SASE 云安全研究与实践

叶朝阳，王欣，张士聪，詹智勇，刘伊莎
（浙江省新型互联网交换中心有限责任公司，浙江 杭州 311215）

摘　要：互联网发展到今天，与传统网络相比已出现了翻天覆地的变化，在当今网络的变革中，“云化”成了企业 IT 架构演进的主流方向，因此对云安全的要求也越来越高，主要介绍了通过 SASE 云安全架构的实践部署，解决客户上云安全问题。提出了独特完整的 SASE 解决方案，该方案将安全功能与 SD-WAN 功能结合，构建统一管控平台、集中部署核心安全资源池按需调用，实现对恶意软件或恶意活动的实时监控、智能分析和自动拦截。实践证明该方案在统一管控、入侵检测与防御、精细化访问控制等方面达到预期效果，能够充分保障企业的云上安全。

关键词：云安全；SASE；SD-WAN
中图分类号：TN929
文献标志码：A
doi:10.11959/j.issn.1000－0801.2022019

Research and practice of SASE cloud security

YE Chaoyang, WANG Xin, ZHANG Shicong, ZHAN Zhiyong, LIU Yisha
Zhejiang Province New-Type Internet Exchange Point Co., Ltd., Hangzhou 311215, China

Abstract: With the development of the Internet today, earth shaking changes have taken place compared with the traditional network. In today's network reform, "cloud" has become the mainstream direction of the evolution of enterprise IT architecture, so the requirements for cloud security are becoming higher and higher. The practical deployment scheme of SASE cloud security architecture was introduced to solve the problem of cloud security for customers. A unique and complete SASE solution was proposed, which combined security functions with SD-WAN functions, and realized real-time monitoring, intelligent analysis and automatic interception of malware or malicious activities by building a unified management and control platform and centralized deployment of core security resource pool. Practice has proved that the scheme achieves the expected results in unified management and control, intrusion detection and defense, fine access control and so on, and can fully ensure the cloud security of enterprises.

Key words: cloud security, SASE, SD-WAN

0　引言

在 Gartner（高德纳，又译顾能公司，是全球较具权威的 IT 研究与顾问咨询公司）2019 年发布的《网络安全的未来在云端》报告中，提出安全访问服务边缘的概念，并将其称为 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

收稿日期：2021−10−28；修回日期：2021−12−20

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。SASE 平台可以支持整个广域网（wide area network，WAN）转换过程，因为它使 IT 能够以敏捷和经济有效的方式提供业务需求的网络和安全功能。因此，SASE 是一个融合了 SD-WAN（软件定义广域网）和网络安全功能的新兴技术，可以很好地支持企业的上云安全。

1　当今企业的 IT 现状及安全困境

1.1　企业的 IT 现状

当前企业数字化转型已是大势所趋，随着大数据、云计算和 5G 新技术的引入，企业 IT 基础设施架构也发生了显著的变化。

- 企业核心应用“云化”，包括企业内部应用云化以及外部应用的互联网。
- 业务场景“边缘化”，越来越多的数据处理和计算下沉到边缘节点完成。
- 办公场景“多样化”，移动办公、远程办公、总部/分支机构协同办公。
- 网络边界转变，网络架构演变到今天，服务、应用和数据越来越多地处在多云、混合云上，无论通过 SaaS（software as a service）访问、公有云访问，还是通过私有云访问，其应用、服务、数据已经分散化，无处不在。带边界层的网络转变如图 1 所示。

1.2　安全困境

在企业核心应用“云化”“边缘化”之后，企业需要敏捷、高速及稳定地访问云资源，无论何时何地，不论是人员还是设备，都能够快速地访问业务应用及数据，但是在满足此需求的同时，又暴露了其他问题，即原来基于 IDC（internet data center）实体中心设计的传统安全防护手段突然失灵了，不能很好地满足企业所需的安全防护要求以及必要的访问控制要求。例如：

- 企业核心应用云化之后，本地 IDC 的防护措施鞭长莫及；
- 企业无法将传统的硬件防火墙、流量清洗、日志审计等安全设备部署在云端；
- 分布式接入后，企业无法对所有接入用户做统一的安全管控；
- 受限于成本，多数企业无法为每个接入点都单独部署安全硬件设备，即便完成部署，也难以实现统一的运维和监控。

