(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2012년05월11일
(11) 등록번호 10-1144332
(24) 등록일자 2012년05월02일

(51) 국제특허분류(Int. Cl.)
H04L 12/24 (2006.01) *H04L 12/22* (2006.01)
H04L 12/28 (2006.01) *H04L 29/06* (2006.01)
(21) 출원번호 10-2011-0127476
(22) 출원일자 2011년12월01일
심사청구일자 2011년12월01일
(56) 선행기술조사문헌
KR100663546 B1*
KR1020040028407 A*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
주식회사 프라이머리넷
경기도 부천시 원미구 부일로233번길 18, 송래프라자 902 (상동)
(72) 발명자
신동원
경기도 부천시 원미구 부일로233번길 18, 송내프라자 9층 902호 (상동)
(74) 대리인
최지연, 정중원, 이명택

전체 청구항 수 : 총 3 항 심사관 : 문형섭

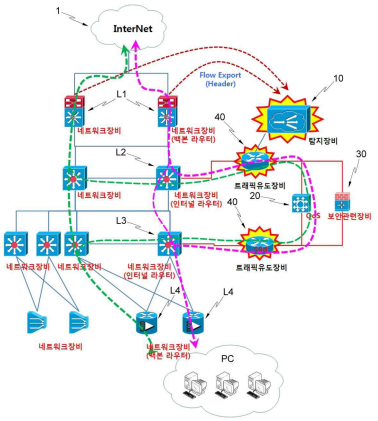
(54) 발명의 명칭 **네트워크 트래픽 처리 시스템**

(57) 요 약

본 발명은 다수의 라우터들을 갖는 네트워크에서의 트래픽 처리 시스템에 관한 것으로서, 보다 상세하게는 별도의 우회경로를 만들어 트래픽을 가공처리하는 가공처리장비를 우회경로에 설치하고, 네트워크로 입력되는 트래픽을 분석하는 탐지장비와, 탐지장비가 분석하여 선택한 해당 트래픽을 우회경로로 유도하여 가공처리장비로 전송하는 트래픽 유도장비를 구비하여, 적은 수의 가공처리장비로도 해당 네트워크로 입력되는 트래픽을 효율적으로 처리할 수 있고, 해당 네트워크에 회선이 증설되더라도 가공처리장비의 추가적인 투자가 필요하지 않고, 가공처리장비와 탐지장비 및 유도장비에 장애가 발생되더라도 네트워크의 서비스에 영향이 없는 네트워크 트래픽 처리 시스템에 관한 것이다.

본 발명에 따른 네트워크 트래픽 처리 시스템은 트래픽의 최적 통신경로를 제공하는 라우터들을 갖는 네트워크에서, 네트워크로 입력되는 트래픽을 분석하는 탐지장비; 상기 라우터들을 상호 연결하는 메인경로에 추가하여 두 라우터를 연결하는 별도의 우회경로 상에 구비되며, 입력되는 트래픽을 가공처리하여 출력하는 가공처리장비; 상기 우회경로 상에 구비되며, 상기 탐지장비가 분석하여 전송하는 대상 트래픽 정보를 바탕으로 상기 라우터에 입력되는 트래픽에서 해당 트래픽을 유도하여 상기 가공처리장비로 전송하고, 상기 가공처리장비에 출력되는 트래픽을 상기 라우터로 전송하는 트래픽 유도장비;를 포함하여 이루어진다.

대 표 도 - 도2



특허청구의 범위

청구항 1

트래픽의 최적 통신경로를 제공하는 라우터들을 갖는 네트워크에서,

네트워크로 입력되는 트래픽을 분석하는 탐지장비;

상기 라우터들을 상호 연결하는 메인경로에 추가하여 두 라우터를 연결하는 별도의 우회경로 상에 구비되며, 입력되는 트래픽을 가공처리하여 출력하는 가공처리장비;

상기 우회경로 상에 구비되며, 상기 탐지장비가 분석하여 전송하는 대상 트래픽 정보를 바탕으로 상기 라우터에 입력되는 트래픽에서 해당 트래픽을 유도하여 상기 가공처리장비로 전송하고, 상기 가공처리장비에 출력되는 트래픽을 상기 라우터로 전송하는 트래픽 유도장비;를 포함하되,

상기 탐지장비는

상기 라우터가 전송하는 플로우 정보를 분석하고,

상기 라우터가 전송하는 플로우 정보와 데이터베이스에 등록저장되어 있는 비정상 트래픽 생성 소스원 정보를 상호 비교하여 우회 대상 트래픽을 분석 탐지하는 것을 특징으로 하는 네트워크 트래픽 처리 시스템.

