运营商 SASE 技术研究报告（2022 年）

CCSA TC610 Report xxx

中国通信标准化协会 TC610

2022 年 9 月

版权声明

前　言

本白皮书在分析运营商 SASE 的场景、架构以及应用的基础上，提出了运营商 SASE 的能力要求、技术要求，并分析了相关的业务场景的 SASE 解决方案。本白皮书为运营商规划和建设 SASE 业务提供了架构设计和技术参考。

本白皮书本研究报告的主要参与人包括中国移动通信集团有限公司，中国电信集团有限公司，北京山石网科信息技术有限公司，新华三技术有限公司等企业，并得到中兴通讯股份有限公司等多家企业的大力支持和配合，在此一并表示感谢。

目 录

一、 概述

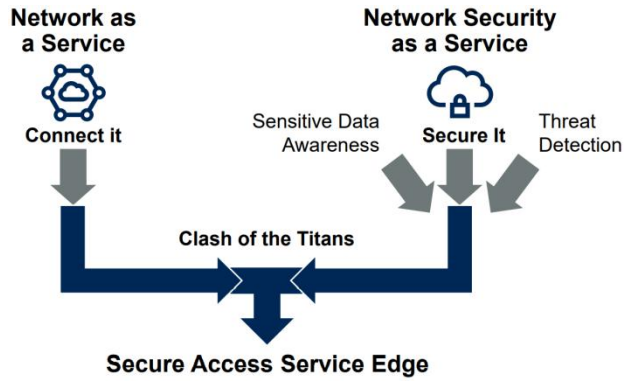
（一） 背景

随着企业数字化转型的推进，移动网络和云计算的全面普及，企业越来越多的核心业务和关键数据从数据中心转移到云上，企业的组织方式和办公方式也发生了的显著变化，越来越多的企业采用多地设立办公地点和支持远程/移动办公的方式。随之而来的，是接入场景的多样化和各分支机构的流量不断增加。据统计，93%的受访企业计划采用多云架构，而 41%的应用程序在多云之间进行数据集成[1]。疫情期间，国内外多家公司加速推行在家办公政策，员工通过办公设备远程/移动办公成为新常态。随着 5G、物联网和边缘计算技术的快速发展，基于网络边缘的低时延、大带宽的业务场景也不断涌现，如：工业园区、视频会议等，业务需部署在靠近终端用户侧，提供快速安全地服务。

企业的传统网络安全架构已不适用业务云化的发展趋势，堆叠单一的安全技术和解决方案，会造成企业安全系统复杂度增加、实际操作困难、效率降低的问题。企业需要在业务数字化转型的过程中，针对多种网络接入场景，根据业务需要灵活配置网络和安全服务，并实现体验和策略要求一致的安全保障。2019 年，Gartner 在报告《Hype Cycle for Enterprise Networking 2019》中首次提出了 SASE（Secure Access Service Edge）的概念，认为 SASE 是解决这一问题的答案，并在随后的报告中进行了详细阐述。

（二） 定义

SASE（Secure Access Service Edge）即安全访问服务边缘。如图 1，根据 Gartner 的定义，SASE 核心理念是一种融合了广域网技术（Network as a Service）和全面网络安全防护(Network Security as a Service)的新型网络服务框架[2]。基于实体[i]的身份标识，结合实时上下文和企业的安全策略，SASE 为企业提供持续的安全防护和信任评估服务[2]。在 SASE 的框架中，身份是访问决策的中心，而不是企业数据中心。



图片来源：Garter: THE FUTURE OF NETWORK SECURITY IS IN THE CLOUD

图 1 SASE 定义[2]

一个合格的 SASE 产品/供应商必须将 SD-WAN 网络服务和安全保障服务结合，具备以下功能特点：

以身份为中心

传统企业的网络安全框架常以固定物理边界来标识信任区域，以 IP+端口来作为应用管理调度的依据，导致用户从内外网接入的体验截然不同，且对内部用户开放了过多权限，内外网的安全策略也难以

[i]这里的实体包含了企业员工、客户、第三方人员、企业分支机构、设备、应用、服务、物联网系统等等。

统一管理。而 SASE 摒弃了传统基于边界的安全模型，以身份作为访问决策的依据，边界或者物理位置只是需要参考的上下文之一。通过对角色、设备信息、用户行为、位置和其他特征的综合信任评估，决定路由选择和访问权限级别，制定全网统一的安全策略，从而确保对应用程序或数据的安全可靠访问。相较而言，用户、设备、应用、服务等在 SASE 框架中都可以拥有一个独立身份，更加灵活；同时 SASE 框架可扩展性强。身份的综合维度越大，安全框架的防护潜力就越大。

基于流量分析

SASE 应具备流量重定向、检查和日志记录的功能。对于加密流量，能够解密检查并重新加密（理想状况下在云端完成）；对于敏感数据，能够正确识别并处理；对于隐私数据，能够隔离保护。要以一次性处理完流量优化和安全审查为目标。

云原生服务

SASE 将安全防护相关功能部署在 SASE 云的 PoP（Points of Presence）点中，由供应商统一提供和维护，降低了企业使用成本；通过云上可视化统一管理平台，降低运维人员操作难度。同时 SASE 依然保留了“盒子”，可以根据企业的需求，将安全决策点分布在企业边缘侧，但是集中管理平台必须在云上，从而提供统一的安全服务和策略管理。

分布式部署

SASE 框架可将安全能力和网络能力下沉到 PoP 点、CPE 或受控设备，从而满足低延迟和敏感数据等需求。分支和用户按照需要就近接

入。为了确保所有网络和安全功能随处可用，并且提供尽可能好的体验，SASE 需要有遍布全球的基础设施以及部署在用户侧满足安全和网络需求的 CPE（Customer Premise Equipment，客户端前置设备）设备或客户端，同时 SASE 管理平台能管理每个 PoP 点或边缘设备上安全和网络能力，推送统一的安全策略，可远程开通和关闭对应安全服务。

兼容各种边缘

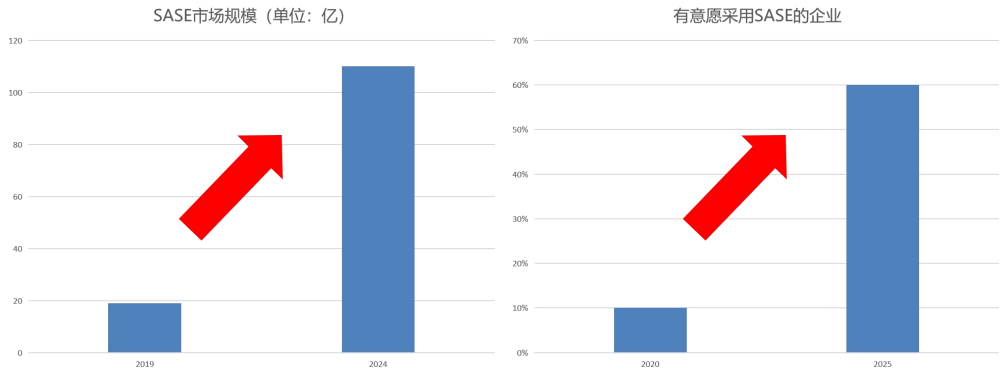
SASE 需要支持各种边缘。满足不同应用场景下边缘的需求，例如工业领域的边缘设备注重安全问题，卫生医疗领域除了安全问题，还注重隐私问题等等。其次，随着边界的模糊化，除了授权设备，很多不受管控的边缘设备也会接入 SASE。不同边缘设备配置、逻辑都不尽相同。因此，SASE 为了确保一致性，需要去支持所有边缘。

通过实现以上功能特点，SASE 框架相比其他安全服务方式，具备统一，灵活，服务三个优势：

- 统一，云平台统一管理安全和网络服务，配置和推行统一的安全策略，达到用户体验的统一，并尽量一次性处理完流量优化和安全审查。
- 灵活，安全功能根据客户的需求部署在云或者边缘侧，既能做到“薄分支，厚云端”，也能做到“厚分支，薄云端”。
- 服务， SASE 包含的技术服务非常丰富，多数企业难以自建自运维完备的安全和网络服务，SASE 将作为服务提供给企业用户，可以降低企业使用 SASE 的成本。

（三） 厂商实现

自 Gartner 于 2019 年提出 SASE 的概念以来，行业内对 SASE 的兴趣不断增加。一些企业非常看好 SASE 的发展前景，积极推出自己的产品，或者通过合作和收购等方式，逐步向 SASE 厂商转变。



数据来源：Garter:2021 STRATEGIC ROADMAP FOR SASE CONVERGENCE

图 2　SASE 市场预测[3]

根据 Gartner 的报告[3]，未来 5 至 10 年，SASE 将会成为主流安全解决方案。如图 2 所示，到 2024 年，SASE 市场规模将从 2019 年的 19 亿美元攀升至 110 亿美元，同时有 30%的企业将采用来自同一供应商的云交付 SWG、CASB、ZTNA 和 FWaaS 功能，而 2020 年这一比例不到 5%；到 2025 年，有至少 60%的企业将有明确的战略和时间表来采用 SASE，而在 2020 年仅有 10%。目前，国内信息安全行业消费正处于由硬件转服务的转型期，国内的 SASE 服务市场 2019 年开始起步，仍处于蓝海，国内乙方解决方案处于初级阶段。目前提供 SASE 的服务的厂商目前主要有安全厂商、网络厂商和云厂商三类。

安全厂商的优势在于安全技术的积累，但往往缺乏网络服务能力，同时只有少部分安全厂商具备从硬件到云的全栈安全产品。他们往往通过自建开发、合作或者收购等方式，加速自身向成熟的 SASE 供应

