Research Gaps and Opportunities for Secure Access Service Edge

Stephanus Petrus van der Walt and Venter Hein
University of Pretoria, South Africa
svdwalt@gmail.com
hventer@cs.up.ac.za

Abstract: This paper provides a contemporary discussion of security as a service from a network perspective and discusses state-of-the-art research conducted within a framework known as Secure Access Service Edge (SASE) (pronounced 'sassy'). SASE is a network security framework proposed by Gartner (2019) (MacDonald, Orans and Skorupa, 2019). This paper gives brief description of cloud concepts and technologies, focuses on network security in the cloud and aims to provide researchers with subjects of future research in SASE. To achieve the aim, the authors evaluate existing papers on SASE and its core components to identify gaps in the literature currently available on SASE.

Keywords: Secure access service edge, secure web gateway, zero trust network access, cloud access broker, digital forensic readiness

1. Introduction

Accessing the Internet is fraught with risk in the form of potential attacks and systems compromise. These risks and threats have forced organisations to make use of their own isolated networks that are typically isolated and protected by a single security stack at head office. With more applications and services having moved to the cloud and users working remotely (a situation that was accelerated by COVID-19), it is becoming impossible to isolate all network traffic. The vulnerability of the cloud became evident in cyberattacks on cloud services (ransomware, data theft, etc.) over the past two years and in the impact it had on organisations. Due to these vulnerabilities, it is imperative to protect all cloud-offered services in the same way that we currently protect our private networks.

The cloud offers virtualised computing, storage and networking resources over the Internet to users in a dynamic way. Owning cloud services is less expensive and much more elastic to scale than local servers. These advantages encourage customers to move their applications and services to the cloud, despite the security risk associated with such services. Traditional network security architectures were designed where the data centre was the crucial point of access for devices and users. With businesses' digital transformation and their adoption of Software as a Service (SaaS) and other cloud services, the traffic flow patterns have changed drastically from almost all traffic internal, i.e., wide area networks (WAN) to most of the traffic Internet-based traffic. With this change, our placement of the network security controls also needs to change to avoid traffic congestion and poor performance from existing security controls. The SASE framework (MacDonald, Orans and Skorupa, 2019) addresses the issue of traffic congestion and poor performance to move security controls to the cloud and delivery network security as a service.

The remainder of this paper is organised as follows: Section 2 provides background on cloud services. Section 3 reviews the SASE current state while research gaps are identified in Section 4. The paper concludes with Section 5.

2. Background

This section presents a background on cloud-computing deployment models, cloud-computing service models, everything as a service and the SASE framework and core components are subsequently explained.

2.1 Cloud Overview

According to (Mell and Grance, 2011) , "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction". In their publication (Mell and Grance, 2011) define cloud computing in terms of four deployment models, i.e. private, community, public and hybrid, and three service models, i.e. Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). These deployment and service models are discussed in more detail in the sections that follow.

2.2 Cloud Deployment Models

A cloud deployment model is described according to where the infrastructure resides and who has control over that infrastructure. A brief description of each follows below:

- A **private cloud** is a cloud infrastructure for restricted use by a single organisation or business.
- A **public cloud** is the most common type of cloud and used when a service provider makes resources, i.e. servers and storage, available to consumers via the Internet.
- A **community cloud** is a joint effort where infrastructure is shared between organisations from a specific community of consumers with the same concerns, e. g. mission, security requirements, policy, and compliance considerations.
- A **hybrid cloud** is a type of cloud infrastructure that results from the combination of two or more distinct cloud infrastructures, i.e., private, community, or public cloud models. A hybrid cloud allows for the flow of data and applications between the different cloud environments.

The next section describes the three cloud services models – Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS).

2.3 Cloud Service Models

Cloud services are described by (Shilpashree, Patil and Parvathi, 2018) and can be classified in three main categories, IaaS, PaaS and SaaS (see Figure 1). Figure 1 shows that server, storage, networking, security, and physical data centre constitute IaaS. IaaS is a subset of PaaS with PaaS adding additional services such as operating systems, development tools and containers. SaaS adds applications to the list of services and is the topmost layer of IaaS and PaaS.

