# Secure Access Service Edge: A Zero Trust Based Framework For Accessing Data Securely

Silafu Yiliyaer
Department of Computer Science
University of Nevada Las Vegas
Las Vegas, NV 89154, USA
yiliyaer@unlv.nevada.edu

Yoohwan Kim
Department of Computer Science
University of Nevada Las Vegas
Las Vegas, NV 89154, USA
Yoohwan.kim@unlv. edu

*Abstract*— **With the growing demand for moving work from home, organizations need to allow more workers to access their private networks through the employer's local Internet. This leads to higher costs to enforce the homeworker access to the organization's resources privately and securely through designated devices and services. Also, the connection latency to the organization's private network over a large group of people can be an issue. Secure Access Service Edge, a framework that bundles many networks utility and security functions at the edge of the cloud to reduce the cost and maintenance for organizations to deploy their network strategy. It also boosts the connection performance of different services for remote workers. SASE uses Zero Trust Architecture as its backbone, without trusting any device or user but authenticate and authorize at each request. Direct the traffic with SD-WAN to the resource. Applying checkpoint functions like Secure Web Gateway and Cloud Access Security Broker to further enforce the security of the organization's assets that lie in the cloud. By the end of this paper, you will understand how those techniques mentioned before work together under the SASE framework to improve organizations' network connections and security.**

***Keywords—Secure Access Service Edge, Zero Trust Architecture, Software Defined Wide Area Network, Secure Web Gateway, Cloud Access Security Broker, Cloud Computing***

## I. Introduction

In most recent years, cloud computing has become one of the favorite technologies for organizations to have. From storing data assets to applying artificial intelligent services. The functionality of the cloud kept driving more companies to apply and adapt to it. According to a 2020 report, more than 90% of global enterprises will deploy a hybrid environment [1]. Another report in the same year found that 97% of IT managers planned to utilize more than one cloud to distribute their workflow to achieve a robust, resilient, and regulatory workspace [2]. In addition, this pandemic has impacted not only the social lifestyle but also the regular setup of a company. More people either have decided or were forced to work at home. Organizations must come up with new plans to satisfy the need for remote working. Flexera 2021 State of the Cloud Report shows that 90% percent of enterprises expect cloud usage to exceed prior plans due to COVID-19, and 50% of them confirm that it will increase [3]. This includes the increased expense of securing their assets in the cloud and private network. Global workplace analytics survey revealed that 69% of U.S. employees worked remotely at the peak of the pandemic. In the other survey, 82% of U.S. employees want to work remotely at least once a week when the pandemic is over [4].

Virtual Private Network (VPN) and Multi-Protocol Label Switching (MPLS) have dominated the private network environment over the past decade. A VPN is an encrypted point-to-point connection within a physical network. An MPLS is a technique that abstracts away the IP forwarding which costs more time and uses label forwarding instead within a private network where every router knows the other router's label. In a traditional remote working setup, VPN and MPLS were used to establish a secure and fast connection between the server in the company's Head Quarter (HQ) and off-premises users. After the user request is being approved, the HQ will retrieve the target resource either in a local datacenter or private cloud, and then send it back to the end-user. This process introduces more latency in exchange for increased security, it will also be very costly when large numbers of people work remotely. MPLS private network is 100 times more costly than regular broadband Internet. And VPN is cheaper but charges fees according to the number of users that are connecting to their private server. The expense to upgrade the network due to more people working remotely will be very costly. To alleviate this issue, Gartner brought a concept called 'Secure Access Service Edge' in its August 2019 report The Future of Network Security in the Cloud [5].

