(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2023년01월09일
(11) 등록번호 10-2486871
(24) 등록일자 2023년01월05일

(51) 국제특허분류(Int. Cl.)
H04L 45/00 (2022.01) *G06F 9/455* (2018.01)
H04L 101/375 (2022.01) *H04L 41/0894* (2022.01)
H04L 41/40 (2022.01) *H04L 45/76* (2022.01)
H04L 61/256 (2022.01) *H04L 9/40* (2022.01)
H04W 88/16 (2009.01)
(52) CPC특허분류
H04L 45/00 (2022.05)
G06F 9/45533 (2013.01)
(21) 출원번호 10-2022-7024107(분할)
(22) 출원일자(국제) 2016년12월02일
심사청구일자 2022년07월13일
(85) 번역문제출일자 2022년07월13일
(65) 공개번호 10-2022-0104279
(43) 공개일자 2022년07월26일
(62) 원출원 특허 10-2018-7019406
원출원일자(국제) 2016년12월02일
심사청구일자 2021년12월01일
(86) 국제출원번호 PCT/IB2016/001827
(87) 국제공개번호 WO 2017/098320
국제공개일자 2017년06월15일
(30) 우선권주장
62/264,791 2015년12월08일 미국(US)
15/090,918 2016년04월05일 미국(US)
(56) 선행기술조사문헌
EP02557854 A2
US08316435 B1
US20120166618 A1
US20120233668 A1

(73) 특허권자
제이피유.아이오 엘티디
이스라엘 49514 페타크 티크바 임버 14 피오 박스 4098
(72) 발명자
슈워츠, 조나단
이스라엘 69626 텔 아비브 모쉬 콜 스트리트 8
말카, 프랭크
이스라엘 40300 크파 요나 피오비 7081 시갈론 스트리트 46
(74) 대리인
양영준, 임규빈, 백만기

전체 청구항 수 : 총 35 항 심사관 : 윤태섭

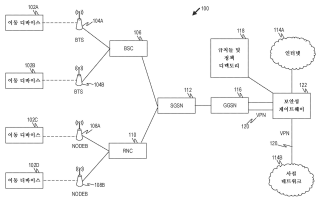
(54) 발명의 명칭 **이동 네트워크 내에서의 라우팅 및 보안성**

(57) 요 약

예시적인 실시예에서, PICNEEC가 제공된다. 그것은 하나 이상의 가상적인 맞춤화된 규칙들 집행기(VCRE) 인스턴스들을 포함하고, 각각의 VCRE 인스턴스는 이동 디바이스들의 그룹에 대응하고, 이동 디바이스들의 그룹에 대하여 개인화된 정책들의 세트를 정의한다. 각각의 VCRE는 라디오 네트워크를 통해 패킷-기반 네트워크와, 대응하

(뒷면에 계속)

대 표 도



는 그룹에서의 이동 디바이스 사이에서 통신된 데이터 패킷을 수신할 시에, 데이터 패킷을 포워딩하기 이전에 데이터 패킷에 대한 VCRE 인스턴스에서 저장된 하나 이상의 정책 규칙들을 실행하도록 구성된다. 각각의 VCRE 인스턴스는 이동 네트워크 제공자의 상이한 고객에 의한 VCRE 인스턴스의 직접적인 액세싱을 통해 서로에 독립적으로 제어된다.

(52) CPC특허분류
H04L 41/0894 (2022.05)
H04L 41/40 (2022.05)
H04L 45/76 (2022.05)
H04L 61/256 (2022.05)
H04L 63/20 (2013.01)
H04W 88/16 (2013.01)
H04L 2101/375 (2022.05)

명 세 서

청구범위

청구항 1

이동 네트워크 제공자에 의한 동작을 위해 하나 이상의 하드웨어 프로세서에 의해 실행가능한 PDN 통합된 맞춤화된 네트워크 에지 인에이블러 및 제어기(PDN Integrated Customized Network Edge Enabler and Controller)(PICNEEC)로서,

메모리; 및

적어도 하나의 가상적인 맞춤화된 규칙들 집행기(Virtual Customized Rules Enforcer)(VCRE) 인스턴스 - 각각의 VCRE 인스턴스는 이동 디바이스들의 그룹에 대응하고 이동 디바이스들의 그룹에 대해 개인화된 정책들의 세트를 정의하고, 각각의 VCRE 인스턴스는 셀룰러-기반 네트워크인 라디오 네트워크를 통해 패킷-기반 네트워크와, 대응하는 그룹에서의 이동 디바이스 사이에서 통신된 데이터 패킷을 수신할 시에, 상기 데이터 패킷을 포워딩하기 이전에 상기 데이터 패킷에 대한 VCRE 인스턴스에서 저장된 하나 이상의 정책 규칙들을 실행하도록 구성되고, 각각의 VCRE 인스턴스는 상기 이동 네트워크 제공자의 상이한 고객에 의한 VCRE 인스턴스의 직접적인 액세싱을 통해 서로 독립적으로 제어되고, 상기 하나 이상의 정책 규칙들은 상기 VCRE 인스턴스와 상기 셀룰러-기반 네트워크 사이의 트래픽에 적용되도록 설계된 정책 규칙들임 - 를

포함하는 PICNEEC.

청구항 2

제1항에 있어서, 상기 데이터 패킷은 서빙 일반 패킷 라디오 서비스(General Packet Radio Service)(GPRS) 지원 노드/서빙(Serving GPRS Support Node/Serving)(SGSN)과, 상기 PICNEEC에 대해 내부적인 게이트웨이 GPRS 지원 노드(Gateway GPRS Support Node)(GGSN) 사이에서 라우팅되는 PICNEEC.

청구항 3

제1항에 있어서, 상기 데이터 패킷은 서빙 게이트웨이(Serving Gateway)(SGW)와, 상기 PICNEEC에 대해 내부적인 패킷 데이터 네트워크 게이트웨이(Packet Data Network Gateway)(PGW) 사이에서 라우팅되는 PICNEEC.

청구항 4

제1항에 있어서, 상기 데이터 패킷은 서빙 일반 패킷 라디오 서비스(GPRS) 지원 노드/서빙(SGSN)과, 상기 PICNEEC에 대해 외부적인 게이트웨이 GPRS 지원 노드(GGSN) 사이에서 라우팅되고, 상기 외부적인 GGSN은 상기 PICNEEC를 통해 인터넷 프로토콜(Internet Protocol)(IP) 접속성 액세스 네트워크에 대한 데이터를 핸들링하는 PICNEEC.

청구항 5

제1항에 있어서, 상기 데이터 패킷은 서빙 게이트웨이(SGW)와, 상기 PICNEEC에 대해 외부적인 PGW 사이에서 라우팅되고, 상기 외부적인 PGW는 상기 PICNEEC를 통해 IP 접속성 액세스 네트워크에 대한 데이터를 핸들링하는 PICNEEC.

청구항 6

제1항에 있어서, 상기 데이터 패킷은 상기 PICNEEC를 통해 상기 데이터 패킷을 핸들링하는 이동 네트워크 서빙 패킷 게이트웨이를 통해 라우팅되는 PICNEEC.

청구항 7

제1항에 있어서, 적어도 하나의 VCRE 인스턴스는 맞춤화된 액세스 포인트 명칭(access point name)(APN)들을 정의하고, 각각의 APN은 네트워크 식별자 및 운영자 식별자를 갖는 PICNEEC.

청구항 8

제1항에 있어서, 적어도 하나의 VCRE 인스턴스는 독립적인 가상 네트워크 기능인 PICNEEC.

청구항 9

제1항에 있어서, 적어도 하나의 VCRE 인스턴스는 독립적인 물리적 네트워크 기능인 PICNEEC.

청구항 10

제1항에 있어서, 적어도 하나의 VCRE 인스턴스는 더 큰 네트워크 기능에서의 규칙들의 서브세트이고, 상기 고객은 규칙들의 특정 서브세트를 오직 액세스할 수 있는 PICNEEC.

청구항 11

제1항에 있어서, 적어도 하나의 VCRE 인스턴스는 VCRE 규칙들 기능(RCF) 콘솔을 이용하여 고객에 의해 생성되는 PICNEEC.

청구항 12

제11항에 있어서, 상기 RCF 콘솔은 보안 쉘(Secure Shell)(SSH) 액세스인 PICNEEC.

청구항 13

제1항에 있어서, 적어도 하나의 VCRE 인스턴스는 VCRE 규칙들 기능(RCF) 애플리케이션을 이용하여 고객에 의해 생성되는 PICNEEC.

청구항 14

제13항에 있어서, 상기 RCF 애플리케이션은 애플리케이션 프로그램 인터페이스(application program interface)(API)인 PICNEEC.

청구항 15

제13항에 있어서, 상기 RCF 애플리케이션은 웹사이트인 PICNEEC.

청구항 16

제13항에 있어서, 상기 RCF 애플리케이션은 전용 컴퓨터 프로그램인 PICNEEC.

청구항 17

제11항에 있어서, 상기 RCF 콘솔은 적어도 하나의 VCRE 인스턴스를 직접적으로 관리하는 PICNEEC.

청구항 18

제13항에 있어서, 상기 RCF 애플리케이션은 적어도 VCRE 인스턴스를 직접적으로 관리하는 PICNEEC.

청구항 19

제11항에 있어서, 상기 RCF 콘솔은 상기 VCRE 인스턴스들 중 적어도 하나를 관리하는 중앙 RCF에 접속하는 PICNEEC.

청구항 20

제13항에 있어서, 상기 RCF 애플리케이션은 상기 VCRE 인스턴스들 중 적어도 하나를 관리하는 중앙 RCF에 접속하는 PICNEEC.

청구항 21

제1항에 있어서, 고객은 대응하는 VCRE 인스턴스와 외부 네트워크 사이의 가상 사설 네트워크(virtual private network)(VPN)를 정의함으로써 상기 대응하는 VCRE 인스턴스를 정의하는 PICNEEC.

청구항 22

제1항에 있어서, 고객은 대응하는 VCRE 인스턴스와 IP 접속성 네트워크들 사이의 네트워크 라우팅을 정의함으로써 상기 대응하는 VCRE 인스턴스를 정의하는 PICNEEC.

청구항 23

제1항에 있어서, 고객은 대응하는 VCRE 인스턴스를 통과하는 패킷 데이터 트래픽에 대한 방화벽 규칙들을 정의함으로써 상기 대응하는 VCRE 인스턴스를 정의하는 PICNEEC.

청구항 24

제1항에 있어서, 고객은 대응하는 VCRE 인스턴스를 통과하는 패킷 데이터 트래픽에 대한 네트워크 어드레스 변환(network address translation)(NAT) 규칙들을 정의함으로써 상기 대응하는 VCRE 인스턴스를 정의하는 PICNEEC.

청구항 25

제1항에 있어서, 고객은 대응하는 VCRE 인스턴스를 통과하는 패킷 데이터 트래픽에 대한 도메인 명칭 시스템(domain name system)(DNS) 설정들을 정의함으로써 상기 대응하는 VCRE 인스턴스를 정의하는 PICNEEC.

청구항 26

제1항에 있어서, 고객은 대응하는 VCRE 인스턴스를 통과하는 패킷 데이터 트래픽에 대한 보안성 규칙들을 정의함으로써 상기 대응하는 VCRE 인스턴스를 정의하는 PICNEEC.

청구항 27

제1항에 있어서, 고객은 IP 어드레스들을 이동 디바이스들에 배정함으로써 대응하는 VCRE 인스턴스를 정의하는 PICNEEC.

청구항 28

제1항에 있어서, 고객은 대응하는 VCRE 인스턴스를 통과하는 트래픽에 대한 하이퍼텍스트 전송 프로토콜 헤더 강화(Hypertext Transfer Protocol Header Enrichment)(HHE) 규칙들을 정의함으로써 상기 대응하는 VCRE 인스턴스를 정의하는 PICNEEC.

청구항 29

방법으로서,

하나 이상의 하드웨어 프로세서에 의해 실행가능한 PICNEEC에서, 셀룰러-기반 네트워크인 라디오 네트워크를 통해 이동 디바이스와 패킷-기반 네트워크 사이에서 전송된 데이터 패킷을 수신하는 단계;

상기 데이터 패킷에서의 정보에 기초하여, 상기 이동 디바이스에 배정된 VCRE 인스턴스 - 상기 VCRE 인스턴스는 상기 PICNEEC를 동작시키는 이동 네트워크 제공자의 고객에 의한 상기 VCRE 인스턴스의 직접적인 액세싱을 통해 상기 PICNEEC에서의 다른 VCRE 인스턴스들에 독립적으로 제어됨 - 를 결정하는 단계;

상기 데이터 패킷에 대해 상기 VCRE 인스턴스에서 정의된 하나 이상의 정책 규칙들을 실행하는 단계 - 상기 하나 이상의 정책 규칙들은 상기 VCRE 인스턴스와 인터넷 프로토콜(IP) 접속성 네트워크들 사이의 라우팅을 위한 라우팅 테이블을 관리하는 규칙 및 상기 VCRE 인스턴스와 상기 셀룰러-기반 네트워크 사이의 트래픽에 적용되도록 설계된 정책 규칙을 포함함 -; 및

상기 라우팅 테이블에 기초하여 상기 데이터 패킷을 라우팅하는 단계

를 포함하는 방법.

청구항 30

제29항에 있어서, 상기 데이터 패킷은 서빙 일반 패킷 라디오 서비스(GPRS) 지원 노드/서빙(SGSN)과, 상기 PICNEEC에 대해 내부적인 게이트웨이 GPRS 지원 노드(GGSN) 사이에서 라우팅되는 방법.

청구항 31

제29항에 있어서, 상기 데이터 패킷은 서빙 게이트웨이(SGW)와, 상기 PICNEEC에 대해 내부적인 PGW 사이에서 라우팅되는 방법.

청구항 32

제29항에 있어서, 상기 데이터 패킷은 서빙 일반 패킷 라디오 서비스(GPRS) 지원 노드/서빙(SGSN)과, 상기 PICNEEC에 대해 외부적인 게이트웨이 GPRS 지원 노드(GGSN) 사이에서 라우팅되고, 상기 외부적인 GGSN은 상기 PICNEEC를 통해 인터넷 프로토콜(IP) 접속성 액세스 네트워크에 대한 데이터를 핸들링하는 방법.

청구항 33

제29항에 있어서, 상기 데이터 패킷은 서빙 게이트웨이(SGW)와, 상기 PICNEEC에 대해 외부적인 PGW 사이에서 라우팅되고, 상기 외부적인 PGW는 상기 PICNEEC를 통해 IP 접속성 액세스 네트워크에 대한 데이터를 핸들링하는 방법.

청구항 34

제29항에 있어서, 상기 데이터 패킷은 상기 PICNEEC를 통해 상기 데이터 패킷을 핸들링하는 이동 네트워크 서빙 패킷 게이트웨이를 통해 라우팅되는 방법.

청구항 35

이동 네트워크 제공자에 의한 동작을 위해 하나 이상의 하드웨어 프로세서에 의해 실행가능한 PDN 통합된 맞춤화된 네트워크 에지 인에이블러 및 제어기(PICNEEC)로서,

적어도 하나의 가상적인 맞춤화된 규칙들 집행기(VCRE) 인스턴스 - 각각의 VCRE 인스턴스는 이동 디바이스들의 그룹에 대응하고 이동 디바이스들의 그룹에 대해 개인화된 정책들의 세트를 정의하고, 각각의 VCRE 인스턴스는 셀룰러-기반 네트워크인 라디오 네트워크를 통해 패킷-기반 네트워크와, 대응하는 그룹에서의 이동 디바이스 사이에서 통신된 데이터 패킷을 수신할 시에, 상기 데이터 패킷을 포워딩하기 이전에 상기 데이터 패킷에 대한 상기 VCRE 인스턴스에서 저장된 하나 이상의 정책 규칙들을 실행하도록 구성되고, 각각의 VCRE 인스턴스는 상기 이동 네트워크 제공자의 상이한 고객에 의한 상기 VCRE 인스턴스의 직접적인 액세싱을 통해 서로 독립적으로 제어되고, 상기 하나 이상의 정책 규칙들은 상기 VCRE 인스턴스와 상기 셀룰러-기반 네트워크 사이의 트래픽에 적용되도록 설계된 정책 규칙들임 - 를 포함하고;

상기 PICNEEC는 3G/4G 네트워크 및 저 전력 광역 네트워크(Low Power Wide Area Network)(LPWAN)에 동시에 접속되는 PICNEEC.

발명의 설명

기 술 분 야

[0001] 우선권

[0002] 이 출원은 2015년 12월 8일자로 출원된 미국 가출원 제62/264,791호의 이익을 주장한다. 이 출원은 2016년 4월 5일자로 출원된 미국 특허 출원 제15/090,918호의 우선권을 또한 주장한다.

[0003] 기술 분야

[0004] 본 개시내용은 일반적으로 이동 라디오 네트워킹에 관한 것이다. 더 구체적으로, 본 개시내용은 이동 라디오 네트워크 내에서의 네트워크 라우팅 및 보안성을 위한 기법을 설명한다.

배 경 기 술

[0005] 이동 네트워크들은 디바이스들이 국제 표준 기구들에 의해 정의된 바와 같이 네트워크 내에서 제공된 기본적인 서비스의 일부로서 (인터넷과 같은) 외부 패킷 교환 네트워크들에 접속하는 것을 허용한다. 이러한 국제 표준 기구들의 예는 이동 통신들을 위한 글로벌 시스템(Global System for Mobile Communications)(GSM)/유니버셜 이동 전기통신 시스템(Universal Mobile Telecommunication System)(UMTS)/롱텀 에볼루션(Long-Term

Evolution)(LTE) 도메인들에 대한 3세대 파트너십 프로젝트(3rd Generation Partnership Project)(3GPP), 시간 분할 다중 액세스(Time Division Multiple Access)(TDMA)/코드 분할 다중 액세스(Code Division Multiple Access)(CDMA)/CDMA2000 네트워크들, 및 LoRa 및 SIGFOX와 같은 더 새로운 네트워크 설계 이니셔티브들을 포함한다.

[0006] 이러한 시스템들에서, 이동 디바이스로 들어가고 이동 디바이스로부터 나오는 패킷 데이터는 라디오 네트워크를 통해, 2G 네트워크에서의 기지국 트랜시버(Base Transceiver Station)(BTS), 3G 네트워크에서의 NodeB, 또는 4G 네트워크에서의 eNodeB와 같은 엘리먼트(element)들로 송신된다. 그 후에, 패킷 데이터는 터널들을 이용하여 2G/3G 네트워크에서의 서빙 일반 패킷 라디오 서비스(General Packet Radio Service)(GPRS) 지원 노드(Serving GPRS Support Node)(SGSN), 또는 4G 네트워크에서의 서빙 게이트웨이(Serving Gateway)(SGW), 또는 다른 이동 네트워크 솔루션들에서의 유사한 디바이스를 향해 전송된다.

[0007] 모든 이동 디바이스들로부터의 GPRS 터널링 프로토콜(GPRS Tunnelling Protocol)(GTP) 터널들은 2G/3G 네트워크에서의 게이트웨이 GPRS 지원 노드(Gateway GPRS Support Node)(GGSN), 또는 4G 네트워크에서의 PDN 게이트웨이(PDN Gateway)(PGW), 또는 다른 이동 네트워크 솔루션들에서의 유사한 디바이스를 향해 응집(aggregate)된다. 그 다음으로, 이 디바이스들은 각각의 접속에서 수 많은 터널들을 포함하는 많은 이더넷(Ethernet) 접속들을 병합한다.

[0008] 그 다음으로, 응집된 GTP 터널들 트래픽을 다수의 데이터 스트림들로 분산시키고 매 단일 스트림을 이동 디바이스에 의해 초기에 지정된 바와 같이, 외부 패킷 교환 네트워크 상의 그 지정된 목적지로 라우팅하는 것은 GGSN 또는 PGW의 책임이다.

[0009] 3GPP 표준들은 각각의 이동 디바이스가 액세스 포인트 명칭(Access Point Name)(APN)으로 칭해진, 그것이 적당한 GGSN 또는 PGW에 접속하게 하는 라우팅 컨텍스트(routing context)를 정의할 것이라는 것을 또한 정의한다. 3GPP 표준들은 각각의 APN이 특정 규칙 세트를 이용하여 방화벽(firewall)을 통해 패킷 데이터를 라우팅하기 위한 능력과 함께, GGSN 또는 PGW 내에서 그 자신의 라우팅 및 보안성 정책을 가지는 것을 허용한다.

[0010] 그러나, 그 또는 그녀가 라우터 장비(예컨대, GGSN 또는 PGW)를 오직 액세스하기 때문에, 이러한 APN 맞춤화된 규칙 세트들은 이동 네트워크 운영자 직원에 의해 정의된다.

[0011] 대조적으로, 이동 네트워크 컨텍스트 외부에서는, 개인들 또는 조직들이 그 자신의 라우팅 및 방화벽 장비를 전개시킬 수 있고 그 디바이스들의 네트워크 능력들에 대한 전체 제어를 유지할 수 있다. 이 정책이 이동 네트워크 운영자에 의해 오직 정의될 수 있기 때문에, 이 능력은 그 이동 디바이스들에 대한 그 자신의 라우팅 및 보안성 정책들을 정의하는 것을 원하는 임의의 개인 또는 조직으로부터 오늘 날에 박탈된다.

도면의 간단한 설명

[0012] 일부 실시예들은 동반되는 도면들의 도들에서 제한이 아니라, 예로서 예시되어 있다.

도 1은 예시적인 실시예에 따라, 이동 네트워크 통신들을 라우팅하기 위한 시스템을 예시하는 블록도이다.

도 2는 예시적인 실시예에 따라, GPRS 서브-네트워크 서비스들을 위한 프로토콜 스택들을 예시하는 블록도이다.

도 3은 SGSN/SGW 및 GGSN/패킷 데이터 네트워크(Packet Data Network)(PDN) 게이트웨이(PDN Gateway)(PGW)를 포함하는 시스템을 예시하는 블록도이다.

도 4는 예시적인 실시예에 따라, SGSN/SGW, 및 GGSN/PGW를 포함하는 PDN 통합된 맞춤화된 네트워크 에지 인에이블러 및 제어기(PDN Integrated Customized Network Edge Enabler and Controller)(PICNEEC)를 포함하는 시스템을 예시하는 블록도이다.

도 5는 예시적인 실시예에 따라, VCRE를 더 상세하게 예시하는 블록도이다.

도 6은 예시적인 실시예에 따라, PICNEEC 정책 데이터 구조를 예시하는 도면이다.

도 7은 예시적인 실시예에 따라, 일 예의 표들을 예시하는 도면이다.

도 8은 예시적인 실시예에 따라, 사용자 인터페이스를 예시하는 스크린 캡처이다.

도 9는 예시적인 실시예에 따라, 사용자 인터페이스를 예시하는 스크린 캡처이다.

도 10은 예시적인 실시예에 따라, 이동 네트워크에서 데이터 패킷들 접속을 확립(establish)하고 핸들링

(handle)하는 방법을 예시하는 상호작용 도면이다.

도 11은 예시적인 실시예에 따라, 이동 네트워크 내로부터 외부 IP 네트워크를 향하는 발신 데이터 패킷을 핸들링하는 방법을 예시하는 흐름도이다.

도 12는 또 다른 예시적인 실시예에 따라, 외부 IP 네트워크로부터 이동 네트워크를 향하는 착신 데이터 패킷을 핸들링하는 방법을 예시하는 흐름도이다.

도 13은 예시적인 실시예에 따라, SGSN/SGW, 및 외부 PICNEEC를 갖는 단독형 GGSN/PGW를 포함하는 시스템을 예시하는 블록도이다.

도 14는 예시적인 실시예에 따라, 외부 PICNEEC를 갖는 이동 네트워크에서 데이터 패킷들을 핸들링하는 방법을 예시하는 상호작용 도면이다.

도 15는 또 다른 예시적인 실시예에 따라, 다수의 SGSN/SGW들 및 다수의 PICNEEC들을 포함하는 시스템을 예시하는 블록도이다.

도 16은 또 다른 예시적인 실시예에 따라, 다수의 SGSN/SGW들 및 다수의 PICNEEC들을 포함하는 시스템을 예시하는 블록도이다.

도 17은 예시적인 실시예에 따라, PICNEEC(1702)를 포함하는 시스템(1700)을 예시하는 블록도이다.

도 18은 본원에서 설명된 다양한 하드웨어 아키텍처들과 함께 이용될 수도 있는 대표적인 소프트웨어 아키텍처를 예시하는 블록도이다.

도 19는 일부 예시적인 실시예들에 따라, 머신-판독가능한 매체(예컨대, 머신-판독가능한 저장 매체)로부터 명령들을 판독할 수 있고 본원에서 논의된 방법론들 중 임의의 하나 이상을 수행할 수 있는 머신의 컴포넌트들을 예시하는 블록도이다.

발명을 실시하기 위한 구체적인 내용

[0013] 뒤따르는 설명은 예시적인 실시예들을 구체화하는 예시적인 시스템들, 방법들, 기법들, 명령 시퀀스들, 및 컴퓨팅 머신 프로그램 제품들을 포함한다. 다음의 설명에서는, 설명의 목적들을 위하여, 수 많은 특정 세부사항들이 발명 요지의 다양한 실시예들의 이해를 제공하기 위하여 기재되어 있다. 그러나, 발명 요지의 실시예들은 이 특정 세부사항들 없이 실시될 수도 있다는 것이 본 기술분야의 통상의 기술자들에게 분명할 것이다. 일반적으로, 널리-공지된 명령 인스턴스들, 프로토콜들, 구조들, 및 기법들은 상세하게 도시되지 않았다.

[0014] 예시적인 실시예에서는, 개인 또는 조직이 이동 네트워크 운영자의 개입 없이 하나 이상의 이동 디바이스들에 대한 라우팅 및/또는 보안성 정책들을 정의하는 것을 허용하는 이동 네트워크 내의 라우팅 시스템이 제공된다.

[0015] 도 1은 예시적인 실시예에 따라, GSM(2G) 및/또는 UMTS(3G) 이동 네트워크들에서의 네트워크 통신들을 라우팅하기 위한 시스템(100)을 예시하는 블록도이다. 시스템(100)은 하나 이상의 이동 디바이스들(102A 내지 102D)을 포함한다. 각각의 이동 디바이스(102A 내지 102D)는 셀 트랜시버(cell transceiver)로서 보편적으로 알려진 라디오 통신기를 가지는 임의의 유형의 디바이스일 수도 있다. 이동 디바이스들(102A 내지 102D)은 예를 들어, 스마트폰들, 태블릿 컴퓨터들, 접속된 자동차들, 센서들, 경보 시스템들 등을 포함한다.

