(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2020년12월07일
(11) 등록번호 10-2187136
(24) 등록일자 2020년11월30일

(51) 국제특허분류(Int. Cl.)
H04L 12/22 (2006.01) *H04L 12/26* (2006.01)
(21) 출원번호 10-2014-0021855
(22) 출원일자 2014년02월25일
심사청구일자 2019년02월25일
(65) 공개번호 10-2015-0100267
(43) 공개일자 2015년09월02일
(56) 선행기술조사문헌
JP2005210513 A*
KR1020060093306 A*
KR1020110016640 A*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
주식회사 케이티
고려대학교 산학협력단
(72) 발명자
정현호
리샤드 알리예프
(뒷면에 계속)
(74) 대리인
특허법인충정

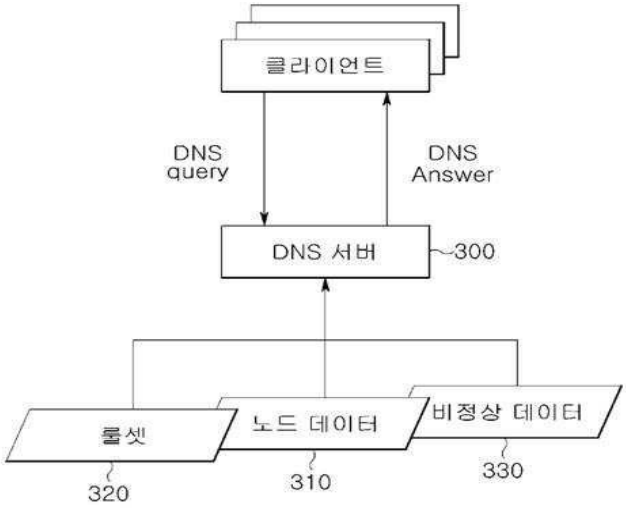
전체 청구항 수 : 총 10 항 심사관 : 나용수

(54) 발명의 명칭 **트래픽 격리를 위한 디엔에스 백엔드 프로세싱 및 그 장치**

(57) 요 약

클라이언트 트래픽 격리에 의해 트래픽을 클라우드 기반 서버로 분산하는 장치 및 방법이 개시된다. 본 발명은 클라이언트의 DNS 질의에 응답하여, 상기 DNS 질의에 대응하는 서버의 복수의 IP 주소 중 선택적 IP 주소를 제공하는 DNS 서버에 있어서, 상기 DNS 서버가 상기 클라이언트의 DNS 질의에 관련된 복수의 서버의 노드 데이터; 및 상기 클라이언트의 IP 주소에 따라 상기 DNS 질의에 관련된 상기 서버 노드의 IP 주소에 대한 DNS 응답을 제공하기 위한 룰 셋을 구비하는 것을 특징으로 한다. 본 발명에 따르면, 클라이언트 그룹별로 상이한 DNS 응답 정책을 적용할 수 있게 한다. 이에 따라, 클라이언트 서비스 그룹별로 상이한 서비스 서버로 트래픽을 격리함으로써 정상적인 사용자에게 원활한 서비스를 제공할 수 있게 된다.

대 표 도 - 도6



(72) 발명자
김봉기

서동원

이시형

이희조

황영헌

명 세 서

청구범위

청구항 1

클라이언트의 DNS 질의에 응답하여, 상기 DNS 질의에 대응하는 메인서버 및 복제서버의 IP 주소 중 선택적 IP 주소를 제공하는 DNS 서버에 있어서,

상기 DNS 서버는,

상기 클라이언트의 IP주소가 속하는 그룹에 따라, 선별적으로 상기 클라이언트의 상기 메인서버로의 접속을 차단하는 트래픽 격리 모드로 동작하고,

상기 DNS 서버는,

상기 클라이언트의 DNS 질의에 대한 DNS 응답을 위해, 상기 메인서버 및 복제서버의 IP 주소를 포함하는 노드 데이터; 및

상기 클라이언트의 IP 주소에 따라 상기 클라이언트가 속하는 그룹을 판별하고, 상기 그룹에 대응하는 메인서버 또는 복제서버의 IP 주소를 상기 DNS 응답으로 제공하기 위한 룰 셋을 구비하는 것을 특징으로 하는 DNS 서버.

청구항 2

삭제

청구항 3

제1항에 있어서,

상기 클라이언트의 DNS 질의에 대하여 상기 메인서버의 IP 주소를 응답하는 디폴트 모드를 더 포함하는 것을 특징으로 하는 DNS 서버.

청구항 4

제1항에 있어서,

상기 노드 데이터는,

상기 메인서버 및 복제서버의 ID와 IP주소를 각각 대응시킨 것을 특징으로 하는 DNS 서버.

청구항 5

제1항에 있어서,

상기 룰 셋은,

상기 클라이언트의 IP 주소에 대응하는 상기 메인 서버 또는 복제서버의 IP 주소를, 상기 DNS 응답으로 제공하는 스크립트를 포함하는 것을 특징으로 하는 DNS 서버.

청구항 6

제1항에 있어서,

상기 클라이언트가 속하는 그룹은, 트래픽 혼잡시 상기 메인서버로의 접속 우선 순위에 따라 분류되는 것을 특

징으로 하는 DNS 서버.

청구항 7

클라이언트의 DNS 질의에 응답하여, 상기 DNS 질의에 대응하는 서버의 복수의 IP 주소 중 선택적 IP 주소를 제공하는 DNS 서버에 있어서,

상기 DNS 서버는,

상기 클라이언트의 DNS 질의에 관련된 복수의 서버의 노드 데이터; 및

상기 클라이언트의 IP 주소에 따라 상기 DNS 질의에 관련된 상기 서버의 IP 주소에 대한 DNS 응답을 제공하기 위한 룰 셋을 구비하는 것으로,

상기 룰 셋은

복수의 그룹으로 그룹화된 상기 클라이언트에 대하여 상기 서버를 대응시킨 것이고,

상기 노드 데이터는 메인서버 및 복제서버에 대한 데이터를 포함하며,

상기 클라이언트의 DNS 질의에 대하여 상기 메인서버의 IP 주소를 응답하는 디폴트 모드; 및

상기 클라이언트의 DNS 질의에 대한 응답으로서, 상기 클라이언트의 IP가 속한 그룹에 따라 선별적으로 상기 클라이언트의 상기 메인서버로의 접속을 차단하는 트래픽 격리 모드로 동작하고,

상기 복수의 그룹은 트래픽 혼잡시 상기 메인서버로의 접속 우선 순위에 따라 분류되는 것으로,

상기 복수의 그룹은,

상기 메인서버로의 최우선 접속을 보장하는 제1 그룹;

상기 메인서버로의 접속을 차단하는 제2 그룹; 및

최소한 상기 복제서버로의 접속을 보장하는 제3 그룹을 포함하는 것을 특징으로 하는 DNS 서버.

