네트워크 기능 가상화 프레임워크 기반 I2NSF 프레임워크 구현 방안에 관한 연구

홍동진, 정재훈
성균관대학교 전자전기컴퓨터공학과
{dong.jin, pauljeong}@skku.edu

A Study on Method to Implement I2NSF Framework based on Network Function Virtualization Framework

Dongjin Hong, Jaehoon (Paul) Jeong
Department of Computer Science and Engineering, Sungkyunkwan Univ.

요 약

본 논문은 ETSI(European Telecommunications Standards Institute) NFV(Network Function Virtualization) 프레임워크를 기반으로 IETF(Internet Engineering Task Force) I2NSF(Interface to Network Security Functions) 프레임워크를 구현하는 방법에 대해 소개한다. IETF I2NSF WG(Working Group)는 네트워크 보안 서비스를 제공하기 위한 표준화를 진행 중이다. 해당 워킹 그룹은 물리적인 보안 기능과 가상화된 보안 기능을 사용할 수 있음을 기술하였지만 구체적인 구현 방안을 제시하지 않았다. 따라서 본 논문에서는 NFV 프레임워크에서 I2NSF 프레임워크를 구현하기 위한 아키텍처를 제안한다. NFV 프레임워크를 사용하여 I2NSF 프레임워크를 구현한다면 물리적인 네트워크 보안 기능과 더불어 가상화된 네트워크 보안 기능 또한 사용이 가능하므로 보안서비스를 더욱 효과적으로 제공할 수 있다.

Ⅰ. 서 론

미국의 시장조사기관인 가트너(Gartner)는 2020년도까지 200억개 이상의 디바이스가 존재할 것이라고 발표했다[1]. 디바이스의 수가 증가함에 따라 네트워크상의 트래픽 량은 점점 증가할 것이고, 이에 따라 현존하는 통신망에 여러 가지 문제가 발생될 것으로 예상된다. 발생 가능한 문제들을 사전에 예방하기 위해 최근 네트워크를 소프트웨어를 통해 동적으로 관리할 수 있는 SDN(Software-Defined Networking)[2] 기술과 네트워크 리소스를 가상화하여 사용 할 수 있는 NFV(Network Functions Virtualization)[3] 기술이 오픈소스 프로젝트를 통해 활발한 연구 및 개발 활동이 이루어지고 있다.

위 두 가지 기술을 토대로 IETF(Internet Engineering Task Force) I2NSF(Interface to Network Security Functions) Working Group[4], [5]은 SDN 및 NFV를 이용하는 네트워크 환경에서 다양한 제조사에서 개발된 네트워크 보안 서비스를 호환시키고 제공하기 위한 표준 인터페이스를 정의하고 구현하는 것을 목표로 활발한 표준화활동을 진행 중이다. I2NSF 프레임워크는 정책 생성과 생성된 정책을 기반으로 Firewall, IDS, IPS, Anti-DDoS, Anti-Virus 등과 같은 네트워크 보안 함수(Network Security Functions, NSF)를 물리적 또는 가상적으로 만들어 규칙을 적용함으로써 보안 서비스를 제공할 수 있음을 기술했다[6]. 하지만 해당 워킹 그룹은 가상화된 보안 기능을 사용할 수 있음을 기술하였지만 구체적인 구현 방안을 제시하지 않았다. 따라서 본 논문에서는 NFV 프레임워크를 기반으로 I2NSF 프레임워크를 구현하기 위한 아키텍처를 제안하고 이를 구현할 방법에 대해 기술한다.

본 논문에서는 IETF I2NSF에서 제안한 프레임워크와 ETSI(European Telecommunications Standards Institute) NFV에서 제안한 프레임워크를 살펴보고 최근 오픈소스 프로젝트를 통해 개발되는 프레임워크들의 구현 상태 또한 살펴본다. 이를 바탕으로 가상화된 보안 기능을 사용할 수 있는 프레임워크를 제안한다.

Ⅱ. 본 론

본 섹션에서는 I2NSF 프레임워크, NFV 프레임워크 그리고 NFV 프레임워크 기반의 I2NSF 프레임워크에 대해 설명한다.

