정 보 보 호 학 회 지
제24권 제1호, 2014. 2

SDN/OpenFlow의 기술 분석 및 보안 측면의 이용 가능성

김 종 수*, 임 설 화**, 김 학 범***

요 약

최근 네트워크 시장의 큰 화두가 되고있는 SDN(Software-Defined Network)은 OpenFlow를 활용한 차세대 네트워크 기술로 각광받고 있다. 아직까지의 SDN은 초기단계에 이르고 있으나 현재의 네트워크 산업이 가지는 한계점을 근본적으로 변화시킬 수 있는 기술로 상당한 잠재력이 내재되어 있다. 특히 SDN 기술을 보안 측면에서 이용하게 되면, 기존의 IDS/IPS 제품의 대응 범위를 게이트웨이에서 엔드 포인트까지의 인프라 전반으로 확장시킬 수 있다. 또한 유연한 트래픽 경로 재설정을 통한 DoS나 DDoS 공격에도 효과적으로 대비할 수 있다. 이에 따라 OpenFlow 및 SDN의 기술 분석과 보안 측면에서의 이용 가능성에 대해 기술하고자 한다.

Ⅰ. 서 론

2000년대 초반부터 네트워크 기술은 음성, 데이터 등 모든 사용자 서비스를 인터넷망에서 통합 지원할 수 있는 대용량 스위칭 및 하드웨어 기술 위주로 발달해 왔다. 이러한 네트워크 기술 발달은 현재 21세기 정보화 사회의 성공으로 이어졌다.

하지만, 정보화 사회의 성공에서 모바일 기기와 콘텐츠의 폭발적인 증가, 서버 가상화, 클라우드 서비스의 출현 등은 기존의 전통적인 네트워크 아키텍처에 대한 새로운 재고를 불러일으키는 주요한 트렌드가 되고 있다. 현재 대부분의 네트워크는 트리 구조로 배열된 이더넷 스위치 계층으로 만들어진 단계적인 구조로 이루어져 있다. 네트워크 부문에서 이러한 계층적인 디자인은 클라이언트-서버 컴퓨팅이 지배적인 상황에서의 일반적인 디자인이다. 하지만 이러한 고정적인 계층적 네트워크 구조는 오늘날의 대규모 기업용 데이터센터, 통신사업자 환경에서 요구되는 역동적인 컴퓨팅·스토리지 환경에는 적합하지 않다[1].

또한 현재의 네트워크 장비들은 기술적 요구를 충족시키기 위해 오늘날 네트워크의 복잡도는 점점 늘어났고, 이로 인해 정책의 일관성은 결여되었다. 그리고 최근에는 데이터센터에 대한 수요가 급속히 늘어나고 비즈니스 요구 사항에 따라 네트워크에 대한 지속적인 확대가 요구되면서 그 복잡성은 점점 증가하게 되었다. 이 때문에 관리해야 할 포인트가 기하급수적으로 늘어나 네트워크의 규모 확대가 불가능해졌다[1].

또 표준 및 개방형 인터페이스의 부족으로 인해 네트워크를 맞춤화하는 네트워크 사업자의 능력이 제한되고, 이로 인해 통신장비 공급업체에 대한 의존도가 높은 것도 장애 요인 중 하나이다.

이러한 문제점과 한계점을 극복하기 위해서 네트워킹 기술을 개방형 네트워킹 기술로 변화시키자는 OpenFlow라는 새로운 아키텍처가 등장하기 시작하였고, OpenFlow기술을 기반으로 SDN(Software-defined networking)이 빠르게 확장되고 있으며 네트워킹 업체, 클라우드 서비스 제공 업체, 정보통신사업자, 네트워크 전문가 등이 강한 관심과 흥미를 가지고 주목하고 있다[1].

이런 SDN을 이용하면 IDS/IPS의 대응 범위를 게이

* 동국대학교 국제정보 대학원 (tndud4ah@gmail.com)
** 동국대학교 국제정보 대학원 (sulhwa.im@gmail.com)
*** 동국대학교 국제정보 대학원 / (주)이너버스 (khb305@innerbus.com)

트웨이부터 네트워크 전체로 확대하여 대응 범위를 더욱 확장시킬 수 있고, 또한 다양한 네트워크 환경에 대응할 수 있도록 분산성을 강화할 수 있다.

이렇게 SDN의 분산성을 강화하여 게이트웨이뿐만 아니라 엔드 포인트까지 기업의 네트워크 전역에서 malware, spyware 및 봇넷의 위협으로부터 보호할 수 있는 능력을 갖출 수 있다.

그래서 본 논문에서는 현 OpenFlow 및 SDN에 대한 분석과 보안 측면의 이용 가능성에 대해 기술하고자 한다.

Ⅱ. OpenFlow

2.1 OpenFlow

2.1.1 OpenFlow의 등장 배경

OpenFlow의 등장 배경은 다음과 같다.

첫째, 네트워크 기술은 비즈니스, 학교와 가정에서 중요한 인프라의 하나이다. 그러나 연구자나 개발자의 입장에서는 이러한 성공이 네트워크 기술의 혁신을 가로 막는 장애 요소가 되었다. 즉 장비 업체별로 장비를 운영하는 방식이 다르고, 사용자 인터페이스가 다르기 때문에 네트워크 연구자나 사용자가 새로운 네트워크 프로토콜을 개발하여 적용하는 것이 매우 어려웠다. 이러한 문제점을 극복하기 위해서 개방형 인터페이스를 갖는 스위치나 라우터 기술이 연구되었다. 그러나 이러한 개방형 인터페이스를 제공하는 네트워크 기술들은 성능 대비 가격이 비싸기 때문에 상용화에 어려움이 있었다. OpenFlow 기술은 이러한 고비용 문제를 극복하고, 사용자나 개발자에게 개방형 표준 인터페이스를 제공하기 위해 출현하였다[2].

