ACTA TECHNICA CORVINIENSIS – Bulletin of Engineering | e–ISSN: 2067 – 3809
Tome XVIII [2025] | Fascicule 1 [January – March]

[1.]Péter András AGG, [1,2.]Zsolt Csaba JOHANYÁK

SECURITY IN SDN

[1.] Department of Information Technology, GAMF Faculty of Engineering and Computer Science, John von Neumann, HUNGARY
[2] Institute of Mechatronics and Vehicle Engineering, Bánki Donát Faculty of Mechanical and Safety Engineering, Óbuda University, HUNGARY

Abstract: Security is very important in all areas of our lives. This does not only mean personal security, but also the security of our data. Nowadays, almost everyone uses the opportunities offered by the online space, which significantly facilitate our lives, but also entails significant security risks. The protection of IT networks has always received great emphasis, but with the spread of Software Defined Networks (SDN), it is perhaps even more important. Talking about network security, authentication, the definition of permissions, and event logging are essential. This article shows how these aspects appear in an SDN environment, and what special protection needs to be considered in the course of the creation of a secure SDN network.
Keywords: Software Defined Networks, SDN, security, API security, machine learning

INTRODUCTION

There is almost no area in our lives where we do not encounter some kind of computer network. Network protection is a fundamental requirement. Security is essential, both for the average user and the system operator. Identification, managing appropriate permissions and, of course, logging is important. This is, of course, just one step towards achieving a secure network. In networks, communication is continuous between the source and the target, with continuous data exchange. Communication channels must be protected, and data must be encrypted to the greatest possible extent so that unauthorized people cannot access it. Equally important is the reliability of the network, i.e., its continuous fast and error-free operation. Therefore, attention must be paid to protect access to resources. One must be prepared for continuous and increasingly intelligent forms of attack and thus prevent the occurrence of malicious events. Continuous monitoring and logging can be of great help in this activity, because new and enhanced defense strategies can be developed depending on the results obtained. The above mentioned protection methods are not only appropriate and necessary for traditional networks but can also be applied to Software-Defined Networks (SDN) [1].

The rest of the article is organized as follows. Section 2 contains a brief introduction to the topic of Software-Defined Networks (SDN). Then, the security of all three layers of SDN will be discussed and the security of inter-layer communication is covered as well in Section 3. Section 4 presents possible future security solutions and guidelines for securing SDN networks. Finally, the conclusions are presented in Section 5.

SOFTWARE DEFINED NETWORKS

The emergence of Software-Defined Networking (SDN) [1] has changed the usual design and management of networks. Unlike traditional networks, SDN separates the data plane from the control plane. Network devices on the data plane perform simple forwarding tasks based on information received from the controller. This method provides centralized management, easier programmability, and fast response to network needs. Understanding the structure and operation of SDN is essential to protect the newly built network with appropriate security measures (see Figure 1). At the bottom of the network stack is the data plane, where the network forwarding devices are located. These devices communicate with the control plane via the southbound interface. This communication is provided, for example, by the OpenFlow [2] protocol. The control plane contains the controllers that provide the necessary control, including appropriate traffic routing decisions, rule creation, and placement. The network hypervisor and the network operating system are also located in this sublayer, which helps to implement the necessary configurations. The application layer situated at the top level communicates with the controller via the northbound interface. This

interface usually uses easy-to-use APIs which can be quickly modified the network behavior depending on current events. In SDN networks [3], it is not enough to solve the protection of the three main layers, but the information exchange between the layers must be provided with appropriate security settings as well.