[0016] 각각의 이동 디바이스(102A 내지 102D)는 라디오 통신들을 통해 이동 네트워크에 접속한다. 도 1에서는, 2 개의 별도의 예의 유형들의 이동 네트워크들이 도시되어 있다. 첫 번째는 GSM-기반 이동 네트워크이다. GSM-기반 이동 네트워크들에서, 이동 디바이스들(102A, 102B)은 기지국 트랜시버(BTS)(104A, 104B)와의 라디오 통신을 통해 접속한다. BTS들(104A, 104B)은 라디오 인터페이스에 대한 종단 노드들이다. 각각의 BTS(104A, 104B)는 하나 이상의 트랜시버들을 포함하고, 라디오 인터페이스의 암호화를 담당한다.

[0017] 그 다음으로, 각각의 BTS(104)는 기지국 제어기(base station controller)(BSC)(106)와 통신한다. 전형적으로, BSC(106)는 그 제어 하에서 수 백 개의 BTS들(104A, 104B)을 가진다. BSC(106)는 라디오 자원들을 이동 디바이스들(102A, 102B)에 할당하고, 주파수들을 관리하고, BTS들 사이의 핸드오버들을 제어하도록 작동한다. BSC(106)는 집신기(concentrator)로서 또한 작동할 수 있어서, BSC(106)로의 많은 저 용량 접속들은 더 작은 수의 접속들로 감소된다.

[0018] 여기에서 도시된 제2 유형의 이동 네트워크는 유니버셜 이동 전기통신 시스템 UMTS-기반 이동 네트워크이다. UMTS-기반 이동 네트워크는 광대역 코드 분할 다중 액세스(wideband code division multiple access)(W-CDMA)

라디오 액세스 기술을 이용한다. 여기서, 이동 디바이스들(102C 내지 102D)은 NodeB(108A, 108B)와의 라디오 통신을 통해 접속한다. NodeB들(108A, 108B)은 라디오 인터페이스에 대한 종단 노드들이다. 각각의 NodeB(108A, 108B)는 하나 이상의 트랜시버들을 포함하고, 라디오 인터페이스의 암호화를 담당한다. 각각의 NodeB(108A 내지 108B)는 CDMA-기반 UMTS 네트워크에서 채널들을 설명하기 위한 코드들을 적용하도록 구성된다. 일반적으로, 각각의 NodeB(108A 내지 108B)는 BTS(104A 내지 104B)가 GSM 네트워크에 대하여 수행하는 UMTS 네트워크에 대한 유사한 기능들을 수행한다.

[0019] 그 다음으로, 각각의 NodeB(108A 내지 108B)는 라디오 네트워크 제어기(radio network controller)(RNC)(110)와 통신한다. 전형적으로, RNC(110)는 그 제어 하에서 수 백 개의 NodeB들(108A, 108B)을 가진다. RNC(110)는 라디오 자원들을 이동 디바이스들(102C, 102D)에 할당하고, 주파수들을 관리하고, NodeB들(108A 내지 108B) 사이의 핸드오버들을 제어하도록 작동한다. RNC(110)는 집신기로서 또한 작동할 수 있어서, RNC(110)로의 많은 저 용량 접속들은 더 작은 수의 접속들로 감소된다.

[0020] 2 개의 상이한 이동 네트워크 유형들이 여기에서 도시되어 있지만, 이 개시내용에서 설명된 개념들은 도 1에서 도시된 네트워크 유형들에 추가적으로, 또는 그 대신에 중 어느 하나로, 오직 단일 네트워크 유형을 가지는 시스템들 뿐만 아니라, 다수의 네트워크 유형들을 가지는 시스템들에서 작동할 것이라는 것이 주목되어야 한다.

[0021] BTS들(104A, 104B) 및/또는 NodeB들(108A, 108B)은 네트워크 내에서 모든 패킷 교환된 데이터를 핸들링하는 서빙 GPRS 지원 노드(SGSN)(112)에 접속한다. 전형적인 시스템(100)에서는 실제적으로 2 개의 형태들의 GPRS 지원 노드(GPRS Support Node)(GSN)들이 있다. 여기에서 관련성이 있는 것은 제1 유형이다: 그 지리적 서비스 영역 내에서 BTS들(104A, 104B 및 NodeB들(108A, 108B)로 그리고 이로부터의 데이터 패킷들의 전달을 전형적으로 담당하는 SSGN. 추가적인 태스크들은 패킷 라우팅 및 전송, 이동성 관리(연결/연결해제 및 이동성 관리), 논리적 링크 관리, 및 과금 기능들을 포함할 수도 있다.

[0022] 일부 예시적인 실시예들에서, SGSN(112)에 대하여 위에서 설명된 기능들은 단순화를 위하여 여기에서 도시되지 않은 서빙 게이트웨이(SGW)에 의해 수행된다. 일부 다른 예시적인 실시예들에서, 일부 다른 유형의 디바이스는 SGSN(112)에 대하여 위에서 설명된 기능들을 수행할 수도 있다. SGSN들(112) 및 SGW들을 포함하는 이 유형들의 디바이스들의 전부는 "응집기(aggregator)들" 또는 "패킷 응집기(packet aggregator)들로 집합적으로 칭해질 수도 있다.

[0023] 데이터 패킷들은 이동 디바이스(102A 내지 102D)로부터 인터넷(114A) 또는 사설 네트워크(114B)와 같은 외부 패킷 교환 데이터 네트워크를 향해 업스트림으로 전송된다. SGSN(112)은 이동 디바이스들(102A 내지 102D)로부터의 데이터 패킷들을 응집하고, 그것들을 GSN의 제2 유형인 게이트웨이 GPRS 지원 노드(GGSN)(116)로 전송한다. GGSN(116)은 GPRS 네트워크와 외부 패킷 교환 네트워크들(114A, 114B) 사이의 인터네트워킹(internetworking)을 담당한다. 외부 네트워크의 관점으로부터, GGSN(116)은 외부 네트워크로부터 GPRS 기반구조를 은닉하므로, GGSN(116)은 서브-네트워크로의 라우터이다. GGSN(116)이 특정 사용자에게 어드레싱된 데이터를 수신할 때, 그것은 사용자가 활성인지를 체크한다. 그러할 경우, GGSN(116)은 데이터를 이동 사용자를 서빙하는 SGSN(112)으로 포워딩한다. 이동 사용자가 비활성일 경우, 데이터는 폐기된다. GGSN(116)은 GPRS 네트워크에서의 사용자 단말의 이동성을 가능하게 하는 앵커점(anchor point)이다.

[0024] GGSN(116)은 각각의 개별적인 데이터 스트림에 대하여, 데이터 스트림이 규칙들 및 정책 디렉토리(118)에서 관련되는 이동 디바이스(102)를 룩업(look up)한다. 규칙들 및 정책 디렉토리(118)는 라우팅 및/또는 보안성을 위한 규칙들을 포함한다. 예를 들어, 규칙들 및 정책 디렉토리(118)는 특정한 이동 디바이스(102)가 특정한 네트워크 방향에서의 데이터 트래픽 라우팅을 가져야 한다는 것, 또는 특정한 보안성 프로토콜(예컨대, IPSec)이 그 이동 디바이스(102)로 및/또는 그 이동 디바이스(102)로부터의 데이터 트래픽을 위하여 이용되어야 한다는 것을 표시할 수도 있다. 그 다음으로, GGSN(116)은 어떤 라우팅 정책들이 데이터 트래픽에 적용되는지를 구현하도록 작동한다.

[0025] 트래픽은 예를 들어, 가상 사설 네트워크(Virtual Private Network)(VPN)(120)를 통해 사설 네트워크(114B)를 향해 지향될 수도 있다. VPN(120)은 규칙들 및 정책 디렉토리(118)에서의 정보를 이용하여 정의되고 제어된다.

[0026] 그 다음으로, (VPN(120)을 갖거나 갖지 않는) 모든 트래픽은 방화벽, 월드 가든(walled garden), 블랙리스트화된 IP들 등과 같은 다수의 네트워크 보안성 메커니즘들을 채용하도록 작동하는 보안성 게이트웨이(122)를 통해 라우팅된다. 보안성 게이트웨이(122)는 디바이스-바이-디바이스(device-by-device)(또는 디바이스의 그룹-바이-디바이스의 그룹(group of device-by-group of device))에 기초하여 프로비저닝(provision)될 수도 있는 보안

성 규칙들을 확립할 시에 규칙들 및 정책 디렉토리(118)에서의 정보를 이용한다.

[0027] 따라서, 집행된 라우팅 규칙들 및 보안성 정책들에 기초하여, 업스트림 데이터 패킷들은 외부 패킷 교환 네트워크(114A, 114B)에서의 그 목적지를 향해 전송된다.

[0028] 다운스트림 패킷들은 외부 패킷 교환 네트워크(114A, 114B)로부터 보안성 게이트웨이(122), VPN(120), GGSN(116), 및 SGSN(112)을 통해, 다시 완전히 대응하는 이동 디바이스(102A 내지 102D)로 전송된다.

[0029] (개인 또는 조직과 같은) 이동 디바이스(102A 내지 102D)를 제어하는 엔티티(entity)는 예를 들어, 개인 또는 조직이 내부 네트워크에서 이러한 엘리먼트들을 제어하는 것처럼, 네트워크 엘리먼트들의 조작, 구성, 및 모니터링을 허용하는 외부 콘솔 또는 다른 유형의 통신을 이용함으로써 보안성 게이트웨이(122), VPN(120), 및 GGSN(116)을 구성할 수도 있다.

[0030] 전형적으로, 이동 디바이스들(102)은 이동 디바이스(102)를 위한 액세스 포인트 명칭(APN)을 구성함으로써 이동 네트워크 상으로 온보드화(onboard)된다. 각각의 이동 디바이스(102)는 그것에 배정된 고유한 APN을 가진다. 예시적인 실시예에서, 시스템(100)은 이동 디바이스(102)로 또는 이동 디바이스(102)로부터의 데이터 트래픽에 대한 라우팅 또는 보안성 정책들을 제공하기 위하여 APN 정보를 사용할 필요가 없다. 디바이스들의 각각의 그룹은 고객이 예를 들어, 미리 정의된 보안성 프로파일들(예컨대, 접속된 자동차, 센서)의 선택, 월드 가든들의 정의, VPN 액세스의 확립들, 방화벽 규칙들의 정의, 및 인터넷 이동 가입자 아이덴티티(Internet Mobile Subscriber Identity)(IMSI)에 기초한 IP 어드레스 할당들을 포함하는 그 또는 그녀의 자신의 설정들을 정의할 수 있는 그 자신의 "라우터/방화벽" 인스턴스(instance)를 배정받는다.

[0031] 도 2는 예시적인 실시예에 따라, GPRS 서브-네트워크 서비스들을 위한 프로토콜 스택들을 예시하는 블록도이다. 이동 디바이스(MS)(200), 기지국(BS)(202), SGSN(204), 및 GGSN(206)이 여기에서 도시된다. GTP(208)는 Gn 인터페이스를 이용하여 SGSN(204)과 GGSN(206) 사이에서 이용된 프로토콜이다. 이것은 계층 3 터널링 프로토콜이다. 발생하는 프로세스는 네트워크의 내부 및 외부의 사용자들을 위한 정상적인 IP 서브-네트워크처럼 보인다. 애플리케이션(210)은 GPRS 네트워크를 통해 반송(carry)되고 GGSN(206)을 통해 출력되는 IP(212)를 통해 통신한다. GGSN(206)과 SGSN(204) 사이에서 이동하고 있는 패킷들은 GTP(208)를 이용한다. 이러한 방법으로, GPRS의 외부 측 상에 위치된 IP 어드레스들은 내부 백본(backbone)을 처리할 필요가 없다. SGSN(204) 상에서, UDP(214) 및 IP(212)는 GTP(208)에 의해 작동된다.

[0032] 서브네트워크 종속적 융합 프로토콜(SubNetwork Dependent Convergence Protocol)(SNDCP)(216) 및 논리적 링크 제어(Logical Link Control)(LLC)(218)는 SGSN(204)과 MS(200) 사이에서 조합으로 이용된다. SNDCP는 사용자 평면 GPRS 프로토콜 스택의 최상단 계층이다. SNDCP(216)는 라디오 채널 상의 부하를 감소시키기 위하여 데이터를 평탄화(flatten)한다. SNDCP(216)의 주요 목적은 네트워크 프로토콜 데이터 유닛(protocol data unit)(PDU)들을 버퍼링하고 세그먼트화하고, 헤더들을 각각의 세그먼트에 추가하고, 그 다음으로, 송신을 위하여 세그먼트를 LLC(218)에 주기 위한 것이다. 패킷들을 암호화함으로써 생성된 안전한 논리적 링크는 LLC(218)에 의해 제공되고, 동일한 LLC(218) 링크는 모바일(mobile)이 단일 SGSN(204) 하에 있는 한 이용된다. SNDCP(216)는 압축 및 압축해제를 또한 수행한다. 사상은 보조를 통해 전송되도록 요구되는 데이터의 양을 감소시키기 위한 것이다. 이와 같이, SNDCP(216)는 압축-관련된 기능들을 위한 패킷-데이터 네트워크(PDN) 프로토콜에 대한 어떤 세부사항들을 종종 인지하고 있다. SNDCP(216)는 PDP 컨텍스트들, 및 PDP 유형, QoS 등과 같은 대응하는 정보를 또한 인지하고 있을 수도 있다. 이 정보는 PDP 컨텍스트 활성화 절차들 동안에 주어진다.

[0033] LLC(218)의 기능은 데이터 송신들의 무결성을 관리하고 보장하기 위한 것이다. LLC(218)는 데이터 링크 계층 링크들을 네트워크 계층 프로토콜들을 위한 서비스들에 제공한다. 이것은 네트워크 컴퓨터들 상에서 상주하는 서비스들에 대한 LLC 서비스 액세스 포인트들에 의해 달성된다. 추가적으로, 전달 요청들 또는 서비스들에 대한 LLC 제어 필드가 있다. LLC(218)는 패킷들의 암호화(ciphering) 및 역암호화(deciphering)를 또한 수행할 수도 있다.

[0034] 도 3은 SGSN/SGW(302) 및 GGSN/PDN 게이트웨이(PGW)(304)를 포함하는 시스템(300)을 예시하는 블록도이다. 예시적인 실시예에서, SGSN/SGW(302)는 도 1의 SGSN(112)일 수도 있고, GGSN/PGW(304)는 도 1의 GGSN(116)일 수도 있다. SGSN/SGW(302)는 이동 라디오 네트워크로부터 Gn 인터페이스를 통해 GGSN/PGW(304)로 데이터를 전송한다. Gn은 GPRS 터널링 프로토콜(GTP) 터널들로 이루어진다. GTP는 터널들을 제어하는 GTP-C, 및 실제적인 사용자 트래픽 데이터인 GTP-U로 분할된다.

[0035] 온라인 과금 시스템(online charging system)(OCS)(306)은 Gy 기준점을 통해 GGSN/PGW(304)에 접속한다.

OCS(306)는, 어떤 터널이 대역폭에 대한 할당량을 가지는지를 GGSN/PGW(304)에 알리고, 또한, 사용자 당 실제적인 서비스 계획 및 계좌 잔고에 기초하여 터널들을 허용하거나 불허하기 위한 청구 시스템이다. 온라인 과금은 2 개의 서브-기능들: 레이팅 및 단위 결정을 가진다. 그것들의 양자는 중앙집중화되거나 탈중앙집중화된 것으로서 구현될 수 있다.

[0036] 레이팅은 단위 결정 기능에 의해 계산된 비-금전적 단위(non-monetary unit)들로부터의 피스(piece)의 계산을 지칭한다. 단위 결정은 서비스 전달을 시작하기 이전에 배정될 비-금전적 단위들(서비스 단위들, 데이터 용량, 시간, 및 이벤트들)의 수의 계산을 지칭한다.

[0037] 온라인 과금에 대한 3 개의 경우들이 구별될 수 있다: 즉각적 이벤트 과금(Immediate Event Charging)(IEC), 단위 예약을 갖는 이벤트 과금(Event Charging with Unit Reservation)(ECUR), 및 단위 예약을 갖는 세션 과금(Session Charging with Unit Reservation)(SCUR).

[0038] IEC는 직접적인 인출(direct debit) 동작을 수반하고, 여기서, 금융 계좌는 적절한 과금에 대하여 즉시 인출된다. ECUR에서는, 금융 단위들이 서비스 전달 이전에 예약되고, 금융 계좌 인출 동작은 서비스 전달의 결론 후에 수행된다. SCUR에서는, 금융 단위들이 세션 감시 이전에 예약되고, 금융 계좌 인출 동작은 세션 종결의 결론 후에 수행된다.

[0039] 오프라인 과금 시스템(offline charging system)(OFCS)(308)은 Gz 기준점을 통해 GGSN/PGW(304)에 접속한다. OFCS(308)는 선불 호출 세부내역 레코드(call detail record)(CDR) 프로세싱을 위한 청구 시스템이다. 오프라인 과금은 네트워크 자원 사용에 대한 과금 정보가 그 자원 사용과 동시에 수집되는 프로세스이다. 그 다음으로, 과금 정보는 논리적 과금 기능들의 체인을 통과하게 된다. 이 프로세스의 종료 시에, CDR 파일들은 네트워크에 의해 생성되고, 그 다음으로, 가입자 청구 및/또는 상호운영자 회계(또는 통계들과 같은 추가적인 기능들)의 목적을 위하여 네트워크 운영자의 청구 도메인으로 전달된다. 청구 도메인은 운영자의 청구 시스템 또는 청구 중재 디바이스와 같은 포스트-프로세싱 시스템들을 전형적으로 포함한다.

[0040] 오프라인 과금 기능들의 예들은 과금 트리거 기능(charging trigger function)(CTF), 과금 데이터 기능(charging data function)(CDF), 및 과금 게이트웨이 기능(charging gateway function)(CGF)을 포함한다. CTF는 네트워크 자원 사용의 관찰에 기초하여 과금 이벤트들을 생성한다. CTF는 네트워크 엘리먼트 내에서 과금가능한 이벤트들에 속하는 정보를 수집하고, 이 정보를 정합하는 과금 이벤트들로 조립하고, 이 과금 이벤트들을 CDF를 향해 전송하기 위한 초점(focal point)이다. CTF는 2 개의 기능적인 블록들: 네트워크 사용자들에 의해 확립된 호출들, 서비스 이벤트들, 또는 세션들에 대한 시그널링 기능들, 또는 그 호출들, 서비스 이벤트들, 또는 세션들에 대한 사용자 트래픽의 핸들링, 또는 이 호출들, 서비스 이벤트들, 또는 세션들을 통한 사용자로의 서비스 전달을 모니터링하는 계좌 메트릭들 수집과, 수집된 회계 메트릭들을 수신하고, 메트릭들 중 하나 이상의 세트로부터 과금가능한 이벤트들의 발생을 결정하고, 그 다음으로, 검출된 과금가능한 이벤트들과 정합하는 과금 이벤트들을 조립하고, 과금 이벤트들을 Rf 인터페이스를 통해 과금 데이터 기능을 향해 포워딩하는 회계 데이터 포워딩으로 이루어진다.

[0041] CDF는 Rf 기준점을 통해 CTF로부터 과금 이벤트들을 수신한다. 그 다음으로, 그것은 CDR들을 구축하기 위하여 과금 이벤트들에서 포함된 정보를 이용한다. CDF에 의해 생성된 CDR들은 Ga 인터페이스 점을 통해 과금 게이트웨이 기능(CGF)으로 즉시 전달된다. CGF는 실시간에 근접한 Ga 인터페이스를 통한 CDF로부터의 CDR 수신, CDR 프리-프로세싱, CDR들의 유효성검사, 통합, 및 (재)포맷팅, CDR 에러 핸들링, 지속적인 CDR 저장, CDR 라우팅 및 필터링, CDR 파일 관리, 및 청구 도메인으로의 CDR 파일 전송과 같은 기능들을 수행한다.

[0042] 패킷 데이터 네트워크(310)는 Gi 기준점을 통해 GGSN/PGW(304)에 접속한다. 패킷 데이터 네트워크(310)는 이동 디바이스들이 데이터를 전송할 수 있는 공공 또는 사설 데이터 네트워크이다. 정책 및 과금 규칙들 기능(PCRF)(312)은 Gx 기준점을 통해 GGSN/PGW(304)에 접속하고 GGSN/PGW(304)에서의 데이터 흐름 정책들을 집행하기 위한 방법의 일부이다. PCRF(312)는 규칙들을 수집하고 그것들을 GGSN/PGW(304)로 통과시키는 것을 담당한다. PCRF(312)는 서비스 데이터 흐름 검출, 게이팅(패킷들을 차단하거나 허용함), QoS 제어, 및 로우-기반 과금(low-based charging)에 관한 네트워크 제어를 제공한다. PCRF(312)는 예를 들어, 서비스 정보가 가입 정보와 일치하지 않을 때에 애플리케이션으로부터 수신된 요청을 거절할 수도 있다.

[0043] PCRF(312)는 Sp 기준점을 통해 가입 프로파일 저장소(subscription profile repository)(SPR)(314)에 접속한다. SPR(314)은 PDN 마다에 기초하여 전형적으로 저장된 가입자 및 가입 정보를 포함하고, 가입자의 허용된 서비스들, 가입자의 허용된 QoS에 대한 정보, 가입자의 과금 관련된 정보, 및 가입자 카테고리와 같은 정

보를 포함할 것이다. PCRF(312)는 각각의 관련된 사용자에 대한 프로파일들을 질의하기 위하여 SPR(314)을 액세스할 수 있다. 애플리케이션 기능(application function)(AF)(316)은 Rx 기준점을 통해 PCRF(312)에 접속하고, 외부 애플리케이션 로직이 PCRF 규칙들을 변경하는 것을 허용한다.

[0044] GGSN/PGW(304)는 PCRF(312)에 의해 만들어진 규칙들을 집행하기 위하여 정책 집행 규칙들 기능(policy enforcement rules function)(PCEF)(318)을 이용한다. GGSN/PGW(304)는 기본적인 라우팅 기능성 뿐만 아니라, VPN의 확립, 네트워크 어드레스 변환(network address translation)(NAT), 및 기본적인 방화벽을 허용하지만, 이 서비스들의 전부는 네트워크 운영자 구성에 기초하고, 이 기능성의 어느 것도 서비스의 실제적인 베어러(bearer)들(이동 디바이스들 및 그 소유자들 뿐만 아니라, 고객들로서 집합적으로 알려진 소유자들을 채용하는 기업들 또는 다른 조직들)에 의해 수정되도록 익스포트(export)되지 않는다. 그것들은 또한, 이동 디바이스들로부터의 특정 패킷 트래픽이 아니라, 접속되는 내부 및 외부 네트워크 엘리먼트들을 향해 지향된다. PCRF(312)는 블랙리스트(예컨대, 금지된 이동 디바이스들, 네트워크 로케이션들, 트래픽 유형들 등의 리스트)를 이용하여 보안성 규칙들을 또한 집행한다.

[0045] 예시적인 실시예에서, 도 3의 시스템(300)은 추가적인 기능성을 허용하도록 수정된다. 이 기능성은 그것의 GGSN 또는 PGW가 단지 2 개의 예의 컴포넌트들인 PDN 통합된 맞춤화된 네트워크 에지 인에이블러 및 제어기(PICNEEC)로 일반적으로 명명될 수도 있다. 도 4는 SGSN 또는 SGW(402), 및 PICNEEC(404)를 포함하는 시스템(400)을 예시하는 블록도이다. 예시적인 실시예에서, SGSN/SGW(402)는 도 1의 SGSN(112)일 수도 있고, GGSN/PGW(418)는 도 1의 GGSN(116)일 수도 있다. SGSN/SGW(402)는 이동 라디오 네트워크로부터 Gn 인터페이스를 통해 GGSN/PGW(418)로 데이터를 전송한다. PICNEEC(404)는 Gi 기준점 상에서 안착되는 가상적인 맞춤화된 규칙들 집행기(Virtual Customized Rules Enforcer)(VCRE)(406)를 포함한다. 그것은 PICNEEC(404)에 대해 내부적이거나, 현존하는 PICNEEC(404)에 대한 애드-온(add-on) 컴포넌트로서의 것 중 어느 하나일 수 있다. VCRE(406)는 시스템(400)에 대한 라우팅, 방화벽, VPN, 및 보안성 특징들을 정의한다. 정책 및 과금 규칙들 기능(PCRF)(408)와 같은 정책 및 과금 규칙들 컴포넌트는 GGSN/PGW(418)에서의 일반적인 정책 및 과금 규칙들을 실행한다.

[0046] 규칙들 맞춤화기 기능(Rules Customizer Function)(RCF)(410)은 외부 저장소, 및 정책 및 보안성 변경들 및 구성들의 전부를 VCRE(406)로 전달하는 제어 기능이다. RCF(410)는 그것이 애플리케이션 기능과 같은 애플리케이션 컴포넌트(412)인 것처럼, Rx 인터페이스를 이용하여 PVRF(408)에 또한 접속할 수도 있다. RCF 콘솔(414)은 라우팅 및 보안성 정책들을 설정하기 위하여 고객에 의해 이용된다. RCF 콘솔(414)은 예를 들어, 웹 포털, 보안 쉘(Secure Shell)(SSH) 액세스, 인간-머신 언어(Man-Machine Language)(MML) 인터페이스 등일 수도 있다.

[0047] RCF 애플리케이션(416)은 예를 들어, 외부 애플리케이션, 이동 디바이스 상의 애플리케이션 등으로부터의 RCF(410)에 대한 애플리케이션 프로그램 인터페이스(application program interface)(API) 액세스를 제공한다.

[0048] 고객은 VCRE를 정의하고, VCRE와 외부 네트워크 사이의 VPN을 정의하는 것, VCRE와 IP 접속성 네트워크들 사이의 네트워크 라우팅을 정의하는 것, VCRE 인스턴스를 통과하는 패킷 데이터 트래픽에 대한 방화벽 규칙들을 정의하는 것, VCRE 인스턴스를 통과하는 패킷 데이터 트래픽에 대한 NAT 규칙들을 정의하는 것, VCRE 인스턴스를 통과하는 패킷 데이터 트래픽에 대한 도메인 명칭 시스템(domain name system)(DNS) 설정들을 정의하는 것, VCRE 인스턴스를 통과하는 패킷 데이터 트래픽에 대한 보안성 규칙들을 정의하는 것, IP 어드레스들을 이동 디바이스들에 배정하는 것, 및 VCRE 인스턴스를 통과하는 트래픽에 대한 하이퍼텍스트 전송 프로토콜(Hypertext Transfer Protocol)(HTTP) 헤더 강화(Header Enrichment)(HHE) 규칙들을 정의하는 것을 포함하지만, 이것으로 제한되지는 않는 다양한 규칙들을 특정하기 위하여, RCF 콘솔(414) 또는 RCF 애플리케이션(416)의 어느 하나를 이용할 수도 있다.

