基于SD-WAN的SASE云安全资源池方案研究

Research on SASE Cloud Security Resource Pool Scheme Based on SD-WAN

王宏鼎[1]，蔺　旋[2]，李长连[2]（1. 中国联合网络通信集团有限公司，北京 100048；2. 中讯邮电咨询设计院有限公司，北京 100048）
Wang Hongding[1]，Lin Xuan[2]，Li Changlian[2]（1. China United Network Communications Group Co.，Ltd.，Beijing 100048，China；2. China Information Technology Designing & Consulting Institute Co.，Ltd.，Beijing 100048，China）

摘　要：
安全访问服务边缘（SASE）模型基于自身特性实现了网络能力和安全能力的分布式云服务交付。基于SASE云原生架构的特性，提出了一种结合SD-WAN网络工具和SDN技术的SASE云安全资源池设计方案。介绍了SASE云安全资源池的整体架构、安全能力端云协同、云安全资源池业务流程设计及方案验证，最后总结SASE云安全资源池的设计建设经验并展望该技术的发展趋势。

关键词：
SASE；SD-WAN；SDN；云安全资源池
doi：10.12045/j.issn.1007-3043.2022.09.011
文章编号：1007-3043（2022）09-0049-06
中图分类号：TN915.08
文献标识码：A
开放科学（资源服务）标识码（OSID）：

Abstract：
The secure access service edge (SASE) model realizes distributed cloud service delivery of network capabilities and security capabilities based on its own characteristics. Based on the cloud native architecture characteristics of SASE, it proposes a SASE cloud security resource pool design scheme that combines SD-WAN network tools and SDN technology. It introduces the overall architecture of the SASE cloud security resource pool, security capability end-cloud collaboration, the design and scheme verification of cloud security resource pool business process. Finally it summarizes the design and construction experience of the SASE cloud security resource pool and looks forward to its technological development trends.

Keywords：
SASE；SD-WAN；SDN；Cloud security resource pool

引用格式：王宏鼎，蔺旋，李长连. 基于SD-WAN的SASE云安全资源池方案研究[J]. 邮电设计技术，2022（9）：49-54.

0 前言

Gartner在2019年发布的《网络安全的未来在云端》中提出一项新的技术概念SASE（Secure Access Service Edge），其定义是一个融合了软件定义广域网和网络安全功能，以支持数字化企业需求的新兴技术[1]。

SASE将广域网与网络安全（如SWG、CASB、FWaaS、ZTNA）结合起来，将本地用户、移动用户以及物联网设备和云资源整合为统一的服务，从而实现网络和安全能力的云交付[2]。目前仍没有形成关于SASE的业务公认标准架构和能够提供完整SASE链条的服务提供商。SASE网络安全模型如图1所示。

传统的网络安全架构选择在数据中心或企业总部的边界部署物理安全设备，通过安全设备的安全防护能力实现对企业重要资产的安全防护。但是传统方案具有购置成本高、部署难度大、运维难度大、灵活性差等问题[3]。本文在SD-WAN的基础上，提出了一

收稿日期：2022-07-20

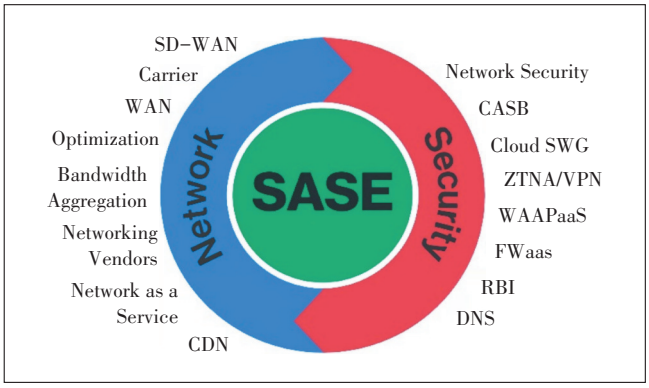

图1　SASE网络安全模型

种SASE云安全资源池完整解决方案，安全能力即服务，提供广域可达的云安全服务交付。相比传统安全方案，云安全资源池方案使用成本低、灵活性高，无需购置部署安全设备，通过管理平台可定制个性化的安全服务，且可进行安全服务能力的弹性扩容。云安全资源池是SASE模型云原生特性的具体应用，也是SASE安全能力栈的重要实现形式，而云安全即服务也成为当前的技术潮流[4]。

