Available online at www.garmian.edu.krd

Passer Journal

Passer 6 (Issue 1) (2024) 27-32

http://passer.garmian.edu.krd/

Comparative Analysis of Flexiwan, OPNSense, and pfSense Cybersecurity Mechanisms in MPLS / SD-WAN Architectures

Rebeen Rebwar Hama Amin[1*], Dana Hasan Ahmed[2]

[1]*Department of Network, Computer Sciences Institute, Sulaimani Polytechnic University, Sulaymaniyah, Kurdistan Region, Iraq.*
[2]*Department of Computer Science, College of Science, University of Garmian, Kalar, Kurdistan Region, Iraq.*

Received 26 March 2023; revised 21 November 2023;
accepted 21 November 2023; available online 11 December 2023

DOI: 10.24271/PSR.2023.390989.1295

ABSTRACT

SD-WAN, a software-defined network used in wide area networks, has grown in popularity among major corporations with geographically spread operations. Given the high prices of WAN connections, the key objective is to employ software-based solutions to offer a cost-effective balance. However, the proliferation of SD-WAN solutions from many vendors and open-sources has led in a rise in the number of threats and vulnerabilities to the technology. This research compares three popular open-source firewall solutions inside a certain design and examines cyber-attack vectors within the SD-WAN architecture using Graphical Network Simulator-3 (GNS3) software simulations. The presented topology consists of three branches, each of which employs one of the suggested firewalls, Flexiwan, OPNSense, or pfSense, and is linked by Multiprotocol Label Switching (MPLS), Virtual Private Network (VPN) and Internet Protocol Security (IPSec) tunnels. The research concludes that the solutions mentioned provide similar mechanisms for security, including confidentiality, integrity, and availability. Simulation results show that these open-source firewalls provide in-depth security features for SD-WAN architectures and can be implemented in such environments. However, the three solutions have vulnerabilities, which can be handled as long as they offer tools for adaptation because they are open-source and can be improved in future batches and updates within their community.

Keywords: SD-WAN, Open-Source Firewalls, MPLS, Ipsec, Flexiwan, Opnsense, Pfsense.

1. Introduction

Software-Defined Wide Area Network (SD-WAN) is a networking technology that allows organizations to connect and manage multiple branch offices and data centers over a wide geographic area. It uses software to create a virtual overlay network that abstracts the underlying physical infrastructure and provides centralized management and control[1]. SD-WAN can improve network performance and reliability by using multiple connection types, such as broadband, Long-Term Evolution (LTE), and MPLS, and dynamically routing traffic across the best available path[2]. It can also make network operations easier by giving visibility and control over all connected devices and applications, as well as automating network policies and configurations[3]. SD-WAN, an extension of Software-Defined Networking (SDN) in the wide area network, provides a solution by virtualizing data traffic management by placing the control plane in a software environment[4,5]. Figure 1 shows a typical SD-WAN-based architecture connecting a branch office to a headquarters using a variety of access WAN technologies.

Several vendors and operators have introduced SD-WAN technology, but some enterprises are still hesitant to adopt it due to concerns regarding the security of company data transmitted via public Internet service and the quality of services compared to legacy or traditional WAN services[6]. Traditional encrypted VPN technology is the most popular choice as the number of sites that can be connected to present networks grows, and the need for exchange security develops. Even though many locations can be connected in a flexible, dynamic, and automatic manner using automated tunneling VPN, maintaining exchanges through these multiple tunnels will encounter a huge obstacle for engineers[7]. Therefore, SD-WAN is the solution that best satisfies this requirement because it offers simplified management. A network architecture based on SD-WAN and automatic VPN must be designed and implemented while taking engineering best practices into account[8]. To achieve such goals and operate such architectures, certain technologies need to be implemented. Several vendors are currently providing SD-WAN security solutions, but there are open-source solutions as well.

* Corresponding author
E-mail address: rebeen.rebwar@spu.edu.iq (Instructor).
Peer-reviewed under the responsibility of the University of Garmian.

