SDN/NFV 환경에서 네트워크 보안 관리를 위한 블록체인 구조 및 절차

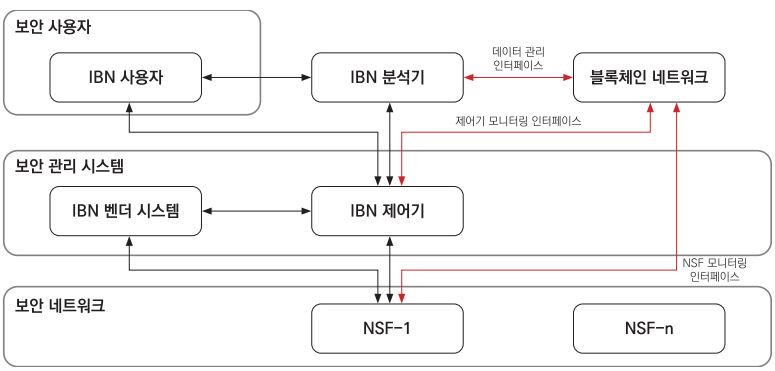
최윤철 한국전자통신연구원 지능정보표준연구실 선임연구원
박정수 한국전자통신연구원 지능정보표준연구실 책임연구원
정재훈 성균관대학교 소프트웨어대학 부교수

1. 머리말

지금은 그 임무를 마치고 종료된 IETF(Internet Engineering Task Force, 국제인터넷표준화기구) I2NSF(Interface to Network Security Functions, 네트워크 보안 기능 인터페이스) WG(Working Group)는 NFV(Network Functions Virtualization, 네트워크 기능 가상화)와 SDN(Software-Defined Networking, 소프트웨어 정의 네트워킹) 기반 I2NSF 프레임워크 표준을 개발했다.

이와 병행해 TTA PG503을 통해 10여 종의 단체 표준들이 제정된 바 있다. 이 표준은 방화벽, DDoS(Distributed Denial of Service) 공격 약화 서비스, 웹 필터, 심층 패킷분석과 같은 NSFs(Network Security Functions, 네트워크 보안 기능)를 정의하고, 사용자, 관리자, SDN 제어기, SDN 스위치 등과의 인터페이스 프로토콜과 데이터모델을 기술한다. 이 NSF들은 NFV 환경 하에서 벤더에 의해 구현돼 클라우드 상에 유지되며, 사용자의 요구사항을 충족시키기 위해 여러 개의 SDN 스위치에 탑재돼 동작하게 된다. 이와 같은 SDN 스위치 탑재 유무는 SDN 제어기에 의해 제어된다.

IETF의 I2NSF 프레임워크 표준은 네트워크 서비스 설정을 자동화해야 한다. 이를 위해 인텐트



[그림 1] IBN-블록체인기반 보안관리 시스템 프레임워크

(Intent)와 같은 네트워크 사용자 및 관리자의 상위 레벨 요구사항을 시스템 설정을 위한 하위레벨 데이터로 변환하기 위한 기능을 확장하고 있다.

SDN/NFV 기반 네트워크 환경에서 네트워크 사용자 및 관리자가 인텐트(Intent)를 생성하고 변환하면, 네트워크 서비스 설정의 자동화가 가능하다. 이러한 서비스를 IBN(Intent-Based Networking, 인텐트-기반 네트워킹)이라고 한다. 그러나 IBN 환경에서 NSF 설정 및 갱신 과정은 보안에 취약하다. 본고는 네트워크 보안 설정 오류 시에 발생하는 문제를 해결하기 위해 기존 I2NSF 프레임워크에 블록체인 네트워크를 연동시키는 방법을 제시하고자 한다.

2. 네트워크 보안 관리를 위한 블록체인 구조 및 절차

2.1 블록체인 연동 구조

I2NSF 프레임워크와 블록체인 네트워크를 연동하는 구조에선 [그림 1]과 같이 보안 제어기, IBN 분석기, NSF 모듈에서 인터페이스를 새롭게 정의해 블록체인 네트워크 내의 저장소에 보안 관련 모니터링 정보를 저장한다. 이를 필요에 따라 분석해 보안 네트워크 내 NSF 재구성 및 재설정이 가능한 것이다. 블록체인 네트워크는 I2NSF 프레임워크와 연동하기 위한 3가지 인터페이스, 즉 데이터 관리, 제어기 모니터링, NSF 모니터링 인터페이스를 갖는다.

