International Journal of Security and Its Applications
Vol. 10, No. 8 (2016), pp.343-352
http://dx.doi.org/10.14257/ijsia.2016.10.8.30

Attack Detection Research for Software Defined Network

Jianfei Zhou and Na Liu

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

Abstract

Software-defined network structure of the network fundamental changes, its network equipment to achieve the hardware and software isolation and virtualization technology underlying hardware, so as to further development of the network provides a platform. This is due to the hardware and software isolation, making the network more vulnerable to attack, thus changing the topology and business information. To solve this problem, the paper depending on the traffic data and the corresponding topology, the method gives security software-defined network, combined with business process model of cloud computing, network security algorithm optimization. Simulation results show that the proposed method is robust to a variety of business, and can effectively prevent network attacks.

Keywords*: Software-defined network; cloud computing; business architecture; network attacks*

1. Introduction

Soft define the network as an emerging technology is developing rapidly in recent years in this demand. Soft define network data network control plane and forwarding plane separation, making the network with dynamic, flexible, programmable features. At the same time, based on this architecture, the new business model has the flexibility and customizability of the current network visualization techniques proposed new requirements, on the one hand, the need for new business were characteristic visual display, network and user the dynamic interaction; on the other hand, should show real-time status of network resources, equipment and resources to facilitate real-time monitoring of network management personnel. Further, since the technology, especially this technology into the network is still in its infancy, the current needs of visualization techniques to show its characteristic features and effects, while countering should technical superiority, making it in the industry to achieve promotion. Architecture brings these advantages, it also raises new problems. Centralized controller layer data forwarding behavior unified control and management, there are inherent security issues, first, because the network open for the upper application, making the centralized controller vulnerable to security threats from the application layer; Second, the centralized controller to host a large number of network load, most likely single point of failure; and finally, the study of the technology is still in its infancy, the relevant protocol standards are not perfect, this is the attacker provides a multiplicative machine. Therefore, preclude the use of appropriate defensive measures to build some safety-critical module. Cloud services are the main mode of the future of Internet services, cloud data centers as an information-processing infrastructure, the efficient coordination of the Internet in large numbers of servers and storage devices, for storage and high-performance processing of massive data. Become the basic demands of the Internet data center.

SDN technology provides flexibility, openness for the current data center network,

ISSN: 1738-9976 IJSIA

scalability, while also facing a number of security issues. These security threats seriously hampered their promotion in the market, therefore more and more experts and scholars industry began to expand research on these issues. SDN security issues traced is due to the concentration of the controller and its open interface provided to the upper caused. Controller as the core of the whole structure, almost all security issues revolve around how to protect its security deployment. The current study security issues usually security issues as the core controller, and as a dividing line, up to NBI (between the application and control planes), the upper application; down south to the interface. NBI refers to the third party interface provides a centralized controller for the network operators. To reach more or less security vulnerability advocated openness, developed by designers for the attacker to provide a convenient. Not currently standardized interfaces so that an attacker could design some applications, the use of a plurality of mismatch between the indirect attack or a direct attack on one by one each of the vulnerabilities, resulting in failure of the centralized controller. Use northbound interface, developers can design three diverse application, they also provide an opportunity for the malicious attacker. Further, the controller is distributed through a policy mechanism underlying physical device management, for example: support structure agreement, issued by way of the flow table for controlling. Therefore, be considered in any deployment controller upper application will be converted to the corresponding policy. Even multiple applications within an application set policy inevitably there are some rules of conflict, without some mechanism to avoid policy conflicts, will lead to the failure of one or more applications, will lead to serious disorders of the entire network control mechanism.

The industry widely recognized southbound interface protocol, the use of secure channel data encrypted manner to prevent theft outside the control and forwarding planes to exchange information, but safe passage protocol used Bian, cannot confirm whether there is a connection terminal after the connection is established threat, and therefore can be forged at the beginning of the relevant certificates for the attacker, a security attack after obtaining certification. In addition, in large networks, due to the presence of the controller to each switch latency problem may occur multiple distribution policy inconsistencies, for example, have been detected if the two conflicting strategies simultaneously executed in the network due to the delay factor, It will lead to policy failure. And traditional security threats facing similar centralized server for centralized control of devastating attacks, the same common denial of service attacks (attacks), injection attacks, and authentication attacks. On the other hand, since the network is currently carrying a huge amount of traffic and network rich and varied business needs of server processing power, storage capacity have put forward new demands. How to achieve the feasibility backup program controller, the controller to the load balancing also become an important direction for protection controllers security.

