(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2009년12월10일
(11) 등록번호 10-0930605
(24) 등록일자 2009년12월01일

(51) Int. Cl.
H04L 12/66 (2006.01) *H04L 12/28* (2006.01)
(21) 출원번호 10-2007-7019135
(22) 출원일자 2006년01월23일
심사청구일자 2007년08월22일
(85) 번역문제출일자 2007년08월21일
(65) 공개번호 10-2007-0091237
(43) 공개일자 2007년09월07일
(86) 국제출원번호 PCT/IB2006/000101
(87) 국제공개번호 WO 2006/079891
국제공개일자 2006년08월03일
(30) 우선권주장
11/045,198 2005년01월27일 미국(US)
(56) 선행기술조사문헌
US20040223500 A1
US20050135269 A1
전체 청구항 수 : 총 17 항

(73) 특허권자
노키아 코포레이션
핀랜드핀-02150 에스푸 카일알라덴티에 4
(72) 발명자
스티르부 블라드
핀랜드 핀-33820 탐페레 만니콘카투 4 씨 16
(74) 대리인
리앤목특허법인

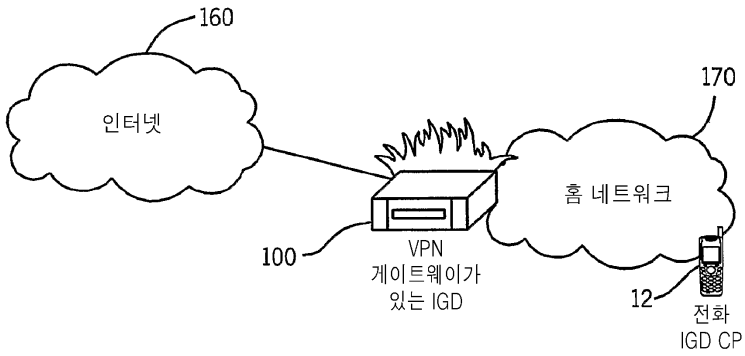
심사관 : 정재헌

(54) UPnP VPN 게이트웨이 환경설정 서비스

(57) 요 약

VPN 게이트웨이 환경설정 서비스를 통해 가상 사설 네트워크를 생성하기 위한 시스템 및 방법. VPN 게이트웨이 환경설정 서비스는 UPnP 제로구성 특성들을 물려받고, 또한 제조업체에 관계없이, VPN 게이트웨이 장치의 환경설정을 가능하게 하는 VPN 게이트웨이를 환경설정하기 위한 인터페이스를 제공한다. 추가적으로 VPN 게이트웨이 환경설정 서비스에 의해 정의되는 장치 제어 프로토콜은 클라이언트에게 게이트웨이-게이트웨이 가상 사설 네트워크들의 환경설정을 가능하게 할 뿐만 아니라 공급하는 것을 제공할 수 있다.

대 표 도 - 도4



특허청구의 범위

청구항 1

제1 인터넷 게이트웨이 장치를 포함하는 제1 근거리 네트워크(local area network)를 제공하는 단계;

가상 사설 네트워크 환경설정(configuration) 서비스를 포함하는 전자 장치를 제공하는 단계;

상기 제1 인터넷 게이트웨이 장치를 통해, 상기 전자 장치 및 상기 제1 근거리 네트워크 내의 다른 장치들 간의 통신을 허용하기 위해, 가상 사설 네트워크 환경설정 서비스를 사용하여 상기 전자 장치를 환경설정하는(configuring) 단계; 및

상기 전자 장치가, 상기 제1 근거리 네트워크 외부에 있을 때, 상기 전자 장치 및 상기 제1 인터넷 게이트웨이 장치 사이에 제1 가상 사설 네트워크 터널을 생성하는 단계를 포함하며, 상기 제1 가상 사설 네트워크 터널은, 상기 전자 장치가 상기 제1 근거리 네트워크 외부에 있는 동안, 상기 전자 장치가 상기 제1 근거리 네트워크 내의 다른 장치들과 직접적으로 통신하는 것을 허용하는,

가상 사설 네트워크를 생성하기 위한 방법.

청구항 2

제1항에 있어서, 상기 전자 장치를 환경설정하는(configuring) 단계는, 상기 전자 장치 내의 요구된 보안 프로토콜들의 조정을 포함하는 가상 사설 네트워크를 생성하기 위한 방법.

청구항 3

제1항에 있어서, 상기 전자 장치를 환경설정하는(configuring) 단계는,

상기 전자 장치 내의 보안 프로토콜들을 위해 인증(authentication) 및 프라이버시 파라미터들의 조정을 포함하는, 가상 사설 네트워크를 생성하기 위한 방법.

청구항 4

제1항에 있어서, 상기 전자 장치를 환경설정하는 단계는, 상기 전자 장치를 위해 세션 타임아웃들의 조정을 포함하는, 가상 사설 네트워크를 생성하기 위한 방법.

청구항 5

제1항에 있어서, 상기 전자 장치를 환경설정하는 단계는, 상기 제1 인터넷 게이트웨이 장치의 적어도 하나의 IP 주소를 얻는 것을 포함하는, 가상 사설 네트워크를 생성하기 위한 방법.

청구항 6

제1항에 있어서, 상기 전자 장치는 휴대용 전화를 포함하는, 가상 사설 네트워크를 생성하기 위한 방법.

