电信云安全分析与思考

Analysis and Consideration of Telecom Cloud Security

张　岩[1]，张艳菲[1]，张曼君[2]（1. 中国联合网络通信集团有限公司，北京 100033；2. 中国联通网络技术研究院，北京 100048）
Zhang Yan[1]，Zhang Yanfei[1]，Zhang Manjun[2]（1. China United Network Communications Group Co.，Ltd.，Beijing 100033，China；2. China Unicom Network Technology Research Institute，Beijing 100048，China）

摘　要：
NFV通过标准化的业务和功能编排，使得在虚拟环境中运行网络成为可能。电信云基于NFV的架构与传统网络基础设施架构存在差异，这也导致了基础设施、网元的运行环境、网络部署和管理、安全等方面的改变，同时也带来了新的安全挑战。在此背景下提出了电信云的安全参考架构，在电信云关注的层级内，按照参考架构梳理了相关安全问题和风险，并针对性地给出了一些建议。

关键词：
NFV；电信云；云安全
doi：10.12045/j.issn.1007-3043.2019.04.014
中图分类号：TN915.08
文献标识码：A
文章编号：1007-3043（2019）04-0063-04

Abstract：
The telecommunication network can be established in a virtual environment via standardized orchestration of business and functions by NFV. There are differences between the telecom cloud based on the NFV architecture and the traditional network infrastructure，which leads to the changes in infrastructure，network element operating environment，network deployment and management，security and other aspects，and brings new security challenges at the same time. The security reference architecture of the telecom cloud is proposed. Within the level of telecom cloud，relevant security issues and risks are sorted out according to the reference architecture. Finally some suggestions are put forward.

Keywords：
NFV；Telecom cloud；Cloud security

引用格式：张岩，张艳菲，张曼君. 电信云安全分析与思考[J]. 邮电设计技术，2019(4)：63-66.

0 引言

电信云[1]基于NFV[2]/SDN[3]/云计算[4]技术，构建面向未来的云化网络基础设施，支撑业务和能力开放实现网络资源的虚拟化，打造高效、弹性、按需的业务服务网络。电信云以其承载业务的虚拟化、软件化、可编程、通用硬件等特性，打破了传统电信设备及业务的烟囱式体系[5]，所有的业务都可以通过管理和编排系统（MANO——Management and Organization）分配虚拟化资源、实例化虚拟网络功能（VNF——Virtual Network Function），实现新业务快速部署、资源灵活调度，简化运维，提高网络资源利用率，提升客户感知[6]。

当前的电信云进展迅速，在广泛关注电信云体系的稳定性、隔离等问题的基础上，电信云的安全问题也越来越受到重视[7]。传统网络中的安全问题，在电信云中也需要分析和防护，如身份伪造、窃听、DDoS攻击、信息泄露、缓冲区溢出攻击和隐私侵犯等[8]。与传统网络相比，电信云以及云化网络的安全问题变得更加复杂，传统云计算中的安全问题也要通盘考虑[9]。电信云体系增加了水平方向的拉通与分层，导致其安全边界的模糊化、分层化，再加上解耦架构引入了多厂商对接，使安全问题难以快速定位和溯源，多层间安全策略难以协同，手工静态配置安全策略无法满足灵活弹性扩缩容的需求。因此，亟需设计新的电信云

收稿日期：2019-02-28

以及云化网络安全防护体系,实现动态、主动、全网协同、智能运维的纵深安全防护。而且安全是电信网络的基本需求,只有采用有效的安全举措消除电信云体系中存在的风险,才能切实保障虚拟化电信云系统的安全运行。

1 电信云安全架构

电信云是基于NFV分层解耦架构的开放平台,NFV模型各组件之间引入了新的组件和网元,形成了通用资源层的横向拉通与专业应用层的纵向拉通,各个层次彼此混叠,每个纵横层次的交叉点都会同时属于2个运维管理体系,这也带来了新的安全问题。参考ITU-T X.805[10]提出的安全模型,NFV电信云架构可以建立相似的多层多平面的安全模型,如图1所示。可以看出,NFV的安全模型和NFV架构参考模型一样,分为3个逻辑层,这3个逻辑层在纵向分为2个平面。逻辑层分别是基础设施安全层、电信网络安全层和终端业务安全层。每个层可以分为2个平面,业务资源安全平面和运维管理安全平面。笔者认为终端应用层的安全问题由应用业务本身来解决,本文主要关注安全基础设施层和电信服务层,并考虑跨层跨平面的安全问题[11-13]。

