December 2015, Vol. 28, No. 4

OSIA
Standards & Technology Review
Journal

http://www.osia.or.kr

ISSN 1738-9887

(사)개방형컴퓨터통신연구회
Open Standards and Internet Association

Contents

• December 2015, Vol. 28, No. 4
• 발 행 인: 신용태
• 편집위원: 한연희
• 발 행 처: 사단법인 개방형컴퓨터통신연구회 / 서울시 강남구 테헤란로 88길22(대치동)
• 발 행 처 TEL. (02)**562-7041** FAX. (02)**562-7040**
• 발 행 일: 2015. 12
• e-Book제작: 쓰리코어

I2NSF 기술 및 표준화 동향

정재훈
성균관대학교 인터랙션사이언스학과

Abstract

IETF(Internet Engineering Task Force) I2NSF(Interface to Network Security Functions) 워킹그룹은 2015년 11월부터 공식적으로 표준활동을 시작하여, 현재 네트워크 가상화를 이용하는 보안미들박스를 위한 네트워크 보안 기능에 대한 표준인터페이스를 표준화하려고 한다. 본고에서는 I2NSF 기술의 표준화 동향을 조명하고, I2NSF 프레임워크 및 표준인터페이스, I2NSF 유스케이스, I2NSF를 위한 정보 모델, 그리고 I2NSF를 이용하는 SDN 기반 보안서비스를 소개한다.

1. 서론

I2NSF(Interface to Network Security Functions)[1]는 NFV(Network Functions Virtualization)[2]를 기본 인프라로 이용하는 네트워크 환경에서 네트워크 보안 서비스(Network Security Service)를 제공하기 위한 표준 인터페이스를 정의하고 구현하는 것을 목표로 한다. I2NSF는 네트워크 서비스 인프라 구축 및 운영 비용을 절감하기 위한 네트워크 기능 가상화인 NFV 기반으로 다양한 네트워크 서비스를 제공할 때 다양한 벤더들의 보안 서비스들이 표준인터페이스로 통일된 방식으로 이용될 수 있게 하고자 한다.

I2NSF의 적용할 수 있는 네트워크는 클라우드, 거주자 네트워크, 모바일 네트워크 등이 있다. 네트워크 사용자 또는 관리자가 보안 정책을 설정하면 I2NSF는 이러한 보안 정책이 해당 네트워크에 적용될 수 있도록 보안함수의 룰이 자동으로 설정될 수 있게 한다. 이러한 자동화된 I2NSF의 보안서비스는 다양한 보안 벤더의 보안함수들이 NFV 플랫폼에서 접근성(availability), 확장성(scalability), 관리성(manageability), 효율성(efficiency)을 고려한 최적화된 보안서비스를 제공할 수 있다.

I2NSF는 2014년 11월에 개최된 IETF 91차 회의에서 BoF(Birds of a Feather, 워킹그룹 형성 회의)로 시작되었고, 2015년 7월에 IETF 93차 회의에서 두 번째 BoF를 개최하였다. 2015년 11

월에 I2NSF는 공식적인 워킹그룹으로 표준화 활동을 본격적으로 시작하였다. I2NSF가 시작된 배경은 최근에 네트워크 서비스 인프라 구축 및 운영 비용을 절감하기 위한 네트워크 기능 가상화인 NFV 연구 및 개발이 유럽 표준화 기구인 ETSI를 중심으로 인터넷 서비스 제공자, 네트워크 장비 회사에 의해 진행되고 있다. 또한 네트워크의 유연하고 효과적 진화와 관리를 위해 데이터 플레인(Data Plane)과 콘트롤 플레인(Control Plane)을 분리하고 제어 서버를 통해 네트워크 디바이스를 관리하는 소프트웨어 중심의 네트워크인 SDN(Software-Defined Networking)을 I2NSF에 적용하려는 연구 및 개발 활동이 활발하다.

본고를 통해 이러한 IETF I2NSF 기술 표준 동향을 살펴볼 것이다. 본고는 다음과 같이 구성되어 있다. 2장에서는 I2NSF 프레임워크 및 표준인터페이스를 설명한다. 3장에서는 I2NSF 유스케이스를 설명한다. 4장에서는 I2NSF를 위한 정보 모델을 설명한다. 5장에서는 I2NSF를 이용하는 SDN 기반 보안서비스를 설명한다. 그리고 6장에서 결론을 내린다.

