# SASE安全访问服务边缘白皮书

CSA GCR cloud security alliance ®
GREATER CHINA REGION

# 致 谢

云安全联盟大中华区（简称：CSA GCR）SASE 工作组在 2021 年 10 月成立。由林冠烨、何国锋担任工作组联席组长，工作组专家来自深信服、中国电信、新华三、Fortinet、绿盟科技、白山云、启明星辰、缔盟云、奇安信、安恒、安全狗、万科、缔安、腾讯、信通院等十多个单位。

本白皮书由 CSA 大中华区 SASE 工作组专家撰写，感谢以下专家的贡献：

联席组长：林冠烨、何国锋

贡献者名单

原创作者：张琦枫、岑义涛、郭思麟、钟施仪、朱传江、毕亲波、廖奎敬、王茜、郑舟、何春根、吴致远、叶晓刚、黄超

审核专家：郭鹏程、姚凯

研究协调员：郭思麟

贡献单位：深信服科技股份有限公司、中国电信股份有限公司研究院、新华三技术有限公司、防特网信息科技（北京）有限公司（Fortinet ）、绿盟科技集团股份有限公司、贵州白山云科技股份有限公司、北京启明星辰信息安全技术有限公司、杭州云缔盟科技有限公司、奇安信科技集团股份有限公司、杭州安恒信息技术股份有限公司、厦门服云信息科技有限公司、上海缔安科技股份有限公司、腾讯云计算（北京）有限责任公司、北森云计算有限公司

（以上排名不分先后）

关于研究工作组的更多介绍，请在 CSA 大中华区官网（https://c-csa.cn/research） 上查看。

如本白皮书有不妥当之处，敬请读者联系 CSA GCR 秘书处给与雅正！联系邮箱： info@c-csa.cn；云安全联盟 CSA 公众号：

# 序 言

云计算、物联网、边缘计算等新兴技术的迅猛发展，对传统安全防御方式带来了极大挑战，CSA 的前沿研究一贯鼓励网络安全创新理念，例如网络业务与安全技术的深度融合。

自 2019 年 Gartner 提出安全访问服务边缘（SASE）的概念起，海外的安全厂商、新创公司，甚至是运营商和网络设备厂商，都纷纷开始投入这个领域，不约而同的推出了自己的解决方案并在市场上得到快速的增长。

2020 年，SASE 在国内也开始成为各类安全厂商们追逐的下一个风口。在市场上各类不同的网络和安全方案都基于自己的技术和模式，提供了 SASE 的解决方案。蓬勃发展对整个行业发展和用户选择是一件好事，但缺乏标准化可能也会导致技术的发展受限于割裂的技术框架，甚至会停滞不前。就像是安全设备的的日志不统一导致安全运营效果的问题。

因此，本白皮书希望联合行业内的专家提供专业的回答来解释 SASE 是什么，基于什么样的技术，如何采用这个技术和解决方案，从而来推动 SASE 在国内的发展。让更多人了解到这个技术带来的变化和好处。同时，这只是个开始，本工作组将会联合厂商推出更多的标准，行业最新的信息，让整个技术规范化和标准化，让 SASE 的技术能在中国加速的发展。

李雨航 Yale Li

CSA 大中华区主席兼研究院院长

# 目录

# 1. SASE 概述

## 1.1 SASE 背景

随着云计算、物联网、5G 等关键技术的不断突破发展，企业数字化转型节奏越来越快。企业为提高核心竞争力，其业务部署环境越来越多样，包括传统的 IDC 机房、私有云、多云、混合云等，同时业务访问端也由单一的内部用户扩展到企业分支用户、企业合作伙伴、远程移动办公终端等。

在这个过程中安全紧随企业的网络和业务架构演进而发展。十几年前，企业业务流量总量不大、流量以内部流转为主、移动办公需求少且默认企业内流量安全，这种情况下集中式安全栈方案得到大规模应用，这种以企业自建数据中心为核心的中心辐射型网络拓扑备受企业青睐。

近几年，随着云端 SaaS 应用普及和企业员工分散导致企业互联网流量增多，中心辐射型网络架构面对高成本的 MPLS 链路、总部集中上网应用访问体验差、安全边界绕行及总部 VPN 容量挑战等问题，不得不顺势改变网络及安全建设思路。在此阶段 SDN 及 NFV 技术的发展促使企业在云端部署统一网络指挥中心成为可能，分支和总部互联可通过更便宜和更大的互联网宽带进行以分散专线压力。同时，对于远程用户来说，云端部署的安全接入网关类服务能够有效解决集中接入的体验和安全问题，此时云端或者总部集中提供网络调度和近源安全监测防护理念越来越深入人心。

现在及未来几年，越来越多的公有云厂商，甚至有全球业务的 ICT 厂商、互联网厂商都在建设自己的数据中心，这些数据中心随着企业业务的不断扩张，业

务范围越来越广，服务数量越来越多，连通性越来越好。也许，是受“云”资源共享商业模式的启发，有声音提出此类拥有全球互联数据中心的企业是否可以将这种互联骨干网作为资源共享出去，企业想要访问的多云、公共 SaaS、互联网等连通问题由此骨干网解决，有互联需求的其他中小型企业均可以把流量引入这张网络中进行流转，同时为了降低时延提供统一的网络就近接入点，在此类接入点上同时部署身份校验、威胁发现、行为监控等按需增值安全服务，这实际上就是当前比较火热未来会成为趋势的安全访问服务边缘 SASE 模型。

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，并在随后的一些列报告中进行了详细阐述，通过对 SASE 的定义理解，我们可以认为 SASE 是企业网络和业务架构演进至“云化”、“服务化”后的自然而然的安全理念。

## 1.2 什么是 SASE

为了适应数字化业务发展的需要，以及保护企业无处不在的业务接入边界，Gartner 在 2019 年发布的报告《网络安全的未来在云端》中首次提出安全访问服务边缘（SASE）这一概念，称其为一种新兴的服务，它将广域网接入与网络安全（如：SWG、CASB、FWaaS、ZTNA）结合起来，在整个会话过程中，综合基于实体的身份、实时上下文、企业安全/合规策略，以一种持续评估风险/信任的服务形式来交付，其中实体的身份可与人员、人员组（分支办公室）、设备、应用、服务、物联网系统或边缘计算场地相关联。

SASE 可以为企业提供全网流量的可见性，包括本地、云和移动端访问应用和互联网的流量，甚至也包括分支之间的流量。SASE 可提供一系列丰富的网络

和安全功能，对流量进行安全检测与路由转发，实现企业全流量的威胁检测与控制，并根据应用优先级进行路由，以确保用户访问应用的体验与安全合规均可得到保障。

从架构层面来看，SASE 需要包含如下服务组件：

- SASE 云基础设施：对于客户透明的 SASE 底座，包含网络与计算能力，提供覆盖全球范围的分布式云服务，能够为客户交付网络和安全能力。
- SASE 管理平台：面向客户的管理界面，实现针对网络和安全能力的统一策略编排，安全与应用性能分析，实时状态监控。
- SASE PoP(Point of presence)：为客户提供就近接入的网络接入节点与安全处理节点。
- SASE 接入边缘：为分支场所，移动用户提供硬件或软件的接入客户端，通常为 SD-WAN CPE 和移动客户端。

