DOI: 10.19729/j.cnki.1673-5188.2018.04.003
http://kns.cnki.net/kcms/detail/34.1294.TN.20181113.0847.002.html, published online November 13, 2018

SDN Based Security Services

ZHANG Yunyong, XU Lei, and TAO Ye
(China Unicom, Beijing 100032, China)

Abstract

With the development and revolution of network in recent years, the scale and complexity of network have become big issues. Traditional hardware based network security solution has shown some significant disadvantages in cloud computing based Internet data centers (IDC), such as high cost and lack of flexibility. With the implementation of software defined networking (SDN), network security solution could be more flexible and efficient, such as SDN based firewall service and SDN based DDoS-attack mitigation service. Moreover, combined with cloud computing and SDN technology, network security services could be lighter-weighted, more flexible, and on-demanded. This paper analyzes some typical SDN based network security services, and provide a research on SDN based cloud security service (network security service pool) and its implementation in IDCs.

Keywords

SDN; network security; cloud security service

1 Introduction

The introducing of software defined networking (SDN) and network function virtualization (NFV) solution changes the network significantly: general hardware, virtualization software, and programmable services. With SDN and NFV, the network operation and maintenance cost is cut down, the utilization of resources is improved, the network flexibility is increased, and the time-to-market of new services is considerably decreased [1].

Therefore, SDN and NFV are considered as the innovation technology for telecommunications network evolution.

However, SDN and NFV also bring new security challenges for telecommunication networks. These new security challenges include:

- The physical security boundary becomes ambiguous, but the network is still protected by static-deployed security devices/appliances and passive security responses according to provisioned security policies, which leads to low-efficient security operation and maintenance, and delayed responses to security attacks [2].
- Network elements are created and deleted dynamically, but security policies cannot be updated accordingly because most security policies are updated by manual operations. Therefore, security management and protection could not be provided for network elements dynamically and automatically.
- SDN and NFV systems lack centralized security policy scheduling cross different devices and services from different vendors; no collaboration between devices always led to inconsistence of security policy.
- With virtualization, eastbound and westbound traffic flow information cross different virtual machines (VMs) may not be captured and analyzed since current security devices/appliances could not recognize those traffic flows. Thus, the current traffic monitoring and interception mechanisms do not apply to the virtualized system and the security view of the operator's network may not be provided.

Therefore, the static, passive, separate and manual operation of traditional security defense systems does not work for SDN/NFV networks. A dynamic, proactive, centralized and intelligent security management capability is needed.

The new framework shall utilize the key advantages of SDN/NFV technology, such as on-demand capacity scale-in/scale-out, virtualization, centralization, and decoupling the data and control planes. This new framework is a layered one and shall provide security orchestration, centralized and automated security policy management, and intelligent security analysis and response [3].

This paper analyzes the security challenges of SDN/NFV network to identify the requirements, defines a software-defined security framework, and then describes the functionalities of each module; finally the reference implementations are also provided.

The software-defined security framework may include the following components [4]:

- Security controller: A security controller is introduced to centralize and automatically control all the security devices,

to gather flow traffic information and system logs from them. The security controller also works as SDN/NFV applications; it interacts with the SDN controller and NFV management and orchestration (MANO) to achieve the flow scheduling and auto scaling of the virtualized security functions. New technology (such as big data and artificial intelligence) can be easily introduced to further improve the intelligence of the security controller [5].

- SDN network: The SDN controller offers flow scheduling function, whole network topology and traffic flow information to the security controller.
- NFV system: The NFV MANO provides virtual machine resources to the virtualized security function and the run-time status of these VMs.

