Journal of Theoretical and Applied Information Technology
15th August 2023. Vol.101. No 15
© 2023 Little Lion Scientific

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

NEXT GENERATION SD-WAN WITH IDPS

JOSEPH NG POH SOON, PHAN KOO YUEN, FADHILAH NUR RANIA, CHAN JIA YI, FONG JUN YIP, NG EE SERN, SITI ZUBAIDA BINTI ZULKIFLI
Faculty of Data Science and Information Technology, INTI International University, Malaysia
Faculty of Information and Communication Technology, Universiti Tunku Abdul Rahman, Malaysia;

E-mail: joseph.ng@newinti.edu.my, phanky@utar.edu.my
i19018013@student.newinti.edu.my, i21020638@student.newinti.edu.my,
i20018760@student.newinti.edu.my, i20018662@student.newinti.edu.my,
i20018611@student.newinti.edu.my,

ABSTRACT

The Wide Area Network and firewall are the current networking technologies that are widely used in most enterprises. However, due to the rapid development of new technologies, there is a rising demand for a new efficient networking solution that could overcome the current technologies' limitations and cater to the end users' new requirements. This research integrated Software Defined Wide Area Networks and Intrusion Detection and Prevention Systems. This paper aims to conduct a systematic review where the effectiveness and benefits of the new technologies are investigated as a proposed solution. that optimized the network to prevent the trombone effect that degrades network performance while recognising malicious activities and preventing attacks. It can also easily detect and alert the network administrator. Combining both technologies is the proposed solution that will enable network performance and security improvements, resulting in an efficient network solution.

Keywords: *Firewall, WAN, SD-WAN, IDPS, Network*

1. INTRODUCTION

In this rapid era of technological advancements, new technologies have been developed. This paper will be the main topic components of WAN, SD-WAN, Firewall, and IDPS. As technology advances, improvements and enhancements are designed to overcome the limitations of the previous version of technologies [1-2]. WAN and firewalls have been prominent topics in network environments. The existing network technologies and infrastructures, such as WAN and firewalls, must satisfy the end user's current demands. Many limitations are being discovered in WAN and firewalls in which new technologies must be discussed and implemented [3]. Most prior studies often discussed the basic concept and features of the SD-WAN and IDPS. However, what differentiates this paper from previous research is that prior studies emphasize how beneficial it is to implement the SD-WAN and IDPS to replace the traditional WAN and firewall. As evidence, [1] proves that the SD-WAN has less latency than the traditional WAN because of the smart routing management. Apart from that, previous research also highlighted how the existing architecture is modified, thus examining their performance operating in different environments such as the cloud Internet of Things (loTs) environment [1] [2] [3] [4] [5] [6] [7]. On the contrary, this paper highlights how combining the existing SD-WAN and IDPS could build a secure and efficient network environment.

As for limitations, the existing research is thoroughly conducted depending on the previous studies. It might occur some inaccurate outcomes. [8] mentioned some challenges of SD-WAN and IDPS that might deserve further investigation, including traffic engineering and monitoring and security. To sum up, this paper proposed an efficient networking solution where SD-WAN and IDPS would be utilized to improve security measures and network quality.

1.1 Problem Statement

Due to the fast evolution of technology, there is a rising need for a better network in terms of effectiveness, efficiency, security, and cost [9] [10] [11]. Concerning WAN, it can be said that it can no longer meet the demands of today's enterprises. WAN is flawed and has many limitations due to the high cost, low utilization, and manual maintenance.

A firewall is the first line of defence in network security. But due to the security policy and firewall rules set by the network administrator, it can only monitor data traffic to filter out suspicious or malicious traffic. Still, it cannot defend against nontechnical security concerns, like social engineering and attackers from the internal network.

1.2 Research Questions & Objectives

As mentioned above, the issues and problems with the current network solutions can be resolved with the proposed solution. Hence, this research paper was done to meet the research objective through the questions stated below:

RQ1: How can IDPS detect and stop attacks without affecting network performance?

RQ2: How does SD-WAN improve network bandwidth and performance?

RQ3: How can SD-WAN meet the requirements of future network demands?

These are the research questions identified for the value creation and listed below are the research objectives necessary to this study.

RO1: To find out if IDPS systems can detect and stop potential attacks without affecting network performance.

RO2: To find out how the SD-WAN improves the network bandwidth and performance.

RO3: To find out if SD-WAN can meet the requirements of future network demands.

Based on the research questions and objectives, this study aims to examine the effectiveness and benefits of the proposed solution, which is the implementation of SD-WAN with IDPS. The proposed solution is expected to meet the demands for an efficient and secure network that will be used in place of a traditional network consisting of a WAN and a firewall.

2. METHODOLOGY

A systematic review is conducted in this paper to examine the efficient network solution called SD-WAN with IDPS, which is the study's goal. The researcher define the research question before searching for previous studies to ensure everything stays within scope. Unlike other research, which consists of experimental and questionnaire data, this bibliographic review is conducted based on the literature analysis. This method minimizes the research bias by connecting all relevant evidence.