商的转变。Fortinet 很早就开始转型并构建了自己的 SD-WAN 网络，在硬件安全和 SD-WAN 服务方面具有优势。Fortinet 的 SASE 产品 FortiGate，被 Gartner 评为广域网和网络防火墙领域的领先者。Palo Alto Networks 也是最早采用 SASE 的厂商之一，收购了 SD-WAN 厂商 CloudGenix，优化了自己的产品，使自己的 SASE 平台能够支持远程办公并部署到更多传统的企业办公地点或零售地点。国内大部分的 SASE 供应商是安全厂商，例如山石、绿盟、深信服等等。其中山石和绿盟主要专注于提供安全产品，都倾向于和运营商合作获得 SD-WAN 的网络服务能力。借助运营商的网络建立 PoP 点，实现完整的 SASE 功能。而深信服致力于构建自有的网络和云服务。于 2020 年推出自己的 SASE 方案 Sangfor Access，在全国多省建立公有云 PoP 点，以 SASE 架构为核心，将已有的安全能力（如上网行为管理、终端安全检测与响应、上网安全防护、内网安全接入等）聚合在云上以服务化模式交付。

网络厂商大多拥有自己的 SD-WAN 网络设施和多个全球分布的 PoP 点，可以在原有网络产品的基础上，强化安全能力，推出自己的 SASE 产品。如：思科推出的 SASE 服务 SD-WAN 17.2 结合了 SD-WAN 网络和思科云安全保护伞（Umbrella），把网络、安全和零信任各个元素联系在一起。CATO Networks 是 Gartner 推荐的全球第一家 SASE 供应商，通过全球分布式云服务，为所有边缘提供企业网络和安全能力。目前，CATO 的全球专用网络中有 50 多个 PoP 点，所有 PoP 点都可以运行 CATO SASE 平台云原生软件堆栈。Versa 在欧美各国有多个

PoP 点，网络服务较为完善，目前也已经实现了全栈安全功能。同时 Versa 可以将安全功能虚拟化，部署在企业边缘侧，企业可以根据安全需求自由选择连接模式，非常灵活。

云厂商本身具有较强的云原生安全防护能力，可以结合网络服务转型 SASE。以阿里云为例，阿里云本身整体安全能力世界排名第二，在中国及东南亚市场具有领导地位，客户资源丰富，又有全球分布的 PoP 点，转型 SASE 条件成熟。2020 年底阿里云正式发布“云原生 SASE 解决方案”，将核心原生安全能力与网络能力融合，为云上用户提供了一个基于阿里云基础架构的 SaaS 化安全服务平台，其中云安全访问服务是阿里云 SASE 架构的核心产品。

表格 1 列举了主流的 SASE 供应商的主要产品和能力。其中√代表该公司的产品具有该项安全功能或者有可替代的功能，×代表该项能力缺失。

表格 1 SASE 供应商能力

厂商分类	厂商	主要产品/方案	核心能力					增强能力		
			SD-WAN	ZTNA	SWG	CASB	FWaaS	WAAP	Sandbox	RBI
运营商	电信	云堤	√	×	×	√	√	×	×	×
安全厂商	Fortinet	FortiSASE SIA	√	√	√	√	√	√	√	×
	Versa	Versa Secure Access	√	√	√	√	√	√	√	√
	PAN	Prisma Access	√	√	√	√	√	×	√	√
	山石	山石 SASE 方案	×	√	√	×	√	×	×	×
	绿盟	NPA、NIA	×	√	√	√	×	√	√	×
	深信服	Sangfor Access	√	√	√	×	√	×	×	×
网络厂商	CATO	Cato Cloud	√	√	√	√	√	×	×	×
	Cisco	SD-WAN 17.2	√	√	√	√	√	×	√	√
	Cloudflare	Cloudflare One	×	√	√	×	√	×	×	√
云厂商	阿里云	阿里云 SASE 方案	√	√	√	√	√	√	×	×

从当前 SASE 供应商能力可以看出，与国外 SASE 供应商相比，国内大部分 SASE 厂商服务功能不完善，有的缺乏 SD-WAN 网络服务，或者 PoP 点较少，覆盖面小，服务功能不完善；有的安全防护功能不全面，缺乏统一认可的安全技术标准对多厂家安全能力进行整合。

（四） 运营商实现 SASE 优势

遍布全球的网络接入是 SASE 服务框架的基础，而运营商网络具有丰富的网络接入、网络承载资源，在网络服务方面具有天然优势。并且在网络安全方面也积极投入并具有丰富的安全运维经验积累，在整合网络和安全服务方面具有天然的优势：

- 网络优势：运营商具有遍布全球的 SD-WAN 网络，可有效优化网络传输，为 SASE 提供丰富的网络服务，此外，运营商已有的其他网络或安全业务可以作为 SASE 建设基础；
- 资源优势：运营商可以在现有的 PoP 点、边缘云、中心云建立安全资源池，实现安全服务分布式部署的同时，节省建设成本；
- 运维优势：运营商具有完备的信息化服务系统、经验丰富的网络、安全运维团队；
- 政策优势：运营商构建运营 SASE，具备网络运营的政策性优势。
- 品牌优势：运营商具有广泛的行业客户基础，强大的品牌效应，由运营商推广的 SASE 服务更容易被企业客户接受；
- 标准优势：运营商通过推动制定企业标准、行业标准，能够将各厂家的网络和安全能力整合，为企业客户提供全栈、最优的网络、安全能力。

因此，运营商被认为是有能力实施 SASE 服务的最佳代表。国内运营商中，中国移动完成 SD-WAN 网络的规划和相关技术规范，在全国已经建设并提供网络服务，并完成 SD-WAN 网络安全服务架构设计，在端云协同安全联动机制、边缘设备安全防护、ZTNA 认证以及 FWaaS 统一纳管方面均有相关技术、产品和应用落地积累；中国电信也已经布局 SASE 业务，一方面与绿盟合作基于云堤的防护 DDoS 攻击、溯源取证等安全功能，建立远程开通定制化服务的网络与安全统一管理的云堤高防安全资源池，应用于“十九大”、“一带一路”峰会、杭州

G20 峰会等 10 余次国家重大活动的网络安防保障任务，同时服务数千家政企客户，同时在云堤基础上研究构建 SASE 框架；另一方面与山石合作，基于电信的 SD-WAN 网络业务和客户，将虚拟防火墙和 WAF 作为安全增值服务，逐步构建 SASE。由运营商对网络和安全能力进行整合，为企业数字化转型提供 SASE 服务，是推动 SASE 服务发展的最优选择。

二、 运营商 SASE 场景

（一） 概述

随着越来越多的企业业务上云，工业互联网边缘计算下沉，远程办公、在线教育、在线医疗等应用场景激增，网络数字化转型已经是大势所趋。相对于过去数据、应用集中部署、网络访问模型固定的场景特点，在新型业务场景下，数据及应用等资源分散在云端、分支机构和数据中心。另外，云端、分支机构和数据中心之间互访频繁、内外用户或第三方等多种实体从任意位置访问数据及应用。这种变化对网络、数据和应用的安全带来了全新的挑战。目前，企业传统边界被打破，访问互连更加动态灵活，传统的安全方案已经无法满足安全防护要求。本文以广域连接、移动/远程办公接入、客户/第三方接入、IoT 和边缘计算接入等场景为例，分析移动通信网络新型业务场景的特点和安全防护需求。

（二） 场景一：广域连接

传统企业网络以企业总部为中心，采用 MPLS 专线实现总部与分支之间的专线连接。分支之间的通信、分支访问互联网，一般要先经

过企业总部，在企业总部部署统一的安全防护措施。随着企业数字化转型和云服务架构的不断推进，越来越多的企业业务迁移到云端，分支与云端之间的互联互通更加广泛，分支直接访问互联网场景更加普遍。企业在数字化转型、网络互联需求激增的情况下，迫切需要大带宽、广连接、高质量、低成本的广域网络服务。

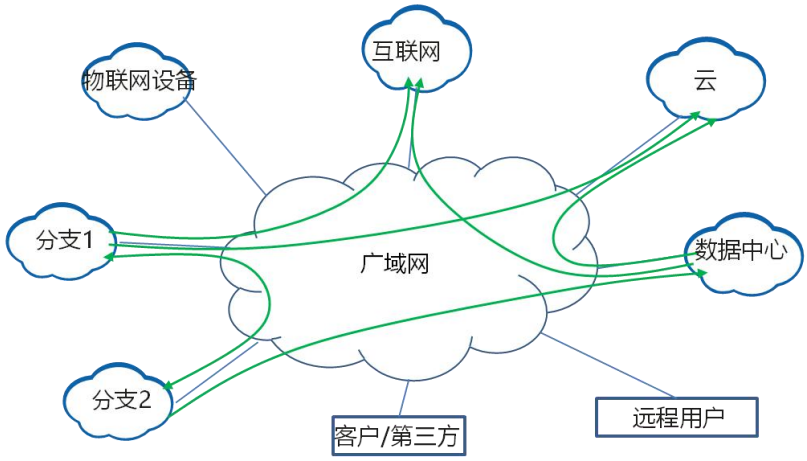


图 3 广域连接

如图 3 所示，新型广域连接，需要实现多实体跨广域网灵活互通，降低用户开支，提升网络服务质量，按需提供增值服务等。另外，还需要将单一的网络连接方式扩展到多种网络连接共存，根据不同服务需求，网络连接状态，动态实时选择采用 MPLS、Internet、5G 等不同的网络连接。广泛的分支、云、总部、Internet 互连代替原有的以企业总部为中心的组网。这些变化导致企业面临的安全威胁增多，为避免企业数据被窃取、篡改，需要在分支之间、分支与云（总部）之间提供专用的加密传输通道；为防护来自互联网的 DDoS 攻击、网络入侵等，需要同时对企业分支、云、总部部署边界安全防护设施；为防止非法用户接入分支、云、总部等，需要在分支、云、总部之间部署专用通道，部署身份认证机制等。

