(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 617 478**

(51) Int. CI.:

H04L 12/70 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **04.11.2011 PCT/CN2011/081824**

(87) Fecha y número de publicación internacional: **19.07.2012 WO2012094919**

(96) Fecha de presentación y número de la solicitud europea: **04.11.2011 E 11855857 (6)**

(97) Fecha y número de publicación de la concesión europea: **21.12.2016 EP 2651080**

(54) Título: **Procedimiento y sistema de control de políticas**

(30) Prioridad:

14.01.2011 CN 201110008179

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
19.06.2017

(73) Titular/es:

ZTE CORPORATION (100.0%)
ZTE Plaza, Keji Road South, Hi-Tech Industrial Park, Nanshan District
Shenzhen, Guangdong 518057, CN

(72) Inventor/es:

ZHOU, XIAOYUN;
ZONG, ZAIFENG y
BI, YIFENG

(74) Agente/Representante:

DURÁN MOYA, Luis Alfonso

DESCRIPCIÓN

Procedimiento y sistema de control de políticas

Sector técnico

El presente documento se refiere a una técnica de control de políticas en la interconexión del 3GPP y el foro de banda ancha (Broadband Forum, BBF), y particularmente, a un procedimiento y a un sistema para el control de políticas.

Antecedentes de la técnica relacionada

La figura 1 es un diagrama esquemático de la arquitectura de componentes del Sistema de paquetes evolucionado (Evolved Packet System, EPS) del Proyecto de asociación de tercera generación (3rd Generation Partnership Project, 3GPP), y en una arquitectura de red EPS en un escenario sin itinerancia mostrada en la figura 1, se incluyen una Red de acceso radioeléctrico terrestre universal evolucionada (Evolved Universal Terrestrial Radio Access Network, E-UTRAN), una Entidad de gestión de la movilidad (Mobility Management Entity, MME), una Pasarela de servicio (Serving Gateway, S-GW), una Pasarela de red de datos por paquetes (Packet Data Network Gateway, P-GW, denominada asimismo PDN GW), un Servidor local de abonado (Home Subscriber Server, HSS), una entidad de la Función de reglas de políticas y tarificación (Policy and Charging Rules Function, PCRF) y otros nodos de soporte.

Donde, una PCRF es un núcleo de Control de políticas y tarificación (Policy and Charging Control, PCC) y es responsable de elaborar las reglas de PCC. La PCRF proporciona reglas de control de red basándose en el flujo de datos del servicio, estos controles de red incluyen la detección del flujo de datos del servicio, el control de la activación, el control de la calidad de servicio (Quality of Service, QoS) y las reglas de tarificación basándose en el flujo de datos y similares. La PCRF envía las reglas de PCC elaboradas por la PCRF a una Función de aplicación de políticas y tarificación (Policy and Charging Enforcement Function, PCEF) para su ejecución, requiriéndose al mismo tiempo que la PCRF garantice asimismo que estas reglas son coherentes con la información de suscripción del usuario. Una base para que la PCRF elabore las reglas de PCC incluye: obtener información relativa a los servicios a partir de una función de solicitud (Application Function, AF); la obtención de información de suscripción del PCC de usuario a partir de un Repositorio de perfiles de suscripción (Subscription Profile Repository, SPR); y la obtención de información de red relativa a la portadora a partir de la PCEF.

El EPS soporta una interconexión entre el EPS y un sistema no 3GPP, la interconexión entre el EPS y el sistema no 3GPP se implementa a través de interfaces S2a/b/c, y la P-GW se utiliza como un nexo entre el sistema 3GPP y el sistema no 3GPP. Tal como se muestra en la figura 1, el sistema no 3GPP está dividido en un acceso IP fiable no 3GPP y un acceso IP no fiable no 3GPP. El acceso IP fiable no 3GPP puede estar conectado a la P-GW directamente a través de una interfaz S2a; se requiere que el acceso IP no fiable no 3GPP se conecte a la P-GW a través de una Pasarela de datos por paquetes evolucionada (Evolved Packet Data Gateway, ePDG), una interfaz entre la ePDG y la P-GW es una interfaz S2b, y se adopta un Protocolo seguridad de Internet (Internet Protocol Security, IPSec) para llevar a cabo la protección mediante cifrado de las señalizaciones y los datos entre un equipo de usuario (User Equipment, UE) y la ePDG. Una interfaz S2c proporciona soporte de control y movilidad relativo a un plano de usuario entre el equipo de usuario (UE) y la P-GW, y un protocolo de gestión de la movilidad soportado por la interfaz S2c es un soporte IPv6 móvil para anfitriones y encaminadores de doble pila (DSMIPv6).

En la actualidad, muchos operadores prestan atención a la Convergencia fijo-móvil (Fixed Mobile Convergence, FMC) y llevan a cabo investigaciones relacionadas con la interconexión del 3GPP y el foro de banda ancha (BBF). Con respecto a un escenario en el que un usuario accede a una red troncal móvil a través de un BBF, es necesario garantizar la QoS en toda la ruta de transmisión de los datos (los datos se transmitirán a través de una red fija y una red móvil). En la actualidad, se lleva a cabo una interacción a través de la PCRF y una Estructura de control de políticas de banda ancha (Broadband Policy Control Framework, BPCF) en el acceso del BBF para garantizar la QoS. La BPCF es una estructura de control de políticas en el acceso del BBF, y para el mensaje de petición de recursos de la PCRF, la BPCF lleva a cabo el control de admisión de recursos o planifica el mensaje de petición de recursos a otros elementos de red (es decir, una Pasarela de red de banda ancha (Broadband Network Gateway, BNG)) de una red de acceso del BBF de acuerdo con las políticas de red, la información de suscripción y similares del acceso del BBF, y los otros elementos de red ejecutan el control de admisión de recursos (es decir, confiando en los otros elementos de red para ejecutar el control de admisión de recursos). Por ejemplo, cuando el UE accede a una red troncal 3GPP a través de una Red inalámbrica de área local (Wireless Local Area Network, WLAN), para garantizar que la demanda total de ancho de banda de todos los servicios de acceso del UE que accede a través de una línea de acceso WLAN no supera el ancho de banda de la línea (por ejemplo, el ancho de banda de la suscripción o un agente físico máximo soportado por la línea), se requiere que la PCRF interactúe con la BPCF cuando lleva a cabo la autorización de la QoS, de manera que la red de acceso del BBF ejecute el control de admisión de recursos.

En la actualidad, el estudio de la interconexión del 3GPP y el BBF incluye principalmente dos aspectos: un escenario en el que el UE del 3GPP accede a un Núcleo de paquetes evolucionado (Evolved Packet Core, EPC) a través de la WLAN del BBF y un escenario en el que el UE del 3GPP accede a la red troncal 3GPP a través de un nodo-B evolucionado local (H(e)NB), donde el H(e)NB toma la red de acceso del BBF como una ruta de encaminamiento (red de retorno) para conectarse a la red troncal 3GPP.

La figura 2 es un diagrama esquemático de un UE del 3GPP que accede a la red troncal 3GPP a través de la WLAN y, tal como se muestra en la figura 2, la red de acceso del BBF se toma como un acceso no fiable no 3GPP. Basándose en la arquitectura mostrada en la figura 2, en la actualidad hay 3 formas de iniciar un establecimiento de sesión de interconexión de políticas (es decir, S9*).

En la forma 1, después de que el UE accede a la red de acceso del BBF, un Servidor de acceso remoto de banda ancha (Broadband Remote Access Server, BRAS)/Pasarela de red de banda ancha (Broadband Network Gateway, BNG) ejecutará una autenticación de acceso basándose en el 3GPP y, al mismo tiempo, la BPCF del BBF inicia activamente una sesión S9* para interactuar con la PCRF del 3GPP. Por lo tanto, la PCRF puede interactuar con la BPCF al llevar a cabo la autorización de la QoS, y la BPCF ejecuta el control de admisión de recursos o confía en otros elementos de red para ejecutar el control de admisión de recursos.

En la forma 2, cuando el UE accede a la red de acceso del BBF, no se ejecuta la autenticación de acceso basada en el 3GPP. Después de que el UE interactúa con la ePDG para establecer un túnel IPSec, la ePDG envía una dirección local del UE (es decir, una dirección asignada al UE por la red de acceso del BBF) a la P-GW, a continuación la P-GW envía la dirección local del UE a la PCRF, y después de determinar la BPCF de acuerdo con la dirección local del UE, la PCRF inicia inversamente un establecimiento de sesión S9* para llevar a cabo una interacción con la BPCF. Por lo tanto, la PCRF puede interactuar con la BPCF al llevar a cabo la autorización de la QoS, y la BPCF ejecuta el control de admisión de recursos o confía en otros elementos de red para ejecutar el control de admisión de recursos.

En la forma 3, cuando el UE accede a la red de acceso del BBF, no se ejecuta la autenticación de acceso basada en el 3GPP. Después de que el UE interactúa con la ePDG para establecer un túnel IPSec, la ePDG envía directamente una dirección local del UE (es decir, una dirección asignada al UE por la red de acceso del BBF) a la PCRF, y después de determinar la BPCF de acuerdo con la dirección local del UE, la PCRF inicia inversamente un establecimiento de sesión S9* para llevar a cabo una interacción con la BPCF. Por lo tanto, la PCRF puede interactuar con la BPCF al llevar a cabo la autorización de la QoS, y la BPCF ejecuta el control de admisión de recursos o confía en otros elementos de red para ejecutar el control de admisión de recursos.

Si el UE necesita que la red asigne recursos al UE cuando el UE lleva a cabo el acceso al servicio, la PCRF envía en primer lugar la información de la QoS de las reglas de PCC elaboradas a la BPCF, para que la red de acceso del BBF ejecute el control de admisión. A continuación, la PCRF envía a la PCEF una regla del PCC aceptada por la red de acceso del BBF. La PCEF lleva a cabo un marcado de Punto de código de servicios diferenciados (Differentiated Services Code Point, DSCP) en una cabecera de un paquete IP de un flujo de datos correspondiente (denominada una cabecera interna de paquete) de acuerdo con la regla del PCC, cuando los paquetes IP del flujo de datos del servicio llegan a la ePDG, la ePDG llevará a cabo la encapsulación IPSec en el paquete IP y llevará a cabo el marcado en una cabecera de un paquete IP del IPSec (denominada una cabecera externa de paquete) de acuerdo con un DSCP de la cabecera del paquete IP (es decir, la cabecera interna de paquete) durante la encapsulación. Por lo tanto, la red de acceso del BBF puede llevar a cabo la planificación de los paquetes de datos de acuerdo con un DSCP de la cabecera del paquete IP del IPSec.

Sin embargo, una premisa del esquema anterior es que la red 3GPP soporte una interconexión entre la red 3GPP y el BBF, cuando la PCRF no soporta una interconexión entre la PCRF y el BBF (incluyendo un escenario en el que el PCC no está implementado en la red 3GPP), la PCRF no interactuará con la BPCF para solicitar el control de admisión. De este modo, esto hará que las reglas de PCC enviadas por la PCRF a la PCEF sean resultados que se decidan de acuerdo con la propia PCRF. La PCEF lleva a cabo el marcado DSCP en las cabeceras de los paquetes IP de los flujos de datos del servicio de acuerdo con las reglas de PCC enviadas por la PCRF o las políticas configuradas localmente por la PCEF (con respecto a un escenario en el que el PCC no está implementado en la red 3GPP). Cuando estos flujos de datos del servicio llegan a la ePDG, la ePDG replica el DSCP de la cabecera externa de paquete del IPSec de acuerdo con las marcas del DSCP de la cabecera interna de paquete. Si estos datos llegan a la red de acceso del BBF, la red de acceso del BBF no distinguirá si estos flujos de datos del servicio pasan por el control de admisión de la red de acceso del BBF, sino que solamente llevará a cabo el envío de acuerdo con el DSCP. De este modo, estos flujos de datos del servicio que no pasan por el control de admisión ocuparán recursos de otros flujos de datos del servicio que pasen por el control de admisión, lo que actualmente conduce a un fallo de todo el mecanismo de control de políticas de FMC.

Cuando el UE accede a 3GPP a través de una red de acceso no fiable que no es BBF utilizando un protocolo DSMIPv6, en la actualidad hay 2 formas de iniciar un establecimiento de sesión de interconexión de políticas (es decir, S9*).

En la forma 1, después de que el UE accede a la red de acceso del BBF, el BRAS/BNG ejecutará una autenticación de acceso basada en el 3GPP y, al mismo tiempo, la BPCF del BBF inicia activamente una sesión S9* para interactuar con la PCRF del 3GPP. Por lo tanto, la PCRF puede interactuar con la BPCF cuando lleva a cabo la autorización de la QoS, y la BPCF ejecuta el control de admisión de recursos o confía en otros elementos de red para ejecutar el control de admisión de recursos.

En la forma 2, cuando el UE accede a la red de acceso del BBF, no se ejecuta la autenticación de acceso basada en el 3GPP. Después de que el UE interactúa con la ePDG para establecer un túnel IPSec, la ePDG envía directamente una dirección local del UE (es decir, una dirección asignada al UE por la red de acceso del BBF) a la PCRF, y después de determinar la BPCF de acuerdo con la dirección local del UE, la PCRF inicia inversamente un establecimiento de sesión S9* para llevar a cabo una interacción con la BPCF. Por lo tanto, la PCRF puede interactuar con la BPCF al llevar a cabo la autorización de la QoS, y la BPCF ejecuta el control de admisión de recursos o confía en otros elementos de red para ejecutar el control de admisión de recursos.

Si el UE requiere que la red asigne recursos al UE cuando el UE lleva a cabo el acceso al servicio, la PCRF envía en primer lugar la información de la QoS de las reglas de PCC elaboradas a la BPCF, para que la red de acceso del BBF ejecute el control de admisión. A continuación, la PCRF envía a la PCEF una regla del PCC aceptada por la red de acceso del BBF. La PCEF lleva a cabo el marcado DSCP en una cabecera de un paquete IP de un flujo de datos correspondiente (denominada cabecera interna de paquete) de acuerdo con la regla del PCC, cuando los paquetes IP del flujo de datos del servicio llegan a la ePDG, la ePDG llevará a cabo la encapsulación IPSec en el paquete IP y llevará a cabo el marcado en una cabecera de un paquete IP de un IPSec (denominada cabecera externa de paquete) de acuerdo con un DSCP de la cabecera del paquete IP (es decir, la cabecera interna de paquete) durante la encapsulación. Por lo tanto, la red de acceso del BBF puede llevar a cabo la planificación de los paquetes de datos de acuerdo con un DSCP de la cabecera del paquete IP del IPSec.

De igual modo, una premisa del esquema anterior es que la red 3GPP soporte una interconexión entre la red 3GPP y el BBF, cuando la PCRF no soporta una interconexión entre la PCRF y el BBF (incluyendo un escenario en el que el PCC no está implementado en la red 3GPP), la PCRF no interactuará con la BPCF para solicitar el control de admisión. Los flujos de datos del servicio que no pasan por el control de admisión ocuparán recursos de otros flujos de datos del servicio que pasan por el control de admisión, lo que actualmente conduce un fallo de todo el mecanismo de control de políticas de FMC.

Cuando el UE accede a 3GPP a través de una red de acceso fiable que no es BBF utilizando un protocolo DSMIPv6, también hay 2 formas para iniciar un establecimiento de sesión de interconexión de políticas (es decir, S9*) en la técnica relacionada.

En la forma 1, después de que el UE accede a la red de acceso del BBF, el BRAS/BNG ejecutará una autenticación de acceso basada en 3GPP y, al mismo tiempo, la BPCF en el BBF inicia activamente una sesión S9* para interactuar con la PCRF del 3GPP. Por lo tanto, la PCRF puede interactuar con la BPCF al llevar a cabo la autorización de la QoS, y la BPCF ejecuta el control de admisión de recursos o confía en otros elementos de red para ejecutar el control de admisión de recursos.

En la forma 2, cuando el UE accede a la red de acceso del BBF, no se ejecuta la autenticación de acceso basada en 3GPP. Después de que el UE interactúa con la P-GW para establecer una asociación de seguridad IPSec, la P-GW envía directamente una dirección local del UE (es decir, una dirección asignada al UE por la red de acceso del BBF) a la PCRF, y después de determinar la BPCF de acuerdo con la dirección local del UE, la PCRF inicia inversamente un establecimiento de sesión S9* para llevar a cabo una interacción con la BPCF. Por lo tanto, la PCRF puede interactuar con la BPCF al llevar a cabo la autorización de la QoS, y la BPCF ejecuta el control de admisión de recursos o confía en otros elementos de red para ejecutar el control de admisión de recursos.

Si el UE requiere que la red asigne recursos al UE cuando el UE lleva a cabo el acceso al servicio, la PCRF envía en primer lugar la información de la QoS de las reglas de PCC elaboradas a la BPCF, de modo que la red de acceso del BBF ejecuta el control de admisión. A continuación, la PCRF envía a la PCEF una regla del PCC aceptada por la red de acceso del BBF. La PCEF lleva a cabo el marcado DSCP en una cabecera de un paquete IP de un flujo de datos correspondiente, de acuerdo con la regla del PCC. Cuando los paquetes IP del flujo de datos del servicio llegan a la red de acceso del BBF, la red de acceso del BBF puede llevar a cabo la planificación de los paquetes de datos según el DSCP de la cabecera del paquete IP.

De igual modo, una premisa del esquema anterior es que la red 3GPP soporte una interconexión entre la red 3GPP y el BBF, cuando la PCRF no soporta una interconexión entre la PCRF y el BBF (incluyendo un escenario en el que el PCC no está implementado en la red 3GPP), la PCRF no interactuará con la BPCF para solicitar el control de admisión. Los flujos de datos del servicio que no pasan a través del control de admisión ocuparán recursos de otros flujos de datos del servicio que pasan a través del control de admisión, lo que actualmente conduce un fallo de todo el mecanismo de control de políticas de FMC.

La figura 3, la figura 4 y la figura 5 son diagramas esquemáticos de arquitecturas del UE 3GPP que accede a la red troncal 3GPP a través de un H(e)NB, donde el H(e)NB toma la red de acceso del BBF como una red de retorno para conectarse a la red troncal 3GPP. En la arquitectura de la figura 3, la PCRF se interconecta directamente con la BPCF, cuando la PCRF lleva a cabo la autorización de la QoS, la PCRF interactúa en primer lugar con la BPCF, después la red de acceso del BBF lleva a cabo satisfactoriamente el control de admisión, la PCRF envía las reglas de PCC y las reglas de la QoS (si son necesarias) a la PCEFy a una Función de vinculación de portadora y de informe de eventos (BBERF) (si existe) respectivamente, la PCEF y la BBERF llevan a cabo el marcado DSCP en los datos de enlace descendente de un flujo de datos del servicio de acuerdo con las reglas de PCC y las reglas de la QoS, y cuando el flujo de datos del servicio llega una pasarela de seguridad (SeGW), la SeGW llevará a cabo la encapsulación IPSec en un paquete IP y llevará a cabo el marcado en una cabecera de un paquete IP del IPSec (denominada cabecera externa de paquete) de acuerdo con un DSCP del paquete IP (es decir, una cabecera interna de paquete) durante la encapsulación. Por lo tanto, la red de acceso del BBF puede llevar a cabo la planificación de los paquetes de datos de acuerdo con el DSCP de la cabecera el paquete IP del IPSec. Con respecto a los datos de enlace ascendente, el H(e)NB lleva a cabo una encapsulación IPSec en el paquete IP y lleva a cabo el marcado en la cabecera del paquete IP del IPsec (denominada cabecera externa de paquete) de acuerdo con el DSCP del paquete IP (es decir, la cabecera interna de paquete) durante la encapsulación. En las arquitecturas de la figura 4 y la figura 5, se introduce una entidad de función de la Función de políticas del H(e)NB (H(e)NB PF), cuando una H(e)NB GW (figura 4) o un H(e)NB (figura 5) recibe una petición de establecimiento de portadora o una petición de modificación de portadora de la red troncal 3GPP (el establecimiento o la modificación de la portadora se inicia después de que la PCEF o la BBERF lleven a cabo la vinculación de portadora de acuerdo con las reglas de PCC o las reglas de la QoS de la PCRF, o se inicia después de que la P-GW o la S-GW lleven a cabo la vinculación de portadora de acuerdo con las políticas locales), la H(e)NB GW o el H(e)NB solicitan a la red de acceso del BBF el control de admisión a través de la H(e)NB PF. Después de recibir una respuesta afirmativa del control de admisión de la red de acceso del BBF, la H(e)NB GW puede proseguir completando un flujo de establecimiento de portadora o un flujo de modificación de portadora. A continuación, la PCEF y la BBERF llevan a cabo el marcado DSCP de acuerdo con las reglas de PCC y las reglas de la QoS, y cuando los datos de enlace descendente del flujo de datos del servicio llegan a la SeGW, la SeGW llevará a cabo la encapsulación IPSec en el paquete IP y llevará a cabo el marcado en la cabecera del paquete IP del IPSec (denominada cabecera externa de paquete) de acuerdo con el DSCP del paquete IP (es decir, la cabecera interna de paquete) durante la encapsulación. Con respecto a los datos de enlace ascendente, el H(e)NB lleva a cabo la encapsulación IPSec en el paquete IP y lleva a cabo el marcado en la cabecera del paquete IP del IPSec (denominada cabecera externa de paquete) de acuerdo con el DSCP del paquete IP (es decir, la cabecera interna de paquete) durante la encapsulación. Por lo tanto, la red de acceso del BBF puede llevar a cabo la planificación de los paquetes de datos de acuerdo con el DSCP de la cabecera del paquete IP del IPSec.

