A Holistic Review of SD-WAN Security Challenges

Raghad A. AlSolami
Department of Electrical & Computer Engineering KAU
Jeddah, Saudi Arabia

Rawan Hussain AlJabali
Department of Electrical & Computer Engineering KAU
Jeddah, Saudi Arabia

Ruaa A. Obeid
Department of Electrical & Computer Engineering KAU
Jeddah, Saudi Arabia

ABSTRACT
While demands on wide area network (WAN) services are gradually increasing, the regular WAN is struggling to cope with the high network services requirements. Recent software-defined wide area networks (SD-WAN) technology has provided a robust network system to handle large and increasing network loads. SD-WAN is providing a central and programmable control on the network system, which ensures more flexibility and agility. Moreover, as it enables the cloud use for network services, security becomes a significant challenge in SD-WAN. As a result, several types of threats among the three network planes need to be handled through a stable security system integrated with the SD-WAN. This article reviews the significant challenges faced in SD-WAN systems facing each plane of the SD-WAN structure, such as intersection attacks, leakage of information threats, and eavesdropping attacks.

General Terms
Computer Networks, Network Security

Keywords
SD-WAN, WAN Security, SD-WAN Challenges, SD-WAN controller

1. INTRODUCTION
Software-Defined Wide Area Network known as (SD-WAN) uses software to control the management, services, and data center remote branches or cloud instances. In other words, this technology is congregating virtual private network (VPN), data compression, and traffic management technologies into a cloud-based provision [1]. SD-WAN is trending nowadays and is one of the fastest-growing segments in the network enterprises. However, SD-WAN is a target for attackers as it supports security services, like, DPI, VPN, firewalls, and encryption, amongst many other services. Operating systems (OS) used in SD-WAN nodes are distributed as Linux-based systems like Ubuntu and Debian, along with other network software products, operating on outdated open-source software with recognized vulnerabilities [2]. Those vulnerabilities can be employed by attackers to escalate privileges in the OS.

The Security threats are far greater in SD-WAN as it operates on an insecure public internet for moving enterprise data. As opposed to the previously implemented enterprise communication; multi-protocol label switching (MPLS) service. One might think, then why the switch to such an unstable solution, especially when the data layer is prone to vulnerabilities which might hinder the availability of the network altogether? Well, it offers more flexibility, costs less, and takes less time in connecting new branches, not to mention the lack of proprietary hardware components needed in SD-WAN architectures [3]. With that being the case, this paper will present the various security threats facing software-defined wide area networks.

2. SOFTWARE DEFINED WIDE AREA NETWORK

2.1 Background of Software Defined Wide Area Network (SD-WAN)
The traditional networks and networking structures become insufficient in fulfilling the dynamically growing networking demands and high rate applications such as cloud computing, 5G, cellular network, big data analysis, and so on. Therefore, the need for an advanced concept and more sufficient network systems for supporting future network requirements has increased. However, the rise of software-defined networks (SDN) is playing a gradually growing role in providing the required flexibility and agility for the high rate network services. The primary key for the high performance of SDN-based networks is that they deliver a centralized and programmable controller for network systems. The logical architecture of the SDN consists of three main layers that are interconnecting throughout different protocols, as illustrated in Figure 1. The primary logical planes are data, control, and application layers ordered from bottom to top [4]. Furthermore, traditional wide area networks (WAN) are challenging problems in providing a robust performance for its demanding network loads with the limited and valuable bandwidth resource. Thus, SDN based WAN technology has become an extensively debated candidate to replace legacy networks to cope with the gradual rise in network traffic [5].

SD-WAN implements the SDN logical structure, which provides a holistic control of the WAN traffic and layers interfacing as well as a full utilization of the bandwidth resources. By benefiting from the central controller of SD-WAN, enterprises now can enhance their application level performance by intelligently shifting traffic with sufficient bandwidth link that suits the necessities of each application in their network. However, even though SD-WAN is improving performance and efficiency, it increases the risk as well. Therefore, vendors of SD-WAN need to ensure a reliable security management system for public Internet connections that are used for WAN traffic and data routing. Additionally, more secure private paths for organizations to route their sensitive data and traffic across is needed. As SD-WAN is an internet-based networking service that enables clouds and services' virtualization, it is subject to many cyber-attacks and other threats among its different planes.

