SASE关键技术与产业发展研究

Key Technology and Industry Development of Secure Access Service Edge

柴瑶琳/CHAI Yaolin，韩维娜/HAN Weina，
张云畅/ZHANG Yunchang，穆琙博/MU Yubo，韩淑君/HAN Shujun
（中国信息通信研究院，中国 北京 100191）
(China Academy of Information and Communication Technology, Beijing 100191, China)

DOI：10.12142/ZTETJ.202402011
网络出版地址：http://kns.cnki.net/kcms/detail/34.1228.TN.20240423.1324.002.html
网络出版日期：2024-04-23
收稿日期：2024-03-02

摘要：安全访问服务边缘（SASE）有机融合云、网、算和安全，支持随时随处的一站式安全访问，是产业数字化转型的革新性网络安全技术。SASE关键技术包括软件定义广域网（SD-WAN）、零信任网络访问（ZTNA）、云原生网络及网络安全即服务等技术，是网络融合安全架构演进的必然趋势。目前中国SASE产业还处于初期探索阶段，需抓住发展机遇，加强技术产品研发创新和标准体系构建，促进SASE产业高质量发展。

关键词：SASE；SD-WAN；ZTNA；云原生网络；网络安全即服务

Abstract: Secure access service edge (SASE) is a revolutionary network security technology for digital transformation of industry by organically integrating cloud, network, computing, and security to support one-step security access anywhere and anytime. The key technologies of SASE include software defined wide area network (SD-WAN), zero trust network access (ZTNA), cloud native network, and network security as a service, which are the inevitable trend of network convergence security architecture evolution. At present, China's SASE industry is still in the early stage of exploration, so it is necessary to seize the development opportunity, strengthen the innovation of technology product development and standard system construction, and promote the high-quality development of SASE industry.

Keywords: SASE; SD-WAN; ZTNA; cloud native network; network security as a service

引用格式：柴瑶琳，韩维娜，张云畅，等．SASE关键技术与产业发展研究[J]. 中兴通讯技术，2024，30(2)：72-75. DOI：10.12142/ZTETJ.202402011
Citation：CHAI Y L, HAN W N, ZHANG Y C, et al. Key technology and industry development of secure access service edge [J]. ZTE technology journal, 2024, 30(2): 72-75. DOI: 10.12142/ZTETJ.202402011

伴随产业数字化转型进程的加快，云网融合应用场景不断深化，网络安全对产业高质量发展的保障作用也不断凸显。各国高度重视网络安全领域的战略布局和创新研究，抢抓国际新技术主导权。近年来，中国也在不断推进网络安全融合领域的新技术创新应用。安全访问服务边缘（SASE）融合网络和安全创新技术（软件定义广域网、零信任、云原生网络等），以及全面构建云-网-算-安全一体化服务，已成为全球网络安全领域关注的研究焦点。

本文将聚焦SASE热点技术，围绕当前发展现状，重点分析关键技术体系，探讨领域应用挑战并提出未来发展建议。

1 SASE发展现状

1.1 国际SASE战略部署加快

SASE成为各国重塑政府整体网络安全架构的首要选择。2021年12月，加拿大政府在《网络与安全战略》文件中明确提出把SASE作为远程办公场景下替代虚拟专用网络（VPN）的重点技术[1]。2022年6月，美国联邦调查局（FBI）发布的“网络企业重新设计计划”（NERI）最新信息请求显示[2]，FBI对规划架构提出了大量具体的安全要求，如零信任、SASE、强隔离、可见性等。

1.2 全球SASE技术标准体系不断完善

SASE技术发展趋近成熟，国际化组织标准建设进程不断加快。根据Gartner 2021年发布的《Hype Cycle for Emerging Technologies》[3]报告统计，SASE位于全球网络创新技术领域最受关注的前30。目前SASE已跨过早期阶段，进入中期阶段，将在未来2～5年重构网络服务业务模式，推动产业变革性发展。紧跟技术发展，全球SASE标准制定步伐不断加快。2022年，全球城域以太网论坛（MEF）联合微软、Verizon Business等全面推动包括MEF W117 SASE

服务属性和框架等标准的制定。中国SASE标准建设进程在产业各方的合作下也逐步推动。中国通信学会等第三方组织开展了《安全访问服务边缘（SASE）整体方案技术要求》《安全访问服务边缘（SASE）能力成熟度》等标准的编制。

