A Web-Based Monitoring System for Network Security Functions in Cloud Security Systems

Patrick Lingga*, Jeonghyeon Kim†, Mose Gu†, and Jaehoon (Paul) Jeong†
* Department of Electrical and Computer Engineering, Sungkyunkwan University, Suwon, Republic of Korea
† Department of Computer Science and Engineering, Sungkyunkwan University, Suwon, Republic of Korea
Email: {patricklink, jeonghyeon12, rna0415, pauljeong}@skku.edu

***Abstract*—Network security is a property of computer networks to ensure the confidentiality and integrity of the computer networks. Network security services can be provided as Virtual Network Functions (VNF) in a cloud environment. It is important to monitor the network security services to make sure them work properly. We propose a web-based monitoring system for Network Security Functions (NSF) in cloud-based security systems. We implemented the monitoring system by collecting the information from an NSF to a centralized database. Then the information is visualized to easily provide the information with users in real time using a web service consisting of React as the front-end and Node.js as the back-end.**

***Index Terms*—Network security function, web-based monitoring, cloud.**

I. Introduction

Network security is one of key functions in computer networks to protect users by detecting, monitoring, and preventing any unwanted threats or unauthorized accesses. With the advancement of cloud computing, most network security services are implemented as Virtual Network Functions (VNF). There are a lot of vendors that provide such network security services to make sure that security threats in the Internet can be eliminated. A problem arises when different vendors try to implement their own network security services. Each vendor usually provides customers with a different way to configure and monitor its services.

The Interface to Network Security Functions (I2NSF) working group in Internet Engineering Task Force (IETF) provides standardized interfaces for Network Security Functions (NSFs) in cloud-based security systems [1]. Fig. 1 shows an I2NSF framework with five components and five interfaces [2]. The I2NSF components are as follows:

- **I2NSF User:** A network administrator to configure a high-level security policy into the I2NSF framework to provide a network security service.
- **Security Controller:** A controller that controls NSFs and translates a high-level security policy from I2NSF User into a low-level security policy for NSF(s).
- **Developer's Management System (DMS):** A provider of an NSF to register the capabilities of the NSF with Security Controller.
- **Network Security Function (NSF):** A network-based security service such as Firewall, Web Filter, and Distributed Denial-of-Service (DDoS)-attack Mitigator.

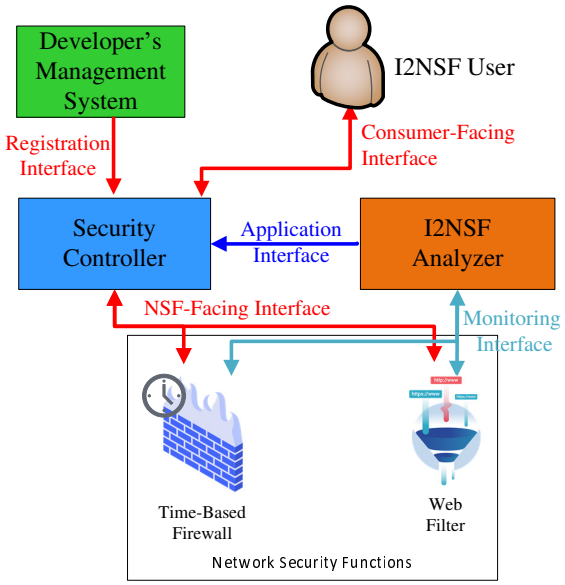

Fig. 1. Interface to Network Security Functions (I2NSF) Framework

- **I2NSF Analyzer:** An analyzer to collect monitoring data from NSFs and analyze them to provide Security Controller with feedback information.

The I2NSF interfaces are as follows:

- **Consumer-Facing Interface:** Used to deliver I2NSF User's high-level security policy to Security Controller.
- **Registration Interface:** Used to register the capabilities of an NSF with Security Controller.
- **NSF-Facing Interface:** Used to deliver a low-level security policy to an NSF.
- **Monitoring Interface:** Used to deliver an NSF's monitoring data to I2NSF Analyzer.
- **Application Interface:** Used to deliver policy reconfiguration or feedback information to Security Controller.

This paper uses the I2NSF Monitoring Interface for a web-based monitoring system [3], which proposes a YANG data model for monitoring an NSF to detect the indication of a harmful activity, irregular network behavior, or system overload in a timely manner. The web-based monitoring system provides real-time visualization of the usages of an NSF's system resources, and the network traffic volumes into and out of an NSF. Note that the source code of this web-based monitoring system is released in the I2NSF GitHub

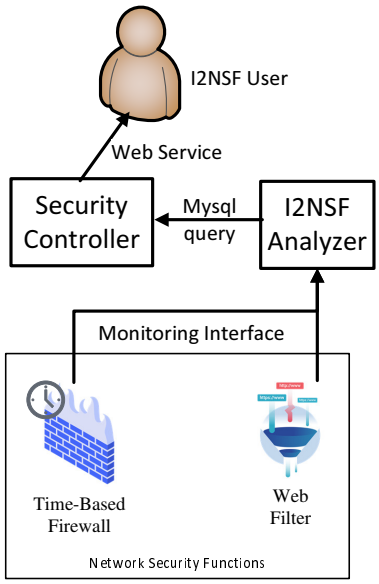

Fig. 2. Web-Based Monitoring Architecture

repository [4] as the IETF-111 hackathon project along with a demonstration video clip in YouTube [5].

