(19)대한민국특허청(KR)
(12) 등록특허공보(B1)

(51) 。Int. Cl.
G06F 15/16 (2006.01)

(45) 공고일자 2006년07월24일
(11) 등록번호 10-0604604
(24) 등록일자 2006년07월18일

(21) 출원번호 10-2004-0045984
(22) 출원일자 2004년06월21일

(65) 공개번호 10-2005-0120875
(43) 공개일자 2005년12월26일

(73) 특허권자 엘지엔시스(주)
서울특별시 마포구 공덕2동 275번지 LG마포빌딩

(72) 발명자 유연식
경기도 수원시 팔달구 영통동 살구골 동아 아파트 717동 501호

이해진
서울특별시 서초구 방배동 782-24번지 302호

(74) 대리인 김삼수

(56) 선행기술조사문헌
KR1020000010253 A
KR1020010044268 A
KR1020020041004 A
* 심사관에 의하여 인용된 문헌

심사관 : 하승규

(54) 서버 보안 솔루션과 네트워크 보안 솔루션을 이용한시스템 보안 방법 및 이를 구현하는 보안시스템

요약

서버 보안 솔루션과 네트워크 보안 솔루션을 이용한 시스템 보안 방법 및 이를 구현하는 보안시스템이 제공된다. 해당 네트워크에 대한 유해한 접근을 차단하는 방화벽과 네트워크에 대한 침입을 차단하는 네트워크 침입방지시스템과 메일서버, FTP 서버 등을 포함하는 서버시스템으로 이루어지는 시스템의 보안 방법에 있어서, 상기 서버시스템에서 유해 트래픽을 탐지하면 유해 트래픽을 전송한 침입시스템에 대한 정보를 네트워크 침입방지시스템에 전송한다. 상기 네트워크 침입방지시스템은 상기 서버시스템으로부터 전송받은 정보를 기반으로 하여 유해 트래픽의 접근을 차단한다. 본 발명에 의하면 서버시스템에서 악의적인 침입 시도를 탐지하여 네트워크 단계에서 침입을 차단함으로써, 제2, 제3의 악의적인 침입시도를 원천적으로 차단할 수 있으며, 반복적인 침입 시도에 따른 네트워크 자원의 소모를 사전에 방지하는 효과가 있다.

대표도

도 2

색인어

서버시스템, 네트워크, 침입방지시스템, 보안, 보안시스템, 보안정책.

명세서

도면의 간단한 설명

도 1은 종래 서버 네트워크 보안시스템의 구성을 보여주는 도면이다.

도 2는 본 발명의 일실시예에 따른 서버 네트워크 보안시스템의 구성을 보여주는 도면이다.

도 3은 본 발명의 일실시예에 따른 서버 보안 솔루션과 네트워크 보안 솔루션을 이용한 시스템 보안 방법을 보여주는 흐름도이다.

100: 접근시스템 120: 인터넷

140: 라우터 300: 방화벽

400: 네트워크 침입탐지시스템 200: 메일 서버

201: FTP 서버 500: 네트워크 침입방지시스템

700: 네트워크 침입방지운영시스템

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 서버 보안 솔루션과 네트워크 보안 솔루션을 이용한 시스템 보안 방법 및 이를 구현하는 보안 시스템에 관한 것으로서, 더욱 상세하게는 서버 보안 솔루션과 네트워크 보안 솔루션을 연동하여서 서버 보안 솔루션에서 탐지한 정보를 기반으로 네트워크 보안 솔루션을 이용하여 유해 시스템으로부터의 접근을 차단하는 방법과 이를 구현하는 보안시스템에 관한 것이다.

최근들어, 컴퓨터와 결합한 정보통신기술의 비약적인 발전에 힘입어 정보화가 가속화도미에 따라 네트워크 환경과 인터넷이 보편화되고, 이러한 네트워크 환경을 통해 정보화가 진전되면서 메인 서버에 다수의 클라이언트 단말이 온라인으로 접속하여 필요한 정보의 교환이나 검색 등을 할 수 있게 되었다.

그러나, 해당 네트워크를 통한 온라인 접속이 가능하다는 점을 악용하여 서버시스템에 침입하고 유해 트래픽을 전송하는 등의 악의적인 네트워크 접근이 빈번하게 일어나고 있다.