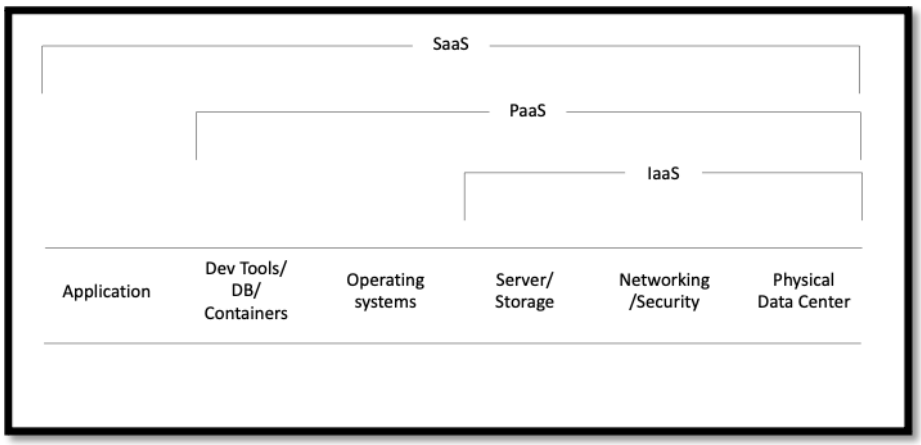

Figure 1: Cloud Services (Stephen Watts, 2019)

- **IaaS** is the first form of cloud computing to provide virtualised resources over the Internet. In an IaaS model, the cloud provider manages the infrastructures such as storage, server and networking resources, while customers must still manage their data, application and operating systems.
- **PaaS** is a cloud computing model that provides an application development environment in the cloud for developers. PaaS is built on top of IaaS and additionally offers services such as middleware, database, containers, etc. for software development. The PaaS customers only manage their applications and data; they are not required to manage the underlying infrastructure or operating system.
- In a **SaaS** cloud computing model, the cloud provider hosts the applications and offers ready-to-use software solutions for businesses. With SaaS, a software vendor may contract a third-party cloud provider to host the application. Larger cloud service providers can also provide all three cloud services.

2.4 Everything as a Service (XaaS)

XaaS is a growing variety of service availability over the Internet via cloud computing, as opposed to on premises. There are countless examples of XaaS, and (Duan, Cao and Sun, 2015) compiled a taxonomy of XaaS. Examples are Storage aaS, Security aaS, Desktop aaS, Database aaS, E-commerce aaS, etc.

This paper focuses on network security aaS and includes firewall as a service (FWaaS), cloud access brokers (CASB), secure web gateways (SWG), zero trust network access (ZTNA) for cloud applications and network as a service (i.e. SD-WAN). A brief description of each is provided below:

- **FWaaS,** also known as cloud firewalls, performs the same functions as a traditional firewall, namely to control traffic sources.
- **CASB** is a cloud-based security policy enforcement point between cloud service consumers and cloud service providers, with the function to block or allow specific applications.
- Cloud **SWG** delivers web security from the cloud to protect web-surfing devices from malware and to enforce corporate compliance.
- **ZTNA** allows only trusted devices access to specific applications and continually authenticates devices and users. A trusted device authentication is not based on IP address, but rather on the identity of the device and the user.
- **SD-WAN** (Software-defined Wide Area Network) is a software-defined approach to the WAN that decouples the network hardware from its control mechanism.

The next section gives an overview of SASE and how the above-mentioned elements for network security as a service are implemented in the SASE framework.

2.5 Secure Access Service Edge (SASE) Overview

One of the most notable frameworks introduced in 2019 was Gartner's cloud network security framework known as SASE. The framework is still in a beginning stage and will probably undergo many changes. (MacDonald, Orans and Skorupa, 2019) gives the following definition of SASE: "The secure access service edge is an emerging offering combining comprehensive WAN capabilities with comprehensive network security functions such as SWG, CASB, FWaaS and ZTNA to support the dynamic secure access needs of digital enterprises." Section 2.5.1 to 2.5.3 discusses why SASE is needed today, SASE's network and security convergence, and a SASE case study.

2.5.1 Why SASE is needed

SASE satisfies the security needs experienced in a highly distributed environment with edge computing, cloud computing, and a workforce that often works from home. Edge computing refers to computing that needs to happen as close as possible to the data to minimise any delays in processing time. Traditionally traffic flows from many different points to a central hub or data centre from where traffic is forwarded to cloud services or elsewhere on the Internet. Experience has shown this design is not efficient, as all traffic is throttled by the central security stack at the data centre. A cloud-native approach – such as using the SASE framework – that does not force traffic through a data centre is then an optimal solution for protecting this new distributed, perimeter-less world.

2.5.2 SASE Network and Security Convergence

With the convergence of network aaS and network security aaS within a SASE deployment. The network services, i.e. SD-WAN, and network security services, i.e. SWG, CASB, ZTNA and FWaaS, are now converged into a single cloud-delivered service model, termed SASE (MacDonald, Orans and Skorupa, 2019). Network and network security teams for support and architectural functions are often different teams in many organisations. For organisations that adopt SASE, there will be a substantial overlap in support and architectural functions between network and security teams. Hence these teams should be collapsed into a single team.

