Advanced Science and Technology Letters
Vol.134 (MAS 2016), pp.87-93
http://dx.doi.org/10.14257/astl.2016.134.15

Security Research for Software Defined Network

[1]Jianfei Zhou, [2]Na Liu

[1]Admission and Employment Office, Chongqing Industry Polytechnic College
fn219@qq.com
[2]School of Information Engineering, Chongqing Industry Polytechnic College
na814@qq.com

With the changing of network structure, software defined network becomes the main structure of the next generation network, which can realize network definition by the software programming according to the control platform, so that the network can be controlled. However, the network configuration is flexible and convenient, but also brings the problem of network security, so that the attacker can configure the network to achieve the purpose of stealing information. To solve this problem, this paper formulated a software defined network security scheme according to the different business classification, simulation results can conclude that the proposed scheme can effectively improve the reliability of the system.

Keywords: software defined network; information security; service differentiation; cyber attacks

1 Introduction

The typical data communication network is composed of user terminal equipments and network infrastructures, network infrastructure equipment is mainly responsible for the data exchange tasks of the switches and routers, as well as media links. The current OF switch is still mainly used ASIC chip, through the ACL implementation, but the support of the OF protocol is limited, the main performance in the flow table width is limited, the flow table capacity is small, do not support some of the changes in the field, etc. Due to lack of demand, chip manufacturers in the development of new OF dedicated chip on the sidelines, as a compromise solution, Broadcom developed a set of tools to support the general ASIC chip programming, so that it supports OpenFlow protocol [1-2].

ISSN: 2287-1233 ASTL

2 Related works

2.1 Research of SDN application layer

On the application level, since the emergence of SDN technology, scientific research institutions, equipment manufacturers, Internet companies, IT service providers and telecom operators are all active in research, continuing to explore and try to promote their business processes.

Japan's NTT is one of the early operators SDN technology research, developed a virtual network controller for multiple data centers for unified service and on-demand configuration, has deployed the data center in Europe, the United States and Japan. Tatsuo Mori, NTT innovative architecture Center Manager at the global SDN technology conference held in May this year, mentioned they are trying to virtualize cloud data center and the routers and switches.

FNsdn-fm projects, China Telecom introduce the need and architecture of SDN research in the existing network, and lead to complete the IP RAN network technology industry standards based on SDN in the country. In the application, Beijing Telecom and HUAWEI complete the commercial deployment of SDN in April this year, the SDN technology is successfully applied to IDC (Internet Data Center) network, and released a series of new IDC business based on SDN. China Unicom is also based on "woyun" to carry out the small scale of SDN application pilot, the pilot focused on the functional verification and test equipment.

2.2 Principle of SDN

Control information interaction is neural network of software defined network, which is particularly important in power dispatch system based on wide area network. SDN used in electric power dispatch system will not take CLEAN SLATE technical route, that is, all the devices are replaced with the OPENFLOW switch, so we must consider the three aspects. Firstly, how to coexist in a network between the SDN control plane and the original network control plane. Secondly, how to guarantee the reliability and timeliness of information interaction in SDN control. Thirdly, which features the realization of SDN has advantages, and which features are more suitable for the original network technology to achieve. In the data center and LAN, due to the equipment type is single, network range is narrow, bandwidth resource is rich, the business model is simple. Therefore, it is very easy to implement single southbound interface and reliable internal control information access, Network control and management of the problem can be modeled as a large part of the controller, the controller is processed.

IP and multimedia Technical Committee (TC1) under the future data network task group (SWG3) software-defined research as the core of future data communications network. The contents include: typical application scenarios

and north to the interface requirements of architecture research, including containing interaction between controller and turn baking Abstract protocol research. Analysis research related industry agreement as a reference.

3 Proposed scheme

The access security problem is contained in the cloud computing. Cloud computing in hides many of the details, both operating process of network management details, also covers service provides the technical details of the process. These details can not be seen often is not available. After the cloud users to submit their own data to the cloud service provider, lost control of the data, you can not know the specific details of processing data in the cloud can not be aware of processing sensitive personal data is processed traces left without means assess the safety of data processing procedure [5].

