클라우드-엣지 보안 서비스를 위한 I2NSF 표준 동향

정재훈
성균관대학교

요 약

본 고에서는 국제 표준화 기구 IETF(Internet Engineering Task Force)의 네트워크 보안 함수(Network Security Function: NSF) 운용을 위한 I2NSF(Interface to Network Security Functions) 프레임워크와 인터페이스 표준화를 소개한다. I2NSF는 클라우드와 엣지 컴퓨팅 환경에서 다양한 보안 솔루션 벤더의 보안 함수들을 통일성 있게 설정 및 관리하기 위한 표준 인터페이스이다. 본 고에서는 이러한 I2NSF라는 표준 프레임워크와 표준 인터페이스의 데이터 모델을 설명하고, I2NSF의 클라우드-엣지 컴퓨팅의 보안 서비스 적용 사례를 소개한다.

Ⅰ. 서 론

현대인들은 인공지능(Artificial Intelligence: AI) 혁명 시대에 살고 있으며 지금까지 겪어 보지 못한 많은 일들을 직면하고 있다. 이에 따라 AI 기반의 다양한 보안 공격들이 더욱 기승을 부리며 우리 사회와 산업에 많은 위협을 주고 있다. 이러한 사이버 보안 위협들로부터 우리 사회와 산업을 지키기 위해서는 AI기반 보안 서비스 시스템 기술 개발 및 표준화가 중요하다.

국제인터넷표준화기구인 IETF(Internet Engineering Task Force)[1]는 이러한 지능형 보안 서비스 시스템 표준화를 위한 I2NSF(Interface to Network Security Functions) 워킹그룹(Working Group: WG)[2]을 2015년 9월에 신설하여 2023년 6월까지 8년 정도 활발히 I2NSF 관련 표준문서들을 개발했다[3]. 네트워크 보안을 위한 서비스는 네트워크 보안 함수(Network Security Function: NSF)라고 명명한다. 이러한 NSF는 가상 네트워크 함수(Virtual Network Function: VNF) 또는 클라우드 네이티브 함수(Cloud-Native Network Function: CNF) 형태로 구현된다. I2NSF WG은 I2NSF 문제기술 및 유스케이스 문서[4], I2NSF 프레임워크 문서[5] 및 소프트웨어 정의 네트워킹(Software-Defined Networking: SDN) 기반 IP 플로우(Flow) 보호 YANG 데이터 모델 문서[6]를 표준 문서인 RFC(Request for Comments)로 제정했다.

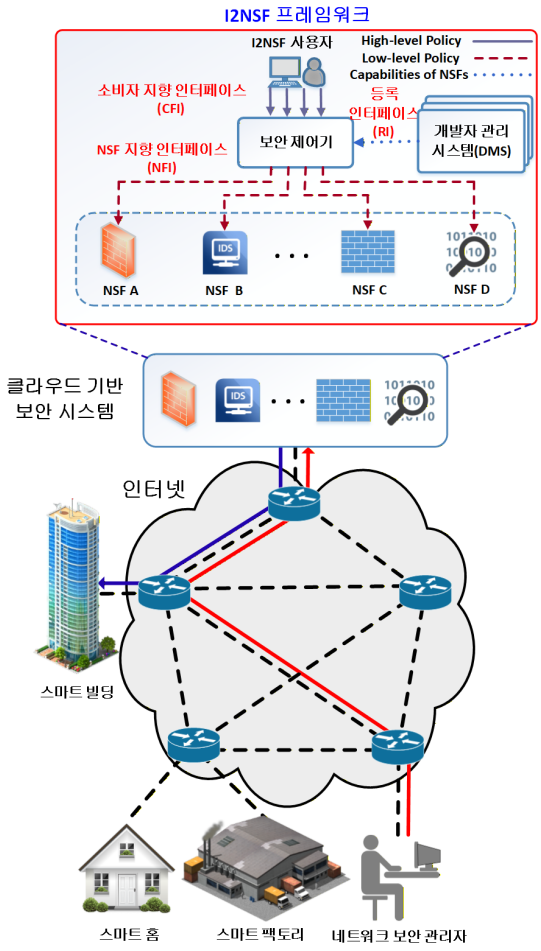

그림 1. 클라우드 기반 I2NSF 보안 시스템

YANG(Yet Another Next Generation)[7]은 네트워크 장비의 구성, 운영 상태, 알림 등을 표현하기 위한 데이터 모델링 언어이다. YANG 기반의 XML 문서는 네트워크 관리 프로토콜인 NETCONF[8] 및 RESTCONF[9]에 의해 해당 장비에 전송되어 네트워크 및 보안 자동화를 구현한다.

클라우드 및 엣지 컴퓨팅 환경에서의 지능형 보안 서비스를 위한 I2NSF 프레임워크는 컴포넌트(Component)들과 이들을 연결하는 인터페이스(Interface)들로 구성된다. I2NSF WG은 표준이 필요한 NSF의 능력(Capability)[10]과 I2NSF 인터페이스들[11-14]을 위한 데이터 모델을 표준화하였다. I2NSF의 인터페이스의 데이터 모델은 이러한 YANG을 통해 기술되었다. 본 고는 네트워크 보안 자동화를 위한 I2NSF 인터페이스들의 YANG 데이터 모델을 개념적으로 설명한다.