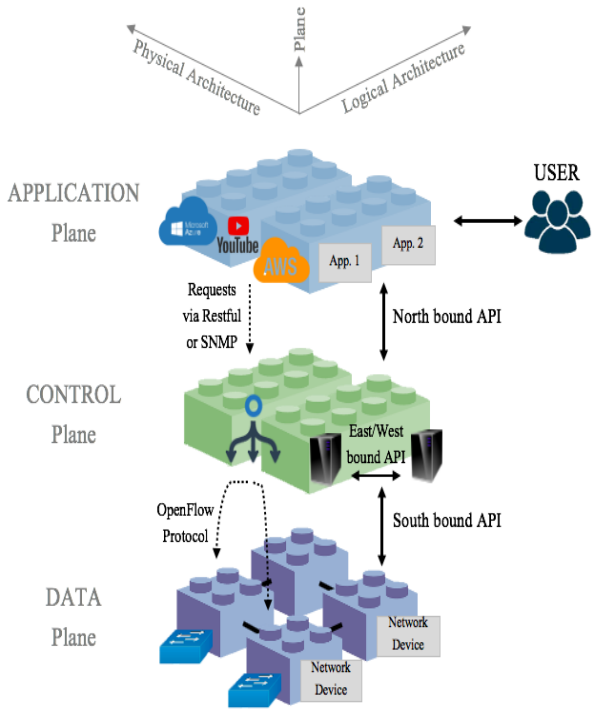

Figure 1 Software-defined wide area network: logical and physical architecture

2.2 SD-WAN Security Challenges

When considering a software-defined wide area network security threats, it is best to look at it from the three planes; it is deemed to have. Which facilitates a comprehensive, holistic view of the challenges facing this new emerging technology.

This paper will outline the basic layout, function, security threats that are present in each of the aforementioned layers in an SD-WAN blueprint.

i. Application Plane

The application plane holds many software applications and network services that either have been designed by the network providers, application developers, or an external service/tool provider enabling them more involvement in controlling the network. The plane's core work is based on interacting with the control plane to execute the control programs according to its' logic and strategies [4]. Some of the plane functions are load balancers, firewalls, traffic shaping, and network applications. The interaction between the application and control plane happens with the help of the northbound API, which if managed correctly is critical to maintain a secure network. However, it does not assure a threat free SDN network [6].

The main functions for the application plane were stated above, and since the security of the SD-WAN depends mainly on the three planes functionality without any breaches. Thus, it is fitting to outline the following current threats imposed on the application layer [7]:

- Leakage of information due to obeying the firewall rules and the cause of data isolation. Which can be used unethically by users and steal other users' information.
- Information interception happens through traffic analysis, where attackers analyze the flow of data between two entities and manage to steal information.

According to [8], a major threat that can happen through this layer, is information disclosure- meaning an attacker can read shared memory or cache and misuse a memory management vulnerability in the hypervisor. This is done by gaining a foothold on a virtual machine inside the SD-WAN application layer. Needless to say, data encryption needed in order to secure communication paths between the VPN end points scan takes place in more than one layer, as maintaining customers' information secure is a critical aspect to study and enhance.

The aforementioned possible threats to the application plane are merely a couple of many that affect the security of the SD-WAN.

ii. Control Plane

The control plane is a software and hardware component playing the role of the network OS, that handles the actual network monitoring, traffic engineering, and quality-of-service (QoS) for the underlying network resources. The control plane implements and manages the different network functions independently from one another. This decoupling makes network operators capable of developing, modifying, debugging, or removing arbitrary functions without affecting others [9]. In a network control layer, functions can also be chained or connected to perform a particular task at a low cost and in a high flexibility software-based manner. The controller is also responsible for guaranteeing high QoS by filling the application requirements through data transferring [10]. As a requirement for distributed controllers, east/west bound API is inferred in this layer to provide common compatibility and interoperability between the different controllers [11], which should be addressed within threat modelling.

The most realistic attacks on an SD-WAN is insecure configuration related threats on the control plane. As a result of the logically central nature of an SD-WAN controller, scalability limitations are challenging the application designers as well as SD-WAN vendors. Another major challenge facing the control panel is when the connectivity with the data plane is lost due to variable propagation delays through long distances. As for large networks, it would be a severe issue to uphold the centralization of the control plane without distributing the controller. The distributed central controller faces some difficulties in ensuring secure consistency and resiliency [12]. Nonetheless, SDN controllers have to exchange information with one another as well as between customer premises equipment (CPE) to optimize the network resources. Another point to emphasize here is the need to encrypt communication between the controller and the CPE to prevent eavesdropping, and any alterations done to the routing control commands.

