安全技术研究所(安全管理中心)
中国移动通信有限公司研究院

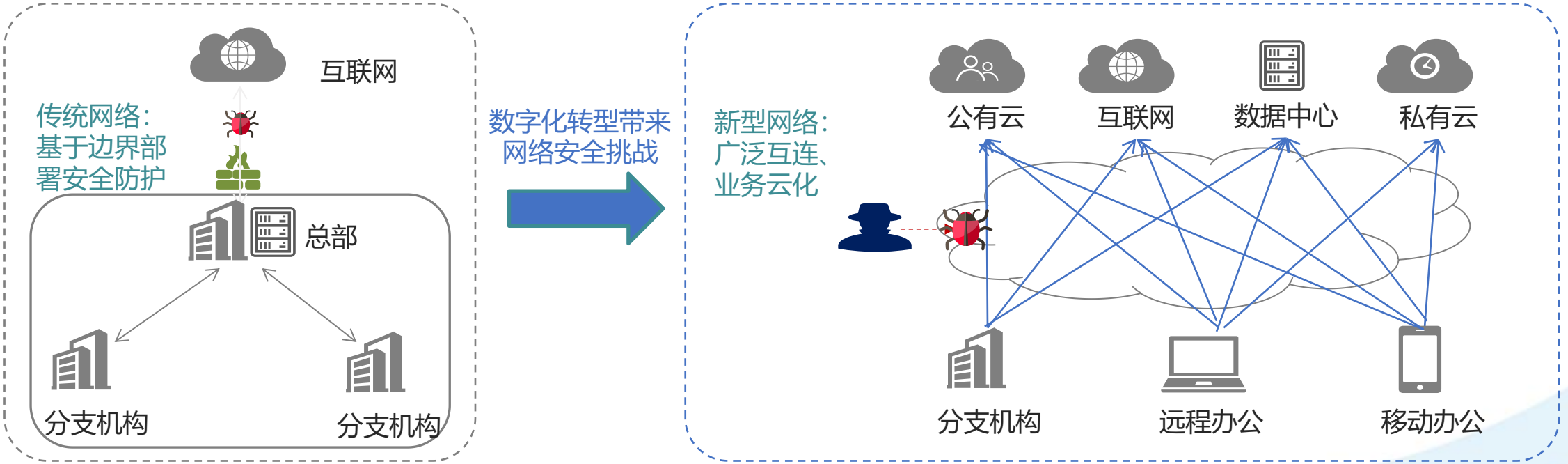
运营商SASE技术思考与实践

中国移动 China Mobile | 研究院 CMRI

2023年09月

目录

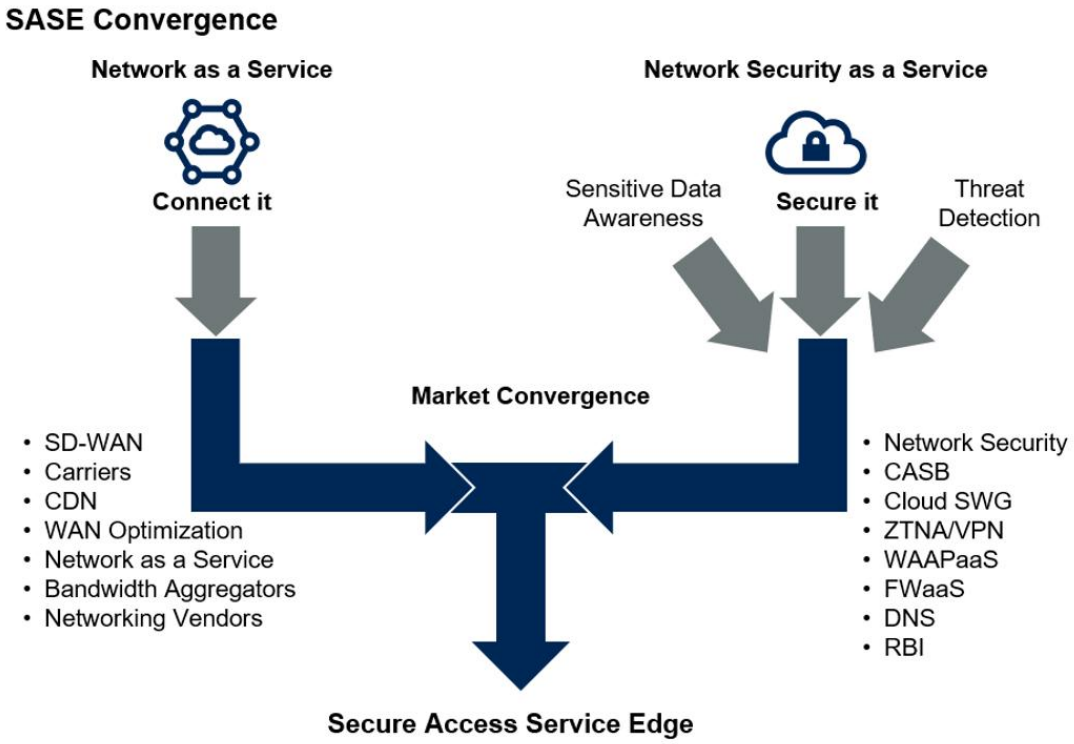
企业数智化转型带来网络安全的变化与挑战



- 业务集中部署
- 内外边界分明
- 连接模式单一
- 流量检测集中
- 分布式的业务增加防护成本
- 远程/移动办公扩大暴露面
- 访问模式变化让网络连接复杂
- 流量分散难以统一安全检测

- **SASE（Secure Access Service Edge，安全访问服务边缘）**，是一种融合了网络即服务（Network as a Service）和安全即服务(Network Security as a Service)的新型服务框架。通过**统一管理分布式部署的网络和安全能力，以身份为核心实现访问控制，**为用户提供易用，灵活，安全，高效的网络和安全服务。

SASE技术特点



- **以身份为中心**：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，决定网络选择和访问权限级别
- **分布式部署**： 可将安全能力和网络能力下沉到靠近用户侧，从而满足网络低延迟和敏感数据本地处理等需求
- **兼容所有边缘**：满足不同应用场景下各类边缘的需求，例如数据中心、云端资源、移动用户、IOT等
- **云原生服务**： 可将安全防护功能直接部署在云中，降低企业建设和使用成本；

- SASE的本质是网络和安全的综合云化服务，具备三大特点：**统一管理、便捷服务和灵活部署**。从而满足了新型企业组网的网络和安全需求，是未来网络和安全服务的大趋势。