〈그림 1〉은 클라우드 기반 I2NSF 보안 시스템을 보여주고 있다[4]. 이러한 클라우드 기반 I2NSF 보안 시스템을 통해 네트워크 보안 관리자는 관할 구역에 있는 스마트 빌딩, 스마트 홈, 스마트 팩토리 등의 네트워크 보안 서비스를 위한 클라우드에 운용되는 네트워크 보안 함수(NSF)를 통해 다양한 보안 서비스들(예, 방화벽, 웹필터, 심층 패킷 분석, 안티 바이러스, DDoS 공격 약화기)을 제공할 수 있다[5]. 〈그림 1〉의 클라우드 기반 I2NSF 보안 시스템은 네트워크 함수 가상화(Network Functions Virtualization: NFV)와 소프트웨어 정의 네트워킹(SDN)을 통해 구현될 수 있다[15][16].

II. Interface to Network Security Functions (I2NSF)

본 장은 I2NSF 프레임워크와 인터페이스 데이터 모델을 설명한다.

1. I2NSF 프레임워크

I2NSF 프레임워크[4]는 네트워크 보안 관리자인 I2NSF 사용자(I2NSF User)가 보안 정책을 수립하고 이를 클라우드에서 보안 서비스에 해당하는 NSF를 구동시키고 모니터링 하는 것을 자동화한다. 〈그림 2〉는 I2NSF 프레임워크를 보여주고 있다.

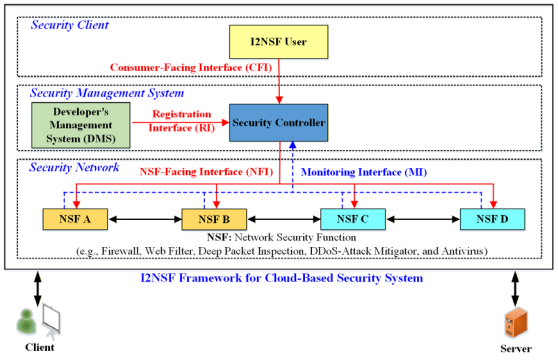

그림 2. I2NSF 프레임워크

보안 정책을 수립하는 네트워크 보안 관리자가 상위 레벨 보안 정책(High-level Security Policy)을 I2NSF 보안 제어기(Security Controller)에게 전송한다. 보안 제어기는 보안 정책 번역기(Security Policy Controller: SPT)를 통해 수신한 상위 레벨 보안 정책을 NSF가 이해할 수 있는 하위 레벨 보안 정책(Low-level Security Policy)으로 번역하고, 이를 수행할 NSF들을 선정한다. 보안 제어기는 번역된 하위 레벨 보안 정책을 해당 NSF들에게 전송한다. 하위 레벨 보안 정책을 수신한 NSF들은 해당 보안 서비스를 수행한다.

소프트웨어 정의 네트워킹(SDN)의 기술을 통해 트래픽 플로우가 거쳐가는 NSF들 간의 암호화된 통신 채널인 IPsec 터널을 효율적으로 설정할 수 있다[6].

2. NSF 능력 데이터 모델

NSF 능력 데이터 모델은 NSF가 지원하는 보안 능력(예, 방화벽, 웹필터)을 기술하기 위한 XML 문서를 생성하기 위한 것이다[10]. 〈그림 3〉은 NSF 능력을 포함하고 있는 I2NSF 프레임워크를 보여주고 있다.

