©SDN-based Security in Virtualized Environments for Cloud Computing

Youngsang Shin, Kyungho Son, Haeryong Park

Information Security Group, Korea Internet & Security Agency, Seoul, South Korea
{ysshin, khson, hrpark}@kisa.or.kr

Abstract: SDN(Software-Defined Networking) is a next-generation networking technology that enables network path setting and control by software programming and entails efficient operation and management by separating the control plane and data plane. Recently, SDN has actively been deployed to virtualize networks for efficient network control and management in cloud environments, which have the characteristics of dynamic IT resource reallocation. This paper studies SDN-based security and analyzes its implication for SDN-based cloud environments. To overcome its limitation in a virtualized environment for a cloud datacenter, we propose a cooperation model between SDN-based and virtualization security to secure both of physical and virtual networks.
[Shin Y, Son K, Park H. **SDN-based Security in Virtualized Environments for Cloud Computing**. *Life Sci J* 2014;11(7):642-647] (ISSN:1097-8135). http://www.lifesciencesite.com. 90

Keywords: SDN Security; Cloud Security; Virtualization Security; SDN; Cloud

1. Introduction

SDDC (Software-Defined Data Center) has recently drawn attention for cloud computing environments because it improves the management efficiency and utilization rate of the cloud data center by virtualizing all resources including server and network. In particular, network virtualization through SDN (Software-defined Networking) is highly demanded to reduce bottlenecks by effectively configuring and efficiently utilizing the network at the cloud data center [1]. SDN is a next-generation networking technology that enables network path setting and control by software programming and entails efficient operation and management by separating the control plane and data plane.

The cost for IT resource usage and management is minimized by increasing the utilization rate of IT resources and management efficiency through the application of virtualization technology to a cloud environment. Server virtualization technology is now stably applied to a cloud environment, but network virtualization is still at its early stage relatively. To improve the situation, efforts to reduce the bottleneck in the cloud infrastructure have been actively made by applying network virtualization based on SDN technology.

This paper studies an SDN-based cloud environment from the perspective of cloud security. For this purpose, we investigate trends of SDN-based security research works in a cloud environment. With SDN technology, various security functions can be virtualized by being implemented as SDN security application. We analyze the structure, utilization scope, and limitations of the SDN security application in cloud environments. We also discuss a virtualization security to overcome the limited security visibility to the virtualized environments which SDN-based security has.

Finally, we propose a cooperation model between SDN-based and virtualization security to secure both of physical and virtual networks in a cloud datacenter. In the model, virtualization security controls the security of virtualized networks in the cloud datacenter while SDN-based security does for the physical networks. In addition, SDN-based security coordinates the security control of the whole cloud datacenter by managing security information and events collected from virtualization security.

2. Overview of SDN

The main concept of SDN is the separation of the control plane and data plane. It is realized by providing an interface that can program network devices using software. Therefore, SDN enables users to perform the programming, automation, and control of network by providing the interface based on the abstraction of data and control planes. These characteristics make it possible to build and manage the scalable and flexible network, meeting the demands of its operator.

SDN is composed of a total of three layers as shown in Figure 1: the infrastructure layer (network equipment), the control layer that controls the network equipment of the sub-layers, and the application layer that implements various functions.

The infrastructure layer abstracts the actual network equipment. The infrastructure provides standardized abstraction for different vendors' network equipment. The standardized abstraction is realized by providing an interface such as the OpenFlow protocol. With this interface, the data plane can be configured on the network.

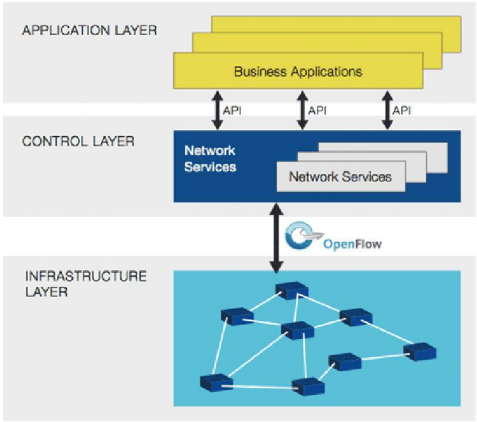

Figure 1. Structural overview of SDN architecture [2]

The control layer abstracts the entire network and plays the role of network OS. In the layer, an SDN controller generates flow rules by managing topologies and policies as network OS. It also collects and analyzes information about the network. It provides the collected information and accepts control commands through an interface to the application layer. The interface is called Northbound API. The flow rules generated by the SDN controller is transferred to the below layer, the infrastructure layer through Southbound API, which is typically an OpenFlow protocol.

