(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2014년11월14일
(11) 등록번호 10-1460651
(24) 등록일자 2014년11월05일

(51) 국제특허분류(Int. Cl.)
H04L 12/26 (2006.01) *H04L 12/22* (2006.01)
(21) 출원번호 10-2013-0054530
(22) 출원일자 2013년05월14일
심사청구일자 2013년05월14일
(56) 선행기술조사문헌
KR1020110132797 A*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
고려대학교 산학협력단

(72) 발명자
이희조

알리예브 라샤드

(뒷면에 계속)

(74) 대리인
특허법인엠에이피에스

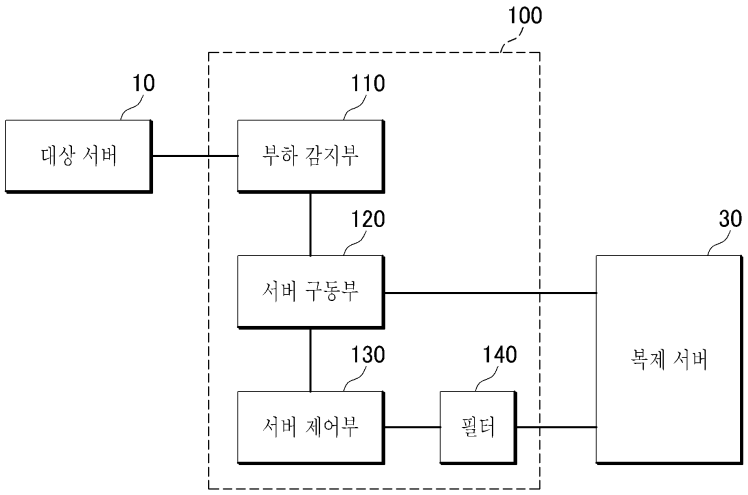
전체 청구항 수 : 총 12 항 심사관 : 석상문

(54) 발명의 명칭 **클라우드 컴퓨팅 기반 서버 부하 분산 장치 및 방법**

(57) 요 약

부하 분산 장치가 대상 서버의 트래픽 또는 부하를 처리시, 대상 서버의 부하량을 모니터링하고 트래픽 집중 현상이 발생하는지 판단하고, 대상 서버에 트래픽 집중 현상이 발생하면, 클라우드 기술로 구현된 복제 서버를 구동하고, 복제 서버로 부하를 분산시킨다.

대 표 도 - 도3



(72) 발명자
서동원

밀번 존

특허청구의 범위

청구항 1

대상 서버의 부하를 분산시키는 장치에 있어서,

대상 서버의 부하량을 모니터링하고 부하량이 기설정된 임계값을 초과하는지 판단하는 부하 감지부;

상기 부하량이 상기 임계값을 초과하는 경우 복제 서버를 구동하는 서버 구동부;

상기 복제 서버가 구동되면, 상기 복제 서버로 부하를 분산시키는 서버 제어부; 및

상기 복제 서버로 분산될 트래픽 중 악성 코드에 의한 트래픽을 처리하는 필터를 포함하되,

상기 복제 서버는 클라우드 기술로 구현된 것인 부하 분산 장치.

청구항 2

제 1 항에 있어서,

상기 서버 구동부는,

상기 대상 서버의 전체 콘텐츠가 복사된 전체 복제 서버를 구동하는 부하 분산 장치.

청구항 3

제 1 항에 있어서,

상기 서버 구동부는,

사용자로부터 일정 횟수 이상으로 반복적으로 요청된 콘텐츠가 상기 대상 서버로부터 복사된 관심 기반 복제 서버를 구동하는 부하 분산 장치

청구항 4

제 1 항에 있어서,

상기 서버 구동부는,

콘텐츠의 타입 별로 상기 대상 서버로부터 복사된 콘텐츠 타입 복제 서버를 구동하는 부하 분산 장치.

청구항 5

제 1 항에 있어서,

상기 서버 제어부는,

DNS 라운드 로빈 방식을 이용하여 부하를 분산하는 DNS 분산 기법, 또는 일정한 확률로 선택된 패킷을 지정된 대상으로 전달하는 스위치 기반 분산 기법을 이용하여 상기 대상 서버의 부하를 분산시키는 부하 분산 장치.

청구항 6

삭제

청구항 7

제 1 항에 있어서,

상기 서버 구동부는,

상기 부하량이 상기 임계값을 초과하지 않는 경우 구동된 상기 복제 서버를 비활성화시키는 부하 분산 장치.

청구항 8

부하 분산 장치가 대상 서버의 부하를 분산하는 방법에 있어서,

대상 서버가 구동되어 서비스가 제공되면 상기 대상 서버의 부하 상황을 모니터링하는 단계;

상기 대상 서버의 부하량이 기설정된 임계값을 초과하면 복제 서버를 활성화시키는 단계;

상기 복제 서버가 활성화되면, 상기 복제 서버에 부하 분산 기법을 활용하여 상기 대상 서버의 부하를 분산시키는 단계; 및

상기 복제 서버로 분산될 트래픽 중 악성 코드에 의한 트래픽을 필터링하는 단계를 포함하되,

상기 복제 서버는 클라우드 기술로 구현된 것인 부하 분산 방법.

