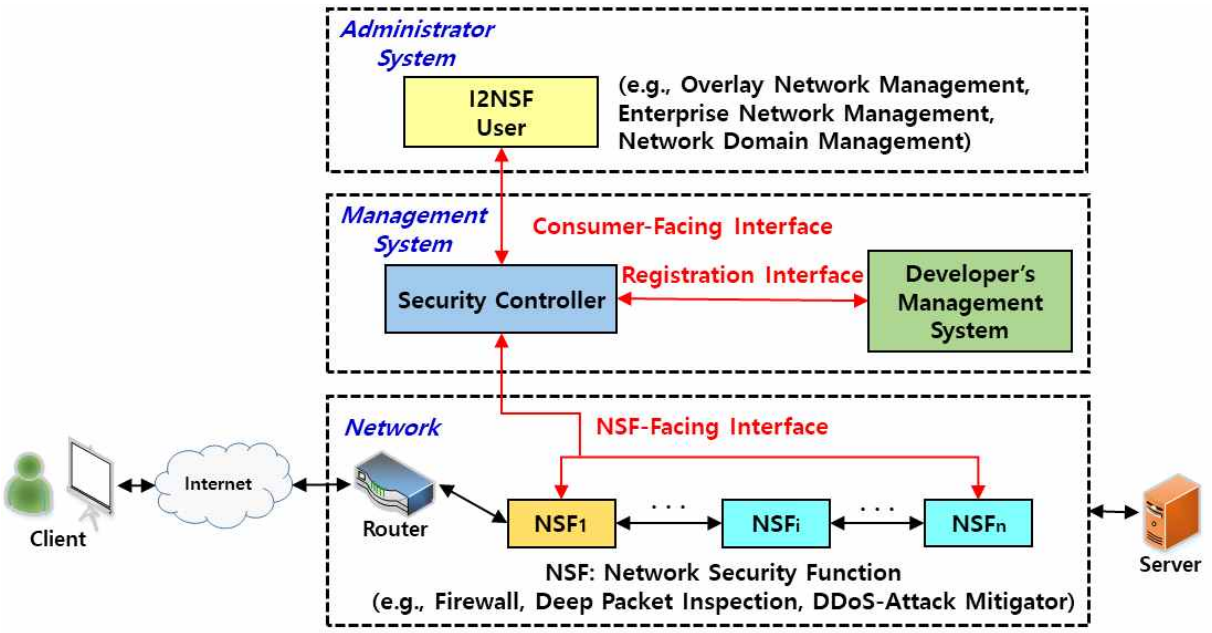
IETF I2NSF 표준화 동향

정재훈(성균관대학교 소프트웨어대학 조교수, pauljeong@skku.edu)

1. 머리말

IETF(Internet Engineering Task Force)의 I2NSF(Interface to Network Security Functions) 워킹그룹(WG, Working Group)은 네트워크 기능 가상화(NFV, Network Functions Virtualization) 환경에서 다양한 보안 벤더들의 네트워크 보안 기능(NSFs, Network Security Functions)을 연결하기 위한 프레임워크 및 인터페이스를 표준화하고 있다. I2NSF는 YANG이라는 데이터 모델 언어 기반으로 관리자 보안 정책을 NSF에게 설정하는 것을 자동화하는 데에 목표를 두고 있다. [그림 1]은 클라우드 기반 보안 서비스를 위한 I2NSF 프레임워크와 주요 I2NSF 인터페이스를 보여주고 있다. I2NSF 프레임워크에서 I2NSF 유저(User)가 고수준 보안 정책(High-level Security Policy)을 정의하여 네트워크에 적용을 요청하면, NSF가 이해할 수 있는 저수준 보안 정책(Low-level Security Policy)에 대한 규칙(Rule)으로 변환되어 해당 NSF에 보안 설정된다. 본고에서는 2018년 3월 16일~24일, 영국 런던에서 개최된 IETF 101차 정기회의에서의 I2NSF 표준화 진행상황에 대해 기술한다.