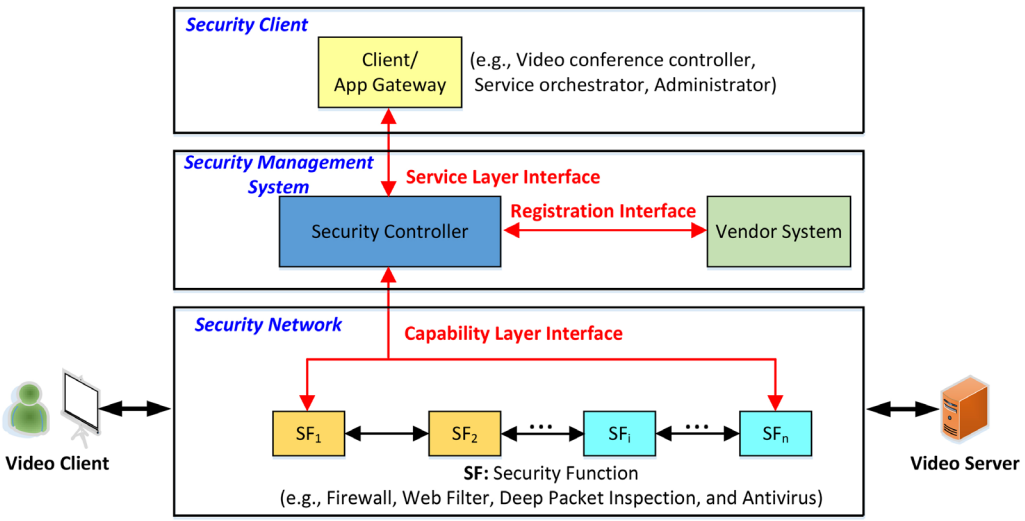

그림 1. I2NSF 프레임워크

2. I2NSF 프레임워크 및 표준인터페이스

I2NSF는 네트워크 서비스의 사용자(Client), 사용자가 NFV 환경에서 보안 서비스를 사용할 수 있게 보안 제어기(Security Controller) 그리고 보안 서비스를 실제로 수행하는 보안 기능(Security Function, SF)으로 구성된다[3,4]. 그림 1은 I2NSF의 프레임워크를 보여주고 있다. 또한 I2NSF 프레임워크에서의 세 가지 인터페이스를 정의하고 있다.

1. 서비스 계층 인터페이스(Service Layer Interface): 보안서비스 사용자(예, 이동통신망 관리자)가 서비스 계층 인터페이스를 통해 보안 제어기에게 고수준 보안정책(High-level

Security Policy)를 전달한다.

2. 기능 계층 인터페이스(Capability Layer Interface): 보안 제어기는 전달받은 고수준 보안 정책을 NFV 상의 보안 기능(SF)에서 실행될 수 있는 저수준 보안기능(Low-level Security Functions)으로 번역한다. 보안 제어기는 이 보안기능을 기능 계층 인터페이스를 통해 적합한 보안 기능 가상 머신 또는 물리 머신에 전달하여 요청된 보안서비스를 실행한다.
3. 등록 인터페이스(Registration Interface): 보안서비스 공급자(예, Symantec, Verisign, AhnLab)는 벤더 관리 시스템(Vendor Management System)을 가지고 등록 인터페이스를 통해 보안 제어기를 거쳐서 I2NSF의 SF에서 실행될 보안서비스 패키지를 설치한다.

I2NSF는 현재 그림 1에서 서비스 인터페이스와 기능 인터페이스를 표준화를 진행할 예정이고, 등록 인터페이스는 I2NSF 표준화에 포함시키지 않을 예정이다. 그림 1은 이러한 I2NSF 프레임워크에서 Video Client는 보안 클라이언트의 보안 정책에 따라 Video Server로부터 Video Streaming Service를 받는 것을 보여주고 있다.

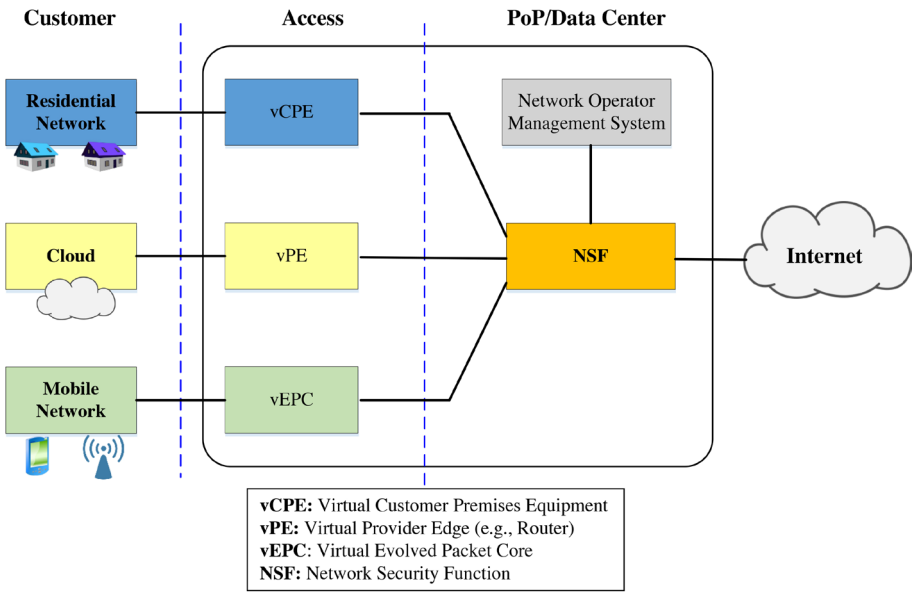

그림 2. I2NSF 유스케이스

3. I2NSF 유스케이스

본 절에서는 I2NSF의 일반적인 유스케이스를 설명한다. 그림 2는 I2NSF를 이용하는 유스케이스를 기술하고 있다[5]. 네트워크 고객(Customer)들은 거주 네트워크(Residential Network), 클라우드(Cloud) 및 이동 네트워크(Mobile Network)에서 보안서비스를 이용하여 안전하게 네트

워킹 기반의 서비스를 받고자 한다. 각 고객 네트워크는 인터넷 서비스 제공자(Internet Service Provider, ISP)가 이러한 고객 네트워크를 수용하기 위해 NFV 환경에서 가상머신에서 동작하는 연결 디바이스(예, vCPE, vPE, vEPC)를 통해 보안서비스 함수(Network Security Function, NFV)를 이용하게 할 수 있다. ISP는 I2NSF를 통해 이러한 고객 네트워크들의 사용자들이 원하는 보안 정책에 따라 적합한 보안서비스 함수를 NFV 환경에게 유연하고도 확장성 있게 이용할 수 있게 하기를 원한다. 보안서비스가 여러 벤더(Vendor)에 의해 제공될 때 I2NSF와 같은 표준인터페이스가 필요하다.

