논문 16-41-04-09 The Journal of Korean Institute of Communications and Information Sciences '16-04 Vol.41 No.04
http://dx.doi.org/10.7840/kics.2016.41.4.451

SFC 기반 DLP 솔루션을 위한 부하분산 시스템

송 왕 은◆, 정 수 환°

Load Balance System for the SFC Based DLP solution

Wang-Eun Song◆, Sou-Hwan Jung°

요 약

본 논문에서는 SFC(Service Function Chaining) 기반 DLP(Data Loss Prevention) 솔루션을 위한 부하분산 시스템을 제안한다. SFC을 기반한 DLP 솔루션은 사용자의 데이터를 분산 처리하지 않으며, 각 DLP 서버는 할당 받은 사용자 단말에서 발생되는 모든 트래픽을 관리한다. 하지만 사용자별 트래픽 사용량이 다르기 때문에 DLP 서버의 리소스 사용량과 유휴량을 고려하지 않는 기존의 순차방식, 최소접속방식과 같은 부하분산 알고리즘을 사용 할 경우 트래픽이 균등하게 분배되지 못 하여, DLP 서버의 과부하 및 시스템 장애를 발생시킨다. 따라서 본 논문에서는 LBM(Load Balance Management) 서버를 통해 DLP 서버의 리소스 사용량을 기반으로 부하분산을 수행하는 SFC 기반 DLP 솔루션을 위한 부하분산 시스템의 아키텍처를 제안한다.

Key Words : Service Function Chaining, Data Loss prevention, Load Balance

ABSTRACT

In this paper, we propose a Load Balance System for SFC based on DLP solution. SFC based on DLP solution does not distribute to the user data and each DLP server manages all traffic generated by the user device. When using existing algorithms such as the Load Balance Round Robin, Least Connection does not consider the resource usage of DLP server so traffic is not efficiently distributed due to different user traffic usage. It causes system failure and overload of the DLP server. Therefore, we propose the architecture of a Load Balance system for SFC based on DLP solution to perform the Load Balance based on the resource usage of DLP server through a LBM server in this paper.

Ⅰ. 서 론

IT 기술의 발전으로 인터넷을 사용 할 수 있는 단말의 보급률이 높아졌으며, 인터넷 서비스 사용량도 급격하게 증가했다. 따라서 인터넷 서비스 공급자들은 사용자에게 원활한 인터넷 서비스를 공급하기 위해 네트워크 상단에 L4/L7 스위치를 설치하여, 다수의 사용자로부터 요청된 서비스를 다수의 서버에 균일하게 분산하는 부하분산 시스템을 도입했다. 하지만 제안 시스템에서 사용되는 SFC는 특정 서비스를 위하여 각 서버들 간의 트래픽 연결 및 연결 순서를 SDN(Software Defined Networking)[1]을 통해 제어한다. 따라서 SFC 기반 DLP 솔루션은 사용자의 단말에서 발생되는 모든 트래픽이 단일 DLP 서버로 할당되기 때문에 기존의 부하분산 시스템을 도입할 경우 순차방식, 최소접속방식 등과 같은 알고리즘을 사용함으로써, DLP 서버의 리소스 사용량을 고려하지 않은 사용자의 분배로인해 DLP 서버의 과부하를 통한 서비스 장애가 발생된다[2]. 따라서 본 논문에서는 SFC를 기반한 DLP 솔루션에 적용할 수 있는 부하분산 시스템을 제안한다. 제안 시스템의 LBM 서버는 각 DLP 서버의 CPU, Memory, 네트워크 부하분산 과 같은 리소스 소모량을 5초마다 전송받으며, 전송받은 정보를 기반으로 서비스 우선순위를 5초마다 생성 및 갱신한다. 이 후 사용자가 DLP 서비스를 이용할 경우 서비스 우선순위를 기반한 SFC를 구성하여 서비스를 제공한다. 제안 시스템은 DLP 서버의 리소스 사용량

