International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 8 Aug 2023, pp: 463-480 www.ijaem.net ISSN: 2395-5252

Software Defined-Wide Area Network (SD-WAN) Security Solutions: A Comparative Study

Mohd Shamshul Anuar bin Omar [1], Hasbullah bin Omar[2]
School of Computing, University Utara Malaysia, Sintok, Kedah, Malaysia[1]
School of Computing, University Utara Malaysia, Sintok, Kedah, Malaysia[2]

Date of Submission: 15-08-2023 Date of Acceptance: 25-08-2023

ABSTRACT: Software-Defined Wide Area Networking (SD-WAN) has emerged as a transformative technology in the field of network management, offering increased flexibility, scalability, and cost-effectiveness. Although numerous solutions from different manufacturers have been made possible by SD-WAN's development, this has also led to an increase in threats against this technology. These security implications have become a critical concern for organizations. This study conducts a comparative analysis of the security features and capabilities of three prominent SD-WAN vendors: Palo Alto, Cisco Viptela, and Aruba. The research aims to provide organizations with insights into the security aspects of these solutions, facilitating informed decision-making. The study evaluates parameters such as encryption, authentication, and threat detection in a physical simulation experiment using actual appliances and components of the selected SD-WAN. The topology is built on a framework with a headquarters and two branches for each solution connected by two alternative links, one MPLS, and the other broadband Internet as a backup link. Distinct differences in security approaches are identified: Palo Alto offers superior security measures and emphasizes comprehensive threat prevention, Cisco Viptela integrates security with networking, and Aruba focuses on Zero Trust principles. The outcomes of this research will aid organizations in understanding the security strengths and weaknesses of Palo Alto, Cisco Viptela, and Aruba in the context of SD-WAN deployments. It will facilitate informed decision-making processes when selecting an SD-WAN vendor aligned with their security requirements. The research findings contribute to the existing body of knowledge in SD-WAN security and provide valuable insights into the evolving landscape of network security in the context of modern wide-area networks.

KEYWORDS: Software-Defined Wide Area Network (SD-WAN), security, comparative analysis, vendors, simulation experiment, decision-making.

I. INTRODUCTION

The idea of a wide area network (WAN) was created to link multiple nodes that were dispersed across various geographic regions. Enterprise networks connect computers and other devices across many business branches, including data centres. With this capability, enterprise networks are considered the foundation of everyday communication. The basic diagram of enterprise networks is depicted in Figure 1. Depending on the form of the organization and its operational needs, such enterprise networks may consist of both Wide Area Networks (WAN) and Local Area Networks (LAN). These networks make it possible for devices and users on the workplace network to securely communicate data. In the beginning, enterprise network solutions ranging from a 9.6Kbps dial-up to a dedicated T1/E1 over X.25 network connection were offered using point-to-point leased lines. The less expensive frame relay service, which required fewer physical connections, took the place of the X.25 network in the late 1990s. As a result, numerous businesses welcomed this technology.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 8 Aug 2023, pp: 463-480 www.ijaem.net ISSN: 2395-5252

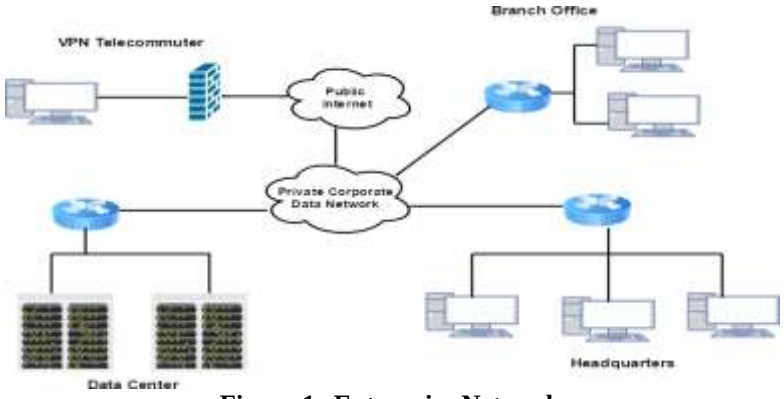

Figure 1: Enterprise Network

The replacement for frame relay service is MPLS was introduced in early 2000. It was developed as an IP-based remedy that uses telecommunications network infrastructure. Network service providers prefer the MPLS-based solution over the frame relay service. Even though many organizations use MPLS, it has costs and capacity restrictions. Compared to the open internet, MPLS connections are still pricey and have limited bandwidth. In Figure 2, MPLS is illustrated as a traditional WAN which consists of several types of dedicated connections and CPEs to serve a branch to HQ connection. Additionally, the development of technologies like IPsec VPN makes it possible to share business data securely over the Internet. The elements led businesses to start looking for MPLS substitutes. On the other hand, service providers have difficulty providing MPLS to the new generation of companies who have started relying on public clouds for their infrastructure. It is challenging for MPLS to connect enterprise branch locations to public clouds housed in external data centres. Network service providers have seen recent revenue declines in the MPLS business because of this business change. As a result, finding a new solution is an endeavour that both enterprises and service providers must accomplish.

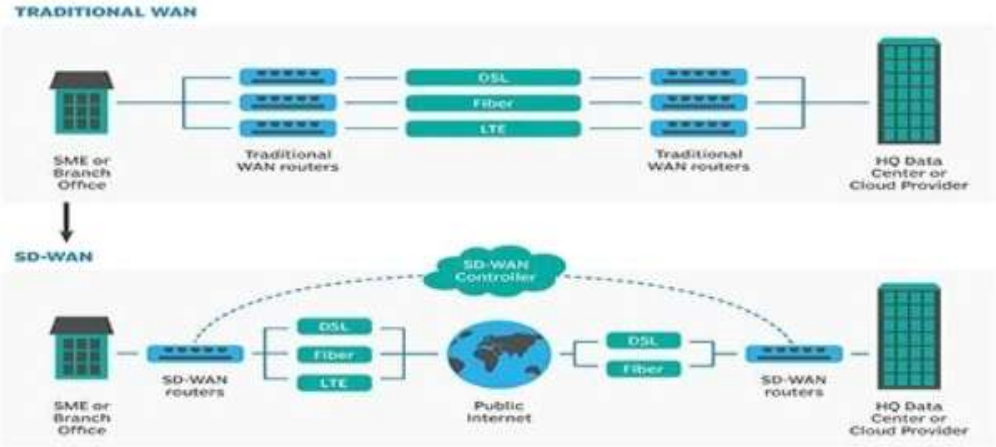

Figure 2: Traditional WAN vs. SD-WAN

The growing demand for agility, flexibility, and scalability in wide-area networks (WANs) has led to the development of Software-defined Wide Area Network (SD-WAN) technology. SD-WAN is derived from Software-Defined Networks (SDN), a methodology based on software drivers and API, allowing its communication with the physical hardware infrastructure, and facilitating administration and device setup. SDN offers an API for configuration and decouples software logic from the hardware . Optimizing virtualizing network services, this Internet-based technology enables flexible management, usual configuration complexity, and scalability . In Figure 3, the three layers of SD-WAN architecture are visible.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 8 Aug 2023, pp: 463-480 www.ijaem.net ISSN: 2395-5252

