이중 방화벽과 다중 필터링을 이용한 DDoS 차단 시스템★

조지호* · 신지용* · 이 극**

요 약

본 논문에서는 DDoS 탐지를 위해 기존의 이중 방화벽에 다중 필터링 방법을 적용한다. 1차 방화벽에서는 외부에서 유입되는 패킷 경로를 분석하여 R-PA(Router Path Anlaysis) 패킷 필터링 알고리즘과 엄격한 홉 카운터 필터링을 적용한다. 2차 방화벽에서는 1차 방화벽을 거쳐서 온 패킷의 데이터를 검사하여 정상적인 패킷과 비정상적인 패킷을 구분하고, 패킷 트래픽이 사용자에게 할당 된 임계치를 초과하는지를 검사하여 DDoS 공격을 차단한다.

DDoS Prevention System Using Double Firewall and Multi-Filtering Method

jiHo Cho* · Jiyong Shin* · Geuk Lee**

ABSTRACT

This paper proposes multi-filtering method on the double firewall to prevent DDoS attack. In the first firewall, R-PA filtering algorithm and rigid hop counter filtering method are applied by analyzing packet paths. In the second firewall, packets are examined to be distinguished abnormal from normal packets. Security policy system monitors each user sessions and if the traffic is over the threshold value, the system blocks that session for an assigned time.

Key words : DDoS, Double Firewall, Packet Filtering

접수일(2014년 3월 20일), 수정일(1차: 2014년 3월 27일), 게재확정일(2014년 3월 28일)

★ 이 논문은 2013년 한남대학교 학술연구조성비 지원에 의하여 연구되었음.

* 한남대학교 컴퓨터공학과
** 한남대학교 컴퓨터공학과 (교신저자)

1. 서 론

최근 인프라 공격(infrastructure attack)이 빠르게 증가하고 있다. 인프라 공격은 인터넷의 인프라를 소모시켜 정상 사용자들이 이용할 수 없도록 만드는 공격 형태이다. 이러한 공격의 예로는 분산 서비스 거부 공격, 슬래머 웜(slammer worm), DNS 캐쉬 중독(DNS cache poisoning) 등이 있다.[1] 분산 서비스 거부 공격은 웹서버, 라우터, DNS 서버 같은 중요한 서비스를 모두 소모해서 정상 사용자가 이용할 수 없도록 만드는 공격 형태이다. 대부분의 분산 서비스 거부 공격 전략은 다수의 분산 공격 에이전트들이 동시에 대상 시스템을 공격하여 대상 시스템의 제한된 리소스를 모두 소모하게 한다.[2]

지난 3년 사이 DDoS(Distributed Denial of Service, 분산서비스 거부) 공격률이 약 20배 정도 증가했고 국내에서는 다수 웹 사이트를 목표한 DDoS 공격이 매년 빈번하게 발생하고 있다. DDoS공격이 점점 다양화 되고 지능화가 되어 DDoS공격의 분석과 추적이 어려워지고 있다. 이에 따라 DDoS공격 방어책에 대한 중요성이 점차 부각되고 있으며 이중 방화벽을 통한 DDoS공격 차단방법도 연구되고 있는 방법 중 하나이다.

앞으로 지속적으로 다양한 패턴의 DDoS공격 유형이 나타날 것으로 예상되며, 본 논문에서는 이러한 DDoS 공격의 유형을 효과 적으로 차단하고 탐지할 수 있는 기법을 제안한다. 제안된 방법은 이중 방화벽을 이용하며, 1차 방화벽에서는 외부에서 유입되는 패킷들의 공격 가능성을 판별하는 하여 보다 견고한 패킷 필터링을 한다. 2차 방화벽에서는 1차 방화벽을 거쳐서 온 패킷의 데이터를 검사하여 정상적인 패킷과 비정상적인 패킷을 구분하고 패킷이 트래픽을 초과하고 있는지, 한 사용자가 임계치를 초과하는지를 검사하여 패킷을 정상적으로 통과시킬지 혹은 제거할지를 판단한다.

