



(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2014년04월01일
 (11) 등록번호 10-1376301
 (24) 등록일자 2014년03월13일

(51) 국제특허분류(Int. Cl.)
 H04L 12/24 (2006.01) H04L 12/851 (2013.01)
 H04L 12/26 (2006.01)
 (21) 출원번호 10-2012-0117676
 (22) 출원일자 2012년10월23일
 심사청구일자 2012년10월23일
 (56) 선행기술조사문헌
 KR101144332 B1*
 *는 심사관에 의하여 인용된 문헌

(73) 특허권자
신동원
 경기도 고양시 덕양구 화신로 105, 2301동 203호
 (행신동, 햇빛마을)
주식회사 프라이머리넷
 경기도 부천시 원미구 부일로233번길 18, 송래프라자 902 (상동)
 (72) 발명자
신동원
 경기도 고양시 덕양구 화신로 105, 2301동 203호
 (행신동, 햇빛마을)
 (74) 대리인
최지연, 정중원, 이명택

전체 청구항 수 : 총 1 항

심사관 : 문형섭

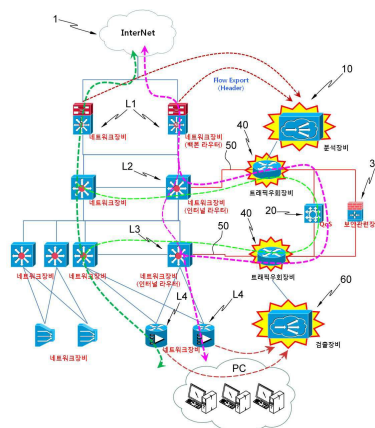
(54) 발명의 명칭 **네트워크 트래픽 관리 시스템**

(57) 요약

본 발명은 다수의 라우터들을 갖는 네트워크에서 트래픽을 관리하여 원활할 네트워크 서비스가 제공되도록 하는 네트워크 트래픽 관리 시스템에 관한 것으로서, 보다 상세하게는 서로서로 연결된 라우터들이 제공하는 기존의 통신경로에 추가하여 별도로 추가통신경로를 만들고 이 추가통신경로에 본 시스템의 서비스를 위한 장비들을 설치하여 본 시스템에 문제가 발생되더라도 기존 네트워크의 서비스에는 어떠한 악영향도 주지 아니하고, 트래픽의 전송속도와 처리순서를 조절하여 서비스 품질을 높이는 QoS장비는 모든 QoS 대상 트래픽을 처리하는 것이 아니고 해당 네트워크에서 통신되는 전체 트래픽의 양이 기준치를 초과하는 때에 비로서 QoS 대상 트래픽을 처리하도록 하여, QoS장비의 부하를 줄여주고 전체 트래픽의 양이 적음에도 QoS장비에서 트래픽을 처리하여 오히려 트래픽의 전송속도가 느려져 서비스 품질이 저하되지 않도록 하는 네트워크 트래픽 관리 시스템에 관한 것이다.

본 발명에 따른 네트워크 트래픽 관리 시스템은 트래픽의 통신경로를 제공하는 라우터들이 서로서로 연결되어 있는 네트워크에서 두 라우터를 별도로 연결하여 추가되는 추가통신경로; 별도로 추가된 상기 추가통신경로 상에 구비되고, 입력되는 트래픽의 전송속도와 처리순서를 조절하는 QoS장비; 네트워크의 어느 한 라우터로 입력되는 트래픽을 분석하는 분석장비; 네트워크의 라우터들 중에서 백본 라우터로 입력되는 트래픽의 양을 검출하는 검출장비; 상기 추가통신경로에 구비되어 트래픽을 상기 QoS장비로 우회 및 라우터로 복귀시키는 우회장비;를 포함하되, 상기 우회장비는 상기 검출장비에서 검출된 트래픽의 양이 기준치를 초과하는 때에 비로서 상기 분석장비가 전송하는 QoS 대상 트래픽을 우회시키는 것을 특징으로 한다.

