Turkish Online Journal of Qualitative Inquiry (TOJQI)
Volume 12, Issue 7, July 2021 : 7589 - 7594

Research Article

# Use cases of SDN for network security

**Rim Mrani Alaoui[1], Niyonzima Pierre Claver[2], Cisse Aissata[2], Modibo Samake[2], Ayoub Bahnasse[3]**

[1]LIMIE Laboratory, ISGA Fez, Morocco
[2]LIMIE Laboratory, ISGA Casablanca, Morocco
[3]ENSAM Casablanca, University Hassan II of Casablanca, Morocco

## Abstract

Network infrastructures have evolved in recent decades. Traditional equipment combining processing and execution capacity can no longer cope with the strong emergence of new flows and variety in the nature of traffic. The Software-defined Network (SDN) paradigm has been proposed to outsource the control plane in a dedicated device called a controller. SDN has been used among other things to improve not only network management, but also quality of service and security. In this paper we will present SDN technology as well as the role that this technology plays in improving network security.

**Keywords** : SDN, Security, Network, automation

## I- Introduction

As today's technology evolves day by day, migration to the cloud brings massive changes in architecture design and network security. For this, the network should be automated. Very advanced tools will then be needed to improve security [1] and that will help meet the challenges posed by digital transformation. Currently, businesses are faced with a challenge of being attacked by an increase in threats. Overcoming this challenge will require advanced tools to manage and protect corporate networks to enhance security. At this point in the evolution of the network, software-implemented networks (SDNs) [2] have the greatest advantage in meeting these challenges. By Definition, SDN is an architectural approach that allows the network to be intelligently and centrally controlled using software. The impact of SDN on network appliances will be extremely positive for businesses. This new technology has shifted the perception of value from hardware to software. A software-defined network uses an SDN controller to manage interactions between applications and network devices, which means that all devices are contained in a centralized node, and communications between network devices and network applications are handled in a secure and transparent manner.

The SDN architecture is made up of the following three layers: the application layer, the control layer and the infrastructure layer.

- The application layer: It contains the applications and services running on the network

- The control layer: This is the controller layer, it is like the brain of the network, it communicates with applications to determine the destination of data packets.
- The infrastructure layer: these are switches and routers, and all physical hardware, these devices receive instructions from the controller on how to route packets.

In order for these layers to communicate, SDN uses application program interfaces (APIs) northbound "Northbound interface (NBI)" and southbound "southbound interface (SBI)".

API Northbound: Applications communicate with the API through the control layer to the north and determine the resources that applications need and their destination.

Southbound APIs: The SDN Controller communicates with network infrastructure, such as routers and switches, through southbound APIs. The network infrastructure is informed of the path that the application data should take, as decided by the controller.

Figure 1 illustrates the architecture of SDN and its different interfaces

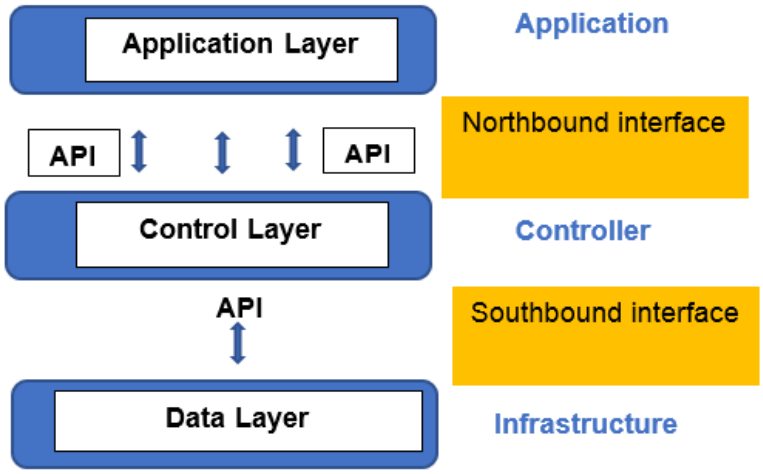


*Figure 1. SDN Architecture*

The remaining of the paper is organized as follows, in section 2 we will present the role SDN plays in the network security. In section 3, we will present related works. In section 4 we will discuss the benefit of SDN on VPN. In section 5 we will present how SDN secure wireless networks, and we will conclude in section 6.

