面向云网融合的电信网安全防护体系参考架构

张鉴，唐洪玉，刘文韬，薄明霞
（中国电信股份有限公司研究院云安全研究所，北京 102209）

摘　要：云网融合已经成为云计算领域的发展趋势，也是电信运营商战略转型的关键步骤。首先从云网融合的内涵、云网融合的典型应用场景和云网融合对电信网的重构方面阐述了云网融合的发展现状；然后从3个方面较为全面地分析了面向云网融合的电信网安全需求；在安全需求分析的基础上提出了电信网面向云网融合的安全防护总体架构，包括构建基础安全防护体系和软件定义安全防护体系两大阶段的工作，并对云网融合基础安全防护体系和软件定义安全防护体系的具体层次和内容做了详尽的阐述；最后对未来的前景进行了展望。

关键词：云网融合；安全体系；软件定义安全
中图分类号：TN929
文献标识码：A
doi: 10.11959/j.issn.1000−0801.2020140

Reference architecture of the telecom network security protection system for cloud network convergence

ZHANG Jian, TANG Hongyu, LIU Wentao, BO Mingxia
Institute of Cloud Security, China Telecom Corporation Limited Research Institute, Beijing 102209, China

Abstract: Cloud network convergence has become a development trend in the field of cloud computing and a key step in the strategic transformation of telecom operators. Firstly, the development status of cloud network convergencewas expounded from the aspects of its connotation, typical application scenarios and the reconstruction of telecom network by cloud network convergence. Then, the security requirements of telecom network for cloud network convergencewere analyzed from three aspects. Based on the analysis of security requirements, the overall security protection architecture of telecom network for cloud network convergence was put forward, including the construction of basic security protection system and the software-defined security protection system, and the specific levels and contents of the basic security protection system and the software-defined security protection system were elaborated. Finally, the prospect of the future was prospected.

Key words: cloud network convergence, security system, software-defined security

收稿日期：2020−03−15；**修回日期**：2020−04−23
基金项目：国家重点研发计划基金资助项目（No.2017YFB0801801）
Foundation Item: The National Key Research and Development Program of China (No.2017YFB0801801)

1　云网融合发展现状

1.1　云网融合的内涵

近年来，随着我国云计算领域的不断发展以及政策的大力推动，企业在云端部署信息系统已经成为一种趋势，企业上云的意识和能力不断增强。在这种场景下，云计算业务的开展需要强大的网络能力来支撑，网络资源的优化同样要借鉴云计算的理念，随着云计算业务的不断落地，网络基础设施需要更好地适应云计算应用的需求，云和网高度协同，不再各自独立，云网融合的概念应运而生。

云网融合的内涵可定义为：基于业务需求和技术创新并行驱动带来的网络架构深刻变革，使得云和网高度协同、互为支撑、互为借鉴的一种概念模式[1]。同时要求承载网络可根据各类云服务需求按需开放网络能力，实现网络与云的敏捷打通、按需互联，并体现智能化、自服务、高速、灵活等特性。云网融合内涵模型如图 1 所示。

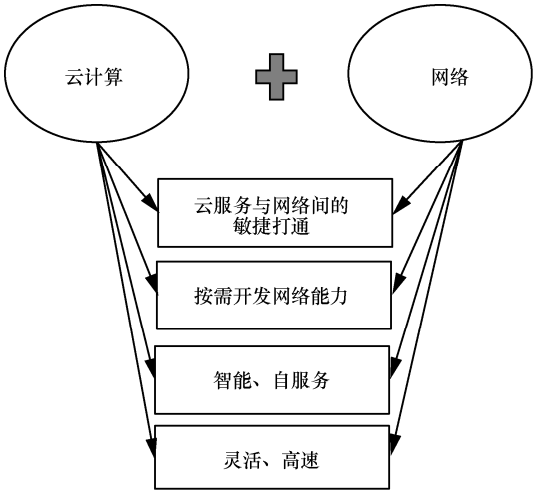


图 1　云网融合内涵模型

1.2　云网融合的典型应用场景

云网融合的应用场景总结起来可分为三大场景：混合云场景、多中心互联场景以及跨云服务商的云资源池互联场景。

（1）混合云场景

混合云场景是指企业本地（私有云、本地数据中心、企业私有 IT 平台）与公有云资源池之间的高速连接，最终实现本地计算环境与云上资源池之间的数据迁移、容灾备份、数据通信等需求。可定义如下主流的两种场景模型：本地计算环境（用户自有 IT 系统、监控中心、数据平台）与云上资源池的互联；本地数据中心（私有云）与云上资源池的互联。

