KIPS Tr. Comp. and Comm. Sys.
Vol.4, No.4 pp.135~140 pISSN: 2287-5891

http://dx.doi.org/10.3745/KTCCS.2015.4.4.135

Implementation and Validation of the Web DDoS Shelter System(WDSS)

Jae-Hyung Park† · Kang-Hyoun Kim††

ABSTRACT

The WDSS improves defensive capacity against web application layer DDoS attack by using web cache server and L7 switch which are added on the DDoS shelter system. When web DDoS attack occurs, security agents divert traffic from backbone network to sub-network of the WDSS and then DDoS protection device and L7 switch block abnormal packets. In the meantime, web cache server responds only to requests of normal clients and maintains stable web service. In this way, the WDSS can counteract the web DDoS attack which generates small traffic and depletes server-client session resource. Furthermore, the WDSS does not require IP tunneling because it is not necessary to retransfer the normal requests to original web server. In this paper, we validate operation of the WDSS and verify defensive capability against web application layer DDoS attacks. In order to do this, we built the WDSS on backbone network of an ISP. And we performed web DDoS tests by using a testing system that consists of zombie PCs. The tests were performed by three types and various amounts of web DDoS attacks. Test results suggest that the WDSS can detect small traffic of the web DDoS attacks which do not have repeat flow whereas the formal DDoS shelter system cannot.

Keywords : Web DDoS, HTTP, Application Layer, Web Cache

웹 DDoS 대피소 시스템(WDSS) 구현 및 성능검증

박 재 형† · 김 강 현††

요 약

WDSS는 네트워크 연동구간을 이용한 DDoS 대피소 시스템에 L7 스위치와 웹캐시서버를 추가 구성하여 웹 응용계층 DDoS 공격에 대한 방어성능을 향상시킨 시스템이다. WDSS는 웹 DDoS 공격 발생 시 백본 네트워크로부터 트래픽을 우회한 뒤 비정상 요청은 DDoS 차단시스템과 L7 스위치에서 차단하고 정상적인 클라이언트의 요청에 대해서만 웹캐시서버가 응답하게 함으로써 소규모 트래픽 기반의 세션 고갈형 DDoS 공격에 대응하고 정상적인 웹서비스를 유지한다. 또한 정상 트래픽을 웹서버로 재전송하기 위한 IP 터널링 설정이 없이도 공격 대응이 가능하다. 본 논문은 WDSS를 국내 ISP 백본 네트워크상에 구축하여 시스템 작동에 대한 유효성과 웹 응용계층 DDoS 공격 방어성능을 검증한 결과를 다룬다. 웹 DDoS 방어성능 평가는 실제 봇넷과 동일한 공격 종류와 패킷수의 공격을 수행할 수 있는 좀비 PC로 구성한 DDoS 모의 테스트 시스템을 이용하여 실시하였다. 웹 응용계층 DDoS 공격 종류와 강도를 달리하여 WDSS의 웹 DDoS 방어성능을 분석한 결과 기존의 DDoS 대피소 시스템에서 탐지/방어하지 못한 소규모 트래픽에 기반하며 동일 플로우를 반복적으로 발생하지 않는 웹 DDoS 공격을 탐지/방어할 수 있었다.

키워드 : 웹 DDoS, HTTP, 응용계층, 웹 캐시

1. 서 론

웹 DDoS는 동일 플로우를 반복적으로 발생하지 않으면서 적은 트래픽으로 이루어지므로 기존 DDoS 보안장비의 플로우, 트래픽 오차 분석기법으로는 대응하기 어렵다. 이러한 문제를 해결하고자 DDoS 공격 탐지 알고리즘을 개선하는 등 관련 연구들이 이뤄졌으나, 기존 방법으로는 예측 불가능하게 진화하는 공격 유형에 대처하기 힘들었다[1-11].

따라서 다양한 네트워크 환경에서도 작동할 수 있으며 새로운 유형의 웹 DDoS 공격에 대해서 유연하게 대처할 수 있는 시스템의 필요성이 대두됨에 따라 WDSS이 제안되었다[12].

