

Review Article

Open Access

Cloud Based Network Management: Leveraging SASE for Efficient and Secure Access

Mohit Bajpai

USA

ABSTRACT

The evolution of network management has been driven by the increasing complexity of modern IT environments, the demand for agile and scalable solutions, and the need for robust security measures. This paper delves into the potential of automation to revolutionize network management, with a concentrated analysis on Secure Access Service Edge as a cutting-edge approach that addresses these pressing challenges. The technical architecture and key features of SASE are comprehensively explored, showcasing its ability to streamline network operations, enhance security posture, and adapt to the dynamic requirements of organizations.

*Corresponding authors

Mohit Bajpai, USA.

Received: December 05, 2022; **Accepted:** December 15, 2022; **Published:** December 28, 2022

Keywords: Network Automation, SASE, Network Management, Cyber Security, Software-Defined Networking (SDN), Zero Trust Network Access (ZTNA), FWaaS, Cloud Access Security Broker (CASB), Cloud Based Secure Access

Introduction

The rapid advancements in cloud computing, the proliferation of mobile devices, and the emergence of the Internet of Things have fundamentally transformed the landscape of network management [1]. Organizations are now faced with the daunting task of overseeing an intricate web of interconnected systems, each with its own set of security vulnerabilities and management requirements. Traditional network management approaches, reliant on manual processes and siloed infrastructure, have proven inadequate in keeping pace with these evolving demands.

Automation has emerged as a transformative solution, empowering network administrators to streamline and optimize their operations. By leveraging the principles of Software-Defined Networking and the capabilities of Artificial Intelligence/Machine Learning (AI/ML), automation can automate a wide range of network management tasks, from configuration management to incident response [2].

At the forefront of this evolution is Secure Access Service Edge, a converged network and security architecture that promises to redefine the way organizations manage and secure their distributed networks.

SASE: A Unified Approach to Network Management

In contrast to the traditionally fragmented and siloed security and network management approaches, the SASE framework provides a cloud-based, integrated platform that seamlessly unifies essential functionalities, such as network connectivity, secure access control, and advanced security features. By consolidating these disparate components into a cohesive solution, SASE empowers organizations to address the complexities of contemporary network management with enhanced efficiency and agility.

The SASE model represents a transformative shift in network management, moving away from the conventional siloed infrastructure and manual processes towards a more integrated and automated approach. By converging network connectivity, security, and cloud-based services into a single, cloud-delivered platform, SASE offers organizations a comprehensive solution to the challenges posed by modern IT environments. This unified approach enables centralized visibility, control, and policy enforcement across the entire network, empowering organizations to optimize their network operations, enhance their security posture, and adapt more readily to evolving business requirements. The technical architecture of SASE is designed to seamlessly integrate and streamline the various components required for effective network management and security.

The SASE architecture is built upon the foundational principles of Software-Defined Networking and cloud-based service delivery. At the core of the SASE model is a cloud-based platform that serves as a central control point, orchestrating and governing the various network and security functions. This cloud-based architecture allows for dynamic and scalable provisioning of resources, ensuring that organizations can rapidly adapt to changes in network traffic, user demands, and security threats.

The SASE Framework Incorporates Several key Components, Including [3]:

- The SASE platform features a secure web gateway, which provides robust web filtering, URL categorization, and advanced threat protection to safeguard users and devices from internet-based attacks.
- The SASE model integrates a cloud-access security broker functionality, enabling organizations to enforce comprehensive access controls, monitor user activities, and mitigate the risks associated with cloud-based applications and services.
- SASE leverages a cloud-delivered firewall, which offers advanced, contextual-based security policies, leveraging real-time threat intelligence to protect the network from both internal and external threats.

These core components are further complemented by other security functionalities, such as zero-trust network access, data loss prevention, and remote browser isolation, ensuring a comprehensive and adaptive security posture.

Automation and SASE: Unlocking the Potential of Network Management

The integration of automation within the SASE framework unlocks a new era of efficient and intelligent network management. By leveraging the power of Artificial Intelligence and Machine Learning, SASE-enabled automation can streamline a wide range of network operations, from dynamic policy enforcement and proactive threat detection to automated incident response and remediation.

Automation plays a crucial role in the SASE model by enabling organizations to effectively manage the complexity of their distributed networks. Through the use of AI-driven analytics and machine learning algorithms, SASE-enabled automation can continuously monitor network traffic, identify anomalies, and automatically trigger appropriate security measures, such as blocking suspicious activities or rerouting traffic to mitigate threats. The cloud-based architecture of SASE allows for the centralized management and automated deployment of network configurations and security policies across the entire organization, ensuring consistency, scalability, and agility in the face of evolving business requirements and emerging cyber threats. By empowering network administrators with SASE-enabled automation, organizations can significantly reduce the time and effort required for manual network management tasks, allowing these skilled professionals to shift their focus towards strategic initiatives that drive business innovation and growth.

Key Components of SASE

The SASE architecture comprises several key components that work in tandem to deliver a comprehensive network management and security solution:

First, the SASE model integrates cloud-based networking capabilities, such as Software-Defined Wide Area Network and Virtual Private Network, to provide secure and optimized connectivity for distributed locations and remote users [4].