청구항 7

제1항에 있어서,

상기 전자 장치를 제2 근거리 네트워크를 위한 제2 인터넷 게이트웨이 장치로 연결하는 단계; 및

상기 제1 인터넷 게이트웨이 장치에 관한 정보를, 상기 전자 장치로부터 상기 제2 인터넷 게이트웨이 장치까지 전송하는[상기 정보는 제2 가상 사설 네트워크 터널이, 상기 제1 인터넷 게이트웨이 장치와 상기 제2 인터넷 게이트웨이 장치 사이에, 생성되도록 함] 단계를 더 포함하며,

상기 제2 가상 사설 네트워크 터널은 상기 전자 장치, 상기 제1 근거리 네트워크 내의 장치들, 및 상기 제2 근거리 네트워크 내의 장치들 간의 통신을 가능하게 하는,

가상 사설 네트워크를 생성하기 위한 방법.

청구항 8

가상 사설 네트워크를 생성하기 위한 컴퓨터 프로그램을 기록한 컴퓨터 판독가능 매체로서, 상기 컴퓨터 프로그램은,

가상 사설 네트워크 환경설정(configuration) 서비스를 포함하는 전자 장치가, 제1 인터넷 게이트웨이 장치를 포함하는 제1 근거리 네트워크 외부에 있는 동안, 상기 제1 인터넷 게이트웨이 장치를 통해, 상기 전자 장치 및 제1 근거리 네트워크 내의 다른 장치들 간의 통신을 허용하기 위해, 가상 사설 네트워크 환경설정 서비스를 사용하여 상기 전자 장치를 환경설정하기 위한 컴퓨터 코드; 및

상기 전자 장치가, 상기 제1 근거리 네트워크 외부에 있을 때, 상기 전자 장치 및 상기 제1 인터넷 게이트웨이 장치 사이에, 제1 가상 사설 네트워크 터널을 생성하며, 상기 제1 가상 사설 네트워크 터널은 상기 제1 근거리 네트워크 내의 다른 장치들과 직접적으로 통신하는 것을 허용하는, 컴퓨터 코드;를 포함하는, 가상 사설 네트워크를 생성하기 위한 컴퓨터 판독가능 매체.

청구항 9

제8항에 있어서,

상기 전자 장치를 환경설정하기 위한 컴퓨터 코드는, 상기 제1 인터넷 게이트웨이 장치의 적어도 하나의 IP 주소를 얻기 위한 컴퓨터 코드를 포함하는,

가상 사설 네트워크를 생성하기 위한 컴퓨터 판독가능 매체.

청구항 10

제8항에 있어서,

상기 전자 장치를 제2 근거리 네트워크를 위한 제2 인터넷 게이트웨이 장치로 연결하기 위한 컴퓨터 코드; 및

상기 제1 인터넷 게이트웨이 장치에 관한 정보를, 상기 전자 장치로부터 상기 제2 인터넷 게이트웨이 장치까지 전송하기 위한[상기 정보는 제2 가상 사설 네트워크 터널이, 상기 제1 인터넷 게이트웨이 장치와 상기 제2 인터넷 게이트웨이 장치 사이에, 생성되도록 함] 컴퓨터 코드;를 더 포함하며,

이때 상기 제2 가상 사설 네트워크 터널은 상기 전자 장치, 상기 제1 근거리 네트워크 내의 장치들, 및 상기 제2 근거리 네트워크 내의 장치들 간의 통신을 가능하게 하는,

가상 사설 네트워크를 생성하기 위한 컴퓨터 판독가능 매체.

청구항 11

프로세서; 및

상기 프로세서에 연결되어 동작하는 메모리 유닛을 포함하며, 상기 메모리 유닛은 제1 인터넷 게이트웨이 장치와의 통신을 할 수 있도록 가상 사설 네트워크 환경설정(configuration) 서비스를 사용하여 전자 장치를 환경설정하기 위한 컴퓨터 코드; 및

전자 장치가 상기 제1 인터넷 게이트웨이 장치에 연관된 상기 제1 근거리 네트워크 외부에 있을 때, 상기 전자 장치 및 상기 제1 인터넷 게이트웨이 장치 사이에 제1 가상 사설 네트워크 터널을 생성하며, 상기 제1 가상 사설 네트워크 터널은, 상기 전자 장치가 상기 제1 근거리 네트워크 외부에 있는 동안, 상기 제1 근거리 네트워크 내의 다른 장치들과 직접적으로 통신하는 것을 허용하는, 컴퓨터 코드;를 포함하는 전자 장치.

청구항 12

제11항에 있어서, 상기 메모리 유닛은,

상기 전자 장치를, 제2 근거리 네트워크를 위한 제2 인터넷 게이트웨이 장치로 연결하기 위한 컴퓨터 코드; 및

상기 제1 인터넷 게이트웨이 장치에 관한 정보를, 상기 전자 장치로부터 상기 제2 인터넷 게이트웨이 장치까지 전송하기 위한 [상기 정보는 상기 제1 인터넷 게이트웨이 장치와 상기 제2 인터넷 게이트웨이 장치 사이에 제2 가상 사설 네트워크 터널이 생성되도록 함] 컴퓨터 코드;를 더 포함하며,

상기 제2 가상 사설 네트워크 터널은 상기 전자 장치, 상기 제1 근거리 네트워크 내의 장치들, 및 상기 제2 근

거리 네트워크 내의 장치들 간의 통신을 가능하게 하는 전자 장치.

청구항 13

제1 인터넷 게이트웨이 장치를 포함하는 제1 근거리 네트워크; 및

전자 장치를 포함하며, 상기 전자 장치는,

프로세서, 및

상기 프로세서에 연결되어 동작하는 메모리 유닛을 포함하며, 상기 메모리 유닛은 제1 인터넷 게이트웨이 장치와의 통신을 할 수 있도록 가상 사설 네트워크 환경설정 서비스를 사용하여 상기 전자 장치를 환경설정하기 위한 컴퓨터 코드; 및

상기 전자 장치가 상기 제1 근거리 네트워크 외부에 있을 때, 상기 전자 장치 및 상기 제1 인터넷 게이트웨이 장치 사이에 제1 가상 사설 네트워크 터널을 생성하며, 상기 제1 가상 사설 네트워크 터널은 상기 전자 장치가 상기 제1 근거리 네트워크 외부에 있는 동안 상기 제1 근거리 네트워크 내의 다른 장치들과 직접적으로 통신하는 것을 허용하는, 컴퓨터 코드를 포함하는 가상 사설 네트워크를 생성하기 위한 시스템.