图2为相对完整的SASE服务链条，作为SASE整体服务链条的重要一环，云安全资源池负责提供安全服务。多分支企业通过SD-WAN搭建的广域网互联，在SD-WAN接入端进行基于身份的认证准入和权限控制，安全资源池提供云化的安全服务并通过SD-WAN实现引流，SD-WAN网管平台和安全能力平台在SASE统一管理平台的协调下实现网络和安全能力的

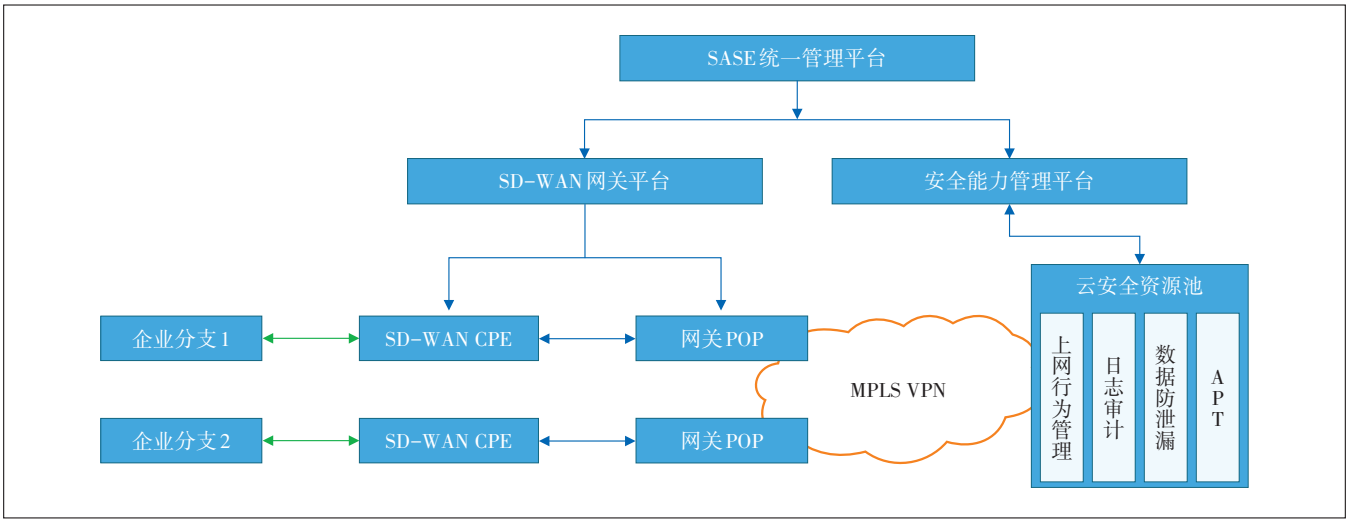

图2　基于SD-WAN的SASE架构图

快速交付[5]。

1 云安全资源池架构设计

SASE网络安全模型的云安全资源池具有云原生和广域分布的特点，一方面支持安全能力的弹性扩容，具备自适应和自恢复的能力，充分分摊安全能力成本；另一方面保证对所有边缘交付快速便捷安全服务。