2.5.3 SASE Case Study

Figure 2 shows that a SD-WAN steers all traffic for Internet or cloud services from branch sites towards the SASE security controls. Thus, the SD-WAN also connects the branch offices with the organisation's private data centre. For roaming users not connected to the SD-WAN, the traffic will be steered with an agent on the roaming user device. The SASE cloud comprises its four core components – SWG, CASB, ZTNA and FWaaS – and can identity any malicious traffic from or to branches and roaming users.

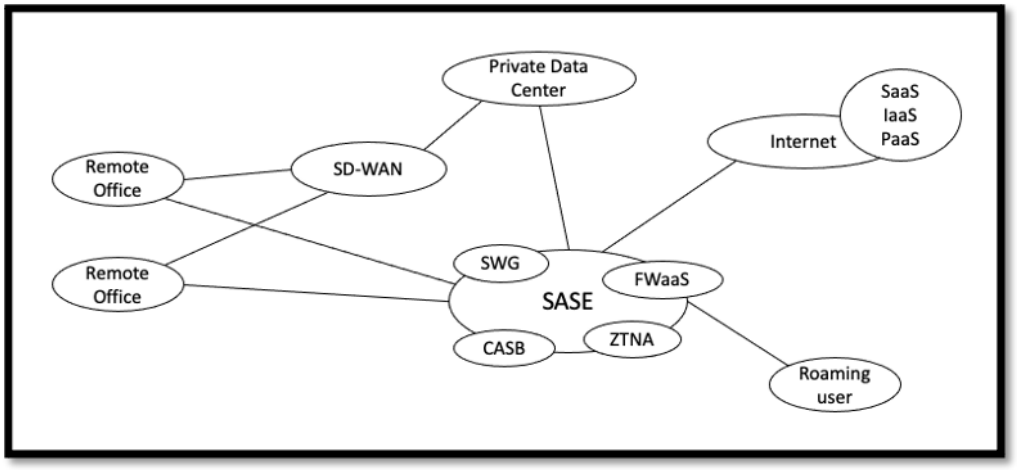

Figure 2: SASE Case study

The next section presents the current state of research with regards to SASE and the five SASE core components.

3. State-of-the-art of SASE

The authors consulted research available on platforms such as the Institute of Electrical and Electronics Engineers (IEEE), Microsoft Academic Research, Google Scholar and the Association for Computing Machinery (ACM) and found only three papers dealing with the topic of SASE. The search was consequently extended to include the SASE core components and numerous papers were found. The SASE core components used to evaluate the state-of-the-art of SASE made use of the SASE framework.

The core components used in the evaluation of SASE state of the artis shown in Table 1. The papers consulted are listed in the left-hand column and an X is entered into the appropriate column to indicate the topic the paper contributes to.

Table 1: Findings

Paper title	**1 SASE**	**2 SD-WAN**	**3 SWG**	**4 CASB**	**5 FWaaS**	**6 ZTNA**	**Ref**
The future of network security is in the cloud	X						(MacDonald, Orans and Skorupa, 2019)
How SASE is defining the future of network security	X						(Wood, 2020)
MEF White Paper MEF SASE Services Framework July 2020	X	X		X			(MEF Forum, 2020)
Software-Defined Wide Area Network (SD-WAN): Architecture, advances and opportunities		X					(Yang *et al.*, 2019)
How to make SD-WAN secure		X					(Wood, 2017)
Development and evaluation of a secure web gateway using existing ICAP open-source tools			X				(Pearce and Hunt, 2010)
SD-WAN revolutionises IoT and edge security		X	X				(Pamplin, 2021)
Firewall as a service in SDN OpenFlow network		X			X		(Arins, 2015)
Application-aware firewall mechanism for software-defined networks		X			X		(Nife and Kotulski, 2020)
Towards a standard SDN-based IPsec management framework		X					(Lopez-Millan, Marin-Lopez and