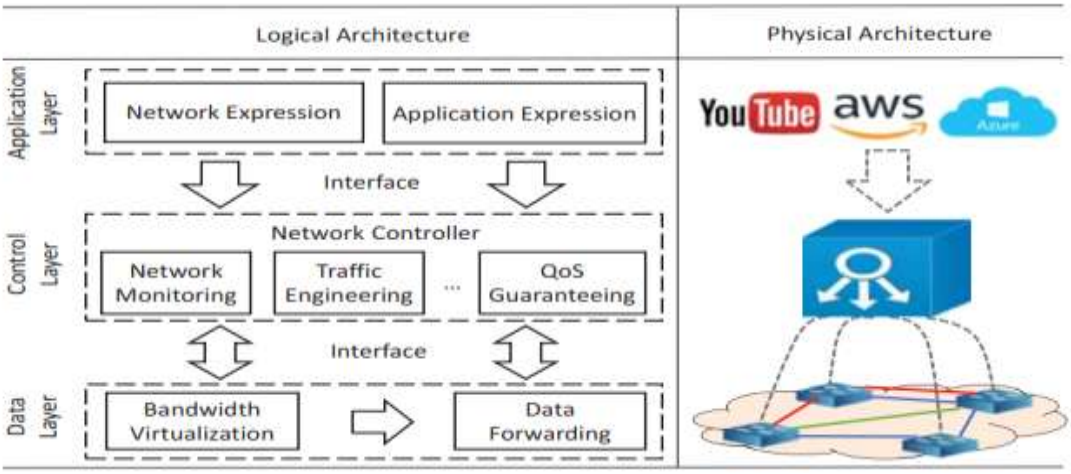

Figure 3: Basic SD-WAN Architecture

The control layer operates autonomously to execute and oversee network activities, whereas the data layer is responsible for managing bandwidth and virtualization of data forwarding. The application layer offers services, and developers and Internet service providers can specify the network requirements for those services . There are two interfaces available for layer-to-layer communication: the NorthBound Interfaces (NBI), which connect applications to the SD-WAN controller, and the SouthBound Interfaces (SBI), which connect the controller to network devices .

According to Gartner, due to SD-WAN performance, cost, and simplicity, 60% of businesses will be using SD-WAN by 2024, up from less than 20% in 2019, to improve agility and support for cloud apps . The new evolution makes it a more appealing attack vector for cybercriminals by adding adaptability that offers security services like Deep Packet Inspection (DPI), Firewalls, and VPN. However, some remedies that have been implemented are out-of-date or expired in open-source SD-WAN . In TCP attacks, such as Man-in-the-Middle (MitM), an attacker intercepts and alters the communication between two parties without their knowledge. This can occur when communication channels between SD-WAN sites are compromised, allowing the attacker to eavesdrop, modify data, or inject malicious content into the communication flow . Another factor to consider is data leakage. Network components may expose TCP/UDP ports, which enables attackers to gather data by exploiting those open ports ;.

On top of the attack as mentioned earlier methods, security breaches on SD-WAN can vary, but here are some of the common types of security breaches or flaws that organizations may experience, as listed in Table 1 below.

Table 1. Common Types of SD-WAN Security Breaches or Flaws

No	Types Of Security Breaches or Flaws	Details
1	Unauthorized Access	Unauthorized access occurs when an attacker gains unauthorized entry into the SD-WAN network or devices. This can happen due to weak or compromised passwords, insecure remote access configurations, or insufficient access controls. Once inside, the attacker can exploit the network and potentially gain access to sensitive data or launch further attacks.
2	Malware and Ransomware Attacks	Malware and ransomware attacks involve introducing malicious software into the SD-WAN infrastructure. This can happen through phishing emails, infected software updates, or compromised websites. Once the malware infiltrates the network, it can spread, disrupt operations, steal data, or demand ransom.
3	Data Breaches	Data breaches involve unauthorized access or

International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 8 Aug 2023, pp: 463-480 www.ijaem.net ISSN: 2395-5252

		disclosure of sensitive or confidential information. This can occur due to inadequate encryption mechanisms, weak data protection practices, or vulnerabilities in the SD-WAN infrastructure. Data breaches can have severe consequences, including financial loss, reputational damage, and legal liabilities.
4	Denial-of-Service (DoS) Attacks	DoS attacks aim to overwhelm or disable the SD-WAN network or specific devices by flooding them with excessive traffic or resource requests. This results in a loss of network availability, making it difficult for legitimate users to access resources and disrupting critical business operations.
5	Configuration and Management Vulnerabilities	Misconfigurations in SD-WAN devices or management interfaces can introduce security vulnerabilities. These misconfigurations allow attackers to bypass security controls, gain unauthorized access, or manipulate the network infrastructure. Common misconfigurations include weak access controls, default or outdated configurations, and improper segmentation.
6	Insider Threats	Insider threats involve employees or individuals with authorized access misusing their privileges to exploit the SD-WAN network. This can include data theft, unauthorized access to sensitive information, or intentional sabotage. Insider threats can be challenging to detect and mitigate since the individuals involved already have legitimate access to the network.
7	Lack of Encryption	Insufficient or improper encryption practices can expose sensitive data transmitted across the SD-WAN network to interception or unauthorized access. Data can be vulnerable to eavesdropping, interception, and tampering without proper encryption mechanisms.

Organizations need to be aware of these common security breaches and implement appropriate security measures, such as strong access controls, regular security assessments, encryption, and employee awareness training, to mitigate the risks associated with SD-WAN deployments.

II. PROBLEM STATEMENT AND RESEARCH OBJECTIVE

SD-WAN optimized software-based network orchestrators to provide more agile, flexible, and scalable network services. SD-WAN technology can optimize application performance, balance network traffic, and secure network communications. The administration of the objects in the SD-WAN architecture is done via network protocols like Secure Socket Shell (SSH), Hypertext Transfer Protocol (HTTP), and Transport Layer Security (TLS). In this study, these protocols are represented through web administration interfaces. However, these are not immune to vulnerabilities and triggered a question of what the key security features and capabilities vendors offer in their SD-WAN solutions. Hence, there is still a knowledge gap on the effectiveness and capabilities of SD-WAN among major vendors available in the market.

Therefore, there is a need to conduct an assessment and comparative study on the effectiveness and capabilities of SD-WAN security features and capabilities. This study will compare the reliability and security aspects of three SD-WAN products: Palo Alto, Aruba, and Cisco Viptela, in different scenarios. Moreover, this study will highlight the limitations, challenges, and opportunities for these products in different network security environments.

This study evaluates and compares the security aspects of three selected SD-WAN brands.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 8 Aug 2023, pp: 463-480 www.ijaem.net ISSN: 2395-5252

Any vulnerabilities discovered will be appropriately disclosed and reported to the respective vendors. Assessment of the strengths and weaknesses of these solutions, as well as the effectiveness and performance of their intrusion detection, malware detection, and security analytics, were captured. The comparative advantages in terms of security underpin the significance of examining and deploying these technologies. This work aims to compare the security features of the selected SD-WAN brands - Palo Alto, Aruba, and Cisco. A simulated environment is being used as part of the study technique to enable the testing of this technology.