청구항 9

제 8 항에 있어서,

상기 복제 서버를 활성화시키는 단계는,

상기 대상 서버의 전체 콘텐츠가 복사된 전체 복제 서버를 활성화시키는 부하 분산 방법.

청구항 10

제 8 항에 있어서,

상기 복제 서버를 활성화시키는 단계는,

사용자로부터 일정 횟수 이상으로 반복적으로 요청된 콘텐츠가 상기 대상 서버로부터 복사된, 관심 기반 복제 서버를 활성화시키는 부하 분산 방법.

청구항 11

제 8 항에 있어서,

상기 복제 서버를 활성화시키는 단계는.

콘텐츠의 타입 별로 상기 대상 서버로부터 복사된 콘텐츠 타입 복제 서버를 활성화 시키고,

상기 부하를 분산시키는 단계는,

상기 콘텐츠의 타입에 따라 상기 대상 서버의 부하를 분산시키는 부하 분산 방법.

청구항 12

제 8 항에 있어서,

상기 부하를 분산시키는 단계는

DNS 라운드 로빈 방식을 이용하여 부하를 분산하는 DNS 분산 기법, 또는 일정한 확률로 선택된 패킷을 지정된 대상으로 전달하는 스위치 기반 분산 기법을 이용하여 부하를 분산시키는 부하 분산 방법.

청구항 13

삭제

청구항 14

제 8 항에 있어서,

상기 대상 서버의 부하량이 상기 임계값을 초과하지 않는 경우 활성화된 상기 복제 서버를 비활성화시키는 단계를 더 포함하는 부하 분산 방법.

명 세 서

기 술 분 야

[0001] 본 발명은 트래픽 과부하 또는 DDoS 공격에 대한 방어 장치 또는 방법에 관한 것으로서, 보다 상세하게는 클라우드 기술을 활용하여 과도한 네트워크 트래픽으로부터 서버를 보호하는 장치 및 방법에 관한 것이다.

배 경 기 술

[0002] 분산 서비스 거부 공격(Distributed-Denial-of-Service attack, 이하에서는 'DDoS 공격'이라고도 함)은 여러 대의 공격자를 분산 배치하여 동시에 동작하게 함으로써 특정 사이트를 공격하는 해킹 방식의 하나이다. 서비스 공격을 위한 도구들을 여러 대의 컴퓨터에 심어놓고 공격 목표인 사이트의 컴퓨터시스템이 처리할 수 없을 정도로 엄청난 분량의 패킷을 동시에 범람시킴으로써 네트워크의 성능을 저하시키거나 시스템을 마비시키는 방식이다.

[0003] 기존 DDoS 공격에 대한 방어 기법은 DDoS 공격의 일정한 규칙을 이용하여 트래픽을 차단하는 데 주력하였다. 하지만, HTTP flood, Slowloris, RUDY와 같은 최근 DDoS 공격 방법은 정상 트래픽 패턴과 유사하므로 이와 같은 규칙을 적용하더라도 많은 양의 악성 트래픽이 여전히 공격 대상 서버에 도달하게 된다. 또한 이러한 규칙 기반의 대응 방법을 이용하는 경우 플래시 크라우드(Flash crowds)와 같은 정상적인 트래픽 집중 현상이 발생할 때도 악성 트래픽으로 오인하는 경우가 발생한다.

[0004] 이와 관련하여, 대한민국 공개 특허 제10-2012-0066465호(발명의 명칭: 서비스 거부 공격 차단 방법)에는 DDoS 공격에 대해 일정한 규칙을 사용하여 트래픽을 차단하는 방법에 관련된 내용이 기술되어 있다.

발명의 내용

해결하려는 과제

[0005] 본 발명은 전술한 종래 기술의 문제점을 해결하기 위한 것으로서, 본 발명의 일부 실시예는 클라우드 복제 서버를 이용하여 대상 서버에 정상 트래픽으로 인한 과부하 또는 DDoS와 같은 공격 상황이 발생하더라도 지속적으로 서비스를 제공할 수 있게 한다.

과제의 해결 수단

[0006] 상술한 기술적 과제를 달성하기 위한 기술적 수단으로서, 본 발명의 제 1 측면에 따른 대상 서버의 부하를 분산하는 장치는, 대상 서버의 부하량을 모니터링하고 부하량이 기설정된 임계값을 초과하는지 판단하는 부하 감지부; 상기 부하량이 상기 임계값을 초과하는 경우 복제 서버를 구동하는 서버 구동부; 및 상기 복제 서버가 구동되면, 상기 복제 서버로 부하를 분산시키는 서버 제어부를 포함하되, 상기 복제 서버는 클라우드 기술로 구현된다.

[0007] 또한, 본 발명의 제 2 측면에 따른, 대상 서버의 부하를 분산하는 방법은, 대상 서버가 구동되어 서비스가 제공되면 상기 대상 서버의 부하 상황을 모니터링하는 단계; 상기 대상 서버의 부하량이 기설정된 임계값을 초과하면 복제 서버를 활성화시키는 단계; 및 상기 복제 서버가 활성화되면, 상기 복제 서버에 부하 분산 기법을 활용하여 상기 대상 서버의 부하를 분산시키는 단계를 포함하되, 상기 복제 서버는 클라우드 기술로 구현된다.

발명의 효과

[0008] 전술한 본 발명의 과제 해결 수단에 의하면, 공격 대상 서버의 성능이 DDoS 공격 및 트래픽 과부하로 인해 저하되지 않고, 서비스 제공자의 지속적인 서비스 제공이 가능하다.

