基于SD-WAN构建SASE模型思路浅析

Research and Design of SASE Model Based on SD-WAN

李长连，马季春，蔺　旋（中讯邮电咨询设计院有限公司，北京 100048）
Li Changlian，Ma Jichun，Lin Xuan（China Information Technology Designing & Consulting Institute Co.，Ltd.，Beijing 100048，China）

摘　要：
介绍了SASE理论体系与特征，提出了使用SD-WAN、SDP、SDS构建SASE模型的设计思路，介绍了SASE的详细架构设计、业务流程设计以及实际业务场景下的部署方案，展望了SASE的技术发展趋势与下一步研究方向。

关键词：
安全访问服务边缘；SD-WAN；软件定义边界；软件定义安全
doi：10.12045/j.issn.1007-3043.2021.06.015
文章编号：1007-3043（2021）06-0078-06
中图分类号：TN915
文献标识码：A
开放科学（资源服务）标识码（OSID）：

Abstract：
It introduces the theoretical model and characteristics of SASE，puts forward the design idea of using SD-WAN，SDP and SDS to build SASE model，introduces the detailed architecture design of SASE，business process design and the deployment scheme under the actual business scenario. At last，it prospects the technology development trend and the future research direction of SASE.

Keywords：
SASE；SD-WAN；SDP；SDS

引用格式：李长连，马季春，蔺旋. 基于SD-WAN构建SASE模型思路浅析[J]. 邮电设计技术，2021(6)：78-83.

0 前言

在2019年下半年，Gartner提出了一项新的技术安全访问服务边缘（SASE——Secure Access Service Edge）。Gartner对SASE的定义为：SASE是一种基于实体的身份、实时上下文、企业安全/合规策略，以及在整个会话中持续评估风险/信任的服务。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[1]。

SASE模型是满足云计算和分布式办公需求的网络安全访问模型，是对传统企业网络架构的升级优化，得到了业界的广泛认同，很多厂商都在推进相关研究与方案落地，但目前还没有形成业内公认的标准架构。本文主要探讨如何基于现有SD-WAN体系构建符合SASE模型的新型架构。

收稿日期：2021-05-20

1 SASE理论体系与特征分析

1.1 理论体系

在传统的企业网络中，数据中心是访问的焦点。Gartner认为，随着企业向软件即服务（SaaS）、云服务和边缘计算平台的过渡，企业数据中心实际上只是一个分支[2]。移动化办公是企业信息化办公的大势所趋，办公所涉及的信息数据，使用的计算终端，正在逐渐走出企业的传统边界，企业安全也正面临着全新的挑战。企业IT资产不再集中于数据中心，而是分布于公有云、私有云、边缘云、数据中心等多种环境，需支

