Cloud-Based Security Service System for User’s Security Intent Support

Jaehoon (Paul) Jeong
Department of Interaction Science, Sungkyunkwan University, Republic of Korea

I. INTRODUCTION

Nowadays, cloud-based services have been popularly provided to the Internet users. For these cloud-based services, security services need to be provided accordingly against well-known or new security attacks. This paper proposes a cloud-based security service system supporting a user’s security intent. When a user specifies his high-level security policy, the security service system needs to understand it, and then enforces the corresponding low-level security service such as firewall, deep packet inspection, data loss prevention, distributed denial of service (DDoS) attack mitigation. Our cloud-based security service system can grasp a user’s security intent, so it can provide him with the intended security services automatically by selecting appropriate network security functions (NSF) in a network functions virtualization (NFV) environment and software-defined networking (SDN) networks.

II. CLOUD-BASED SECURITY SERVICE SYSTEM

A. Interface to Network Security Functions (I2NSF)

Internet Engineering Task Force (IETF) Interface to Network Security Functions (I2NSF) working group is working for standard interfaces of cloud-based security service systems. Fig. 1 shows an I2NSF security service system whose main components are I2NSF User, Security Controller, Developer’s Management System, and NSFs. In Table 1, I2NSF interfaces are listed up along with their control protocol. Developer’s Management System registers its NSF into Security Controller with its capability information via Registration Interface.

B. Intent-Based Security Service System

I2NSF User (as a network administrator or a customer) can specify a high-level security policy, and deliver it to Security Controller via Consumer-Facing Interface. Security Controller translates the high-level security policy into the corresponding low-level security policy with its policy translator. The low-level security policy will be delivered to an appropriate NSF which configures the policy in its local repository for security enforcement. Both the high-level and low-level security policies can be described in XML files for RESTCONF or NETCONF though YANG data models for each I2NSF interface in Table 1. Thus, the I2NSF security service system in Fig. 1 can autonomously provide a user with security services for the user’s security intent.

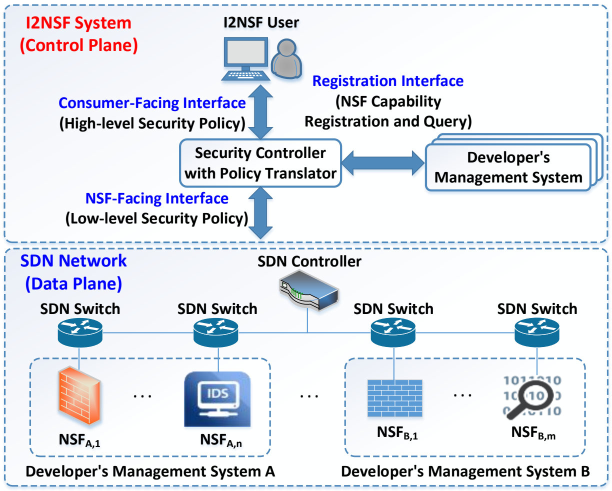

Figure 1: I2NSF Security Service System

Table 1: I2NSF Interface and Control Protocol

I2NSF Interface	Control Protocol
Consumer-Facing Interface	RESTCONF
NSF-Facing Interface	NETCONF
Registration Interface	NETCONF

ACKNOWLEDGMENT

This work was supported by Institute for Information & communications Technology Promotion (IITP) grant funded by the Korea government (MSIP) (No.R-20160222-002755).

REFERENCES

1. S. Hyun et al., "Interface to Network Security Functions for Cloud-Based Security Services", IEEE Communications Magazine, Vol. 56, Issue 1, January 2018.
2. Sungkyunkwan University, “I2NSF Open Source Project”, https://github.com/kimjinyong/i2nsf-framework