(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2012년07월06일
(11) 등록번호 10-1156584
(24) 등록일자 2012년06월08일

(51) 국제특허분류(Int. Cl.)
H04L 12/24 (2006.01) *H04L 29/06* (2006.01)
(21) 출원번호 10-2007-7002969
(22) 출원일자(국제) 2005년07월28일
심사청구일자 2010년06월23일
(85) 번역문제출일자 2007년02월07일
(65) 공개번호 10-2007-0064585
(43) 공개일자 2007년06월21일
(86) 국제출원번호 PCT/GB2005/002961
(87) 국제공개번호 WO 2006/016106
국제공개일자 2006년02월16일
(30) 우선권주장
0417620.2 2004년08월07일 영국(GB)
10/942,635 2004년09월16일 미국(US)
(56) 선행기술조사문헌
US06105027 A
US20030135611 A1
US19985828833 A1
전체 청구항 수 : 총 44 항

(73) 특허권자
웹센스 유케이 리미티드
영국 이시4브이 6제이에이 런던 뉴브릿지 스트리트 100
(72) 발명자
존슨 케빈
영국, 스트라트포드쉬어 에스티5 8알큐, 뉴케슬-언더-리메,브래드웰, 올드 홀 드라이브 64
포인턴 리차드
영국, 스토크-온-트렌트 에스티7 3비엘, 스콜라 그린, 리틀 모스1에이
(74) 대리인
정홍식

심사관 : 홍경아

(54) 발명의 명칭 **리소스 액세스 필터링 시스템 및 방법**

(57) 요 약

원격 디바이스(32)의 인터넷 액세스들이 실시간으로 원격 서버(33)에 의해 모니터되고 제어되는 원격지 필터링 및 모니터링 시스템 및 방법이 기술된다. 상기 시스템은 또한 오프라인 로깅 및 후속 업로딩, 조정가능한 필터링 감도들 및 특정 HTTP 포트 필터링을 지원한다.

대 표 도 - 도1

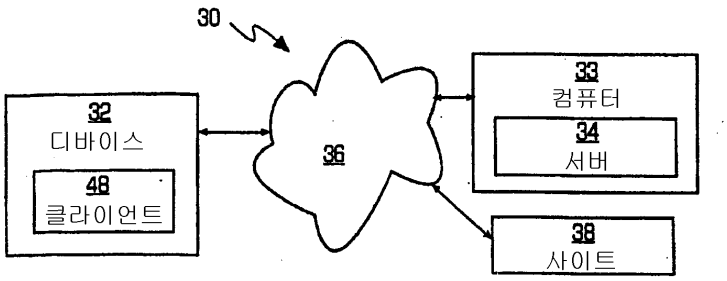

FIG. 1

특허청구의 범위

청구항 1

리소스 액세스 필터링 시스템(resource access filtering system)에 있어서,

컴퓨터(33);

디바이스(32) 상의 클라이언트(48)를 포함하고, 상기 클라이언트(48)는 상기 컴퓨터(33)에 대한 원격 접속을 확립하고, 상기 클라이언트(48)는 상기 디바이스(32)에 의해 리소스를 액세스하기 위한 요청에 대한 정보를 수집하는 모듈 및 상기 수집된 정보를 상기 컴퓨터(33)로 통신하는 모듈을 더 포함하고,

상기 컴퓨터(33)는 상기 수집된 정보에 기초하여 상기 디바이스(32)의 상기 리소스 액세스를 분류(categorize)하는 모듈 및 상기 클라이언트(48)가 상기 컴퓨터(33)의 리소스 액세스 판정에 기초하여 상기 디바이스(32)에 의한 상기 리소스에 대한 상기 액세스를 제어하도록, 리소스 액세스 판정을 상기 클라이언트(48)에 실시간으로 통신하는 모듈을 포함하는, 리소스 액세스 필터링 시스템.

청구항 2

제 1 항에 있어서,

상기 리소스 액세스 판정은 허가 판정(allow decision) 또는 차단 판정(blolck decision)을 상기 클라이언트(48)에 제공하고, 그것에 의해 상기 클라이언트(48)는 상기 요청된 리소스에 대한 액세스를 허용 또는 차단하는, 리소스 액세스 필터링 시스템.

청구항 3

제 1 항 또는 제 2 항에 있어서,

상기 클라이언트(48)는 상기 요청된 리소스가 회사 네트워크를 통해 통신되는지의 여부를 검출하고 상기 회사 네트워크를 통해 통신되는 상기 요청된 리소스에 대해 상기 클라이언트 필터링을 디스에이블하는 모듈을 더 포함하는, 리소스 액세스 필터링 시스템.

청구항 4

제 1 항 또는 제 2 항에 있어서,

상기 클라이언트(48)는 상기 클라이언트(48)가 상기 컴퓨터(33)과 통신할 수 없을 때 상기 디바이스(32)의 상기 리소스 액세스들을 제어하는 오프라인 필터링 모듈을 더 포함하는, 리소스 액세스 필터링 시스템.

청구항 5

제 4 항에 있어서,

상기 오프라인 필터링 모듈은 허가의 모든 리소스 액세스 모드(allow all resource access mode), 차단의 모든 리소스 액세스 모드(block all resource access mode) 및 로깅(logging)을 갖는 허가의 모든 리소스 액세스 모드(allow resource access with logging mode)를 구비하는 하나 이상의 모드를 제공하는, 리소스 액세스 필터링 시스템.

청구항 6

제 5 항에 있어서,

상기 로깅을 갖는 허가의 모든 리소스 액세스 모드는 오프라인 로그들에 의해 이용되는 대역폭을 제어하기 위해 상기 컴퓨터(33)에 업로드(upload)되는 상기 오프라인 로그들을 스로틀링(throttling)하기 위한 모듈을 더 포함하는, 리소스 액세스 필터링 시스템.

청구항 7

제 4 항에 있어서,

오프라인 필터링 모듈의 모드는 상기 컴퓨터(33)에 의해 선택되는, 리소스 액세스 필터링 시스템.

청구항 8

제 1 항 또는 제 2 항에 있어서,

상기 클라이언트(48)는 HTTP 포트들로서 취급될 포트들 및 필터링된 포트들을 나타내는 상기 컴퓨터(33)로부터 다운로드된 필터링된 포트 리스트(filtered port list)를 가지는, 리소스 액세스 필터링 시스템.

청구항 9

제 8 항에 있어서,

상기 클라이언트(48)는 필터링된 포트(filtered port)로서 특별히 식별되지 않은 포트에 대해 상기 디바이스(32)의 상기 리소스 액세스들을 제어하는 필터링되지 않은 포트 모듈(unfiltered ports module)을 더 포함하는, 리소스 액세스 필터링 시스템.

청구항 10

제 9 항에 있어서,

상기 필터링되지 않은 포트 모듈은 허가의 모든 리소스 액세스 모드, 차단의 모든 리소스 액세스 모드 및 가능한 필터링 및/또는 로깅을 위한 컴퓨터(33)로의 전송 모드를 더 포함하는, 리소스 액세스 필터링 시스템.

청구항 11

제 8 항에 있어서,

필터링되지 않은 포트 모듈의 모드는 상기 컴퓨터(33)에 의해 선택되는, 리소스 액세스 필터링 시스템.

청구항 12

제 1 항 또는 제 2 항에 있어서,

상기 클라이언트(48)는 상기 클라이언트(48)에 대한 리소스 액세스의 필터링 레벨을 제어하는 필터링 감도 모듈(filtering sensitivity module)을 더 포함하고, 그것에 의해 상기 클라이언트(48)는 상기 필터링의 레벨에 기초하여 상기 컴퓨터로 상기 수집된 정보를 제공할지의 여부를 결정하는, 리소스 액세스 필터링 시스템.

청구항 13

제 12 항에 있어서,

상기 필터링 감도 모듈은 고감도 레벨 모드, 중간 감도 레벨 모드, 낮은 감도 레벨 모드 및 자동 감도 레벨 모드(automatic sensitivity level mode)를 더 포함하는, 리소스 액세스 필터링 시스템.

청구항 14

제 12 항에 있어서,

상기 필터링 감도 모듈의 모드는 상기 컴퓨터(33)에 의해 선택되는, 리소스 액세스 필터링 시스템.

청구항 15

제 1 항 또는 제 2 항에 있어서,

상기 컴퓨터(33)는 상기 디바이스들의 상기 리소스 액세스들의 요약(summary)을 발생하기 위해 상기 컴퓨터(33)에 접속된 상기 디바이스들의 상기 리소스 액세스들을 모니터하는 모니터 모듈을 더 포함하는, 리소스 액세스 필터링 시스템.

청구항 16

제 1 항 또는 제 2 항에 있어서,

상기 액세스되는 리소스는 웹 페이지, 파일 전송 프로토콜 사이트, 이메일 사이트, 보안 웹 사이트, 및 뉴스 사이트(news site) 중 어느 하나를 포함하는, 리소스 액세스 필터링 시스템.

청구항 17

제 1 항 또는 제 2 항에 있어서,

상기 디바이스(32)는 개인 휴대 단말(personal digital assistant), 셀룰러 폰(cellular phone), 퍼스널 컴퓨터, 랩탑 컴퓨터, 팜탑 컴퓨터(parmtop computer) 및 전기 기기(appliance) 중 어느 하나를 포함하는, 리소스 액세스 필터링 시스템.

청구항 18

제 1 항 또는 제 2 항에 있어서,

상기 클라이언트(48)는 상기 디바이스(32)에 대한 성능 마스크(capability mask)를 생성하고 그 성능 마스크를 상기 컴퓨터(33)에 통신하는 모듈을 더 포함하고, 상기 성능 마스크는 상기 디바이스(32)의 필터링 성능들에 대한 정보를 포함하는, 리소스 액세스 필터링 시스템.

청구항 19

제 1 항 또는 제 2 항에 있어서,

상기 수집된 정보 및 상기 리소스 액세스 판정은 TCP 포트(80)를 통해 하이퍼텍스트 전송 프로토콜을 이용하여 상기 클라이언트(48)와 컴퓨터(33) 사이에서 통신되는, 리소스 액세스 필터링 시스템.

청구항 20

제 19 항에 있어서,

상기 수집된 정보에 대한 프로토콜은 하이퍼텍스트 전송 프로토콜 POST 동작을 더 포함하는, 리소스 액세스 필터링 시스템.

청구항 21

제 1 항 또는 제 2 항에 있어서,

상기 리소스 액세스 판정을 위한 프로토콜은 웹 페이지 포맷의 데이터를 더 포함하는, 리소스 액세스 필터링 시스템.

청구항 22

컴퓨터(33)와 컴퓨터(33)에 대한 접속을 확립하는 디바이스(32) 상의 클라이언트(48)를 이용하는 리소스 액세스 필터링 방법에 있어서,

상기 디바이스(32)에 의해 리소스를 액세스하기 위한 요청에 대한 정보를 클라이언트(48)에 의해 수집하는 단계;

원격 통신에 의해 상기 수집된 정보를 상기 컴퓨터(33)에 통신하는 단계;

상기 컴퓨터(33)에서, 상기 수집된 정보에 기초하여 상기 디바이스(32)의 상기 리소스 액세스를 분류하는 단계; 및

상기 클라이언트(48)가 상기 컴퓨터(33)의 리소스 액세스 판정에 기초하여 상기 디바이스(32)에 의한 상기 리소스로의 액세스를 제어하도록 실시간으로 상기 클라이언트(48)에 리소스 액세스 판정을 통신하는 단계를 포함하는, 리소스 액세스 필터링 방법.

청구항 23

제 22 항에 있어서,

상기 리소스 액세스 판정은 상기 클라이언트(48)에 허가 판정 또는 차단 판정을 제공하고, 그것에 의해 상기 클라이언트(48)는 상기 요청된 리소스로의 액세스를 허가 또는 차단하는, 리소스 액세스 필터링 방법.

