(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 894 365**

(51) Int. CI.:

H04W 12/088 (2011.01)
H04L 29/06 (2006.01)
H04L 29/12 (2006.01)
H04W 88/16 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **02.12.2016 PCT/IB2016/001827**

(87) Fecha y número de publicación internacional: **15.06.2017 WO17098320**

(96) Fecha de presentación y número de la solicitud europea: **02.12.2016 E 16872480 (5)**

(97) Fecha y número de publicación de la concesión europea: **21.07.2021 EP 3387817**

(54) Título: **Encaminamiento y seguridad en una red móvil**

(30) Prioridad:

08.12.2015 US 201562264791 P
05.04.2016 US 201615090918

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
14.02.2022

(73) Titular/es:

JPU.IO LTD (100.0%)
PO Box 4098 Imber 14
49514 Petach Tikva, IL

(72) Inventor/es:

SCHWARTZ, JONATHAN y
MALKA, FRANCK

(74) Agente/Representante:

ISERN JARA, Jorge

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín Europeo de Patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre Concesión de Patentes Europeas).

DESCRIPCIÓN

Encaminamiento y seguridad en una red móvil

Campo técnico

La presente divulgación se refiere, en general, a interconexiones en red de radio móvil. Más específicamente, la presente divulgación describe una técnica para encaminamiento y seguridad de red en una red de radio móvil.

Antecedentes

Las redes móviles permiten que los dispositivos se conecten a redes de conmutación de paquetes externas (tales como internet) como parte del servicio básico proporcionado en la red como se define por organismos de normas internacionales. Un ejemplo de tales organismos de normas internacionales incluye los dominios del Proyecto Asociación de 3ª Generación (3GPP) para el Sistema Global para Comunicación Móvil (GSM)/Sistema Universal de Telecomunicación Móvil (UMTS)/Evolución a Largo Plazo (LTE), las redes de Acceso Múltiple por División en el Tiempo (TDMA)/Acceso Múltiple por División de Código (CDMA)/CDMA2000 y las iniciativas de diseño de red más modernas tales como LoRa y SIGFOX.

En tales sistemas, los datos de paquetes que vienen a y desde un dispositivo móvil se transmiten mediante las redes de radio a elementos tales como una Estación Transceptora Base (BTS) en una red de 2G, un Nodo B en una red de 3G o un eNodo B en una red de 4G. Posteriormente, los datos de paquetes se envían usando túneles hacia un Nodo de Soporte (SGSN) del Servicio General de Paquetes de Radio de Servicio (GPRS) en una red de 2G/3G o a la Pasarela de Servicio (SGW) en una red de 4G o dispositivo similar en otras soluciones de red móvil.

Los túneles del protocolo de Tunelización de GPRS (GTP) desde todos los dispositivos móviles se agregan hacia un Nodo de Soporte de GPRS de pasarela (GGSN) en una red de 2G/3G o de la Pasarela de PDN (PGW) en una red de 4G o dispositivo similar en otras soluciones de red móvil. Estos dispositivos a continuación se fusionan en muchas conexiones de Ethernet que contienen numerosos túneles en cada conexión.

Es entonces la responsabilidad del GGSN o de la PGW dispersar los túneles de tráfico de GTP agregados en múltiples flujos de datos y encaminar cada único flujo a su destino diseñado en la red de conmutación de paquetes externa como se diseñó inicialmente por el dispositivo móvil.

Las normas del 3GPP también definen que cada dispositivo móvil definirá un contexto de encaminamiento con el que se conecta a al GGSN o a la PGW apropiada, denominado el Nombre de Punto de Acceso (APN). Las normas del 3GPP permiten que cada APN tenga su propia política de encaminamiento y seguridad en el GGSN o la PGW junto con la capacidad para encaminar los datos de paquete a través de un cortafuegos usando un conjunto de reglas específico.

Sin embargo, tales conjuntos de reglas personalizadas de APN se definen por el personal del operador de la red móvil ya que él o ella tienen acceso único al equipo encaminador (por ejemplo, el GGSN o la PGW).

En contraste, fuera del contexto de la red móvil, los individuos o las organizaciones pueden desplegar su propio equipo de encaminamiento y de cortafuegos para mantener el control total sobre las capacidades de red de sus dispositivos. Esta capacidad hoy en día está privada de cualquier organización individual que desee definir sus propias políticas de encaminamiento y seguridad en sus dispositivos móviles, ya que esta política puede definirse únicamente por el operador de red móvil.

El documento US8316435 describe un cortafuegos compatible con MPLS que permite que se apliquen políticas de seguridad de cortafuegos a tráfico de MPLS. El cortafuegos puede implementarse en un dispositivo de encaminamiento que puede generar información de mapeo para que el cortafuegos mapee unas VPN del cliente a etiquetas de MPLS específicas para los túneles de MPLS que llevan el tráfico del cliente. El documento US2012/233668 se refiere a la capacidad de extensión del usuario en un sistema de informática en la nube. Las interfaces de módulos de extensión pueden usarse para modificar la asignación de recursos virtuales a físicos a través de múltiples dispositivos. El documento EP2557854 analiza el establecimiento de una VPN móvil en la que las redes de proveedor de servicio cooperan para extender un área de encaminamiento virtual de un proveedor de servicio doméstico hasta el perímetro de una red de proveedor de servicio visitada posibilitando de esta manera la continuidad de la dirección de IP para un dispositivo inalámbrico en itinerancia.

Sumario

La invención es un método y aparato como se define en las reivindicaciones adjuntas.

Breve descripción de los dibujos

Se ilustran algunas realizaciones a modo de ejemplo y no a modo de limitación en las figuras de los dibujos adjuntos, en las que:

La Figura 1 es un diagrama de bloques que ilustra un sistema, de acuerdo con una realización de ejemplo, para encaminar comunicaciones de red móvil.
La Figura 2 es un diagrama de bloques que ilustra pilas de protocolo para servicios de subred de GPRS, de acuerdo con una realización de ejemplo.
La Figura 3 es un diagrama de bloques que ilustra un sistema que incluye un SGSN/SGW y un GGSN/pasarela (PGW) de Red de Datos de Paquetes (PDN).
La Figura 4 es un diagrama de bloques que ilustra un sistema, de acuerdo con una realización de ejemplo, que incluye un SGSN/SGW y un Habilitador y Controlador de Perímetro de Red Personalizada Integrada de PDN (PICNEEC) que incluye un GGSN/PGW.
La Figura 5 es un diagrama de bloques que ilustra un VCRE, en más detalle, de acuerdo con una realización de ejemplo.
La Figura 6 es un diagrama que ilustra una estructura de datos de política de PICNEEC de acuerdo con una realización de ejemplo.
La Figura 7 es un diagrama que ilustra tablas ilustrativas de acuerdo con una realización de ejemplo.
La Figura 8 es una captura de pantalla que ilustra una interfaz de usuario de acuerdo con una realización de ejemplo.
La Figura 9 es una captura de pantalla que ilustra una interfaz de usuario de acuerdo con otra realización de ejemplo.
La Figura 10 es un diagrama de interacción que ilustra un método, de acuerdo con una realización de ejemplo, del establecimiento y manejo de conexión de paquetes de datos en una red móvil.
La Figura 11 es un diagrama de flujo que ilustra un método, de acuerdo con una realización de ejemplo, del manejo de un paquete de datos saliente desde dentro de una red móvil hacia una red de IP externa.
La Figura 12 es un diagrama de flujo que ilustra un método, de acuerdo con otra realización de ejemplo, del manejo de un paquete de datos entrante desde una red de IP externa hacia la red móvil.
La Figura 13 es un diagrama de bloques que ilustra un sistema, de acuerdo con una realización de ejemplo, que incluye un SGSN/SGW y un GGSN/PGW independiente con un PICNEEC externo.
La Figura 14 es un diagrama de interacción que ilustra un método, de acuerdo con una realización de ejemplo, del manejo de paquetes de datos en una red móvil con un PICNEEC externo.
La Figura 15 es un diagrama de bloques, de acuerdo con otra realización de ejemplo, que ilustra un sistema que incluye múltiples SGSN/SGW y múltiples PICNEEC.
La Figura 16 es un diagrama de bloques que ilustra un sistema, de acuerdo con otra realización de ejemplo, que incluye múltiples SGSN/SGW y múltiples PICNEEC.
La Figura 17 es un diagrama de bloques que ilustra un sistema 1700 que incluye un PICNEEC 1702, de acuerdo con una realización de ejemplo.
La Figura 18 es un diagrama de bloques que ilustra una arquitectura de software representativa, que puede usarse en conjunto con diversas arquitecturas de hardware descritas en el presente documento.
La Figura 19 es un diagrama de bloques que ilustra componentes de una máquina, de acuerdo con algunas realizaciones de ejemplo, que pueden leer instrucciones de un medio legible por máquina (por ejemplo, un medio de almacenamiento legible por máquina) y realizar una cualquiera o más de las metodologías analizadas en el presente documento.

Descripción detallada

La descripción que sigue incluye sistemas, métodos, técnicas, secuencias de instrucciones y productos informáticos de programa de máquina ilustrativos que incorporan realizaciones ilustrativas. En la siguiente descripción, para propósitos de explicación, se exponen numerosos detalles específicos para proporcionar un entendimiento de diversas realizaciones de la materia objeto inventiva. Sin embargo, será evidente para los expertos en la materia, que las realizaciones de la materia objeto inventiva pueden ponerse en práctica sin estos detalles específicos. En general, no se han mostrado con detalle instancias, protocolos, estructuras y técnicas bien conocidos.

En una realización de ejemplo, se proporciona un sistema de encaminamiento en una red móvil que permite que un individuo o una organización definan políticas de encaminamiento y/o de seguridad para uno o más dispositivos móviles sin la intervención de un operador de red móvil.

La Figura 1 es un diagrama de bloques que ilustra un sistema 100, de acuerdo con una realización de ejemplo, para encaminar comunicaciones de red en unas redes móviles de GSM (2G) y/o UMTS (3G). El sistema 100 incluye uno o más dispositivos 102A-102D móviles. Cada dispositivo 102A-102D móvil puede ser cualquier tipo de dispositivo que tiene un comunicador de radio, comúnmente conocido como un transceptor celular. Los dispositivos 102A-102D móviles incluyen, por ejemplo, teléfonos inteligentes, ordenadores de tableta, automóviles conectados, sensores, sistemas de alarma, etc.

Cada dispositivo 102A-102D móvil se conecta a una red móvil mediante comunicaciones por radio. En la Figura 1, se representan dos tipos de redes móviles de ejemplo separadas. La primera es una red móvil basada en GSM. En redes móviles basadas en GSM, los dispositivos 102A, 102B móviles se conectan mediante comunicación por radio con una

estación transceptora base (BTS) 104A, 104B. Las BTS 104A, 104B son nodos de terminación para la interfaz de radio. Cada BTS 104A, 104B incluye uno o más transceptores y es responsable del cifrado de la interfaz de radio.

Cada BTS 104 está entonces en comunicación con un controlador de estación base (BSC) 106. Típicamente, un BSC 106 tiene cientos de BTS 104A, 104B bajo su control. El BSC 106 actúa para ubicar recursos de radio a los dispositivos 102A, 102B móviles, administra frecuencias y controla traspasos entre BTS. El BSC 106 puede actuar también como un concentrador, de modo que muchas conexiones de capacidad baja al BSC 106 quedan reducidas a un número menor de conexiones.

El segundo tipo de red móvil representada en este punto es una red móvil basada en el Sistema Universal de Telecomunicaciones Móviles UMTS. Una red móvil basada en UMTS usa tecnología de acceso por radio de acceso múltiple por división de código de banda ancha (W-CDMA). En este punto, los dispositivos 102C-102D móviles se conectan mediante comunicación por radio con un Nodo B 108A, 108B. Los Nodos B 108A, 108B son nodos de terminación para la interfaz de radio. Cada Nodo B 108A, 108B incluye uno o más transceptores y es responsable del cifrado de la interfaz de radio. Cada Nodo B 108A-108B está configurado para aplicar códigos para describir canales en una red de UMTS basada en CDMA. En general, cada Nodo B 108A-108B realiza funciones similares para la red de UMTS que las que realiza la BTS 104A-104B para la red de GSM.

Cada Nodo B 108A-108B está entonces en comunicación con un controlador de red de radio (RNC) 110. Típicamente, un RNC 110 tiene cientos de Nodos B 108A, 108B bajo su control. El RNC 110 actúa para ubicar recursos de radio a los dispositivos 102C, 102D móviles, administra frecuencias y controla traspasos entre los Nodos B 108A-108B. El RNC 110 puede actuar también como un concentrador, de modo que muchas conexiones de capacidad baja al RNC 110 quedan reducidas a un número menor de conexiones.

Debería observarse que, aunque se representan en este punto dos tipos de red móvil diferentes, los conceptos descritos en esta divulgación funcionarán en sistemas que tienen únicamente un único tipo de red, así como en sistemas que tienen múltiples tipos de red, además de o en lugar de los tipos de red representados en la Figura 1.

Las BTS 104A, 104B y/o los Nodos B 108A, 108B se conectan a un nodo de soporte de GPRS de servicio (SGSN) 112, que maneja todos los datos de conmutación de paquetes en la red. Existen en la actualidad dos formas de Nodos de Soporte de GPRS (GSN) en un sistema 100 típico. En este punto, es de relevancia el primer tipo: el SSGN, que típicamente es responsable de la entrega de paquetes de datos a y desde las BTS 104A, 104B y los Nodos B 108A, 108B en su área de servicio geográfica. Tareas adicionales pueden incluir el encaminamiento y la transferencia de paquetes, la gestión de movilidad (conexión/desconexión y gestión de movilidad), gestión de enlace lógico y funciones de cobro.

En algunas realizaciones de ejemplo, las funciones anteriormente descritas con respecto a un SGSN 112 se realizan por una pasarela de servicio (SGW), que por simplicidad no se representa en este punto. En algunas otras realizaciones de ejemplo, algún otro tipo de dispositivo puede realizar las funciones anteriormente descritas con respecto al SGSN 112. Todos estos tipos de dispositivos, incluyendo los SGSN 112 y las SGW, pueden denominarse de manera colectiva "agregadores" o "agregadores de paquetes".

Los paquetes de datos se envían aguas arriba desde un dispositivo 102A-102D móvil hacia una red de datos de conmutación de paquetes externa, tal como internet 114A o una red 114B privada. El SGSN 112 agrega los paquetes de datos de los dispositivos 102A-102D móviles y los envía a un nodo de soporte de GPRS de pasarela (GGSN) 116, que es el segundo tipo de GSN. El GGSN 116 es responsable de la interconexión en red entre la red de GPRS y las redes 114A, 114B de conmutación de paquetes externas. Desde un punto de vista de la red externa, el GGSN 116 es un encaminador a una subred, puesto que el GGSN 116 oculta la infraestructura de GPRS de la red externa. Cuando el GGSN 116 recibe datos direccionados a un usuario específico, comprueba si el usuario está activo. Si lo está, el GGSN 116 reenvía los datos al SGSN 112 que da servicio al usuario móvil. Si el usuario móvil está inactivo, se descartan los datos. El GGSN 116 es el punto de anclaje que posibilita la movilidad del terminal de usuario en la red de GPRS.

El GGSN 116 busca, para cada flujo de datos individual, el dispositivo 102 móvil para el que el flujo de datos es relevante en un directorio 118 de reglas y política. El directorio 118 de reglas y política contiene reglas para encaminamiento y/o seguridad. Por ejemplo, el directorio 118 de reglas y política puede indicar que un dispositivo móvil 102 particular debe tener encaminamiento de tráfico de datos en una dirección de red particular, o que debe usarse un protocolo de seguridad particular (por ejemplo, IPSec) para tráfico de datos a y/o desde ese dispositivo 102 móvil. El GGSN 116 a continuación actúa para implementar sean cual sean las políticas de encaminamiento al tráfico de datos.

El tráfico puede dirigirse, por ejemplo, hacia la red 114B privada mediante una Red Privada Virtual (VPN) 120. La VPN 120 se define y controla usando información en el directorio 118 de reglas y política.

Todo el tráfico (con o sin una VPN 120) se encamina a continuación a través de una pasarela 122 de seguridad, que actúa para emplear múltiples mecanismos de seguridad de red, tales como un cortafuegos, jardín vallado, IP en la lista

negra, etc. La pasarela 122 de seguridad usa información en el directorio 118 de reglas y política al establecer las reglas de seguridad, que pueden aprovisionarse en una base de dispositivo a dispositivo (o de grupo de dispositivos a grupo de dispositivos).

Por lo tanto, basándose en las reglas de encaminamiento y en las políticas de seguridad aplicadas, los paquetes de datos aguas arriba se envían hacia su destino en una red 114A, 114B de conmutación de paquetes externa.

Los paquetes aguas abajo se envían desde la red 114A, 114B de conmutación de paquetes externa a través de la pasarela 122 de seguridad, la VPN 120, el GGSN 116 y el SGSN 112 hasta el correspondiente dispositivo 102A-102D móvil.

La entidad que controla el dispositivo 102A-102D móvil (tal como un individuo u organización) puede configurar la pasarela 122 de seguridad, la VPN 120 y el GGSN 116 usando, por ejemplo, una consola externa u otro tipo de comunicación que permite la manipulación, configuración y monitorización de los elementos de red como si el individuo o la organización controlara tales elementos en la red interna.

Típicamente, los dispositivos 102 móviles están incorporados en una red móvil configurando un Nombre de Punto de Acceso (APN) para el dispositivo 102 móvil. Cada dispositivo 102 móvil tiene un APN único asignado para él. En una realización de ejemplo, el sistema 100 no tiene que utilizar información de APN para proporcionar políticas de encaminamiento o de seguridad para tráfico de datos a o desde un dispositivo 102 móvil. Cada grupo de dispositivos tiene asignada su propia instancia de "encaminador/cortafuegos" donde un cliente puede definir sus propios ajustes que incluyen, por ejemplo, la selección de perfiles de seguridad predefinidos (por ejemplo, coche conectado, sensor), la definición de jardines vallados, establecimientos de acceso de VPN, definición de reglas de cortafuegos y ubicaciones de dirección de IP basándose en la Identidad de Abonado Móvil de Internet (IMSI).

La Figura 2 es un diagrama de bloques que ilustra pilas de protocolo para servicios de subred de GPRS, de acuerdo con una realización de ejemplo. Se representa en este punto un dispositivo móvil (MS) 200, la estación base (BS) 202, el SGSN 204 y el GGSN 206. El GTP 208 es el protocolo usado entre el SGSN 204 y el GGSN 206 que usa la interfaz Gn. Este es un protocolo de tunelización de capa 3. El proceso que tiene lugar parece como una subred de IP normal para los usuarios dentro y fuera de la red. Una aplicación 210 se comunica mediante IP 212, que se lleva a través de la red de GPRS y sale del GGSN 206. Los paquetes que se mueven entre el GGSN 206 y el SGSN 204 usan GTP 208. De esta manera las direcciones de IP ubicadas en el lado externo del GPRS no tienen que tratar con la red troncal interna. En el SGSN 204, se ejecuta UDP 214 e IP 212 por GTP 208.

Se usa el Protocolo de Convergencia Dependiente de Subred (SNDCP) 216 y el Control de Enlace Lógico (LLC) 218 en combinación entre el SGSN 204 y el MS 200. SNDCP es la capa más superior de la pila de protocolo de GPRS del plano de usuario. El SNDCP 216 aplana los datos para reducir la carga en el canal de radio. El propósito principal de SNDCP 216 es almacenar en memoria intermedia y segmentar la unidad de datos de protocolo (PDU) de red, añadir encabezados a cada segmento, y, a continuación, proporcionar el segmento al LLC 218 para su transmisión. Se proporciona un enlace lógico seguro creado encriptando paquetes por LLC 218 y se usa el mismo enlace de LLC 218 siempre que un móvil esté bajo un único SGSN 204. SNDCP 216 también realiza compresión y descompresión. La idea es reducir la cantidad de datos que se requiere que se envíen en el transcurso de la comunicación. Como tal, el SNDCP 216 a menudo tiene conocimiento de ciertos detalles acerca del protocolo de red de datos de paquetes (PDN) para funciones relacionadas con la compresión. El SNDCP 216 puede tener también conocimiento de contextos de PDP y correspondiente información, tal como el tipo de PDP, QoS, etc. Esta información se proporciona durante unos procedimientos de activación de contexto PDP.

La función del LLC 218 es gestionar y garantizar la integridad de las transmisiones de datos. El LLC 218 proporciona enlaces de capa de enlace de datos a servicios para los protocolos de capa de red. Esto se consigue mediante puntos de acceso de servicio de LLC para los servicios que residen en ordenadores de red. Adicionalmente, hay un campo de control de LLC para la entrega de solicitudes o servicios. El LLC 218 puede realizar también cifrado y descifrado de paquetes.

La Figura 3 es un diagrama de bloques que ilustra un sistema 300 que incluye un SGSN/SGW 302 y un GGSN/Pasarela de PDN (PGW) 304. En una realización de ejemplo, el SGSN/SGW 302 puede ser el SGSN 112 de la Figura 1 y el GGSN/PGW 304 puede ser el GGSN 116 de la Figura 1. El SGSN/SGW 302 transfiere datos desde la red de radio móvil al GGSN/PGW 304 mediante un puerto de interfaz Gn. El Gn está comprendido de túneles del Protocolo de Tunelización de GPRS (GTP). GTP se divide en GTP-C, que controla los túneles y GTP-U, que es son los datos de tráfico de usuario reales.

Un sistema de cobro en línea (OCS) 306 se conecta al GGSN/PGW 304 mediante un punto de referencia Gy. El OCS 306 es un sistema de facturación que le indica al GGSN/PGW 304 si un cierto túnel tiene una cuota en el ancho de banda, y también permite o deja de permitir túneles basándose en el plan de servicio real y el saldo de cuenta para el usuario. El cobro en línea tiene dos subfunciones: calificación y determinación de unidad. Ambas de ellas, pueden implementarse centralizadas o descentralizadas.

La calificación se refiere al cálculo de una pieza de las unidades no monetarias calculadas por la función de determinación de unidad. La determinación de unidad hace referencia al cálculo del número de unidades no monetarias (unidades de servicio, volumen de datos, tiempo y eventos) que deben asignarse antes de empezar la entrega de servicio.

Pueden distinguirse tres casos para el cobro en línea: Cobro de Evento Inmediato (IEC), Cobro de Evento con Reserva de Unidad (ECUR) y Cobro de Sesión con Reserva de Unidad (SCUR).

IEC implica una operación de débito directa, donde se debita inmediatamente una cuenta financiera para una facturación apropiada. En ECUR, las unidades financieras se reservan antes de la entrega de servicio, y se lleva a cabo una operación de débito de cuenta financiera después de la conclusión de la entrega de servicio. En SCUR, las unidades financieras se reservan antes de la supervisión de sesión, y se lleva a cabo una operación de débito de cuenta financiera siguiendo la conclusión de la terminación de la sesión.

