(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 113206814 B
(45)授权公告日 2022.11.18

(21)申请号 202010077699.7
(22)申请日 2020.01.31
(65)同一申请的已公布的文献号
申请公布号 CN 113206814 A
(43)申请公布日 2021.08.03
(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 黄亚达
(74)专利代理机构 北京同达信恒知识产权代理有限公司 11291
专利代理师 落爱青
(51)Int.Cl.
H04W 12/121(2021.01)
H04L 9/40(2022.01)

(56)对比文件
CN 110351229 A,2019.10.18
CN 110312279 A,2019.10.08
US 2019222489 A1,2019.07.18
CN 110602735 A,2019.12.20

审查员 范振坤

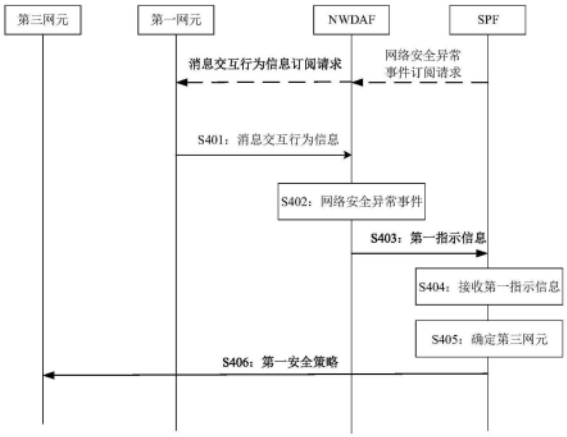
权利要求书5页 说明书29页 附图6页

(54)发明名称

一种网络事件处理方法、装置及可读存储介质

(57)摘要

本申请公开了一种网络事件处理方法、装置及可读存储介质，该方法包括：安全事件处理功能网元接收数据分析网元发送的第一指示信息，第一指示信息用于指示第二网元发生网络安全异常事件；安全事件处理功能网元根据第一指示信息，确定出与第二网元具有关联关系的N个第三网元；针对N个第三网元中的一个第三网元，第三网元具有对第二网元的业务进行处理的能力；针对N个第三网元中的一个第三网元，安全事件处理功能网元向第三网元发送第三网元对应的第一安全策略，第三网元对应的第一安全策略中包括用于指示第三网元停止对第二网元的业务进行处理的指示信息。



CN 113206814 B

1.一种网络事件处理方法,其特征在于,包括:

安全事件处理功能网元接收网络数据分析功能网元发送的第一指示信息,所述第一指示信息用于指示第二核心网网元发生网络安全异常事件;

所述安全事件处理功能网元根据所述第一指示信息,确定出与所述第二核心网网元的业务相关的N个第三核心网网元;所述第三核心网网元具有对所述第二核心网网元的业务进行处理的能力;N为正整数;

所述安全事件处理功能网元向所述N个第三核心网网元中的每个第三核心网网元发送该第三核心网网元对应的第一安全策略,所述第一安全策略用于所述第三核心网网元对所述第二核心网网元对应的业务进行隔离;

其中,所述N个第三核心网网元包括以下的一项或多项:

接入和移动性管理功能网元、消息转发网元、网元发现功能网元、网络路由管理网元、虚拟化资源管理网元、策略控制功能网元。

2.如权利要求1所述的方法,其特征在于,所述第一安全策略用于对所述第二核心网网元对应的业务进行隔离,包括以下的一项或多项:

所述接入和移动性管理功能网元对应的所述第一安全策略用于释放所述第二核心网网元中的用户会话;

所述消息转发网元对应的所述第一安全策略用于停止所述第二核心网网元的消息转发;

所述网元发现功能网元对应的所述第一安全策略用于停止或撤销所述第二核心网网元的用户的授权;

所述网络路由管理网元对应的所述第一安全策略用于停止所述第二核心网网元的网段的消息的路由转发;

所述虚拟化资源管理网元对应的所述第一安全策略用于释放所述第二核心网网元对应的虚拟机。

3.如权利要求1所述的方法,其特征在于,所述第一指示信息还用于指示所述网络安全异常事件对应的异常业务;

所述方法还包括:

所述安全事件处理功能网元根据所述第一指示信息,确定出与所述第二核心网网元相关的M个第四核心网网元;所述第四核心网网元具有对所述异常业务进行处理的能力;M为正整数;

所述安全事件处理功能网元向所述M个第四核心网网元中的每个第四核心网网元发送该第四核心网网元对应的第二安全策略,所述第二安全策略用于所述第四核心网网元停止对所述异常业务进行处理;

其中,所述M个第四核心网网元包括以下的一项或多项:

接入和移动性管理功能网元、消息转发网元、网元发现功能网元、网络路由管理网元、虚拟化资源管理网元、策略控制功能网元。

4.如权利要求3所述的方法,其特征在于,所述第二安全策略用于所述第四核心网网元停止对所述异常业务进行处理,包括以下的一项或多项:

所述接入和移动性管理功能网元对应的所述第二安全策略用于忽略所述异常业务的

请求,或者用于释放所述异常业务对应的用户会话;

所述策略控制功能网元对应的所述第二安全策略用于元释放所述异常业务对应的用户会话;

所述消息转发网元对应的所述第二安全策略用于忽略所述异常业务对应的消息转发;

所述网元发现功能网元对应的所述第二安全策略用于停止或撤销对所述异常业务的用户的授权;

所述网络路由管理网元对应的所述第二安全策略用于忽略对所述异常业务的网段的消息的路由转发。

5.一种网络事件处理方法,其特征在于,包括:

网络数据分析功能网元获取K个第一核心网网元的消息交互行为信息,所述消息交互行为信息包括用于指示所述第一核心网网元传输的消息的属性信息,所述第一核心网网元传输的消息包括所述第一核心网网元与第二核心网网元之间传输的消息;所述K为正整数;

所述网络数据分析功能网元根据所述K个第一核心网网元的消息交互行为信息,确定出所述第二核心网网元发生网络安全异常事件;

所述网络数据分析功能网元向安全事件处理功能网元发送第一指示信息,所述第一指示信息用于指示所述第二核心网网元发生所述网络安全异常事件;

所述第一指示信息指示所述安全事件处理功能网元向N个第三核心网网元中的每个第三核心网网元发送该第三核心网网元对应的第一安全策略,所述第一安全策略用于所述第三核心网网元对所述第二核心网网元对应的业务进行隔离;

其中,所述N个第三核心网网元包括以下的一项或多项:

接入和移动性管理功能网元、消息转发网元、网元发现功能网元、网络路由管理网元、虚拟化资源管理网元、策略控制功能网元。

6.如权利要求5所述的方法,其特征在于,所述第一核心网网元传输的消息的属性信息包括以下一项或多项:

所述消息的类型、所述消息的消息内容、所述第一核心网网元上传输所述消息的接口、所述消息对应的对端传输所述消息的接口。

7.如权利要求5所述的方法,其特征在于,所述网络数据分析功能网元根据所述K个第一核心网网元的消息交互行为信息,确定出所述第二核心网网元发生网络安全异常事件,包括:

所述网络数据分析功能网元若确定所述第一核心网网元接收到来自第二核心网网元的消息的数量大于第一阈值,则确定存在所述第二核心网网元对所述第一核心网网元的分布式拒绝服务攻击事件;所述第一阈值为根据历史消息频率确定的。

8.如权利要求5所述的方法,其特征在于,所述K个第一核心网网元的消息交互行为信息包括:第一消息和第二消息;

所述网络数据分析功能网元根据所述K个第一核心网网元的消息交互行为信息,确定出所述第二核心网网元发生网络安全异常事件,包括:

所述网络数据分析功能网元若确定所述第一消息中的所述第二核心网网元的第一身份标识与所述第二消息中所述第二核心网网元的第二身份标识不一致,则确定所述第二核心网网元存在网络安全异常事件。

9.如权利要求5所述的方法,其特征在于,所述K个第一核心网网元的消息交互行为信息包括:来自所述K个第一核心网网元的第一终端设备的交互行为消息;

所述网络数据分析功能网元根据所述K个第一核心网网元的消息交互行为信息,确定出所述第二核心网网元发生网络安全异常事件,包括:

所述网络数据分析功能网元若确定所述第一终端设备的交互行为消息不一致,则确定所述第一终端设备存在网络安全异常事件。

10.如权利要求5所述的方法,其特征在于,所述K个第一核心网网元的消息交互行为信息包括:来自所述K个第一核心网网元的第二终端设备的交互行为消息和来自所述第二核心网网元的所述第二终端设备的用户信息查询请求;

所述网络数据分析功能网元根据所述K个第一核心网网元的消息交互行为信息,确定出所述第二核心网网元发生网络安全异常事件,包括:

所述网络数据分析功能网元若确定来自所述第二核心网网元的所述第二终端设备的用户信息查询请求中所述第二核心网网元的网元标识不一致,则确定所述网元标识不一致对应的至少两个核心网网元发生网络安全异常事件。

11.一种网络事件处理装置,其特征在于,包括:

收发器,用于接收网络数据分析功能网元发送的第一指示信息;所述第一指示信息用于指示第二核心网网元发生网络安全异常事件;

处理器,用于根据所述第一指示信息,确定出与所述第二核心网网元的业务相关的N个第三核心网网元;所述第三核心网网元具有对所述第二核心网网元的业务进行处理的能力;N为正整数;

所述收发器,还用于向N个第三核心网网元中的每个第三核心网网元发送该第三核心网网元对应的第一安全策略,所述第一安全策略用于所述第三核心网网元对所述第二核心网网元的业务进行隔离;

其中,所述N个第三核心网网元包括以下的一项或多项:

接入和移动性管理功能网元、消息转发网元、网元发现功能网元、网络路由管理网元、虚拟化资源管理网元、策略控制功能网元。

12.如权利要求11所述的装置,其特征在于,所述第一安全策略用于对所述第二核心网网元的业务进行隔离,包括以下的一项或多项:

所述接入和移动性管理功能网元对应的所述第一安全策略用于释放所述第二核心网网元的用户会话;

所述消息转发网元对应的所述第一安全策略用于停止所述第二核心网网元的消息转发;

所述网元发现功能网元对应的所述第一安全策略用于停止或撤销所述第二核心网网元的用户的授权;

所述网络路由管理网元对应的所述第一安全策略用于停止所述第二核心网网元的网段的消息的路由转发;

所述虚拟化资源管理网元对应的所述第一安全策略用于释放所述第二核心网网元对应的虚拟机。

13.如权利要求11所述的装置,其特征在于,所述第一指示信息还用于指示所述网络安

全异常事件对应的异常业务；

所述处理器，具体用于根据所述第一指示信息，确定出与所述第二核心网网元相关的M个第四核心网网元；所述第四核心网网元具有对所述异常业务进行处理的能力；

所述收发器，用于向所述M个第四核心网网元中的每个第四核心网网元发送该第四核心网网元对应的第二安全策略，所述第二安全策略用于停止对所述异常业务进行处理。

14.如权利要求13所述的装置，其特征在于，所述第二安全策略用于所述第四核心网网元停止对所述异常业务进行处理，包括以下的一项或多项：

所述接入和移动性管理功能网元对应的所述第二安全策略用于忽略所述异常业务的请求，或者用于释放所述异常业务对应的用户会话；

所述策略控制功能网元对应的所述第二安全策略用于释放所述异常业务对应的用户会话；

所述消息转发网元对应的所述第二安全策略用于忽略所述异常业务对应的消息转发；

所述网元发现功能网元对应的所述第二安全策略用于停止或撤销对所述异常业务的用户的授权；

所述网络路由管理网元对应的所述第二安全策略用于忽略对所述异常业务的网段的消息的路由转发。

15.一种网络事件处理装置，其特征在于，包括：

收发器，用于获取K个第一核心网网元的消息交互行为信息，所述消息交互行为信息包括用于指示所述第一核心网网元传输的消息的属性信息；所述第一核心网网元传输的消息包括所述第一核心网网元与第二核心网网元之间传输的消息所述K为正整数；

处理器，用于根据所述K个第一核心网网元的消息交互行为信息，确定出所述第二核心网网元发生网络安全异常事件；

所述收发器，向安全事件处理功能网元发送第一指示信息，所述第一指示信息用于指示所述第二核心网网元发生所述网络安全异常事件；

所述第一指示信息指示所述安全事件处理功能网元向N个第三核心网网元中的每个第三核心网网元发送该第三核心网网元对应的第一安全策略，所述第一安全策略用于所述第三核心网网元对所述第二核心网网元对应的业务进行隔离；

其中，所述N个第三核心网网元包括以下的一项或多项：

接入和移动性管理功能网元、消息转发网元、网元发现功能网元、网络路由管理网元、虚拟化资源管理网元、策略控制功能网元。

16.如权利要求15所述的装置，其特征在于，所述第一核心网网元传输的消息的属性信息包括以下一项或多项：

所述消息的类型、所述消息的消息内容、所述第一核心网网元上传输所述消息的接口、所述消息对应的对端传输所述消息的接口。

17.如权利要求15所述的装置，其特征在于，所述处理器，具体用于：

若确定所述第一核心网网元接收到来自第二核心网网元的消息的数量大于第一阈值，则确定存在所述第二核心网网元对所述第一核心网网元的分布式拒绝服务攻击事件；所述第一阈值为根据历史消息频率确定的。

18.如权利要求15所述的装置，其特征在于，所述K个第一核心网网元的消息交互行为

信息包括:第一消息和第二消息;

所述处理器,具体用于:若确定所述第一消息中的所述第二核心网网元的第一身份标识与所述第二消息中所述第二核心网网元的第二身份标识不一致,则确定所述第二核心网网元存在网络安全异常事件。

19.如权利要求15所述的装置,其特征在于,所述K个第一核心网网元的消息交互行为信息包括:来自所述K个第一核心网网元的第一终端设备的交互行为消息;

所述处理器,具体用于:

若确定所述第一终端设备的交互行为消息不一致,则确定所述第一终端设备存在网络安全异常事件。

20.如权利要求15所述的装置,其特征在于,所述K个第一核心网网元的消息交互行为信息包括:来自所述K个第一核心网网元的第二终端设备的交互行为消息和来自所述第二核心网网元的所述第二终端设备的用户信息查询请求;

所述处理器,具体用于:

若确定来自所述第二核心网网元的所述第二终端设备的用户信息查询请求中所述第二核心网网元的网元标识不一致,则确定所述网元标识不一致对应的至少两个核心网网元发生网络安全异常事件。

21.一种通信装置,其特征在于,所述装置包括处理器和通信接口,

所述通信接口,用于输入和/或输出信息;

所述处理器,用于执行计算机程序或指令,使得权利要求1-10中任一项所述的方法被执行。

22.一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存储有计算机可执行指令,所述计算机可执行指令在被计算机调用时,使所述计算机执行如权利要求1至10任一项所述的方法。

一种网络事件处理方法、装置及可读存储介质

技术领域

[0001] 本申请涉及移动通信技术领域，尤其涉及一种网络事件处理方法、装置及可读存储介质。

背景技术

[0002] 随着第五代移动通信技术(5th generation mobile networks,5G)应用到垂直行业的业务，包括医疗健康、智能家具和智能交通等，5G核心网由于引入的很多IT技术，如虚拟化平台，容器平台，越来越多的开源第三方IT组件的应用，再加上多方供应商的共同参与组网，5G网络承载的业务价值越来越高，将会吸引越来越专业的黑客或国家级网络部队对5G网络发起渗透、潜伏和攻击。

[0003] 第三代合作伙伴计划(3rd generation partnership project,3GPP)规范，在5G网络架构中的网络数据分析功能(NetWork Data Analysis Function,NWDAF)网元可以进行网络数据分析。网络数据分析功能可以从网络功能网元(network function,NF)网元以及操作管理维护(Operation,Administration,and Maintenance,OAM)系统获取数据，经过分析处理，将结果提供给NF网元、应用功能(application function,AF)使用。

[0004] 目前通过NWDAF网元进行网络安全的分析只包括对异常用户识别分析服务，例如，NWDAF网元收到第一网元订阅异常用户的识别服务，NWDAF网元可以根据该订阅，向对应的网元，例如，接入与移动性管理功能(access and mobility management function,AMF)网元和会话管理功能(session management function,SMF)网元等，采集用户的会话消息和计费消息等信息，进而NWDAF网元可以根据采集的用户的会话消息和计费消息，确定是否有异常用户。在确定有异常用户时，NWDAF网元可以向订阅异常用户的第一网元发送异常用户的通知消息，进而第一网元可以根据该通知消息对异常用户进行处理。

[0005] 但是，上述方法中，仅能分析出用户发生异常的事件，且也仅是针对订阅异常用户的网元进行异常用户的通知，可以看出，现有针对网络异常事件的处理方案较为单一，网络安全性较差。

发明内容

[0006] 本申请实施例提供一种网络事件处理方法及装置、可读存储介质，用以当第二网元发生网络异常事件，则确定第二网元相关的N个第三网元，以使N个第三网元对第二网元对应的业务进行隔离处理，如此，可以对网络异常事件所关联网元均进行处理，从而对网络的安全隐患进行更全面的处理，从而可以提高网络的安全性。

[0007] 本申请中的第一网元可以核心网网元，第二网元可以包括第二核心网网元，第三网元可以包括第三核心网网元，第四网元可以包括第四核心网网元。

[0008] 第一方面，本申请实施例提供一种网络事件处理方法，包括：安全事件处理功能网元接收网络数据分析功能网元发送的第一指示信息，所述第一指示信息用于指示所述第二网元发生网络安全异常事件；所述安全事件处理功能网元根据所述第一指示信息，确定出

与所述第二网元具有关联关系的N个第三网元;针对所述N个第三网元中的一个第三网元,所述第三网元具有对所述第二网元的业务进行处理的能力;针对所述N个第三网元中的一个第三网元,所述安全事件处理功能网元向所述第三网元发送所述第三网元对应的第一安全策略,所述第三网元对应的第一安全策略中包括用于指示所述第三网元对所述第二网元对应的业务进行隔离的指示信息。

