Proxy Server Group과 Dynamic DNS를 이용한 DDoS 방어 구축 방안★

신상일* · 김민수* · 이동휘**

요 약

본 연구는 DDoS(Distributed Denial of Service, 분산 서비스 거부) 공격에 대하여 기존의 방어 전략의 한계가 드러나고 있는 시점에서, 공격력을 감소시키고 공격대상을 분산시키는 DDoS 공격 방어 구축 방안을 제시하였다.

현재 DDoS 공격은 개인·기업·연구소·대학·주요 포털 사이트·금융기관 등으로 그 목표와 범위가 광범위해지는 특징을 지니고 있다. 또한 공격 양상도 네트워크 대역인 Layer 3를 소진하는 공격기법에서 웹 어플리케이션인 Layer 7을 주목표로 공격이 변화하고 있다.

이러한 DDoS 공격에 대하여 Proxy Server Group과 Dynamic DNS를 이용한 DDoS 공격을 효율적으로 분산·감소시키기 위한 구축방안을 제시하였다.

Method of Preventing DDoS Using Proxy Server Group and Dynamic DNS

Sang Il Shin* · Min Su Kim* · DongHwi Lee**

ABSTRACT

As the existing strategy of preventing DDoS(Distributed Denial of Service) attacks has limitations, this study is intended to suggest the more effective method of preventing DDoS attacks which reduces attack power and distributes attack targets.

Currently, DDoS attacks have a wide range of targets such as individuals, businesses, labs, universities, major portal sites and financial institutions. In addition, types of attacks change from exhausting layer 3, network band to primarily targeting layer 7.

In response to DDoS attacks, this study suggests how to distribute and decrease DDoS threats effectively and efficiently using Proxy Server Group and Dynamic DNS.

Key words : DDoS, Proxy, Reverse Proxy Server Group, DNS, Dynamic DNS,

접수일(2012년 12월 3일), 수정일(1차: 2012년 12월 14일), 게재확정일(2012년 12월 24일)

★ 본 연구는 지식경제부 산업기술보호특화센터 지원으로 수행되었음.

* 경기대학교 산업보안학과

** 경기대학교 산업보안학과(교신저자)

1. 서 론

DDoS(Distributed Denial of Service, 분산 서비스 거부) 공격은 공격자가 다수의 PC에 악성코드를 감염시켜, 공격자의 지시에 따라 대량의 유해 트래픽을 특정 사이트나 시스템에 전송하여 정상적인 서비스를 방해하는 좀비PC활용 공격기법이다.

기존의 DDoS 공격이 주로 공공기관과 주요 포털 사이트, 금융권을 대상으로 이루어 졌지만, 현재의 DDoS 공격은 개인·기업·연구소·대학 등 거의 모든 사이트가 공격 대상으로 목표와 범위가 광범위해지는 특징을 갖고 있다.

또한 공격 양상도 네트워크 대역인 Layer 3를 소진하는 공격기법에서 웹 어플리케이션인 Layer 7을 주 목표로 공격이 변화하고 있다.

이로 인하여 전문적인 지식이나 장비 없이도 DDoS 공격 대행업체에 비용을 지불하여 공격을 수행할 수 있는 DDoS 공격서비스를 제공하는 산업으로도 발전하고 있다.

이러한 DDoS 공격은 다른 네트워크 해킹과 마찬가지로 근본적으로 TCP/IP의 3-Way Handshaking의 취약점을 기반으로 하고 있기 때문에, 기존의 네트워크 통신 프로토콜을 보완 또는 대처하지 않는 한 근본적으로 해결하기 어렵다.

하지만 기존의 방어 전략의 한계가 드러나고 있는 시점에서 공격력을 감소시키고 공격대상을 분산시키는 DDoS 공격 방어가 최선의 대응책일 것이다.

따라서 본 논문에서는 기존의 방어 방법과 더불어 새로운 방어방법인 Proxy 서버와 DDNS(Dynamic DNS)를 이용한 DDoS 공격을 효과적으로 방어할 수 있는 방안을 제시하고자 한다.

