2015 29th International Conference on Advanced Information Networking and Applications Workshops

A Survey on Interfaces to Network Security Functions in Network Virtualization

Hyunsu Jang*, Jaehoon (Paul) Jeong†, Hyoungshick Kim*, and Jung-Soo Park‡
* Department of Computer Science & Engineering, Sungkyunkwan University, Republic of Korea
† Department of Interaction Science, Sungkyunkwan University, Republic of Korea
‡ Electronics and Telecommunications Research Institute, Republic of Korea
Email: {jhs4071,pauljeong,hyoung}@skku.edu, pjs@etri.re.kr

***Abstract*—Network Functions Virtualization (NFV) opens new opportunities and challenges for security community. Unlike existing physical network infrastructure, in a virtualized network platform, security services can be dynamically deployed and maintained to cope with the threat of sophisticated network attacks that are increasing over time. This paper surveys the activity that many security vendors and Internet service providers are trying to define common interfaces for NFV-based security services through the analysis of use cases and related technologies. This activity is currently lead by Internet Engineering Task Force (IETF) that is an international Internet standardization organization.**

I. Introduction

Network Functions Virtualization (NFV) is an emerging trend that network functions are implemented and provided in software, which ran on commondity hardware [1]. The key idea is to implement network functions on top of a virtualized network consisting of switches, routers, and access points. This virtualized network enables us to deploy new network services in a flexible manner.

NFV introduces an opportunity for security community. Due to the increase of sophisticated network attacks, the effectiveness of existing security services is somewhat limited. Thus, newly updated security services should be accordingly provided for networks to cope with such sophisticated security attacks over time. For example, rules for a firewall service should be dynamically maintained to filter out new patterns of suspicious network traffic.

Many vendors havr already offered Security as a Service in cloud. However, all their solutions are proprietary, with different interfaces and different modes of operation. Such security services follow a peer-to-peer model. Some functions in the security services can be hosted in data centers geographically far away from the clients that need the functions. Thus, this model requires network traffic to be forwarded to the remote data centers. On the other hand, a competing model requires clients to download their desired functions to local devices from data centers. In this model, it is difficult to maintain consistent software updates across all the devices. In addition, the current mode of operation for Security as a Service (SaaS) via a Cloud infrastructure does not have any common interfaces and mechanisms for clients or applications to verify whether or not the required functions can fulfill the policies needed by the clients or applications. Therefore, there is a lack of the efficient service policy support in the current network infrastructure.

Internet Engineering Task Force (IETF) has recently started discussing ways to apply NFV technologies to security applications [1]. Security services such as firewall, intrusion detection system (IDS), and intrusion prevention system (IPS) could be deployed as network services running on top of a network virtualiztion platform. IETF is currently investigating common network security applications and their requirements to define standard security interfaces. These interfaces will make it easy for third parties to develop security applications with network resources. In this paper, we will introduce the basic concept of NFV and its key challenging issues that are actively discussed in IETF.

The remaining of the paper is constructed as follows: Section II describes the basic concept of NFV and the needs of interfaces for NFV. Section III introduces key use cases for network security functions. Finally, Section IV concludes the paper along with future work.

II. Interfaces to Network Security Functions

The demand for cloud-based security services is growing [2]. Small and medium-sized businesses (SMBs) are increasingly adopting cloud-based security services to replace on-premises security tools, while larger enterprises are deploying a mix of traditional and cloud-based security services [3] [4].

Despite their increasing popularity, most common cloud security services do not yet have standard interfaces by which users or clients can invoke functions for their desired security services in networks. The standardization of these interfaces for network security functions is required to specify how these services can be dynamically provisioned, updated, and verified to fulfill on-demand requests. Therefore, these network security functions should be standardized to accommodate the required security services in cloud framework in an efficient and flexible manner.

Linda et al. [5] particularly raised an issue of using a customized network configuration based on virtual machines (VMs). Fig. 1 shows how various security functions can be deployed on top of a virtualized network in order to satisfy a variety of users' demands for security services.