[0009] 通过上述方法,安全事件处理功能网元获取网络数据分析功能网元发送的网络安全异常事件,确认第二网元发送安全异常,进而安全事件处理功能网元根据第二网元,确认与第二网元具有关联关系的第三网元,例如,可以为与第二网元发生信令交互的网元,也可以是为第二网元提供服务的网元,通过向第三网元发送对应的第一安全策略,使得第三网元对第二网元的相关业务进行隔离,相比现有技术仅发送给订阅安全事件的网元的处理方式,可以更加全面的隔离第二网元产生的网络异常事件对网络的影响,进而提高网络的安全性。

[0010] 在一种可能的实现方式中,所述第三网元为所述安全事件处理功能网元向所述第三网元发送所述第三网元对应的第一安全策略,包括所述安全事件处理功能网元向所述AMF网元发送所述接入与移动性管理功能网元对应的第一安全策略,所述接入与移动性管理功能网元对应的第一安全策略包括用于指示所述接入与移动性管理功能网元对所述第二网元对应的业务进行隔离的指示信息。接入与移动性管理功能网元对所述第二网元对应的业务进行隔离具体可以是指接入与移动性管理功能网元不再对第二网元发来的消息进行处理,从而可以避免接入与移动性管理功能网元对发生网络安全异常事件的第二网元的消息进行处理所导致的网络安全事件的发生,可以进一步提高网络安全性。

[0011] 在一种可能的实现方式中,所述安全事件处理功能网元向所述第三网元发送所述第三网元对应的第一安全策略,包括,所述安全事件处理功能网元向消息转发网元发送所述消息转发网元对应的第一安全策略,所述消息转发网元对应的第一安全策略包括用于指示所述消息转发网元停止对所述第二网元的消息转发的指示信息。进而,可以使得消息转发网元不再对第二网元的消息进行转发,从而可以避免消息转发网元对发生网络安全异常事件的第二网元的消息进行转发所导致第二网元的网络安全事件的扩散,可以进一步提高网络安全性。

[0012] 在一种可能的实现方式中,所述安全事件处理功能网元向所述第三网元发送所述第三网元对应的第一安全策略,包括所述安全事件处理功能网元向所述网络仓库功能(network function repository function,NRF)网元发送所述NRF网元对应的第一安全策略,所述NRF网元对应的第一安全策略包括用于指示所述NRF网元不再对所述第二网元的用户授权指示信息,和/或,撤销所述第二网元的用户的授权指示信息;进而,可以使得NRF网元停止或撤销对第二网元的用户授权,从而可以避免第二网元的用户所导致第二网元的网络安全事件的发生,可以进一步提高网络安全性。

[0013] 在一种可能的实现方式中,所述安全事件处理功能网元向所述第三网元发送所述第三网元对应的第一安全策略,包括,所述安全事件处理功能网元向所述路由传输控制器发送所述路由传输控制器对应的第一安全策略,所述路由传输控制器对应的第一安全策略包括用于指示所述路由传输控制器网元忽略对所述第二网元的网段的消息的路由转发请求的指示信息;进而,可以使得路由传输控制器停止对第二网元的网段的消息的路由转发,

从而可以避免路由传输控制器对发生网络安全事件的第二网元的消息的路由转发所导致第二网元的网络安全事件的发生,可以进一步提高网络安全性。

[0014] 在一种可能的实现方式中,所述安全事件处理功能网元向所述第三网元发送所述第三网元对应的第一安全策略,包括所述安全事件处理功能网元向所述虚拟化资源管理网元发送所述虚拟化资源管理网元对应的第一安全策略,所述虚拟化资源管理网元对应的第一安全策略包括用于指示所述虚拟化资源管理网元释放所述第二网元对应的虚拟机的指示信息。进而,可以使得虚拟化资源管理网元释放第二网元对应的虚拟机,从而可以停止第二网元的虚拟机的运行,以避免第二网元的网络安全事件的发生,可以进一步提高网络安全性。

[0015] 在一种可能的实现方式中,所述安全事件处理功能网元向所述第三网元发送所述第三网元对应的第一安全策略,包括所述安全事件处理功能网元向所述接入与移动性管理功能网元发送所述接入与移动性管理功能网元对应的第一安全策略,所述接入与移动性管理功能网元对应的第一安全策略包括用于指示所述接入与移动性管理功能网元释放所述第二网元所绑定的用户的指示信息。进而,可以使得接入与移动性管理功能网元释放第二网元的用户,从而可以避免第二网元的用户所导致第二网元的网络安全事件的发生,可以进一步提高网络安全性。

[0016] 一种可能的设计,所述第一指示信息还用于指示所述网络安全异常事件对应的异常业务;所述安全事件处理功能网元根据所述第一指示信息,确定出与所述第二网元具有关联关系的M个第四网元;针对所述M个第四网元中的一个第四网元,所述第四网元具有对所述异常业务进行处理的能力;所述安全事件处理功能网元向所述第四网元发送所述第四网元对应的第二安全策略,所述第四网元对应的第二安全策略中包括用于指示所述第四网元停止或撤销对所述异常业务进行处理的指示信息。

[0017] 上述方法中,通过网络安全异常事件对应的异常业务,确定异常业务涉及的第四网元,进而向第四网元发送对应的第二安全策略,使得第四网元对第二网元涉及的异常业务进行有效隔离,减少异常网元产生的异常业务对网络性能的影响。

[0018] 在一种可能的实现方式中,所述安全事件处理功能网元向所述第四网元发送所述第四网元对应的第二安全策略,包括所述安全事件处理功能网元向所述接入与移动性管理功能网元发送所述接入与移动性管理功能网元对应的第二安全策略,所述接入与移动性管理功能网元对应的第二安全策略包括用于指示所述第四网元对所述第二网元的异常业务进行隔离的指示信息;如此可以使接入与移动性管理功能网元不再对第二网元的异常业务进行处理,从而可以避免接入与移动性管理功能网元对发生网络安全异常事件的第二网元的异常业务进行处理所导致的网络安全事件的发生,可以进一步提高网络安全性。

[0019] 在一种可能的实现方式中,所述安全事件处理功能网元向所述第四网元发送所述第四网元对应的第二安全策略,包括所述安全事件处理功能网元向所述接入与移动性管理功能网元发送所述接入与移动性管理功能网元对应的第二安全策略,所述接入与移动性管理功能网元对应的第二安全策略包括用于指示所述接入与移动性管理功能网元释放所述异常业务对应的用户的指示信息;如此可以使接入与移动性管理功能网元释放第二网元的异常业务对应的用户,从而可以避免第二网元的异常业务对应的用户所导致的网络安全事件的发生,可以进一步提高网络安全性。

[0020] 在一种可能的实现方式中,所述安全事件处理功能网元向所述第四网元发送所述第四网元对应的第二安全策略,包括所述安全事件处理功能网元向所述策略控制功能(policy control function,PCF)网元发送所述PCF网元对应的第二安全策略,所述PCF网元对应的第二安全策略包括用于指示所述PCF网元释放所述异常业务对应的用户的指示信息;如此可以使PCF网元释放第二网元的异常业务对应的用户,从而可以避免第二网元的异常业务对应的用户所导致的网络安全事件的发生,可以进一步提高网络安全性。

[0021] 在一种可能的实现方式中,所述安全事件处理功能网元向所述第四网元发送所述第四网元对应的第二安全策略,包括所述安全事件处理功能网元向所述消息转发网元发送所述消息转发网元对应的第二安全策略,所述消息转发网元对应的第二安全策略包括用于指示所述消息转发网元忽略对所述第二网元的异常业务的消息转发请求的指示信息;进而,可以使得消息转发网元忽略对第二网元的异常业务的消息转发请求的指示信息,从而可以避免消息转发网元对发生网络安全事件的第二网元的异常业务的消息的转发所导致异常业务的网络安全事件的发生,可以进一步提高网络安全性。

[0022] 在一种可能的实现方式中,所述安全事件处理功能网元向所述第四网元发送所述第四网元对应的第二安全策略,包括所述安全事件处理功能网元向所述NRF网元发送所述NRF网元对应的第二安全策略,所述NRF网元对应的第二安全策略包括用于指示所述NRF网元停止或撤销对所述第二网元的异常业务的用户授权的指示信息;如此可以使NRF网元停止或释放第二网元的异常业务对应的用户的授权,从而可以避免第二网元的异常业务对应的用户所导致的网络安全事件的发生,可以进一步提高网络安全性。

[0023] 在一种可能的实现方式中,所述安全事件处理功能网元向所述第四网元发送所述第四网元对应的第二安全策略,包括所述安全事件处理功能网元向所述路由传输控制器发送所述路由传输控制器对应的第二安全策略,所述路由传输控制器对应的第二安全策略包括用于指示所述路由传输控制器忽略对所述第二网元的网段的消息的路由转发请求的指示信息。进而,可以使得路由传输控制器忽略对第二网元的异常业务的消息路由转发请求的指示信息,从而可以避免路由传输控制器对发生网络安全事件的第二网元的异常业务的消息的路由转发所导致异常业务的网络安全事件的发生,可以进一步提高网络安全性。

[0024] 第二方面,本申请提供一种网络事件处理方法,网络数据分析功能网元获取K个第一网元的消息交互行为信息,针对所述K个第一网元中的一个第一网元,所述第一网元的消息交互行为信息包括用于指示所述第一网元传输的消息的属性信息;所述K为正整数;所述网络数据分析功能网元根据所述K个第一网元的消息交互行为信息,确定出第二网元发生网络安全异常事件;所述网络数据分析功能网元向安全事件处理功能网元发送第一指示信息,所述第一指示信息用于指示所述第二网元发生所述网络安全异常事件。

[0025] 相比现有技术,通过增加K个第一网元的消息交互行为信息的获取服务,使得NDWAF网元可以获取各网元的消息交互行为信息,进而通过对第一网元传输的消息的属性信息进行分析,确定出第二网元发生网络安全异常事件,相比现有技术中只能识别用户的异常行为,本申请实施例的方法中可以获取网元的网络安全异常事件,进而有效的发现现有技术中无法发现的网络安全异常的情况,以提高网络的安全性。

[0026] 一种可能的设计,针对所述K个第一网元中的一个第一网元,所述第一网元传输的消息的属性信息,包括以下一项或多项:所述消息的类型、所述消息的消息内容、所述第一

网元上传输所述消息的接口、所述消息对应的对端传输所述消息的接口。进而，第一网元向网络数据分析功能网元传输的消息的属性信息可以包括网元间交互时产生的消息对应的相关信息，进而，网络数据分析功能网元可以根据网元间交互时产生的消息对应的相关信息，对网元间是否发送网络安全异常事件作出判断，以有效的识别出是否发生网络安全异常事件。

[0027] 一种可能的设计，所述数据分析网元若确定所述第一网元接收到来自第二网元的消息的数量大于第一阈值，则确定存在所述第二网元对所述第一网元的分布式拒绝服务(distributed denial of service,DDoS)攻击事件；所述第一阈值为根据历史消息频率确定的。

[0028] 通过上述方法，网络数据分析功能网元根据第一网元接收到的第二网元的消息的数量，确定发生异常，进而可以确定出第二网元为异常网元，以及识别出第二网元发生DDoS攻击事件，从而可以指示SPF针对第二网元发生的DDoS攻击的网络安全异常事件进行对应的处理，从而提高网络安全性。

[0029] 一种可能的设计，所述K个第一网元的消息交互行为信息包括：第一消息和第二消息；所述数据分析网元若确定所述第一消息中的第二网元的第一身份标识与所述第二消息中所述第二网元的第二身份标识不一致，则确定所述第二网元存在网络安全异常事件。进而，网络数据分析功能网元根据不同消息中携带的第二网元的身份标识不一致，可以确定第二网元存在网络安全异常事件，从而可以指示SPF针对第二网元携带的第二网元的身份标识不一致的网络安全异常事件进行对应的处理，从而提高网络安全性。

[0030] 一种可能的设计，所述K个第一网元的消息交互行为信息包括：来自所述K个第一网元的第一终端设备(user equipment,UE)的交互行为消息；所述数据分析网元若确定来自第二网元的所述第一UE的交互行为消息不一致，则确定来自第二网元的所述第一UE存在网络安全异常事件。进而，网络数据分析功能网元根据不同消息中第一UE相关的交互行为消息中存在无法对应的消息，可以确定第一UE存在网络安全异常事件，另外由于第一UE的交互行为消息来自于第二网元，进而可以确定第二网元存在网络安全异常事件，从而可以指示SPF针对第二网元的第一UE的交互行为消息不一致的网络安全异常事件进行对应的处理，从而提高网络安全性。

[0031] 一种可能的设计，所述K个第一网元的消息交互行为信息包括：来自所述K个第一网元的第二UE的交互行为消息和来自第二网元的所述第二UE的用户信息查询请求；所述数据分析网元若确定来自第二网元的所述第二UE的用户信息查询请求中，所述第二网元中的网元标识不一致，则确定所述网元标识不一致对应的至少两个网元发生网络安全异常事件。网络数据分析功能网元根据不同消息中相同UE涉及的网元的网元标识不一致，确定涉及的网元存在网络安全异常事件，从而可以指示SPF针对涉及的网元的网元标识不一致的网络安全异常事件进行对应的处理，从而提高网络安全性。

[0032] 第三方面，提供了一种通信装置用于实现上述各种方法。该通信装置可以为上述第一方面中的安全事件处理功能网元，或者包含上述安全事件处理功能网元的装置；或者，该通信装置可以为上述第二方面中的网络数据分析功能网元，或者包含上述网络数据分析功能网元的装置。该通信装置包括实现上述方法相应的模块、单元、或手段(means)，该模块、单元、或means可以通过硬件实现，软件实现，或者通过硬件执行相应的软件实现。该硬

件或软件包括一个或多个与上述功能相对应的模块或单元。

[0033] 第六方面，提供了一种通信装置，包括：处理器和存储器；该存储器用于存储计算机指令，当该处理器执行该指令时，以使该通信装置执行上述任一方面所述的方法。该通信装置可以为上述第一方面中的安全事件处理功能网元，或者包含上述安全事件处理功能网元的装置；或者，该通信装置可以为上述第二方面中的网络数据分析功能网元，或者包含上述网络数据分析功能网元的装置。

[0034] 第七方面，提供了一种通信装置，包括：处理器；该处理器用于与存储器耦合，并读取存储器中的指令之后，根据该指令执行如上述任一方面所述的方法。该通信装置可以为上述第一方面中的安全事件处理功能网元，或者包含上述安全事件处理功能网元的装置；或者，该通信装置可以为上述第二方面中的网络数据分析功能网元，或者包含上述网络数据分析功能网元的装置。

[0035] 第八方面，提供了一种计算机可读存储介质，该计算机可读存储介质中存储有指令，当其在计算机上运行时，使得计算机可以执行上述任一方面所述的方法。

[0036] 第九方面，提供了一种包含指令的计算机程序产品，当其在计算机上运行时，使得计算机可以执行上述任一方面所述的方法。

[0037] 第十方面，提供了一种通信装置(例如，该通信装置可以是芯片或芯片系统)，该通信装置包括处理器，用于实现上述任一方面中所涉及的功能。在一种可能的设计中，该通信装置还包括存储器，该存储器，用于保存必要的程序指令和数据。该通信装置是芯片系统时，可以由芯片构成，也可以包含芯片和其他分立器件。

[0038] 其中，第五方面至第十方面中任一种设计方式所带来的技术效果可参见上述第一方面或第二方面中不同设计方式所带来的技术效果，此处不再赘述。

[0039] 第十一方面，提供了一种通信系统，该通信系统包括：安全事件处理功能网元接收网络数据分析功能网元发送的第一指示信息，所述第一指示信息用于指示所述第二网元发生网络安全异常事件；所述安全事件处理功能网元根据所述第一指示信息，确定出与所述第二网元具有关联关系的N个第三网元；针对所述N个第三网元中的一个第三网元，所述第三网元具有对所述第二网元的业务进行处理的能力；针对所述N个第三网元中的一个第三网元，所述安全事件处理功能网元向所述第三网元发送所述第三网元对应的第一安全策略，所述第三网元对应的第一安全策略中包括用于指示所述第三网元对所述第二网元对应的业务进行隔离的指示信息。网络数据分析功能网元获取K个第一网元的消息交互行为信息，针对所述K个第一网元中的一个第一网元，所述第一网元的消息交互行为信息包括用于指示所述第一网元传输的消息的属性信息；所述K为正整数；所述网络数据分析功能网元根据所述K个第一网元的消息交互行为信息，确定出第二网元发生网络安全异常事件；所述网络数据分析功能网元向安全事件处理功能网元发送第一指示信息，所述第一指示信息用于指示所述第二网元发生所述网络安全异常事件。其中，第十一方面所带来的技术效果可参见上述第一方面或第二方面中所带来的技术效果，此处不再赘述。

附图说明

[0040] 图1为本申请提供的一种网络架构示意图；

[0041] 图2为基于服务化架构的5G网络架构示意图；

[0042] 图3为基于点对点接口的5G网络架构示意图；

[0043] 图4为本申请提供的一种网络事件处理方法流程示意图；

[0044] 图5为本申请提供的一种网络事件处理方法流程示意图；

[0045] 图6为本申请提供的一种网络事件处理方法流程示意图；

[0046] 图7为本申请提供的一种网络事件处理方法流程示意图；

[0047] 图8为本申请提供的一种网络事件处理装置示意图；

[0048] 图9为本申请提供的一种网络事件处理装置示意图。

具体实施方式

[0049] 图1示例性示出了本申请实施例提供的一种通信系统10。如图1所示，该通信系统10包括网络数据分析功能网元101和安全事件处理功能网元102。该网络数据分析功能网元101和安全事件处理功能(security policy function,SPF)网元102之间可以直接通信，也可以通过其他设备的转发进行通信，本申请实施例对此不做具体限定。