청구항 8

제7항에 있어서,

상기 제3 그룹은,

상기 클라이언트의 IP 주소가 상기 메인서버 또는 복제서버로의 과거 접속 이력이 있는가 여부에 따라 구분되는 것을 특징으로 하는 DNS 서버.

청구항 9

제7항에 있어서,

상기 제3 그룹은,

상기 클라이언트의 IP 주소가 상기 메인서버 또는 복제서버로의 과거 접속 이력이 있는 IP 주소와 IP 접두어가 동일한가 여부에 따라 구분되는 것을 특징으로 하는 DNS 서버.

청구항 10

제1항에 있어서,

상기 DNS 서버는 PDNS로 구현되는 것을 특징으로 하는 DNS 서버.

청구항 11

DNS 서버에 도메인 네임에 대응하는 메인서버, 복제서버 및 검역서버를 포함하는 복수의 서버에 대한 노드 데이터를 입력하는 단계;

상기 DNS 서버에 클라이언트의 IP 주소와, 상기 클라이언트 IP 주소에 대응하여 응답되어야 할 상기 복수의 서버에 관한 룰 셋을 입력하는 단계;

네트워크 트래픽이 비정상 상태임을 통보 받는 경우, 상기 클라이언트의 IP주소가 속하는 그룹에 따라, 선별적으로 상기 클라이언트의 상기 메인서버로의 접속을 차단하는 트래픽 격리 모드로 동작하고, 상기 노드 데이터 및 상기 룰 셋에 기초하여, 클라이언트의 DNS 질의에 대한 응답으로 상기 클라이언트의 IP 주소에 대응하는 상기 서버의 IP 주소를 제공하도록 설정하는 단계; 및

상기 설정에 따라 클라이언트의 DNS 질의에 대하여 응답하는 단계를 포함하는 것으로,

상기 노드 데이터는

상기 클라이언트의 DNS 질의에 대한 DNS 응답을 위해, 상기 복수의 서버들의 IP 주소를 포함하고,

상기 룰 셋은

상기 클라이언트의 IP 주소에 따라 상기 클라이언트가 속하는 그룹을 판별하고, 상기 그룹에 대응하는 서버의 IP 주소를 상기 DNS 응답으로 제공하도록 하는 것을 특징으로 하는 DNS 서버의 백엔드 프로세싱 방법.

발명의 설명

기 술 분 야

[0001] 본 발명은 분산 서비스 거부 공격 등의 네트워크 트래픽 및 이로 인한 서버 부하를 관리하기 위한 방법에 관한 것으로서, 보다 상세하게는 클라이언트 트래픽 격리에 의해 트래픽을 클라우드 기반 서버로 분산하는 방법 및 장치에 관한 것이다.

배 경 기 술

[0002] 분산 서비스 거부 공격은 여러 대의 공격자를 분산 배치하여 동시에 동작하게 함으로써 특정 사이트를 공격하는 해킹 방식의 하나이다. 이 방식은 서비스 공격을 위한 도구들을 여러 대의 컴퓨터에 심어놓고 공격 목표인 사이트의 컴퓨터 시스템이 처리할 수 없을 정도로 엄청난 분량의 패킷을 동시에 범람시킴으로써 네트워크의 성능을 저하시키거나 시스템을 마비시키게 된다.

[0003] 기존 DDoS 공격에 대한 방어 기법은 DDoS 공격의 일정한 규칙을 이용하여 트래픽을 차단하여 폐기하는 데 주력하였다. 그러나 최근의 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] 한편, 한국등록특허 제900491호는 오리진 서버를 포함하는 복수의 서버로 구성하고, 오리진 서버의 트래픽 상태가 분산 서비스 거부 공격 상태로 판단되는 경우, 오리진 서버의 IP 주소를 복수의 서버로 IP 주소로 변경하여 오리진 서버의 부하를 경감하는 방식의 대응 방법을 제시하고 있다.

[0005] 그러나, 이와 같은 로드 밸런싱 기반의 트래픽 우회 메커니즘은 트래픽 혼잡시 정상적인 사용자들에게 지속적인 서비스를 보장하기가 어렵다.

발명의 내용

해결하려는 과제

[0006] 상기 종래 기술의 문제점을 해결하기 위하여 본 발명은 로드 밸런싱 기반이 아닌 트래픽 격리(Traffic Isolation) 기반의 DNS 서비스 정책을 제공하는 것을 목적으로 한다.

[0007] 또한, 본 발명은 네트워크 사업자의 사전 설정된 DNS 정책에 따라 사용자 그룹별로 상이한 서비스 서버로 접속하게 하는 것을 목적으로 한다.

[0008] 또한, 본 발명은 사용자를 상이한 주소의 서버로 유도하기 위한 DNS 백엔드 프로세싱 방법을 제공하는 것을 목적으로 한다.

[0009] 또한, 본 발명은 전술한 DNS 백엔드 프로세싱을 수행하기 위한 DNS 서버를 제공하는 것을 목적으로 한다.

[0010] 또한, 본 발명은 트래픽 분리에도 불구하고 사용자의 불편을 최소화 할 수 있는 사용자 분류 기법을 제공하는 것을 목적으로 한다.

과제의 해결 수단

[0011] 상기 기술적 과제를 달성하기 위하여 본 발명은, 클라이언트의 DNS 질의에 응답하여, 상기 DNS 질의에 대응하는 서버의 복수의 IP 주소 중 선택적 IP 주소를 제공하는 DNS 서버에 있어서, 상기 DNS 서버는, 상기 클라이언트의 DNS 질의에 관련된 복수의 서버의 노드 데이터; 및 상기 클라이언트의 IP 주소에 따라 상기 DNS 질의에 관련된 상기 서버 노드의 IP 주소에 대한 DNS 응답을 제공하기 위한 룰 셋을 구비하는 것을 특징으로 하는 DNS 서버를 제공한다.

[0012] 본 발명에서 상기 룰 셋은 복수의 그룹으로 그룹화된 상기 클라이언트에 대하여 상기 서버 노드를 대응시키는 스크립트를 포함할 수 있다.

[0013] 본 발명에서 상기 노드 데이터는 메인서버 및 복제서버에 대한 데이터를 포함하고, 상기 클라이언트의 DNS 질의에 대하여 상기 메인서버의 IP 주소를 응답하는 디폴트 모드; 및 상기 클라이언트의 DNS 질의에 대한 응답으로서, 상기 클라이언트의 IP가 속한 그룹에 따라 선별적으로 상기 클라이언트의 상기 메인서버로의 접속을 차단하는 트래픽 격리 모드로 동작하는 것을 특징으로 한다.

