Digital Innovations & Contemporary Research in SCIENCE, ENGINEERING & TECHNOLOGY
Vol. 11. No. 4, December, 2023

Article Citation Format
Olebara, C.C. (2023) The SASE (SASSY): Situational Awareness of a Digital Initiative Disruptive Framework
Journal of Digital Innovations & Contemporary Research in Science, Engineering & Technology. Vol. 11, No. 4. Pp 47-64
dx.doi.org/10.22624/AIMS/DIGITAL/V11N4P4
www.isteams.net/digitaljournal.

Article Progress Time Stamps
Article Type: Research Article
Manuscript Received: 24th September, 2023
Review Type: Blind Peer
Final Acceptance: 14th December, 2023

The SASE (SASSY): Situational Awareness of a Digital Initiative Disruptive Framework

Olebara Comfort Chinaza

Department of Computer Science
Faculty of Physical Science
Imo State University,
Owerri, Imo State, Nigeria.
E-mail: chiiprime@gmail.com
ORCID ID: 0000-0002-5891-4206

ABSTRACT

This paper is geared towards presenting situational awareness on a disruptive framework in the cybersecurity field through a short report. This framework is the result of a research by Gartner inc., a technological research and consulting firm. Gartner conducts technology-based research and makes their findings available through conferences or consultancy. SASE pronounced SASSY is an acronym for Secure Access Service Edge. This objective of the SASE framework is to help organizations provide an accessible, cost effective, and latency free service in an era where most organizational functions have been migrated to the cloud and remote working is the new normal. With this migration comes the need a cloud-based security for the organizational data, services, network access. Five cybersecurity tools are proposed in the SASE bundle which are SD WAN, CASB, SWG, and ZTNA. In this paper, the researcher outlines the evolution from the pre COVID enterprise mode of operation to the post COVID mode, describes the SASE framework in detail and present the roadmap. Migration procedures which include installation of SD WAN Controller, configuration of the loading of the routers' and switches' data and control planes into the Software Defined Controller. Having full view of the various offerings of key business security vendors will help business in making informed decisions that will be cost effective, provide required scalability, and also provide feature visibility to users before subscription.

Keyword: Cybersecurity, cloud security, FWaaS, SDN, MPLS, Internet, Edge/cloud computing, SASE, SD WAN, ZTNA, CASB

1. INTRODUCTION

The Migration of companies from traditional network environment to the cloud is a trend ushered in by the COVID-19 pandemic, disrupting the way businesses are conducted and leading to new ways where cloud and cloud-based services are the drivers of the business world (Smith, 2020).
Many businesses failed, while some others that were already using cloud and cloud-based services gained traction. Gartner Inc, is a research and consultancy firm based in Stanford, Connecticut, USA. They conduct technology-based researches and share their findings through consultancy services or keynotes, recommending best practices on the issue under research. Gartner carried out several surveys in 2020, 2021and 2022 with

various questions and on different target groups. Some research questions that addressed business leaders investments are outlined.

The company, in 2020 conducted a survey on 145 business leaders who are decision makers and board of directors across the globe, with the question:

"As a result of the pandemic, where are you going to change your investment and where will you invest strongly?".

The responses showed that 71% of the business leaders will invest strongly in Digital Technology initiatives while workforce, business expansion/diversification, profit improvement, customer engagement, efficiency and productivity, financial, innovation, cost efficiency, mergers & acquisition, business strategy, growth, globalization, manufacturing, and business management had between 14 % - 27 %. This indicates a of wide margin between business leaders intended investment in digital technology initiatives and their investment in any other business sector (Smith, 2020)

In a related survey, the company asked 262 business leaders:

"Please tell us your organization's top 5 business priorities in the next 2 years (2021, 2022.
The result shows that 66% of business leaders have digital technology initiatives as first choice in a sum of five business priorities, with customer engagement, profit improvement, growth, merger & acquisition, globalization, efficiency and productivity, business expansion/diversification, effective business management, manufacturing, and innovation and R & D, coming as first choice in between 11% - 29% of the responses. Digital technology initiatives sector was again rated as the next-gen business investment priority (Wheeler, 2021).

The change in strategic business priorities brought about a hybrid workforce, which is the willingness of employers to have remote workers, with various remote work patterns. Garner, Inc. survey on 127 respondents drawn from Human Resource, Legal, Financial and other fields of business revealed that 82% of respondents say they will allow employees work remote some of the time, 47% will allow permanent remote working mode, 43% will give flex days while 42% will allow flex hours (Baker, 2020). Investment in digital tech initiatives in the post COVID era implies moving with the disruptive technology of cloud services and applications that allow the organizations to participate in the trending business innovations.

All survey results translate to massive migration from traditional business environments, with traditional Networking devices like routers and switches and connections based on Multipoint Label Switching or dedicated circuits to: The cloud where i) hybrid workforce can be better managed ii) configuration of network devices data, control and management planes can be less complex iii) cloud-based application, and services are available and provide cost effective options.

1.1 Cloud-Based Security Needs: Gartner Inc. Proposal

These new business trends call for a shift from the old ways of securing the work environment, where security stack is provided at locations where organizations have presence. There is need for the organizations' Chief Information Security Officers to move its security services where the business now operates from, which is the cloud. Cloud-based security for the cloud applications and services that will be accessed from various locations by remote workers, using various devices as well as the network to and from data centers, public or private cloud storage and the overall organizational communication channels need to be secured. Various applications, and security enforcement points have been developed, with different areas of applications, security targets, and cloud-based resources accessed.

In this paper, the Gartner Inc. proposal is expounded and its extant features highlighted to create better

understanding of the concept, reason migration, and recommendations for intending migrants.

1.2 Security and the Cyber Security Concept and Domains

The term security is associated with safety. The appropriate definition for it depends on the area where it is applied. According to (International Telecommunication Union, 2013), security is the process of maintaining an acceptable level of perceived risk. The authors identified confidentiality, integrity and availability as the features of security.