## II- SDN for network security

Thanks to SDN paradigm, networks can benefit of several advantages related to security:

- Centralized network control: Traditionally, devices like the router, switches and others make their own decisions about inbound or outbound traffic, but with SDN the traffic will be routed through a single centralized controller. This increases security by making IDS and IPS data entry more efficient, i.e. SDN regulates data packets through a single firewall and improves data capture capability.

- The SDN advises in the process of identifying a user, determining the permissions granted to this user and keeping a record of the resources accessed. Users can now be uniquely identified by assigning attributes to them, and the system can use this information to access the identifier to determine the privileges granted to the operator who has been authenticated. This will help us identify vulnerable or faulty nodes and isolate them from open or listening ports.

- Simple configuration: we know that the configuration of VLANs is not an easy task. They are more used by companies to increase greater security. The more VLANs implemented within companies lead to more complications for the people who manage them. With the help of SDN, organizations can automate VLAN configuration and improve the traceability of those configurations. So, it will allow dynamic programming and restructuring of network settings, which reduces the risk of DDoS attacks.

- Granular segmentation that helps augment documentation, integrate applications with network monitoring, and add security features quickly and accurately.
- SDN provides automatic quarantine capabilities for specific network points infected with malicious code

In the other hand, SDN does not miss the downside, there are exactly the risks that the controller can break and attackers enter the network. This is why in best security practices, controllers should be supervised, so other measures should be taken such as network traffic monitoring, system patches, access control and high availability to operate. protect against potential denial of service attacks. But when it comes to security and SDN, it's clear that the security benefits of SDN outweigh the security risks. This development requires companies to plan and adapt the SDN architecture through the use of automation features. these methods remain more secure for organizations wanting to create a network capable of proactively managing evolving threats.

## III- Related works

Security provided by SDN is an active research field. Several works have been carried out proposing solutions to improve network security by adopting the SDN approach. K.A. Noghani et al [3] proposed a SDN based framework that automates the Ethernet VPN deployment and management inside SDN-based data centers using OpenStack and OpenDaylight controler. Alharbi, A. et al. [4] proposed an approach managing a complex dynamic multipoint VPN based on a SDN controller; authors exploited legacy equipment and used SNMP, SSH as SBI. Authors proposed Smart SDN Policy Management based VPN Multipoint for centralizing security policies management using a new Java interface. In the same context, Samier Barguil et al. [5] presented an a hybrid SDN approach in which the definition of a VPN service is made with a modeling language, their approach is supported for several manufacturers. Sean W. et al. [6] conducted a review about security challenges of Wireless networks adopting SDN. Authors highlighted that in addition to traditional wireless vulnerabilities, SDN communications especially between control layer and data layer can extended risk area. In [7], authors proposed a novel contribution of secure-by-design SDN-based framework for Wireless Sensors Networks; Secure node admission and end-to-end key distribution to support secure communication are considered key services.

## IV- VPN by SDN

Businesses and their IT teams face the following major challenges with traditional VPN service offerings: manual provisioning and complex management.

- Inability to adapt to the dynamic business environment and respond quickly to simple requests to move, add and modify.
- Limited service functionality and rigidity of standard VPN offerings.
- Geographic reach limits of a single-operator VPN service.
- High complexity in branch office deployments.

Then they are tightly connected to a dedicated network infrastructure of a service provider.

Implementing a software-defined network (SDN) brings many benefits to the business: streamlined architecture, network agility, and even improved security. But at the fundamental operations level, its main advantage is that it allows users to establish virtual private networks (VPNs) quickly and without having to learn a host of archaic network provisioning skills.
VPN, of course, is the abstract network environment that allows applications to connect to local and distributed resources on the cloud or edge. By integrating their deployment into a DevOps-centric SDN architecture, worker productivity receives a huge boost just as data and data services are about to form the core of the business model.

SDN VPNs are based on an overlay model that uses any IP network to provide underlayer connectivity between sites. This gives you maximum flexibility for your locations and also support for multiple access technologies. Likewise, you have the flexibility to combine available networks from multiple providers and use all available access technologies. It gives you the freedom to use the most available technologies in any particular location, so you can get service where and when you need it.
Hiding your IP address with an SDN VPN helps to hide your identity from websites, apps, and services that want to follow you. Good SDN VPNs also hide your activity from your Internet service provider, mobile operator, and anyone else who may be overhearing, with a layer of strong encryption.
Using an SDN VPN protects you against a variety of attacks, including packet sniffing, rogue Wi-Fi networks, and man-in-the-middle attacks. mobile users use an SDN VPN whenever they visit an untrusted network like free public Wi-Fi.

