소프트웨어 정의 네트워킹과 네트워크 기능 가상화를 이용한 클라우드 네트워크에서의 보안 서비스 제공 방법론에 대한 연구

김진우, 신승원
한국과학기술원 전산학부 정보보호대학원
e-mail : {jinwoookim, kangheedo, claude}@kaist.ac.kr

A study on method to provide security services to Cloud Network with Software Defined Networking and Network Function Virtualization

Jinwoo Kim, Seungwon Shin
Graduate School of Information Security
School of Computing, KAIST

요 약

현재 클라우드 네트워크는 복잡성 및 거대한 규모로 인해 기존 네트워크와는 차별화된 양상을 보이고 있다. 하드웨어 기반 보안 장비로만 보안 서비스를 제공하기에는 한정적 자원을 고려하였을 때 한계가 있으며, 온 디맨드 서비스와 멀티 테넌시로 인한 동적인 네트워크 환경은 관리자가 외부의 보안 위협뿐만 아니라 내부의 위협도 고려해야하도록 만든다. 본 논문에서는 SDN 과 NFV 를 이용하여 언급한 문제점들을 해결하고, 효과적인 보안 서비스를 제공할 수 있는 방법론을 제시하도록 한다.

1. 서론

오늘날 클라우드 네트워크는 그 규모가 매우 거대하고 복잡하며, 시시각각 변하는 동적인 환경을 이루고 있다. 클라우드 네트워크의 내부에는 수많은 물리 서버 및 가상 머신이 있으며, 각각 서로 다른 네트워크 환경 설정을 가지고 있다. 물리 서버와 가상 머신은 동적으로 추가되거나 제거될 수 있으며, 환경 설정 역시 또한 동적으로 변할 수 있다. 이러한 복잡한 네트워크 환경에서의 보안성을 보장하기 위해서, 네트워크 관리자는 방화벽(Firewall) 이나 침입 탐지 시스템(Intrusion Detection System, IDS) 같은 하드웨어 보안 장비를 설치해야만 한다. 그러나 한정적인 자원을 고려할 때, 거대한 네트워크 환경에서 모든 엔드 호스트(End Host) 지점에 이를 적용하는 것은 쉽지 않다.

소프트웨어 정의 네트워킹(Software-Defined Networking, SDN) [2] 은 네트워크 분야에서 혁신적인 기술, 나아가 하나의 트렌드로써 각광받고 있다. SDN 은 기존 네트워크의 제어 평면(Control Plane)과 데이터 평면(Data Plane)을 분리함으로써, 프로그래머블(Programmable)한 환경을 네트워크 관리자에게 제공한다. 네트워크 관리자는 SDN 컨트롤러 상에서 기존의 하드웨어 보안장비를 네트워크 애플리케이션으로 구현함으로써, 사용자에게 비즈니스 서비스를 보다 편리하고 유연하게 적용할 수 있다. 이러한 장점 때문에 엔터프라이즈 네트워크의 관리자들도 SDN 을 적극 도입하고 있는 상황이다[3].

네트워크 기능 가상화 (Network Function Virtualization, NFV) [9] 역시 차세대 네트워킹 기술로써 주목받고 있다. 현재 보안장비들은 대부분 전용 하드웨어 장비, 즉 미들 박스에 귀속되어 있다. 이러한 미들박스를 가상화 하여 범용 일반 서버에 필요한 네트워크 기능을 온 디맨드 방식으로 제공하는 것이 NFV 의 개념이다.

본 논문에서는 SDN 및 NFV 를 활용하여 클라우드 네트워크 환경에서 효과적인 보안 서비스 제공을 위한 방법론을 제시한다. 또한 수집 및 분석 되어야할 네트워크 특징(Feature) 들을 제시하고 가능한 유즈케이스 시나리오에 대해 알아보도록 한다.

