(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 746 351**

(51) Int. CI.:

H04L 12/26 (2006.01)
H04L 12/24 (2006.01)
H04W 24/00 (2009.01)
H04W 28/10 (2009.01)
H04L 29/08 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **23.09.2016 PCT/CN2016/099891**

(87) Fecha y número de publicación internacional: **06.07.2017 WO17113900**

(96) Fecha de presentación y número de la solicitud europea: **23.09.2016 E 16880693 (3)**

(97) Fecha y número de publicación de la concesión europea: **17.07.2019 EP 3297213**

(54) Título: **Método y aparato para identificar información de aplicación en tráfico de red**

(30) Prioridad:

28.12.2015 CN 201511000809

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
05.03.2020

(73) Titular/es:

HUAWEI TECHNOLOGIES CO., LTD. (100.0%)
Huawei Administration Building, Bantian, Longgang District
Shenzhen, Guangdong 518129, CN

(72) Inventor/es:

LI, YOUYONG y
XIONG, YING

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

DESCRIPCIÓN

Método y aparato para identificar información de aplicación en tráfico de red.

Campo técnico

La presente solicitud se refiere al campo de las tecnologías de comunicaciones de ordenador y de red y, en particular, a un método para identificar información de aplicación en el tráfico de red y a un aparato para identificar información de aplicación en el tráfico de red.

Antecedentes

Con el rápido desarrollo de las tecnologías de Internet, varias aplicaciones, incluidos servicios y juegos, implementadas según las tecnologías de Internet se convierten en cada vez más abundantes. Con el fin de satisfacer varias demandas de una empresa o una autoridad reguladora de la red, por ejemplo, para implementar la gestión y el control del comportamiento en línea de un usuario, o clasificar aplicaciones populares actuales mediante la recolección de estadística sobre el tráfico, la identificación del tráfico se convierte en una función básica de un dispositivo de seguridad de red. El dispositivo de seguridad de red incluye un dispositivo de reenvío de paquetes que tiene una función de análisis y gestión de tráfico como, por ejemplo, una pasarela de seguridad, un cortafuegos y un dispositivo de inspección profunda de paquetes (Inspección Profunda de Paquetes, DPI, por sus siglas en inglés).

Las tecnologías de identificación de tráfico se clasifican en una tecnología de identificación de protocolo y una tecnología de identificación de aplicación. Como su nombre implica, la tecnología de identificación de protocolo significa que un dispositivo de seguridad de red determina un tipo de protocolo al cual pertenece cada tren de datos en el tráfico que fluye a través del dispositivo y, además, puede determinar proporciones de trenes de datos de diferentes tipos de protocolo en el tráfico total.

Una "aplicación" en la presente solicitud se refiere al software de aplicación que provee una función específica y que tiene una capacidad de acceso a la red y de procesamiento de paquetes. Después de que dicho software de aplicación se ejecuta en un dispositivo terminal, una interfaz de red en el dispositivo terminal puede habilitarse, una conexión a otro dispositivo terminal en una red se establece mediante el uso de la interfaz habilitada, y una serie de paquetes se transmiten mediante el uso de la conexión establecida. Entonces, las funciones específicas, por ejemplo, un navegador Internet Explorer (IE), software de mensajería instantánea Tencent QQ, y un cliente FileZilla de Protocolo de Transferencia de Archivos (Protocolo de Transferencia de Archivos, FTP, por sus siglas en inglés), se proveen a un usuario mediante el procesamiento de los paquetes recibidos.

Una aplicación se ejecuta en un protocolo; en otras palabras, múltiples aplicaciones diferentes pueden ejecutarse en un mismo tipo de protocolo. Por ejemplo, un cliente entre pares (entre pares, P2P, por sus siglas en inglés) y un navegador se implementan, ambos, según el protocolo de Transferencia de Hipertexto (Protocolo de Transferencia de Hipertexto, HTTP, por sus siglas en inglés). Por lo tanto, si la identificación de tráfico, y la gestión y el control se llevan a cabo según solamente el protocolo HTTP, si un tren de datos se envía por el cliente P2P o se envía por el navegador no puede identificarse. Si un tipo de una aplicación que envía un tren de datos del protocolo HTTP puede identificarse mediante el uso de la tecnología de identificación de aplicación, si un usuario está llevando a cabo una actividad de acceso a la red relacionada con el trabajo o está jugando un juego en línea no relacionado con el trabajo puede saberse, para bloquear el tráfico provocado por el juego en línea. Por lo tanto, en comparación con una tecnología de identificación de protocolo convencional, una tecnología de identificación de aplicación puede usarse para obtener un efecto de gestión y control más correcto.

Una tecnología de identificación de aplicación existente principalmente incluye una tecnología de identificación basada en las características, una tecnología de identificación heurística y una tecnología de identificación de asociación.

La tecnología de identificación basada en las características se refiere a la identificación, mediante el uso de una característica de diseño de formato de un paquete específico a una aplicación como, por ejemplo, una palabra clave distintiva, o un contenido de campo en una ubicación fija, de una aplicación que envía el paquete. Por ejemplo, después de que el dispositivo de seguridad de red recibe un paquete, si el paquete lleva una palabra clave "PPLiveVA" se consulta, y si el paquete lleva la palabra clave "PPLiveVA", ello indica que una aplicación que envía el paquete es una televisión web PPTV.

La tecnología de identificación heurística se refiere a la obtención, mediante el análisis de fenómenos como, por ejemplo, una longitud de un paquete enviado por una aplicación, una regularidad de aparición de un carácter en el contenido del paquete, una regularidad de interacción de dos lados de comunicación, y un intervalo de envío de paquetes, de una regla estadística que puede usarse para distinguir la aplicación de otra aplicación, y luego distinguir, mediante el uso de la regla, la aplicación que envía el paquete. La tecnología de identificación heurística tiene un efecto de identificación particular en un paquete cifrado, o un paquete que se envía mediante el uso de un

protocolo no divulgado privado. Sin embargo, dado que la regla se obtiene por análisis estadístico, se provocan los problemas de una tasa de informes fallidos y tasa de informes falsos relativamente altas.

La tecnología de identificación de asociación se refiere a la concordancia de una dirección IP, un número de puerto y un identificador de protocolo que son de un paquete con una regla de identificación de asociación que incluye correspondencias entre una aplicación, y una dirección IP, un número de puerto y un identificador de protocolo, para identificar una aplicación que envía el paquete.