[0009] 또한, 전술한 본 발명의 과제 해결 수단에 의하면, 트래픽 과부하 상황에서 정상 사용자를 악성 사용자로 오인하여 대상 서버의 서비스 공급을 중단시키는 오탐이 발생하지 않는다.

도면의 간단한 설명

[0010] 도 1은 종래의 DDoS 방어 방법인 필터 전파 방법을 설명하기 위한 도면이다.

도 2는 본원 발명의 일 실시예에 따른 부하 분산 장치의 동작 개념을 설명하기 위한 도면이다.

도 3은 본 발명의 일 실시예에 따른, 대상 서버의 부하 분산 장치의 상세 구성을 도시한 도면이다.

도 4는 본 발명의 일 실시예에 따른 서버 제어부가 트래픽 또는 부하를 분산시키는 시스템 구축 예를 도시한다.

도 5는 본 발명의 일 실시예에 따른, 부하 분산 장치가 대상 서버의 트래픽 또는 부하를 분산시키는 방법에 대한 순서도이다.

발명을 실시하기 위한 구체적인 내용

[0011] 아래에서는 첨부한 도면을 참조하여 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 본 발명의 실시예를 상세히 설명한다. 그러나 본 발명은 여러 가지 상이한 형태로 구현될 수 있으며 여기에서 설명하는 실시예에 한정되지 않는다. 그리고 도면에서 본 발명을 명확하게 설명하기 위해서 설명과 관계없는 부분은 생략하였으며, 명세서 전체를 통하여 유사한 부분에 대해서는 유사한 도면 부호를 붙였다.

[0012] 명세서 전체에서, 어떤 부분이 다른 부분과 "연결"되어 있다고 할 때, 이는 "직접적으로 연결"되어 있는 경우뿐 아니라, 그 중간에 다른 소자를 사이에 두고 "전기적으로 연결"되어 있는 경우도 포함한다. 또한 어떤 부분이 어떤 구성요소를 "포함"한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성요소를 더 포함할 수 있는 것을 의미한다.

[0013] 본원 명세서 전체에서, 어떤 부분이 어떤 구성요소를 "포함" 한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성 요소를 더 포함할 수 있는 것을 의미한다. 본원 명세서 전체에서 사용되는 정도의 용어 "~(하는) 단계" 또는 "~의 단계"는 "~ 를 위한 단계"를 의미하지 않는다.

[0014] 본원 명세서 전체에서, "트래픽" 이라고 함은, 특별히 반대되는 기재가 없는 한, 어떤 통신장치나 시스템에 걸리는 부하를 의미한다.

[0015] 도 1은 종래의 DDoS 방어 방법인 필터 전파 방법을 설명하기 위한 도면이다.

[0016] 종래의 DDoS 방어 방법으로, 필터 전파 방법은 방화벽이나 IDS/IPS (Intrusion Detection/Protection System) 등을 설치하여 공격 대상 서버를 방어하는 것에 집중되어 있었다.

[0017] 그러나, 정상 상황과 비슷한 유형의 신종 악성 공격 현상이나, 정상적이면서 일시적으로 트래픽이 집중되는 현상이 발생할 경우, 과도한 트래픽이 대상 서버에 집중되어 서버의 서비스 장애의 원인이 된다.

[0018] 도 2는 본원 발명의 일 실시예에 따른 부하 분산 장치의 동작 개념을 설명하기 위한 도면이다. 종래의 방법은 사용자로부터 대상 서버까지의 경로가 제한되어 있지만, 본 발명에서는 여러 곳에 분산된 복제 서버가 대상 서버의 서비스를 대신 제공해 주기 때문에 사용자로부터 대상 서버까지의 경로가 다변화되며, 대부분의 트래픽은 대상 서버까지 도달하지 않는다.

[0019] 이러한 종래의 문제점을 해결하기 위해, 본 발명은 클라우드 기술을 활용하여 대상 서버와 같은 기능을 수행하는 복제 서버를 구축하고, 과도한 트래픽이 대상 서버로 집중될 시에는 복제 서버로 트래픽을 분산시킴으로써 지속적인 서비스를 가능하게 한다.

[0020] 도 3은 본 발명의 일 실시예에 따른, 대상 서버의 부하 분산 장치의 상세 구성을 도시한 도면이다.

[0021] 부하 분산 장치(100)는 부하 감지부(110), 서버 구동부(120), 서버 제어부(130) 및 필터(140)를 포함한다.

[0022] 부하 감지부(110)는, 대상 서버(10)의 부하량을 모니터링하고, 대상 서버(10)에 트래픽 집중 현상이 나타났는지 판단한다. 본 발명의 일 실시예에 따른 부하 감지부(110)는, 트래픽 집중 현상 판단 시, 대상 서버(10)의 부하량이 기설정된 임계값을 초과하는지로 판단할 수 있다. 이때, 본 발명의 일 실시예에 따라, 임계값은 서비스 제공자가 설정할 수 있는데, 여러 대의 공격자를 분산 배치하여 동시에 '서비스 거부 공격(Denial of Service attack, DoS)'을 함으로써 시스템이 더는 정상적 서비스를 제공할 수 없게 하는, DDoS 공격 상황에 대비하여 임계값을 설정할 수 있다. 이외에도 서비스 제공자는 사용자에게 보다 품질 높은 서비스를 제공하기 위해 일정 수준 이상의 부하량을 감지하도록 임계값을 낮게 설정할 수도 있다.