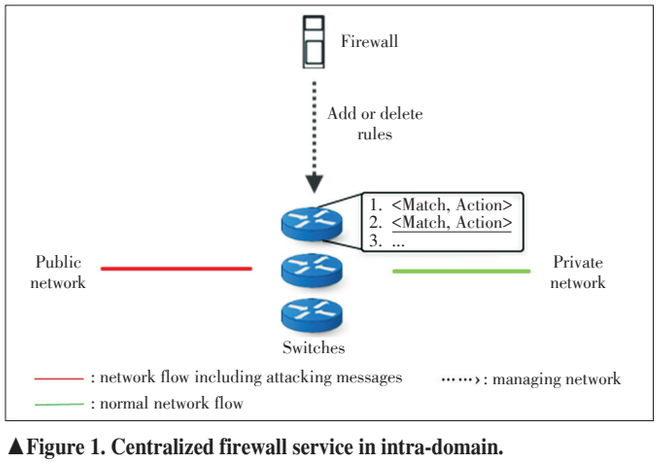
2 Typical SDN Based Security Services

2.1 SDN Based Firewall Service

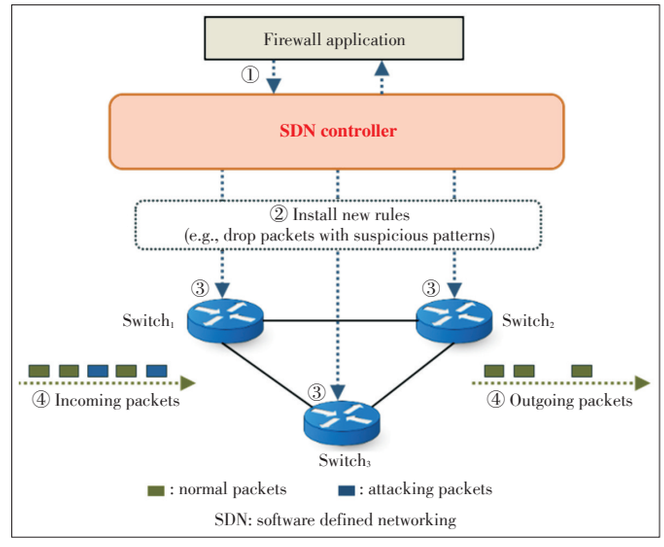
The SDN based firewall service is centralized and can manage network resources and manage firewall rules flexibly. As shown in **Fig. 1**, a SDN based centralized firewall management system could manage firewall rules and switches more flexible.

By using SDN controller, a packet-filtering strategy, which is issued by the firewall application (software or hardware), could be easily converted to a flow table through the controller. However, a protocol between the controller and switches (e.g., openflow and netconf) is only able to match up to the transmission control protocol (TCP) layer at present, and there is no corresponding field to set the identification information of data packets above the TCP layer. Therefore, it cannot be achieved to identify the information above the TCP layer firewall strategy without changing the protocol [6].

Fig. 2 shows an example scenario of centralized firewall service for switches and the process of filtering the attacking network messages through this security system. This scenario concentrates on SDN switches and shows that how a user can manage a centralized firewall service.



▲Figure 1. Centralized firewall service in intra-domain.



▲Figure 2. An example scenario of centralized firewall service.

As a precondition for this scenario, a security manager should specify a new policy to firewall application when the information about a new attacking network message is recognized. In order to prevent packets from including this attacking network messages, the user adds the new policy to the firewall application running on top of the SDN controller.

The process includes four steps:

- Step 1: A firewall application (could be software or hardware) should specify new security policies when the attacking network messages is warned. And these new policies could be added to the SDN controller.
- Step 2: A new flow entry might be distributed to each switch by a SDN controller after installing it. Therefore, the SDN controller sends a flow insert operation that contains the rules (e.g., "drop packets with the attacking network messages file") to all the SDN switches.

The reported new attacking network messages is either a known attacking network messages or a "zero-day" attacking network messages. As for a known attacking network messages, some mechanisms such as "signatures" and "thumbprints" are developed for firewall service to detect and defend it. However, for a "zero-day" attacking network messages, it should be scanned and detected before any countermeasure is applied to defend it. Attacking network messages deliver malicious payloads that could exploit some vulnerable applications or services. Those attacking network messages might be detected by inspecting the packet payload.