그림 3. I2NSF 기능 계층 인터페이스를 위한 정보 모델

4. I2NSF를 위한 정보 모델

I2NSF 워킹그룹은 서비스 계층 인터페이스와 기능 계층 인터페이스의 표준화를 목표로 하고 있다. 서비스 계층 인터페이스는 고수준 응용 프로그램(예, Openstack, BSS/OSS)와 보안 제어기 사이의 통신 채널과 보안서비스 요청 정보 모델(Information Model)을 통일해야 한다[6]. 서비스 계층 인터페이스의 목표는 응용 계층에서의 보안서비스를 다양한 보안 디바이스와 그들의 디바이스 수준의 보안 함수로부터 독립시키는 것이다. 이러한 목표를 위한 정보 모델을 의도 기반의 정보모델(Intent-based Information Model)이라 명한다.

기능 계층 인터페이스는 네트워크 보안함수인 NSF(예, Firewall, AAA, IPS, Anti-DDoS, Anti-Virus)들이 NFV 환경에서 가상머신에 동작하든 물리적 기기(Physical Appliance)에서 동작하든 간에 보안 제어기와의 통일된 인터랙션을 제공해야 한다. 현재는 NSF 벤더(Vendor)들이 보안 함수 제어를 위해 각기 다른 인터페이스와 정보모델을 제공하고 있는데, I2NSF는 이러한 인터페이스와 정보모델의 표준화를 목표로 하고 있다. I2NSF의 기능 계층 인터페이스는 NSF들을 상위 계층 보안서비스 요청으로부터 분리시키고 NSF들이 제공하는 보안 기능을 명확히 하는 것을 목표로 한다. 기능 계층 인터페이스는 그림 3과 같이 네트워크 보안 제어(Network Security Control), 컨텐트 보안 제어(Content Security Control) 및 공격 약화 제어(Attack Mitigation Control)를 지원한다[6]. 본 절에서는 기능 계층 인터페이스가 방금 언급된 세가지 제어를 위한 정보모델(Information Model)을 기술한다.

4.1 네트워크 보안 제어(Network Security Control)

네트워크 보안 제어(Network Security Control)은 방화벽과 같이 선행적으로 정의된 보안정책 기반으로 네트워크를 통과하는 트래픽을 감찰하고 처리하는 기능을 말한다. 보안 기능(Security Capability)는 패킷 또는 플로우 관점에서 네트워크를 통과하는 패킷을 감찰하고는 패킷 처리 엔진(Packet-processing Engine)을 의미한다. 보안 기능은 패킷 감찰을 위해 패킷의 헤더(Header)와 페이로드(Payload)를 감찰한다. 또한 패킷의 플로우의 콘텍스트 상태(Context State)를 유지하면서 적절한 액션(Action)을 취한다.

기능 계층 인터페이스는 패킷 및 플로우를 감찰하고 처리하는 정책 디자인 패러다임으로 “Subject-Object-Action-Function” 패러다임을 제안하고 있다. 그림 4는 네트워크 보안제어를 위한 Subject-Object-Action-Function 패러다임을 보여주고 있다. 이 패러다임에 의해 패킷에 연관된 Subject와 Object에 따라 적합한 Action과 Function을 수행하여 패킷 기반으로 보안 서비스를 실시한다.

Subject는 보안 정책에서 매칭 조건(Matching Condition)을 위해 패킷 헤더나 페이로드에서 직간접적으로 획득되는 정보 또는 속성(Attribute)을 의미한다. Object는 패킷이나 플로우를 위한 컨텍스트 정보를 의미한다.

Object는 User, Schedule, Region, Target 및 State를 지정한다. User는 네트워크 플로우가 연관된 사용자 또는 사용자 그룹 정보(예, Name, ID, Password, Type, Authentication Mode, IP Address)를 의미한다. Schedule은 네트워크 플로우가 발생하는 시간 및 시간대를 의미한다. Region은 네트워크 트래픽이 연관된 위치를 의미한다. Target은 네트워크 환경에서 서비스, 응용 프로그램 및 디바이스를 지칭한다. 서비스는 Protocol Type(예, TCP, UDP, ICMP, IP)과 Port Number로 구분되는 응용 프로그램을 의미한다. 디바이스를 구분하는 속성은 Type(예, Router, Switch, PC, IOS, Android)과 디바이스 Owner를 포함한다. State는 네트워크 플로우가 연관된 다양한 상태를 의미한다. 예를 들면, State는 TCP Session State(즉, New, Established, Related, Invalid, Untracked) 또는 디바이스의 접근 모드(예, Wire, Wireless, VPN)를 가리킬 수 있다.

Action은 트래픽 필터링(Filtering) 또는 스프레션(Suppression)을 위한 액션을 의미한다. 예를 들면, 액션들은 거부(deny), 허용(permit), 미러(mirror), 디벌젼(diversion), 레이트 리미팅(rate limiting), 블랙/화이트 리스트(black/white list), QoS 액션(QoS actions), 루트 블랙 홀(route black hole) 등이 있다.