둘째, 기존의 인터넷 장비들은 폐쇄적인 구조를 가지고 있어서 사용자가 자유롭게 설정 및 제어를 하는 데 한계가 있었다. 서비스 업자들은 네트워크 장비 벤더에 의해 제공된 인터넷 환경에서 서비스를 제공해야 했고, 이는 소비자들의 다양한 요구를 충족시킬 수 없었다. 따라서 이러한 제약으로부터 자유로워지기 위해 OpenFlow 기술이 등장하였다[3].

셋째, 현재의 인터넷은 분산 제어 구조를 가지고 있기 때문에 기능적으로 확산되고 복잡해진 환경에서 시장의 새로운 요구에 따라 신속한 변화를 적용하는 데에 걸림돌이 되고 있다. 이러한 구조적인 한계를 극복하고자 서비스 기능 별로 사용 목적에 최적화된 제어 방식을 제공하기 위해 등장하게 되었다[3].

넷째, 현재의 네트워크 장비는 여러 계층의 많은 프로토콜을 각각 지원하여 동작한다. 이는 관리나 운영을 복잡하게 만들고 설정이나 운영에 여러 가지 오류를 발생시키게 된다. 이로 인해 망 운영시간의 감소와 운영비용 상승의 주원인이 되고 있다[3].

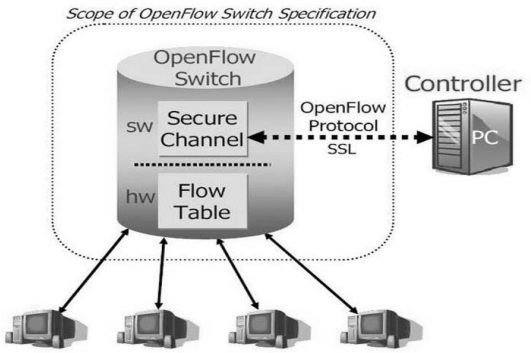
2.1.2 OpenFlow 동작 방식

OpenFlow시스템은 OpenFlow Controller(이하 컨트롤러)와 OpenFlow Switch(이하 스위치)로 구성된다. 컨트롤러와 스위치는 OpenFlow Protocol로 연결되며, 스위치 내부에는 Secure Channel과 Flow Table이 존재한다. Flow Table은 패킷 전달 경로와 동작 방식에 대한 정보를 가지고 있다. Secure Channel은 원격 제어 프로세스인 컨트롤러와 연결을 하고 컨트롤러와 스위치 간에 사용하는 커맨드와 패킷을 보낼 수 있도록 한다. OpenFlow Protocol은 스위치와 컨트롤러에 대한 개방형 프로토콜을 제공한다[4].

패킷이 발생하게 되면 제일 먼저 FlowTable에 해당 패킷의 정보가 존재하는지 확인을 한다. Flow Table에 해당 패킷에 대한 정보가 있으면 그에 맞게 패킷을 처리하고, 정보가 없으면 해당 패킷에 대한 제어 정보를 컨트롤러에게 요청한다. 스위치로부터 제어 정보를 요청받은 컨트롤러는 내부에 존재하는 패킷 제어 정보를 확인하고, 해당 결과를 스위치에 전달한다. 컨트롤러 내의 패킷 제어 정보는 외부에서 API를 통해 입력할 수 있다. 스위치는 컨트롤러에게 전달 받은 제어 정보를 Flow Table에 저장하고, 이후 동일한 패킷이 발생하면 Flow Table에 있는 정보를 활용하여 패킷을 전달한다[5].

OpenFlow는 SDN 아키텍처의 Control layer(제어 계층)와 Forwarding layer(전달 계층) 사이에 정의된 최초의 표준 통신 인터페이스이다.

OpenFlow는 스위치나 라우터 같은 네트워크 장비의 패킷 전달기능 제어를 직접적으로 할 수 있게 해준다. 기존의 네트워크 장비들은 메인프레임 같이 단일화 되어있고, 폐쇄적인 특성을 가지고 있었고, 개방형 인터페



〔그림 1〕 OpenFlow 시스템 구성[4]

이스는 없었다. 즉, OpenFlow와 같은 기능의 표준 프로토콜이 존재하지 않아 전달 기능에 개방형 인터페이스가 없었다[6].

하지만 환경이 변화하면서 네트워크 제어 기능을 네트워크 장비에서 분리해 논리적으로 중앙 집중화된 제어 소프트웨어로 전환하는 데 OpenFlow와 같은 프로토콜이 필요해졌다. OpenFlow프로토콜은 네트워크 장비와 SDN 제어 소프트웨어 사이에 인터페이스로서 양쪽에서 실행된다[6].

OpenFlow는 SDN의 핵심 요소로서 일종의 라우팅 프로토콜과 같은 표준 통신 인터페이스이다. 따라서 OpenFlow는 컨트롤러와 OpenFlow 지원 네트워크 장비 사이에서 커뮤니케이션을 담당한다. 또한 OpenFlow는 사용 패턴이나 애플리케이션, 클라우드 등의 자원에 대한 파라미터를 기반으로 트래픽의 경로나 동작 절차를 정의할 수 있다[7]. 이를 통해 OpenFlow 기반의 SDN 아키텍처는 응용프로그램, 사용자 및 세션 수준의 실시간 변화에 대응해 네트워크를 사용 할 수 있도록 세부적인 제어 기능을 제공한다.

