(19)대한민국특허청(KR)
(12) 공개특허공보(A)

(51) 。Int. Cl.
G06F 17/00 (2006.01)
H04L 12/28 (2006.01)
H04L 12/66 (2006.01)

(11) 공개번호 10-2006-0091223
(43) 공개일자 2006년08월18일

(21) 출원번호 10-2005-0096432
(22) 출원일자 2005년10월13일

(30) 우선권주장 11/056,276 2005년02월14일 미국(US)
60/618,139 2004년10월14일 미국(US)

(71) 출원인 마이크로소프트 코포레이션
미국 워싱턴주 (우편번호 : 98052) 레드몬드 원 마이크로소프트 웨이

(72) 발명자 스완더, 브라이언 디.
미국 98052 워싱턴주 레드몬드 원 마이크로소프트 웨이마이크로소프트 코포레이션 내
블랙, 크리스토퍼 제이.
미국 98052 워싱턴주 레드몬드 원 마이크로소프트 웨이마이크로소프트 코포레이션 내
요한슨, 제스퍼 엠.
미국 98052 워싱턴주 레드몬드 원 마이크로소프트 웨이마이크로소프트 코포레이션 내
머씨, 카르틱 엔.
미국 98052 워싱턴주 레드몬드 원 마이크로소프트 웨이마이크로소프트 코포레이션 내
메이필드, 폴 쥐.
미국 98052 워싱턴주 레드몬드 원 마이크로소프트 웨이마이크로소프트 코포레이션 내

(74) 대리인 주성민
이중희
백만기

심사청구 : 없음

(54) ＩＰＳＥＣ을 사용한 네트워크 쿼런틴을 제공하는 시스템및 방법

요약

무효하거나 손상된 상태들을 가진 머신들이 호스트(host) 자원들을 액세스하는 것을 제한하도록 하는 시스템 및 방법이 제공된다. 클라이언트 머신에 위치된 쿼런틴 에이전트(Quarantine Agent;QA)는 복수 개의 쿼런틴 정책(policy) 클라이언트들로부터 헬스 진술서들(Statements of Health)을 받는다. QA는 진술서들을 패키지에 포장하여 그 패키지를 쿼런틴 시행

클라이언트(Quarantine Enforcement Clients;QEC)에게 제공한다. QEC는 쿼런틴 헬스 증명서 서버(Health Certificate Server;HCS)에게 헬스 증명서의 요구와 함께 그 패키지를 전송한다. 클라이언트가 유효한 헬스 진술서들을 제공하면, HCS는 클라이언트에게 IPsec 섹션 교섭(negotiation)에 사용될 수 있는 헬스 증명서를 교부한다.

대표도

도 2

색인어

네트워크 격리 모델, 쿼런틴 링, 경계 링, 보호 링, 쿼런틴 에이전트(QA), 쿼런틴 정책, 헬스 증명서, 쿼런틴 시행 클라이언트(QEC), 헬스 증명서 서버(HCS), IPsec

명세서

도면의 간단한 설명

도 1a는 본 발명이 동작하는 네트워크 환경의 일 예를 일반적으로 도시하는 스키마도이다.

도 1b는 본 발명이 존재하는 컴퓨터 시스템의 예를 일반적으로 도시하는 블럭도이다.

도 2는 본 발명의 일 실시예의 컴포넌트들의 인터랙션을 도시하는 스키마도이다.

도 3은 본 발명의 네트워크 격리 모델(network isolation model)을 도시한다.

도 4는 본 발명의 쿼런틴 시행 클라이언트(Quarantine Enforcement Client;QEC)를 도시한다.

도 5는 본 발명에 따라 클라이언트가 헬스 증명서(health certificate)를 얻는 프로세스를 도시한다.

도 6은 본 발명에 따라 클라이언트가 호스트(host)와 통신을 개시하는 프로세스를 도시한다.

<도면의 주요 부분에 대한 부호의 설명>

200 : AFW QEC를 갖는 클라이언트 시스템

240 : VPN 게이트웨이

250 : DHCP 서버

210 : 헬스 증명서 서버

220 : IAS 서버

230 : 정책 서버들

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 일반적으로 컴퓨터 액세스 관리에 관한 것이고, 더 구체적으로는, 클라이언트들이 호스트 자원들에 액세스하도록 하기 전에 클라이언트들의 보안 상태를 검사하는 것에 관한 것이다.

컴퓨터 네트워크에서, 클라이언트, 서버, 및 피어(peer)는 일반적으로 신뢰 모델들(trust models)과 메카니즘들을 사용하여 비승인된 사용자들이 네트워크의 호스트 컴퓨터들로의 액세스를 얻지 못하도록 한다. 이들 신뢰 모델들과 메카니즘들은 악성이지 않은 사용자들을 식별하기 위해 사용된다. 그러나, 사용자 머신이 사용자가 모르는 상태에서 다른 컴퓨터들에 위험할 수 있다. 예를 들어, 머신이 바이러스를 포함할 수 있고, 또는 사용자가 모르는 보안 구멍(security hole)을 가질 수 있다. 그러므로, 사용자가 얼마나 악성이지 않은지에 무관하게, 사용자 머신의 안전치 못한 상태는 보안 결함들이 수리될 때까지 네트워크로부터 격리되는 결과를 가져야 한다.

IPsec은, 데이터 암호화 및 데이터 무결성(integrity)을 포함하는, 통신을 보안하기 위해 복수 개의 기능들을 정의한다. IPsec은 인증 헤더(Authentication Header;AH)를 사용하여 암호화 없이 소스 인증 및 무결성을 제공하고, 캡슐화 보안 페이로드(Encapsulating Security Payload;ESP)를 사용하여 암호화로 인증 및 무결성을 제공한다. IPsec으로, 단지 송신자와 수신자만이 보안 키를 안다. 인증 데이터가 유효하면, 수신자는 통신이 송신자로부터 왔슴 및 그것이 전송 동안 변경되지 않았슴을 안다.

IPsec은 TCP/IP(Transmission Control Protocol/Internet Protocol) 스택 내의 층으로서 상상될 수 있다. 이 층은 각 컴퓨터의 보안 정책 및 송신자와 수신자 간의 교섭된 보안 연관관계에 의해 제어된다. 이 정책은 필터들의 집합 및 연관된 보안 작용들(behaviors)로 구성된다. 패킷의 IP 주소, 프로토콜, 및 포트 번호가 필터와 매치하면, 패킷은 연관된 보안 작용에 따른다. 그런 제1 패킷은 송신자와 수신자 간의 보안 연관관계의 교섭을 트리거(trigger)한다. IKE(Internet Key Exchange)는 이 교섭을 위한 표준 프로토콜이다. IKE 교섭 동안, 2개의 컴퓨터들은 인증 및 데이터-보안 방법들에 동의하고, 상호 인증을 수행하고, 및 그 후 후속적 데이터 암호화를 위한 공유 키를 생성한다.

보안 연계가 수립된 후에, 데이터 전송은, 그것이 원격 수신자에게 전송하는 패킷들에 데이터 보안 처리를 적용하여, 각 컴퓨터에 대해 진행할 수 있다. 처리는 단순히 전송된 데이터의 무결성을 확실히 할 수 있거나, 또는 그것은 그것을 또한 암호화할 수 있다. IP 페이로드들(payloads)에 대한 데이터 무결성 및 데이터 인증은 IP 헤더(IP header)와 전송 헤더(transport header) 간에 위치된 인증 헤더(AH)에 의해 제공될 수 있다. 인증 헤더는, 송신자를 확인하고, 메시지가 전송 중에 수정되지 않았슴을 확실히 하고, 및 리플레이 어택(replay attack)을 방지하기 위해 함께 사용되는, 인증 데이터와 시퀀스 번호를 포함한다.