Un sistema de cobro fuera de línea (OFCS) 308 se conecta al GGSN/PGW 304 mediante el punto de referencia Gz. El OFCS 308 es un sistema de facturación para el procesamiento de registro detallado de llamada (CDR) post pago. La facturación fuera de línea es un proceso donde se recopila la información de cobro por el uso de recursos de red concurrentemente con ese uso de recursos. La información de cobro se pasa a continuación a través de una cadena de funciones de facturación lógicas. Al final de este proceso, se generan ficheros de CDR por la red, que a continuación se transfieren al dominio de la facturación del operador de red para el propósito de la facturación de abonado y/o la contabilidad del interoperador (o funciones adicionales tales como estadísticas). El dominio de facturación típicamente incluye sistemas de post-procesamiento tales como el sistema de facturación o el dispositivo de mediación de facturación del operador.

Ejemplos de funciones de cobro fuera de línea incluyen la función de activador de cobro (CTF), la función de datos de cobro (CDF) y la función de pasarela de cobro (CGF). La CTF genera eventos de cobro basándose en la observación de uso de recursos de red. La CTF es el punto focal para recopilar la información que pertenece a eventos cobrables dentro del elemento de red, ensamblar esta información en eventos de cobro coincidentes y enviar estos eventos de cobro hacia la CDF. La CTF está compuesta de dos bloques funcionales: colección de métricas de contabilidad, que monitoriza funciones de señalización para eventos de servicio de llamadas o sesiones establecidas por los usuarios de red, o el manejo de tráfico de usuario para estas llamadas, eventos de servicio o sesiones, o la entrega de servicio al usuario mediante estas llamadas, eventos de servicio o sesiones, y reenvío de datos de contabilidad, que recibe las métricas de contabilidad recopiladas y determina la aparición de eventos que pueden cobrarse de un conjunto de una o más de las métricas y, a continuación, ensambla eventos de cobro que coinciden con los eventos que pueden cobrarse detectados, y reenvía los eventos de cobro hacia la Función de Datos de Cobro mediante una interfaz Rf.

La CDF recibe eventos de cobro desde la CTF mediante el punto de referencia Rf. A continuación, usa la información contenida en los eventos de cobro para construir los CDR. Los CDR producidos por la CDF se transfieren inmediatamente a la Función de Pasarela de Cobro (CGF) mediante el punto de interfaz Ga. La CGF realiza funciones tales como la recepción de CDR desde la CDF mediante la interfaz Ga casi en tiempo real, preprocesamiento de CDR, validación, consolidación y (re)formateo de CDR, manejo de error de CDR, almacenamiento de CDR persistente, encaminamiento y filtración de CDR, gestión de fichero de CDR y transferencia de fichero de CDR al dominio de la facturación

La red 310 de datos de paquetes se conecta al GGSN/PGW 304 mediante el punto de referencia Gi. La red 310 de datos de paquetes es una red de datos pública o privada a la que los dispositivos móviles pueden enviar datos. Una función de reglas de política y cobro (PCRF) 312 se conecta al GGSN/PGW 304 mediante el punto de referencia Gx, que es parte de un método para aplicar políticas de flujo de datos en el GGSN/PGW 304. La PCRF 312 se encarga de la recogida de las reglas y de pasarlas al GGSN/PGW 304. La PCRF 312 proporciona control de red con respecto a la detección de flujo de datos de servicio, sincronización de puertas (bloquear o permitir paquetes), control de QoS y el cobro basado en pequeña cantidad. Por ejemplo, la PCRF 312 puede rechazar una solicitud recibida de una aplicación cuando la información de servicio no es consistente con la información de suscripción.

La PCRF 312 se conecta a un repositorio de perfiles de suscripción (SPR) 314 mediante el punto de referencia Sp. El SPR 314 contiene información de abonado y de suscripción, típicamente almacenada en una base por PDN, e incluiría información tal como los servicios permitidos del abonado, información sobre la QoS permitida del abonado, la información relacionada con el cobro del abonado y una categoría de abonado. La PCRF 312 puede acceder al SPR 314 para consultar perfiles para cada usuario relevante. Una función de aplicación (AF) 316 se conecta a la PCRF 312 mediante el punto de referencia Rx y permite a la lógica de aplicación externa cambiar las reglas de PCRF.

El GGSN/PGW 304 usa una función de reglas de aplicación de política (PCEF) 318 para aplicar las reglas realizadas por la PCRF 312. Aunque el GGSN/PGW 304 permite funcionalidad de encaminamiento básico, así como el establecimiento de VPN, traducción de dirección de red (NAT) y cortafuegos básico, todos estos servicios están basados en la configuración del operador de red, y ninguna de esta funcionalidad se exporta para que se modifique por las portadoras reales del servicio (dispositivos móviles y sus propietarios, así como corporaciones u otras organizaciones que emplean los propietarios, colectivamente conocidos como clientes). También son dirigidos hacia

la conexión de elementos de red internos y externos y no al tráfico de paquetes específico de los dispositivos móviles. La PCRF 312 también aplica reglas de seguridad usando una lista negra (por ejemplo, lista de dispositivos móviles, ubicaciones de red, tipos de tráfico, etc. prohibidos).

En una realización de ejemplo, el sistema 300 de la Figura 3 está modificado para permitir funcionalidad adicional. Esta funcionalidad puede nombrarse, en general, Posibilitador y Controlador de Perímetro de Red Personalizado Integrado de PDN (PICNEEC) del que un GGSN o una PGW son solamente dos componentes de ejemplo. La Figura 4 es un diagrama de bloques que ilustra un sistema 400 que incluye un SGSN o SGW 402 y un PICNEEC 404. En una realización de ejemplo, el SGSN/SGW 402 puede ser el SGSN 112 de la Figura 1 y el GGSN/PGW 418 puede ser el GGSN 116 de la Figura 1. El SGSN/SGW 402 transfiere datos desde la red de radio móvil al GGSN/PGW 418 mediante un puerto de interfaz Gn. El PICNEEC 404 incluye un Aplicador de Reglas Personalizado Virtual (VCRE) 406, que se asienta en el punto de referencia Gi. Puede ser interno al PICNEEC 404 o como un componente de extensión a un PICNEEC 404 existente. El VCRE 406 define el encaminamiento, cortafuegos, VPN y características de seguridad para el sistema 400. Un Componente de Reglas de Política y Cobro, tal como una función de reglas de política y cobro (PCRF) 408 ejecuta unas reglas de política y cobro generales en el GGSN/PGW 418.

Una Función de Personalizador de Reglas (RCF) 410 es un repositorio externo y controla la función que transfiere todos los cambios y configuraciones de política y seguridad al VCRE 406. La RCF 410 puede conectarse también a la PVRF 408 usando una interfaz Rx, ya que es un componente 412 de aplicación, tal como una función de aplicación. Se usa una consola 414 de RCF por un cliente para establecer las políticas de encaminamiento y seguridad. La consola 414 de RCF puede ser, por ejemplo, un portal web, un acceso de Interfaz de Comandos Seguro (SSH), una interfaz de Lenguaje Hombre-Máquina (MML), etc.

Una aplicación 416 de RCF proporciona un acceso de interfaz de programa de aplicación (API) a la RCF 410, desde, por ejemplo, una aplicación externa, aplicación en un dispositivo móvil, etc.

El cliente puede usar la consola 414 de RCF o la aplicación 416 de RCF para definir un VCRE y especificar diversas reglas, que incluyen, pero sin limitación, definir una VPN entre el VCRE y una red externa, definir encaminamiento de red entre el VCRE y redes de conectividad de IP, definir reglas de cortafuegos para tráfico de datos de paquetes que pasa a través de la instancia de VCRE, definir reglas de NAT para tráfico de datos de paquetes que pasa a través de la instancia de VCRE, definir ajustes de sistema de nombre de dominios (DNS) para tráfico de datos de paquetes que pasa a través de la instancia de VCRE, definir reglas de seguridad para tráfico de datos de paquetes que pasa a través de la instancia de VCRE, asignar direcciones de IP a dispositivos móviles, y definir unas reglas de Enriquecimiento de Encabezado (HHE) de Protocolo de Transferencia de Hipertexto (HTTP) para paso de tráfico a través de la instancia de VCRE.

HHE significa que cuando el dispositivo móvil crea una solicitud de HTTP hacia un servidor de HTTP, el tráfico pasa a través de un intermediario de HTTP (normalmente el propio GGSN/PGW) que añade información a los encabezados de HTTP que permite que el servidor de HTTP identifique desde dónde provino la solicitud. Tal información puede incluir un MSISDN (el número de teléfono del dispositivo móvil) o un IMSI.

La Figura 5 es un diagrama de bloques que ilustra en más detalle un VCRE 500, tal como el VCRE 406 de la Figura 4, de acuerdo con una realización de ejemplo. El VCRE 500 se divide en múltiples instancias 502A-502N virtuales de un cortafuegos/encaminador/VPN/aplicador de seguridad. Cada conjunto de dispositivos móviles o incluso un único dispositivo móvil se maneja por una única instancia 502A-502N de VCRE. Para cada instancia, pueden definirse múltiples reglas. Por ejemplo, la instancia 502A de VCRE corresponde al grupo 504A de dispositivos, que contiene tres dispositivos. La instancia 502A de VCRE indica que las conexiones pueden establecerse únicamente en una empresa 506 mediante una VPN 508. La instancia 502B de VCRE corresponde a un grupo 504B de dispositivos, que contiene dos dispositivos. La instancia 502B de VCRE indica que pueden realizarse las conexiones en la empresa 506 mediante una VPN 510 o que pueden conectarse a Internet 512. La instancia 502C de VCRE corresponde al grupo 504C de dispositivos, que únicamente contiene un único dispositivo. La instancia 502C de VCRE indica que pueden realizarse conexiones a una nube 514 privada, no mediante una VPN, sino mediante un jardín vallado (donde las direcciones de IP a las que está permitido a acceder un dispositivo están limitadas).

El VCRE 500 puede incluir adicionalmente un bloque 516 de control, que actúa para realizar funciones que están implicadas, en general, entre todas las instancias 502A-502N de VCRE. Estas funciones incluyen, por ejemplo, el establecimiento de las instancias de VCRE, la asignación de dispositivos móviles específicos a instancias 502A-502N de VCRE y el borrado de instancias 502A-502N de VCRE. Adicionalmente, como se observará en más detalle a continuación, en el caso de que el VCRE 500 sea externo a un GGSN, el bloque 516 de control de VCRE informa al GGSN de la dirección de IP para el dispositivo móvil y reenvía todo el tráfico desde esa dirección de IP a la instancia 502A-502N de VCRE correcta.

Cada instancia 502A-502N de VCRE puede contener una estructura de datos de VCRE que almacena la información que necesita para el encaminamiento y las reglas de seguridad.

Cada instancia 502A-502N de VCRE se controla independientemente entre sí mediante el acceso directo de la instancia 502A-502N de VCRE por un cliente diferente del proveedor de red móvil (la entidad controlada por el PICNEEC).

La Figura 6 es un diagrama que ilustra la estructura 600 de datos de política de VCRE de acuerdo con una realización de ejemplo. Cada estructura 600 de datos de política de VCRE puede incluir un componente 602 de política con un campo de nombre donde puede especificarse un nombre para la política. Fijado a este componente 602 de política se encuentra un componente 604 de reglas de NAT, un componente 606 de reglas de cortafuegos, un componente 608 de reglas de IP, un componente 610 de jardín vallado y un componente 612 de VPN. Debería observarse que, no todas las estructuras de datos de VRCE necesitan tener todos estos componentes 604-612. El cliente puede escoger y elegir cuáles de estos componentes 604-612 incluir basándose en las necesidades de la política. Por ejemplo, si una política particular usa un jardín vallado pero no VPN, el componente 610 de jardín vallado puede incluirse, pero excluirse el componente 612 de VPN.

El componente 604 de reglas de NAT puede contener campos tales como la dirección de origen, dirección de destino, protocolo, puerto, dirección para y puerto para. El componente 606 de reglas de cortafuegos puede contener campos tales como dirección de destino, dirección de origen, protocolo, puerto y acción. El componente 608 de reglas de IP puede contener campos tales como la dirección y pasarela de destino. El componente 610 de jardín vallado puede incluir campos tales como la dirección de destino de ubicaciones permitidas para acceder. El componente 612 de VPN puede contener campos tales como la dirección de destino, dirección de origen y una clave compartida previa.

Un componente 602 de política puede incluir subcomponentes adicionales, tales como reglas de filtro, reglas de encaminamiento, reglas de rastreo de paquetes, reglas de inspección de paquetes profunda (DPI), reglas de equilibrado de carga y otros componentes que se emplean en redes basadas en IP modernas.

La Figura 7 es un diagrama que ilustra tablas ilustrativas de acuerdo con una realización de ejemplo. Una tabla 700 de usuario puede contener una lista de nombres 702A, 702B de usuario. Los nombres 702A, 702B de usuario pueden utilizarse en las otras tablas 704-710. Una tabla 704 de perfil contiene una columna para nombres 712 de usuario y una columna para correspondientes perfiles 714 asociados con cada nombre 702A, 702B de usuario. Por lo tanto, en este punto, por ejemplo, cada nombre 702A, 702B de usuario tiene dos posibles perfiles. Por ejemplo, Cars Co. 702A puede tener un perfil de N.A. Perfil de Flota (Perfil de Flota de América del Norte) o Perfil de Flota S.A. (Perfil de Flota de América del Sur). Una tabla 706 de dispositivos contiene una indicación de un nombre 716 de dispositivo individual, el IMSI 718 de los correspondientes dispositivos, el nombre de usuario asociado con el dispositivo 720, y el perfil asociado con el dispositivo 722. Como puede observarse, puede haber múltiples dispositivos asociados con cada usuario, y cada dispositivo individual puede tener un perfil diferente.

Una tabla 708 de reglas proporciona una serie de reglas asociadas con cada perfil 724 de seguridad. Por ejemplo, puede definirse un tipo 726 de regla, acción 728, protocolo 730, dirección 732 de IP de origen, dirección 734 de IP de destino, puerto 736 y orden 738 para cada regla. Por supuesto, estos son únicamente ejemplos de los diversos diferentes tipos de reglas que pueden definirse.

Una tabla 710 de jardín vallado proporciona una serie de direcciones 740 de IP a las que un correspondiente perfil 742 permite acceso, mientras que se prohíben todas las otras direcciones.

La Figura 8 es una captura de pantalla que ilustra una interfaz 800 de usuario de acuerdo con una realización de ejemplo. La interfaz 800 de usuario puede proporcionarse como parte de una consola 414 de RCF y/o aplicación 416 de RCF, como se ha descrito anteriormente. La interfaz 800 de usuario permite a un usuario, tal como a un administrador de una empresa, crear una o más reglas y asociar estas reglas con grupos de dispositivos de seguridad. Cuando se selecciona, la pestaña 802 permite que el usuario edite, borre o añada políticas de comunicación de entrada (por ejemplo, políticas para comunicaciones que se envían desde una red 512, 514 de datos de paquetes a un dispositivo). Cuando se selecciona, la pestaña 804 permite que el usuario edite, borre o añada políticas de comunicación de salida (por ejemplo, políticas para comunicaciones que se envían desde un dispositivo a una red 512, 514 de datos de paquetes. Cuando se selecciona, la pestaña 806 permite que el usuario añada o borre miembros de grupo (por ejemplo, dispositivos que son parte de este grupo de seguridad). Adicionalmente, el botón 808 permite que el usuario añada un nuevo puerto de servicio.

La Figura 9 es una captura de pantalla que ilustra una interfaz 900 de usuario de acuerdo con otra realización de ejemplo. La interfaz 900 de usuario puede presentarse cuando el usuario selecciona el botón 808 de la interfaz 800 de usuario de la Figura 8. En este punto, puede asignarse al puerto un nombre 902, descripción 904, tipo 906 de servicio, protocolo 908, número 910 de puerto, rango 912 y comportamiento 914 de puerto.

La Figura 10 es un diagrama de interacción que ilustra un método 1000, de acuerdo con una realización de ejemplo, de manejo de paquetes de datos en una red móvil. El método 1000 puede utilizar un conjunto móvil (MS) 1002, un SGSN/SGW 1004, un PICNEEC 1001 con un GGSN/PGW 1006 interno, un VCRE 1008, una RCF 1010 y una instancia 1012 de VCRE que se conecta a una red de datos de paquetes (PDN) 1014. El MS 1002 puede ser la agrupación de dispositivos móviles que es el objeto de las reglas de seguridad y/o cortafuegos descritas en el presente documento.

En la operación 1016, el MS 1002 intenta registrarse en la red y autenticarse a sí mismo mediante el SGSN/SGW 1004. Esto se llama crear un contexto de protocolo de datos de paquetes (PDP). El contexto de PDP es una estructura de datos que estará presente tanto en el SGSN/SGW 1004 como en el GGSN/PGW 1006 para contener la información de sesión del abonado cuando el abonado tiene una sesión activa. Cuando un dispositivo móvil desea usar un GPRS, en primer lugar, conecta y, a continuación, activa el contexto de PDP. Esto asigna una estructura de datos de contexto de PDP en el SGSN/SGW 1004 que está visitando actualmente el abonado y el GGSN/PGW 1006 que da servicio al punto de acceso del abonado. La información capturada puede incluir la dirección de IP del abonado, la Identidad de Abonado Móvil Internacional (IMSI) de los abonados, y los ID de punto terminal del túnel en el GGSN/PGW 1006 y/o el SGSN/SGW 1004.

En la operación 1018, el SGSN/SGW 1004 a continuación solicita al GGSN/PGW 1006 que cree el contexto de PDP. En la operación 1020, el GGSN/PGW 1006 pide al VCRE 1008 que asigne una instancia 1012 de VCRE para el MS 1002. En la operación 1022, el VCRE 1008 solicita un perfil que corresponde al MS 1002 desde la RCF 1010, que lo devuelve en la operación 1024. En la operación 1026, el VCRE 1008 asigna el perfil a la instancia 1012 de VCRE. En la operación 1028, el GGSN/PGW 1006 crea una respuesta de PDP y la envía al SGSN/SGW 1004, que, en la operación 1030, activa una respuesta de PDP al MS 1002.

En esta etapa, el tráfico de GTP puede pasar desde el MS 1002 a través del SGSN/SGW 1004 y al GGSN/PGW 1006. Esto se representa en las operaciones 1032 y 1034. En la operación 1036, el GGSN/PGW 1006 desencapsula los túneles de GTP y pasa el tráfico de IP hacia la instancia 1012 de VCRE. La instancia 1012 de VCRE aplica la política tanto en el tráfico saliente 1038 como en el entrante 1040.

En realidad, el protocolo de GTP se descompone en una sección de control, conocida como GTP-C, y un protocolo de tunelización basado en IP conocido como GTP-U, y, por lo tanto, en esta etapa, el tráfico de IP puede formatearse realmente de acuerdo con el protocolo de GTP-U. Se identifican túneles separados por un identificador de punto terminal de túnel (TEID) en los mensajes de GTP-U, que puede ser un número aleatorio asignado dinámicamente. Si el número aleatorio es de calidad criptográfica, entonces proporciona una medida de seguridad contra ciertos tipos de ataques.

La Figura 11 es un diagrama de flujo que ilustra un método 1100, de acuerdo con una realización de ejemplo, de manejo de un paquete de datos de entrada en una red móvil. Esta figura representa el manejo de un paquete "aguas arriba", en concreto, un paquete enviado desde un dispositivo móvil en la red móvil a una red basada en paquetes. En una realización de ejemplo, este método 1100 puede realizarse por un PICNEEC, o similares. En la operación 1102, se recibe un paquete de datos desde un dispositivo móvil. Este paquete de datos puede generarse por, por ejemplo, una aplicación que se ejecuta en el dispositivo móvil. En la operación 1104, una Función de Ejecución de Política y Cobro (PCEF) realiza la aplicación de este paquete de datos. Esta aplicación de PCEF incluye la aplicación de decisiones de política tales como la Calidad de Servicio (QoS) y el cobro en línea y fuera de línea. En la operación 1106, el VCRE decide si el paquete está bajo una regla de cortafuegos. Esto se determina examinando, por ejemplo, la política en la instancia de VCRE que corresponde al dispositivo móvil. En caso afirmativo, a continuación, en la operación 1108, se realiza la aplicación de cortafuegos previa al encaminamiento usando la política. En una realización de ejemplo, la aplicación de cortafuegos previa al encaminamiento incluye marcar paquetes particulares. Por ejemplo, puede ser deseable hacer que se envíe tráfico de HTTP normal mediante un tráfico de VPN y HTTP a un sitio web específico mediante otra VPN. Las reglas de aplicación de cortafuegos previas al encaminamiento pueden actuar para marcar los paquetes de acuerdo con las reglas. En la operación 1110, se realiza encaminamiento. Esto puede incluir, por ejemplo, encaminar paquetes de acuerdo con la manera en que se marcaron durante la aplicación de cortafuegos previa al encaminamiento. En la operación 1112, se determina si el paquete se asienta detrás de NAT. Esto se determina examinando, por ejemplo, la política en la instancia de VCRE que corresponde al dispositivo móvil. En caso afirmativo, a continuación, en la operación 1114, se aplica SAT de origen (con posibles reglas de NAT) en el paquete usando la política.

En la operación 1116, se determina si se aplica un cortafuegos después de la decisión de NAT y encaminamiento. Esto se determina examinando, por ejemplo, la política en la instancia de VCRE que corresponde al dispositivo móvil. En caso afirmativo, a continuación, en la operación 1118, se realiza aplicación de cortafuegos posterior al encaminamiento usando la política. En una realización de ejemplo, la aplicación de cortafuegos posterior al encaminamiento puede incluir reglas que modifican características de paquete, tales como tamaño de paquete y encabezados de paquete, después de que se haya completado el proceso de encaminamiento. En la operación 1120, se determina si se usa una política de seguridad como la encriptación de IPSEC. Esto se determina examinando, por ejemplo, la política en la instancia de VCRE que corresponde al dispositivo móvil. En caso afirmativo, a continuación, en la operación 1122, se realiza encriptación o alguna otra técnica de seguridad. En la operación 1124, se envía el paquete final a la red basada en paquetes exterior.

La Figura 12 es un diagrama de flujo que ilustra un método 1200, de acuerdo con otra realización de ejemplo, de manejo de un paquete de datos de entrada en una red móvil. Esta figura representa el manejo de un paquete "aguas abajo", en concreto un paquete enviado desde una red basada en paquetes a un dispositivo móvil en la red móvil. En una realización de ejemplo, este método 1200 puede realizarse por un PICNEEC, o similares. En la operación 1202,

se recibe un paquete de datos desde una red basada en paquetes. En la operación 1204, se usa una dirección de destino del paquete de datos para recuperar una instancia de VCRE basada en la dirección. Por ejemplo, la dirección de destino puede ser una dirección de Protocolo de Internet (IP) y la instancia de VCRE puede tener una dirección de IP, lista de direcciones de IP, o intervalo de direcciones de IP como un campo que puede buscarse para recuperar la política.

En la operación 1206, se determina si la política indica que se usa la NAT para la dirección de IP. En caso afirmativo, a continuación, en la operación 1208, puede aplicarse una política de NAT a la dirección de IP para mantener una sesión en el paquete aguas abajo basándose en la dirección de IP con NAT aplicada.

En la operación 1210, se determina si se define una política de cortafuegos para la dirección de IP. En caso afirmativo, a continuación, en la operación 1212, pueden ejecutarse reglas de encaminamiento previo. En una realización de ejemplo, esto puede incluir reglas para ayudar a bloquear ataques de denegación de servicio distribuidos (DDOS). El tráfico de direcciones de IP particulares puede marcarse de acuerdo con las reglas de cortafuegos previas al encaminamiento, así como añadirse a una lista negra si supera un umbral.

