SDN-based Security Services using Interface to Network Security Functions

Jinyong Kim*, Mahdi Daghmehchi*, 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: {wlsdyd0930,mdaghmechi,pauljeong,hyoung}@skku.edu, pjs@etri.re.kr

***Abstract*—This paper proposes a framework for security services using Software-Defined Networking (SDN) and Interface to Network Security Functions (I2NSF). It specifies requirements for such a framework for security services based on network virtualization. It describes two representative security services, such as (i) centralized firewall and (ii) DDoS-attack mitigation systems. For each service, this paper discusses the limitations of existing systems and presents a possible SDN-based system to protect network resources by controlling suspicious and dangerous network traffic.**

I. Introduction

Software-Defined Networking (SDN) is a set of techniques that enables users to directly program, orchestrate, control and manage network resources through software (e.g., SDN applications). It relocates the control of network resources to a dedicated network element, namely SDN controller. The SDN controller uses the interface and arbitrates the control of network resources in a logically centralized manner. It also manages and configures the distributed network resources and provides and abstracted view of the network resources to the SDN applications. The SDN application can customize and automate the operations (including management) of the abstracted network resources in a programmable manner via this interface [1]–[5].

Due to the increase of sophisticated network attacks, the legacy security services become difficult to cope with such network attacks in an autonomous manner. SDN has been introduced to make networks more controllable and manageable, and this SDN technology will be promising to autonomously deal with such network attacks in a prompt manner. By this trend, this paper describes a framework, objectives and requirements to support the protection of network resources through SDN-based security services using a common interface to Network Security Functions (NSF) [6]. It uses an interface to NSF (I2NSF) for such SDN-based security services that are performed in virtual machines through network functions virtualization [7]. Also this paer addresses the challenges of the existing systems for security services. As feasible solutions to handle these challenges, this paper proposes two use cases of the security services, such as centralized firewall system and centralized DDoS-attack mitigation system.

For the centralized firewall system, this paper raises limitations in legacy firewalls in terms of flexibility and administration costs. Since in many cases, access control management for firewall is manually performed, it is difficult to add the access control policy rules corresponding to new network attacks in a prompt and autonomous manner. Thus, this situation requires expensive administration costs. This paper introduces a use case of SDN-based firewall system to overcome these limitations. For the centralized DDoS-attack mitigation system, this paper raises limitations in legacy DDoS-attack mitigation techniques in terms of flexibility and administration costs. Since in many cases, network configuration for the mitigation is manually performed, it is difficult to dynamically configure network devices to limit and control suspicious network traffic for DDoS attacks. This paper introduces a use case of SDN-based DDoS-attack mitigation system to provide an autonomous and prompt configuration for suspicious network traffic. Note that this paper is the enhanced version of our early paper [5] and IETF Internet draft [8].

The rest of this paper is organized as follows: Section II formulates our SDN-based security services. Section III suggests two representative examples as SDN-based security services. Section IV addresses challenging research issuses. We finally conclude this paper along with future work in Section V.

II. Overview

This section describes the referenced architecture to support SDN- based security services, such as centralized firewall system and centralized DDoS-attack mitigation system. Also, it describes a framework for SDN-based security services using I2NSF.

Fig. 1 shows a framework for SDN-based security services. As shown in the figure, applications for security services (e.g., firewall and DDoS-attack mitigation) run on the top of an SDN controller [1], [2]. When an administrator enforces security policies for the security services through an application interface, the SDN controller generates the corresponding access control policy rules (or network configuration) 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. 2 shows a framework to support SDN-based security services using I2NSF [6]. As shown in Fig. 2, client and application gateway (AppGW) can use security services with their high-level security policies through security controller. Security controller calls function-level security services via Capability Layer Interface, which are performed by security applications, running on top of virtual machines