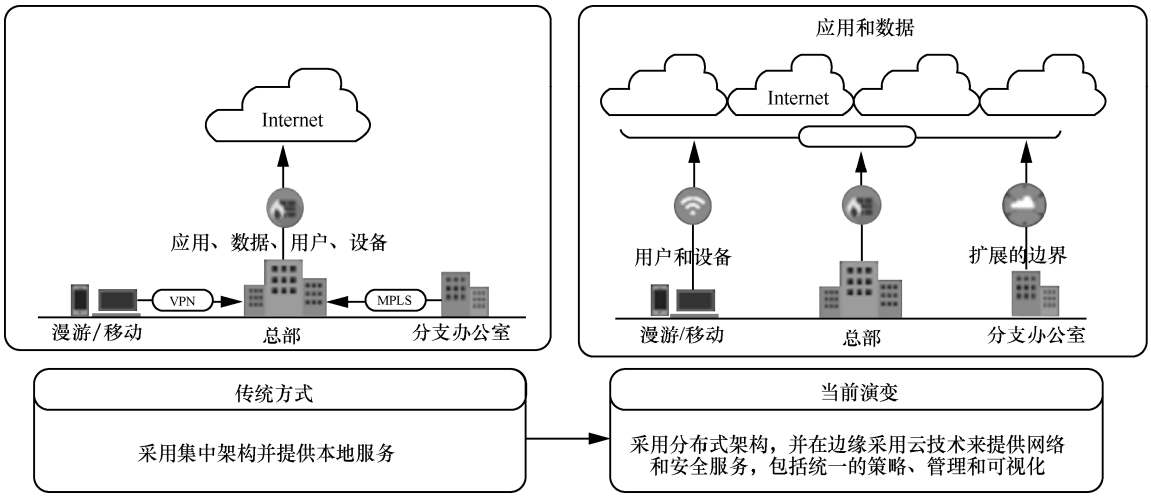


图 1　带边界层的网络转变

“云化”“边缘化”对传统 IT 基础设施的安全带来了全新的挑战，企业原先的边界正在被打破，传统的硬件安全方案已经无法满足企业数字化转型中的防护要求，企业亟须实时、全面、统一管理的安全防护手段。应运而生的 SASE 架构更能适应边缘计算、云服务和混合云等 IT 环境，更快速、更安全地帮助企业完成数字化转型。

2 SASE 云安全架构

2.1 SASE 主要特征

根据 Gartner 的定义，SASE 有如下 4 个主要特征。

（1）身份驱动

不仅仅是 IP 地址，用户和资源身份也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——这些都由与每个网络连接相关联的身份所驱动。采用该方法，公司企业为用户开发一套网络和安全策略，无须考虑设备或地理位置，从而降低运营开销。

（2）云原生架构

SASE 架构利用云的几个主要功能，包括弹性、自适应性、自恢复能力和自维护功能，提供一个可以分摊客户开销以提供最大效率的平台，可方便地适应新兴业务需求，而且随处可用。

（3）支持所有边缘

SASE 为所有公司资源（数据中心、分公司、云资源和移动用户）创建了一个网络。举个例子，SD-WAN 设备支持物理边缘，而移动客户端和无客户端浏览器连接四处游走的用户。

（4）全球分布

为确保所有网络和安全功能随处可用，并向全部边缘交付尽可能好的体验，SASE 云必须全球分布。因此，Gartner 指出，必须扩展自身覆盖面，向企业边缘交付低时延服务。

最终，SASE 架构的目标是要能够更容易地实现安全的云环境。SASE 以一个安全的全球 SD-WAN 服务代替了难以管理的技术大杂烩。

2.2 业界主流观点及架构

数字业务转型颠覆了网络和安全服务的设计模式，将重心转到了用户和设备的身份上，不再聚焦数据中心。SASE 是一项云计算服务，降低了复杂性和成本，旨在向企业整体交付聚合的网络和安全服务。SASE 摆脱了分散集成和地理位置的约束，SASE 分布式安全服务原理如图 2 所示。