Sin embargo, la premisa de los tres esquemas de arquitectura es que la red 3GPP soporte también una interconexión entre la red 3GPP y el BBF (la figura 3 es para una interconexión entre la PCRF y la BPCF, la figura 4 y la figura 5 son para una interconexión entre la H(e)NB PF y la BPCF), con respecto a la figura 3, cuando la PCRF no soporta una interconexión entre la PCRF y el BBF, la PCRF no interactuará con la BPCF para solicitar el control de admisión. De este modo, hará que las reglas de PCC enviadas por la PCRF a la PCEF sean resultados que se deciden de acuerdo con la propia PCRF. La PCEF lleva a cabo el marcado DSCP en las cabeceras de los paquetes IP de enlace descendente de los flujos de datos del servicio de acuerdo con las reglas de PCC enviadas por la PCRF. Cuando estos flujos de datos del servicio llegan a la SeGW, la SeGW replica el DSCP de la cabecera externa de paquete del IPSec de acuerdo con las marcas DSCP de la cabecera interna de paquete. Si estos datos llegan a la red de acceso del BBF, la red de acceso del BBF no distinguirá si estos flujos de datos del servicio pasan por el control de admisión de la red de acceso del BBR, sino que únicamente llevará a cabo el envío de acuerdo con el DSCP. Con respecto a los flujos de datos de enlace ascendente, el H(e)NB lleva a cabo de manera similar la encapsulación IPSec en el paquete IP de los datos de enlace ascendente y lleva a cabo el marcado en la cabecera del paquete IP del IPSec (denominada la cabecera externa de paquete) de acuerdo con el DSCP del paquete IP (es decir, la cabecera interna de paquete) durante la encapsulación. De este modo, los flujos de datos del servicio que no pasan a través del control de admisión ocuparán recursos de otros flujos de datos del servicio que pasan a través del control de admisión, lo que en la actualidad conduce un fallo de todo el mecanismo de control de políticas de FMC.

Si consideramos un escenario en el que el UE 3GPP y la entidad de red fija del BBF existen permanentemente, los flujos de datos del servicio de la entidad de red fija que no pasan a través del control de admisión también pueden ocupar recursos de los flujos de datos del servicio del UE 3GPP que pasan a través del control de admisión.

El documento "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Study on Support of BBF Access Interworking (Release 11) (Proyecto de asociación de tercera generación; Grupo de especificaciones técnicas, Aspectos del sistema y servicios; Estudio sobre el soporte del funcionamiento conjunto en el acceso del BBF (edición 11)) (2010-11-30), XP050462032, describe que la red del BBF lleva a cabo la clasificación de paquetes basándose en el DSCP de los paquetes entrantes y la PGW en el dominio del 3GPP establece un marcado DSCP por flujo en cada cabecera externa de paquete.

Resumen de la invención

El problema técnico que se tiene que resolver mediante el presente documento consiste en dar a conocer un procedimiento y un sistema para el control de políticas como el definido en las reivindicaciones independientes, mediante los cuales los flujos de datos del servicio que no pasan a través del control de admisión de una red de acceso del BBF no ocupen recursos de los flujos de datos del servicio que pasan a través del control de admisión de la red de acceso del BBF.

Un procedimiento de control de políticas comprende:

una entidad de red del Proyecto de asociación de tercera generación (3GPP) que envía información de la cabecera externa de paquete IP a una entidad de la red de acceso del Foro de banda ancha (BBF);

la entidad de la red de acceso del BBF planifica un paquete de datos que corresponde a la información de la cabecera externa del paquete IP de acuerdo con un Punto de código de servicios diferenciados (DSCP) del paquete de datos.

El procedimiento comprende además: la entidad de la red de acceso del BBF planifica un paquete de datos que no se corresponde con la información de la cabecera externa del paquete IP de acuerdo con una política local.

Donde, la etapa de que la entidad de red del 3GPP envía la información de la cabecera externa del paquete IP a una entidad de la red de acceso del BBF comprende:

una Pasarela de datos por paquetes evolucionada (ePDG) de una red 3GPP envía la información de la cabecera externa del paquete IP a una Función de reglas de políticas y tarificación (PCRF) a través de una Pasarela de red de datos por paquetes (P-GW), la PCRF envía la información de la cabecera externa del paquete IP a una Estructura de control de políticas de banda ancha (BPCF) de una red de acceso del BBF, y la BPCF envía la información de la cabecera externa del paquete IP a la entidad de la red de acceso del BBF; o,

la ePDG envía directamente la información de la cabecera externa del paquete IP a la PCRF, la PCRF envía la información de la cabecera externa del paquete IP a la BPCF, y la BPCF envía la información de la cabecera externa del paquete IP a la entidad de la red de acceso del BBF; o,

la P-GW envía la información de la cabecera externa del paquete IP a la PCRF, la PCRF envía la información de la cabecera externa del paquete IP a la BPCF, y la BPCF envía la información de la cabecera externa del paquete IP a la entidad de la red de acceso del BBF; o

la ePDG envía la información de la cabecera externa del paquete IP a la PCRF a través de la P-GW, la PCRF envía la información de la cabecera externa del paquete IP a la entidad de la red de acceso del BBF; o,

la ePDG envía directamente la información de la cabecera externa del paquete IP a la PCRF, la PCRF envía la información de la cabecera externa del paquete IP a la entidad de la red de acceso del BBF; o,

la P-GW envía la información de la cabecera externa del paquete IP a la PCRF, la PCRF envía la información de la cabecera externa del paquete IP a la entidad de la red de acceso del BBF.

Donde, la etapa de que la PCRF envía la información de la cabecera externa del paquete IP a la BPCF o a la entidad de la red de acceso del BBF comprende:

cuando se lleva a cabo la autorización de la calidad de servicio, la PCRF envía la información de la cabecera externa del paquete IP a la BPCF o a la entidad de la red de acceso del BBF; o,

cuando se inicia un establecimiento de sesión de interconexión de políticas con la BPCF, la PCRF envía la información de la cabecera externa del paquete IP a la BPCF o a la entidad de la red de acceso del BBF.

Donde, la etapa de que la entidad de red del 3GPP envía la información de la cabecera externa del paquete IP a la entidad de la red de acceso del BBF comprende:

una Pasarela de seguridad (SeGW) de la red 3GPP envía la información de la cabecera externa del paquete IP a la Función de políticas del H(e)NB (H(e)NB PF) o a la red de acceso del BBF, la H(e)NB PF envía la información de la cabecera externa del paquete IP a la BPCF, y la BPCF envía la información de la cabecera externa del paquete IP a la entidad de la red de acceso del BBF; o,

la SeGW envía la información de la cabecera externa del paquete IP a la PCRF, la PCRF envía la información de la cabecera externa del paquete IP a la BPCF, y la BPCF envía la información de la cabecera externa del paquete IP a la entidad de la red de acceso del BBF; o

la SeGW envía la información de la cabecera externa del paquete IP a la H(e)NB PF, la H(e)NB PF envía la información de la cabecera externa del paquete IP a la entidad de la red de acceso del BBF; o,

la SeGW envía la información de la cabecera externa del paquete IP a la PCRF, la PCRF envía la información de la cabecera externa del paquete IP a la entidad de la red de acceso del BBF.

Donde, la etapa de que la H(e)NB PF envía la información de la cabecera externa del paquete IP a la BPCF de la entidad de la red de acceso del BBF comprende:

cuando se inicia un establecimiento de sesión de interconexión de políticas con la BPCF o la entidad de la red de acceso del BBF, la H(e)NB PF envía la información de la cabecera externa del paquete IP a la BPCF o a la entidad de la red de acceso del BBF;

la etapa de que la PCRF envía la información de la cabecera externa del paquete IP a la BPCF o a la entidad de la red de acceso del BBF comprende:

cuando se inicia el establecimiento de sesión de interconexión de políticas con la BPCF o la entidad de la red de acceso del BBF, la PCRF envía la información de la cabecera externa del paquete IP a la BPCF o a la entidad de la red de acceso del BBF.

Donde, la información de la cabecera externa del paquete IP comprende por lo menos una dirección IP local de un equipo de usuario (UE).

Donde, si se detecta una NA(P)T entre el UE y la ePDG o entre el UE y la P-GW, la información de la cabecera externa del paquete IP comprende un número de puerto de origen del Protocolo de datagramas de usuario (User Datagram Protocolo, UDP) y la dirección IP local del UE.

Donde, el número de puerto de origen UDP es un número de puerto de origen UDP IPSec o un número de puerto de origen UDP de una señalización de actualización de vinculación DSMIP.

Donde, la información de la cabecera externa del paquete IP es un filtro de paquetes que contiene la información correspondiente.

Donde, la información de la cabecera externa del paquete IP comprende por lo menos una dirección IP local de un H(e)NB.

Donde, si se detecta una NA(P)T entre el H(e)NB y la SeGW, la información de la cabecera externa del paquete IP comprende un número de puerto de origen UDP y la dirección IP local del H(e)NB.

Donde, el número de puerto de origen UDP es un número de puerto de origen UDP IPSec.

Donde, la información de la cabecera externa del paquete IP es un filtro de paquetes que contiene la información correspondiente.

Un sistema de control de políticas comprende: una entidad de red del 3GPP y una entidad de la red de acceso del Foro de banda ancha (BBF), en el que:

la entidad de red del 3GPP está configurada para: enviar la información de la cabecera externa del paquete IP a la entidad de la red de acceso del BBF;

la entidad de la red de acceso del BBF está configurada para: planificar un paquete de datos que corresponde a la información de la cabecera externa del paquete IP de acuerdo con un Punto de código de servicios diferenciados (DSCP) del paquete de datos.

Donde, la entidad de la red de acceso del BBF está configurada además para: planificar un paquete de datos que no se corresponde con la información de la cabecera externa del paquete IP de acuerdo con una política local.

El sistema comprende además: una Estructura de control de políticas de banda ancha (BPCF) de una red de acceso del BBF, en el que:

la entidad de red del 3GPP comprende una Pasarela de red de datos por paquetes (P-GW), una Pasarela de datos por paquetes evolucionada (ePDG) y una Función de reglas de políticas y tarificación (PCRF), en el que:

la ePDG está configurada para: enviar la información de la cabecera externa del paquete IP a la PCRF a través de la P-GW; o enviar directamente la información de la cabecera externa del paquete IP a la PCRF;

la P-GW está configurada para: asistir a la ePDG para enviar la información de la cabecera externa del paquete IP a la PCRF; o enviar la información de la cabecera externa del paquete IP a la PCRF por sí misma;

la PCRF está configurada para: enviar la información de la cabecera externa del paquete IP a la BPCF o enviar la información de la cabecera externa del paquete IP a la entidad de la red de acceso del BBF;

la BPCF está configurada para: enviar la información de la cabecera externa del paquete IP a la entidad de la red de acceso del BBF.

Donde, la PCRF está configurada para enviar la información de la cabecera externa del paquete IP a la BPCF o a la entidad de la red de acceso del BBF del siguiente modo:

cuando se lleva a cabo la autorización de la calidad de servicio, envía la información de la cabecera externa del paquete IP a la BPCF o a la entidad de la red de acceso del BBF; o

cuando se inicia un establecimiento de sesión de interconexión de políticas con la BPCF o la entidad de la red de acceso del BBF, envía la información de la cabecera externa del paquete IP a la BPCF o a la BPCF.

El sistema comprende además una BPCF, en el que:

la entidad de red del 3GPP comprende una Pasarela de seguridad (SeGW) y una Función de políticas del H(e)NB (H(e)NB PF), o comprende una SeGW y una PCRF, en el que:

la SeGW está configurada para: enviar la información de la cabecera externa del paquete IP a la H(e)NB PF;

la H(e)NB PF está configurada para: enviar la información de la cabecera externa del paquete IP a la BPCF;

la BPCF está configurada para: enviar la información de la cabecera externa del paquete IP a la entidad de la red de acceso del BBF; o,

la entidad de red del 3GPP comprende la SeGW y la PCRF, donde:

la SeGW está configurada para: enviar la información de la cabecera externa del paquete IP a la PCRF;

la PCRF está configurada para: enviar la información de la cabecera externa del paquete IP a la BPCF o a la entidad de la red de acceso del BBF;

la BPCF está configurada para: enviar la información de la cabecera externa del paquete IP a la entidad de la red de acceso del BBF.

Donde, la H(e)NB PF de la PCRF está configurada para enviar la información de la cabecera externa del paquete IP a la BPCF o a la entidad de la red de acceso del BBF del siguiente modo:

cuando se inicia un establecimiento de sesión de interconexión de políticas con la BPCF o la entidad de la red de acceso del BBF, envía la información de la cabecera externa del paquete IP a la BPCF o a la entidad de la red de acceso del BBF.

Donde, la información de la cabecera externa del paquete IP comprende por lo menos una dirección IP local de un equipo de usuario (UE).

Donde, si se detecta una NA(P)T entre el UE y la ePDG o entre el UE y la P-GW, la información de la cabecera externa del paquete IP comprende un número de puerto de origen UDP y la dirección IP local del UE.

Donde, el número de puerto de origen UDP es un número de puerto de origen UDP IPSec o un número de puerto de origen UDP de una señalización de actualización de vinculación DSMIP.

Donde, la información de la cabecera externa del paquete IP es un filtro de paquetes que contiene la información correspondiente.

Donde la información de la cabecera externa del paquete IP comprende por lo menos una dirección IP local de un H(e)NB.

Donde, si se detecta una NA(P)T entre el H(e)NB y la SeGW, la información de la cabecera externa del paquete IP comprende un número de puerto de origen UDP y la dirección IP local del H(e)NB.

Donde, el número de puerto de origen UDP es un número de puerto de origen UDP IPSec.

Donde, la información de la cabecera externa del paquete IP es un filtro de paquetes que contiene la información correspondiente.

Un sistema de la red de acceso del Foro de banda ancha (BBF) comprende una entidad de la red de acceso del BBF, en el que:

la entidad de la red de acceso del BBF está configurada para: recibir la información de la cabecera externa del paquete IP enviada por una red 3GPP, y planificar un paquete de datos que corresponde a la información de la cabecera externa del paquete IP de acuerdo con un Punto de código de servicios diferenciados (DSCP) del paquete de datos.

Donde, la entidad de la red de acceso del BBF está configurada además para: planificar un paquete de datos que no se corresponde con la información de la cabecera externa del paquete IP de acuerdo con una política local.

El sistema comprende además: una estructura de control de políticas de banda ancha (BPCF), en el que:

la BPCF está configurada para: después de que una Pasarela de datos por paquetes evolucionada (eDPG) de la red 3GPP envía la información de la cabecera externa del paquete IP a una Función de reglas de políticas y tarificación (PCRF) a través de una Pasarela de red de datos por paquetes (P-GW), recibir la información de la cabecera externa del paquete IP enviada por la PCRF; o después de que la ePDG envía directamente la información de la cabecera externa del paquete IP a la PCRF, recibir la información de la cabecera externa del paquete IP enviada por la PCRF; o después de que la P-GW envía la información de la cabecera externa del paquete IP a la PCRF, recibir la información de la cabecera externa del paquete IP enviada por la PCRF, y enviar la información de la cabecera externa del paquete IP a la entidad de la red de acceso del BBF; o,

recibir la información de la cabecera externa del paquete IP enviada por una Pasarela de seguridad (SeGW) de la red 3GPP a través de una Función de políticas de H(e)NB (H(e)NB PF) de la red de acceso del BBF; o recibir la información de la cabecera externa del paquete IP enviada por la SeGW a través de la PCRF, y enviar la información de la cabecera externa del paquete IP a la entidad de la red de acceso del BBF.

Donde, la BPCF está configurada además para: recibir la información de la cabecera externa del paquete IP enviada por la PCRF al llevar a cabo la autorización de la calidad de servicio; o,

recibir la información de la cabecera externa del paquete IP enviada por la PCRF al iniciar un establecimiento de sesión de interconexión de políticas con la BPCF; o,

recibir la información de la cabecera externa del paquete IP enviada por la H(e)NB PF o la PCRF al iniciar el establecimiento de sesión de interconexión de políticas con la BPCF.

En el esquema técnico anterior, la red de acceso del BBF guarda las cabeceras externas de los paquetes IP, cuando los datos llegan a la red de acceso del BBF, la entidad de la red de acceso del BBF lleva a cabo en primer lugar el filtrado de acuerdo con las cabeceras externas de los paquetes IP guardadas, y solamente cuando los flujos de datos del servicio de las cabeceras externas de los paquetes IP se corresponden, lleva a cabo la planificación de datos de acuerdo con los DSCP; con respecto a los flujos de datos del servicio que no se corresponden, la entidad de la red de acceso del BBF lleva a cabo el procesamiento de acuerdo con las políticas locales (por ejemplo, se remarcan los DSCP con prioridades más bajas). De este modo, los flujos de datos del servicio que no pasen a través del control de admisión no ocuparán recursos de otros flujos de datos del servicio que pasan a través del control de admisión.

Breve descripción de los dibujos

La figura 1 es un diagrama esquemático de la arquitectura de componentes del EPS.

La figura 2 es un diagrama esquemático de un UE que accede a la red troncal 3GPP a través de una red de acceso WLAN.

La figura 3 es un diagrama esquemático 1 de un UE que accede a la red troncal 3GPP a través de un H(e)NB.

La figura 4 es un diagrama esquemático 2 de un UE que accede a la red troncal 3GPP a través de un H(e)NB.

La figura 5 es un diagrama esquemático 3 de un UE que accede a la red troncal 3GPP a través de un H(e)NB.

La figura 6 es un diagrama de flujo 1 de una sesión S9* de acuerdo con el ejemplo 1 del presente documento.

La figura 7 es un diagrama de flujo 2 de una sesión S9* de acuerdo con el ejemplo 2 del presente documento.

La figura 8 es un diagrama de flujo 3 de una sesión S9* de acuerdo con el ejemplo 3 del presente documento.

La figura 9 es un diagrama de flujo de una entidad de la red de acceso del BBF que obtiene las cabeceras externas de los paquetes IP en el proceso de conexión de un UE a un EPS bajo la arquitectura mostrada en la figura 3, de acuerdo con el ejemplo 4 del presente documento.

La figura 10 es un diagrama de flujo de una entidad de la red de acceso del BBF que obtiene las cabeceras externas de los paquetes IP después de que sea encendido un H(e)NB bajo la arquitectura de la figura 4, de acuerdo con el ejemplo 5 del presente documento.

La figura 11 es un diagrama de flujo de una entidad de la red de acceso del BBF que obtiene las cabeceras externas de los paquetes IP después de que sea encendido un H(e)NB bajo la arquitectura de la figura 5, de acuerdo con el ejemplo 6 del presente documento.

Realizaciones preferentes de la invención

El presente documento da a conocer un procedimiento de control de políticas, que incluye:

una red 3GPP envía una cabecera externa de paquete IP a una entidad de la red de acceso del BBF;

la entidad de la red de acceso del BBF planifica un paquete de datos que corresponde a la cabecera externa de paquete IP de acuerdo con un Punto de código de servicios diferenciados (DSCP) del paquete de datos, y planifica un paquete de datos que no se corresponde con la cabecera externa de paquete IP de acuerdo con una política local.

Donde, la cabecera externa del paquete IP es una cabecera externa de paquete IP de un túnel IPSec. El túnel IPSec es un túnel IPSec entre un equipo de usuario y una Pasarela de datos por paquetes evolucionada (ePDG), o entre un equipo de usuario y una P-GW, o entre un H(e)NB y una pasarela de seguridad.

Donde, la etapa de que la red 3GPP envíe la cabecera externa de paquete IP a una entidad de la red de acceso del BBF incluye:

(1) La Pasarela de datos por paquetes evolucionada (ePDG) envía la cabecera externa de paquete IP a la P-GW, y la P-GW envía la cabecera externa de paquete IP a una PCRF; o la ePDG envía directamente la cabecera externa de paquete IP a la PCRF; o la P-GW envía la cabecera externa de paquete IP a la PCRF;

la PCRF envía la cabecera externa de paquete IP a una BPCF; la PCRF envía la cabecera externa de paquete IP a la BPCF cuando lleva a cabo la autorización de la calidad de servicio; o la PCRF envía la cabecera externa de paquete IP a la BPCF cuando inicia un establecimiento de sesión de interconexión de políticas con la BPCF.

(2) La Pasarela de seguridad (SeGW) envía la cabecera externa de paquete IP a una función de políticas de H(e)NB (H(e)NB PF) o a la PCRF;

la H(e)NB PF o la PCRF envía la cabecera externa de paquete IP a la BPCF; la H(e)NB PF o la PCRF envía la cabecera externa de paquete IP a la BPCF cuando inicia un establecimiento de sesión de interconexión de políticas con la BPCF; y

la BPCF envía la cabecera externa de paquete IP a la entidad de la red de acceso del BBF.

Ejemplo 1

La figura 6 es un diagrama de flujo de una BPCF que inicia una sesión S9* en un escenario sin itinerancia en el que un UE accede a una red troncal 3GPP a través de una red de acceso no fiable del BBF de acuerdo con el ejemplo del presente documento. En la figura 6, se adopta un protocolo PMIPv6 entre una ePDG y una P-GW.

En la etapa -601-, después de que el UE accede al sistema de acceso del BBF, se ejecuta una autenticación de acceso basada en 3GPP, y el UE proporciona una Identidad de abonado móvil internacional (International Mobile Subscriber Identity, IMSI) (utilizada para la autenticación de acceso).

En la etapa -602-, el UE obtiene una dirección IP local de la red de acceso del BBF. La dirección puede ser asignada por una Pasarela residencial (Residential Gateway, RG) o una BNG.

En la etapa -603-, después de la activación de la etapa -601- o la etapa -602-, se informa a la BPCF de que el UE accede a la red de acceso del BBF.

En la etapa -604-, la BPCF envía a una PCRF un mensaje de establecimiento de sesión de control de pasarela que incluye un identificador de usuario.