（三） 场景二：移动/远程办公接入

近年来受疫情影响以及企业为了缩减办公成本，需要为员工提供网络远程访问权限，方便员工随时随地办公。如图 4 所示，员工在家、出差时，需要使用笔记本电脑、手机等移动终端，无缝访问位于云端、数据中心的企业应用，并且能够同时访问互联网。

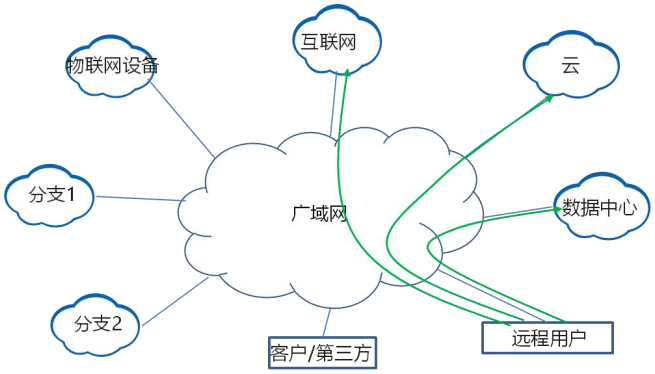


图 4 移动/远程办公接入

移动/远程办公场景下，为避免员工移动/远程办公终端被入侵后作为跳板攻击企业内部网络和应用，一般采用受管办公终端接入企业应用。企业应保护受管办公终端的安全，如过滤恶意网站、检测邮件安全，防病毒防入侵等。员工访问位于云端、企业内部的应用时，企业安全防护体系需要认证鉴权员工身份、监控员工行为，并持续对员工行为进行信任评估等。在员工移动/远程办公终端和企业应用之间加密传输数据，避免企业数据被泄露、篡改。检测员工终端下载的企业数据，避免员工下载、获取非授权数据等。

（四） 场景三：客户/第三方接入

随着企业业务云化部署，客户、第三方（承包商、合作伙伴等）访问的企业服务可能部署在企业总部，也可能部署在云端。企业安全

防护系统需要在云端和企业总部为客户、第三方提供一致的安全防护策略。

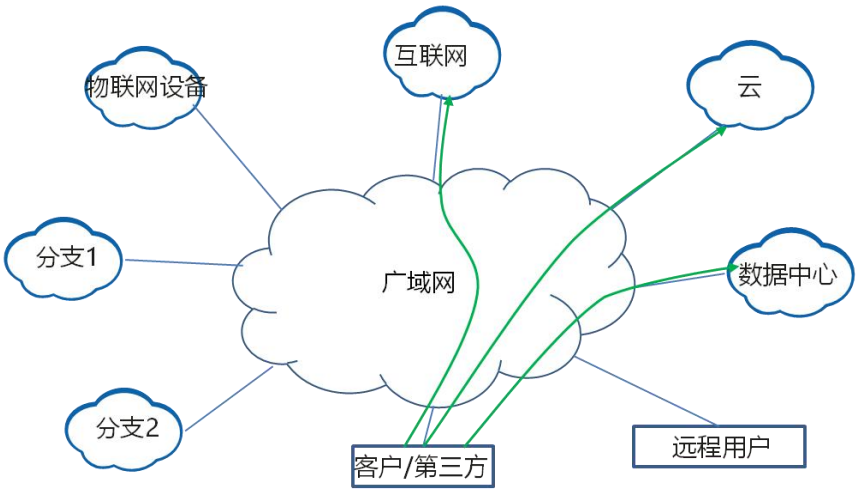


图 5 客户/第三方接入

客户、第三方的终端在访问企业服务的同时，也会访问互联网，并且客户、第三方终端一般不在企业管控范围内，终端自身的安全防护水平差异大，更容易被攻击者利用，成为攻击企业应用的跳板。为保护企业应用安全，企业需要限制客户、第三方的权限，重点防护来自客户、第三方的网络威胁。客户、第三方访问位于云端、企业内部的企业应用时，企业除了对访问者认证鉴权和行为监控外，还需要部署 WEB 防护设施、防病毒设施、入侵检测系统等，保护云端和企业总部的应用程序安全。另外，企业还需要监控加密/非加密数据流，防止非授权数据、敏感数据从企业内部流出。

（五） 场景四：IoT 和边缘计算接入

随着底层技术的进步以及应用的不断丰富，全球物联网产业实现爆发式增长。海量物联网终端接入到网络中，与物联网管理平台之间互相通信。一些 5G、IoT 场景对时延、可靠性要求高，需要将流量卸

载到本地边缘计算节点进行快速运算和处理。边缘计算节点对数据处理后，再将处理结果上送到云端或者数据中心。

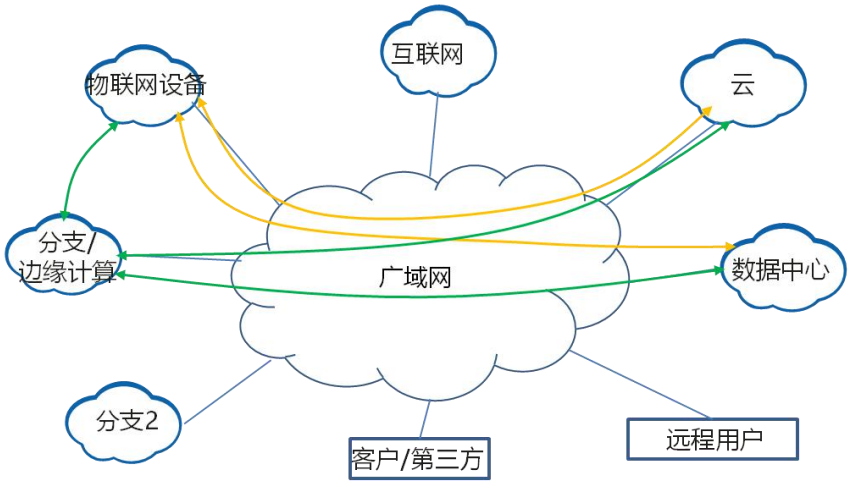


图 6 IoT 和边缘计算接入

IoT 设备接入到网络时，需要对 IoT 设备进行设备认证防止仿冒设备接入；需要防护来自海量 IoT 设备的 DDoS 攻击、网络入侵；需要对 IoT 终端的地址模糊化处理防止敏感信息泄露。边缘计算节点需要实现安全存储数据，防止用户数据泄露；需要实现租户资源隔离，为不同行业客户提供独立的网络、计算、存储资源；需要在 IoT 终端和边缘计算节点之间、边缘计算节点和云/数据中心之间建立加密安全通道，实现对用户业务数据的保护等。

在实际商业运行环境中，单一的接入场景一般无法满足企业需求，企业网络往往运行在多个基本接入场景构成的混合场景，例如：某跨国餐饮公司在世界各地有分店，分店与总数据中心互访，而员工或第三方要向餐饮客户送外卖，需要移动/远程办公接入和第三方接入。

三、 运营商 SASE 架构

（一） 功能需求

由上文场景中提取了如下需求清单，并列出满足需求的网络和安全能力。

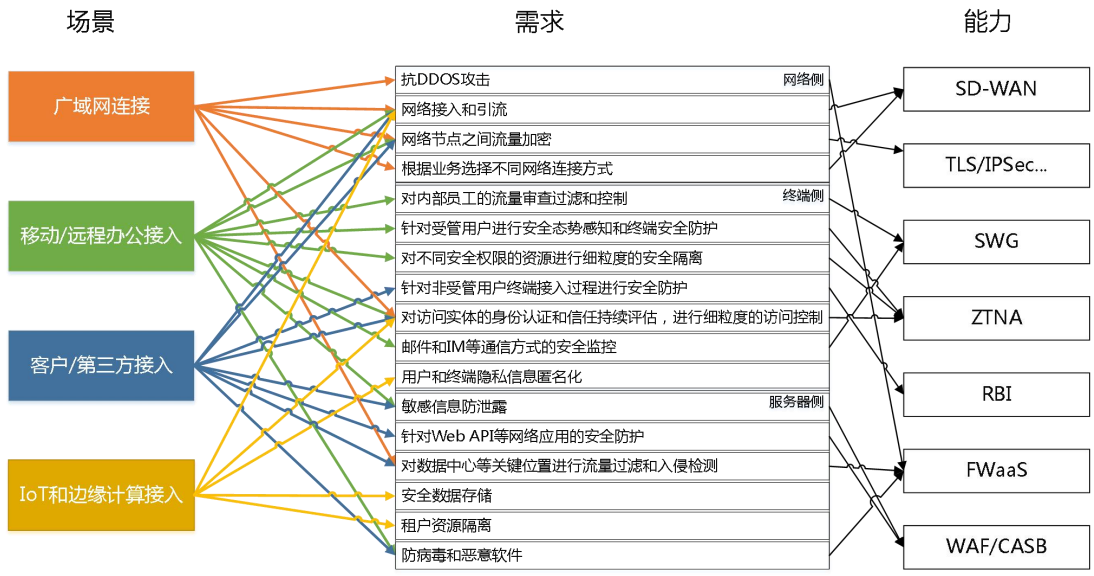


图 7　场景、需求、能力的映射关系

为了满足场景的需求清单，SASE 不仅包含满足对应需求的安全和网络能力，还需要能力的管理、编排和配置管理，即 SASE 框架的编排支撑层，此外还包括用户管理 SASE 框架能力、呈现分析结果和总体态势的管理呈现层，以及为其他层功能提供部署载体的基础设施层。