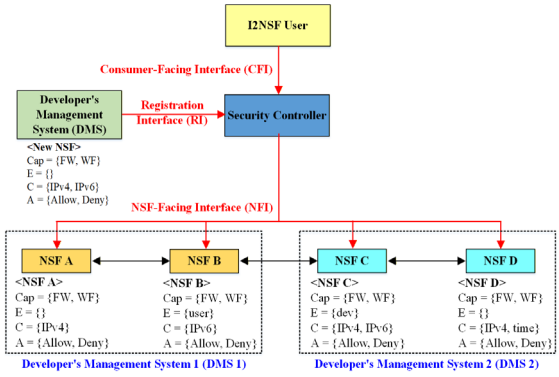

그림 3. NSF 능력 정보 포함한 I2NSF 프레임워크

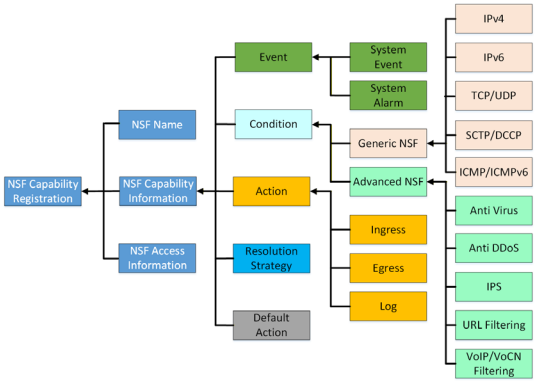

그림 4. 등록 인터페이스 데이터 모델

3. 등록 인터페이스

등록 인터페이스(Registration Interface)는 NSF 능력과 NSF 접속 정보(즉, IP 주소와 포트 번호)를 보안 제어기(Security Controller)에게 등록하기 위한 인터페이스이다[11]. 〈그림 3〉에서 개발자 관리 시스템(Developer's Management System: DMS)은 네트워크 보안 함수(NSF) 구동을 위한 시스템 이미지를 제공하고, 해당 NSF의 능력과 접속 정보를 보안 제어기에게 등록 인터페이스를 통해 등록한다.

〈그림 4〉는 등록 인터페이스의 데이터 모델을 보여주고 있다. 본 모델은 NSF Name(NSF 이름), NSF Capability Information(NSF 능력 정보), NSF Access Information(NSF 접속 정보)으로 구성된다. NSF Capability Information은 Event-Condition-Action(이벤트-컨디션-액션)에 의한 보안 함수의 능력을 기술하고 있다.

4. 소비자 지향 인터페이스

소비자 지향 인터페이스(Consumer-Facing Interface: CFI)는 I2NSF 사용자가 상위 레벨 보안 정책을 기술하고, 이를 보안 제어기에 전달하기 위한 인터페이스이다[12].

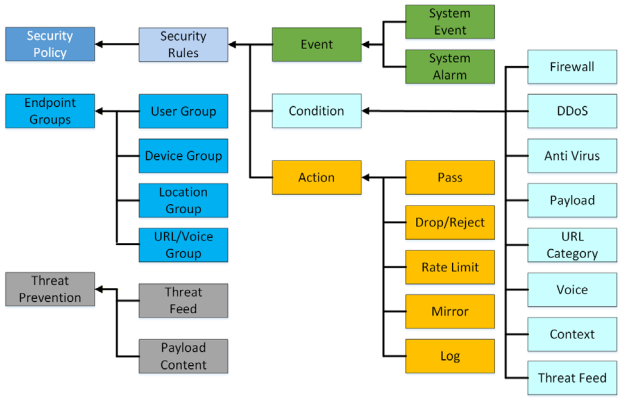

그림 5. 소비자 지향 인터페이스 데이터 모델

〈그림 5〉는 소비자 지향 인터페이스의 데이터 모델을 보여주고 있다. 보안 정책(Security Policy)는 다수의 보안 규칙(Security Rule)을 포함할 수 있다. 각 보안 규칙은 이벤트, 컨디션, 액션으로 구성된다.

이벤트는 시스템 이벤트(System Event)와 시스템 알람(System Alarm)으로 구성된다. 시스템 이벤트는 알림(Alert)라고도 하는데, 구성(Configuration)의 변경, 접근 위반, 세션 및 트래픽 플로우의 정보에 대한 경고를 나타낸다. 시스템 알람은 시스템 하드웨어에서의 서비스 품질 저하에 관련된 경고를 나타낸다.

컨디션은 다양한 보안 함수 능력에 따른 비교 항목들을 포함한다. 지원하는 보안 서비스는 방화벽(Firewall), DDoS(Distributed Denial-of-Service) 약화기(Mitigator), 안티 바이러스(Anti Virus), 심층 패킷 분석(Deep Packet Inspection: DPI)을 위한 페이로드(Payload) 분석, 웹 필터를 위한 URL 분류(URL Category), Voice over IP 또는 Voice over LTE/5G 보안을 위한 음성(Voice) 서비스 분석, 콘텍스트(Context) 분석, 위협 피드(Threat Feed) 분석 등이다. 콘텍스트는 조건을 위한 기타 정보(예, 시간, 응용, 디바이스 타입, 사용자 컨디션, 지리적 위치)를 의미한다. 위협 피드는 보안 공격 정보의 소스(Source)를 기술한다.

액션(Action)은 검사 받는 패킷의 통과(Pass), 제거(Drop/Reject), 속도 제어(Rate Limit), 복사(Mirror), 로그(Log) 등이 있다.

〈그림 5〉에서 종단 그룹(Endpoint Group)은 보안 정책에 해당되는 객체(Object)들의 그룹을 나타낸다. 종단 그룹은 사용자 그룹(User Group), 디바이스 그룹(Device Group), 위치 그룹(Location Group), URL/보이스 그룹(URL/Voice Group)을 포함한다. CFI를 통한 이러한 그룹에 해당하는 보안 정책을 수립할 수 있다. 위협 방지(Threat Prevention)은 위협 피드(Threat Feed)와 페이로드 콘텐트(Payload Content)로 구성된다. 이러한 위협 방지는 이미 알려진 보안 공격을 포함한 패킷의 내용을 포함한 것을 통해 이러한 보안 공격을 탐지하기 위한 것이다.

