TTA Standard

정보통신단체표준(국문표준)
TTAx.xx-xx.xxxx/R1

제정일: 2019 년 xx 월 xx 일
개정일: 200x 년 xx 월 xx 일

SDN 기반의 네트워크 보안 기능의 인터페이스(I2NSF) 프레임워크 - 제 7부 : 보안 정책 번역기의 구조 및 절차

Interface to Network Security Functions (I2NSF) Framework Using Software-Defined Networking - Part7: Architecture and Process of Security Policy Translator

TTA 한국정보통신기술협회
Telecommunications Technology Association

표준초안 검토 위원회	**사이버보안 프로젝트그룹(PG503)**				
표준안 심의 위원회	**정보보호 기술위원회(TC5)**				
	성명	**소 속**	**직위**	**위원회 및 직위**	**표준번호**
표준(과제) 제안	정재훈	성균관대학교	부교수	PG503 - 위원	
표준 초안 작성자	정재훈	성균관대학교	부교수	PG503 - 위원	
	정재홍	성균관대학교	석사과정		
	양진혁	성균관대학교	석사과정		
사무국 담당	박수정	TTA	책임	사무국	

본 표준 발간 이전에 접수된 지식재산권 확약서 정보는 본 표준의 '부록(지식재산권 확약서 정보)'에 명시하고 있으며, 이후 접수된 지식재산권 확약서는 TTA 웹사이트에서 확인할 수 있습니다.
본 표준과 관련하여 접수된 확약서 외의 지식재산권이 존재할 수 있습니다.

발행인 : 한국정보통신기술협회 회장
발행처 : 한국정보통신기술협회
13591, 경기도 성남시 분당구 분당로 47
Tel : 031-724-0114, Fax : 031-724-0109
발행일 : 2018.08

서 문

1 표준의 목적

본 문서는 I2NSF(Interface to Network Security Functions) 프레임워크[1]에서의 보안 정책 변환을 위한 보안 정책 번역기(Security Policy Translator)의 구조 및 절차(Architecture and Process)를 기술한다. I2NSF 사용자가 보안 서비스에 대한 고수준 보안 정책을 제공하면 보안 제어기(Security Controller)의 보안 정책 번역기가 네트워크 보안 기능(Network Security Functions, NSFs)에 대한 저수준 보안 정책으로 변환한다.

2 주요 내용 요약

일반적으로 보안을 요구하는 사용자는 NSF에 대한 전문적인 지식을 모르기 때문에 사용자가 NSF의 전문적인 관여 없이 서비스를 받을 수 있도록 시스템을 설계해야 한다. 이를 위해 I2NSF는 비전문가인 사용자가 NSF 정책을 설정하도록 도와주는 정책 변환기를 필요로 한다. 본 문서에서는 보안 정책 번역기의 새로운 설계를 제안한다. I2NSF 시스템의 편리한 관리를 위해 오토마타 이론을 사용하여 정책 번역기를 구성한다. 먼저, 결정적 유한 오토마타(Deterministic Finite Automaton, DFA)를 사용하여 고급 정책에서 데이터를 추출하는 추출자(Extractor)를 구축한다. 두 번째로 NSF에 필요한 추상 데이터로부터 특정 데이터로 데이터를 매핑(mapping)하기 위해 NSF 데이터베이스 기반 데이터 변환기(Data Converter)를 구축한다. 마지막으로 문맥-자유 문법(Context-free Grammar, CFG)을 사용하여 각 NSF를 위한 저수준 정책을 생성하는 생성자(Generator)를 구축한다.

3 인용 표준과의 비교

3.1 인용 표준과의 관련성

- 해당 사항 없음

3.2 인용 표준과 본 표준의 비교표

- 해당 사항 없음

Preface

1 Purpose

This document describes the architecture and process of a security policy translator for security policy translation in the I2NSF (Interface to Network Security Functions) framework. When a user provides a high-level security policy for security services, the security policy translator of the security controller translates it into a low-level security policy for network security functions (NSFs).

2 Summary

In general, users who require security must know that NSF has no expert knowledge, so the system must be designed so that users can get services without the professional involvement of NSF. To this end, I2NSF requires a policy converter to help non-expert users set up NSF policies. This document proposes a new design of the security policy translator. To facilitate the management of the I2NSF system, a policy translator is constructed using automata theory. First, we construct an extractor that extracts data from the advanced policy using deterministic finite automaton (DFA). Second, we build an NSF database-based data converter to map data from abstract data to NSF specific data. Finally, we construct a generator that creates a low-level policy for each NSF using a context-free grammar (CFG).

3 Relationship to Reference Standards

N/A
(*국문 서문의 3.1항 부분을 작성하되, 필요 시 3.2항의 비교표 작성)

목 차

SDN 기반의 네트워크 보안 기능의 인터페이스(I2NSF) 프레임워크 - 제7부 : 보안 정책 번역기의 구조 및 절차 (Interface to Network Security Functions (I2NSF) Framework Using Software-Defined Networking - Part7: Architecture and Process of Security Policy Translator)

1 적용 범위

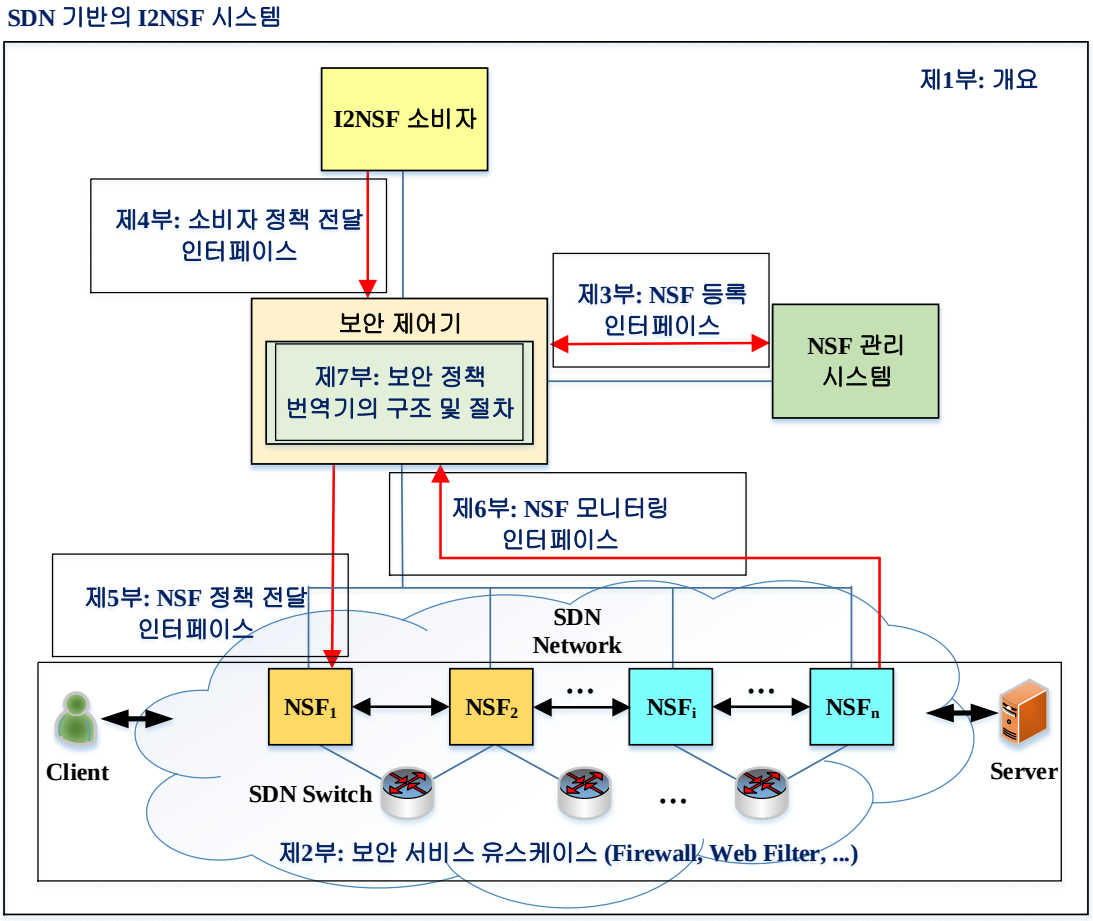
TTAK.KO-12.0314(SDN 기반의 네트워크 보안 기능의 인터페이스(I2NSF) 프레임워크 - 제1부: 개요)[I-3-1]는 서로 다른 솔루션 벤더에서 개발된 NSF(Network Security Function)을 유연하게 사용하기 위하여 I2NSF(Interface to Network Security Functions) 프레임워크를 정의한다. 네트워크를 운영하는 보안 관리자(또는 시스템 관리자)는 네트워크에 적용할 고수준 보안 정책(High-level Security Policy)를 보안 제어기(Security Controller)에게 전달한다. 보안 제어기는 이 고수준 보안 정책을 수행할 네트워크 보안 함수(Network Security Function, NSF)를 선정하고, 이 NSF가 이해할 수 있는 저수준 보안 정책(Low-level Security Policy)으로 번역한다. 본 문서는 I2NSF 프레임워크에서 보안 제어기에서 보안 정책 번역을 수행하는 보안 정책 번역기의 설계 및 구현을 위한 표준을 기술한다. 본 문서는 고수준 보안 정책과 저수준 보안 정책 간의 관계, 번역기의 구조, 번역 프로세스를 기술한다.