Finally, there is a wide range of cloud types of attack threat. According to the classification of cloud services, network attacks can be divided into: SAAS attackers, such as packaging, browser based attacks; PAAS attacks, such as cloud injection attacks, metadata trick attack; IAAS attacks, including denial of service attacks, buffer overflow attacks, anti-virus and cloud spam processing. For these attacks, cloud service providers should have the ability to resist attacks and cyber threats.

3.1 SDN security access design

OpenFlow as the mainstream technology of the SDN architecture, the OpenFlow protocol to join the traditional switch to form a OpenFlow switch, based on the built-in flow table design data forwarding strategy. The remote controller is transmitted to the switch by the lower current. By configuring the flow table, the OpenFlow switch can be accepted or rejected by the user request according to the predetermined policy. API is a functional module to the interface of the controller, a part of the function strategy can be stored in the SDN controller, which can be sent to the OpenFlow switching device. At the same time, the SDN controller is designed for the whole process of data forwarding through the API [6-7].

Rely on cloud computing provides a powerful computing and storage support, security services can greatly enhance the security services to respond to the threat of defense, the acquisition speed of abnormal events and event correlation analysis and other capabilities to enhance the entire network security capabilities. Furthermore, since the security services specifically for cloud access security cloud service, you can do in-depth research in the cloud security services to provide better meet user demand security services.

3.2 Network attack detection

Network intrusion detection technology is a technology which is applied to computer virus detection, and it can also be used to detect whether the strategy is used to detect the security of the deployed application. At present, the common use of malicious code detection technology has the integrity verification, the behavior analysis detection technology and the entity characteristic code detection and so on. At the same time, the input and output rules of the program are analyzed, and the two code rule database is generated according to the test result: S (Security) and M (Malicious).

3.3 Attack success rate prediction algorithm

The successful execution of attack must rely on certain preconditions, such as the OS version, user rights, and whether the specific port is open. These conditions are not satisfied or only partially satisfied, the probability of attack is obviously lower; in contrast, the attack is relatively high probability of success. Further, according to the experience of network security, we can know that the success rate of the attack has a high sensitivity to the change of security measures. In summary, in order to objectively reflect the attack success rate and related factors restricting relations and enhance the relative discrimination findings, we propose to estimate the success rate of attacks empirical formula is:

$$SR = \frac{n}{e^{J\beta}} \tag{1}$$

Among them, n is the matching degree between the premise condition and the node vulnerability information, J is the target node using security measure intensity, β is the sensitive factor [9].

4 Experimental results and analysis

Testing of the cloud access scheme based on the SDN, we must first ensure the function of each module to achieve normal. Function module is the focus of this part of the test, the purpose of the experiment is to verify the feasibility of OpenFlow technology for secure cloud access solutions, verify the correctness of the functional module in the OpenFlow environment can handle the user request, the controller can save the network management strategy in the control level, the function module of the expansion and rapid recovery ability. Another purpose of the experiment is to verify that in a complex network environment, the controller can request for the user to select the optimal access path and in this way to enhance the user experience, this part of the test parameters focused primarily on the delay characteristics. Because the function module of the three units of the security services to provide a similar pattern to the network attacks and threats to detect the network attack to provide a case study of the service, to

build the experimental environment. Its computer simulation environment is shown in Table 1.

Table 1. VM configuration

	Processor	Memory	Hard drive
VM_1	1×2 GHz	4 GHz	500 GB
VM_2	2×2 GHz	8 GHz	1 TB
VM_3	4×2 GHz	16 GHz	2 TB
VM_4	8×2 GHz	32 GHz	4 TB

The simulation process is generally shown in the following figure, according to the virtual task and scheduling to achieve the model, the core algorithm for the development of the preparation of its scheduling interval according to the different simulation environment, need to set up a separate.

