基于软件定义的5G网络安全能力架构

Security Capability Architecture of Software-Defined 5G Network

张鉴/ZHANG Jian，唐洪玉/TANG Hongyu，侯云晓/HOU Yunxiao
（中国电信股份有限公司网络与信息安全研究院，上海 200000）
(China Telecom Corporation Limited Network and Information Security Research Institute, Shanghai 200000, China)

摘要：基于5G网络“云化”和“软件定义化”的特点，提出了基于软件定义的安全能力架构。认为该架构能够实现5G网络模块化的、可调用的、快速部署的内生安全能力，能够更好地满足5G业务多样化和5G系统架构变迁所带来的安全新需求。

关键词：5G网络；软件定义；安全架构

Abstract: Based on the characteristics of "cloudification" and "software definition" of 5G network, a security capability architecture based on software-defined network is proposed. This architecture can realize the modular, invoked and rapidly deployed endogenous security capability of 5G network, which can better meet the new security requirements brought by the diversification of 5G service and the change of 5G system architecture.

Key words: 5G network; software defined; security architecture

DOI：10.12142/ZTETJ.201904005
网络出版地址：http://kns.cnki.net/kcms/detail/34.1228.TN.20190716.1059.004.html

网络出版日期：2019-07-16
收稿日期：2019-05-22

5G不仅是下一代移动通信网络基础设施，而且是未来数字世界的使能者。5G网络全新业务场景的出现和5G网络架构的变迁，均对5G网络的安全能力提出了全新挑战。5G网络需要具备模块化、可编排、可灵活调度的安全防御能力，满足不同应用场景的动态、差异化的安全要求，从而构建安全可信的网络空间。

软件定义的理念为建设5G安全能力提供了全新的思路，随着5G网络系统架构“云化”和“软件定义化”的变革，建设基于软件定义的安全能力体系成为可能。本文中，我们基于软件定义的理念，提出了全新的5G网络安全能力架构，并对该架构的部署方式、主要模块和接口功能，以及带来的价值赋能进行了全面的阐述和分析，为5G网络安全建设提供有借鉴性的参考。

1 5G网络总体架构

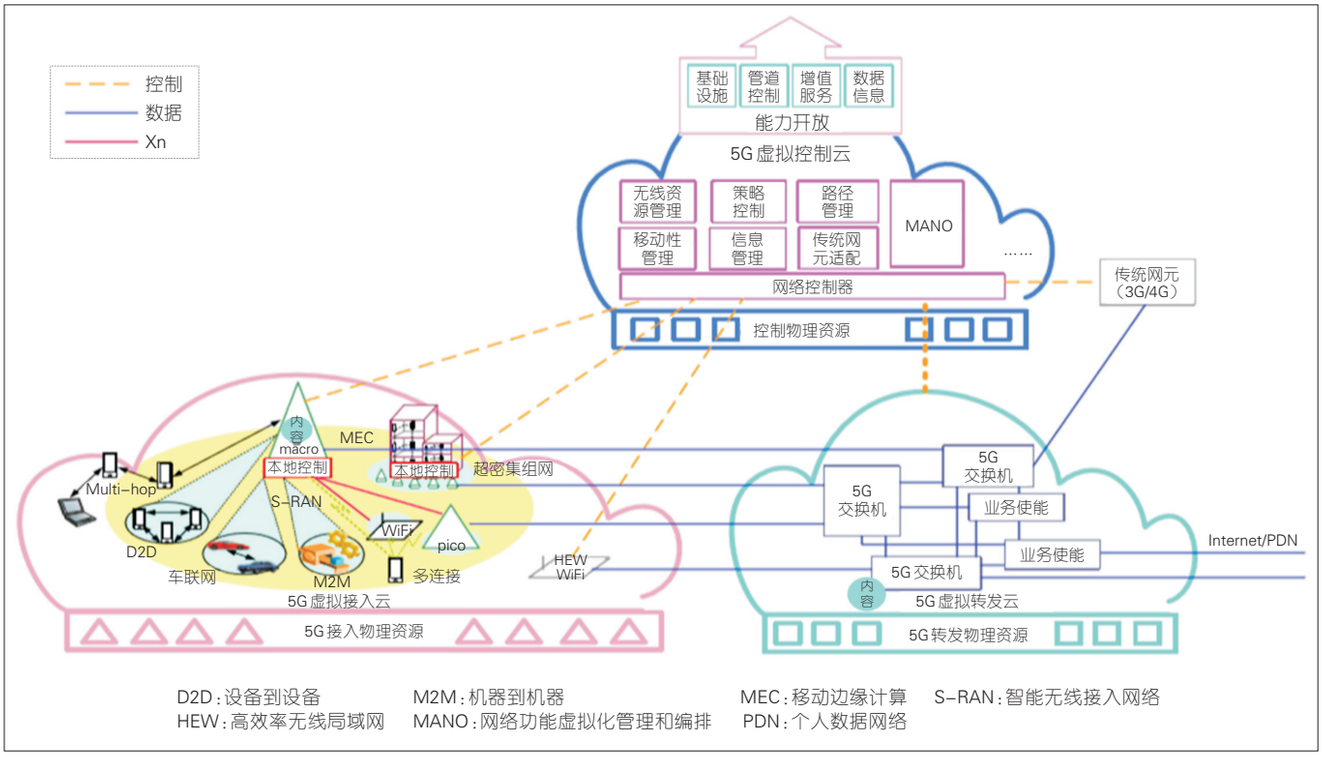
未来的5G网络将更加灵活、智能、融合和开放。5G目标网络逻辑架构简称“三朵云”架构，包括接入云、控制云和转发云3个逻辑域，如图1所示。

