

EX 1005



(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2007년10월09일
(11) 등록번호 10-0765340
(24) 등록일자 2007년10월02일

(51) Int. Cl.

H04L 12/22(2006.01) H04L 12/26(2006.01)

H04L 12/28(2006.01)

(21) 출원번호 10-2006-0028732

(22) 출원일자 2006년03월30일

심사청구일자 2006년03월30일

(65) 공개번호 10-2006-0035680

공개일자 2006년04월26일

(56) 선행기술조사문헌

KR1020030047958 A

JP2002111732 A

(73) 특허권자

지니네트웍스(주)

경기 성남시 수정구 복정동 423 동서울대학창업보육센터 5404

(72) 발명자

이동범

경기 의왕시 내손동 반도보라 208동 702호

김계연

경기 의왕시 오전동 23 대명구름채 아파트 203동 1002호

(뒷면에 계속)

(74) 대리인

최덕용

전체 청구항 수 : 총 2 항

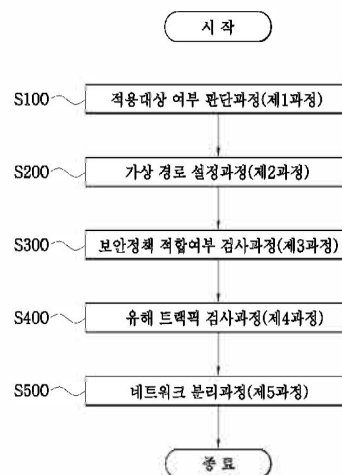
심사관 : 김병균

(54) 가상의 인라인 네트워크 보안방법

(57) 요약

본 발명은 네트워크 패킷을 분석하여 보안 정책의 적합 여부와 침입 여부의 판단하기 위한 시스템으로, 물리적으로 인라인(In-Line) 구조를 설치하지 않으면서도, 네트워크 세그먼트 또는 동일 VLAN 상에 존재하는 단말기 중 통제가 필요한 단말기들의 MAC 주소 요청 응답을 보안장비의 MAC 주소로 변조하여 응답함으로써, 단말기들의 통신 내용이 보안장비를 경유하게 한 후, 보안 정책의 적합 여부를 판단하여 접근 제어를 수행할 수 있도록 하는 가상의 인라인 네트워크 보안 방법에 관한 것이며, 그 구성은, 특정 장비가 가상 경로 설정의 적용 대상이 되는지의 여부를 판단하는 제1 과정(S100)과, 상기 제1 과정(S100)을 통해 특정장비가 가상 경로 설정대상에 적합하다 판단되면 적용 대상 장비의 가상 경로를 설정하는 제2 과정(S200)과, 상기 설정된 가상 경로의 트래픽이 보안 정책에 적합한가를 검사하는 제3 과정(S300)과, 상기 가상 경로의 트래픽이 유해 트래픽인가를 검사하는 제4 과정(S400)과, 상기 가상 경로의 시스템을 네트워크에서 분리하는 제5 과정(S500)을 포함하여 된 것이다.

도 3



(72) 발명자

이민상

경기 하남시 신장2동 현대홈타운 101동 1806호

김용권

경기 성남시 분당구 수내동 양지한양 501동 502호

박준우

경기 용인시 수지구 죽전1동 현대홈타운 3차 2

단지, 501동 1501호

특허청구의 범위

청구항 1

복수개의 단말기와 상기 단말기들과 연결되는 L2스위치(허브)로 이루어지는 내부망이 복수개 형성되고, 동시에 DB(데이터 베이스) 서버와, APP(Application) 서버와 연결되는 L2 스위치(허브)가 구성되며, 상기 허브들과 연결되는 백본스위치와, 상기 백본스위치에 연결되는 인라인 방화벽과, 상기 인라인방화벽에 연결되는 라우터 및 인터넷을 포함하는 네트워크 장치에, 상기 각 내부 망의 허브와, DB서버 및 APP서버가 연결되는 L2 스위치(허브)에 각각 인라인(In-line) 시스템을 구축하여 된 인라인 네트워크 장치에 있어서,

상기 단말기(노드)에서 발생하는 MAC 요청 패킷을 모니터링 하는 단계(S110)와, 상기 MAC 요청 패킷의 출발지 주소 및 MAC 주소를 추출하는 단계(S120)와, 상기 추출된 MAC 요청 패킷의 출발지 주소 및 MAC 주소를 MAC주소, IP주소, OS(운영체제), 사용자, 사용시간 및 동작방법을 저장 및 확인할 수 있는 노드 테이블(TABLE)에 추가하는 단계(S130)와, 상기 추출한 노드에 대한 운영체제(OS) 추측(Guessing)하는 단계(S140)로 이루어져 특정 장비가 가상 경로 설정의 적용 대상이 되는지의 여부를 판단하는 제1 과정(S100);

상기 노드 테이블의 노드에 동작방법을 설정하는 단계(S210)와, 노드 테이블의 노드에 보안정책을 연결하는 단계(S220)와, 상기 동작방법에 의해 설정된 "가상 경로" 노드의 모든 MAC 주소 요청에 대해 가상 경로 시스템의 MAC 주소로 응답하는 단계(S230)로 이루어져 상기 제1 과정(S100)을 통해 특정장비가 가상 경로 설정대상에 적합하다 판단되면 적용 대상 장비의 가상 경로를 설정하는 제2 과정(S200);

상기 가상 경로 시스템으로 유입되는 패킷에서 프로토콜, 목적지 주소 및 목적지 포트 번호 등을 추출하는 단계(S310)와, 목적지 주소, 목적지 포트, 시간대 및 실행 여부를 저장 및 확인할 수 있는 보안정책 테이블을 참조하여 대응 여부를 결정하는 단계(S320)로 이루어져 상기 설정된 가상 경로의 트래픽이 보안 정책에 적합한가를 검사하는 제3 과정(S300);

패킷의 페이로드(payload)를 추출하는 단계(S410)와, 유해/악성 데이터베이스(DB)를 참조하는 단계(S420)와, 상기 패킷의 페이로드(payload)와 유해/악성 데이터베이스(DB)의 일치 여부를 판단하는 단계(S430)와, 상기 판단 단계(S430)에서 상기 패킷의 페이로드(payload)와 유해/악성 데이터베이스(DB)가 일치하면 상기 노드 테이블에 동작방법을 변경(차단)하는 단계(S440)와, 상기 판단단계(S430)에서 상기 패킷의 페이로드(payload)와 유해/악성 데이터베이스(DB)가 일치하지 아니하면 해당 패킷을 전송하는 단계(S450)와, 해당 행위에 대한 검사 기록 로그를 작성하는 단계(S460)로 이루어져 상기 가상 경로의 트래픽이 유해 트래픽인가를 검사하는 제4 과정(S400); 및

상기 노드 테이블의 동작방법(모드) 참조하여 악성 노드를 구분하는 단계(S510)와, 상기 악성 노드로 거트된 MAC 주소 응답 패킷을 주기적으로 전송하는 단계(S520)와, 상기 악성 노드의 모든 MAC 주소 요청에 대해 거트된 MAC 주소로 패킷을 발송하는 단계(S530)로 이루어져 상기 가상 경로의 시스템을 네트워크에서 분리하는 제5 과정(S500)을 포함하여 된 것을 특징으로 하는 가상의 인라인 네트워크 보안방법.

청구항 2

삭제

청구항 3

삭제

청구항 4

삭제

청구항 5

제 1 항에 있어서,

상기 제3과정(S300)의 보안정책 테이블을 참조하여 대응 여부를 결정하는 단계(S320)는, 상기 대응 여부를 판단하는 단계(S321)와, 상기 판단단계(S321)에서 허용일 경우에는 해당 패킷을 포워딩(forwarding)하는 단계(S322)와, 상기 판단단계(S321)에서 거부일 경우에는 해당 패킷을 폐기하는 단계(S323)로 구성된 것을 특징으로 하

는 가상의 인라인 네트워크 보안방법.

청구항 6

삭제

청구항 7

삭제

명세서

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

- <13> 본 발명은 네트워크 내의 침입 차단 시스템(Firewall) 및 침입 방지 시스템(Intrusion Prevention System)과 같이 네트워크 패킷을 분석하여 보안 정책의 적합 여부와 침입 여부의 판단하기 위한 시스템에 관한 것으로, 더욱 상세하게는 물리적으로 인라인(In-Line) 구조를 설치하지 않으면서도, 네트워크 세그먼트 또는 동일 VLAN 상에 존재하는 단말기 중 통제가 필요한 단말기들의 MAC 주소 요청 응답을 보안장비의 MAC 주소로 변조하여 응답함으로써, 단말기들의 통신 내용이 보안장비를 경유하게 한 후, 보안 정책의 적합 여부를 판단하여 접근 제어를 수행할 수 있도록 하는 가상의 인라인 네트워크 보안 방법에 관한 것이다.
- <14> 주지한 바와 같은 침입 차단 시스템이나 침입 방지 시스템과 같은 네트워크 보안 장비들은 설치 구성의 형태에 따라 라우터 모드(Router mode)와 브리지 모드(Bridge mode)로 나뉜다.
- <15> 상기 라우터 모드(Router mode)는 패킷이 입력되는 네트워크 인터페이스 카드의 IP 주소 대역과 패킷이 출력되는 네트워크 인터페이스 카드의 IP 주소 대역이 서로 상이하게 설치되는 형태이다.
- <16> 이러한 방식을 기존에 사용 중인 네트워크에 장비를 설치할 경우 기존 네트워크 IP 주소 형태를 변경해야 하는 작업이 수반된다.
- <17> 상기 브리지 모드(Bridge mode)는 상기 라우터 모드(Router mode)와는 달리 입력 네트워크 인터페이스의 카드와 출력 네트워크 인터페이스의 카드의 IP 대역이 동일한 네트워크 주소 대역을 사용하기 때문에 설치 시에 라우터 모드(Router mode)와 같이 네트워크 IP 변경 작업이 필요 없고, 단지 네트워크 라인을 물리적으로 절제 하여 장비를 삽입하면 되는 방식이다.
- <18> 한편, 일반적인 네트워크 보안 장비들은 상기 라우터 모드(Router mode) 또는 브리지 모드(Bridge mode)에 관계없이 기 설치된 네트워크 선을 단절하여 중간에 보안 장비를 설치하는 인라인(In-Line) 구성의 형태로 이루어진다.
- <19> 이와 같은 종래의 네트워크 보안 장비 설치하는 라우터 모드(Router mode)나 브리지 모드(Bridge mode)가 모두 인라인(In-line) 형태로 구성되어지는 관계로, 물리적 인라인(In-line) 구조는 설치 작업 시에 네트워크의 사용 중단, 정상적인 통신흐름이후에는 설치 후 속도 지연 현상, 설치 장비가 장애 시에는 다른 네트워크의 통신이 모두 두절되는 현상이 불가피 하였다.
- <20> 결국, 이와 같은 인라인(In-Line) 구성은 네트워크를 통과하는 모든 패킷을 볼 수 있게 됨에 따라 보안성이 높아지는 장점은 있으나, 상기 인라인(In-Line) 구성으로 인하여 모든 단말기들에게 동시에 속도 지연 현상 및 장애 시 전체 네트워크의 통신이 두절되는 문제점이 발생하게 되었다.
- <21> 이와 같은 종래의 시스템을 도 1을 참조하여 설명한다.
- <22> 도시된 바와 같이 종래의 네트워크 보안장치는 제1내부망(10)의 제1단말기(11)에서 제2내부망(20)의 제4단말기(21)로의 통신을 제한하기 위해서는 제1 L2스위치(14)와 백본스위치(40) 구간 사이에 제1보안장비(15)를 인라인(In-line)으로 설치하여 통신 트래픽을 제어하게 된다.
- <23> 상기 제1 L2스위치(14)와 백본스위치(40) 구간에 설치된 제1보안장비(15)는 제1내부망(10)에서 다른 망(네트워크)로 연결되는 모든 트래픽이 보안장비를 반드시 경유하도록 되어 있기 때문에 통신 대상 사이의 전달

되는 TCP/IP 패킷의 헤더 정보(출발지 주소, 목적지 주소, 목적지 포트 등)를 이용하여 정책에 부합 여부를 판단하여 통과 및 차단 여부를 결정하게 된다.

