

Design and Implementation of a Security Control Architecture for Software-Defined Networking

Tie-jun LIU¹, Zhao-wen LIN² and Jie XU³

¹10 Xitucheng RD, Haidian DIST, 100876 Beijing, P.R. CHINA

²10 Xitucheng RD, Haidian DIST, 100876 Beijing, P.R. CHINA

³10 Xitucheng RD, Haidian DIST, 100876 Beijing, P.R. CHINA

Keywords: SDN, SDS, Security Controller.

Abstract. Compared with traditional networking, Software-Defined Networking (SDN) enables to solve the scalability, flexibility and other aspects of the problems. However, there still have some questions about previous relevant works for security control. Thus, in this paper, we analyze the new challenges and then propose a SDN security control architecture to strengthen security control. In such a structure, security control is separated from SDN controller as a separate security controller. The security controller is used to actualize security control through both flow-based protection and agency-based protection. The method of flow monitoring in SDN networks as well as the agency deployed in nodes helps the developers to implement the security functions. We then implement this architecture and verify its scalability and robustness.

Introduction

Along with the development of new network technology, such as big data, cloud compute and network virtualization, the conventional network can no longer meet the requirement of high flexibility and scalability. The separation of control plane and forwarding plane in Software-Defined Networking (SDN) [1] makes network programmability possible, which could address the above issues. SDN defines an architecture that a logically-centralized controller to simplify management over the whole network. The controller, managing all network devices such as routers and switches, can not only optimize flow routes and divert but also balance traffic to improve the network efficiency. Still, there are some challenges emerged when implementing a SDN architecture [2]. One of the most important aspect is SDN security, which won the attention of IETF and its profiles are defined [3].

Recently, SDN security architecture is summarized as Virtualized Security Appliance (VSA) and Software Defined Security (SDS) in many research work [4]. VSA is displayed in the SDN network as a logical topology which is traditional security device after virtualization. It improves the automation level of the security operation. Based on the SDN design concept, SDS allows to separate the security control plane from data plane. With the establishment of a global security status table, security controller could generate different security services for different types of attacks. SDS, improving the openness and efficiency, is more accords with the trend of SDN security architecture.

Currently, there are some instances of SDS security architecture. FRESCO [5] added a security control module in the SDN controller. It proposes monitoring traffic information by using the script in the security control module to detect attacks. Although its proxy module method is consistent with the principle of SDS scalability, it is integrated with the depth of the controller. Besides, the use of a large number of

scripts easily make the controller load too high which becomes the bottleneck of the controller. In addition, the FRESCO application, involving no underlying security device, could not achieve the depth of protection. Meanwhile, the authoritative security organization NS Focus proposed a security architecture by using a Security Agency in the SDN controller [6]. They separated the security plane from control plane and put forward the concept of security controller responsible for the security aspects of its architecture. However, the build-in Security Agency, which is applied to communicating with security controller, would limit the scalability of its architecture and could not entirely decouple the security plane from control plane.

The traditional networking threats are also existed on the SDN networking, but its profile changes with SDN architecture. The impact of DOS/DDoS attacks with a centralized SDN controller can be worse than that with a single router. An attacker controlled SDN controller could potentially infect all the switches it managed. Meanwhile, SDN controller takes a control of security through switches by flow table and without direct interaction with the security device or nodes. It means that SDN controller could not make a depth detection in the global view and could not realize and response the new security threat fast. SDN separates control plane from data plane making the networks programmable, though the existing architecture couples control plane and security plane together, which is not in accordance with SDN design concept. And the use of a lot of scripts driven security make the controller with low scalability and compatibility, sometimes inefficiently. NSFOCUS proposes the security controller for the security content, but it still has a security agent in SDN controller to interact with security controller. For each module increased to need the agent to make an appropriate changes, which means its architecture did not achieve the full decoupling of security and control.

In this paper, we analyze some SDN security challenges mentioned above and propose solutions to solve them. A SDN security control architecture is proposed and implemented to strengthen the SDN security control. Security control is separated from SDN controller completely as security controller for all the security related affairs. We deployed sflow on the OVS[7] to forward traffic to the collector in security controller to detect and against threats by calling the northbound interface of SDN controller. And a security agency is deployed in security devices and nodes to monitor device status and interact with security controller for depth control. In one word, this architecture take control of security by both flow monitor based control and security agency based control. This paper intensively discusses the rationalization and implementation detail of the architecture. Moreover, its robustness and efficiency is verified.

The organization is as follows. The design principles of this security architecture are discussed in Section I. The detailed description and implementation of the architecture are shown in Section II. Section III evaluates the performance, robustness and efficiency of this architecture.

The Security Architecture for SDN

Design Principles

The design principles of this security architecture of network attack detection and mitigation in SDN environment this paper proposed are based on the key properties below.

Security Controller

Based on the challenges mentioned above, this paper proposes the security controller completely independent with SDN controller. Security controller can not only support the REST API for SDN security APP management but also interact with the data layer to configure the switch devices. When it is necessary to operate with Open Flow, security controller would not program anything in SDN controller but call the SDN controller interfaces. Security controller could detect anomaly flows from switches and analysis it to protect the network.