To implement security services in such a virtulized network platform, the most challenging issue is to define standard interfaces for common security functions. With these interfaces, users can develop their own security services according to their requirements. For example, with predefined common

978-1-4799-1775-4/15 $31.00 © 2015 IEEE
DOI 10.1109/WAINA.2015.103

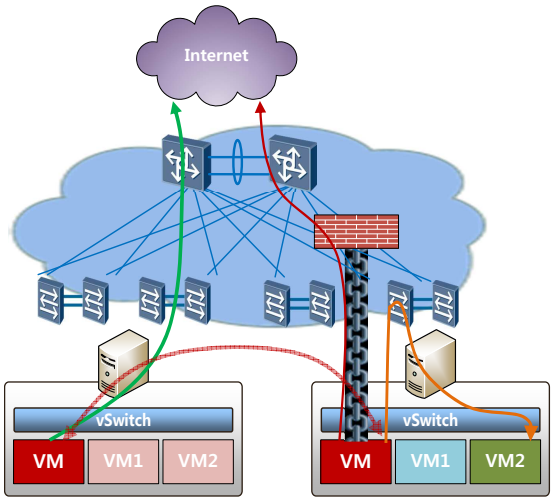

Fig. 1. Provision of Network Security Functions in Virtual Network

security functions (such as user authentication, user privilege control, packet filtering, network configuration, logging, and reporting), a firewall application can be constructed by selectively choosing a subset of these functions.

III. Use Cases for Virtualized Network Security Functions

In this section, we present some representative use cases for network security functions and their interfaces.

A. Use Cases in Access Networks

Lopez et al. [6] proposed use cases for an open operation, administration, and management (OAM) interface to virtualized security services for residential and mobile network access. Since security services are generally hard to manipulate and become expensive for client devices in access networks, cloud-based security services have attracted great attention from the securiy community. In particular, NFV could effectively be applied to facilitate the management of various resources for the benefits of client devices, which may not physically have the code of the network functions.

For the access networks, typical security applications are (i) traffic inspection, (ii) traffic manipulation, and (iii) traffic impersonation. First, traffic inspection requires a security function such as *deep packet inspection* (DPI) to analyze incoming and outgoing network traffic. Second, traffic manipulation requires security functions such as IPS, firewall, and virtual private network (VPN) to control network traffic. Last, traffic impersonation is used to monitor intruders' activities and defend networks against incoming threats by designing decoy systems (e.g., honeypots) to lure potential attackers away from critical systems in the networks.

Fig. 2 shows a use case of NFV for residential network access. As shown in this figure, a virtualized residential gateway (vRGW) can be used to securely manage the connection between home network and public network. That is, NFV allows users to define their own customized requirements. An example of a user policy is as follows: "*My son is allowed to access Facebook from 18:30 to 20:00*".

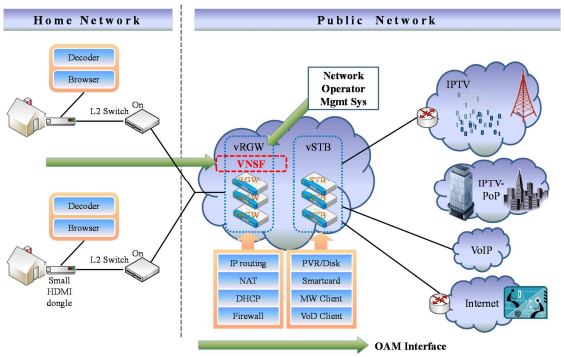

Fig. 2. Use Case of Network Functions Virtualization for vCPE

B. Use Case in Integrated Security with Mobile Networks

In [7], M. Qi et al. explained the limitations of security protection services that provide for users in mobile networks, such as 3G and 4G-LTE. Under the current network access environment, devices to use security services are limited. Also, such security functions are general and fixed in network access procedure.

To overcome the limitations of network security services, the authors addresses the need of NFV-based network security function (NSF) virtualization that is currently being studied actively. In this NSF environment, user devices with a software module invoking security functions from the cloud can enjoy the maximum system performance by letting heavy security functions be performed in the cloud. In this cloud framework, operators can provide more flexible security functions for user devices through network functions. In order to provide more flexible security functions, standard interfaces between operator networks and user devices should be defined. These interfaces will be used to request, negotiate, allocate, and operate NSF from operator networks. The authors propose three use cases for using the interfaces in mobile network environment: (i) Security configuration (e.g., authentication and encryption), (ii) Optional security function negotiation (e.g., firewall, antivirus software, junk mail filter, and anti-spam message), and (iii) Security request from a user device.

An operator network can send specific security configurations and optional security service list to user devices. The user devices can send security policy and function request to the operator network through interfaces to NSF. Therefore, through these interfaces, the operator network could provide more flexible and tailored security functions for user devices, which can provide a more efficient and customized protection for each end user.