（二） 概述

SASE 的基础框架分为管理呈现，关键能力，编排支撑，基础设施四部分。

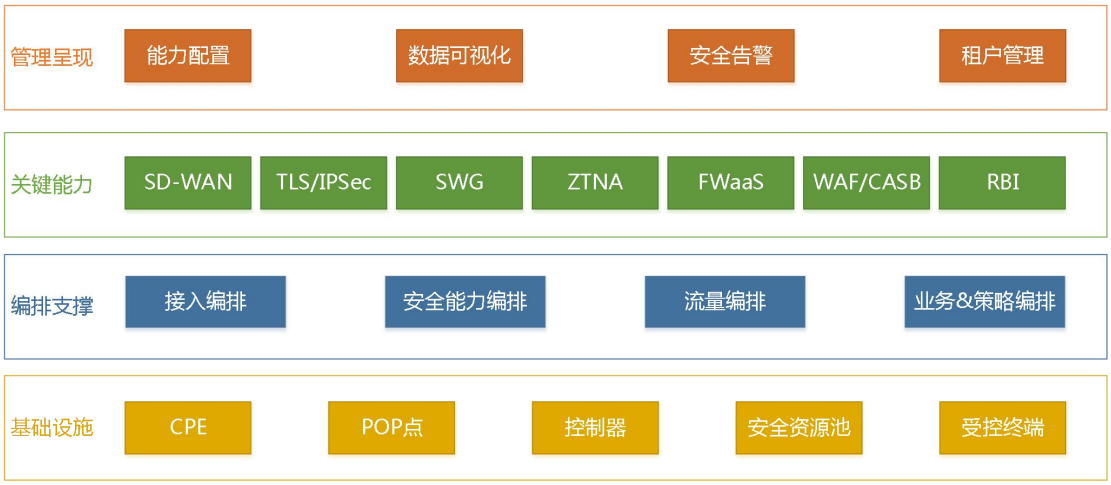


图 8 SASE 基础框架

基础设施层是部署运维管理，关键技术，基础支撑的软硬件设施，主要包括：CPE，PoP 点，控制器等 SD-WAN 基础网元，安全资源池等基础部署设施，以及受控终端等的软硬件设施，将在第四章详述；编排支撑层主要是对关键网络和安全能力的编排和管理，主要包括：接入编排、安全业务编排、安全能力编排、流量编排等，将在第五章详述；关键能力层为 SASE 框架针对场景需求提供网络和安全能力，其相关技术将在第六章详述；管理呈现层，是 SASE 对用户呈现的界面，主要包括能力配置，增值订阅，数据反馈分析，安全告警，租户管理等功能。

（三） 部署参考框架

SASE 的部署参考框架分为四部分：SASE 云、SASE PoP 点、SASE 边缘设备和 SASE 管理平台。

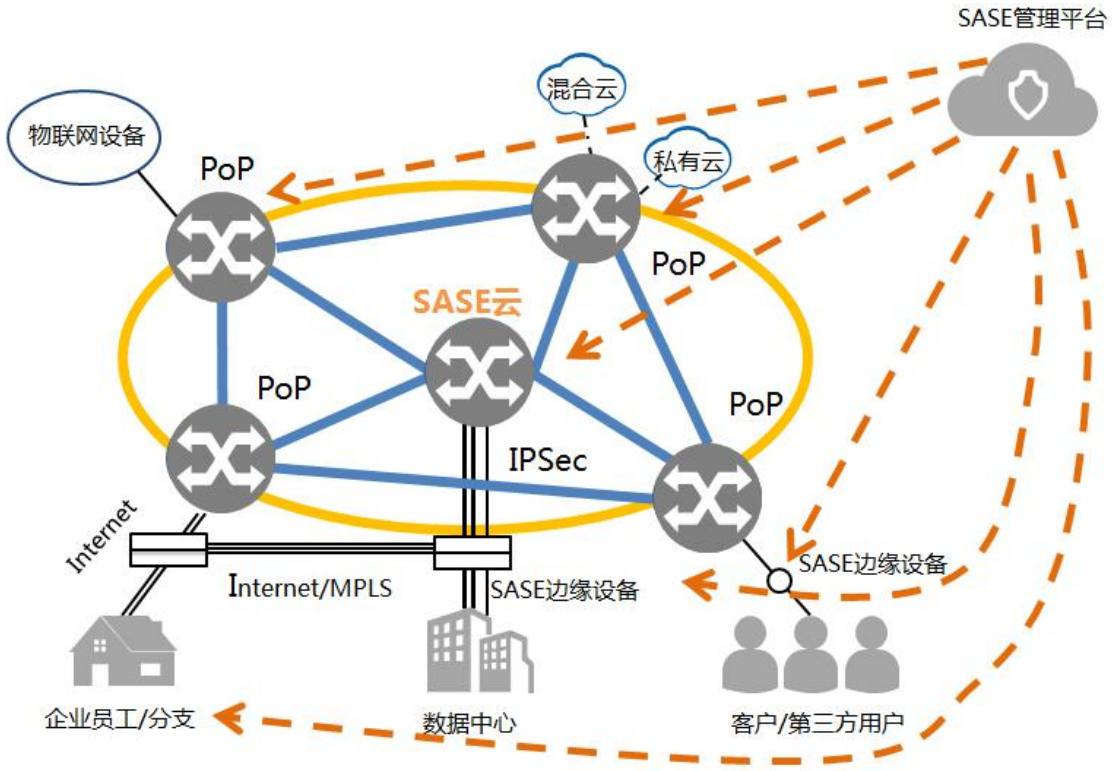


图 9　　SASE 部署参考框架

SASE 云是一张遍布全球的，整合了各种网络和安全功能的，可以服务各种边缘接入的多租户的云服务。内部结构对客户完全透明，由各地分布的 PoPs 点组成。

SASE PoP 点是 SASE 云的组成节点，作为 SASE 基础设施层的一部分，受 SASE 编排支撑层管控，承载 SASE 关键能力，可按需部署各类网络和安全能力，是 SASE 安全即服务功能的主要实现点。

SASE 边缘设备，包含受控终端和 CPE，作为 SASE 基础设施层的一部分，通过加密的通道连接到 SASE 云中适用的 PoP 点。SASE 边缘设备上可按需部署各种资源需求较低的网络和安全能力，受 SASE 编排支撑层管控，承载 SASE 关键能力，从而保证 SASE 框架的灵活性。

SASE 管理平台是一个统一的可视可管的控制平台，承载了 SASE 编排支撑层和管理呈现层的主要功能，负责网络和安全能力统一管理、

网络和安全策略配置、可视化运维等功能。客户可以按需订阅网络和安全服务，有选择地启用服务，配置它们来执行公司策略。

四、 运营商 SASE 基础设施层

（一） 概述

SASE 基础设施层是实现 SASE 网络和安全服务的软硬件基础，主要包括受控终端、CPE、PoP 点、安全资源池、控制器，实现 SASE 服务的编排支撑、提供网络和安全能力、实现 SASE 业务运营。

（二） 受控终端

企业员工、供应商、用户等，通过受控终端接入到 SASE 网络。受控终端设备形态可以是电脑、手机、平板电脑、小型移动网关等。在受控终端安装安全 SASE 客户端，通过 SASE 客户端对接 SASE 管理系统、提供网络和安全服务。

- 通过 SASE 客户端对受控终端提供网络服务，接入就近 PoP 点以便实现 SD-WAN 网络调优；
- 通过 SASE 客户端对受控终端提供安全服务，如上网行为管理、零信任接入、流量加密等；
- 通过 SASE 客户端被 SASE 编排支撑层纳管，实现对受控终端的管理。

（三） CPE

CPE（Customer Premise Equipment，客户前置设备）位于企业客户侧，用于实现将企业设备接入到 SASE 网络，产品形态可能是专用硬件设备，也能是通用服务器设备。

- CPE 受控制器管控实现按需引流，可同时支持接入多种网络接入方式，如互联网、专线、4G/5G 等，能够为企业客户不同业务提供不同类型的网络服务；能够根据网络状态调整企业客户网络连接等。
- CPE 将企业客户数据流量引流到 PoP 点，实现分支互通、分支入云、分支上互联网等网络服务。
- CPE 设备可自带防火墙、入侵检测等安全防护能力，保护企业网络安全；支持与 PoP 点之间建立加密隧道，实现对企业流量的保护。

（四） PoP 点

PoP 点，网络服务商提供的网络接入点，将企业 CPE、移动终端接入到 SASE 网络，并将数据流量向目的设备转发。SASE 服务商需要建立遍布全球的 PoP 点，并在 PoP 点建立分布式的安全资源池，为企业数字化转型提供网络和安全接入服务。

- PoP 点受控制器管控，可同时支持多种网络，如互联网、专线、4G/5G 等，可实现为企业客户不同业务提供不同类型的网络服务；可实现根据网络状态调整企业客户网络连接等。
- PoP 点转发企业客户数据流量，实现分支互通、分支入云、分支上互联网等网络服务。
- PoP 点支持 SD-WAN 网络优化功能，支持基于企业业务的网络加速、质量调优等功能。

- PoP 点承载安全能力，为企业用户提供多租户、按需部署、弹性伸缩的云化安全能力。
- PoP 点提供安全隧道加密能力，例如 IPSec（Internet Protocol Security，互联网安全协议），支持与 CPE、移动终端、其他 PoP 点、云/数据中心网关之间建立加密隧道。

（五） 安全资源池

SASE 可包含分布式安全资源池，支持多企业共享，降低资源池成本和提供资源池使用效率。SASE 安全资源池就近建立在网络转发路径上，如 PoP 点、专用安全云、公有云等，为企业客户提供实现低延时、就近防护的安全服务。SASE 安全资源池内的安全能力，可以是在通用服务器上部署的组件化安全能力，也可以是基于专用安全设备的云化安全能力。

- 安全资源池可部署丰富安全能力，具体应包括基于零信任的安全访问控制、SWG、FWaaS、CASB、入侵检测、WAF 等。
- 安全资源池支持多租户、按需部署、弹性伸缩的云化安全能力，为企业客户不同业务提供独立的、按需部署的安全防护。
- 安全资源池支持自动化编排，受 SASE 编排支撑层管控，实现网络与安全的融合、安全能力的按需部署。