[0050] 如图1所示，网络数据分析功能网元101，用于获取K个第一网元的消息交互行为信息，针对所述K个第一网元中的一个第一网元，所述第一网元的消息交互行为信息包括用于指示所述第一网元传输的消息的属性信息；所述K为正整数；所述网络数据分析功能网元根据所述K个第一网元的消息交互行为信息，确定出第二网元发生网络安全异常事件；所述网络数据分析功能网元向SPF网元发送第一指示信息，所述第一指示信息用于指示所述第二网元发生所述网络安全异常事件。

[0051] 安全事件处理功能网元102，用于接收网络数据分析功能网元发送的第一指示信息，所述第一指示信息用于指示所述第二网元发生网络安全异常事件；所述SPF网元根据所述第一指示信息，确定出与所述第二网元具有关联关系的N个第三网元；针对所述N个第三网元中的一个第三网元，所述第三网元具有对所述第二网元的业务进行处理的能力；针对所述N个第三网元中的一个第三网元，所述SPF网元向所述第三网元发送所述第三网元对应的第一安全策略，所述第三网元对应的第一安全策略中包括用于指示所述第三网元对所述第二网元对应的业务进行隔离的指示信息。

[0052] 其中，上述方案的具体实现将在后续方法实施例中详细阐述，在此不予赘述。

[0053] 基于本申请实施例提供的通信系统，相比现有技术，通过增加K个第一网元的消息交互行为信息的获取服务，使得网络数据分析功能网元可以获取各网元的消息交互行为信息，进而通过对第一网元传输的消息的属性信息进行分析，确定出第二网元发生网络安全异常事件，相比现有技术中只能识别用户的异常行为，本申请实施例的方法中可以获取网元的网络安全异常事件，进而有效的发现现有技术中无法发现的网络安全异常的情况，安全事件处理功能网元获取网络数据分析功能网元101发送的网络安全异常事件，确认第二网元发送安全异常，进而安全事件处理功能网元根据第二网元，确认与第二网元具有关联关系的第三网元，例如，可以为与第二网元发生信令交互的网元，也可以是为第二网元提供服务的网元，通过向第三网元发送对应的第一安全策略，使得第三网元对第二网元的相关业务进行隔离，相比现有技术仅发送给订阅安全事件的网元的处理方式，可以更加全面的隔离第二网元产生的网络异常事件对网络的影响，进而提高网络的安全性。

[0054] 本申请实施例的系统架构可以应用于5G网络架构，图2和图3示例性示出了本申请

实施例的通信系统10应用于5G网络架构的示意图。下面结合图2和图3,对系统架构中的相关网元进行介绍。

[0055] 终端设备,可以是用于实现无线通信功能的设备,例如终端或者可用于终端中的芯片等。其中,终端可以是5G网络或者未来演进的PLMN中的用户设备(user equipment,UE)、接入终端、终端单元、终端站、移动站、移动台、远方站、远程终端、移动设备、无线通信设备、终端代理或终端装置等。接入终端可以是蜂窝电话、无绳电话、会话启动协议(session initiation protocol,SIP)电话、无线本地环路(wireless local loop,WLL)站、个人数字助理(personal digital assistant,PDA)、具有无线通信功能的手持设备、计算设备或连接到无线调制解调器的其它处理设备、车载设备或可穿戴设备,虚拟现实(virtual reality,VR)终端设备、增强现实(augmented reality,AR)终端设备、工业控制(industrial control)中的无线终端、无人驾驶(self driving)中的无线终端、远程医疗(remote medical)中的无线终端、智能电网(smart grid)中的无线终端、运输安全(transportation safety)中的无线终端、智慧城市(smart city)中的无线终端、智慧家庭(smart home)中的无线终端等。终端可以是移动的,也可以是固定的。

[0056] 上述终端设备可通过运营商网络提供的接口(例如N1等)与运营商网络建立连接,使用运营商网络提供的数据和/或语音等服务。终端设备还可通过运营商网络访问DN,使用DN上部署的运营商业务,和/或第三方提供的业务。其中,上述第三方可为运营商网络和终端设备之外的服务方,可为终端设备提供他数据和/或语音等服务。其中,上述第三方的具体表现形式,具体可根据实际应用场景确定,在此不做限制。

[0057] RAN是运营商网络的子网络,是运营商网络中业务节点与终端设备之间的实施系统。终端设备要接入运营商网络,首先是经过RAN,进而可通过RAN与运营商网络的业务节点连接。本申请中的RAN设备,是一种为终端设备提供无线通信功能的设备,RAN设备也称为接入网设备。本申请中的RAN设备包括但不限于:5G中的下一代基站(gnodeB,gNB)、演进型节点B(evolved node B,eNB)、无线网络控制器(radio network controller,RNC)、节点B(node B,NB)、基站控制器(base station controller,BSC)、基站收发台(base transceiver station,BTS)、家庭基站(例如,home evolved nodeB,或home node B,HNB)、基带单元(baseBand unit,BBU)、传输点(transmitting and receiving point,TRP)、发射点(transmitting point,TP)、移动交换中心等。为方便说明,本申请中将RAN设备简称为RAN。

[0058] 可选的,本申请实施例中的RAN设备指的是接入核心网的设备,例如可以是基站,宽带网络业务网关(broadband network gateway,BNG),汇聚交换机,非第三代合作伙伴计划(3rd generation partnership project,3GPP)接入设备等。基站可以包括各种形式的基站,例如:宏基站,微基站(也称为小站),中继站,接入点等。

[0059] AMF网元,接入和移动性管理功能,主要支持终端的注册管理、连接性管理以及移动性管理等功能,是由运营商网络提供的控制面网元,负责终端设备接入运营商网络的接入控制和移动性管理,例如包括移动状态管理,分配用户临时身份标识,认证和授权用户等功能。

[0060] SMF网元,会话管理功能,主要支持会话建立,修改和释放等功能,此外还负责UE IP地址分配和管理、UPF选择和控制、UPF和AN节点之间的隧道维护业务和会话连续性

(Service and Session Continuity,SSC)模式选择、漫游等会话相关的功能。是由运营商网络提供的控制面网元,负责管理终端设备的协议数据单元(protocol data unit,PDU)会话。PDU会话是一个用于传输PDU的通道,终端设备需要通过PDU会话与DN互相传送PDU。PDU会话由SMF网元负责建立、维护和删除等。

[0061] UPF网元,用户平面功能,主要负责数据报文的分组路由和转发。是由运营商提供的网关,是运营商网络与DN通信的网关。UPF网元包括数据包路由和传输、包检测、业务用量上报、服务质量(Quality of Service,QoS)处理、合法监听、上行包检测、下行数据包存储等用户面相关的功能。

[0062] DN,也可以称为分组数据网络(packet data network,PDN),是位于运营商网络之外的网络,运营商网络可以接入多个DN,DN上可部署多种业务,可为终端设备提供数据和/或语音等服务。例如,DN是某智能工厂的私有网络,智能工厂安装在车间的传感器可为终端设备,DN中部署了传感器的控制服务器,控制服务器可为传感器提供服务。传感器可与控制服务器通信,获取控制服务器的指令,根据指令将采集的传感器数据传送给控制服务器等。又例如,DN是某公司的内部办公网络,该公司员工的手机或者电脑可为终端设备,员工的手机或者电脑可以访问公司内部办公网络上的信息、数据资源等。

[0063] UDM网元,是由运营商提供的控制面网元,负责存储运营商网络中签约用户的用户永久标识符(subscriber permanent identifier,SUPI)、信任状(credential)、安全上下文(security context)、签约数据等信息。UDM网元所存储的这些信息可用于终端设备接入运营商网络的认证和授权。其中,上述运营商网络的签约用户具体可为使用运营商网络提供的业务的用户,例如使用中国电信的手机芯卡的用户,或者使用中国移动的手机芯卡的用户等。上述签约用户的永久签约标识(Subscription Permanent Identifier,SUPI)可为该手机芯卡的号码等。上述签约用户的信任状、安全上下文可为该手机芯卡的加密密钥或者跟该手机芯卡加密相关的信息等存储的小文件,用于认证和/或授权。上述安全上下文可为存储在用户本地终端(例如手机)上的数据(cookie)或者令牌(token)等。上述签约用户的签约数据可为该手机芯卡的配套业务,例如该手机芯卡的流量套餐或者使用网络等。需要说明的是,永久标识符、信任状、安全上下文、认证数据(cookie)、以及令牌等同认证、授权相关的信息,在本发明本申请文件中,为了描述方便起见不做区分、限制。如果不做特殊说明,本申请实施例将以用安全上下文为例进行来描述,但本申请实施例同样适用于其他表述方式的认证、和/或授权信息。

[0064] AUSF网元,认证服务器功能,支持用户的接入认证。是由运营商提供的控制面网元,通常可用于一级认证,即终端设备(签约用户)与运营商网络之间的认证。AUSF网元接收到签约用户发起的认证请求之后,可通过UDM网元中存储的认证信息和/或授权信息对签约用户进行认证和/或授权,或者通过UDM网元生成签约用户的认证和/或授权信息。AUSF网元可向签约用户反馈认证信息和/或授权信息。

[0065] NEF网元,是由运营商提供控制面网元。NEF网元以安全的方式对第三方开放运营商网络的对外接口。在SMF网元需要与第三方的网元通信时,NEF网元可作为SMF网元与第三方的网元通信的中继。NEF网元作为中继时,可作为签约用户的标识信息的翻译,以及第三方的网元的标识信息的翻译。比如,NEF将签约用户的SUPI从运营商网络发送到第三方时,可以将SUPI翻译成其对应的外部身份标识(identity,ID)。反之,NEF网元将外部ID(第三方

的网元ID)发送到运营商网络时,可将其翻译成SUPI。

[0066] 应用功能(Application Function,AF)网元,主要提供应用层服务,还支持与5G核心网交互来提供服务,例如影响数据路由决策,策略控制功能或者向网络侧提供第三方的一些服务。在具体应用中,AF网元一般是指第三方服务器或应用服务器。

[0067] PCF网元,策略控制功能,支持统一的策略框架来管理网络行为。

[0068] 是由运营商提供的控制面功能,用于向网络网元提供策略。作为一种实现方式,策略可以包括接入控制策略、移动性管理策略、计费相关策略、QoS相关策略和授权相关策略等。

[0069] NRF网元,可用于提供网元发现功能,基于其他网元的请求,提供网元类型对应的网元信息,如地址信息和/或标识信息等。NRF网元还提供网元管理服务,如网元注册、更新、去注册以及网元状态订阅和推送等。

[0070] CHF网元,用于提供计费功能,支持用户的离线和在线计费功能。

[0071] NWDAF网元,用于网络数据分析功能。负责安全数据的分析和异常安全事件识别。

[0072] SPF网元,用于安全策略功能,支持网络级安全策略控制,负责安全事件的策略确定和协同。

[0073] 图1中的网络数据分析功能网元101对应的网元或者实体可以为该5G网络架构中的NWDAF网元,图1中的安全事件处理功能网元102所对应的网元或者实体可以为该5G网络架构中的SPF网元。本申请实施例中以网络数据分析功能网元101为NWDAF网元,安全事件处理功能网元102为SPF网元为例进行阐述。

[0074] 本申请实施例中的网络数据分析功能网元或安全事件处理功能网元也可以称之为通信装置,其可以是一个通用设备或者是一个专用设备,本申请实施例对此不做具体限定。本申请实施例中的网络数据分析功能网元或安全事件处理功能网元的相关功能可以由一个设备实现,也可以由多个设备共同实现,还可以是由一个设备内的一个或多个功能模块实现,本申请实施例对此不做具体限定。可以理解的是,上述功能既可以是硬件设备中的网络元件,也可以是在专用硬件上运行的软件功能,或者是硬件与软件的结合,或者是平台(例如,云平台)上实例化的虚拟化功能。本申请中,网络数据分析功能网元是指具备数据收集和分析以及获取数据分析结果功能的网元,其可以是图1或图2中的NWDAF网元,也可以是管理数据分析服务(Management data analysis service,MDAS)网元或者其他具备类似功能的网元。为方便说明,本申请后续以网络数据分析功能网元为5G中的NWDAF网元为例进行说明,且可以将网络数据分析功能网元简称为NWDAF网元。本申请实施例中,NWDAF网元也可以称为网络分析功能、或网络分析功能网元,其具有相同的含义,这里做统一说明。

[0075] 本申请实施例提供一种NWDAF网元的部署方式。其中,NWDAF可以为分布式实现,分布式实体可以部署在5GC NF侧、RAN侧(图中以RAN设备为gNB为例)、UE内部。部署在5GC NF/gNB侧时,可以作为一个软件模块内置在5GC NF/gNB内部。NWDAF的各分布式实体间存在交互接口。为在实际部署中,AMF网元侧和SMF侧的NWDAF部署可以为独立的物理设备、或独立的虚拟设备、或部署在AMF网元/SMF中的软件模块、或者在物理位置或网络位置上接近AMF网元或SMF部署的独立的软件模块。NWDAF可以与5GC NF、gNB、OAM交互获取信息、以及从UE获取信息,将分析结果提供给AF,包括中心侧的AF、以及部署在各边缘移动边缘计算(Mobile Edge Computing,MEC)的分布式AF实体。NWDAF网元可以从NF网元(如图2或图3所

示的SMF、PCF网元、RAN、UPF等)、AF、数据仓库或OAM中的一个或多个获取待分析的数据，然后进行分析并获得数据分析结果。其中，NWDAF网元进行数据分析可以是基于某个消费者网元(比如，消费者网元可以是NF网元、RAN设备、终端设备等)发送的数据分析请求或订阅消息而触发的，或者是数据分析网元根据其他条件触发的，比如周期性地触发、初始事件触发等。数据分析网元在获得数据分析结果之后，可以向请求获取数据分析结果的消费者网元发送数据分析结果，或者将数据分析结果存储于数据仓库，或者存储于数据分析网元中。

[0076] 此外，如图2所示，为基于服务化架构的5G网络架构示意图。其中，该5G网络架构中还可以包括以下网元中的一个或多个：网络开放功能(network exposure function，NEF)网元、PCF网元、统一数据管理(unified data management，UDM)网元、NRF网元、AF网元、NWDAF网元、认证服务器功能(authentication server function，AUSF)网元、AMF网元、SMF网元、(无线)接入网((radio)access network，(R)AN)以及用户面功能(user plane function，UPF)网元等，本申请实施例对此不做具体限定。上述5G网络架构中，除(无线)接入网部分之外的部分可以称为核心网络部分。为方便说明，后续以(R)AN称为RAN为例进行说明。

[0077] 其中，终端设备通过下一代网络(next generation，N)1接口(简称N1)与AMF网元通信，RAN设备通过N2接口(简称N2)与AMF网元通信，RAN设备通过N3接口(简称N3)与UPF网元通信，UPF网元通过N6接口(简称N6)与DN通信，AMF网元通过N11接口(简称N11)与SMF网元通信，AMF网元通过N8接口(简称N8)与UDM网元通信，AMF网元通过N12接口(简称N12)与AUSF网元通信，AMF网元通过N15接口(简称N15)与PCF网元通信，SMF网元通过N7接口(简称N7)与PCF网元通信，SMF网元通过N4接口(简称N4)与UPF网元通信，SMF网元通过N10接口(简称N10)与UDM网元通信，UDM网元通过N13接口(简称N13)与AUSF网元通信，PCF网元通过N5接口(简称N5)与AF网元通信。

[0078] 此外，需要说明的是，图2所示的5G网络架构中的AMF网元、SMF网元、UDM网元、AUSF网元、PCF网元、LSMF网元或者AF网元等控制面网元也可以采用服务化接口进行交互。比如，如图2所示，AMF网元对外提供的服务化接口可以为Namf；SMF网元对外提供的服务化接口可以为Nsmf；UDM网元对外提供的服务化接口可以为Nudm；PCF网元对外提供的服务化接口可以为Npcf，AUSF网元对外提供的服务化接口可以为Nausf，AF网元对外提供的服务化接口可以为Naf。相关描述可以参考23501标准中的5G系统架构(5G system architecture)，在此不予赘述。本申请实施例提供一种SPF网元的部署方式。SPF网元的部署方式可以有多种，其中，SPF网元可以为分布式实现，分布式实体可以部署在5GC NF侧、RAN侧(图中以RAN设备为gNB为例)、UE内部。如图2所示，表示新增NF SPF网元的可能的部署方式，SPF网元可以作为5G心网的标准NF，通过SBA接口和标准定义的5G核心网NF直接进行对接。

[0079] 如图3所示，为基于点对点接口的5G网络架构示意图，其中的网元的功能的介绍可以参考图2中对应的网元的功能的介绍，不再赘述。图3与图2的主要区别在于：图2中的各个网元之间的接口是点对点的接口，而不是服务化的接口。

[0080] 在图3所示的架构中，终端设备通过N1接口(简称N1)与AMF网元通信，RAN设备通过N2接口(简称N2)与AMF网元通信，RAN设备通过N3接口(简称N3)与UPF网元通信，UPF网元通过N6接口(简称N6)与DN通信，AMF网元通过N11接口(简称N11)与SMF网元通信，AMF网元通过N8接口(简称N8)与UDM网元通信，AMF网元通过N12接口(简称N12)与AUSF网元通信，AMF网元

通过N15接口(简称N15)与vPCF网元通信;SMF网元通过N7接口(简称N7)与vPCF网元通信,vPCF网元通过N24接口(简称N24)与hPCF网元通信,vPCF网元通过N5接口(简称N5)与AF网元通信,SMF网元通过N4接口(简称N4)与UPF网元通信,SMF网元通过N10接口(简称N10)与UDM网元通信,UDM网元通过N13接口(简称N13)与AUSF网元通信。

