International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 06 Issue: 06 | June - 2022 Impact Factor: 7.185 ISSN: 2582-3930

Software Defined Network Security: A Study

V SAI VINITH, DR SMITHA RAJGOPAL

Department of Master of Computer Application , Dayananda Sagar College of Engineering

Abstract-

This paper will give you a brief and some knowledge about the Software Defined Network (SDN) Security. Based on the general definition of software defined network we know that it is made up of number of nodes, and it decouples the network control and data plans. The network across the world helps to transfer and enables to connect data. Software Defined Network is a astute networking technique, as its infrastructure is abstracted from conglomeration and its states are rationally centralized. The SDN architecture authorize networks to diligently monitor traffic and diagnose threats to facilitates network forensics, safety carrier insertion and safety policy transformation. The SDN model is foremost controlled by a central unit called controller. All the communication takes place through this controller. However, it has a drawback of getting hacked. The entire system crashes if the controller fails, the complete system will get corrupted or breakdown. This paper highlights the present and future security challenges in Software Defined Network (SDN).

Introduction-

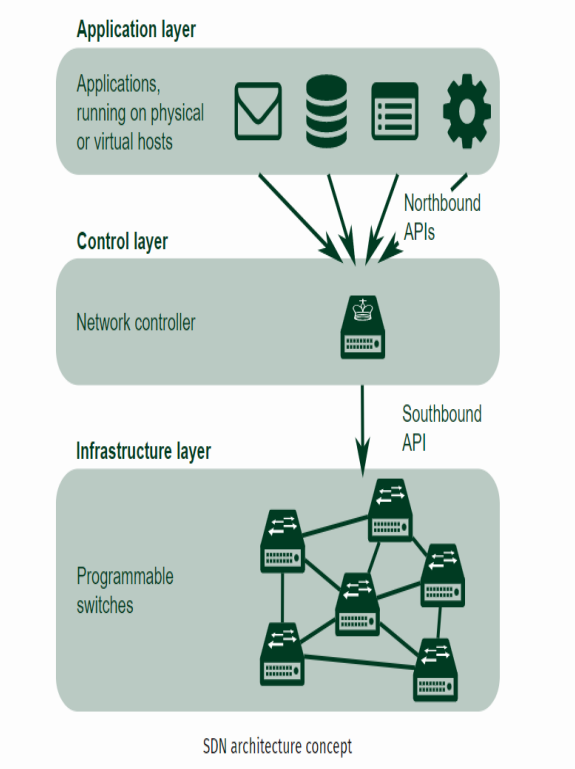
Software Defined Networking (SDN) it has been around in concept and practiced for nearly a decade. Software Defined Network has become one of the most important network architectures for simplifying network management, innovation in communication, agile and flexible. The new control functions can be executed in Software Defined Network by writing software-based logic in the control plane which deploys the decision logic in the forwarding plane through standard interfaces. A Network Operating System in the control plane provides network to the different services and applications that are performed on top of the control plane.

The networking in Software Defined Network is unified which enables in reducing the risk of scheme impact and network side security policies. It amplifies the network security with the centralized control of network conduct, global visibility of the network condition and run time manipulation of traffic forwarding rules. It proposes use cases of security services, such as intrusion detection, network segmentation, firewalling system, access controls and centralized DDoS attack mitigation system. For all this centralized system and services, the administration cost is expensive, this paper introduces a use case of SDN based firewall system to get the better of these limitations and it also brings in a use case of SDN based DDoS attack mitigation system to provide an independent and prompt configuration for unsure network traffic.

Software Defined Network (SDN) Architecture-

Software Defined Network is an architecture evolving that is dynamic, cost-effective, adaptable, manageable and making it ideal for the higher bandwidth, effective nature of applications. This architecture disaffiliates the control of networks and gives permission to forward functions which the network control to become directly programmable and the primary infrastructure to be

pre-occupied for applications and network services. The schema and requirements of applications are proposed in various kinds of architecture which currently have group and production. Among these are generally acquired one was proposed by the Open Network Foundation (ONF).



SDN architecture concept

i. **Application Layer-** The application layer consists of programs that can provide network essentials and can also provide and programmatically communicate there pertinent network behaviour for the SDN. It also consists of application, network services and tools that are used to interact with control layer.

ii. **Control Layer-** The control layer is the mid layer that connects the application layer and infrastructure layer. It has Northbound interface proceeds to the instructions to the networking components and the Southbound interface processes the instructions and requirements sent by the application layer. It additionally sends returned obligatory information abstracted from the networking devices to the utility for it function optimally.

iii. **Infrastructure Layer-** This layer consists of networking devices that control the data processing and forwarding capabilities for the network. This layer is responsible for collecting the network position like network topology, traffic data, network consumption, etc and dispatch them to control layer.