（六） 控制器

SASE 管控的范围包括网络和安全，SASE 的控制器将网络和安全融合，实现网络流量引流和安全防护策略配置。设备形态上可以是将

网络和安全控制能力集中管理的控制器，也可以是独立的网络控制器和安全控制器，可根据业务规模多级部署。

- SASE 控制器实现受控终端、CPE、PoP、安全资源池的配置、监控、数据收集、信息上报，监控网络运行状态，控制网络流量转发路径。
- SASE 控制器支持向安全资源池配置安全防护策略，实现企业客户接入到不同安全资源池时，安全防护策略一致。
- SASE 控制器可根据网络规模级联部署，一级控制器统一管理二级控制器，二级控制器管理下挂设备。
- SASE 控制器北向对接 SASE 编排支撑层，将企业客户定制的服务在网络和安全资源池中最终实现。

五、 运营商 SASE 编排支撑层

(一) 概述

安全访问服务边缘 SASE 是网络连接能力与安全防护能力实现全面融合的服务提供形式。其一方面为用户提供端到端的连接与管理，实现高质量、低延时的网络通信。另一方面，将安全能力向边缘侧下沉，并支持轻量级、弹性扩展、按需使用的服务交付，就需要对安全和网络能力的统一编排和管理。SASE 框架的编排支撑主要包含接入编排，安全业务编排，安全能力编排，流量编排。

（二） 接入编排

接入编排将终端流量引导到适用的 PoP 点上。最常用的方案是 SD-WAN，在客户侧部署 CPE 设备，将流量引到适用的 PoP 点上来，也可以在终端设备上安装代理软件进行引流；具体功能如下：

- **全局负载、智能选路能力**：流量识别和全局负载能力，可基于 4~7 层流量信息并结合高效的智能调度算法，实现企业分支出口流量（访问公网流量/访问企业总部流量/访问公有云流量等）的智能隔离和按需选路。
- **隧道加密和流量牵引能力**：终端或 CPE 与 PoP 点之间建立加密隧道能力，针对企业流量实现按需引流和安全保障。可通过 IPSec、SSL、VPN 等技术实现。
- **多种网络环境的接入方式**：支持互联网接入、专线接入、4G/5G 接入等多种接入方式；
- **统一身份认证和权限管控能力**：支持通过多因素的认证能力，能够对接入对象实现统一身份认证，保障用户身份和设备合法性；通过用户风险、终端风险、UEBA 等信息进行综合评估，动态调整安全访问权限策略；可从应用、功能、身份、接口等维度，基于最小化原则，实现细粒度的访问控制；

（三） 安全业务编排

安全业务编排将用户安全需求的配置翻译成安全能力和策略配置推送给对应的安全能力，以及从安全能力获取处理结果，并翻译成用户或运维人员可见的统一数据格式。具体功能如下：

- **统一配置功能**：将 SASE 管理呈现层得到的用户策略配置，同步推送给全网部署的安全能力执行点。
- **安全能力处理结果反馈**：以统一格式实时向 SASE 管理呈现层反馈安全处理结果，以支持安全编排过程中，针对不同安全能力处理结果的实时响应。支持对系统和安全能力的日志采集、反馈与统计；支持告警展示与告警阈值配置；支持对全网安全能力的性能监控；
- **智能策略响应**：针对全网的安全态势，在运营人员接入之前，进行基本的智能策略响应。

（四） 安全能力编排

SASE 是一种 SaaS 化的网络安全服务，按照不同的安全业务需求，需要对多种安全能力进行灵活的编排，即对部署在不同基础设施上的能力自动化的创建、组网和配置。具体功能如下：

- **虚拟安全能力**：为了实现能力的自动化创建，需要能力的虚拟化部署，既可在虚拟机中部署，也可在容器中部署。
- **集中化的安全管理能力**：对安全能力进行集中化资源管理，策略管理，资源监控，同时提供统一的计量计费、服务模板、工单流转、运营与运维数据反馈等内容。

（五） 流量编排

接入编排将终端流量引到 PoP 点后，为了向用户提供安全服务，还需要再按需的把流量引入相应的安全能力，从 PoP 点到安全能力的引流过程即流量编排，需要使用到 SDN 技术、服务链技术以及各种不

同的隧道封装或路由技术，关键要保证不同用户流量的标识和隔离。具体功能如下：

- **流量解析和分析能力**：对用户接入的流量进行识别和分析能力，例如：识别流量的 TCP/UDP 协议、源目 IP 地址、Mac 地址、地域信息能力；接入端身份、客户端信息、登录时间等能力；识别流量的应用类型、应用协议信息能力；对用户流量信息进行统计分析能力等；
- **流量隔离和引导**：针对业务、用户、租户、优先级等不同属性的流量进行切片隔离，将其引流到不同安全能力，形成安全处理链，并最终引流到流量目的地。
- **网络统一监控能力**：支持全网流量信息、链路状态与性能的实时反馈；支持网络拓扑呈现，展示节点、接入终端的状态分布，应用流量分布，异常分支与终端的概要信息反馈。
- **多云资源连接能力**：支持将终端流量通过互联网或私网引流到多个主流公有云、私有云。

六、 运营商 SASE 关键能力层

(一) 概述

SASE 关键能力层主要包含 SD-WAN、基于零信任的安全访问控制、安全 Web 网关、云访问安全代理、防火墙即服务五个关键能力，这些能力可按需部署在 SASE 基础设施层上，SASE 编排支撑层的管理。其中 SD-WAN 是 SASE 重要的网络技术，实现了接入编排和流量编排功能，是整个 SASE 架构的基础，能提供统一的网络管理，解决网络服务按

需开通需求，同时 SD-WAN 还能将网络和安全结合，实现动态路由和安全访问控制；而基于零信任的安全访问控制 ZTNA 是 SASE 最关键的安全技术，接入方从任意位置接入时都必须统一通过基于 ZTNA 接入认证系统，以基于用户、设备、网络和应用的复合身份技术配合动态权限机制，解决面向所有边缘的统一接入的安全需求，实现 SASE 的身份驱动和边缘接入安全；安全 Web 网关（Secure Web Gateway，SWG）通常部署在公司内部用户对外访问的网关上，实现对内部员工的流量审查过滤和访问控制；云访问安全代理（Cloud Access Security Broker，CASB）部署在网络云外部，实现对云的防护和监控；防火墙即服务 FWaaS（包括入侵防御系统 IPS/入侵检测系统 IDS），通常部署在数据中心和分支机构等存储数据资源的关键节点上，实现对关键位置的流量过滤和入侵检测。

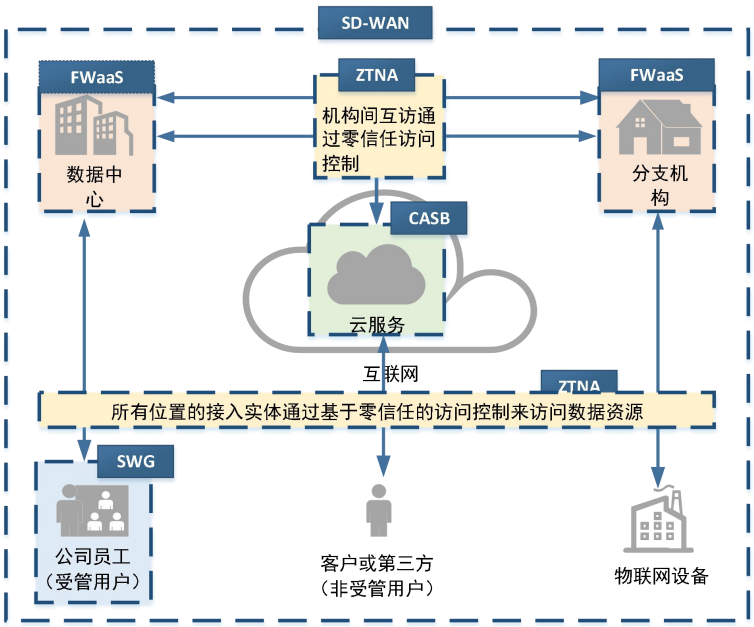


图 10　SASE 关键技术的部署位置和作用

由于技术众多、实现复杂，现有的 SASE 提供商通常在 SD-WAN 的基础上，集成二到三个关键安全技术，并提供统一的安全管控。

（二） SD-WAN

SD-WAN，软件定义广域网是将软件定义网络(SDN)技术应用到广域网（WAN）场景中的服务，即通过控制器来控制边缘 CPE 设备上路由转发策略，从而不依赖于专有的物理设备，弹性地解决了多分支结构企业网络在支持差异化服务等级应用能力、网络灵活度、线路成本、安全传输等方面正面临持续增长的压力，与必须做预配置的多协议标签交换（MPLS）链路相比，SD-WAN 网络架构具备弹性和低成本等优势[4]。

（三） 基于零信任的安全访问控制（ZTNA）

ZTNA：Zero-Trust Network Access，基于零信任的安全访问控制，即基于零信任的理念实现的网络访问控制技术。

零信任的核心理念为核心思想为“Never Trust,Always Verify”，即打破物理边界防护的局限性，不再默认信任物理安全边界内部的任何用户、设备或者系统、应用，而以身份认证作为核心，将认证和授权作为访问控制的基础[5]。该理念应用在访问控制领域：

- 将所有访问请求都默认为不可信，不再以位置作为安全依据，对所有访问请求采取安全措施。
- 采用最小授权策略和动态访问控制，即根据访问方，访问内容以及访问方式等上下文的来动态对访问方授权。
- 在访问开始对用户，设备，网络和应用进行身份认证，在每次访问过程中，对访问行为进行动态信任评分，以信任评分作为访问授权的依据。