- Step 3: An SDN switch adds a flow entry dropping future packets with the attacking network messages file to its flow table when receiving the flow insert operation about the attacking network messages file. After that, the SDN switch can drop the packets with the attacking network messages file.
- Step 4: When receiving any packets with attacking network

messages file, an SDN switch completely drops the packets. Any packets with attacking network messages files cannot be passed to the switches under the applied rules.

When an SDN switch receives a type of packet that it has not processed before, it deletes this packet and sends a report to the controller about this kind of packets. The controller analyzes whether this is an attack. If this is an attack, the controller sends a message to the firewall application and Step 1 will be executed. If not, the controller keeps a regular flow entry to tell the switches how to handle this sequence of afterwards packets.

2.2 SDN Based Honeypot Service

The SDN-based centralized honeypot can manage honeypot places. As shown in **Fig. 3**, a centralized honeypot manages switches and new routing paths to the honeypots to attract attackers to a place used as a trap. The honeypot is configured as the intended attack target and reports the collected information to the centralized honeypot service [7].

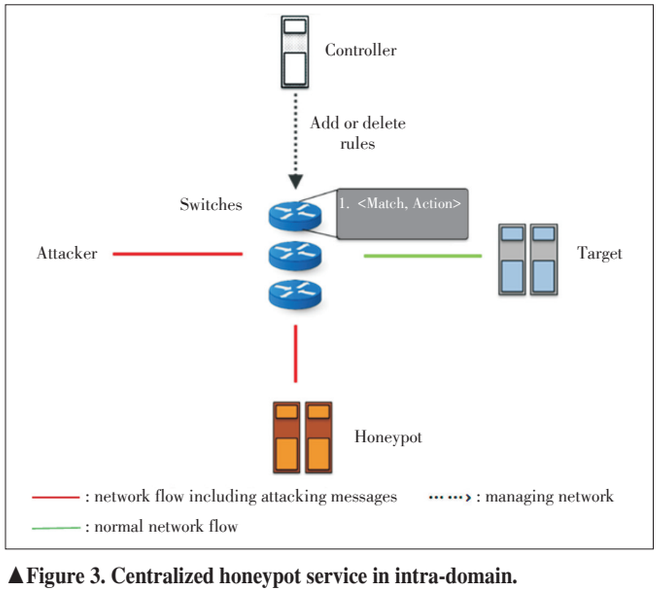
Fig. 4 shows a centralized honeypot service for switches. Adding a routing path to a honeypot scenario shows that how a security manager can use a centralized honeypot system. This scenario concentrates on SDN switches.

The process of adding a routing path to a honeypot instead of the actual target includes four steps as follows:

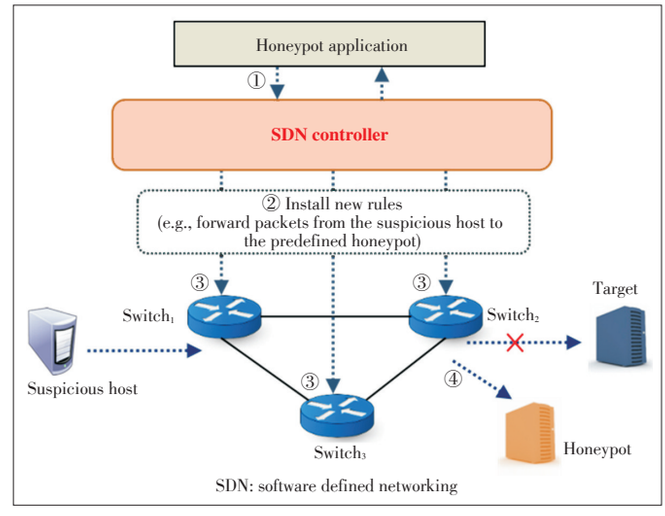
- Step 1: A honeypot application installs new rules to the SDN controller

A honeypot application should specify new rules when the information about a suspicious host is reported. In order to monitor the traffic from the suspicious host, the new rules (e.g., "forward packets from the suspicious host to a honeypot") is added to the SDN controller by honeypot application running on top of the SDN controller.

