SDN/NFV 기반 보안 서비스를 위한 IETF I2NSF 표준화 동향

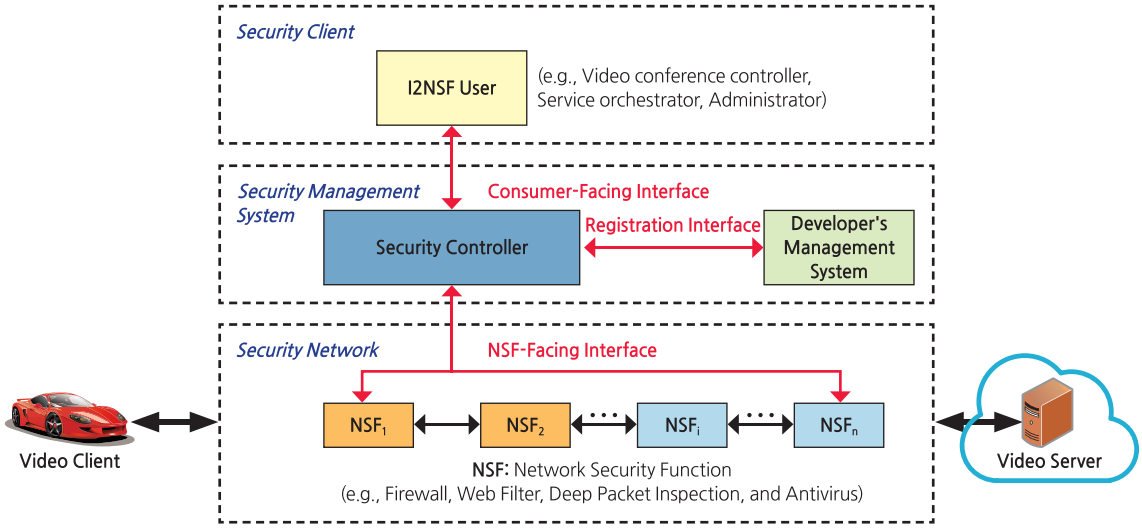
정재훈 _ 성균관대학교 소프트웨어학과 교수

1. 머리말

소프트웨어 정의 네트워킹(SDN, Software-Defined Networking)과 네트워크 기능 가상화(Network Functions Virtualization)는 클라우드 기반 보안 서비스를 가능한 환경을 조성했다. 이러한 환경에서 네트워크 관리자나 사용자의 보안 정책에 대한 보안 서비스를 수행하는 다양한 벤더의 네트워크 보안 함수(NSF, Network Security Function) 생성 및 정책 설정을 하기 위한 클라우드 기반 보안 서비스 시스템의 프레임워크와 이 프레임워크의 주요 컴포넌트 간의 인터페이스의 필요성이 대두되었다. 이러한 필요성을 해소하기 위해 국제인터넷표준화기구인 IETF(Internet Engineering Task Force)는 I2NSF(Interface to Network Security Functions) 워킹그룹(WG)을 2015년 11월에 창설하여 클라우드 기반 보안 시스템의 프레임워크와 인터페이스를 위한 표준화를 4년 동안 진행하고 있다[1]~[3]. 본고에서는 I2NSF WG의 표준화 동향과 오픈소스 기반 I2NSF 해커톤 프로젝트에 대해 소개한다.