2. 관련연구

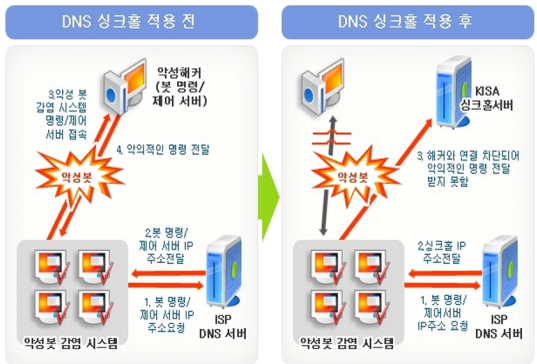
2.1 ACL

네트워크 장비에서 사용하는 가장 일반적인 유해 트래픽 차단 기술이다. IP주소, 서비스 포트 그리고 컨텐츠를 기반으로 한 차단이 가능하지만 이 방법은 접근통제를 위한 별도의 ASIC화된 모듈이 없을 경우 네트워크 장비에 많은 부담을 주어 성능저하의 원인이 된다.[3] 또한 많은 네트워크 장비를 보유하고 있는 기관의 경우, 이들 장비들에 접근통제 정책을 업데이트하기 위해서 별도의 스크립트를 작성하거나, 그렇지 않은 경우 개별적으로 로그인하여 설정을 변경하여야 하는 어려움이 있다.

2.2 DNS 싱크홀

악성봇에 감염된 컴퓨터가 C&C 서버 로 접속하려는 연결시도를 사전에 차단함으로써 DDoS 공격이나 개인정보 유출 등의 악의적 행위 수행을 사전에 방지하는 시스템이다. C&C 서버나 다운로드 사이트의 도메인 이름을 알고 있는 경우 좀비 PC의 DNS 질의에 대한 응답을 조정하여 C&C 서버로 접속할 시 DNS 싱크홀 서버로 우회시켜 공격 명령을 차단하는 기법이다. 좀비 PC가 DNS로 C&C의 주소 정보를 질의하면 DNS 서버에 저장된 싱크홀 서버의 주소를 대신 전달하여 C&C와의 연결을 차단할 수 있다. 이처럼 DNS 싱크홀을 이용하면 봇에 감염된 가입자 PC의 정보를 획득할 수 있으며, 효과적으로 C&C 서버와 봇의 연결을 차단하는 동시에 행위를 모니터링할 수 있다.

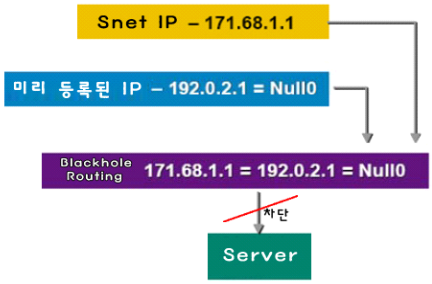
DNS싱크홀은 개인 사용자가 악성도메인으로 접근하는 것을 싱크홀 서버로 우회시킨다.



(그림 1) DNS 싱크홀 동작원리

2.3 블랙홀 라우팅(Blackhole Routing)

라우터에서 대상 서버의 IP로 전송되는 모든 트래픽을 차단한 후 블랙홀이라고 하는 일종의 폐기 장소로 보내서 소멸시키는 기법이다. 사전에 미리 등록된 IP로 전송되는 패킷을 Null 0로 설정해 놓으면 결과적으로 해당 목적지로 가는 트래픽을 차단한다. 등록된 IP로 전송되는 패킷을 Null 0라는 가상 인터페이스로 전송하여 제거하기 때문에 Null 0라우팅 또는 Null 0 필터링 이라고도 한다.[4]