2. Related Works

2.1. SDN Security Research

Reduce the use of the API, to develop a unified standard API, to defend against the attacker's malicious attacks. Also, you can develop appropriate auditing standards, the deployment of security flaws isolate fundamentally. However, due to the flexibility of the code, the standards have encountered great obstacles. Currently, the northbound interface standardization issues still in its infancy. Scholars have put forward an application authentication framework called through authentication and authorization mechanisms to prevent malicious applications access networks. But the certification process only by means of encryption, if malicious applications get a key, through the relevant certification audit mechanisms, security threats, the same can not be avoided. Researchers and from malicious code detection direction of the upper application to avoid security threats, but

the data [6] proposed mining method is only suitable for detecting some open source application code, for some non-open source applications will no longer fit. Document [7] design policy conflict detection module can better detect and policy network will have to be configured in a conflict between the policy enforcement, [8], the design called safe execution core modules can be detected potential conflicts policy rules, and through the design of a certain security policy program implanted inside the controller, while the inspection policy rule violations discovered malicious applications. One kind SDN control framework, by setting the threshold limit certain events frequently access controller, and the load is transferred to the underlying pressure for processing, to avoid the possibility of malicious attack traffic controller for the attack. For authentication attacks, some scholars have proposed the use of the access control user roles for different user applications to verify.

User plane interface provides a view through the interface, so that users can trigger the service to observe the service status (ready, were to end) and provide the resources the state graph; Application Controller plane (responsible for using the correlation algorithm for scheduling joint data center network resources and application resources transport plane, select the data center business places; control plane through the square by agreement to collect, abstract transport plane of the optical link information reported by plane transport plane consists mainly of the underlying grid flexible optical network resources available light. slots and hops).

2.2. SDN Intrusion Detection

Network security has attracted wide attention, the development of intrusion detection technologies are maturing. Traditional intrusion detection techniques include signature-based detection, anomaly detection and detection based on artificial intelligence algorithms. Intrusion detection feature must be defined based on a set of rules and features that can be used to determine certain rules and intrusions. Therefore, feature-based intrusion detection technology can achieve high accuracy and minimum false alarm rate. But this intrusion detection methods can not detect unknown attacks, 0day exploits known attacks or some variant. Signature-based intrusion detection system can increase attack detection capabilities through frequent updates rules or feature data. In the feature detection section SNORT, the information and load characteristics of the known intrusion in the form of a packet header matching to determine whether suffering from some kind of attack. In the SDN, the feature-based intrusion detection technology can also be used to detect known attacks, it can be placed in the network can also be placed in the controller. With traditional networks, it can not detect unknown attacks SDN network.

Anomaly-based intrusion detection is also called behavior-based intrusion detection, detection of the main host or network activity and normal behavior whether such intrusion detection technology compared to exhibit abnormal. In these intrusion detection technology, often contain some data mining, statistical models and hidden Markov model algorithm. First abnormality detection process generally legitimate user activity data collected over time, and then observe the stage host or network behavior, and then use statistical methods to test the legality of such acts. This method can detect intrusion detection has not been found in known attacks. The key factor anomaly intrusion detection method is to generate some kind of rules to reduce the unknown or known attacks false alarm rate.

Some soft computing method can be used to deal with uncertain or partially true behavioral data to reduce the false positive rate of intrusion detection system. These soft computing methods including artificial neural networks, fuzzy logic, and association rule mining, support vector machines, genetic algorithms, and artificial immunity. These algorithms can be used to improve the detection accuracy and detection effect and feature-based anomaly intrusion detection system. Canady is proposed for the network misuse detected three-layer neural network. Wherein the feature vector contains nine

network features: protocol id, source port, destination port, source IP address, destination IP address, ICMP type, ICMP code, the length of the original data and the original data. But the extremely low accuracy of intrusion detection. Moradi and Zulkernine proposed intrusion detection system based on multilayer perceptron. Using more hidden layers can improve the accuracy of neural network algorithm based intrusion detection system. There are some intrusion detection system is based on self-organizing map or distributed delay neural network algorithms to improve the detection accuracy. Which can be quickly distributed delay neural network classification. Data and conversion data. Other soft computing algorithm proposed above can also be used in combination to improve the accuracy. Vieira *et. al.*, Application Anomaly Detection cloud computing environments artificial neural network algorithm, and indicate in order to improve the accuracy of intrusion detection, there must be more training samples, more hidden layers and the training phase.

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. For business continuity and robustness of the network requires a relatively high service, cloud computing security incidents may cause the interruption of its business, the business and the user can not consider the loss.

Data integrity requirements can not be changed by the user outside of authorized users, privacy requires that only authorized users can read the data, the data availability requirements can be undisturbed for the cloud used by the user. Cloud computing should strengthen the identity authentication, access rights assignment, data isolation control management for unauthorized users.