持内网、固定互联网、移动互联网、物联网等多种访问方式，网络访问模型日趋复杂，传统的边界安全访问模型不再适用，安全访问服务边缘（SASE）应运而生。

如图1所示，SASE将先前分散的网络和安全服务融合在一起，将本地用户、移动用户以及IoT设备和云资源，整合为统一的服务。

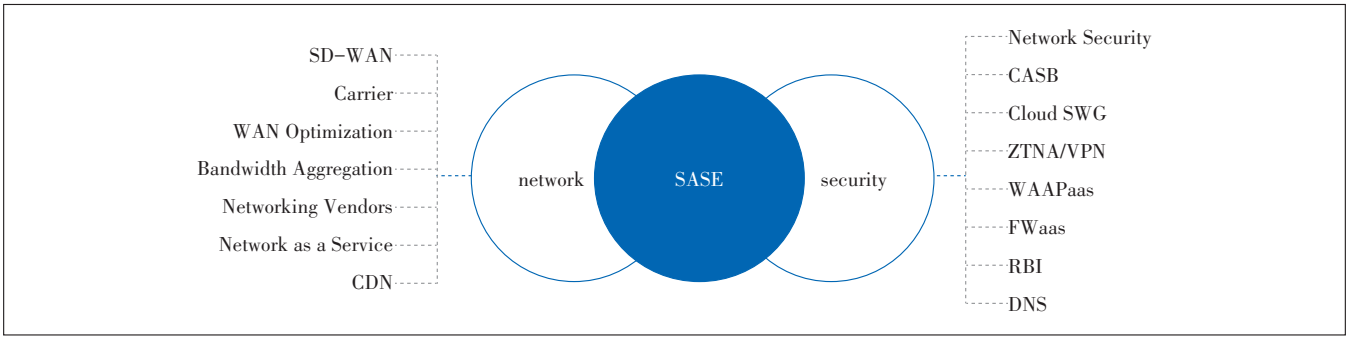

图1　SASE理论体系图

SASE的WAN端依赖于SD-WAN提供商、运营商、内容交付网络、网络即服务提供商、带宽聚合器和网络设备供应商提供的功能。

安全方面依靠云访问安全代理、云安全Web网关、零信任网络访问、防火墙即服务、Web API保护即服务、DNS和远程浏览器隔离。

1.2 特征分析

SASE有4个主要特征：身份驱动、云原生、支持所有边缘、广域分布。

身份驱动：由用户和资源身份，而不是IP地址，决定网络互连体验和访问权限级别。服务质量、路由选择、应用的风险安全控制，所有这些都由与每个网络连接相关联的身份所驱动。

云原生：SASE架构利用云的几个主要特性，包括弹性伸缩、自适应、自恢复和自维护，降低客户成本开销，快速方便地适应新兴业务需求，而且随处可用。

支持所有边缘：SASE为所有公司资源创建了一个网络，覆盖了数据中心、分公司、云资源和移动用户。

广域分布：为确保网络和安全功能随处可用，并向边缘交付尽可能好的体验，SASE云服务必须广域分布。

2 SASE模型设计思路

通过对SASE理论模型以及特征的分析，可以看出SASE是SD-WAN、云计算、虚拟化等技术与安全功能的融合，可以由软件定义广域网SD-WAN、软件定义边界SDP与软件定义安全服务SD-SEC技术融合来实现。图2给出了SASE模型设计图。

2.1 核心组件分析

2.1.1 SD-WAN

SD-WAN全称为软件定义广域网，是将SDN技术应用到广域网场景中所形成的一种服务[3]。它通过虚拟化技术、应用级的策略、自动化网络连接及可管理的边缘CPE设备实现广域地理范围的企业网络、数据中心、互联网应用及云服务连接。SD-WAN主要由SD-WAN控制器、POP点和CPE组成[4]，其技术架构如图3所示。