<24> 이러한 일반적인 인라인(In-line) 네트워크 보안장비 구성은 통신시의 네트워크 속도 지연 현상과 보안장비 장애 시 네트워크가 단절되는 부작용을 유발하게 된다.

<25> 또한, 제1내부망(10)에 있는 제1단말기(11)와 제2단말기(12)간의 통신 시에는 두 단말기간의 전달되는 패킷이 제1보안장비(15)를 경유하지 않기 때문에 접속을 제어할 수 없는 한계점을 지닌다.

발명이 이루고자 하는 기술적 과제

<26> 본 발명은 상기한 문제점을 해결하고자 창안된 것으로, 본 발명의 목적은 가상의 인라인(In-line) 기술로서, 실제 물리적인 구성은 인라인(in-line) 형태가 아니지만, 통신 당사자들이 보안장비를 경유하여 통신하게끔 함으로써 물리적인 인라인(In-line) 구성에서와 같은 보안 동작을 할 수 있도록 한 가상의 인라인 네트워크 보안 방법을 제공하는 것에 있다.

<27> 또한, 본 발명의 다른 목적은 네트워크에 보안장비 설치 시, 네트워크 중단 없이 장비를 설치할 수 있게 하며, 장비 장애 시에 종래에 발생하는 네트워크 장애 확산(Single point of failure)이 발생하지 않으며, 인가된 네트워크 장비는 가상의 인라인(in-line) 구성된 장비를 통하지 않고 통신할 수 있게 함으로써 속도 지연 현상을 배제시킨 가상의 인라인 네트워크 보안 방법을 제공하는 것에 있다.

<28> 또한, 본 발명의 다른 목적은 보안장비를 경유해서 외부로 나가는 트래픽뿐만 아니라 동일 네트워크 내에 있는 단말기 간의 통신 및 트래픽을 제어하는 가상의 인라인 네트워크 보안 방법을 제공하는 것에 있다.

<29> 또한, 본 발명의 또 다른 목적은 다수의 내부 망에 비인가 시스템의 사용통제 및 이상 트래픽을 발생시키는 시스템을 효과적으로 차단하는 용도에 적합하도록 한 가상의 인라인 네트워크 보안 방법을 제공하는 것에 있다.

발명의 구성 및 작용

<30> 이와 같은 목적을 달성하기 위한 본 발명은 복수개의 단말기와 상기 단말기들과 연결되는 L2스위치(허브)로 이루어지는 내부망이 복수개 형성되고, 동시에 DB(데이터 베이스) 서버와, APP(Application) 서버와 연결되는 L2스위치(허브)가 구성되며, 상기 허브들과 연결되는 백본스위치와, 상기 백본스위치에 연결되는 인라인 방화벽과, 상기 인라인방화벽에 연결되는 라우터 및 인터넷을 포함하는 네트워크 장치에, 상기 각 내부 망의 허브와, DB서버 및 APP서버가 연결되는 L2 스위치(허브)에 각각 인라인(In-line) 시스템을 구축하여 된 인라인 네트워크 장치에 있어서, 상기 단말기(노드)에서 발생하는 MAC 요청 패킷을 모니터링 하는 단계(S110)와, 상기 MAC 요청 패킷의 출발지 주소 및 MAC 주소를 추출하는 단계(S120)와, 상기 추출된 MAC 요청 패킷의 출발지 주소 및 MAC 주소를 MAC주소, IP주소, OS(운영체제), 사용자, 사용시간 및 동작방법을 저장 및 확인할 수 있는 노드 테이블(TABLE)에 추가하는 단계(S130)와, 상기 추출한 노드에 대한 운영체제(OS) 추측(Guessing)하는 단계(S140)로 이루어져 특정 장비가 가상 경로 설정의 적용 대상이 되는지의 여부를 판단하는 제1 과정(S100); 상기 노드 테이블의 노드에 동작방법을 설정하는 단계(S210)와, 노드 테이블의 노드에 보안정책을 연결하는 단계(S220)와, 상기 동작방법에 의해 설정된 "가상 경로" 노드의 모든 MAC 주소 요청에 대해 가상 경로 시스템의 MAC 주소로 응답하는 단계(S230)로 이루어져 상기 제1 과정(S100)을 통해 특정장비가 가상 경로 설정대상에 적합하다 판단되면 적용 대상 장비의 가상 경로를 설정하는 제2 과정(S200); 상기 가상 경로 시스템으로 유입되는 패킷에서 프로토콜, 목적지 주소 및 목적지 포트 번호 등을 추출하는 단계(S310)와, 목적지 주소, 목적지 포트, 시간대 및 실행 여부를 저장 및 확인할 수 있는 보안정책 테이블을 참조하여 대응 여부를 결정하는 단계(S320)로 이루어져 상기 설정된 가상 경로의 트래픽이 보안 정책에 적합한가를 검사하는 제3 과정(S300); 패킷의 페이로드(payload)를 추출하는 단계(S410)와, 유해/악성 데이터베이스(DB)를 참조하는 단계(S420)와, 상기 패킷의 페이로드(payload)와 유해/악성 데이터베이스(DB)의 일치 여부를 판단하는 단계(S430)와, 상기 판단단계(S430)에서 상기 패킷의 페이로드(payload)와 유해/악성 데이터베이스(DB)가 일치하면 상기 노드 테이블에 동작방법을 변경(차단)하는 단계(S440)와, 상기 판단단계(S430)에서 상기 패킷의 페이로드(payload)와 유해/악성 데이터베이스(DB)가 일치하지 아니하면 해당 패킷을 전송하는 단계(S450)와, 해당 행위에 대한 검사 기록 로그를 작성하는 단계(S460)로 이루어져 상기 가상 경로의 트래픽이 유해 트래픽인가를 검사하는 제4 과정(S400); 및 상기 노드 테이블의 동작방법(모드) 참조하여 악성 노드를 구분하는 단계(S510)와, 상기 악성 노드로 거짓된 MAC 주소 응답 패킷을 주기적으로 전송하는 단계(S520)와, 상기 악성 노드의 모든 MAC 주소 요청에 대해 거짓된 MAC

주소로 패킷을 발송하는 단계(S530)로 이루어져 상기 가상 경로의 시스템을 네트워크에서 분리하는 제5 과정(S500)을 포함하여 된 가상의 인라인 네트워크 보안방법을 특징으로 한다.

- <31> 이하, 첨부된 도면을 참조하여 본 발명의 바람직한 실시 예들을 보다 상세히 설명한다.
- <32> 도 2는 본 발명이 적용되는 가상의 인라인 네트워크 보안장치의 구성도이다.
- <33> 도시된 바와 같이, 본 발명이 적용되는 가상의 인라인 네트워크 보안장치는 종래의 구성과 다르게 일반 단말기와 같은 형태로 장비를 네트워크에 연결한 후 동작한다.
- <34> 즉, 복수개의 단말기와, 상기 단말기들과 연결되는 L2 스위치(허브)로 이루어지는 내부 망이 복수 개 형성되고, 동시에 DB(데이터베이스) 서버(33)와, APP(Application) 서버(34)와 연결되는 L2 스위치(허브)(32)가 구성되며, 상기 허브들과 연결되는 백본스위치(40)와, 상기 백본스위치(40)에 연결되는 인라인방화벽(50)과, 상기 인라인방화벽(50)에 연결되는 라우터(60) 및 인터넷을 포함하는 네트워크장치에 있어서, 상기 각 내부 망의 허브와, DB서버(33) 및 APP서버(34)가 연결되는 L2 스위치(허브)(32)에 각각 인라인(In-line)(16,26,35) 시스템을 구축하여 구성한 것이다.
- <35> 이와 같이 구성된 가상 인라인 네트워크 보안장치에 적용되는 본 발명에 있어서, 제1내부망(100)의 제1단말기(11)의 네트워크 통제를 실시하고자 하면, 상기 제1단말기(11)가 패킷을 통신 상대방이나 전달자(gateway)의 하드웨어 주소(MAC 주소)를 요청하게 되는데, 이러한 주소 요청을 가상의 인라인(16,26,35) 시스템이 감지하여 자신의 MAC주소로 제1단말기(11)에 응답을 한다.
- <36> 상기 응답 후에는 제1단말기(1)에서 발생하는 패킷이 가상의 인라인 시스템에 도달하기 때문에 패킷의 정보 및 데이터를 분석하여 접근제어를 수행하게 된다.
- <37> 또한, 동일 네트워크상에 있는 단말기들, 즉 제2, 또는 제3단말기가 제1단말기(11)와의 직접 패킷을 전달하는 것을 방지하기 위하여, 네트워크상의 단말기 중에 제1단말기(11)에게 직접 패킷을 전달하고자 하는 특정 단말기(12 또는 13)의 MAC 주소에 요청하는 응답에 대해서도 가상의 인라인 시스템이 자신의 MAC주소로 응답함으로써 제어 대상이 되는 제1단말기(11)와의 통신을 위해 입, 출력되는 모든 패킷은 보안센서를 경유하게 되는 것이다.
- <38> 도 3은 본 발명에 따른 가상의 인라인 네트워크 보안방법의 제어 흐름도이다.
- <39> 도시된 바와 같이, 본 발명에 따른 가상의 인라인 네트워크 보안방법은, 특정 장비가 가상 경로 설정의 적용 대상이 되는지의 여부를 판단하는 제1 과정(S100)과, 상기 제1 과정(S100)을 통해 특정장비가 가상 경로 설정대상에 적합하다 판단되면 적용 대상 장비의 가상 경로를 설정하는 제2 과정(S200)과, 상기 설정된 가상 경로의 트래픽이 보안 정책에 적합한가를 검사하는 제3 과정(S300)과, 상기 가상 경로의 트래픽이 유해 트래픽인가를 검사하는 제4 과정(S400)과, 상기 가상 경로의 시스템을 네트워크에서 분리하는 제5 과정(S500)을 포함한다.
- <40> 상기 제1 과정(S100)에서, 상기 보안 장비는 단말기 장비에서 발생하는 MAC address 요청(Request) 패킷을 분석하여, 출발지 주소와 MAC(Media Access Control) 주소를 추출한다.
- <41> 상기 출발지 주소와, MAC 주소, 클라이언트의 운영체제(OS) 및 기타 단말기의 상태를 판단하여 가상 경로 대상 시스템인지를 판별한다.
- <42> 상기 제2 과정(S200)에서, 가상 경로 대상인지가 판별되면 가상 경로를 설정하기 위해 대상 시스템에서 발생하는 MAC 주소 요청에 가상 경로 시스템이 자신의 MAC 주소로 응답한다.
- <43> 상기 가상 경로 대상이 되는 시스템의 MAC 주소를 다른 단말기가 요청하는 경우에도 가상 경로 시스템이 자신의 MAC 주소로 ARP 패킷을 발송한다.
- <44> 상기 제3 과정(S300)에서는, 상기 대상 시스템에서 발생하는 패킷의 프로토콜, 목적지 주소, 목적지 포트 등을 검사하여 통과 여부를 판단한다.
- <45> 상기 제4 과정(S400)에서는, 대상 시스템에서 발생하는 패킷의 데이터 내용을 점검하여 유해 트래픽이 포함되어 있는지를 판별한다.
- <46> 상기 제5 과정(S500)에서는, 상기 제4 과정(S400)에서 유해 트래픽이 발견된 시스템은 해당 시스템에게 거짓(Fake) MAC 주소 응답 패킷을 주기적으로 발송함으로써 유해 시스템의 통신을 완전히 차단한다.
- <47> 도 4는 상기 도 3의 제1 과정(S100)을 상세히 나타낸 제어 흐름도이다.

