



(19) 대한민국특허청(KR)

(12) 등록특허공보(B1)

(45) 공고일자 2015년04월10일

(11) 등록번호 10-1511474

(24) 등록일자 2015년04월06일

(51) 국제특허분류(Int. Cl.)

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

(21) 출원번호 10-2014-0069158

(22) 출원일자 2014년06월09일

심사청구일자 2014년06월09일

(56) 선행기술조사문헌

KR1020070011711 A*

KR1020090078691 A*

*는 심사관에 의하여 인용된 문헌

(73) 특허권자

플러스기술주식회사

서울특별시 강남구 바고개로1길 10, 3층(수서동, 현대벤처빌)

(72) 발명자

이용환

서울특별시 강남구 바고개로1길 10, 3층 (수서동, 현대벤처빌)

박민혁

서울특별시 강남구 바고개로1길 10, 3층 (수서동, 현대벤처빌)

(뒷면에 계속)

(74) 대리인

특허법인 무한

전체 청구항 수 : 총 11 항

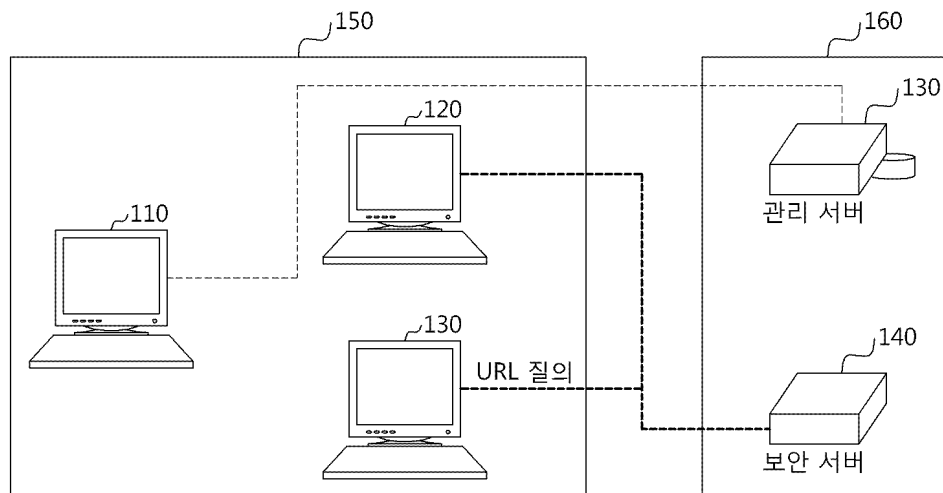
심사관 : 석상문

(54) 발명의 명칭 에이전트 프로그램을 이용한 인터넷 접속 차단 방법

(57) 요약

실시예에 따른 사용자 단말에 설치된 에이전트 프로그램을 이용하여 인터넷 접속을 차단하는 방법은, 도메인 주소 및 상기 도메인 주소에 대응하는 카테고리를 URL 관별 정보로 유지하는 단계; 상기 에이전트 프로그램을 이용하여 상기 사용자 단말에 설치된 웹 브라우저로부터의 HTTP Request 패킷을 분석하여 상기 HTTP Request 패킷의 목적지 도메인 주소를 식별하는 단계; 상기 URL 관별 정보를 이용하여 상기 HTTP Request 패킷의 목적지 도메인 주소에 대응하는 카테고리를 식별하는 단계; 및 상기 식별된 카테고리에 따라 상기 HTTP Request 패킷에 대한 인터넷 접속을 차단하는 단계를 포함할 수 있다.

대표도



(72) 발명자

임준혁

서울특별시 강남구 밤고개로1길 10, 3층 (수서동,
현대벤처빌)

강경태

서울특별시 강남구 밤고개로1길 10, 3층 (수서동,
현대벤처빌)

명세서

청구범위

청구항 1

사용자 단말에 설치된 에이전트 프로그램을 이용하여 인터넷 접속을 차단하는 방법에 있어서,

도메인 주소 및 상기 도메인 주소에 대응하는 카테고리를 URL 판별 정보로 유지하는 단계;

상기 에이전트 프로그램을 이용하여 상기 사용자 단말에 설치된 웹 브라우저로부터의 HTTP Request 패킷을 분석하여 상기 HTTP Request 패킷의 목적지 도메인 주소를 식별하는 단계;

상기 URL 판별 정보를 이용하여 상기 HTTP Request 패킷의 목적지 도메인 주소에 대응하는 카테고리를 식별하는 단계; 및

상기 식별된 카테고리에 따라 상기 HTTP Request 패킷에 대한 인터넷 접속을 차단하는 단계;

상기 카테고리에 따른 인터넷 접속 차단 여부에 관한 정책을 정책 정보로 유지하는 단계;

상기 에이전트 프로그램은 회사 코드를 포함하고, 상기 회사 코드를 이용하여 관리 서버에게 정책 정보를 요청하는 단계; 및

상기 관리 서버로부터 상기 회사 코드에 대응한 정책 정보를 수신하는 단계

를 포함하고,

상기 식별된 카테고리에 따라 상기 HTTP Request 패킷에 대한 인터넷 접속을 차단하는 단계는,

상기 정책 정보를 이용하여 상기 식별된 카테고리에 대한 인터넷 접속 차단 여부에 따라 상기 HTTP Request 패킷에 대한 인터넷 접속을 차단하는 단계

를 포함하는 인터넷 접속 차단 방법.

청구항 2

삭제

청구항 3

삭제

청구항 4

제1항에 있어서,

상기 HTTP Request 패킷에 대한 인터넷 접속을 차단하는 단계는,

상기 HTTP Request 패킷에 대한 가짜 루프백 HTTP Response 패킷을 생성하는 단계; 및

상기 가짜 루프백 HTTP Response 패킷을 상기 HTTP Request 패킷을 생성한 웹 브라우저에게 전달하는 단계

를 포함하는 인터넷 접속 차단 방법.

청구항 5

사용자 단말에 설치된 에이전트 프로그램을 이용하여 인터넷 접속을 차단하는 방법에 있어서,

도메인 주소 및 상기 도메인 주소에 대응하는 카테고리를 URL 판별 정보로 유지하는 단계;

상기 에이전트 프로그램을 이용하여 상기 사용자 단말에 설치된 웹 브라우저로부터의 HTTP Request 패킷을 분석하여 상기 HTTP Request 패킷의 목적지 도메인 주소를 식별하는 단계;

상기 URL 판별 정보를 이용하여 상기 HTTP Request 패킷의 목적지 도메인 주소에 대응하는 카테고리를 식별하는

단계;

상기 식별된 카테고리에 따라 상기 HTTP Request 패킷에 대한 인터넷 접속을 차단하는 단계;

상기 사용자 단말로부터의 DNS 요청 패킷을 분석하여 쿼리 도메인 주소를 식별하는 단계;

상기 쿼리 도메인 주소가 상기 URL 판별 정보에 포함되어 있는지 판단하는 단계;

상기 쿼리 도메인 주소가 상기 URL 판별 정보에 포함되어 있지 않은 경우, 상기 쿼리 도메인 주소를 보안 서버로 송신하는 단계;

상기 보안 서버로부터 상기 쿼리 도메인 주소에 대응하는 카테고리를 수신하는 단계; 및

상기 쿼리 도메인 주소 및 상기 쿼리 도메인 주소에 대응하는 카테고리를 상기 URL 판별 정보에 저장하는 단계를 포함하는 인터넷 접속 차단 방법.

청구항 6

제5항에 있어서,

상기 사용자 단말로부터의 최근 N개의 DNS 요청 패킷에 대응하는 도메인 주소 및 상기 도메인 주소에 대응하는 카테고리를 상기 URL 판별 정보에 유지하고, 나머지 도메인 주소 및 카테고리는 상기 URL 판별 정보로부터 삭제하는 단계

를 더 포함하는 인터넷 접속 차단 방법.