En la operación 1214, el paquete de datos se encamina de acuerdo con una política de encaminamiento. En la operación 1216, se determina si se usa una política de seguridad como la encriptación de IPSEC. Esto se determina examinando, por ejemplo, la política en la instancia de VCRE que corresponde a la dirección de IP. En caso afirmativo, a continuación, en la operación 1218, se realiza desencriptación o alguna otra técnica de seguridad.

En la operación 1220, se determina si se define una política de cortafuegos para la dirección de IP. En caso afirmativo, a continuación, en la operación 1222, pueden ejecutarse reglas de encaminamiento posterior. En la operación 1224, una PCEF puede realizar la aplicación en el paquete de datos. En la operación 1226, se envía el paquete final al dispositivo de usuario que corresponde a la dirección de IP.

En otra realización de ejemplo, un PICNEEC está ubicado de manera externa al GGSN/PGW. La Figura 13 es un diagrama de bloques que ilustra un sistema 1300, de acuerdo con una realización de ejemplo, que incluye un SGSN/SGW 1302 y un GGSN/PGW 1304. En una realización de ejemplo, el SGSN/SGW 1302 puede ser el SGSN 110 de la Figura 1 y el GGSN/PGW 1304 puede ser el GGSN 114 de la Figura 1. El SGSN/SGW 1302 transfiere datos desde la red de radio móvil al GGSN/PGW 1304 mediante un puerto de interfaz Gn. El GGSN/PGW 1304 se comunica mediante un puerto Gi a un PICNEEC 1306 externo, que se asienta en el punto de referencia Gi. El VCRE 1318 dentro del PICNEEC 1306 define las características de encaminamiento, cortafuegos, VPN y seguridad para el sistema 1300. Una Función de Ejecución de Reglas de Política y Cobro (PREF) 1308 ejecuta reglas de política y cobro generales.

Una Función de Personalizador de Reglas (RCF) 1310 actúa como un repositorio externo y controla la función que transfiere todos los cambios y configuraciones de política y seguridad al VCRE 1318. La RCF 1310 puede conectarse también a la PCRF 1308 usando una interfaz Rx, ya que es una Función 1312 de Aplicación. Se usa una consola 1314 de RCF por un cliente para establecer las políticas de cortafuegos y seguridad. La consola 1314 de RCF puede ser, por ejemplo, un portal web, un acceso de Interfaz de Comandos Seguro (SSH), una interfaz de Lenguaje Hombre-Máquina (MML), etc.

Una aplicación 1316 de RCF proporciona un acceso de interfaz de programa de aplicación (API) a la RCF 1310, desde, por ejemplo, una aplicación externa, aplicación en un dispositivo móvil, etc.

Debería observarse que, aunque la descripción anterior analiza mecanismos para que el PICNEEC 1306 se conecte a redes de 3G/4G, en algunas realizaciones de ejemplo, el PICNEEC 1306 también puede conectarse simultáneamente a Redes de Área Extensa de Baja Energía (LPWAN), tales como LoRa y SIGFOX.

La Figura 14 es un diagrama de interacción que ilustra un método 1400, de acuerdo con una realización de ejemplo, de manejo de paquetes de datos en una red móvil con un PICNEEC externo. El método 1400 puede utilizar un conjunto móvil (MS) 1402, un SGSN/SGW 1404, un GGSN/PGW 1406, un PICNEEC 1401 externo con un VCRE 1408, una RCF 1410, una instancia 1412 de VCRE que se conecta a una red de datos de paquetes (PDN) 1414. El MS 1402 puede ser la agrupación de dispositivos móviles que es el objeto de las reglas de seguridad y/o cortafuegos descritas en el presente documento.

En la operación 1416, el MS 1402 intenta registrarse en la red y autenticarse a sí mismo mediante el SGSN/SGW 1404. Esto se llama crear un contexto de protocolo de datos de paquetes (PDP). En la operación 1418, el SGSN/SGW 1404 a continuación solicita que el GGSN/PGW 1406 cree el contexto de PDP. En la operación 1420, el GGSN/PGW 1406 pide que el PICNEEC 1408 externo asigne una dirección de IP para un contexto de PDP. Esto puede realizarse usando protocolos tales como DHCP o RADIUS. En la operación 1422, el VCRE 1408 de PICNEEC solicita un perfil que corresponde al MS 1402 desde la RCF 1410, que lo devuelve en la operación 1424. En la operación 1426, el VCRE 1408 de PICNEEC asigna el contexto de PDP de la dirección de IP lo devuelve. En la operación 1428, el GGSN/PGW 1406 crea una respuesta de PDP y la envía al SGSN/SGW 1404, que, en la operación 1430, activa una respuesta de PDP al MS 1402.

En esta etapa, el tráfico de GTP puede pasar desde el MS 1402 a través del SGSN/SGW 1404 y al GGSN/PGW 1406. Esto se representa en las operaciones 1432 y 1434. En la operación 1436, el GGSN/PGW 1406 desencapsula los túneles de GTP y para el tráfico de IP hacia el VCRE 1408 de PICNEEC externo, que, a continuación, encamina el tráfico de IP en la operación 1438 a la instancia 1412 de VCRE apropiada basándose en la dirección de origen del tráfico. La instancia 1412 de VCRE aplica la política tanto en el tráfico saliente 1440 como en el entrante 1442. El resultado es que el tráfico de IP desde la PDN se encamina desde la instancia 1442 de VCRE al VCRE 1408 de PICNEEC externo, que adquiere el conocimiento basándose en la dirección de origen para encaminar el tráfico de vuelta al GGSN/PGW 1406.

En ciertos casos, un grupo de dispositivos particular puede contener dispositivos que operan en diferentes redes celulares que posiblemente usan diferentes formatos entre sí. Por ejemplo, haciendo referencia de vuelta a la Figura 5, el grupo 504A de dispositivos puede contener un dispositivo que opera en una red de GSM y otro dispositivo que opera en una red de CDMA. Esto puede ocurrir en un caso donde, por ejemplo, una empresa permita a sus empleados usar sus dispositivos celulares personales para uso laboral, y un empleado puede tener un dispositivo compatible con una red diferente a otra (por ejemplo, de un proveedor de servicio celular diferente). Otro ejemplo sería el uso de tecnología de IP Móvil de Intermediario (PMIP) que permite itinerancia de IP entre tecnologías de red. El resultado neto es que una instancia de VCRE ubicada en un PICNEEC puede no ser alcanzable, al menos no directamente, desde un dispositivo que se conecte a un PICNEEC diferente. En el caso de un dispositivo que opere en una red de GSM y otro dispositivo que opere en una red Wi-Fi, el dispositivo que opera en la red de GSM puede tener su tráfico encaminado a través de un PICNEEC mientras que el dispositivo que opera en la red Wi-Fi puede tener su tráfico encaminado a través de una Pasarela de Acceso Móvil (MAG). Hay varias posibilidades sobre cómo manejar tales casos.

En una primera realización de ejemplo, el cliente simplemente crea las mismas reglas/políticas para el grupo de dispositivos en múltiples diferentes PICNEEC. Esto se realiza utilizando el cliente una consola de RCF o aplicación de RCF separada para cada uno de los múltiples PICNEEC. Por supuesto, esta puede no ser una solución deseable puesto que fuerza al cliente a realizar trabajo adicional y también conlleva el riesgo de que al repetir la creación de las reglas/políticas, el cliente puede cometer un error y provocar de manera inadvertida que las reglas/políticas en una instancia de VCRE para el grupo de dispositivos en un PICNEEC sean diferentes que la correspondiente instancia de VCRE para el grupo de dispositivos en otro PICNEEC, y, por lo tanto, provocar que se apliquen diferentes reglas/políticas a dispositivos que deben tener reglas/políticas idénticas.

En una segunda realización de ejemplo, se realiza replicación en los PICNEEC de modo que cuando se crea una instancia de VCRE o se modifica en un PICNEEC la instancia de VCRE se replica en los otros correspondientes PICNEEC. La Figura 15 es un diagrama de bloques, de acuerdo con otra realización de ejemplo, que ilustra un sistema 1500 que incluye múltiples SGSN/SGW 1502A, 1502B, 1502C y múltiples PICNEEC 1504A, 1504B, 1504C. Cada PICNEEC 1504A-1504C puede mantener una función de reglas de VCRE local (L-VCRE) 1506A-1506C que gestiona las instancias de VCRE asignadas al correspondiente PICNEEC 1504A-1504C. Un servicio 1512A-1512C de replicación en cada PICNEEC 1504A-1504C hace que se replique el L-VCRE 1506A-1506C entre los PICNEEC 1504A-1504C, manteniendo por lo tanto instancias de VCRE consistentes entre los PICNEEC 1504A-1504C. Por lo tanto, incluso aunque un cliente pueda crear o modificar reglas y políticas para un grupo de dispositivos usando uno de cualquier número de diferentes consolas 1508A-1508C de RCF y aplicaciones 1510A-1510C de RCF, las instancias de VCRE son constantes como si el cliente repitiera la creación o modificación de las reglas y políticas exactamente de la misma manera en cada una de las consolas 1508A-1508C de RCF o aplicaciones 1510A-1510C de RCF diferentes.

En una tercera realización de ejemplo se proporciona una Función Personalizadora de Reglas central (C-RCF) que actúa como un único punto de interfaz para que el cliente establezca o modifique reglas/políticas para un grupo de dispositivos y la C-RCF distribuye las reglas/políticas a múltiples funciones de reglas de VCRE locales. La Figura 16 es un diagrama de bloques que ilustra un sistema 1600, de acuerdo con otra realización de ejemplo, que incluye múltiples SGSN/SGW 1602A, 1602B, 1602C y múltiples PICNEEC 1604A, 1604B, 1604C. Cada PICNEEC 1604A-1604C puede mantener una función de reglas de VCRE local (L-VCRE) 1606A-1606C que gestiona las instancias de VCRE asignadas al correspondiente PICNEEC 1604A-1604C. Una Función Personalizadora de Reglas central (C-RCF) 1608 actúa como un único punto de interfaz para la consola 1610 de RCF y la aplicación 1612 de RCF y actúa para distribuir cualquier regla/política establecida mediante la consola 1610 de RCF y la aplicación 1612 de RCF a todas las funciones 1606A-1606C de reglas de VCRE locales, estableciendo por lo tanto consistencia entre ellas.

Otro escenario posible es que un dispositivo conmute de un tipo de red a otro, siendo servidas ambas redes por un único PICNEEC. Aunque esto no requiere ninguna replicación de instancias de VCRE entre múltiples PICNEEC, en una realización de ejemplo, se restablece el contexto de PDP cuando se cambia la red. Por lo tanto, en el caso de una ocurrencia de este tipo, el PICNEEC puede reasignar la instancia de VCRE correcta cuando se restablece el contexto de PDP.

Debería observarse que, aunque la divulgación anterior describe aspectos relacionados con un GGSN y/o PGW, pueden aplicarse las mismas técnicas y componentes a cualquier pasarela de interconexión en red que recibe comunicaciones transmitidas a través de una red de radio móvil. GGSN es una realización usada principalmente en

redes de 3G mientras que PGW es una realización usada principalmente en redes de 4G, pero hay otras tecnologías de radio, tales como CDMA, WI MAX, LoRa y SIGFOX, así como tecnologías de radio no creadas aún que pueden utilizar una pasarela de interconexión en red de acuerdo con la presente divulgación.

La Figura 17 es un diagrama de bloques que ilustra un sistema 1700 que incluye un PICNEEC 1702, de acuerdo con una realización de ejemplo. El PICNEEC 1702 es compatible con cualquier número de diferentes tipos de pasarelas 1704A-1704C de radio, que reciben y envían transmisiones de radio desde y a dispositivos 1706A-1706F móviles. Aunque no se representa, el PICNEEC puede incluir o estar en comunicación con un Aplicador de Reglas Personalizado Virtual (VCRE). El VCRE define las características de encaminamiento, cortafuegos, VPN y seguridad para el sistema 1700, y, específicamente, para las comunicaciones entre los dispositivos 1706A-1706F móviles y la red 1708 externa.

Una Función de Personalizador de Reglas (RCF) 1710 es un repositorio externo y controla la función que transfiere todos los cambios y configuraciones de política y seguridad al VCRE. Se usa una consola 1712 de RCF por un cliente para establecer las políticas de encaminamiento y seguridad. La consola 1712 de RCF puede ser, por ejemplo, un portal web, un acceso de Interfaz de Comandos Seguro (SSH), una interfaz de Lenguaje Hombre-Máquina (MML), etc.

Una aplicación 1714 de RCF proporciona un acceso de interfaz de programa de aplicación (API) a la RCF, desde, por ejemplo, una aplicación externa, aplicación en un dispositivo móvil, etc.

MÓDULOS, COMPONENTES Y LÓGICA

Se describen ciertas realizaciones en el presente documento que incluyen lógica o un número de componentes, módulos o mecanismos. Los módulos pueden constituir módulos de software (por ejemplo, código incorporado en un medio legible por máquina) o módulos de hardware. Un "módulo de hardware" es una unidad tangible que puede realizar ciertas operaciones y puede estar configurada o dispuesta en una cierta manera física. En diversas realizaciones de ejemplo, uno o más sistemas informáticos (por ejemplo, un sistema informático independiente, un sistema informático de cliente o un sistema informático de servidor) o uno o más módulos de hardware de un sistema informático (por ejemplo, un procesador o un grupo de procesadores) pueden estar configurados por software (por ejemplo, una aplicación o porción de aplicación) como un módulo de hardware que opera para realizar ciertas operaciones como se describe en el presente documento.

En algunas realizaciones, un módulo de hardware puede implementarse de manera mecánica, electrónica o cualquier combinación adecuada de las mismas. Por ejemplo, un módulo de hardware puede incluir circuitería o lógica especializada que está configurada permanentemente para realizar ciertas operaciones. Por ejemplo, un módulo de hardware puede ser un procesador de propósito especial, tal como un campo de matrices de puertas programables (FPGA) o un circuito integrado específico de la aplicación (ASIC). Un módulo de hardware puede incluir también lógica o circuitería programable que está configurada de manera temporal por software para realizar ciertas operaciones. Por ejemplo, un módulo de hardware puede incluir software ejecutado por un procesador de propósito general u otro procesador programable. Una vez configurado por tal software, los módulos de hardware se vuelven máquinas específicas (o componentes específicos de una máquina) adaptados de manera única para realizar las funciones configuradas y ya no son más procesadores de propósito general. Se apreciará que, la decisión de implementar un módulo de hardware mecánicamente, en circuitería configurada especializada y de manera permanente, o en circuitería configurada de manera temporal (por ejemplo, configurada por software) puede verse impulsado por consideraciones de coste y de tiempo.

Por consiguiente, la oración "módulo de hardware" debe entenderse que abarca una entidad tangible, que es una entidad que está físicamente construida, permanentemente configurada (por ejemplo, de cableado permanente), o temporalmente configurada (por ejemplo, programada) para operar de una cierta manera o para realizar ciertas operaciones descritas en el presente documento. Como se usa en el presente documento, "módulo implementado por hardware" hace referencia a un módulo de hardware. Considerando realizaciones en las que los módulos de hardware están temporalmente configurados (por ejemplo, programados), cada uno de los módulos de hardware no necesita estar configurado o generado en instancias en una instancia cualquiera en el tiempo. Por ejemplo, cuando un módulo de hardware comprende un procesador de propósito general configurado por software para convertirse en un procesador de propósito especial, el procesador de propósito general puede estar configurado como respectivamente diferentes procesadores de propósito especial (por ejemplo, que comprenden diferentes módulos de hardware) en diferentes momentos. El software configura en consecuencia un procesador o procesadores particulares, por ejemplo, para constituir un módulo de hardware particular en una instancia de tiempo y para constituir un módulo de hardware diferente en una instancia de tiempo diferente.

Los módulos de hardware pueden proporcionar información a, y recibir información desde, otros módulos de hardware. Por consiguiente, los módulos de hardware descritos pueden considerarse como que están comunicativamente acoplados. Cuando existen múltiples módulos de hardware al mismo tiempo, pueden conseguirse las comunicaciones a través de transmisión de señales (por ejemplo, a través de circuitos y buses apropiados) entre o a través de dos o más de los módulos de hardware. En las realizaciones en las que múltiples módulos de hardware están configurados o generados en instancias en diferentes tiempos, las comunicaciones entre tales módulos de hardware pueden

conseguirse, por ejemplo, a través del almacenamiento y la recuperación de información en estructuras de memoria a las que tienen acceso los múltiples módulos de hardware. Por ejemplo, un módulo de hardware puede realizar una operación y almacenar la salida de esa la operación en un dispositivo de memoria al que está acoplado de manera comunicativa. Un módulo de hardware adicional puede acceder, en un momento posterior, al dispositivo de memoria para recuperar y procesar la salida almacenada. Los módulos de hardware pueden iniciar también comunicaciones con dispositivos de entrada o de salida, y pueden operar en un recurso (por ejemplo, una colección de información).

Las diversas operaciones de los métodos de ejemplo descritos en el presente documento pueden realizarse, al menos parcialmente, por uno o más procesadores que están configurados temporalmente (por ejemplo, por software) o configurados permanentemente para realizar las operaciones relevantes. Ya sea que estén configurados de forma temporal o permanente, dichos procesadores pueden constituir módulos implementados por procesadores que operan para realizar una o más operaciones o funciones descritas en el presente documento. Como se usa en el presente documento, "módulo implementado por procesador" hace referencia a un módulo de hardware implementado usando uno o más procesadores.

De manera similar, los métodos descritos en el presente documento pueden implementarse al menos parcialmente con un procesador, siendo un procesador o procesadores particulares un ejemplo de hardware. Por ejemplo, al menos algunas de las operaciones de un método pueden realizarse por uno o más procesadores o módulos implementados por procesador. Además, el uno o más procesadores también pueden operar para soportar la realización de las operaciones relevantes en un entorno de "informática en la nube" o como un "software como servicio" (SaaS). Por ejemplo, al menos algunas de las operaciones pueden realizarse por un grupo de ordenadores (como ejemplos de máquinas que incluyen procesadores), siendo estas operaciones accesibles a través de una red (por ejemplo, Internet) y a través de una o más interfaces apropiadas (por ejemplo, una interfaz de programa de aplicación (API)).

El rendimiento de algunas de las operaciones puede distribuirse entre los procesadores, que no solo se encuentran dentro de una sola máquina, sino que están desplegados en varias máquinas. En algunas realizaciones de ejemplo, los procesadores o módulos implementados por procesador pueden ubicarse en una única ubicación geográfica (por ejemplo, dentro de un entorno doméstico, un entorno de oficina o una granja de servidores). En otras realizaciones de ejemplo, los procesadores o módulos implementados por procesador pueden distribuirse a través de un número de ubicaciones geográficas.

MÁQUINA Y ARQUITECTURA DE SOFTWARE

Los módulos, métodos, aplicaciones, y así sucesivamente, descritos en conjunto con las Figuras 1-16 se implementan, en algunas realizaciones, en el contexto de una máquina y arquitectura de software asociada. Las secciones a continuación describen arquitectura o arquitecturas de software y arquitectura o arquitecturas de máquina (por ejemplo, hardware) representativas que son adecuadas para su uso con las realizaciones desveladas.

Las arquitecturas de software se usan en conjunto con arquitecturas de hardware para crear dispositivos y máquinas adaptados a propósitos particulares. Por ejemplo, una arquitectura de hardware particular acoplada con una arquitectura de software particular creará un dispositivo móvil, tal como un teléfono móvil, dispositivo de tableta o así sucesivamente. Una arquitectura de hardware y de software ligeramente diferente puede producir un dispositivo inteligente para su uso en el "Internet de las Cosas" mientras que otra combinación más produce un ordenador de servidor para su uso en una arquitectura de informática en la nube. No todas las combinaciones de tales arquitecturas de software y hardware se presentan en este punto, ya que los expertos en la materia pueden entender fácilmente cómo implementar la materia objeto inventiva en diferentes contextos de la divulgación contenida en el presente documento.

ARQUITECTURA DE SOFTWARE

La Figura 18 es un diagrama 1800 de bloques que ilustra una arquitectura 1802 de software representativa, que puede usarse en conjunto con diversas arquitecturas de hardware descritas en el presente documento. La Figura 18 es simplemente un ejemplo no limitante de una arquitectura 1802 de software y se apreciará que pueden implementarse muchas otras arquitecturas para facilitar la funcionalidad descrita en el presente documento. La arquitectura 1802 de software puede ejecutarse en hardware, tal como la máquina 1900 de la Figura 19 que incluye, entre otras cosas, los procesadores 1910, la memoria/almacenamiento 1930 y los componentes 1950 de E/S. Se ilustra una capa 1804 de hardware representativa y puede representar, por ejemplo, la máquina 1900 de la Figura 19. La capa 1804 de hardware representativa comprende una o más unidades 1806 de procesamiento que tienen instrucciones 1808 ejecutables asociadas. Las instrucciones 1808 ejecutables representan las instrucciones ejecutables de la arquitectura 1802 de software, que incluyen la implementación de los métodos, módulos y así sucesivamente de las Figuras 1-16. La capa 1804 de hardware también incluye los módulos 1810 de memoria y/o almacenamiento, que también tienen las instrucciones 1808 ejecutables. La capa 1804 de hardware puede comprender también otro hardware 1812 que representa cualquier otro hardware de la capa 1804 de hardware, tal como el otro hardware ilustrado como parte de la máquina 1900.

En la arquitectura de ejemplo de la Figura 18, la arquitectura 1802 de software puede conceptualizarse como una pila de capas donde cada capa proporciona funcionalidad particular. Por ejemplo, la arquitectura 1802 de software puede incluir capas tales como un sistema 1814 operativo, bibliotecas 1816, estructuras/soporte intermedio 1818, aplicaciones 1820 y la capa 1844 de presentación. Operacionalmente, las aplicaciones 1820 y/u otros componentes en las capas pueden invocar las solicitudes 1824 de interfaz de programación de aplicación (API) a través de la pila de software y recibir una respuesta, valores devueltos, y así sucesivamente, ilustrados como los mensajes 1826 en respuesta a las solicitudes 1824 de API. Las capas ilustradas son representativas en su naturaleza y no todas las arquitecturas de software tienen todas las capas. Por ejemplo, algunos sistemas operativos móviles o de propósito especial pueden no proporcionar unas estructuras/soporte intermedio 1818, mientras que otros pueden proporcionar una capa de este tipo. Otras arquitecturas de software pueden incluir capas adicionales o diferentes.

El sistema 1814 operativo puede gestionar recursos de hardware y proporcionar servicios comunes. El sistema 1814 operativo puede incluir, por ejemplo, un núcleo 1828, servicios 1830 y controladores 1832. El núcleo 1828 puede actuar como una capa de abstracción entre el hardware y las otras capas de software. Por ejemplo, el núcleo 1828 puede ser responsable de la gestión de memoria, de la gestión del procesador (por ejemplo, planificación), de la gestión de componentes, interconexión en red, ajustes de seguridad y así sucesivamente. Los servicios 1830 pueden proporcionar otros servicios comunes para las otras capas de software. Los controladores 1832 pueden ser responsables de controlar o interactuar con el hardware subyacente. Por ejemplo, los controladores 1832 pueden incluir controladores de visualización, controladores de cámara, controladores de Bluetooth®, controladores de memoria flash, controladores de comunicación serie (por ejemplo, controladores de Bus Serie Universal (USB)), controladores Wi-Fi®, controladores de audio, controladores de gestión de potencial y así sucesivamente, dependiendo de la configuración de hardware.

