(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 108370368 B
(45)授权公告日 2020.04.21

(21)申请号 201680073792.2

(22)申请日 2016.09.20

(65)同一申请的已公布的文献号
申请公布号 CN 108370368 A

(43)申请公布日 2018.08.03

(85)PCT国际申请进入国家阶段日
2018.06.20

(86)PCT国际申请的申请数据
PCT/CN2016/099455 2016.09.20

(87)PCT国际申请的公布数据
WO2018/053686 ZH 2018.03.29

(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 林青春 靳涛 王江胜

(74)专利代理机构 北京弘权知识产权代理事务所(普通合伙) 11363
代理人 逯长明 许伟群

(51)Int.Cl.
H04L 29/02(2006.01)

(56)对比文件
CN 105847237 A,2016.08.10,
CN 105376246 A,2016.03.02,

审查员 兰慧敏

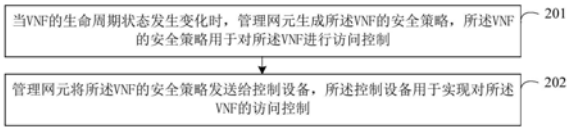
权利要求书2页 说明书10页 附图2页

(54)发明名称

安全策略部署方法与装置

(57)摘要

本申请提供了安全策略发送方法及装置,所述方法包括:当虚拟网络功能VNF的生命周期状态发生变化时,管理网元生成所述VNF的安全策略,所述VNF的安全策略用于对所述VNF进行访问控制;所述管理网元将所述VNF的安全策略发送给控制设备。其中,所述管理网元时用于对所述VNF进行生命周期管理的网元、采用本申请实施例所述提供的方法或装置,可以在VNF的生命周期状态发生变化时,及时调整VNF的安全策略,大大减少因为VNF发生变化而导致VNF安全策略出现漏洞的可能性。



CN 108370368 B

1.一种安全策略部署方法,其特征在于,包括:

当虚拟网络功能VNF的生命周期状态发生变化时,管理网元生成所述VNF的安全策略,所述VNF的安全策略用于对所述VNF进行访问控制;

所述管理网元将所述VNF的安全策略发送给控制设备,所述控制设备用于实现对所述VNF的访问控制;

当所述VNF部署在至少两个虚拟部件上时,所述安全策略包括第一安全策略,所述第一安全策略用于对所述至少两个虚拟部件之间进行访问控制或安全隔离。

2.如权利要求1所述的方法,其特征在于,所述管理网元生成所述VNF的安全策略,包括:

所述管理网元根据所述虚拟部件所要实现的功能确定所述虚拟部件之间的网络隔离需求,并生成与所述虚拟部件的网络隔离需求相匹配的所述第一安全策略;或者,

所述管理网元根据所述虚拟部件所要实现的功能确定所述虚拟部件的访问控制需求,并生成与所述访问控制需求相匹配的所述第一安全策略;或者,

所述管理网元获取所述VNF的配置信息,并从预设的备选安全策略中选取与所述配置信息相匹配的一个作为所述第一安全策略。

3.如权利要求1或2所述的方法,其特征在于,所述控制设备为所述VNF,所述管理网元将所述VNF的安全策略发送给控制设备,包括:

所述管理网元将所述第一安全策略经由虚拟基础设施管理器VIM发送给所述VNF;或者,

所述管理网元将所述第一安全策略经由网元管理系统EMS发送给所述VNF。

4.如权利要求1或2所述的方法,其特征在于,所述安全策略还包括第二安全策略,所述第二安全策略用于对所述VNF与关联网元之间进行访问控制或安全隔离,其中,所述关联网元是指所述VNF所属网络中除所述VNF之外的其他网元。

5.如权利要求4所述的方法,其特征在于,所述管理网元生成第二安全策略,包括:

所述管理网元根据所述VNF所要实现的功能确定所述VNF之间的网络隔离需求,并生成与所述VNF的网络隔离需求相匹配的所述第二安全策略;或者,

所述管理网元根据所述VNF所要实现的功能,确定所述VNF的访问控制需求,并生成与所述访问控制需求相匹配的所述第二安全策略。

6.如权利要求4或5所述的方法,其特征在于,所述控制设备为向所述VNF提供网络服务的网关设备,所述管理网元将所述VNF的安全策略发送给控制设备,包括:

所述管理网元将所述第二安全策略经由VIM发送给所述网关设备,或者,

所述管理网元将所述第二安全策略经由EMS发送给所述网关设备。

7.一种安全策略部署装置,其特征在于,包括:

生成单元,用于当虚拟网络功能VNF的生命周期状态发生变化时,生成所述VNF的安全策略,所述VNF的安全策略用于对所述VNF进行访问控制;

发送单元,用于将所述VNF的安全策略发送给控制设备,所述控制设备用于实现对所述VNF的访问控制;

其中,当所述VNF部署在至少两个虚拟部件上时,所述安全策略包括第一安全策略,所述第一安全策略用于对所述至少两个虚拟部件之间进行访问控制或安全隔离。

8.如权利要求7所述的装置,其特征在于,

所述生成单元,具体用于根据所述虚拟部件所要实现的功能确定所述虚拟部件之间的网络隔离需求,并生成与所述虚拟部件的网络隔离需求相匹配的所述第一安全策略;或者,根据所述虚拟部件所要实现的功能,确定所述虚拟部件的访问控制需求,并生成与所述访问控制需求相匹配的所述第一安全策略;或者,获取所述VNF的配置信息,并从预设的备选安全策略中选取与所述配置信息相匹配的一个作为所述第一安全策略。