III. RELATED WORK

Numerous research and contributions on cyber security have emerged in tandem with the SD-WAN's expansion. Digital data is more exposed to numerous threats due to the new network paradigm, which shifted its design from private networks such as MPLS to Internet cloud-based networks . For that, organizations require all WAN connectivity to be more secure by employing communication protocols that accommodate the latest technology demands. Listed below are several related studies of security issues on cloud-based networks, as depicted in Table 2.

Table 2. Security Concerns on Cloud-based Data and Networks.

Author	Paper Title	Description	Security Concern
Mijuskovic & Ferati, (2019)	Cloud Storage Privacy and Security User Awareness	These systems offer essentially the same benefits but share similar weaknesses in data privacy and security, including data loss, replication, and unauthorized data release to third-party businesses .	CIA Triad
Mishra & Jena, (2019)	Security of cloud storage: A survey	Insiders with access to cloud storage vendors can view the content of the data. The user has no control over their personal information.	Lack of Control
Nagesh, Kumar, & Rajgopal, (2018)	Cloud architectures encountering data security and privacy concerns - A review.	Data integrity maintenance is one of the significant issues among the multiple security risks cloud servers offer.	CIA Triad
Odun-Ayo, Ajayi, Akanle, & Ahuja, (2018)	An overview of data storage in cloud computing	Data integrity, confidentiality, privacy, and availability threats exist in the cloud computing environment .	CIA Triad
Gordeychik, Kolegov, & Nikolaev, (2018)	SD-WAN Internet Census.	Most SD-WAN vendors have known vulnerabilities related to out-of-date software and insecure configuration. This study provided and discussed the findings of passive and active fingerprinting for SD-WAN systems utilizing the "Shodan" and "Censys" search engines and custom automation tools	Lack of Control
Wendland & Banse, (2017)	Threat analysis of container-as-a-service for Network Function Virtualization.	The research concentrates on a virtualization strategy based on containers and considers NVFI architecture's Container-as-a-Service platform for SDN. Additionally, the report examines security risks and offers NFV security mitigation tactics .	CIA Triad
Lal, Taleb, & Dutta, (2017)	NFV: Security threats and best practices	The NFVI is subject to serious security risks, which discusses and suggests best practices for preventing them. The following high-level techniques are considered: secure booting, isolation, remote attestation, NFV image signing, kernel hardening, and so forth. It should be noted that no SD-WAN device uses those suggested	CIA Triad

International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 8 Aug 2023, pp: 463-480 www.ijaem.net ISSN: 2395-5252

Yoon, et al., (2017)	Flow wars: Systemizing the attack surface and defenses in software-defined networks.	A thorough investigation into potential misuse or exploitation strategies for an OpenFlow-based SDN stack, and the creation of a fundamental SDN attack surface, give a broad classification of ways to misuse or directly attack the SDN. Management and orchestration plane tests were skipped and only considering the attack surfaces on the control and data planes .	Lack of Control
Bogineni, (2016)	Verizon SDN-NFV Reference Architecture	Eight layers of threat vectors related to securely delivering a service in a network based on SDN, NFV, and virtualization are provided by the Verizon SDN-NFV Reference Architecture. The document offers standard requirements, fundamental recommendations, and reference architecture .	CIA Triad
(Hizver, 2015)	Taxonomic Modeling of Security Threats in Software-Defined Networking	Threats to the SDN are systematically identified by threat sources, vulnerability sources, threats, and actions are listed, and the integrated SDN. The work is theoretical and offers no actual instances of SDN vulnerabilities or attacks. Additionally, the report lists typical attacks applicable to both ordinary computer systems and SDNs .	CIA Triad

In the works of, studies of SD-WAN internet-based solutions are conducted to look for flaws in SD-WAN appliances using NMAP and Shodan and searching for security weaknesses in the CVE databases. The security of the CPE was assessed, as demonstrated by a team of researchers from Carnagie-Mellon University and Gordeychik, which focused on a surface assault on the CPE . Both researchers analyze and measure the attack surfaces of the provided system. Their final section offers suggestions for risk management at the SD level, secure communications, and web administration security. Most of the vulnerabilities listed are commercial solutions.

There is also specific research that concentrates on the security of the SD-WAN orchestrator and identifies the main security considerations to consider while analyzing an orchestrator. Unauthorized access, data leakage, and denial of service are some of the security concerns considered when analyzing the SD-WAN orchestrator. The interface analysis of the orchestrator is then performed using references .

In both types of SD-WAN research, a common attack on SD-WAN was executed. In Figure 4, a Man-in-the-Middle attack is illustrated. This type of attack is typically caused by the misuse of keys and certificates, and the potential for such attacks in SD-WAN is demonstrated using tools such as Nessus, NMAP, Nikto, and Wireshark. A literature review on threat analysis and penetration testing serves as the larger framework for this study.

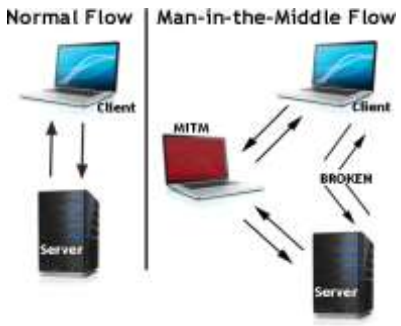

Figure 4 Man in the Middle Attack

A comparative study of SD-WAN solutions, similar studies, and reports with the same approach will be referred. Gartner, well-known research and advisory firm, published annual reports on SD-WAN, which typically provide insights, analysis, and evaluations of different vendors and solutions in the SD-WAN market, helping businesses make informed decisions when considering SD-WAN deployments . While Gartner adopts a comprehensive approach to comparison, Gordeychik employs an experimental comparative methodology to demonstrate that most SD-WAN providers had identifiable flaws associated with outdated software and insecure settings. The author analyzed SD-WAN systems by utilizing the "Shodan" and "Censys" search

International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 8 Aug 2023, pp: 463-480 www.ijaem.net ISSN: 2395-5252

engines, as well as custom-developed automation tools, to obtain both passive and active fingerprinting results ;. In this regard, the study suggested by Gordeychik presents a list of SD-WAN vulnerability levels. The authors found that being an entirely IP-based solution makes cybercriminals vulnerable and alluring by establishing that the most frequent attacks are concentrated on the management level and zero-day vulnerabilities.

IV. METHODOLOGY

To compare the cyber security defenses against common assaults, three SD-WAN solutions by Palo Alto Networks, Aruba, and Cisco Viptela were compared using an experimental methodology. A comparative study is used to assess and compare the security solutions offered by the selected SD-WAN vendor, allowing for a systematic and structured analysis of the vendors' security features and capabilities. Primary and secondary data sources will be used in the data collection process.

Primary data will be collected through a physical experiment on security testing and evaluation on all three SD-WAN appliances; Palo Alto Networks, Aruba, and Cisco Viptela. The security requirements are based on a model produced by the ONUG SD-WAN working group, which offers a list of tactical and strategic demands for an SD-WAN system, including security demands . It also evaluates the SD-WAN solution's security requirements to acquire comprehensive data on the security features of their SD-WAN solutions. Secondary data will be collected through an extensive review of relevant literature, including academic journals, conference proceedings, white papers, vendor documentation, and industry reports. This will provide a comprehensive understanding of the current state of SD-WAN security and the offerings of the selected vendors.

