A Security Service on-demand Architecture in SDN

Li-Der Chou[1], Chia-Wei Tseng[1], Yu-Ki Huang[1], Kuo-Chung Chen[2], Tsung-Fu Ou[2], Chia-Kuan Yen[2]

[1]Dept. of Computer Science and Information Engineering, National Central University, Taoyuan, Taiwan
[2]Information & Communication Research Division, National Chung-Shan Institute of Science and Technology, Taoyuan, Taiwan

cld@csie.ncu.edu.tw, cwtseng@g.ncu.edu.tw, victor377228@hotmail.com, gjong@ms13.hinet.net, rogerone7@gmail.com, ckyen@csie.io

***Abstract*—Network security management and information risk control bring challenges to the existing networks. Traditional network architectures are ill-suited to meet the requirements of today's Information and Communication Technology (ICT) service providers and end users. Software Defined Networking (SDN) and Network Functions Virtualization (NFV) are new technologies that can provide unlimited opportunities for next generation network. Both SDN and NFV technologies are not only transforming network infrastructure from complicate physical entities to virtual and programmable nodes, but also bringing significant changes to the development of ICT. SDN and NFV enable software-driven service chain named Service Function Chain (SFC), a technology controlling the traffic flow to the appropriate applications and delivering an abstract sequenced set of service functions according to the various service requirements. In conclusion, a novel architecture as a security service platform with on-demand virtual network functions is proposed. The solution offers a security service function chain that enables ICT service providers to provision a dynamic and flexible secure service on the SDN network. Advantages of the proposed architecture are on-demand, cost effective and flexibility.**

***Keywords*— SDN, NFV, SFC, Security service on-demand, OpenFlow, Network Mangement**

I. INTRODUCTION

With the popularization of networking environment, a huge number of new attack vectors has emerged in today's network environment, which include: mobile devices, web services and cloud applications, Hypervisor, social media, browsers, social networks, etc. Network and Information Security Management for service provider is facing the new challenges. The future development of mobile cloud will leading for growth of the variety and quantity of attack vectors. Therefore, the construction of flexible and cost effective security protection architecture for reducing information security risk and enhancing services efficiency, meeting different user's security requirements, and providing security services on-demand solution with centralized control and flexible management has become the objective of future network security research topics[1].

The traditional network security devices such as firewall, intrusion detection system (IDS), and Internet content filtering are mostly deployed at the gates of network to form a physical security border. In addition to becoming a huge burden in terms of equipment investment and maintenance overhead, this kind of deployment way cannot meet the security, manageability, portability, and adaptability of rapid response required by future network system. The introduction of SDN has brought a specific solution for this issue, especially the OpenFlow based SDN architecture [2][3]. SDN is originated from the open standards-based OpenFlow funded by the Clean Slate Project of Stanford University. The research progress of OpenFlow has laid down the foundation for the development of programmable network, and this standard has become one of the research topic of US National GENI (Global Environment for Network Innovations) Project and the concept of SDN to be gradually formed [4]. The architecture, technical specifications, and development of SDN have also been officially launched along with the founding of Open Networking Foundation (ONF) [5][6][7]. The main purpose of SDN is to solve the problem of limitation of traditional network architecture, where the network is divided into Control Plane and Data Plane. By granting the network administration authority to the software controller on the control plane with centralized control approach, the network architecture can be re-arranged by software program. This kind of control mode has changed the limitation of traditional network design in the past. It has been withdrawn from existing network architecture and become programmable network. With the entire network controlled by one single logic point, the centralized control and flexible operation of network can be accomplished

In addition to the attention of SDN, the NFV has also become a hot topic recently [8][9][10]. Unlike SDN, the purpose of NFV is to solve the problems faced by Internet Service Providers (ISP). With the growth of ISP network equipment, it will take a long time and cost for searching proper deployment plans and evaluating capacity, energy consumption and softwarization technology of network equipment in order to meet diversified customer demands upon starting new network businesses. However, all equipment in existing hardware-oriented plans are not compatible and interoperable to each other such that a huge amount of equipment cost and deployment time consumption may only lead to a small amount of profit. In the light of this, NFV decouples network functions from underlying hardware so they run as software images on commercial off-the-shelf and purpose-built hardware. It does so by using standard virtualization technologies (compute, network, and storage) to virtualize the network functions. In addition to equipment function virtualization, ISPs have also tried to upgrade existing equipment with virtualization function via NFV technology such that they can flexibly introduce new services while reducing capital expenditures and operation and maintenance cost for networking equipment.