<48> 도시된 바와 같이, 상기 제1 과정(S100)은 단말기(이하 '노드'라 함)에서 발생하는 MAC 요청 패킷을 모니터링 하는 단계(S110)와, 상기 MAC 요청 패킷의 출발지 주소 및 MAC 주소를 추출하는 단계(S120)와, 상기 추출된 MAC 요청 패킷의 출발지 주소 및 MAC 주소를 MAC주소, IP주소, OS(운영체제), 사용자, 사용시간 및 동작방법(모드) 등을 저장 및 확인할 수 있는 노드(단말기) 테이블(TABLE)에 추가하는 단계(S130)와, 상기 추출한 노드에 대한 운영체제(OS) 추측(Guessing)하는 단계(S140)로 구성된다.

<49> 하기 표 1에는 상기 노드 테이블에 대한 일례가 구성되어 있다.

<50> <표 1>

<51> [노드 테이블]

MAC 주소	IP 주소	OS	사용자	시간	동작방법
00:13:D4:04:BD:C0	192.168.1.2	Linux			허용
00:0F:EA:6D:71:2A	192.168.1.1	Windows XP	Kimpd		가상경로
00:90:FB:09:0F:17	192.168.1.3	Windows XP		ANYTIME	격리

<53> 따라서 이를 살펴보면,

<54> 특정 장비가 가상 경로 설정의 적용 대상이 되는지의 여부를 판단하는 제1 과정(S100)은, 네트워크상에서 MAC 요청 패킷을 모니터링 하여, 상기 MAC 요청 패킷의 출발지 주소와, MAC 주소를 추출하게 된다.

<55> 또한, 상기 추출된 MAC 요청(Request) 패킷의 출발지 주소 및 MAC 주소를 노드 테이블(TABLE)에 추가하고, 상기 추출한 노드에 대한 운영체제(OS) 인식할 수 있게 된다.

<56> 도 5는 상기 도 3의 제2 과정(S200)을 상세히 나타낸 제어 흐름도이다.

<57> 도시된 바와 같이, 상기 제2 과정(S200)은, 상기 노드 테이블의 노드에 동작방법을 설정하는 단계(S210)와, 노드 테이블의 노드에 보안정책을 연결하는 단계(S220)와, 상기 동작방법에 의해 설정된 "가상 경로"노드의 모든 MAC 주소 요청에 대해 가상 경로 시스템의 MAC 주소로 응답하는 단계(S230)로 구성된다.

<58> 하기 표 2에는 상기 보안정책 테이블에 대한 일례가 구성되어 있다.

<59> <표 2>

목적지 주소	목적지 port	시간대	Action
192.168.2.1	TCP/80	ANYTIME	ALLOW
10.10.1.1	TCP/25	ANYTIME	ALLOW
10.10.1.1	UDP/53	ANYTIME	ALLOW

<61> 따라서 이를 살펴보면,

<62> 상기 제1 과정(S100)을 통해 특정장비가 가상 경로 설정대상에 적합하다 판단되면 적용 대상 장비의 가상 경로를 설정하는 제2 과정(S200)은, 상기 노드 테이블의 노드에 동작방법을 설정하고, 상기 노드 테이블의 노드에 보안정책을 연결하며, 상기 동작방법에 의해 설정된 "가상 경로"노드의 모든 MAC 주소 요청에 대해 가상 경로 시스템의 MAC 주소로 응답한다.

<63> 도 6은 상기 도 3의 제3 과정(S300)을 상세히 나타낸 제어 흐름도이다.

<64> 도시된 바와 같이, 상기 제3 과정(S300)은, 상기 가상 경로 시스템으로 유입되는 패킷에서 프로토콜, 목적지 주소 및 목적지 포트 번호 등을 추출하는 단계(S310)와, 목적지 주소, 목적지 포트, 시간대 및 실행여부 등을 저장 및 확인할 수 있는 보안정책 테이블을 참조하여 대응 여부를 결정하는 단계(S320)로 구성된다.

<65> 상기 보안정책 테이블을 참조하여 대응 여부를 결정하는 단계(S320)는, 대응 여부를 판단하는 단계(S321)와, 상기 판단단계(S321)에서 허용일 경우에는 해당 패킷을 포워딩(forwarding)하는 단계(S322)와, 상기 판단단계(S321)에서 거부일 경우에는 해당 패킷을 폐기하는 단계(S323)를 더 포함한다.

<66> 따라서 이를 살펴보면,

- <67> 설정된 가상 경로의 트래픽이 보안 정책에 적합한가를 검사하는 제3 과정(S300)은, 상기 가상 경로 시스템으로 유입되는 패킷에서 프로토콜, 목적지 주소 및 목적지 포트 번호 등을 추출한 후, 상기 보안정책 테이블을 참조하여 대응 여부를 판단한다.
- <68> 그리고 상기 판단 결과, 허용일 경우에는 해당 패킷을 포워딩(forwarding)하고, 상기 판단 결과, 거부일 경우에는 해당 패킷을 폐기하게 되는 것이다.
- <69> 도 7은 상기 도 3의 제4 과정(S400)을 상세히 나타낸 제어 흐름도이다.
- <70> 도시된 바와 같이, 상기 제4 과정(S400)은 패킷의 페이로드(payload)를 추출하는 단계(S410)와, 유해/악성 데이터베이스(DB)를 참조하는 단계(S420)와, 상기 패킷의 페이로드(payload)와 유해/악성 데이터베이스(DB)의 일치 여부를 판단하는 단계(S430)와, 상기 판단단계(S430)에서 상기 패킷의 페이로드(payload)와 유해/악성 데이터베이스(DB)가 일치하면 노드 테이블에 동작방법을 변경(차단)하는 단계(S440)와, 상기 판단단계(S430)에서 상기 패킷의 페이로드(payload)와 유해/악성 데이터베이스(DB)가 일치하지 아니하면 해당 패킷을 전송하는 단계(S450)와, 해당 행위에 대한 감사 기록 로그를 작성하는 단계(S460)로 구성된다.
- <71> 이의 동작을 살펴보면,
- <72> 가상 경로의 트래픽이 유해 트래픽인가를 검사하는 제4 과정(S400)은, 패킷의 페이로드(payload)를 추출하고, 유해/악성 데이터베이스(DB)를 참조한 후, 상기 패킷의 페이로드(payload)와 유해/악성 데이터베이스(DB)의 일치 여부를 판단한다.
- <73> 상기 판단 결과, 상기 패킷의 페이로드(payload)와 유해/악성 데이터베이스(DB)가 일치하면 노드 테이블에 동작 방법을 변경(차단)하고, 상기 판단 결과, 상기 패킷의 페이로드(payload)와 유해/악성 데이터베이스(DB)가 일치하지 아니하면 해당 패킷을 전송하는 것이다. 그리고 이의 해당 행위에 대한 감사 기록 로그를 작성한다.
- <74> 도 8은 상기 도 3의 제5 과정(S500)을 상세히 나타낸 제어 흐름도이다.
- <75> 도시된 바와 같이, 제5 과정(S500)은 노드 테이블의 동작방법(모드)을 참조하여 악성 노드를 구분하는 단계(S510)와, 상기 악성 노드로 거짓된 MAC 주소 응답 패킷을 주기적으로 전송하는 단계(S520)와, 상기 악성 노드의 모든 MAC 주소 요청에 대해 거짓된 MAC 주소로 패킷을 발송하는 단계(S530)로 구성된다.
- <76> 따라서 이의 동작을 살펴보면,
- <77> 가상 경로의 시스템을 네트워크에서 분리하는 제5 과정(S500)은, 노드 테이블의 동작방법(모드)을 참조하여 악성 노드를 구분하여, 상기 악성 노드로 거짓된 MAC 주소 응답 패킷을 주기적으로 전송한다.
- <78> 그리고 상기 악성 노드의 모든 MAC 주소 요청에 대해 거짓된 MAC 주소로 패킷을 발송하게 되는 것이다.