（四） 安全 Web 网关（SWG）

SWG：Secure Web Gateway，安全 Web 网关。公司用于过滤员工的 WEB 访问，避免员工设备被恶意程序感染。SWG 至少包括 URL 过滤，恶意代码检测和过滤，用于 WEB 访问和即时通信和视频会议等基于 WEB 的软件。SWG 具备如下作用：

- 禁止员工访问不适当的网站或内容
- 在员工设备上，实施安全策略来加强公司内部的互联网访问
- 避免公司敏感数据泄露

SWG 可通过实体设备，虚拟设备，软件以及基于云或者混合等方式部署。SASE 框架中，SWG 可以基于云或混合等方式部署在边缘接入设备，设备本地处理一部分最常见的 URL 过滤，并访问云端来查询更多 URL 的合法性，作为端云结合安全能力的一部分。

（五） 云访问安全代理（CASB）

CASB：Cloud Access Security Broker，云访问安全代理，用于监听和管理云应用与用户之间的流量，保护云服务。云访问安全代理(CASB)可帮助组织消除在迁移至云后可能出现的安全漏洞。它通过实施访问策略来控制整个云体系（IaaS、PaaS 和 SaaS）的使用情况，确保管理员和用户能够安全访问和使用云资源。CASB 的核心价值是解决以下四个问题：

- 深度可视化：发现影子 IT，云服务，能够实现对用户活动的可视化。

- 数据安全：执行以数据为中心的安全，包括加密、令牌化、访问控制、信息权利管理。
- 威胁防护：检测和相应恶意的内部单位、特权用户威胁、入侵账户。
- 合规性：确定云中的敏感数据，并执行数据泄露防护策略，满足合规要求。

CASB 通常作为代理部署在企业数据中心，可通过 API、转发代理、反向代理等方式来实现。

（六） 防火墙即服务（FWaaS）

FWaaS：Firewall as a Service，防火墙即服务。防火墙即服务（FWaaS）是指提供下一代防火墙（NGFW）功能的云防火墙，包括访问控制，例如 URL 过滤、高级威胁防御（ATP）、入侵防御系统（IPS）、DNS 安全性和深度包感知（DPI）等功能。FWaaS 具备如下特点[6]：

基于用户防护：有别于传统基于 IP 或 MAC 地址来区分数据流的防火墙策略，FWaaS 具备用户身份管理系统系统，可实现基于用户的安全防护策略和可视化管控。

面向应用安全：FWaaS 具备“智能流检测”和“虚拟化远程接入”的特点。即一方面对各种应用进行深层次识别，分辨不同应用的流量，另一方将虚拟化技术与远程接入技术结合为远程接入终端提供虚拟化应用发布和虚拟桌面的功能，使终端无需装任何客户端即能与服务器端进行数据交互，达到终端与业务分离的目的。

云原生：相比传统的 NGFW，FWaaS 最大的特点是将安全策略部分或全部移至云端，取代传统硬件防火墙设备，来降低成本，简化部署和配置，并增强可扩展性。管理员可通过单一控制台进行集中策略管控，动态功能开启，对任意边界接入接入的相关用户，提供统一的安全防护策略。

（七） 其他新兴安全技术

目前，还有其他的新兴技术保护网络安全，包括云 Web 应用程序和 API 保护即服务(WAAP)、软件定义边界(SDP)、远程浏览器隔离(Remote Browser Isolation, RBI)和网络沙箱(Network sandbox)等。

云 WAAP 是云 web 应用防火墙服务的演变，并扩展了其范围和安全深度，是继 WAF 之后的更全面的运行时保护。WAAP 服务结合了 DDoS 保护、bot 缓解、API 保护和 web 应用防火墙(WAF)，部署速度更快，组织维护起来也更容易。据 Gartner 称，到 2023 年，30%以上的面向公众的 Web 应用程序和 API 将受到云 WAAP 的保护[7]。

SDP 旨在通过网络隐身技术，构建起一个云安全边界，确保只有合法的身份、设备和网络环境等实体才能接入，对其他工具完全不可见。由于看不到目标，因此有效地规避了各种安全风险。同时，SDP 还有一个很重要的零信任机制，就是在访问过程中对实体行为持续进行安全等级评估，并对风险行为进行动态控制，从而有效保护网络安全。

RBI 解决方案是针对浏览器安全威胁防护提出的安全防御方案。它该技术将 Web 浏览活动控制在一个孤立的云环境，保护用户免遭网站上可能隐藏的任何恶意软件或恶意代码的侵害。

网络沙箱是一个虚拟系统程序，为运行中的程序提供的隔离环境。它允许用户在沙盘环境中运行浏览器或其他程序，运行所产生的变化可以随后删除，通常是为一些来源不可信、具破坏力或无法判定意图的程序提供隔离空间。

七、 运营商 SASE 管理呈现层

SASE 管理呈现层即为用户以及运维人员提供的管理界面，包括：能力配置，数据反馈分析，安全告警，租户管理等功能。

- 能力配置：通过统一的界面实现针对安全能力进行集中化的订阅开通，资源管理，策略管理，资源监控，同时提供统一的计量计费、服务模板、工单流转等诸多内容。
- 数据可视化：构建运营与运维数据大屏，对全网流量信息、链路状态与性能、以及安全检测和处理结果的实时展示；网络拓扑呈现，展示节点、接入终端的状态分布，应用流量分布，异常分支与终端的概要信息展示。系统自身和各安全能力日志的统一展示、统计、分析与检索和导出，支持安全态势可视化展示，通过时间、空间等多种维度展示 IT 架构总体安全情况。
- 安全告警：当安全处置过程中，出现紧急情况，支持对用户和运营人员的安全告警，可通过手机，微信等渠道。
- 租户管理：对用户下属租户进行权限分类和配置管理。

八、 SASE 应用案例

(一) 概述

目前，SASE 在国内外已经有多个落地应用案例，通过对已落地案例的调研分析，现有 SASE 落地案例主要集中在多分支接入、移动办公/远程接入和互联网暴露面统一管理三个方向。

（二） 案例一：SASE 的多分支接入案例

场景背景：

零售业，金融业，物流等行业的连锁公司需要在全国全球各地建立大量分支机构，需要以较低成本，同时满足以下三点需求：

- 企业组网需要满足三种相互隔离的连接需求:分支机构连接数据中心、分支机构之间的互访、分支机构访问互联网和公有云。
- 连锁公司的核心业务流量需要高可靠性和高安全性，如零售业的 POS 机流量，金融行业的金融业务处理流量，物流行业的物流业务流量。
- 随着一带一路发展，大量国内连锁企业出海，在海外建立分支机构，需实现全球接入。

SASE 能够以较低的成本实现以上三点需求，可在多分支接入场景中广泛应用落地。多分支接入场景的 SASE 改造典型案例如下：

某连锁企业在全球有 1000+ 家分支，每个分支机构设备通过 MPLS 连接数据中心和其他分支，通过普通线路连接互联网和常用云服务。

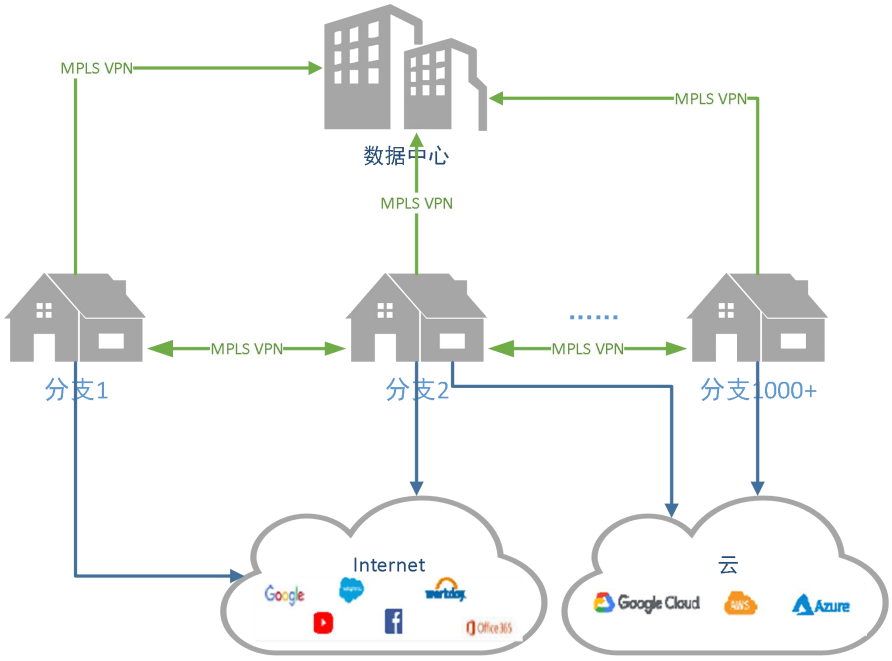


图 11 多分支接入典型场景

场景需求：

- 全球的统一的网络和安全解决方案，分支就近接入。
- 核心业务流量需要保证高安全性和高可靠性，尤其是业务高峰期，需与其他流量进行切片和隔离。
- 为了简化管理节省成本，希望一套设备和线路，同时访问数据中心、其他分支、互联网以及云服务，还能保证各种流量安全隔离，并保护和规范员工上网行为。
- 弹性的流量扩容，更方便的建立新的分支站点。
- 安全策略统一制定和推送。