Therefore, this research compares three common open-source firewalls, namely Flexiwan, OPNSense, and pfSense, in an SD-WAN over an MPLS environment. FlexiWAN is an SD-WAN open-source solution that is designed to replace traditional WAN routers by enabling network administrators to optimize WAN connectivity through its advanced features. It provides multiple WAN link aggregation, load balancing, application steering, and centralized management features, and it is considered a cost-effective solution for Small and Medium-sized Businesses (SMBs) as well as large enterprises. pfSense, on the other hand, is a popular open-source firewall and routing platform based on the FreeBSD operating system. It provides an easy-to-use web-based interface and offers a range of features, such as VPN connectivity, load balancing, high-availability, and captive portal functionality, making it ideal for small to medium-sized businesses[9]. OPNSense is a fork of pfSense and offers many of the same features but with a focus on security and usability enhancements. It provides a more modern user interface and adds additional security features such as two-factor authentication and intrusion detection and prevention[10]. Several studies analyzed open-source firewalls and compared them to commercial solutions. However, there are no studies that could be found to compare and contrast multiple open-source security solutions used particularly in a single MPLS / SD-WAN architecture. We perform a study in which we test three main firewalls to determine if they could be utilized in SD-WAN. Previous literatures utilize specific security penetration testing processes, and we attempt to apply such approaches to evaluate the validity of our work.

The comparative study of these open-source solutions reveals advantages regarding management, security, and performance that underpin the significance of the examination and deployment of these technologies. The goal of this work is to compare and contrast the security features of three major open-source SD-WAN firewalls. A simulated environment is being used as part of the study technique to enable the testing of these technologies.

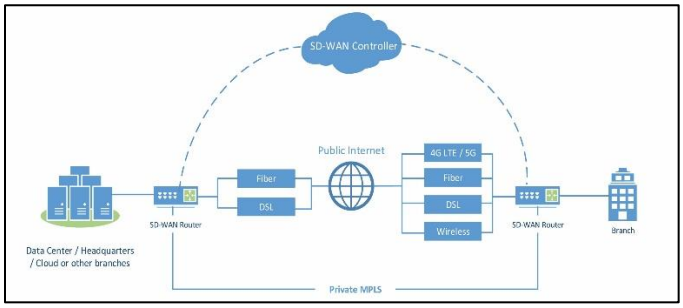

Figure 1: SD-WAN Architecture.

2. Related Works

The implementation of SD-WAN technology has grown significantly in recent years due to its ability to provide enhanced network performance and cost savings for organizations. However, the increased use of SD-WAN also presents new security challenges that must be addressed. To this end, several research studies have been conducted to compare and evaluate different cybersecurity mechanisms in SD-WAN architectures. The objective of the study in[11] is to compare commercial cybersecurity mechanisms with open-source solutions implemented in a specific SD-WAN architecture. The article discusses the potential cyber-attack vectors inside an SD-WAN architecture and presents a solution to these risks and vulnerabilities using the GNS3 software simulation. The SD-WAN topology shown in the article consists of two branches and a headquarters linked by two redundant lines, one through MPLS and the other via broadband Internet. The study's findings show that the commercial solution (Fortigate) provides stronger security procedures emphasizing on confidentiality, integrity, and availability. The open-source solution (Flexiwan) on the other hand, owing to community contributions, provides tools for adaption to new threats.

The study of[12] compares pfSense and OPNSense, two of the most widely used open-source firewalls. Without any extra attachments, they have examined the security that firewalls offer by default. In order to accomplish this, they ran four separate attacks against the firewalls and compared the outcomes. Consequently, they have shown that both offer the same level of protection, but when an attacker attempts to use Brute force attacks on both firewalls, pfSense has a small advantage. Another study compares the Quality of Service (QoS) and SD-WAN performance to standard MPLS and Ethernet over Internet Protocol (EoIP) by testing an Indonesian company's active WAN using those three connections between two major cities. The ITU-T G.1010 standard was used as a reference for measuring service and performance[13]. In the work of[14], the article suggests a unified SD-WAN design to address the inflexibility issues of the current SD-WAN design. In this new design, the SDN controller serves as the central component of the entire SD-WAN system and is implemented at the organization's headquarters. In contrast to other SD-WAN solutions, the forwarding layer of this integrated SD-WAN architecture relies heavily on Customer Premises Equipment (CPE) and OpenFlow switches to perform data forwarding and receiving functions.