C. Use Case in Data Center

In [8], Leymann et al. proposed data-center use cases and the corresonding requirements. The authors presented network services (e.g., firewall) that require a highly scalability and accommodate the on-demand security requests of user devices that are connected to a data center.

Fig. 3 shows the security framework based on data center. As shown in the figure, when the data center consists of network and security equipments from several vendors, data

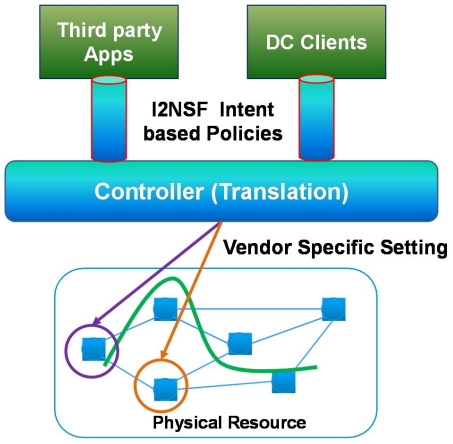

Fig. 3. Provision of Security Services in Data Center

center clients (denoted as DC Clients) can request security functions to a controller in the data center via NSF interfaces, and then such security functions are forwarded to the third party applications that will run the security furnctions and return the results to the clients. Several important requirements for data center are as follows:

- The dynamic creation, enablement, disablement, and removal of network security applications for clients.
- The policy-driven placement of new security service instances into the right administrative domain.
- The attachment of appropriate security and traffic policies to service instances.
- The management of deployed instances in terms of fault monitoring, utilization monitoring, event logging, and inventory.
- The support of distributed architectures and deployments.
- The translation of security policies into functional tasks.
- The translation of functional tasks into vendor-specific configuration sets.
- The retrieval of information such as configuration, utilization, and status.

With the requirements above, NSF will be a promising security service framework for data centers. Therefore, the standard interfaces should be defined to support security services in data centers for service providers (e.g., Google and Facebook) and large enterprise networks.

D. Use Case in Security Services based on Software-Defined Networking

In [9], Jeong et al. proposed a framework for security services based on Software-Defined Networking (SDN) and suggests two use cases for network security services. First of all, the authors addressed the limitations of legacy firewall systems and proposed security services such as SDN-based firewall system as an effective alternative to overcome these limitations.

Fig. 4 shows the framework to support SDN-based security services and applications for security services (e.g., firewall and DDoS-attack mitigator) run on top of SDN controller. When an administrator enforces security policies for the security services through an application interface, SDN controller generates the corresponding access control policy rules to meet such security policies in an autonomous and prompt manner. According to the generated access control policy rules, the network resources such as switches take an action to mitigate network attacks, for example, dropping packets with suspicious patterns.

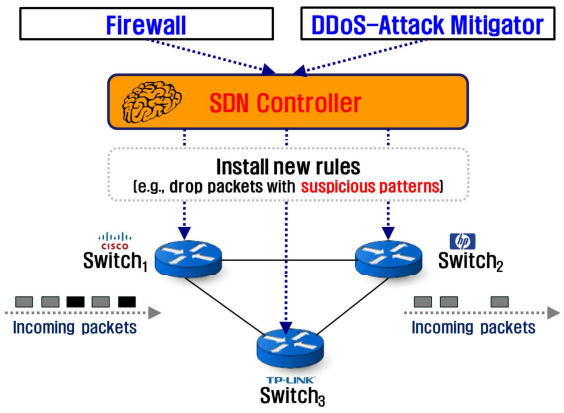

Fig. 4. SDN-based security services framework

The authors specified requirements to support the protection of dynamic and flexible network resource management to mitigate network attacks using security services based on SDN. Also, they introduced two use cases of the security services, such as centralized firewall system and centralized DDoS-attack mitigation system.