The application layer consists of the SDN applications that provide various business functions including network-related functions. The SDN application collects the necessary flow information using Northbound API and sets the SDN controller to be able to control the network. Since various network-related functions including security-related ones can be implemented in the form of the SDN application, a third party other than the SDN controller developer can effortlessly develop and apply various network functions.

3. SDN-based Security

3.1 SDN Security Application

Network-based security functions can be implemented as SDN security applications. For example, network-based security functions based on network flow information such as firewall, scan attack detection, and DDoS detection, can be easily implemented as SDN security applications.

An SDN network equipment ("OpenFlow" network equipment, hereafter) queries a flow rule to the SDN controller when a new flow that is not included in a flow table in the OpenFlow network equipment comes in. At this point, an SDN security application can obtain information about the flow from the SDN controller. Once the flow information is obtained, the security function as the SDN security application can perform its job. The flow rule to decide how to handle the flow in question will be sent to the OpenFlow network equipment depending on the execution result of the security function.

Figure 2 shows an example of implementing a firewall function as an SDN security application. Assuming the application has a rule that blocks all of packets sent to host B by host A, the firewall SDN application performs the following. Host A sends a packet to Host B (①). Upon receiving the packet, the OpenFlow switch queries a flow rule to the SDN controller to process the flow (②). The firewall SDN application decides to block the queried flow by applying the access control rule (③). The SDN controller sends the block flow rule for the flow in question to the OpenFlow switch (④), which blocks the packet in question as the received flow rule (⑤).

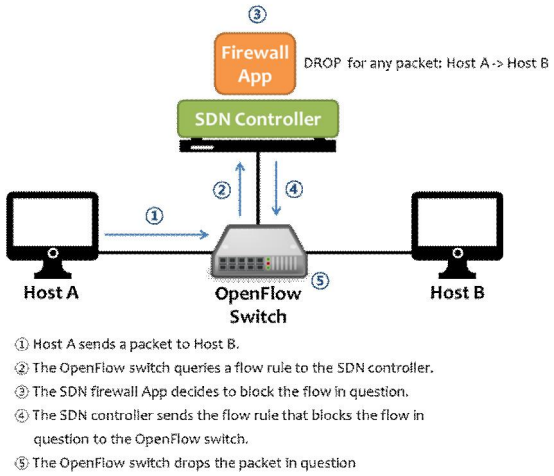

Figure 2. Overview of SDN security application for firewall function

Currently, there are some limitations on the security functions that can be implemented as SDN security applications. Since the SDN security application can acquire only the basic flow information (that is, 5-tuple information) and statistical information, DPI(Deep Packet Inspection)-based functions that entail the analysis of a network packet payload cannot be implemented. To develop more various security functions by overcoming the limitations on the information that can be acquired by the SDN controller, the SDN controller should be able to obtain more extended information about the traffic flow and provide the Northbound API for it. The OpenFlow network equipment needs to be sophisticated to provide such extended information.

3.2 SDN Security Framework

An SDN security application can be effectively developed by implementing the network

security functions in an integrated manner through the SDN controller. However, the process of SDN application development itself entails the complexity of flow information interpretation. Shin *et al.* propose an SDN security framework, *FRESCO* to remove the complexity and ensure efficiency of the SDN security application development in [3]. As a framework that provides a development environment for the security application, *FRESCO* interprets the low-level flow information, and processes and manages it as high-level network-related information for the security application. *FRESCO* can also apply security policies. The SDN security framework partly solves the problem of limited flow information by providing the flow information in an interpreted form. However, the types of the information are still limited. More sophisticated security applications require more extensive information including the payload of packets. They demand that such extended information is collected from OpenFlow network equipment and provided by the SDN controller. Some of functions supported by *FRESCO* have been applied to the open source SDN controller, *Floodlight*, which was released as *Security-Enhanced Floodlight* recently. Therefore, those functions can be immediately used in SDN environments [4].