TTAK.KO-12.0314-part2(SDN 기반의 네트워크 보안 기능의 인터페이스(I2NSF) 프레임워크 - 제2부: 보안 서비스 유스케이스)[I-3-2]는 I2NSF를 적용할 수 있는 유스케이스(예, 방화벽, 웹 필터, DDoS 공격 약화기, 악의적인 VoIP/VoLTE 트래픽 차단)를 소개하고, 보안 정책 XML 코드를 보여준다. 이 유스케이스 문서에 있는 고수준 보안 정책 XML 코드를 저수준 보안 정책 XML 코드를 번역할 수 있는 번역기를 본 문서에게 기술한다.

<표 1-1>과 (그림 1-1)는 보안 정책 번역기의 구조 및 절차의 연계(Family) 표준을 나타내는 표와 그림이다.

<표 1-1> SDN 기반의 I2NSF 시스템의 연계 표준 문서

순서	표준 번호	표준 제목
1	TTAK.KO-12.0314-Part1	제1부: 개요
2	TTAK.KO-12.0314-Part2	제2부: 보안 서비스 유스케이스
3	TTAK.KO-12.0314-Part3	제3부: NSF 등록 인터페이스
4	TTAK.KO-12.0314-Part4	제4부: 소비자 정책 전달 인터페이스
5	TTAK.KO-12.0314-Part5	제5부: NSF 정책 전달 인터페이스
6	TTAK.KO-12.0314-Part6 (예정)	제6부: NSF 모니터링 인터페이스
7	TTAK.KO-12.0314-Part7 (예정)	제7부: 보안 정책 번역기의 구조 및 절차



(그림 1-1) SDN 기반의 I2NSF 시스템의 연계 표준 적용 범위

이 문서는 기본적으로 데이터 모델이 있는 둘 이상의 인터페이스 사이의 연결을 담당하는 모든 컴포넌트에 적용이 가능하다. 본 문서에서 제안하는 번역기는 인터페이스의 데이터 모델 구조를 기반으로 유동적으로 구축이 가능하기 때문에 중간자 컴포넌트에게 큰 이점을 제공한다. 정책 번역기는 중간자가 전달받은 정책을 하위 인터페이스의 데이터 모델에 맞추어 번역이 가능하도록 만들어주며, 사용자가 효율적으로 관리할 수 있게 설계되었다.

또한, 전달받은 정책에 적합한 컴포넌트를 동적으로 검색하는 기능을 제공한다. I2NSF를 이용하는 사용자가 원하는 정보만으로 하위 인터페이스 너머의 컴포넌트를 자동으로 탐색이 가능하다. 이 이점은 I2NSF 프레임워크에 적용될 수 있는 특수성을 가진다.

2 인용 표준 (스타일 적용-대항목/소항목)

해당 없음.

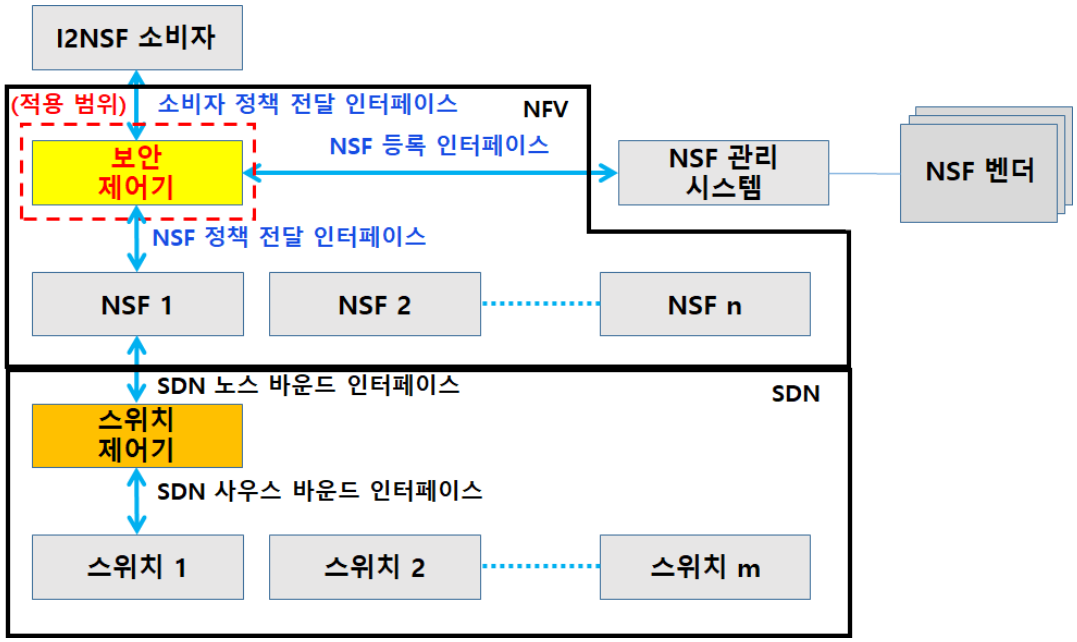
3 용어 정의 (스타일 적용-대항목/소항목)

이 문서는 RFC8329 문서[1]와 I2NSF 용어문서[2]의 용어 정의를 따른다.

4 약어

CFG	Context-free Grammar
DFA	Deterministic Finite Automaton
I2NSF	Interface to Network Security Function
NSF	Network Security Function

5 I2NSF 시스템을 위한 보안 정책 번역기



(그림 5-1) I2NSF 프레임워크

본 문서는 I2NSF (Interface to Network Security Functions) 프레임워크에서의 보안 정책 번역 체계를 정의한다[1][I-3-1]. (그림 5-1)은 I2NSF 프레임워크를 보여준다.

정책 번역기는 I2NSF 프레임워크의 보안 제어기(Security Controller)에 있으며 고수준 보안 정책을 네트워크 보안 기능(Network Security Functions, NSFs)의 하위 수준 보안 정책으로 변환한다. 고수준 정책은 I2NSF 프레임워크의 I2NSF 소비자에 의해 생성되고 소비자 정책 전달 인터페이스(Consumer-Facing Interface)[I-3-4]를 통해 보안 제어기에 전달된다. 저수준 정책은 보안 제어기에서 번역하고 NSF 정책 전달 인터페이스(NSF-Facing Interface)[I-3-5]를 통해 저수준 정책에 해당하는 규칙을 해당 NSF들에 설정한다.

우선 이 문서는 I2NSF 프레임워크에서의 보안 정책 번역기의 필요성을 제시한다. 다음으로 보안 정책 번역기의 구조를 설명한다. 마지막으로 이 문서에서 제시한 보안 정책 번역기를 적용하였을 때 가지는 유익한 기능을 설명한다.