从能力层面来看，SASE 需要包含主要的网络和安全能力：

- 网络即服务（Network as a Service）
  - SD-WAN
  - 服务质量保障 QoS
  - 高级路由
  - SaaS 加速
  - 内容交付或缓存
  - 广域网优化
  - 分布式连接
- 安全即服务（Security as a Service）

- FWaaS
- ZTNA/VPN
- 安全 Web 网关
- SSL 深度检测
- 云沙箱
- IPS 入侵防御系统
- CASB 云访问安全代理
- RBI 远程浏览器隔离

SASE 的四个主要特点：

- 身份驱动：不像传统单点方案是基于设备特征或 IP 来识别资源或访问源，SASE 采用基于零信任的方法，以身份为依据，对是否能够接入平台和是否有访问目标应用的访问权限来进行控制。
- 云原生：SASE 能够以云原生、“即服务”的方式提供给客户使用，是一种 OpEx 的采购模式，且能够提供多租户、可扩展、快速变更服务内容等能力。
- 全边缘覆盖：SASE 作为企业广域网的新“核心”，能够支持所有企业边缘接入，并为其提供网络和安全能力，无论接入用户或网络位于何地，并能提供端到端的路径或应用优化以确保访问体验。
- 分布式连接：为了实现就近接入的应用访问体验和端到端可控，SASE 提供商必须提供近源的 PoP 接入点，交付高性能、低延迟的服务给企业访问者，包含企业本地网络、企业云资源和远程办公用户。

## 1.3 SASE 的核心能力概述

在 SASE 中，企业数据中心只是用户和设备需要访问的众多互联网服务中的

一个而不再是网络架构的中心，实体的身份成为访问决策的新中心。SASE 可以交付聚合的网络服务及网络安全服务，完成传统网络架构和安全硬件堆叠在数字化转型浪潮下的结构化转变，简单来说，SASE 介于用户和企业资源之间，为企业提供全面、敏捷和可适应的服务。为了应对办公习惯的转变如移动办公、居家办公，应对基础设施云化、应用 SaaS 化转型带来的挑战，快速适应 IT 基础设施弹性、灵活的需求，将割裂的、碎片化的云化/本地安全整合，紧跟 IT 数字化转型进程，SASE 必须要具备以下核心能力：

**一、云原生安全架构**

SASE 以云服务的形式交付网络和安全，是面向云计算开发部署运维的解决方案，其云原生架构使服务更具灵活性、弹性可扩展，具备自适应性、自恢复能力和自维护功能，不与特定硬件平台绑定，能够适配与集成多种云平台应用，形成网络与安全的综合云化，为用户提供了一个成本更低、匹配度更高、效率更高的平台，可以快速适应新兴业务需求。

**二、广泛覆盖的边缘节点**

SASE 将能力分布在边缘，提供接入、处理、执行能力，提供全网内低延时、安全的访问，SASE 基于云基础架构提供多种安全服务，例如威胁检测、DNS 安全、数据防泄密、Web 过滤、沙箱、下一代防火墙、上网审计、终端安全、ZTNA 等策略，且能力栈以分布式形式在全球部署，每个边缘接入节点都具有一致的网络和安全服务能力。依托覆盖全球的边缘云节点，保证在任何地方都可以提供统一的高质量网络和安全服务，使用户无论多分支办公、远程移动办公都享受与总部同级别的上网安全防护、隐私数据保护，满足企业数字化业务与资源动态扩展场景，全方位覆盖安全边界。

**三、统一控制中心**

为统一调度不同地理位置上实时都在发生的服务请求，SASE 需要具备一个统一的控制中心作为 SASE 的中枢神经系统，监控所有云节点并实施集中管控，除了主要的网络配置和安全策略的下发和同步，还包括软件和数据库的更新以及服务组件的配置管理。服务组件间通过控制中心保持通信，每个组件都能够实时获得全云运行状况，策略也能下发到所有服务组件。

**四、持续自适应风险与信任评估中心**

全球海量的日志数据同步到 SASE 数据中心，数据中心基于海量日志数据，结合大数据分析、机器学习能力、UEBA 技术等，提供全球威胁情报，持续感知监测风险。让 SASE 用户获得关于安全、行为、状态等多维度的分析与告警服务。

五、零信任访问架构

SASE 的落地践行在零信任架构之上，任何身份都是在“默认拒绝”的基础上进行连接、认证、访问等动作，比如路由、权限、安全控制等均依赖于身份，并且严格防止任何访问/威胁在网络中横向移动/扩散。采用零信任架构，使用访问实体的身份来作为访问决策的新中心，根据实体上下文信息来判断身份，简化访问的策略设置，让企业从复杂的设备逻辑和分散的地理位置中抽身出来，聚焦于身份管理与对应的控制策略，构建带着零信任基因的 SASE，从访问逻辑和 IT 架构上保障安全、可信、便捷与弹性。

**六、网络即服务**

对于任何类型的用户，都通过轻量级边缘组件来抓取流量并建立和 PoP 的连接。组件可以是 SD-WAN 设备、智能引流器、VPN 应用或是浏览器插件等，安全和网络处理统一在分布式节点中完成，以服务化的模式提供用户所需的能力。其中，网络即服务包括网络接入能力、智能选路能力、流量 QoS 能力、多云连接能力、网络加速能力、网络冗余能力等，以满足用户终端、分支、数据中心间数据互通、网络管理与加速等需求。

**七、安全即服务**

将安全能力集中部署在边缘 PoP 节点中以服务化的模式交付，构建完整的安全能力栈如威胁检测、DNS 安全、数据防泄密、Web 过滤、沙箱、下一代防火墙、上网审计、终端安全、ZTNA 等，用户可以按需获取所需的安全能力并且根据实际情况随时弹性扩展能力，以满足日益复杂的安全需求以及亟待减负的运维需要。

**八、云网安融合管理能力**

SASE 将安全与网络深度融合，只需要一个统一管控平台，实现全局资源编排，提供统一的身份管理能力，网络与安全的配置能力、运维能力、监控能力，以及全局态势感知与分析能力等。交付一个平台即可实现企业移动办公人员、分支机构、总部统一的 IT 管理能力，企业无需购买和管理多点传统硬件产品，大大降低 IT 建设成本和运维压力。

## 1.4 SASE 和 ZTE 的关系

Forrester 在 2021 年 2 月发表了 David Holmes 和 Andre Kindness 的关键报告，提出了安全和网络服务的零信任边缘模型（Zero Trust Edge，简称 ZTE），明确指出 SASE 就是零信任边缘。可以说这个定义对于网络和安全行业而言都是一个重要里程碑。