Security controller contains four modules that flow monitor monitoring the flow through switches, security agency reacts with the security devices and nodes, attack mitigation center for attack mitigation.

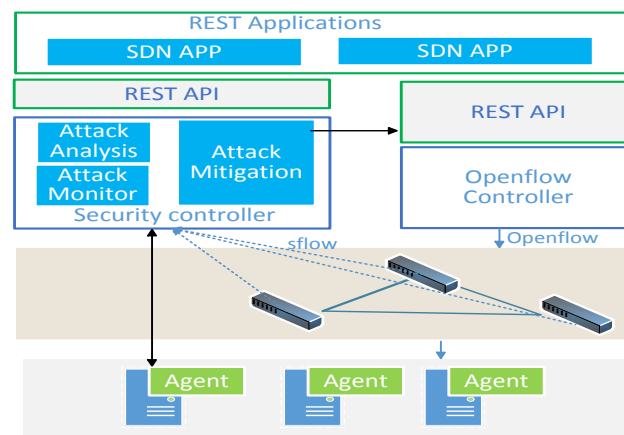


Figure1. Software Defined Security Architecture

Scalable Attack Detection

As shown in the Figure 1, OVS have been adopted to forwarding device due to confirm to the implement condition characteristics that can only provide virtual device. OVS is not only support OpenFlow but also support the most traffic analysis tools such as sflow, netflow, etc. The traffic analysis tools carry out the flow sampling to the collector in the security controller and the collector get the flow for sampling analysis. The collector would alarm the security controller mitigation module when identified the abnormal flow. Then the mitigation module would mitigate the attack by calling the SDN controller provided northbound interfaces to change the OVSs flow table.

Compared with the other traffic analysis tools, sflow has the following advantages. Sflow makes we can put the sampling traffic through OVS to the collector only since we configure the target collector related on the OVS. Sflow has the advantage of low load on OVS and not forwarding all the flow but sample flow acquisition. Moreover, sflow can keep online all the time because of its OVS embedded.

Attack Mitigation

A network attack could be divided into three steps: start the source of attack, attack spread and the destination be attacked. Most of the existing security architecture defends attacks at the attacks spread step by flow operations. But the existing approach always drops all the flows when the attacker hide in a normal flow, its discarding flow trend to be useful. Afterwards, there is another way to defend attacks at the attacking destination to limit the attacker. So when facing a network attack,

security controller can defend a network attack not only by calling SDN network controller API for flow operations but also by configuring devices to limit attacker.

To date, the existing SDN security architecture mostly works in flow plane, and it is not the best way to solve the network attacks by drop all the flows fitting the filter. Flow based protection solves network attacking problems during its forwarding, and we can solve it at the attack destination. When security controller detected a network attack, it would automatically deploy the specific security service in the target node for cooperative prevention to improve the robustness of the network. Automatically deployment requires an agent in the node for security controller controlling and it can polling node status information to security controller.

Implementation

As the principle and architecture described above, this section will show you the implementation of this architecture.

Architecture Topological

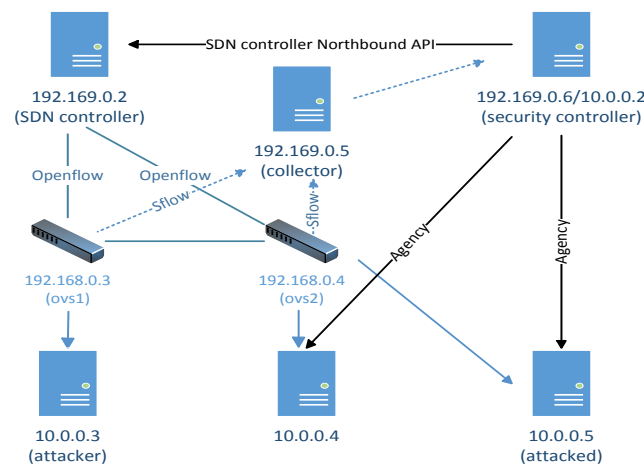


Figure 2. Security Architecture Topological

As shown in Figure 2, one SDN controller service for the whole SDN networks and owns two switches which implements from OVS. Flow monitor is deployed in switches and there is a collector receive the monitored flow. Besides, all the nodes are with a proxy for the security controller.

Sflow based Flow Monitor and Collector

Network attacks can be identified by the flow analysis through traffic devices. By monitoring the flow speed and the number of features to identify the abnormal flow and alarm to the security controller.

As the collector, InMon's sFlow-RT[8] module delivers real-time network, host and application visibility to SDN applications, making possible the development of new classes of performance aware application, such as load balancing and denial of service protection.

Sflow can provide the interface of periodical network packet statistical sampling and can provide the interface of traffic information. And its low management costs almost won't cause any burden to be counted equipment. Sflow deployment is divided into two parts: the sFlow agent and sFlow collector. Sflow agent embedded in network equipment to get real-time information and encapsulated into sflow message sent to the sflow collector. Then the sflow collector summary statistics are obtained.