5.1 보안 정책 번역기의 필요성

I2NSF 프레임워크의 목적은 다양하고 복잡한 네트워크 보안 기능들을 사용자가 편리하게 이용할 수 있도록 통합 인터페이스를 제공하는 것이다. I2NSF 프레임워크가 본 문서에서 제안하는 보안 정책 번역기를 필요로 하는 이유는 사용자가 NSF에 대한 전반적인 지식이 없어도 보안 정책을 쉽게 내려주기 위함이다.

보안을 요구하는 사용자는 일반적으로 NSF에 대한 지식을 가지고 있지 않다. 예를 들면, 사용자가 NSF의 사용을 원할 때, 보통 “아들의 컴퓨터가 유해한 사이트에 접속하는 것을 막아주시오”라고 원하지, 절대 “웹사이트 필터링 NSF에 115.145.178.177의 IP 주소에서 www.example.com 웹사이트로 이동하는 패킷을 막도록 설정하시오”라고 요구하지 않는다. 보안을 요구하는 사용자는 단순히 유해한 특정 웹사이트에 접속하는 것을 막아달라는 추상적인 정보만을 전달할 수 있다. 만약 두 번째와 같이 보안 정책을 생성해야 한다면, NSF에 대한 전문적인 지식이 없이는 절대 정책을 내려주지 못할 것이며, 이는 편리하게 NSF를 제공한다고 볼 수 없다.

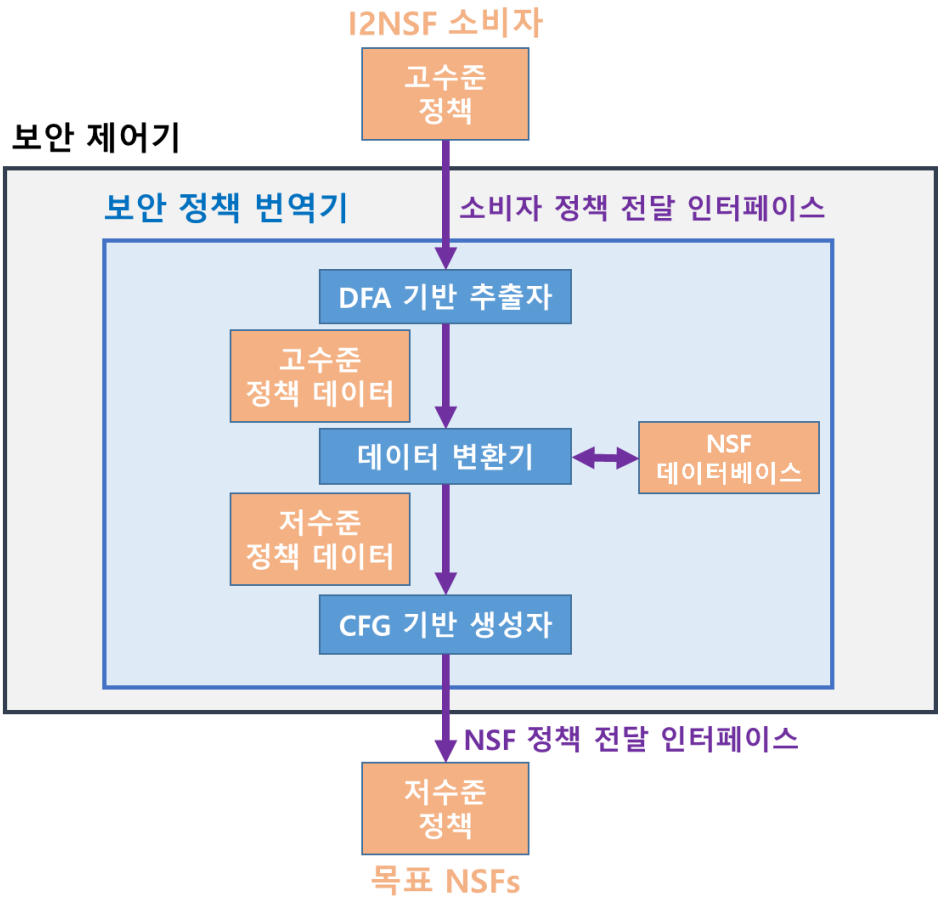
사용자가 NSF에 대한 전문적인 지식 없이 정책을 생성할 수 있도록 하기 위해서는 아래와 같이 세 가지의 기능을 지원해야 한다.

첫째, 서로 다른 데이터 모델을 가지는 두 인터페이스 간의 정보 전달을 맞춰주어야 한다. 각 인터페이스는 목적 및 기능에 부합한 고유의 데이터 모델을 가지고 있으며, 정보 전달을 위해서는 고유의 데이터 모델에 맞게 정책을 변환하여 전달해 주어야 한다. I2NSF 프레임워크는 사용자와 NSF 사이의 중간자 역할이기 때문에 정책을 데이터 모델에 맞추어 변환해주는 번역기를 필요로 한다.

둘째, 고수준 정책이 담고 있는 추상적인 데이터를 NSF가 이해할 수 있는 구체적인 데이터로 변환해주어야 한다. 예를 들어, NSF는 “아들의 컴퓨터”나 “유해한 사이트”와 같이 추상적인 데이터들을 해석하는 능력이 없다. 즉, NSF에 정상적으로 정책을 설정하기 위해서는 “IP 주소 115.145.178.177”이나 “웹사이트 www.example.com”과 같이 NSF가 해석할 수 있는 구체적인 데이터로 변환해주어야 한다.

셋째, 사용자가 생성한 고수준 보안 정책을 실현하기 위해 필요한 NSF를 자동으로 찾아주어야 한다. 유해 사이트의 접속을 막기 위해 필요한 NSF는 “웹사이트 필터”이다. 사용자가 NSF에 대한 전문적인 지식 없이 정책을 내리고 싶을 때, 정책을 실현하기 위해 필요한 NSF를 자동으로 찾아주어야 하며, 이 기능을 정책 프로비저닝(provisioning)이라 부른다.

5.2 보안 정책 번역기의 구조

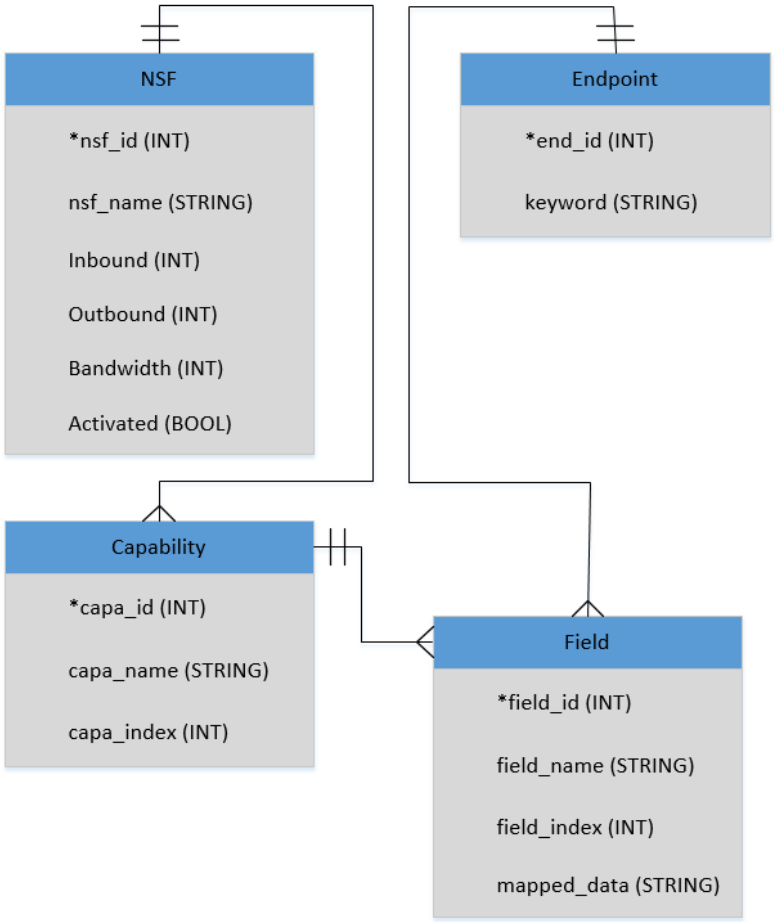


(그림 5-2) 보안 정책 번역기의 구조

(그림 5-2)는 보안 정책 번역기의 구조를 보여준다. 보안 정책 번역기는 크게 세 개의 컴포넌트로 나누어져 있다. 우선 I2NSF 사용자로부터 전달받은 고수준 정책을 결정적

유한 오토마타(Deterministic Finite Automaton, DFA)를 기반으로 구성된 추출자(Extractor)가 데이터를 추출한다. 다음으로, 추출된 데이터를 데이터 변환기(Data Converter)가 NSF의 능력(Capability)에 적합한 형태로 변환한다. 마지막으로, 문맥-자유 문법(Context-free Grammar, CFG)을 기반으로 구성된 생성자(Generator)가 변환된 데이터를 이용하여 NSF를 위한 저수준 보안 정책을 생성한다.