[0014] 본 발명에서 상기 노드 데이터는, 상기 서버 노드의 ID와 상기 서버 노드의 IP를 대응된 데이터이다.

[0015] 또한, 상기 룰 셋은, 상기 클라이언트의 IP 주소에 대응하는 서버 노드의 IP 주소를 응답하는 스크립트를 포함할 수 있다.

[0016] 본 발명에서 상기 복수의 그룹은 트래픽 혼잡시 상기 메인서버로의 접속 우선 순위에 따라 분류되는 것을 특징으로 한다. 이 때, 상기 복수의 그룹은, 상기 메인서버로의 최우선 접속을 보장하는 제1 그룹; 상기 메인서버로의 접속을 차단하는 제2 그룹; 및 최소한 상기 복제서버로의 접속을 보장하는 제3 그룹을 포함할 수 있다.

[0017] 또한, 상기 제3 그룹은, 상기 클라이언트의 IP 주소가 상기 메인서버 또는 복제서버로의 과거 접속 이력이 있는가 여부 보다 구체적으로는 과거 접속 이력이 있는 IP 주소와 IP 접두어가 동일한가 여부에 따라 구분될 수 있다.

[0018] 본 발명에서 상기 DNS 서버는 PDNS로 바람직하게 구현될 수 있다.

[0019] 또한 상기 다른 기술적 과제를 달성하기 위하여 본 발명은 DNS 서버에 도메인 네임에 대응하는 메인서버, 복제서버 및 검역서버를 포함하는 복수의 서버에 대한 노드 데이터를 입력하는 단계와, 상기 DNS 서버에 클라이언트의 IP 주소와 상기 클라이언트 IP 주소에 대응하여 응답되어야 할 상기 복수의 서버 노드에 관한 룰 셋을 입력하는 단계; 네트워크 트래픽이 비정상 상태임을 통보 받는 경우, 상기 노드 데이터 및 상기 룰 셋에 기초하여, 클라이언트의 DNS 질의에 대한 응답으로 상기 클라이언트의 IP 주소에 대응하는 상기 서버 노드의 IP 주소를 제공하도록 설정하는 단계; 및 상기 설정에 따라 클라이언트의 DNS 질의에 대하여 응답하는 단계를 포함하는 DNS 서버의 백엔드 프로세싱 방법을 제공한다.

발명의 효과

[0020] 본 발명에 따르면, 클라이언트의 거동에 기초하여 클라이언트 서비스 그룹을 정적 화이트 리스트, 동적 화이트 리스트, 블랙 리스트, 동적 화이트리스트로 구분하여 각 클라이언트 그룹별로 상이한 DNS 응답 정책을 적용할 수 있게 한다. 이에 따라, 클라이언트의 트래픽 요청을 상이한 서비스 서버로 트래픽을 격리하여, 정상적인 사용자에게 원활한 서비스를 제공할 수 있게 된다.

[0021] 또한, 본 발명에 따른 사용자 그룹 분류는 IP 스푸핑(spoofing) 기법 등을 이용한 악의적 요청의 경우에도 정상적 사용자의 서비스 접속 피해를 최소화할 수 있게 된다.

도면의 간단한 설명

[0022] 도 1은 본 발명의 바람직한 실시예에 따른 공격 트래픽 분산 방법을 구현하기 위한 전체 시스템 구성을 모식적으로 도시한 도면이다.

도 2는 본 발명의 바람직한 실시예에 따른 복제서버의 운영 및 트래픽 분산 절차를 개략적으로 도시한 도면이다.

도 3은 트래픽 분리의 전제로서 사용자 그룹 분류를 위한 분류 장치를 모식적으로 도시한 도면이다.

도 4는 본 발명에 따른 DNS 백엔드 프로세싱을 위한 사용자 분류의 일례를 모식적으로 도시한 도면이다.

도 5는 리스트 작성부에 의해 작성된 블랙리스트 보고서를 예시적으로 도시한 도면이다.

도 6은 본 발명의 바람직한 실시예에 따른 트래픽 분리를 설명하기 위한 시스템 아키텍처를 도시한 도면이다.

도 7은 본 발명의 바람직한 실시예에 따른 DNS 서버의 백엔드 프로세싱 절차를 도시하고 있다.

발명을 실시하기 위한 구체적인 내용

[0023] 이하, 첨부한 도면을 참조하여, 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 본 발명을 상술한다. 그러나 본 발명은 아래에서 예시한 것과 다른 형태로 구현될 수 있으며 여기에서 설명하는 실시예에 한정되지 않는다. 또, 도면에서 본 발명을 명확하게 설명하기 위해서 설명과 관계없는 부분은 생략하였으며, 명세서 전체를 통하여 유사한 부분에 대해서는 유사한 도면 부호를 붙였다.

[0024] 본 발명을 설명함에 있어서, 관련된 공지 구성 또는 기능에 대한 구체적인 설명이 본 발명의 요지를 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명은 생략한다.

[0025] 도 1은 본 발명의 바람직한 실시예에 따른 공격 트래픽 분산 방법을 구현하기 위한 전체 시스템 구성을 모식적으로 도시한 도면이다.

[0026] 도시된 바와 같이, 메인 서버(SM)와 다수의 복제서버(R11, R12, R21, R23)가 인터넷 서비스 공급자(Internet Service Provider)에 의해 제공되는 네트워크(Network; 10)에 분산되어 있다.

[0027] 본 발명에서 메인 서버(SM)는 예컨대 'www.naver.com'과 같은 도메인 네임을 가지고 웹 페이지 상의 서비스를 구현하는 웹 서버일 수 있다.

[0028] 상기 복제서버(R11, R12, R21, R23)는 상기 메인 서버가 보유한 원본 콘텐츠의 전부 또는 일부의 사본을 구비하여 메인 서버(R11, R12, R21, R23)의 기능을 제공할 수 있는 서버를 말한다.

[0029] 복제서버(R11, R12, R21, R23)는 다양한 유형으로 구현될 수 있다. 먼저, 복제서버는 메인 서버의 전체 콘텐츠를 복제서버에 복사하는 형태로 구성될 수 있다. 복제 소요 시간이 오래 걸리고, 저장 장치의 자원이 많이 요구되지만, 사용자에게 가장 안정적인 서비스를 제공할 수 있다.