ESP는, 보호되는 데이터를 암호화하여 비밀성과 무결성을 제공하고 IP ESP의 데이터 부분에 그 암호화된 데이터를 배치하는, 아키텍처의 키 형식이다. 사용자의 보안 필수사항들에 따라, 이 메카니즘은 전송층 세그먼트(예를 들어, TCP, UDP, ICMP, IGMP) 또는 전체 IP 데이터그램을 암호화하기 위해 사용될 수 있다. 보호되는 데이터를 캡슐화하는 것은 전체 원래의 데이터그램에 대해 비밀성을 제공하기 위해 필요하다. ESP 헤더는 IP 헤더 이후에 그리고 상위 층 프로토콜 헤더(전송 모드) 이전에 또는 캡슐화된 IP 헤더 이전에(터널 모드) 삽입된다.

그러나, 종래 인증 프로시저는 안전치 못하거나 또는 악성이기도 한 머신들이 호스트를 액세스하는 것을 방지하지 않는다. 컴퓨터가 유효한 인증을 제공할 수 있지만, 머신 자체에 바이러스가 감염될 수 있거나, 또는 머신이 다른 컴퓨터의 네트워크 자원들을 액세스하도록 허용되기 전에 교정되어야 되는, 보안 구멍을 포함할 수 있다. 따라서, 클라이언트들이, 그들이 보안 검사들을 통과할 때까지, 호스트를 액세스하는 것이 허용되지 않음을 확실히 하기 위한 시스템 및 방법에 대한 필요가 이 분야에서 존재한다.

발명이 이루고자 하는 기술적 과제

전술된 것의 관점에서, 본 발명은, 클라이언트로부터의 클라이언트 헬스 진술서를 포함하는 IKE(Internet Key Exchange)를 수신하고, 클라이언트 헬스 진술서를 확인하고, 클라이언트 헬스 진술서가 유효하면 호스트 헬스 진술서를 클라이언트에게 전송하고, 및 클라이언트 헬스 진술서가 무효하면 호스트에 클라이언트 액세스를 거절하여, IPsec(IP Security Protocol)을 사용하여 네트워크에서 선택적 네트워크 격리(selective network isolation)를 호스트가 제공하도록 하는 방법을 제공한다. 헬스 진술서는 네트워크의 보안 정책들에 클라이언트들의 적합성을 기술한다. 방법은 클라이언트 헬스 증명서가 수용가능하면 선택적으로 암호화된 통신을 통해 클라이언트와 통신하는 것을 더 포함한다. 헬스 증명서는 본 발명의 다양한 실시예들에서 x509 증명서, 커버로스(Kerberos) 티켓, 또는 WS-보안 토큰일 수 있다.

본 발명의 다른 실시예는, 헬스 증명서 서버에 한 개 이상의 헬스 진술서들을 전송하고, 헬스 증명서 서버로부터 헬스 진술서 응답을 수신하고, 및 헬스 진술서가 헬스 증명서 서버에 의해 확인되면, 헬스 증명서를 수신하고, 및 호스트에 클라이언

트 액세스를 부여하기 전에 클라이언트로부터 클라이언트 헬스 증명서를 요구하는 IPsec 정책을 구현하기 위해 호스트를 구성하는 것을 포함하는, 헬스 증명서를 호스트가 입수하도록 하는 방법을 제공한다. 헬스 진술서가 유효하지 않으면, 헬스 진술서 응답은 호스트가 네트워크 보안 정책들에 적합하지 않음을 나타낸다.

본 발명의 다른 실시예는 네트워크 격리 모델을 구현하는 컴퓨터 네트워크에 관한 것이다. 네트워크는, 각 컴퓨터가 헬스 증명서를 소유하고 유효한 헬스 증명서를 또한 소유하는 컴퓨터들과만 통신하는 제1 그룹의 컴퓨터들, 각 컴퓨터가 헬스 증명서를 소유하고 네트워크의 모든 다른 컴퓨터들과 통신하는 제2 그룹의 컴퓨터들, 및 각 컴퓨터가 헬스 증명서를 소유하지 않고 네트워크에서 다른 컴퓨터들의 전부 또는 일부와 통신하는 제3 그룹의 컴퓨터들을 포함한다. 제1 그룹의 컴퓨터들 간에서 및 제1 그룹의 컴퓨터들과 제2 그룹의 컴퓨터들 간에서 통신은 IPsec를 사용하여 이루어진다.

본 발명의 추가 특징들과 이점들은 첨부 도면들의 참조로 진행하는 다음 설명적 실시예들의 상세한 설명으로부터 명백하게 된다.

발명의 구성 및 작용

본 명세서에 병합되어 일부를 형성하는 첨부 도면들은 본 발명의 여러 양태들을 설명하고, 설명과 함께 본 발명의 원칙들을 설명하기 위한 역할을 한다.

본 발명이 특정 선호되는 실시예들과 연관하여 기재될 것인 한편, 이들 실시예들에 그것을 제한할 의도는 없다. 그와 반대로, 첨부된 청구범위에 의해 정의된 바와 같이 모든 대체본, 수정본, 및 동등물을 본 발명의 취지 및 범위 내에 포함되는 것으로서 포함하려고 의도된다.

도면들의 참조에서, 유사 참조 부호들은 유사 구성요소들을 참조하고, 본 발명은 적절한 컴퓨팅 환경에서 구현되는 것으로서 설명된다. 다음 설명은 본 발명의 실시예들에 기초하고, 본 명세서에 명백히 기재되지 않는 다른 실시예들에 대해 본 발명을 제한하는 것으로서 받아들여져서는 안 된다.

본 발명이 사용될 수 있는 네트워크 환경의 일 예는 이제 도 1a의 참조로 설명될 것이다. 네트워크의 예는, 구름으로 표현된, 네트워크(111)를 통해 서로 통신하는 여러 컴퓨터들(110)을 포함한다. 네트워크(111)는, 라우터, 게이트웨이, 스위치 등과 같은, 다수의 잘-알려진 컴포넌트들을 포함할 수 있고, 유선 및/또는 무선 매체를 통해 컴퓨터들(110)이 통신하도록 한다. 네트워크(111)에서 서로 인터랙팅할 때, 한 개 이상의 컴퓨터들은, 다른 컴퓨터들에 대해, 클라이언트, 네트워크 서버, 퀴런틴 서버, 또는 피어로서 동작할 수 있다. 따라서, 본 발명의 다양한 실시예들은 클라이언트, 네트워크 서버, 퀴런틴 서버, 피어, 또는 이들의 조합들에서, 본 명세서에 포함된 특정 예들이 이들 유형들의 컴퓨터들의 전부를 참조하지는 않지만, 실시될 수 있다.

도 1b는 본 발명이 구현될 수 있는 적절한 컴퓨팅 시스템 환경(100)의 일 예를 도시한다. 컴퓨팅 시스템 환경(100)은 단지 적절한 컴퓨팅 환경의 일 예일 뿐이고, 본 발명의 사용이나 기능의 범위에 대해 어떤 제한을 제안하려고 의도되지는 않는다. 컴퓨팅 환경(100)은 컴퓨팅 환경(100)의 예에서 도시된 컴포넌트들 중의 임의의 것 또는 조합에 관련된 임의의 종속성 또는 요구사항을 갖는 것으로서 해석되어서도 안 된다.

본 발명은 다수의 다른 일반-목적 또는 특수-목적 컴퓨팅 시스템 환경이나 구성과 동작한다. 본 발명과 사용하기에 적절할 수 있는 잘 알려진 컴퓨팅 시스템, 환경, 및 구성의 예들로는, 개인용 컴퓨터, 서버 컴퓨터, 핸드헬드나 랩톱 디바이스, 멀티프로세서 시스템, 마이크로프로세서-기반 시스템, 셋톱-박스, 프로그램가능한 소비자 전자제품, 네트워크 PC, 미니 컴퓨터, 메인프레임 컴퓨터, 위의 시스템들이나 디바이스들 중의 임의의 것을 포함하는 분산 컴퓨팅 환경, 및 기타 등등을 포함하지만, 이에 제한되지는 않는다.

