(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2009년06월03일
(11) 등록번호 10-0900491
(24) 등록일자 2009년05월26일

(51) Int. Cl.
G06F 21/00 (2006.01) *G06F 15/00* (2006.01)
H04L 12/24 (2006.01)
(21) 출원번호 10-2008-0121365
(22) 출원일자 2008년12월02일
심사청구일자 2008년12월02일
(56) 선행기술조사문헌
JP2001069169 A
KR1020030059204 A
KR1020040011123 A
JP2003067279 A
전체 청구항 수 : 총 19 항

(73) 특허권자
(주)씨디네트웍스
서울 강남구 역삼동 828-7 한동빌딩 6,7F
(72) 발명자
나원택
서울특별시 강남구 역삼동 828-7 한동빌딩 2층
백형성
서울특별시 강남구 역삼동 828-7 한동빌딩 2층
(뒷면에 계속)
(74) 대리인
반중혁

심사관 : 강윤석

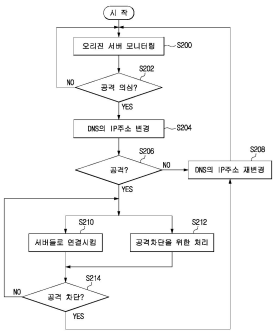
(54) 분산 서비스 거부 공격의 차단 방법 및 장치

(57) 요 약

분산 서비스 거부 공격의 차단 방법 및 장치가 개시된다. 본 발명의 바람직한 일 실시예에 따르면, 오리진 서버의 트래픽(traffic) 상태가 분산 서비스 거부 공격인지 판단하여 오리진 서버의 트래픽 상태가 분산 서비스 거부 공격으로 판단되는 경우, DNS로 오리진 서버의 IP(Internet Protocol) 주소를 복수개의 서버 중 적어도 하나로 변경하도록 요청한다.

본 발명에 따르면, 정상적인 서비스 제공 요청을 수용할 수 있으면서도 분산 서비스 거부 공격의 판단과 차단할 수 있으며, 분산 서비스 거부 공격의 판단과 차단을 위해 각 사이트나 서버들마다 분산 서비스 거부 공격의 판단과 차단을 위한 장치 등을 설치하지 않아도 되어 비용을 절감하면서도 효과적으로 분산 서비스 거부 공격의 판단과 차단이 이루어질 수 있는 장점이 있다.

대 표 도 - 도2



(72) 발명자

변춘환

서울특별시 강남구 역삼동 828-7 한동빌딩 2층

임정우

서울특별시 강남구 역삼동 828-7 한동빌딩 2층

한효수

서울특별시 강남구 역삼동 828-7 한동빌딩 6층

특허청구의 범위

청구항 1

DNS(Domain Name System), 공격 판단 장치, 복수개의 서버 및 오리진 서버(Origin server)를 포함하는 네트워크 시스템에서 상기 공격 판단 장치에 의해 수행될 수 있는 상기 오리진 서버로의 분산 서비스 거부 공격(DDoS: Distributed Denial of Service)을 차단하는 방법에 있어서,

상기 오리진 서버의 트래픽(traffic) 상태가 분산 서비스 거부 공격인지 판단하는 단계(a); 및

상기 오리진 서버의 트래픽(traffic) 상태가 분산 서비스 거부 공격으로 판단되는 경우, 상기 DNS로 상기 오리진 서버의 IP(Internet Protocol) 주소를 상기 복수개의 서버 중 적어도 하나로 변경하도록 요청하는 단계(b)를 포함하는 것을 특징으로 하는 분산 서비스 거부 공격의 차단 방법.

청구항 2

제1항에 있어서,

상기 단계(a)는 상기 오리진 서버의 트래픽(traffic) 상태를 모니터링하는 단계를 더 포함하는 것을 특징으로 하는 분산 서비스 거부 공격의 차단 방법.

청구항 3

제2항에 있어서,

상기 오리진 서버의 트래픽 상태의 모니터링은 상기 오리진 서버의 트래픽 상태가 미리 설정된 값을 초과하는지 모니터링하고,

상기 오리진 서버의 트래픽 상태가 미리 설정된 값을 초과하는 경우 상기 오리진 서버의 트래픽 상태가 분산 서비스 거부 공격인지 판단하는 것을 특징으로 하는 분산 서비스 거부 공격의 차단 방법.

청구항 4

제3항에 있어서,

상기 단계(a)에서 상기 오리진 서버의 트래픽 상태가 미리 설정된 값을 초과하는 경우 상기 오리진 서버의 트래픽 상태가 분산 서비스 거부 공격인지 판단하기 전, 상기 DNS로 상기 오리진 서버의 IP 주소를 상기 복수개의 서버 중 적어도 하나로 변경하도록 요청하는 것을 특징으로 하는 분산 서비스 거부 공격의 차단 방법.

청구항 5

제4항에 있어서,

상기 단계(b)에서 상기 오리진 서버의 트래픽 상태가 분산 서비스 거부 공격이 아닌 것으로 판단되는 경우 상기 DNS로 상기 복수개의 서버 중 적어도 하나로 변경된 IP 주소를 상기 오리진 서버의 IP 주소를 변경하도록 요청하는 것을 특징으로 하는 분산 서비스 거부 공격의 차단 방법.

청구항 6

제1항에 있어서,

상기 단계(b)는,

상기 오리진 서버의 트래픽 상태가 분산 서비스 거부 공격으로 판단되는 경우 상기 오리진 서버로의 서비스 제공 요청에 대한 트래픽을 차단하여 상기 분산 서비스 거부 공격을 차단하는 단계를 더 포함하는 것을 특징으로 하는 분산 서비스 거부 공격의 차단 방법.

청구항 7

제6항에 있어서,

상기 오리진 서버로의 서비스 제공 요청에 대한 트래픽을 차단하여 상기 분산 서비스 거부 공격의 차단이 완료

된 경우 상기 DNS로 상기 복수개의 서버 중 적어도 하나로 변경된 IP 주소를 상기 오리진 서버의 IP 주소를 변경하도록 요청하는 것을 특징으로 하는 분산 서비스 거부 공격의 차단 방법.

청구항 8

제1항에 있어서,

상기 네트워크 시스템은 LB(Load Balancer)를 더 포함하고,

상기 단계(b)에서 상기 DNS로 상기 오리진 서버의 IP 주소를 상기 복수개의 서버 중 적어도 하나로 변경하도록 요청하는 것은 상기 LB로 상기 변경되는 IP 주소를 제공하여 수행되는 것을 특징으로 하는 분산 서비스 거부 공격의 차단 방법.

청구항 9

제1항에 있어서,

상기 오리진 서버의 트래픽 상태가 분산 서비스 거부 공격으로 판단되어 상기 DNS로 상기 오리진 서버의 IP 주소를 상기 복수개의 서버 중 적어도 하나로 변경하도록 요청하는 경우,

상기 복수개의 서버 중 적어도 하나는 상기 오리진 서버로 상기 오리진 서버에서 제공하는 콘텐츠의 전송을 요청하는 것을 특징으로 하는 분산 서비스 거부 공격의 차단 방법.

청구항 10

DNS(Domain Name System), 복수개의 서버 및 오리진 서버(Origin server)를 포함하는 네트워크 시스템에서 상기 오리진 서버로의 분산 서비스 거부 공격(DDoS: Distributed Denial of Service)을 차단하는 장치에 있어서,

상기 오리진 서버의 트래픽 상태가 분산 서비스 거부 공격인지 판단하는 공격 판단부; 및

상기 공격 판단부에서 상기 오리진 서버의 트래픽 상태가 분산 서비스 거부 공격인지 판단하는 경우, 상기 DNS로 상기 오리진 서버의 IP(Internet Protocol) 주소를 상기 복수개의 서버 중 적어도 하나로 변경하도록 요청하는 IP 주소 변경부를 포함하는 것을 특징으로 하는 분산 서비스 거부 공격의 차단 장치.

청구항 11

제10항에 있어서,

분산 서비스 거부 공격의 차단 장치는 상기 오리진 서버의 트래픽(traffic) 상태를 모니터링하는 모니터링부를 더 포함하는 것을 특징으로 하는 분산 서비스 거부 공격의 차단 장치.