（2）多中心互联场景

多中心互联场景是指同一云服务商的不同资源池间的高速互联，解决分布在不同地域的云资源池互联问题。企业可通过在不同的资源池部署应用完成备份、数据迁移等任务。

（3）跨云服务商的云资源池互联场景

跨云服务商的云资源池互联是指不同的云服务商的公有云资源池间的高速互联，该场景解决不同厂商公有云资源池的互联问题，最终实现跨云服务商、云资源池的互联。跨云服务商的云资源池互联也叫多云互联。

1.3　云网融合对电信网的重构

基础电信运营商始终处于云网融合领域的头部，强大的基础网络能力与政企资源是运营商的最大优势，同时近年来电信运营商在云计算领域的投入和能力不断加强，云网融合已经成为电信运营商战略转型的关键步骤。

以软件定义和弹性伸缩计算模式等为代表的云网融合技术，给电信领域的网元实现、业务实现、业务运营等各个方面带来巨大变化，为新的网络架构带来敏捷、灵活的体验。云网融合对电信行业的重构将主要基于以下 4 个方面来实现[2]。

（1）架构重构

建立以数据中心（data center，DC）为中心的云化架构，支持新业务的快速上线与调整。

（2）网络重构

通过 SDN/NFV 实现灵活智能的网络，自动感知业务需求，包括自动感知 VM 上线、VNF 上

线、VNF 业务变化（如动态增加业务地址、VM 迁移、VM 消除）以及调整网络连接等，实现网随云动[3]。

（3）业务重构

基于统一的云平台重构不同的电信业务，实现按需业务部署与调整，降低新业务的上线周期。

（4）运营重构

通过“全在线”、按需自动化、智能化、互联网化的运营模式，将业务运营模式从管理型转变为服务型，提升业务体验。

2 面向云网融合的电信网安全需求分析

传统电信网作为一个相对“封闭”的网络，经历了多年的发展，在业务部署以及管理模式上已经形成固有体系，在安全领域积累了大量成熟的技术和运维经验，可保障现有的电信网安全、平稳地运行。随着引入以 SDN/NFV 为代表的云网融合技术，未来电信网的网络架构在技术、建设、运营管理模式上均与传统网络存在较大的差异，会带来全新的安全挑战[4]。

（1）“封闭”网络演进为“开放”网络

相对于传统电信网基于专用硬件以及软硬件紧耦合的技术体系，以通用硬件、云计算和虚拟化为代表的新的技术体系降低了电信设备制造、开发的准入门槛，在引入更多竞争者的同时，也推动了电信网架构的开放。硬件绑定的封闭设备解耦成通用硬件和软件，并且共享硬件资源，导致传统靠专用硬件和软件构成的安全方案逐渐消失。电信系统扁平化和分层化引入了更多的攻击界面，再加上未来开源成为必然选择，安全漏洞和风险变得难以避免。

（2）新系统和网元的引入，增加了安全防护和运营的难度

未来电信网涉及新一代运营管理系统、SDN 控制器、MANO、异厂商 VNF 等，虚拟化技术进一步增加了系统组件的数量，需要管理运营的实体数量呈指数级上升，这又进一步增加了账户、权限管理的复杂度。如何快速地发现和解决问题、灵活地部署业务、规避安全攻击、降低安全运维成本，成为运营管理面临的巨大挑战。

（3）安全边界和策略的动态变化，要求弹性的安全编排能力

未来电信网中所有网元功能可根据业务的需求动态进行扩/缩容、迁移。相应地，在 SDN 控制器的调度下，网络的拓扑可能根据业务的需要进行动态变化，如果安全策略无法根据这种变化及时、快速地调整，就可能被攻击者利用，导致安全风险（比如业务数据泄露、业务中断等）。并且，由于虚拟化和资源池化的应用，不同业务可能共享相同的物理、计算、存储资源，单纯的物理隔离方案不再有效。因此，单个业务系统的安全风险可能导致与其共享计算、存储和网络资源的其他业务系统遭受安全攻击，甚至波及整个网络。为了满足网络和业务动态性要求，需提供自动化、智能化、自适应的安全服务、按需灵活生成和加载安全策略的能力，确保网络和业务动态变化时，安全策略下发和配置生效的实时性、一致性。同时，需要跨物理/虚拟层的安全协同方案，以应对虚拟化带来的系统复杂性。

3 面向云网融合的电信网安全防护参考架构

3.1 面向云网融合的安全防护体系总体架构

基于面向云网融合的电信网安全需求分析，未来电信网首先应解决引入云计算、SDN 和 NFV 后的安全风险，确保未来电信网部署阶段的基本安全保障；在此基础上，应实现安全策略的动态、灵活部署，满足业务需求，为用户提供按需的安全服务。