Forrester 将 ZTE 定义如下：

“A Zero Trust edge solution securely connects and transports traffic, using Zero Trust access principles, in and out of remote sites leveraging mostly cloud-based security and networking services.” 即 ZTE 解决方案以零信任为原则，来实现企业办公地点出和入流量的安全连接和数据传输。

举例说明，对于企业上网访问搜索引擎、新闻网站等这类流向互联网的流量，

是应以身份为核心去保障每个员工的上网安全，针对不同的员工、设备、行为，SASE 在云端执行不同的访问控制和安全防护策略；而对于企业访问企业应用的流量，例如 ERP、CRM 等，SASE 也是以零信任理念做访问控制的，例如访问过程中检测到访问者行为异常，可以随时中断连接。

归根结底，ZTE 和 SASE 的目标都是要让用户可以在任意地点更好、更安全地办公，同时让企业数据得到更好的安全保障，两者没有本质不同。

## 1.5 SASE 发展现状及趋势

### 1.5.1 SASE 发展现状

SASE 概念一经提出便吸引了业界高度关注。历经两年的发展，从全球来看 SASE 产品逐渐成型、应用场景逐步落地、用户数量初具规模，但各供应商针对 SASE 的解决方案不完全一致。总的来说，目前 SASE 领域主要存在五个现状：

**一、概念理解存在偏差，标准有待统一**

目前市场对 SASE 仍存在理解偏差，如认为 SASE 可以解决一切安全问题、SD-WAN 就是 SASE 等，也存在供应商将堆叠式的安全产品，打包的解决方案作为 SASE 对企业提供服务的现象。

供应商不同的概念理解和不同的技术架构路径导致提供的 SASE 能力和标准不一，国内外对 SASE 的评估标准也不统一。就国内而言行业目前仍然缺少行业或官方统一标准。

**二、供应商持续投入，企业逐步应用**

Garnter 发布的《Hype Cycle for Emerging Technologies,2021》（2021 新兴技术成熟度曲线）中显示 SASE 目前正处于期望膨胀期，各供应商通过研发、合作、并购等方式不断完善自身 SASE 解决方案能力，例如 Zscaler 收购 Edgewise

Neworks 补充 CASB 能力，Palo Alto Networks 收购 SD-WAN 供应商 CloudGenix 等。但仍需再有一段时间才能具备提供完整的 SASE 服务能力。

SASE 所具备的分布式边缘接入能力、可扩展性等特点使其在企业远程办公、跨区域互联等场景得到了一定的应用。

**三、企业网络和安全能力建设步伐不一，本土化发展仍需探索**

网络架构和网络安全的转型难易程度，以及部分企业网络和安全独立建设，造成在建设 SASE 过程中出现网络建设和安全建设不同步的现象。企业网络和业务逐步上云，云化的安全服务相对滞后。

对于 SASE 的定义而言，应该是云原生化的、分布式的、重云端轻分支的、策略统一管理的。 但是在国内具体落地时还需要考虑不同供应商情况、不同行业特征以及政策发展要求。例如国内企业级 SaaS 产品尚未标准化，因此 CASB 在国内 SASE 供应商的解决方案中作为非核心模块，落地优先级不高。

**四、SASE 供应商技术积累不足**

供应商在建设 SASE 的过程中，一个专业的 SASE 团队可以起到事半功倍的效果，但是 SASE 作为网络服务和网络安全服务的融合体，亦需要网络专家和网络安全专家通力合作，两种专家的磨合、两种技术的融合对建设 SASE 的供应商都是一个重大挑战。目前 SASE 还处于起步阶段，技术积累还需时日。

**五、企业尚未进入大规模采用阶段**

企业在实施 SASE 落地过程中，如何解决漫长的硬件寿命更换周期和现有的软件合约带来的替换成本过高的问题也迫在眉睫。

## 1.5.2 SASE 发展趋势

在远程办公、云端数据保护、企业数字化转型及安全建设和政策的驱动下边缘安全的建设势在必行，目前 SASE 是解决分布式访问的最适方案，由于环境等

诸多因素，SASE 未来的发展趋势主要有以下五个：

**一、SASE 服务落地建设循序渐进**

企业的替换成本、SASE 能力建设成熟度等多方影响下，SASE 服务的采用更可能是渐进式的，先解决单独的业务场景需求，逐渐整合一体以解决更多问题。

**二、未来一段时间交付形式持续多样化**

SASE 的理想状态是完全云交付，但是考虑到企业的替换成本，国内的使用习惯、行业特性等，短期内 SASE 的交付形式仍会有多种形态，包含云原生部署、私有化部署、混合部署等形式。

**三、多种方式完善 SASE 服务能力**

SASE 能力的建设非一朝一夕可以完成，短期来看，在 SASE 发展初期，各供应商可通过相互合作、收购、并购等方式为企业提供完整的 SASE 服务，并有望通过技术架构调整、整合，实现在单个节点，通过接入点便可执行全部网络策略和安全策略；长期来看，各 SASE 供应商必将呈现百家争鸣的盛况。

**四、各项服务能力大幅提升**

一方面随着行业标准的统一、产品能力的成熟，SASE 对远程员工、云端数据的保护能力，边缘多样化的接入能力等都将有大幅提升。例如 SASE 通过统一管理平台对数据进行集中管理，可使敏感数据的防护及威胁检测能力更上一层楼。另一方面 SASE 本身是要求拥有统一的控制平台及技术架构，统一的控制管理能力将打破碎片化的用户体验，进一步提升运维效率。

再者供应商未来可通过 SASE 提供统一的安全托管服务，这将进一步促进安全托管服务行业的发展。

**五、应用场景不断丰富**

目前供应商在建设 SASE 时已开始考虑未来接入 IOT、车联网等场景，随着 5G 的商用化发展，其与 SASE 相得益彰，将在更多的应用场景中发挥其价值。

# 2. SASE 核心技术

## 2.1 边缘计算

2016 年 5 月，韦恩州立大学施巍松教授给出了边缘计算的正式定义：边缘计算是指在网络边缘执行计算的一种新型计算模型，边缘计算操作的对象包括来自于云服务的下行数据和来自于万物互联服务的上行数据，而边缘计算的边缘是指从数据源到云计算中心路径之间的任意计算和网络资源，是一个连续系统。边缘计算为云计算能力下沉的一种新型计算模式，在靠近用户和物或数据源的网络边缘侧，融合计算、网络、存储、应用和安全的分布式计算系统，就近提供低延时和智能化服务，其边缘计算节点部署的位置靠近用户端或数据产生的端侧。边缘计算的智能互联服务可以很好地满足不同行业在数字化变革过程中对业务实时、数据融合、安全与隐私保护等多方面的关键需求。

边缘的优势主要体现在两个方面，一是在更靠近数据源所在的本地计算，尽可能地不用将数据回传到云端，减少数据往返云端的等待时间和网络成本，降低响应时延、减轻云端压力、降低带宽成本；二是拉通云端能力，能提供全网调度、算力分发等云服务，边缘云可离线运行并支持断点续传，本地数据可以得到更高的安全保护可以更好地适配数据不出园区的安全规定。