Las características y reglas de las cuales depende la tecnología de identificación de aplicación existente se obtienen todas mediante el análisis manual de una gran cantidad de paquetes recogidos. Un fabricante de dispositivos de seguridad de red o una agencia de tercero que colabora con el fabricante de dispositivos de seguridad de red carga una biblioteca de reglas de actualización que incluye una característica y una regla a un sitio web de actualización del fabricante de software, y un dispositivo de seguridad de red obtiene la biblioteca de reglas de actualización del sitio web de actualización, para asegurar una capacidad de identificación del dispositivo de seguridad de red. Sin embargo, debido a factores como, por ejemplo, una actualización no oportuna de una biblioteca de reglas, y la baja exactitud de la tecnología de identificación heurística, por medio de la tecnología de identificación de aplicación existente, una proporción considerable del tráfico de red aún no puede identificarse, o un resultado de identificación incorrecto se obtiene para una proporción considerable del tráfico de red.

El documento US 2013/238782 describe un método para identificar una aplicación asociada a flujos IP que se desplazan entre múltiples móviles y un elemento de red en una red de comunicación mediante el uso de paquetes de sistema de nombres de dominio (DNS, por sus siglas en inglés). El elemento de red construye una tabla de mapeo que mapea direcciones IP a información de aplicación correspondiente según paquetes DNS recibidos.

Compendio

Las realizaciones de la presente solicitud según las reivindicaciones independientes proveen un método, un dispositivo terminal y sistemas para identificar información de aplicación en el tráfico de red, para mejorar un efecto de identificación de una tecnología de identificación de aplicación.

Las realizaciones de la presente solicitud proveen las siguientes soluciones técnicas:

Según un primer aspecto, se provee un método para identificar información de aplicación en un tráfico de red, y el método se ejecuta por un dispositivo terminal. Una primera tabla de correspondencia en el dispositivo terminal almacena, en una forma de registro, una correspondencia entre un identificador de un proceso que se ejecuta en el dispositivo terminal y un identificador de un tren de datos creado por el proceso. Una segunda tabla de correspondencia en el dispositivo terminal almacena, en una forma de registro, una correspondencia entre un identificador de una aplicación y un identificador de un proceso creado por la aplicación. El identificador del tren de datos es una 5-tupla que incluye una dirección de origen, un puerto de origen, una dirección de destino, un puerto de destino y un identificador de protocolo.

El método incluye:

recibir un identificador, enviado por un dispositivo de seguridad de red, de un primer tren de datos;

consultar, en la primera tabla de correspondencia, un primer registro en el cual el identificador del primer tren de datos se almacena;

si el primer registro se encuentra, obtener un identificador de un proceso en el primer registro, y consultar, en la segunda tabla de correspondencia, un segundo registro en el cual el identificador del proceso en el primer registro se almacena;

si el segundo registro se encuentra, obtener un identificador de una aplicación del segundo registro, y enviar el identificador de la aplicación al dispositivo de seguridad de red.

Según el método para identificar información de aplicación en el tráfico de red provisto en la presente realización de la presente solicitud, el dispositivo terminal encuentra, según el identificador del tren de datos enviado por el dispositivo de seguridad de red, una tabla de correspondencia localmente almacenada, y luego realimenta el identificador de la aplicación al dispositivo de seguridad de red y, de esta manera, asiste al dispositivo de seguridad de red en la determinación de un resultado de identificación de aplicación del tren de datos. En comparación con la técnica anterior, en el método anterior, más aplicaciones pueden identificarse por medio de la interacción entre el dispositivo de seguridad de red y el dispositivo terminal, de modo que una proporción del tráfico no identificado en el tráfico total se reduce, y un efecto de identificación del tráfico de red se mejora.

El dispositivo terminal puede obtener y actualizar la primera tabla de correspondencia de las siguientes maneras para asegurar la característica de tiempo real de la primera tabla de correspondencia y reducir el espacio de almacenamiento ocupado.

De manera opcional, el dispositivo terminal obtiene la primera tabla de correspondencia mediante el uso de las siguientes etapas:

obtener, por el dispositivo terminal mediante el uso de una interfaz provista por un sistema operativo, un identificador de al menos un proceso que se ejecuta en el dispositivo terminal; y

para cada identificador obtenido de un proceso, obtener, por el dispositivo terminal, un identificador de un tren de datos creado por el proceso, generar un registro que incluye el identificador del proceso y el identificador del tren de datos, y almacenar el registro en la primera tabla de correspondencia.

De manera opcional, el dispositivo terminal obtiene la primera tabla de correspondencia mediante el uso de las siguientes etapas:

obtener, por el dispositivo terminal mediante el uso de una función de gancho, un episodio en el que el sistema operativo crea un proceso;

obtener un identificador del proceso recientemente creado del episodio de creación de un proceso; y

obtener un identificador de un tren de datos creado por el proceso recientemente creado, generar un registro que incluye el identificador del proceso recientemente creado y el identificador del tren de datos creado por el proceso recientemente creado, y almacenar el registro en la primera tabla de correspondencia; y

el dispositivo terminal obtiene la primera tabla de correspondencia que además incluye:

obtener, por el dispositivo terminal mediante el uso de la función de gancho, un episodio en el que el sistema operativo abandona un proceso; y

obtener un identificador del proceso abandonado del episodio de abandono de un proceso, y eliminar, de la primera tabla de correspondencia, un registro que incluye el identificador del proceso abandonado.

De manera opcional, un registro en la primera tabla de correspondencia además incluye un último tiempo de actividad de un tren de datos; y el método además incluye:

determinar, por el dispositivo terminal, un registro caducado en la primera tabla de correspondencia, donde el registro caducado es un registro en el cual un intervalo de tiempo entre un último tiempo de actividad que es de un tren de datos y que se incluye en el registro caducado y un tiempo actual supera un intervalo de tiempo predeterminado; y

eliminar el registro caducado.

De manera opcional, después de que el dispositivo terminal obtiene la primera tabla de correspondencia, el método además incluye:

obtener, por el dispositivo terminal mediante el uso de la función de gancho, un paquete transmitido por el dispositivo terminal;

obtener, del paquete obtenido, un identificador de un tren de datos al cual el paquete pertenece; y

actualizar un último tiempo de actividad de un tren de datos en un registro que se encuentra en la primera tabla de correspondencia y que incluye el identificador del tren de datos al cual el paquete pertenece al tiempo actual.

