(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2014년03월06일
(11) 등록번호 10-1369727
(24) 등록일자 2014년02월26일

(51) 국제특허분류(Int. Cl.)
H04L 12/26 (2006.01)
(21) 출원번호 10-2012-0075630
(22) 출원일자 2012년07월11일
심사청구일자 2012년07월11일
(65) 공개번호 10-2014-0022975
(43) 공개일자 2014년02월26일
(56) 선행기술조사문헌
KR1020110059963 A*
KR1020110119915 A
KR1020100013989 A
*는 심사관에 의하여 인용된 문헌
기술이전 희망 : **기술양도, 실시권허여, 기술지도**

(73) 특허권자
한국전자통신연구원
대전광역시 유성구 가정로 218 (가정동)
(72) 발명자
김덕진
대전 유성구 반석서로 109, 706동 1002호 (반석동, 반석마을7단지아파트)
한병진
경기 수원시 권선구 구운로47번길 56-4, 403호 (구운동, 에쿠스빌)
(뒷면에 계속)
(74) 대리인
한양특허법인

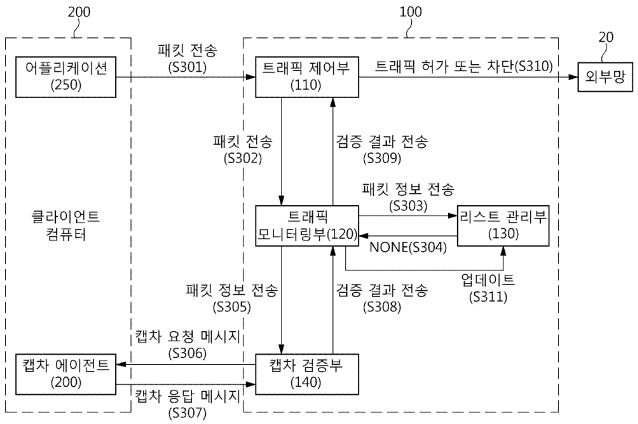
전체 청구항 수 : 총 9 항 심사관 : 전용해

(54) 발명의 명칭 **캡차를 기반으로 하는 트래픽 제어 장치 및 그 방법**

(57) 요 약

캡차를 기반으로 하는 트래픽 제어 장치 및 그 방법이 개시된다. 본 발명에 따른 트래픽 제어 장치는 내부망과 외부망 사이에서 송수신되는 패킷을 모니터링하는 트래픽 모니터링부, 패킷에 해당하는 패킷 정보가 접근 제어 리스트에 존재하지 않는 경우, 패킷 정보에 해당하는 캡차 요청 메시지를 내부망의 클라이언트 컴퓨터로 전송하고, 캡차 요청 메시지에 대응하는 캡차 응답 메시지를 전달받아, 캡차 응답 메시지를 검증하는 캡차 검증부, 패킷 정보가 접근 제어 리스트에 존재하는 경우, 접근 제어 리스트에서 패킷 정보에 해당하는 통제 정책을 검출하는 리스트 관리부, 및 캡차 응답 메시지를 검증한 결과 또는 통제 정책을 토대로 내부망과 외부망 사이의 트래픽을 제어하는 트래픽 제어부를 포함한다.

대 표 도



(72) 발명자

이철우

대전 유성구 유성대로1679번길 8-15, 404호 (전민동)

이만희

대전 유성구 엑스포로 448, 210동 1002호 (전민동, 엑스포아파트)

배병철

대전광역시 서구 문예로 174, 116동 1105호(둔산동 샘머리아파트)

오형근

대전 유성구 지족로 343, 204동 204호 (지족동, 반석마을2단지아파트)

손기욱

대전 유성구 엑스포로 501, 109동 1506호 (전민동, 청구나래아파트)

특허청구의 범위

청구항 1

내부망과 외부망 사이에서 송수신되는 패킷에 해당하는 패킷 정보가 접근 제어 리스트에 존재하는지 확인하는 단계;

상기 접근 제어 리스트에 패킷 정보가 없는 경우, 상기 패킷 정보에 해당하는 캡차 값을 생성하는 단계;

상기 캡차 값을 포함하는 캡차 요청 메시지를 상기 내부망의 클라이언트 컴퓨터로 전송하고, 상기 캡차 요청 메시지에 대응하는 캡차 응답 메시지를 전달받는 단계; 및

상기 캡차 응답 메시지를 검증하고, 검증한 결과를 토대로 상기 내부망과 외부망 사이의 트래픽을 제어하는 단계

를 포함하고,

상기 내부망과 외부망 사이의 트래픽을 제어하는 단계는

상기 캡차 응답 메시지를 검증한 결과를 상기 접근 제어 리스트에 업데이트하는 것을 특징으로 하는 트래픽 제어 방법.

청구항 2

청구항 1에 있어서,

상기 캡차 요청 메시지는 상기 캡차 값뿐만 아니라 상기 패킷 정보에 해당하는 도메인 정보, 위치 정보를 포함하는 것을 특징으로 하는 트래픽 제어 방법.

청구항 3

청구항 1에 있어서,

상기 캡차 응답 메시지를 전달받는 단계는

상기 클라이언트 컴퓨터의 사용자에게 상기 캡차 요청 메시지를 제공하고, 상기 사용자로부터 상기 캡차 응답 메시지를 전달받는 것을 특징으로 하는 트래픽 제어 방법.

청구항 4

삭제

청구항 5

청구항 1에 있어서,

상기 캡차 응답 메시지는 상기 트래픽을 발생한 주체가 실제 사람인지 악성코드인지를 구별할 수 있는 정보를 포함하는 것을 특징으로 하는 트래픽 제어 방법.

청구항 6

내부망과 외부망 사이에서 송수신되는 패킷에 해당하는 패킷 정보가 접근 제어 리스트에 존재하는지 확인하는 단계;

상기 접근 제어 리스트에 패킷 정보가 있는 경우, 상기 접근 제어 리스트에서 상기 패킷 정보에 해당하는 통제 정책을 검출하는 단계; 및

상기 통제 정책을 토대로 상기 내부망과 외부망 사이의 트래픽을 제어하는 단계

를 포함하고,

상기 접근 제어 리스트는

사전에 트래픽을 제어한 결과를 토대로 설정한 상기 통제 정책, 패킷의 출발지 주소, 목적지 주소를 포함하는 것을 특징으로 하는 트래픽 제어 방법.