In SASE, organizations distribute *inspection points* to various regions over the Internet so that end-user can access the company's assets anywhere at any time with security policies enforced, shown in Figure 1. This greatly reduces the burden of the organization's network compared to the MPLS and VPN network where all traffic is backhauling towards the organization's private central inspection point which increases congestion and latency when there are large amounts of the remote workforce. SASE starts with Zero Trust Architecture (ZTA) security model [6]. It erases the difference between the private network and the public network. Every request will be verified first as if it is being sent by an untrusted subject. After approval, the connection between end-user and resource will be established with the help of Software-Defined Wide Area Network service [7]. This will ensure that the connection is efficient and encrypted. SASE also leverages the Secure Web Gateway (SWG) [8] system as a checkpoint to make sure that no malicious network traffic either enters or leaves an organization.

When the request reaches the resource in the cloud or the private network, the Cloud Access Security Broker (CASB) [9] will enforce the organizations' policies and monitor the activities.

With SASE in place, all access will be direct access from end-user to resource. It aims to reduce the network complexity, latency, and cost for the enterprise [10]. In the meantime, provide easy implementation and maintenance. Combine with multiple security services, the organization's assets will be safely accessed through both private and public networks.

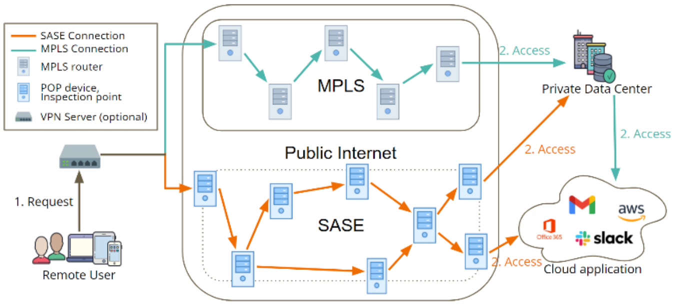

Fig 1. Comparison between the private MPLS, VPN model vs SASE framework.

In this paper, we will review the core components of SASE framework including Zero Trust Architecture, SD-WAN, Secure Web Gateway, and Cloud Access Security Broker. Then we will illustrate how SASE can be deployed in organizations and how it operates. We will then discuss how the SASE core components work together to prevent attacks, challenges in implementing SASE, the transition to SASE from traditional system, and how SASE can aid machine leaning. For a quick reference, we have summarized the acronyms used in this paper in Table I.

TABLE I. LIST OF ACRONYMS

| Abbreviation | Acronym |
|---|---|
| VPN | Virtual Private Network |
| MPLS | Multi-Protocol Label Switching |
| HQ | Head Quarter |
| SASE | Secure Access Service Edge |
| ZTA | Zero Trust Architecture |
| SD-WAN | Software Defined Wide Area Network |
| SWG | Secure Web Gateway |
| CASB | Cloud Access Secure Broker |
| MFA | Multi-Factor Authentication |
| PKI | Public Key Infrastructure |
| OS | Operation System |
| SDP | Software Defined Perimeter |
| POP | Point Of Presence |
| DLP | Data Loss Prevention |
| URL | Uniform Resource Locator |
| ISP | Internet Service Provider |

## II. FEATURES OF THE SASE FRAMEWORK

### A. *Zero Trust Archetecture (ZTA)*

ZTA is an architecture that uses a set of guiding principles for workflow, system designs, and operations to minimize the threat. All devices and users are considered as potential malicious attackers when initiating the request. Based on its principle [6], four layers of protection should be in place:

- Verify Every User: User can be of many. Either company's employees or related personnel. When they are accessing a resource, ZTA will first check their user identification, this could be several factors such as username/password, text message, phone call using Multi-Factor Authentication (MFA), and a certificate that is provided by an enterprise owned Public Key Infrastructure (PKI).

- Verify Every Device: When working on-site, even though organizations have their policy to enforce users to use managed devices that are been provided, a personal device like a cell phone can still access its private network which will prompt a threat to the company. When working remotely, this issue will be enlarged if the user device that is connected to the private network is un-managed [11]. In order to protect private assets from every angle, ZTA verifies every device that is connected to. This includes Operating System (OS) name, version, software used, patch level, location of the device, and other relative data.