The authors reviewed the relevant published studies and journals through various databases such as Google Scholar, ResearchGate, and IEEE Xplore to obtain the literature papers that address the research questions. Several keywords such as "Software Defined Wide Area Network", "SD-WAN", "Intrusion Detection Prevention System", "IDPS", "Intrusion Detection System", "IDS" "Intrusion Prevention System", "IPS", "security", "efficient network", "capabilities" and "architecture" are utilized to allow the search engines to find these relevant papers. Apart from this, the literature papers are all written in English and were published in the last 10 years. Any papers that are not related to SD-WAN and IDPS will be excluded. However, due to the limited published papers on new technologies such as SD-WAN and IDPS, other literature papers on network infrastructure and environment are also considered.

After screening the relevant published studies and journals, data that aligns with our research objectives were extracted and interpreted. The result of our study leads to an efficient network solution that incorporates both the benefits of SD-WAN and IDPS. Nevertheless, there is still a potential bias in the systematic review where the previous studies might overpredict or overestimate the outcome. Upon review, these findings prove that the effectiveness of the proposed solution is excellent.

3. LITERATURE REVIEW

3.1 Current Operation Process and Technology Environment

In the intranet environment, many tools have been used to secure the host from outside, and the firewall was one of them. Nowadays, almost all the time, when people hear about a Firewall, people will think that a Firewall is a security that helps to prevent any unauthorized or malicious software from trying to get permission to access the computer. But in other words, a Firewall is a mechanism that will help control and monitor the network traffic and protect the external and internal communications and system. The four categories for Firewalls are stateful inspection firewall, packet filtering firewall, application-level gateway, and circuit-level gateway [12]. These four categories are based on the functionality of the firewall system. Moreover, the firewall will also protect those with industrial protocols, for example, Distributed Network Protocol 3 and Modbus [7] [13]. However, firewalls that use a stateful inspection or packet filtering are unable to examine payload data that carries malicious information within their protocols [14]. Many firewall systems are necessary for large-scale network traffic inspection because a firewall's traffic inspection capabilities are constrained by network processing speed, memory size, and power usage

[15]. A firewall cannot function or process information effectively when traffic volume increases. The firewall offers secure significant border security for the intranet.

As for the extranet, the focused tool will be the WAN (Wide Area Network). WAN is a telecommunications network, one of the essential components of deployment in the current Internet world. Multiple Local Area Networks (LANs) dispersed across various geographic areas are connected by a Wide Area Network (WAN). In the early 1980s, the first WAN deployment was released to the public. In the following years, the WANs were continuously improved. At first, leased lines were used in vast area connections to link two distant facilities, but the disadvantages are that leased lines are high costs and constrained speeds of connection method. In today's world, many businesses and organizations use WANs to transfer important data between their corporate headquarters, distant business branches, and even cloud data centres. With the advent of Frame Relay, Asynchronous Transfer Mode, and Multi-Protocol Label Switching, the WAN saw numerous changes. Leased lines and virtual private networks are a couple of the many WAN options suggested over the years. Each technology or solution takes a distinct stance in the dependability, cost, and Quality of Service (QoS) trade-off. Out of all these technologies, MPLS is the one that is now being widely used and can efficiently guarantee Quality of Service (QoS). Additionally, nearly any underlay network can be used to establish a VPN overlay WAN, especially when linking business sites to the Internet via direct, low-cost connections [3]

3.2 Current Process and Technology Limitations

3.2.1 Firewall

Firewalls can be classified as either host-based or network-based, depending on where the firewall is located. A network-based firewall is situated at the ingress backbone point and inspects data traffic to filter abnormal traffic flows or malicious activities. A host-based firewall is situated at the network edge and detects assaults within a given host. Depending on how the firewall inspects packets, it can be classified as a stateful inspection firewall, packet filtering firewall, application-level gateway, and circuit-level gateway. [12]. However, in some cases, firewalls that use a stateful inspection or packet filtering are unable to examine payload data that carries malicious information within their protocols. During large-scale network traffic inspection, many firewall systems are necessary because a firewall's traffic inspection capabilities are constrained by network processing speed, memory size, and power usage [8]. When traffic volume increases, a firewall cannot function or process information effectively.

Secure major border security for the intranet is offered by the firewall. However, some technologies and extendable protocols like Internet Printing Protocol (IPP) and Web Distributed Authoring and Versioning (WebDAV) can bypass standard firewall configurations by exploiting HTTP with authentication and encryption, which can be used to transfer malicious files [20]. Some protocols that claim to apply to firewalls are made to work around how most firewalls are set up.

To some extent, the firewall functions as a gateway and simplifies network security management. This is because an inside network administrative setting firewall cannot be held liable for its poor administrative settings and security policies. Internal users cannot be prevented from accessing malicious websites or approving external threats that leave the system vulnerable [9] [10] [11] [17]. As a result, the intruder may discover an open door behind the firewall, which the network administrator cannot prevent.

3.2.2 Wide area network (WAN)

Over the decades, a variety of WAN solutions have been developed, including leased lines, Frame Relays, Multiprotocol Label Switching (MPLS), and Virtual Private Networks (VPN) [3] ~~[10]~~. Each of the solutions has its disadvantages and advantages. However, MPLS has limitations ranging from cost, inefficiencies, and flexibility [7]. MPLS is costly as it guarantees Quality of Service (QoS). It is also inefficient as MPLS requires the installation of specific hardware to manage the application traffic. As more and more applications require high bandwidth, MPLS is known to be incapable of dealing with the needs of the modern world [8][18].