## 2.2 零信任网络访问

### 2.2.1 为什么需要 ZTNA

零信任（Zero Trust）最早是由约翰·金德瓦格（John Kindervag）担任 Forrester Research 副总裁兼首席分析师期间创建的。这是一次对传统安全模

型假设的彻底颠覆。

传统模型假设：组织网络内的所有事物都应受到信任。事实上，一旦进入网络，用户（包括威胁行为者和恶意内部人员)可以自由地横向移动、访问甚至泄露他们权限之外的任何数据。这显然是个很大的漏洞。

零信任网络访问(Zero-Trust Network Access，以下称 ZTNA)则认为：不能信任出入网络的任何内容。应创建一种以数据为中心的全新边界，通过强身份验证技术保护数据。

来看一组 Gartner 统计的企业办公&应用管理场景数据：

- 25%的公司让其 40%的员工远程办公
- 超过 67%的员工使用他们自己的设备办公
- 80%的自带设备(BYOD)均为完全非托管设备
- 企业约 50%的时间都在运行基于云的应用程序
- 只有不到 10%的组织表示他们完全了解哪些设备访问了他们的网络

可以看出，数字化转型和云计算推动的业务生态无形中扩大了可攻击面。以传统安全技术(防火墙和 VPN)构建的企业边界，无法阻挡不断向企业内部渗透的威胁。企业边界本身也在云业务场景下瓦解。

“内部等于可信任”和“外部等于不可信任”的旧安全观念需要被打破。由此，ZTNA 应运而生。

ZTNA 环境下，企业应用程序在公网上不再可见，可以免受攻击者的攻击。通过信任代理建立企业应用程序和用户之间的连接，根据身份、属性和环境动态授予访问权限，从而防止未经授权的用户进入并进一步防止数据泄露。对于数字化转型的企业，基于云的 ZTNA 产品，又提供了可扩展性和易用性。

### 2.2.2 ZTNA 模型

业界的 ZTNA 产品主要有两种概念模型：由客户端启动的 ZTNA 和服务器启动的 ZTNA。

■ 客户端启动的 ZTNA，如图 1 所示。

规范流程：

1. 安装在授权设备上的客户端将有关其安全环境的信息发送到控制器。
2. 控制器提示用户进行身份验证，并返回允许的应用程序列表。
3. 在对用户和设备进行身份验证之后，控制器才允许终端连接至安全网关。（这些网关可以避免服务器直接面向互联网，并保护应用程序免受 DDoS 攻击。）
4. 当客户端与控制器建立连接，有些 ZTNA 方案在数据链路中保持与控制器的连接，有些不保持。

优势：没有网络协议的限制，可以采集丰富客户端信息作为风险和威胁评估的数据源，如：终端安全，安全补丁，网络信息等。

缺点：客户端部署会增加企业管理员的工作，同时需要考虑各种终端的兼容性。

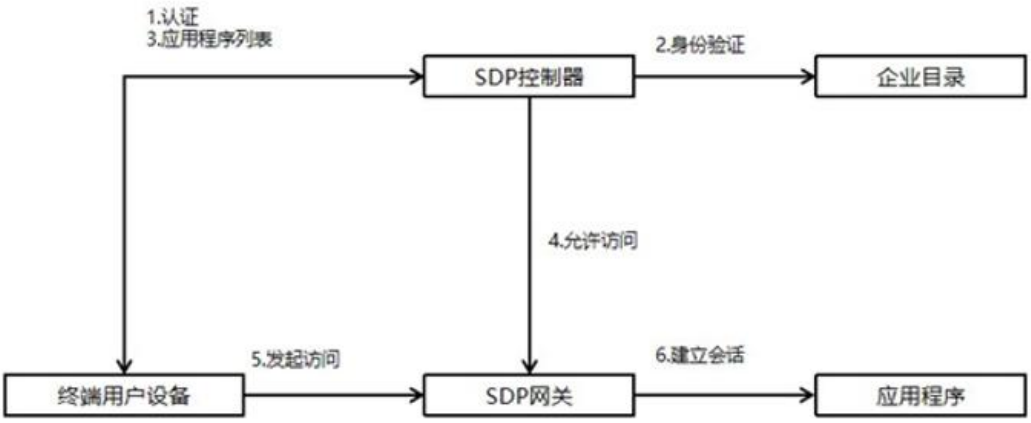


图 1 客户端启动的 ZTNA 概念模型

■ 服务器启动的 ZTNA，如图 2 所示。

SDP 连接器与应用安装在同一网络中，由 SDP 连接器建立并维护一条出站连接，它直接连接到 SDP 供应商的云。

用户向 SDP 供应商进行身份验证后才能访问受保护的应用程序。之后，供应商通常会向企业身份管理系统进行身份验证。SDP 供应商把通过 SDP 代理访问与直接访问的应用数据流隔离开来。企业防火墙无需为入站流量开设通道。但是，供应商的网络成为另一个必须评估的网络安全性的要素。

优势：最终用户的设备上不需要安装客户端，这对非受管控设备是一个很有吸引力的方法。

缺点：应用程序的协议必须基于 HTTP/HTTPS，仅限于 Web 应用程序和部分协议的访问方式。

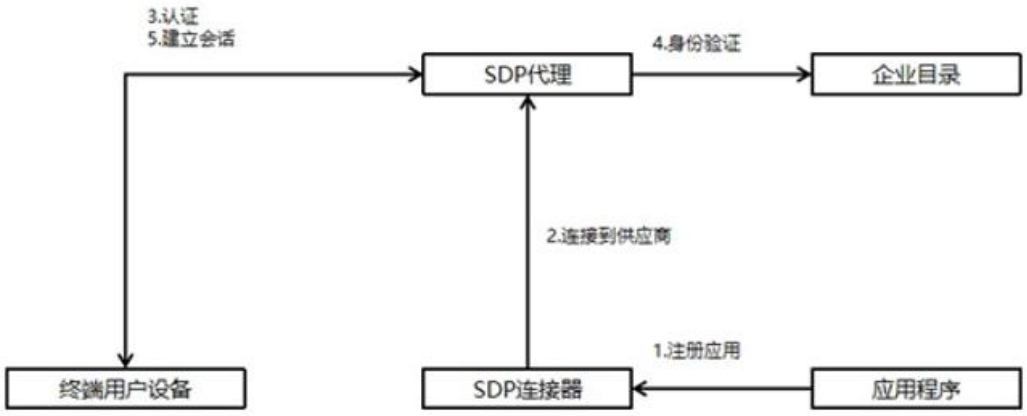


图 2 服务器启动的 ZTNA 概念模型

## 2.3 网络即服务

安全访问服务边缘（SASE）是一种新兴的服务，它将广域网组网与网络安全结合起来，从而满足数字化业的动态安全访问需求。

SASE 架构的网络即服务应具备基础网络连接能力，可以基于专线、互联网或者 4G/5G 移动网络作为底层介质，采用 SD-WAN 组网技术，实现用户终端、分支机构、企业总部、数据中心间数据互通、网络管理与应用加速等能力。

