Research on Software-Defined Network Security Technology Based on Cloud Data Center

Fengyi Chen

konkuk University, Seoul, 143-701, R.O.K

fengyi96@naver.com

Keywords: Cloud data, SDN, Safe practice

Abstract: With the expansion of network scale and diversification of services, the original network architecture can not meet the future development needs. As a new network architecture, Software Defined Network (SDN) is proposed. SDN can realize centralized control and global optimization of the network by separating control and forwarding, and open programmable interface can realize dynamic control and scheduling optimization of network resources. Centralized control, openness and programmability not only promote the rapid development of network technology, but also bring new security problems and threats. The user requirements faced by cloud data centers are diversified, differentiated and highly customized. In this paper, SDN security technology is analyzed and studied based on cloud data center. A spectrum-based SDN deployment algorithm is proposed. Make full use of the capabilities of the whole network to mitigate attacks, effectively improve the anti-attack capability of SDN data layer and enhance the availability of data layer infrastructure.

1. Introduction

As more and more businesses migrate to the cloud data center, the user needs of the cloud data center show the characteristics of diversification, differentiation, and high customization [1]. In order to meet the above requirements, SDN with high programmability and strong flexibility is increasingly deployed in cloud data centers and has become an important network infrastructure of cloud data centers [2]. SDN technology subverts the operating mode of the traditional network, decouples the control plane and the data plane, realizes the centralized management and control of the control layer, and the fast forwarding deployment of the data layer. It has the characteristics of flexibility, openness, programmability, and virtualization. It has been widely used in the fields of cloud computing and virtualization technology [3]. However, while SDN brings convenience, it also brings new security issues. Once the attack on the SDN data layer is successfully implemented, the availability of cloud services and cloud network infrastructure, the correctness of network status data, and the reliability of network decisions will not be guaranteed. The consequences and losses caused by it Will be immeasurable [4].

At present, the research on the security of the SDN data layer of the cloud data center is in the ascendant, and there are still many problems that need to be studied and resolved [5]. Network forwarding equipment has insufficient hardware implementation methods and software processing capabilities, which makes the SDN data layer infrastructure very fragile in the face of brute force attacks. Traditional network closely couples control logic and data forwarding to network equipment, which brings complexity of network control plane management. SDN separates the control function from the network node, and uses an open software model to obtain and configure the network in a unified state based on the controller [6]. SDN's feature of centralized acquisition of network resource information is helpful for network security monitoring and detection. With the help of SDN controller to obtain real-time network global information and analyze it, it can detect and prevent network attacks more quickly. It is precisely because the SDN controller has this kind of centralized management and control that the risk of the controller being attacked increases. The SDN data layer lacks a fault-tolerant mechanism. Malicious or wrong internal nodes can easily

DOI: 10.25236/iiiece.2022.030

destroy the correctness of the network state data, thereby threatening the reliability of the network [7]. In the SDN environment, the data stream of the service running on the host needs to be forwarded through the data layer. Therefore, the special nature of the SDN data layer will inevitably affect the host and the services running on it. When the host faces an attack, it is necessary to formulate a comprehensive consideration of SDN The characteristics of the service, the characteristics of the service, the characteristics of the attack, and the attack mitigation method of how to maintain the quality of service [8]. SDN separates the control plane from the data plane. The centralized control of the control plane simplifies network configuration management, realizes flexible deployment, and improves network performance. Using SDN's feature of centralized information acquisition can supervise and detect security threats in the network and improve network security. However, with the continuous emergence of innovative security applications based on SDN, traditional security challenges and opportunities coexist.

2. Cloud Data Center and SDN

2.1 Cloud Data Center

Cloud computing is a new parallel computing mode based on Internet, which consists of thousands of servers and computers in remote data centers. Cloud computing can provide various software and hardware resources and network services. Users access the data center through various terminal devices and rent cloud computing resources according to their own needs. Cloud data center can provide users with the required services in a short time, realize diversified and comprehensive network construction of users, and ensure users' experience [9]. Based on SDN centralized control mode, comprehensive analysis of network state can be realized, so as to quickly formulate attack mitigation strategies. Using the programmability of SDN, the self-adaptive generation, installation and deletion of network flow processing rules can be realized, so that the network policy can be quickly implemented. Using distributed processing technology to realize subnetting and load balancing to avoid single point of failure. The correctness and timeliness of normal network traffic forwarding can be ensured by network traffic caching, packet polling and retransmission based on network protocol, which can effectively mitigate attacks and effectively ensure the service quality of network services, thus improving the availability of network services.