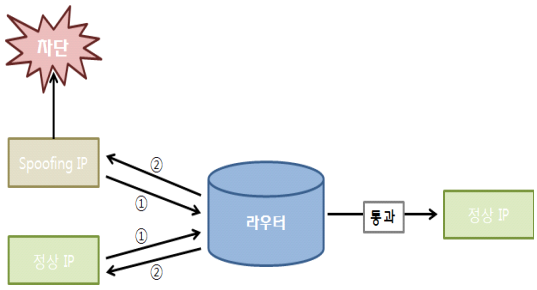
(그림 2) 블랙홀 라우팅(Blackhole Routing)

2.4 uRPF(unicast Reverse Path Forwarding)

출발지 IP 주소를 위장한 IP 스프핑(Spoofing) 공격을 차단해 줄 수 있는 기술로서, 라우터가 패킷을 받으면 출발지 IP 주소를 확인하여 해당 IP로 갈수 있는 역경로가 존재하는지 확인함으로써 출발지 IP주소를 신뢰 할 수 있다.

라우터로 패킷이 들어올 때 패킷의 입력 인터페이스로의 역경로가 존재하는 확인하여 만약 역경로가 존재하면 통과 시킨다. 존재하지 않으면 그 패킷은 출발지 IP 주소가 위조된 패킷으로 판단하여 제거한다.[5]

DDoS공격이 자신의 출발지 주소를 위장하므로 uRPF는 상당히 효과적인 서비스 거부 공격 차단 방법이 될 수 있다. 하지만 이 기술 역시 다수의 라우팅 경로가 존재하는 비대칭 망구조를 가지고 있을 경우 적용의 한계가 있으며, 스푸핑을 방지하는 것 이외에 다양한 DDoS공격에 대한 대응 기능이 없다는 단점이 있다.[4]



(그림 3) uRPF(unicast Reverse Path Forwarding)

2.5 기존 DDoS 방어시스템의 구성과 문제점

2.5.1 기존 DDoS 방어시스템의 구성

기존의 DDoS 방어시스템은 OIS 7계층의 3계층, 4계층, 7계층에 대한 고대역 DDoS공격 방어가 가능하도록 구성되어 있다. 고대역 DDoS 공격의 탐지를 위해 방어시스템에 보안정책을 설정하여 정해진 범위를 넘어서는 과도한 트래픽이 발행하는 경우 DDoS로 탐지 하도록 하고 있다. 정해진 시간동안에 임계치를 초과하면 이를 인지하도록 하는 대역폭 제한(Traffic Rate Limit) 정책을 통해 대규모로 발생되는 플루딩(Flooding) 공격을 탐지 하고 모든 패킷의 데이터 부분까지 검사하여 유해성 여부를 검사 할 수 있도록 구성되어 있다. 또한 들어오는 모든 패킷을 분석하고 처리하여야 하는 부담을 줄이기 위해 특정 IP에서의 공격빈도를 파악하여 공격자 또는 좀비 PC로 인지된 경우 블랙리스트에 등록하고 패킷을 제거하도록 하여 패킷처리에 대한 성능 향상을 꾀하고 있다.

2.5.2 기존 DDoS 공격 대응 방안 문제점

기존의 DDoS 방어시스템들은 DDoS대응 방안을 기반으로 하여 개발되어진 시스템으로 고대역 DDoS 공격에 초점이 맞추어져 있어 저대역 DDoS공격에 대한 대응 방안이 없다. 공격으로 탐지된 IP 및 서비스 포트에 대해 패킷의 제거 기능만 지원한다. 고대역 DDoS 공격 경우 특정상 공격 IP의 대부분이 무작위로 위조된 IP를 사용하게 되는데, 이때 방어시스템에 의해 탐지된 IP의 블랙리스트 등록과 제거(drop)로 인해 정상적인 IP를 사용하고 있는 사용자의 서비스 요청