[0081] 本申请实施例还提供一种SPF网元的部署方式,如图3所示,SPF网元可以作为管理面功能,通过管理面接口,间接和5G核心网NF进行对接。如图3所示,与安全策略SPF网元之对接的NF可以有很多,随着网络功能的演进可以扩展。举例来说,与安全策略SPF网元之对接的NF可以包括:处理UE信令相关的AMF网元/SMF网元;处理UE策略和签约数据相关的PCF网元/UDM;处理核心网NF间通讯的NRF网元/SCF网元;还可以和核心网NF网元外的相关功能领域对接入如虚拟化资源管理网元和路由传输控制器(software defined network,SDN)网元,从而在更广的功能领域中对安全事件进行响应。下面以图3的逻辑连接图进行举例说明,在具体实施过程中,SPF网元可以是图3通过SBA接口直接对接,也可以为图3通过管理面接口间接对接,在此不做限定。需要说明的是,该图仅给出了一种实现方式,实际应用中也可以有其他部署方式,比如部署一个NWDAF网元和一个SPF网元,或者,将SPF网元部署在NWDAF网元中(比如部署在中心位置)。

[0082] 本申请中的NF网元可以是图2或图3中的核心网网元,即5G核心网(5G Core Network,5GC)NFs,或者还可以是未来通信系统,如第六代(6th generation,6G)中的核心网网元,即6GC NFs。为方便说明,本申请实施例以NF为5GC NFs为例进行说明。需要说明的是,本申请实施例后续描述时,可以将NF称为5GC NF,当有多个NF时,也可以描述为5GC NFs,或者简称为NFs。

[0083] NWDAF网元是5G新引入的网络功能,为5G核心网其他网络功能提供数据分析服务,分析的信息可以过去事件的统计信息,也可以是预测信息。根据当前3GPP协议23.288-g10,NWDAF网元已经支持了一些分析用例:如切片负载,业务体验,网络性能、用户相关行为等分析。其中用户相关的行为分析中涉及非正常的用户行为分析,用于识别被劫持或滥用的用户终端,从而防止用户终端被盗用,或被用于向网络发起攻击等事件。网络功能可以直接或间接的向NWDAF网元订阅安全相关的数据分析服务,例如,处于5G核心网内部的可信的消费网络功能(consumer NF)可以直接向NWDAF网元订阅用户识别分析服务,例如,订阅的用户识别分析服务可以为NWDAF网元分析订阅服务(Nnwdaf_Analytics Subscription_Subscribe),用于网络功能向NWDAF网元订阅异常用户识别分析服务。外部的应用功能可以向网络能力开放功能(network exposure function,NEF)发送订阅请求;进而,NEF向NWDAF网元转发该订阅请求,以使AF向NWDAF网元订阅用户识别分析服务。NWDAF网元根据分析和运营商的策略,确定用户行为分析结果为AF订阅的用户识别分析服务对应的订阅消息,向订阅该用户行为分析服务的NEF发送用户行为分析结果,以使NEF向AF发送用户行为分析结果。或者,NWDAF网元根据分析和运营商的策略,确定用户行为分析结果为消费者NF网元订阅的用户识别分析服务对应的订阅消息,则可以向订阅该用户行为分析服务的消费者NF发送用户行为分析结果。订阅异常用户识别分析服务的网元对用户行为分析结果进行相应的处理,如释放对应的终端。但是,NWDAF网元只分析UE行为信息,对核心网网络功能的行为没有分析。而5G核心网由于引入的很多IT技术,如虚拟化平台,容器平台,越来越多的开源第三方IT组件的应用,再加上多方供应商的共同参与组网,直接对5G核心网网络功能进行攻

击、渗透和劫持等安全异常行为，通过上述方案，NWDAF网元是无法确定出核心网网络功能进行攻击、渗透和劫持等安全异常行为，导致核心网存在安全隐患。另外，由于用户行为分析服务仅能通过向NWDAF网元订阅，来获取NWDAF网元对用户行为分析的结果，而在很多场景下，安全异常行为涉及到多个网络功能的参与，一个安全异常行为可能会影响多个网络功能的正常运行，而上述用户行为分析服务的订阅方式，使得用户行为分析结果只会发送给订阅用户行为分析服务的网元，而真的该安全异常行为涉及到的其他网络功能无法获取到该用户行为分析结果，也无法针对涉及到的安全异常行为进行处理，也导致了核心网的网元的安全性不高。

[0084] 基于上述内容，本申请实施例提供一种网络事件处理方法，如图4所示，为本申请实施例提供的网络性能数据分析方法流程示意图，包括以下步骤：

[0085] 步骤401:NWDAF网元获取K个第一网元的消息交互行为信息。

[0086] 其中，所述消息交互行为信息可以与所述核心网网元的功能对应。例如，核心网网元可以为上述实施例中的任一种网元。K个第一网元的消息交互行为信息可以为NWDAF网元订阅的第一网元的消息交互行为信息，也可以为NWDAF网元订阅的第一网元获取的其他核心网网元的消息交互行为信息。针对所述K个第一网元中的一个第一网元，所述第一网元的消息交互行为信息包括用于指示所述第一网元传输的消息的属性信息；所述K为正整数。其中，所述第一网元传输的消息的属性信息，可以包括：所述消息的类型，类型具体可以根据第一网元传输的消息的接口确定)；所述消息的消息内容(例如，UE标识，网元的IP地址，网元的标识，网元的证书，请求的内容等)、所述第一网元上传输所述消息的接口(可以根据第一网元确定，例如，NWDAF网元分析订阅服务接口，事件分析服务(Nnwdaf_AnalyticsInfo)接口，NWDAF网元分析通知(Nnwdaf_AnalyticsInfo_Notif)，AMF网元通信接口(Namf_Communication)，AMF网元事件开放服务接口，SMF事件开放服务接口，SPF网元安全策略接口，安全日志(Nnf_SecurityLog)接口等)；所述消息对应的对端传输所述消息的接口(可以根据第一网元的对端的网元确定，例如，NWDAF网元分析订阅服务接口，AMF网元事件开放服务接口，SMF事件开放服务接口，SPF网元安全策略接口等)。

[0087] 在步骤401中，一种可能的方式，NWDAF网元可以向K个第一网元发送消息交互行为信息订阅请求，用于订阅K个第一网元的消息交互行为信息；其中，第一网元的消息交互行为信息可以为第一网元生成的消息交互行为信息，也可以为第一网元获取的其他核心网网元的消息交互行为信息。

[0088] 举例来说，NWDAF网元订阅的第一网元可以为AMF网元，进而AMF网元可以将终端设备接入运营商网络的接入信息和移动性信息，例如包括移动状态信息，分配给用户的临时身份标识，认证信息和授权用户信息等上报至NWDAF网元。AMF网元也可以将SMF发送给AMF网元的会话建立，会话修改和会话释放、UE的IP地址、选择的UPF等会话相关的信息作为消息交互行为信息上报至NWDAF网元。

[0089] 另一种举例，NWDAF网元通过AMF网元的开放接口，向AMF网元发送用户行为订阅请求，用于订阅AMF网元事件开放服务(Namf_EventExposure)，以获取终端的接入移动性等UE行为信息。AMF网元可以以周期性的方式，向NWDAF网元发送UE行为消息；UE行为信息可以包括：UE的位置信息(可以包括UE所在的跟踪区标识TAI或小区标识Cell ID)，UE的接入技术类型，UE移入或移出兴趣区，UE注册状态变更等。AMF网元可以通过订阅或者AMF网元可以以

事件的方式，向NWDAF网元发送UE行为消息。

[0090] 再比如，NWDAF网元可以通过订阅SMF的开放服务接口，例如，SMF事件开放服务(Nsmf_EventExposure)，以获取UE会话管理等UE行为信息。SMF也可以周期性或事件性的向NWDAF网元上报UE会话消息。其中，UE会话消息可以包括一下UE行为信息：UE的IP地址变更，PDU会话释放，用户面路径变更等通话信息或计费信息等。

[0091] 步骤402：NWDAF网元根据所述K个第一网元的消息交互行为信息，确定出第二网元发生网络安全异常事件。

[0092] 下面以K个第一网元为1个第一网元，消息交互行为信息包括第一网元接收到来自第二网元的消息为例进行说明。当然，消息交互行为信息也可以为第一网元直接发送的，也可以为通过其他网元发送给第一网元的信令消息等方式获取的，在此不做限定。

[0093] 在步骤402中，一种可能的实现方式，NWDAF网元可以根据消息交互行为信息发送的消息频率，确定是否存在网络安全异常事件。例如，若确定所述第一网元接收到来自第二网元的消息的数量大于第一阈值，则确定存在所述第二网元对所述第一网元的DDoS攻击事件；所述第一阈值为根据历史消息频率确定的。

[0094] 另一种可能的实现方式，NWDAF网元可以根据消息交互行为信息确定出第一网元的第一消息与第二网元的第二消息存在不一致，则确定可能存在网络安全异常事件。

[0095] 在上述步骤402中，NWDAF网元确定出第二网元发生网络安全异常事件可以有多种可能地实施方式，下面通过实施方式a1、实施方式a2和实施方式a3对此进行介绍。

[0096] 实施方式a1，数据分析网元根据K个第一网元的消息交互行为信息包括的第一消息和第二消息确定可能存在网络安全异常事件。若确定所述第一消息中的第二网元的第一身份标识与所述第二消息中所述第二网元的第二身份标识不一致，则确定所述第二网元存在网络安全异常事件。

[0097] 以所述第一网元为计费功能网元CHF，会话管理功能网元SMF为例。所述第一消息为来自SMF的第一UE标识的第一计费请求；所述第二消息为AMF网元针对UE标识的注册信息；此时，所述数据分析网元若确定所述UE标识的注册信息中不包括第一UE标识的注册信息；则可以确定第一计费请求中的第一UE标识为非法注册信息，因此，第一网元可能存在篡改事件。

[0098] 实施方式a2，数据分析网元根据K个第一网元的消息交互行为信息包括的来自所述K个第一网元的第一UE的交互行为消息，确定所述第一UE是否存在网络安全异常事件。此时，若确定所述第一UE的交互行为消息不一致，则确定所述第一UE存在网络安全异常事件。

[0099] 举例来说，以所述第一网元为计费功能网元CHF和AMF网元为例。所述第一消息为第一UE标识的第一计费请求；所述第二消息为AMF网元针对UE标识的注册信息；此时，所述数据分析网元若确定所述UE标识的注册信息中不包括第一UE标识的注册信息；则可以确定第一计费请求中的第一UE标识为非法注册信息，可以确定第一UE可能存在被篡改的网络安全异常事件。

[0100] 再比如，NWDAF网元可以根据AMF网元和SMF上报的UE行为消息，进行用户行为分析。具体的，NWDAF网元可以根据内部数据分析算法，对AMF网元和SMF上报的用户行为信息进行分析，对被误用或被劫持的用户和用户行为进行识别。例如，可以识别异常的UE位置，异常长时间的数据流，异常频繁接入等，进而确定第一UE存在网络安全异常事件。

[0101] 实施方式a3,数据分析网元根据K个第一网元的消息交互行为信息包括的述K个第一网元的第二UE的交互行为消息和来自第二网元的所述第二UE的用户信息查询请求,确定网元可能存在网络安全异常事件。数据分析网元若确定来自第二网元的所述第二UE的用户信息查询请求中,所述第二网元中的网元标识不一致,则确定所述网元标识不一致对应的至少两个网元发生网络安全异常事件。

[0102] 以第一网元可以为SMF1,第二网元为SMF2,第二网元非法获取SMF1的证书向AMF网元发送第二UE的用户信息查询请求,以非法窃取第二UE的用户信息为例。所述用户信息查询请求包括第一网元的证书和第二网元的网元标识,例如,第二网元的IP地址或端口;SMF1向AMF网元发送第二消息,第二消息可以是SMF1与AMF网元交互的任一消息或多个消息的集合;其中,第二消息包括:第一网元的网元标识,例如,第一网元的证书,第一网元的IP地址或端口等。此时,所述数据分析网元可以根据第二UE的用户信息查询请求与第二消息,确定第二UE的用户信息查询请求中的网元的证书与第二消息对应网元的证书一致,但是,第二UE的用户信息查询请求对应的网元的IP地址与第二消息中的网元的IP地址不一致,判定第二UE的用户信息查询请求对应的网元,与第二消息中对应的网元发生网络安全异常事件。

[0103] 步骤403:NWDAF网元向SPF网元发送第一指示信息。

[0104] 其中,所述第一指示信息用于指示所述第二网元发生所述网络安全异常事件。

[0105] 实施方式b1,一种可能的设计,网络安全异常事件可以包括:第一网元受到DDoS攻击事件。例如,根据消息交互行为信息,确定第二网元对第一网元发起DDoS攻击,则可以确定第二网元和/或第一网元存在网络安全异常事件。

[0106] 实施方式b2,网络安全异常事件可以包括:第二网元和/或第一网元的安全异常事件;第二网元和/或第一网元的安全异常事件可以存在多种异常。例如,第一网元或第二网元可能存在被冒用的风险,一种可能的场景中,第二网元和/或第一网元的安全异常事件可以表示为:第一网元的第一消息与第二网元的第二消息存在不一致的网络安全异常事件,第一消息与第二消息中存在相同的标识信息;此时,可以认为第一网元和/或第二网元可能存在被冒用的风险,进一步的,NWDAF网元还可以根据与第一消息相关的其他消息,或者与第二消息相关的其他消息进行比较,确定第一网元的第一消息与第二网元的第二消息不一致的原因,进而确定被冒用或被篡改的网元,进而,确定该网络安全异常事件为第一网元和/或第二网元被冒用或被篡改。

[0107] 实施方式b3,第二网元和/或第一网元可能存在窃取用户信息的网络安全异常事件,一种可能的场景中,第二网元和/或第一网元的安全异常事件可以表示为:第一网元的第一身份标识与第一网元的第二身份标识不一致,且第一网元向第二网元发送用户信息的查询请求,此时,第一网元可能存在窃取用户信息的安全异常事件。

[0108] 实施方式b4,网络安全异常事件还可以包括:用户的网络安全异常事件;例如,一种可能的场景中,用户的安全异常事件可以表示为:第一网元发送的第一消息中携带的第一用户标识,与第二网元发送的第二消息中携带的第一用户标识相同,且第一消息与第二消息不一致,也可以确定为第一用户标识对应的用户存在网络安全异常事件。

[0109] 实施方式b5,网络安全异常事件还可以包括:异常业务的网络安全异常事件。例如,所述K个第一网元的消息交互行为信息包括:来自所述K个第一网元的第二UE的交互行为消息和来自第二网元的所述第二UE的用户信息查询请求;所述数据分析网元若确定来自

第二网元的所述第二UE的用户信息查询请求中，所述第二网元中的网元标识不一致，则可以确定第二UE的用户信息查询请求为异常业务，并且确定所述网元标识不一致对应的至少两个网元存在异常业务的网络安全异常事件。

[0110] 通过增加各5G核心网网元的消息交互信息的服务接口，使得NDWAF可以获取各网元的消息交互行为信息，进而通过对个网元的消息交互行为信息的分析，提升网络功能异常行为检测能力，进而有效提升对网络功能的安全入侵事件的识别率和识别的准确度。

[0111] 步骤404：SPF网元接收NWDAF网元发送的第一指示信息。

[0112] 在具体实施过程中，SPF网元可以向NWDAF网元发送网络安全异常事件订阅请求，以获取来自NWDAF网元的网络安全异常事件的第一指示信息，当然还可以向NWDAF网元发送网络安全异常事件的查询请求，以接收NWDAF网元发送的第一指示信息，在此不做限定。

[0113] 步骤405：SPF网元根据所述第一指示信息，确定出与所述第二网元具有关联关系的N个第三网元。

[0114] 其中，针对所述N个第三网元中的一个第三网元，所述第三网元具有对所述第二网元的业务进行处理的能力。

[0115] 步骤406：针对所述N个第三网元中的一个第三网元，SPF网元向所述第三网元发送所述第三网元对应的第一安全策略。

[0116] 其中，所述第三网元对应的第一安全策略中包括用于指示所述第三网元停止对所述第二网元的相关业务进行处理的指示信息。

[0117] 实施方式c1，SPF网元可以根据不同的网络安全异常事件的类型，确定不同的安全策略。例如，可以根据网络安全异常事件所关联的第三网元，设置对各第三网元的隔离策略，还可以根据网络安全异常事件所关联的用户，设置对各用户的隔离策略，当然，也可以根据网络安全异常事件所关联的用户，设置对各用户所涉及的第三网元的隔离策略。

[0118] 例如，网络安全异常事件为第二网元对所述第一网元的DDoS攻击事件；此时，第三网元可以为第二网元和/或第二网元相关的网元，可以根据DDoS攻击事件，确定对第三网元的隔离策略。例如，SPF网元根据所述DDoS攻击事件，确定对所述第三网元的相关业务进行隔离，并释放所述第三网元上对应用户。

[0119] 示例c1，第三网元可以为AMF网元，所述SPF网元向所述AMF网元发送所述AMF网元对应的第一安全策略，所述AMF网元对应的第一安全策略包括用于指示所述AMF网元停止对所述第二网元的消息的处理的指示信息；所述AMF网元对应的第一安全策略包括用于指示所述AMF网元释放所述第二网元所绑定的用户。再比如，SPF网元可以指示AMF网元停止建立和/或释放与第二网元相关的用户会话；具体的实施过程可以包括：SPF网元向AMF网元发送第一安全策略消息；所述第一安全策略消息用于指示所述AMF网元释放所述第二网元建立的用户会话。