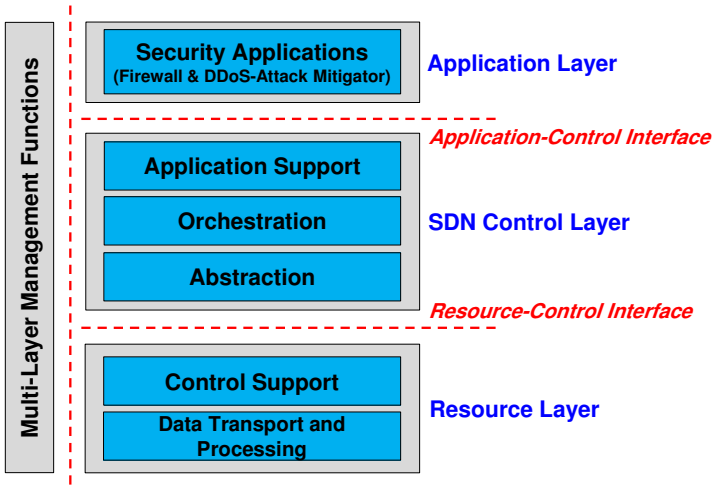

Fig. 1. High-level Architecture for SDN-based Security Services

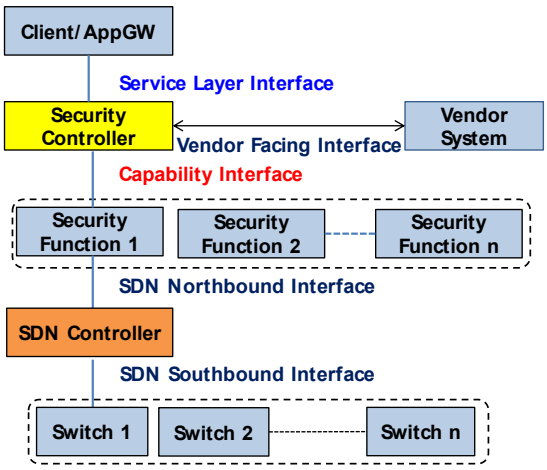

Fig. 2. A Framework for SDN-based Security Service using I2NSF

through NFV [7]. Security application asks SDN controller to perform its required security functions on switches under the supervision of SDN controller. Finally, SDN Controller sets up forwarding rules for the security services on Switches via SDN Southbound Interface. NSF facing interface between security controller and security applications can be implemented by Network Configuration Protocol [9] with a data modeling language called YANG [10] that describes function-level security services.

A. Objectives

We have the following objectives for SDN-based security services:

1) Prompt reaction to new network attacks: SDN-based security services should allow private networks to defend themselves against new sophisticated network attacks.
2) Autonomous defense from network attacks: SDN-based security services should identify the category of network attack (e.g., worms and DDoS attacks) and take counteraction for the defense without the intervention of network administrators.
3) Network-load-aware resource allocation: SDN-based security services should measure the overhead of resources for security services and dynamically select resources considering load balance for the maximum network performance.

B. Requirements

SDN-based security services provide dynamic and flexible network resource management to mitigate network attacks, such as malicious traffic and DDoS attacks. In order to support this capability, the requirements for SDN-based security services are described as follows:

1) SDN-based security services are required to support the programmability of network resources to mitigate network attacks.
2) SDN-based security services are required to support the orchestration of network resources and SDN applications to mitigate network attacks.
3) SDN-based security services are required to provide an application interface allowing the management of access control policies in an autonomous and prompt manner.
4) SDN-based security services are required to provide a resource-control interface for control of network resources to mitigate network attacks.
5) SDN-based security services are required to provide the logically centralized control of network resources to mitigate network attacks.

III. Examples of SDN-based Security Services

This section introduces two representative security services based on SDN: (i) centralized firewall system and (ii) centralized DDoS-attack mitigation system.

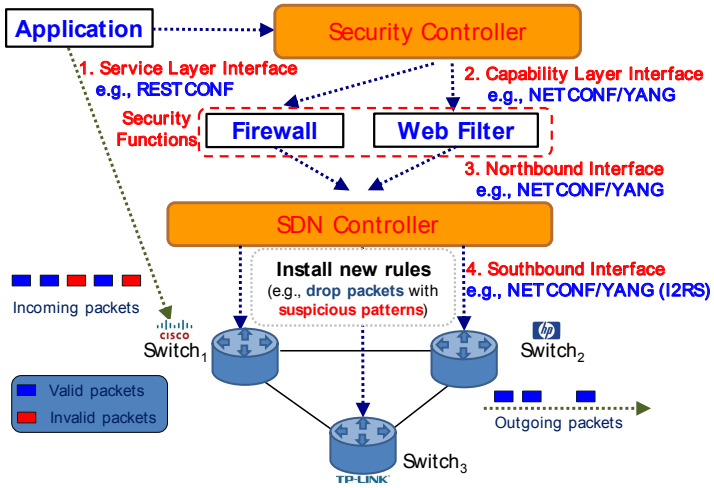

Fig. 3. Procedure of firewall operation in our centralized firewall system

A. Centralized Firewall System

For the centralized firewall system, a centralized network firewall can manage each network resources and firewall rules can be managed flexibly by centralized server. The centralized network firewall manages each switches and firewall rules can

be added or deleted. Fig. 3 shows the procedure of firewall operations in our centralized firewall system as follows:

1) Application asks for security services with high-level security policies to Security Controller via Service Layer Interface (e.g., RESTCONF).
2) Security Controller calls function-level security services via Capability Layer Interface (e.g., NETCONF/YANG).
3) Security Functions (e.g., firewall and web filter) tells SDN Controller its required Security services via Northbound Interface (e.g., NETCONF/YANG).
4) SDN Controller installs new rules (e.g., drop packets with the suspicious pattern) for the security services into Switches via Southbound Interfae (e.g., NETCONF/YANG).