The physical experiment was chosen to imitate the actual production environment of SD-WAN networks and direct knowledge in designing, configuring, and testing a wide range of topologies and scenarios, as depicted in Figure 5. The Palo Alto, Aruba, and Cisco network topologies were implemented using respective brands of SD-WAN routers that connected to MPLS and broadband networks. Nessus was used for fingerprinting, enabling automated scanning and vulnerability analysis of computer systems. NMAP satisfies the requirements for ideal scanning for manual testing. The Nikto tool was configured for the web penetration test case. Wireshark was used to analyze streams of data packets sent between network computers, networks of networks, and between the Internet and other networks. These packets are meant for specific computers, but a sniffer packet allows IT professionals, end-users, or malevolent attackers to inspect any packet within the network.

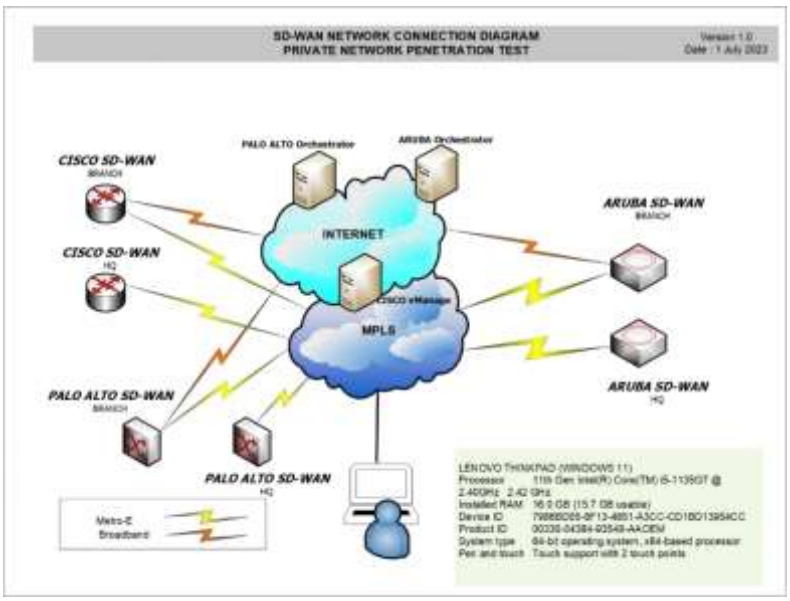

Figure 5: SD-WAN Experiment Network Diagram

The interconnection of core networks and the behaviour of the selected CPEs are physically set up in a controlled MPLS environment. Most commercial SD-WAN installations exhibit an architectural framework that establishes connectivity between a central office and several

International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 8 Aug 2023, pp: 463-480 www.ijaem.net ISSN: 2395-5252

branch locations. The structure and quantity of components may vary depending on the source. Each of the three providers oversees the management of devices through an Orchestrator hosted on the Internet. The proposed simulation scenarios involve a setup consisting of two nodes, specifically branch offices, and headquarters. These nodes are interconnected through an MPLS and backup Internet links, as depicted in Figure 5.
The parameters of the configured scenarios are shown in Table 3.

Table 3. Simulation Parameters

	Value		
	Palo Alto	**Aruba**	**Cisco**
CPE	3	3	3
Alternate links (Private MPLS /Public Broadband)	Yes	Yes	Yes
SSH	Yes	Yes	Yes
Web Console	Yes	Yes	Yes
HTTPS	Yes	Yes	Yes
Orchestrator	Yes	Yes	Yes
Version	Palo Alto Prisma SDWAN Version 14.0.0-11	Silver Peak Unity Release 9.0.6.40158	Cisco Vmanage Platform version 20.6.4
CPE	Prisma ION 3000	EC-XS 8.3.6.0_86373	ISR 1100X 4G
IPsec Tunnel	Yes	Yes	Yes
	Pre-shared Key	Pre-shared Key	Pre-shared Key

V. FINDINGS

As mentioned in the previous chapter, the data collected from primary and secondary sources will be synthesized and interpreted to generate meaningful insights. The comparative analysis results and vendor-provided information will be integrated to provide a comprehensive overview of the security solutions offered by each vendor.

A. PRIMARY DATA: EXPERIMENTS

A machine with an 11th Gen Intel(R) Core (TM) i5-1135G7 processor and 16GB of RAM, with a Windows 11 operating system, was used in the experiment. It hosted a Kali Linux operating system on VirtualBox. Nessus, Nikto, and the NMAP are the tools used. The Nessus vulnerability scanner provided one of the largest security vulnerability knowledge bases and hundreds of plugins that can be activated for thorough, adaptable searches. This scanner identifies security holes in the operating system, installed patches, and installed services of the targeted host and suggests ways to fix them . Nikto is a web server analysis program that can identify and assess a wide range of default and unprotected files, settings, and programs on almost any web server. A free and open-source tool for launching exploits on distant target computers is the Nmap. A legitimate penetration tester can use Nmap's tools after installing it on a system to take advantage of vulnerabilities in the remote system . Attacks on the web administration, HTTP, and SD-WAN surface were used. The outcomes were assessed on a qualitative level.

I. User Authentication

The user authentication experiment aimed to determine whether the user's login information is encrypted and whether the SD-WAN vendors offer two-factor authentication. The sample of Experiment 1 on the encrypted login is shown in Figure 6. The outcomes of the experiments are depicted in Table 4 below.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 8 Aug 2023, pp: 463-480 www.ijaem.net ISSN: 2395-5252

Table 4. User Authentication Results

SD-WAN Vendor	Palo Alto Networks	Aruba (HPE)	Cisco Viptela
Experiment 1: User Authentication: Wireshark and email notification	TLS 1.2	TLS 1.2	TLS 1.3
	The results for this experiment showed that only Cisco deployed TLS 1.3, while Aruba and Palo Alto used TLS 1.2. Transport Layer Security (TLS) is a cryptographic protocol securing internet communication. TLS 1.2 and 1.3 differ in keys. TLS 1.3 reduced handshake steps, improving speed and security. It eliminated weaker encryption algorithms and enhanced forward secrecy. 1.3 mandates Perfect Forward Secrecy (PFS) by default and removes obsolete features. The resumption process was simplified for quicker reconnections. Overall, TLS 1.3 enhances security, reduces latency, and streamlines connections compared to TLS 1.2.		
	Multi-Factor Authentication (MFA)	Multi-Factor Authentication (MFA)	Multi-Factor Authentication (MFA)
	All three SD-WAN vendors provide this security feature through email as an alternate authenticator. It is a security method that requires users to provide two or more authentication factors to access an account or system. These factors typically fall into three categories: something you know (like a password or PIN), something you have (like a smartphone or hardware token), and something you are (biometric data like fingerprints or facial recognition). MFA significantly enhances security by adding an extra layer of protection against unauthorized access, as even if one factor is compromised, the attacker would still need the other factor(s) to gain access.		