### 2.3.1 网络接入服务

支持不同办公场地环境的接入需求，包括固定地址机构接入，频繁变更地址的机构接入，移动工作组或个人办公环境接入小微企业共享办公环境接入；

支持不同网络接入技术，包括运营商专线（MPLS VPN），互联网拨号接入，互联网专线接以及 4G/5G 移动网络接入；

支持 SD-WAN 网关的多种灵活上线服务，包括自动注零配置上线，手动配置模板上线；

支持 SD-WAN 网关的多种接入安全认证方式，包括提供基于终端设备的接认证， 基于用户的接入认证方式；

支持多种 SD-WAN 网关形式，包硬件网关、虚拟化网关、客户端接入；

支持网络接入的高可靠服务，包括 SD-WAN 网关支持多线接入，出口线路故障的自动切换连接机制，以及 SD-WAN 网关的 HA 部方式。

### 2.3.2 灵活组网服务

支持多种灵活组网的拓扑结构，包括 hub-spoke，full mesh，partial-mesh；

支持多种隧道连接组网方式，包括 IPsec VPN、GRE、L2TP 等，建议支持 L2TP over IPSec、IPSec over GRE。L2TP over IPSec；

支持基于不同拓扑结构的组网调整能力，包括用户能按需添加或删减 SD-WAN 网关，调整不同分支 SD-WAN 网关的缺省接节点；调整 SD-WAN 网关之间的路径选择；

支持组网高可靠服务，包括链路冗余（如专线和互联网冗余）、PoP 点冗余，以及故障时跨 PoP 点的路径切换；

支持用户按需调整组网带宽的需求，包括 SD-WAN 网关的接入带宽调、组网隧道的带宽调整、基于应用的带宽灵活分配；

支持 SD-WAN 网络的多云访问能力，可以综合管理多个云供应商的多云连接， 创建一个安全低延迟的多云环境。

### 2.3.3 组网安全服务

支持针对 SD-WAN 隧道传送数据的加密能力，保障网络传送信息的机密性、完整性和可用性，使用的密码算法包括非对称密码算法、对称密码算法、密码杂凑算法。

支持 SD-WAN 网关的密钥管理能力，使用的密钥种类应包括设备密钥、工作密钥和会话密钥，应支持对各类密钥的生成、分发、存储、使用、更新、备份、恢复、销毁全生命周期进行管理，其过程应符合国家密码管理部门的相关要求。

支持 SD-WAN 网关的基础安全防护能力，包括防火墙访问控制、网络防攻击、恶意件识别阻断、终端接入验证和授权、威胁情报和行为分析等。

支持 SD-WAN 管控平台与 SD-WAN 网关等组件的自身安全，包括管控平台和 SD-WAN 网关之间采用 HTTPS 等方式对数据传输进行必要的认证和加密，以防止信令通道被控制或者造成数据泄露。

### 2.3.4 基于应用的服务保障

支持网络识别能力，包括识别流量的 TCP/UDP 协议、源目 IP 地址、Mac 地址、地域信息等能力。

支持应用识别能力，包括识别流量的应用类型、应用协议信息能力。

支持基于应用对网络服务质量的要求为应用选择转发路径的能力，包括基 QoS 优先级动态选路，基于 SLA 探测动态选路，基于带宽选路等。

支持通过网络边缘节点针对延时要求敏感业务进行访问加速能力包括网页、web 应用的缓存加速服务，音视频等文件压缩传输加速服务，及支持实时音视频流的优化服务。

### 2.3.5 统一监控和策略管理服务

支持统一管控平台，提供统一的监控运维、组网和安全策略的统一管理，支持统一网络和流量编排。

支持统一管控平台的可视化的服务界面，展示大屏等通用能力，包括物理设备的可视化、网络状态的可视化、应用状态的可视化、基于地图的网络拓扑可视化等。

支持统一管控平台的多租户服能力，应支持租户之间的网络隔离、数据访问隔离，不允许跨租户的数据访问。

支持 SD-WAN 全网状态监控，支持运行管理员与租查看全网或者租户自己的网络流量信息、链路状态与性能（时延、丢包等参数）。

支持对不同 SD-WAN 网关的统一管理，包括 SD-WAN 网关的配置上线管理、组网接口配置、组网策略配置、安全策略配置以及告警信息配置等。

支对 SD-WAN 网关的日志的采集和统一管理，支持日志查询和基于日志的规则分析。

支持统一管控平台的高可靠部署，支持主备部署方式或者集群部署方式。

## 2.4 安全即服务

SASE 将安全能力分布在边缘，在边缘具备提供接入、处理与执行能力，提供全网内低延时、安全的访问能力。SASE 的安全能力应采用云原生架构使得安全能力具备快速弹性扩容、快速迭代更新、高性能和低延迟的特点。用户采用订阅模式按需使用所需的安全能力，安全能力按需使用按量计费。同时 SASE 服务商的边缘接入节点需覆盖在全国主要地域，让用户能享受到低延迟服务。

从用户角度来看，SASE 的安全即服务目前有三个主要应用场景。

首先是企业员工终端设备访问互联网或访问外部应用

其次是企业外部人员访问企业内部资源

最后是企业内部人员访问企业内部资源

### 2.4.1 企业员工安全访问互联网或外部应用

企业管理员工终端设备（如：电脑、手机或平板电脑）访问互联网或访问外部应用。 在该场景下，企业需要用终端安全、网络安全、内容安全和数据安全的各种安全能力帮助企业来管理和保护员工的上网终端、保护上网行为和保护访问外部应用的安全。适合在 SASE 部署的安全能力如下：

- 网络安全：

SASE 的安全即服务解决方案应具备网络安全能力，包含网络威胁防护和流量安全检测能力。

支持网络访问控制的能力。

支持检测和防护从企业内到外部的网络攻击行为。

支持通过 UEBA 发现未知威胁，增强安全可见性，提升发现安全威胁的能效。

支持威胁情报的能力，通过最新的威胁情报数据发现 0day 和 Nday 攻击。

支持内置恶意域名库，针对互联网访问流量和 DNS 流量进行分析、检测与阻断。

- 内容安全：

SASE 的安全即服务解决方案应具备内容安全能力，包含上网行为分析和上网行为管控。

支持识别 P2P、网盘、网络购物、股票、游戏、即时通讯等主流应用协议。

支持以用户、位置、时间和终端类型等维度对 P2P、网络购物、股票、游戏、即时通讯等应用进行阻断或者限速。

支持内置 URL 库，并支持以用户、位置、时间和终端类型等维度进行 URL 过滤。

支持上网行为审计，对员工访问的网站、应用、邮件等进行审计。

支持上网行为分析，帮助企业以泄密风险、工作效率 、离职倾向等维度帮助企业降低风险。

- 数据安全：

SASE 的安全即服务解决方案应具备数据安全能力，包含网络数据泄露防护和终端数据泄露防护。

支持网络数据泄露防护：识别、控制网络传输中的敏感数据，控制或监视通过邮件、WEB、FTP 等网络协议传送敏感数据。

支持终端数据泄露防护：识别终端的敏感数据违规使用、发送等进行策略控制；对敏感数据的终端使用行为进行监控。

### 2.4.2 企业外部人员安全访问企业内部资源

从用户角度来看，SASE 另外一个主场景是企业外部人员访问企业内部资源。企业外部人员的设备和身份是非受控的，外部人员终端是没有访问代理工具，因此需要外部人员访问到 SASE 代理接入点后相关的安全功能就可以提供了。在该场景下，企业需要用主机安全、网络安全、应用安全和数据安全的安全能力帮助企业来保护外部人员访问内部资源，以免出现内部资源遭受威胁，数据出现泄漏等问题。适合在 SASE 部署的安全能力如下：