With respect to information management for data at rest or in transit, it is necessary to ensure that the security features listed above are met. Data at rest include data in organization's data centers to which the organization grants various access levels to employees and vendors/contractors through various connection channels. While data in transit are data packets with the instructions in the network devices' data, control, and management planes, as well as the transport protocols conveying them. The figure 4 below displays the various domains that require protection such as the Application security, information security, network security, operational security, data security(encryption), access control, end-user education, and disaster recovery.

(Seemma et al., 2018) defines Cybersecurity as techniques that are employed to safeguard the cyber environment of a user or organization. The authors further describes cybersecurity as the act of being protected from cyber terrorism, warfare, and espionage. (Vishik et al., 2016) gave a more elaborate definition: "Cybersecurity is the activity or process, ability or capability or state whereby information and communication systems and the information contained therein are protected from and or defended against damage, unauthorized us or modification or exploitation".

In (Craigen et al., 2014) view, the term cybersecurity has no concise definition, hence describing it as the organization and collection of resources, processes and structures used to protect the cyberspace and associated systems. With cyberspace referring to the environment where computer-based communications take place (International Telecommunication Union, 2013), while computer communications in this context is associated with the exchange of data between computers.

2. OVERALL BUSINESS OPERATIONS

In this study, business operations are viewed from the network and security operations of the business operations. Most business enterprises have physical locations as branches of a headquarters, with staff at both the branches and the headquarter. Data is resided on a data centers and accessed though various VPN technologies such as IPSec VPN, or Dynamic Multipoint VPN (DMVPN).

2.1 Pre-COVID Era

Traditional Local Area Network is a data communication that covers a wider geographical area than the local Area network (Vachon & Graziani, 2008). It uses transmission facilities provided by service providers or carriers such as telephone or cable companies, providing network capabilities to support mission critical, data intensive traffic such as video, voice and data (Cisco, 1999),(Vachon & Graziani, 2008). For (NGCLOUDX, 2022) traditional WAN that connects branch offices to headquarters and employs Multipoint Label switching (MPLS) as primary connection while the internet is the secondary connection. IPSec overlays were used to connect the branches to data centers using a point-to-point tunneling. Users (remote workers, vendors, onsite workers) access internet applications by connecting to the data centers through a VPN adapter. At the data center, a firewall enforces

security policies before allowing access to the required internet application such as cloud-based service (AWS, AZURE, Google cloud) or SaaS applications such as Office 365, Zoom, Salesforce. Figure 1 below is a diagram of the traditional WAN connection described, drawn using MS Office tools. (Wallace, 2022) describes the traditional WAN topology with different locations as having physical devices interconnected in an overlay network or physical structure. Each location has physical networking and security infrastructure installed

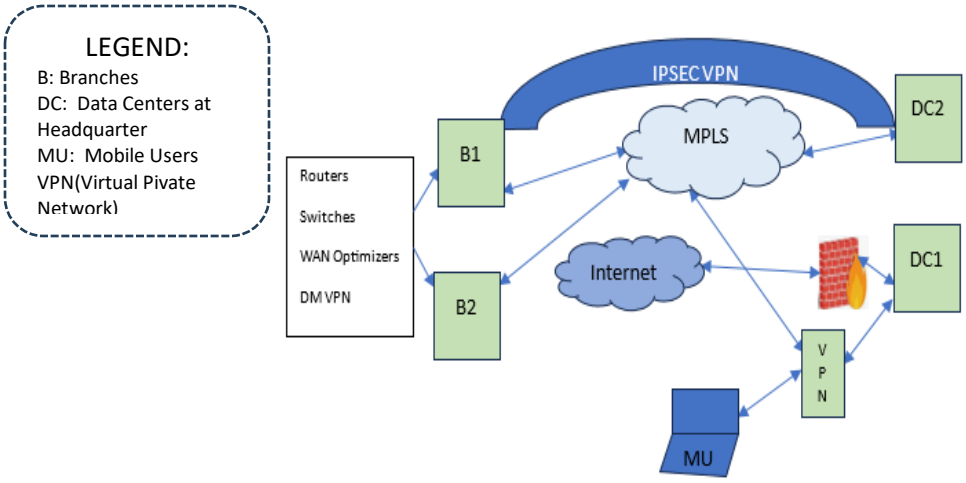

Figure 1: Pre-COVID Business Network. Tool: MS Office (NGCLOUDX, 2022)

(Awasthi & Hardware, 2020) painted a vivid picture of the challenges of migrating from a traditional network environment in post COVID era. The author described the business model with over 100 branches scattered around the globe, with activities that involved downloading rich media content, and about 2000 users. The bandwidth demand was high, and traffic backhaul was evident. Also, low speed tier1 connections following Multipoint Label Switching connections which, though reliable, were cost-intensive considering the low bandwidth, jitters, and latency they produced.

In a traditional communication network, devices such as routers and switches have 3 planes of operation: Data plane which is concerned with getting a frame or packet in one interface and out of the ingress interface as fast as possible (Wallace, 2022). Data planes are designed to be reliable which is achieved by heavily distributing the logic across nodes in the network. When the number of redundant nodes and interconnection are numerous, the traffic is routed through various paths to manage node failure and help the network recover from failure (Mas-Machuca et al., 2020). The authors find providing reliability as described above as being cost-intensive since providing for excess resources is required. The tables used to forward data by the data plane are populated by the control plane. The traditional communication network is presented in figure 2 below:

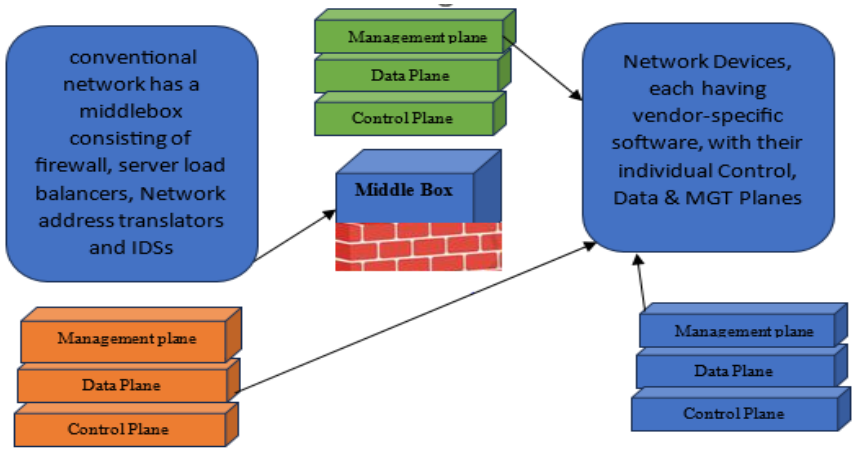

Figure 2: Traditional Communication Network

In a traditional Computer network various network devices communicate with each other using individual vendor-defined software, protocol and interfaces for configuration. The routers, switches and middlebox which consist of server load balances, network address translators and Intrusion Detection Systems and some of the network devices that make network management complex (Schlenker, 2023).