대표도 - 도2



특허청구의 범위

청구항 1

트래픽의 통신경로를 제공하는 라우터들이 서로서로 연결되어 있는 네트워크에서 두 라우터를 별도로 연결하여 추가되는 추가통신경로(50);

별도로 추가된 상기 추가통신경로(50) 상에 구비되고, 입력되는 트래픽의 전송속도와 처리순서를 조절하는 QoS 장비(20);

네트워크의 어느 한 라우터로 입력되는 트래픽을 분석하는 분석장비(10);

네트워크의 라우터들 중에서 백본 라우터로 입력되는 트래픽의 양을 검출하는 검출장비(60);

상기 추가통신경로(50)에 구비되어 트래픽을 상기 QoS장비(20)로 우회 및 라우터로 복귀시키는 우회장비(40);를 포함하되,

상기 검출장비(60)는 연결된 라우터에 입출력되는 트래픽의 패킷 양을 검출하여, 실시간으로 해당 네트워크에서 입출력되는 전체 트래픽 양을 파악하고, 파악된 전체 트래픽의 양이 기준치를 초과하는 때에 이를 상기 우회장비(40)로 알리며,

상기 우회장비(40)는 상기 검출장비(60)에서 검출된 트래픽의 양이 기준치를 초과하는 때에 상기 분석장비(10)가 전송하는 QoS대상 트래픽을 우회시키고,

상기 추가통신경로(50) 상에 구비되고, 입력되는 트래픽의 악성코드나 바이러스의 감염 여부를 판단하여 차단하는 보안장비(30);를 더 포함하고,

상기 분석장비(10)는 네트워크로 입력되는 트래픽을 분석하여 상기 QoS장비(20)에서 처리가 필요한 QoS 대상 트래픽과 상기 보안장비(30)에서 처리가 필요한 보안 대상 트래픽을 추출하고, 추출된 트래픽들에 대한 정보를 상기 우회장비(40)로 전송하는 것을 특징으로 하는 네트워크 트래픽 관리 시스템.

청구항 2

삭제

명세서

기술분야

[0001] 본 발명은 다수의 라우터들을 갖는 네트워크에서 트래픽을 관리하여 원활할 네트워크 서비스가 제공되도록 하는 네트워크 트래픽 관리 시스템에 관한 것으로서, 보다 상세하게는

[0002] 서로서로 연결된 라우터들이 제공하는 기존의 통신경로에 추가하여 별도로 추가통신경로를 만들고 이 추가통신 경로에 본 시스템의 서비스를 위한 장비들을 설치하여 본 시스템에 문제가 발생되더라도 기존 네트워크의 서비스에는 어떠한 악영향도 주지 아니하고,

[0003] 트래픽의 전송속도와 처리순서를 조절하여 서비스 품질을 높이는 QoS장비는 모든 QoS 대상 트래픽을 처리하는 것이 아니고 해당 네트워크에서 통신되는 전체 트래픽의 양이 기준치를 초과하는 때에 비로서 QoS 대상 트래픽을 처리하도록 하여, QoS장비의 부하를 줄여주고 전체 트래픽의 양이 적음에도 QoS장비에서 트래픽을 처리하여 오히려 트래픽의 전송속도가 느려져 서비스 품질이 저하되지 않도록 하는 네트워크 트래픽 관리 시스템에 관한 것이다.

배경기술

[0004] 최근 인터넷 통신기술이 급속히 발전함에 따라 단위 네트워크의 수가 무수히 많아지고 있으며, 네트워크 상호

간과 네트워크와 사용자 단말기 간의 데이터 트래픽(데이터 통신) 양도 많아지고 있다.