SDN/NFV 所提供的动态资源调度、弹性性能扩展、软件定义等能力，为安全策略的动态、灵活部署的解决方案提供了重要的思路指导。基于电信网在云网融合技术和业务上的新特点，提出

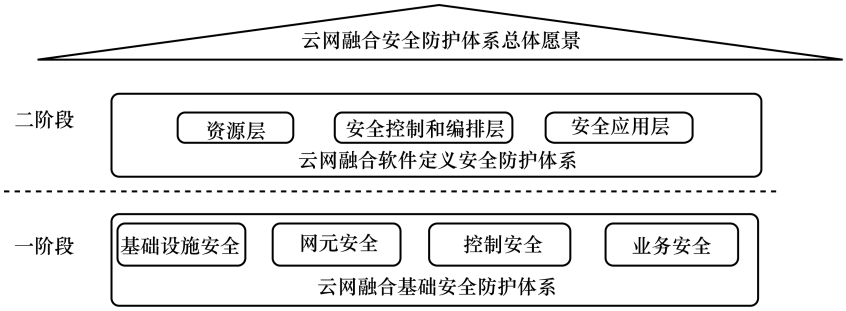


图 2　面向云网融合的电信网安全防护体系总体架构

安全防护体系的总体架构，如图 2 所示，在此架构中安全可以分为两个阶段推进[5]。

（1）基础安全防护体系

针对云计算、SDN/NFV 的技术特点，从基础设施安全、网元安全、控制安全、业务安全、安全管控等各层面，全面构建面向云网融合的基础安全防护体系，重点工作包括构建可信环境、Hypervisor 加固、SDN 控制器安全加固、MANO 安全加固、虚拟化的安全设备（比如虚拟防火墙）、安全隔离方案等，解决虚拟化安全、SDN 控制器安全、MANO 安全等重点安全问题。

（2）软件定义安全防护体系

从安全资源池、安全控制和编排、安全服务三大层面构建基于 SDN/NFV 的软件定义安全体系，充分利用 SDN 集中控制、灵活调度流量、NFV 管理和编排虚拟化资源等设计全新的安全方案，实现安全资源的集中管理和编排以及灵活、按需的部署，即软件定义安全。

3.2　云网融合基础安全防护体系

面向云网融合的电信网首先要构建自身的基础安全防护体系，包括基础设施安全、网元安全、控制安全、业务安全、安全管控五大层面，具体如图 3 所示[6]。总体设计目标是保护未来电信网基础设施、管理系统以及承载业务的安全可靠。