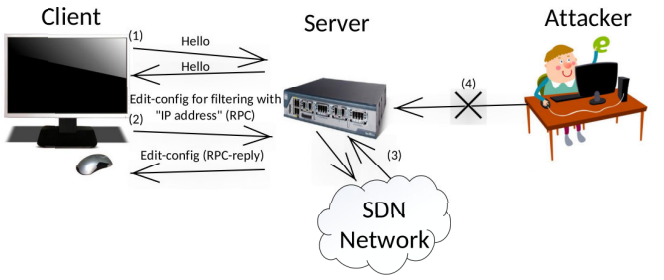

Fig. 4. Procedure for SDN-based Firewall Filtering

For the above centralized firewall system, the existing SDN protocols can be used through NETCONF/YANG between the firewall application and switches [1], [2], [4], [11]. Fig. 4 shows procedure for SDN-based Firewall Filtering as follows:

1) Client and Server make a session by using NETCONF/YANG.
2) Client configures the firewall table of Server to block specific IP addresses.
3) Server (i.e., security function in virtual machine) asks firewall filtering to be set up in Network Switch through SDN Controller
4) After the configuration of the firewall table, packets from an attacker are dropped down

Legacy firewalls have some challenges such as the expensive cost, performance, management of access control, establishment of policy, and packet-based access mechanism. The Proposed framework can resolve these challenges through the above centralized firewall system based on SDN as follows.

- Cost: The cost of adding firewalls to network resources such as routers, gateways, and switches is substantial due to the reason that we need to add firewall on each network resource. To solve this, each network resource can be managed centrally such that a single firewall is manipulated by a centralized server.
- Performance: The performance of firewalls is often slower than the link speed of their network interfaces. Every network resource needs to check firewall rules according to network conditions. Firewalls can be adaptively deployed, depending on network conditions in our framework.
- The management of access control: Since there may be hundreds of network resources in an administered network, the dynamic management of access control for security services like firewall is a challenge. In our framework, firewall rules can be dynamically added for new network attacks.
- The establishment of policy: Policy should be established for each network resource. However, it is difficult to describe what flows are permitted or denied within a specific organization network under management. Thus, a centralized view is helpful to determine security policies for such a network.
- Packet-based access mechanism: Packet-based access mechanism is not enough in practice since the basic unit of access control is usually users or applications. Therefore, application level rules can be defined and added to the firewall system through the centralized server.

B. Centralized DDoS-attack Mitigation System

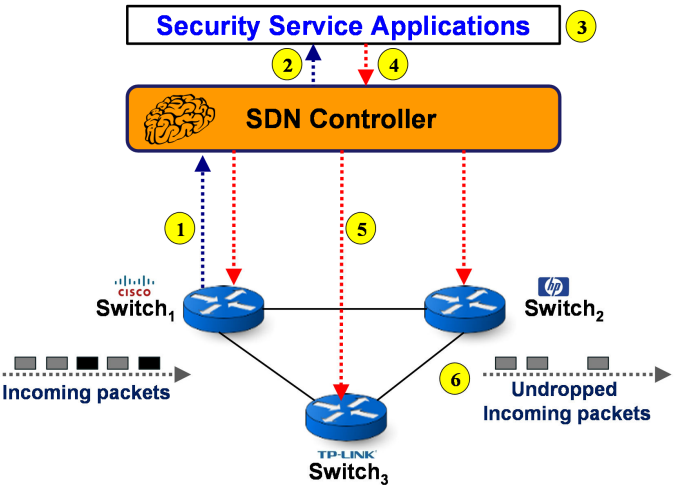

Fig. 5. Procedure of DDoS-attack mitigation operation in our centralized DDoS-attack mitigation system

For the centralized DDoS-attack mitigation system, a DDoS-attack mitigation system can add, delete or modify rules to each switch. The centralized DDoS-attack mitigation system defends servers against DDoS attacks outside private network, that is, from public network. Fig. 5 shows the procedure of DDoS-attack mitigation operations in our centralized DDoS-attack mitigation system as follows:

1) $Switch_1$ periodically reports an inter-arrival pattern of a flows packets to SDN Controller.
2) SDN Controller forwards the flows inter-arrival pattern to an appropriate security service application, such as DDoS-Attack Mitigator.
3) DDoS-Attack Mitigator analyzes the reported pattern for the flow.
4) If DDoS-Attack Mitigator regards the pattern as a DDoS attack, it computes a packet dropping probability corresponding to suspiciousness level and reports this DDoS-attack flow to SDN Controller.