청구항 12

제11항에 있어서,

상기 모니터링부는 상기 오리진 서버의 트래픽 상태의 모니터링은 상기 오리진 서버의 트래픽 상태가 미리 설정된 값을 초과하는지 모니터링하고,

상기 모니터링부의 모니터링 결과가 상기 오리진 서버의 트래픽 상태가 미리 설정된 값을 초과하는 경우,

상기 공격 판단부는 상기 오리진 서버의 트래픽 상태가 분산 서비스 거부 공격인지 판단하는 것을 특징으로 하는 분산 서비스 거부 공격의 차단 장치.

청구항 13

제12항에 있어서,

상기 모니터링부는 모니터링 결과가 상기 오리진 서버의 트래픽 상태가 미리 설정된 값을 초과하는 경우,

상기 IP 주소 변경부는 상기 공격 판단부에서 상기 오리진 서버의 트래픽 상태가 분산 서비스 거부 공격인지 판단하기 전, 상기 DNS로 상기 오리진 서버의 IP 주소를 상기 복수개의 서버 중 적어도 하나로 변경하도록 요청하는 것을 특징으로 하는 분산 서비스 거부 공격의 차단 장치.

청구항 14

제13항에 있어서,

상기 공격 판단부가 상기 오리진 서버의 트래픽 상태가 분산 서비스 거부 공격이 아닌 것으로 판단하는 경우,

상기 IP 주소 변경부는 상기 DNS로 상기 복수개의 서버 중 적어도 하나로 변경된 IP 주소를 상기 오리진 서버의 IP 주소를 변경하도록 요청하는 것을 특징으로 하는 분산 서비스 거부 공격의 차단 장치.

청구항 15

제10항에 있어서,

상기 공격 판단부에서 상기 오리진 서버의 트래픽 상태를 분산 서비스 거부 공격으로 판단하는 경우,

상기 오리진 서버로의 서비스 제공 요청에 대한 트래픽을 차단하여 상기 분산 서비스 거부 공격을 차단하는 공격 차단부를 더 포함하는 것을 특징으로 하는 분산 서비스 거부 공격의 차단 장치.

청구항 16

제15항에 있어서,

상기 공격 차단부에서 상기 분산 서비스 거부 공격의 차단을 완료한 경우,

상기 IP 주소 변경부는 상기 DNS로 상기 복수개의 서버 중 적어도 하나로 변경된 IP 주소를 상기 오리진 서버의 IP 주소를 변경하도록 요청하는 것을 특징으로 하는 분산 서비스 거부 공격의 차단 장치.

청구항 17

제10항에 있어서,

상기 네트워크 시스템은 LB(Load Balancer)를 더 포함하고,

상기 IP 주소 변경부는 상기 LB로 상기 변경되는 IP 주소를 제공하여 상기 DNS에서 상기 오리진 서버의 IP 주소를 상기 복수개의 서버 중 적어도 하나로 변경되도록 하는 것을 특징으로 하는 분산 서비스 거부 공격의 차단 장치.

청구항 18

제10항에 있어서,

상기 공격 판단부에서 상기 오리진 서버의 트래픽 상태가 분산 서비스 거부 공격으로 판단하여 상기 IP 주소 변경부에서 상기 DNS로 상기 오리진 서버의 IP 주소를 상기 복수개의 서버 중 적어도 하나로 변경하도록 요청하는 경우,

상기 복수개의 서버 중 적어도 하나는 상기 오리진 서버로 상기 오리진 서버에서 제공하는 콘텐츠의 전송을 요청하는 것을 특징으로 하는 분산 서비스 거부 공격의 차단 장치.

청구항 19

DNS(Domain Name System), 공격 판단 장치, 복수개의 서버 및 오리진 서버(Origin server)를 포함하는 네트워크 시스템에서 상기 공격 판단 장치에 의해 수행될 수 있는 분산 서비스 거부 공격(DDoS: Distributed Denial of Service)의 차단 방법이 구현되도록, 상기 공격 판단 장치에 의해 실행될 수 있는 명령어들의 프로그램이 구현되어 있으며 상기 공격 판단 장치에 의해 판독될 수 있는 프로그램을 기록한 기록매체에 있어서,

상기 오리진 서버의 트래픽(traffic) 상태가 분산 서비스 거부 공격인지 판단하는 단계(a); 및

상기 오리진 서버의 트래픽(traffic) 상태가 분산 서비스 거부 공격으로 판단되는 경우, 상기 DNS로 상기 오리진 서버의 IP(Internet Protocol) 주소를 상기 복수개의 서버 중 적어도 하나로 변경하도록 요청하는 단계(b)를 포함하는 것을 특징으로 하는 분산 서비스 거부 공격의 차단 방법을 구현하기 위한 프로그램을 기록한 기록매체.

명 세 서

발명의 상세한 설명

기 술 분 야

<1> 본 발명은 분산 서비스 거부 공격의 차단 방법 및 장치에 관한 것으로서, 보다 상세하게는 미리 설치된 통신망의 다른 장치들을 활용하여 분산 서비스 거부 공격을 판단하여 차단할 수 있게 하는 방법 및 장치에 관한 것이다.

배 경 기 술

<2> 통신망의 발달과 함께 데이터를 전송하는 다양한 방법과 기술들이 개발되고 있다.

<3> 통신망 특히 인터넷의 발달로 모든 정보를 가장 빠르게, 손쉽게 통신망을 통해 얻을 수 있게 되어 점차 우리 생활의 일부분으로 자리 잡아가고 있다.

<4> 그러나 인터넷과 같은 통신망은 본질적으로 다수가 용이하게 접속할 수 있는 통신망이므로 통신망에 산재한 자원을 충분히 활용하면서도 개인이나 회사의 중요한 정보를 통신망으로부터 보호해 줄 수 있는 통신망의 보안이 중요한 문제로 대두되고 있다.

<5> 특히, 통신망 중 인터넷의 다수가 용이하게 접속할 수 있는 특징을 이용하여 악의적으로 특정 회사의 서버 즉 웹 사이트로의 트래픽을 폭증시켜 특정 회사의 웹 사이트를 공격하는 분산 서비스 거부(Distributed Denial of Service) 공격이 심각한 문제로 대두되고 있다.

<6> 분산 서비스 거부 공격은 여러 ISP(Internet Service Provider)에 분산 접속되어 있는 다수의 PC와 같은 클라이언트가 특정 목적지 즉 특정 사이트나 서버로 일제히 방해 트래픽을 집중시켜 해당 특정 사이트 등이 정상적인 서비스를 할 수 없는 상황을 초래하는 공격이다.

<7> 이러한 분산 서비스 거부 공격은 정상적인 사용자의 서비스 요청과 구분하기 어렵고, 트래픽 요청이 갑자기 증가하는 등 분산 서비스 거부 공격으로 의심된다고 하여 무조건적으로 사용자로부터의 콘텐츠 제공이나 웹 페이지 제공 요청과 같은 서비스 요청을 차단하는 경우 정상적인 사용자의 서비스 요청에 대응하지 못할 수 있어 분산 서비스 거부 공격을 판단하고 차단하기 어려운 문제점이 있다.

<8> 이러한 문제점으로 인하여 분산 서비스 거부 공격을 판단하고 차단하기 위한 다양한 방법들이 연구되어 제안되고 있다.

<9> 종래의 분산 서비스 거부 공격 판단 방법의 종류를 살펴보면, 먼저 네트워크 상의 접점 장비를 이용한 판단의 방법이 있다.

<10> 이 방법은 네트워크 스위치나 회선 상에서의 트래픽의 일부 또는 전부를 검사하고 트래픽의 비정상 여부를 판단하여 분산 서비스 거부 공격을 판단하는 방법이다.

<11> 이러한 네트워크의 접점 장비를 통하여 분산 서비스 거부 공격을 판단하는 경우에는 패킷의 내용을 알 수 있어 네트워크 스위치가 L7인 경우 즉 7 레이어(Layer)까지도 분산 서비스 거부 공격 판단이 가능한 이점이 있다.

<12> 그러나 네트워크의 모든 관문에 접점 장비를 설치하여야 하므로 네트워크의 규모가 증가하면 할수록 비용이 크게 증가되는 단점이 있다.

<13> 종래의 분산 서비스 거부 공격의 또 다른 판단 방법으로는 네트워크 행동 분석(Network Behavior Analysis)을 통한 분산 서비스 거부 공격 판단 방법이 있다.