云安全资源池由统一的云计算管理平台、资源池内部的安全能力集以及统一的安全能力管理平台组成。

云计算管理平台统管云安全资源池内部所有计算和网络资源，提供资源的管理、调度能力。安全能力集根据不同安全能力的特点分配不同的软件资源，并对网络进行合理的规划，对上网行为管理、数据防泄漏等不同的安全能力VPC进行必要的隔离，保障资源池内部模块的网络和业务安全。安全能力管理平台通过API接口实现对资源池内的多种安全能力的统一管理，实现用户管理、策略管理、任务管理、性能监控、记录审计等功能，图3为云安全资源池的整体功能架构[6]。

1.1 云计算管理平台

云管平台是SASE云安全资源池的重要组成部分，负责安全资源池的资源管理和运维工作，对各类安全能力VPC进行集中管理，实现对计算资源、存储资源、网络资源的申请、操作、回收以及监控等功能。并将物理分散的数据中心资源进行逻辑统一管理，通过灵活的资源调度策略，包括错峰复用、动态伸缩、跨

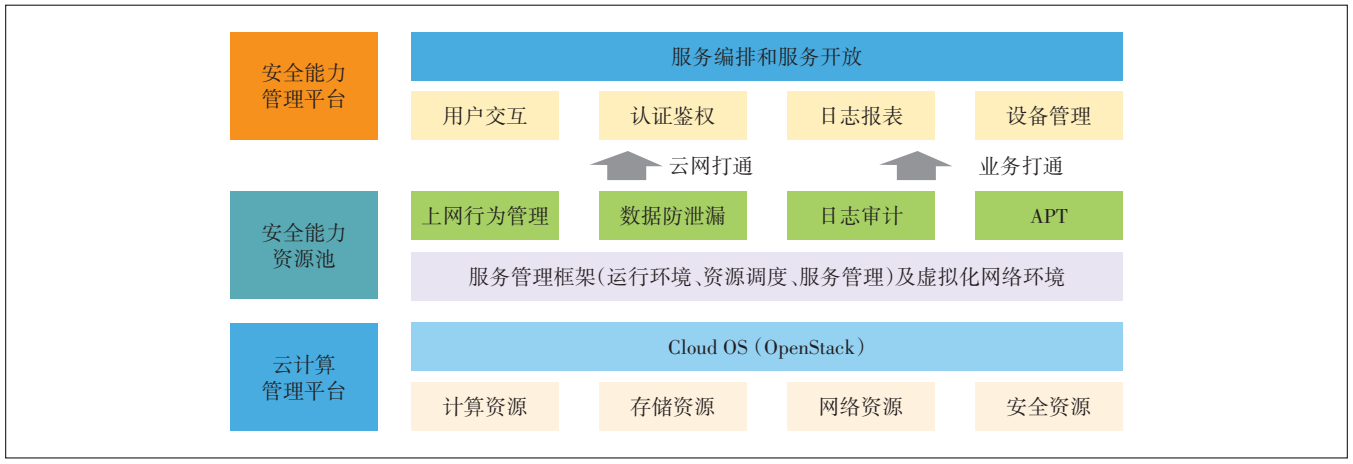

图3　云安全资源池功能架构

数据中心共享和迁移等技术手段，实现应用的灵活部署。

OpenStack架构已逐渐成为业界事实标准，在构建云管理平台时，建议优选OpenStack架构以保证兼容性和开放性[7]。

1.2 云安全能力资源池

云安全能力资源池主要为用户提供多种云化的安全能力，因此需要在资源池内部署包含多种安全产品的安全能力集，而不同安全能力需要合理规划并分配相应的计算资源、网络资源和存储资源等。

SASE云安全资源池能力根据用户需求和安全能力规划部署流量类和扫描类等安全产品，流量类产品包括安全服务、日志审计、数据防泄漏等，扫描类产品包括漏扫扫描等主动探测类的安全能力。此外，云安全资源池的所有安全能力需要满足虚拟化部署的要求，能力集与安全能力管理平台和云管平台通过虚拟网络设备实现互联[8]。