The control plane is where algorithms run, for example, a router runs OSPF(Open Shortest Path First), which is a router protocol used to find the shortest path that packets can use to arrive their destination as they pass through a set of connected networks (Burke, 2020), while the switch runs spanning tree protocol of this plane (Wallace, 2022). The spanning tree protocol defines a root switch and a loop free path from the root to all switches in the layer 2 network. It also ensures that redundant data paths are in blocked state. When there is failure of a network segment in the spanning tree and redundant path is available, the spanning tree recalculates the spanning tree topology and activates the standby path (Cisco, 2019).
In data-control plane interaction, the routers first confirm that the interfaces are in order, after which hello packets are sent over their OSPF interface using Hello protocol to discover neighbors. After routers or systems in an OSPF network ensure that their interfaces are functional, they first send out Hello packets, using the Hello protocol over their OSPF interfaces, to discover neighbors which are routers and system having interfaces to a common network (Ibm.com, 2023). OSPF Hello protocol and database exchange describes an analogy of communication between two systems in the same network. The process from discovering neighbors and establishing adjacency between systems in the same network subnet 9.7.85.0. with both systems having OSPF interfaces 9.7.85.1 and 9.7.85.2 respectively, to the subnet. The subnet belongs to area 1.1.1.1. the phases in the OSPF hello protocol are described (Ibm.com, 2023).

In EXSTART phase, the routers or system (two systems in this example agree on master/subordinate roles, in the second phase, EXCHANGE, the two systems exchange database description packets Link State Advertisements (LSAs) that are not included in the link state of each system. Next is the LOADING phase where each system sends Link State Request Packets to request that the neighbor sends LSAs stored in the retransmission list during the EXCHANGE. The neighbor (a router or another system) responds with LSAs in Link State Update packets. The FULL phase, after LSAs exchange and linking state databases synchronization, adjacency is established between the two systems. (Ibm.com, 2023).

After establishment of adjacency between all systems and routers in an area, each system or router sends an LSA to share its adjacencies and also report its state, which helps the systems or routers discover changes and update their link-state databases (Ibm.com, 2023). The management plane is used to configure a router or

switch. The administrator secure shells into a switch to configure it. In the distributed control plane as described above, the control planes of the devices are distributed in the devices with each device having its own control plane. (Wallace, 202).

2.2 Post-COVID Business Operations: Software Defined Network (SDN)

In SDN, the individual control planes on the network devices are ran inside the SDN controller.

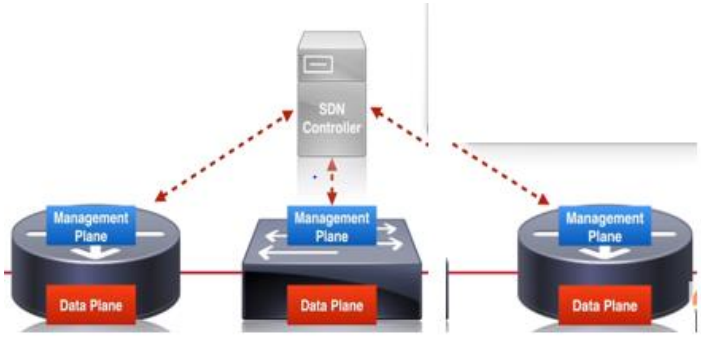

Figure 3: Software Defined Network (Wallace, 2022)

The SDN Controller appliance will be responsible for running all configurations and algorithms, while sending updates information down to the device through Application Programming Interface (API).. the API going from controller down to the device is a south-bound interface. In a drawing of SDN managed devices, the devices are drawn below the SDN-Controller hence the API that sits between them is called South-Bound Interface (SBI) (Suhail & Ajaz, 2022). Example of SBI is CISCO openflow.

Figure 3 above present the SDN controller with devices drawn under the controller. In SDN, administrators carry out intent-based networking, which is the use of http verbs to express their intended configuration on each device using an Application Programming Interface. An intent-based configuration instruction are statements such as how the administrator wants to treat voice traffic or the level of security or the quality of service level he wants to give to an application. The intent-based networking is not carried out on an individual device, but through an application which presents the intent to the controller using a North-Bound API (Wallace, 2022) (Tijare & Vasudevan, 2016). The North-bound API known as REST (Representational State Transfer) API. The information sent to the controller using http verb is formatted using json (Javascript Object Notation).

SD WAN (Software Defined Wide Area Network)

In the migration from traditional network to Software Defined Wide Area Network defined by (Awasthi & Hardware, 2020). In SD WAN a virtual topology is placed on top of the physical topology. In the virtual infrastructure, a logical connection exists between one site and another from the router's viewpoint. This in reality, represents multiple routers in between.

There is a presence of virtual secured tunnels that are set up through the WAN, using the SD WAN controller and since the control plane resides in the SD WAN, all physical WAN connections from Metro ethernet, cable modem or MPLS to cellular , can be defined by educating the SD WAN controller about the technologies, and it will in turn carry out the defined tasks and also send appropriate configuration commands to the routers, since it have knowledge of the routers' features. It also gives the security predictable performance and quality of service that are available in traditional point to point WAN connections (NGCLOUDX, 2022).

