Secure Access Service Edge

Subjects: Computer Science, Software Engineering

Contributor: HandWiki Xu

Secure Access Service Edge (SASE) is a term coined by analyst firm Gartner, SASE simplifies wide-area networking (WAN) and security by delivering both as a cloud service directly to the source of connection (user, device, branch office, IoT device, edge computing location) rather than the enterprise data center. Security is based on identity, real-time context and enterprise security and compliance policies. An identity may be attached to anything from a person/user to a device, branch office, cloud service, application, IoT system, or an edge computing location. SASE is meant to be a simplified WAN and security solution for a mobile, global workplace that relies on cloud applications and data. The common solution of backhauling all WAN traffic over long distances to one or a few corporate data centers for security functions adds network latency when users and their cloud applications are globally dispersed, rather than on-premises. By targeting services to the edge at the connection source, SASE eliminates the latency caused by backhauling.

Keywords: network latency ; edge computing ; cloud service

1. Overview

SASE combines SD-WAN with a stack of security functions, including Cloud Access Security Brokers (CASB), Secure Web Gateways (SWG), antivirus/malware inspection, virtual private networking (VPN), firewall as a service (FWaaS), and data loss prevention (DLP), all delivered by a single cloud service at the network edge.[1]

SASE SD-WAN service enhancements may include traffic prioritization, WAN optimization and converged backbones to enhance reliability and maximize performance.[2]

WAN and security functions are typically delivered as a single service at globally dispersed SASE points of presence (PoPs) located as close as possible to dispersed users, branch offices and cloud services.[3] To access SASE services, edge locations or users connect to the closest available PoP. SASE vendors may contract with several backbone providers and peering partners to offer customers fast, low-latency WAN performance for long-distance PoP-to-PoP connections.[3]

2. History and Drivers

The term SASE was coined by Gartner analysts Neil McDonald and Joe Skorupa and described in a July 29, 2019 Networking Hype Cycle[4] and Market Trends Report, How to Win as WAN Edge and Security Converge into the Secure Access Service Edge[5] and an August 30, 2019 Gartner report, The Future of Network Security is in the Cloud.[3]

SASE is driven by the rise of mobile, edge and cloud computing in the enterprise at the expense of the LAN and corporate data center. As users, applications and data move out of the enterprise data center to the cloud and network edge, moving security and WAN to the edge as well is necessary to minimize latency and performance issues[6]

The cloud model is meant to delegate and simplify delivery of SD-WAN and security functions to multiple edge computing devices and locations. Based on policy, different security functions may also be applied to different connections and sessions from the same entity, whether SaaS applications, social media, data center applications or personal banking, according to Gartner.[3]

The cloud architecture boasts typical cloud enhancements such as elasticity, flexibility, agility, global reach and delegated management.

3. Required Characteristics

SASE has many characteristics and components, but the principal elements are:

- Convergence of WAN and network and network security functions.
- A cloud-native architecture delivering converged WAN and security as a service that offers the scalability, elasticity, adaptability and self-healing typical of all cloud services.
- Globally distributed fabric of PoPs guaranteeing a full range of WAN and security capabilities with low latency, wherever business offices, cloud applications and mobile users are located. To deliver low latency at any location, SASE PoPs have to be more numerous and extensive than those offered by typical public cloud providers and SASE providers must have extensive peering relationships.
- Identity-driven services. An identity can be attached to anything from a person or branch office to a device, application, service, IoT device or edge computing location at the source of connection. Identity is the most significant context affecting SASE security policy. However, location, time of day, risk/trust posture of the connecting device and application and data sensitivity will provide other real-time context determining the security services and policies applied to and throughout each WAN session.
- Support for all edges equally, including physical locations, cloud data centers, users' mobile devices and edge computing, with placement of all capabilities at the local PoP rather than the edge location. Edge connections to the local PoP may vary from an SD-WAN for a branch office to a VPN client or clientless Web access for a mobile user, to multiple tunnels from the cloud or direct cloud connections inside a global data center.[6]

4. Features

Gartner and others have cited numerous features/benefits of a SASE architecture for the mobile, cloud enabled enterprise. These include:

4.1. Reduced Complexity

Reduced complexity that comes with the cloud model and a single vendor for all WAN and security functions, vs. multiple security appliances from multiple vendors at each location. Reduced complexity also comes from a single-pass architecture that decrypts the traffic stream and inspects it once with multiple policy engines rather than chaining multiple inspection services together.