Paper title	**1 SASE**	**2 SD-WAN**	**3 SWG**	**4 CASB**	**5 FWaaS**	**6 ZTNA**	**Ref**
The future of network security is in the cloud	X						(MacDonald, Orans and Skorupa, 2019)
How SASE is defining the future of network security	X						(Wood, 2020)
MEF White Paper MEF SASE Services Framework July 2020	X	X		X			(MEF Forum, 2020)
Software-Defined Wide Area Network (SD-WAN): Architecture, advances and opportunities		X					(Yang *et al.*, 2019)
How to make SD-WAN secure		X					(Wood, 2017)
Development and evaluation of a secure web gateway using existing ICAP open-source tools			X				(Pearce and Hunt, 2010)
SD-WAN revolutionises IoT and edge security		X	X				(Pamplin, 2021)
Firewall as a service in SDN OpenFlow network		X			X		(Arins, 2015)
							Pereniguez-Garcia, 2019)
A firewall-adversarial testing approach for software-defined networks					X		(Malkawi *et al.*, 2021)
Enhancing features of cloud computing using cloud access security brokers to avoid data breaches				X			(Kaur and Gupta, 2019)
Cloud Access Security Broker (CASB): A pattern for secure access to cloud services				X			(Fernandez, Yoshioka and Washizaki, 2015)
CPFirewall: A novel parallel firewall scheme for FWaaS in the cloud environment					X		(Wang *et al.*, 2015)
Implementation of firewall as a Service for OpenStack Virtualization Systems					X		(Hoang and Bui, 2021)
Relevance of Zero Trust Network Architecture and its rapid adoption amidst Work From Home enforced by COVID-19						X	(D. A. Deshpande, 2021)
Cloud Access Security Brokers (CASBs)				X			(Gartner Inc., 2016)
Enhancing security of cloud platform with Cloud Access Security Broker				X			(Ahmad, Mehfuz and Beg, 2021)
Dynamic Cloud Access Security Broker using Artificial Intelligence				X			(Bhattacharya *et al.*, 2021)
A Study on rapid adoption of Zero Trust Network Architectures by global organizations due to COVID-19 Pandemic						X	(A. Deshpande, 2021)
Beyond Zero Trust: Trust is a vulnerability						X	(Campbell, 2020)
Survivable zero trust for cloud computing environments						X	(Ferretti *et al.*, 2021)
The top three factors driving zero trust adoption						X	(Embrey, 2020)
Never trust, always verify: A multivocal literature review on current knowledge and research gaps of zero trust						X	(Buck *et al.*, 2021a)

Paper title	1 SASE	2 SD-WAN	3 SWG	4 CASB	5 FWaaS	6 ZTNA	Ref
The future of network security is in the cloud	X						(MacDonald, Orans and Skorupa, 2019)
How SASE is defining the future of network security	X						(Wood, 2020)
MEF White Paper MEF SASE Services Framework July 2020	X	X		X			(MEF Forum, 2020)
Software-Defined Wide Area Network (SD-WAN): Architecture, advances and opportunities		X					(Yang *et al.*, 2019)
How to make SD-WAN secure		X					(Wood, 2017)
Development and evaluation of a secure web gateway using existing ICAP open-source tools			X				(Pearce and Hunt, 2010)
SD-WAN revolutionises IoT and edge security		X	X				(Pamplin, 2021)
Firewall as a service in SDN OpenFlow network		X			X		(Arins, 2015)
Survey on Zero-Trust Network Security						X	(Yan and Wang, 2020)
A Zero Trust Approach to Network Security						X	(Assunção, 2019)
Latest trend in network security as Zero Trust Security Model						X	(Uttarwar and Kalia, 2019)
Zero Trust Architecture, SP 800-207						X	(NIST, 2020)

The criteria used to evaluate the papers are based on the research relevance to SASE, the number of papers in the mentioned field and gaps in the current SASE research. The next sections briefly discuss the current state of literature of the different topics and its evaluation on each of the components numbered from 1 to 6 in Table 1.

3.1 Secure Access Service Edge (SASE)

Very few contributions were found to be available on the topic of SASE in general, because it is still a very new framework (MacDonald, Orans and Skorupa, 2019). The MEF (originally known as the Metro Ethernet Forum and later re-branded to simply MEF) White Paper (MEF Forum, 2020) defines the MEF SASE Services Framework, which can be used for the implementation of SASE. It provides a way for enterprises and service providers to compare each vendor's approach towards SASE. (Wood, 2020), describes SASE from a SASE provider's point of view and the benefits of SASE.

3.2 Software-defined wide area network (SD-WAN)

A search for SD-WAN returned an extensive list of contributions. A search for "SD-WAN" and "security" on the resulted in fewer returns but is more relevant to this paper and future research on SASE. (Lopez-Millan, Marin-Lopez and Pereniguez-Garcia, 2019) proposes a solution to manage IPsec Security Associations (IPsec SAs) used for encrypting SD-WAN tunnels. The solution by (Lopez-Millan, Marin-Lopez and Pereniguez-Garcia, 2019) can be expanded for SASE framework standardisation (discussed later in Section 4.4).

3.3 Secure Web Gateway (SWG)

The next component is SWG and, again, very little research has been published on this topic. There are also few instances where SWG and SASE are mentioned in the same article. The topic of SWG nevertheless shows many research opportunities within the context of SASE.

3.4 Cloud Access Security Broker (CASB)

The search for "cloud access security broker" returned significant results and the mentioned papers covered a vast diversity of topics. (D Curwin *et al.*, 2021) deal with what a CASB is, while (Obregon, 2017) suggests an approach to use CASB to secure SaaS.