1.3 安全能力管理平台

安全能力管理平台对云安全资源池内的所有安全能力进行纳管和对接，实现对所有安全能力的账户、策略、任务等多个维度的管理，并实现对多种安全能力数据的实时审计和综合展现等功能，建设成为以用户为中心的综合运营业务平台和标准大数据运营分析体系[9]。

1.3.1 服务编排

安全能力管理平台需要结合SDN技术，利用虚拟路由器、虚拟交换机、防火墙等网络设备，实现安全能力VPC之间的网络隔离，还需要实现安全业务编排、负载均衡及动态扩容等。

针对订购多项安全服务的用户，用户可通过安全能力管理平台自定义安全能力链条，选择个性化的流量处理方案；针对单个安全服务，在不影响用户业务的前提下，用户可以通过安全能力管理平台对安全服务的处理能力进行动态扩容[10]。

1.3.2 服务开放

本文的研究内容为基于SD-WAN的SASE云安全资源池解决方案，安全能力管理平台需要和SD-WAN平台进行能力的对接，需要对SD-WAN及其他云网产品提供SaaS化的服务，实现对资源池应用适配和调度服务，向上提供标准的平台访问框架和能力开放服务[11]。

2 SASE云安全资源池业务流程设计

SASE云安全资源池解决方案适用于使用SD-WAN作为组网工具且对云化安全服务有需求的企业。本文提出的云安全资源池解决方案利用SD-WAN实现用户流量到资源池的引流，而且与其他资源池方案相比，本文的方案具有端云安全能力协同的独特优势。

2.1 引流方案设计

云安全资源池可部署在多个POP点，为节点下的用户提供云化的安全服务，而对于流量类的安全服务，需要将用户流量引流至资源池处，经过处理后进入指定网络。本文的SASE云安全资源池基于SD-WAN，资源池的引流需要通过SD-WAN将用户流量从用户的POP节点利用策略路由引流至云安全资源池所在的POP节点，经过用户流量隔离后进入资源池。云安全资源池引流方案如图4所示。