Las bibliotecas 1816 pueden proporcionar una infraestructura común que puede utilizarse por las aplicaciones 1820 y/u otros componentes y/o capas. Las bibliotecas 1816 típicamente proporcionan funcionalidad que permite que otros módulos de software realicen tareas de una manera más fácil que interconectar directamente con el sistema 1814 operativo subyacente funcionalmente (por ejemplo, el núcleo 1828, los servicios 1830 y/o los controladores 1832). Las bibliotecas 1816 pueden incluir bibliotecas 1834 de sistema (por ejemplo, la biblioteca C convencional) que pueden proporcionar funciones tales como funciones de asignación de memoria, funciones de manipulación de cadenas, funciones matemáticas y similares. Además, las bibliotecas 1816 pueden incluir bibliotecas 1836 de API tales como las bibliotecas de medios (por ejemplo, bibliotecas para soportar la presentación y manipulación de diversos formatos de medios tales como MPEG4, H.264, MP3, AAC, AMR, JPG, PNG), bibliotecas gráficas (por ejemplo, una estructura de OpenGL que puede usarse para representar 2D y 3D en un contenido gráfico en una pantalla), bibliotecas de base de datos (por ejemplo, SQLite que puede proporcionar diversas funciones de base de datos relacionales), bibliotecas web (por ejemplo, WebKit que puede proporcionar funcionalidad de exploración web) y similares. Las bibliotecas 1816 pueden incluir también una amplia diversidad de otras bibliotecas 1838 para proporcionar muchas otras API a las aplicaciones 1820 y otros componentes/módulos de software.

Las estructuras/soporte intermedio 1818 (también en ocasiones denominado como soporte intermedio) pueden proporcionar una infraestructura común de nivel superior que puede utilizarse por las aplicaciones 1820 y/u otros componentes/módulos de software. Por ejemplo, las estructuras/soporte intermedio 1818 pueden proporcionar diversas funciones de interfaz de usuario gráfica (GUI), gestión de recursos de alto nivel, servicios de ubicación de alto nivel y así sucesivamente. Las estructuras/soporte intermedio 1818 pueden proporcionar un espectro amplio de otras API que pueden utilizarse por las aplicaciones 1820 y/u otros componentes/módulos de software, alguno de los que pueden ser específicos a un sistema operativo o plataforma particular.

Las aplicaciones 1820 incluyen aplicaciones 1840 integradas y/o aplicaciones 1842 de terceros. Ejemplos de aplicaciones 1840 integradas representativas pueden incluir, pero sin limitación, una aplicación de contactos, una aplicación de explorador, una aplicación de lector de libros, una aplicación de ubicación, una aplicación de medios, una aplicación de mensajería y/o una aplicación de juegos. Las aplicaciones 1842 de terceros pueden incluir cualquiera de las aplicaciones 1840 integradas, así como una amplia diversidad de otras aplicaciones. En un ejemplo específico, la aplicación 1842 de terceros (por ejemplo, una aplicación desarrollada usando el kit de desarrollo de software (SDK) de Android™ o iOS™ por una entidad distinta del proveedor de la plataforma particular) puede ser software móvil que se ejecuta en un sistema operativo móvil tal como iOS™, Android™, Windows® Phone u otros sistemas operativos móviles. En este ejemplo, la aplicación 1842 de terceros puede invocar las solicitudes 1824 de API proporcionadas por el sistema operativo móvil, tal como el sistema 1814 operativo, para facilitar la funcionalidad descrita en el presente documento.

Las aplicaciones 1820 pueden utilizar las funciones de sistema operativo integradas (por ejemplo, el núcleo 1828, los servicios 1830 y/o los controladores 1832), las bibliotecas (por ejemplo, las bibliotecas 1834 de sistema, las bibliotecas 1836 API y otras bibliotecas 1838), las estructuras/soporte intermedio 1818 para crear interfaces de usuario para interactuar con usuarios del sistema. Como alternativa, o adicionalmente, en algunos sistemas, las interacciones con un usuario pueden tener lugar a través de una capa de presentación, tal como la capa 1844 de presentación. En estos sistemas, la "lógica" de la aplicación/módulo puede estar separada de los aspectos de la aplicación/módulo que interactúan con un usuario.

Algunas arquitecturas de software utilizan máquinas virtuales. En el ejemplo de la Figura 18, esto se ilustra por la máquina 1848 virtual. Una máquina virtual crea un entorno de software donde las aplicaciones/módulos pueden ejecutarse como si estuvieran ejecutándose en una máquina de hardware (tal como la máquina 1900 de la Figura 19, por ejemplo). Una máquina 1848 virtual está alojada por un sistema operativo anfitrión (el sistema 1814 operativo en la Figura 18) y típicamente, aunque no siempre, tiene un monitor 1846 de máquina virtual, que gestiona la operación de la máquina 1848 virtual, así como la interfaz con el sistema operativo anfitrión (es decir, el sistema 1814 operativo). Una arquitectura de software se ejecuta en la máquina 1848 virtual, tal como un sistema 1850 operativo, las bibliotecas 1852, las estructuras/soporte intermedio 1854, las aplicaciones 1856 y/o la capa 1858 de presentación. Estas capas de la arquitectura de software que se ejecutan en la máquina 1848 virtual pueden ser las mismas que corresponden a las capas previamente descritas o pueden ser diferentes.

ARQUITECTURA DE MÁQUINA Y MEDIO LEGIBLE POR MÁQUINA DE EJEMPLO

La Figura 19 es un diagrama de bloques que ilustra componentes de una máquina 1900, de acuerdo con algunas realizaciones de ejemplo, que pueden leer instrucciones 1916 de un medio legible por máquina (por ejemplo, un medio de almacenamiento legible por máquina) y realizar una cualquiera o más de las metodologías analizadas en el presente documento. Específicamente, la Figura 19 muestra una representación esquemática de la máquina 1900 en la forma de ejemplo de un sistema informático, dentro del que las instrucciones 1916 (por ejemplo, un software, un programa, una aplicación, una miniaplicación, una aplicación u otro código ejecutable) hacen que la máquina 1900 realice las metodologías anteriormente descritas con respecto a los puntos terminales (por ejemplo, dispositivos móviles, un dispositivo en las redes externas) anteriormente descritos. Las instrucciones 1916 transforman la máquina 1900 no programada general en una máquina particular programada para llevar a cabo las funciones descritas e ilustradas de la manera descrita. En realizaciones alternativas, la máquina 1900 opera como un dispositivo independiente o puede estar acoplada (por ejemplo, en red) a otras máquinas. En un despliegue en red, la máquina 1900 puede operar en la capacidad de una máquina de servidor o en una máquina de cliente en un entorno de red de servidor-cliente, o como una máquina de pares en un entorno de red entre pares (o distribuido). La máquina 1900 puede comprender, pero sin limitación, un ordenador de servidor, un ordenador de cliente, un ordenador personal (PC), un ordenador de tableta, un ordenador portátil, un portátil, un decodificador de salón (STB), un asistente digital personal (PDA), un sistema de medios de entretenimiento, un teléfono celular, un teléfono inteligente, un dispositivo móvil, un dispositivo llevable (por ejemplo, un reloj inteligente), un dispositivo de hogar inteligente (por ejemplo, un dispositivo inteligente), otros dispositivos inteligentes, un dispositivo de web, un encaminador de red, un conmutador de red, un puente de red o cualquier máquina que pueda ejecutar las instrucciones 1916, de manera secuencial o de otra, que especifican acciones para que se lleven a cabo por la máquina 1900. Además, aunque únicamente se ilustra una única máquina 1900, el término "máquina" deberá tomarse también que incluye una colección de máquinas 1900 que ejecutan de manera individual o conjunta las instrucciones 1916 para realizar una cualquiera o más de las metodologías analizadas en el presente documento.

La máquina 1900 puede incluir los procesadores 1910, la memoria/almacenamiento 1930 y los componentes 1950 de E/S, que pueden estar configurados para comunicarse entre sí, tal como mediante un bus 1902. En una realización de ejemplo, los procesadores 1910 (por ejemplo, una unidad de procesamiento central (CPU), un procesador informático de conjunto de instrucciones reducido (RISC), un procesador informático de conjunto de instrucciones complejo (CISC), una unidad de procesamiento de gráficos (GPU), un procesador de señales digitales (DSP), un circuito integrado específico de la aplicación (ASIC), un circuito integrado de radio-frecuencia (RFIC), otro procesador o cualquier combinación adecuada de los mismos) pueden incluir, por ejemplo, el procesador 1912 y el procesador 1914 que pueden ejecutar las instrucciones 1916. El término "procesador" se pretende que incluya el procesador 1912, 1914 de múltiples núcleos que puede comprender dos o más procesadores 1912, 1914 independientes (en ocasiones denominados "núcleos") que pueden ejecutar las instrucciones 1916 simultáneamente. Aunque la Figura 19 muestra múltiples procesadores 1910, la máquina 1900 puede incluir un único procesador 1912, 1914 con un único núcleo, un único procesador 1912, 1914 con múltiples núcleos (por ejemplo, un procesador 1912, 1914 de múltiples núcleos), múltiples procesadores 1912, 1914 con un único núcleo, múltiples procesadores 1912, 1914 con múltiples núcleos o cualquier combinación de los mismos.

La memoria/almacenamiento 1930 puede incluir una memoria 1932, tal como una memoria principal u otro almacenamiento de memoria y una unidad 1936 de almacenamiento, ambas accesibles a los procesadores 1910 tal como mediante el bus 1902. La unidad 1936 de almacenamiento y la memoria 1932 almacenan las instrucciones 1916 que incorporan cualquiera de una o más de las metodologías o funciones descritas en el presente documento. Las instrucciones 1916 pueden residir también, completa o parcialmente, en la memoria 1932, en la unidad 1936 de almacenamiento, en al menos uno de los procesadores 1910 (por ejemplo, en la memoria caché del procesador 1912, 1914), o en cualquier combinación adecuada de los mismos, durante la ejecución de los mismos por la máquina 1900. Por consiguiente, la memoria 1932, la unidad 1936 de almacenamiento y la memoria de los procesadores 1910 son ejemplos de medios legibles por máquina.

Como se usa en el presente documento, "medio legible por máquina" significa un dispositivo que puede almacenar instrucciones 1916 y datos temporal o permanentemente y puede incluir, pero sin limitación, memoria de acceso aleatorio (RAM), memoria de sólo lectura (ROM), memoria intermedia, memoria flash, medios ópticos, medios magnéticos, memoria caché, otros tipos de almacenamiento (por ejemplo, memoria de sólo lectura programable

borrable (EEPROM)) y/o cualquier combinación adecuada de los mismos. La expresión "medio legible por máquina" debe tomarse para que incluya un único medio o múltiples medios (por ejemplo, una base de datos centralizada o distribuida o cachés y servidores asociados) que pueden almacenar las instrucciones 1916. La expresión "medio legible por máquina" debe tomarse también para que incluya cualquier medio, o combinación de múltiples medios, que puedan almacenar o llevar instrucciones (por ejemplo, las instrucciones 1916) para su ejecución por una máquina (por ejemplo, la máquina 1900), de manera que las instrucciones 1916, cuando se ejecutan por uno o más procesadores de la máquina 1900 (por ejemplo, los procesadores 1910), hacen que la máquina 1900 realice una cualquiera o más de las metodologías descritas en el presente documento. Por consiguiente, un "medio legible por máquina" se refiere a un único aparato o dispositivo de almacenamiento, así como sistemas de almacenamiento "basados en la nube" o redes de almacenamiento que incluyen múltiples aparatos o dispositivos de almacenamiento.

Los componentes 1950 de E/S pueden incluir una amplia diversidad de componentes para recibir entrada, proporcionar salida, producir salida, transmitir información, intercambiar información, capturar mediciones y así sucesivamente. Los componentes 1950 de E/S específicos que están incluidos en una máquina particular dependerán del tipo de máquina 1900. Por ejemplo, máquinas portátiles tales como los teléfonos móviles probablemente incluirán un dispositivo de entrada táctil u otros mecanismos de entrada de este tipo, mientras que una máquina de servidor desatendida probablemente no incluirá un dispositivo de entrada táctil de este tipo. Se apreciará que los componentes 1950 de E/S pueden incluir muchos otros componentes que no se muestran en la Figura 19. Los componentes 1950 de E/S están agrupados de acuerdo con la funcionalidad simplemente para simplificar el siguiente análisis y la agrupación no es limitante de manera alguna. En diversas realizaciones de ejemplo, los componentes 1950 de E/S pueden incluir los componentes 1952 de salida y los componentes 1954 de entrada. Los componentes 1952 de salida pueden incluir componentes visuales (por ejemplo, una pantalla, tal como un panel de visualización de plasma (PDP), una pantalla de diodo de emisión de luz (LED), una pantalla de cristal líquido (LCD), un proyector, o un tubo de rayos catódicos (CRT)), componentes acústicos (por ejemplo, altavoces), componentes hápticos (por ejemplo, un motor vibratorio, mecanismos de resistencia), otros generadores de señales y así sucesivamente. Los componentes 1954 de entrada pueden incluir componentes de entrada alfanumérica (por ejemplo, un teclado, una pantalla táctil configurada para recibir entrada alfanumérica, un teclado foto-óptico u otros componentes de entrada alfanumérica), componentes de entrada basados en señalamiento (por ejemplo, un ratón, un panel táctil, una bola de mando, una palanca de mandos, un sensor de movimiento u otro instrumento de señalamiento), componentes de entrada táctil (por ejemplo, un botón físico, una pantalla táctil que proporciona ubicación y/o fuerza de toques o gestos táctiles u otros componentes de entrada táctil), componentes de entrada de audio (por ejemplo, un micrófono) y similares.

En realizaciones de ejemplo adicionales, los componentes 1950 de E/S pueden incluir componentes 1956 biométricos, componentes 1958 de movimiento, componentes 1960 ambientales o componentes 1962 de posición entre una amplia gama de otros componentes. Por ejemplo, los componentes 1956 biométricos pueden incluir componentes para detectar expresiones (por ejemplo, expresiones manuales, expresiones faciales, expresiones vocales, gestos corporales o seguimiento del ojo), medir señales biológicas (por ejemplo, presión sanguínea, frecuencia cardiaca, temperatura corporal, transpiración u ondas cerebrales), identificar una persona (por ejemplo, identificación de voz, identificación retinal, identificación facial, identificación de huella dactilar o identificación basada en electroencefalograma) y similares. Los componentes 1958 de movimiento pueden incluir componentes de sensor de aceleración (por ejemplo, acelerómetro), componentes de sensor de gravitación, componentes de sensor de rotación (por ejemplo, giroscopio) y así sucesivamente. Los componentes 1960 ambientales pueden incluir, por ejemplo, componentes de sensor de iluminación (por ejemplo, fotómetro), componentes de sensor de temperatura (por ejemplo, uno o más termómetros que detectan la temperatura ambiente), componentes de sensor de humedad, componentes de sensor de presión (por ejemplo, barómetro), componentes de sensor acústicos (por ejemplo, uno o más micrófonos que detectan el ruido de fondo), componentes de sensor de proximidad (por ejemplo, sensores de infrarrojos que detectan objetos cercanos), sensores de gas (por ejemplo, sensores de detección de gas para detección de concentraciones de gases peligrosos por seguridad o para medir contaminantes en la atmósfera) u otros componentes que pueden proporcionar indicaciones, mediciones o señales que corresponden a un entorno físico circundante. Los componentes 1962 de posición pueden incluir componentes de sensor de ubicación (por ejemplo, un componente de receptor del Sistema de Posición Global (GPS)), componentes de sensor de altitud (por ejemplo, altímetros o barómetros que detectan la presión del aire desde la que puede derivarse la altitud), componentes de sensor de orientación (por ejemplo, magnetómetros) y similares.

La comunicación puede implementarse usando una amplia diversidad de tecnologías. Los componentes 1950 de E/S pueden incluir componentes 1964 de comunicación operativos para acoplar la máquina 1900 a una red 1980 o dispositivos 1970 mediante el acoplamiento 1982 y el acoplamiento 1972 respectivamente. Por ejemplo, los componentes 1964 de comunicación pueden incluir un componente de interfaz de red u otro dispositivo adecuado para interconectar con la red 1980. En ejemplos adicionales, los componentes 1964 de comunicación pueden incluir componentes de comunicación alámbrica, componentes de comunicación inalámbrica, componentes de comunicación celular, componentes de comunicación de campo cercano (NFC), componentes de Bluetooth® (por ejemplo, Bluetooth® de Baja Energía), componentes Wi-Fi® y otros componentes de comunicación para proporcionar comunicación mediante otras modalidades. Los dispositivos 1970 pueden ser otra máquina o cualquiera de una amplia diversidad de dispositivos periféricos (por ejemplo, un dispositivo periférico acoplado mediante un Bus Serie Universal (USB)).

Además, los componentes 1964 de comunicación pueden detectar identificadores o incluir componentes operables para detectar identificadores. Por ejemplo, los componentes 1964 de comunicación pueden incluir componentes lectores de etiquetas de identificación por radio frecuencia (RFID), componentes de detección de etiqueta inteligente de NFC, componentes de lector óptico (por ejemplo, un sensor óptico para detectar códigos de barras unidimensionales tales como un código de barras de Código de Producto Universal (UPC), códigos de barras multidimensionales tales como el código de Respuesta Rápida (QR), código Aztec, matriz de datos, Dataglyph, código MaxiCode, PDF417, código Ultra Code, código de barras UCC RSS-2D y otros códigos ópticos) o componentes de detección acústicos (por ejemplo, micrófonos para identificar señales de audio etiquetadas). Además, puede derivarse una diversidad de información mediante los componentes 1964 de comunicación, tal como la ubicación mediante geo-localización del Protocolo de Internet (IP), ubicación mediante triangulación de señal Wi-Fi®, ubicación mediante detección de una señal de baliza de NFC que puede indicar una ubicación particular y así sucesivamente.

MEDIO DE TRANSMISIÓN

En diversas realizaciones de ejemplo, una o más porciones de la red 1980 pueden ser una red ad hoc, una intranet, una extranet, una red privada virtual (VPN), una red de área local (LAN), una LAN inalámbrica (WLAN), una red de área extensa (WAN), una WAN inalámbrica (WWAN), una red de área metropolitana (MAN), Internet, una porción de Internet, una porción de la red telefónica pública conmutada (PSTN), una red sencilla del servicio telefónico antiguo (POTS), una red de telefonía celular, una red inalámbrica, una red Wi-Fi®, otro tipo de red o una combinación de dos o más de tales redes. Por ejemplo, la red 1980 o una porción de la red 1980 puede incluir una red inalámbrica o celular y el acoplamiento 1982 puede ser una conexión de Acceso Múltiple por División de Código (CDMA), una conexión del Sistema Global para Comunicación Móvil (GSM) u otro tipo de acoplamiento celular o inalámbrico. En este ejemplo, el acoplamiento 1982 puede implementar cualquiera de una diversidad de tipos de tecnología de transferencia de datos, tal como Tecnología de Transmisión de Radio de Portadora Única (1xRTT), tecnología de la Evolución-Datos Optimizados (EVDO), tecnología del Servicio General de Paquetes de Radio (GPRS), tecnología de Tasas de Datos Mejoradas para la Evolución de GSM (EDGE), Proyecto Asociación de la tercera Generación (3GPP) que incluye 3G, redes inalámbricas de la cuarta generación (4G), Sistema Universal de Telecomunicaciones Móviles (UMTS), Acceso por Paquetes de Alta Velocidad (HSPA), Interoperabilidad Mundial para Acceso por Microondas (WiMAX), la norma de la Evolución a Largo Plazo (LTE) otras definidas por diversas organizaciones de ajuste de normas, otros protocolos de largo alcance u otra tecnología de transferencia de datos.

Las instrucciones 1916 pueden transmitirse o recibirse a través de la red 1980 usando un medio de transmisión mediante un dispositivo de interfaz de red (por ejemplo, un componente de interfaz de red incluido en los componentes 1964 de comunicación) y que utiliza uno cualquiera de un número de protocolos de transferencia bien conocidos (por ejemplo, el protocolo de transferencia de hipertexto (HTTP)). De manera similar, las instrucciones 1916 pueden transmitirse o recibirse usando un medio de transmisión mediante el acoplamiento 1972 (por ejemplo, un acoplamiento entre pares) a los dispositivos 1970. La expresión "medio de transmisión" debe tomarse para que incluya cualquier medio intangible que pueda almacenar, codificar o llevar instrucciones 1916 para su ejecución por la máquina 1900 e incluye señales de comunicaciones digitales o analógicas u otro medio intangible para facilitar la comunicación de tal software. Un medio de transmisión es una realización de un medio legible por máquina.

IDIOMA

A lo largo de la presente memoria descriptiva, varias instancias pueden implementar componentes, operaciones o estructuras descritas como una única instancia. Aunque las operaciones individuales de uno o más métodos se ilustran y describen como operaciones separadas, una o más de las operaciones individuales pueden realizarse simultáneamente y nada requiere que las operaciones se realicen en el orden ilustrado. Las estructuras y la funcionalidad presentadas como componentes separados en las configuraciones se pueden implementar como una estructura o componente combinado. De forma similar, las estructuras y la funcionalidad presentadas como un único componente se pueden implementar como componentes separados. Estas y otras variaciones, modificaciones, adiciones y mejoras entran dentro del alcance de la materia objeto del presente documento.

Aunque se ha descrito una vista general de la materia objeto inventiva con referencia a realizaciones de ejemplo específicas, pueden realizarse diversas modificaciones y cambios a estas realizaciones sin alejarse del ámbito más amplio de las realizaciones de la presente divulgación. Se puede hacer referencia en el presente documento a tales realizaciones de la materia objeto inventiva, individual o colectivamente, mediante la expresión "invención" meramente por razones de conveniencia y sin tener por objeto limitar voluntariamente el alcance de la presente solicitud a divulgación o concepto inventivo individual alguno si, de hecho, se divulga más de uno.

Las realizaciones ilustradas en el presente documento se describen en suficiente detalle para posibilitar a los expertos en la materia poner en práctica las enseñanzas desveladas. Pueden usarse y derivarse otras realizaciones a partir de las mismas, de manera que pueden realizarse sustituciones y cambios estructurales y lógicos sin alejarse del alcance de esta divulgación. La descripción detallada, por lo tanto, no ha de tomarse en un sentido limitante, y el alcance de diversas realizaciones se define únicamente por las reivindicaciones adjuntas.