청구항 14

제13항에 있어서, 상기 메모리 유닛은,

상기 전자 장치를 제2 근거리 네트워크를 위한 제2 인터넷 게이트웨이 장치로 연결하기 위한 컴퓨터 코드; 및

상기 제1 인터넷 게이트웨이 장치에 관한 정보를 상기 전자 장치로부터 상기 제2 인터넷 게이트웨이 장치까지 전송하는 [상기 정보는 상기 제1 인터넷 게이트웨이 장치와 상기 제2 인터넷 게이트웨이 장치 사이에 제2 가상 사설 네트워크 터널이 생성되도록 함] 컴퓨터 코드를 더 포함하고,

상기 제2 가상 사설 네트워크 터널은 상기 전자 장치, 상기 제1 근거리 네트워크 내의 장치들, 및 상기 제2 근거리 네트워크 내의 장치들 간의 통신을 가능하게 하는 시스템.

청구항 15

제1 네트워크 내에 위치한 제1 인터넷 게이트웨이 장치; 및

제2 네트워크 내에 위치한 제2 인터넷 게이트웨이 장치를 포함하고,

상기 제1 인터넷 게이트웨이 장치와 상기 제2 인터넷 게이트웨이 장치의 각각이, 상기 제1 인터넷 게이트웨이 장치 및 상기 제2 인터넷 게이트웨이 장치 사이에 제1 가상 사설 네트워크 터널을 생성할 수 있도록, 가상 사설 네트워크 환경설정 서비스를 사용하여 각각의 인터넷 게이트웨이 장치를 환경설정하기 위한 [상기 제1 가상 사설 네트워크 터널은 상기 제1 네트워크 내의 장치들 및 상기 제2 네트워크 내의 장치들 사이에 통신을 할 수 있게 함] 컴퓨터 코드를 포함하고, 그리고

상기 제1 인터넷 게이트웨이 장치와 상기 제2 인터넷 게이트웨이 장치의 적어도 1개가, 전자 장치가 상기 제1 네트워크 및 제2 네트워크 외부에 있는 때, 상기 전자 장치와의 제2 가상 사설 네트워크 터널을 생성하기 위한 컴퓨터 코드를 포함하고,

제2 가상 사설 네트워크 터널은 상기 전자 장치가 상기 제1 네트워크와 상기 제2 네트워크 중 하나의 밖에 있는 때, 상기 전자 장치가 상기 제1 네트워크와 상기 제2 네트워크 중 하나 내의 다른 장치와 직접적으로 통신하는 것을 허용하는,

가상 사설 네트워크를 생성하기 위한 시스템.

청구항 16

이동 전자 장치; 및

상기 이동 전자 장치 내에 만들어진 인터넷 게이트웨이 장치 제어 포인트[그 인터넷 게이트웨이 장치 제어 포인트는 가상 사설 네트워크 환경설정 서비스를 포함]를 포함하고,

상기 가상 사설 네트워크 환경설정 서비스는, 원격 인터넷 게이트웨이 장치와의 가상 사설 네트워크 터널의 생

성을 할 수 있게 하고, 상기 가상 사설 네트워크 터널은, 상기 이동 전자 장치가 네트워크의 밖에 있는 동일한, 상기 이동 전자 장치와, 상기 원격 인터넷 게이트웨이 장치와 동일한 네트워크 내의 장치들 사이에 통신을 할 수 있게 하는 가상 사설 네트워크를 생성하기 위한 시스템.

청구항 17

인터넷 게이트웨이 장치에 있어서,

가상 사설 네트워크 게이트웨이; 및

가상 사설 네트워크 환경설정 서비스를 포함하고,

상기 가상 사설 네트워크 환경설정 서비스는 상기 가상 사설 네트워크 게이트웨이 및 원격 네트워크 사이에 제1 가상 사설 네트워크 터널의 생성을 할 수 있게 하고,

상기 제1 가상 사설 네트워크 터널은 상기 인터넷 게이트웨이 장치 및 상기 원격 네트워크 내의 장치들 사이에 통신을 할 수 있게 하고,

상기 가상 사설 네트워크 환경설정 서비스는, 상기 가상 사설 네트워크 게이트웨이와, 그 홈 네트워크의 외부 장치 사이에 제2 가상 사설 네트워크 터널의 생성을 가능하게 하는 것에 의해, 그 홈 네트워크의 외부 장치가 상기 홈 네트워크 내의 장치들과 직접적으로 통신하는 것을 가능하게 하는, 인터넷 게이트웨이 장치.

청구항 18

삭제

청구항 19

삭제

청구항 20

삭제

청구항 21

삭제

명 세 서

기 술 분 야

<1> 본 발명은 일반적으로 가상 사설 네트워크(virtual private networks)들에 관련된다. 좀더 자세히는, 본 발명은 LAN(local area network) 및 네트워크 외부의(out-of-network) 전자 장치 간의 상호작용을 허용하는 가상 사설 네트워크들의 생성에 관련된다.

