

## I2NSF 표준화 동향

정재훈 (성균관대학교 소프트웨어학과) / FIF Architecture Security WG

I2NSF(Interface to Network Security Functions)는 NFV(Network Functions Virtualization) 인프라 기반의 네트워크 환경에서 네트워크 보안 함수(Network Security Function, NSF)를 제공하기 위한 프레임워크(Framework)와 표준 인터페이스(Interface)를 정의하고, 각 인터페이스에 대한 정보 및 데이터 모델 스펙 작성 및 오픈소스 개발을 목표로 한다. I2NSF가 시작된 배경은 최근에 네트워크 서비스 인프라 구축 및 운영 비용을 절감하기 위한 네트워크 함수 가상화인 NFV 연구 및 개발이 유럽 표준화 기구인 ETSI를 중심으로 인터넷 서비스 제공자, 네트워크 장비 회사에 의해 진행되고 있다. 또한 네트워크의 유연하고 효과적 진화와 관리를 위해 네트워크 시스템을 데이터 플레인(Data Plane), 컨트롤 플레인(Control Plane), 매니지먼트 플레인(Management Plane)으로 분리하고, 컨트롤러를 통해 네트워크 디바이스를 중앙집중식으로 관리하는 소프트웨어 중심의 네트워크인 SDN(Software-Defined Networking)를 I2NSF에 적용하려는 연구 및 개발 활동이 한국 성균관대에 의해 주도되고 있다.