청구항 7

삭제

청구항 8

내부망과 외부망 사이에서 송수신되는 패킷을 모니터링하는 트래픽 모니터링부;

상기 패킷에 해당하는 패킷 정보가 접근 제어 리스트에 존재하지 않는 경우, 상기 패킷 정보에 해당하는 캡차 요청 메시지를 상기 내부망의 클라이언트 컴퓨터로 전송하고, 상기 캡차 요청 메시지에 대응하는 캡차 응답 메시지를 전달받아, 상기 캡차 응답 메시지를 검증하는 캡차 검증부;

상기 패킷 정보가 상기 접근 제어 리스트에 존재하는 경우, 상기 접근 제어 리스트에서 상기 패킷 정보에 해당하는 통제 정책을 검출하는 리스트 관리부; 및

상기 캡차 응답 메시지를 검증한 결과 또는 상기 통제 정책을 토대로 상기 내부망과 외부망 사이의 트래픽을 제어하는 트래픽 제어부

를 포함하고,

상기 리스트 관리부는

상기 캡차 응답 메시지를 검증한 결과를 토대로 상기 접근 제어 리스트를 업데이트하여 관리하는 것을 특징으로 하는 트래픽 제어 장치.

청구항 9

청구항 8에 있어서,

상기 캡차 검증부는

상기 패킷 정보에 해당하는 캡차 값을 생성하고, 상기 캡차 값과 상기 패킷 정보에 해당하는 도메인 정보, 위치 정보를 포함하는 상기 캡차 요청 메시지를 상기 클라이언트 컴퓨터로 전송하는 것을 특징으로 하는 트래픽 제어 장치.

청구항 10

청구항 8에 있어서,

상기 캡차 검증부는

상기 트래픽을 발생한 주체가 실제 사람인지 악성코드인지를 구별할 수 있는 정보를 포함하는 상기 캡차 응답 메시지를 상기 클라이언트 컴퓨터의 사용자로부터 전달받는 것을 특징으로 하는 트래픽 제어 장치.

청구항 11

청구항 8에 있어서,

상기 캡차 요청 메시지가 포함하는 캡차 값을 생성하는데 있어 필요한 도메인 정보를 수집하는 수집부

를 더 포함하는 트래픽 제어 장치.

청구항 12

삭제

명 세 서

기 술 분 야

[0001] 본 발명은 캡차를 기반으로 하는 트래픽 제어 장치 및 그 방법에 관한 것으로, 특히 사용자들의 인터넷 사용 정

보를 학습하고, 학습한 결과와 캡차를 이용하여 악성코드에 의해 사용자의 내부 자료가 외부로 유출되는 것을 방지하는 트래픽 제어 장치 및 그 방법에 관한 것이다.

배 경 기 술

[0002] 사용자가 인식하지 못한 상태에서 악성코드에 의해 사용자의 자료가 외부로 유출되는 보안 사고가 발생하고 있다. 이러한 사고를 예방하기 위해 현재 안티바이러스 기술 및 네트워크 침입 감지 시스템(Intrusion Detection System, IDS) 기술 그리고 데이터 유출 방지(Data Leakage/Loss Prevention, DLP) 기술들이 활용되고 있다.

[0003] 안티바이러스 기술이나 네트워크 IDS 기술들은 외부에서 들어오는 공격에 대해 방어하기 위한 기술이다. 여기서, 안티바이러스 기술은 외부로부터 유입된 악성코드가 사용자의 컴퓨터에 설치되거나 실행되는 것을 탐지한다. 네트워크 IDS 기술은 네트워크 트래픽을 조사하여 외부에서 내부로 유입되는 트래픽 중에 유해한 트래픽이 존재하는지 탐지한다.

[0004] 이러한 기술들은 악성코드 및 악성 트래픽이라고 식별할 수 있는 시그니처 정보를 가지고 있다. 그리고 시그니처 정보에 일치하는 악성코드가 메모리나 파일 상에 존재하거나, 시그니처 정보에 일치하는 악성트래픽이 네트워크 패킷 상에 존재할 경우 이를 탐지하고 동작하지 않도록 처리한다.

[0005] 한편, 네트워크 DLP 기술들은 사용자의 내부 자료가 유출될 수 있는 네트워크 프로토콜을 모두 분석하고 분석된 결과에 기반을 두어 외부로 나가는 트래픽을 분석하고 내부 자료가 빠져나가는 것을 탐지한다.

[0006] 한국 공개 특허 제2011-0059963호는 유해 트래픽 차단 장치 및 방법과 이를 이용한 유해 트래픽 차단 시스템에 관한 것으로, 클라이언트에서 서비스 제공 서버로 향하는 트래픽 양이 기설정된 트래픽 양을 초과하면 이상 트래픽 감지 신호를 발생시키고, 캡차 인증을 수행하여 정상 클라이언트와 좀비 클라이언트를 구분하며, 좀비 클라이언트에서 발생한 트래픽을 유해 트래픽으로 판단하여 차단하는 기술을 기재하고 있습니다. 이는 서비스 제공 서버를 보호하기 위한 방법으로 클라이언트에서 발생하는 이상 트래픽을 클라이언트가 속한 네트워크에서 차단하지는 않는다.

[0007] 내부 자료가 공개되는 것을 방지하기 위해 활용된 종래의 기술에는 몇 가지 단점이 있다. 시그니처 기반으로 탐지를 수행하는 안티바이러스 기술이나 네트워크 IDS 기술들은 시그니처 정보가 없는 신규 악성코드에 의한 자료 유출을 탐지할 수 없다. 그리고 성능상의 이유로 주로 외부에서 내부로 들어오는 공격에 집중하여 방어를 수행하기 때문에 내부에서 유출되는 자료를 탐지하기에는 적절하지 않다.