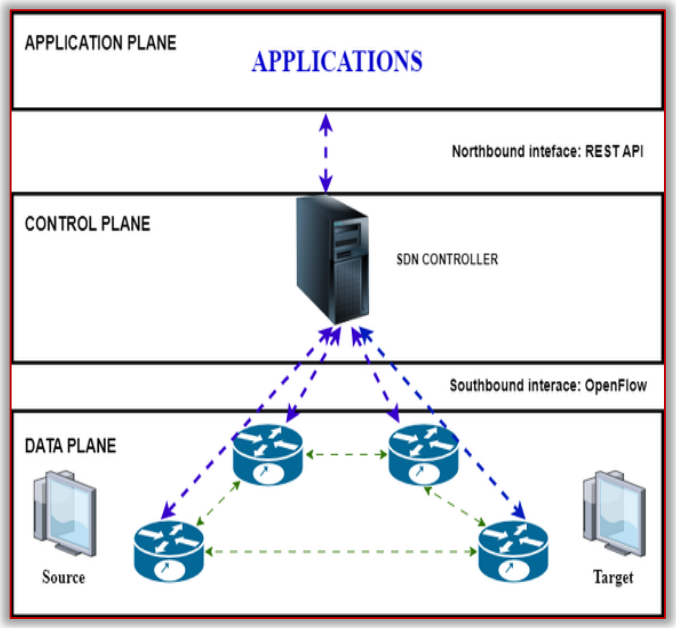

Figure 1. SDN architecture

SECURITY OF SDN PLANES

Compared to traditional networks, it is worth applying more detailed, complex security [4] settings in SDN networks, with particular attention to which layer is exposed to which attacks and threats.

The SDN data plane contains physical and virtual network devices (switches, routers) that make decisions about the appropriate data transmission based on commands received from the SDN controller. For proper security [5], it is important to authenticate the devices, regularly update the firmware, and segment the network to make it easier to manage smaller units [6].

The control plane is the most important part of the SDN network. This layer contains the SDN controllers, which manage and control the network devices in the data plane, and thus the data flow, via the southbound interface. The controller transforms the expectations and instructions of the application layer into network configurations and the policies associated with them. To ensure that the control layer is secure [7], it is essential to protect the controller as much as possible, ensure secure communication, and apply redundancy (more controllers) [8].

The application layer of SDN networks contains the network applications (e.g. network monitoring, traffic management systems, and other applications that facilitate secure operation), which deliver the necessary information for the proper operation of the network via the SDN controller. Communication between the applications and the SDN controller is ensured via the northbound interface using APIs (Application Programming Interfaces). Managing permissions and using updates is also important in this layer. In the following three subsections, the security measures required for each layer are presented in detail.

Data plane security

- *Check flow rules:* The network devices in the data plane ensure the data flow. Accordingly, it is essential to check the flow rules: The flow rules [9] determine how packets are handled on the network. The rules that ensure the flow must be checked, updated, and corrected if necessary. This process should be automated in SDN networks, because automation facilitates the identification of errors that might be overlooked during manual configuration, thus achieving more secure operation.
- *QoS and rate limiting* are important tools against DoS attacks [10] [11] and ensure efficient use of network resources. Rate limiting is useful to avoid a single source overloading the network, thereby preventing a possible DoS attack that could paralyze the system with a traffic flood. Attention should be paid to the creation of QoS policies and the setting of traffic priorities. Proper prioritization helps important applications to operate smoothly even in the event of a possible attack. The setting of rules should be solved dynamically, if possible, so that the system reacts according to the current situation.
- *Network segmentation – Virtual network*: Dividing the network into smaller parts significantly increases the effectiveness of security settings [12]. During segmentation, division into parts helps to isolate security risks, i.e. a threat that has arisen in one segment does not spread to the entire network. One of the tools for segmentation is the use of virtual networks in SDN networks. These special networks ensure the separation of individual departments, which facilitates efficient and secure traffic- and access-

control. Special protection rules can be set up to meet the needs of the current segment, which specifically protect, for example, critical operations and data. The central control used in SDN simplifies the implementation and monitoring of the rule system for virtual networks.

— *Policy enforcement – automation:* One of the important features of SDN is the ability to automate the enforcement of security policies. Automation [12] helps to avoid possible human errors (humans are the weakest element of the network) to apply policies correctly regardless of the size and topology of the network and according to actual needs. Automation significantly reduces administrative activity, saving the administrator from manual installation, protecting the network from possible errors made here. The central programmability of SDN networks allows the creation of security policies that can be dynamically modified according to real-time attacks.

— *Monitoring - Real-Time Monitoring - Logging*: Monitoring or real-time observation enables immediate detection of deviations from established rules and helps in rapid response [13]. Continuous logging of these observations is important. Detailed, immediate logging helps in later error management and the development of a more effective control system according to the given attacks and emergencies.