청구항 24

제 22 항 또는 제 23 항에 있어서,

상기 클라이언트(48)는 상기 요청된 리소스가 회사 네트워크를 통해 통신되는지의 여부를 검출하고 상기 회사 네트워크를 통해 통신되는 상기 요청된 리소스에 대한 상기 클라이언트 필터링을 디스에이블하는 모듈을 더 포함하는, 리소스 액세스 필터링 방법.

청구항 25

제 22 항 또는 제 23 항에 있어서,

상기 클라이언트(48)는 상기 클라이언트(48)가 상기 컴퓨터(33)와 통신할 수 없을 때 상기 디바이스(32)의 상기 리소스 액세스들을 제어하는 오프라인 필터링 모듈을 더 포함하는, 리소스 액세스 필터링 방법.

청구항 26

제 25 항에 있어서,

상기 오프라인 필터링 모듈은 허가의 모든 리소스 액세스 모드, 차단의 모든 리소스 액세스 모드 및 로깅을 갖는 허가의 모든 리소스 액세스 모드를 포함하는 하나 이상의 모드를 제공하는, 리소스 액세스 필터링 방법.

청구항 27

제 26 항에 있어서,

상기 로깅을 갖는 허가의 모든 리소스 액세스 모드는 오프라인 로그들에 의해 이용되는 대역폭을 제어하기 위해 상기 컴퓨터(33)에 업로드된 상기 오프라인 로그들을 스로틀링하는 모듈을 더 포함하는, 리소스 액세스 필터링 방법.

청구항 28

제 25 항에 있어서,

오프라인 필터링 모듈의 모드는 상기 컴퓨터(33)에 의해 선택되는, 리소스 액세스 필터링 방법.

청구항 29

제 22 항 또는 제 23 항에 있어서,

상기 클라이언트(48)는 필터링될 포트들 및 HTTP 포트들로서 취급될 포트들을 나타내는 상기 컴퓨터(33)로부터 다운로드되는 필터링된 포트 리스트를 가지는, 리소스 액세스 필터링 방법.

청구항 30

제 29 항에 있어서,

상기 클라이언트(48)는 필터링된 포트로서 특별히 식별되지 않은 포트에 대해 상기 디바이스(32)의 상기 리소스 액세스를 제어하는 필터링되지 않은 포트 모듈을 더 포함하는, 리소스 액세스 필터링 방법.

청구항 31

제 30 항에 있어서,

상기 필터링되지 않은 포트 모듈은 허가의 모든 리소스 액세스 모드, 차단의 모든 리소스 액세스 모드 및 가능한 필터링 및/또는 로깅을 위한 컴퓨터(33)로의 전송 모드를 더 포함하는, 리소스 액세스 필터링 방법.

청구항 32

제 29 항에 있어서,

필터링되지 않은 포트 모듈의 모드는 상기 컴퓨터(33)에 의해 선택되는, 리소스 액세스 필터링 방법.

청구항 33

제 22 항 또는 제 23 항에 있어서,

상기 클라이언트(48)는 상기 클라이언트(48)에 대한 리소스 액세스들의 필터링 레벨을 제어하는 필터링 감도 모듈을 더 포함하고, 그것에 의해 상기 클라이언트(48)는 상기 필터링의 레벨에 기초하여 상기 컴퓨터로 상기 수집된 정보를 제공할지의 여부를 결정하는, 리소스 액세스 필터링 방법.

청구항 34

제 33 항에 있어서,

상기 필터링 감도 모듈은 고감도 레벨 모드, 중간 감도 레벨 모드, 낮은 감도 레벨 모드 및 자동 감도 레벨 모드를 더 포함하는, 리소스 액세스 필터링 방법.

청구항 35

제 33 항에 있어서,

상기 필터링 감도 모듈의 모드는 상기 컴퓨터(33)에 의해 선택되는, 리소스 액세스 필터링 방법.

청구항 36

제 22 항 또는 제 23 항에 있어서,

상기 컴퓨터(33)는 상기 디바이스들의 상기 리소스 액세스들의 요약을 발생하기 위해 상기 컴퓨터(33)에 접속된 상기 디바이스들의 상기 리소스 액세스들을 모니터하는 모니터 모듈을 더 포함하는, 리소스 액세스 필터링 방법.

청구항 37

제 22 항 또는 제 23 항에 있어서,

상기 액세스되는 리소스는 웹 페이지, 파일 전송 프로토콜 사이트, 이메일 사이트, 보안 웹 사이트, 및 뉴스 사이트 중 하나를 더 포함하는, 리소스 액세스 필터링 방법.

청구항 38

제 22 항 또는 제 23 항에 있어서,

상기 디바이스(32)는 개인 휴대 단말, 셀룰러 폰, 퍼스널 컴퓨터, 랩탑 컴퓨터, 팜탑 컴퓨터 및 전기 기기 중 하나를 더 포함하는, 리소스 액세스 필터링 방법.

청구항 39

제 22 항 또는 제 23 항에 있어서,

상기 클라이언트(48)는 상기 디바이스(32)에 대한 성능 마스크를 생성하고 그 성능 마스크를 상기 컴퓨터(33)에 통신하는 모듈을 더 포함하고, 상기 성능 마스크는 상기 디바이스(32)의 필터링 성능들에 대한 정보를 포함하는, 리소스 액세스 필터링 방법.

청구항 40

제 22 항 또는 제 23 항에 있어서,

상기 수집된 정보 및 상기 리소스 액세스 판정은 TCP 포트(80)를 통해 하이퍼텍스트 전송 프로토콜을 이용하여 상기 클라이언트(48)와 컴퓨터(33) 사이에서 통신되는, 리소스 액세스 필터링 방법.

청구항 41

제 40 항에 있어서,

상기 수집된 정보에 대한 프로토콜은 하이퍼텍스트 전송 프로토콜 POST 동작을 더 포함하는, 리소스 액세스 필터링 방법.

청구항 42

제 22 항 또는 제 23 항에 있어서,

상기 리소스 액세스 판정을 위한 프로토콜은 웹 페이지 포맷의 데이터를 더 포함하는, 리소스 액세스 필터링 방법.

청구항 43

리소스 액세스 필터링 시스템을 위한 컴퓨터(33)에 있어서,

원격 디바이스(32)에 의해 리소스를 액세스하기 위한 요청에 대한 정보를 수신하는 모듈로서, 리소스 액세스 요청에 대한 상기 정보는 상기 원격 디바이스(32) 상의 클라이언트(48)로부터 원격으로 통신되는, 상기 정보를 수신하는 모듈;

상기 정보에 기초하여 상기 원격 디바이스(32)의 상기 리소스 액세스를 분류하는 모듈; 및

상기 클라이언트(48)가 상기 컴퓨터(33)의 리소스 액세스 판정에 기초하여 상기 원격 디바이스(32)에 의한 상기 리소스로의 액세스를 제어하도록 실시간으로 상기 클라이언트(48)에 리소스 액세스 판정을 통신하는 모듈을 포함하는, 리소스 액세스 필터링 시스템을 위한 컴퓨터.

청구항 44

원격 컴퓨터(33)와 통신하는 디바이스(32) 상에 위치된 원격 액세스 필터링 클라이언트(48)에 있어서,

상기 디바이스(32)에 의한 리소스를 액세스하기 위한 요청에 대한 정보를 수집하는 모듈;

상기 수집된 정보를 상기 컴퓨터(33)에 통신하는 모듈; 및

상기 컴퓨터(33)로부터 리소스 액세스 판정을 수신하고 상기 컴퓨터(33)의 상기 리소스 액세스 판정에 기초하여 상기 디바이스(32)에 의한 상기 리소스로의 상기 액세스를 제어하는 모듈을 포함하는, 원격 액세스 필터링 클라이언트.

명 세 서

기 술 분 야

[0001] 본 발명의 분야는 일반적으로 필터링 시스템에 관한 것으로서, 특히 컴퓨터 구현 리소스 액세스 필터링 시스템 및 방법에 관한 것이다.

배 경 기 술

[0002] 컨텐트(content) 또는 이메일들(e-mails)을 필터링하는 시스템들 및 소프트웨어가 잘 알려져 있다. 예를 들면, 잘 알려진 방화벽들(fire-walls) 및 프록시 서버들(proxy servers)은 해커들(hackers), 악의적인 바이러스들(malicious viruses) 및 웜들(worms)로부터 회사 인트러넷(corporate intranet)과 같은 내부 컴퓨터 네트워크를 보호하기 위해 이들 기능들 중 일부를 수행한다. 방화벽/프록시 서버가 허가되지 않은 인터넷 액세스를 필터링할 수 있게 하고 사용자들이 이들 원하지 않는 이메일 메시지들을 수신하지 않도록 하기 위한 잘 알려진 시스템이 또한 있다. 전형적으로, 이들 시스템들은 회사 네트워크에 게이트웨이로서 작용하는 서버와 협력한다. 상기 서버는 전형적으로 서버가 입출력 트래픽(incoming and outgoing traffic)에 대해 필터링 동작들을 수행하는 몇가지 기능(소프트웨어 또는 하드웨어로)을 가진다.

[0003] 원격 작업(remote working)은 많은 분야들에 걸쳐 그리고 많은 산업들에서 더 널리 보급되고 있다. 원격 컴퓨팅 장치는 회사 네트워크 또는 LAN으로부터 원격으로 사용된다. 몇몇 시스템에서, 원격 디바이스는 그 자신의 필터링을 수행할 수 있지만, 그것은 코포레이션-와이드 허용가능 용도 정책(corporate-wide acceptable usage policy(AUP))을 강제하기가 훨씬 더 곤란하고 상기 원격 디바이스는 그 자신이 리소스 액세스들을 필터링하기 위해 추가 처리 전력을 요구한다. 전형적으로, 원격 디바이스의 사용자는 컴퓨터 네트워크로부터 리소스들, 예컨대 이메일 메시지들, FTP 또는 WWW 사이트로의 여러가지 상이한 파일들, 뉴스그룹(newsgroup)으로부터의 포스팅(posting)을 액세스할 수 있다. 따라서, 컴퓨터 네트워크로부터 리소스에 액세스하기 위한 원격 디바이스 요청을 필터링하는 시스템을 제공하는 것이 바람직하다. 따라서, 이들 목적들을 달성하는 필터링 시스템 및 방법을 제공하는 것이 바람직하고, 본 발명은 이러한 목적을 달성하는 데 있다.

발명의 상세한 설명

[0004] 본 발명에 따르면 첨부된 청구항들에 기재된 것과 같은 장치 및 방법이 제공된다. 본 발명의 최선의(preferred) 특징들은 종속 청구항들 및 다음의 상세한 설명으로부터 명백해질 것이다.

[0005] 원격 디바이스의 리소스 액세스의 모니터링 및 필터링을 허용하는 필터링 시스템 및 방법이 제공된다. 최선의 시스템은 컴퍼니가 사무실(office)의 벽을 넘어 그 회사의 허용가능한 사용 정책을 확대할 수 있게 한다. 특히, 상기 시스템은, 예컨대 모바일 및 원격 피고용인 및 집에서 작업하는 피고용인에 의해 사용되는 것과 같은, 회사가 원격 디바이스들에 의해 액세스된 리소스들을 관리할 수 있게 허용한다. 본 발명은 또한 컴퓨터 및 상기 시스템을 위한 클라이언트를 제공한다.

[0006] 최선의 실시예에 있어서, 상기 시스템은 컴퓨터와 통신하는 원격 디바이스 위에 설치된 클라이언트를 포함한다. 상기 원격 디바이스는 컴퓨터와 원격으로 통신하며, 예컨대 동일 로컬 네트워크의 일부가 아니다. 전형적으로, 상기 원격 디바이스는 인터넷과 같은 글로벌 네트워크 또는 광역 네트워크를 통해 통신한다. 서버 컴퓨터는 원격 디바이스의 리소스 액세스 요청들을 모니터 및 필터링한다. 클라이언트는 디바이스에 의한 리소스를 액세스하기 위한 요청에 대한 정보를 수집하는 모듈 및 상기 수집된 정보를 컴퓨터에 통신하는 모듈을 가진다. 상기 컴퓨터는 상기 수집된 정보에 기초하여 상기 디바이스의 리소스 액세스를 분류하는 모듈 및 리소스 액세스 판정을 클라이언트에 실시간으로 통신하는 모듈을 가진다. 이 후, 클라이언트는 컴퓨터의 리소스 액세스 판정에 기초하여 상기 디바이스에 의한 리소스로의 액세스를 제어한다.

