云原生架构与SASE安全融合实践

Integration Practice of Cloud Native Architecture and SASE

贺译册[1]，余思阳[1]，曹京卫[1]，高贯银[2]，徐宝辰[2]（1. 中国联合网络通信集团有限公司，北京 100033；2. 中讯邮电咨询设计院有限公司，北京 100048）

He Yice[1]，Yu Siyang[1]，Cao Jingwei[1]，Gao Guanyin[2]，Xu Baochen[2]（1. China United Network Communications Group Co.，Ltd.，Beijing 100033，China；2. China Information Technology Designing & Consulting Institute Co.，Ltd.，Beijing 100048，China）

摘　要：

面对数字化转型与复杂网络安全威胁，构建可靠的安全防护体系至关重要。研究了云原生架构下安全访问服务边缘（SASE）模型的构建。聚焦云原生技术特性和SASE在多云及分布式环境下的应用，通过案例分析与理论研讨发现，集成SASE的安全服务可有效实现身份验证、加密通信和细粒度访问控制，显著提升网络安全性和管理灵活性。此外，提出了一种统一管理框架，规范了SASE在身份验证、网络连接和威胁防御中的配置策略，强化网络安全并简化复杂环境中的安全操作。

关键词：

云原生安全；安全访问服务边缘；网络安全；身份验证；加密通信

doi：10.12045/j.issn.1007-3043.2024.08.015

文章编号：1007-3043（2024）08-0073-05

中图分类号：TP393

文献标识码：A

开放科学（资源服务）标识码（OSID）：

Abstract：

Facing digital transformation and complex network security threats，building a reliable security defense system is crucial. It explores the construction of Secure Access Service Edge （SASE） model within a cloud-native architecture. Focusing on the characteristics of cloud-native technologies and the application of SASE in multi-cloud and distributed environments，through case analysis and theoretical discussion，it shows that integrating SASE security services can effectively achieve identity verification，encrypted communication，and fine-grained access control，which significantly enhances network security and management flexibility. Additionally，it proposes an unified management framework that standardizes SASE configuration strategies for identity verification，network connection，and threat defense，strengthens network security and simplifies security operations in complex environments.

Keywords：

Cloud native security；Security access service edge；Network security；Identity verification；Encrypted communication

引用格式：贺译册，余思阳，曹京卫，等. 云原生架构与SASE安全融合实践[J]. 邮电设计技术，2024（8）：73-77.

0 引言

随着企业数字化转型升级，业务逐渐互联网化、多云化和移动化，内外网边界模糊，业务访问已从单一网络模式转向交错复杂的模式，企业所面临的网络安全挑战也愈发严峻，传统的网络安全架构已无法满足日益复杂的网络安全需求。安全访问服务边缘（SASE）[1]作为一种集成了网络服务能力和安全服务能力的服务模型，能够将来自企业分支或者移动办公的流量就近接入融合了网络能力和安全能力的安全边缘节点，并进行统一管理，保证用户以一致的安全能力访问云端、数据中心和互联网中的所有应用，可有效帮助企业满足合规性要求并提高数据保护水平[2]。

本文在充分分析基于云原生的SASE的技术发展及现状、通用技术框架、网络服务能力、安全服务能力、应用场景、标准的基础上，提出基于云原生的SASE服务能力要求的标准化需求，给出相应的标准化建议，为业界SASE的设计、开发、应用等提供指导和参考。

收稿日期：2024-07-03

1 SASE理念

SASE是一种融合了网络与安全解决方案的新服务模型[3]，它将下一代广域网（如SD-WAN）的基础设施与各种云原生的网络安全功能〔如安全Web网关（SWG）、防火墙即服务（FWaaS）、零信任网络访问（ZTNA）、数据防泄密分析和防泄密阻断（DLP）、云访问安全代理（CASB）等〕集成起来，满足数字化企业动态安全访问资源（如数据中心、云服务）的需求[4]。传统网络安全服务模型[5-6]与SASE模型的对比见表1。

