A Case Study: Leveraging SASE Technology for Zero Trust Implementation in Cloud Environments

Joo Hyun Lee
Department of ICT Convergence Engineering
Kangnam University
Yong-in, South Korea
leejoohyunoffice@gmail.com

Jungsoo Park
Department of ICT Convergence Engineering
Kangnam University
Yong-in, South Korea
jspark@kangnam.ac.kr

Recently, the changes in the cybersecurity environment and the proliferation of cloud-based services have highlighted the limitations of traditional security models. Zero Trust (ZT) is a security concept based on the principle of trusting no one. Zero Trust Architecture (ZTA) is a security framework that operates without trusting any device or user, instead requiring authentication and authorization for each request. This concept shares similarities with Secure Access Service Edge (SASE), a framework that integrates multiple network and security functions at the cloud edge, reducing costs and maintenance for organizations implementing their network strategies. Zero Trust is a response to modern enterprise network trends, including remote users, bring your own device (BYOD), and cloud-based assets that exist outside traditional enterprise network boundaries. In this paper, we will analyze SASE within the context of Zero Trust Architecture and recommend an adoption strategy.

Keywords—Zero Trust Architecture, Cloud Security, SASE

I. Introduction

The rapid shift towards cloud-based services and remote work environments has exposed the limitations of traditional security models[1]. In response, the Zero Trust security model has emerged as a critical framework, based on the principle that no entity—whether inside or outside the network—should be trusted by default. Instead, every user and device must undergo continuous verification to access network resources. This concept challenges the conventional security approach, which typically distinguishes between trusted internal networks and untrusted external ones. Zero Trust enforces strict identity verification, device authentication, and least privilege access, providing a more resilient security posture against evolving cyber threats.

To implement Zero Trust effectively in modern, distributed environments, Zero Trust Architecture (ZTA) was developed. ZTA operationalizes Zero Trust principles by incorporating multi-factor authentication, device health checks, and the least privilege access policies across all system layers. These layers involve verifying every user, validating every device, and enforcing the least privilege access to minimizing security risks[4].

In cloud-based and hybrid network environments, Zero Trust can be enabled through Secure Access Service Edge (SASE). SASE integrates wide-area networking (WAN) and security services into a single, cloud-delivered solution that meets the dynamic and flexible needs of modern organizations. By combining Zero Trust Network Access (ZTNA), Cloud Access Security Brokers (CASB), Secure Web Gateways (SWG), and Next-Generation Firewalls (NGFW), SASE allows enterprises to implement Zero Trust seamlessly in cloud-native architectures[4].

In this paper, we explore possible case studies for applying SASE to implement Zero Trust in cloud environments, compare each case, and propose a model for applying SASE.

II. Related Work

A. Zero Trust Architecture

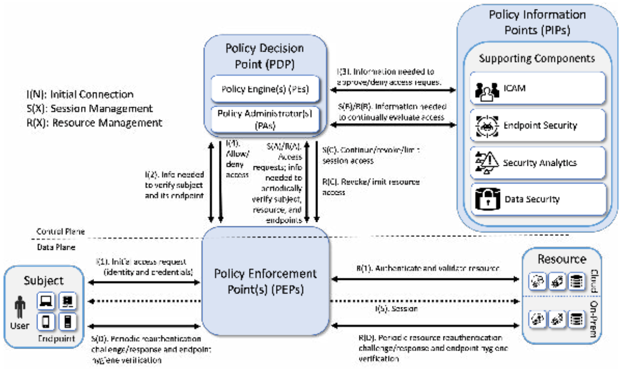
Policy Information Points (PIPs)
Supporting Components
ICAM
Endpoint Security
Security Analytics
Data Security
Policy Decision Point (PDP)
Policy Engine(s) (PEs)
Policy Administrator(s) (PAs)
I(N): Initial Connection
S(X): Session Management
R(X): Resource Management
I(3). Information needed to approve/deny access request
S(B)/R(B). Information needed to continually evaluate access
I(2). Info needed to verify subject and its endpoint
I(4). Allow/deny access
S(A)/R(A). Access requests; info needed to periodically verify subject, resource, and endpoints
S(C). Continue/revoke/limit session access
R(C). Revoke/limit resource access
Control Plane
Data Plane
Subject
User
Endpoint
I(1). Initial access request (identity and credentials)
Policy Enforcement Point(s) (PEPs)
R(1). Authenticate and validate resource
I(5). Session
S(D). Periodic reauthentication challenge/response and endpoint hygiene verification
R(D). Periodic resource reauthentication challenge/response and endpoint hygiene verification
Resource
Cloud
On-Prem

