Virtual Switch 환경에서 트래픽 감시 방안 연구

홍민희, 김다미, 박철근, 김성기
선문대학교 정보통신공학과

e-mail: { minixhom, kdm2715, ckpark, skkim }@sunmoon.ac.kr

A Study on Traffic Monitoring Method in Virtual Switch

Min-Hee Hong, Da-Mi Kim, Cheul-Geun Park, Sung-Ki Kim
Dept. of Information and Communication Engineering, Sun Moon University

요 약

본 논문에서는 네트워크 가상화 장비인 Virtual Switch을 이용하여 트래픽을 모니터링하는 방안을 연구한다. Virtual Switch 환경에서는 일반적인 트래픽 모니터링 방법을 적용하기에는 제약이 있어, 제약을 극복하고 트래픽을 모니터링 하기 위한 방안이 필요하다. 본 연구에서는 트래픽 측정용 VM을 이용하여 Virtual Switch 환경의 트래픽을 모니터링하는 방법을 제안한다.

1. 서론

네트워크는 여러 네트워크 장비를 조합하여 통신이 가능하도록 구축되었다. 일반적으로 네트워크 구성은 시스템이 추가되거나 변경될 때마다 장비도 추가·변경하는 비용이 발생한다. 최근에는 네트워크 가상화 기술 사용해서 네트워크 구성이 확대되고 있다[1,2]. 가상화를 적용한 장비에는 하나의 네트워크 자원을 논리적으로 분할하여 여러 개의 네트워크 자원으로 사용하는 방법과 여러 개의 네트워크 자원을 논리적으로 통합하여 하나의 네트워크 자원처럼 사용하는 기술이 있다.

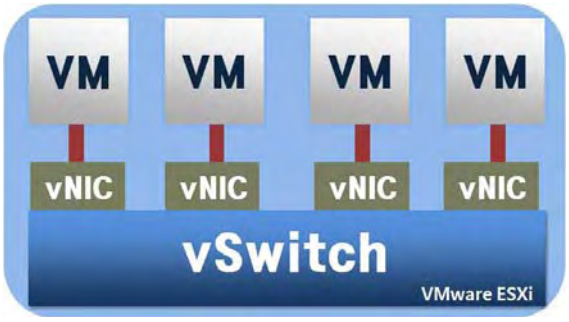
네트워크 장비 분할 기술에 사용하는 장비는 Switch 다. 물리적 Switch는 보안을 위해 트래픽을 모니터링해서 패킷을 감시하고 침입자를 탐지하지만 VMware에서 제공하는 vSwitch는 보안 정책 상 기존의 방법을 적용하는데 제약이 있다[3].

본 논문에서는 이러한 문제를 해결하기 위하여 가상화 VM 자원을 트래픽 데이터를 수집할 수 있도록 구성하는 방법 제안한다. 본 논문에서는 VMware ESXi 환경에서 VM 자원을 연동시켜 통신 VM(Virtual Machine)에 통신 트래픽 데이터를 수집하고 Netflow 도구[4]를 이용하여 트래픽 활동을 분석하는 방법을 제안한다.

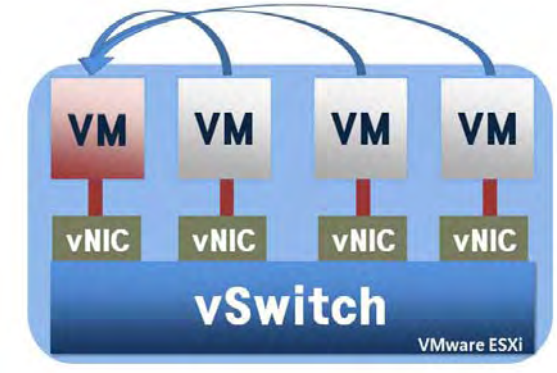
2. 시스템 구조

(그림 1)은 일반적인 Virtual Switch 환경의 시스템 구조이고, (그림 2)는 제안하는 Virtual Switch 환경의 시스템 구조이다

(그림 2)는 VMware ESXi 환경에서 트래픽 측정을 위해 특정 하나의 VM에 트래픽을 모두 보내어 WireShark을 이용하여 트래픽을 측정 할 수 있도록 하는 시스템 구조이다.