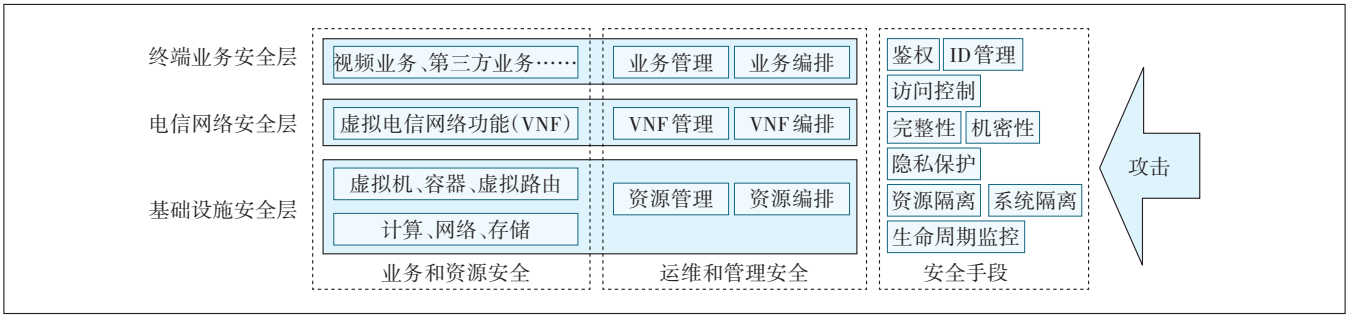

图1　NFV电信云安全参考架构

2 电信云安全问题分析

2.1 基础设施层安全

电信云基础设施主要包括了计算、网络、存储类的物理资源和虚拟资源,在目前电信云的发展阶段中,计算资源以虚拟机(VM——Virtual Machine)为主,容器技术尚未大规模应用。VM运行在通用服务器上,VM所在主机的不确定性导致安全边界缺失、模糊化。基础设施层的业务和资源安全平面是连接底层的硬件资源和上层的VM,包含路径、数据交互和处理模型的平面。在此平面内,存在安全问题的主体是VM,一般可以分为以下几种安全威胁[14]。

a)攻击者篡改VM软件镜像,安装恶意程序,通过设备驱动接口的漏洞攻击中间件。该攻击可能发生在VM加载过程或者VM加载之后,会导致VM信息泄露以及宿主机OS的安全风险。

b)攻击者通过VM特殊的虚拟磁盘驱动接口,可绕过虚拟磁盘系统的隔离机制,非法访问其他用户的磁盘空间,降低信息的机密性。

c)恶意VM可能访问一些传输类网元,导致服务面的电信协议遭到攻击,如分布式拒绝服务(DDoS——Distributed Denial of Service)攻击、畸形报文攻击,这会使传输协议出现故障和网络中断。

d)恶意VM通过非授权的通信路径访问其他VM及其应用。在VM中运行恶意程序和木马病毒,访问分配给其他VM的虚拟存储/内存,或者从外部攻击虚拟路由器暴露的IP地址。

基础设施层的运维管理平面中包含基础设施的管理接口、接口中传递的数据以及处理这些数据的功能模块。通常,基础设施层的安全管理聚焦在用户的VM或者运维网络,主要分为以下几类安全问题。

a)攻击者可能通过DC外部的访问端口,连接到MANO或者本地的运维网络,或者通过VM连接到管理VM。侵入后可以通过非授权的MANO或者本地运维管理账户登录到VM,执行非授权操作,严重的还可以控制VNF。

b)攻击者通过用户VM或者运营维护网络连接到vRouter的管理接口,非法登录到管理面,运行非法操作;或者连接VIM并发起攻击,以获得对虚拟化资源的管理权限。

2.2 电信网络安全

在VNF中,由于网络功能的虚拟化,使得在面对DDoS等攻击时,虚拟化网元的业务处理性能更低。而且VNF所属的VM在网络中的位置是流动的,VNF在

生命周期内会根据负载和规则自动创建、迁移、扩缩容、终止，这也增加了VM迁移中信息暴露的可能性。对管理平面来说，NFV体系新引入了MANO、云管平台等管理模块，如果在新模块的安全问题上应对不当将带来整个系统的风险。

NFV架构中还引入了很多新的接口，这些接口在电信云中都继承了下来，比如虚拟化基础设施管理器（VIM——Virtualized Infrastructure Management）的API、MANO内组件之间的互通接口等，除了继承的NFV接口，电信云还有一些根据需求自定义的管理接口，而这些接口的开放会带来以下通信安全风险。

a）在OSS/BSS-NFVO、NFVO-VNFM、VNFM-VNF以及VNFM/NFVO-VIM几种接口的调用指令中，可能存在某个网元或系统实体的仿冒，它们会劫持指令。仿冒的假实体可能会获取运维权限、VNF操作权限，可能影响特定或者全网的用户和服务。非NFV参考架构中的接口同样存在此风险。

b）由于服务组件可以独立部署，NFVO和自定义管理平台等对外平台可以实现Web登录和访问，这使Web门户成为新的攻击点，攻击者可能通过破解登录账户或者绕过认证机制来实现对NFVO等对外平台的非法访问。