[0049] HHE는 이동 디바이스가 HTTP 서버를 향한 http 요청을 생성할 때, 트래픽은 HTTP 서버가 요청이 어디에서 나왔는지를 식별하는 것을 허용하는 정보를 HTTP 헤더들에 추가하는 HTTP 프록시(통상적으로, GGSN/PGW 자체)를 통과한다는 것을 의미한다. 이러한 정보는 MSISDN(이동 디바이스 전화 번호) 또는 IMSI를 포함할 수 있다.

[0050] 도 5는 예시적인 실시예에 따라, 도 4의 VCRE(406)와 같은 VCRE(500)를 더 상세하게 예시하는 블록도이다. VCRE(500)는 방화벽/라우터/VPN/보안성 집행기의 다수의 가상적인 인스턴스들(502A 내지 502N)로 분할된다. 이동 디바이스들의 각각의 세트 도는 심지어 단일 이동 디바이스는 단일 VCRE 인스턴스(502A 내지 502N)에 의해 핸들링된다. 각각의 인스턴스에 대하여, 다수의 규칙들이 정의될 수 있다. 예를 들어, VCRE 인스턴스(502A)는 3 개의 디바이스들을 포함하는 디바이스 그룹(504A)에 대응한다. VCRE 인스턴스(502A)는 접속들이 VPN(508)을 통해 회사(506)로 오직 확립될 수도 있다는 것을 표시한다. VCRE 인스턴스(502B)는 2 개의 디바이스들을 포함

하는 디바이스 그룹(504B)에 대응한다. VCRE 인스턴스(502B)는 접속들이 VPN(510)을 통해 회사(506)로 행해질 수도 있거나 인터넷(512)에 접속할 수 있다는 것을 표시한다. VCRE 인스턴스(502C)는 단일 디바이스를 오직 포함하는 디바이스 그룹(504C)에 대응한다. VCRE 인스턴스(502C)는 접속들이 (디바이스가 액세스하도록 허용되는 IP 어드레스들이 제한될 경우에) VPN에 의해서가 아니라 월드 가든에 의해 사설 클라우드(514)로 행해질 수도 있다는 것을 표시한다.

[0051] VCRE(500)는 모든 VCRE 인스턴스들(502A 내지 502N) 중에서 일반적으로 수반되는 기능들을 수행하도록 작동하는 제어 블록(516)을 추가적으로 포함할 수도 있다. 이 기능들은 예를 들어, VCRE 인스턴스들의 확립, VCRE 인스턴스들(502A 내지 502N)로의 특정 이동 디바이스들의 할당, 및 VCRE 인스턴스들(502A 내지 502N)의 삭제를 포함한다. 추가적으로, 이하에서 더 상세하게 알게 되는 바와 같이, VCRE(500)가 GGSN에 대해 외부적인 경우, VCRE 제어 블록(516)은 이동 디바이스에 대한 IP 어드레스를 GGSN에 통지하고, 모든 트래픽을 그 IP 어드레스로부터 올바른 VCRE 인스턴스(502A 내지 502N)로 포워딩한다.

[0052] 각각의 VCRE 인스턴스(502A 내지 502N)는 그것이 라우팅 및 보안성 규칙들에 대하여 필요로 하는 정보를 저장하는 VCRE 데이터 구조를 포함할 수도 있다.

[0053] 각각의 VCRE 인스턴스(502A 내지 502N)는 이동 네트워크 제공자의 상이한 고객(PICNEEC를 제어한 엔티티)에 의한 VCRE 인스턴스(502A 내지 502N)의 직접적인 액세싱을 통해 서로에 독립적으로 제어된다.

[0054] 도 6은 예시적인 실시예에 따라, VCRE 정책 데이터 구조(600)를 예시하는 도면이다. 각각의 VCRE 정책 데이터 구조(600)는 정책에 대한 명칭이 특정될 수 있는 명칭 필드를 갖는 정책 컴포넌트(602)를 포함할 수도 있다. 이 정책 컴포넌트(602)에 연결된 것은 NAT 규칙들 컴포넌트(604), 방화벽 규칙들 컴포넌트(606), IP 규칙들 컴포넌트(608), 월드 가든 컴포넌트(610), 및 VPN 컴포넌트(612)이다. 모든 VCRE 데이터 구조들이 이 컴포넌트들(604 내지 612)의 전부를 가질 필요가 있는 것은 아니라는 것이 주목되어야 한다. 고객은 정책의 필요성들에 기초하여 이 컴포넌트들(604 내지 612) 중 어느 것을 포함할 것인지를 택할 수 있고 선택할 수 있다. 예를 들어, 특정한 정책이 월드 가든을 이용하지만, VPN을 이용하지 않을 경우, 월드 가든 컴포넌트(610)는 포함될 수도 있지만, VPN 컴포넌트(612)는 제외될 수도 있다.

[0055] NAT 규칙들 컴포넌트(604)는 출발지 어드레스, 목적지 어드레스, 프로토콜, 포트, 대상 어드레스(to address), 및 대상 포트(to port)와 같은 필드들을 포함할 수도 있다. 방화벽 규칙들 컴포넌트(606)는 목적지 어드레스, 출발지 어드레스, 프로토콜, 포트, 및 액션과 같은 필드들을 포함할 수도 있다. IP 규칙들 컴포넌트(608)는 목적지 어드레스 및 게이트웨이와 같은 필드들을 포함할 수도 있다. 월드 가든 컴포넌트(610)는 액세스하기 위한 허용된 로케이션들의 목적지 어드레스와 같은 필드들을 포함할 수도 있다. VPN 컴포넌트(612)는 목적지 어드레스, 출발지 어드레스, 및 사전 공유된 키와 같은 필드들을 포함할 수도 있다.

[0056] 정책 컴포넌트(602)는 필터 규칙들, 라우팅 규칙들, 패킷 스니퍼(packet sniffer) 규칙들, 심층 패킷 검사(deep packet inspection)(DPI) 규칙들, 부하 밸런싱 규칙들, 및 최신 IP 기반 네트워크들에서 채용되는 다른 컴포넌트들과 같은 추가적인 하위 컴포넌트들을 포함할 수도 있다.

[0057] 도 7은 예시적인 실시예에 따라, 일 예의 표들을 예시하는 도면이다. 사용자 표(700)는 사용자 명칭들(702A, 702B)의 리스트를 포함할 수도 있다. 사용자 명칭들(702A, 702B)은 다른 표들(704 내지 710)에서 사용될 수도 있다. 프로파일 표(704)는 사용자 명칭들(712)에 대한 열(column), 및 각각의 사용자 명칭(702A, 702B)과 연관된 대응하는 프로파일들(714)에 대한 열을 포함한다. 따라서, 여기에서는, 예를 들어, 각각의 사용자 명칭(702A, 702B)이 2 개의 가능한 프로파일들을 가진다. 예를 들어, Cars Co.(702A)는 N.A. 선단 프로파일(북미 선단 프로파일) 또는 S.A. 선단 프로파일(남미 선단 프로파일)의 프로파일을 가질 수 있다. 디바이스 표(706)는 개별적인 디바이스 명칭(716), 디바이스들 대응하는 IMSI(718), 디바이스와 연관된 사용자 명칭(720), 및 디바이스와 연관된 프로파일(722)의 표시를 포함한다. 알 수 있는 바와 같이, 각각의 사용자와 연관된 다수의 디바이스들이 있을 수도 있고, 각각의 개별적인 디바이스는 상이한 프로파일을 가질 수도 있다.

[0058] 규칙 표(708)는 각각의 보안성 프로파일(724)과 연관된 일련의 규칙들을 제공한다. 예를 들어, 규칙 유형(726), 액션(728), 프로토콜(730), 출발지 IP 어드레스(732), 목적지 IP 어드레스(734), 포트(736), 및 순서(738)가 각각의 규칙에 대하여 정의될 수도 있다. 물론, 이것들은 정의될 수 있는 다양한 상이한 유형들의 규칙들의 단지 예들이다.

[0059] 월드 가든 표(710)는 모든 다른 어드레스들을 금지하면서, 대응하는 프로파일(742)이 액세스를 허용하는 일련의 IP 어드레스들(740)을 제공한다.

[0060] 도 8은 예시적인 실시예에 따라, 사용자 인터페이스(800)를 예시하는 스크린 캡처이다. 사용자 인터페이스(800)는 더 이전에 설명된 바와 같이, RCF 콘솔(414) 및/또는 RCF 애플리케이션(416)의 일부로서 제공될 수도 있다. 사용자 인터페이스(800)는 회사의 관리자와 같은 사용자가 하나 이상의 규칙들을 생성하고 그 규칙들을 디바이스들의 보안성 그룹들과 연관시키는 것을 허용한다. 선택될 때, 탭(802)은 사용자가 인바운드 통신 정책들(예컨대, 패킷 데이터 네트워크(512, 514)로부터 디바이스로 전송되는 통신들에 대한 정책들)을 편집하거나, 삭제하거나, 추가하는 것을 허용한다. 선택될 때, 탭(804)은 사용자가 아웃바운드 통신 정책들(예컨대, 디바이스로부터 패킷 데이터 네트워크(512, 514)로 전송되는 통신들에 대한 정책들)을 편집하거나, 삭제하거나, 추가하는 것을 허용한다. 선택될 때, 탭(806)은 사용자가 그룹 멤버들(예컨대, 이 보안성 그룹의 일부인 디바이스들)을 추가하거나 삭제하는 것을 허용한다. 추가적으로, 버튼(808)은 사용자가 새로운 서비스 포트를 추가하는 것을 허용한다.

[0061] 도 9는 또 다른 예시적인 실시예에 따라, 사용자 인터페이스(900)를 예시하는 스크린 캡처이다. 사용자 인터페이스(900)는 사용자가 도 8의 사용자 인터페이스(800)의 버튼(808)을 선택할 때에 제시될 수도 있다. 여기서, 포트는 명칭(902), 설명(904), 서비스 유형(906), 프로토콜(908), 포트 번호(910), 범위(912), 및 포트 거동(914)을 배정받을 수 있다.

[0062] 도 10은 예시적인 실시예에 따라, 이동 네트워크에서 데이터 패킷들을 핸들링하는 방법(1000)을 예시하는 상호작용 도면이다. 방법(1000)은 이동 세트(mobile set)(MS)(1002), SGSN/SGW(1004), PICNEEC(1001)를 사용할 수도 있고, PICNEEC(1001)는 내부 GGSN/PGW(1006), VCRE(1008), RCF(1010), 및 패킷 데이터 네트워크(PDN)(1014)에 접속하는 VCRE 인스턴스(1012)를 갖는다. MS(1002)는 본원에서 설명된 보안성 및/또는 방화벽 규칙들의 대상물인 이동 디바이스들의 그룹일 수도 있다.

[0063] 동작(1016)에서, MS(1002)는 네트워크에 등록하고 SGSN/SGW(1004)를 통해 자신을 인증하는 것을 시도한다. 이것은 패킷 데이터 프로토콜(packet data protocol)(PDP)을 생성하는 것으로 칭해진다. PDP 컨텍스트는 가입자가 활성 세션을 가질 때에 가입자의 세션 정보를 포함하기 위하여, SGSN/SGW(1004) 및 GGSN/PGW(1006)의 양자상에서 제시될 데이터 구조이다. 이동 디바이스가 GPRS를 이용하는 것을 희망할 때, 그것은 먼저 연결하고, 그 다음으로, PDP 컨텍스트를 활성화한다. 이것은 가입자가 현재 방문하고 있는 SGSN/SGW(1004)와, 가입자의 액세스 포인트를 서빙하는 GGSN/PGW(1006)에서 PDP 컨텍스트 데이터 구조를 할당한다. 캡처된 정보는 가입자의 IP 어드레스, 가입자들 국제 이동 가입자 아이덴티티(International Mobile Subscriber Identity)(IMSI), 및 GGSN/PGW(1006) 및/또는 SGSN/SGW(1004)에서의 터널 종점 ID들을 포함할 수도 있다.

[0064] 동작(1018)에서는, 그 다음으로, SGSN/SGW(1004)는 GGSN/PGW(1006)가 PDP 컨텍스트를 생성할 것을 요청한다. 동작(1020)에서, GGSN/PGW(1006)는 MS(1002)에 대한 VCRE 인스턴스(1012)를 배정할 것을 VCRE(1008)에 요청한다. 동작(1022)에서, VCRE(1008)는 RCF(1010)로부터 MS(1002)에 대응하는 프로파일을 요청하고, RCF(1010)는 동작(1024)에서 그것을 반환한다. 동작(1026)에서, VCRE(1008)는 프로파일을 VCRE 인스턴스(1012)에 배정한다. 동작(1028)에서, GGSN/PGW(1006)는 PDP 응답을 생성하고 그것을 SGSN/SGW(1004)로 전송하고, SGSN/SGW(1004)는 동작(1030)에서, MS(1002)로의 PDP 응답을 활성화한다.

[0065] 이 단계에서, GTP 트래픽은 MS(1002)로부터 SGSN/SGW(1004)를 통해 GGSN/PGW(1006)로 통과할 수 있다. 이것은 동작들(1032 및 1034)에서 표현된다. 동작(1036)에서, GGSN/PGW(1006)는 GTP 터널들을 역캡슐화(decapsulate)하고, IP 트래픽을 적절한 VCRE 인스턴스(1012)로 통과시킨다. VCRE 인스턴스(1012)는 양자의 발신(1038) 및 착신(1040) 트래픽에 대한 정책을 집행한다.

[0066] 실제적으로, GTP 프로토콜은 GTP-C로 알려진 제어 섹션 및 GTP-U로 알려진 IP-기반 터널링 프로토콜로 분리되고, 이 때문에, 이 단계에서는, IP 트래픽이 GTP-U 프로토콜에 따라 실제적으로 포맷될 수도 있다. 별도의 터널들은 동적으로 할당된 난수일 수도 있는, GTP-U 메시지들에서의 터널 종점 식별자(tunnel endpoint identifier)(TEID)에 의해 식별된다. 난수가 암호 품질일 경우, 그것은 어떤 유형들의 공격들에 대한 보안성의 수단을 제공한다.

[0067] 도 11은 예시적인 실시예에 따라, 이동 네트워크에서 착신 데이터 패킷을 핸들링하는 방법(1100)을 예시하는 흐름도이다. 이 도면은 "업스트림" 패킷, 즉, 이동 네트워크에서의 이동 디바이스로부터 패킷 기반 네트워크로 전송된 패킷의 핸들링을 표현한다. 예시적인 실시예에서, 이 방법(1100)은 PICNEEC 또는 등에 의해 수행될 수도 있다. 동작(1102)에서, 데이터 패킷은 이동 디바이스로부터 수신된다. 이 데이터 패킷은 예를 들어, 이동 디바이스 상에서 작동하는 애플리케이션에 의해 생성될 수도 있다. 동작(1104)에서, 정책 및 과금 실행 기능(Policy and Charging Execution Function)(PCEF)은 이 데이터 패킷에 대한 집행을 수행한다. 이 PCEF 집행은

서비스 품질(Quality of Service)(QoS) 및 온라인 및 오프라인 과금과 같은 정책 판단들의 집행을 포함한다. 동작(1106)에서, VCRE는 패킷이 방화벽 규칙 아래에 있는지를 판단한다. 이것은 예를 들어, 이동 디바이스에 대응하는 VCRE 인스턴스에서 정책을 검사함으로써 결정된다. 그러할 경우, 동작(1108)에서는, 프리-라우팅 방화벽 집행(pre-routing firewall enforcement)이 정책을 이용하여 수행된다. 예시적인 실시예에서, 프리-라우팅 방화벽 집행은 특정한 패킷들을 마킹하는 것을 포함한다. 예를 들어, 규칙적인 HTTP 트래픽이 하나의 VPN을 통해 전송되는 것과, 특정 웹사이트로의 HTTP 트래픽이 또 다른 VPN을 통해 전송되는 것이 바람직할 수도 있다. 프리-라우팅 방화벽 집행 규칙들은 규칙들에 따라 패킷들을 마킹하도록 작동할 수도 있다. 동작(1110)에서는, 라우팅이 수행된다. 이것은 예를 들어, 패킷들이 프리-라우팅 방화벽 집행 동안에 마킹되었던 방법에 따라 패킷들을 라우팅하는 것을 포함할 수도 있다. 동작(1112)에서는, 패킷이 NAT 후방에 안착되는지가 결정된다. 이것은 예를 들어, 이동 디바이스에 대응하는 VCRE 인스턴스에서 정책을 검사함으로써 결정된다. 그러할 경우, 동작(1114)에서, (가능한 NAT 규칙들을 갖는) 출발지 SAT는 정책을 이용하여 패킷 상에서 적용된다.

[0068] 동작(1116)에서는, 방화벽이 NAT 및 라우팅 판단 후에 적용되는지가 결정된다. 이것은 예를 들어, 이동 디바이스에 대응하는 VCRE 인스턴스에서 정책을 검사함으로써 결정된다. 그러할 경우, 동작(1118)에서는, 포스트-라우팅 방화벽 집행(post-routing firewall enforcement)이 정책을 이용하여 수행된다. 예시적인 실시예에서, 포스트-라우팅 방화벽 집행은 라우팅 프로세스가 완료된 후, 패킷 크기 및 패킷 헤더들과 같은 패킷 특성들을 변경하는 규칙들을 포함할 수도 있다. 동작(1120)에서는, IPSEC 암호화와 같은 보안성 정책이 이용되는지가 결정된다. 이것은 예를 들어, 이동 디바이스에 대응하는 VCRE 인스턴스에서 정책을 검사함으로써 결정된다. 그러할 경우, 동작(1122)에서는, 암호화 또는 일부 다른 보안성 기법이 수행된다. 동작(1124)에서, 최종적인 패킷은 외부 패킷 기반 네트워크의 외부로 전송된다.

[0069] 도 12는 또 다른 예시적인 실시예에 따라, 이동 네트워크에서 착신 데이터 패킷을 핸들링하는 방법(1200)을 예시하는 흐름도이다. 이 도면은 "다운스트림" 패킷, 즉, 패킷 기반 네트워크로부터 이동 네트워크에서의 이동 디바이스로 전송된 패킷의 핸들링을 표현한다. 예시적인 실시예에서, 이 방법(1200)은 PICNEEC 또는 등에 의해 수행될 수도 있다. 동작(1202)에서, 데이터 패킷은 패킷 기반 네트워크로부터 수신된다. 동작(1204)에서, 데이터 패킷의 목적지 어드레스는 어드레스에 기초하여 VCRE 인스턴스를 검색(retrieve)하기 위하여 이용된다. 예를 들어, 목적지 어드레스는 인터넷 프로토콜(Internet Protocol)(IP) 어드레스일 수도 있고, VCRE 인스턴스는 정책을 검색하기 위하여 서치될 수도 있는 필드로서, IP 어드레스, IP 어드레스들의 리스트, 또는 IP 어드레스 범위를 가질 수도 있다.

[0070] 동작(1206)에서는, 정책이 NAT가 IP 어드레스에 대하여 이용된다는 것을 표시하는지 여부가 결정된다. 그러할 경우, 동작(1208)에서, NAT 정책은 NAT된 IP 어드레스에 기초한 다운스트림 패킷에 대한 세션을 유지하기 위하여 IP 어드레스에 적용될 수도 있다.

[0071] 동작(1210)에서는, 방화벽 정책이 IP 어드레스에 대하여 정의되는지 여부가 결정된다. 그러할 경우, 동작(1212)에서는, 프리-라우팅 방화벽 규칙들이 실행될 수도 있다. 예시적인 실시예에서, 이것은 분산된 서비스 거부(distributed denial of service)(DDOS) 공격들을 차단하는 것을 보조하기 위한 규칙들을 포함할 수도 있다. 특정한 IP 어드레스들로부터의 트래픽은 프리-라우팅 방화벽 규칙들에 따라 마킹될 수도 있을 뿐만 아니라, 그것들이 임계치를 초과할 경우에 블랙리스트에 추가될 수도 있다.

[0072] 동작(1214)에서는, 데이터 패킷이 라우팅 정책에 따라 라우팅된다. 동작(1216)에서는, IPSEC 암호화와 같은 보안성 정책이 이용되는지가 결정된다. 이것은 예를 들어, IP 어드레스에 대응하는 VCRE 인스턴스에서 정책을 검사함으로써 결정된다. 그러할 경우, 동작(1218)에서는, 복호화 또는 일부 다른 보안성 기법이 수행된다.

[0073] 동작(1220)에서는, 방화벽 정책이 IP 어드레스에 대하여 정의되는지 여부가 결정된다. 그러할 경우, 동작(1222)에서는, 포스트-라우팅 방화벽 규칙들이 실행될 수도 있다. 동작(1224)에서, PCEF는 데이터 패킷에 대한 집행을 수행할 수도 있다. 동작(1226)에서, 최종적인 패킷은 IP 어드레스에 대응하는 사용자 디바이스로 전송된다.

[0074] 또 다른 예시적인 실시예에서, PICNEEC는 GGSN/PGW에 대해 외부적으로 위치된다. 도 13은 예시적인 실시예에 따라, SGSN/SGW(1302) 및 GGSN/PGW(1304)를 포함하는 시스템(1300)을 예시하는 블록도이다. 예시적인 실시예에서, SGSN/SGW(1302)는 도 1의 SGSN(110)일 수도 있고, GGSN/PGW(1304)는 도 1의 GGSN(114)일 수도 있다. SGSN/SGW(1302)는 이동 라디오 네트워크로부터 Gn 인터페이스를 통해 GGSN/PGW(1304)로 데이터를 전송한다. GGSN/PGW(1304)는 Gi 포트를 통해, Gi 기준점 상에 안착되는 외부 PICNEEC(1306)로 통신한다. PICNEEC(1306) 내부의 VCRE(1318)는 시스템(1300)에 대한 라우팅, 방화벽, VPN, 및 보안성 특징들을 정의한다. 정책 및 과금

규칙들 실행 기능(Policy and Charging Rules Execution Function)(PREF)(1308)은 일반적인 정책 및 과금 규칙들을 실행한다.

[0075] 규칙들 맞춤화기 기능(RCF)(1310)은 외부 저장소, 및 정책 및 보안성 변경들 및 구성들의 전부를 VCRE(1318)로 전달하는 제어 기능으로서 작동한다. RCF(1310)는 그것이 애플리케이션 기능(1312)인 것처럼, Rx 인터페이스를 이용하여 PCRF(1308)에 또한 접속할 수도 있다. RCF 콘솔(1314)은 방화벽 및 보안성 정책들을 설정하기 위하여 고객에 의해 이용된다. RCF 콘솔(1314)은 예를 들어, 웹 포털, 보안 쉘(SSH) 액세스, 인간-머신 언어(MML) 인터페이스 등일 수도 있다.

[0076] RCF 애플리케이션(1316)은 예를 들어, 외부 애플리케이션, 이동 디바이스 상의 애플리케이션 등으로부터의 RCF(1310)에 대한 애플리케이션 프로그램 인터페이스(API) 액세스를 제공한다.

[0077] 상기 설명은 PICNEEC(1306)가 3G/4G 네트워크들에 접속하기 위한 메커니즘들을 논의하지만, 일부 예시적인 실시예들에서, PICNEEC(1306)는 LoRa 및 SIGFOX와 같은 저 전력 광역 네트워크(Low Power Wide Area Network)(LPWAN)들에 또한 동시에 접속할 수 있다는 것이 주목되어야 한다.

[0078] 도 14는 예시적인 실시예에 따라, 외부 PICNEEC를 갖는 이동 네트워크에서 데이터 패킷들을 핸들링하는 방법(1400)을 예시하는 상호작용 도면이다. 방법(1400)은 이동 세트(MS)(1402), SGSN/SGW(1404), GGSN/PGW(1406), 외부 PICNEEC(1401)를 사용할 수도 있고, 외부 PICNEEC(1401)는 VCRE(1408), RCF(1410), 패킷 데이터 네트워크(PDN)(1414)에 접속하는 VCRE 인스턴스(1412)를 갖는다. MS(1402)는 본원에서 설명된 보안성 및/또는 방화벽 규칙들의 대상물인 이동 디바이스들의 그룹일 수도 있다.

[0079] 동작(1416)에서, MS(1402)는 네트워크에 등록하고 SGSN/SGW(1404)를 통해 자신을 인증하는 것을 시도한다. 이것은 패킷 데이터 프로토콜(PDP)을 생성하는 것으로 칭해진다. 동작(1418)에서는, 그 다음으로, SGSN/SGW(1404)는 GGSN/PGW(1406)가 PDP 컨텍스트를 생성할 것을 요청한다. 동작(1420)에서, GGSN/PGW(1406)는 PDP 컨텍스트에 대한 IP 어드레스를 할당할 것을 외부 PICNEEC(1408)에 요청한다. 이것은 DHCP 또는 RADIUS와 같은 프로토콜들을 이용하여 수행될 수도 있다. 동작(1422)에서, 외부 PICNEEC VCRE(1408)는 RCF(1410)로부터 MS(1402)에 대응하는 프로파일을 요청하고, RCF(1410)는 동작(1424)에서 그것을 반환한다. 동작(1426)에서, 외부 PICNEEC VCRE(1408)는 IP 어드레스를 PDP 컨텍스트에 배정하고 그것을 반환한다. 동작(1428)에서, GGSN/PGW(1406)는 PDP 응답을 생성하고 그것을 SGSN/SGW(1404)로 전송하고, SGSN/SGW(1404)는 동작(1430)에서, MS(1402)로의 PDP 응답을 활성화한다.