- 网络安全

支持网络访问控制的能力。

支持检测和防护从企业外部到内部的网络攻击行为。

支持威胁情报的能力，通过最新的威胁情报数据发现 0day 和 Nday 攻击。

支持通过 UEBA 发现未知威胁，增强安全可见性，提升发现安全威胁的能效。

支持内置恶意域名库，针对 DNS 流量进行分析、检测与阻断。

- 应用安全

支持应用常见安全漏洞扫描。

支持 0Day 等高级威胁漏洞扫描。

支持通过语义分析技术实现 HTTP 和 HTTPS 协议的攻击防护。

支持 CC 攻击防护。

支持网页篡改、恶意爬虫攻击防护。

- 数据安全

支持网络数据泄露防护：识别、控制网络传输中的敏感数据，控制或监视通过邮件、WEB、FTP 等网络协议传送敏感数据。

支持传输加密：外部与内部资源的交互都采用加密协议。

支持数据加密：内部资源的关键数据采取加密方式存储。支持数据安全审计：

对数据资源的访问和使用行为进行审计。

支持存储敏感数据发现：支持发现存储在服务器和数据库中的敏感数据。

### 2.4.3 企业内部人员安全访问企业内部资源

从用户角度来看，SASE 目前还有一个主场景是企业内部员工安全访问企业内部资源。该场景以零信任技术架构为核心来进行构建，企业内部人员的设备受控（即：内部人员的终端设备需集成特定 Agent）访问时的身份是受控（即：内部人员访问时需要通过身份认证），最后内部人员访问到 SASE 代理接入点后通过信任度策略的安全检查后就可以访问到内部资源了。在该场景下，安全访问服务边缘平台的 SDP 作为内部员工安全访问接入的统一入口 ，接收用户访问请求，在访问终端和身份经过验证之后，根据零信任安全访问策略执行判定，判断通过即可安全访问内部资源。同时在对访问内部资源进行 Web 防护，并且加入 DLP 的能力防止数据泄露的风险。适合在 SASE 部署的安全能力如下：

- 访问模式能力

  支持 B/S 访问模式，如使用浏览器作为代理客户端。

  支持 C/S 访问模式，如通过 Agent 作为代理客户端。

  支持多种终端设备接入能力，如 PC、手机、Pad 等设备。

- 身份安全能力

  支持双因子认证的安全能力，如账户密码+短信认证，账户密码+动态口令等。

  支持对接 AD，LDAP 等第三方认证服务的能力。

  支持生物认证能力，如人脸识别、指纹识别等。

- 零信任安全评估能力

  零信任评估支持动态评估算法，具有基于身份、基于终端安全状况、基

于行为、基于环境动态进行综合分析与评估的能力，为安全访问的策略判定提供依据。

支持管理访问终端的能力，至少具备终端白名单、终端安全情况评估等；

支持接收、分析、处理内部或外部安全分析系统所收集的信息的能力，进行更精准的风险识别和信任评估，收集的信息如用户账户信息、安全分析信息、日志信息等；

支持数据处理能力，支持数据清洗、归并、格式化等，满足算法的数据格式要求；

支持人工智能等技术建设算法模型，并支持人工方式配置安全评估规则。

- 零信任安全控制策略能力

支持接收、分析、处理零信任安全评估组件给出的评估信息的能力，基于评估信息并综合其他信息如权限判定信息，向零信任安全策略执行下发最终策略执行动作，如存在风险以及作为用户冻结、用户权限降低和阻断访问的决策。

- 其他安全能力能力

支持 Web 攻击防护能力，防止内部员工的恶意攻击行为；

支持 DLP 的能力，防止内部员工出现数据泄露的行为；

支持访问终端管理 Agent 和终端 EDR 的 Agent 合二为一，提升零信任安全访问易用性 。

综上所述企业可以根据自身的实际安全需求，按需订阅 SASE 提供的各种安全能力。使得企业可以快速满足内部人员安全访问互联网和外部应用、外部人员安全访问内部资源的需求和内部人员安全访问内部资源的需求。

# 3. SASE 应用场景

## 3.1 连锁及加盟企业

连锁及加盟类企业其网点往往分布范围广，员工数量众多，网络和安全需求多元化。以某大型集团酒店为例，其在 16 个国家经营着近 6900 家酒店，国内酒店网点遍布中国 400 多个城市，拥有超过 10 万名员工，办公业务系统积累海量诸如客房预订、旅客入住登记涉及公民隐私的敏感数据。

随着连锁运营的拓展，新开业的网点越来越多，连锁及加盟类企业每新开一家网点，出于网络安全考虑，往往都需要申请两条链路，一条百兆互联网链路供网点客户上网使用，另外需要部署一条 4M 专线访问总部办公业务应用。由于专线费用较高，且传统专线网络可获取性较差，光纤/电缆需要单独部署，耗费的周期长，用户迫切希望能够通过新技术，在确保网络安全的前提下将专线替换为互联网线路，降低 IT 运营成本。

**用户需求**

用户希望采用基于 SD-WAN 和零信任的 SASE 解决方案实现了互联网链路的合理利用和安全加固，结合网络感知业务、业务智能调度，打造高质量、低成本、可感知的全球互联 WAN，以及构建一个以身份为中心的策略模型以实现关键业务应用和敏感数据动态的访问控制，同时满足网络安全、应用安全和数据安全的要求。具体需求如下：

- 降低 WAN 成本。通过引入互联网链路，预设应用和路径的优先级，将流量调度到互联网线路上，同时支持关键业务应用的智能选路，降低企业使用 WAN 的成本。

- 简化运维，提升运维效率。通过网络控制器对 WAN 进行集中控制和管理，实现可视化的监控管理和快速故障定位，使 WAN 的运维更简单。
- 由于线路直接连接在互联网上，考虑采用零信任安全方案来防范业务应用、敏感数据暴露在互联网、连锁或加盟网点等可能遭受的网络攻击、数据泄露等安全风险。