Function은 네트워크 트래픽에 대해 벤더에 의해 정의된 고급 처리(Advanced Treatment)를 위해 호출될 수 있는 보안 기능을 의미한다.

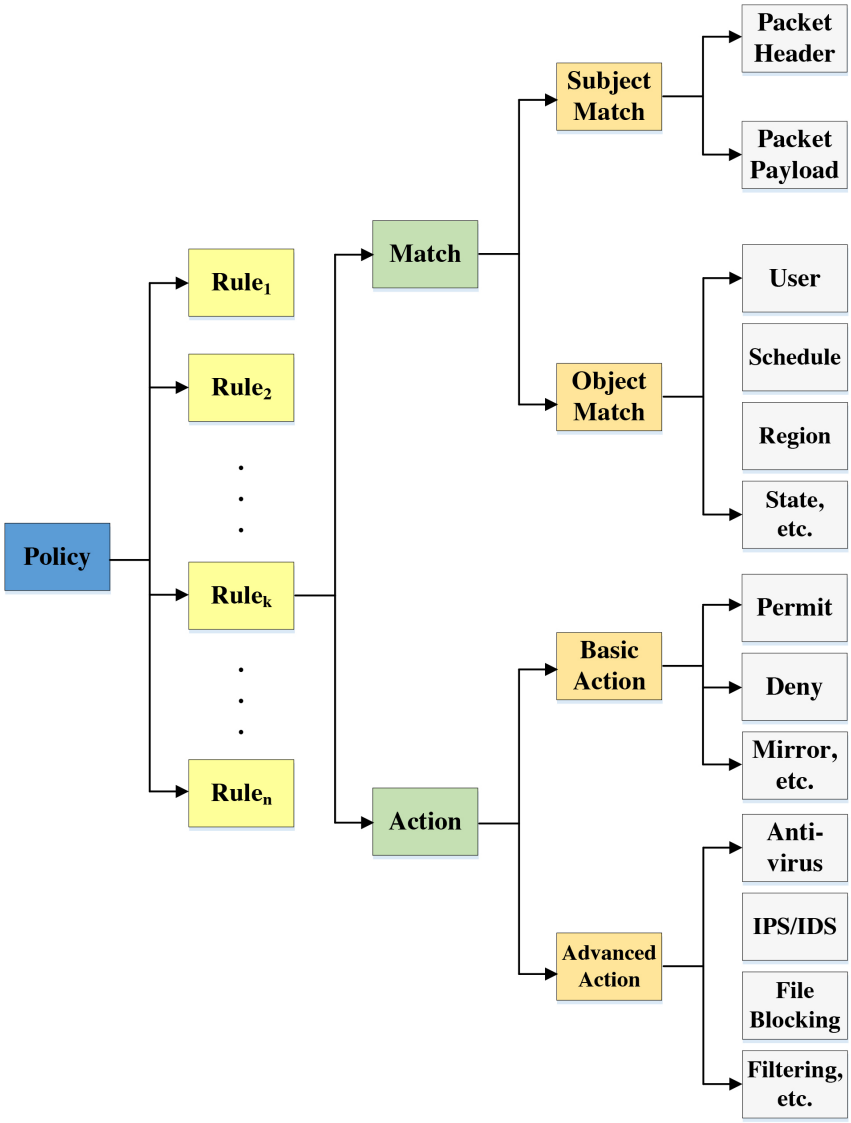

그림 4. 네트워크 보안제어를 위한 Subject-Object-Action-Function 패러다임

4.2 컨텐트 보안 제어(Content Security Control)

컨텐트 보안 제어(Content Security Control)은 응용 계층에 적용되는 보안 기능의 영역으로 패킷의 컨텐트를 기반으로 수행하는 보안 제어를 의미한다. 예를 들면, 컨텐트 보안 제어는 침입방지, 바이러스 검출, 악의성 URL 및 정크 이메일 필터링, 불법적 웹 접근 및 데이터 획득 블라킹 등을 포함한다.

응용 계층의 위협의 각 타입은 독특한 특성이 있기 때문에 각 타입에 적합한 방법으로 방어를 해야 한다. 새로운 응용 계층의 위협이 빨리 생성될 수 있으므로 이러한 위협에 대해 방어를 즉각적으

로 할 수 있는 많은 보안 기능들이 필요하다. 이러한 컨텐트 보안 제어는 유연성(Flexibility), 일반성(Generality), 확장성(Scalability) 및 자동화(Automation)를 기반으로 디자인 되어야 한다.

유연성을 위해 각 보안 기능은 다른 기능들과의 최소한의 오버랩 또는 독립성을 가지는 독립된 함수로 구성되어야 한다. 이러한 디자인으로 보안 기능들이 쉽게 이용되거나 합쳐져야 되고 하나의 보안 기능의 변경이 다른 보안 기능에 영향을 주어서는 안 된다.

일반성을 위해 각 보안 기능은 추상화(Abstraction)와 합병(Consolidation)을 고려하여 그 기능이 프로그램 가능할 수 있고 그 기능의 처리 결과 및 통계 정보를 보고할 수 있는 통일된 인터페이스를 가져야 한다. 또한 멀티 벤더 간의 상호통신을 지원해야 한다.

확장성을 위해 보안 기능을 담은 시스템의 스케일이 커지거나 작아지는 것이 지원되어야 한다. 이러한 확장성은 변하기 쉬운 네트워크 트래픽 및 서비스 요청으로부터의 성능 요구사항을 만족시킬 수 있다. 보안 기능은 보안 제어기가 보안 기능이 스케일 업 또는 다운되는 결정을 할 수 있도록 통계정보를 제공해야 한다.