청구항 7

사용자 단말에 설치된 에이전트 프로그램을 이용하여 인터넷 접속을 차단하는 방법에 있어서,

IP 주소 및 상기 IP 주소에 대응하는 카테고리를 URL 판별 정보로 유지하는 단계;

상기 에이전트 프로그램을 이용하여 상기 사용자 단말에 설치된 애플리케이션으로부터의 TCP 패킷을 분석하는 단계;

상기 TCP 패킷의 ACK 필드 및 PSH 필드가 세트되어 있는지 판단하는 단계;

상기 TCP 패킷의 ACK 필드 및 PSH 필드가 세트되어 있는 경우, 상기 TCP 패킷의 목적지 IP 주소를 식별하는 단계;

상기 URL 판별 정보를 이용하여 상기 TCP 패킷의 목적지 IP 주소에 대응하는 카테고리를 식별하는 단계; 및

상기 식별된 카테고리에 따라 상기 TCP 패킷에 대한 인터넷 접속을 차단하는 단계

를 포함하는 인터넷 접속 차단 방법.

청구항 8

제7항에 있어서,

상기 카테고리에 따른 인터넷 접속 차단 여부에 관한 정책을 정책 정보로 유지하는 단계

를 더 포함하고,

상기 식별된 카테고리에 따라 상기 TCP 패킷에 대한 인터넷 접속을 차단하는 단계는,

상기 정책 정보를 이용하여 상기 식별된 카테고리에 대한 인터넷 접속 차단 여부에 따라 상기 TCP 패킷에 대한 인터넷 접속을 차단하는 단계

를 포함하는 인터넷 접속 차단 방법.

청구항 9

제8항에 있어서,

상기 에이전트 프로그램은 회사 코드를 포함하고, 상기 회사 코드를 이용하여 관리 서버에게 정책 정보를 요청

하는 단계; 및

상기 관리 서버로부터 상기 회사 코드에 대응한 정책 정보를 수신하는 단계를 포함하는 인터넷 접속 차단 방법.

청구항 10

제8항에 있어서,

상기 TCP 패킷에 대한 인터넷 접속을 차단하는 단계는,

상기 TCP 패킷에 대한 가짜 루프백 TCP 응답 패킷을 생성하는 단계; 및

상기 가짜 루프백 TCP 응답 패킷을 상기 TCP 패킷을 생성한 애플리케이션에게 전달하는 단계를 포함하는 인터넷 접속 차단 방법.

청구항 11

제7항에 있어서,

상기 TCP 패킷의 SYN 필드가 세트되어 있는지 판단하는 단계;

상기 TCP 패킷의 SYN 필드가 세트되어 있는 경우, 상기 TCP 패킷의 목적지 IP 주소를 식별하는 단계;

상기 목적지 IP 주소가 상기 URL 판별 정보에 포함되어 있는지 판단하는 단계;

상기 목적지 IP 주소가 상기 URL 판별 정보에 포함되어 있지 않은 경우, 상기 목적지 IP 주소를 보안 서버로 송신하는 단계;

상기 보안 서버로부터 상기 목적지 IP 주소에 대응하는 카테고리를 수신하는 단계; 및

상기 목적지 IP 주소 및 상기 목적지 IP 주소에 대응하는 카테고리를 상기 URL 판별 정보에 저장하는 단계를 더 포함하는 인터넷 접속 차단 방법.

청구항 12

제7항에 있어서,

상기 TCP 패킷의 목적지 IP 주소를 식별하는 단계는,

상기 TCP 패킷이 포함된 IP 패킷으로부터 상기 목적지 IP 주소를 식별하는 단계를 포함하는 인터넷 접속 차단 방법.

청구항 13

제1항 및 제4항 내지 제12항 중 어느 한 항의 방법을 실행하는 컴퓨터 판독 가능한 프로그램을 기록한 컴퓨터 판독 가능 기록매체.

발명의 설명

기술 분야

[0001] 아래의 설명은 인터넷 접속을 차단하는 방법에 관한 것으로, 유해 사이트의 접근을 차단하는 기술에 관한 것이다.

배경 기술

[0002] 웹 사이트를 통해 악성코드에 감염되는 경우가 해마다 증가하고 있으며, 인터넷을 통한 개인정보 유출 등의 이슈가 크게 대두되고 있다. 방화벽이나 유해사이트 차단 시스템 등이 URL 기반의 사이트 접속 통제가 어렵다는 점을 악용하여 HTTPS기반의 우회접속 서비스들이 우후죽순 생겨나고 있다.

[0003] 한국공개특허 제2012-0070403호는 접속 네트워크에 상관없이 사용자 환경에 맞게 적응적으로 사용자 단말에 설

치되어 동작하는 웹 에이전트 기반으로 시스템 로그를 분석하고 유해 사이트 리스트를 관리하여 웹브라우저 액션을 탐지하고 유해 사이트의 접근을 차단하는 방법을 제안하고 있다. 하지만, 상기 발명은 접속을 시도하는 URL을 입력함으로써 유해 사이트를 추가할 뿐 목적지 IP 주소에 대한 카테고리를 이용하여 인터넷 접속을 차단하는 방법은 제안하지 못하고 있다. 이에 따라, 에이전트 프로그램을 통해서 요청 패킷에 대하여 카테고리에 따른 URL관별 정보를 식별하고 차단 패킷에 대하여 가짜 루프백을 전송함으로써 효율적으로 인터넷 접속을 차단하는 방법이 필요하다.

발명의 내용

해결하려는 과제

[0004] 일 실시예에 따른 에이전트 프로그램을 이용하여 인터넷 접속을 차단하는 방법을 제공할 수 있다.

과제의 해결 수단

[0005] 일 실시예에 따른 사용자 단말에 설치된 에이전트 프로그램을 이용하여 인터넷 접속을 차단하는 방법은, 도메인 주소 및 상기 도메인 주소에 대응하는 카테고리를 URL 관별 정보로 유지하는 단계; 상기 에이전트 프로그램을 이용하여 상기 사용자 단말에 설치된 웹 브라우저로부터의 HTTP Request 패킷을 분석하여 상기 HTTP Request 패킷의 목적지 도메인 주소를 식별하는 단계; 상기 URL 관별 정보를 이용하여 상기 HTTP Request 패킷의 목적지 도메인 주소에 대응하는 카테고리를 식별하는 단계; 및 상기 식별된 카테고리에 따라 상기 HTTP Request 패킷에 대한 인터넷 접속을 차단하는 단계를 포함할 수 있다.

[0006] 일측에 따르면, 인터넷 접속을 차단하는 방법은, 상기 카테고리에 따른 인터넷 접속 차단 여부에 관한 정책을 정책 정보로 유지하는 단계를 더 포함하고, 상기 식별된 카테고리에 따라 상기 HTTP Request 패킷에 대한 인터넷 접속을 차단하는 단계는, 상기 정책 정보를 이용하여 상기 식별된 카테고리에 대한 인터넷 접속 차단 여부에 따라 상기 HTTP Request 패킷에 대한 인터넷 접속을 차단하는 단계를 포함할 수 있다.

[0007] 또 다른 일측에 따르면, 상기 에이전트 프로그램은 회사 코드를 포함하고, 상기 회사 코드를 이용하여 관리 서버에게 정책 정보를 요청하는 단계; 및 상기 관리 서버로부터 상기 회사 코드에 대응한 정책 정보를 수신하는 단계를 포함할 수 있다.

[0008] 또 다른 일측에 따르면, 상기 HTTP Request 패킷에 대한 인터넷 접속을 차단하는 단계는, 상기 HTTP Request 패킷에 대한 가짜 루프백 HTTP Response 패킷을 생성하는 단계; 및 상기 가짜 루프백 HTTP Response 패킷을 상기 HTTP Request 패킷을 생성한 웹 브라우저에게 전달하는 단계를 포함할 수 있다.