종래 이러한 악의적인 시스템 접근을 차단하기 위한 보안 솔루션이 제공되어 왔다. 종래 보안 시스템에 대해서 크게 두가지 기술로 나누어 설명한다. 도 1은 종래 서버 네트워크 보안시스템의 구성을 보여주는 도면이다.

첫번째 기술은 종래 보안시스템은 접근시스템(100)의 IP 주소나 메일 서버(200), FTP 서버(201) 등의 서버시스템에 대한 서비스 포트 번호의 정보를 기반으로 유해 트래픽의 접근을 차단하는 방화벽(300)과, 미러링 또는 탭핑 등의 적절한 방법을 통해 만들어진 패킷의 복사본을 이용하여 네트워크 기반의 침입을 탐지하여 관리자에게 경보 등을 하는 네트워크 침입탐지시스템(400)의 연동을 통하여 컨텐츠 기반의 유해 공격, 서비스 거부(DoS)를 유발시키는 공격 등을 차단하는 구성을 택하였다. 연동의 방식은 방화벽이 제공하는 응용 프로그램 프로토콜 인터페이스(Application Protocol Interface: API)를 통해 네트워크 침입탐지시스템(400)이 직접 차단하고자 하는 접근시스템(100)의 IP 주소나 서버시스템(200, 201)의 서비스 포트 번호 등을 전달하는 것이다.

네트워크 침입탐지시스템(400)에서 공격을 탐지하게 되면 직접 차단하고자 하는 접근시스템(100)의 IP 주소나 서버시스템(200, 201)의 서비스 포트 번호 등을 방화벽(300)에 전달한다. 이렇게 수신한 정보를 이용하여 방화벽(300)은 접근시스템(100)의 IP주소로부터 접근하는 것을 막거나 서버시스템(200, 201)의 서비스 포트 번호를 받아 서버시스템(200, 201)의 특정 서비스 포트로의 접근을 막는다.

두번째 기술은 서버 시스템(200, 201)에 서버보안솔루션을 직접 운영하여 해당 서버에 대한 유해한 접근 시도에 대하여 탐지 또는 거부를 하도록 함으로써 서버의 자원을 사용하지 못하게 하는 방법이다.

첫번째 기술은 서버의 불법 사용을 위한 악의적인 시도(예를 들어, 불법 로그인의 반복적인 시도, 서버 내 접근 제한된 리소스에 대한 접근 시도 등)나 암호화된 침입 시도 등에 대해서는 탐지할 수 없는 한계를 갖고 있고, 이로 인해서 유해한 시도로부터 네트워크 및 서버 자원을 완벽하게 지키지 못하는 문제점을 갖고 있다.

두번째 기술은 방화벽(300)과 네트워크 침입탐지시스템(400)의 연동을 통한 기술 구성이 해결하지 못한 서버에 대해 악의적인 접근 시도에 대한 거부를 통하여 서버 시스템(200, 201)을 보호하고 있으나, 해당 서버에 대한 악의적인 시도가 반복됨에 따라 네트워크 자원에 대한 유해 트래픽이 지속적으로 발생하여, 정상적인 네트워크 통신 작업의 지체를 초래할 수 있는 문제점이 있다. 또한, 다른 서버에 대한 악의적인 제2, 제3의 시도가 반복되면서 서버의 서비스 제공에도 영향을 초래하게 되는 문제점이 있다.

발명이 이루고자 하는 기술적 과제

본 발명은 이러한 점을 감안하여 이루어진 것으로서, 서버 보안 솔루션에서 탐지한 정보를 기반으로 해당 유해 시스템으로부터의 접근을 네트워크 보안 솔루션으로 차단하는 시스템 보안 방법 및 이를 구현하는 보안시스템을 제공하는데 그 목적이 있다.

