오픈플로우를 이용한 Open DPI 플랫폼 구조

이왕봉[*,**], 박상길[*], 김상완[*,**], 이준경[*], 김상하[**]
[*]한국전자통신연구원 통신인터넷연구소
[**]충남대학교 컴퓨터공학과
e-mail : wangbong@gmail.com

An Open DPI Platform Architecture using OpenFlow

Wangbong Lee[*,**], Sang-Kil Park[*], Sang-Wan Kim[*,**], Joon-Kyung Lee[*], Sang-Ha Kim[**]
*Internet Research Lab., Electronics Telecommunication Research Institute
**Dept. of Computer Science and Engineering, Chungnam National University

요 약

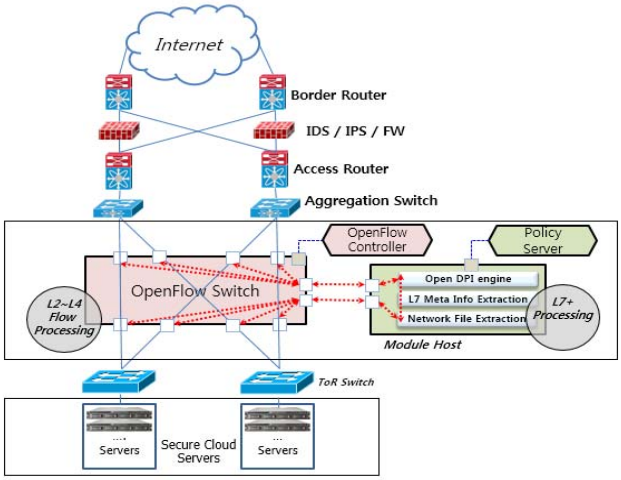
서버 하드웨어 성능 향상과 가상화 소프트웨어 기술의 발달로 클라우드 컴퓨팅 환경은 꾸준히 확산되고 있으며, 이에 따라 인터넷 트래픽 또한 대용량화와 집중화가 진행 중이다. 이와 함께, 지속적인 DDoS 공격 및 사이버테러는 전자정부, 금융, 등 모든 조직을 대상으로 꾸준하게 일어나고 있다. 다양한 사이버테러 공격에 대응하고, 대용량 클라우드 서비스 트래픽을 정밀 분석하는 정책서버 기반의 서비스별/사용자별/그룹별 트래픽 모니터링 및 제어 관리가 필요하다. 본 논문에서 이를 위한 오픈플로우 기반의 고성능 Open DPI(Deep Packet Inspection) 플랫폼 구조를 제안한다.

1. 서론

최근 인터넷 망은 지속적인 DDoS 공격과 시스템 해킹 및 주요 정보 유출 문제로 인해 심각한 안전성을 위협받고 있다. 미국 IBM 에 따르면, 전 세계적으로 하루 38 만건, 연 1 억 3700 만건의 사이버공격이 감행되고 있다고 하며, 우리나라의 경우에도 전자정부, 금융 등 국가 모든 조직을 대상으로 오늘날까지도 꾸준하게 APT(Advanced Persistent Threat) 공격 등이 진행되고 있다[1]. 이러한 네트워크 보안 위협은 기존 방어 방식으로는 대응이 쉽지 않으며, 이를 효과적으로 방어하기 위해 새로운 DPI(Deep Packet Inspection) 기반 기술을 이용하여 트래픽 내의 패킷 속에 포함된 일련의 금지된 행위들을 차단하기 위한 방어 방법들이 연구되고 있다[2][3]. 또한, 서버 하드웨어 성능 향상과 가상화 소프트웨어 기술의 발달로 클라우드 컴퓨팅 환경은 꾸준히 확산되고 있으며, 이와 함께 인터넷 트래픽 또한 대용량화와 집중화가 진행 중이다. 따라서, 다양한 사이버테러 공격에 빠르게 대응하고, 대용량 클라우드 서비스 트래픽을 정밀 분석하는 정책서버 기반의 서비스별/사용자별/그룹별 트래픽 모니터링 및 제어 관리가 필요하다. 본 논문에서는 이를 위해 오픈플로우 기반의 고성능 Open DPI 플랫폼을 제안한다.

