(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 662 173**

(51) Int. CI.:

H04L 29/12 (2006.01)
H04L 29/06 (2006.01)
H04L 12/851 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **19.06.2015 E 15172891 (2)**

(97) Fecha y número de publicación de la concesión europea: **20.12.2017 EP 2981046**

(54) Título: **Identificación de servicios proporcionados en conexiones seguras que usan el almacenamiento en caché de DNS**

(30) Prioridad:

27.07.2014 US 201414341809

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
05.04.2018

(73) Titular/es:

VASONA NETWORKS, INC. (100.0%)
2025 Gateway Place, Suite 285
San Jose, CA 95110, US

(72) Inventor/es:

WEILL, OFER;
BAR-YANAI, RONI y
ASA, ISHAI

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Identificación de servicios proporcionados en conexiones seguras que usan el almacenamiento en caché de DNS

Campo de la invención

La presente invención se refiere generalmente a sistemas de comunicación, y particularmente a métodos y sistemas para identificar servicios proporcionados sobre conexiones protegidas.

Antecedentes de la invención

Las diferentes redes de comunicación permiten a los usuarios de la red consumir ciertos servicios en la red. Tales servicios incluyen, por ejemplo, búsqueda en la web, descarga de archivos, y la entrega de contenidos multimedia.

Algunos servicios de red pueden ser proporcionados en conexiones protegidas. El tráfico de red entregado en conexiones protegidas está típicamente cifrado de modo que solamente las partes que establecen la conexión protegida pueden descifrar el contenido del tráfico.

En la técnica se conocen protocolos para comunicación protegida. Por ejemplo, el Seguro de Protocolo de Transferencia de Hipertexto (HTTPS) es un protocolo de comunicaciones para proteger la comunicación que tiene una capa de seguridad subyacente, es decir el protocolo de Capa Seguridad de Capa de Transporte (TLS). El HTTPS está especificado, por ejemplo, en RFC 2818 del Grupo de Trabajo de Ingeniería de Internet (IETF), titulado “HTTP OVER TLS”, Mayo 2000. La TLS está descrita, por ejemplo, en RFC 5246, titulado “El Protocolo de Seguridad de Capa de Transporte (TLS)”, versión 1.2, Agosto 2008.

La página web “Captura de consultas de DNS con DNSQuery Sniffer – Hacker 10- Security Hacker” (http://www.hacker10.com/other-computing/capture-dns-queries-with-dnsquery-sniffer/; a la que se ha accedido el 19 de Julio de 2016) divulga una aplicación de Windows que captura unas consultas del DNS del ordenador. La aplicación se describe como siendo útil para la solución de problemas de resolución de nombres, para comprobar si un nombre de dominio está siendo puesto en la lista negra por un IP DNS y para un sistema administrador para monitorizar las actividades de los usuarios de la red.

La “Guía de Usuario para ASA CX y Cisco Prime Security Manager 9.1” (http://www.cisco.com/c/en/us/td/docs/security/asacx/9-1/user/guide/b User Guide para ASA CX y PRSM 9 1.pdf; a la que se ha accedido el 19 de Julio de 2016) divulga la Capa de Conectores de Protección (SSL) y la gestión de flujo del tráfico (TLS). El documento describe las reglas de aplicación para el tráfico encriptado desencriptándolo primero para determinar el contenido del tráfico.

Compendio de la invención

Las realizaciones de las invenciones están definidas por las reivindicaciones anejas. La presente invención será más fácilmente entendida a partir de la siguiente descripción detallada de sus realizaciones tomadas conjuntamente con los dibujos en los que:

Breve descripción de los dibujos

La Figura 1 es un diagrama de bloques que ilustra esquemáticamente un sistema de comunicaciones de acuerdo con una realización de la presente invención;

La Figura 2 es un diagrama de bloques que ilustra esquemáticamente un gestor de tráfico de acuerdo con una realización de la presente invención;

La Figura 3 es un diagrama de flujos que ilustra esquemáticamente un método para el almacenamiento en caché del DNS y del o los tipos de servicio respectivos, de acuerdo con una realización de la presente invención; y

La Figura 4 es un diagrama de flujos que ilustra esquemáticamente un método para identificar el o los tipos de servicio de sesión y controlar el tráfico de la sesión basado en el o los tipos de servicios, de acuerdo con una realización de la presente invención.

Descripción detallada de las realizaciones

Visión de conjunto

En diversos sistemas de comunicación los usuarios de la red pueden consumir ciertos servicios sobre la red. Un servidor que proporciona un servicio a los usuarios de la red también se hace referencia aquí como un ordenador principal servidor, o simplemente ordenador principal por brevedad. El usuario típicamente ejecuta un programa o aplicación adecuado (por ejemplo, un explorador web) que gestiona la comunicación con el ordenador principal servidor y permite que el usuario consuma el servicio proporcionado. El flujo de los mensajes de tráfico comunicados entre el usuario y el ordenador principal servidor es referido aquí como una sesión de comunicación.

Los servicios de la red pueden ser varios tipos de servicios tales como navegación por la web, entrega de videos y transferencia de archivos. Algunos de los mensajes de tráfico en una sesión de comunicación pueden incluir información indicativa del tipo de servicio que proporciona la sesión. No obstante, cuando la comunicación es segura, el tráfico de la sesión es típicamente encriptado. Por lo tanto, cualquier información en el contenido del tráfico que pueda estar relacionada con el tipo de servicio proporcionado no está disponible para los elementos de la red distintos de los del usuario y el ordenador principal servidor que fija la sesión.

Las realizaciones de la presente invención que están descritas aquí proporcionan unos métodos y sistemas mejorados para identificar el tipo de servicio que un usuario consume en una conexión protegida. El tipo de servicio identificado puede ser usado, por ejemplo, para el control selectivo dependiente del tipo de servicio del tráfico entregado en sesiones de comunicación individuales. Por ejemplo, cuando la demanda de servicios de la red se aproxima o supera la capacidad de la red, el tráfico puede ser controlado de modo que los servicios que son en tiempo real por naturaleza son entregados con una mayor prioridad que otros servicios. Por ejemplo, a las sesiones de navegación por la web se les puede dar prioridad sobre las sesiones de descarga de archivos.

Cuando se inicia la comunicación con un ordenador principal servidor el usuario típicamente realiza procesos de apretón de manos y de negociación, incluyendo una fase de resolución de Sistema de Nombres de Dominios (DNS), en donde el usuario intercambia información DNS con un servidor DNS. El usuario típicamente envía un mensaje de solicitud de DNS que incluye un nombre de dominio que identifica el ordenador principal servidor a un servidor DNS, el cual responde devolviendo la respectiva dirección IP del ordenador principal servidor. El nombre del dominio (o nombre del ordenador principal) del ordenador principal, puede comprender, por ejemplo, un Identificador Uniforme de Recursos (URI) o un Localizador Uniforme de Recursos (URL).

El usuario usa entonces la dirección IP del ordenador principal para establecer una sesión de comunicación con el ordenador principal servidor. Por ejemplo, en algunas realizaciones, la sesión de comunicación comprende una sesión de comunicación de HTTPS, y el usuario y el ordenador principal servidor intercambian mensajes de establecimiento de la sesión de acuerdo con la especificación del HTTPS antes citada.

En las realizaciones desveladas un gestor de tráfico está instalado en una red de comunicación inalámbrica, por ejemplo entre la Red de Acceso de Radio (RAN) y la Red de Núcleos (CN). El gestor de tráfico intercepta mensajes DNS que son enviados en preparación para establecer sesiones de comunicación protegidas. El gestor de tráfico extrae de los mensajes interceptados una información DNS que es indicativa de los respectivos tipos de servicios de las sesiones para ser establecidas e identifica uno o más tipos de servicios que están relacionados con la información DNS. El gestor de tráfico almacena en caché la información DNS extraída con el o los tipos de servicios identificados en una memoria caché DNS. Los tipos de servicios en caché también son referidos aquí como tipos de servicios basados en IP.