De manera opcional, después de que el dispositivo terminal obtiene la primera tabla de correspondencia, el método además incluye:

obtener, por el dispositivo terminal mediante el uso de la función de gancho, un paquete transmitido por el dispositivo terminal;

obtener, del paquete obtenido, un identificador de estado de paquete y un identificador de un tren de datos al cual el paquete pertenece; y

si el identificador de estado de paquete es FIN, eliminar, de la primera tabla de correspondencia, un registro que incluye el identificador del tren de datos al cual el paquete pertenece.

Con el fin de obtener un tren de datos completo para facilitar el análisis posterior como, por ejemplo, una extracción de regla, de manera opcional, después de obtener un identificador de un proceso en el primer registro, el método además incluye:

establecer una bandera de recolección de paquetes para el identificador del proceso, donde la bandera de recolección de paquetes se usa para ordenar al dispositivo terminal que obtenga y almacene, después de capturar mediante el uso de la interfaz del sistema operativo un paquete transmitido por el proceso, un tren de datos completo posteriormente transmitido por el proceso.

Según un segundo aspecto, se provee un dispositivo terminal. El dispositivo terminal incluye una memoria, un procesador y una interfaz de red, y la memoria, el procesador y la interfaz de red se comunican entre sí mediante el uso de un bus.

La memoria almacena el código de programa, una primera tabla de correspondencia y una segunda tabla de correspondencia, donde la primera tabla de correspondencia almacena, en una forma de registro, una correspondencia entre un identificador de un proceso que se ejecuta en el dispositivo terminal y un identificador de un tren de datos creado por el proceso, la segunda tabla de correspondencia almacena, en una forma de registro, una correspondencia entre un identificador de una aplicación y un identificador de un proceso creado por la aplicación, y el identificador del tren de datos es una 5-tupla que incluye una dirección de origen, un puerto de origen, una dirección de destino, un puerto de destino y un identificador de protocolo.

La interfaz de red se configura para recibir un identificador, enviado por un dispositivo de seguridad de red, de un primer tren de datos.

El procesador se adapta para consultar, en la primera tabla de correspondencia, un primer registro en el cual el identificador del primer tren de datos se almacena; si el primer registro se encuentra, obtener un identificador de un proceso en el primer registro, y consultar, en la segunda tabla de correspondencia, un segundo registro en el cual el identificador del proceso en el primer registro se almacena; si el segundo registro se encuentra, obtener un identificador de una aplicación del segundo registro.

La interfaz de red se configura además para, si el segundo registro se encuentra, enviar el identificador de la aplicación obtenida por el procesador al dispositivo de seguridad de red.

De manera opcional, el procesador se configura además para obtener la primera tabla de correspondencia mediante el uso de las siguientes operaciones: obtener, mediante el uso de una interfaz provista por un sistema operativo, un identificador de al menos un proceso que se está ejecutando en el dispositivo terminal; y para cada identificador obtenido de un proceso, obtener, por el dispositivo terminal, un identificador de un tren de datos creado por el proceso, generar un registro que incluye el identificador del proceso y el identificador del tren de datos, y almacenar el registro en la primera tabla de correspondencia.

De manera opcional, el procesador se configura además para obtener la primera tabla de correspondencia mediante el uso de las siguientes operaciones:

obtener, mediante el uso de una función de gancho, un episodio en el que el sistema operativo crea un proceso;

obtener un identificador del proceso recientemente creado del episodio de creación de un proceso; y

obtener un identificador de un tren de datos creado por el proceso recientemente creado, generar un registro que incluye el identificador del proceso recientemente creado y el identificador del tren de datos creado por el proceso recientemente creado, y almacenar el registro en la primera tabla de correspondencia; y

obtener, mediante el uso de la función de gancho, un episodio en el que el sistema operativo abandona un proceso; y

obtener un identificador del proceso abandonado del episodio de abandono de un proceso, y eliminar, de la primera tabla de correspondencia, un registro que incluye el identificador del proceso abandonado.

De manera opcional, un registro en la primera tabla de correspondencia además incluye un último tiempo de actividad de un tren de datos; y

el procesador se configura además para: determinar un registro caducado en la primera tabla de correspondencia, donde el registro caducado es un registro en el cual un intervalo de tiempo entre un último tiempo de actividad que es de un tren de datos y que se incluye en el registro caducado y un tiempo actual supera un intervalo de tiempo predeterminado; y eliminar el registro caducado.

De manera opcional, el procesador se configura además para: después de obtener la primera tabla de correspondencia, obtener, por el dispositivo terminal mediante el uso de la función de gancho, un paquete transmitido por el dispositivo terminal;

obtener, del paquete obtenido, un identificador de un tren de datos al cual el paquete pertenece; y

actualizar un último tiempo de actividad de un tren de datos en un registro que se encuentra en la primera tabla de correspondencia y que incluye el identificador del tren de datos al cual el paquete pertenece al tiempo actual.

De manera opcional, el procesador se configura además para: después de obtener la primera tabla de correspondencia, obtener, por el dispositivo terminal mediante el uso de la función de gancho, un paquete transmitido por el dispositivo terminal;

obtener, del paquete obtenido, un identificador de estado de paquete y un identificador de un tren de datos al cual el paquete pertenece; y

si el identificador de estado de paquete es FIN, eliminar, de la primera tabla de correspondencia, un registro que incluye el identificador del tren de datos al cual el paquete pertenece.

Según un tercer aspecto, se provee un sistema para identificar información de aplicación en el tráfico de red, que incluye un dispositivo de seguridad de red y un dispositivo terminal.

El dispositivo de seguridad de red se configura para: recibir un primer tren de datos, y obtener un identificador del primer tren de datos, donde el identificador del primer tren de datos es una 5-tupla que incluye una dirección de origen, un puerto de origen, una dirección de destino, un puerto de destino y un identificador de protocolo; enviar el identificador del primer tren de datos al dispositivo terminal según la dirección de origen o la dirección de destino en el identificador del primer tren de datos, donde una dirección del dispositivo terminal es la dirección de origen o la dirección de destino en el identificador del primer tren de datos; recibir un identificador de una aplicación enviada por el dispositivo terminal; y determinar que el identificador recibido de la aplicación es un identificador de una aplicación que envía el primer tren de datos.