WDSS는 L7 스위치와 웹캐시서버를 이용하며, 클라이언트-서버 간 연결 및 세션 자원을 관리함으로써 웹 DDoS 방어성능을 개선한다. 웹 DDoS 발생 시 트래픽은 목적지 서버가 아닌 WDSS로 우회되며 DDoS 차단시스템이 L3, L4 DDoS 공격을 1차로 방어한 후 L7 스위치와 웹캐시서버가 L7 DDoS 공격을 방어하여 최종적으로 웹캐시서버는

† 준 회 원 : 한국방송통신대학교 정보과학과 석사
†† 종신회원 : 한국방송통신대학교 컴퓨터과학과 교수
Manuscript Received : October 17, 2014
First Revision : December 26, 2014
Accepted : December 29, 2014
* Corresponding Author : Jae-Hyung Park(earstec@gmail.com)

정상적인 HTTP 요청에 대해서만 응답한다. 한편, 웹캐시 서버는 본래 웹서버와 별도의 라우팅 경로를 통하여 웹콘텐츠를 동기화한다. 웹캐시서버는 클라이언트의 요청에 직접 콘텐츠를 응답하므로, IP 터널링 설정이 불가능한 액세스 라우터에 수용되어있는 웹서버라 할지라도 WDSS 이용이 가능하다는 특징을 가지고 있다.

WDSS는 보호대상 웹서버의 웹페이지 응답시간을 주기적으로 체크하다가 응답시간이 오차 범위를 초과할 시 웹 DDoS 공격발생으로 간주한다. 만약 웹페이지 응답이 지연되거나 오류가 발생할 경우에는 패킷을 수동 분석하여 웹 DDoS 공격 유무를 확인하므로 트래픽 오차 및 플로우 오차 분석 방법에 비하여 공격 탐지 확률이 상승되는 효과가 있다[13].

본 논문에서는 WDSS를 국내 ISP의 백본 네트워크상에 실제 구축한 후 시스템 유효성을 검증하고 표준적인 절차에 걸쳐 웹 응용계층 DDoS 방어성능을 평가한 결과를 다룬다. 실제 DDoS 공격과 동일한 환경에서 WDSS 작동 유효성을 검증하고 DDoS 방어성능을 평가하기 위하여 좀비 PC로 봇넷을 구성한 DDoS 모의훈련 시스템을 이용하여 웹 DDoS 공격 종류와 트래픽을 변화시켜가며 테스트한 결과를 수치적으로 분석하였다.

2. DDoS 대피소 시스템 연구 동향

기존 DDoS 대피소 시스템은 Fig. 1과 같이 DDoS 차단시스템이 이상트래픽을 필터링한 후 정상트래픽을 목적지로 전달하기 위해서 IP 터널링을 필수적으로 요구한다. 또한 불규칙 소규모 트래픽으로 이루어지는 웹 DDoS 공격에 취약하다. 이러한 한계점을 보완하기 위한 연구 동향은 아래와 같다.

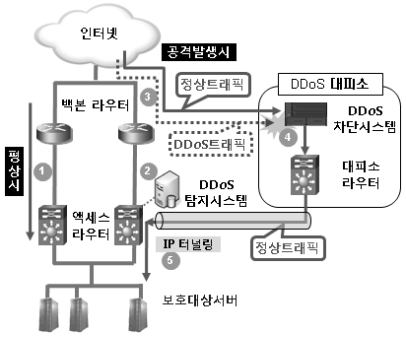

Fig. 1. Existing DDoS Shelter System

2.1 DDoS 차단시스템 알고리즘 업데이트

웹 DDoS 탐지 및 차단 알고리즘을 개선하여 DDoS 차단시스템에 적용함으로써 웹 DDoS 대응 성능을 향상시킨다. 그 예로는 웹서버 접속 IP별 Request 비율이 일정하게 변화할 시 공격으로 판단하여 트래픽을 차단하는 방법, 프로토콜 패턴분석에 의거하여 좀비 PC로 의심되는 IP를 블랙리스트로 분류하여 자원할당을 조절하는 방법, HTTP POST Request에서 두 번째 패킷부터 데이터 양이 급격하게 적어지는 경우 HTTP POST 공격으로 판단하는 방법 등이 있다[1, 2]. 하지만 알고리즘 개선과 관련한 연구는 주로 공격형태와 트래픽 패턴을 분석한 후에 사후 대처하는 방식으로 이루어지므로 웹 DDoS에 의한 웹서버 자원 소모 문제를 즉각적으로 대처하기는 어렵다.

2.2 L4 스위치 트래픽 플로우 컨트롤

Fig. 2와 같이 DDoS 차단시스템 상단에 L4 계층 스위치를 배치하고 트래픽 플로우 학습기능을 이용하여 패킷 통과 비율을 조절함으로써 DDoS 공격을 완화하는 방법이다.