## V- Wireless par SDN :

The rise of devices like smartphones, tablets and mobile cloud services places a demand for dynamic wireless network services. This demand creates new requirements for the network architecture, such as flexibility in management and configuration, adaptability and independence from suppliers. To meet these requirements, Software Defined Wireless Network (SDWN) has been proposed as a cost effective solution.

Software Defined Wireless Networking (SDWN) is the use of SDN concepts in wireless networks. By using a controller in the control plane, SDWN facilitates the creation of new adaptive mechanisms according to different applications and user demands, such as mobility (handover), security and quality of service.

From the perspective of software-defined networking (SDN) assigns flexible routing and can be supported by the various communication models that exist in Wireless Sensor Networks (WSNs), which are associated from devices to limited resources to collect environmental information.
WSN has an important tool for real world applications, which improves the information gathering process in many planes such as precision agriculture, biodiversity monitoring / research, elderly monitoring, disabled monitoring and the health support. There are many applications for WSN in which security services, such as confidentiality, integrity and authentication of data sources.

SDN-based secure wireless communication for sensor networks addresses security issues, such as secure admission of nodes, key distribution, and establishment of a secure control channel.
Secure node admission is the process that allows new nodes to be authenticated and accepted by all other nodes in the network, often enabled by asymmetric cryptographic primitives. On the other hand, the authenticity, confidentiality and integrity of the data are achievable thanks to symmetric cryptography, such as an authenticated encryption algorithm with associated data.

The characteristics of the wireless network affect the use of other software-defined approaches, such as Open Flow. It is highly desirable that the control packets fit in the link layer transmission unit. In addition, the number of control packets should be kept to a minimum, as they are transmitted in-band (as opposed to wired networks, which typically use out-of-band control.

## VI- Conclusion

In this paper, we have cited the example of SDN deployment to improve the security of the network infrastructure. SDN technology brings a lot of flexibility and security including network security. By decoupling control and data planes, new policies can be applied on a single node without having to touch existing equipment.

## VII- References

[1] BAHNASSE, Ayoub, LOUHAB, Fatima Ezzahraa, TALEA, Mohamed, et al. Towards a new approach for adaptive security management in new generation virtual private networks. In : 2017 International Conference on Wireless Networks and Mobile Communications (WINCOM). IEEE, 2017. p. 1-6.

[2] Bahnasse, A., Louhab, F. E., Oulahyane, H. A., Talea, M., & Bakali, A. (2018). Novel SDN architecture for smart MPLS traffic engineering-DiffServ aware management. Future Generation Computer Systems, 87, 115-126.

[3] Noghani, K. A., Benet, C. H., Kassler, A., Marotta, A., Jestin, P., & Srivastava, V. V. (2017, May). Automating ethernet vpn deployment in sdn-based data centers. In 2017 Fourth International Conference on Software Defined Systems (SDS) (pp. 61-66). IEEE.

[4] Alharbi, A., Bahnasse, A., Talea, M., Oulahyane, H. A., & Louhab, F. E. (2017, October). Smart SDN Policy Management Based VPN Multipoint. In First International Conference on Real Time Intelligent Systems (pp. 250-263). Springer, Cham.

[5] Barguil, S., de Dios, O. G., Alvarez, V. L., Gagliano, R., Carretero, I., & Vilalta, R. (2020, November). Experimental validation of L3 VPN Network Model for improving VPN service design and provisioning. In 2020 16th International Conference on Network and Service Management (CNSM) (pp. 1-5). IEEE.

[6] Pritchard, S. W., Hancke, G. P., & Abu-Mahfouz, A. M. (2017, July). Security in software-defined wireless sensor networks: Threats, challenges and potential solutions. In 2017 IEEE 15th International Conference on Industrial Informatics (INDIN) (pp. 168-173). IEEE.

[7] Alves, R. C., Oliveira, D. A., Pereira, G. C., Albertini, B. C., & Margi, C. B. (2018). WS3N: wireless secure SDN-based communication for sensor networks. Security and Communication Networks, 2018.