- Step 2: The SDN controller distributes new rules to appropriate SDN switches



▲Figure 3. Centralized honeypot service in intra-domain.



▲Figure 4. An example scenario for centralized honeypot service.

The new rules might be distributed to each switch by the SDN controller after installing it. Therefore, the SDN controller sends a flow insert operation that contains the rule (e.g., "forward packets from the suspicious host to a honeypot") to all the SDN switches.

- Step 3: All the SDN switches apply the new rules into their flow tables.

All the SDN switches add a flow entry forwarding future packets from the suspicious host to a honeypot to their flow tables when receiving the flow insert operation about the suspicious host. After that, the SDN switch can forward the packets from the suspicious host to a honeypot.

- Step 4: An SDN switch executes the new rules to support honeypot service

When receiving any packets from the suspicious host, an SDN switch forwards the packets to a honeypot. In this way, any packets from the suspicious host cannot be passed to an actual target host switch under the applied rules. The forwarded packets are collected in the honeypot.

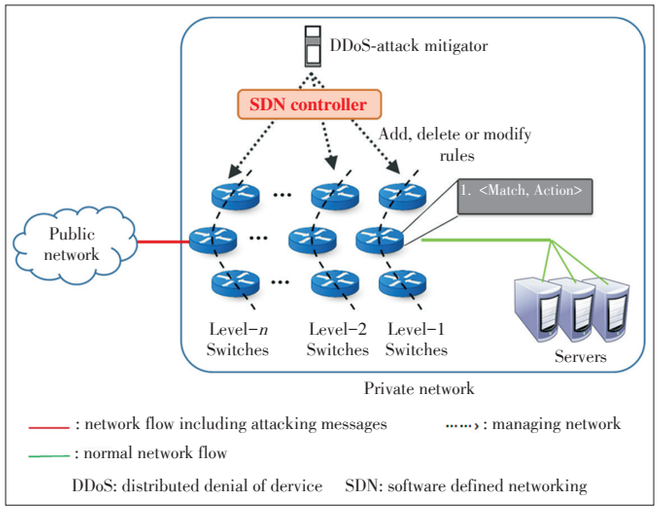
2.3 SDN Based DDoS-Attack Mitigation Service

Fig. 5 shows a centralized distributed denial of service attack (DDoSattack) mitigation service. This service adds, deletes or modifies rules to each switch. Unlike the centralized firewall service, this service is mainly on the inter-domain level.

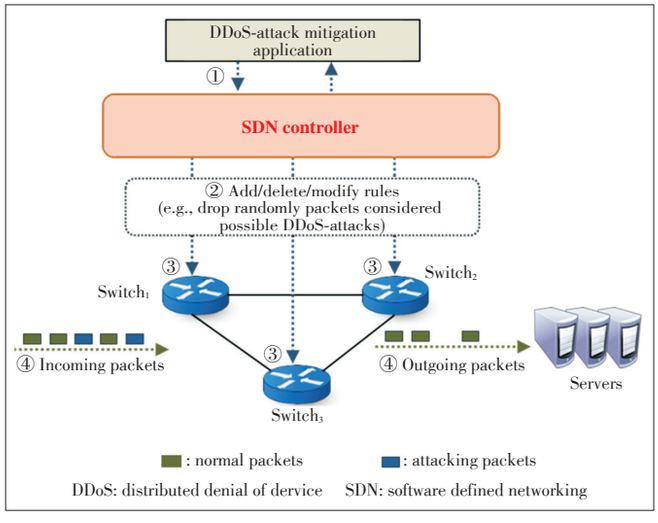
Fig. 6 shows an example scenario of centralized DDoS-attack mitigation for stateless servers. The process against Domain Name Services (DNS) DDoS attacks include four steps as follows.

