네트워크 보안 기능을 위한 프레임워크 개발

김진용 O, 정재훈
성균관대학교 전자전기컴퓨터공학과
timkim@skku.edu, pauljeong@skku.edu

Framework Development for Network Security Functions

Jinyong (Tim) Kim O, Jaehoon (Paul) Jeong
Department of Computer Science and Engineering,
Sungkyunkwan University

요 약

네트워크 공격이 다양해지고 복잡해짐에 따라 네트워크 통신의 무결성, 기밀성, 이용가능성을 보장하기 위하여 많은 보안 제조사들은 다양한 네트워크 보안 기능(Network Security Functions, NSFs)들을 개발하고 있다. 이와 같이 다양한 보안 제조사에서 개발된 보안 기능들은 서로 다른 인터페이스를 가지고 있어 다양한 네트워크 보안 기능들을 이용하고 있는 보안 서비스 관리자들은 서로 다른 인터페이스로 인해 호환성의 문제를 겪고 있다. 국제인터넷표준화기구인 Internet Engineering Task Force (IETF)의 Interface to Network Security Functions (I2NSF) Working Group에서는 이러한 문제를 해결하고자 표준 인터페이스를 제정하고 있으며, 이와 관련된 네트워크 보안 기능 프레임워크를 설계하고 있다. 본 논문은 IETF I2NSF WG에서 제안하고 있는 프레임워크를 살펴보고 이를 바탕으로 직접 구현한 내용을 제안한다.

1. 소 개

네트워크 보안 기능(Network Security Functions, NSFs)이란 네트워크 통신의 무결성, 기밀성, 이용가능성을 보장하기 위하여 악의적인 네트워크 트래픽을 감지하고 이를 차단하거나 완화하도록 하는 기능을 말한다. 이러한 네트워크 보안 기능들은 보안 정책 및 규칙을 기반으로 동작하며 보안 관리자들은 보안 정책 및 규칙을 생성하여 네트워크 보안 기능에 적용한다. 이와 같이 적용된 정책 및 규칙을 기반으로 네트워크 보안 기능들은 악의적인 네트워크 트래픽들을 감지, 차단 완화하는 보안서비스를 제공한다.

최근에는 네트워크 공격이 다양해지고 복잡해짐에 따라 이를 막기 위하여 많은 제조사들은 다양한 보안 기능들을 개발하고 있다. 하지만 네트워크 보안 기능 인터페이스에 대한 표준 인터페이스가 없어 다양한 네트워크 보안 기능들을 이용하고 있는 보안 서비스 관리자들이 보안 정책 규칙 생성 및 적용에 어려움을 겪고 있다. 이러한 문제를 해결하고자 Internet Engineering Task Force (IETF)의 Interface to Network Security Functions (I2NSF) Working Group (WG)[1]에서 표준 인터페이스[2][3]를 제정하고 있으며 이와 관련된 네트워크 보안 기능 프레임워크[4]를 설계 하고 있다.

본 논문에서는 IETF I2NSF WG에서 제안하고 있는 프레임워크를 살펴보고 이를 바탕으로 구현한 내용을 제안한다. 제안된 프로그램은 IETF 해커톤[5] 프로그램에서 개발되었으며 Best University Award[6]를 수상하였다.

2. I2NSF 프레임워크 구조

본 섹션에서는 I2NSF 프레임워크에서 사용되는 컴퍼넌트들과 인터페이스 대해서 설명한다. 그림 1은 I2NSF 프레임워크를 보여준다.

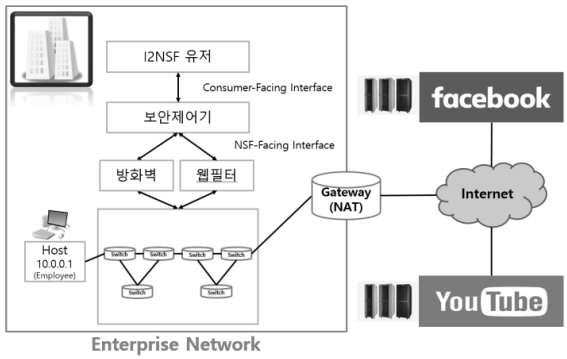

그림 1. I2NSF 프레임워크

2.1. I2NSF 프레임워크 컴퍼넌트

본 섹션에서는 I2NSF 프레임워크 컴퍼넌트 대해서 설명한다. I2NSF 프레임워크 컴퍼넌트는 I2NSF 유저, 보안 제어기, 네트워크 보안 기능(방화벽 및 웹필터)들로 이루어져 있다.

2.1.1. I2NSF 유저

고수준 보안 정책 규칙을 생성하는 컴퍼넌트. 본 컴퍼넌트는 웹으로 구현 되었으며 I2NSF 유저에서 생성된 고수준 보안 정책 규칙들은 RESTCONF 프로토콜[7]을 통해 보안제어기에 전달 된다.