OpenFlow는 서로 다른 스위치나 라우터에 대한 Flow Table 프로그램을 개방형 프로토콜로 제공하기 때문에 네트워크 관리자는 생산부서나 연구부서의 트래픽 흐름을 나눌 수 있게 된다. 연구자들은 경로를 선택하여 패킷 흐름을 통제할 수 있다. 이 방법을 이용하면 새로운 라우팅 프로토콜, 보안 모델, 주소 지정 체계나 IP 선택을 시도할 수 있다[6].

현재 IP 기반의 라우팅은 데이터 흐름이 동일한 경로를 따라야 하기 때문에 애플리케이션 계층과 세션 계층에서의 다양한 요구사항을 반영할 수 있는 컨트롤을 제공하지 못한다. 네트워크 장비인 라우터나 스위치는 하드웨어 기반의 플로우 테이블을 이용하여 네트워크 트래픽을 처리하고 있다. 하지만 OpenFlow 기술은 소프트웨어 컨트롤러를 통해 플로우 테이블을 조작하여 데이터 경로를 설정 할 수 있다[6].

따라서 OpenFlow기반의 SDN 아키텍처는 기존의 인프라와 원활하게 통합할 수 있고, 필요로 하는 네트워크 세그먼트에만 마이그레이션 경로를 제공할 수 있는 정밀한 제어가 가능하다. 이를 통해 네트워크는 실시간 변화에 대응할 수 있게 된다. 이와 같이 OpenFlow 프로토콜은 SDN의 핵심요소 이며, 네트워크 장비의 전달 기능에 직접적인 조작이 가능한 유일한 SDN 프로토콜의 표준이다. OpenFlow 기반 SDN은 기존의 물리 및 가상 네트워크에 사용가능 하고, OpenFlow는 더욱 광범위한 용도로 적용할 수 있다. OpenFlow는 간단한 펌웨어나 소프트웨어 업그레이드를 통해 구현될 수 있다. 또한 네트워크 장비는 전통적인 전달기능과 OpenFlow 기반을 모두 지원할 수 있다. 이 때문에, 다양한 네트워크 장비들이 존재할 지라도 기업이나 통신사업자들이 OpenFlow 기반의 SDN 기술을 쉽게 도입할 수 있다[6].

2.2 ONF

ONF는 Open Networking Foundation의 약자로서 2011년 3월 22일 비영리, 상호 이익을 바탕으로 설립되었다[3]. 이 단체는 개방형 표준 개발을 통해 SDN의 발전과 활용을 촉진하는 것을 목표로 한다.

ONF는 네트워크 사용자가 하드웨어 형태에 얽매이지 않고 자신의 요구 사항에 맞게 네트워크를 제어 및 관리할 수 있는 소프트웨어 정의 네트워킹(SDN) 기술을 촉진시키기 위해 OpenFlow를 SDN의 핵심 요소로 선정했다[8].

ONF의 이사회는 여덟 명의 멤버로 구성되어있다. 여섯 개의 설립 회사가 각각 한 명씩 지정한 여섯 명의 이사와 두 명의 창립자로 구성되었고, 여섯 개의 설립 회사는 대규모 네트워크 운영자 및 사용자 그룹을 대표하는 도이치 텔레콤(Deutsche Telecom), 페이스북(Facebook),구글(Google),마이크로소프트(Microsoft), 버라이즌(Verizon)과 야후(Yahoo)이며, 두 명의 창립자는 UC버클리 대학 교수인 Scott Shenker와 스탠포드 대학 교수인 Nick McKeown 이외에 사무총장으로 Dan Pitt이 ONF의 운영을 총괄 관리하고 있다. ONF에 참가한 기업들은 대부분 신규 서비스를 선보이고 자신

들의 네트워크를 원활하게 운영하기 위한 목적으로 참가했다. 이러한 이유로 ONF는 실제 이용자 기업의 주도 하에 기술표준화를 진행하고 있다. 국내 회원사로는 ETRI, KT, 삼성, SKT가 회원으로 활동하고 있다[3].

III. SDN 소개

3.1 SDN

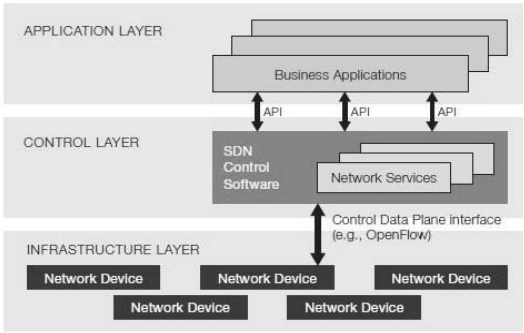
3.1.1 SDN의 정의[9]

소프트웨어 정의 네트워킹(Software Defined Networking: SDN)은 네트워크 제어 기능이 packet forwarding과 분리되어 직접 프로그래밍을 지원하는 기존과 다른 네트워크 아키텍처이다[3]. 과거에는 개별 네트워크 장비는 하드웨어와 제어 기능이 분리되어 있지 않았다. 하지만 SDN에서는 제어 영역이 분리되어 있어 하드웨어에 얽매이지 않고 직접 프로그래밍 할 수 있다. 이렇게 제어 영역을 마이그레이션 함으로써 응용프로그램과 네트워크 서비스를 논리적 또는 가상적인 개체로서 네트워크를 관리 및 제어 할 수 있다.

[그림 2]은 SDN 아키텍처의 구조를 나타내고 있다. 네트워크를 전체적으로 제어하는 소프트웨어 기반의 SDN 컨트롤러에 네트워크의 핵심적인 기능이 집중되어 있다. 따라서 네트워크는 하나의 논리적 스위치와 같은 응용 프로그램으로 나타난다. 기업과 통신사업자는 하나의 논리적인 관점에서 네트워크를 설계 및 운영하게 되고, 이는 네트워크 벤더로부터 독립적인 네트워크 제어를 가능하게 한다, SDN 컨트롤러를 제어하면 네트워크 장비를 단순화 할 수 있기 때문에 수천 가지 이상의 프로토콜 표준을 이해하고 처리할 필요가 없다.