[0007] 특히 최선의 실시예에 있어서, 상기 리소스 액세스 판정은 "허가(allow)" 또는 "차단(block)" 판정 중 하나이다. 즉, 판정은 디바이스가 상기 요청된 리소스를 액세스할 수 있게 허용하거나 차단하는 것이다. 유리하게는, 클라이언트는 최소 처리 전력 및 메모리를 요구하고, 필터링 시스템을 지원할 수 있는 디바이스들의 수 및 유형은 증가된다.

[0008] 클라이언트 디바이스가 컴퓨터와 접속할 수 없는 경우가 있다. 디바이스가 필터링 시스템의 서버와의 접속을 잃었을 때, 오프라인 기능은 클라이언트가 미리 정해진 정책에 따라 상기 디바이스의 리소스 액세스를 계속 필터링하게 허용한다. 이상적으로, 미리 정해진 정책은 서버에서 중앙집중식으로 관리되고 서버는 오프라인 필터링 기능 모드를 설정한다. 일 모드에서, 상기 클라이언트는 모든 액세스 요청들을 허용할 수 있고, 이들 리소스 액세스의 로그를 발생한다. 로그는 클라이언트가 서버와의 접속을 다시 확립하면 서버로 다시 통신될 수 있다.

[0009] 많은 디바이스들이 국부적 및 원격적 모두로 사용된다. 즉, 디바이스는 때때로 사용자가 회사 사무실에 있을 때와 같이 로컬 네트워크 내에서 국부적으로 사용된다. 다른 때에는, 동일한 디바이스는 예컨대 사용자가 집에서 떠나 이동하거나 일하고 있을 때, 원격으로 사용된다. 이들 2가지 환경들에서 리소스 액세스 요청들의 필터링을 효과적으로 관리할 필요가 있다. 최선의 실시예에서, 상기 시스템은 요청된 리소스가 회사 네트워크를 통해 통신되는지의 여부를 검출하고 회사 네트워크를 통해 통신되는 요청된 리소스에 대한 필터링을 인에이블하는 모듈을 포함한다.

[0010] 최선의 필터링되지 않은 포트들의 필터링 기능은 시스템이 심지어 필터링되지 않은 포트들이 어떤 방식으로 필터링될 수 있도록 필터링된 포트들로서 특별히 식별되지 않은 TCP 포트들에 대한 필터링 방법(filtering strategy)을 특정할 수 있게 허용한다.

[0011] 또, 최선의 시스템은 관리자(administrator)가 고감도 레벨, 중간 감도 레벨, 낮은 감도 레벨 또는 자동 감도 레벨 사이에서 각 클라이언트에 대한 필터링 감도 레벨을 조정할 수 있게 허용한다. 상기 필터링 감도 레벨은 예를 들면 느린 인터넷 접속을 갖는 디바이스에 대해, 예컨대 셀룰러 폰을 위한 GPRS 접속에 대해 조정될 수 있다.

[0012] 상기 시스템은 서버에 접속된 모든 디바이스들 또는 각 디바이스의 리소스 액세스들에 대한 레포트들을 시스템이 발생할 수 있게 허용하는 모니터링 능력(monitoring capability)을 제공할 수 있다.

[0013] 최선의 시스템은 컴퍼니의 법적 책임(company's legal liabilities)을 감소시킬 수 있는 데, 예컨대 그 이유는 컴퍼니가 업무 시간 중 부적절한 웹 사이트로의 액세스를 더욱 제어할 수 있기 때문이다. 상기 시스템은 업무 시간 중 어떤 인터넷 액세스도 업무-관련 웹 사이트들로 제한될 수 있기 때문에 피고용인의 생산성을 증가시킬 수 있다. 상기 시스템은 또한 상기 시스템이 인터넷 서비스 제공자 또는 외부 모뎀을 이용하는 피고용인을 통해 작업 장소로 들어올 수 있는 바이러스들 및 악의적인 콘텐트를 방어할 수 있다는 점에서 네트워크

보안성(network security)을 제공할 수 있다.

[0014] 본 발명의 더 나은 이해를 위해 그리고 어떻게 본 발명의 실시예들이 실행될 수 있는지를 보이기 위해, 첨부하는 개략도를 예로서 참조할 것이다.

실 시 예

[0023] 본 발명은 클라이언트/서버 기반 컴퓨터-구현, 소프트웨어-기반 디바이스 리소스 액세스 필터링 및 모니터링 시스템에 특히 적용가능하며, 이러한 관점에서 본 발명이 기술될 것이다. 그러나, 본 발명에 따른 시스템 및 방법은 시스템이 다양한 상이한 컴퓨터 아키텍쳐들을 이용하여 구현될 수 있고 다양한 상이한 원격 디바이스들로 구현될 수 있으므로 더 큰 유용성을 갖는다는 것을 알 수 있는 것이다. 상기 시스템은 임의의 컴퓨팅 디바이스를 이용하여 구현될 수 있고, 여기서 컴퓨터 디바이스는 적어도 프로세서, 메모리 및 충분한 컴퓨팅 전력을 갖는 입력/출력 디바이스를 가져서 컴퓨팅 디바이스가 본원에 기술된 시스템과 상호작용할 수 있고 여기에 기재된 기본 필터링 기능들을 수행할 수 있는 데, 그 이유는 각 클라이언트가 이하에 기술되는 기능들 모두를 반드시 수행할 수 있어야 하는 것이 아니기 때문이다. 상기 시스템은 소프트웨어 또는 하드웨어로 구현될 수 있다. 소프트웨어 실시예에 있어서, 상기 시스템은 서버에 하나 이상의 소프트웨어 모듈 및 클라이언트에 하나 이상의 모듈을 포함할 수 있고, 여기서 각 모듈은 서버 또는 클라이언트의 프로세서에 의해 실행되는 복수 라인의 컴퓨터 코드를 더 포함할 수 있다. 지금, 원격 디바이스 모니터링 시스템의 실시예가 설명될 것이다.

[0024] 도 1은 본 발명에 따른 디바이스 리소스 액세스 필터링 시스템(30)의 예를 나타낸 도면이다. 상기 시스템(30)은 이 실시예에서 서버 소프트웨어(서버 소프트웨어; 34)를 갖춘 컴퓨터와 같은 원격 컴퓨터 디바이스(33)에 접속하는 디바이스(32)(클라이언트(48)로서 알려진 소프트웨어 코드의 피스(piece)를 갖는)가, 이 실시예에서의 인터넷, 광대역 네트워크(wide area network; WAN), 로컬 에어리어 네트워크(local area network; LAN), 메트로폴리탄 에어리어 네트워크(metropolitan area network; MAN) 또는 월드 와이드 웹(World Wide Web)과 같은 컴퓨터 네트워크(36)를 통해 모니터링되고 사이트(38) 상의 리소스들에 대한 상기 디바이스 액세스가 필터링되게 허용한다. 상기 사이트(38)는 디바이스(32)의 사용자에 의해 요청된 리소스의 소스이다. 더 상세하게는, 상기 서버(34)는 리소스들에 대한 상기 디바이스의 액세스를 원격으로 필터링(제어 및/또는 분석)할 수 있다. 본 발명에 따르면, 상기 디바이스(32)의 이러한 원격 모니터링을 달성하기 위한 기능은 상기 디바이스(32)와 상기 서버(34) 사이에서 분할된다. 이것은 상기 디바이스(32)와 상기 서버(34) 사이의 네트워크 트래픽을 감소시키고 이메일들, 웹 페이지들, 파일 전송 프로토콜(file transfer protocol; FTP) 사이트들, 뉴스그룹들 등을 포함하는 다양한 리소스들에 대한 액세스의 중앙집중 제어 및 모니터링을 허용한다. 본 발명에 따르면, 상기 서버(34)는 또한 상기 디바이스가 상기 사이트(38)에 대한 액세스 요청과 관련된 어드레스로부터 컨텐트를 수신하고 데이터를 다운로드하는 등을 하는 것이 허용될 것인지의 여부를 결정하기 위해 리소스들의 시도된 액세스(attempted access)와 연관된 데이터를 수신할 수 있다. 상기 디바이스 및 서버는 소유 프로토콜(proprietary protocol)에 기초하는 특정 프로토콜을 이용하여 서로 통신할 수 있다. 상기 시스템은 컴퓨터 네트워크 액세스의 실시간 필터링을 제공하고 그것에 의해 원격 컴퓨터(33)가, 예컨대 최선의 실시예에서는 상기 서버(34)가 필터링 결정들을 행하고 및/또는 조정하기 위해 이용된다.

[0025] 상기 시스템을 위한 프로토콜은, 클라이언트(48)가 다양한 원격 네트워크들(회사가 약간 제어를 하거나 하지 않는)에서 및 원격 네트워크들에 대해 작용할 것이 예상되므로, 이들 원격 네트워크들과 가능하게는 호환가능하고 그 결과 클라이언트(48)는 이들 원격 네트워크들을 통해 동작할 수 있다. 예를 들면, 상기 프로토콜은 방화벽 및 프록시들과 호환가능하다. 이 프로토콜은 상이한 데이터 포맷들 및 호환성을 갖는 다양한 상이한 디바이스들을 취급하고 수용하므로 프로토콜은 상이한 디바이스들에 대한 수들 및 스트링들에 대한 표준 데이터 포맷을 제공한다. 프로토콜은 또한 서버가 제한된 대역폭을 이용하여 많은 수의 클라이언트들을 취급할 필요가 있고 클라이언트가 서버에 대해 느린 인터넷 접속을 이용할 수 있어야 하기 때문에 사이즈가 콤팩트하다. 본 발명의 최선의 실시예에 따라, 프로토콜은 아주 다양한 네트워크들과의 호환성을 증가시키기 위해, HTTP 인벨로프(HTTP envelope)를 이용하는 TCP 포트(80)를 통해 하이퍼텍스트 전송 프로토콜 (HTTP)을 이용한다. 인터넷에 대한 액세스를 허용하는 이들 네트워크들에 있어서, 대부분의 기본 액세스는 포트(80)를 통해 출력 접속 요청들을 포함할 웹 액세스이므로 포트(80)가 전형적으로 이용 가능하며 이 프로토콜을 위해 사용된다. 몇몇 네트워크들은 단지 HTTP 스타일 요청 및 응답을 예측하는 프록시 서버를 통한 인터넷 웹 액세스를 허용하므로 HTTP 프로토콜이 이 시스템에 사용된다. 게다가, 몇몇 방화벽들이 인터넷 액세스들을 검사하고 포트(80)가 HTTP 이외의 프로토콜들에 대해 이용될 때 경고를 발하여 시스템의 프로토콜은 HTTP를 이용할

수 있다.

[0026] 본 발명에 따르면, HTTP 프로토콜은 클라이언트(48)에 의한 요청들 및 클라이언트로 되돌아간 서버(34)로부터의 응답을 위해 시스템에 의해 사용될 수 있다. HTTP에 의해, 단지 클라이언트(48)가 통신을 시작할 수 있고, 그것은 임의의 패러미터 데이터와 함께 클라이언트가 요청하는 동작이 어느 것인지를 식별하기 위해 잘 알려진 HTTP POST를 수행함으로써 이것을 수행한다. 이러한 요청의 포맷 예는:

[0027] POSThttp://[Nomad_module_Path]? [Operation_Code] HTTP/1.1\r\n

[0028] Host: [Host]\r\n

[0029] Content-Length: [Size_of_Encoded_Data]\r\n

[0030] Content-Type : application/x-www-form-urlencoded\r\n\r\n

[0031] [Encoded_Data]

[0032] 서버로부터 클라이언트로의 응답에 있어서, 상기 프로토콜은 다시 HTTP 프로토콜을 모방하고 그래서 우리의 복귀된 데이터는 웹 페이지인 것처럼 보인다. 이러한 응답의 포맷 예는:

[0033] Content-Type: text/html\r\n

[0034] <html><head><title>

[0035] SMF

[0036] </title></head><body>

[0037] [Encoded_Data]

[0038] </bodyX/html>

[0039] 상기 프로토콜에 대한 연산 코드들(상기 요청 포맷 예에서의 [Operation_Code] 변수를 참조하라)은 시스템 프로토콜을 이용하여 요청될 수 있는 다양한 연산들을 지정한다. [Encoded Data]는 클라이언트(48)로부터 수집된 정보를 상기 서버로 제공하고 리소스 액세스 판정을 상기 서버(34)로부터 원격 디바이스(32) 상의 클라이언트(48)로 되돌려 보낸다.