청구항 2

삭제

청구항 3

삭제

청구항 4

제 1 항에 있어서,

상기 탐지장비는 해당 네트워크와 다른 네트워크 또는 사용자 단말을 연결하는 백본 라우터에 입력되는 트래픽을 분석하고,

상기 우회경로에 구비되는 가공처리장비는 상기 백본 라우터에 직접 연결되는 인터넷 라우터에서 해당 트래픽을 입력받는 것을 특징으로 하는 네트워크 트래픽 처리 시스템.

청구항 5

제 1 항 또는 제 4 항에 있어서,

상기 탐지장비는 입력되는 트래픽을 분석하여 바이러스나 악성 봇에 감염된 PC의 IP를 추출하는 것을 특징으로 하는 네트워크 트래픽 처리 시스템.

명 세 서

기 술 분 야

[0001] 본 발명은 다수의 라우터들을 갖는 네트워크에서의 트래픽 처리 시스템에 관한 것으로서, 보다 상세하게는 별도의 우회경로를 만들어 트래픽을 가공처리하는 가공처리장비를 우회경로에 설치하고, 네트워크로 입력되는 트래픽을 분석하는 탐지장비와, 탐지장비가 분석하여 선택한 해당 트래픽을 우회경로로 유도하여 가공처리장비로 전송하는 트래픽 유도장비를 구비하여, 적은 수의 가공처리장비로도 해당 네트워크로 입력되는 트래픽을 효율적으로 처리할 수 있고, 해당 네트워크에 회선이 증설되더라도 가공처리장비의 추가적인 투자가 필요하지 않고, 가공처리장비와 탐지장비 및 유도장비에 장애가 발생되더라도 네트워크의 서비스에 영향이 없는 네트워크 트래픽 처리 시스템에 관한 것이며, 또한, 탐지장비에서 라우터가 전송하는 플로우 정보를 바탕으로 과다 트래픽을 유발하거나 DDOS와 같은 네트워크나 서버에 위협이 되는 행위를 유발하는 비정상적 트래픽을 탐지하여 우회시켜

처리하며, 바이러스나 악성 봇에 감염된 PC의 IP를 추출하는 네트워크 트래픽 처리 시스템에 관한 것이다.

배 경 기 술

[0002] 최근 인터넷 통신기술이 급속히 발전함에 따라 단위 네트워크의 수가 무수히 많아지고 있으며, 네트워크 상호 간과 네트워크와 사용자 단말 간의 데이터 트래픽(데이터 통신) 양도 많아지고 있다.

[0003] 일반적으로 하나의 네트워크(내부망)에는 수많은 사용자 단말이 연결되며, 여러 외부 네트워크(외부망)과 연결된다. 그래서 네트워크에는 여러 경로(사용자 단말이나 외부 네트워크)에서 입력되는 트래픽을 목적지에 최적의 통신경로를 통해 신속히 전송하기 위해 라우터들이 다수 구비된다.

[0004] 그리고 네트워크에는 트래픽의 품질을 높이기 위한 가공처리자장비로서, 입출력되는 트래픽의 전송 속도를 조절하고 처리순서를 조절하는 QoS장비와, 트래픽에 포함된 악성코드 등을 필터링하는 보안장비가 구비된다.

[0005] 도1은 종래기술에 따른 네트워크의 구성도를 도시한 것으로서, 도면에서 확인할 수 있듯이, 다수의 라우터를 상호 연결하는 메인경로에 QoS장비와 보안장비가 설치되고, QoS장비와 보안장비는 네트워크로 입력되는 모든 트래픽을 가공처리할 수 있도록 각각 다수개가 구비된다. 다시 말해 외부 네트워크와 사용자 단말 간을 연결하는 라우터들에 의해 설정 가능한 모든 통신경로에는 하나 이상의 QoS장비와 보안장비가 구비된다.

[0006] 위와 같은 종래기술에 따른 네트워크 구성은 다음과 같은 여러 문제가 있다.