- Enforce Least Privilege: This means whenever a request is being approved, ZTA will check the user info, access level, footprints over the private network, and their device security level, and then give the least privilege to access the necessary asset. It will restrict both visibility and accessibility, therefore minimizing the threat.

- Collect Information: One of the most important functionalities of ZTA is information collection. Since ZTA considers every end-user as a threat, following their footprint is a key to alert by the potential malicious action. It will also provide enough data to refine the enterprise network policies and the end user's privilege. It is done by a program called Authentication Manager located in one of the private datacenters. It collects these incoming data and analyzes them in real-time. Whenever a suspicious activity occurs in any device, it will send an updated security policy to that device where it can behave accordingly to stop that malicious behavior.

ZTA has different implementations. One of the best choices for the SASE framework will be the Device Agent/Gateway Model. This approach is sometimes referred to as Software Defined Perimeter (SDP) [12]. It redefines the traditional perimeter-based security where hackers can easily access other resources within the same private network once they break through the outer layer security mechanism. This causes lateral damage to the organization. With ZTA, every resource either in the private or public network requires authentication and authorization whenever they are accessed [13], shown in Figure 2. This approach mitigates the most common network-based attacks by unauthorized users [14]. ZTA will be performed every time when each individual resource is being requested. It will apply the verification by the policy only for that resource and start the connection after approval. It is also integrated into many blockchain-based security measurements [15], especially in a vehicular ad-hoc network [16].

### B. *Software Defined Wide Area Network (SD-WAN)*

SD-WAN has a similar ideology as SASE. It manages connections between each application within organizations private and public could. It reduces the need for network traffic back to the central data center which reduces the saturation over enterprise private networks. It also optimizes the traffic flow to reduce the bandwidth in the network [17]. Encryption can be performed between end-to-end connections.

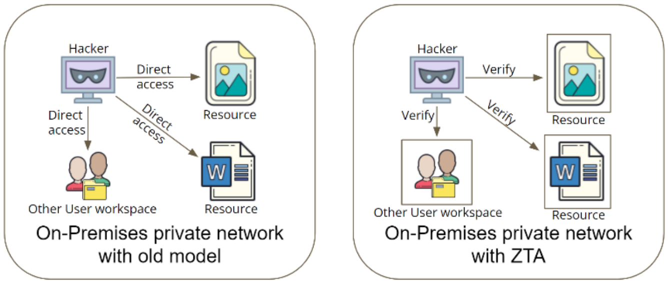

Fig 2. Traditional private network on the left vs the private network with Zero Trust Architecture on the right.

SD-WAN uses software to configure the traffic path instead of just relying on the router, just like building a virtual pathway over many real physical network connections between different devices. It allows organizations to have full control over how their traffic is being delivered and intelligently pick the best path for each traffic. This is archived by setting up many Point-of-Presence (POP) devices at the edge of the public Internet. These devices can be SD-WAN routers and Inspection devices. All these devices send their status and records constantly to the Authentication Manager where it analyzes the traffic flow and user behavior to prevent network congestion [18] and malicious activity, shown in Figure 3.

With the booming of cloud computing, SD-WAN has also evolved to 3.0 which is also called "SD-WAN as a service". Technology providers place SD-WAN software and devices at multiple POP locations over the public Internet. So that without an MPLS network, SD-WAN can still provide all its functionalities.

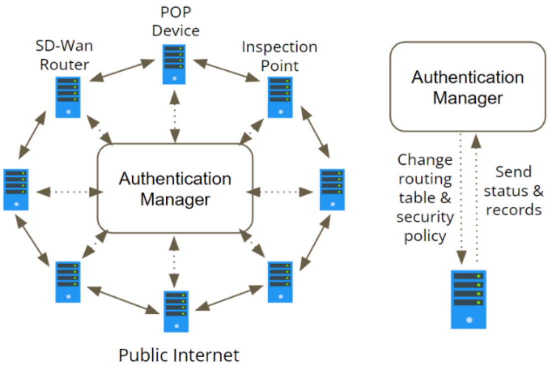

Fig 3. SD-WAN strategy over Public Internet with many POP devices on the edge.