El dispositivo terminal se configura para almacenar una primera tabla de correspondencia y una segunda tabla de correspondencia, donde la primera tabla de correspondencia almacena, en una forma de registro, una correspondencia entre un identificador de un proceso que se ejecuta en el dispositivo terminal y un identificador de un tren de datos creado por el proceso, la segunda tabla de correspondencia almacena, en una forma de registro, una segunda correspondencia entre un identificador de una aplicación y un identificador de un proceso creado por la aplicación, y el identificador del tren de datos es una 5-tupla que incluye una dirección de origen, un puerto de origen, una dirección de destino, un puerto de destino y un identificador de protocolo.

El dispositivo terminal se configura para: recibir el identificador, enviado por el dispositivo de seguridad de red, del primer tren de datos; consultar, en la primera tabla de correspondencia, un primer registro en el cual el identificador del primer tren de datos se almacena; si el primer registro se encuentra, obtener un identificador de un proceso en el primer registro, y consultar, en la segunda tabla de correspondencia, un segundo registro en el cual el identificador del proceso en el primer registro se almacena; si el segundo registro se encuentra, obtener un identificador de una aplicación del segundo registro; y enviar el identificador de la aplicación al dispositivo de seguridad de red.

En el sistema para identificar información de aplicación en el tráfico de red provisto en la presente realización de la presente solicitud, el dispositivo de seguridad de red determina un resultado de identificación de aplicación de un tren de datos según una realimentación del dispositivo terminal. En comparación con la técnica anterior, en el sistema anterior, más aplicaciones pueden identificarse por medio de la interacción entre el dispositivo de seguridad de red y el dispositivo terminal, de modo que una proporción del tráfico no identificado en el tráfico total se reduce, y un efecto de identificación de tráfico de red se mejora.

Según un cuarto aspecto, se provee un sistema para identificar información de aplicación en el tráfico de red, que incluye:

un dispositivo terminal, un dispositivo de seguridad de red y un dispositivo de procesamiento de datos;

el dispositivo de seguridad de red se configura para recibir un primer tren de datos, generar un primer registro de identificación después de determinar un identificador de una aplicación que envía el primer tren de datos, donde el primer registro de identificación incluye un identificador del primer tren de datos y el identificador de la aplicación, y el identificador del tren de datos es una 5-tupla que incluye una dirección de origen, un puerto de origen, una dirección de destino, un puerto de destino y un identificador de protocolo; y enviar el primer registro de identificación al dispositivo de procesamiento de datos;

el dispositivo terminal se configura para obtener un identificador de un proceso que se ejecuta en el dispositivo terminal y un identificador de un segundo tren de datos creado por el proceso, para generar un segundo registro de identificación, donde el segundo registro de identificación incluye el identificador del segundo tren de datos y el identificador del proceso; obtener una tabla de correspondencia, donde cada registro en la tabla de correspondencia almacena un identificador de una aplicación y un identificador de un proceso creado por la aplicación; y enviar el segundo registro de identificación y la tabla de correspondencia al dispositivo de procesamiento de datos;

el dispositivo de procesamiento de datos se configura para recibir el primer registro de identificación del dispositivo de seguridad de red, recibir el segundo registro de identificación y la tabla de correspondencia del dispositivo terminal; determinar si el identificador del primer tren de datos comprendido en el primer registro de identificación es igual al identificador del segundo tren de datos comprendido en el segundo registro de identificación; si el identificador del primer tren de datos incluido en el primer registro de identificación es igual al identificador del segundo tren de datos incluido en el segundo registro de identificación, consultar si un primer registro de asociación existe en la tabla de correspondencia, donde el primer registro de asociación almacena el identificador de la aplicación incluida en el primer registro de identificación y el identificador del proceso incluido en el segundo registro de identificación; si el primer registro de asociación no existe, determinar que el primer registro de identificación es un registro de identificación incorrecto.

Según el sistema para identificar información de aplicación en el tráfico de red provisto en la presente realización de la presente solicitud, un dispositivo de procesamiento de datos puede identificar, mediante comparación de un registro de identificación del dispositivo terminal con el del dispositivo de seguridad de red, un registro de identificación incorrecto que es del dispositivo de seguridad de red y que es difícil de encontrar mediante el uso de la técnica anterior. Por lo tanto, un efecto de identificación de tráfico de red se mejora.

De manera opcional, el dispositivo de procesamiento de datos incluye una memoria, un procesador y una interfaz de red, y la memoria, el procesador y la interfaz de red se comunican entre sí mediante el uso de un bus.

La memoria almacena un código de programa.

La interfaz de red se configura para: recibir el primer registro de identificación del dispositivo de seguridad de red, y recibir el segundo registro de identificación y la tabla de correspondencia del dispositivo terminal.

El procesador se adapta para, si el identificador del primer tren de datos incluido en el primer registro de identificación es igual al identificador del segundo tren de datos incluido en el segundo registro de identificación, consultar si un primer registro de asociación existe en la tabla de correspondencia, donde el primer registro de asociación almacena el identificador de la aplicación incluida en el primer registro de identificación y un identificador de un proceso incluido en el segundo registro de identificación; y

si el primer registro de asociación no existe, determinar que el primer registro de identificación es un registro de identificación incorrecto.

En el sistema para identificar información de aplicación en el tráfico de red provisto en la presente realización de la presente solicitud, el dispositivo de procesamiento de datos puede identificar, mediante comparación de un registro de identificación del dispositivo terminal con el del dispositivo de seguridad de red, un registro de identificación incorrecto que es del dispositivo de seguridad de red y que es difícil de encontrar mediante el uso de la técnica anterior. Por lo tanto, un efecto de identificación de tráfico de red se mejora.

Breve descripción de los dibujos

Con el fin de describir las soluciones técnicas en las realizaciones de la presente solicitud o en la técnica anterior de forma más clara, a continuación se describen brevemente los dibujos anexos requeridos para describir las realizaciones o la técnica anterior. De manera aparente, los dibujos anexos en la siguiente descripción muestran algunas realizaciones de la presente invención, y una persona con experiencia ordinaria en la técnica puede incluso derivar otros dibujos a partir de dichos dibujos anexos sin esfuerzos creativos.