[0080] 이 단계에서, GTP 트래픽은 MS(1402)로부터 SGSN/SGW(1404)를 통해 GGSN/PGW(1406)로 통과할 수 있다. 이것은 동작들(1432 및 1434)에서 표현된다. 동작(1436)에서, GGSN/PGW(1406)는 GTP 터널들을 역캡슐화하고, IP 트래픽을 외부 PICNEEC VCRE(1408)를 향해 통과시키고, 외부 PICNEEC VCRE(1408)는 그 다음으로, 동작(1438)에서, 트래픽의 출발지 어드레스에 기초하여 IP 트래픽을 적절한 VCRE 인스턴스(1412)로 라우팅한다. VCRE 인스턴스(1412)는 양자의 발신(1440) 및 착신(1442) 트래픽에 대한 정책을 집행한다. 결과는 PDN으로부터의 IP 트래픽이 VCRE 인스턴스(1442)로부터, 출발지 어드레스에 기초하여 트래픽을 다시 GGSN/PGW(1406)로 라우팅하는 것을 아는 외부 PICNEEC VCRE(1408)로 라우팅된다는 것이다.

[0081] 어떤 사례들에서, 특정한 디바이스 그룹은 서로와는 상이한 포맷들을 아마도 이용하는 상이한 셀룰러 네트워크들에서 동작하는 디바이스들을 포함할 수도 있다. 예를 들어, 도 5를 다시 참조하면, 디바이스 그룹(504A)은 GSM 네트워크 상에서 동작하는 하나의 디바이스, 및 CDMA 네트워크 상에서 동작하는 또 다른 디바이스를 포함할 수도 있다. 이것은 예를 들어, 회사가 그 피고용인들이 작업 이용을 위한 그 개인용 셀룰러 디바이스들을 이용하는 것을 허용하고, 하나의 피고용인이 또 다른 것과는 (예컨대, 상이한 셀 서비스 제공자로부터의) 상이한 네트워크와 호환가능한 디바이스를 가질 수도 있는 사례에서 발생할 수 있다. 또 다른 예는 네트워크 기술들 사이의 IP 로밍(roaming)을 허용하는 프록시 이동 IP(Proxy Mobile IP)(PMIP) 기술의 사용일 것이다. 순수한 결과는 하나의 PICNEEC 상에서 위치된 VCRE 인스턴스가 상이한 PICNEEC에 접속하는 디바이스로부터 적어도 직접적이지 않게 도달가능하지 않을 수도 있다는 것이다. GSM 네트워크 상에서 동작하는 하나의 디바이스 및 Wi-Fi 네트워크 상에서 동작하는 또 다른 디바이스의 경우, GSM 네트워크 상에서 동작하는 디바이스는 그 트래픽이 PICNEEC를 통해 라우팅되게 할 수도 있는 반면, Wi-Fi 네트워크 상에서 동작하는 디바이스는 그 트래픽이 이동 액세스 게이트웨이(Mobile Access Gateway)(MAG)를 통해 라우팅되게 할 수도 있다. 이러한 경우들을 어떻게 핸들링할 것인지에 대한 몇몇 가능성들이 있다.

[0082] 제1 예시적인 실시예에서, 고객은 다수의 상이한 PICNEEC들 상의 디바이스 그룹에 대한 동일한 규칙들/정책들을

간단하게 생성한다. 이것은 고객이 다수의 PICNEEC들의 각각에 대한 별도의 RCF 콘솔 또는 RCF 애플리케이션을 사용함으로써 수행된다. 물론, 이것은 바람직한 솔루션이 아닐 수도 있는데, 왜냐하면 이 솔루션은 고객이 여분의 작업을 수행할 것을 강요하고, 또한, 규칙들/정책들의 생성을 반복할 시에, 고객이 실수를 행할 수도 있고, 우연히 하나의 PICNEEC 상의 디바이스 그룹에 대한 VCRE 인스턴스에서의 규칙들/정책들이 또 다른 PICNEEC 상의 디바이스 그룹에 대한 대응하는 VCRE 인스턴스와는 상이하게 할 수도 있고, 따라서, 상이한 규칙들/정책들이 동일한 규칙들/정책들을 가져야 하는 디바이스들에 적용되게 할 수도 있는 위험과 함께 나오기 때문이다.

[0083] 제2 예시적인 실시예에서는, VCRE 인스턴스가 하나의 PICNEEC 상에서 생성되거나 수정될 때, VCRE 인스턴스가 다른 대응하는 PICNEEC들 상에서 복제되도록, 복제가 PICNEEC들에서 수행된다. 도 15는 또 다른 예시적인 실시예에 따라, 다수의 SGSN/SGW들(1502A, 1502B, 1502C) 및 다수의 PICNEEC들(1504A, 1504B, 1504C)을 포함하는 시스템(1500)을 예시하는 블록도이다. 각각의 PICNEEC(1504A 내지 1504C)는 대응하는 PICNEEC(1504A 내지 1504C)에 배정된 VCRE 인스턴스들을 관리하는 로컬 VCRE 규칙들 기능(local VCRE rules function)(L-VCRE)(1506A 내지 1506C)을 유지할 수도 있다. 각각의 PICNEEC(1504A 내지 1504C) 상의 복제 서비스(1512A 내지 1512C)는 L-VCRE(1506A 내지 1506C)가 PICNEEC들(1504A 내지 1504C) 사이에서 복제되게 하고, 따라서, PICNEEC들(1504A 내지 1504C) 사이에서 일관성 있는 VCRE 인스턴스들을 유지한다. 따라서, 고객이 임의의 수의 상이한 RCF 콘솔들(1508A 내지 1508C) 및 RCF 애플리케이션들(1510A 내지 1510C) 중 하나를 이용하여 디바이스 그룹에 대한 규칙들 및 정책들을 생성할 수도 있거나 수정할 수도 있더라도, VCRE 인스턴스들은 고객이 상이한 RCF 콘솔들(1508A 내지 1508C) 또는 RCF 애플리케이션들(1510A 내지 1510C)의 각각 상에서 정확하게 동일한 방법으로 규칙들 및 정책들의 생성 또는 수정을 반복한 것처럼 일정하다.

[0084] 제3 예시적인 실시예에서는, 고객이 디바이스 그룹에 대한 규칙들/정책들을 확립하거나 수정하기 위한 단일의 인터페이스 점으로서 작동하는 중앙 규칙들 맞춤화기 기능(central Rules Customizer Function)(C-RCF)이 제공되고, C-RCF는 규칙들/정책들을 다수의 로컬 VCRE 규칙들 기능들로 분산시킨다. 도 16은 또 다른 예시적인 실시예에 따라, 다수의 SGSN/SGW들(1602A, 1602B, 1602C) 및 다수의 PICNEEC들(1604A, 1604B, 1604C)을 포함하는 시스템(1600)을 예시하는 블록도이다. 각각의 PICNEEC(1604A 내지 1604C)는 대응하는 PICNEEC(1604A 내지 1604C)에 배정된 VCRE 인스턴스들을 관리하는 로컬 VCRE 규칙들 기능(L-VCRE)(1606A 내지 1606C)을 유지할 수도 있다. 중앙 규칙들 맞춤화기 기능(C-RCF)(1608)은 RCF 콘솔(1610) 및 RCF 애플리케이션(1612)에 대한 단일의 인터페이스 점으로서 작동하고, RCF 콘솔(1610) 및 RCF 애플리케이션(1612)을 통해 확립된 임의의 규칙들/정책들을 로컬 VCRE 규칙들 기능들(1606A 내지 1606C)의 전부로 분산시키도록 작동하고, 따라서, 그것들 사이에서 일관성을 확립한다.

[0085] 또 다른 가능한 시나리오는 디바이스가 하나의 유형의 네트워크로부터 또 다른 것으로 스위칭하지만, 양자의 네트워크들은 단일 PICNEEC에 의해 서비스된다는 것이다. 이것은 다수의 PICNEEC들 사이에서의 VCRE 인스턴스들의 임의의 복제를 요구하지 않지만, 예시적인 실시예에서, PDP 컨텍스트는 네트워크가 변경될 때에 재확립된다. 따라서, 이러한 발생의 경우, PICNEEC는 PDP 컨텍스트가 재확립될 때에 올바른 VCRE 인스턴스를 재배정할 수도 있다.

[0086] 위의 개시내용은 GGSN 및/또는 PGW에 관련되는 양태들을 설명하지만, 동일한 기법들 및 컴포넌트들이 이동 라디오 네트워크 상에서 송신된 통신들을 수신하는 임의의 네트워킹 게이트웨이에 적용될 수도 있다는 것이 주목되어야 한다. GGSN은 3G 네트워크들에서 주로 이용된 실시예인 반면, PGW는 4G 네트워크들에서 주로 이용된 실시예이지만, CDMA, WIMAX, LoRa, 및 SIGFOX와 같은 다른 라디오 기술들 뿐만 아니라, 당면한 개시내용에 따라 네트워킹 게이트웨이를 사용할 수도 있는 아직 만들어지지 않은 라디오 기술들이 있다.

[0087] 도 17은 예시적인 실시예에 따라, PICNEEC(1702)를 포함하는 시스템(1700)을 예시하는 블록도이다. PICNEEC(1702)는 이동 디바이스들(1706A 내지 1706F)로부터 라디오 송신들을 수신하고 라디오 송신들을 이동 디바이스들(1706A 내지 1706F)로 전송하는 임의의 수의 상이한 유형들의 라디오 게이트웨이들(1704A 내지 1704C)과 호환가능하다. 도시되지 않았지만, PICNEEC는 가상적인 맞춤화된 규칙들 집행기(VCRE)를 포함할 수도 있거나, 가상적인 맞춤화된 규칙들 집행기(VCRE)와 통신할 수도 있다. VCRE는 시스템(1700)에 대한, 그리고 구체적으로 이동 디바이스들(1706A 내지 1706F)과 외부 네트워크(1708) 사이의 통신들에 대한 라우팅, 방화벽, VPN, 및 보안성 특징들을 정의한다.

[0088] 규칙들 맞춤화기 기능(RCF)(1710)은 외부 저장소, 및 정책 및 보안성 변경들 및 구성들의 전부를 VCRE로 전달하는 제어 기능이다. RCF 콘솔(1712)은 라우팅 및 보안성 정책들을 설정하기 위하여 고객에 의해 이용된다. RCF

콘솔(1712)은 예를 들어, 웹 포털, 보안 쉘(SSH) 액세스, 인간-머신 언어(MML) 인터페이스 등일 수도 있다.

[0089] RCF 애플리케이션(1714)은 예를 들어, 외부 애플리케이션, 이동 디바이스 상의 애플리케이션 등으로부터의 RCF에 대한 애플리케이션 프로그램 인터페이스(API) 액세스를 제공한다.

[0090] 모듈들, 컴포넌트들, 및 로직

[0091] 어떤 실시예들은 로직 또는 다수의 컴포넌트들, 모듈들, 또는 메커니즘들을 포함하는 것으로서 본원에서 설명된다. 모듈들은 소프트웨어 모듈들(예컨대, 머신-판독가능한 매체 상에서 구체화된 코드) 또는 하드웨어 모듈들의 어느 하나를 구성할 수도 있다. "하드웨어 모듈"은 어떤 동작들을 수행할 수 있는 유형의 유닛이고, 어떤 물리적 방식으로 구성될 수도 있거나 배열될 수도 있다. 다양한 예시적인 실시예들에서, 하나 이상의 컴퓨터 시스템들(예컨대, 단독형,컴퓨터 시스템, 클라이언트 컴퓨터 시스템, 또는 서버 컴퓨터 시스템) 또는 컴퓨터 시스템의 하나 이상의 하드웨어 모듈들(예컨대, 프로세서 또는 프로세서들의 그룹)은 본원에서 설명된 바와 같은 어떤 동작들을 수행하도록 동작하는 하드웨어 모듈로서 소프트웨어(예컨대, 애플리케이션 또는 애플리케이션 부분)에 의해 구성될 수도 있다.

[0092] 일부 실시예들에서, 하드웨어 모듈은 기계적으로, 전자적으로, 또는 그 임의의 적당한 조합으로 구현될 수도 있다. 예를 들어, 하드웨어 모듈은 어떤 동작들을 수행하도록 영구적으로 구성되는 전용 회로부 또는 로직을 포함할 수도 있다. 예를 들어, 하드웨어 모듈은 필드-프로그래밍가능한 게이트 어레이(field-programmable gate array)(FPGA) 또는 애플리케이션 특정 집적 회로(application specific integrated circuit)(ASIC)와 같은 특수-목적 프로세서일 수도 있다. 하드웨어 모듈은 어떤 동작들을 수행하기 위하여 소프트웨어에 의해 일시적으로 구성되는 프로그래밍가능한 로직 또는 회로부를 또한 포함할 수도 있다. 예를 들어, 하드웨어 모듈은 범용 프로세서 또는 다른 프로그래밍가능한 프로세서에 의해 실행된 소프트웨어를 포함할 수도 있다. 일단 이러한 소프트웨어에 의해 구성되면, 하드웨어 모듈들은 구성된 기능들을 수행하도록 고유하게 설계된 특정 머신들(또는 머신의 특정 컴포넌트들)이 되고, 더 이상 범용 프로세서들이 아니다. 전용이며 영구적으로 구성된 회로부에서, 또는 (예컨대, 소프트웨어에 의해 구성된) 일시적으로 구성된 회로부에서 하드웨어 모듈을 기계적으로 구현하기 위한 판단은 비용 및 시간 고려사항들에 의해 추진될 수도 있다는 것이 인식될 것이다.

[0093] 따라서, 어구 "하드웨어 모듈"은 어떤 방식으로 동작하거나 본원에서 설명된 어떤 동작들을 수행하도록 물리적으로 구축되거나, 영구적으로 구성(예컨대, 하드와이어링(hardwired))되거나, 또는 일시적으로 구성(예컨대, 프로그래밍)되는 엔티티인, 유형의 엔티티(tangible entity)를 망라하는 것으로 이해되어야 한다. 본원에서 이용된 바와 같이, "하드웨어-구현된 모듈"은 하드웨어 모듈을 지칭한다. 하드웨어 모듈들이 일시적으로 구성(예컨대, 프로그래밍)되는 실시예들을 고려하면, 하드웨어 모듈들의 각각은 시간에 있어서의 임의의 하나의 인스턴스에서 구성되거나 인스턴스화(instantiate)될 필요가 없다. 예를 들어, 하드웨어 모듈이 특수-목적 프로세서가 되도록 소프트웨어에 의해 구성된 범용 프로세서를 포함할 경우, 범용 프로세서는 상이한 시간들에서 (예컨대, 상이한 하드웨어 모듈들을 포함하는) 각각 상이한 특수-목적 프로세서들로서 구성될 수도 있다. 따라서, 소프트웨어는 예를 들어, 시간의 하나의 인스턴스에서 특정한 하드웨어 모듈을 구성하고, 시간의 상이한 인스턴스에서 상이한 하드웨어 모듈을 구성하도록 특정한 프로세서 또는 프로세서들을 구성한다.

[0094] 하드웨어 모듈들은 정보를 다른 하드웨어 모듈들에 제공할 수 있고, 다른 하드웨어 모듈들로부터 정보를 수신할 수 있다. 따라서, 설명된 하드웨어 모듈들은 통신가능하게 결합되는 것으로서 간주될 수도 있다. 다수의 하드웨어 모듈들이 동시에 존재할 경우, 통신들은 하드웨어 모듈들 중 2 개 이상 사이에서 또는 그 중에서 (예컨대, 적절한 회로들 및 버스들 상에서) 신호 송신을 통해 달성될 수도 있다. 다수의 하드웨어 모듈들이 상이한 시간들에서 구성되거나 인스턴스화되는 실시예들에서, 이러한 하드웨어 모듈들 사이의 통신들은 예를 들어, 다수의 하드웨어 모듈들이 액세스하는 메모리 구조들에서의 정보의 저장 및 검색을 통해 달성될 수도 있다. 예를 들어, 하나의 하드웨어 모듈은 동작을 수행할 수도 있고, 그것이 통신가능하게 결합되는 메모리 디바이스에서 그 동작의 출력을 저장할 수도 있다. 그 다음으로, 추가의 하드웨어 모듈은 저장된 출력을 검색하고 프로세싱하기 위하여 더 이후의 시간에 메모리 디바이스를 액세스할 수도 있다. 하드웨어 모듈들은 입력 또는 출력 디바이스들과의 통신들을 또한 개시할 수도 있고, 자원(예컨대, 정보의 집합)에 대해 동작할 수 있다.

[0095] 본원에서 설명된 예시적인 방법들의 다양한 동작들은 적어도 부분적으로, 관련된 동작들을 수행하도록 (예컨대, 소프트웨어에 의해) 일시적으로 구성되거나 영구적으로 구성되는 하나 이상의 프로세서들에 의해 수행될 수도 있다. 일시적으로 또는 영구적으로 구성되든지 간에, 이러한 프로세서들은 본원에서 설명된 하나 이상의 동작들 또는 기능들을 수행하도록 동작하는 프로세서-구현된 모듈들을 구성할 수도 있다. 본원에서 이용된 바와 같이, "프로세서-구현된 모듈"은 하나 이상의 프로세서들을 이용하여 구현된 하드웨어 모듈을 지칭한다.

[0096] 유사하게, 본원에서 설명된 방법들은 적어도 부분적으로 프로세서-구현될 수도 있고, 특정한 프로세서 또는 프로세서들은 하드웨어의 예일 수도 있다. 예를 들어, 방법의 동작들의 적어도 일부는 하나 이상의 프로세서들 또는 프로세서-구현된 모듈들에 의해 수행될 수도 있다. 또한, 하나 이상의 프로세서들은 "클라우드 컴퓨팅" 환경에서 또는 "서비스로서의 소프트웨어(software as a service)"(SaaS)로서 관련된 동작들의 수행을 지원하도록 또한 동작할 수도 있다. 예를 들어, 동작들의 적어도 일부는 (프로세서들을 포함하는 머신들의 예들로서의) 컴퓨터들의 그룹에 의해 수행될 수도 있고, 이 동작들은 네트워크(예컨대, 인터넷)을 통해, 그리고 하나 이상의 적절한 인터페이스들(예컨대, 애플리케이션 프로그램 인터페이스(API))을 통해 액세스가능하다.

[0097] 동작들 중 어떤 것의 수행은 단일 머신 내에서 상주할 뿐만 아니라, 다수의 머신들에 걸쳐 전개된 프로세서들 사이에서 분산될 수도 있다. 일부 예시적인 실시예들에서, 프로세서들 또는 프로세서-구현된 모듈들은 (가정 환경, 사무실 환경, 또는 서버 팜(server farm) 내에서) 단일 지리적 로케이션에서 위치될 수도 있다. 다른 예시적인 실시예들에서, 프로세서들 또는 프로세서-구현된 모듈들은 다수의 지리적 로케이션들에 걸쳐 분산될 수도 있다.

[0098] 머신 및 소프트웨어 아키텍처

[0099] 도 1 내지 도 16과 함께 설명된 모듈들, 방법들, 애플리케이션들 및 등은 머신 및 연관된 소프트웨어 아키텍처의 맥락에서 일부 실시예들에서 구현된다. 이하의 섹션들은 개시된 실시예들과의 이용을 위하여 적당한 대표적인 소프트웨어 아키텍처(들) 및 머신(예컨대, 하드웨어) 아키텍처(들)를 설명한다.

[0100] 소프트웨어 아키텍처들은 특정한 목적들을 위하여 설계된 디바이스들 및 머신들을 생성하기 위하여 하드웨어 아키텍처들과 함께 이용된다. 예를 들어, 특정한 소프트웨어 아키텍처와 결합된 특정한 하드웨어 아키텍처는 이동 전화, 태블릿 디바이스, 또는 등과 같은 이동 디바이스를 생성할 것이다. 약간 상이한 하드웨어 및 소프트웨어 아키텍처는 "사물 인터넷"에서의 이용을 위한 스마트 디바이스를 산출할 수도 있는 반면, 또 다른 조합은 클라우드 컴퓨팅 아키텍처 내에서의 이용을 위한 서버 컴퓨터를 생성한다. 본 기술 분야의 통상의 기술자들은 본원에서 포함된 개시내용과는 상이한 맥락들에서 발명 요지를 어떻게 구현할 것인지를 용이하게 이해할 수 있으므로, 이러한 소프트웨어 및 하드웨어 아키텍처들의 모든 조합들이 여기에서 제시되지는 않는다.

[0101] 소프트웨어 아키텍처

[0102] 도 18은 본원에서 설명된 다양한 하드웨어 아키텍처들과 함께 이용될 수도 있는 대표적인 소프트웨어 아키텍처(1802)를 예시하는 블록도(1800)이다. 도 18은 소프트웨어 아키텍처(1802)의 단지 비-제한적인 예이고, 많은 다른 아키텍처들이 본원에서 설명된 기능성을 용이하게 하기 위하여 구현될 수도 있다는 것이 인식될 것이다. 소프트웨어 아키텍처(1802)는 그 중에서도, 프로세서들(1910), 메모리/스토리지(1930), 및 I/O 컴포넌트들(1950)을 포함하는 도 19의 머신(1900)과 같은 하드웨어 상에서 실행되고 있을 수도 있다. 대표적인 하드웨어 계층(1804)이 예시되고, 예를 들어, 도 19의 머신(1900)을 표현할 수 있다. 대표적인 하드웨어 계층(1804)은 연관된 실행가능한 명령들(1808)을 가지는 하나 이상의 프로세싱 유닛들(1806)을 포함한다. 실행가능한 명령들(1808)은 도 1 내지 도 16의 방법들, 모듈들 및 등의 구현예를 포함하는 소프트웨어 아키텍처(1802)의 실행가능한 명령들을 표현한다. 하드웨어 계층(1804)은 실행가능한 명령들(1808)을 또한 가지는 메모리 및/또는 저장 모듈들(1810)을 또한 포함한다. 하드웨어 계층(1804)은 머신(1900)의 일부로서 예시된 다른 하드웨어와 같은, 하드웨어 계층(1804)의 임의의 다른 하드웨어를 표현하는 다른 하드웨어(1812)를 또한 포함할 수도 있다.

[0103] 도 18의 예시적인 아키텍처에서, 소프트웨어 아키텍처(1802)는 각각의 계층이 특정한 기능성을 제공하는 계층들의 스택으로서 개념화될 수도 있다. 예를 들어, 소프트웨어 아키텍처(1802)는 오퍼레이팅 시스템(1814), 라이브러리들(1816), 프레임워크들/미들웨어(1818), 애플리케이션들(1820), 및 제시 계층(1844)과 같은 계층들을 포함할 수도 있다. 동작적으로, 계층들 내에서의 애플리케이션들(1820) 및/또는 다른 컴포넌트들은 소프트웨어 스택을 통해 애플리케이션 프로그래밍 인터페이스(API) 호출들(1824)을 소환할 수도 있고, API 호출들(1824)에 응답하여 메시지들(1826)로서 예시된 응답, 반환된 값들 및 등을 수신할 수도 있다. 예시된 계층들은 본질적으로 대표적이고, 모든 소프트웨어 아키텍처들은 모든 계층들을 가지지는 않는다. 예를 들어, 일부 이동 또는 특수 목적 오퍼레이팅 시스템들은 프레임워크들/미들웨어(1818)를 제공하지 않을 수도 있지만, 다른 것들은 이러한 계층을 제공할 수도 있다. 다른 소프트웨어 아키텍처들은 추가적인 또는 상이한 계층들을 포함할 수도 있다.

[0104] 오퍼레이팅 시스템(1814)은 하드웨어 자원들을 관리할 수도 있고, 공통적인 서비스들을 제공할 수도 있다. 오퍼레이팅 시스템(1814)은 예를 들어, 커널(kernel)(1828), 서비스들(1830), 및 구동기들(1832)을 포함할 수도

있다. 커널(1828)은 하드웨어와 다른 소프트웨어 계층들 사이의 추상화 계층으로서 작동할 수도 있다. 예를 들어, 커널(1828)은 메모리 관리, 프로세서 관리(예컨대, 스케줄링), 컴포넌트 관리, 네트워킹, 보안성 설정들 및 등을 담당할 수도 있다. 서비스들(1830)은 다른 소프트웨어 계층들에 대한 다른 공통적인 서비스들을 제공할 수도 있다. 구동기들(1832)은 기초적인 하드웨어를 제어하거나 기초적인 하드웨어와 인터페이싱하는 것을 담당할 수도 있다. 예를 들어, 구동기들(1832)은 하드웨어 구성에 따라, 디스플레이 구동기들, 카메라 구동기들, Bluetooth® 구동기들, 플래시 메모리 구동기들, 직렬 통신 구동기들(예컨대, 유니버셜 직렬 버스(Universal Serial Bus)(USB) 구동기들), Wi-Fi® 구동기들, 오디오 구동기들, 전력 관리 구동기들 및 등을 포함할 수도 있다.

[0105] 라이브러리들(1816)은 애플리케이션들(1820) 및/또는 다른 컴포넌트들 및/또는 계층들에 의해 사용될 수도 있는 공통적인 기반구조를 제공할 수도 있다. 라이브러리들(1816)은 다른 소프트웨어 모듈들이 기초적인 오프레이팅 시스템(1814) 기능성(예컨대, 커널(1828), 서비스들(1830), 및/또는 구동기들(1832))과 직접적으로 인터페이싱하는 것보다 더 용이한 방식으로 태스크들을 수행하는 것을 허용하는 기능성을 전형적으로 제공한다. 라이브러리들(1816)은 메모리 할당 기능들, 스트링 조작 기능들, 수학적인 기능들 및 등과 같은 기능들을 제공할 수도 있는 시스템 라이브러리들(1834)(예컨대, C 표준 라이브러리)을 포함할 수도 있다. 게다가, 라이브러리들(1816)은 미디어 라이브러리들(예컨대, MPEG4, H.264, MP3, AAC, AMR, JPG, PNG와 같은 다양한 미디어 포맷의 제시 및 조작을 지원하기 위한 라이브러리들), 그래픽 라이브러리들(예컨대, 디스플레이 상의 그래픽 컨텐츠에서 2D 및 3D를 렌더링하기 위하여 이용될 수도 있는 OpenGL 프레임워크), 데이터베이스 라이브러리들(예컨대, 다양한 관계 데이터베이스 기능들을 제공할 수도 있는 SQLite), 웹 라이브러리들(예컨대, 웹 브라우징 기능성을 제공할 수도 있는 WebKit) 및 등과 같은 API 라이브러리들(1836)을 포함할 수도 있다. 라이브러리들(1816)은 많은 다른 API들을 애플리케이션들(1820) 및 다른 소프트웨어 컴포넌트들/모듈들에 제공하기 위한 광범위한 다른 라이브러리들(1838)을 또한 포함할 수도 있다.