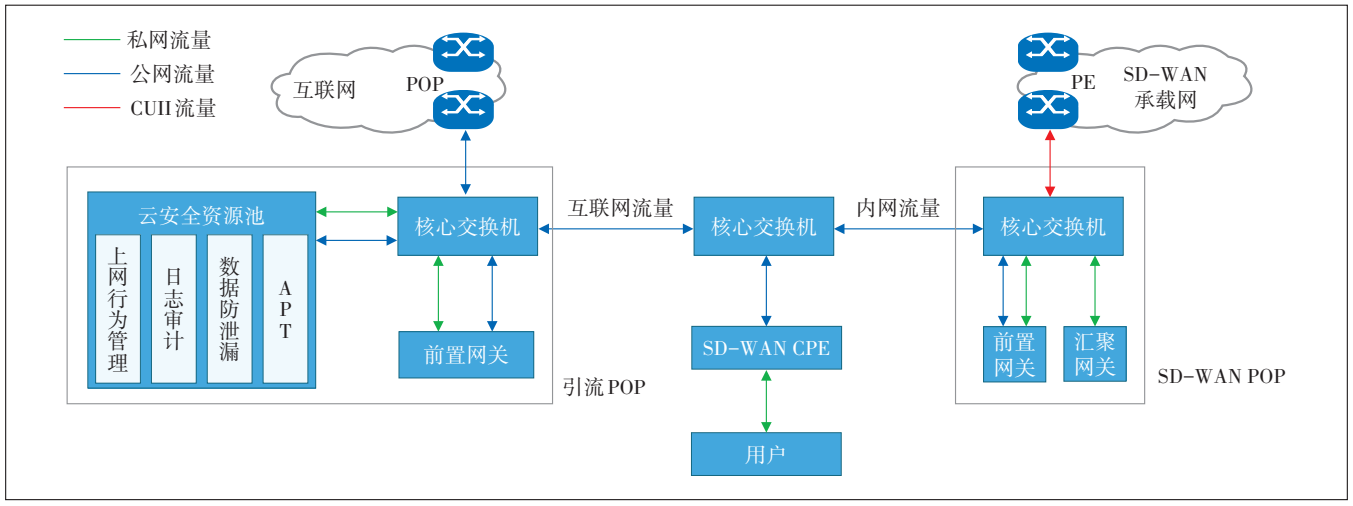

图4　云安全资源池引流方案

通过部署前置网关在云安全资源池所在节点建设SD-WAN的专用引流节点，该节点独立于SD-WAN其他的业务节点，建设引流POP节点一方面可降低对SD-WAN业务的影响，另一方面降低了云安全资源池的部署要求和引流工作的难度[12]。

2.2 安全能力端云协同

基于SD-WAN的SASE模型架构为企业用户提供一套完整的网络、安全服务，用户在终端进行用户身份验证后再接入所属的广域网络，安全服务部署在用户网络可达的云端安全资源池。

基于SD-WAN的云安全资源池依托SASE模型，利用安全管理平台的统一管理和策略同步，具有端云安全能力协同的优势，通过集成安全能力的SD-WAN接入终端与云安全资源池进行联动，实现从端到云的安全能力协同。特别是针对流量类的安全服务，用户流量通过SD-WAN终端时，接入终端针对需要拦截的流量进行处理，随后将处理日志同步到安全能力管理平台，对于其他流量，终端不做任何处理直接放行，云安全资源池则对流量进行审计、处理和展现，该策略降低了用户链路的负载，提高了云安全资源池的有效利用率。安全能力端云协同如图5所示。

2.3 业务流程设计

此处以流量类安全服务为例，阐述包括引流、端云协同的SASE云安全资源池的安全业务的整体流程。

SD-WAN用户在未启用安全业务时，用户的互联网流量经CPE接入SD-WAN网络，通过加密隧道汇聚到网关POP后直接进入目标网络，而基于SD-WAN的SASE云安全资源池方案业务流程如图6所示。