이는 네트워크 관리자가 분산되어 있는 다양한 네트워크 장비에 프로그래밍 방식으로 단순화시켜 네트워크를 설정할 수 있게 해준다. 따라서 네트워크 관리자가 일일이 수동으로 설정을 변경해야 했던 수고를 줄일 수 있다.

또한, SDN 컨트롤러의 중앙 집권화 된 인테리전스를 활용하여 네트워크 문제를 실시간으로 해결할 수 있고, 새로운 애플리케이션이나 네트워크 서비스를 배치할 때도 기존에는 몇 주, 몇 달의 시간이 걸리던 작업을 몇 시간, 며칠로 줄일 수 있다. SDN은 네트워크를 제어계층(Control Layer)에 중앙 집중화함으로써, 네트워크의



〔그림 2〕 SDN 아키텍처 구조[9]

구성 설정, 관리, 보안 등에 있어 관리자에게 유연성을 제공하며, 역동적이고 자동화된 SDN 프로그램을 통해 네트워크 리소스를 최적화할 수 있다. 그리고 기존에 네트워크 장비들이 폐쇄적인 소프트웨어 환경을 가진 반면에, SDN을 이용하면 관리자들이 필요한 프로그램을 스스로 작성하여 사용할 수 있기 때문에 네트워크 장비 벤더에서 기능을 추가해 주기를 기다리지 않아도 된다.

SDN 아키텍처는 사용자가 비즈니스 목표를 달성하기 위한 맞춤형 네트워크 서비스를 구현할 수 있도록 API를 제공한다. 제공되는 API에는 라우팅, 멀티 캐스트, 보안, 액세스 제어, 대역폭 관리, 트래픽 엔지니어링, 프로세서 및 스토리지 최적화, 서비스 품질, 에너지 사용량과 모든 형태의 정책관리를 포함하고 있다. SDN 컨트롤과 애플리케이션 계층 사이에 개방형 API를 사용함으로써 세부 사항에 얽매이지 않고 비즈니스 애플리케이션들을 운영할 수 있다. 따라서 SDN은 애플리케이션을 단순 애플리케이션이 아닌 사용자 정의 애플리케이션으로 인식하고 네트워크를 단순 네트워크가 아닌 네트워크 기능 별로 인식한다. 그 결과, 컴퓨팅, 스토리지 및 네트워크 자원을 최적화 할 수 있다.

3.1.2 SDN/OpenFlow의 도입 장점[10]

기업이나 통신사업자의 경우에는 가격 경쟁력을 높이기 위해 SDN 기술 도입이 불가피하다. OpenFlow 기반 SDN 기술은 높은 대역폭과 동적인 최신 애플리케이션 등에 대응할 수 있다. 또한 끊임없이 변하는 비즈니스 요구 사항을 적용할 수 있게 해주며, 운영 및 관리의 복잡성을 줄여 준다. 기업이나 통신사업자가 OpenFlow 기반 SDN을 도입함에 따라 얻을 수 있는 이점은 다음과 같다[9].

첫째, 멀티 벤더 환경에서 중앙 집중화 된 제어가 가능하다. SDN 제어 소프트웨어는 스위치, 라우터, 가상 스위치 등 모든 벤더의 OpenFlow 기반 네트워크 장비를 제어할 수 있다. 관리자는 각 벤더별 장비를 개별적으로 관리하는 것이 아니라, SDN 기반의 통합 관리가 가능하고, 이 관리 도구를 이용해 전체 네트워크에 걸쳐 신속한 장비 배치, 설정 및 업데이트가 가능하다.

둘째, 자동화를 통해 복잡성이 감소된다. OpenFlow 기반 SDN은 유연한 네트워크 자동화와 관리 프레임워크를 제공해 오늘날 수동으로 작업하는 많은 일들을 자동화한다. 이러한 자동화 도구들은 운용상의 오버헤드를 줄일 수 있고, 작업자의 실수에 의한 네트워크 불안정도 줄여준다. 또한 새롭게 등장한 IT-as-a-Service와 셀프서비스 프로비저닝 모델을 지원한다. 이외에도 SDN으로 클라우드 기반 애플리케이션을 인텔리전스 통합 및 프로비저닝 시스템을 통해 관리할 수 있어 운용상의 오버헤드를 줄여 비즈니스 신속성을 높일 수 있다.

셋째, 기업의 혁신을 가속화한다. SDN의 채택은 네트워크 사업자들이 특정 비즈니스 요구사항이나 특정 사용자 요구 사항을 충족하기 위해 실시간으로 네트워크를 적합하게 프로그램하고 재사용하여 비즈니스 혁신을 가속화한다. SDN과 OpenFlow는 네트워크 인프라를 가상화하고 각각의 네트워크 서비스로부터 추상화하여 신속하게 네트워크 문제를 해결하고, 새로운 서비스 및 새로운 네트워크 기능을 도입할 수 있다.

넷째, 네트워크의 신뢰성과 보안성 향상이다. SDN은 관리자가 OpenFlow를 통해 높은 수준의 설정과 정책을 수립할 수 있게 해준다. OpenFlow 기반 SDN 아키텍처는 엔드포인트, 서비스나 애플리케이션을 추가하고 이동하는 등 정책에 변화가 있을 때, 각각의 네트워크 장비에서 개별적으로 설정해야 할 수고를 덜어준다. 이는 설정이나 정책의 불일치로 인한 네트워크 장애의 가능성을 줄일 수 있다. 왜냐하면 SDN 컨트롤러가 네트워크에 대한 가시성을 제공하고, 이를 제어할 수 있기 때문에 접근 제어, 보안, 트래픽 엔지니어링, 서비스 품질, 정책이 지사나 사내, 데이터 센터를 포함하는 유·무선 네트워크 인프라의 일관성을 유지할 수 있게 보장한다.

