# Intent-Based Security System for Cloud Security Services

Chaehong Chung[*], Patrick Lingga[*], and Jaehoon (Paul) Jeong[†]

[*]Department of Electrical and Computer Engineering, Sungkyunkwan University,

[†] Department of Interaction Science, Sungkyunkwan University

{darkhong, patricklink, pauljeong}@skku.edu

## Abstract

To provide Intent-Based Security System (IBSS) for cloud security services, real-time monitoring and analyzing security policies are required with security policy translator. This paper proposes the architecture and procedure of IBSS to provide robust and flexible security services on dynamically changed situations. Basically, this IBSS runs on Software-Defined Networking (SDN) and Network Functions Virtualization (NFV) environments, and can provide customers with an efficient way for security services based on security policies.

## Ⅰ. Introduction

Network security is an important piece in computer networks consisting of security policies to eliminate and monitor unauthorized intrusion. With the advancement of cloud computing and Network Functions Virtualization (NFV), security services using the cloud computing with NFV have been provided. These services are developed by distinct vendors which provide proprietary configuration and management schemes for their services, which are not interoperable with the services of other vendors. This non-interoperability of the security services lets a network administrator spend a lot of time and efforts to properly configure them. A network administrator is also prone to make mistakes when a managed network is large.

Intent-Based Networking (IBN) technology minimizes errors that can occur when an administrator sets up a network. The IBN technology enables the real-time verification of whether network devices operate correctly within the context of intents (i.e., policies) to ensure the network to run properly.

In the context of the IBN, if dynamic network change detection and network reconfiguration is not performed in real time, the performance of the network will not be good according a user's intents (i.e., policies). It is also difficult to ensure that the intents of the user are enforced properly on the network. In addition, there is no reliable logging system for identifying errors and problems that occurred during network operation time [1].

There are some related works about dynamic network configuration using the IBN technology. Tsuzaki et al. proposed a method that enables a network administrator to update the network configuration reactively according to the change of external environment [4]. T. Szyrkowiec proposed an architecture for automatic intent-based provisioning in a multilayer IP, Ethernet, and optical network [5]. This architecture chooses the appropriate encryption layer using Software-Defined Networking (SDN) orchestrator.

This paper focuses on the automation of configuration for cloud security services, which is based on the intents of a user. The proposed scheme uses feedback regarding the real-time conditions of the SDN and NFV environment for the security controller to manage Network Security Functions (NSF) in the NFV system.

## Ⅱ. Intent-Based Security System

The IBSS is designed to not only configure security polices, but also monitor and analyze the polices. It enables these intent-based security policies to be enforced in the network. Our goal is to make an IBSS for cloud security services by both configuring security policies for NSFs and reconfiguring the monitored and analyzed security policies accordingly.

For these cloud security services, they need to support a user's security intent according to a variety of security attacks. When a user specifies a high-level security policy, which is based on a natural language, the security system needs to understand what the user's security policy is. Then its security controller needs to translate it into the corresponding low-level security policy which can apply the intent to the corresponding NSFs such as firewall, deep packet inspection, and DDoS attack mitigation.

An SDN controller plays a role of forwarding packets through its SDN switches and NSFs in the network according to the security polices given to it. Also, it can monitor the traffic flows in real time and