a）SD-WAN用户下发安全服务订单后，SD-WAN

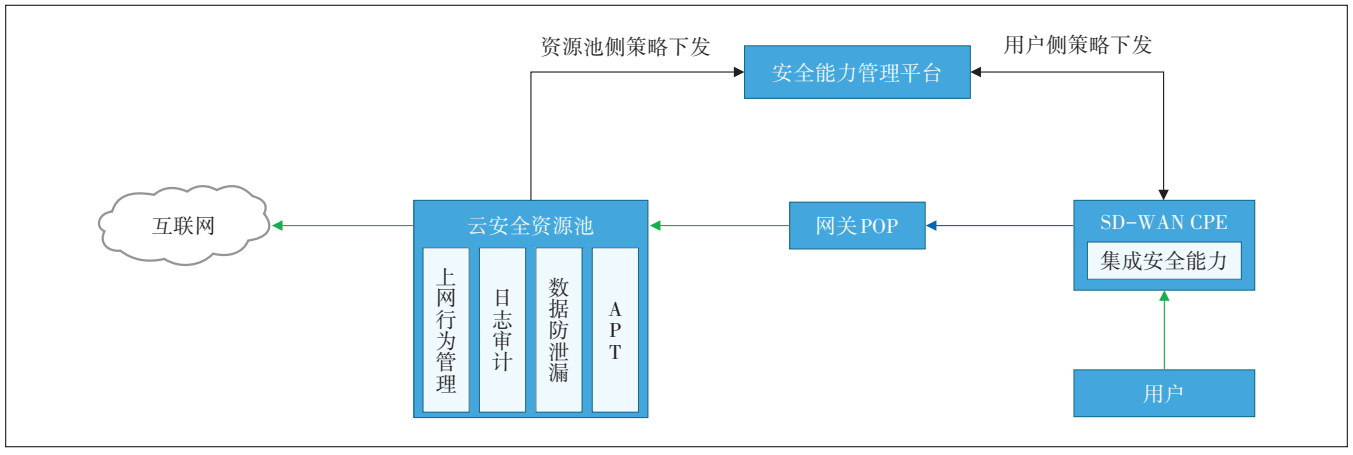

图5　安全能力端云协同

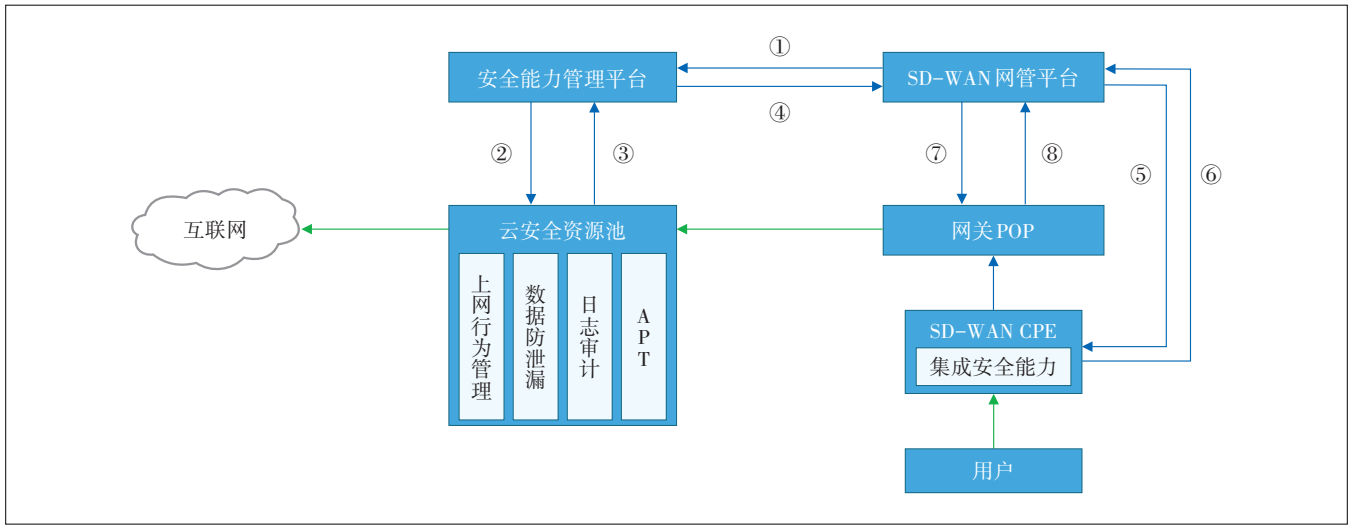

图6　SASE云安全资源池业务流程

网管平台根据用户订单业务参数向安全能力管理平台发送安全服务任务配置等信息。

b）安全能力管理平台确认安全资源余量并启动资源池中的安全服务引擎，然后下发用户的云端资源池安全服务策略至引擎侧。

c）安全资源池完成安全服务能力准备后，向安全能力管理平台反馈任务下发结果。

d）安全能力管理平台向SD-WAN网管平台反馈安全业务下发情况并返回用户侧安全CPE的安全服务策略，用于用户侧的协同任务下发。

e）SD-WAN网管平台向用户CPE下发用户侧安全服务策略。

f）用户侧安全网关CPE向SD-WAN网管平台反馈策略下发结果，完成整体安全能力准备。

g）SD-WAN网管平台下发网络配置，将用户上网流量从专用引流POP点引流至安全服务云安全资源池。

h）用户节点网关POP向SD-WAN网管平台反馈用户上网流量的引流结果。

至此，云安全资源池的业务流程形成闭环，在安全能力管理平台的协调之下实现安全能力的端云协同，对用户的网络和资源进行高效的安全防护[13]。

3 方案对比分析

在传统的本地部署方案中，企业需要在网络出口处部署安全设备，而多分支企业则需要异地部署多套设备；而基于SD-WAN的SASE云安全资源池解决方案将安全能力云化，为各个分支提供安全服务。上网行为管理方案对比如图7所示。