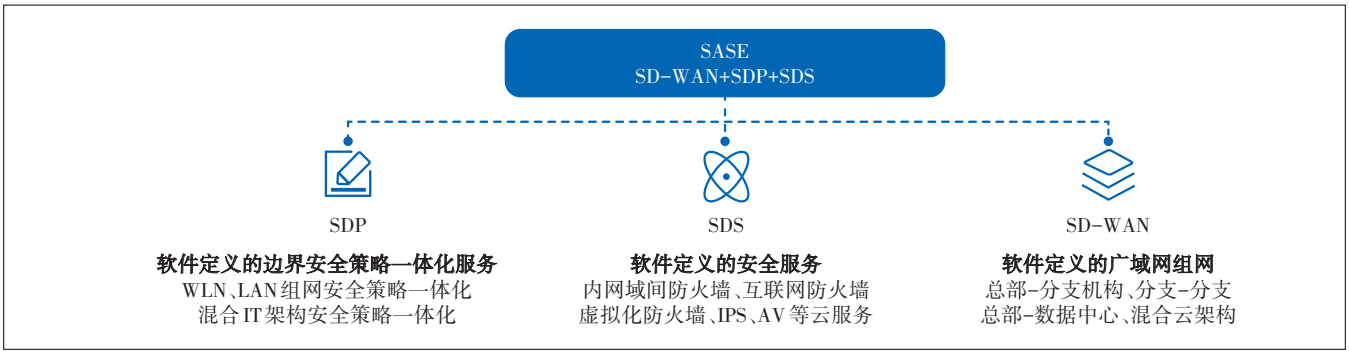

图2　SASE模型设计图

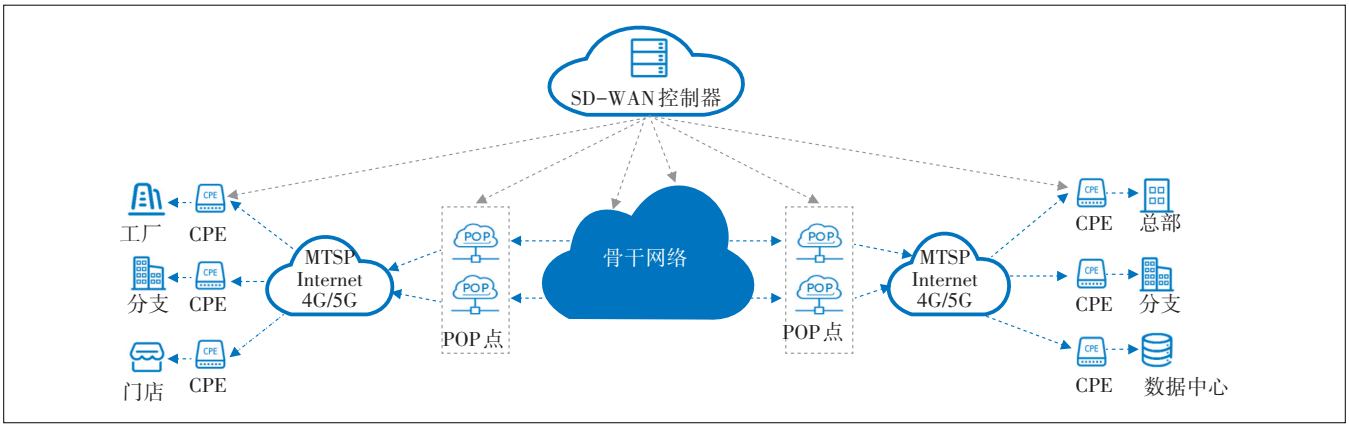

图3　SD-WAN技术架构图

2.1.2 SDP

零信任代表了新一代的网络安全防护理念，它的关键在于打破默认的“信任”，即“持续验证，永不信任”。默认不信任企业网络内外的任何人、设备和系统，基于身份认证和授权重新构建访问控制的信任基础，从而确保身份可信、设备可信、应用可信和链路可信。

2007年美国国防信息系统局提出了一个创新的加密安全解决方案——SDP软件定义边界，后来被云安全联盟采纳，并于2015年被Google公司落地成BeyondCorp项目，SDP是目前最好的实现零信任理念的技术架构之一。

SDP也被称为“黑云”(Black Cloud)，是基于策略创建安全边界，用于将服务与不安全的网络隔离开。SDP要求在获得对受保护服务器的网络访问之前，先对端点进行身份验证和授权，然后在请求系统和应用程序之间实时创建加密连接。SDP将用户的数据和基础设施等关键IT资产隐藏在用户自己的黑云里，这些关键IT资产对外是不可见的。如果黑客无法知道目标在何方，那么攻击将无法进行[5]。

如图4所示，SDP包括SDP客户端、SDP控制器、SDP安全网关以及5个安全保护组件(单数据包授权、Mutual TLS、设备校验、动态防火墙、应用绑定)。

2.1.3 SDS

软件定义安全(SDS——Software Defined Security)是从软件定义网络(SDN)引申而来，原理是将物理及虚拟的网络安全设备与其接入模式、部署方式、实现功能进行了解耦，底层抽象为安全资源池里的资源，顶层统一通过软件编程的方式进行智能化、自动化的业务编排和管理，以完成相应的安全功能，从而实现

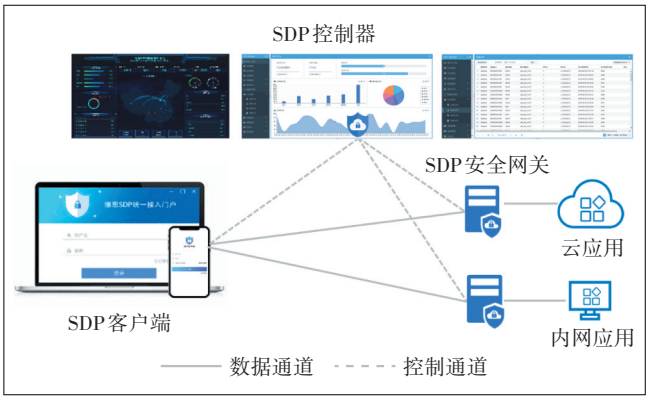

图4　SDP技术架构图

一种灵活的安全防护(见图5)。

2.2 SASE架构设计

本文所提出的SASE架构的创新设计思路主要有：

a) 底层协议替换：传统SD-WAN一般使用IP-Sec技术构建长连接、固定的通信隧道，而SASE模型关注的是客户安全接入具体应用，一旦客户访问应用结束就需要立刻关闭，因此TLS连接是更好的加密隧道选择。