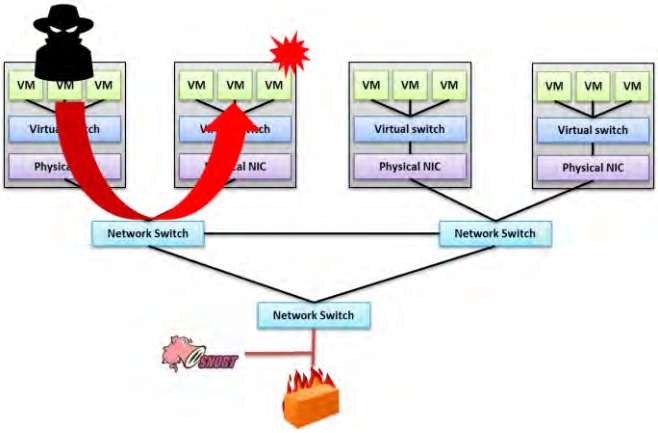
2. 본론

본 절에서는 현재 클라우드 네트워크의 특징을 살펴보고, 보안 서비스 제공의 어려운 점에 대해 알아본다. 이어서 이를 해결하기 위해 SDN 및 NFV 를 이용한 방법론을 제시하고, 동작 시나리오에 대해서 알아보도록 한다.

2.1 문제 정의

클라우드 네트워크는 다음과 같은 특징을 가지고 있다. 첫째, 수많은 물리 서버와 가상 머신으로 이루어져있다. 2012 년 까지 아마존 웹 서비스(Amazon Web Service, AWS)의 물리 서버는 약 45 만개로 추산되며, 물리 서버당 10 개의 가상머신을 가진다고 가정하면 약 450 만개의 가상 머신이 존재한다고 예측된다[1]. 수 많은 물리 서버와 가상 머신에 보안 서비스를 제공하기위해 보안 장비를 모든 지점에 설치하는 것은 사실상 불가능하다. 둘째, 네트워크 설정과 정책이 매우 다양하고 복잡하다. 클라우드 네트워크는 멀티 테넌시(Multi-Tenancy)를 지향하기 때문에 하나의 물리 서버를 여러 테넌트(Tenant)들이 가상 머신 들을 사용하는 경우가 많다. 따라서 네트워크 설정과 정책이 테넌트 마다 제 각각이다. 셋째, 내부 서버와 가상 머신이 유동적이다. 클라우드 네트워크는 사용자의 요구에 따라 온-디맨드(On-Demand) 식의 서비스를 제공한다. 따라서 기존 네트워크처럼 노드들이 정적이지 않기 때문에 일관된 보안 서비스를 적용하기 어렵다.

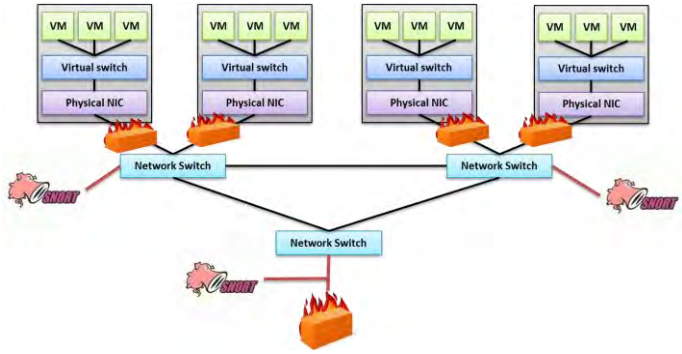
이러한 특성들 때문에 그림 1 과 같이 보안장비를 데이터 센터의 코어 스위치에만 설치하게 된다면, 내부 가상 머신이 공격자에 의해 탈취되었을 때, 다른 가상 머신으로 향하는 악성 트래픽을 감지하기 어렵게 된다.



(그림 1) 내부 트래픽 감시의 어려움

이를 해결하기 위해서는 그림 2 와 같이 모든 물리 서버 지점에 보안 장비를 설치해야 한다. 그러나 모든 엔드 포인트 지점에 하드웨어 보안 장비를 설치하는 것은 엄청난 비용을 감안해야 하며, 거대한 클라우드 네트워크의 규모를 고려했을 때 이는 거의 불가능하다.

이상의 문제 정의를 통하여 현재 클라우드 네트워크 환경에서 보안성을 보장하기 위해 다음과 같은 과제를 해결해야 한다. 첫째, 한정적인 보안 장비 자원을 어떻게 관리할 것인가? 둘째, 동적인 네트워크 환경에서 어떻게 보안 서비스를 효과적으로 제공할 것인가? 셋째, 내부 또는 외부 위협으로부터 클라우드 네트워크를 어떻게 보호할 것인가?



(그림 2) 한정된 보안 장비

2.2 방법론

본 논문에서는 위에서 제시한 과제를 해결하기 위해 다음과 같은 접근 방법을 제시한다. ① SDN 컨트롤러에서 수집한 네트워크 정보들을 기반으로 의심스러운 호스트를 파악한다. ② NFV 를 이용하여 온 디맨드 보안 서비스를 제공한다.