1.3 SASE整体产业发展势头良好

全球SASE产业生态正在形成，供需两方积极行动促进规模化部署。思科、微软、VMware、Palo Alto Networks等一批美国头部企业全面布局SASE市场，融资活跃度较高。此外，电信运营商、网络安全企业、云安全企业、网络设备厂商等产业各方积极加大SASE研发投入，加紧、重点推出SASE产品[4]。同步从需方侧观察，垂直行业包括电信、金融、能源等开始重视采用SASE架构，逐步试点部署。SASE应用正不断从传统网络安全领域扩展到云网/算网融合、边缘安全、物联网等新应用场景。根据国际第三方咨询架构Dell'Oro Group 2022年3月份公布的《网络安全报告》[5]数据显示，2021年SASE网络和安全总支出已超过40亿美元，增长率达到37%。

在新需求、新应用、新威胁的牵引下，以SD-WAN、防火墙、零信任网络访问、云安全访问为主的SASE产品体系不断完善，贯穿基础设施层安全、平台安全、应用安全3个层次以提供一体化网络安全服务。总体上看，SASE整体产业发展稳步向好，市场活跃度不断提升，产品应用不断丰富。

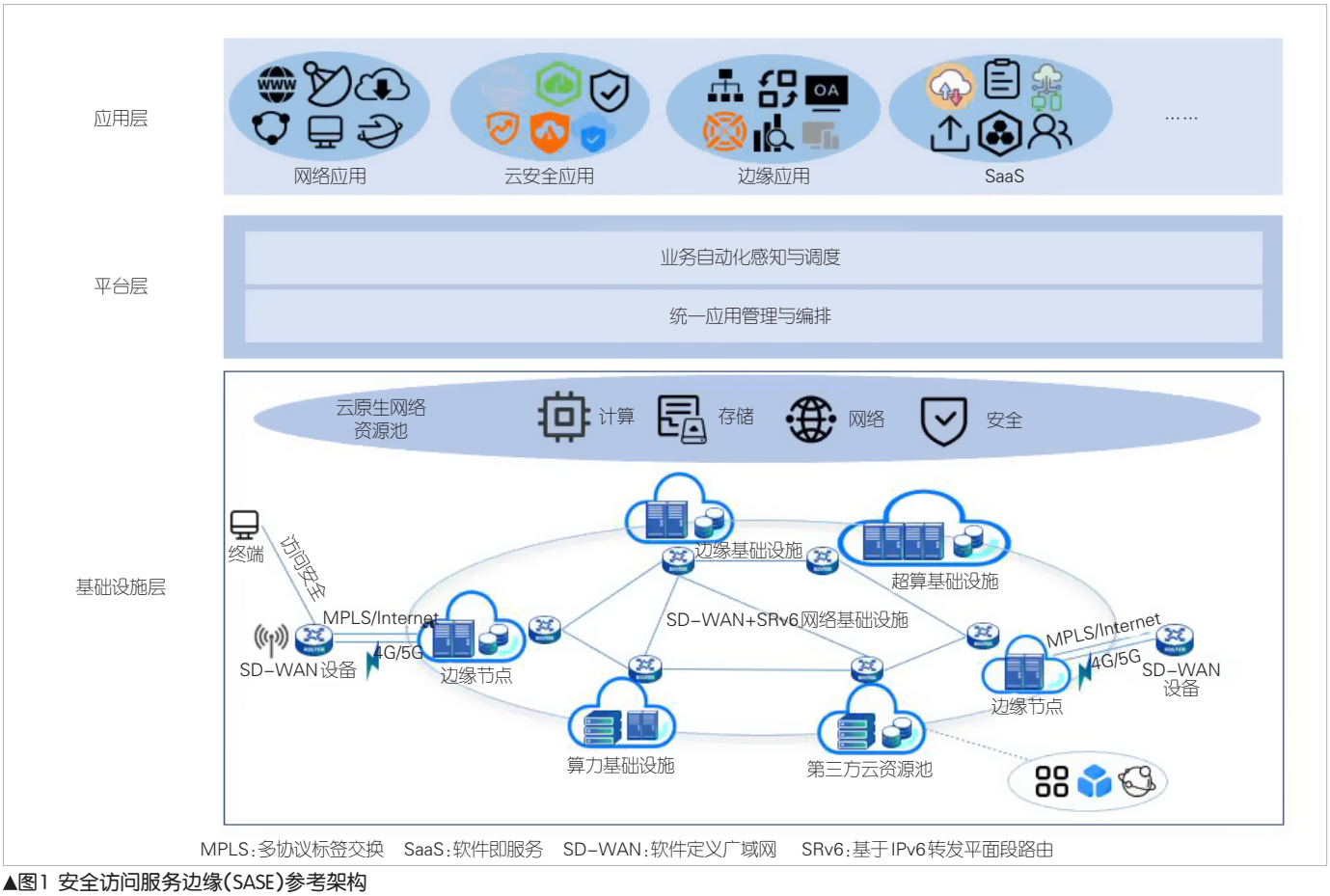
2 SASE参考架构及关键技术

2.1 SASE参考架构

SASE是融合网络能力与安全能力并进行统一管理和交付的创新技术体系，如图1所示，集成了SD-WAN、零信任网络访问、云原生网络、网络安全即服务等多个关键技术能力。SASE目前已经在金融、能源、电信等多场景得到广泛应用，成为数字基础设施建设发展的重要内涵。