Moreover, it is found that some limitations and challenges come with the use of a traditional WAN. This is due to its complex nature, which makes it dependent on a third party, which usually is an internet service provider (ISP). It can be said that WAN consists of many devices, all of which must be configured to ensure that the network will run without issue. These configurations are generally done manually, which is time-consuming and can result in errors [19]. Not only that but in the event of having to prepare for an increase in data traffic, flexible and quick upgrades are difficult to be implemented in the network.

Other than that, the implementation of WAN is high in cost [19]. This is because the more extensive the network, the more costly it will need. It was found that internet traffic, meaning that the cost of WAN bandwidth, will also increase in the coming years [8] [18]. Because of this, the demand and supply of WAN and its costs should be considered before implementation.

The average utilization of bandwidth in WAN is also not fully optimized. It is found that the average utilization of a busy network in a WAN is just 40-60% [17]. This is due to two reasons which are link and device failures and the lack of coordination among services that use the same network. This is because WANs are usually over-provisioned, and services deliver traffic whenever and however they want, which in turn causes a high spike in bandwidth usage.

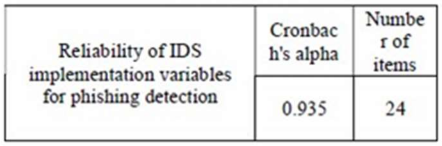
3.3 Future Process Environment Using New Technology

A software-defined wide area network (SD-WAN) is a new WAN solution that has been developed to overcome the limitations of MPLS. SD-WAN utilizes software-defined networking (SDN) approach by using software-based controllers to communicate with the underlying hardware and software [12]. SDN has made it simple to employ open virtual switches and programmable APIs without installing specialized hardware [11]. This approach allows SD-WAN to reduce the costs of network infrastructures and provides flexibility in the network [13]. It ensures QoS is achieved without compromising the cost [10]. SD-WAN selects the path of least resistance for application transport, which decreases the cost of the WAN and maximizes available bandwidth by connecting to the cloud [12].

The development of IDPS provides a robust platform for network security [13]. It is acknowledged as one of the central core architectural solutions for an organization's information technology network security, as the IDPS can recognize malicious activities and prevent attacks from occurring [1] [2]. Even if an attack is being entered, it can easily detect and alert the network administrator, who can then take the necessary action. With the help of IDPS, the organization does not need to worry about its valuable and confidential data being hacked and stolen. It increases the security of sensitive information while preventing the negative impacts of network attacks [1].

4. RESEARCH METHODS

Table 1: Information of the Reliability Statistics of Research Variables [11]



Reliability of IDS implementation variables for phishing detection	Cronbach's alpha	Number of items
	0.935	24

The finding in Table 1 shows that the research variable of Cronbach's alpha is greater than 0.9, meaning that the reliability of the IDS implementation for security threats in the organization is excellent [4] [5] [6] [22] [23] [24] [25] [26] [27] [28] [29] [30][31].

5.0 FINDINGS AND DISCUSSION

5.1 Conceptual Solutions

5.2 Software-Defined Wide Area Network (SD-WAN)

SD-WAN comprises three planes: data, control, and application. The data plane is responsible for data forwarding and bandwidth virtualization [8] [18]. It facilitates communication between different site locations by creating a logical architecture that operates on the physical infrastructure to ensure data transmission [1]. The control plane has several network functions that network administrators may customize to further suit their needs [8] [18]. This plane would also administer the configurations of devices in the network including its policies and routing information [1]. The application or orchestration plane enables network providers and software developers to transform their requirements into network configurations [8] [18]. This layer would also provide policies and a security framework for the business [1].

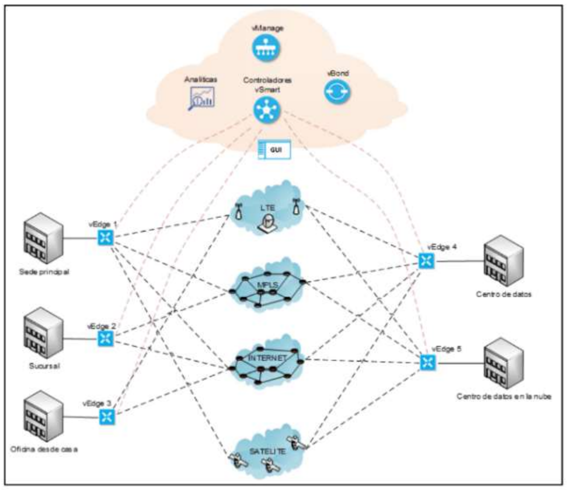


Figure 1: SD-WAN Network Architecture [16]

5.2.1 SD-WAN architecture

The figure depicts the architecture of SD-WAN, which consists of vEdge routers, vManage dashboard, vBond Orchestrator, and vSmart Controller. The vEdge routers exist at the site location, which ensures communication is established through a secure and private tunnel connection [1]. The vManage allows network administrators to manage the network via a dashboard. On the other hand, the vSmart Controller controls the routing and data traffic of the vEdge routers, while the vBond Orchestrator establishes connections between the vEdge routers and the vSmart Controller.