[0106] 프레임워크들/미들웨어(1818)(또한 때때로, 미들웨어로서 지칭됨)는 애플리케이션들(1820) 및/또는 다른 소프트웨어 컴포넌트들/모듈들에 의해 사용될 수도 있는 더 하이-레벨의 공통적인 기반구조를 제공할 수도 있다. 예를 들어, 프레임워크들/미들웨어(1818)는 다양한 그래픽 사용자 인터페이스(graphic user interface)(GUI) 기능들, 하이-레벨 자원 관리, 하이-레벨 로케이션 서비스들 및 등을 제공할 수도 있다. 프레임워크들/미들웨어(1818)는 그 일부가 특정한 오퍼레이팅 시스템 또는 플랫폼에 특정적일 수도 있는 애플리케이션들(1820) 및/또는 다른 소프트웨어 컴포넌트들/모듈들에 의해 사용될 수도 있는 다른 API들의 넓은 스펙트럼을 제공할 수도 있다.

[0107] 애플리케이션들(1820)은 내장된 애플리케이션들(1840) 및/또는 제3자 애플리케이션들(1842)을 포함한다. 대표적인 내장된 애플리케이션들(1840)의 예들은 연락처들 애플리케이션, 브라우저 애플리케이션, 북 판독기 애플리케이션, 로케이션 애플리케이션, 미디어 애플리케이션, 메시징 애플리케이션, 및/또는 게임 애플리케이션을 포함할 수도 있지만, 이것으로 제한되지는 않는다. 제3자 애플리케이션들(1842)은 내장된 애플리케이션들(1840) 중 임의의 것 뿐만 아니라, 다른 애플리케이션들의 넓은 모음을 포함할 수도 있다. 특정 예에서, 제3자 애플리케이션(1842)(예컨대, 특정한 플랫폼의 벤더(vendor) 이외의 엔티티에 의해 Android™ 또는 iOS™ 소프트웨어 개발 키트(software development kit)(SDK)를 이용하여 개발된 애플리케이션)은 iOS™, Android™, Windows® 전화, 또는 다른 이동 오퍼레이팅 시스템들과 같은 이동 오퍼레이팅 시스템 상에서 작동되는 이동 소프트웨어일 수도 있다. 이 예에서, 제3자 애플리케이션(1842)은 본원에서 설명된 기능성을 용이하게 하기 위하여 오퍼레이팅 시스템(1814)과 같은 이동 오퍼레이팅 시스템에 의해 제공된 API 호출들(1824)을 소환할 수도 있다.

[0108] 애플리케이션들(1820)은 시스템의 사용자들과 상호작용하기 위한 사용자 인터페이스들을 생성하기 위하여, 내장된 오퍼레이팅 시스템 기능들(예컨대, 커널(1828), 서비스들(1830), 및/또는 구동기들(1832)), 라이브러리들(예컨대, 시스템 라이브러리들(1834), API 라이브러리들(1836), 및 다른 라이브러리들(1838)), 프레임워크들/미들웨어(1818)를 사용할 수도 있다. 대안적으로 또는 추가적으로, 일부 시스템들에서, 사용자와의 상호작용들은 제시 계층(1844)과 같은 제시 계층을 통해 발생할 수도 있다. 이 시스템들에서, 애플리케이션/모듈 "로직"은 사용자와 상호작용하는 애플리케이션/모듈의 양태들로부터 분리될 수 있다.

[0109] 일부 소프트웨어 아키텍처들은 가상 머신(virtual machine)들을 사용한다. 도 18의 예에서, 이것은 가상 머신(1848)에 의해 예시된다. 가상 머신은 애플리케이션들/모듈들이 (예를 들어, 도 19의 머신(1900)과 같은) 하드웨어 머신 상에서 실행되고 있는 것처럼 실행될 수 있는 소프트웨어 환경을 생성한다. 가상 머신(1848)은 호스트 오퍼레이팅 시스템(도 18에서의 오퍼레이팅 시스템(1814))에 의해 호스팅되고, 전형적으로, 항상 그러하지는 않지만, 가상 머신(1848)의 동작 뿐만 아니라, 호스트 오퍼레이팅 시스템(즉, 오퍼레이팅 시스템(1814))과의 인

터페이스를 관리하는 가상 머신 모니터(1846)를 가진다. 소프트웨어 아키텍처는 오퍼레이팅 시스템(1850), 라이브러리들(1852), 프레임워크들/미들웨어(1854), 애플리케이션들(1856), 및/또는 제시 계층(1858)과 같은 가상 머신(1848) 내에서 실행된다. 가상 머신(1848) 내에서 실행되는 소프트웨어 아키텍처의 이 계층들은 이전에 설명된 대응하는 계층들과 동일할 수 있거나, 상이할 수도 있다.

[0110] 예시적인 머신 아키텍처 및 머신-판독가능한 매체

[0111] 도 19는 일부 예시적인 실시예들에 따라, 머신-판독가능한 매체(예컨대, 머신-판독가능한 저장 매체)로부터 명령들(1916)을 판독할 수 있고 본원에서 논의된 방법론들 중 임의의 하나 이상을 수행할 수 있는 머신(1900)의 컴포넌트들을 예시하는 블록도이다. 구체적으로, 도 19는 컴퓨터 시스템의 예시적인 형태에서의 머신(1900)의 도해적 표현을 도시하고, 컴퓨터 시스템 내에서, 명령들(1916)(예컨대, 소프트웨어, 프로그램, 애플리케이션, 애플릿(applet), 앱(app), 또는 다른 실행가능한 코드)은 머신(1900)으로 하여금, 위에서 설명된 종점들(예컨대, 이동 디바이스들, 외부 네트워크들에서의 디바이스)에 대하여 위에서 설명된 방법론들을 수행하게 한다. 명령들(1916)은 일반적인 비-프로그래밍된 머신(1900)을 설명되고 예시된 기능들을 설명된 방식으로 수행하도록 프로그래밍된 특정한 머신으로 변환한다. 대안적인 실시예들에서, 머신(1900)은 단독형 디바이스로서 동작하거나, 다른 머신들에 결합(예컨대, 네트워크화)될 수도 있다. 네트워크화된 전개에서, 머신(1900)은 서버-클라이언트 네트워크 환경에서의 서버 머신 또는 클라이언트 머신의 자격으로, 또는 피어-투-피어(peer-to-peer)(또는 분산된) 네트워크 환경에서의 피어 머신으로서 동작할 수도 있다. 머신(1900)은 서버 컴퓨터, 클라이언트 컴퓨터, 개인용 컴퓨터(personal computer)(PC), 태블릿 컴퓨터, 랩톱 컴퓨터, 넷북, 셋톱 박스(set-top box)(STB), 개인 정보 단말(personal digital assistant)(PDA), 엔터테인먼트 미디어 시스템, 셀룰러 전화, 스마트폰, 이동 디바이스, 웨어러블 디바이스(예컨대, 스마트 시계), 스마트 홈 디바이스(예컨대, 스마트 기기), 다른 스마트 디바이스들, 웹 기기, 네트워크 라우터, 네트워크 스위치, 네트워크 브릿지, 또는 머신(1900)에 의해 취해져야 할 액션들을 특정하는 명령들(1916)을 순차적으로 또는 이와 다르게 실행할 수 있는 임의의 머신을 포함할 수도 있지만, 이것으로 제한되지는 않는다. 또한, 오직 단일 머신(1900)이 예시되어 있지만, 용어 "머신"은 본원에서 논의된 방법론들 중 임의의 하나 이상을 수행하기 위한 명령들(1916)을 개별적으로 또는 공동으로 실행하는 머신들(1900)의 집합을 포함하도록 또한 택해질 것이다.

[0112] 머신(1900)은 버스(1902)를 통한 것과 같이, 서로 통신하도록 구성될 수도 있는 프로세서들(1910), 메모리/스토리지(1930), 및 I/O 컴포넌트들(1950)을 포함할 수도 있다. 예시적인 실시예에서, 프로세서들(1910)(예컨대, 중앙 프로세싱 유닛(central processing unit)(CPU), 축소 명령 세트 컴퓨팅(reduced instruction set computing)(RISC) 프로세서, 복합 명령 세트 컴퓨팅(complex instruction set computing)(CISC) 프로세서, 그래픽 프로세싱 유닛(graphics processing unit)(GPU), 디지털 신호 프로세서(digital signal processor)(DSP), 애플리케이션 특정 집적 회로(application specific integrated circuit)(ASIC), 라디오-주파수 집적 회로(radio-frequency integrated circuit)(RFIC), 또 다른 프로세서, 또는 그 임의의 적당한 조합)은 예를 들어, 명령들(1916)을 실행할 수도 있는 프로세서(1912) 및 프로세서(1914)를 포함할 수도 있다. 용어 "프로세서"는 명령들(1916)을 동시에 실행할 수도 있는 2 개 이상의 독립적인 프로세서들(1912, 1914)(때때로, "코어들"로서 지칭됨)을 포함할 수도 있는 멀티-코어 프로세서(1912, 1914)를 포함하도록 의도된다. 도 19는 다수의 프로세서들(1910)을 도시하지만, 머신(1900)은 단일 코어를 갖는 단일 프로세서(1912, 1914), 다수의 코어들을 갖는 단일 프로세서(1912, 1914)(예컨대, 멀티-코어 프로세서(1912, 1914)), 단일 코어를 갖는 다수의 프로세서들(1912, 1914), 다수의 코어들을 갖는 다수의 프로세서들(1912, 1914), 또는 그 임의의 조합을 포함할 수도 있다.

[0113] 메모리/스토리지(1930)는 주 메모리 또는 다른 메모리 스토리지와 같은 메모리(1932), 및 저장 유닛(1936)을 포함할 수도 있고, 양자는 버스(1902)를 통한 것과 같이 프로세서들(1910)에 의해 액세스가능하다. 저장 유닛(1936) 및 메모리(1932)는 본원에서 설명된 방법론들 또는 기능들 중 임의의 하나 이상을 구체화하는 명령들(1916)을 저장한다. 명령들(1916)은 머신(1900)에 의한 그 실행 동안에, 메모리(1932) 내에서, 저장 유닛(1936) 내에서, 프로세서들(1910) 중 적어도 하나 내에서(예컨대, 프로세서(1912, 1914)의 캐시 메모리 내에서), 또는 그 임의의 적당한 조합으로 완전히 또는 부분적으로 또한 상주할 수도 있다. 따라서, 메모리(1932), 저장 유닛(1936), 및 프로세서들(1910)의 메모리는 머신-판독가능한 매체들의 예들이다.

[0114] 본원에서 이용된 바와 같이, "머신-판독가능한 매체"는 명령들(1916) 및 데이터를 일시적으로 또는 영구적으로 저장할 수 있는 디바이스를 의미하고, 랜덤-액세스 메모리(random-access memory)(RAM), 판독-전용 메모리(read-only memory)(ROM), 버퍼 메모리, 플래시 메모리, 광학 매체들, 자기 매체들, 캐시 메모리, 다른 유형들의 스토리지(예컨대, 소거가능 프로그래밍가능한 판독-전용 메모리(erasable programmable read-only

memory)(EEPROM)), 및/또는 그 임의의 적당한 조합을 포함할 수도 있지만, 이것으로 제한되지는 않는다. 용어 "머신-판독가능한 매체"는 명령들(1916)을 저장할 수 있는 단일 매체 또는 다수의 매체들(예컨대, 중앙집중화된 또는 분산된 데이터베이스들, 또는 연관된 캐시들 및 서버들)을 포함하도록 택해져야 한다. 용어 "머신-판독가능한 매체"는 머신(예컨대, 머신(1900))에 의한 실행을 위하여 명령들(예컨대, 명령들(1916))을 저장할 수 있거나 반송할 수 있는 임의의 매체, 또는 다수의 매체들의 조합을 포함하도록 또한 택해질 것이어서, 명령들(1916)은, 머신(1900)의 하나 이상의 프로세서들(예컨대, 프로세서들(1910))에 의해 실행될 때, 머신(1900)으로 하여금, 본원에서 설명된 방법론들 중 임의의 하나 이상을 수행하게 한다. 따라서, "머신-판독가능한 매체"는 단일 저장 장치 또는 디바이스 뿐만 아니라, 다수의 저장 장치 또는 디바이스들을 포함하는 "클라우드-기반" 저장 시스템들 또는 저장 네트워크들을 지칭한다.

[0115] I/O 컴포넌트들(1950)은 입력을 수신하고, 출력을 제공하고, 출력을 생성하고, 정보를 송신하고, 정보를 교환하고, 측정들을 캡처하는 등을 위한 광범위한 컴포넌트들을 포함할 수도 있다. 특정한 머신에서 포함되는 특정 I/O 컴포넌트들(1950)은 머신(1900)의 유형에 종속될 것이다. 예를 들어, 이동 전화들과 같은 휴대용 머신들은 터치 입력 디바이스 또는 다른 이러한 입력 메커니즘들을 포함할 가능성이 있을 것이지만, 헤드리스 서버 머신(headless server machine)은 이러한 터치 입력 디바이스를 포함하지 않을 가능성이 있다. I/O 컴포넌트들(1950)은 도 19에서 도시되지 않은 많은 다른 컴포넌트들을 포함할 수도 있다는 것이 인식될 것이다. I/O 컴포넌트들(1950)은 다음의 논의를 단지 단순화하기 위한 기능성에 따라 그룹화되고, 그룹은 결코 제한하는 것이 아니다. 다양한 예시적인 실시예들에서, I/O 컴포넌트들(1950)은 출력 컴포넌트들(1952) 및 입력 컴포넌트들(1954)을 포함할 수도 있다. 출력 컴포넌트들(1952)은 시각 컴포넌트들(예컨대, 플라즈마 디스플레이 패널(plasma display panel)(PDP), 발광 다이오드(light emitting diode)(LED) 디스플레이, 액정 디스플레이(liquid crystal display)(LCD), 프로젝터, 또는 음극선관(cathode ray tube)(CRT)과 같은 디스플레이), 음향 컴포넌트들(예컨대, 스피커들), 촉각 컴포넌트들(예컨대, 진동 모터, 저항 메커니즘들), 다른 신호 생성기들 및 등을 포함할 수도 있다. 입력 컴포넌트들(1954)은 영숫자 입력 컴포넌트들(예컨대, 키보드, 영숫자 입력을 수신하도록 구성된 터치 스크린, 포토-광 키보드(photo-optical keyboard), 또는 다른 영숫자 입력 컴포넌트들), 점 기반 입력 컴포넌트들(예컨대, 마우스, 터치패드, 트랙볼, 조이스틱, 모션 센서, 또는 다른 포인팅 도구), 촉각 입력 컴포넌트들(예컨대, 물리적 버튼, 터치들 또는 터치 제스처들의 로케이션 및/또는 힘을 제공하는 터치 스크린, 또는 다른 촉각 입력 컴포넌트들), 오디오 입력 컴포넌트들(예컨대, 마이크로폰) 및 등을 포함할 수도 있다.

[0116] 추가의 예시적인 실시예들에서, I/O 컴포넌트들(1950)은 다양한 다른 컴포넌트들 중에서, 생체계측 컴포넌트들(1956), 모션 컴포넌트들(1958), 환경적 컴포넌트들(1960), 또는 위치 컴포넌트들(1962)을 포함할 수도 있다. 예를 들어, 생체계측 컴포넌트들(1956)은 표현들(예컨대, 손 표현들, 얼굴 표정들, 발성 표현들, 신체 제스처들, 또는 시선 추적)을 검출하고, 생체신호들(예컨대, 혈압, 심박수, 신체 온도, 땀, 또는 뇌파들)을 측정하고, 사람을 식별(예컨대, 음성 식별, 망막 식별, 얼굴 식별, 지문 식별, 또는 뇌전도(electroencephalogram) 기반 식별)하는 등을 위한 컴포넌트들을 포함할 수도 있다. 모션 컴포넌트들(1958)은 가속도 센서 컴포넌트들(예컨대, 가속도계), 중력 센서 컴포넌트들, 회전 센서 컴포넌트들(예컨대, 자이로스코프(gyroscope)) 및 등을 포함할 수도 있다. 환경적 컴포넌트들(1960)은 예를 들어, 조명 센서 컴포넌트들(예컨대, 광도계(photometer)), 온도 센서 컴포넌트들(예컨대, 주위 온도를 검출하는 하나 이상의 온도계), 습도 센서 컴포넌트들, 압력 센서 컴포넌트들(예컨대, 기압계), 음향 센서 컴포넌트들(예컨대, 배경 잡음을 검출하는 하나 이상의 마이크로폰들), 근접성 센서 컴포넌트들(예컨대, 근처의 객체들을 검출하는 적외선 센서들), 기체 센서들(예컨대, 안전을 위하여 유해 기체들의 농도들을 검출하거나 대기에서의 오염원들을 측정하기 위한 기체 검출 센서들), 또는 주변의 물리적 환경에 대응하는 표시들, 측정들, 또는 신호들을 제공할 수도 있는 다른 컴포넌트들을 포함할 수도 있다. 위치 컴포넌트들(1962)은 로케이션 센서 컴포넌트들(예컨대, 글로벌 위치 시스템(Global Position System)(GPS) 수신기 컴포넌트), 고도 센서 컴포넌트들(예컨대, 고도가 유도될 수도 있는 공기 압력을 검출하는 고도계들 또는 기압계들), 방위 센서 컴포넌트들(예컨대, 자력계들) 및 등을 포함할 수도 있다.

[0117] 통신은 광범위한 기술들을 이용하여 구현될 수도 있다. I/O 컴포넌트들(1950)은 각각 결합(1982) 및 결합(1972)을 통해 머신(1900)을 네트워크(1980) 또는 디바이스들(1970)에 결합하도록 동작가능한 통신 컴포넌트들(1964)을 포함할 수도 있다. 예를 들어, 통신 컴포넌트들(1964)은 네트워크(1980)와 인터페이싱하기 위한 네트워크 인터페이스 컴포넌트 또는 다른 적당한 디바이스를 포함할 수도 있다. 추가의 예들에서, 통신 컴포넌트들(1964)은 유선 통신 컴포넌트들, 무선 통신 컴포넌트들, 셀룰러 통신 컴포넌트들, 근접장 통신(near field communication)(NFC) 컴포넌트들, Bluetooth® 컴포넌트들(예컨대, Bluetooth® 로우 에너지(Low Energy)),

Wi-Fi® 컴포넌트들, 및 다른 양상(modality)들을 통해 통신을 제공하기 위한 다른 통신 컴포넌트들을 포함할 수도 있다. 디바이스들(1970)은 또 다른 머신, 또는 광범위한 주변 디바이스들(예컨대, 유니버셜 직렬 버스(USB)를 통해 결합된 주변 디바이스) 중 임의의 것일 수도 있다.

[0118] 또한, 통신 컴포넌트들(1964)은 식별자들을 검출할 수도 있거나, 식별자들을 검출하도록 동작가능한 컴포넌트들을 포함할 수도 있다. 예를 들어, 통신 컴포넌트들(1964)은 라디오 주파수 식별(radio frequency identification)(RFID) 태그 판독기 컴포넌트들, NFC 스마트 태그 검출 컴포넌트들, 광학 판독기 컴포넌트들(예컨대, 유니버셜 제품 코드(Universal Product Code)(UPC) 바 코드와 같은 1 차원 바 코드들, 신속 응답(Quick Response)(QR) 코드, 아즈텍 코드(Aztec code), 데이터 매트릭스(Data Matrix), Dataglyph, MaxiCode, PDF417, 울트라 코드(Ultra Code), UCC RSS-2D 바 코드와 같은 다차원 바 코드들, 및 다른 광학 코드들을 검출하기 위한 광학 센서), 또는 음향 검출 컴포넌트들(예컨대, 태그된 오디오 신호들을 식별하기 위한 마이크로폰들)을 포함할 수도 있다. 게다가, 인터넷 프로토콜(IP) 지오-로케이션(geo-location)을 통한 로케이션, Wi-Fi® 신호 삼각측량을 통한 로케이션, 특정한 로케이션을 표시할 수도 있는 NFC 비콘 신호(beacon signal)를 검출하는 것을 통한 로케이션 및 등과 같은 다양한 정보는 통신 컴포넌트들(1964)을 통해 유도될 수도 있다.

[0119] 송신 매체

[0120] 다양한 예시적인 실시예들에서, 네트워크(1980)의 하나 이상의 부분들은 애드 혹(ad hoc) 네트워크, 인트라넷(intranet), 익스트라넷(extranet), 가상 사설 네트워크(virtual private network)(VPN), 로컬 영역 네트워크(local area network)(LAN), 무선 LAN(wireless LAN)(WLAN), 광역 네트워크(WAN), 무선 WAN (WWAN), 도시 지역 네트워크(MAN), 인터넷, 인터넷의 부분, 공공 교환 전화 네트워크(public switched telephone network)(PSTN)의 부분, 기존 전화 서비스(plain old telephone service)(POTS) 네트워크, 셀룰러 전화 네트워크, 무선 네트워크, Wi-Fi® 네트워크, 또 다른 유형의 네트워크, 또는 2 개 이상의 이러한 네트워크들의 조합일 수도 있다. 예를 들어, 네트워크(1980) 또는 네트워크(1980)의 부분은 무선 또는 셀룰러 네트워크를 포함할 수도 있고, 결합(1982)은 코드 분할 다중 액세스(CDMA) 접속, 이동 통신들을 위한 글로벌 시스템(GSM) 접속, 또는 다른 유형의 셀룰러 또는 무선 결합일 수도 있다. 이 예에서, 결합(1982)은 단일 캐리어 라디오 송신 기술(Single Carrier Radio Transmission Technology)(1xRTT), 진화-데이터 최적화(Evolution-Data Optimized)(EVDO) 기술, 일반 패킷 라디오 서비스(GPRS) 기술, GSM 진화를 위한 개량된 데이터 레이트들(Enhanced Data rates for GSM Evolution)(EDGE) 기술, 3G를 포함하는 3세대 파트너십 프로젝트(3GPP), 4세대 무선(4G) 네트워크들, 유니버셜 이동 전기통신 시스템(UMTS), 고속 패킷 액세스(High Speed Packet Access)(HSPA), 마이크로파 액세스를 위한 전세계 상호운용성(Worldwide Interoperability for Microwave Access)(WiMAX), 롱텀 에볼루션(LTE) 표준, 다양한 표준 설정 조직들에 의해 정의된 다른 것들, 또는 다른 데이터 전송 기술과 같은 다양한 유형들의 데이터 전송 기술 중 임의의 것을 구현할 수도 있다.

[0121] 명령들(1916)은 네트워크 인터페이스 디바이스(예컨대, 통신 컴포넌트들(1964) 내에 포함된 네트워크 인터페이스 컴포넌트)를 통해 송신 매체를 이용하여, 그리고 다수의 널리-공지된 전송 프로토콜들(예컨대, 하이퍼텍스트 전송 프로토콜(HTTP)) 중 임의의 하나를 사용하여 네트워크(1980) 상에서 송신될 수도 있거나 수신될 수도 있다. 유사하게, 명령들(1916)은 디바이스들(1970)로의 결합(1972)(예컨대, 피어-투-피어 결합)을 통해 송신 매체를 이용하여 송신될 수도 있거나 수신될 수도 있다. 용어 "송신 매체"는 머신(1900)에 의한 실행을 위한 명령들(1916)을 저장할 수 있거나, 인코딩할 수 있거나, 반송할 수 있는 임의의 비유형(intangible) 매체를 포함하도록 택해질 것이고, 이러한 소프트웨어의 통신을 가능하게 하기 위한 디지털 또는 아날로그 통신 신호들 또는 다른 비유형 매체를 포함한다. 송신 매체는 머신 판독가능한 매체의 일 실시예이다.

[0122] 다음의 번호부여된 예들은 실시예를 포함한다.

[0123] 1. 이동 네트워크 제공자에 의한 동작을 위한 PDN 통합된 맞춤화된 네트워크 에지 인에이블러 및 제어기(PDN Integrated Customized Network Edge Enabler and Controller)(PICNEEC)로서,

[0124] 적어도 하나의 가상적인 맞춤화된 규칙들 집행기(Virtual Customized Rules Enforcer)(VCRE) 인스턴스 - 각각의 VCRE 인스턴스는 이동 디바이스들의 그룹에 대응하고 이동 디바이스들의 그룹에 대해 개인화된 정책들의 세트를 정의하고, 각각의 VCRE는 라디오 네트워크를 통해 패킷-기반 네트워크와, 대응하는 그룹에서의 이동 디바이스 사이에서 통신된 데이터 패킷을 수신할 시에, 데이터 패킷을 포워딩하기 이전에 데이터 패킷에 대한 VCRE 인스턴스에서 저장된 하나 이상의 정책 규칙들을 실행하도록 구성되고, 각각의 VCRE 인스턴스는 이동 네트워크 제공자의 상이한 고객에 의한 VCRE 인스턴스의 직접적인 액세싱을 통해 서로 독립적으로 제어됨 - 를 포함하는 PICNEEC.

[0125] 2. 예 1의 PICNEEC에 있어서, 데이터 패킷은 서빙 일반 패킷 라디오 서비스(GPRS) 지원 노드/서빙(SGSN)과, PICNEEC에 대해 내부적인 게이트웨이 GPRS 지원 노드(GGSN) 사이에서 라우팅되는 PICNEEC.

[0126] 3. 예 1 또는 예 2의 PICNEEC에 있어서, 데이터 패킷은 서빙 게이트웨이(SGW)와, PICNEEC에 대해 내부적인 패킷 데이터 네트워크 게이트웨이(PGW) 사이에서 라우팅되는 PICNEEC.

[0127] 4. 예들 1 내지 3 중 어느 한 예의 PICNEEC에 있어서, 데이터 패킷은 서빙 일반 패킷 라디오 서비스(GPRS) 지원 노드/서빙(SGSN)과, PICNEEC에 대해 외부적인 게이트웨이 GPRS 지원 노드(GGSN) 사이에서 라우팅되고, 외부적인 GGSN은 PICNEEC를 통해 인터넷 프로토콜(IP) 접속성 액세스 네트워크에 대한 데이터를 핸들링하는 PICNEEC.

[0128] 5. 예들 1 내지 4 중 어느 한 예의 PICNEEC에 있어서, 데이터 패킷은 서빙 게이트웨이(SGW)와, PICNEEC에 대해 외부적인 PGW 사이에서 라우팅되고, 외부적인 PGW는 PICNEEC를 통해 IP 접속성 액세스 네트워크에 대한 데이터를 핸들링하는 PICNEEC.

[0129] 6. 예들 1 내지 5 중 어느 한 예의 PICNEEC에 있어서, 데이터 패킷은 PICNEEC를 통해 데이터 패킷을 핸들링하는 이동 네트워크 서빙 패킷 게이트웨이를 통해 라우팅되는 PICNEEC.