Some Cloud-based Security Applications

In this section, a few cloud-based security products will be discussed, as they are the constituents of the proposed framework presented by this paper.
- CASB (Cloud Access Security Broker)
-ZTNA (Zero Trust Network Access
- SWG (Secure Web Gateway)

Cloud Access Security Broker

(Mallick, 2022) defined CASB as software or hardware solution that mediates between two layers that are connected. It mediates between enterprise core (servers, data centres, endpoints and users) and surrounding cloud environment. Is an on-premises or Cloud-based security policy placed between users and cloud-based applications. It consolidates multiple types of security policy enforcement (Gartner inc, 2022).

Features

-Inspects SaaS applications & returns the application IP address if no threat is detected
-Visibility/DLP: tools to control data users can transfer/share
-Configuration auditing: Tools that compare detected changes to approved Request For Changes (RFCs)
-Single Sign-On/Identity Access Management (IAM) tool used by admin to assign single digital identity
-Cloud governance & Risk assessment: CASB provides catalogue of cloud services scoring them according to the risk assessment and trustworthiness level they provide. Figure 4 presents the CASB view.

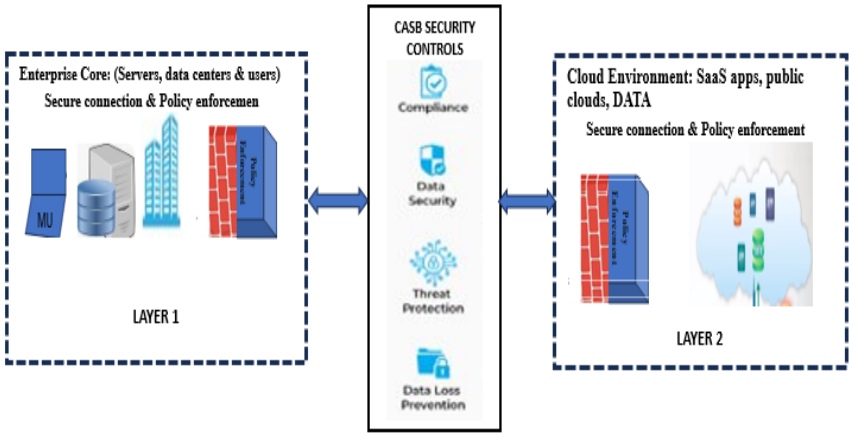

Figure 4: CASB (Gartner inc, 2022)

ZTNA (Zero Trust Network Access)

According to (Skyhighsecurity, 2022) ZTNA enforces granular policies in providing Zero Trust access to private applications that are hosted on clouds and enterprise data centers, by remote workers and devices.

Features

-Runs on Software defined perimeter
-Segregates network access from application access
-zero trust for SSO credentials: grants least access by matching user id, device id & location
-Granular access to application & data instead of network
-Lateral movement not allowed since users are connected directly to the data or application required. ZTNA

structure is presented in figure 5 below

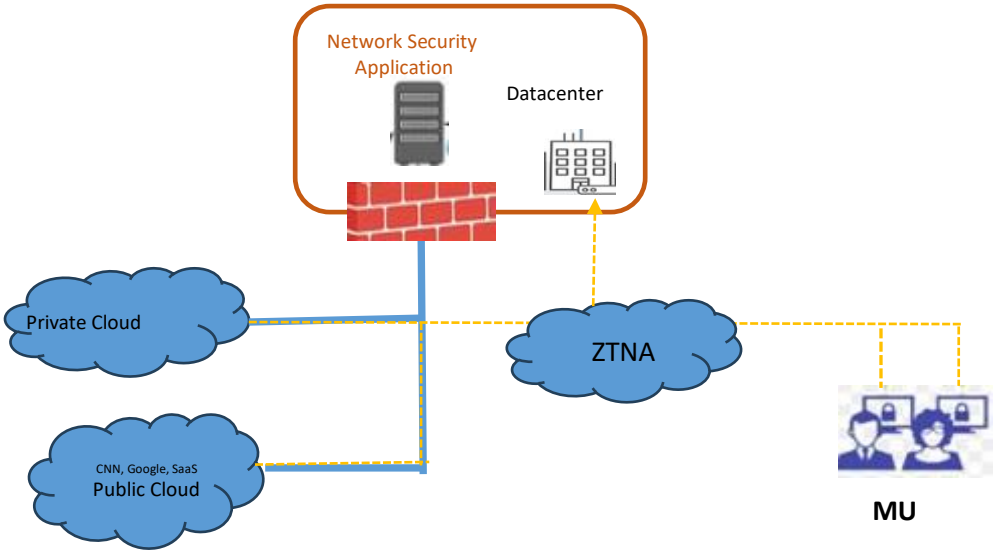

Figure 5: ZTNA (Skyhighsecurity, 2022)

Secure Web Gateway

Enforces policies on: WHEN? HOW?, WHERE?, WHO?, WHAT? internal users interact with the web. 2. inspects webpage content for malware 3. Data Loss Prevention (Inspect outbound traffic in search of phrases that match social security or credit card number or related sensitive information theft, then blocks it to prevent data loss 4. URL filtering using database of known malicious websites. It's main function it to give users a secure internet surfing experience. SWG sits between mobile users, headquarters/data centers, remote locations, firewall at the data centers, and the internet. Figure 6 below presents the SWG.

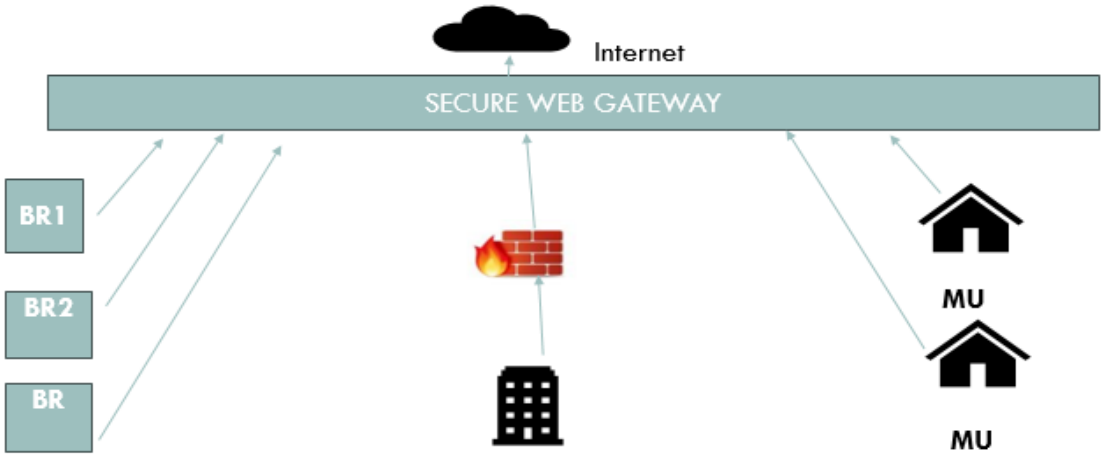

Figure 6: Secure Web Gateway

SD WAN (Software Defined Wide Area Network)