[0009] 또 다른 일측에 따르면, 상기 사용자 단말로부터의 DNS 요청 패킷을 분석하여 쿼리 도메인 주소를 식별하는 단계; 상기 쿼리 도메인 주소가 상기 URL 관별 정보에 포함되어 있는지 판단하는 단계; 상기 쿼리 도메인 주소가 상기 URL 관별 정보에 포함되어 있지 않은 경우, 상기 쿼리 도메인 주소를 보안 서버로 송신하는 단계; 상기 보안 서버로부터 상기 쿼리 도메인 주소에 대응하는 카테고리를 수신하는 단계; 및 상기 쿼리 도메인 주소 및 상기 쿼리 도메인 주소에 대응하는 카테고리를 상기 URL 관별 정보에 저장하는 단계를 더 포함할 수 있다.

[0010] 또 다른 일측에 따르면, 인터넷 접속을 차단하는 방법은, 상기 사용자 단말로부터의 최근 N개의 DNS 요청 패킷에 대응하는 도메인 주소 및 상기 도메인 주소에 대응하는 카테고리를 상기 URL 관별 정보에 유지하고, 나머지 도메인 주소 및 카테고리는 상기 URL 관별 정보로부터 삭제하는 단계를 더 포함할 수 있다.

[0011] 일 실시예에 따른 사용자 단말에 설치된 에이전트 프로그램을 이용하여 인터넷 접속을 차단하는 방법은, IP 주소 및 상기 IP 주소에 대응하는 카테고리를 URL 관별 정보로 유지하는 단계; 상기 에이전트 프로그램을 이용하여 상기 사용자 단말에 설치된 애플리케이션으로부터의 TCP 패킷을 분석하는 단계; 상기 TCP 패킷의 ACK 필드 및 PSH 필드가 세트되어 있는지 판단하는 단계; 상기 TCP 패킷의 ACK 필드 및 PSH 필드가 세트되어 있는 경우, 상기 TCP 패킷의 목적지 IP 주소를 식별하는 단계; 상기 URL 관별 정보를 이용하여 상기 TCP 패킷의 목적지 IP 주소에 대응하는 카테고리를 식별하는 단계; 및 상기 식별된 카테고리에 따라 상기 TCP 패킷에 대한 인터넷 접속을 차단하는 단계를 포함할 수 있다.

[0012] 일측에 따르면, 인터넷 접속을 차단하는 방법은, 상기 카테고리에 따른 인터넷 접속 차단 여부에 관한 정책을 정책 정보로 유지하는 단계를 더 포함하고, 상기 식별된 카테고리에 따라 상기 TCP 패킷에 대한 인터넷 접속을 차단하는 단계는, 상기 정책 정보를 이용하여 상기 식별된 카테고리에 대한 인터넷 접속 차단 여부에 따라 상기

TCP 패킷에 대한 인터넷 접속을 차단하는 단계를 포함할 수 있다.

[0013] 또 다른 일측에 따르면, 인터넷 접속을 차단하는 방법은, 상기 에이전트 프로그램은 회사 코드를 포함하고, 상기 회사 코드를 이용하여 관리 서버에게 정책 정보를 요청하는 단계; 및 상기 관리 서버로부터 상기 회사 코드에 대응한 정책 정보를 수신하는 단계를 포함할 수 있다.

[0014] 또 다른 일측에 따르면, 상기 TCP 패킷에 대한 인터넷 접속을 차단하는 단계는, 상기 TCP 패킷에 대한 가짜 루프백 TCP 응답 패킷을 생성하는 단계; 및 상기 가짜 루프백 TCP 응답 패킷을 상기 TCP 패킷을 생성한 애플리케이션에게 전달하는 단계를 포함할 수 있다.

[0015] 또 다른 일측에 따르면, 인터넷 접속을 차단하는 방법은, 상기 TCP 패킷의 SYN 필드가 세트되어 있는지 판단하는 단계; 상기 TCP 패킷의 SYN 필드가 세트되어 있는 경우, 상기 TCP 패킷의 목적지 IP 주소를 식별하는 단계; 상기 목적지 IP 주소가 상기 URL 판별 정보에 포함되어 있는지 판단하는 단계; 상기 목적지 IP 주소가 상기 URL 판별 정보에 포함되어 있지 않은 경우, 상기 목적지 IP 주소를 보안 서버로 송신하는 단계; 상기 보안 서버로부터 상기 목적지 IP 주소에 대응하는 카테고리를 수신하는 단계; 및 상기 목적지 IP 주소 및 상기 목적지 IP 주소에 대응하는 카테고리를 상기 URL 판별 정보에 저장하는 단계를 더 포함할 수 있다.

[0016] 또 다른 일측에 따르면, 상기 TCP 패킷의 목적지 IP 주소를 식별하는 단계는, 상기 TCP 패킷이 포함된 IP 패킷으로부터 상기 목적지 IP 주소를 식별하는 단계를 포함할 수 있다.

발명의 효과

[0017] 일 실시예에 따른 인터넷 접속 차단 장치는 도메인 주소 및 도메인 주소에 대응하는 카테고리를 URL 판별 정보로 유지함으로써 카테고리에 따른 인터넷 접속 차단 여부에 따라 인터넷 접속 사이트를 차단할 수 있다. 또한, 목적지 IP 주소 및 목적지 IP 주소에 대응하는 카테고리를 URL 판별 정보로 유지함으로써, 카테고리에 따른 인터넷 접속 차단 여부에 따라 애플리케이션을 차단할 수 있다.

도면의 간단한 설명

[0018] 도 1은 일 실시예에 따른 사용자 단말에 에이전트 프로그램을 이용하여 인터넷 접속을 차단하는 동작을 나타낸 도면이다.

도 2는 일 실시예에 따른 HTTP 요청에 대하여 인터넷 접속을 차단하는 동작을 나타낸 도면이다.

도 3은 일 실시예에 따른 TCP 요청에 대하여 인터넷 접속을 차단하는 동작을 나타낸 도면이다.

도 4는 일 실시예에 따른 에이전트 프로그램을 이용하여 인터넷 접속을 차단하는 방법을 나타낸 흐름도이다.

도 5는 일 실시예에 따른 에이전트 프로그램을 이용하여 인터넷 접속을 차단하는 방법을 나타낸 흐름도이다.

도 6은 일 실시예에 따른 보안 서버의 URL 판별 정보를 유지하는 방법을 나타낸 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0019] 이하, 실시예를 첨부한 도면을 참조하여 상세히 설명한다.

[0020] 도 1은 일 실시예에 따른 사용자 단말에 에이전트 프로그램을 이용하여 인터넷 접속을 차단하는 동작을 나타낸 도면이다.

[0021] 도 1은 사용자 단말(예를 들면, PC)(110, 120, 130)에서 에이전트 프로그램을 이용하여 인터넷 접속 사이트를 판별하는 방법에 대해서 설명하기 위한 것으로, 단말(110, 120, 130)에 에이전트 프로그램이 설치될 수 있다. 에이전트 프로그램은 사용자 단말(110, 120, 130)에 설치되어 인터넷 접속 사이트를 감시할 수 있고, 인터넷 접속 사이트를 차단할 수 있다.

[0022] 고객사(150)는 ISP(Internet Service Provider)(160)에 의하여 차단하고자 하는 인터넷 사이트 접속을 차단할 수 있다. 예를 들면, 고객사(150)의 단말에는 에이전트 프로그램이 설치될 수 있으며, IPS(160)에는 정책을 관리하는 관리 서버(130) 및 URL 판별 정보를 저장하고, 저장된 URL 판별 정보를 이용하여 에이전트 프로그램으로부터 요청된 질의에 대하여 응답하는 보안 서버(140)를 포함할 수 있다.

[0023] 에이전트 프로그램은 관리 서버(130)에 의하여 정책을 수신할 수 있다. 예를 들면, 관리자가 관리자 PC(110)를 통하여 관리 서버(130)에 정책을 입력할 수 있고, 직원 PC(120, 130)는 회사 코드를 입력함으로써 관리자가 입

력한 정책을 수신할 수 있다. 이때, 정책을 입력할 때, 관리자 PC(110)를 통하여 정책을 입력할 수 있고, 정책 입력이 가능한 해당 PC를 설정하여 해당 PC를 통해서 정책을 입력할 수 있다. 예를 들면, 해당 PC에 PC용 UI를 통해서 정책을 입력할 수 있다.