[0040] 도 1를 다시 참조하면, 디바이스(32)가 이하에 특정된 필터링 기능들을 수행하도록 충분한 컴퓨팅 리소스드를 가지는 임의의 컴퓨팅 디바이스이므로 컴퓨터 네트워크로부터 리소스들을 액세스하기 위해 상기 디바이스(32)는 적어도 프로세서, 몇몇 메모리 및 몇몇 메카니즘을 가져야 한다. 예를 들면, 상기 디바이스(32)는 셀룰러 폰, 개인 휴대 단말, 퍼스널 컴퓨터, 랩탑 컴퓨터, 팜탑 컴퓨터, 또는 컴퓨터 네트워크 액세스 등을 달성하는 데 충분한 컴퓨팅 리소스들을 갖는 전기 기기일 수 있다. 따라서, 상기 디바이스는 무선 디바이스들, 셀룰러 전화 디바이스들, 무선 이메일 디바이스들, 무선 개인 휴대 단말 디바이스들, 예컨대 팜 디바이스(Palm device), 트레오 디바이스(Treo device), 림 블랙베이 디바이스(RIM Blackberry device), 유선 퍼스널 컴퓨터, 유선 랩탑 컴퓨터 또는 무선으로 접속된 컴퓨팅 디바이스를 구비할 수 있다. 본 발명에 따르면, 상기 시스템은 다양한 필터링 기능들을 수행할 수 있고 각 디바이스는 반드시 여기에 기술된 필터링 특징들 모두를 지원할 수 있어야 하는 것은 아니다. 예를 들면, 셀룰러 폰은 "허가 및 로그(Allow and Log)"의 오프라인 모드에 요구되는 암호화된 URL들의 리스트를 저장하기에 충분한 메모리를 가지는 않는 경향이 있다. 따라서, 필터링을 수행할 각 디바이스의 필터링 능력을 시스템에 경고하는 것이 바람직하다. 본 발명에 따르면, 성능 마스크가 이러한 목적을 위해 사용될 수 있다. 특히, 디바이스(32)가 상기 시스템에 로그인할 경우, 그것은 상기 디바이스에 대한 성능 마스크를 상기 디바이스가 특정 디바이스 및 그 특성들에 기초하여 제공할 수 있고 및/또는 제공할 수 없는 기능을 서버에게 알리는 서버로 통신할 수 있다.

[0041] 상기 사이트(38)는 컴퓨터 네트워크를 통해 액세스될 수 있는 임의의 리소스들, 예컨대 이메일, 다운로드된 데이터 (PDF 파일들, 텍스트 파일들, 워드 문서들, HTML 파일들, 짚(zip) 파일들 등), FTP 사이트 또는

TELNET 서버를 저장할 수 있다. 본 발명은 클라이언트/서버 아키텍처가 예시 목적으로 도시되었지만 시스템의 임의의 특정 아키텍처(및 시스템내의 컴퓨터들의 관계들)에 제한되지 않는다. 예를 들면, 상기 시스템은 원격 컴퓨터(34) 기능이 분산되어 있는 피어 투 피어 아키텍처(peer-to-peer achitecture)를 이용하여 구현될 수 있다. 게다가, 본 발명은 시스템이 리소스들 또는 임의의 새로운 리소스의 유형 또는 리소스의 유형을 다룰 수 있도록 구성될 수 있기 때문에 리소스들의 임의의 특정 유형에 제한되지 않는다.

[0042] 도 2는 도 1에 도시된 시스템(30)의 예의 추가 상세들을 도시한 도면이다. 이 예에서, 상기 디바이스(32)는 상기 사이트(38)(도 1 참조)에 있는 리소스들을 액세스 할 수 있고 이 예에서는 전형적인 서버 컴퓨터인 컴퓨터(34)에 의해 모니터링되는 퍼스널 컴퓨터이다. 상기 디바이스는 잘 알려진 방식으로 서로 상호접속되는 하나 이상의 프로세서들(40), 영구 저장 디바이스(42) 및 메모리(44)를 포함할 수 있다. 상기 영구 저장 디바이스는 예를 들면 플래시 메모리와 같은 불휘발성 메모리, 하드 디스크 드라이브, 기록가능한 광학 드라이브, 제거가능한 매체 드라이브 또는 디바이스(32)의 전원이 꺼져 있는 동안 데이터 및 명령들의 저장을 허용하는 다른 저장 메카니즘을 포함할 수 있다. 상기 메모리(44)는 예를 들면 SRAM, DRAM 또는 디바이스에 전원이 들어와 있는 동안 프로세서(들)(40)에 의해 실행되는 데이터 및 명령들을 임시 저장하는 다른 구조일 수 있다. 상기 디바이스(32)는 상기 사이트(38) 및 서버(34)를 액세스하기 위한 몇몇 메카니즘(도시하지 않음), 예컨대 유선 접속(예컨대 케이블 모뎀 및 케이블과 같은) 또는 무선 접속 (예컨대 802.11 링크, 셀룰러 링크 또는 GPRS 링크)을 더 포함할 수 있다. 상기 디바이스(32)는 상기 디바이스의 동작 중 상기 메모리(4)에 상주하고 잘 알려져 있는 것과 같이 프로세서(들)(40)에 의해 실행되는 운영 시스템(46)을 더 포함할 수 있다. 본 발명은 임의의 특정 유형의 운영 시스템에 한정되지 않고 다양한 상이한 운영 시스템들로 구현될 수 있다. 본 발명에 따라 필터링 및 모니터링 시스템을 구현하기 위해, 상기 디바이스(32)는 이하에 더 상세히 기술되는 필터링 시스템의 클라이언트 기능들을 수행하도록 프로세서(들)(40)에 의해 실행되고 상기 메모리(44)에 저장되는 클라이언트(48)(이 예에서 복수 라인의 컴퓨터 명령들 및 데이터를 포함하는 소프트웨어 애플리케이션/소프트웨어 모듈로서 도시됨)를 더 구비할 수 있다. 본 발명의 최선의 실시예에서, 클라이언트는 복수 라인의 컴퓨터 코드를 가진 하나 이상의 소프트웨어 모듈들을 더 포함하고 여기서 각 모듈은 필터링 시스템의 상이한 기능들을 수행하고 모듈들의 조합들은 클라이언트 기능들을 구현한다. 상기 클라이언트(48)는 또 예컨대 상기 디바이스(32)에 플러그인되는 플러그-인 매체 카드(plug-in media card)와 같은 혼합된 하드웨어/소프트웨어 디바이스, 또는 ASIC에 임베딩되는 클라이언트를 갖는 ASIC와 같은 하드웨어 디바이스로서 구현될 수 있다. 상기 디바이스(32)의 사용자가 도 1에 도시된 사이트(38) 상의 리소스와 같은 원격 리소스의 액세스를 시도할 경우, 상기 클라이언트(48)는 상기 액세스를 인터셉트하고 본 발명의 일 실시예에서 상기 서버(34)에 나중에 전송될 액세스에 대한 데이터를 수집한다. 상기 클라이언트(48)는 또 리소스 액세스에 대한 데이터를 수집할 수 있고 이 후 본 발명의 다른 실시예에서 액세스 요청 자체에 대한 결정을 내린다. 각 사용자(및/또는 각 디바이스)에 대한 액세스 레벨은 특정 사용자에 맞추어질 수 있다.

[0043] 상기 서버(34)는 잘 알려진 것과 같이 상호 접속된 하나 이상의 프로세서(들)(50), 영구 저장 디바이스(52) 및 메모리(54)를 더 포함할 수 있다. 상기 서버는 본 발명에 따라 필터링 시스템과 연관된 데이터 및 소프트웨어 코드를 저장하는 데이터베이스(56)를 더 포함할 수 있다. 상기 서버는 잘 알려진 운영 시스템(58) 및 이 예에서는 메모리(54)에 상주하는 소프트웨어의 피스(piece)로 나타내고 리소스 액세스 요청들을 처리하고 디바이스(32)가 본 발명의 일 실시예에서 상기 사이트(38) 상의 리소스를 액세스할 수 있는지의 여부를 결정하는 필터링/분류 모듈(filtering/categorization module; 60)을 더 포함할 수 있다. 상기 모듈(60) (바람직하게는 하나 이상의 소프트웨어 모듈들을 포함하는)은 필터링 시스템과 연관된 관리 기능들을 구비하는 필터링 시스템의 상이한 기능들을 구현하고 필터링 작용들과 연관된 데이터베이스에 데이터를 저장하고 요청하기 위해 데이터베이스(56)와 상호 작용할 수 있다.

[0044] 각 디바이스(32)를 고유하게 식별하기 위해, 각 디바이스에는 구성 및 필터링 요청들을 특정 디바이스에 연결하고 특정 디바이스에 대한 필터링 로그들(logs)이 데이터베이스에 저장되도록 허용하는 고유 식별자가 할당된다. 또한, 서버(34)에 대한 각 디바이스(32)에 의한 초기 로그-인과 고유 식별자의 조합은 상기 서버(34)가 필터링 판정들을 수행하고 있을 때 각 리소스 액세스 요청 중 상기 디바이스(32)와 컴퓨터(34) 사이에서 전달될 데이터의 양을 감소시킨다. 본 발명의 이 실시예에서, 상기 필터링 시스템은 실시간으로 원격 리소스로의 디바이스에 의한 액세스의 필터링을 허용하고 여기서 서버는 필터링 판정들을 달성하기 위해 사용된다. 즉, 서버는 상기 시스템의 대부분의 처리 및 메모리 작업로드를 수행하고, 매우 적은 요구가 클라이언트에서 행해진다. 본 발명의 다른 실시예에서, 상기 디바이스는 그 자신의 필터링 판정들을 수행할 수 있다. 특히, 서버가 상기 디바이스에 대해 이용가능하지 않을 경우, 상기 클라이언트는 서버에 의해 지정되는 오프라인 모드로 동작하고, 예를 들면 클라이언트는 상기 액세스들을 로그하고 이후 접속(connectivity)이 다시 확립될 때 서

버로 로그를 업로드한다.

[0045] 도 3은 디바이스(32) 및 서버(34)의 더 상세들을 나타내는 디바이스 리소스 액세스 필터링 및 모니터링 시스템의 클라이언트/서버 실시예의 추가 상세들을 도시한 도면이다. 이 예에서, 상기 디바이스(32)는 전형적인 퍼스널 컴퓨터 상에서 사용될 수 있는 하나 이상의 전형적인 소프트웨어 애플리케이션들, 예컨대 웹 브라우저(70), AOL 브라우저(72), 아웃룩 익스프레스(Outlook Express; 74), 아웃룩(Outlook; 76), FTP 클라이언트(도시하지 않음), 고퍼 클라이언트(Gopher client; 도시하지 않음) 및/또는 뉴스 리더(news reader; 78)를 구비할 수 있다. 원격 리소스의 액세스를 시도하는 이들 전형적인 소프트웨어 애플리케이션들 중 어느 하나를 사용할 때, 원격 리소스 액세스에 대한 정보가 상기 클라이언트(48)에 의해 인터셉트되어 특정 리소스에 대한 액세스가 특정 디바이스에 대해 허용되어야 하는지를 판정하기 위해 상기 서버(34)에 보내질 수 있다. 일 실시예에 있어서, 상기 서버(34) 측 상에서, 상기 서버는 상기 디바이스(32) 상의 상기 클라이언트(48)로부터 데이터를 수신하는 마이크로소프트 인터넷 정보 서버(Internet Information server(IIS); 80)를 더 포함할 수 있다. 본 발명은 IIS를 사용하는 것에 제한되지 않고 다른 방식들로 구현될 수 있다. 상기 IIS 서버(80)는 이후 분류 엔진(84)으로 데이터를 보내는 IIS 플러그-인(82)으로 그 정보를 보낼 수 있다. IIS 플러그-인(82)은 클라이언트 데이터베이스(56a)(최선의 실시예에서 도 2에 도시된 데이터베이스(56)의 일부 또는 별도의 데이터베이스)를 이용하여 상기 디바이스(32)와 연관된 특정 클라이언트를 결정할 수 있고, 여기서 클라이언트-데이터베이스는 관리 모듈(administration module; 86)을 이용하여 유지될 수 있다. 상기 관리 모듈은 예를 들면, 도 7을 참조하여 더 상세히 기술되는 것과 같이 클라이언트 데이터베이스(56a)에 저장될 수 있는 각 클라이언트에 대한 설정들과 함께 원격 디바이스들 상에 설치되는 모든 모니터링된 클라이언트들의 리스트를 포함할 수 있다.