[0030] 이와 달리, 사용자의 요청이 빈번한 특정 콘텐츠를 복제서버에 복사하는 형 태로 복제서버가 구성될 수 있다. 이와 같은 관심기반 복제서버는 사용자 요청이 빈번한 콘텐츠인지 여부를 콘텐츠에 대한 사용자의 요청 횟수에 기반하여 판단할 수 있다. 관심 기반 복제서버는 상대적으로 적은 자원이 요구되지만, 서비스 제공자는 어떤 콘텐츠에 사용자들이 관심을 두는지 모니터링 해야 하고, 이에 따라 복제서버의 콘텐츠를 갱신해야 한다.

[0031] 또한, 멀티미디어 파일, 문서 파일, 사용자 파일 등으로 콘텐츠의 타입을 나누어 콘텐츠를 저장하는 콘텐츠 타입 기반 복제서버로 구성될 수도 있다. 즉, 하나의 복제서버는 하나 이상의 콘텐츠 타입을 담당하게 된다. 이

때, 콘텐츠 타입이란, 콘텐츠의 파일 형식이 될 수 있고, 기설정된 콘텐츠의 분류가 될 수도 있다.

[0032] 본 발명에서 복제서버(R11, R12, R21, R23)는 클라우드 컴퓨팅 기술로 구현될 수 있다. 클라우드 컴퓨팅은 서로 다른 물리적인 위치에 존재하는 컴퓨터들의 자원을 가상화 기술로 통합해 제공하는 기술로, 복제서버의 자원을 효율적으로 사용할 수 있게 하며, 가상 공간에 있는 서버의 자원을 이용하여 복제서버를 구축할 수 있도록 한다. 물리적으로, 상기 복제서버는 메인 서버 관리자가 관리하는 데이터 센터 또는 상기 관리자와 약정 관계에 있는 다른 사업자의 데이터 센터 내에 위치할 수 있다.

[0033] 본 발명에서 상기 복제서버가 반드시 클라우드 컴퓨팅 기술로 구현되어야 하는 것은 아니고 별도의 내부 또는 외부의 리소스로 구성되는 것도 가능하다.

[0034] 본 발명에 따르면, 네트워크(10)에 연결된 사용자(U)와 공격자(A)를 포함하는 네트워크 트래픽은 적절히 분리된다.

[0035] 정상 동작 모드에서 상기 사용자(U)에 의해 전송되는 정상 패킷(normal packet)은 네트워크(10) 상의 경로를 거쳐 메인 서버(SM)로 전송된다.

[0036] 악의의 사용자(A)의 DDoS 공격에 의한 패킷(Attack Packets) 범람과 같은 트래픽 혼잡시 메인 서버로 향하는 네트워크 경로 상의 적절한 위치에 복제서버가 활성화된다. 상기 복제서버는 활성화 될 위치에 관계된 데이터 센터의 관리자로 전송되는 서버 용량, 개수 및 활성화 시점 등을 포함하는 개시 메시지(invoke message)에 의해 활성화될 수 있다. 상기 복제서버는 상기 메인서버와 동기화된다. 상기 복제서버와 메인 서버의 동기화를 위하여 별도의 네트워크 예컨대 콘텐츠 전달 네트워크(CDN)가 구성될 수도 있을 것이다.

[0037] DDoS 공격시 범람 패킷(attack flood)은 상기 메인 서버로의 네트워크 경로 상에 위치한 활성화 된 복제서버(R11, R12)로 리디렉션 된다.

[0038] 본 발명에서 상기 복제서버의 활성화 위치(activate location) 및 요구되는 리소스를 결정하기 위하여 상기 네트워크(10)의 메인서버(SM)의 인접 위치에는 복제서버 관리장치(100)와 같은 별도의 수단이 부가될 수 있다.

[0039] 상기 복제서버 관리장치(100)는 네트워크(10)의 트래픽 및 상기 메인 서버(SM)의 상태를 모니터링하고, 이에 기초하여 복제서버와 관련한 자원(Resoruce)을 관리한다. 상기 복제서버 관리장치(100)는 복제서버의 개시(invoction) 여부를 결정하기 위하여 별도의 IDS(Intrusion Detection System)로부터 DDoS 공격 여부에 대한 정보를 수신하여 복제서버의 개시 여부 결정에 참조할 수 있다.

[0040] 이상 도 1을 참조하여 설명한 바와 같이, 상기 공격자(A) 및 사용자(U1, U2, U3)의 트래픽은 복제 서버를 포함하는 여러 서버로 분산된다. 본 발명에 따른 트래픽의 분산 방법에 대해서는 후술한다.

[0041] 도 2는 본 발명의 바람직한 실시예에 따른 복제서버의 운영 및 트래픽 분산 절차를 개략적으로 도시한 도면이다.

[0042] 도 2를 참조하면, 악의의 공격자 등에 의해 트래픽 혼잡이 발생하는 경우 IDS(Intrusion Detection System) 등의 수단에 의해 비정상 상태가 검출된다(S100). 비정상 상태가 검출되면, 네트워크에 산재한 복제서버가 개시(invoke)된다(S110). 복제서버가 개시되면 클라이언트 트래픽은 다수의 복제서버로 분리된다(S120). 이 때, 후술하는 바와 같이 DNS 백엔드 프로세싱 기반의 트래픽 분리(Traffic Isolation) 방식이 적용된다. 공격이 종료되고 네트워크 트래픽이 정상 상태로 회귀하면 복제서버는 중지된다(S130).

[0043] 도 3은 트래픽 분리의 전제로서 사용자 그룹 분류를 위한 분류 장치를 모식적으로 도시한 도면이다.

[0044] 도면을 참조하면, 상기 사용자 그룹 분류 장치(200)는 모니터링부(210), IP 추출부(220) 및 리스트 작성부(230)을 포함하여 구성될 수 있다.

[0045] 본 발명에서 상기 모니터링부(210)는 IDS로부터 DDoS가 검출 통보를 수신하거나 메인서버에 대한 클라이언트 IP의 접속 기록을 모니터링 한다.

[0046] IDS로부터 DDoS 검출 통보와 같은 비정상 상태 메시지가 수신하는 경우 IP 추출부(220)는 해당 메시지에서 DDoS 공격에 관여한 IP 주소를 추출한다. 상기 리스트 작성부(230)는 추출된 IP 주소를 근거로 블랙리스트를 작성할 수 있다.

[0047] 또한, 상기 모니터링부(210)는 메인서버 및/또는 복제서버로 접속하는 IP의 리스트를 모니터링하고, 상기 IP 추출부(220)는 추출된 IP의 접속 기록을 관리한다. 예컨대, 상기 IP 추출부(220)는 접속한 IP의 접두어와 접속 빈

도를 기록할 수 있다.

[0048] 도 5는 리스트 작성부에 의해 작성된 블랙리스트 보고서를 예시적으로 도시한 도면이다.