El gestor de tráfico puede almacenar en caché la información DNS (por ejemplo, la dirección IP del ordenador principal servidor) y los respectivos tipos de servicios por usuario (es decir, equipamiento por usuario – UE), más generalmente por área geográfica, o ambos localmente por usuario y globalmente por área geográfica.

En algunas realizaciones el gestor de tráfico identifica el o los tipos de servicios asociados con una sesión de comunicación dada usando varias fuentes de información integradas en el tráfico de la sesión (es decir, además de o en lugar de los tipos de servicios en caché) y aplica una policía de tráfico para controlar el tráfico de la sesión de comunicación dada dependiendo del o de los tipos de servicios identificados (posiblemente en combinación con unos criterios adicionales). A medida que avanza la sesión el gestor de tráfico puede interceptar una información adicional relacionada con el tipo de servicio, lo cual se hace disponible para identificar los tipos de servicios dinámicamente y con más precisión.

El gestor de tráfico puede identificar de diversas maneras el tipo de servicio asociado con una sesión de comunicación dada. En una realización el gestor de tráfico identifica el o los tipos de servicios asignando el URI extraído para un mensaje de respuesta DNS al respectivo o tipos de servicio más predefinidos.

En otra realización el gestor de tráfico intercepta en el tráfico de la sesión de comunicación dada una dirección IP de ordenador principal, y recupera del DNS en caché el o los tipos de servicios basados en IP que están asociados con la dirección IP del ordenador principal. En una realización, aunque no necesariamente, el gestor de tráfico usa esta característica cuando el mensaje de respuesta DNS está perdido, por ejemplo, debido a que el usuario tiene la información DNS almacenada en caché localmente y no genera un mensaje de solicitud de DNS.

Como se puede apreciar, las anteriores técnicas suponen que el gestor de tráfico es capaz de interceptar los mensajes DNS que preceden a la sesión. Además, las direcciones URI e IP asignadas a la sesión no pueden ser siempre indicativas de un único tipo de servicio. En algunas realizaciones el gestor de tráfico aborda estos problemas empleando diversas técnicas complementarias.

Por ejemplo, en algunas realizaciones el gestor de tráfico identifica el tipo de servicio interceptando un mensaje de solicitud de iniciación de sesión que el usuario envía al ordenador principal para establecer una sesión de comunicación protegida, y si el mensaje de solicitud de iniciación de sesión incluye una Indicación de Nombre de la

Sesión (SNI), el gestor de tráfico asigna el SNI a un respectivo tipo de servicio predefinido, también referido aquí como un tipo de servicio basado en SNI.

En otras realizaciones el gestor de tráfico intercepta un mensaje de respuesta de iniciación de sesión que el ordenador principal envía al usuario en respuesta a la recepción del mensaje de solicitud de iniciación de la sesión. El mensaje de respuesta de la iniciación típicamente comprende un certificado que es indicativo de uno o más tipos de servicios. El gestor de tráfico asigna una información relacionada con el tipo de servicio que está integrado en el certificado en uno o más tipos de servicios predefinidos, los cuales son también referidos aquí como tipo o tipos de servicios basados en certificados.

En otras realizaciones más el gestor de tráfico monitoriza ciertas características del flujo de la sesión para determinar los tipos de servicio basados en el flujo. Por ejemplo, el gestor de tráfico monitoriza el volumen de datos entregado en una sesión de comunicación dada desde la iniciación de la sesión y distingue entre un tipo de servicio de descarga y un servicio de navegación basado en el volumen de datos. Otro ejemplo de las características de control del flujo y de los tipos de servicios relacionados se da más adelante.

En algunas realizaciones una unidad de decisión acepta los tipos de servicios que fueron identificados usando las diversas fuentes de información. Las fuentes de información incluyen el o los tipos de servicios basados en SNI, basados en certificados y basados en el flujo como se ha descrito anteriormente. La unidad de decisión combina los tipos de servicios de las diversas fuentes usando cualquier método apropiado y produce uno o más tipos de servicios actualizados. El gestor de tráfico almacena a continuación los tipos de servicios actualizados en un respectivo estado de la sesión.

Cuando se intercepta el tráfico de una sesión cuyo estado incluye uno o más tipo o tipos de servicios, el gestor de tráfico aplica una policía de control de tráfico a la sesión basada en el tipo o tipos de servicios, y posiblemente en otra información dinámica.

El gestor de tráfico puede aplicar cualquier policía de tráfico adecuada basada en o los tipos de servicios identificados. En una realización ejemplo el gestor de tráfico controla la velocidad de entrega de datos del tráfico de la sesión de comunicación dada. Por ejemplo, el gestor de tráfico puede dar una prioridad de entrega mayor a las sesiones que entregan contenidos multimedia que a otras sesiones. Alternativa o adicionalmente, el gestor de tráfico puede aplicar la policía de tráfico basada en información dinámica tal como, por ejemplo, condiciones de congestión que evolucionan en la red de comunicaciones.

En las técnicas reveladas un gestor de tráfico deduce el o los tipos de servicios a partir de la información llevada en mensajes que el usuario y el ordenador principal del servicio intercambian en la preparación para establecer una sesión de comunicación protegida. El gestor de tráfico almacena en caché el tipo de servicio identificado en una memoria caché, y usa la información en caché para identificar el tipo de servicio de las subsiguientes sesiones de comunicación. Adicionalmente, el gestor de tráfico almacena los tipos de servicios identificados en un estado de la sesión y actualiza el o los tipos de servicios basados en otra información que es interceptada en el tráfico de la sesión y asignada a los respectivos tipos de servicios. El gestor de tráfico usa el o los tipos de servicios en el estado de la sesión para controlar sobre la marcha el tráfico de la sesión.

Descripción del sistema

La Figura 1 es un diagrama de bloques que ilustra esquemáticamente un sistema de comunicación 20 de acuerdo con una realización de la presente invención. El sistema 20 puede comprender cualquier red de comunicación apropiada tal como, por ejemplo, una red inalámbrica, una red terrestre, o una combinación de redes inalámbrica y terrestre. Adicionalmente, el sistema 20 puede entregar tráfico a través de la red usando cualesquiera interfaces y protocolos relacionados apropiados, y cualesquiera velocidades de datos apropiadas.

En el ejemplo presente el sistema de comunicación 20 comprende una red de comunicación móvil en la que la Red de Acceso por Radio (RAN) 24, junto con una Red de Núcleo (CN) 28, permite a múltiples terminales móviles 32 acceder a diversos servicios en la red. Los servicios pueden originar en, o entregados a través de una parte terrestre de la red tal como, por ejemplo, una red de área extendida o local (WAN/LAN), o red Internet 36.

En el ejemplo de la Figura 1 el sistema de comunicación 20 comprende un Sistema Universal de Telecomunicaciones Móviles (UMTS) 3GPP. En el UMTS, el RAN 24 es parte de una Red de Acceso (AN), la cual está también referida como Red de Acceso Universal de Radio Terrestre (UTRAN). La UTRAN está descrita, por ejemplo, en la Especificación Técnica TS 25.401 de 3GPP, titulada “Proyecto de Asociación de 3ª Generación; Red de Acceso de Radio de Grupo de Especificación Técnica; descripción general de UTRAN”, (3GPP TS 25.401, versión 12.0.0, Edición 12), Diciembre 2013.

La RAN 24 comprende un Controlador de Red de Radio (RNC) 40, que proporciona unas funcionalidades de control a una o más Estaciones de Base (BSs) 42, también referidas como Nodos Bs. Las funcionalidades del RNC 40 y del Nodo B 42 pueden ser puestas en práctica en el mismo dispositivo, o pueden ser puestas en práctica en dispositivos físicamente independientes.