3.5 Firewall as a service (FWaaS)

In the available literature, the authors found only six papers in their search for "FWaaS". (Hoang and Bui, 2021) proposes the implementation of a firewalling service for cloud systems using OpenStack. (Wei *et al.*, 2016) in turn propose a solution to hide sensitive network policies such as firewall rules from cloud security providers, as they may be leaked and exploited by attackers. The feasibility of implementing the above solution to all SASE components can be investigated.

3.6 Zero trust network access (ZTNA)

Significant research was done in the field of ZTNA over the past two years because the global COVID-19 pandemic and worldwide lockdowns have forced people to work from home. (Wei *et al.*, 2016) confirm the rapid adoption of ZTNA by many organisations due to COVID-19. Legacy hardware VPNs that were designed when a small portion of users were working from home, could not be scaled up for a larger percentage of employees working from home. The ZTNA solution therefore created multiple on-demand micro connections between users' devices and cloud applications, in order to overcome the scalability issues. (Buck *et al.*, 2021) discuss the flaws of current network security solutions and maintain that the zero-trust model follows the idea that no network – internal or external – can be trusted.

3.7 Summary of current literature

Table 2 gives a summary of the papers identified in SASE state-of-the-art research. The relevance of these papers to SASE (in the authors' opinion) is indicated in the second column on a scale from 1 to 5 – where 1 means the least significant and 5 means the most significant relevance to SASE. The core components were then sorted from high to low according to their relevance to SASE.

The authors argue that a relevance of 5 is allocated to SASE because these papers focus entirely on Gartner's SASE framework. The authors allocate a 1 to SD-WAN since SD-WAN, in the context of SASE, is only used to steer traffic to a SASE cloud from branch offices. It, therefore, does not have a significant impact on the organisation of SASE. The role of SWG is to steer traffic to a SASE cloud, and then to monitor and inspect traffic before it is routed to the appropriate cloud service. Since the SWG in a SASE deployment performs several functions, i.e. content filtering, decryption of traffic, data loss prevention for cloud application, and enriches metadata context for investigations, SWG was allocated a 4 out of 5 for the role of SWG in SASE. FWaaS was allocated a 2 since the FWaaS SASE component performs the same role as an on-premises firewall, but with all the benefits of an IaaS offering. ZTNA creates the boundaries to allow only trusted users and devices to access applications. In a SASE deployment, ZTNA becomes a policy enforcement point via a trust broker between users and devices and applications. The trust broker removes applications from public visibility and reduces the attack surface, therefore ZTNA was allocated a 4 out of 5. CASB was rated a 3 because CASB enforces a policy enforcement point between applications and users for security and compliance purposes. Examples of policy enforcements include authentication, authorisation, logging, device profiling and malware detection.

Table 2: Summary of papers

SASE components evaluated	Relevance to SASE 1 - 5	Number of papers
SASE	5	3
ZTNA	4	10
SWG	4	2
CASB	3	6
FWaaS	2	5
SD-WAN	1	7

4. Potential research gaps in SASE

As stated before, the SASE framework converge network and network security aaS. Section 4.1 to 4.4 identifies and discusses gaps in the current research. Section 4.5 summarises the gaps and provides a high-level solution.

4.1 Using SASE as a Managed Detection and Response (MDR) Service for MSSPs

Research is needed to demonstrate how managed security service providers (MSSPs) can use SASE for a managed detection and response (MDR) service. Many large organisations manage their own network and security infrastructure and do not make use of MSSPs; also demonstrated a SASE deployment from an organisational view. In addition to the MDR service, MSSPs also offer Security Operations Centre as a Service (SOCaaS). Due to the convergence of network and security support teams in a SASE environment, the monitoring

of SASE infrastructure makes a convincing case for a combined SOC and NOC. (Miloslavskaya, 2018) describes the advantages of a Network Security Intelligence Centre (NSIC) which is a combination of a Security Intelligence Centre (SIC) and a Network Operations Centre (NOC).

The section that follows discusses the second shortcoming, namely the collection of security events and the transfer of events to a SIEM tool used in a SOC.

4.2 SIEM Integration into SASE via APIs and not Traditional Syslog

Security events are generated by SASE components and maybe a SIEM tool is not needed. Gartner's SASE framework does not address the subject of a security operations centre (SOC) for the monitoring of SASE components. Gartner does however mention application programming interface (API) inspection as a critical capability for a SASE vendor. (MacDonald, Orans and Skorupa, 2019) This implies that some form of monitoring and response capability is needed.