SD-WAN has the potential to transform WAN services because it supports the concept of Application-driven networking, which requires the network to cater to the needs of applications, services, and customers. It involves centralized management of WAN networks, often closely tied to cloud computing and security, which enables customers to easily manage their networks regardless of the connectivity provider. SD-WAN is a significant topic that impacts WAN environments, and it challenges the way we have traditionally used network services. It has the potential to change the way we use communication services in the future, and several industries are interested in deploying it, including the education sector, according to our analysis[15]. SDN is a popular subject in the field of communication technology, and many researchers are working on it. However, implementing or testing it is challenging, which is why some research focuses only on the theoretical aspects of SDN. Recent research shows that SD-WANs can improve QoS, provide better network control, and connect branch offices to a core group network or data centers separated by intervals. SD-WAN may assist networks in delivering consistent and unified security across all networks. This research analyzes SD-WAN designs and their operating principles, as well as aspects including virtualization and programmability. SD-WAN makes

use of Internet-based WANs to provide multi-service networks and VPN services[16].

3. Simulation Scheme

To simulate the SD-WAN networks, the GNS3 tool was chosen for its cost-effectiveness in which it is free and open-source, reliability, and ability to design and test extensive topologies. For the topology, all three firewalls were implemented and configured in a single GNS3 project, along with a VMware workstation which is a licensed software used to operate virtual machines. Each branch has its own client and web administrator, which are represented as servers in the topology. Since the majority of business SD-WAN implementations use an architecture that connects branches to a central MPLS cloud, the simulation scenarios were designed with the three branch offices connected by MPLS and IPSec tunnels. In the MPLS topology there are routers represented as Provider (P) and Provider Edge (PE). Further, Nessus and Network Mapper (NMAP) were used for vulnerability evaluation and scanning, respectively, and Nikto, Hydra, Ncrack, Medusa and Burp Suite were used for brute force and web penetration testing. All of the mentioned penetration tools are free and available for public use. The study provides a detailed overview of the testing parameters and configuration of the experimental setup.

The suggested firewall functionality and core network connection are simulated using GNS3 with connections to VMware Workstation as a hypervisor. Depending on the solution, the installation and operation of components vary. In the case of the Flexiwan firewall, it can be installed on the Linux-based operating systems such as Ubuntu, whereas OPNsense is based on the FreeBSD operating system. Furthermore, it has its own firmware to install, which is quite similar to pfSense's installation. A design with three branch offices (nodes) connected by an MPLS link is suggested for the simulation scenarios, as shown in Figure 2.

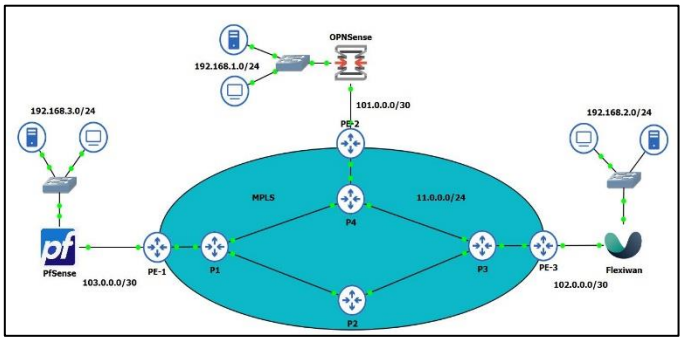

Figure 2: Simulation Scheme.

3.1 Comparative Analysis and Simulation Parameters

Certain information and parameters have been collected regarding each of the solutions before the simulation, and table 1, provides a detailed description of these parameters. Flexiwan is an ideal firewall for MPLS / SD-WAN environments due to its advanced SD-WAN features, traffic shaping, application steering, dynamic path selection, load balancing, and failover capabilities. While OPNSense offers similar features to pfSense, it also has additional security features and advanced SD-WAN features such as dynamic path selection, traffic shaping, and failover capabilities, making it an ideal choice for complex MPLS and SD-WAN environments.

Both Flexiwan and OPNSense provide advanced features that are essential for optimizing WAN connectivity and ensuring maximum uptime, making them the most suitable options for MPLS and SD-WAN environments. Table 2 shows the comparison analysis of the three open-source firewalls based on simulation parameters, considering their security features and suitability for SD-WAN architectures. It can be observed that all three solutions provide comparable security features, but since pfSense has known issues with redundant gateways and central management, it is less ideal for complex and enterprise architectures.