The SD WAN model offers support for on-premises applications hosted in data centers, private or public cloud, such as Microsoft office 365, Zoom, Salesforce etcetera (Arubanetworking.com, 2023).

SD WAN Features

The features of SD WAN Is itemized below. These may differ from vendor to vendor depending weather the vendor gives basic or advanced SD WAN. It is important for organizations to have full view of the features included in the SD WAN offering of a vendor. A checklist of what to expect is itemized below:

-Zero touch (intent-based configuration), support for centralized configuration, enabling fast deployment of changes
-Edge functions such as routing, security services, service chaining to third-party security services, and WAN Optimization.
-Traffic management based on pre-defined rule, programmed using API, with ability for continuous self- learning.
-Consistent Quality of Service Experience(QOEx) as it uses multiple forms of WAN transport to direct traffic to a single path and redirect it if the path fails.
-End-to-end segmentation from LAN-WAN-Data center and LAN-WAN-Cloud. Policy change is programmed centrally using SDN controller and then forwarded to all nodes for update. The SD WAN architecture is presented in figure 7 below

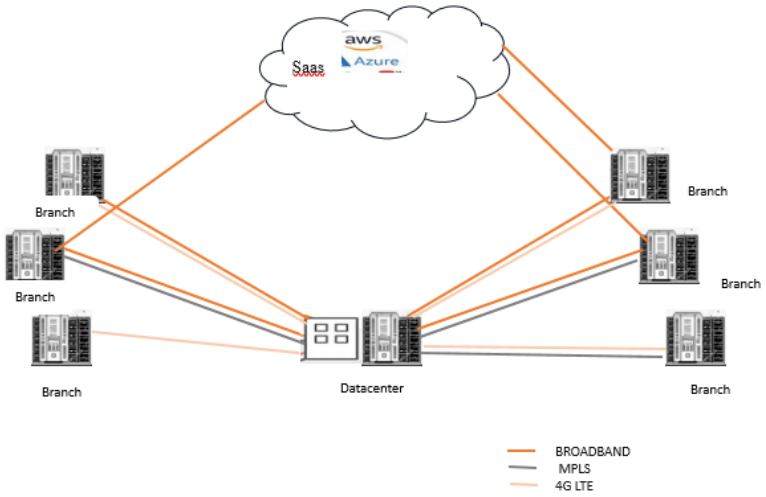

Figure 7: SD WAN Architecture (Arubanetworking.com, 2023)

3. METHODOLOGY

The proposal for a single offering that offers comprehensive cybersecurity services for data communication is presented. SASE is a disruptive framework that was coined in the year 2019 by Gartner Inc., a technology-based research company that carries out IT-based researches and report their findings either through consultancy or keynotes and white papers. The SASE framework is presented in this section and its role to achieving cybersecurity expounded. Migration procedures as well as recommendations for effective and efficient SASE adoption is also given.

The SASE Concept

SASE, an acronym for Secure Access Service Edge pronounced SASSY was coined in the year 2019 by Gartner inc. It is a framework that advocates convergence of some cloud security products instead of purchasing individually as a result of cost, thereby not providing adequate security for data at rest and in transit. The framework is made up of 2 categories: the Network aspect and the security aspect. Table 11 below presents SASE framework concept which is the convergence of network and security services to support organizations' secure access needs. The SASE concept is presented in figure 8 below:

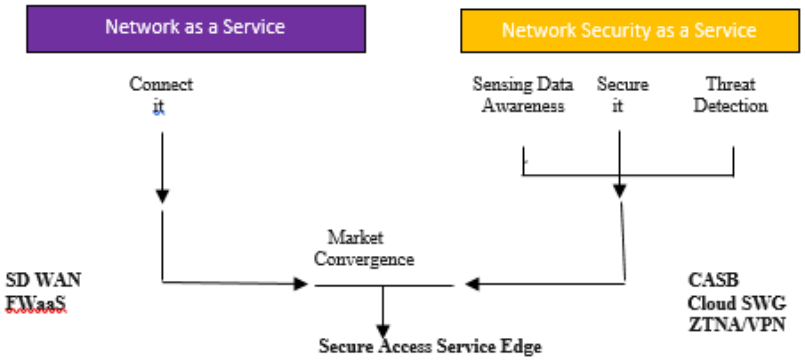

Figure 8: SASE concept (Smith, 2020)

SASE is an edge-based service. Edge platform is a software used for automated deployment, update, and management of distributed applications. Edge computing is computing which implies that it is deployed closer to where data is produced and does not sit fully in the cloud. In edge computing applications are accessed and analyzed on the edge platform, thereby providing high throughput, jitters and latency free experience.

Purpose of SASE

Following the massive migration of business owner to the cloud and cloud-based services, the need arose for security services that will protect the organizations data.

-Gartner survey (Baker, 2020) shows that employers would have many of their workers to work in a hybrid workforce pattern. Putting more workers on remote work mode results in heavy traffic on the traditional network as it has to enforce the security policies before granting each access request. it is necessary for internet to be the primary connectivity so as to have higher bandwidth, less jitters and latency.

Sase Usecases

The SASE framework use cases for the network category are:
SD WAN (Software Defined Wide Area Network)
FWaaS (Firewall as a Service)

SASE framework use cases for Secure Service Edge:

CASB (Cloud Access Security Broker)
ZTNA (Zero Trust Network Access)
SWG (Secure Web Gateway)

These technologies are existing single offerings. SASE proposes having vendors combine the services and offer them as a bundle so that organizations can have all networking and security needs covered and having only organization's business services to worry about.