5.2.2 SD-WAN capabilities

1) Supports Various Types of Connections: SD-WAN could support many types of connections that enterprises commonly use, such as MPLS, LTE, and Wireless connections, in which it selects the least path of resistance for application transport [8]. The technologies used for network detection and signal significantly impact network bandwidth. Therefore, utilizing SD-WAN would substantially optimize the use of network bandwidth.

2) Policy-Based-Routing: SD-WAN can route data based on a set of criteria that network administrators have configured. If a communication failure occurs in one of the paths, the policy-based routing would significantly maintain the network by switching the paths to other available connections in the network [32]. SD-WAN reduces network downtime, delay, and latency by utilizing policy based-routing, which prevents the trombone effect that degrades network performance, which is the main weakness of MPLS [8] [18].

3) Cloud Integration: As more and more enterprises utilize Software-as-a-Service (SaaS) and Infrastructure-as-a-Service (IaaS) applications, SD-WAN has cloud integration capabilities where it can be configured within the domain of the cloud service provider for IaaS and connect itself to the nearest point of presence for SaaS [8] [9] [10] [33]. This streamlines the routing from a branch location to the data centre. As a result, traffic backhaul from the cloud could be minimized with SD-WAN.

5.2.3 Performance comparison between SD-WAN and traditional WAN

According to [34], the traditional WAN solution has a higher latency when the network is saturated. A higher latency also applies to SD-WAN in a saturated network. However, it is less significant than a traditional WAN. This is due to the smart routing management by the vSmart Controller [34]

Table 2: Latency Between SD-WAN And Traditional Wan [34]

			WIthout Saturation	With Saturation	
	Hop	IP	Final trace (ms)	Final trace (ms)	Difference (ms)
Traditional WAN	0	192.168.10.10	0.379	0.281	-0.10
	1	192.168.10.1	1.392	1.707	0.32
	2	10.10.10.254	2.693	790.459	787.77
	3	3.3.3.2	3.768	2540.401	2536.63
	4	30.30.30.1	4.892	5.298	0.41
	5	192.168.20.10	8.479	8.162	-0.32
SDWAN	0	192.168.10.10	0.575	1.053	0.48
	1	192.168.10.1	1.702	15.051	13.35
	2	192.168.20.1	4.111	34.763	30.65
	3	192.168.20.10	3.65	81.746	78.10

Table 3: Jitter Between SD-WAN And Traditional Wan [34]

			WIthout Saturation	With Saturation	
	Hop	IP	Jitter (ms)	Jitter (ms)	Difference (ms)
Traditional WAN	0	192.168.10.10	0.552	0.798	0.25
	1	192.168.10.1	0.527	1.086	0.56
	2	10.10.10.254	1.453	609.051	607.60
	3	3.3.3.2	1.301	495.176	493.88
	4	30.30.30.1	2.592	59.992	57.40
	5	192.168.20.10	1.176	182.506	181.33
SDWAN	0	192.168.10.10	0.28	0.29	0.01
	1	192.168.10.1	1.091	3.819	2.73
	2	192.168.20.1	1.336	7.11	5.77
	3	192.168.20.10	1.054	14.724	13.67

SD-WAN also has a lower value of jitter where latency variation during data transmission is significantly lower than traditional WAN. The findings from [34] prove that SD-WAN has a higher Quality of Service (QoS) than traditional WAN.

5.3 Intrusion Detection and Prevention Systems (IDPS)

IDPS can be proposed as a solution because of its detection, prevention, and reaction capability when facing intrusion. IDPS cannot be recognizable to attackers, thus limiting communication with some other network components [2]. Another reason to use IDPS is to overcome the limitations of the traditional firewalls, which are insufficient to adapt to the global utilization of the Internet that generate more new security threats. Generally, IDPS performs monitoring, detection, and reaction operation [5].

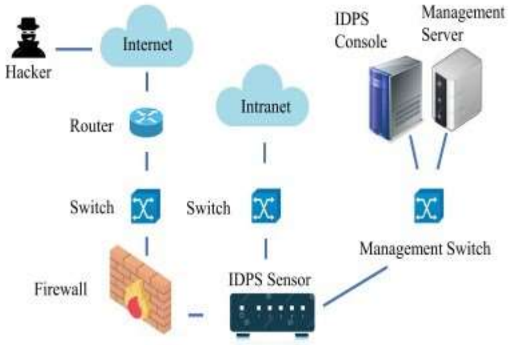


Figure 2: Working Principle of IDPS [2]

As illustrated in Figure 2, IDPS architecture consists of a firewall, a sensor, a management server, and a console [2]. A firewall is deployed at the network's entry point, followed by the IDPS sensor that is used to monitor and analyze incoming network traffic. When suspicious activity is detected, it searches for pre-defined patterns to determine whether that behaviour is an attack. An alarm message can be sent to the network administrator if there is a matched pattern. IDPS will send the information to the management server and console simultaneously [6] [35]