The development of distributed cloud data center brings a series of new problems: First, large-scale and distributed networks need centralized management to improve the maintenance efficiency and availability of data center. Secondly, the traffic engineering of cloud data center, whose main purpose is to carry cloud computing business, is also facing a severe test. Classification of high-traffic applications, such as cloud computing and data backup, directly affects the quality of services provided by data centers. Thirdly, across the distributed characteristics of the Internet and the development of virtualization and other technologies, the network security of cloud data center is facing the challenge of the new situation [10]. Cloud data network service center should meet the necessary service characteristics of the growing network security center, which mainly includes portability, flexibility and efficiency. Convenience requires that the cloud data center can provide users with the required services in a short time, realize diversified and comprehensive network formation of users, and ensure users' experience. Flexibility is required. Cloud data center can keep pace with the times, change the content and form for users according to different users' situations and different needs, and provide users with all-round services. Validity requires the same kind of resources, which can be reused in the data center. Information sharing and resource sharing truly realize the efficient use of resources. Combining the attack mitigation method of SDN technology and distributed processing technology, it provides two-way protection to ensure the quality of service for hosts in SDN data layer of cloud data center, and improves the availability of network services. In order to provide better cloud services and their applications, cloud data centers need higher performance networks to meet the communication needs among server clusters. Research on network architecture of cloud data center has become an important research branch to improve network performance of cloud data center.

2.2 Research on SDN Network Security

SDN has brought a brand-new revolution to the network, while bringing new security problems and threats. It also provides a new solution to the network security problem. SDN has many features that traditional networks don't have, such as global view of network, dynamic policy control, fine-grained centralized control of network, etc. These advantages bring new opportunities to network security. The centralized management and control of SDN makes the network configuration, access control and global status information centralized in the controller, so it is necessary to improve the security of the controller. The main solution is to increase the ability of security check and authority management on the controller to solve the problems of illegal access in the application layer and fraudulent use of false identity in the data layer.

The control layer of SDN consists of one or more controllers, and its logically centralized control mode can provide a global network perspective. The network administrator can send messages to the data layer through the control layer to instruct the data layer how to handle network traffic. In SDN architecture, the control layer acts as a bridge between the upper and lower layers of communication. It collects all kinds of network information from the data layer and transmits it to applications in the application layer. Once a security problem occurs in the data layer, the control layer and application layer above it will be affected.

Application layer security threats With the vigorous development of SDN, SDN applications are gradually enriched and diversified, and SDN application stores also appear. However, the security of SDN application is also a problem that can not be ignored. There are two main aspects of application layer security threats, one is the threat caused by malicious applications. The other is the threat caused by mutual interference of common applications or running errors. Applications in SDN application layer use the northbound interface to get the information of the underlying resources through the controller for interaction. If the application goes wrong, such as being implanted with malicious code, the whole network will be threatened. Therefore, it is necessary to ensure the security and legality of each application.

3. Design of SDN Security Service Architecture Based on Cloud Data

The hierarchical structure of traditional IP network, with relatively independent layers and good flexibility, has also achieved great success. With the continuous expansion of network scale, the increase of users and access devices, the rapid growth of traffic, and the closed state of vertical integration of software and hardware, the difficulty of network management is also increasing and the operating cost is increasing. SDN technology breaks the traditional network architecture, realizes the separation of control and forwarding and virtualization of underlying hardware. The control layer can better control the network traffic by maintaining the whole network view. The underlying hardware devices only focus on data forwarding, which simplifies deployment and improves efficiency. The application layer business calls the required network abstract resources through programming, which is convenient for users to configure and deploy the network quickly. Taking the data center network as an example, the new data center will become a key area for integrating all kinds of high-bandwidth applications, data and dynamic service delivery, which puts forward higher requirements for the performance, reliability, security, maintainability and robustness of the network architecture. The dynamic nature of applications and services requires breaking the closed state of the network and dynamically and flexibly scheduling network resources to meet the needs of applications and services. SDN architecture is shown in figure 1.

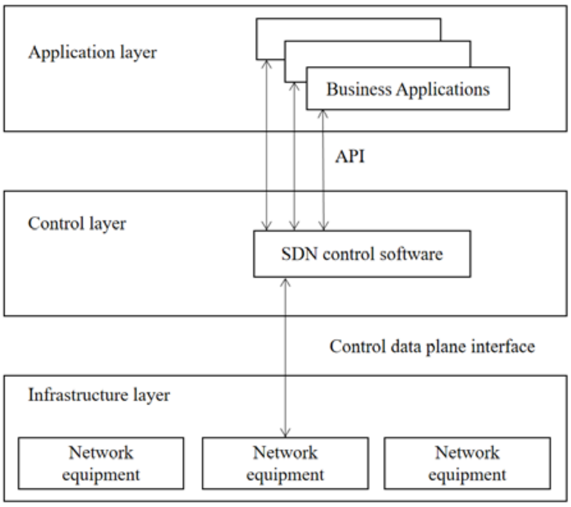

Fig.1 SDN System Architecture

Bottom-up can be divided into infrastructure layer, control layer and application layer. The controller of the control layer and the routing equipment of the infrastructure layer communicate through the southbound interface of SDN, which has a unified standard. This paper adopts OpenFlow protocol. And the application programs of the controller application layer communicate via the SDN northbound interface, which allows users to develop according to their needs. Controller is the core component of the control layer, through which users can logically centrally control network devices. The infrastructure layer is composed of network devices such as OpenFlow switches and performs simple routing and forwarding functions. OpenFlow switch consists of flow table, secure channel and OpenFlow protocol. The processing unit of OpenFlow switch is flow table, and OpenFlow protocol is based on the concept of flow to match rules, which makes network devices more flexible when forwarding data. OpenFlow architecture is shown in Figure 2.