Alternativamente, el sistema de comunicaciones 20 puede comprender una red de Evolución a Largo Plazo (LTE) en la que la RAN 24 comprende una Red de Acceso de Radio Terrestre Universal Evolucionada (E-UTRAN) en la que las BSs 42 comprenden un dispositivo eNodeB que típicamente incluye las funcionalidades de control del RNC 40. E-UTRA es descrita, por ejemplo, en la Especificación Técnica TS 36.300 de 3GPP titulada "Red de Acceso de Radio de Grupo; Acceso Universal de Radio Terrestre Evolucionada (E-UTRA) y Red de Acceso Universal de Radio Terrestre Evolucionada (E-UTRAN); Descripción general", (3GPP TS 36.300, versión 11.7.0, Edición 11), Septiembre, 2013.

El terminal móvil 32, que está también referido en las redes UMTS y LTE como un Equipo de Usuario (UE), puede comprender cualquier dispositivo inalámbrico tal como, por ejemplo, un teléfono manual, un ordenador portátil equipado con un adaptador móvil de banda ancha, un dispositivo de cálculo móvil habilitado para conexión inalámbrica, o cualquier otro tipo de terminal de comunicación inalámbrica apropiado.

Los servicios de datos de red son a veces proporcionados usando un protocolo de Paquete general de servicios de radio (GPRS). El GPRS es una tecnología de comunicaciones móviles de 2,5 G y 3 G que permite a los operadores de la red móvil ofrecer a sus suscriptores móviles unos servicios de datos basados en paquetes tales como el acceso a Internet en redes GSM (y otras). Una red de núcleo GPRS proporciona, entre otras tareas, una gestión de movilidad, gestión de la sesión y transporte para servicios de paquetes de Protocolo Internet (IP) en varias redes tales como, por ejemplo, las redes GSM y WCDMA. En el ejemplo del sistema de comunicación 20, CN 28 comprende una red de núcleo que comprende un Nodo de Soporte de Servicio de GPRS (SGSN) 44, y un Nodo de Soporte de Pasillo de Conexión de GPRS (GGSN) 46.

El SGSN 44 es típicamente responsable de la entrega de paquetes de datos desde y a las BSs 42 dentro del área de servicio geográfico del SGSN. Entre otras tareas, el SGSN 44 realiza el encaminamiento y transferencia del paquete, la gestión de la movilidad, así como funciones de autentificación y carga. El SGSN 44 almacena información del lugar (por ejemplo, información actual de la célula servidora e información de indicación de la posición del móvil) de los usuarios del GPSS que están registrados con el SGSN.

El GGSN 46 es responsable de la interconexión entre el CN 28 y las redes externas de conmutación de paquetes tal como la red Internet 36. Cuando se reciben paquetes de datos destinados a un UE 32 dado, el GGSN 46 reenvía los datos al SGSN que está sirviendo al UE dado. En la dirección opuesta el GGSN 46 encamina los paquetes originados en móviles a un respectivo destino en la red. El GGSN 46 convierte los paquetes GPRS que vienen del SGSN 44 en el formato de protocolo de paquetes de datos (PDP) (por ejemplo, IP o X.25) y envía los paquetes de datos en la correspondiente red de paquetes de datos.

El sistema de comunicación 20 comprende además un Sistema de Nombres de Dominio (DNS) 48, el cual traslada los nombres de dominio en las direcciones IP respectivas. Cuando se inicia una sesión de comunicación con un ordenador principal el UE 32 típicamente primero envía el nombre del dominio del ordenador principal al DNS 48, el cual responde enviando la correspondiente dirección IP del ordenador principal al UE. El UE a continuación usa la dirección IP para fijar una sesión de comunicación protegida con el ordenador principal.

Un gestor de tráfico 50 se interconecta entre RNC 40 y SGSN 44. El gestor de tráfico intercepta mensajes DNS (y otros) intercambiados a través de la red. Como se describirá con detalle más adelante, el gestor de tráfico usa técnicas de almacenamiento en caché de DNS para identificar el tipo de servicio entregado dentro de cada sesión de comunicación, y aplica una respectiva policía de tráfico a la sesión de comunicación dependiendo del servicio identificado. En algunas realizaciones la policía de tráfico puede depender del tipo de servicio identificado en combinación con unos criterios adicionales.

El sistema 20 de configuración de la red en la Figura 1 es una configuración ejemplo, que es escogida puramente por el bien de la claridad conceptual. En realizaciones alternativas cualquier otra configuración apropiada puede también ser usada. Por ejemplo, la configuración de la red en la Figura 1 comprende unidades de RNC y SGSN únicas. No obstante, en redes UMTS prácticas las funcionalidades de las unidades RNC y GGSN pueden estar distribuidas sobre muchas de tales unidades. De este modo, el GGSN puede comunicar con muchos SGSNs, y cada SGSN puede comunicar con muchos RNCs.

Aunque la descripción que sigue se refiere principalmente a redes UMTS, tales como la red representada en la Figura 1 anterior, las técnicas reveladas son también aplicables a otras redes de comunicación apropiadas con las adaptaciones necesarias. Por ejemplo, cuando el sistema de comunicaciones 20 comprende una red 3GPP LTE la funcionalidad del GGSN 46 puede desplazarse a un pasillo de conexión de Evolución de la Arquitectura del Sistema (SAE), y la funcionalidad del SGSN 44 puede ser puesta en práctica en una Entidad de Gestión de Movilidad (MME), ambas SAE y MME no están mostradas en la Figura 1. Como otro ejemplo, el sistema 20 puede comprender una red de comunicaciones totalmente terrestre, y el terminal 32 puede comprender un Ordenador Personal (PC) o un ordenador portátil.

Tipo de servicio de identificación que usa almacenamiento en caché de dns

El UE 32 puede ejecutar uno o más programas o aplicaciones para consumir diversos servicios en la red, estando cada servicio asociado con un respectivo tipo de servicio (o muchos tipos). Por ejemplo, los servicios de la red

incluyen navegación por la web, descarga de archivos (por ejemplo, fecha de solicitud), juegos en la red, correo electrónico (e-mail), fax por internet, y consumo de contenidos multimedia tales como contenidos de imágenes, vídeo o audio.

La descripción que sigue se refiere principalmente a servicios que son proporcionados al UE 32 en una conexión protegida. Cuando la comunicación entre el UE y el ordenador principal que proporciona el servicio está protegida, cualquier información en el tráfico de la sesión que puede ser indicativa del tipo de servicio típicamente permanece no disponible a elementos de trabajo otros que el UE y el ordenador principal de servicio. Como se describirá en adelante con detalle, el gestor de tráfico 50 intercepta y analiza ciertos mensajes de tráfico que el UE y ordenador principal de servicio intercambian durante el establecimiento de la conexión, y otros mensajes de la sesión para deducir el tipo de servicio de un servicio que es proporcionado en la conexión protegida.

La Figura 2 es un diagrama de bloques que ilustra esquemáticamente un gestor de tráfico 50 de acuerdo con una realización de la presente invención. El gestor de tráfico 50 puede ser usado, por ejemplo, en el sistema de comunicación 20 descrito en la Figura 1 anterior, o en cualquier otra red de comunicación apropiada. El gestor de tráfico 50 comprende un procesador 52 que ejecuta las diversas tareas del gestor de tráfico, y una memoria caché 54 de DNS que almacena en caché información de DNS y los respectivos tipos de servicios identificados como se describe más adelante.