2.2 블록체인 연동 절차

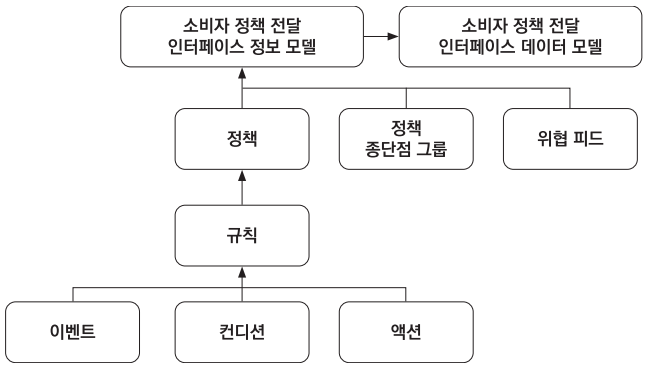
I2NSF 프레임워크에서 블록체인 연동을 위한 절차는 다음과 같다.

① IBN 사용자에 의해 블록체인에 저장할 데이터의 범위와 주기를 설정한다.
② IBN 사용자가 작성한 상위레벨 인텐트, IBN 제어기를 통해 변환된 하위레벨 인텐트 정보를 블록체인 네트워크에 저장한다.
③ IBN 사용자에 의해 설정된 데이터 범위 및 네트워크 모니터링 주기에 따른 NSF 모니터링 정보를 블록체인 네트워크에 저장한다.
④ IBN 분석기에서 네트워크 보안에 대한 무결성·부인 방지·검증이 필요한 경우 블록체인 네트워크에 데이터를 요청·수신해 분석을 수행한다.
⑤ IBN 분석기는 보안 네트워크 모니터링 수행 결과를 IBN 사용자에게 전달한다.

3. 블록체인 연동 인터페이스

3.1 제어기 모니터링 인터페이스

IBN 보안 제어기는 상위레벨(고수준) 보안 정책을 SDN/NFV 네트워크 환경에서 보안 기능이 이해할 수 있는 하위레벨(저수준) 보안 정책으로 변환한다.



[그림 2] 소비자 정책 정보 모델의 객체

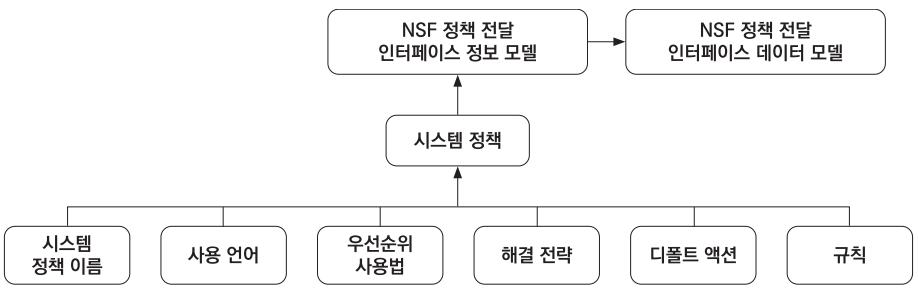
이때 IBN 보안 제어기는 IBN 사용자와 블록체인 네트워크로부터 보안 정책을 전달받는다. 특히, 제어기 모니터링 인터페이스를 통해 상위레벨 및 하위레벨의 보안 정책을 블록체인 네트워크에 저장하거나 모니터링된 정보를 전달받는다.

상위레벨 보안 정책 데이터 모델은 [그림 2]와 같고, 참고문헌 [2]에서 정의한 형식을 따른다. 하위레벨 보안 정책 데이터 모델은 [그림 3]과 같고, 참고문헌 [3]에서 정의한 형식을 따른다. 블록체인 네트워크에 상위레벨 및 하위레벨의 보안 정책을 저장하고, 관리자의 의도대로 보안 정책이 변환·반영됐는지 NSF 모니터링을 통해 확인할 수 있다.