5. 네트워크 보안 함수 지향 인터페이스

네트워크 보안 함수 지향 인터페이스(NSF-Facing Interface: NFI)는 보안 제어기에 의해 생성된 하위 레벨 보안 정책을 해당 네트워크 보안 함수(NSF)에게 전달하기 위한 인터페이스이다[13].

〈그림 6〉은 네트워크 보안 함수 지향 인터페이스의 데이터 모델을 보여주고 있다. 보안 정책(Security Policy)은 보안 규칙(Security Rule), 해결 전략(Resolution Strategy), 규칙 그룹(Rule Group)으로 구성된다.

보안 규칙은 CFI의 보안 규칙과 동일하게 이벤트, 컨디션, 액션으로 구성된다. 이벤트는 CFI의 이벤트와 동일하다.

컨디션은 CFI의 컨디션과 유사하나 프로토콜 스택의 링크 계층의 프레임 헤드 필드들, 네트워크 계층의 IPv4/IPv6 패킷 헤드 필드들, 전송 계층의 TCP/UDP 세그먼트/데이터그램 헤드 필드들, 다른 전송 계층 프로토콜인 SCTP/DCCP 패킷 헤드 필드들, 인터넷 제어 프로토콜인 ICMP/ICMPv6 데이터그램 헤드 필드들, 웹 필터를 위한 URL 분류(URL Category)를 위

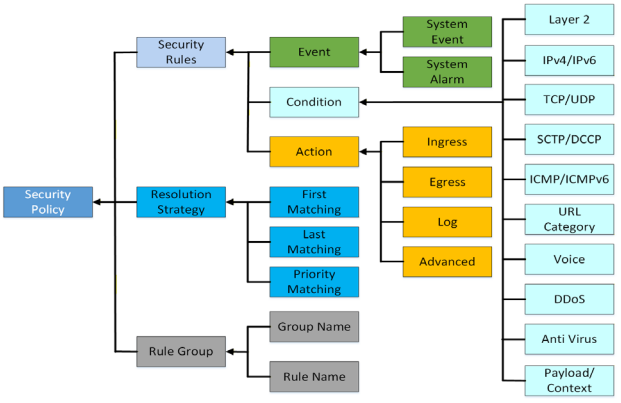

그림 6. NSF 지향 인터페이스 데이터 모델

한 HTTP/HTTPS 메시지 필드들, Voice over IP 또는 Voice over LTE/5G 보안을 위한 음성(Voice) 전송 패킷 헤드 필드들, DDoS(Distributed Denial-of-Service) 약화기(Mitigator) 관련 정보, 안티 바이러스(Anti Virus) 관련 정보, 페이로드/콘텍스트 정보를 비교 분석한다.

액션은 패킷이 들어 올 때 수행하는 Ingress Action, 패킷이 나갈 때 수행하는 Egress Action, 패킷 관련 정보를 로깅하는 Log Action, 패킷 관련 기타 액션(예, 터널링, 변환)을 위한 Advanced Action으로 구성된다.

해결 전략은 새로 설정되는 보안 규칙이 기존에 설정된 보안 규칙과 충돌이 발생할 때 이를 해결하는 규칙을 정의한다. 대표적인 해결 전략으로 처음 규칙 매칭(First Matching), 마지막 규칙 매칭(Last Matching), 우선 순위 매칭(Priority Matching)이 있다.

규칙 그룹으로 그룹 이름(Group Name)과 규칙 이름(Rule Name)이 있다. 그룹 이름은 규칙들의 그룹에 대한 이름이다. 규칙 이름은 규칙들의 이름들을 리스트로 포함한다.

6. 모니터링 인터페이스

모니터링 인터페이스(Monitoring Interface: MI)는 각 NSF가 자신이 생성한 모니터링 데이터를 분석하도록 하기 위해 NSF 모니터링 데이터 분석기(예, 보안 제어기)에게 전달하기 위한 인터페이스이다[14].

〈그림 7〉은 모니터링 인터페이스의 데이터 모델을 보여주고 있다. 모니터링 데이터(Monitoring Data)는 이벤트(Event), 로그(Log), 카운터(Counter)로 구성된다. 이벤트는 시스템 알람, 시스템 이벤트, NSF 이벤트로 구성된다. 로그는 시스템 로그와 NSF 로그로 구성된다. 카운터는 시스템 카운터와 NSF 카운터로 구성된다. 보다 자세한 정보는 MI 문서를 참고하기 바란다.

Ⅲ. 보안 관리 자동화 시스템

본 장은I2NSF 프레임워크를 통한 보안 관리 자동화 시스템을 기술한다.