본 발명은 컴퓨터에 의해 실행되는, 프로그램 모듈들과 같은, 컴퓨터-실행가능 명령들의 일반 문맥으로 기재될 것이다. 일반적으로, 프로그램 모듈들은, 특정 작업들을 수행하거나 또는 특정 추상 데이터 유형들을 구현하는 루틴, 프로그램, 객체, 컴포넌트, 데이터 구조 등을 포함한다. 본 발명은 또한 네트워크를 통해 링크된 원격 프로세싱 디바이스들에 의해 작업들이 수행되는 분산 컴퓨팅 환경들에서 실시될 수 있다. 분산 컴퓨팅 환경에서, 프로그램 모듈들은 메모리-저장 디바이스들을 포함하는 로컬 및 원격 컴퓨터-저장 매체 모두에 위치될 수 있다.

도 1b의 참조에서, 본 발명을 구현하는 시스템의 예는, 본 발명의 컨텍스트 내에서 클라이언트, 네트워크 서버, 퀴런틴 서버, 또는 피어로서 동작할 수 있는, 컴퓨터(110)의 형태로 일반-목적 컴퓨팅 디바이스를 포함한다. 컴퓨터(110)의 컴포넌트들은 프로세싱 유닛(120), 시스템 메모리(130), 및 프로세싱 유닛(120)으로 시스템 메모리(130)를 포함하는 다양한 시

스템 컴포넌트들을 결합하는 시스템 버스(121)를 포함할 수 있지만, 이에 제한되지는 않는다. 시스템 버스(121)는 메모리 버스나 메모리 제어기, 주변기기 버스, 및 다양한 버스 구조들 중의 임의의 것을 사용하는 로컬 버스를 포함하는 여러 유형의 버스 구조들 중의 임의의 것일 수 있다. 예를 들어, 하지만 이에 제한적이지는 않고, 그런 아키텍처들은 ISA(Industry Standard Architecture) 버스, MCA(Micro Channel Architecture) 버스, EISA(Enhanced ISA) 버스, VESA(Video Electronics Standards Associate) 로컬 버스, 및 또한 메자닌 버스로서 알려진 PCI(Peripheral Component Interconnect) 버스를 포함한다.

컴퓨터(110)는 통상적으로 다양한 컴퓨터-판독가능 매체를 포함한다. 컴퓨터-판독가능 매체는 컴퓨터(110)에 의해 액세스를 될 수 있는 임의의 이용가능한 매체일 수 있고, 휘발성과 비휘발성 매체, 분리형과 비분리형 매체 모두를 포함한다. 예를 들어, 하지만 이에 제한적이지는 않고, 컴퓨터-판독가능 매체는 컴퓨터 저장 매체 및 통신 매체를 포함할 수 있다. 컴퓨터 저장 매체는 컴퓨터-판독가능 명령, 데이터 구조, 프로그램 모듈, 또는 기타 데이터와 같은 정보 저장을 위한 임의의 방법이나 기술로 구현되는 휘발성과 비휘발성, 분리형과 비분리형 매체 모두를 포함한다. 컴퓨터 저장 매체는 RAM, ROM, EEPROM, 플래쉬 메모리나 다른 메모리 기술, CD-ROM, DVD(digital versatile disks)나 다른 광 디스크 저장장치, 자기 카세트, 자기 테이프, 자기 디스크 저장장치나 다른 자기 저장 디바이스, 또는 원하는 정보를 저장하기 위해 사용될 수 있고 컴퓨터(110)에 의해 액세스를 할 수 있는 임의의 다른 매체를 포함하지만, 이에 제한되지는 않는다. 통신 매체는 통상적으로 컴퓨터-판독가능 명령, 데이터 구조, 데이터 모듈, 또는 반송파나 다른 전송 메카니즘과 같은 변조 데이터 신호의 다른 데이터를 구현하고, 임의의 정보 전달 매체를 포함한다. "변조 데이터 신호"라는 용어는 신호에서 정보를 인코딩하는 방식에서 그것의 한 개 이상의 특성들이 설정되거나 변경되는 신호를 의미한다. 예를 들어, 하지만 이에 제한되지는 않고, 통신 매체는 유선 네트워크나 직접 유선 접속과 같은 유선 매체, 및 음향, RF, 적외선, 및 다른 무선 매체와 같은 무선 매체를 포함한다. 상술된 것들 중의 임의의 것의 조합들은 또한 컴퓨터-판독가능 매체의 범위 내에 포함되어야 한다.

시스템 메모리(130)는 ROM(read only memory;131) 및 RAM(random access memory;132)과 같은 휘발성 및 비휘발성 메모리의 형태로 컴퓨터 저장 매체를 포함한다. 스타트업 동안과 같이, 컴퓨터(110) 내의 구성요소들 간의 정보 전송을 돕는 기본 루틴들을 포함하는, BIOS(basic input/output system;133)는 통상적으로 ROM(131)에 저장된다. RAM(132)은 통상적으로 프로세싱 유닛(120)에 의해 즉시 액세스를 할 수 있거나 또는 현재 동작 중인 데이터와 프로그램 모듈들을 포함한다. 예를 들어, 하지만 이에 제한되지는 않고, 도 1b는 운영 시스템(134), 응용 프로그램들(135), 다른 프로그램 모듈들(136), 및 프로그램 데이터(137)를 도시한다.

컴퓨터(110)는 또한 다른 분리형/비분리형, 휘발성/비휘발성 컴퓨터 저장 매체를 포함할 수 있다. 단지 예로서, 도 1b는 비분리형, 비휘발성 자기 매체에 읽고 쓰는 하드 디스크 드라이브(141), 분리형, 비휘발성 자기 디스크(152)에 읽고 쓰는 자기 디스크 드라이브(151), 및 CD ROM이나 다른 광 매체와 같은 분리형, 비휘발성 광 디스크(156)에 읽고 쓰는 광 디스크 드라이브(155)를 도시한다. 컴퓨팅 환경(100)의 예에 사용될 수 있는 다른 분리형/비분리형, 휘발성/비휘발성 컴퓨터 저장 매체는, 자기 테이프 카세트, 플래쉬 메모리 카드, DVD, 디지탈 비디오 테이프, 반도체 RAM, 반도체 ROM, 및 기타 등등을 포함하지만, 이에 제한되지는 않는다. 하드 디스크 드라이브(141)는 통상적으로 인터페이스(140)와 같은 비분리형 메모리 인터페이스를 통해 시스템 버스(121)에 접속되고, 자기 디스크 드라이브(151)와 광 디스크 드라이브(155)는 통상적으로, 인터페이스(150)와 같은, 분리형 메모리 인터페이스에 의해 시스템 버스(121)에 접속된다.

위에 논의되고 도 1b에 도시된 드라이브들과 그들과 연계된 컴퓨터 저장 매체는 컴퓨터-판독가능 명령, 데이터 구조, 프로그램 모듈, 및 컴퓨터(110)에 대한 다른 데이터의 저장을 제공한다. 도 1b에서, 예를 들어, 하드 디스크 드라이브(141)는 운영 시스템(144), 응용 프로그램들(145), 다른 프로그램 모듈들(146), 및 프로그램 데이터(147)를 저장하는 것으로서 도시된다. 이들 컴포넌트들이 운영 시스템(134), 응용 프로그램들(135), 다른 프로그램 모듈들(136), 및 프로그램 데이터(137)과 동일하거나 다를 수 있슴을 주목한다. 운영 시스템(144), 응용 프로그램들(145), 다른 프로그램 모듈들(146), 및 프로그램 데이터(147)는, 최소한, 그들이 다른 복사본들임을 설명하기 위해 다른 부호들이 주어진다.

사용자는 키보드(162) 및, 마우스, 트랙볼, 또는 터치 패드로서 일반적으로 일컬어지는, 포인팅 디바이스(161)와 같은 입력 디바이스들을 통해 컴퓨터(110)로 커맨드와 정보를 입력할 수 있다. 다른 입력 디바이스들로는(도시 안됨) 마이크로폰, 조이스틱, 게임 패드, 위성 접시, 스캐너 등을 포함할 수 있다. 이들과 다른 입력 디바이스들은 종종 시스템 버스(121)에 결합된 사용자 입력 인터페이스(160)를 통해 프로세싱 유닛(120)에 접속되지만, 병렬 포트, 게임 포트, 또는 USB(universal serial bus)와 같은, 다른 인터페이스나 버스 구조들에 의해 접속될 수 있다. 모니터(191)나 다른 유형의 디스플레이 디바이스는 또한, 비디오 인터페이스(190)와 같은, 인터페이스를 통해 시스템 버스(121)에 접속된다. 모니터(191)에 추가하여, 컴퓨터(110)는 또한 출력 주변기기 인터페이스(195)를 통해 접속될 수 있는 스피커들(197) 및 프린터(196)와 같은 다른 주변 출력 디바이스들을 포함할 수 있다.