- Step 1: A mitigation application installs new rules to SDN controller

A DDoS-attack mitigation application should specify new rules when a new DDoS-attack is detected. In order to prevent



▲Figure 5. Centralized DDoS-attack mitigation service in inter-domain.



▲Figure 6. An example scenario for centralized DDoS-attack mitigation for stateless servers.

packets from reaching servers to waste the servers' resources, the new rule (e.g., "drop DDoS-attack packets randomly with some probability") is added to the SDN controller. This rule addition is performed by DDoS-attack mitigation application running on top of the SDN controller.

- Step 2: An SDN controller distributes new rules to appropriate switches

The new rules might be distributed to each switch by a SDN controller after installing it. Therefore, the SDN controller sends a flow insert operation that contains the rule (e.g., "drop randomly packets considered DDoS attacks with a certain probability") to all the SDN switches.

- Step 3: All the SDN switches apply new rules into their flow tables

All the SDN switches add a flow entry to their flow tables for dropping the packets in a DDoS-attack when receiving the flow insert operation about the DDoS-attack mitigation. After that, the SDN switch can drop these packets with a probability proportional to the DDoS-attack severity.

- Step 4: An SDN switch executes new rules to mitigate DDoS-attacks

An SDN switch completely drops the packets selected when receiving any packets in a DDoS-attack.

Fig. 7 shows an example scenario where the SDN controller can manage a centralized DDoS-attack mitigation.

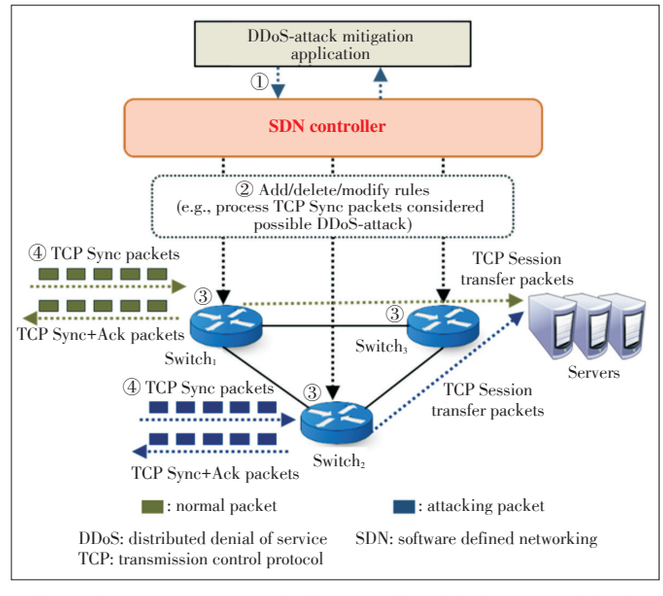
- Step 1: A mitigation application installs new rules to the SDN controller

A DDoS-attack mitigation application should select the switch that performs the role of proxy for TCP service. New rule addition is performed by DDoS-attack mitigation application running on top of the SDN controller.

- Step 2: A SDN controller distributes new rules to appropriate switches

The installed new rules might be distributed to appropriate switches for DDoS attack mitigation by an SDN controller. The SDN controller then sends a flow insert operation that contains the rule (e.g., "generate TCP Sync+Ack for packets considered DDoS attacks") to all the SDN switches. Therefore, a new rule is installed into the selected switch so that it can generate TCP Sync-Ack packets for TCP Sync as request. If the same requests arrive much more frequently than the expected rate, the SDN controller selects a new switch to serve the role of server. For the normal TCP Sync, the switch transfers the TCP session to the corresponding server in the private network. It can also be managed centrally by the SDN controller such that a security manager can determine security policies for their services.