[0024] 예를 들면, 관리자 PC(110)는 게임 사이트 및 성인 사이트를 차단하기 위하여 관리 서버(130)에 "게임 사이트 및 성인 사이트를 차단"하는 정책을 입력시킬 수 있다. 직원 PC(120, 130)에 회사 코드(예를 들면, 0000)를 입력할 수 있고, 관리 서버(130)로부터 "게임 사이트 및 성인 사이트를 차단"이라는 정책을 수신할 수 있다.

[0025] 보안 서버(140)는 사용자 단말로부터 DNS 요청 패킷을 분석하여 쿼리 도메인 주소를 식별할 수 있다. 예를 들면, 클라이언트가 www.game.com에 접속하기 위하여 www.game.com이라는 도메인 주소를 입력할 경우, DNS 서버로부터 www.game.com에 매치되는 IP주소를 추출할 수 있고, 도메인 주소 및 도메인 주소에 따른 IP주소를 식별할 수 있다. www.game.com에 대한 IP주소가 123.123.123.123이라면, DNS 쿼리 헤더의 쿼리 필드에 www.game.com이 입력될 수 있고, 도메인 네임에 대한 IP주소는 answer필드에서 123.123.123.123이라는 IP주소 값을 받을 수 있다.

[0026] 사용자 단말은 보안 서버(140)에 www.game.com이라는 도메인 주소를 송신할 수 있고, 보안 서버(140)는 송신된 도메인 주소인 www.game.com이라는 도메인 주소 및 도메인 주소에 대한 카테고리를 사용자 단말에 전송할 수 있다.

[0027] 보안 서버(140)는 쿼리 도메인 주소가 URL 판별 정보에 포함되어 있는지 판단할 수 있다. 예를 들면, 쿼리 도메인 주소가 www.game.com이라면, 보안 서버(140)는 URL 판별 정보에 www.game.com이 이미 저장되어 있는지 판단할 수 있다. 쿼리 도메인 주소가 URL 판별 정보에 포함되어 있지 않은 경우, 사용자 단말은 쿼리 도메인 주소를 보안 서버로 송신할 수 있다.

[0028] 사용자 단말은 보안 서버로부터 쿼리 도메인 주소에 대응하는 카테고리를 수신할 수 있다. 예를 들면, 보안 서버는 www.game.com에 대한 카테고리를 클라이언트에 전송할 수 있으며, 클라이언트는 "www.game.com, 게임"이라는 쿼리 도메인 주소 및 쿼리 도메인 주소에 대응하는 카테고리를 수신할 수 있다.

[0029] 보안 서버(140)는 상기 쿼리 도메인 주소 및 쿼리 도메인 주소에 대응하는 카테고리를 URL 판별 정보에 저장할 수 있다. 예를 들면, URL 판별 정보는 도메인 주소 및 도메인 주소에 대응하는 카테고리를 포함할 수 있으며, www.ggg.com, www.aaa.com등의 성인 사이트는 게임으로 분류하고, www.game.com, www.def.com 과 같이 게임 사이트는 게임으로 분류하여 저장할 수 있다.

[0030] 에이전트 프로그램을 이용하여 사용자 단말에 설치된 웹 브라우저로부터의 HTTP Request 패킷을 분석하여 HTTP Request 패킷의 목적지 도메인 주소를 식별할 수 있다. URL 판별 정보를 이용하여 HTTP Request 패킷의 목적지 도메인 주소에 대응하는 카테고리를 식별할 수 있다. 식별된 카테고리에 따라 HTTP Request 패킷에 대한 인터넷 접속을 차단할 수 있다. 예를 들면, HTTP Request 패킷의 도메인 주소가 www.game.com이라면 차단 대상이므로, 가짜 루프백 HTTP Request 패킷을 생성하고, 생성한 가짜 루프백 HTTP Request 패킷을 HTTP Request 패킷을 생성한 웹 브라우저에게 전달할 수 있다.

[0031] 또한, 예를 들면, 관리자 PC(110)는 메신저 애플리케이션을 차단하기 위하여 관리 서버(130)에 "메신저 차단"하는 정책을 입력시킬 수 있다. 직원 PC(120, 130)에 회사 코드(예를 들면, 0000)를 입력할 수 있고, 관리 서버(130)로부터 "메신저 차단"이라는 정책을 수신할 수 있다.

[0032] 직원 PC 1(120)는 TCP 패킷의 SYN 필드가 세트되어 있는지 판단할 수 있다. TCP 패킷의 SYN 필드가 세트되어 있는 경우, TCP 패킷의 목적지 IP 주소를 식별할 수 있다. 보안 서버(140)는 목적지 IP 주소가 URL 판별 정보에 포함되어 있는지 판단할 수 있다. 예를 들면, 목적지 IP 주소가 111.111.111.111이라면, 보안 서버는 URL 판별 정보에 111.111.111.111이 이미 저장되어 있는지 판단할 수 있다.

[0033] 목적지 IP 주소가 URL 판별 정보에 포함되어 있지 않은 경우, 직원 PC 1(120)은 보안 서버(140)로 목적지 IP 주소를 송신할 수 있다. 예를 들면, 클라이언트가 MSN Messenger에 접속한다면, TCP 패킷의 SYN 필드가 세트되어 있는지 판단한 후, TCP 패킷의 목적지 IP 주소를 식별할 수 있다. 예를 들면, MSN Messenger의 IP주소가 111.111.111.111을 식별할 수 있다. 클라이언트는 보안 서버(140)에 111.111.111.111이라는 목적지 IP 주소를 송신할 수 있고, 보안 서버(140)는 송신된 목적지 주소인 111.111.111.111이라는 목적지 IP 주소 및 목적지 IP 주소에 대한 카테고리를 클라이언트에 전송할 수 있다. 직원 PC1(120)은 보안 서버(140)로부터 쿼리 도메인 주소에 대응하는 카테고리를 수신할 수 있다. 예를 들면, 보안 서버는 111.111.111.111에 대한 카테고리를 클라이언트에 전송할 수 있으며, 클라이언트는 "111.111.111.111, 메신저"라는 목적지 IP 주소 및 목적지 IP 주소에

대응하는 카테고리를 수신할 수 있다.

