I2NSF Framework를 위한 XSLT 기반의 네트워크 보안정책 변환 기법

홍동진, 김진용, 정재훈
성균관대학교 전자전기컴퓨터공학과
{dong.jin, timkim, pauljeong}@skku.edu

A Method of Policy Translation for I2NSF Framework based on XSLT

Dongjin Hong, Jinyong (Tim) Kim, and Jaehoon (Paul) Jeong
Department of Computer Science and Engineering, Sungkyunkwan Univ.

요 약

본 논문은 IETF(Internet Engineering Task Force) I2NSF(Interface to Network Security Functions) 프레임워크가 관리하는 네트워크 보안 기능(Network Security Functions, NSFs)에 정책을 설정하기 위한 상위 수준의 정책을 하위 수준의 정책으로 번역하는 방법에 대해 소개한다. IETF I2NSF WG(Working Group)는 네트워크 보안 기능을 효율적으로 관리하고 제공하기 위한 표준화를 진행 중이다. 해당 워킹 그룹은 관리자가 생성한 상위 수준의 정책이 보안제어기(Security Controller)에 의해 하위 수준의 정책으로 번역되어 네트워크 보안 기능에 설정된다고 기술하였다. 하지만 구체적인 정책 번역 방안을 제시하지 않았다. 따라서 본 논문에서는 XSLT(Extensible Stylesheet Language Transformations)를 이용하여 상위 수준의 정책을 하위 수준의 정책으로 번역하는 방법을 제안한다.

Ⅰ. 서 론

컴퓨터 네트워크는 라우터, 스위치, 허브 등의 많은 하드웨어와 여러 프로토콜을 포함한 소프트웨어의 복잡한 조합으로 이루어져있다. 이러한 복잡성은 방대한 규모의 네트워크에서 오류가 발생하면 찾기 어려울 뿐만 아니라 관리함에 있어 어려움을 겪는다. 또한, 미국의 시장조사기관인 가트너(Gartner)는 2020년도까지 200억개 이상의 디바이스가 존재할 것이라고 발표했다[1]. 이것은 개인이나 집단을 위한 스마트 디바이스의 수가 증가하고 많은 트래픽을 유발함을 의미한다. 스마트 디바이스의 수가 증가함에 따라 예측할 수 없는 대량의 트래픽은 다양하고 새로운 공격에 이용될 것으로 예측된다.

이러한 문제를 해결하기 위해 IETF(Internet Engineering Task Force) I2NSF(Interface to Network Security Functions) Working Group[2], [3]은 다양한 제조사에서 개발된 네트워크 보안 서비스를 호환시키고 제공하기 위한 표준 인터페이스를 정의하고 구현하여 미래에 발생할 수 있는 다양한 공격을 막고 약화시키기는 것을 목표로 활발한 표준화활동을 진행 중이다. 해당 WG는 최근 오픈소스 프로젝트를 통해 활발한 연구 및 개발 활동이 이루어지고 있는 네트워크를 소프트웨어를 통해 동적으로 관리하는 소프트웨어 정의 네트워킹(Software-Defined Networking, SDN)[4] 기술과 네트워크 리소스를 가상화하여 사용가능하게 하는 네트워크 기능 가상화(Network Functions Virtualization, NFV)[5] 기술을 이용해 I2NSF 프레임워크를 설계 및 구현중이다. I2NSF 프레임워크는 SDN 및 NFV를 이용하는 네트워크 환경에서 관리자가 생성한 상위 수준 정책이 보안제어기(Security Controller)에 의해 하위 수준 정책으로 번역되어 물리적 또는 가상적으로 만들어진 방화벽(Firewall), 침입 탐지 시스템(Intrusion Detection System, IDS), 침입 방지 시스템(Intrusion Prevention System, IPS) 그리고 심층 패킷 분석(Deep Packet Inspection, DPI) 등과 같은 네트워크 보안 함수(Network Security Functions, NSF)에 적용함으로써 보안 서비스를 제공할 수 있음을 기술했다[6]. 하지만 해당 워킹 그룹은 상위 수준 정책이 하위 수준 정책으로 번역됨을 기술하였지만 구체적인 구현 방안을 제시하지 않았고 해당 워킹 그룹의 표준화 범위에 포함되지 않는다고 기술했다.