SASE发展历程

➢ **SASE框架理念逐步被广泛认同，实践、标准化相结合，逐步走向产品化市场化道路。**

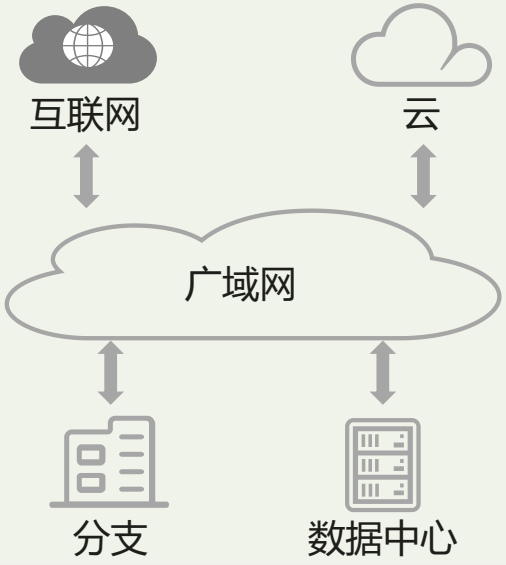
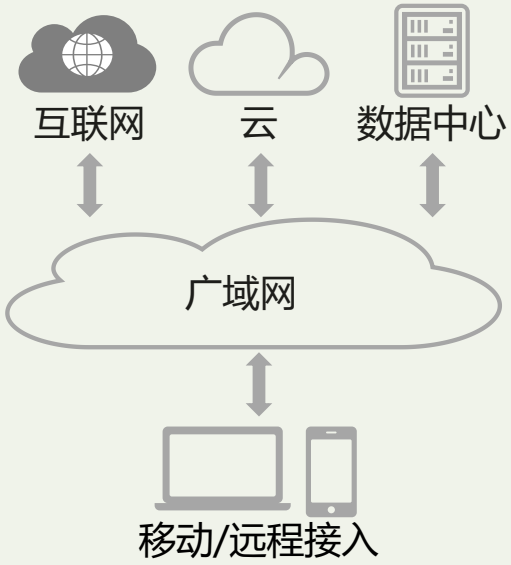
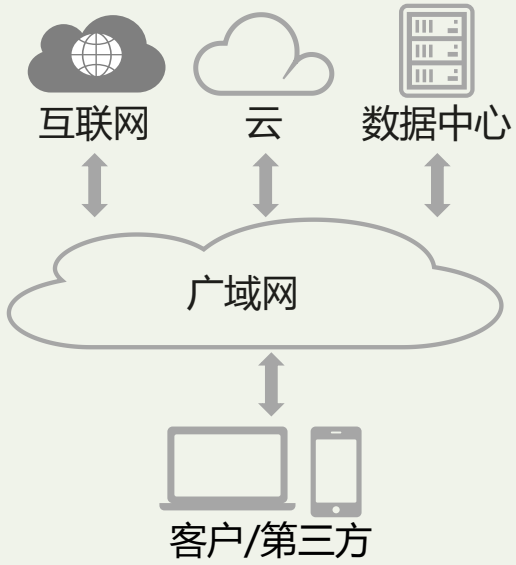
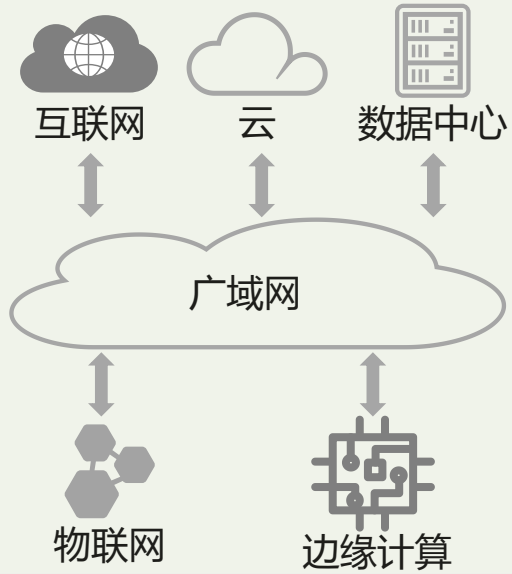
- 2023年Gartner发布的《**Hype Cycle for ICT in China, 2023**》：SASE目前**正处于期望膨胀期**，各个厂商通过研发并购等方式完善SASE解决方案的能力
- 国际主要SASE厂商： Fortinet 、 Versa 、 Cisco、 Cloudflare、CATO等
- 国内中国移动、中国电信、绿盟、深信服、阿里云等大量厂商纷纷推出SASE解决方案

- 2023年3月，中国移动在ITU立项《**Guidelines for security orchestration of service access process**》
- 2022年10月，MEF发布《**MEF W117 SASE Service Attributes and Service Framework**》
- **2021年CCSA、中国通信学会和云计算开源产业联盟立项了多个SASE的相关项目，**包含SASE功能编排管理框架、SASE能力成熟度要求，总体技术要求，关键技术指标，服务质量要求，整体技术方案等

- 2023年7月中国移动在GTI发布《**Operator Secure Access Service Edge White Paper**》
- 2022年3月CSA GCR发布《 **SASE安全访问服务边缘白皮书** 》
- 2021年11月电信发布《**安全访问服务边缘 (SASE) 技术应用白皮书**》
- 2019年CATO推出**第一个SASE解决方案**