<14> 네트워크 행동 분석을 통한 분산 서비스 거부 공격 판단 방법은 네트워크 스위치에서 생성하는 데이터 정보를 수집하여 트래픽의 비정상 여부를 판단하는 방법으로서 특정 사이트의 운영자의 입장에서는 비용을 줄일 수 있고, 분산 서비스 거부 공격 판단시 변형된 분산 서비스 거부 공격의 판단도 유효하게 할 수 있는 이점이 있다.

<15> 그러나 네트워크 행동 분석을 통한 분산 서비스 거부 공격 판단 방법의 경우 L4 정보에만 의존하므로 네트워크 스위치가 L7인 경우 분산 서비스 거부 공격 판단이 불가능한 단점이 있다.

<16> 분산 서비스 거부 공격 판단의 다음 방법으로 Honey Net을 통한 분산 서비스 거부 공격 판단의 방법이 있다.

<17> Honey Net을 통한 분산 서비스 거부 공격 판단 방법은 공격 선행 단계인 Bot 감염 단계를 추적하는 방법으로서 분산 서비스 거부 공격의 근원지를 특정할 수 있어 분산 서비스 거부 공격의 원천 봉쇄가 가능하고 정확한 공격의 성격과 방식의 분석이 가능한 장점이 있다.

<18> 그러나 비용이 크게 증가되고 특정 시점과 특정 장소로의 특정 공격을 신속하게 판단할 확률이 낮은 단점이 있다.

<19> 이러한 분산 서비스 거부 공격 판단이 이루어지면 분산 서비스 거부 공격을 차단이 이루어지게 된다.

<20> 분산 서비스 거부 공격의 차단 방법은 네트워크 상의 접점을 차단하는 방법, ISP 전체 경로의 차단 방법 또는 IDC의 광대역 접점 차단 방법 등이 있다.

<21> 그러나, 이러한 분산 서비스 거부 공격의 차단 방법은 분산 서비스 거부 공격과 정상적인 서비스 요청을 명확하게 구별하여 판단하기 어렵기 때문에 트래픽이 집중되는 네트워크 상의 IDC 등의 접점이나 ISP 경로를 차단하므로 정상적인 서비스 요청까지도 차단하게 되므로 정상적인 서비스 제공 요청을 수용할 수 없는 문제점이 있다.

<22> 또한 분산 서비스 거부 공격의 판단과 차단을 위해 각 사이트나 서버들마다 분산 서비스 거부 공격의 판단과 차단을 위한 장치 등을 설치하여야 하며 이로 인해 비용이 크게 증가되며, 이러한 장치들을 설치하더라도 분산 서비스 거부 공격의 판단과 차단에 한계가 있는 문제점이 있다.

발명의 내용

해결 하고자하는 과제

<23> 상기한 바와 같은 종래의 문제점을 해결하기 위해, 본 발명은 정상적인 서비스 제공 요청을 수용할 수 있으면서도 분산 서비스 거부 공격의 판단과 차단할 수 있는 분산 서비스 거부 공격의 차단 방법 및 장치를 제안하는 것이다.

<24> 또한, 분산 서비스 거부 공격의 판단과 차단을 위해 각 사이트나 서버들마다 분산 서비스 거부 공격의 판단과 차단을 위한 장치 등을 설치하지 않아도 되어 비용을 절감하면서도 효과적으로 분산 서비스 거부 공격의 판단과 차단이 이루어질 수 있는 분산 서비스 거부 공격의 차단 방법 및 장치를 제안하는 것이다.

<25> 본 발명의 또 다른 목적들은 이하의 실시예에 대한 설명을 통해 쉽게 이해될 수 있을 것이다.

과제 해결수단

<26> 상기한 바와 같은 목적을 달성하기 위해, 본 발명의 일 측면에 따르면 분산 서비스 거부 공격의 차단 방법이 제공된다.

<27> 본 발명의 바람직한 일 실시예에 따르면, DNS(Domain Name System), 공격 판단 장치, 복수개의 서버 및 오리진 서버(Origin server)를 포함하는 네트워크 시스템에서 상기 공격 판단 장치에 의해 수행될 수 있는 상기 오리진 서버로의 분산 서비스 거부 공격(DDoS: Distributed Denial of Service)을 차단하는 방법에 있어서, 상기 오리진 서버의 트래픽(traffic) 상태가 분산 서비스 거부 공격인지 판단하는 단계(a); 및 상기 오리진 서버의 트래픽 상태가 분산 서비스 거부 공격으로 판단되는 경우, 상기 DNS로 상기 오리진 서버의 IP(Internet Protocol) 주소를 상기 복수개의 서버 중 적어도 하나로 변경하도록 요청하는 단계(b)를 포함하는 것을 특징으로 하는 분산 서비스 거부 공격의 차단 방법이 제공된다.

<28> 상기 단계(a)는 상기 오리진 서버의 트래픽(traffic) 상태를 모니터링하는 단계를 더 포함할 수 있으며, 상기 오리진 서버의 트래픽 상태의 모니터링은 상기 오리진 서버의 트래픽 상태가 미리 설정된 값을 초과하는지 모니터링하고, 상기 오리진 서버의 트래픽 상태가 미리 설정된 값을 초과하는 경우 상기 단계(b)에서 상기 오리진 서버의 트래픽 상태가 분산 서비스 거부 공격인지 판단할 수 있다.

<29> 또한, 상기 단계(a)에서 상기 오리진 서버의 트래픽 상태가 미리 설정된 값을 초과하는 경우 상기 단계(b)에서 상기 오리진 서버의 트래픽 상태가 분산 서비스 거부 공격인지 판단하기 전, 상기 DNS로 상기 오리진 서버의 IP 주소를 상기 복수개의 서버 중 적어도 하나로 변경하도록 요청할 수 있다.

<30> 그리고 상기 단계(b)에서 상기 오리진 서버의 트래픽 상태가 분산 서비스 거부 공격이 아닌 것으로 판단되는 경우 상기 DNS로 상기 복수개의 서버 중 적어도 하나로 변경된 IP 주소를 상기 오리진 서버의 IP 주소를 변경

하도록 요청할 수 있다.

<31> 상기 단계(b)는, 상기 오리진 서버의 트래픽 상태가 분산 서비스 거부 공격으로 판단되는 경우 상기 오리진 서버로의 서비스 제공 요청에 대한 트래픽을 차단하여 상기 분산 서비스 거부 공격을 차단하는 단계를 더 포함할 수 있다.

<32> 그리고, 상기 오리진 서버로의 서비스 제공 요청에 대한 트래픽을 차단하여 상기 분산 서비스 거부 공격의 차단이 완료된 경우 상기 DNS로 상기 복수개의 서버 중 적어도 하나로 변경된 IP 주소를 상기 오리진 서버의 IP 주소를 변경하도록 요청할 수 있다.

<33> 상기 네트워크 시스템은 LB(Load Balancer)를 더 포함하고, 상기 단계(b)에서 상기 DNS로 상기 오리진 서버의 IP 주소를 상기 복수개의 서버 중 적어도 하나로 변경하도록 요청하는 것은 상기 LB로 상기 변경되는 IP 주소를 제공하여 수행될 수 있다.

<34> 상기 오리진 서버의 트래픽 상태가 분산 서비스 거부 공격으로 판단되어 상기 DNS로 상기 오리진 서버의 IP 주소를 상기 복수개의 서버 중 적어도 하나로 변경하도록 요청하는 경우, 상기 복수개의 서버 중 적어도 하나는 상기 오리진 서버로 상기 오리진 서버에서 제공하는 콘텐츠의 전송을 요청할 수 있다.

<35> 본 발명의 다른 측면에 의하면, 분산 서비스 거부 공격의 차단 장치가 제공된다.

<36> 본 발명의 바람직한 일 실시예에 따르면, DNS(Domain Name System), 복수개의 서버 및 오리진 서버(Origin server)를 포함하는 네트워크 시스템에서 상기 오리진 서버로의 분산 서비스 거부 공격(DDoS: Distributed Denial of Service)을 차단하는 장치에 있어서, 상기 오리진 서버의 트래픽 상태가 분산 서비스 거부 공격인지 판단하는 공격 판단부; 및 상기 공격 판단부에서 상기 오리진 서버의 트래픽 상태가 분산 서비스 거부 공격인지 판단하는 경우, 상기 DNS로 상기 오리진 서버의 IP(Internet Protocol) 주소를 상기 복수개의 서버 중 적어도 하나로 변경하도록 요청하는 IP 주소 변경부를 포함하는 것을 특징으로 하는 분산 서비스 거부 공격의 차단 장치가 제공된다.