따라서, 본 논문에서는 XSLT(Extensible Sylesheet Language Transformations)[7]를 기반으로 I2NSF 프레임워크에 필요한 상위 수준 정책을 하위 수준 정책으로 번역하는 방법을 제안하고 구현방법에 대해 기술한다.

Ⅱ. 본 론

본 섹션에서는 I2NSF 프레임워크, XSLT(Extensible Stylesheet Language Transformations) 그리고 XSLT 기반의 정책 번역에 대해 설명한다.

1. I2NSF 프레임워크

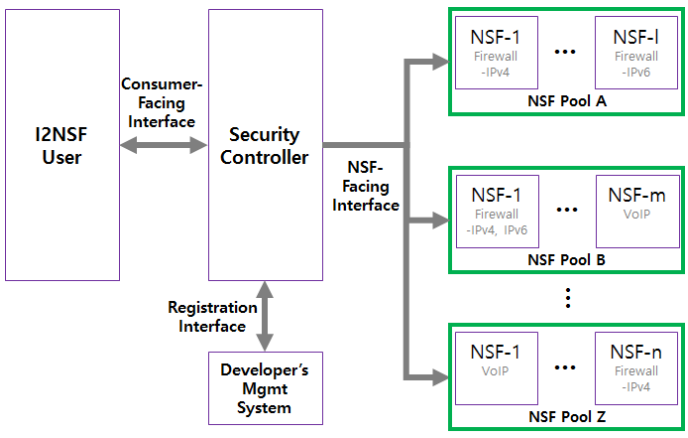

그림 1. I2NSF 프레임워크

그림 1은 I2NSF 프레임워크를 보여준다. I2NSF 프레임워크의 기본적인 동작 과정은 다음과 같다. 네트워크 보안 관리자는 I2NSF User를 통해 상위 수준 보안 정책 규칙을 생성하고 RESTCONF 프로토콜[8]을 사용하는 Consumer Facing Interface를 통해 보안 제어기에게 전달된다. 보안 제어기는 상위 수준 보안 정책을 네트워크 보안 기능이 이해할 수 있는 하위 수준 보안 정책으로 번역하고 NETCONF 프로토콜[9]을 통해 알맞은 네트워크 보안 기능에게 전달한다. 하위 수준 보안 정책을 전달 받은 네트워크 보안 기능은 이를 반영하여 다양하고 복잡한 공격들로부터 네트워크를 보호한다. Registration Interface는 네트워크 보안 기능을 개발하는 제조사가 개발한 네트워크 보안 기능을 I2NSF 프레임워크에 등록하여 사용이 가능하게 한다. 현재 Registration Interface를 제외한 프레임워크는 I2NSF WG이 IETF Hackathon[10]에 참여하여 구현했고 주기적으로 추가적인 기능들을 추가하며 프레임워크를 완성도 있게 발전시키고 있다.

2. Extensible Stylesheet Language Transformations

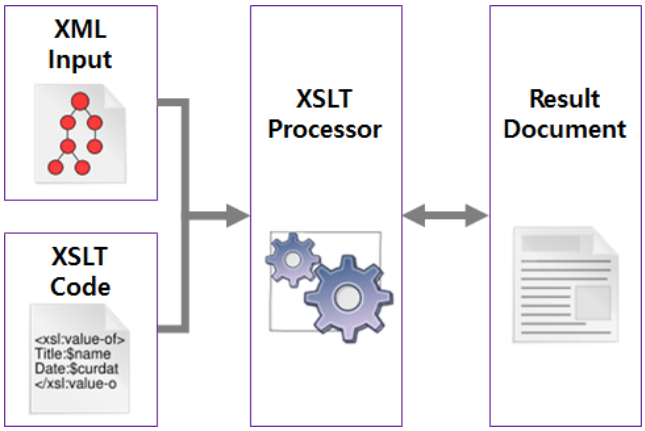

그림 2. XSLT의 문서 프로세싱 과정

XSLT는 XML 문서를 XML 또는 다른 형식의 문서로 변환하는데 사용하는 W3C(World Wide Web Consortium)[11]에서 제정한 XML 기반의 언어이다. 그림 2는 XSLT의 문서 프로세싱 과정을 보여준다. 원본 문서인 XML Input은 변경되지 않으며, 원본 문서와 원본 문서를 적용시킬 스타일시트인 XSLT Code를 기반으로 XSLT Processor가 새로운 문서인 Result Document를 생성한다.