- [0005] 일반적으로 하나의 네트워크(내부망)에는 수많은 사용자 단말기가 연결되며, 여러 외부 네트워크(외부망)와 연결된다.
- [0006] 그리고 네트워크에는 여러 경로(사용자 단말이나 외부 네트워크)에서 입력되는 트래픽을 목적지에 최적의 통신 경로를 통해 신속히 전송하기 위해 라우터들이 다수 구비된다.
- [0007] 네트워크에는 트래픽의 품질을 높이기 위한 장비로서, 입출력되는 트래픽의 전송 속도를 조절하고 처리순서를 조절하는 QoS장비와, 트래픽에 포함된 악성코드 등을 필터링하는 보안장비가 구비된다.
- [0008] 도1은 일반적인 네트워크의 구성도를 도시한 것으로서, 도면에서 확인할 수 있듯이, 다수의 라우터를 상호 연결하는 통신경로에 QoS장비와 보안장비가 설치되고,
- [0009] 상기 QoS장비와 보안장비는 네트워크로 입력되는 모든 트래픽을 가공처리할 수 있도록 각각 다수개가 구비된다.
- [0010] 다시 말해 외부 네트워크와 사용자 단말기 간을 연결하는 라우터들에 의해 설정 가능한 모든 통신경로에는 하나 이상의 QoS장비와 보안장비가 구비된다.
- [0011] 위와 같은 종래기술에 따른 네트워크 구성은 다음과 같은 여러 문제가 있다.
- [0012] 첫째, 해당 네트워크가 외부 네트워크와 사용자 단말기 간을 연결하는 모든 통신경로 상에 QoS장비와 보안장비가 구비되도록 하기 위해 많은 수의 QoS장비와 보안장비가 필요하다.
- [0013] 둘째, 트래픽 양이 늘어나거나 해당 네트워크에 연결되는 외부 네트워크나 사용자 단말이 늘어나 라우터를 추가 설치하는 때에 일반적으로 QoS장비와 보안장비도 동반되어 추가 설치된다.
- [0014] 셋째, QoS장비와 보안장비에 장애가 발생한 때에 장애가 발생된 QoS장비와 보안장비를 거치는 통신경로를 통한 트래픽 서비스의 중단 또는 예러가 발생한다.
- [0015] 넷째, 각각의 보안장비는 입력되는 트래픽의 정보 전체(즉, 헤더정보와 콘텐츠정보)에 대하여 악성코드나 바이러스가 포함되어 있는지를 검사하기 때문에 시간이 오래 소요되고, 일명 좀비PC에서 전송되는 트래픽의 경우 보안장치에서 비정상 트래픽으로 걸러내지 못하는 일이 종종 발생된다.
- [0016] 위와 같이 종래의 일반적인 네트워크가 갖는 문제를 해결하기 위해 본 출원인은 등록특허 제1144332호 "네트워크 트래픽 처리 시스템"을 제안하여, 네트워크의 기존 통신경로에 추가하여 별도의 추가통신경로(즉, 추가통신경로(50))를 만들고, 추가통신경로에 QoS장비와 보안장비를 설치하고, 해당 네트워크로 입출력되는 트래픽 중에서 QoS 대상 트래픽과 보안 대상 트래픽을 추가통신경로로 우회시켜 처리함으로써 위와 같은 문제를 해결하였다.
- [0017] 그런데 본 출원인의 상기 등록특허 제1144332호는 모든 QoS 대상 트래픽을 우회시켜 추가통신경로(50)에 설치된 QoS장비가 처리하도록 하고 있어서, QoS장비의 처리 부하를 가중시키고 경우에 따라서는 오히려 트래픽의 전송 속도를 느리게 하는 문제가 있다.
- [0018] 즉, 해당 네트워크에서 입출력되는 전체 트래픽의 양이 적어서 QoS 대상 트래픽을 처리(즉, 속도조절 및 처리순서 조절)하지 아니하여도 해당 네트워크에서 트래픽의 흐름이 원활하게 이루어질 것인데에도 불구하고 QoS 대상

트래픽이라는 이유만으로 QoS장비에서 이를 처리함으로써, QoS장비의 처리 부하가 가중되고, 처리에 따른 시간 만큼 트래픽의 전송속도가 느려진다.

[0019] 이처럼 해당 네트워크에서 입출력되는 전체 트래픽의 양과 무관하게 모든 QoS 대상 트래픽을 처리함에 따른 문제는 도1에 도시된 일반적인 네트워크에서도 발생된다.