It also provides a Data Loss Prevention (DLP) mechanism for the organization. By scanning the entire organization network, it will intelligently route traffic to a lesser congestion path. When important communication is being established, SD-WAN can aggregate the traffic into multiple connections so that it will not affect the communication if any connection is lost.

SASE leverage the benefit of SD-WAN in a single corporate environment which connects all their assets within a private and public cloud. It also builds robust security measurements while SD-WAN carrying out the traffic.

### C. *Secure Web Gateway (SWG)*

SWG is a semi firewall system that protects employees from accessing malicious content over the private network. Protect your network been accessed by software/malware traffic from entering. It also provides Uniform Resource Locator (URL) filtering for malicious code detection. It enforces the organization's policies [8].

Within the SASE framework, SWG can partner up with ZTA by applying its security policy to further inspect the traffic flow and record their behavior. Combining it with SD-WAN will enforce every traffic flow to organizations' assets meets their security requirements and drop unwanted threats, as shown in Figure 3.

The fundamental difference between SWG and a firewall is that firewalls automatically drop, and pass traffics based on the policies placed on them. Whereas traffic in SWG is monitored and recorded to make policy changes. It is a complementary technology for a firewall which is a powerful security tool to prevent danger to the network at any time. SWG applies security policies dynamically and analysis the intention through the user behavior. These two and other security methods can work together to provide robust and clean network connections [19].

### D. *Cloud Access Security Broker (CASB)*

CASB is the last fortress of this journey. It is one of the endpoint protection mechanisms which is also programable. It lies on the cloud where it connects to various cloud applications to monitor both end-user and corporate data. Organizations are also implementing it for on-premises data because of its data protection functionalities.

Whenever a request is being made by the end-user, the traffic passes all the inspection points to reach the data center. Before it gets its desired resources, the CASB will first direct the traffic to itself for more inspection. It scans packets for any malicious activities. It then enforces the least privilege based on the user category. Connection with resources will be made after all the checkups are performed and no treats are found. It also enforces security policies to data at rest, stopping any access and download for sensitive data.

Combining it with many other endpoint protections will provide greater security functionalities for the data at rest.

It can team up with ZTA in the SASE framework to monitor and record the behavior of the traffic and apply security policies in the cloud [20].

## III. SASE DEPLOYMENT AND OPERATION

In this section, we will illustrate the process of deploying a simple SASE framework with all the technologies introduced above. Since SASE is a framework so there will be many other implementations based on the requirements of organizations. It involves many other technologies besides those four that we have introduced earlier.

One of the SASE framework agendas is to put security inspection points over the Internet instead of just relying on a dedicated server within organizations. In this way, any access can be reviewed at any location at any time by the closest inspection point which saves time and effort. The security policy in each inspection point will be the same as the one on the dedicated server.

ZTA is the backbone of the SASE framework. Every connection that is being made either on-premises or by remote users and devices must be verified first. Many modern attacks have been done by insider attacks. This shows us threats also appear in the organization’s private network. ZTA naturally mitigates these types of threads due to its concept which is “trust no one but always verify”. This policy applies to on-premises users and devices.

When a user registers themselves to any organization, information exchange will be performed by both parties. User will send their own and device information (like password, phone number, OS name, patch level, etc.) to organizations. The Organization will send a certificate from their private PKI to users, and the least privilege will be given to them. After this process, users can access the organization’s data with the privilege that applies to them. Each time a request sends to any inspection point on the Internet, the requested party will be first authenticated with MFA methods and other credentials that can indicate who that user is. The device being used by that user is also going to be checked to prevent any malicious activities initial its communication with the organization’s assets by a compromised device, as shown in Figure 4.