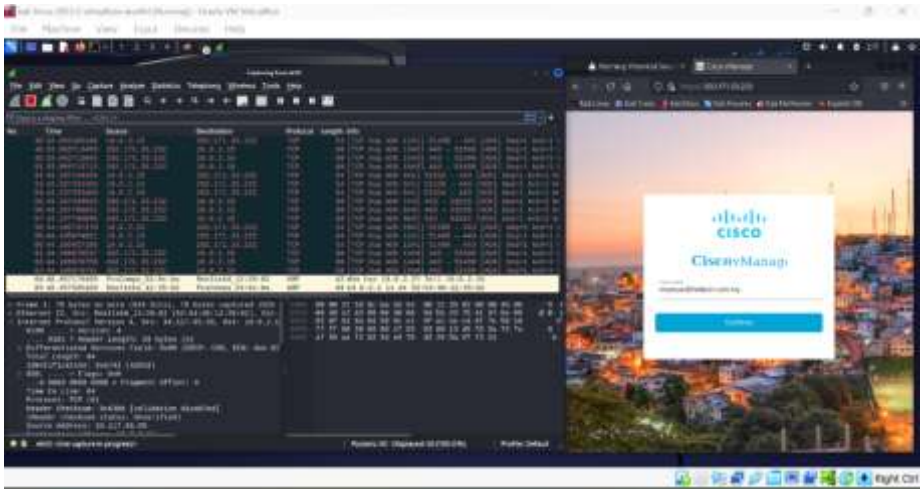

Figure 6. Example of Wireshark findings in Experiment 1: Authentication.

II. Encrypted Data in Transit

This experiment aimed to ascertain whether data is encrypted in transit when uploaded to an SD-WAN. In this experiment, data was uploaded to the selected SD-WAN, and Wireshark was used to track the data's movement and look for any unencrypted data. If connections between the SD-WAN appliance and the Orchestrator or between two sites are intercepted, encryption in transit is crucial to protect user data. Data is encrypted before transmission, endpoints are authenticated, and data is decrypted and validated as it arrives to achieve this security. The use of Wireshark is demonstrated in Figure 7. The results of the experiments are depicted in Table 5 below.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 8 Aug 2023, pp: 463-480 www.ijaem.net ISSN: 2395-5252

Table 5. Encrypted Data in Transit Results

SD-WAN Vendor	Palo Alto Networks	Aruba (HPE)	Cisco Viptela
Experiment 2: Encrypted Data in Transit: Wireshark	Data Encrypted. The server's name is exposed.	Data Encrypted. The server pieces of information are exposed; name, location	Data fully encrypted
	Wireshark allows users to capture and inspect packets travelling over a network, providing detailed information about the network traffic. All three SD-WAN vendors used AES 128 for their encryption and SHA 256 for the integrity hash algorithm. Thus, all data are well encrypted and secured from sniffing activities. Both Palo and Aruba systems lack a self-signed certificate by default that would provide a secure HTTPS connection for management. Typically, plain text is used to pass the credentials. As a result, Palo and Aruba did expose the info of the server names, which eventually can lead to further exploitation. Only Cisco managed to hide server info in this experiment.		

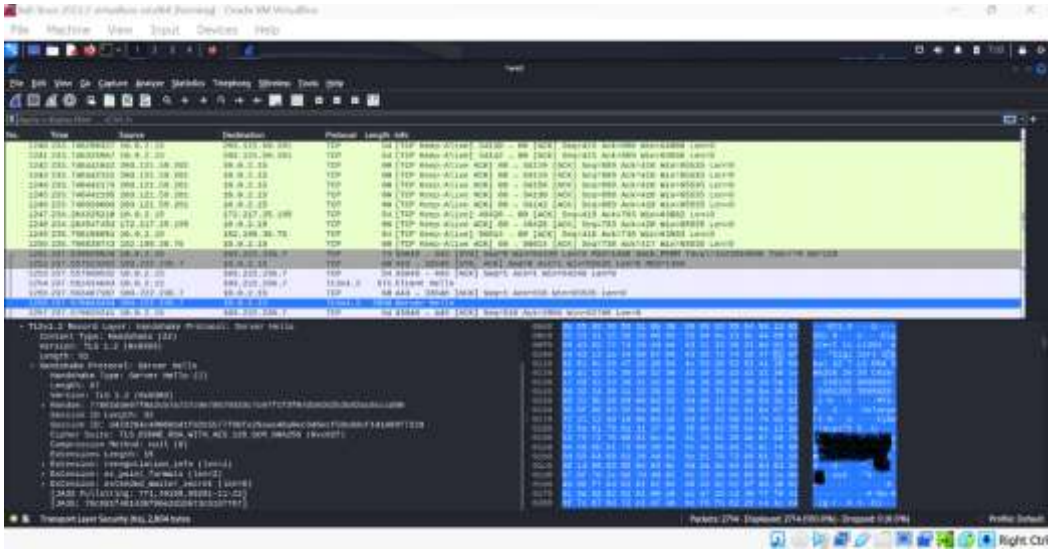

Figure 7. Example of Wireshark findings in Experiment 2: Encrypted Data in Transit.

III. Vulnerability Analysis Results

Vulnerability assessment is the process of defining, identifying, classifying, and ranking vulnerabilities in computer systems, applications, and network infrastructures. People can notice and respond to dangers to their environment by using the knowledge, awareness, and risk background provided by vulnerability assessments. A vulnerability assessment procedure's objective is to discover threats and the risks they pose. Three vulnerability scanners such as Nessus, Nikto, and the Nmap, were executed in this vulnerability assessment experiment.

Table 6. Vulnerability Analysis

SD-WAN Vendor	Palo Alto Networks	Aruba (HPE)	Cisco Viptela
Experiment 3: Vulnerability Analysis: Nessus, Nikto, NMAP	No vulnerability was detected.	1 Critical vulnerability detected.	14 medium and 4 low vulnerabilities were detected.
	Nessus is used as a vulnerability scanner to analyze systems for security flaws. It identifies potential weaknesses, misconfigurations, and outdated software. The findings include severity levels, detailed descriptions, and possible solutions for each issue. In this experiment, all findings are reported to respective vendors.		

International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 8 Aug 2023, pp: 463-480 www.ijaem.net ISSN: 2395-5252

	Host protected from the scan.	4 items reported.	1 item reported.
	Nikto is a comprehensive web server scan report identifying potential security issues and vulnerabilities in its target. It checks for outdated software versions, known vulnerabilities, misconfigurations, and other weaknesses. The scan results reported that Aruba has the most reported items, followed by Cisco. In contrast, Palo Alto Orchestrator is protected from Nikto Scanner. All scanning failed.		
	2 open ports were detected	3 open ports were detected	8 open ports were detected
	Nmap scanner results show which ports are open, and it may expose access to potential attack surface and exploitation of possible vulnerabilities in the target system.		

Figure 8. Example of Nessus findings in Experiment 3: Vulnerability Analysis.