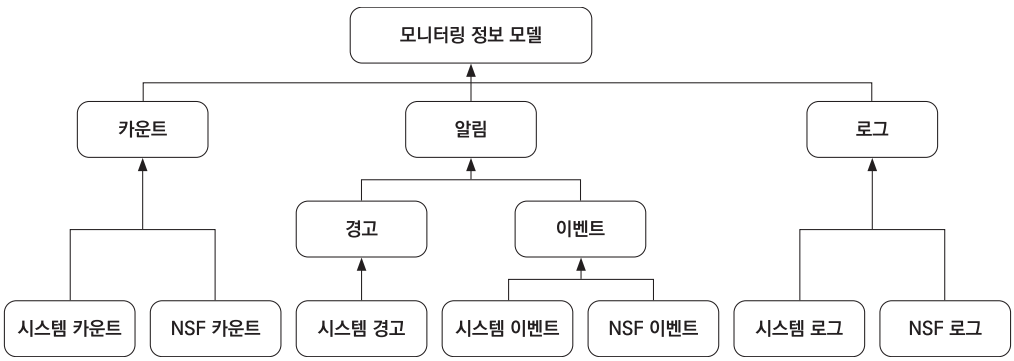
3.2 NSF 모니터링 인터페이스

SDN/NFV 기반 네트워크 환경에서 보안 서비스를 제공하려면 NSF에 보안 정책을 설정하고, NSF 상태를 지속적으로 모니터링해야 한다. 이 인터페이스가 NSF 모니터링 인터페이스다. 이 인터페이스를 통해 NSF의 이벤트 및 규격화된 활동 로그가 전달되며, 해당 정보는 네트워크 상에서 발생한 문제점의 원인 분석에 활용된다.

NSF 모니터링 데이터 모델은 [그림 4]와 같고, 참고문헌 [4]에서 정의한 형식을 따른다. 제어기 모니터링 정보와 NSF 모니터링 정보를 취합해 관리자의 의도가 네트워크에 반영됐는지 확인하고 점검한다. 또 NSF 시스템 모니터링 정보에서 버전 정보를 추가해 시스템 업데이트 여부 및 관리에 활용한다. 버전 정보를 기반으로 NSF에서 발생할 수 있는 공급망 공격



[그림 3] NSF 정책 정보 모델의 객체



[그림 4] NSF 모니터링 정보 모델의 객체

문제를 해결할 수 있는 정보를 블록체인 네트워크에 저장하고 관리한다.

3.3 데이터 관리 인터페이스

I2NSF 프레임워크의 IBN 분석기는 IBN 사용자 보안 정책 의도에 따라 SDN/NFV 기반 네트워크 환경에 잘 반영됐는지 검증한다. 모니터링된 네트워크 정보를 취합하고 의도대로 반영됐는지를 분석해 그 결과를 IBN 제어기에 피드백한다.

IBN 제어기 요청에 따라 블록체인 네트워크는 데이터 관리 인터페이스를 통해 보안 제어기 정책 정보와 NSF 모니터링 정보를 받을 수 있다. 상위레벨 보안 정책 데이터 모델은 [그림 2]와 같고, 참고문헌 [2]에서 정의한 형식을 따른다. 하위레벨 보안 정책 데이터 모델은 [그림 3]과 같고, 참고문헌 [3]에서 정의한 형식을 따른다. NSF 모니터링 데이터 모델은 [그림 4]와 같고, 참고문헌 [4]에서 정의한 형식을 따른다. 여기에 NSF 관리를 위한 버전 정보를 추가로 요청할 수 있다.

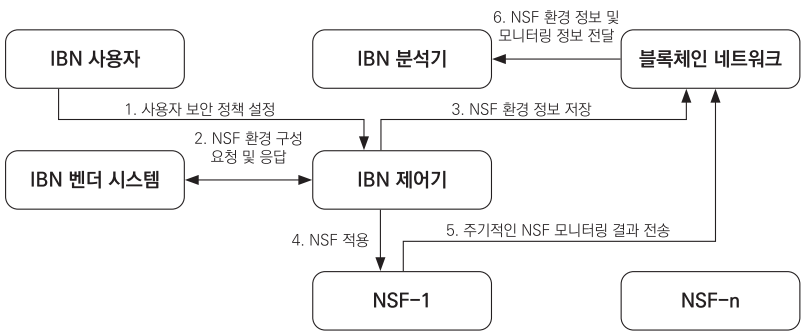
4. 블록체인 기반 네트워크 보안 유즈케이스

4.1 네트워크 오류 검증 시나리오

[그림 5]는 IBN 사용자가 설정한 사용자 보안 정책이 NSF 시스템에 잘 반영됐는지 점검하는 예제다. 여기선 IBN 사용자가 입력한 고수준 인텐트 정보와 IBN 제어기에서 변환된 저수준 인텐트 정보, 그리고 인텐트 반영을 확인하기 위한 네트워크 모니터링 정보를 블록체인 네트워크에 저장한다. 이후 IBN 사용자가 의도한 보안 설정을 상위레벨보안 정책으로 IBN 제어기에 전달하고, 이를 IBN 제어기에서 하위레벨 보안 정책으로 번역해 IBN 벤더 시스템에 NSF 환경 구성에 대한 정보를 요청하고 응답을 받는다. 이후 각각의 NSF에 시스템이 적용된다.