b) 全面云化：不同于传统SD-WAN与安全资源池以盒式设备为主，本文所提出的SASE架构，除了某些场景下客户要求硬件CPE之外，所有CPE、POP、安全资源池均采用云化部署方式，实现能力灵活控制与资源弹性供给。

c) 全面拥抱零信任：SDP的设计理念在本架构得到全面应用，采用SPA(单包授权认证)、MTLS(双向认证)、动态防火墙、设备验证和应用绑定共五重防御机制，实时采集分析所有用户行为，根据用户行为实时计算并更新信任度模型数值，以此为基础动态调整用

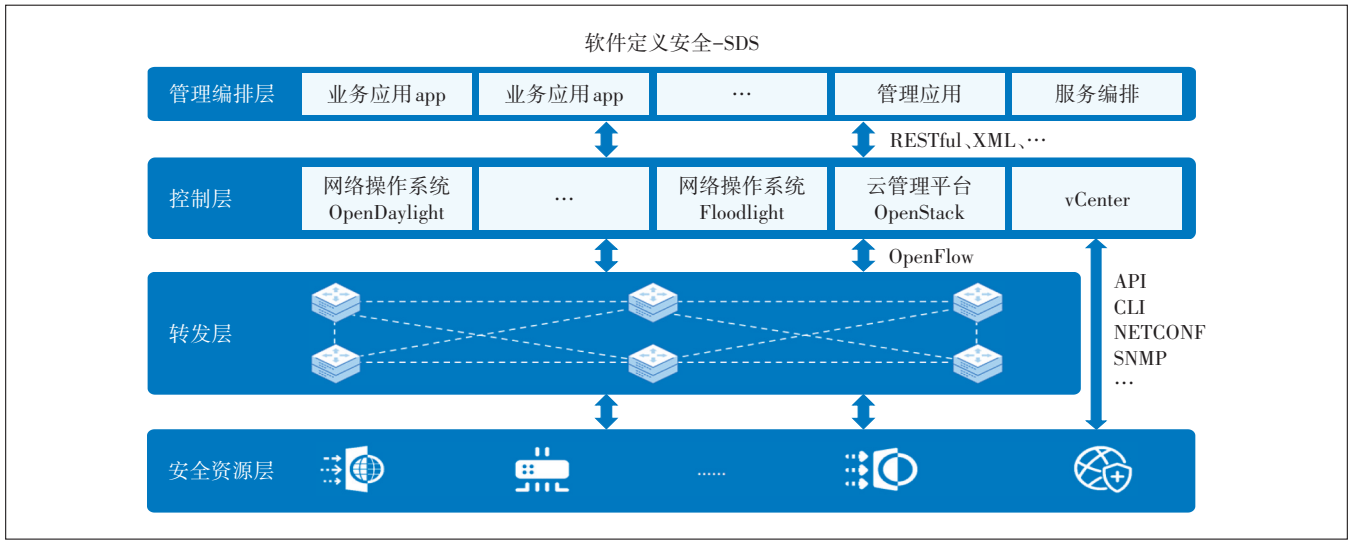

图5　SDS技术架构图

户应用访问权限。

根据以上的设计思路，SASE架构包括管控平台、云化POP、CPE和客户端4个层次，设计架构如图6所示。主要包括：

a）SASE管控平台：相比传统SD-WAN控制器，增加了用于实现客户零信任认证与授权的SDP&4A功能模块，控制器需要同时实现对POP、CPE、云安全资源池、云CPE内所部署各类安全能力的统一命令控制，由安全编排器、网络编排器分别实现网络安全、网络路由的业务编排，2个编排器之间实现控制协同，安全大脑和威胁情报中心实现对全网威胁情报的搜集整理与输出赋能，并对SASE中各安全能力实时监测防护所产生的数据进行处理，生成威胁情报与安全态势感知。

b）云POP与云安全资源池：部署在边缘云或者骨干网节点，通过云POP的加密隧道构建一张高质量虚拟化骨干专网，为了实现对多客户的高质量网络支撑，云POP点部署范围应尽量实现广域分布，云POP具备智能选路、流量聚合、流量加解密等功能，并采用虚拟机或者容器化部署方式，以支持弹性伸缩；云安全资源池和云POP部署在云内同一个VPC内，可共享底层流量处理引擎以加速性能，资源池内部署防火