컴퓨터(110)는, 원격 컴퓨터(180)와 같은, 한 개 이상의 원격 컴퓨터들로 논리 접속들을 사용하여 네트워크 환경에서 동작할 수 있다. 원격 컴퓨터(180)는 개인용 컴퓨터, 서버, 라우터, 네트워크 PC, 피어 디바이스, 또는 기타 일반 네트워크 노드일 수 있고, 단지 메모리 저장 디바이스(181)만이 도 1b에 도시되었지만, 통상적으로 개인용 컴퓨터(110)와 관련된 위에 기재된 구성요소들 중의 다수나 전부를 포함한다. 도 1b에 도시된 논리 접속들은 LAN(local area network;171)과 WAN(wide area network;173)을 포함하고, 또한 다른 네트워크들을 포함할 수 있다. 그런 네트워크 환경들은 사무실, 기업-전반 컴퓨터 네트워크, 인트라넷, 및 인터넷에서 일반적이다.

LAN 네트워크 환경에서 사용될 때, 개인용 컴퓨터(110)는 네트워크 인터페이스나 어댑터(170)를 통해 LAN(171)에 접속된다. WAN 네트워크 환경에서 사용될 때, 컴퓨터(110)는 통상적으로, 인터넷과 같은, WAN(173)에서 통신을 개설하는 모뎀(172)이나 다른 수단을 포함한다. 내장이나 외장일 수 있는, 모뎀(172)은 사용자 입력 인터페이스(160)나 다른 적절한 메카니즘을 통해 시스템 버스(121)에 접속될 수 있다. 네트워크 환경에서, 개인용 컴퓨터(110), 또는 그것의 일부, 와 관련되어 도시된 프로그램 모듈들은 원격 메모리 저장 디바이스(181)에 저장될 수 있다. 예를 들어, 하지만 이에 제한되지는 않고, 도 1b는 원격 응용 프로그램들(185)이 메모리 디바이스(181)에 존재하는 것으로서 도시한다. 도시된 네트워크 접속들은 예일 뿐이고, 컴퓨터들 간에 통신 링크를 개설하는 다른 수단이 사용될 수 있슴을 이해할 것이다.

아래 설명에서, 본 발명은, 달리 지시되지 않는 한, 한 개 이상의 컴퓨터들에 의해 수행되는 동작들의 행위들과 기호 표현들을 참조하여 기재된다. 그렇게 해서, 때때로 컴퓨터-실행되는 것으로서 일컬어지는 그런 행위들과 동작들은 컴퓨터의 프로세싱 유닛에 의해 구조적 형태로 데이터를 나타내는 전기 신호들의 조작을 포함함을 이해할 것이다. 이 조작은 데이터를 변환하거나, 또는 당업자들에 의해 잘 이해되는 방식으로 컴퓨터의 동작을 재구성하거나 또는 그렇지 않으면 변경하는, 컴퓨터의 메모리 시스템의 위치들에서 그들을 관리한다. 데이터가 관리되는 데이터 구조들은 데이터 형식에 의해 정의되는 특정 특성들을 갖는 물리적 메모리 위치들이다. 그러나, 본 발명이 전술된 문맥으로 기재되는 한편, 당업자들이라면 이후에 기재되는 다양한 행위들과 동작들이 또한 하드웨어에서도 구현될 수 있슴을 이해할 것처럼, 이것은 제한적이려고 의도되지 않는다.

본 발명은 IPsec(IP Security) 프로토콜과 호스트 방화벽들을 조합하여 네트워크 격리를 제공하는 네트워크 액세스 보호(Network Access Protection;NAP)에 대한 시행 메카니즘(enforcement mechanism)에 관한 것이다. IPsec과 호스트 방화벽의 조합은 인증 방화벽(Authenticating Firewall;AFW)로서 일컬어진다. 쿼런틴 시행 클라이언트(Quarantine Enforcement Client;QEC)는 IPsec 및 방화벽 정책을 조정하기 위해 호스트에 동작한다. QEC는 또한 다른 IPsec 정책-가동된 호스트들과 통신하기 위해 헬스 증명서를 얻는 것에 대한 책임이 있다.

도 2는 본 발명이 구현될 수 있는 통상적 네트워크 환경을 도시한다. 클라이언트(200)는 헬스 증명서 서버(Health Certificate Server;HCS;210)에 헬스 진술서(Statement of Health;SoH)를 전송한다. 정책 서버들 230a, 230b, 230c로부터 업데이트된 정책 필수사항들을 관리하는, 인터넷 인증 서버(Internet Authentication Server;IAS;220)를 통해 HCS는 SoH를 확인한다. SoH가 모든 정책 필수사항들을 통과하면, HCS(210)는 클라이언트(200)에게 헬스 증명서를 발행한다. 그 다음, 클라이언트(200)는 헬스 증명서를 사용하여, 도 2의 VPN 게이트웨이(240) 또는 DHCP 서버(250)와 같은, 다른 보호된 시스템들과 통신할 수 있다.

HCS는 헬스 검사들을 만족하는 클라이언트들에게 증명서들을 발행한다. 일 실시예에서, 헬스 증명서는 매우 단기 존속시간(구성가능하지만, 수시간 동안)을 갖는 X509이다. 그러나, 헬스 증명서는, 커버로스(Kerberos) 티켓이나 WS-보안 토큰과 같은, 시스템의 헬스를 나타내는 임의의 확인가능한 데이터 구조일 수 있다. 일단 시스템이 헬스 증명서를 가지면, 그것은 다른 시스템들에 인증하여 그것의 헬스를 증명하기 위해 그것을 사용할 수 있다. 일 실시예에서, HCS는 자립형(standalone)이고, 이것은 하나가 이미 설치되었으면 PKI 계층구조(hierarchy)로 병합할 필요가 없슴을 의미한다. 다른 실시예에서, HCS는 관리 목적으로 또는 특정 개체들에 헬스 증명서들이 묶이도록 하기 위해 기존 PKI에 병합된다. 표준 NAP 부트스트랩핑(bootstrapping)의 부분으로서, 클라이언트는 그것의 HCS로부터 루트 증명서(root certificate)가 주어질 것이다. 클라이언트는 쿼런틴 목적들에 전용되는 사설 저장소(private store)에 이 루트를 설치할 수 있거나(기존 PKI가 사용 중이면, 루트 신뢰가 이미 제공되었고 부트스트랩이 불필요함을 시스템은 가정함), 또는 그것은 머신이나 사용자를 위한 표준 증명서 저장소에 루트를 설치할 것이다.

AFW 격리는, DHCP와 802.1x와 같은, 다른 쿼런틴 시행 메카니즘들에 의해 제공되는 격리와는 다르다. 네트워크 접속이 제공되고 있는 지점에서 중앙에서 시행되는 것에 반하여, AFW 격리는 각 개별 호스트에 의해 분산 방식으로 시행된다. 이것은, DHCP 또는 802.1x 쿼런틴과 같은, 다른 시행 메카니즘들에서는 불가능한 것인, 네트워크에 악성 호스트들이 존재하더라도 각 호스트에 그 자신을 보호하기 위한 능력이 주어짐을 의미한다. AFW는 호스트 당, 포트(port) 당, 또는 응용 프로그램 당 기반으로 제공될 수 있는 단 한 개의 격리 옵션이다.