(그림 1) 일반적인 Virtual Switch 시스템 구조



(그림 2) 제안하는 Virtual Switch 시스템 구조

3. 제안하는 방안

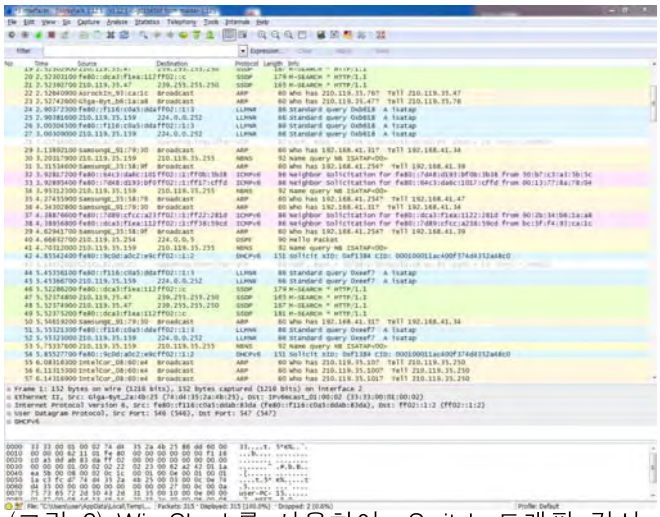
같은 ESXi 호스트에서 전송되는 트래픽을 캡쳐하려면 가상 스위치(vSwitch)를 구성하고 VM의 포트 그룹이 promiscuous mode를 이용할 수 있도록 설정해야한다. 그리고 promiscuous mode가 활성화 된 WireShark에서 네트워크 트래픽을 캡쳐한다.

vSwitch의 포트 그룹에 대한 promiscuous mode 전환은 간단하다. VMware의 vCenter Server 또는 vSphere 클라이언트 중 하나의 vSphere 호스트에서 구성 탭을 선택하고 하드웨어 세션에서 네트워크를 선택한다. vSwitch는 속성을 선택하고 보안 탭에서 promiscuous mode를 활성화하고 있는 포트 그룹을 지정한다.

마지막으로 실제 네트워크 카드에 모든 네트워크 트래픽을 수신하고 스위치 포트를 연결한다. VM의 ESXi 호스트에 연결이 완료되면 VM은 네트워크 트래픽을 감시할 수 있다.

promiscuous mode가 활성화되면 네트워크 트래픽 분석을 시작할 수 있다. 패킷 추가 분석을 원할 경우 네트워크 트래픽을 지정하는 필터를 구성하여 패킷의 특정 정보를 찾을 수 있다.

4. 결과



(그림 3) WireShark를 사용하여 vSwitch 트래픽 감시

(그림 3)은 vSwitch의 트래픽을 감시하기 위해 하나의 특정 VM에 트래픽을 모두 보내어 WireShark를 이용하여 트래픽을 감시한 모습니다.

5. 결론

본 논문에서는 VMware ESXi 환경에서 VM 자원을 연동시켜 하나의 특정 통신 VM(Virtual Machine)에 트래픽 데이터를 수집하여 트래픽을 분석 하였다.

참고문헌

[1] 김대영, 문수복, 박성용, 변성혁, 이순석, 신명기, 정일영 “네트워크 가상화에 대한 고찰”, 정보과학회지, 제26권 제10호, 2008.10.

[2] 강승석, 손예진, 문은지 “클라우드 컴퓨팅 서비스 구현을 위한 네트워크 가상화 연구”, 한국지역정보화학회지, 제13권 제3호, 2010.09.

[3] 민영기, 고갑승 “클라우드 컴퓨팅 환경에서의 가상머신 보안 취약점 탐지 도구 설계”, 보안공학연구논문지, 제 9권 제 6호. 2012.12.

[4] 오도은, 이진기 "Netflow 기반 실시간 네트워크 트래픽 분석 시스템 설계 및 구현", 정보통신산업진흥원, 2002.