SDN Impact on Securities - Software Defined Network is not a solution for all the networking challenges, it makes handling many common issues effortless. The safety of cloud and the ability is merged which is one's own SDN community, to construct a custom machine which is obvious of holes and updates with the latest patches that seems easier. That significantly boosts safety.

i. **A cloud or multi cloud strategy provides greater security-** Cloud computing provides greater security than other infrastructure. Many enterprises that implement suitable cloud visibility and control tools will experience less security failures in data centres. The companies take all the security benefits and advantages from the cloud by relocating their networks and using the clouds to enhance infrastructure.

ii. **Update manage your network from a single point-** The SDN controller is places a very important role in a network and it provides wide range of benefits. Without any needs of changing the hardware the administrator is provided with the single control panel to be in charge of the entire network, maintain, supervise and update all network components. Designing a cyber-stronghold around the SDN controller should be the highest cyber-security preference for all SDN end users.

iii. **A Granular Approach-** Accepting the SDN also provides a special way to adapt procedures and react to the threats. Filtering out and blocking malicious traffic without harming the rest of the networks operation by the centralized controller. However, any doubtful activity will be automatically redirected and reported to the administrators.

iv. **Open-source technologies-** According to the traditional and legacy networking tools, the SDN is an open-source software, thus the code can be modified any time. The single vulnerabilities is less likely to undetected. The open source SDN networks are similar on one plane, where each is different and infinitely adjustable. This ensures the company that the system they use fits their needs. The open-source blocks make it more dependable and splitting may lead to exploiting vulnerabilities in a restricted system.

SDN Security Based on 5G Network-

The Software Defined Network is considered to meet the upcoming needs of the 5G mobile networks. The centralized security controller that interacts with SDN network controller, workable and network-aware security services will be provided for mobile users on high request. The security applications can be implemented easily in the architecture through application interface on top of security controller. It enables the on-demand reliable service and running in parallel with the mobile network zone. This feature undertakes the on-demand reliable service and the flexibility of deployment.

Drawbacks and Benefits of SDN-

Advantages of SDN

i. ***Centralization-*** Software Defined Network allows centralized management of the entire network. All of the networking devices can be observed and administered from an imperative location.

ii. ***Cost-*** Software Defined Network universal results in value saving with the aid of using the use of higher server utilization and improved virtualization. SDN decreases network operations by enabling multiple performances.

iii. ***Scalability-*** The infrastructure of the network can be exchanged instantly without the need of acquiring and configuring resources.

iv. ***Security-*** The Software Defined Network controller provides security to the entire network. It is also equipped with single management system. One single entity controls for security and features.

v. ***Optimization-*** The use of Software Defined Network deploys the hardware devices. the existing and new hardware can be assigned with a particular cause with the use of Software Defined Network controllers.

Disadvantages of SDN

i. ***Complexity-*** There is no standardized security protocol for SDN. Only the expertise can handle The Software Defined Network system are able to prevent major attacks by the one who are expert in handling.

ii. ***Maintenance-*** The prime aspect of networking for transferring out its operations is Maintaenance. SDN lacks in maintenance.

iii. ***Latency-*** The speed of interaction between the network and the devices depends on the number of virtualized resources. If in need of more speed, more virtualized resources can be introduced. Now it results in significant amount of latency.

iv. ***Configuration-*** Reconfiguring SDN network involves lots of expenses.

Especially while enforcing SDN protocols and controller it can't be configured.

v. ***Device Security***- SDN is liberty from the use of conventional firewall and switches. The security included with them is vomited.

Conclusion-

The prominence of the SDN has conquered the requirement and need of reliable, trustworthy, well-managed and flexible networks. However, due to the separation of two planes, SDN is at risk to more attack vectors than traditional networks. This means that the accessibility, originality, stability, integrity and secrecy of network and control traffic could be harshly affected. This paper highlights some of the basic threats, impact on securities, SDN architecture, security based on 5G network and drawbacks and benefits. Software Defined Network also suffers reliability concerns which are much familiar to the structure of wireless SDN along with the matter that provoke by using wireless medium. Besides, in spite of threat or issues, the reliability advantages in a centralized Software Defined Network framework are being utilized by research efforts, which are live-time programmability and global traffic monitoring capability.

References-

[1] https://www.ieee.org/

[2] https://www.kaggle.com/

[3]https://yourtechdiet.com/blogs/software-defined-networking-sdn/

[4] Authors: Ijaz Ahmad, Suneth Namal, Mika Ylianttila, Senior Member, IEEE, and Andrei Gurtov, Senior Member, IEEE Title: Security in Software Defined Networks year: 2015 http://www.ieee.org/publications_standards/publications/rights/index.html

[5] Title: Network Security in Software defined Networks (SDN) Authors: Neetu Faujdar, Aparna Sinha, Harsh Sharma, Eshaan Verma, Amity School of Engineering and Technology Amity University Noida, India Year: 2020[IEEE]

[6]https://www.google.com/search?q=sdn+security