978-1-5090-1325-8/16/$31.00 ©2016 IEEE

SDN and NFV enables software-driven service chain named SFC. SFC is a kind of network technology currently under research and development by IETF which is formulated by the work groups of IETF Service Function Chain Working Group (SFC WG) and Source Packet Routing in Network Working Group (SPRING WG) [11][12]. The purpose of SFC is to guide the user traffic flow to required service with respect to user's requirements. With this deployment model, the service can be topology independent by using SDN technology to guide user traffic flows to be processed by different service functions, thus forming the Service Function Chain. Along with increasing scale of Internet, services are getting further diversified and applications are getting more and more complicated. This technology will allow service providers utilize network infrastructure more efficiently with reduced the cost of operation and maintenance of equipment, and to develop innovative network information security application and service.

The main goal of this paper is designed a security service on-demand architecture based on the SFC technology that increase the flexibility of network security service and reduce capital expenditures requirements, supporting innovative services and applications in the mobile cloud environment.

Our major contributions are summarized as follows:

- We designed a security service on-demand architecture and ensure proper security controls with SDN security solutions.
- We define the Security SFC operations and scenarios over SDN environment. This paper provides the basic guide for SFC deployment with SDN and NFV.

The rest of the paper is organized as follows: in Section II, the background and related works are addressed. Section III describe the design of the security service on-demand architecture, and the SFC operations and deployment scenarios. The last section concludes this paper and addresses potential future works in the future networks.

II. Background and Related Works

SDN is an approach to building computer networks that separates and abstracts elements of these systems. Figure 1 introduces the basic SDN components, with terminology similar to that from the original ONF white paper [13].

The basic SDN components comprise three layers, infrastructure, control and application layers. The infrastructure layer (data plane) comprises network elements, which expose their capabilities toward the control layer (controller plane) via interfaces southbound from the controller. The SDN applications exist in the application layer (application plane), and communicate their network requirements toward the controller plane via northbound interfaces, often called NBIs. In the middle, the SDN controller translates the applications' requirements and exerts low-level control over the network elements, while providing relevant information up to the SDN applications.

OpenFlow, considered the first SDN standard, which provides an open, standards-based interface to control how data packets are forwarded through the network [14]. Figure 2 is an example to illustrate OpenFlow architecture. The OpenFlow provides a basic set of global management abstractions, which can be used to control features such as topology changes and packet filtering. The OpenFlow technology consists of three parts: (1) A flow table in which each flow entry is associated with an action telling the switch how to process the flow, (2) A secure channel connecting the switch to a remote control processor (a controller), allowing commands and packets to be sent between the controller and the switch, and (3) an OpenFlow protocol provides an open and standard interface for the controller to communicate with to the switch. The OpenFlow provides multiple benefits including the possibility to have the ability to dynamically modify the network depending on the requirements, allowing the new rules propagation throughout the entire network and another benefit is to have a simplification of network management.