Table 1: Comparison Analysis and Simulation Parameters Descriptions[11].

Parameter	Descriptions
Authentication Methods	Authentication is a key process in cybersecurity that refers to the act of authenticating a user's, system's, or entity's identity while attempting to access a system or data. Examples related to this study are password, Certificate-based Authentication, Public Key Infrastructure (PKI), Single Sign-On (SSO), Multi-factor Authentication (MFA) and One-time passwords (OTP).
Encryption algorithm	Encryption algorithms are mathematical procedures or sets of rules that are used to encrypted / decrypt data. Encryption is a critical aspect of security. There are two major types of encryption algorithms: 1. Symmetric Encryption such as Advanced Encryption Standard (AES), Data Encryption Standard (DES), and Triple DES (3DES). 2. Asymmetric Encryption such as RSA (Rivest-Shamir-Adleman), Diffie-Hellman, and Elliptic Curve Cryptography (ECC).
Hashing Algorithm	Hashing algorithms are mathematical functions that take an input and output a fixed-length string of characters that appear randomly. Examples are: Message Digest Algorithm 5 (MD5), Secure Hash Algorithm (SHA) and Hash-based Message Authentication Code (HMAC).

Key Exchange Mechanism	A key exchange mechanism is a cryptographic technique used by two parties securely establish a shared secret key via an unsecure communication channel. Examples are: Diffie-Hellman Key Exchange, Elliptic Curve Diffie-Hellman (ECDH) and RSA Key Exchange.
VPN Connectivity	VPNs provide safe communications by utilizing various encryption techniques. Protocols that are often used include: OpenVPN and IPsec.
IKE Version	Internet Key Exchange (IKE) is a protocol that is used to establish security associations (SA) and negotiate cryptographic keys for secure communication over VPNs. IKE operates in two phases: Phase 1 (IKEv1) and Phase 2 (IKEv2).

Table 2: Comparison Analysis based on the Simulation Parameters[10-12,17].

	Flexiwan	**OPNSense**	**pfSense**
Authentication Methods	user authentication, MFA, X.509 digital certificates, and SSO	user authentication, external authentication servers, X.509 digital certificates and captive portal authentication	user authentication, external authentication servers, X.509 digital certificates, captive portal authentication, and SSO
Encryption Algorithm	AES (128-bit, 192-bit, and 256-bit), 3DES and Blowfish	AES (128-bit, 192-bit, and 256-bit), Blowfish, 3DES and CAST-128	AES (128-bit, 192-bit, and 256-bit), Blowfish, 3DES and CAST-128
Hashing Algorithm	SHA-256 and SHA-512	SHA-256, SHA-512, and HMAC-SHA256	SHA-256 and SHA-512
Key Exchange Mechanism	Diffie-Hellman	Diffie-Hellman and ECDH	Diffie-Hellman and ECDH
VPN Connectivity	IPsec for secure communication over the Internet and OpenVPN for secure communication.	IPsec for secure communication over the Internet and OpenVPN for secure communication.	IPsec for secure communication over the Internet and OpenVPN for secure communication.
IKE Version	1,2	1,2	1,2
Suitability for MPLS / SD-WAN Environments	Ideal	Ideal for complex MPLS / SD-WAN environments	Suitable but less ideal for complex MPLS / SD-WAN environments (Enterprise architectures)

4. Simulation Results

The GNS3 simulations were performed on a high-end computer with an 8-core processor and 64GB of memory, and simulations were run three times, each time for one of the firewalls. Attacks on the web administration, Denial-of-Service (DoS) attacks, and brute force were used to attack and test the CPEs. The outcomes were assessed on a qualitative level. Depending on the firewall, solutions differ. The connections were maintained in the web-based client; despite the fact that the web administrator is typically inaccessible, a straightforward TCP attack such as a Flood Synchronize (SYN) attack on port 443 completely shuts down the branches. Yet these firewalls have rules to stop DoS at the IP level, and a lack of initial configurations could reveal a vulnerability. The Flood SYN vulnerability exists on TCP port 8080, and the firewall's driver handles all provisioning and updates.