※ 본 연구는 미래창조과학부 및 정보통신기술진흥센터의 대학 IT연구센터육성 지원사업의 연구결과로 수행되었습니다. (IITP-2016-H8501-16-1008)
※ 본 연구는 산업통상자원부 및 한국산업기술평가관리원의 우수기술연구센터(ATC)사업의 일환으로 수행되었습니다. (1415140278, 클라우드 컴퓨팅 환경하에서 정보보안 서비스를 제공하기 위한 SecaaS 프레임워크 원천기술 개발과 이를 이용한 1Gbps급 모바일 정보유출방지 서비스 구축)
◆ First Author : Soongsil University Department of Electronic Engineering, dhkddms1234@nate.com, 학생회원
° Corresponding Author : Soongsil University Department of Electronic Engineering, souhwanj@ssu.ac.kr, 종신회원
논문번호 : KICS2016-02-034, Received February 24, 2016; Revised March 9, 2016; Accepted March 16, 2016

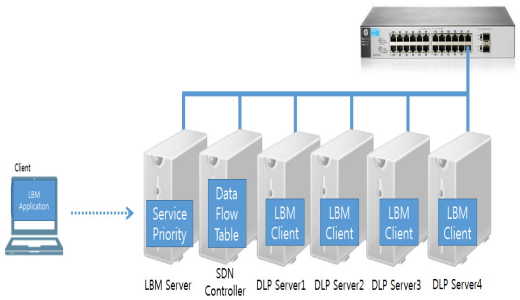

그림 1. 제안 시스템 아키텍처 구성도
Fig. 1. The proposed System Architecture Diagram

을 기반하여 사용자를 배분하여 기존 부하분산 시스템을 이용 할 경우 발생되는 DLP 서버의 과부하 문제를 방지 할 수 있다.

Ⅱ. 제안하는 아키텍처

2.1 제안 아키텍처 구성도

본 논문에서 제안하는 SFC 기반 DLP 솔루션을 위한 부하분산 시스템이다. 부하분산 시스템의 관리를 위한 LBM 서버, DLP 서버의 리소스 사용량과 유휴량을 전송하는 LBM 클라이언트, 사용자와 DLP 서버 간의 SDN을 통한 SFC를 구성하기 위한 SDN Controller, SDN Controller에서 생성된 Data Flow Table을 수행하기 위한 SDN Switch 구성된다. 아키텍처 구성은 그림 1과 같다. LBM 서버는 부하분산 시스템의 관리서버이며, DLP 서버에 설치된 LBM 클라이언트로부터 5초마다 전송받은 시스템 리소스 사용량과 유휴량 정보를 바탕으로 DLP 서버들의 서비스 우선순위를 생성 및 갱신하여 DB 저장한다. 또한 사용자의 서비스 시작 요청 메시지를 전송받을 경우 서비스 우선순위를 바탕으로 사용자와 DLP 서버 간의 SFC 구성을 위한 Data Flow 정보를 SDN Controller에 전송하며, 서비스 종료 요청 메시지를 전송받을 경우 사용자와 DLP 서버간의 구성된 SFC 해제하기 위한 메시지를 SDN Controller에 전송한다. LBM 클라이언트는 각 DLP 서버에 설치되어 있으며, 시스템 리소스 사용량과 유휴량을 5초마다 LBM 서버에 전송한다. SDN Controller는 LBM 서버로 부터 전송받은 Data Flow 정보를 바탕으로 Data Flow Table을 생성하며, SDN Switch가 Data Flow Table 대로 동작하도록 하며, 서비스 종료 요청 시 LBM 서버로부터 전송받은 Data Flow 삭제 메시지를 수행한다. SDN Switch는 SDN Controller에서 생성된 Data Flow 테이블을 기반으로 사용자의 단말에서 발생된 트래픽을 특정 DLP 서버에 전송한다. LBM 어플리케이션은 사용자의 단말에 설치되어 있으며, 인증 받은 사용자의 서비스 요청과 SFC 구성에 필요한 사용자 정보를 LBM 서버에 전송한다. 또한 사용자의 DLP 서비스 종료 요청 시 LBM 서버에 서비스 종료 요청 메시지를 전송한다. DLP 서버는 네트워크 DLP이며, 트래픽 분석 장치를 브릿지 네트워크에 구성하여 사용자 단말의 트래픽을 전송받는 네트워크 인터페이스와 트래픽 검사 후 외부로 전송시키는 인터페이스로 구성된다. 전송된 모든 트래픽은 사전에 중요 정보의 포함 유무를 검사하고 중요 정보가 감지 될 경우 정보 유출을 차단한다.