La memoria caché 54 puede comprender cualquier tipo apropiado de memoria volátil o no volátil tal como, por ejemplo, una Memoria de Acceso Aleatorio (RAM) o Memoria Flash. Alternativamente, la memoria caché 54 puede comprender un dispositivo de almacenamiento magnético tal como una Unidad de Disco Duro (HDD) o cualquier otro medio de almacenamiento apropiado.

El procesador 52 comprende un analizador de DNS 60 que intercepta los mensajes intercambiados entre los UEs 32 y el DNS 48. Típicamente, un mensaje DNS que se origina por el UE 32 incluye el URI que identifica el ordenador principal de servicio, y el mensaje de respuesta de DNS originado por el DNS 48 incluye el URI y la respectiva dirección IP del ordenador principal.

En algunas realizaciones el analizador 60 de DNS intercepta solamente el mensaje de respuesta del DNS y extrae el URI y la respectiva dirección IP del mensaje de respuesta del DNS. Un URI del asignador 62 de tipo o tipos de servicios (o simplemente asignador 62 por brevedad) asigna el URI a uno o más tipos de servicios predefinidos, y almacena en caché la dirección IP del ordenador principal y los respectivos tipos de servicios en caché DNS 54 (si todavía no están almacenados en caché). El o los tipos de servicios en caché están también referidos aquí como tipos de servicios basados en IP.

En algunas realizaciones el caché DNS 54 comprende un área de caché local y un área de caché global. En el área de caché local el caché DNS 54 almacena direcciones IP y los respectivos tipos de servicios basados en IP por separado por UE. En el área de caché global el caché DNS 54 almacena direcciones IP y los respectivos tipos de servicios basados en IP globalmente por área geográfica (por ejemplo, para todos los UEs servidos por un BS dado).

Al consultar el caché DNS 54 con una dirección IP dada, el caché 54 genera los respectivos tipos de servicios y entrega los tipos de servicios a una unidad de decisión 66 de tipo o tipos de servicios (también referida aquí como unidad de decisión 66 por brevedad), que recibe los tipos de servicios de varias fuentes y genera un tipo (o tipos) de servicios actualizados como se describirá más adelante. La consulta de una cierta dirección IP en caché DNS 54 es típicamente hecha en el área local para una UE dada, y si la dirección IP no está almacenada en caché localmente para el UE dado, el caché DNS busca la dirección IP en el área de caché global. Almacenando en caché la dirección IP del ordenador principal y el o los respectivos tipos de servicios es posible para el procesador recuperar el o los tipos de servicios basados en IP dada solamente la dirección IP del ordenador principal.

Cuando el asignador 62 acepta un URI del analizador 60 de DNS, el asignador 62 asigna el URI a uno o más tipos de servicios predefinidos. Típicamente, el asignador 62 intenta convertir el URI en un único tipo de servicio, si es posible. El asignador 62 puede usar cualquier método apropiado para convertir los URIs en un tipo o tipos de servicios. Por ejemplo, el asignador 62 puede identificar ciertas cadenas de textos dentro del URI y asignar estas cadenas a tipos de servicios basados en un esquema de asignación predefinido.

Cuando la información integrada en el URI con respecto al tipo de servicio es ambigua, el asignador 62 puede asignar el URI en un conjunto de dos o más tipos de servicios, o a un único tipo de servicio que captura muchos servicios. Por ejemplo, el asignador 62 puede asignar un único servicio que captura muchos servicios. Por ejemplo, el asignador 62 puede asignar un URI dado a uno de los tipos de servicios: entrega de vídeo, entrega de multimedia, una lista de tipos de servicios que incluye la entrega de vídeo y audio, o algún tipo general de servicio de entrega en tiempo real.

En algunas realizaciones, al establecer una sesión protegida, el UE 32 y el ordenador principal servidor realizan un proceso de apretón de manos en el que el UE 32 solicita un certificado del ordenador principal. El AS será descrito más adelante. El procesador 52 comprende un SNI / certificado analizador 68 que intercepta y analiza mensajes de establecimiento de la sesión con el fin de identificación del tipo de servicio.

En algunas realizaciones un único ordenador principal servidor puede hospedar muchos nombres del ordenador principal de DNS en la misma dirección IP, correspondiendo cada uno a un servicio diferente. En tales realizaciones el UE puede enviar al ordenador principal servidor una solicitud que incluye una Indicación de Nombre del Servidor (SNI), que identifica un nombre del ordenador principal seleccionado entre los múltiples nombres del ordenador principal en el ordenador principal servidor. Un SNI dado corresponde típicamente a un único tipo de servicio. El SNI está definido, por ejemplo, en las especificaciones IETF RFC 3546, tituladas “Ampliaciones de Seguridad de la Capa de Transporte (TLS)”, publicadas en Junio de 2003.

Cuando se recibe una solicitud de UE que incluye una SNI, el ordenador principal servidor responde presentando al UE un certificado que incluye el nombre del ordenador principal que está asociado con el SNI. En contraste con los SNIs, un certificado puede corresponder a un único tipo de servicio o a muchos tipos de servicios, por ejemplo cuando el ordenador principal servidor incluye un único nombre del ordenador principal o muchos nombres del ordenador principal, respectivamente.

Como se ha descrito antes, el procesador 52 comprende un de SNI / analizador de certificado 68 que intercepta mensajes relacionados con la fase de establecimiento de sesiones protegidas. Cuando el SNI / analizador de certificado 68 intercepta un mensaje de solicitud de UE que incluye un SNI, el analizador 68 asigna el SNI a un respectivo servicio predefinido y envía este tipo de servicio basado en SNI a la unidad de decisión 66.

Cuando el analizador 68 intercepta además la respuesta del ordenador principal servidor, incluyendo el respectivo certificado, el analizador 68 asigna la información relacionada del tipo de servicio integrada en el certificado en los respectivos uno o más tipos de servicios predefinidos y envía estos tipos de servicios basados en certificados a la unidad de decisión 66.

El procesador 52 comprende un estado 72 de la sesión, que gestiona información del estado de las sesiones activas que son interceptadas por el gestor de tráfico 50. El procesador 52 puede identificar sesiones individuales en el estado 72 de la sesión usando cualquier método apropiado tal como, por ejemplo, asignando a cada sesión un respectivo identificador de la sesión. El estado 72 de la sesión almacena los tipos de servicios generados a partir de la unidad de decisión 66 en asociación con la respectiva sesión de comunicación.

En algunos casos los mensajes de respuesta de DNS del DNS 48 no están disponibles. Por ejemplo, el UE puede almacenar en caché la dirección IP del ordenador principal internamente y por lo tanto no solicita la dirección IP al DNS 48. Como otro ejemplo, la fase del DNS puede haber ocurrido cuando el UE fue servido por otro BS y por lo tanto el analizador de DNS podría no interceptar los mensajes de DNS. El procesador 52 comprende un IP / analizador de sesión 76 que intercepta las direcciones IP del ordenador principal relacionadas con las sesiones activas almacenadas en el estado 72 de la sesión. El procesador usa la dirección IP interceptada para consultar el área global del DNS caché 54 para recuperar los respectivos tipos de servicios basados en IP.

Cuando un mensaje interceptado pertenece a una sección activa para la que el tipo de servicio es todavía desconocido, el IP / analizador de sesión 76 extrae la dirección IP del ordenador principal del mensaje interceptado, y consulta la dirección IP en el DNS caché 54. Si la dirección IP es encontrada en el caché de área local o en el caché de área global, el DNS caché 54 entrega el o los tipos de servicios basados en IP respectivos a la unidad de decisión 66 que genera uno o más tipos de servicios actualizados como se ha descrito antes. El procesador 52 almacena a continuación el o los tipos de servicios actualizados en el estado 72 de la sesión.

Cuando los servicios basados en IP no están disponibles en el DNS caché, el procesador puede usar un tipo de servicio por defecto, o intentar derivar uno o más tipos de servicios, por ejemplo, a partir de la información integrada en los mensajes de establecimiento de la sesión, o a partir de las características del flujo, como se describirá con detalle más adelante.