- [0034] 보안 서버(140)는 IP 주소 및 IP 주소에 대응하는 카테고리를 URL 판별 정보에 저장할 수 있다. 예를 들면, URL 판별 정보는 IP 주소 및 IP 주소에 대응하는 카테고리를 포함할 수 있으며, 100.100.100.111, 111.1111.111.111 은 메신저 애플리케이션이므로 메신저로 분류하여 저장할 수 있다.
- [0035] 에이전트 프로그램을 이용하여 사용자 단말에 설치된 애플리케이션으로부터의 TCP 패킷을 분석할 수 있다. TCP 패킷의 ACK 필드 및 PSH 필드가 세트되어 있는 경우, TCP 패킷의 목적지 IP 주소를 식별할 수 있다. 식별된 카테고리에 따라 TCP 패킷에 대한 인터넷 접속을 차단할 수 있다. 예를 들면 TCP 패킷의 목적지 IP 주소가 100.100.100.111이라면, 상기 TCP패킷은 차단 대상이므로 가짜 루프백 TCP 응답 패킷을 생성하고, 가짜 루프백 TCP 응답 패킷을 TCP 패킷을 생성한 애플리케이션에게 전달할 수 있다.
- [0036] 도 2는 일 실시예에 따른 HTTP 요청에 대하여 인터넷 접속을 차단하는 동작을 나타낸 도면이다.
- [0037] 도 2는 클라이언트가 www.google.com에 접속한다고 가정한다. 클라이언트(220)는 예를 들면, PC와 같은 단말기일 수 있으며, 클라이언트 PC에 에이전트 프로그램이 설치될 수 있고, 에이전트 프로그램에 카테고리에 따른 인터넷 접속 차단 여부에 관한 정책이 적용되어 있을 수 있다. 예를 들면, "인터넷 포털 사이트를 차단하시오"가 정책일 수 있다.
- [0038] 클라이언트(220)가 윈도우 브라우저를 통하여 www.google.com이라는 도메인 주소를 입력함으로써 google(210)에 접속할 수 있고, DNS 서버는 도메인 주소인 www.google.com에 따른 IP주소를 추출할 수 있다. 예를 들면, DNS 서버는 www.google.com에 따른 IP 주소인 121.123.012.221를 추출하여 클라이언트(220)에게 전송할 수 있다.
- [0039] 클라이언트(220)는 보안 서버(230)에 URL 질의(207)를 할 수 있고, 보안 서버(230)는 URL 질의 결과(208)를 클라이언트(220)에 전송할 수 있다. 클라이언트(220)는 www.google.com이라는 도메인 주소를 보안 서버에 전송할 수 있고, 보안 서버(230)는 전송된 도메인 주소인 www.google.com에 대한 카테고리, 예를 들면, 포털 사이트를 클라이언트(220)에게 전송할 수 있다. 예를 들면, 보안 서버(230)는 URL 질의 결과 값인 www.google.com, 포털 사이트를 클라이언트(220)에 전송할 수 있다.
- [0040] 이때, 3way-handshaking이 이루어질 수 있다. 클라이언트로부터 google로 패킷의 SYN 플래그를 셋팅하여 전송할 수 있고(203), SYN+ACK 응답을 클라이언트가 수신하면, 패킷의 ACK필드를 google에 전송함으로써 세션이 연결될 수 있다(204).
- [0041] URL 캐시는 클라이언트로부터 최근 N개의 DNS 요청 패킷에 대응하는 도메인 주소 및 도메인 주소에 대응하는 카테고리를 URL 판별 정보에 유지하고, 나머지 도메인 주소 및 카테고리를 URL 판별 정보로부터 삭제할 수 있다(209). 예를 들면, 보안 서버에 도메인 주소 및 도메인 주소에 따른 카테고리가 이미 저장되어 있다면, 클라이언트는 URL 캐시에 URL 판별 정보가 저장되어 있기 때문에 보안 서버에 도메인 주소를 전송하지 않아도 된다.
- [0042] 클라이언트(220)는 URL 판별 정보를 이용하여 HTTP Request 패킷의 목적지 도메인 주소에 대응하는 카테고리를 식별할 수 있다. 예를 들면, www.google.com의 IP 주소인 121.123.012.221의 카테고리가 포털 사이트임이 식별될 수 있다. 정책이 포털 사이트를 차단하는 것이므로, 식별된 카테고리에 따라 HTTP Request 패킷에 대한 인터넷 접속을 차단할 수 있다. HTTP Request 패킷(205)에 대한 가짜 루프백 HTTP Request 패킷을 생성하고(210), 가짜 루프백 HTTP Response 패킷(206)을 HTTP Request 패킷을 생성한 google(210)에 전달함으로써 인터넷 접속을 차단할 수 있다.
- [0043] 도 3은 일 실시예에 따른 TCP 요청에 대하여 인터넷 접속을 차단하는 동작을 나타낸 도면이다.
- [0044] 도 3은 클라이언트(320)가 애플리케이션(예를 들면, MSN messenger)(310)에 접속한다고 가정한다. 클라이언트(320)는 예를 들면, PC와 같은 단말기일 수 있으며, 클라이언트 PC에 에이전트 프로그램이 설치될 수 있고, 에이전트 프로그램에 카테고리에 따른 인터넷 접속 차단 여부에 관한 정책이 적용되어 있을 수 있다. 예를 들면, "메신저를 차단하시오."가 정책일 수 있다.
- [0045] 클라이언트(320)가 윈도우를 통하여 MSN messenger를 입력함으로써 MSN(310)에 접속할 수 있고, 이때, 3way-handshaking이 이루어질 수 있다. 클라이언트로부터 MSN(310)으로 패킷의 SYN 플래그를 셋팅하여 전송할 수 있고(301), SYN+ACK 응답을 클라이언트가 수신하면, 패킷의 ACK필드를 MSN에 전송함으로써 세션이 연결될 수 있다(302). TCP 패킷의 SYN 필드가 세트되었는지 판단할 수 있다. TCP 패킷의 SYN 필드가 세트되어 있는 경우, TCP 패킷의 목적지 IP주소를 식별할 수 있다. 예를 들면, 목적지 IP 주소인 100.100.111.111일 수가 있다.

- [0046] 클라이언트(320)는 보안 서버(330)에 URL 질의(305)를 할 수 있고, 보안 서버(330)는 URL 질의 결과(306)를 클라이언트(320)에 전송할 수 있다. 클라이언트(320)는 100.100.111.111 이라는 목적지 IP 주소를 보안 서버에 전송할 수 있고, 보안 서버(330)는 전송된 목적지 IP 주소인 100.100.111.111 에 대한 카테고리, 예를 들면, 메시지를 클라이언트(320)에게 전송할 수 있다. 예를 들면, 보안 서버(230)는 URL 질의 결과 값인 "100.100.111.111, 메시지"를 클라이언트(320)에 전송할 수 있다.
- [0047] URL 캐시는 클라이언트(320)로부터 최근 N개의TCP 패킷에 대응하는 목적지 IP 주소 및 목적지 IP 주소에 대응하는 카테고리를 URL 판별 정보에 유지하고, 나머지 목적지 IP 주소 및 카테고리를 URL 판별 정보로부터 삭제할 수 있다(308). 예를 들면, 이미 접속하려고 했던 애플리케이션이라면, 에이전트 프로그램의 URL 캐시에 URL 판별 정보가 저장되어 있기 때문에 보안 서버에 목적지 IP 주소를 전송하지 않고, URL 캐시에 저장된 URL 판별 정보를 이용하여 목적지 IP주소에 따른 카테고리를 식별할 수 있다.
- [0048] 에이전트 프로그램을 이용하여 사용자 단말에 설치된 애플리케이션으로부터의 TCP 패킷을 분석할 수 있다. 이때, TCP 패킷의 ACK 필드 및 PSH 필드가 세트되어 있는지 판단할 수 있다(303). TCP 패킷의 ACK 필드 및 PSH 필드가 세트되어 있는 경우, TCP 패킷의 목적지 IP 주소를 식별할 수 있다. URL 판별 정보를 이용하여 TCP 패킷의 목적지 IP 주소에 대응하는 카테고리를 식별할 수 있다. 예를 들면, MSN 목적지 IP주소의 100.100.111.111 카테고리가 메시지가 식별될 수 있다. 정책이 메시지를 차단하는 것이므로, 식별된 카테고리에 따라 TCP 패킷에 대한 인터넷 접속을 차단할 수 있다. TCP 패킷에 대한 가짜 루프백 TCP 응답 패킷을 생성하고(303), 가짜 루프백 TCP 응답 패킷(308)을 TCP 패킷을 생성한MSN(310)에 전달함으로써 인터넷 접속을 차단할 수 있다(304).
- [0049] 도 4는 일 실시예에 따른 에이전트 프로그램을 이용하여 인터넷 접속을 차단하는 방법을 나타낸 흐름도이다.
- [0050] 사용자 단말에 에이전트 프로그램이 설치될 수 있으며, 에이전트 프로그램은 회사 코드를 포함하고, 회사 코드를 이용하여 관리 서버에게 정책 정보를 요청할 수 있다. 관리 서버로부터 회사 코드에 대응한 정책 정보를 수신할 수 있다.
- [0051] 단계(411)에서 인터넷 접속 차단 장치는 도메인 주소 및 도메인 주소에 대응하는 카테고리를 URL 판별 정보로 유지할 수 있다. 예를 들면, 인터넷 접속 차단 장치는 www.bcd.com라는 도메인 주소 및 www.bcd.com에 대한 카테고리인 포털 사이트를 URL 판별 정보로 유지할 수 있고, www.def.com라는 도메인 주소 및 www.def.com에 대한 카테고리인 포털 사이트를 URL 판별 정보로 유지할 수 있다.
- [0052] 단계(412)에서 인터넷 접속 차단 장치는 카테고리에 따른 인터넷 접속 차단 여부에 관한 정책을 정책 정보로 유지할 수 있다. 예를 들면, 인터넷 접속 차단 장치는 "게임 사이트에 대해서 차단하시오"라는 정책을 정책 정보로 유지할 수 있다.
- [0053] 단계(413)에서 인터넷 접속 차단 장치는 사용자 단말로부터 DNS 요청 패킷을 분석하여 쿼리 도메인 주소를 식별할 수 있다.
- [0054] 단계(414)에서 인터넷 접속 차단 장치는 쿼리 도메인 주소가 URL 판별 정보에 포함되어 있는지 판단할 수 있다. 예를 들면, 쿼리 도메인 주소가 www.abc.com이라면, 인터넷 접속 차단 장치는 URL 판별 정보에 www.abc.com 및 www.abc.com에 대한 카테고리가 포함되어 있는지 판단할 수 있다.
- [0055] 단계(415)에서 인터넷 접속 차단 장치는 쿼리 도메인 주소가 URL 판별 정보에 포함되어 있지 않은 경우, 쿼리 도메인 주소를 보안 서버로 송신할 수 있다. 예를 들면, 쿼리 도메인 주소가 www.abc.com이 URL 판별 정보에 포함되어 있지 않은 경우, 쿼리 도메인 주소인 www.abc.com를 보안 서버에 송신할 수 있다.
- [0056] 단계(416)에서 인터넷 접속 차단 장치는 보안 서버로부터 쿼리 도메인 주소에 대응하는 카테고리를 수신할 수 있다. 예를 들면, 인터넷 접속 차단 장치는 www.abc.com에 대한 카테고리인 게임 사이트를 수신할 수 있다.
- [0057] 단계(417)에서 인터넷 접속 차단 장치는 쿼리 도메인 주소 및 쿼리 도메인 주소에 대응하는 카테고리를 URL 판별 정보에 저장할 수 있다. 예를 들면, 인터넷 접속 차단 장치는 www.abc.com, 게임 사이트를 URL 판별 정보에 저장할 수 있다.
- [0058] 단계(418)에서 인터넷 접속 차단 장치는 에이전트 프로그램을 이용하여 사용자 단말에 설치된 웹 브라우저로부터의 HTTP Request 패킷을 분석하여 HTTP Request 패킷의 목적지 도메인 주소를 식별할 수 있다.
- [0059] 단계(419)에서 인터넷 접속 차단 장치는 URL 판별 정보를 이용하여 HTTP Request 패킷의 목적지 도메인 주소에