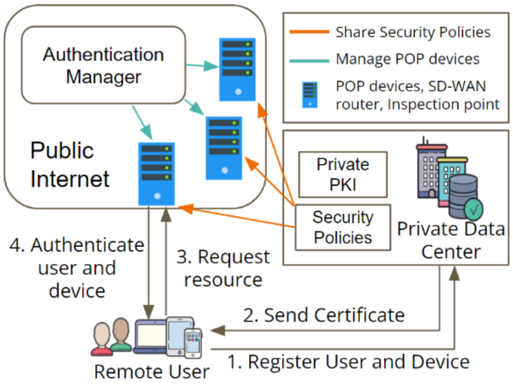

Fig 4. Authentication process

Once all the authentications are done, the traffic from that user will be inspected. This is where all types of Firewalls and Secure Gate Way are put into work. Firewalls will block all the unwanted traffic based on pre-defined policies upon them, whereas SWG will inspect any malware and malicious code within the traffic. SWG will also start monitoring the traffic and report it to the information collector in HQ or any other dedicated location. When the traffic passes through all Firewalls and SWG, it will be sent to the SD-WAN router. SD-WAN router will check the packet type, how important the communication is, its destination, and network status to find the best pathway for this packet to travel through either private or the public Internet. It will also provide many data loss prevention functionalities to protect the integrity of the communication. Encryption can be performed between multiple Point of Presence locations, as shown in Figure 5.

When the traffic reaches the data center either in the cloud or HQ, CASB will act as a gatekeeper in front of the required resources. The CASB will first redirect the traffic to itself and inspect it to detect any malware and malicious code. It will stop any action that downloads the sensitive data. It applies the least privilege to users so they can only see and use what they can base on their role. After the inspection is performed, the connection will be formed by the resource and the user. CASB will still monitor the resource in case any malicious activity occurs. It also sends the behavior records of that traffic for the Authentication Manager to further inspection, as shown in Figure 6.

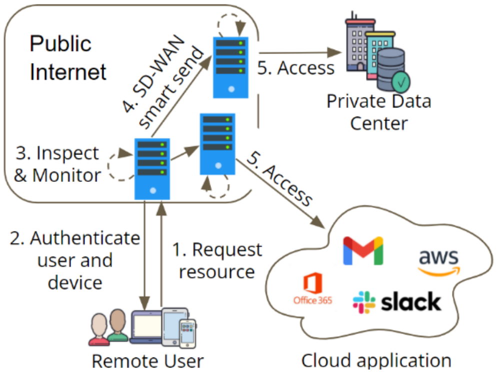

Fig 5. Routing and Inspection

Finally, users will get what they requested after all these processes are finished. That does not mean these users are clean and can proceed without any inspections. The SASE framework will keep authenticate these users and inspect their traffic every time they communicate with organizations. This is also the fundamental principle of ZTA which treats everyone as a suspicious party.

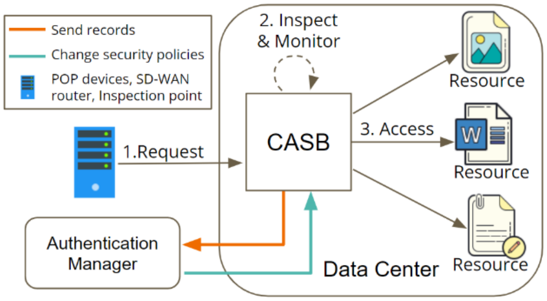

Fig 6. CASB as a gatekeeper.