5.2.1 NSF 데이터베이스



(그림 5-3) NSF 데이터베이스의 개체-관계 다이어그램

NSF 데이터베이스에는 고수준 보안 정책 데이터를 저수준 보안 정책 데이터로 변환하는 데 필요한 모든 정보가 들어있다. NSF 데이터베이스의 내용은 "엔드포인트 정보"와 "NSF 기능 정보"로 분류된다.

"엔드포인트 정보"는 "아들의 PC", "악의적 웹사이트"와 같이 추상적인 고수준 정책 데이터를 "10.0.0.1", "illegal.com"과 같은 구체적인 저수준 정책 데이터로 변환하는 데 필요

하다. 사용자가 보안 정책이 적용될 목표를 지정할 때, 구체적인 저수준 정책 데이터를 사용한다면 NSF의 접근성이 떨어진다. 따라서 사용자의 편의성을 고려하기 위해서는 추상적인 고수준 정책 데이터를 사용자로부터 수신해야 하며, 보안 제어기는 이를 엔드포인트 정보로써 NSF 데이터베이스에 저장해야 한다. 엔드포인트 정보는 I2NSF 사용자가 소비자 정책 전달 인터페이스를 거쳐 고수준 정책으로 제공하고, 보안 제어기는 수신한 정보를 NSF 데이터베이스에 저장한다.

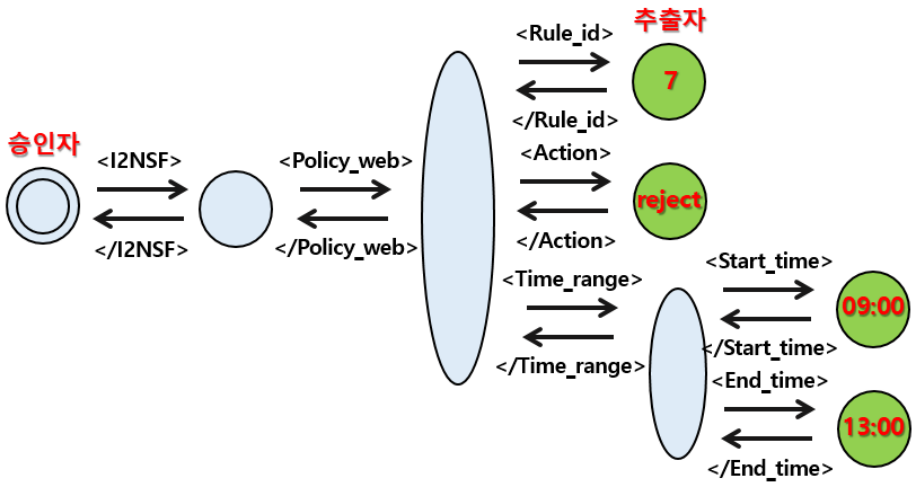
"NSF 기능 정보"는 NSF가 지원 가능한 기능들에 대한 정보이다. NSF 기능 정보는 보안 정책의 설립에 필요한 NSF들을 탐색할 때 사용된다. NSF 기능 정보는 등록 인터페이스를 통해 NSF 관리 시스템에서 제공하고, 보안 제어기는 수신한 정보를 NSF 데이터베이스에 저장한다. 또한 NSF가 NSF 정책 전달 인터페이스를 거쳐 보안 제어기에 모니터링 정보를 전송하면, 보안 제어기는 이를 참고하여 NSF 데이터베이스를 유동적으로 수정할 수 있다.

(그림 5-3)은 NSF 데이터베이스의 개체-관계 다이어그램(Entity-Relationship Diagram)을 보여준다. 이 다이어그램은 NSF 관리 시스템에서 제공받은 NSF 기능 정보와 I2NSF 유저에게 받은 엔드포인트 정보로 설계되었다. NSF, Capability, Endpoint, 그리고 Field라는 명칭의 네 가지 객체로 구성되며, 각 객체에는 키 값을 갖는 속성(*key value) 외의 다양한 속성 값과 변수 타입을 나타낸다. 그리고 각 관계선은 일대다의 관계 정보를 나타낸다. NSF 데이터베이스의 다이어그램은 보안 정책 번역기가 필요한 모든 정보를 보여주어 네트워크 시스템 관리자에게 NSF 데이터베이스 관리의 효율성을 줄 수 있다.

5.2.2 결정적 유한 오토마타(DFA) 기반 추출자(Extractor)

사용자는 인터페이스의 데이터 모델을 기반으로 데이터를 담아 고수준 보안 정책을 생성하고 전달한다. 따라서 데이터 모델을 서로의 컴포넌트가 정확하게 알고 있다면, 데이터가 담겨 있는 위치를 알 수 있다.

데이터의 위치를 쉽게 찾을 수 있기 위한 아이디어로 DFA를 사용하는 것을 제안한다. DFA는 유한 개의 상태(state)를 전이시킬 때마다 특정 동작을 수행하는 기계 구조이다. 계층 구조를 명시해주기 위한 데이터 모델의 특정 키워드가 입력될 때마다 상태를 이전시켜 데이터를 포함하고 있는 위치를 빠르게 찾아나가고 해당 데이터를 추출한다. DFA 기반 추출자는 아래와 같이 구성된다. 데이터 모델의 계층 구조를 그대로 반영하여 쉽고 유동적으로 구축할 수 있다.



(그림 5-4) DFA 기반 추출자의 구조

```
<I2NSF>
  <Policy_web>
      <Rule_id>7</Rule_id>
      <Action>reject</Action>
      <Time_range>
          <Start_time>09:00</Start_time>
          <End_time>13:00</End_time>
      </Time_range>
  </Policy_web>
</I2NSF>
```

(그림 5-5) 고수준 정책의 예시

(그림 5-4)는 DFA 기반 추출자의 구조를 보여준다. 그리고, (그림 5-5)는 DFA 기반 추출자의 동작 과정을 설명하기 위한 고수준 정책의 예시이다. DFA 기반 추출자는 쉽게 (그림 5-5)와 같은 고수준 정책의 데이터를 추출할 수 있다. DFA의 시작 지점은 '승인자'이다. 먼저 고수준 정책의 첫 입력인 <I2NSF> 태그를 읽으며, 상태를 '중간자'로 전이한다. 그 후, <Policy_web> 태그를 읽으며, 상태를 또 다른 '중간자'로 전이한다. 다음으로, <Rule_id> 태그를 읽으며 상태를 '추출자'로 전이한다. <Rule_id> 태그 안에는 고수준 정책의 데이터가 담겨 있으므로 해당하는 데이터를 읽으며 추출한다. 데이터 추출 이후 종료 태그인 </Rule_id>를 읽으며 이전의 '중간자' 상태로 전이한다. 만약 모든 고수준 정책을 DFA가 읽었다면 상태는 처음 시작점인 '승인자'로 돌아가게 된다. DFA를 이용하면 고수준 정책 내의 데이터를 쉽게 추출할 수 있다. 추출이 완료된 데이터는 다음 컴포넌트인 데이터 변환기에 전달한다.

