Advances in Computer, Signals and Systems (2018) 2: 1-7
Clausius Scientific Press, Canada

Research on Firewall in Software Defined Network

Cunqun Fan[a], Manyun Lin, Xiangang Zhao, Lizi Xie, Xi Zhang[b,*]

National Satellite Meteorological Centre, Beijing, China

[a] email:fancq@cma.gov.cn, [b] email:zhangx@cma.gov.cn
*corresponding author

Keywords: Software defined networking; Firewall; Network architecture; Network attacks

Abstract: Software defined networking (SDN) technology decouples traditional network architectures to control planes and data planes, providing a new solution for developing new network applications and future Internet technologies. However, with the advent of SDN-related network equipment, security issues have become an important factor restricting its development. Traditional firewall in the face of constantly updated a large number of network attacks loopholes, the urgent need for the firewall to deal with dangerous mechanisms for innovation. This paper presents a SDN firewall architecture that describes its mode of operation and deploys it in the control plane. Simulation shows that the firewall policy has high security in the software defined network environment.

1. Introduction

In 2008, Professor Nick Meowm of Stanford University and others proposed the concept of OpenFlow, an open protocol standard funded by the Clean Slate program[1]. With further research on OpenFlow technology, software defined networking (SDN) is further proposed. Based on the Openflow protocol SDN technology is a new type of network architecture, the central controller in the form of software exists in the network architecture of the control layer, the original data forwarding layer of each device on the control part of the global centralized management of the network to be Replacement, to achieve the entire network operation of the centralized control and strategy issued. In the traditional Internet, the control function is responsible for the data forwarding decision, and the data forwarding function is responsible for the data forwarding[2]. They are tightly coupled to the same layer of network infrastructure. It is precisely because this control and forwarding highly coupled network architecture mechanism Its network control plane management becomes quite complex, when new network technology appears, it is very difficult to dispose on the original network in time[3,4]. This form of network architecture in its scalability and flexibility is difficult to keep up with the rapid development of today's network. Under the SDN network architecture standardized by the OpenFlow protocol, the control forwarding structure of the network enables the control forwarding policy to exist in the controller. The policy is delivered to the data forwarding layer through the controller to guide the network infrastructure devices Switch) for data forwarding. As a result, the functions of the forwarding layer will become simple and efficient, and

the integration of new network technologies and protocols in existing networks will be made easier. Compared with the traditional the network has dramatically improved. The logic control and data forwarding separation of this control thinking is the basis of SDN technology.

Paper [5] proposed a new firewall security system based on the architecture of software defined networking. They analyse the architecture and main functional modules of this novel firewa11 system, and expatiate on the data flow procedure of the firewal1. And they use OpenFlow switch and Floodlight controller to construct a verification environment for SDN firewall, and experiment it in light of different scene. Paper [6] introduced the relevant knowledge of SDN firewall architecture, a stateful firewall policies be designed by a software-defined network programming language pyretic based on IP address recognition, and deployed in the control plane. In order to fully show the flexibility and control of fine-grained firewall policy in software defined network environments, a stateful firewall policy is deployed and issued in the virtual network.

Compared with the deployment characteristics of traditional firewalls, the firewall deployment in the Openflow protocol SDN environment is not directly deployed on the border of the protected network[7]. Instead, the SDN firewall is deployed under the control of the central controller in the control layer Therefore, the upgrade, modification, and configuration of the firewall need not be performed one by one on the hardware devices that are in a secure state in the forwarding layer. This network operation mechanism speeds up the development and deployment of the firewall. In the SDN architecture, the deployment and delivery of firewall policies also have their own unique features: 1) flexible, through the programmable interface provided by the SDN controller, flexibility to develop a differentiated firewall strategy to build a flexible response to different security Demand firewall application; 2) high efficiency, because the SDN controller in the control layer can monitor the running status of the network infrastructure in real time so that the state of the firewall policy operation can be monitored and managed more timely and accurately, timely feedback 3) The flow table structure standardized by OpenFlow protocol in a fine-grained, SDN environment flattens the processing level for forwarding the data packet in the network, so that the data in the network is controlled by the OpenFlow protocol Under the standard data forwarding processing to meet the fine-grained requirements. The SDN firewall policy not only meets the traditional firewall access control and isolation functions, but also further abstract and processes the fields and network resources in the OpenFlow flow entry so that the firewall can have coarse-grained and fine-grained Selective space.