## IV. Discussions

### A. *Defense-in-Depth in SASE*

ZTA can prevent many suspicious activities by trusting no one and verifying them whenever they communicate with the organization through broadband Internet. This is very effective against lateral threat movement within a private network like insider attack. This type of threat has increased in size in recent years. With ZTA, even the on-premises access will be verified before it accesses resources somewhere else inside the network. SWG will tag along with Firewalls and other defense mechanisms to prevent many other types of attack. They protect the resources by eliminating the malicious packet before they get to their destination. CASB's role is to be a gatekeeper in between any traffic and their targeted resource. It performs an endpoint defend mechanism. It is the last place to detect any suspicious traffic. It also 'knows' what type of resources reside in its environment and applies policy enforcement to them and the traffic so that only applicable resources are visible to the requested user. SD-WAN on the other hand act as a captain within the network to guide traffic to their destination smoothly.

### *B. Obstacles in SASE*

ZTA-based SASE needs to authenticate users in every move that they take, not to mention the number of inspection points along the way of accessing resources. This chain process will create lots of latency and reduce user experience. But it has to be in this way since every traffic pass through the public Internet where malicious parties can initial attacks at any point. However, technology is evolving very fast, hardware is becoming more and more powerful, the Internet speed is nothing like 10 years ago and better methods are developed to break through the bottleneck. Also, using micro-segmentation to group different datacenters, cloud environments, and different physical regions creates a group structure where you can apply the ZTA process just once in each group is another option [21]. Organizations that are willing to use SASE solutions will benefit from these evolving technologies and have more control over their network.

There are many other techniques that can be placed into this framework besides ZTA, SD-WAN, SWG, and CASB. These other technologies offer more visibility to organizations' public and private networks give them more control over how their connections work. They also provide a variety of security functions to further ensure the safety of organizations' assets. But the downside is that organizations need to purchase devices that are capable of these functions like SD-WAN, SWG, and many others. Also, security vendors which provide these functions will buddle up some of them in order to provide full SASE support. These are some of the additional expenses for companies. Although it looks like more things to pay it is still way cheaper than a stand-along MPLS network, and vendors might give a good deal with more functionalities.

### *C. Transition to SASE*

Private networks like MPLS and VPN still have their own benefits compared to the SASE framework. MPLS has been implemented by many organizations. It has a very robust environment. Transmission within the MPLS is much faster. These will still be one of the go-for reasons for MPLS by many organizations that are capable of affording the service fee. VPN on the other hand is also very popular due to its pricing and convenience. It is a lot cheaper than MPLS but also provides strong security. It is easy to implement. It is the best option for small businesses in the market. Large corporations will combine these two types of private networks and deploy them strategically to reduce the overall expense and utilize their advantages within their network.

SASE is a newer model that needs more tryouts to test its robustness. According to a survey from Versa Networks, 34% of businesses claim that they already implemented the SASE framework, and an additional 30% say they are planning to adopt it within the next 6 to 12 months. Despite its growth in recognition, the survey also shows that 69% of the IT and security professionals are not clear what the SASE does and how it does it. We think there might be at least 2 reasons for that: First, the SASE framework is a very new strategy and companies are forced to change their deployment during the pandemic. These lead them to choose technologies that are familiar and reliable in a short chaotic time span. Second, the SASE framework is like a Lego, where users can construct it with many different pieces. It is not an easy task to build up to something you desired out of many different choices. But, with more organizations adopting it, people will see the overall benefits of using the SASE framework, therefore, implementing it themselves. It is just a start.

Internet Service Provider (ISP) AT&T provides SD-WAN services [22] that start with only $219 per month. Many other vendors provide SASE framework like Cisco [23], Fortinet [24], VMware [25], Zscaler [26], and Cato Networks [27].

### *D. Machine Learning with SASE*

Most of the programs that lie on different devices in the SASE framework are featured with programmability. This leads to a possibility of infusion with Machine Learning technologies which are taking critical roles in cybersecurity attack detection in recent years [28]. The Authentication Manager within the organization's network is the best fit for this task. It collects all records from different source devices and applications for analytic purposes which can also be fed to a machine learning algorithm. This algorithm can then be used to detect any suspicious activity [29] and alert the organization in real-time, as shown in Figure 7. It can form an automatic pipeline where it updates the entire or partial network security policies and enforces the targeted devices or applications to take action regarding the threat. In 2021, Artificial Intelligent is more used in the field of cybersecurity. The SASE framework provides strong support for this infusion.