2. 오픈플로우를 이용한 Open DPI 플랫폼

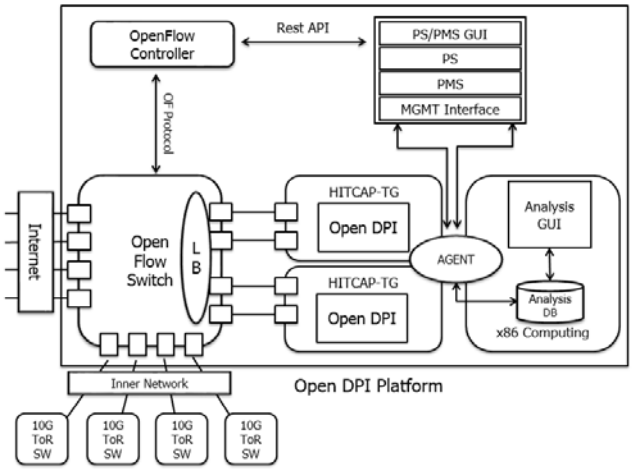
라우터 혹은 스위치는 제어 기능과 데이터 처리 기능을 비롯한 여러 프로토콜 기능들을 하드웨어에 내장하고 있으며, 그 설정 방법도 각 벤더마다 다양하다. 이러한 시스템에서 사용하는 프로토콜들은 IETF를 비롯한 표준화 단체에 의해 결정되고, 해당 벤더들이 해당 제품에 기능을 이식할 수 있다. 이러한 장비들에 사용자가 필요로 하는 기능을 만들어 적용하는 것은 어려운 일이다. 이를 위해, 장비들의 개방(Open)을 통해 다양한 어플리케이션들이 요구하는 기능을 네트워크가 수용할 수 있도록 SDN(Software Defined Network)의 개념이 출현하였다. 오픈플로우 기술은 SDN 을 실현하기에 적합한 기술의 하나로 평가되고 있으며, 현재 오픈플로우 컨트롤러와 네트워크 장치간 인터페이스 규격이 정의되고 있다[4].



(그림 1)오픈플로우를 이용한 Open DPI 플랫폼 적용 예

고성능 Open DPI 플랫폼기술은 이중화된 클라우드망에서 서비스별/사용자별/그룹별 트래픽 모니터링 및 정밀 분석하기 위해 오픈플로우 제어기/스위치를 적

용한다. 오픈플로우 기술을 적용함으로써, 특화된 로드 분산 기능 구현하여 효율적인 부하 분산 처리가 가능하게 된다. 또한, 개방화된 API(Application Layer Interface)를 사용하여 스위치에 대한 관리를 정책서버와 통합할 수 있게 되는 장점이 있다. 오픈플로우 스위치를 통해 이중화된 클라우드 망이 인터넷으로 연결되며, 정책에 따라, L2-L4 플로우 처리를 한 후 DPI 플랫폼에 트래픽이 전달된다. 그림 1 은 오픈플로우를 이용한 고성능 Open DPI 플랫폼의 적용 예이다. 인터넷에서 유입되는 다양한 트래픽을 오픈플로우 스위치를 통해 L2-L4 플로우 프로세싱을 하여 플로우 관리를 하고, 정책에 의해 설정된 규칙에 따라 필터링을 실현하거나, 해당 트래픽을 Open DPI 플랫폼에 전달하여, 해당 트래픽을 분석한다.



(그림 2)오픈플로우를 이용한 Open DPI 플랫폼 구조

고성능의 Open DPI 플랫폼을 제공하기 위해 그림 2 와 같은 기능과 구성요소가 요구된다. 오픈플로우 기능의 스위치와 컨트롤러는 정책서버(PS: Policy Server)의 기본 정책에 따라 L4 필터링 기능과 트래픽 분산 기능을 제공한다. 오픈플로우 컨트롤러는 정책서버에 플로우 관리를 위한 REST(REpresentational State Transfer) API 를 제공하게 되며, 스위치에서 트래픽 분산기능이 가능하도록 오픈플로우컨트롤러에서 플로우를 분석하여 플로우에 대한 정책을 설정한다. 트래픽 분산기능은 오픈 소스 기반의 Floodlight OpenFlow 컨트롤러를 적용하여 개발하였다. 트래픽 분산기능은 입력되는 트래픽을 플로우로 구분한 후, 트래픽 양에 따라 Open DPI 플랫폼의 처리 부하를 조절하는 기능을 수행한다.