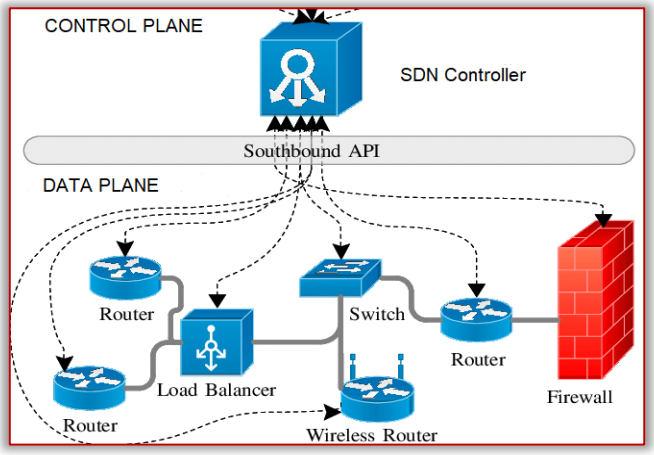

Figure 2. Data Plane - SBI - Control Plane [16]

— *Interlayer communication and security:* The communication between layers is facilitated by well-defined interfaces, northbound and southbound interfaces [14]. The data plane is connected to the control plane by the southbound interface (SBI) (Figure 2). Protocol security and mutual authentication are essential to protect the channel. Communication between the lower two layers is implemented via the open standard OpenFlow protocol, which can be protected by SSL/TLS protocols [15].

Control plane security

The control plane contains SDN controllers, which are practically the basis for ensuring smooth network operation. Perhaps the most important task in SDN security is to properly protect these controllers. The device authentication and network segmentation, as already have mentioned at the data plane are indispensable.

— *SDN Controller Security Authentication and authorization:* The basis of SDN controller security is the creation of authentication and authorization solutions [12] [13]. It is necessary to ensure that only authorized users and applications can communicate with the controller.

— *User Authentication - Application Authentication:* In the network, it is worth identifying users with a multi-factor authentication (MFA) method, not just a username and password. Role-Based Access Control (RBAC) is recommended for applications, which always works on the principle of the least privilege, ensuring that the given applications only access the resources they need.

— *Encryption – data transmission*: During data transmission, encryption is indispensable for the security of communication within SDN networks (not only in SDN, but also in traditional networks). It can be used to prevent unauthorized users from accessing data during communication with the controller. It is important because otherwise unauthorized users could read and manipulate the data, which could have a decisive impact on the operation of the network. The Transport Layer Security (TLS) protocol already mentioned in the data plane can be used for data encryption, but other methods can also be applied.

— *Redundancy – load balancing – backups:* In legacy networks, redundant devices and redundant paths are used. This is not different in SDN networks either. Since the SDN controller is the soul of the network, high availability has to be ensured. This is coupled with ensuring the reliability of the device. The redundant use of multiple controllers helps to ensure that in the event of a failure, there are no problems in the operation of the network,

no reconfiguration is required, the only task is to activate the redundant device, which can provide uninterrupted operation with a small delay. The use of redundant controllers also promotes proper load balancing, which on the other hand improves performance and can divide the fault range into smaller parts, thereby increasing fault tolerance. These solutions ensure that the network continues to operate at the expected level even in the event of a possible cyber-attack or a simple hardware failure. However, redundancy does not replace regular backups. It is important to regularly back up and the controller configuration, which helps to ensure that the configuration can be restored quickly in the event of a network failure with as little data loss as possible [12] [13] [14].

— *Interlayer Communication and Security - Providing Northbound Interface:* In SDN networks, the Northbound Interface (NBI) (see Fig. 3) is a very important sublayer. It provides communication between the SDN controller and the applications that manage and monitor the network. In terms of maintaining the security of the NBI, preventing application-level attacks is one of the most important tasks, because here an attack can jeopardize the operation of the entire network [14]. The application programming interfaces (APIs) used in NBI must be made secure and applying appropriate API keys. OAuth tokens must be used to verify authentication and related permissions.

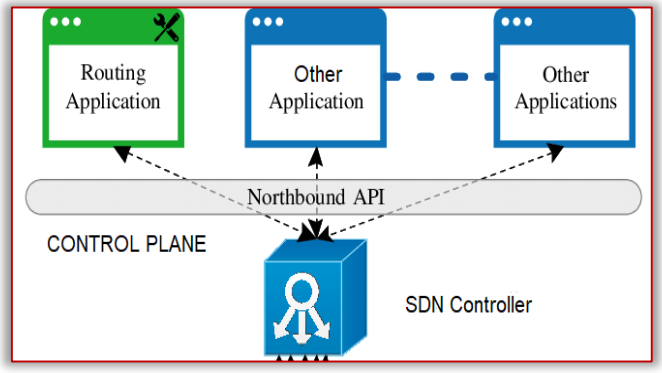

Figure 3. Control Plane - NBI - Application Plane [16]

— *API security - design - authentication:* When designing the API, security considerations must be integrated from the beginning, with particular attention given to preventing potential attacks. It may be useful to use HTTPS instead of HTTP protocol, and to design the current rate limit. Strong authentication is indispensable. In addition to the above-mentioned API keys, multi-factor authentication and role-based access control can also be useful, which can also be used to protect the controller. These solutions allow only trusted applications to communicate with the SDN controller.

