Journal of Network and Information Security
11 (1) 2023, 28-33
http://www.publishingindia.com/jnis

The Future of Networking is Here: SASE for a Stronger, More Secure Network

Ravi Tanguturi[1*] and Saraswati Bhimini[2]
[1]Cloud Security Architect at Lookout Inc., Certificate of Cloud Security Knowledge (CCSK),
Bachelor of Technology in Computer Science, Jawahar Lal Nehru Technological University, Hyderabad, India.
Email: tanguturi@hotmail.com
[2]Cloud Application Engineer, Massachusetts Institute of Technology, Cloud & DevOps – Continuous Transformation,
Bachelor of Technology in Computer Science, Jawahar Lal Nehru Technological University, Hyderabad, India.
Email: bhimini@hotmail.com

Abstract: The world of networking is rapidly evolving and the traditional approach to network security and performance is no longer sufficient for the demands of modern businesses. The introduction of Software-Defined Wide Area Networking (SD-WAN) has paved the way for a new era of networking solutions and SASE (Secure Access Service Edge) is at the forefront of this revolution. This paper explores the need for a better security approach for future. Concept of SASE and its potential to transform the way organizations approach network security and performance, by integrating both security and networking functions into a single solution. SASE promises to deliver stronger and more secure networks, while also reducing complexity and streamlining operations. This paper also provides an overview of SASE technology and its benefits and outlines the key considerations for organizations looking to adopt SASE as part of their digital transformation journey. The future of networking is here, and SASE is leading the way.

Keywords: CASB, Cloud security, Network security, NGFWs, Posture management, SASE, SD-WAN, SWG, ZTNA.

I. Background of the Study

The increasing complexity and sophistication of cyber threats have put pressure on organizations to re-evaluate their approach to network security. At the same time, the rise of cloud computing and remote work has created a need for more flexible and scalable networking solutions. The traditional approach to network security, which involves disparate solutions for firewall, VPN, and network optimization, has become increasingly cumbersome and inadequate.

This has led to the emergence of Software-Defined Wide Area Networking (SD-WAN), which has transformed the way organizations approach networking. SD-WAN has made it possible to centralize network management and optimize traffic routing, while also reducing complexity and cost. However, the integration of security functions has remained a challenge, leading to the introduction of a new concept in networking – SASE (Secure Access Service Edge).

SASE represents a paradigm shift in networking, as it integrates both security and networking functions into a single solution. This convergence of security and networking provides a more secure and efficient network, while also reducing complexity and streamlining operations. SASE is rapidly gaining traction in the market, with industry experts forecasting that the SASE market will grow rapidly over the next few years.

Given the growing importance of SASE in the world of networking, this study aims to provide an overview of SASE technology and its benefits and outline the key considerations for organizations looking to adopt SASE as part of their digital transformation journey. The objective of this study is to provide a comprehensive understanding of SASE and its potential to revolutionize the way organizations approach network security and performance.

II. Literature Review

Several studies have been conducted on the SASE adoption, architecture, illustration of SASE, including definition, key characteristics, reported benefits and challenges across the world. Some of them are referenced below:

Mohammed Nurul Islam; Ricardo Colomo-Palacios; Sabarathinam Chockalingam - Secure Access Service Edge: A Multivocal Literature Review [8].

Michael Wood - How SASE is defining the future of network security [9].

Aniket Deshpande - A Study on Rapid Adoption of Zero Trust Network Architectures by Global Organizations Due to COVID-19 Pandemic [10].

Neil MacDonald, Lawrence Orans, Joe Skorupa - The Future of Network Security is in the Cloud [11].

III. Significance of the Study

The significance of this study lies in its contribution to the growing body of literature on SASE and its potential to revolutionize the way organizations approach network security and performance. This study provides a comprehensive overview of SASE technology, its benefits, and the key considerations for organizations looking to adopt SASE. By exploring the concept of SASE and its potential impact on the world of networking, this study serves as a valuable resource for organizations looking to stay ahead of the curve in a rapidly evolving digital landscape.

Moreover, this study highlights the importance of SASE in addressing the growing challenges facing organizations in terms of network security and performance. The integration of security and networking functions into a single solution offers a more secure and efficient network, while also reducing complexity and streamlining operations. This study provides insights into the potential of SASE to transform the way organizations approach network security and offers a roadmap for organizations looking to adopt SASE as part of their digital transformation journey.