从层次结构上看，SASE包括应用层、平台层、基础设施层3个主要部分。

1）SASE应用层：支撑各类应用（包括网络应用、安全应用、边缘应用、SaaS、融合应用等）安全防护要求。



MPLS：多协议标签交换 SaaS：软件即服务 SD-WAN：软件定义广域网 SRv6：基于IPv6转发平面段路由

▲图1 安全访问服务边缘(SASE)参考架构

2）SASE平台层：通过身份安全、网络安全、应用与数据安全功能组件来支撑云、网、算、安全资源的编排安全、运维安全、协同安全等一体化平台安全。

3）基础设施层：作为SASE基础设施资源底座，包括物理基础设施和虚拟化基础设施资源池两层。其中，物理基础设施层包含所有的物理和虚拟的SD-WAN设备、计算节点、边缘节点、公有云、私有云、数据中心、第三方云资源池，虚拟化基础设施资源池将物理基础设施资源统一抽象为计算资源、网络资源、存储资源、安全资源等。

2.2 SASE关键技术

SASE的关键技术包括SD-WAN、零信任网络访问、云原生网络、网络安全即服务等。

1）SD-WAN

SD-WAN作为SASE的网络技术底座，以业务与应用为导向，融合软件定义网络（SDN）、网络功能虚拟化（NFV）、网络编排与探测等多种技术，能够以平台或托管方式提供基础网络连接、广域网加速、安全防御等多种SASE服务。通过对SASE网络的抽象和建模，SD-WAN将上层网络业务和底层网络基础设施具体实现架构进行解耦，通过在SASE平台部署独立的控制面，将网络转发和控制进行分离，从而实现SASE网络集中管控和自动化运维。

2）零信任网络访问

零信任网络访问作为SASE的安全引擎，基于零信任“持续验证、永不信任”的安全理念，通过细颗粒度的身份识别和用户访问行为的上下文信息（包括设备信息、访问时间、访问地点等）来授予动态访问权限，并持续评估访问主体的信任值。零信任网络访问基于统一的数字化身份安全访问体系，赋能SASE形成统一安全访问管控机制，切实保障了无边界、自适应、弹性访问、可持续安全评估的应用体验。

3）云原生网络

云原生网络将SASE网络能力下沉到云中，实现网络资源软硬件解耦、网络资源弹性部署、云网服务一体协同等应用需求。通过k8s开放架构，SASE使用轻量级虚拟化容器技术构建网络功能，支持横跨本地和公有云环境，将防火墙、入侵防御系统（IPS）、网站应用级入侵防御系统（WAF）、用户终端设备（CPE）等网络功能部署在不同容器组（POD）中，作为微服务开发和交付，支持以度量、跟踪和日志记录的方式将每个网络功能POD内部状态外部化等。云原生网络技术全面构建了SASE网络应用新模式，从单体到微服务化转变，实现网络能力插件化、弹性化、自动化。

4）网络安全即服务

网络安全即服务是将SASE网络安全功能（包括防火墙、云访问安全代理、IPS、WAF、SWG等）SaaS化的体现，可提供一站式一体化全流程的安全服务。网络安全即服务重点解决了传统网络安全设备软硬一体、网络安全应用烟囱式、新业务新功能交付低效等主要问题。SASE通过支持网络安全功能云化部署和应用程序编程接口（API）开放化，全面构建网络安全即服务能力体系。网络安全即服务将持续根据SASE实时业务情况来动态创建、响应和变更SASE网络安全能力参数配置，以满足各类资源弹性扩缩、应用轻量化、业务弹性化、服务快速上线的新需求。

3 中国SASE发展面临三大挑战

1）SASE网络和安全统一管理机制尚未形成

产业在推进SASE部署建设时，尚缺乏相应的网络和安全统一管理机制，主要表现在：一是企业对网络安全的重视不足，安全防御意识薄弱，主动建设SASE网络安全平台意愿弱；二是缺乏网络和安全的统一规划，网安业务体系各自为政，亟需SASE相关政策指引；三是SASE作为重要行业关键信息技术基础设施，企业投入资金不足，缺少必要的安全管理保障措施，存在一定的网络安全风险。

2）SASE技术成熟度低且标准体系不完善

SASE技术融合复杂度高，架构部署存在相关技术服务质量参差不齐问题，具体表现在：一是SASE产品服务标准不统一，适用于特定行业特性、需求的SASE应用标准规范缺乏；二是缺乏行业通用SASE平台，亟需探索适应行业特征和发展需求的新型融合架构模式；三是现有网络安全基础设施融合能力不足，SASE产品质量和稳定性有待提高，部分产品在使用过程中可能会出现故障或漏洞，需要及时修复和升级。