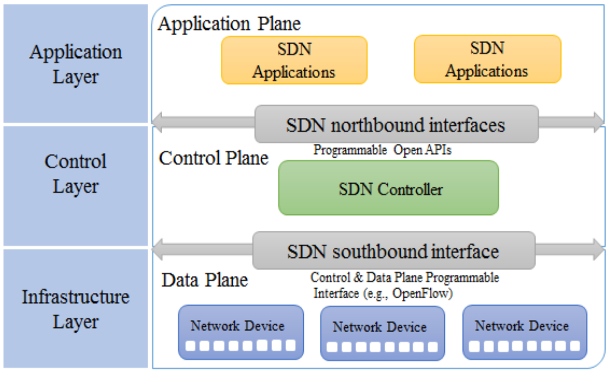

Fig. 1 Basic SDN Components

To satisfy the demands on network design and deployment as well as service application, IETF is developing a new technology called Service Function Chain, which can connect the functions of network service by virtual links. The main purpose of SFC is to lead the traffic flow of users to their required services according to users' demands. This kind of flexible deployment model allows Service Functions like Firewall, IDS, IPS, WEB Proxy and others deployed in network in any forms, which is topology independent. The Service Function Chain is established after mutually-connected service functions in the SDN network. SFC technology can bring huge reform in the deployment of network service in the future, which allows network provider make more flexible dispatch and application on service resources, effectively improving utilization of service application and reducing costs. The

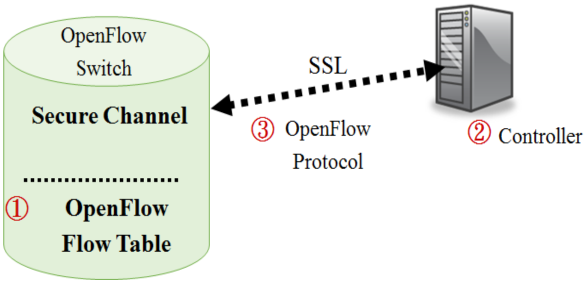

Fig. 2 OpenFlow Protocol Architecture

combining network security service and SFC can be the basis of innovating a new mobile cloud network security service.

Figure 3 illustrates the flow chart of SFC. SFC is mainly utilizing Service Classifier to make identification of different traffic flows and then classify them to the corresponding Network Forwards for SFC-Encapsulation; then transfer them to the Service Forward for a specific Service Function Chain; besides the function of selecting Service Function Path, Service SFC-Encapsulation also provide information exchanges of metadata/context of Forward node in Data plane. The function of SFC Proxy is similar to Gateway, which mainly make distinctions between the traffic flow of SFC-unware and SFC-aware functions. For the practical application, due to current SFC technology is still at draft status of IETF standard, currently SFC still face the service deployment problem in the real telecommunication network [15].

In the traditional networks, no matter the packet requirement is same or not for each traffic flow, they all need to go through the same path. While with the technologies of SDN and NFV, they can lead different traffic flows to their required services according to users' demands, meanwhile it can also inspire the technical research of SFC. From related research literatures, many researchers propose various implementing mechanism for SFC. In the framework of NGSON (Next-Generation Service Overlay Network), Service Overlay Network (SON) is a new network service framework which is formed by the combination of original service-oriented architecture and service delivery platform to realize service functions [16][17]. SON makes virtualization of service functions which were at entity network, through the service-oriented method to do flow routing. SON is in the position between Services and Underlying networks, while NGSON is under the framework of SON, making a design of service transfer system for the part of service routing. Through the system and its equipment, the flexible deployment and management of SFC is achieved. Since SDN technology determining the development direction of network, the combination of NGSON and SDN will form a combination of network resources and service function routing, which can achieve a comprehensive management on the future network[18][19].

The system architecture and operation procedure proposed in this paper is about SDN centralized control method covering from a single logical point to the whole network that can lead traffic flow of users to be processed by different security service functions aiming to users' attachment requirements; while the mutual connected service function can also be deployed with different SFCs according to traffic categories of users. That will improve the efficiency of utilizing network infrastructures and reduce costs in maintenance and management of facility application, to achieve effective management and flexible application of information security strategy[20].