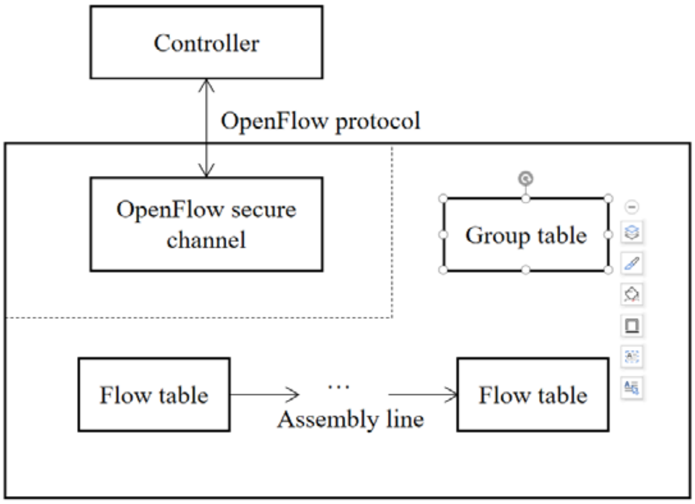

Fig.2 Openflow Architecture

The data layer is the infrastructure layer of SDN, the basic support for the normal operation of the network system, and it is very important in the whole SDN framework. The correct operation of the data packet is the prerequisite for the correct delivery of business data, the correct implementation of access control policies and the correct modification of network data packets. The network state information it provides is the basis for generating various network policies. Once the data layer has security problems, the control layer and application layer on it will be affected. Then the correctness of network decision-making and network behavior of the whole network will not be guaranteed. It can be seen that the security of data layer plays a vital role in the security of the whole SDN. In the process of cloud data users from mirror data service to virtual data service center, there are still factors of network instability. However, the network security and the degree of information protection of the network are particularly important for users, which directly affects the user experience.

4. Conclusions

With the continuous development of cloud data center, especially the appearance of distributed cloud data center, today's data center has evolved into a high-performance computing place that involves servers with a scale of 100,000 or even one million, is geographically dispersed across the WAN, and integrates the operation and storage of big data. As a new computing mode, cloud computing has been widely used for its unique technologies in data storage, data management and data processing. SDN, which is characterized by high programmability and flexibility, is increasingly deployed in cloud data centers, and has become an important network infrastructure of cloud data centers. At present, SDN has made great development and progress, with a very broad development prospect and space, and many security problems, which require the joint efforts of researchers to make it more perfect. The position of the controller in SDN architecture is very important. From the analysis, it can be seen that the security problems of SDN mainly focus on the control layer, so improving the security of the controller will be the further research direction of SDN network security in the future. In addition, the standardization of northbound interface can provide a more unified method for authentication and authority management between control layer and application layer, which will also be the focus of future research.

References

[1] Liu Min, Teng Hua, He Xianbo. Software-defined network DDoS real-time security system based on kernel function[J]. Journal of Computer Application Research, 2020, 037(003):843-846,850.

[2] Zhao Jianli, Zhang Xiaoyan, Zhao Jiankun, et al. Research on Transmission Line Ice Monitoring Method Based on Image and Stress[J]. Automation and Instrumentation, 2018, 33(10): 5.

[3] Wang Mengmeng, Liu Jianwei, Chen Jie, etc. Software Defined Network: Security Model, Mechanism and Research Progress[J]. Journal of Software, 2016(4): 24.

[4] Zhang Yuqing, Wang Xiaofei, Liu Xuefeng, et al. Overview of cloud computing environment security [J]. Journal of Software, 2016, 027(006):1328-1348.

[5] Wei Wei, Qin Hua, Liu Wenmao. Software-defined access control framework for cloud environment[J]. Computer Engineering and Design, 2018, 39(12):51-56.

[6] Zhang Ye, Shang Jin, Jiang Dongyi. Research and practice of cloud data center network security service architecture[J]. Information Network Security, 2016(9):6.

[7] Shi Yue, Li Xianglong, Dai Fangfang. An enhanced software-defined network security framework based on attribute-based encryption[J]. Information Network Security, 2018(1): 8.

[8] Wu Zehui, Wei Qiang. Software-defined network controller cluster fail-safe recovery method based on OwnShip-Proof model[J]. Information Network Security, 2016(12): 13-18.

[9] Lu Ping, Dong Zhenjiang, Yang Yong. Development Trend of Integration Business Technology in the M-ICT Era[J]. ZTE Technology, 2016, 022(002): 61-66.

[10] Shi Zhikai, Zhu Guosheng. Research on software-defined network security[J]. Computer Applications, 2017, 037(0z1):75-79.