AFW 쿼런틴은, 도 3에 도시된 바와 같이, 3개 이상의 논리 링들(logical rings)로 물리적 네트워크를 분리한다. 각 컴퓨터는 임의의 주어진 시간에 단지 한 개의 논리 링에만 존재한다. 링들은 헬스 증명서 소유 및 헬스 증명서 통신 필수사항들로 정의된다. 링들은 여전히 유해한 시스템들로부터의 어택들로부터 건전한 시스템들을 보호하면서 모든 시스템들에게 최대 통신 능력들을 준다. 보호 링(Protected Ring)은 헬스 증명서들을 가지며, 그들의 피어들이 헬스 증명서들을 갖도록 요구할 것인 컴퓨터들의 집합으로서 정의된다. 대부분 클라이언트들과 서버들은 이 링에 존재할 것이다. 보호 링의 컴퓨터들은, 관리자에 의해 정의된 사이트(site) 정책에 따라, 보호 링이나 경계 링(Boundary ring)에서 컴퓨터들의 일부 또는 전부와 자유롭게 통신할 수 있다. 보호 링의 컴퓨터가 통신을 개시한다고 가정하면, 다시 말하면, 사이트 정책에 따라, 그들은 쿼런틴 링(Quarantine Ring)의 컴퓨터들과 통신할 수 있다. 예를 들어, 보호 링의 클라이언트는 쿼런틴 링의 서버로부터 웹 페이지를 요구할 수 있다. 그러나, 쿼런틴 링의 클라이언트는 보호 링의 서버로부터 웹 페이지를 요구하는 것이 금지된다. 관리자가 특정 응용 프로그램들(전체 컴퓨터들에 반하여)을 쿼런틴하기를 결정하면, 단지 이들 응용 프로그램들에 링들 간의 통신이 제한된다. 예를 들어, FTP 통신이 쿼런틴되면, 쿼런틴 링의 FTP 클라이언트들은 보호 링의 FTP 서버들로의 접속이 금지될 것이다. 그러나, 이 특정 경우, 동일 2개의 컴퓨터들은 그들의 링 멤버쉽에 무관하게 HTTP를 통해 자유롭게 통신할 수 있을 것이다.

경계 링은 헬스 증명서들을 갖지만, 그들의 피어들이 헬스 증명서들을 갖도록 요구하지는 않는 컴퓨터들의 집합으로서 정의된다. 그런 컴퓨터들은, 링 멤버쉽에 무관하게, 임의의 다른 컴퓨터들과 자유롭게 통신할 수 있다. 경계 링은 통상적으로 거기에 있기 위해 특정하게 구성된 매우 소수의 컴퓨터들을 포함할 것이다. 경계 링의 시스템들은 보통 링 멤버쉽에 무관하게 모든 클라이언트들에 트래픽(traffic)을 개시할 필요가 있는 서버들일 것이다. 예를 들어, 패치(patch) 서버는 쿼런틴 링의 클라이언트들에게 패치들을 제공하여 이들 클라이언트들에게 헬스 증명서들이 발행되도록 할 필요가 있다. 또한, 그것은 보호 링의 클라이언트를 서비스하고, 보호 링의 관리 서버들로부터의 통신을 받을 필요가 있다.

쿼런틴 링은 헬스 증명서들을 갖지 않는 컴퓨터들의 집합으로서 정의된다. 그들이 헬스 검사들을 완료하지 않았기 때문에 그들은 헬스 증명서들을 갖지 않을 것이고, 그들은 네트워크에서 게스트들(quests)이거나, 또는 그들은 쿼런틴 시스템에 참여할 수 없다. 쿼런틴 링의 컴퓨터들은 보호 링의 컴퓨터들을 제외하고 자유롭게 통신할 수 있다. 당업자들이라면, 다른 격리 모델들이 IPsec 정책들과 필수사항들을 변경하여 구현될 수 있슴을 인식할 것이다.

도 4의 참조에서, 쿼런틴 플랫폼 아키텍처는 AFW QEC(430)를 가진 클라이언트(400)에 확장된다. AFW QEC의 목적은 헬스 증명서 서버와 교섭하여 헬스 증명서를 얻고 IPsec과 방화벽 컴포넌트들을 대응하여 구성하는 것이다. 쿼런틴 에이전트(Quarantine Agent;QA)는 SHA(System Health Agents;410a, 410b, 410c)를 조정하여 SoH를 어셈블(assemble)한다. 각 SHA(410a, 410b, 410c)는 클라이언트가 헬스 증명서를 위해 필요한 모든 정책들과 필수사항들을 만족시키는지를 판정하는 것에 대한 책임이 있다. QA(420)는 SHA API를 통해 이들 검사들의 결과들을 얻어, QEC(430)에 제공될 수 있는 SoH로 그들을 어셈블한다. QEC(430)가 새 헬스 증명서를 얻을 때, QEC(430)는 먼저 SoH와 임의의 인증 자격증들(authentification credentials)을 HCS(470)에 통신한다. 일 실시예에서, 이 통신은 보안된 HTTP(Hypertext Transfer Protocol)를 통해서 된다. QEC(430)가 모든 정책 필수사항들을 만족시키면, QEC(430)는 HCS(470)로부터 SoH 응답과 헬스 증명서를 수신한다. QEC(430)는 방화벽과 IPsec 서브시스템들(460)에 디폴트 쿼런틴 규칙들을 구성한다. 쿼런틴 시스템이 자립형이면, QEC는 사설 증명서 저장소(450)에 헬스 증명서를 배치한다. 클라이언트가 모든 헬스 검사들을 통과하지 않으면, QEC는 HCS로부터 클라이언트가 한 개 이상의 정책 필수사항들을 만족시키지 못했슴을 알리는 한 개 이상의 SoH 응답들을 수신한다. SoH 응답은 클라이언트가 만족시키지 못한 특정 필수사항들을 상세화할 것이다. 그 다음, QEC는 클라이언트를 다시 정상 상태로 되돌리기에 필요한 패치들과 업데이트들을 설치하기 위해 수리 서버(fix-up server)를 탐색할 것이다.

도 5는 시스템이 AFW 쿼런틴 시스템에 참여할 때 따르는 프로세스를 도시한다. 단계(510)에서, 시스템은 부트한다. 그것은 그것의 DHCP 서버로부터 제한되지 않은 IP 주소들을 얻는다(DHCP-기반 쿼런틴 시행이 전개(deploy)되지 않았다고 가정함). 시스템의 방화벽은 "예외없이 가동(on with no exceptions)" 모드에 있어서, 다른 시스템은 그것에 접속할 수 없다. 이 시점에서, 시스템은 그것이 최신 헬스 증명서를 갖지 않으므로 쿼런틴 링에 있는다. 그것은 다른 쿼런틴된 시스템들과 통신할 수 있고, 인터넷을 액세스할 수 있다. 보호 링의 컴퓨터들은 이 시스템이 그들에 접속하는 것을 막는다. 단계(520)에서, AFW QEC는 시작한다. QEC는 HCS에 접속을 시작하고, 단계(530)에서는, 신뢰되는 HCS 서버들의 리스트에 대해 그 증명서를 확인하는 것에 의해 이 HCS가 신뢰된다는 것을 확인한다. 단계(540)에서, QEC는 HCS에 클라이언트의 현재 SoH 정보를 송신한다. HCS는 단계(550)에서 IAS 서버로 SoH 정보를 전달한다. 단계(560)에서, IAS 서버는 SoH 정보 및 그것의 구성된 정책에 기초하여 헬스 증명서를 클라이언트에게 교부해야 할지를 판정한다. IAS 서버는 클라이언트에게 헬스 증명서를 발행해야 하는지를 나타내는 값과 함께 헬스 증명서 서버에 SoHR(SoH Responses)을 리턴한다.

단계(570)에서, 헬스 증명서 서버는 AFW QEC에 SoHR들을 되돌려 전달한다. 클라이언트가 헬스 검사들을 통과하면, 그것에 또한 헬스 증명서가 이때 발행된다. 새 SoH 정보가 쿼런틴 에이전트에 도착할 때마다 또는 현재 헬스 증명서가 만기에 가까왔을 때마다, AFW QEC는 단계들(530 내지 570)을 거쳐갈 것이다. AFW QEC에게 헬스 증명서가 발행되면, 그것은 단계(580)에서 컴퓨터의 머신 저장소에 그 증명서를 추가한다. 그것은 IPsec 서브시스템이 그것이 할 수 있는 임의의 피어에 헬스 증명서로 인증하려고 시도하도록 구성한다. 그것은 IPsec을 사용하여 헬스 증명서로 인증되는 임의의 피어로부터의 인입(incoming) 접속들을 허용하도록 호스트 방화벽을 구성한다. 이 시점에서, 컴퓨터는 이제 보호 링에서 동작하고 있다.