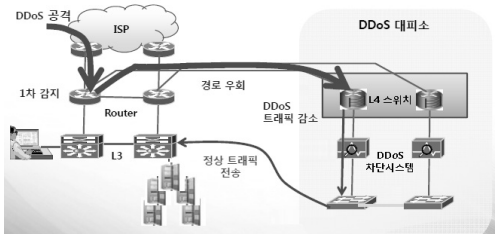

Fig. 2. L4 Switch Traffic Control(Source : ETRI)

L4 스위치는 인터페이스 또는 IP별 플로우 통계값을 분석하여 평상시 정상적인 트래픽 발생 패턴을 보인 IP들은 화이트리스트에 등록하고 알려지지 않은 DDoS 공격 패킷은 사전에 차단한다. 하지만 이 방법으로는 TCP, UDP 기반의 플로우 흐름상으로 이상행위가 아니지만 응용계층에서 변칙적인 접속을 시도하는 공격의 경우 방어하지 못하는 경우가 발생한다.

2.3 목적지 IP 변경을 통한 트래픽 리다이렉트

Fig. 3과 같이 보호대상 URL에 해당하는 DNS의 호스트 정보를 보호대상 웹서버의 IP에서 DDoS 대피소의 차단시스템 IP로 변경하여 트래픽을 우회하고 필터링을 거친 정상트래픽의 목적지 IP를 다시 보호대상 웹서버 IP로 변경한다.

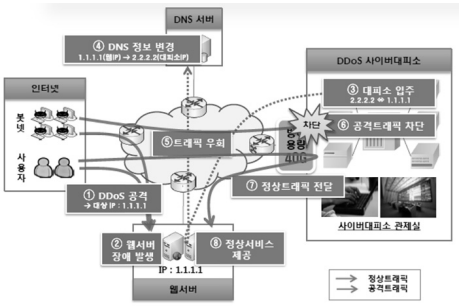

Fig. 3. Traffic Redirect by Changing DNS IP (Source : KISA)

이 방법은 DDoS 대피소 출구에서 각 패킷의 목적지 IP를 변경하기 때문에 IP 터널링이 없이도 목적지까지 정상트래픽을 전달할 수 있다. 하지만, DDoS 발생 시에 필터링을 거친 정상 HTTP Request 패킷의 목적지 IP를 변경하는 과정이 지속적으로 수반되어야 하므로 웹페이지 로딩시간이 증가한다는 단점이 존재한다. 또한 신종 웹 DDoS 공격발생으로 보안전용장비에서 차단에 실패할 경우 모든 잔존 트래픽은 보호대상 웹서버 측으로 그대로 전달되기 때문에 보호대상 서버에 위협이 될 수 있다.

3. WDSS 트래픽 우회 방식

기존 DDoS 대피소는 L7스위치와 웹캐시서버 없이 단지 IP 기반으로 트래픽의 라우팅 경로를 변경하여 트래픽을 우회하여 DDoS 방어시스템에서 필터링한 후 IP 터널링을 통하여 정상트래픽만 본래 목적지로 보내주는 방식이었다. 하지만, 웹 DDoS 공격 시에는 HTTP 프로토콜을 이용하므로 트래픽 우회 방식에도 차이점이 있어야 한다. WDSS에서 트래픽을 우회하는 방식은 다음의 두 가지가 있다.

3.1 DNS Host IP 변경 방식

DNS IP 변경 방식은 Fig. 4와 같이 DNS Host IP 정보를 Real IP에서 웹캐시서버의 IP로 변경하여 해당 URL로 페이지를 요청하는 패킷을 웹캐시서버로 향하게 하는 것이다.

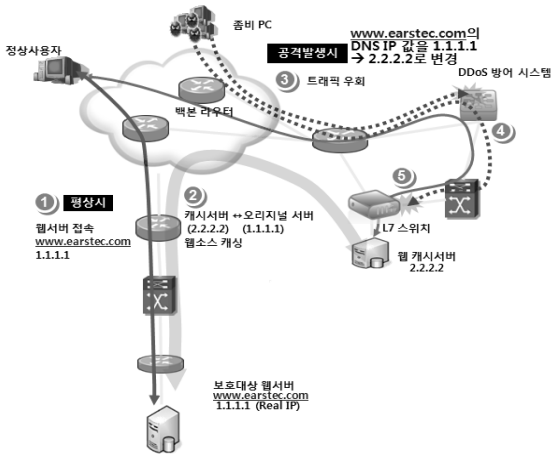

Fig. 4. Changing DNS Host IP Type

① (정상 접속) 정상적으로 접속하고자 하는 이용자는 보호대상 웹서버로부터 HTTP 응답을 받아 웹페이지를 열람한다.

② (웹콘텐츠 캐싱) 보호 대상 웹서버와 WDSS의 웹캐시서버는 사전에 설정된 경로를 통해 정적/동적 웹콘텐츠를 동기화한다.