<37> 분산 서비스 거부 공격의 차단 장치는 상기 오리진 서버의 트래픽(traffic) 상태를 모니터링하는 모니터링부를 더 포함할 수 있으며, 상기 모니터링부는 상기 오리진 서버의 트래픽 상태의 모니터링은 상기 오리진 서버의 트래픽 상태가 미리 설정된 값을 초과하는지 모니터링하고, 상기 모니터링부의 모니터링 결과가 상기 오리진 서버의 트래픽 상태가 미리 설정된 값을 초과하는 경우, 상기 공격 판단부는 상기 오리진 서버의 트래픽 상태가 분산 서비스 거부 공격인지 판단할 수 있다.

<38> 그리고 상기 모니터링부는 모니터링 결과가 상기 오리진 서버의 트래픽 상태가 미리 설정된 값을 초과하는 경우, 상기 IP 주소 변경부는 상기 공격 판단부에서 상기 오리진 서버의 트래픽 상태가 분산 서비스 거부 공격인지 판단하기 전, 상기 DNS로 상기 오리진 서버의 IP 주소를 상기 복수개의 서버 중 적어도 하나로 변경하도록 요청할 수 있다.

<39> 또한, 상기 공격 판단부가 상기 오리진 서버의 트래픽 상태가 분산 서비스 거부 공격이 아닌 것으로 판단하는 경우, 상기 IP 주소 변경부는 상기 DNS로 상기 복수개의 서버 중 적어도 하나로 변경된 IP 주소를 상기 오리진 서버의 IP 주소를 변경하도록 요청할 수 있다.

<40> 상기 공격 판단부에서 상기 오리진 서버의 트래픽 상태를 분산 서비스 거부 공격으로 판단하는 경우, 상기 오리진 서버로의 서비스 제공 요청에 대한 트래픽을 차단하여 상기 분산 서비스 거부 공격을 차단하는 공격 차단부를 더 포함할 수 있다.

<41> 그리고 상기 공격 차단부에서 상기 분산 서비스 거부 공격의 차단을 완료한 경우, 상기 IP 주소 변경부는 상기 DNS로 상기 복수개의 서버 중 적어도 하나로 변경된 IP 주소를 상기 오리진 서버의 IP 주소를 변경하도록 요청할 수 있다.

<42> 상기 네트워크 시스템은 LB(Load Balancer)를 더 포함하고, 상기 IP 주소 변경부는 상기 LB로 상기 변경되는 IP 주소를 제공하여 상기 DNS에서 상기 오리진 서버의 IP 주소를 상기 복수개의 서버 중 적어도 하나로 변경되도록 할 수 있다.

<43> 상기 공격 판단부에서 상기 오리진 서버의 트래픽 상태가 분산 서비스 거부 공격으로 판단하여 상기 IP 주소 변경부에서 상기 DNS로 상기 오리진 서버의 IP 주소를 상기 복수개의 서버 중 적어도 하나로 변경하도록 요청하는 경우, 상기 복수개의 서버 중 적어도 하나는 상기 오리진 서버로 상기 오리진 서버에서 제공하는 콘텐츠

의 전송을 요청할 수 있다.

<44> 본 발명의 다른 측면에 의하면, 분산 서비스 거부 공격의 차단 방법을 구현하기 위한 프로그램을 기록한 기록매체가 제공된다.

<45> 본 발명의 바람직한 일 실시예에 따르면, DNS(Domain Name System), 공격 판단 장치, 복수개의 서버 및 오리진 서버(Origin server)를 포함하는 네트워크 시스템에서 상기 공격 판단 장치에 의해 수행될 수 있는 분산 서비스 거부 공격(DDoS: Distributed Denial of Service)의 차단 방법이 구현되도록, 상기 공격 판단 장치에 의해 실행될 수 있는 명령어들의 프로그램이 구현되어 있으며 상기 공격 판단 장치에 의해 판독될 수 있는 프로그램을 기록한 기록매체에 있어서, 상기 오리진 서버의 트래픽(traffic) 상태가 분산 서비스 거부 공격인지 판단하는 단계(a); 및 상기 오리진 서버의 트래픽(traffic) 상태가 분산 서비스 거부 공격으로 판단되는 경우, 상기 DNS로 상기 오리진 서버의 IP(Internet Protocol) 주소를 상기 복수개의 서버 중 적어도 하나로 변경하도록 요청하는 단계(b)를 포함하는 것을 특징으로 하는 분산 서비스 거부 공격의 차단 방법을 구현하기 위한 프로그램을 기록한 기록매체가 제공된다.

<46> 상기 단계(a)는 상기 오리진 서버의 트래픽(traffic) 상태를 모니터링하는 단계를 더 포함할 수 있으며, 상기 오리진 서버의 트래픽 상태의 모니터링은 상기 오리진 서버의 트래픽 상태가 미리 설정된 값을 초과하는지 모니터링하고, 상기 오리진 서버의 트래픽 상태가 미리 설정된 값을 초과하는 경우 상기 단계(b)에서 상기 오리진 서버의 트래픽 상태가 분산 서비스 거부 공격인지 판단할 수 있다.

<47> 또한, 상기 단계(a)에서 상기 오리진 서버의 트래픽 상태가 미리 설정된 값을 초과하는 경우 상기 단계(b)에서 상기 오리진 서버의 트래픽 상태가 분산 서비스 거부 공격인지 판단하기 전, 상기 DNS로 상기 오리진 서버의 IP 주소를 상기 복수개의 서버 중 적어도 하나로 변경하도록 요청할 수 있다.

<48> 그리고 상기 단계(b)에서 상기 오리진 서버의 트래픽 상태가 분산 서비스 거부 공격이 아닌 것으로 판단되는 경우 상기 DNS로 상기 복수개의 서버 중 적어도 하나로 변경된 IP 주소를 상기 오리진 서버의 IP 주소를 변경하도록 요청할 수 있다.

<49> 상기 단계(b)는, 상기 오리진 서버의 트래픽 상태가 분산 서비스 거부 공격으로 판단되는 경우 상기 오리진 서버로의 서비스 제공 요청에 대한 트래픽을 차단하여 상기 분산 서비스 거부 공격을 차단하는 단계를 더 포함할 수 있다.

<50> 그리고, 상기 오리진 서버로의 서비스 제공 요청에 대한 트래픽을 차단하여 상기 분산 서비스 거부 공격의 차단이 완료된 경우 상기 DNS로 상기 복수개의 서버 중 적어도 하나로 변경된 IP 주소를 상기 오리진 서버의 IP 주소를 변경하도록 요청할 수 있다.

<51> 상기 네트워크 시스템은 LB(Load Balancer)를 더 포함하고, 상기 단계(b)에서 상기 DNS로 상기 오리진 서버의 IP 주소를 상기 복수개의 서버 중 적어도 하나로 변경하도록 요청하는 것은 상기 LB로 상기 변경되는 IP 주소를 제공하여 수행될 수 있다.

<52> 상기 오리진 서버의 트래픽 상태가 분산 서비스 거부 공격으로 판단되어 상기 DNS로 상기 오리진 서버의 IP 주소를 상기 복수개의 서버 중 적어도 하나로 변경하도록 요청하는 경우, 상기 복수개의 서버 중 적어도 하나는 상기 오리진 서버로 상기 오리진 서버에서 제공하는 콘텐츠의 전송을 요청할 수 있다.

효 과

<53> 이상에서 설명한 바와 같이, 본 발명에 의한 분산 서비스 거부 공격의 차단 방법 및 장치에 의하면 정상적인 서비스 제공 요청을 수용할 수 있으면서도 분산 서비스 거부 공격의 판단과 차단할 수 있는 장점이 있다.

<54> 또한 분산 서비스 거부 공격의 판단과 차단을 위해 각 사이트나 서버들마다 분산 서비스 거부 공격의 판단과 차단을 위한 장치 등을 설치하지 않아도 되어 비용을 절감하면서도 효과적으로 분산 서비스 거부 공격의 판단과 차단이 이루어질 수 있는 장점이 있다.

발명의 실시를 위한 구체적인 내용

<55> 본 발명은 다양한 변경을 가할 수 있고 여러 가지 실시예를 가질 수 있는 바, 특정 실시예들을 도면에 예시하고 상세한 설명에 상세하게 설명하고자 한다. 그러나, 이는 본 발명을 특정한 실시 형태에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변경, 균등물 내지 대체물을 포함하는 것으로 이해

되어야 한다.