발명의 내용

해결하려는 과제

[0008] 본 발명의 목적은 사용자들의 인터넷 사용 정보를 학습하고, 학습한 결과와 캡차를 이용하여 악성코드에 의해 사용자의 내부 자료가 외부로 유출되는 것을 방지하는 트래픽 제어 장치 및 그 방법을 제공하는 것이다.

과제의 해결 수단

[0009] 상기한 목적을 달성하기 위한 본 발명에 따른 트래픽 제어 방법은

[0010] 내부망과 외부망 사이에서 송수신되는 패킷에 해당하는 패킷 정보가 접근 제어 리스트에 존재하는지 확인하는 단계; 상기 접근 제어 리스트에 패킷 정보가 없는 경우, 상기 패킷 정보에 해당하는 캡차 값을 생성하는 단계; 상기 캡차 값을 포함하는 캡차 요청 메시지를 상기 내부망의 클라이언트 컴퓨터로 전송하고, 상기 캡차 요청 메시지에 대응하는 캡차 응답 메시지를 전달받는 단계; 및 상기 캡차 응답 메시지를 검증하고, 검증한 결과를 토대로 상기 내부망과 외부망 사이의 트래픽을 제어하는 단계를 포함한다.

[0011] 이 때, 상기 캡차 요청 메시지는 상기 캡차 값뿐만 아니라 상기 패킷 정보에 해당하는 도메인 정보, 위치 정보를 포함하는 것을 특징으로 한다.

[0012] 이 때, 상기 캡차 응답 메시지를 전달받는 단계는 상기 클라이언트 컴퓨터의 사용자에게 상기 캡차 요청 메시지를 제공하고, 상기 사용자로부터 상기 캡차 응답 메시지를 전달받는 것을 특징으로 한다.

[0013] 이 때, 상기 내부망과 외부망 사이의 트래픽을 제어하는 단계는 상기 캡차 응답 메시지를 검증한 결과를 상기 접근 제어 리스트에 업데이트하는 것을 특징으로 한다.

[0014] 이 때, 상기 캡차 응답 메시지는 상기 트래픽을 발생한 주체가 실제 사람인지 악성코드인지를 구별할 수 있는 정보를 포함하는 것을 특징으로 한다.

[0015] 또한, 본 발명의 일실시예에 따른 트래픽 제어 방법은

[0016] 내부망과 외부망 사이에서 송수신되는 패킷에 해당하는 패킷 정보가 접근 제어 리스트에 존재하는지 확인하는 단계; 상기 접근 제어 리스트에 패킷 정보가 있는 경우, 상기 접근 제어 리스트에서 상기 패킷 정보에 해당하는 통제 정책을 검출하는 단계; 및 상기 통제 정책을 토대로 상기 내부망과 외부망 사이의 트래픽을 제어하는 단계를 포함한다.

[0017] 이 때, 상기 접근 제어 리스트는 사전에 트래픽을 제어한 결과를 토대로 설정한 상기 통제 정책, 패킷의 출발지 주소, 목적지 주소를 포함하는 것을 특징으로 한다.

[0018] 또한, 본 발명의 일실시예에 따른 트래픽 제어 장치는

[0019] 내부망과 외부망 사이에서 송수신되는 패킷을 모니터링하는 트래픽 모니터링부; 상기 패킷에 해당하는 패킷 정보가 접근 제어 리스트에 존재하지 않는 경우, 상기 패킷 정보에 해당하는 캡차 요청 메시지를 상기 내부망의 클라이언트 컴퓨터로 전송하고, 상기 캡차 요청 메시지에 대응하는 캡차 응답 메시지를 전달받아, 상기 캡차 응답 메시지를 검증하는 캡차 검증부; 상기 패킷 정보가 상기 접근 제어 리스트에 존재하는 경우, 상기 접근 제어 리스트에서 상기 패킷 정보에 해당하는 통제 정책을 검출하는 리스트 관리부; 및 상기 캡차 응답 메시지를 검증한 결과 또는 상기 통제 정책을 토대로 상기 내부망과 외부망 사이의 트래픽을 제어하는 트래픽 제어부를 포함한다.

[0020] 이 때, 상기 캡차 검증부는 상기 패킷 정보에 해당하는 캡차 값을 생성하고, 상기 캡차 값과 상기 패킷 정보에 해당하는 도메인 정보, 위치 정보를 포함하는 상기 캡차 요청 메시지를 상기 클라이언트 컴퓨터로 전송하는 것을 특징으로 한다.

[0021] 이 때, 상기 캡차 검증부는 상기 트래픽을 발생한 주체가 실제 사람인지 악성코드인지를 구별할 수 있는 정보를 포함하는 상기 캡차 응답 메시지를 상기 클라이언트 컴퓨터의 사용자로부터 전달받는 것을 특징으로 한다.

[0022] 이 때, 트래픽 제어 장치는 상기 캡차 요청 메시지가 포함하는 캡차 값을 생성하는데 있어 필요한 도메인 정보를 수집하는 수집부를 더 포함한다.

[0023] 이 때, 상기 리스트 관리부는 상기 캡차 응답 메시지를 검증한 결과를 토대로 상기 접근 제어 리스트를 업데이트하여 관리하는 것을 특징으로 한다.

발명의 효과

[0024] 본 발명에 따르면, 캡차를 기반으로 하는 트래픽 제어 장치 및 그 방법은 시그니처 정보가 없는 악성코드에 대해서도 캡차를 기반으로 트래픽을 제어함으로써, 악성코드에 의한 자료 유출을 방지할 수 있다.

도면의 간단한 설명

[0025] 도 1은 본 발명의 실시예에 따른 캡차를 기반으로 하는 트래픽 제어 장치가 적용되는 환경을 나타내는 도면이다.

도 2는 본 발명의 실시예에 따른 캡차를 기반으로 하는 트래픽 제어 장치를 개략적으로 나타내는 구성도이다.

도 3은 본 발명의 실시예에 따른 접근 제어 리스트에 패킷 정보가 존재하지 않는 경우 클라이언트 컴퓨터 내 어플리케이션에 의해 발생하는 트래픽을 제어하는 방법을 나타내는 흐름도이다.