발명의 구성 및 작용

이러한 목적을 달성하기 위한 본 발명에서, 서버 보안 솔루션과 네트워크 보안 솔루션을 이용한 시스템 보안 방법은 해당 네트워크에 대한 유해한 접근을 차단하는 방화벽과 네트워크에 대한 침입을 차단하는 네트워크 침입방지시스템과 메일서버, FTP 서버 등을 포함하는 서버시스템으로 이루어지는 시스템의 보안 방법에 있어서, 상기 서버시스템에서 유해 트래픽을 탐지하면 유해 트래픽을 전송한 침입시스템에 대한 정보를 네트워크 침입방지시스템에 전송하는 제1단계와, 상기 네트워크 침입방지시스템은 상기 서버시스템으로부터 전송받은 정보를 기반으로 하여 유해 트래픽의 접근을 차단하는 제2단계를 구비한다.

상기 제1단계에서 상기 서버시스템은 상기 침입시스템에 대한 정보와 함께 네트워크의 침입에 대응하기 위한 정보를 상기 네트워크 침입방지시스템과 침입방지운영시스템에 전송하며, 상기 제1단계 후에 상기 침입방지운영시스템은 상기 서버시스템으로부터 전송받은 정보를 기존의 보안정책에 추가하여 업데이트하고 이를 상기 서버시스템과 네트워크 침입방지시스템에 전송하며, 상기 제2단계에서 상기 네트워크 침입방지시스템은 상기 서버시스템으로부터 전송받은 정보 또는 상기 업데이트된 보안정책을 기반으로 하여 유해 트래픽을 탐지하고 차단하며, 이에 대한 정보를 상기 침입방지운영시스템에 전송하며, 상기 제2단계 후에 상기 침입방지운영시스템은 상기 네트워크 침입방지시스템으로부터 전송받은 정보를 상기 업데이트된 보안정책에 추가하여 다시 업데이트할 수 있다.

상기 서버시스템에는 서버보안을 위한 소프트웨어인 서버보안에이전트가 설치되고, 이 서버보안에이전트가 유해 트래픽을 탐지하고 이에 대한 정보를 상기 네트워크 침입방지시스템과 상기 침입방지운영시스템에 전송하는 것이 바람직하다.

상기 침입시스템에 대한 정보는 침입시스템 아이피 주소, 접근 포트에 대한 정보이고, 상기 침입에 대응하기 위한 정보는 트래픽 차단 유형, 트래픽 차단 시간에 대한 정보일 수도 있다.

상기 방법을 구현하는 보안시스템은 서버에 대한 악의적인 침입 시도에 대하여 유해 트래픽을 탐지하고 유해 트래픽을 전송한 침입시스템에 대한 정보를 네트워크 침입방지시스템에 전송하는 서버시스템과, 상기 서버시스템으로부터 전송받은 정보를 기반으로 유해 트래픽의 접근을 차단하는 네트워크 침입방지시스템을 포함하여 이루어진다.

상기 서버시스템 및 상기 네트워크 침입방지시스템의 운영에 필요한 보안정책을 설정, 변경, 관리하는 침입방지운영시스템을 더 포함할 수 있다.

상기 서버시스템에는 유해 트래픽을 탐지하고 이에 대한 정보를 상기 네트워크 침입방지시스템에 전송하는 소프트웨어인 서버보안에이전트가 설치되는 것이 바람직하다.

이하, 첨부된 도면을 참조해서 본 발명의 실시예를 상세히 설명하면 다음과 같다. 우선 각 도면의 구성 요소들에 참조 부호를 부가함에 있어서, 동일한 구성 요소들에 한해서는 비록 다른 도면상에 표시되더라도 가능한 한 동일한 부호를 가지도록 하고 있음에 유의해야 한다. 그리고, 본 발명을 설명함에 있어서, 관련된 공지 기능 혹은 구성에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우 그 상세한 설명을 생략한다.

도 2는 본 발명의 일실시예에 따른 서버 네트워크 보안시스템의 구성을 보여주는 도면이다. 보안시스템은 해당 네트워크에 대한 유해한 접근을 차단하는 방화벽(300), 네트워크 침입방지시스템(500), 서버시스템(600~603), 침입방지운영시스템(700), 서버보안 에이전트(800~803) 등으로 이루어진다.

