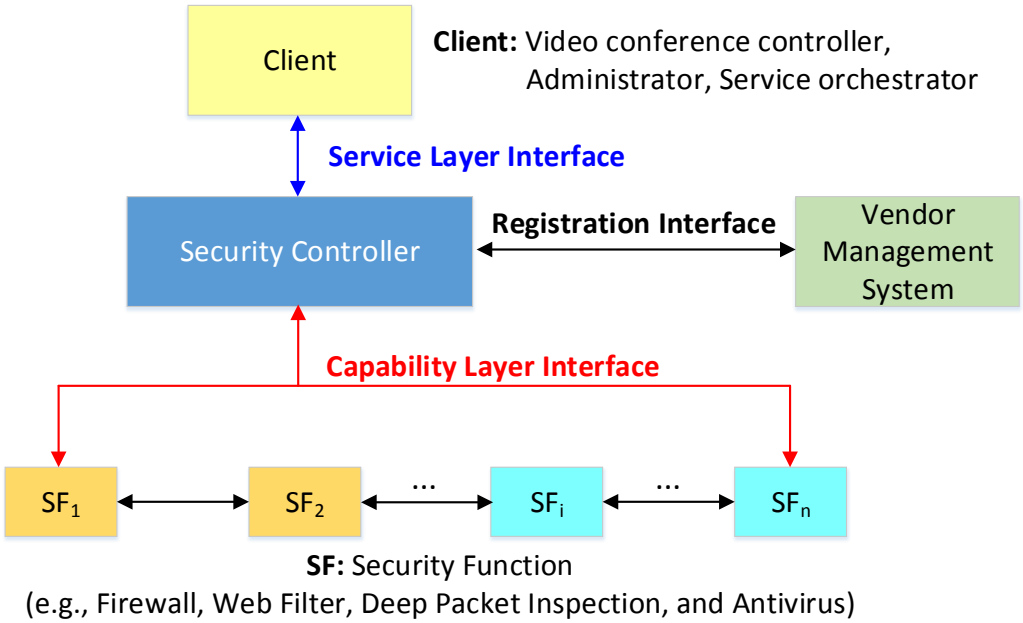
[정보보호] IETF 네트워크 보안 기능 인터페이스(I2NSF) 표준화

IETF(Internet Engineering Task Force) I2NSF(Interface to Network Security Functions) BoF[1]에서 2015년 7월 회의에 본인이 속한 성균관대학교와 전자통신연구원은 “I2NSF를 이용하는 SDN기반 보안 서비스”[2] 표준의 필요성을 제안하였다. 본고에서는 I2NSF를 소개하고 본인이 표준화하고 있는 “I2NSF를 이용하는 SDN기반 보안 서비스”를 소개하고자 한다.

네트워크 보안 기능 인터페이스(I2NSF)



<그림 1> I2NSF 아키텍처

I2NSF(Interface to Network Security Functions)는 NFV(Network Functions Virtualization)[3]를 기본 인프라로 이용하는 네트워크 환경에서 네트워크 보안 서비스(Network Security Service)를 제공하기 위한 표준 인터페이스를 정의하고 구현하는 것을 목표로 한다. I2NSF는 2014년 11월에 개최된 IETF 91차 회의에서 BoF로 시작되었고, 지난 IETF 93차 회의에서 두 번째 BoF를 개최하였다. I2NSF가 시작된 배경은 최근에 네트워크 서비스 인프라 구축 및 운영 비용을 절감하기 위한 네트워크 기능 가상화인 NFV 연구 및 개발이 유럽 표준화 기구인 ETSI를

중심으로 인터넷 서비스 제공자, 네트워크 장비 회사에 의해 진행되고 있다[3]. 또한 네트워크의 유연하고 효과적 진화와 관리를 위해 데이터 플레인(Data Plane)과 콘트롤 플레인(Control Plane)의 분리하고 제어 서버를 통해 네트워크 디바이스를 관리하는 소프트웨어 중심의 네트워크인 SDN(Software-Defined Networking)[4]을 I2NSF에 적용하려는 연구 및 개발 활동이 활발하다.