발명의 내용

해결하려는 과제

[0020] 본 발명은 위와 같이 종래기술에 따른 본 출원인의 등록특허가 갖는 문제를 해결하기 위해 안출된 발명으로서,

[0021] 해당 네트워크로 입출력되는 전체 트래픽의 양이 기준치 이하일 때에는 QoS 대상 트래픽을 별도로 처리하지 않고, 기준치를 초과하는 때에 비로서 처리함으로써 QoS장비의 처리 부하를 경감시키고 보다 고품질의 트래픽 서비스를 제공할 수 있는 네트워크 트래픽 관리 시스템을 제공함을 목적으로 한다.

과제의 해결 수단

[0022] 이와 같은 목적을 달성하기 위한 본 발명에 따른 네트워크 트래픽 관리 시스템은

[0023] 트래픽의 통신경로를 제공하는 라우터들이 서로서로 연결되어 있는 네트워크에서 두 라우터를 별도로 연결하여 추가되는 추가통신경로;

[0024] 별도로 추가된 상기 추가통신경로 상에 구비되고, 입력되는 트래픽의 전송속도와 처리순서를 조절하는 QoS장비;

[0025] 네트워크의 어느 한 라우터로 입력되는 트래픽을 분석하는 분석장비;

[0026] 네트워크의 라우터들 중에서 백본 라우터로 입력되는 트래픽의 양을 검출하는 검출장비;

[0027] 상기 추가통신경로에 구비되어 트래픽을 상기 QoS장비로 우회 및 라우터로 복귀시키는 우회장비;를 포함하되,

[0028] 상기 우회장비는 상기 검출장비에서 검출된 트래픽의 양이 기준치를 초과하는 때에 비로서 상기 분석장비가 전송하는 QoS 대상 트래픽을 우회시키는 것을 특징으로 한다.

[0029] 그리고 상기 추가통신경로 상에 구비되고, 입력되는 트래픽의 악성코드나 바이러스의 감염 여부를 판단하여 차단하는 보안장비;를 더 포함하는 것을 특징으로 한다.

발명의 효과

[0030] 이와 같은 구성을 갖는 본 발명에 따른 네트워크 트래픽 관리 시스템은 네트워크의 기존 통신경로에 별도로 추가한 추가통신경로를 만들고, 이 추가통신경로에 본 시스템에 따른 장비들을 설치함으로써 본 시스템에 문제가 발생되더라도 기존 네트워크는 아무런 영향을 받지 않고 네트워크 서비스를 계속해서 제공할 수 있고,

[0031] 이에 더불어 QoS 대상 트래픽이라는 이유만으로 모든 QoS 대상 트래픽을 처리하는 것이 아니고 해당 네트워크에서 입출력되는 전체 트래픽 양이 기준치를 초과하여 네트워크 서비스의 품질을 저하시킬 우려가 있는 때에 비로서 QoS 대상 트래픽을 추가통신경로로 우회시키고 QoS장비가 우회된 QoS 대상 트래픽을 처리하도록 하여, QoS장비의 처리 부하를 경감시키고 네트워크 서비스의 품질을 한 차원 업그레이드시킨

[0032] 네트워크 트래픽 관리 시스템으로서, 산업발전에 매우 유용한 발명이다.

도면의 간단한 설명

[0033] 도 1 은 종래기술에 따른 일반적인 네트워크 구성도.