SASE 将网络控制置于云端边缘，而不是企业数据中心。与需要单独配置和管理的分层云服务

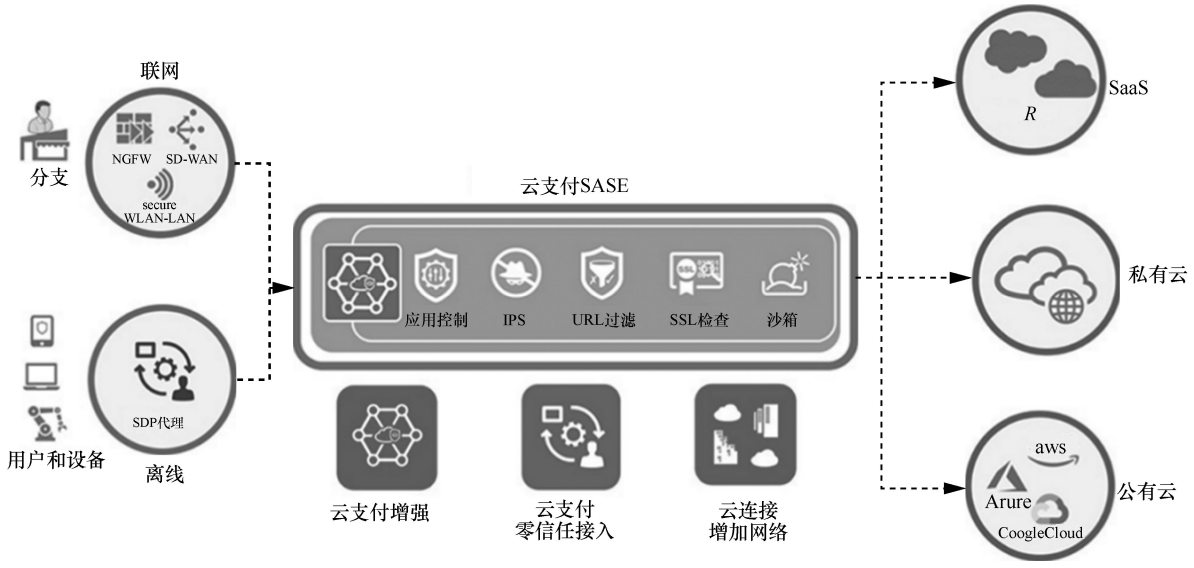


图 2 SASE 分布式安全服务原理

不同，SASE 简化了网络和安全服务，以创建安全、无缝的网络边缘。通过在边缘网络上实施基于身份的零信任访问策略，企业可以将其网络边界扩展到任何远程用户、分支机构、设备或应用程序。这消除了对传统 VPN 和防火墙的需求，并使企业能够更细致地控制其网络安全策略。

2.3　SASE 核心工作原理

SASE 的理念是借助 SD-WAN 搭建的虚拟化架构去集中化，将核心能力附加到边缘进行，以满足当前和未来云上和移动业务的动态需求。SASE 将软件定义广域网（SD-WAN）能力与多种安全功能整合，通过单一云平台进行交付和管理。SASE 产品 5 个核心安全部分和工作原理如下。

（1）安全 Web 网关（secure Web gateway，SWG）

SWG 也称为安全互联网网关，它从 Web 流量中过滤不需要的内容，阻止未经授权的用户行为，并执行公司安全策略，从而防止网络威胁和数据泄露。SWG 可以部署在任何地方，因此是确保远程员工安全的理想选择。

（2）云访问安全代理（cloud access security broker，CASB）

CASB 为云托管服务执行多项安全功能，包括揭示影子 IT（未经授权的公司系统）、通过访问控制和数据丢失防护（DLP）保护机密数据、确保符合数据隐私法规等。

（3）防火墙即服务（firewall-as-a-service，FWaaS）

FWaaS 是指用云端防火墙服务作为交付的防火墙，保护云端平台、基础设施和应用程序免受网络攻击。与传统防火墙不同，FWaaS 不是物理设备，而是一组安全能力，其中包括 URL 过滤、入侵防御以及对所有网络流量的统一策略管理。

（4）零信任网络访问（zero-trust network access，ZTNA）

ZTNA 平台锁定内部资源，不允许公开查看，并要求对每个受保护应用程序的每个用户进行实时验证，以帮助防止潜在的数据泄露。

（5）远程浏览器隔离（remote browser isolation，RBI）

RBI 是让浏览器运行在远程云端的安全沙箱里，和本地终端隔离，这样即使浏览器被感染，恶意软件也无法侵害终端用户的系统。

3　SASE 实践方案

SASE 架构作为业界的主流方向，交换中心也对此进行了探索，并设计了交换中心 SASE 架构，旨在为上云客户提供更安全的环境。本文将从能力架构方案、系统架构方案、安全资源池服务编排方案 3 方面具体阐述 SASE 架构的组成，然后通过对实际的部署方案的阐述说明本架构的优化点、核心能力和价值优势。

3.1　SASE 能力架构方案

核心能力是即插即用可视化、网络优化与安全管控。主要分为两大部分：安全云管理平台和安全资源池。交换中心 SASE 能力架构方案如图 3 所示。

安全云管理平台用于集中管理各类软硬件安全产品，实现云安全服务灵活编排，为云平台和云租户提供灵活、高性能的安全能力。平台能够提供安全服务化、流量编排、策略管理、计量计费、态势呈现等诸多功能，为各类政企用户的云安全保驾护航。