5.2.3 데이터 변환기(Data Converter)

데이터 변환은 I2NSF 프레임워크에 등록된 NSF의 능력(capability)에 대한 정보를 기반으로 이루어진다. 추출된 데이터가 어떤 종류의 정보인지는 데이터 모델을 참고하여 쉽게 알 수 있다.

추출되어 전달받은 데이터는 고수준 정책 내의 데이터이기 때문에 추상적이다. NSF가 쉽게 인식하기 힘든 추상적인 데이터이기 때문에, NSF의 능력에 맞추어 데이터를 변환해 주어야 한다. 데이터 변환기는 보안 제어기(Security Controller)가 가지는 NSF에 대한 데이터베이스를 참고하여 데이터를 변환한다. 데이터의 종류와 내용을 키워드로 데이터베이스를 검색하면 NSF가 이해할 수 있는 구체적인 데이터로 변환할 수 있다.

데이터를 변환할 때에는 소비자 정책 전달 인터페이스를 통한 고수준 보안 정책 데이터와 NSF 정책 전달 인터페이스를 위한 저수준 보안 정책 데이터 간의 매핑 정보가 필요하다. 각 인터페이스 사이의 데이터 값을 전달하기 위한 매핑 정보의 예시는 아래와 같다.

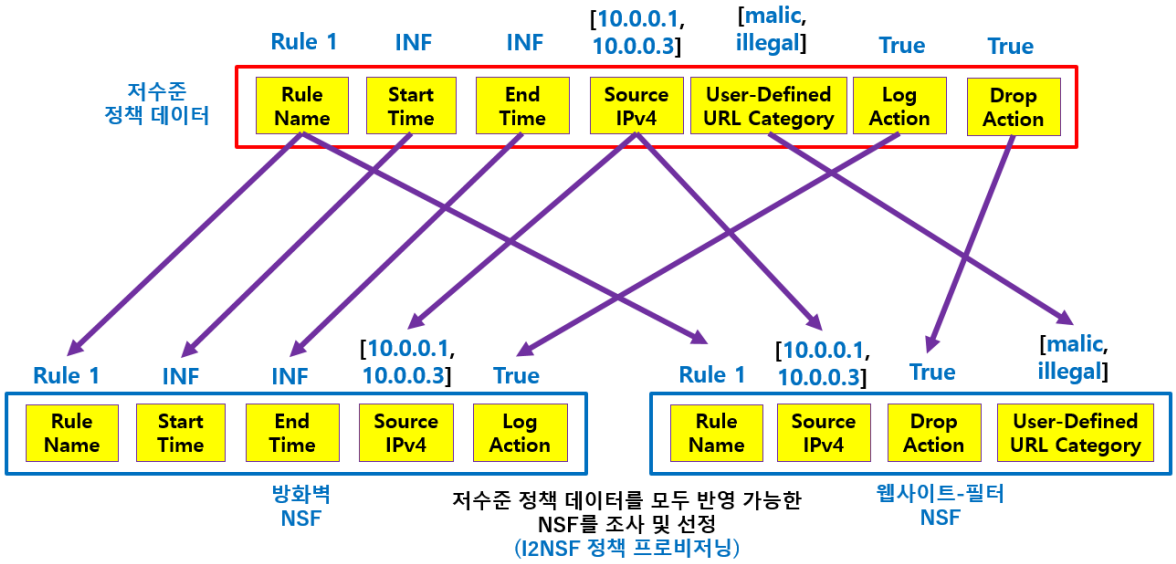
```
/consumer-facing/policy/policy-name
        -> mapping: /nsf-facing/i2nsf-security-policy/system-policy
                    /system-policy-name
```

위의 매핑 정보는 소비자 정책 전달 인터페이스의 ‘policy-name’을 NSF 정책 전달 인터페이스의 ‘system-policy-name’으로 매핑한 것이다. 더 자세한 매핑 정보는 부록 I-1을 참고할 수 있다.

5.2.4 문맥-자유 문법(CFG) 기반 정책 생성자(Generator)

정책 생성자에서는 크게 두 가지의 역할을 수행한다. 첫째로는 보안 정책만으로 적합한 NSF을 자동으로 선택하는 정책 프로비저닝(provisioning)이며, 둘째로는 변환된 데이터를 인터페이스의 데이터 모델에 맞추어 저수준 보안 정책을 생성하는 것이다.

우선, 변환된 데이터들의 타입을 NSF들의 능력(capability)와 비교하여 적합한 NSF들을 검색하는 정책 프로비저닝을 지원한다. 정책 프로비저닝 과정은 예시를 들어 자세히 설명한다.



(그림 5-6) 정책 프로비저닝(provisioning)

(그림 5-6)은 정책 프로비저닝으로 적합한 NSF를 선택하고, 그에 맞는 데이터를 각 NSF에 전달하는 과정을 보여준다. 데이터에 로그와 시간에 대한 정보가 포함되어 있으므로, 이를 수행해줄 "시간-기반 방화벽"을 선택한 뒤 데이터를 전달할 수 있다. 또한 접속을 막고자 하는 웹사이트 정보가 데이터에 포함되어 있으므로, 이를 수행해줄 "웹사이트 필터" NSF가 필요하다는 사실을 유추할 수 있기에 선택한 뒤 데이터를 전달한다. NSF의 능력과 데이터를 모두 비교하여 정책을 완벽히 수행할 수 있는 NSF를 모두 선택하고 데이터를 전달하는 과정을 생성자가 위와 같이 수행한다.

변환된 데이터와 정책을 전달해야 하는 NSF가 선정되었을 때, 저수준 보안 정책을 데이터 모델을 기반으로 생성할 수 있다. 이는 문맥-자유 문법(Context-free Grammar, CFG)이라는 오토마타 이론을 통해 생성할 수 있다. 문맥-자유 문법이란 특정한 상태(state)를 상태와 키워드의 조합으로 전이시켜나가는 생산 문장(production)의 집합이다. 여러 생산 문장이 모여 특수한 조건의 문자열을 생산할 수 있기 때문에 문법이라 정의한다. 생성하고자 하는 저수준 보안 정책 또한 데이터 모델이라는 특수한 조건을 만족해야 하는 문자열로 볼 수 있기 때문에 CFG를 도입하여 생성자를 구축하였다.

생성자가 사용하는 CFG는 두 가지 유형의 생산 문장으로 나누어진다. 본 문서는 두 가지 유형의 생산 문장을 '내용 생산 문장(content production)'과 '구조 생산 문장(structure production)'으로 정의한다.

'내용 생산 문장'은 저수준 보안 정책에 데이터를 담기 위한 생산 문장이다. 데이터 모델의 키워드로 데이터를 감싸주는 생산 문장과 실제 데이터를 문장에 주입하는 문장으로 구성되어 있다. 아래에 있는 수식의 형태로 '내용 생산 문장'을 정의한다.

[content] → [content][content] (중복 허용 시 추가)

[content] → <content-tag>[data]</content-tag>

[data] → data:1 | data:2 | … | data:n

예시로, IP 주소를 담는 <ipv4> 태그를 생성하기 위해서는 아래와 같이 내용 생산 문장을 작성한다.