Since the web administrators lack a means to restrict the number of attempts to log in to the firewalls. Because the Hydra tool can find basic keys (e.g., 12345, admin) within a minute or less, it may be accessed using keys without pre-configured password policies. Regarding Command-Line Interface (CLI) administration, all three solutions offer Secure Shell (SSH) administration; however, the default Ubuntu 22.04 solution includes OpenSSH Server, which has several security flaws. Table 3 displays the simulation's security attacks and discovered vulnerabilities.

Despite this, the scanners were successful in discovering and locating the CPEs. Based on the scanner results, all three solutions have no visible vulnerabilities, and manual testing failed to uncover security flaws. All three of them use strong authentication systems and each request is made using a special token that the user creates themselves in the administration. Moreover, every packet is encrypted during a man-in-the-middle attack using the encryption algorithm suggested by each solution. These technologies enable the implementation of IPsec tunnels between the branches, guaranteeing the data's integrity and secrecy. Although A template selector with default settings may be used to configure the IPsec tunnel, it still requires hash function methods to guarantee authentication and integrity.

Table 3: Attacks and Vulnerabilities.

	Flexiwan	OPNSense	pfSense
Brute Force (SSH 6 characters long)	Failed	Failed	Failed
Brute Force (Web login 6 characters long)	Failed	Failed	Failed
DoS (TCP SYN Flood Attack)	Successful	Successful	Successful
DoS (ICMP Flood Attack)	Successful	Successful	Successful
DoS (Application layer attacks)	Successful	Successful	Successful
NMAP (Scan)	Successful	Successful	Successful
Nessus (Scan)	Successful	Successful	Successful

Conclusion

Ensuring high levels of security is crucial for many technologies used in critical or business systems. This paper examines the most common threats in SD-WAN and compares the security mechanisms and mitigations provided by three common open-source solutions through multiple simulations in GNS3 software. The findings show that the solutions provide effective cybersecurity mechanisms for mitigating common attacks, but they are more vulnerable to brute force or dictionary attacks due to their lack of limits on login requests per minute if no password policies are in place. Along with IPsec tunnels, all three firewalls employ strong cryptographic algorithms for authentication and integrity. However, default configurations and a lack of hardening in these solutions can lead to vulnerabilities that can be dealt with since they are open-source and improvements can be applied.

Conflict of interests

None

Acknowledgements

Acknowledgment is conveyed to Dr. Shakhawan Al-Zangana and Mr. Jamil Enayati for their invaluable support and guidance throughout the process of completing and publishing the research paper. The endeavor proved to be a highly enlightening educational experience. Within this framework, an opportunity is seized to express profound gratitude to Mr. Dana Hasan; his collaboration and contributions played an indispensable role, without which the realization of the research project would not have been achievable.