3.3 SDN Security Application in Cloud Environments

Demand for the provision of security functions as SecaaS (Security As A Service) gets increasingly higher in the cloud [5,6]. As IT resources such as infrastructure, platform, and software are served as service in IaaS (Infrastructure as a Service), PaaS (Platform as a Service), and SaaS (Software as a Service) respectively, security functions can be efficiently provided as service in cloud environments

Shin and Gu propose a security monitoring service *CloudWatcher* for a cloud network in [7]. *CloudWatcher* enables applying security functions such as IPS(**I**ntrusion **P**revention **S**ystem) that cannot be performed by the SDN security application due to the limitations of the SDN security application as using existing network security equipment. *CloudWatcher* registers the locations of security equipment on the network and dynamically creates a routing rule and applies it to OpenFlow network equipment, so that network packets to apply security policies to can pass through security equipment, to which the security policy in question can be applied.

Not only does an SDN security application reroute network traffic to existing security equipment, but it can also improve the efficiency of the security equipment by performing security operations. In Figure 3, both of an existing DDoS(**D**istributed **D**enial of **S**ervice) security equipment and an SDN security application are used to respond to DDoS. First, the SDN security application detects abnormal flows that have the characteristics of DDoS attacks using the flow information. Only when the flow seems to be suspicious, it is rerouted to the specialized equipment used for detecting the abnormality in question, i.e., DDoS equipment for detailed analysis. Thus, the availability of security equipment in question can be improved because normal network traffic is not sent to the DDoS equipment. The work in [8] proposes a DDoS security solution to combine an SDN security application and a DDoS equipment by applying the concept described above.

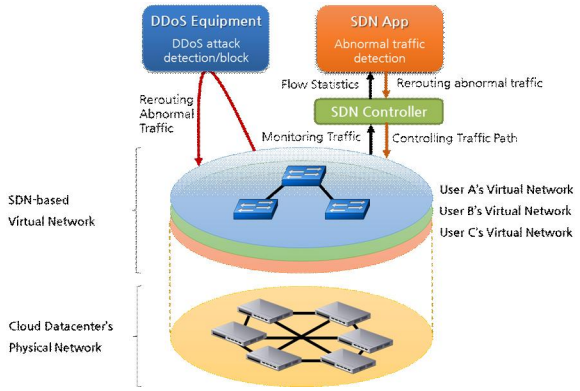

Figure 3. Overview of DDoS detection with a help of an SDN security application

4. SDN-based Security for Cloud

4.1 Limitation of SDN-based Security

Despite the strengths of SDN security as described so far, there are critical limitations when applying those SDN security technologies to a cloud environment, where the infrastructure is dynamically readjusted at the user's request. Virtualization is a key technology to realize the concept of cloud providing the IT resource demanded by the user in a timely manner. Generally, cloud is composed of virtualized systems, so that a virtual machine is the minimum host unit in the cloud. In particular, virtual packets passed between virtual machines inside a virtualized system do not leave the virtualized system. Virtual packets transferred among internal virtual machines in the virtualized system are switched by a virtual switch only within the virtualization system. Thus, the virtual packets inside the virtualized system are invisible to SDN security technologies. For SDN security application to monitor the virtual packets, the packets need to be taken from the virtualized system and rerouted to the SDN security application even when the virtual packets are only for virtual machines inside the virtualized system. However, this

rerouting of the virtual packets through the external security equipment can cause a non-trivial network performance deterioration. In addition, it can cause security vulnerability because an additional attack path can be created if the packets are rerouted to the outside of the virtualized system. Furthermore, the current SDN technology does not provide a way for SDN security applications to directly obtain the rerouted packet through a SDN controller. It can acquire only flow statistics.

4.2 VMI-based Virtualization Security

VMI-based virtualization security methodology was studied to detect network intrusion among virtual machines within a virtualized system [9,10,11,12,13,14]. The technique is applied as a form of virtual security appliance inside the virtualized system, performing intrusion detection by monitoring a virtualization network with a help of a hypervisor which orchestrates the virtualization. Therefore, intrusion detection is enabled by providing visibility to the virtualization layer within the virtualization system, which is a security blind zone to existing security equipments. In other words, such VMI-based virtualization security can responds to intrusion into virtual networks within the virtualized system. Thus, virtualization security can provide the security visibility to SDN-based security by sharing security information while SDN-based security deals with intrusion into the network that connects the virtualized systems within the cloud as in Figure 4. We elaborate this approach as a cooperation model between SDN-based security and virtualization security in Section 4.5