네트워크 침입방지시스템(500)은 IPS(Intrusion Prevention System)라고도 하며 IDS(Intrusion Detection System)가 특정 패턴을 기반으로 공격자의 침입을 탐지하는데 그치는 반면 네트워크 침입방지시스템(IPS)(500)은 공격탐지를 뛰어넘어 탐지된 공격에 대해 웹 연결을 끊는 등 적극적으로 방지한다는 데에 특징이 있으며, 그 외에 프로토콜, IP주소, 포트주소, 애플리케이션 등의 네트워크 상의 정보를 활용하여 트래픽의 양을 조절하기도 한다. 본 발명에서는 이와 같은 역할 외에 서버시스템(600~603)으로부터 침입 시스템 정보를 전송받아 저장하고 이를 기반으로 유해 트래픽의 접근을 차단하는 기능을 더 수행한다.

서버시스템(600~603)에는 서버에 대한 악의적인 침입 시도를 탐지하기 위한 서버보안 에이전트(800~803)가 설치되어 있다. 서버보안 에이전트(800~803)는 원칙적으로 상기 네트워크 침입방지시스템(500)이 탐지할 수 없는 유형의 유해 트래픽을 탐지하고 이에 대한 정보를 네트워크 침입방지시스템(500)에 전송하여 해당 유해 트래픽의 차단을 요청한다.

삭제

침입방지운영시스템(700)은 서버시스템(600~603) 및 네트워크 침입방지시스템(500)의 운영에 필요한 보안정책을 설정, 변경, 관리하는 역할을 한다.

서버시스템(600~603)에 악의적인 침입을 시도하는 것은 다양한 형태가 될 수 있다. 첫번째는 접근시스템(100)에서 침입하고자 하는 서버시스템(600~603)의 관리자 권한을 얻기 위해 계속적인 로그인 시도를 하는 경우이다. 이러한 경우 서버보안 에이전트(800~803)가 이를 탐지하여 접근시스템(100)의 사용자에 대한 정보를 네트워크 통신을 이용하여 네트워크 침입방지시스템(500)으로 전달한다. 네트워크 침입방지시스템(500)은 서버시스템(600~603)으로부터 수신한 정보를 이용하여 접근시스템(100)으로부터의 연결이나 시도를 차단한다.

두번째는 접근시스템(100)에서 Telnet이나 FTP 등을 이용하여 서버시스템(600~603)의 중요한 자원(파일 또는 레지스트리)이나 허가되지 않은 자원에 접근한 경우이다. 이러한 경우 서버보안 에이전트(800~803)가 이를 탐지하여 접근시스템(100)의 사용자에 대한 정보를 네트워크 통신을 통해 네트워크 침입방지시스템(500)으로 전달한다. 네트워트 침입방지시스템(500)은 수신된 정보를 바탕으로 연결을 차단하게 된다.

세번째는 접근시스템(100)에서 네트워크 침입방지시스템을 우회하여 서버시스템(600~603)에 접근하는 경우이다. 우회하는 방법은 Fragmentation 이나 암호화를 이용하는 등의 방법이 있는데, 네트워크 침입방지시스템(500)은 이를 탐지하지 못한다. 이러한 경우 서버시스템(600~603)에 설치된 서버보안 에이전트(800~803)는 호스트 기반이기 때문에 이를 탐지하여 접근시스템(100)의 정보를 네트워크 침입방지시스템(500)에 전달하여 공격시도를 차단한다.

이러한 보안시스템에서 서버와 네트워크를 이용하여 시스템을 보안하는 방법을 구체적으로 설명하고자 한다.

이러한 방법은 크게 두단계를 거친다. 서버시스템(600~603)에서 유해 트래픽을 탐지하면 유해 트래픽을 전송한 침입시스템에 대한 정보를 네트워크 침입방지시스템(500)에 전송하는 단계와, 네트워크 침입방지시스템(500)은 서버시스템(600~603)으로부터 전송받은 정보를 기반으로 하여 유해 트래픽의 접근을 차단하는 단계이다.

이러한 단계를 더욱 세분하여 설명하면 다음과 같다.

도 3은 본 발명의 일실시예에 따른 서버 보안 솔루션과 네트워크 보안 솔루션을 이용한 시스템 보안 방법을 보여주는 흐름도이다.

