A Framework for Security Services based on Software-Defined Networking

Jaehoon (Paul) Jeong*, Jihyeok Seo†, Geumhwan Cho†, Hyoungshick Kim†, and Jung-Soo Park‡
* Department of Interaction Science, Sungkyunkwan University, Republic of Korea
† Department of Computer Science & Engineering, Sungkyunkwan University, Republic of Korea
‡ Electronics and Telecommunications Research Institute, Republic of Korea
Email: {pauljeong,seojh43,geumhwan,hyoung}@skku.edu, pjs@etri.re.kr

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

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. Also, it manages the distributed network resources and provides the abstracted view of the network resources for 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]–[4].

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 raises requirements to support the protection of network resources by using security services based on SDN. Also, 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 that can be regarded as 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 IETF Internet draft [5].

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

II. Problem Formulation

This section describes the referenced architecture to support SDN-based security services, such as centralized firewall system and centralized DDoS-attack mitigation system.

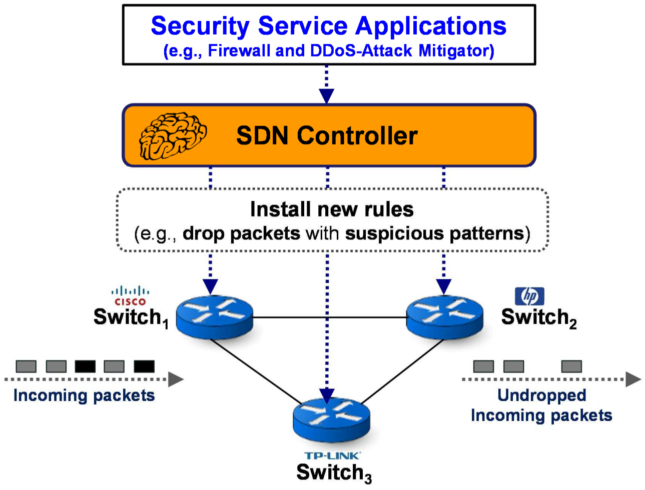
Security Service Applications
(e.g., Firewall and DDoS-Attack Mitigator)
SDN Controller
Install new rules
(e.g., drop packets with suspicious patterns)
CISCO
Switch$_1$
Switch$_2$
TP-LINK
Switch$_3$
Incoming packets
Undropped
Incoming packets

Fig. 1. A Framework for SDN-based Security Services

Fig. 2 shows a framework for SDN-based security services. As shown in the figure, applications for security services (e.g., firewall and DDoS-attack mitigator) 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

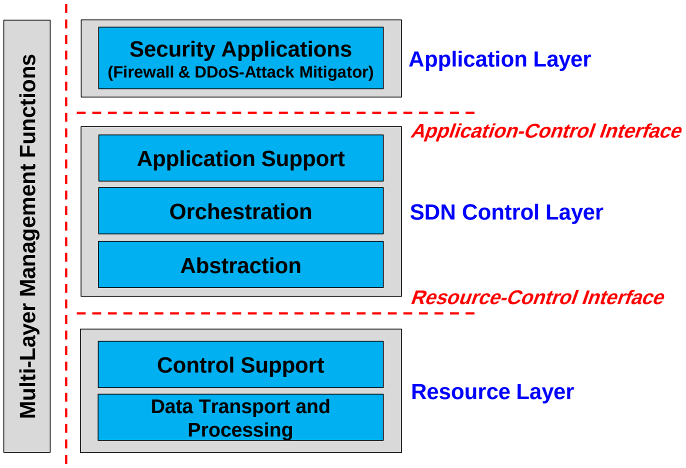
Multi-Layer Management Functions
Security Applications
(Firewall & DDoS-Attack Mitigator)
Application Layer
Application-Control Interface
Application Support
Orchestration
Abstraction
SDN Control Layer
Resource-Control Interface
Control Support
Data Transport and Processing
Resource Layer

Fig. 2. High-level Architecture for SDN-based Security Services

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 our high-level architecture for SDN-based security services. In this paper, we specify the interaction among security service applications, SDN controllers, and switches through interfaces (i.e., application-control interface and resource-control interface).

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

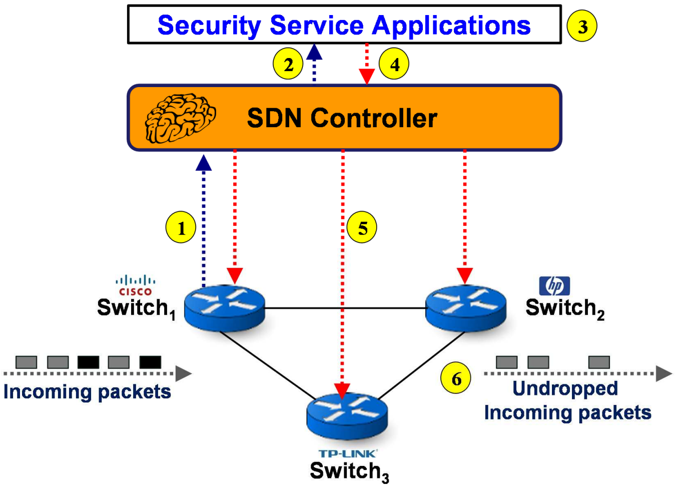

Fig. 3. SDN-based Security Services

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.

A. Centralized Firewall System

For the centralized firewall system, a centralized network firewall can manage each network resource and firewall rules can be managed flexibly by a centralized server. That is, the centralized network firewall controls each switch for the network source managenent and the firewall rules can be added or deleted dynamically. Fig. 3 shows the procedure of firewall operations in our centralized firewall system as follows:

1) $Switch_1$ forwards an unknown flow's packet to SDN Controller.
2) SDN Controller forwards the unknown flow's packet to an appropriate security service application, such as Firewall.
3) Firewall analyzes the headers and contents of the packet.
4) If Firewall regards the packet as a malware's packet with a suspicious pattern, it reports the malware's packet to SDN Controller.
5) SDN Controller installs new rules (e.g., drop packets with the suspicious pattern) into switches.
6) The malware's packets are dropped by switches.

Legacy firewalls have some challenges such as the expensive cost, performance, management of access control, establishment of policy, and packet-based access mechanism. These challenges can be resolved through the centralized firewall system based on SDN that is proposed in this paper. This is because firewall rules can be managed flexibly by a centralized server that analyzes the network traffic in real time. These challenges for firewalls can be resolved by our framework 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:** Sine 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.

Note that the existing SDN protocols can be used through standard interfaces between firewall applications and switches [1], [2], [4], [6].

B. *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. 3 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 flow's packets to SDN Controller.
2) SDN Controller forwards the flow's 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 flow's 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 and can be resolved by our framework in a similar way, 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 the 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 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 the existing SDN switches and protocols. For example, deep packet inspection should be performed by 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 determine how much intelligence switches should have in terms of performance and autonomy.

V. Conclusion

In this paper, we proposed our framework for security services based on Software-Defined Networking. 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 emulator [7] and OMNeT++ simulator [8], and also 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 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] 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, "Requirements for Security Services based on Software-Defined Networking," *IETF draft-jeong-i2nsf-sdn-security-services-00*, Oct. 2014.

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

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

[8] OMNeT++, "A discrete event simulation environment," http://www.omnetpp.org.