[ip-content] → [ip-content][ip-content] (중복 허용을 위함)

[ip-content] → <ipv4>[data]</ipv4>

[data] → 10.0.0.1 | 10.0.0.3

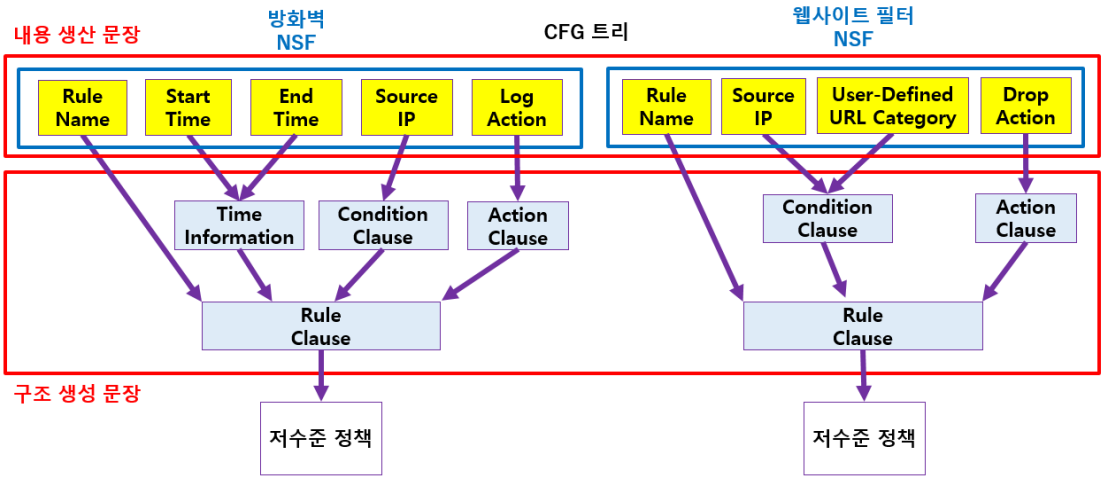
'구조 생산 문장'은 저수준 보안 정책을 구성하는 태그들을 그룹으로 묶어 구성하기 위한 생산 문장이다. 서로 다른 태그들을 계층적으로 구성하여 인터페이스 데이터 모델을 맞춰주기 위해 정의되었다. 아래에 있는 수식으로 '구조 생산 문장'을 정의한다.

[structure] → <structure-tag>[state:1][state:2]…[state:n]</structure-tag>

예시로, 정책의 이름과 데이터 정보를 묶어주는 <I2NSF> 태그를 아래와 같이 구조 생산 문장을 작성하여 생성한다.

[i2nsf] → <I2NSF>[rule-name][rules]</I2NSF>

각 생성 문장은 인터페이스의 데이터 모델에 따라 계층 관계를 가진다. (그림 5-7)은 각 생성 문장들 사이의 계층 구조를 시각화한 정책 생성자 모식도이다. 또한, (그림 5-8)은 CFG 기반 생성자에 의해 생성되어 웹사이트 필터 NSF로 전달되는 저수준 보안 정책의 예시이다.



(그림 5-7) CFG 기반 생성자의 구조

```
<I2NSF>
    <rule-name>block_web</rule-name>
    <rules>
        <condition>
            <packet>
                <ipv4>10.0.0.1</ipv4>
                <ipv4>10.0.0.3</ipv4>
            </packet>
            <payload>
                <url>malicious.com</url>
                <url>illegal.com</url>
            </payload>
        </condition>
        <action>drop</action>
    </rules>
</I2NSF>
```

(그림 5-8) 저수준 정책의 예시

5.3 보안 정책 번역기의 추가적 이점

본 문서에서 제안한 보안 정책 번역기는 사용 시 세 가지의 추가적인 이점을 가진다. 첫째, 고수준 정책의 문법 오류를 자동으로 번역기가 감지할 수 있다. 둘째, 번역기가 실행되는 도중에도 동작 정지 없이 동적으로 수정 가능하다. 마지막으로, 데이터 모델 등의 환경 변화에도 쉽게 적응할 수 있다.

5.3.1 고수준 정책의 문법 오류 자동 감지

본 문서에서 제안하는 번역기는 고수준 정책의 문법 오류를 쉽게 감지할 수 있다. 고수준 정책의 문법 오류는 크게 두 가지로 나뉜다. 첫 번째로는 계층 구조를 명시하기 위한 키워드를 잘못 입력한 경우이며, 두 번째로는 작성한 고수준 정책의 계층 구조 자체가 데이터 모델을 위반하는 경우이다.

위와 같은 문법 오류는 추출자를 구성하는 DFA의 시작점 상태를 승인자(accepter)로 설정하는 것으로 감지할 수 있다. 만약 고수준 정책에 따라 상태를 모두 이전하였을 때, 처음 상태인 승인자로 돌아오지 못했다면, 중간에 문법적인 오류로 인해 정상적으로 상태가 이전되지 못했음을 의미한다. 따라서 정책의 문법 오류를 추출자의 선에서 쉽게 감지 후 사용자에게 보고할 수 있다.

5.3.2 번역기의 동적 관리

본 문서에서 제안하는 번역기는 시각화가 가능하다는 장점이 있다. 추출자와 생성자는 데이터 모델의 계층 구조를 그대로 따르기 때문에 쉽게 시각화가 가능하다. 데이터 변환기는 연동된 데이터베이스를 기반으로 실행되기 때문에, 데이터베이스를 참고하면 데이터 매핑이 어떻게 되었는지 쉽게 확인할 수 있다.

또한, 모든 번역기의 컴포넌트는 모듈화가 되어있기 때문에, 동작하는 도중에도 동적으로 수정될 수 있다. I2NSF 프레임워크는 사용자에게 보안을 제공해야 하므로 서비스가 도중에 중단될 경우 사용자의 보안이 일시적으로 위험해진다. 따라서, 일부 데이터 모델이나 데이터베이스가 중간에 수정되어도 I2NSF 프레임워크는 사용자의 보안을 지키기 위해 지속적으로 돌아가고 있어야 한다. 이 문서에서 제안하는 번역기는 모듈화가 이루어져 있기 때문에 번역기가 실행되는 도중에도 쉽게 업데이트를 진행할 수 있다는 이점을 가진다.

5.3.3 번역기의 적응 능력

번역기는 연결된 인터페이스들의 데이터 모델을 기반으로 계층적으로 구성되어 있다. 따라서, 데이터 모델의 수정 사항이 발생하더라도, 부분적인 계층 구조 수정을 통해 쉽게 변화된 환경에 적응할 수 있다.

만약 고수준 보안 정책이 전달되는 인터페이스의 데이터 모델이 수정되는 경우, 번역기의 추출자를 구성하는 DFA의 일부를 수정하여 변화에 적응할 수 있다. 또한, 만약 저수준 보안 정책이 NSF에 전달되는 인터페이스의 데이터 모델이 수정되는 경우, 번역기의 생성자를 구성하는 CFG의 일부를 수정하여 변화에 적응할 수 있다. 데이터 모델은 계층 구조이기 때문에 어떠한 형태의 변화에도 번역기가 적응할 수 있다.

부 록 Ⅰ-1

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

데이터 변환기를 위한 매핑 정보

이 부록에서는 데이터 변환기를 위한 매핑 정보를 정의한다.

Source Object	Target Object	Meaning	Type
/consumer-facing/policy/policy-name	/nsf-facing/i2nsf-security-policy/system-policy/system-policy-name	정책 이름 매핑 정보	mapping
/consumer-facing/policy/rule/rule-name	/nsf-facing/i2nsf-security-policy/system-policy/rules/rule-name	룰 이름 매핑 정보	mapping
/consumer-facing/policy /rule/event/time-information/time/begin-time	/nsf-facing/i2nsf-security-policy/system-policy/rules/time-zone/absolute-time-zone/start-time	시작 시간 매핑 정보	mapping
/consumer-facing/policy /rule/event/time-information/time/end-time	/nsf-facing/i2nsf-security-policy/system-policy/rules/time-zone/absolute-time-zone/end-time	종료 시간 매핑 정보	mapping
/consumer-facing/policy/rule/condition /firewall-condition/source-target/src-target	/consumer-facing/policy/endpoint-group/user-group/name	firewall-condition 소스 타겟 참조 정보	reference
/consumer-facing/policy /endpoint-group/user-group/date	/nsf-facing/i2nsf-security-policy/rule/date	날짜 매핑 정보	mapping
/consumer-facing/policy/endpoint-group/user-group/ip-address	/nsf-facing/i2nsf-security-policy/system-policy/rules/condition-clause-container/packet-security-ipv4-condition/pkt-sec-ipv4-src/ipv4-address/ipv4	IP 주소 매핑 정보	mapping
/consumer-facing/policy /endpoint-group/user-group/range-ip-address/start-	/nsf-facing/i2nsf-security-policy/system-policy/rules/condition-clause-	시작 IP 주소 매핑 정보	mapping