자동화를 위해 보안 기능은 자동 탐색(Auto-discovery), 자동 협상(Auto-negotiation) 및 자동 갱신(Automatic Update)을 지원해야 한다.

4.3 공격 약화 제어(Attack Mitigation Control)

공격 약화 제어(Attack Mitigation Control)은 다양한 네트워크 공격을 발견하고 약화시킬 수 있는 기능이다. 오늘날의 네트워크 공격은 크게 DDoS Attack과 Single-packet Attack로 분류된다.

DDoS Attack은 네트워크 계층 DDoS 공격과 응용 계층 DDoS 공격으로 구분된다. 네트워크 계층 DDoS 공격은 SYN flood, UDP flood, ICMP flood, IP fragment flood 등이 있다. 응용 계층 DDoS 공격은 http flood, https flood, DNS flood, DNS amplification, SSL DDoS 등이 있다.

Single-packet Attack는 Scanning/Sniffing 공격, Malformed Packet 공격, Special Packet 공격으로 구분된다. Scanning/Sniffing 공격은 IP sweep, Port scanning 등이 있다. Malformed Packet 공격은 Ping of Death, Teardrop 등이 있다. Special Packet 공격은 Oversized ICMP, Tracert, IP timestamp option packets 등이 있다.

이러한 네트워크 공격들은 고유한 네트워크 행동 및 패킷/플로우 특성이 있으므로 공격 약화 제어는 이러한 공격을 즉각 발견해서 약화시킬 수 있게 디자인 되어야 한다.

5. I2NSF를 이용하는 SDN 기반 보안서비스

I2NSF 프레임워크와 정보 모델을 기반으로 SDN 기반의 보안 서비스 프레임워크에 대한 IETF 기고서가 제안되었다[7]. 본 기고서는 I2NSF을 사용하는 SDN 기반의 보안 서비스에서의 목적 및

요구사항을 기술하였고, 아울러 중앙집중식 방화벽 시스템과 중앙집중식 DDoS 공격 약화 시스템의 두 가지 유스케이스를 제시하였다. 첫 번째 유스케이스는 SDN 네트워크에서 NETCONF/YANG을 기반으로 방화벽 기능인 IP Address Filtering과 Web Filtering이다. 두 번째 유스케이스는 DDoS-Attack Mitigator이다. I2NSF를 이용하는 SDN 기반 보안서비스를 위해 기능 계층 인터페이스는 I2NSF의 정보 모델로 구현 가능하고, 서비스 계층 인터페이스는 SUPA 워킹그룹[8]에서 정의한 Policy Abstraction을 이용할 수 있다. 본 절에서는 이러한 I2NSF를 이용한 SDN 기반 보안 서비스에 대해 기술한다.

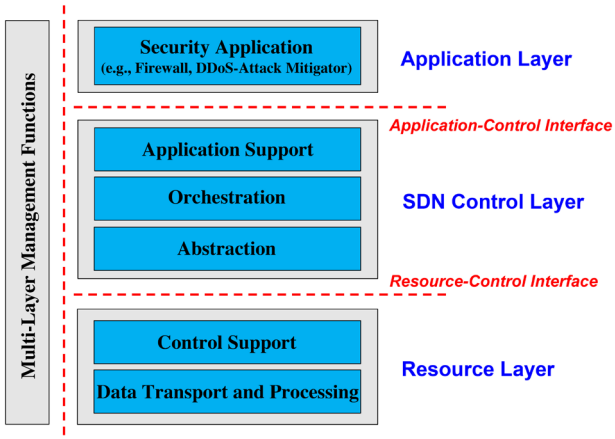

그림 5. SDN 기반 보안서비스를 위한 고수준 아키텍쳐

5.1 보안서비스를 위한 I2NSF를 이용한 SDN 기반 보안서비스 아키텍쳐

SDN은 관리자가 소프트웨어를 통해 네트워크 리소스들을 직접 프로그램하고, 오케스트레이트하고, 제어하고, 관리하는 기술을 제공하고 있다. 이러한 SDN은 SDN 제어기라는 네트워크 구성요소에게 네트워크 리소스들의 제어권을 부여하고 있다. 보안 서비스는 통상적으로 응용 프로그램으로 제공이 되나 네트워크 리소스들과 밀접한 관계를 가지고 있다. 네트워크 사용자 또는 관리자의 상위수준 보안정책에서 요청하는 보안 서비스를 SDN 네트워크에 자동으로 반영하기 위해서는 I2NSF의 프레임워크와 인터페이스를 이용할 수 있다.

그림 5는 중앙집중식 방화벽 시스템과 중앙집중식 DDoS 공격 약화 시스템과 같은 SDN 기반 보안서비스들을 지원하기 위한 레퍼런스 아키텍쳐를 보여주고 있다. 그림에서처럼 보안서비스(예, 방화벽, DDoS 공격 약화 서비스, 웹 필터, 딥 패킷 인스펙션)로써 보안 함수들은 SDN 컨트롤러를 통해 SDN 네트워크에서 동작한다. 관리자가 언급된 보안서비스들에 대한 보안정책을 응용 인터페이스를 통해 전달하면 SDN 컨트롤러는 자율적이면서 신속하게 해당 접근 제어 정책 규칙들을 생성한다. 생성된 접근 제어 정책 규칙에 따라 스위치와 같은 네트워크 리소스들은 의심되는 패턴을 가지는 패킷을 제거함으로써 네트워크 공격을 약화시키는 조치를 취한다.