- Step 3: All the SDN switches apply the new rule into their flow tables



▲Figure 7. An example scenario for centralized DDoS-attack mitigation for stateful servers.

All the SDN switches add a flow entry to their flow tables for dropping future packets in any DDoS-attacks when receiving the flow insert operation about the DDoS attacks. After that, the SDN switch can generate TCP Sync-Ack packets with a probability proportional to the DDoS-attack severity.

- Step 4: An SDN switch executes the new rule to mitigate DDoS-attacks

An SDN switch completely responds to TCP Sync packets from an adversary host randomly when receiving DDoS-attack packets. DDoS-attack requests for stateful servers are handled by the switches instead of actual servers.

3 SDN Based Cloud Security Services

With the implementation of SDN, network security service could be more flexible and efficient. As shown in **Fig. 8**, the SDN based cloud security service solution has two main system modules: the SDN based security controller and security service pool [8].

The SDN based security controller provides security for service network control and VNFs management. Based on the SDN controller and cloud computing platform, this module implements SDN based security control, secure VNF and service management, cloud service customer (CSC) management, and service-level agreement (SLA) monitoring [9].

Based on virtualization and NFV technology, the security service pool is implemented with multiple network security VNF or simply integrated with third-party security software with open API. The security resource pool is a combination of original physical security devices (hardware boxes such as firewall, web application firewall (WAF), intrusion prevention system (IPS)) and virtual security devices (such as virtual firewall, virtual wireless application protocol (WAP), and virtual IPS). These devices are abstracted with basic features and unified interface, so that the security controller can orchestrate these security functions, set security policies to them, and obtain flow traffic information from them [10].

Compared with traditional hardware-based network security solutions, SDN based cloud security services have several advantages such as multiple service types and more flexible functions in future networks, Internet data center (IDC) and cloud computing platforms.

Benefited from NFV technology, the security service pool could provide multiple virtual security resources, with lower cost and fewer hardware resources. Many small- and medium-size IDC providers only implement minimized security function, which could only provide basic security functions such as firewall and anti-DDoS devices, due to the high cost of security hardware. With the implementation of security service pool, the IDC provider could provide more types of security services with lower cost, while the security of IDC and tenant network is also enhanced.

Based on the SDN and cloud computing technology, the security controller could bring more flexible security service functions. Security resources could be provided and modified on demand. The service function chain could provide CSC private security network. Security resources could automatically migrate with the migration of tenant network and resources.

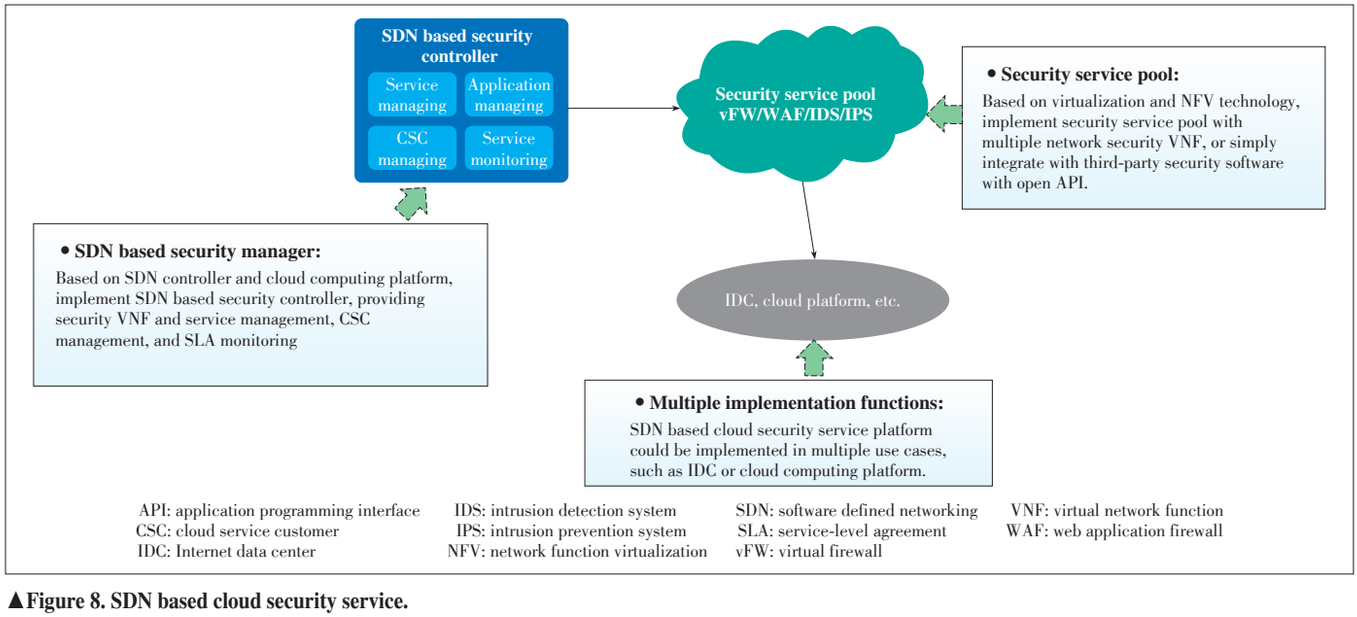
Fig. 9 defines a process of SDN based cloud security service to the CSC, which include the following three steps.