Source Object	Target Object	Meaning	Type
ip-address	container/packet-security-ipv4-condition/pkt-sec-ipv4-src/range-ipv4-address/start-ipv4-address		
/consumer-facing/policy/endpoint-group/user-group/range-ip-address/end-ip-address	/nsf-facing/i2nsf-security-policy/system-policy/rules/condition-clause-container/packet-security-ipv4-condition/pkt-sec-ipv4-src/range-ipv4-address/end-ipv4-address	종말 IP 주소 매핑 정보	mapping
/consumer-facing/policy/rule/condition/firewall-condition/destination-target/dest-target	/consumer-facing/policy/endpoint-group/user-group/name	firewall-condition 목적지 참조 정보	reference
/consumer-facing/policy/endpoint-group/user-group/date	/nsf-facing/i2nsf-security-policy/system-policy/rule/date	날짜 매핑 정보	mapping
/consumer-facing/policy/endpoint-group/user-group/ip-address	/nsf-facing/i2nsf-security-policy/system-policy/rules/condition-clause-container/packet-security-ipv4-condition/pkt-sec-ipv4-dest/ipv4-address/ipv4	IP 주소 매핑 정보	mapping
/consumer-facing/policy/endpoint-group/user-group/range-ip-address/start-ip-address	/nsf-facing/i2nsf-security-policy/system-policy/rules/condition-clause-container/packet-security-ipv4-condition/pkt-sec-ipv4-dest/range-ipv4-address/start-ipv4-address	시작 IP 주소 매핑 정보	mapping
/consumer-facing/policy/endpoint-group/user-group/range-ip-address/end-ip-address	/nsf-facing/i2nsf-security-policy/system-policy/rules/condition-clause-container/packet-security-ipv4-condition/pkt-sec-ipv4-dest/range-ipv4-address/end-ipv4-address	종말 IP 주소 매핑 정보	mapping
/consumer-	/consumer-	ddos-	referenc

Source Object	Target Object	Meaning	Type
facing/policy/rule/condition/ddos-condition/source-target/src-target	facing/policy/endpoint-group/device-group/name	condition 소스 타겟 참조 정보	e
/consumer-facing/policy/endpoint-group/device-group/date	/nsf-facing/i2nsf-security-policy/rule/date	날짜 매핑 정보	mapping
/consumer-facing/policy/endpoint-group/device-group/ip-address	/nsf-facing/i2nsf-security-policy/system-policy/rules/condition-clause-container/packet-security-ipv4-condition/pkt-sec-ipv4-src/ipv4-address/ipv4	IP 주소 매핑 정보	mapping
/consumer-facing/policy/endpoint-group/device-group/range-ip-address/start-ip-address	/nsf-facing/i2nsf-security-policy/system-policy/rules/condition-clause-container/packet-security-ipv4-condition/pkt-sec-ipv4-src/range-ipv4-address/start-ipv4-address	시작 IP 주소 매핑 정보	mapping
/consumer-facing/policy/endpoint-group/device-group/range-ip-address/end-ip-address	/nsf-facing/i2nsf-security-policy/system-policy/rules/condition-clause-container/packet-security-ipv4-condition/pkt-sec-ipv4-src/range-ipv4-address/end-ipv4-address	종말 IP 주소 매핑 정보	mapping
/consumer-facing/policy/rule/condition/ddos-condition/destination-target/dest-target	/consumer-facing/policy/endpoint-group/device-group/name	ddos-condition 목적지 참조 정보	reference
/consumer-facing/policy/endpoint-group/device-group/date	/nsf-facing/i2nsf-security-policy/rule/date	날짜 매핑 정보	mapping
/consumer-facing/policy/endpoint-group/device-group/ip-address	/nsf-facing/i2nsf-security-policy/system-policy/rules/condition-clause-container/packet-security-ipv4-condition/pkt-sec-ipv4-dest/ipv4-address/ipv4	IP 주소 매핑 정보	mapping

Source Object	Target Object	Meaning	Type
/consumer-facing/policy/endpoint-group/device-group/range-ip-address/start-ip-address	/nsf-facing/i2nsf-security-policy/system-policy/rules/condition-clause-container/packet-security-ipv4-condition/pkt-sec-ipv4-dest/range-ipv4-address/start-ipv4-address	시작 IP 주소 매핑 정보	mapping
/consumer-facing/policy/endpoint-group/device-group/range-ip-address/end-ip-address	/nsf-facing/i2nsf-security-policy/system-policy/rules/condition-clause-container/packet-security-ipv4-condition/pkt-sec-ipv4-dest/range-ipv4-address/end-ipv4-address	종말 IP 주소 매핑 정보	mapping
/consumer-facing/policy/rule/condition/ddos-condition/rate-limit/packet-per-second	/nsf-facing/i2nsf-security-policy/system-policy/rules/condition-clause-container/packet-security-ddos-condition/pkt-sec-alert-rate	초당 패킷 비율 매핑 정보	mapping
/consumer-facing/policy/rule/condition/custom-condition/source-target/src-target	/consumer-facing/policy/threat-prevention/payload-content/name	threat-prevention 소스 타겟 참조 정보	reference
/consumer-facing/policy/threat-prevention/payload-content/date	/nsf-facing/i2nsf-security-policy/system-policy/rules/date	날짜 매핑 정보	mapping
/consumer-facing/policy/threat-prevention/payload-content/content	/nsf-facing/i2nsf-security-policy/system-policy/rules/condition-clause-container/packet-security-payload-condition/pkt-payload-content	payload 상태 매핑 정보	mapping
/consumer-facing/policy/rule/condition/custom-condition/destination-target/dest-target	/consumer-facing/policy/threat-prevention/payload-content/name	threat-prevention 목적지 참조 정보	reference
/consumer-facing/policy/threat-prevention/payload-content/date	/nsf-facing/i2nsf-security-policy/system-policy/rules/date	날짜 매핑 정보	mapping

Source Object	Target Object	Meaning	Type
/consumer-facing/policy/threat-prevention/payload-content/content	/nsf-facing/i2nsf-security-policy/system-policy/rules/condition-clause-container/packet-security-payload-condition/pkt-payload-content	payload 상태 매핑 정보	mapping
/consumer-facing/policy/rule/condition/custom-condition/threat-feed-condition/source-target/src-target	/consumer-facing/policy/threat-prevention/threat-feed-list/name	threat-feed-condition 소스 타겟 참조 정보	reference
/consumer-facing/policy/threat-prevention/threat-feed-list/date	/nsf-facing/i2nsf-security-policy/system-policy/rules/date	날짜 매핑 정보	mapping
/consumer-facing/policy/threat-prevention/threat-feed-list/threat-feed-server/ip-address	/nsf-facing/i2nsf-security-policy/system-policy/rules/condition-clause-container/packet-security-ipv4-condition/pkt-sec-ipv4-src/ipv4-address/ipv4	IP 주소 매핑 정보	mapping
/consumer-facing/policy/threat-prevention/threat-feed-list/threat-feed-server/range-ip-address/start-ip-address	/nsf-facing/i2nsf-security-policy/system-policy/rules/condition-clause-container/packet-security-ipv4-condition/pkt-sec-ipv4-src/range-ipv4-address/start-ipv4-address	시작 IP 주소 매핑 정보	mapping
/consumer-facing/policy/threat-prevention/threat-feed-list/threat-feed-server/range-ip-address/end-ip-address	/nsf-facing/i2nsf-security-policy/system-policy/rules/condition-clause-container/packet-security-ipv4-condition/pkt-sec-ipv4-src/range-ipv4-address/end-ipv4-address	종말 IP 주소 매핑 정보	mapping
/consumer-facing/policy/threat-prevention/threat-feed-list/threat-feed-server/threat-feed-description	/nsf-facing/i2nsf-security-policy/system-policy/rules/condition-clause-container/packet-security-ipv4-condition/ipv4-description	threat-feed-description 매핑 정보	mapping
/consumer-	/consumer-facing/policy/threat-	threat-	referenc