References

1. S. Troia, L. M. M. Zorello, A. J. Maralit and G. Maier, "SD-WAN: An Open-Source Implementation for Enterprise Networking Services," 2020 22nd International Conference on Transparent Optical Networks (ICTON), Bari, Italy, 2020, pp. 1-4, doi: 10.1109/ICTON51198.2020.9203058.
2. L. Borgianni, S. Troia, D. Adami, G. Maier and S. Giordano, "From MPLS to SD-WAN to ensure QoS and QoE in cloud-based applications," 2023 IEEE 9th International Conference on Network Softwarization (NetSoft), Madrid, Spain, 2023, pp. 366-369, doi: 10.1109/NetSoft57336.2023.10175470.
3. P. Iddalagi and A. Mishra, "Impact Analysis of Tunnel Probing Protocol on SD-WAN's Mainstream Traffic," 2023 15th International Conference on COMmunication Systems & NETworkS (COMSNETS), Bangalore, India, 2023, pp. 252-259, doi: 10.1109/COMSNETS56262.2023.10041375.
4. P. Zhang et al., "Real-Time Malicious Traffic Detection With Online Isolation Forest Over SD-WAN," in IEEE Transactions on Information Forensics and Security, vol. 18, pp. 2076-2090, 2023, doi: 10.1109/TIFS.2023.3262121.
5. W. Pratiwi and D. Gunawan, "Design and Strategy Deployment of SD-WAN Technology: In Indonesia (Case Study: PT. XYZ)," 2021 International Conference on Green Energy, Computing and Sustainable Technology (GECOST), Miri, Malaysia, 2021, pp. 1-6, doi: 10.1109/GECOST52368.2021.9538796.
6. S. Troia, L. M. Moreira Zorello and G. Maier, "SD-WAN: how the control of the network can be shifted from core to edge," 2021 International Conference on Optical Network Design and Modeling (ONDM), Gothenburg, Sweden, 2021, pp. 1-3, doi: 10.23919/ONDM51796.2021.9492375.
7. S. Troia, M. Mazzara, M. Savi, L. M. M. Zorello and G. Maier, "Resilience of Delay-Sensitive Services With Transport-Layer Monitoring in SD-WAN," in IEEE Transactions on Network and Service Management, vol. 19, no. 3, pp. 2652-2663, Sept. 2022, doi: 10.1109/TNSM.2022.3191943.
8. W. Rose Varuna and R. Vadivel, "Recent Trends in Potential Security Solutions for SD-WAN: A Systematic Review," in Intelligent Computing and Innovation on Data Science, S.L. Peng, S.Y. Hsieh, S. Gopalakrishnan, and B. Duraisamy, Eds. Singapore: Springer, 2021, vol. 248, pp. 1-13, doi: 10.1007/978-981-16-3153-5_1.
9. P. SenthilKumar and M. Muthukumar, "A Study on Firewall System, Scheduling and Routing using pfsense Scheme," 2018 International Conference on Intelligent Computing and Communication for Smart World (I2C2SW), Erode, India, 2018, pp. 14-17, doi: 10.1109/I2C2SW45816.2018.8997167.
10. Julio Cesar Bueno de Camargo, OPNsense Beginner to Professional: Protect networks and build next-generation firewalls easily with OPNsense , Packt Publishing, 2022.
11. J. R. Bustamante and D. Avila-Pesantez, "Comparative analysis of Cybersecurity mechanisms in SD-WAN architectures: A preliminary results," 2021 IEEE Engineering International Research Conference (EIRCON), Lima, Peru, 2021, pp. 1-4, doi: 10.1109/EIRCON52903.2021.9613418.
12. H. J. Kiratsata, D. P. Raval, P. K. Viras, P. Lalwani, H. Patel and P. S. D., "Behaviour Analysis of Open-Source Firewalls Under Security Crisis," 2022 International Conference on Wireless Communications Signal Processing and Networking (WiSPNET), Chennai, India, 2022, pp. 105-109, doi: 10.1109/WiSPNET54241.2022.9767176.
13. R. Y. Manova, E. Sukmadirana and N. S. Nurmanah, "Comparative Analysis of Quality of Service and Performance of MPLS, EoIP and SD-WAN," 2022 1st International Conference on Information System & Information Technology (ICISIT), Yogyakarta, Indonesia, 2022, pp. 403-408, doi: 10.1109/ICISIT54091.2022.9872806.
14. G. Mine, J. Hai, L. Jin and Z. Huiying, "A design of SD-WAN-oriented wide area network access," 2020 International Conference on Computer Communication and Network Security (CCNS), Xi'an, China, 2020, pp. 174-177, doi: 10.1109/CCNS50731.2020.00046.

15. P. Segeč, M. Moravčik, J. Uratmová, J. Papán and O. Yeremenko, "SD-WAN - architecture, functions and benefits," 2020 18th International Conference on Emerging eLearning Technologies and Applications (ICETA), Košice, Slovenia, 2020, pp. 593-599, doi: 10.1109/ICETA51985.2020.9379257.

16. K. G. Yalda, D. J. Hamad and N. Ţăpuş, "A survey on Software-defined Wide Area Network (SD- WAN) architectures," 2022 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA), Ankara, Turkey, 2022, pp. 1-5, doi: 10.1109/HORA55278.2022.9799862.

17. Patel, Krupa C., and Priyanka Sharma. "A Review paper on pfsense-an Open source firewall introducing with different capabilities & customization." International Journal of Advance Research and Innovative Ideas in Education 3 (2017): 2395-4396.