— *Monitoring and logging* [12] [13] [14] are a key part of network security, especially during inter-layer communication. They enable the detection of suspicious activities and the response to events that indicate an attack. Monitoring requires the use of tools and techniques that can monitor API requests, responses, and possible discrepancies in real time. Continuous, detailed logging records events between the control layer and the application layer. The information displayed in the log (e.g. IP addresses, user data, user actions, and time stamps) helps in the preparation of analyses in the event of an attack or error, thus making it possible to develop more effective defences later. Monitoring and logging help in sending an alert in the event of a suspicious activity, or in carrying out an immediate response. With a well-defined problem-solving plan, it is possible to act more effectively and quicker to prevent a possible intrusion attempt. Although new and new attack methods are emerging each day, with a carefully protected control layer, an attack attempt can be thwarted and prevented with a good chance.

Application plane security

The application layer [12] [13] [14] contains software that ensures network management. It is essential to check and verify the authenticity of applications in this layer, which can prevent the appearance of malicious software in SDN networks. Authentication and the regulation of appropriate access permissions, such as access to vulnerable functions or data, are important. A useful solution is the allocation of role-based access, which can help to more easily limit certain operations and monitor the processes occurring in the network.

The application layer is connected to the control layer via the northbound interface, so it is essential to properly protect the APIs that provide the connection. Protecting these applications significantly increases the security of the network, which can prevent policy manipulation and unauthorized access. It is important to check software updates and use

the latest version, which ensures the highest possible level of security. The use of continuous logging is also essential in this layer.

THE FUTURE IN SDN SECURITY

SDN networks are constantly evolving, new solutions are emerging, and security challenges are becoming more and more complex. In order to keep the network protected, it is essential to use new methods, such as artificial intelligence (AI) and machine learning (ML), or the Zero Trust security model.

AI and Machine Learning

Artificial intelligence (AI) and machine learning (ML) are making a significant contribution to network security, enabling more effective threat detection and automated, faster and more reliable responses to detected intrusion attempts [17]. ML and AI can analyze large amounts of data in real time, creating patterns and deviations that allow for early detection of potential attacks and defense against them. Of course, this solution requires continuous learning to keep up with emerging attacks.

Zero Trust Networks

The zero trust security model [18], which works on the principle of "never trust, always verify", can play an important role in the SDN environment. In this method, it is mandatory to continuously verify the identity of users and devices, regardless of where in the network they are located, thus reducing the number of insider threats and unauthorized access. For this continuous verification to be sufficiently effective, it is essential to segment the network. The segments operate independently of each other, based on appropriate, strict access rules. Protecting smaller units is more efficient, faster and more reliable. It is important to use dynamic policies instead of static policies. Dynamic security policies adapt to the current environment and user behavior, thus ensuring that access is allowed or denied based on real-time assessments. The Zero trust solution increases the security of the SDN environment by verifying every access request, significantly reducing the possibility of attacks.

CONCLUSIONS

Like the security of traditional networks, the protection of SDN networks is also very important. Nowadays, SDN networks are slowly but surely replacing the existing infrastructure. Of course, challenges must be faced in the course of the transition, including replacing the existing infrastructure with a new environment. It is a money-consuming and time-consuming task. It is also important to note that operating an SDN network requires much higher qualified network administrators, whose training is also not a cheap item. It is also certain that the possibilities offered by SDN (separation, central control) may cause some difficulties from a security perspective, primarily due to the use of southbound and northbound interfaces. However, with appropriate authentication, encryption, a dynamic rule system, as well as good monitoring and logging, much more effective network protection can be created. Not to mention the possibilities offered by AI and ML mentioned above.

References

[1] D. Kreutz, F. M. V. Ramos, P. Esteves Verissimo, C. Esteve Rothenberg, S. Azodolmolky, and S. Uhlig, "Software-Defined Networking: A Comprehensive Survey," Proc. IEEE, vol. 103, no. 1, pp. 14–76, Jan. 2015

[2] A. Lara, A. Kolasani, and B. Ramamurthy, "Network Innovation using OpenFlow: A Survey," IEEE Commun. Surv. Tutorials, vol. 16, no. 1, pp. 493–512, 2014.