Source Object	Target Object	Meaning	Type
facing/policy/rule/condition/custom-condition/threat-feed-condition/destination-target/dest-target	prevention/threat-feed-list/name	feed-condition 목적지 참조 정보	e
/consumer-facing/policy/threat-prevention/threat-feed-list/date	/nsf-facing/i2nsf-security-policy/system-policy/rules/date	날짜 매핑 정보	mapping
/consumer-facing/policy/threat-prevention/threat-feed-list/threat-feed-server/ip-address	/nsf-facing/i2nsf-security-policy/system-policy/rules/condition-clause-container/packet-security-ipv4-condition/pkt-sec-ipv4-dest/ipv4-address/ipv4	IP 주소 매핑 정보	mapping
/consumer-facing/policy/threat-prevention/threat-feed-list/threat-feed-server/range-ip-address/start-ip-address	/nsf-facing/i2nsf-security-policy/system-policy/rules/condition-clause-container/packet-security-ipv4-condition/pkt-sec-ipv4-dest/range-ipv4-address/start-ipv4-address	시작 IP 주소 매핑 정보	mapping
/consumer-facing/policy/threat-prevention/threat-feed-list/threat-feed-server/range-ip-address/end-ip-address	/nsf-facing/i2nsf-security-policy/system-policy/rules/condition-clause-container/packet-security-ipv4-condition/pkt-sec-ipv4-dest/range-ipv4-address/end-ipv4-address	종말 IP 주소 매핑 정보	mapping
/consumer-facing/policy/threat-prevention/threat-feed-list/threat-feed-server/threat-feed-description	/nsf-facing/i2nsf-security-policy/system-policy/rules/condition-clause-container/packet-security-ipv4-condition/ipv4-description	threat-feed-description 매핑 정보	mapping
/consumer-facing/policy/rule/action/name	/nsf-facing/i2nsf-security-policy/system-policy/rules/action-clause-container/packet-action/ingress-action	ingress-action 매핑 정보	mapping
/consumer-facing/policy/rule/action/name	/nsf-facing/i2nsf-security-policy/system-policy/rules/action-clause-	egress-action 매핑 정보	mapping

Source Object	Target Object	Meaning	Type
	container/packet-action/egress-action		
/consumer-facing/policy/rule/action/name	/nsf-facing/i2nsf-security-policy/system-policy/rules/action-clause-container/packet-action/log-action	log-action 매핑 정보	mapping
/consumer-facing/policy/rule/action/name	/nsf-facing/i2nsf-security-policy/system-policy/rules/action-clause-container/advanced-action/content-security-control	content-security-control 매핑 정보	mapping
/consumer-facing/policy/rule/action/name	/nsf-facing/i2nsf-security-policy/system-policy/rules/action-clause-container/advanced-action/attack-mitigation-control	attack-mitigation-control 매핑 정보	mapping
/consumer-facing/policy/rule/ipsec-method	/nsf-facing/i2nsf-ipsec	ipsec-method 매핑 정보	mapping
/consumer-facing/policy-domain/name	/nsf-facing/i2nsf-security-policy/system-policy/rule-group/groups/group-name	도메인 이름 매핑 정보	mapping

부 록 II-1

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

지식재산권 확약서 정보

(※ 본 표준 발간 이전에 접수된 지식재산권 확약서가 있는 경우에 작성하며, 해당 사항이 없는 경우, 각 항목별로 '해당 사항 없음'으로 기재하고, 본 양식을 삭제하지 않음)

II-1.1 지식재산권 확약서(1)

- 발명의 명칭: 네트워크 보안 기능과의 인터페이스에서의 보안 정책 번역
- 권리자의 성명: 정재훈, 양진혁
- 출원 번호: 10-2019-0027216
- 출원 연월일: 2019. 03. 08
- 실시조건
- 확약서 접수일

부 록 II-2

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

시험인증 관련 사항

- 해당 사항 없음

부 록 II-3

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

본 표준의 연계(family) 표준

II-3.1 TTAK.KO-12.0314-part1, "SDN 기반의 네트워크 보안 기능의 인터페이스(I2NSF) 프레임워크 - 제1부: 개요", 정재훈, 현상원, 김형식, 김진용, 김은수, 위사랑, 박정수, 2017년 12월.

"SDN 기반의 네트워크 보안 기능의 인터페이스(I2NSF) 프레임워크 - 제1부: 개요[II-3.1]" 연계 표준은 네트워크 보안 기능을 위한 인터페이스를 사용하는 SDN 기반 보안 시스템에 대한 프레임워크를 기술한 문서로 본 표준은 연계표준에서의 보안 제어기의 핵심 기능인 보안 정책 번역 구조를 기술한다.

II-3.2 TTAK.KO-12.0314-part2, "SDN 기반의 네트워크 보안 기능의 인터페이스(I2NSF) 프레임워크 - 제2부: 보안 서비스 유스케이스", 정재훈, 김진용, 김은수, 위사랑, 2018년 12월.

"SDN 기반의 네트워크 보안 기능의 인터페이스(I2NSF) 프레임워크 - 제2부: 보안 서비스 유스케이스[II-3.2]" 연계 표준은 네트워크 보안 기능을 위한 인터페이스를 사용하는 SDN 기반 보안 시스템에 대한 프레임워크를 이용한 보안 서비스 유스케이스를 기술한 문서로 본 표준은 연계표준에서의 보안 제어기의 핵심 기능인 보안 정책 번역 구조를 기술한다.

II-3.3 TTAK.KO-12.0314-part3, "SDN 기반의 네트워크 보안 기능의 인터페이스(I2NSF) 프레임워크- 제3부: NSF 등록 인터페이스", 정재훈, 현상원, 노태균, 위사랑, 2019년 6월.

"SDN 기반의 네트워크 보안 기능의 인터페이스(I2NSF) 프레임워크- 제3부: NSF 등록 인터페이스[II-3.3]" 연계 표준은 네트워크 보안 기능을 위한 인터페이스를 사용하는 SDN 기반 보안 시스템에 대한 프레임워크 중 NSF 등록 인터페이스를 기술한 문서로 본 표준은 연계표준에 적응 가능한 보안 제어기 내에서의 번역 과정을 서술한다.

Ⅱ-3.4 TTAK.KO-12.0314-part4, “SDN 기반의 네트워크 보안 기능의 인터페이스(I2NSF) 프레임워크- 제4부: 소비자 정책 전달 인터페이스”, 정재훈, 김형식, 김은수, 2019년 6월.

“SDN 기반의 네트워크 보안 기능의 인터페이스(I2NSF) 프레임워크- 제4부: 소비자 정책 전달 인터페이스[Ⅱ-3.4]” 연계 표준은 네트워크 보안 기능을 위한 인터페이스를 사용하는 SDN 기반 보안 시스템에 대한 프레임워크 중 소비자 정책 전달 인터페이스를 기술한 문서로 본 표준은 연계표준에 적응 가능한 보안 제어기 내에서의 번역 과정을 서술한다.

Ⅱ-3.5 TTAK.KO-12.0314-part5, “SDN 기반의 네트워크 보안 기능의 인터페이스(I2NSF) 프레임워크- 제5부: NSF 정책 전달 인터페이스”, 정재훈, 김진용, 박정수, 2019년 6월.

“SDN 기반의 네트워크 보안 기능의 인터페이스(I2NSF) 프레임워크- 제5부: NSF 정책 전달 인터페이스[Ⅱ-3.5]” 연계 표준은 네트워크 보안 기능을 위한 인터페이스를 사용하는 SDN 기반 보안 시스템에 대한 프레임워크 중 NSF 정책 전달 인터페이스를 기술한 문서로 본 표준은 연계표준에 적응 가능한 보안 제어기 내에서의 번역 과정을 서술한다.

부 록 II-4

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

참고 문헌

II-4.1 규정 참조 표준

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

2. 정보 참조 표준

[2] S. Hares, J. Strassner, D. Lopez, L. Xia, and H. Birkholz, “Interface to Network Security Functions (I2NSF) Terminology”, draft-ietf-i2nsf-terminology-08, July 2019.

부 록 II-5

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

영문표준 해설서

- 해당 사항 없음

부 록 II-6

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

표준의 이력

판수	채택일	표준번호	내용	담당 위원회