In conclusion, the significance of this study lies in its contribution to the understanding of SASE and its potential to revolutionize the way organizations approach network security and performance. By providing a comprehensive overview of SASE technology and its benefits, this study serves as a valuable resource for organizations looking to stay ahead of the curve in a rapidly evolving digital landscape.

IV. Statement of the Problem

The increasing sophistication of cyber threats and the rapid adoption of cloud computing and remote work have put pressure on organizations to re-evaluate their approach to network security. The traditional approach to network security, which involves disparate solutions for firewall, VPN, and network optimization, has become increasingly cumbersome and inadequate. This has resulted in a growing need for more flexible and scalable networking solutions that can address the growing challenges facing organizations in terms of network security and performance.

However, the integration of security functions into networking solutions has remained a challenge, leading to a fragmented approach to network security that is neither secure nor efficient. This has created a gap in the market for a solution that can integrate both security and networking functions into a single solution. This gap is the statement of the problem addressed in this study.

Considering these challenges, the objective of this study is to provide a comprehensive understanding of SASE (Secure Access Service Edge) technology and its potential to revolutionize the way organizations approach network security and performance. The study aims to address the following questions:

- What is SASE technology and how does it differ from traditional approaches to network security?
- What are the benefits of SASE technology and how does it address the challenges facing organizations in terms of network security and performance?
- What are the key considerations for organizations looking to adopt SASE as part of their digital transformation journey?

The significance of this study lies in its contribution to the understanding of SASE and its potential to revolutionize the way organizations approach network security and performance. By providing a comprehensive overview of SASE technology and its benefits, this study serves as a valuable resource for organizations looking to stay ahead of the curve in a rapidly evolving digital landscape.

V. Purpose of the Study

The purpose of this study is to provide a comprehensive understanding of SASE (Secure Access Service Edge) technology and its potential to revolutionize the way organizations approach network security and performance.

The study aims to provide a comprehensive understanding of SASE technology and its potential to address the growing challenges facing organizations in terms of network security and performance. By exploring the concept of SASE and its benefits, this study aims to serve as a roadmap for organizations looking to adopt SASE as part of their digital transformation journey. In conclusion, the purpose of this study is to provide a comprehensive understanding of SASE and its potential to revolutionize the way organizations approach network security and performance.

VI. Objectives of the Study

The study aims to achieve the following objectives:

- To provide an overview of SASE technology and its benefits and outline the key considerations for organizations looking to adopt SASE as part of their digital transformation journey.
- To explore the concept of SASE and its potential impact on the world of networking and provide insights into the potential of SASE to transform the way organizations approach network security.
- To serve as a valuable resource for organizations looking to stay ahead of the curve in a rapidly evolving digital landscape.

VII. What is Secure Access Service Edge?

According to Gartner "Secure access service edge (SASE) delivers converged network and security as a service capability, including SD-WAN, SWG, CASB, NGFW and zero trust network access (ZTNA). SASE supports branch office, remote worker, and on-premises secure access use cases. SASE is primarily delivered as a service and enables zero trust access based on the identity of the device or entity, combined with real-time context and security and compliance policies" [1].

The primary focus of SASE is to provide secure access to networks and resources for branch offices, remote workers, and on-premises users. It delivers this secure access by using zero trust principles, which are based on the identity of the device or entity accessing the network, in conjunction with real-time context and security and compliance policies.

SASE is delivered as a service, which means that organizations don't have to manage and maintain the infrastructure themselves. This also enables organizations to easily scale their network and security capabilities as their needs change over time.

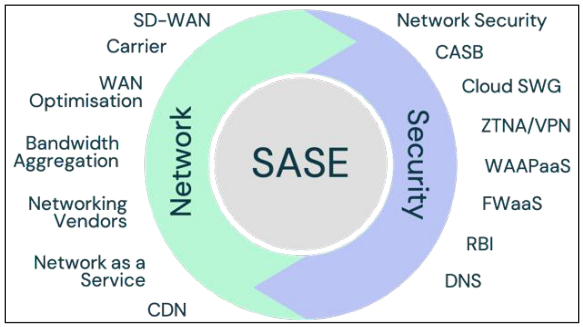

Fig. 1: Key Capabilities that Constitute a SASE [12]

Software-Defined WAN (SD-WAN) solutions provide a replacement for traditional WAN routers and are agnostic to WAN transport technologies. SD-WAN provides dynamic, policy-based, application path selection across multiple WAN connections and supports service chaining for additional services such as WAN optimization and firewalls [2].