2. I2NSF 프레임워크

I2NSF WG은 클라우드 기반 보안 서비스 시스템 개발을 위해 RFC 문서로 I2NSF 프레임워크를 표준화하였다[3]. [그림 1]은 I2NSF 프레임워크와 I2NSF 인터페이스를 보여주고 있다. I2NSF 프레임워크의 주요 컴포넌트는 I2NSF User(I2NSF 사용자), Security Controller(보안 제어기), Developer's Management System(DMS, 개발자 관리 시스템), Network Security Function(NSF, 네트워크 보안 함수)으로 구성된다. I2NSF User는 보안 정책(Security Policy)을 정해서 내리는 네트워크 관리자가 사용하는 Security Client(보안 클라이언트)이다. Security Controller는 I2NSF User의 보안 정책을 수신하여 그 보안 정책에 해당하는 보안 서비스에 대한 NSF들을 선정하여 각 NSF에 보안 정책 규칙(Security Policy Rule)을 설정하는 구성(Configuration)을 생성하여 각 NSF에게 전달한다. NSF는 보안 서비스를 수행하는 보안 함수(예: Firewall, Web Filter, Deep Packet Inspection(DPI), Antivirus)로써 하드웨어기반 보안 디바이스인 Physical Network Function(PNF) 또는



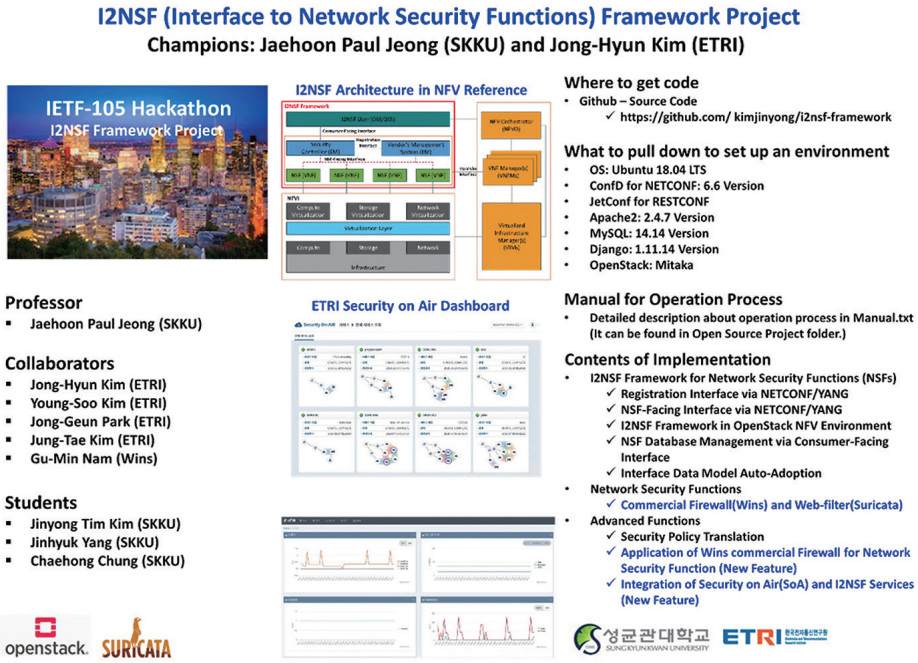
[그림 1] I2NSF 프레임워크 및 인터페이스

NFV 시스템에서 생성된 소프트웨어기반 보안 모듈인 Virtual Network Function(VNF) 형태로 동작한다. Developer's Management System은 보안 솔루션을 제공하는 벤더(Vendor)가 보안 솔루션을 탑재한 VNF 또는 PNF의 기능(Capability) 등록을 수행하는 벤더 관리 시스템이다.

I2NSF 프레임워크는 [그림 1]과 같이 Consumer-Facing Interface(CFI, 소비자 직면 인터페이스)[8], NSF-Facing Interface(NFI, 네트워크 보안 함수 직면 인터페이스)[9], Registration Interface(RI, 등록 인터페이스)[10] 등 3개의 인터페이스를 갖고 있다. 소비자 직면 인터페이스인 CFI는 I2NSF User와 Security Controller 사이의 인터페이스로써 I2NSF User가 고수준 보안 정책(High-level Security Policy)을 Security Controller에게 전송하는 데 사용하는 인터페이스이다. Security Controller가 수신한 고수준 보안 정책을 NSF가 이해할 수 있는 저수준 보안 정책(Low-level Security Policy)으로 번역한다. NSF 직면 인터페이스인 NFI는 Security Controller와 NSF 사이의 인터페이스로써 Security Controller가 번역한 저수준 보안 정책을 NSF로 전송하는 데 사용하는 인터페이스이다. 등록 인터페이스인 RI는 개발자 관리 시스템인 DMS와 Security Controller 사이의 인터페이스로써 DMS가 자신이 관리하는 NSF의 접근정보(예: IP 주소, TCP 포트번호)와 능력(Capability)을 Security Controller에 등록하여 Security Controller가 저수준 보안 정책에 대한 해당 NSF를 선정할 수 있게 한다.