5.3.1 Intrusion detection systems (IDS)

As mentioned above, IDS is used to monitor the events occurring in the network and analyze them for signals of potential incidents, which are violations or suspicious activities of attacks on computer security regulations [36]. Incidents can be caused by a variety of aspects, such as malware, worms, probe attacks, unauthorized access, and vice-versa. Traditionally, the firewall filters the traffic based on IP addresses and port numbers. In this case, an attacker could utilize an HTTP port to attack the organization's web server. In contrast, with the use of IDS, it compares the signature of web traffic with the database known attack signatures, and then it distinguishes between the legitimate traffic and the attempted attack on the web server. Rather than using a firewall that only inspects the network packet's header, it is encouraged to utilize IDS which provides a full security inspection of both the network packet's header and data contents. It safeguards the network against the attack.

5.3.2 Intrusion prevention systems (IPS)

IPS was developed when the IDS could not combat the increased number of cyber-attacks [37]. The IPS technology differs from IDS in that it can prevent and stop the detected threat from being successful. When suspicious traffic is detected, the IPS automatically blocks it, logs the attack, and adds the source IP address to the block list for a certain amount of time. The IPS are implemented in-line in the network, generally in layer 2. It searches for potentially harmful incoming packets to enhance the network firewall's work that only actively identifies traffic based on IP address and port numbers [21]. It ensures protection against the intrusions that take place in the network. As an inline security component, the IPS works fast and also be able to respond to the attack accurately to eliminate threats because the intrusion can happen in near-real time. Furthermore, other than prevention capability, there are several response techniques applied by the IPS to mitigate the attack when the attack is entered into the network environment [21]:

1) Blocking the network traffic: When the attack enters the network, IPS can stop it by terminating the attacker’s connection and blocking access to the target user account or IP source address.

2) Change the security environment: IPS can change the security control configuration to interrupt an attack. For example, in the network firewall configuration that denies access to the target system, the IPS can identify the latest patches of the application to a system. As long as IPS detects an intrusion event, it will reconfigure and reprogram the firewall to increase the protection against previously unknown vulnerabilities. This helps to prevent similar attacks in the future.

3) Change the attack content: IPS has capable of removing and dropping the malicious data packets from an attack and declaring it harmless. It reduces the risk of severe network and resource damage. For example, the IPS can eliminate an email with a malicious file attachment, and the organization recipients will receive a clean email. Also, IPS can replace malicious content such as false links with warnings messages.

4) Reset the connection: IPS can reset the TCP connection by repackaging the payloads and removing infected attachments from servers. When the attack is entered, IPS immediately terminates the TCP session that is being exploited by an outsider attacker. It closes the connection between the sender and the receiver or to the web server, thus informing the sender to establish another new connection and resend the traffic if necessary.

5.3.3 IDPS security capabilities

IDPS technologies offer a wide range of security capabilities based on different types, namely information gathering, logging, detection, and prevention.

1) Information gathering: IDPS able to collect information by observing the system activities on the network. It can recognize the software and application used by hosts and identify the general characteristic of a network. Blacklists and whitelists are included in IDPS, allowing the administrators to determine whether they should block the coming activity or not [6]. With this, the network can grasp the information and understand the purpose of that entire event coming into the network.

2) Logging: IDPS collects, and stores data related to detected events over a period. The logged data can be utilized to confirm the source of compromise effectively. The administrators will keep those logs locally and centrally to support the integrity and availability of the data. Logging is crucial as it helps the organization identify the network's pattern of activities. As a result, it provides the standard of compromise.

3) Detection: IDPS detects the presence of malicious threats by utilizing signature-based detection, anomaly-based detection, and protocol-based techniques [6]. From the latest findings [11], IDPS increasingly leverages machine learning, data mining, and artificial intelligence technologies to process large amounts of data and identify threats that signature and anomaly detection would miss. An attack will be recognized when some traffic is not conforming to the regular standard. With this, it provided a defence against both internal and external threats.

4) Prevention: IDPS is mainly focused on the IPS where it can adjust the firewall rules and avoid malicious traffic when an attack is detected. The main objective of this capability is to prevent malicious attacks from destroying the network. When IDS generates the alert, the network administrator can either enable or disable the prevention feature in IPS, making them operate as IDS [21]. In addition, when an attack is entered into the network, the response techniques applied by IPS such as blocking IP addresses, dropping malicious data packets, resetting the connections, and reconfiguring a firewall make the IDPS becomes a robust platform for network security.

The study of IDS and IPS has provided the realization of the significance of IDPS technology in securing the network environment [11]. mentioned that IDPS could detect and stop potential attacks without affecting network performance. To summarize, it is essential to have detection, prevention, and reaction capabilities in an adequate security network.