[0120] 示例c2，第三网元可以为消息转发网元，因此，SPF网元可以指示消息转发(service communication proxy，SCP)网元停止对来自所述第二网元的消息的转发，具体的实施过程可以包括：SPF网元向消息转发网元SCP网元发送第一安全策略消息；所述第一安全策略消息包括所述第二网元的NF标识或IP地址；所述第一安全策略消息用于指示所述SCP网元停止对来自所述第二网元的消息的转发。

[0121] 示例c3，第三网元可以为网络中的任一可能与第二网元建立通信连接的网元。因

此,SPF网元可以指示第三网元停止与第二网元建立通信连接,具体的实施过程可以包括:SPF网元向第三网元发送第二安全策略消息;所述第一安全策略消息包括所述第二网元的NF标识;所述第二安全策略消息用于所述第三网元忽略与所述第二网元建立连接。

[0122] 举例来说,所述第三网元为NRF网元,所述SPF网元向所述NRF网元发送所述NRF网元对应的第一安全策略,所述NRF网元对应的第一安全策略包括用于指示所述NRF网元停止对所述第二网元的用户授权;

[0123] 举例来说,第三网元可以为路由传输控制器SDN网元,SPF网元可以指示SDN网元阻止所述第二网元对应的网段的消息的路由转发。具体的实施过程可以包括:SPF网元向路由传输控制器SDN网元,发送第一安全策略消息;所述第一安全策略消息用于指示所述SDN网元阻止所述第二网元对应的网段的消息的路由转发。

[0124] 举例来说,所述第三网元为虚拟化资源管理(network functions virtualisation management and orchestration,MANO)网元,所述SPF网元向所述MANO网元发送所述MANO网元对应的第一安全策略,所述MANO网元对应的第一安全策略包括用于指示所述MANO网元释放所述第二网元对应的虚拟机。

[0125] 实施方式d1,所述第一指示信息还可以用于指示所述网络安全异常事件对应的异常业务。SPF网元可以根据异常业务,确定出需执行第二安全策略的第四网元。具体的,SPF网元可以根据所述第一指示信息,确定出与所述第二网元具有关联关系的M个第四网元;针对所述M个第四网元中的一个第四网元,所述第四网元具有对所述异常业务进行处理的能力;针对所述M个第四网元中的一个第四网元,SPF网元可以向所述第四网元发送所述第四网元对应的第二安全策略,所述第四网元对应的第二安全策略中包括用于指示所述第四网元停止或撤销对所述异常业务进行处理的指示信息。

[0126] 在实施方式d1下可以有多种应用场景,下面通过下述场景1和场景2进行示例。

[0127] 场景1,所述第一网元传输的消息包括第一消息和第二消息,所述第一消息中的第一UE的交互行为消息与所述第二消息中第一UE的交互行为消息不一致,其可能的原因是,第一消息中的第一UE的交互行为消息存在篡改,也可能为第二消息中的第一UE的交互行为消息存在篡改,NWDAF网元可以根据K个第一网元传输的消息中,涉及的第一UE的其他交互行为消息,确定存在篡改的为第一消息还是第二消息。此处,以第一消息中的第一UE标识存在篡改为例进行说明。其他第一UE的交互行为消息存在篡改确定的第二安全策略可以参考第一消息中的第一UE标识存在篡改的实施例,在此不再赘述。

[0128] 在场景1下,针对第一消息中的第一UE标识存在篡改问题,下面通过示例d1-d5进行介绍。

[0129] 示例d1,第四网元可以为SMF网元,此时,SPF网元可以对SMF网元发起的第一UE的业务进行隔离,即,可以指示SMF网元停止执行第一UE对应的操作。例如,停止执行所述SMF网元生成的所述第一UE的业务请求,并释放所述第一UE与所述SMF网元的会话。在具体实施过程中,可以包括:SPF网元生成第二安全策略请求;所述第二安全策略请求用于停止执行所述SMF网元生成的所述第一UE的业务请求;并释放所述第一UE与所述SMF网元的会话。

[0130] 示例d2,所述第四网元为AMF网元,所述SPF网元向所述AMF网元发送所述AMF网元对应的第二安全策略,所述AMF网元对应的第二安全策略包括用于指示所述AMF网元停止执行所述异常业务的请求;例如,异常业务可以为第一网元相关的第一UE的会话,AMF网元可

以释放所述第一UE的会话。具体可以包括:SPF网元向所述AMF网元发送异常用户的安全策略请求;所述异常用户的安全策略请求用于指示所述AMF网元释放所述第一UE的会话。进一步的,所述SPF网元还可以向所述AMF网元发送所述AMF网元对应的第二安全策略,所述AMF网元对应的第二安全策略包括用于指示所述AMF网元释放所述异常业务对应的用户,例如,第一UE。

[0131] 示例d3,所述第四网元为AMF网元,若SPF网元确定SMF网元存在被冒用的风险,SPF网元还可以对AMF网元中与SMF网元的业务进行隔离。例如,可以指示SMF网元相关的AMF网元,释放与所述SMF网元向AMF网元发起的请求中涉及的第一UE标识的UE的会话。此时,由于可能涉及存在被冒用的风险的网元可能包括多个网元,可以对由SMF网元发起的业务请求全部或部分进行隔离。例如,若SPF网元可以确定被冒用的网元和冒用的网元,则可以将冒用的网元作为隔离的网元,对冒用的网元发起的业务进行隔离。若SPF网元无法确定被冒用的网元和冒用的网元,只能确定网元存在被冒用的风险,则可以将存在被冒用的风险的网元发起的业务都进行隔离。在具体实施过程中,可以包括:SPF网元向所述AMF网元发送异常用户的安全策略请求;所述异常用户的安全策略请求用于指示所述AMF网元释放所述SMF网元相关的UE的会话。

[0132] 示例d4,所述第四网元为PCF网元,所述SPF网元向所述PCF网元发送所述PCF网元对应的第二安全策略,所述PCF网元对应的第二安全策略包括用于指示所述PCF网元释放所述异常业务对应的用户,以使PCF网元对涉及第一UE标识的用户进行隔离。在具体实施过程中,可以包括:SPF网元向PCF网元发送异常用户的安全策略请求;所述异常用户的安全策略请求用于指示所述PCF网元释放所述第一UE标识的会话及网络。

[0133] 示例d5,SPF网元若确定所述第一UE标识的篡改对象为第二网元,则可以认为第二网元存在被冒用的风险,进而,可以向第四网元发起针对第二网元的异常业务的隔离的第二安全策略。具体的,SPF网元可以向所述第四网元发送第二安全策略请求;所述第二安全策略请求用于指示对所述第二网元的异常业务进行隔离。例如,所述第四网元为SCP网元,所述SPF网元向所述SCP网元发送所述SCP网元对应的第二安全策略,所述SCP网元对应的第二安全策略包括用于指示所述SCP网元停止对所述第二网元的异常业务的消息转发;或者,所述第四网元为NRF网元,所述SPF网元向所述NRF网元发送所述NRF网元对应的第二安全策略,所述NRF网元对应的第二安全策略包括用于指示所述NRF网元停止对所述第二网元的异常业务的用户授权;或者,所述第四网元为SDN网元,所述SPF网元向所述SDN网元发送所述SDN网元对应的第二安全策略,所述SDN网元对应的第二安全策略包括用于指示所述SDN网元停止对所述第二网元的异常业务的网段的消息的路由转发。

[0134] 场景2,以窃取用户隐私消息的场景为例进行说明。此时,NWDAF网元或SPF网元可以通过存在网元查询用户信息的方式,确定可能存在窃取用户隐私消息的网络安全事件,NWDAF网元或SPF网元通过所述第一消息中的第二网元的第一身份标识与所述第二消息中所述第二网元的第二身份标识不一致,确定窃取用户隐私消息的对象为第二网元,则可以确定第二网元存在被冒用的风险。当然,NWDAF网元或SPF网元还可以根据其他交互行为消息的不一致,确定存在窃取用户隐私消息的对象,在此不再赘述。

[0135] 在具体的场景中,以第二网元为第一SMF,第一网元为AMF网元为例;第一消息可以包括:所述第二网元向所述第一网元发送的第三UE信息的查询请求;查询请求包括所述第

一网元的第一身份标识;第二消息包括:所述第一网元的第二身份标识。NWDAF网元若根据所述第二网元的第一身份标识与所述第二网元的第二身份标识不一致,且所述第一身份标识存在网络安全异常事件,则可以确定与所述第一身份标识对应的第二网元为异常网元。此时,安全异常事件中可以包括:指示第一SMF为异常网元。再比如,SPF网元根据所述第二网元的第一身份标识与所述第二网元的第二身份标识不一致,且所述第一身份标识存在网络安全异常事件,则可以确定与所述第一身份标识对应第一SMF为异常网元。

[0136] 例如,第一身份标识可以为第一SMF网元对应的IP地址IP1,若第二网元窃取了第二SMF的TSL证书,用于向第一网元发送第三UE信息的查询请求的验证,此时,NWDAF网元可以接收到来自AMF网元的第一消息,第一消息中包括:第一SMF网元的IP1,第二SMF网元的TSL证书,第三UE信息的查询请求。NWDAF网元还可以接收到第二SMF网元发送的第二消息,第二消息中包括:第二SMF网元的IP2,第二SMF网元的TSL证书。

[0137] 进而,NWDAF网元根据第一消息和第二消息,可以确定第一SMF网元发送的第三UE信息的查询请求存在网络安全异常。进一步的,NWDAF网元还可以根据第二SMF网元发送的包括有TSL证书的其他UE信息的查询请求,及第二SMF网元的第二身份标识(第二SMF网元对应的IP地址IP2),确认第一SMF网元为异常网元。

[0138] 进而,SPF网元根据NWDAF网元的网络安全异常事件,确定第二安全策略。第二安全策略可以为针对第二网元的会话或网络的隔离,和/或第二网元涉及的用户的会话或网络的隔离。具体的,可以包括:SPF网元根据所述异常网元,生成第二安全策略,对所述异常网元的业务进行隔离,和/或释放所述异常网元上对应用户;SPF网元向第四网元发送第二安全策略;第二安全策略用于指示所述第四网元停止向所述异常网元发送用户的相关信息。

[0139] 通过上述方法,当NWDAF网元检测到安全异常事件后,还可以向新增的安全事件处理功能SPF网元通知网络安全异常事件,进而,由SPF网元通过和各领域的新增安全策略接口,协同和联合多功能领域,对网络安全事件进行响应,有效提升对安全异常事件的处理,有效提高网络安全性能。可以有效控制安全异常对网络的影响。

[0140] 下面对本申请实施例提供的网络事件处理方法进行具体描述。一种具体的实现方法,包含两个主要网络功能,一个是NWDAF网元,负责安全数据的分析和异常安全事件识别,NWDAF用于订阅其对应的网元的消息交互信息。一个是新增的安全策略网元SPF网元,负责网络安全事件的策略确定和网络安全异常事件的处理。如图5所示,为本申请实施例提供的网络性能数据分析方法流程示意图。以NF(例如,第二网元)被劫持,恶意对其他NF(例如,第一网元)进行DDoS攻击,影响第一网元涉及的其他网元NF的可用性为例进行说明。该方法包括以下步骤:

[0141] 步骤501:NWDAF网元接收第一网元的消息交互行为信息。

[0142] 一种可能的方式,获取第一网元的消息交互行为信息的方式可以通过第一网元对应的数据开放接口,如AMF网元可以通过扩展的事件开放服务(Namf_EventExposure)接口获取的,SMF可以通过扩展的事件开放服务(Nsmf_EventExposure)接口获取的。在具体实施过程中,消息交互行为信息接口还可以为扩展后的事件分析服务(Nnwdaf_AnalyticsInfo)接口,用于增加消息交互行为信息的分析类型,例如,NF行为异常,用户行为异常等。此外还可以通过携带NF筛选参数,对需要分析NF范围进行限制或筛选,以节省NWDAF网元分析的数据量,提高网络数据分析的效率。例如,NF筛选参数可以包括以下至少一项:NF类型,NF标识

或NF列表,NF所属的切片等参数。

[0143] 另一种可能的方式,步骤501a中,NWDAF网元向NF发送NF的消息交互信息的订阅请求,以获得NF发送的消息交互行为信息。NWDAF网元获取NF的消息交互行为信息可以为NF与其他NF信令交互的消息交互行为信息,也可以通过新增的信令,例如,NF安全日志(Nnf_SecurityLog),向NF订阅NF消息交互行为信息。订阅的NF的消息交互行为信息,可以包括NF所有发送和接受的接口消息类型,所有消息发生的事件和接口消息的内容等。其中,接口消息的内容可以包括:接口消息的完整数据,摘要,关键信息等。具体NF对应支持的接口可以参见上述实施例,在此不再赘述。

[0144] 假如第二网元被外部用户恶意渗透控制,通过向周边NF频繁发送第一消息,例如,SMF1通过AMF网元通信接口(Namf_Communication)向AMF网元1短时间发送多个第一消息,导致AMF网元1处理资源和接口带宽资源占用,处理正常业务能力下降。此时,AMF网元1根据NWDAF网元消息交互行为信息的收集要求,周期性或事件性上报第二网元向第一网元发送的消息,作为第一网元的消息交互行为信息。

[0145] 步骤502:NWDAF网元对AMF网元1的交互事件进行分类判断,确定网络安全异常事件。

[0146] 其中,网络安全异常事件为第一网元受到第二网元的DDoS攻击。

[0147] 一种可能的实现方式,NWDAF网元根据内部算法,例如,根据指定规则判断,如AMF网元1的历史流量模型,确定在指定时间内接收第二网元NF的消息升超过预设阈值,则确定AMF网元1的交互事件过程发生业务突发飙,可能存在DDoS攻击。另一种可能的实现方式,根据机器学习或人工智能(artificial intelligence,AI)算法,根据历史异常或正常业务信令交互数据训练后的模型,对第一网元AMF网元1的交互事件过程进行分类判断是否存在DDoS攻击。本申请实施例不限定具体算法,NWDAF网元可以根据具体采用的算法判断第一网元NF可能被DDos攻击。

[0148] 步骤503:NWDAF网元向SPF网元发送第一指示信息。

[0149] 其中,第一指示信息可以为NWDAF网元分析通知(Nnwdaf_AnalyticsInfo_Notif)消息,包括:第一网元AMF网元1可能受到第二网元SMF1的DDos攻击。

[0150] 在一种可能的实现方式,SPF网元可以通过NWDAF网元的分析服务(Nnwdaf_AnalyticsInfo)接口,向NWDAF网元发送网络安全异常事件的订阅请求,进而NWDAF网元可以根据网络安全异常事件的订阅请求,确定需要向SPF网元上报第一网元AMF网元1可能受到第二网元SMF1的DDos攻击。

[0151] 步骤504:SPF网元根据第一指示信息,确定第一安全策略。

[0152] 具体的,安全策略可以为本地或后台配置的安全策略,进而,SPF网元根据NF类型,确定第二网元SMF可能被入侵,并根据DDoS攻击等其他NF对应的安全策略的条件判断,确定对第二网元执行的安全策略。

[0153] 例如,SPF网元确定第二网元发起DDoS攻击,可以确定第二网元需进行业务和网络隔离,另外,由于第二网元为SMF1,因此,还需要对SMF涉及的用户的会话进行隔离,释放SMF1上对应用户。业务和网络的隔离可以有多种处理手段。例如,SPF网元可以将安全策略指令发送至业务或网络对应的控制中心的网元,进而使得业务或网络对应的控制中心的网元执行对应第二网元的安全策略消息。

[0154] 步骤505:SPF网元向第三网元发送第一安全策略。

[0155] 在步骤504a中,第三网元为SCP网元,SPF网元可以向SCP网元发送第一安全策略,指示SCP网元停止转发第二网元的消息,其中第一安全策略消息可以携带第二网元SMF1的网元标识NF ID或IP地址。

[0156] 在步骤504b中,第三网元为NRF网元,根据第一安全策略,SPF网元可以向NRF网元发送第一安全策略,指示NRF网元隔离NF和SMF1之间的相互发现,避免SMF1和NF之间建立连接。消息中可以携带SMF1对应的NF标识。

[0157] 在步骤504c中,第三网元为PCF网元或AMF网元,SPF网元可以向PCF网元或AMF网元发送第一安全策略,用于指示释放对应的第二网元的用户会话。

[0158] 具体的,对于第二网元SMF1上可能现有的业务,SPF网元可以通过向PCF网元或直接向对应的AMF网元发送第二网元的安全策略消息,用于指示释放对应SMF1的用户。或者,SPF网元可以通过直接向对应的AMF网元发送第二网元的安全策略消息,用于指示释放对应SMF1的用户。

[0159] 在步骤504d中,第三网元为SDN网元,SPF网元还可以向SDN网元发送第一安全策略,用于指示SDN网元在路由层面隔离SMF1对应的网段,以使SPF网元实现在5G核心网NF范围外的网元对SMF1的隔离。

[0160] 步骤505:第三网元接收到第一安全策略,执行第一安全策略。

[0161] 在步骤505a中,SCP网元接收第一安全策略,根据指示的第一安全策略,停止对应SMF1的消息转发,对于已经接收到的第二网元SMF1发出的消息,可以进行丢包处理。

[0162] 在步骤505b中,NRF网元接收第一安全策略后,根据指示的第一安全策略,拒绝所有该SMF1发起的对其他NF的发现请求,同时不返回SMF1作为其他NF对SMF的发现请求,从而隔离了SMF1和其他NF之间的连接发起。