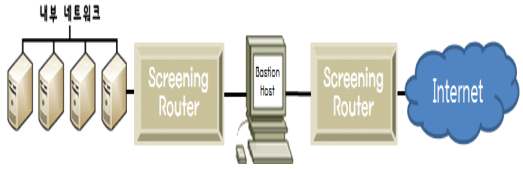
도 같이 제거되는 문제점이 존재한다. 또한 일시적인 네트워크 장애에 의한 패킷의 비정상 전송으로 인해 7계층에서 DDoS로 판단되는 경우에도 동일한 문제점으로 인해 정상적인 서비스를 받을 수 없게 된다.[6]

3. 이중 방화벽과 다중 필터링

3.1 이중 방화벽

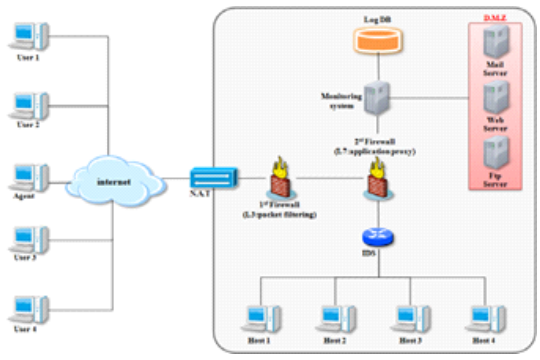
일반적인 이중 방화벽은 인터넷과 내부 네트워크를 스크린 된 게이트웨이를 통해서 연결하며, 스크린 된 서브네트에는 방화벽 시스템이 설치되어 있다. 인터넷과 스크린 된 서브네트 사이 그리고 서브네트와 내부 네트워크 사이에는 스크리닝 라우터를 사용한다.

스크리닝 라우터는 인터넷과 스크린 된 서브네트 그리고 내부 네트워크와 스크린 된 서브네트 사이에 각각 놓이며, 입출력되는 패킷 트래픽을 패킷 필터 규칙을 이용하여 필터링하게 되며, 스크린 된 서브네트에 설치된 베스천 호스트는 프락시 서버(응용 게이트웨이)를 이용하여 명확히 진입이 허용되지 않은 모든 트래픽을 거절하는 기능을 수행한다. 이러한 구성에서 스크린 된 서브네트에 대한 액세스는 베스천 호스트를 통해서만 가능하기 때문에 침입자가 스크린 된 서브네트를 통과하는 것은 어렵다.[7] 만약 인터넷을 통해 내부 네트워크로 침입하려고 한다면 침입자는 자기가 자유롭게 내부 네트워크를 액세스할 수 있도록 인터넷, 스크린 된 서브네트 그리고 내부 네트워크의 라우팅 테이블을 재구성해야만 가능하다. 그러나 스크리닝 라우터가 존재하기 때문에 이는 힘들다. 비록 베스천 호스트가 침해되었더라도 침입자는 내부 네트워크상에 존재하는 호스트로 침입해야 하고, 그리고 스크린 된 서브네트를 액세스하기 위해서 스크리닝 라우터를 통과해야 한다.



(그림 4) 이중 방화벽

3.2 시스템 구조



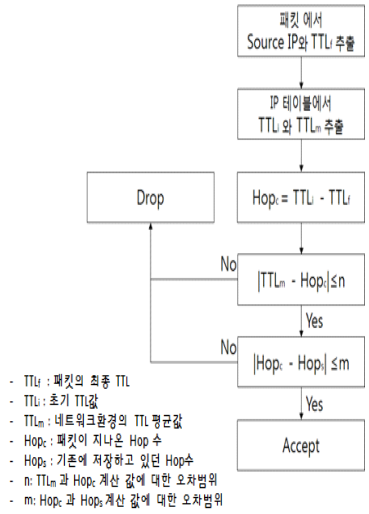
(그림 5) 이중 방화벽 구조

(그림 5)는 본 논문에서 사용하는 이중방화벽 구조이다. 이 구조는 이미 제안된 시스템이다.[8] 내 외부와의 격리상태를 논리적으로 구분하기 위해 NAT(Network Address Translation)를 사용한다.