2. 관련연구

본 장에서는 기존의 DDoS 공격의 방어 기법을 알아보고 본 논문에서 제시한 DDos 방어 기법인 Proxy 서버와 DNS 공격유형 및 방어에 대하여 살펴보고자 한다.

2.1 DDoS 공격 및 방어

2.1.1 DDoS 공격 기술

DDoS 공격의 유형을 살펴보면 Flooding 공격, Connection 기반 공격, Application 기반 공격 유형으로 구분할 수 있다.

기존의 공격유형이 동일한 공격기법을 지속적으로 발생하는 것과 달리 발전된 공격유형은 Syn, UDP, ICMP, HTTP Flooding 공격과 웹 어플리케이션의 과부하를 동시에 공격하는 등의 다양한 공격이 발생하는 사례가 늘고 있다[1][2][3][4].

2.1.2 DDoS 공격 탐지 및 차단

DDoS 공격을 탐지할 수 있는 방법은 기존의 IDS/IPS, 방화벽 등을 활용하는 방법이나 DDoS 전용 대응시스템이나 망 차원의 Netflow, MRTG(Multi Router Traffic Grapher) 등을 이용하는 방법이 있다[5]. 또한, 웹 서비스 사용자 page 이동경로에 따른 분류, 허용된 사용자에 한해 웹 서비스 접속을 허용하는 Admission Control을 통한 대응 방안 등이 제안되고 있다[6][7].

2.2 Proxy 서버

Proxy 서버는 자신을 통해 컴퓨터나 네트워크가 다른 네트워크나 컴퓨터에 간접적으로 접속할 수 있게 함으로써, 접속을 시도한 클라이언트와 최종 접속된 서버 사이에 중계역할을 수행하는 기능을 갖는다[8]. 즉, 사용자의 접속정보를 프록시 캐시(Proxy Cache)에 일시 보관하고 여러 사용자가 이를 공유하여 망의 부하와 웹서버의 부하를 감소시키는 역할을 하며, 동시에 사용자에 대한 서비스 속도를 개선하는 기능을 제공할 뿐만 아니라, 제한적인 대역폭을 갖는 구간에서 인증서버 역할을 대신하여 인증을 해주는 역할을 하고 있다[9].

2.3 DNS 공격유형

DNS에 대한 공격 유형은 크게 4가지로 네임 서버의 침입, 네임서버에 대한 서비스 거부 공격, DNS 스

푸핑 공격, 내부 네트워크의 정보 유출로 분류할 수 있고[10], 공격 형태 또한 변화하고 있다[11]. 이러한 DNS의 취약점을 해결하기 위해 DNS에 대한 보안 확장인 DNSSEC(DNS Security Extensions)의 개념이 제시되었다[12][13].

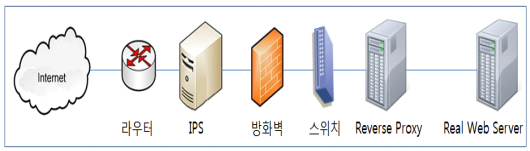
3. 제안하는 방법

DDoS 공격을 위해서는 공격 대상과 공격 지속 시간이라는 두 가지 요소가 반드시 필요하다. 해커는 공격 대상의 IP, 도메인 네임 등의 정보를 사전에 수집하여 공격 시 IP, 도메인 네임 또는 두 가지 모두를 지정하여 공격할 수 있다.

3.1 Reverse Proxy Group를 이용한 DDoS 방어

Reverse Proxy는 실 서버 앞에 위치하여 마치 실 서버처럼 동작하므로 사용자와 공격자는 실 서버의 중요한 정보(O/S, 시스템 자원, IP 주소 등)를 알 수 없으며 Reverse Proxy를 실 서버로 착각하게 된다.

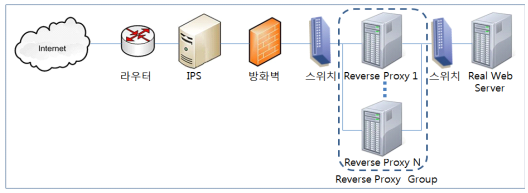
(그림 1)은 Reverse Proxy를 이용한 DDoS 방어의 일반적 시스템 구조이다.