- Step 1: CSC requests cloud security services

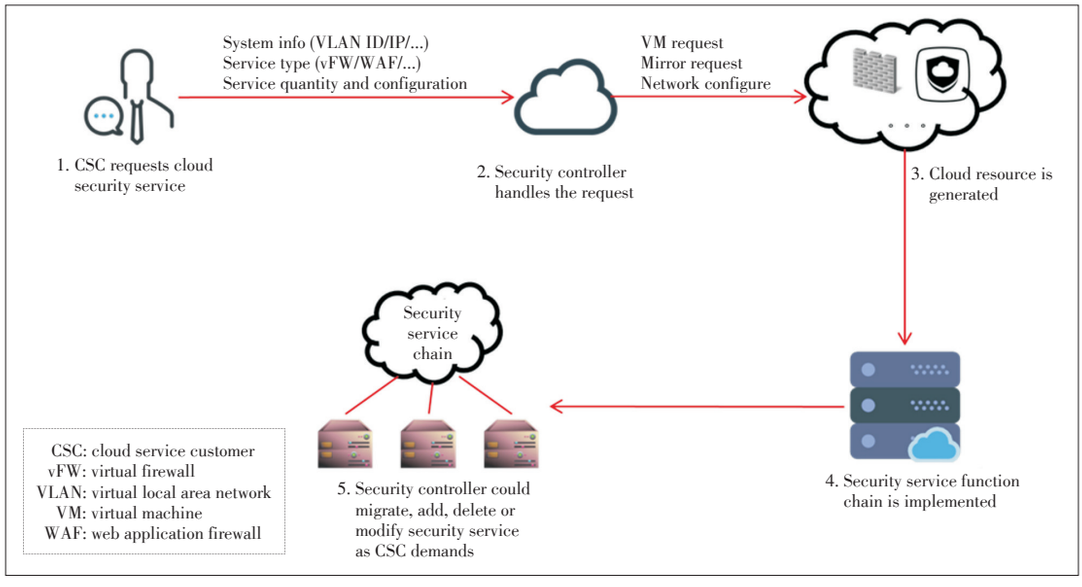
CSC could request cloud security services with the system information (such as VLAN id, and IP), service type (such as vFW and WAF), and service quantity and configuration.

- Step 2: Security controller handles the request

Configuring the CSC request (with some necessary identifi-



▲Figure 8. SDN based cloud security service.