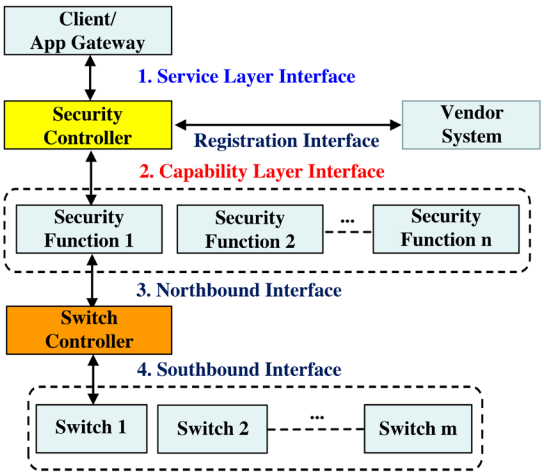

그림 6. I2NSF를 이용하는 SDN 기반 보안서비스를 위한 프레임워크

그림 6은 I2NSF를 이용하는 SDN 기반 보안서비스를 지원하는 프레임워크를 보여주고 있다. 그림에서 보이는 것처럼 클라언트 또는 응용 게이트웨이(App Gateway)는 고수준 보안정책을 서비스 계층 인터페이스를 통해 보안 제어기(Security Controller)에게 전달한다. 보안 콘트롤러는 전달받은 고수준 보안정책을 저수준 보안정책으로 번역하여 기능 계층 인터페이스를 통해 저수준 보안정책을 수행할 수 있는 보안 함수들에게 전달한다. 보안 함수들은 NFV 환경의 가상머신 또는 물리적 머신에서 동작할 수 있다. 이러한 보안 함수들은 스위치 제어기의 관리 하에 있는 스위치들에서 요청된 보안서비스가 될 수 있도록 스위치 제어기에게 요청한다. 보안 제어기와 보안 함수들 사이에 존재하는 기능 계층 인터페이스는 IETF의 네트워크 구성 프로토콜인 NETCONF[9]와 데이터 모델링 언어인 YANG[10]을 통해 구현될 수 있다. YANG은 함수 수준의 보안서비스를 기술하는데 용이하다.

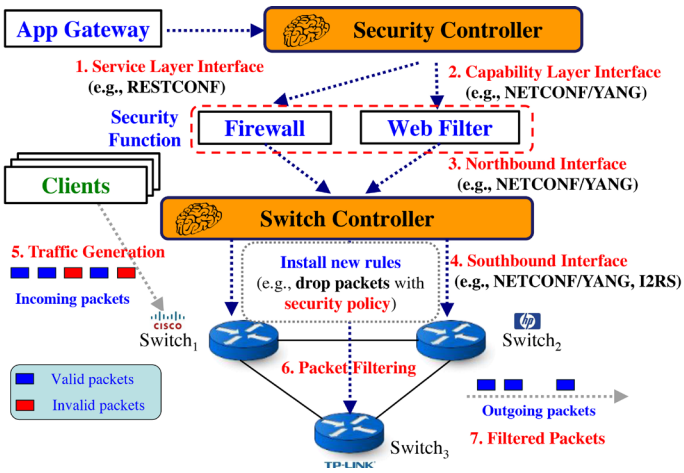

그림 7. SDN 기반 보안서비스 프레임워크를 이용하는 보안서비스 과정

그림 7은 SDN 기반 보안서비스 프레임워크를 이용하는 보안서비스 과정을 보여주고 있다.

1. 네트워크 관리자는 응용 게이트웨이(App Gateway)는 서비스 계층 인터페이스(Service Layer Interface)를 통해 보안 제어기(Security Controller)에게 고수준 보안정책을 전달한다. 예를 들면, 회사 보안정책으로 회사 내 일반사원들은 오전과 오후 근무시간에는 페이스북과 같은 SNS(Social Networking Service) 사이트에는 접속하지 못하지만, 점심시간에는 접속하는 것이 허용된다. 하지만 임원들은 SNS 사이트에 언제든지 접속할 수 있다.
2. 보안 제어기는 이러한 고수준 보안정책을 네트워크에 적용할 수 있는 저수준 보안정책으로 번역하여 기능 계층 인터페이스(Capability Layer Interface)를 통해 보안함수(예, Firewall, Web Filter)에게 전달한다.
3. NFV 환경에서 가상머신에서 동작하는 보안함수는 저수준 보안정책을 노스바운드 인터페이스(Northbound Interface)를 통해 스위치 제어기(Switch Controller)에게 전달한다. 일반사원 및 임원들에 따라 선택된 방화벽 정책을 스위치 제어기에게 전달한다.
4. 스위치 제어기는 보안정책을 네트워크에 적용하기 위해 사우스바운드 인터페이스(Southbound Interface)를 통해 각 스위치(Switch)에게 해당 보안정책에 대한 플로우 테이블 엔트리를 셋업한다. 일반사원 및 임원들에 따른 방화벽 정책에 따라 각 사용자들의 단말들의 IP 주소에 따라 네트워크에서 인바운드 트래픽과 아웃바운드 트랙픽에 대한 방화벽을 위한 플로우 테이블 엔트리를 셋업한다. 일반사원은 SNS 사이트로의 향하거나 SNS 사이트로부터 생성된 패킷을 업무시간대에 따라 포워딩을 결정하나 임원들의 경우에는 업무시간에 관계없이 포워딩을 허용한다.
5. 네트워크 내의 클라이언트(Client)들은 트래픽을 발생시킨다. 업무시간에 사원들이 SNS 사이트를 접속하기 위한 패킷을 생성한다.
6. 네트워크 내의 클라이언트들이 발생하는 트래픽은 보안정책에 따라 네트워크의 스위치에 의해 필터되거나 포워딩된다. 업무시간에 발생된 사원들의 SNS와 연관된 패킷들은 드롭(drop)된다.
7. 보안정책에 만족되는 패킷은 네트워크를 통과하나 그렇지 않은 패킷은 네트워크에서 드롭된다.