For SD-WAN to perform sufficiently, the reliability of the controller needs to be maintained at a high level, which requires failure handling. Failures can occur in different forms, such as device, data, or link failure.

iii. Data Plane

The data plane of any network is in charge of transporting data packets across a network that traverse in a multifaceted way, from lower, physical layer all the way to the application layer. The data layer is classified into two main functions; bandwidth virtualization and data forwarding, which consists of hardware or software components of the router or switch. These components are related to forwarding user traffic/data from one interface to another, depending on the bandwidth provided by bandwidth virtualization. While there are a

couple of protocols set in this layer, one of the most prominent is OpenFlow, as it is one of the significant contributors of the Open Network Foundation [13]. OpenFlow is one of the dynamic control protocols, which means session policies are pre-provisioned in the switch and only updated when the user makes alterations. The southbound interface/API (SBI) serves as the protocol plug-in, allowing it to operate between the SD-WAN controller and the network.

Four different attacks are comprised in the SBI, containing interaction, availability, eavesdropping, and TCP attacks. For an interception attack, the threat aims to corrupt the network behavior by adjusting the swapping of messages, such as network spoofing or man-in-the-middle MITM attack using ARP poisoning. As for availability, it refers to denial of service (DoS) attacks, where it chokes the available bandwidth capacity. DoS overfloods the SBI with requests causing the network implementation to crash [14]. Other threats can happen in the packets being handled, some of which can be in the form of traffic rerouting, and arbitrary code execution [15]. Routing threats comprise of targeting known protocols such as SNMP, NetConf, BGP, etc. One of the known threats is prefix hijacking, which is corrupting internet routing tables maintained using BGP. In order to securely connect sites, IPsec, DTLS, and SRTP tunnels are used, since WAN is over the public internet. In general, the consequences of switch malware in the data layer can lead to modifying route configuration which results in SD-WAN service integrity failure or unavailability.

3. MARKET STRATEGY

As hinted earlier in this article, SD-WAN comprises of software and hardware components, depending on the type of architecture the network enterprise chooses to install. Accordingly, the SD-WAN service comes with various parts to be developed/manufactured and deployed into the market. It is appropriate to say that with all the numerous security threats surrounding this service, being the first on the market is an advantage on other service providers given that the product/service maintains a reputable, prompt on-demand customer service team in the case of software malfunction or attacks to the network. Therefore, service providers must definitely keep their testing's ongoing even after dispatching their first version, as to enhance what is being offered. According to the International Data Corporation (IDC), it is predicted that the SD-WAN market will extend to a 5.25 US Billion-dollar turnover by 2023 [16]. With that said, companies that are developing their SD-WAN portfolios are taking a successful path by improving and investing capital into strengthening the broadband connection creating a secure SD-WAN for the market.

4. CURRENT AND FUTURE TRENDS

The SD-WAN's hot market triggered its suppliers to develop innovated solutions. Studies have shown that there are significant gaps in the existing SD-WAN structure, which reflects on all applications that use it. The newest mechanism does not provide a high level of security, which is crucial for today's complex and large-scale market. With today's fast-growing technologies, the improvements to each layer of the SD-WAN architecture is unpredictable, which results in providing opportunities for network designers and developers to enhance the SD-WAN security massively. One approach is to use machine learning (ML), deep reinforcement methods to reduce the average flow of data in data center scale networks [17]. Another area of future study is the infrastructure control, where robust authentication and different authorizations can be implemented to enhance the security level against malicious attacks.

5. CONCLUSION

This report enumerates the security threats on the SD-WAN from three planes. A brief history is added to explore how the SD-WAN grows with more demand on its applications. To fully understand how an attack can occur, each plane was described to give an insight into the plane's current situation and weak areas that will potentially affect the overall security of the network. Leakage of information is one of the threats from the application plane, another threat is security consistency and reliability from the Control Plane, and interaction of data caused by the Data Plane. These threats exemplify the massive pool of areas of development and improvement, where researchers are expanding their experience with SD-WAN to solve the current challenges. The future market of SD-WAN is up-and-coming, as one prediction stated that it would extend to be more than five billion US dollars in the next few years. The different planes of the SD-WAN expose it to many areas of development, one of which is using ML to minimize data flow. The SD-WAN's market is promising and opens the doors for developers and innovators to enhance its security.