On the basis of good service scalability and rapid recovery of services, SDN-based Secure Cloud Access program if it is reasonable to schedule resources, it will definitely reduce the waste of resources, to solve some of the equipment overloading problems. The load balancing method of the system uses the static resource scheduling strategy, such as weighted round robin scheduling algorithm, the target address hash scheduling, but the static algorithm is difficult to adapt to the dynamic changes of the cloud environment K user request. On the other hand, with the increasing demand of computing resources, the overall energy consumption is also growing, high energy consumption directly lead to low resource utilization, system management costs increase. In order to integrate the resources effectively, reduce the number of hardware and improve the utilization of the resources, we propose the optimal path algorithm. This algorithm can be the best route calculated in real time according to the data transmission node traffic and communication loss. In order to test the impact of the optimal path algorithm on user access delay, the throughput of IPS is firstly measured, and the change range of IPS load is determined. As shown in Figure 1, the packet length is 64, 128, 256, 512, 658, 769, 886, 1024, 1270, 1532, bytes of IPS device without packet loss, the maximum transmission rate, that is, the throughput. Under the restriction of gigabit network card, the throughput of the packet length increases with the increase of the length of the packet, and the maximum reached 672Mbps.

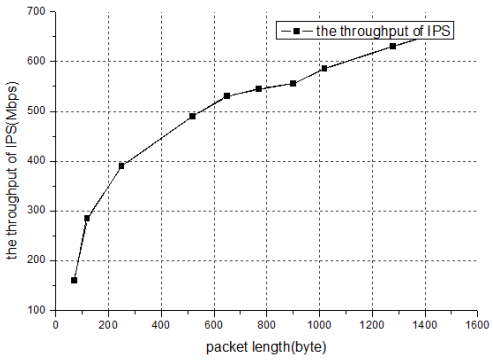

Fig. 1. SDN system throughput

5 Conclusion

According to the characteristics of the software defined network, this paper proposes access security mechanism of software defined network, network attack detection method and the success rate of network attack prediction, these mechanisms and methods can effectively ensure the security of the network, which can be applied to security of the software defined network. The large-scale deployment of software defined network makes the security problem more and more attention. The security problem of cloud computing structure in software defined network needs to be explored in the future.

References

1. Sezer, S., Scott-Hayward, S., Chouhan. PK.: Are we ready for SDN? Implementation challenges for software-defined networks [J]. Communications Magazine, IEEE, 2013, 51(7): 36-43.
2. Shin, S., Porras, P., Yegneswaran, V., A Framework For Integrating Security Services into Software-Defined Networks [J]. Proceedings of the 2013 Open Networking Summit (Research Track poster paper), ser. ONS, 2013, 13.
3. Baldini, G., Sturman, T., Biswas, AR., Security aspects in software defined radio and cognitive radio networks: a survey and a way ahead [J]. Communications Surveys & Tutorials, IEEE, 2012, 14(2): 355-379.
4. John, W., Pentikousis, K., Agapiou, G.: Research directions in network service chaining[C]//Future Networks and Services (SDN4FNS), 2013 IEEE SDN for. IEEE, 2013: 1-7.
5. Rothenberg, CE., Nascimento, MR., Salvador, MR.: Revisiting routing control platforms with the eyes and muscles of software-defined networking[C]//Proceedings of the first workshop on Hot topics in software defined networks. ACM, 2012: 13-18.
6. Kim, H., Feamster, N.: Improving network management with software defined networking [J]. Communications Magazine, IEEE, 2013, 51(2): 114-119.

7. Singh, S., Khan, RA., Agrawal, A.: Flow Installation in Open Flow Based Software Defined Network; A Security Perspective [J]. innovation, 2015, 4(1).
8. Shin, S., Yegneswaran, V., Porras, P.: Avant-guard: Scalable and vigilant switch flow management in software-defined networks[C]//Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security. ACM, 2013: 413-424.
9. Pentikousis, K., Wang, Y., Hu, W.: Mobileflow: Toward software-defined mobile networks [J]. Communications Magazine, IEEE, 2013, 51(7): 44-53.