表1 传统网络安全服务模型与SASE模型对比

对比项	传统网络安全模型	SASE模型
远程访问本地资源	大部分传统网络模型在很大程度上通过SSL/TLS（传输层安全协议）或专用端点客户端的VPN技术[5]访问	SASE可以代替VPN。用户连接到SASE以访问本地资源和云服务。安全策略由SASE控制台定义和应用
访问云资源	本地网络对云资源的访问和其访问其他互联网内容一样，都是通过传统的防火墙、代理和路由控件实现[6]	SASE为SaaS、PaaS和IaaS提供优化的、简化的、可感知云的网络访问。这些访问依赖API集成并需要中高端用户请求自检
网络访问控制	大多数本地环境都依赖路由、防火墙和代理进行访问控制	SASE服务将多个网络安全和访问控制（包括防火墙服务）汇总到统一结构上
安全服务	依赖于企业自建和维护的本地安全设备，如防火墙、入侵检测系统、VPN等，通常集中于数据中心和办公室网络边界	集成到基于云的架构中，提供对分布式用户和设备的统一安全保护

2 基于云原生架构的SASE安全服务

SASE安全基于云原生架构，将SD-WAN、SWG、CASB、ZTNA和下一代防火墙（NGFW）等网络和安全服务集成到一个统一的云平台中[7]，灵活性高且可扩展性强，同时采用零信任安全模型，对每个访问请求进行验证和授权，并通过全球分布的服务节点确保安全策略和访问控制的一致[8]。

SASE安全防护架构可通过集成的云原生安全功能和零信任模型显著提升整体安全性，增强对分布式用户、设备和多云环境的灵活保护，简化运营和管理流程，降低对本地硬件设备的依赖，并优化全球用户的访问体验，提高生产力和用户满意度。SASE整体安全服务架构如图1所示。