Security Controller Agency

Network attack information can also be obtained by monitoring in the target, each node in SDN network deployment installation node agent, the security status of real-time monitoring, and exception information timely feedback to the safety controller.

Agent server is a module in security controller, agent client is in the compute nodes and security devices. Agents are mainly used for monitoring the security status and the deployment of security resources, including a large file breakpoint transmission is a main method to realize the deployment of security resources.

Anomaly Detection

Security Controller defines the type of attack and characteristics first, and then through the way of traffic monitoring or SC agent monitoring to capture the attack, match it based on the attack defined to identify what kind of attack for processing.

Anomaly Mitigation

According to the recognized attack types, Security Controller make different security operations. It can change the SDN controller controlled flow traffic tables by call the REST API controller supported for defense, it also can deploy distributed security resources to the node agent for defense.

Evaluation

Simulated Attacks

Step 1: Configure sflow

Configure the sflow to monitor the switches and lead the flow to the collector

Step 2: Define flows

Flows are defined by naming the packet attributes used to group packets into flows (keys), a value to associate with the flow, and a filter to select specific traffic.

Step 3: Define thresholds

Define a threshold for a defined flow.

Step 4: Monitor flows

The events that beyond the thresholds will be alarmed to the security controller.

Step 5: DOS attack-nping

Nmap [9] is a powerful tool to simulate network attacks, nping is a command to simulate a DOS attack

Step 6: Attack detection

The application polls for events, using "long polling" to receive asynchronous notification of new events.

Step 7: Deploy control

The OpenFlow controller is instructed to drop traffic from the external attacker or the security controller will deploy security resource into the nodes it controlled.

Mitigating Results

This experiment using flood to simulate DOS attack, 10.0.0.2 as attack node, 10.0.0.3 as target node, using the command "ping - f 10.0.0.3". Figure 3 shows the real-time traffic statistics which through the OVS1. The first part showed the traffic without a security controller, besides, the second part showed the traffic with a security controller. It is clearly that the security controller mitigates the traffic when the flow reaches the defined threshold.

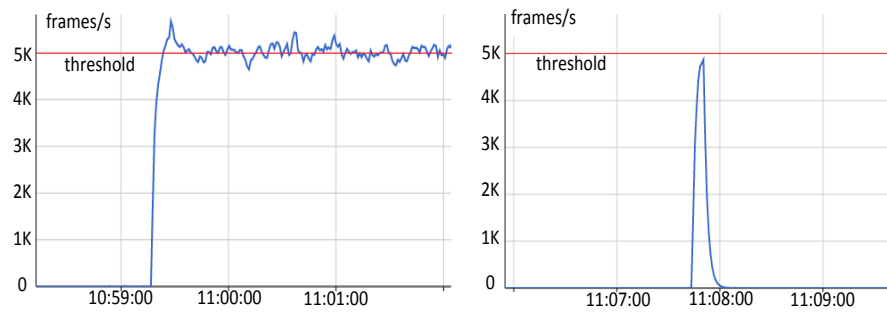


Figure3. Implemented this architecture SDN networks with DOS attack

Meanwhile, security controller deployed a security strategy which added the node 10.0.0.2 to the firewall of 10.0.0.3 by the agency in the security controller.

Conclusions

This paper proposes the security controller of SDN security architecture for both flow-based protection and agent-based protection. It simulates the DOS attack and verified the rationality and feasibility of this architecture and its implementation. Moreover, the method of flow monitoring in SDN networks and the agency deployed in security devices and nodes helps the developers to implement the security functions. However, more types of attack are needed to be simulated to verify this architecture. We also plan to improve the scalability and robustness of this SDN security architecture.

Acknowledgement

This paper is based on the research of BUPT and CETC 54 for SDN protection system and supported by the International Mobile-Internet Security Engineering Lab of BUPT.

References

- [1] Nunes BAA, Mendonca M, Nguyen XN, et al. A survey of software-defined networking: Past, present, and future of programmable networks[J]. IEEE Communications Surveys & Tutorials, 2014, 16(3): 1617-1634.
- [2] Hakiri A, Gokhale A, Berthou P, et al. Software-defined networking: Challenges and research opportunities for future internet[J]. Computer Networks, 2014, 75: 453-471.
- [3] Haleplidis E, Pentikousis K, Denazis S, et al. Software-defined networking (sdn): Layers and architecture terminology[R]. 2015.
- [4] Xiao-feng QIU, Liang Z, Teng GAO. VSA and SDS: Two security architectures in SDN[J]. Journal of Chinese Computer Systems, 2013, 34(10): 2298-2303.
- [5] Shin S, Porras P A, Yegneswaran V, et al. FRESKO: Modular Composable Security Services for Software-Defined Networks[C]//NDSS. 2013.
- [6] Information on [http://blog.nsfocus.net/wp-content/uploads/2015/09/2015-NSFOCUS-SDS- Whitepaper.pdf](http://blog.nsfocus.net/wp-content/uploads/2015/09/2015-NSFOCUS-SDS-Whitepaper.pdf)
- [7] Information on <http://www.openvswitch.org>

- [8] Information on <http://sflow-rt.com>
- [9] Information on <https://nmap.org>