[0007] 첫째, 해당 네트워크가 외부 네트워크와 사용자 단말 간을 연결하는 모든 통신경로 상에 QoS장비와 보안장비가 구비되도록 하기 위해 많은 수의 QoS장비와 보안장비가 필요하다.

[0008] 둘째, 트래픽 양이 늘어나거나 해당 네트워크에 연결되는 외부 네트워크나 사용자 단말이 늘어나 라우터를 추가 설치하는 때에 일반적으로 QoS장비와 보안장비도 동반되어 추가 설치된다.

[0009] 셋째, QoS장비와 보안장비에 장애가 발생한 때에 장애가 발생된 QoS장비와 보안장비를 거치는 통신경로를 통한 트래픽 서비스의 중단 또는 에러가 발생한다.

[0010] 넷째, 각각의 보안장비는 입력되는 트래픽의 정보 전체(즉, 헤더정보와 컨텐츠정보)에 대하여 악성코드나 바이러스가 포함되어 있는지를 검사하기 때문에 시간이 오래 소요되고, 일명 좀비PC에서 전송되는 트래픽의 경우 보안장비에서 비정상 트래픽으로 걸러내지 못하는 일이 종종 발생된다.

발명의 내용

해결하려는 과제

[0011] 본 발명은 위와 같이 종래기술에 따른 네트워크 구서이 갖는 문제를 해결하기 위해 안출된 발명으로서,

[0012] 네트워크에 설치되는 가공처리장비로서 QoS장비와 보안장비를 최소화하여 경제적 부담을 줄이고, 네트워크 내의 회선과 라우터 장비의 증설시에 QoS장비와 보안장비의 동반 증설이 필요 없어 경제적 부담을 줄이고 증설작업을 간소화하는 네트워크 트래픽 처리 시스템을 제공함을 목적으로 하고,

[0013] 라우터들을 상호 연결하는 메인경로 외에 추가적으로 우회경로를 만들고 우회경로에 QoS장비와 보안장비를 설치함으로써, QoS장비와 보안장비에 장애가 발생되더라도 네트워크의 트래픽 서비스에는 영향이 없는 네트워크 트래픽 처리 시스템을 제공함을 또 다른 목적으로 하고,

[0014] QoS장비와 보안장비는 모든 트래픽에 대하여 가공처리하는 것이 아니라, 탐지장비가 분석하여 선택된 해당 트래픽만을 처리하도록 하여 QoS장비와 보안장비의 처리 부하를 완화하는 네트워크 트래픽 처리 시스템을 제공함을 또 다른 목적으로 하고,

[0015] 라우터가 전송하는 플로우 정보와 데이터베이스에 등록저장된 비정상 트래픽 생성 소스원 정보를 상호 비교하여 악성봇이나 바이러스에 관련된 트래픽을 신속하고 신뢰성 높게 탐지하고, 우회경로로 우회시켜 보안장비에서 정밀 검사가 이루어지도록 한 네트워크 트래픽 처리 시스템을 제공함을 또 다른 목적으로 한다.

[0016] 아울러, 탐지장비는 비정상 트래픽으로 탐지된 트래픽을 분석하여 바이러스나 악성 봇에 감염된 PC의 IP를 추출하고, 추출된 감염 PC의 IP를 데이터베이스화하여 관리함으로써 감염 PC에 대한 사후 조치가 이루어질 수 있도록 하는 네트워크 트래픽 처리 시스템을 제공함을 또 다른 목적으로 한다.

과제의 해결 수단

[0017] 이와 같은 목적을 달성하기 위한 본 발명에 따른 네트워크 트래픽 처리 시스템은

[0018] 트래픽의 최적 통신경로를 제공하는 라우터들을 갖는 네트워크에서,

[0019] 네트워크로 입력되는 트래픽을 분석하는 탐지장비;

[0020] 상기 라우터들을 상호 연결하는 메인경로에 추가하여 두 라우터를 연결하는 별도의 우회경로 상에 구비되며, 입력되는 트래픽을 가공처리하여 출력하는 가공처리장비;

[0021] 상기 우회경로 상에 구비되며, 상기 탐지장비가 분석하여 전송하는 대상 트래픽 정보를 바탕으로 상기 라우터에 입력되는 트래픽에서 해당 트래픽을 유도하여 상기 가공처리장비로 전송하고, 상기 가공처리장비에 출력되는 트래픽을 상기 라우터로 전송하는 트래픽 유도장비;를 포함하여 이루어진다.