③ (공격 발생) 웹페이지 응답이 지연되거나, 접속장애 시 웹 응용계층 DDoS 공격 발생 유무를 분석한다. 공격발생임이 확인되면 테스트 웹페이지의 URL(www.earstec.com)에 해당하는 DNS Host IP 정보를 Real IP(1.1.1.1)에서 WDSS 웹캐시서버 IP(2.2.2.2)로 변경한다. DNS Host IP 변경이 완료되면 www.earstec.com을 요청한 트래픽은 전량 WDSS로 우회된다.

④ (공격 차단) DDoS 방어시스템은 L3, L4 DDoS와 일부 L7 DDoS를 차단한다(1차 차단). L7스위치는 TCP Connection을 관리하고, Set-Cookie 설정과 세션테이블 관리 등을 통해 웹 DDoS 공격 트래픽을 차단한다(2차 HTTP DDoS 방어).

⑤ L7 스위치는 정상적인 HTTP Request라고 판단된 패킷만을 웹캐시서버로 전달하고 웹캐시서버는 이에 대한 HTTP Response 패킷을 L7스위치로 응답한다. L7 스위치는 세션 정보를 참고하여 클라이언트에게 최종적으로 HTTP Response 패킷을 전달한다.

3.2 Second IP 설정 방식

웹서버가 서비스에 사용하는 Real IP 외에 여분의 공인 IP를 확보해두었을 때 사용할 수 있는 방식이다. DNS Host IP 변경 방식에서는 글로벌 DNS에 IP 변경정보가 전파되기까지 시간이 경과되는 반면에, Second IP 설정 방식은 백본 네트워크에서 라우팅 경로를 변경하는 것으로 빠른 대응이 가능하다.

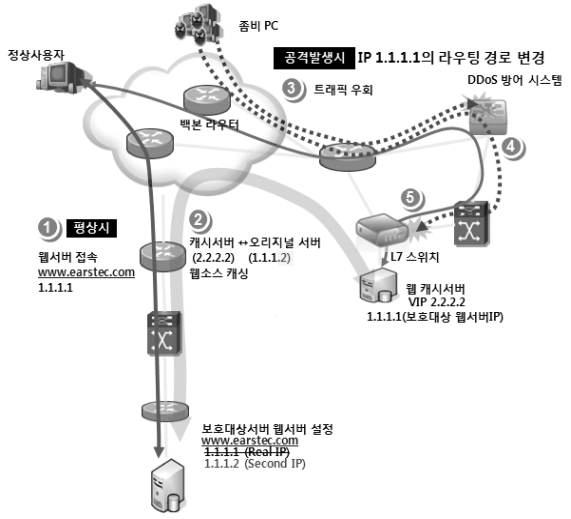

Fig. 5. Setting Second IP Type

Fig. 5와 같이 Second IP 설정 방식은 전반적으로 DNS Host IP 변경 방식과 비슷한 절차로 작동하지만, 트래픽을 우회할 때 동작상에 차이점이 있다.

① (정상 접속) DNS Host IP 방식과 동일

② (웹콘텐츠 캐싱) DNS Host IP 변경 방식에서는 웹캐시서버가 웹서버의 Real IP와 통신하였지만 Second IP 설정 방식에서는 웹캐시서버가 웹서버로부터 웹콘텐츠를 캐싱 하기 위해서 Second IP와 통신한다.

③ (공격 발생) 웹서버 Real IP(1.1.1.1)의 라우팅 경로를 WDSS 방향으로 설정하고 www.earstec.com로 향하는 모든 HTTP 요청은 웹캐시서버로 우회된다.

④ (공격 차단) DDoS 방어시스템은 L3, L4 DDoS와 일부 L7 DDoS를 차단한다(1차 차단). L7스위치는 TCP Connection을 관리하고, Set-Cookie 설정과 세션테이블 관리 등을 통해 웹 DDoS 공격 트래픽을 차단한다(2차 HTTP DDoS 방어).

⑤ L7 스위치는 정상적인 HTTP Request라고 판단된 패킷만을 웹캐시서버로 전달하고 웹캐시서버는 이에 대한 HTTP Response 패킷을 L7스위치로 응답한다. L7 스위치는 세션 정보를 참고하여 클라이언트에게 최종적으로 HTTP Response 패킷을 전달한다.

3.3 WDSS 트래픽 우회방식별 특징

WDSS 트래픽 우회방식별 특징은 Table 1과 같이 정리할 수 있다. 트래픽 우회방식 선택은 웹서버 측의 네트워크 환경과 기술적용 가능성, 비용 등을 고려하여 결정한다.