특히 기업이나 통신사업자들은 이를 통해 운용비용과 오류를 줄이고, 보다 동적이고 일관성 있는 구성 및 정책 설정이 가능해진다.

다섯째, 좀 더 세분화된 네트워크 제어가 가능하다. OpenFlow 기반 제어 모델은 추상화되고 자동화된 방식으로 관리자가 세션, 사용자, 장비, 애플리케이션 단을 포함한 정책들을 더 세분화하여 정교한 설정을 할 수 있게 도와준다. 이런 제어는 고객들이 같은 인프라를 공유할 때 트래픽 격리, 보안, 탄력적인 자원 관리를 유지하면서 클라우드 사업자에게 멀티테넌시를 지원한다.

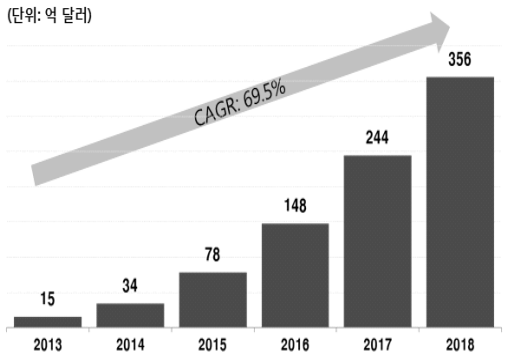
마지막으로 사용자에게 좀 더 나은 경험을 제공한다. 중앙 집중화된 네트워크 제어와 상위 레벨 애플리케이션의 상태 정보를 사용할 수 있도록 함으로써 SDN 인프라는 동적인 사용자의 요구 사항의 더 나은 적용이 가능하다. 예를 들면, OpenFlow 기반의 SDN은 네트워크에서 실시간으로 사용가능한 대역폭을 탐지해서 비디오 애플리케이션에 맞는 비디오 해상도를 자동 조절하여 끊어지지 않는 동영상 서비스를 이용할 수 있다.

3.2 SDN/OpenFlow의 시장 전망

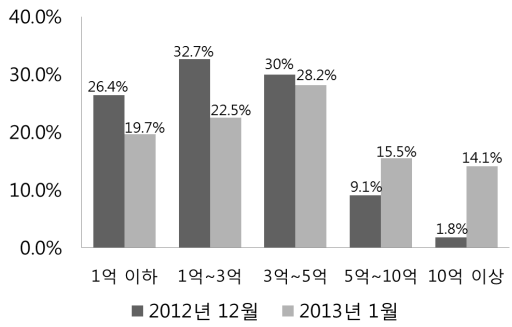
미래 네트워킹의 새로운 아키텍처로 부상하고 있는 SDN은 도입기 단계로서 점차 전세계적으로 투자를 확대하고 있다.

시장조사 기관인 IDC는 2012년 6월에 예측한 전세계 SDN 시장 전망치를 2배 가까이 늘렸다. 첫 보고서에서는 2013년 SDN 시장이 1억6800만딜러. 2016년 20억달러로 예측했으나, 최근에는 2013년 SDN 시장은 3억6000만달러, 2016년 37억달러를 형성할 것으로 내다봤다[11].

이처럼 SDN이 긍정적인 이유는 기존의 통합된 가치



〔그림 3〕 전세계 SDN 시장 규모 전망[12]



〔그림 4〕 한국 SDN 투자계획 규모[14]

사슬이 반도체, 네트워크 장비, 컨트롤러, 애플리케이션, 수요자 등으로 분화되면서 강력한 생태계가 형성되고 있기 때문이다. SDN 기술이 확산 및 표준화를 구축하여 성공할 수 있는 인프라, 보조기술, 보완재 등 필요한 기반이 구축되고 있다. 즉, 수요자가 표준을 주도하고 있으며, 관련 가치사슬의 분화를 통해 구성기술 및 보완재, 인프라 등의 확산으로 성공에 유리한 환경이 조성되고 있다고 볼 수 있다[13].

한국에서도 SDN 도입을 위한 기업·기관의 대단위 투자 움직임이 한층 가시화되고 있다. 오픈플로우코리아가 최근 발표한 '2013년 1월 한국 SDN 시장조사' 보고서에 따르면, SDN 도입을 검토하거나 계획 중인 기업의 비율이 응답자의 78.9%에 달했다. 계획 중인 SDN 투자 규모는 3~5억이 28.2%로 가장 많았고, 1~3억(22.5%), 1억 이하(19.7%), 5~10억(15.5%), 10억 이상(14.1%) 순으로 나타났다. 기업별로 올해 SDN 투자 예산을 확대 편성하고 있다는 것으로 해석할 수 있다. 국내 SDN 시장이 빠른 속도로 움직이고 있다는 것을 알 수 있다[11].