2.1.2. 보안 제어기

네트워크 보안 기능을 관리하는 컴퍼넌트. 본 컴퍼넌트는 I2NSF 유저로부터 받은 고수준 보안 정책을 저수준 보안 정책으로 번역하고 번역된 저수준 보안 정책을 NETCONF 프로토콜[8]을 통해 알맞은 네트워크 보안 기능에 전달한다.

2.1.3. 네트워크 보안 기능

네트워크 통신의 무결성 및 기밀성을 보장하기 위하여 악의적인 네트워크 트래픽을 감지하고 차단하는 컴퍼넌트. 본 컴퍼넌트는 보안 제어기로부터 받은 저수준 보안 정책을 이용하여 보안 정책이 수립된다.

2.2 I2NSF 프레임워크 인터페이스

본 섹션에서는 I2NSF 프레임워크 인터페이스 대해서 설명한다. I2NSF 프레임워크 인터페이스는 Consumer-Facing Interface와 NSF-Facing Interface로 이루어져 있다.

2.2.1 Consumer-Facing Interface

I2NSF 유저와 보안 제어기 사이의 인터페이스. 본 인터페이스를 통해 I2NSF 유저에서 생성된 고수준 보안 정책 규칙들이 보안 제어기에 전달 될 수 있다.

2.2.2 NSF-Facing Interface

보안제어기와 네트워크 보안 기능 사이의 인터페이스. 본 인터페이스를 통해 보안 제어기에서 번역된 저수준 보안 정책 규칙들이 네트워크 보안 기능에 전달 될 수 있다.

3. I2NSF 프레임워크 구현 및 적용 시나리오

본 섹션에서는 I2NSF WG에서 제안하고 있는 프레임워크 타당성 검증을 위해 구현한 내용을 보여주며 실제 네트워크 환경 속에서 어떻게 적용이 될 수 있는지를 회사 네트워크 시나리오를 이용하여 I2NSF 프레임워크의 타당성을 검증하였다. 본 네트워크 토폴로지는 미니넷(mininet)[9]을 이용하여 구현하였다.

3.1. 시나리오 구성

본 섹션에서는 I2NSF 프레임워크 적용 시나리오 대해서 설명한다. I2NSF 프레임워크 적용 시나리오로는 방화벽을 사용한 회사 방화벽 시나리오와 웹필터를 사용한 회사 웹필터 시나리오로 이루어져 있다.

3.1.1 회사 방화벽 시나리오

본 시나리오에서는 회사에서의 방화벽 시나리오를 보여 준다. 본 시나리오에서는 회사 내부 네트워크에서의 원치 않은 네트워크 서비스를 차단하기 위하여 패킷의 포트 번호를 검사하여 차단한다.

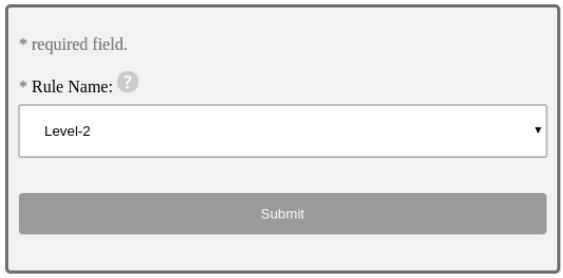

그림 2. 회사 방화벽을 위한 고수준 보안 정책

그림 2는 보안 정책 생성을 위한 I2NSF 유저의 고수준 보안 정책을 보여준다. 이와 같이 I2NSF 유저에서는 관리자들이 쉽게 보안 정책을 생성하기 위하여 고수준 보안 정책을 제공한다. 이렇게 생성된 고수준 보안 정책은 RESTCONF 프로토콜을 통해 보안 제어기에 전달되며 보안제어기는 전달 받은 고수준 보안 정책을 저수준 보안 정책으로 번역 한다. 이때 번역된 저수준 보안 정책은 I2NSF WG에서 제정하고 있는 NSF-Facing Interface 표준에 맞춰 변환되며 표준 데이터 모델을 위하여 YANG[10] 데이터 모델을 이용한다. 이와 같이 변환된 저수준 보안 정책은 NETCONF 프로토콜을 통해 방화벽으로 전달된다. 방화벽은 전달 받은 저수준 보안 정책을 이용하여 보안 정책을 수립한다.

```
pass tcp any any -> any [23,109,110,143,443] (
msg:"Enterprise Mode"; sid:20; rev:1;)
reject tcp any any -> any any (msg:"Enterprise
 Mode-TCP"; sid:2001; rev:1;)
```

그림 3. 회사 방화벽을 위한 저수준 보안 정책

그림 3은 알맞게 설정된 원치 않은 서비스를 차단하기 위한 회사 방화벽 보안 정책을 보여 준다.

3.1.2 회사 웹필터 시나리오

본 시나리오에서는 회사에서의 웹필터 시나리오를 보여 준다. 본 웹필터 시나리오는 회사 내부 네트워크에서의 원치 않은 웹사이트를 차단하기 위하여 패킷 페이로드 내용을 검사하여 차단한다.