对基于SD-WAN的SASE云安全资源池解决方案与传统安全解决方案进行对比分析，其结果如表1所示。

a）传统方案设备购置成本高，部署周期长，运维管理成本高，灵活性差，策略同步难度大。

b）云安全资源池方案无需本地部署安全设备，无需运维，灵活性高，策略同步方便。

c）云安全资源池方案通过端云协同，显著提高了安全能力利用率，降低了网络链路负担，与传统方案的安全功能与性能无明显差异。

d）云安全资源池解决方案结合分支企业的基础SD-WAN网络，实现了整个网络安全架构的SASE全链条实现。

4 结束语

SASE已成为新的网络和安全设计模式，将逐渐取代以数据为中心的传统网络安全模型。本文提出了基于SD-WAN的SASE云安全资源池解决方案，通过端云安全能力协同为企业提供低成本、快捷方便的安全服务。基于SD-WAN的SASE云安全资源池作为SASE模型的重要一环，实现网络安全即服务，具有较为广阔的市场前景。

云安全资源池在实际应用中无法覆盖全部应用场景，比如当用户的流量较大时，云安全资源池方案会造成用户的网络链路负载较大，影响上网体验，需

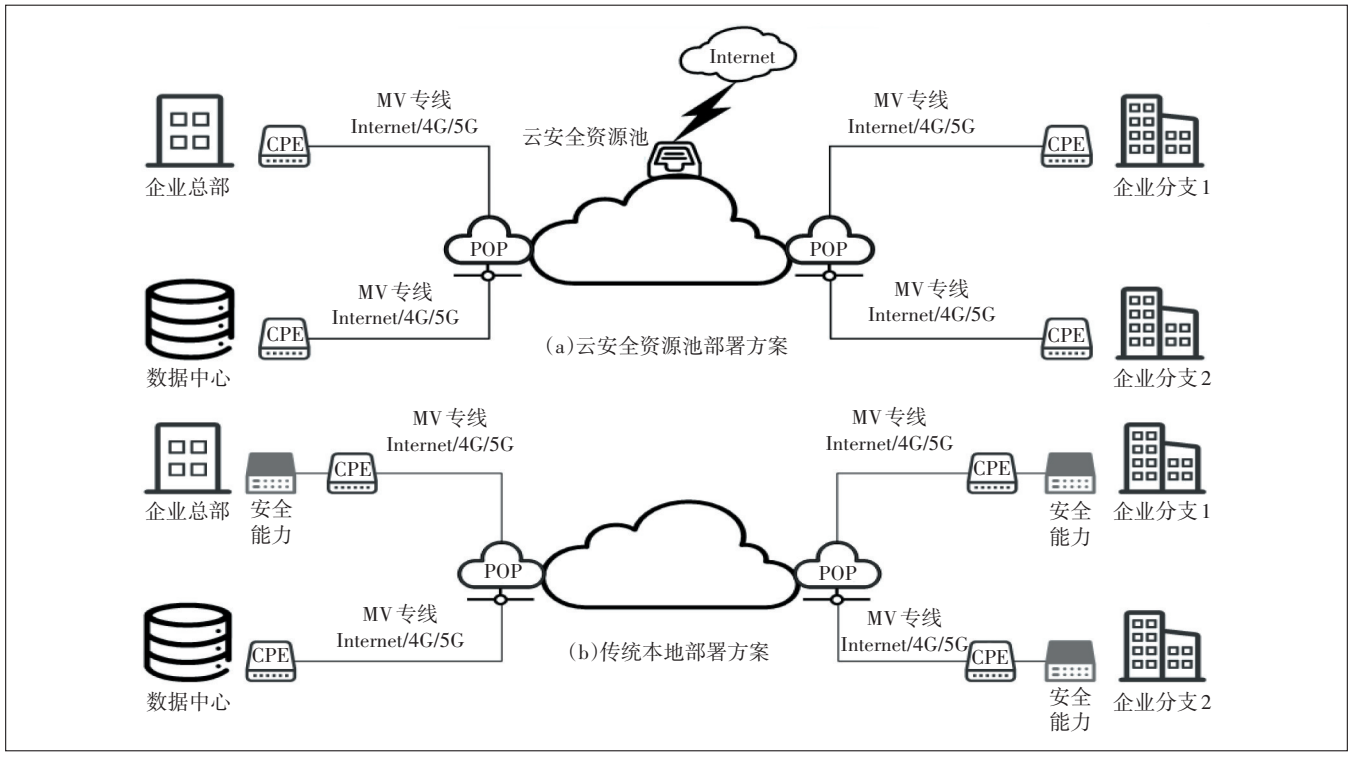

图7　上网行为管理方案对比

表1　安全方案对比分析

对比项	传统方案	云安全资源池方案
使用成本	较高	低
维护成本	较高	低
系统功能	全部功能	全部功能
用户体验	时延低	时延较低

要根据使用需求进行方案选择。此外，目前云计算平台大多使用虚机形式部署安全能力，该部署方式存在配置工作复杂、浪费计算存储资源等缺点，而容器化部署可在适配云安全资源池整体架构的基础上解决上述问题，因此容器化是云安全资源池的重要发展方向[14]。

参考文献：

[1] 张晓军. 实现SASE从理论到落地[J]. 网络安全和信息化，2021(1)：121-123.
[2] 智勇. 基于SASE构建零信任网络安全[J]. 信息与电脑，2022，34(1)：227-230