Figure 1. Zero Trust Architecture

Zero Trust Architecture (ZTA) is a security framework that applies guiding principles to workflows, system designs, and operations to minimize security threats[1]. Introduced by the Jericho Forum in 2004, Zero Trust is based on the idea of "Never trust, always verify" and was developed to address the limitations of traditional firewall-based security. ZTA requires continuous authentication and authorization to access specific resources based on predefined criteria.

The Zero Trust model operates through three core components: the Policy Engine (PE), Policy Administrator (PA), and Policy Enforcement Point (PEP)[4]. In this architecture, untrusted subjects entering the system are processed by the PEP, which forwards information to the Policy Decision Point (PDP)

979-8-3315-0694-0/25/$31.00 ©2025 IEEE

to determine the appropriate action. The PE, located within the PDP, uses a trust algorithm to make access decisions, and the PA then communicates these decisions to the PEP, deciding whether to grant or deny access to the requested resource. The PEP continuously interacts with the PA to monitor any changes or updates, enforcing policies throughout the system[3].

ZTA policies can be categorized into different types based on location and attributes, such as Device Agent/Gateway, Enclave, Resource Portal, and Device Application Sandbox[5]. Organizations need to select an appropriate Zero Trust implementation strategy based on their specific needs. The three main approaches for implementing Zero Trust are Enhanced Identity Governance, Micro-Segmentation, and utilizing Network Infrastructure and Software Defined Perimeters. According to NIST 800-207, all three approaches should be considered to build a robust Zero Trust architecture[4]. ZTA is defined by NIST as a cybersecurity framework that applies Zero Trust principles to the relationships and workflows within an organization.

B. *Secure Access Service Edge(SASE)*

Secure Access Service Edge (SASE) is an architectural framework that combines wide-area networking (WAN) capabilities with comprehensive security services in a cloud-native environment[2]. As organizations increasingly adopt cloud services and enable remote workforces, the traditional network perimeter is dissolving, making it difficult to maintain consistent security policies. SASE addresses this challenge by bringing security and networking functions closer to users, devices, or applications, regardless of their location.

SASE integrates several security solutions, including Zero Trust Network Access (ZTNA), Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), Next-Generation Firewalls (NGFW), and Software-Defined Wide Area Network (SD-WAN), into a unified, cloud-delivered service[2]. This architecture supports dynamic scalability and flexibility, ensuring secure access to applications and data from any location.

Key Components of SASE:

- Zero Trust Network Access (ZTNA): ZTNA is a core component of the SASE model, enforcing Zero Trust principles by verifying users and devices before granting access to applications[11]. It provides secure, segmented access to resources based on user identity and context, minimizing lateral movement within the network[11].
- Cloud Access Security Broker (CASB): CASBs control access to cloud services, ensuring sensitive data protection while monitoring and governing cloud usage. In a SASE framework, CASB is integrated to provide seamless cloud security across the enterprise[3].
- Secure Web Gateway (SWG): SWG filters web traffic and enforces security policies, protecting users from web-based threats and ensuring internet usage complies with organizational standards[9].
- Next-Generation Firewall (NGFW): NGFWs offer advanced network security functions, including intrusion prevention, deep packet inspection, and application control. In a SASE environment, NGFWs are delivered as a service, providing strong protection against network-based threats[3].
- Software-Defined Wide Area Network (SD-WAN): SD-WAN enhances network performance by intelligently routing traffic across different WAN connections. In a SASE architecture, SD-WAN integrates with security functions to ensure high-performance, secure access to applications, no matter where they are hosted[8].

C. *Related Work*

Many studies have been conducted on implementing Zero Trust in cloud environments. In particular, research has been carried out on applying SASE or incorporating some of its features. Through these studies, various strategies have been discussed to ensure the effective application of Zero Trust in cloud environments used by enterprises.