2.1 SASE技术架构

SASE将网络与安全能力云原生化，从而实现云化、动态、分布式的安全服务架构[9]。SASE服务商在选择解决方案部署架构时，优先选择与自身其他产品

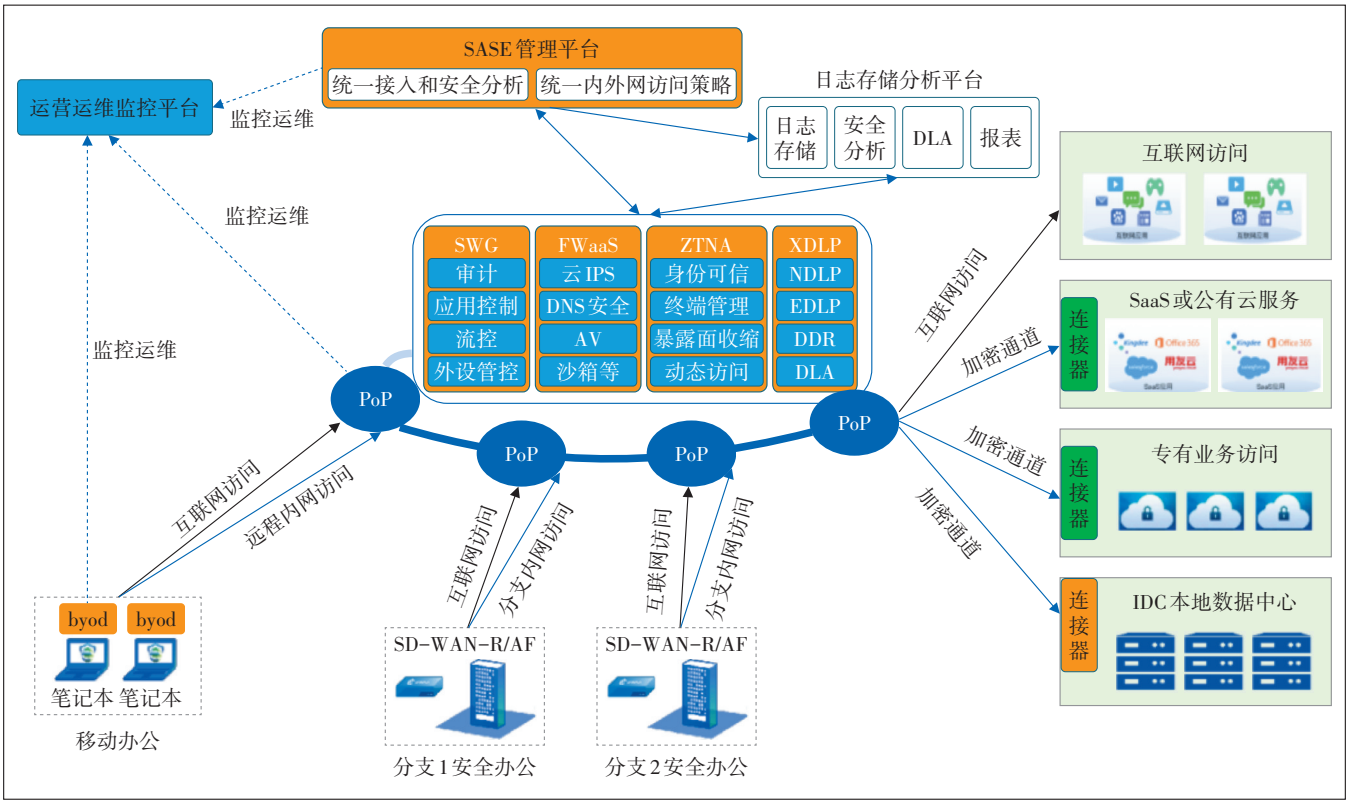

图1 基于云原生的SASE安全服务整体架构

兼容性强的方案，如软件优势、硬件优势、资源池部署优势等。目前SASE主流的部署架构有2种：基于PoP点的SASE架构和基于接入网关的SASE架构[10]。

2.1.1 基于PoP点的SASE架构

基于PoP点的SASE架构是指将SASE的主要能力集成到PoP点，将其改造为分布式安全资源池，并提供接入服务的一种架构（见图2）。该架构可以看做是SD-WAN架构[11]的升级，目前SD-WAN服务提供商、运营商都广泛采用此种架构[12]。