4.2. Universal Access

A SASE architecture is architected to provide consistent fast, secure access to any resource from any entity at any location, as opposed to access primarily based on the corporate data center.

4.3. Cost Efficiency

Cost efficiency of the cloud model, which shifts up-front capital costs to monthly subscription fees, consolidates providers and vendors, and reduces the number of physical and virtual branch appliances and software agents IT has to purchase manage and maintain in-house. Cost reduction also comes from delegation of maintenance, upgrades and hardware refreshes to the SASE provider.

4.4. Performance

Performance of applications and services enhanced by latency-optimized routing, which is particularly beneficial for latency-sensitive video, VoIP and collaboration applications. SASE providers can optimize and route traffic through high-performance backbones contracted with carrier and peering partners.

4.5. Ease of Use

Ease of use Depending on the implementation, SASE is likely to reduce the number of apps and agents required for a device to a single app and provides a consistent experience to the user regardless of where they are or what they are accessing.

4.6. Consistent Security

Consistent security via a single cloud service for all WAN security functions and WAN connections. Security is based on the same set of policies, with the same security functions delivered by the same cloud service to any access session, regardless of application, user or device location and destination (cloud, data center application). Once the SASE provider adapts to a new threat, the adaption can be available to all the edges.[3]

5. SASE Vendors

Although there are differences in the details with the name of the features in Secure Access Service Edge (SASE), some vendors [7] [8] are offering the SASE. It is for a cloud-delivered secure service that combines network and security functions with optimized WAN capabilities including dynamic, secure access to multiple links. [9]

6. Criticism

Criticism of SASE has come from several sources, including IDC and IHS Markit, as cited in a November 9, 2019 sdxcentral post written by Tobias Mann.[10] Both analyst firms criticize SASE as a Gartner term that is neither a new market, technology nor product, but rather an integration of existing technology with a single source of management.

Clifford Grossner of IHS Markit criticizes the lack of analytics, artificial intelligence and machine learning as part of the SASE concept and the likelihood that enterprises won't want to get all SD-WAN and security functions from a single vendor. Gartner counters that service chaining of security and SD-WAN functions from multiple vendors yields “inconsistent services, poor manageability and high latency.”[11]

IDC analyst Brandon Butler cites IDC's position that SD-WAN will evolve to SD-Branch, defined as centralized deployment and management of virtualized SD-WAN and security functions at multiple branch office locations.

Nevertheless, Cato Networks, Infoblox, and Palo Alto[12] have introduced offerings in the SASE market.

7. Complementary Technology

7.1. SD-WAN

SD-WAN is a technology that simplifies wide area networking through centralized control of the networking hardware or software that directs traffic across the WAN. It also allows organizations to combine or replace private WAN connections with Internet broadband, LTE and/or 5g connections. The central controller sets policies and prioritizes, optimizes and routes WAN traffic, selecting the best link and path dynamically for optimum performance. SD-WAN vendors may offer some security functions with their SD-WAN virtual or physical appliances, which are typically deployed at the data center or branch office.

Typically SASE incorporates SD-WAN as part of a cloud service that also delivers mobile access and a full security stack delivered from a local PoP.

7.2. Network as a Service (NaaS)

SASE and NaaS overlap in concept. NaaS delivers virtualized network infrastructure and services using a cloud subscription business model. Like SASE it offers reduced complexity and management costs. Typically, different NaaS providers offer different service packages, such as a package of WAN and secure VPN's as a service, bandwidth on demand, or hosted networks as a service. By contrast SASE is meant to be a single comprehensive secure SD-WAN solution for branch offices, mobile users, data centers and any other secure enterprise WAN requirement.[13]

7.3. Next Generation Firewall (NGFW)

NGFW combines a traditional firewall with other security and networking functions geared to the virtualized data center. Security functions include application control, deep and encrypted packet inspection, intrusion prevention, Web site filtering, anti-malware, identity management, threat intelligence and even WAN quality of service and bandwidth management.[14]

NGFW offers a subset of the security stack offered by SASE, and typically doesn't include SD-WAN services. NGFW may be deployed on premises or as a cloud service, while SASE is a cloud architecture by definition. While SASE focuses security on WAN connections, a NGFW can be deployed anywhere including internally in the data center.