[0163] 在步骤505c中,AMF网元接受SPF网元的第一安全策略后,对SMF1建立的用户会话,发起连接释放。

[0164] 在步骤505d中,SDN网元接收第一安全策略后,向对应的路由器发送配置,拒绝对应SMF1的原地址网段或目标地址网段的路由转发。

[0165] 下面一种具体的实现方法,包含两个主要网络功能,可以部署在一个网元上,也可以单独部署,在此不做限定。以部署在一个网元上为例,即第一网元包括NWDAF,NWDAF网元,安全策略网元SPF网元的功能,第一网元负责安全数据的分析和异常安全事件识别,并订阅网元的消息交互行为信息,第一网元还负责安全事件的安全策略的确定和安全异常事件的处理协同。SPF网元可以不作为单独的NF部署,作为功能嵌入NWDAF网元中。

[0166] 一种可能的场景中,当NF发送的消息被恶意篡改,例如,第二网元为SMF,SMF发出的计费请求被恶意篡改,将盗打用户的UE ID中的UE1改为UE2,从而导致恶意盗打,非法获利的场景。如图6所示,为本申请实施例提供的一种网络事件处理方法流程示意图,该方法包括以下步骤:

[0167] 步骤601:AMF网元向NWDAF网元发送消息交互行为信息。

[0168] 其中,消息交互行为信息可以为UE1完成注册的消息,也可以为UE发起的UE1的业务消息。AMF网元可以通过事件发布服务接口或安全日志接口将UE1已注册的消息交互行为信息上报给NWDAF网元,指示UE1已注册。

[0169] 步骤602:第二网元向第一网元发送第一消息。

[0170] 其中,第二网元为被篡改的网元,向第一网元发送业务请求。例如,以第二网元为SMF1,SMF1中的用户标识UE1被篡改为用户标识UE2。具体的篡改方式可以为,被篡改的第一网元SMF1中,可能存在计费消息的处理模块被篡改,例如,第一网元SMF1的处理模块被注入恶意程序,可以将盗打用户的用户标识UE1产生的计费账单中的用户标识修改为UE2。以第一网元为CHF网元为例,第一消息为SMF1发送的计费请求消息(Nchf_ConvergedCharging),计费请求携带被篡改的用户标识(UE2)。

[0171] 步骤603:CHF向NWDAF网元发送消息交互行为信息。

[0172] 例如,CHF可以将第二网元发送的第一消息作为消息交互行为信息发送给NWDAF网元。

[0173] 进一步的,CHF可以根据第二网元发送的计费请求,为用户UE2产生一条计费账单。此时,CHF可以将计费账单,及第一消息作为消息交互行为信息,发送给NWDAF网元。也可以将计费账单作为一个消息交互行为信息,发送给NWDAF网元,用于指示第一网元SMF1请求对UE2产生一条计费的网络行为。

[0174] 步骤604:NWDAF网元/SPF网元确定网络安全异常事件,并向PSF发送第一指示信息。

[0175] 一种可能的实现方式,NWDAF网元可以根据UE2计费消息的完整性,判断是否出现恶意盗打的网络安全异常事件。一种可能的场景中,SMF1可能被劫持,导致NWDAF网元可能无法根据计费消息的完整性,判断是否出现恶意盗打的问题,因此,NWDAF网元可以根据多个网元涉及到的同一用户的会话的相关交互的消息,比较是否存在不一致的消息,进而确定被篡改的对象。例如,第一消息可以为涉及SMF1处理UE2的计费消息,第二消息可以为涉及SMF1处理UE2的会话消息,或者,第二消息可以为涉及其他网元处理UE2的会话消息,则NWDAF网元可以根据第一消息是否与第二消息不一致,判断是否存在网络安全异常事件。例如,若确定第一网元并没有上报SMF1处理UE2的会话业务的第二消息,则NWDAF网元可以确定SMF1没有处理UE2的业务,即可以确定SMF1请求对UE2产生一条计费请求的网络行为存在网络安全异常,且UE2对应的会话并不是第一网元处理的,因此,SMF1发送给CHF的请求时错误的,SMF1的关键模块可能被入侵,使得第一网元的关键业务数据账单数据被篡改。具体的,NWDAF网元可以根据规则异常判断,或使用其他如大数据的AI算法等,确定异常的计费账单,进而确定网络安全异常事件。

[0176] 步骤605:SPF网元根据网络安全事件,确定第二安全策略,并向第四网元发送第二安全策略。

[0177] 在步骤605a中,SPF网元发送第二安全策略给AMF网元,第二安全策略用于指示SMF1的UE1用户异常,建议AMF网元停止对异常用户UE1的计费,并释放对应的用户UE1。

[0178] 若SPF网元设置在NWDAF网元上,第二安全策略的消息格式可以为NWDAF网元的分析服务消息(nwdaf_AnalyticsInfo),或者SPF网元的安全策略消息(SecPolicy)。

[0179] 步骤605b:SPF网元发送安全策略给CHF,通知SMF1发送的UE2的计费消息为异常计费消息。

[0180] 步骤605c:SPF网元发送安全策略给PCF网元,通知UE1异常,用于指示停止UE1的用户使用网络,或者停止UE1对指定会话的使用。

[0181] 步骤606:第四网元接收第二安全策略,并执行第二安全策略。

[0182] 步骤606a:AMF网元根据第二安全策略,可以对UE1发起释放消息。

[0183] 步骤606b:CHF根据第二安全策略,停止SMF1发起的UE2的计费账单产生。

[0184] 步骤606c:PCF网元根据第二安全策略,可以停止UE1的用户使用网络,或者停止UE1对指定会话的使用。

[0185] 步骤607:SPF网元根据网络安全事件,确定第一安全策略,并向第三网元发送第一安全策略。

[0186] 步骤607a:SPF网元向NRF网元发送第一安全策略。

[0187] 其中,第一安全策略用于指示第一网元SMF1异常,需对第一网元SMF1进行隔离。

[0188] 步骤607:第三网元根据第一安全策略,执行第一安全策略。

[0189] 步骤608a:NRF网元根据安全策略消息,可以停止SMF1和其他网元NF之间的相互发现。

[0190] 此外实施例一中第一安全策略也都可以应用到本实施例,具体选择的方案可以根据SPF网元的第一安全策略确定。

[0191] 下面一种具体的实现方法,包含两个主要网络功能,可以部署在一个网元上,即第一网元包括NWDAF,NWDAF网元,安全策略网元SPF网元的功能,第一网元负责安全数据的分析和异常安全事件识别,并订阅其对应的网元的信息。第一网元还负责安全事件的策略确定和协同。在该实例中,假设NF的身份信息被盗取,导致盗取身份信息的网元可以冒用该身份信息,进而非法获取用户信息,造成关键信息泄露。如图7所示,为本申请实施例提供的一种网络事件处理方法流程示意图,该方法包括以下步骤:

[0192] 步骤701:SMF2向AMF网元发送UE2的信息查询请求。

[0193] 其中,SMF2通过非法获取SMF1的TLS证书与AMF网元建立连接,并通过AMF网元的事件发布服务的接口向AMF网元发送UE2的位置信息的查询请求。一种可能的方式,SMF2非法获取SMF1的TLS认证证书。SMF1被黑客通过后台远程控制,或是黑客通过漏洞注入的一个应用,进而通过对SMF1的内部网络渗透,获取了SMF1的TLS认证证书。进而,SMF2可以假冒SMF1的身份,向AMF网元发送用户信息的查询请求,进而非法获取用户的信息。

[0194] 步骤702:第一网元AMF网元向NWDAF网元发送消息交互行为信息。

[0195] AMF网元可以将向SMF2发送的UE2的位置信息作为消息交互行为信息,还可以将接收到的SMF2发送的UE2的位置信息的查询请求作为消息交互行为信息,周期性或事件性的上报到NWDAF网元。例如,消息交互行为信息可以包括:SMF2发送的UE2的位置信息的查询请求,SMF2的IP地址IP1,SMF1的TLS证书等。

[0196] 进一步的,AMF网元根据UE2的信息查询请求,向SMF2发送UE2的位置信息。此时,AMF网元可以将向SMF2发送的UE2的位置信息作为消息交互行为信息,周期性或事件性的上报到NWDAF网元。

[0197] 步骤702a:SMF1向NWDAF网元发送消息交互行为信息。

[0198] 进而,NWDAF网元还可能接收到SMF1向NWDAF网元上报的消息交互行为信息,其中,消息交互行为信息包括SMF1的标识,例如,SMF1的IP地址IP1。

[0199] 步骤703:NWDAF网元根据消息交互行为信息,确定存在网络安全异常事件的第二网元。

[0200] 具体的，NWDAF网元可以根据第二网元AMF网元发送的消息交互行为信息，及SMF1网元上报的消息交互行为信息，UE2的信息查询请求的请求方SMF2的IP地址，与SMF1向NWDAF网元上报的消息交互行为信息中的SMF1的IP地址不同，可以确认，至少有1个SMF为异常网元，此时可以将第二网元确认为SMF1和SMF2。进一步的，NWDAF网元还可以根据SMF2针对UE发送的查询请求，及SMF1针对UE发送的查询请求，进一步比较是否存在不一致的消息交互行为信息，进而确定异常网元。例如，NWDAF网元确定SMF1网元只请求了UE1的信息，并未发送对UE2的位置信息的查询请求。也可以确定，SMF2网元存在网络安全异常事件。NWDAF网元可以进一步根据其他网元NF上报的消息交互行为信息，确定IP2对应的第二网元SMF2可能是假冒的，UE2的位置信息可能被泄露。

[0201] 步骤704：NWDAF网元向SPF网元发送第一指示信息，用于指示网络安全异常事件。

[0202] 步骤705：SPF网元接收第一指示信息，并根据第一指示信息，向第四网元发送第二安全策略。

[0203] 在步骤705a中，SPF网元可以向AMF网元发送第二安全策略。

[0204] 其中，第二安全策略用于指示UE2的信息泄露，并指示AMF网元停止或流控UE2的消息的发送和接收。例如，AMF网元可以根据第二安全策略，停止响应UE2信息的查询请求，或者，还可以设置为停止响应来自SMF1或SMF2的异常网元请求的UE2的信息的查询请求，避免影响其他网元的正常业务。

[0205] 步骤706：第四网元根据接收到的第二安全策略，执行第二安全策略。

[0206] 在步骤706a中，AMF网元根据第二安全策略，停止向SMF2发送UE2的用户信息，或者，AMF网元根据第二安全策略，停止向SMF1发送UE2的位置信息。具体的实施方式可以根据确定的异常网元确定，例如，若确定异常网元为SMF2，则可以只停止向SMF2发送UE2的用户信息，若确定异常网元为SMF2或SMF1，则可以停止向SMF1和SMF2发送UE2的用户信息。

[0207] 步骤707：SPF网元根据第一指示信息，向第三网元发送第一安全策略。

[0208] 步骤707a：SPF网元可以向SCP网元发送第二安全策略。

[0209] 其中，第二安全策略用于指示SCP网元停止对SMF1或SMF2的消息转发。其中，SCP网元可以根据消息中携带的IP地址确定SMF2网元，例如，消息中携带的IP地址为IP2，则可以确认该消息的发送方为SMF2，避免SMF2携带SMF1的证书所产生的干扰。

[0210] 步骤707b：SPF网元可以向虚拟机资源管理中心MANO网元发送第一安全策略；

[0211] 其中，第一安全策略用于指示MANO网元释放IP2对应的SMF2的虚拟机，进而阻止第二SMF网元SMF2的网络渗透和信息窃取。

[0212] 步骤708：第一网元根据接收到的第一安全策略，执行第一安全策略。

[0213] 步骤708a：SCP网元根据第一安全策略，停止对SMF1或SMF2的消息转发。

[0214] 步骤708b：MANO网元根据第一安全策略，释放IP2对应的第二SMF网元SMF2的虚拟机。

[0215] 此外实施例一中第一安全策略也可以应用到本实施例，具体选择的方案可以根据SPF网元的第一安全策略确定。

[0216] 上述主要从各个网元之间交互的角度对本申请实施例提供的方案进行了介绍。可以理解的是，上述实现各网元为了实现上述功能，其包含了执行各个功能相应的硬件结构和/或软件模块。本领域技术人员应该很容易意识到，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,本发明能够以硬件或硬件和计算机软件的结合形式来实现。某个功能究竟以硬件还是计算机软件驱动硬件的方式来执行,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。

[0217] 如图8所示,为本申请实施例所涉及的网络事件处理装置的一种可能的示例性框图,该装置800可以以软件或硬件的形式存在。装置800可以包括:处理单元802和通信单元801。作为一种实现方式,该通信单元801可以包括接收单元和发送单元。处理单元802用于对装置800的动作进行控制管理。通信单元801用于支持装置800与其他网络实体的通信。

[0218] 其中,处理单元802可以是处理器或控制器,例如可以是通用中央处理器(central processing unit,CPU),通用处理器,数字信号处理(digital signal processing,DSP),专用集成电路(application specific integrated circuits,ASIC),现场可编程门阵列(field programmable gate array,FPGA)或者其他可编程逻辑器件、晶体管逻辑器件、硬件部件或者其任意组合。其可以实现或执行结合本申请实施例公开内容所描述的各种示例性的逻辑方框,模块和电路。所述处理器也可以是实现计算功能的组合,例如包括一个或多个微处理器组合,DSP和微处理器的组合等等。通信单元801是一种该装置的接口电路,用于从其它装置接收信号。例如,当该装置以芯片的方式实现时,该通信单元801是该芯片用于从其它芯片或装置接收信号的接口电路,或者,是该芯片用于向其它芯片或装置发送信号的接口电路。

[0219] 该装置800可以为上述实施例中的NWDAF网元或SPF网元,还可以为用于NWDAF网元的芯片或SPF网元的芯片。例如,当装置800为NWDAF网元或SPF网元时,该处理单元802例如可以是处理器,该通信单元801例如可以是收发器。可选的,该收发器可以包括射频电路,该存储单元例如可以是存储器。例如,当装置800为用于数据分析网元或安全事件处理SPF网元的芯片时,该处理单元802例如可以是处理器,该通信单元801例如可以是输入/输出接口、管脚或电路等。该处理单元802可执行存储单元存储的计算机执行指令,可选地,该存储单元为该芯片内的存储单元,如寄存器、缓存等,该存储单元还可以是该数据分析网元或安全事件处理SPF网元内的位于该芯片外部的存储单元,如只读存储器(read-only memory,ROM)或可存储静态信息和指令的其他类型的静态存储设备,随机存取存储器(random access memory,RAM)等。

[0220] 在一种实施例中,该装置800为上述实施例中的NWDAF网元。所述通信单元801,用于获取K个第一网元的消息交互行为信息,针对所述K个第一网元中的一个第一网元,所述第一网元的信令交互行为信息包括用于指示所述第一网元传输的消息的属性信息;所述K为正整数;向SPF网元发送第一指示信息,所述第一指示信息用于指示所述第二网元发生所述网络安全异常事件。处理单元802,用于根据所述K个第一网元的消息交互行为信息,确定出第二网元发生网络安全异常事件;

[0221] 该装置800为上述实施例中的NWDAF网元的情况下,一种可能的设计,针对所述K个第一网元中的一个第一网元,所述第一网元传输的消息的属性信息,包括以下一项或多项:所述消息的类型、所述消息的消息内容、所述第一网元上传输所述消息的接口、所述消息对应的对端传输所述消息的接口。

[0222] 该装置800为上述实施例中的NWDAF网元的情况下,一种可能的设计,处理单元

802,用于若确定所述第一网元接收到来自第二网元的消息的数量大于第一阈值,则确定存在所述第二网元对所述第一网元的DDoS攻击事件;所述第一阈值为根据历史消息频率确定的。

[0223] 该装置800为上述实施例中的NWDAF网元的情况下,一种可能的设计,所述K个第一网元的消息交互行为信息包括:第一消息和第二消息;处理单元802,用于若确定所述第一消息中的第二网元的第一身份标识与所述第二消息中所述第二网元的第二身份标识不一致,则确定所述第二网元存在网络安全异常事件。

[0224] 该装置800为上述实施例中的NWDAF网元的情况下,一种可能的设计,所述K个第一网元的消息交互行为信息包括:来自所述K个第一网元的第一UE的交互行为消息;处理单元802,用于若确定所述第一UE的交互行为消息不一致,则确定所述第一UE存在网络安全异常事件。

[0225] 该装置800为上述实施例中的NWDAF网元的情况下,一种可能的设计,所述K个第一网元的消息交互行为信息包括:来自所述K个第一网元的第二UE的交互行为消息和来自第二网元的所述第二UE的用户信息查询请求;处理单元802,用于若确定来自第二网元的所述第二UE的用户信息查询请求中,所述第二网元中的网元标识不一致,则确定所述网元标识不一致对应的至少两个网元发生网络安全异常事件。

[0226] 可以理解的是,该装置用于上述网络事件处理方法时的具体实现过程以及相应的有益效果,可以参考前述方法实施例中的相关描述,这里不再赘述。

[0227] 在另一种实施例中,该装置800为上述实施例中的SPF网元。所述通信单元801,用于接收NWDAF网元发送的第一指示信息,所述第一指示信息用于指示所述第二网元发生网络安全异常事件;针对所述N个第三网元中的一个第三网元,向所述第三网元发送所述第三网元对应的第一安全策略,所述第三网元对应的第一安全策略中包括用于指示所述第三网元对所述第二网元对应的业务进行隔离的指示信息。处理单元802,用于根据所述第一指示信息,确定出与所述第二网元具有关联关系的N个第三网元;针对所述N个第三网元中的一个第三网元,所述第三网元具有对所述第二网元的业务进行处理的能力。

[0228] 该装置800为上述实施例中的SPF网元的情况下,一种可能的设计,通信单元801,用于执行以下一项或多项:

[0229] 所述第三网元为AMF网元,向所述AMF网元发送所述AMF网元对应的第一安全策略,所述AMF网元对应的第一安全策略包括用于指示所述AMF网元停止对所述第二网元的消息的处理的指示信息;所述第三网元为SCP网元,向所述SCP网元发送所述SCP网元对应的第一安全策略,所述SCP网元对应的第一安全策略包括用于指示所述SCP网元停止对所述第二网元的消息转发;所述第三网元为NRF网元,向所述NRF网元发送所述NRF网元对应的第一安全策略,所述NRF网元对应的第一安全策略包括用于指示所述NRF网元停止对所述第二网元的用户授权;所述第三网元为SDN网元,向所述SDN网元发送所述SDN网元对应的第一安全策略,所述SDN网元对应的第一安全策略包括用于指示所述SDN网元停止对所述第二网元的网段的消息的路由转发;所述第三网元为MANO网元,向所述MANO网元发送所述MANO网元对应的第一安全策略,所述MANO网元对应的第一安全策略包括用于指示所述MANO网元释放所述第二网元对应的虚拟机;所述第三网元为AMF网元,向所述AMF网元发送所述AMF网元对应的第一安全策略,所述AMF网元对应的第一安全策略包括用于指示所述AMF网元释放所述第二

网元所绑定的用户。

[0230] 该装置800为上述实施例中的SPF网元的情况下，一种可能的设计，所述第一指示信息还用于指示所述网络安全异常事件对应的异常业务；处理单元802，用于根据所述第一指示信息，确定出与所述第二网元具有关联关系的M个第四网元；针对所述M个第四网元中的一个第四网元，所述第四网元具有对所述异常业务进行处理的能力；针对所述M个第四网元中的一个第四网元，所述通信单元801，用于向所述第四网元发送所述第四网元对应的第二安全策略，所述第四网元对应的第二安全策略中包括用于指示所述第四网元停止或撤销对所述异常业务进行处理的指示信息。

[0231] 该装置800为上述实施例中的SPF网元的情况下，一种可能的设计，通信单元801，用于执行以下至少一项：

[0232] 所述第四网元为AMF网元，向所述AMF网元发送所述AMF网元对应的第二安全策略，所述AMF网元对应的第二安全策略包括用于指示所述第四网元停止执行所述异常业务的请求；所述第四网元为AMF网元或PCF网元，F向所述AMF网元发送所述AMF网元对应的第二安全策略，所述AMF网元对应的第二安全策略包括用于指示所述AMF网元释放所述异常业务对应的用户；或者，向所述PCF网元发送所述PCF网元对应的第二安全策略，所述PCF网元对应的第二安全策略包括用于指示所述PCF网元释放所述异常业务对应的用户；所述第四网元为SCP网元，向所述SCP网元发送所述SCP网元对应的第二安全策略，所述SCP网元对应的第二安全策略包括用于指示所述SCP网元停止对所述第二网元的消息转发；所述第四网元为NRF网元，向所述NRF网元发送所述NRF网元对应的第二安全策略，所述NRF网元对应的第二安全策略包括用于指示所述NRF网元停止对所述第二网元的用户授权；所述第四网元为SDN网元，向所述SDN网元发送所述SDN网元对应的第二安全策略，所述SDN网元对应的第二安全策略包括用于指示所述SDN网元停止对所述第二网元的网段的消息的路由转发。

[0233] 如图9所示，为本申请实施例提供的一种网络事件处理装置示意图，该装置可以是上述实施例中的NWDAF网元和/或SPF网元。该装置900包括：处理器902和通信接口903，可选的，装置900还可以包括存储器901。可选的，装置900还可以包括通信线路904。其中，通信接口903、处理器902以及存储器901可以通过通信线路904相互连接；通信线路904可以是外设部件互连标准(peripheral component interconnect，简称PCI)总线或扩展工业标准结构(extended industry standard architecture，简称EISA)总线等。所述通信线路904可以分为地址总线、数据总线、控制总线等。为便于表示，图9中仅用一条粗线表示，但并不表示仅有一根总线或一种类型的总线。

[0234] 处理器902可以是一个CPU，微处理器，ASIC，或一个或多个用于控制本申请实施例方案程序执行的集成电路。

[0235] 处理器902，可以用于根据K个第一网元的消息交互行为信息，确定出第二网元发生网络安全异常事件；所述网络数据分析功能网元向SPF网元发送第一指示信息，所述第一指示信息用于指示所述第二网元发生所述网络安全异常事件；和/或，根据所述第一指示信息，确定出与所述第二网元具有关联关系的N个第三网元；针对所述N个第三网元中的一个第三网元，所述第三网元具有对所述第二网元的业务进行处理的能力；针对所述N个第三网元中的一个第三网元。

[0236] 通信接口903，使用任何收发器一类的装置，用于与其他设备或通信网络通信，如

以太网,无线接入网(radio access network,RAN),无线局域网(wireless local area networks,WLAN),有线接入网等。

[0237] 通信接口903,可以用于获取K个第一网元的消息交互行为信息,针对所述K个第一网元中的一个第一网元,所述第一网元的消息交互行为信息包括用于指示所述第一网元传输的消息的属性信息;所述K为正整数;或者,用于接收网络数据分析功能网元发送的第一指示信息,所述第一指示信息用于指示所述第二网元发生网络安全异常事件;所述SPF网元所述SPF网元向所述第三网元发送所述第三网元对应的第一安全策略,所述第三网元对应的第一安全策略中包括用于指示所述第三网元对所述第二网元对应的业务进行隔离的指示信息。

[0238] 其中,上述方案的具体实现将在后续方法实施例中详细阐述,在此不予赘述。

[0239] 存储器901可以是ROM或可存储静态信息和指令的其他类型的静态存储设备,RAM或者可存储信息和指令的其他类型的动态存储设备,也可以是电可擦可编程只读存储器(electrically erasable programmable read-only memory,EEPROM)、只读光盘(compact disc read-only memory,CD-ROM)或其他光盘存储、光碟存储(包括压缩光碟、激光碟、光碟、数字通用光碟、蓝光光碟等)、磁盘存储介质或者其他磁存储设备、或者能够用于携带或存储具有指令或数据结构形式的期望的程序代码并能够由计算机存取的任何其他介质,但不限于此。存储器可以是独立存在,通过通信线路904与处理器相连接。存储器也可以和处理器集成在一起。

[0240] 其中,存储器901用于存储执行本申请实施例方案的计算机执行指令,并由处理器902来控制执行。处理器902用于执行存储器901中存储的计算机执行指令,从而实现本申请实施例上述实施例提供的网络事件处理方法。

[0241] 可选的,本申请实施例中的计算机执行指令也可以称之为应用程序代码,本申请实施例对此不作具体限定。

[0242] 在本申请的描述中,除非另有说明,“/”表示前后关联的对象是一种“或”的关系,例如,A/B可以表示A或B;本申请中的“和/或”仅仅是一种描述关联对象的关联关系,表示可以存在三种关系,例如,A和/或B,可以表示:单独存在A,同时存在A和B,单独存在B这三种情况,其中A,B可以是单数或者复数。并且,在本申请的描述中,除非另有说明,“多个”是指两个或多于两个。“以下至少一项(个)”或其类似表达,是指的这些项中的任意组合,包括单项(个)或复数项(个)的任意组合。例如,a,b,或c中的至少一项(个),可以表示:a,b,c,a-b,a-c,b-c,或a-b-c,其中a,b,c可以是单个,也可以是多个。另外,为了便于清楚描述本申请实施例的技术方案,在本申请的实施例中,采用了“第一”、“第二”等字样对功能和作用基本相同的相同项或相似项进行区分。本领域技术人员可以理解“第一”、“第二”等字样并不对数量和执行次序进行限定,并且“第一”、“第二”等字样也并不限定一定不同。同时,在本申请实施例中,“示例性的”或者“例如”等词用于表示作例子、例证或说明。本申请实施例中被描述为“示例性的”或者“例如”的任何实施例或设计方案不应被解释为比其它实施例或设计方案更优选或更具优势。确切而言,使用“示例性的”或者“例如”等词旨在以具体方式呈现相关概念,便于理解。

[0243] 此外,本申请实施例描述的网络架构以及业务场景是为了更加清楚的说明本申请实施例的技术方案,并不构成对于本申请实施例提供的技术方案的限定,本领域普通技术

人员可知,随着网络架构的演变和新业务场景的出现,本申请实施例提供的技术方案对于类似的技术问题,同样适用。

[0244] 在上述实施例中,可以全部或部分地通过软件、硬件、固件或者其任意组合来实现。当使用软件实现时,可以全部或部分地以计算机程序产品的形式实现。所述计算机程序产品包括一个或多个计算机指令。在计算机上加载和执行所述计算机程序指令时,全部或部分地产生按照本申请实施例所述的流程或功能。所述计算机可以是通用计算机、专用计算机、计算机网络、或者其他可编程装置。所述计算机指令可以存储在计算机可读存储介质中,或者从一个计算机可读存储介质向另一个计算机可读存储介质传输,例如,所述计算机指令可以从一个网站站点、计算机、服务器或数据中心通过有线(例如同轴电缆、光纤、数字用户线(DSL))或无线(例如红外、无线、微波等)方式向另一个网站站点、计算机、服务器或数据中心进行传输。所述计算机可读存储介质可以是计算机能够存取的任何可用介质或者是包括一个或多个可用介质集成的服务器、数据中心等数据存储设备。所述可用介质可以是磁性介质,(例如,软盘、硬盘、磁带)、光介质(例如,DVD)、或者半导体介质(例如固态硬盘(Solid State Disk,SSD))等。

[0245] 本申请实施例中所描述的各种说明性的逻辑单元和电路可以通过通用处理器,数字信号处理器,专用集成电路(ASIC),现场可编程门阵列(FPGA)或其它可编程逻辑装置,离散门或晶体管逻辑,离散硬件部件,或上述任何组合的设计来实现或操作所描述的功能。通用处理器可以为微处理器,可选地,该通用处理器也可以为任何传统的处理器、控制器、微控制器或状态机。处理器也可以通过计算装置的组合来实现,例如数字信号处理器和微处理器,多个微处理器,一个或多个微处理器联合一个数字信号处理器核,或任何其它类似的配置来实现。

[0246] 本申请实施例中所描述的方法或算法的步骤可以直接嵌入硬件、处理器执行的软件单元、或者这两者的结合。软件单元可以存储于RAM存储器、闪存、ROM存储器、EPROM存储器、EEPROM存储器、寄存器、硬盘、可移动磁盘、CD-ROM或本领域中其它任意形式的存储媒介中。示例性地,存储媒介可以与处理器连接,以使得处理器可以从存储媒介中读取信息,并可以向存储媒介存写信息。可选地,存储媒介还可以集成到处理器中。处理器和存储媒介可以设置于ASIC中。

[0247] 这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上,使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理,从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

[0248] 尽管结合具体特征及其实施例对本申请进行了描述,显而易见的,在不脱离本申请的精神和范围的情况下,可对其进行各种修改和组合。相应地,本说明书和附图仅仅是所附权利要求所界定的本申请的示例性说明,且视为已覆盖本申请范围内的任意和所有修改、变化、组合或等同物。显然,本领域的技术人员可以对本申请进行各种改动和变型而不脱离本申请的范围。这样,倘若本申请的这些修改和变型属于本申请权利要求及其等同技术的范围之内,则本申请也意图包括这些改动和变型在内。

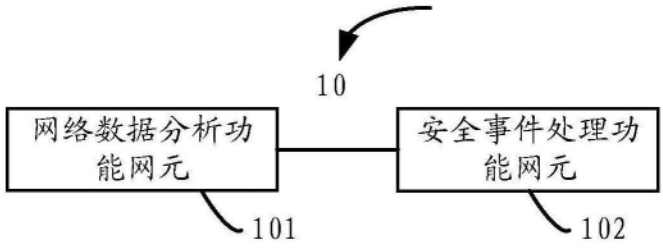

10
网络数据分析功能网元
安全事件处理功能网元
101
102

图1

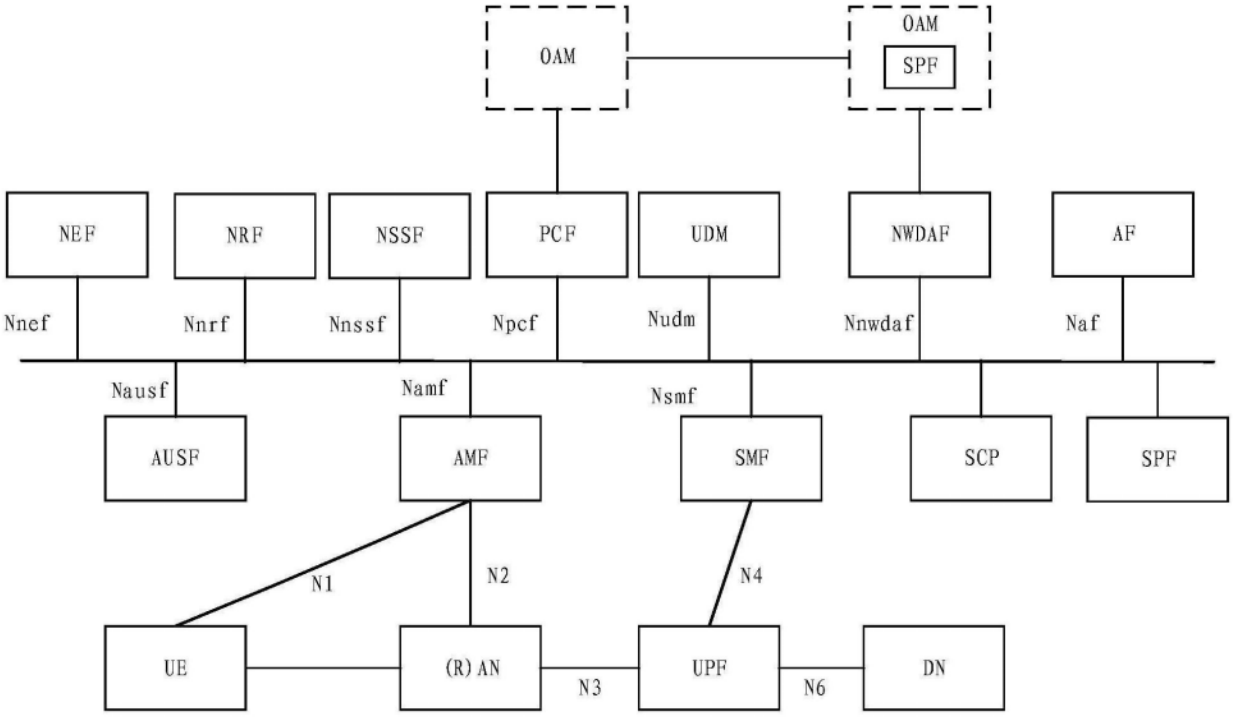

OAM
OAM
SPF
NEF
NRF
NSSF
PCF
UDM
NWDAF
AF
Nnef
Nnrf
Nnssf
Npcf
Nudm
Nnwdaf
Naf
Nausf
Namf
Nsmf
AUSF
AMF
SMF
SCP
SPF
N1
N2
N4
UE
(R)AN
UPF
DN
N3
N6

图2

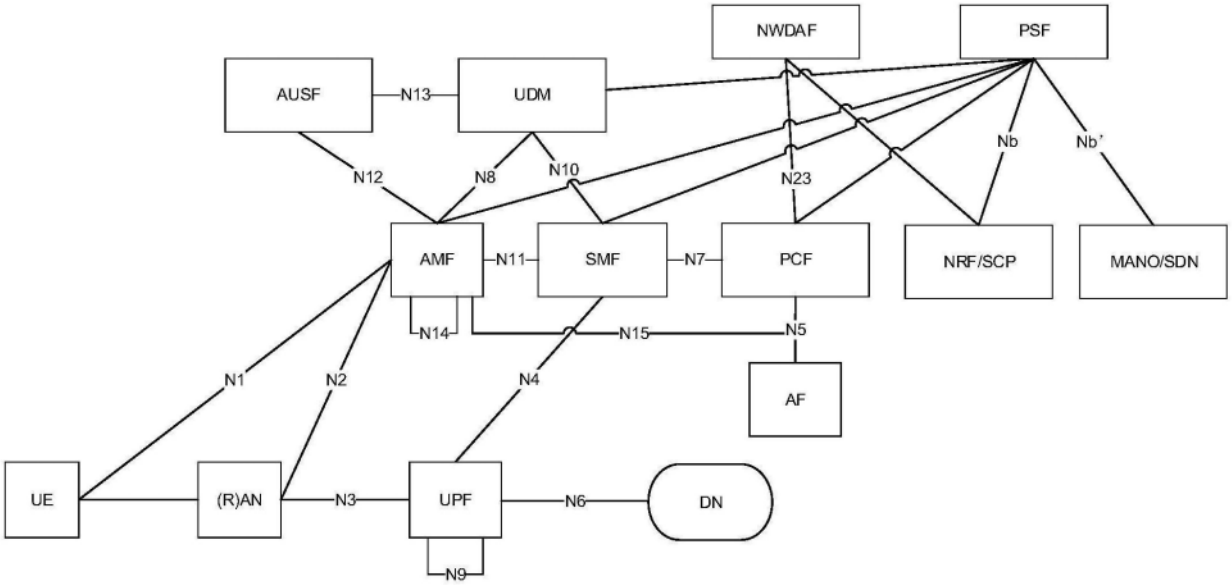

NWDAF
PSF
AUSF
N13
UDM
N12
N8
N10
N23
Nb
Nb'
AMF
N11
SMF
N7
PCF
NRF/SCP
MANO/SDN
N14
N15
N5
AF
N1
N2
N4
UE
(R)AN
N3
UPF
N6
DN
N9