<56> 각 도면을 설명하면서 유사한 참조부호를 유사한 구성요소에 대해 사용하였다. 본 발명을 설명함에 있어서 관련된 공지 기술에 대한 구체적인 설명이 본 발명의 요지를 흐릴 수 있다고 판단되는 경우 그 상세한 설명을 생략한다.

<57> 제1, 제2 등의 용어는 다양한 구성 요소들을 설명하는데 사용될 수 있지만, 상기 구성 요소들은 상기 용어들에 의해 한정되어서는 안 된다. 상기 용어들은 하나의 구성요소를 다른 구성요소로부터 구별하는 목적으로만 사용된다.

<58> 예를 들어, 본 발명의 권리 범위를 벗어나지 않으면서 제1 구성요소는 제2 구성요소로 명명될 수 있고, 유사하게 제2 구성요소도 제1 구성요소로 명명될 수 있다.

<59> 및/또는 이라는 용어는 복수의 관련된 기재된 항목들의 조합 또는 복수의 관련된 기재된 항목들 중의 어느 항목을 포함한다.

<60> 어떤 구성요소가 다른 구성요소에 "연결되어" 있다거나 "접속되어" 있다고 언급된 때에는, 그 다른 구성요소에 직접적으로 연결되어 있거나 또는 접속되어 있을 수도 있지만, 중간에 다른 구성요소가 존재할 수도 있다고 이해되어야 할 것이다.

<61> 반면에, 어떤 구성요소가 다른 구성요소에 "직접 연결되어" 있다거나 "직접 접속되어" 있다고 언급된 때에는, 중간에 다른 구성요소가 존재하지 않는 것으로 이해되어야 할 것이다.

<62> 본 출원에서 사용한 용어는 단지 특정한 실시예를 설명하기 위해 사용된 것으로, 본 발명을 한정하려는 의도가 아니다.

<63> 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 출원에서, "포함하다" 또는 "가지다" 등의 용어는 명세서상에 기재된 특징, 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것이 존재함을 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.

<64> 다르게 정의되지 않는 한, 기술적이거나 과학적인 용어를 포함해서 여기서 사용되는 모든 용어들은 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 것과 동일한 의미를 가지고 있다.

<65> 일반적으로 사용되는 사전에 정의되어 있는 것과 같은 용어들은 관련 기술의 문맥상 가지는 의미와 일치하는 의미를 가지는 것으로 해석되어야 하며, 본 출원에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.

<66> 이하, 첨부된 도면을 참조하여 본 발명에 따른 바람직한 실시예를 상세히 설명하되, 도면 부호에 관계없이 동일하거나 대응하는 구성 요소는 동일한 참조 번호를 부여하고 이에 대한 중복되는 설명은 생략하기로 한다.

<67> 도 1은 본 발명의 바람직한 일 실시예에 따른 분산 서비스 거부 공격의 차단 방법이 적용될 수 있는 네트워크 시스템의 구성을 도시한 도면이다.

<68> 도 1에 도시된 바와 같이, 본 발명의 바람직한 일 실시예에 따른 분산 서비스 거부 공격의 차단 방법이 적용될 수 있는 네트워크 시스템은 복수의 사용자(100a, 100b, 100c,…100n)와 DNS(Domain Name System)(120), LB(Load Balancer)(130), 공격 판단 장치(140), 복수개의 서버(150a, 150b, 150c,…150n) 및 오리진 서버(Origin server)(160)를 포함할 수 있으며, 각각의 구성 요소들은 통신망(110)을 통해 연결된다.

<69> 본 발명에서는 통신망(110)은 온라인 및 이동 통신망 등 다양한 종류의 통신망일 수 있으며, 통신망의 종류나 형태에는 아무런 제한이 없다.

<70> 사용자(100)는 통신망(110)을 통해 웹 페이지나 콘텐츠의 제공 등의 서비스 제공 요청을 하며 이러한 요청은 오리진 서버(160)로 전송되어 오리진 서버(160)에서의 응답을 통해 웹 페이지나 콘텐츠 등이 사용자(100)에게 수신될 수 있다.

<71> 도 1에서는 사용자(100)로 명칭하였으나 실제로 PC(Personal Computer)또는 PDA(Personal Digital Assistant) 및 휴대 전화 등의 휴대 단말기와 같은 디지털 처리 장치를 이용하여 통신망(110)을 통해 웹 페이지나 콘텐츠 등을 요청하는 사용자가 이용하는 디지털 처리 장치일 수 있으며, 이러한 사용자들(100)은 여러 ISP(Internet Service Provider)에 분산되어 접속할 수 있다.

<72> DNS(120)는 통신망(110)에서 도메인이나 호스트 이름을 숫자로 된 IP 주소(Internet Protocol Address)로 해석해주는 네임 서비스 시스템이다.

<73> 이러한 DNS(120)는 네임 서버와 도메인 네임과 IP 주소를 매칭하는 참조 테이블 또는 데이터베이스를 포함할 수 있으며, 로컬 DNS와 상위 DNS 등의 계층 구조를 형성할 수도 있다

<74> 또한, 복수개의 네임 서버를 포함하거나 계층 구조를 이루는 경우 복수개의 DNS(120) 또는 DNS(120)를 구성하는 서버 중 네임 서비스를 제공할 서버를 결정하는 장치를 포함할 수 있다.

<75> 이하의 설명에서는 이러한 장치들을 모두 포함하여 DNS(120)라 명칭하기로 하며, 사용자 등의 도메인이나 호스트 이름에 상응하는 IP 주소를 해석해주기 위한 기능은 이러한 DNS(120) 내에서의 장치들 중 하나 또는 장치들 간의 통신을 통해 이루어 질 수 있다.

<76> LB(130)는 복수개의 서버(150a, 150b, 150c,…150n)에서 사용자(100)가 요청한 콘텐츠를 요청하는 경우 DNS(120)와 연결되어 콘텐츠를 제공한 최적의 서버를 결정하고 결정된 서버의 정보를 DNS(120)에 제공하는 로드 밸런싱(load balancing)을 수행하는 장치이다.

<77> LB(130)는 예를 들어, 사용자(100)가 요청한 콘텐츠에 대하여 복수개의 서버(150a, 150b, 150c,…150n)가 모두 제공할 수 있는 경우 복수개의 서버(150a, 150b, 150c,…150n) 중 가장 부하(load)가 적은 서버 또는 사용자(100)가 요청한 콘텐츠를 저장하고 있는 서버에서 사용자(100)에게 콘텐츠를 제공하도록 할 수 있다.

<78> 이때, 사용자(100)의 디지털 처리 장치에 설치된 웹 브라우저에서 도메인 네임을 입력하면 DNS(120)는 사용자가 요청한 도메인 네임에 매칭되는 서버의 IP 주소로 응답하게 된다.

<79> 이때 응답할 주소의 결정은 LB(130)가 복수개의 서버(150a, 150b, 150c,…150n)와 연결되어 복수개의 서버(150a, 150b, 150c,…150n)의 상태 정보에 따라 최적의 서버를 선택하여 선택된 최적의 서버 정보를 DNS(120)로 제공함으로써 수행된다.

<80> 이러한 LB(130)는 본래의 콘텐츠를 제공하는 오리진 서버(160)와도 연결되어 복수개의 서버(150a, 150b, 150c,…150n)뿐만 아니라 오리진 서버(160)도 포함하여 최적의 서버를 선택하는 로드 밸런싱을 수행할 수 있다.

<81> 오리진 서버(160)도 포함하여 최적의 서버를 선택하는 것은 예를 들면, 제공하고자 하는 콘텐츠가 복수개의 서버(150a, 150b, 150c,…150n)에 저장되어 있지 않은 경우 오리진 서버(160)를 통해 해당 콘텐츠를 제공받도록 하는 것도 가능하나 이에 한정되는 것은 아니다.

<82> 한편, 이러한 사용자(100)가 요청하는 콘텐츠를 복수개의 서버(150a, 150b, 150c,…150n)에 저장하여 사용자(100)가 요청하는 콘텐츠의 원본을 가진 오리진 서버(160)의 부하를 줄여주고 보다 빠르고 정확하게 콘텐츠의 전송이 이루어질 수 있도록 하는 것을 콘텐츠 전송망(CDN: Contents Delivery Network) 서비스라고 한다.