(그림 1) Reverse Proxy를 이용한 DDoS방어

Reverse Proxy를 사용하는 이유는 공격자가 공격을 감행하더라도 모든 공격은 프락시 서버가 받게 되어 프락시 서버가 다운되더라도 실 서버는 공격에 직접 노출되지 않기 때문에 시스템 구성 정보만 변경하면 언제든지 즉각적인 서비스가 가능하다.

(그림 2)는 이러한 Reverse Proxy 서버를 Group화하여 구성한 시스템 구조이다.



(그림 2) Reverse Proxy Group를 이용한 DDoS방어

3.2 DDNS를 이용한 DDoS 방어

DDNS의 원래 목적은 유동 IP의 지원과 실시간으로 DNS 정보를 수정하고 확산시키는데 있지만, 이런 기능을 DDoS 방어의 목적으로도 사용할 수 있다.

즉, DDoS 공격 중에 공격 대상의 IP가 변경된다면 공격 패킷은 목적지를 잃어버리고 네트워크를 떠돌다가 TTL(Time To Live)값이 0으로 변하는 순간 네트워크 장비에 의해 폐기될 것이고 이를 인지하지 못한 공격자는 공격을 계속하게 되고, 인지를 한 공격자는 공격 툴을 재 구동 해야만 될 것이다.

DDNS는 DNS 정보(도메인, IP 등)를 도메인 소유자가 네트워크를 통해 직접 변경할 수 있으므로, 공격받는 중에 IP를 변경하거나 일정주기로 IP가 자동으로 변경되도록 하여 공격자의 공격을 차단할 수 있다.

3.3 Reverse Proxy Group 와 DDNS를 사용한 DDoS 방어

Web 서비스 환경에서 Reverse Proxy Group과 DDNS를 사용하여 DDoS를 방어할 수 있는 모델을 제한하고자 하며 서비스 제공 형태 및 각자의 시스템 환경에 따라 변경 될 수도 있을 것이다.

제안된 구성에서 사용되는 용어는 다음과 같다.

- RP *N* : Reverse Proxy 번호 (예: RP 1 = Reverse Proxy 1)
- Active : DDNS에 의해 변경된 IP를 소유한 Reverse Proxy (실 서버 앞에서 서비스를 중개)
- 각각의 Reverse Proxy는 모두 고유한 IP를 가지고 있으며 어떠한 경우에도 중복되지 않는다.

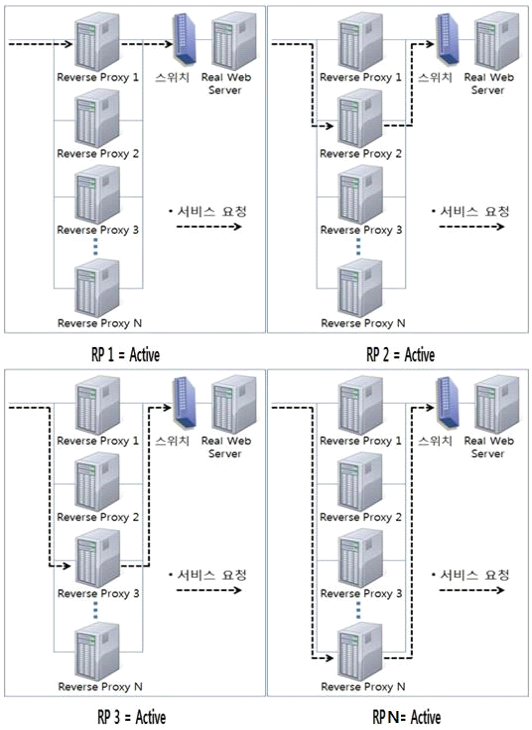
3.3.1 DDNS를 이용한 Active 변경

(그림 3)은 DDNS가 일정 주기로 도메인 네임에

대응하는 IP를 변경시켜 주므로, 그에 따라 Active가 변경되며 Reverse Proxy N까지 도달하면 다음은 다시 Reverse Proxy 1부터 재 시작되는 순환구조이다.

만약 공격자가가 IP 변경 패턴(보유한 IP 수, 변경 순서, 변경 주기) 등의 사전 정보를 수집할 수 있으므로 무작위로 변경할 수 있다.