SASE Implementation

To implement SASE cloud security, the following steps should be followed:
The Chief Information Security Officer (CISO) needs to have clear objectives, a blue print of the security system they want to follow, proper planning on private and public cloud deployments, then implementation of security blueprint and then, final digital transformation. The framework has three layers:

Base layer and two SASE layers

The base layer is the point where actual resources are: Branch offices, mobile users working remotely, contractors, consumers and vendors.

After the base layer, the two SASE layers will follow. The first SASE layer is the SD WAN Layer (Network as a Service) with its accompanying FWaaS (Firewall as a Service). The SD WAN can replace existing on-premise service. The next SASE layer is the Secure Service Edge.

Security as a Service layer.

Traffic from the base layer first comes to the first layer (Network as a Service) where most vendors offer FWaaS with the SD WAN, then to the second layer (Security as a Service) which has Zero Trust Network Access, Cloud Access Security Broker, and Secure Web Gateway, security services. From the security layer the internet, SaaS applications, public cloud services, and data centers, can be accessed. The traffic flow framework described ensures that adequate security is enforced, internet surfing is safe, SaaS applications accessed is filtered by the two layers. Figure 9 presents a conceptual view of the overall organizational architecture with SASE implementation. Conceptual View of SASE Implementation (Office 365 sketch)

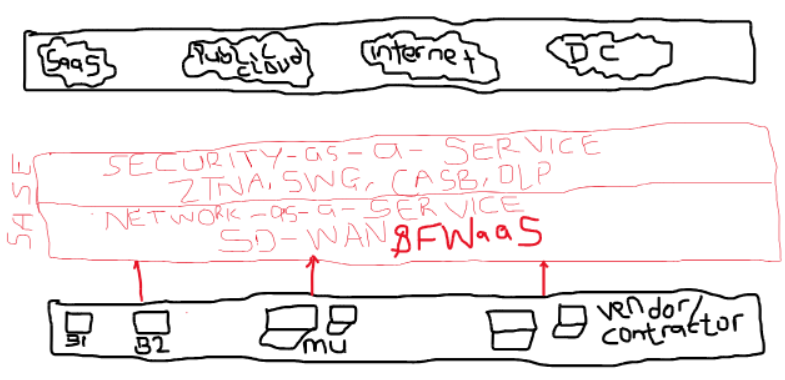

Figure 9: Conceptual Framework of SASE Implementation (Adapted from NGCLOUDX, 2022)

The SASE ROADMAP

The SASE ROADMAP is presented in figure 10 below:

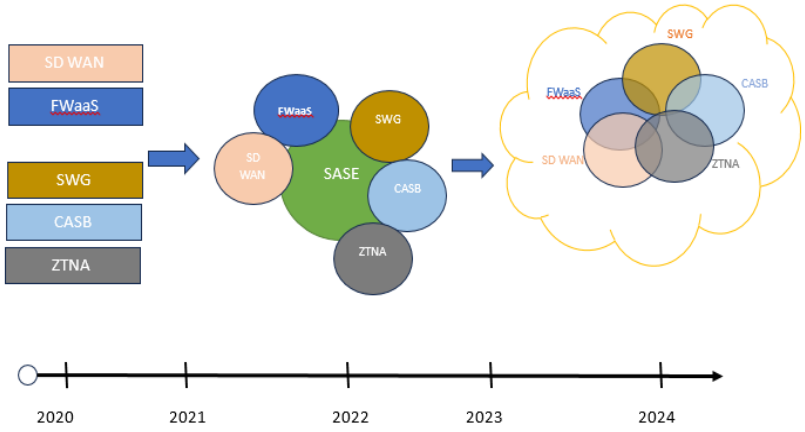

Figure 10: SASE Roadmap (Smith, 2020)

Figure 10 presents the SASE roadmap. In the year 2020, the five selected networking and security products were offered individually. Between 2021 and 2022, there has been move by vendors to have the product bundles. With SD WAN and FWaaS as one bundle and SSE products (CASB, ZTNA and SWG) as a second bundle. Presently (2023) the technological move is towards having a wholesome product that will offer all five products in one unit and without separate subscriptions.

Migrating to SD WAN

The centralization of the control plane of network devices in a software defined Network Controller in what migration implies. The use of Northbound API such as REST(Representational State Transfer) API to carry out intent-based configuration, which is the use of http verbs to state intended configuration choice on a device such as "I want to give this application this level of security and this level of quality of service"(Wallace, 2022). The http verb is formatted using json (JavaScript object network). The SDN controller will run configurations as contained in the intent-based configuration and algorithms, while sending updates information down to the device through a South bound API interface such as openflow southbound API.

The Role of SASE in Cybersecurity

Integrity, availability, and reliability are the major characteristics of cyber security. These qualities, when achieved in applications, information, network, or operations, through employment of tools such as end-user education, access control, access control, as well as disaster recovery techniques result in better user experience. The adoption of SASE's two bundles offering has improved the overall Result On Investment of deploying organizations, as they benefit from being white-listed, having visibility of all organizational activities, as well as having rich bandwidth and secured access. Also, being assessed as trustworthy as other organizations try to access the organization's services will open new business connections and increase consumers' confidence in transacting with the organization. Cyber security
components and the proposed SASE single-buy bundle is presented in figure 11 below.