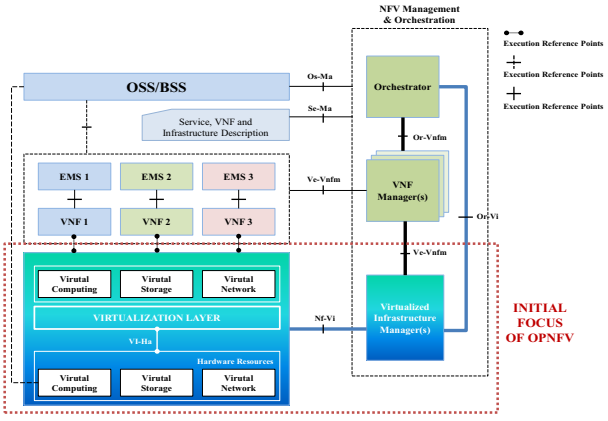

Fig. 5. OPNFV Architecture Framework [10]

E. An Open Platform for NFV

In [10], Downley et al. explained an NFV reference platform that is being implemented by Open Platform for NFV (OPNFV) [11] as an open source project. The initial scope of OPNFV is to provide NFV Infrastructure (NFVI), Virtualized Infrastructure Management (VIM), and API for other components of NFV. These NFV components compose

Basic Infrastructure required to Virtualized Network Functions (VNFs) and Management and Network Orchestration (MANO) Components.

Fig. 5 shows OPNFV Architecture Framework. Through Virtualization Layer, Physical Computing Hardware, Storage Hardware and Network Hardware are mapped into Virtual Computing modules, Virtual Storage modules and Virtual Network modules dynamically. These mappings are controlled by Virtualized Infrastructure Manager. VNF Manager operates actual VNFs by interacting with Virtualized Infrastructure Managers.

IV. Conclusion

Enterprises today increasingly consume cloud-based network security functions. However, most companies that consume cloud-based security services use off-premise provider-managed clouds. We argue that it is important to consider the need of common interfaces for network security functions that can be offered on any kinds of cloud regardless of locations or operators. This paper introduced and described use cases and techniques that are being discussed for common interfaces and framework for network security functions. We believe that these network security functions can accommodate security services in the current computing environments in mobile devices and cloud in an efficient and flexible manner. Therefore, the standardization of interfaces to network security functions will be a prerequite for the effective security services.

Acknowledgment

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Science, ICT & Future Planning (2014006438). This work was also partly supported by the ICT R&D program of MKE/KEIT [10041244, SmartTV 2.0 Software Platform] and ETRI. This research was supported in part by Global Research Laboratory Program (2013K1A1A2A02078326) through NRF, and the ICT R&D program of MSIP/IITP (14-824-09-013, Resilient Cyber-Physical Systems Research) and the DGIST Research and Development Program (CPS Global Center) funded by the Ministry of Science, ICT & Future Planning. Note that Jaehoon (Paul) Jeong is the corresponding author.

References

[1] ETSI ISG, "Network Functions Virtualization Introductory White Paper," http://portal.etsi.org/portal/server.pt/community/NFV/367.

[2] E. Messer, "Gartner: Cloud-based security as a service set to take off," in *Network World*. Gartner, Oct. 2013.

[3] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," *Journal of Network Computer Applications*, vol. 34, Jan. 2011.

[4] S. Natarajan and T. Wolf, "Security issues in network virtualization for the future internet," in *ICNC*. IEEE, Feb. 2012.

[5] L. Dunbar, M. Zarny, C. Jacquenet, and S. Chakrabarty, "Interface to network security functions problem statement," in *draft-dunbar-i2nsf-problem-statement-01.pdf*. IETF I2NSF WG, Nov. 2014.

[6] D. Lopez and A. Pastor, "Access use cases for an open oam interface to virtualized security services," in *draft-pastor-i2nsf-access-usecases-00.pdf*. IETF I2NSF WG, Oct. 2014.

[7] M. Qi and X. Zhuang, "Integrated security with access network use case," in *draft-qi-i2nsf-access-network-usecase-00.pdf*. IETF I2NSF WG, Oct. 2014.

[8] N. Leymann, M. Zarny, S. Magee, and L. Dunbar, "I2nsf data center use cases," in *draft-zarny-i2nsf-data-center-use-cases-00.pdf*. IETF I2NSF WG, Oct. 2014.

[9] J. Jeong, H. Kim, and J. Park, "Requirements for security services based on software-defined networking," in *draft-jeong-i2nsf-sdn-security-services-00.pdf*. IETF I2NSF WG, Oct. 2014.

[10] C. Price and S. Rivera, "Opnfv: An open platform to accelerate nfv," in *White Paper*. A Linux Foundation Collaborative Project, Oct. 2012.

[11] OPNFV, "Open platform for nfv," https://www.opnfv.org.