La Figura 1A es un diagrama esquemático de un sistema para identificar información de aplicación en el tráfico de red según una realización de la presente solicitud;

la Figura 1B es un diagrama esquemático de otro sistema para identificar información de aplicación en el tráfico de red según una realización de la presente solicitud;

la Figura 2A y Figura 2B son un diagrama de flujo de un método para identificar información de aplicación en el tráfico de red según una realización de la presente solicitud;

la Figura 3A es un diagrama de flujo de obtención de una primera tabla de correspondencia según una realización de la presente solicitud;

la Figura 3B-1 y Figura 3B-2 son un diagrama de flujo de actualización de una primera tabla de correspondencia según una realización de la presente solicitud;

la Figura 4A y Figura 4B son un diagrama de flujo de obtención de un tren de datos completo según una realización de la presente solicitud;

la Figura 5A es un diagrama estructural esquemático de un dispositivo terminal según una realización de la presente solicitud;

la Figura 5B es un diagrama estructural esquemático de otro dispositivo terminal según una realización de la presente solicitud;

la Figura 6A es un diagrama estructural esquemático de un dispositivo de seguridad de red según una realización de la presente solicitud;

la Figura 6B es un diagrama estructural esquemático de otro dispositivo de seguridad de red según una realización de la presente solicitud;

la Figura 7 es un diagrama esquemático de otro sistema para identificar información de aplicación en el tráfico de red según una realización de la presente solicitud;

la Figura 8A-1 a la Figura 8A-3 son un diagrama de interacción de un método para identificar información de aplicación en el tráfico de red según una realización de la presente solicitud;

la Figura 8B-1 y Figura 8B-2 son un diagrama de interacción de otro método para identificar información de aplicación en el tráfico de red según una realización de la presente solicitud;

la Figura 9A es un diagrama estructural esquemático de un dispositivo de procesamiento de datos según una realización de la presente solicitud; y

la Figura 9B es un diagrama estructural esquemático de otro dispositivo de procesamiento de datos según una realización de la presente solicitud.

Descripción de las realizaciones

Un "tren de datos" en la presente solicitud se refiere a una serie de paquetes que se transmiten entre dos dispositivos terminales dentro de un segmento de tiempo particular y que se determinan mediante el uso de una dirección de origen, un puerto de origen, una dirección de destino, un puerto de destino y un tipo de protocolo. El dispositivo terminal en la presente solicitud puede ser un dispositivo que tiene una función de acceso a la red y una capacidad de ejecución de software de aplicación como, por ejemplo, un ordenador portátil, un servidor o un terminal móvil. Un identificador del tren de datos se refiere a una 5-tupla que incluye una dirección de origen, un puerto de origen, una dirección de destino, un puerto de destino y un identificador de protocolo.

Una tecnología de identificación de aplicación significa que un dispositivo de seguridad de red determina qué software de aplicación en el dispositivo terminal envía un tren de datos.

En un método para identificar información de aplicación en el tráfico de red provisto en una realización de la presente solicitud, algunos trenes de datos que no pueden identificarse mediante el uso de una tecnología de identificación de aplicación existente pueden identificarse por medio de la interacción entre el dispositivo de seguridad de red y el dispositivo terminal, de modo que una proporción del tráfico de red que no puede identificarse en el tráfico de red total se reduce, y una tasa de éxito de identificación de aplicación se mejora; o algunos registros de identificación incorrectos pueden identificarse, de modo que una tasa de informes falsos se reduce, y la exactitud de identificación de aplicación se mejora.

Realización 1

La Figura 1A y Figura 1B son diagramas esquemáticos de un sistema para identificar información de aplicación en el tráfico de red según una realización de la presente solicitud. El sistema incluye un dispositivo 110 terminal y un dispositivo 120 de seguridad de red.

El dispositivo 120 de seguridad de red puede desplegarse en dos maneras de despliegue. Una primera manera de despliegue es una manera de despliegue en el trayecto que se muestra en la Figura 1A. El dispositivo 120 de seguridad de red es un dispositivo que tiene una función de reenvío de paquetes. Por ejemplo, el dispositivo 110 terminal puede ser un ordenador personal o un servidor ubicado en una red de área local, y el dispositivo 120 de seguridad de red es un dispositivo cortafuegos en la red de área local. El dispositivo 110 terminal puede, de manera alternativa, ser un ordenador personal o un servidor ubicado en Internet, y el dispositivo 120 de seguridad de red es una pasarela de seguridad en Internet. En dicha manera de despliegue, después de obtener un tren de datos que fluye a través del dispositivo 120 de seguridad de red, el dispositivo 120 de seguridad de red determina una aplicación que envía el tren de datos y que se encuentra en el dispositivo terminal. En la descripción posterior de la presente solicitud, también se hace referencia al presente proceso como identificación, por el dispositivo 120 de seguridad de red, de una aplicación de un tren de datos que fluye a través del dispositivo 120 de seguridad de red, para resumir. Además, una política de seguridad se almacena en el dispositivo 120 de seguridad de red. Después de obtener un resultado de identificación de aplicación del tren de datos, el dispositivo 120 de seguridad de red

determina, según la política de seguridad, una manera de procesamiento posterior para el tren de datos, por ejemplo, bloquear el tren de datos o reenviar el tren de datos. Un proceso detallado se describe en las siguientes realizaciones con referencia a los ejemplos.

Una segunda manera de despliegue es una manera de despliegue fuera del trayecto que se muestra en la Figura 1B. El dispositivo 120 de seguridad de red es un dispositivo de trayecto indirecto que tiene una función de recolección de estadística de tráfico, y se configura para recoger estadística sobre proporciones de tráfico de varias aplicaciones en el tráfico total, y puede además obtener información de clasificación de las varias aplicaciones. El dispositivo 120 de seguridad de red recibe un tren de datos en espejo enviado por un dispositivo de reenvío de paquetes, identifica una aplicación del tren de datos en espejo, actualiza un registro estadístico según un resultado de identificación y produce, de manera regular, un resultado estadístico.

Independientemente de la manera de despliegue en el trayecto que se muestra en la Figura 1A o de la manera de despliegue fuera del trayecto que se muestra en la Figura 1B, el dispositivo 120 de seguridad de red necesita intercambiar mensajes con el dispositivo 110 terminal. A continuación se describe una función del dispositivo 120 de seguridad de red y una función del dispositivo 110 terminal. La función del dispositivo 120 de seguridad de red y la función del dispositivo 110 terminal pueden implementarse, respectivamente, por un módulo de software en el dispositivo 120 de seguridad de red y un módulo de software en el dispositivo 110 terminal. Por ejemplo, la siguiente función del dispositivo 120 de seguridad de red se implementa por un módulo de identificación de aplicación en el dispositivo 120 de seguridad de red, y la función del dispositivo 110 terminal se implementa por un agente (Agente) en el dispositivo 110 terminal.