더불어 주기적인 모니터링 정보는 블록체인 네트워크에 저장된다. IBN 제어기에서는 상위레벨 보안 정책과 하위레벨 보안 정책 매핑 정보를 블록체인 네트워크에 저장한다. IBN 분석기에서는 블록체인 네트워크에 보안 정책 정보 및 모니터링 정보를 요청해 데이터를 분석하고, SDN/NFV 네트워크 환경에서 보안 정책이 잘 적용되고 있는지에 대한 분석 결과를 IBN 사용자에게 전달한다.

VoIP/VoLTE 트래픽 차단 서비스에 대한 네트워크 오류 검증 동작 시나리오는 다음과 같다.



[그림 5] BN-블록체인기반 네트워크 오류 검증 예제

① IBN 사용자는 IBN 제어기에 다음의 보안 정책을 설정한다.
- 악의적 공격자의 VoIP/VoLTE 트래픽을 차단한다.
- VoIP/VoLTE 트래픽 중 5060, 5061 포트로 보내지는 패킷은 차단한다.
- 악의적 공격자인 1111@voip.black.com은 차단한다.

② IBN 제어기는 IBN 벤더 시스템에게 NSF 환경 구성을 요청한다.
- 방화벽 서비스 요청 및 설정 응답을 요청한다.
- VoIP/VoLTE 서비스 요청 및 설정 응답을 요청한다.

③ IBN 제어기는 블록체인 네트워크에 NSF 환경 정보를 저장한다.
- 방화벽 서비스를 위한 NSF 환경을 설정한다.
  • VoIP/VoLTE 트래픽 차단 ⋯› 5060, 5061
  • 악의적 공격자 차단 ⋯› 1111@voip.black.com
- VoIP/VoLTE 서비스를 위한 NSF 환경을 설정한다.

④ IBN 제어기에서 NSF를 적용한다.
- 방화벽 및 VoIP/VoLTE 서비스가 활성화된다.

⑤ NSF에서 주기적으로 블록체인 네트워크에 모니터링 결과를 전송한다. 전송되는 정보는 다음과 같다.
- 방화벽 서비스 상태 및 통계정보
- VoIP/VoLTE 서비스 상태 및 통계정보

⑥ 블록체인 네트워크에서 IBN 분석기에 아래의 정보를 전달한다.
- NSF 환경 정보
- NSF 모니터링 정보

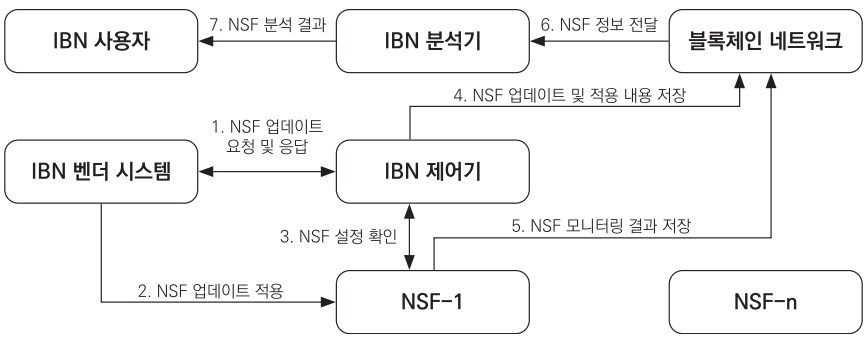
4.2 공급망 공격 검증 시나리오

공급망 공격은 SDN/NFV 시스템, 데이터에 대한 접근 권한을 가진 외부 공급업체를 통해 시스템에 침투할 때 발생할 수 있는 공격이다. 예를 들어, 권한을 가진 시스템 외부 관리자는 펌웨어 또는 소프트웨어 업데이트를 수행할 수 있다. 공급망 공격은 이러한 경로를 탈취해 변조된 펌웨어 또는 소프트웨어를 설치해 공격하는 형태다.