En la etapa -605-, la PCRF devuelve a la BPCF un mensaje de acuse de establecimiento de sesión de control de pasarela. Puede ser necesario que la PCRF interactúe con un SPR para obtener de un usuario una decisión de la política de suscripción de usuario.

En la etapa -606-, después de seleccionar la ePDG, el UE inicia un proceso de establecimiento de un túnel IKEv2 y lleva a cabo una autenticación utilizando un Protocolo de autenticación extensible (Extensible Authentication Protocol, EAP). Si existe una NA(P)T entre el UE y la ePDG (por ejemplo, existe la NA(P)T en la RG), una señalización IKEv2 ejecutará una NAT transversal.

En la etapa -607-, después de seleccionar la P-GW, la ePDG envía un mensaje de actualización de vinculación de servidor intermediario a la P-GW, y el mensaje de actualización de vinculación de servidor intermediario lleva el identificador de usuario, un identificador de la PDN y la información de cabecera externa de paquete IP. Con respecto a un escenario S2b, todos los flujos de datos del servicio se encapsularán con un túnel IPSec entre el UE y la ePDG. Por lo tanto, en ese momento, la información de cabecera externa de paquete IP puede ser información de cabecera externa de paquete IP del túnel IPSec establecido entre el UE y la ePDG. Con el fin de identificar unívocamente este túnel IPSec, la información de cabecera externa de paquete IP del túnel IPSec incluye por lo menos una dirección de origen en la señalización IKEv2 enviada por el UE y recibida por la ePDG (es decir, una dirección de origen IPSec, con respecto a una dirección de enlace ascendente del UE). La información de cabecera externa de paquete IP del túnel IPSec puede incluir asimismo un número de puerto de origen UDP en la señalización IKEv2 enviada por el UE y recibida por la ePDG (es decir, un número de puerto de origen IPSec, con respecto a la dirección de enlace ascendente del UE, también denominado como un número de puerto de origen UDP, al igual que anteriormente), una dirección de la ePDG, un número de puerto de recepción de la ePDG (es decir, un número de puerto de destino UDP, con respecto a la dirección de enlace ascendente del UE) y tipos de protocolos y similares.

Dado que la señalización IKEv2 puede haber pasado por el NA(P)T transversal, la dirección de origen y el número de puerto de origen recibidos por la ePDG pueden ser diferentes de la dirección de origen y el número de puerto de origen cuando el UE lleva a cabo el envío. Si la señalización IKEv2 no pasa por el NA(P)T transversal, la dirección de origen es la dirección local obtenida cuando el UE accede a la red de acceso del BBF.

Con respecto a un escenario en el que no existe NA(P)T entre el UE y la ePDG, la dirección de origen en la señalización IKEv2 enviada por el UE y recibida por la ePDG es una dirección IP local asignada por la red de acceso del BBF, y la dirección puede identificar unívocamente los flujos de datos del servicio del UE encapsulados con el túnel IPSec, por lo que la información de cabecera externa de paquete IP contiene por lo menos la dirección IP local.

Con respecto a un escenario en el que exista NAT (1:1) entre el UE y la ePDG, la dirección de origen en la señalización IKEv2 enviada por el UE y recibida por la ePDG es una dirección IP de red pública después de pasar por la NAT, pero debido a la NAT 1:1, la dirección puede seguir identificando unívocamente los flujos de datos del servicio del UE encapsulados con el túnel IPSec, por loque la información de cabecera externa de paquete IP contiene por lo menos la dirección de origen en la señalización IKEv2 enviada por el UE y recibida por la ePDG (es decir, la dirección IP de red pública después de pasar por la NAT de la red de acceso del BBF, si la NAT está en la RG, la dirección es una dirección de la RG).

Con respecto a NAT (N:1) (es decir, NAPT) entre el UE y la ePDG, la encapsulación UDP se tiene que llevar a cabo en los flujos de datos del servicio durante el NAT transversal, y la NAPT asignará el número de puerto de origen UDP (con respecto a la dirección de enlace ascendente del UE) al túnel IPSec. Por lo tanto, con el fin de identificar unívocamente los flujos de datos del servicio del UE encapsulados con el túnel IPSec, la información de cabecera externa de paquete IP contiene por lo menos la dirección de origen en la señalización IKEv2 enviada por el UE y recibida por la ePDG (es decir, la dirección IP de red pública después de pasar por la NAT de la red de acceso del BBF, si la NAT está en la RG, la dirección es la dirección de la RG) y el número de puerto de origen en la señalización IKEv2 enviada por el UE y recibida por la ePDG (es decir, un número de puerto de origen UDP IPSec).

Para mayor comodidad de las descripciones, la dirección IP del UE después de pasar por la NAT se denomina asimismo dirección IP local. Por lo tanto, la información de cabecera externa de paquete IP incluye por lo menos la dirección IP local del UE. Si se detecta la NA(P)T entre el UE y la ePDG, la información de cabecera externa de paquete IP puede incluir asimismo el número de puerto de origen UDP IPSec. La información de cabecera externa de paquete IP puede contener asimismo información tal como la dirección de la ePDG, un número de puerto de destino UDP IPSec (con respecto a la dirección de enlace ascendente del UE) y tipos de protocolos y similares.

Indudablemente, la información de cabecera externa de paquete IP puede ser un filtro de paquetes, y el filtro de paquetes contiene por lo menos la dirección IP local del UE. Si se detecta la NA(P)T entre el UE y la ePDG, el filtro de paquetes puede contener asimismo el número de puerto de origen UDP IPSec. El filtro de paquetes puede

contener asimismo información tal como la dirección de la ePDG, un número de puerto de destino UDP IPSec (con respecto a la dirección de enlace ascendente del UE) y tipos de protocolos y similares.

En la etapa -608-, la P-GW asigna una dirección IP al UE, y una PCEF ubicada en la P-GW envía un mensaje de indicación de establecimiento de sesión IP-CAN a la PCRF, y el mensaje de indicación de establecimiento de sesión IP-CAN lleva el identificador de usuario, el identificador de la PDN, la dirección IP asignada al UE y la información de cabecera externa de paquete IP.

En la etapa -609-, la PCRF lleva a cabo una estimación de acuerdo con el identificador de usuario y el identificador de PDN, y si no existen datos relevantes de la suscripción de usuario, una H-PCRF interactuará con el SPR para obtener los datos de la suscripción. La PCRF elabora reglas de PCC de acuerdo con los datos de la suscripción, las políticas de red y los atributos de la red de acceso y similares, y devuelve a la PCEF un mensaje de acuse que incluye las reglas de PCC.

En la etapa -610-, la P-GW envía un mensaje de actualización de la dirección IP de la P-GW a un servidor de AAA y envía una dirección de la P-GW al servidor de AAA, y el servidor de AAA interactúa adicionalmente con un HSS y guarda la dirección de la P-GW en el HSS.

En la etapa -611-, la P-GW devuelve a la ePDG un mensaje de acuse de vinculación de servidor intermediario, y el mensaje de acuse de vinculación de servidor intermediario lleva la dirección IP asignada al UE.

En la etapa -612-, la actualización de vinculación de servidor intermediario es satisfactoria, y se establece el túnel IPSec entre el UE y la ePDG.

En la etapa -613-, la ePDG envía al UE una señalización IKEv2 final, en la que se incluye la dirección IP del UE.

En la etapa -614-, la PCRF proporciona a la BPCF la información de cabecera externa de paquete IP.

En la etapa -615-, la BPCF proporciona la información de cabecera externa de paquete IP a una entidad de la red de acceso del BBF (por ejemplo, BNG/BRAS).

En la etapa -616-, la entidad de la red de acceso del BBF (BNG/BRAS) devuelve el mensaje de acuse después de guardar las cabeceras externas de los paquetes IP.

En la etapa -617-, la BPCF devuelve el mensaje de acuse a la PCRF.

La etapa -614- se puede ejecutar después de la etapa -609-.

Por medio del flujo anterior, se establece una sesión entre la PCRF y la BPCF, y la red de acceso del BBF (BNG/BRAS) obtiene la información de cabecera externa de paquete IP. Cuando el UE necesita que la red asigne recursos al UE cuando lleva a cabo un acceso a los servicios, la PCRF envía en primer lugar a la BPCF la información de la QoS de las reglas de PCC elaboradas, de tal modo que la red de acceso del BBF ejecuta el control de admisión. A continuación, la PCRF envía a la PCEF una regla del PCC aceptada por la red de acceso del BBF. La PCEF lleva a cabo el marcado DSCP en una cabecera de un paquete IP de datos de enlace descendente de un flujo de datos correspondiente (denominada una cabecera interna de paquete) de acuerdo con la regla del PCC, cuando los paquetes IP del flujo de datos del servicio lleguen a la ePDG, la ePDG llevará a cabo la encapsulación IPSec del paquete IP y llevará a cabo la réplica DSCP. Cuando estos datos llegan a la red de acceso del BBF, la entidad de la red de acceso del BBF lleva a cabo en primer lugar un filtrado de acuerdo con las cabeceras externas de los paquetes IP guardadas, y solamente cuando los flujos de datos del servicio de la información de cabecera externa de paquete IP se corresponden, lleva a cabo la planificación de los datos de acuerdo con los DSCP; con respecto a los flujos de datos del servicio que no se corresponden, la entidad de la red de acceso del BBF lleva a cabo el procesamiento de acuerdo con las políticas locales (por ejemplo, se remarcan los DSCP con prioridades inferiores). Con respecto a los datos de enlace ascendente de los flujos de datos del servicio, el UE lleva a cabo la encapsulación IPSec y lleva a cabo la réplica DSCP, cuando los datos llegan a la red de acceso del BBF, la entidad de la red de acceso del BBF lleva a cabo en primer lugar el filtrado de acuerdo con la información de cabecera externa de paquete IP guardada, y solamente cuando los flujos de datos del servicio de la información de cabecera externa de paquete IP se corresponden, lleva a cabo la planificación de datos de acuerdo con los DSCP; con respecto a los flujos de datos que no se corresponden, la entidad de la red de acceso del BBF lleva a cabo el procesamiento de acuerdo con las políticas locales (por ejemplo, se remarcan los DSCP con prioridades inferiores). De este modo, los flujos de datos del servicio que no pasen a través del control de admisión no ocuparán recursos de otros flujos de datos del servicio que pasen por el control de admisión.

Ejemplo 2

La figura 7 es un diagrama de flujo de una P-GW que activa una PCRF para iniciar una sesión S9* en un escenario sin itinerancia cuando un UE accede a una red troncal 3GPP a través de una red de acceso no fiable del BBF de

acuerdo con el presente documento. En la figura 7, se adopta un protocolo PMIPv6 entre una ePDG y la P-GW.

En la etapa -701-, después de que el UE accede al sistema de acceso del BBF, el sistema de acceso del BBF asigna una dirección IP local al UE. El UE inicia un proceso de establecimiento de túnel IKEv2 y lleva a cabo la autenticación utilizando un EAP. La ePDG interactúa con un servidor de AAA (el servidor de AAA interactúa adicionalmente con un HSS) para completar la autenticación EAP.

En la etapa -702-, después de seleccionar la P-GW, la ePDG envía a la P-GW un mensaje de actualización de vinculación de servidor intermediario, y el mensaje de actualización de vinculación de servidor intermediario lleva un identificador de usuario, un identificador de la PDN y la información de cabecera externa de paquete IP. Con respecto a un escenario S2b, todos los flujos de datos del servicio se encapsularán con un túnel IPSec entre el UE y la ePDG. Por lo tanto, en ese momento, la información de cabecera externa de paquete IP puede ser la información de cabecera externa de paquete IP del túnel IPSec establecido entre el UE y la ePDG. Con el fin de identificar unívocamente este túnel IPSec, la información de cabecera externa del paquete IP del túnel IPSec incluye por lo menos una dirección de origen en una señalización IKEv2 enviada por el UE y recibida por la ePDG (es decir, una dirección de origen IPSec, con respecto a una dirección de enlace ascendente del UE). La información de cabecera externa de paquete IP del túnel IPSec puede contener asimismo un número de puerto de origen en la señalización IKEv2 enviada por el UE y recibida por la ePDG (es decir, un número de puerto de origen IPSec, con respecto a la dirección de enlace ascendente del UE), una dirección de la ePDG, un número de puerto de recepción UDP de la ePDG (es decir, un número de puerto de destino UDP, con respecto a la dirección de enlace ascendente del UE) y tipos de protocolos y similares.

Dado que la señalización IKEv2 puede haber pasado por la NAT transversal, la dirección de origen y el número de puerto de origen recibidos por la ePDG pueden ser diferentes de la dirección de origen y el número de puerto de origen cuando el UE lleva a cabo el envío. Si la señalización IKEv2 no pasa por la NAT transversal, la dirección de origen es la dirección local obtenida cuando el UE accede a la red de acceso del BBF.

Con respecto a un escenario en el que no existe NAT entre el UE y la ePDG, la dirección de origen en la señalización IKEv2 enviada por el UE y recibida por la ePDG es una dirección IP local asignada por la red de acceso del BBF, y la dirección puede identificar unívocamente los flujos de datos del servicio del UE encapsulados con el túnel IPSec, por lo que la información de cabecera externa de paquete IP contiene por lo menos la dirección IP local.

Con respecto a un escenario de NAT (1:1) existente entre el UE y la ePDG, la dirección de origen en la señalización IKEv2 enviada por el UE y recibida por la ePDG es una dirección IP de red pública después de pasar por la NAT, pero debido a la NAT 1:1, la dirección puede seguir identificando unívocamente los flujos de datos del servicio del UE encapsulados con el túnel IPSec, por lo que la información de cabecera externa de paquete IP contiene por lo menos la dirección de origen en la señalización IKEv2 enviada por el UE y recibida por la ePDG (es decir, la dirección IP de red pública después de pasar por la NAT de la red de acceso del BBF, si la NAT está en una RG, la dirección es una dirección de la RG).

Con respecto a NAT (N:1) (es decir, NAPT) entre el UE y la ePDG, se debe llevar a cabo una encapsulación UDP en los flujos de datos del servicio durante el NAPT transversal, y la NAPT asignará un número de puerto de origen UDP (con respecto a la dirección de enlace ascendente del UE) al túnel IPSec. Por lo tanto, con el fin de identificar unívocamente los flujos de datos del servicio del UE encapsulados con el túnel IPSec, la información de cabecera externa de paquete IP contiene por lo menos la dirección de origen en la señalización IKEv2 enviada por el UE y recibida por la ePDG (es decir, la dirección IP de red pública después de pasar por la NAT de la red de acceso del BBF, si la NAPT está en una RG, la dirección es una dirección de la RG) y el número de puerto de origen en la señalización IKEv2 enviada por el UE y recibida por la ePDG (es decir, un número de puerto de origen UDP IPSec).

Para mayor comodidad de las descripciones, la dirección IP del UE después de pasar por la NAT se denomina asimismo dirección IP local. Por lo tanto, la información de cabecera externa de paquete IP incluye por lo menos la dirección IP local del UE. Si se detecta la NA(P)T entre el UE y la ePDG, la información de cabecera externa de paquete IP puede contener asimismo el número de puerto de origen UDP IPSec. La información de cabecera externa de paquete IP puede contener asimismo información tal como la dirección de la ePDG, un número de puerto de destino UDP IPSec (con respecto a la dirección de enlace ascendente del UE) y tipos de protocolos y similares.

Indudablemente, durante la implementación específica, la información de cabecera externa de paquete IP puede ser un filtro de paquetes, y el filtro de paquetes contiene por lo menos la dirección IP local del UE. Si se detecta la NA(P)T entre el UE y la ePDG, el filtro de paquetes puede contener asimismo el número de puerto de origen UDP IPSec. El filtro de paquetes puede contener asimismo información tal como la dirección de la ePDG, un número de puerto de destino UDP IPSec (con respecto a la dirección de enlace ascendente del UE) y tipos de protocolos y similares.

En la etapa -703-, la P-GW asigna una dirección IP al UE, y una PCEF ubicada en la P-GW envía un mensaje de indicación de establecimiento de sesión IP-CAN a la PCRF, y el mensaje de indicación de establecimiento de sesión

IP-CAN lleva el identificador de usuario, el identificador de la PDN, la dirección IP asignada al UE y la información de cabecera externa de paquete IP.

En la etapa -704-, la PCRF lleva a cabo una estimación de acuerdo con el identificador de usuario y el identificador de la PDN, y si no existen datos relevantes de la suscripción de usuario, la PCRF interactuará con un SPR para obtener los datos de la suscripción. La PCRF elabora reglas de PCC de acuerdo con los datos de la suscripción, las políticas de red y los atributos de la red de acceso y similares. La PCRF devuelve a la PCEF un mensaje de acuse que incluye las reglas de PCC.

En la etapa -705-, la P-GW envía un mensaje de actualización de la dirección IP de la P-GW al servidor de AAA y envía una dirección de la P-GW al servidor de AAA, y el servidor de AAA interactúa adicionalmente con el HSS y guarda la dirección de la P-GW en el HSS.

En la etapa -706-, la P-GW devuelve un mensaje de acuse de vinculación de servidor intermediario a la ePDG, y el mensaje de acuse de vinculación de servidor intermediario lleva la dirección IP asignada al UE.

En la etapa -707-, la actualización de vinculación de servidor intermediario es satisfactoria, y se establece el túnel IPSec entre el UE y la ePDG.

En la etapa -708-, la ePDG envía al UE una señalización IKEv2 final, en la que se incluye la dirección IP del UE.

En la etapa -709-, la PCRF determina una BPCF de la red de acceso del BBF a la que el UE accede actualmente de acuerdo con la información de cabecera externa de paquete IP, y envía a la BPCF un mensaje de establecimiento de sesión de control de pasarela iniciado por la PCRF, y la información de cabecera externa de paquete IP se incluye en el mensaje de establecimiento de sesión de control de pasarela.

La etapa -709- se puede ejecutar después de la etapa -703-.

En la etapa -710-, la BPCF proporciona cabeceras externas de los paquetes IP a una entidad de la red de acceso del BBF (por ejemplo BNG/BRAS).

En la etapa -711-, la entidad de la red de acceso del BBF devuelve el mensaje de acuse después de guardar las cabeceras externas de los paquetes IP.

En la etapa -712-, la BPCF devuelve el mensaje de acuse a la PCRF.

Por medio del flujo anterior, se establece una sesión entre la PCRF y la BPCF, y la entidad de la red de acceso del BBF (BNG/BRAS) obtiene la información de cabecera externa de paquete IP. Si el UE requiere que la red asigne recursos al UE cuando el UE lleva a cabo el acceso al servicio, la PCRF envía en primer lugar a la BPCF la información de la QoS de las reglas de PCC elaboradas, para que la red de acceso del BBF ejecute el control de admisión. A continuación, la PCRF envía a la PCEF una regla del PCC aceptada por la red de acceso del BBF. La PCEF lleva a cabo un marcado DSCP en una cabecera de un paquete IP de enlace descendente de un flujo de datos correspondiente (denominada cabecera interna de paquete) de acuerdo con la regla del PCC, cuando los paquetes IP del flujo de datos del servicio lleguen a la ePDG, la ePDG llevará a cabo la encapsulación IPSec en el paquete IP y llevará a cabo la réplica DSCP. Cuando estos datos lleguen a la red de acceso del BBF, la entidad de la red de acceso del BBF lleva a cabo en primer lugar el filtrado de acuerdo con la información de cabecera externa de paquete IP guardada, y solamente cuando los flujos de datos del servicio de la información de cabecera externa de paquete IP se corresponden, lleva a cabo la planificación de los datos de acuerdo con los DSCP; con respecto a los flujos de datos del servicio que no se corresponden, la entidad de la red de acceso del BBF lleva a cabo el procesamiento de acuerdo con las políticas locales (por ejemplo, se remarcan los DSCP con prioridades inferiores). Con respecto a los datos de enlace ascendente de los flujos de datos del servicio, el UE lleva a cabo la encapsulación IPSec y lleva a cabo la réplica DSCP, cuando los datos llegan a la red de acceso del BBF, la entidad de la red de acceso del BBF lleva a cabo en primer lugar el filtrado de acuerdo con la información de cabecera externa de paquete IP guardada, y solamente cuando los flujos de datos del servicio de la información de cabecera externa de paquete IP se corresponden, lleva a cabo la planificación de los datos de acuerdo con los DSCP; con respecto a los flujos de datos del servicio que no se corresponden, la entidad de la red de acceso del BBF lleva a cabo el procesamiento de acuerdo con las políticas locales (por ejemplo, se remarcan los DSCP con prioridades inferiores). Por lo tanto, los flujos de datos del servicio que no pasan por el control de admisión no ocuparán recursos de otros flujos de datos del servicio que pasen por el control de admisión.

El ejemplo se aplica asimismo a escenarios de itinerancia (incluyendo un escenario de itinerancia con enrutamiento local o un escenario de itinerancia con desvío local).

Con respecto a un escenario de adopción de un protocolo GTP entre la ePDG y la P-GW, el flujo es similar. La ePDG transportará la información de cabecera externa de paquete IP en el mensaje de petición de establecimiento de sesión.

Ejemplo 3

La figura 8 es un diagrama de flujo de una P-GW que activa una PCRF para iniciar una sesión S9* en un escenario sin itinerancia cuando un UE accede a una red troncal 3GPP a través de una red de acceso del BBF no fiable, de acuerdo con el presente documento. En la figura 8, se adopta un protocolo PMIPv6 entre una ePDG y la P-GW.

En la etapa -801-, después de que el UE accede al sistema de acceso del BBF, el sistema de acceso del BBF asigna una dirección IP local al UE. El UE inicia un proceso de establecimiento de túnel IKEv2 y lleva a cabo una autenticación utilizando un EAP. La ePDG interactúa con un servidor de AAA (el servidor de AAA interactúa adicionalmente con un HSS) para completar la autenticación EAP.