[0022] 그리고 상기 탐지장비는 상기 라우터가 전송하는 플로우 정보를 분석하는 것을 특징으로 하고,

[0023] 상기 탐지장비는 상기 라우터가 전송하는 플로우 정보와 데이터베이스에 등록저장되어 있는 비정상 트래픽 생성 소스원 정보를 상호 비교하여 우회 대상 트래픽을 분석 탐지하는 것을 특징으로 하고,

[0024] 상기 탐지장비 해당 네트워크와 다른 네트워크 또는 사용자 단말을 연결하는 백본 라우터에 입력되는 트래픽을 분석하고,

[0025] 상기 우회경로에 구비되는 가공처리장비는 상기 백본 라우터에 직접 연결되는 인터널 라우터에서 해당 트래픽을 입력받는 것을 특징으로 하고,

[0026] 상기 탐지장비는 입력되는 트래픽을 분석하여 바이러스나 악성 봇에 감염된 PC의 IP를 추출하는 것을 특징으로 한다.

발명의 효과

[0027] 이와 같은 구성을 갖는 본 발명에 따른 네트워크 트래픽 처리 시스템은 가공처리장비로서 QoS장비와 보안장비의 수를 최소화하여 경제적 부담이 적고, 회선이나 라우터의 증설시에 QoS장비와 보안장비의 동반 증설이 필요 없어 증설 작업이 보다 간편하고, 별도의 우회경로를 만들어 QoS장비와 보안장비를 설치함으로써 QoS장비와 보안장비에 장애가 발생되더라도 네트워크의 트래픽 서비스에 문제가 없고, 악성코드를 포함하는 트래픽과 처리속도나 처리순서 조절이 필요한 트래픽 등의 문제가 있는 트래픽만을 우회경로로 유도하여 처리함으로써 QoS장비와 보안장비의 부하를 줄일 수 있고, 라우터가 전송하는 플로우 정보를 분석하여 우회경로로 우회시킬 트래픽을 탐지하여 탐지 속도가 빠르고, 악성봇이나 바이러스에 관련된 데이터베이스의 소스원 정보를 이용하여 비정상 트래픽을 탐지하도록 하여 우회시켜야함에도 간과하여 우회시키지 못하는 경우의 발생이 최소화 되고, 비정상 트래픽으로 탐지된 트래픽 중에서 바이러스나 악성 봇에 감염된 PC의 IP를 추출하여 데이터베이스화하여 감염 PC의 관리가 가능해진다.

도면의 간단한 설명

[0028] 도 1 은 종래기술에 따른 네트워크 구성도.

도 2 는 본 발명에 따른 네트워크 트래픽 처리 시스템이 도입된 네트워크 구성도.

발명을 실시하기 위한 구체적인 내용

[0029] 이하, 도면을 참조하여 본 발명에 따른 네트워크 트래픽 처리 시스템에 대하여 보다 상세하게 설명한다.

[0030] 도2에서 보는 바와 같이 본 발명에 따른 네트워크 트래픽 처리 시스템은 트래픽의 최적 통신경로를 제공하는 라우터들(L1~L4)을 갖는 네트워크와,입력되는 트래픽을 분석하는 탐지장비(10)와, 입력되는 트래픽을 가공처리하는 가공처리장비(20, 30)와, 가공처리가 필요한 트래픽을 우회경로로 유도하는 트래픽 유도장비(40)를 포함한다.

[0031] 상기 네트워크는 일반적으로 외부의 네트워크와 사용자 단말(3)을 연결하여 외부 네트워크(1)에서 입력되는 트래픽(즉, 하향 트래픽)을 사용자 단말(3)로 전송하거나 사용자 단말(3)에서 입력되는 트래픽(즉, 상향 트래픽)을 외부 네트워크(1)로 전송하고, 외부 네트워크(1)와 또 다른 외부 네트워크(1)를 연결하여 외부 네트워크(1)간에 트래픽을 전송하기도 한다.

[0032] 상기 네트워크에는 다수의 라우터(L1~L4)들로 구성되고, 라우터(L1~L4)들은 서로 그물망 처럼 연결되어 입력되는 트랙픽이 목적지까지 최적의 통신경로를 통해 전송되도록 한다.