Next, SASE incorporates advanced security functionalities, including Firewall-as-a-Service, Secure Web Gateway, and Zero Trust Network Access, to enforce granular access control, mitigate cyber threats, and protect sensitive data in transit [5,2].

Additionally, SASE leverages the power of Cloud Access Security Broker to monitor and control the use of cloud-based applications, ensuring compliance with organizational policies and data protection regulations.

The seamless integration of these components under a unified platform is a hallmark of the SASE approach, enabling organizations to streamline their network management, enhance security, and respond to the dynamic demands of modern IT environments [4,2,6].

Technical Architecture of SASE

The technical architecture of SASE is designed to seamlessly integrate network connectivity, security, and cloud-based services into a cohesive and scalable solution.

At the core of the SASE architecture is the cloud-based service delivery model, which provides organizations with on-demand

access to network and security functionalities. This cloud-centric approach enables organizations to rapidly scale their network and security capabilities, eliminate the need for on-premises hardware, and benefit from the economies of scale offered by cloud infrastructure.

The SASE Architecture Typically Comprises the Following Key Components

- **Cloud-based Networking Services:** This includes Software-Defined Wide Area Network and Virtual Private Network capabilities, which enable secure and optimized connectivity for distributed locations and remote users.
- **Secure Access Control:** SASE incorporates various access control mechanisms, such as Zero Trust Network Access and Multi-Factor Authentication, to ensure that only authorized users and devices can access network resources.
- **Zero Trust Network Access (ZTNA):** is a security framework that assumes no user or device, whether inside or outside the network, should be trusted by default. Every access request is thoroughly verified before granting access to network resources, ensuring that security is maintained even if a user's credentials are compromised or if a device is compromised.
- **Advanced Security Capabilities:** The SASE framework integrates security functionalities like Firewall-as-a-Service, Secure Web Gateway, and Cloud Access Security Broker to protect against cyber threats and enforce data protection policies.
- **Centralized Management and Analytics:** SASE provides a centralized control plane that enables network administrators to manage and orchestrate policies, monitor network and security events, and obtain actionable insights through data analytics.

The integration of these components, combined with the power of automation, enables SASE to deliver a holistic and adaptive network management solution that can effectively address the challenges posed by modern IT environments. Following Diagram (Figure 1) depicts the SASE architecture and interaction between each components.

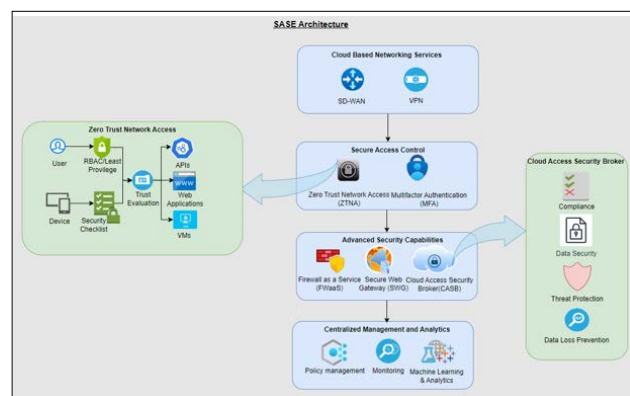


Figure 1

Conclusion

The emergence of SASE represents a significant shift in the way organizations approach network management and security. By consolidating essential network and security functionalities into a cloud-delivered, integrated platform, SASE offers a more efficient, scalable, and secure solution to the challenges posed by modern IT environments.

The Key Advantages of SASE Include

- Unified and automated network management through the

integration of cloud-based networking, security, and access control capabilities.

- Enhanced security through the implementation of advanced security measures, such as Zero Trust Network Access and Cloud Access Security Broker, to protect against cyber threats and data breaches.
- Improved agility and scalability, enabling organizations to rapidly adapt to changing business requirements and scale their network and security capabilities as needed.

As organizations continue to grapple with the complexities of distributed IT infrastructure and the increasing security risks, the SASE model presents a compelling solution that can help them navigate these challenges with greater efficiency, flexibility, and confidence.

References

1. Kafle VP, Fukushima Y, Martínez-Julia P, Miyazawa T (2018) Consideration On Automation of 5G Network Slicing with Machine Learning <https://doi.org/10.23919/itu-wt.2018.8597639>.
2. Benzaid C, Taleb T (2022) AI for Beyond 5G Networks: A Cyber-Security Defense or Offense Enabler? <https://doi.org/10.48550/arxiv.2201.02730>.
3. Yang B, Wu J, Wang H, Tsai W (2012) SmartSaaS: Model and Architecture <https://doi.org/10.4028/www.scientific.net/aef.6-7.1010>.
4. Kreutz D, Ramos FMV, Veríssimo P, Rothenberg CE, Azodolmolky S, et al. (2014) Software-Defined Networking: A Comprehensive Survey <https://doi.org/10.48550/arxiv.1406.0440>.
5. Lam J, Abbas H (2020) Machine Learning based Anomaly Detection for 5G Networks <https://doi.org/10.48550/arxiv.2003.03474>.
6. Feamster N, Rexford J (2018) Why (and How) Networks Should Run Themselves <https://doi.org/10.1145/3232755.3234555>.

Copyright: ©2022 Mohit Bajpai. This is an open-access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.