安全云平台与业务云平台松耦合，通过部署独立的安全资源池实现在不改变原有云结构的同时，为平台和租户提供全方面的安全能力。平台除了可通过独立的界面实现安全组件的资源管理、策略管理和资源监控外，还提供统一的计量计费、服务模板、工单流转、运营与运维大屏等诸多内容。

在面向需要高性能的大型场景时，由于租户数量多、服务节点数多，增加软硬混合资源池方

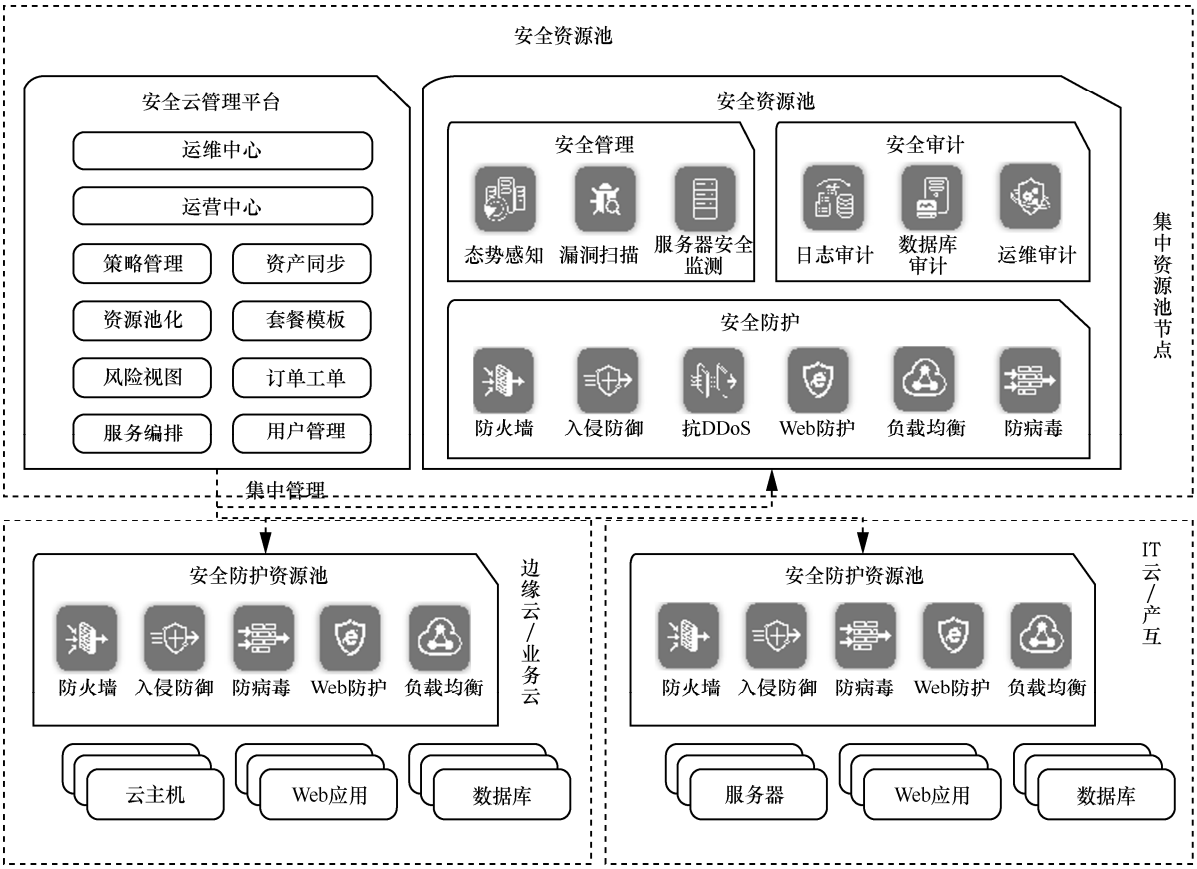


图 3　SASE 能力架构方案

案，即为该场景使用频率较高的安全设施配置专用高性能硬件，其余则通过平台调度。该方案的优势为通过高性能的硬件安全资源与灵活的软件安全资源结合的方式，保障业务的稳定性与高效性。安全能力可以灵活选择，具有全网统一的安全运营与运维视角。

3.2　SASE 系统架构方案

SASE 系统架构方案主要包含三大模块：统一的云安全一体化管理平台、集中化安全能力池和近源端安全能力池。交换中心 SASE 系统架构如图 4 所示。

（1）统一的云安全一体化管理平台

平台可以适用不同场景、不同业务的云用户，为用户提供多场景、个性化安全能力服务；平台可以实现对集中化安全能力池和云网 POP 近源端安全能力池的集中调度管理；平台拥有标准 API 与各安全组件对接，实现安全能力的统一配置、编排和使用。