II. Design and Implementation

This section presents the design and implementation of the web-based monitoring system for NSFs. For this design and implementation, this paper focuses on four components such as I2NSF User, Security Controller, I2NSF Analyzer, and NSFs, as shown in Fig. 2. To monitor the status of NSFs, I2NSF Analyzer utilizes NETCONF's subscription [6] on each NSF to acquire monitoring data in real time. By using the NETCONF subscription, any event detected by the NSFs will be delivered to I2NSF Analyzer. The implementation of NETCONF is performed with ConfD that is provided by Tailf [7]. For the NSF Monitoring Interface, the YANG data model in [3] is used to deliver an NSF's monitoring data to I2NSF Analyzer.

When they are received by I2NSF Analyzer, the NSF monitoring data are saved in a central database in Security Controller with MySQL query, which has the status information of every NSF. Security Controller provides the visualized monitoring data as a web service to I2NSF User. This web service consists of React as a front-end and Node.js as a back-end. The front-end of React performs the real-time visualization of NSF monitoring data, and the back-end of Node.js performs the data delivery from the central database to a web front-end for visualization. The front-end and back-end use the pre-implemented REST API to display real-time monitoring data on a web page of a web browser. The web browser can display the usages of memory, CPU, and disk of an NSF as well as the incoming and outgoing network traffic.

The web-based monitoring system in the I2NSF framework monitored a stress test on an NSF with a controlled Denial of Service (DoS) Attack to the NSF. Fig. 3 shows the real-time visualization of NSF monitoring data. The graphs in Fig. 3 show the change during the stress test by a DoS attack. It is visible that the memory usage fluctuates and the incoming

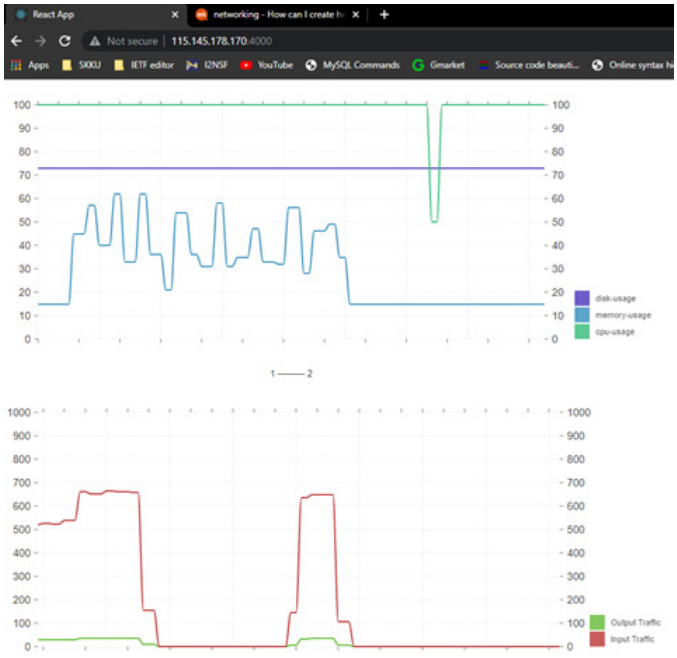

Fig. 3. Visualized Monitoring Data for NSF

and outgoing traffic peaked when the stress test by the DoS attack is activated. Thus, it is concluded that the proposed web-based monitoring system can provide real-time visualization for effective NSF monitoring.

III. Conclusion

The proposed web-based monitoring system can provide I2NSF User with real-time visualization of an NSF's resource usage and network traffic so that I2NSF can understand the status of an NSF and detect a security attack (e.g., DoS attack) in the NSF. As future work, we will enhance I2NSF Analyzer to perform the analysis of system diagnosis and security attack detection with machine learning.

IV. Acknowledgment

This work was supported by IITP grant (2019-0-01343) and ITRC grant (IITP-2021-2017-0-01633). Note that Jaehoon (Paul) Jeong is the corresponding author.

References

[1] IETF. Interface to Network Security Functions (I2NSF). [Online]. Available: https://datatracker.ietf.org/wg/i2nsf/documents/

[2] D. Lopez, E. Lopez, L. Dunbar, J. Strassner, and R. Kumar, "Framework for Interface to Network Security Functions," RFC 8329, Feb. 2018. [Online]. Available: https://rfc-editor.org/rfc/rfc8329.txt

[3] J. Jeong, P. Lingga, S. Hares, L. Xia, and H. Birkholz, "I2NSF NSF Monitoring Interface YANG Data Model," Internet Engineering Task Force, Internet-Draft draft-ietf-i2nsf-nsf-monitoring-data-model-10, Sep. 2021, work in Progress. [Online]. Available: https://datatracker.ietf.org/doc/html/draft-ietf-i2nsf-nsf-monitoring-data-model-10

[4] I2NSF Hackathon Open-Source Project. I2NSF GitHub Repository. [Online]. Available: https://github.com/jaehoonpaul/i2nsf-framework/tree/master/Hackathon-111

[5] I2NSF Hackathon Project Demonstration. I2NSF YouTube Video Clip. [Online]. Available: https://youtu.be/gHzZKpJ9zak

[6] H. Trevino and S. Chisholm, "NETCONF Event Notifications," RFC 5277, Jul. 2008. [Online]. Available: https://rfc-editor.org/rfc/rfc5277.txt

[7] Tail-f. ConfD. [Online]. Available: https://www.tail-f.com/confd-basic/