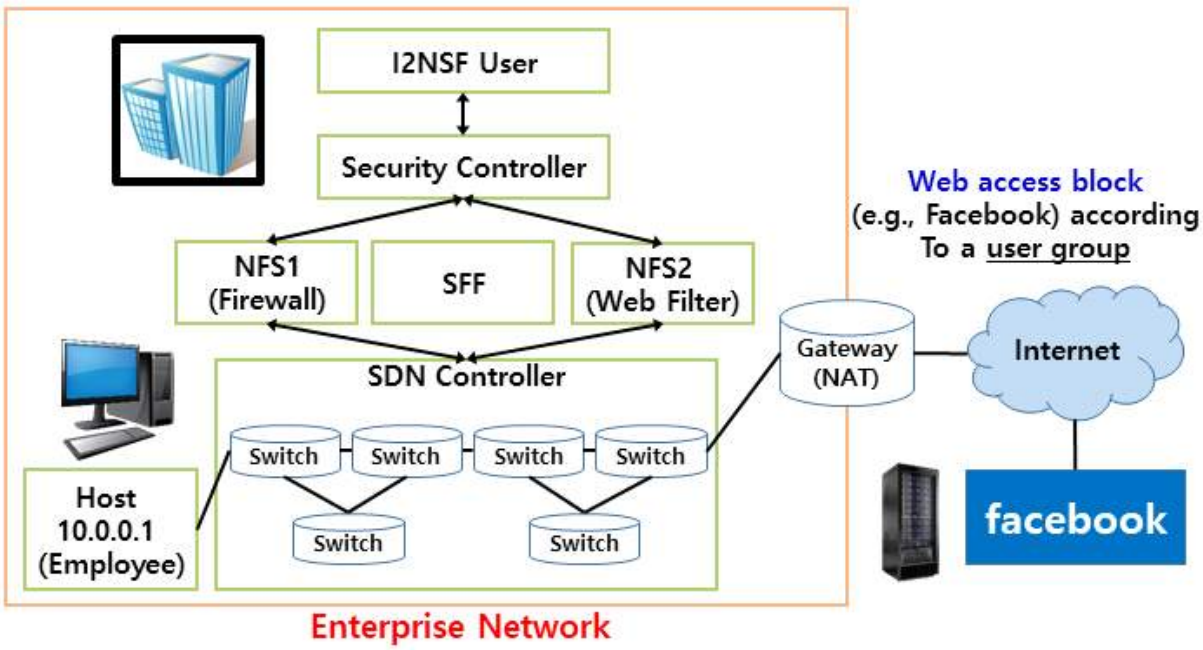
[그림 1] 클라우드 기반 보안 서비스를 위한 I2NSF 프레임워크

2. 회의 주요 결과

I2NSF WG은 현재까지 Problem Statement 및 Use Case를 표준문서인 RFC 8192로 등록했고, I2NSF Framework를 RFC 8329로 등록했다. 2018년 2월, 성균관대의 NSF-Facing Interface의 Data Model기고서와 Consumer-Facing Interface의 Data Model 기고서 2건이 I2NSF WG문서로 채택되었다. 현재 I2NSF WG문서로는 다음과 같다.

- I2NSF 적용 WG 문서
- NSF Capability 정보 모델 WG 문서
- Consumer-Facing Interface에 대한 요구사항분석 WG 문서
- SDN 기반 IPsec 플로우 보호 WG 문서
- I2NSF Terminology WG 문서

IETF 101차 정기회의에서 I2NSF WG는 I2NSF Capability에 대한 데이터 모델 기고서, Consumer-Facing Interface에 대한 정보 모델 기고서 및 데이터 모델 기고서, Registration Interface에 대한 정보 모델 기고서 및 데이터 모델 기고서를 WG문서로 채택하기 위한 논의를 하였다. I2NSF WG은 정보 모델과 데이터 모델에 대한 로드맵에 따라 2018년에 주요 정보 모델 및 데이터 모델에 대한 문서를 RFC 출간을 위한 IESG 제출을 목표로 하고 있다.



[그림 2] IETF-101 I2NSF 해커톤 프로젝트

I2NSF WG은 IETF 101차 해커톤(Hackathon)을 통해 보안 서비스를 NSF로 매핑하는 Dynamic Configuration과 Consumer-Facing Interface를 최신 데이터 모델을 기반으로 RESTCONF로 구현하였다. [그림 2]와 같이 User Group에 따라 Web Access Block 보안 서비스를 시연하였다. Web Filter를 위해 IDS/IPS 오픈 소스인 Suricata를 이용하였다. I2NSF를 위해 제안된 SFC(Service Function Chaining)-Enabled Traffic Steering 아키텍처에 따라 웹 관련 패킷들을 보안 서비스(예, Firewall, Web Filter)를 수행하는 SF(Service Function)인 NSF들을 통해 포워딩하기 위해 SFF(Service Function Forwarder)가 이용될 수 있다. 본 해커톤을 통해 I2NSF 프레임워크와 데이터 지향(Data-Driven)의 인터페이스를 통한 효과적인 보안 서비스에 대한 POC(Proof of Concept)를 수행하였다.

이번 I2NSF 워킹그룹 회의에서 성균관대는 다음의 9건의 기고서를 발표하였다.

① I2NSF Applicability;
② I2NSF Capability Data Model;
③ I2NSF NSF-Facing Interface Data Model;
④ I2NSF Consumer-Facing Interface Information Model;
⑤ I2NSF Consumer-Facing Interface Data Model;
⑥ I2NSF Registration Interface Information Model;
⑦ I2NSF Registration Interface Data Model;
⑧ NSF Monitoring Data Model;
⑨ Service Function Chaining-Enabled I2NSF Architecture.