9.如权利要求7或8所述的装置,其特征在于,

所述发送单元,具体用于当所述控制设备为所述VNF时,将所述第一安全策略经由虚拟基础设施管理器VIM或网元管理系统EMS发送给所述VNF。

10.如权利要求7所述的装置,其特征在于,

所述安全策略还包括第二安全策略,所述第二安全策略用于对所述VNF与关联网元之间进行访问控制或安全隔离,其中,所述关联网元是指所述VNF所属网络中除所述VNF之外的其他网元。

11.如权利要求10所述的装置,其特征在于,

所述生成单元,具体用根据所述VNF所要实现的功能确定所述VNF之间的网络隔离需求,并生成与所述VNF的网络隔离需求相匹配的所述第二安全策略;或者,根据所述VNF所要实现的功能,确定所述VNF的访问控制需求,并生成与所述访问控制需求相匹配的所述第二安全策略。

12.如权利要求10或11所述的装置,其特征在于,

所述发送单元,具体用于当所述控制设备为向所述VNF提供网络服务的网关设备时,将所述第二安全策略经由VIM或EMS发送给所用于为所述VNF提供网络服务的网关设备。

安全策略部署方法与装置

技术领域

[0001] 本申请涉及网络领域，尤其涉及安全策略部署方法与装置。

背景技术

[0002] 传统网络系统是指利用将多个地理位置不同、功能独立的多个网络设备互联起来，以实现资源共享或信息传递的系统。由于传统网络系统由于在部署完成之后，其所包含网络设备及各个网络设备之间的网络连接关系相对固定，因而很难对其所提供的网络服务(network service，简称NS)进行调整。

[0003] 为便于根据实际需要对NS进行调整，越来越多使用者开始使用网络功能虚拟化(network function virtualisation，简称NFV)技术利用网络功能虚拟化基础设施(network functions virtualisation infrastructure，简称NFVI)来构建网络系统。在采用NFV技术构建的网络系统中，虚拟网络功能管理器(virtualised network function manager，简称VNFM)可以根据网络系统所要实现的NS创建、调整或终止相应的虚拟化网络功能(virtualised network function，简称VNF)；网络功能虚拟化编排器(network functions virtualisation orchestrator，简称NFVO)则可以对VNF进行重排以实现对NS的调整。

[0004] 为保证网络系统能够安全平稳运行，传统网络系统中的网络设备必须配置有相应的安全策略，网络设备可以根据安全策略进行访问控制，以方式。由于传统网络所包含网络设备及各个网络设备之间的网络连接关系相对固定，因此在为传统网络系统中的网络设备配置安全策略时，在网络系统的规划和设计阶段，可以由技术人员考虑根据网络设备的类型及网络设备之间的连接关系为各个网络设备设计相应的安全策略；然后在安装部署各个网络设备时，由技术人员手动将安全策略下发至相应的网络设备，从而实现网络设备的安全策略配置。

[0005] 在采用NFV技术构建的网络系统中，各个VNF及NS也必须配置有相应的安全策略。但是在采用NFV技术构建的网络系统中，各个VNF都存在一定的生命周期(lifecycle)。在生命周期管理过程中确定VNF可能会不断发生变化。例如，VNF所包含的组件、VNF所包含组件之间的连接关系、以及VNF之间的连接关系，可能在会随着生命周期管理的过程而不断发生变化。

[0006] 如果采用传统网络系统中的安全策略配置方式，由技术人员手动为采用NFV技术构建的网络系统中的VNF配置安全策略，很可能会因为技术人员未能及时发现VNF的变化，或因为技术人员未能对在VNF发生变化后，未能即使对VNF的安全策略进行调整，从而导致VNF的安全策略出现漏洞，影响网络系统的安全性。

发明内容

[0007] 本申请提供了安全策略部署方法与装置，以解决采用传统方式为网络系统中的VNF配置安全策略，容易导致VNF的安全策略出现漏洞的问题。

[0008] 第一方面，本申请提供了一种安全策略部署方法，该方法包括：当虚拟网络功能VNF的生命周期状态发生变化时，管理网元生成所述VNF的安全策略，所述VNF的安全策略用于对所述VNF进行访问控制；所述管理网元将所述VNF的安全策略发送给控制设备，所述控制设备用于实现对所述VNF的访问控制。其中，所述管理网元可以包括VNFM或NFVO，所述控制设备可以包括所述VNF或用于为所述VNF提供网络访问的网关设备。采用本方面所提供的技术方案，管理网元可以在VNF的生命周期状态发生变化时，及时调整VNF的安全策略，大大减少因为VNF发生变化而导致VNF安全策略出现漏洞的可能性。

[0009] 结合第一方面，在第一方面第一种可能的实现方式中，当所述VNF部署在至少两个虚拟部件上时，所述安全策略包括第一安全策略，所述第一安全策略用于对所述至少两个虚拟部件之间进行访问控制或安全隔离。采用本实现方式所提供的技术方案，管理网元可以在VNF自身发生变化时，及时调整VNF的安全策略，从减少因VNF自身发生变化而导致VNF安全策略出现漏洞的可能性。

[0010] 结合第一方面第一种可能的实现方式，在第一方面第二种可能的实现方式中，所述管理网元生成所述VNF的安全策略，包括：所述管理网元根据所述虚拟部件所要实现的功能确定所述虚拟部件之间的网络隔离需求，并生成与所述虚拟部件的网络隔离需求相匹配的所述第一安全策略；或者，所述管理网元根据所述虚拟部件所要实现的功能确定所述虚拟部件的访问控制需求，并生成与所述访问控制需求相匹配的所述第一安全策略；或者，所述管理网元获取所述VNF的配置信息，并从预设的备选安全策略中选取与所述配置信息相匹配的一个作为所述第一安全策略。采用本实现方式所提供的技术方案，管理网元可以准确生成在发生生命周期状态变化后，所述VNF所需的安全策略，进一步降低VNF的安全策略出现漏洞的可能性。