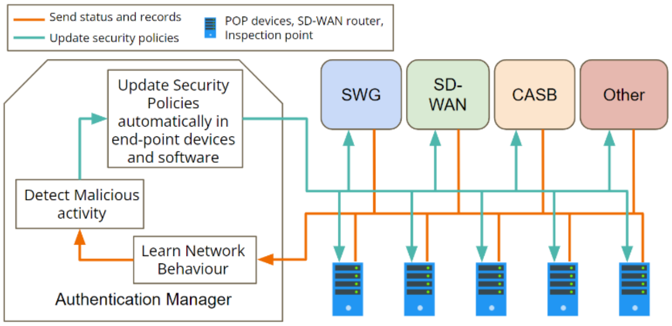
Send status and records
Update security policies
POP devices, SD-WAN router, Inspection point
Update Security Policies automatically in end-point devices and software
Detect Malicious activity
Learn Network Behaviour
Authentication Manager
SWG
SD-WAN
CASB
Other

Fig 7. Machine learning with the SASE framework

## V. Conclusion

The SASE framework consists of many different technologies. Combining which component together is the choice for organizations to make based on their requirements. In this paper, we showed cased this newer broadband communication model that provides cheaper deployment and stronger security measurements. We also discussed how Artificial Intelligent can contribute to it and make it capable of archiving a fully automated smart network that reduce latency and faster reaction towards many types of malicious attack.

## VI. References

[1] International Data Corporation, “IDC expects 2021 to be the year of multi-cloud as global COVID-19 pandemic reaffirms critical need for business agility ,” March 31, 2020.

[2] Business Wire, “Infrastructure and security challenges threaten multi-cloud and edge deployments, new survey from Volterra shows ,” March 9, 2020

[3] Flexera 2021 State of the Cloud Report, https://info.flexera.com/CM-REPORT-State-of-the Cloud?lead_source=Website%20Visitor&id=Blog, Accessed on Dec. 20, 2021

[4] Global Workplace Analytics, “Telework in the 21st Century”, https://globalworkplaceanalytics.com/telecommuting-statistics, Accessed on Dec. 20, 2021

[5] Invest Implications: ‘The Future of Network Security Is in the Cloud’, 13 September 2019, Gartner, https://www.gartner.com/en/documents/3957375/invest-implications-the-future-of-network-security-is-in, Accessed on Dec. 20, 2021

[6] Rose, Scott; Borchert, Oliver; Mitchell, Stu; Connelly, Sean, "Zero Trust Architecture", August 10, 2020, https://www.nist.gov/publications/zero-trust-architecture, Accessed on Dec. 20, 2021

[7] Sebastian Troia, Ligia Maria Moreira Zorello, Guido Maier (2021). *SD-WAN: how the control of the network can be shifted from core to edge*. 2021 International Conference on Optical Network Design and Modeling (ONDM), Gothenburg, Sweden

[8] Gartner, “Definition of Secure Web GateWay”, https://www.gartner.com/en/information-technology/glossary/secure-web-gateway, Accessed on Dec. 20, 2021

[9] Shahnawaz Ahmad, Shabana Mehfuz, Javed Beg (2020). *Securely Work from Home with CASB Policies under COVID-19 Pandemic: A Short Review*. 2020 9th International Conference System Modeling and Advancement in Research Trends (SMART), Moradabad, India

[10] "The Network for the Digital Business Starts with the Secure Access Service Edge (SASE)". *Cato Networks*. https://go.catonetworks.com/The-Network-Starts-with-SASE.html, Accessed on Dec. 20, 2021