도 4는 본 발명의 실시예에 따른 접근 제어 리스트에 패킷 정보가 존재하는 경우 클라이언트 컴퓨터 내 어플리케이션에 의해 발생하는 트래픽을 제어하는 방법을 나타내는 흐름도이다.

도 5는 본 발명의 실시예에 따른 트래픽 제어 장치와 캡차 에이전트 간의 캡차 메시지 송수신 과정을 나타내는 도면이다.

발명을 실시하기 위한 구체적인 내용

[0026] 본 발명을 첨부된 도면을 참조하여 상세히 설명하면 다음과 같다. 여기서, 반복되는 설명, 본 발명의 요지를 불필요하게 흐릴 수 있는 공지 기능, 및 구성에 대한 상세한 설명은 생략한다. 본 발명의 실시형태는 당 업계에서 평균적인 지식을 가진 자에게 본 발명을 보다 완전하게 설명하기 위해서 제공되는 것이다. 따라서, 도면에서의 요소들의 형상 및 크기 등은 보다 명확한 설명을 위해 과장될 수 있다.

[0027] 이하, 본 발명에 따른 바람직한 실시예 따른 캡차를 기반으로 하는 트래픽 제어 장치 및 그 방법에 대하여 첨부한 도면을 참조하여 상세하게 설명한다.

[0028] 도 1은 본 발명의 실시예에 따른 캡차를 기반으로 하는 트래픽 제어 장치가 적용되는 환경을 나타내는 도면이다.

[0029] 도 1을 참고하면, 본 발명의 실시예에 따른 캡차를 기반으로 트래픽을 제어하는 네트워크 환경은 내부망(10)과 외부망(20)을 연결하는 네트워크 포인트에 위치하는 트래픽 제어 장치(100), 내부망(10)과 연결되는 복수개의 클라이언트 컴퓨터(11~13)가 각각 포함하는 캡차 에이전트(200) 및 외부망(20)의 서버(21~23)를 포함한다.

[0030] 트래픽 제어 장치(100)는 내부망(10)과 외부망(20) 사이에 위치하여 네트워크 패킷을 검사하고, 해당 패킷을 외부망(20)으로 전달할지 차단할지를 결정한다. 이를 위하여, 트래픽 제어 장치(100)는 내부망(10)과 연결되는 복수개의 클라이언트 컴퓨터(11~13)와 통신을 수행해야 한다.

[0031] 악성코드가 존재하지 않은 클라이언트 컴퓨터(11 및 12)의 어플리케이션이 트래픽 제어 장치(100)가 접근을 허용한 외부망(20)의 서버(21 및 22)에 접속하는 경우에는 트래픽 제어 장치(100)가 구축되지 않았을 때와 동일하게 외부 서비스를 이용할 수 있다.

[0032] 반면에, 악성코드(30)가 존재하는 클라이언트 컴퓨터(13)의 어플리게이션이 접근 허용 여부가 아직 결정되지 않은 외부망(20)의 서버(23)에 접속하는 경우에는 트래픽 제어 장치(100)는 캡차 메시지를 생성하고, 생성한 캡차 메시지를 클라이언트 컴퓨터(13)의 캡차 에이전트(200)에 전송한다. 여기서, 캡차 메시지는 사용자가 의도하지 않았는데 발생한 패킷에 대해 사용자가 판별할 수 있도록 하는 메시지로써, 패킷에 대한 DNS(Domain Name System/Domain Name Server) 정보와 같은 추가 정보를 포함한다.

[0033] 그러면, 캡차 에이전트(200)는 사용자가 접근 허용 여부를 식별할 수 있도록, 캡차 메시지에 해당하는 캡차 인증창을 화면에 표시한다.

[0034] 트래픽 제어 장치(100)는 캡차 인증창을 통해 사용자로부터 전달받은 캡차 응답을 이용하여 해당 패킷에 대해 처리하고, 캡차 응답은 학습되어 재사용된다. 그러나, 사용자가 아닌 악성코드(30)는 캡차 메시지에 대응하는 캡차 응답을 트래픽 제어 장치(100)로 전달할 수 없으므로, 해당 트래픽이 차단된다.

[0035] 다음, 트래픽 제어 장치(100)를 도 2를 참조하여 상세하게 설명한다.

[0036] 도 2는 본 발명의 실시예에 따른 캡차를 기반으로 하는 트래픽 제어 장치를 개략적으로 나타내는 구성도이다.

[0037] 도 2를 참고하면, 트래픽 제어 장치(100)는 트래픽 제어부(110), 트래픽 모니터링부(120), 리스트 관리부(130), 캡차 검증부(140) 및 DNS 수집부(150)를 포함한다.

[0038] 트래픽 제어부(110)는 내부망(10)과 외부망(20) 사이에서 송수신되는 패킷에 대응하는 통제 정책과 캡차 검증 결과를 토대로 패킷의 송수신 즉, 트래픽을 허가(PASS) 하거나 차단(BLOCK)한다.

[0039] 예를 들어, 트래픽 제어부(110)는 내부망(10)에서 외부망(20)으로 전달되는 트래픽을 우선적으로 보류하고, 내부망(10)과 외부망(20) 사이에서 송수신되는 모든 패킷들을 트래픽 모니터링부(120)로 전달한다.

[0040] 트래픽 모니터링부(120)는 트래픽 제어부(110)에서 제어하는 패킷들을 모니터링하고, 패킷 각각에 해당하는 패킷 정보를 리스트 관리부(130) 및 캡차 검증부(140)로 전달한다. 다음, 트래픽 모니터링부(120)는 패킷 정보에 대응하는 통제 정책을 리스트 관리부(130)로부터 전달받거나, 패킷 정보에 대응하는 검증 결과를 캡차 검증부(140)로부터 전달받는다.

[0041] 구체적으로, 트래픽 모니터링부(120)는 패킷 정보를 리스트 관리부(130)에 전달하여, 패킷 정보가 접근 제어 리

스트에 존재하는지를 확인한다.

[0042] 트래픽 모니터링부(120)는 패킷 정보가 접근 제어 리스트에 존재하는 경우, 리스트 관리부(130)에서 설정된 통제 정책을 트래픽 제어부(110)로 전달한다.