SDN 의 가장 큰 강점은 중앙 집중형 제어 평면(Centralized Control Plane) 에서 데이터 평면의 모든 네트워크 정보들을 수집할 수 있다는 점이다. 따라서 우리는 이러한 네트워크 정보들을 바탕으로 네트워크/물리 호스트/가상 머신의 건강도(Healthiness)를 정의한다. 건강도를 결정짓는 네트워크의 특징(Feature)들은 표 1 과 같이 크게 호스트의 평판 기반 (Reputation Based), 행위 기반 (Behavior Based) 으로 나누어 진다. 이러한 특징들에 대해서 산술적인 점수 (Score)를 매겨서 이상 징후를 보이는 호스트를 판별한다.

평판 기반 방식은 EFFORT[5]에서의 프로세서 평판 분석 모듈 (Process Reputation Analysis Module)이 프로세스의 평판을 프로세스의 시그니쳐가 블랙리스트나 후이스, 검색 엔진에서 조회되는 지에 따라 점수를 책정하여 악성 호스트인지 아닌 지를 판별하는 것에 기반한다. 행위 기반 방식에서의 TCP 연결 성공/실패 비율은 3 Way Handshaking 이 성립 시 TCP 연결 성공, 그 외에는 실패로 가정하여 비율을 산출한다. 호스트가 SYN 플러딩 공격(SYN Flooding Attack)을 할 때, 이러한 비율이 낮아지므로 의심이 가는 호스트(Suspicious Host) 라고 할 수 있다. DNS 요청/응답 쌍 비율은 DNS 의 요청과 응답 트래픽을 모니터링 하여 비율을 산출하며, 비율이 높아질수록 DNS 요청에 비해 응답이 많은 것이므로 DNS 증폭 공격 (DNS Amplification Attack)을 수행하는 호스트일 확률이 높다[6]. 초당 바이트 수(Bytes Per Second)와 초당 패킷 수(Packets Per Second)는 먼저 SDN 컨트롤러가 오픈플로(OpenFlow) 스위치[8]에 설치된 플로 룰에 대해서 플로 통계 (Flow Statistics) 메시지를 주기적으로 요청을 보내, 스위치로부터 누적된 바이트 카운트 (Byte Count) 및 패킷 카운트 (Packet Count)를 알아낸 후에 경과 시간으로 나눔으로써 계산할 수 있다.

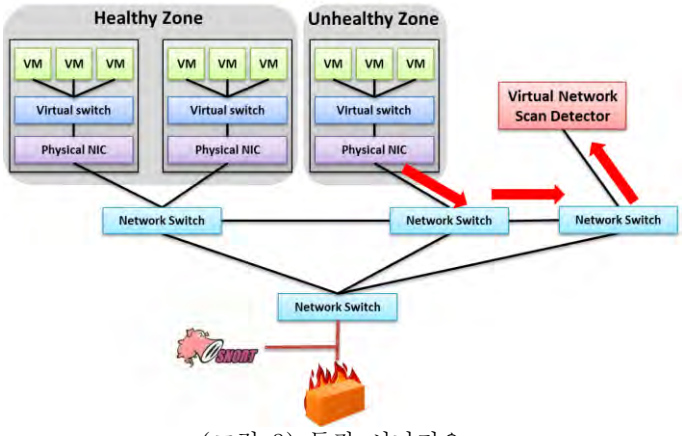
분 류	특 징	설 명
평판 기반 (Reputation Based) [5]	블랙리스트 (Blacklist)	호스트 또는 호스트가 접촉하려는 대상이 블랙리스트(예: SpamHaus[7])에 있는지 여부
	후이스 (Whois)	호스트 또는 호스트가 접촉하려는 대상이 후이스에 등록되어있는 지 여부
	검색엔진 (Search Engine)	호스트 또는 호스트가 접촉하려는 대상이 검색엔진에서 결과로 나오는 지 여부
행위 기반 (Behavior Based)	TCP 연결 성공/실패 비율 (TCP Connection Success/Failure Rate)	호스트의 TCP 연결 성공/실패 비율, 3 Way-Handshaking 이 성립하면 TCP 성공 그 외에는 실패로 간주
	DNS 요청/응답 쌍 비율 (DNS Request/Reply Pair Rate) [6]	호스트의 DNS 요청/응답 쌍 비율
	초당 바이트 수 (Bytes Per Second)	해당 호스트를 출발지로 하는 플로우의 초당 바이트 수
	초당 패킷 수 (Packets Per Second)	해당 호스트를 출발지로 하는 플로우의 호스트의 초당 패킷 수