5.4 SD-WAN With IDPS

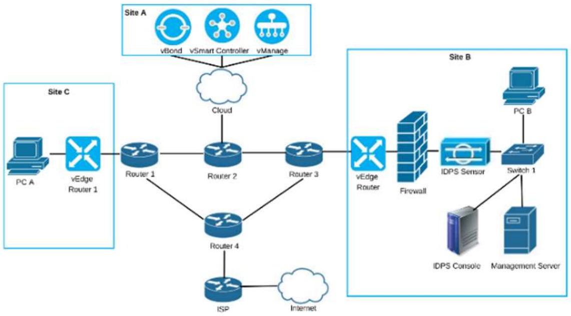


Figure 3: SD-WAN with IDPS

From the findings above, an efficient network solution would be established by leveraging the benefits of SD-WAN and IDPS together. SD-WAN would significantly meet the network demands as enterprises are moving towards SaaS and IaaS applications. On the other hand, IDPS would establish better security for the enterprise's internal network.

To implement the SD-WAN with IDPS security, a mix of hardware and software components is necessary. These components include network configuration and monitoring software, SD-WAN appliances, and IDPS sensors. There are some limitations when implementing IDPS as it may result in some additional network overhead. The IDPS sensors must analyze network traffic in real-time to detect threats, which might raise the CPU and memory use of the hardware. Despite the limitation of IDPS, with the advancement of hardware and software technologies, it is now possible to use SD-WAN with IDPS security without experiencing significant performance degradation.

Overall, SD-WAN with IDPS can offer many enterprises a highly effective and efficient network solution. It can lessen network outages, increase network efficiency, and strengthen network security. However, the outcomes will depend on the enterprises' needs and goals and the efficiency of the system's configuration and operation. The network's scale, the desired level of security, and the resources available will all impact how the solution is designed and implemented. So, it is essential to carefully evaluate the needs of the enterprise and install SD-WAN and IDPS in a way that is in line with those needs.

5.4.1 Value creations

1) Improved operational efficiency: As the utilization of SaaS and IaaS applications grows in enterprises, supplying the demand for a network with cloud integration capabilities is crucial. SD-

WAN can minimize the traffic backhaul from the cloud as it streamlines the routing from the branch location to the data centre resulting in improved operational efficiency in the network [33]. SD-WAN also enables the flexibility of enterprises that wishes to backhaul specific traffic back to their data centre for security purposes by routing data based on a set of criteria that network administrators have configured.

2) Enhance the reputation: Both the detection and response capabilities in IDPS technologies undoubtedly safeguard the network environment. A secured network environment can promote safe browsing and improve reputation by preventing suspicious outsiders from being accessible to the internal network environment [34]. As a result, denying access to these unknown outsiders reduces the chance that these infections and malware will be introduced into the company network.

Integrating SD-WAN with the cloud could also enhance the enterprise's reputation by providing excellent user experience through faster network access for SaaS and IaaS applications by utilizing Policy Based-Routing [35]. Once the client knows the company systems are being protected and are providing excellent user experience, their confidence in trusting and using the company's resources rises, enhancing their reputation to the public [36].

3) Financial benefit: An SDN approach has enabled SD-WAN to utilize software to establish communications without the need to install specialized hardware, which reduces the costs of network infrastructures [38]. Different enterprises may use more than one type of connection of which SD-WAN is capable. It has been proven that SD-WAN has a lower latency and jitter than traditional WAN. It can select the best path with the least resistance, using all the available network bandwidth while maintaining excellent performance for a lower price.

5.4.2 Strategy and guideline in the real application

SD-WAN with IDPS is proposed as a framework and strategy in real-world applications to address today's growing security challenges and network performance. Traditional network security solutions such as firewalls and WAN are no longer adequate to suffice the latest need of enterprises and to protect against the latest threats as they increasingly rely on cloud-based applications, mobile devices, and remote workers.

In terms of practical applications, SD-WAN with IDPS can be used in a variety of settings, including:

1. Multi-site enterprises need to safely and effectively connect their remote sites and data centres.
2. Government organizations often handle confidential and sensitive data that require real-time monitoring and threat protection.
3. Healthcare businesses must provide dependable and effective connectivity between their sites while simultaneously guaranteeing the confidentiality and privacy of patient data.
4. Financial institutions must ensure both reliable and effective connectivity across their sites and adhere to legal standards for security and data protection.

Some considerations that must be considered when deploying SD-WAN with IDPS are as follows:

1. Carrying out a comprehensive risk analysis to determine the organization's unique security requirements and business needs.
2. Establishing thorough security policies and processes to ensure reliable and efficient security controls.
3. Ensuring the compatibility of the current network infrastructures with the proposed solution, SD-WAN with IDPS.
4. Consistently observing and examining network traffic to find potential threats and weak points.

6. CONCLUSION

Technological advancements have changed how enterprises operate their business. Cloud applications have made it evident that the current network infrastructures do not suffice end-user demands due to the traffic backhaul resulting in slower network access. There is also a dire need to enhance the internal network's security measures to prevent cyberattacks that could negatively impact enterprises. Therefore, an efficient and secure networking solution is necessary to maintain the enterprise's productivity and reputation. The proposed efficient networking solution has addressed the research objectives where SD-WAN and IDPS provide a flexible and secure network. SD-WAN could overcome the limitations of WAN, such as the complexity in configuration, high implementation cost, and less optimization in bandwidth utilization. At the same time, the IDPS has a detection and prevention mechanism which allows the enterprise to detect and stop malicious activities while maintaining the network performance in which firewalls are lacking. In the future, it will be possible to configure a new network environment, as illustrated in the paper, so that both the internal and external networks can fulfil the current demands of the end user. To summarize, SD-WAN with IDPS could keep the enterprise competitive by staying up to date with the latest cost-effective technological advancements that provide operational efficiency. As a result, the enterprise's reputation would also improve.