대응하는 카테고리를 식별할 수 있다.

- [0060] 단계(419)에서 인터넷 접속 차단 장치는 식별된 카테고리에 따라 HTTP Request 패킷에 대한 인터넷 접속을 차단할 수 있다. 인터넷 접속 차단 장치는 정책 정보를 이용하여 식별된 카테고리에 대한 인터넷 접속 차단 여부에 따라 HTTP Request 패킷에 대한 인터넷 접속을 차단할 수 있다. 예를 들면, HTTP Request 패킷의 도메인 주소가 www.abc.com이라면, 게임 사이트는 차단 대상이므로 HTTP Request 패킷에 대한 가짜 루프백 HTTP Request 패킷을 생성할 수 있고, 생성된 가짜 루프백 HTTP Response 패킷을 HTTP Request 패킷을 생성한 웹 브라우저에 전달할 수 있다.
- [0061] 도 5는 일 실시예에 따른 에이전트 프로그램을 이용하여 인터넷 접속을 차단하는 방법을 나타낸 흐름도이다.
- [0062] 단계(511)에서 인터넷 접속 차단 장치는 IP 주소 및 IP 주소에 대응하는 카테고리를 URL 판별 정보로 유지할 수 있다. 예를 들면, 인터넷 접속 차단 장치는 100.101.102.103 이라는 IP 주소 및 100.101.102.103 에 대한 카테고리인 메신저를 URL 판별 정보로 유지할 수 있다.
- [0063] 단계(512)에서 인터넷 접속 차단 장치는 카테고리에 따른 인터넷 접속 차단 여부에 관한 정책을 정책 정보로 유지할 수 있다. 예를 들면, 인터넷 접속 차단 장치는 "메신저 애플리케이션에 대해서 차단하시오"라는 정책을 정책 정보로 유지할 수 있다.
- [0064] 단계(513)에서 인터넷 접속 차단 장치는 TCP 패킷의 SYN 필드가 세트되어 있는지 판단할 수 있다.
- [0065] 단계(514)에서 인터넷 접속 차단 장치는 TCP 패킷의 SYN 필드가 세트되어 있는 경우, TCP 패킷의 목적지 IP 주소를 식별할 수 있다. TCP 패킷의 포함된 IP 패킷으로부터 목적지 IP 주소를 식별할 수 있다.
- [0066] 단계(515)에서 인터넷 접속 차단 장치는 목적지 IP 주소가 URL 판별 정보에 포함되어 있는지 판단할 수 있다. 예를 들면, 목적지 IP 주소가 111.112.123.133 이라면, 인터넷 접속 차단 장치는 URL 판별 정보에 111.112.123.133 및 111.112.123.133에 대한 카테고리가 포함되어 있는지 판단할 수 있다.
- [0067] 단계(516)에서 인터넷 접속 차단 장치는 목적지 IP 주소가 URL 판별 정보에 포함되어 있지 않은 경우, 목적지 IP 주소를 보안 서버로 송신할 수 있다. 예를 들면, 목적지 IP 주소 111.112.123.133이 URL 판별 정보에 포함되어 있지 않은 경우, 목적지 IP 주소인 111.112.123.133을 보안 서버에 송신할 수 있다.
- [0068] 단계(517)에서 인터넷 접속 차단 장치는 보안 서버로부터 목적지 IP 주소에 대응하는 카테고리를 수신할 수 있다. 예를 들면, 인터넷 접속 차단 장치는 111.112.123.133에 대응하는 카테고리인 메신저를 수신할 수 있다.
- [0069] 단계(518)에서 인터넷 접속 차단 장치는 목적지 IP 주소 및 목적지 IP 주소에 대응하는 카테고리를 URL 판별 정보에 저장할 수 있다. 예를 들면, 인터넷 접속 차단 장치는 "111.112.123.133, 메신저"를 URL 판별 정보에 저장할 수 있다.
- [0070] 단계(519)에서 인터넷 접속 차단 장치는 에이전트 프로그램을 이용하여 사용자 단말에 설치된 애플리케이션으로부터의 TCP 패킷을 분석할 수 있다.
- [0071] 단계(520)에서 인터넷 접속 차단 장치는 TCP 패킷의 ACK 필드 및 PSH 필드가 세트되어 있는 경우, TCP 패킷의 목적지 IP 주소를 식별할 수 있다.
- [0072] 단계(521)에서 인터넷 접속 차단 장치는 식별된 카테고리에 따라 TCP 패킷에 대한 인터넷 접속을 차단할 수 있다. 정책 정보를 이용하여 식별된 카테고리에 대한 인터넷 접속 차단 여부에 따라 TCP 패킷에 대한 인터넷 접속을 차단할 수 있다. 예를 들면, TCP 패킷의 목적지 IP 주소가 100,100,100,111이라면, 상기 TCP 패킷은 차단 대상이므로 가짜 루프백 TCP 응답 패킷을 생성하고, 가짜 루프백 TCP 응답 패킷을 TCP 패킷을 생성한 애플리케이션에게 전달할 수 있다.
- [0073] 도 6은 일 실시예에 따른 보안 서버의 URL 판별 정보를 유지하는 방법을 나타낸 흐름도이다.
- [0074] URL 판별 정보는 도메인 주소 및 도메인 주소에 대응하는 카테고리를 저장할 수 있고, IP 주소 및 IP 주소에 대응하는 카테고리를 저장할 수 있다.
- [0075] 단계(610)에서 보안 서버는 도메인 주소 및 도메인 주소에 대응하는 카테고리를 URL 판별 정보로 유지할 수 있다.
- [0076] 단계(620)에서 보안 서버는 사용자 단말의 에이전트 프로그램으로부터 쿼리 도메인 주소를 수신할 수 있다.