总体架构基于软件定义网络（SDN）、网络功能虚拟化（NFV）、云计算等关键技术推动网络架构重构，构建简洁、敏捷、集约、开放的网络新架构[1]。

（1）接入云：支持接入控制和承载分离、接入资源的协同管理，满足未来多种部署场景（例如集中、分布、无线Mesh），并实现基站的即插即用。

（2）控制云：实现网络控制功能集中，网元功能具备虚拟化、软件化以及重构性，支持第三方的网络能力开放。

（3）转发云：将控制功能剥离，使转发的功能靠近各个基站，将不同的业务能力与转发能力融合。



▲图1 “三朵云”5G网络总体逻辑架构

在上述5G网络架构中，SDN技术是连接控制云和转发云的关键；NFV将转发云中的转发设备和多个控制云中的网元用通用设备来替代，从而节省成本；三朵云中的资源调度、弹性扩展和自动化管理都是依赖基础的云计算平台。

2 5G网络安全需求分析

2.1 业务多样化需要差异化的安全能力

国际电信联盟（ITU）定义了5G的3大应用场景：增强移动宽带（eMBB）、海量机器类通信（mMTC）、高可靠低时延（uRLLC）。不同的业务会有差异化的需求，5G需要针对eMBB、mMTC和uRLLC 3种应用场景提供不同安全需求的保护机制。eMBB聚焦对带宽和用户体验有极高需求的业务，不同业务的安全保护强度需求是有差异的，因此需要针对客户提供的安全能力具备可编排性和模块化；mMTC聚焦连接密度较高的场景，终端具有资源能耗受限、网络拓扑动态变化、以数据为中心等特点，因此需要轻量级的安全算法、简单高效的安全协议；uRLLC侧重于高安全低时延性的通信业务，需要既保证高级别的安全保护措施又不能额外增加通信时延，因此需要安全能力的敏捷快速部署[2]。

2.2 新技术、新架构带来的安全挑战

5G新的网络架构引入了SDN、NFV技术，解耦了设备的控制面和数据面。这为基于多厂家通用信息技术（IT）硬件平台建立新型的设备信任关系创造了有利条件，但是也给安全方面带来很多挑战。

首先是传统封闭管理模式下的安全边界和保障模式都在发生深刻的变化，业务的开放性、用户的自定义和资源的可视化应用给云平台的安全可信带来前所未有的挑战；其次，计算、存储及网络资源共享化，会引入虚拟机安全、虚拟化软件安全、数据安全等问题。5G网络中NFV虚拟化技术的应用，可进一步简化网络功能的部署和更新，使得部分功能网元以虚拟功能的形式部署在云化的基础设施上。5G需要考虑虚拟化基础设施的安全机制，从而保障其业务在虚拟化环境下能够安全运行；还需要定义更好的安

全隔离手段，增强虚拟功能网元之间的安全管理。基于虚拟网络的切片也需要安全机制，以保证切片的安全运营和用户的正常接入。

因此，传统的安全防护模式已不再适用，5G的发展迫切需要利用5G网络架构的有利条件，挖掘出5G网络的内生安全属性，建立基于软件定义的新型安全能力架构，实现构建高可信、高安全的5G网络的目标[3]。

3 基于软件定义构建5G网络安全能力框架

3.1 软件定义安全逻辑架构

借鉴软件定义的理念和SDN架构，软件定义安全（SDS）逻辑架构包括3个层面，从下向上依次是：基础设施层、控制层、应用层，具体如图2所示。

（1）应用层：包括各种各样的安全应用及服务，实现安全业务的封装、编排和对外提供。

（2）控制层：核心是安全控制器，南向通过应用程序编程（API）接口和安全资源池进行互动，对安全资源池进行管理和调度；北向通过API对外提供封装后的安全能力甚至是安全业务；东西向和网络控制器、云等互通，实现安全流量的检测和安全策略的下发和控制。