Como se usa en el presente documento, el término "o" puede interpretarse en sentido inclusivo o exclusivo. Además, pueden proporcionarse instancias plurales para recursos, operaciones o estructuras descritas en el presente documento como una única instancia. Adicionalmente, los límites entre diversos recursos, operaciones, módulos, motores y almacenes de datos son en cierto modo arbitrarios y se ilustran operaciones particulares en un contexto de configuraciones ilustrativas específicas. Se prevén otras asignaciones de funcionalidad y pueden caer aún dentro del alcance de diversas realizaciones de la presente divulgación. En general, las estructuras y la funcionalidad presentadas como recursos separados en las configuraciones de ejemplo pueden implementarse como una estructura o recurso combinado. De manera similar, las estructuras y la funcionalidad presentadas como un único recurso pueden implementarse como recursos separados. Estas y otras variaciones, modificaciones, adiciones y mejoras caen dentro de un alcance de las realizaciones de la presente divulgación según se representa por las reivindicaciones adjuntas. La memoria descriptiva y dibujos, por consiguiente, deben considerarse en un sentido ilustrativo en lugar de un sentido restrictivo.

REIVINDICACIONES

1. Un habilitador y controlador de perímetro de red personalizado integrado de PDN, PICNEEC, (404; 1306) para su operación por un proveedor de red móvil, que comprende:

al menos un aplicador de reglas personalizadas virtual, VCRE, (406; 500; 1318; 1408), estando dividido el VCRE en una pluralidad de instancias (502A-502N; 1012; 1412) de VCRE, correspondiendo cada instancia (502A-502N; 1012; 1412) de VCRE a un grupo de dispositivos móviles y que define un conjunto de políticas personalizadas para el grupo de dispositivos móviles,
en donde el PICNEEC (404; 1306) está configurado para recibir (1034; 1102; 1202) un paquete de datos comunicado entre una red basada en paquetes y un dispositivo móvil, comunicándose el paquete de datos (1032, 1034; 1432, 1434) mediante los nodos (402, 418; 1004, 1006; 1302, 1304; 1404, 1406) en una red de radio,

determinar (1204), basándose en información en el paquete de datos, una instancia (502A-502N; 1012; 1412) de VCRE de entre las al menos unas instancias de VCRE que corresponden al dispositivo móvil,
ejecutar (1208, 1210, 1212, 1214, 1216) una o más reglas de política almacenadas en la instancia (502A-502N; 1012; 1412) de VCRE determinada en el paquete de datos, y a continuación
encaminar (1038, 1040; 1110; 1214; 1440, 1442) el paquete de datos de acuerdo con la regla de política ejecutada o cada una;

en donde cada instancia (502A-502N; 1012; 1412) de VCRE se controla independientemente entre sí mediante acceso directo de la instancia (502A-502N; 1012; 1412) de VCRE por un cliente diferente del proveedor de red móvil; y en donde las reglas de política almacenadas en la instancia (502A-502N; 1012; 1412) de VCRE incluyen una regla de cliente especificada que define una red privada virtual, VPN, entre el VCRE (406; 500; 1318; 1408) y una red externa y una regla de cliente especificada que define el encaminamiento de red entre el VCRE (406; 500; 1318; 1408) y las redes de conectividad del protocolo de internet, IP.

2. El PICNEEC de la reivindicación 1, en donde el paquete de datos se encamina entre:

un nodo de soporte, SGSN, del servicio general de paquetes de radio de servicio, GPRS, y un nodo de soporte de GPRS de pasarela, GGSN, interno al PICNEEC;
una pasarela de servicio, SGW, y una pasarela de red de datos de paquetes, PGW, internas al PICNEEC;
un SGSN y un GGSN externos al PICNEEC, manejando el GGSN externo datos para una red de acceso de conectividad del protocolo de internet, IP, a través del PICNEEC; o
una SGW y una PGW externas al PICNEEC, manejando la PGW externa datos para una red de acceso de conectividad de IP a través del PICNEEC.

3. El PICNEEC de la reivindicación 1 o la reivindicación 2, en donde el paquete de datos se encamina a través de una pasarela de paquetes de servicio de red móvil que maneja el paquete de datos a través del PICNEEC.

4. El PICNEEC de la reivindicación 1, en donde la al menos una instancia de VCRE:

define nombres de punto de acceso, APN, personalizados;
es una función de red virtual independiente;
es una función de red física independiente;
es un subconjunto de reglas en una función de red más grande, en donde el cliente únicamente puede acceder al subconjunto de reglas específicas; o
se crea por un cliente usando la consola (414) de función de reglas de VCRE, RCF.

5. El PICNEEC de la reivindicación 4, en donde la consola (414) de RCF es un acceso de interfaz de comandos seguro, SSH.

6. El PICNEEC de una cualquiera de las reivindicaciones 1 a 5, en donde se crea al menos una instancia de VCRE por un cliente usando una aplicación (416) de función personalizadora de reglas de VCRE, RCF.

7. El PICNEEC de la reivindicación 6, en donde la aplicación (416) de RCF es una interfaz de programa de aplicación, API, un sitio web o un programa informático especializado.

8. El PICNEEC de la reivindicación 4, en donde la consola de RCF o la aplicación de RCF gestiona la al menos una instancia de VCRE directamente, o
en donde la consola de RCF o la aplicación de RCF se conecta a una RCF central que gestiona al menos una de las instancias de VCRE.

9. El PICNEEC de una cualquiera de las reivindicaciones 1 a 8, en donde un cliente define una correspondiente instancia de VCRE:

especificando la regla que define la VPN entre la correspondiente instancia de VCRE y la red externa, o
especificando la regla que define el encaminamiento de red entre la correspondiente instancia de VCRE y las redes de conectividad de IP, o
definiendo reglas de cortafuegos para tráfico de datos de paquetes que pasa a través de la correspondiente instancia de VCRE, o
definiendo reglas de traducción de dirección de red, NAT, para el tráfico de datos de paquetes que pasa a través de la correspondiente instancia de VCRE, o
definiendo ajustes de sistema de nombre de dominio, DNS, para tráfico de datos de paquetes que pasa a través de la correspondiente instancia de VCRE, o
definiendo reglas de seguridad para tráfico de datos de paquetes que pasa a través de la correspondiente instancia de VCRE, o
asignando direcciones de IP a dispositivos móviles, o
definiendo reglas de enriquecimiento de encabezado de protocolo de transferencia de hipertexto, HHE, para tráfico que pasa a través de la correspondiente instancia de VCRE.

10. El PICNEEC de la reivindicación 1
en donde el PICNEEC está conectado simultáneamente a una red de 3G/4G y una red de área extensa de baja energía, LPWAN.

11. Un método que comprende:

recibir, en un aplicador de reglas personalizadas virtual, VCRE de un posibilitador y controlador de perímetro de red personalizado integrado de PDN, PICNEEC, un paquete de datos enviado entre un dispositivo móvil y una red basada en paquetes, comunicándose el paquete de datos mediante los nodos en una red de radio;
determinar, basándose en información en el paquete de datos, una instancia de VCRE asignada al dispositivo móvil de entre una pluralidad de instancias de VCRE en el VCRE, la instancia de VCRE controlada independiente de otras instancias de VCRE en el PICNEEC mediante acceso directo de la instancia de VCRE por un cliente de un proveedor de red móvil que opera el PICNEEC;
ejecutar una o más reglas de política definidas en la instancia de VCRE determinada en el paquete de datos, en donde las reglas de política definidas incluyen una regla de cliente especificada que define una red privada virtual, VPN, entre el VCRE y una red externa y una regla de cliente especificada que define encaminamiento de red entre el VCRE y redes de conectividad del protocolo de internet, IP; y encaminar el paquete de datos de acuerdo con la regla de política ejecutada o cada una.

12. El método de la reivindicación 11, en donde el paquete de datos se encamina entre:

un nodo de soporte, SGSN, del servicio general de paquetes de radio de servicio, GPRS, y un nodo de soporte de GPRS de pasarela, GGSN, interno al PICNEEC;
una pasarela de servicio, SGW, y una pasarela de red de datos de paquetes, PGW, internas al PICNEEC;
un SGSN y un GGSN externos al PICNEEC, manejando el GGSN externo datos para una red de acceso de conectividad de IP a través del PICNEEC; o
una SGW y una PGW externas al PICNEEC, manejando la PGW externa datos para una red de acceso de conectividad de IP a través del PICNEEC.

13. El método de la reivindicación 11 o la reivindicación 12, en donde el paquete de datos se encamina a través de una pasarela de paquetes de servicio de red móvil que maneja el paquete de datos a través del PICNEEC.

14. Un medio legible por máquina que lleva código legible por máquina para controlar un procesador de una máquina para llevar a cabo el método de una cualquiera de las reivindicaciones 11 a 13.

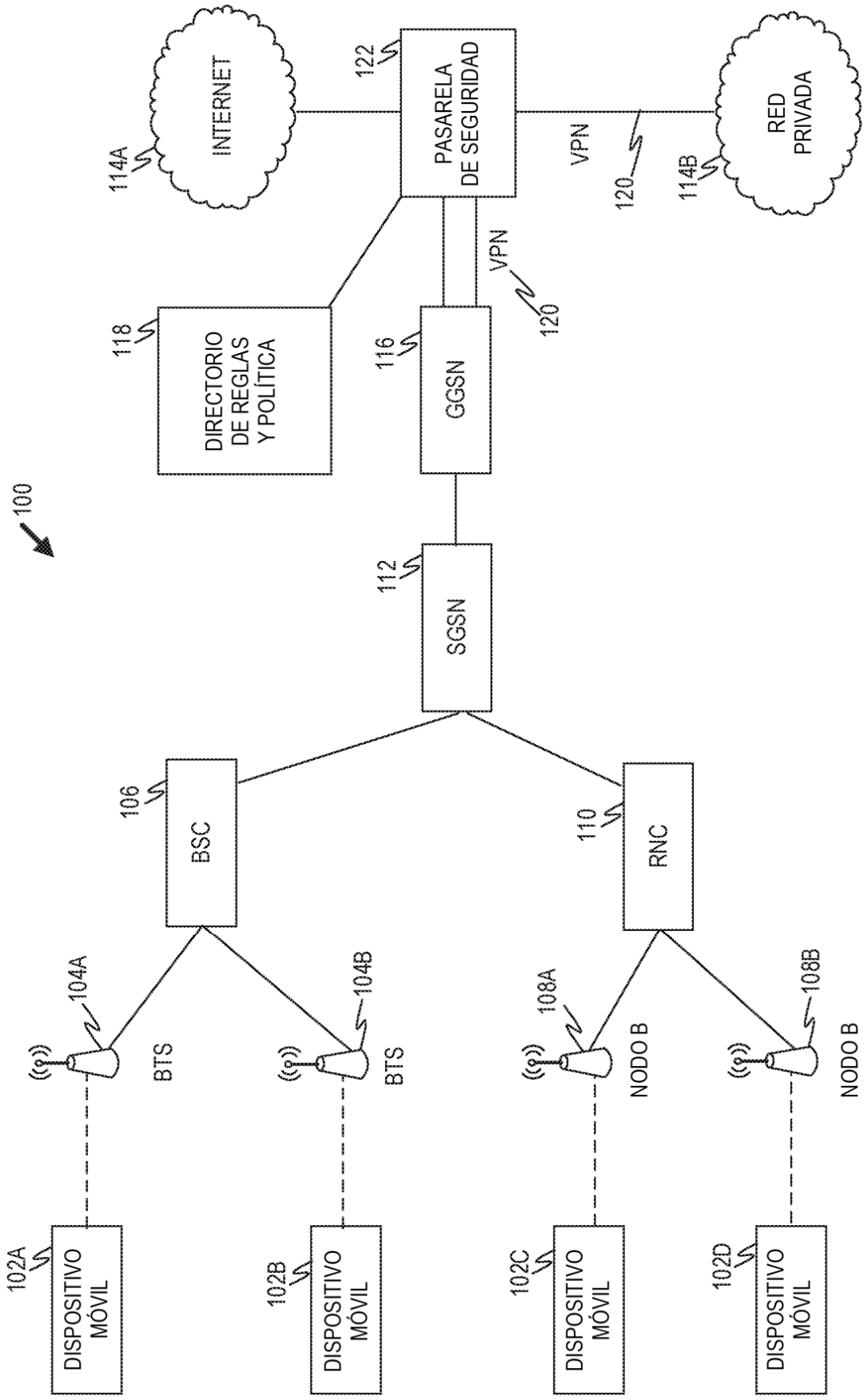
100
INTERNET
114A
122
PASARELA DE SEGURIDAD
VPN
120
114B
RED PRIVADA
VPN
120
118
DIRECTORIO DE REGLAS Y POLÍTICA
116
GGSN
112
SGSN
106
BSC
110
RNC
104A
BTS
104B
BTS
108A
NODO B
108B
NODO B
102A
DISPOSITIVO MÓVIL
102B
DISPOSITIVO MÓVIL
102C
DISPOSITIVO MÓVIL
102D
DISPOSITIVO MÓVIL

FIG. 1

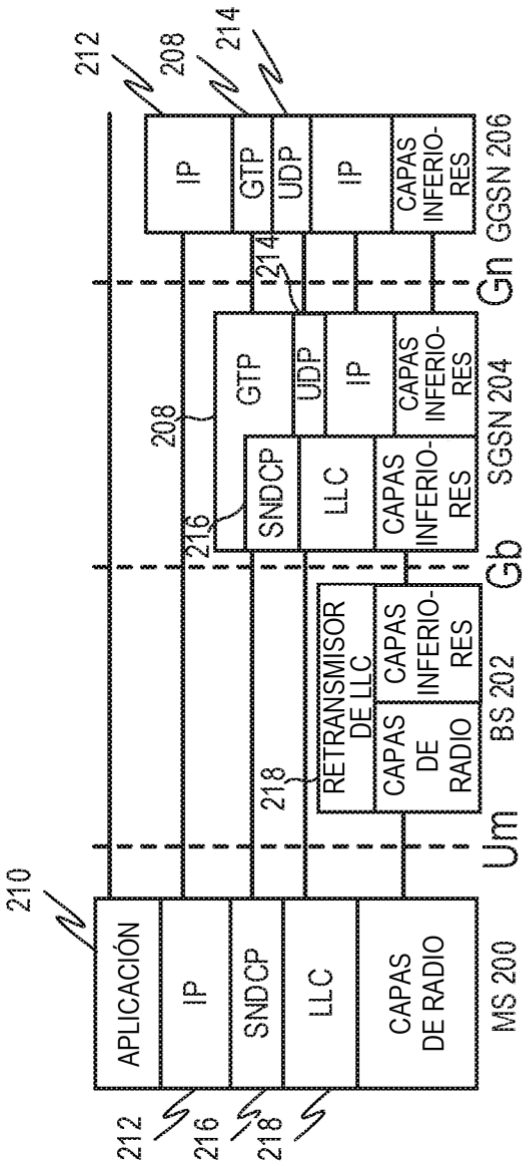
212
208
214
IP
GTP
UDP
IP
CAPAS INFERIO-RES
GGSN 206
Gn
214
208
GTP
UDP
IP
CAPAS INFERIO-RES
SGSN 204
216
SNDCP
LLC
CAPAS INFERIO-RES
Gb
RETRANSMISOR DE LLC
CAPAS INFERIO-RES
218
CAPAS DE RADIO
BS 202
Um
210
APLICACIÓN
IP
SNDCP
LLC
CAPAS DE RADIO
MS 200
212
216
218

FIG. 2

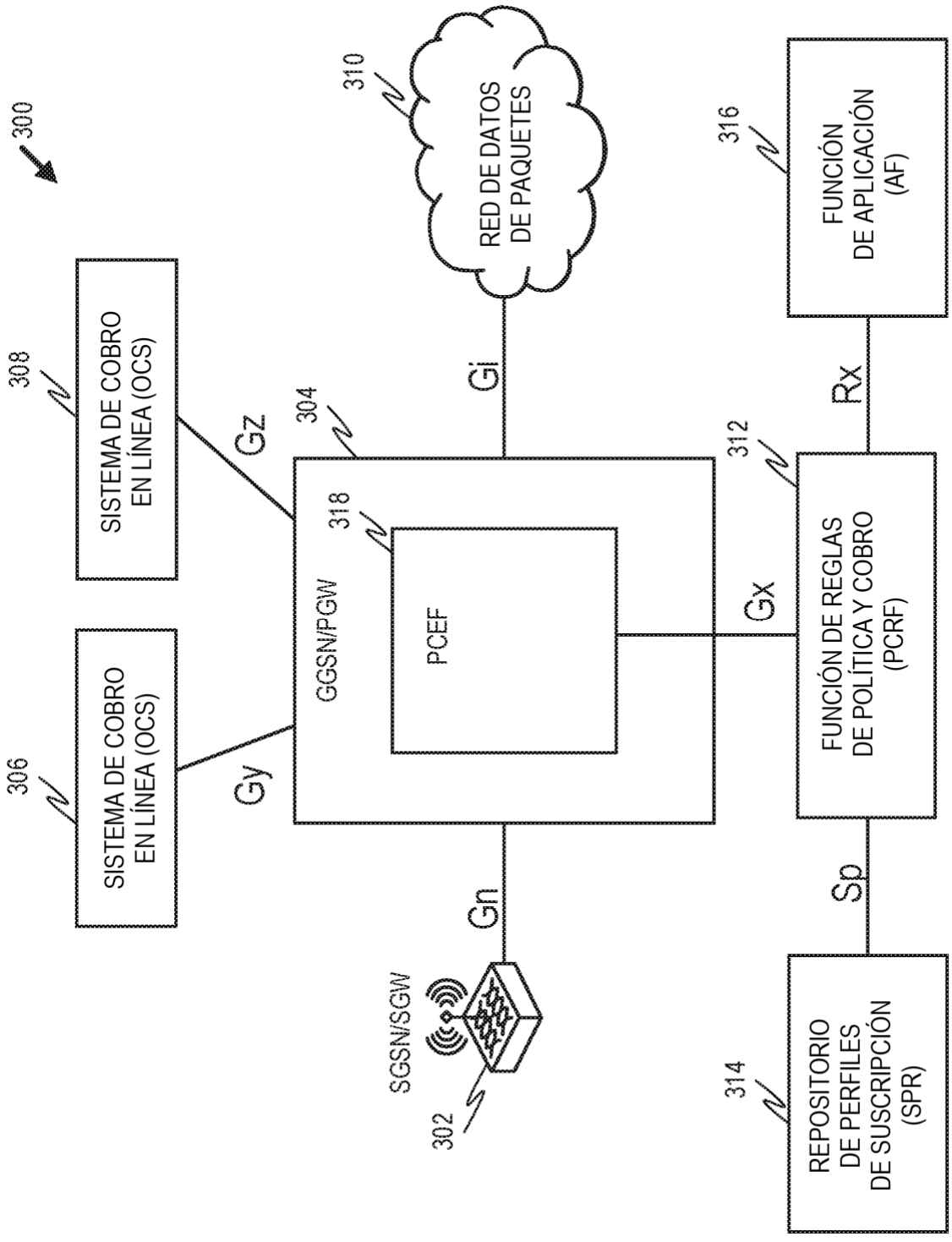
300
310
RED DE DATOS DE PAQUETES
316
FUNCIÓN DE APLICACIÓN (AF)
308
SISTEMA DE COBRO EN LÍNEA (OCS)
Gz
304
Gi
Rx
312
318
PCEF
GGSN/PGW
Gx
FUNCIÓN DE REGLAS DE POLÍTICA Y COBRO (PCRF)
306
SISTEMA DE COBRO EN LÍNEA (OCS)
Gy
Gn
Sp
SGSN/SGW
302
314
REPOSITORIO DE PERFILES DE SUSCRIPCIÓN (SPR)

FIG. 3

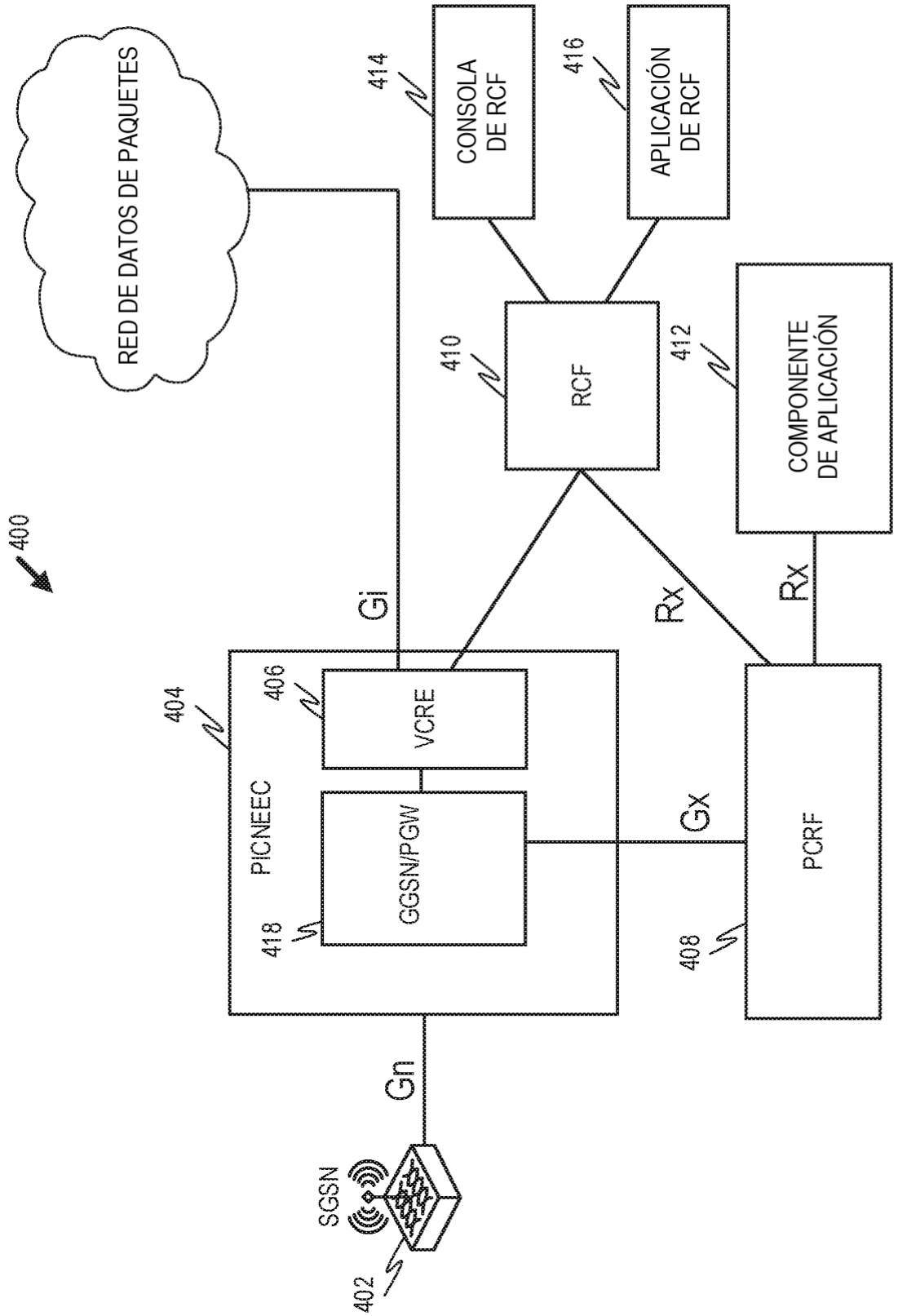
400
RED DE DATOS DE PAQUETES
414
CONSOLA DE RCF
416
APLICACIÓN DE RCF
410
RCF
412
COMPONENTE DE APLICACIÓN
Gi
Rx
Rx
404
PICNEEC
406
VCRE
418
GGSN/PGW
Gx
408
PCRF
Gn
SGSN
402

