IBIMA Publishing
Communications of International Proceedings
https://ibimapublishing.com/p-articles/39SP/2022/3941222/
Vol. 2022 (27), Article ID 3941222

Existing Methods of Security Anomaly Detection in Software Defined Networks (SDN)*

Szymon SZCZUREK and Zbigniew PIOTROWSKI

Military University of Technology, Warsaw, Poland

Correspondence should be addressed to: Szymon SZCZUREK, szymon.szczurek@wat.edu.pl

* Presented at the 39th IBIMA International Conference, 30-31 May 2022, Granada, Spain

Abstract

Software Defined Network (SDN) allows for scalability and flexibility unseen in traditional networking. Development of services and increasing threats from malicious software and attackers may put SDN-based network in danger. To ensure SDN controller security and prevent network overload the monitoring measures required. There are numerous solutions to fix numerous issues. Most of them are adapted to certain usage scenario providing pleasing results.

The development of the SDN network poses new challenges and often requires new approaches to security in SDN networks. The use of mechanisms enabling anomaly detection allows for quick and flexible reactions to occurring dangers. Constant monitoring of network traffic, state of the controller, network devices and endpoint hardware are the key aspects of detecting anomalies in SDN networks. Standard SDN network architecture is susceptible to many security problems. Centralization of a whole network control in the SDN controller causes a high risk of interruption of the whole network due to a failure of one device. This is why ensuring that the SDN works properly is one of the priorities in the area of SDN network security. The use of applications supporting network anomaly detection has been key in the field of SDN security research. Thanks to the diagnostic tools currently available in SDN networks, it is possible to determine the network status based on analysis, and not only thanks to the analysis of tests, but also data flows. This involves the need to log the packets and entries of data flows from subordinate inputs. Not without a reason, security is a key aspect of the SDN network architecture design. The use of centralized network control opens many possibilities for attackers for multiple attack types on a main network controller. Without proper security measures these networks are prone to DoS attacks, injecting malicious network traffic, and similar dangers. There is a need for implementing network's activity monitoring for all kinds of intrusions and implementations in order to effectively detect anomalies and breaches. Some of the anomaly detection solutions often demand additional modules for network switches.

Cite this Article as: Szymon SZCZUREK and Zbigniew PIOTROWSKI, Vol. 2022 (27) "Existing Methods of Security Anomaly Detection in Software Defined Networks (SDN)" Communications of International Proceedings, Vol. 2022 (27), Article ID 3941222