But the difficulty is that, for a variety of customer service needs, cloud service providers must dynamically respond to user requests. Cloud users do not know the location of data storage, and do not know how to handle the data server, do not understand the situation through the network transmission, and even do not know which cloud service providers to provide services. Cloud computing has a high degree of flexibility and scalability, which makes it difficult for cloud computing to make sure the user data access security. Even cloud service providers do not know the exact location of the data, it is difficult to ensure the confidentiality of cloud user privacy data. There is also a situation, assuming that the cloud service providers have established a trust service relationship with cloud users, but this cloud service providers need to provide the calculation and storage facilities with other providers. Thus, other infrastructure providers have access to sensitive user data, user access security threat. This partnership will extend cloud users and cloud service providers to a third-party provider levels. Cloud users have the freedom to choose the right cloud service provider category. If cloud services fail to meet the actual needs of the user or the need to develop new services and service providers, then the original cloud service providers need to interact with the new service provider data. The current cloud computing industry has no standards or policies to ensure the security of business migration and data interaction between the cloud service providers, no technology to protect the user's business continuity is not affected.

At present, although the access security for cloud users has such a classification, but there is no standard system, but from the point of view of cloud computing can be found to have many similarities, such as providing data audit services; for different cloud users

to allocate the corresponding access rights. For cloud computing user data migration, but also need to invest more research. Industry needs a standard of cloud access security system to promote the progress of cloud access security. Combined with literature research, there are three aspects of the problem of cloud access security.

Firstly, cloud computing, user data in the cloud storage and processing, the user's data on the cloud is lack of effective control. This requires that the cloud service provider must ensure that the data can be used and will not be malicious delete, change, steal. Even if the problem of security, malicious behavior, system failure, cloud service providers should be able to provide lasting service. At this point, the cloud service provider's audit is very important. Audit allows users to define their control requirements, know the internal management process, analysis of external audit reports, the operation of the cloud.

Secondly, since the multi-tenant cloud environment characteristics, resulting in a user access to cloud resources, there is a user authentication and permissions allocation. In view of this problem, cloud service providers must provide authentication and authentication mechanism to effectively prevent users from obtaining valid data.

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. You can pre-design flow table entries on the controller according to user needs, the policy will function stored in the control level. Secure Cloud Access-based OpenFlow technology implementation model shown in Figure 3-3. Model consists of three parts: cloud users, cloud service providers CSP, function modules and API. Function module through the API interface and SDN controller to negotiate network management strategy, control the access route of cloud users, to provide access to the purpose of security services. For the sake of simplicity, only a cloud service provider and a set of functional modules have been drawn in the picture. According to cloud access security defense framework, functional module is composed of three units: data integrity detection, unified user management, network attacks and threat detection; each unit corresponds to the previous access security issues, to achieve an access security features The user's first request is forwarded to the functional module, which is accepted or rejected by the functional module. 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.

The basic process of the model is: when the cloud user requests access to the security service, the OpenFlow switch is assigned to the corresponding function module according to the service type. The functional module handles user requests, determines the data forwarding / blocking or access to the user's access / refused access, will perform the results through the API interface to inform the controller. The controller generates the corresponding flow table according to the feedback, and sends the data forwarding operation to the OpenFlow switch. After the same user request, the OpenFlow switch can be performed according to the flow table entries in the history of the service, and the user requests no need to pass the function module again. For cloud customized services, you

can configure the corresponding flow table entry to complete the assigned functions directly on the SDN controller. You can define the access security management model for the cloud security service cloud model. It provides access to the security aspects of the service to the user, in the form of services to provide users with security. A large number of network security equipment cluster together, forming a special security service cloud access security issues. Based on the analysis of the cloud access security framework, security services cloud can provide security services such as data integrity detection, unified user management, blocking network attacks and other security services, has a good scalability. Compared with the traditional security technology, security service cloud can greatly improve the defense capability, improve the system response rate, increase the system size, meet the needs of users more and more complex access security needs.

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. One of the most typical applications of the integrity verification technology is the verification and technology, such as the use of cyclic redundancy code to determine whether there is a certain bit in the file, complete the signature verification of the entire code, to prevent the application configuration. Real feature code detection is the use of a large number of malicious code provided by the malicious code to establish a database, and extract the characteristics of the code to be detected, and one by one to verify the database. The behavior analysis and detection technology mainly determine whether the malicious code exists in the host to modify the behavior, and through the code generated by the network behavior and the normal network behavior of the user's security detection. Based on the above techniques, we have developed two detection schemes, which are static detection and dynamic detection: 1) the static detection mechanism is mainly used to analyze the configuration of the code, including its module, programming skills, infection, *etc*., to determine whether it is malicious code, and the use of cyclic redundancy code for the entire code signature verification. 2) the dynamic detection mechanism is used to test the code of the test, and the behavior of the code can be generated using a certain debugging tool. 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). After the detection process, we can use data mining methods commonly used classification: Naive Bayes, malicious code judgment. The code vector is X, the normal procedure appears the prior probability $P(\mathrm{S})$, the malicious program appears the probability $P(\mathrm{M})$, the X is the normal procedure the posteriori $P(\mathrm{S}|X)$, X is malicious program of the posterior probability $P(\mathrm{M}|X)$, and set the threshold α, At this time according to formula (1) to realize the network attack judgment

$$P(\mathrm{S}|X) \geq P(M|X) \&\& P(M|X) > \alpha \Rightarrow XCM \tag{1}$$

Finally, the characteristic code database is filled in order to prepare the next strategy for verification.