FIG. 4

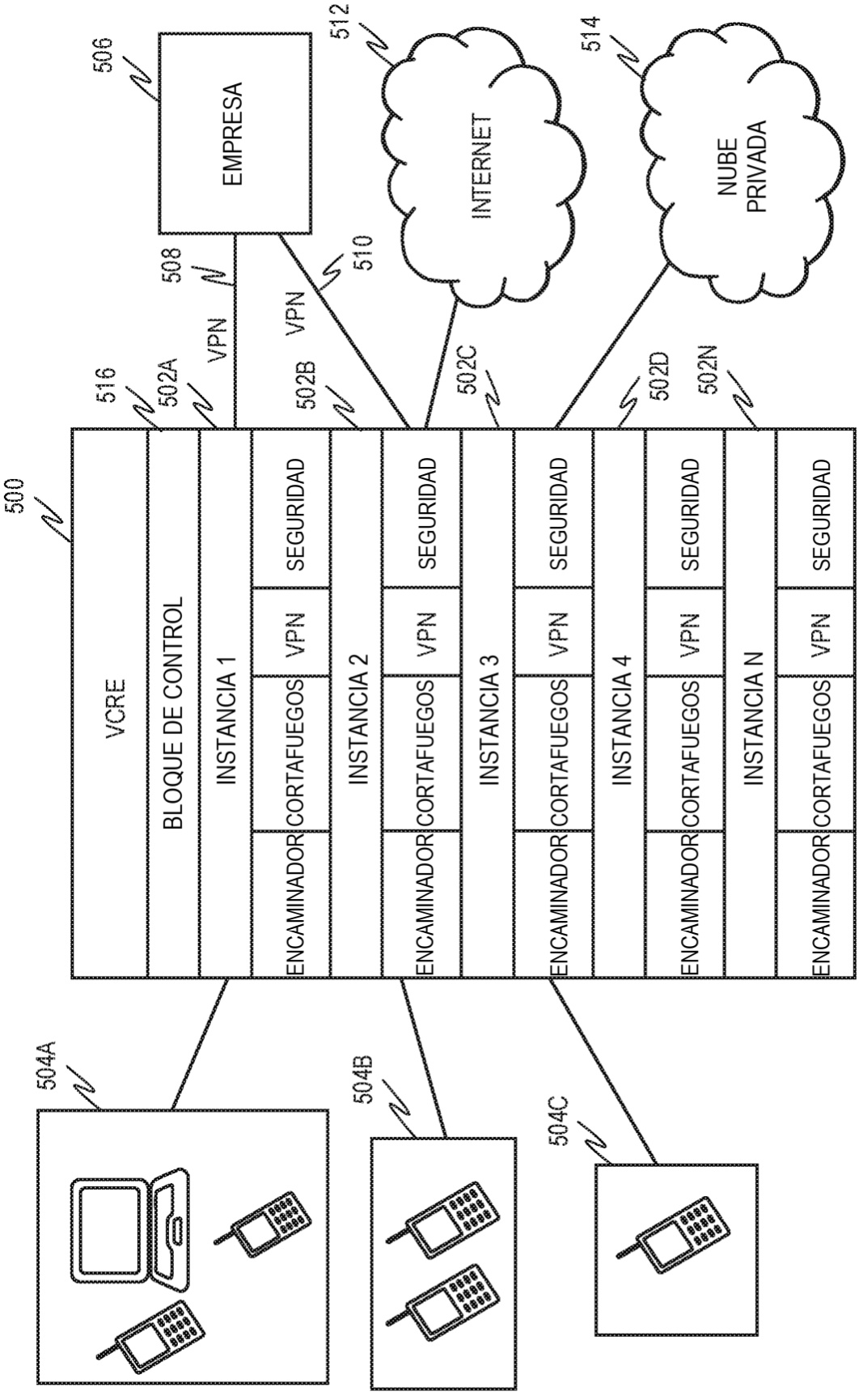
500
VCRE
BLOQUE DE CONTROL
INSTANCIA 1
INSTANCIA 2
INSTANCIA 3
INSTANCIA 4
INSTANCIA N
ENCAMINADOR
CORTAFUEGOS
VPN
SEGURIDAD
502A
502B
502C
502D
502N
516
504A
504B
504C
506
EMPRESA
508
510
512
INTERNET
514
NUBE PRIVADA
VPN
VPN

FIG. 5

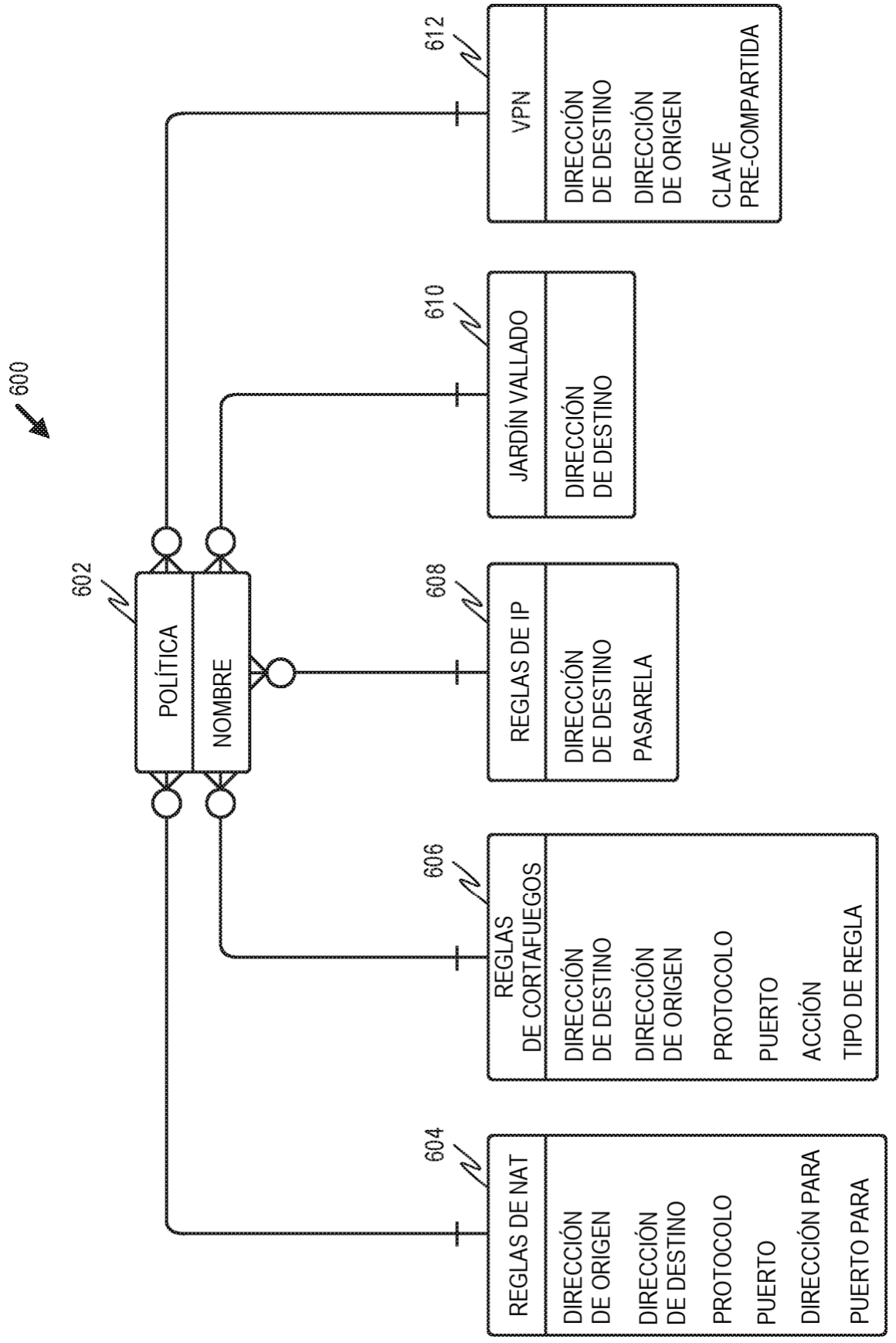
600
602
POLÍTICA
NOMBRE
604
REGLAS DE NAT
DIRECCIÓN DE ORIGEN
DIRECCIÓN DE DESTINO
PROTOCOLO
PUERTO
DIRECCIÓN PARA
PUERTO PARA
606
REGLAS DE CORTAFUEGOS
DIRECCIÓN DE DESTINO
DIRECCIÓN DE ORIGEN
PROTOCOLO
PUERTO
ACCIÓN
TIPO DE REGLA
608
REGLAS DE IP
DIRECCIÓN DE DESTINO
PASARELA
610
JARDÍN VALLADO
DIRECCIÓN DE DESTINO
612
VPN
DIRECCIÓN DE DESTINO
DIRECCIÓN DE ORIGEN
CLAVE PRE-COMPARTIDA

FIG. 6

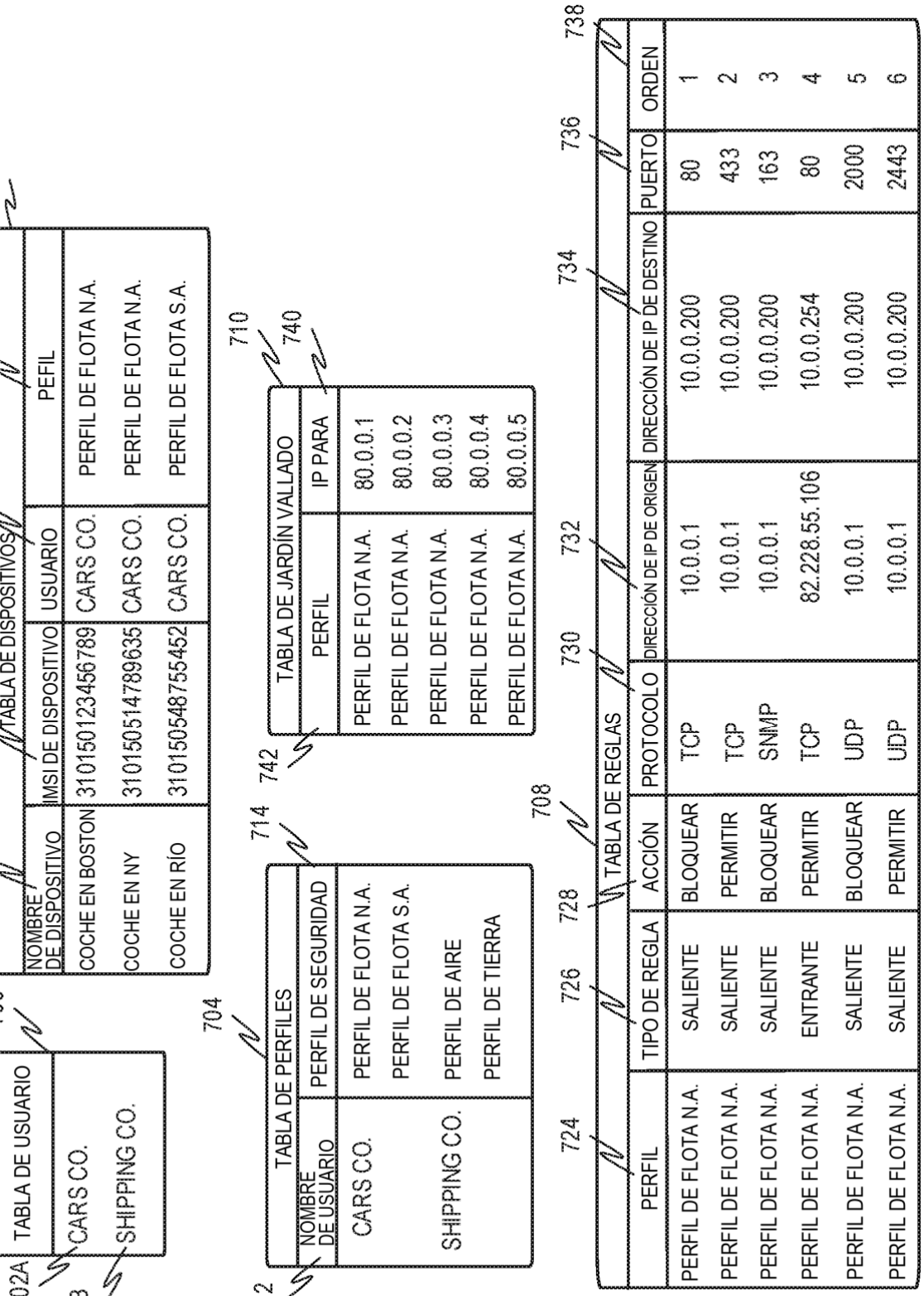
700
TABLA DE USUARIO
CARS CO.
SHIPPING CO.
702A
702B
704
TABLA DE PERFILES
NOMBRE DE USUARIO
PERFIL DE SEGURIDAD
CARS CO.
PERFIL DE FLOTA N.A.
PERFIL DE FLOTA S.A.
SHIPPING CO.
PERFIL DE AIRE
PERFIL DE TIERRA
706
TABLA DE DISPOSITIVOS
NOMBRE DE DISPOSITIVO
IMSI DE DISPOSITIVO
USUARIO
PEFIL
COCHE EN BOSTON
310150123456789
CARS CO.
PERFIL DE FLOTA N.A.
COCHE EN NY
310150514789635
CARS CO.
PERFIL DE FLOTA N.A.
COCHE EN RÍO
310150548755452
CARS CO.
PERFIL DE FLOTA S.A.
708
TABLA DE REGLAS
PERFIL
TIPO DE REGLA
ACCIÓN
PROTOCOLO
DIRECCIÓN DE IP DE ORIGEN
DIRECCIÓN DE IP DE DESTINO
PUERTO
ORDEN
PERFIL DE FLOTA N.A.
SALIENTE
BLOQUEAR
TCP
10.0.0.1
10.0.0.200
80
1
PERFIL DE FLOTA N.A.
SALIENTE
PERMITIR
TCP
10.0.0.1
10.0.0.200
433
2
PERFIL DE FLOTA N.A.
SALIENTE
BLOQUEAR
SNMP
10.0.0.1
10.0.0.200
163
3
PERFIL DE FLOTA N.A.
ENTRANTE
PERMITIR
TCP
82.228.55.106
10.0.0.254
80
4
PERFIL DE FLOTA N.A.
SALIENTE
BLOQUEAR
UDP
10.0.0.1
10.0.0.200
2000
5
PERFIL DE FLOTA N.A.
SALIENTE
PERMITIR
UDP
10.0.0.1
10.0.0.200
2443
6
710
TABLA DE JARDÍN VALLADO
PERFIL
IP PARA
PERFIL DE FLOTA N.A.
80.0.0.1
PERFIL DE FLOTA N.A.
80.0.0.2
PERFIL DE FLOTA N.A.
80.0.0.3
PERFIL DE FLOTA N.A.
80.0.0.4
PERFIL DE FLOTA N.A.
80.0.0.5
712
714
716
718
720
722
724
726
728
730
732
734
736
738
740
742

FIG. 7

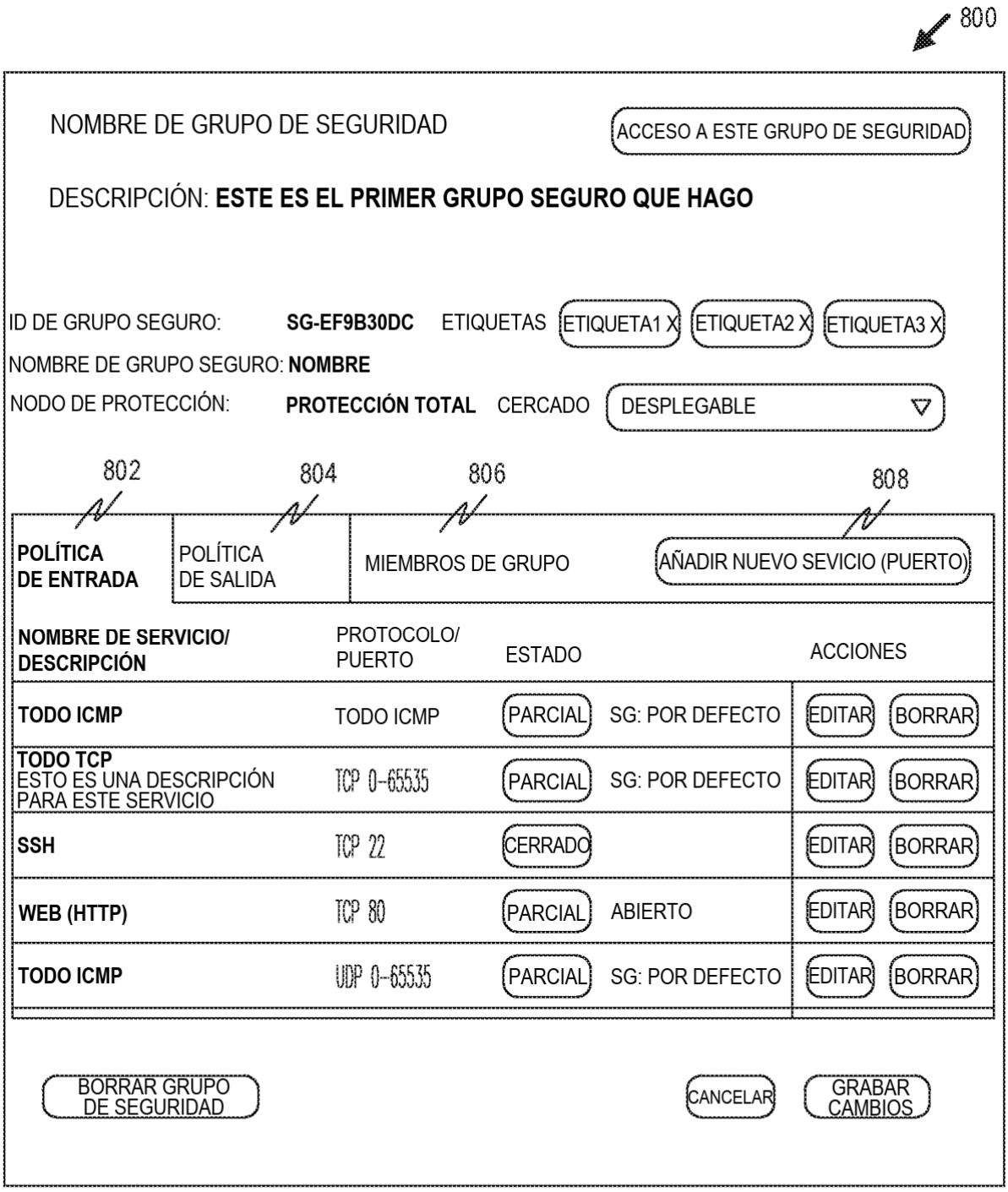
800
NOMBRE DE GRUPO DE SEGURIDAD
ACCESO A ESTE GRUPO DE SEGURIDAD
DESCRIPCIÓN: ESTE ES EL PRIMER GRUPO SEGURO QUE HAGO
ID DE GRUPO SEGURO: SG-EF9B30DC
ETIQUETAS
ETIQUETA1 X
ETIQUETA2 X
ETIQUETA3 X
NOMBRE DE GRUPO SEGURO: NOMBRE
NODO DE PROTECCIÓN: PROTECCIÓN TOTAL
CERCADO
DESPLEGABLE
802
804
806
808
POLÍTICA DE ENTRADA
POLÍTICA DE SALIDA
MIEMBROS DE GRUPO
AÑADIR NUEVO SEVICIO (PUERTO)
NOMBRE DE SERVICIO/ DESCRIPCIÓN
PROTOCOLO/ PUERTO
ESTADO
ACCIONES
TODO ICMP
TODO ICMP
PARCIAL
SG: POR DEFECTO
EDITAR
BORRAR
TODO TCP
ESTO ES UNA DESCRIPCIÓN PARA ESTE SERVICIO
TCP 0-65535
PARCIAL
SG: POR DEFECTO
EDITAR
BORRAR
SSH
TCP 22
CERRADO
EDITAR
BORRAR
WEB (HTTP)
TCP 80
PARCIAL
ABIERTO
EDITAR
BORRAR
TODO ICMP
UDP 0-65535
PARCIAL
SG: POR DEFECTO
EDITAR
BORRAR
BORRAR GRUPO DE SEGURIDAD
CANCELAR
GRABAR CAMBIOS

FIG. 8

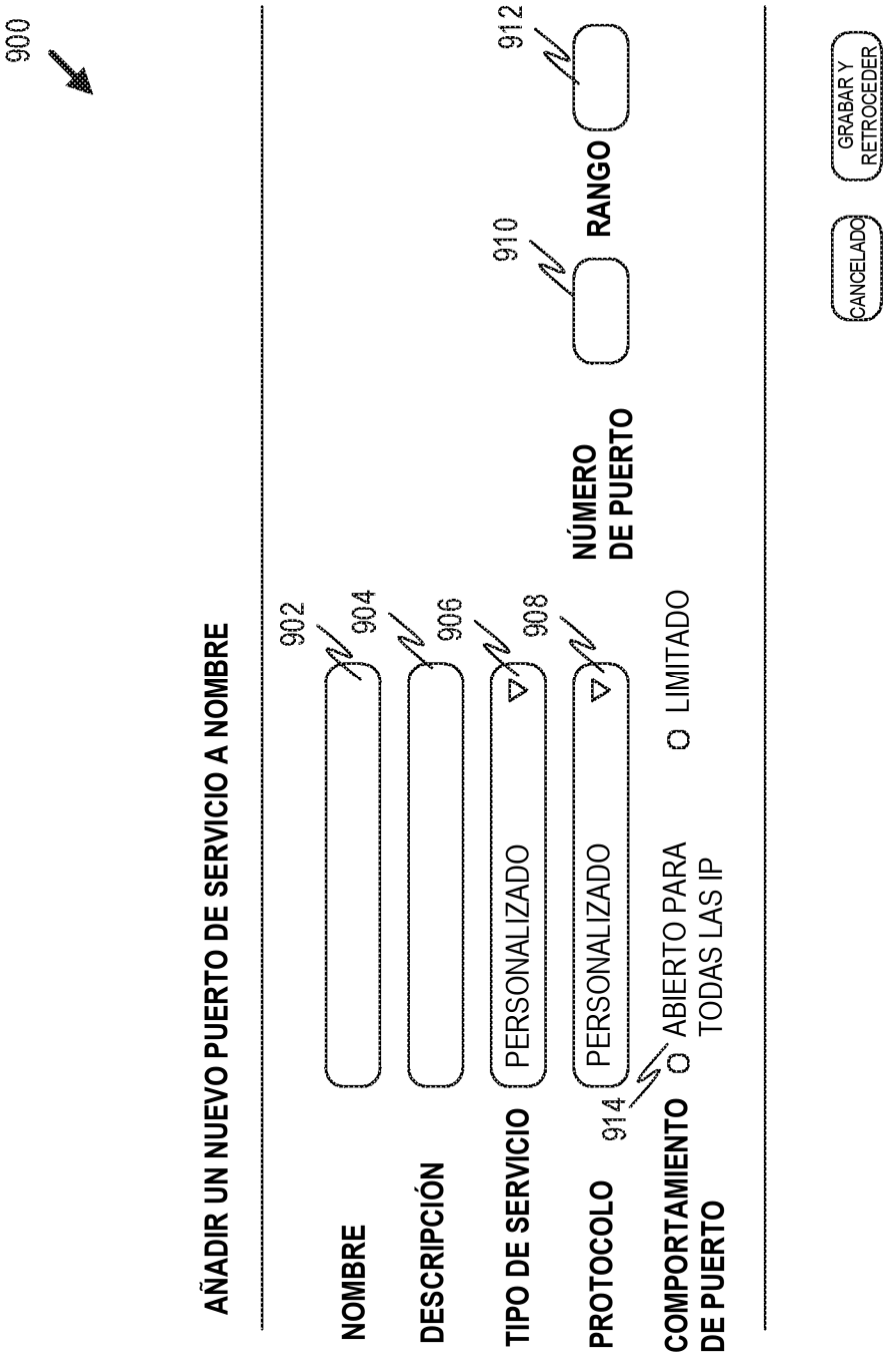
900
AÑADIR UN NUEVO PUERTO DE SERVICIO A NOMBRE
902
NOMBRE
904
DESCRIPCIÓN
906
TIPO DE SERVICIO
PERSONALIZADO
908
PROTOCOLO
PERSONALIZADO
914
COMPORTAMIENTO DE PUERTO
ABIERTO PARA TODAS LAS IP
LIMITADO
910
NÚMERO DE PUERTO
RANGO
912
CANCELADO
GRABAR Y RETROCEDER