- [0077] 단계(630)에서 보안 서버는 수신된 쿼리 도메인 주소 및 쿼리 도메인 주소에 대응하는 카테고리를 URL 판별 정보로 유지할 수 있다.
- [0078] 단계(640)에서 보안 서버는 쿼리 도메인 주소 및 쿼리 도메인 주소에 따른 카테고리를 에이전트 프로그램에 송신할 수 있다.
- [0079] 예를 들면, 보안 서버는 도메인 주소뿐만 아니라 IP 주소 및 IP 주소에 대응하는 카테고리를 URL 판별 정보로 유지할 수 있다. 보안 서버는 목적지 IP 주소를 수신할 수 있고, 목적지 IP 주소 및 목적지 IP 주소에 대응하는 카테고리를 URL 판별 정보로 유지할 수 있다. 보안 서버는 목적지 IP 주소 및 목적지 IP 주소에 따른 카테고리를 에이전트 프로그램에 송신할 수 있다.
- [0080] 이상에서 설명된 장치는 하드웨어 구성요소, 소프트웨어 구성요소, 및/또는 하드웨어 구성요소 및 소프트웨어 구성요소의 조합으로 구현될 수 있다. 예를 들어, 실시예들에서 설명된 장치 및 구성요소는, 예를 들어, 프로세서, 콘트롤러, ALU(arithmetic logic unit), 디지털 신호 프로세서(digital signal processor), 마이크로컴퓨터, FPA(field programmable array), PLU(programmable logic unit), 마이크로프로세서, 또는 명령(instruction)을 실행하고 응답할 수 있는 다른 어떠한 장치와 같이, 하나 이상의 범용 컴퓨터 또는 특수 목적 컴퓨터를 이용하여 구현될 수 있다. 처리 장치는 운영 체제(OS) 및 상기 운영 체제 상에서 수행되는 하나 이상의 소프트웨어 애플리케이션을 수행할 수 있다. 또한, 처리 장치는 소프트웨어의 실행에 응답하여, 데이터를 접근, 저장, 조작, 처리 및 생성할 수도 있다. 이해의 편의를 위하여, 처리 장치는 하나가 사용되는 것으로 설명된 경우도 있지만, 해당 기술분야에서 통상의 지식을 가진 자는, 처리 장치가 복수 개의 처리 요소(processing element) 및/또는 복수 유형의 처리 요소를 포함할 수 있음을 알 수 있다. 예를 들어, 처리 장치는 복수 개의 프로세서 또는 하나의 프로세서 및 하나의 콘트롤러를 포함할 수 있다. 또한, 병렬 프로세서(parallel processor)와 같은, 다른 처리 구성(processing configuration)도 가능하다.
- [0081] 소프트웨어는 컴퓨터 프로그램(computer program), 코드(code), 명령(instruction), 또는 이들 중 하나 이상의 조합을 포함할 수 있으며, 원하는 대로 동작하도록 처리 장치를 구성하거나 독립적으로 또는 결합적으로(collectively) 처리 장치를 명령할 수 있다. 소프트웨어 및/또는 데이터는, 처리 장치에 의하여 해석되거나 처리 장치에 명령 또는 데이터를 제공하기 위하여, 어떤 유형의 기계, 구성요소(component), 물리적 장치, 가상 장치(virtual equipment), 컴퓨터 저장 매체 또는 장치, 또는 전송되는 신호 파(signal wave)에 영구적으로, 또는 일시적으로 구체화(embody)될 수 있다. 소프트웨어는 네트워크로 연결된 컴퓨터 시스템 상에 분산되어서, 분산된 방법으로 저장되거나 실행될 수도 있다. 소프트웨어 및 데이터는 하나 이상의 컴퓨터 판독 가능 기록 매체에 저장될 수 있다.
- [0082] 실시예에 따른 방법은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 실시예를 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(magnetic media), CD-ROM, DVD와 같은 광기록 매체(optical media), 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical media), 및 롬(ROM), 램(RAM), 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함한다. 상기된 하드웨어 장치는 실시예의 동작을 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.
- [0083] 이상과 같이 실시예들이 비록 한정된 실시예와 도면에 의해 설명되었으나, 해당 기술분야에서 통상의 지식을 가진 자라면 상기의 기재로부터 다양한 수정 및 변형이 가능하다. 예를 들어, 설명된 기술들이 설명된 방법과 다른 순서로 수행되거나, 및/또는 설명된 시스템, 구조, 장치, 회로 등의 구성요소들이 설명된 방법과 다른 형태로 결합 또는 조합되거나, 다른 구성요소 또는 균등물에 의하여 대치되거나 치환되더라도 적절한 결과가 달성될 수 있다.
- [0084] 그러므로, 다른 구현들, 다른 실시예들 및 특허청구범위와 균등한 것들도 후술하는 특허청구범위의 범위에 속한다.

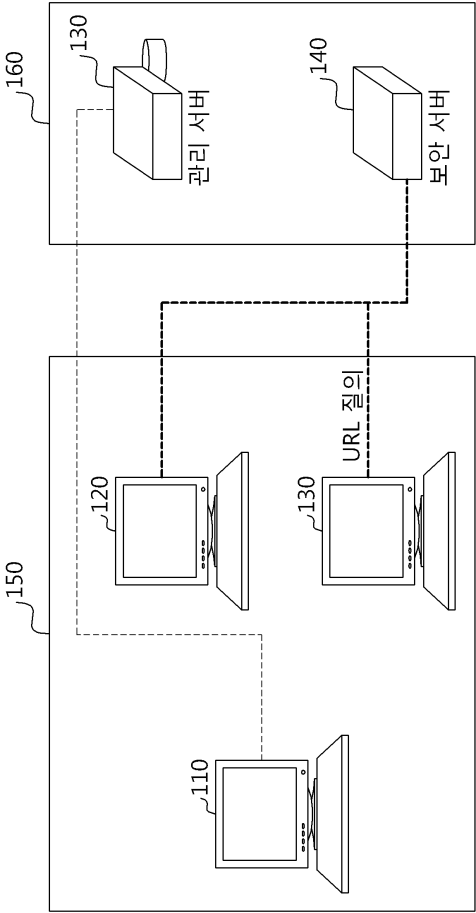
부호의 설명

[0085]

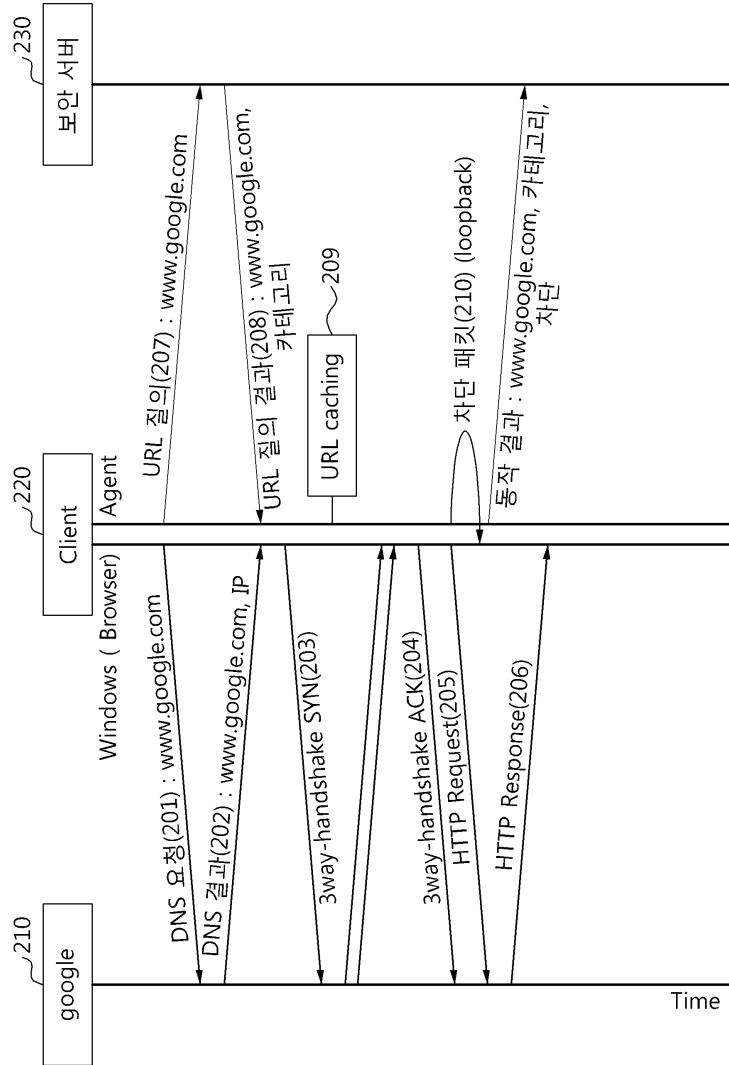
- 110: 관리자 PC
- 120: PC
- 130: 관리 서버
- 131: PC
- 140: 보안 서버
- 150: 고객사
- 160: ISP