[0011] 结合第一方面第一种可能的实现方式或第一方面第二种可能的实现方式，在第一方面第三种可能的实现方式中，所述控制设备为所述VNF，所述管理网元将所述VNF的安全策略发送给控制设备，包括：所述管理网元将所述第一安全策略经由虚拟基础设施管理器VIM发送给所述VNF；或者，所述管理网元将所述第一安全策略经由网元管理系统EMS发送给所述VNF。采用本实现方式所提供的技术方案，管理网元可以快速实现安全策略的部署，从而进一步降低VNF的安全策略出现漏洞的可能性。

[0012] 结合第一方面或第一方面第一至三种可能的实现方式其中任一种，在第一方面第四种可能的实现方式中，所述安全策略包括第二安全策略，所述第二安全策略用于对所述VNF与关联网元之间进行访问控制或安全隔离，其中，所述关联网元是指所述VNF所属网络中除所述VNF之外的其他网元。采用本实现方式所提供的技术方案，管理网元可以在VNF与关联网元之间的关系发生变化时，及时调整VNF的安全策略，从减少因VNF与关联网元之间的关系发生变化而导致VNF安全策略出现漏洞的可能性。

[0013] 结合第一方面第四种可能的实现方式，在第一方面第五种可能的实现方式中，所述管理网元生成第二安全策略，包括：所述管理网元根据所述VNF所要实现的功能确定所述VNF之间的网络隔离需求，并生成与所述VNF的网络隔离需求相匹配的所述第二安全策略；或者，所述管理网元根据所述VNF所要实现的功能，确定所述VNF的访问控制需求，并生成与所述访问控制需求相匹配的所述第二安全策略。采用本实现方式所提供的技术方案，管理网元可以准确生成在发生生命周期状态变化后，所述VNF所需的安全策略，进一步降低VNF

的安全策略出现漏洞的可能性。

[0014] 结合第一方面第四或五种可能的实现方式，在第一方面第六种可能的实现方式中，所述控制设备为向所述VNF提供网络服务的网关设备，所述管理网元将所述VNF的安全策略发送给控制设备，包括：所述管理网元将所述第二安全策略经由VIM发送给所述网关设备，或者，所述管理网元将所述第二安全策略经由EMS发送给所述网关设备。采用本实现方式所提供的技术方案，管理网元可以快速实现安全策略的部署，从而进一步降低VNF的安全策略出现漏洞的可能性。

[0015] 第二方面，本申请还提供了一种安全策略部署装置，该装置可以包括用于执行前述第一方面及第一方面各种实现方式中方法步骤的单元模块。

[0016] 第三方面，本申请还提供了另一管理网元，该管理网元可以用于执行前述第一方面或第一方面各实现方式中的方法步骤。其中，所述管理网元可以为

[0017] 采用本申请实施例所述提供的方法或装置，可以在VNF的生命周期状态发生变化时，及时调整VNF的安全策略，大大减少因为VNF发生变化而导致VNF安全策略出现漏洞的可能性。

附图说明

[0018] 为了更清楚地说明本申请的技术方案，下面将对实施例中所需要使用的附图作简单地介绍，显而易见地，对于本领域普通技术人员而言，在不付出创造性劳动性的前提下，还可以根据这些附图获得其他的附图。

[0019] 图1为本申请网络系统的一个结构示意图；

[0020] 图2为本申请安全策略配置方法一个实施例的流程示意图；

[0021] 图3为本申请安全策略配置方法另一个实施例的流程示意图；

[0022] 图4为本申请安全策略配置方法另一个实施例的流程示意图；

[0023] 图5为本申请安全策略配置装置一个实施例的结构示意图；

[0024] 图6为本申请管理网元一个实施例的结构示意图。

具体实施方式

[0025] 本申请各个实施例中的网络系统可以是指利用虚拟基础设施管理器(virtualised infrastructure manager，简称VIM)等设备所管理的网络功能虚拟化基础设施(network functions virtualisation infrastructure，简称NFVI)所创建的网络系统。

[0026] 在本申请各个实施例中，部件网络功能管理器(virtualised network function manager，简称VNFM)可以利用NFVI生成一定数量的部件网络功能(virtualised network function，简称VNF)并对VNF进行生命周期管理。网络功能虚拟化编排器(network functions virtualisation orchestrator，简称NFVO)则可以通过VNFM对所述VNF及其对应的NFVI进行部署，操作，管理及协调，以实现一定的网络服务(network service，简称NS)。

[0027] 在本申请各个实施例中，VNF可以部署在一个或一个以上的部件上，所述部件可以单独实现一定的功能，也可以通过相互配合实现一定的功能，例如，所述部件可以单独或互

相配合以实现数据处理、数据存储等功能，从而使得所述VNF可以实现一定的网络服务(network service，简称NS)。通常情况下，每一个所述NS可以由至少一个VNF来实现，同一个VNF也可以用于实现不同NS。因此也可以认为，每一个NS包含至少一个VNF或每一个NS由至少一个VNF组成。其中，所述部件可以为实体部件，例如服务器，或者也可以虚拟部件，例如虚拟机(virtual machine，简称VM)。

[0028] 在本申请各个实施例中，VNF的生命周期状态发生变化可以包括：VNF实例化(VNF instantiation)，VNF缩容(VNF scale-in)，VNF扩容(VNF scale-out)，VNF下线(VNF termination)等。其中，VNF被创建，VNF被变更及VNF被重排，其中，VNF实例化可以是指VNF被创建是，即VNF被VNFM利用NFVI创建出来；VNF缩容(VNF scale-in)与VNF扩容(VNF scale-out)是指VNF被变更，即VNF中的部件被增加、减少或调整，或VNF所要实现的NS被调整，或者VNF与其他网元之间的关系被调整。其中，VNF中的部件可以是指用于部署所述VNF的部件。