All management interfaces appear to be secure, according to the Nikto automated scanner. Palo Alto is completely secure; it uses a robust authentication system from Aruba and Cisco. The outdated OS versions are to blame for the vulnerabilities discovered. See how the Aruba CPE has a critical vulnerability in Table 6 and Figure 8

International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 8 Aug 2023, pp: 463-480 www.ijaem.net ISSN: 2395-5252

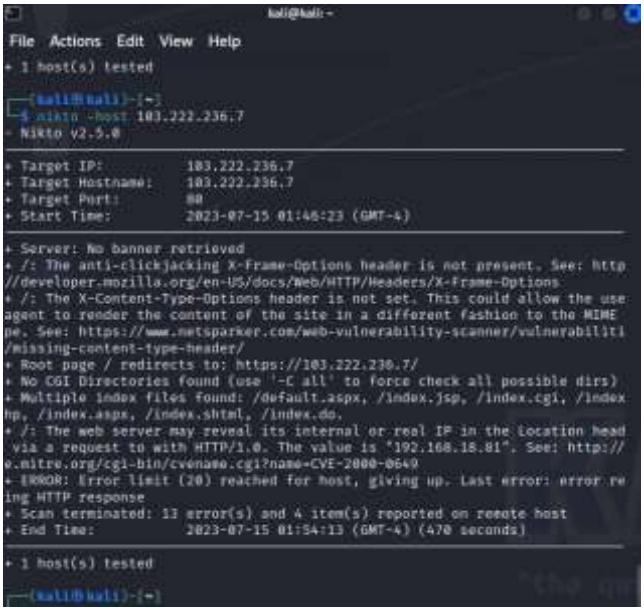

Figure 9. Example of Nikto findings in Experiment 3: Vulnerability Analysis.

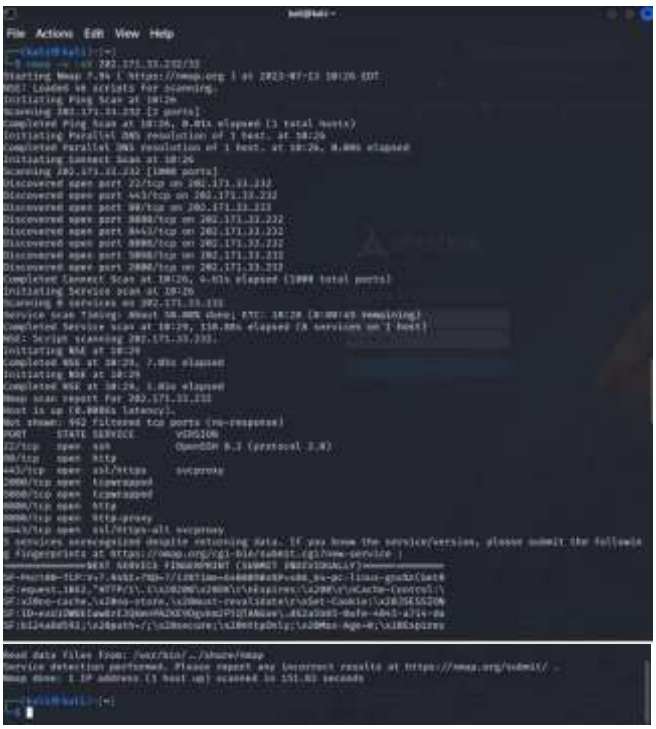

Figure 10. Example of Nmap findings in Experiment 3: Vulnerability Analysis.

Based on the findings of Nikto and Nmap in Figure 9 and Figure 10, further penetration tests were conducted; manual, semi-auto, and automated concluded that those ports were secured and no successed exploitation. This proves that the user input for each form is appropriately sanitized, and the thick web application is another reason to be highlighted, as depicted in Figure 11.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 8 Aug 2023, pp: 463-480 www.ijaem.net ISSN: 2395-5252

Figure 11. Example result of further enumeration to trigger directory traversal.

IV.Cryptography

All traffic is encrypted when a Man-in-the-Middle assault is being conducted using the technique each solution suggests, such as Authentication Header (AH) and Encapsulating Security Payload (ESP). Both technologies enable the implementation of IPsec tunnels between the main office and branch CPEs, guaranteeing the data's integrity and secrecy. The parameters for each solution are displayed in Table 7, and the encrypted data are displayed in Figure 12.

Table 7. IPsec Tunnel Parameters

SD-WAN Vendor	Palo Alto Networks	Aruba	Cisco
IKE Version	1,2	1,2	1,2
Authentication Methods	Preshared Key, Certificado digital	Preshared Key, Certificado digital	Preshared Key, Certificado digital
Encryption algorithm	DES-MD5, DES -SHA1 DES-SHA256, DES-SHA384, DES- SHA512	DES-MD5, DES -SHA1 DES-SHA256, DES-SHA384, DES- SHA512	DES-MD5, DES -SHA1 DES-SHA256, DES-SHA384, DES- SHA512
Hashing Algorithm	MD5, SHA-256, SHA-512, SHA-384	MD5, SHA-256, SHA-512, SHA-384	MD5, SHA-256, SHA-512, SHA-384

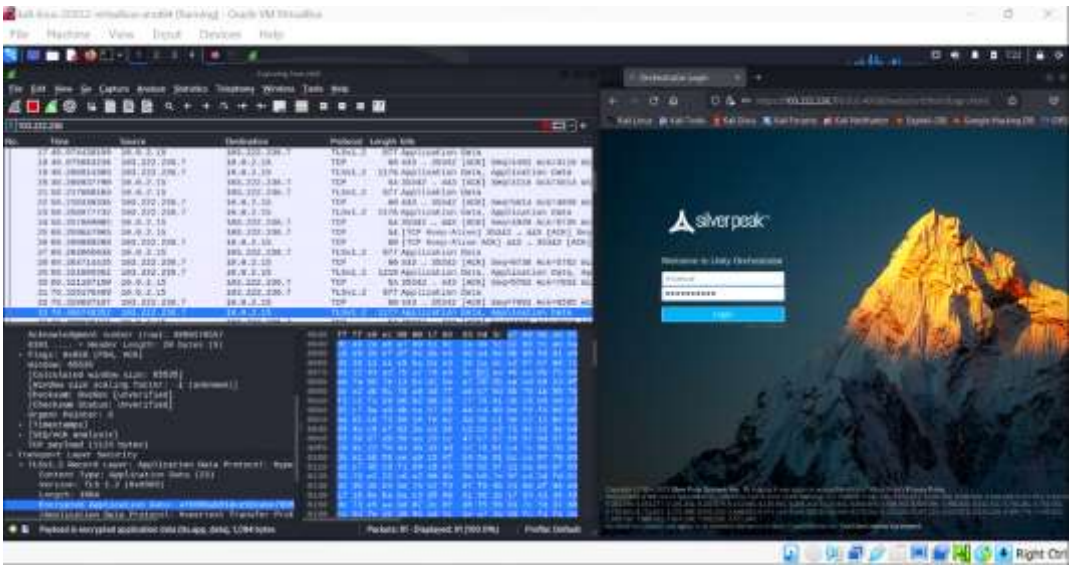

Figure 12. Example result of encrypted data captured.

B. SECONDARY DATA: VENDOR-PROVIDED INFORMATION

A matrix or summarized table of each vendor's SD-WAN solution's key security features and capabilities are compared. This matrix will provide a visual representation of the comparison, making it easier to identify the similarities and

International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 8 Aug 2023, pp: 463-480 www.ijaem.net ISSN: 2395-5252

differences between the vendors, as depicted in Table 8 below.