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. In addition, the success rate of the attack is also influenced by the security measures taken by the target node, and the relationship between them is inversely related. The stronger the security measures, the lower the success rate, the lower the security measures, the higher the success rate. 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:

$$SR = \frac{n}{e^{J\beta}} \tag{2}$$

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.

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. The communication loss of the PS device link is positively related to the load, and the delay caused by the smaller IPS device is less. At the beginning of the experiment, the load of two IPS was 10%, the default mode is served by IPS I; then, the load of IPS I is gradually increased, the controller uses the optimal path algorithm, and the data traffic of two IPS devices is observed by Wireshark. The results are shown as Table 2.

Table 2. Data Traffic Comparison Results

Step	IPS I Loading	IPS I obtain data	IPS II obtain data	Shortest path Take effect
1	15%	Y	N	N
2	56%	Y	N	Y
3	72%	Y	N	N
4	78%	N	Y	Y
5	93%	N	Y	Y

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 4-12, 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.

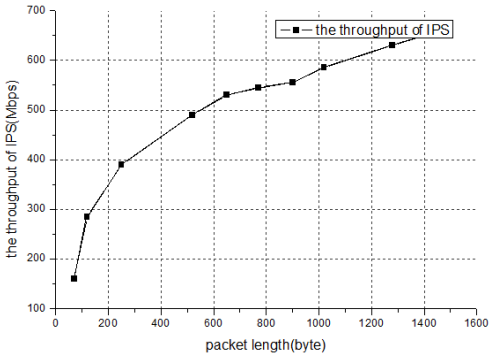


Figure 2. SDN System Throughput

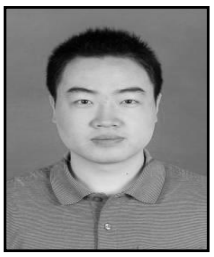
5. Conclusion

Due to the technical characteristics of software-defined network, which is more vulnerable to intrusions and attacks. In this paper, network intrusion and attack problem, a security mechanism is based on software-defined network; and according to network security, network attack detection methods were improved, a successful attack on the network to predict. Predict network attack methods to improve the safety performance of the SDN network, and can be applied to cloud computing among SDN network.

References

[1] Sezer S., Scott-Hayward S. and Chouhan P. K., "Are we ready for SDN? Implementation challenges for software-defined networks[J]", Communications Magazine, IEEE, vol. 51, no. 7, **(2013)**, pp. 36-43.
[2] Shin S., Porras P. and 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. and Biswas A. R., "Security aspects in software defined radio and cognitive radio networks: a survey and a way ahead[J]", Communications Surveys & Tutorials, IEEE, vol. 14, no. 2, **(2012)**, pp. 355-379.
[4] John W., Pentikousis K. and Agapiou G., "Research directions in network service chaining[C]", //Future Networks and Services (SDN4FNS), 2013 IEEE SDN for. IEEE, **(2013)**, pp. 1-7.
[5] Rothenberg C. E., Nascimento M. R. and Salvador M. R., "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)**, pp. 13-18.
[6] Kim H. and Feamster N., "Improving network management with software defined networking[J]", Communications Magazine, IEEE, vol. 51, no. 2, **(2013)**, pp. 114-119.
[7] Singh S., Khan R. A. and Agrawal A., "Flow Installation in Open Flow Based Software Defined Network; A Security Perspective[J]", innovation, vol. 4, no. 1, **(2015)**.
[8] Shin S., Yegneswaran V. and 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)**, pp. 413-424.
[9] Pentikousis K., Wang Y. and Hu W., "Mobileflow: Toward software-defined mobile networks[J]", Communications Magazine, IEEE, vol. 51, no. 7, **(2013)**, pp. 44-53.

Authors



Jianfei Zhou, He received the Bachelor degree in Engineering in College of computer and Information Science from Southwestern Normal University, and the Master's degree of Engineering in Computer Technology field From College of Computer Science of Chongqing University, China in 2004 and 2012 respectively. He is currently researching on Computer network, Information security, Graphics and Image Processing.

Na Liu, She received the Bachelor degree in Engineering in College of computer and Information Science from Southwestern Normal University, and the Master's degree of Engineering in Computer Technology field From College of Computer Science of Chongqing University, China in 2004 and 2013 respectively. She is currently researching on Database technology, Graphics and Image Processing.