[0130] 7. 예들 1 내지 6 중 어느 한 예의 PICNEEC에 있어서, 적어도 하나의 VCRE 인스턴스는 맞춤화된 액세스 포인트 명칭(APN)들을 정의하는 PICNEEC.

[0131] 8. 예들 1 내지 7 중 어느 한 예의 PICNEEC에 있어서, 적어도 하나의 VCRE 인스턴스는 독립적인 가상 네트워크 기능인 PICNEEC.

[0132] 9. 예들 1 내지 8 중 어느 한 예의 PICNEEC에 있어서, 적어도 하나의 VCRE 인스턴스는 독립적인 물리적 네트워크 기능인 PICNEEC.

[0133] 10. 예들 1 내지 9 중 어느 한 예의 PICNEEC에 있어서, 적어도 하나의 VCRE 인스턴스는 더 큰 네트워크 기능에서의 규칙들의 서브세트이고, 고객은 규칙들의 특정 서브세트를 오직 액세스할 수 있는 PICNEEC.

[0134] 11. 예들 1 내지 10 중 어느 한 예의 PICNEEC에 있어서, 적어도 하나의 VCRE 인스턴스는 VCRE 규칙들 기능(RCF) 콘솔을 이용하여 고객에 의해 생성되는 PICNEEC.

[0135] 12. 예 10의 PICNEEC에 있어서, RCF 콘솔은 보안 쉘(SSH) 액세스인 PICNEEC.

[0136] 13. 예들 1 내지 12 중 어느 한 예의 PICNEEC에 있어서, 적어도 하나의 VCRE 인스턴스는 VCRE 규칙들 기능(RCF) 애플리케이션을 이용하여 고객에 의해 생성되는 PICNEEC.

[0137] 14. 예 13의 PICNEEC에 있어서, RCF 애플리케이션은 애플리케이션 프로그램 인터페이스(API)인 PICNEEC.

[0138] 15. 예 13의 PICNEEC에 있어서, RCF 애플리케이션은 웹사이트인 PICNEEC.

[0139] 16. 예 13의 PICNEEC에 있어서, RCF 애플리케이션은 전용 컴퓨터 프로그램인 PICNEEC.

[0140] 17. 예 11의 PICNEEC에 있어서, RCF 콘솔은 적어도 하나의 VCRE 인스턴스를 직접적으로 관리하는 PICNEEC.

[0141] 18. 예들 13 내지 16 중 어느 한 예의 PICNEEC에 있어서, RCF 애플리케이션은 적어도 VCRE 인스턴스를 직접적으로 관리하는 PICNEEC.

[0142] 19. 예 11의 PICNEEC에 있어서, RCF 콘솔은 VCRE 인스턴스들 중 적어도 하나를 관리하는 중앙 RCF에 접속하는 PICNEEC.

[0143] 20. 예들 13 내지 16 중 어느 한 예의 PICNEEC에 있어서, RCF 애플리케이션은 VCRE 인스턴스들 중 적어도 하나를 관리하는 중앙 RCF에 접속하는 PICNEEC.

[0144] 21. 예들 1 내지 20 중 어느 한 예의 PICNEEC에 있어서, 고객은 대응하는 VCRE 인스턴스와 외부 네트워크 사이의 가상 사설 네트워크(VPN)를 정의함으로써 대응하는 VCRE 인스턴스를 정의하는 PICNEEC.

[0145] 22. 예들 1 내지 21 중 어느 한 예의 PICNEEC에 있어서, 고객은 대응하는 VCRE 인스턴스와 IP 접속성 네트워크들 사이의 네트워크 라우팅을 정의함으로써 대응하는 VCRE 인스턴스를 정의하는 PICNEEC.

[0146] 23. 예들 1 내지 22 중 어느 한 예의 PICNEEC에 있어서, 고객은 대응하는 VCRE 인스턴스를 통과하는 패킷 데이터 트래픽에 대한 방화벽 규칙들을 정의함으로써 대응하는 VCRE 인스턴스를 정의하는 PICNEEC.

[0147] 24. 예들 1 내지 23 중 어느 한 예의 PICNEEC에 있어서, 고객은 대응하는 VCRE 인스턴스를 통과하는 패킷 데이터 트래픽에 대한 네트워크 어드레스 변환(NAT) 규칙들을 정의함으로써 대응하는 VCRE 인스턴스를 정의하는 PICNEEC.

[0148] 25. 예들 1 내지 24 중 어느 한 예의 PICNEEC에 있어서, 고객은 대응하는 VCRE 인스턴스를 통과하는 패킷 데이터 트래픽에 대한 도메인 명칭 시스템(DNS) 설정들을 정의함으로써 대응하는 VCRE 인스턴스를 정의하는 PICNEEC.

[0149] 26. 예들 1 내지 25 중 어느 한 예의 PICNEEC에 있어서, 고객은 대응하는 VCRE 인스턴스를 통과하는 패킷 데이터 트래픽에 대한 보안성 규칙들을 정의함으로써 대응하는 VCRE 인스턴스를 정의하는 PICNEEC.

[0150] 27. 예들 1 내지 26 중 어느 한 예의 PICNEEC에 있어서, 고객은 IP 어드레스들을 이동 디바이스들에 배정함으로써 대응하는 VCRE 인스턴스를 정의하는 PICNEEC.

[0151] 28. 예들 1 내지 27 중 어느 한 예의 PICNEEC에 있어서, 고객은 대응하는 VCRE 인스턴스를 통과하는 트래픽에 대한 하이퍼텍스트 전송 프로토콜 헤더 강화(HHE) 규칙들을 정의함으로써 대응하는 VCRE 인스턴스를 정의하는 PICNEEC.

[0152] 29. 방법으로서,

[0153] PICNEEC에서, 라디오 네트워크를 통해 이동 디바이스와 패킷-기반 네트워크 사이에서 전송된 데이터 패킷을 수신하는 단계;

[0154] 데이터 패킷에서의 정보에 기초하여, 이동 디바이스에 배정된 VCRE 인스턴스 - VCRE 인스턴스는 PICNEEC를 동작시키는 이동 네트워크 제공자의 고객에 의한 VCRE 인스턴스의 직접적인 액세싱을 통해 PICNEEC에서의 다른 VCRE 인스턴스들에 독립적으로 제어됨 - 를 결정하는 단계;

[0155] 데이터 패킷에 대해 VCRE 인스턴스에서 정의된 하나 이상의 정책 규칙들을 실행하는 단계; 및

[0156] 데이터 패킷을 라우팅하는 단계를 포함하는 방법.

[0157] 30. 예 29의 방법에 있어서, 데이터 패킷은 서빙 일반 패킷 라디오 서비스(GPRS) 지원 노드/서빙(SGSN)과, PICNEEC에 대해 내부적인 게이트웨이 GPRS 지원 노드(GGSN) 사이에서 라우팅되는 방법.

[0158] 31. 예 29의 방법에 있어서, 데이터 패킷은 서빙 게이트웨이(SGW)와, PICNEEC에 대해 내부적인 PGW 사이에서 라우팅되는 방법.

[0159] 32. 예 29의 방법에 있어서, 데이터 패킷은 서빙 일반 패킷 라디오 서비스(GPRS) 지원 노드/서빙(SGSN)과, PICNEEC에 대해 외부적인 게이트웨이 GPRS 지원 노드(GGSN) 사이에서 라우팅되고, 외부적인 GGSN은 PICNEEC를 통해 인터넷 프로토콜(IP) 접속성 액세스 네트워크에 대한 데이터를 핸들링하는 방법.

[0160] 33. 예 29의 방법에 있어서, 데이터 패킷은 서빙 게이트웨이(SGW)와, PICNEEC에 대해 외부적인 PGW 사이에서 라우팅되고, 외부적인 PGW는 PICNEEC를 통해 IP 접속성 액세스 네트워크에 대한 데이터를 핸들링하는 방법.

[0161] 34. 예 29의 방법에 있어서, 데이터 패킷은 PICNEEC를 통해 데이터 패킷을 핸들링하는 이동 네트워크 서빙 패킷 게이트웨이를 통해 라우팅되는 방법.

[0162] 35. 이동 네트워크 제공자에 의한 동작을 위한 PDN 통합된 맞춤화된 네트워크 에지 인에이블러 및 제어기(PICNEEC)로서,

[0163] 적어도 하나의 가상적인 맞춤화된 규칙들 집행기(VCRE) 인스턴스 - 각각의 VCRE 인스턴스는 이동 디바이스들의 그룹에 대응하고 이동 디바이스들의 그룹에 대해 개인화된 정책들의 세트를 정의하고, 각각의 VCRE는 라디오 네트워크를 통해 패킷-기반 네트워크와, 대응하는 그룹에서의 이동 디바이스 사이에서 통신된 데이터 패킷을 수신할 시에, 데이터 패킷을 포워딩하기 이전에 데이터 패킷에 대한 VCRE 인스턴스에서 저장된 하나 이상의 정책 규칙들을 실행하도록 구성되고, 각각의 VCRE 인스턴스는 이동 네트워크 제공자의 상이한 고객에 의한 VCRE 인스턴스의 직접적인 액세싱을 통해 서로 독립적으로 제어됨 - 를 포함하고;

[0164] PICNEEC는 3G/4G 네트워크 및 저 전력 광역 네트워크(LPWAN)에 동시에 접속되는 PICNEEC.

[0165] 36. 예들 29 내지 34 중 어느 한 예의 방법을 수행하도록 머신의 프로세서를 제어하기 위한 머신 판독가능한 코드를 반송하는 머신 판독가능한 매체.

[0166] 언어

[0167] 이 명세서의 전반에 걸쳐, 복수의 사례들은 단일 사례로서 설명된 컴포넌트들, 동작들, 또는 구조들을 구현할 수도 있다. 하나 이상의 방법들의 개별적인 동작들은 별도의 동작들로서 예시되고 설명되지만, 개별적인 동작들 중 하나 이상은 동시에 수행될 수도 있고, 어떤 것도 동작들이 예시된 순서로 수행되는 것을 요구하지는 않는다. 예시적인 구성들에서 별도의 컴포넌트들로서 제시된 구조들 및 기능성은 조합된 구조 또는 컴포넌트로서 구현될 수도 있다. 유사하게, 단일 컴포넌트로서 제시된 구조들 및 기능성은 별도의 컴포넌트들로서 구현될 수도 있다. 이러한 그리고 다른 변형들, 수정들, 추가들, 및 개선들은 본원에서의 요지의 범위 내에 속한다.

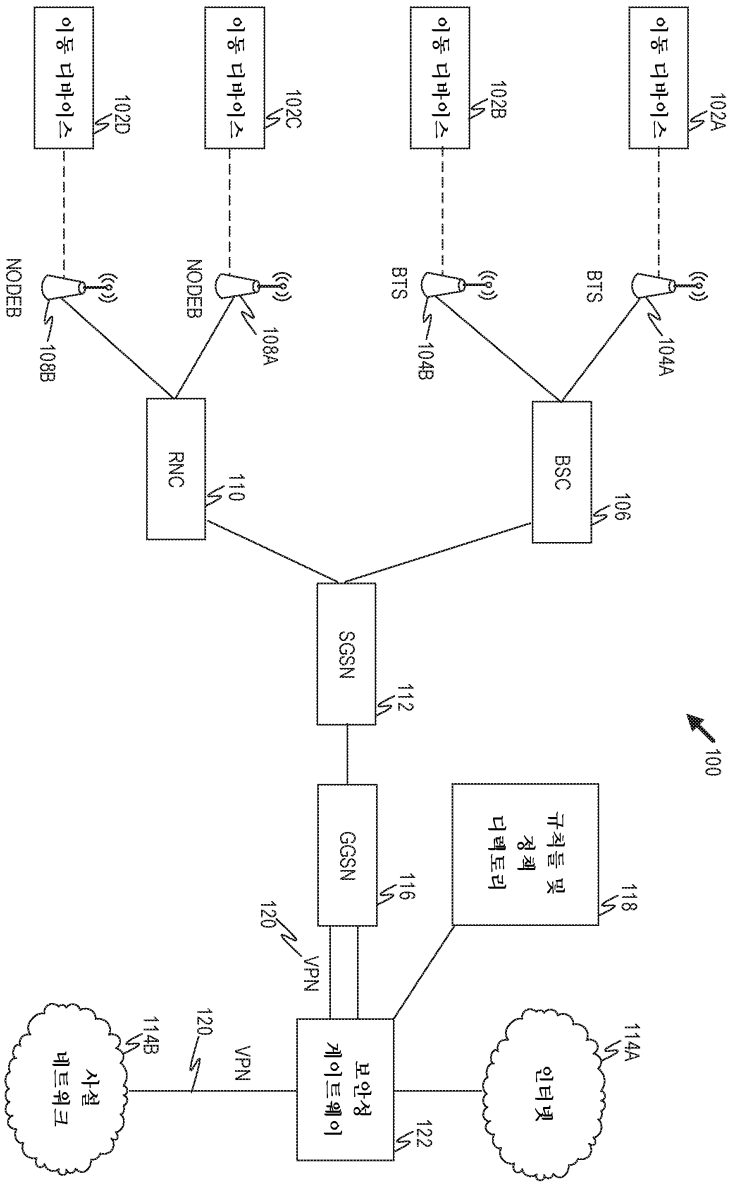
[0168] 발명 요지의 개요는 특정 예시적인 실시예들을 참조하여 설명되었지만, 본 개시내용의 실시예들의 더 넓은 범위로부터 이탈하지 않으면서, 다양한 수정들 및 변경들이 이 실시예들에 대해 행해질 수도 있다. 발명 요지의 이러한 실시예들은 단지 편의상, 그리고 이 출원의 범위를 임의의 단일 개시내용, 또는 하나를 초과하는 것이 실제로 개시될 경우에 발명 개념으로 자발적으로 제한하도록 의도하지 않으면서, 용어 "발명"에 의해 개별적으로 또는 집합적으로 본원에서 지칭될 수도 있다.

[0169] 본원에서 예시된 실시예들은 본 기술분야의 통상의 기술자들이 개시된 교시사항들을 실시하는 것을 가능하게 할 정도로 충분히 상세하게 설명된다. 다른 실시예들이 이용될 수도 있고 그로부터 유도될 수도 있어서, 구조적 및 논리적 치환들 및 변경들은 이 개시내용의 범위로부터 이탈하지 않으면서 행해질 수도 있다. 그러므로, 상세한 설명은 제한적인 의미로 택해진 것이 아니고, 다양한 실시예들의 범위는 이러한 청구항들에 부여되는 등가물들의 전체 범위와 함께, 오직 첨부된 청구항들에 의해 정의된다.

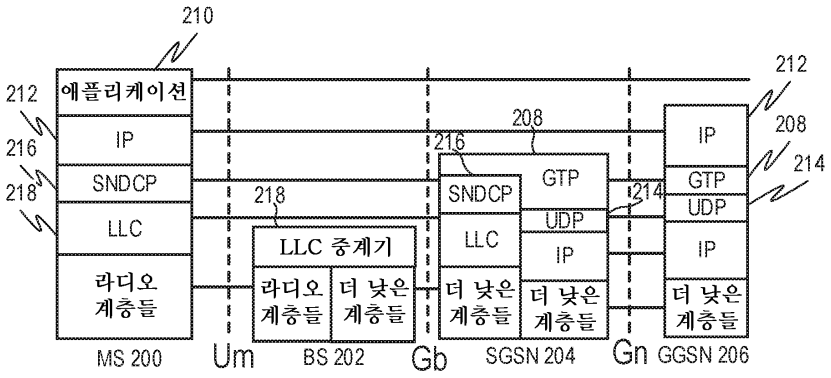
[0170] 본원에서 이용된 바와 같이, 용어 "또는"은 포괄적 또는 배타적 의미의 어느 하나로 해석될 수도 있다. 또한, 복수의 사례들은 본원에서 설명된 자원들, 동작들, 또는 구조들에 대하여 단일 사례로서 제공될 수도 잇다. 추가적으로, 다양한 자원들, 동작들, 모듈들, 엔진들, 및 데이터 저장소들 사이의 경계들은 다소 임의적이고, 특정한 동작들은 특정 예시적인 구성들의 맥락에서 예시된다. 기능성의 다른 할당들이 구상되고, 본 개시내용의 다양한 실시예들의 범위 내에 속할 수도 있다. 일반적으로, 예시적인 구성들에서 별도의 자원들로서 제시된 구조들 및 기능성은 조합된 구조 또는 자원으로서 구현될 수도 있다. 유사하게, 단일 자원으로서 제시된 구조들 및 기능성은 별도의 자원들로서 구현될 수도 있다. 이러한 그리고 다른 변형들, 수정들, 추가들, 및 개선들은 첨부된 청구항들에 의해 표현된 바와 같이 본 개시내용의 실시예들의 범위 내에 속한다. 따라서, 명세서 및 도면들은 한정적인 의미보다는 예시적으로 간주되어야 한다.

도면

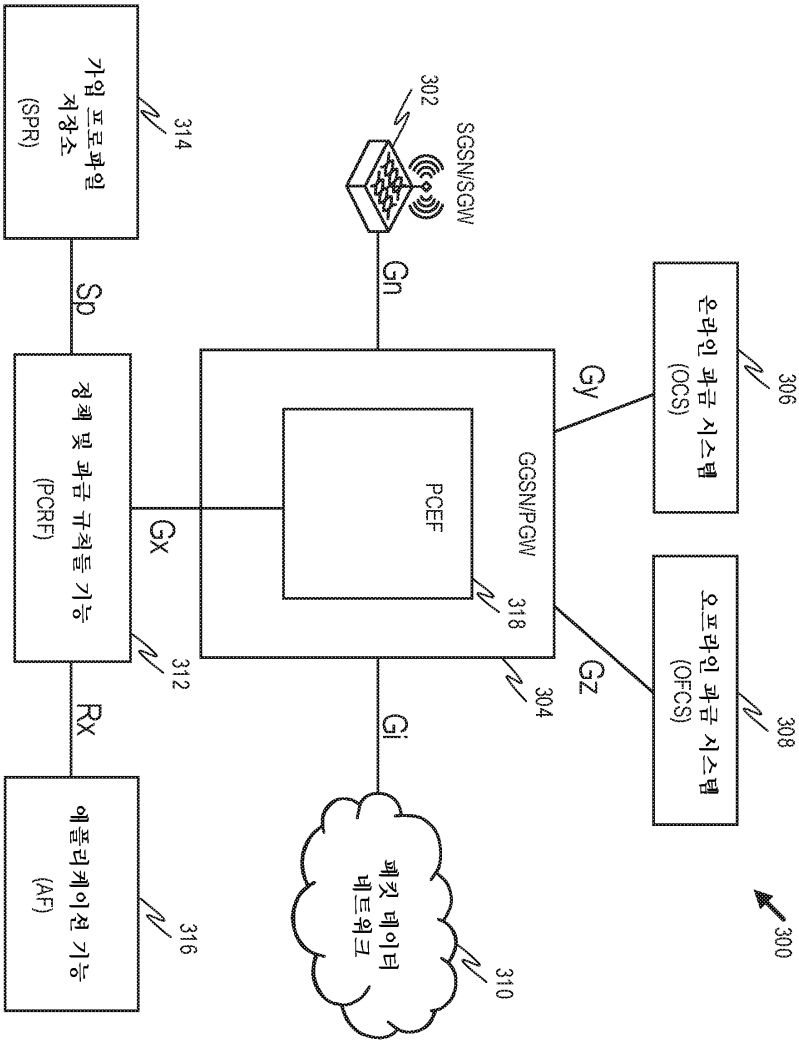
도면1


이동 디바이스
102D
102C
102B
102A
NODEB
108B
108A
BTS
104B
104A
RNC
110
BSC
106
SGSN
112
100
GGSN
116
규칙들 및 정책 디렉토리
118
120
VPN
114B
사설 네트워크
보안성 게이트웨이
122
인터넷
114A

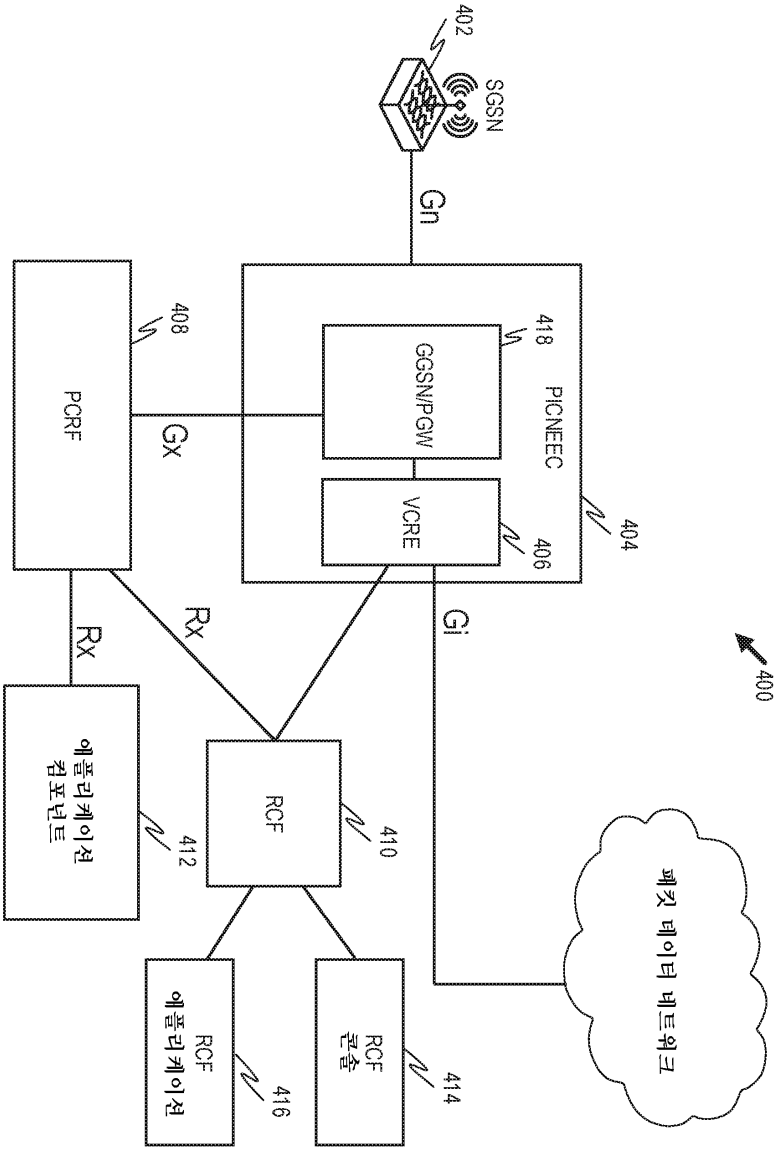
도면2


210
212
에플리케이션
IP
216
SNDCP
218
LLC
라디오 계층들
MS 200
Um
LLC 중계기
라디오 계층들
더 낮은 계층들
BS 202
208
Gb
SNDCP
GTP
UDP
IP
더 낮은 계층들
SGSN 204
Gn
GGSN 206
214

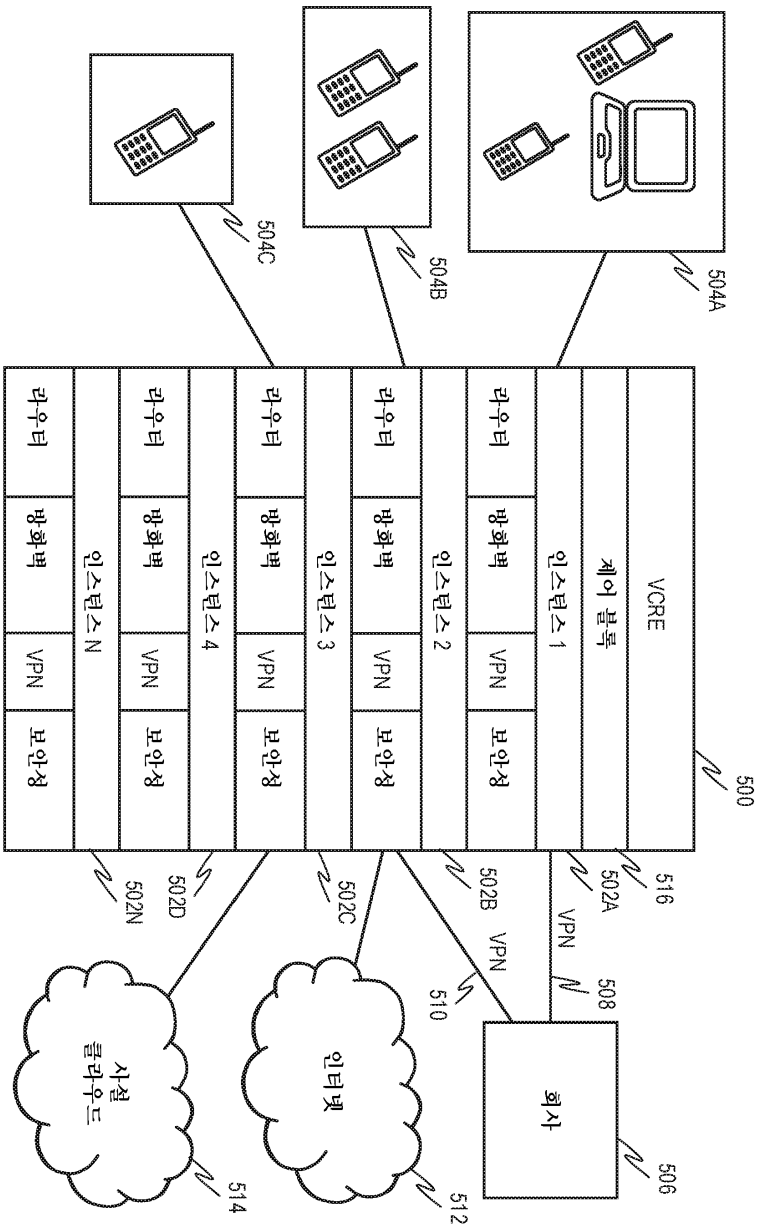
도면3


가입 프로파일 저장소 (SPR)
314
Sp
정책 및 과금 규칙들 기능 (PCRF)
312
Rx
애플리케이션 기능 (AF)
316
302
SGSN/SGW
Gn
GGSN/PGW
PCEF
318
304
Gx
Gy
Gz
Gi
온라인 과금 시스템 (OCS)
306
오프라인 과금 시스템 (OFCS)
308
패킷 데이터 네트워크
310
300