[0049] 도시된 바와 같이, 보고서의 제1 열(D1)에는 해당 리포트의 작성 일시가 기록되며, 해당 리포트에서 추가되는 신규한 IP 주소가 몇 개인지를 알려준다. 예컨대, 도 5의 열(D1)에는 "0"이라고 기재하여 직전 보고서에 비해 새로운 IP가 추가되지 않았음을 표현하고 있다.

[0050] 또한, 상기 보고서의 제2열 이하에는 DDoS 공격 빈도와 해당 IP 주소가 나열된다. 예컨대 "25 : 192. 168. 1. 14"는 IP 주소 192. 168. 1. 14로부터 총 25회의 공격 시도가 있었다는 것을 알려준다.

[0051] 이상과 같이, 상기 사용자 분류 장치는 IDS와 같은 외부의 시스템, 메인서버 및/또는 복제서버와 연동하여 접속한 사용자를 적절한 기준에 따라 분류한다. 물론, 본 발명에서 상기 사용자 분류장치(200)는 도 1과 관련한 메인서버의 일부 콤포넌트로 구현되거나 복제서버 관리장치(100)와 같이 별도의 콤포넌트로 구현될 수 있다. 또한, 상기 사용자 분류장치(100)는 상기 복제서버 관리장치(100)와 통합된 콤포넌트로 구현될 수 있을 것이다.

[0052] 본 발명에서 사용자는 크게 3가지 유형으로 분류될 수 있다. 먼저, 최우선권을 갖는 클라이언트 그룹은 화이트 리스트로 분류될 수 있을 것이다. 다음으로, 가장 낮은 우선권을 갖는 그룹은 블랙리스트로 분류될 수 있을 것이다. 또한, 나머지 클라이언트는 비나인 리스트에 편입될 수 있을 것이다. 이 그룹은 보통의 우선권을 가지며, 잠재적으로 화이트 리스트나 블랙 리스트에 편입될 가능성이 있는 그룹이다.

[0053] 본 발명에 따르면, 화이트 리스트, 블랙 리스트 및 비나인 리스트는 자동적으로 생성될 수 있다. 예컨대, 화이트 리스트는 기업 고객과 같은 VIP 클라이언트로 선별된 특정 클라이언트가 포함될 수 있다. 또한, 블랙 리스트는 과거 DDoS 공격에 참여하거나 악용된 IP를 갖는 그룹이다. 따라서, 과거 공격 이력 및 고객 정보를 활용함으로써 화이트 리스트와 블랙 리스트가 분류될 수 있고, 나머지 클라이언트는 모두 비나인 리스트로 분류될 수 있다.

[0054] 본 발명에서 클라이언트 그룹은 사용자의 과거 거동에 근거하여 보다 세분화 할 수 있다. 도 4는 본 발명에 따른 DNS 백엔드 프로세싱을 위한 사용자 분류의 일례를 모식적으로 도시한 도면이다.

[0055] 도 4에서 각 클라이언트 그룹은 다음과 같이 분류된다.

[0056] SW : 정적 화이트 리스트(Static White List)

[0057] DW : 동적 화이트 리스트(Dynamic White List)

[0058] BL : 블랙 리스트(Black List)

[0059] BN : 비나인 리스트(Benign List)

[0060] MW : 혼성 화이트 리스트(Mixed White List)

[0061] SG : 정적 그레이 리스트(Static Gray List)

[0062] DG : 동적 그레이 리스트(Dynamic Gray List)

[0063] GL : 그레이 리스트(Gray List)

[0064] SW는 VIP 고객 그룹으로 선별된 특정 그룹을 지칭한다. 이 그룹은 대부분 정적 IP 주소를 갖는 클라이언트 그룹이다. BL은 과거 DDoS 공격에 사용된 IP 주소를 갖는 클라이언트 그룹이다.

[0065] DW는 과거 접속 기록이 있는 IP 주소의 클라이언트를 포함하여 구성된다. 보다 바람직하게는 접속 기록이 있는 IP 주소와 동일한 접두어를 갖는 클라이언트 IP가 DW에 포함될 수 있다. 이를 위해 다음과 같이 IP 주소 접두어와 접속 회수를 포함하는 테이블이 DW 분류를 위해 사용될 수 있다. 표 1의 테이블은 전술한 사용자 분류 장치에 의해 획득될 수 있다.

표 1

[0066]

IP Prefix	Frequency (# of connection)
98. 24. 64. *	10

140. 22. 29. *	5
…	…

[0067] IP 접두어를 기초로 한 DW 그룹의 사용자 분류는 다음과 같은 장점을 갖는다. 통계적으로 종전 접속 이력이 있는 IP 주소와 동일 접두어를 갖는 IP 주소로부터의 접속은 99% 이상 합법적인 사용자로 추정될 수 있다. 따라서, 접속 기록과 IP 접두어를 이용하여 클라이언트를 DW 그룹으로 편성하는 것은 합법적인 사용자를 구분하는 중요한 방편이 될 수 있다. 다만, 이들 그룹에 대한 서비스는 SW 그룹에 비해서는 우선 순위가 낮게 되는 것이 바람직하다.

[0068] 본 발명에서 위 DW, SW 및 BL 그룹에 속하는 속성을 갖는 클라이언트는 보다 세분화될 수 있다. 클라이언트 IP가 SW와 DW에 동시에 속하는 클라이언트는 MW 그룹으로 분류한다. 이 그룹은 DW에 비해 높은 서비스 우선 순위를 부여할 수 있다. 또한, SW와 BL에 동시에 속하는 클라이언트 IP는 SG 그룹으로, DW와 BL에 동시에 속하는 클라이언트 IP는 DG로 분류된다. 이 그룹은 각각 BL 그룹에 비해 높은 서비스 우선 순위가 부여될 수 있다. 또한, 상기 SW, DW 및 BL 그룹에 동시에 속하는 클라이언트는 GL로 분류되며, SG와 DG에 비해 높은 우선 순위가 부여될 수 있다. 한편, 기타 IP 접속 기록을 갖지 않는 클라이언트는 BN 그룹으로 분류될 수 있다. BN 그룹은 검역 서버로의 격리 우선 순위가 BL, DG, SG 및 GL 그룹에 비해 낮으며, 메인서버로의 트래픽 격리 순위에서도 SW, MW 및 DW보다 낮도록 유지할 수 있다.

[0069] 각 클라이언트 그룹에 대하여 메인서버로부터 트래픽 분리(Traffic Isolation)가 우선적으로 적용되는 순위는 다음과 같다.

표 2

[0070]

Priority	그룹
1	BL
2	DG
3	SG
4	GL
5	BN
6	DW
7	MW
8	SW

[0071] 도 6은 본 발명의 바람직한 실시예에 따른 트래픽 분리를 설명하기 위한 시스템 아키텍처를 도시한 도면이다.