[그림 1]은 Video Client인 자동차가 클라우드에 있는 Video Server로부터 비디오 스트리밍 서비스를 I2NSF 시스템을 통해 보안적으로 안전하게 서비스를 받는 것을 기술하고 있다. 차량 네트워크의 보안 설정을 위해 I2NSF User는 차량의 비디오 서비스에 대한 고수준 보안 정책을 Security Controller에게 송부하면 Security Controller는 저수준 보안 정책으로 번역하여 해당 NSF들(예, Firewall, Web Filter, DPI. Antivirus)에게 해당 저수준 보안 정책 규칙(Low-level Security Policy Rule)을 송부하여 차량 트래픽

[그림 2] IETF-105 해커톤[1]

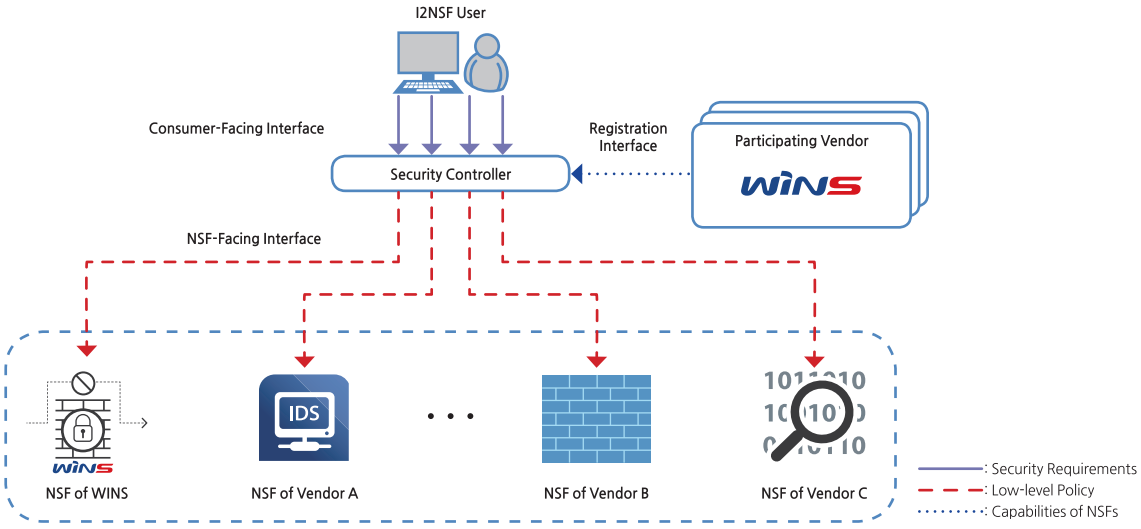


[그림 3]] I2NSF 프레임워크 해커톤 프로젝트 포스터

을 위한 보안 서비스를 클라우드에서 수행한다.