FIG. 9

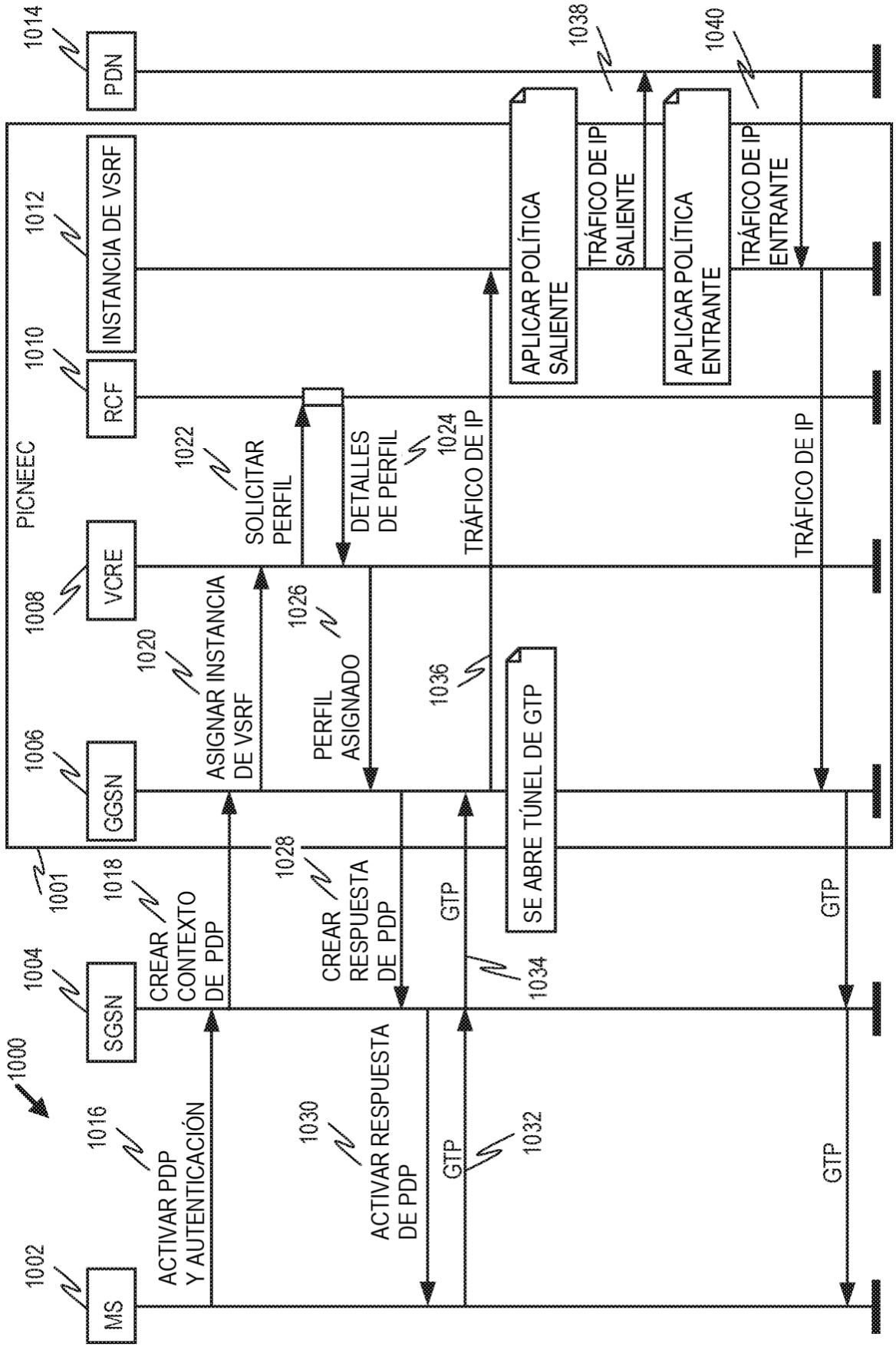
1000
1001
1002
MS
1004
SGSN
1006
GGSN
1008
VCRE
1010
RCF
1012
INSTANCIA DE VSRF
1014
PDN
PICNEEC
1016
ACTIVAR PDP Y AUTENTICACIÓN
1018
CREAR CONTEXTO DE PDP
1020
ASIGNAR INSTANCIA DE VSRF
1022
SOLICITAR PERFIL
1024
DETALLES DE PERFIL
1026
PERFIL ASIGNADO
1028
CREAR RESPUESTA DE PDP
1030
ACTIVAR RESPUESTA DE PDP
1032
GTP
1034
GTP
1036
SE ABRE TÚNEL DE GTP
1038
APLICAR POLÍTICA SALIENTE
TRÁFICO DE IP SALIENTE
1040
APLICAR POLÍTICA ENTRANTE
TRÁFICO DE IP ENTRANTE
TRÁFICO DE IP
TRÁFICO DE IP
GTP
GTP

FIG. 10

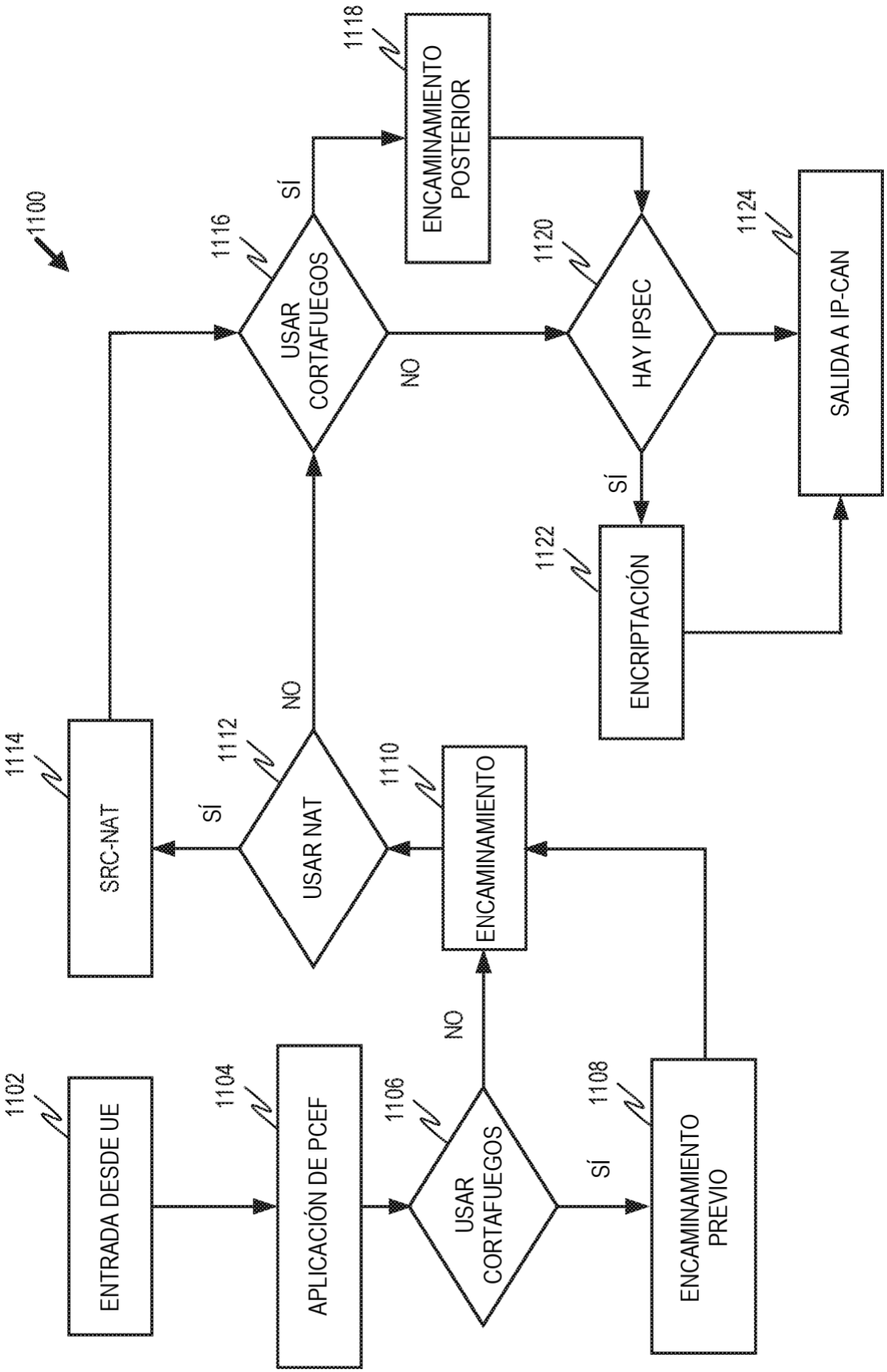
1100
1102
ENTRADA DESDE UE
1104
APLICACIÓN DE PCEF
1106
USAR CORTAFUEGOS
NO
SÍ
1108
ENCAMINAMIENTO PREVIO
1110
ENCAMINAMIENTO
1112
USAR NAT
NO
SÍ
1114
SRC-NAT
1116
USAR CORTAFUEGOS
NO
SÍ
1118
ENCAMINAMIENTO POSTERIOR
1120
HAY IPSEC
SÍ
1122
ENCRIPTACIÓN
1124
SALIDA A IP-CAN

FIG. 11

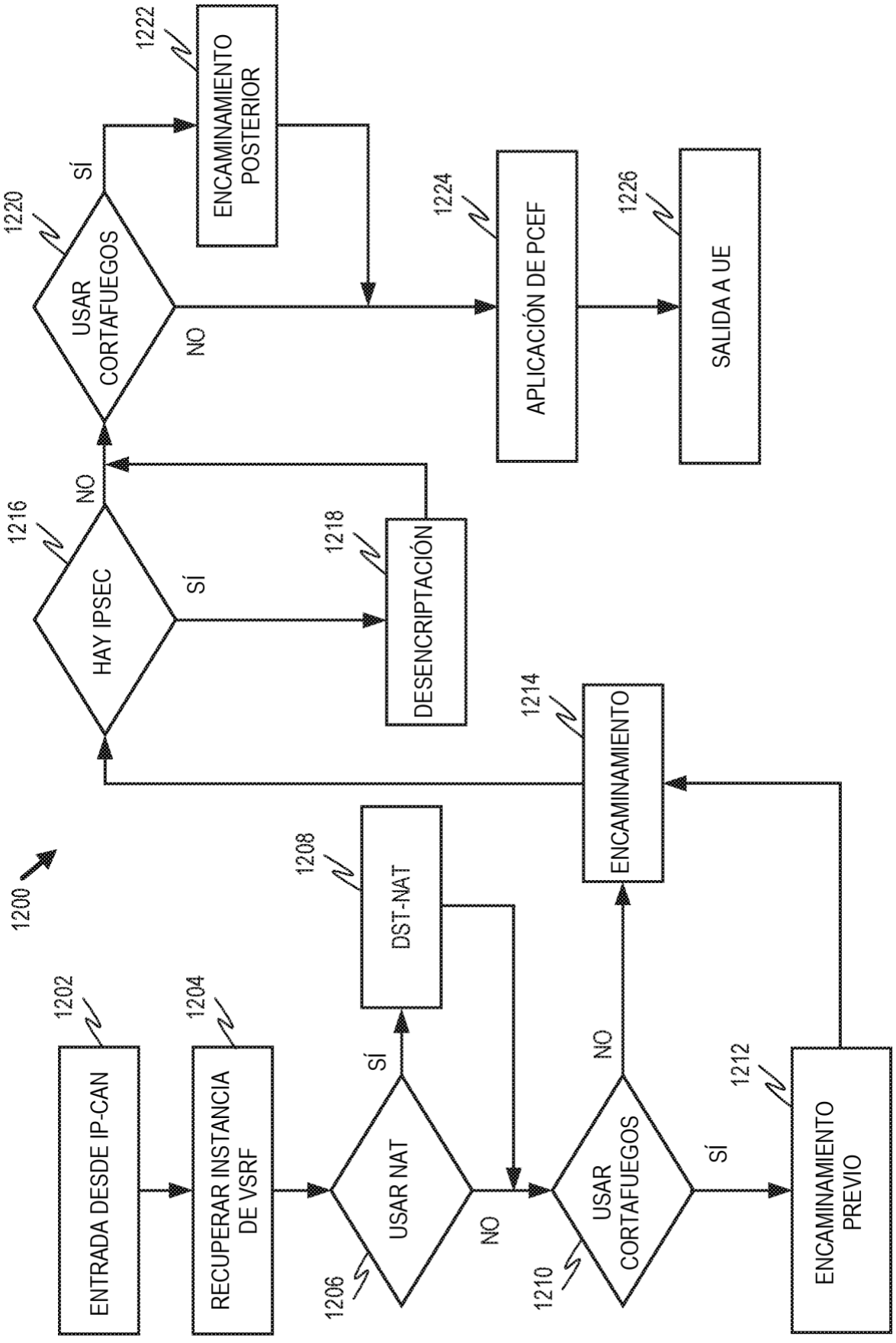
1200
1202
ENTRADA DESDE IP-CAN
1204
RECUPERAR INSTANCIA DE VSRF
1206
USAR NAT
SÍ
1208
DST-NAT
NO
1210
USAR CORTAFUEGOS
NO
1212
ENCAMINAMIENTO PREVIO
SÍ
1214
ENCAMINAMIENTO
1216
HAY IPSEC
NO
SÍ
1218
DESENCRIPTACIÓN
1220
USAR CORTAFUEGOS
SÍ
1222
ENCAMINAMIENTO POSTERIOR
NO
1224
APLICACIÓN DE PCEF
1226
SALIDA A UE

FIG. 12

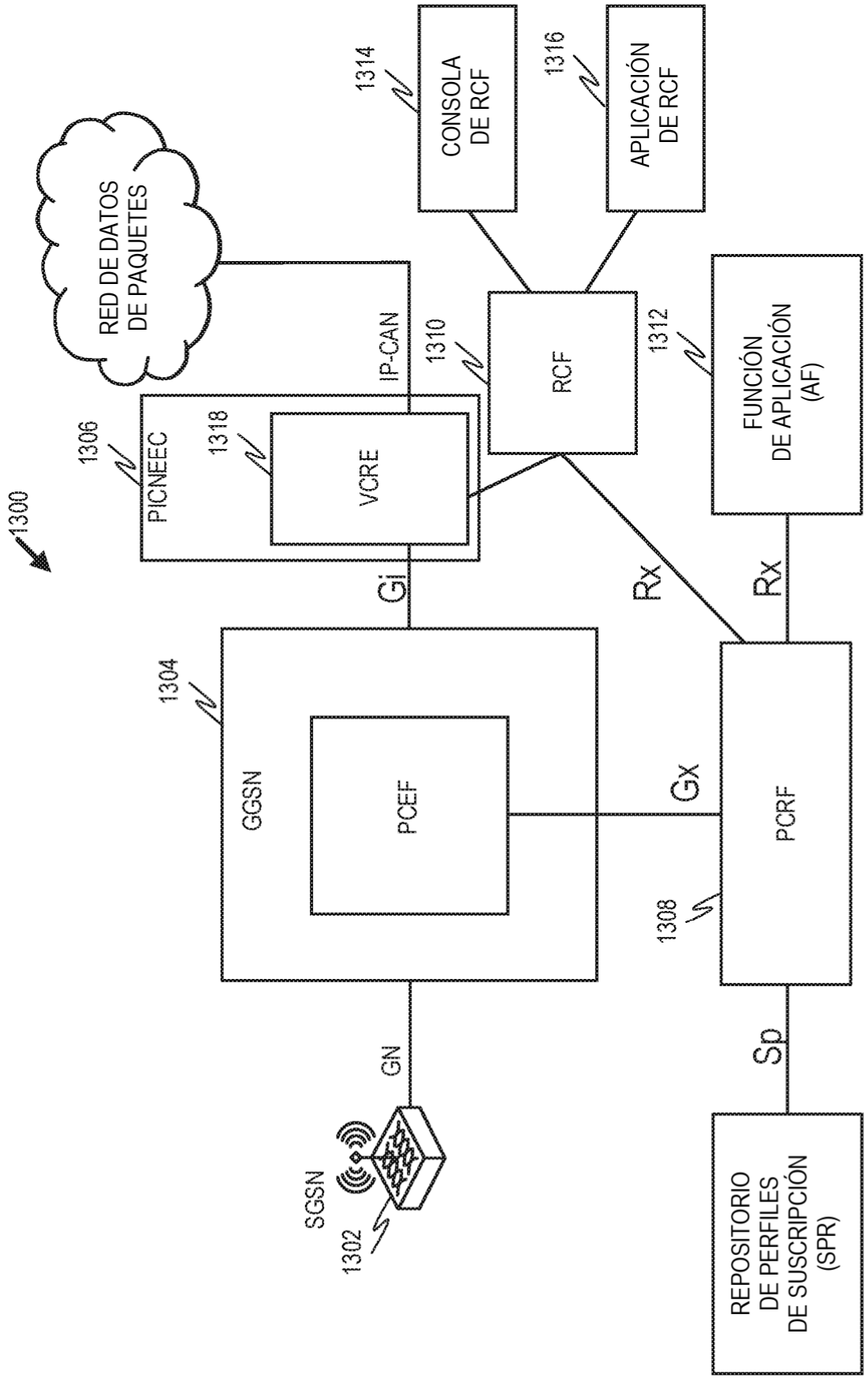
1300
RED DE DATOS DE PAQUETES
1314
CONSOLA DE RCF
1316
APLICACIÓN DE RCF
IP-CAN
1310
RCF
1312
FUNCIÓN DE APLICACIÓN (AF)
1306
PICNEEC
1318
VCRE
Gi
Rx
Rx
1304
GGSN
PCEF
Gx
PCRF
1308
GN
SGSN
1302
Sp
REPOSITORIO DE PERFILES DE SUSCRIPCIÓN (SPR)

FIG. 13

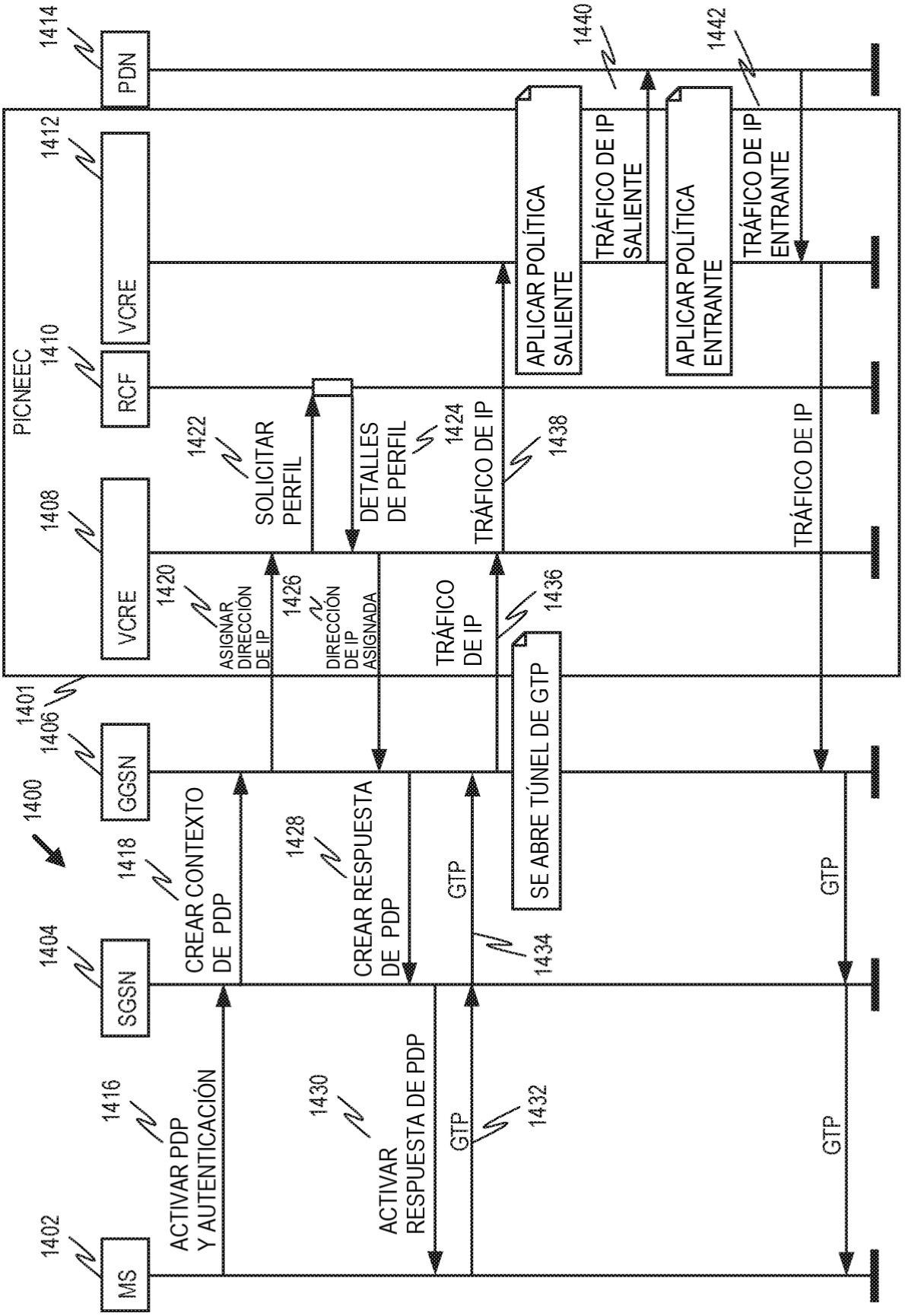
1400
1401
PICNEEC
MS
1402
SGSN
1404
GGSN
1406
VCRE
1408
RCF
1410
VCRE
1412
PDN
1414
ACTIVAR PDP Y AUTENTICACIÓN
1416
CREAR CONTEXTO DE PDP
1418
ASIGNAR DIRECCIÓN DE IP
1420
SOLICITAR PERFIL
1422
DETALLES DE PERFIL
1424
DIRECCIÓN DE IP ASIGNADA
1426
CREAR RESPUESTA DE PDP
1428
ACTIVAR RESPUESTA DE PDP
1430
GTP
1432
GTP
1434
TRÁFICO DE IP
1436
SE ABRE TÚNEL DE GTP
TRÁFICO DE IP
1438
APLICAR POLÍTICA SALIENTE
1440
TRÁFICO DE IP SALIENTE
APLICAR POLÍTICA ENTRANTE
1442
TRÁFICO DE IP ENTRANTE
GTP
GTP
TRÁFICO DE IP