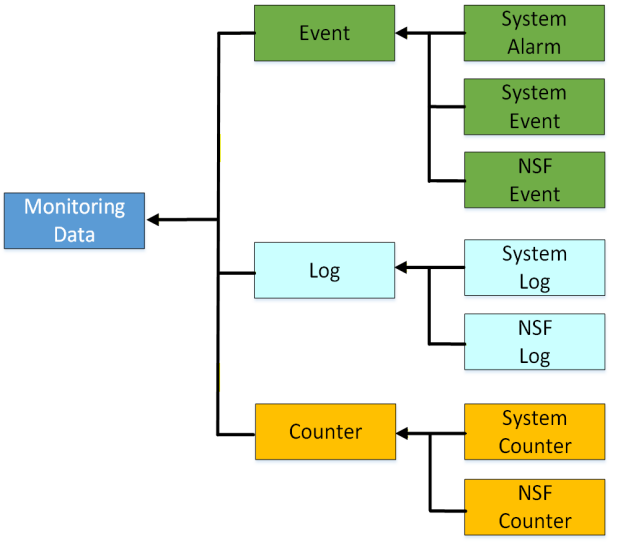

그림 7. 모니터링 인터페이스 데이터 모델

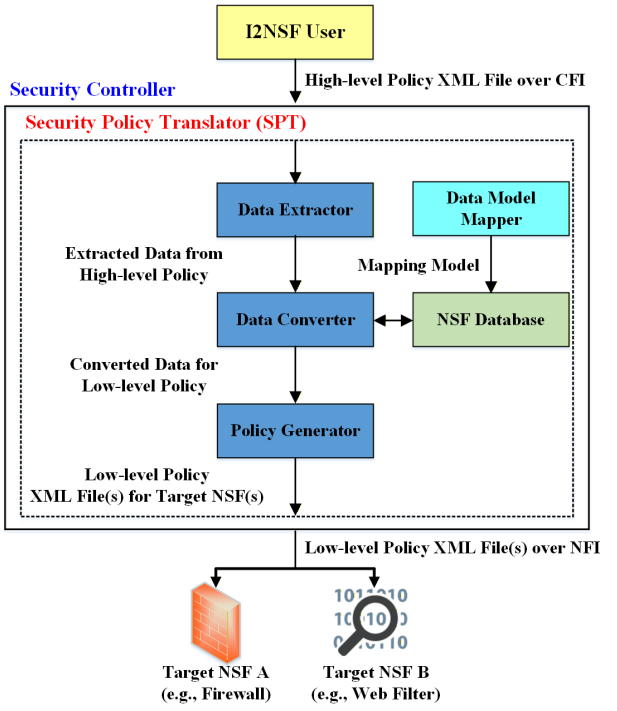

그림 8. 보안 정책 번역기

1. 보안 정책 번역기

보안 제어기는 상위 레벨 보안 정책을 하위 레벨 보안 정책으로 자동으로 번역하는 보안 정책 번역기(Security Policy Translator: SPT)를 포함하고 있다[17].

〈그림 8〉은 보안 정책 번역기의 구성 및 번역 과정을 기술하고 있다. 보안 정책 번역기는 데이터 모델 매퍼(Data Model Mapper), 데이터 추출기(Data Extractor), 데이터 변환기(Data Converter), 정책 생성기(Policy Generator), NSF 데이터베이스(NSF Database)로 구성된다.

보안 정책 번역을 위한 선행 작업으로 CFI YANG 데이터 모델과 NFI YANG 데이터 모델 간의 매핑을 수행해야 한다. 데이터 모델 매퍼는 상위 레벨 보안 정책을 구성하는 CFI YANG 데이터 모델의 모듈과 하위 레벨 보안 정책을 구성하는 NFI YANG 데이터 모델의 모듈을 매핑하는 컴포넌트이다. 즉 CFI 보안 정책의 각 필드를 NFI 보안 정책의 해당 필드로 매핑을 수행하는데, 이러한 매핑 정보를 NSF 데이터베이스에 저장한다.

I2NSF 사용자는 상위 레벨 보안 정책 XML 파일을 CFI를 통해 보안 제어기에게 전송한다. 보안 제어기의 보안 정책 번역기(SPT)는 이러한 상위 레벨 보안 정책 XML 파일을 대응하는 하위 레벨 보안 정책 XML 파일로 번역을 수행한다. 1단계로 SPT의 데이터 추출기는 상위 레벨 보안 정책 XML 파일에서 보안 정책 및 규칙에 대한 키워드를 추출하는 컴포넌트이다. 2단계로 SPT의 데이터 변환기는 상위 레벨 보안 정책의 키워드를 하위 레벨 보안 정책의 키워드로 변화하기 위한 컴포넌트이다. 3단계로 SPT의 정책 생성기는 하위 레벨 보안 정책의 키워드들을 가지고 NFI YANG 데이터 모델에 부합하는 하위 레벨 보안 정책 XML 파일을 생성한다.

보안 제어기는 보안 정책 및 규칙 정보를 기반으로 해당 보안 서비스들을 수행할 네트워크 보안 함수들(NSFs)을 선택한다. 보안 제어기는 해당 NSF들에게 하위 레벨 보안 정책을 전송한다. 하위 레벨 보안 정책을 수신한 NSF들은 해당 보안 서비스를 수행한다.