정책서버 및 플랫폼 관리시스템(PMS: Platform Management System)을 통해 Open DPI 플랫폼에서 수행되는 정책 그룹 별 정책을 관리한다. 주요기능은 Open DPI 플랫폼(ODP: Open DPI Platform) 적용 정책 관리 기능, Open DPI 플랫폼 시스템 관리 기능, 정책서버와 플랫폼 관리시스템 간 연동 기능이다. Open DPI 플랫폼은 40Gbps 급 트래픽에 대한 정밀 DPI 엔진 및 메타정보 추출 시스템의 기능을 제공한다.

주요 기능으로 네트워크 데이터 모니터링 기능, 네트워크 트래픽 분석 기능, 네트워크 이상징후 감시 기능 등이다. Open DPI 플랫폼(ODP)의 에이전트는 플랫폼 관리시스템(PMS)에서 전달하는 다양한 메시지와 정책을 ODP 의 패킷 처리 전용 하드웨어(HITCAP-TG)에 전달하는 기능을 수행한다. 분석 GUI 는 DPI 엔진을 통해 분석된 다양한 정보를 이용하여 사용자에게 트래픽 통계정보 및 트래픽 분석 결과를 제공한다. 실시간으로 정보가 업데이트되며, 이상 트래픽의 발견 시 알람 정보를 발생하도록 한다. HITCAP-TG 는 Tilera 네트워크 프로세서를 사용하여 패킷 처리를 고속화하기 위해 설계한 패킷 처리 전용 프로세싱 보드이다[5]. HITCAP-TG 는 네트워크 데이터 모니터링 기능 및 분석 기능을 수행하는 DPI 엔진으로 오픈 소스 기반의 Suricata 을 사용한다[6]. 다양한 트래픽 정책을 구현하기 위해 Suricata 를 이용하여 새로운 트래픽 시그너쳐, 트래픽 규칙 등을 추가한다.

3. 추후 연구 방향 및 결론

현재 고성능의 Open DPI 플랫폼은 프로토타입이 완성되어 기본적인 시험을 진행하고 있다. 다양한 시험을 위해 하나의 물리서버에 4 개의 가상화 서버 컴퓨팅 환경을 구성하고 클라이언트의 시연을 위해 2 가지 종류의 클라이언트 네트워크를 구성한다. 하나의 물리서버에는 다수개의 가상 컴퓨팅 환경을 구성한다. 공격을 수행하는 리눅스 머신과 VoD(Video On Demand)서비스를 포함한 다양한 서비스 접속을 위한 리눅스 클라이언트 및 윈도우 클라이언트를 구성한다. 무선 네트워크를 통하여 다양한 모바일 디바이스를 이용하여, 웹페이지에 접속하여 유통되는 메타데이터 및 파일 등을 추출하는 시험을 통해 실시간 서비스에 대한 검출 여부를 확인할 수 있다.

고성능의 Open DPI 플랫폼을 통해 트래픽 분석, 탐지 및 제어/관리 기술 개발을 통해 사업자/고객 트래픽 중요 정보보호 및 주요 사이트에 대한 서비스 생존성 보장이 가능할 수 있다. 또한 정책서버 기반의 서비스별/사용자별/그룹별 트래픽 모니터링과 제어를 통한 투명하고 효율적인 클라우드 운영환경 구축하여 대용량 클라우드 서비스 트래픽 정밀 분석을 실현할 수 있다. 위와 같은 기능이 수행 가능한 Open DPI 플랫폼을 이용하여 대용량 클라우드 네트워크 환경 하의 서비스 보호 분야 시스템으로 적용할 수 있으며, 그 외, 이상 트래픽 및 DDoS 공격에 대한 실시간 탐지 및 제어 분야, 엔터프라이즈 망, 중요 웹서버 사이트 및 서비스 보호 통합관제, 유해 트래픽 차단 등을 위한 정책 기반의 실시간 트래픽 제어기술 분야에도 적용이 가능하다.

참고문헌

[1] www.pressian.com/news/article.html?no=64670
[2] A.Callado, C.Kamienski, G.Szabo, et al., "A Survey on Internet Traffic Identification," Communications Surveys & Tutorials, IEEE, vol. 11, no. 3, pp. 37-52, 3rd Quarter 2009
[3] Milton L. Mueller et al, “Deep packet inspection and bandwidth management: Battles over BitTorrent in Canada and the United States,” Vol. 36, Issue 6, July 2012
[4] www.opennetworking.org
[5] www.tilera.com
[6] suricata-ids.org