REFERENCES

[1] L. Santos, C. Rabadao, and R. Goncalves, “Intrusion detection systems in the Internet of Things: A literature review”, *13th Iberian Conference on Information Systems and Technologies (CISTI)*, June 2018, doi: 10.23919/cisti.2018.8399291.

[2] N. Mazhar, R. Salleh, M. Asif, and M. Zeeshan, “SDN based Intrusion Detection and Prevention Systems using Manufacturer Usage Description: A Survey”, *International Journal of Advanced Computer Science and Applications*, Vol. 11, No. 12, 2020, pp. 717–718, 721–722, doi: 10.14569/ijacsa.2020.0111283.

[3] S. Troia, F. Sapienza, L. Vare, and G. Maier, "On Deep Reinforcement Learning for Traffic Engineering in SD-WAN", *IEEE Journal on Selected Areas in Communications*, Vol. 39, No. 7, 2020, pp. 2198-2212, doi: 10.1109/jsac.2020.3041385.

[4] S. Lee, K.-Y. Chan, and T.-Y. Chen, “Design and Implementation of an SD-WAN VPN System to Support Multipath and Multi-WAN-Hop Routing in the Public Internet”, *TechRxiv*, 2020, doi: 10.36227/techrxiv.12423701.v1.

[5] A. Javadpour, P. Pinto, F. Ja'fari, and W. Zhang, “DMAIDPS: a distributed multi-agent intrusion detection and prevention system for cloud IoT environments”, *Cluster Computing*, 2022, doi: 10.1007/s10586-022-03621-3.

[6] P. I. Radoglou-Grammatikis and P. G. Sarigiannidis, “Securing the Smart Grid: A Comprehensive Compilation of Intrusion Detection and Prevention Systems”, *IEEE Access*, Vol. 7, 2019, pp. 46600, doi: 10.1109/access.2019.2909807.

[7] S. Badotra, and S. Panda, “A Survey on Software Defined Wide Area Network”, *International Journal of Applied Science and Engineering*, Vol. 17, 2020, doi: 10.6703/IJASE.202003_17(1).059.

[8] Z. Qin, “SD-WAN for Bandwidth and Delay Improvements on the Internet”, *SHS Web of Conferences*, Vol. 144, 2022, pp. 02004, doi: 10.1007/s10586-022-03621-3.

[9] Ala Mohamed Ali Mohamed, Poh Soon Joseph Ng, Wong See Wan, Phan Koo Yuen, and Lim Ean Heng, “Hot Standby Router Protocol for a Private University in Malaysia”, *International Journal of Scientific Engineering and Technology*, 4(3), 2015, pp. 172-174.

[10] Sathis Kumar Batumalai, Joseph Ng Poh Soon, Choo Peng Yin, Wong See Wan, Phan Koo Yuen, and Lim Eng Heng, “IP redundancy and load balancing with gateway load balancing protocol”, *International Journal of Scientific Engineering and Technology*, 4(3), 2015, pp. 218-222

[11] A. Sahifa and M. Gerami, “Implementation of Intrusion Detection Systems in Order to Detect Phishing in the Banking Industry”, *International Journal of Information & Communication Technology Research*, Vol. 12, No. 2, 2000, pp. 23-28.

[12] P. Radoglou-Grammatikis, P. Sarigiannidis, T. Liatifis, T. Apostolakos, and S. Oikonomou, “An overview of the firewall systems in the Smart Grid Paradigm,” *2018 Global Information Infrastructure and Networking Symposium (GIIS)*, 2018.

[13] C. O. Akanbi, I. K. Ogundoyin, J. O. Akintola and K. Ameenah, “A Prototype Model of an IoT-based Door System using Double-access Fingerprint Technique”, *NIGERIAN JOURNAL OF TECHNOLOGICAL DEVELOPMENT*, Vol. 17, No. 2, 2020, pp. 142-149.

[14] D. Li, H. Guo, J. Zhou, L. Zhou, and J. W. Wong, “SCADAWALL: A CPI-enabled firewall model for SCADA security”, *Computers & Security*, Vol. 80, 2019, pp. 134–154.

[15] S. Kim, S. Yoon, J. Narantuya and H. Lim, “Secure Collecting, Optimizing, and Deploying of Firewall Rules in Software-Defined Networks”, *IEEE Access*, Vol. 8, 2020, pp. 15166-15177, doi: 10.1109

[16] G. Zhang, and W. Li, “A Security Reinforcement Scheme for the Server”, *2018 4th International Conference on Education, Management and Information Technology (ICEMIT 2018)*, 2018.

[17] A. Abro, A. U. Nabi, and M. Ahmed, "An Overview of Firewall Types, Technologies, and Functionalities", *International Journal of Computing and Related Technologies*, Vol. 3, No. 1, 2022.

[18] JosephNg, P.S., Eaw H.C., "Still Technology Acceptance Model? Reborn: Exostructure as a Service Model.", *Int. J. Bus. Inf. Syst*., 2021.