图3

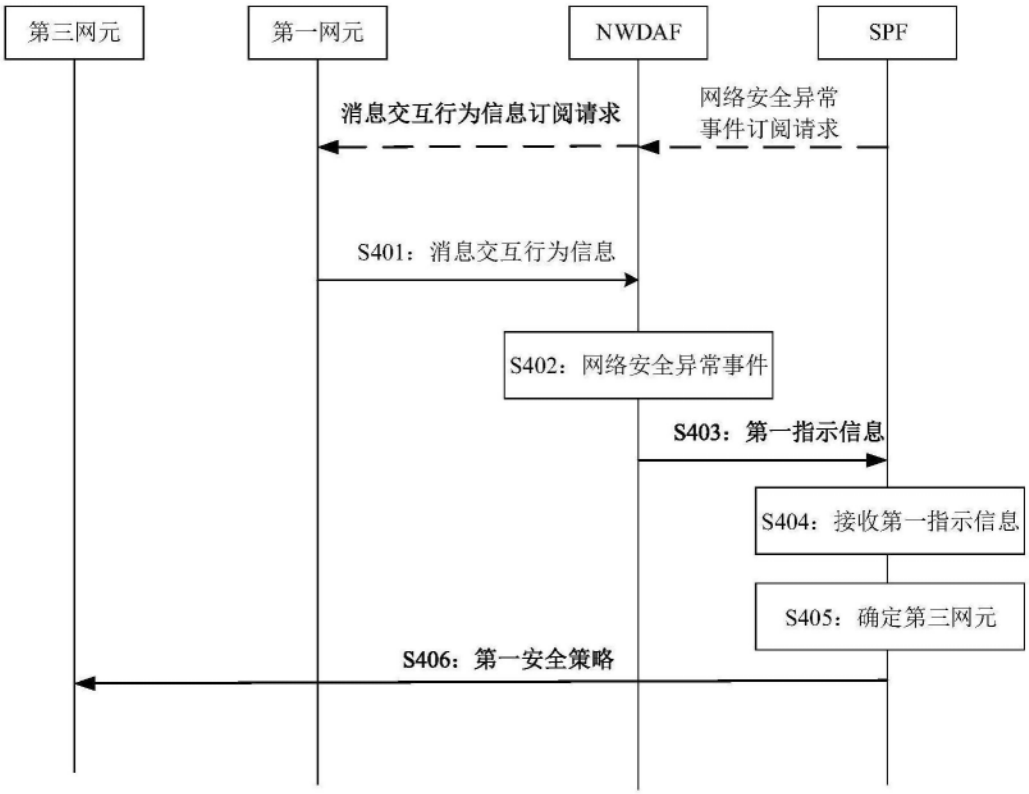

第三网元
第一网元
NWDAF
SPF
消息交互行为信息订阅请求
网络安全异常
事件订阅请求
S401：消息交互行为信息
S402：网络安全异常事件
S403：第一指示信息
S404：接收第一指示信息
S405：确定第三网元
S406：第一安全策略

图4

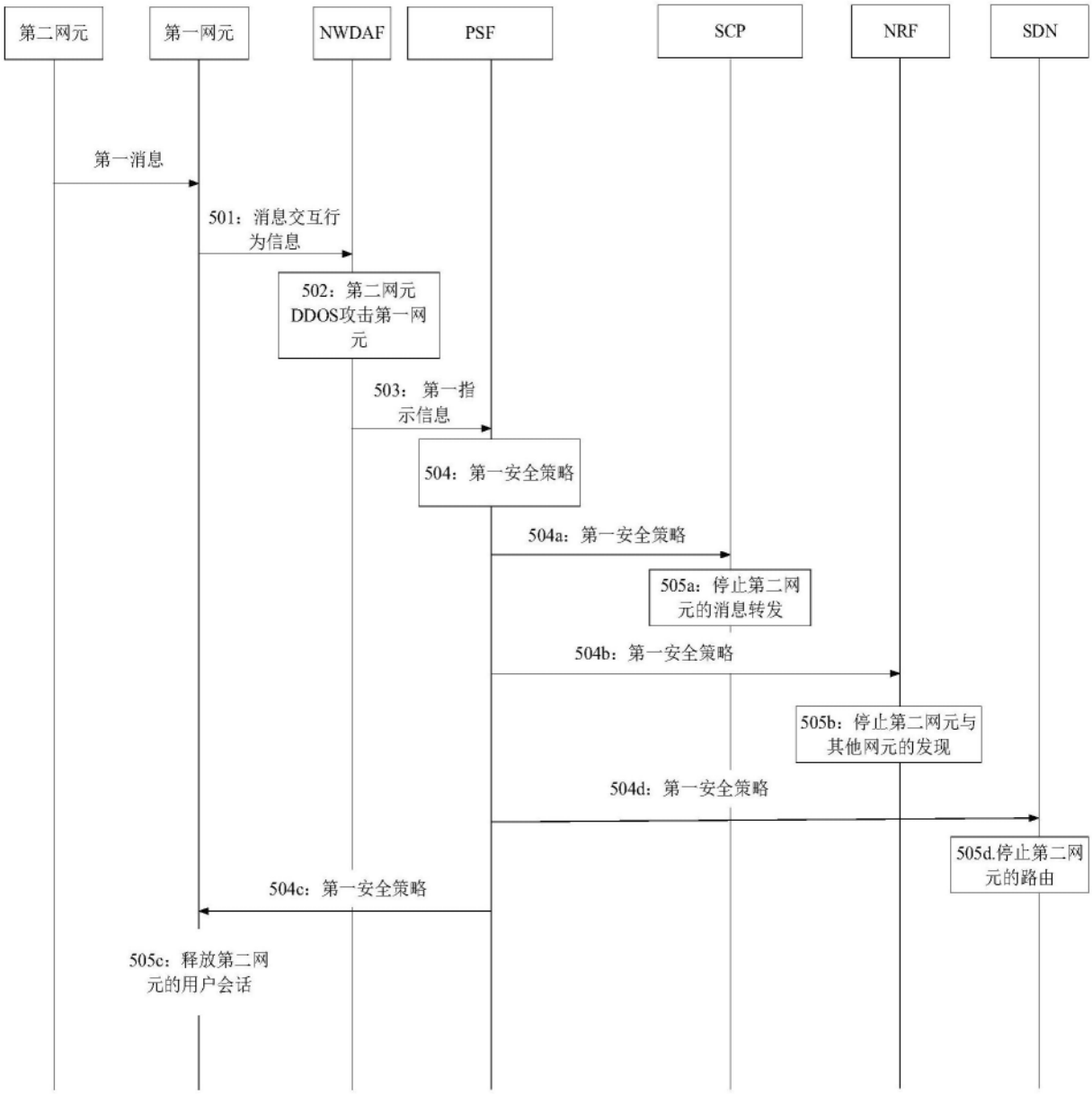

第二网元
第一网元
NWDAF
PSF
SCP
NRF
SDN
第一消息
501：消息交互行为信息
502：第二网元DDOS攻击第一网元
503：第一指示信息
504：第一安全策略
504a：第一安全策略
505a：停止第二网元的消息转发
504b：第一安全策略
505b：停止第二网元与其他网元的发现
504d：第一安全策略
505d.停止第二网元的路由
504c：第一安全策略
505c：释放第二网元的用户会话

图5

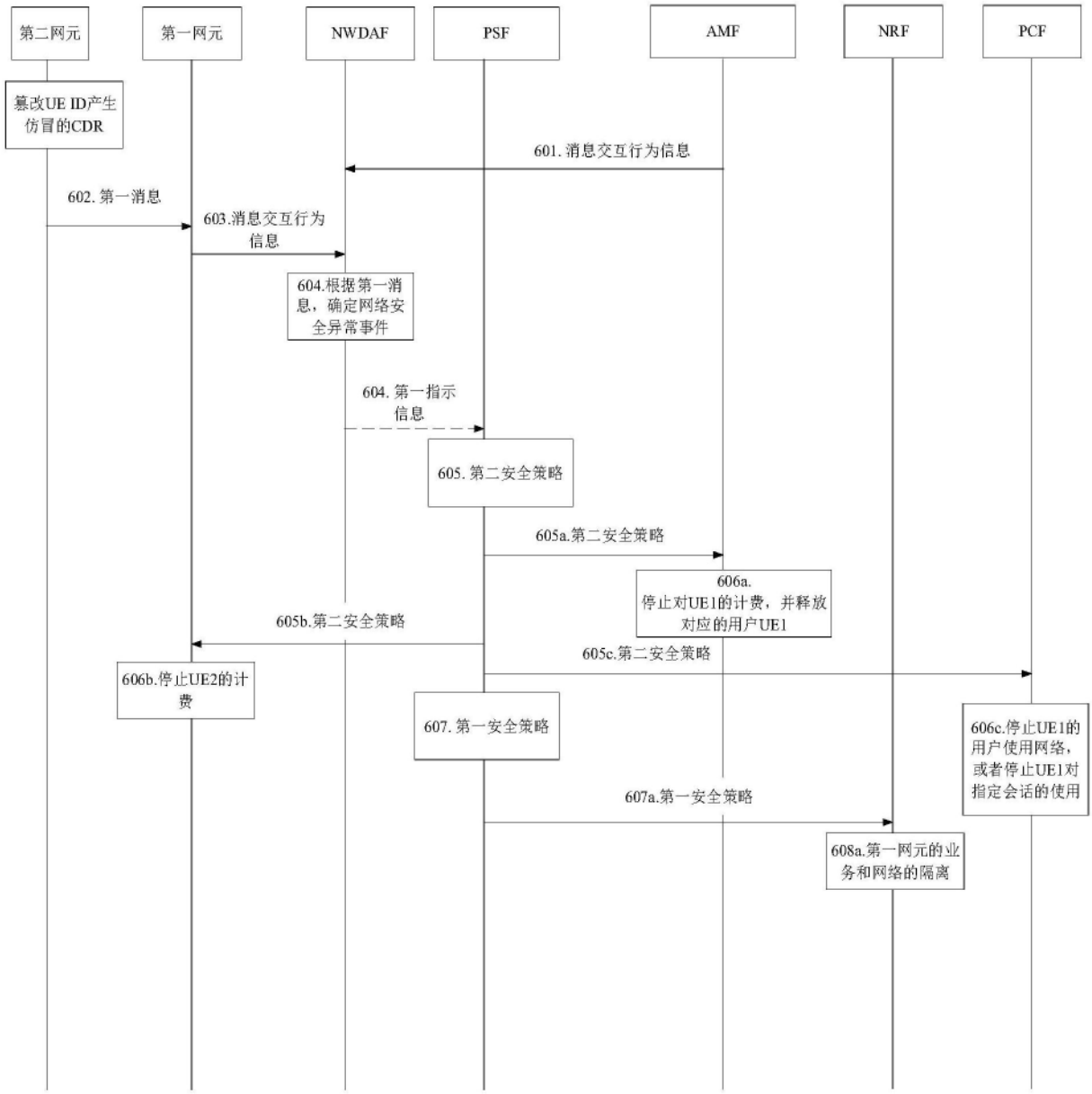

第二网元
第一网元
NWDAF
PSF
AMF
NRF
PCF
篡改UE ID产生仿冒的CDR
601. 消息交互行为信息
602. 第一消息
603.消息交互行为信息
604.根据第一消息，确定网络安全异常事件
604. 第一指示信息
605. 第二安全策略
605a.第二安全策略
606a.
停止对UE1的计费，并释放对应的用户UE1
605b.第二安全策略
605c.第二安全策略
606b.停止UE2的计费
607. 第一安全策略
606c.停止UE1的用户使用网络，或者停止UE1对指定会话的使用
607a.第一安全策略
608a.第一网元的业务和网络的隔离

图6

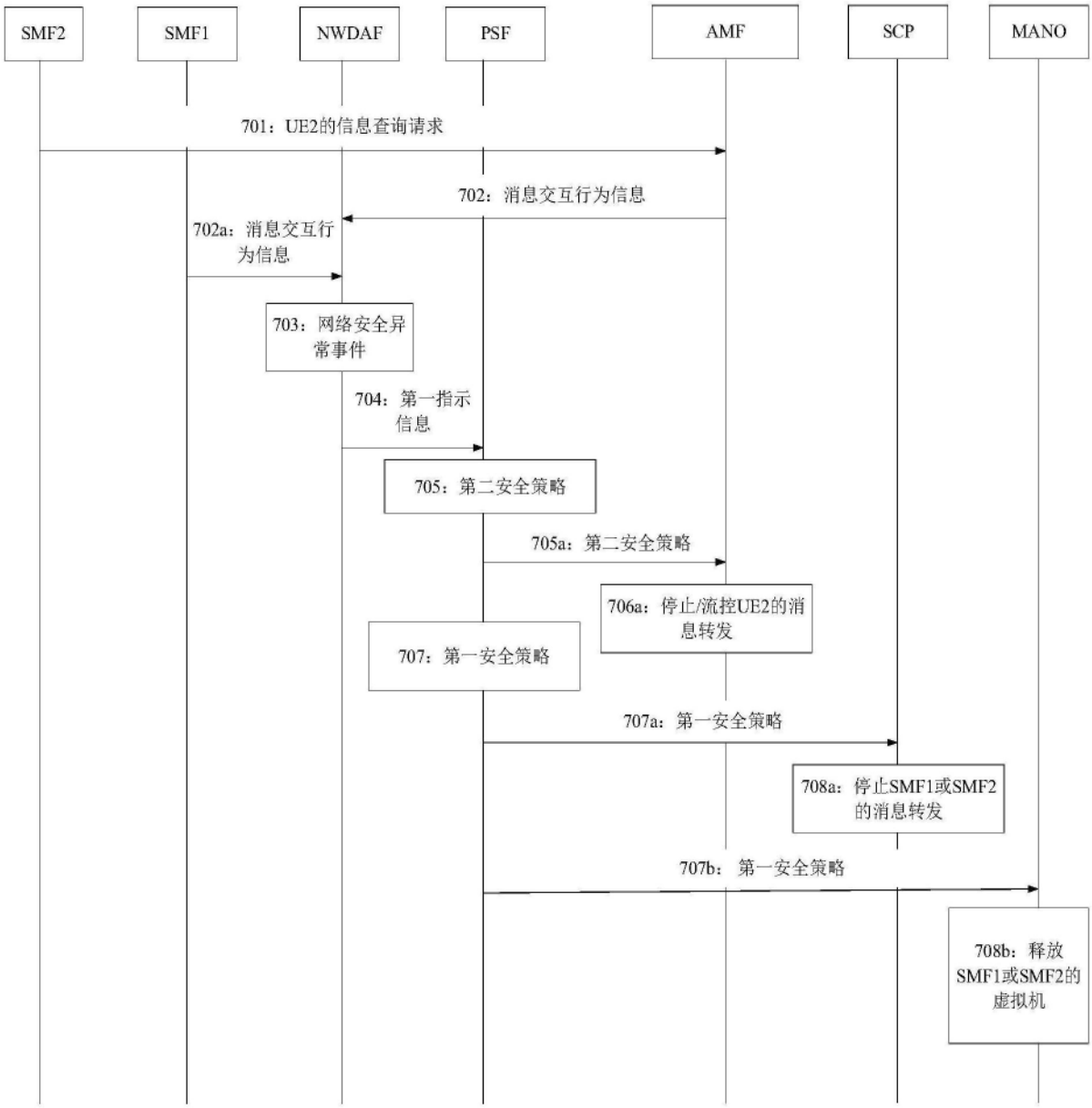

SMF2
SMF1
NWDAF
PSF
AMF
SCP
MANO
701：UE2的信息查询请求
702：消息交互行为信息
702a：消息交互行为信息
703：网络安全异常事件
704：第一指示信息
705：第二安全策略
705a：第二安全策略
706a：停止/流控UE2的消息转发
707：第一安全策略
707a：第一安全策略
708a：停止SMF1或SMF2的消息转发
707b：第一安全策略
708b：释放SMF1或SMF2的虚拟机

图7

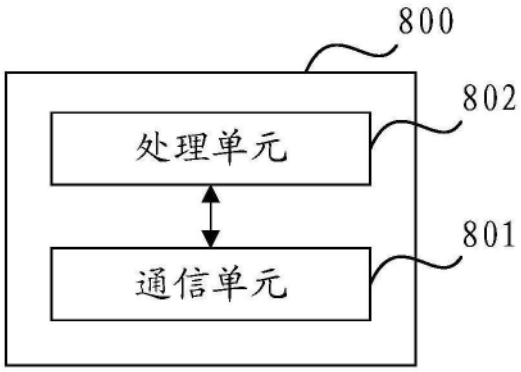


图8

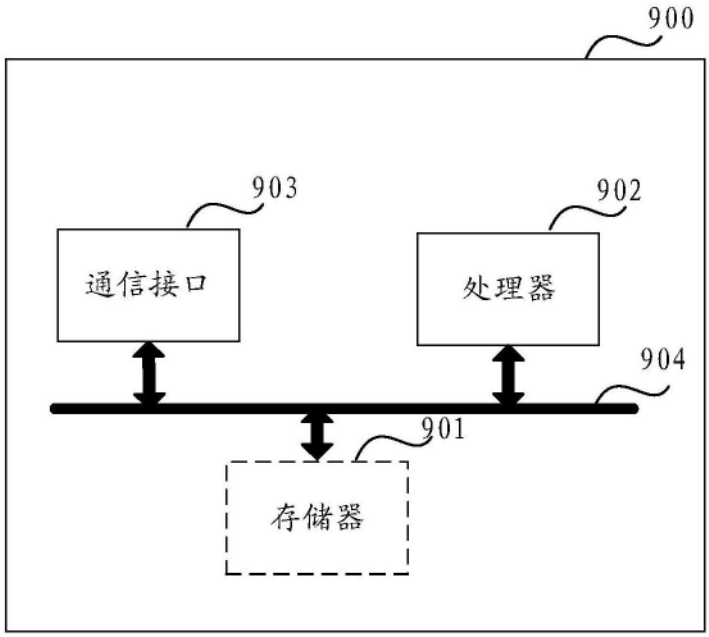


图9