- 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**

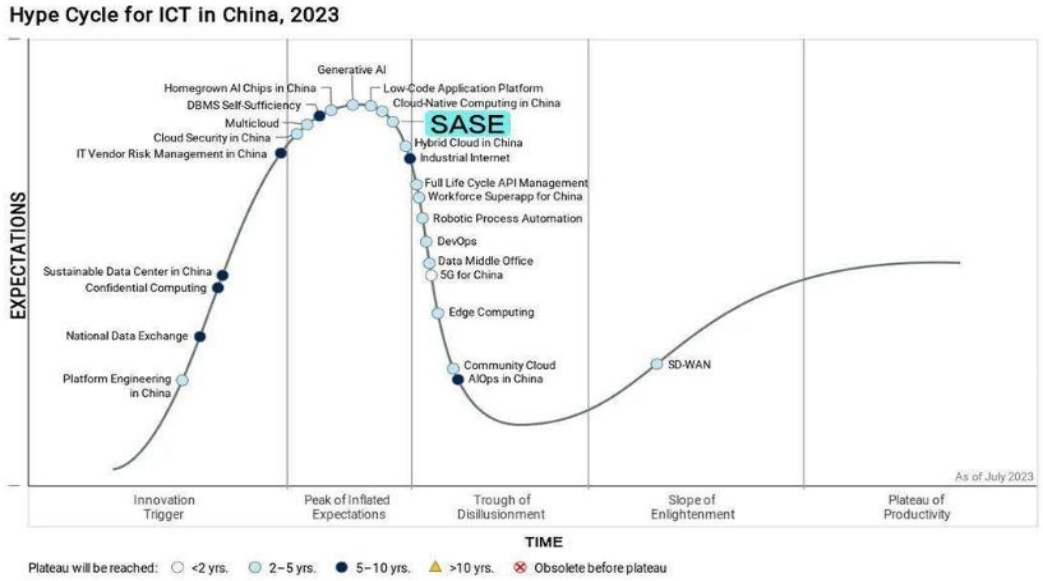
SASE应用场景

广域连接： 多实体跨广域网灵活互连	移动/远程接入： 受控安全接入	客户/第三方接入： 非受控安全接入	IOT/边缘接入： 海量接入，计算下沉
			
➢ SASE提供全互连、自动化网络，实现全球分布的分支机构、多云部署的业务之间直接互连 ➢ SASE提供云原生、分布式部署安全防护能力，降低企业自建安全防线成本	➢ SASE提供全网接入，实现接入地点不受限制 ➢SASE提供通过受控终端和分布式部署安全资源池，对移动、远程接入进行鉴别、监控，不同接入点提供一致性的服务和防护	➢ SASE提供全网接入，实现接入地点不受限制 ➢SASE防护来自非受控设备的威胁， 监控客户/第三方访问行为，防护敏感数据泄露等	➢ SASE兼容多种网络接入，支持边缘计算、IOT等网络接入 ➢SASE支持将安全防护能力下沉，就近实现IoT设备接入认证、防护海量设备DDoS攻击、边缘技术安全防护等

SASE市场介绍

➢ Gartner SASE市场研究和预测：

- 未来5至10年，SASE将会成为主流安全解决方案。
- 到2024年，SASE市场规模将从2019年的19亿美元攀升至110亿美元。大中华地区市场规模为7.69亿美元
- 2025年至少60%的企业将有明确的战略和时间表采用SASE；



➢ 目前提供SASE的服务的企业主要有运营商、安全厂商、网络厂商和云厂商四类。

运营商

- 优势：网络和云等基础设施资源丰富
- 措施：与网络厂商和安全厂商合作，在全国建立安全能力资源池，对外提供SASE服务。

安全厂商

- 优势：安全技术积累
- 措施：
  - 部分厂商专注于安全能力，与其他企业合作SASE。
  - 部分厂商通过开发、合作、收购等方式获网络能力，提供SASE服务。