Table 8. Matrix of the Key Security Features and Capabilities

SD-WAN Vendor	Palo Alto Networks	Aruba (HPE)	Cisco Viptela
Security Features	Next-Generation Firewall (NGFW)	Stateful Firewall	Zone-Based Firewall
	Next-Generation Firewall (NGFW): Offers advanced security features like application control and intrusion prevention, providing better threat protection. Stateful Firewall: Provides basic packet filtering and tracks connection state, suitable for simple security requirements. Zone-Based Firewall: Divides networks into security zones, controlling traffic flow between them, effective for granular network segmentation.		
	Intrusion Prevention System (IPS)	Intrusion Detection and Prevention (IDP)	Intrusion Detection and Prevention (IDP)
	Intrusion Detection and Prevention (IDP) identifies and stops potential threats, while an Intrusion Prevention System (IPS) actively blocks malicious activities. Both are essential for security, but IPS is more effective as it proactively prevents intrusions.		
	Secure Web Gateway (SWG)	Web Filtering	Web Filtering
	Secure Web Gateway (SWG) provides advanced security features, including URL filtering, application control, antivirus scanning, and data loss prevention. Web Filtering focuses solely on blocking or allowing access to specific websites based on predefined categories. SWG is more comprehensive and effective for overall web security		
Scalability	High Scalability and Performance	Scalable Architecture	Scalable Architecture
	High Scalability/Performance allows for handling many users/requests efficiently. Scalable Architecture refers to a system's ability to grow/adapt without losing performance. Both are crucial, but Scalable Architecture is better, ensuring sustainable growth without compromising performance.		
Encryption	Offers strong encryption using IPsec and SSL/TLS protocols. Provides end-to-end encryption for data privacy and integrity.	Provides encryption using IPsec and SSL/TLS protocols for secure communication. Supports encryption at the overlay level.	Offers encryption using IPsec and DTLS protocols to ensure secure data transmission across the SD-WAN network.
	Palo Alto offers the best SD-WAN security features with strong IPsec and SSL/TLS encryption, ensuring end-to-end data privacy and integrity. Aruba comes second, supporting IPsec and SSL/TLS encryption at the overlay level. Cisco ranks third with IPsec and DTLS protocols for secure data transmission.		
Authentication	Provides various authentication mechanisms, including multi-factor authentication (MFA), certificate-based authentication, and integration with identity providers.	Supports multiple authentication methods, including MFA, certificate-based authentication, and integration with directory services.	Offers authentication options such as MFA, certificate-based authentication, and integration with third-party identity providers.
	Palo Alto is the best, providing various authentication mechanisms, including robust multi-factor authentication (MFA) and seamless integration with identity providers. Aruba is in second place for supporting multiple authentication methods, including MFA and certificate-based authentication, with directory services integration. Cisco is third,		

	offering similar authentication options, including MFA and certificate-based authentication, but lacking specific third-party identity provider integration.		
Access Control	Implements granular access control policies based on user identity, device type, and application. Supports role-based access control (RBAC) for fine-grained control over resource access.	Offers flexible access control policies based on user, device, and application, allowing granular control over resource access. Supports RBAC for user management.	Provides access control mechanisms based on user identity, device type, and application, allowing administrators to define and enforce policies for resource access.
	Palo Alto's SD-WAN security features stand out as the best, providing the most extensive and fine-grained control over resource access through a combination of user identity, device type, application-based policies, and role-based access control. Aruba follows closely with its flexible access control options. At the same time, Cisco's features provide effective access control based on user identity, device, and application but may have slightly fewer granular control capabilities compared to the other two.		
Threat Intelligence	Integrates with Palo Alto Networks Threat Intelligence Cloud, providing real-time updates on emerging threats. Offers advanced threat detection and prevention capabilities.	Leverages Aruba Threat Defense to detect and mitigate network threats. Integrates with threat intelligence feeds and offers threat detection capabilities.	Integrates with Cisco Talos Intelligence and other third-party threat intelligence feeds to provide real-time threat detection and prevention.
	Palo Alto offers the most comprehensive SD-WAN security with real-time updates on threats through its Threat Intelligence Cloud and advanced detection and prevention capabilities. Cisco provides strong real-time threat detection and prevention by integrating with Cisco Talos Intelligence and third-party feeds. Aruba's Threat Defense and integration with threat intelligence feeds deliver decent threat detection and mitigation.		
Logging and Monitoring	Offers comprehensive logging and monitoring capabilities, including centralized logging, real-time analytics, and customizable dashboards. Provides visibility into security events and network performance.	Provides centralized logging and monitoring features, enabling real-time visibility into security events and network performance. Offers customizable dashboards and analytics.	Offers logging and monitoring capabilities, including centralized logging, real-time analytics, and customizable dashboards. Provides visibility into security events and network performance.
	Palo Alto stands out as the best due to its comprehensive logging, monitoring, and analytics capabilities, providing real-time visibility into security events and network performance. Cisco closely follows with similar features. Aruba is third but still offers centralized logging and monitoring, customizable dashboards, and analytics.		
Integration	Integrates with other Palo Alto Networks security products, such as Next-Generation Firewalls (NGFW) and Security Operations Center (SOC) platforms, for comprehensive security coverage.	Integrates with Aruba ClearPass for advanced network access control. It also integrates with other security solutions for enhanced threat detection and response.	Integrates with Cisco security solutions, such as Cisco Firepower NGFW and Cisco Umbrella, for a comprehensive security ecosystem. Supports integration with third-party security tools.
	Palo Alto is considered the best due to its robust integration with its own security products, offering a highly cohesive and comprehensive security approach within its ecosystem. Cisco follows closely, providing a flexible ecosystem with its solutions and third-party integrations. Aruba, while still offering valuable security features, ranks third with relatively fewer native integrations.		
Complia	Helps organizations achieve	Offers compliance	Assists organizations in

International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 8 Aug 2023, pp: 463-480 www.ijaem.net ISSN: 2395-5252

nce	compliance with industry regulations, such as PCI DSS, HIPAA, and GDPR, through built-in security controls and reporting capabilities.	reporting features and helps organizations meet industry-specific regulatory requirements. Provides reporting and audit trail capabilities.	meeting compliance requirements through built-in security controls and compliance reporting features. Supports reporting and audit trail functionalities.
	Palo Alto's robust security controls and extensive reporting capabilities make it the best choice for achieving compliance with various industry regulations. Cisco follows closely with similar features, while Aruba offers compliance support with its reporting and audit trail functionalities.		

VI. CONCLUSIONS

It is crucial to keep the security levels of many burgeoning technologies used in mission-critical or commercial systems at high levels. By providing organizations with a flexible and simple-to-manage network solution, SD-WAN is revolutionizing the way businesses network in the future. Currently, businesses are attempting to cut costs by removing MPLS links, and service providers are having trouble supporting the cloudification of MPLS. Due to this trend, providers are now considering SD-WAN as a superior enterprise solution. However, as enterprise networks are desirable targets for attackers, implementing IP-based SD-WAN will raise the danger of prospective attacks. Enterprise networks are always a target for hackers because they house expensive computing resources and data. Therefore, before widely implementing the new technology, service providers and businesses give top emphasis to SD-WAN security. In this paper, we examined Palo Alto, Aruba, and Cisco SD-WAN technology and disclosed prevalent dangers and security flaws of SD-WAN before showcasing potential assaults against it. The enterprise WAN networks, numerous prior solutions, and the idea of SD-WAN were initially investigated. We also discussed the necessity for security analysis of SD-WAN and the relevant literature to use for that analysis.