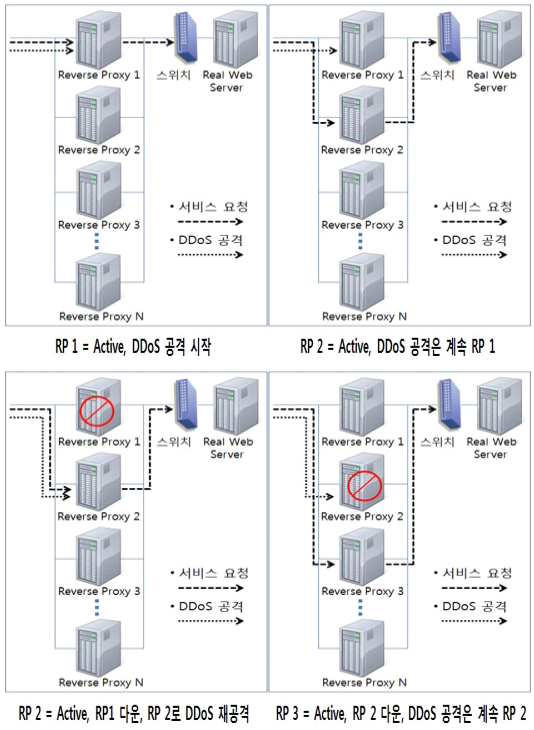
또한, Reverse Proxy Group에 속한 Reverse Proxy의 수가 적을 경우 순차적, 무작위 방법 모두 공격자의 사전 정보 수집을 차단하기 위해 주기적으로 Reverse Proxy Group에 속한 모든 Reverse Proxy의 IP를 변경할 수 있다.



(그림 3) DDNS를 이용한 순차적 Active

3.3.2 DDNS 이용 System에 대한 DDoS 공격

(그림 4)는 제안된 Reverse Proxy Group와 DDNS 이용 시스템에 대한 DDoS 공격이 발생한 경우로, 서비스 관리자가 설정한 주기로 도메인 네임에 대응하는 IP가 DDNS에 의해 자동 변경하여 서비스 마비를 차단하게 해준다.



(그림 4) DDNS 이용 System에 대한 DDos 공격

4. 비교 검증

본 논문에서 제안된 Reverse proxy Server Group을 5개로 구성한 시스템과 일반적으로 Reverse Proxy Server Group을 1개로 구성된 시스템을 비교 검증하였다.

검증을 위하여 DDoS 공격은 Breaking Point를 사용하였고, 공격 시간은 각 10분에 제안된 시스템에는 Active = 5분으로 IP 변경을 제한하였다.

<표 1>은 두 시스템 구성간의 비교를 나타낸 것이다. 두 시스템의 구성에 DDoS 공격 시간을 10분으로 하였으나 일반적인 시스템 구조에서는 2분 23초만에 서비스가 정지하여, 76.16%의 공격 성공률을 보였다.

반면 제안된 시스템 구조에서는 동일한 조건에서 Reverse Proxy Server Group이 공격을 방어하여 실 Server가 정상 작동 하였고, Reverse Proxy Server Group의 Server 시스템 1개가 정지하여 Active = 5분

으로 하였을 경우, 26.16%의 공격 성공률을 보였다.

<표 1> 시스템 간 비교 분석

	일반적인 구조	제안된 구조
공격 시간	10분	10분
공격 지속시간	2분 23초	10분
서비스 다운시간	7분 37초	2분 37초
Active 주기	-	5분
System 상태	실 Server 정지	Proxy Server 1대 정지
공격 성공률	76.16%	26.16%

5. 결 론

본 논문은 DDoS 공격의 범위 및 형태가 발전함에 따라 체계적인 방어 방법과 대응 방안을 제시하고자, Reverse Proxy Group과 DDNS를 이용한 DDoS 방어 구축 방안에 대하여 연구하였다.

이를 위하여 일반적인 Reverse Proxy System과 제안된 Reverse Proxy Group System을 구성하였고, 제안된 System은 DDNS를 활용하여 Active = 5분으로 IP 변경값을 넣어 구성하였다.