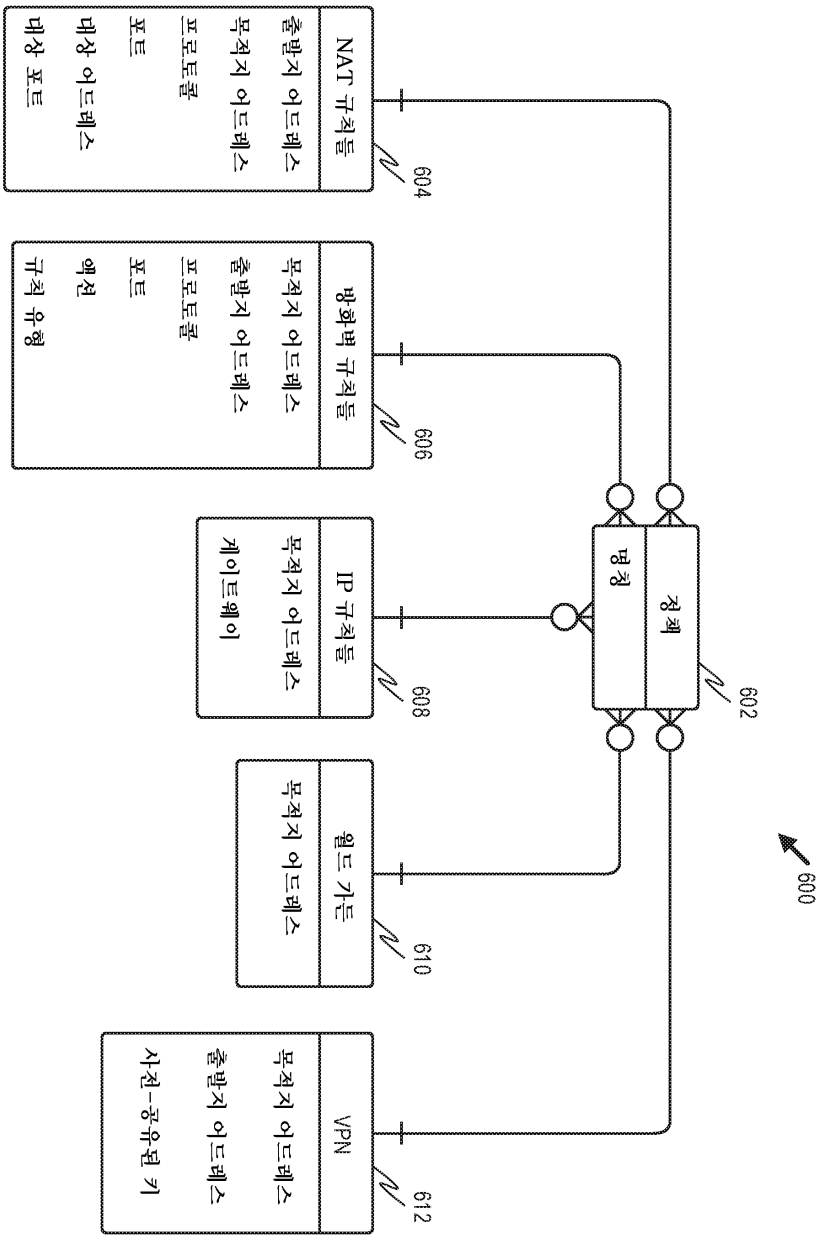
도면4


402
SGSN
Gn
408
PCRF
Gx
418
GGSN/PGW
PICNEEC
404
VCRE
406
Rx
Rx
Gi
400
에플리케이션
컴포넌트
412
RCF
410
RCF
에플리케이션
416
RCF
콘솔
414
패킷 데이터 네트워크

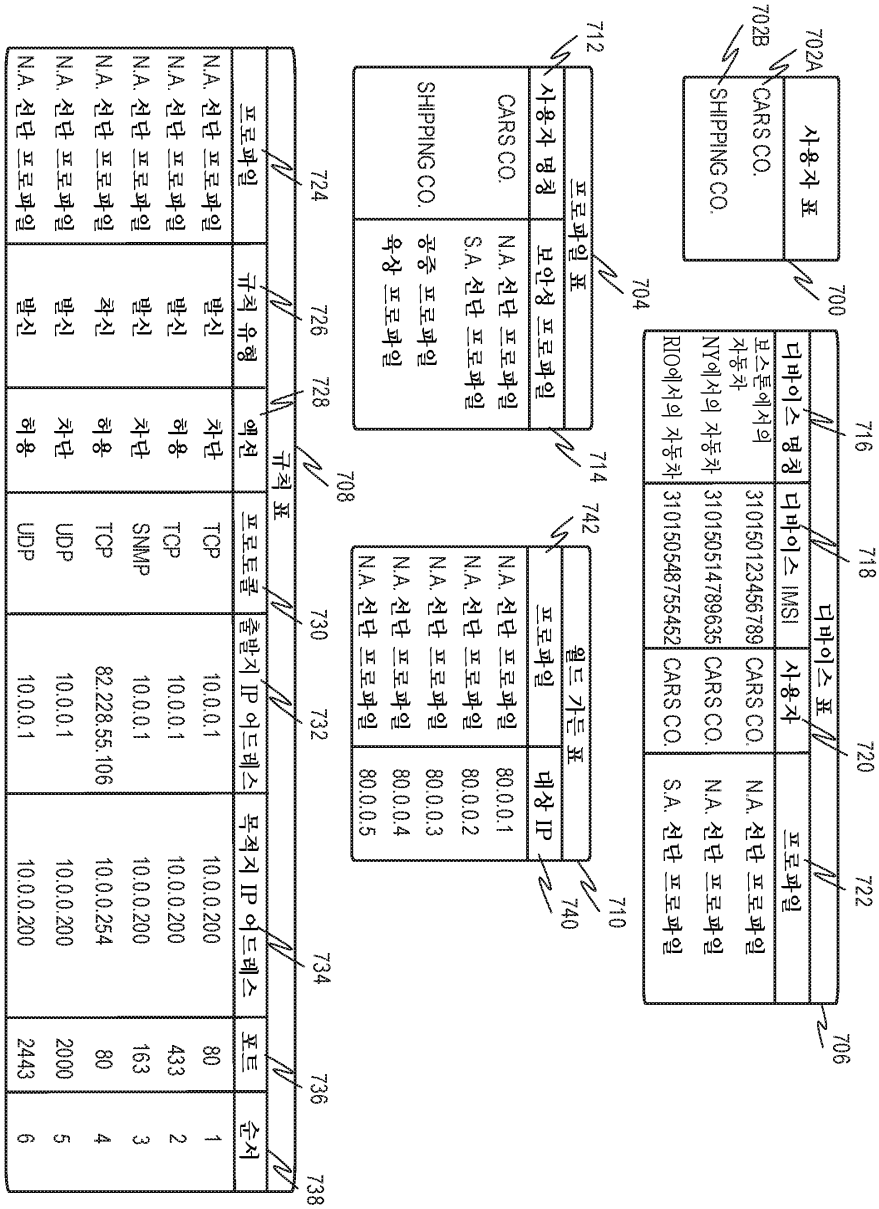
도면5


504A
504B
504C
500
VCRE
제어 블록
인스턴스 1
인스턴스 2
인스턴스 3
인스턴스 4
인스턴스 N
라우터
방화벽
VPN
보안성
516
502A
502B
502C
502D
502N
VPN
508
510
회사
506
인터넷
512
사설
클라우드
514

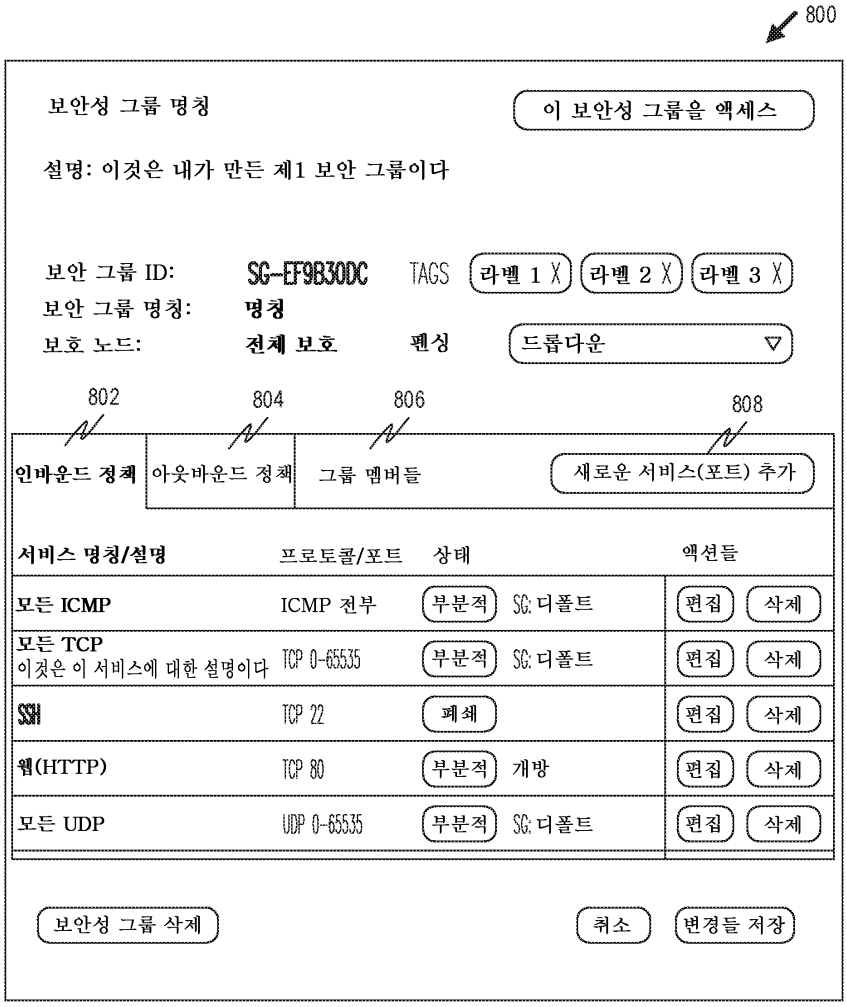
도면6


600
602
정책
명칭
NAT 규칙들
604
출발지 어드레스
목적지 어드레스
프로토콜
포트
대상 어드레스
대상 포트
방화벽 규칙들
606
목적지 어드레스
출발지 어드레스
프로토콜
포트
액션
규칙 유형
IP 규칙들
608
목적지 어드레스
게이트웨이
월드 가든
610
목적지 어드레스
VPN
612
목적지 어드레스
출발지 어드레스
사전-공유된 키

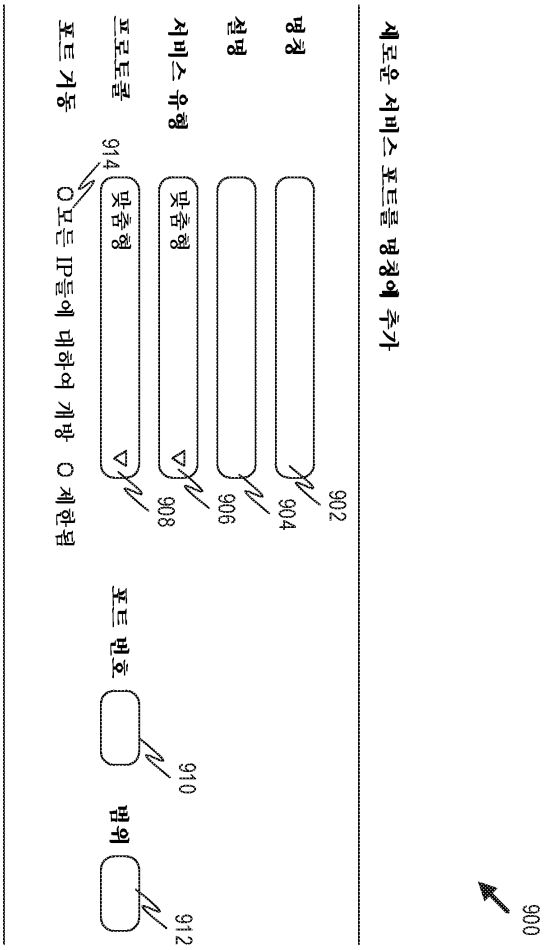
도면7


사용자 표
CARS CO.
SHIPPING CO.
디바이스 표
디바이스 명칭
디바이스 IMSI
사용자
프로파일
보스톤에서의 자동차
NY에서의 자동차
RIO에서의 자동차
310150123456789
310150514789635
310150548755452
CARS CO.
CARS CO.
S.A. 천단 프로파일
N.A. 천단 프로파일
프로파일 표
사용자 명칭
보안성 프로파일
CARS CO.
SHIPPING CO.
N.A. 천단 프로파일
S.A. 천단 프로파일
공중 프로파일
육상 프로파일
월드 가든 표
프로파일
대상 IP
N.A. 천단 프로파일
N.A. 천단 프로파일
N.A. 천단 프로파일
N.A. 천단 프로파일
N.A. 천단 프로파일
80.0.0.1
80.0.0.2
80.0.0.3
80.0.0.4
80.0.0.5
규칙 표
프로파일
규칙 유형
액션
프로토콜
출발지 IP 어드레스
목적지 IP 어드레스
포트
순서
N.A. 천단 프로파일
N.A. 천단 프로파일
N.A. 천단 프로파일
N.A. 천단 프로파일
N.A. 천단 프로파일
N.A. 천단 프로파일
발신
발신
발신
착신
발신
발신
차단
허용
차단
허용
차단
UDP
TCP
TCP
SNMP
TCP
UDP
UDP
10.0.0.1
10.0.0.1
10.0.0.1
82.228.55.106
10.0.0.1
10.0.0.1
10.0.0.200
10.0.0.200
10.0.0.200
10.0.0.254
10.0.0.200
10.0.0.200
80
433
163
80
2000
2443
1
2
3
4
5
6

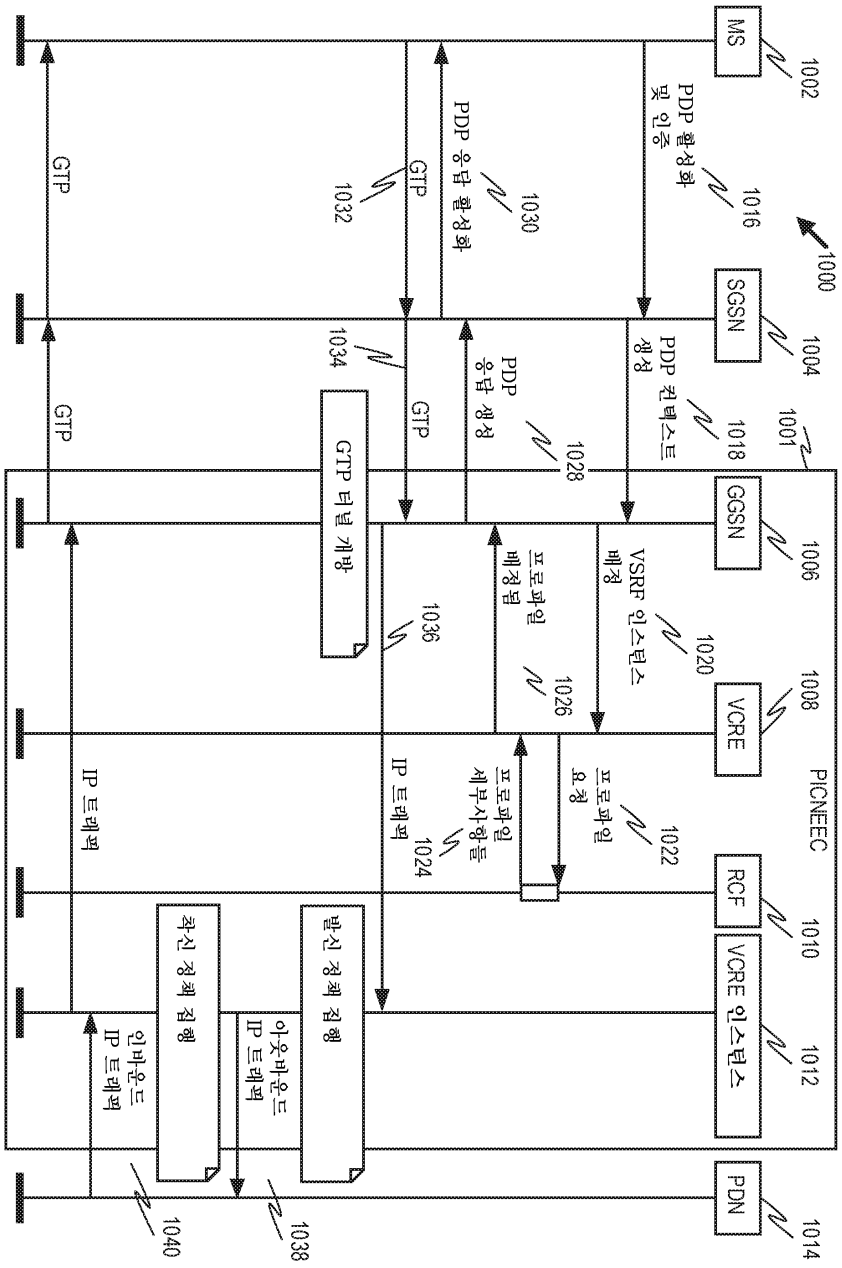
도면8


800
보안성 그룹 명칭
이 보안성 그룹을 액세스
설명: 이것은 내가 만든 제1 보안 그룹이다
보안 그룹 ID:
SG-EF9B30DC
TAGS
라벨 1 X
라벨 2 X
라벨 3 X
보안 그룹 명칭:
명칭
보호 노드:
전체 보호
펜싱
드롭다운
802
804
806
808
인바운드 정책
아웃바운드 정책
그룹 멤버들
새로운 서비스(포트) 추가
서비스 명칭/설명
프로토콜/포트
상태
액션들
모든 ICMP
ICMP 전부
부분적
SG 디폴트
편집
삭제
모든 TCP
이것은 이 서비스에 대한 설명이다
TCP 0-65535
부분적
SG 디폴트
편집
삭제
SSH
TCP 22
폐쇄
편집
삭제
웹(HTTP)
TCP 80
부분적
개방
편집
삭제
모든 UDP
UDP 0-65535
부분적
SG 디폴트
편집
삭제
보안성 그룹 삭제
취소
변경들 저장

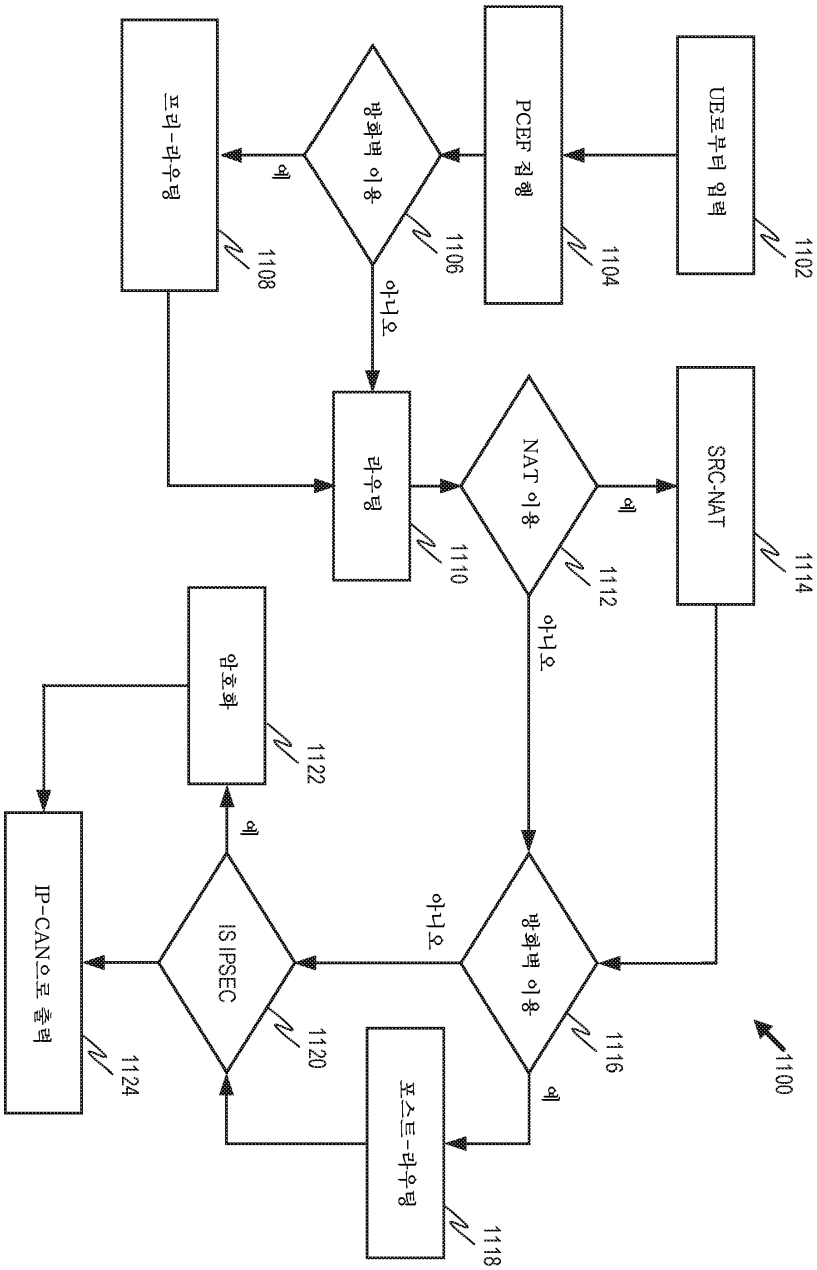
도면9


900
새로운 서비스 포트를 명칭에 추가
902
명칭
904
설명
906
서비스 유형
맞춤형
908
프로토콜
맞춤형
914
포트 번호
910
범위
912
포트 개방
○모든 IP들에 대하여 개방 ○제한됨
취소
저장 및 이전

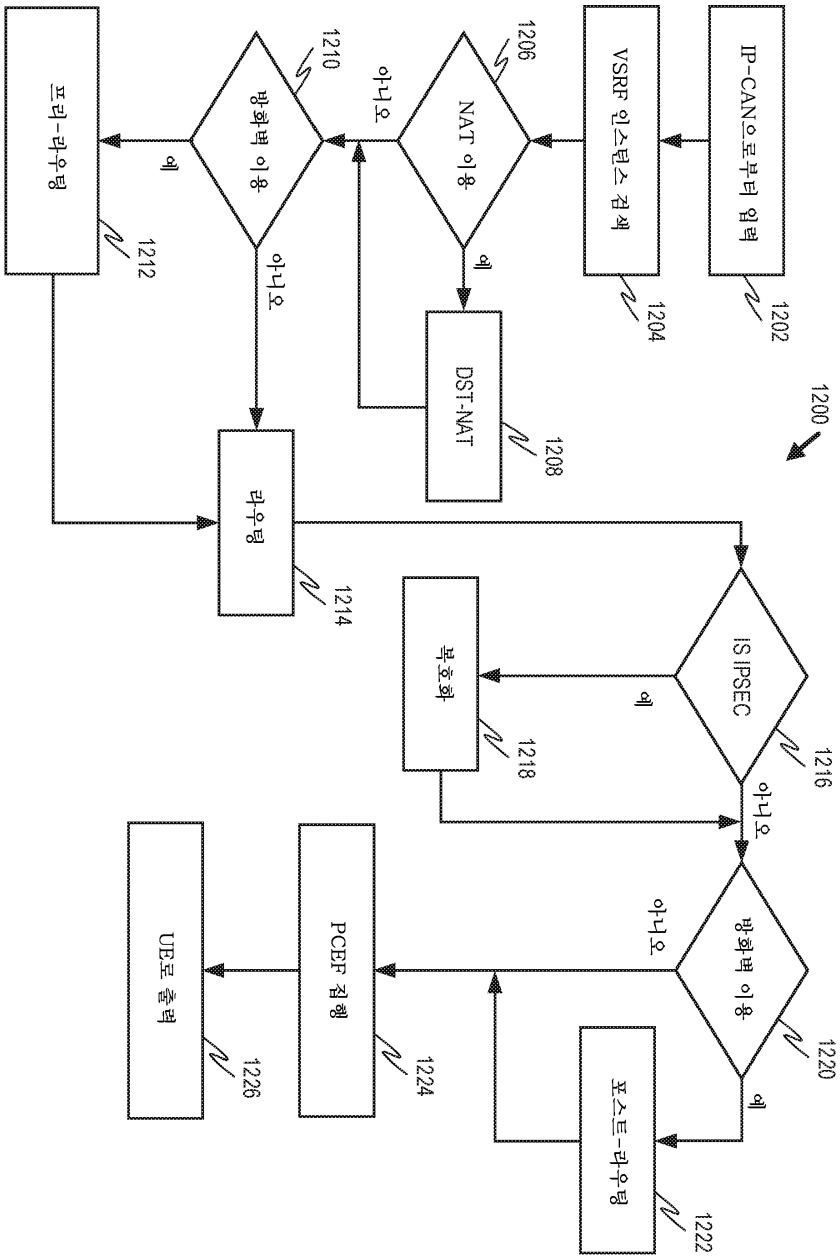
도면10


MS
1002
PDP 활성화 및 인증
1016
1000
SGSN
1004
PDP 컨텍스트 생성
1018
1001
GGSN
1006
VSRF 인스턴스 배정
1020
VCRE
1008
PICNEEC
프로파일 배정됨
1026
프로파일 요청
1022
RCF
1010
VCRE 인스턴스
1012
PDN
1014
GTP
1032
PDP 응답 활성화
1030
PDP 응답 생성
1028
GTP
1034
GTP 터널 개방
1036
GTP
IP 트래픽
프로파일 세부사항들
1024
IP 트래픽
착신 정책 집행
발신 정책 집행
아웃바운드 IP 트래픽
인바운드 IP 트래픽
1040
1038