（2）集中化安全能力池

监测审计类等安全能力集中云化部署，实现资源化、服务化和目录化，按需快速开通调用；向云侧输出可调用的安全能力；安全能力资源共建共享，节约化建设运营。

（3）近源端安全能力池

部分网关类安全能力近源端部署，沉入云内，作为集中安全能力池的延伸，经由安全管理平台统一管理，通过近源网络流量牵引实现安全防护。快速实现云平台内南北向流量的检测防护，保证用户对安全能力的性能需求。

3.3　SASE 安全资源池服务编排方案

对城域流量和云租户访问流量的防护，编排不同的服务方案，对城域流量同步镜像给态势感

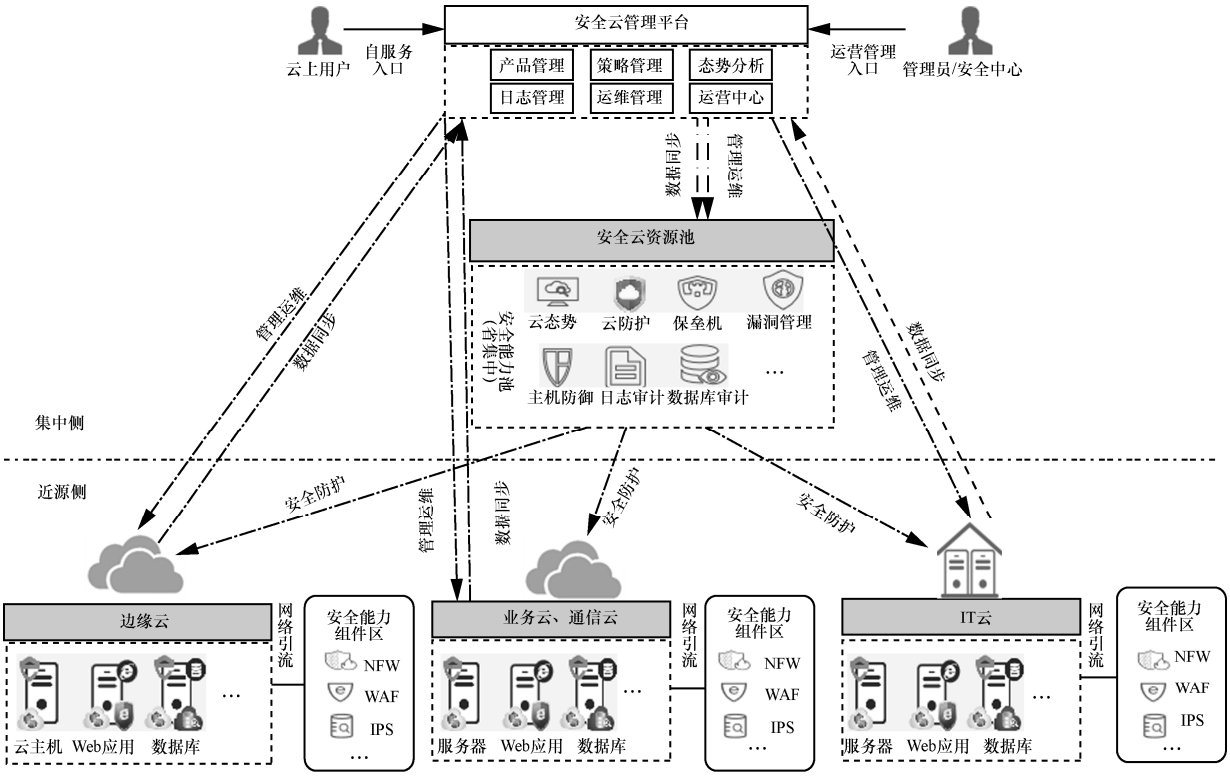


图 4　交换中心 SASE 系统架构

知平台进行威胁检测，交换中心 SASE 安全资源池服务编排方案如图 5 所示。

方案说明如下。

- 安全云管理平台实现对安全产品的纳管，可实现对软硬件资源的拉起、调度、编排、策略管理、计量计费、报表、统一运维、数据运营等功能。
- 防火墙、负载均衡和交换机等硬件设备，采用双机方式部署，提高网络的可靠性。
- 规划单独的安全资源池，虚拟化的安全网元（堡垒机、WAF、数据库审计等）采用虚拟机上线方式接入租户业务网络。
- 安全云管理平台对安全资源池内的网元纳管以及安全业务网元将安全日志发送给态势感知直接走安全网元的管理网通道。