[0046] 상기 IIS 플러그-인(82)은 오프라인 필터링 모듈, 필터링되지 않은 포트들 모듈 및/또는 필터링 감도 모듈을 더 포함할 수 있다. 상기 서버(34)는 이후 오프라인 모드, 필터링되지 않은 포트들 모드 및 특정 클라이언트에 대한 필터링 감도 설정들을 오프라인 필터링, 필터링되지 않은 포트들 필터링 및 필터링 감도 레벨들을 구현하는 클라이언트에 통신할 수 있다. 상기 클라이언트는 오프라인 필터링 모듈, 필터링되지 않은 포트들 모듈 및 필터링 감도 모듈을 포함할 수 있고, 여기서 각 모듈은 클라이언트의 각각의 기능들을 구현하고 각 모듈은 클라이언트가 상주하는 디바이스의 프로세서에 의해 실행되는 컴퓨터 코드의 복수의 라인으로서 구형될 수 있다.

[0047] 상기 분류 엔진(84)은 룰스 관리 모듈(88)에 의해 유지될 수 있는 룰스 데이터베이스(56b)(최선의 실시예에서 도 2의 데이터베이스(56)의 일부 또는 별도의 데이터베이스)로부터 분류 룰스(분류 룰들)를 꺼내 올 수 있다. 룰스 관리 모듈(88)은 또 도 8를 참조하여 이하에 더 상세히 기술되는 새로운 룰(rule)을 생성하는 데 사용될 수 있다. 분류 엔진은 그 결과들을 모니터 모듈(90)에 의해 유지되는 모니터 데이터베이스(56c)(최선의 실시예에서 도 2의 데이터베이스(56)의 일부 또는 별도의 데이터 베이스)에 저장할 수 있다. 상기 모니터 모듈(90)은 예를 들면, 각 클라이언트 또는 모든 클라이언트들의 웹 서핑 습관에 대한 정보를 수집 및 디스플레이할 수 있다. 상기 모니터 모듈(90)은 또 접속이 요청되었을 때 모니터링 시스템의 사용자가 디바이스들의 원격 사용자를 위한 인터넷 접속들을 보여주도록 허용하는 실시간 모니터 모듈(도시하지 않음)을 구비할 수 있다. 본 발명에 따르면, 분류 엔진은 하나 이상의 데이터 피스에 기초하여 특정 정보 요청을 분류할 수 있다. 정보 요청은 우선 상기 디바이스에 의해 액세스될 사이트 어드레스에 기초하여 분류될 수 있다. 상기 분류 엔진은 또 1) 디바이스의 호스트명 또는 서버측 구성가능 대체명(상기 디바이스가 호스트명을 가지지 않을 경우); 및/또는 상기 디바이스의 현재 사용자명 또는 서버측 구성가능한 대체명(사용자명을 가지지 않는 디바이스들에 대해)을 사용할 수 있다. 따라서, 분류 기준(및 그러므로 액세스가능한 리소스들)은 특정 디바이스/사용자에 대해 구성가능하다. 예를 들면, 액세스의 레벨은 컴퍼니내의 피고용자의 선임권(seniority) 또는 상태에 기초하여 변할 수 있다. 관리자 모듈(도시하지 않음)은 사용자가 서버상에서 자동으로 일어날 수 있는 이벤트들, 예컨대 데이터베이스 업데이트들, 데이터베이스 유지보수 태스크들 등을 설정할 수 있게 허용하는 스케쥴러를 구비할 수 있다. 상기 관리자 모듈은 또 사용자가 사이트를 분류/재분류할 수 있게 허용한다. 가상 제어 에이전트(virtual control agent)(도시하지 않음)는 카테고리를 가지지 않은 사용자에 의해 액세스된 사이트들을 자동으로 방문하고 분류하기 위해 인공 지능을 사용하는 선택 모듈이다. 상기 관리자 모듈은 또 웹 레포팅 모듈을 가지며 그 결과 상기 시스템은 클라이언트 데이터 및 서핑 습관들에 대한 리포트들을 발생할 수 있다. 다양한 원격 컴퓨터(34) 모듈 각각은 본원에 기재된 기능들을 구현하는 복수의 라인들의 코드를 갖는 소프트웨어의 피스일 수 있다.

[0048] 도 4는 본 발명의 디바이스 클라이언트/서버 실시예의 서버 부분(34)의 추가 상세들을 도시한 도면이고, 도 5는 본 발명의 상기 디바이스 클라이언트/서버 실시예의 디바이스(32) 부분의 추가 상세들을 도시한 도면이다.

도 4에 도시된 것과 같이, 상기 서버(34)의 구현이 도시되고 여기서 SQL 데이터베이스는 상기 시스템 및 웹 필터 룰스들 엔진 서비스를 위한 데이터를 저장하기 위해 사용된다. 본 발명에 따른 필터링 룰의 예 및 어떻게 룰이 생성되는 가에 대해서는 도 8를 참조하여 이하에 더 상세히 설명된다. 도 5에 도시된 것과 같이, 상기 디바이스 상의 상기 클라이언트(48)는 사용자 인터페이스 부분(100), 클라이언트 통신 계층(102), 네트워크 인터셉터 계층(104) 및 이하에 기술되는 것과 같은 특정 클라이언트(48)에 대한 구성들 및 임의의 로그 파일들을 저장하는 저장 매체(106)를 더 포함한다. 최선의 실시예에 있어서, 이들 부분들 및 계층들 각각은 상기 디바이스의 프로세서에 의해 실행되는 소프트웨어의 피스이다. 사용자 인터페이스 부분(100)은 사용자에게 디스플레이되는 모니터링 시스템의 사용자 인터페이스를 발생하고 구성 사용자 인터페이스 스크린들(configuration user interface screens)을 구비할 수 있다. 상기 네트워크 인터셉터 계층(104)은 외부 사이트로의 리소스 액세스 요청으로부터 데이터를 수집할 수 있고, 클라이언트 통신 계층(102)은 그 데이터를 상기 서버(34)로 전송하고 서버의 리소스 액세스 판정을 수신하고 그 판정을 구현하기 위한 포맷으로 포맷할 수 있다.

[0049] 본 발명에 따른 상기 시스템의 정상 동작 중, 상기 디바이스는 아마존 닷 컴(Amazon.com)으로부터의 웹 페이지와 같은, 원격 사이트 상의 리소스에 대한 리소스 액세스 요청을 개시할 수 있고, 상기 클라이언트(48)는 사이트 어드레스와 같은 그 요청과 연관된 데이터를 캡쳐한다. 상기 클라이언트는 또 상기 디바이스 식별자 및 다른 디바이스 데이터를 수집하고 이 후 리소스 액세스 요청 데이터를 상기 서버(34)로 전송할 수 있다. 상기 서버는 이후 리소스 액세스 요청 데이터에 기초하여, 분류/필터링 판정을 행하여 리소스 액세스 판정을 발생하고 이후 상기 리소스 액세스 판정을 상기 클라이언트(48)로 되돌려 보내서 상기 클라이언트는 적절한 동작들을 취할 수 있다. 따라서, 상기 원격 서버는 상기 디바이스(32)의 리소스 액세스 요청들의 실시간 모니터링 및 필터링을 수행할 수 있다. 그러나, 상기 서버(34)가 상기 디바이스에 대해 이용가능하지 않다면(어떠한 이유로), 이 때 상기 디바이스는 오프라인 필터링을 수행할 수 있고 여기서 상기 디바이스(32)는 그 자신의 모니터링 및 필터링을 담당한다. 상기 디바이스(및 그러므로 클라이언트)가 서버에 접속할 수 없을 때, 클라이언트가 인터넷에 접속되어 있는 동안 예컨대 5분마다 규칙적으로 재접속을 시도할 것이다.

[0050] 오프라인 필터링 중, 상기 디바이스/클라이언트는 상기 서버에 의해 특정 클라이언트의 구성에 기초하여 상이한 동작 모드로 동작할 수 있다. 예를 들면, 상기 클라이언트(48)는 모든 인터넷 액세스들을 허용하지만, 각 리소스 액세스 요청을 나중에 서버로 업로드될 수 있는 로컬 로그 파일("Log & Allow" 모드)로 로그할 수 있다. 대안으로, 클라이언트는 모든 인터넷 액세스("Block All" 모드)를 차단할 수 있고 또는 로그인이 없는("Allow All" 모드) 모든 인터넷 액세스를 허용할 수 있다. 본 발명에 따르면, 클라이언트 상에 기록된 상기 오프라인 로그들은 위에 기술한 것과 같은 메모리 또는 영구 저장 디바이스와 같은 상기 디바이스의 로컬 저장장치에 저장될 수 있다. 만약 로그가 서버에 나중에 업로드되면, 로그 파일은 이후 상기 디바이스 상에서 삭제될 수 있다. 최선의 실시예에 있어서, 로그 파일은 암호화될 수 있다. 상기 로그 파일은 클라이언트의 허가되지 않은 탬퍼링(unauthorized tampering)을 검출하기 위해 몇몇 기본 모니터링 능력을 더 구비할 수 있다. 본 발명에 따르면, 오프라인 로그 업로딩이 대역폭 스로틀링을 구비하여 서버가 온라인으로 다시 돌아왔을 때, 그들의 로그들을 서버로 업로드하려고 하는 모든 다수의 클라이언트들에 의해 오버로드되지 않는다.

[0051] 본 발명에 따르면, 상기 서버는 시스템 관리자, 예컨대 회사의 치프 정보 사무관(Chief Information Officer) 또는 클라이언트 자신(자동화 알고리즘을 사용하는)이 본 발명에 따른 필터링 및 모니터링 동작을 조정할 수 있게 허용하는 관리자 모듈(86)을 구비할 수 있다. 예를 들면, 각 디바이스를 위한 상기 시스템의 필터링 감도(인터넷 액세스들이 특정 디바이스에 대해 필터링되는 레벨)가 맞춰지고/조정되어 필터링되는 인터넷 트래픽의 양이 모니터링 및 필터링 동작들에 전용되는 디바이스의 대역폭 양을 감소시키는 특정 디바이스에 대해 감소될 수 있다. 예를 들면, 느린 인터넷 접속을 갖는 디바이스, 예컨대 셀룰러 폰용 GPRS는 조정된 감도를 가질 수 있다. 본 발명에 따르면, 임의의 디바이스에 대한 필터링 감도는 상기 디바이스의 임의의 특정 특징들에 기초하여 조정될 수 있다. 상기 시스템의 최선의 실시예에 있어서는 높은 필터링 레벨, 중간 필터링 레벨, 낮은 필터링 레벨 및 자동 필터링 레벨이 있을 수 있다. 높은 필터링 감도 레벨에서, 상기 시스템이 예를 들면, 모든 난-하이퍼텍스트 전송 프로토콜 (HTTP) 포트들 및 모든 HTTP 요청들을 필터링할 수 있어 이러한 설정은 예를 들면 팝업 애드들(pop-up ads)을 포함해서 모든 리소스들을 필터링할 수 있다. 높은 필터링 감도는 매우 철저한 필터링을 제공하지만, 디바이스가 많은 리소스 액세스 요청들을 하고 있으면 필터링 속도 및 성능에 영향을 줄 수 있다. 중간 레벨의 감도에서, 모든 난-HTTP 포트들이 분류되지만, HTTP 페이지 요청들만이 분류되며 이미지 파일들, 사운드 파일들, 스타일 시트들(style sheets) 및 XML 요청들은 분류되지 않는다. 낮은 감도 레벨에서, 모든 난-HTTP 포트들이 분류되지만, HTTP 요청의 상기 서버 어드레스 부분만이 분류되고 그 결과들이 매우 짧은 시간동안 캐시될 수 있다. 자동 레벨의 감도에서, 클라이언트는 평균 서버 응답 시간

(응답 레이턴시: response latency) 및 미리 구성된 임계치들에 기초하여 고, 중, 저 레벨을 선택한다. 자동 모드에서, 상기 클라이언트는 감도를 조정하는 코드의 피스를 구비할 수 있다. 예를 들면, 고 레벨은 상기 응답 레이턴시가 미리 정해진 시간 기간 미만인 동안 사용되며 이후 중간 레벨로 리셋될 수 있다.