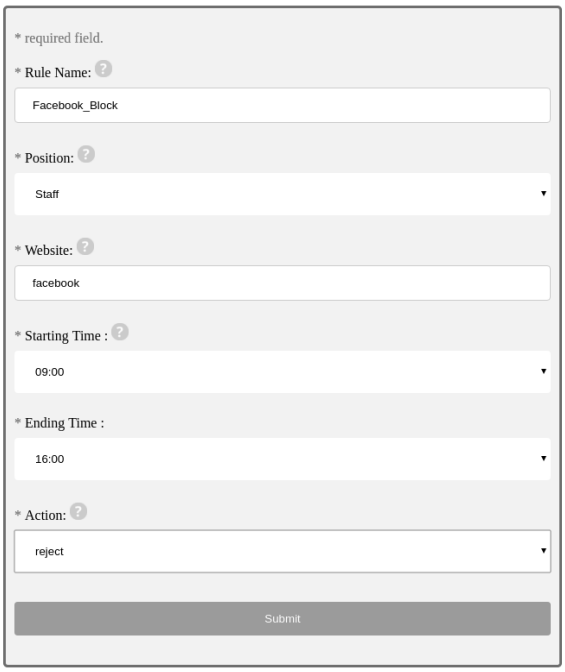

그림 4. 회사 웹필터를 위한 고수준 보안 정책

그림 4는 보안 정책 생성을 위한 I2NSF 유저의 고수준 보안 정책을 보여준다. 3.1.1의 회사 방화벽 시나리오와 같이 이렇게 생성된 고수준 보안 정책은 RESTCONF 프로토콜을 통해 보안 제어기에 전달되며 보안제어기는 전달 받은 고수준 보안 정책을 저수준 보안 정책으로 번역 한다. 이와 같이 변환된 저수준 보안 정책은 NETCONF 프로토콜을 통해 웹필터로 전달된다. 웹필터는 전달 받은 저수준 보안 정책을 이용하여 보안 정책을 수립한다.

```
reject tcp [10.0.0.1,10.0.0.2,10.0.0.3,10.0.0.4,10.0.0.5,1
0.0.0.6,10.0.0.7,10.0.0.8,10.0.0.9] any -> any any (msg:"W
ebsite Reject"; content:"facebook"; nocase; sid:1; rev:1;)
```

그림 5. 회사 웹필터를 위한 저수준 보안 정책

그림 5은 알맞게 설정된 원치 않은 웹사이트를 차단하기 위한 회사 웹필터 보안 정책을 보여 준다.

4. 결론

본 논문에서는 IETF I2NSF WG에서 제안한 네트워크 보안 기능을 위한 프레임워크를 살펴보았고 프레임워크 타당성 검증을 위해 회사 네트워크에서의 2가지 시나리오를 이용하여 구현한 내용을 보여주었다. 이와 같이 구현된 프로그램을 통해 I2NSF 프레임워크의 타당성을 보여주었다. 향후 연구로써 미니넷 환경이 아닌 오픈스택(Open Stack)[11]을 이용하여 보다 실제 환경에 가깝게 구현하여 실제 환경에 적용될 수 있도록 구현할 예정이다.

5. Acknowledgment

이 논문은 2017년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업(No. 2017R1D1A1B03035885)이고, 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구(No. 2016-0-00078, 맞춤형 보안서비스 제공을 위한 클라우드 기반 지능형 보안 기술 개발)임.

6. 참고문헌

[1] IETF I2NSF Working Group, “Interface to Network Security Functions(I2NSF)”, http://datatracker.ietf.org/wg/i2nsf

[2] Xia, L., Strassner, J., Basile, C., and D. Lopez, “Information Model of NSFs Capabilities”, IETF Internet Draft, draft-xibassnez-i2nsf-capability-02, July 2017.

[3] Kumar, R., Lohiya, A., Qi, D., Bitar, N., Palislamovic, S., and L. Xia, “Information model for Client-Facing Interface to Security Controller”, IETF Internet Draft, draft-kumar-i2nsf-client-facing-interface-im-03, July 2017.

[4] Lopez, D., Lopez, E., Dunbar, L., Strassner, J., and R. Kumar, “Framework for Interface to Network Security Functions”, IETF Internet Draft, draft-ietf-i2nsf-framework-06, July 2017.

[5] IETF Hackathon, “IETF Hackathon Program”, https://www.ietf.org/hackathon/

[6] Hackathon Award, “Best University Award”, https://communities.cisco.com/community/developer/opensource/blog/2017/07/23/running-code-is-king-at-ietf-99-in-prague/

[7] Bierman, A., Bjorklund, M., and K. Watsen, “RESTCONF Protocol”, RFC 8040, January 2017.

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

[9] Mininet, “An instant virtual network on your laptop”, http://mininet.org

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

[11] Open Stack, “Open source software for creating private and public cloud”, https://www.openstack.org/