SASE 解决方案：

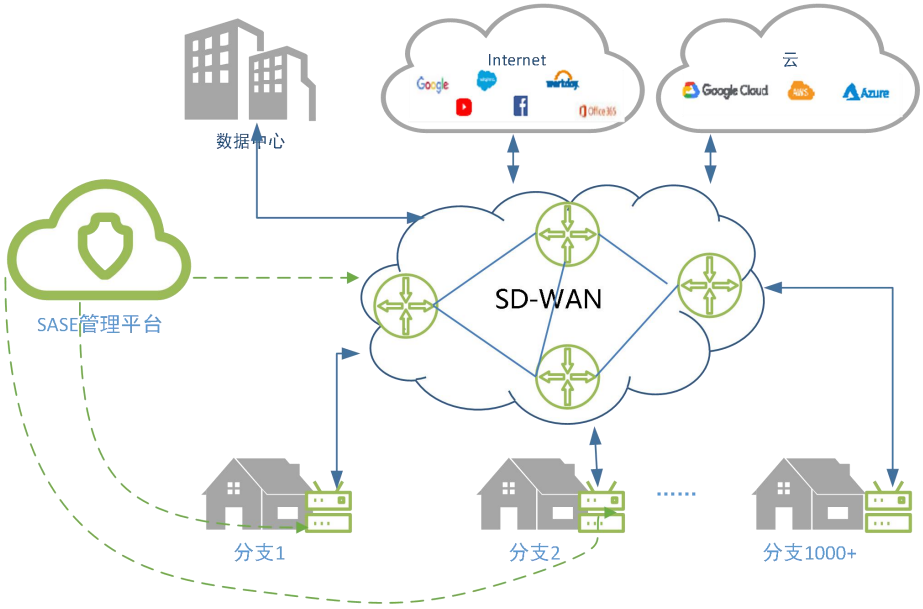


图 12 多分支接入典型场景 SASE 改造方案

- 遍布全球 SASE 的 PoP 点，分支机构可就近接入。
- PoP 点上按需部署 SWG 等安全功能，规范和保护员工上网行为，减少多分支下的安全设备投入。
- 每个分支部署 SASE CPE，接入互联网、数据中心、其他分支等，减少网络设备数量。SASE CPE 根据内容识别、隔离、切片核心业务流量和访客流量等其它门店内流量，针对高峰期的核心业务流量进行网络质量保障。
- 通过 SD-WAN，实现业务自动化开通和弹性扩容。
- SASE 管理平台实现网络和安全统一管控。

（三） 案例二：SASE 的移动办公/远程接入案例

移动办公/远程接入场景下，员工移动/远程办公终端会成为攻击者入侵的入口、企业信息泄露的通道，因此，企业需要对员工终端进

行统一管控和安全防护，并部署防泄密、身份信息校验等安全防护能力。

- 为避免移动/远程场景下员工访问恶意软件或带病毒网站、接收有害邮件，导致员工终端受到入侵，攻击者以此为跳板攻击企业关键资产的事件发生，企业需要统一管理员工移动/远程办公终端，并进行恶意网站过滤、邮件安全检测、防病毒等安全防护。
- 为降低移动/远程场景下，员工访问企业内部应用、云端服务时，由于终端环境不可控造成的安全风险，需要对员工身份进行识别，监控员工行为并根据员工行为持续地进行实时信任评估。
- 为防止移动/远程场景下员工通过办公终端传输的企业数据被窃听、篡改的风险，给企业造成损失，企业需要对传输数据进行加密，防止企业数据被泄露、篡改。
- 为解决移动/远程办公时，传统 VPN 无法抵达云端服务，互联网接入云端服务面临安全性风险的问题和员工通过移动/远程办公终端使用传统 VPN 接入内网应用，权限无法细粒度管控，不能具体到应用、到员工，员工获取非授权数据的问题，企业更新网络接入能力，细粒度管控到每个员工、应用的权限，并检测员工终端传输企业数据，避免员工获取非授权数据。

通过部署 SASE 系统满足企业需求，SASE 控制中心设置在云端，用户边缘按需部署多个 PoP 点，便于员工移动/远程办公终端接入系

统。办公终端上安装具有引流等功能的 SASE 客户端，负责将员工上网流量引流到 PoP 点。

SASE 平台在 PoP 点开通多种安全能力保证移动/远程办公全流程中的安全，包括恶意网站过滤、邮件安全检测、防病毒模块等。通过高级威胁检测防护模块防护未知威胁，开通 EDR 模块实现事件快速响应。

PoP 点加载零信任上网行为管理模块，实现员工上网准入、多因素认证并持续地对员工上网行为、所处环境等实体信息进行实时信任评估和权限管理。PoP 点加载 DLP 功能模块，通过身份校验和传输数据加密等操作，保证企业数据在移动/远程办公传输过程中的安全，实现企业数据防泄密。

员工移动/远程办公终端流量通过 SASE 客户端引流至边缘 PoP 点，通过 PoP 点访问内部应用或云端服务，无需通过 VPN 进行加密传输，PoP 点上的身份管理模块实时身份信息校验，维持员工最小访问权限，无法访问任何非授权资源，保证企业数据安全性。

通过 SASE 系统，为企业提供全套的上网安全、防泄密、终端防护服务。

SASE 系统总体架构图如下。

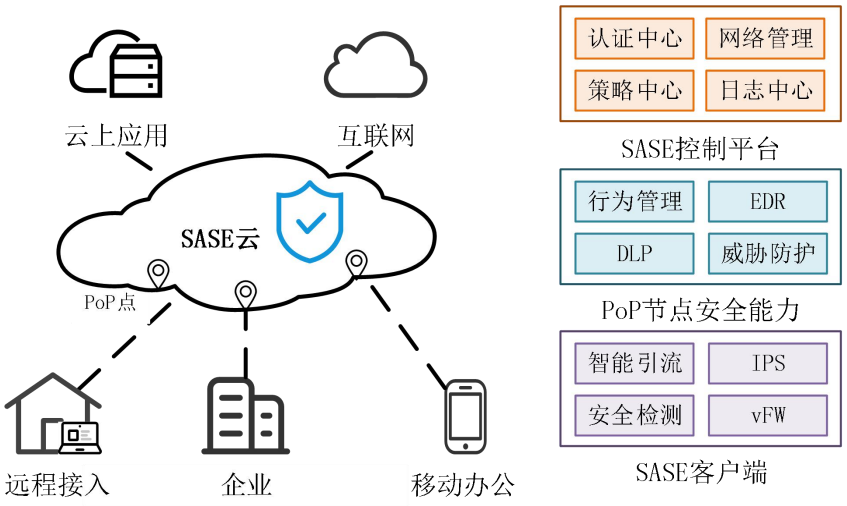


图 13 SASE 的移动办公/远程接入案例总体架构图

运营商提供 SASE 服务的优势是运营商具备完善的 SASE 系统所需要的基础设施，包括网络接入资源、PoP 点、云资源和安全能力等，无需用户投资建设 SASE 基础设施。用户通过服务化的方式即可享受运营商提供的 SASE 服务，配置快，成本低。

运营商可为企业提供企业侧 SASE 设备租赁服务，用户租赁运营商设备，无需自购企业侧硬件设备进行更新，降低用户成本。

运营商可为企业提供完善的网络和安全运维服务，用户无需为 SASE 系统部署大量专业运维人员进行系统维护，可交付运营商完成日常维护。

（四） 案例三：SASE 的互联网暴露面统一管理场景

场景背景：

十三五以来，国务院、国资委发布中央企业信息化工作的指导意见，明确要求：能源、电力等的重要信息系统和互联网等基础信息网络要严格安全管理，减少政府机关的互联网连接点数量。国务院发布国家政务信息化工程建设规划，要求“减少各部门互联网出入口数量，

推进党政机关互联网统一接入。国资委下发明确要求：加快集团公司及所属企业互联网出入口收敛切实减少暴露面和风险点，初步形成基础设施一张网、资产态势一张图安全监管一盘棋、风险管控一条线、产业服务一站通等支撑能力。

因以上政策要求，政企、能源、电力等行业的相关企业亟需收敛暴露面，并在数据汇聚节点上进行流量过滤监控，保证上网行为合规。该类场景的 SASE 改造的典型案例如下：

某大型国企集团原本通过多个 PoP 点上互联网，但在国务院和国资委政策要求下，必须收敛企业互联网出入口，各分支和总部流量从有限个出入口统一接入互联网。同时企业分支机构之间和总部中心直接互访，无需汇聚到互联网出入口。

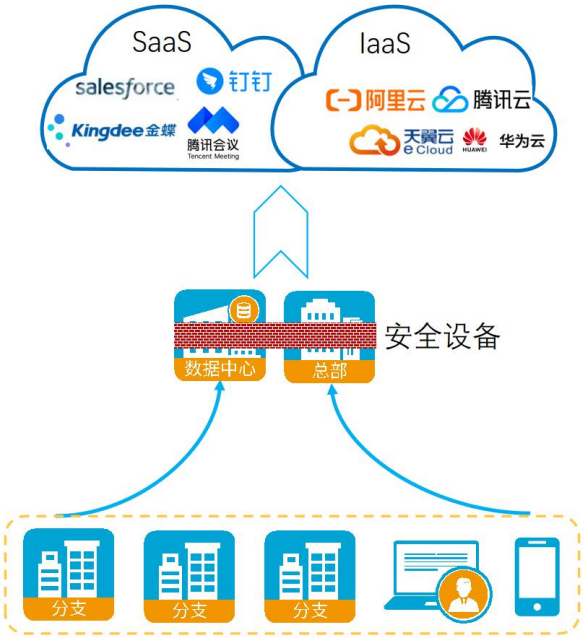


图 14　互联网暴露面统一管理典型场景

场景需求：

- 收敛互联网出入口。

- 互联网流量通过大型分支机构或者总部的广域网专线汇总到区域中心的统一互联网出口访问 Internet，满足流量归集需求。
- 要求不同云中心分管一个片区，且互为备份。
- 各分支按需组网，互联流量不经总部绕转。
- 保护和规范分支机构和总部中心访问互联网的行为，防范恶意软件、恶意连接和数据泄露以及未授权的资源访问、并实现上网行为合规化。
- 保护分支之间与总部中心的互访行为，防范恶意软件，恶意连接和数据泄露以及未授权的资源访问。
- 重点保护主要分支节点和数据中心，来防范入侵和 DNS 攻击和 APT 攻击等安全威胁。
- 提供持续的安全能力与服务。