[0072] 도 6을 참조하면, DNS 서버는 클라이언트로부터 DNS 질의(query)에 대하여 응답(answer)한다.

[0073] 상기 DNS 서버는 바람직하게는 PDNS (Power DNS)로 구현될 수 있다. PDNS는 상기 클라이언트의 질의에 포함된 소스 IP에 따라 다양한 응답이 가능하도록 하는 백엔드 스크립트를 보유할 수 있다.

[0074] 도 6에는 상기 DNS 서버가 트래픽 분리를 수행하기 위한 입력이 도시되어 있다. 상기 입력으로는 노드 데이터(310), 룰 셋(320) 및 비정상 데이터(330)가 포함된다.

[0075] 상기 노드 데이터(310)는 서비스의 제공을 위한 메인서버와 복제서버의 ID 및 주소 정보를 포함한다. 또한, 상기 노드 데이터에는 추가 정보가 포함될 수 있다. 예컨대, 상기 추가 정보는 해당 서버에 대한 명칭 또는 설명, 서버의 크기(capacity) 및 기타 부가 데이터가 포함될 수 있다. 예시적으로 상기 노드 데이터는 아래 표 3과 같이 구성될 수 있다.

[0076] 상기 노드 데이터(310)는 전술한 메인서버 또는 복제서버 관리장치로부터 전송될 수 있다.

표 3

[0077]

Node ID	IP Address	Reserved
0	192.168.1.10	Main Server/capacity/additional data
1	192.168.1.100	Replica #1/capacity/additional data
2	192.168.1.101	Replica #2/capacity/additional data

[0078] 상기 룰 셋(rule set)은 DNS 서버의 백엔드 스크립트의 구현을 위한 규칙들을 논리적으로 기술한 파일 형태로 된 룰들을 지칭한다.

[0079] 예컨대, 상기 룰들은 질의에 관련된 소스 IP에 대하여 해당 IP의 전술한 사용자 구분에 따라 어떠한 DNS 응답을 제공할 것인가에 관한 정보를 포함한다.

[0080] 룰들은 다음과 같이 '\n'과 같은 개행문자에 의해 분리될 수 있다.

[0081] (if $ip eq "192.168.1.12") && ($qtype eq "A" || $qtype eq "ANY") \n

[0082] …….. \n

[0083] EOF

[0084] 예컨대, 상기 룰들은 입력된 IP가 블랙리스트로 분류된 IP인 경우 특정 노드(예컨대 검역서버 노드)로 전송하는 스크립트를 포함할 수 있다. 또한, 화이트리스트로 분류된 IP에 대해서는 다른 노드(예컨대 메인서버 노드)로 전송하는 스크립트를 포함할 수 있다. 또한, 동적 화이트리스트로 분류된 IP에 대해서는 또 다른 노드(예컨대 복제서버)로 전송하는 스크립트를 포함할 수 있다.

[0085] 상기 룰들은 전술한 사용자 분류 장치의 보고서에 기초하여 작성될 수 있다. 또한, 상기 룰들은 시스템 운영자에 의해 작성되거나 외부의 시스템으로부터 전송될 수 있다.

[0086] 부가적으로, 비정상 데이터가 상기 DNS 서버로 입력될 수 있다. 상기 비정상 데이터는 트래픽 이상의 유형에 관한 정보를 포함한다. 예컨대, 상기 비정상 데이터는 어떤 DDoS 공격 유형인지에 관한 정보를 포함할 수 있다. 상기 비정상 상태에 관한 정보는 전술한 룰 셋에 반영되어 트래픽 격리의 수행에 참조될 수 있다.

[0087] 상기 DNS 서버는 상기 클라이언트로부터의 질의 패킷으로부터 상기 클라이언트의 IP 어드레스나 패킷 소스 IP 어드레스를 추출한다. 전술한 룰 셋에 기초하여 추출된 IP 어드레스에 대한 적당한 DNS 응답이 제공된다.

[0088] 도 7은 본 발명의 바람직한 실시예에 따른 DNS 서버의 백엔드 프로세싱 절차를 도시하고 있다.

[0089] 도 7을 참조하면, 먼저 DNS 서버에 노드 데이터(S210) 및 룰 셋(S210)이 제공된다(S210, S212).

[0090] IDS 등에 의해 제공되는 정보에 기초하여 네트워크 트래픽이 비정상 상태인가 여부가 결정된다(S214). 비정상 상태가 아닌 경우, 상기 DNS 서버는 디폴트 모드의 DNS 기능으로 동작한다(S216).

[0091] 비정상 상태인 경우, DNS 질의에 대한 트래픽 격리 모드가 개시된다.

[0092] 상기 DNS 서버로 DDoS 공격 유형 정보가 입력되며(S220), 클라이언트의 DNS 질의에 대하여 입력된 룰 셋 및 노드 데이터에 기초하여 적절한 DNS 응답이 제공된다.

[0093] 질의에 관련된 클라이언트의 IP 주소에 기초하여 해당 IP 주소가 블랙리스트로 분류된 경우(S224), 해당 클라이언트를 검역서버의 주소로 인도하는 DNS 응답이 제공된다(S226).

[0094] 해당 IP 주소가 정적 화이트리스트로 분류된 경우(S228) 메인서버의 주소로 인도하는 DNS 응답에 제공되고(S230), 해당 IP 주소가 동적 화이트리스트로 분류된 경우(S232) 해당 클라이언트를 복제서버로 인도하는 DNS 응답이 제공된다(S234).

[0095] 도시하지 않았지만, 도 5와 관련하여 설명한 다른 IP 주소 그룹의 클라이언트 질의에 대해서 적절한 DNS 응답이 제공될 수 있다.