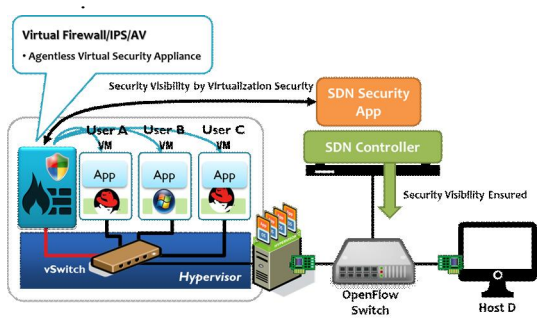

Figure 4. SDN security application cooperating with virtualization security

4.3 Cooperation Model

We propose a cooperation model between SDN-based security and virtualization security in Figure 5. The cloud datacenter includes both of virtualized and physical areas. While servers, storages, and networks are virtualized, they need to be connected over physical networks. In the model, the SDN-based security covers the physical networks. The virtualization security controls the virtualized networks. The common limitation of SDN-based and virtualization security is that they cannot monitor and control the other's territory. Thus, the cooperation model provides the full coverage of security control for a cloud datacenter.

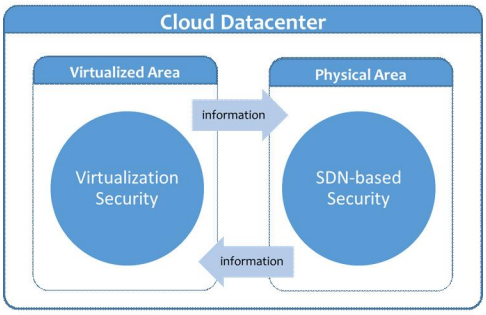

Figure 5. Cooperation model between SDN-based security and virtualization security

We depict the features of each security in our cooperation model in Table 1. First of all, SDN-based security is implemented as SDN application while virtualization security works as virtual security appliance. SDN-based and virtualization security control the security of physical networks in the cloud datacenter and virtual networks in a virtualized system respectively.

Although each of security in the model controls the security of virtualized and physical resources respectively, their main roles are a bit different in our model. In a virtualized environment for a cloud computing, multi-tenancy is an important aspect and the smallest unit of computing is a virtual machine. This means that virtual machines in a single physical server cannot be assumed to be rented by a single user. There is no static security border between virtual machines rented by different users. The group of virtual machines rented by the same user can be changed anytime. Virtualization security needs to monitor all the virtual traffic inside a virtualized system. Thus, the virtualization security is the main horsepower to control the network security in the cloud. However, it can cover only the virtual networks inside a single virtualized system. Thus, the centralized coordinator for security is required for all of the virtualization security controls in a cloud datacenter. SDN-based security can take that responsibility in addition to the security control of physical networks in a cloud datacenter in Figure 6.

Table 1. Features of SDN-based and virtualization security in the cooperation model

Feature	**SDN-based Security**	**Virtualization Security**
Form factor	SDN application	Virtual security appliance
Area covered by security functions	Physical networks	Virtual networks
Main roles	• Security information and event management (Security monitoring, Security correlation analysis and others) • Network-based security function	Network-/host-based security functions (Firewall, Intrusion Detection / Prevention
APIs	• Attack information • Abnormal traffic information	• Security events • Security information (Virtual resource usage information)

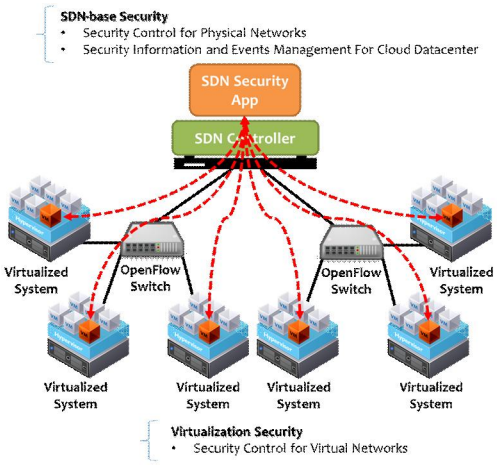

Figure 6. SDN-based security as security coordinator

Based on the main roles of SDN-based and virtualization security, SDN-based security provides attack and abnormal traffic information to virtualization security. With the information, virtualization security can proactively response to attacks which have not seen yet in the virtual network. Virtualization security delivers security event and security information including virtual resource usage. With the provided information, SDN-based security can manage the security event and information of the datacenter with a centralized view. Thus, SDN-based security can control the security level of all of the resources including virtualized network and server. Furthermore, it can detect more sophisticated attacks by correlating security events and information which look unrelated in each of virtualization security.