En algunas realizaciones el IP / analizador de sesión 76 infiere información con respecto al tipo de servicio de una sesión dada monitorizando ciertas características de flujo de la sesión. Por ejemplo, en una realización el IP / analizador de sesión 76 monitoriza el volumen de datos entregado desde la iniciación de la sesión y distingue entre una descarga o servicio de navegación basado en el volumen de datos. Por ejemplo, cuando el volumen de datos excede un volumen predefinido (por ejemplo, en bytes), el procesador puede inferir que el tipo de servicio se refiere a un servicio de descarga y no a una navegación por la web. Otras características de flujo que pueden indicar el tipo de servicio incluyen el tamaño del paquete, el paso del paquete, y la fluctuación de los intervalos entre paquetes. Por ejemplo, una corriente de voz típicamente comprende paquetes cortos a alguna velocidad constante, en tanto que una corriente de vídeo típicamente comprende unos paquetes mayores a una velocidad constante.

El procesador 52 comprende además una policía de tráfico 80 y un controlador de tráfico 84. La policía de tráfico 80 mantiene unas reglas de control de tráfico múltiples que el controlador de tráfico 84 puede aplicar a sesiones de comunicación individuales. Las acciones que el controlador de tráfico 84 puede emprender incluyen, por ejemplo, la regulación del tráfico, posponiendo la entrega del tráfico a un momento posterior, y el bloqueo del tráfico. Alternativa o adicionalmente, el controlador de tráfico 84 puede ser usado para monitorizar el tráfico así como para informar del tráfico. El controlador de tráfico 84 puede aplicar la policía de tráfico separadamente por UE o por área geográfica tal como por BSs 42.

La policía de tráfico 80 selecciona unas reglas de control de tráfico predefinidas para aplicar a una sesión dada basada en los respectivos tipos de servicio que están almacenados en el respectivo estado en el estado 72 de la sesión. Por ejemplo, una regla de tráfico para sesiones que entregan contenidos de vídeo (u otros servicios que son de tiempo real por naturaleza) puede asignar a tales sesiones una prioridad más alta sobre las sesiones que proporcionan otros servicios. Como otro ejemplo, una regla de tráfico para una sesión que proporciona una actualización de la aplicación del servicio de descarga puede decir que el tráfico para esta sesión debería ser reducido o pospuesto a un momento posterior.

La policía de tráfico 80 puede adicionalmente seleccionar qué regla de tráfico aplicar basada en la información de red dinámica proporcionada por un analizador a largo plazo 88 del procesador 52. Por ejemplo, el analizador a largo plazo 88 puede monitorizar la carga de tráfico en BSs 42 para detectar una congestión y aplicar una regla de tráfico seleccionada solamente a sesiones que son entregadas por medio de BSs que llegan a estar congestionadas.

En algunas realizaciones en las cuales el almacenamiento en caché es hecho separadamente por UE, por área geográfica o ambos, la policía de tráfico 80 puede controlar solamente el tráfico de los UEs o de las áreas geográficas seleccionados respectivamente.

La configuración del gestor de tráfico 50 en la Figura 2 es una configuración ejemplo que es elegido puramente por consideración de claridad conceptual. En realizaciones alternativas también puede ser usada otra configuración apropiada. Los diferentes elementos del procesador 52 pueden ser puestos en práctica usando cualquier soporte físico apropiado, tal como en un Circuito Integrado de Aplicación Específica (ASIC) o Disposición de Puertas de Campo Programable (FPGA). En algunas realizaciones algunos elementos del procesador 52 pueden ser puestas en práctica usando un soporte lógico o usando una combinación de elementos de soporte físico y de soporte lógico.

En algunas realizaciones el procesador 52 comprende un procesador de propósito general que está programado en soporte físico para realizar las funciones aquí descritas. El soporte físico puede ser descargado al procesador en forma electrónica sobre una red, por ejemplo, o puede alternativa o adicionalmente ser proporcionado y/o almacenado en medios tangibles no transitorios tales como una memoria magnética, óptica, o electrónica.

La Figura 3 es un diagrama de flujos que ilustra esquemáticamente un método para almacenar en caché información de DNS y el o los tipos de servicio respectivos de acuerdo con una realización de la presente invención. El método comienza en un paso de interceptación 100 de DNS en el que el analizador de DNS 60 intercepta un mensaje de respuesta de DNS que el DNS 48 envía a un UE dado en respuesta a la recepción de un mensaje de solicitud de DNS. El mensaje de respuesta de DNS incluye el URI (o URL) solicitado y la dirección IP resuelta de DNS del ordenador principal.

En un paso de asignación 104 el URI del asignador 62 del o de los tipos de servicios asigna el URI interceptado en el paso 100 a uno o más tipo o tipos de servicios predefinidos como se ha descrito anteriormente. En un paso 108 de almacenamiento en caché el caché DNS 54 almacena la dirección IP desde el paso 100 en asociación con la generación del o los tipos de servicios en el paso 104. El DNS caché 54 almacena la dirección IP y el o los respectivos tipos de servicios para el UE dado en el área de caché local, así como en el área de caché global. El método a continuación vuelve atrás al paso 100 para interceptar los subsiguientes mensajes de respuesta de DNS destinados al UE dado o a otros UEs.

La Figura 4 es un diagrama de flujos que ilustra esquemáticamente un método para identificar el o los tipos de servicios de la sesión y controlar el tráfico de la sesión basado en el o los tipos de servicios de acuerdo con una realización de la presente invención. El método es típicamente ejecutado para sesiones activas cuyos tipo o tipos de servicios son almacenados en su estado en el estado 72 de la sesión.

El método comienza en un paso 200 de intercepción de la sesión, en el cual un analizador 76 IP/sesión y SNI / analizador de certificados 68 intercepta un mensaje que pertenece a una sesión activa dada. Dependiendo del mensaje interceptado en el paso 200, el procesador ejecuta uno de los pasos 204, 208, 212 o 216, los cuales son descritos más adelante, para obtener uno o más tipos de servicios relacionados con la sesión dada.

En un paso de consulta 204 el analizador IP/sesión 76 usa una dirección IP del ordenador principal interceptada en el paso 200 para consultar el caché 54 como se ha descrito antes. En respuesta a la operación de consulta el caché de DNS recupera los respectivos tipos de servicios basados en IP a partir del DNS caché como se ha descrito anteriormente, y entrega los tipos de servicios basados en IP a la unidad de decisión 66.

En un paso de asignación 208 de SNI / analizador de certificados 68 asigna un SNI en una solicitud de UE interceptada para el establecimiento de la sesión a un tipo de servicio basado en SNI y entrega el tipo de servicio basado en SNI a la unidad de decisión 66.

En un paso 212 de asignación de certificado el SNI / analizador de certificados 68 asigna un certificado que fue interceptado en el paso 200 en un mensaje de respuesta del ordenador principal, en uno o más tipos de servicios predefinidos basados en certificados para ser entregados a la unidad de decisión 66.

En un paso 216 de estimación de las características del flujo, el IP / analizador de sesión 76 estima las características del flujo de los mensajes de la sesión y asigna las características del flujo a uno o más tipos de servicios predefinidos basados en el flujo. Varios ejemplos de las características del flujo y de los tipos de servicios relacionados fueron dados anteriormente.

En un paso 220 de decisión la unidad 66 de decisión acepta el o los tipos de servicios derivados en uno de los pasos 204, 208, 212 y 216 anteriores, es decir tipos de servicios basados en IP, basados en SNI, basados en el certificado y basados en el flujo, y produce uno o más tipos de servicios actualizados. En un paso 224 de actualización de estado el procesador 52 almacena el o los tipos de servicios derivados en el paso 220 en el estado 72 de la sesión.