발명의 효과

- <79> 이상에서와 같이 본 발명은 가상의 인라인(In-line) 기술로서, 실제 물리적인 구성은 인라인(in-line) 형태가 아니지만, 통신 당사자들이 보안장비를 경유하여 통신하게끔 함으로써 물리적인 인라인(In-line) 구성에서와 같은 보안 동작을 할 수 있다.
- <80> 또한, 본 발명은 네트워크에 보안장비 설치 시, 네트워크 중단 없이 장비를 설치할 수 있게 하며, 장비 장애 시에 종래에 발생하는 네트워크 장애 확산(Single point of failure)이 발생하지 않으며, 인가된 네트워크 장비는 가상의 인라인(in-line) 구성된 장비를 통하지 않고 통신할 수 있게 함으로써 속도 지연 현상을 배제시킨 장점이 있다.
- <81> 또한, 본 발명은 보안장비를 경유해서 외부로 나가는 트래픽뿐만 아니라 동일 네트워크 내에 있는 단말기 간의 통신 및 트래픽을 제어할 수 있는 이점이 있다.
- <82> 또한, 본 발명은 다수의 내부 망에 비인가 시스템의 사용통제 및 이상 트래픽을 발생시키는 시스템을 효과적으로 차단할 수 있는 장점이 있다.

도면의 간단한 설명

- <1> 도 1은 종래의 네트워크 보안장치의 구성도,
- <2> 도 2는 본 발명이 적용되는 가상의 인라인 네트워크 보안장치의 구성도,

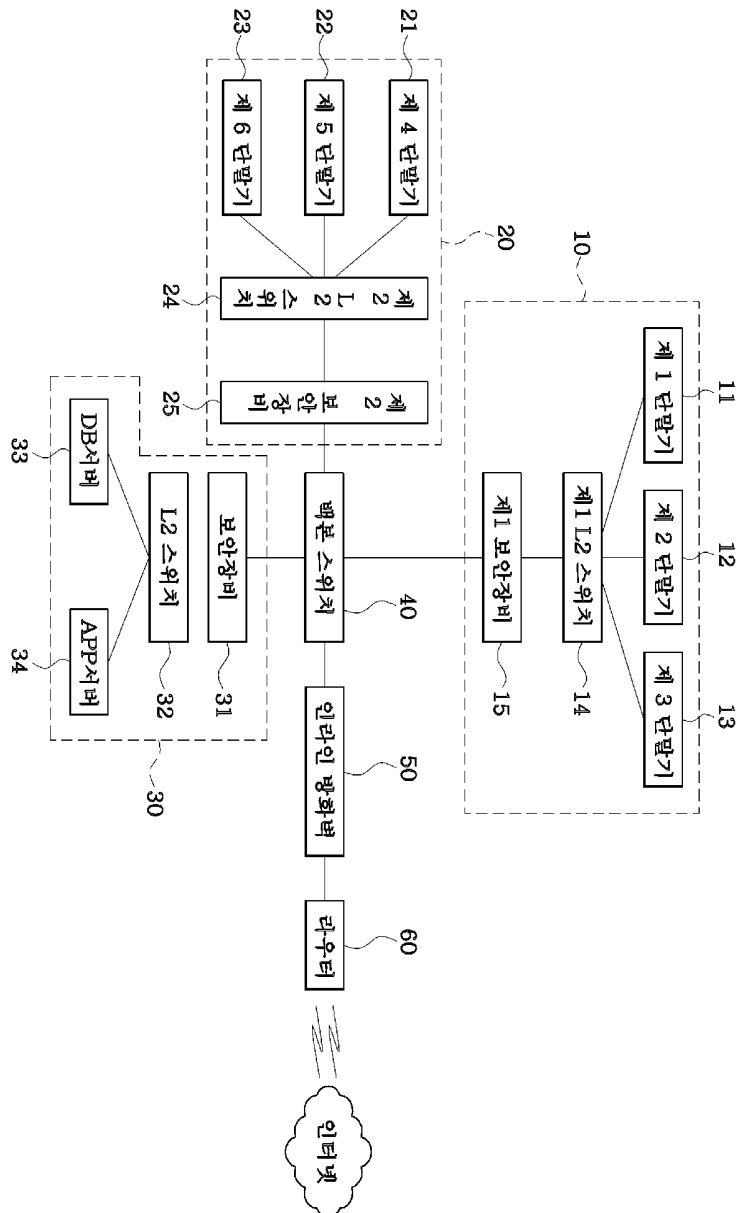
- <3> 도 3은 본 발명에 따른 가상의 인라인 네트워크 보안방법의 제어 흐름도,
 <4> 도 4는 상기 도 3의 제1과정을 상세히 나타낸 제어 흐름도,
 <5> 도 5는 상기 도 3의 제2과정을 상세히 나타낸 제어 흐름도,
 <6> 도 6은 상기 도 3의 제3과정을 상세히 나타낸 제어 흐름도,
 <7> 도 7은 상기 도 3의 제4과정을 상세히 나타낸 제어 흐름도,
 <8> 도 8은 상기 도 3의 제5과정을 상세히 나타낸 제어 흐름도이다.

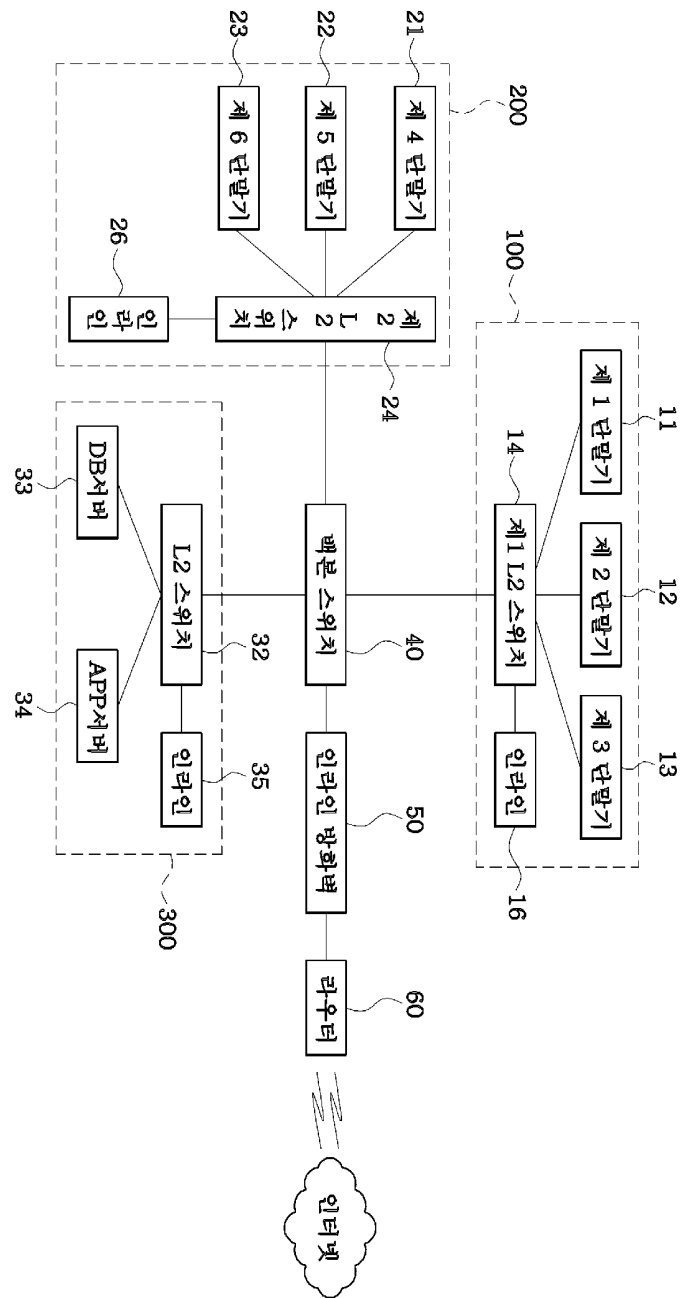
<9> < 도면의 주요부분에 대한 부호의 설명 >

- <10> 100: 제1 내부망 200: 제2 내부망
 <11> 16,26,35: 인라인 40: 백본스위치
 <12> 50: 인라인방화벽 60: 라우터