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

발명을 실시하기 위한 구체적인 내용

- [0034] 이하, 도면을 참조하여 본 발명에 따른 네트워크 트래픽 관리 시스템에 대하여 보다 구체적으로 설명한다.
- [0035] 본 발명의 구성을 보다 구체적으로 설명하기에 앞서,
- [0036] 본 발명은 다양한 변경을 가할 수 있고 여러 가지 형태를 가질 수 있는 바, 구현예(態樣, aspect)(또는 실시예)들을 본문에 상세하게 설명하고자 한다. 그러나 이는 본 발명을 특정한 개시 형태에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술범위에 포함되는 모든 변경, 균등물 내지 대체물을 포함하는 것으로 이해되어야 한다.
- [0037] 각 도면에서 동일한 참조부호, 특히 십의 자리 및 일의 자리 수, 또는 십의 자리, 일의 자리 및 알파벳이 동일한 참조부호는 동일 또는 유사한 기능을 갖는 부재를 나타내고, 특별한 언급이 없을 경우 도면의 각 참조부호가 지칭하는 부재는 이러한 기준에 준하는 부재로 파악하면 된다.
- [0038] 또 각 도면에서 구성요소들은 이해의 편의 등을 고려하여 크기나 두께를 과장되게 크거나(또는 두껍게) 작게(또는 얇게) 표현하거나, 단순화하여 표현하고 있으나 이에 의하여 본 발명의 보호범위가 제한적으로 해석되어서는 안 된다.
- [0039] 본 명세서에서 사용한 용어는 단지 특정한 구현예(태양, 態樣, aspect)(또는 실시예)를 설명하기 위해 사용된 것으로, 본 발명을 한정하려는 의도가 아니다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 출원에서, ~포함하다~ 또는 ~이루어진다~ 등의 용어는 명세서 상에 기재된 특징, 숫자, 단계, 동작, 구성요소, 부분품 또는 이들을 조합한 것이 존재함을 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성요소, 부분품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.
- [0040] 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. 일반적으로 사용되는 사전에 정의되어 있는 것과 같은 용어들은 관련 기술의 문맥 상 가지는 의미와 일치하는 의미를 가지는 것으로 해석되어야 하며, 본 출원에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.
- [0041] 도2에서 보는 바와 같이 본 발명에 따른 네트워크 트래픽 처리 시스템은 트래픽의 최적 통신경로를 제공하는 라우터들(L1~L4)을 갖는 기존 네트워크에서 본 시스템에 따른 서비스 제공을 위해 별도로 추가되는 추가통신경로(50)와, 추가통신경로(50)에 설치되는 QoS장비(20), 보안장비(30) 및 우회장비(40), 그리고 추가통신경로(50)로 우회될 트래픽을 분석 및 검출하는 분석장비(10)와 검출장비(60)를 포함한다.
- [0042] 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.
- [0043] 상기 네트워크에는 다수의 라우터(L1~L4)들로 구성되고, 라우터(L1~L4)들은 서로 그물망 처럼 연결되어 입력되는 트래픽이 목적지까지 최적의 통신경로를 통해 전송되도록 한다.
- [0044] 참고로, 라우터(L1~L4)들을 상호 연결하여 트래픽이 전송되는 통신경로를 '기존 통신경로'라고 정의하고, 본 발명의 시스템 구현을 위해 두 라우터를 상호 연결하여 추가적으로 별도 연결한 경로를 '추가통신경로'라고 정의한다.

- [0045] 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.
- [0046] 상기 분석장비(10)는 네트워크로 입력되는 트래픽을 분석하여 상기 QoS장비(20)에서 처리가 필요한 QoS 대상 트래픽과 상기 보안장비(30)에서 처리가 필요한 보안 대상 트래픽을 추출하고, 추출된 트래픽들에 대한 정보를 상기 트래픽 우회장비(40)로 전송한다.
- [0047] 상기 검출장비(60)는 해당 네트워크로 입출력되는 트래픽의 양을 검출하고, 검출된 트래픽 양에 대한 정보를 상기 트래픽 우회장비(40)로 전송한다.
- [0048] 상기 분석장비(10)와 검출장비(60)는 상기 라우터를 통해 네트워크로 입출력되는 트래픽의 정보를 전송받아 각각 분석 및 검출을 하게 되는데, 트래픽이 네트워크로 처음 입력되는 백본 라우터(L1, L4)로부터 트래픽 정보를 전송받아 보다 신속한 처리가 되도록 하는 것이 바람직하다.
- [0049]
- [0050] 상기 분석장비(10)는 연결된 라우터에서 입력되는 트래픽의 패킷 중에서 추출한 플로우 정보를 전송받아 해당 트래픽을 분석한다.
- [0051] 여기서, 상기 플로우 정보는 라우터로 입력되는 트래픽의 패킷에서 헤더부분의 정보를 추출하고, 추출된 헤더 정보를 설정된 양식으로 변환한 정보로서, 송신처 IP, 수신처 IP, 프로토콜, 포트, 어플리케이션 등에 대한 정보를 포함한다.
- [0052]
- [0053] 상기 분석장비(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, 트로이안, 백도어, 디도스, 악성봇 등)가 포함된 트래픽을 선별하여 선택한다. 이외에도 분석장비(10)가 트래픽을 분석하여 선별 선택하는 방법에는 사용자의 설정에 따라 다양한 것이 있을 것이다.
- [0054] 상기 분석장비(10)가 추가통신경로(50)의 보안장비로 보낼 비정상 트래픽(예, 악성봇, 바이러스, 악성코드 등)으로 선별 선택할 때에는 신속하면서도 비정상 트래픽임에도 간과하는 상황이 발생하는 것을 최소화하는 것이 바람직하다.
- [0055] 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.
- [0056] 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.
- [0057] 그리고 상기 비정상 트래픽 생성 소스원은 IP, 포트, 프로토콜, 어플리케이션 등의 정보로 데이터베이스에 등록 저장된다.