2.2 제안 아키텍처의 장점

본 논문에서 제안하는 아키텍처는 SFC 환경을 적용하는 다수의 사용자를 DLP 서버에 효율적으로 분산 할 수 있는 부하분산 시스템이다. 사용자의 단말과 SFC가 구성된 DLP 서버는 사용자의 단말에서 발생되는 모든 트래픽을 관리하기 때문에 사용자 분배 시 사용자 별 상이한 트래픽 발생량을 고려하지 않는 순차방식, 최소접속방식 등과 같은 부하분산 시스템을 적용할 경우 DLP 서버의 과부하로 인해 서비스 장애가 발생된다. 하지만 제안 아키텍처에서 LBM 서버는 LBM 클라이언트로부터 5초마다 수집된 DLP 서버의 리소스 사용량과 유휴량 정보를 기반으로 부하분산을 수행하기 때문에 사용자의 DLP 서비스 요청시 서비스 우선순위를 기반으로 현재 가장 리소스 유휴량이 많은 DLP 서버에 사용자 단말을 할당함으로써, 특정 DLP 서버에 트래픽 집중으로 인한 서버 과부하 및 서비스 장애를 사전에 방지 할 수 있는 장점이 있다.

하지만 제안 아키텍처에는 새로운 사용자가 DLP 솔루션을 사용할 때 적용되는 부하분산 시스템으로써, 사전에 DLP 서버와 SFC가 구성된 사용자 단말의 부하분산 사용량의 증가로 인한 DLP 서버의 과부하 문제가 남아있다. 따라서 DLP 서버와 SFC가 구성된 사용자 단말의 급격한 트래픽 증가량으로 인한 서버 과부하를 효율적으로 분산 시킬 수 있는 부하분산 시스템에 대한 추가적인 연구가 필요하다.

Ⅲ. 동작 프로토콜

제안하는 SFC 기반 DLP 솔루션을 위한 부하분산 시스템의 동작 프로토콜은 그림 2와 같다. LBM 서버는 LBM 클라이언트에서 전송받은 정보를 기반으로

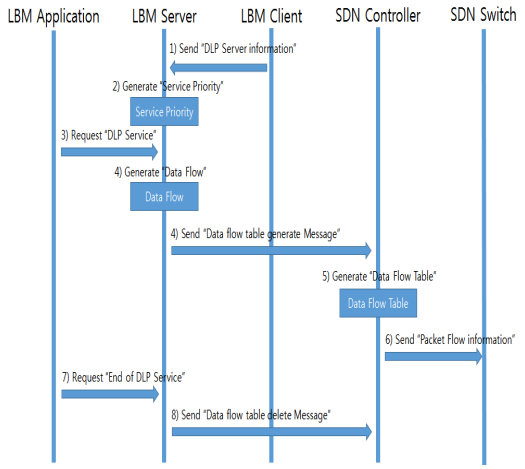

그림 2. 제안 시스템 동작 과정
Fig. 2. Operation of the proposed system

서비스 우선순위를 생성 및 갱신한다. 이 후 사용자가 DLP 서비스 이용 요청 시 SDN Controller에 서비스 우선순위를 기반으로 생성된 Data Flow Table을 전송하여 사용자와 DLP 간의 SFC을 구성함으로써 사용자에게 DLP 서비스를 제공한다.