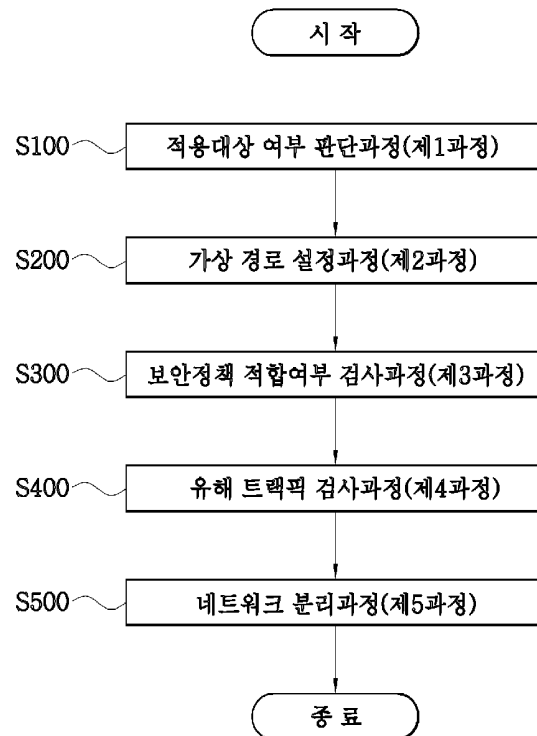
도면

도면1

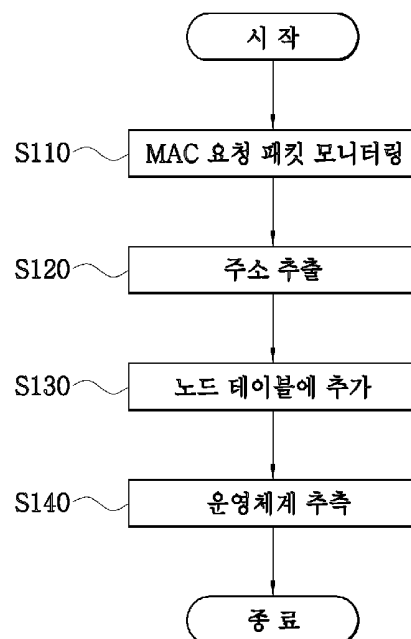




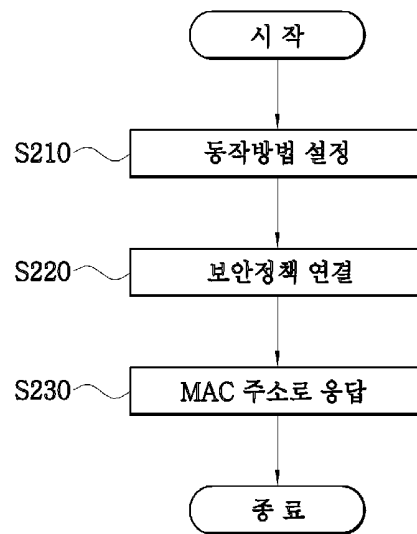
도면3



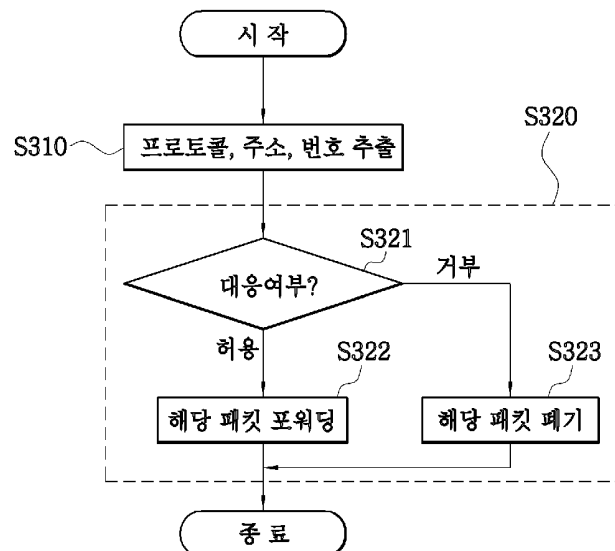
도면4



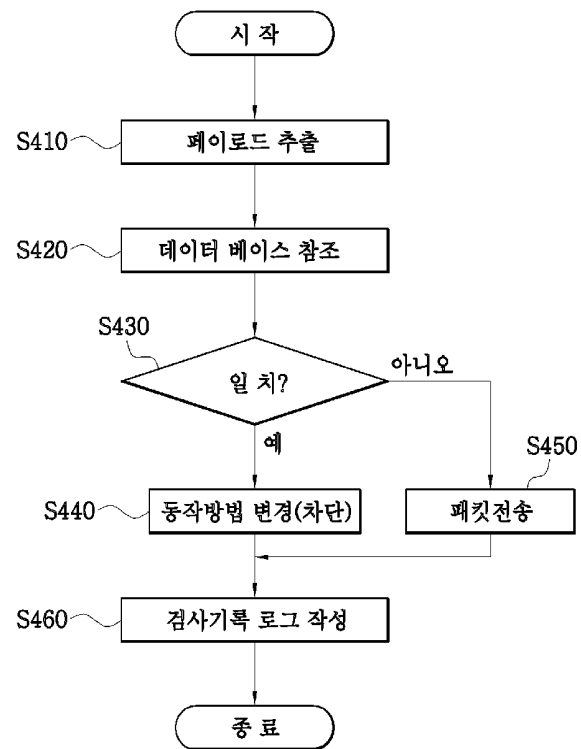
도면5



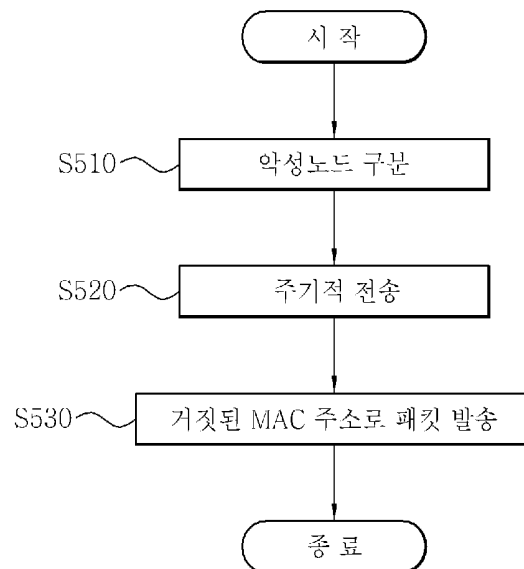
도면6



도면7



도면8





**(19) Korean Intellectual
Property Office (KR)
(12) Patent Registration
Notification (B1)**

**(45) Date of
Publication** **October 9, 2007**
**(11) Registration
Number** **10-0765340**
**(24) Registration
Date** **October 2, 2007**

(51) Int. Cl.

H04L 12/22 (2006.01) **H04L 12/26** (2006.01)
H04L 12/28 (2006.01)

(21) Application No. **10-2006-0028732**(22) Application Date **March 30, 2006**

Date of Examination **March 30, 2006**
Request

(65) Publication No. **10-2006-0035680**Publication Date **April 26, 2006**

(56) Prior Art Search Documents

KR1020030047958 A

JP2002111732 A

(73) Patentee

Genie Networks (Ltd.)

5404, Dong Seoul University Entrepreneurship Incubation
Center, 423 Bokjeong-dong, Sujeong-gu, Seongnam-si,
Gyeonggi-do

(72) Inventor

Dong-beom Lee

208-702, Bando Bora, Naeson-dong, Uiwang-si,
Gyeonggi-do

Gye-yeon Kim

203-1002, Daemyeong Gureumchae Apt., 23 Ojeon-dong,
Uiwang-si, Gyeonggi-do

(Continued on reverse page)

(74) Agent

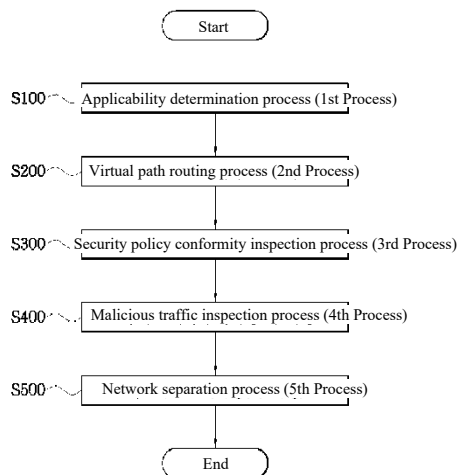
Deok-yong Choi

Total Number of Claims: 2

Examiner: Byeong-gyun Kim

(54) Virtual In-line Network Security Method**(57) Abstract**

This invention is a system that analyzes network packets to determine conformity with security policy and presence/absence of intrusion, and it pertains to a virtual in-line network security method that modulates the responses to MAC address requests of devices requiring control among the devices present in a network segment or the same VLAN into a security equipment's MAC address without installing a physical in-line structure in order to cause the communication details of the devices to go through the security equipment, where the conformity with the security policy is determined in order to perform the access control. The composition of the invention includes: A 1st process (S100) that determines whether a particular equipment is suitable for virtual path routing; a 2nd process (S200) that routes the virtual path of the applicable equipment when the specific equipment is determined to be suitable for virtual path routing through the aforesaid 1st process (S100); a 3rd process (S300) that inspects whether the traffic of the virtual path routed is in conformity with the security policy; a 4th process (S400) that inspects whether the traffic of the aforesaid virtual path is a harmful traffic; and, a 5th process (S500) that separates the system of the aforesaid virtual path from the network.

Representative Drawing - Fig. 3

(72) Inventor

Min-sang Lee

101-1806 Hyundai Hometown, Shinjang 2-dong, Hanam-si,
Gyeonggi

Yong-kwon Kim

501-502, Yangji Hanyang, Sunae-dong, Bundang-gu,
Seongnam-si, Gyeonggi

Jun-woo Park

501-1501, Hyundai Hometown 3-cha Complex 2,
Jukjeon 1-dong, Suji-gu, Yongin-si, Gyeonggi

Scope of Claims

Claim 1

In an in-line network mechanism consisting of a network mechanism achieved by inclusion of multiple internal networks encompassing multiple devices and an L2 switch (hub) connected to the aforesaid devices, an L2 switch (hub) connected to a DB (database) server and APP (application) server, a backbone switch connected to the aforesaid hubs, in-line firewall connected to the aforesaid backbone switch, a router connected to the aforesaid in-line firewall and the internet and construction of an in-line system on each one of the aforesaid internal network's hub and L2 switch (hub) connected to the DB server and APP server, a security method for virtual in-line network characterized by:

A 1st process that determines whether a particular equipment is subject to virtual path routing (S100), which consists of the step of monitoring MAC request packet generated in the aforesaid device (node) (S110), the step of extracting the origin address and MAC address of the aforesaid MAC request packet (S120), the step of adding the aforesaid origin address and MAC address of the MAC request packet to the node table (TABLE) that can store and verify MAC address, IP address, OS (operating system), user, time of use, and operation method (S130) and the step of estimating (guessing) the operating system (OS) of the aforesaid extracted node (S140);

a 2nd process that routes the virtual path of the applicable equipment (S200) when a particular equipment is considered suitable for virtual path routing through the aforesaid 1st process (S100), which consists of the step of configuring the method of operation of the node of the aforesaid node table (S210), the step of connecting security policy to the node of the node table (S220) and the step of responding with MAC address of the virtual path system to all MAC address requests from the "virtual path" node configured through the aforesaid method of operation (S230);

a 3rd process that inspects whether the traffic of the aforesaid virtual path routed is in conformity with the security policy (S300), which consists of the step of extracting the protocol, destination address, destination port number, etc. from packets entering into the aforesaid virtual path system (S310) and the step of determining whether to respond by referring to the security policy table that can store and verify the destination address, destination port, time zone, and execution (S320);

a 4th process that inspects whether the traffic of the aforesaid virtual path is a harmful traffic (S400), which consists of the step of extracting a packet's payload (S410), the step of referring to a harmful/malicious database (DB) (S420), the step of determining whether the aforesaid packet's payload matches the harmful/malicious database (DB) (S430), the step of modifying (blocking) the method of operation on the aforesaid node table (S440) if the aforesaid packet's payload matches the harmful/malicious database (DB) in the aforesaid determination step (S430), the step of transmitting the packet (S450) if the aforesaid packet's payload does not match the harmful/malicious database (DB) in the aforesaid determination step (S430) and the step of producing an inspection record log of the action (S460); and,

a 5th process that separates the aforesaid virtual path's system from the network (S500), which consists of the step of classifying malicious node by referring to the method of operation (mode) of the aforesaid node table (S510), the step of periodically transmitting false MAC address response packets to the aforesaid malicious node (S520) and the step of sending packets to false MAC addresses in response to all MAC address requests from the aforesaid malicious node (S530).

Claim 2

Deleted

Claim 3

Deleted

Claim 4

Deleted

Claim 5

A security method for virtual in-line network described in Claim 1 that is characterized by:

The step of determining whether to respond (S320) by referring to the security policy table of the aforesaid 3rd process (S300) consisting of the step of determining whether or not to respond (S321), the step of forwarding the corresponding packet (S322) if permitted in the aforesaid determination step (S321) and the step of discarding the corresponding packet (S323) if rejected in the aforesaid determination step (S321).