2.3 跨层安全分析

跨层的攻击通常由电信云内部的威胁发起。某些实体被授权在某一层实现某些功能，但是此实体可能利用系统的漏洞或者错误的配置发起对其他层的攻击。例如，恶意的VNF可能窃听或篡改基础设施层管理面的信令，或者由基础设施层实体监听VNF通信，访问用户数据。

在虚拟化环境中，物理资源可以在空间或时间维度共享。在空间维度，物理资源（如同一个CPU、物理磁盘）可能由多个租户共享，攻击者可以通过攻击一个物理资源而影响多个租户；在时间维度，相同的CPU、内存和物理磁盘分区可能被先后分配给不同的租户。攻击者不仅攻击当前的功能实体，并且还有可能获得在此之前承载功能实体的残留数据，进行跟踪。又或者提前在物理设备上留下病毒以攻击后续承载的功能实体，

3 电信云安全的思考与建议

基于上述分析，可以看出，电信云中的安全问题是多方面的，相比之前的电信网络安全更为复杂，在电信云即将进入实际部署阶段，笔者对电信云的安全问题给出了一些建议[16]。

3.1 基础设施层的安全建议

3.1.1 关于虚拟机VM

电信云要具备对VM访问控制的管理能力，包括用户管理、登录鉴权、操作授权和日志审计。支持以VM为粒度定义逻辑边界，这项功能可以考虑由VIM实现，也可以由独立的管理平台实现。由于虚拟化环境中资源的通用性与集中性，在安全强度上需要依据业务和数据的敏感性做特殊处理，例如可以去掉功能调试组件及其他可修改功能的组件，或完全移出不使用的组件和硬件接口[17]。

VM中运行的应用不能直接访问宿主机的资源，需要通过权限最小化等手段，保证VM内部运行的应用不能访问其他VM的存储资源；VM中运行的进程需要遵循最小权限原则，不应给进程不必要的root权限；对VM镜像进行校验，防止非法篡改。

对于中间件发起的访问虚拟化资源的请求（例如创建一个VM，动态扩容等）VIM都需要做实体认证和访问控制。电信云要提供授权和鉴权机制，阻止其他VM或者网络路径的访问。VM之间原则上不建立通信路径，如果确需通信，需要在成功的授权和鉴权之后才能建立通信连接。

电信云要建立运维的监控能力，对物理和虚拟化资源进行监控，控制虚拟机所消耗的服务器资源（CPU、网络带宽、存储），保障受到攻击的虚拟机不会对同一台物理主机上运行的其他虚拟机造成影响。

电信云应具备对Guest OS和Host OS的安全加固能力，应关闭不使用的服务和网络协议，产品对外部提供的服务要开启访问限制（限制不必要的访问），启用的网络服务要遵循安全参数配置要求，系统中未使用的软件必须卸载。

3.1.2 关于网络和存储

虚拟路由器的管理端口需要支持用户管理、登录鉴权、操作授权以及日志审计；虚拟路由器支持抵御畸形报文攻击、DDoS攻击和仿冒攻击；不可信任的网络访问虚拟网络的管理平面时，需先访问相应网关。

确保针对存储数据的安全控制能够应用到逻辑和物理存储实体上，不会因信息在物理存储上的位置改变而旁路对其实施的安全控制手段；对物理存储实体的直接访问功能需要具备禁止或限制的能力；支持各个VNF网元和NS虚拟存储资源之间的逻辑隔离。

确保用户数据可以在物理存储设备层面上被有效清除,例如在迁移或删除虚拟机后,镜像文件、快照文件能被完全清除。租户主动解除或释放使用的存储资源时,所有数据在物理存储设备级别上也必须有效清除,确保不能由其他租户恢复。

3.2 电信网络层的安全建议

OSS/BSS/NFVO/VNFM/VNF只有在通过认证的前提下,才能接受其他组件对自身接口的调用,NFVO或自定义管理平台的Web入口访问需要支持授权和鉴权机制,以识别和认证用户实体。

安全机制需要涵盖VNF的整个生命周期的操作(如VNF创建、初始化、升级、更新、销毁),要支持不同的账户、角色、不同的权限划分,满足管理组件的不同管理需求。

系统和业务中的敏感数据必须被加密,以防止传输和存储过程中的非授权读取和篡改;对虚拟环境中的用户面、控制面和管理面进行隔离,不同安全域之间也要隔离。

3.3 跨层的安全建议

跨层安全的关键是系统资源和功能的隔离,首先要隔离内部和外部的实体,内部和外部可以是相对于VM、VNF、DC或物理位置;其次隔离不同的层/平面/租户。跨层调用需要更高的授权,且其流程数量应该最小化;垂直的安全设计和安全调度可以发现跨安全域的攻击。此外,各层的管理者和各个资源的租户处理自己内部的安全事件。