[0043] 트래픽 모니터링부(120)는 패킷 정보가 접근 제어 리스트에 존재하지 않는 경우, 패킷 정보를 캡차 검증부(140)로 전달하고, 패킷 정보에 대응하는 검증 결과를 캡차 검증부(140)로부터 전달받는다.

[0044] 또한, 트래픽 모니터링부(120)는 검증 결과를 리스트 관리부(130)로 전달함으로써, 향후 내부망(10)의 동일한 출발지 주소를 갖는 트래픽이 동일한 외부망(20)의 동일한 목적지 주소를 갖는 트래픽을 동일하게 제어(허가 또는 차단) 할 수 있도록 한다.

[0045] 또한, 트래픽 모니터링부(120)는 모니터링하는 패킷들이 DNS 정보를 포함하는 경우, 이를 DNS 수집부(150)로 전달한다.

[0046] 리스트 관리부(130)는 접근 제어 리스트를 관리하고, 접근 제어 리스트 내 패킷 정보에 해당하는 통제 정책을 설정한다. 여기서, 접근 제어 리스트는 통제 정책뿐만 아니라 패킷의 출발지 주소(IP, Port), 목적지 주소(IP, Port)를 비롯한 트래픽을 제어하는데 필요한 정보들을 포함한다.

[0047] 캡차 검증부(140)는 트래픽 모니터링부(120)로부터 전달받은 패킷 정보에 해당하는 캡차 값을 생성하고, 생성한 캡차 값, 패킷 정보에 해당하는 도메인 정보, 패킷 정보와 관련된 정보 등을 포함하는 캡차 요청 메시지를 내부망(10)의 클라이언트 컴퓨터(11~13)로 전달한다. 다음, 캡차 검증부(140)는 캡차 요청 메시지에 대응하는 캡차 응답 메시지를 전달받고, 전달받은 캡차 응답 메시지를 검증하고, 검증 결과를 트래픽 모니터링부(120)로 전달한다.

[0048] DNS 수집부(150)는 트래픽 모니터링부(120)로부터 전달받은 DNS 정보를 관리한다. 즉, DNS 수집부(150)는 내부망(10)에서 수집된 DNS 정보를 관리한다. 여기서, DNS 정보는 캡차 검증부(140)에서 캡차값을 생성하는데 있어 필요한 도메인 정보이다.

[0049] 다음, 트래픽 제어 장치(100)가 복수개의 클라이언트 컴퓨터(11~13) 중 특정 클라이언트 컴퓨터 내 어플리케이션에 의해 발생하는 트래픽을 캡차를 이용하여 외부로 전송하는 방법을 도 3을 참조하여 상세하게 설명한다.

[0050] 도 3은 본 발명의 실시예에 따른 클라이언트 컴퓨터 내 어플리케이션에 의해 발생하는 트래픽을 제어하는 방법을 나타내는 흐름도이다.

[0051] 먼저, 트래픽 제어 장치(100)는 내부망(10)과 외부망(20) 사이에 위치하여, 내부망(10)과 외부망(20) 사이에서 전송되는 트래픽을 제어한다. 이를 위하여, 트래픽 제어 장치(100)는 트래픽 제어부(110), 트래픽 모니터링부(120), 리스트 관리부(130) 및 캡차 검증부(140)를 포함한다.

[0052] 도 3을 참고하면, 내부망(10)의 클라이언트 컴퓨터 내 어플리케이션(250)은 외부망(20)의 서버로 전송할 패킷을 트래픽 제어 장치(100)의 트래픽 제어부(110)로 전송한다(S301).

[0053] 트래픽 제어부(110)는 내부망(10)에서 외부망(20)으로 전달되는 트래픽을 보류하고, S301 단계에서 전달받은 패킷을 트래픽 모니터링부(120)로 전송한다(S302).

[0054] 트래픽 모니터링부(120)는 전달받은 패킷에 해당하는 패킷 정보를 리스트 관리부(130)로 전송한다(S303).

[0055] 리스트 관리부(130)는 사전에 저장되어 있는 접근 제어 리스트에 S303 단계에서 전달받은 패킷 정보가 존재하는지를 확인하고, 확인 후 존재하지 않는다는 결과(NONE)를 트래픽 모니터링부(120)로 전송한다(S304).

[0056] 트래픽 모니터링부(120)는 접근 제어 리스트에 전달받은 패킷에 해당하는 패킷 정보가 없는 경우, 패킷 정보를 캡차 검증부(140)로 전송한다(S305).

[0057] 캡차 검증부(140)는 패킷 정보에 해당하는 캡차 값을 생성하고, 생성한 캡차 값, 패킷 정보에 해당하는 도메인 정보, 패킷 정보와 관련된 정보 등을 포함하는 캡차 요청 메시지를 클라이언트 컴퓨터 내 캡차 에이전트(200)로 전송한다(S306).

[0058] 클라이언트 컴퓨터 내 캡차 에이전트(200)는 캡차 요청 메시지를 클라이언트 컴퓨터의 사용자에게 제공하고, 사용자로부터 캡차 응답 메시지를 입력받는다. 이때, 사용자는 정상적인 캡차 응답 메시지를 입력할 수 있으나,

악성코드는 정상적인 캡차 응답 메시지를 입력할 수 없다.

[0059] 다음, 캡차 에이전트(200)는 캡차 응답 메시지를 캡차 검증부(140)로 전송한다(S307).

[0060] 캡차 검증부(140)는 캡차 응답 메시지를 검증하고, 검증 결과를 트래픽 모니터링부(120)로 전달한다(S308). 본 발명의 실시예에 따른, 캡차 검증부(140)가 캡차 요청 메시지를 캡차 에이전트(200)로 전송하고, 캡차 에이전트(200)로부터 캡차 응답 메시지를 전달받아, 이를 토대로 검증 과정을 수행한 결과를 캡차 검증 결과라고 할 수 있으며, 이와 같은 과정을 캡차 검증 과정이라고 할 수 있다.

[0061] 트래픽 모니터링부(120)는 S308 단계에서 전달받은 검증 결과를 트래픽 제어부(110)로 전송한다(S309).