En la etapa -802-, la ePDG envía a la PCRF un mensaje de establecimiento de sesión de control de pasarela que incluye la información de cabecera externa de paquete IP. Con respecto a un escenario S2b, todos los flujos de datos del servicio se encapsularán con un túnel IPSec entre el UE y la ePDG. Por lo tanto, en ese momento, la información de cabecera externa de paquete IP puede ser información de cabecera externa de paquete IP del túnel IPSec establecido entre el UE y la ePDG. Con el fin de identificar unívocamente este túnel IPSec, la información de cabecera externa de paquete IP del túnel IPSec incluye por lo menos una dirección de origen en una señalización IKEv2 enviada por el UE y recibida por la ePDG (es decir, una dirección de origen IPSec, con respecto a una dirección de enlace ascendente del UE). La información de cabecera externa de paquete IP del túnel IPSec puede contener asimismo un número de puerto de origen en la señalización IKEv2 enviada por el UE y recibida por la ePDG (es decir, un número de puerto de origen IPSec, con respecto a la dirección de enlace ascendente del UE), una dirección de la ePDG, un número de puerto de recepción UDP de la ePDG (es decir, un número de puerto de destino UDP, con respecto a la dirección de enlace ascendente del UE) y tipos de protocolos y similares.

Como la señalización IKEv2 puede haber pasado por la NAT transversal, la dirección de origen y el número de puerto de origen recibidos por la ePDG pueden ser diferentes de la dirección de origen y el número de puerto de origen cuando el UE lleva a cabo el envío. Si la señalización IKEv2 no pasa por la NAT transversal, la dirección de origen es una dirección local obtenida cuando el UE accede a la red de acceso del BBF.

Con respecto a un escenario en el que no existe NAT entre el UE y la ePDG, la dirección de origen en la señalización IKEv2 enviada por el UE y recibida por la ePDG es una dirección IP local asignada por la red de acceso del BBF, y la dirección puede identificar unívocamente los flujos de datos del servicio del UE encapsulados con el túnel IPSec, por lo que la información de cabecera externa de paquete IP incluye por lo menos la dirección IP local.

Con respecto a un escenario de NAT (1:1) existente entre el UE y la ePDG, la dirección de origen en la señalización IKEv2 enviada por el UE y recibida por la ePDG es una dirección IP de red pública después de pasar por la NAT, pero debido a la NAT 1:1, la dirección puede seguir identificando unívocamente los flujos de datos del servicio del UE encapsulados con el túnel IPSec, por lo que la información de cabecera externa de paquete IP contiene por lo menos la dirección de origen en la señalización IKEv2 enviada por el UE y recibida por la ePDG (es decir, la dirección IP de red pública después de pasar por la NAT de la red de acceso del BBF, si la NAT está en una RG, la dirección es una dirección de la RG).

Con respecto a NAT (N:1) (es decir, NAPT) entre el UE y la ePDG, es necesario llevar a cabo una encapsulación UDP en los flujos de datos del servicio durante el NAPT transversal, y la NAPT asignará un número de puerto de origen UDP al túnel IPSec (con respecto a la dirección de enlace ascendente del UE). Por lo tanto, con el fin de identificar unívocamente los flujos de datos del servicio del UE encapsulados con el túnel IPSec, la información de cabecera externa de paquete IP incluye por lo menos la dirección de origen en la señalización IKEv2 enviada por el UE y recibida por la ePDG (es decir, la dirección IP de red pública después de pasar por la NAT de la red de acceso del BBF, si la NAT está en una RG, la dirección es la dirección de la RG) y el número de puerto de origen en la señalización IKEv2 enviada por el UE y recibida por la ePDG (es decir, un número de puerto de origen UDP IPSec).

Para mayor comodidad de la descripción, la dirección IP del UE después de pasar por la NAT también se denomina como dirección IP local. Por lo tanto, la información de cabecera externa de paquete IP incluye por lo menos la dirección IP local del UE. Si se detecta la NA(P)T entre el UE y la ePDG, la información de cabecera externa de paquete IP puede contener asimismo el número de puerto de origen UDP IPSec. La información de cabecera externa de paquete IP puede contener asimismo información tal como la dirección de la ePDG, un número de puerto de destino UDP IPSec (con respecto a la dirección de enlace ascendente del UE) y tipos de protocolos y similares.

Indudablemente, durante la implementación específica, la información de cabecera externa de paquete IP puede ser un filtro de paquetes, y el filtro de paquetes contiene por lo menos la dirección IP local del UE. Si se detecta la NA(P)T entre el UE y la ePDG, el filtro de paquetes puede contener asimismo el número de puerto de origen UDP IPSec. El filtro de paquetes puede contener asimismo información tal como la dirección de la ePDG, el número de puerto de destino UDP IPSec (con respecto a la dirección de enlace ascendente del UE) y tipos de protocolos y similares.

En la etapa -803-, la PCRF devuelve a la ePDG el mensaje de acuse.

En la etapa -804-, después de seleccionar la P-GW, la ePDG envía un mensaje de actualización de vinculación de servidor intermediario a la P-GW, y el mensaje de actualización de vinculación de servidor intermediario lleva un identificador de usuario, un identificador de la PDN y la información de cabecera externa de paquete IP.

En la etapa -805-, la P-GW asigna una dirección IP al UE, y una PCEF ubicada en la P-GW envía un mensaje de indicación de establecimiento de sesión IP-CAN a la PCRF, y el mensaje de indicación de establecimiento de sesión IP-CAN lleva el identificador de usuario, el identificador de la PDN y la dirección IP asignada al UE.

En la etapa -806-, la PCRF lleva a cabo una estimación de acuerdo con el identificador de usuario y el identificador de la PDN, y si no existen datos relevantes de la suscripción de usuario, una H-PCRF interactuará con un SPR para obtener la información de la suscripción. La PCRF elabora reglas de PCC de acuerdo con los datos de la suscripción, las políticas de red y los atributos de la red de acceso y similares. La PCRF devuelve a la PCEF un mensaje de acuse que incluye las reglas de PCC.

En la etapa -807-, la P-GW envía un mensaje de actualización de la dirección IP de la P-GW al servidor de AAA y envía una dirección de la P-GW al servidor de AAA, y el servidor de AAA interactúa adicionalmente con el HSS y guarda la dirección de la P-GW en el HSS.

En la etapa -808-, la P-GW devuelve el mensaje de acuse de vinculación de servidor intermediario a la ePDG, y el mensaje de acuse de vinculación de servidor intermediario lleva la dirección IP asignada al UE.

En la etapa -809-, la actualización de vinculación de servidor intermediario es satisfactoria, y se establece el túnel IPSec entre el UE y la ePDG.

En la etapa -810-, la ePDG envía al UE una señalización IKEv2 final, en la que se incluye la dirección IP del UE.

En la etapa -811-, la PCRF determina una BPCF de la red de acceso del BBF a la que el UE accede actualmente de acuerdo con la información de cabecera externa de paquete IP, y envía a la BPCF el mensaje de establecimiento de sesión de control de pasarela iniciado por la PCRF, y la información de cabecera externa de paquete IP se incluye en el mensaje de establecimiento de sesión de control de pasarela.

La etapa -811- se puede ejecutar asimismo después de la etapa -802-.

En la etapa -812-, la BPCF proporciona cabeceras externas de los paquetes IP a una entidad de la red de acceso del BBF (por ejemplo BNG/BRAS).

En la etapa -813-, la entidad de la red de acceso del BBF devuelve el mensaje de acuse después de guardar las cabeceras externas de los paquetes IP.

En la etapa -814-, la BPCF devuelve el mensaje de acuse a la PCRF.

Por medio del flujo anterior, se establece una sesión entre la PCRF y la BPCF, y la red de acceso del BBF (BNG/BRAS) obtiene la información de cabecera externa de paquete IP. Si el UE requiere que la red asigne recursos al UE cuando el UE lleva a cabo el acceso al servicio, la PCRF envía en primer lugar a la BPCF la información de la QoS de las reglas de PCC elaboradas, para que la red de acceso del BBF ejecute el control de admisión. A continuación, la PCRF envía a la PCEF una regla del PCC aceptada por la red de acceso del BBF. La PCEF lleva a cabo el marcado DSCP en una cabecera de un paquete IP de los datos de enlace descendente de un flujo de datos correspondiente (denominada una cabecera interna de paquete) de acuerdo con la regla del PCC, cuando los paquetes IP del flujo de datos del servicio llegan a la ePDG, la ePDG llevará a cabo la encapsulación IPSec en el paquete IP y llevará a cabo la réplica DSCP. Cuando estos datos llegan a la red de acceso del BBF, la entidad de la red de acceso del BBF lleva a cabo en primer lugar el filtrado de acuerdo con la información de cabecera externa de paquete IP guardada, y solamente cuando los flujos de datos del servicio de la información de cabecera externa de paquete IP se corresponden, lleva a cabo la planificación de los datos de acuerdo con los DSCP; con respecto a los flujos de datos del servicio que no se corresponden, la entidad de la red de acceso del BBF lleva a cabo el procesamiento de acuerdo con las políticas locales (por ejemplo, se remarcan los DSCP con prioridades más bajas). Con respecto a los datos de enlace ascendente de los flujos de datos del servicio, el UE lleva a cabo la encapsulación IPSec y lleva a cabo la réplica DSCP, cuando los datos llegan a la red de acceso del BBF, la entidad de la red de acceso del BBF lleva a cabo en primer lugar el filtrado de acuerdo con la información de cabecera externa de paquete IP guardada, y solamente cuando los flujos de datos del servicio de la información de cabecera externa de paquete IP se corresponden, lleva a cabo la planificación de los datos de acuerdo con los DSCP; con respecto a los flujos de datos del servicio que no se corresponden, la entidad de la red de acceso del BBF lleva a cabo el procesamiento de acuerdo con las políticas locales (por ejemplo, se remarcan los DSCP con prioridades más bajas). De este modo, los flujos de datos del servicio que no pasan por el control de admisión no ocuparán recursos de otros flujos de datos del servicio que pasen por el control de admisión.

El ejemplo se aplica asimismo a escenarios de itinerancia (incluyendo un escenario de itinerancia con enrutamiento local o un escenario de itinerancia con desvío local).

Con respecto a un escenario de adopción de un protocolo GTP entre la DPG y la P-GW, el flujo es similar. La ePDG transportará la información de cabecera externa de paquete IP en el mensaje de petición de establecimiento de sesión.

Con respecto a un escenario en el que el UE accede a la red troncal 3GPP a través de una red de acceso fiable del BBF y el UE utiliza un acceso DSMIPv6,

(1) cuando se establece un túnel IPSec entre el UE y la P-GW para encapsular los datos del plano de usuario, la P-GW envía la información de cabecera externa de paquete IP (es decir, la información de cabecera externa de paquete IP del túnel IPSec) a la PCRF, la PCRF envía la información de cabecera externa de paquete IP a la BPCF, y a continuación la BPCF envía la información de cabecera externa de paquete IP a la entidad de la red de acceso del BBF. La entidad de la red de acceso del BBF lleva a cabo una equiparación en los paquetes de datos de acuerdo con la información de cabecera externa de paquete IP y además ejecuta la planificación de los paquetes de datos de acuerdo con los DSCP. Los flujos e ideas relevantes son similares al ejemplo anterior, y no se repetirán. Donde, la información de cabecera externa de paquete IP contiene por lo menos la dirección IP local del UE. Si se detecta la NA(P)T entre el UE y la ePDG, puede contener asimismose el número de puerto de origen UDP IPSec (con respecto a la dirección de enlace ascendente del UE). Indudablemente, también se puede incluir información tal como una dirección de la P-GW, el número de puerto de destino UDP de IPSec (con respecto a la dirección de enlace ascendente del UE) y tipos de protocolos, etc.

(2) cuando no se adopta el túnel IPSec entre el UE y la P-GW para encapsular los datos del plano de usuario, la P-GW envía la información de cabecera externa de paquete IP (es decir, la información de cabecera externa de paquete IP de un túnel DSMIPv6) a la PCRF, la PCRF envía la información de cabecera externa de paquete IP a la BPCF y, a continuación, la BPCF envía la información de cabecera externa de paquete IP a la entidad de la red de acceso del BBF. La entidad de la red de acceso del BBF lleva a cabo la equiparación en los paquetes de datos de acuerdo con la información de cabecera externa de paquete IP y ejecuta también la planificación de los paquetes de datos de acuerdo con los DSCP. Los flujos e ideas relevantes son similares al ejemplo anterior, y no se repetirán. Donde, la información de cabecera externa de paquete IP contiene por lo menos la dirección IP local del UE. Si se detecta la NA(P)T entre el UE y la ePDG, también se puede incluir un número de puerto de origen UDP de una señalización de actualización de vinculación DSMIPv6 (con respecto a la dirección de enlace ascendente del UE, el número de puerto es un número de puerto UDP asignado por la NAPT cuando la señalización de actualización de vinculación atraviesa la NAPT cuando el UE lleva a cabo la actualización de vinculación). Indudablemente, también se puede incluir información tal como una dirección de la P-GW, un número de puerto de destino UDP de la señalización de actualización de vinculación DSMIPv6 (con respecto a la dirección de enlace ascendente del UE) y tipos de protocolos, etc.

De igual modo, con respecto a un escenario en el que el UE accede a la red troncal 3GPP a través de la red de acceso no fiable del BBF y el UE utiliza el acceso DSMIPv6,

(1) cuando se establece un túnel IPSec entre el UE y la ePDG, todos los flujos de datos del servicio entre el UE y la P-GW se encapsularán con el túnel IPSec. La ePDG envía la información de cabecera externa de paquete IP (es decir, la información de cabecera externa de paquete IP del túnel IPSec) a la PCRF, la PCRF envía la información de cabecera externa de paquete IP a la BPCF y, a continuación, la BPCF envía la información de cabecera externa de paquete IP a la entidad de la red de acceso del BBF.

La entidad de la red de acceso del BBF lleva a cabo la equiparación en los paquetes de datos de acuerdo con la información de cabecera externa de paquete IP y ejecuta además la planificación de los paquetes de datos de acuerdo con los DSCP. Los flujos e ideas relevantes son similares al ejemplo anterior, y no se repetirán. Donde la anterior información de cabecera externa de paquete IP incluye por lo menos la dirección IP local del UE. Si se detecta la NA(P)T entre el UE y la ePDG, también se puede incluir el número de puerto de origen UDP IPSec (con respecto a la dirección de enlace ascendente del UE). También se puede incluir información tal como una dirección de la ePDG, un número de puerto de destino UDP IPSec (con respecto a la dirección de enlace ascendente del UE) y tipos de protocolos, etc.

Con respecto a la información de cabecera externa de paquete IP en los escenarios DSMIPv6 anteriores, ésta se puede implementar asimismo en forma de un filtro de paquetes.

Ejemplo 4

La figura 9 es un flujo de una entidad de la red de acceso del BBF que obtiene cabeceras externas de los paquetes IP durante el proceso de conexión del UE a un EPS bajo la arquitectura mostrada en la figura 3.

En la etapa -901-, después de que sea encendido un HeNB, éste obtiene una dirección IP (es decir, una dirección IP local) del Equipo de las instalaciones del cliente (Customer Premises Equipment, CPE) asignada por una red de acceso del BBF, y el HeNB utiliza la dirección IP del CPE para llevar a cabo una interacción de señalización IKEv2 con una SeGW y establece un túnel IPSec. En este proceso, la SeGW asigna una dirección IP del HeNB al HeNB, que se utiliza para que el HeNB interactúe con otros elementos de red 3GPP; y la SeGW obtiene la información de cabecera externa de paquete IP. Con respecto a un escenario con HeNB, todos los flujos de datos del servicio del HeNB se encapsularán con el túnel IPSec entre el HeNB y la SeGW. Por lo tanto, en ese momento, la información de cabecera externa de paquete IP puede ser la información de cabecera externa de paquete IP del túnel IPSec establecido entre el HeNB y la SeGW. Con el fin de identificar unívocamente este túnel IPSec, la información de cabecera externa de paquete IP del túnel IPSec incluye por lo menos una dirección de origen en una señalización IKEv2 enviada por el HeNB y recibida por la SeGW (es decir, una dirección de origen de IPSec, con respecto a una dirección de enlace ascendente del HeNB). La información de cabecera externa de paquete IP del túnel IPSec puede contener asimismo un número de puerto de origen en la señalización IKEv2 enviada por el HeNB y recibida por la SeGW (es decir, un número de puerto de origen IPSec, con respecto a la dirección de enlace ascendente del HeNB), una dirección de la SeGW, un número de puerto de recepción UDP de la SeGW (es decir, un número de puerto de destino, con respecto a la dirección de enlace ascendente del HeNB) y tipos de protocolos y similares.

Dado que la señalización IKEv2 puede haber pasado por la NAT transversal, la dirección de origen y el número de puerto de origen recibidos por la SeGW pueden ser diferentes de la dirección de origen y el número de puerto de origen cuando el HeNB lleva a cabo el envío. Si la señalización IKEv2 no pasa por el NA(P)T transversal, la dirección de origen es la dirección IP local obtenida cuando el HeNB accede a la red de acceso del BBF.

Con respecto a un escenario en el que no existe NAT entre el HeNB y la SeGW, la dirección de origen en la señalización IKEv2 enviada por el HeNB y recibida por la SeGW es la dirección IP local asignada por la red de acceso del BBF, y la dirección puede identificar unívocamente los flujos de datos del servicio del HeNB encapsulados con el túnel IPSec, por lo que la información de cabecera externa de paquete IP incluye por lo menos la dirección IP local.

Con respecto a un escenario de NAT (1:1) existente entre el HeNB y la SeGW, la dirección de origen en la señalización IKEv2 enviada por el HeNB y recibida por la SeGW es una dirección IP de red pública después de pasar por la NAT, pero debido a la NAT 1:1, la dirección puede seguir identificando unívocamente los flujos de datos del servicio del HeNB encapsulados con el túnel IPSec, por lo que la información de cabecera externa de paquete IP incluye por lo menos la dirección de origen en la señalización IKEv2 enviada por el HeNB y recibida por la SeGW (es decir, la dirección IP de red pública después de pasar por la NAT de la red de acceso del BBF, si la NAT está en una RG, la dirección es una dirección de la RG).

Con respecto a NAT (N:1) (es decir, NAPT) entre el HeNB y la SeGW, se debe llevar a cabo una encapsulación UDP en los flujos de datos del servicio durante el NAPT transversal, y la NAPT asignará un número de puerto de origen UDP (con respecto a la dirección de enlace ascendente del HeNB) al túnel IPSec. Por lo tanto, con el fin de identificar unívocamente los flujos de datos del servicio del UE encapsulados con el túnel IPSec, la información de cabecera externa de paquete IP contiene por lo menos la dirección de origen en la señalización IKEv2 enviada por el HeNB y recibida por la SeGW (es decir, la dirección IP de red pública después de pasar por la NAT de la red de acceso del BBF, si la NAT está en la RG, la dirección es una dirección de la RG) y el número de puerto de origen en la señalización IKEv2 enviada por el HeNB y recibida por la SeGW (es decir, un número de puerto de origen UDP IPSec).

Para mayor comodidad de las descripciones, la dirección IP del HeNB después de pasar por la NAT también se denomina como dirección IP local. Por lo tanto, la información de cabecera externa de paquete IP incluye por lo menos la dirección IP local del HeNB. Si se detecta la NA(P)T entre el HeNB y la SeGW, la información de cabecera externa de paquete IP puede contener asimismo el número de puerto de origen UDP IPSec. La información de cabecera externa de paquete IP puede contener asimismo información tal como la dirección de la SeGW, un número de puerto de destino UDP IPSec (con respecto a la dirección de enlace ascendente del HeNB) y tipos de protocolos y similares.

Indudablemente, durante la implementación específica, la información de cabecera externa de paquete IP puede ser un filtro de paquetes, y el filtro de paquetes contiene por lo menos la dirección IP local del HeNB. Si se detecta la NA(P)T entre el HeNB y la SeGW, el filtro de paquetes también puede contener el número de puerto de origen UDP IPSec. El filtro de paquetes también puede contener información tal como la dirección de la SeGW, el número de puerto de destino UDP IPSec (con respecto a la dirección de enlace ascendente del HeNB) y tipos de protocolos y similares.

En la etapa -902-, el UE envía al HeNB un mensaje de petición de conexión que incluye un identificador de usuario.

En la etapa -903-, el HeNB envía a un MME el mensaje de petición de conexión que incluye el identificador de usuario. Cuando el mensaje pasa por la SeGW, la SeGW añade la información de cabecera externa de paquete IP obtenida en la etapa -901- al mensaje que se llevará al MME.

En la etapa -904-, el MME envía a un HSS una petición de actualización de la posición que incluye el identificador de usuario.

En la etapa -905-, el HSS devuelve al MME una respuesta de actualización de la posición para devolver la información de suscripción del usuario.

En la etapa -906-, el MME envía a una S-GW una petición de establecimiento de sesión que incluye el identificador de usuario, un identificador de la PDN y la información de cabecera externa de paquete IP.

En la etapa -907-, la S-GW envía a una P-GW la petición de establecimiento de sesión que incluye el identificador de usuario, el identificador de la PDN y la información de cabecera externa de paquete IP.

En la etapa -908-, la P-GW envía a una PCRF una indicación de establecimiento de sesión IP-CAN que incluye el identificador de usuario, el identificador de la PDN y la información de cabecera externa de paquete IP.

En la etapa -909-, la PCRF determina una BPCF de la red de acceso del BBF a la que el UE accede actualmente de acuerdo con las cabeceras externas de los paquetes IP, y envía a la BPCF un mensaje de establecimiento de sesión de control de pasarela iniciado por la PCRF, y la información de cabecera externa de paquete IP se incluye en el mensaje de establecimiento de sesión de control de pasarela.