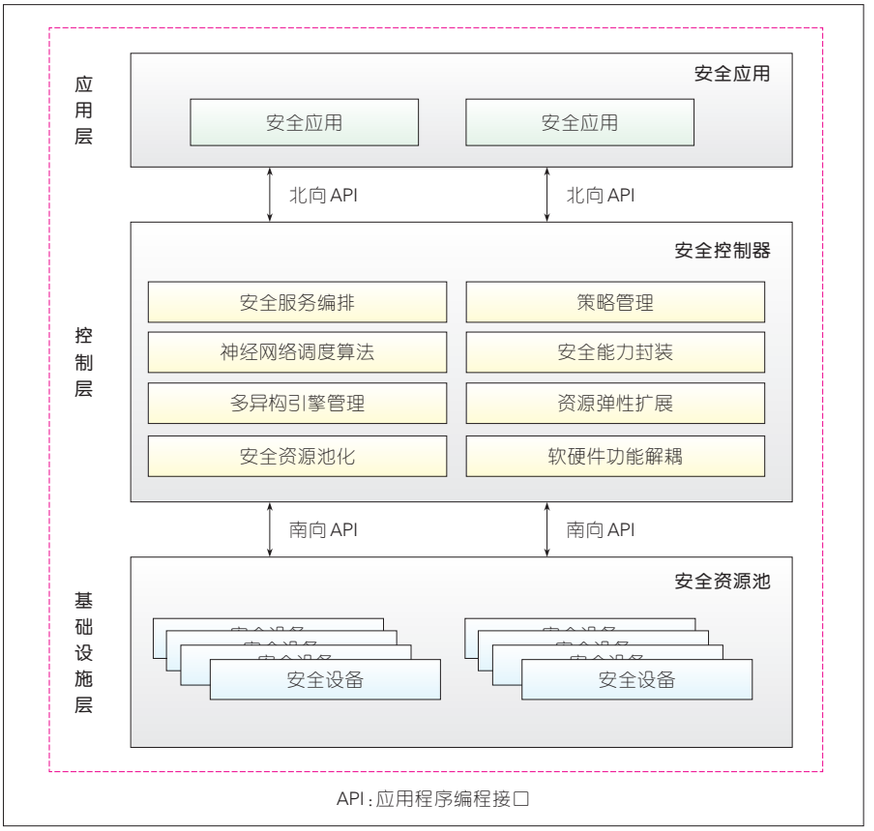
（3）基础设施层：包括各种硬件、软件形态的安全设备、安全引擎，提供安全的原子功能，形成云化的安全资源池。

软件定义安全架构相应的接口包括北向接口（控制层与应用层接口）和南向接口（控制层与基础设施层接口），具体如图3所示。

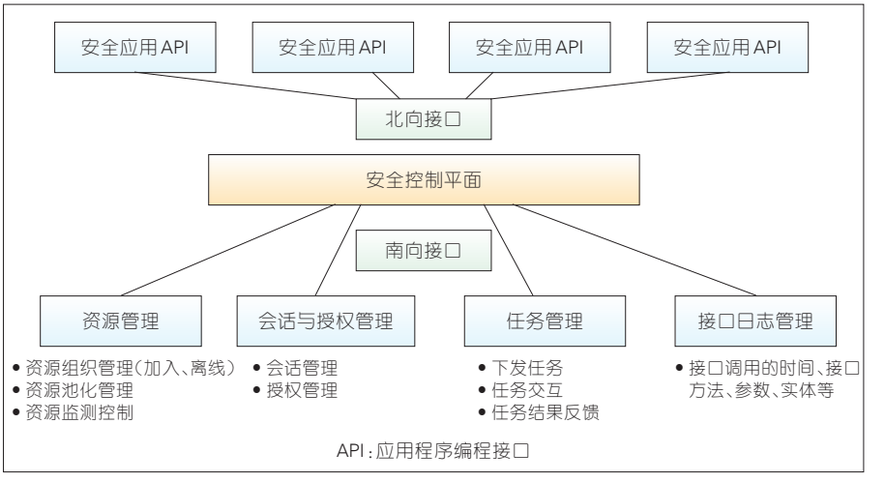
（1）北向接口：控制层与应用层接口（NBI）。

- 连接SDS控制器和用户应用之间的重要纽带；
- 为应用平面提供安全能力，可用于上层应用开发和资源编排；
- 具有多样化的特征。

（2）南向接口：控制层与基础设



▲图2 软件定义安全逻辑架构



▲图3 软件定义安全南北向接口

施层接口(SBI)。

• 控制平面与基础设施平面交互安全策略以及设备信息等数据的信息;