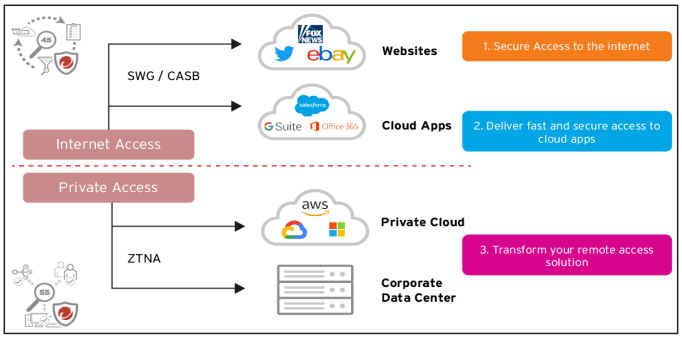

Fig. 2

Secure Web Gateway (SWG) solutions protect Web-surfing PCs from infection and enforce company policies. A secure Web gateway is a solution that filters unwanted software/malware from user-initiated Web/Internet traffic and enforces corporate and regulatory policy compliance. These gateways must, at a minimum, include URL filtering, malicious-code detection and filtering, and application controls for popular Web-based applications, such as instant messaging (IM) and Skype. Native or integrated data leak prevention is also increasingly included [3].

Cloud Access Security Brokers (CASBS) are on-premises, or cloud-based security policy enforcement points, placed between cloud service consumers and cloud service providers to combine and interject enterprise security policies as the cloud-based resources are accessed. CASBs consolidate multiple types of security policy enforcement. Example security policies include authentication, single sign-on, authorization, credential mapping, device profiling, encryption, tokenization, logging, alerting, malware detection/prevention and so on [4].

Zero Trust Network Access (ZTNA) is a product or service that creates an identity- and context-based, logical access boundary around an application or set of applications. The applications are hidden from discovery, and access is restricted via a trust broker to a set of named entities. The broker verifies the identity, context, and policy adherence of the specified participants before allowing access and prohibits lateral movement elsewhere in the network. This removes application assets from public visibility and significantly reduces the surface area for attack [5].

Next-Generation Firewalls (NGFWs) are deep-packet inspection firewalls that move beyond port/protocol inspection and blocking to add application-level inspection, intrusion prevention, and bringing intelligence from outside the firewall. An *NGFW* should not be confused with a stand-alone network intrusion prevention system (IPS), which includes a commodity or non-enterprise firewall, or a firewall and IPS in the same appliance that are not closely integrated [6].

Here is an Example of SASE Architecture described by TrendMicro [13].

VIII. Research on SASE Adoption [7]

The 2021 SASE Trends report found that nearly half of those surveyed (48%) view SASE as a security-first initiative, while 31% see it as a network-first strategy. SASE adoption is most often being led by Senior IT leaders, and is still relatively early, with only 37% having begun implementing a plan. Among early SASE adopters, most (58%) indicated ZTNA was a starting point - likely because supporting hybrid work and remote employees are among the top use cases for SASE. Related, 79% have accelerated their plans for SASE adoption because of the pandemic. In fact, 71% of companies plan to replace their VPN with ZTNA. It was also found that supporting business ecosystem partners is critical since one of out every three users who need access to resources is a third-party (34%).

While 70% believe that SASE adoption will take at least one year, there are undoubtedly significant business benefits for the IT leaders who embrace SASE. ESG found that organizations that had begun to implement SASE reported a variety of benefits such as fewer security incidents, reduced costs, better user experiences, and less downtime. In fact, 85% of respondents reported at least 3 benefits from their SASE implementation. Over half (55%) of those who had begun SASE initiatives indicated their organization had a dedicated SASE program budget, and 80% expect spending on SASE to increase going forward.