배 경 기 술

<2> 범용 플러그 엔 플레이(Universal Plug and Play, UPnP) 기술은 지능형 어플라이언스들(intelligent appliances), 무선 장치들, 및 모든 유형들의 퍼스널 컴퓨터들의 편재형 피어 투 피어 네트워크 연결(pervasive peer-to-peer network connectivity)을 위한 아키텍처를 정의한다. UPnP 기술은 인터넷으로 연결된 집, 소기업, 공중 장소들, 또는 시스템들 어디에서든지, 애드혹(ad-hoc) 또는 관리되지 않는 네트워크들로의 사용하기 용이하고, 유연하고, 표준들에 기반하는 연결을 가져다주도록 설계되었다. UPnP 기술은 무결절성 근접 네트워킹(seamless proximity networking)을 가능하게 하기 위해, 네트워크로 연결된(networked) 장치들 사이에 제어 및 데이터 전송을 제공하는 것에 추가하여, TCP/IP 및 웹 기술들에 영향을 주는 분산화된(distributed), 오픈 네트워킹 아키텍처를 제공한다.

<3> UPnP 장치 아키텍처(UPnP Device Architecture, UDA)는 광범위한 벤더(vendor)들로부터의 일정 범위의 장치 카테고리들을 위해 자동 검색(automatic discovery) 뿐 아니라, 제로-구성(zero-configuration), "투명(invisible)" 네트워킹을 지원하도록 설계된다. 이런 아키텍처 하에서, 장치는 네트워크에 동적으로 결합하고,

IP 주소를 얻고, 장치들의 성능들(capabilities)을 전달하고, 네트워크 내의 다른 장치들의 존재 및 성능들에 관해 알 수 있다.

<4> UPnP 인터넷 게이트웨이 장치(Internet Gateway Device, IGD)는 홈 네트워크를 인터넷과 같은 광역 네트워크(wide area network, WAN)로 연결하는 장치이다. IGD는 적어도 광역 네트워크(WAN) 인터페이스(DSL, 케이블, 이더넷 연결(Ethernet connection), 또는 다른 유형의 연결 형식임) 및 근거리 네트워크(local area network, LAN) 인터페이스(이더넷 또는 무선 랜(WLAN) 연결, 또는 다른 유형의 연결 형식임)을 가지고 있다. UPnP IGD은 다수의 WAN 및 LAN 관련된 서비스들을 포함한다.

<5> IPSec(IP Security)을 사용하는 가상 사설 네트워크들(Virtual Private Networks, VPNs)은 인터넷과 같은 공중망(public network)에 의해 제공된 기반구조(infrastructure)를 사용하는 네트워크에 안전하게 연결하기 위해 가장 광범위하게 사용되는 기술들 중의 하나이다.

<6> 수많은 새로운 기술들이 홈 네트워크들로의 원격 액세스를 가능하게 하기 위해 현재 구현되고 있다. 홈 네트워크들로의 원격 액세스를 할 수 있게 하는 제안된 기술들 중의 하나의 기술은 이동 전화와 같은 원격 장치 및, 홈네트워크 내에 위치한 인터넷 게이트웨이 사이에서 VPN의 사용을 포함한다. 현재 발전되고 있는, VPN 표준들은 IPsec의 사용을 포함하고, IPsec은 암호 알고리즘들(cryptographic algorithms)들 및 IP 네트워크들 기능의 방식(the way IP networks function)의 심오한 이해를 요구하는 매우 복잡한 기술 표준이다. IPsec 기술을 전개하는 장치들을 환경설정하는 것은 포함된 많은 수의 파라미터들 때문에 복잡한 작업이다. 정확한 환경설정(configuration)은 특정 VPN 클라이언트가 VPN 게이트웨이에 연결할 수 있고, 따라서 DLNA 원격 액세스 시나리오들을 가능하게 하는 것을 보장한다. 그러나, 대부분의 소비자들은 본질적인 기술의 전문 지식을 가지고 있지 않으므로 , 이런 VPN 장치들을 정확하게 환경설정할 수 있는 필수 기술들을 가질 수 없다.

<7> 기업(corporate) 환경에서, 수많은 독점적인(proprietary) 해결책들이 이런 문제들을 해결하기 위해 발전하였다. 이런 해결책들은 종종 VPN 게이트웨이 제조업체에 의해 제공된다. 그러나, 이런 해결책들은 특정 VPN 게이트웨이 하드웨어에 종속되어 상호 운용될 수 없고, 해결책들의 비용들은 보통 일반적인 소비자들의 범위 훨씬 밖이다.

발명의 상세한 설명

<8> 본 발명은 IGD와 함께 배치된 VPN 게이트웨이를 환경설정할 수 있게 하는 오픈 인터페이스의 사용을 포함한다. 본 발명은 게이트웨이-게이트웨이 VPN을 설립하기 위해 VPN 게이트웨이가 있는 다른 IGD를 환경설정하기 위한 메커니즘 뿐만 아니라, UPnP 메시지들을 통해 VPN 클라이언트들에게 VPN 파라미터들을 공급해주기 위한 메커니즘을 제공한다.

<9> 본 발명은 종래의 시스템들에 비해 수많은 이점을 제공한다. 본 발명의 시스템 및 방법들 하에서, 사용자는 다양한 VPN 장치들의 제조업체 또는 제조업체들에 상관없이, VPN 파라미터들을 구성하는 능력을 가질 수 있다. 본 발명이 가진 복잡성은 상대적으로 낮고, 본 발명은 본 발명 전에는, 사업체, 대규모, 공공 기관의 사용자들에게만 이용가능했던, VPN 기술들을 일반적인 소비자들에게도 액세스할 수 있게 만든다.

<10> 본 발명의 이런 그리고 다른 목적들, 이점들, 및 특징들은 본 발명의 동작 구성 및 방식과 함께, 첨부된 도면들에 연결되어 고려될 때, 아래의 상세한 설명들로부터 명백해질 것이고, 동일한 엘리먼트들은 아래에 설명될 몇몇의 도면들을 통해 동일한 참조번호들을 가질 것이다.