[0062] 트래픽 제어부(110)는 S309 단계에서 전달받은 검증 결과를 토대로 패킷의 송수신 즉, 트래픽을 허가(PASS) 하거나 차단(BLOCK)한다(S310).

[0063] 또한, 트래픽 모니터링부(120)는 S308 단계에서 전달받은 검증 결과를 리스트 관리부(130)로 전달하여, 리스트 관리부(130)에서 검증 결과를 업데이트하여 관리(S311)함으로써, 향후 내부망(10)의 동일한 출발지 주소를 갖는 트래픽이 동일한 외부망(20)의 동일한 목적지 주소를 갖는 트래픽을 동일하게 제어(허가 또는 차단) 할 수 있도록 한다.

[0064] 다음, 트래픽 제어 장치(100)가 복수개의 클라이언트 컴퓨터(11~13) 중 특정 클라이언트 컴퓨터 내 어플리케이션에 의해 발생하는 트래픽을 사전에 검증된 캡차 검증 결과를 포함하는 접근 제어 리스트에 따라 외부로 전송하는 방법을 도 4를 참조하여 상세하게 설명한다.

[0065] 도 4는 본 발명의 실시예에 따른 클라이언트 컴퓨터 내 어플리케이션에 의해 발생하는 트래픽을 제어하는 방법을 나타내는 흐름도이다.

[0066] 먼저, 트래픽 제어 장치(100)는 내부망(10)과 외부망(20) 사이에 위치하여, 내부망(10)과 외부망(20) 사이에서 전송되는 트래픽을 제어한다. 이를 위하여, 트래픽 제어 장치(100)는 트래픽 제어부(110), 트래픽 모니터링부(120) 및 리스트 관리부(130)를 포함한다. 여기서, 도 4의 리스트 관리부(130)는 도 3의 리스트 관리부(130)와 다르게, 접근 제어 리스트뿐만 아니라, 접근 제어 리스트 내 패킷 정보에 해당하는 통제 정책을 포함한다.

[0067] 도 4를 참고하면, 내부망(10)의 클라이언트 컴퓨터 내 어플리케이션(250)은 외부망(20)의 서버로 전송할 패킷을 트래픽 제어 장치(100)의 트래픽 제어부(110)로 전송한다(S401).

[0068] 트래픽 제어부(110)는 내부망(10)에서 외부망(20)으로 전달되는 트래픽을 보류하고, S401 단계에서 전달받은 패킷을 트래픽 모니터링부(120)로 전송한다(S402).

[0069] 트래픽 모니터링부(120)는 전달받은 패킷에 해당하는 패킷 정보를 리스트 관리부(130)로 전송한다(S403).

[0070] 리스트 관리부(130)는 사전에 저장되어 있는 접근 제어 리스트에 S303 단계에서 전달받은 패킷 정보가 존재하는지를 확인하고, 확인 결과 패킷 정보가 존재하는 경우에 패킷 정보에 해당하는 통제 정책을 트래픽 모니터링부(120)로 전송한다(S404).

[0071] 트래픽 모니터링부(120)는 S404 단계에서 전달받은 통제 정책을 트래픽 제어부(110)로 전달한다(S405).

[0072] 트래픽 제어부(110)는 S405 단계에서 전달받은 통제 정책을 토대로 패킷의 송수신 즉, 트래픽을 허가(PASS) 하거나 차단(BLOCK)한다(S406).

[0073] 다음, 트래픽 제어 장치(100)와 내부망(10)의 클라이언트 컴퓨터 내 캡차 에이전트(200)간의 캡차 메시지(예를 들어, 캡차 요청 메시지, 캡차 응답 메시지)의 송수신 과정을 도 5를 참조하여 상세하게 설명한다.

[0074] 도 5는 본 발명의 실시예에 따른 트래픽 제어 장치와 캡차 에이전트 간의 캡차 메시지 송수신 과정을 나타내는 도면이다.

[0075] 도 5를 참고하면, 캡차 에이전트(200)는 클라이언트 컴퓨터의 사용자와의 인터페이스를 담당하는 인터페이스부(210)와 트래픽 제어 장치(100)와의 통신을 수행하는 캡차 통신부(220)를 포함한다.

[0076] 트래픽 모니터링부(120)는 클라이언트 컴퓨터의 정보를 포함하는 패킷 정보를 캡차 검증부(140)로 전달한다.

[0077] 캡차 검증부(140)는 캡차 생성부(141)와 캡차 통신 하위부(142)를 포함한다.

[0078] 캡차 생성부(141)는 패킷 정보와 특정 난수값을 이용하여 악성 코드가 올바른 값을 응답할 수 없도록 새로운 캡차 값을 생성한다.

[0079] 캡차 통신 하위부(142)는 패킷 정보를 DNS 수집부(150)의 DNS 정보 검색부(151)로 전달하고, 전달한 패킷 정보에 해당하는 패킷 정보와 관련된 정보 즉, 도메인 정보 및 위치(국가) 정보를 DNS 정보 검색부(151)로부터 전달받는다. 이처럼, DNS 정보 검색부(151)는 도메인 정보를 포함하는 도메인 정보 저장부(152)와 위치(국가) 정보를 포함하는 위치 정보 저장부(153)과 연동하여 동작한다.

[0080] 다음, 캡차 통신 하위부(142)는 패킷 정보와 관련된 정보 즉, 도메인 정보 및 위치(국가) 정보를 캡차 생성부(141)로 전달한다.

[0081] 캡차 생성부(141)는 생성한 캡차 값과 패킷 정보와 관련된 정보를 포함하는 캡차 요청 메시지를 생성하고, 생성한 캡차 요청 메시지를 캡차 에이전트(200)로 전달한다.

[0082] 캡차 에이전트(200)의 캡차 통신부(220)는 캡차 요청 메시지를 수신하고, 이를 인터페이스부(210)로 전달한다.

[0083] 인터페이스부(210)는 캡차 요청 메시지에 해당하는 캡차 인증창을 클라이언트 컴퓨터의 화면에 표시하고, 사용자의 입력을 기다린다. 이때, 사용자는 해당 트래픽을 허가할지 차단할지를 선택하고, 선택한 결과 즉, 캡차 응답 메시지를 인터페이스부(210)로 전달한다. 다음, 인터페이스부(210)는 사용자의 입력에 해당하는 캡차 응답 메시지를 캡차 통신부(220)로 전달한다.