En un paso 228 de determinación de policía, la policía de tráfico 80 selecciona una o más reglas de tráfico basadas en el o los tipos de servicios actualizados en el estado 72 de la sesión y en la información dinámica de la red proporcionada por el analizador 88 a largo plazo, tal como, por ejemplo, las condiciones de congestión en la red.

En otra realización la regla de tráfico puede relacionarse con la calidad de servicio que experimenta el usuario. Por ejemplo, comparando la entrega de vídeo con la actualización de la solicitud, el usuario típicamente experimenta una mayor degradación en la calidad del servicio cuando la red falla al entregar el contenido del vídeo en tiempo real que cuando la red retrasa el proceso de descarga durante la actualización de la solicitud. Por lo tanto, una regla de tráfico puede asignar una mayor prioridad a la entrega del vídeo que a la actualización de la solicitud.

En un paso 232 de solicitud de policía el controlador de tráfico 84 aplica las reglas de tráfico seleccionadas en el paso 228 al tráfico de la sesión dada. Típicamente el controlador de tráfico 84 aplica la policía de tráfico sobre una base de paquete por paquete. El método a continuación vuelve atrás al paso 200 para interceptar los subsiguientes mensajes de tráfico de la sesión.

Los métodos antes descritos son unos métodos ejemplares, y otros métodos pueden ser usados en realizaciones alternativas. Aunque las técnicas reveladas se refieren principalmente a sesiones de comunicación protegida, las técnicas son también aplicables a sesiones de comunicación no protegidas, por ejemplo excluyendo las realizaciones que infieren el tipo de servicio a partir de mensajes que están relacionados con el establecimiento de una sesión protegida.

Se apreciará que las realizaciones antes descritas son citadas aquí a modo de ejemplo, y que la presente invención no está limitada a lo que ha sido particularmente mostrado y descrito aquí anteriormente. Más bien, el alcance de la presente invención está solamente definido por las reivindicaciones anejas.

REIVINDICACIONES

1. Un método de comunicación que comprende:

interceptar el Sistema de Nombre de Dominio, DNS, mensajes que son enviados en una red de comunicación en preparación para fijar las respectivas sesiones de comunicación que proporcionan los respectivos servicios asociados con los respectivos tipos de servicios, en donde las sesiones de comunicación están asociadas con los respectivos usuarios (32) que consumen los respectivos servicios, y con las respectivas áreas geográficas (42) en las que las sesiones de comunicación son entregadas;

extraer de los mensajes DNS interceptados una información DNS que es indicativa de los respectivos tipos de servicios, y almacenar en caché la información DNS extraída globalmente para pluralidades de usuarios por área geográfica (42) y no sólo por usuario (32); e

identificar un tipo de servicio (220) asociado con una sesión de comunicación dada que usa la información DNS globalmente almacenada en caché, y aplicar una policía de tráfico (232) a la sesión de comunicación dada dependiendo del tipo de servicio identificado.

2. El método de acuerdo con la reivindicación 1, en donde la sesión de comunicación dada entrega un servicio respectivo en una conexión protegida.

3. El método de acuerdo con la reivindicación 1 o 2, en donde la extracción de información DNS comprende extraer de los mensajes de DNS Identificadores de Recursos Uniformes, URIs, identificar ordenadores principales en la red de comunicaciones a la que los usuarios intentan conectarse, y las respectivas direcciones IP de los ordenadores principales, y asignar los URIs extraídos a uno o más tipos de servicios predefinidos, y en donde almacenar en caché la información de DNS comprende almacenar en caché las direcciones IP extraídas y los uno o más tipos de servicios en asociación uno con otro.

4. El método de acuerdo con la reivindicación 3, en donde la identificación del tipo de servicio comprende interceptar en el tráfico de la sesión de comunicación dada una dirección IP del ordenador principal de un ordenador principal asociado con la sesión de comunicación dada, recuperar un URI del ordenador principal almacenado en caché, que está asociado con las direcciones IP del ordenador principal, y asignar el URI del ordenador principal a los respectivos uno o más tipos de servicios predefinidos.

5. El método de acuerdo con la reivindicación 3, en donde la información almacenar en caché el DNS comprende almacenar en caché la dirección IP y el tipo de servicio identificado ambos localmente por usuario y globalmente por área geográfica, y en donde la identificación del tipo de servicio comprende recuperar el tipo de servicio almacenado en caché globalmente solamente si falla la recuperación del servicio almacenado en caché localmente.

6. El método de acuerdo con la reivindicación 5, en donde la aplicación de la policía de tráfico comprende aplicar la policía de tráfico separadamente por usuario.

7. El método de acuerdo con la reivindicación 5, en donde la aplicación de la policía de tráfico comprende aplicar la policía de tráfico separadamente por el área geográfica.

8. El método de acuerdo con las reivindicaciones 1 a 7, en donde el tipo de servicio comprende adicionalmente interceptar un mensaje de solicitud de iniciación de la sesión que un usuario envía a un ordenador principal para establecer la sesión de comunicación dada, y si el mensaje de solicitud de iniciación incluye una Indicación del Nombre de la Sesión, SNI, asignar el SNI a un respectivo tipo de servicio predefinido.

9. El método de acuerdo con las reivindicaciones 1 a 8, en donde la identificación del tipo de servicio comprende interceptar un certificado que un ordenador principal envía a un usuario en la fijación de la sesión de comunicación dada, y asignar una información relacionada con el tipo de servicio integrado en el certificado a uno o más tipos de servicios predefinidos.

10. El método de acuerdo con las reivindicaciones 1 a 9, en donde la identificación del tipo de servicio comprende monitorizar las características del flujo de la sesión de comunicación dada, e identificar el tipo de servicio basado en las características del flujo.

11. El método de acuerdo con cualquiera de las reivindicaciones 1 a 10, en donde la aplicación de la policía de tráfico comprende cambiar una velocidad de entrega de datos de tráfico de la sesión de comunicación dada.

12. El método de acuerdo con cualquiera de las reivindicaciones 1 a 11, en donde la aplicación de la policía de tráfico comprende aplicar la policía de tráfico basada en las condiciones de congestión que se desarrollan en la red de comunicaciones.

13. Un aparato que comprende:

una memoria caché (54); y

un procesador (52), el cual está configurado para interceptar mensajes del Sistema de Nombre del Dominio, DNS, que son enviados en una red de comunicación en preparación para fijar unas respectivas sesiones de comunicación que proporcionan unos respectivos servicios asociados con unos tipos de servicios respectivos, en donde las sesiones de comunicación están asociadas con usuarios respectivos (32) que consumen los respectivos servicios, y con las respectivas áreas geográficas (42) en las cuales las sesiones de comunicación son entregadas, para extraer de los mensajes DNS interceptados una información de DNS que es indicativa de los respectivos tipos de servicios, para almacenar en caché la información de DND extraída globalmente para pluralidades de usuarios por área geográfica (42) y no por usuario (32), para identificar un tipo de servicio (220) asociado con una sesión de comunicación dada usando la información de DNS globalmente almacenada en caché, y para aplicar una policía de tráfico (232) a la sesión de comunicación dada dependiendo del tipo de servicio identificado.

14. El aparato de acuerdo con la reivindicación 13, en donde el procesador está configurado para extraer de los mensajes DNS Identificadores de Recursos Uniformes, URIs, ordenadores principales que identifican en la red de comunicación a qué usuarios intentar conectar, y las respectivas direcciones IP de los ordenadores principales, y asignar los URIs extraídos a uno o más tipos de servicios predefinidos, y almacenar en caché las direcciones IP extraídas y el uno o más tipos de servicios en asociación entre sí.