[3] A. S. Mustafa, D. Mkpanam, and A. Abdullahi, "Security in Software Defined Networks (SDN): Challenges and Research Opportunities for Nigeria.," IJCATR, vol. 7, no. 8, pp. 297–300, Jul. 2018

[4] M. Dabbagh, B. Hamdaoui, M. Guizani, and A. Rayes, "Software-defined networking security: pros and cons," IEEE Commun. Mag., vol. 53, no. 6, pp. 73–79, Jun. 2015.

[5] A. Pradhan and R. Mathew, "Solutions to Vulnerabilities and Threats in Software Defined Networking (SDN)," Procedia Computer Science, vol. 171, pp. 2581–2589, 2020

[6] S. Mishra, Department of Computer Engineering, College of Computer & Information, Majmaah University, Saudi Arabia, M. A. R. AlShehri, and Department of Information Technology, College of Computer & Information Sciences, Majmaah University, Saudi Arabia, "Software Defined Networking: Research Issues, Challenges and Opportunities," Indian Journal of Science and Technology, vol. 10, no. 29, pp. 1–9, Feb. 2017

[7] B. Gorkemli, S. Tatlicioglu, A. M. Tekalp, S. Civanlar, and E. Lokman, "Dynamic Control Plane for SDN at Scale," IEEE J. Select. Areas Commun., vol. 36, no. 12, pp. 2688–2701, Dec. 2018

[8] M. Iqbal, F. Iqbal, F. Mohsin, M. Rizwan, and F. Ahmad, "Security Issues in Software Defined Networking (SDN): Risks, Challenges and Potential Solutions," IJACSA, vol. 10, no. 10, 2019.

[9] Cisco, "What Is Zero-Trust Networking?" [Online]. Available: https://www.cisco.com/site/us/en/learn/topics/networking/what-is-zero-trust-networking.html

[10] R. Sanjeetha, K. N. A. Shastry, H. R. Chetan, and A. Kanavalli, "Mitigating HTTP GET FLOOD DDoS attack using an SDN controller," in 2020 International Conference on Recent Trends on Electronics, Information, Communication & Technology (RTEICT), Bangalore, India: IEEE, Nov. 2020, pp. 6–10

[11] C. Benzaid, M. Boukhalfa, and T. Taleb, "Robust Self-Protection Against Application-Layer (D)DoS Attacks in SDN Environment," in 2020 IEEE Wireless Communications and Networking Conference (WCNC), Seoul, Korea (South): IEEE, May 2020, pp. 1–6.

[12] T. Bakhshi, "Securing wireless software defined networks: Appraising threats, defenses & research challenges," in 2018 International Conference

on Advancements in Computational Sciences (ICACS), Lahore, Pakistan: IEEE, Feb. 2018, pp. 1–6.

[13] Paromita Nag, Siddhartha Chatterjee, and Shirsha Mullick, "Security Issues in Software Defined Network (SDN)," 2024.

[14] S. T. Ali, V. Sivaraman, A. Radford, and S. Jha, "A Survey of Securing Networks Using Software Defined Networking," IEEE Trans. Rel., vol. 64, no. 3, pp. 1086–1097, Sep. 2015

[15] W. Li, W. Meng, and L. F. Kwok, "A survey on OpenFlow-based Software Defined Networks: Security challenges and countermeasures," Journal of Network and Computer Applications, vol. 68, pp. 126–139, Jun. 2016.

[16] M. K. Awad, M. El-Shafei, T. Dimitriou, Y. Rafique, M. Baidas, and A. Alhusaini, "Power-efficient routing for SDN with discrete link rates and size-limited flow tables: A tree-based particle swarm optimization approach," Int J Network Mgmt, vol. 27, no. 5, p. e1972, Sep. 2017.

[17] S. Rysbekov, A. Aitbanov, Z. Abdiakhmetova, and A. Kartbayev, "Advancing network security: a comparative research of machine learning techniques for intrusion detection," IJECE, vol. 15, no. 2, pp. 2271–2281, Apr. 2025.

[18] Y. Ren, Z. Wang, P. K. Sharma, F. Alqahtani, A. Tolba, and J. Wang, "Zero Trust Networks: Evolution and Application from Concept to Practice," CMC, vol. 82, no. 2, pp. 1593–1613, 2025

ISSN: 2067-3809