실 시 예

<17> 도 1 및 도 2는 본 발명이 구현될 수 있는 하나의 대표적인 이동 전화(12)를 도시한다. 그러나, 본 발명은 하나의 특정 유형의 이동 전화(12) 또는 다른 전자 장치에 제한되는 의도가 아님은 이해되어야 한다. 예를 들어, 본 발명은 PDA(personal digital assistant) 및 이동 전화의 콤비네이션, PDA, IMD(integrated messaging device), 데스크탑 컴퓨터, 및 노트북 컴퓨터에 포함될 수 있다. 도 1 및 도 2의 이동 전화(12)는 하우징(30), LCD(liquid crystal display) 형태의 디스플레이(32), 키패드(34), 마이크(36), 이어피스(ear-piece)(38), 배터리(40), 적외선 포트(42), 안테나(44), 본 발명의 하나의 실시 예에 따른 범용 IC 카드(universal integrated circuit card, UICC) 형태의 스마트 카드(46), 시스템 클록(clock)(43), 카드 리더(reader)(48), 무선 인터페이스 회로(52), 코덱 회로(54), 제어기(56), 및 메모리(58)를 포함한다. 개개의 회로들 및 엘리먼트들은 예를 들어. 노키아의 이동 전화들의 범위 내인 당업계에 주지된 모든 유형이다.

<18> 통신 장치들은 비록 제한되지는 않지만, 코드 분할 다중 접속(Code Division Multiple Access, CDMA), 이동 통신 세계화 시스템(Global System for Mobile Communications, GSM), 범용 이동 통신 시스템(Universal Mobile Telecommunications System, UMTS), 시간 분할 다중 접속(Time Division Multiple Access, TDMA), 주파수 분할 다중 접속(Frequency Division Multiple Access, FDMA), 전송 제어 프로토콜/인터넷 프로토콜(Transmission Control Protocol/Internet Protocol, TCP/IP), 단문 메시징 서비스(Short Messaging Service, SMS), 멀티미디어 메시징 서비스(Multimedia Messaging Service, MMS), 이메일, 인스턴스 메시징 서비스(Instant Messaging Service, IMS), 블루투스, IEEE 802.11, 등을 포함하는 다양한 전송 시스템을 사용하여 통신할 수 있다.

<19> 본 발명은 IGD와 나란히 놓인(collocated) VPN 게이트웨이의 환경설정(configuration)을 가능하게 하는 오픈 인터페이스를 제공한다. VPN 파라미터들은 UPnP 메시지들을 통해 VPN 클라언트들을 위해 준비될 수 있다. 추가로, 또 다른 IGD는 게이트웨이-게이트웨이 VPN을 설립하기 위해 VPN 게이트웨이와 동시에 환경설정될 수 있다.

<20> 본 발명의 서비스는 즉 자택 및 소규모 사무실의 LAN들인, 관리되지 않는 네트워크 공간을 위해 VPN 게이트웨이를 제어, 모니터링 및 환경설정(configuration)을 가능하게 한다. 본 발명은 VPN 게이트웨이를 설정(setting up), VPN 클라이언트들을 환경설정(configuring)/ 공급, 및 사용 문제들을 진단 및 모니터링하기 위해 요구되는 핵심 엘리먼트들에 중점을 둔다. 본 발명은 설정(setup) 경험을 단순화시키고, VPN 게이트웨이 상의 문제들을 진단 및 모니터링하는 프레임웍(framework)을 제공한다.

<21> 본 발명은 많은 상이한 기능들을 가능하게 한다. 예를 들어, 본 발명은 암호 알고리즘 및 해시 함수(hash function)들의 사용을 통해, VPN 게이트웨이에 의해 받아들여진 IPsec 터널의 보안(security) 파라미터들의 원격 설정(remote setup) 및 구성을 허용한다. 본 발명은 또한 공유 키(shared key)들 및 공인인증서(certificate)들의 사용을 통해 VPN 게이트웨이에 의해 받아들여진 인증(authentication) 모드의 원격 설정 및 구성을 허용한다. VPN 터널의 원격 진단들 및 모니터링 뿐만 아니라, VPN 클라이언트 설정(setting)들의 원격 구성 및 준비가 또한 가능하다.

<22> 도 3은 LAN 및 WAN에서, 인터넷 게이트웨이 장치(100) 및 그 장치와 다른 장치들과의 관계의 표현이다. 인터넷 게이트웨이 장치(100)는 복수의 WAN 장치들(110) 및 복수의 LAN 장치들(120)을 포함한다. 복수의 LAN 장치들(120)은 하나 이상의 LAN들(140) 내에 위치한 복수의 클라이언트 장치들(130)에 연결할 수 있다. 복수의 WAN 장치들(110)은 인터넷(160) 또는 또 다른 WAN 내에 위치한 다양한 인터넷 서비스 제공자들(Internet Service Providers, ISPs)(150)에 연결할 수 있다. 이런 전체 배열은 인터넷 게이트웨이 장치(100)가 클라이언트 장치들(130) 및 개개의 ISP들 사이에서 경로(conduit) 역할을 하게 허용한다.

<23> 도 4는 본 발명의 VPN 환경설정(configuration) 서비스를 지원하는 빌트인(built-in) IGD 제어 포인트를 갖는 이동전화(12)가, VPN 게이트웨이 서포트(support)를 갖는 IGD 장치(100)를 환경설정하기(configure) 위해 사용되는 시나리오를 설명한다. 이동 전화(12)는 홈 네트워크(170) 내에서 IGD 장치(100)의 LAN 인터페이스를 통해 연결된다. 이동 전화(12) 내의 애플리케이션은 요구된 보안 프로토콜들, 보안 프로토콜들의 인증 및 프라이버시(privacy) 파라미터들, 그리고 세션 타임-아웃들(time-outs)을 조정하기 위해 VPN 환경설정을 편집할 수 있다. 환경설정 단계가 종료된 후에, 이제 VPN 클라이언트인, 이동 전화(12)는 새로운 환경설정(configuration)의 사용을 개시할 수 있다.