[0029] 参见图1，为本申请网络系统一个实施例的结构示意图。

[0030] 如图1所示，网络系统可以包括第一VNF、第二VNF及第三VNF，所述第一VNF、第二VNF及所述第三VNF均与网关设备连接。其中，所述网关设备用于为所述VNF提供网络服务，可以为虚拟网关设备，也可以为实体网关设备，例如，所述网络服务可以包括：虚拟局域网(virtual local area network，简称VLAN)服务、虚拟专用网络(virtual private network，简称VPN)服务或防火墙服务等；所述虚拟网关设备通常可以包括：虚拟交换机(virtual switch)、虚拟路由器(virtual router)、虚拟防火墙(virtual firewall)等。

[0031] 所述网络系统中的VNF可以部署在多个虚拟设备或实体设备上，例如，图1所示中VNF部署在第一部件、第二部件与第三部件上，其中，第一部件和第二部件相配合用于实现VNF的内部功能，第三部件则用于对外提供服务。因此，所述第一部件与所述第二部件可以构成第一子网，而所述第三部件则可以构成第三子网。所述第一部件、第二部件及第三部件可以均为虚拟部件也可以部分为虚拟部件而部分为实体部件。

[0032] 需要说明的是，上述网络系统还可以包含更多或更少的VNF、网关设备。除所述VNF与所述网关设备之外，所述网络系统还可以包括管理网元、VIM或网元管理系统(element management system，简称EMS)等其他网元。其中，所述管理网元可以是任意能够获知VNF的生命周期状态发生变化的网元，通常情况下所述管理网元可以为VNFM或NFVO，或者也可以为VIM或其他网元。

[0033] 下面结合附图对本申请安全策略部署方法进行进一步说明。

[0034] 参见图2，为本申请安全策略部署方法一个实施例的流程图。

[0035] 步骤201，当VNF的生命周期状态发生变化时，管理网元生成所述VNF的安全策略，所述VNF的安全策略用于对所述VNF进行访问控制。

[0036] 其中，管理网元可以监控VNF的生命周期状态，也可对VNF进行生命周期管理。

[0037] 具体地，管理网元可以对VNF进行生命周期管理，导致VNF的生命周期状态发生变化。例如，管理网元利用NFVI创建第一VNF，又如，管理网元将所述第一VNF中的第四部件替换为第三部件，均会导致第一VNF的生命周期状态发生变化。再如，管理网元将第一VNF由为第二VNF提供服务调整至为第三VNF提供服务，使第一VNF、第二VNF及第三VNF的生命周期状态均发生变化。

[0038] 需要说明的是，上述管理网元对VNF进行生命周期管理，不但会导致VNF的生命周期状态发生变化，而且还会导致VNF对安全策略的需求发生变化。因此管理网元可以在VNF的生命周期状态发生变化时，生成所述VNF的安全策略。其中，所述VNF的安全策略可以包括用于实现VNF免受各类网络攻击的各种策略和规则。

[0039] 例如，当管理网元将所述第一VNF中的第四部件替换为第三部件时，由于所述VNF中的部件发生了变化，所述VNF的安全策略需求也会随之发生变化，因此所述管理网元可以在所述VNF的生命周期状态发生变化时，生成所述VNF的安全策略，以满足所述VNF的安全策略需求。

[0040] 其中，所述VNF的安全策略可以包括第一安全策略和/或第二安全策略。所述第一安全策略用于在VNF部署在至少两个部件上时，对所述部件之间进行访问控制或安全隔离；所述第二安全策略则用于对所述VNF与关联网元之间进行访问控制或安全隔离，其中，所述关联网元是指所述VNF所属网络中除所述VNF之外的其他网元。

[0041] 例如，当网络系统的组成如图1所示时，所述第一安全策略用于对第一部件、第二部件及第三部件之间进行访问控制或安全隔离；而所述第二安全策略则用于对第一VNF、第二VNF及第三VNF之间进行访问控制或安全隔离。其中，所述第一安全策略可以包括访问控制列表(access control list，简称ACL)等；所述第二安全策略则可以包括基于开放式系统互联(open system interconnection，简称OSI)模型的第二层的VLAN策略、基于OSI模型的第三层的VPN策略或用于控制VNF与其他网元之间访问的访问控制策略等。

[0042] 步骤202，管理网元将所述VNF的安全策略发送给控制设备，其中，所述控制设备指是指用于实现对所述VNF的访问控制的网元。

[0043] 所述控制设备可以包括所述VNF本身或者网关设备，其中，所述网关设备为向所述VNF提供网络服务的网关设备，即VNF的服务网关。例如，网络系统的结构如图1所示时，当第一VNF发生生命周期状态变化时，所述控制设备可以包括所述第一VNF与网关设备。

[0044] 所述管理网元可以通过不同的途径将所述VNF的安全策略发送给对应的控制设备。例如，当所述VNF的安全策略包括第一安全策略时，管理网元可以在生成所述第一安全策略之后，将所述第一安全策略发送给所述VNF；当所述VNF的安全策略包括第一安全策略时，管理网元可以在生成所述第二安全策略之后，将所述第二安全策略经发送给所述网关设备。

[0045] 采用本实施例所提供的技术方案，管理网元可以在VNF的生命周期状态发生变化时，及时调整VNF的安全策略，大大减少因为VNF发生变化而导致VNF安全策略出现漏洞的可能性。

[0046] VNF的生命周期状态发生变化可以包括VNF中的部件发生变化，也可以包括VNF所提供的服务或服务的对象发生变化等。根据VNF的生命周期状态发生变化所包括的内容不同，本申请安全策略部署的具体实现方式也不相同，下面结合其它附图对所述VNF的安全策略包含所述第一安全策略及所述安全策略包含所述第二安全策略这两种情况为例，对本申请安全策略部署方法做进一步说明。