**解决方案**

针对连锁及加盟类企业用户需求，推荐采用基于 SD-WAN 的 SASE 整体解决方案。具体部署环境如图 3 所示：

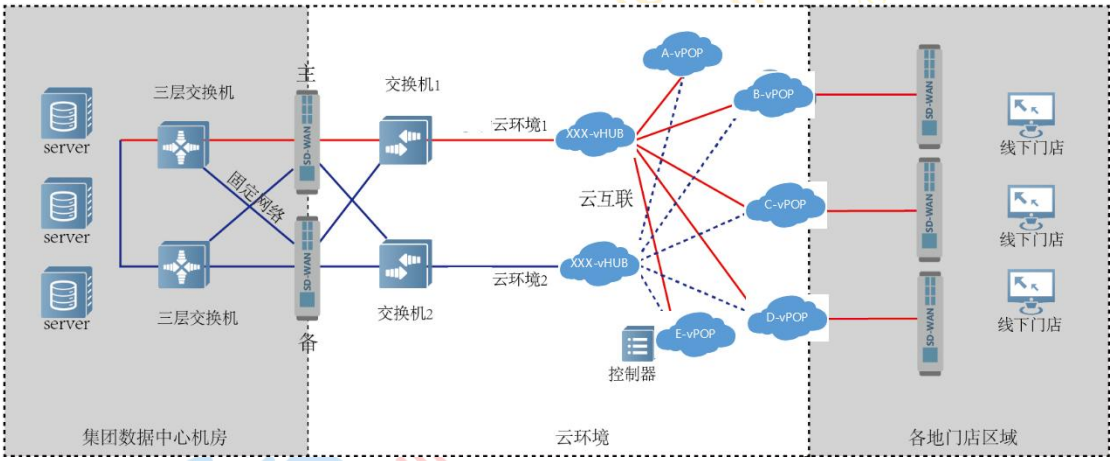


图 3 连锁类 SASE 整体解决方案

部署 2 条云专线通往该集团数据中心机房，分别连接到机房 SD-WAN 与 A 地、B 地 POP 相连。各地网点出口通过 SD-WAN，采用双机热备方式，避免单点故障，主设备连接互联网专线，并通 4G/5G 移动链路备份，备份设备默认连接网点互联网线路。当主设备两条链路都失效后，则通过 HA 切换到备份设备，通过网点 Inernet 线路连接，实现链路的三重备份，确保业务冗余性。

网点的 SD-WAN 设备则采用就近原则，分别与两台 vPOP 建立主、备隧道连接。vPOP 分别与 A 地、B 地的 vHUB 建立主备隧道连接。

全网开启 BGP，通过 BGP 实现路由发布和基础路径选择。开启链路质量探测功能，实现全网路径感知。

通过以上部署，实现了任意 hub、pop、云专线链路、数据中心 SD-WAN、连锁或加盟网点设备、线路故障，都具备冗余，确保业务连续性。

在云端 vPOP 节点部署 ZTNA、FWSaaS 产品，基于零信任方案实现连锁及加盟网点与集团数据中心的安全互访，并避免遭受网络攻击和数据泄露。

**方案优势**

- 全网冗余、确保业务连续性：所有设备、线路、PoP 点，均实现冗余设计，避免单点故障。
- 集中控制，简化运维：采用最新的 SD-WAN 技术，实现“零配置”下发，解决传统设备开局慢，需要专业运维人员的问题。网点上线无需专业运维人员，通过邮件、手机开局等方式，让控制器自动获取完整配置。通过控制器实现是设备自动组网，最大程度规避人工配置出现失误。
- 增强安全，满足合规：通过部署实施零信任方案，安全管理员可以在云端统一对所有连锁或加盟网点的业务访问进行审计管控、信息文件防泄漏和终端威胁检测等安全防护，满足《网络安全法》、《数据安全法》等合规性要求。
- 降低成本、提升效率：通过互联网实现连锁或加盟网点到骨干网 PoP 的 SD-WAN 接入，免去了铺设“最后一公里”的线路，能够快速响应企业客户的需求，加速分支业务的开通。

## 3.2 跨地域分支机构

针对跨地域的集团公司存在分支机构的的场景，传统方式是拉一条专线或通过 VPN 接入到集团统一的网络规划池，需要同时在分支网络提供网络防护等安全设备，以及面临进行安全设备的运营维护等工作投入，因此管理成本会很高。同时，分支机构不仅需要访问集团总部数据中心的业务系统，还经常需要访问互联

网上的 SaaS 和公有云服务。

**用户需求：**

- 分支机构用户能够访问到总部的资源
- 支持新分支的无缝扩展
- 对分支机构用户终端设备的安全管理
- 较低的网络建设和运维成本，对于分支机构已部署的安全设备或产品能够充分历利用
- 访问总部或公有云资源时保护通信数据的安全
- 全球性集团企业还需要考虑全球网络的访问延迟问题

**解决方案：**

为了提高分支机构的网络安全接入能力，需要以一种支持对总部 IDC、互联网 SaaS 等所有资源都能够安全、便捷、稳定的方式访问的网络架构，如图 4 所示。

SASE 可以支持跨地域分支机构对总部和云上资源的无缝访问。企业可以通过快速、可靠的互联网连接，优化访问链路，增强用户体验，同时借助 SASE 的云化安全策略，全面开展检查流量、审核身份、访问控制等安全防护，这比在分支机构部署多套安全设备也能节省大量的成本。

在具体实施上，无论企业分支机构的网络是全新建设还是对已有网络的升级，都需要进行基于 SASE 架构的整体方案设计和规划，梳理分支位置、人员、数据、应用、设备等网络和安全需求，制定符合企业网络和安全策略的 SASE 实施步骤。

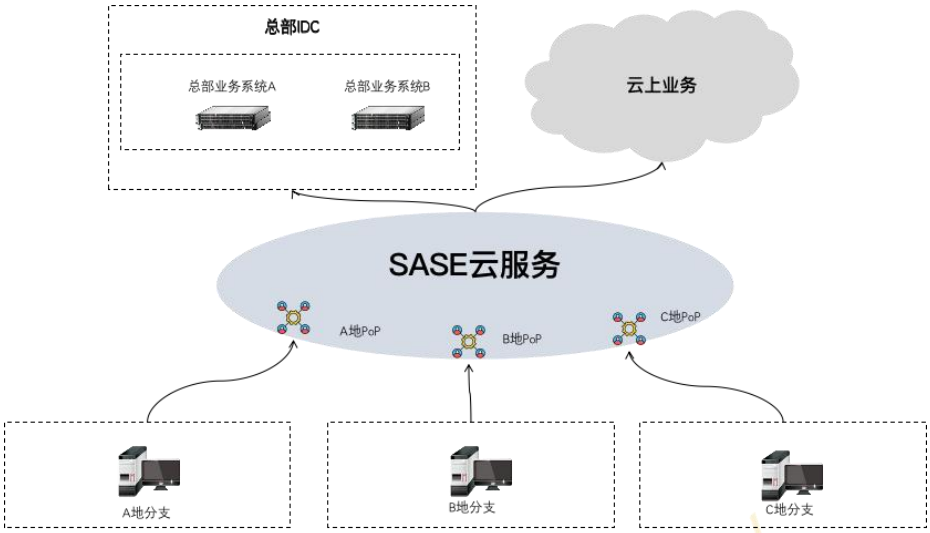


图 4 分支机构 SASE 部署方案

**方案优势**

- 多地域、靠近分支机构所在地的 PoP 节点接入，优化访问链路信息传输效率
- 基于零信任的安全终端管理、通信加密、多因素身份认证、最小权限、动态访问控制等安全能力，保障访问过程的安全
- 基于互联网的接入，比专线等形式降低成本
- SaaS 云服务的交付模式，比 VPN 等传统设备+私有化部署的形式支持更好的可扩展性