（1）基础设施安全

基础设施安全是云网融合电信网安全的基础，包含物理基础设施源安全和虚拟基础设施安全两个方面。

- 物理基础设施安全包括物理环境安全、物理资源可信（可信计算技术应用于物理资源的认证授权）、物理 I/O 可信（物理 I/O 接口的访问控制）。

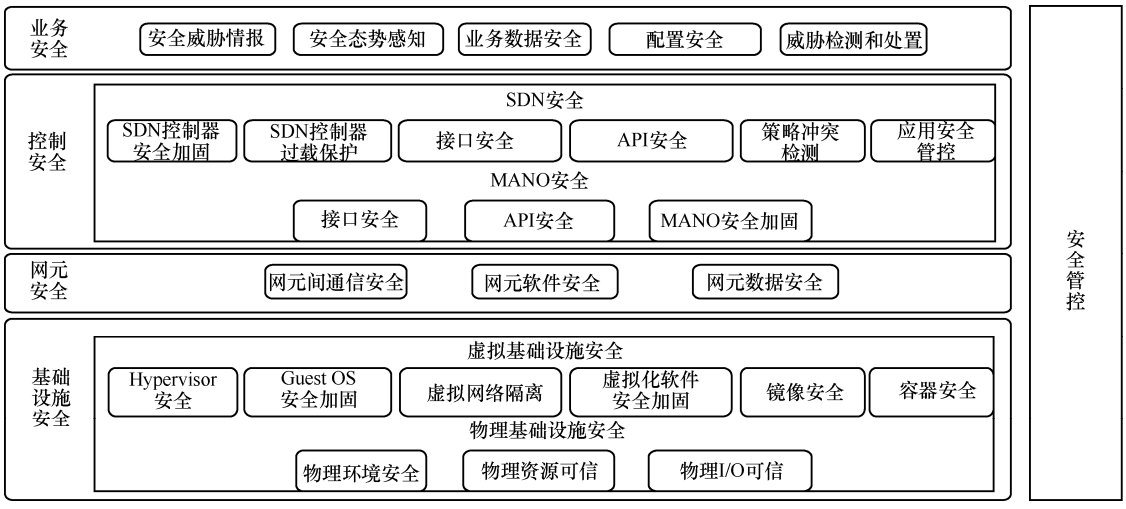


图 3　云网融合基础安全防护体系

- 虚拟基础设施安全通过 Hypervisor 及虚拟机操作系统安全加固、虚拟化软件安全加固、虚拟网络隔离、镜像安全、容器安全等保证虚拟资源的安全隔离、敏感数据的安全等。

（2）网元安全

主要包括网元间通信安全、网元软件安全以及网元自身存储的数据安全，与传统电信网络中的网元安全要求相同。

（3）控制安全

主要包括 SDN 安全和 MANO 安全[7]。

- SDN 控制安全包括 SDN 控制器安全加固、SDN 控制器过载保护、应用安全管控及策略冲突检测等，并通过接口安全、API 安全保证 SDN 控制器及南北向接口的安全。
- MANO 安全：通过 MANO 安全加固、接口安全和 API 安全等保证 MANO 系统的安全。

（4）业务安全

业务安全通过安全威胁情报、安全态势感知、威胁检测和处置及时发现和处理安全风险；通过业务数据安全、配置安全保护敏感数据和安全策略的统一配置。

（5）安全管控

包含统一账号管理、统一认证管理、统一授权管理和统一安全审计，实现对云网融合电信网的统一安全管理。

3.3 云网融合软件定义安全防护体系

面向云网融合的网络安全体系，不只单纯实现自身的安全防护，而是需要统一的安全能力编排，并对接 SDN 和 NFV，调度和编排虚拟和物理安全资源池，实现安全资源自动分配、安全业务自动化发放、安全策略自动适应网络业务变化（网络安全协同）、整网高级威胁实时响应防护（安全分析联动）等能力需求，多网元、多层次协同保障网络安全。在此基础上，通过构建安全资源池和安全集中编排点，并结合大数据和人工智能技术，实现安全策略的集中管理和编排，为用户按需提供安全服务。面向云网融合的软件定义安全防护体系架构如图 4 所示[8]，软件定义安全架构主要包含资源层、安全控制及编排层、安全应用层，各部分的功能描述如下。

（1）资源层

资源层包含物理设施层和安全资源池等，其中：

- 物理设施资源由服务器、存储设备、交换机和路由器等组成，为虚拟化安全功能和业务提供物理资源；
- 安全资源池由虚拟化的安全功能（即虚拟安全网元）和物理安全设备等组成。安全设备接收来自交换机的流量并对该流量执行安全策略。虚拟安全网元可以根据业务需求，