<24> 아래는 본 발명의 하나의 실시 예에 따라, VPN 클라이언트에게 VPN 파라미터들을 공급하기 위한 하나의 대표적인 시스템이다. 이런 상황에서, 이동 전화(12)는 VPN 클라이언트 애플리케이션을 가진다. 빌트인 IGD 제어 포인트는 LAN 인터페이스를 통해 IGD를 VPN 게이트웨이와 연결하기 위해 사용된다. 빌트인 IGD 제어 포인트는 VPN 게이트웨이 파라미터들을 읽고, 그것이 이동 전화에서 작동하는 때 자기 자신을 환경설정한다. 게이트웨이를 환경설정하기 위해 필요한 파라미터들은, 비록 제한되지는 않지만, VPN 게이트웨이의 IP 주소(들), 보안 프로토콜들, 및 보안 프로토콜들에 특정된 인증 및 프라이버시 파라미터들이다. 이후에, 도 5에 도시된 것과 같이, 이동 전화(12)가 원격 장소에 있고, 홈 네트워크(170)로부터 떨어져 있을 때, VPN 클라이언트 애플리케이션은 VPN 클라이언트 애플리케이션이 모든 필수 파라미터들을 가지므로, 홈 VPN 게이트웨이와 더불어 VPN 터널(190)을 생성할 수 있다.

<25> 본 발명은 게이트웨이-게이트웨이 VPN을 생성하기 위해 또 다른 VPN 게이트웨이를 환경설정하는데(configure) 사용될 수 있다. 예를 들어, 사용자 A가 사용자 B를 방문하고, 사용자 A의 홈 네트워크(210) 내에 위치한 퍼스널 비디오 레코더(personal video recorder)(200) 내에 저장된 수많은 미디어 파일들에 액세스해서, 사용자 B의 홈 네트워크(230) 내의 텔레비전(220)에서 그 파일들을 보기를 원하는 상황이, 발생할 수 있다. 이런 작업을 달성하기 위해, 도 6에 도시된 것과 같이, 2개의 홈 네트워크들(210, 230)이 하나의 단일 가상 홈 네트워크로 본

질상 합병될 수 있도록, IGD-IGD VPN 터널(235)이 홈 네트워크 A의 IGD(240)와 홈 네트워크 B의 IGD(250) 사이에 생성된다. 이런 배열에서, 사용자 A의 이동 전화(12) 내의 IGD 제어 포인트는 자체의 홈 VPN 게이트웨이(이것은 홈 네트워크 A의 IGD(240)임)에 관해 필요한 모든 정보를 가진다고 가정한다. 다음 단계는 이동 전화(12)가 VPN 게이트웨이 서포트를 갖는 홈 네트워크 B의 IGD(250)에 LAN 인터페이스를 통해 연결하는 것을 포함한다. 이동 전화(12)는 VPN 터널을 설립하기 위해 필수 정보를 VPN 게이트웨이로 전송한다. 이런 정보는, VPN 게이트웨이의 IP 주소(들), 보안 프로토콜들, 및 보안 프로토콜들에 특정된 인증 및 프라이버시 파라미터들이며, 그것들에 제한되지는 않는다.

<26> 아래는 본 발명의 하나의 특정 실시 예를 구현하기 위한 과정이다. 진행하기에 앞서, 포함된 장치들 및 네트워크들에 관련된 수많은 가정을 한다. 첫째, 사용자의 홈 네트워크는 사용자의 집에서 상시(always-on) 연결을 포함한다고 가정한다. 이런 연결은 광대역 연결, 또는 어떤 다른 종류의 연결을 포함한다. 포함된 장치들을 UPnP를 할 수 있고, 포함된 VPN 제품들(즉, VPN 게이트웨이 및 VPN 클라이언트)은 가상 사설 네트워크 컨소시엄(irtual Private Network Consortium, VPNC)에 의해 공표된 표준들에 따라 테스트된다. 이런 표준들은 인터넷 상의 http://www.vpnc.org/testing.html에서 찾아질 수 있다. 또한, VPN 게이트웨이가 있는 IGD는 UPnP IGD VPN 환경설정 서비스를 포함한다고 가정한다.

<27> 이런 상황에서, 사용자는 새로운 인터넷 게이트웨이 장치를 구매한다. 인터넷 게이트웨이 장치에 대한 특징 리스트는 원격 액세스를 위한 서포트를 표시한다. 사용자는 인터넷 게이트웨이 장치를 홈 네트워크에 꽂고, 설정 소프트웨어를 설치한다. 설정 마법사(wizard)는 인터넷 게이트웨이 장치를 환경설정하기 위해 사용된다. 설정 소프트웨어는 보안 프로토콜들을 위한 인증 및 프라이버시 파라미터들 뿐만 아니라, 보안 프로토콜들을 구성하기 위해 사용된다. 설정 소프트웨어는 또한 VPN 게이트웨이를 특정 WAN 인터페이스들에 연결한다. 설정 소프트웨어는 빌트인 UPnP IGD 제어 포인트를 포함한다. 그 시점에서, VPN 게이트웨이가 있는 IGD는 사용 준비가 된다. 향상된 기능성을 고려하면, VPN은 홈 네트워크 풀(pool)로부터 원격 장치들까지 IP 주소들을 제공한다.