<83> 한편, LB(130), 공격 판단 장치(140), 복수개의 서버(150a, 150b, 150c,…150n)는 콘텐츠 전송을 수행하는 콘텐츠 전송 서비스 제공자 Contents Delivery Network Service Provider)에 의해 제공될 수 있으나 이에 한정되는 것은 아니다.

<84> 본 발명의 바람직한 일 실시예에 따르면, 콘텐츠 전송망에서 오리진 서버(160)를 모니터링하여 오리진 서버(160)에 대한 분산 서비스 거부 공격 여부를 판단하여 차단하는 공격 판단 장치(140)를 포함한다.

<85> 공격 판단 장치(140)는 복수개의 서버(150a, 150b, 150c,…150n)와 연결될 수 있으며, 또한 본 발명에 의한 네트워크 시스템을 구성하는 다른 구성 요소들(사용자(100a, 100b, 100c,…100n), DNS(Domain Name System)(120), LB(Load Balancer)(130) 및 오리진 서버(Origin server)(160))와 연결될 수 있다.

<86> 한편, 도 1에서는 복수개의 서버(150a, 150b, 150c,…150n)들이 공격 판단 장치(140)을 통해 통신망(110)에 연결되는 것으로 도시하였으나, 이는 설명의 편의를 위한 것으로서 공격 판단 장치(140)를 통해서만 통신망(110)에 연결되지 않을 수 있음은 자명하다.

<87> 본 발명의 바람직한 일 실시예에 따르면 공격 판단 장치(140)가 오리진 서버(160)의 상태를 모니터링하고 오리진 서버(160)로의 분산 서비스 거부 공격으로 의심되는 트래픽이 발생되는 경우 DNS(120)로 오리진 서버(160)의 주소를 복수개의 서버(150a, 150b, 150c,…150n)들의 IP 주소로 변경하도록 요청할 수 있다.

<88> 이러한 경우 DNS(120)로 오리진 서버(160)의 주소를 복수개의 서버(150a, 150b, 150c,…150n)들의 IP 주소로

변경하도록 요청하는 것은 로드 밸런싱을 수행하는 LB(130)를 통해 수행될 수 있다.

<89> 예를 들어, 공격 판단 장치(140)가 LB(130)와의 통신을 통해 사용자가 요청한 서비스의 제공이 이루어질 수 있는 최적의 서버를 오리진 서버(160)에서 복수개의 서버(150a, 150b, 150c,…150n) 중 하나로 설정하도록 함으로써 DNS(120)는 LB(130)와의 통신을 통해 오리진 서버(160)에 대한 IP 주소 요청에 대하여 복수개의 서버(150a, 150b, 150c,…150n) 중 하나로 IP 주소 응답을 하도록 하는 것이 가능하다.

<90> 일단 복수개의 서버(150a, 150b, 150c,…150n)들이 오리진 서버(160)를 대신하여 사용자(100)들의 서비스 요청에 대하여 응답하도록 할 수 있으며, 복수개의 서버(150a, 150b, 150c,…150n)들이 오리진 서버(160)를 대신하여 사용자(100)들의 서비스 요청에 대하여 응답하는 동안 공격 판단 장치(140)는 분산 서비스 거부 공격으로 의심되는 트래픽이 분산 서비스 거부 공격인지 판단하여 분산 서비스 거부 공격인 경우 분산 서비스 거부 공격에 대한 차단을 수행할 수 있도록 한다.

<91> 한편, 공격 판단 장치(140)가 오리진 서버(160)로의 분산 서비스 거부 공격으로 의심되는 트래픽을 감지하는 경우 복수개의 서버(150a, 150b, 150c,…150n)들이 오리진 서버(160)를 대신하여 사용자(100)들의 서비스 요청에 대하여 응답하기 위해 복수개의 서버(150a, 150b, 150c,…150n)들이 오리진 서버(160)로부터 오리진 서버(160)에서 제공하는 콘텐츠 등을 전달받을 수 있다.

<92> 물론 복수개의 서버(150a, 150b, 150c,…150n)들이 미리 오리진 서버(160)에서 제공하는 콘텐츠 등을 저장하고 있는 경우 오리진 서버(160)에서 제공하는 콘텐츠 등의 전달은 이루어지지 않을 수 있다.

<93> 이러한 본 발명에 의한 분산 서비스 거부 공격에 대한 차단 방법에 의하면 이미 설치되어 있는 콘텐츠 전송망의 구성 요소들을 활용하여 분산 서비스 거부 공격을 차단할 수 있게 된다.

<94> 또한, 콘텐츠 제공 등을 수행하는 각각의 웹 사이트 등은 일일이 분산 서비스 거부 공격의 판단 및 차단을 위한 시스템을 구축하지 않아도 되게 된다.

<95> 그리고 오리진 서버(160)에서 제공하는 콘텐츠의 제공 등이 지속적으로 이루어지게 하면서도 분산 서비스 거부 공격에 대한 판단과 차단이 가능하게 된다.

<96> 이러한 본 발명의 바람직한 일 실시예에 따른 분산 서비스 거부 공격의 차단 방법이 적용될 수 있는 네트워크 시스템의 구성을 참조하여 본 발명의 바람직한 일 실시예에 따른 분산 서비스 거부 공격의 차단 방법이 적용되는 순서를 살펴본다.

<97> 도 2는 본 발명의 바람직한 일 실시예에 따른 분산 서비스 거부 공격의 차단 방법이 적용되는 순서를 도시한 순서도이다.

<98> 본 발명의 바람직한 일 실시예에 따른 분산 서비스 거부 공격의 차단 방법은 전술한 도 1에서 도시한 공격 판단 장치(140)에서 수행될 수 있다.

<99> 먼저 도 2에 도시된 바와 같이, 공격 판단 장치(140)에서 오리진 서버(160)의 상태를 모니터링한다(S200).

<100> 이러한 오리진 서버(160) 상태의 모니터링은 본 발명에 의한 분산 서비스 거부 공격의 차단 방법이 적용될 수 있는 사이트나 서버들에 포함되어 구성되거나 별도의 장치에서 수행되는 것도 가능하다.

<101> 그리고 모니터링 결과를 본 발명의 바람직한 일 실시예에 의한 공격 판단 장치(140)로 수신하는 것도 가능하며, 이 경우 본 발명의 바람직한 일 실시예에 의한 분산 서비스 거부 공격의 차단 방법에서 단계 200은 포함되지 않을 수도 있다.

<102> 오리진 서버(160)로의 분산 서비스 거부 공격으로 의심되는 트래픽이 발생되는지 판단하여(S202), 오리진 서버(160)로의 분산 서비스 거부 공격으로 의심되는 경우 즉 분산 서비스 거부 공격으로 의심되는 트래픽이 발생되는 경우, 예를 들면 특정 시간대에 평균 트래픽보다 많은 트래픽이 오리진 서버(160)에서 발생되는 경우에 공격 판단 장치(140)는 DNS(120)로 오리진 서버(160)의 주소를 복수개의 서버(150a, 150b, 150c,…150n)들의 IP 주소로 변경하도록 요청하여 DNS(120)에서 IP 주소가 변경되도록 한다(S204).

<103> 한편, 도 2에서는 미도시하였으나 전술한 바와 같이 오리진 서버(160)로의 분산 서비스 거부 공격으로 의심되는 경우에도 일단 복수개의 서버(150a, 150b, 150c,…150n)들이 오리진 서버(160)를 대신하여 사용자(100)들의 서비스 요청에 대하여 응답하도록 할 수 있다.

<104> 또한, 복수개의 서버(150a, 150b, 150c,…150n)들뿐만 아니라 오리진 서버(160)를 포함하여 사용자(100)들의

서비스 요청에 대하여 응답하도록 하는 것도 가능하다.

<105> 분산 서비스 거부 공격인지 여부를 판단하는 동안 일단 복수개의 서버(150a, 150b, 150c,…150n)들이 오리진 서버(160)를 대신하여 사용자(100)들의 서비스 요청에 대하여 응답하도록 하는 것은 실제 분산 서비스 거부 공격인지 아니면 정상적인 서비스 요청이나 그 요청이 많은 것인지 여부를 판단하는 동안에도 오리진 서버(160)가 분산 서비스 거부 공격에 의해 정상적인 서비스를 제공하지 못하는 경우가 발생될 수 있으므로 오리진 서버(160)에서 제공하는 서비스 제공의 안정성을 높일 수 있게 하기 위한 것이다.