• 将差异化的安全设备抽象成统一的安全资源池,集中管理,统一部署;

• 打破传统硬件资源的封闭性,为不同设备厂商、不同功能的安全设备提供了管理和部署方面的便利条件。

3.2 5G网络软件定义安全防护框架

5G网络增强了开放服务能力,基于SDN/NFV的编排能力是5G网络的重要能力集;因此,基于SDN/NFV的统一编排能力,可以将软件定义安全的架构应用到5G网络安全防护体系中,从而保障5G网络具备保证各项业务安全的安全机制。基于软件定义的5G安全防护框架具体如图4所示[4-5]。

基于软件定义的5G安全防护框架的主要有6个模块。

(1)安全服务层:向5G垂直行业和5G用户提供可定制化、可编程的安全服务。

(2)安全控制及编排层:根据来自安全服务层或安全数据分析层的安全需求,将安全策略下发给相应的安全设备实现安全防护。

(3)安全分析器:使用大数据、人工智能等技术,将安全分析的结果转化为安全需求再发送给安全编排器。

(4)网络控制及资源编排层:包含SDN控制器和MANO系统。SDN控制器根据来自安全控制层的策略,实现流量的编排、管理。MANO系统实现对安全功能需要的虚拟化资源的编排、管理,以及虚拟安全网元的生命周期管理。