Claim 6

Deleted

Claim 7

Deleted

Specification**Detailed Description of the Invention*****Purpose of the Invention******Technical Field of the Invention and Prior Art***

- <13> The invention pertains to a system for analyzing network packets to determine the conformity with security policy and presence/absence of intrusion as in network intrusion blocking systems (firewall) and intrusion prevention systems, and more particularly a security method for virtual in-line network that modulates responses to MAC address requests from devices requiring control among the devices present in a network segment or the same VLAN into a security equipment's MAC address without installing a physical in-line structure in order to cause the communication details of the devices to go through the security equipment, where the conformity with the security policy is determined to perform access control.
- <14> Network security equipment such as firewalls or intrusion prevention systems like the ones noted can be divided into a router mode or a bridge mode according to the installation configuration.
- <15> In the aforesaid router mode, the IP address bandwidth of the network interface card where packets are inputted and the IP address bandwidth of the network interface card where packets are outputted are installed differently from each other.
- <16> Installing equipment on a network that is already using this method requires changing the existing network IP address format.
- <17> Unlike the aforesaid router mode, the aforesaid bridge mode uses a network address bandwidth of the same IP bandwidth for the input network interface card and the output network interface card, and therefore, there is no need to change the network IP upon installation unlike the router mode, and the only processes needed are physically switching network lines and inserting the equipment.
- <18> On the other hand, typical network security equipment is manifested in an in-line configuration where existing network lines are severed and security equipment is installed midway regardless of the router mode or bridge mode.
- <19> Because such conventional installation of network security equipment is configured in the in-line format in both router mode and bridge mode, the physical in-line structure could not avoid interruption in network use upon installation work, post-installation delay in the speed after normal communication flow is established, and network communication failure in the event of the installed equipment's failure.
- <20> In the end, such in-line configuration had the advantage of heightening security as all packets passing through the network became visible, yet the aforesaid in-line configuration caused the problem of delay in speed and the loss of communication in the event of a failure for all devices.
- <21> Such conventional system is explained by referring to Fig. 1.
- <22> As shown, in order to restrict communication from Device 1 (11) of Internal Network 1 (10) to Device 4 (21) of Internal Network 2 (20), a conventional network security mechanism will control the communication traffic through in-line installation of Security Equipment 1 (15) in the segment between L2 Switch 1 (14) and Backbone Switch (40).
- <23> Because Security Equipment 1 (15) installed on the aforesaid L2 Switch 1 (14) and Backbone Switch (40) segment requires all traffic from Internal Network 1 (10) to other networks to pass through the security equipment, the pass/block decision is made based on the conformity with the policy by referring to the header information (origin address, destination address, destination port, etc.) of TCP/IP packets transmitted between communication counterparts.

<24> Such configuration of typical in-line network security equipment causes the adverse effect of network speed delays during communication and network disconnection in the event of a security equipment failure.

<25> In addition, communicating between Device 1 (11) and Device 2 (12) in Internal Network 1 (10) retains the limitation of the inability to control the connection because the packets transmitted between the two devices do not pass through Security Equipment 1 (15).

Technical Objectives that the Inventions Intends to Achieve

<26> The invention is designed to solve the above-described problems, and the invention's objective is to provide a virtual in-line network security method that can provide the same security operation as a physical in-line configuration by causing communication parties to communicate through security equipment despite the fact that the actual physical configuration is not in the in-line format.

<27> Also, another objective of the invention is to provide a virtual in-line network security method that allows installation of equipment without network interruption upon installing security equipment on the network, does not cause spread of network failure (single point of failure) which conventionally occurs upon equipment failure, and prevents delay in speed by allowing authorized network equipment to communicate without going through the virtual in-line equipment.

<28> Further, another objective of the invention is to provide a virtual in-line network security method that controls communication and traffic between devices on the same network as well as traffic heading to external destinations through the security equipment.

<29> In addition, another objective of the invention is to provide a virtual in-line network security method suitable for controlling use by unauthorized systems on multiple internal networks and for use in effectively blocking systems that causes abnormal traffic.

Composition and Effects of the Invention

<30> In an in-line network mechanism consisting of a network mechanism achieved by inclusion of multiple internal networks encompassing multiple devices and an L2 switch (hub) connected to the aforesaid devices, an L2 switch (hub) connected to a DB (database) server and APP (application) server, a backbone switch connected to the aforesaid hubs, in-line firewall connected to the aforesaid backbone switch, a router connected to the aforesaid in-line firewall and the internet and construction of an in-line system on each one of the aforesaid internal network's hub and L2 switch (hub) connected to the DB server and APP server, the invention designed to achieve aforesaid objectives is characterized by a virtual in-line network security method comprising of: A 1st process that determines whether a particular equipment is subject to virtual path routing (S100), which consists of the step of monitoring MAC request packet generated in the aforesaid device (node) (S110), the step of extracting the origin address and MAC address of the aforesaid MAC request packet (S120), the step of adding the aforesaid origin address and MAC address of the aforesaid extracted MAC request packet to the node table (TABLE) that can store and check MAC address, IP address, OS (operating system), user, time of use, and operation method (S130) and the step of estimating (guessing) the operating system (OS) of the aforesaid extracted node (S140); a 2nd process that routes the virtual path of applicable equipment (S200) when a particular equipment is considered suitable for virtual path routing through the aforesaid 1st process (S100), which consists of the step of configuring the method of operation of the node of the aforesaid node table (S210), a step of linking security policy to the node of the node table (S220) and the step of responding with MAC address of the virtual path system to all MAC address requests from the "virtual path" node configured through the aforesaid method of operation (S230); a 3rd process that inspects whether the traffic of the aforesaid virtual path routed is in conformity with the security policy (S300), which consists of the step of extracting the protocol, destination address, destination port number, etc. from packets entering into the aforesaid virtual path system (S310) and the step of determining whether to respond by referring to the security policy table that can store and verify the destination address, destination port, time zone, and execution (S320); a 4th process that inspects whether the traffic of the aforesaid virtual path is a harmful traffic (S400), which consists of the step of extracting a packet's payload (S410), the step of referring to a harmful/malicious database (DB) (S420), the step of determining whether the aforesaid packet's payload matches the harmful/malicious database (DB) (S430), the step of modifying (blocking) the method of operation on the aforesaid node table (S440) if the aforesaid packet's payload matches the harmful/malicious database (DB) in the aforesaid determination step (S430), the step of transmitting the packet (S450) if the aforesaid packet's payload does not match the harmful/malicious database (DB) in the aforesaid determination step (S430) and the step of producing an inspection record log of the action (S460); and, a 5th process that separates the aforesaid virtual path's system from the network (S500), which consists of the step of classifying malicious node by referring to the method of operation (mode) of the aforesaid node table (S510), the step of periodically transmitting false MAC address response packets to the aforesaid malicious node (S520) and the step of sending packets to

false MAC addresses in response to all MAC address requests from the aforesaid malicious node (S530).

- <31> Below, desirable embodiment of the invention is explained in greater details by referring to the accompanying drawings:
- <32> Fig. 2 is a schematic diagram of a virtual in-line network security mechanism to which the present invention is applied.
- <33> As shown, the virtual in-line network security mechanism to which the present invention is applied operates after connecting the equipment to the network in the form of a general device, unlike the conventional configuration.
- <34> In other words, in a network mechanism comprising multiple internal networks encompassing multiple devices and an L2 switch (hub) connected to the aforesaid devices, an L2 Switch (hub) (32) connected to a DB (database) Server (33) and APP (Application) Server (34), a Backbone Switch (40) connected to the aforesaid hubs, In-line Firewall (50) connected to the aforesaid Backbone Switch (40), a Router (60) connected to the aforesaid In-line Firewall (50) and the internet, it is achieved by constructing of an in-line system (16, 26, 35) on each one of the aforesaid internal network's hub and L2 Switch (hub) (32) connected to the DB Server (33) and APP Server (34).
- <35> To control the network of Device 1 (11) of Internal Network 1 (100) in the invention applied to the virtual in-line network supplementation mechanism composed in this manner, Device 1 (11) requests the packet to be addressed to the hardware address (MAC address) of the communication counterpart or the forwarder (gateway), and the virtual inline system (16, 26, 35) detects such address request and responds to Device 1 (11) with its MAC address.
- <36> With the packet generated in Device 1 (1) arriving at the virtual in-line system after the aforesaid response, access control is performed by analyzing the packet's information and data.
- <37> In addition, in order to prevent devices on the same network such as Device 2 or Device 3 from forwarding the packet directly to Device 1 (11), the virtual in-line system responds with its MAC address to all MAC address requests from a specific device (12 or 13) among all devices on the network that intends to forward packets directly to Device 1 (11), which causes all packets inputted/outputted for communication with Device 1 (11) subject to control to go through the security sensor.
- <38> Fig. 3 is a control flowchart of the virtual in-line network security method of the invention.
- <39> As shown, the virtual in-line network security method embodying the invention includes the 1st process (S100) that determines whether a particular equipment is subject to virtual path routing, the 2nd process (S200) that configures a virtual path of the equipment if the equipment is determined to be suitable for virtual path routing through the 1st process (S100), the 3rd process (S300) that inspects whether the traffic of the aforesaid virtual path routed is in conformity with the security policy, the 4th process (S400) that inspects whether the traffic in the aforesaid virtual path is a harmful traffic, and the 5th process (S500) that separates the virtual path's system from the network.
- <40> In the 1st process (S100) described above, the aforesaid security equipment analyzes the MAC address request packet generated in the device equipment and extracts the origin address and MAC (Media Access Control) address.
- <41> Whether it is a system subject to a virtual path is determined based on the aforesaid origin address, MAC address, client's operating system (OS), and other device conditions.
- <42> In the 2nd process (S200) described above, once it is determined to be subject to a virtual path, the virtual path system responds with its MAC address to the MAC address request generated in the target system to route a virtual path.
- <43> Even if another device requests the MAC address of the system subject to the aforesaid virtual path, the virtual path system sends ARP packet to its MAC address.
- <44> In the 3rd process (S300) described above, whether to pass is determined by inspecting the protocol, destination address, destination port, etc. of the packet generated in the aforesaid target system.
- <45> In the 4th process (S400) described above, the data content of the packet generated in the target system is inspected to determine whether any harmful traffic is contained.
- <46> In the 5th process (S500) described above, false (fake) MAC address response packets are transmitted periodically to a system found to have harmful traffic in the aforesaid 4th process (S400), thereby blocking the communication of the harmful system entirely.
- <47> Fig. 4 is a control flowchart depicting the details of the 1st process (S100) of the aforesaid Fig. 3.

As shown, the aforesaid 1st process (S100) consists of the step of monitoring MAC request packet generated in a device (hereinafter referred to as “node”) (S110), the step of extracting the origin address and MAC address of the MAC request packet (S120), the step of adding the origin address and MAC address of the extracted MAC request packet to the node (device) table that can store and verify MAC address, IP address, OS (operating system), user, usage time and the method of operation (mode), etc. (S130), and the step of estimating (Guessing) the operating system (OS) of the extracted node (S140).