6. REFERENCES

[1] P. A. Dhakulkar, P. S. Dubey, A. A. Gaikwad and S. P. Dhokane, "Software Defined Wide Area Network," International Journal of Innovations in Engineering and Science, vol. 3, no. 6, pp. 27-32, 2018.

[2] S. Gordeychik, D. Kolegov and A. Nikolaev, "SD-WAN Internet Census," ArXiv, 2018.

[3] A. Rajendran, Security Analysis of a Software Defined Wide Area Network Solution, Espoo: Royal Institute of Technology, 2016.

[4] F. Bannour, S. Souihi and A. Mellouk, "Distributed SDN Control: Survey, Taxonomy, and Challenges," 2018.

[5] O. N. F. TR-511, "Principles and Practices for Security Software-Defined Networks," 4 2015. [Online]. Available: https://www.opennetworking.org/wp-content/uploads/2014/10/Principles_and_Practices_for_Securing_Software-Defined_Networks_applied_to_OFv1.3.4_V1.0.pdf. [Accessed 14 3 2020].

[6] M. Niemiec , P. Jaglarz, M. Jekot, P. Cholda and P. Borylo, "Risk Assessment Approach to Secure Northbound Interface of SDN Networks," in International Conference on Computing, Networking and Communications (ICNC), Honolulu, HI, USA, 2019, pp. 164-169.

[7] L. R. Bays, R. R. Oliveira, M. P. Barcellos and L. P. Gaspary, "Virtual network security: threats, countermeasures, and challenges," Journal of Internet Services and Applications, 2016.

[8] M. Dirksen, A security architecture for software defined wide area networks, Leiden: Faculty of Governance and Global Affairs, 2018.

[9] Aaron Gember-Jacobson, Raajay Viswanathan, Chaithan Prakash, Robert Grandl, Junaid Khalid, Sourav Das, and Aditya Akella, "OpenNF: Enabling Innovation in Network Function Control," ACM SIGCOMM Computer Communication Review, vol. 44, no. 4, 2014.

[10] Mohammad R. Abbasi, Ajay Guleria, and Mandalika S.

Devi, "Traffic Engineering in Software Defined Networks: A Survey," Journal of Telecommunications and Information Technology, vol. nr 4, pp. 3--14, 2016.

[11] D. Kreutz, F. M. V. Ramos, P. E. Veríssimo, C. E. Rothenberg, S. Azodolmolky and S. Uhlig, "Software-Defined Networking: A Comprehensive Survey," Proceedings of the IEEE, vol. 103, no. 1, pp. 14-76, Jan. 2015.

[12] Z. Yang, Y. Cui, B. Li, Y. Liu and Y. Xu, "Software-Defined Wide Area Network (SD-WAN): Architecture, Advances and Opportunities," in 28th International Conference on Computer Communication and Networks (ICCCN), Valencia, Spain, 2019.

[13] J. Benabbou1, K. Elbaamrani and N. Idboufker, "Security in OpenFlow-based SDN, opportunities and challenges," PHOTONIC NETWORK COMMUNICATIONS, vol. 37, no. 1, pp. 1-23, 2019.

[14] A. Shaghaghi, M. A. Kaafar, R. Buyya and S. Jha, "Software-Defined Network (SDN) Data Plane Security: Issues, Solutions and Future Directions," in Handbook of Computer Networks and Cyber Security, Cham, Springer, 2020.

[15] S. Gordeychik and D. Kolegov, "SD-WAN Threat Landscape," ArXiv, 2018.

[16] M. FRAMINGHAM, "SD-WAN Infrastructure Market Poised to Reach $5.25 Billion in 2023, According to New IDC Forecast," International Data Corporation, 24 July 2019. [Online]. Available: https://www.idc.com/getdoc.jsp?containerId=prUS45380319. [Accessed 14 March 2020].

[17] L. Chen, J. Lingys, K. Chen and F. Liu, "AuTO: Scaling Deep Reinforcement Learning for Datacenter-Scale Automatic Traffic Optimization," 2018.