그림 2의 프로토콜 동작과정을 순서에 따라 아래와 같이 설명한다.

1) 각 DLP 서버에 설치된 LBM 클라이언트는 5초마다 CPU, Memory, 네트워크 트래픽의 사용량과 유휴량 정보를 LBM 서버로 전송한다.

2) LBM 클라이언트에서 전송받은 정보를 기반으로 자체 알고리즘을 사용하여 DLP 서버의 서비스 우선순위를 5초마다 생성 및 갱신하여 DB에 저장한다.

3) 사용자가 DLP 서비스 어플리케이션에 접속 시, LBM 서버에 해당 사용자의 서비스 요청 메시지와 SFC 구성에 필요한 단말의 IP 주소 및 사용자 정보를 전송한다.

4) LBM 서버는 사용자의 DLP 서비스 요청 메시지를 전송받을 경우 DB에 저장된 DLP 서버스 우선순위와 사용자 정보를 기반으로 Data Flow를 생성하여 SDN Controller에 전송한다.

5) SDN Controller는 전송받은 Data Flow를 기반으로 Data Flow Table을 생성한다.

6) SDN Switch은 Data Flow Table을 기반으로 트래픽을 전송하며, Data Flow Table과 일치하지 않는 트래픽이 감지될 경우, SDN Controller 확인 후 동작한다.

7) 사용자가 DLP 서비스를 종료할 경우 LBM 어플리케이션은 LBM 서버에 서비스 종료 메시지를 전송한다.

8) 서비스 종료 메시지를 받은 LBM 서버는 사용자와 DLP 서버 간 SFC 구성 삭제 메세지를 SDN Controller에서 전송한다.

위의 동작과정과 같이 LBM 서버에서 사용자의 서비스 요청 메시지를 받을 경우 서비스 우선순위를 기반으로 사용자 단말과 DLP 서버간의 SFC를 구성하며, 서비스 종료 요청 메시지를 받을 경우 사용자 단말과 DLP 서버간의 SFC 구성을 삭제하는 과정으로 이루어진다.

Ⅳ. 결 론

본 논문에서는 SFC 기반 DLP 솔루션을 위한 부하분산 시스템을 제안하였다. SFC 기반으로 DLP 서비스를 구성할 경우 한 사용자 단말에서 발생한 모든 트래픽을 단일 DLP 서버에 할당한다. 때문에 한명의 사용자 일지라도 다수의 사용자보다 사용하는 데이터량이 많을 경우 기존의 순차방식, 최소접속방식을 적용할 경우 DLP 서버의 과부하 문제를 야기 할 수 있다. 하지만 제안 시스템은 DLP서버의 리소스 사용량과 유휴량을 바탕으로 생성된 서비스 우선순위를 이용하여 부하분산을 수행하기 때문에 SFC 환경의 DLP 서비스를 사용하는 다수의 사용자를 다수의 서버에 적절하게 분배함으로써, 서버의 과부하 문제를 사전에 방지 할 수 있는 장점이 있다.

향후 제안 시스템을 실제 인터넷 서비스 환경에 구현하여, 부하분산 시스템이 다수의 사용자 단말을 다수의 DLP 서버에 할당하는 테스트의 결과 값을 통해 부하분산 시스템에 관한 성능측정이 필요하다.

References

[1] G. Lee, I. Jang, W. Kim, S. Joo, M. Kim, S. Pack, and C.-H. Kang, “CSDN-based middlebox management framework in integrated wired and wireless networks,” *J. KICS*, vol. 39B, no. 06, pp. 379-386, 2014.

[2] W. Zhang, “Linux virtual sever for scalable network services,” *Ottawa Linux Symp.*, 2000, http://www.linuxvirtualserver.org/lvs.pdf