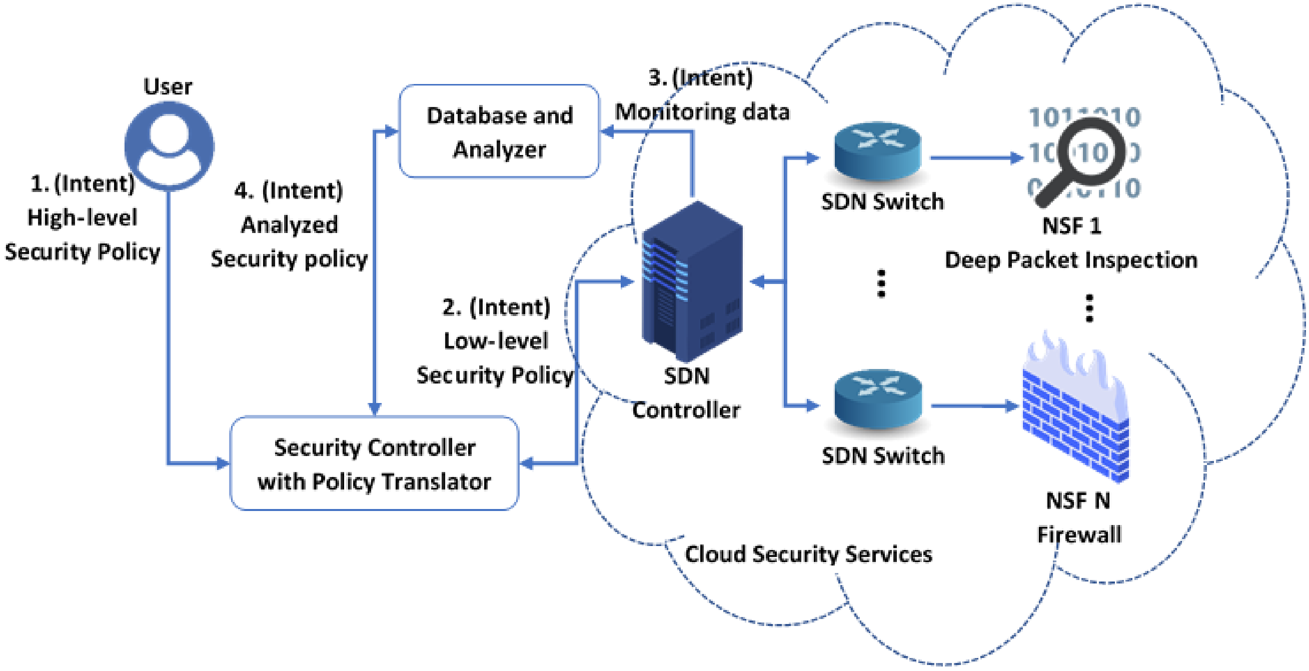

Figure 1. Intent-Based Security System Architecture

forwards the packets of the traffic flows to a database and traffic analyser for security monitoring. They collect the monitored data, and analyze them to see whether the user's intents are perfectly applied in the network or not. If the analyzer finds that the intent is not appropriately applied due to a user's mistakes or dynamically changed situations, it sends the analyzed security policy to the security controller. Then, the security controller can update and reconfigure the intent (e.g., analyzed security policy) without a user's engagement for updating the policy.

Figure 1 shows the architecture of our proposed intent-based security system for cloud security services. The first step is that a user specifies intent-based high-level security policy. From the second step to the fourth step, the security controller configures the security policy to the corresponding NSFs. Moreover, it can reconfigure the analysed security policy using its monitored data and analyzer. This intent-based security system can realize a user's security intent, so it can automatically provide with intended security services.

## Ⅲ. Conclusion and Future Work

In this paper, the intent-based security system for cloud security services is addressed. Especially, if the user's security policy is not applied properly because of dynamic situations, this system can reconfigure the policy according to analyzed intended security policy. It is possible because the security controller takes over translating security policies to configure (or reconfigure) while real-time monitored and analyzed data are carried out for automating security configuration. In future, we will implement analyzer using machine learning techniques and compare for performance evaluation.

## ACKNOWLEDGMENT

This work was supported by NRF grant (2017R1D1A1B03035885) and IITP grant (2019-2017-0-01633). Note that Jaehoon (Paul) Jeong is the corresponding author.

## References

[1] R. Davis, "The Data Encryption Standard in Perspective", IEEE Communications Society Magazine, vol. 16, no. 6, pp. 5-9, Nov. 1978.

[2] Miles E. Smid, "From DES to AES", 2000, (http://www.nist.gov/aes).

[3] A. Shamir, "On the Security of DES", Advances in Cryptology, Proc. Crypto '85, pp. 280-285, Aug. 1985.

[4] Y. Tsuzaki and Y. Okabe, "Reactive Configuration Updating for Intent-Based Networking", *2017 International Conference on Information Networking (ICOIN)*, Da Nang, pp. 97-102, 2017.

[5] T. Szyrkowiec et al., "Automatic Intent-Based Secure Service Creation through a Multilayer SDN Network Orchestration", *IEEE/OSA Journal of Optical Communications and Networking*, vol. 10, no. 4, pp. 289-297, April 2018.

[6] J. Jeong, "Cloud-Based Security Service System for User's Security Intent Support", US-Korea Conference, August 2019.