[0052] 본 발명에 따르면, 상기 시스템은 모든 TCP/IP 포트들을 필터링할 수 있고 여기서 포트들의 몇몇은 상기 사이트(38)에서 리소스에 직접 행해지거나 프록시 서버를 통해 행해지는 HTTP 웹 요청들로서 취급된다. 특정 컴퓨니가 필터링 또는 모니터링에 관심이 없는 포트들에 대한 디바이스 액세스를 위한 서버와의 불필요한 통신을 감소시키기 위해, 상기 디바이스(32)는 어느 포트들이 상기 서버에 통신될 것인가 그리고 이들 포트들 중 어느 것이 HTTP 웹 요청들로서 취급될 것인가를 (서버에 의해) 알려질 수 있다. 따라서, 상기 서버는 특정 컴퓨니에 대해 필터링되지 않은 포트들(서버에 통신될 포트들의 리스트)과 함께 구성될 수 있다. 본 발명에 따르면, HTTP 요청들로서 필터링 및/또는 취급할 포트들의 리스트는 상기 디바이스의 로그인 과정 중 디바이스에 통신된다. 상기 클라이언트는 이후 상기 디바이스 상에서 실행하는 애플리케이션이 필터링되지 않은 포트의 액세스를 시도할 경우 취해지는 자동 동작인 필터링되지 않은 포트 동작을 수행할 수 있다. 현재의 구현 및 상기 시스템의 일 실시예에 있어서, HTTP 포트들 및 필터링 포트들의 리스트는 상기 서버 소프트웨어로 하드코딩된다. 본 발명의 다른 실시예에 있어서, 상기 서버는 룰들의 세트/리스트(조정/맞추어질 수 있는)를 분석하고 모니터링된 포트들의 리스트는 상기 룰들로부터 자동으로 발생된다. 필터링되지 않은 동작들은 예를 들면 이들 포트 요청들 모두가 허용되는 허가 올 옵션(allow all option)("Allow All" 모드), 모든 필터링되지 않은 포트들에 대한 액세스가 차단되는 블록 올 옵션(block all option)("Block All" 모드) 및 포트 요청이 전형적인 웹 필터에서 모든 포트들에 보통 영향을 주는, 예컨대 성인 컨텐트로부터 모든 사람을 차단하는 룰스에 유용한 상기 서버로 통신되는 필터 옵션(filter option)("Filter" 모드)을 구비할 수 있다.

[0053] 도 6A 및 도 6B는 본 발명에 따른 필터링 시스템의 설치의 2가지 상이한 예들이다. 각 설치에 있어서, 상기 서버(34)는 상기 디바이스들(32)(클라이언트들을 갖는)이 TCP 포트(80)를 통해 서버에 액세스할 수 있도록 위치된다. 도 6A에 있어서, 상기 서버(34)는 메인 보호 네트워크(112) (내부 컴퓨팅 디바이스들(114)를 갖는) 외부에 위치되고 도시된 브리지/라우터/방화벽 디바이스(110)를 통해 회사 네트워크에 접속되어 상기 디바이스들(32)이 상기 서버(34)를 액세스할 수 있다. 도 6B에 도시된 예에 있어서, 상기 서버(34)는 네트워크(112) 내에 위치될 수 있고 이때 방화벽(110)은 트래픽이 서버(34)에 관련되는 한 TCP 포트(80)에 대한 트래픽을 허용하도록 구성될 수 있다. 양자의 경우에 있어서, 상기 디바이스(32)는 상기 서버(34)와 통신할 수 있고 그러므로 상기 서버는 원격 모니터링 및 필터링 동작들을 수행할 수 있다.

[0054] 도 7은 클라이언트 관리자 모듈의 예시적인 구현을 위한 사용자 인터페이스(120)의 예를 나타낸다. 상기 관리자는 상기 시스템에 대한 주 관리 지위에 있고 각 원격 디바이스의 주문 가능한 설명 및 각 특정 디바이스에 대한 설정들을 제공한다. 상기 사용자 인터페이스(120)는 요약 부분(122) 및 클라이언트 상세 부분(124)을 포함하고 여기서 상기 요약 부분(122)은 상기 시스템 (이 예에서는 간단히 하기 위해 하나만 도시되어 있음)에 현재 들어가거나 로그인된 모든 클라이언트를 나열한다. 관리자 모듈의 사용자가 요약 부분으로부터 특정 클라이언트를 선택하면, 클라이언트 상세 부분(124)은 특정 클라이언트 및 클라이언트가 실행되고 있는 디바이스에 대한 상세 설정 및 다른 정보를 나타낸다. 상기 클라이언트 상세 부분(124)은 또한 클라이언트 정보 부분(126) 및 클라이언트 설정 부분(128)을 구비할 수 있고 여기서 상기 클라이언트 정보 부분은 특정 선택된 클라이언트/디바이스에 대한 정보를 나열하고 상기 클라이언트 설정 부분은 관리자가 특정 클라이언트/디바이스에 대한 필터링/모니터링의 설정들을 조정/세트/리세트할 수 있게 허용한다. 클라이언트 정보 부분에 나타낸 것과 같이, 각 클라이언트는 각 클라이언트에 대한 설정들이 데이터베이스에 저장될 수 있도록 각 클라이언트를 고유하게 식별하는 고유 식별번호(도 7에 도시된 클라이언트 Id)를 가진다.

[0055] 클라이언트 설정 부분(128)에 있어서, 상기 관리자는 예를 들면, 오프라인 동작 설정(130), 필터링되지 않은 포트들 설정(132), 필터 감도 설정(134), 사용자명 설정(136) 및 호스트명 설정(138)을 포함한 다양한 필터링 및 모니터링 설정들을 설정할 수 있다. 상기한 바와 같이, 오프라인 동작 설정(130)은 상기 서버가 클라이언트에 대해 이용가능하지 않게 될 때 클라이언트가 어떻게 동작할 것인지의 옵션을 관리자가 선택할 수 있게 허용하고 오프라인 동작들은 최선의 실시예에 있어서, "모두 허가(Allow All)", "모두 차단(Block All)" 또는 "로그 및 허가(Log and Allow)"로부터 선택될 수 있다. 상기 필터링되지 않은 포트들 설정(132)은 필터링된 포트들에 포함되지 않은 포트들이 상기 디바이스의 사용자에 의해 액세스될 때 특정 클라이언트가 행동해야할 방법을 관리자가 세트할 수 있게 허용한다. 본 발명의 최선의 실시예에 있어서, TCP 포트들의 선택된 리스트는 상기 클라이언트와 상기 서버 사이의 총 트래픽을 감소시키기 위해 모니터링되도록 선택된다. 모니터링되는 포트들의 실제 선택은 관리자 모듈을 이용하여 수정될 수 있다. 디폴트 TCP 포트들의 리스트는 예를 들면

다음의 표에 나타낸 것을 포함할 수 있다:

[0056]

포트	애플리케이션	수
HTTP	웹 트래픽	80, 8000, 8080
HTTPS	보안 웹 트래픽	443
FTP	파일 전송	21
NNTP	뉴스 그룹들	119
POP3	이메일(수신)	110
SMTP	이메일(송신)	25
AOL	아메리칸 온라인	11523

[0057] 따라서, 관리자에 의해 필터링되고 모니터링된 포트들에 추가되는 것으로 특정되지 않은 임의의 포트에 대해, 필터링되지 않은 포트들 설정이 적용될 것이다. 상기한 바와 같이, 필터링되지 않은 포트 선택들은, 최선의 실시예에서, 모두 허가(Allow All), 모두 차단(Block All) 및 필터 모드들을 포함할 수 있다. 필터 감도 설정(134)은 관리자가 클리언트에 대한 필터링의 감도 레벨을 설정할 수 있게 허용한다. 상기한 바와 같이, 상기 선택들은 최선의 실시예에서, 높은 필터링 레벨, 중간 필터링 레벨, 낮은 필터링 레벨 및 자동 필터링 레벨을 포함할 수 있다.

[0058] 일반적으로, 상기 필터링 룰들은 사용자명 또는 호스트명에 기초할 수 있다. 따라서, 사용자명이 룰에 의해 지정되면, 이 때 사용자에 의해 사용되는 디바이스와 상관없이, 사용자 필터링 룰들이 적용된다. 호스트명이 룰에 지정되면, 이 때 어느 사용자가 특정 디바이스에 로그인하는가와는 상관없이 상기 호스트명에 기초한 룰들이 그 특정 디바이스에 적용된다. 따라서, 사용자명 설정(136)은 관리자가 특정 디바이스에 적용되는 사용자를 설정할 수 있게 허용한다. 이 사용자명은 클라이언트 디바이스에 대한 모든 필터링 결정들을 위해 상기 서버에 의해 사용된다. 상기 이름은 이 후 특정 클라이언트 사용자에 대해 적절한 필터링을 결정하기 위해 룰스 데이터베이스내의 룰들에 대해 체크하기 위해 사용될 수 있다. 사용자명 설정은 최선의 실시예에 있어서, 관리자가 클라이언트 지정명 모드, 서버 오버라이드 모드 또는 서버 디폴트 모드로부터 선택할 수 있게 허용한다. 클라이언트 지정 모드에 있어서, 사용자가 클라이언트를 실행하는 디바이스로 로그인하면, 상기 클라이언트는 서버에 사용자명으로서 사용되는 사용자 로그인명을 전송한다. 상기 서버 오버라이드 모드에 있어서, 상기 관리자는 조직에 대한 필터링 룰들이 특정 사용자에게 적용되도록 사용자를 개체로서 구체적으로 정의하지 않고, 엔지니어, 비서, 모바일 피고용인 등과 같이 조직의 구성원으로서 이러한 사용자를 식별하기 위해 이름을 지정할 수 있다. 예를 들면, 컴퍼니는 여행 보험 판매원에 대해 사용되는 모바일 디바이스들의 컬렉션(collection)을 가질 수 있고, 이들 모바일 디바이스들을 사용하는 어떠한 사람이라도 이들의 개개의 사용자명보다는 오히려 "판매원(salesman)의 역할에 따라 필터링되어야 한다. 그러므로, '판매원'에게 일에 필요한 특정 사이트들로 들어갈 수 있게 허용하는 룰들이 생성될 수 있다. 이러한 모드는 또 클라이언트가 이동 전화와 같은 사용자명을 제공할 수 없을 때 사용될 수 있다. 상기 서버 디폴트 모드가 클라이언트 지정 모드 및 서버 오버라이드 모드가 사용되지 않을 때 사용되어 상기 디바이스는 여전히 어떤 레벨에서 필터링될 수 있다. 상기 호스트명 설정(138)이 실제 디바이스(상기 디바이스의 사용자와는 대조적으로)를 지정하여 상기 디바이스를 이용하는 개체와 관계없이 디바이스들의 그룹에 대한 필터링 룰들에 따라 디바이스들 또는 디바이스들의 그룹들(특별한 특징을 갖는)이 함께 그루핑되고, 인식되고 필터링된다. 상기 호스트명 설정들은, 최선의 실시예에서, 관리자가 클라이언트 지정 호스트명 모드, 서버 오버라이드 모드 및 서버 디폴트 모드로부터 선택할 수 있게 허용한다. 클라이언트 지정 모드에 있어서, 디바이스의 클라이언트는, 상기 사용자가 상기 디바이스를 로그인하면, 상기 디바이스의 네크워크명을 서버에 제공한다. 상기 서버 오버라이드 모드에서, 상기 호스트명은 호스트명을 공급할 수 없는 예컨대 모바일 전화와 같은 디바이스들에 유용한 그룹의 구성원으로서 상기 디바이스를 식별하기 위해 사용된다. 상기 서버 디폴트 모드에 있어서, 상기 디바이스가 여전히 어떤 레벨에서 필터링될 수 있도록 이것은 클라이언트 지정 모드 및 서버 오버라이드 모드가 사용되지 않을 때 사용

되는 호스트명이다.