Table 1. Summary of Key Topics Addressed in Various Research Papers on SASE, SD-WAN, SWG, CASB, and ZTNA

Paper	1 SASE	2 SD-WAN	3 SWG	4 CASB	5 ZTNA
MacDonald et al.	□				
Yang et al.		□			
Pearce et al.			□		
Fernandez et al.				□	
MEF Forum,2020	□	□		□	
D.A. Deshpande et al.					□

MacDonald et al. emphasizes that traditional network security architectures centered around data centers are no longer suitable for the dynamic access requirements of digital businesses. It introduces the concept of Secure Access Service Edge (SASE), which converges networking and security services into a cloud-delivered solution based on identity and context. SASE supports digital transformation by enabling secure, low-latency access to cloud services and remote users. Enterprises are advised to adopt SASE for improved agility, reduced complexity, and enhanced security[7].

Yang et al. discusses Software-Defined Wide Area Network (SD-WAN) as a next-generation network architecture that addresses the limitations of traditional WANs in meeting modern application demands. SD-WAN enables centralized control, flexibility, and the ability to define policies based on application requirements. It consists of three layers: the data layer (traffic handling and bandwidth virtualization), the control layer (centralized management), and the application layer (translating application needs into network policies). SD-WAN offers enhanced network management and scalability compared to legacy WAN architectures[8].

Pearce et al. paper presents a Secure Web Gateway (SWG) system using open-source tools like Squid, Greasyspoon ICAP Server, and ClamAV to provide enhanced web security. It discusses the SWG's effectiveness in mitigating web-based threats through URL redirection, content sanitization, and user notifications. The system, built as a web proxy, performs various security tasks, including request modification and response filtering, to protect users from malicious web content. Performance and effectiveness tests indicate its potential as a low-cost SWG solution suitable for small organizations and individual users[9].

Fernandez et al. discusses about how Cloud Access Security Broker acts as a security layer between users and cloud service providers. CASBs help organizations apply security policies and access controls, ensuring data protection even with the cloud service provider's limited application-specific knowledge. They unify access management, enable data encryption with consumer-specific keys, and support compliance by auditing access logs. CASBs integrate security seamlessly into cloud ecosystems, supporting access from varied devices while protecting sensitive organizational data[10].

The MEF white paper offers insights into SASE, SD-WAN, and CASB within a framework aimed at secure and efficient digital service delivery. SASE integrates network and security functions to connect users with applications through a unified policy-based framework. It leverages a range of security services—like firewall, threat prevention, and identity-based policies—combined with SD-WAN or other networking functionalities to ensure security and performance across cloud environments. SD-WAN is described as a versatile tool for routing and optimizing paths across service edges and clouds, ensuring consistent connectivity and performance for dispersed network locations, often with encrypted and segmented routing for secure traffic management. CASB provides data protection, threat detection, and user authentication for SaaS applications, supporting a zero-trust framework where access control and data security are maintained consistently across varied cloud services[12].

D. A. Deshpande et al. discusses about Zero Trust Network Architecture(ZTNA) and correlation from working at home because of COVID-19. ZTNA incorporates multifactor authentication, least privilege access, and micro-segmentation, creating robust defenses that limit unauthorized access across network zones. Unlike older models that allowed unrestricted access once inside the network perimeter, ZTNA enforces policies that restrict lateral movement within the network, thus minimizing attack surfaces. By using multi-factor authentication, least-privilege access, and micro-segmentation, ZTNA prevents unauthorized access and ensures that only verified and necessary permissions are granted. This framework is adaptable both within organizational premises and in cloud environments, supporting secure remote access and addressing modern cybersecurity needs.[11].

Through this, we can observe that current research efforts primarily focus on specific aspects of Zero Trust and SASE, indicating that the integration of these concepts into existing technologies has not been fully realized. This highlights the need for a more comprehensive approach in adopting Zero Trust and SASE. Therefore, we have conducted a study to explore a broader range of cases, aiming to bring us a step closer to effectively implementing Zero Trust and SASE.