El dispositivo 120 de seguridad de red se configura para recibir un primer tren de datos, obtener un identificador del primer tren de datos, y enviar el identificador del tren de datos al dispositivo 110 terminal según una dirección de origen o una dirección de destino en el identificador del primer tren de datos, donde una dirección del dispositivo 110 terminal es la dirección de origen o la dirección de destino en el identificador del primer tren de datos; recibir un identificador de una aplicación enviada por el dispositivo 110 terminal; y determinar que el identificador recibido de la aplicación es un identificador de una aplicación que envía el primer tren de datos.

De manera opcional, una política de seguridad se almacena en el dispositivo 120 de seguridad de red. La política de seguridad es una regla preconfigurada sobre el permiso de reenvío de un tren de datos particular, o sobre la prohibición de reenvío de un tren de datos particular. Por ejemplo, "permitir la navegación (WB, por sus siglas en inglés)-por defecto denegar todos" indica que solo el reenvío de un tren de datos enviado por un navegador se permite, y el reenvío de un tren de datos enviado por otra aplicación se prohíbe. Por ejemplo, "denegar QQ denegar P2P-por defecto permitir todos" indica que el reenvío de trenes de datos enviados solamente por software de mensajería instantánea QQ y software de cliente P2P se prohíbe, y el reenvío de un tren de datos enviado por otra aplicación se permite. Para una política de seguridad configurada para permitir el reenvío de algunos trenes de datos, dicha política de seguridad incluye un identificador de una aplicación que se permite que lleve a cabo el reenvío. Por ejemplo, una política de seguridad permite solo el reenvío de un tren de datos enviado por un navegador, es decir, un identificador de una aplicación que se permite que lleve a cabo el reenvío es un identificador WB del navegador. Después de recibir un tren de datos, el dispositivo 120 de seguridad de red reenvía el tren de datos si el dispositivo 120 de seguridad de red identifica que un identificador de una aplicación que envía el tren de datos es WB, o el dispositivo 120 de seguridad de red bloquea el tren de datos si el dispositivo 120 de seguridad de red identifica que un identificador de una aplicación que envía el tren de datos es un identificador P2P de un cliente P2P antes que WB.

Cuando recibe un paquete del primer tren de datos, el dispositivo 120 de seguridad de red primero identifica el primer tren de datos mediante el uso de una tecnología de identificación de aplicación existente como, por ejemplo, una tecnología de identificación basada en las características, una tecnología de identificación heurística o una tecnología de identificación de asociación.

Una política de seguridad usada para permitir el reenvío de un tren de datos particular se usa como un ejemplo. Si un resultado de identificación puede obtenerse, se determina si la política de seguridad incluye un identificador identificado de una aplicación. El paquete del primer tren de datos se reenvía si la política de seguridad incluye el identificador identificado de la aplicación, o el paquete del primer tren de datos se bloquea si la política de seguridad no incluye el identificador identificado de la aplicación. Si el dispositivo 120 de seguridad de red no puede obtener un resultado de identificación según la anterior tecnología de identificación de aplicación existente, es decir, el identificador de la aplicación que envía el primer tren de datos no puede determinarse, el dispositivo 120 de seguridad de red obtiene el identificador del primer tren de datos, y envía el identificador del primer tren de datos a un dispositivo terminal identificado por la dirección de origen en el identificador del primer tren de datos, o envía el identificador del primer tren de datos a un dispositivo terminal identificado por la dirección de destino en el identificador del primer tren de datos, para obtener un identificador de una aplicación devuelta por el dispositivo terminal por medio de la interacción con el dispositivo terminal, y determinar que el identificador de la aplicación que envía el primer tren de datos es el identificador de la aplicación devuelta por el dispositivo terminal.

Debe notarse que el dispositivo de seguridad de red puede enviar, cuando el resultado de identificación no puede obtenerse, el identificador del primer tren de datos al dispositivo terminal identificado por la dirección de origen en el identificador del primer tren de datos, o el identificador del primer tren de datos al dispositivo terminal identificado por la dirección de destino en el identificador del primer tren de datos. Además, para mejorar la exactitud de identificación, por ejemplo, cuando la tecnología de identificación de asociación se usa para llevar a cabo la identificación de aplicación y una regla de identificación de asociación concuerda por primera vez, para confirmar la exactitud de la regla de identificación de asociación, el dispositivo de seguridad de red puede también enviar el identificador del primer tren de datos al dispositivo terminal; comparar un identificador de una aplicación posteriormente devuelta por el dispositivo terminal con un resultado de identificación obtenido según la regla de identificación de asociación; y si el identificador de la aplicación es igual al resultado de identificación, determinar que la regla de identificación de asociación es correcta.

El dispositivo 110 terminal se configura para obtener una primera tabla de correspondencia y una segunda tabla de correspondencia. Cada registro en la primera tabla de correspondencia almacena un identificador de un proceso que se ejecuta en el dispositivo 110 terminal y un identificador de un tren de datos creado por el proceso. El identificador del tren de datos es una 5-tupla que incluye una dirección de origen, un puerto de origen, una dirección de destino, un puerto de destino y un identificador de protocolo.

Cada registro en la segunda tabla de correspondencia almacena un identificador de una aplicación y un identificador de un proceso creado por la aplicación. En la presente realización, una aplicación es software de aplicación. Después de ejecutar una aplicación, un OS crea al menos un proceso, y cada proceso implementa una función relativamente independiente. Es decir, una aplicación corresponde a al menos un proceso. Normalmente, un proceso puede crearse y usarse por una aplicación solamente. Solo una cantidad extremadamente pequeña de procesos de sistema puede usarse por múltiples aplicaciones y el presente caso no se toma en cuenta en la presente solicitud. Dichos procesos no se registran en la primera tabla de correspondencia y la segunda tabla de correspondencia.