[0047] 参见图3，为本申请安全策略部署方法另一个实施例的流程示意图。如图3所示，该实施例可以包括：

[0048] 步骤301，当VNF的生命周期状态发生变化时，管理网元生成第一安全策略。

[0049] VNF的生命周期状态发生变化可以仅包括VNF中的部件发生变化，其中，VNF中的部件发生变化则可以包括部件所要实现的功能发生变化或用于部署所述VNF中的部件发生变化等。以图1为例，第一VNF中的部件发生变化可以包括：第四部件被替换为第三部件，或第一部件与第二部件所要实现的功能发生交换等。

[0050] VNF中的部件发生变化会导致VNF的安全策略需求发生变化。为满足变化后的安全策略需求，所述管理网元可以在VNF的生命周期状态发生变化后，生成第一安全策略。所述第一安全策略可以包括第一网络隔离策略和/或第一访问控制策略等内容。其中，所述第一网络隔离策略实现对所述VNF中的部件之间进行网络隔离，所述第一访问控制策略用于对访问目标为所述部件的访问请求进行访问控制。

[0051] 管理网元可以根据所述VNF中的部件所要实现的功能确定所述部件之间的网络隔离需求；然后生成与所述部件的网络隔离需求相匹配的第一网络隔离策略。或者，所述管理网元也可以根据所述VNF中的部件所要实现的功能确定所述部件之间的问控制需求；然后生成与所述部件之间的访问控制需求相匹配的第一访问控制策略。在此需要说明的是，所述管理网元可以只生成所述第一访问控制策略，或者所述管理网元也可以只生成所述第一网络隔离策略，或者，所述管理网元也可以既生成所述第一访问控制策略又生成第一网络隔离策略，所述第一访问控制策略及所述第一网络隔离策略均为所述第一安全策略。

[0052] 以图1为例，如果第一部件和第二部件相配合用于实现第一VNF的内部功能，第三部件用于对外提供服务，那么需要将第三部件与另外两个部件相隔离，从而在第一VNF内部形成相互隔离的第一子网与第二子网。其中，第一子网可以包含第一部件与第二部件；而第二子网则可以仅包含第三部件。因此所述第一安全策略可以包括用于将第三部件与另外两个部件隔离为不同子网的第一隔离策略。

[0053] 再如，如果在第一子网中只允许第一部件通过第一端口与第二部件进行数据传输，而在第二子网中只允许第三部件通过第二端口与其他网元进行数据传输，那么所述访问控制策略可以包括第一ACL与第二ACL，所述第一ACL用于控制第一部件与第二部件之间的流量只能通过第一端口传输；所述第二ACL用于控制第三部件只能通过第二端口与其他网元进行数据传输。

[0054] 网络隔离需求和/或所述部件之间的问控制需求都可以依据所述第一配置信息确定。其中，所述第一配置信息可以包括：VNF内部部件接口或外部接口上配置的IP地址、所述内部接口或外部接口上所提供的服务、所述内部接口或所述外部接口的连接关系等信息中的全部或部分。

[0055] 在实际使用中，管理网元对所述VNF进行生命周期管理往往需要基于配置信息，同一类VNF所对应的配置信息通常相同，并且所要需要的第一安全策略通常也相同。因此管理网元或其他网元可以预先生成与各类配置信息相对应的备选安全策略；当所述VNF发生生命周期状态变化时，所述管理网元获取所述VNF的配置信息；然后从预设的备选安全策略中选取与所述配置信息相匹配的一个作为所述第一安全策略。

[0056] 步骤302，管理网元将所述第一安全策略发送给所述VNF。

[0057] 由于管理网元与所述VNF之间可能并非直接通过网络接口或内部接口连接，因此在生成所述第一安全策略之后，管理网元可以将所述第一安全策略发送给VIM，然后由VIM将所述第一安全策略发送给所述VNF。

[0058] 或者，当所述网络系统中存在网元管理系统(element management system，简称EMS)时，所述管理网元也可以将所述第一安全策略发送给EMS，然后由EMS将所述第一安全策略发送给所述VNF，从而实现第一安全策略的部署。其中，EMS可以用于对各个网元进行管理。

[0059] 采用该实施例所提供的技术方案，管理网元可以在VNF自身发生变化时，及时调整VNF的安全策略，从减少因VNF自身发生变化而导致VNF安全策略出现漏洞的可能性。

[0060] 参见图4，为本申请安全策略部署方法另一个实施例的流程示意图。如图4所示，该实施例可以包括：

[0061] 步骤401，当VNF的生命周期状态发生变化时，管理网元生成第二安全策略。

[0062] VNF的生命周期状态发生变化也可以仅包括VNF所提供的服务或服务的对象发生变化等。以图1为例，第一VNF的生命周期状态变化可以包括第一VNF所提供的服务发生变化，或第一VNF由为第二VNF提供服务变化成为第三VNF提供服务等。

[0063] VNF所提供的服务或服务的对象发生变化也会导致VNF的安全策略需求发生变化。为满足变化后的安全策略需求，所述管理网元可以在VNF的生命周期状态发生变化后，生成第二安全策略。所述第二安全策略可以包括第二网络隔离策略和/或第二访问控制策略等内容。其中，所述第二网络隔离策略实现对所述VNF与关联网元进行网络隔离，所述第二访问控制策略则用于对访问目标为所述VNF访问请求进行访问控制。