3. XSLT 기반의 정책 번역

I2NSF 프레임워크에서 사용하는 RESTCONF 프로토콜과 NETCONF 프로토콜은 통신을 위해 XML 문서 형식을 지원하도록 설계되었고 XML 문서 형식을 원하는 대로 변경할 수 있는 XSLT를 사용해 User가 이해하기 쉬운 정책을 네트워크 보안 기능이 이해할 수 있는 정책으로 번역하는 것이 가능하다. 따라서 본 연구에서는 앞서 설명한 I2NSF 프레임워크의 동작 과정 중 보안 제어기가 전달받은 상위 수준 보안 정책을 하위 수준 보안 정책으로 번역하는 것을 XSLT를 기반으로 구현하였다. I2NSF User가 생성한 상위 수준 보안 정책은 XML 문서 형식으로 파싱되고 이는 그림2의 XML Input에 해당된다. 또한, I2NSF 프레임워크상의 대표적인 네트워크 보안기능은 Snort[12]의 룰 형식을 지원한다. 이에 맞춰 미리 정의한 스타일시트와 함께 상위 수준 보안정책이 XSLT 프로세서에게 넘겨지고 XSLT의 문서 프로세싱의 결과로 네트워크 보안 기능이 이해할 수 있는 정책이 얻어지도록 구현을 완료하였다.

Ⅲ. 결 론

본 논문에서는 IETF I2NSF 프레임워크가 관리하는 네트워크 보안 기능에 정책을 설정하기 위한 단계 중 상위 수준의 정책을 하위 수준의 정책으로 번역하기 위해 XSLT를 조사하고 이를 기반으로 정책 번역을 구현하였다. 본 논문에 제안된 정책 번역 방식이 표준화에 기여할 수 있다고 믿는다. 향후 연구로 현재 구현의 결과인 정적인 정책 번역이 아니라, 동적인 정책 번역을 위해 스타일시트를 동적으로 정의할 수 있는 새로운 알고리즘을 설계하여 동적으로 번역하고 이를 기반으로 얻은 결과를 검증하는 방법에 대해 연구하려 한다.

ACKNOWLEDGMENT

"본 논문은 2017년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구(2016-0-00078, 맞춤형 보안서비스 제공을 위한 클라우드 기반 지능형 보안 기술 개발)이고, 본 연구는 과학기술정보통신부 및 정보통신기술진흥센터의 대학ICT연구센터육성지원사업의 연구결과로 수행되었음" (IITP-2017-0-01633).

참 고 문 헌

[1] Gartner, Inc., "Gartner Says the Internet of Things Installed Base Will Grow to 26 Billion Units By 2020", http://www.gartner.com/newsroom/id/2636073.

[2] IETF, "The Internet Engineering Task Force", https://ietf.org

[3] IETF I2NSF Working Group, "Interface to Network Security Functions(I2NSF)", https://datatracker.ietf.org/wg/i2nsf/charter

[4] ONF, "Software-Defined Networking: The New Norm for Networks", ONF White Paper, April. 2012.

[5] ETSI-NFV, "Network Functions Virtualization (NFV); Architectural Framework", ETSI GS NFV 002 V1.2.1, December. 2014.

[6] J. Jeong, S. Hyun, T. Ahn, S. Hares, and D. Lopez, "Applicability of Interfaces to Network Security Functions to Network-Based Security Services", IETF draft-ietf-i2nsf-applicability-01, Nov. 2017.

[7] XSLT, "XSL Transformations", http://www.w3.org/TR/xslt/

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

[9] R. Enns, M. Bjorklund, J. Schoenwaelder, and A. Bierman, "Network Configuration Protocol (NETCONF)," IETF RFC 6421, Jun, 2011.

[10] IETF Hackathon, "Hackathon on Every The Internet Engineering Task Force Meeting", https://ietf.org/hackathon/index.html

[11] W3C, "World Wide Web Consortium", http://www.w3.org/

[12] Snort, "Open Source Intrusion Prevention System", https://www.snort.org/