서버시스템(600~603)의 서버보안 에이전트(800~803)는 서버시스템을 구성하는 각 서버에 설치되어 있으면서 해당 서버에 유입된 유해 트래픽이 발생시키는 여러 가지 이벤트를 모니터링하고 있다가 미리 설정된 보안정책에 따라 해당 이벤트의 내용를 저장하는 방식으로 유해 트래픽을 탐지한다(S310).
서버시스템(600~603)은 상기 탐지된 유해 트래픽을 발송한 침입시스템에 대한 정보 및 해당 침입에 대응하기 위한 정보를 네트워크 침입방지시스템(500)에 전송한다(S320). 여기서, 침입시스템에 대한 정보는 침입시스템의 아이피 주소, 접근 포트에 대한 정보가 될 수 있고, 침입에 대응하기 위한 정보는 트래픽 차단 유형, 트래픽 차단 시간에 대한 정보가 될 수 있다.

한편, 상기 S320 단계에서 서버시스템(600~603)은 침입시스템 정보 및 대응 정보를 침입방지운영시스템(700)에도 더 전송할 수 있는데, 침입방지운영시스템(700)은 서버시스템(600~603)으로부터 전송받은 정보를 바탕으로 기존의 보안정책을 업데이트한다(S330). 그리고, 업데이트된 보안정책을 서버시스템(600~603)과 네트워크 침입방지시스템(500)에 각각 전송하여 새로운 보안정책에 의해 유해 트래픽 탐지 및 차단이 수행되도록 한다(S340).

네트워크 침입방지시스템(500)은 서버시스템(600~603)으로부터 전송받은 정보를 기반으로 하되 업데이트된 보안정책에 따라 유해 트래픽을 탐지하고 차단한다(S350). 그리고, 탐지 및 차단한 트래픽에 대한 로그 정보를 침입방지운영시스템(700)에 전송한다(S360).

침입방지운영시스템(700)은 네트워크 침입방지시스템(500)으로부터 전송받은 정보를 기존의 보안정책에 추가하여 다시 업데이트한다(S370).

이상 본 발명을 몇 가지 바람직한 실시예를 사용하여 설명하였으나, 이들 실시예는 예시적인 것이며 한정적인 것이 아니다. 본 발명이 속하는 기술분야에서 통상의 지식을 지닌 자라면 본 발명의 사상과 첨부된 특허청구범위에 제시된 권리범위에서 벗어나지 않으면서 다양한 변화와 수정을 가할 수 있음을 이해할 것이다.

발명의 효과

이상에서 설명한 바와 같이, 본 발명에 의하면 서버시스템에서 악의적인 침입 시도를 탐지하여 네트워크 단계에서 침입을 차단함으로써, 제2, 제3의 악의적인 침입시도를 원천적으로 차단할 수 있으며, 반복적인 침입 시도에 따른 네트워크 자원의 소모를 사전에 방지하는 효과가 있다. 부가적으로 다른 서버들에 대한 유해 침입 시도를 차단함으로써, 서버시스템이 악의적인 시도에 대한 응답을 하지 않게 되므로 리소스 활용을 높일 수 있는 효과가 있다.

(57) 청구의 범위

청구항 1.

해당 네트워크에 대한 유해한 접근을 차단하는 방화벽과 네트워크에 대한 침입을 차단하는 네트워크 침입방지시스템과 메일서버, FTP 서버 등을 포함하는 서버시스템으로 이루어지는 시스템의 보안 방법에 있어서,

상기 서버시스템에서 유해 트래픽을 탐지하면 유해 트래픽을 전송한 침입시스템에 대한 정보를 네트워크 침입방지시스템에 전송하는 제1단계와,

상기 네트워크 침입방지시스템은 상기 서버시스템으로부터 전송받은 정보를 기반으로 하여 유해 트래픽의 접근을 차단하는 제2단계

를 구비하는 것을 특징으로 하는 서버 보안 솔루션과 네트워크 보안 솔루션을 이용한 시스템 보안 방법.

청구항 2.