2. The Architecture of SDN Network and Firewall

2.1. SDN Network Architecture

As an emerging programmable network architecture, SDN decouples the traditional tightly coupled network architecture of network equipment into application layer, control layer and forwarding layer, and realizes the real-time concentration of network state operation based on OpenFlow standardized protocol Control and network applications programmable, as shown in Figure 1.

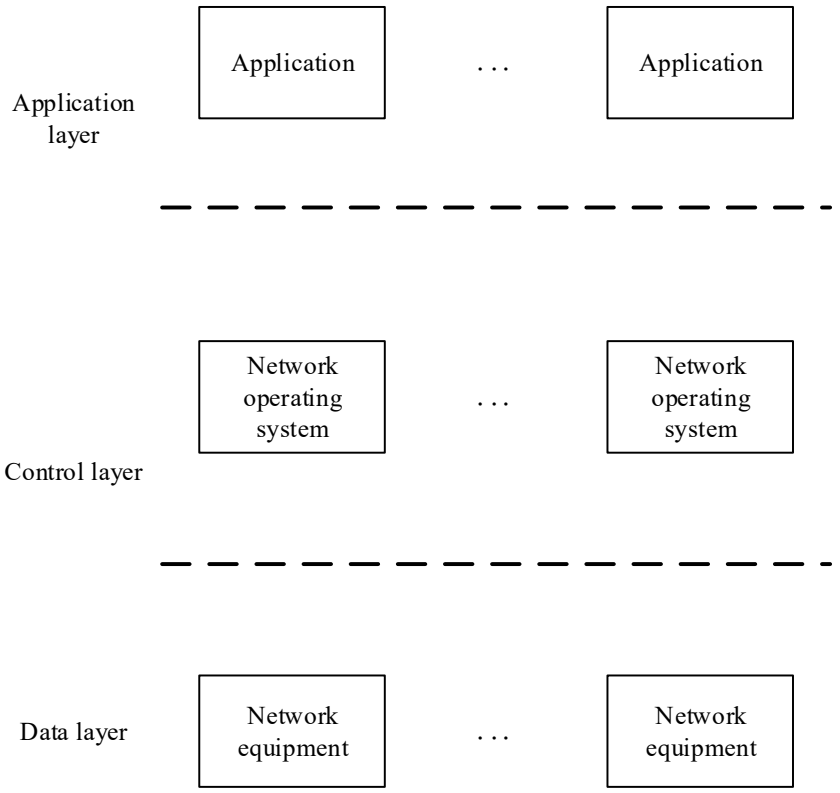

Figure 1 SDN network architecture

In the SDN network architecture, it is crucial to complete the openness and standardization of the interfaces between the various layers: (1) the interface between the control plane and the data plane (also known as the southbound interface), which shields the network infrastructure resources from being typed , Supported protocols, etc., enables data plane network devices (such as switches) to receive instructions from the control plane through the standardized OpenFlow protocol. The SDN controller performs link discovery, topology management, policy formulation, and entry issuance through a southbound protocol. The link discovery and topology management mainly involves that the controller uses the uplink channel of the southbound interface to unify the reported information of the underlying switching device Monitoring and statistics; (2) Control layer and application layer interface (also known as northbound interface), northbound interface for network users or network administrators to provide sufficient openness, so that managers can use the application layer software in the control plane The central controller issues commands and policies to the data forwarding layer to complete the control and service of the entire managed network.