도면

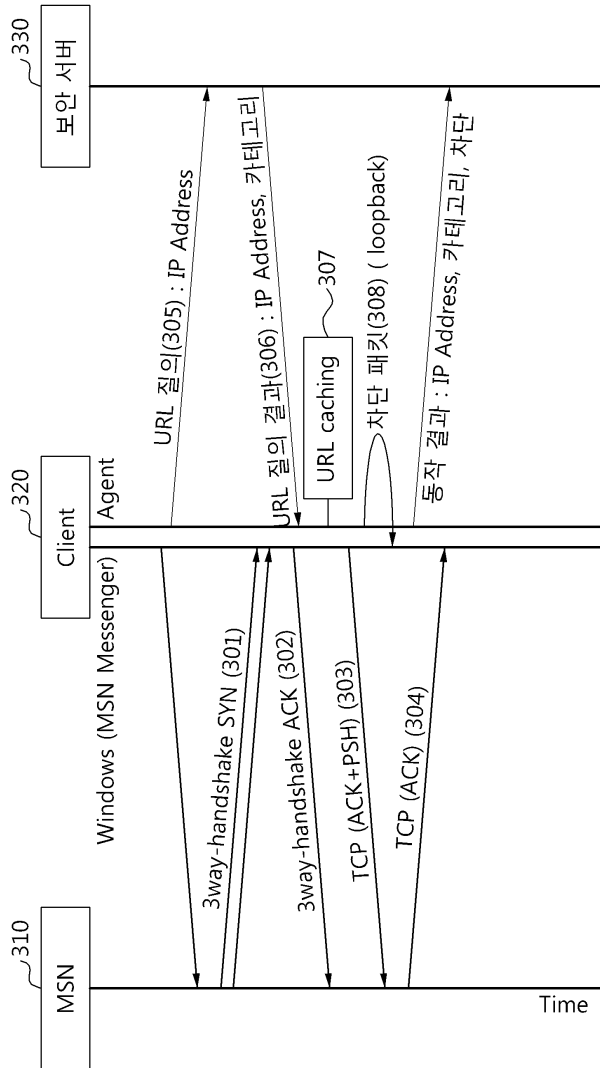
도면1



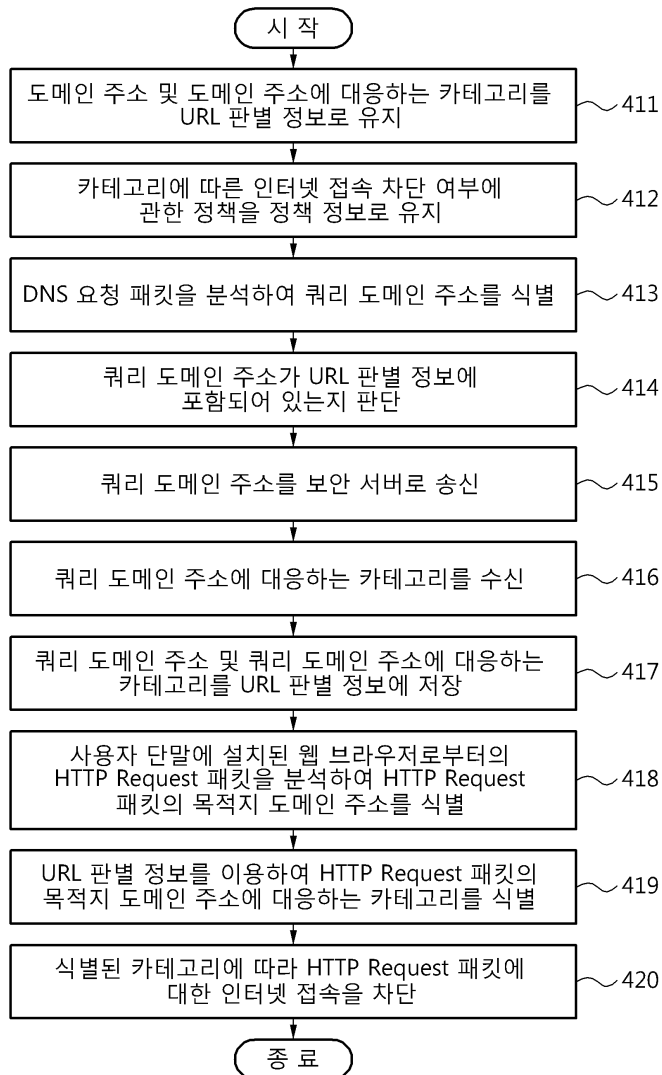
도면2



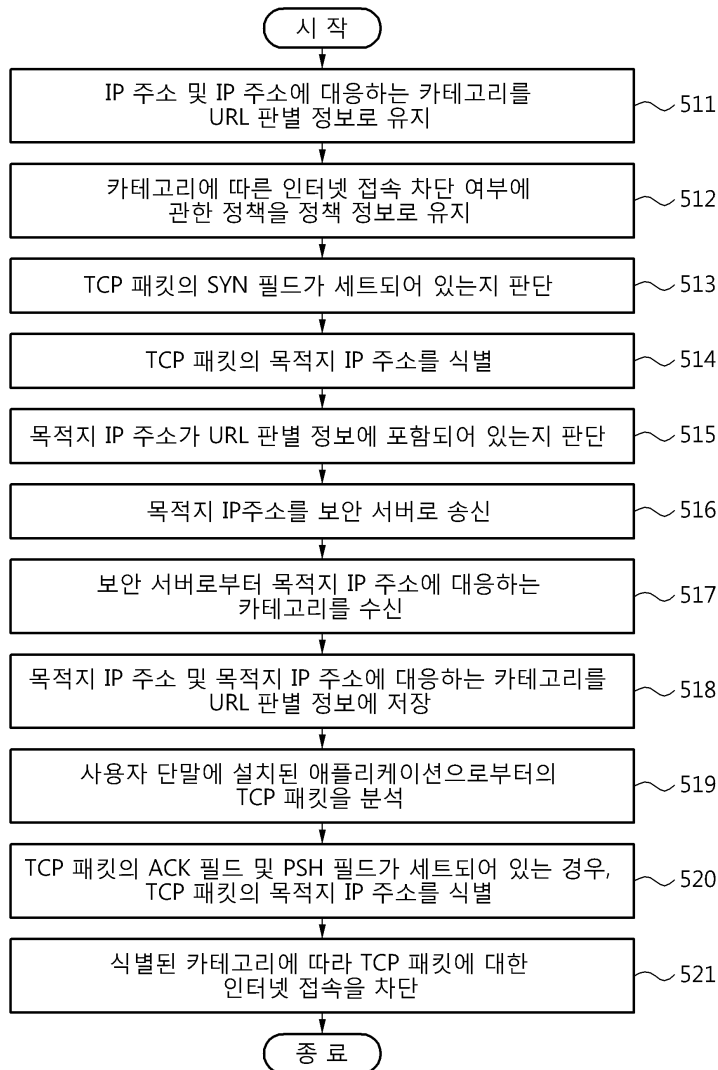
도면3



도면4



도면5



도면6