网络厂商

- 优势：SD-WAN等网络技术积累
- 措施：在网络基础上增强安全能力，提供SASE服务。

云厂商

- 优势：云原生安全防护能力
- 措施：结合网络服务转型SASE

目录

运营商SASE优势

➢ **运营商作为网络基础设施的提供者，建设SASE具有明显优势，具体表现在网络和云基础设施完善、集成推广能力强、品牌影响力大等方面：**

资源优势

- 遍布全球的SD-WAN网络和专线，可有效优化网络传输，为SASE提供丰富的网络服务
- 庞大边缘云、中心云、PoP点上建立安全资源池，实现安全服务分布式部署，SASE边缘设备可以复用运营商的网络CPE，降低SASE建设成本

集成优势

- 运营商集成经验丰富，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

品牌优势

- 运营商拥有广泛的行业客户基础和强大的品牌效应，由运营商推广的SASE服务更容易被企业客户接受

运营商SASE技术架构

- **SASE部署参考框架包含SASE云，SASE PoP，SASE 边缘设备和SASE中心平台。**

SASE云：整合了各种网络和安全功能

- 提供面向各种边缘接入、多租户云服务。

SASE PoP点：SASE云的组成节点

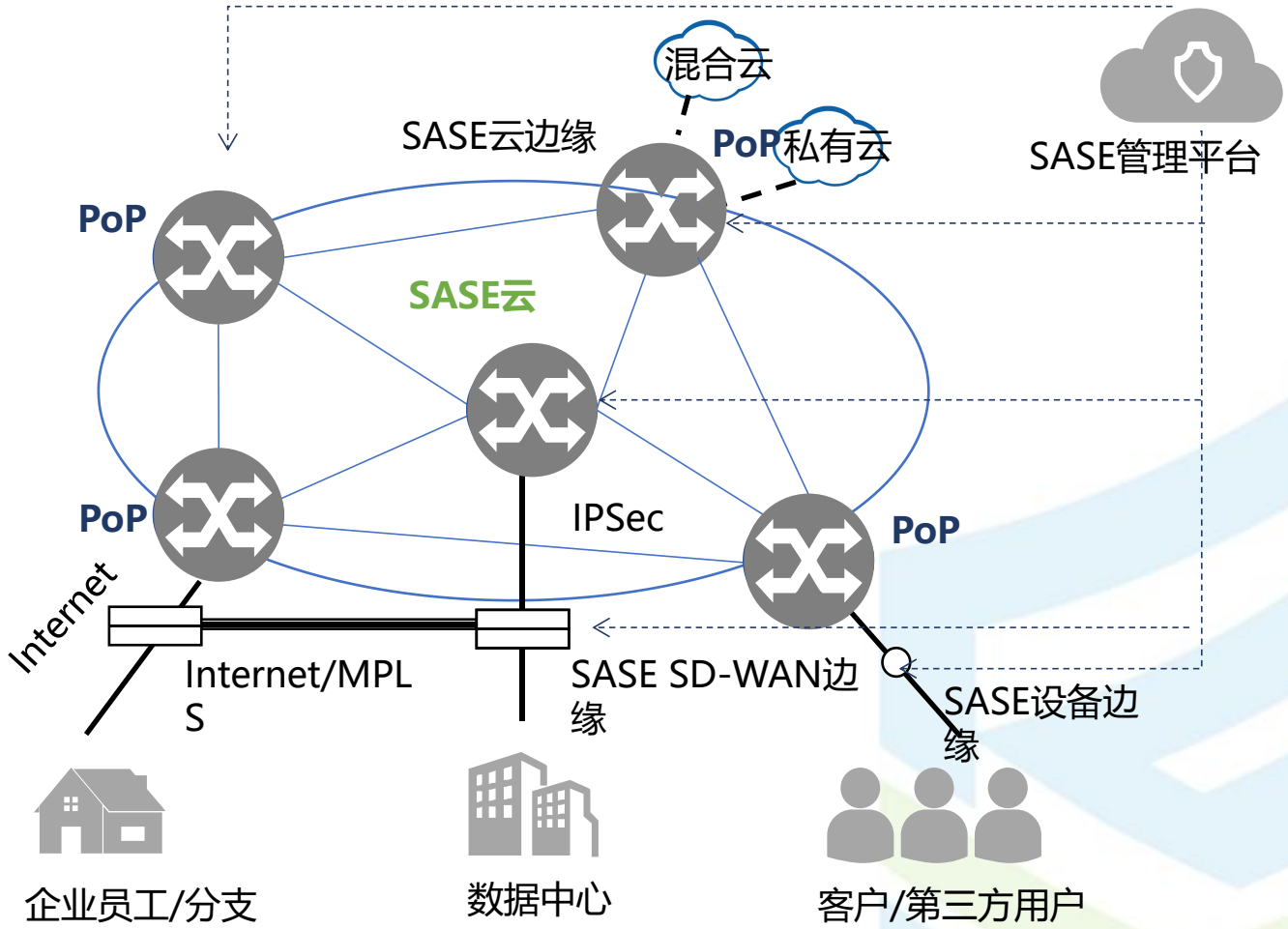
- SASE入网点，可按需部署ZTNA，SWG等各类网络和安全能力。

SASE边缘设备：包含受控终端和CPE

- 通过加密的通道连接到SASE云中适用的PoP点。
- 可按需部署各种资源需求较低的网络和安全能力，从而保证SASE框架的灵活性。

SASE管理平台：统一的可视可管的控制平台

- 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。

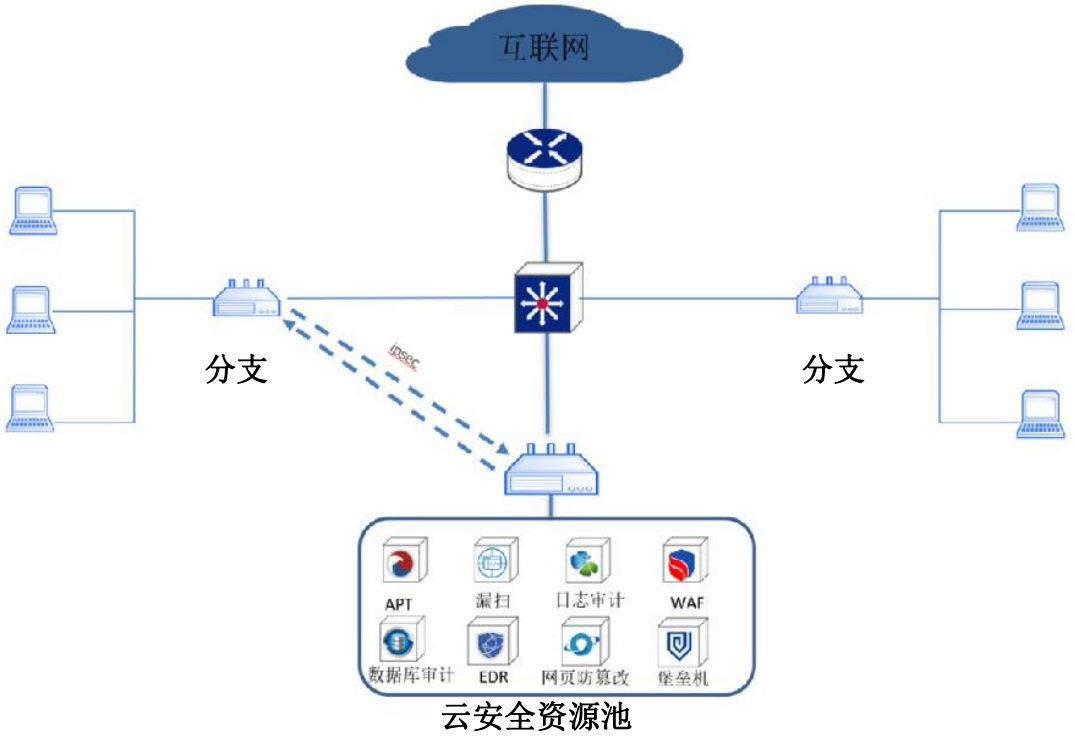


运营商实践： 分支上网SASE方案

➢ **分支上网**：面向中小企业用户提供集传统防火墙、入侵防御、病毒防护、上网行为管控、威胁检测等安全模块于一体的智慧安全专线，并通过**云端平台进行订阅、管理与联防。**