1. I2NSF 프레임워크

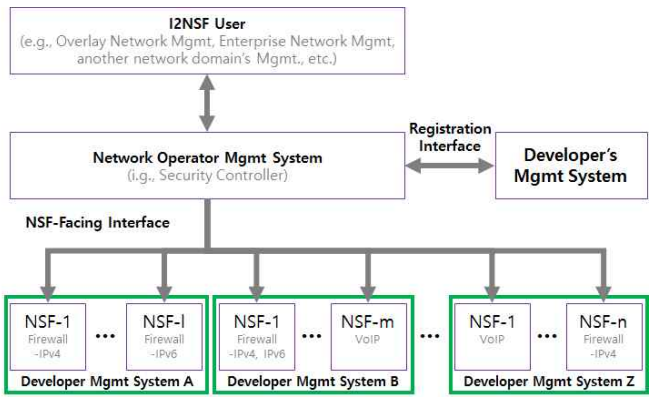

그림 1. I2NSF 프레임워크

그림 1은 I2NSF 프레임워크를 보여준다. I2NSF 유저는 웹 UI를 통해 고수준 보안 정책 규칙을 생성하고 RESTCONF 프로토콜[7]을 사용하는 Consumer Facing Interface를 통해 네트워크 운영 관리 시스템에게 전달된다. 네트워크 운영 관리 시스템은 고수준 보안 정책을 네트워크 보안 기능이 이해할 수 있는 저수준으로 번역하고 NETCONF 프로토콜[8]을 통해 알맞은 네트워크 보안 기능에게 전달한다. 저수준 보안 정책을 전달 받은 네트워크 보안 기능은 이를 반영하여 다양하고 복잡한 공격들로부터 네트워크를 보호한다. Registration Interface는 네트워크 보안 기능을 개발하는 제조사가 개발한 네트워크 보안 기능을 I2NSF 프레임워크에 등록하여 사용이 가능하게 한다. 해당 인터페이스는 NFV 프레임워크에서 VNF(Virtual Network Function)를 생성하고 생명주기를 관리하는 것이

아닌 이미 생성된 VNF를 I2NSF 프레임워크에 등록하는 역할을 한다. 현재 Registration Interface를 제외한 프레임워크는 구현된 상태다.

2. NFV 프레임워크

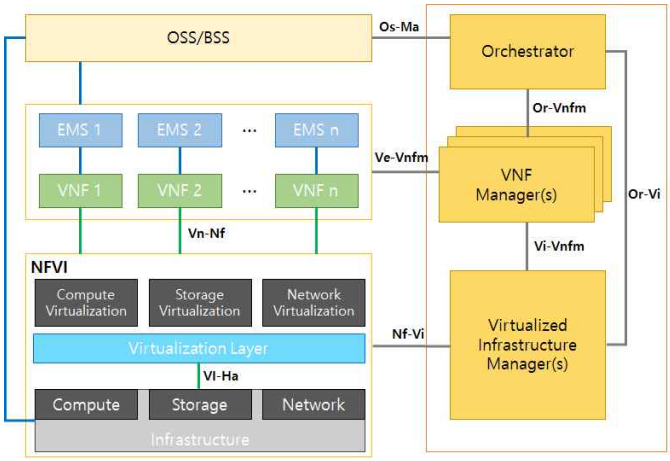

그림 2. NFV 프레임워크

그림 2는 NFV 프레임워크를 보여준다. NFV 프레임워크의 핵심은 우측의 MANO(Management and Orchestration)로 불리는 Orchestrator, VNFM(VNF Manager) 그리고 VIM(Virtualized Infrastructure Manager)이다. NFV 플랫폼에서 적용되는 자원, 장애 등에 대한 정책을 관리하거나 적용하기 위한 기능을 제공하는 Orchestrator, VNF를 관리하는 EMS(Entity Management System)의 요청에 따라 VNF 인스턴스에 대한 생성, 종료, 스케일링 등 전반적인 생명주기를 관리하는 VNFM 마지막으로 VIM은 Orchestrator나 VNFM의 요청에 따라 모든 가상 자원에 대한 자원 할당, 해제, 예약기능을 수행한다. 각 엔티티들은 인터페이스로 연결된다. 현재 해당 프레임워크는 OPNFV[9] 프로젝트를 통해 NFVI(NFV Infrastructure)와 VIM이 구현되어 통합된 상태이고 이에 대한 테스트를 진행하고 주기적으로 버전을 업데이트하여 배포하고 있다.