Security events generated by SASE components traditionally send a syslog message to a security information and event management (SIEM) tool via a transport protocol such as syslog or XML. This means that the SASE components forwards the events to a SIEM tool. As an alternative, events can be triggered with an API integration from a SIEM tool to the SASE components and this means that the SIEM tools pulls or fetches the events – as opposed to pushing them. The event logs of Security as a Service (SECaaS) solution are stored with the SECaaS solution provided by the service provider for a short period of time. For long-term event storage, the service provider could store the event data in cloud storage like an Amazon S3 bucket. The benefit of using an API integration as the data source for a SIEM tool is that the number of logs is significantly reduced. Furthermore, the quality of data received by the SIEM tool is improved. Section 4.3 address how to enable digital forensic readiness in the SASE core components.

4.3 Digital Forensic Readiness (DFR) with SASE

Digital forensic readiness (DFR) is still an evolving field but extremely important for saving time and cost in digital forensic investigation. According to (Tan, 2001), digital forensic readiness has two objectives: maximising an environment's ability to collect credible digital evidence and minimising the cost of forensics in an incident response. To recognise the benefits of DFR, more research is needed to construct a framework to ensure all SASE core components are DFR according to ISO/IEC 27043:2015 (Valjarevic, Venter and Petrovic, 2017).

Research done by (Lagrasse *et al.*, 2020) for a framework on DFR in software-defined networks can be applied to be SD-WAN traffic routed towards a SASE cloud. Take into consideration that all SD-WAN tunnel traffic is encrypted with IPsec encryption protocol and as a result all Potential Digital Evidence (PDE) needs to be collected at the edge or hub SD-WAN router. Furthermore, the potential digital evidence collected from the SASE components must be forensically sound and have the potential to withstand legal scrutiny and meet evidence admissibility requirements in a court of law. The DFR framework described by (Lagrasse *et al.*, 2020) uses natural language processing (NLP) to discover and identify cybercrime incidents in the cloud. This technique to use NLP can also be used for a DFR Framework for SASE core components. Section 4.4 discusses the alignment of the SASE framework to existing cloud security standards and frameworks.

4.4 Standardisation of the SASE framework

In our opinion, the Gartner paper on SASE establishes a capability framework that recommends certain functionalities i.e., CASB, FWaaS, ZTNA, SWG and SD-WAN. In our experience multiple vendors build SASE solutions around their existing product capabilities and not according to a standard. Using a standard together with a framework has the following benefits; a common language, a common understanding of requirements, facilitating product integration, enabling regional and international functionality and integration, common technical requirements and cost projections.

To realise the benefits of using standards and tested frameworks, our future research would build on the existing Gartner SASE capability framework by aligning it to existing cloud security standards and frameworks. The next section presents a summary of the gaps discussed and provides a high-level solution to each shortcoming in a table format.

4.5 Summary of research gaps

Table 3 summarises the potential research challenges and suggests a high-level solution to the potential research gaps as identified in Sections 4.1 to 4.4. These solutions should be explored in future research.

Table 3: Summary of research gaps

Potential research gap	Brief description of gap	High-level solution
Using SASE as a MDR service for MSSPs	All SASE components are offered from management service providers (MSPs) and management security service providers (MSSPs). The SASE SD-WAN component has been monitored from a NOC and the other components from a SOC, and the drawback is that they do this disjointly.	Demonstrate how SASE detection and response can be used by MSSPs and how to monitor the SASE core components from a NSIC (i.e. the combination of a SOC and a NOC)
SIEM integration into SASE via APIs and not via traditional syslog	The Gartner SASE framework does not address the subject of a SOC for monitoring SASE.	Use the API capabilities available in SIEM tools to collect security events from the SASE core components (which are also presented through APIs). An API call is sent to an external application to retrieve requested data, i.e. relevant security events, in the SASE components. The benefit of using APIs is that the number of logs is significantly reduced and the quality of data received is improved.
DFR in SASE	Since all SASE components are delivered from the cloud not afll of these components are digital forensically ready.	Develop a DFR framework for all SASE core components in order to improve on existing standards.
SASE Framework	In the opinion of the authors, the Gartner SASE framework is already used by multiple vendors and customers; however, it is not aligned to existing standards. This means the SASE framework requires more rigorous testing.	The benefits of using a standard or framework involve the use of a common language; a common understanding of requirements; product integration; regional and international functionality and integration; adherence to common technical requirements; and the facilitation of cost projections. Future research should build on the Gartner SASE capability frameworks and align them to existing cloud security standards and frameworks.