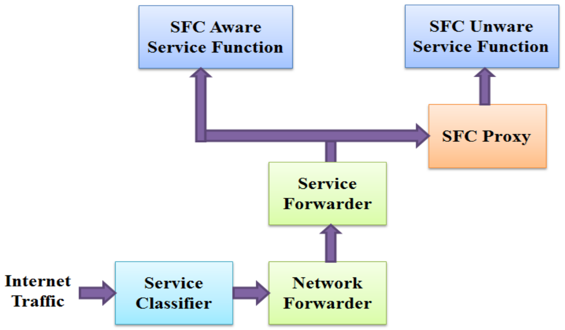

Fig. 3 SFC Flowchart

III. Proposed Security Service On-demand Architecture

In this paper, we focuses on designing control framework of SFC traffic flow paths, allowing Flow from source end passing a series of customized information security services then entering the destination, to ensure that the defense effects of network security; and provide flexible customization on every link to realize information security service with differentiation and optional deployments.

As illustrated in Fig. 4, the traffic flows are generated from the network A and the network B is the destination, each traffic flow can through the different service function path to reach their destination, the operation of SFC is similar to a mobile network value-added services, but more flexibility. Such architecture can provide value-added and self-defined services.

In consideration of the requirements on network security, if we import all service flows for network security testing, though it may prevent the flaws of information security, it will also lose the service efficiency, For instance in each Service Function, if we need to test every Flow, it will cause the delay time among endpoints increase and bring influences on the whole service efficiency; however, if we can make appropriate deployment on network security service according to practical situations, it can not only prevent the network security flaws, but also improve overall service efficiency; for example, known that streaming service is an audio transmission, there's no need to import that traffic flow for network security testing, which can avoid huge traffic processing dragging down the service efficiency. Therefore a mechanism of mobile cloud network security service on-demand is necessary. Moreover, common DDoS attack will usually consume service resources to be unable to provide normal services. If we can make dynamic allocation of Load Balance service with NFV technology, or deploy Botnet detecting services for traffic flow, the operation time of the system will be extend enough to make counter measures, which improves system validity. Therefore not only realizing SFC can make a flexible order of the comprehensive services, also practicing NFV will bring benefits on the operation and deployment of overall service resources.