The OpenFlow-based SDN technology brings operators and users more flexible network management, more efficient resource utilization, and more flexible resource scheduling. We divide it into three parts and explain: (1) more flexible network control, its standardized southbound interface shields the heterogeneity of the underlying device, managers can be achieved at the control layer through the controller Uniform control of the entire network, that is, through the SDN central controller on the forwarding layer issued instructions and strategies, without manual network hardware configuration; (2) more efficient resource utilization, as the SDN controller monitors the entire network infrastructure The state of the facility and the global control over the network real-time information, so as to be able to allocate network resources more intelligently and in real time and effectively improve the utilization rate of network resources; (3) more flexible resource scheduling, various services at the application layer Needs and applications can be achieved through the northbound interface, and then the SDN controller at the control layer sends

the network policy to the data forwarding layer through the southbound interface, thereby implementing more flexible resource scheduling.

2.2. The Firewall Composition Based on SDN Network

The software firewall under the OpenFlow-based SDN environment mainly consists of five functional modules, as shown in Figure 2.

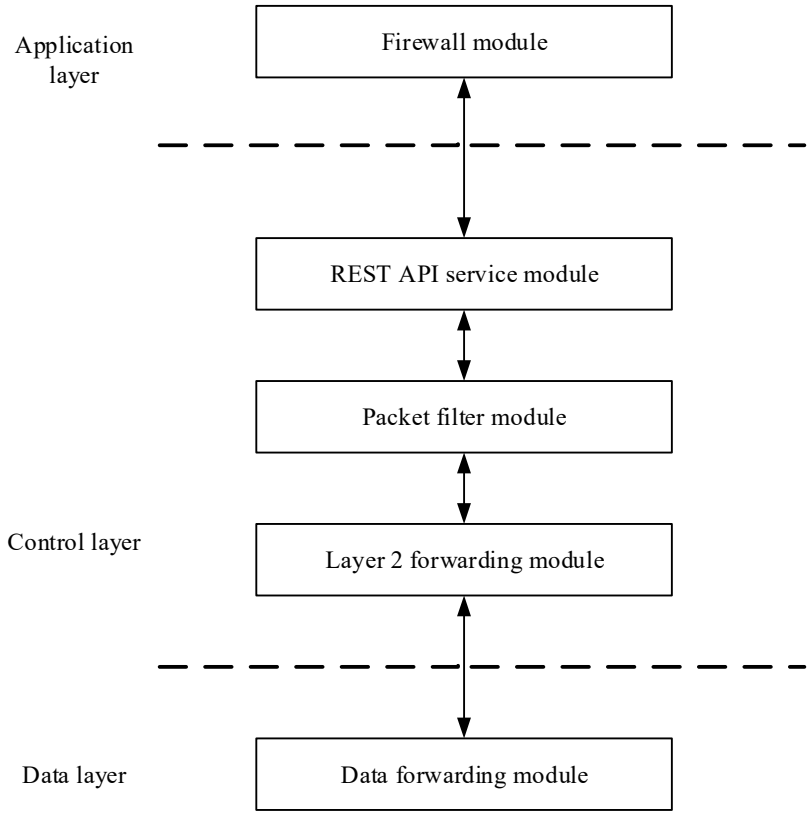

Figure 2 SDN network firewall structure

2.2.1. Firewall Module

This module is equivalent to an application at the application layer, and periodically obtains the operation status information of the underlying network through the control layer. For example, the underlying switch receives a large number of malicious data packets or network link failure of some of the links, real-time assessment of the current network security status, so as to adjust the network status query frequency, timely delivery through the controller to the data forwarding layer corresponding Packet filtering rules and a series of effective measures to provide an effective network security barrier.

2.2.2. REST API Service Module

In the control plane REST API service module is actually completed with the upper application layer docking, which is mentioned before the southbound interface, and packet filtering module is through this standardized and open programmable interface to complete with the upper firewall Module interaction. In the module, an open and programmable interface provided to the application layer, that is, a REST API, also follows the related protocols such as HTTP in the network.