<28> 이동 전화와 같은, 특정 장치에서 원격 액세스를 위해, 사용자는 원격 액세스를 가능하게 하는 새로운 소프트웨어 패키지를 이동 전화 내에 설치한다. 이후에, 사용자가 사무실을 떠날 때, 홈 네트워크 내의 장치에서 개시되는 활동(activity)을 하길 원하는지 결정한다. 사용자는 이때 활동을 개시하기 위해 원격 액세스를 통해 홈 네트워크로 연결되는 이동 전화를 가질 수 있다.

<29> 게이트웨이-게이트웨이 VPN이 생성될 수 있는 상황은 아래와 같이 설명될 수있다. 제1 사용자 및 제2 사용자는 각각 제1 홈 네트워크 및 제2 홈 네트워크로 지칭되는, 자신의 홈 네트워크를 가질 수 있다. 제1 사용자가 제2 홈 네트워크 근처에 있고 제2 사용자로 하여금 제1 홈 네트워크로 액세스하기를 원하는 경우, 제1 사용자는 제1 네트워크로의 원격 액세스를 위해 제2 사용자의 인터넷 게이트웨이를 구성하도록 자신의 이동전화를 사용할 수 있다. 따라서 제1 사용자는 제2 홈 네트워크의 인터넷 게이트웨이로의 일시 액세스를 허용하고 게이트웨이-게이트웨이 VPN을 생성하는 연결을 개시할 수 있다.

<30> 본 발명은 본 발명의 방법에 따른 단계들의 일반적 문맥 내에 설명되고, 이것은 네트워크 환경들에서 컴퓨터들에 의해 실행되는 프로그램 코드와 같은 컴퓨터 실행가능 명령들을 포함하는 프로그램 생성물에 의해 하나의 실시 예에서 구현될 수 있다.

<31> 일반적으로, 프로그램 모듈들은 특정 업무들을 수행하거나 특정한 추상적인 데이터 유형들을 구현하는, 루틴(routine)들, 프로그램들, 오브젝트들, 컴포넌트들, 데이터 구조들 등을 포함한다. 데이터 구조들에 연관된 컴퓨터 실행가능한 명령들 및 프로그램 모듈들은 개시된 본 발명에 따른 방법들의 단계들을 실행하기 위한 프로그램 코드의 예들을 나타낸다. 이런 실행가능한 명령들 또는 연관된 데이터 구조들의 특정 시퀀스(sequence)는 이런 단계들 내에 설명된 기능들을 구현하기 위한 행동(act)들에 대응하는 예들을 나타낸다.

<32> 본 발명의 소프트웨어 및 웹 구현들은 다양한 데이터베이스의 탐색 단계들, 상관관계(correlation) 단계들, 비교 단계들 및 결정 단계들을 완성하기 위한 규칙 기반의 논리 및 다른 논리를 갖는 표준 프로그래밍 기법들로 완성될 수 있다. 명세서 및 청구항들에서 사용되는 "컴포넌트" 및 "모듈"이라는 용어들은 소프트웨어 코드의 하나 이상의 라인들을 사용하는 구현들, 및/ 또는 하드웨어 구현들, 및/ 또는 수동 입력들을 수신하기 위한 장비를 포함하도록 의도된 것임을 또한 유의해야 한다.

<33> 전술한 본 발명의 실시 예들의 설명은 예시 및 설명의 목적으로 제시되었다. 그것은 본발명의 모든 것을 망라하거나, 개시된 정확한 형태로 본 발명을 제한하려는 의도가 아니고, 수정들 및 변화들이 위에서 교시된 것에 비추어 가능하거나 본 발명의 실행으로부터 얻어질 수 있다. 본 발명의 원리들 및 당업자가 다양한 실시 예들에서

그리고 심사숙고되는 특정 용도에 적합한 다양한 변경들로 본 발명을 이용할 수 있게 하는본 발명의 원리들의 실제적인 애플리케이션을 설명하기 위해, 실시 예들이 선택되고 설명되었다.

도면의 간단한 설명

<11> 도 1은 본 발명의 구현에 사용될 수 있는 이동 전화의 투시도.

<12> 도 2는 도 1의 이동 전화의 전화 회로의 개략적인 표현을 도시한 도면.

<13> 도 3은 LAN 및 WAN 내에서 인터넷 게이트웨이 장치와 그것의 다른 장치들과의 관계를 표현하는 도면.

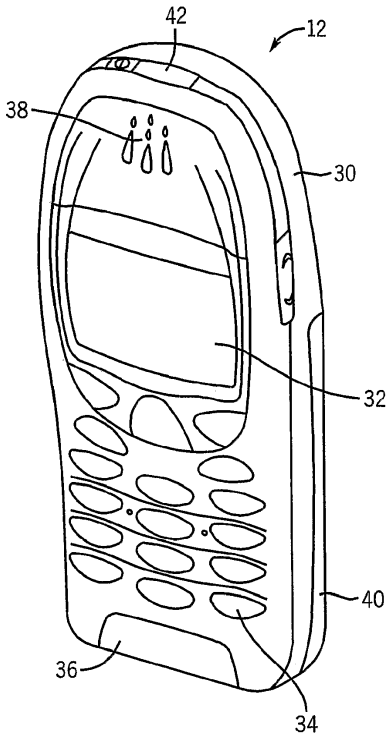
<14> 도 4는 본 발명을 지원하는 빌트인(built-in) IGD 제어 포인트(IGD control point)를 갖는 이동전화가 VPN 게이트웨이 서포트(support)를 갖는 인터넷 게이트웨이 장치를 환경설정하기 위해 사용되는 시나리오를 표현하는 도면.

<15> 도 5는 VPN 터널이 인터넷 게이트웨이 장치와 홈 네트워크 외부에 있는 전자장치 사이에 형성되는 상황을 표현하는 도면.