〈그림 9〉는 시간 기반 방화벽 서비스를 보여주고 있다. 상위 레벨 보안 정책은 회사 네트워크에 연결된 사원들(Employees)은 업무시간(오전 9시~오후 6시)까지 소셜 네트워킹 서비스(Social Networking Service: SNS) 웹사이트들(예, facebook, instagram)에 접속하지 못하게 하는 한다. 이러한 정책이 SPT에게 전달되면 SPT의 데이터 추출기는 Employee 키워드와 SNS Websites 키워드를 추출한다. SPT의 데이터 변환기는 NSF 데이터베이스를 참고해서 Employee들을 사용하고 있는 컴퓨터나 모바일 디바이스의 IP 주소들(또는 IP 서브넷)로 변환한다. SPT 정책 생성기는 PyangBind 오픈 소스를 통해 변환된 키워드들을 NFI YANG 데이터 모델에 부합하는 하위 레벨 보안 정책 XML 파일들을 생성한다. 이러한 XML 파일들은 해당 NSF들, 즉 방화벽(Firewall)과 웹 필터(Web Filter)에게 전송된다.

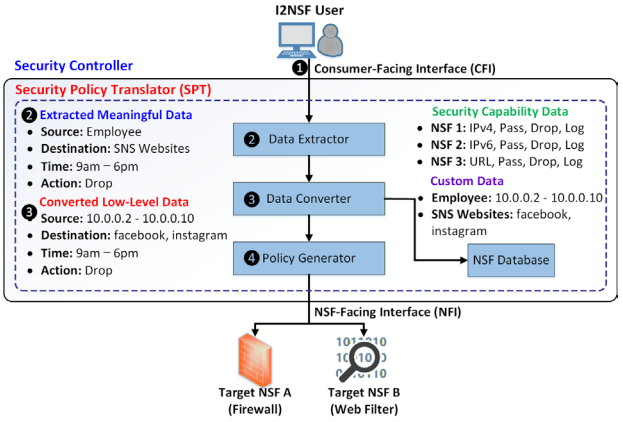

그림 9. 시간 기반 방화벽 서비스

2. 폐쇄 루프 보안 제어

I2NSF 사용자가 설정한 보안 정책이 보안 시스템에서 의도대로 정확히 수행되고 있음을 검정(Validation)할 필요가 있다. 이러한 검정은 폐쇄 루프 보안 제어(Closed-Loop Security Control)를 통해 수행될 수 있다[18].

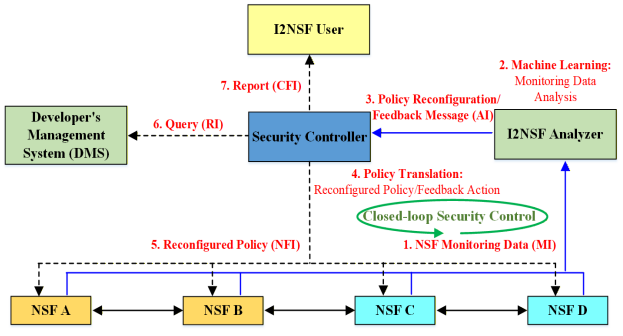

그림 10. 폐쇄 루프 보안 제어 I2NSF 프레임워크

〈그림 10〉은 폐쇄 루프 보안 제어를 지원하는 I2NSF 프레임워크를 보여주고 있다. 이러한 폐쇄 루프 보안 제어를 위해 NSF 모니터링 데이터를 분석하는 I2NSF 분석기(I2NSF Analyzer)와 분석 결과인 정책 재설정(Policy Reconfiguration)과 피드백 메시지(Feedback Message)를 보안 제어기에게 전달하기 위한 분석 인터페이스(Analytics Interface: AI)가 추가되어 있다.

3. 자연어 인텐트 기반 보안 정책 설정

거대 언어 모델(Large Language Model: LLM)의 발전으로 보안 정책을 자연어로 말하거나 글로 작성하면 이를 상위 레벨 보안 정책으로 번역할 수 있다[19]. LLM인 T5-Flan[20] 또는 GPT-3[21]를 통해 프롬프트 러닝을 통해 자연어 보안 정책의 인텐트(Intent)를 CFI 상위 레벨 보안 정책으로 번역할 수 있다[22].