本方案优势如下。

- 通过高性能的硬件安全资源与灵活的软件安全资源结合的方式，保障业务的稳定性与高效性。
- 全网统一的安全运营与运维视角。

3.4　SASE 组网拓扑

接入企业通过边缘网关接入交换中心，由边缘网关部署的安全综合网关提供安全防护，而后接入公有云和边缘云，或经过外墙和抗 DDoS 攻击等防护后接入经互联网接入边缘云。交换中心 SASE 组网拓扑如图 6 所示。

该组网拓扑的优化点如下。

（1）中小企业简化组网

中小企业可以直接接入边缘网关，使用边缘网关的防护能力，也可以使用 SD-WAN 通过互联网接入外墙，一点接入访问各公有云和边缘云节点，大大简化了中小企业的组网结构。

（2）多边缘节点统一安全纳管

由云安全管理中心对全网安全设备进行统一纳管，实现全网能力可视、资源可视、安全状态可视。

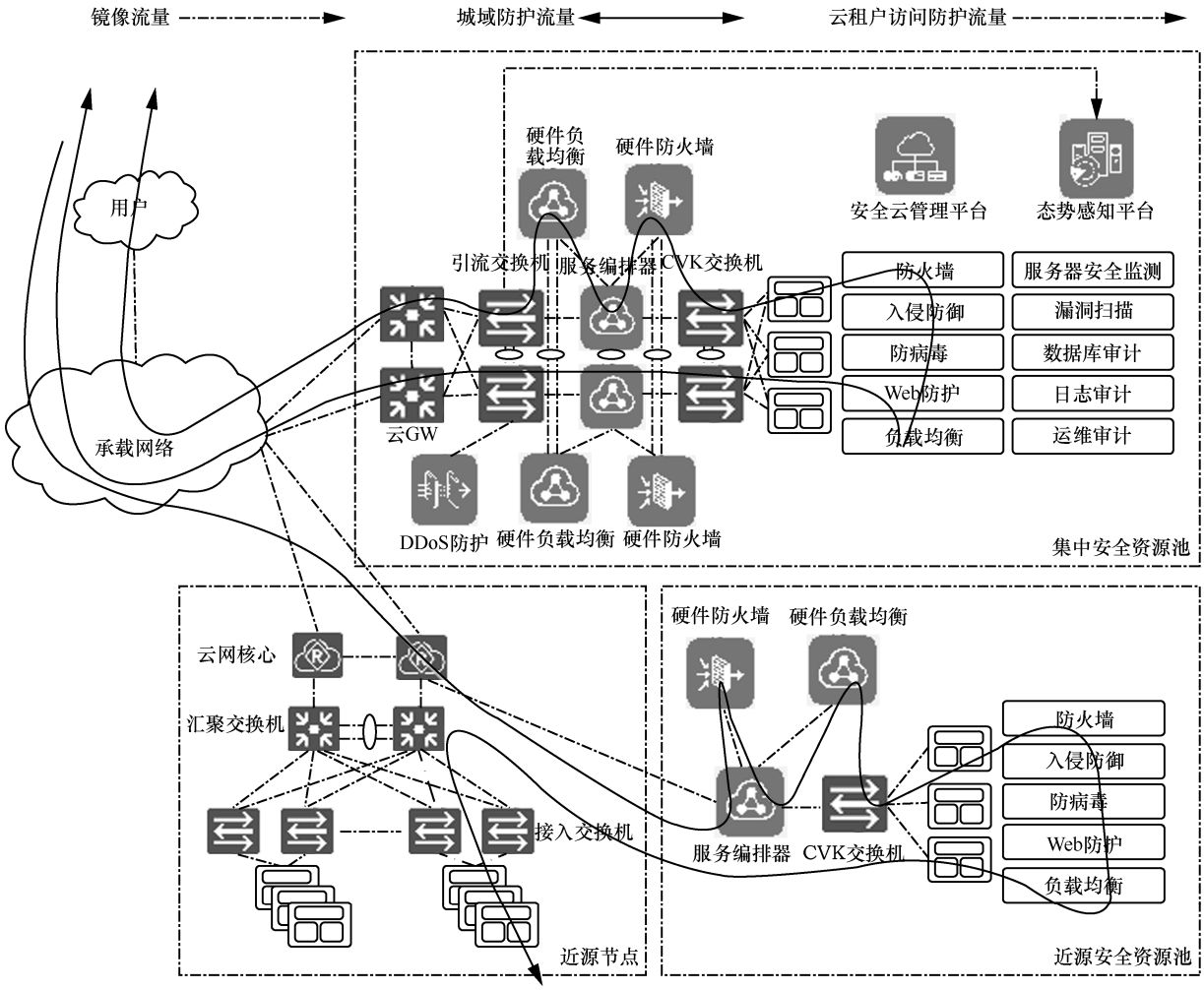


图 5　SASE 安全资源池服务编排方案

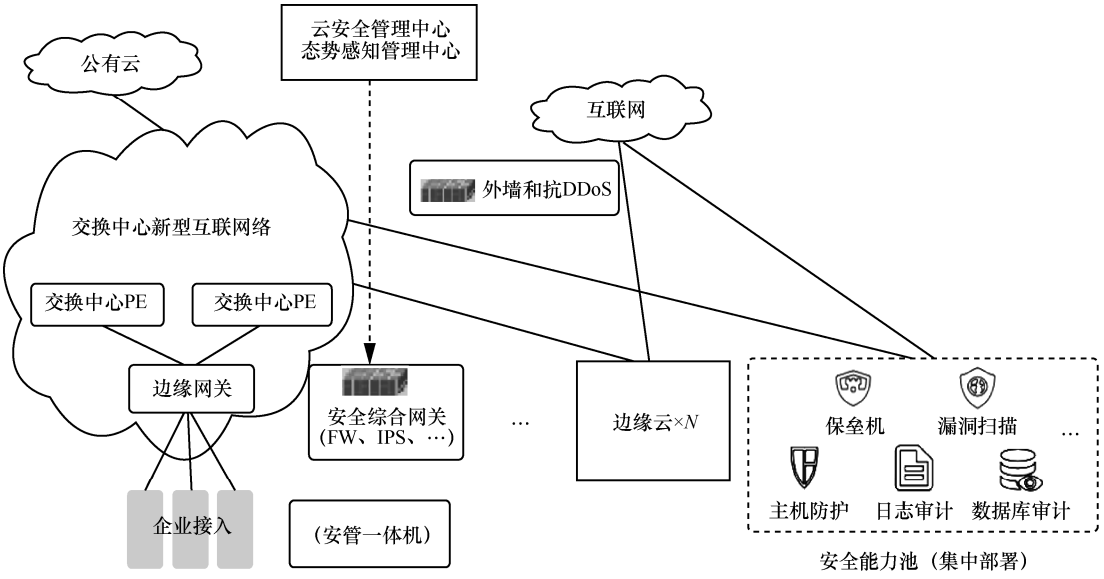


图 6　SASE 组网拓扑

（3）运维审计能力集中上收

在交换中心统一部署安全能力池，实现运维审计各项功能集中管理，实现可管可控。

（4）安全综合网关近源端流量防护

将安全综合网关部署在近源端，就近防护，减少对其他企业的影响。部署方式可以是独立部署方式，也可以是池化部署方式，当采用池化部署方式时，由云安全中心统一为所有客户分配安全能力池资源。

3.5　SASE 核心能力

（1）灵活接入