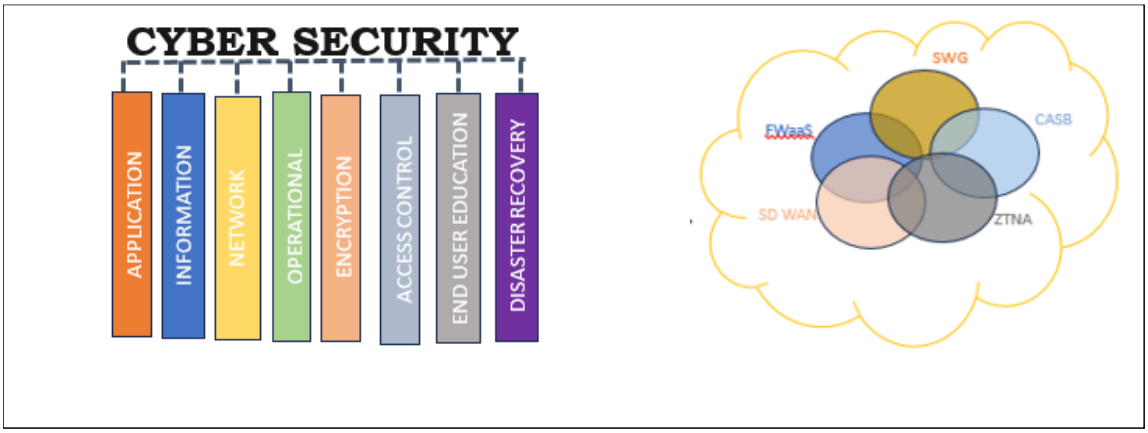

Figure 11: One buy Network/Security solution for organization's cloud-based business management

8. SASE Vendors and their Security Offerings

In this section, key SASE vendors and their Network and Secure Service Edge(SSE) features, as well as other cybersecurity services they offer, is presented.

1. Zscalar

Products:

i) Zscalar Private Access(ZPA) for internal connection to enterprice network
ii) Zscalar Internet Access (ZIA) is Zscalar's solution for connecting users to applications on the internet
iii) Zscalar Digital Experience (ZDX) solution provides end-to-end visibility and troubleshoots enduser performance issues. It provides Network and endpint

POP

Points of Presence(POP) are points where service subscribers connect their edge sites to a SASE vendor for the processing of the customer traffic.
Zscalar has a global footprint of over 150 data center locations

SASE offering

SSE(ZTNA, SWG, CASB)

Security Provisioning

FWaas, Data Loss Prevention, cloud sandbox,SSL inspection, Internet Protocol Security(IPS), DNS, malware protection, web content filtering, Threat prevention.

2. Palo Alto Networks

Products

1. Prisma Access for SSE(ZTNA, SWG, CASB)
2. FWaaS to protect branches
3. Next-generation firewalls (NGFWs)to protect data centers
4. CloudGenix SD WAN rename to Prisma SD WAN to connect sites.

POP

According to TechTarget.com, Palo Alto has over 100 points of presence in 75 countries.

SASE offering

SSE (ZTNA, SWG, CASB)
SD WAN
FWaaS
NGFWs

Security Provisioning

URL filtering, DNS security,IoT security, web content filtering, Threat prevention, Data Loss Prevention, SaaS security,bi directional SSL inspection, policy management, Shadow IT visibility, sandboxing.

3. CISCO

Products

Cisco Umbrella for SSE (CASB, ZTNA, SWG)
Cisco Meraki for SD WAN(supports 4G and 5G only)
Cisco Viptela for SD WAN(supports cellular wireless for load balancing

POP

community.cisco.com defines Point of Presence (POP) as an access point or physical location at which two or more networks or devices share a connection. Cisco has over 200 points of presence.

SASE offering

SSE(ZTNA, SWG, CASB)
SD WAN oferring

Security Provisioning

FWaas, Data Loss Prevention, DNS layer security, SSL inspection, web content filtering, malware protection, SecureX, threat intelligence.
Other SASE vendors providing.

4. CATO Networks

Products

CATO SASE(CASB, ZTNA, SWG)

POP
60

Security Provisioning

FWaas, web content filtering, nextgen malware protection, IPs, Managed Detection and Response (MDR).

5. Netskope

Product

Netskope SSE(CASB, ZTNA, SWG)

Security Provisioning

FWaas, DataLoss Prevention, advanced analytics, IoT security, addition of AI and ML technology for more accurate and cloud app categorization

Other SASE vendors are:

Proofpoint
Baracuda Networks
Menlo security
Cloudflare & Forcepoint.

4. CONCLUSION

This paper presented the challenges faced by businesses all over the world following the COVID-19 lock-down. The migration to the cloud as a business survival strategy, the survey results showing the direction of business investmentsAlso massive migration to cloud and cloud-based services neccesitates provissioning of cloud-based security for businesses. These research outcomes brought about the development of a framework that will make trasitioning to the cloud easy and cost effective. SASE (Secure Access Service Edge) was developed as a five-component framework with Networking capabilities that overides the physical Router and associated configuration challenges into a Software Defined Network that allows configuration to be centralized in a SD Controller, as well as security tripple security offering that covers internet surffing, applications and network access safty, and secure access to cloud-based applcations and services. While providing high bandwidth that eliminates latency and jitters, thereby guaranteeing Quality of Service Experience (QoEx). All domains that require protection will be adequately protected as many of the SASE products have overlapping capabilities including Data Loss Prevention,

Trusthwordiness scoring and segregation between networ and application access. The result indicates that over 70% of CEOs, and top management decision makers will invest I n Digital Tech initiatives.

5. RECOMMENDATIONS

-Transitioning into the SASE framework should be a gradual process. The routers and switches used in the traditional WAN can be used in the transition process by setting a central Software Defined Controller and bringing in all the routers' and switches' data and control planes into the central SD Controller. This way they are no longer configured independently but through the Application programming Interfaces (Openflow or REST) for South-bound and North-bound communications.

-It is important for organizations to have full view of the features included in the products offered by a vendor. Is the SD WAN basic or advanced. Some vendors choose to offer either the Network end alone (ZScalar) or both the network and the security (CISCO).

Knowledge of a vendor's Points of Presence (PoP) is necessary in this era of remote working. Remote workers should endeavor to adopt global best practices that ensure cyber hygiene(Olebara, 2022), (Ukwandu et al., 2023), (Ugwu et al., 2022)

Bust ability issues refer to how scalable the vendor's products are, in case of company expansion and site/location addition.

REFERENCES

Arubanetworking.com. (2023). What is SD-WAN? https://www.arubanetworks.com/faq/what-is-sd-wan/#:~:text=Unlike the traditional router-centric,the highest levels of application

Awasthi, A., & Hardware, R. (2020). Journey From Traditional Network to SD-WAN. April.