3. NFV 프레임워크 기반의 I2NSF 프레임워크

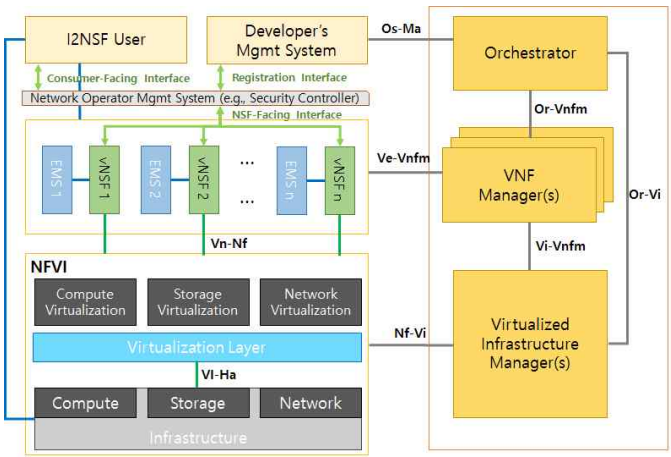

그림 3. NFV 프레임워크 기반의 I2NSF 프레임워크

그림 3은 NFV 프레임워크 기반의 I2NSF 프레임워크를 보여준다. 본 논문이 제안하는 NFV 프레임워크 기반의 I2NSF 프레임워크는 앞서 설명한 기능을 모두 지원하며 NFV 프레임워크의 기능 또한 지원하고 두 프레임워크의 호환이 이루어져야 한다. 해당 프레임워크가 가상화된 네트워크 기능인 vNSF를 생성, 등록 그리고 사용하기 위한 과정은 다음과 같다. 우선 개발자 관리 시스템이 MANO에게 VNF 생성을 요청하면 MANO는 NFV 프레임워크가 정의한 과정을 통해 VNF를 만든다. 이후 개발자 관리 시스템이 Registration 인터페이스를 통해 I2NSF 프레임워크에 생성된 vNSF를 등록한다. 최종적으로 기존 I2NSF 프레임워크와 같은 방식으로 NSF에 보안 정책을 내려 보안 서비스를 제공한다.

Ⅲ. 결 론

본 논문에서는 IETF I2NSF 프레임워크에서 네트워크 보안 함수를 가상화하여 사용하기 위해 NFV 프레임워크를 기반으로 설계하고 이를 구현하기 위한 아키텍처에 대해 연구하였다. 본 논문에 제안된 프레임워크가 SDN 및 NFV 기반의 프레임워크에 대한 표준화를 위해 기여할 수 있다고 믿는다. 향후 연구로 제안한 아키텍처를 기반으로 오픈스택(Open Stack)[10]을 포함해 여러 오픈소스를 사용해 이를 구현하려 한다.

ACKNOWLEDGMENT

"본 논문은 2017년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구(2016-0-00078, 맞춤형 보안서비스 제공을 위한 클라우드 기반 지능형 보안 기술 개발)이고, 과학기술정보통신부 및 정보통신기술진흥센터의 SW중심대학지원사업의 연구결과로 수행되었음(2015-0-00914)".

참 고 문 헌

[1] Gartner, Inc., "Gartner Says the Internet of Things Installed Base Will Grow to 26 Billion Units By 2020", http://www.gartner.com/newsroom/id/2636073.

[2] ONF, "Software-Defined Networking: The New Norm for Networks", ONF White Paper, April. 2012.

[3] ETSI-NFV, "Network Functions Virtualization (NFV); Architectural Framework", ETSI GS NFV 002 V1.2.1, December. 2014.

[4] IETF, "The Internet Engineering Task Force", https://ietf.org

[5] IETF I2NSF Working Group, "Interface to Network Security Functions(I2NSF)", https://datatracker.ietf.org/wg/i2nsf/charter

[6] J. Jeong, S. Hyun, T. Ahn, S. Hares, and D. Lopez, "Applicability of Interfaces to Network Security Functions to Network-Based Security Services", IETF draft-ietf-i2nsf-applicability, October. 2017.

[7] A. Bierman, M. Bjorklund, and K. Watsen, "RESTCONF Protocol", IETF RFC 8040, Jan, 2017.

[8] R. Enns, M. Bjorklund, J. Schoenwaelder, and A. Bierman, "Network Configuration Protocol (NETCONF)," IETF RFC 6421, Jun, 2011.

[9] OPNFV, "Open Platform for NFV", https://www.opnfv.org/

[10] Openstack, "Open source software for creating private and public clouds", https://www.openstack.org/