15. El aparato de acuerdo con la reivindicación 13 o 14, en donde el procesador está configurado para identificar el tipo de servicio interceptando en tráfico de la sesión de comunicación dada una dirección IP de ordenador principal de un ordenador principal asociado con la sesión de comunicación dada, recuperando un URI de ordenador principal almacenado en caché que está asociado con la dirección IP del ordenador principal, y asignando el URI del ordenador principal y la dirección IP del ordenador principal a los respectivos uno o más tipos de servicios predefinidos.

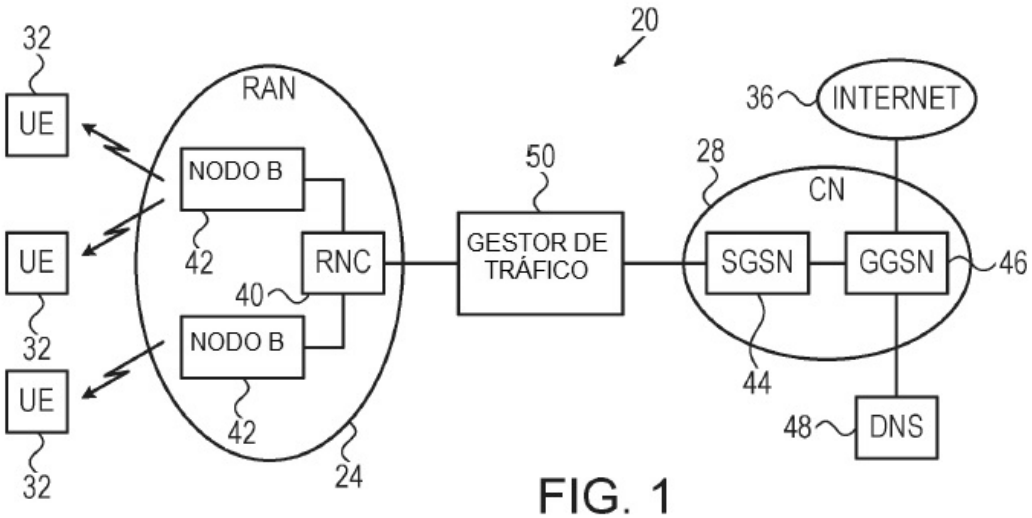
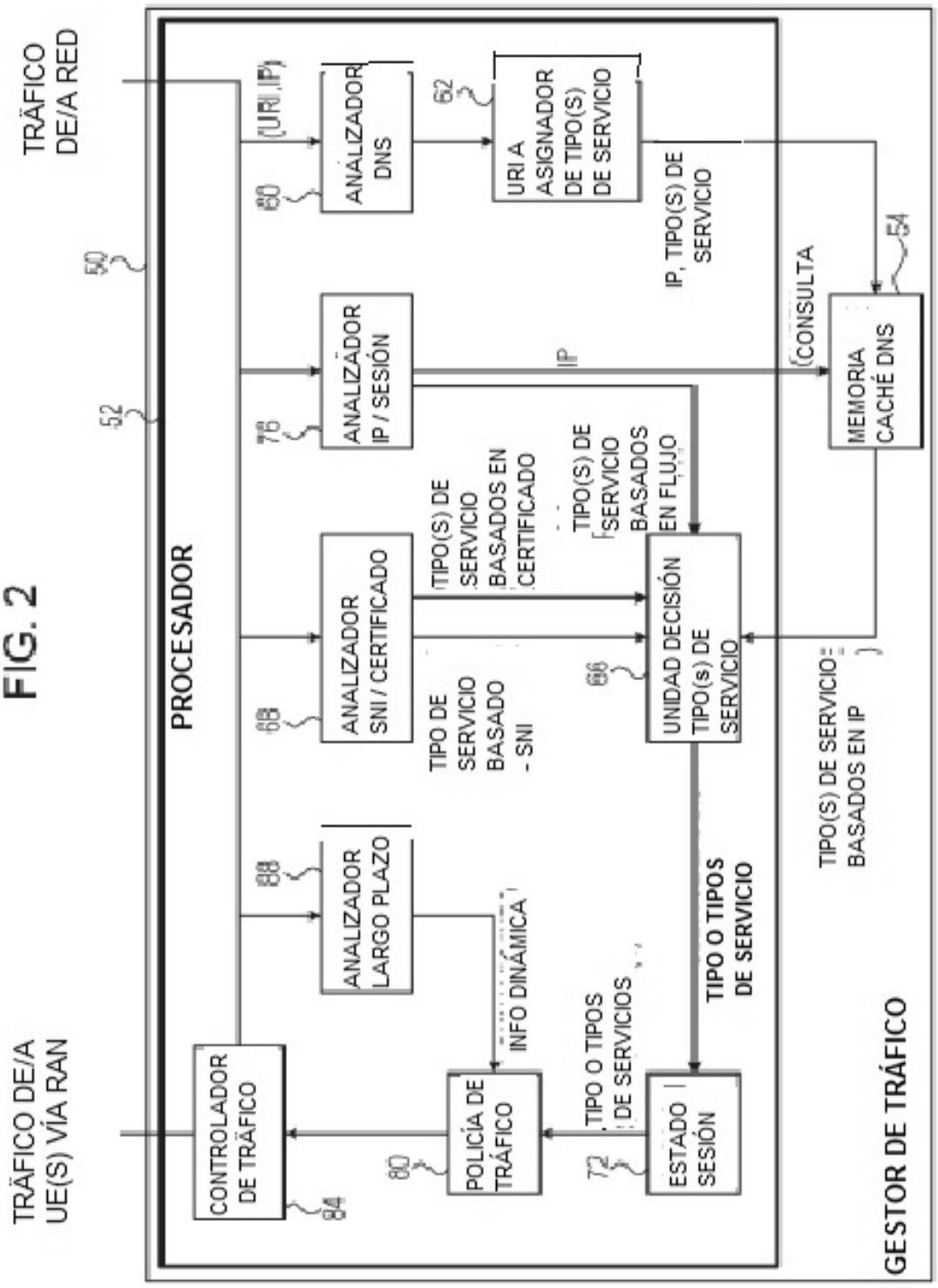

20
32
UE
RAN
NODO B
42
RNC
40
NODO B
42
24
50
GESTOR DE TRÁFICO
36
INTERNET
28
CN
SGSN
GGSN
46
44
48
DNS

FIG. 1

FIG. 2


TRÁFICO DE/A RED
TRÁFICO DE/A UE(S) VÍA RAN
PROCESADOR
GESTOR DE TRÁFICO
50
52
54
60
62
66
68
72
76
80
84
88
(URI, IP)
ANALIZADOR DNS
URI A ASIGNADOR DE TIPO(S) DE SERVICIO
IP, TIPO(S) DE SERVICIO
ANALIZADOR IP / SESIÓN
IP
(CONSULTA
MEMORIA CACHÉ DNS
TIPO(S) DE SERVICIO BASADOS EN CERTIFICADO
TIPO(S) DE SERVICIO BASADOS EN FLUJO
ANALIZADOR SNI / CERTIFICADO
TIPO DE SERVICIO BASADO - SNI
UNIDAD DECISIÓN TIPO(s) DE SERVICIO
TIPO(S) DE SERVICIO= BASADOS EN IP
ANALIZADOR LARGO PLAZO
INFO DINÁMICA
CONTROLADOR DE TRÁFICO
POLICÍA DE TRÁFICO
TIPO O TIPOS DE SERVICIOS
ESTADO SESIÓN
TIPO O TIPOS DE SERVICIO