AFW 쿼런틴에 참여할 수 없는 시스템은 단순히 쿼런틴 링에 부트하여 거기에 남아있는다. 그것은 인터넷 및 경계 링이나 쿼런틴 링의 임의의 다른 컴퓨터들을 액세스할 수 있을 것이다. 보호 링 컴퓨터들은 이들 컴퓨터들에 접속할 수 있을 것이지만, 그 반대는 안 된다.

도 6은 클라이언트가 IPsec-가동된 호스트들과 통신을 개시하는 프로세스를 도시한다. 단계(610)에서, 클라이언트는 클라이언트의 헬스 증명서를 포함하는 IKE 패킷을 호스트에게 송신한다. 단계(620)에서, 호스트는 헬스 증명서를 확인하고, 그 자신의 헬스 증명서를 제공하여 응답한다. 단계(630)에서, 클라이언트는 ESP를 사용하여 TCP/IP 핸드쉐이크를 시작한다. 단계(640)에서, 핸드쉐이크는 완료되고, 선택적으로 암호화되는 통신이 클라이언트와 호스트 간에 개통된다.

본 발명의 다양한 실시예들의 전술된 설명은 설명과 기재 목적으로 제공되었다. 실시예들 전체를 포함하거나 또는 개시된 정확한 실시예들로 본 발명을 제한하려고 의도되지는 않는다. 다수의 수정이나 변형은 위의 설명의 관점에서 가능하다. 논의된 실시예들은 본 발명의 원칙들에 대해 최상의 설명을 제공하기 위해 선택되어 기재되고, 그러므로 다양한 실시예들에서 및 특정 사용에 적절한 것으로서 다양한 수정들과 당업자가 사용할 수 있도록 하는 그것의 실용적 응용 프로그램이 고려된다. 모든 그런 수정들과 변형들은, 첨부된 청구범위에 의해, 그들이 정당하게, 법적으로, 및 공정하게 권리가 있는 범위에 따라 해석될 때, 결정되는 것으로서 본 발명의 범위 내에 있다.

발명의 효과

본 발명은 안전치 못한 클라이언트들을 네트워크에서 선택적으로 격리시켜 호스트 자원들로의 액세스를 제한하는 방법 및 시스템을 개시한다. 클라이언트들은 헬스 증명서가 요구되며, 그 헬스 증명서들의 적합성을 확인하기 위해 그 헬스 증명서들은 헬스 증명서 서버(HCS)로 전송되어, 네트워크 보안 정책에 기초하여 적합성이 판정되고, 그 결과에 따라 유효한 헬스 증명서를 가진 클라이언트들에게 호스트 자원들로의 액세스가 부여된다.

(57) 청구의 범위

청구항 1.

IPsec(IP Security Protocol)을 사용하여 네트워크에서 선택적 네트워크 격리를 호스트가 제공하도록 하는 방법으로서,

클라이언트로부터 클라이언트 헬스 증명서(health certificate)를 포함하는 IKE(Internet Key Exchange) 패킷을 수신하는 단계;

상기 클라이언트 헬스 증명서를 확인하는 단계;

상기 클라이언트 헬스 증명서가 유효하면 호스트 헬스 증명서를 상기 클라이언트에게 전송하는 단계; 및

상기 클라이언트 헬스 증명서가 무효하면 상기 호스트로의 상기 클라이언트 액세스를 거절하는 단계

를 포함하는 방법.

청구항 2.

제1항에 있어서, 헬스 증명서는 상기 증명서의 소유자가 상기 네트워크의 보안 정책들(security policies)에 적합하다고 나타내는 방법.

청구항 3.

제1항에 있어서, 상기 클라이언트 헬스 증명서가 유효하면 IPsec 통신을 통해 상기 클라이언트와 통신하는 단계를 더 포함하는 방법.

청구항 4.

제1항에 있어서, 상기 헬스 증명서는 X509 증명서인 방법.

청구항 5.

제1항에 있어서, 상기 헬스 증명서는 커버로스(Kerberos) 티켓인 방법.

청구항 6.

제1항에 있어서, 상기 헬스 증명서는 WS-보안 토큰인 방법.

청구항 7.

제1항의 방법을 수행하기 위한 컴퓨터-실행가능한 명령들을 저장한 컴퓨터-판독가능 매체.

청구항 8.

호스트가 헬스 증명서를 얻기 위한 방법으로서,

헬스 증명서 서버에 적어도 한 개의 헬스 진술서(statement of health)를 전송하는 단계;

헬스 증명서 서버로부터 적어도 한 개의 헬스 진술서 응답을 수신하는 단계; 및

상기 적어도 한 개의 헬스 진술서가 상기 헬스 증명서 서버에 의해 확인되면, 헬스 증명서를 수신하는 단계 및 상기 호스트로의 클라이언트 액세스를 부여하기 전에 상기 클라이언트로부터 클라이언트 헬스 증명서를 요구하는 IPsec 정책을 구현하기 위해 상기 호스트를 구성하는 단계

를 포함하는 방법.

청구항 9.

제8항에 있어서, 상기 적어도 한 개의 헬스 진술서가 유효하지 않으면, 상기 적어도 한 개의 헬스 진술서 응답은 상기 호스트가 네트워크 보안 정책들에 적합하지 않다고 나타내는 방법.

청구항 10.

제8항에 있어서, 상기 헬스 증명서는 X509 증명서인 방법.

청구항 11.

제8항에 있어서, 상기 헬스 증명서는 커버로스 티켓인 방법.

청구항 12.

제8항에 있어서, 상기 헬스 증명서는 WS-보안 토큰인 방법.

청구항 13.

제8항의 방법을 수행하기 위한 컴퓨터-실행가능 명령들을 저장하는 컴퓨터-판독가능 매체.

청구항 14.

네트워크 격리 모델을 구현하는 컴퓨터 네트워크로서,

각 컴퓨터가 헬스 증명서를 소유하고 또한 유효한 헬스 증명서를 소유한 컴퓨터들과만 통신하는 제1 그룹의 컴퓨터들;

각 컴퓨터가 헬스 증명서를 소유하고 상기 네트워크에서 모든 다른 컴퓨터들과 통신하는 제2 그룹의 컴퓨터들; 및

각 컴퓨터가 헬스 증명서를 소유하지 않고 상기 네트워크의 모든 다른 컴퓨터들과 통신하는 제3 그룹의 컴퓨터들

을 포함하는 컴퓨터 네트워크.

청구항 15.

제14항에 있어서, 상기 제1 그룹의 컴퓨터들 간에서 및 상기 제1 그룹의 컴퓨터들과 상기 제2 그룹의 컴퓨터들 간에서 통신은 IPsec을 사용하여 이루어지는 네트워크.

청구항 16.

제14항에 있어서, 상기 헬스 증명서는 X509 증명서인 네트워크.

청구항 17.

제14항에 있어서, 상기 헬스 증명서는 커버로스 티켓인 네트워크.

청구항 18.

제14항에 있어서, 상기 헬스 증명서는 WS-보안 토큰인 네트워크.

청구항 19.