En la etapa -910-, la BPCF proporciona la información de cabecera externa de paquete IP a una entidad de la red de acceso del BBF (por ejemplo, BGN/BRAS).

En la etapa -911-, la entidad de la red de acceso del BBF devuelve el mensaje de acuse a la BPCF después de guardar la información de cabecera externa de paquete IP.

En la etapa -912-, la BPCF devuelve el mensaje de respuesta a la PCRF.

En la etapa -913-, la PCRF devuelve un acuse de establecimiento de sesión IP-CAN a una PCEF.

En la etapa -914-, la P-GW de pasarela en la que se encuentra la PCEF envía una respuesta de establecimiento de sesión a la S-GW.

En la etapa -915-, la S-GW devuelve la respuesta de establecimiento de sesión al MME.

En la etapa -916-, se lleva a cabo una interacción entre el MME, el HeNB y el UE para establecer una portadora radioeléctrica.

En la etapa -917-, el MME interactúa con la S-GW para actualizar la portadora.

Por medio del flujo anterior, se establece una sesión entre la PCRF y la BPCF, y la red de acceso del BBF (BNG/BRAS) obtiene la información de cabecera externa de paquete IP. Si el UE requiere que la red asigne recursos al UE cuando el UE lleva a cabo el acceso al servicio, la PCRF envía en primer lugar a la BPCF la información de la QoS de las reglas de PCC elaboradas, para que la red de acceso del BBF ejecute el control de admisión. A continuación, la PCRF envía a la PCEF una regla del PCC aceptada por la red de acceso del BBF. La PCEF lleva a cabo el marcado DSCP en una cabecera de un paquete IP de los datos de enlace descendente de un flujo de datos correspondiente (denominada una cabecera interna de paquete) de acuerdo con la regla del PCC, cuando los paquetes IP del flujo de datos del servicio llegan a la SeGW, la SeGW llevará a cabo una encapsulación IPSec en el paquete IP y llevará a cabo la réplica DSCP. Cuando estos datos llegan a la red de acceso del BBF, la entidad de la red de acceso del BBF lleva a cabo en primer lugar el filtrado de acuerdo con la información de cabecera externa de paquete IP guardada, y solamente cuando los flujos de datos del servicio de la información de cabecera externa de paquete IP se corresponden, lleva a cabo la planificación de los datos de acuerdo con los DSCP; con respecto a los flujos de datos del servicio que no se corresponden, la entidad de la red de acceso del BBF lleva a cabo el procesamiento de acuerdo con las políticas locales (por ejemplo, se remarcan los DSCP con prioridades más bajas). Con respecto a los datos de enlace ascendente de los flujos de datos del servicio, el HeNB lleva a cabo la encapsulación IPSec y lleva a cabo la réplica DSCP, cuando los datos llegan a la red de acceso del BBF, la entidad de la red de acceso del BBF lleva a cabo en primer lugar el filtrado de acuerdo con la información de cabecera externa de paquete IP guardada, y solamente cuando los flujos de datos del servicio de la información de cabecera externa de paquete IP se corresponden, lleva a cabo la planificación de los datos de acuerdo con los DSCP; con respecto a los flujos de datos del servicio que no se corresponden, la entidad de la red de acceso del BBF lleva a cabo el procesamiento de acuerdo con las políticas locales (por ejemplo, se remarcan los DSCP con prioridades más bajas). De este modo, los flujos de datos del servicio que no pasen por el control de admisión no ocuparán recursos de otros flujos de datos del servicio que pasen por el control de admisión.

Con respecto a un proceso de acceso de un HNB a un sistema UMTS a través de la conexión, el flujo en el que la entidad de la red de acceso del BBF obtiene la información de cabecera externa de paquete IP es similar a éste. En ese momento, la información de cabecera externa de paquete IP puede ser la información de cabecera externa de paquete IP de un túnel IPSec establecido entre el HNB y la SeGW. Con el fin de identificar unívocamente el túnel IPSec, la información de cabecera externa de paquete IP del túnel IPSec incluye por lo menos una dirección de origen en una señalización IKEv2 enviada por el HNB y recibida por la SeGW (es decir, una dirección de origen de IPSec, con respecto a la dirección de enlace ascendente del HNB). La información de cabecera externa de paquete IP del túnel IPSec puede contener asimismo un número de puerto de origen en la señalización IKEv2 enviada por el HNB y recibida por la SeGW (es decir, un número de puerto de origen IPSec, con respecto a la dirección de enlace ascendente del HNB) si se detecta la NA(P)T entre el HNB y la SeGW. Indudablemente, también se pueden incluir una dirección de la SeGW, un número de puerto de recepción UDP de la SeGW (es decir, un número de puerto de destino UDP, con respecto a la dirección de enlace ascendente del HNB) y tipos de protocolos, etc. De igual modo, la información de cabecera externa de paquete IP se puede implementar asimismo en una forma del filtro de paquetes.

En otros ejemplos, en la etapa -901-, la SeGW envía la información de cabecera externa de paquete IP al HeNB, en la etapa -902-, el HeNB envía la información de cabecera externa de paquete IP al MME, y el resto de etapas no cambian.

Ejemplo 5

La figura 10 es un flujo de una entidad de la red de acceso del BBF que obtiene las cabeceras externas de los paquetes IP después de que sea encendido un H(e)NB en la arquitectura de la figura 4.

En la etapa -1001-, después de que sea encendido el H(e)NB, éste obtiene una dirección IP del CPE (es decir, una dirección IP local) asignada por una red de acceso del BBF, y el H(e)NB utiliza la dirección IP del CPE para llevar a cabo una interacción de señalización IKEv2 con una SeGW y establece un túnel IPSec. En este proceso, la SeGW asigna una dirección IP del H(e)NB al H(e)NB que se utiliza para que el H(e)NB interactúe con otros elementos de red 3GPP.

En la etapa -1002-, la SeGW informa a una H(e)NB PF de una relación de asociación entre la dirección IP del CPE y la dirección IP del H(e)NB, donde se transporta la información de cabecera externa de paquete IP. Con respecto a un escenario con un H(e)NB, todos los flujos de datos del servicio del H(e)NB se encapsularán con el túnel IPSec entre el H(e)NB y la SeGW. Por lo tanto, en ese momento, la información de cabecera externa de paquete IP puede ser la información de cabecera externa de paquete IP del túnel IPSec establecido entre el H(e)NB y la SeGW. Con el fin de identificar unívocamente este túnel IPSec, la información de cabecera externa de paquete IP del túnel IPSec incluye por lo menos una dirección de origen en una señalización IKEv2 enviada por el H(e)NB y recibida por la SeGW (es decir, una dirección de origen de IPSec, con respecto a una dirección de enlace ascendente del H(e)NB. La información de cabecera externa de paquete IP del túnel IPSec puede contener asimismo un número de puerto de origen en la señalización IKEv2 enviada por el H(e)NB y recibida por la SeGW (es decir, un número de puerto de origen IPSec, con respecto a la dirección de enlace ascendente del H(e)NB), una dirección de la SeGW, un número de puerto de recepción UDP de la SeGW (es decir, un número de puerto de destino UDP, con respecto a la dirección de enlace ascendente del H(e)NB) y tipos de protocolos y similares.

Dado que la señalización IKEv2 puede haber pasado por el NA(P)T transversal, la dirección de origen y el número de puerto de origen recibidos por la SeGW pueden ser diferentes de la dirección de origen y el número de puerto de origen cuando el H(e)NB lleva a cabo el envío. Si la señalización IKEv2 no pasa por la NAT transversal, la dirección de origen es la dirección IP del CPE obtenida cuando el H(e)NB accede a la red de acceso del BBF.

Con respecto a un escenario en el que no existe NAT entre el N(e)NB y la SeGW, la dirección de origen en la señalización IKEv2 enviada por el H(e)NB y recibida por la SeGW es la dirección IP local asignada por la red de acceso del BBF, y la dirección puede identificar unívocamente los flujos de datos del servicio del H(e)NB encapsulados con el túnel IPSec, por lo que la información de cabecera externa de paquete IP contiene por lo menos la dirección IP local.

Con respecto a un escenario de NAT(1:1) existente entre el H(e)NB y la SeGW, la dirección de origen en la señalización IKEv2 enviada por el H(e)NB y recibida por la SeGW es una dirección IP de red pública después de pasar por la NAT, pero debido a la NAT 1:1, la dirección puede seguir identificando unívocamente los flujos de datos del servicio del H(e)NB encapsulados con el túnel IPSec, por lo que la información de cabecera externa de paquete IP contiene por lo menos la dirección de origen en la señalización IKEv2 enviada por el H(e)NB y recibida por la SeGW (es decir, la dirección IP de red pública después de pasar por la NAT de la red de acceso del BBF, si la NAT está en una RG, la dirección es una dirección de la RG).

Con respecto a NAT (N:1) (es decir, NAPT) entre el H(e)NB y la SeGW, es necesario llevar a cabo una encapsulación UDP en los flujos de datos del servicio durante el NAPT transversal, y la NAPT asignará un número de puerto de origen UDP (con respecto a la dirección de enlace ascendente del H(e)NB) al túnel IPSec. Por lo tanto,

con el fin de identificar unívocamente los flujos de datos del servicio del UE encapsulados con el túnel IPSec, la información de cabecera externa de paquete IP contiene por lo menos la dirección de origen en la señalización IKEv2 enviada por el H(e)NB y recibida por la SeGW (es decir, la dirección IP de red pública después de pasar por la NAT de la red de acceso del BBF, si la NAT está en la RG, la dirección es una dirección de la RG) y el número de puerto de origen en la señalización IKEv2 enviada por el H(e)NB y recibida por la SeGW (es decir, un número de puerto de origen UDP IPSec).

Para mayor comodidad de la descripción, la dirección IP del H(e)NB después de pasar por la NAT también se denomina como la dirección IP local. Por lo tanto, la información de cabecera externa de paquete IP incluye por lo menos la dirección IP local del H(e)NB. Si se detecta la NA(P)T entre el H(e)NB y la SeGW, la información de cabecera externa de paquete IP puede contener asimismo el número de puerto de origen UDP IPSec. La información de cabecera externa de paquete IP puede contener asimismo información tal como la dirección de la SeGW, un número de puerto de destino UDP IPSec (con respecto a la dirección de enlace ascendente del H(e)NB y tipos de protocolos y similares.

Indudablemente, durante la implementación específica, la información de cabecera externa de paquete IP puede ser un filtro de paquetes, y el filtro de paquetes contiene por lo menos la dirección IP local del H(e)NB. Si se detecta la NA(P)T entre el H(e)NB y la SeGW, el filtro de paquetes también puede contener el número de puerto de origen UDP IPSec. El filtro de paquetes también puede contener información tal como la dirección de la SeGW, el número de puerto de destino UDP IPSec (con respecto a la dirección de enlace ascendente del H(e)NB y tipos de protocolos y similares.

En la etapa -1003-, la H(e)NB PF devuelve un mensaje de aceptación después de guardar la relación de asociación.

En la etapa -1004-, se establece una conexión S1 o una conexión Iuh entre el H(e)NB y una H(e)NB GW o entre el H(e)NB y un MME.

En la etapa -1005-, se establece una sesión T2 entre la H(e)NB GW y la H(e)NB PF o entre el MME y la H(e)NB PF, en la que se transporta el ID de la CSG y la dirección IP del H(e)NB.

En la etapa -1006-, la H(e)NB PF asocia la sesión T2 con la etapa -1002- de acuerdo con la dirección IP del H(e)NB, obteniendo de ese modo la dirección IP del CPE del H(e)NB, y la H(e)NB PF determina una BPCF de la red de acceso del BBF a la que accede el H(e)NB de acuerdo con la dirección IP del CPE. La H(e)NB PF establece una sesión S9* con la BPCF, en la que se transporta la dirección IP del CPE y la información de cabecera externa de paquete IP.

En la etapa -1007-, la BPCF proporciona la información de cabecera externa de paquete IP a una entidad de la red de acceso del BBF (por ejemplo, BNG/BRAS).

En la etapa -1008-, la entidad de la red de acceso del BBF devuelve un mensaje de acuse a la BPCF después de guardar la información de cabecera externa de paquete IP.

En la etapa -1009-, la BPCF devuelve el mensaje de respuesta a la H(e)NB PF.

En la etapa -1010-, la H(e)NB PF devuelve el mensaje de respuesta a la H(e)NB GW o al MME.

Por medio del flujo anterior, se establece una sesión entre la H(e)NB PF y la BPCF, y la red de acceso del BBF (BNG/BRAS) obtiene la información de cabecera externa de paquete IP. Si el UE necesita que la red asigne recursos al UE cuando el UE lleva a cabo el acceso al servicio, la PCRF envía en primer lugar a la BPCF la información de la QoS de las reglas de PCC elaboradas, para que la red de acceso del BBF ejecute el control de admisión. A continuación, la PCRF envía a la PCEF una regla del PCC aceptada por la red de acceso del BBF. La PCEF lleva a cabo el marcado DSCP en una cabecera de un paquete IP de los datos de enlace descendente de un flujo de datos correspondiente (denominada una cabecera interna de paquete) de acuerdo con la regla del PCC, cuando los paquetes IP del flujo de datos del servicio llegan a la SeGW, la SeGW llevará a cabo la encapsulación IPSec en el paquete IP y llevará a cabo la réplica DSCP. Cuando estos datos llegan a la red de acceso del BBF, la entidad de la red de acceso del BBF lleva a cabo en primer lugar el filtrado de acuerdo con la información de cabecera externa de paquete IP guardada, y solamente cuando los flujos de datos del servicio de la información de cabecera externa de paquete IP se corresponden, lleva a cabo la planificación de los datos de acuerdo con los DSCP; con respecto a los flujos de datos del servicio que no se corresponden, la entidad de la red de acceso del BBF lleva a cabo el procesamiento de acuerdo con las políticas locales (por ejemplo, se remarcan los DSCP con prioridades más bajas). Con respecto a los datos de enlace ascendente de los flujos de datos del servicio, el H(e)NB lleva a cabo la encapsulación IPSec y lleva a cabo la réplica DSCP, cuando los datos llegan a la red de acceso del BBF, la entidad de la red de acceso del BBF lleva a cabo en primer lugar el filtrado de acuerdo con las cabeceras externas de los paquetes IP guardadas, y solamente cuando los flujos de datos del servicio de la información de cabecera externa de paquete IP se corresponden, lleva a cabo la planificación de los datos de acuerdo con los DSCP; con respecto a los flujos de datos del servicio que no se corresponden, la entidad de la red de acceso del

BBF lleva a cabo el procesamiento de acuerdo con las políticas locales (por ejemplo, se remarcan los DSCP con prioridades más bajas). Por lo tanto, los flujos de datos del servicio que no pasen por el control de admisión no ocuparán recursos de otros flujos de datos del servicio que pasen por el control de admisión.

En otros ejemplos, si no existe una interfaz entre la SeGW y la H(e)NB PF, en la etapa -1001-, la SeGW envía la información de cabecera externa de paquete IP al H(e)NB, la etapa -1002- y la etapa -1003- no se ejecutan, en la etapa -1004-, el H(e)NB envía la información de cabecera externa de paquete IP a la H(e)NB PF, y el resto de etapas no cambian.

Ejemplo 6

La figura 11 es un flujo de una entidad de la red de acceso del BBF que obtiene las cabeceras externas de los paquetes IP después de que sea encendido un H(e)NB bajo la arquitectura de la figura 5.

En la etapa -1101-, después de que sea encendido el H(e)NB, éste obtiene una dirección IP (es decir, una dirección IP local) del Equipo de las instalaciones del cliente (CPE) asignada por una red de acceso del BBF, y el H(e)NB utiliza la dirección IP del CPE para llevar a cabo la interacción de señalización IKEv2 con una SeGW y establece un túnel IPSec. En este proceso, la SeGW asigna una dirección IP del H(e)NB al H(e)NB que se utiliza para que el H(e)NB interactúe con otros elementos de la red 3GPP.

En la etapa -1102-, la SeGW informa a una H(e)NB PF de una relación de asociación entre la dirección IP del CPE y la dirección IP del H(e)NB, donde se transporta la información de cabecera externa de paquete IP. Con respecto a un escenario con H(e)NB, todos los flujos de datos del servicio del H(e)NB se encapsularán con el túnel IPSec entre el H(e)NB y la SeGW. Por lo tanto, en ese momento, la información de cabecera externa de paquete IP puede ser la información de cabecera externa de paquete IP del túnel IPSec establecido entre el H(e)NB y la SeGW. Con el fin de identificar unívocamente este túnel IPSec, la información de cabecera externa de paquete IP del túnel IPSec incluye por lo menos una dirección de origen en la señalización IKEv2 enviada por el H(e)NB y recibida por la SeGW (es decir, una dirección de origen IPSec, con respecto a una dirección de enlace ascendente del H(e)NB). La información de cabecera externa de paquete IP del túnel IPSec puede contener asimismo un número de puerto de origen en la señalización IKEv2 enviada por el H(e)NB y recibida por la SeGW (es decir, un número de puerto de origen IPSec, con respecto a la dirección de enlace ascendente del H(e)NB), una dirección de la SeGW, un número de puerto de recepción UDP de la SeGW (es decir, un número de puerto de destino del UDP, con respecto a la dirección de enlace ascendente del H(e)NB) y tipos de protocolos y similares.

Dado que la señalización IKEv2 puede haber pasado por la NAT transversal, la dirección de origen y el número de puerto de origen recibidos por la SeGW pueden ser diferentes de la dirección de origen y el número de puerto de origen cuando el UE lleva a cabo el envío. Si la señalización IKEv2 no pasa por la NAT transversal, la dirección de origen es una dirección IP del CPE obtenida cuando el UE accede a la red de acceso del BBF.

Con respecto a un escenario en el que no existe NAT entre el H(e)NB y la SeGW, la dirección de origen en la señalización IKEv2 enviada por el H(e)NB y recibida por la SeGW es la dirección IP local asignada por la red de acceso del BBF, y la dirección puede identificar unívocamente los flujos de datos del servicio del H(e)NB encapsulados con el túnel IPSec, por lo que la información de cabecera externa de paquete IP contiene por lo menos la dirección IP local.

Con respecto a un escenario de NAT (1:1) existente entre el H(e)NB y la SeGW, la dirección de origen en la señalización IKEv2 enviada por el H(e)NB y recibida por la SeGW es una dirección IP de red pública después de pasar por la NAT, pero debido a la NAT 1:1, la dirección puede seguir identificando unívocamente los flujos de datos del servicio del H(e)NB encapsulados con el túnel IPSec, por lo que la información de cabecera externa de paquete IP contiene por lo menos la dirección de origen en la señalización IKEv2 enviada por el H(e)NB y recibida por la SeGW (es decir, la dirección IP de red pública después de pasar por la NAT de la red de acceso del BBF, si la NAT está en una RG, la dirección es una dirección de la RG).

Con respecto a NAT (N:1) (es decir, NAPT) entre el H(e)NB y la SeGW, es necesario llevar a cabo una encapsulación UDP en los flujos de datos del servicio durante el NAPT transversal, y la NAPT asignará un número de puerto de origen UDP (con respecto a la dirección de enlace ascendente del H(e)NB) al túnel IPSec. Por lo tanto, con el fin de identificar unívocamente los flujos de datos del servicio del UE encapsulados con el túnel IPSec, la información de cabecera externa de paquete IP contiene por lo menos la dirección de origen en la señalización IKEv2 enviada por el H(e)NB y recibida por la SeGW (es decir, la dirección IP de red pública después de pasar por la NAT de la red de acceso del BBF, si la NAT está en la RG, la dirección es una dirección de la RG) y el número de puerto de origen en la señalización IKEv2 enviada por el H(e)NB y recibida por la SeGW (es decir, un número de puerto de origen UDP IPSec).

Para mayor comodidad de la descripción, la dirección IP del H(e)NB después de pasar por la NAT también se denomina como la dirección IP local. Por lo tanto la información de cabecera externa de paquete IP incluye por lo menos la dirección IP del H(e)NB. Si se detecta la NA(P)T entre el H(e)NB y la SeGW, la información de cabecera

externa de paquete IP puede contener asimismo el número de puerto de origen UDP IPSec. La información de cabecera externa de paquete IP puede contener asimismo información tal como la dirección de la SeGW, un número de puerto de destino UDP IPSec (con respecto a la dirección de enlace ascendente del H(e)NB) y tipos de protocolos y similares.

Indudablemente, durante la implementación específica, la información de cabecera externa de paquete IP puede ser un filtro de paquetes, y el filtro de paquetes contiene por lo menos la dirección IP local del H(e)NB. Si se detecta la NA(P)T entre el H(e)NB y la SeGW, el filtro de paquetes también puede contener el número de puerto de origen UDP IPSec. El filtro de paquetes también puede contener información tal como la dirección de la SeGW, el número de puerto de destino UDP IPSec (con respecto a la dirección de enlace ascendente del H(e)NB) y tipos de protocolos y similares.

En la etapa -1103-, la H(e)NB PF devuelve el mensaje de aceptación después de guardar la relación de asociación.

En la etapa -1104-, se establece una conexión S1 o una conexión Iuh entre el H(e)NB y una H(e)NB GW o entre el H(e)NB y un MME.

En la etapa -1105-, se establece una sesión T2 entre el H(e)NB y la H(e)NB PF, en la que se transporta un ID de la CSG y la dirección IP del H(e)NB.