<106> 한편, 분산 서비스 거부 공격인지 여부를 판단하는 동안이 아니라 분산 서비스 거부 공격인지 여부를 판단한 후에만 복수개의 서버(150a, 150b, 150c,…150n)들이 오리진 서버(160)를 대신하여 사용자(100)들의 서비스 요청에 대하여 응답하도록 하는 것도 가능하다.

<107> 공격 판단 장치(140)는 분산 서비스 거부 공격으로 의심되는 트래픽이 분산 서비스 거부 공격인지 판단하여(S206) 분산 서비스 거부 공격이 아닌 것으로 판단되는 경우 DNS(120)로 복수개의 서버(150a, 150b, 150c,…150n)들의 IP 주소를 오리진 서버(160)의 주소로 변경하도록 요청하여 DNS(120)의 IP 주소가 변경되도록 한다(S208).

<108> 그러나 분산 서비스 거부 공격인지 판단되는 경우 복수개의 서버(150a, 150b, 150c,…150n)들이 오리진 서버(160)를 대신하여 사용자(100)들의 서비스 요청에 대하여 응답하도록 하도록 복수개의 서버(150a, 150b, 150c,…150n)들을 포함하는 사용자(100)들의 서비스 요청을 콘텐츠 전송망에 연결시킨다(S210).

<109> 한편, 전술한 바와 같이 DNS(120)로 오리진 서버(160) 또는 복수개의 서버(150a, 150b, 150c,…150n)의 IP 주소로 변경하도록 요청하는 것은 로드 밸런싱을 수행하는 LB(130)를 통해 수행될 수 있다.

<110> 그리고 도 2에서는 오리진 서버(160)에서의 안정적인 서비스의 제공이 가능하도록 하기 위해 오리진 서버(160)로의 트래픽이 분산 서비스 거부 공격으로 의심되는지 판단하는 단계 202 및 오리진 서버(160)로의 트래픽이 분산 서비스 거부 공격으로 의심되는 경우 DNS(120)로 오리진 서버(160)의 IP 주소의 변경을 요청하는 단계 204를 더 포함하였으나, 오리진 서버(160)로의 트래픽 모니터링을 통해 즉시 분산 서비스 거부 공격인지 여부를 판단하거나 판단할 수 있는 경우라면 단계 202 및 단계 204는 포함하지 않을 수 있다.

<111> 그러나, 전술한 바와 같이 분산 서비스 거부 공격의 경우 사용자의 정상적인 서비스 제공 요청과 구분하기 어려우므로 예를 들면, 오리진 서버(160)로의 특정 시간대의 트래픽이 미리 설정된 값 이상으로 증가하는 경우 이를 단계 202에서와 같이 분산 서비스 거부 공격으로 의심되는 것으로 판단하도록 설정할 수 있다.

<112> 그리고 오리진 서버(160)로의 트래픽을 다시 자세하게 분석하여 단계 206에서와 같이 최종적으로 분산 서비스 거부 공격인지 아닌지 판단하도록 하는 것도 가능하다.

<113> 한편, 본 발명에 의한 공격 판단 장치(140)가 분산 서비스 거부 공격인지 판단하는 것은 전술한 네트워크 상의 접점 장비를 이용한 판단의 방법이나, 네트워크 행동 분석(Network Behavior Analysis)을 통한 분산 서비스 거부 공격 판단의 방법 또는 Honey Net을 통한 분산 서비스 거부 공격 판단의 방법뿐만 아니라 다양한 방법의 분산 서비스 거부 공격에 대한 판단 방법이 적용될 수 있으며, 분산 서비스 거부 공격에 대한 판단이 이루어질 수 있는 방법이라면 아무런 제한이 없다.

<114> 공격 판단 장치(140)가 오리진 서버(160)로의 분산 서비스 거부 공격으로 의심되는 트래픽을 모니터링하는 경우 복수개의 서버(150a, 150b, 150c,…150n)들이 오리진 서버(160)를 대신하여 사용자(100)들의 서비스 요청에 응답하기 위해 복수개의 서버(150a, 150b, 150c,…150n)들이 오리진 서버(160)로부터 오리진 서버(160)에서 제공하는 콘텐츠 등을 전달받을 수 있다.

<115> 물론 복수개의 서버(150a, 150b, 150c,…150n)들이 미리 오리진 서버(160)에서 제공하는 콘텐츠 등을 저장하고 있는 경우 오리진 서버(160)에서 제공하는 콘텐츠 등의 복수개의 서버(150a, 150b, 150c,…150n)로의 전달은 이루어지지 않을 수 있음은 전술한 바와 같다.

<116> 그리고 이와 함께 분산 서비스 거부 공격에 대한 차단을 수행할 수 있도록 하는 처리를 수행한다(S212).

<117> 이러한 분산 서비스 거부 공격에 대한 차단은 전술한 네트워크 상의 접점을 차단하는 방법이나 ISP 전체 경로의 차단 방법 또는 IDC의 광대역 접점 차단 방법뿐만 아니라 다양한 방법의 분산 서비스 거부 공격에 대한 차단 방법이 적용될 수 있으며, 분산 서비스 거부 공격에 대한 차단이 이루어질 수 있는 방법이라면 아무런 제한이 없다.

<118> 그리고 이러한 분산 서비스 거부 공격에 대한 차단은 본 발명의 바람직한 일 실시에에 따른 공격 판단 장치(140)에서 수행되거나 공격 판단 장치(140)로부터 정보를 수신하여 별도의 장치에서 수행되도록 하는 것도 가능함은 자명하다.

<119> 이러한 분산 서비스 거부 공격에 대한 차단이 이루어지고 최종적으로 분산 서비스 공격에 대하여 완전히 차단되었거나 분산 서비스 거부 공격이 종료되었는지 판단하여(S214) 분산 서비스 공격에 대하여 완전히 차단되었거나 분산 서비스 거부 공격이 종료된 것으로 판단되는 경우 DNS(120)로 복수개의 서버(150a, 150b, 150c, …150n)들의 IP 주소를 오리진 서버(160)의 주소로 변경하도록 요청하여 DNS(120)의 IP 주소가 변경되도록 한다(S208).

<120> 이러한 본 발명에 의한 분산 서비스 거부 공격에 대한 차단 방법에 의하면 콘텐츠 제공이나 웹 페이지 제공 등을 수행하는 각각의 웹 사이트들이나 서버들은 일일이 분산 서비스 거부 공격의 판단 및 차단을 위한 시스템을 구축하지 않아도 되게 된다.

<121> 또한, 분산 서비스 거부 공격이 발생하지 않는 정상적인 네트워크 상태인 경우에는 콘텐츠 전송망을 이용하지 않게 되지만 분산 서비스 거부 공격시에는 이미 구축되어 있는 콘텐츠 전송망의 구성 요소들을 활용하여 분산 서비스 거부 공격을 차단할 수 있게 되는 것이다.

<122> 그리고, 콘텐츠 전송망 서비스의 특성을 이용하여 오리진 서버(160)에서 제공하는 콘텐츠의 제공 등이 지속적으로 이루어지게 하면서 분산 서비스 거부 공격에 대한 판단과 차단이 가능하게 할 수 있게 한다.

<123> 한편, 이러한 전술한 본 발명에 의한 분산 서비스 거부 공격의 차단 방법은 프로그램으로 구현되어 컴퓨터로 읽을 수 있는 기록매체(씨디롬, 램, 롬, 플로피 디스크, 하드디스크, 광자기디스크 등)에 저장될 수 있다.

<124> 이하에서는 도 3을 본 발명의 바람직한 일 실시예에 따른 분산 서비스 거부 공격의 차단 방법이 적용되게 하는 공격 판단 장치의 구성을 살펴보기로 한다.

<125> 도 3은 본 발명의 바람직한 일 실시예에 따른 분산 서비스 거부 공격의 차단 방법이 적용되게 하는 장치인 공격 판단 장치(140)의 구성을 도시한 도면이다.

<126> 도 3에 도시된 바와 같이 본 발명의 바람직한 일 실시예에 따른 분산 서비스 거부 공격의 차단 방법이 적용되게 하는 공격 판단 장치(140)는 모니터링부(300), 공격 판단부(310), IP주소 변경부(320) 및 공격 차단부(330)를 포함할 수 있다.

<127> 모니터링부(300)는 오리진 서버(160)의 상태를 모니터링하여 오리진 서버(160)로의 분산 서비스 거부 공격으로 의심되는 트래픽이 발생되는지 감시한다.