[3] 胡建强. 基于SD-SEC的云安全资源池设计与实现[J]. 信息与电脑，2020，32(11)：213-216.
[4] 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.
[5] 叶朝阳，王欣，张士聪，等. SASE云安全研究与实践[J]. 电信科学，2022，38(1)：140-149.
[6] 姚岳. 运营商云资源池规划建设与运维管理研究[J]. 电信技术，2015(4)：39-41，45.
[7] 张誌，高卫荣. 电信运营商私有云资源池构建思路[J]. 科学与信息化，2017(36)：45-46.
[8] 吴晨花，王瑶，李映壮. 基于SDN安全云资源池提升中小企业安全防护能力[J]. 科技创新导报，2019，16(5)：140-143.
[9] 司炜. 电信运营商云资源池思路及实现方案研究[J]. 中国新通信，2017，19(17)：102-103.
[10] 闻琛阳，姚娟. SDN技术在云计算资源池的应用及探讨[J]. 信息系统工程，2018(5)：25.
[11] 乔延臣，张结辉，陈晓帆. 基于安全资源池的云安全解决方案[J]. 信息技术与标准化，2018(9)：57-62.
[12] 牛佳，颜永明，赵乾艮，等. SD-WAN多云聚合平台接入方案研究[J]. 电信科学，2022，38(2)：130-138.
[13] 宋洋. 上海电信云资源池IaaS云安全技术分析[J]. 电信技术，2017(6)：84-88.
[14] 邱晨，陈亚峰，周伟. 基于容器化OpenStack云平台及Ceph存储的私有云实施案例[J]. 邮电设计技术，2018(8)：51-56.

作者简介：
王宏鼎，毕业于北京大学，中国联通智网创新中心网络产品研发总监，高级工程师，博士，主要从事网络SDN、云网产品、网络安全产品研发等工作；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；李长连，毕业于西北工业大学，高级工程师，硕士，主要从事网络安全技术研究工作。