This research aims to identify user security concerns regarding SD-WAN and assist users in considering the security of their data traverse in their network. The project conducted experiments using various security tools, including open-source and free tools. The selected SD-WAN vendors were detailed in the literature review, and their security characteristics were compared to provide a comprehensive comparative analysis. The experimental approach was used on all three SD-WAN products. All respective solutions offer superior cybersecurity procedures and offer mitigations to frequent assaults, according to the security tests.

All solutions offered ensure both confidentiality and integrity protection. Additionally, IPsec tunnels can withstand the cryptographic technique's strength utilized for verification and validity purposes. The ability of Palo Alto to offer and implement several cryptographic techniques and features, whereas Aruba and Cisco did not, is the most obvious distinction. We must also acknowledge that most current vulnerabilities result from default settings or a basic hardening in the solutions. The default setup is already more than vulnerable, so each orchestrator's administration requires a further hardening step. By examining each of its many parts and interactions, we examined all components of the selected SD-WAN. As a result, numerous attack surfaces and security flaws were discovered. Finally, the mitigation techniques to prevent attacks on the flaws were suggested as a foundation for a more secure hardening process to address the issues.

LIMITATIONS

i. The study's findings and conclusions may be influenced by the available information at the time of research and the specific products and versions analyzed.
ii. The comparative analysis is limited to the selected vendors and may not encompass all SD-WAN security solutions in the market.
iii. The study may have unique contextual factors that may not apply to all organizations or regions.
iv. The study does not include an exhaustive assessment of the SD-WAN solutions' performance, cost, or other non-security-related aspects.

It is important to acknowledge these limitations while interpreting the results and consider further research and analysis to comprehensively understand the SD-WAN security landscape.

FUTURE WORK

International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 8 Aug 2023, pp: 463-480 www.ijaem.net ISSN: 2395-5252

Future work should focus on continuity security assessment using additional vulnerability scanners and more research on the privacy and security of SD-WAN. The current research faced limitations, such as restricted access to security tools and vulnerability scanners, limited functionality of Nessus tools, and time limitations for specific security features. Additionally, SD-WAN security is too secret and hazardous to analyse for weaknesses too deeply.

Different approaches should also be considered; for example, the Technology Acceptance Model (TAM), a famous theoretical framework that explains and forecasts people's acceptance, can be proposed to further study the level of embracement of new technology from all sorts of angles, especially security. Future work should consider new technologies that can work together to create a secure and dynamic SD-WAN environment, such as zero-trust networking, SASE, and AI-powered threat detection. A broader comparative analysis by including more sophisticated security penetration tools or even other SD-WAN brand options like Fortinet or Juniper. With the inclusion of all proposed items, a more thorough analysis of additional attack vectors could improve cybersecurity perspectives for various systems and produce potential rules to protect the foundation of enterprise SD-WAN networks. Researchers have identified several emerging trends in SD-WAN security to be further explored and evaluated in future studies:

i. Secure Access Service Edge (SASE): The convergence of SD-WAN and cloud security, known as SASE, combines networking and security capabilities into a unified architecture. SASE provides secure access to applications and data, regardless of location, and offers integrated security services like firewall-as-a-service and secure web gateways.
ii. Zero-Trust Networking: Zero-trust principles are gaining momentum in SD-WAN deployments. By assuming that every user and device is untrusted until proven otherwise, zero-trust networking ensures robust access control and continuously monitors network traffic for potential threats.
iii. Artificial Intelligence in Threat Detection: AI and machine learning techniques are employed to enhance threat detection and response capabilities in SD-WAN security. These technologies enable the analysis of large volumes of network data to identify anomalies, detect potential security breaches, and automate incident response; .

C. SIGNIFICANCE OF THE RESEARCH

The comparative study SD-WAN security provided by Palo Alto Networks, Aruba, and Cisco Viptela holds several significant implications:

i. **Infor**med Decision-Making

The comparative study provides valuable insights into the security features and capabilities different SD-WAN vendors offer. This information is crucial for organizations considering SD-WAN adoption, enabling them to make informed decisions based on their specific security requirements.

ii. Security Best Practices:

By examining the strengths and weaknesses of each vendor's security solutions, the research contributes to identifying security best practices in SD-WAN deployments. Organizations can leverage this knowledge to implement adequate security measures and mitigate potential vulnerabilities.

iii. Enhanced Network Security:

SD-WAN deployments introduce new security challenges, and understanding the security solutions provided by vendors helps organizations address these challenges effectively. The research helps organizations prioritize security considerations and select vendors offering robust security features, enhancing network security.

iv. Future Research and Development:

The findings of this research can serve as a foundation for future studies in SD-WAN security. It identifies gaps, strengths, and weaknesses in the current solutions, which can inspire further research and development efforts to improve SD-WAN security technologies and practices.

This study is significant as it contributes to the body of knowledge on SD-WAN security, assists organizations in making informed decisions, promote best practices, enhances network security, and sets the stage for future advancements in SD-WAN security solutions.

The study findings demonstrated that by offering SD-WAN solutions, company networks can be exposed to new vulnerabilities. Attackers would readily take advantage of these flaws and cause harm and loss to the organizations given the size of previous attacks on enterprise networks.

Therefore, before supplying the technology to businesses, suppliers and service providers should be aware of these vulnerabilities. As a precaution, they should also put in place sufficient defences to lessen the threats. If they choose to disregard these security flaws, SD-WAN will be the target of numerous assaults after being widely implemented. All findings were escalated to the vendor, and based on the prompt responses, there are signs of improvement in the security deployment of the product.

Organizations should carefully evaluate their specific needs, assess the maturity and compatibility of solutions, and consider working with trusted vendors or consulting experts to implement them effectively. Staying informed about the latest advancements in these technologies and their impact on SD-WAN security is essential for adapting security strategies accordingly. Key improvements include data security and data breach analysis, learning more about penetration testing, using paid tools for strong data, and allocating sufficient time for research.

Overall, the study highlights the growing importance of SD-WAN security and the need for robust solutions to address the unique challenges of SD-WAN deployments. Encryption, authentication, access control, and threat intelligence are critical security features in SD-WAN solutions. Best practices such as a defense-in-depth approach, zero-trust networking, regular security audits, and partnering with secure SD-WAN vendors are recommended to effectively implement secure SD-WAN solutions. Emerging trends, including SASE, zero-trust networking, and AI in threat detection, hold promise for further enhancing SD-WAN security. Continued research and collaboration between academia and industry are essential to stay ahead of evolving threats and ensure the secure adoption of SD-WAN technologies.

ACKNOWLEDGEMENT

The authors would like to thank to all School of Computing members who involved in this study. This study was conducted for the purpose of Cyber Security Research Project. This work was supported by Universiti Utara Malaysia.