5.2 SDN 기반 보안서비스 유스케이스

본 절은 중앙집중식 방화벽 시스템과 중앙집중식 DDoS 공격 약화 시스템의 SDN 기반의 두 가지 보안서비스의 유스케이스를 소개한다.

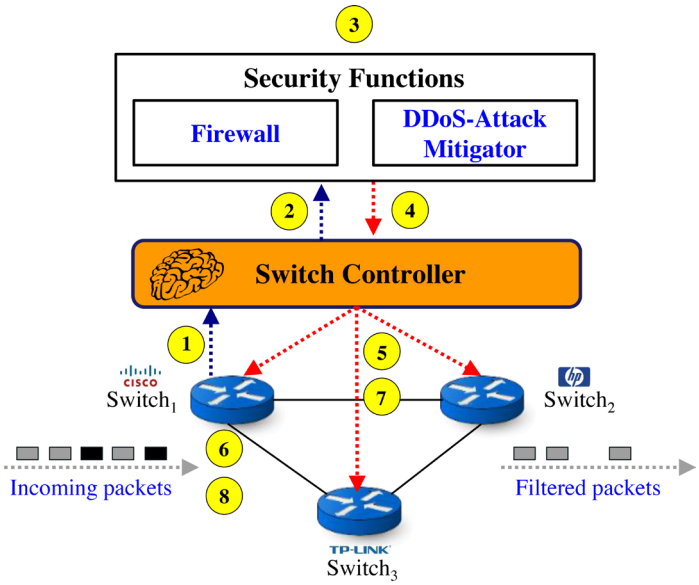

그림8. SDN 기반 보안서비스 유스케이스

5.2.1 중앙집중식 방화벽 시스템

중앙집중식 방화벽 시스템은 SDN 네트워크의 각 네트워크 리소스를 관리하고, 가상머신에서 동작하는 방화벽 보안함수라는 서버를 통해 방화벽 규칙을 동적이면서 유연하게 각 네트워크 리소스에 적용한다. 중앙집중식 방화벽 시스템에서의 방화벽 오퍼레이션은 그림 8에 기술된 다음의 절차로 수행된다.

1. 스위치는 알려지지 않은 플로우에 대한 패킷을 스위치 제어기에게 포워딩한다.
2. 스위치 제어기는 알려지지 않은 플로우에 대한 패킷을 방화벽 보안서비스 응용(즉 보안 함수)에게 포워딩한다.
3. 방화벽은 패킷의 헤드와 페이로드를 분석한다.
4. 방화벽이 그 패킷을 의심되는 패턴을 가지는 맬웨어(Malware) 패킷으로 간주하면 이 패킷의 플로우가 맬웨어라고 스위치 제어기에게 보고하고 단계 5를 수행한다. 그렇지 않으면 그 패킷의 플로우가 정상적인 것으로 스위치 제어기에게 보고하고 단계 7을 수행한다.
5. 스위치 제어기는 해당 플로우를 드롭할 수 있는 새로운 규칙을 스위치의 플로우 테이블에 인스톨한다.
6. 해당 플로우의 패킷이 스위치에 도착하면 스위치는 그 패킷을 드롭한다.
7. 스위치 제어기는 해당 플로우를 포워딩할 수 있는 새로운 규칙을 스위치의 플로우 테이블에 인스톨한다.

8. 해당 플로우의 패킷이 스위치에 도착하면 스위치는 그 패킷을 포워딩한다.

위의 중앙집중식 방화벽 시스템을 위해서는 기존의 SDN 프로토콜들이 방화벽 응용과 스위치 사이의 표준인터페이스들을 통해 사용될 수 있다

5.2.2 중앙집중식 DDoS 공격 약화 시스템

중앙집중식 방화벽 시스템은 SDN 네트워크의 각 네트워크 리소스를 관리하고, 가상머신에서 동작하는 방화벽 보안함수라는 서버를 통해 방화벽 규칙을 동적이면서 유연하게 각 네트워크 리소스에 적용한다. 중앙집중식 방화벽 시스템에서의 방화벽 오퍼레이션은 그림 8에 기술된 다음의 절차로 수행된다.