<128> 한편, 도 3에서는 공격 판단 장치(140)에 모니터링부(300)를 포함하는 것으로 도시하였으나, 이러한 모니터링부(300)는 본 발명에 의한 분산 서비스 거부 공격의 차단 방법이 적용될 수 있는 사이트나 서버들에 포함되어 구성되거나 별도로 구성되는 것도 가능하다.

<129> 그리고 모니터링부(300)에서의 모니터링 결과를 본 발명의 바람직한 일 실시예에 의한 공격 판단 장치(140)로 수신하는 것도 가능하며, 이 경우 본 발명의 바람직한 일 실시예에 의한 공격 판단 장치(140)에는 모니터링부(300)가 포함되지 않을 수도 있다.

<130> 공격 판단부(310)는 모니터링부(330)에서 모니터링된 분산 서비스 거부 공격으로 의심되는 트래픽이 오리진 서버(160)로의 분산 서비스 거부 공격인지 판단한다.

<131> IP주소 변경부(320)는 공격 판단부(310)에서 오리진 서버(160)로의 트래픽이 분산 서비스 거부 공격으로 판단되는 경우 오리진 서버(160)의 IP 주소를 복수개의 서버(150a, 150b, 150c,…150n)의 IP 주소로 변경하도록 DNS(120)에 요청한다.

<132> 오리진 서버(160)에서 제공하는 서비스의 안정성을 높일 수 있게 하기 위해 공격 판단부(310)에서 분산 서비스 거부 공격인지 여부를 판단하는 동안 일단 복수개의 서버(150a, 150b, 150c,…150n)가 오리진 서버(160)를 대신하여 사용자(100)들의 서비스 요청에 대하여 응답하도록 하는 경우에도 IP주소 변경부(320)는 오리진 서버(160)의 IP 주소를 복수개의 서버(150a, 150b, 150c,…150n)의 IP 주소로 변경하도록 DNS(120)에 요청할 수 있음은 전술한 바와 같다.

<133> 공격 차단부(330)는 공격 판단부(310)에서 오리진 서버(160)로의 트래픽을 분산 서비스 거부 공격으로 판단하

는 경우 오리진 서버(160)로의 트래픽을 차단하는 등의 방법으로 오리진 서버(120)에 대한 분산 서비스 거부 공격을 차단한다.

<134> 이러한 공격 차단부(330)는 본 발명의 바람직한 일 실시예에 따른 분산 서비스 거부 공격의 차단 방법이 적용되게 하는 공격 판단 장치(140)와 별도의 장치로 구성되어 분산 서비스 거부 공격의 차단을 수행하도록 하는 것도 가능하다.

<135> 그리고 본 발명의 바람직한 일 실시예에 따른 공격 판단 장치(140)는 콘텐츠 전송망을 구성하는 장치 예를 들면, 복수개의 서버(150a, 150b, 150c,…150n)를 관리하는 장치에 그 기능들을 포함하여 구성될 수도 있다

<136> 상기한 본 발명의 바람직한 실시예는 예시의 목적을 위해 개시된 것이고, 본 발명에 대해 통상의 지식을 가진 당업자라면 본 발명의 사상과 범위 안에서 다양한 수정, 변경, 부가가 가능할 것이며, 이러한 수정, 변경 및 부가는 하기의 특허청구범위에 속하는 것으로 보아야 할 것이다.

도면의 간단한 설명

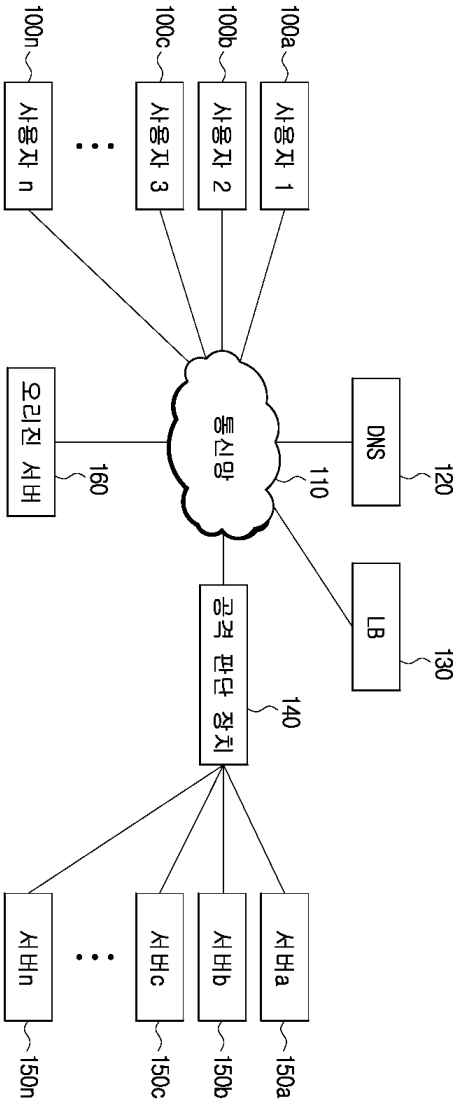
<137> 도 1은 본 발명의 바람직한 일 실시예에 따른 분산 서비스 거부 공격의 차단 방법이 적용될 수 있는 네트워크 시스템의 구성을 도시한 도면.

<138> 도 2는 본 발명의 바람직한 일 실시예에 따른 분산 서비스 거부 공격의 차단 방법이 적용되는 순서를 도시한 순서도.

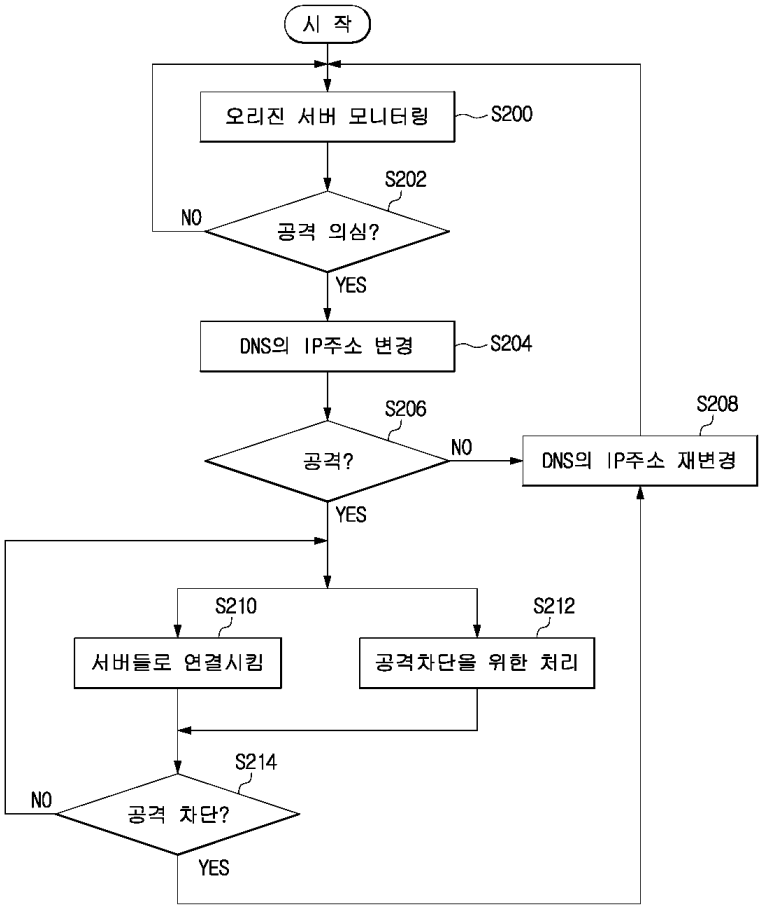
<139> 도 3은 본 발명의 바람직한 일 실시예에 따른 분산 서비스 거부 공격의 차단 방법이 적용되게 하는 공격 판단 장치의 구성을 도시한 도면.

도면

도면1


100a
100b
100c
100n
사용자 1
사용자 2
사용자 3
사용자 n
통신망
110
DNS
120
LB
130
오리진 서버
160
공격 판단 장치
140
서버a
서버b
서버c
서버n
150a
150b
150c
150n

도면2


시 작
오리진 서버 모니터링
S200
S202
NO
공격 의심?
YES
DNS의 IP주소 변경
S204
S206
S208
공격?
NO
DNS의 IP주소 재변경
YES
S210
S212
서버들로 연결시킴
공격차단을 위한 처리
S214
NO
공격 차단?
YES

도면3