需求

- 统一订阅和管理安全能力
- 呈现端云的全局安全态势数据
- 降低使用和维护成本
- 定期扫描漏洞，主动发现挖矿、僵尸网络、APT攻击等安全威胁，管控员工在上班时间上网行为

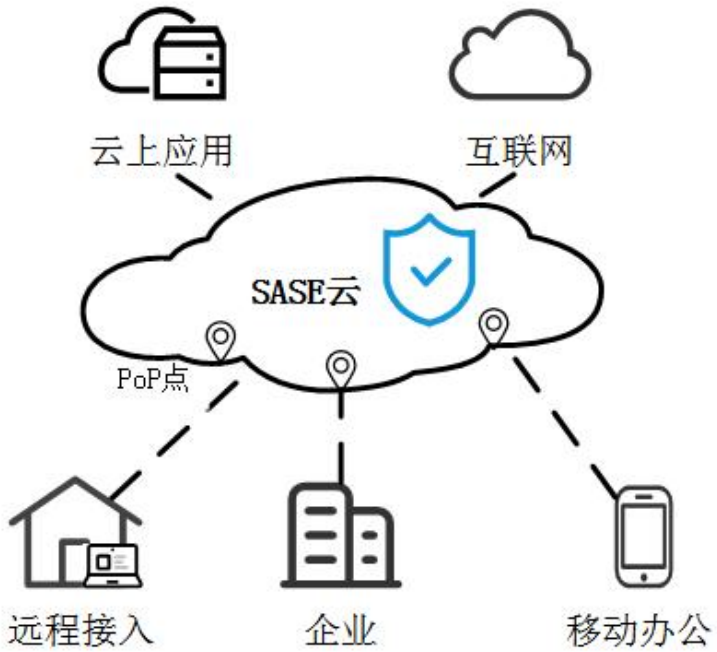


云端一站式订阅与管理	本地+云端一体运营	运维+服务，降低使用成本	资源池部署漏扫、入侵检测、管控上网行为等安全能力

运营商实践：远程办公/远程接入方案

- **远程办公/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。SASE服务对员工终端进行**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。

需求
• 避免员工访问恶意软件或带毒网站，保护员工移动/远程办公终端安全 • 避免非法访问，保护企业内部应用和云端服务 • 防止敏感数据被泄露和篡改 • 解决传统VPN无法细粒度访问控制