FIG. 14

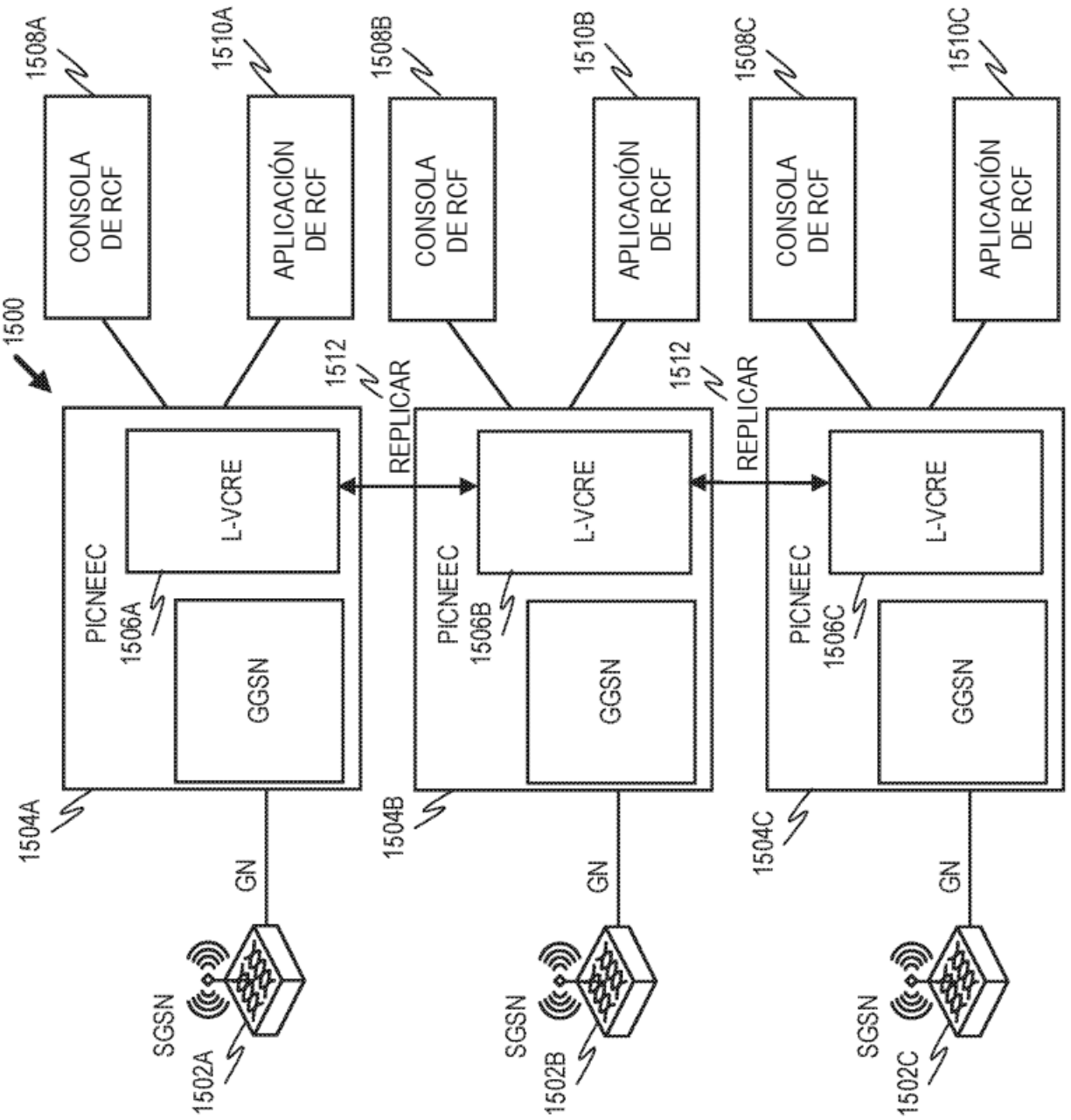
1500
1508A
CONSOLA DE RCF
1510A
APLICACIÓN DE RCF
1508B
CONSOLA DE RCF
1510B
APLICACIÓN DE RCF
1508C
CONSOLA DE RCF
1510C
APLICACIÓN DE RCF
1512
REPLICAR
1512
REPLICAR
PICNEEC
1506A
L-VCRE
GGSN
1504A
PICNEEC
1506B
L-VCRE
GGSN
1504B
PICNEEC
1506C
L-VCRE
GGSN
1504C
GN
GN
GN
SGSN
1502A
SGSN
1502B
SGSN
1502C

FIG. 15

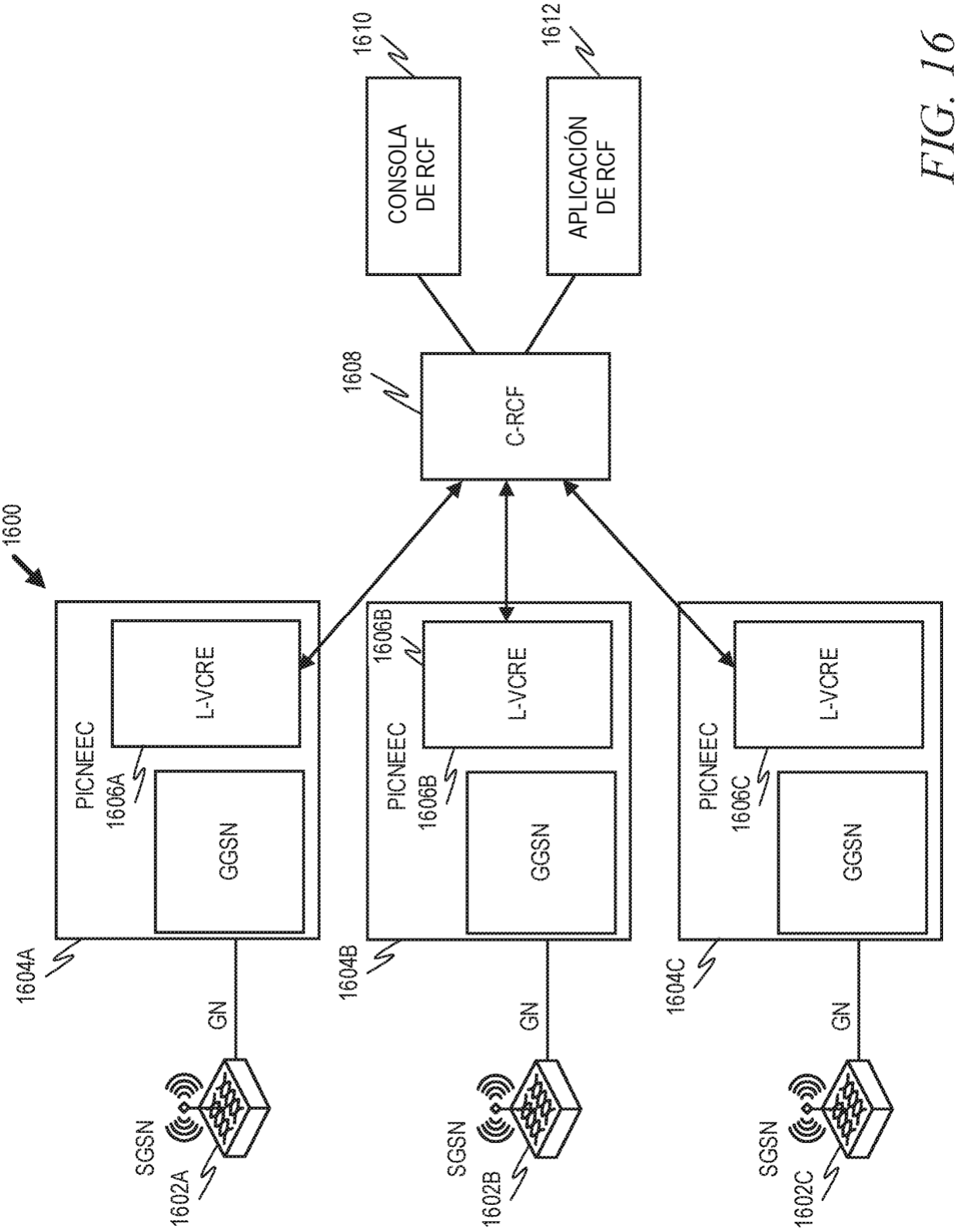
1600
1610
CONSOLA DE RCF
1612
APLICACIÓN DE RCF
1608
C-RCF
PICNEEC
1606A
L-VCRE
GGSN
1604A
GN
SGSN
1602A
1606B
1604B
1602B
1606C
1604C
1602C

FIG. 16

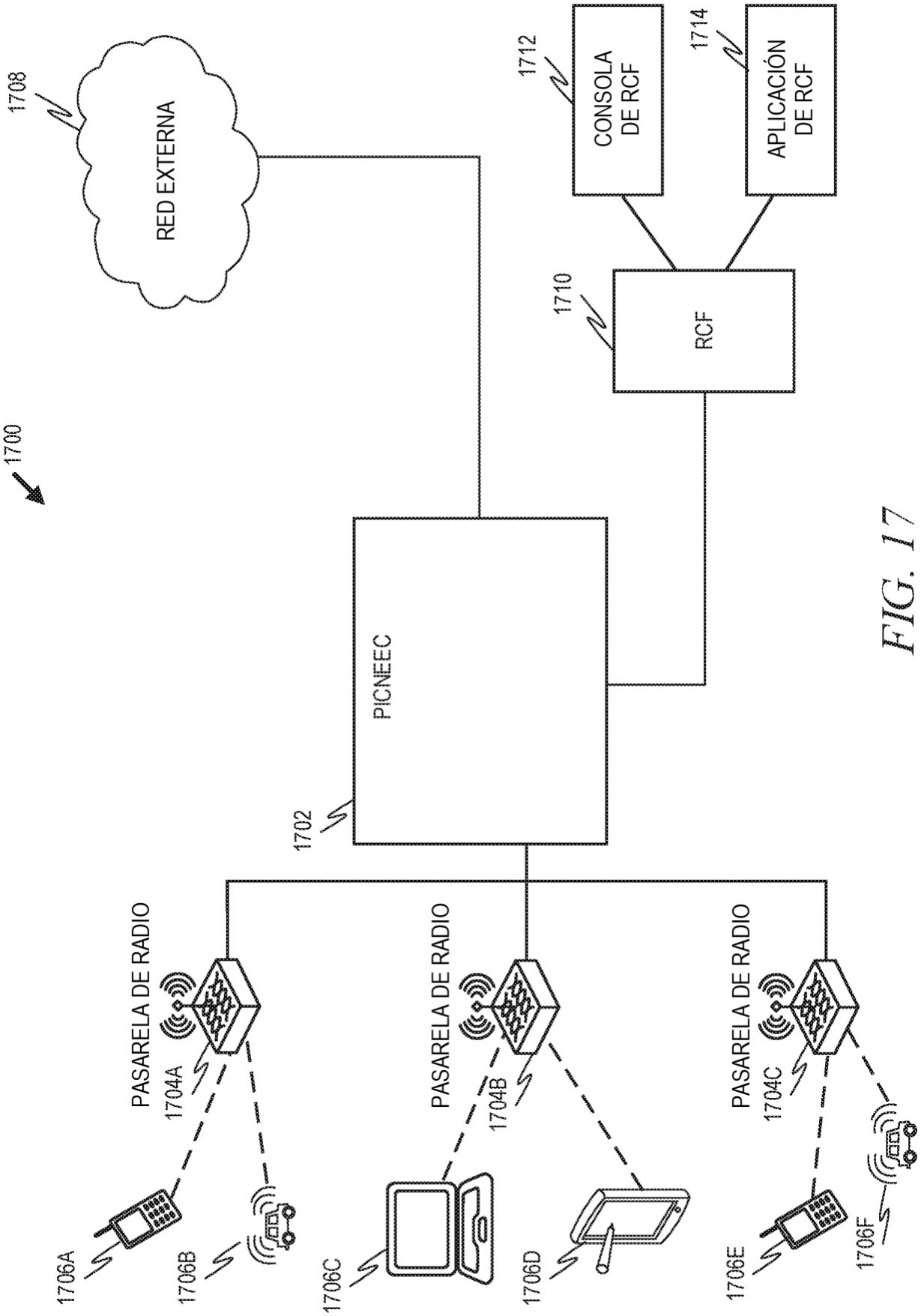
1700
1708
RED EXTERNA
1712
CONSOLA DE RCF
1714
APLICACIÓN DE RCF
1710
RCF
1702
PICNEEC
PASARELA DE RADIO
1704A
PASARELA DE RADIO
1704B
PASARELA DE RADIO
1704C
1706A
1706B
1706C
1706D
1706E
1706F

FIG. 17

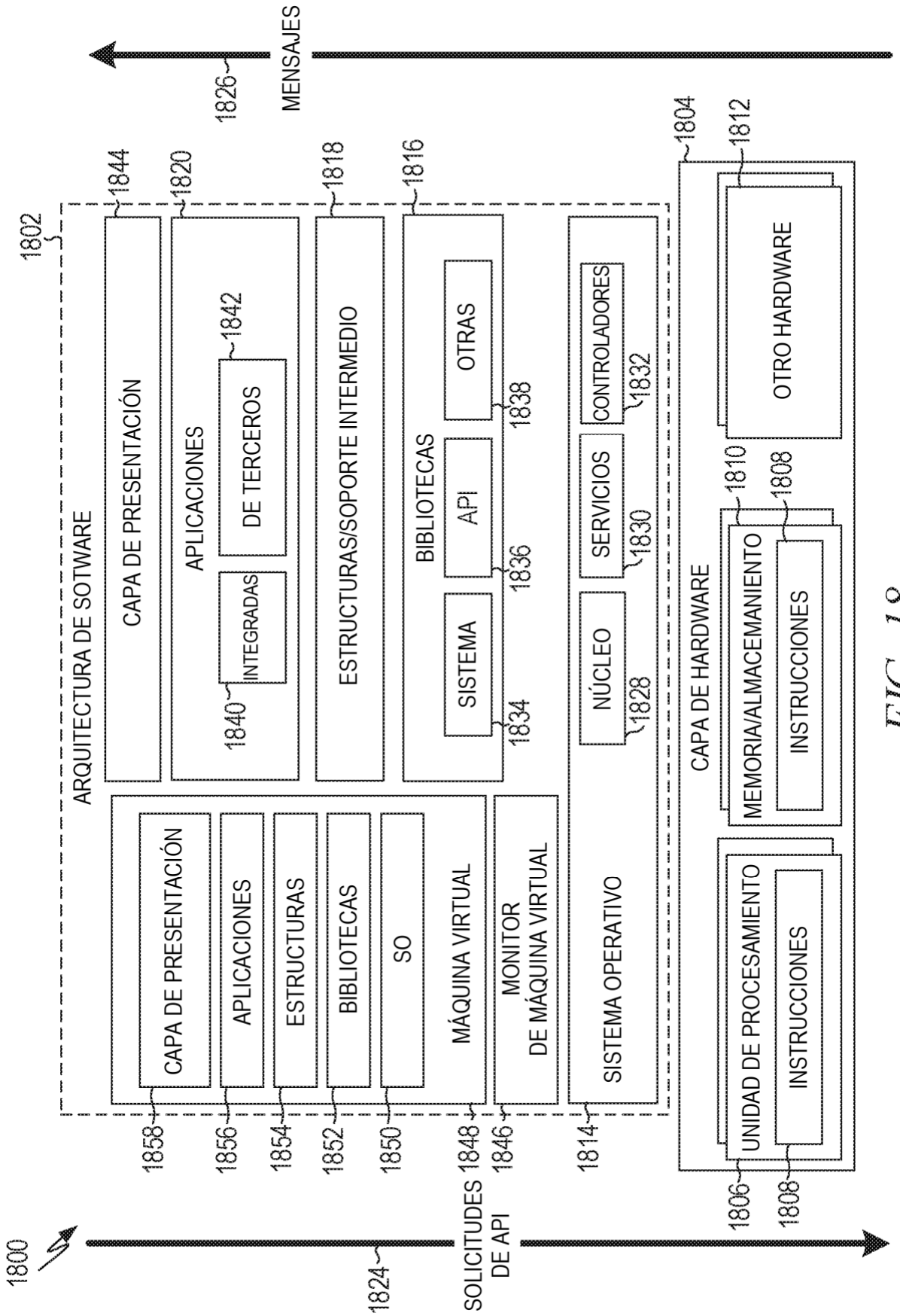
1800
1802
ARQUITECTURA DE SOTWARE
1826
MENSAJES
1824
SOLICITUDES DE API
CAPA DE PRESENTACIÓN
1858
APLICACIONES
1856
ESTRUCTURAS
1854
BIBLIOTECAS
1852
SO
1850
MÁQUINA VIRTUAL
1848
MONITOR DE MÁQUINA VIRTUAL
1846
SISTEMA OPERATIVO
1814
1844
CAPA DE PRESENTACIÓN
1820
APLICACIONES
1840
INTEGRADAS
1842
DE TERCEROS
1818
ESTRUCTURAS/SOPORTE INTERMEDIO
1816
BIBLIOTECAS
SISTEMA
1834
API
1836
OTRAS
1838
NÚCLEO
1828
SERVICIOS
1830
CONTROLADORES
1832
1804
CAPA DE HARDWARE
1806
UNIDAD DE PROCESAMIENTO
1808
INSTRUCCIONES
1810
MEMORIA/ALMACEMANIENTO
1808
INSTRUCCIONES
1812
OTRO HARDWARE

FIG. 18

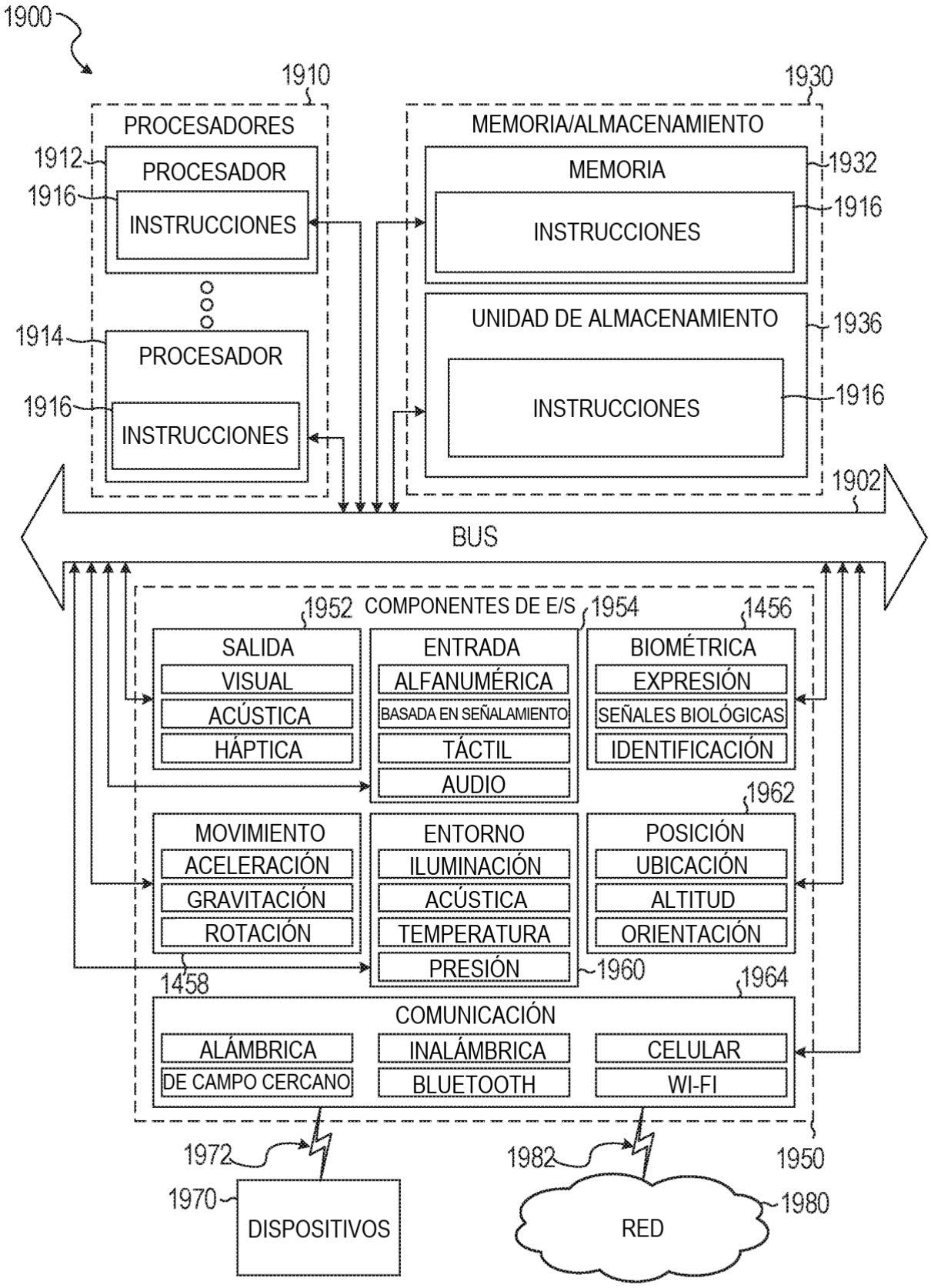
1900
1910
PROCESADORES
1912
PROCESADOR
1916
INSTRUCCIONES
1914
PROCESADOR
1916
INSTRUCCIONES
1930
MEMORIA/ALMACENAMIENTO
MEMORIA
1932
1916
INSTRUCCIONES
UNIDAD DE ALMACENAMIENTO
1936
1916
INSTRUCCIONES
1902
BUS
1952 COMPONENTES DE E/S
1954
1456
SALIDA
VISUAL
ACÚSTICA
HÁPTICA
ENTRADA
ALFANUMÉRICA
BASADA EN SEÑALAMIENTO
TÁCTIL
AUDIO
BIOMÉTRICA
EXPRESIÓN
SEÑALES BIOLÓGICAS
IDENTIFICACIÓN
1962
MOVIMIENTO
ACELERACIÓN
GRAVITACIÓN
ROTACIÓN
ENTORNO
ILUMINACIÓN
ACÚSTICA
TEMPERATURA
PRESIÓN
1960
POSICIÓN
UBICACIÓN
ALTITUD
ORIENTACIÓN
1458
1964
COMUNICACIÓN
ALÁMBRICA
DE CAMPO CERCANO
INALÁMBRICA
BLUETOOTH
CELULAR
WI-FI
1950
1972
1970
DISPOSITIVOS
1982
RED
1980

FIG. 19