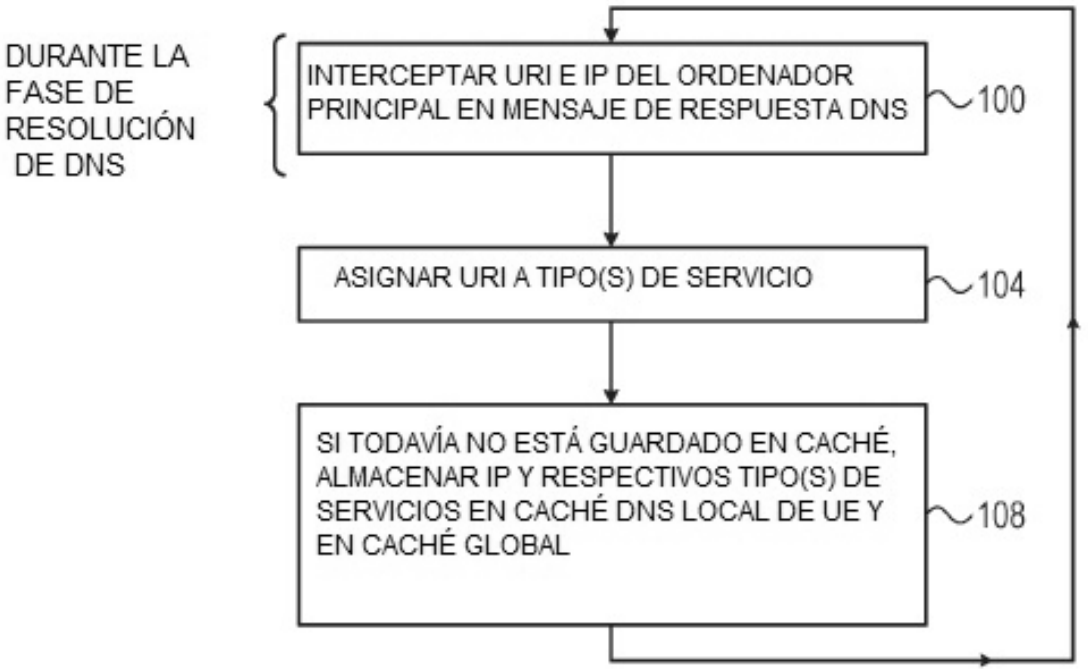

DURANTE LA FASE DE RESOLUCIÓN DE DNS
INTERCEPTAR URI E IP DEL ORDENADOR PRINCIPAL EN MENSAJE DE RESPUESTA DNS
100
ASIGNAR URI A TIPO(S) DE SERVICIO
104
SI TODAVÍA NO ESTÁ GUARDADO EN CACHÉ, ALMACENAR IP Y RESPECTIVOS TIPO(S) DE SERVICIOS EN CACHÉ DNS LOCAL DE UE Y EN CACHÉ GLOBAL
108

FIG. 3

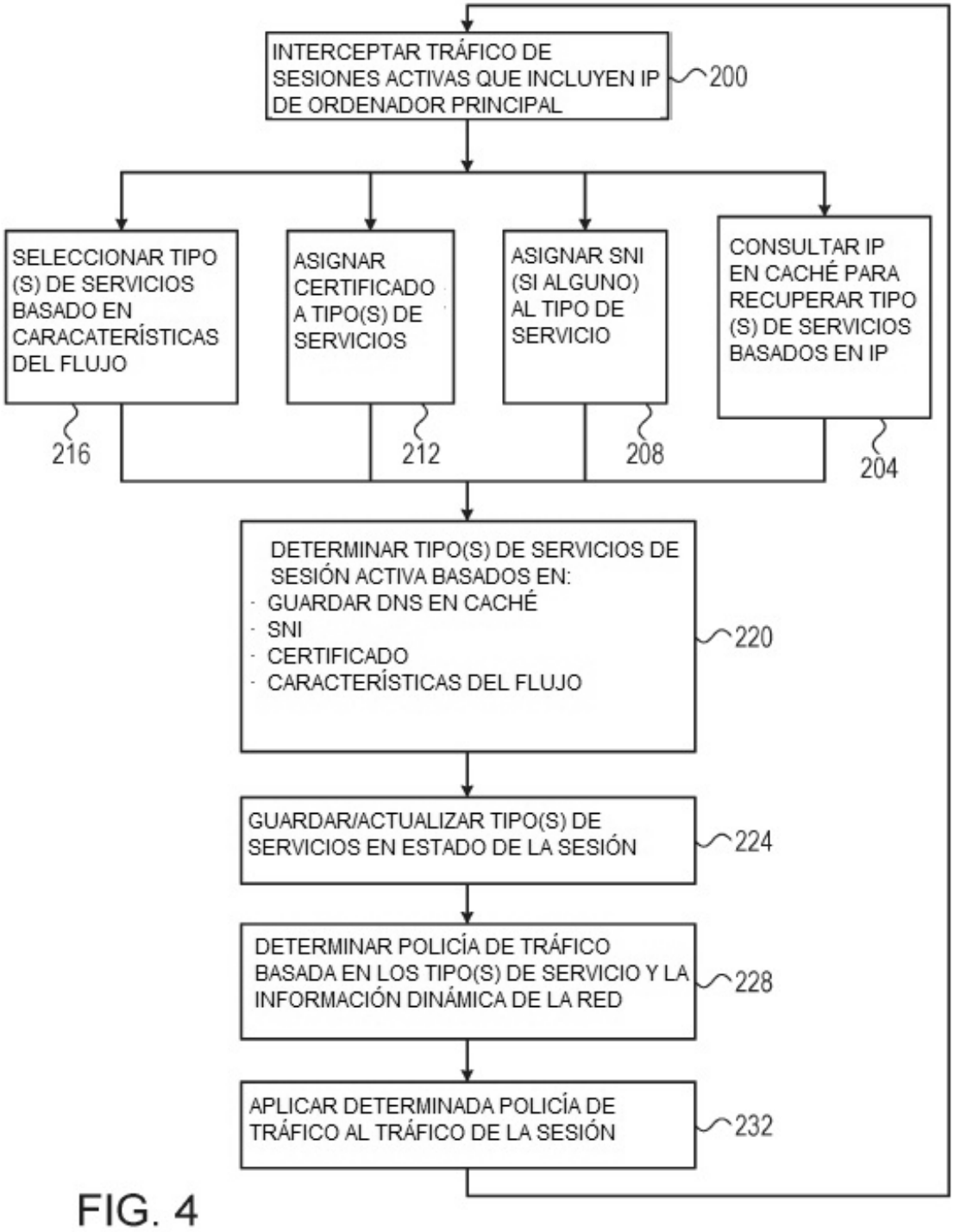

INTERCEPTAR TRÁFICO DE SESIONES ACTIVAS QUE INCLUYEN IP DE ORDENADOR PRINCIPAL
200
SELECCIONAR TIPO (S) DE SERVICIOS BASADO EN CARACATERÍSTICAS DEL FLUJO
216
ASIGNAR CERTIFICADO A TIPO(S) DE SERVICIOS
212
ASIGNAR SNI (SI ALGUNO) AL TIPO DE SERVICIO
208
CONSULTAR IP EN CACHÉ PARA RECUPERAR TIPO (S) DE SERVICIOS BASADOS EN IP
204
DETERMINAR TIPO(S) DE SERVICIOS DE SESIÓN ACTIVA BASADOS EN:
- GUARDAR DNS EN CACHÉ
- SNI
- CERTIFICADO
- CARACTERÍSTICAS DEL FLUJO
220
GUARDAR/ACTUALIZAR TIPO(S) DE SERVICIOS EN ESTADO DE LA SESIÓN
224
DETERMINAR POLICÍA DE TRÁFICO BASADA EN LOS TIPO(S) DE SERVICIO Y LA INFORMACIÓN DINÁMICA DE LA RED
228
APLICAR DETERMINADA POLICÍA DE TRÁFICO AL TRÁFICO DE LA SESIÓN
232

FIG. 4