[19] Z. Yang, Y. Cui, B. Li, Y. Liu and Y. Xu, "Software-Defined Wide Area Network (SD-WAN): Architecture, Advances and Opportunities", *2019 28th International Conference on Computer Communication and Networks (ICCCN)*, 2019, pp. 1-9, doi: 10.1109/ICCCN.2019.8847124.

[20] O. Michel and E. Keller, "SDN in wide-area networks: A survey", *2017 Fourth International Conference on Software Defined Systems (SDS)*, 2017, pp. 37-42, doi: 10.1109/SDS.2017.7939138.

[21] S. Thapa and A. Mailewa, "The Role of Intrusion Detection/Prevention Systems in Modern Computer Networks: A Review", *Easy Chair Publications*, 2020, pp. 4-8

[22] JosephNg P.S., and Eaw H.C., "Making financial sense from EaaS for "MSE" during economic uncertainty", *Adv. Intell. Syst. Comput,* Vol. 1, 2021, pp. 976-989.

[23] JosephNg, "P. Economic Turbulence and EaaS Grid Computing", *Preprints, September 3*, 2021, 2021090329,https://doi.org/10.20944/preprints202109.0329.v1.

[24] JosephNg, "P.S. EaaS Infrastructure Disruptor for "MSE". *Int. J. Bus. Inf. Syst*, 2019, pp. 373-385.

[25] JosephNg, "P.S. EaaS Optimization: Available yet hidden information technology infrastructure inside Medium Size Enterprise", *J. Technol. Forecast. Soc. Chang.*, Vol. 132, 2018, pp. 165-173.

[26] Soon, J.P., and Moy, K.C., "Beyond barebone cloud infrastructure services: Stumbling competitiveness during economic turbulence", *J. Sci. Technol*. Vol. 24, 2016, pp. 101–121.

[27] Soon, J.N.P., Wan, W.S., Yuean, P.K., and Heng, L.J., "Barebone Cloud IaaS: Revitalisation Disruptive Technology", *Int. J. Bus. Inf. Syst.*, Vol. 18, 2015, pp. 107–126.

[28] Joseph, N.P.S., Mahmood A.K., Choo P.Y., Wong S.W., Phan K.Y., and Lim E.H, "IaaS Cloud Optimization during Economic Turbulence for Malaysia Small and Medium Enterprise", *Int. J. Bus. Inf. Syst.*, Vol. 16, No. 2, 2014, pp. 196-208.

[29] Joseph, N.P.S., Mahmood, A.K., Choo, P.Y., Wong S.W., Phan K.Y., and Lim E.H., "Battles in volatile information and communication technology landscape: The Malaysia small and medium enterprise case", *Int. J. Bus. Inf. Syst.*, Vol. 13, 2013, pp. 217-234.

[30] Joseph N.P.S., Kang C.M., Mahmood A.K., Choo P.Y., Wong S.W., Phan K.Y., and Lim E.H., "Exostructure Services for Infrastructure Resources Optimization", *J. Telecommun. Electron. Comput. Eng.*, Vol. 8, 2016, pp. 65-69.

[31] Joseph N.P.S., Choo P., Wong S., Phan K., and Lim E., "Hibernating ICT Infrastructure During Rainy Days", *J. Emerg. Trends Comput. Inf. Sci.*, Vol.3, 2012, pp. 112-116.

[32] S. P. Rachuri, A. A. Ansari, D. Tandur, A. A. Kherani and S. Chouksey, "Network-Coded SD-WAN in Multi-Access Systems for Delay Control", *2019 International Conference on contemporary Computing and Informatics (IC3I)*, 2019, pp. 32-37, doi: 10.1109/IC3I46837.2019.9055565.

[33] Joseph Ng Poh Soon, Shaaban Hassan Ramadhan Abdulla, Lim Eng Heng Choo Peng Yin, Wong See Wan, and Phan Koo Yuen, "Implementing of Virtual Router Redundancy Protocol in a Private University", *Journal of Industrial and Intelligent Information*, 1(4), 2013, pp. 255-259.

[34] C. J. Diaz, L. Andrade-Arenas, J. G. Arellano, and M. A. Lengua, "Analysis about benefits of software-defined Wide Area Network: A New Alternative for WAN Connectivity", *International Journal of Advanced Computer Science and Applications*, Vol. 13, No. 1, 2022.

[35] M. Ozkan-Okay, R. Samet, O. Aslan, and D. Gupta, "A Comprehensive Systematic Literature Review on Intrusion Detection Systems", *IEEE Access*, Vol. 9, 2021, pp. 157728, doi: 10.1109/access.2021.3129336.

[36] K. Coulibaly, "An overview of Intrusion Detection and Prevention Systems", *ResearchGate*, 2020, pp. 1–4.

[37] M. S. M. Subair, A. Sahthiyan, S. S. Bhaskaran, F. N. Zaini, A. F. Rozley, and P. S. JosephNg, "Enhanced Network Solution for Flexible Working Environment", *2022 IEEE 10th Conference on Systems*, Process & Control (ICSPC), Malacca, Malaysia, 2022.