En la etapa -1106-, la H(e)NB PF asocia la sesión T2 con la etapa -1102- de acuerdo con la dirección IP del H(e)NB, obteniendo de este modo la dirección IP del CPE del H(e)NB, y la H(e)NB PF determina una BPCF de la red de acceso del BBF a la que accede el H(e)NB de acuerdo con la dirección IP del CPE. La H(e)NB PF establece una sesión S9* con la BPCF, en la que se transporta la dirección IP del CPE y la información de cabecera externa de paquete IP.

En la etapa -1107- la BPCF proporciona la información de cabecera externa de paquete IP a una entidad de la red de acceso del BBF (por ejemplo, BNG/BRAS).

En la etapa -1108-, la entidad de la red de acceso del BBF devuelve un mensaje de acuse a la BPCF después de guardar la información de cabecera externa de paquete IP.

En la etapa -1109-, la BPCF devuelve un mensaje de respuesta a la H(e)NB PF.

En la etapa -1110-, la H(e)NB PF devuelve el mensaje de respuesta al H(e)NB.

Por medio del flujo anterior, se establece una sesión entre la H(e)NB PF y la BPCF, y la red de acceso del BBF (BNG/BRAS) obtiene la información de cabecera externa de paquete IP. Si el UE requiere que la red asigne recursos al UE cuando el UE lleva a cabo el acceso al servicio, la PCRF envía en primer lugar a la BPCF información de la QoS de las reglas de PCC elaboradas, para que la red de acceso del BBF ejecute el control de admisión. A continuación, la PCRF envía a la PCEF una regla del PCC aceptada por la red de acceso del BBF. La PCEF lleva a cabo el marcado DSCP en una cabecera de un paquete IP de los datos de enlace descendente de un flujo de datos correspondiente (denominada cabecera interna de paquete) de acuerdo con la regla del PCC, cuando los paquetes IP del flujo de datos del servicio llegan a la SeGW, la SeGW llevará a cabo una encapsulación IPSec en el paquete IP y llevará a cabo la réplica DSCP. Cuando estos datos llegan a la red de acceso del BBF, la entidad de la red de acceso del BBF lleva a cabo en primer lugar el filtrado de acuerdo con la información de cabecera externa de paquete IP guardada, y solamente cuando los flujos de datos del servicio de la información de cabecera externa de paquete IP se corresponden, lleva a cabo la planificación de los datos de acuerdo con los DSCP; con respecto a los flujos de datos del servicio sin coincidencia, la entidad de la red de acceso del BBF lleva a cabo el procesamiento de acuerdo con las políticas locales (por ejemplo, se remarcan los DSCP con prioridades más bajas). Con respecto a los datos de enlace ascendente de los flujos de datos del servicio, el UE lleva a cabo la encapsulacion IPSec y lleva a cabo la réplica DSCP, cuando los datos llegan la red de acceso del BBF, la entidad de la red de acceso del BBF en primer lugar lleva a cabo el filtrado de acuerdo con la información de cabecera externa de paquete IP guardada, y solamente cuando los flujos de datos del servicio de la información de cabecera externa de paquete IP se corresponden, lleva a cabo la planificación de los datos de acuerdo con los DSCP; con respecto a los flujos de datos del servicio que no se corresponden, la entidad de la red de acceso del BBF lleva a cabo el procesamiento de acuerdo con las políticas locales (por ejemplo, se remarcan los DSCP con prioridades inferiores). De este modo, los flujos de datos del servicio que no pasen por el control de admisión no ocuparán recursos de otros flujos de datos del servicio que pasen por el control de admisión.

En otros ejemplos, si no existe una interfaz entre la SeGW y la H(e)NB PF, en la etapa -1101-, la SeGW envía la información de cabecera externa de paquete IP al H(e)NB, la etapa -1102- y la etapa -1103- no se ejecutan, en la etapa -1104-, el H(e)NB envía la información de cabecera externa de paquete IP a la H(e)NB PF, y el resto de etapas no cambian.

Con respecto a todos los ejemplos anteriores, cuando la entidad de la red de acceso del BBF lleva a cabo la equiparación en los paquetes IP de acuerdo con la información de cabecera externa de paquete IP, si no se equipara ningún paquete IP, solamente cuando se produce congestión de red, éste lleva a cabo la planificación de los datos de acuerdo con las políticas locales, y si los recursos siguen siendo suficientes actualmente, sigue llevando a cabo el envío de acuerdo con los DSCP.

Los procedimientos que son aplicables al escenario de convergencia en el que hay una interfaz directa entre la PCRF y el BNG/BRAS mientras que no se produce la BPCF son similares a los procedimientos anteriores. La única excepción es que la información de cabecera externa de paquete IP se envía mediante la PCRF al BNG/BRAS directamente sin pasar por la BPCF.

El presente documento también proporciona un sistema de control de políticas, que incluye: una entidad de red 3GPP y una entidad de la red de acceso del Foro de banda ancha (BBF), en que:

la entidad de red 3GPP está configurada para: enviar la información de cabecera externa de paquete IP a la entidad de la red de acceso del BBF;

la entidad de la red de acceso del BBF está configurada para: planificar un paquete de datos que corresponde a la información de cabecera externa de paquete IP de acuerdo con un Punto de código de servicios diferenciados (DSCP) del paquete de datos.

Donde, la entidad de la red de acceso del BBF está configurada además para: planificar un paquete de datos que no se corresponde con la información de cabecera externa de paquete IP de acuerdo con una política local.

Donde, el sistema incluye asismismo una Estructura de control de políticas de banda ancha (BPCF), y la entidad de red 3GPP incluye una Pasarela de datos por paquetes evolucionada (ePDG) y una Función de reglas de políticas y tarificación (PCRF), en que:

la ePDG está configurada para enviar la información de cabecera externa de paquete IP a una Pasarela de red de datos por paquetes (P-GW), y la P-GW envía la información de cabecera externa de paquete IP a la Función de reglas de políticas y tarificación (PCRF); o la ePDG envía directamente la información de cabecera externa de paquete IP a la PCRF.

la PCRF está configurada para: enviar la información de cabecera externa de paquete IP a la BPCF;

la BPCF está configurada para: enviar la información de cabecera externa de paquete IP a la entidad de la red de acceso del BBF.

O, la entidad de red 3GPP incluye una P-GW y una PCRF:

la P-GW está configurada para: enviar la información de cabecera externa de paquete IP a la PCRF;

la PCRF está configurada para: enviar la información de cabecera externa de paquete IP a la BPCF o a la entidad de la red de acceso del BBF;

la BPCF está configurada para: enviar la información de cabecera externa de paquete IP a la entidad de la red de acceso del BBF.

La PCRF está configurada para enviar la información de cabecera externa de paquete IP a la BPCF o a la entidad de la red de acceso del BBF del siguiente modo: cuando se lleva a cabo la autorización de la calidad de servicio, envía la información de cabecera externa de paquete IP a la BPCF o a la entidad de la red de acceso del BBF; o, cuando se inicia un establecimiento de sesión de interconexión de políticas con el BPCF o la entidad de la red de acceso del BBF, envía la información de cabecera externa de paquete IP a la BPCF o a la entidad de la red de acceso del BBF.

Donde, el sistema incluye asismismo una Estructura de control de políticas de banda ancha (BPCF), y la entidad de red 3GPP incluye una Pasarela de seguridad y una Función de políticas de H(e)NB, o incluye una Pasarela de seguridad y una PCRF, en que:

la Pasarela de seguridad está configurada para: enviar la información de cabecera externa de paquete IP a la Función de políticas de H(e)NB;

la Función de políticas de H(e)NB está configurada para: enviar la información de cabecera externa de paquete IP a la BPCF;

la BPCF está configurada para: enviar la información de cabecera externa de paquete IP a la entidad de la red de acceso del BBF.

O,

la Pasarela de seguridad está configurada para: enviar la información de cabecera externa de paquete IP a la PCRF;

la PCRF está configurada para: enviar la información de cabecera externa de paquete IP a la BPCF o a la entidad de la red de acceso del BBF;

la BPCF está configurada para: enviar la información de cabecera externa de paquete IP a la entidad de la red de acceso del BBF.

Donde, la función de políticas de H(e)NB o la PCRF está configurada para enviar la información de cabecera externa de paquete IP a la BPCF o a la entidad de la red de acceso del BBF del siguiente modo: cuando se inicia un establecimiento de sesión de interconexión de políticas con la BPCF o la entidad de la red de acceso del BBF, envía la información de cabecera externa de paquete IP a la BPCF o a la entidad de la red de acceso del BBF.

Donde, la información de cabecera externa de paquete IP es la información de cabecera externa de paquete IP de un túnel IPSec. El túnel IPSec es un túnel IPSec entre el equipo de usuario y la ePDG, o entre el equipo de usuario y la P-GW, o entre el H(e)NB y la pasarela de seguridad.

La descripción anterior incluye solamente los ejemplos preferentes del presente documento, que no se utiliza para limitar el alcance de la protección del presente documento. Todas las modificaciones, sustituciones equivalentes y mejoras, etc. llevadas a cabo dentro del principio del presente documento quedarán dentro del alcance de la protección del presente documento.

Aplicabilidad industrial

En el esquema técnico anterior, la red de acceso del BBF guarda las cabeceras externas de los paquetes IP, cuando los datos llegan a la red de acceso del BBF, la entidad de la red de acceso del BBF lleva a cabo en primer lugar el filtrado de acuerdo con las cabeceras externas de los paquetes IP guardadas, y solamente cuando los flujos de datos del servicio de las cabeceras externas de los paquetes IP se corresponden, lleva a cabo la planificación de los datos de acuerdo con los DSCP; con respecto a los flujos de datos del servicio que no se corresponden, la entidad de la red de acceso del BBF lleva a cabo un procesamiento de acuerdo con las políticas locales (por ejemplo, se remarcan los DSCP con prioridades más bajas). De este modo, los flujos de datos del servicio que no pasen por el control de admisión no ocuparán recursos de otros flujos de datos del servicio que pasen por el control de admisión. Por lo tanto, el presente documento tiene una aplicabilidad industrial extremadamente potente.

REIVINDICACIONES

1. Procedimiento de control de políticas, caracterizado porque comprende que:

una entidad de la red de acceso del Foro de banda ancha, BBF, recibe y guarda la información de cabecera externa de paquete IP, Protocolo de Internet, enviada por una entidad de red del Proyecto de asociación de tercera generación, 3GPP; en que dicha cabecera externa de paquete IP es una cabecera de un paquete IP de un Protocolo de seguridad de Internet, IPSec, o es una cabecera de un soporte IPv6 móvil para un túnel de anfitriones y encaminadores de doble pila DSMIPv6;

la entidad de la red de acceso del BBF lleva a cabo el filtrado de acuerdo con la información de cabecera externa de paquete IP recibida, cuando los datos llegan a la red de acceso del BBF;

la entidad de la red de acceso del BBF planifica un paquete de datos de acuerdo con un Punto de código de servicios diferenciados, DSCP, del paquete de datos cuando una información de cabecera externa de paquete IP del paquete de datos se corresponde con la información de cabecera externa de paquete IP recibida por la entidad de la red de acceso del BBF, y la entidad de la red de acceso del BBF planifica el paquete de datos que no se corresponde con la información de cabecera externa de paquete IP recibida y guardada por la entidad de la red de acceso del BBF de acuerdo con una política de la entidad de la red de acceso del BBF.

2. Procedimiento de control de políticas, según la reivindicación 1, en el que, la etapa de que la entidad de la red de acceso del BBF recibe la información de cabecera externa de paquete IP enviada por una entidad de red 3GPP comprende que:

una Pasarela de datos por paquetes evolucionada, ePDG, de una red 3GPP envía la información de cabecera externa de paquete IP a una Función de reglas de políticas y tarificación, PCRF, a través de una Pasarela de red de datos por paquetes, P-GW, enviando la PCRF la información de cabecera externa de paquete IP a una Estructura de control de políticas de banda ancha, BPCF, de una red de acceso del BBF, y enviando la BPCF la información de cabecera externa de paquete IP a la entidad de la red de acceso del BBF; o,

la ePDG envía directamente la información de cabecera externa de paquete IP a la PCRF, enviando la PCRF la información de cabecera externa de paquete IP a la BPCF, y enviando la BPCF la información de cabecera externa de paquete IP a la entidad de la red de acceso del BBF; o

la P-GW envía la información de cabecera externa de paquete IP a la PCRF, enviando la PCRF la información de cabecera externa de paquete IP a la BPCF, y enviando la BPCF la información de cabecera externa de paquete IP a la entidad de la red de acceso del BBF; o

la ePDG envía la información de cabecera externa de paquete IP a la PCRF a través de la P-GW, enviando la PCRF la información de cabecera externa de paquete IP a la entidad de la red de acceso del BBF; o,

la ePDG envía directamente la información de cabecera externa de paquete IP a la PCRF, enviando la PCRF la información de cabecera externa de paquete IP a la entidad de la red de acceso del BBF; o,

la P-GW envía la información de cabecera externa de paquete IP a la PCRF, enviando la PCRF la información de cabecera externa de paquete IP a la entidad de la red de acceso del BBF.

3. Procedimiento de control de políticas, según la reivindicación 1, en el que, la etapa de que una entidad de la red de acceso del BBF recibe la información de cabecera externa de paquete IP enviada por una entidad de red 3GPP comprende que:

una Pasarela de seguridad, SeGW, de la red 3GPP envía la información de cabecera externa de paquete IP a una Función de políticas de H(e)NB, H(e)NB PF, de la red de acceso del BBF, enviando la H(e)NB PF la información de cabecera externa de paquete IP a la BPCF, y enviando la BPCF la información de cabecera externa de paquete IP a la entidad de la red de acceso del BBF; o,

la SeGW envía la información de cabecera externa de paquete IP a la PCRF, enviando la PCRF la información de cabecera externa de paquete IP a la BPCF, y enviando la BPCF la información de cabecera externa de paquete IP a la entidad de la red de acceso del BBF; o

la SeGW de la red 3GPP envía la información de cabecera externa de paquete IP a la H(e)NB PF, enviando la H(e)NB PF la información de cabecera externa de paquete IP a la entidad de la red de acceso del BBF; o,

la SeGW envía la información de cabecera externa de paquete IP a la PCRF, enviando la PCRF la información de cabecera externa de paquete IP a la entidad de la red de acceso del BBF.

4. Procedimiento de control de políticas, según la reivindicación 3, en el que, la etapa de que la H(e)NB PF envía la información de cabecera externa de paquete IP a la BPCF comprende que:

cuando se inicia un establecimiento de sesión de interconexión de políticas con la BPCF, la H(e)NB PF envía la información de cabecera externa de paquete IP a la BPCF;

la etapa de que la PCRF envía la información de cabecera externa de paquete IP a la BPCF comprende que:

cuando se inicia el establecimiento de sesión de interconexión de políticas con la BPCF, la PCRF envía la información de cabecera externa de paquete IP a la BPCF.

5. Procedimiento de control de políticas, según cualquiera de las reivindicaciones 1 o 2, en el que, la información de cabecera externa de paquete IP comprende por lo menos una dirección IP de un equipo de usuario, UE, obtenida de la entidad de la red de acceso del BBF;

o,

en el que, la información de cabecera externa de paquete IP comprende una dirección IP de una ePDG o una P-GW y una dirección IP de un equipo de usuario, UE, obtenidas de la entidad de la red de acceso del BBF;

o,

en el que, si se detecta una NA(P)T entre el UE y la ePDG o entre el UE y la P-GW, la información de cabecera externa de paquete IP comprende un número de puerto de origen del Protocolo de datagramas de usuario, UDP, y la dirección IP del UE obtenida de la entidad de la red de acceso del BBF,

en el que, el número de puerto de origen UDP es un número de puerto de origen UDP IPSec o un número de puerto de origen UDP de una señalización de actualización de vinculación DSMIP.

6. Procedimiento de control de políticas, según la reivindicación 1, 3 o 4, en el que, la información de cabecera externa de paquete IP comprende por lo menos una dirección IP de un H(e)NB obtenida de la entidad de la red de acceso del BBF,

o,

en el que, si se detecta una NA(P)T entre el H(e)NB y la SeGW, la información de cabecera externa de paquete IP comprende un número de puerto de origen UDP y la dirección IP del H(e)NB obtenida de la entidad de la red de acceso del BBF,

en el que, el número de puerto de origen UDP es un número de puerto de origen UDP IPSec.

7. Procedimiento de control de políticas, según la reivindicación 5 o 6, en el que la información de cabecera externa de paquete IP es un filtro de paquetes que contiene la información correspondiente.

8. Sistema de control de políticas, **caracterizado porque**, comprende:

una entidad de red 3GPP y una entidad de la red de acceso del Foro de banda ancha, BBF, en el que:

la entidad de red 3GPP está configurada para enviar la información de cabecera externa de paquete IP a la entidad de la red de acceso del BBF; en el que dicha cabecera externa de paquete IP es una cabecera de paquete IP de protocolo de seguridad de Internet, IPSec, o es una cabecera de soporte IPV6 móvil para un túnel de anfitriones y encaminadores de doble pila DSMIPv6;

la entidad de la red de acceso del BBF está configurada para llevar a cabo el filtrado de acuerdo con la información de cabecera externa de paquete IP recibida cuando los datos llegan a la red de acceso del BBF;

la entidad de la red de acceso del BBF está configurada para planificar un paquete de datos de acuerdo con un Punto de código de servicios diferenciados, DSCP, del paquete de datos cuando una información de cabecera externa de paquete IP del paquete de datos se corresponde con la información de cabecera externa de paquete IP recibida y guardada por la entidad de la red de acceso del BBF, y la entidad de la red de acceso del BBF planifica el paquete de datos que no se corresponde con la información de cabecera externa de paquete IP recibida y guardada por la entidad de la red de acceso del BBF de acuerdo con una política de la entidad de la red de acceso del BBF.

9. Sistema de control de políticas, según la reivindicación 8, en el que, la información de cabecera externa de paquete IP comprende por lo menos una dirección IP de un equipo de usuario, UE, o una dirección IP de un H(e)NB obtenida de la entidad de la red de acceso del BBF,

o,

en el caso en que la información de cabecera externa de paquete IP comprende una dirección IP de un equipo de usuario, UE, obtenida de la entidad de la red de acceso del BBF y, en el que la información de cabecera externa de paquete IP comprende una dirección IP de la ePDG o la P-GW,

o,

en el que si se detecta una NA(P)T entre el UE y la ePDG o entre el UE y la P-GW, la información de cabecera externa de paquete IP comprende un número de puerto de origen UDP y la dirección IP del UE obtenida de la entidad de la red de acceso del BBF,

en el que, el número de puerto de origen UDP es un número de puerto de origen UDP IPSec o un número de puerto de origen UDP de una señalización de actualización de vinculación DSMIP,

en el caso en que la información de cabecera externa de paquete IP comprende por lo menos una dirección IP de un H(e)NB obtenida de la entidad de la red de acceso del BBF y, en el que, si se detecta una NA(P)T entre el H(e)NB y la SeGW, la información de cabecera externa de paquete IP comprende un número de puerto de origen UDP,

en el que, el número de puerto de origen UDP es un número de puerto de origen UDP IPSec.

10. Sistema de control de políticas, según la reivindicación 9, en el que, la información de cabecera externa de paquete IP es un filtro de paquetes que contiene la información correspondiente.

11. Sistema de la red de acceso del Foro de banda ancha, BBF, **caracterizado porque** comprende una entidad de la red de acceso del BBF, en el que:

la entidad de la red de acceso del BBF está configurada para: recibir y guardar la información de cabecera externa de paquete IP enviada por una red del Proyecto de asociación de tercera generación, 3GPP, en el que dicha cabecera externa de paquete IP es una cabecera de un paquete IP de Protocolo de seguridad de Internet, IPSec, o es una cabecera de soporte IPv6 móvil para un túnel de anfitriones y encaminadores de doble pila DSMIPv6; llevar a cabo el filtrado de acuerdo con la información de cabecera externa de paquete IP recibida cuando los datos llegan a la red de acceso del BBF; y planificar un paquete de datos de acuerdo con un Punto de código de servicios diferenciados, DSCP, del paquete de datos cuando una información de cabecera externa de paquete IP del paquete de datos se corresponde con la información de cabecera externa de paquete IP recibida y guardada por la entidad de la red de acceso del BBF, y planificar el paquete de datos que no se corresponde con la información de cabecera externa de paquete IP recibida y guardada por la entidad de la red de acceso del BBF de acuerdo con una política de la entidad de la red de acceso del BBF.

12. Sistema de la red de acceso del BBF, según la reivindicación 11, que comprende además: una Estructura de control de políticas de banda ancha, BPCF, en el que:

la BPCF está configurada para: después de que una Pasarela de datos por paquetes evolucionada, ePDG, de la red 3GPP envía la información de cabecera externa de paquete IP a una Función de reglas de políticas y tarificación, PCRF, a través de una Pasarela de red de datos por paquetes, P-GW, recibir la información de cabecera externa de paquete IP enviada por la PCRF; o después de que la ePDG envía directamente la información de cabecera externa de paquete IP a la PCRF, recibir la información de cabecera externa de paquete IP enviada por la PCRF; o después de que la P-GW envía la información de cabecera externa de paquete IP a la PCRF, recibir la información de cabecera externa de paquete IP enviada por la PCRF, y enviar la información de cabecera externa de paquete IP a la entidad de la red de acceso del BBF; o,

recibir la información de cabecera externa de paquete IP enviada por una Pasarela de seguridad, SeGW, de la red 3GPP a través de una Función de políticas de H(e)NB, H(e)NB PF, de una red de acceso del BBF; o recibir la información de cabecera externa de paquete IP enviada por la SeGW a través de la PCRF, y enviar la información de cabecera externa de paquete IP a la entidad de la red de acceso del BBF.