[0084] 캡차 통신부(220)는 캡차 응답 메시지를 캡차 통신 하위부(142)를 통해 트래픽 모니터링부(120)로 전달한다. 결국 사용자가 차단한 트래픽과 악성코드에 의해 응답되지 못한 트래픽은 트래픽 제어 장치(100)에 의해 차단된다.

[0085] 이와 같이, 본 발명은 사용자가 접근하기 원하는 트래픽인지 판별 가능토록 사용자에게 캡차 요청 메시지를 보내고, 캡차 요청 메시지에 대응하는 캡차 응답 메시지에 따라 해당 트래픽의 외부 연결을 허가 혹은 차단한다. 여기서, 캡차 요청 메시지와 캡차 응답 메시지 즉, 캡차 메시지는 트래픽을 발생한 주체가 실제 사람인지 아니면 악성코드인지를 구별하는 메시지에 해당한다. 캡차 메시지를 이용하여 사람은 구별 할 수 있지만, 악성코드는 구별하기 어렵게 의도적으로 왜곡한 문자나 그림 또는 음성과 같은 형태로 되어있다. 따라서, 본 발명은 캡차 응답 메시지를 축적하고, 트래픽을 제어한 결과를 학습하여 접근 제어 리스트를 생성한다.

[0086] 본 발명은 이렇게 생성한 접근 제어 리스트에 따라 해당 기관의 내부에서 외부로 접근을 시도하는 악성 코드에 의한 트래픽을 제어함으로써 자료 유출을 방지할 수 있다.

[0087] 이상에서와 같이 도면과 명세서에서 최적의 실시예가 개시되었다. 여기서 특정한 용어들이 사용되었으나, 이는 단지 본 발명을 설명하기 위한 목적에서 사용된 것이지 의미 한정이나 특허청구범위에 기재된 본 발명의 범위를 제한하기 위하여 사용된 것은 아니다. 그러므로, 본 기술 분야의 통상의 지식을 가진자라면 이로부터 다양한 변형 및 균등한 타 실시예가 가능하다는 점을 이해할 것이다. 따라서, 본 발명의 진정한 기술적 보호범위는 첨부된 특허청구범위의 기술적 사상에 의해 정해져야 할 것이다.