3. IETF-105 I2NSF Hackathon Project

2019년 7월에 IETF 105차 정기회의가 캐나다 몬트리올에서 개최되었다[4]. IETF 정기회의 전에 열리는 해커톤(Hackathon)은 많은 WG의 멤버들이 참석하여 자신의 워킹그룹에서 진행하고 있는 표준화 기술에 대한 POC(Proof of Concept)를 보여주기 위해 개최된다. 이번 IETF 105차 해커톤은 7월 20일부터 21일까지 2일간 개최되었으며, 현장 참석자 280명이 참석, 42개의 팀으로 구성되어 진행했다[1]. [그림 2]는 IETF-105 해커톤 모습을 보여주고 있는데, 각 팀들은 해당 WG 기고서를 POC를 위한 구현 및 테스트



[그림 4] IETF-105 해커톤을 위한 I2NSF 시스템 아키텍처

를 하고 있다. 이번 I2NSF 해커톤 발표에서 성균관대는 클라우드 기반 보안 서비스 시스템인 I2NSF의 기술을 한국전자통신연구원(ETRI)에서 개발한 보안 클라우드 시스템(SoA, Security on Air)에 설치하여 상용 방화벽과 오픈소스 기반 웹필터를 시연하였다. [그림 3]은 I2NSF 프레임워크 해커톤 프로젝트의 포스터이다.

이번 해커톤에서 I2NSF Framework 프로젝트는 네 가지를 구현 및 데모를 하였다. 첫째는 I2NSF 프레임워크와 I2NSF 인터페이스를 OpenStack 환경에서 구현하는 것이고, 둘째는 ETRI의 SoA라는 보안 클라우드에서 I2NSF Security Controller를 구현하는 것이고, 셋째는 상용 Wins 방화벽과 오픈소스 Suricata 기반 웹필터를 NSF로 이용하는 것이고, 보안 정책 번역기를 통해 고수준 보안 정책을 저수준 보안 정책으로 번역하여 시간 기반 웹필터(Time-Based Web Filter)와 방화벽(Firewall) 서비스를 제공하였다. [그림 4]는 I2NSF 해커톤 프로젝트의 I2NSF 시스템 아키텍처를 보여주고 있다. 이번 해커톤에서 I2NSF 프레임워크 프로젝트는 NFV 환경을 위한 ETRI 공공 클라우드에서 I2NSF 시스템이 표준 인터페이스들은 통해 상용 NSF와 오픈소스 NSF를 이용한 효과적인 클라우드 기반 보안 서비스의 가능성을 입증하였다.

4. IETF-105 I2NSF WG 정기회의

IETF-105 I2NSF WG 정기회의에서는 I2NSF Applicability 문서[5]의 업데이트 사항, I2NSF Framework Hackathon Project 보고, I2NSF IPsec 관리 문서[6], I2NSF 주요 인터페이스 데이터 모델 문서[7]~[10], I2NSF NSF 모니터링 데이터 모델 문서[11], I2NSF Security Policy Translation 문서[12]에 대한 발표가 있었다. I2NSF Applicability 문서는 IESG(Internet Engineer Steering Group)에 의해 검토되어 수정사항을 저자들이 반영하게 하여 담당 Security Area Director인 Roman Danyliw가 최종 검토를 받고 있는데, 2019년 11월 즈음에 Informational RFC로 IESG 승인을 받을 예정이

다. I2NSF IPsec 관리 문서, NSF Capability 정보 모델[13] 및 I2NSF 주요 인터페이스 데이터 모델 문서[7]~[10]는 2019년 11월에 IESG에 제출하여 심의를 받아 12월 안으로 RFC 승인을 목표로 하고 있다. 주요 인터페이스에 대한 데이터 모델 문서의 RFC 출간 이후 I2NSF WG은 Rechartering을 통해 새로운 표준 아이템을 선정해서 계속 워킹그룹을 유지할지 또는 클로징할 11월 IETF-106 정기회의(싱가포르)에서 의장단과 핵심 멤버들이 논의할 예정이다.