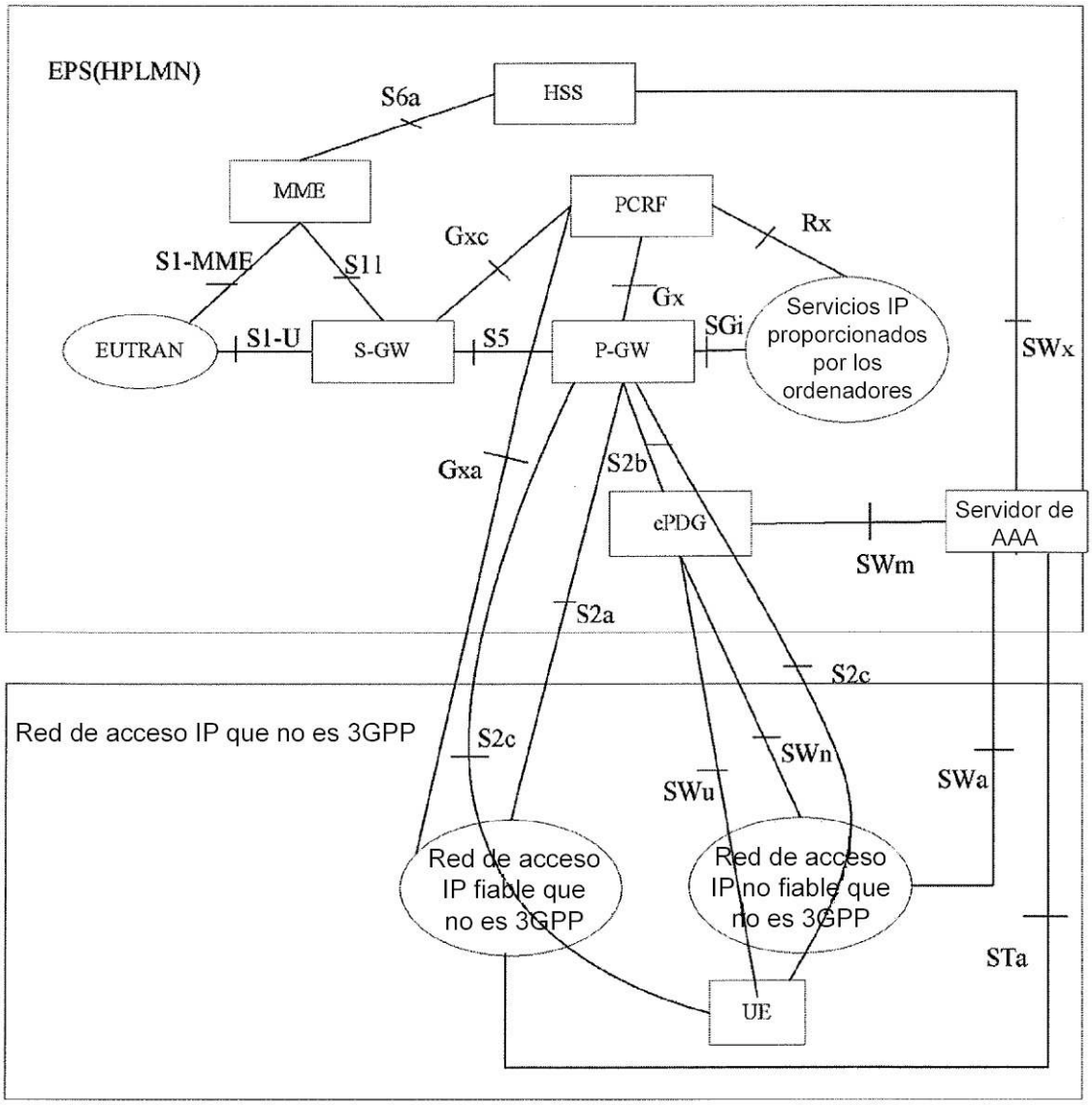
EPS(HPLMN)
HSS
S6a
MME
PCRF
Rx
Gxc
S1-MME
S11
Gx
Servicios IP proporcionados por los ordenadores
SGi
EUTRAN
S1-U
S-GW
S5
P-GW
SWx
Gxa
S2b
ePDG
Servidor de AAA
SWm
S2a
S2c
Red de acceso IP que no es 3GPP
S2c
SWn
SWu
SWa
Red de acceso IP fiable que no es 3GPP
Red de acceso IP no fiable que no es 3GPP
STa
UE

FIG. 1

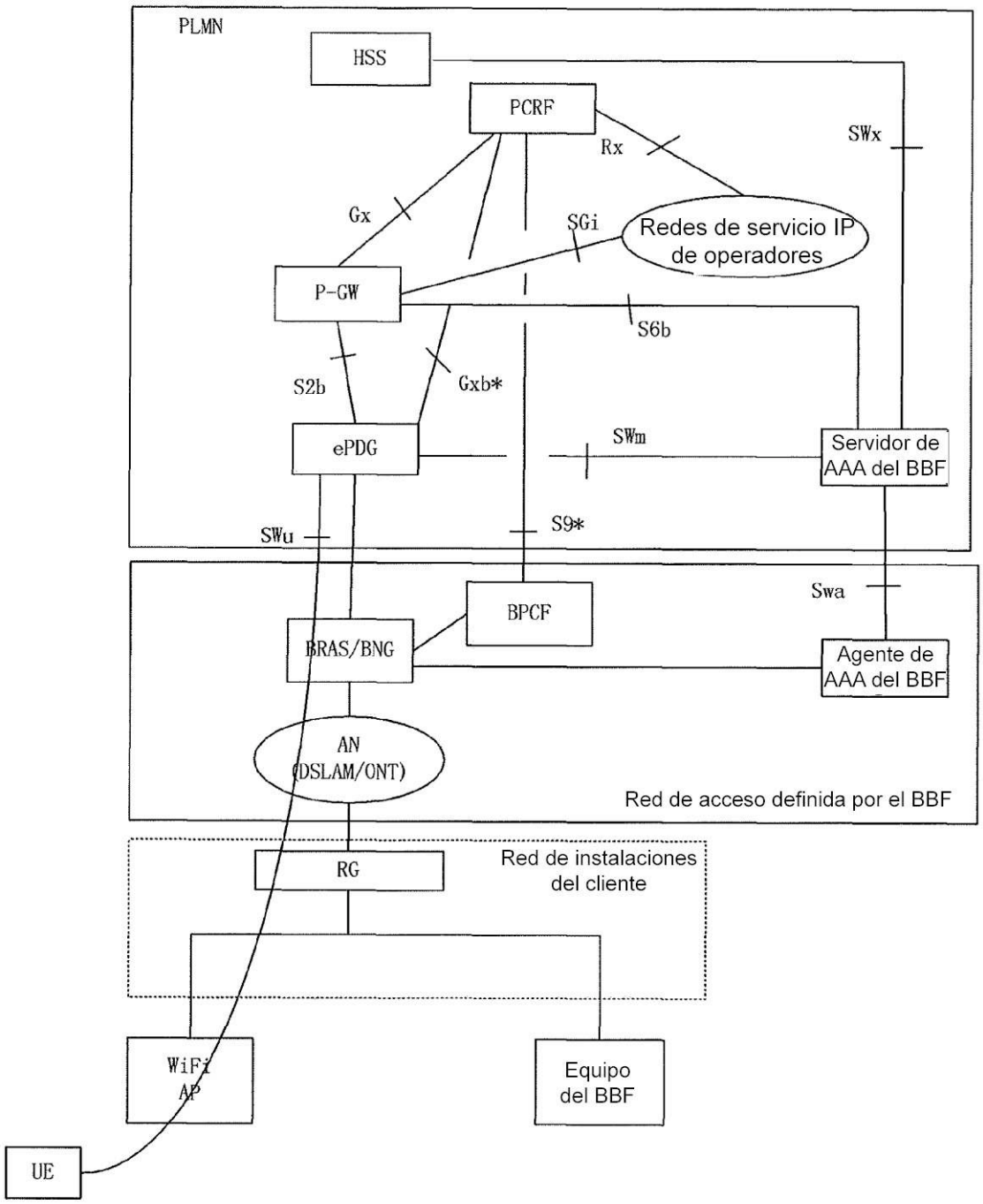
PLMN
HSS
PCRF
SWx
Rx
Gx
SGi
Redes de servicio IP de operadores
P-GW
S6b
S2b
Gxb*
ePDG
SWm
Servidor de AAA del BBF
SWu
S9*
Swa
BPCF
BRAS/BNG
Agente de AAA del BBF
AN (DSLAM/ONT)
Red de acceso definida por el BBF
RG
Red de instalaciones del cliente
WiFi AP
Equipo del BBF
UE

FIG. 2

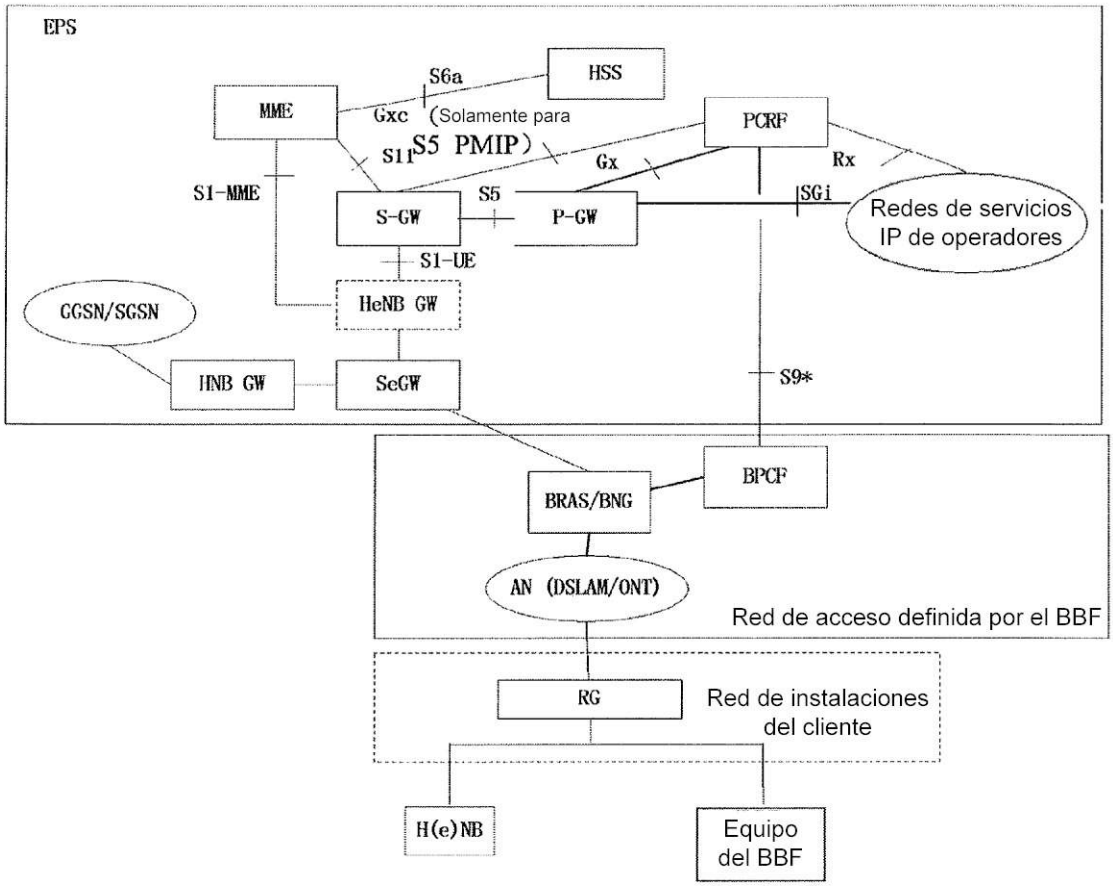
EPS
HSS
S6a
MME
Gxc
(Solamente para
S11
S5 PMIP)
PCRF
Gx
Rx
S1-MME
S5
SGi
S-GW
P-GW
Redes de servicios
IP de operadores
S1-UE
HeNB GW
GGSN/SGSN
HNB GW
SeGW
S9*
BPCF
BRAS/BNG
AN (DSLAM/ONT)
Red de acceso definida por el BBF
RG
Red de instalaciones
del cliente
H(e)NB
Equipo
del BBF

FIG. 3

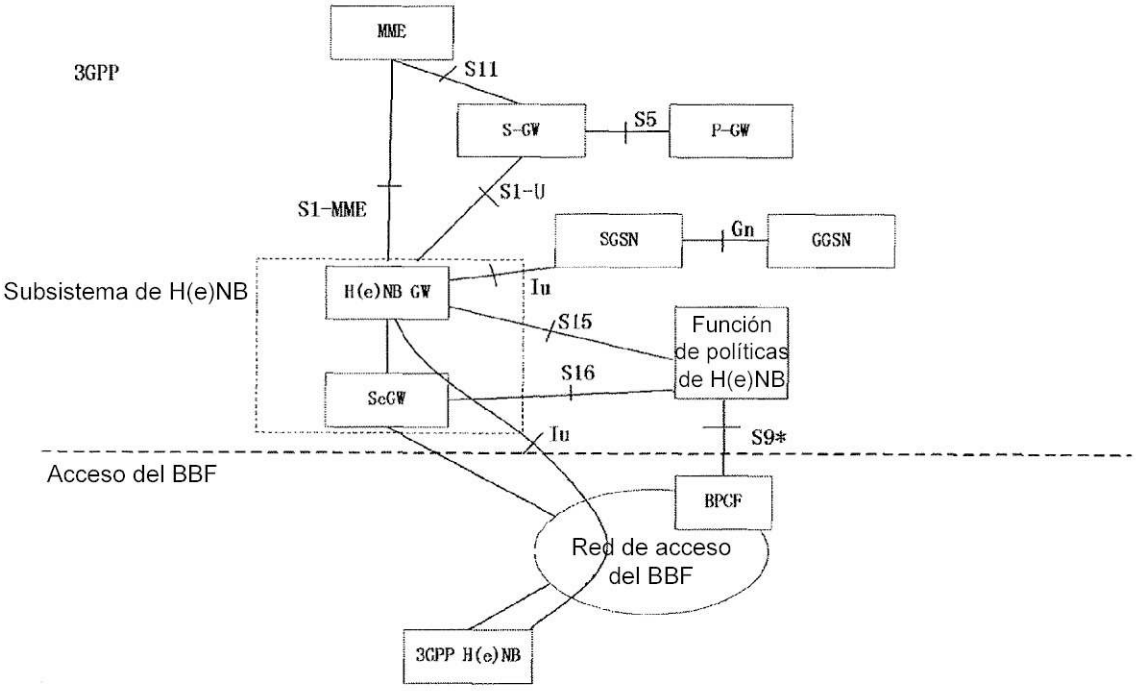
MME
3GPP
S11
S-GW
S5
P-GW
S1-MME
S1-U
SGSN
Gn
GGSN
Subsistema de H(e)NB
H(e)NB GW
Iu
S15
Función de políticas de H(e)NB
S16
ScGW
Iu
S9*
Acceso del BBF
BPCF
Red de acceso del BBF
3GPP H(e)NB

FIG. 4

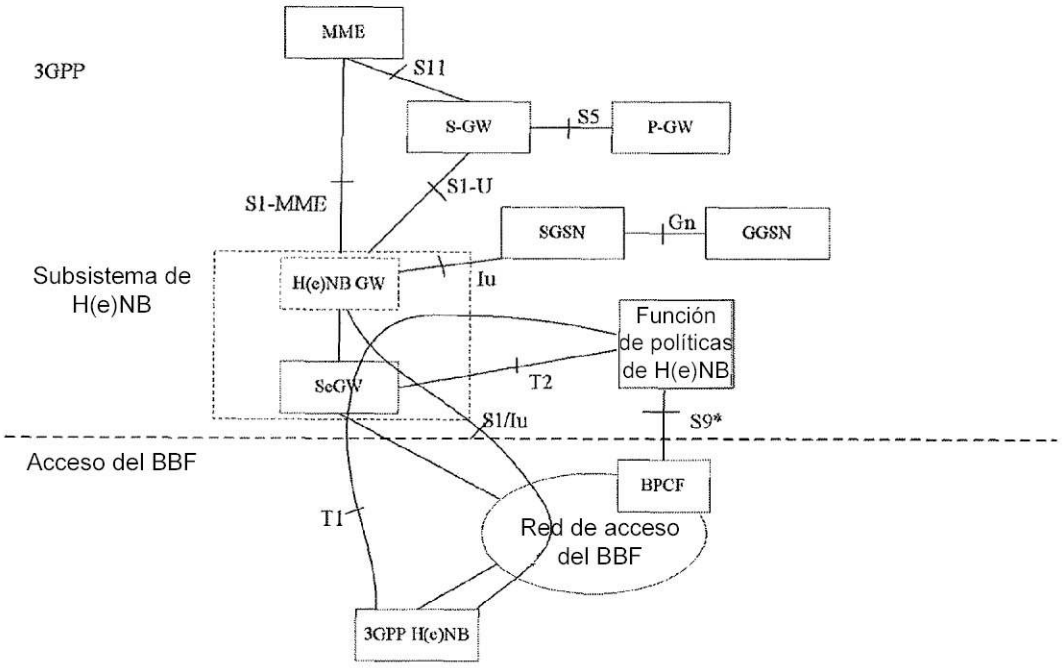
MME
3GPP
S11
S-GW
S5
P-GW
S1-MME
S1-U
SGSN
Gn
GGSN
Subsistema de H(e)NB
H(e)NB GW
Iu
Función de políticas de H(e)NB
ScGW
T2
S1/Iu
S9*
Acceso del BBF
BPCF
T1
Red de acceso del BBF
3GPP H(e)NB

FIG. 5

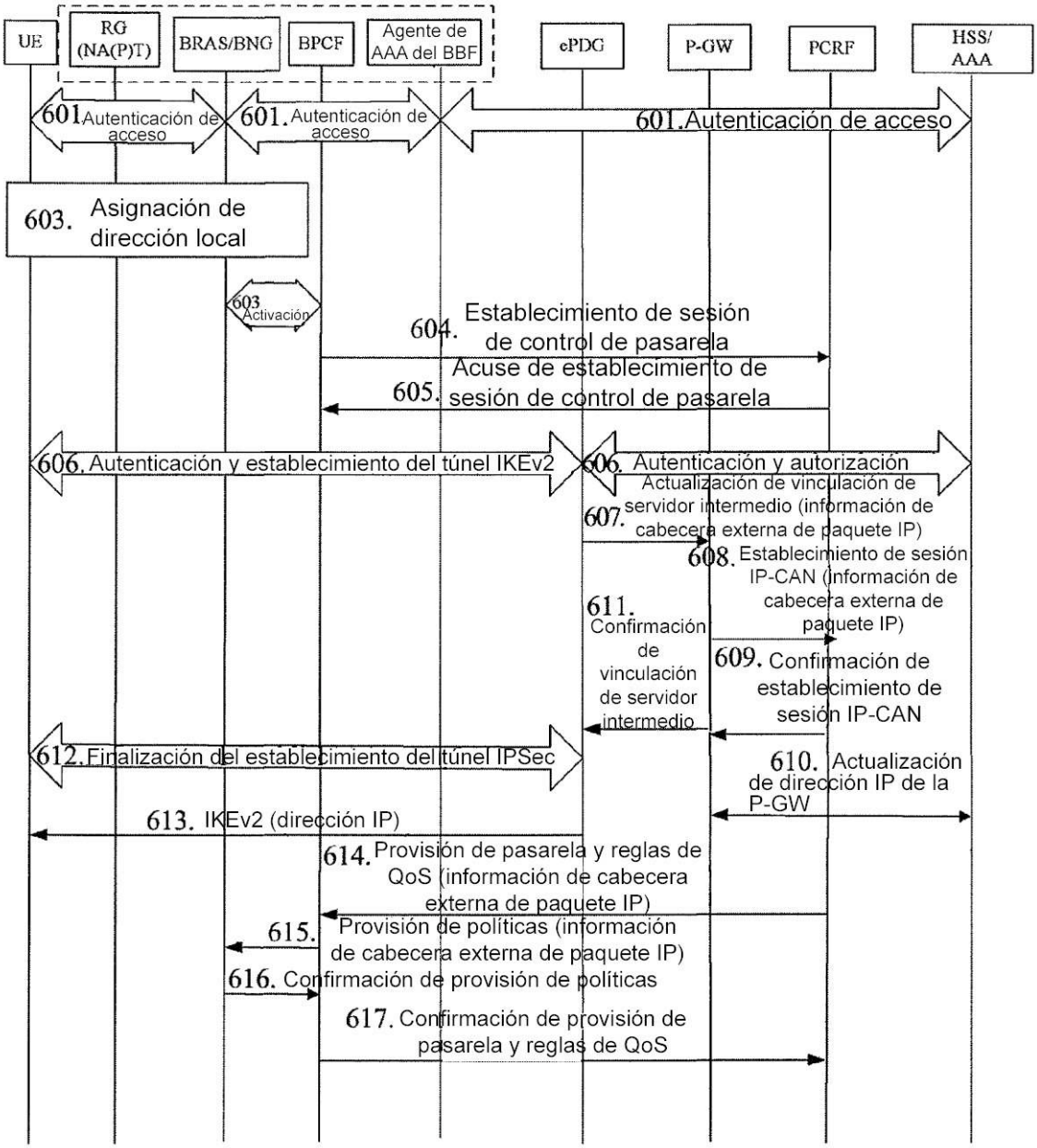
UE
RG (NA(P)T)
BRAS/BNG
BPCF
Agente de AAA del BBF
ePDG
P-GW
PCRF
HSS/ AAA
601 Autenticación de acceso
601. Autenticación de acceso
601. Autenticación de acceso
603. Asignación de dirección local
603 Activación
604. Establecimiento de sesión de control de pasarela
605. Acuse de establecimiento de sesión de control de pasarela
606. Autenticación y establecimiento del túnel IKEv2
606. Autenticación y autorización
607. Actualización de vinculación de servidor intermedio (información de cabecera externa de paquete IP)
608. Establecimiento de sesión IP-CAN (información de cabecera externa de paquete IP)
609. Confirmación de establecimiento de sesión IP-CAN
610. Actualización de dirección IP de la P-GW
611. Confirmación de vinculación de servidor intermedio
612. Finalización del establecimiento del túnel IPSec
613. IKEv2 (dirección IP)
614. Provisión de pasarela y reglas de QoS (información de cabecera externa de paquete IP)
615. Provisión de políticas (información de cabecera externa de paquete IP)
616. Confirmación de provisión de políticas
617. Confirmación de provisión de pasarela y reglas de QoS