[11] BYOD Security – The “Managed vs. Unmanaged” Device Strategy. https://www.bitglass.com/blog/how-to-address-the-byod-security-issue, Accessed on Dec. 20, 2021

[12] Everson L. Rosa Lucion, Raul Ceretta Nunes (2018). *Software Defined Perimeter: Improvements in the Security of Single Packet Authorization and user Authentication*. 2018 XLIV Latin American Computer Conference (CLEI), Sao Paulo, Brazil

[13] Allison Wylde (2021). *Zero trust: Never trust, always verify*. 2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), Dublin, Ireland

[14] Gartner, April 29, 2019 “Market Guide for Zero Trust Access”, https://www.gartner.com/en/documents/3912802/market-guide-for-zero-trust-network-access, Accessed on Dec. 20, 2021

[15] Annapurna P Patil, Gaurav Karkal, Jugal Wadhwa, Meer Sawood, K Dhanush Reddy (2020). *Design and Implementation of a Consensus Algorithm to build Zero Trust Model*. 2020 IEEE 17th India Council International Conference (INDICON), New Delhi, India

[16] Hritik Sateesh, Pavol Zavarsky (2020). *State-of-the-Art VANET Trust Models: Challenges and Recommendations*. 2020 11th IEEE Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), Vancouver, BC, Canada

[17] S. Rajagopalan (2020). *An Overview of SD-WAN Load Balancing for WAN Connections*. 2020 4th International Conference on Electronics, Communication and Aerospace Technology (ICECA), Coimbatore, India

[18] Sebastian Troia, Federico Sapienza, Leonardo Varé, Guido Maier (2020, December 03). On Deep Reinforcement Learning for Traffic Engineering in SD-WAN. *IEEE Journal on Selected Areas in Communications*, 39(7), 2198 - 2212

[19] YourTechDiet, “Gateway vs Firewall: More Secure Web Browser Server”, https://yourtechdiet.com/blogs/gateway-vs-firewall-more-secure-web-browser-server/, Accessed on Dec. 20, 2021

[20] Saima Mehraj, M. Tariq Banday (2020). *Establishing a Zero Trust Strategy in Cloud Computing Environment*. 2020 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India

[21] Pengfeng Zhang, Chuan Tian, Tao Shang, Lin Liu, Lei Li, Wenting Wang, Yiming Zhao (2021). *Dynamic access control technology based on zero-trust light verification network model*. 2021 International Conference on Communications, Information System and Computer Engineering (CISCE), Beijing, China

[22] AT&T SD-WAN service, https://www.business.att.com/products/sd-wan.html, Accessed on Dec. 20, 2021

[23] Cisco SASE service, https://www.cisco.com/c/en/us/products/security/sase.html, Accessed on Dec. 28, 2021

[24] Fotinet SASE service, https://www.fortinet.com/products/sase, Accessed on Dec. 28, 2021

[25] VMware SASE service, https://www.vmware.com/products/secure-access-service-edge-sase.html, Accessed on Dec. 28, 2021

[26] Zscaler SASE service, https://www.zscaler.com/capabilities/secure-access-service-edge, Accessed on Dec. 28, 2021

[27] Cato Networks SASE service, https://www.catonetworks.com/sase/, Accessed on Dec. 28, 2021

[28] Azar Salih, Subhi T. Zeebaree, Sadeeq Ameen, Ahmed Alkhyyat, Hnan M. Shukur (2021). *A Survey on the Role of Artificial Intelligence, Machine Learning and Deep Learning for Cybersecurity Attack Detection*. 2021 7th International Engineering Conference “Research & Innovation amid Global Pandemic" (IEC), Erbil, Iraq

[29] Ivan Ortiz Garcés, Maria Fernada Cazares, Roberto Omar Andrade (2019). *Detection of Phishing Attacks with Machine Learning Techniques in Cognitive Security Architecture*. 2019 International Conference on Computational Science and Computational Intelligence (CSCI), Las Vegas, NV, USA