5. Related Works

A VMI(Virtual Machine Introspection)-based intrusion detection approach senses a malicious activity in VM(Virtual Machine) by inspecting the internal status of VM[9,10,14]. It scrutinizes the virtual memory, CPU registers, and storage of VM and traces a sign of intrusion. Garfinkel and Rosenblum in [10] present a VMI-based IDS architecture, which employs registering a callback for pre-defined malicious events in VM as well as polling any malicious change in the VM's internal states including memory and CPU registers. Their IDS performs a signature-based detection. Payne *et al.* in [9] include a block I/O activity into the list of monitored entities and present a VMI library.

The VMI-based approach requires API to hypervisor, which is an interface to obtain information from and control to hypervisor. *VMware* implements VMI libraries, *VMsafe* API and *vShield Endpoint Security* API for their hypervisor, *VMware ESXi*. These APIs support the access to the memory, CPU registers, and files in storages of VM. *Juniper Networks' vGW* [12] and *TrendMicro's Deep Security* [13] are based on those APIs. *Juniper Networks' vGW* implements virtual IPS by using *VMsafe* API to access and filter virtual network packets. *TrendMicro's Deep Security* relies on *vShield Endpoint Security* API to access and virus-scan files owned by each VM.

6. Conclusion

SDN is actively deployed for efficient network setup and control management based on network virtualization in a cloud environment, which has the characteristic of dynamically reallocating IT resources. We analyze the recent trends of SDN-based security research from the perspective of responding to network intrusion in a virtualized environment for cloud computing. Various security functions can be implemented as SDN security applications. Note, however, that there are limitations on the security functions that can be implemented due to the limitations on the information that can be obtained using the SDN controller and lack of visibility on the inside of the virtualized system. Such limitations can be overcome by deploying the VMI-based virtualization security. We present the cooperation model between SDN-based and virtualization security which can encompass both of

virtualized and physical network security in a cloud computing environment.

Acknowledgements:

This work was supported by the IT R&D program of MOTIE/KEIT. [10041872, Development of Virtual Network Intrusion Prevention Techniques: Analysis, Detection, and Prevention of Hacking in Virtualized Environments for Cloud Computing].

Corresponding Author:
Dr. Youngsang Shin
Korea Internet & Security Agency
Seoul, South Korea
E-mail: ysshin@kisa.or.kr

References

1. Digital Daily, "A New Fashion in the Cloud Age 'SDN'", http://www.ddaily.co.kr/news/news_view.php?uid=97889
2. Open Networking Foundation, "Software-Defined Networking: The New Form for Networks," https://www.opennetworking.org/images/stories/downloads/sdn-resources/white-papers/wp-sdn-newnorm.pdf
3. Seungwon Shin, Philip Porras, Vinod Yegneswaran, Martin Fong, Guofei Gu, and Mabry Tyson, "FRESCO: Modular Composable Security Services for Software-Defined Networks", Proceedings of NDSS 2013.
4. Project Floodlight, http://www.projectfloodlight.org
5. Jonghun Lee, Seungwook Jung, Souhwan Jung, "Trend of Security As a Service", Review of Korea Institute of Information & Cryptology, Vol. 22, No. 7, 2012.
6. Cloud Security Alliance, "SecaaS," https://cloudsecurityalliance.org/research/secaas/
7. Seungwon Shin and Guofei Gu, "CloudWatcher: Network Security Monitoring using OpenFlow in Dynamic Cloud Networks (or: How to Provide Security Monitoring as a Service in Clouds?)," Proceedings of IEEE International Conference on Network Protocols (ICNP), 2012.
8. Radware Ltd., "DefenseFlow – Software Defined Networking Application," http://www.radware.com/Products/DefenseFlow/
9. Bryan D. Payne, Martim D.P. de A. Carbone and Wenke Lee, "Secure and Flexible Monitoring of Virtual Machines," Proceedings of ACSAC, 2007.
10. Tal Garfinkel and Mendel Rosenblum, "A Virtual Machine Introspection Based Architecture for Intrusion Detection," Proceedings of NDSS, 2003.
11. Youngsang Shin, Miyeon Yoon, Kyungho Son, "Design of a Versatile Hypervisor-based Platform for Virtual Network-Host Intrusion Prevention," Proceedings of ICIPM, 2013.
12. Juniper Networks, "vGW Series Virtual Gateway," http://www.juniper.net/as/en/products-services/security/vgw-series/
13. Trend Micro, "Deep Security," http://www.trendmicro.com/us/enterprise/cloud-solutions/deep-security/index.html
14. Thomas Kittel, "Design and Implementation of a Virtual Machine Introspection based Intrusion Detection System," Master's Thesis, Technische Universität München.

3/10/2014