2.2.3. Packet Filter Module

The module contains a set of filtering rules, the rules of the packet filter module defines the specific operation of the packet, the received data to complete the adoption or discard decision. Baotou covers multiple domains, such as source IP address, destination IP address, source MAC address, destination MAC address, and communication protocol number. The filtering rules in the packet filtering module mainly match the parameter values of multiple domains in the data packet header. The process of packet filtering is to control whether the data packet is passed or discarded directly by parsing the received data packet in the control plane and checking the parameter value of the header matching field of the data packet.

2.2.4. Layer 2 Forwarding Module

The module mainly interacts with the data forwarding layer through OpenFlow protocol, and the control information of the data packet is transmitted to the data forwarding layer through this module. The Layer 2 forwarding module mainly performs regular statistics on the network topology or the flow entry in the data forwarding layer and transmits the obtained information to the controller, which is equivalent to the hub of the command center and the data forwarding layer in the entire network.

2.2.5. Data Forwarding Module

The module runs on some devices that support the OpenFlow protocol (mainly refers to the switch that supports the OpenFlow protocol), but simply completes the forwarding of the data packet. The flow table existing in the switch is also established according to the OpenFlow protocol. The flow entry consists of a match field, a counter, and an action. Forwarding data is to prioritize the flow entries in the switch. For packets that match successfully, the action of the flow entry and the counter function are performed directly. For example, the packet is forwarded to a port of the switch and recorded in the counter the number of forwarding packages. For unsuccessful packets will be PACKET_IN sent to the controller for processing.

2.3. Firewall Workflow

Simulation when the underlying forwarding device receives the packet, through the firewall process, as shown in Figure 3.