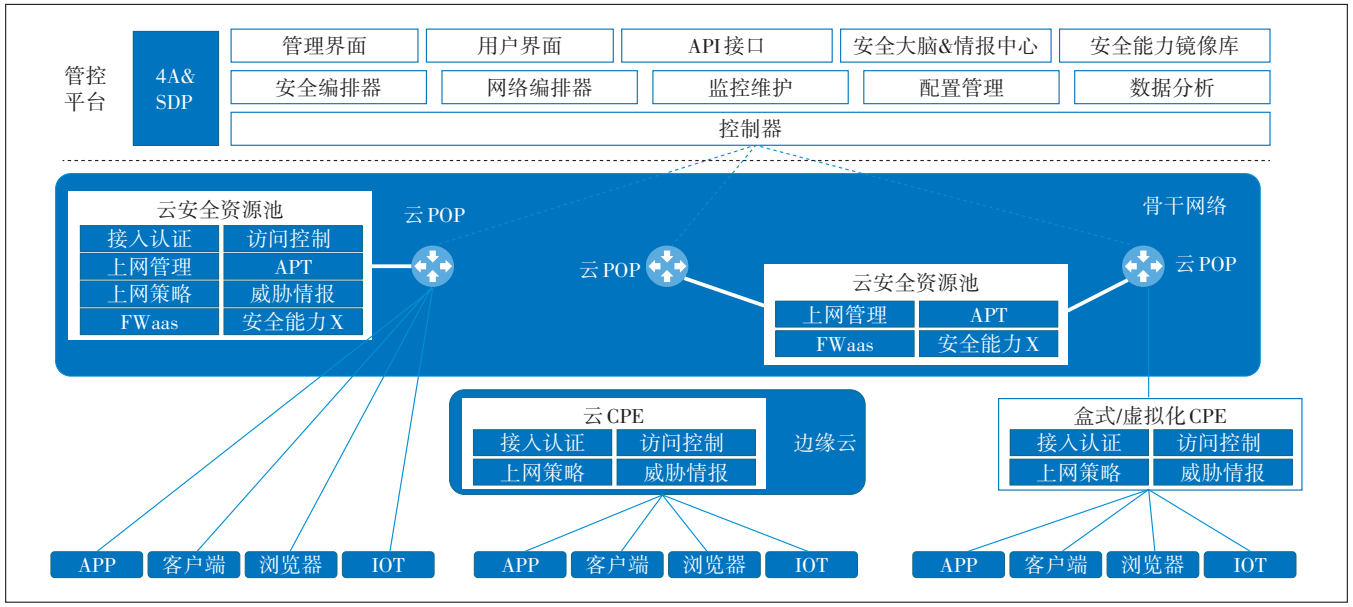

图6　SASE架构设计图

墙、WAF、APT、IPS、上网行为管理等各类云安全能力，由上层控制器统一实现对云安全能力与客户的资源匹配、安全策略配置、安全能力顺序编排、安全能力启停、客户流量牵引与回注等操作。

c）云CPE/盒式CPE/虚拟化CPE：部署在边缘云或者客户现场，采用何种CPE部署方式，取决于客户端访问形式、客户侧资源等因素，SASE虽然强调了云原生，但硬件CPE在很多场景下具备部署简单、网络性能强、资源依赖少、易于维护等优势，具有不可替代性。CPE除了具备流量汇聚、加解密等功能，还需要实现零信任认证、访问控制、上网策略管理、威胁情报同步等安全功能，也可提供防火墙、IPS、上网行为管理等高级安全功能，实现安全能力的下沉与近端处置。

d）客户端：SASE支持移动手机APP、电脑客户端、浏览器、SDK等多种安全接入方式，为实现更安全的接入认证，客户端应具备本地计算环境的安全扫描与安全信息搜集能力，也可与本地的防病毒等安全软件实现一体化集成。