◀**Figure 9. Process of SDN based cloud security service.**

cation methods), the security controller could handle the request and send another request for the basic cloud resource (VM, cloud mirror type, network configuration, etc.) to the cloud management platform.

• Step 3: Cloud resource generation and service function chain implementation

The cloud management platform handles the request, generates the resource, and then sends the resource information back to the security controller. The controller implements the security function chain with the demands of CSC.

4 Conclusions

With the development of new network technology such as SDN and NFV, network security faces some new challenges, threats, but also opportunities. Combining and implementing SDN and traditional network security functions could bring more flexible, efficient, lower cost network security services to the end customers. As the new Information and communication technology (ICT) technologies such as 5G and artificial intelligence (AI) are being implemented in the Internet and IDC, more network and information security challenges would rise up. Therefore, implementing new ICT technology in security industry would be a new trend [11].

References

[1] J. Carapinha, P. Feil, P. Weissmann, et al., "Network virtualization–opportunities and challenges for operators," in *Future Internet - FIS* 2010, J. Carapinha, P. Feil, P. Weissmann, et al. eds. Berlin/Heidelberg, Germany: Springer Berlin Heidelberg, 2010, pp. 138–147.

[2] D. A. Joseph, A. Tavakoli, and I. Stoica, "A policy-aware switching layer for data centers," in *Proc. ACM SIGCOMM* 2008 *Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications*, Seattle, USA. 2008, pp. 51–62. doi:10.1145/1402958.1402966.

[3] *Security Requirements and Reference Architecture for Software-Defined Networking*, ITU-T X.1038, Oct. 2016.

[4] *Service Function Chaining (SFC) Architecture*, IETF RFC 7665, Oct. 2015.

[5] Z. Y. Hu, M. W. Wang, X. Q. Yan, et al., "A comprehensive security architecture for SDN," in *IEEE 18th International Conference on Intelligence in Next Generation Networks*, Paris, France, 2015, pp. 30–37. doi:10.1109/ICIN.2015.7073803.

[6] *Security Services Using the Software-Defined Networking*, ITU-T X.1042, Sept. 2018.

[7] R. Bifulco and G. Karame G, "Towards a richer set of services in software-defined networks," in *2014 Workshop on Security of Emerging Networking Technologies*, San Diego, USA, 2014. doi:10.14722/sent.2014.23006.

[8] *Functional Requirements of Software-Defined Networking*, ITU-T Y.3301, Sept. 2016.

[9] *Security Framework for Cloud Computing*, ITU-T X.1601, Oct. 2015.

[10] *Security Requirements for Software as a Service Application Environments*, ITU-T X.1602, Mar. 2016.

[11] *Functional Architecture of Software-Defined Networking*, ITU-T Y.3302, Jan. 2017.

Manuscript received: 2018-07-01

Biographies

ZHANG Yunyong (zhangyy@chiaunicom.cn) serves as President of China Unicom Research Institute, Vice President of the Ministry of Industry and Information Technology SDN Industry Alliance, China, Vice President of the Technical Committee for New Prominent Forum in China Institute of Telecommunications. He is also a professor-level senior engineer, outstanding member of China Computer Federation, member of the 13th National Committee of CPPCC, national candidate for the Project of Millions of Talents. He was awarded the State Department Special Allowance and the title of "China's Middle-aged and Young Experts with Outstanding Contributions". He has achieved 64 authorized patents and 37 software copyrights.

XU Lei (xulei56@chinaunicom.cn) is a manager of cloud computing with China Unicom Research Institute. His research interests include cloud computing, SDN/NFV, and information security. He has achieved 20 authorized patents and 20 software copyrights. He is an editor of very first worldwide ITU cloud computing standards.

TAO Ye (taoy10@chinaunicom.cn) is the director of the Cloud Security Research Group of China Unicom Research Institute. His research interests include information security, network security, SDN/NFV security, and anti-telecom fraud. He has achieved 10 authorized patents and 10 software copyrights. He is the chief-editor of 2 published ITU standards.