[0059] 도 8은 룰스 관리자 모듈의 구현을 위해 사용자 인터페이스(150)의 예를 나타낸다. 룰스 관리자는 상기 시스템의 허가된 사용자가 하나 이상의 필터링 룰들을 생성할 수 있게 허용한다. 상기 사용자 인터페이스는 각 룰의 상이한 특징들/설정들, 예컨대 룰의 유형, 룰이 적용되는 사용자/디바이스, 룰이 적용되는 컨텐트의 유형, 상기 룰에 대한 임계치 및 디스플레이의 상이한 컬럼에 배열된 룰의 통지 특징과 함께 각 룰(152)을 행으로서 디스플레이에 나타낸다. 룰들의 유형들은 ALLOW (룰에 의해 지정된 컨텐트를 허용), DISALLOW (룰에 의해 지정된 컨텐트를 허용하지 않음) 또는 THRESHOLD (임계값들 내에 있으면 룰에 의해 지정된 컨텐트를 허용)를 구비한다. 임계치 룰들에 있어서, 룰에 의해 지정된 사용자는 예를 들면 설정된 시간 기간 동안 인터넷을 액세스하도록 허용될 수 있다. 각 룰에 있어서, 상기 관리자는 룰이 필터링 동작들 중 적용되는 클라이언트들/디바이스들 또는 클라이언트들 또는 디바이스들의 그룹들을 지정할 수 있다. 각 룰에 있어서, 상기 관리자는 필터링될 컨텐트의 유형을 지정할 수 있다. 예를 들면, 도 8에 도시된 것과 같이, 비록 룰이 어떤 유형의 컨텐트라도 필터링할 수 있도록 하기 위해 생성되며 어떤 유형의 컨텐트도 상기 시스템에 부가될 수 있어 새로운 유형의 컨텐트가 미래에 필터링될 수 있지만, 상기 컨텐트는 성인/성적으로 노골적인, 여행(travel), 갬블링(gambling), 실행가능한 것 등등일 수 있다. 각 룰은 룰이 적용되는 시간, 예컨대 언제든지(ANYTIME), 일과후 및 주말, 일과시간 등을 지정하며, 여기서 상이한 시간 기간들이 새로운 이름 및 사용자에 의해 지정된 시간 기간이 주어질 수 있다. 각 룰은 또 상기한 것과 같은 임계치 및 특정 컨텐트가 사용자에 의해 액세스될 때 상기 시스템에서 통지를 받는 사람을 지정하는 통지 특징을 가질 수 있다.

[0060] 본 발명에 따르면, 룰 관리자에 의해 발생된 상기 필터링 룰들은 하루 중 어떤 시간에 인터넷의 어떤 분야를 액세스할 수 있는 사람을 통제할 수 있다. 상기 룰들은 긍정적(사이트들, "성적으로 노골적인"과 같은 사이트들 또는 리소스들의 카테고리에 대한 액세스를 허용) 또는 부정적(사이트들, 사이트들 또는 리소스들의 카테고리에 대한 액세스를 거절)일 수 있다. 일반적으로, 각 룰은 각 필터링 룰의 상이한 특징들을 특정하는 유형(Type), 누가(Who), 어디서(Where), 언제(When), 통지(Notify), 임계치(Threshold) 및 HTTP 거절 오브젝트들(HTTP Deny objects)(이들 중 몇몇만이 도 8에 도시됨)을 포함할 수 있다. 상기 유형(Type) 오브젝트는 상기 룰이 허용, 불허 또는 임계 룰인 때를 지정하는 데이터를 포함한다. 누가(Who) 오브젝트는 룰이 적용될 수 있는 개체를 지정하는 데이터를 포함하고, 여기서 상기 오브젝트는 개체, 사람의 그룹, 누구나, 아무도 등등을 지정할 수 있다. 어디(Where) 오브젝트는 상기 요청된 리소스의 출처(origin)(예컨대 웹 사이트)를 지정하는 데이터를 포함하지만, 또한 예를 들면 "성적으로 노골적인(Sexually explicit)" 또는 "ftp"와 같은 사이트들의 카테고리를 지정할 수 있다. 언제(When) 오브젝트는 리소스 요청이 허용되거나 부정되는 시간 및/또는 일자들을 지정하는 데이터를 포함한다. 통지(Notify) 오브젝트는 특정 리소스 요청이 그 룰을 트리거할 때, 예컨대 이메일에 의해 통지될 수 있는 하나 이상의 개체들을 지정하는 데이터를 포함한다. 임계치(Threshold) 오브젝트는 특정 시간 기간 동안 서핑하는 데 소비된 시간 및 데이터의 양의 한계를 지정하는 데이터를 포함한다. HTTP 거절 오브젝트는 상기 룰이 트리거될 때 특정 유형의 거절 페이지((거친(harsh), 강한 또는 부드러운)가 사용자에게 보내진 것을 지정하는 데이터를 포함한다. 각각의 새로운 룰에 있어서, 룰들 관리자는 사용자가 정보를 입력하고 드롭 다운 메뉴들(drop down menus)을 이용함으로써 룰의 이들 특징들을 지정할 수 있게 허용한다.

[0061] 본 발명에 따르면, 상기 시스템은 회사 네트워크로부터 떨어진 디바이스들을 필터링한다. 특정 디바이스가 회사 네트워크로 다시 전이하고, 예컨대 랩톱이 도로 위에서 사용되고 이후 회사 네트워크로 다시 플러그인 될 경우, 회사 네트워크의 필터링 정책(예를 들면 정적 피고용인들에 대한)이 그것이 회사 네트워크 내에 있는 한 특정 디바이스에 대해 사용되는 것이 바람직하다. 본 발명에 따르면, 클라이언트는 회사 네트워크 필터링 정책이 사용될 수 있도록 회사 네트워크를 통해 통신될 이들 리소스 요청들에 대한 클라이언트 필터링 기능들을 디스에이블링하기 위해 상기 디바이스의 특정 리소스 요청이 회사 네트워크(예컨대 클라이언트가 있는 디바이스가 회사 네트워크에 접속되어 있을 때)를 통해 통신될지의 여부를 검출하는 소프트웨어 모듈을 구비할 수 있다. 다른 예로서, 디바이스는 회사 네트워크에 접속될 수 있지만 또한 무선 모뎀에 접속될 수 있고 클라이언트 필터링이 무선 모뎀을 통해 통신되는 리소스 요청들에 사용될 수 있지만 회사 네트워크를 통해 통신되는 리소스 요청들에 대해서는 사용되지 않을 수 있다.

[0062] 이상 일부 최선의 실시예들이 도시되고 기술되었지만, 이 기술분야에서 숙련된 사람은 다양한 변경예들 및 변형예들이 첨부 청구항들에 정의된 것과 같은 본 발명의 범위를 벗어나지 않고 만들어질 수 있다는 것을 알 수 있을 것이다. 주의할 점은 이 출원과 관련하여 본 명세서와 동시에 또는 이전에 출원되고 이 명세서와 함께 공람된 모든 논문 및 문서와 관련이 있고, 이와 같은 논문 및 문헌의 내용은 본원에 참조문헌으로서

포함된다.

[0063] 이 명세서(임의의 첨부 청구항들, 요약 및 도면들을 포함)에 개시된 특징들 모두 및/또는 그렇게 개시된 임의의 방법 또는 공정 단계들 모두는 적어도 이와 같은 특징들 및/또는 단계들의 몇몇이 서로 배제되는 조합들을 제외하고, 임의의 조합으로 결합될 수 있다.

[0064] 이 명세서(임의의 첨부 청구항들, 요약 및 도면들을 포함)에 개시된 각 특징은 달리 일부러 언급하지 않는 한, 동일, 등가 또는 유사한 목적으로 작용하는 다른 특징들로 대체될 수 있다. 따라서, 달리 일부러 언급하지 않는 한, 개시된 각 특징은 포괄적인 등가물의 시리즈 또는 유사한 특징들의 단지 일예이다.

[0065] 본 발명은 상기 실시예(들)의 상세들로 제한되지 않는다. 본 발명은 이 명세서(임의의 첨부 청구항들, 요약 및 도면들을 포함)에 개시된 특징들의 임의의 신규의 하나 또는 임의의 신규의 조합 또는 이와 같이 개시된 임의의 방법 또는 공정의 단계들의 임의의 신규의 하나 또는 임의의 신규의 조합으로 확대할 수 있다.

도면의 간단한 설명

[0015] 도 1은 본 발명에 따른 디바이스 리소스 액세스 필터링 및 모니터링 시스템의 예를 나타낸 도면.

[0016] 도 2는 도 1에 도시된 디바이스 리소스 액세스 필터링 및 모니터링 시스템의 추가 상세들을 나타낸 도면.

[0017] 도 3은 디바이스 및 서버를 더욱 상세하게 나타낸 디바이스 리소스 액세스 필터링 및 모니터링 시스템의 클라이언트/서버 실시예의 추가 상세들을 나타낸 도면.

[0018] 도 4는 도 3의 시스템의 서버 부분의 추가 상세들을 나타낸 도면.

[0019] 도 5는 도 3의 시스템의 클라이언트 부분의 추가 상세들을 나타낸 도면.

[0020] 도 6A 및 도 6B는 본 발명에 따른 디바이스 리소스 액세스 필터링 및 모니터링 시스템의 설치(installation)의 2가지 상이한 예들을 나타낸 도면.

[0021] 도 7은 상기 시스템의 클라이언트 관리자 모듈의 예시적인 구현을 위한 사용자 인터페이스의 예를 나타낸 도면.

[0022] 도 8은 상기 시스템의 룰스 관리자 모듈(rules administrator module)의 구현을 위한 사용자 인터페이스의 예를 나타낸 도면.