2.1.2 基于接入网关的SASE架构

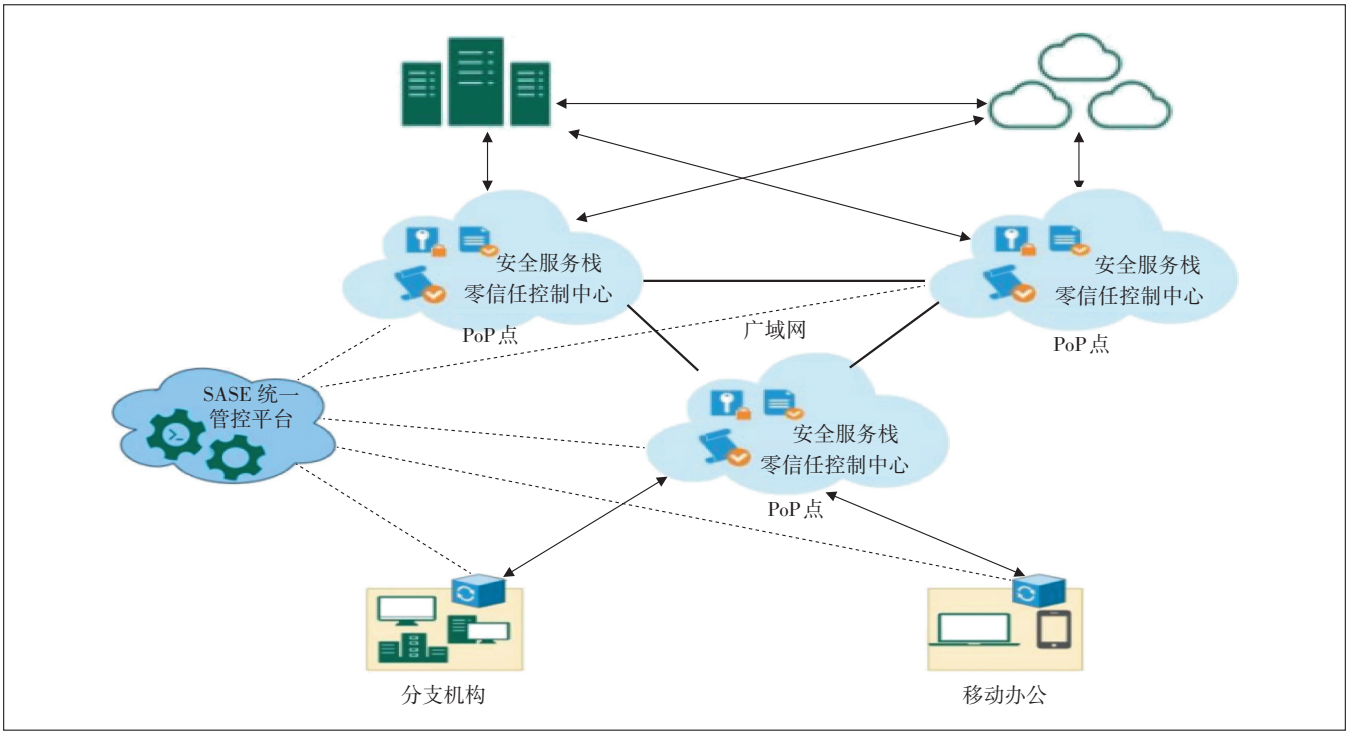

图2 基于PoP点的SASE架构

与基于PoP点的架构不同，基于接入网关的SASE架构将功能组件集成在接入网关而非服务商提供的PoP点中，因此省去了PoP点的建设与网络互联（见图3）。此类架构多出现于网络硬件厂商，优势在于减少了PoP点覆盖范围不足导致偏远地区用户无法就近访问的情况的发生。

2.1.3 网络和安全服务组件

SASE需要融合提供安全服务与网络服务，需要具备的3个核心能力为安全服务能力、网络服务能力和统一管理能力。

a）安全服务能力。在PoP提供融合安全能力，必备能力包括SWG、ZTNA、FWaaS能力，可选能力包括DLP、CASB、RBI、终端等安全能力。

b）网络服务能力。必备能力包括软件或硬件SD-WAN，可选能力包括广域网优化、DEM、骨干网服务等能力。

c）统一管理能力。在SASE统一管理平台提供网络服务管理、安全服务管理、PoP云资源管理、运维管

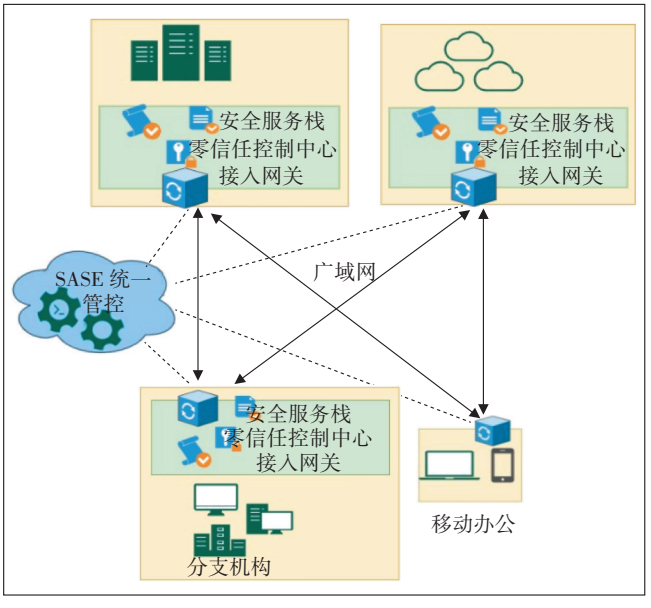

图3 基于接入网关的SASE架构

理、用户和身份管理等管理能力，各个能力和服务在一个管理面进行配置和使用。

2.2 关键技术及实现流程

2.2.1 SASE关键技术

a）云原生架构。SASE云原生架构由云原生控制器、底层平台容器化和高性能容器网络3个部分构成[13]。通过云原生技术能力，SASE将支持微服务、高可用、弹性伸缩、故障自愈、DevOps持续开发和集成等能力，以支撑SASE业务的快速发展和快速部署。

b）零信任交换网络。通过构建SASE零信任交换网络提供更高级别的安全保护，无论用户身在何处，都能安全地访问企业网络和互联网资源。基于零信任（Zero Trust）[14]理念，即不信任任何用户、设备或网络，对每个用户和设备进行验证和授权，以确保访问和数据的安全。

c）流量接入处理。分支机构或移动用户，支持通过标准协议IPsecVPN、GRE、代理等，将边缘组件的流量按需接入SASE的PoP点[15]。由PoP点对流量进行管理，实现应用识别、URL、安全防护、流控、DLP等能力。