[0064] 所述管理网元可以根据所述VNF所要实现的功能确定所述VNF之间的网络隔离需求；然后生成与所述VNF的网络隔离需求相匹配的所述第二安全策略。或者，所述管理网元也可以根据所述VNF所要实现的功能，确定所述VNF的访问控制需求；然后生成与所述访问控制需求相匹配的所述第二安全策略。在此需要说明的是，所述管理网元可以只生成所述第二访问控制策略，或者所述管理网元也可以只生成所述第二网络隔离策略，或者，所述管理网元也可以既生成所述第二访问控制策略又生成第二网络隔离策略，所述第二访问控制策略及所述第二网络隔离策略均为所述第二安全策略。

[0065] 例如，当所述网络系统的结构如图1所示时，如果为保证第一VNF的安全性，只允许第二VNF与第一VNF进行通信，那么所述第二安全策略中就需要包含第三ACL，所述第三ACL用于控制第一VNF只能与第二VNF进行数据传输。或者，管理网元也可以生成VLAN策略或VPN策略来实现只允许第二VNF与第一VNF进行通信。

[0066] 步骤402，管理网元将所述第二安全策略发送给网关设备。

[0067] 由于对VNF的隔离或访问控制通常需要由网关设备来实现，因此管理网元在生成所述第二安全策略后，可以将所述第二安全策略发送给所述网关设备。其中，所述网关设备可以包括向所述VNF提供网络服务的网络设备，所述网络设备可以为一个也可以为更多。当所述网关设备为两个以上时，根据所提供的网络服务的类型不同，所述网关设备也为不同的类型。

[0068] 由于管理网元与所述网关设备之间也可能并非直接连接，因此在生成所述第二安全策略之后，管理网元可以将所述第二安全策略发送给VIM，然后由VIM将所述第一安全策略发送给所述网关设备。

[0069] 或者，当所述网络系统中存在EMS时，所述管理网元也可以将所述第二安全策略发送给EMS，然后由EMS将所述第二安全策略发送给所述网关设备，从而实现第二安全策略的

部署。其中，EMS可以用于对各个网元进行管理。

[0070] 采用本实施例所提供的技术方案，管理网元可以在VNF的生命周期状态发生变化时，及时调整VNF的安全策略，大大减少因为VNF发生变化而导致VNF安全策略出现漏洞的可能性。

[0071] 在此需要说明的是，因此在所述VNF发生生命周期状态变化时，管理网元可能仅需生成所述第一安全策略；也可以仅需生成所述第二安全策略，或者也可以既需生成第一安全策略又需生成第二安全策略；在既需要生成所述第一安全策略，又需要生成所述第二安全策略时，两者可以各自独立被生成，并且两个被生成的先后顺序在本申请中不做限定。

[0072] 采用本实现方式所提供的技术方案，管理网元可以在VNF与关联网元之间的关系发生变化时，及时调整VNF的安全策略，从减少因VNF与关联网元之间的关系发生变化而导致VNF安全策略出现漏洞的可能性。

[0073] 参见图5，为本申请安全策略部署装置一个实施例的结构示意图。所述装置可以为前述实施例中的管理网元或为所述管理网元的一部分。

[0074] 如图5所示，该安全策略部署装置可以包括：生成单元501及发送单元502。

[0075] 其中，生成单元501，用于当虚拟网络功能VNF的生命周期状态发生变化时，生成所述VNF的安全策略，所述VNF的安全策略用于对所述VNF进行访问控制；发送单元502，用于将所述VNF的安全策略发送给控制设备。

[0076] 可选的，所述生成单元501，所述生成单元501，具体用于当所述VNF由至少两个虚拟部件构成时，生成第一安全策略，所述第一安全策略用于对所述虚拟部件之间进行访问控制或安全隔离。

[0077] 可选的，所述生成单元501，具体用于根据所述虚拟部件所要实现的功能确定所述虚拟部件之间的网络隔离需求，并生成与所述虚拟部件的网络隔离需求相匹配的所述第一安全策略；或者，根据所述虚拟部件所要实现的功能，确定所述虚拟部件的访问控制需求，并生成与所述访问控制需求相匹配的所述第一安全策略；或者，从预设的备选安全策略中选取与所述VNF的配置信息相匹配的一个作为所述第一安全策略。。

[0078] 可选的，所述发送单元502，具体用于将所述第一安全策略经由虚拟基础设施管理器VIM发送给所述VNF，或者，将所述第一安全策略经由网元管理系统EMS发送给所述VNF。

[0079] 可选的，所述生成单元501，具体用于生成第二安全策略，所述第二安全策略用于对所述VNF与关联网元之间进行访问控制或安全隔离，其中，所述关联网元是指所述VNF所属网络中除所述VNF之外的其他网元。

[0080] 可选的，所述生成单元501，具体用于根据所述VNF所要实现的功能确定所述VNF之间的网络隔离需求，并生成与所述VNF的网络隔离需求相匹配的所述第二安全策略；或者，根据所述VNF所要实现的功能，确定所述VNF的访问控制需求，并生成与所述访问控制需求相匹配的所述第二安全策略。

[0081] 可选的，所述发送单元502，具体用于将所述第二安全策略经由VIM发送给所用于为所述VNF提供网络服务的网关设备，或者，将所述第二安全策略经由EMS发送给所述网关设备。

[0082] 参见图6，为本申请管理网元一个实施例的结构示意图。所述管理网元可以为NFVO或VNFM。

[0083] 如图6所示,所述管理网元可以包括:处理器601、存储器602及通信接口603。

[0084] 其中,所述处理器601为管理网元的控制中心,利用各种接口和线路连接整个管理网元的各个部分,通过运行或执行存储在存储器内的软件程序和/或模块,以及调用存储在存储器内的数据,以执行管理网元的各种功能和/或处理数据。所述处理器可以是中央处理器(central processing unit,简称CPU),网络处理器(network processor,简称NP)或者CPU和NP的组合。处理器还可以进一步包括硬件芯片。上述硬件芯片可以是专用集成电路(application-specific integrated circuit,简称ASIC),可编程逻辑器件(programmable logic device,简称PLD)或其组合。上述PLD可以是复杂可编程逻辑器件(complex programmable logic device,简称CPLD),现场可编程逻辑门阵列(field-programmable gate array,简称FPGA),通用阵列逻辑(generic array logic,简称GAL)或其任意组合。在本申请实施例中,所述管理网络可以通过读取存储器602中的数据或调用通信接口603实现前述实施中安全策略配置方法的全部或部分法步骤。