Ⅳ. OpenFlow를 통한 네트워크 보안

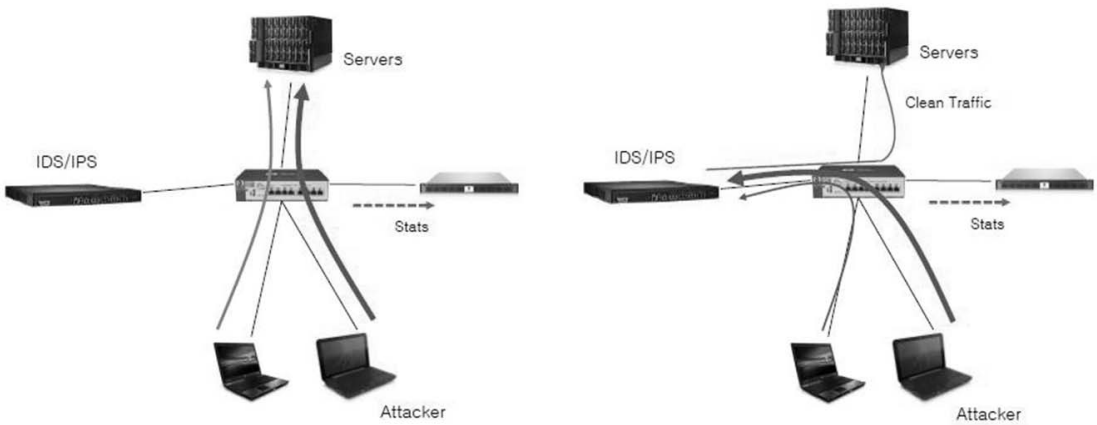
OpenFlow기반 SDN의 장점 중 하나는 네트워크의 안정성 및 보안성에 있다. 즉, OpenFlow를 이용하여 불법 트래픽을 자동으로 감지하고 이에 대한 처리가 가능하다. 또한 악의적 트래픽이 발생 했을 때 IDS /IPS를 반드시 경유하도록 경로를 변경 할 수 있다.

기존의 네트워크 환경에서는 IDS/IPS를 이용해 내부망에서 악의적 트래픽 발생 시 감지하기가 현실적으로 매우 어려웠다. 하지만 OpenFlow 망 내에서는 관리자의 정책에 따라 악의적인 트래픽을 동적으로 IDS/IPS를 경유하도록 경로 변경이 가능하다.

OpenFlow기반 SDN을 이용하여 기대할 수 있는 또 다른 보안 효과는 다음과 같다. DDoS 공격이나 내·외부에서 행해질 수 있는 공격, Malware 탐지를 통한 엔드포인트 보안, 가상화 서버 보안을 위한 네트워크 보안 가상화 등을 통해 OpenFlow 망 내의 위해를 일으킬 수 있는 모든 트래픽에 대한 파악과 처리가 가능하다. 또한 이를 기반으로 네트워크 망의 안정성을 확보할 수 있다.

특히 네트워크 보안 가상화는 기존의 정적인 규칙을 통해 관리되던 가상 방화벽과는 달리 네트워크 보안 정책뿐만 아니라 실시간 세션 상태를 확인해 자동으로 네트워크 패킷을 분산함으로써 병목현상을 해소할 수 있다.

그리고 네트워크를 중앙 집중화하여 관리할 수 있기 때문에 네트워크 전체에 걸친 Access Control이나 보안



〔그림 5〕 OpenFlow를 통한 네트워크보안 구성 전과 구성 후[15]

정책 관리를 자동화하여 관리자가 좀 더 편리하게 보안 관리를 할 수 있도록 도와준다.

최근에는 이러한 OpenFlow 기술을 기반으로 하는 상용 Controller를 가지고 있는 벤더들이 보안 시장으로 진입을 하고 있다.

4.1 DDoS 보안

SDN 기술을 이용한 보안 제품은 네트워크 전반에 걸친 공격 차단 서비스와 DoS 및 DDoS 방어가 가능하다. SDN 제어장치의 Northbound API를 이용해 기본적인 DDoS 방어 서비스를 프로그래밍할 수 있다.

SDN 제어 플레인을 활용하여 데이터 플레인을 수집하고 제어함으로써 DDoS 방어를 장비 기반에서 네트워크의 전반적인 서비스로 옮겨와 매우 낮은 비용으로 네트워크 증가 값을 지능적으로 추출해 실시간으로 네트워크 공격을 탐지할 수 있다.

이렇게 SDN 기술의 프로그래밍을 사용하여 DoS와 DDoS 네트워크 플러딩 공격을 적극적으로 방어할 수 있다.

또한 OpenFlow에 기초하는 네트워크 전반에 걸친 통계 자료를 수집하여 기업 인프라의 과거 데이터들과 종합하여 임계치를 설정하여 자동으로 공격에 대응할 수 있도록 마이그레이션을 할 수 있다. 이렇게 정상 트래픽 기준을 설정하게 되면 DDoS 공격으로 판단되어지는 비정상 트래픽을 식별하기 위해 통계 자료를 이용할 수 있다. 전통적인 DDoS 공격 방어 솔루션이 순수한 속도 기반이었다면, SDN 기술을 이용하여 속도 기반 파라메터와 속도와 관계없는 파라메터 둘 사이의 상관관계를 통해 공격의 정도를 결정 할 수 있다.

〔표 1〕 공격의 정도를 결정하기 위한 벡터 종류[16]

구분	벡터명
속도 기반의 행위 파라메터	패킷 속도(PPS)
	대역폭(Mbps)
	연결 속도(CPS)
속도와 관계없는 행위 파라메터	프로토콜 실패
	평균 패킷 크기 분포
	연결 분포
기타	네트워크 안에 있는 보호 자원에 대한 공격 시도로 의심되는 써드 파티의 알림과 로그

마지막으로 공격이 탐지되면, 의심스러운 트래픽을 우회할 수 있도록 네트워크를 프로그래밍하면 된다. 이때, Northbound API를 이용해 공격으로부터 개체를 보호하기 위해 트래픽 경로를 재설정할 수 있다.