1차 방화벽에서는 패킷들을 2단계로 나누어 작업을 한다. 먼저 패킷이 라우터를 지나오면서 경로 정보를 이용해 패킷을 구분한다. 그리고 스푸핑 된 소스IP를 가지고 들어오는 패킷은 원래의 소스 IP의 홉 카운트 값과 다르면 스푸핑 된 패킷은 제거된다.[8] 기존의 패킷 필터링에 경로명(Path Identification)을 적용하여 보다 엄격한 패킷 필터링인 R-PA(Router Path Analysis) 패킷 필터링 방법을 사용한다.[11]

3.2.1 홉 카운터를 이용한 패킷 필터링

스푸핑된 IP 패킷은 희생자에게 도착하였을 때, 원래의 IP 주소의 홉 카운트(Hop Count) 값을 가지고 있기 때문에 IP 패킷이 스푸핑된 패킷인지 정상 패킷인진 가능하다.



(그림 6) 엄격한 HCF

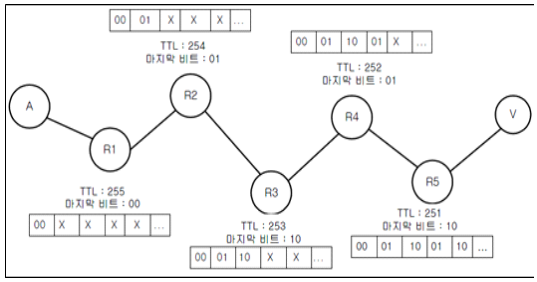
라우터 경로 분석을 통해 패킷 필터링을 한 후 다시 TTL(Time to Live)값을 이용하여 필터링을 한번 더한다. 기존의 각 IP에 대한 패킷 정보를 가지고 있어야 하고 이로 인해 필터링 과정이 지연 되는 문제점을 보안하기 위해 이전의 TTL의 활동을 근거로 하여 통계적으로 분석하여 계산된 평균값 사용(TTLm)한다.

1차 필터링된 패킷이 들어오면 Source IP와 마지막 TTL값을 추출한다. 그다음 기존의 초기 TTL값과 TTL 평균값을 IP 테이블에서 정보를 가지고 온다. 테이블 정보의 초기 TTL 값과 패킷의 마지막 TTL 값을 가지고 패킷이 지나온 홉 카운트를 계산을 하고 그 계산된 값은 평균 TTL 값과 비교를 통해 정상 패킷 여부를 판단한다. 통과되면 마지막으로 패킷이 지나온 홉 카운트와 기존에 저장되어 있던 홉 카운트를 비교하여 정상 패킷 여부를 판단한다.[9][10] 이때 평균 TTL 값과 패킷이 지나온 홉 카운트를 계산 한 값과 그리고 패킷이 자나온 홉 카운트 값과 기존의 저장되어 있던 홉 카운트를 계산 한 값에 대한 오차범위가 존재한다.

3.2.2 경로 분석을 이용한 패킷 필터링

3.2.2.1 라우터 경로 분석

패킷이 지나온 라우터의 경로가 같으면 같은 경로명 값을 갖는다. 경로명 값은 라우터를 지나오면서 패킷 마킹을 통해 이루어진다. 패킷이 라우터에 도착했을 때, 라우터는 IP의 마지막 n비트를 패킷의 16비트 ID 필드에 TTL(Time to Live) 값을 계산한 위치의 비트열에 마킹을 한다. 이렇게 마킹 된 값들은 패킷이 지나온 경로에 따라 다른 값을 갖기에 공격자가 IP를 위조하여도 경로명 값을 보고 구별할 수 있다. 이걸 이용해서 피해 호스트(V)는 공격 패킷의 블랙리스트를 만들어 피해 호스트로 들어오는 공격 패킷을 경로명 값을 가지고 필터링을 할 수 있다.[11]