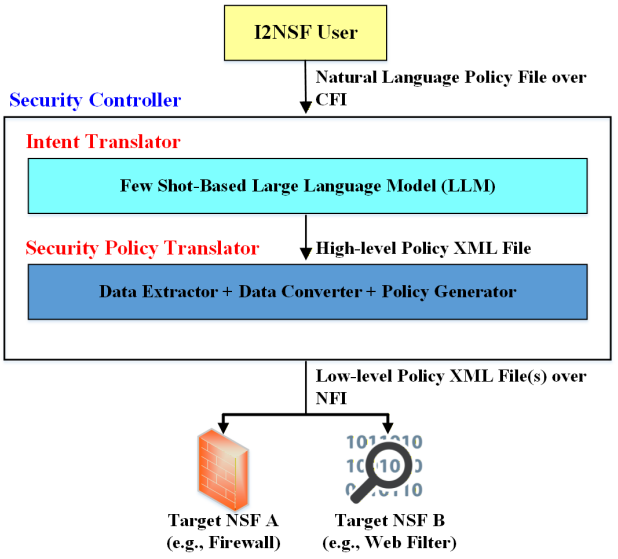

그림 11. 자연어 보안 정책 번역 과정

〈그림 11〉은 I2NSF 사용자의 자연어 보안 정책 번역이 의도 번역기를 통해 상위 레벨 보안 정책이 생성되고, 이러한 상위 레벨 보안 정책인 보안 정책 번역기에 의한 하위 레벨 보안 정책으로 번역되는 과정을 보여주고 있다.

Ⅳ. 엣지 기반 I2NSF 보안 시스템

본 장은 I2NSF 프레임워크가 5G 네트워크에서의 보안 서비스를 효과적으로 지원할 수 있는 엣지 기반 I2NSF 보안 시스템을 기술한다.

1. 5G 네트워크에서의 기존의 I2NSF 적용 제약점

I2NSF 프레임워크를 5G 네트워크에 적용할 때 네트워크 보안 함수를 5G 코어 네트워크 외부에 있는 클라우드에 운용하게 되면 보안 서비스를 위해 사용자 단말(User Equipment: UE)의 패킷이 NSF가 있는 클라우드를 경유해서 데이터 통신을 하고 있는 서버 또는 다른 단말에게 비최적화 경로로 전달되는 단점이 있다[23].

〈그림 1〉에서 스마트 빌딩에 있는 사원이 스마트폰으로 업무에 필요한 서버에 접속할 때 클라우드에 있는 방화벽 같은 보안 서비스를 거쳐서 해당 서버로 데이터 통신을 하므로 불필요한 지연 시간이 발생한다. 이처럼 클라우드 기반의 보안 서비스로 인해 발생하는 비최적화 패킷 경로 문제를 해결할 필요가 있다.

2. 5G 네트워크를 위한 엣지 기반 보안 시스템

I2NSF 프레임워크를 5G 코어 네트워크와 결합해서 사용자 단말(UE)가 현재 위치한 무선 접속 네트워크에 연결된 라우터에 해당하는 사용자 플레인 함수(User Plane Function: UPF) 내부에 관련 네트워크 보안 함수(NSF)를 운용하면 비최적화 문제를 해결할 수 있다[23].

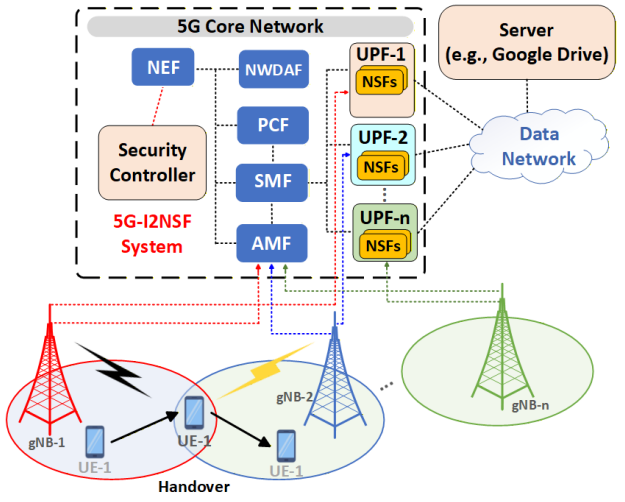

그림 12. 5G 네트워크를 위한 I2NSF 엣지 보안 시스템

〈그림 12〉는 5G 네트워크를 위한 I2NSF 엣지 보안 시스템을 보여주고 있다. 사용자 단말 UE-1이 현재 연결된 무선 접속 네트워크의 기지국(gNodeB: gNB)인 gNB-1의 인접 UPF인 UPF-1에 NSF들에게 보안 서비스를 받는다. UE-1이 인접 무선 접속 네트워크로 이동할 때 새로운 무선 접속 네트워크를 담당하는 gNB-2에 연결된 UPF-2에 UE-1을 위한 보안 서비스를 수행하는 NSF들을 운용한다. 이렇게 함으로써 UE와 서버 간의 최적화 경로 상의 NSF들을 통해 보안 서비스를 받을 수 있으므로 경로 최적화 문제를 해결할 수 있다.

V. 결론

본 고에서는 I2NSF 프레임워크를 이용한 클라우드-엣지 기반 보안 시스템 및 표준 문서들을 소개하였다. 특히 보안 서비스 자동화를 위한 I2NSF 프레임워크 확장은 IETF의 리서치 기구인 IRTF(Internet Research Task Force)의 네트워크 관리 리서치 그룹(Network Management Research Group: NMRG)에서 의도 기반 네트워킹(Intent-Based Networking: IBN) 유스케이스 문서에서 표준화되고 있다. 본 저자의 연구팀은 5G 네트워크를 위한 I2NSF와 자연어 기반 보안 정책 번역을 위한 의도 번역기 기술을 IETF 해커톤 프로젝트 및 인터넷 기고서를 통해 계속 표준화를 진행할 예정이다.