[0023] 한편, 서버 구동부(120)는, 트래픽 집중 현상이 발생하면 부하를 분산시키기 위한 복제 서버(30)를 구동한다.

[0024] 그리고, 서버 제어부(130)는, 서버 구동부(120)의 동작에 따라 복제 서버(30)가 구동되면, 복제 서버(30)로 트래픽 또는 부하를 분산시킨다.

[0025] 이때, 본 발명의 복제 서버(30)는 클라우드 컴퓨팅 기술로 구현될 수 있다. 그러나 복제 서버(30)는 반드시 클라우드 컴퓨팅 기술로 구현되어야 하는 것은 아니고 별도의 내부 또는 외부의 리소스로 구성되는 것도 가능하다. 클라우드 컴퓨팅은 서로 다른 물리적인 위치에 존재하는 컴퓨터들의 자원을 가상화 기술로 통합해

제공하는 기술로, 복제 서버(30)의 자원을 효율적으로 사용할 수 있게 한다. 본 발명은 가상 공간에 있는 서버의 자원을 이용하여 복제 서버(30)를 구축할 수 있도록 한다.

[0026] 이때, 상술한 서버 구동부(120)가 구동하는 본 발명의 복제 서버(30)는 구축 방식에 따라 세 가지로 세분화된다.

[0027] 먼저, 복제 서버(30)는 대상 서버(10)의 전체 콘텐츠를 복제 서버에 복사하는 형태로 구성될 수 있다. 복제소요시간이 오래 걸리고, 저장장치의 자원이 많이 요구되지만, 사용자에게 가장 안정적인 서비스를 제공할 수 있다.

[0028] 다음으로, 사용자의 요청이 빈번한 특정 콘텐츠를 복제 서버에 복사하는 형태로 복제 서버가 구성될 수 있다. 이와 같은 관심기반 복제 서버는 사용자 요청이 빈번한 콘텐츠 인지 여부를 콘텐츠에 대한 사용자의 요청 횟수에 기반하여 판단할 수 있다. 관심 기반 복제 서버는 상대적으로 적은 자원이 요구되지만, 서비스 제공자는 어떤 콘텐츠에 사용자들이 관심을 두는지 모니터링 해야 하고, 이에 따라 복제 서버의 콘텐츠를 갱신해야 한다.

[0029] 다음으로, 콘텐츠 타입 기반 복제 서버는 멀티미디어 파일, 문서 파일, 사용자 파일 등으로 콘텐츠의 타입을 나누어 콘텐츠를 복제 서버에 저장한다. 즉, 한 복제 서버는 하나 이상의 콘텐츠 타입을 담당하게 된다. 이 때, 콘텐츠 타입이란, 콘텐츠의 파일 형식이 될 수 있고, 기설정된 콘텐츠의 분류가 될 수도 있다.

[0030] 한편, 서버 제어부(130)가 상술한 복제 서버(30)에 트래픽 또는 부하를 분산시키는 방법으로 다음과 같은 방법이 사용될 수 있다.

[0031] 우선, DNS 기반 부하 분산 방법은, DNS 라운드 로빈(DNS Round Robin)이라는 기법을 상황에 따라 동적으로 활용한다. DNS 라운드 로빈이란, DNS(Domain Name System)를 이용하여 하나의 서비스를 여러 대의 서버에 분산시키는 방식을 말한다. 예를 들어 www.example.com에 대한 서비스를 1.1.1.1이라는 IP를 소유한 서버가 담당하고 있었다면, 과도한 트래픽이 집중될 시에는 1.1.1.2, 1.1.1.3등의 복제 서버(30) IP를 해당 도메인의 담당 서버로 추가 등록하여 사용자의 트래픽이 복제 서버(30)로 분산될 수 있도록 한다.

[0032] 한편, 스위치 기반 부하 분산 방법은, 네트워크 스위치에는 특정 IP 영역을 근원지 IP로 가지는 패킷 혹은 일정 확률로 선택된 패킷을 지정된 대상으로 전달하는 기능이 있는데, 이 기능을 활용하여 복제 서버(30)로 트래픽이 분산되도록 설정하는 방식이다.

[0033] 도 4는 본 발명의 일 실시예에 따른 서버 제어부(130)가 트래픽 또는 부하를 분산시키는 시스템 구축 예를 보여준다. www1은 웹서버이고, www2와 www3는 www1과 같은 기능을 수행하는 복제 서버이다. User들로부터 www1으로 향하는 트래픽은 DNS 라운드 로빈과 Switch의 패킷 전달 기능에 의하여 www2와 www3로 분산될 수 있다.

[0034] 이때, 네트워크는 근거리 통신망(Local Area Network, LAN), 역 통신망(Wide Area Network, WAN) 또는 부가가치 통신망(Value Added Network, VAN) 등과 같은 유선 네트워크나 이동 통신망(mobile radio communication network) 또는 위성 통신망 등과 같은 모든 종류의 무선 네트워크로 구현될 수 있다.