5. Conclusion

The aim of this paper was to establish the present state of development of SASE and to discuss future research opportunities for SASE. An overview was given of cloud services and the different cloud deployment models and cloud service models were discussed. The paper also discussed XaaS (everything as a service) with a focus on network security as a service, i.e. FWaaS, CASB, SWG, ZTNA and SD-WAN, and gave a brief description of each. An overview of the Gartner SASE framework was provided, coupled with a motivation of why SASE is needed today. The convergence of network and network security as a service within in a SASE deployment was discussed and explored in a case study with the SASE framework. This paper then reviewed and evaluated current literature contributions made to SASE and its core components. Our study showed that only scant research literature is currently available on SASE. Therefore, the criteria for reviewed and evaluated literature to be included in the paper were expanded to encompass all the SASE core components.

The paper proceeded to identify four gaps in SASE research. Firstly, the SASE components are monitored disjointly by a NOC and SOC. Secondly, the Gartner SASE framework does not address the matter of a SOC for monitoring of the SASE core components. Thirdly, not all the SASE components are digital forensically ready. Lastly, the SASE framework is not aligned to existing frameworks and standards. Finally, the paper suggested four potential future research endeavours in SASE to address the shortcomings mentioned above. The first topic for future research involved the use of SASE as a managed detection and response (MDR) service for MSSPs. Secondly, SIEM integration into SASE should be done via APIs, and not via traditional logging. Thirdly, digital forensic readiness (DFR) should be incorporated into SASE, and lastly, the SASE framework should be standardised.

References

Ahmad, S., Mehfuz, S. and Beg, J. (2021) 'Enhancing Security of Cloud Platform with Cloud Access Security Broker', in *Lecture Notes in Networks and Systems*. doi: 10.1007/978-981-16-0882-7_27.

Arins, A. (2015) 'Firewall as a service in SDN OpenFlow network', in *Advances in Information, Electronic and Electrical Engineering, AIEEE 2015 - Proceedings of the 2015 IEEE 3rd Workshop*. doi: 10.1109/AIEEE.2015.7367309.

Assunção, P. (2019) 'A Zero Trust Approach to Network Security', *Proceedings of the Digital Privacy and Security Conference*.

Bhattacharya, D. *et al.* (2021) 'Dynamic Cloud Access Security Broker Using Artificial Intelligence', in *Lecture Notes in Networks and Systems*. doi: 10.1007/978-981-15-7106-0_33.

Buck, C. *et al.* (2021a) 'Never trust, always verify: A multivocal literature review on current knowledge and research gaps of zero-trust', *Computers & Security*, 110, p. 102436. doi: 10.1016/J.COSE.2021.102436.

Buck, C. *et al.* (2021b) 'Never trust, always verify: A multivocal literature review on current knowledge and research gaps of zero-trust', *Computers & Security*, 110. doi: 10.1016/j.cose.2021.102436.

Campbell, M. (2020) 'Beyond Zero Trust: Trust Is a Vulnerability', *Computer*, 53(10). doi: 10.1109/MC.2020.3011081.

D Curwin *et al.* (2021) *What is Cloud App Security? | Microsoft Docs*, *Microsoft*. Available at: https://docs.microsoft.com/en-us/cloud-app-security/what-is-cloud-app-security.

Deshpande, A. (2021) 'A Study on Rapid Adoption of Zero Trust Network Architectures by Global Organizations Due to COVID-19 Pandemic', in *New Visions in Science and Technology Vol. 1*. doi: 10.9734/bpi/nvst/v1/3640f.

Deshpande, D. A. (2021) 'Relevance of Zero Trust Network Architecture amidts and it's rapid adoption amidts Work From Home enforced by COVID-19', *Psychology and Education Journal*, 58(1). doi: 10.17762/pae.v58i1.2190.

Duan, Y., Cao, Y. and Sun, X. (2015) 'Various "aaS" of everything as a service', in *2015 IEEE/ACIS 16th International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing, SNPD 2015 - Proceedings*. doi: 10.1109/SNPD.2015.7176215.

Embrey, B. (2020) 'The top three factors driving zero trust adoption', *Computer Fraud and Security*, 2020(9). doi: 10.1016/S1361-3723(20)30097-X.

Fernandez, E. B., Yoshioka, N. and Washizaki, H. (2015) 'Cloud Access Security Broker (CASB): A pattern for secure access to cloud services', *4th Asian Conference on Pattern Languages of Programs*.

Ferretti, L. *et al.* (2021) 'Survivable zero trust for cloud computing environments', *Computers and Security*, 110. doi: 10.1016/j.cose.2021.102419.

Gartner Inc. (2016) *Cloud Access Security Brokers (CASBs)*, *Peer Insights*.

Hoang, X. T. and Bui, N. D. (2021) 'An Implementation of Firewall as a Service for OpenStack Virtualization Systems', in *Lecture Notes in Networks and Systems*. doi: 10.1007/978-981-16-2094-2_12.