Acknowledgements

이 논문은 2025년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구이고(No. RS-2024-00398199), 한국연구재단의 지원을 받아 수행된 연구임(No. 2023R1A2C2002990).

참 고 문 헌

[1] IETF (Internet Engineering Task Force) Website, https://www.ietf.org/

[2] I2NSF (Interface to Network Security Functions) Working Group Website, https://datatracker.ietf.org/wg/i2nsf/about/

[3] I2NSF WG Documents, https://datatracker.ietf.org/wg/i2nsf/documents/

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

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

[6] R. Marin-Lopez, G. Lopez, F. Pereniguez-Garcia, "A YANG Data Model for IPsec Flow Protection Based on Software-Defined Networking (SDN)", IETF, RFC 9061, July 2021.

[7] M. Bjorklund, "YANG - A Data Modeling Language for the Network Configuration Protocol (NETCONF)", IETF, RFC 6020, October 2010.

[8] R. Enns, M. Bjorklund, J. Schoenwaelder, and A. Bierman, "Network Configuration Protocol (NETCONF)", IETF, RFC 6241, June 2011.

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

[10] S. Hares, J. Jeong, J. Kim, R. Moskowitz, and Q. Lin, "I2NSF Capability YANG Data Model", Internet-Draft, draft-ietf-i2nsf-capability-data-model-32, May 2022.

[11] S. Hyun, J. Jeong, T. Roh, S. Wi, and J. Park, "I2NSF Registration Interface YANG Data Model for NSF Capability Registration", Internet-Draft, draft-ietf-i2nsf-registration-interface-dm-26, May 2023.

[12] J. Jeong, C. Chung, T. Ahn, R. Kumar, and S. Hares, "I2NSF Consumer-Facing Interface YANG Data Model", Internet-Draft, draft-ietf-i2nsf-consumer-facing-interface-dm-31, May 2023.

[13] J. Kim, J. Jeong, J. Park, S. Hares, and Q. Lin, "I2NSF Network Security Function-Facing Interface YANG Data Model", Internet-Draft, draft-ietf-i2nsf-nsf-facing-interface-dm-29, June 2022.

[14] J. Jeong, P. Lingga, S. Hares, L. Xia, and H. Birkholz, "I2NSF NSF Monitoring Interface YANG Data Model", Internet-Draft, draft-ietf-i2nsf-nsf-monitoring-data-model-20, June 2022.

[15] 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-19, April 2025.

[16] J. Jeong and P. Lingga, "CBSS: Cloud-Based Security System with Interface to Network Security Functions", The 14th International Conference on Mobile Computing and Ubiquitous Networking (ICMU 2023), Kyoto, Japan, November 2023.

[17] P. Lingga, J. Jeong, J. Yang, and J. Kim, "SPT: Security Policy Translator for Network Security Functions in Cloud-Based Security Services", IEEE Transactions on Dependable and Secure Computing, Vol. 21, No. 6, November/December 2024.

[18] P. Lingga, J. Jeong, and L Dunbar, "ICSC: Intent-Based Closed-Loop Security Control System for Cloud-Based Security Services", IEEE Communications Magazine, December 2024.

[19] M. Rodriguez, J. Berasategui, and J. Jeong, "Security Policy Generation for Cloud-Based Security Services using Large Language Model", KICS-2025-Winter, Pyeongchang, Korea, February 2025.

[20] H. Chung et al., "Scaling Instruction-Finetuned Language Models", arXiv arXiv:2210.11416, Available: https://arxiv.org/abs/2210.11416, October 2022.

[21] T. Brown et al., "Language Models are Few-Shot Learners", arXiv arXiv:2005.14165, Available: https://arxiv.org/abs/2005.14165, May 2020.

[22] M. Gu and J. Jeong, "An Intent Translation Framework for Internet of Things", Internet-Draft, draft-gu-nmrg-intent-translator-02, October 2025.

[23] Y. Ahn, J. Jeong, and Y. Kim, "An Integrated Security Service System for 5G Networks using an I2NSF Framework", Internet-Draft, draft-ahn-nmrg-5g-security-i2nsf-framework-00, October 2025.

약 력

정 재 훈

1999년 성균관대학교 정보공학과 학사
2001년 서울대학교 컴퓨터공학과 석사
2009년 University of Minnesota 컴퓨터공학과 박사
2001년~2004년 한국전자통신연구원 표준연구센터 연구원
2010년~2012년 Brocade Communications Systems 소프트웨어 엔지니어
2015년~현재: TTA ICT 국제표준화 전문가
2012년~현재: 성균관대학교 소프트웨어학과 교수
관심분야: 의도 기반 네트워킹, 차량 네트워킹, 사물인터넷, 네트워크 보안, IETF 표준화