[0035] 한편, 본 발명은 필터(140)를 더 포함할 수 있는데, 본 발명의 일 실시예에 따른 필터는 서버 제어부(130)에 의해 상기 복제 서버로 분산될 트래픽 중 악성 코드에 의한 트래픽을 처리하는 구성요소이다. 필터(140)는 대상 서버(10)가 악성코드에 의한 공격을 받으면, 복제 서버로 트래픽을 분산시키는 것 이외에도 악성코드에 대한 별도의 처리를 하기 위한 구성요소다.

[0036] 한편, 본 발명의 일 실시예에 따른 서버 구동부(130)는, 트래픽 집중 현상이 종료되면, 즉 부하량이 기설정된 임계값을 초과하지 않는 경우 복제 서버(30)를 비활성화시킬 수 있다.

[0037] 도 5는 본 발명의 일 실시예에 따른, 부하 분산 장치가 대상 서버의 트래픽 또는 부하를 분산시키는 방법에 대한 순서도이다.

[0038] 우선, 부하 분산 장치는 대상 서버가 구동되어 서비스가 제공되면 대상 서버의 부하 상황을 모니터링 한다(S410).

[0039] 이어서, DDoS 공격 상황, 또는 특정 사건이나 발표 이후에 관련 사이트에 접속하는 사람들이 갑자기 늘어나는 플래시 크라우드(Flash crowds) 현상과 같은 정상적인 트래픽 집중 현상 등이 발생하면 복제 서버를 활성화한다(S420).

[0040] 본 발명의 일 실시예에 따르면, 트래픽 집중 현상이 나타난 것인지는 대상 서버의 부하량이 기설정된 임계값을 초과하는지로 판단할 수 있다.

[0041] 한편, 활성화되는 본 발명의 복제 서버는 구축 방식에 따라 세 가지로 세분화될 수 있는데, 전체 복제 서버, 관심 기반 복제 서버 및 콘텐츠 타입 기반 복제 서버가 그 실시예다.

[0042] 먼저, 복제 서버는 대상 서버의 전체 콘텐츠를 복제 서버에 복사하는 형태로 구성될 수 있다. 복제소요시간이 오래 걸리고, 저장장치의 자원이 많이 요구되지만, 사용자에게 가장 안정적인 서비스를 제공할 수 있다.

[0043] 다음으로, 사용자의 요청이 빈번한 특정 콘텐츠를 복제 서버에 복사하는 형태로 복제 서버가 구성될 수 있다. 이와 같은 관심 기반 복제 서버는 사용자 요청이 빈번한 콘텐츠 인지 여부를 콘텐츠에 대한 사용자의 요청 횟수에 기반하여 판단할 수 있다. 관심 기반 복제 서버는 상대적으로 적은 자원이 요구되지만, 서비스 제공자는 어떤 콘텐츠에 사용자들이 관심을 두는지 모니터링 해야 하고, 이에 따라 복제 서버의 콘텐츠를 갱신해야 한다.

[0044] 이러한 관심 기반 복제 서버로 복제 서버를 구성하는 경우, 복제 서버를 활성화시키는 단계(S420) 이전에, 사용자의 요청 콘텐츠가 상기 관심 기반 복제 서버에 복사된 콘텐츠인지 확인하는 단계를 더 포함할 수 있다. 이는 본 발명이 사용자가 관심을 두는 콘텐츠 요청에 의한 부하를 복제 서버에 재분배하기 위함이다.

[0045] 다음으로, 콘텐츠 타입 기반 복제 서버는 멀티미디어 파일, 문서 파일, 사용자 파일 등으로 콘텐츠의 타입을 나누어 콘텐츠를 복제 서버에 저장한다. 즉 한 복제 서버는 하나 이상의 콘텐츠 타입을 담당하게 된다. 이 때, 콘텐츠 타입이란, 콘텐츠의 파일 형식이 될 수 있고, 기설정된 콘텐츠의 분류가 될 수도 있다.

[0046] 이러한 콘텐츠 타입 기반 복제 서버로 복제 서버를 구성하는 경우, 복제 서버를 활성화시키는 단계(S420) 이전에, 사용자의 요청 콘텐츠의 타입을 확인하는 단계를 더 포함할 수 있고, 본 발명은 후에 설명할 부하를 분산시키는 단계(S430)에서 타입에 따라 상기 대상 서버의 부하를 분산시킬 수 있다. 이는 사용자의 콘텐츠의 타입에 따라 각각 다른 복제 서버로 부하를 재분배하기 위함이다.

[0047] 이때, 본 발명의 복제 서버(30)는 클라우드 컴퓨팅 기술로 구현될 수 있다. 그러나 복제 서버(30)는 반드시 클라우드 컴퓨팅 기술로 구현되어야 하는 것은 아니고 별도의 내부 또는 외부의 리소스로 구성되는 것도 가능하다. 클라우드 컴퓨팅은 서로 다른 물리적인 위치에 존재하는 컴퓨터들의 자원을 가상화 기술로 통합해 제공하는 기술로, 복제 서버(30)의 자원을 효율적으로 사용할 수 있게 한다. 본 발명은 가상 공간에 있는 서버의 자원을 이용하여 복제 서버를 구축할 수 있도록 한다.

[0048] 이어서, 부하 분산 기법을 활용하여 부하를 분산시킨다(S430). 이때, 부하를 분산시키는 방법으로 다음과 같은 방법이 사용될 수 있다.