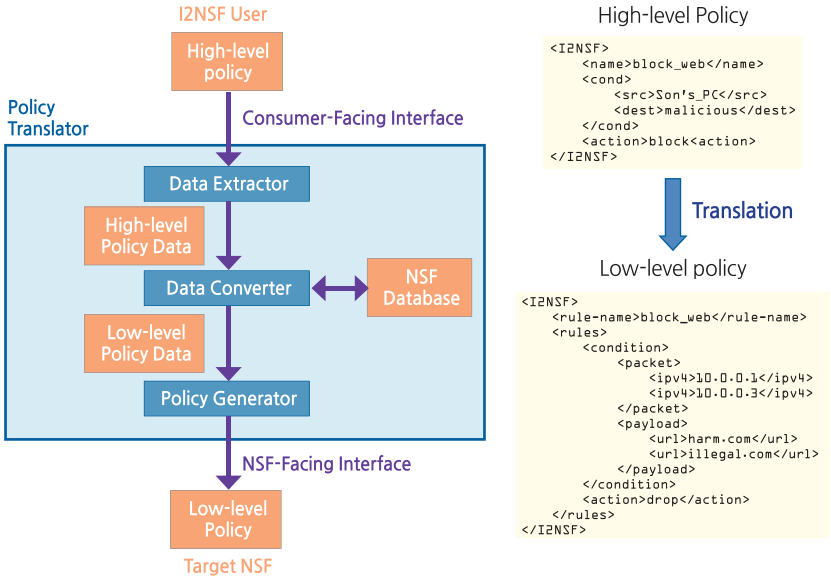
성균관대는 이번 I2NSF 워킹그룹 회의에서 다음 7건의 기고서를 제출 또는 발표하였다.

- I2NSF Applicability[5]
- I2NSF Capability Data Model[7]
- I2NSF Consumer-Facing Interface Data Model[8]
- I2NSF NSF-Facing Interface Data Model[9]
- I2NSF Registration Interface Data Model[10]
- NSF Monitoring Data Model[11]
- Security Policy Translation for I2NSF[12]

이번 I2NSF WG 회의를 위해 I2NSF Applicability 문서[5]는 Security Area Director인 Roman Danyliw의 코멘트를 반영하였고, Transport Area의 Review Team Member인 Tommy Pauly의 코멘트에 대한 수정사항을 반영하여 개정되었다. Roman Danyliw의 주요 코멘트는 Developer's Management System(DMS)과 연관된 보안 공격(즉 Inside attack과 Supply chain attack) 및 해결방안이었다. Inside attack으로 악의적인 DMS가 악의적인 NSF를 Security Controller에 제공하여 I2NSF System에서 운용되게 함으로써 I2NSF System이 보안 서비스를 제대로 할 수 없게 할 수 있다. Supply chain attack으로 보안 공격을 받아 악의적으로 변경된 DMS(Compromised DMS)가 수정된 NSF 인스턴스가 I2NSF System에서 운용되게 하여 보안 서비스를 제대로 제공할 수 없게 하거나 시스템의 중요한 정보를 도청할 수 있다. 이러한 보안 공격을 막기 위해서는 DMS를 모니터링하는 것이 필요하다. 검토자인 Tommy Pauly의 주요 코멘트는 HTTP Packet이 TLS(Transport Layer Security)로 암호화되었을 때도 웹필터를 수행할 수 있는 방법을 논의하라는 것이었다. TLS 버전 1.3 이전에는 인증서(Certificate)에 URL에 해당하는 IP 주소가 있는데, 이 IP 주소를 통해 웹필터링을 수행할 수 있다. 또한 TLS를 이용하는 TCP 세션 패킷이 암호화되지 않은 Server Name Indication(SNI)을 이용할 때, SNI에 포함되어 있는 IP 주소를 통해 웹필터링을 수행할 수 있다. 또한 URL을 획득할 수 없는 경우에는 URL에 포함된 서버의 DNS 네임을 IP 주소를 변환하는 DNS Name Resolution 과정에 관찰되는 서버의 URL에 해당되는 IP 주소를 파악하여 이 IP 주소를 통해 방화벽을 통해 웹필터링을 수행할 수 있다.