SASE 解决方案：

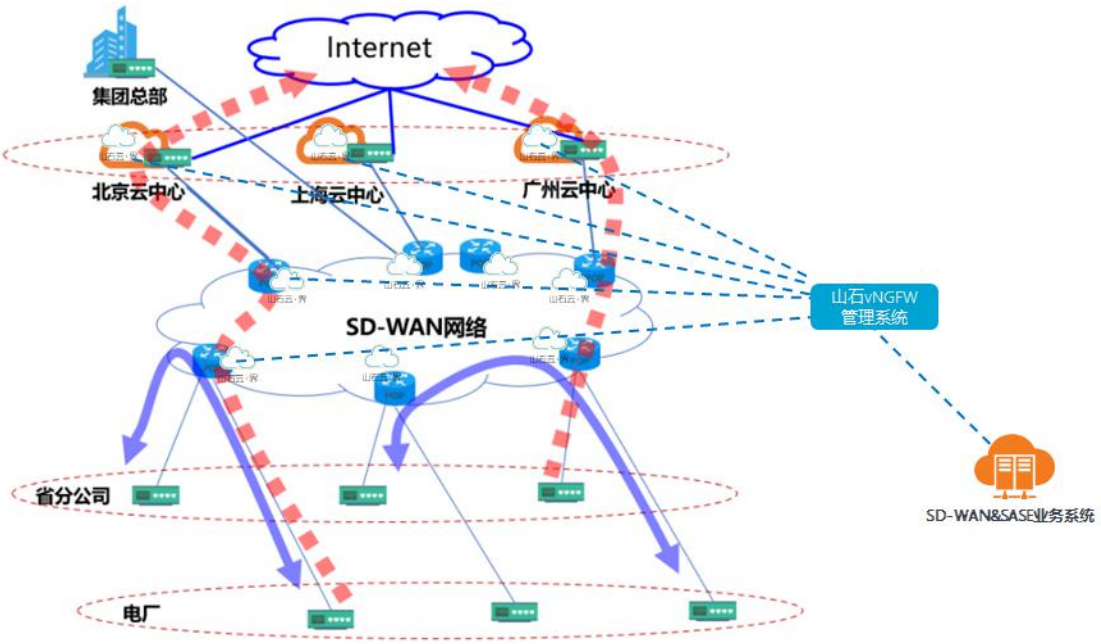


图 15 SASE 互联网暴露面统一管理的总体架构图

- 互联网出口部署性能匹配数量的 vNGFW，互联网出口路由设备按租户给 vNGFW 引流（南北向安全：应用防火墙、入侵防御、病毒过滤、URL 过滤、带宽管理）
- 每个 PoP 点部署性能匹配数量的 vNGFW，PoP 点路由设备按租户给 vNGFW 引流（东西向安全：应用防火墙、入侵防御）
- 所有 vNGFW 都被分租户集中管理
- vNGFW 管理系统提供 API 供 SD-WAN&SASE 业务系统进行业务包装

九、 SASE 建设技术难点

SASE 框架自提出以来，因其适应国内外网络发展的新需求，国内外厂商纷纷投入布局。运营商建设提供 SASE 服务框架存在天然优势，也存在待突破的技术难点，为了能纳管调度多厂商和多部署位置的网络和安全能力，下面围绕 SASE 四层框架分析建设技术难点：

SASE 基础设施层

SASE 框架下的网络和安全能力来自多家厂商，部署的模式有虚拟部署，容器部署，物理部署等多种方式，差异巨大，且可部署在 CPE，运营商 POP 点，安全能力资源池和受控终端等多个位置。技术难点在于：

- 各类网络和安全能力通常来自不同的网络，难以打通网络，实现多个厂商多部署位置的网络能力和安全能力的统一调度。
- SASE 框架下基础设施类型多，厂商和品牌都不同，难以对基础设施实现统一的运行状态监控和日志告警收集处理。

SASE 编排支撑层

SASE 编排支撑层，需要对安全和网络能力的统一编排和管理，主要功能包含安全业务编排，安全能力编排，网络能力编排。主要技术难点在于：

- 需要面向多个厂商，不同部署位置，不同类型的网络和安全能力进行统一调度和编排，目前缺乏统一的功能编排管理框架以及相关接口标准，导致集成效率低成本高，需要大量适配工作。
- 各个厂商的功能接口差异较大，且功能设计的执行逻辑也不同，同时纳管和编排多个厂商的网络和安全功能的难度较大。

SASE 关键能力层

SASE 关键能力层，由多家网络和安全厂商参与提供能力，网络和安全能力需要统一接口，才能实现统一调度和编排。其技术难点主要在于：

- 各个网络和安全产品之间的功能划分不明确。各类安全能力之间存在功能重叠的问题，且不同厂商提供的安全能力覆盖范围也不同，需要一套成熟的原子能力划分，用于指导厂商设计标准化原子产品功能，从而高效的实现安全能力之间综合编排。
- 各类安全能力普遍缺乏统一的一致性接口。接口必须具备注册，调用，日志反馈，运行状态监控等基本功能。目前安全能力接口标准化的过程正在进行中，尚处在针对特定安全能力（如防护墙，漏洞扫描等）的标准化过程。尚未出现安全能力的统一接口，便于不同厂商不同类型的安全能力的统一编排和调度。

SASE 管理呈现层

SASE 管理呈现层即为用户以及运维人员提供的管理界面，包括：能力配置，数据反馈分析，安全告警，租户管理等功能。其技术难点主要在于：

- SASE 涉及的网络和安全能力类型非常多，导致 SASE 管理呈现层的配置管理的 UI 界面复杂，需要用户了解相关安全能力的原理和配置方式，使用和学习成本非常高。
- SASE 涉及多个厂商多种部署方式和部署位置且多种类型的网络和安全能力，其产生的日志告警，运行状态等运维数据量大而类型多，难以分析处理和呈现，很难直观的让用户了解策略执行结果以及整个系统的运行状态。

运营商为推进 SASE 服务框架大规模商用，增强网络和安全附加值收益，下一步需重点关注以上问题。

十、 总结

本研究报告介绍了 SASE 框架的产生背景、定义特点、发展现状以及运营商构建 SASE 框架优势，归纳了 SASE 框架的适用场景，总结场景所需的网络和安全能力，构建了 SASE 的基础架构，并简要介绍 SASE 基础架构所包含的管理呈现，关键能力，编排支撑，基础设施四个部分，给出了 SASE 的应用案例，总结了运营商建设 SASE 需关注的技术难点，对运营商构建 SASE 框架提供了指导建议。

十一、 缩略语

缩略语	英文全称	中文含义

SASE	Secure Access Service Edge	安全访问服务边缘
IAM	Identity and Access Management	身份管理与访问控制
NGFW	Next generation firewall	下一代防火墙
vNGFW	virtual Next generation firewall	虚拟下一代防火墙
SWG	Secure Web Gateway	安全 Web 网关
SD-WAN	Software Defined Wide Area Network	软件定义广域网
CASB	Cloud Access Security Broker	云访问安全代理
ZTNA	Zero-Trust Network Access	基于零信任的安全访问控制
FWaaS	Firewall as a Service	防火墙即服务
PoP	Point Of Presence	
WAAP	Web Application and API Protection	云 Web 应用程序和 API 保护即服务
WAF	Web Application Firewall	Web 应用防火墙
Sandbox	Network sandbox	网络沙箱
RBI	Remote Browser Isolation	远程浏览器隔离
MPLS	Multi-Protocol Label Switching	多协议标签交换
DDoS	Distributed Denial of Service	分布式拒绝服务攻击

IoT	Internet of Things	物联网
MEC	Mobile Edge Computing	移动边缘计算
CPE	Customer Premise Equipment	客户前置设备
DTLS	Datagram Transport Layer Security	数据包传输层安全性协议
IPsec	Internet Protocol Security	互联网安全协议
SSL	Secure Socket Layer	
VPN	Virtual Private Network	虚拟专用网络
SaaS	Software-as-a-Service	软件即服务
SDP	Software Defined Perimeter	软件定义边界
UEBA	User and entity behavior analytics	用户和实体行为分析技术

[1] FLEXERA™ 2020 STATE OF THE CLOUD REPORT, FLEXERA, 2020

[2] THE FUTURE OF NETWORK SECURITY IS IN THE CLOUD , NEIL MACDONALD, LAWRENCE ORANS, JOE SKORUPA, 2019-08-30

[3] 2021 STRATEGIC ROADMAP FOR SASE CONVERGENCE ,NEIL MACDONALD, NAT SMITH, LAWRENCE ORANS, JOE SKORUPA, 2021-03-25

[4] SD-WAN 关键技术, 柴瑶琳/CHAI YAOLIN，穆博/MU YUBO，马军锋/MA JUNFENG, 2019-03-26

[5] ZERO TRUST NETWORKS: BUILDING SECURE SYSTEMS IN UNTRUSTED NETWORKS. , E. GILMAN, D. BARTH, 2017

[6]WHAT IS FIREWALL AS A SERVICE? : HTTPS://WWW.ZSCALER.COM/RESOURCES/SECURITY-TERMS-GLOSSARY/WHAT-IS-FIREWALL-AS-A-SERVICE

[7] DEFINING CLOUD WEB APPLICATION AND API PROTECTION SERVICES., GARTNER, 2017-10-24

中国通信标准化协会 TC610

地址：北京市海淀区花园北路 52 号

邮政编码：100191

联系电话：010-62300069

传真：010-62300094

网址：www.sdnfv.org