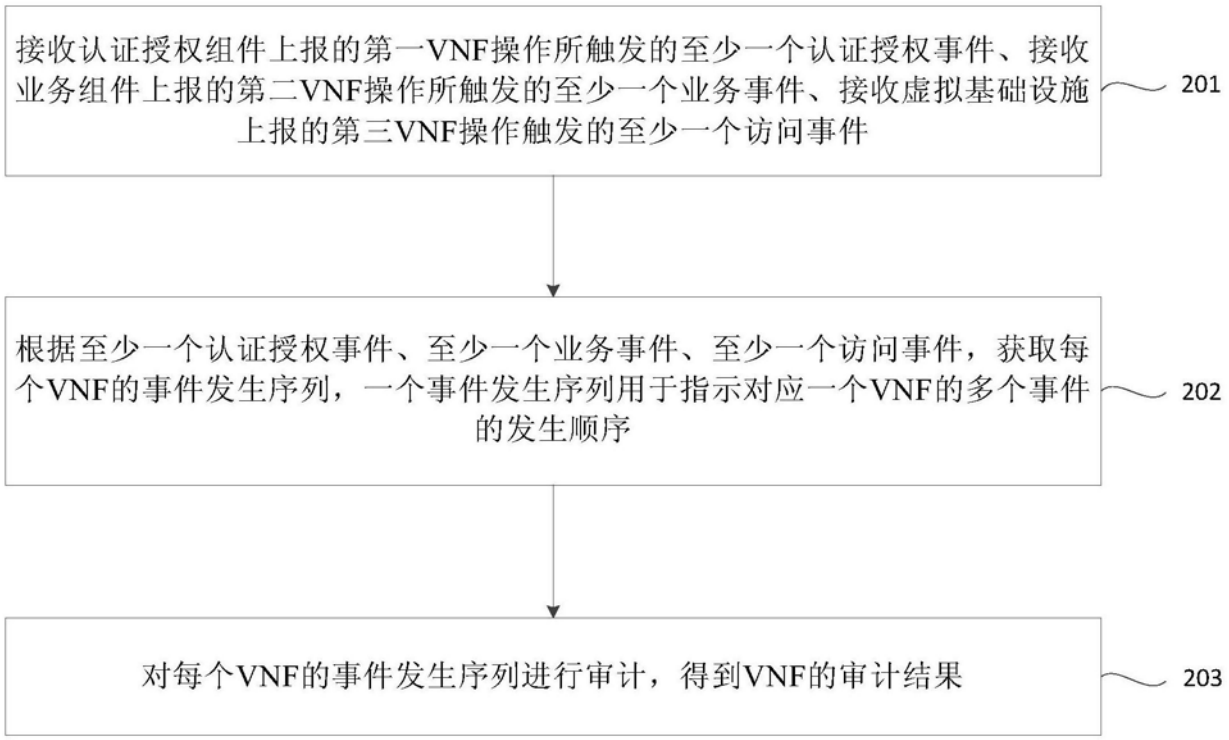

接收认证授权组件上报的第一VNF操作所触发的至少一个认证授权事件、接收业务组件上报的第二VNF操作所触发的至少一个业务事件、接收虚拟基础设施上报的第三VNF操作触发的至少一个访问事件
201
根据至少一个认证授权事件、至少一个业务事件、至少一个访问事件，获取每个VNF的事件发生序列，一个事件发生序列用于指示对应一个VNF的多个事件的发生顺序
202
对每个VNF的事件发生序列进行审计，得到VNF的审计结果
203