3）SASE产业生态仍在初期且发展力量不强

当前，SASE在垂直行业的应用尚未进入大规模部署阶段，SASE产业生态尚未闭环。SASE产业涵盖网络服务提供商、安全服务提供商、设备制造商等，产业生态各方协同性差，供需对接不足。同时，产业仍缺乏融合领域人才培养。

4 SASE产业发展建议

1）加强统筹谋划，形成系统完善的监管机制

一是提升企业网络安全风险认知，推动企业完善自身网络安全管理体系，明确网络安全责权，积极主动增强SASE网络安全平台建设，切实保障关键数据安全；二是针对重点行业关键部门，出台相关政策要求，明确SASE路线图，指

导SASE网络设施和安全设施统一规划、同步建设、分步实施；三是鼓励相关主管部门配套专项资金，并建立健全试点工作机制，推动企业保质保量落实SASE融合试点应用和完善相应保障措施。

2）强化研究新创，建立自主核心的SASE技术体系

围绕SASE的网络体系、平台体系和安全体系，强化核心技术研究，主要包括：一是建立和完善SASE标准体系，指导产业数字化转型工作与SASE关键技术体系的融合应用，持续提升SASE技术与企业业务融合发展水平；二是建设通用技术平台，运用零信任、云原生、SaaS等新一代信息技术，探索构建适应行业特征和发展需求的新型融合架构模式，建设敏捷高效可复用的SASE融合基础设施，提升服务能力；三是优化基础设施，综合采用内置于设备、虚拟化、软件化、可动态加载和配置等方式，实现SASE基础设施升级，增强系统的自身安全属性和灵活部署性，提升安全防护效果。

3）注重培育引导，打造具有竞争力的产业生态

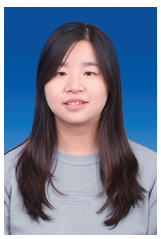
打造SASE产业合作平台，整合电信运营商、网络安全企业、互联网企业等产学研用资源，共同孵化SASE产品方案，实现产业链深度融合。建立SASE行业应用示范标杆，推广SASE优秀案例，全面加深SASE行业实践部署，配套SASE人才培养计划，保障企业SASE网络安全一体化能力建设。

参考文献

[1] 党小东, 柴瑶琳, 穆琋博, 等. 安全访问服务边缘产业发展现状及未来发展趋势 [J]. 信息安全与通信保密, 2023(9): 19-26
[2] Federal Bureau of Investigation. Network enterprise redesign initiative [EB/OL]. (2022-10-01)[2024-02-25]. https://sam.gov/opp/396968fc403b4d838794200355513ae4/view#attachments-links
[3] Gartner.Hype cycle for enterprise networking [EB/OL]. [2024-02-25]. https://blogs. gartner. com/andrew-lerner/2021/10/11/networking-hype-cycle-2021/
[4] 王茜, 陈晨, 井俊丰, 等. 大型企业SASE解决方案及应用实践 [J]. 中兴通讯技术, 2023, 27(2): 45-50. DOI:10.12142/ZTETJ.202301009
[5] Dell'Oro Group. 2021年SASE以37%的增长率改变了市场格局 [EB/OL]. [2024-02-25]. https://mp.weixin.qq.com/s/b689uXP5Vyg0auJVw7Erug

作 者 简 介

柴瑶琳，中国信息通信研究院技术与标准研究所高级项目主管；主要从事SD-WAN、零信任、算网安全等相关技术研究工作；参与20余项行业标准/团体标准研制工作，发表论文10余篇，授权/申请技术专利6项，拥有计算机软件著作权7项，组织发布行业白皮书3个。



韩维娜，中国信息通信研究院技术与标准研究所技术专家；主要从事SD-WAN、网络算力化等相关领域的研究工作；参与多个白皮书撰写、标准研制等工作，目前参编完成著作1本、行业白皮书1个，参与起草行业标准/团体标准5项。

张云畅，中国信息通信研究院技术与标准研究所技术专家；主要从事零信任、算网安全等方面研究工作；参与多个零信任白皮书撰写、标准研制等工作，目前参编完成著作1本、行业白皮书1个，参与研制行业标准/团体标准5项。

穆琋博，中国信息通信研究院技术与标准研究所互联网中心副主任、高级工程师；主要从事算网融合、未来网络、云计算等方面的研究工作；牵头多个技术体系的标准研制，发表论文10余篇，拥有计算机软件著作权12项。

韩淑君，中国信息通信研究院技术与标准研究所高级项目主管；主要研究方向包括算网融合、云计算、人工智能、区块链等；发表论文10余篇，拥有计算机软件著作权3项。