依托广覆盖的网络资源，为各种分布式用户、场所提供随时随地的灵活接入，并实现性能、可靠性、安全性的精确控制，帮助企业安全地实现数字化转型所需的动态接入和访问能力。

（2）跨地加速

凭借 SD-WAN 的核心优势，通过将网络设备的控制面与数据面分离，实现了网络流量的灵活控制，使网络作为管道更加智能，为企业提供多维度的网络加速能力。

（3）身份驱动

融合零信任安全理念，将身份作为安全策略最重要的上下文因素，通过用户、设备、时间、场地、被访问应用和数据灵敏度等多维度信息，实现针对网络服务质量、路由选择、应用安全风险控制的细粒度落地。

（4）按需安全

将云原生安全能力与网络能力进行全面融合，能够根据用户实际需要，在邻近实体的分布式执行点处，按需提供满足安全监管需求、企业安全策略以及具体业务安全需求的安全能力。

（5）持续运营

以公司集中化安全运营服务能力为依托，为用户提供持续的态势感知、事件监测、威胁分析、情报管理、通报预警、应急处置等服务能力，帮助用户实现安全能力的切实落地和安全事件的高效应对。

3.6　SASE 价值优势

（1）提升用户多场景下网络和安全的性能保障

通过 POP（point of purchase）提供基于时延优化的路由策略，全面支持企业数字化转型、边缘计算和员工移动接入等多场景下的网络和安全需求，实现针对关键、敏感业务的性能和时延保障。

（2）增加用户安全部署灵活度并降低安全建设成本

通过安全云交付的形式，企业的安全扩容需求摆脱传统硬件容量的限制，可以根据需要随时增加新的安全能力。同时，与传统物理架构模式相比，大幅降低了企业安全建设和扩容的成本。