도면

도면1

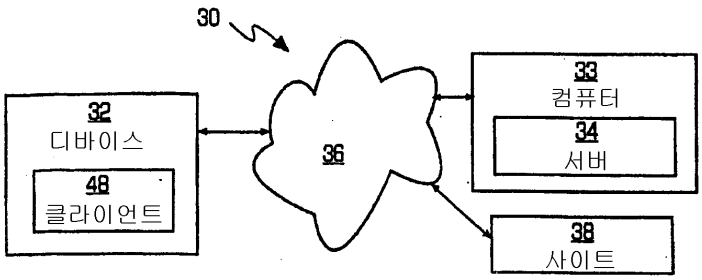

FIG. 1

도면2

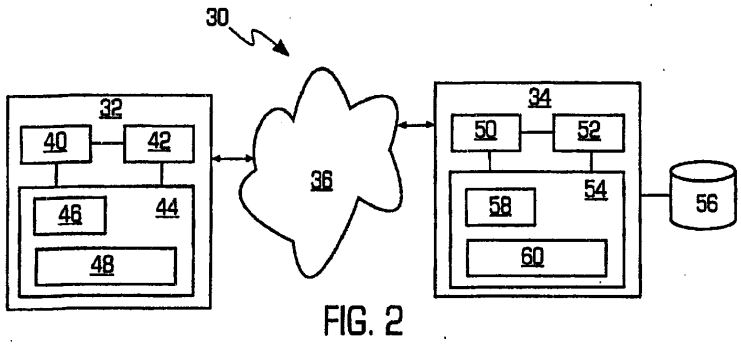

FIG. 2

도면3

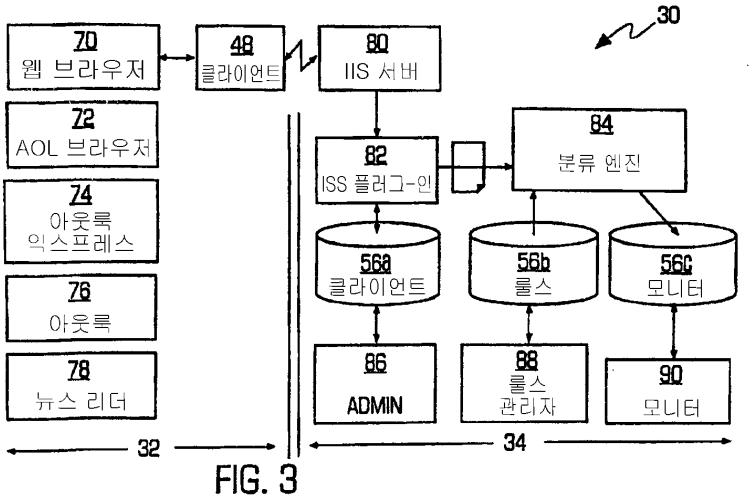

FIG. 3

도면4

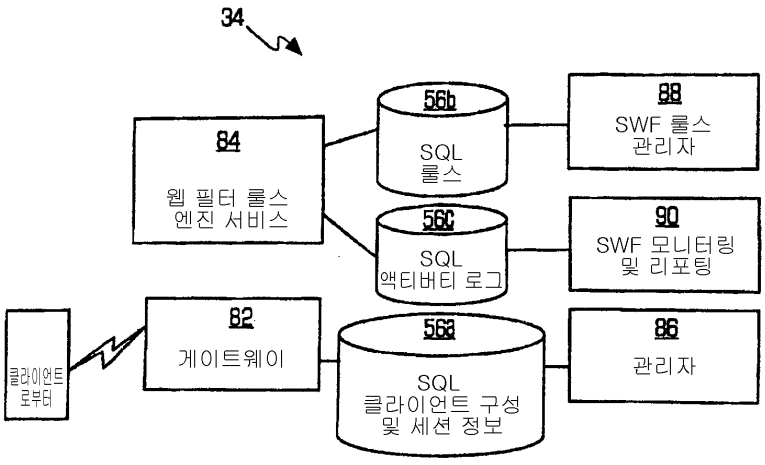

FIG. 4

도면5

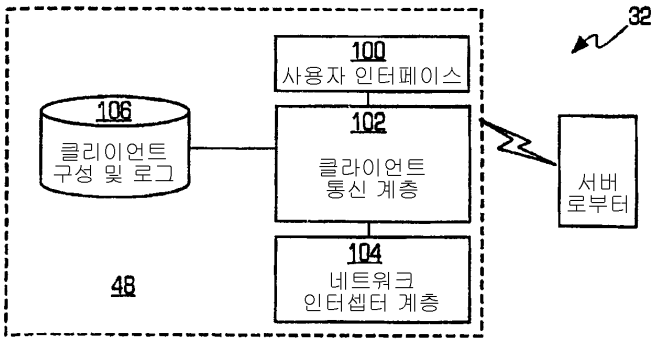

FIG. 5

도면6A

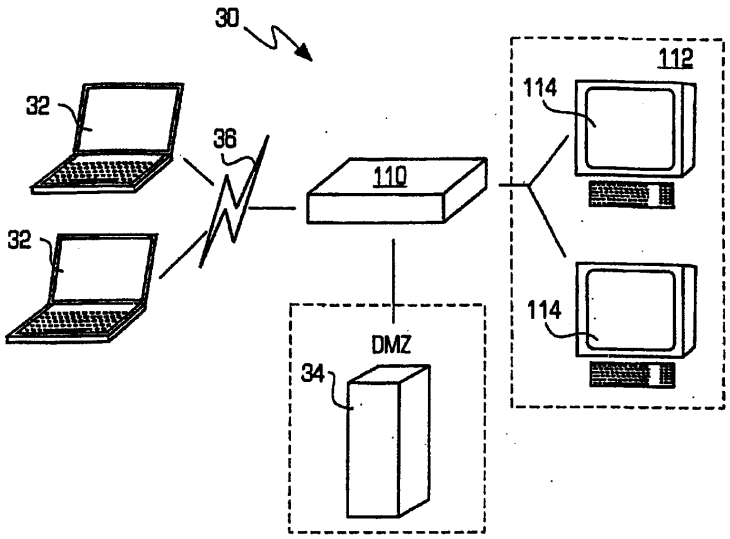

FIG. 6A

도면6B

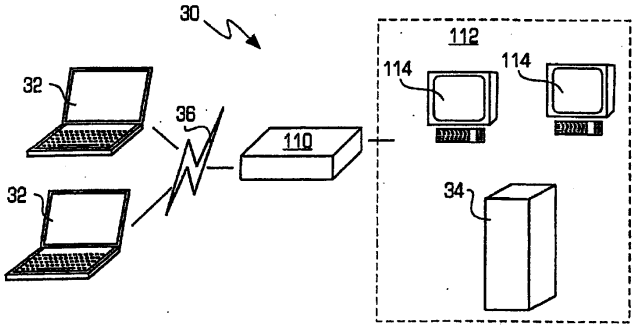

FIG. 6B

도면7

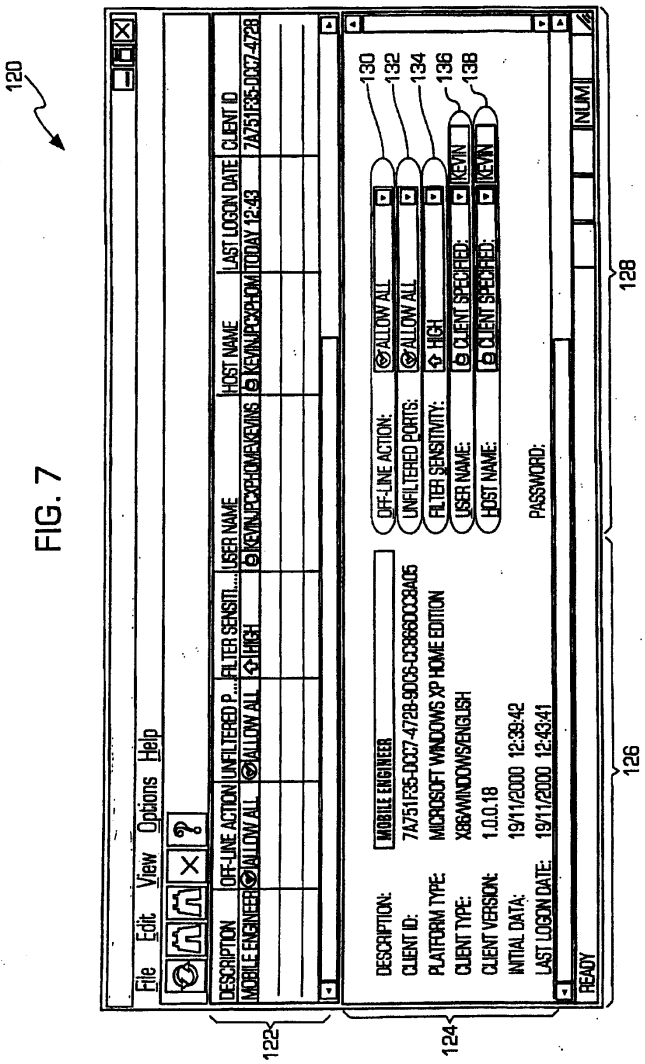
120
File Edit View Options Help
DESCRIPTION
OFF-LINE ACTION
UNFILTERED P...
FILTER SENSIT...
USER NAME
HOST NAME
LAST LOGON DATE
CLIENT ID
MOBILE ENGINEER
ALLOW ALL
ALLOW ALL
HIGH
KEVIN
KEVIN-PC
KEVIN-PC
TODAY 12:43
7A7516
122
DESCRIPTION:
MOBILE ENGINEER
CLIENT ID:
7A7516
PLATFORM TYPE:
MICROSOFT WINDOWS XP HOME EDITION
CLIENT TYPE:
X86/WINDOWS/ENGLISH
CLIENT VERSION:
1.0.0.18
INITIAL DATA:
19/11/2000 12:39:42
LAST LOGON DATE:
19/11/2000 12:43:41
124
OFF-LINE ACTION:
ALLOW ALL
UNFILTERED PORTS:
ALLOW ALL
FILTER SENSITIVITY:
HIGH
USER NAME:
CLIENT SPECIFIED:
KEVIN
HOST NAME:
CLIENT SPECIFIED:
KEVIN
PASSWORD:
130
132
134
136
138
126
128
READY
NUM

FIG. 7

도면8

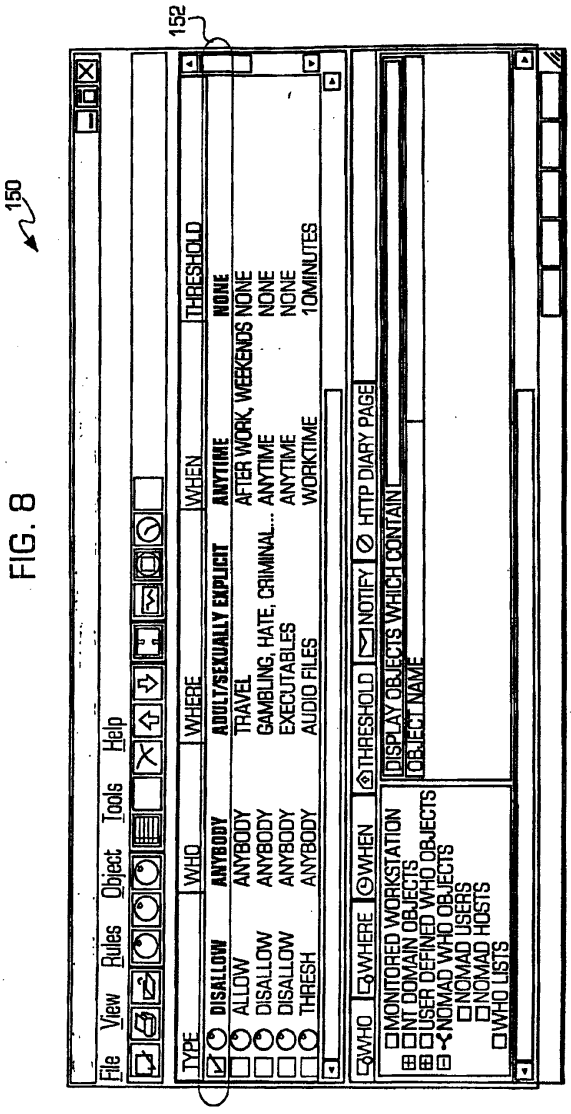
150
152
File View Rules Object Tools Help
TYPE
WHO
WHERE
WHEN
THRESHOLD
DISALLOW ANYBODY ADULT/SEXUALLY EXPLICIT ANYTIME NONE
ALLOW ANYBODY TRAVEL AFTER WORK, WEEKENDS NONE
DISALLOW ANYBODY GAMBLING, HATE, CRIMINAL... ANYTIME NONE
DISALLOW ANYBODY EXECUTABLES ANYTIME NONE
THRESH ANYBODY AUDIO FILES WORKTIME 10MINUTES
WHO
WHERE
WHEN
THRESHOLD
NOTIFY
HTTP DIARY PAGE
MONITORED WORKSTATION
NT DOMAIN OBJECTS
USER DEFINED WHO OBJECTS
NOMAD WHO OBJECTS
NOMAD USERS
NOMAD HOSTS
WHO LISTS
DISPLAY OBJECTS WHICH CONTAIN
OBJECT NAME

FIG. 8