IX. Benefits of Secure Access Service Edge

SASE is a new approach to network security and performance that combines various security functions into a single solution. Adopting a Secure Access Service Edge (SASE) solution is becoming increasingly important for enterprises as they navigate the complexities of modern security and network architecture. Here are a few qualitative metrics that support the suggestion for SASE adoption:

Simplified Architecture: By combining security and networking into one solution, SASE simplifies the architecture and reduces the number of separate components required.

Increased Flexibility: SASE solutions provide a unified and flexible approach to security and networking, enabling organizations to adapt quickly and easily to changing business needs, such as remote work and cloud migrations.

Improved Security Posture: SASE solutions provide a centralized, cloud-based security infrastructure that can help organizations improve their overall security posture by reducing the attack surface, detecting, and mitigating threats, and providing a secure access experience for users.

Enhanced User Experience: SASE solutions provide a seamless user experience by delivering security services closer to the user, reducing latency, and improving performance.

Reduced Complexity: SASE solutions simplify the security and networking landscape by consolidating multiple solutions into a single, integrated platform, reducing the need for multiple point solutions and the complexity that comes with managing them.

Increased Agility: SASE solutions enable organizations to quickly respond to new security threats and changing business needs by leveraging the scalability and elasticity of the cloud, as well as the ability to easily update and deploy new security services.

Centralized Management: SASE solutions provide a single point of control for security and networking, allowing organizations to manage and monitor their security posture, and make rapid changes as needed more easily.

Cost Savings: By consolidating multiple point solutions into a single platform, organizations can reduce costs associated with hardware, software licenses, and management, while also improving efficiency and productivity.

Improved Compliance: SASE solutions provide a unified security infrastructure that can help organizations meet their compliance requirements more easily and effectively, by providing a comprehensive view of their security posture and automating compliance reporting.

Scalability: SASE solutions are designed to be scalable, providing organizations with the ability to quickly add new users, locations, and devices, and meet the changing needs of their business.

Threat Protection: SASE solutions provide real-time threat protection, leveraging machine learning, artificial intelligence, and other advanced technologies to quickly detect and mitigate security threats before they can cause harm.

These metrics provide a compelling case for why SASE is becoming a must-have for enterprises looking to improve their security posture, reduce complexity, and support their rapidly evolving business needs. SASE solutions are designed to meet the challenges of modern security and network architecture and provide organizations with the tools they need to succeed in a rapidly changing digital landscape.

X. Key Considerations for SASE adoption

Organizations looking to adopt SASE as part of their digital transformation journey should consider the following key factors:

Network Architecture: Organizations should assess their existing network architecture and determine how this technology can integrate with their existing systems and infrastructure.

Security Requirements: Organizations should carefully evaluate their security requirements, including the types of security functions they need, and the level of protection required, and ensure that this technology can meet those needs.

Cloud Adoption: Organizations should consider their current and future cloud adoption plans and determine how SASE can support their cloud-first strategy.

Network Performance: Organizations should assess their network performance requirements, including the need for low latency and high throughput, and determine if it can meet those requirements.

User Experience: Organizations should evaluate the user experience and ensure that SASE can provide a seamless and secure experience for remote workers and mobile users.

Cost: Organizations should consider the total cost of ownership, including the costs of hardware, software, and ongoing support and maintenance, when evaluating.

Vendor Selection: Not all SASE products are equal. Organizations should carefully evaluate vendors, considering

factors such as the vendor's experience and expertise, product offerings, and customer references.

By considering these key factors, organizations can ensure that they are making the right decision when it comes to adopting SASE as part of their digital transformation journey.

XI. SASE Use Cases

SASE technology has a wide range of potential use cases, some of which are specific to industries or domains. Some of these domain-specific use cases are:

Healthcare: SASE can provide secure access to sensitive patient data for remote workers, ensuring that confidential information is always protected.

Financial Services: SASE can provide secure access to financial systems and data for remote workers, reducing the risk of data breaches and ensuring the security of sensitive information.

Government: SASE can provide secure access to government networks and systems for remote workers, ensuring that confidential information is always protected.

Retail: SASE can provide secure access to point-of-sale systems and other retail systems for remote workers, reducing the risk of data breaches and ensuring the security of sensitive information.