이러한 I2NSF는 네트워크 서비스의 사용자(Client), 사용자가 NFV 환경에서 보안 서비스를 사용할 수 있게 보안 제어기(Security Controller) 그리고 보안 서비스를 실제로 수행하는 보안 기능(Security Function, SF)으로 구성된다. 그림 1은 I2NSF의 아키텍처를 보여주고 있다. 또한 I2NSF 아키텍처에서의 세 가지 인터페이스를 정의하고 있다.

① 서비스 계층 인터페이스(Service Layer Interface): 보안서비스 사용자(예, 이동통신망 관리자)가 서비스 계층 인터페이스를 통해 보안 제어기에게 고수준 보안정책(High-level Security Policy)를 전달한다.

② 기능 계층 인터페이스(Capability Layer Interface): 보안 제어기는 전달받은 고수준 보안정책을 NFV 상의 보안 기능(SF)에서 실행될 수 있는 저수준 보안기능(Low-level Security Functions)으로 번역한다. 보안 제어기는 이 보안기능을 기능 계층 인터페이스를 통해 적합한 보안 기능 가상 머신 또는 물리 머신에 전달하여 요청된 보안서비스를 실행한다.

③ 등록 인터페이스(Registration Interface): 보안서비스 공급자(예, Symantec, Verisign, AhnLab)는 벤더 관리 시스템(Vendor Management System)을 가지고 등록 인터페이스를 통해 보안 제어기를 거쳐서 I2NSF의 SF에서 실행될 보안서비스 패키지를 설치한다.

I2NSF는 현재 <그림 1>에서 서비스 인터페이스와 기능 인터페이스를 표준화를 진행할 예정이고, 등록 인터페이스는 I2NSF 표준화에 포함시키지 않을 예정이다.

네트워크 보안 기능 인터페이스(I2NSF)

성균관대학교에 소속된 본인은 전자통신연구원과 공동으로 I2NSF 프레임워크와 정보 모델을 기반으로 SDN기반의 보안 서비스 문서를 발표했다. 먼저 I2NSF을 사용하는 SDN기반의 보안

서비스에서의 목적 및 요구사항을 기술하였고, 아울러 중앙집중식 방화벽 시스템과 중앙집중식 DDoS 공격 약화 시스템의 두 가지 유스케이스를 제시하였다. 다음 단계로 SDN 네트워크에서 NETCONF/YANG을 기반으로 방화벽의 예제로 IP Address Filtering을 구현을 위한 기능 계층 인터페이스를 구현할 예정이다. 또한 서비스 계층 인터페이스의 정보 모델을 위해 SUPA BoF에서 정의한 Policy Abstraction을 이용할 예정이다.

I2NSF는 2015년 7월에 체코 프라하에서 개최된 IETF 93차 회의에서 워킹그룹으로 승격하기 위한 두 번째 BoF에서는 I2NSF 프레임워크 문서, Gap Analysis 문서, 문제 기술 문서, I2NSF 정보 모델 문서, 유스케이스 문서, 가능한 해결기법 문서들이 발표되었고, I2NSF BoF Charter 질의 및 응답과 수정에 대한 논의를 하였다.

결언

지난 IETF 93차 회의에서는 참가한 많은 보안 전문가들이 I2NSF의 필요성에 동의하였고, 올 9월에 I2NSF는 워킹그룹으로 승인되어서 본격적인 표준화 활동을 시작하였다. 성균관대학교와 한국전자통신연구원도 I2NSF에서 SDN기반 보안 서비스, 기능 계층 인터페이스 및 YANG기반 정보 모델에 적극적으로 참여할 예정이다.

참고문헌

[1] I2NSF, https://datatracker.ietf.org/wg/i2nsf/charter/

[2] 정재훈, 김형식, 박정수, “Software-Defined Networking Based Security Services using Interface to Network Security Functions”, draft-jeong-i2nsf-sdn-security-services-02, 2015년 7월.

[3] ETSI-NFV, “Network Functions Virtualisation (NFV); Architectural Framework”, ETSI GS NFV 002 V1.1.1, October 2013.

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

정재훈 (성균관대학교 소프트웨어학과 교수, pauljeong@skku.edu)