[0049] 우선, DNS 기반 부하 분산 방법이 있는데, 이 방법은 DNS 라운드 로빈(DNS Round Robin)이라는 기법을 상황에 따라 동적으로 활용한다. DNS 라운드 로빈 방식을 이용하면, DNS(Domain Name System)를 이용하여 하나의 서비스를 여러 대의 서버에 분산시킬 수 있다.

[0050] 또한, 스위치 기반 부하 분산 방법이 있는데, 네트워크 스위치에 있는 특정 IP 영역을 근원지 IP로 가지는 패킷 혹은 일정 확률로 선택된 패킷을 지정된 대상으로 전달하는 이 방법의 기능을 활용하여 복제 서버로 트래픽이 분산되도록 설정할 수 있다.

[0051] 이어서, 본 발명의 일 실시예에 따르면, 필터를 사용하여 알려진 악성 트래픽에 대한 처리를 결정할 수 있다(S440).

[0052] 이어서, 본 발명의 일 실시예에 따르면, 대상 서버의 부하 상황은 지속적으로 모니터링 되며 대상 서버의 트래픽 과부하 상황이 종료되면 복제 서버가 비활성화된다(S450).

[0053] 이러한 부하 분산 장치 또는 부하 분산 방법을 이용하는 경우, 공격 대상 서버의 성능이 DDoS 공격 및 트래픽 과부하로 인해 저하되지 않고, 서비스 제공자의 지속적인 서비스 제공이 가능하다. 또한 트래픽 과부하 상황에서 정상 사용자를 악성 사용자로 오인하여 대상 서버의 서비스 공급을 중단시키는 오탐이 발생하지 않을 것이다.

[0054] 참고로, 본 발명의 실시예에 따른 도 3에 도시된 구성 요소들은 소프트웨어 또는 FPGA(Field Programmable Gate Array) 또는 ASIC(Application Specific Integrated Circuit)와 같은 하드웨어 구성 요소를 의미하며, 소정의

역할들을 수행한다.

[0055] 그렇지만 '구성 요소들'은 소프트웨어 또는 하드웨어에 한정되는 의미는 아니며, 각 구성 요소는 어드레싱할 수 있는 저장 매체에 있도록 구성될 수도 있고 하나 또는 그 이상의 프로세서들을 재생시키도록 구성될 수도 있다.

[0056] 따라서, 일 예로서 구성 요소는 소프트웨어 구성 요소들, 객체지향 소프트웨어 구성 요소들, 클래스 구성 요소들 및 태스크 구성 요소들과 같은 구성 요소들과 프로세스들, 함수들, 속성들, 프로시저들, 서브루틴들, 프로그램 코드의 세그먼트들, 드라이버들, 펌웨어, 마이크로 코드, 회로, 데이터, 데이터베이스, 데이터 구조들, 테이블들, 어레이들 및 변수들을 포함한다.

[0057] 구성 요소들과 해당 구성 요소들 안에서 제공되는 기능은 더 작은 수의 구성 요소들로 결합되거나 추가적인 구성 요소들로 더 분리될 수 있다.

[0058] 본 발명의 일 실시예는 컴퓨터에 의해 실행되는 프로그램 모듈과 같은 컴퓨터에 의해 실행 가능한 명령어를 포함하는 기록 매체의 형태로도 구현될 수 있다. 컴퓨터 판독 가능 매체는 컴퓨터에 의해 액세스될 수 있는 임의의 가용 매체일 수 있고, 휘발성 및 비휘발성 매체, 분리형 및 비분리형 매체를 모두 포함한다. 또한, 컴퓨터 판독가능 매체는 컴퓨터 저장 매체 및 통신 매체를 모두 포함할 수 있다. 컴퓨터 저장 매체는 컴퓨터 판독가능 명령어, 데이터 구조, 프로그램 모듈 또는 기타 데이터와 같은 정보의 저장을 위한 임의의 방법 또는 기술로 구현된 휘발성 및 비휘발성, 분리형 및 비분리형 매체를 모두 포함한다. 통신 매체는 전형적으로 컴퓨터 판독 가능 명령어, 데이터 구조, 프로그램 모듈, 또는 반송파와 같은 변조된 데이터 신호의 기타 데이터, 또는 기타 전송 메커니즘을 포함하며, 임의의 정보 전달 매체를 포함한다.

[0059] 상술한 본 발명에 따른 부하 분산 장치 및 방법은 컴퓨터로 읽을 수 있는 기록 매체에 컴퓨터가 읽을 수 있는 코드로서 구현되는 것이 가능하다. 컴퓨터가 읽을 수 있는 기록매체로는 컴퓨터 시스템에 의하여 해독될 수 있는 데이터가 저장된 모든 종류의 기록 매체를 포함한다. 예를 들어, ROM(Read Only Memory), RAM(Random Access Memory), 자기 테이프, 자기 디스크, 플래시 메모리, 광 데이터 저장장치 등이 있을 수 있다. 또한, 컴퓨터가 읽을 수 있는 기록매체는 컴퓨터 통신망으로 연결된 컴퓨터 시스템에 분산되어, 분산방식으로 읽을 수 있는 코드로서 저장되고 실행될 수 있다.

[0060] 본 발명의 장치 및 방법은 특정 실시예와 관련하여 설명되었지만, 그것들의 구성 요소 또는 동작의 일부 또는 전부는 범용 하드웨어 아키텍쳐를 갖는 컴퓨터 시스템을 사용하여 구현될 수 있다.