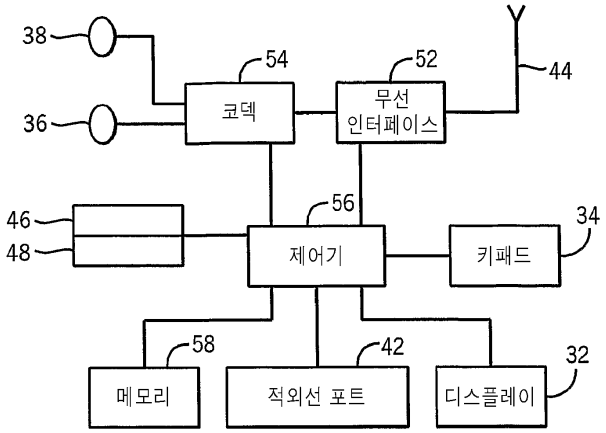
<16> 도 6은 VPN 게이트웨이-게이트웨이 터널이 홈 네트워크들 사이에 생성되는 상황을 표현하는 도면.

도면

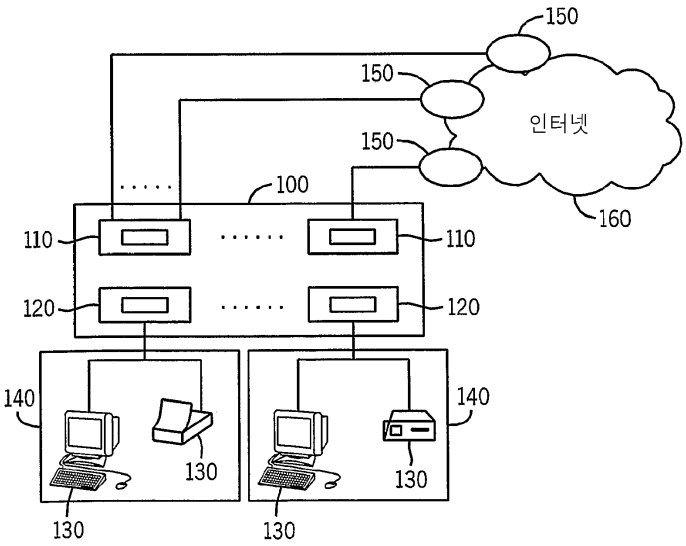
도면1



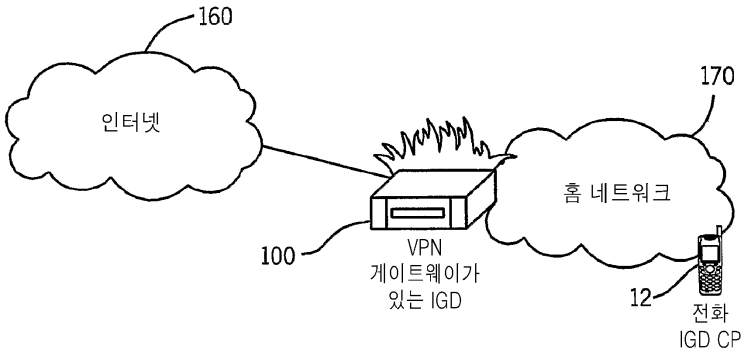
도면2


38
36
54
코덱
52
무선
인터페이스
44
46
48
56
제어기
키패드
34
58
메모리
42
적외선 포트
32
디스플레이

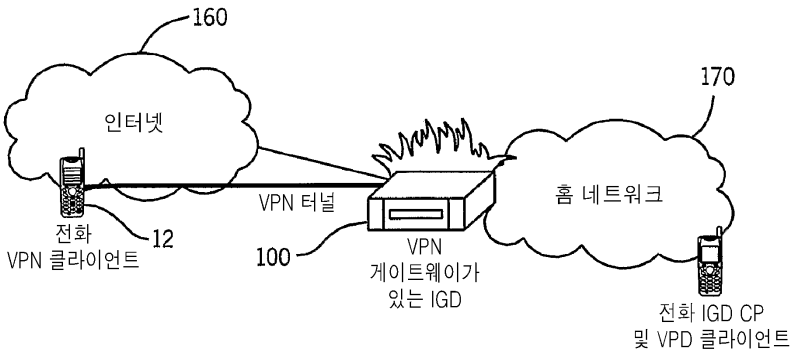
도면3


150
150
150
인터넷
160
100
110
110
120
120
140
140
130
130
130
130

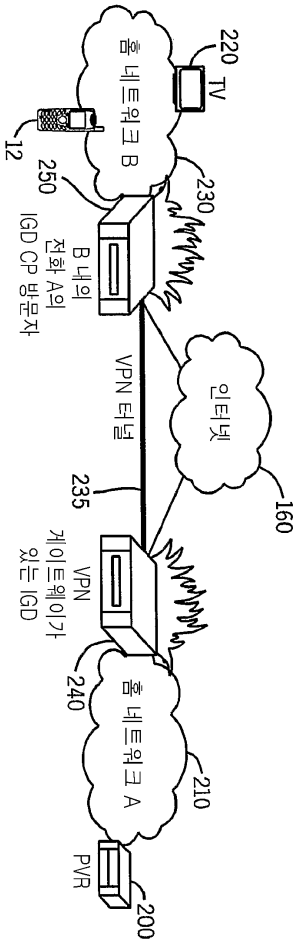
도면4


160
인터넷
170
홈 네트워크
100
VPN
게이트웨이가
있는 IGD
12
전화
IGD CP

도면5



도면6



【심사관 직권보정사항】

【직권보정 1】

【보정항목】 청구범위

【보정세부항목】 청구항 제11항 4번째 줄

【변경전】

상기 전자 장치를

【변경후】

전자 장치를