[0085] 所述存储器602可以包括易失性存储器(volatile memory),例如随机存取内存(random access memory,简称RAM);还可以包括非易失性存储器(non-volatile memory),例如快闪存储器(flash memory),硬盘(hard disk drive,简称HDD)或固态硬盘(solid-state drive,简称SSD);存储器还可以包括上述种类的存储器的组合。所述存储器中可以存储有程序或代码,所述管理网元中的处理器通过执行所述程序或代码可以实现所述管理网元的功能。

[0086] 所述通信接口603可以用于接收或发送数据,所述通信接口可以在所述处理器的控制下向终端设备或其他管理网元发送数据;所述通信接口在所述处理器的控制下接收终端设备或其他管理网元发送的数据。

[0087] 在本申请中,所述处理器601可以用于当虚拟网络功能VNF的生命周期状态发生变化时,生成所述VNF的安全策略,所述VNF的安全策略用于对所述VNF进行访问控制;所述通信接口603,可以用于将所述VNF的安全策略发送给控制设备。

[0088] 可选的,所述处理器601,还可以用于当所述VNF由至少两个虚拟部件构成时,生成第一安全策略,所述第一安全策略用于对所述虚拟部件之间进行访问控制或安全隔离。

[0089] 可选的,所述处理器601,还可以用于根据所述虚拟部件所要实现的功能确定所述虚拟部件之间的网络隔离需求,并生成与所述虚拟部件的网络隔离需求相匹配的所述第一安全策略;或者,根据所述虚拟部件所要实现的功能,确定所述虚拟部件的访问控制需求,并生成与所述访问控制需求相匹配的所述第一安全策略;或者,从预设的备选安全策略中选取与所述VNF的配置信息相匹配的一个作为所述第一安全策略。

[0090] 可选的,所述通信接口603,还可以用于将所述第一安全策略经由VIM发送给所述VNF,或者,将所述第一安全策略经由EMS发送给所述VNF。

[0091] 可选的,所述处理器601,还可以用于生成第二安全策略,所述第二安全策略用于对所述VNF与关联网元之间进行访问控制或安全隔离,其中,所述关联网元是指所述VNF所属网络中除所述VNF之外的其他网元。

[0092] 可选的,所述处理器601,还可以用于根据所述VNF所要实现的功能确定所述VNF之间的网络隔离需求,并生成与所述VNF的网络隔离需求相匹配的所述第二安全策略;或者,根据所述VNF所要实现的功能,确定所述VNF的访问控制需求,并生成与所述访问控制需求

相匹配的所述第二安全策略。

[0093] 可选的，所述通信接口603，还可以用于将所述第二安全策略经由VIM发送给所用于为所述VNF提供网络服务的网关设备，或者，将所述第二安全策略经由EMS发送给所述网关设备。

[0094] 具体实现中，本申请还提供一种计算机存储介质，其中，该计算机存储介质可存储有程序，该程序执行时可包括本申请提供的安全策略配置方法各实施例中的部分或全部步骤。所述的存储介质可为磁碟、光盘、只读存储记忆体(英文:read-only memory，简称ROM)或随机存储记忆体(英文:random access memory，简称RAM)等。

[0095] 本领域的技术人员可以清楚地了解到本申请实施例中的技术可借助软件加必需的通用硬件平台的方式来实现。基于这样的理解，本申请实施例中的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来，该计算机软件产品可以存储在存储介质中，如ROM/RAM、磁碟、光盘等，包括若干指令用以使得一台计算机设备(可以是个人计算机，服务器，或者网络设备等)执行本申请各个实施例或者实施例的某些部分所述的方法。

[0096] 本说明书中各个实施例之间相同相似的部分互相参见即可。尤其，对于安全策略配置装置及管理网元实施例而言，由于其基本相似于方法实施例，所以描述的比较简单，相关之处参见方法实施例中的说明即可。