2.2.2 SASE服务实现流程

a）安全服务编排和统一网络调度。SASE框架提供了多种安全和网络功能，用户可按需订阅所需的功能模块。当用户流量通过边缘组件接入到SASE PoP后，SASE统一管理平台可根据用户订阅的网络功能、安全功能模块，自动编排用户流量经过时对应的安全业务功能。

b）全局配置一致性。SASE框架采用广泛分布式节点为用户提供服务，用户可能处于任何位置。网络与安全融合的编排策略为了给用户提供最优的网络接入体验，会编排用户接入任意最优的PoP点，所以用户也会分散接入任意的PoP点。为了保障对用户提供一致性的防护，需要保障所有SASE PoP对该用户执行一致的策略配置。

配置下发与执行流程如下。

a）管理员在策略配置平台完成防护策略、安全策略等的配置，配置内容统一存储在安全管理模块中。

b）网络管理模块完成对用户流量的编排下发后，将编排结果同步给安全管理模块。

c）安全管理模块若检测到编排结果中存在的PoP点还未加载过该用户的策略配置，则主动将该用户的最新策略配置推送下发到对应的PoP点；若管理员更新了策略配置，也将主动推送下发更新。

d）当用户流量接入到任一PoP点后，PoP点也会实时检测是否加载了该用户的策略配置，若未加载，则主动向安全管理模块获取该用户的最新策略配置，以避免安全管理模块主动推送时可能出现的网络错误、服务错误等异常场景。

e）用户最新的策略配置将由安全功能模块进行加载生效，以实现对用户的一致性防护 。

3 典型应用场景

3.1 电子政务外网安全

随着政务业务的快速发展，政务外网承载的业务场景日益多样化，对电子政务外网提出了泛在性、移动性、灵活性和安全性的接入要求。为满足其安全防护需求，以SASE架构为基础，在国家政务外网互联网区构建SASE运营管理平台和分布式安全边缘节点（PoP点），提供安全接入、边界防护和安全审计管控等可扩展的安全功能。通过将接入政务外网的终端访问流量引流到PoP节点进行安全防护，满足区县、乡镇和街道办等分散位置的政务部门的安全需求。

a）身份认证需求。接入电子政务外网的终端类型复杂，需通过身份梳理和认证，实现基于身份的安全访问。支持账号密码、短信等多种认证方式，以及短信、邮件、TOTP等二次认证方式，以保障接入安全。

b）传输安全需求。对于通过互联网接入的终端，需保障其安全性。提供端到端加密隧道能力，以确保传输安全。

c）风险终端访问阻断能力。通过IPS和病毒防护，阻断移动终端威胁的横向扩散。

d）上网合规管控。政务外网微末分支下沉互联网安全访问审计能力，SASE云安全服务平台提供上网审计、管控、攻击防护和恶意代码防护能力。

e）便捷运维管理。根据电子政务外网覆盖全国的“中央、省、市、县”四级网络现状，提供区域级PoP点能力，覆盖小分支和移动终端。末端及移动用户接入具备简单、安全、灵活的特性，客户端和设备可实现云端自动化部署，缩短安全落地周期。

3.2 5G专网安全

5G专网带来了IT、OT和IOT的网络融合，各类终端数量多、类型杂、分布广，导致接入难管控、网络边界隔离不足、访问审计缺失等问题，缺乏行为分析与高级威胁监测能力，增加了管理区和生产区业务网的风险。因此，亟需建立5G安全整体防护体系。通过在

MEC中心节点部署SASE PoP节点，设置5G安全接入专区，实现对5G终端接入MEC的安全管控（如内网、5G专网、互联网），并实现5G终端与MEC边界、内网业务及内网办公的整体安全防护。通过融合安全运营平台，实现安全、简易的运营支撑。

a）终端入网：确保合法终端入网。对进入内网的终端进行身份认证，确保合法终端入网。支持识别多种物联网设备，并对移动端设备进行一机两网管控和违规外联监测。

b）边界安全：保障5G专网与内网边界安全。从资产识别、风险监测、安全防护等方面对物联网边界提供安全防护，避免网络安全风险渗透内网，保障内网环境安全。

c）业务安全：构建轻量业务防护体系。通过对承载业务主机和访问业务终端的持续监控和检测响应，解决业务“最后一公里”的安全隐患，防止病毒入侵、漏洞利用、挖矿等网络安全问题。

d）融合安全运营：构建高效的运营体系。通过终端行为分析、事件溯源和高效联动，解决IT+OT+IOT安全运营中的威胁识别、定位、溯源及管理难题，高效对抗威胁并简化运营工作。