<표 1> 건강도 (Healthiness) 측정을 위한 네트워크 특징

이렇게 측정된 건강도를 기준으로 네트워크/호스트/가상 머신에 따라 지역(Zone)을 정의하고 이는 후술할 시나리오에서 트래픽 리다이렉션(Traffic Redirection)의 판별 기준이 된다. 이 후 건강도가 낮은 지역 근처에 보안 지점 (Security Point)을 지정하고 이 곳에 NFV 를 이용하여 보안 서비스 애플리케이션을 배치(Deployment) 하도록 한다.

2.3 유즈케이스 시나리오

그림 3 은 측정된 건강도를 기준으로 건강 지역 (Healthy Zone), 건강하지 못한 지역 (Unhealthy Zone) 으로 나눈 모습이다. 건강하지 못한 지역 근처에 가까운 스위치(노드 홉 수 기준) 를 선정하여 해당 스위치에 연결되어있는 호스트에 NFV 를 이용하여 가상 네트워크 스캔 감지기 (Virtual Network Scan Detector)를 배치한다. 이후 건강하지 못한 지역에서 나오는 트래픽은 네트워크 스캔 감지기를 거치도록 플로 룰을 스위치에 추가해 놓도록 한다.



(그림 3) 동작 시나리오

3. 결론

클라우드 네트워크의 규모가 점점 커짐에 따라 보안 이슈는 계속해서 생겨날 전망이다. 기존 네트워크와는 비교할 수 없는 규모를 고려하면, 하드웨어 기반의 보안 장비로는 한정적인 리소스로 인해 선택적인 지점에 이를 설치 할 수 밖에 없고 이는 곧 보안 위협에 대해 충분히 대비하지 못하는 결과를 야기할 수 있을 것이다. 따라서 본 논문에서는 차세대 네트워킹 기술로써 평가받는 SDN 및 NFV 를 이용하여 소프트웨어 기반의 유연하고 효율적인 보안 서비스를 제공 하는 방법론을 제시하였다. SDN 의 중앙 집중형 제어 평면을 이용하여 데이터 평면의 네트워크 트래픽 정보를 수집한 뒤, 이를 기반으로 지역을 나누었다. 이 후 건강 하지 못한 지역 근처에 NFV 를 이용하여 가상 보안 애플리케이션을 배치하고, 플로룰을 설치하여 해당 지역에서 나오는 트래픽을 해당 NFV 노드로 우회시키도록 하였다.

참고문헌

[1] Estimate: Amazon Cloud Backed by 450,000 Servers, http://www.datacenterknowledge.com/archives/2012/03/14/estimate-amazon-cloud-backed-by-450000-servers/
[2] Casado, Martin, et al. "Ethane: taking control of the enterprise." ACM SIGCOMM Computer Communication Review. Vol. 37. No. 4. ACM, 2007.
[3] S. Jain et al, “B4: Experience with a globally-deployed software defined WAN,” in Proc. ACM SIGCOMM 2013, pp. 3-14, Hong Kong, China, Aug. 2013.
[4] Shin, Seungwon, and Guofei Gu. "CloudWatcher: Network security monitoring using OpenFlow in dynamic cloud networks (or: How to provide security monitoring as a service in clouds?)." Network Protocols (ICNP), 2012 20th IEEE International Conference on. IEEE, 2012.
[5] Shin, Seungwon, Zhaoyan Xu, and Guofei Gu. "EFFORT: A new host–network cooperated framework for efficient and effective bot malware detection."Computer Networks 57.13 (2013): 2628-2642.
[6] Kambourakis, Georgios, et al. "Detecting DNS amplification attacks." Critical information infrastructures security. Springer Berlin Heidelberg, 2007. 185-196.
[7] Spamhaus, The Spamhaus Project, https://www.spamhaus.org/
[8] OpenFlow 1.3 Specification, https://www.opennetworking.org/images/stories/downloads/sdn-resources/onf-specifications/openflow/openflow-spec-v1.3.0.pdf
[9] Network functions virtualisation – introductory white paper, http://portal.etsi.org/NFV/NFV_White_Paper.pdf.