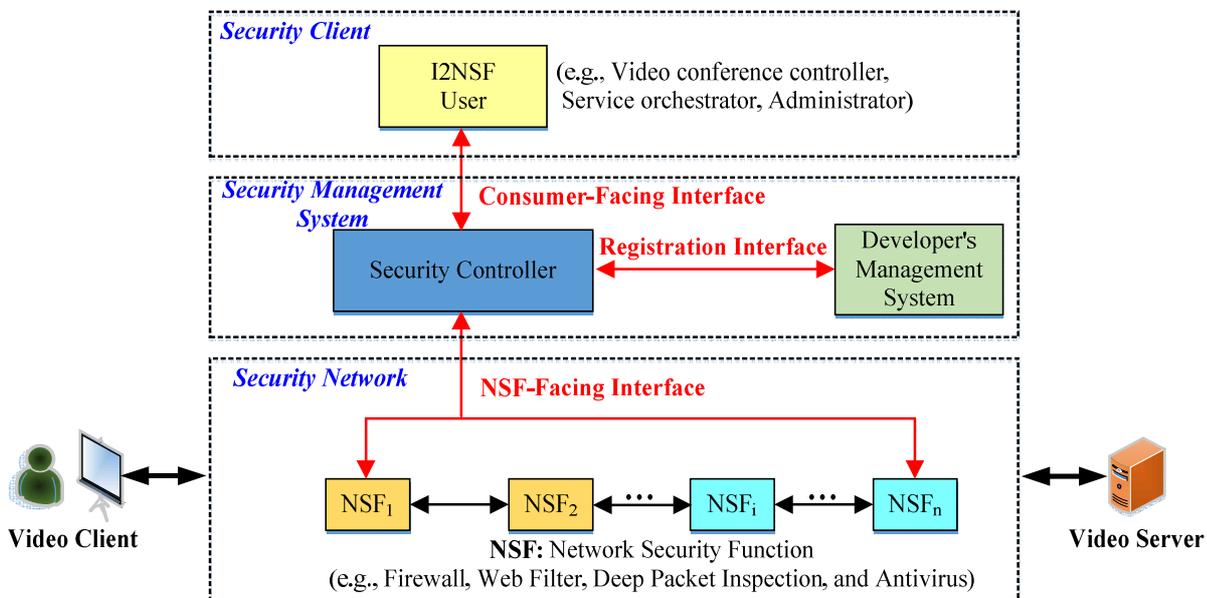


그림 1. I2NSF Framework

그림 1은 I2NSF의 프레임워크를 보여주고 있다. 이러한 I2NSF 프레임워크는 I2NSF 관리자(I2NSF User), 보안 컨트롤러(Security Controller), 개발자 관리 시스템(Developer's Management System) 및 네트워크 보안 함수(NSF)로 구성되어 있다. I2NSF 관리자는 네트워크 관리자의 서비스에 대한 고수준 보안 정책(High-level Security Policy)을 설정하는 보안 클라이언트(Security Client)이다. 보안 컨트롤러는 I2NSF 관리자가 전달한 고수준 보안 정책을 저수준 보안 정책(Low-level Security Policy)으로 변환하고 이를 수행할 NSF를 선택한다. 개발자 관리 시스템은 I2NSF 프레임워크에서 사용될 NSF의 등록, 생성, 소멸 등을 담당한다. 이와 같이 보안 컨트롤러와 개발자 관리 시스템은 I2NSF의 보안 관리 시스템(Security Management System)을 구성한다. NSF는 보안 서비스를 실제로 수행하는 네트워크 보안 함수로써 사용자 데이터를 안전하게 전달하는 보안 네트워크(Security Network)를 구성한다.

I2NSF는 그림 1과 같이 소비자 방향 인터페이스(Consumer-Facing Interface), NSF 방향 인터페이스(NSF-Facing Interface), 등록 인터페이스(Registration Interface)의 세가지 인터페이스를 가지고 있다. I2NSF 관리자가 소비자 방향 인터페이스를 통해 보안 컨트롤러에게 고수준 보안정책을 전달한다. 보안 컨트롤러는 전달받은 고수준 보안정책을 NFV 상의 네트워크 보안 함수(NSF)에서 실행될 수 있는 저수준 보안함수로 번역하여 이 보안 함수를 NSF 방향 인터페이스를 통해 적합한 보안 함수 가상 머신 또는 물리적 머신에 전달하여 요청된 보안 서비스가 실행되게 한다. 개발자 관리 시스템은 등록 인터페이스를 통해 보안 컨트롤러와 통신하며 NSF를 관리한다. 그림 1과 같이 I2NSF 프레임워크에서 보안 정책에 따른 보안 서비스가 설정이 되면 VOD(Video On-Demand) 같은 비디오 서비스를 Video Client가 Video Server로부터 설정된 보안 수준에서 안전하게 제공받을 수 있다.

I2NSF WG는 현재 Gap Analysis 기고서, Problem Statement 및 Use Case 기고서, I2NSF Framework 기고서, I2NSF Terminology 기고서 및 Client-Facing Interface의 요구사항 기고서를 WG 문서로 채택하였다. 특히 Problem Statement 및 Use Case 기고서는 RFC 승인을 위해 현재 IESG(Internet Engineering Steering Group)에서 심사를 받고 있다. 성균관대가 제안한 SDN 네트워크 관련 기고서가 I2NSF Problem Statement 및 Use Cases WG 문서에 병합되었다. IETF 98차 시카고 회의에서 성균관대, ETRI 및 KT는 I2NSF Project로 IETF Hackathon에 참가해서 I2NSF WG의 프레임워크와 데이터 지향(Data-Driven)의 인터페이스를 구현해서 I2NSF에 대한 POC(Proof of Concept)를 수행하였다. 또한 성균관대는 이번 I2NSF 워킹그룹 회의에서 다음의 6건의 기고서를 발표하였다.

- I2NSF Capability에 대한 YANG Data Model
- I2NSF NSF-Facing Interface에 대한 YANG Data Model
- Security Management를 위한 I2NSF Consumer-Facing Interface에 대한 YANG Data Model
- I2NSF 프레임워크에서의 NSF-triggered Traffic Steering
- I2NSF Registration Interface에 대한 Information Model
- I2NSF Registration Interface에 대한 Data Model

본 기고서 발표에서 특히 I2NSF 보안 서비스를 위한 기능(Capability) 정보 모델에 기반한 NSF-triggered Traffic Steering 및 NSF 관리하기 위한 Registration Interface를 제안하였다.

인터넷의 네트워크 전반적인 구조가 SDN/NFV 중심으로 혁신되는 상황에서 클라우드 기반의 보안 서비스가 보편화될 예정이므로 국내 ISP, 보안 소프트웨어 기업들은 이러한 I2NSF 표준기술에 보조를 맞추어 보안 서비스 기술을 개발해야 세계적인 경쟁력을 확보할 수 있을 것이다. 이에 성균관대는 ETRI 및 KT와 협력하여 I2NSF 기반의 보안 시스템 개발 및 표준화에 적극적으로 참여하여 한국이 이러한 네트워크 가상화 기반 보안 서비스 분야를 선도할 수 있도록 노력할 예정이다.