安装SASE客户端将访问流量引导**就近PoP点**

PoP点部署**恶意网站过滤、防病毒等模块**保护员工访问和办公终端安全

零信任系统实现员工**身份认证和持续信任评估**

PoP点部署**DLP**等模块保护数据安全

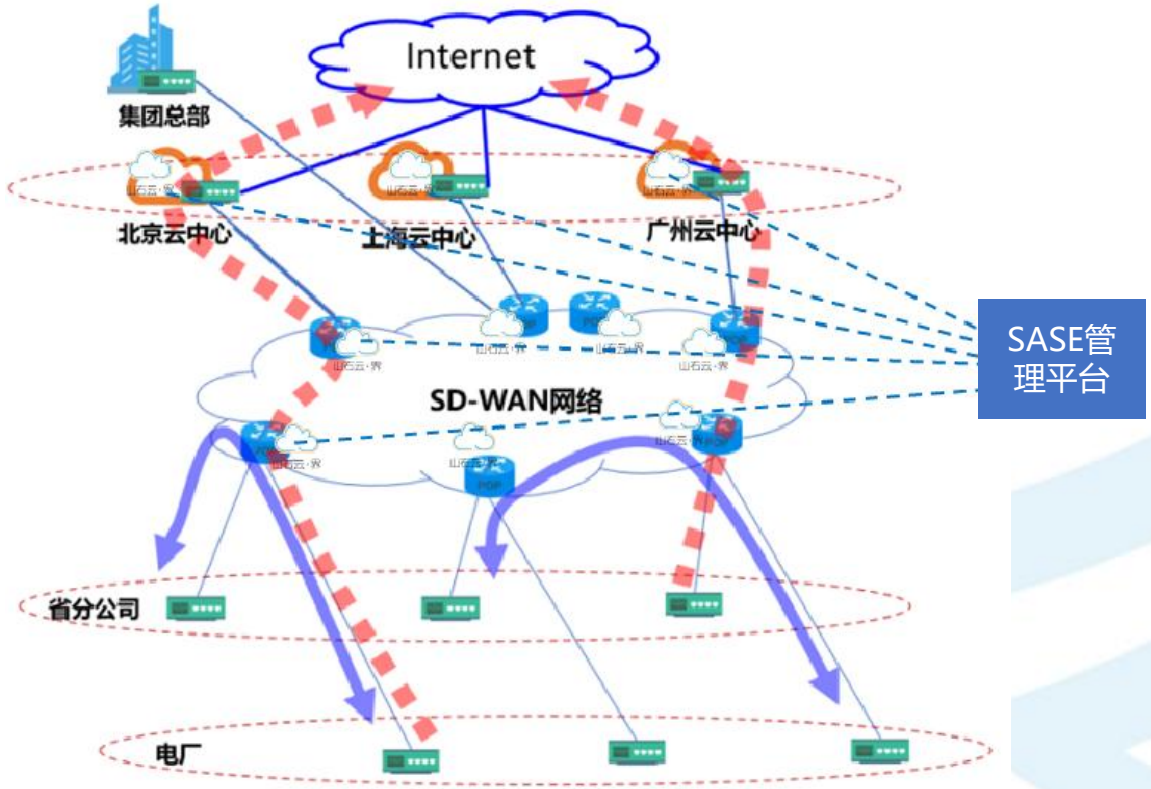
PoP点部署**访问控制**，避免非法访问

运营商实践： 统一出口SASE方案

➢ **互联网暴露面统一管理**：政策要求，政企、能源等关键行业的亟需收敛暴露面，进行流量过滤监控，保证上网行为合规。SASE为垂直行业客户收敛上网数据出口和东西向访问控制，提供统一的流量过滤和行为管控服务

需求

- 收敛上网数据出口
- 规范分支机构上网行为
- 各个分支按需组网，互联流量不经总部
- 保护分支节点和数据中心之间的互访行为
- 重点保护主要分支节点和数据中心
- 安全和网络策略统一制定和推送



通过SD-WAN引流收敛上网出口

互联网出入口部署**过滤监控**和**审计**上网流量数据等功能模块

SD-WAN部署**应用防火墙、入侵检测**等模块

SD-WAN&SASE业务系统集中管理所有安全和网络功能

目录

运营商SASE建设挑战与展望

➢ **国内运营商已推动SASE技术试点与项目应用，但还面临诸多挑战：分布式部署的异构安全能力编排管理困难，产业生态不完善，应用场景较为单一。**

- SASE 技术的发展需要制定统一和标准化的技术规范，促进行业的良性发展。

研究和标准

- SASE作为一种新的网络安全和接入模型，需要各行业间相互合作来实现。运营商需要与云服务、安全和网络等供应商进行紧密的合作。

生态合作

- 未来运营商可以通过不断优化和创新，拓展SASE应用场景，例如结合算力网络，应用于物联网，加速办公，AI计算等方向。

场景扩展

谢谢！