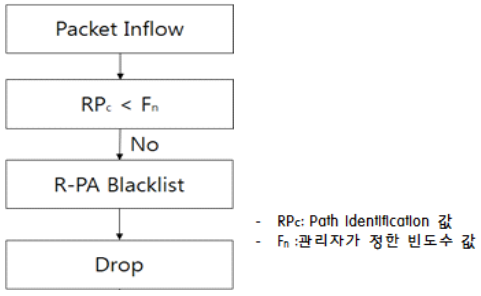
(그림 7) 라우터 경로 분석

공격자(A), 피해자(V) 그리고 중간의 라우터들(R)로 구성되어 있다. 기본적인 마킹 방법은 라우터들이 그들이 전송하는 패킷의 IP명 필드(IP Identification Field)에 라우터 IP주소의 마지막 n비트를 표시를 한다. 경로명을 표시를 할 위치를 정하기 위해서는 16비트를 n개의 섹션으로 나누고(16/n) 인덱스로 패킷의 TTL 값을 이용한다.(TTL mod [16/n]) 표시 할 위치에 라우터들은 자신의 IP주소를 이용하여 만들어낸 n비트를 삽입하게 된다. 피해자는 이 경로 명값을 비교하여 공격패킷을 차단하게 된다.[12] 경로 명 기법은 매우 단순하게 설계되어 있어서 중간 라우터들에 게 큰 오버헤드(overhead)를 주지 않으며, 상위 라우터들의 도움 없이 피해자가 직접적이며 즉각적인 필터링이 가능하다는 장점이 있다.

공격자는 같은 경로의 경로 명 마킹 값을 여러 개의 마킹 값으로 바꾸기 위해 초기 TTL 값을 변경할 수 있다. 이에 대응하기 위해 피해 호스트는 TTL 값을 검사해서 패킷 내의 가장 오래된 마킹 위치를 찾을 수 있고, 이 위치를 기준으로 나머지 값들을 회전시켜서 다른 TTL 값에 대해 고유한 경로 명 마킹 값

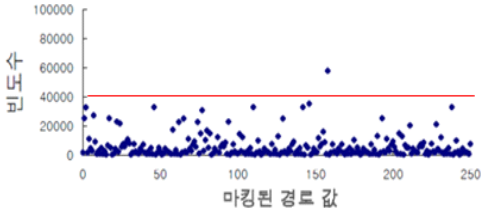
을 얻을 수 있다.

3.2.2.2 R-PA(Router Path Analysis) 패킷 필터링 기법



(그림 8) 라우터 경로 분석을 이용한 패킷 필터링

모든 네트워크 경로를 공격 경로와 정상 경로로 구분하고 공격 경로로 부터 오는 패킷을 필터링하는 것이다. 공격 경로와 정상 경로를 구별 할 수 있는 기준은 트래픽 양이다. 즉, 자주 발생하는 마킹 값을 포함하는 패킷을 탐지하는 것이다. 패킷이 들어오면 경로 명값의 빈도수를 측정하여 자주 발생하는 마킹 값을 찾아내고 관리자가 정한 필터링 값 이상이면 해당 패킷은 제거된다.[11][12]

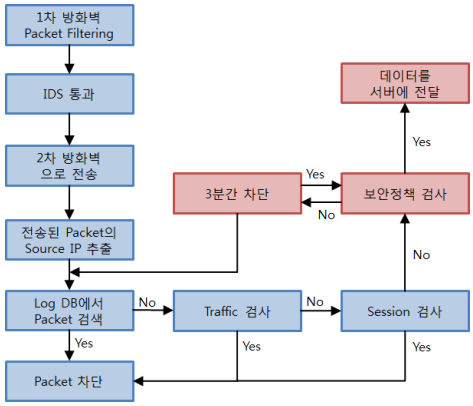


(그림 9) 마킹 빈도수 측정

의심 패킷에 대해서는 나중에 또 들어오는 것을 방지하기 위해 R-PA 블랙리스트(Blacklist)에 추가한 뒤 제거한다.