[0061] 전술한 본 발명의 설명은 예시를 위한 것이며, 본 발명이 속하는 기술분야의 통상의 지식을 가진 자는 본 발명의 기술적 사상이나 필수적인 특징을 변경하지 않고서 다른 구체적인 형태로 쉽게 변형이 가능하다는 것을 이해할 수 있을 것이다. 그러므로 이상에서 기술한 실시예들은 모든 면에서 예시적인 것이며 한정적이 아닌 것으로 이해해야만 한다. 예를 들어, 단일형으로 설명되어 있는 각 구성 요소는 분산되어 실시될 수도 있으며, 마찬가지로 분산된 것으로 설명되어 있는 구성 요소들도 결합된 형태로 실시될 수 있다.

[0062] 본 발명의 범위는 상기 상세한 설명보다는 후술하는 특허청구범위에 의하여 나타내어지며, 특허청구범위의 의미 및 범위 그리고 그 균등 개념으로부터 도출되는 모든 변경 또는 변형된 형태가 본 발명의 범위에 포함되는 것으로 해석되어야 한다.

부호의 설명

[0063] 10: 대상 서버

30: 복제 서버

100: 부하 분산 장치

110: 부하 감지부

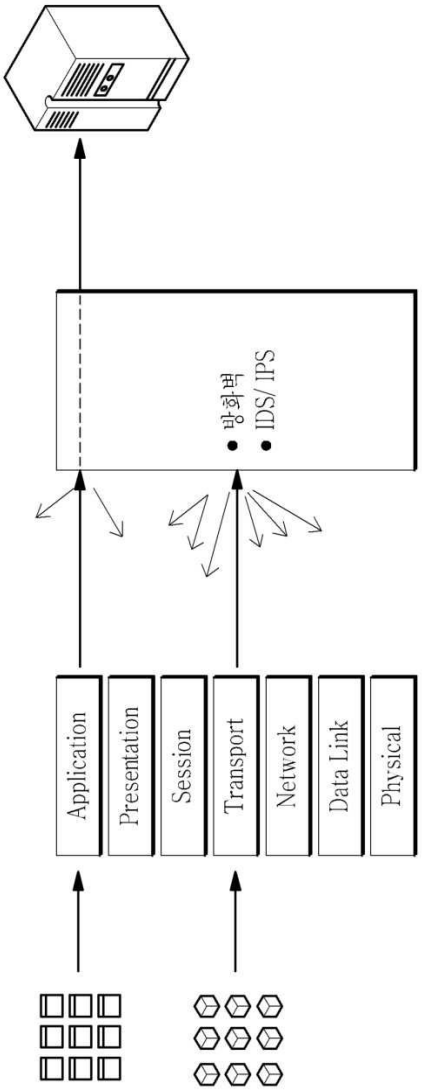
120: 서버 구동부