[0033] 참고로, 라우터(L1~L4)들을 상호 연결하여 트래픽이 전송되는 통신경로를 '메인경로'라고 정의하고, 본 발명의 시스템 구현을 위해 두 라우터를 상호 연결하여 추가적으로 별도 연결한 경로를 '우회경로'라고 정의한다.

[0034] 상기 라우터는 내부망(즉, 해당 네트워크)과 외부망(즉, 외부 네트워크(1))를 연결하는 주요 회선에 설치되는 백본 라우터(L1, L4)와, 해당 네트워크 내의 회선에 설치되는 인터널 라우터(L2,L3)로 구분할 수 있는데, 본 발명에서는 사용자 단말(3)도 외부망의 일종으로 취급하여 사용자 단말(3)과 해당 네트워크를 연결하는 회선에 설치되는 라우터(L4)도 백본 라우터로 취급한다. 네트워크에는 일반적으로 인터널 라우터(L2,L3) 뿐만 아니라 백본 라우터(L1, L4)도 다수개가 구비된다.

[0035] 상기 탐지장비(10)는 네트워크로 입력되는 트래픽을 분석하여 가공처리장비(20, 30)를 통해 가공처리가 필요한 트래픽을 선별하여 선택하고, 선택된 트래픽에 대한 정보를 상기 트래픽 유도장비(40)로 전송한다.

[0036] 상기 탐지장비(10)는 상기 라우터를 통해 네트워크로 입력되는 트래픽의 정보를 전송받게 되는데, 트래픽이 네트워크로 처음 입력되는 백본 라우터(L1, L4)로부터 트래픽 정보를 전송받아 보다 신속한 처리가 되도록 하는 것이 바람직하다.

[0037]

[0038] 상기 탐지장비(10)는 일반적으로 상기 라우터가 입력되는 트래픽의 패킷 중에서 추출한 플로우 정보를 전송받아 해당 트래픽을 분석한다.

[0039] 여기서, 상기 플로우 정보는 라우터라 입력되는 트래픽의 패킷에서 헤더부분의 정보를 추출하고, 추출된 헤더 정보를 설정된 양식으로 변환한 정보로서, 송신처 IP, 수신처 IP, 프로토콜, 포트, 어플리케이션 등에 대한 정보를 포함한다.

[0040]

[0041] 상기 탐지장비(10)가 플로우 정보를 바탕으로 트래픽을 분석하여 우회시킬 트래픽을 선별 선택하는 방식의 예로는 다음과 같은 것들이 있을 수 있다. 첫째, 단위시간에 해당 라우터로 입력되는 트래픽의 양을 체크하여 기준 양을 초과하는 경우에는 기 설정된 조건(예;동일 IP의 트래픽 양, 각 트래픽의 데이터 양, 트래픽의 출처나 목적지 등)에 해당하는 트래픽을 선별 선택한다. 둘째, 스팸성이나 광고성 트래픽 출처로 등록된 트래픽을 선별 선택한다. 셋째, 트래픽에 악성코드(예, 바이러스, 웜, 트로이얀, 백도어, 디도스, 악성봇 등)가 포함된 트팩픽을 선별하여 선택한다. 이외에도 탐지장비(10)가 트래픽을 분석하여 선별 선택하는 방법에는 사용자의 설정에 따라 다양한 것이 있을 것이다.

[0042] 상기 탐지장비(10)가 우회경로의 보안장비로 보낼 비정상 트래픽(예, 악성봇, 바이러스, 악성코드 등)으로 선별 선택할 때에는 신속하면서도 비정상 트래픽임에도 간과하는 상황이 발생되는 것을 최소화는 것이 바람직하다.

[0043] 이를 위해 본 발명은 데이터베이스에 비정상 트래픽과 관련된 비정상 트래픽 생성 소스원 정보를 수시로 갱신 등록저장하고, 라우터가 전송하는 플로우정보와 상기 비정상 생성 소스원 정보를 상호 매칭시켜 비교 분석한다.

[0044] 여기서, 비정상 트래픽 생성 소스원은 비정상 트래픽을 생성했던 전력이 있는 PC, 서버, 마스터, 사이트는 물론이고, 이러한 PC, 서버, 마스터, 사이트 등과 접속하여 비정상 트래픽을 생성할 가능성이 큰 PC, 서버, 마스터, 사이트 등을 포함한다.