Por ejemplo, después de que una aplicación nombrada "Sogou input method" se ejecuta, un proceso nombrado "SogouCloud.exe" y un proceso nombrado "SogouSmartInfo.exe" se crean. El proceso nombrado "SogouCloud.exe" se usa para obtener, de un servidor de red, información como, por ejemplo, una biblioteca de fuentes actualizada, y un icono de barra de visualización. El proceso nombrado "SogouSmartInfo.exe" se usa para obtener, del servidor de red, una regla de identificación de asociación inteligente que se usa para predecir, según una palabra deletreada por un usuario, una palabra que se deletreará por el usuario, para mejorar la eficacia de entrada.

Después de que cada proceso se ejecuta, según el diseño del código de programa, no pueden crearse trenes de datos, o uno o más trenes de datos pueden crearse. Es decir, un proceso puede corresponder a uno o más trenes de datos.

El dispositivo 110 terminal recibe el identificador, enviado por el dispositivo de seguridad de red, del primer tren de datos; encuentra, en la primera tabla de correspondencia, un primer registro en el cual el identificador del primer tren de datos se almacena, para obtener un identificador de un proceso en el primer registro; encuentra, en la segunda tabla de correspondencia, un segundo registro en el cual el identificador del proceso en el primer registro se almacena, para obtener un identificador de una aplicación del segundo registro; y envía el identificador de la aplicación al dispositivo de seguridad de red.

A continuación se describe, mediante referencia a la Figura 2A y Figura 2B con referencia a un ejemplo específico, un método para identificar información de aplicación en el tráfico de red provisto en la presente invención. Un dispositivo de seguridad de red provisto en la presente realización puede ser el dispositivo 120 de seguridad de red en la Figura 1A o Figura 1B.

Etapa 201: El dispositivo de seguridad de red encuentra un tren de datos no identificado. De manera específica, cuando lleva a cabo la identificación de aplicación en el tren de datos, el dispositivo de seguridad de red recibe al menos un paquete del tren de datos. Para cada paquete del tren de datos, después de que una característica en el paquete se almacena en caché de forma selectiva según una regla, el paquete se reenvía. Cuando un último paquete que indica que el tren de datos está por finalizar, por ejemplo, un paquete cuyo identificador de estado de paquete es FIN se recibe, o después de que una cantidad especificada de paquetes de un tren de datos se recibe y se reenvía, si una aplicación que envía el tren de datos aún no puede identificarse mediante el uso de una tecnología de identificación de aplicación existente, se determina que el tren de datos es un tren de datos no identificado.

Etapa 202: El dispositivo de seguridad de red obtiene un identificador del tren de datos no identificado. El dispositivo de seguridad de red analiza un paquete de un tren de datos no identificado almacenado en caché para obtener una 5-tupla del paquete, y usa la 5-tupla como el identificador del tren de datos no identificado, donde la 5-tupla incluye una dirección IP de origen, un puerto de origen, una dirección IP de destino, un puerto de destino y un tipo de protocolo. Por ejemplo, la información sobre la 5-tupla obtenida es "tcp 192.168.1.211:3020-201.6.8.30:6682".

Etapa 203: El dispositivo de seguridad de red encapsula un identificador "tcp 192.168.1.211:3020-201.6.8.30:6682" del tren de datos en un paquete P1, y envía el paquete P1 a un dispositivo terminal.

De manera opcional, el dispositivo de seguridad de red puede enviar el identificador "tcp 192.168.1.211:3020-201.6.8.30:6682" del tren de datos a un dispositivo terminal cuya dirección IP es 192.168.1.211, o enviar el identificador "tcp 192.168.1.211:3020-201.6.8.30:6682" del tren de datos a un dispositivo terminal cuya dirección IP es 201.6.8.30, o enviar el identificador "tcp 192.168.1.211:3020-201.6.8.30:6682" del tren de datos a un dispositivo terminal cuya dirección IP es 192.168.1.211 y un dispositivo terminal cuya dirección IP es 201.6.8.30.

Dado que el dispositivo terminal cuya dirección IP es 192.168.1.211 y el dispositivo terminal cuya dirección IP es 201.6.8.30 pueden llevar a cabo etapas de procesamiento similares, en aras de la brevedad, a continuación se usa solamente el dispositivo terminal cuya dirección IP es 192.168.1.211 como un ejemplo para la descripción en la presente realización.

Etapa 204: El dispositivo terminal recibe el paquete P1 enviado por el dispositivo de seguridad de red y analiza el paquete P1 para obtener el identificador "tcp 192.168.1.211:3020-201.6.8.30:6682", llevado en el paquete P1, del tren de datos.

Etapa 205: El dispositivo terminal consulta una primera tabla de correspondencia para un registro en el cual el identificador "tcp 192.168.1.211:3020-201.6.8.30:6682" del tren de datos se almacena; y si el registro se encuentra, lleva a cabo la etapa 206, o si el registro no se encuentra, termina el procesamiento.

Etapa 206: El dispositivo terminal obtiene, del registro encontrado en el cual el identificador "tcp 192.168.1.211:3020-201.6.8.30:6682" del tren de datos se almacena, un identificador SogouCloud.exe que es de un proceso y que corresponde al identificador "tcp 192.168.1.211:3020-201.6.8.30:6682" del tren de datos.

El dispositivo terminal almacena dos tablas de correspondencia. Cada registro en la primera tabla de correspondencia almacena un identificador de un proceso que se ejecuta en el dispositivo terminal y un identificador de un tren de datos creado por el proceso. Cada registro en una segunda tabla de correspondencia almacena un identificador de una aplicación y un identificador de un proceso creado por la aplicación. De manera aparente, el dispositivo terminal puede, de forma alternativa, usar una tabla de correspondencia para almacenar correspondencias entre los tres identificadores: un identificador de una aplicación, un identificador de un proceso creado por la aplicación y un identificador de un tren de datos creado por el proceso. En la presente solicitud, meramente en aras de la conveniencia en la descripción posterior, una correspondencia entre el identificador del proceso y el identificador del tren de datos creado por el proceso se almacena en la primera tabla de correspondencia, y una correspondencia entre el identificador de la aplicación y el identificador del proceso creado por la aplicación se almacena en la segunda tabla de correspondencia. Cuando una tabla de correspondencia consolidada se usa para almacenar las correspondencias anteriores, el identificador de la aplicación se almacena en una primera columna, el identificador del proceso creado por la aplicación se almacena en una segunda columna, y el identificador del tren de datos creado por el proceso se almacena en una tercera columna. En realizaciones posteriores de la presente solicitud, un proceso de consulta de la primera tabla de correspondencia es equivalente a la consulta de la primera columna y la segunda columna de la tabla de correspondencia consolidada, y un proceso de consulta de la segunda tabla de correspondencia en las realizaciones posteriores es equivalente a la consulta de la segunda columna y la tercera columna de la tabla de correspondencia consolidada.