Table 1. Features of Two Types of WDSS

구분	DNS Host IP 변경 방식
장점	• 추가의 공인 IP를 확보하기 위한 비용이 들지 않음 • 웹캐시서버 IP가 고정되므로 악성 포트를 사전에 차단하는 등 이상트래픽에 대한 사전대응을 강화할 수 있음 • WDSS 수용라우터와 L7스위치 간의 통신에 웹캐시서버 IP를 이용하므로 관리가 편리함
단점	• 해커가 웹서버의 URL이 아닌 Real IP로 직접 공격 시 WDSS로 대응이 어려움 • 트래픽 우회 시 DNS Host IP 정보 변경 과정과 DNS 간 변경이력 전파로 인하여 대응시간이 길어짐 • 웹서버는 공인 IP를 1개만 보유하고 있으므로(서비스용) 웹캐시서버-웹서버 간에 상시적인 콘텐츠 동기화는 불가능함

구분	Second IP 설정 방식
장점	• DNS Host IP 정보 변경 없이 라우팅 경로 변경만으로 신속하게 공격에 대응할 수 있음 • 웹캐시서버 IP가 외부에 노출되지 않으므로 보안성이 강화됨 • 웹캐시서버-웹서버 간에 콘텐츠 동기화가 원활함
단점	• WDSS 수용라우터와 L7스위치 간에 라우팅 프로토콜 설정 및 경로 관리가 어려움 • IP 변경사항을 WDSS에 미반영 시 작동에 차질이 발생함

4. 시스템 유효성 검증 및 방어성능 평가

웹 DDoS 대응체계 수립을 위하여 WDSS를 과천에 위치한 국내 ISP의 네트워크 관제센터에 실구축하였다. 이번 절에서는 WDSS로 하여금 테스트 웹사이트를 보호하도록 한 후 시스템 작동 유효성을 검증하고 웹 DDoS 방어성능을 평가한 결과를 다룬다. 첫 번째 단계로 웹캐시서버의 기능을 검증하였으며 웹 DDoS 공격 발생 시 기존 DDoS 대피소 시스템의 방어성능과 WDSS의 방어성능을 비교하였다. 다음으로 DDoS 공격이 없는 평상시 웹페이지 로딩 속도와 웹 DDoS 공격이 발생하여 WDSS로 트래픽을 우회하여 웹캐시서버에서 응답하는 경우의 웹페이지 로딩속도를 비교하였다.

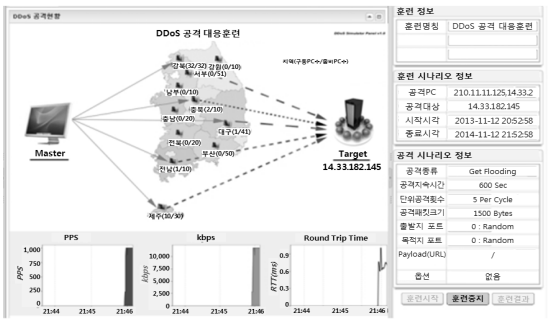

Fig. 6. DDoS Simulation Training System

DDoS 방어성능 검증을 수행하기 위하여 전국적으로 분포된 유휴서버를 이용하여 마스터 서버와 좀비 PC로 봇넷을 구성한 모의 DDoS 시스템을 사용하였다. Fig. 6은 모의 DDoS 시스템의 관리자 화면이며 공격종류, 공격시간, 공격목표, 공격량 등을 설정하고 공격명령을 내릴 수 있다.

각각의 좀비 PC에는 NetBot Attacker 6.0으로 작성된 악성코드를 이용하여 공격명령 모니터링 프로세스와 트래픽 발생 프로세스를 생성하였고, 모의 DDoS 시스템 관리자 웹페이지 서버에는 NetBot Attacker Host 프로그램을 구동하였다.

봇넷 구성에 사용된 컴퓨터의 사양은 다음과 같다.

- CPU : Intel Xeon Dual Core 2.0 GHz
- Memory : 4G(2G*2)
- OS : CentOS release 5.6(Final)

4.1 웹캐시서버 기능 검증

Table 2는 웹캐시서버 기능 검증의 시험항목별 검증 내용과 결과를 보여준다. 해외 ISO9001 및 국내 NET 신기술인증, Inno-Biz 인증에 의거한 테스트 결과 전 항목에서 정상적인 기능을 하였으며 안정적인 웹서비스를 제공하기에 적합한 결과를 얻었다. 웹캐시서버의 사양은 다음과 같다.