Table 1 below shows an example of the aforesaid node table.

<Table 1>

[Node Table]

MAC address	IP address	OS	User	Time	Operation method
00:13:D4:04:BD:C0	192.168.1.2	Linux			Allow
00:0F:EA:6D:71:2A	192.168.1.1	Windows XP	Kimpd		Virtual path
00:90:FB:09:0F:17	192.168.1.3	Windows XP		ANYTIME	Separation

Therefore, according to the above,

the 1st process (S100), which determines whether a particular device is subject to a virtual path routing, monitors MAC request packets on the network and extracts the origin address and MAC address of the MAC request packets.

In addition, the origin address and MAC address of the extracted MAC request packet are added to the node table (TABLE) and it becomes possible to recognize the operating system (OS) of the aforesaid extracted node.

Fig. 5 is a control flowchart depicting the details of the 2nd process (S200) of the aforesaid Fig. 3.

As shown, the 2nd process (S200) consists of the step of configuring the method of operation on the node of the aforesaid node table (S210), the step of linking the security policy to the node of the node table (S220), and the step of responding with the virtual path system’s MAC address to all MAC address requests of the “virtual path” node configured by the aforesaid method of operation (S230).

Table 2 below shows an example of the aforesaid supplementary policy table.

<Table 2>

Destination address	Destination port	Time zone	Action
192.168.2.1	TCP/80	ANYTIME	ALLOW
10.10.1.1	TCP/25	ANYTIME	ALLOW
10.10.1.1	UDP/53	ANYTIME	ALLOW

Therefore, according to the above,

if through the aforesaid 1st process (S100), a particular equipment is determined to be suitable for virtual path routing, the 2nd process (S200), which is routing the virtual path of the applicable equipment, configures the method of operation in the node of the aforesaid node table, links the security policy to the node of the aforesaid node table, and responds with the MAC address of the virtual path system to all MAC address requests of the “virtual path” node configured by the aforesaid method of operation.

Fig. 6 is a control flowchart depicting the details of the 3rd process (S300) of the aforesaid Fig. 3.

As shown, the aforesaid 3rd process (S300) consists of the step of extracting the protocol, destination address, destination port number, etc. from the packets entering the virtual path system (S310) and the step of deciding whether to respond by referring to the security policy table (S320) that can store and verify the destination address, destination port, time zone, execution, etc.

The step of determining whether to respond (S320) by referring to the security policy table further includes the step of determining whether to respond (S321), the step of forwarding the corresponding packet (S322) in case of permission in the aforesaid determination step (S321) and the step of discarding the corresponding packet (S323) in case of rejection in the aforesaid determination step (S321).

Therefore, according to the above,

the 3rd process (S300), which inspects whether the traffic of the virtual path routed is in conformity with the security policy, extracts the protocol, destination address, destination port number, etc. from the packet entering the virtual path system, and determines whether to respond by referring to the aforesaid security policy table.

And if the above determination results in permission, the corresponding packet is forwarded, whereas the packet is discarded in case of rejection.

Fig. 7 is a control flowchart depicting the details of the 4th process (S400) of the aforesaid Fig. 3.

As shown, the aforesaid 4th process (S400) consists of the step of extracting a payload of a packet (S410), the step of referring to the harmful/malicious database (DB) (S420), the step of determining whether the packet's payload matches the harmful/malicious database (DB) (S430), the step of modifying (blocking) the method of operation in the node table (S440) if the payload (payload) of the aforesaid packet matches the harmful/malicious data base (DB) in the aforesaid determination step (S430), the step of transmitting the corresponding packet (S450) if the payload of the aforesaid packet does not match the harmful/malicious database (DB) in the aforesaid determination step (S430), and the step of producing the audit record log for the action (S460).

To examine the operation,

the 4th process (S400), which inspects whether the traffic in the virtual path is harmful traffic extracts the packet's payload, refers to the harmful/malicious database (DB) and determines whether the packet's payload matches the harmful/malicious database (DB).

If the aforesaid determination results in a match between the aforesaid packet's payload and the harmful/malicious database (DB), the method of operation is changed (blocked) in the node table. If the payload of the aforesaid packet does not match the harmful/malicious database (DB), the corresponding packet is transmitted. Next, an inspection record log of the action is produced.

Fig. 8 is a control flowchart depicting the details of the 5th process (S500) of the aforesaid Fig. 3.

As shown, the 5th process (S500) consists of the step of classifying malicious nodes (S510) by referring to the operation method (mode) of the node table, the step of periodically transmitting false MAC address response packets to the aforesaid malicious node (S520) and the step of sending packets of false MAC addresses in response to all MAC address requests of the malicious node (S530).

To examine the operation,

the 5th process (S500), which separates the virtual path system from a network, refers to the method of operation (mode) of the node table to classify malicious nodes and periodically transmits false MAC address response packets to the malicious node.

And it sends packets of false MAC addresses in responds to all MAC address requests of the aforesaid malicious node.

Effects of the Invention

As described above, the invention is a virtual in-line technology, and its physical configuration is not an actual in-line; yet, by causing communication parties to communicate through the security equipment, it can perform the same security operation as in a physical in-line configuration.

Also, the invention has the advantage of enabling installation of the security equipment on network without any network interruption, preventing the spread of network failure (single point of failure) conventionally seen in equipment failures and preventing delay in speed by allowing authorized network equipment to communicate without going through the virtual in-line equipment.

In addition, the invention has the advantage of being able to control the traffic and communication between the devices on the same network as well as the outward traffic going through the security equipment.

Further, the invention has the advantage of controlling use by unauthorized systems in multiple internal networks and effectively blocking the systems that generate abnormal traffic.

Brief Description of Drawings

Fig. 1 is a schematic drawing of a conventional network security mechanism.

Fig. 2 is a schematic drawing of a virtual in-line network security mechanism to which the present invention is applied.

- <3> Fig. 3 is a control flowchart of the virtual in-line network security method of the invention.
- <4> Fig. 4 is a control flowchart depicting the details of the 1st Process of the aforesaid Fig. 3.
- <5> Fig. 5 is a control flowchart depicting the details of the 2nd Process of the aforesaid Fig. 3.
- <6> Fig. 6 is a control flowchart depicting the details of the 3rd Process of the aforesaid Fig. 3.
- <7> Fig. 7 is a control flowchart depicting the details of the 4th Process of the aforesaid Fig. 3.
- <8> Fig. 8 is a control flowchart depicting the details of the 5th Process of the aforesaid Fig. 3.
- <9> <Description of the Symbols Indicating Primary Elements of the Drawings>
- <10> 100: Internal Network 1 200: Internal Network 2
- <11> 16, 26, 35: In-line 40: Backbone Switch
- <12> 50: In-line Firewall 60: Router