2.3 SASE业务流程设计

如图7所示，SASE架构用于客户内网跨广域访问、移动办公访问、内网访问互联网等很多场景，此处仅以客户跨广域访问应用为例说明其业务流程设计。

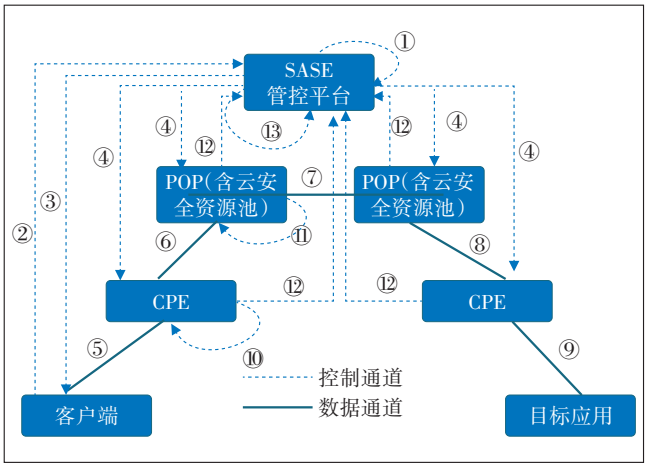

图7　SASE业务流程设计示意图

a）SASE管控平台建立全局视角的用户应用访问控制矩阵，建立每个用户的签约安全策略、网络路由策略与QoS质量保证。

b）用户访问目标应用系统，在客户端输入相应的认证信息（用户名、密码、手机短信校验码等），向SASE控制器发起SPA认证请求（包含认证信息以及设备信息）。

c）SASE管控平台对客户端SPA认证信息进行验证，关联用户应用访问控制矩阵，与客户端建立TLS连接，返回授权票据、第一跳CPE信息。

d）SASE管控平台向所有POP以及CPE下发安全控制策略、路由策略与QoS。

e）客户端携带授权票据对第一跳CPE进行SPA敲门认证，CPE对客户端SPA认证信息进行验证，建立TLS连接。

f）CPE根据路由选择POP，携带授权票据对POP进行SPA敲门认证，POP对认证信息进行验证，建立TLS连接。

g）POP点根据路由选择下一跳POP，携带授权票据对POP进行SPA敲门认证，POP对认证信息进行验证，建立TLS连接。

h）POP根据路由选择CPE，携带授权票据对CPE进行SPA敲门认证，CPE对认证信息进行验证，建立TLS连接。

i）CPE根据路由与目标应用之间建立TLS连接。

j）用户流量达到CPE之后，CPE加载客户安全控制策略，对客户流量进行访问控制、上网管控等安全操作。

k）用户流量达到POP之后，POP加载用户签约安全策略，启动云安全资源池内相应安全能力，牵引客户流量进行监测与防护，并进行回注或者下一跳路由。

l）所有的CPE与POP实时向SASE管控平台上传安全日志。

m）SASE管控平台根据安全日志对用户行为进行分析，实时调整用户安全策略与应用访问控制矩阵。

3 SASE部署方案设计与验证

SASE架构在实际客户应用场景中，需要根据客户需求进行灵活裁剪与针对性部署，本文以某中型股份制银行为例进行SASE部署方案设计与验证，该银行在全国范围内拥有数量众多的分行与支行，分行与支行均有专线互联，另一方面，分行与支行均存在互联网访问需求，存在的主要安全问题与需求包括：