Manufacturing: SASE can provide secure access to manufacturing systems and data for remote workers, ensuring that confidential information is always protected.

Education: SASE can provide secure access to educational systems and data for remote workers, ensuring that confidential information is always protected.

Telecommunications: SASE can provide secure access to telecommunications systems and data for remote workers, ensuring that confidential information is always protected.

These are just a few examples of domain-specific use cases for SASE technology. The flexibility and scalability of SASE make it an ideal solution for organizations in a wide range of industries and domains.

XII. Recommendations of the Study

Based on the findings of the study "The Future of Network Security: SASE", the following recommendations can be made:

- Organizations should consider adopting SASE as part of their digital transformation journey to address the growing challenges of network security and performance.
- Organizations should evaluate their current network security posture and assess the benefits of SASE in addressing their specific needs.
- Organizations should collaborate with a trusted vendor or service provider that has expertise in SASE technology to ensure a smooth and successful deployment.
- Organizations should prioritize a phased approach to deployment, starting with a small pilot project and gradually scaling up as needed.
- Organizations should regularly monitor and review their SASE implementation to ensure that it is meeting their needs and that security policies and protocols are up-to-date.
- Organizations should invest in training and education for their IT staff to ensure that they have the knowledge and skills necessary to effectively manage and maintain their SASE implementation.
- Organizations should stay informed of the latest developments in SASE technology and regularly evaluate their SASE implementation to ensure that it continues to meet their needs in an ever-evolving digital landscape.

In conclusion, SASE has the potential to revolutionize the way organizations approach network security and performance. By following these recommendations, organizations can ensure a successful deployment of SASE technology and reap the benefits of a more secure and efficient network.

References

[1] Secure Access Service Edge. [Online]. Available: https://www.gartner.com/en/information-technology/glossary/secure-access-service-edge-sase

[2] Software-defined WAN. [Online]. Available: https://www.gartner.com/en/information-technology/glossary/software-defined-wan-sd-wan

[3] Secure Web Gateway. [Online]. Available: https://www.gartner.com/en/information-technology/glossary/secure-web-gateway

[4] Cloud Access Security Broker. [Online]. Available: https://www.gartner.com/en/information-technology/glossary/cloud-access-security-brokers-casbs

[5] Zero Trust Network Access. [Online]. Available: https://www.gartner.com/en/information-technology/glossary/zero-trust-network-access-ztna-

[6] Next Gen Firewalls. [Online]. Available: https://www.gartner.com/en/information-technology/glossary/next-generation-firewalls-ngfws

[7] Enterprise Security Group (ESG) SASE Adoption. [Online]. Available: https://www.prnewswire.com/news-releases/esg-research-finds-sase-adoption-has-accelerated-multi-vendor-approaches-are-preferred-and-ztna-projects-are-leading-the-way-301382214.html

[8] Secure Access Service Edge: A Multivocal Literature Review. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/ 9732396/authors#authors

[9] How SASE is defining the future of network security Available: https://www.magonlinelibrary.com/doi/abs/10.1016/S1353-4858%2820%2930139-2

[10] A Study on Rapid Adoption of Zero Trust Network Architectures by Global Organizations Due to COVID-19 Pandemic. [Online]. Available: https://www.researchgate.net/profile/Aniket-Deshpande-4/publication/353946808_A_Study_on_Rapid_Adoption_of_Zero_Trust_Network_Architectures_by_Global_Organizations_Due_to_COVID-19_Pandemic/links/611b993c0c2bfa282a4df2ca/A-Study-on-Rapid-Adoption-of-Zero-Trust-Network-Architectures-by-Global-Organizations-Due-to-COVID-19-Pandemic.pdf

[11] The Future of Network Security is in the Cloud. [Online]. Available: https://scholar.googleusercontent.com/scholar?q=cache:v5NWJPbVBF8J:scholar.google.com/+SASE+adoption+&hl=en&as_sdt=0,31&as_vis=1

[12] Key Capabilities that Constitute SASE. [Online]. Available: https://cavellgroup.com/sase-ultimate-guide/

[13] SASE Architecture. [Online]. Available: https://www.trendmicro.com/en_us/ciso/22/h/secure-access-service-edge-sase-security-company.html