제1항에 있어서,

상기 제1단계에서 상기 서버시스템은 상기 침입시스템에 대한 정보와 함께 네트워크의 침입에 대응하기 위한 정보를 상기 네트워크 침입방지시스템과 침입방지운영시스템에 전송하며,

상기 제1단계 후에 상기 침입방지운영시스템은 상기 서버시스템으로부터 전송받은 정보를 기존의 보안정책에 추가하여 업데이트하고 이를 상기 서버시스템과 네트워크 침입방지시스템에 전송하며,

상기 제2단계에서 상기 네트워크 침입방지시스템은 상기 서버시스템으로부터 전송받은 정보 또는 상기 업데이트된 보안정책을 기반으로 하여 유해 트래픽을 탐지하고 차단하며, 이에 대한 정보를 상기 침입방지운영시스템에 전송하며,

상기 제2단계 후에 상기 침입방지운영시스템은 상기 네트워크 침입방지시스템으로부터 전송받은 정보를 상기 업데이트된 보안정책에 추가하여 다시 업데이트하는 것을 특징으로 하는 서버 보안 솔루션과 네트워크 보안 솔루션을 이용한 시스템 보안 방법.

청구항 3.

제2항에 있어서,

상기 서버시스템에는 서버보안을 위한 소프트웨어인 서버보안에이전트가 설치되고, 이 서버보안에이전트가 유해 트래픽을 탐지하고 이에 대한 정보를 상기 네트워크 침입방지시스템과 상기 침입방지운영시스템에 전송하는 것을 특징으로 하는 서버 보안 솔루션과 네트워크 보안 솔루션을 이용한 시스템 보안 방법.

청구항 4.

제2항에 있어서,

상기 침입시스템에 대한 정보는 침입시스템 아이피 주소, 접근 포트에 대한 정보이고, 상기 침입에 대응하기 위한 정보는 트래픽 차단 유형, 트래픽 차단 시간에 대한 정보인 것을 특징으로 하는 서버 보안 솔루션과 네트워크 보안 솔루션을 이용한 시스템 보안 방법.

청구항 5.

서버에 대한 악의적인 침입 시도에 대하여 유해 트래픽을 탐지하고 유해 트래픽을 전송한 침입시스템에 대한 정보를 네트워크 침입방지시스템에 전송하는 서버시스템과,

상기 서버시스템으로부터 전송받은 정보를 기반으로 유해 트래픽의 접근을 차단하는 네트워크 침입방지시스템

을 포함하는 보안시스템.

청구항 6.

제5항에 있어서,

상기 서버시스템 및 상기 네트워크 침입방지시스템의 운영에 필요한 보안정책을 설정, 변경, 관리하는 침입방지운영시스템을 더 포함하는 것을 특징으로 하는 보안시스템.

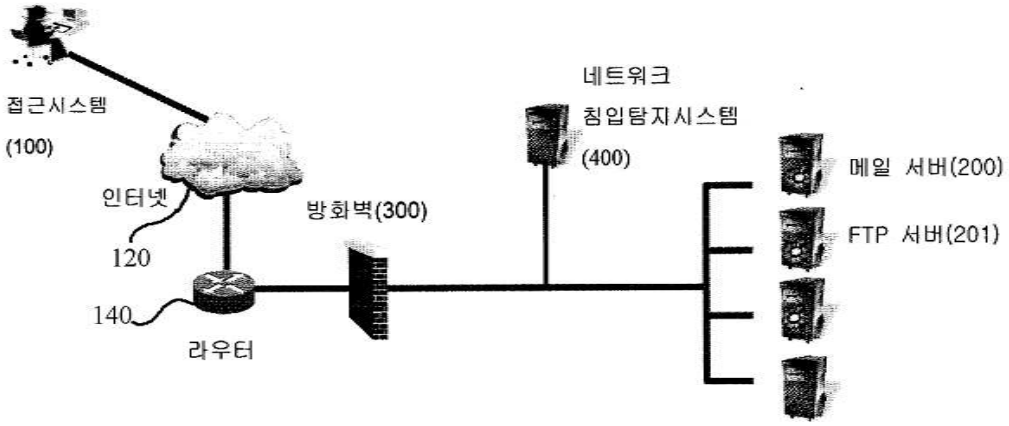
청구항 7.