FIG. 6

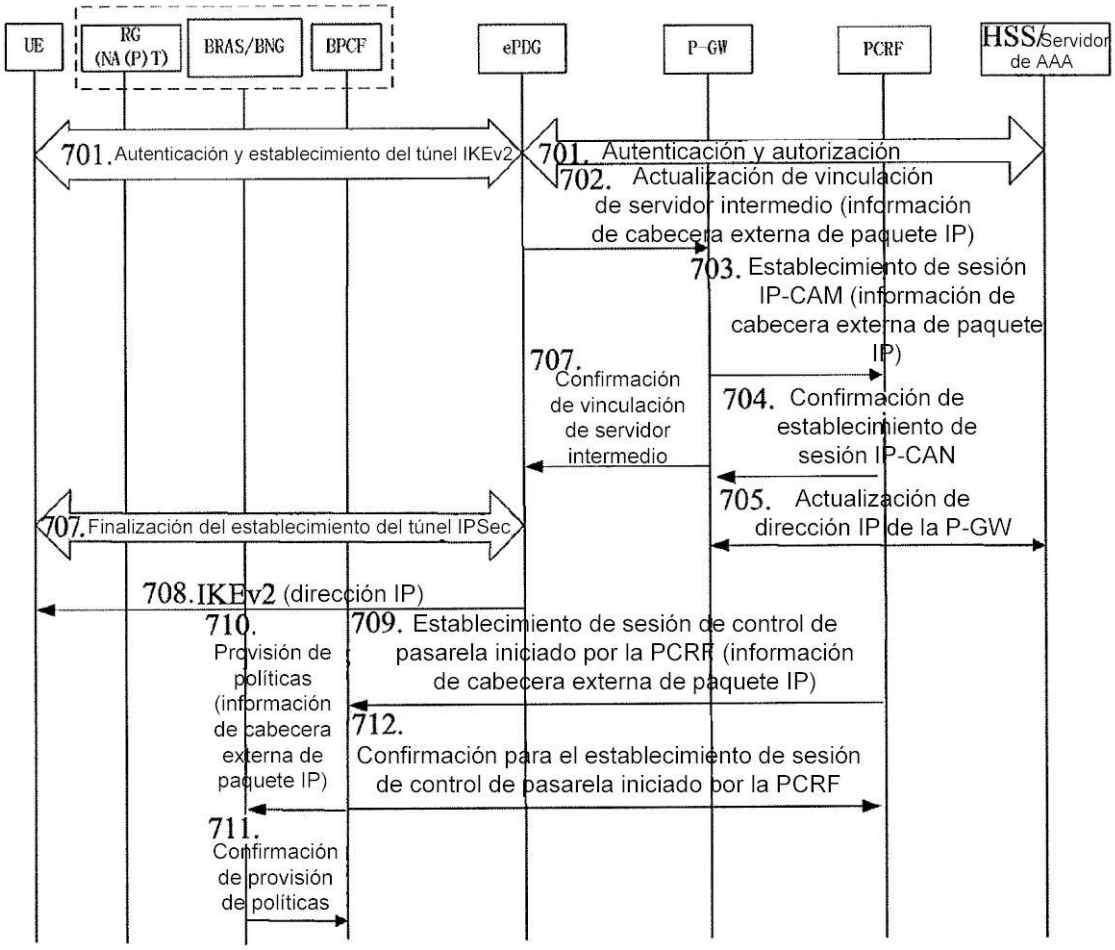
UE
RG (NA (P) T)
BRAS/BNG
BPCF
ePDG
P-GW
PCRF
HSS/Servidor de AAA
701. Autenticación y establecimiento del túnel IKEv2
701. Autenticación y autorización
702. Actualización de vinculación de servidor intermedio (información de cabecera externa de paquete IP)
703. Establecimiento de sesión IP-CAM (información de cabecera externa de paquete IP)
707. Confirmación de vinculación de servidor intermedio
704. Confirmación de establecimiento de sesión IP-CAN
705. Actualización de dirección IP de la P-GW
707. Finalización del establecimiento del túnel IPSec
708. IKEv2 (dirección IP)
710. Provisión de políticas (información de cabecera externa de paquete IP)
709. Establecimiento de sesión de control de pasarela iniciado por la PCRF (información de cabecera externa de paquete IP)
712. Confirmación para el establecimiento de sesión de control de pasarela iniciado por la PCRF
711. Confirmación de provisión de políticas

FIG. 7

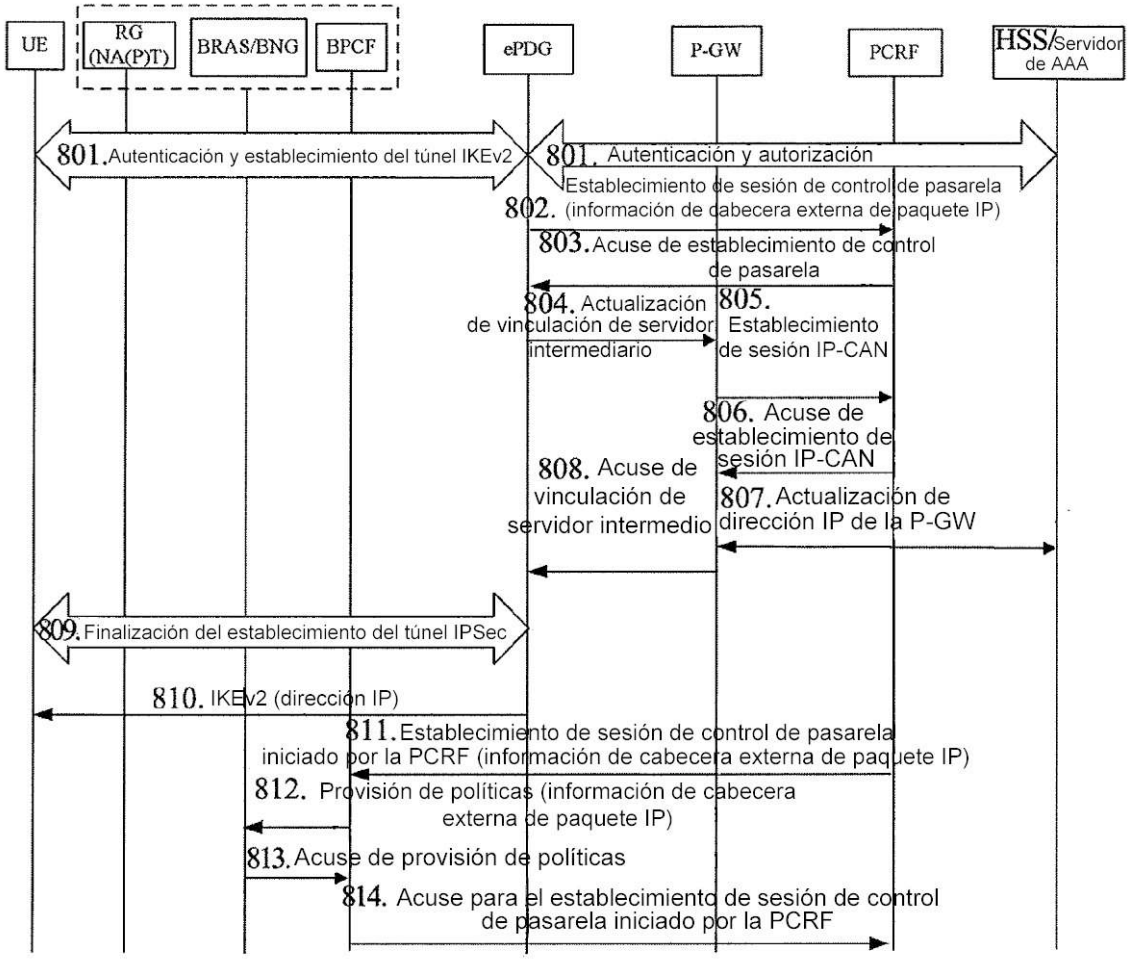
UE
RG (NA(P)T)
BRAS/BNG
BPCF
ePDG
P-GW
PCRF
HSS/Servidor de AAA
801. Autenticación y establecimiento del túnel IKEv2
801. Autenticación y autorización
Establecimiento de sesión de control de pasarela
802. (información de cabecera externa de paquete IP)
803. Acuse de establecimiento de control de pasarela
804. Actualización de vinculación de servidor intermediario
805. Establecimiento de sesión IP-CAN
806. Acuse de establecimiento de sesión IP-CAN
808. Acuse de vinculación de servidor intermedio
807. Actualización de dirección IP de la P-GW
809. Finalización del establecimiento del túnel IPSec
810. IKEv2 (dirección IP)
811. Establecimiento de sesión de control de pasarela iniciado por la PCRF (información de cabecera externa de paquete IP)
812. Provisión de políticas (información de cabecera externa de paquete IP)
813. Acuse de provisión de políticas
814. Acuse para el establecimiento de sesión de control de pasarela iniciado por la PCRF

FIG. 8

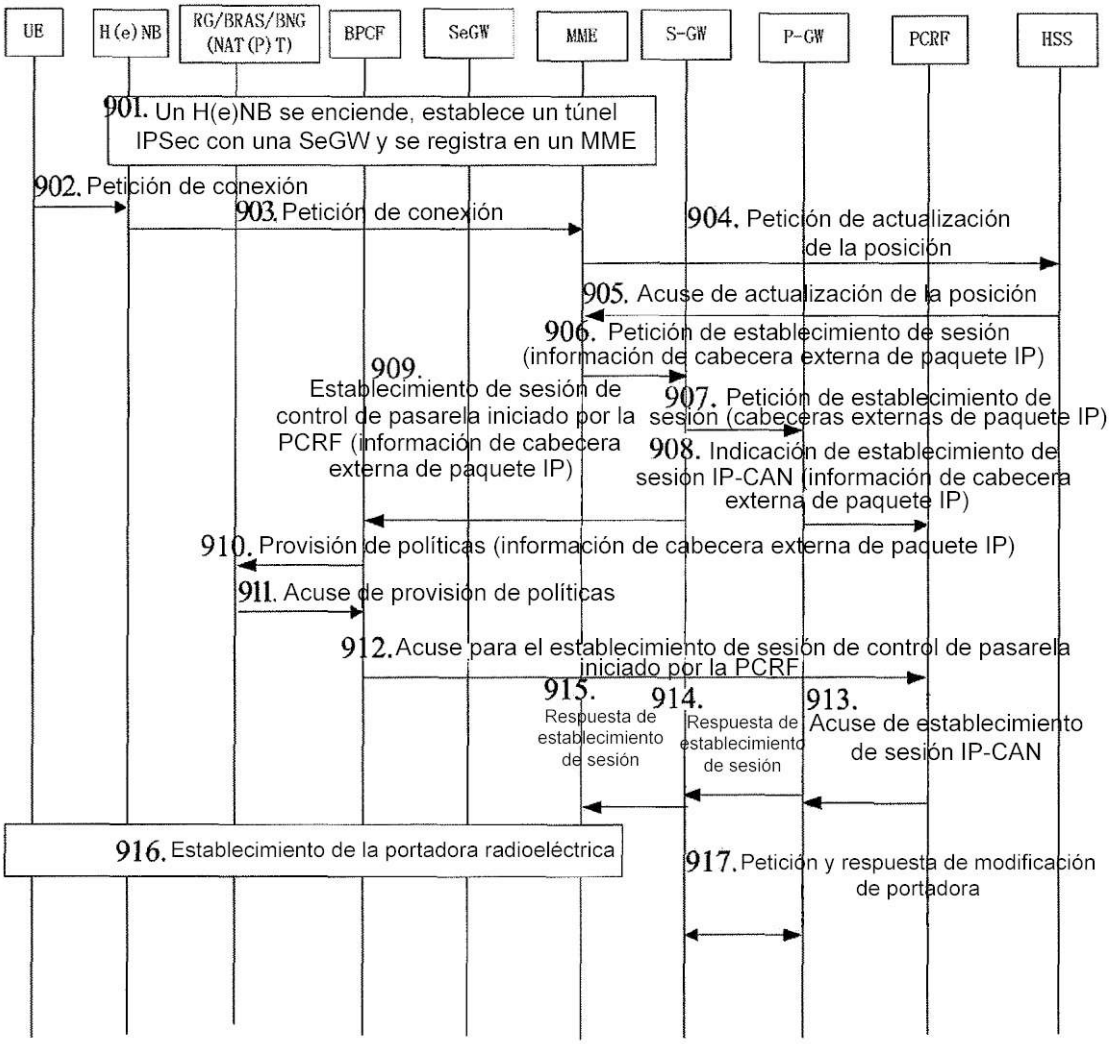
UE
H(e)NB
RG/BRAS/BNG (NAT(P)T)
BPCF
SeGW
MME
S-GW
P-GW
PCRF
HSS
901. Un H(e)NB se enciende, establece un túnel IPSec con una SeGW y se registra en un MME
902. Petición de conexión
903. Petición de conexión
904. Petición de actualización de la posición
905. Acuse de actualización de la posición
906. Petición de establecimiento de sesión (información de cabecera externa de paquete IP)
909. Establecimiento de sesión de control de pasarela iniciado por la PCRF (información de cabecera externa de paquete IP)
907. Petición de establecimiento de sesión (cabeceras externas de paquete IP)
908. Indicación de establecimiento de sesión IP-CAN (información de cabecera externa de paquete IP)
910. Provisión de políticas (información de cabecera externa de paquete IP)
911. Acuse de provisión de políticas
912. Acuse para el establecimiento de sesión de control de pasarela iniciado por la PCRF
915. Respuesta de establecimiento de sesión
914. Respuesta de establecimiento de sesión
913. Acuse de establecimiento de sesión IP-CAN
916. Establecimiento de la portadora radioeléctrica
917. Petición y respuesta de modificación de portadora

FIG. 9

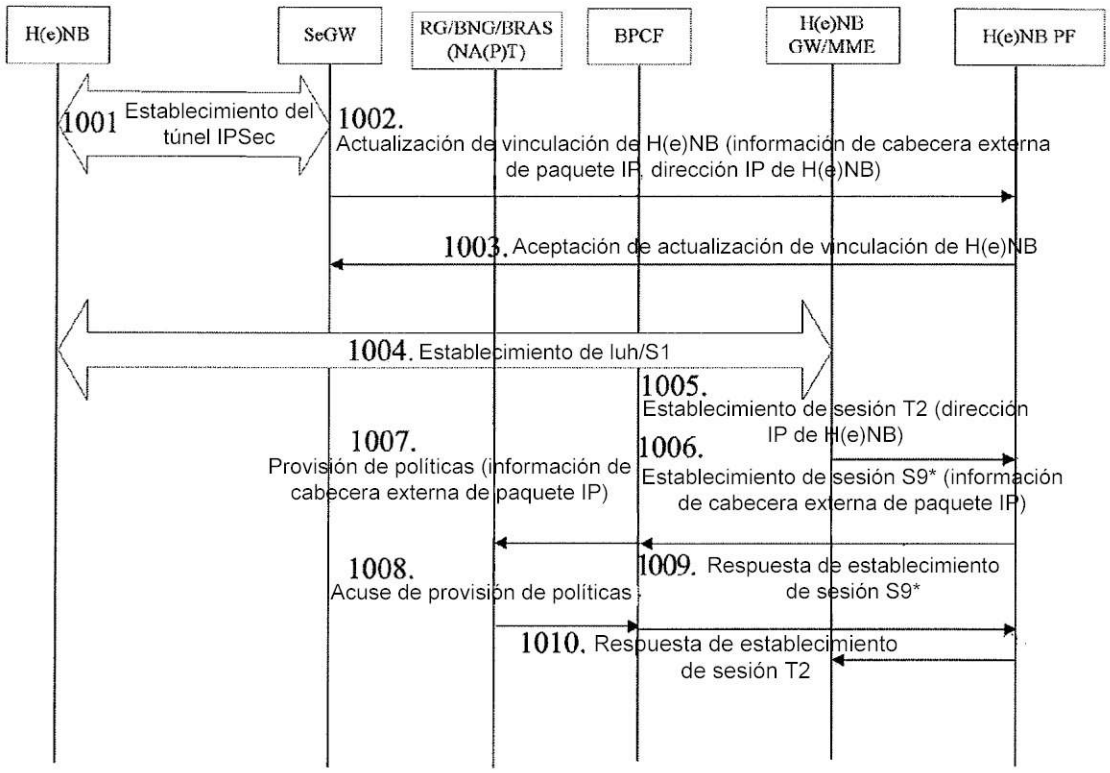
H(e)NB
SeGW
RG/BNG/BRAS (NA(P)T)
BPCF
H(e)NB GW/MME
H(e)NB PF
1001 Establecimiento del túnel IPSec
1002. Actualización de vinculación de H(e)NB (información de cabecera externa de paquete IP, dirección IP de H(e)NB)
1003. Aceptación de actualización de vinculación de H(e)NB
1004. Establecimiento de Iuh/S1
1005. Establecimiento de sesión T2 (dirección IP de H(e)NB)
1006. Establecimiento de sesión S9* (información de cabecera externa de paquete IP)
1007. Provisión de políticas (información de cabecera externa de paquete IP)
1008. Acuse de provisión de políticas
1009. Respuesta de establecimiento de sesión S9*
1010. Respuesta de establecimiento de sesión T2

FIG. 10

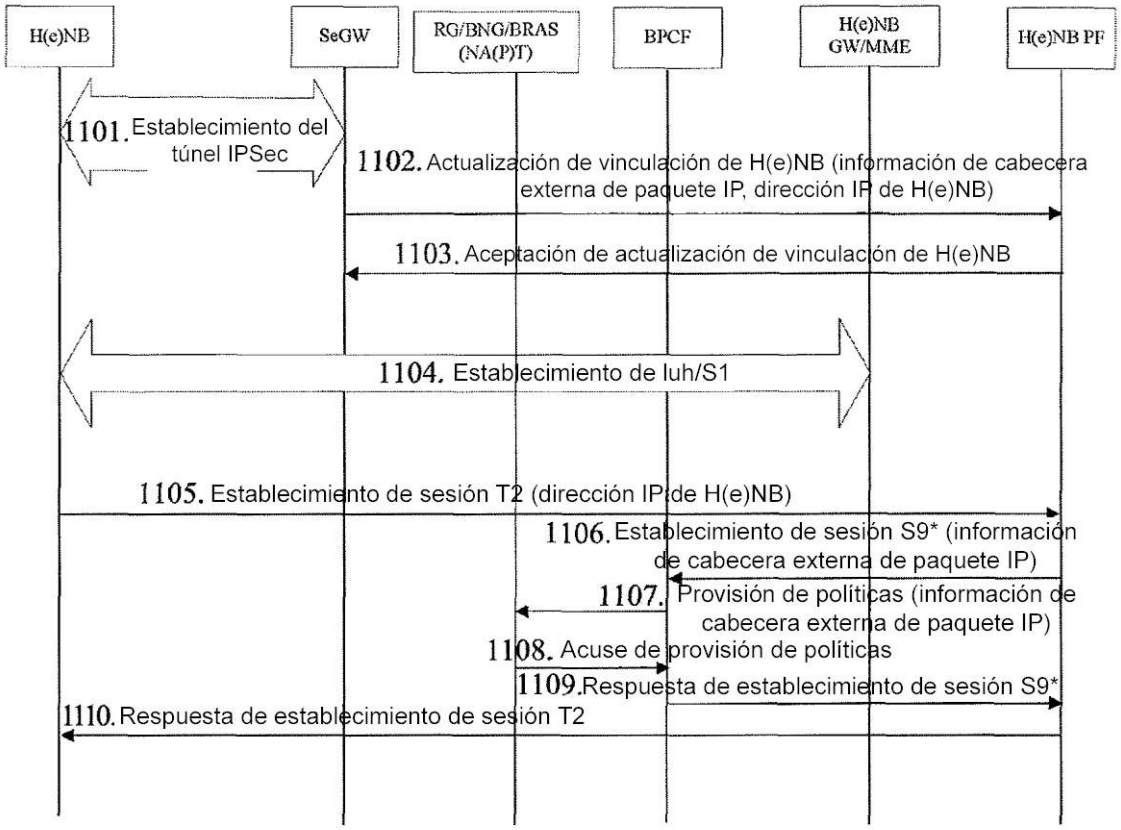
H(e)NB
SeGW
RG/BNG/BRAS (NA(P)T)
BPCF
H(e)NB GW/MME
H(e)NB PF
1101. Establecimiento del túnel IPSec
1102. Actualización de vinculación de H(e)NB (información de cabecera externa de paquete IP, dirección IP de H(e)NB)
1103. Aceptación de actualización de vinculación de H(e)NB
1104. Establecimiento de luh/S1
1105. Establecimiento de sesión T2 (dirección IP de H(e)NB)
1106. Establecimiento de sesión S9* (información de cabecera externa de paquete IP)
1107. Provisión de políticas (información de cabecera externa de paquete IP)
1108. Acuse de provisión de políticas
1109. Respuesta de establecimiento de sesión S9*
1110. Respuesta de establecimiento de sesión T2

FIG. 11