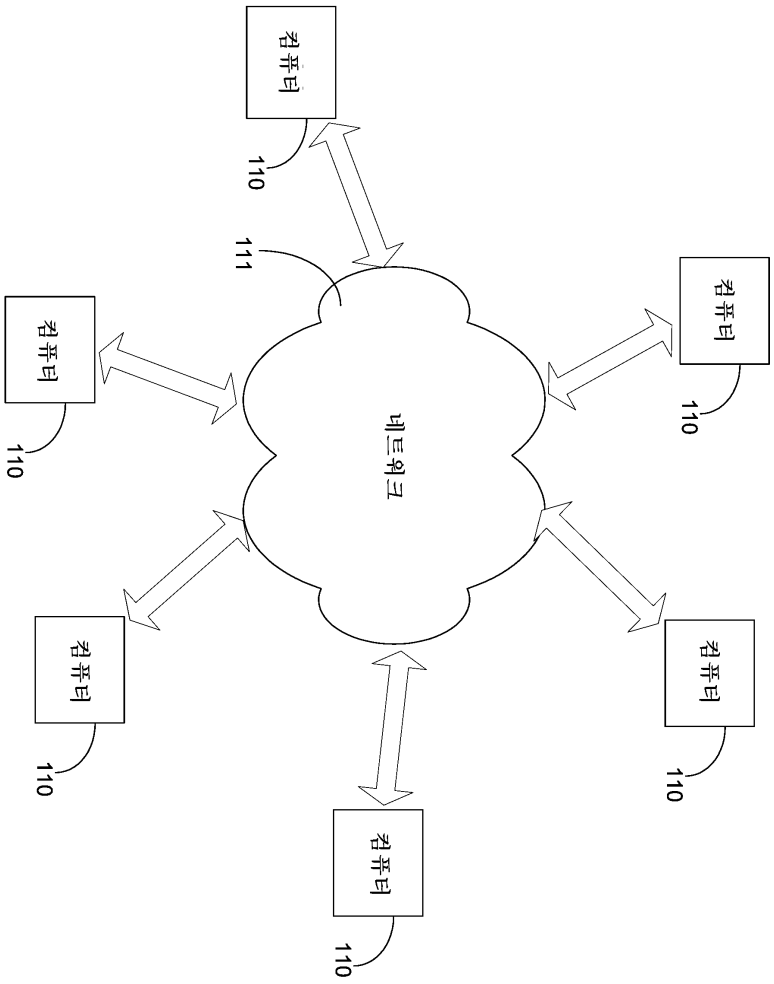
제14항에 있어서, 상기 헬스 증명서는 상기 증명서의 소유자가 상기 네트워크의 수립된 보안 정책들에 적합하다고 나타내는 네트워크.

청구항 20.

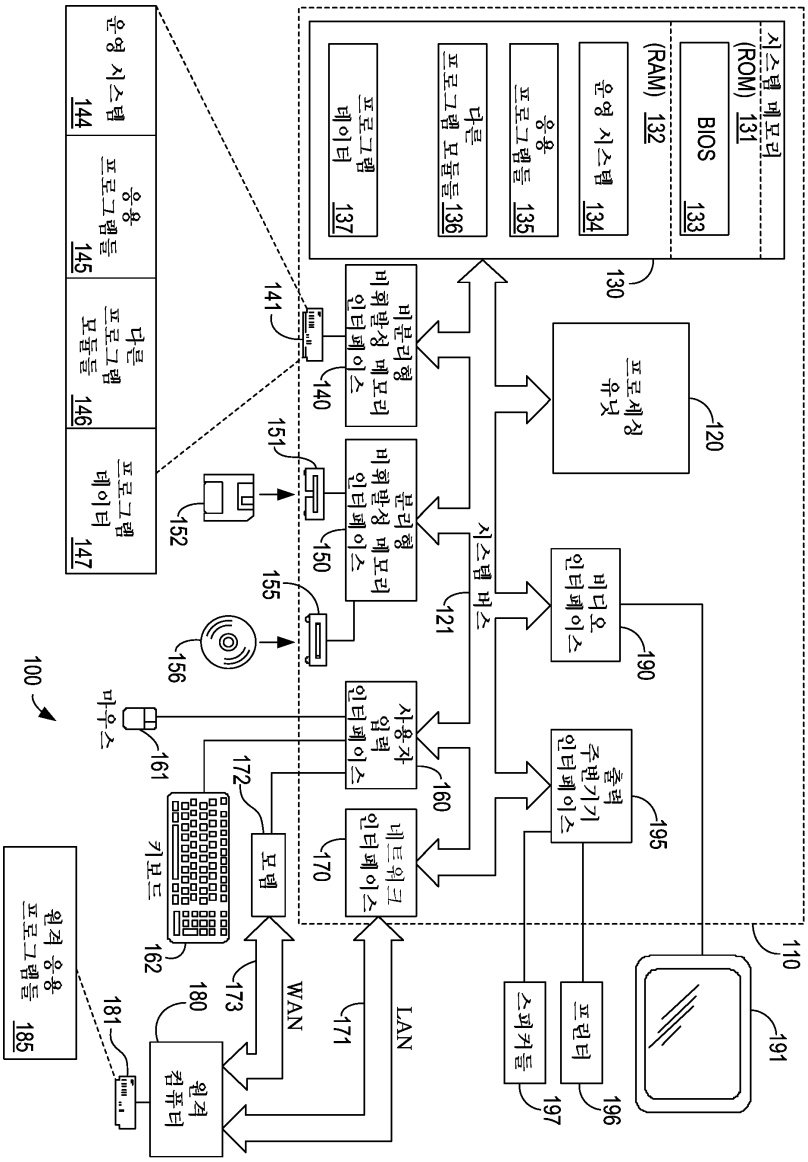
제14항에 있어서, 상기 제1 그룹의 컴퓨터들은 상기 제3 그룹의 컴퓨터들과 통신을 개시할 수 있지만, 상기 제3 그룹의 컴퓨터들은 상기 제1 그룹의 컴퓨터들과 통신을 개시할 수 없는 네트워크.