[0045] 그리고 상기 비정상 트래픽 생성 소스원은 IP, 포트, 프로토콜, 어플리케이션 등의 정보로 데이터베이스에 등록 저장된다.

[0046] 그리고 상기 탐지장비(10)가 상기 라우터(L1)가 전송하는 플로우 정보로부터 해당 트래픽에 악성코드(바이러스)가 포함되어 있는 것으로 탐지되고, 악성코드의 유입이 트래픽의 송신처 PC의 감염에 의한 것으로 파악될 때에는 해당 PC, 즉,바이러스나 악성 봇에 감염된 PC의 IP를 추출하여 데이터베이스화하여, 감염된 PC의 관리에 사용할 수 있도록 한다.

[0047] 상기 가공처리장비(20, 30)는 네트워크의 트랙픽 서비스 품질을 높이는 장비로서, 입력되는 트래픽을 가공처리하여 출력한다.

[0048] 상기 가공처리장비(20, 30)로는 대역폭을 조절을 통해 동시에 통과할 수 있는 트래픽의 양을 조절함으로써 속도를 조절하고, 병목현상이 발생된 경우 입력된 트래픽의 종류나 출처 등으로부터 처리순서(즉, 출력순서)를 조절하는 등의 역할을 하는 QoS(Quality of Service)장비(20)와, 트랙픽에 악성코드가 포함되어 있는 경우 필터링하여 악성코드를 제거하거나 트래픽을 전송을 차단하는 등의 역할을 하는 보안장비(30)가 있다. 상기 QoS장비(20)와 보안장비(30) 자체는 공지기술에 해당하므로 이에 대한 구체적인 설명은 생략한다.

[0049] 상기 가공처리장비(20, 30)는 네트워크의 라우터(L1~L4)들을 상호 연결하는 메인경로 외에 추가적으로 설치하여

두 라우터(L2, L3)를 연결하는 우회경로에 구비되어, 어느 한 라우터에서 입력되는 트래픽을 가공처리 한 후에 다른 라우터로 출력한다. 이때, 우회경로에 연결되는 두 라우터에서 트래픽이 입력되는 라우터(하향 트래픽 기준시; L2)는 상기 탐지장비(10)가 트래픽의 정보를 입력받는 백본 라우터(하향 트래픽 기준시;L1)에 직접 연결된 인터널 라우터(L2)를 사용하여 트래픽이 보다 빨리 가공처리 과정을 거치도록 하는 것이 바람직하다.

[0050] 상기 트래픽 유도장비(40)는 상기 우회경로의 두 라우터(l 2, L3)와 가공처리장비(20, 30) 사이에 각각 구비되고, 상기 탐지장비(10)가 분석하여 선별 선택한 해당 트래픽을 우회경로에 연결된 라우터(L2)에서 유도하여 상기 가공처리장비(20, 30)로 전송하고, 상기 가공처리장비(20, 30)가 출력하는 트래픽을 우회경로에 연결된 또 다른 라우터(L3)로 전송한다.

[0051] 상기 트래픽 유도장비(40)는 상기 탐지장비(10)가 전송하는 선별 선택된 해당 트래픽에 대한 정보를 우회경로에 연결된 라우터(L2)에 전송하고, 이를 전송받은 라우터(L2)는 입력되는 트래픽 중에서 해당 트래픽을 유도장비(40)로 전송하여 해당 트래픽이 우회경로에 유도되도록 한다.

[0052] 상기 탐지장비(10)와 트래픽 유도자이(40)는 외부 네트워크에서 사용자 단말로 향하는 하향 트래픽을 탐지 및 유도할 수도 있고, 사용자 단말에서 외부 네트워크로 향하는 상향 트래픽을 탐지 및 유도할 수도 있고, 하향 트래픽과 상향 트래픽을 모두, 그리고 동시에 탐지 및 유도할 수도 있다.

[0053] 이상에서 본 발명을 설명함에 있어 첨부된 도면을 참조하여 특정 구조를 갖는 네트워크 트래픽 처리 시스템에 대해 설명하였으나 본 발명은 당업자에 의하여 다양한 변형 및 변경이 가능하고, 이러한 변형 및 변경은 본 발명의 보호범위에 속하는 것으로 해석되어야 한다.