3.2.3 2차방화벽과 트래픽 감시

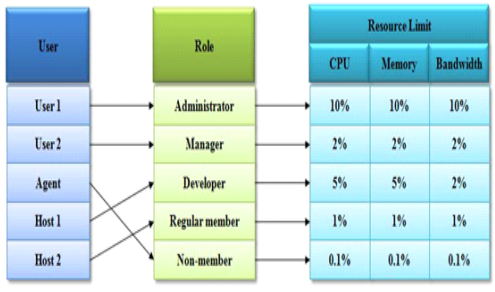
2차 방화벽에서는 7계층 방화벽으로 1차 방화벽에서 온 패킷과 IDS를 지나온 패킷들의 데이터를 검사하여 패킷을 구분 한다. 패킷이 트래픽을 초과하고 있는지, 한 사용자가 임계치를 초과하는지를 검사한다. 그리고 정상적으로 통과시킬지 제거할지를 결정을 통해 1차 방화벽을 거쳐서 온 패킷의 데이터를 검사하여 정상적인 패킷과 비정상적인 패킷을 구분한다. 1,2차 방화벽을 필터링 된 패킷은 모니터링 시스템으로 전송하게 된다. 모니터링 시스템은 관리자가 정한 보안정책에 따라 사용자별로 허용 가능하니 시스템 자원을 할당하고 실시간으로 탐지 및 차단, 허용을 결정한다.[9]



(그림 10) 2차 방화벽과 모니터링 시스템

3.2.4 보안정책(Security Policy)

모니터링이 참조하는 보안 정책은 기존 서버들이 감당할 수 있는 임계치를 정해 놓고 통계적으로 분석하여 설정한다. 2차 방화벽에서 사용자의 세션 수의 임계치를 확인한다. 꾸준히 보안 정책과 사용자와 서버의 활동을 비교함으로써 서버다운 및 불법적인 행동을 방지한다.[9][13]



(그림 11) 사용자별 보안정책

사용자의 역할과 역할등급에 맞는 자원 한계치에 대한 보안정책을 정하고 사용자 역할에 맞는 리소스를 사용할 수 있도록 임계치를 설정한다. 정해진 보안정책을 벗어나는 행동을 하였을 경우 1차적으로 3분간 인터럽트 상태로 남겨두고 똑같은 상황이 되풀이 될 경우 IP를 차단 한다.

4. 결 론

인터넷이 급속도로 발달되면서 DDoS 공격 또한 기존의 공격 방법을 응용하여 DDoS공격 방법이 다양화되어 가고 있다. 최근에 DDoS공격률이 증가함으로 인해 기존의 방화벽보다 좀 더 견고한 방화벽 및 대응 시스템이 요구 되고 있다. 기존의 DDoS공격탐지 기법은 일정기간동안 트래픽을 수집하고 분석하여 임계치를 설정을 했다. 하지만 기존의 DDoS공격 탐지 기법은 DDoS 공격이 발생할 경우 공격 초기에 탐지가 어려워 피해를 입거나 탐지를 하더라도 이미 피해를 입어 대응하기가 힘든 상황이 발생한다.

본 논문에서는 기존의 패킷 필터링 방법들과 이중 방화벽 기법을 차용하여 강화된 DDoS 차단 시스템을 제안한다. 1차 방화벽에서는 외부에서 유입되는 패킷들의 공격 가능성을 판별하기 위해 라우터 분석을 통해 보다 견고하고 엄격한 R-PA(Router Path Anlaysis) 패킷 필터링 방법을 결합한다. 이로 인하여 기존의 홉 카운트 필터링의 문제점인 모든 IP 주소마다 패킷에 대한 정보를 가지고 있어 하며 이로 이한 필터링이 지연되는 것을 방지 할 수 가 있다. 그리고 오탐지율도 줄일 수 있다. 2차 방화벽에서는 1차 방화벽을 거쳐서 온 패킷의 데이터를 검사하여 정상적인 패킷과 비정상적인 패킷을 구분하고 패킷이 트래픽을 초과하고 있는지, 한 사용자가 임계치를 초과하는지를 검사하여 정상적으로 통과시킬지 제거할지를 결정한다. 이렇게 1차 방화벽, 2차 방화벽을 사용하여 동시에 내·외부 패킷을 구분하여 처리함으로서 시스템 과부화를 방지할 수 있다.