도면

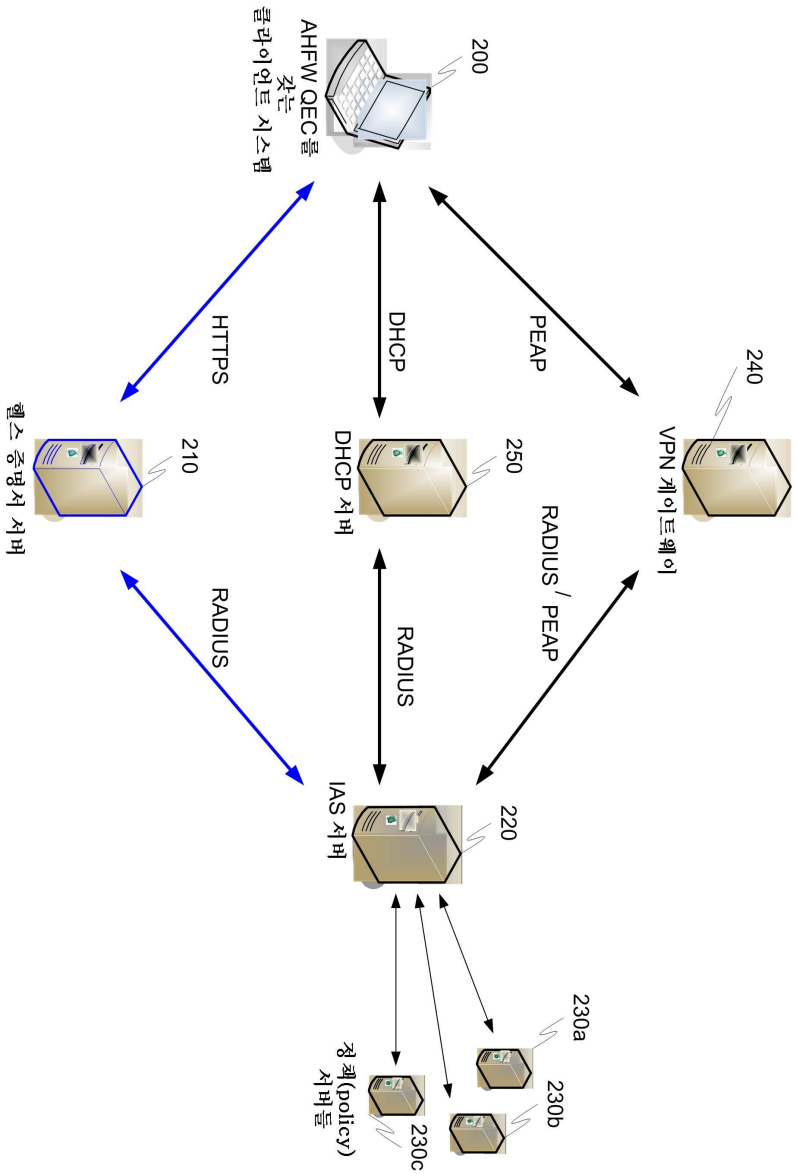
도면1a



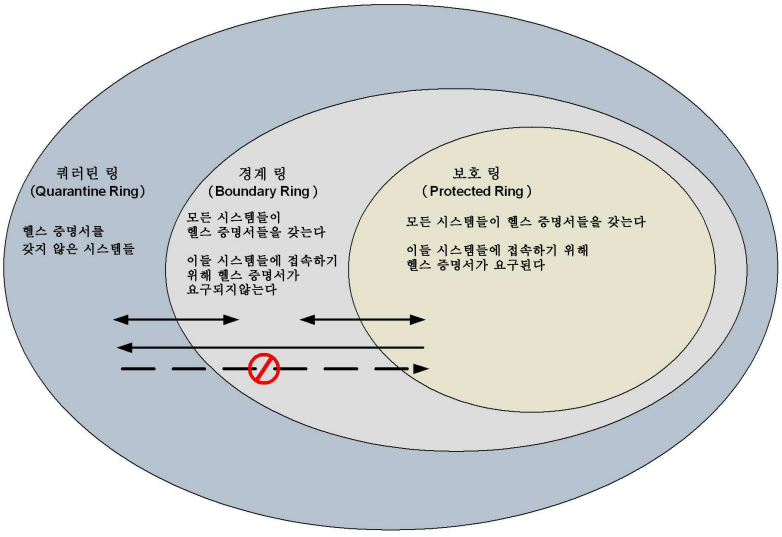
도면1b


시스템 메모리 (ROM) 131
BIOS 133
(RAM) 132
운영 시스템 134
응용 프로그램들 135
다른 프로그램 모듈들 136
프로그램 데이터 137
130
프로세싱 유닛 120
비휘발성 메모리 인터페이스 140
141
비휘발성 메모리 인터페이스 150
151
152
155
156
시스템 버스 121
비디오 인터페이스 190
출력 주변기기 인터페이스 195
사용자 입력 인터페이스 160
네트워크 인터페이스 170
모뎀 172
키보드 162
마우스 161
100
110
191
스피커들 197
프린터 196
WAN 173
LAN 171
원격 컴퓨터 180
181
원격 응용 프로그램들 185
운영 시스템 144
응용 프로그램들 145
다른 프로그램 모듈들 146
프로그램 데이터 147

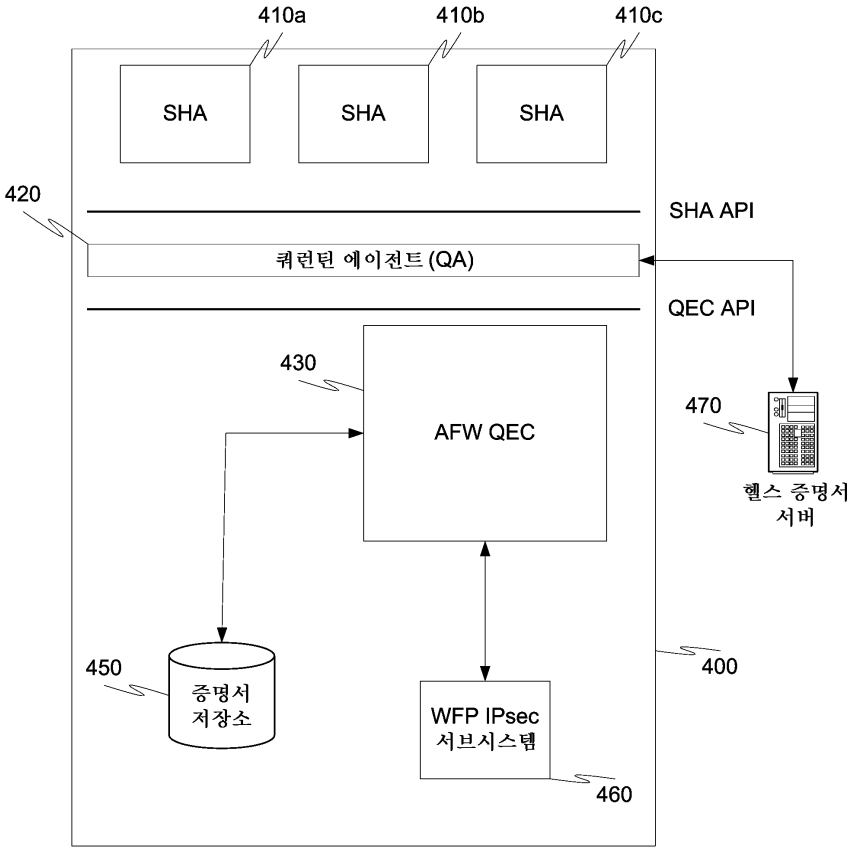
도면2


AHFW QEC를 갖는 클라이언트 시스템
200
HTTPS
DHCP
PEAP
헬스 증명서 서버
210
DHCP 서버
250
VPN 게이트웨이
240
RADIUS
RADIUS
RADIUS / PEAP
IAS 서버
220
정책(policy) 서버들
230a
230b
230c

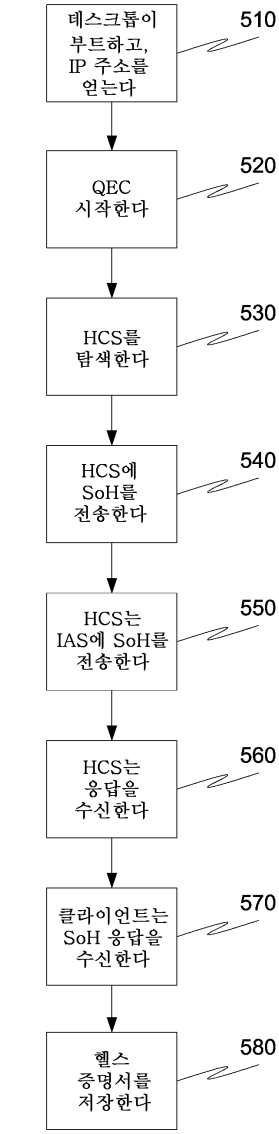
도면3


쿼러틴 링
(Quarantine Ring)
헬스 증명서를
갖지 않은 시스템들
경계 링
(Boundary Ring)
모든 시스템들이
헬스 증명서들을 갖는다
이들 시스템들에 접속하기
위해 헬스 증명서가
요구되지않는다
보호 링
(Protected Ring)
모든 시스템들이 헬스 증명서들을 갖는다
이들 시스템들에 접속하기 위해
헬스 증명서가 요구된다

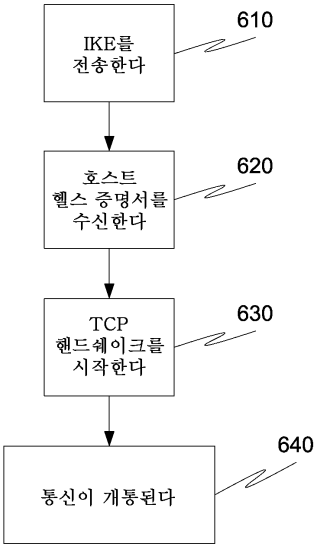
도면4


410a
410b
410c
SHA
SHA
SHA
420
SHA API
퀴런틴 에이전트 (QA)
QEC API
430
AFW QEC
470
헬스 증명서
서버
450
증명서
저장소
WFP IPsec
서브시스템
460
400

도면5


데스크톱이 부트하고, IP 주소를 얻는다
510
QEC 시작한다
520
HCS를 탐색한다
530
HCS에 SoH를 전송한다
540
HCS는 IAS에 SoH를 전송한다
550
HCS는 응답을 수신한다
560
클라이언트는 SoH 응답을 수신한다
570
헬스 증명서를 저장한다
580

도면6


IKE를 전송한다
610
호스트 헬스 증명서를 수신한다
620
TCP 핸드쉐이크를 시작한다
630
통신이 개통된다
640