- CPU : Intel Xeon CPU 2.40 GHz
- Memory : 32GB(8G*4)
- OS : 64bit CentOS Linux kernel 2.6

Table 2. Functional Test Result of the Web Cache Server

번호	시험항목	결과	내용
1	장비 1대당 최대 접속 세션수	양호	100만 세션(1000kpps) 지원
2	리버스캐싱 기능 지원 및 멀티 도메인 리버스 캐싱 기능 시험	양호	10개 이상의 도메인 설정 후 실제 웹페이지 캐싱 정상 동작 확인 (포털, 신문, 금융 등)
3	웹 세션 관리 기능 시험	양호	세션 관리를 위한 연결지속관리 기능 정상동작
4	JPG, GIF, PNG / HTML, HTM, XML / Flash / 파일 등 캐싱 지원 확인	양호	access.log 분석 결과 각 파일의 Request에 대하여 HIT/200 확인
5	웹Cache 내에 전달된 콘텐츠의 TTL(Max-age)값의 변경이 가능한지 확인	양호	HTTP 최소, 최대 객체 갱신 시간을 설정 확인
6	특정 파일 타입에 대한 강제캐시, 캐시해제 기능을 지원하는지 확인	양호	강제 캐싱 정책설정 확인
7	장비 내부적으로 Process 및 CPU에 대한 부하분산 여부	양호	멀티 프로세싱 및 CPU 로드밸런싱 작동 확인
8	하드디스크의 기본 캐싱 이외에 RAM 상에 Caching Size 할당 여부	양호	시스템 정보의 메모리 캐시 크기 확인하여 최대 5GB의 캐싱 사이즈 확인
9	이미지 캐싱을 위한 디스크 캐시방식을 지원하는지 확인	양호	시스템 정보에서 메모리 캐시와 디스크 캐시 크기와 실제 디스크 사이즈 변화량 확인
10	SSL 기능 제공 확인	양호	443포트를 사용한 https 페이지 정상출력

4.2 WDSS 방어성능 평가

모의 DDoS 시스템을 이용하여 테스트 웹페이지를 대상으로 모의 DDoS 공격을 실시하였다. 공격에 가담하는 좀비 PC 수를 점차적으로 줄이면서 트래픽이 작아짐에 따라 기존 DDoS 대피소 시스템과 WDSS가 방어할 수 있는 성능을 비교 분석하였다. DDoS 공격정보는 다음과 같다.

- 보호대상 웹페이지 : www.earstec.com
- 공격 종류 : HTTP GET Flooding, HTTP CC Attack, HTTP POST Attack
- 공격당 지속시간 : 180초
- 패킷당 크기 : 512Bytes

기존 DDoS 대피소 시스템의 DDoS 탐지시스템은 Fig. 7과 같이 웹 DDoS의 pps가 오차범위를 넘어갈 때만 공격을 탐지하고 DDoS 차단시스템은 동일 플로우를 반복적으로 발생하는 IP만을 차단한다.

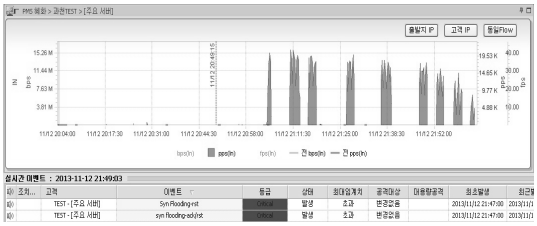

Fig. 7. Detected DDoS by the Existing DDoS Shelter

이러한 방식으로는 HTTP CC Attack과 HTTP POST Attack 등 소규모 트래픽 기반이면서 동일 플로우 수가 적은 공격은 탐지하지 못하며 단지 트래픽 오차의 임계치를 초과하는 용량의 HTTP GET Flooding과 TCP SYN Flooding과 같은 공격만 방어할 수 있다. 모의 DDoS 시스템에서 발생하는 트래픽을 점차 줄여가며 측정한 결과 DDoS 대피소 시스템은 Fig. 8과 같이 공격트래픽이 5 kpps 이하일 경우, 탐지 임계치를 초과하지 않으므로 공격경보 이벤트가 '해제'되면서 공격이 발생하지 않는 것으로 판단하였다. 따라서 실제 발생 중인 DDoS 공격에 대한 탐지 및 방어에 실패하게 된다.

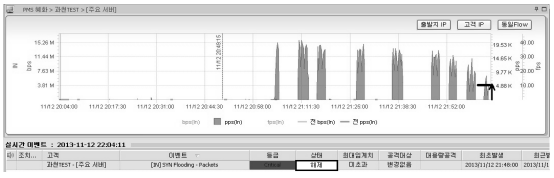

Fig. 8. Fail to Detect DDoS by the Existing DDoS Shelter

Fig. 9는 테스트 대상의 웹페이지에 대하여 30초 간격으로 웹 로딩시간을 측정한 결과이다. 4.75kpps의 HTTP CC Attack 시 기존 DDoS 대피소 시스템은 이를 탐지하지 못하며 DDoS 공격으로 인하여 서비스가 지연됨에 따라 웹 로딩속도에 변동을 보인다. 웹 로딩시간이 최소 2.247초에서 최대 9.247초까지 변동하며, 때때로 페이지 출력에 오류가 발생하는 결과를 보여준다.