Drawings

Fig. 1

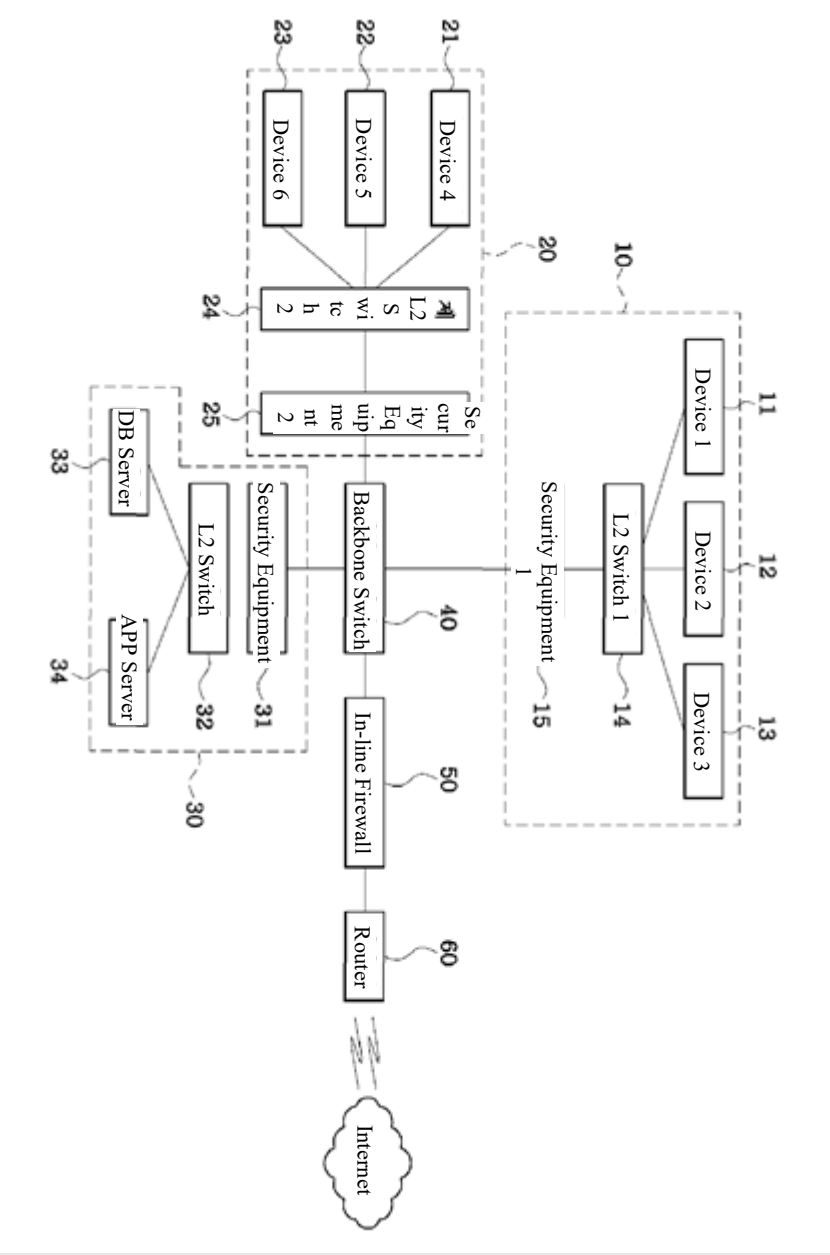


Fig. 2

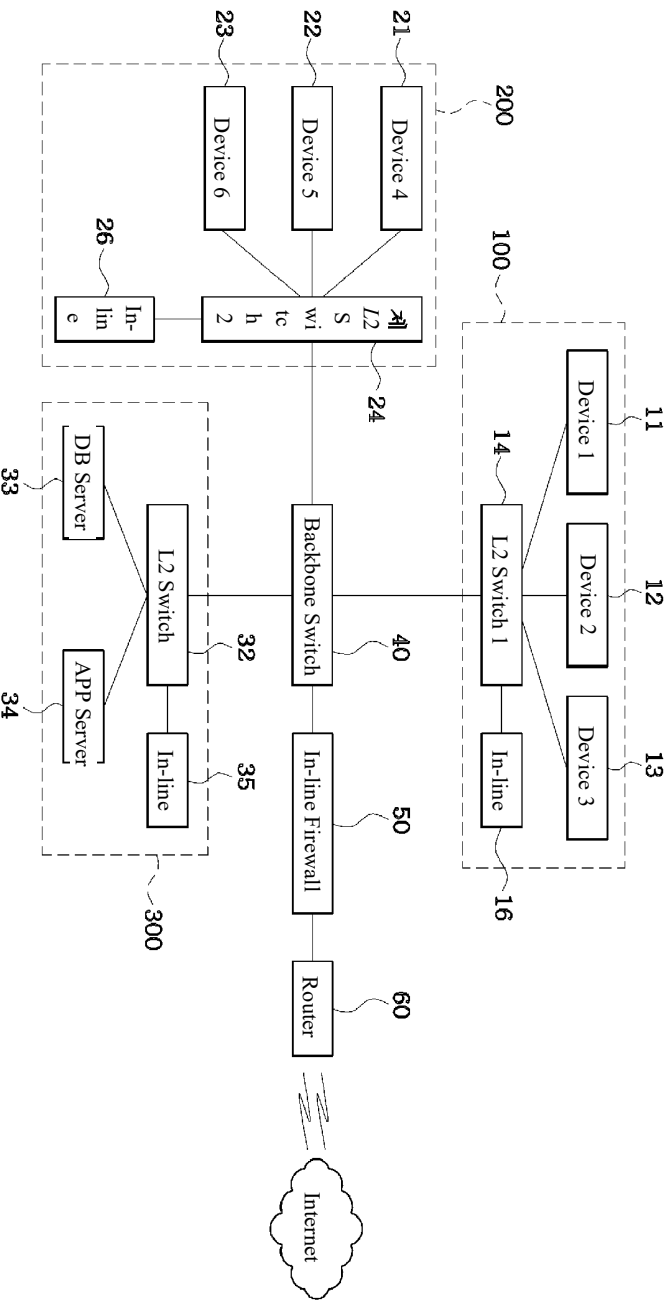


Fig. 3

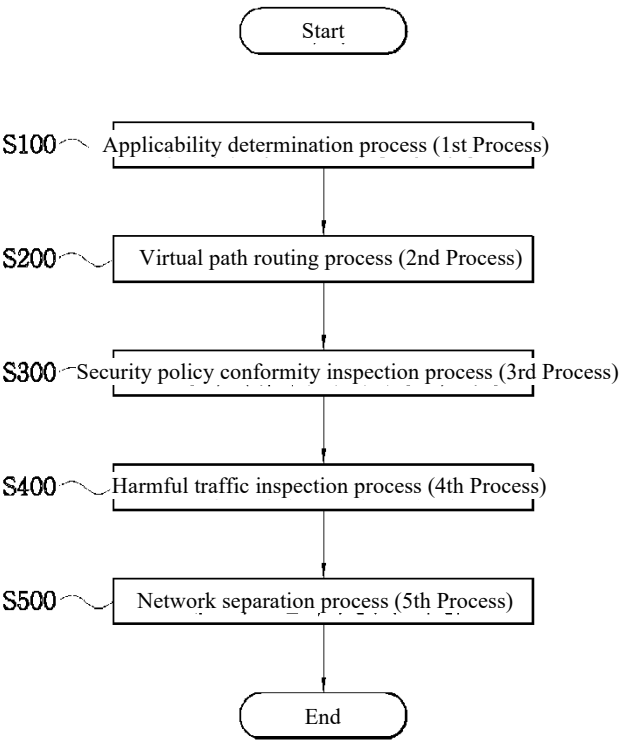


Fig. 4

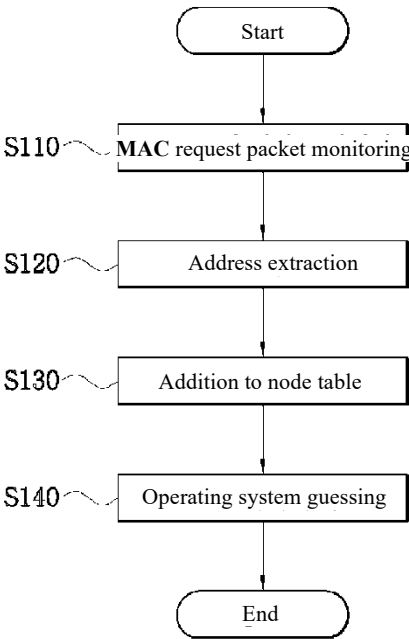


Fig. 5

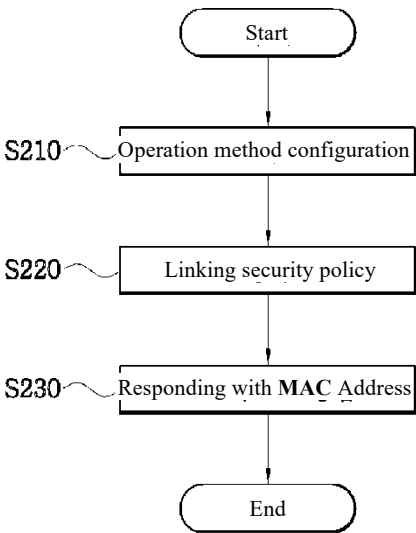


Fig. 6

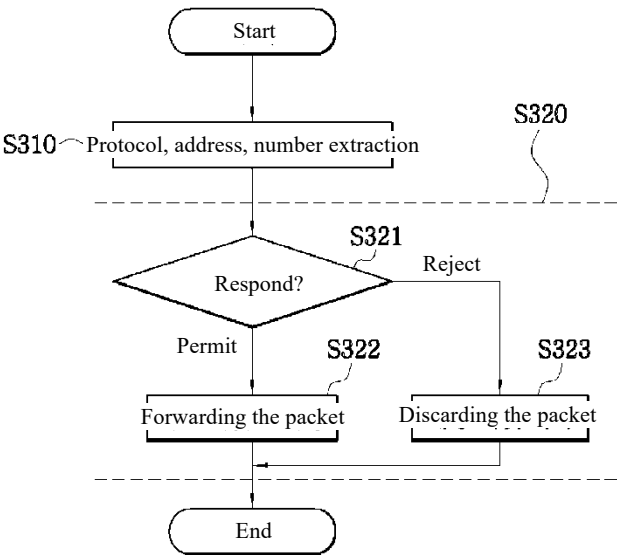


Fig. 7

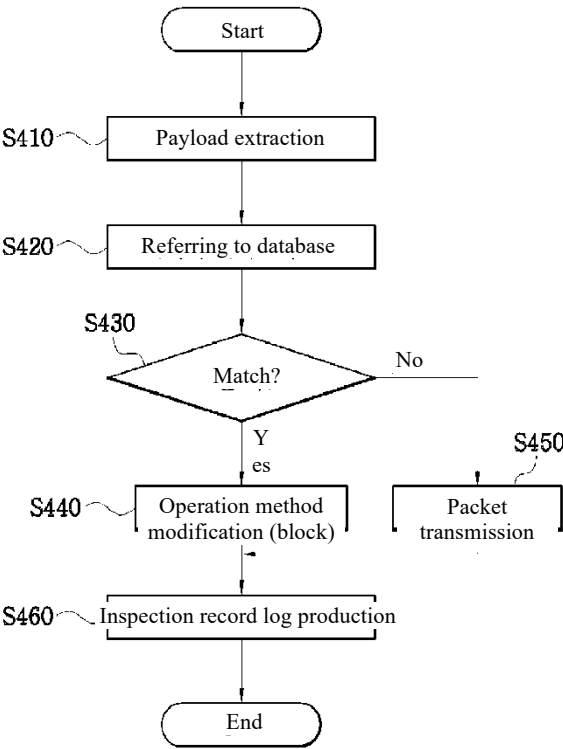
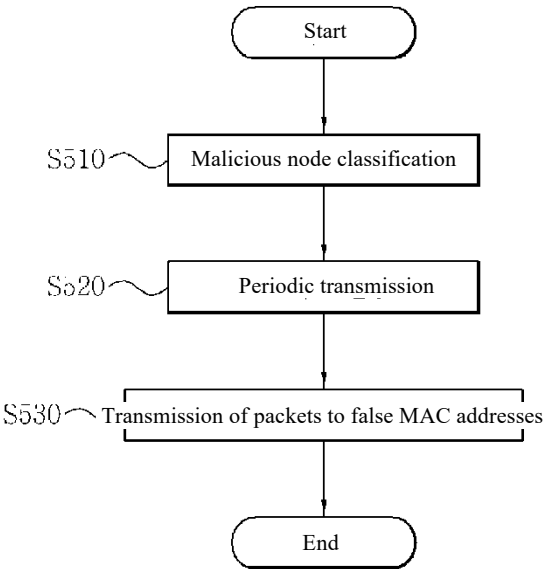


Fig. 8





STATE OF NEW YORK
CITY OF NEW YORK
COUNTY OF NEW YORK

CERTIFICATION

I, Jacqueline Yorke, as an employee of TransPerfect Translations, Inc., do hereby certify, to the best of my knowledge and belief, that the provided Korean into English translation(s) of the source document(s) listed below are true and accurate under penalty of perjury:

- EX1005 - KR_100765340_B1

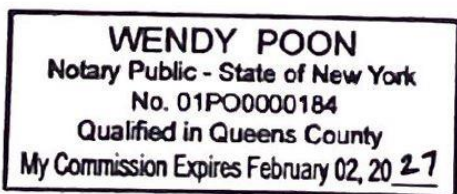
TransPerfect Translations, Inc., a translation organization with over 90 offices on six continents, is a leader in professional translations. TransPerfect Translations, Inc. has over twenty years experience translating into the above language pair, its work being accepted by business organizations, governmental authorities and courts throughout the United States and internationally.

TransPerfect Translations, Inc. affirms that the provided translation was produced in according to our ISO 9001:2015 and ISO 17100:2015 certified quality management system, and also that the agents responsible for said translation(s) are qualified to translate and review documents for the above language pair, and are not a relation to any of the parties named in the source document(s).

Jacqueline Yorke, Project Manager

Sworn to before me this
Monday, July 07, 2025

Signature, Notary Public



Stamp, Notary Public

LANGUAGE AND TECHNOLOGY SOLUTIONS FOR GLOBAL BUSINESS

1250 BROADWAY, 32ND FLOOR, NEW YORK, NY 10001 | T 212.689.5555 | F 212.689.1059 | WWW.TRANSPERFECT.COM
OFFICES IN 90 CITIES WORLDWIDE