(5)资源池:包含硬件资源、安全资源池以及业务资源池。

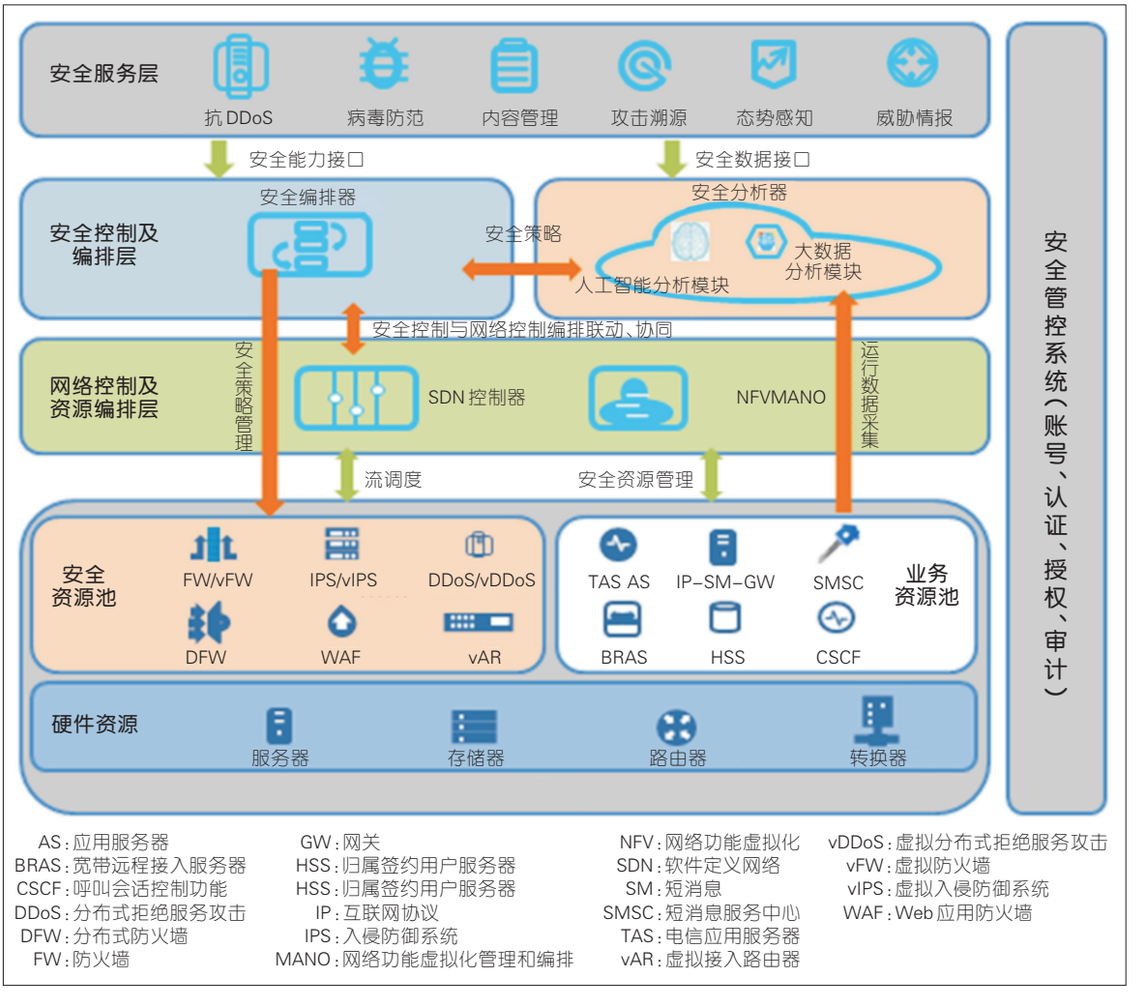


图4▶ 基于软件定义的5G安全防护框架

(6)安全管控系统:包含统一账号管理、认证管理、授权管理以及审计管理,可将安全控制器、智能分析与可视化工具等统一纳入至安全管控体系。

3.3 软件定义的5G网络安全能力架构优势

通过构建基于软件定义的5G安全能力架构,能够实现5G网络模块化的、可调用的、快速部署的内生安全能力,能够更好地满足5G业务多样化和5G系统架构变迁所带来的安全新需求。

(1)安全能力模块化管理,实现架构的可扩展和可编排。

基于软件定义的架构,可以将网络安全能力进行独立的服务化定义,封装为安全能力模块。其他功能在授权的基础上,可以调用此安全能力模块。这里安全能力包括用户身份管理、认证鉴权、密钥管理及安全上下文的管理等。安全能力的模块化增强了安全能力的精细灵活化管理,支持基于安全编排的弹性灵活调用,同时支持对调用安全能力的授权。5G网络内的安全能力以模块化的方式部署,并能够通过相应接口方便调用。通过组合不同的安全功能,可以灵活地提供安全能力以满足多种业务的安全需求。

(2)安全功能的快速部署以及调用。

基于软件定义的架构,在安全能力模块化的、可调用的、可组合的基础之上,可实现安全功能自动化管理,包括安全功能的部署、编排、配置、调用等。相对于传统的人工配置的方式,该架构可以极大地提高效率,节省成本,使垂直行业可以直接安全地部署业务,从而降低了业务门槛并缩短部署时间。

(3)安全能力开放,实现价值的共赢。

基于软件定义的架构,垂直行业可以直接使用运营商开放的安全能力,降低了一些新型垂直行业的业务门槛和成本,缩短上市时间。通过安全能力开放,运营商可以盘活网络资产和基础设施,开创新的利益增长点;可以打破管道化运营和封闭网络模式,以电信网络为中心构建安全生态系统;可以提升差异化竞争力,形成运营商、垂直行业、安全厂商、个人用户的生态链,合作共赢共创商业价值。

4 结束语

5G安全需要针对更加多样化的应用场景、差异化的网络服务方式以及新型网络架构,提供全方位的安全保障。目前,5G试商用化工作正在全面启动,因此尽早明确5G网络安全需求,建设符合5G安全需求和网络特性的安全能力架构,是当前一项紧迫的重要工作。本文中我们基于软件定义的理念,提出了全新的5G网络安全能力架构,希望能为5G网络安全建设提供有借鉴性的参考。

参考文献

[1] 中国电信.中国电信5G技术白皮书[R].2018
[2] 3GPP.5GSecurity Architecture and Procedures for 5G System:3GPP TS 33.501 version 15.4.0 Release 15[S].2019
[3] 3GPP.System Architecture for the 5G System: 3GPP TS 23.501 V16.0.2[S].2019
[4] Open Networking Foundation. Software Defined Networking:the New Norm for Networks[EB/OL].(2013-11-16)[2019-05-22]. https://www.techylib.com/en/view/shapecart/software-defined_networking_the_new_norm_for_networks
[5] 华为.华为5G安全架构白皮书[R].2017
[6] ETSI.Network Functions Virtualization (NFV) Security and Trust Guidance: ETSI GR NFV-SEC 003 V1.2.1[S].2016

作 者 简 介

张鉴,中国电信股份有限公司网络与信息安全研究院云安全研究所高级工程师;主要研究方向为云安全、5G安全、安全攻防。

唐洪玉,中国电信股份有限公司网络与信息安全研究院云安全研究所长;主要研究方向为云安全、态势感知、威胁情报。

侯云晓,中国电信股份有限公司网络与信息安全研究院云安全研究所工程师;主要研究方向为威胁情报、云安全、5G安全。