Fig. 9. Web Page Loading Time Test

반면 WDSS를 이용하여 5kpps 이하의 DDoS 공격에 대응한 결과 웹 Fig. 10과 같이 모든 DDoS 공격을 차단하였으며 0.2초 초반대의 안정적인 웹 로딩시간을 보였다.

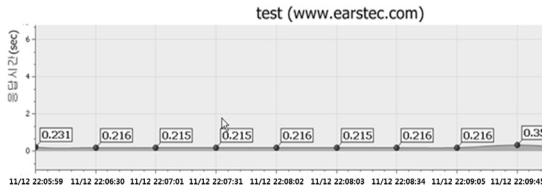

Fig. 10. Success to Protect the Web Page by the WDSS

WDSS는 웹 응용계층 DDoS 공격을 차단한 후 웹캐시서버로부터 정상적인 응답을 보내주므로 웹페이지가 정상적으로 출력할 수 있었다.

4.3 웹페이지 로딩시간 비교

테스트 웹페이지를 보호대상 웹서버로부터 직접 응답받는 경우와 웹캐시서버로부터 응답받을 경우의 로딩시간을 비교 측정하였다. 응답시간 측정 시 사용한 툴은 Cache Flow WebTimer Version 2.3.5이며 일반 인터넷 가입자의 PC로 시간 간격 5초, 반복횟수 5회로 웹페이지를 요청하여, 응답시간의 평균값을 계산하였다.

Table 3. Comparison of Web Loading Time

구분	Client1(WDSS와 동일 ISP의 PC)	Client2(WDSS와 다른 ISP의 PC)
① 평상시 - 웹서버 응답	209 ms	364 ms
② 공격 시 - WDSS 응답	228 ms	515 ms
② / ①	1.09	1.41

Table 3에서 Client1은 WDSS가 구축된 백본 네트워크와 동일한 네트워크 가입자 PC이며 Client2는 WDSS와 다른 타 ISP의 네트워크에 수용된 가입자 PC이다. 각각의 PC로부터 테스트 웹페이지에 접속할 시 웹 로딩속도를 측정하였다. 웹 로딩시간 측정 결과, 웹 DDoS 공격 방어 시에는 트래픽 우회와 공격 트래픽 처리, 웹캐시서버로부터의 응답시간이 소요되므로 로딩시간은 평상시 웹서버로부터 직접 로딩할 때에 비해 증가하였다. Client1과 Client2의 공격 시/평상시 로딩시간 비율은 각각 1.09, 1.41배의 값을 보였다. Cleint2의 로딩시간이 더 긴 이유는 타 ISP의 경우 IX 구간을 거친 후 WDSS로 트래픽이 유입되어 공격 방어 시 패킷 처리가 느려지기 때문이다.

5. 결 론

본 논문은 기존 연구에서 제안한 웹 DDoS 대피소 시스템, 즉 WDSS를 국내 ISP의 백본 네트워크에 실구축한 후 작동 유효성을 검증한 결과와 웹 DDoS 공격에 대한 방어성능 평가 결과를 다루었다[12, 13]. L7 스위치는 TCP Connection 관리와 HTTP Session 관리로 비정상적인 HTTP Request를 차단하며 HTTP GET Flood, CC Attack, HTTP POST Attack 등 웹 응용계층의 세션 고갈형 DDoS 공격을 방어한다. 또한 DDoS 공격 발생 시 HTTP Request 트래픽을 우회하여 웹캐시서버로부터 직접 응답하도록 하고, 웹캐시서버는 보호대상 서버로부터 동적/정적 콘텐츠를 캐싱 하여 웹페이지 서비스가 지속되도록 하여 IP 터널링 설정이 불가능한 라우터에 수용되어있는 서버라 하더라도 DDoS 대피소 시스템을 이용할 수 있게 되었다.

웹 DDoS 방어성능 검증 실험에서는 웹 DDoS 트래픽의 bps와 pps를 조절하면서 기존 DDoS 대피소와 WDSS의 공격 탐지 여부와 이상트래픽 차단 후 웹페이지가 정상적으로 출력되는지의 여부를 알아보았다. 실험 결과 WDSS는 일정 pps 이하의 트래픽으로 구성되고 동일 플로우가 반복적으로 발생하지 않아 기존 DDoS 대피소가 탐지/방어하지 못하는 웹 DDoS 공격 또한 대응할 수 있었다. 또한 웹 DDoS 공격이 발생하여 WDSS로부터 웹페이지 응답을 받더라도 로딩시간에 큰 지연이 없었으며 웹서비스 가용성을 유지할 수 있었다.