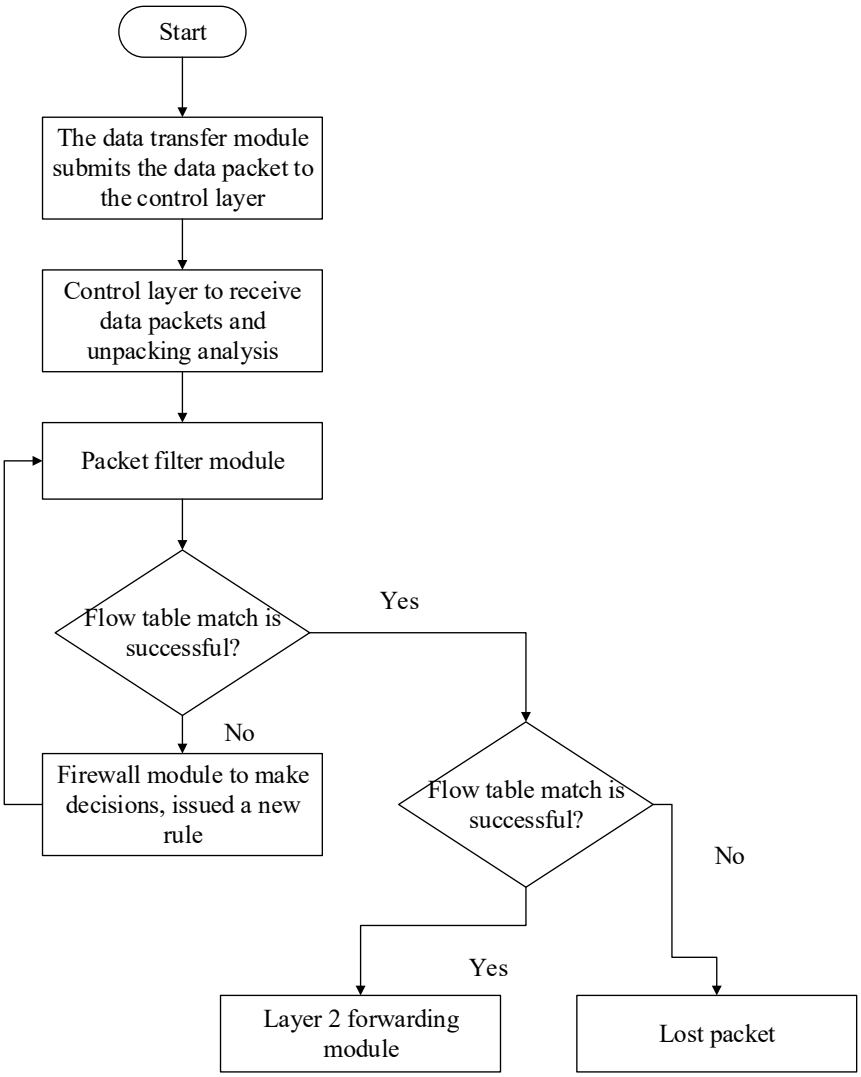

Figure 3 Firewall workflow

(1) When an OpenFlow switch receives a packet that can not match the flow table, it sends an exception message to the control layer. The control layer receives the underlying exception message, and the collected information is fed back to the firewall module of the application layer. Firewall module to develop security strategy, start the control layer packet filtering module for packet filtering.

(2) Data forwarding module forced the data packets into the control layer unpacking test.

(3) After entering the control layer, the control layer is responsible for extracting information from Baotou. For the packet filtering module, the main need is to mark bits such as the source address, destination address and port number of the data packet, and match with the pre-established rules Match until the rule table is exhausted. If the match is successful, only two actions are performed. If the action is allowed, then again to the second floor module for normal forwarding. On the contrary is to stop, packet filtering module to discard packets directly, and blocking communication.

(4) If no corresponding packet rules are found, the packet filtering module will return information to the upper firewall module through the control layer, and the firewall module will make corresponding decisions to decide the specific operation process.

(5) The new rules issued by the firewall module generate a specific URL request for the open REST API port. Then process the URL request through the REST API service module, the URI in the URL request points to the packet filtering module, and the packet filtering module generates the packet filtering rule according to the corresponding URL request. The packet filtering module processes the packet according to the new rule, decides to drop or forward, and stores the new rule in the rule table so as to be used next time to reach a real-time updated and on-demand firewall.

3. Conclusions

Software defined networking (SDN) technology decouples traditional network architectures to control planes and data planes, providing a new solution for developing new network applications and future Internet technologies. However, with the advent of SDN-related network equipment, security issues have become an important factor restricting its development. Traditional firewall in the face of constantly updated a large number of network attacks loopholes, the urgent need for the firewall to deal with dangerous mechanisms for innovation. This paper presents a SDN firewall architecture that describes its mode of operation and deploys it in the control plane. Simulation shows that the firewall policy has high security in the software defined network environment.

Acknowledgements

The work presented in this study is supported by National High-tech R&D Program (2011AA12A104).

References

[1] Mckeown N, Anderson T, Balakrishnan H, et al. “OpenFlow:enabling innovation in campus networks,” Acm Sigcomm Computer Communication Review, 2008, 38(2):69-74.
[2]Elliott C. “GENI: Opening up new classes of experiments in global networking,” IEEE Internet Computing, 2010,14(1):39-42.
[3]Jérôme F, Dolberg L, Festor O, et al. “Network security through software defined networking:a survey,” ACM, 2014:1-8.
[4]Singh S, Khan R A, Agrawal A. “Flow Installation in Open Flow Based Software Defined Network,” A Security Perspective, 2015, 4.
[5]C. Yanan, D. Chen, C. Lingwei and L. Xiaoyuan. “Design and implementation of software defined networking based firewall system,” Computer Applications and Software, 2015, 32 (1):286-288.
[6]L. Qi, C. Yunfang, Z. Wei. “Design and Implementation of Stateful Firewall Based on Software-defined Networking,” Netinfo Security, 2015, (11):47-52.
[7]Shuhaimi F A, Jose M, Singh A V. “Software defined network as solution to overcome security challenges in IoT,” International Conference on Reliability, INFOCOM Technologies and Optimization. IEEE, 2016.