4 总结

利用基于云原生架构的SASE安全防护技术构建企业新型网络安全防护体系，已逐渐成为行业内的共识。这种融合实践不仅提升了企业的安全防护能力，还增强了业务的灵活性和可扩展性。通过调研多个现实案例，发现云原生和SASE的融合能够为企业带来显著的安全和业务价值。然而，这一融合过程并非一帆风顺。企业在实施过程中可能会面临技术集成难度大、安全配置复杂、人员技能不足等挑战。为了克服这些挑战，企业需要加强技术培训、完善安全管理制度、建立专业的安全运营团队，并不断优化和更新自身的安全策略。

展望未来，随着技术的不断进步和应用的深入，云原生和SASE的融合将会进一步拓展其应用场景和深度。企业可以探索将更多先进的安全技术融入到云原生平台中，如零信任网络、微服务等，以构建更加完善和智能的网络安全防护体系。同时，企业还需要关注网络安全威胁的不断演变，及时调整自身的安全策略和防护措施。通过持续的研究和创新，企业可以不断提升自身的网络安全防护能力，确保业务的稳定和安全运行。

参考文献：

[1] 高巍，陈磊，张红兵，等. 云原生技术和平台研究与实践[J]. 数字通信世界，2023(8)：43-45.
[2] 俞智超，刘国碧. 后云计算时代物流企业云原生技术应用的理论与实践探讨[J]. 商业经济研究，2024(3)：98-101.
[3] 闫媛媛，张玉强，杜朝阳. 基于云原生技术的专用车制造云平台的研究与应用[J]. 重型汽车，2023(2)：8-9.
[4] 陈国. 云原生技术赋能数智化转型升级[J]. 电信工程技术与标准化，2021，34(5)：1-9.
[5] 余雨，刘婷婷. 将云原生技术引入《Web开发技术》课程的研究[J]. 教育现代化，2021，8(9)：20-23.
[6] 周世杰. 计算机系统与网络安全技术[M]. 2版. 北京：高等教育出版社，2022.
[7] 李汶泽. 计算机通信网络的数据安全维护策略分析[J]. 文摘版：工程技术，2022(7)：85-87.
[8] 王大鹏. 计算机网络安全管理与有效运行探究[J]. 中国新技术新产品，2013(7)：42.
[9] 王业超，宋德星. 美印网络安全合作：外在转变、内生动力及矛盾增生[J]. 南亚研究，2023(1)：70-96.
[10] 蒋宁，范纯龙，张睿航，等. 基于模型的零信任网络安全架构[J]. 小型微型计算机系统，2023，44(8)：1819-1826.
[11] MAYER D，LEVER F，Gühr M. Data analysis procedures for time-resolved x-ray photoelectron spectroscopy at a SASE free-electron-laser[J]. Journal of Physics B：Atomic，Molecular and Optical Physics，2022，55(5)：054002.
[12] KASHIWAGI S，KON Y，KATO R，et al. Sase-fel experiment in the far-infrared region using a strong focuing wiggler[C]//The 3rd annual meeting of Particle Accelerator Society of Japan and the 31th Linear Accelerator Meeting in Japan. Sendai：PASJ，2006：520-522.
[13] HONDA Y，ADACHI M，EGUCHI S，et al. Construction and commissioning of infrared SASE-FEL at cERL[EB/OL]. [2024-03-12]. https://arxiv.org/abs/2106.13247.
[14] SASEMARKET PROJECTED TO REACH US $6 BILLION：DELL'ORO GROUP[J]. Commswire magazine：Incisive，intormed，independent，objective，2023.
[15] SHINTAKE T，KITAMURA H，ISHIKAWA T. X-ray FEL project at SPring-8 Japan[J]. AIP Conference Proceedings，2004，705(1)：117-120.

作者简介：
贺译册，毕业于北京交通大学，工程师，学士，主要从事网络安全、终端安全、数据安全等产品的研究、设计、研发和规划工作；余思阳，毕业于北京邮电大学，工程师，硕士，主要从事网络安全体系规划及产品研究工作；曹京卫，高级工程师，主要从事运营商网络信息安全的规划、建设与运营，网络安全产品、网络安全数据服务产品开发工作；高贯银，毕业于北京师范大学，硕士，主要从事网络安全相关系统的研发及研究工作；徐宝辰，毕业于西安电子科技大学，学士，主要从事网络架构设计规划、云原生产品及云原生网络架构的研究及设计工作。