130: 서버 제어부

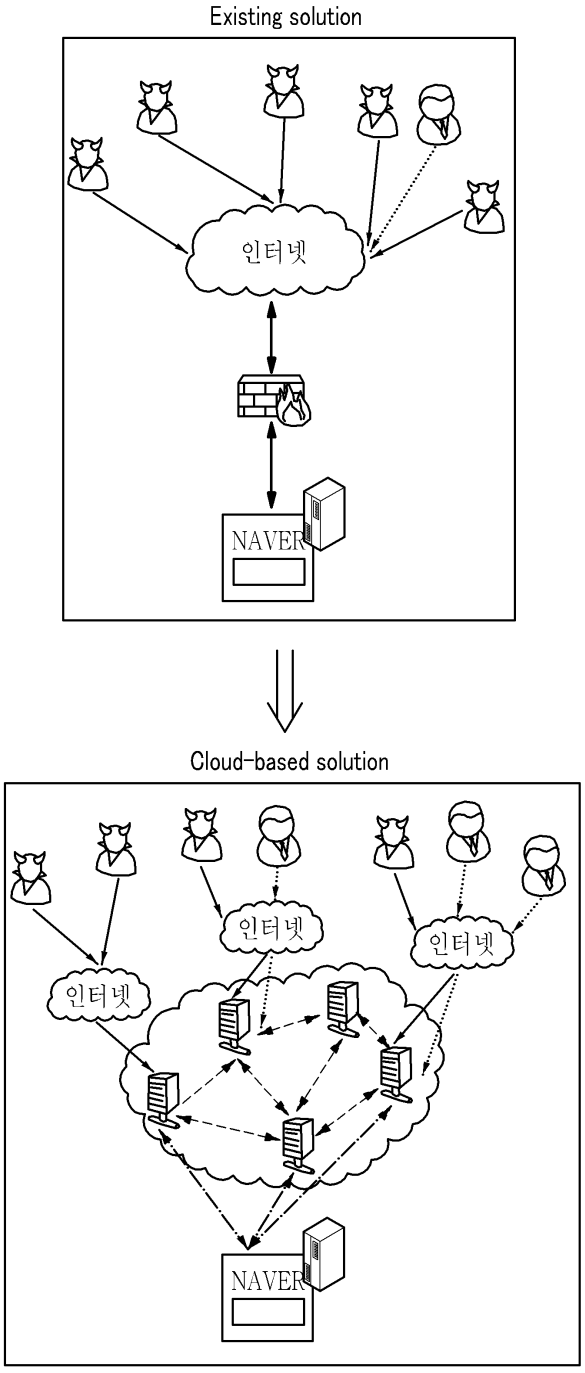
140: 필터

도면

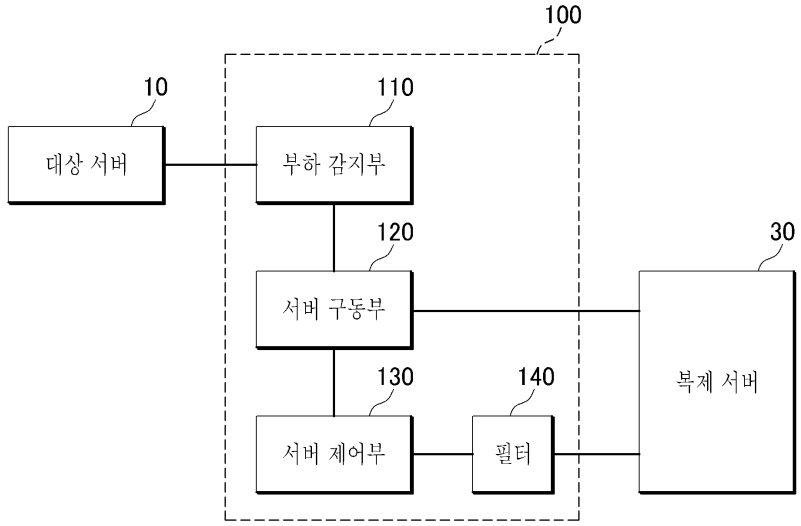
도면1


방화벽
IDS/ IPS
Application
Presentation
Session
Transport
Network
Data Link
Physical

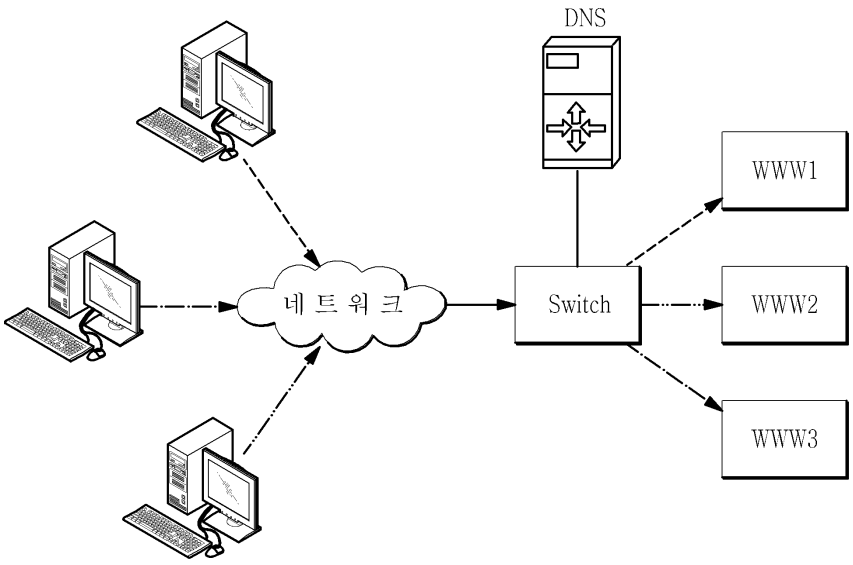
도면2


Existing solution
인터넷
NAVER
Cloud-based solution
인터넷
인터넷
인터넷
NAVER

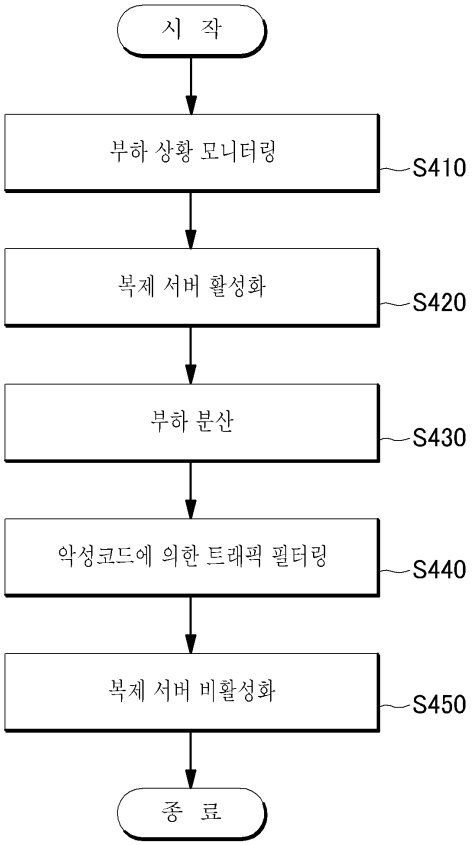
도면3


100
10
110
대상 서버
부하 감지부
120
30
서버 구동부
복제 서버
130
140
서버 제어부
필터

도면4


DNS
WWW1
네 트 워 크
Switch
WWW2
WWW3

도면5


시 작
부하 상황 모니터링
S410
복제 서버 활성화
S420
부하 분산
S430
악성코드에 의한 트래픽 필터링
S440
복제 서버 비활성화
S450
종 료