제5항에 있어서,

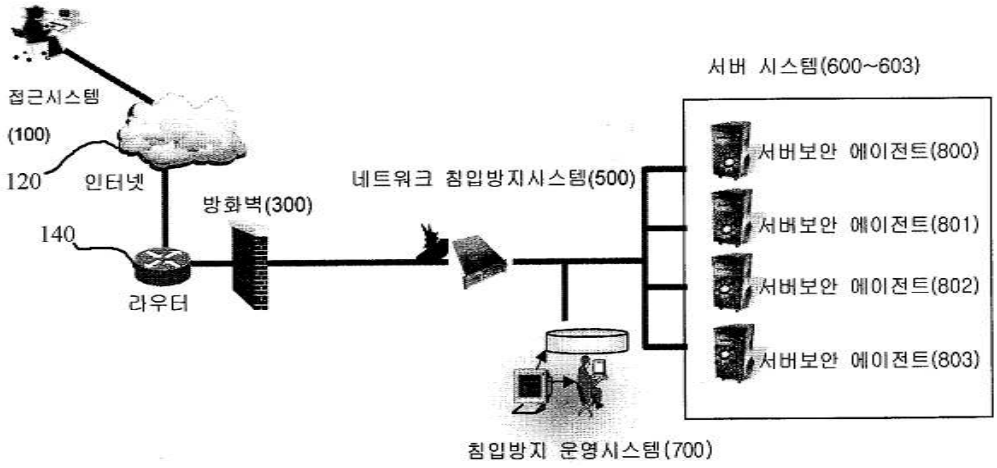
상기 서버시스템에는 유해 트래픽을 탐지하고 이에 대한 정보를 상기 네트워크 침입방지시스템에 전송하는 소프트웨어인 서버보안에이전트가 설치되는 것을 특징으로 하는 보안시스템.

도면

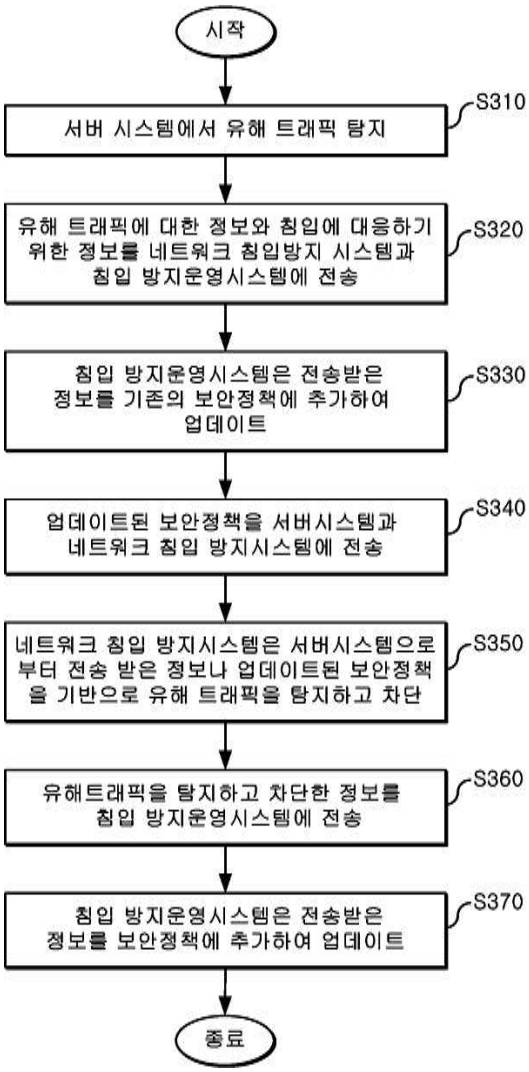
도면1



도면2



도면3


시작
서버 시스템에서 유해 트래픽 탐지
S310
유해 트래픽에 대한 정보와 침입에 대응하기 위한 정보를 네트워크 침입방지 시스템과 침입 방지운영시스템에 전송
S320
침입 방지운영시스템은 전송받은 정보를 기존의 보안정책에 추가하여 업데이트
S330
업데이트된 보안정책을 서버시스템과 네트워크 침입 방지시스템에 전송
S340
네트워크 침입 방지시스템은 서버시스템으로부터 전송 받은 정보나 업데이트된 보안정책을 기반으로 유해 트래픽을 탐지하고 차단
S350
유해트래픽을 탐지하고 차단한 정보를 침입 방지운영시스템에 전송
S360
침입 방지운영시스템은 전송받은 정보를 보안정책에 추가하여 업데이트
S370
종료