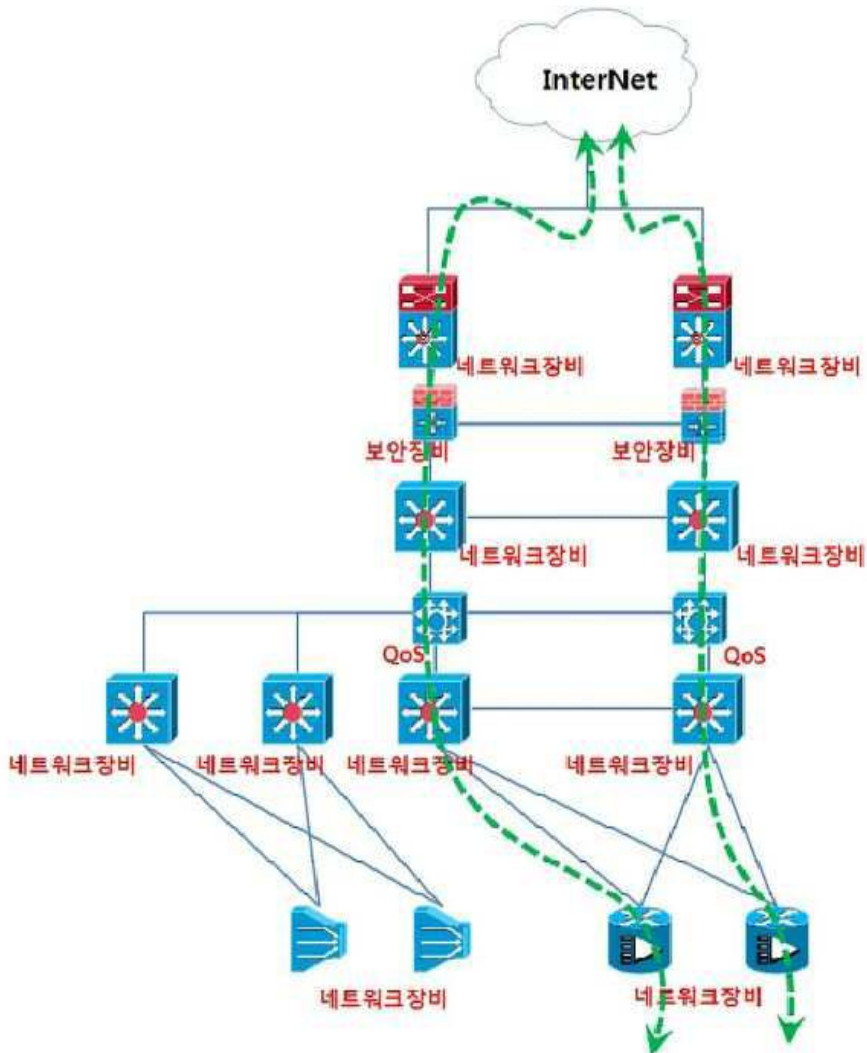
- [0058] 그리고 상기 분석장비(10)가 상기 라우터(L1)가 전송하는 플로우 정보로부터 해당 트래픽에 악성코드(바이러스)가 포함되어 있는 것으로 탐지되고, 악성코드의 유입이 트래픽의 송신처 PC의 감염에 의한 것으로 파악될 때에는 해당 PC, 즉, 바이러스나 악성 봇에 감염된 PC의 IP를 추출하여 데이터베이스화하여, 감염된 PC의 관리에 사용할 수 있도록 한다.
- [0059] 상기 검출장비(60)는 연결된 라우터에 입출력되는 트래픽의 패킷 양을 검출하여, 그때그때 실시간으로 해당 네트워크에서 입출력되는 전체 트래픽 양을 파악하고, 파악된 전체 트래픽의 양이 기준치를 초과하는 때에 이를 상기 우회장비(40)로 알린다.
- [0060] 상기 우회장비(40)는 상기 분석장비(10)가 전송하는 보안 대상 트래픽에 해당하는 트래픽은 모두 추가통신경로(50)로 우회시켜 상기 보안장비(30)로 전송하고, 상기 분석장비(10)가 전송하는 QoS 대상 트래픽은 상기 검출장비(60)로부터 현재 네트워크의 전체 트래픽 양이 기준치를 초과하고 있다는 정보가 전송된 때에만 상기 추가통신경로(50)로 우회시켜 상기 QoS장비(20)로 전송한다.
- [0061] 상기 QoS장비(20)와 보안장비(30)는 네트워크의 트래픽 서비스 품질을 높이는 장비로서, 각각 입력되는 QoS 대상 트래픽의 전송속도와 처리순서를 조절하고, 보안 대상 트래픽을 차단시키거나 포함된 악성코드 등을 필터링하여 제거한다.
- [0062] 다시 말해, 상기 QoS장비(20)는 대역폭의 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 하고, 상기 보안장비(30)는 트래픽에 악성코드가 포함되어 있는 경우 필터링하여 악성코드를 제거하거나 트래픽을 전송을 차단한다. 상기 QoS장비(20)와 보안장비(30) 자체는 공지기술에 해당하므로 이에 대한 구체적인 설명은 생략한다.