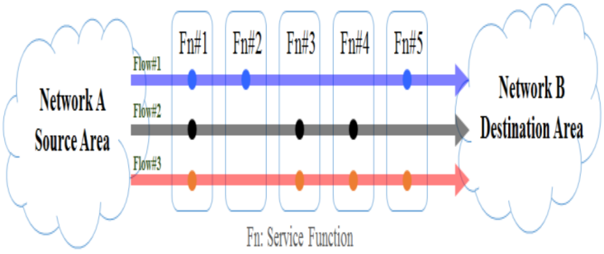

Fig. 4 Example of different SFC Traffic Flows' paths

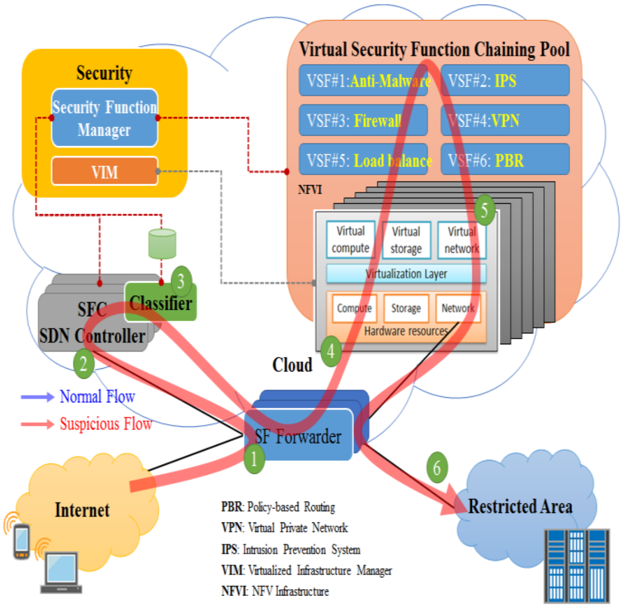

Fig. 5 The Security Service on-demand SFCs System

Figure 5 is an example to illustrate security service on-demand system architecture. To achieve the purpose of security service on-demand, first, we have to make relevant network security services into software. In this part, we utilizes Open Source to deploy and build required network security service and transfer these services into Virtual Service Function(VSF) templates; these VSFs can dynamically deployment of template into NFV infrastructure (NFVI) resources pool and make operation through virtualized calculation, storage and network resources. While the resources allocation of this resources pool management will be through Virtualized Infrastructure Manager (VIM) of Security Orchestrator. To realize flexible deployment of SFC, we need to determine the role of each VSF and its order through Security Function Manager. Once the order and applied rules are settled, SDN Controller will be notified and upgrading to fit the packet routing table of Service Function Forwarder (SFF), then leading every Flow respectively. Furthermore, to improve the recognition of traffic flow, we will set a Classifier matching with Controller end, to identify the property of traffic flow and help with SFC decision for Security Function Manager.

The operation procedure of the security service on-demand system is describe as follows.

(1) The packet from mobile devices will enter SFF for routing table query first, if the Flow entry is listed in forwarding table, then the corresponding packet transfer will start. SFF can be a standard OpenFlow Switch.
(2) If the Flow has no corresponding routing policy, then the packet will be transferred to SFC SDN Controller.
(3) At the moment, the SFC SDN Controller will make analysis on packet property by Classifier and then access decision database of Security Function Manager to update related information of this packet properties.
(4) If there is decision information of this Flow in decision database, the SFC SDN Controller will turn it into corresponding content of routing information and update forwarding table of SFF, to ensure that the flow can be leaded to corresponding service chain.
(5) Then the Flow will start designated SFC routing, since Security Function Manager has determined the corresponding SFC routing to the decision, every corresponding VSF can lead flows to next VSF after its processing to complete required service chains.
(6) After the Flow complete all demand service chains, SF Forwarder will lead Flow to the destination according its original destination location.

The steps above are the operation procedures of security service on-demand system. In addition, when any one of service chains is interrupted or abnormal, VSF will report to Security Function Manager and ask for decisions to SFC SDN Controller to deal with the direction of the Flow. Therefore a dynamic guiding mechanism of service chain can be realized. Meanwhile Security Function Manager can receive external orders itself, to make operations on SFC SDN Controller, to change real-time routing of the traffic flow. Except provide dynamic deployments on information security service chains against the Flow, Security Orchestrator also include the management mechanism of Security Function Manager, and its operation process is as follows:

(1) Security Function Manager will make judgment on current communication according to the updated information of packet property by Classifier, if any abnormality is spotted, it follows the decision policy to deployment service dynamically.
(2) Security Function Manager decides the categories and amount of VSF, if the amount is not correct with current deployment, VIM will be notified to make new deployment.
(3) After VIM receive the notice from Security Function Manager, it will load service template into NFVI resources pool and report related calculations, storage and network resources to Security Function Manager after service is initialized.
(4) Security Function Manager will check NFVI resource situation regularly, and make fine tuning on current VSF deployment according to NFVI status.

For example, an unknown traffic flow from mobile devices entering SF Forwarder, will be directed to SFC SDN Controller, if identified as Normal Flow by Classifier, it can directly enter restricted area to its destination; if identified as Suspicious Flow, then according to decisions, this Suspicious Flow will be directed to Virtual Security Function Chaining Pool for SFC routing. For example, if with services from IPS and Anti-Malware Detection, it will direct the Flow to the corresponding services orderly. If result turning normal, it will be redirected to the restricted area, and Classifier will be notified to mark this traffic flow as Normal Flow to avoid later traffic flow going through the SFC path. Therefore, besides meeting the requirements of security detection, it can also improve operation efficiency of network security system. Certainly, if the Flow has been identified as DDoS attack by Classifier, it will be under blocking in SF Forwarder and Security Function Manager will be notified to open load balance service to increase system availability. Moreover, the system can not only be established in networks with different sources and destinations, but also can be established in single network to operate customized network security service, which includes the defense from internet to intranet and security control from intranet to internet.