7.4. Firewall as a Service (FWaaS)

FWaaS is a firewall offered as a cloud service, rather than on premises as software or hardware. Most FWaaS providers offer NGFW capabilities.[15] Typically, an entire organization is connected to a single FWaaS cloud with no requirement for maintaining its own firewall infrastructure. SASE combines edge FWaaS with other security functions and SD-WAN.[3]

8. Marketplace

Gartner classifies SaaS as an emerging market with several vendors offering a large number of SASE capabilities, but no single provider offering the entire SASE portfolio. It lists 14 companies in several market categories as SASE players, including Zscaler, Cloudflare, Cisco, Akamai, Palo Alto Networks, Symantec, VMware, Cato Networks and Netskope, and expects some of the major cloud providers to move into this category.[16] Gartner doesn't expect a complete SASE offering to be available until sometime in 2020.[3]

9. Standards

MEF which was created as the Metro Ethernet Forum, has become a next generation standards organization with a broad focus around software defined network and security infrastructure services for service provider, technology manufacturers, and enterprise network design. For the purpose of creating a future where interoperation between "best of breed" solutions is possible, MEF set out to create a number of industry standards that could be leveraged for training as well as integration. The MEF SASE Services Definition (MEF W117) committee was established and will be providing a draft technical specification for public use. This specification has been the work of a number of technology manufacturers as well as several service providers and is based on current MEF Technical Specifications such as MEF 70.1 Draft Release 1 SD-WAN Service Attributes and Service Framework.

References

1. "The Network for the Digital Business Starts with the Secure Access Service Edge (SASE)" (in en). 2019. https://go.catonetworks.com/The-Network-Starts-with-SASE.html.
2. Conran, Matt (2019-10-24). "The evolution to Secure Access Service Edge (SASE) is being driven by necessity" (in en). https://www.networkworld.com/article/3448276/the-evolution-to-secure-access-service-edge-sase-is-being-driven-by-necessity.html.
3. MacDonald, Neil; Orans, Lawrence; Skorupa, Joe (August 30, 2019). "The Future of Network Security Is in the Cloud". Gartner. https://www.gartner.com/doc/reprints?id=1-1OG9EZYB&ct=190903&st=sb.
4. "Hype Cycle for Enterprise Networking, 2019" (in en). https://www.gartner.com/en/documents/3947237/hype-cycle-for-enterprise-networking-2019.
5. "Market Trends: How to Win as WAN Edge and Security Converge Into the Secure Access Service Edge" (in en). https://www.gartner.com/en/documents/3953690/market-trends-how-to-win-as-wan-edge-and-security-conver.
6. Conran, Matt (2019-10-03). "Secure Access Service Edge (SASE): A reflection of our times" (in en). https://www.networkworld.com/article/3442941/secure-access-service-edge-sase-a-reflection-of-our-times.html.
7. https://www.cisco.com/c/en/us/products/security/sase.html
8. https://go.catonetworks.com/The-Network-Starts-with-SASE.html
9. https://www.fortinet.com/resources/cyberglossary/sase
10. "Analysts Debate SASE's Merits as Vendors Board Hype Train". https://www.sdxcentral.com/articles/news/analysts-debate-sases-merits-as-vendors-board-the-hype-train/2019/11/.
11. "Analysts Debate SASE's Merits as Vendors Board Hype Train - SDxCentral" (in en-US). SDxCentral. 2019-11-09. https://www.sdxcentral.com/articles/news/analysts-debate-sases-merits-as-vendors-board-the-hype-train/2019/11/.
12. "Palo Alto Networks Leaps Into SASE Market - SDxCentral" (in en-US). SDxCentral. 2019-11-16. https://www.sdxcentral.com/articles/news/palo-alto-networks-leaps-into-sase-market/2019/11/.
13. "NaaS Meets SD-WAN: What is NaaS anyway and How Will It Impact Your SaaS, PaaS, and Cloud Strategy?" (in en). https://www.catonetworks.com/blog/taking-network-as-a-service-naas-to-the-next-level.
14. "What is a Next Generation Firewall? Learn about the differences between NGFW and traditional firewalls". 2017-11-27. https://digitalguardian.com/blog/what-next-generation-firewall-learn-about-differences-between-ngfw-and-traditional-firewalls.
15. "What is Firewall as a Service (FWaaS) and Why You Need It" (in en). https://www.catonetworks.com/blog/what-is-firewall-as-a-service-fwaas-and-why-you-need-it.
16. Riley, Steve; Lawson, Craig (October 22, 2019). "Magic Quadrant for Cloud Access Security Brokers". Gartner. https://www.gartner.com/doc/reprints?id=1-1XOFCANJ&ct=191024&st=sb.

Retrieved from https://encyclopedia.pub/entry/history/show/81622