부호의 설명

[0088] 10; 내부망

11~13; 복수개의 클라이언트 컴퓨터

20; 외부망

21~23; 서버

30; 악성코드

100; 트래픽 제어 장치

110; 트래픽 제어부

120; 트래픽 모니터링부

130; 리스트 관리부

140; 캡차 검증부

150; DNS 수집부

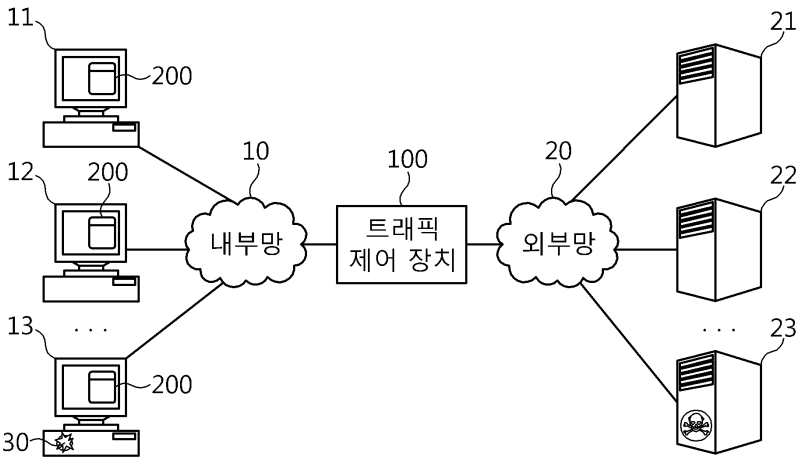
200; 캡차 에이전트

210; 인터페이스부

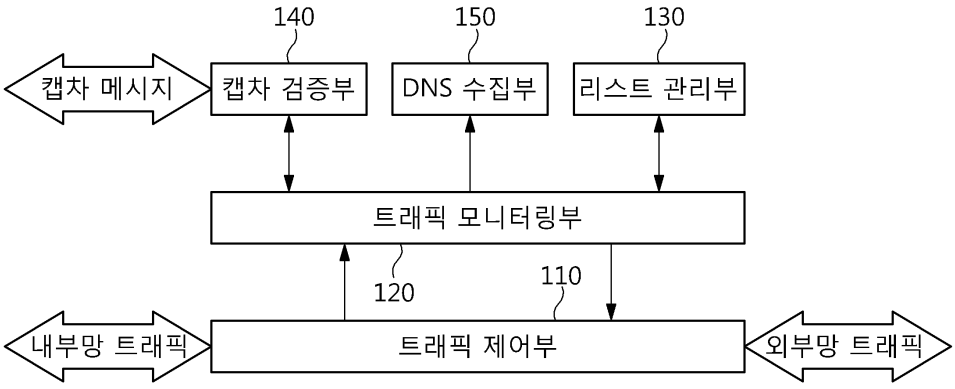
220; 캡차 통신부

도면

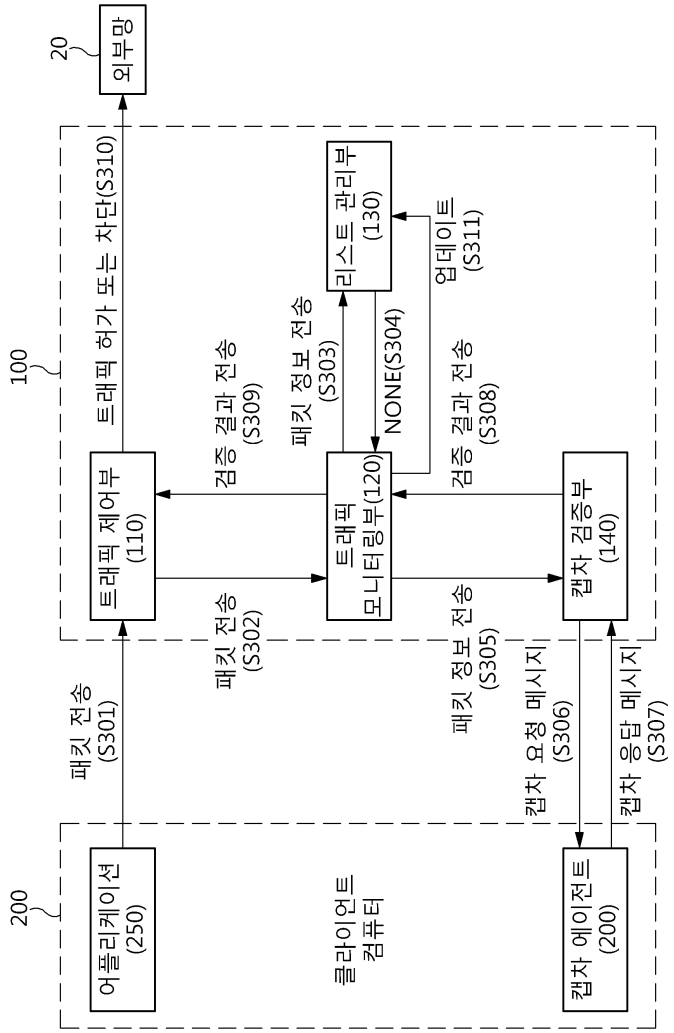
도면1



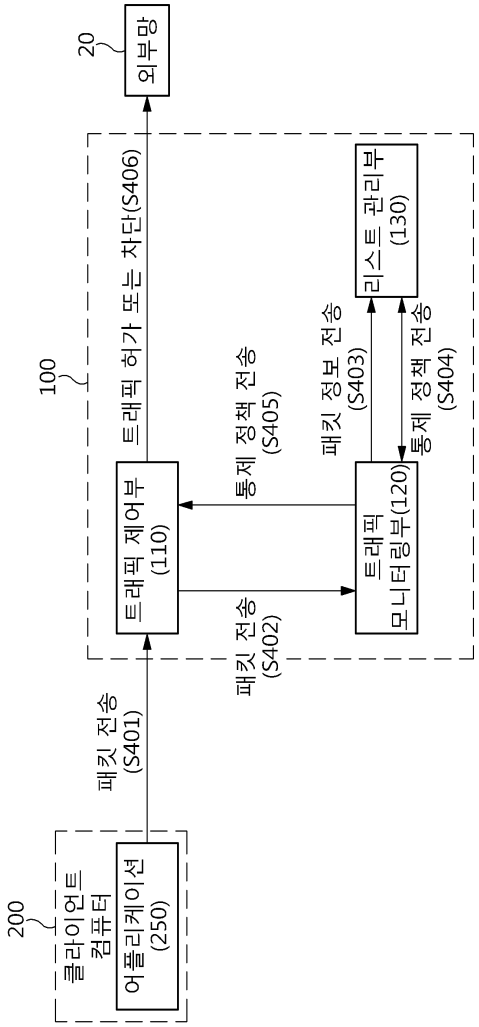
도면2



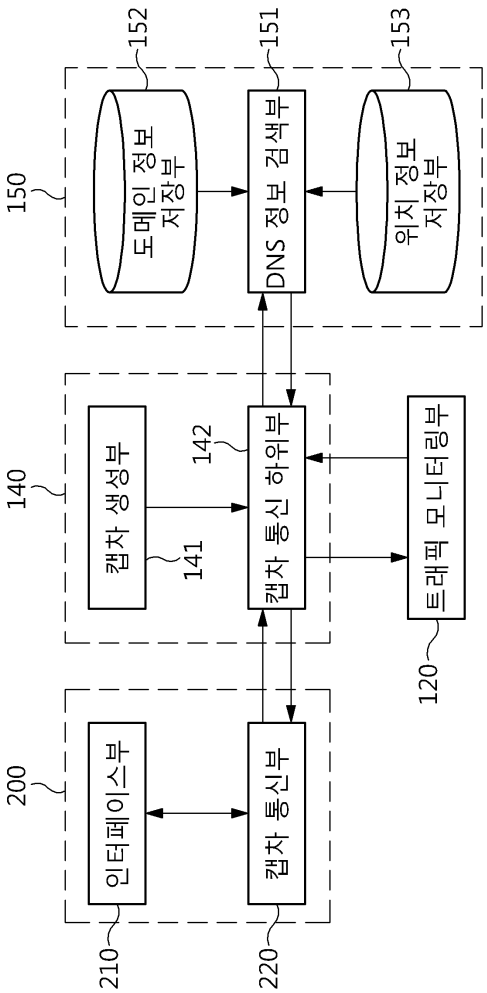
도면3


20
외부망
100
트래픽 허가 또는 차단(S310)
리스트 관리부 (130)
업데이트 (S311)
검증 결과 전송 (S309)
패킷 정보 전송 (S303)
NONE(S304)
검증 결과 전송 (S308)
트래픽 제어부 (110)
트래픽 모니터링부(120)
캡차 검증부 (140)
패킷 전송 (S302)
패킷 정보 전송 (S305)
패킷 전송 (S301)
캡차 요청 메시지 (S306)
캡차 응답 메시지 (S307)
200
어플리케이션 (250)
클라이언트 컴퓨터
캡차 에이전트 (200)

도면4


200
클라이언트 컴퓨터
어플리케이션 (250)
패킷 전송 (S401)
100
트래픽 제어부 (110)
트래픽 모니터링부(120)
패킷 전송 (S402)
통제 정책 전송 (S405)
패킷 정보 전송 (S403)
통제 정책 전송 (S404)
리스트 관리부 (130)
트래픽 허가 또는 차단(S406)
20
외부망

도면5


150
152
도메인 정보 저장부
151
DNS 정보 검색부
153
위치 정보 저장부
140
캡차 생성부
141
142
캡차 통신 하위부
트래픽 모니터링부
120
200
인터페이스부
210
캡차 통신부
220