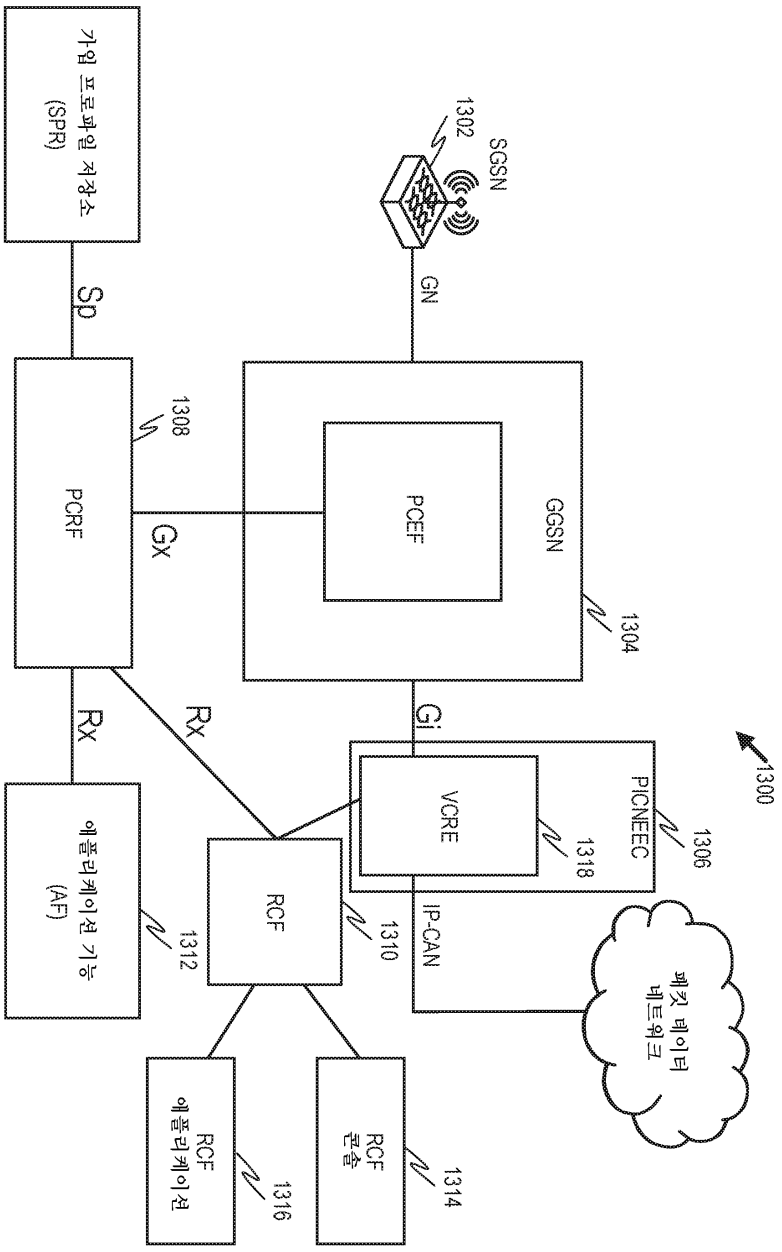
도면11


UE로부터 입력
1102
PCEF 집행
1104
방화벽 이용
1106
예
아니오
프리-라우팅
1108
라우팅
1110
NAT 이용
1112
예
아니오
SRC-NAT
1114
방화벽 이용
1116
예
아니오
포스트-라우팅
1118
IS IPSEC
1120
예
아니오
암호화
1122
IP-CAN으로 출력
1124
1100

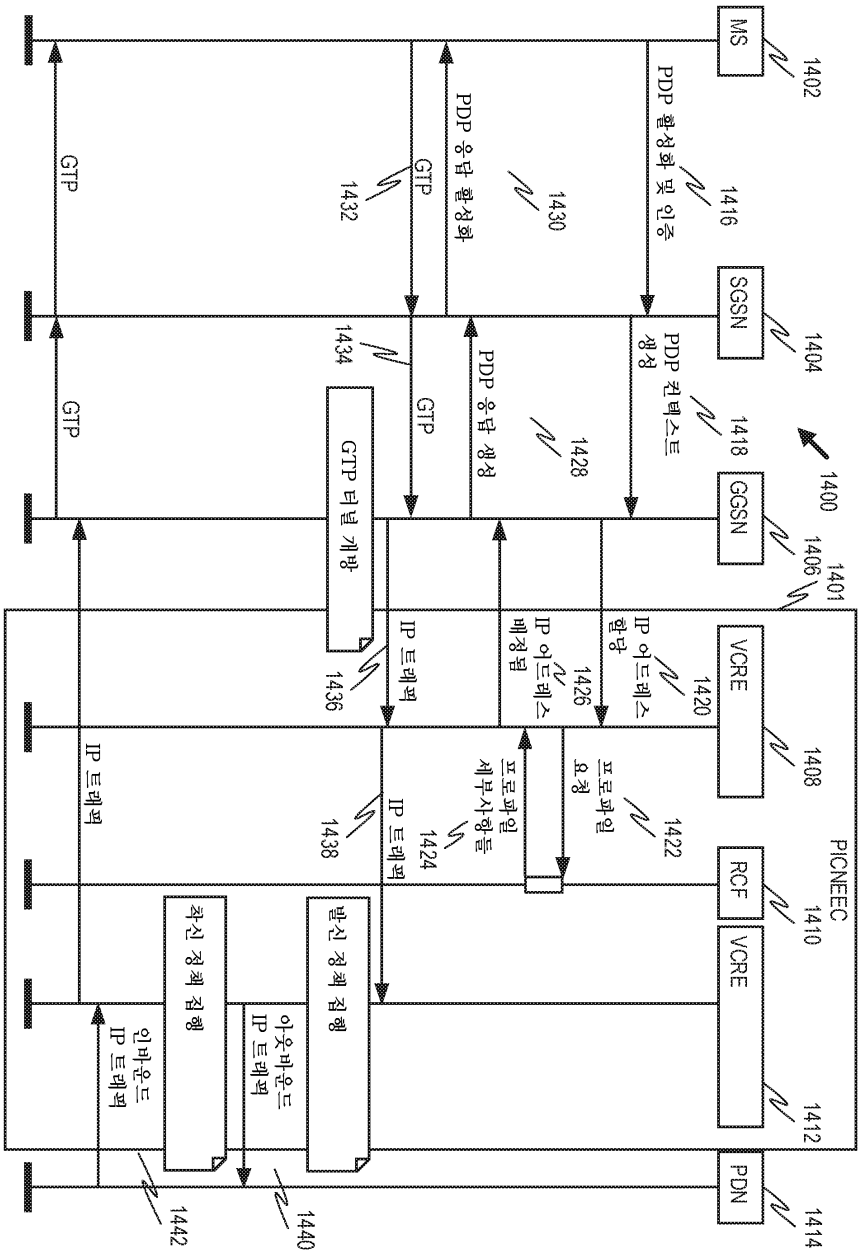
도면12


1200
IP-CAN으로부터 입력
1202
VSRF 인스턴스 검색
1204
NAT 이용
1206
예
아니오
DST-NAT
1208
방화벽 이용
1210
예
아니오
프리-라우팅
1212
라우팅
1214
IS IPSEC
1216
예
복호화
1218
아니오
방화벽 이용
1220
아니오
예
포스트-라우팅
1222
PCEF 집행
1224
UE로 출력
1226

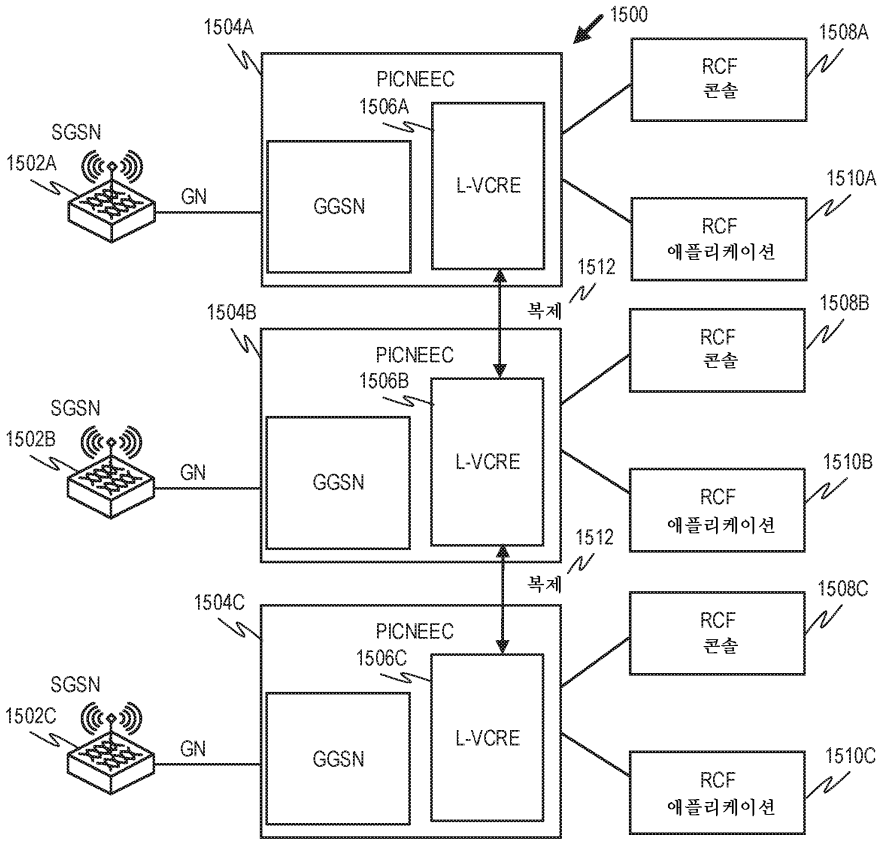
도면13


가입 프로파일 저장소
(SPR)
Sp
PCRF
1308
Gx
Rx
Rx
에플리케이션 기능
(AF)
1312
SGSN
1302
Gn
PCEF
GGSN
1304
Gi
VCRE
PICNEEC
1318
1306
1300
RCF
1310
IP-CAN
패킷 데이터
네트워크
RCF
에플리케이션
1316
RCF
콘솔
1314

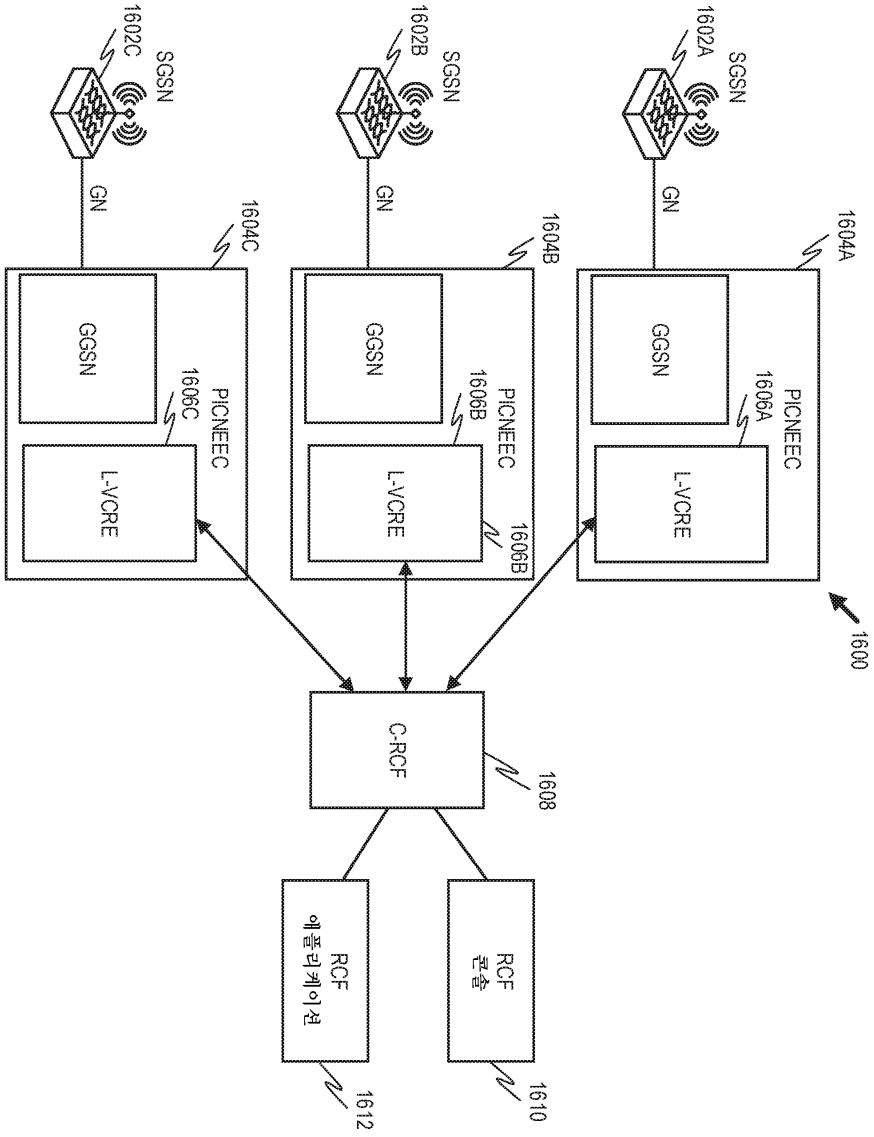
도면14


MS
1402
PDP 활성화 및 인증
1416
SGSN
1404
PDP 컨텍스트 생성
1418
GGSN
1406
1400
1401
PDP 응답 활성화
1430
GTP
1432
PDP 응답 생성
1428
GTP
1434
GTP 터널 개방
GTP
GTP
IP 어드레스 할당
1420
VCRE
1408
IP 어드레스 베경됨
1426
IP 트래픽
1436
프로파일 요청
1422
RCF
1410
프로파일 세부사항들
1424
IP 트래픽
1438
VCRE
1412
IP 트래픽
발신 정책 집행
착신 정책 집행
아웃바운드 IP 트래픽
인바운드 IP 트래픽
PICNEEC
PDN
1414
1440
1442

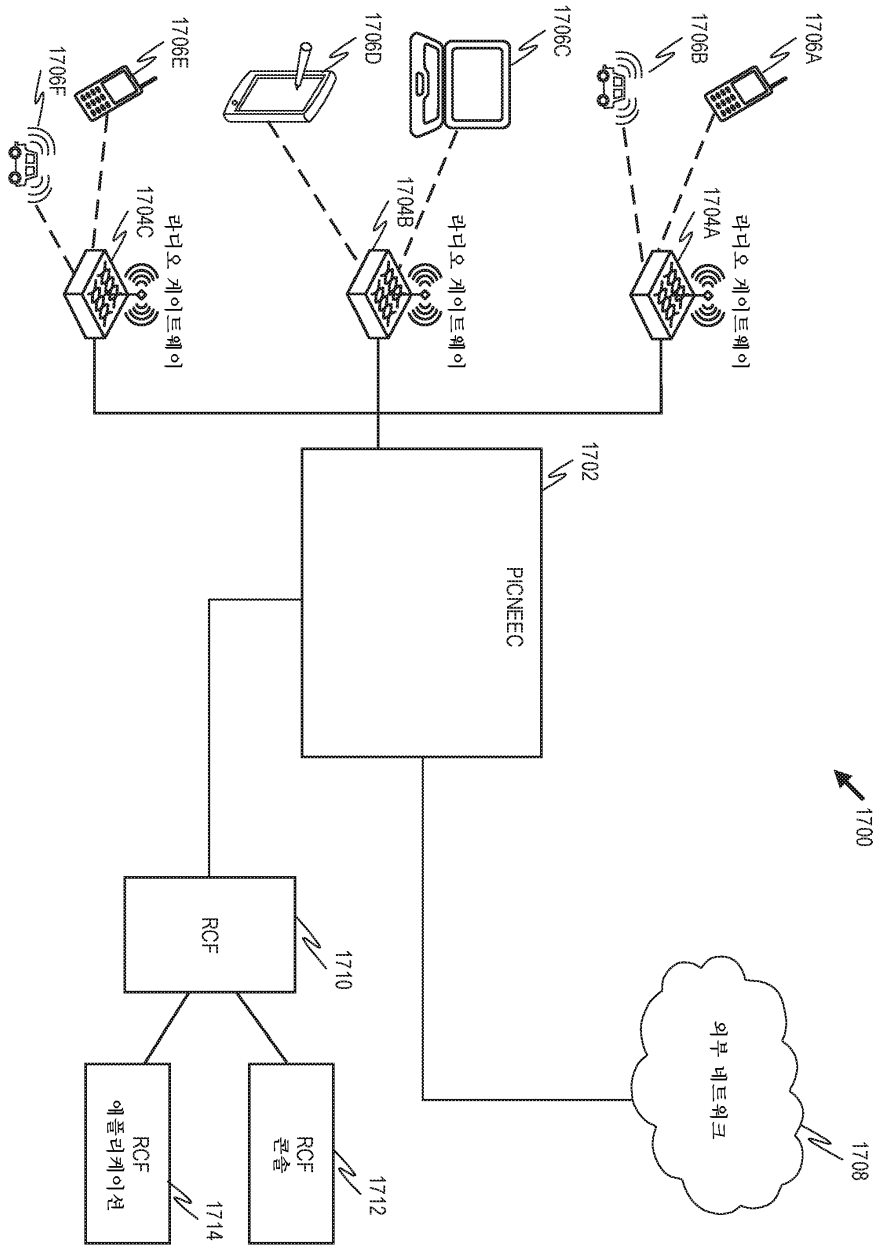
도면15


1500
1504A
PICNEEC
1506A
GGSN
L-VCRE
SGSN
1502A
GN
1508A
RCF
콘솔
1510A
RCF
애플리케이션
1512
복제
1504B
PICNEEC
1506B
GGSN
L-VCRE
SGSN
1502B
GN
1508B
RCF
콘솔
1510B
RCF
애플리케이션
1512
복제
1504C
PICNEEC
1506C
GGSN
L-VCRE
SGSN
1502C
GN
1508C
RCF
콘솔
1510C
RCF
애플리케이션

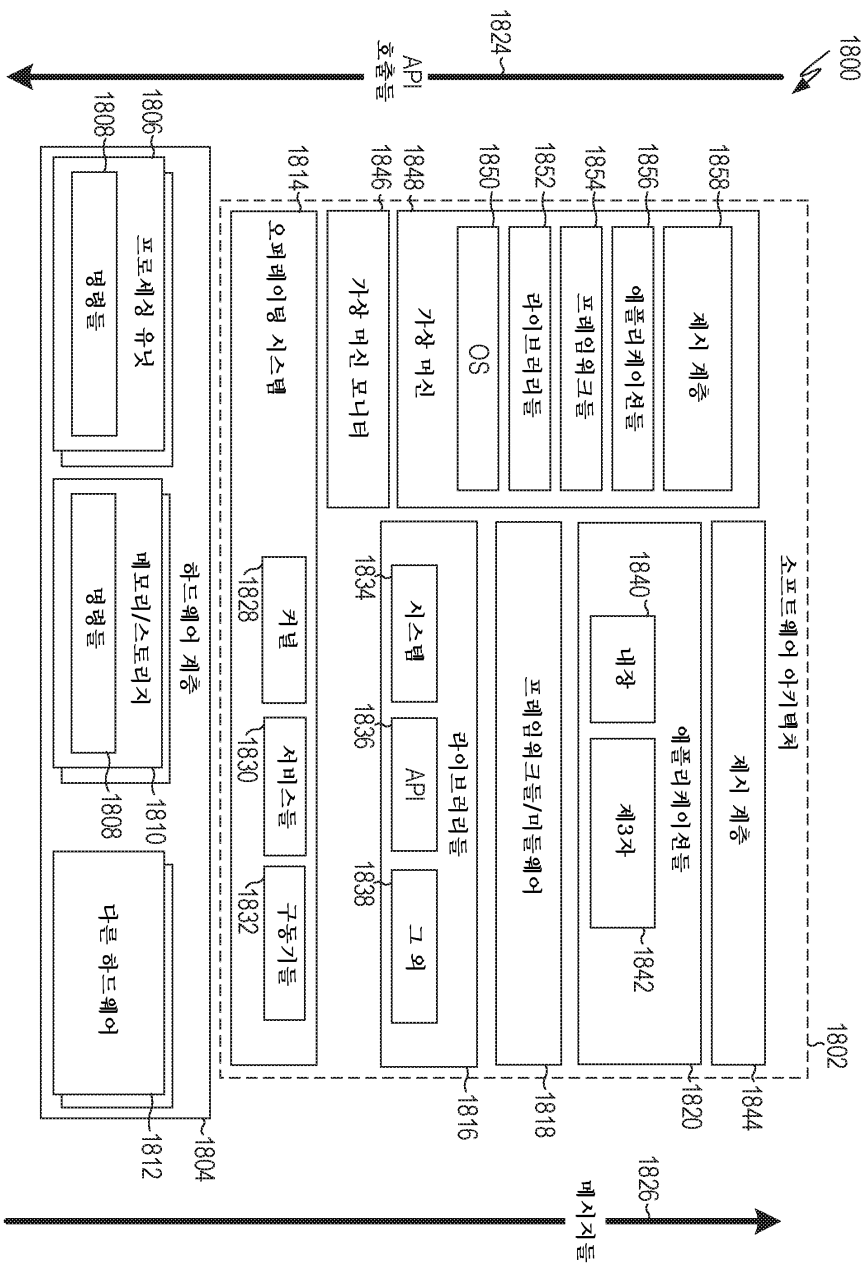
도면16


1602C
SGSN
1602B
SGSN
1602A
SGSN
GN
GN
GN
1604C
1604B
1604A
GGSN
GGSN
GGSN
PICNEEC
1606C
PICNEEC
1606B
PICNEEC
1606A
L-VCRE
L-VCRE
L-VCRE
1606B
1600
C-RCF
1608
RCF
에플리케이션
RCF
콘솔
1612
1610

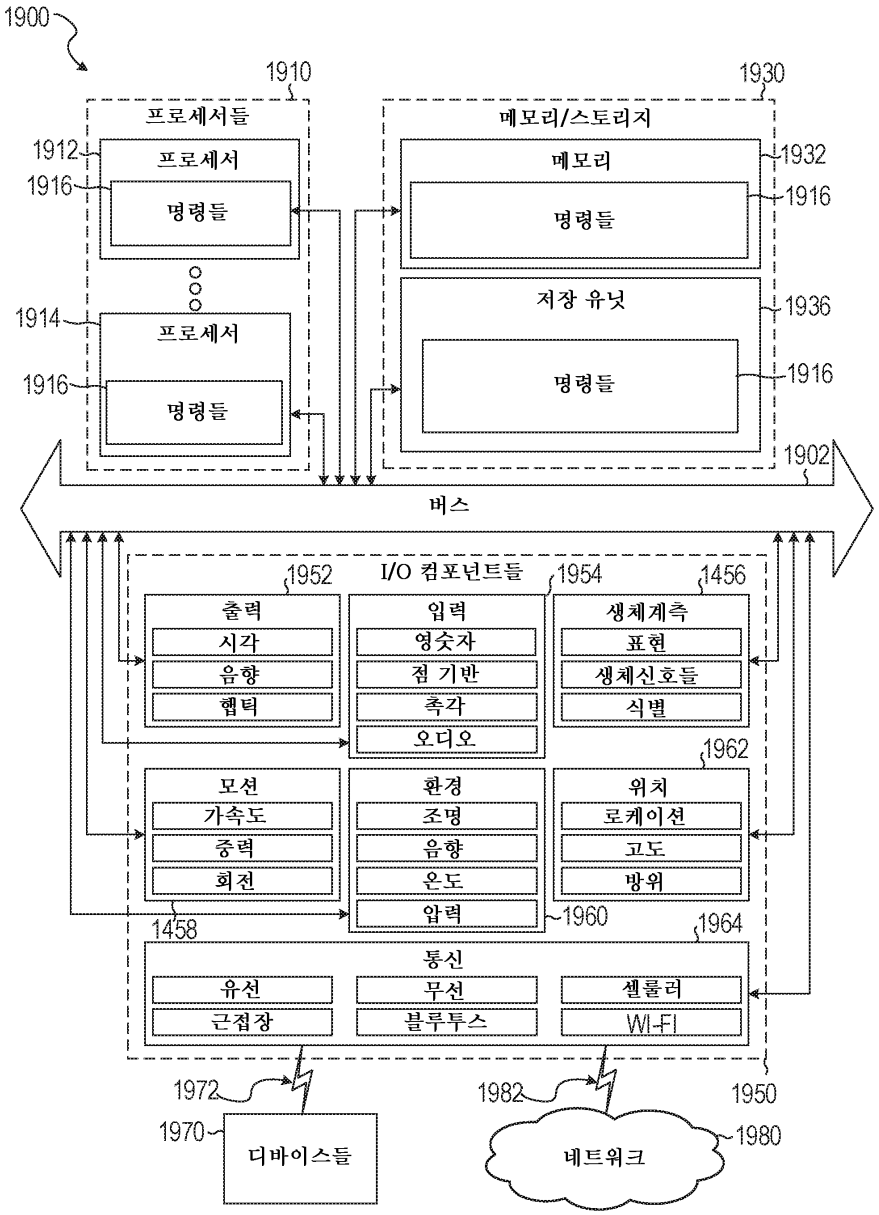
도면17


1706A
1706B
1706C
1706D
1706E
1706F
라디오 게이트웨이
1704A
라디오 게이트웨이
1704B
라디오 게이트웨이
1704C
1702
PICNEEC
1700
RCF
1710
외부 네트워크
1708
RCF
콘솔
1712
RCF
에플리케이션
1714

도면18


1800
1824
API 호출들
1802
소프트웨어 아키텍처
제시 계층
1858
에플리케이션들
1856
프레임워크들
1854
라이브러리들
1852
OS
1850
가상 머신
1848
가상 머신 모니터
1846
오퍼레이팅 시스템
1814
커널
1828
서비스들
1830
구동기들
1832
라이브러리들
1816
시스템
1834
API
1836
그 외
1838
프레임워크들/미들웨어
1818
에플리케이션들
1820
내장
1840
제3자
1842
제시 계층
1844
1826
메시지들
하드웨어 계층
1804
프로세싱 유닛
1806
명령들
1808
메모리/스토리지
1810
명령들
1808
다른 하드웨어
1812

도면19


1900
1910
프로세서들
1912
프로세서
1916
명령들
1914
프로세서
1916
명령들
1930
메모리/스토리지
메모리
1932
1916
명령들
저장 유닛
1936
1916
명령들
1902
버스
1952
I/O 컴포넌트들
1954
1456
출력
시각
음향
햅틱
입력
영숫자
점 기반
촉각
오디오
생체계측
표현
생체신호들
식별
1962
모션
가속도
중력
회전
환경
조명
음향
온도
압력
위치
로케이션
고도
방위
1458
1960
1964
통신
유선
근접장
무선
블루투스
셀룰러
WI-FI
1972
1970
디바이스들
1982
1950
네트워크
1980