[0097] 以上所述的本申请实施方式并不构成对本申请保护范围的限定。

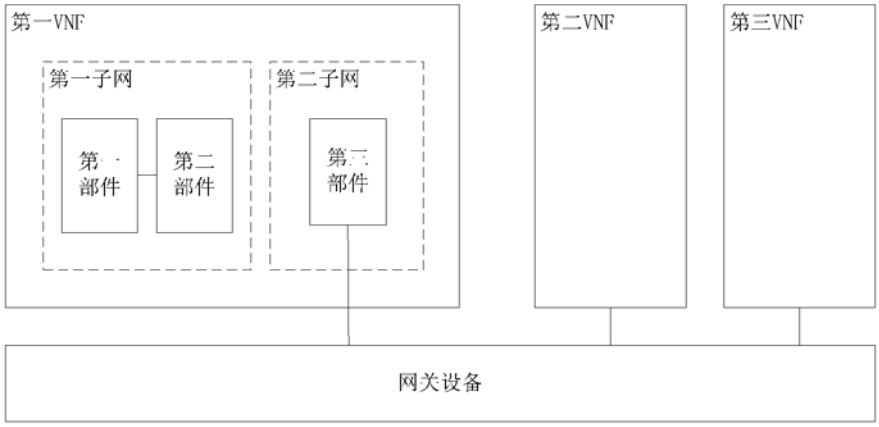

第一VNF
第一子网
第二子网
第一部件
第二部件
第三部件
第二VNF
第三VNF
网关设备

图1

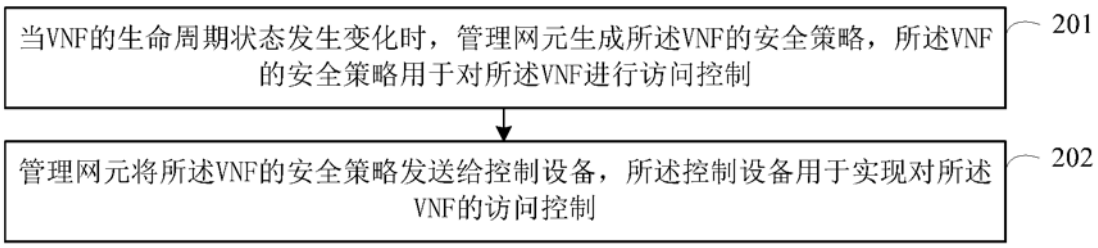

当VNF的生命周期状态发生变化时，管理网元生成所述VNF的安全策略，所述VNF的安全策略用于对所述VNF进行访问控制
201
管理网元将所述VNF的安全策略发送给控制设备，所述控制设备用于实现对所述VNF的访问控制
202

图2

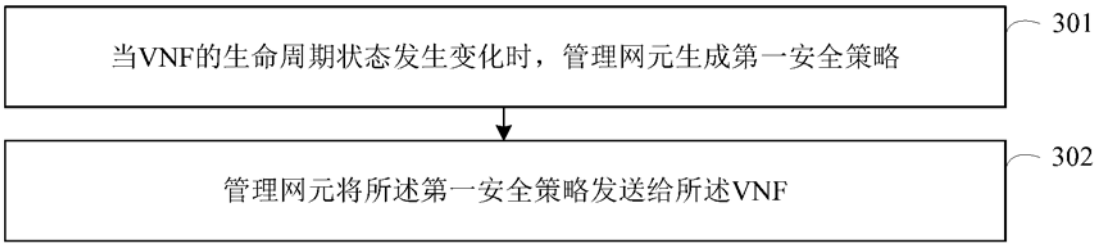

当VNF的生命周期状态发生变化时，管理网元生成第一安全策略
301
管理网元将所述第一安全策略发送给所述VNF
302

图3

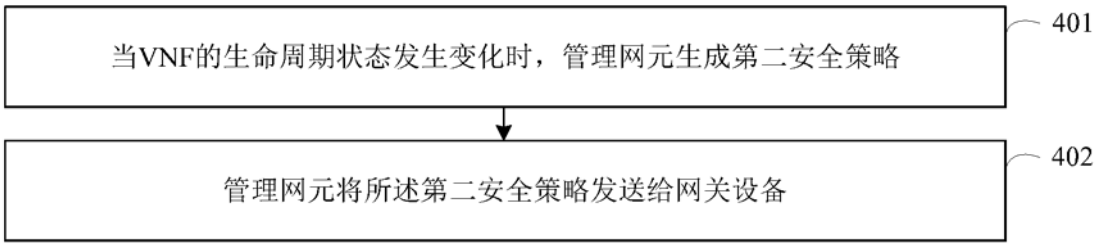

当VNF的生命周期状态发生变化时，管理网元生成第二安全策略
401
管理网元将所述第二安全策略发送给网关设备
402

图4

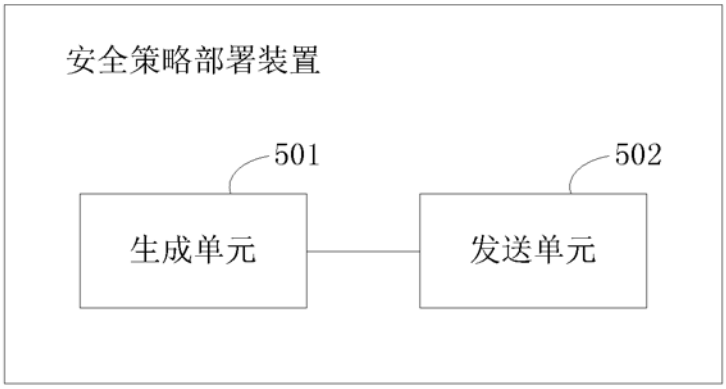


图5

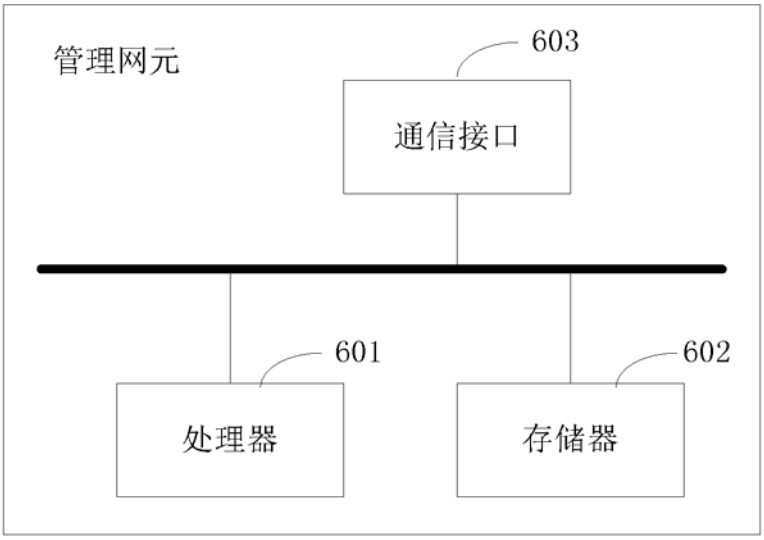


图6