SDN 기반 IPsec 플로우 보호 WG 문서[6]는 NSF 간의 IPsec 보안 채널 설정을 위해 기존의 IKEv2를 이용하는 방법(IKE Case)과 Security Controller를 통해 IPsec 보안 채널을 설정하는 방법(IKEless Case)을 제안하고 있다. 새로 만들어질 SPD(Security Policy Database) Selector를 본 문서의 I2NSF SDN 기반 IPsec에서 이용할 수 있게 IANA Registry를 본 문서에 포함하는 것을 논의하였다. SDN 기반 IPsec을 위한 YANG 데이터 모델 문서는 WG Last Call을 2019년 4월과 5월에 걸쳐서 WG의 의견을 수렴하여 반영했고, YANG Doctor의 리뷰를 받아 YANG 데이터 모델을 수정하고 있으며, 11월에 IESG에 제출되어 RFC 출간을 위한 심의를 받을 예정이다.

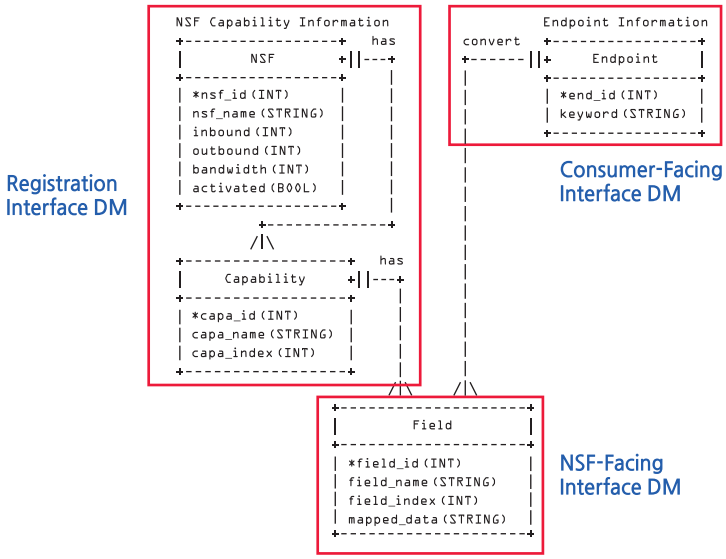
I2NSF 주요 인터페이스와 NSF 모니터링의 YANG



[그림 5] I2NSF 보안 정책 번역기의 아키텍처

데이터 모델 문서[7]~[10]의 수정 사항이 발표되었다. I2NSF NSF Capability와 I2NSF Interface의 YANG 데이터 모델 문서[7]~[10]의 YANG Module은 YANG Doctor의 리뷰를 받았고, 저자들은 리뷰를 기반으로 데이터 모델 문서를 수정하였다. I2NSF Capability 정보 데이터 모델 저자들은 YANG Guidelines 문서[14]에 따라 I2NSF Capability 데이터 모델[7], Consumer-Facing Interface 데이터 모델[8], NSF-Facing Interface 데이터 모델[9], Registration Interface 데이터 모델[10], NSF 모니터링 데이터 모델[11] 문서들을 수정하였다. 저자들은 수정된 데이터 모델에 따라 세 가지 보안 서비스에 연관된 XML Configuration Example을 수정하였다. 세 가지 보안 서비스는 Firewall과 Time-based Firewall, Web Filter와 VoIP/VoLTE 보안, HTTP 또는 HTTPS Flood-Attack Mitigator이다. IETF-105 정기회의 이후에 YANG Doctor는 추가로 수정할 사항을 저자들에게 전달했고, 저자들은 추가 수정사항을 반영하여 IETF-106 정기회의 전에 수정본을 제출했다. 저자들은 4개의 데이터 모델 문서에 대한 WG Last Call을 I2NSF WG 의장단에게 요청했다. IETF-106 정기회의 전에 I2NSF Interface에 대한 데이터 모델 문서가 IESG에서 심의되어 2019년 12월 안으로 RFC로 승인되는 것을 목표로 하고 있다.