## 3.3 远程和移动办公

以某金融企业为例，该企业在全国范围内有两个 IDC 中心，分别位于 S 市和 W 市，由于业务发展的需要，内网的服务器分布于两市中，两市互为备份。如图 5 所示：

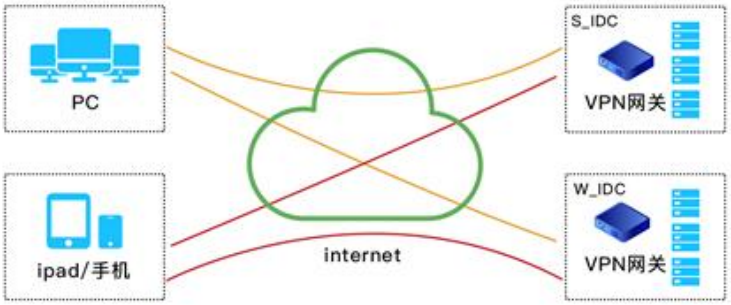


图 5 远程办公场景

业务人员外勤进行业务操作时，使用平板/笔记本等移动终端访问内网业务时，需要根据实际业务的归属地，连接对应地市的 VPN 网关。当需要切换到另一种业务系统且归属在另一个地市，业务人员需要断开当前的 VPN 连接，再连接至另一地的 VPN 网关，这对于业务人员的办公效率是一种拖累，同时访问质量不稳定也无法得到根本性解决。

**用户需求**

- 移动用户在任何时候能够访问到总部的资源
- 新用户的快速开通
- 移动用户终端设备的安全管控
- 较低的网络建设和运维成本
- 访问总部或公有云资源时保护通信数据的安全
- 移动用户访问企业资源能实现就近接入保障良好体验

**解决方案**

通过 SASE 服务的改造基于 VPN 的移动办公接入架构，遍布全国的 PoP 节点

首先可有效解决互联网环境访问的质量问题和办公终端的上网安全问题。同时PoP除了网络优化功能以外，基于“零信任”的思想，还承担起了终端用户的身份授权和访问权限的管控功能，而这一系列的策略通过SASE Controller统一下发和管理。一旦鉴权成功，用户终端将携带访问票据（Auth_Success_Token）向S市和W市分别发起登录连接，终端用户即可享受同屏显示两市的所有业务应用，无须再反复切换。实现基于身份的零信任方案控制，同时实现无缝切换的介入体验：终端通过SASE软件客户端或是SDK形式集成在企业业务APP中实现轻量部署，做到了用户全程无感知。SASE Controller通过API接口可与企业内部多种认证模块对接，终端客户端或SDK可接收来自所连的PoP下发的安全策略/访问权限等一系列的更新和推送，让终端安全成为现实。

改造后的SASE解决方案如图6所示：

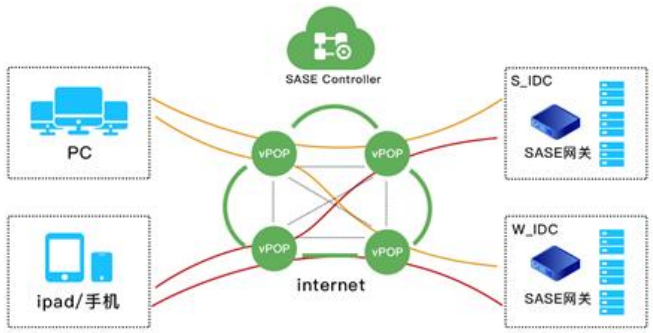


图6　远程办公SASE解决方案

**方案优势**

- 用户实现就近的PoP节点接入，优化访问链路信息传输效率，保障客户体验
- 基于零信任的安全终端管理、通信加密、多因素身份认证、最小权限、动态访问控制等安全能力，保障访问过程的安全

- PoP 点的网络安全服务，保障移动办公电脑的上网安全
- 对所有用户提供一致的安全管理，减少网管维护成本
- SaaS 云服务的交付模式，比 VPN 等传统设备+私有化部署的形式支持更好的可扩展性

# 4. 总结

企业数字化转型和业务上云是 SASE 的重要驱动力。企业的数据中心不再是承载企业资源和用户访问的唯一中心，SaaS 等大量基于云计算服务的部署，以及新兴的边缘计算平台，颠覆了传统的网络和应用架构模式，使企业网络架构出现“内外翻转”的现象。与此同时，数字化转型需要随时随地访问应用和服务（很多应用位于公有云或采用 SaaS 服务）传统的网络和网络安全体系架构无法满足数字业务的动态安全访问需求。SASE 架构可以很好的解决资源分散、漫游访问的安全访问需求，适合于多类场景，如连锁及加盟类企业、跨地域分支机构、远程和移动办公等。

采用 SASE 架构，企业边界不再是一个位置；而是一组动态创建的、基于策略的安全访问服务边缘。SASE 的本质是基于身份认证的整合网络和安全的边缘融合服务，是典型的云网安融合的新兴产品。SASE 可提供两大类服务，网络即服务，如网络安全接入、灵活组网、组网安全；安全即服务，如防火墙、云访问代理、恶意流量识别、上网流量管理等。

SASE 将极大的改变产业业态。第一、促使网络厂商和安全厂商的融合；第二、是云网运营商向云网安运营商的转型，安全将成为刚需，无处不在；第三、专业安全厂商研发重点从设备研发转向 VNF 的研发和专业服务，推出以安全为主 SASE 服务，同时网络能力为以和云网运营商共建和合作的模式；第四、企业安

全从业者能力要求大大降低，工作重心从设备采购配置向安全服务订阅管理转移，更多关注业务或应用安全，如 DevSecOps，实现安全左移。

根据 Gartner 预测，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，到 2024 年，至少 40%的企业将有明确的战略采用 SASE，而在 2018 年年底这一比例不到 1%。（Gartner，2019）SASE 市场已迎来传统 IT 厂商、云计算厂商、安全厂商、CDN 厂商、互联网企业等多方势力的角逐，包括思科、VMware、Palo Alto Networks、Cato Networks、Akamai、腾讯等。随着时间的推移，SASE 产业必将蓬勃发展。