IV. Conclusions

The emergence of SDN, NFV and SFC presents the opportunity transformation ally improve cybersecurity. In this paper we design a security service on-demand architecture that combined SDN with NFV technology to achieve SFC operation. In our design, SFC enables various network functions to provide diversity security service for different users, reduce the overhead of the manual installation and the risk of service alert. Service providers can use this solution to build rapidly and flexible security services while simultaneously optimizing the usage of compute and networking resources.

Acknowledgment

The work described in this paper was supported in part by National Chung-Shan Institute of Science & Technology (Project No. NCSIST-A9I-V102).

References

[1] Zilole Simate, "Evaluation of mobile network security" , Information Science, Computing and Telecommunications (PACT), Pan African International Conference, Lusaka, pp.170-175, 2013.

[2] Openflow.org, 'OpenFlow » What is OpenFlow?', 2015. Available: http://www.OpenFlow.org/wp/learnmore/.

[3] F. Hu, Q. Hao, and K. Bao, ”Survey on Software-Defined Network and OpenFlow: From Concept to Implementation,” IEEE Communications Surveys & Tutorials, vol. 16, issue 4, pp. 2181 - 2206, May 2014.

[4] GENI. Available: http://groups.geni.net/geni

[5] Open Networking Foundation, Available : https://www.opennetworking.org.

[6] Open Networking Foundation, SDN in the Campus Environment, September 30, 2013.

[7] Open Networking Foundation, OpenFlow-enabled SDN and Network Functions Virtualization, February 2014.

[8] Jokin Garay, Jon Matias, Juanjo Unzilla and Eduardo Jacob, " Service description in the NFV revolution: Trends, challenges and a way forward" , IEEE Communications Magazine, Vol.54 , Issue 3, pp.68-74

[9] Laxmana Rao Battula, Freescale, Hyderabad, "Network Security Function Virtualization(NSFV) towards Cloud computing with NFV Over Openflow infrastructure: Challenges and novel approaches, " Advances in Computing, Communications and Informatics (ICACCI, 2014 International Conference, New Delhi, pp.1622-1628, Sept. 2014.

[10] Nathalie Omnes, Marc Bouillon ; Gael Fromentoux and Olivier Le Grand," A programmable and virtualized network & IT infrastructure for the internet of things: How can NFV & SDN help for facing the upcoming challenges" , 18th International Conference on Intelligence in Next Generation Networks

[11] Service Function Chaining (sfc). Available: https://datatracker.ietf.org/wg/sfc/documents/

[12] Source Packet Routing in Networking (spring). Available: https://datatracker.ietf.org/wg/spring/documents/

[13] Open Networking Foundation, SDN Architecture, Issue 1, ONF TR-502, June 2014.

[14] N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker and J. Turner, 'OpenFlow', SIGCOMM Comput. Commun. Rev., vol. 38, no. 2, p. 69, 2008.

[15] Problem Statement for Service Function Chaining, Available: https://tools.ietf.org/html/rfc7498#section-2

[16] Z. Duan, Z. Zhang, and Y. T. Hou, “Service Overlay Networks: SLAs, QoS, and Bandwidth Provisioning,” IEEE/ACM Trans. Net., vol. 11, 2003, pp. 870–83. T. Erl, SOA: Principles of Service Design, 1st ed., Prentice Hall, 2007.

[17] C. Pavlovski, “Service Delivery Platforms in Practice,” IEEE Commun. Mag., vol.45, no. 3, pp. 114–21, 2007

[18] S. Lee and S. Kang, 'NGSON: features, state of the art, and realiz ation', IEEE Communications Magazine, vol. 50, no. 1, pp. 54-61, 2012.

[19] F. Paganelli, M. Ulema and B. Martini, 'Context-aware service composition and delivery in NGSONs over SDN', IEEE Communications Magazine, vol. 52, no. 8, pp. 97-105, 2014.

[20] Ram Gopal Lakshmi Narayanan, "Software Defined Networks for Mobile Application Services." Software Defined Mobile Networks (SDMN): Beyond LTE Network Architecture, pp. 209-224, JUN. 2015