I2NSF 프레임워크 환경에서 악의적 사용자는 NSF 관리 시스템을 통해 NSF 시스템 업데이트 요청을 진행할 수 있다. 이에 대한 예제는 [그림 6]과 같다. 해당 예제에선 NSF 관리 로그, NSF 설정 정보, NSF 모니터링 정보를 블록체인 네트워크에 저장한다. 예제에서 IBN 벤더 시스템은 IBN 제어기에 NSF 업데이트 요청을 발생시키고, IBN 제어기가 응답을 회신한다. 이러한 응답을 수신한 IBN 벤더 시스템은 NSF 업데이트를 적용한다. 그리고 IBN 제어기에서는 업데이트된 NSF에서 IBN 사용자가 최초로 요청했던 설정이 잘 적용돼 있는지 확인하다. NSF 시스템은 주기적으로 블록체인 네트워크에 모니터링 정보 및 NSF 버전 정보를 전달한다. IBN 제어기에서는 NSF 업데이트 및 적용 정보를 블록체인 네트워크에 전달한다.

IBN 분석기에서는 블록체인 네트워크에 NSF 정보와 모니터링 정보를 요청해, NSF 업데이트가 정상적으로 이루어졌는지를 분석한다. 해당 결과정보는 IBN 사용자에게 전달된다.

VoIP/VoLTE 트래픽 차단 서비스에 대한 공급망 공격 검증 동작 시나리오는 다음과 같다.



[그림 6] IBN-블록체인기반 공급망 공격 예제

① IBN 제어기는 IBN 벤더 시스템에 NSF 업데이트를 요청한다.
- 방화벽 서비스 업데이트 요청 및 설정 응답을 요청한다.
- VoIP/VoLTE 서비스 업데이트 요청 및 설정 응답을 요청한다.

② IBN 벤더 시스템은 NSF에 업데이트를 적용한다.
- 방화벽 서비스를 업데이트한다.
  • 악의적 공격자(이메일) 및 VoIP/VoLTE 트래픽 차단 기능 추가
- VoIP/VoLTE 서비스를 업데이트한다.
  • 음성 서비스 지연 개선 패치 적용

③ IBN 제어기에서 NSF 설정을 확인한다.
- 방화벽 및 VoIP/VoLTE 서비스 설정을 확인한다.
  • VoIP/VoLTE 트래픽 차단 ⋯› 5060, 5061
  • 악의적 공격자 차단 ⋯› 1111@voip.black.com

④ IBN 제어기는 블록체인 네트워크에 NSF 업데이트를 적용 및 저장한다.
- 방화벽 서비스를 위한 NSF 설정은 다음과 같다
  • VoIP/VoLTE 트래픽 차단 ⋯› 5060, 5061
  • 악의적 공격자 차단 ⋯› 1111@voip.black.com
- VoIP/VoLTE 서비스를 위한 NSF를 설정한다.
  • 음성 서비스 지연 개선 패치 내용 및 버전 정보

⑤ NSF에서 주기적으로 블록체인 네트워크에게 다음과 같은 모니터링 결과를 전송한다.
- 방화벽 서비스 상태 및 통계정보
- VoIP/VoLTE 서비스 상태 및 통계정보

⑥ 블록체인 네트워크에서 IBN 분석기에게 아래의 정보를 전달한다.
- NSF 환경 정보
- NSF 모니터링 정보

⑦ IBN 분석기는 NSF 분석 결과를 IBN 사용자에게 전달한다.

5. 맺음말

네트워크 기능 가상화로 인해 NSF의 공급 사슬 보안 문제, 네트워크 자동화에 따른 보안 문제가 발생하고 있다. 그에 대한 원인을 파악하고 해결방안을 제시해야 하는데, 원인 파악보다 문제 해결이 더욱 중요하다. 본고에서는 I2NSF 프레임워크 환경에서 블록체인 기술을 활용해 해결방안을 제시했다. 향후 블록체인 네트워크 내에서 저장되는 블록 구조와 인터페이스별 데이터모델을 연구하고자 한다.

참고문헌

[1] 최윤철, 박정수, 정재훈. “SDN 기반의 네트워크 보안 기능의 인터페이스(I2NSF) 프레임워크 - 제10부:네트워크 보안 관리를 위한 블록체인 구조 및 절차” TTAK.KO-12.0314-Part10 (2023)

[2] J. P. Jeong, et al. “I2NSF Consumer-Facing Interface YANG Data Model.” InternetDraft draft-ietf-i2nsf-consumer-facing-interface-dm-31 (2023)

[3] J. T. Kim, et al. “I2NSF Network Security Function-Facing Interface YANG Data Model.” Internet-Draft draft-ietf-i2nsf-nsf-facing-interface-dm-29 (2022)

[4] J. P. Jeong, et al. “I2NSF NSF Monitoring Interface YANG Data Model,” InternetDraft draft-ietf-i2nsf-nsf-monitoring-data-model-20 (2022)