최근에는 DNS, 메일서버 등을 대상으로 한 응용계층 DDoS 공격이 증가하는 추세이다. 하지만, WDSS는 웹콘텐츠만을 캐싱 하기 때문에 그 이용이 웹서버를 대상으로 한 공격 방어에만 제한된다는 한계점이 여전히 존재한다. 이어지는 연구에서는 TCP 프록시 서버를 추가하여 TCP 계층 이상의 어떠한 응용계층 프로토콜에 대한 DDoS 공격에 대해서도 방어를 할 수 있는 DDoS 대피소 시스템 구성에 대한 연구를 진행할 것이다. 이와 더불어 L7 스위치의 로드밸런싱 기능을 이용하여 캐시 서버를 다중화함으로써 동시다발적인 대규모 공격의 방어에 대한 방어 시스템 구축에 대한 연구방향을 모색해야 할 것이다.

References

[1] Saman Taghavi Zargar, James Joshi, and David Tipper, “A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks,” *Communications Surveys & Tutorials*, IEEE, Vol.15, Issue.4, Mar., 2013.

[2] Ahmad Sanmorino, Setiadi Yazid, “DDoS Attack detection method and mitigation using pattern of the flow,” Information and Communication Technology (ICoICT), 2013 International Conference on, Mar., 2013.

[3] P. K. Park, S. M. Yoo, HoYong Ryu, and Cheol Hong Kim, “Service-Oriented DDoS Detection Mechanism Using Pseudo State in a Flow Router,” Information Science and Applications (ICISA), 2013 International Conference on, Jun., 2013.

[4] Sujatha Sivabalan1, Dr P J Radcliffe, “A Novel Framework to detect and block DDoS attack at the Application layer,” TENCON Spring Conference, 2013 IEEE, Apr., 2013.

[5] S. Renuka Devi, P. Yogesh, “An Effective Approach to Counter Application Layer DDoS Attacks,” Computing Communication & Networking Technologies (ICCCNT), 2012 Third International Conference on, Jul., 2012.

[6] Baik, N., Sungsoo Ahn, and Namhi Kang, “Effective DDoS Attack Defense Scheme Using Web Service Performance Measurement,” Communications Magazine, Ubiquitous and Future Networks (ICUFN), 2012 Fourth International Conference on, Jul., 2012.

[7] Veronika Durcekova, Ladislav Schwartz, and Nahid Shahmehri, “Sophisticated Denial of Service Attacks Aimed at Application Layer,” ELEKTRO, May., 2012.

[8] Jin Wang, Xiaolong Yang, and Keping Long, “Web DDoS Detection Schemes Based on Measuring User's Access Behavior with Large Deviation,” Global Telecommunications Conference (GLOBECOM 2011), 2011 IEEE, No.1, Dec., 2011.

[9] Yi Xie, Shun-zheng Yu, “Monitoring the Application-Layer DDoS Attacks for Popular Websites,” Networking, IEEE/ACM Transactions on, Vol.17, Issue.1, Feb., 2009.

[10] Supranamaya Ranjan, Ram Swaminathan, Mustafa Uysal, Antonio Nucci, and Edward Knightly, “DDoS-Shield: DDoS-Resilient Scheduling to Counter Application Layer Attacks,” Networking, IEEE/ACM Transactions on, Vol.17, Issue.1, Feb., 2009.

[11] T. J. Lee, C. S. Im, C. T. Im, and H. C. Jung, “Light-weight Defense Mechanisms for application layer DDoS Attacks in the Web Services,” KIISC, 20-5, 2010.

[12] J. H. Park, K. H. Kim, “A Web DDoS Defence System using Network Linkage,” 39th KIPS autumn academic conference 20-1, 2013.

[13] J. H. Park, K. H. Kim, “The Web DDoS Shelter System (WDSS) to Counter Web Application Layer DDoS Attacks,” Department of Computer Science Graduate School Korea National Open University, 2014.

박 재 형

e-mail : earstec@gmail.com

2008년 서울대학교 전기공학부(학사)

2014년 한국방송통신대학교 정보과학과(이학석사)

2010년~2013년 KT 네트워크관제센터

2013년~2014년 KT 경제경영연구소

2014년~현 재 KT 컨설팅지원단

김 강 현

e-mail : khkim@knou.ac.kr

1983년 고려대학교 수학교육과(학사)

1985년 고려대학교 전산학(이학석사)

1989년 고려대학교 전산학(이학박사)

1987년~1989년 대전공업대학 전산학과 조교수

1990년~현 재 한국방송통신대학교 컴퓨터과학과 교수