III. Case Study

We have conducted several case studies on how to implement Zero Trust by applying SASE or combining specific SASE components, depending on various access environments and the location of cloud resources. Since each organization utilizes a different cloud environment, and users may connect from various locations, these case studies aim to offer tailored solutions that allow Zero Trust to be effectively integrated into cloud environments. By considering the unique characteristics of each scenario, we propose methods for applying Zero Trust in a flexible manner across different cloud architectures.

Our study classifies the environment based on whether resources are hosted in a private cloud or a public cloud, and suggests the best approach for Zero Trust implementation in each case. We also introduce methods to adopt Zero Trust based on user access scenarios, such as when users are within the internal network, connecting from branch offices, accessing remotely, or when external users need to connect. By examining these various use cases, we aim to provide strategies that enable organizations to flexibly apply Zero Trust according to their specific cloud environments and access needs. Table 1 below shows the classification we have established.

While fully adopting SASE would provide stronger security, it is essential to introduce components in a way that aligns with the company's environment and situation, allowing for gradual development based on their maturity level. Therefore, this study provides a relevant case study tailored to these needs.

TABLE 2. Classification of Zero Trust Implementation Methods Based on Cloud Environment and Access Scenarios

User Location	**Resource**	
	Private Cloud	**Public Cloud**
Local	ZTNA, IAM, SDP	CASB, ZTNA, NGFW

User Location	Resource	
	Private Cloud	Public Cloud
Branch	SD-WAN, ZTNA, IAM	SD-WAN, CASB, ZTNA
Remote	ZTNA, MFA, SDP	ZTNA, CASB, NGFW
External User	ZTNA, IAM, SDP	ZTNA, CASB, MFA

- Internal User - Private Cloud Access

When internal users access private cloud resources, this scenario is generally considered more secure. However, under the Zero Trust principles, no user or device is inherently trusted, and continuous verification is required even within the internal network. In this case, ZTNA can be used to continuously verify the identity of internal users, ensuring that they are granted the minimum necessary access to cloud resources. IAM strengthens identity and access management for users, while SDP can further segment and secure the network perimeter. By restricting access even within the internal network, organizations can reduce potential security threats to private cloud resources.

- Internal User - Public Cloud Access

Even though internal users are connecting from within the organization, accessing public cloud resources involves interacting with external environments, requiring additional security measures. CASB can be used to monitor and control data usage in the public cloud, while ZTNA ensures that internal users only have the minimum required access to public cloud resources, with continuous verification. NGFW provides advanced firewall protection for the public cloud environment, safeguarding traffic and data from external threats.

- Branch User - Private Cloud Access

When branch office users connect to the private cloud, it is crucial to optimize network performance between the branch and headquarters while maintaining security. SD-WAN helps optimize network traffic between the branch and the private cloud, while ZTNA ensures that branch users are continuously authenticated and granted minimum necessary access to the private cloud. IAM manages the access rights of branch users, ensuring secure access to private cloud resources. In this scenario, maintaining secure and stable communication between the branch and headquarters is key.

- Branch User - Public Cloud Access

In this scenario, branch office users accessing public cloud resources need optimized network performance along with enhanced security. SD-WAN optimizes network traffic to the public cloud, while CASB ensures that the activities of branch users in the public cloud are monitored and controlled. ZTNA continues to enforce identity verification and access control, ensuring branch users have limited access based on their needs in the public cloud environment.

- Remote User - Private Cloud Access

Remote users require strong security protocols to access private cloud resources safely. ZTNA ensures continuous identity verification for remote users, granting only the minimum access needed to private cloud resources. MFA adds an extra layer of authentication, strengthening security, while SDP protects the remote access path and minimizes security threats. Securing remote users' access to private cloud resources is critical in this scenario.

- Remote User - Public Cloud Access

Remote users connecting to public cloud resources interact with external environments, requiring additional security. ZTNA ensures continuous verification and minimal access control for remote users, while CASB monitors and manages their activities in the public cloud. NGFW provides advanced protection for public cloud traffic and data, securing it from external threats.

- External User (Partners/Clients) - Private Cloud Access

When external users, such as partners or clients, access private cloud resources, limited and tightly controlled access is essential. ZTNA verifies the identity of external users, allowing them restricted access to only the necessary resources. IAM rigorously manages external users' identities and access rights, while SDP protects access paths, ensuring that only authorized users can connect to private cloud resources. This ensures that external users can access private cloud resources securely, without compromising internal security.