이번 회의에서는 보안 정책 번역(Security Policy Translation) 문서에 대한 중요성이 어필되었고 WG 문서 채택을 논의하였다[12]. 보안 정책 번역기(Security Policy Translator)는 Security Controller에서 I2NSF User로부터의 고수준 보안 정책 XML 파일을 NSF가 이해할 수 있는 저수준 보안 정책 XML 파일로 번역한다. [그림 5]는 보안 정책 번역기의 아키텍처를 보여주고 있다. 고수준 보안 정책(High-level Security Policy)이 보안 정책 번역기로 전달되는 보안 정책 번역기는 Data Extractor를 통해 고수준 보안 정책에 연관된 Tag 값을 추출한다. Data Converter는 NSF Database를 참조하여 고수준 보안 정책 Tag



[그림 6] I2NSF 보안 정책 번역기의 NSF Database의 ER Diagram

값을 저수준 보안 정책 Tag 값으로 변환하고 저수준 보안 정책을 수행할 NSF들을 선택한다. Policy Generator는 저수준 보안 정책 Tag 값을 가지고 저수준 보안 정책 XML 파일을 생성한다.

본 IETF-105 정기회의를 위한 본 보안 정책 번역 문서의 주요 수정사항으로 보안 정책 번역기에 사용되는 NSF Database의 Entity-Relationship(ER) Diagram을 포함했고, 고수준 보안 정책의 YANG와 저수준 보안 정책의 YANG의 매핑을 기술하였다. [그림 6]은 보안 정책 번역기의 NSF Database의 ER Diagram을 기술하고 있다. 이 ER Diagram은 I2NSF User로부터 수신한 Endpoint 정보와 Developer's Management System(DMS)으로부터 수신한 NSF Capability 정보를 표시하여 보안 정책 번역에 필요한 엔터티(즉 NSF, Capability, Endpoint, Field)를 정의하고 엔터티 간의 관계를 표시하여 I2NSF System 개발자가 보안 정책 번역기를 수행하기 위해 제공할 정보를 표시한다. I2NSF WG의 Charter에 보안 정책 번역이 포함되어 있지 않아서 본 문서가 당장은 WG Adoption이 되지 않겠지만 11월 IETF-106 정기회의에서 I2NSF WG 의장단과 논의하여 I2NSF WG의 Charter를 개정하여 보안 정책 번역을 WG 아이템을 포함할지 논의할 예정이다.

2019년 11월 IETF-106 정기회의에서 I2NSF WG의 Rechartering을 위해 Security Policy Translator 문서뿐만 아니라 NFV 환경에서 I2NSF System을 구현하고 운용하기 위한 문서[15]도 논의될 예정이다. 또한 I2NSF Security Controller와 SFC(Service Function Chaining) Classifier 간의 연동과 I2NSF Security Controller와 SDN Controller 간의 연동을 위한 데이터 모델도 WG 아이템으로 논의될 예정이다. 아울러 I2NSF Security Controller에 Security Policy Translator를 운용하기 위해 필요한 NSF Database를 설정하기 위한 I2NSF User와 I2NSF Security Controller 간의 연동을 위한 Consumer-Facing Interface 데이터 모델도 WG 아이템으로 논의할 예정이다.