5) SDN Controller installs new rules into switches (e.g., forward packets with the suspicious inter-arrival pattern with a dropping probability).
6) The suspicious flows packets are randomly dropped by switches with the dropping probability.

The servers are categorized into stateless servers (e.g., DNS servers) and stateful servers (e.g., web servers). In a DDoS-attack mitigation system in a private network, switches are configured in multi-levels to provide the dynamic defense lines against a variety of DDoS attacks. The centralized DDoS-attack mitigation system has the same challenges with the centralized firewall system, as discussed in Section III-A.

IV. Research Issues

In this section, we discuss further research issues for SDN-based security services. We have the following research issues:

- To prevent unauthorized control of switches, a secure and authenticated channel between SDN controller and switches should be established. That is, we need to consider a proper key management for secure communication between them.
- Inherently, a centralized server (i.e., SDN controller) will suffer from a single point of failure and/or compromise. Without the protection of SDN controller, it is not possible to deploy SDN-based security services.
- To support the SDN-based security services, we need to consider changes in existing SDN switches and protocols. For example, deep packet inspection should be provided in SDN switches to reduce performance degradation.
- In theory, SDN seems a reasonable architecture to provide centralized security services. However, when we consider many switches and hosts, the communication between SDN controller and switches becomes a potential bottleneck, so scalability issue should be addressed.
- To support security services in an autonomous and scalable fashion, switches should have some intelligence to perform decision-making for security attacks. Thus, it is an important issue to how much intelligence switches should have in terms of performance and autonomy.
- Eficient interfaces to network security functions should be implemented by NETCONF/YANG in network virtualization environments such that SDN switches can be fast configured according to required security services. This is possible by the efficient interaction between Security Controller and SDN Controller.

V. Conclusion

In this paper, we proposed a framework for security services based on Software-Defined Networking and Interface to Network Security Functions. Based on this framework, we suggested two representative security services, such as firewall and DDoS-attack mitigator. As future work, we will develop our proposed framework in Mininet [12] and investigate other security services, such as encryption/decryption, junk mail filtering, and anti-spam service.

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 MSIP/IITP [R0166-15-1041, Standard Development of Network Security based SDN]. Note that Jaehoon (Paul) Jeong is the corresponding author.

References

[1] Recommendation ITU-T Y.3300, "Framework of Software-Defined Networking," *ITU-T*, Jun. 2014.

[2] Open Networking Foundation, "SDN Architecture," *ONF*, Jun. 2014.

[3] H. Kim and N. Feamster, "Improving Network Management with Software Defined Networking," *IEEE Communications Magazine*, vol. 51, no. 2, pp. 114–119, Feb. 2013.

[4] Open Networking Foundation, "OpenFlow Switch Specification (Version 1.4.0)," *ONF*, Oct. 2013.

[5] J. Jeong, H. Kim, and J. Park, "A Framework for Security Services based on Software-Defined Networking," *DC2*, Mar. 2015.

[6] E. Lopez, D. Lopez, L. Dunbar, X. Zhuang, J. Parrott, R. Krishnan, and S. Durbha, "Framework for Interface to Network Security Functions," *IETF draft-merged-i2nsf-framework-02*, Jun. 2015.

[7] ETSI-NFV, "Network Functions Virtualisation (NFV) ; Architectural Framework," *ETSI*, Oct. 2013.

[8] J. Jeong, H. Kim, and J. Park, "Requirements for Security Services based on Software-Defined Networking," *IETF draft-jeong-i2nsf-sdn-security-services-02*, Jul. 2015.

[9] R. Enns, M. Bjorklund, J. Schoenwaelder, and A. Bierman, "Network Configuration Protocol (NETCONF)," *IETF RFC 6241*, Jun. 2011.

[10] M. Bjorklund, "YANG - A Data Modeling Language for the Network Configuration Protocol (NETCONF)," *IETF RFC 6020*, Oct. 2010.

[11] M. Boucadair and C. Jacquenet, "Software-Defined Networking: A Perspective from within a Service Provider Environment," *RFC 7149*, Mar. 2014.

[12] Mininet, "An instant virtual network on your laptop," http://mininet.org.