1. 스위치는 주기적으로 플로우의 인터어라이벌(inter-arrival) 패턴을 스위치 제어기에게 보고한다.
2. 스위치 제어기는 보고 받은 플로우의 인터어라이벌 패턴을 DDOS 공격 약화 보안서비스 응용(즉 보안 함수)에게 포워딩한다.
3. DDoS 공격 약화 응용은 보고된 플로우의 패턴을 분석한다.
4. DDoS 공격 약화 응용이 그 패턴을 DDoS 공격으로 간주하면 이 패킷의 DDoS 공격 의심도에 따른 패킷 드롭 확률을 계산하고 스위치 제어기에게 이 패킷의 플로우가 DDoS 공격에 대한 패킷 드롭 확률을 전달하고 단계 5를 수행한다. 그렇지 않으면 그 패킷의 플로우가 정상적인 것으로 스위치 제어기에게 보고하고 단계 7을 수행한다.
5. 스위치 제어기는 해당 플로우를 드롭 확률로 드롭할 수 있는 새로운 규칙을 스위치의 플로우 테이블에 인스톨한다.
6. 해당 플로우의 패킷이 스위치에 도착하면 스위치는 그 패킷을 드롭 확률에 따라 드롭한다.
7. 스위치 제어기는 해당 플로우를 드롭 확률에 관계없이 포워딩 할 수 있는 새로운 규칙을 스위치의 플로우 테이블에 인스톨한다.
8. 해당 플로우의 패킷이 스위치에 도착하면 스위치는 그 패킷을 포워딩한다.

위의 중앙집중식 DDoS 공격 약화 시스템을 위해서는 기존의 SDN 프로토콜들이 DDoS 공격 약화 응용과 스위치 사이의 표준인터페이스들을 통해 사용될 수 있다.

이상과 같이 I2NSF는 NSF 환경 및 SDN 네트워크에서 보안서비스를 유연성, 일반성, 확장성 및 자동화 관점에서 효과적으로 지원을 할 수 있으므로 차세대 인터넷 보안을 위한 중요한 기술임에 틀림없다.

5. 결론

I2NSF(Interface to Network Security Functions)는 클라우드와 네트워크 가상화 기반의 네트워킹 환경에서 다수의 보안솔루션 벤더들의 보안서비스에게 표준 인터페이스를 제공하고자 한다. 네트워크 기능 가상화(Network Functions Virtualization, NFV)와 소프트웨어 기반의 네트워킹(Software-Defined Networking, SDN)이 인터넷에 도입이 될 전망이므로 I2NSF는 중요한 기술로 부각되고 있다. IETF 94차 I2NSF WG 회의를 통해 NFV환경에서의 보안 서비스를 위한 I2NSF 표준인터페이스 작업이 본격적으로 시작되었다. Ericsson 및 Cisco와 같은 네트워크 벤더들이 I2NSF에 많은 관심을 가지고 있었다.

성균관대와 ETRI는 I2NSF를 이용하는 SDN 기반의 보안서비스 프레임워크 및 유스케이스를 제안하였다. 성균관대와 ETRI 제안한 SDN-based Security Services를 위한 Capability Layer Interface 및 YANG Data Modeling을 구현을 하여 I2NSF 워킹그룹에서 보다 적극적으로 표준화에 참여할 예정이다. 한국통신도 SDN/NFV 기반의 보안서비스에 많은 관심을 가지고 있다. 한국은 초고속 인터넷 인프라를 기반으로 SDN/NFV의 연구 및 구현을 통해 본 I2NSF WG에서 많은 기여를 할 수 있도록 노력해야 할 것이다.

Acknowledgement

본 연구는 2014년도 정부(미래창조과학부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업[2014R1A1A1006438]과 미래창조과학부 및 정보통신기술진흥센터의 정보통신·방송 연구개발 사업 [R0166-15-1041, 중앙 집중제어 기반 네트워크 보안기술 표준개발]의 일환으로 수행하였음.

References

[1] Interface to Network Security Functions (i2nsf), https://datatracker.ietf.org/wg/i2nsf/charter/

[2] ETSI-NFV, “Network Functions Virtualization (NFV); Architectural Framework”, ETSI GS NFV 002 V1.1.1, October 2013.

[3] L. Dunbar et al., “Interface to Network Security Functions (I2NSF) Problem Statement”, draft-dunbar-i2nsf-problem-statement-05, May 2015.

[4] E. Lopez et al., “Framework for Interface to Network Security Functions”, draft-merged-i2nsf-framework-04, October 2015.
[5] A. Pastor et al., “Use Cases and Requirements for an Interface to Network Security Functions”, draft-pastor-i2nsf-merged-use-cases-00, June 2015.
[6] L. Xia et al., “Information Model of Interface to Network Security Functions Capability Interface”, draft-xia-i2nsf-capability-interface-im-04, October 2015.
[7] J. Jeong, H. Kim, and J. Park, “Software-Defined Networking Based Security Services using Interface to Network Security Functions”, draft-jeong-i2nsf-sdn-security-services-03, October 2015.
[8] Simplified Use of Policy Abstractions (supa), http://datatracker.ietf.org/wg/supa/charter/
[9] R. Enns et al., “Network Configuration Protocol (NETCONF)”, RFC 6241, June 2011.
[10] M. Bjorklund, “YANG - A Data Modeling Language for the Network Configuration Protocol (NETCONF)”, RFC 6020, October 2010.

Biography

정 재 훈

- 1999년 : 성균관대학교 정보공학과 학사
- 2001년 : 서울대학교 컴퓨터공학과 석사
- 2009년 : 미네소타대학교 컴퓨터공학과 박사
- 2001년~2004년 : 한국전자통신연구원 표준연구센터 연구원
- 2010년~2012년 : Brocade 소프트웨어 엔지니어
- 주요 관심분야 : 사이버물리시스템, 사물인터넷, 차량네트워크
- e-mail : pauljeong@skku.edu

OSIA
Standards & Technology Review
Journal