Baker, M. (2020). Gartner Survey Reveals 82% of Company Leaders Plan to Allow Employees to Work Remotely Some of the Time Now Organizations Must Manage a More Complex, Hybrid Workforce. https://www.gartner.com/en/newsroom/press-releases/2020-07-14-gartner-survey-reveals-82-percent-of-company-leaders-plan-to-allow-employees-to-work-remotely-some-of-the-time

Burke, J. (2020). DEFINITION OSPF (Open Shortest Path First). https://www.techtarget.com/searchnetworking/definition/OSPF-Open-Shortest-Path-First#:~:text=Routers connect networks using the,a set of connected networks.

Cisco. (2019). Spanning Tree Protocol. https://content.cisco.com/chapter.sjs?uri=/searchable/chapter/content/en/us/td/docs/ios-xml/ios/lanswitch/configuration/xe-16-7/lanswitch-xe-16-7-book/lsw-span-tree-prot.html.xml

Cisco, S. (1999). Introduction to WAN Technologies • Technologies Take-Away Message. 1–27.

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining Cybersecurity. Technology Innovation Management Review, 4(10), 13–21. https://doi.org/10.22215/timreview835

Gartner inc. (2022). Cloud Access Security Brokers (CASBs). https://www.gartner.com/en/information-technology/glossary/cloud-access-security-brokers-casbs#:~:text=Cloud access security brokers (CASBs) are on-premises%2C,cloud-based resources are accessed.

Ibm.com. (2023). Open Shortest Path First. https://www.ibm.com/docs/en/i/7.4?topic=routing-open-shortest-path-first

International Telecommunication Union. (2013). Introduction to security cyberspace , cybercrime and cybersecurity. Africa Cert. https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Introduction to the Concept of IT Security.pdf

Mallick, C. B. (2022). What Is a Cloud Access Security Broker? Definition, Pillars, Architecture, and Uses.

Mas-Machuca, C., Musumeci, F., Vizarreta, P., Pezaros, D., Jouët, S., Tornatore, M., Hmaity, A., Liyanage, M., Gurtov, A., & Braeken, A. (2020). Reliable Control and Data Planes for Softwarized Networks. July 2021, 243–270. https://doi.org/10.1007/978-3-030-44685-7_10

NGCLOUDX. (2022). Prisma Access Overview | Palo Alto Prisma Training | SASE Training.

https://www.youtube.com/watch?v=MOKFhEbKFns

Olebara, C. C. (2022). Researchers ' Cyber First-Aid. Journal of Emerging Technologies (JET), Volume 2(Issue 2), 42–54. https://journals.jozacpublishers.com/jet/article/view/195

Schlenker, M. (2023). Software Defined Networking (Part 1). https://www.omscs-notes.com/computer-networks/software-defined-networking-part-1/

Seemma, P. S., Nandhini, S., & Sowmiya, M. (2018). Overview of Cyber Security. Ijarcce, 7(11), 125–128. https://doi.org/10.17148/ijarcce.2018.71127

Skyhighsecurity. (2022). What is Zero Trust Network Access (ZTNA)? https://www.skyhighsecurity.com/cybersecurity-defined/what-is-ztna.html

Smith, N. (2020). (251) Gartner Keynote: Cloud Security, Managed Services & SASE and Preparing for the Future - YouTube. https://www.youtube.com/watch?v=3gCqUjy_MV0&t=1545s

Suhail, A., & Ajaz, H. M. (2022). SDN Interfaces: Protocols, Taxonomy and Challenges. International Journal of Wireless and Microwave Technologies, 12(2), 11–32. https://doi.org/10.5815/ijwmt.2022.02.02

Ugwu, C., Ani, C., Ezema, M., Asogwa, C., Ome, U., Obayi, A., Ebem, D., Olebara, C., & Ukwandu, E. (2022). Towards Determining the Effect of Age and Educational Level on Cyber-Hygiene. Proceedings of the 2022 IEEE Nigeria 4th International Conference on Disruptive Technologies for Sustainable Development, NIGERCON 2022, May. https://doi.org/10.1109/NIGERCON54645.2022.9803154

Ukwandu, E., Okafor, E. N. C., Ikerionwu, C., Olebara, C., & Ugwu, C. (2023). Assessing Cyber-Security Readiness of Nigeria to Industry 4 . 0. Springer Nature Singapore. https://doi.org/10.1007/978-981-19-6414-5

Vachon, B., & Graziani, R. (2008). Accessing the WAN CCNA Exploration Companion Guide.

Vijay Tijare, P., & Vasudevan, D. (2016). IJESRT INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY THE NORTHBOUND APIs OF SOFTWARE DEFINED NETWORKS. © International Journal of Engineering Sciences & Research Technology, 501(October). https://doi.org/10.5281/zenodo.160891

Vishik, C., Matsubara, M., & Plonk, A. (2016). Key Concepts in Cyber Security: Towards a Common Policy and Technology Context for Cyber Security Norms. International Cyber Norms: Legal, Policy & Industry Perspective, 221–242.

Wallace, K. (2022). SDN, SD-WAN, & SD-Access Simplified... Seriously!

Wheeler, J. A. (2021). IRM Remains Gartner Top Emerging Tech Topic in 2021. https://blogs.gartner.com/john-wheeler/irm-remains-gartner-top-emerging-tech-topic-in-2021/

https://docs.paloaltonetworks.com/prisma/prisma-access/3-1/prisma-access-panorama-admin/prepare-the-prisma-access-infrastructure/list-of-prisma-access-locations

https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/autonomous-dem/autonomous-dem-administration.pdf

https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/prisma-access/prisma-access-administration.pdf

https://www.techtarget.com/searchnetworking/tip/The-pros-and-cons-of-Palo-Alto-Networks-SASE-platform

https://www.techtarget.com/searchnetworking/tip/The-pros-and-cons-of-Palo-Alto-Networks-SASE-platform

https://community.cisco.com/t5/network-management/different-between-central-office-and-point-of-presence/td-p/4095504