부호의 설명

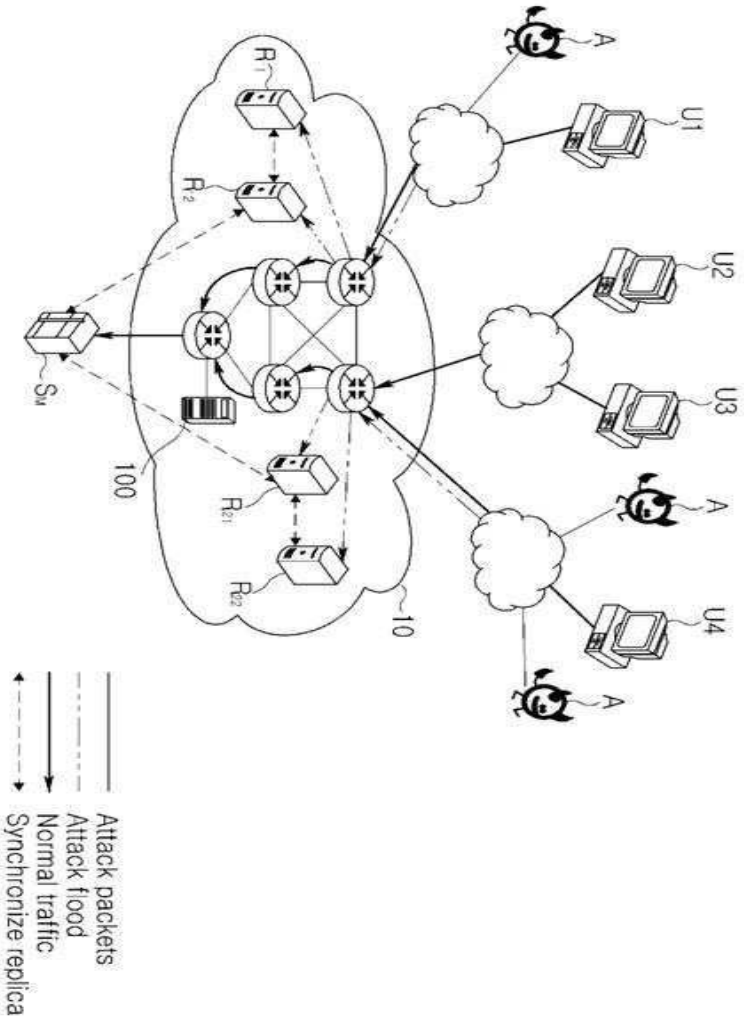
[0096]

A	공격자
U	사용자
R	복제서버
10	네트워크

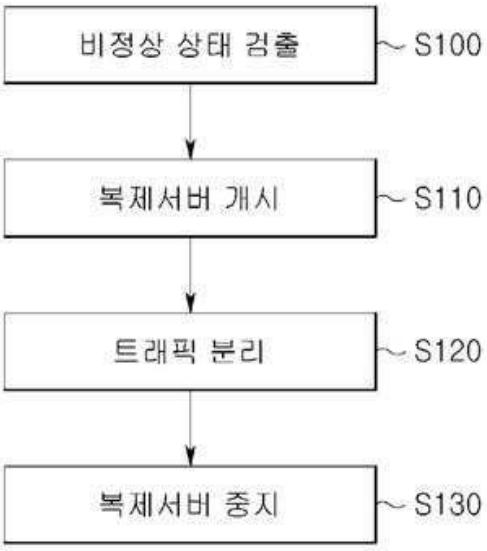
100	복제서버 자원관리장치
200	사용자 분류 장치
210	IP 추출부
220	리스트 작성부
300	DNS 서버
310	노드 데이터
320	룰 셋
330	비정상 데이터