4.2 악성코드 보안

네트워크상의 유저가 Web 사이트에 액세스 하려고 하면 DNS 요청이 생성된다. 생성된 요청과 보유하고 있는 malware 배포원 리스트와 일치했을 경우, OpenFlow 프로토콜을 이용하여 네트워크 전체에 걸쳐 대응 방법을 마련한다. 세부적으로는 malware 배포원의 요청을 리디렉션 할 수 있는 것 외에 유저에게 경고 송신 등의 조치도 할 수 있다.

예를 들어 기업의 사용자가 이메일에 포함된 링크를 클릭했을 경우 다음과 같은 동작이 실행된다[17].

① 사용자의 DNS 쿼리가 로컬에 존재하는 OpenFlow 기반의 액세스 스위치로 전송된다.
② OpenFlow 정책에 따라, SDN 컨트롤러에 해당 트래픽을 전달한다.
③ SDN 컨트롤러가 쿼리를 수신하면, malware 배포원 DB의 호스트네임과 일치하는 지 확인한다.
④ 해당 사이트가 합법적이라고 판단하면 쿼리는 제어 계층의 스위치를 통해 전달된다. 반면, 해당 사이트가 문제가 있다고 판단되거나 위협을 감지하면, 클라이언트에게 해당 패킷을 돌려보내고 로그 관리 시스템에 로그를 남기는 등의 조치를 취해 사용자가 위협에 접근하는 것을 방지한다.

이러한 동작은 Web 트래픽 전체가 아닌 DNS 트래픽만을 캡처하고, 처리하기 때문에 높은 효율성을 갖는다.

4.3 가상화 보안

SDN 기술을 이용하면 자동화된 워크로드 프로비져닝의 광범위한 채택과 데이터 센터의 가상화 확산으로 인해 야기되는 특수한 문제점과 기회에 맞게 설계된 새로운 형태의 네트워크 보안 솔루션을 제공할 수 있다.

가상화는 초기에는 서버 통합과 같은 주로 전략적인 이익을 위해 배치되었으나 현재의 가상화는 IT가 비즈니스에 더욱 적합하고 즉각적인 반응을 위한 동적 할당

과 워크로드 프로비전을 위한 기술의 사용이 점차 증가하고 있다.

이처럼 가상화는 현재 컴퓨팅을 위한 주류이다. 소프트웨어 정의 저장장치(Software-Defined Storage, SDS)와 소프트웨어 정의 네트워킹(Software-Defined Networking, SDN)을 통해 스토리지와 네트워킹의 가상화가 가능하다. 또한 소프트웨어 정의 보안(Software-Defined Security, SDSec)이라는 새로운 종류의 솔루션을 개척하여, 가상화를 네트워크 보안 영역으로 확장시키고 있다[18].

SDN은 Forwarding plane으로부터 Network Control plane을 추출한다. 즉, Security Control plane 또한 분리가 가능하다는 것이다. 그 결과 어떠한 환경에서도 단일 시스템처럼 동작하고, 가상 머신처럼 밀접하게 결합할 수 있는 동적인 분산시스템이 된다.

따라서 SDN을 이용하면 동적이고 민첩한 가상 환경에 적용되어 기존 보안 솔루션과 호스트 기반의 가상 보안 솔루션이 가지고 있는 프로비저닝, 토폴로지, 성능 및 병목 현상을 해결한다.

이는 Standalone으로 동작하는 소프트웨어인 가상 방화벽과는 매우 다른 형태로 동작할 수 있다. 가상방화벽은 다양한 보안 기능을 가지고 동작하지만, 기존의 방화벽처럼 정적인 규칙에 따라서 제어되고 관리된다.

반면에 SDN을 이용하면 네트워크 보안 정책뿐만 아니라 실시간 세션 상태까지도 Control 플레인에서 파악하여 자동적으로 분산처리가 가능하다. 그 결과로 컴퓨터와 네트워크 가상화를 통한 데이터 센터 가상화를 방해했던 병목 현상을 제거한다. 또한 가상화와 소프트웨어 정의 프로비저닝의 제공으로 데이터 센터 설계자와 운영자에게 더욱 유연해지고 효과적인 아키텍처를 제공한다.

하지만 기존 보안의 성능과 위상적 제한은 물리적 인프라와 가상 영역에서 같은 상황이다. 즉, 가상화는 많은 네트워크의 설계 규칙을 바꿨지만, 네트워크 기반 보안의 필요성을 제거하지는 못했다. 가상화가 변화시킨 것은 언제, 어디서나 위치에 독립적인 네트워크 레벨의 보안 정책 필요성이다. 이는 근본적인 새로운 요구 사항이고, SDN이 해결책이 될 수 있다.

Ⅴ. 결 론

기존 네트워크의 한계점에 대응하는 네트워킹 기술로 부상하고 있는 SDN은 인터넷 인프라 패러다임의 전환 시작이며, 이는 네트워크 보안 영역에서도 큰 영향력을 미칠 것이다. 가상화 기술이 각광을 받으면서, 서버 가상화 뿐만이 아닌 네트워크 가상화도 고려해야한다. 네트워크가 가상화가 되면 기존의 네트워크 기반 보안 제품들의 가상화도 필요하게 될 것이며, 가상화를 통한 운영 비용 절감은 기업에게 있어 큰 이점으로 작용할 것이다.

또한 SDN을 도입하면 하드웨어와 별개로 자유롭게 네트워크의 운영·관리를 간소화하고 최적의 데이터 흐름을 설계·지원하여 대역폭의 효율적 사용과 DDoS 등의 공격 또한 효율적으로 방어 할 수 있다. 이를 통해 망 제어 및 보안 관리가 유연해지고, 스케일 확장과 신규 서비스 도입 시간 단축 등이 가능해 질 것이며, 네트워크 운영비용 절감이 가능해질 것으로 기대 된다.