4 结束语

基于NFV/SDN/云计算技术的电信云为网络云化提供了技术基础,但同时带来了更多新的安全风险,给网络云化带来了潜在的危害和挑战。随着虚拟化技术不断演进和发展,虚拟机、容器以及更先进的虚拟化形态会出现和应用在电信云中,运营商需要全面考虑潜在的安全威胁,建立多层次的安全体系,最大程度上减少新技术应用和新体系架构中的安全问题,为网络云化提供安全可信赖的电信云基础设施,降低新一代网络中的安全风险。

参考文献:

[1] 中国联通通信云架构白皮书[EB/OL].[2019-01-01]. https://max.book118.com/html/2017/1229/146407939.shtm.

[2] Network Functions Virtualisation (NFV); Architectural Framework: ETSI GS NFV 002[S/OL]. [2019-01-01]. https://www.etsi.org/deliver/etsi_gs/NFV/001_099/002/01.02.01_60/gs_NFV002v010201p.pdf.

[3] MCKEOWN N, ANDERSON T, BALAKRISHNAN H, et al. OpenFlow: enabling innovation in campus networks[J]. Acm Sigcomm Computer Communication Review, 2008, 38(2): 69-74.

[4] 张应福,黄鹏,陈超. 云计算技术及其在下一代数据中心建设中的应用[J]. 通信与信息技术,2011(1):39-42.

[5] 鞠卫国,张云帆,王跃庆,等. NFV三层解耦下的新型网络基础设施研究[J]. 通信与信息技术,2018(6):47-50.

[6] 王帅. 对于NFV中MANO域的研究与实现[D]. 北京:北京邮电大学,2018.

[7] 方琰崴,陈亚权. 基于虚拟化的电信云网络安全解决方案[J]. 移动通信,2018,42(12):1-7.

[8] WANG S, JUN W U, YANG W, et al. Novel architectures and security solutions of programmable software-defined networking: a comprehensive survey[J]. Frontiers of Information Technology & Electronic Engineering, 2019, 19(12): 1500-1522.

[9] 拱长青,肖芸,李梦飞,等. 云计算安全研究综述[J]. 沈阳航空航天大学学报,2017,34(4):1-17.

[10] Security architecture for systems providing end-to-end communications: ITU-T X.805[S/OL]. [2019-01-01]. https://www.itu.int/rec/T-REC-X.805-200310-I/en.

[11] Network Functions Virtualisation (NFV); NFV Security; Cataloguing security features in management software: ETSI GS NFV SEC 002[S/OL].[2019-01-01]. https://www.etsi.org/deliver/etsi_gs/NFV-SEC/001_099/002/01.01.01_60/gs_NFV-SEC002v010101p.pdf.

[12] Network Functions Virtualisation (NFV); Security Guide; Report on Security Aspects and Regulatory Concern: ETSI GS NFV-SEC 006[S/OL].[2019-01-01]. https://www.etsi.org/deliver/etsi_gs/NFV-SEC/001_099/006/01.01.01_60/gs_NFV-SEC006v010101p.pdf.

[13] Network Functions Virtualisation (NFV); Security Monitoring; Report on Use Cases and Requirements: ETSI GS NFV-SEC 008[S/OL]. [2019-01-01]. https://www.etsi.org/deliver/etsi_gs/NFV-SEC/001_099/.

[14] 吴宏建,张如意,芦玥. NFV安全风险分析及应对建议[J]. 信息通信技术与政策,2018,11(11):68-72.

[15] SDN/NFV产业联盟. 基于SDN/NFV的电信网安全技术白皮书[EB/OL]. [2019-01-01]. http://www.sdnfv.org.

[16] 中国联通网络功能虚拟化安全技术规范:QB/CU T2D-096(2016)[S]. 北京:中国联通,2016.

[17] Network Functions Virtualisation (NFV); Virtualisatoin Requirements: ETSI GS NFV 004[S/OL].[2019-01-01]. https://www.etsi.org/deliver/etsi_gs/NFV/001_099/004/01.01.01_60/gs_NFV004v010101p.pdf.

作者简介:

张岩,高级工程师,博士,主要从事电信云/NFV/SDN相关技术研究工作;张艳菲,硕士,主要从事云数据中心网络/SDN相关技术研究工作;张曼君,高级工程师,博士,主要从事网络安全技术相关研究工作。