도면

도면1



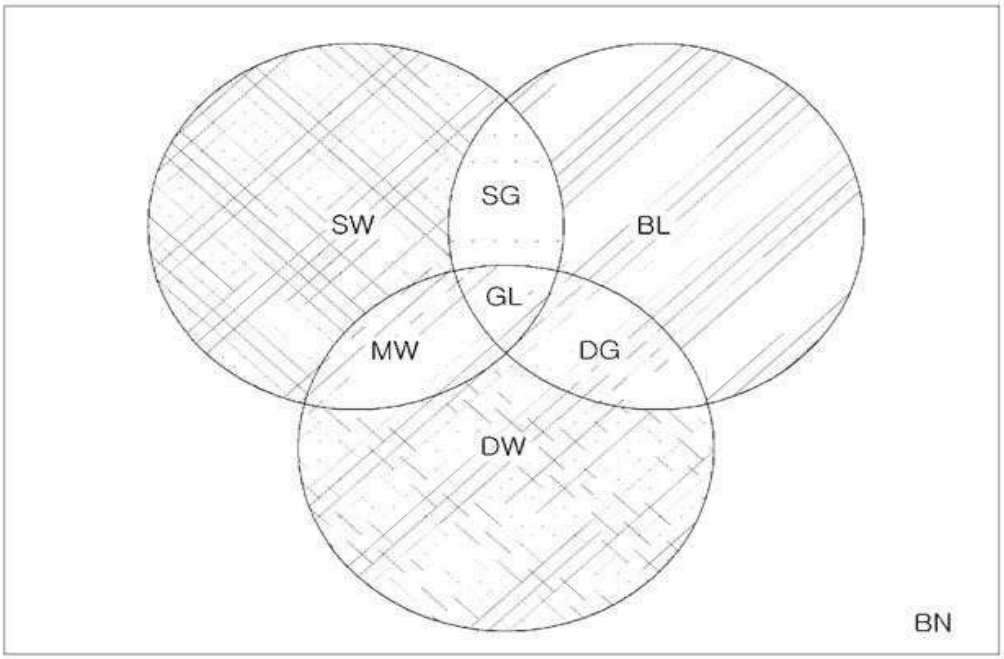
도면2


비정상 상태 검출
S100
복제서버 개시
S110
트래픽 분리
S120
복제서버 중지
S130

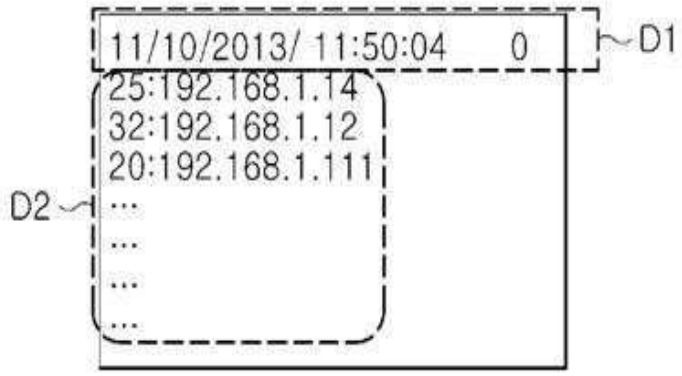
도면3


200
모니터링부
210
IP 추출부
220
리스트 작성부
230

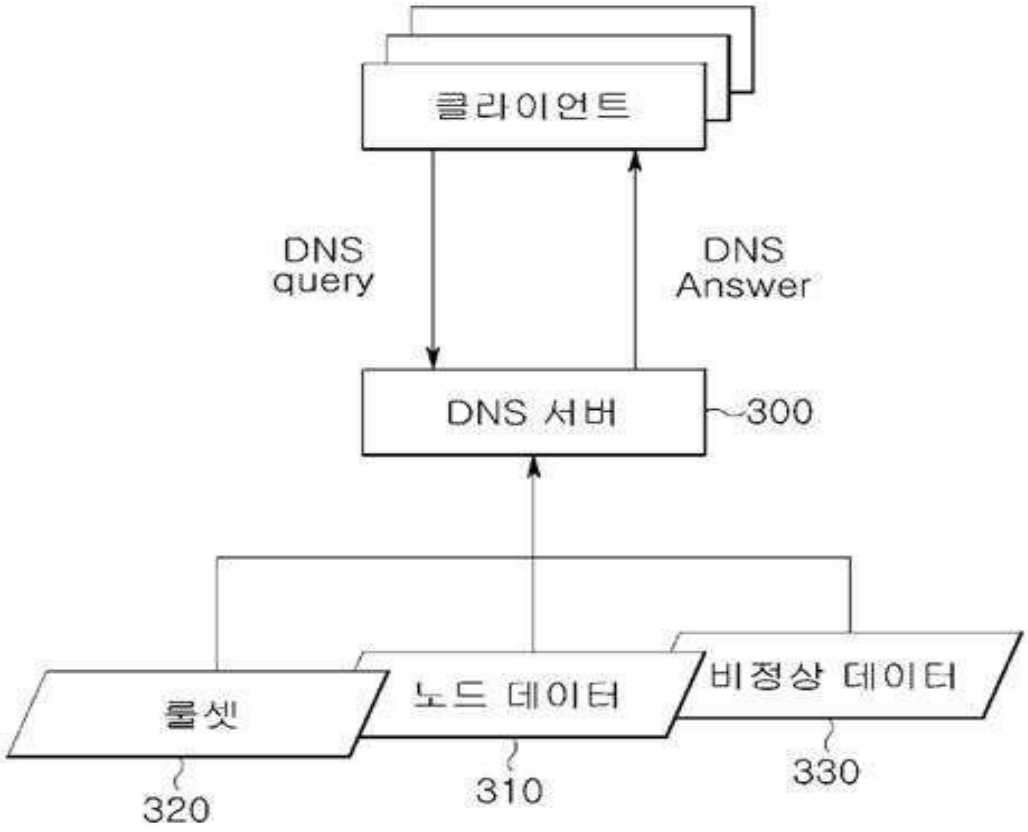
도면4


SW
SG
BL
GL
MW
DG
DW
BN

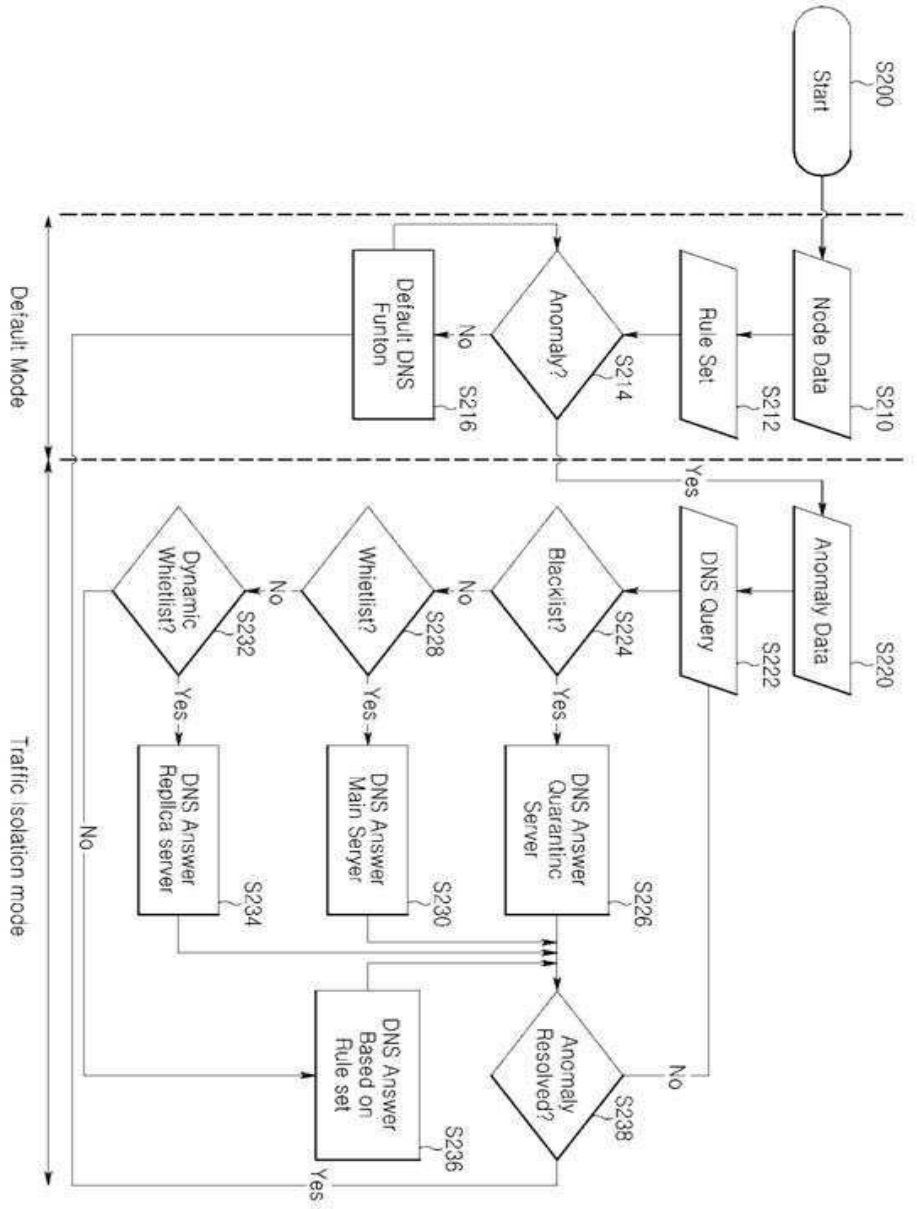
도면5


11/10/2013/ 11:50:04 0
D1
25:192.168.1.14
32:192.168.1.12
20:192.168.1.111
D2
...
...
...
...

도면6


클라이언트
DNS query
DNS Answer
DNS 서버
300
룰셋
노드 데이터
비정상 데이터
320
310
330

도면7



【심사관 직권보정사항】

【직권보정 1】

【보정항목】 청구범위

【보정세부항목】 청구항 3

【변경전】

제2항에 있어서,

상기 클라이언트의 DNS 질의에 대하여 상기 메인서버의 IP 주소를 응답하는 디폴트 모드를 더 포함하는 것을 특징으로 하는 DNS 서버.

【변경후】

제1항에 있어서,

상기 클라이언트의 DNS 질의에 대하여 상기 메인서버의 IP 주소를 응답하는 디폴트 모드를 더 포함하는 것을 특징으로 하는 DNS 서버.