- External User (Partners/Clients) - Public Cloud Access

External users accessing public cloud resources require enhanced security to prevent unauthorized access. ZTNA ensures continuous identity verification for external users, granting them only the minimum necessary access to public cloud resources. CASB monitors external users' activities in the public cloud, preventing data leakage and enforcing security policies. MFA adds a multi-step authentication process, ensuring that external users can access the public cloud securely.

These eight scenarios present tailored solutions for applying Zero Trust and SASE based on different users and cloud environments. Each scenario highlights the appropriate security technologies to minimize potential security threats and establish a secure working environment within cloud infrastructures. Organizations can use these scenarios to develop customized security strategies for their unique access situations and implement the Zero Trust model effectively.

IV. Conclusion

As the cybersecurity landscape continues to evolve, the limitations of traditional security models are becoming increasingly evident, particularly in the face of cloud adoption and the expansion of remote work environments. Zero Trust Architecture (ZTA) provides a robust alternative by implementing a security model based on the assumption that no entity, inside or outside the network, can be trusted without continuous verification. By integrating Zero Trust with Secure Access Service Edge (SASE), organizations can ensure secure and scalable access to both cloud and on-premises resources, while reducing the complexity of network management.

SASE offers an ideal framework for implementing Zero Trust in a cloud-native environment, incorporating integrated security solutions such as Zero Trust Network Access (ZTNA), Cloud Access Security Brokers (CASB), and Next-Generation Firewalls (NGFW).

In cases where it is difficult for organizations to fully implement all SASE technologies, we have provided a case study demonstrating how organizations can apply Zero Trust (ZT) to cloud environments safely through minimal implementation. Based on these research results, we will later conduct a security analysis of each model, focusing on the location and safety of the Policy Enforcement Point (PEP).

Acknowledgment

This research was supported by the MSIT(Ministry of Science and ICT), Korea, under the ITRC(Information Technology Research Center) support program(IITP-2024-2020-0-01602) supervised by the IITP(Institute for Information & Communications Technology Planning & Evaluation)

References

[1] Stafford, V. "Zero trust architecture." *NIST special publication* 800 (2020): 207.

[2] YILIYAER, Silafu; KIM, Yoohwan. Secure access service edge: A zero trust based framework for accessing data securely. In: 2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC). IEEE, 2022. p. 0586-0591.

[3] Carnegie Mellon University / Software Engineering Institute SEI Federal Zero Trust Industry Day Deploying a Zero Trust Architecture per NIST SP 800-207.

[4] Kerman, Alper, et al. "Implementing a zero trust architecture." *National Institute of Standards and Technology* 2020 (2020): 17-17.K. Elissa, "Title of paper if known," unpublished.

[5] Assunção, Pedro. "A zero trust approach to network security." *Proceedings of the Digital Privacy and Security Conference*. Vol. 2019. Porto Protugal, 2019.

[6] Buck, Christoph, et al. "Never trust, always verify: A multivocal literature review on current knowledge and research gaps of zero-trust." *Computers & Security* 110 (2021): 102436.

[7] MacDonald, Neil, Lawrence Orans, and Joe Skorupa. "The Future of Network Security Is in the Cloud." *Gartner* (2019).

[8] Yang, Zhenjie, et al. "Software-defined wide area network (SD-WAN): Architecture, advances and opportunities." *2019 28th International Conference on Computer Communication and Networks (ICCCN)*. IEEE, 2019.

[9] Pearce, Michael, and Ray Hunt. "Development and evaluation of a secure web gateway using existing ICAP open source tools." (2010).

[10] Fernandez, Eduardo B., Nobukazu Yoshioka, and Hironori Washizaki. "Cloud Access Security Broker (CASB): A pattern for secure access to cloud services." *4th Asian Conference on Pattern Languages of Programs, Asian PLoP*. Vol. 15. 2015.

[11] Deshpande, Aniket. "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 (2021): 5672-5677.

[12] MEF Forum, 2020. "MEF White Paper MEF SASE Services Framework July 2020" MEF 2020036