부호의 설명

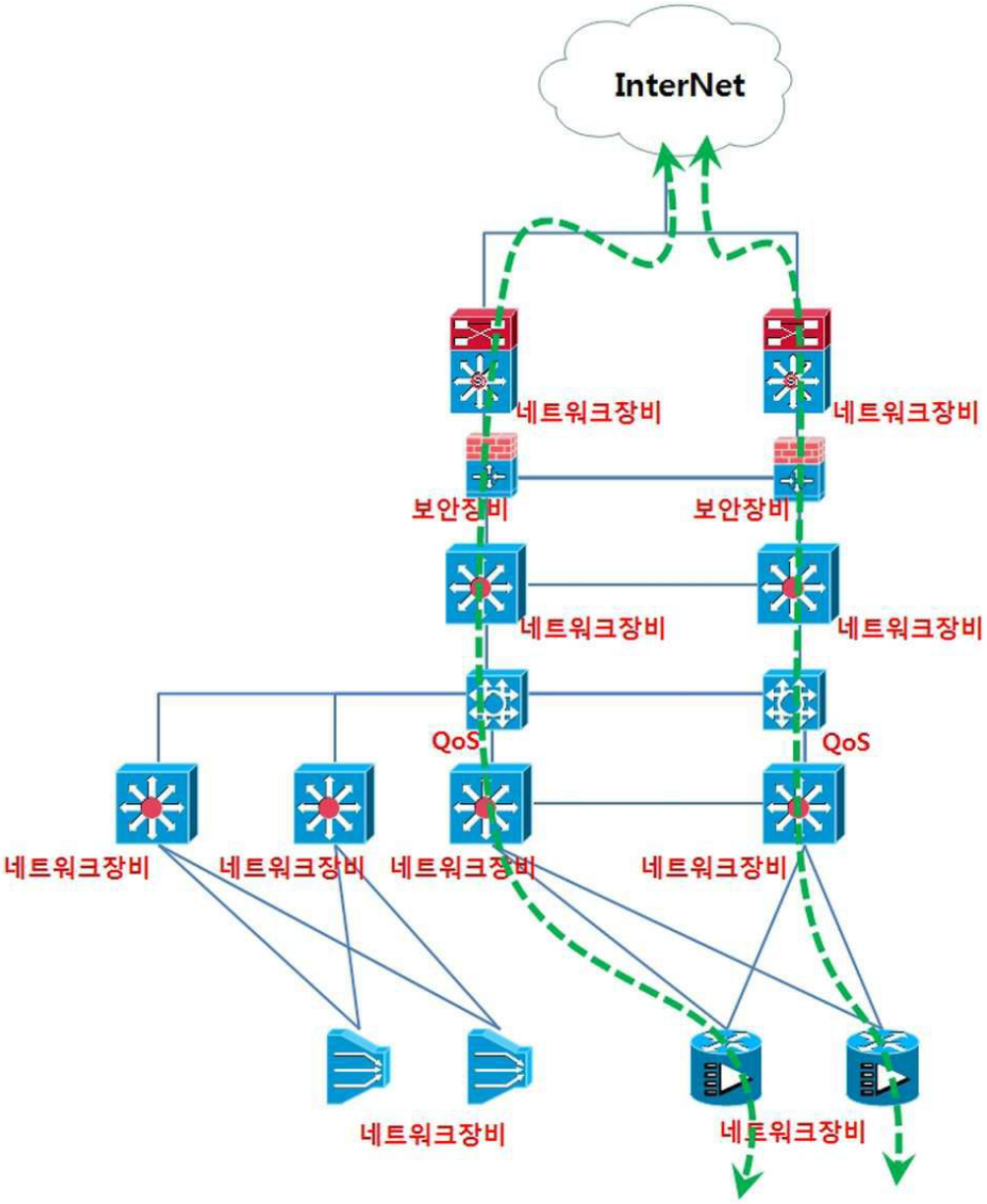
[0054] L1~L4 : 라우터 10 : 탐지장비

20 : QoS장비 30 : 보안장비

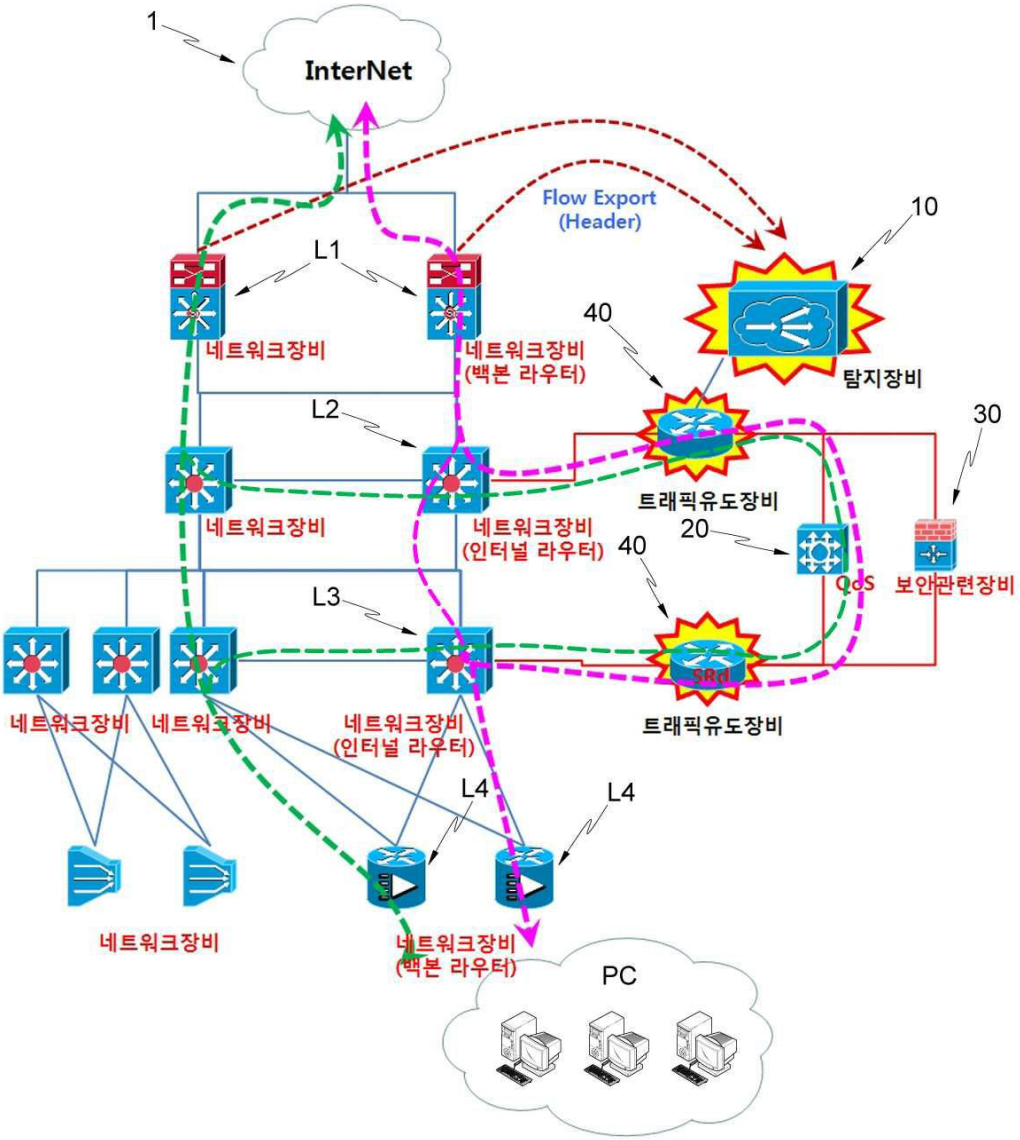
40 : 트래픽 유도장비

도면

도면1


InterNet
네트워크장비
네트워크장비
보안장비
보안장비
네트워크장비
네트워크장비
QoS
QoS
네트워크장비
네트워크장비
네트워크장비
네트워크장비
네트워크장비
네트워크장비

도면2


1
InterNet
Flow Export
(Header)
10
L1
40
네트워크장비
네트워크장비
(백본 라우터)
탐지장비
L2
30
트래픽유도장비
네트워크장비
네트워크장비
(인터널 라우터)
40
20
QoS
보안관련장비
L3
SRd
네트워크장비
네트워크장비
네트워크장비
(인터널 라우터)
트래픽유도장비
L4
L4
네트워크장비
네트워크장비
(백본 라우터)
PC