Kaur, S. and Gupta, R. (2019) 'Enhancing Features of Cloud Computing Using Cloud Access Security Brokers to Avoid Data Breaches', *European Journal of Engineering Research and Science*, 4(10). doi: 10.24018/ejers.2019.4.10.1518.

Lagrasse, M. *et al.* (2020) 'Digital forensic readiness framework for software-defined networks using a trigger-based collection mechanism', in *Proceedings of the 15th International Conference on Cyber Warfare and Security, ICCWS 2020*. doi: 10.34190/ICCWS.20.045.

Lopez-Millan, G., Marin-Lopez, R. and Pereniguez-Garcia, F. (2019) 'Towards a standard SDN-based IPsec management framework', *Computer Standards and Interfaces*, 66. doi: 10.1016/j.csi.2019.103357.

MacDonald, N., Orans, L. and Skorupa, J. (2019) 'The Future of Network Security Is in the Cloud', *Gartner*, (August).

Malkawi, R. *et al.* (2021) 'A firewall-adversarial testing approach for software defined networks', *Journal of Theoretical and Applied Information Technology*, 99(1).

MEF Forum (2020) 'MEF White Paper MEF SASE Services Framework July 2020'.

Mell, P. and Grance, T. (2011) 'The NIST definition of cloud computing', *Nova Science Publishers, Inc., (2011), 171-173*, pp. 171–173.

Miloslavskaya, N. (2018) 'Network Security Intelligence Center as a combination of SIC and NOC', in *Procedia Computer Science*. doi: 10.1016/j.procs.2018.11.084.

Nife, F. N. and Kotulski, Z. (2020) 'Application-Aware Firewall Mechanism for Software Defined Networks', *Journal of Network and Systems Management*, 28(3). doi: 10.1007/s10922-020-09518-z.

NIST (2020) 'Zero Trust Architecture, SP 800-207', *National Institute of Standards and Technology Special Publication*, SP 800-207.

Obregon, L. (2017) *A technical approach at securing SaaS using Cloud Access Security Brokers*, *SANS*.

Pamplin, S. (2021) 'SD-WAN revolutionises IoT and edge security', *Network Security*, 2021(8). doi: 10.1016/s1353-4858(21)00090-8.

Pearce, M. and Hunt, R. (2010) 'Development and evaluation of a secure web gateway using existing ICAP open source tools', in *Proceedings of the 8th Australian Information Security Management Conference*.

Shilpashree, S., Patil, R. R. and Parvathi, C. (2018) 'Cloud computing an overview', *International Journal of Engineering and Technology(UAE)*, 7(4). doi: 10.14419/ijet.v7i4.10904.

Stephen Watts, M. R. (2019) *SaaS vs PaaS vs IaaS: What's The Difference & How To Choose – BMC Software | Blogs*. Available at: https://www.bmc.com/blogs/saas-vs-paas-vs-iaas-whats-the-difference-and-how-to-choose/ (Accessed: 16 September 2021).

Tan, J. (2001) 'Forensic Readiness Assessment', *Cambridge, MA:@ Stake*.

Uttarwar, V. U. and Kalia, A. A. (2019) 'Latest Trend in Network Security as Zero Trust Security Model', *National Journal of Computer and Applied Science*, 2.

Valjarevic, A., Venter, H. and Petrovic, R. (2017) 'ISO/IEC 27043:2015 - Role and application', in *24th Telecommunications Forum, TELFOR 2016*. doi: 10.1109/TELFOR.2016.7818718.

Wang, Z. *et al.* (2015) 'CPFirewall: A novel parallel firewall scheme for fwaas in the cloud environment', in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. doi: 10.1007/978-3-319-26979-5_9.

Wei, L. *et al.* (2016) 'A firewall of two clouds: Preserving outsourced firewall policy confidentiality with heterogeneity', in *2016 IEEE Global Communications Conference, GLOBECOM 2016 - Proceedings*. doi: 10.1109/GLOCOM.2016.7841497.

Wood, M. (2017) 'How to make SD-WAN secure', *Network Security*, 2017(1), pp. 12–14. doi: 10.1016/S1353-4858(17)30006-5.

Wood, M. (2020) 'How SASE is defining the future of network security', *Network Security*, 2020(12), pp. 6–8. doi: 10.1016/S1353-4858(20)30139-2.

Yan, X. and Wang, H. (2020) 'Survey on Zero-Trust Network Security', in *Communications in Computer and Information Science*. doi: 10.1007/978-981-15-8083-3_5.

Yang, Z. *et al.* (2019) 'Software-defined wide area network (SD-WAN): architecture, advances and opportunities', in *Proceedings - International Conference on Computer Communications and Networks, ICCCN*. doi: 10.1109/ICCCN.2019.8847124.