하지만, 문제점도 존재한다. 컴퓨팅 분야에서의 소프트웨어 취약성이 네트워크 분야에서도 발생할 가능성이 높으므로 문제 해결을 위한 다양한 소프트웨어 경쟁력 강화가 필요하다. OpenFlow 규격의 지속적 확장 지원과 플로우 인지 및 처리에 대한 확장성 및 Controller의 확장성, 보안 문제, 망 관리 체계와의 조율, 서버 가상화의 통합적 지원 등을 비롯한 다양한 이슈들에 대해 많은 연구가 필요하다.

비록 SDN 기술이 초기 도입 과정에 있으나, 기존 네트워크 산업의 아키텍처를 근본적으로 변화 또는 혁신시킬 수 있는 기술로 평가받고 있다. 따라서 네트워크 분야에서 경쟁력을 강화할 수 있는 기회로 SDN을 활용하여 미래를 대비해야하는 당위성이 존재하며 마찬가지로 네트워크 보안 분야에서도 SDN을 이용한 보안 솔루션 개발로 미래를 대비해야 할 것이다.

약어정리

API	Application Programming Interface
CPS	Connection Per Second
DDoS	Distributed Denial of Service
DNS	Domain Name System
DoS	Denial of Service

IDS	Intrusion Detection System
IPS	Intrusion Prevention System
Mbps	Megabits Per Second
ONF	Open Networking Foundation
PPS	Packet Per Second
SDN	Software-Defined Network
SDS	Software-Defined Storage
WAN	Wide Area Network

참고문헌

[1] “Software-Defined Networking: The New Norm for Networks”, ONF White Paper, pp.3-6, Apr.2012.

[2] 윤빈영, 이범철, “미래 네트워킹 기술 SDN”, 전자통신동향분석 제27권 제2호, Apr.2012

[3] 임용재, 백선경, 김동철, 연승준, “네트워크의 패러다임 전환:OpenFlow”, PM Issue Report 2012-제1권 이슈1, Jul.2012

[4] Nick McKeown, Tom Anderson, Hari Balakrishnan, Guru Parulkar, Larry Peterson, Jennifer Rexford, Scott Shenker, Jonathan Turner, “OpenFlow: Enabling Innovation in Campus Networks”, Mar.2008.

[5] “OpenFlow Switch Specication Version 1.0.0(Wire Ptorocol 0x01)”, ONF, Dec.2009.

[6] “Software-Defined Networking: The New Norm for Networks”, ONF White Paper, pp.8-16, Apr.2012.

[7] 김민식·임순옥 “차세대 네트워크 제어·관리 기술인 SDN 등장과 전망(Ⅰ)” 방송통신정책 제24권 12호 통권 534호, pp.13-14, Jul.2012.

[8] https://www.opennetworking.org/, 2013. 10

[9] “Software-Defined Networking: The New Norm for Networks”, ONF White Paper, pp.2, pp.7-8, Apr.2012.

[10] “Software-Defined Networking: The New Norm for Networks”, ONF White Paper, pp.10-12, Apr.2012.

[11] 이유지, “‘SDN’ 대단위 투자 움직임 가시화”, 디지털데일리, Feb.2013.

[12] “2013년, SDN 시장 본격화 원년”, 해외 ICT R&D 정책동향(2013년 05호), pp44, 2013

[13] 김민식, 임순옥, “SDN, 새로운 별로 떠오르다”, KTOA 한국통신사업자연합회 2012 AUTUMN_vol.62, 2012

[14] http://www.openflow.or.kr, 2013.10

[15] 김숙향, “SDN use case” 발표자료, Oct.2012.

[16] RADWARE, “DefenseFlow: The SDN Application that Programs Networks for DoS Security”, radware solution brief

[17] HP, “Realizing the power of SDN with HP Virtual Application Networks“, HP Technical white paper

[18] http://www.varmour.com/technology.html, 2013.11

〈저 자 소 개〉

김 종 수 (Jong-Soo Kim)
학생회원

2011년 2월 : 대구대학교 전산학과 졸업
2013년 3월~현재 : 동국대학교 정보보호학과 석사과정
<관심분야> 네트워크 프로그래밍, 침투테스트, 네트워크보안

임 설 화 (Sul-Hwa Im)
학생회원

2013년 3월~현재 : 동국대학교 정보보호학과 석사과정
<관심분야> 모바일 보안, 보안 컨설팅, 클라우드 컴퓨팅 보안, 네트워크 보안

김 학 범 (Hak-Beom KIM)
정회원

1990년 8월 : 중앙대학교 대학원 전자계산학과 졸업(공학석사)
2001년 2월 : 아주대학교 대학원 컴퓨터공학과 졸업(공학박사)
1991년 10월~1996년 6월 : 한국전산원 주임연구원
1996년 7월~2001년 8월 : 한국정보보호진흥원(KISA) 기술표준팀장
2001년 9월~2003년 1월 : (주)드림시큐리티 상무이사
2003년 2월~2005년 3월 : (주)장미디어인터렉티브 상무이사
2008년 4월~2009년 6월 : 인포섹(주) 수석컨설턴트
2009년 7월~2010년 12월 : 에스지에이(주) 연구소장
2011년 9월~2013년 3월 : (주)지엔에스인증원 ISMS본부장
2001년 3월~2009년 2월 : 순천향대학교 정보보호학과 겸임교수
2005년 9월~현재 : 동국대학교 국제정보대학원 겸임교수
2011년 7월~현재 : 한국정보보호학회 이사
2013년 4월~현재 : ㈜이너버스 연구소장
<관심분야> 통합로그 시스템, 빅데이터 보안, 클라우드 컴퓨팅 보안, 개인정보보호, PIMS