본 회의에서 I2NSF Capability 정보 모델에 동기화되는 데이터 모델 표준화가 강조되었다. 데이터 모델 저자들은 정보 모델 저자들의 제안에 따라 객체지향적인 디자인(Object-Oriented Design)을 기반으로 I2NSF Capability 데이터 모델, NSF-Facing Interface 데이터 모델, Consumer-Facing Interface 데이터 모델, Registration Interface 데이터 모델 문서들을 수정할 예정이다. 스페인 텔레포니카의 Diego Lopez는 정보 모델과 데이터 모델을 하나의 문서로 병합하자고 제안했으나, 성균관대 정재훈 교수는 정보 모델은 사람들이 모델을 이해하기에 유용하므로 정보 모델과 데이터 모델이 일관되게 작성된다면 분리된 문서로 출간하는 것이 좋다고 의견을 발표했다.

I2NSF Applicability 문서는 SFC(Service Function Chaining)-Enabled Traffic Steering과 NFV Use Case를 포함하여 개정작업을 하여 6월, WG Last Call(WGLC)을 거쳐 RFC 출판을 위해 IESG에 제출될 예정이다. NSF-Facing Interface 문서는 Capability 정보 모델 문서의 저자들의 의견을 반영하여 개정이 되었다. IETF-101 해커톤을 통해 본 문서의 데이터 모델이 검증되었다. 본 문서는 개정작업하여 10월, WGLC를 거쳐 RFC 출판을 위해 IESG에 제출될 예정이다.

I2NSF Consumer-Facing Interface 정보 모델 기고서와 데이터 모델 문서가 발표되었는데, I2NSF Capability 정보 모델을 반영하고 실제 보안 정책을 고수준 보안 정책으로 표현하기 위해 Threat Analysis를 위해 사용되는 STIX(Structured Threat Information Expression) 데이터 모델을 참고하여 개정작업을 할 예정이다. I2NSF WG 의장인 Linda Dunbar는 Software- Defined Security Service WG의 엔터프라이즈 유스 케이스(Enterprise Use Case)를 참고하여 Consumer-Facing Interface 정보 모델을 보완할 것을 제안했다. 본 문서는 개정작업 후 10월, WGLC를 거쳐 RFC 출판을 위해 IESG에 제출될 예정이다.

NSF Monitoring Data Model 문서는 NSF Monitoring Information Model의 저자인 Henk Birkholz의 제안에 따라 재사용성을 위한 Identity를 갖는 구조와 Notification Feature를 포함하게 개정되었다. 현재 Data Model은 Notification의 정의에 따라 Periodic Push와 On-change Push를 지원하게 되었다. Registration Interface 정보 모델 기고서와 데이터 모델 기고서는 Registration Interface에 대해 Capability 등록, Capability 쿼리, NSF Lifecycle 관리를 위한 MANO(Management and Orchestration)와의 Interaction을 정의하고 있다. WG에서는 Registration Interface는 Capability 등록과 Capability 쿼리만을 다루고 MANO와의 Interaction에 대한 이슈는 구현 고려사항으로 언급하기로 했다.

3. 맺음말

차세대 인터넷은 5G 모바일 네트워크와 사물인터넷(IoT) 중심으로 네트워크 서비스를 위해 SDN/NFV 중심으로 개편될 예정이다. 이러한 환경에서 국민, 기업, 국가기관의 안전을 위해 보안 및 프라이버시의 중요성은 더욱 부각될 전망이다. SDN/NFV 환경에서 다양한 보안 서비스 벤더의 솔루션을 효과적으로 사용하는 클라우드 기반의 보안 서비스가 보편화될 예정인데, IETF I2NSF는 이러한 클라우드 기반 보안 서비스를 위한 최적화된 프레임워크 및 표준 인터페이스를 제안하고 있다. 따라서 이러한 추세에 맞추어 국내 보안 소프트웨어 기업들 및 ISP는 I2NSF 표준기술을 조기에 도입하여 실제 네트워크에 구현 및 운영함으로써 향후 네트워크 보안 시장에서 큰 경쟁력을 갖출 수 있을 것이다. 성균관대, KT 및 ETRI는 계속 협력하여 I2NSF 기반 클라우드 보안 서비스 시스템 관련 표준화를 주도하고, 신규 표준화 아이템을 발굴할 예정이다. 또한 이들 기관은 효과적인 I2NSF 표준화를 위해 오픈스택(OpenStack) 기반으로 NFV 시스템을 구축하고, 이를 바탕으로 I2NSF Framework과 Interface들을 개발 및 검증하여 I2NSF 표준화 선도를 할 예정이다.