5. 맺음말

5세대 이동통신 네트워크(5G)가 상용화된 시점에서 소프트웨어 정의 네트워킹(SDN)과 네트워크 기능 가상화(NFV)를 기반으로 한 클라우드 컴퓨팅과 에지 컴퓨팅이 5G의 핵심 기술로 이용될 전망이다. 이러한 클라우드와 에지 컴퓨팅에 있어서 안전하고 안정적인 네트워크 서비스를 제공하기 위해 클라우드 기반 보안 서비스 시스템이 필요하다. 이러한 클라우드 기반 보안 서비스 시스템에서 다양한 보안 솔루션 벤더들이 제공하는 보안 솔루션을 효과적으로 운용하기 위해서는 I2NSF의 프레임워크와 표준 인터페이스가 필요하다. 본 저자는 수차례의 IETF 해커톤을 통해 Data-driven Security Service Automation의 POC를 하였다. 이러한 클라우드 기반 보안 서비스의 추세에 맞추어 국내 중소 보안업체들은 회사의 보안 솔루션이 클라우드와 에지 컴퓨팅 환경에서 잘 동작할 수 있는 보안 솔루션을 준비할 때 보안 시장에서 경쟁력을 확보할 수 있을 것이다. 성균관대는 국내 보안업체들이 국내외 보장 시장에서 경쟁력을 갖도록 I2NSF 기술을 오픈소스 기반으로 개발하고 있으며, 숭실대, ETRI 및 KT와 계속 협력하여 I2NSF 표준 기술 및 오픈소스 기반 I2NSF 시스템 개발을 계속 선도해 나갈 예정이다.

[참고문헌]

[1] I2NSF Working Group, https://datatracker.ietf.org/wg/i2nsf/about/

[2] S. Hares, D. Lopez, M. Zarny, C. Jacquenet, R. Kumar, and J. Jeong, 'Interface to Network Security Functions (I2NSF): Problem Statement and Use Cases', RFC 8192, July 2017.

[3] D. Lopez, E. Lopez, L. Dunbar, J. Strassner, and R. Kumar, 'Framework for Interface to Network Security Functions', RFC 8329, February 2018.NSF

[4] IETF 105 Highlights, https://www.ietf.org/blog/ietf-105-highlights/

[5] J. Jeong, S. Hyun, T. Ahn, S. Hares, and D. Lopez, 'Applicability of Interfaces to Network Security Functions to Network-Based Security Services', draft-ietf-i2nsf-applicability-17(work in progress), August 2019.

[6] R. Marin-Lopez, G. Lopez-Millan, and F. Pereniguez-Garcia, 'Software-Defined Networking(SDN)-based IPsec Flow Protection', draft-ietf-i2nsf-sdn-ipsec-flow-protection-07(work in progress), August 2019.

[7] S. Hares, J. Jeong, J. Kim, R. Moskowitz, and Q. Lin, 'I2NSF Capability YANG Data Model', draft-ietf-i2nsf-capability-data-model-05(work in progress), July 2019.

[8] J. Jeong, E. Kim, T. Ahn, R. Kumar, and S. Hares, 'I2NSF Consumer-Facing Interface YANG Data Model', draft-ietf-i2nsf-consumer-facing-interface-dm-06(work in progress), July 2019.

[9] J. Kim, J. Jeong, J. Park, S. Hares, and Q. Lin, 'I2NSF Network Security Function-Facing Interface YANG Data Model', draft-ietf-i2nsf-nsf-facing-interface-dm-07(work in progress), July 2019.

[10] S. Hyun, J. Jeong, T. Roh, S. Wi, and J. Park, 'I2NSF Registration Interface YANG Data Model', draft-ietf-i2nsf-registration-interface-dm-05(work in progress), July 2019.

[11] J. Jeong, C. Chung, S. Hares, L. Xia, and H. Birkholz, 'I2NSF NSF Monitoring YANG Data Model', draft-ietf-i2nsf-nsf-monitoring-data-model-01(work in progress), July 2019.

[12] J. Jeong, J. Yang, C. Chung, and J. Kim, 'Security Policy Translation in Interface to Network Security Functions', draft-yang-i2nsf-security-policy-translation-04(work in progress), July 2019.

[13] L. Xia, J. Strassner, C. Basile, and D. Lopez, 'Information Model of NSFs Capabilities', draft-ietf-i2nsf-capability-05(work in progress), April 2019.

[14] A. Bierman, 'Guidelines for Authors and Reviewers of YANG Data Model Documents', RFC 6087, January 2011.

[15] H. Yang, Y. Kim, J. Jeong, and J. Kim, 'I2NSF on the NFV Reference Architecture', draft-yang-i2nsf-nfv-architecture-05(work in progress), July 2019.