참고문헌

[1] David Moore, Slammer Worm, http://www.cs.berkeley.edu/~nweaver/sapphire/.

[2] 서동민, 서버 마비시키는 좀비 공격 - 디도스(DDoS) 공격, http://it.donga.com/openstudy/4064/

[3] 이지선, 이민순, 이병수, 해킹과 보안 마스터, 이한출판사, 2004.

[4] DDoS 공격유형 및 보안장비별 대응방법, NCIA, 2010.

[5] Juan M. Estevez-Tapiador and Pedro Garcia-Teodoro and jesus E.Diaz-Verdejo, Anomaly Detection Methods in Wired Network: a Survey and Taxonomy, Computer Communication, 2004.

[6] 이형수, 저대역 DDoS 공격 대응 시스템 (Respond System for Low-Level DDoS Attack), 숭실대학교, 2011

[7] 장세덕, TCP/IP 유무선 네트워크, 대림출판사, 2005

[8] Jung-Hyo Park, Hyun-Chul Kim, Moon-Seog Jun, *"Efficient detection and defense techniques of using two firewalls and a monitoring system for DDoS attacks,"* Proceedings of KIISE(D), Vol. 36, No. 4, pp78~81, 2009.

[9] 서우석, 박대우, 전문석, *"DDoS 공격기법과 다중 방화벽 기법을 이용한 방어에 관한 연구,"* 한국컴퓨터학회 학술대회 논문집, 18권 1호, pp231~240, 2010.

[10] 안지용, 고속 패킷 필터링 알고리즘 개발 (Development of a Fast Packet Filtering Algorithm), 숭실대학교, 2002.

[11] Yonghoon Jeong, Manpyo Hong , Hongjin Yeh, *"An Efficient Implementation of Hop Count Filtering using Path Identification Mechanism,"* Proceedings of KIISE(A), Vol. 31, No. 1, pp322~324, 2004.

[11] KangSin Lee, Dynamic Path Identification Method to Defend Against DDoS Attack, Korea University, 2005.

[13] Karanjit siyank, Chris Hare, Internet Filerwalls

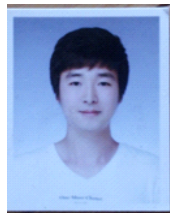
and Network Secureity, New Rider Pub. 1996.
[14] 김동수, 능력 토큰을 이용한 SYN 범람 공격 방어 프레임워크, 아주대학교, 2005.

[저 자 소 개]

조 지 호 (jiHo Cho)

2012년 한남대학교 컴퓨터공학과 학사
2014년 한남대학교 대학원
컴퓨터공학과 석사 졸업
현 재 한남대학교 대학원
컴퓨터공학과 박사과정 재학 중

email : charismaup@nate.com



신 지 용 (Jiyong Shin)

2014년 한남대학교
컴퓨터공학과 학사 졸업
현 재 한남대학교 대학원
컴퓨터공학과 석사과정
재학 중

email : shinpar90@naver.com

이 극 (Geuk Lee)

1983년 경북대학교
전자계산공학과 졸업
1986년 서울대학교
컴퓨터 공학과 석사 졸업
1993년 서울대학교
컴퓨터 공학과 박사 졸업
2003년~2012년 지경부지정RIC 민군겸용
보안공학 연구센터(SERC) 소장
1988년~현재 한남대학교
컴퓨터공학과 교수

email : leegeuk@hnu.kr