（3）提升用户安全效能并降低安全运营复杂度

企业安全技术人员不用再陷入安全基础设施的常规配置和维护工作中，而可以专注于业务应用的安全需求挖掘和策略规划，有效降低安全运营的复杂度。

4　SASE 能力验证

在图 6 组网拓扑下，企业通过专线或 SD-WAN 接入交换中心新型互联网络，通过 SASE 安全防护后提供至各公有云的访问。交换中心通过实践对新型 SASE 架构的统一管控能力、零信任内网访问管控能力、入侵检测与防御能力、精细化访问控制能力进行了验证，验证结果如下。

（1）统一管控能力验证

主要验证云安全一体化管理平台对全网安全资源池资源的管理能力，交换中心安全云管理平台兼备网络、安全、配置、运维、资产、API 管理等能力，达到预期效果。

（2）零信任内网访问管控能力验证

实现通过自研 HTTPS 加密传输协议，基于动态身份认证，支持端到端（TCP）、端到应用（HTTP/HTTPS）的最小权限访问控制。相较于传统 VPN 访问，访问更快速、运维更高效、部署更便捷、系统安全性更高。

图 7　数据量化安全防护的显示界面

（3）入侵检测与防御能力验证

云防火墙内置了威胁检测引擎，可对互联网上的恶意流量入侵活动和常规攻击行为进行实时阻断和拦截，并提供精准的威胁检测虚拟补丁，智能阻断入侵风险。数据量化安全防护的显示界面如图 7 所示。

（4）精细化访问控制能力验证

实现统一管理互联网到业务的访问控制策略和业务与业务之间的微隔离策略，实现支持全网流量可视和业务间访问关系可视，全面保护企业和用户的网络安全。

但由于现阶段很多企业未能实现智能网关接入，因此未能实现 Internet 就近加密接入以获得更加智能、可靠、安全的上云体验，还需要不断进行探索升级。

5　结束语

交换中心通过部署 SASE 架构，很好地满足了企业上云的安全需求，也满足了企业多分支机构的安全管理、移动办公安全管理、中小企业一体化办公安全管理等场景的需求。在未来的发展中，随着云安全重要性的提升，SASE 架构也会越来越完善，为用户提供更丰富的解决方案，交换中心也需要与时俱进不断探索，不断满足当前和未来上云业务的动态需求。

参考文献：

[1] 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(06): 78-83.
LI C L, MA J C, LIN X. Research and design of SASE model based on SD-WAN[J]. Designing Techniques of Posts and Telecommunications, 2021(6): 78-83.

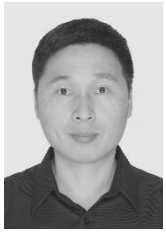
[2] 林世荣, 姜守旭. 软件定义企业级无线网络平台设计与实现[J]. 智能计算机与应用, 2021, 11(02): 210-215.
LIN S R, JIANG S X. Design and implementation of software defined enterprise wireless network platform[J]. Intelligent Computer and Applications, 2021, 11(2): 210-215.

[3] 章岐贵, 黄海, 汪有杰. 基于零信任的软件定义边界安全模型研究[J]. 信息技术与信息化, 2020(11): 92-94.
ZHANG Q G, HUANG H, WANG Y J. Research on software definition boundary security model based on zero trust[J]. Information Technology and Informatization, 2020(11): 92-94.

[4] 康敏. 内生安全 SD-WAN 网络架构与关键设备方案研究[J]. 信息安全与通信保密, 2021, 19(7): 95-104.
KANG M. Research on an endogenous safety SD-WAN network architecture and technical proposal of key equipment[J]. Information Security and Communications Privacy, 2021, 19(7): 95-104.

[5] 网络安全的未来在云端[EB]. 2019.
secure-access-service-edge[EB]. 2019.

[作者简介]



叶朝阳（1976− ），男，浙江省新型互联网交换中心有限责任公司高级工程师、总经理，中国互联网协会互联网互联互通工作委员会副主任委员，主要研究方向为新型互联网交换中心相关的新技术、新业务的开发和推广。

王欣（1973− ），男，浙江省新型互联网交换中心有限责任公司副总经理，主要研究方向为新型互联网交换中心相关的新技术、新业务的开发和推广。

张士聪（1990− ），男，浙江省新型互联网交换中心有限责任公司技术部经理，主要研究方向为新型互联与网络架构。

詹智勇（1985− ），男，浙江省新型互联网交换中心有限责任公司高级工程师，主要研究方向为新型互联网络架构、新型互联网络安全等。

刘伊莎（1992− ），女，浙江省新型互联网交换中心有限责任公司 IT 工程师，主要研究方向为新型互联与网络架构信息化。