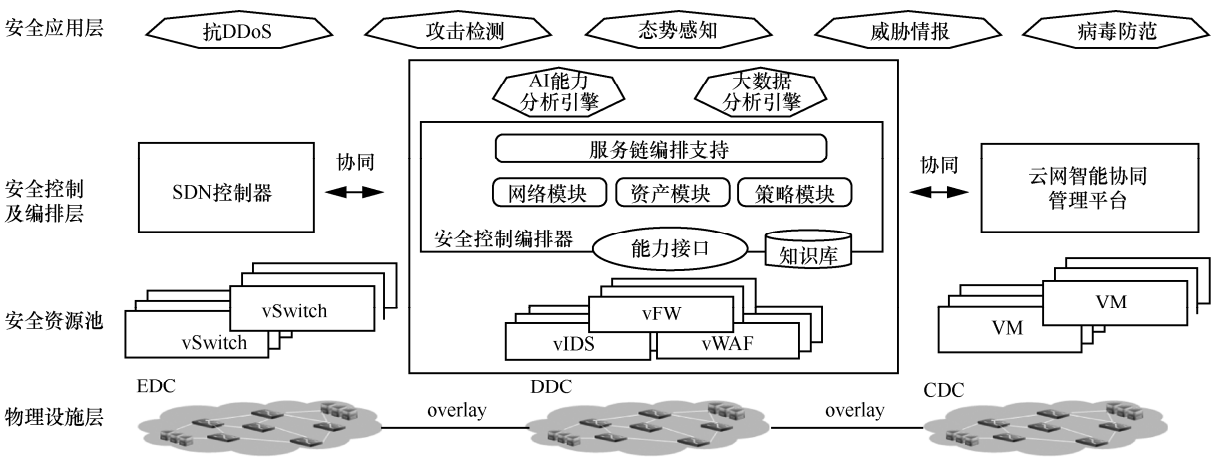


图 4 面向云网融合的软件定义安全防护体系架构

由控制和编排层实现安全功能的弹性伸缩。

（2）安全控制及编排层

根据来自安全应用层的安全需求，安全控制编排器将安全策略下发给相应的安全设备实现安全防护。安全控制编排器在向安全设备下发安全策略之前，应先将引流策略下发给 SDN 控制器，由 SDN 控制器实现流量的编排；如果现有的安全资源不能满足安全需求，安全编排器还需向云网协同管理系统下发虚拟资源分配请求，以扩充所需的虚拟资源或者创建并启动满足特定安全需求的虚拟化安全网元。

安全控制及编排层可采用大数据、人工智能等技术，构建安全分析引擎，基于各虚拟网元及物理网元的安全日志、流量日志、文件、终端行为等多维度分析安全威胁，将安全分析结果转化为安全需求，发送给安全控制编排器。

（3）安全应用层

安全应用层基于安全控制及编排层提供的安全能力及安全数据向用户提供可定制化、可编程的安全服务，这些安全服务可集成在用户的最终应用中。用户可通过此功能按需购买安全服务。订购功能和服务通过 API 调用提交给安全控制编排器。安全控制编排器根据安全控制策略和用户需求实现安全资源的管理和编排，为用户提供按需安全服务。

4　结束语

云网融合已经成为云计算领域的发展趋势，也是电信运营商战略转型的关键步骤。随着云网融合进程的不断深化，业务需求和技术创新并行驱动加速网络架构发生深刻变革。本文在分析云网融合给电信网带来的安全挑战的基础上，提出了面向云网融合的电信网安全防护体系的总体安全参考架构，并针对基础安全防护体系和软件定义安全体系的关键技术提出了发展建议，期望能对电信网演进中的安全方案提供借鉴，以提升未来电信网络的安全性。

参考文献：

[1] 云计算开源产业联盟. 云网融合发展白皮书[R]. 2019.
Cloud Computing Open Source Industry Alliance. White paper on cloud network integration development[R]. 2019.

[2] 中国电信. CTNet 2025 网络架构白皮书[R]. 2016.
China Telecom. CTNet 2025 network architecture white paper[R]. 2016.

[3] 王海宁, 赵慧玲. NFVO 标准和实践[J]. 电信科学, 2017, 33(4): 3-9.
WANG H N, ZHAO H L. NFVO standards and practice[J]. Telecommunications Science, 2017, 33(4): 3-9.

[4] 腾讯安全云鼎实验室. 2019 云安全威胁报告[R]. 2019.
Tencent YunDing Security Lab. Cloud security threat report[R]. 2019.

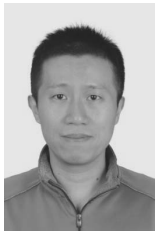
[5] 胡腾, 李观文, 周华春. 面向服务的数据中心安全框架[J]. 电信科学, 2018, 34(1): 8-16.
HU T, LI G W, ZHOU H C. Service-oriented security framework for datacenter networks[J]. Telecommunications Science, 2018, 34(1): 8-16.

[6] 张鉴, 唐洪玉, 张静. 中国电信云计算业务平台安全建设探讨[J]. 电信技术, 2017(6): 57-61.
ZHANG J, TANG H Y, ZHANG J. Discussion on the security construction of China telecom cloud computing business platform[J]. Telecom Technology, 2017(6): 57-61.

[7] ETSI. Network functions virtualization (NFV) security and trust guidance: ETSI GR NFV-SEC 003 V1.2.1[S]. 2016.

[8] 张鉴, 唐洪玉, 侯云晓. 基于软件定义的 5G 网络安全能力架构[J]. 中兴通讯技术, 2019(8): 25-29.
ZHANG J, TANG H Y, HOU Y X. Security capability architecture of software-defined 5G network[J]. ZTE Communications Technology, 2019(8): 25-29.

[作者简介]



张鉴（1976– ），男，中国电信股份有限公司研究院云安全研究所高级工程师，主要研究方向为云安全、安全攻防、5G 安全。

唐洪玉（1977– ），男，中国电信股份有限公司研究院云安全研究所所长，主要研究方向为云安全、态势感知、威胁情报。

刘文韬（1989– ），男，中国电信股份有限公司研究院云安全研究所工程师，主要研究方向为云安全、威胁情报。

薄明霞（1978– ），女，中国电信股份有限公司研究院云安全研究所高级工程师，主要研究方向为云安全、威胁情报。