- [0063] 상기 QoS장비(20)와 보안장비(30)는 네트워크의 라우터(L1~L4)들을 상호 연결하는 기존 통신경로 외에 추가적으로 설치하여 두 라우터(L2, L3)를 연결하는 추가통신경로(50)에 구비되어, 어느 한 라우터에서 입력되는 트래픽을 가공처리 한 후에 다른 라우터로 출력한다. 이때, 추가통신경로(50)에 연결되는 두 라우터에서 트래픽이 입력되는 라우터(하향 트래픽 기준시; L2)는 상기 분석장비(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.
- [0064] 상기 트래픽 우회장비(40)는 상기 추가통신경로(50)의 두 라우터(L2, L3)와 상기 QoS장비(20) 및 보안장비(30) 사이에 각각 구비되고, 상기 분석장비(10)가 분석하여 선별 선택한 해당 트래픽과 상기 검출장비(60)에 의해 검출된 트래픽을 추가통신경로(50)에 연결된 라우터(L2)에서 유도하여 상기 QoS장비(20)와 보안장비(30)로 전송하고, 상기 QoS장비(20)와 보안장비(30)가 출력하는 트래픽을 추가통신경로(50)에 연결된 또 다른 라우터(L3)로 전송한다.
- [0065] 상기 트래픽 우회장비(40)는 상기 분석장비(10)가 전송하는 선별 선택된 해당 트래픽에 대한 정보를 추가통신경로(50)에 연결된 라우터(L2)에 전송하고, 이를 전송받은 라우터(L2)는 입력되는 트래픽 중에서 해당 트래픽을 우회장비(40)로 전송하여 해당 트래픽이 추가통신경로(50)에 우회되도록 한다.
- [0066] 이상에서 본 발명을 설명함에 있어 첨부된 도면을 참조하여 특정 형상과 구조를 갖는 네트워크 트래픽 관리 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