图2

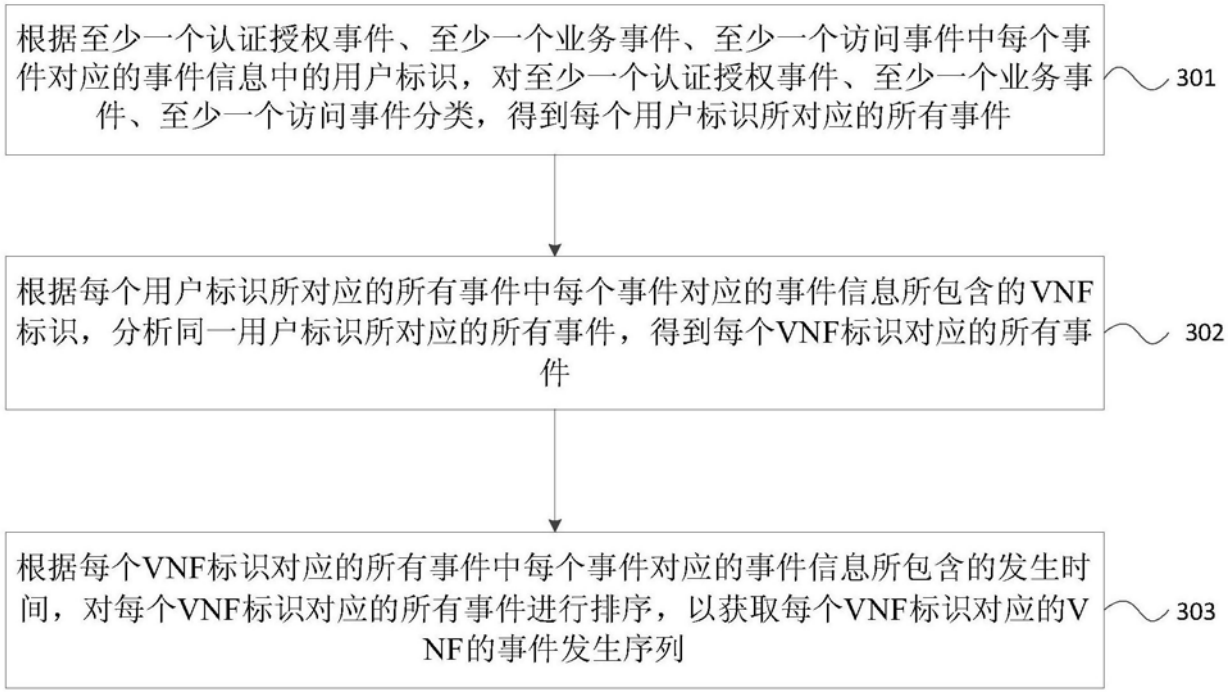

根据至少一个认证授权事件、至少一个业务事件、至少一个访问事件中每个事件对应的事件信息中的用户标识，对至少一个认证授权事件、至少一个业务事件、至少一个访问事件分类，得到每个用户标识所对应的所有事件
301
根据每个用户标识所对应的所有事件中每个事件对应的事件信息所包含的VNF标识，分析同一用户标识所对应的所有事件，得到每个VNF标识对应的所有事件
302
根据每个VNF标识对应的所有事件中每个事件对应的事件信息所包含的发生时间，对每个VNF标识对应的所有事件进行排序，以获取每个VNF标识对应的VNF的事件发生序列
303

图3

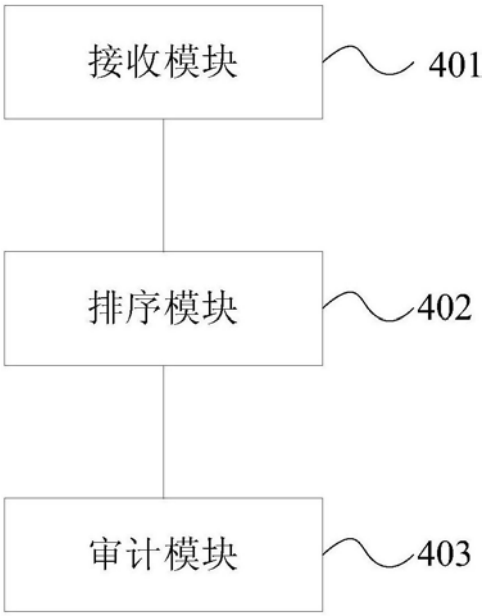


图4