a）分行与支行内存在大量敏感数据，需要防止数据通过互联网泄露。

b）分行与支行均部署了数量众多的硬件上网行为管理设备，每年硬件购置与维护费用高昂，无法快速实现统一的上网策略管理，新需求响应慢。

从上网行为集中管控、敏感数据统一防护、降低成本、需求弹性扩展、集中维护等多角度考虑，考虑引入本文所设计的SASE架构（见图8），主要设计思路包括：

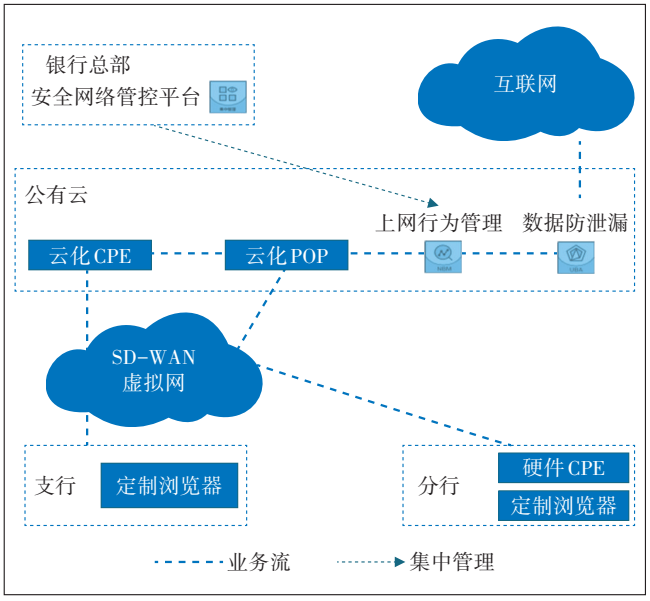

图8　SASE部署方案示意图

a）为了实现零信任认证，要求所有上网终端必须安装定制浏览器，未安装定制浏览器的终端无法上网。

b）关闭所有分行与支行的互联网出口，只保留访问POP或者云CPE的白名单。

c）由于资源限制，同时为了降低成本，便于后期维护，对于规模较小、带宽需求不大的支行/分行采用客户端直接访问云CPE的模式；对于规模较大、带宽需求较大的分行可以考虑部署硬件CPE，提升传输质量并节省带宽。

d）选择主流公有云，在31个省分的省会区域公有云节点上部署云CPE、云POP以及云安全资源池，资源池内部署上网行为管理与数据防泄漏功能，流量编排顺序是先引流到上网行为管理，然后进行数据防泄漏检查，最后出互联网。

上述SASE架构方案已在该股份制银行得到了部署验证，运行效果如下。

a）分行/支行客户上网体验与之前保持一致。

b）银行整体安全设备购置、运营与维护成本费用大幅下降。

c）互联网与数据暴露面得到有效控制，安全管控能力显著提升。

d）实现集团级安全集中运营与监控，可以快速调整安全策略并响应新需求。

4　结束语

SASE模型目前已经成为国内外网络安全领域与通信领域的研究热点，也是云计算、网络安全、广域网通信技术深度融合的范例，本文创新性地提出了基于SD-WAN、SDS、SDP构建SASE架构，采用通信协议栈融合、零信任、云计算等技术解决了三者技术融合的难题，设计了具体的业务处理流程以及部署参考架构，可以有效地解决客户的广域网通信与安全需求。

SASE模型并不是万能的网络安全解决方案，它仍然存在很多技术难题需要进一步的研究。

a）SASE模型可以实现网络隐身与可信任实体安全访问，但对可信任实体通过安全网关之后的操作缺乏监控与管理手段，也难以完全避免恶意攻击者以可信任客户端为跳板发起攻击，因此需要研究SASE模型与微隔离、态势感知、APT监测等其他安全手段的技术融合问题。

b）SASE模型中云POP的安全资源池要求用户提供证书对加密流量进行解密，以实现入侵检测、上网行为管理等安全操作，会增加资源消耗与网络时延，客户对提供证书也有安全担忧，因此加密流量的安全监测与防护也是一个重要研究方向。

参考文献：

[1] 国家互联网应急中心（CNCERT）. 2019年我国互联网网络安全态势综述[R/OL].[2021-03-25]. https://www.cert.org.cn/publish/main/upload/File/2019-year.pdf.

[2] 孙志，齐学功，金怡，等. 涉密内网安全防护体系的研究与实践[J]. 信息安全与通信保密，2011(6)：36-38.

[3] 刁兴玲，梅雅鑫. SD-WAN应运而生 助力企业在5G时代实现数字化转型[J]. 通信世界，2019(32)：47-48.

[4] 杨锋. SD-WAN应用场景和规模部署挑战浅析[J]. 通信世界，2019(34)：47-48.

[5] PINGREE L，CONTU R，KISH D，et al. Gartner Predicts 2016：Security Solutions[EB/OL]. [2021-03-25]. https://www.gartner.com/doc/3175024/predicts-security-solutions.

作者简介：
李长连，毕业于西北工业大学，硕士，高级工程师，主要从事网络安全技术研究、规划咨询、网络安全产品研发与运营工作；马季春，教授级高工，主要从事数据通信网络咨询、规划、设计，以及云网协同、网络安全、网络大数据等的创新研发工作；蔺旋，毕业于西安交通大学，硕士，主要从事网络安全技术的研究工作。