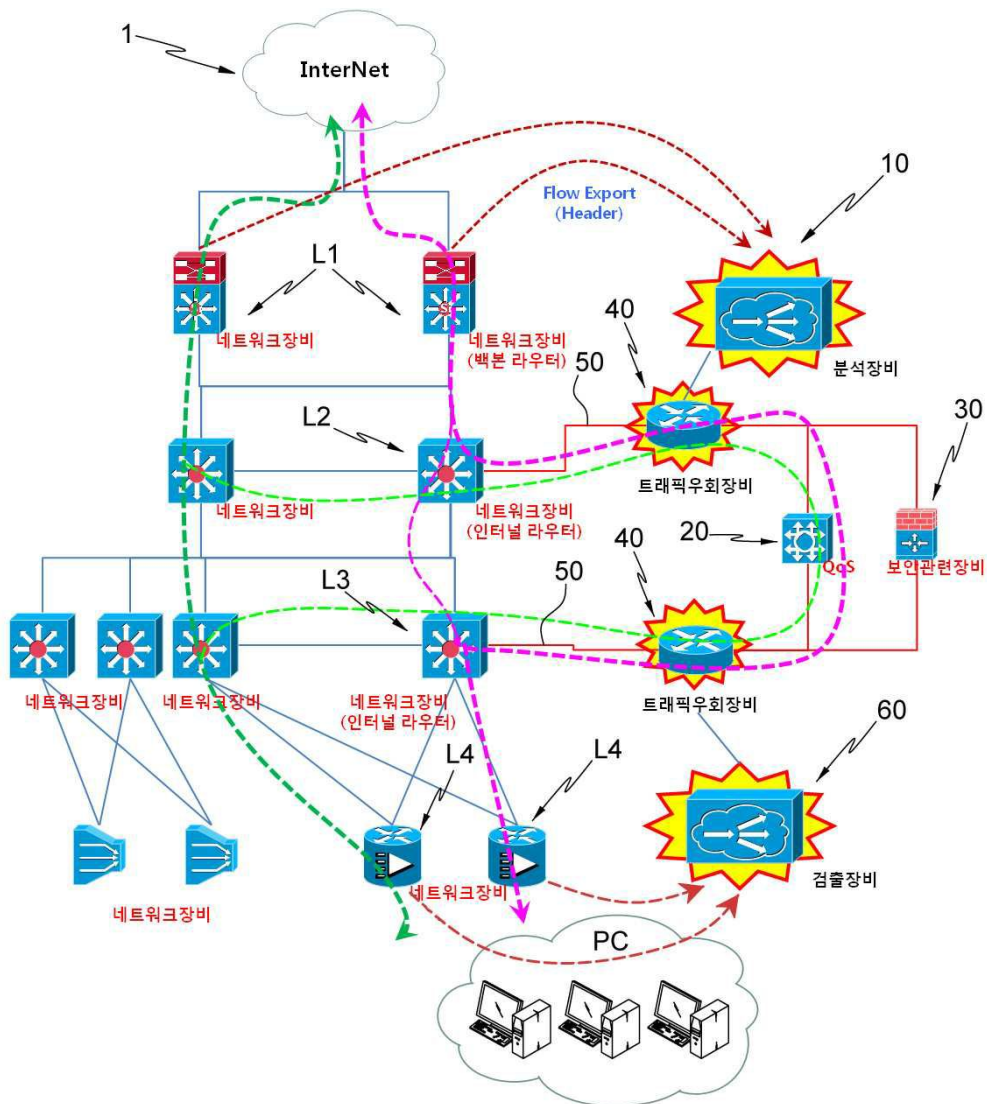
- [0067] L1~L4 : 라우터
 10 : 분석장비
 20 : QoS장비
 40 : 우회장비
 60 : 검출장비
 10 : 분석장비
 30 : 보안장비
 50 : 추가통신경로

도면

도면1



도면2



【심사관 직권보정사항】

【직권보정 1】

【보정항목】 청구범위

【보정세부항목】 제1항

【변경전】

별도로 (~) QoS장비

【변경후】

별도로 (~) QoS장비