두 시스템을 비교한 결과 일반적인 시스템은 2분 23초만에 실 Server가 정지하여 76.16%의 공격 성공률을 나타냈다.

반면, 제안된 시스템에서는 실 Server가 정상적으로 운영되고, Proxy Server 1대가 정지하여 26.16%의 공격 성공률이 나타났다.

결국, 제안된 시스템의 RP의 개수에 따라 공격 방어율이 달라 질수 있음을 알 수 있다.

하지만 제안된 구축 방안은 방어 장비를 대신하는 것이 아니기 때문에 네트워크 대역인 Layer 3의 소진성 공격을 받는다면 서버의 동작 여부와 상관없이 서비스가 마비될 것이다.

이를 위하여 최소한의 방어 장비를 구축하여 1차적인 방어를 하여야 한다.

따라서, 방어 장비의 구축과 전략을 잘 세운다면 DDoS 공격을 감소시키거나 분산시켜 효율적인 방어를 할 수 있을 것이다.

참고문헌

[1] Jelena Mirkovic, “D-WARD : Source-End Defense Against Distributed Denial-of Service-Attacks”, Ph. D. Dissertation, Computer Science, UCLA, 2003.

[2] jelena Mirkovic and peter Reiher, “A Taxonomy of DDoS Attack and DDoS Defence Mechanisms”, ACM SIGCOMM Computer Communication Review, pp.32-39, 2004.

[3] 서진원 외, “다단계 방어기법을 활용한 DDoS 방어시스템 설계”, 한국정보보호학회, Vol.22, No.3, p.681, 2012.

[4] 구자현, “서비스 거부 공격(Denial of Service)의 유형 및 대응”, 주간기술동향, 1377호, p.6, 2008.

[5] 김태원 외, “패킷 카운팅을 이용한 DoS/DDoS 공격 탐지 알고리즘 및 이를 이용한 시스템”, 한국시뮬레이션학회, Vol.19, No.4, pp.153-154, 2010.

[6] Takeshi Yatagai, “Detection of HTTP GET Flood Attack Based on Analysis of Page Access Behavior”, PACRIM, pp.232-235, 2007

[7] M. Srivatsa et al, “Mitigating Application Level Denial of Service Attacks on Web Servers”, ACM Transactions on WEB, Vol.2 Issue.3, 2008.

[8] 강신범 외, “프록시 서비스를 통한 범죄 위협과 프라이버시 보호에 관한 연구”, 정보보호학회, Vol.22, No.2, pp.318-319, 2012.

[9] 임차성 외, “SSL MITM 프록시 공격에 대한 효과적 방어방법”, 한국정보과학회, Vol.16, No.6, pp.693-694, 2010.

[10] A. Householder, B. King, “Securing an Internet name Server”, CERT Coordination Center, 2002.

[11] 전용희 외, “DDoS 공격 및 대응 기법 분류”, 정보보호학회, Vol.19, No.3, pp.46-57, 2009.
[12] 김학주 외, “도메인네임시스템의 취약점 분석과 보안 확장(DNSSEC)”, 한국통신학회, Vol.20, No. 7, pp.18-19, 2003.
[13] D. Eastlake, “Domain Name System Security Extension”, RFC 2535, 1999.

[저 자 소 개]

신 상 일 (Sang-Il Shin)

2004년 컴퓨터공학사
2007년 컴퓨터공학석사
2011년 현재 경기대학교
산업보안학과 박사과정

email : sishin69@hanmail.net

김 민 수 (Min-Su Kim)

2004년 컴퓨터공학사
2012년 경호안전학석사
2012년 현재 경기대학교
산업보안학과 박사과정

email : fortcom@hanmail.net

이 동 휘(DongHwi Lee)

2000년 경기대학교 컴퓨터과학과
(이학사)
2003년 경기대학교
정보보호기술공학과
(공학석사)
2006년 경기대학교 정보보호학과
(정보보호학박사)
2011년~2012년 5월 University of Colorado Denver, Dept. of Computer Science and Engineering
현재 경기대학교 산업보안학과

email : dhclub@naver.com