La primera tabla de correspondencia almacenada en el dispositivo terminal se muestra en la Tabla 1. Un proceso en el cual el dispositivo terminal obtiene la primera tabla de correspondencia se describirá posteriormente en detalle con referencia a un diagrama de flujo.

Tabla 1

Identificador de un proceso	Identificador de un tren de datos
SogouCloud.exe	tcp 192.168.1.211:3020-201.6.8.30:6682
	tcp 192.168.1.211:3021-201.6.8.30:6682
	tcp 192.168.1.211:3022-201.6.8.30:6682
SogouSmartInfo.exe	tcp 192.168.1.211:3023-201.6.8.30:6683
	tcp 192.168.1.211:3024-201.6.8.30:6683

Identificador de un proceso	Identificador de un tren de datos
	tcp 192.168.1.211:3025-201.6.8.30:6683
kxescore.exe	tcp 192.168.1.211:6120-168.3.56.120:1138
kxetray.exe	tcp 192.168.1.211:6121-168.3.56.120:1138
	tcp 192.168.1.211:6122-168.3.56.120:1138

El dispositivo terminal descubre, en la Tabla 1, que un registro que incluye el identificador "tcp 192.168.1.211:3020-201.6.8.30:6682" del tren de datos es el registro en la primera fila, y luego obtiene el identificador SogouCloud.exe del proceso en el registro en la primera fila.

Etapa 207: El dispositivo terminal consulta una segunda tabla de correspondencia para un registro en el cual el identificador SogouCloud.exe del proceso se almacena; y si el registro se encuentra, lleva a cabo la etapa 208, o si el registro no se encuentra, termina el procesamiento.

Etapa 208: El dispositivo terminal obtiene, del registro encontrado en el cual el identificador SogouCloud.exe del proceso se almacena, un identificador que es de una aplicación y que corresponde al identificador SogouCloud.exe del proceso. En la presente realización, el identificador puede ser un nombre "Sogou input method" de la aplicación.

La segunda tabla de correspondencia almacenada en el dispositivo terminal se muestra en la Tabla 2. La segunda tabla de correspondencia puede recolectarse por un fabricante de software del agente. El personal de investigación y desarrollo y diseño puede conocer, mediante el uso de un paquete de instalación de software de aplicación, o un cambio de una lista de proceso después de que el software de aplicación se ejecuta, qué procesos comienzan después de que el software de aplicación se ejecuta, para obtener una correspondencia entre un identificador de una aplicación y un identificador de un proceso. En realidad, con el fin de reducir el espacio de almacenamiento del dispositivo terminal y mejorar la eficacia de ejecución, el fabricante de software no necesita recoger todas las correspondencias entre identificadores de aplicaciones e identificadores de procesos, y solo necesita recolectar información sobre procesos que comienzan por una aplicación común que provoca, fácilmente, informes fallidos e informes falsos en un proceso de identificación de una aplicación de tráfico de red. El agente en el dispositivo terminal puede, de manera regular, obtener la segunda tabla de correspondencia de un sitio web de actualización.

Tabla 2

Identificador de una aplicación	Identificador de un proceso
Sogou input method	SogouCloud.exe
	SogouSmartInfo.exe
Huawei Security Guard	kxescore.exe
	kxetray.exe

El dispositivo terminal descubre, en la Tabla 2, que un registro que incluye el identificador SogouCloud.exe del proceso es el registro en la primera fila, y luego obtiene el nombre "Sogou input method" de la aplicación en el registro en la primera fila. Un identificador de una aplicación puede ser en múltiples formas. Para una descripción más visual, la presente realización directamente usa un nombre de una aplicación para representar un identificador de la solicitud. Durante la aplicación práctica, para facilitar el mantenimiento, el fabricante de software normalmente asigna un número a cada aplicación según una regla de asignación prestablecida, y el número se usa para representar un identificador de la aplicación.

Etapa 209: El dispositivo terminal encapsula el nombre encontrado "Sogou input method" de la aplicación en un paquete P2, y envía el paquete P2 al dispositivo de seguridad de red.

Dado que el dispositivo de seguridad de red y el dispositivo terminal pueden llevar a cabo múltiples interacciones en paralelo para identificar aplicaciones de múltiples trenes de datos diferentes, para un procesamiento simple y conveniente por el dispositivo de seguridad de red, el dispositivo terminal puede encapsular, en un mismo paquete, un identificador de un tren de datos y un identificador de una aplicación determinada según el tren de datos, y enviar el paquete al dispositivo de seguridad de red. En el presente ejemplo, el dispositivo terminal encapsula el identificador "tcp 192.168.1.211:3020-201.6.8.30:6682" del tren de datos y el nombre "Sogou input method" de la aplicación en el paquete P2, y envía el paquete P2 al dispositivo de seguridad de red.

Etapa 210: El dispositivo de seguridad de red recibe el paquete P2 enviado por el dispositivo terminal, y analiza el paquete P2 para obtener el identificador "tcp 192.168.1.211:3020-201.6.8.30:6682" del tren de datos y el nombre "Sogou input method" de la aplicación que se llevan en el paquete P2.

Etapa 211: El dispositivo de seguridad de red encuentra un registro correspondiente en una tabla de flujo según el identificador, llevado en P2, del tren de datos, y completa el nombre, llevado en P2, de la aplicación en la tabla como un resultado de identificación.

El dispositivo de seguridad de red mantiene una tabla de flujo. Cada registro en la tabla de flujo corresponde a un tren de datos, y registra información relacionada como, por ejemplo, un estado y un resultado de identificación, del tren de datos. En la presente etapa, el dispositivo de seguridad de red obtiene un registro de identificación "tcp 192.168.1.211:3020-201.6.8.30:6682 Sogou input method".

De manera opcional, después de que el dispositivo de seguridad de red obtiene el registro de identificación en la etapa 211, para reducir múltiples interacciones posteriores entre el dispositivo de seguridad de red y el dispositivo terminal para un tren de datos de un mismo identificador, el dispositivo de seguridad de red puede generar una regla de identificación de asociación.

Etapa 212: El dispositivo de seguridad de red genera una primera regla de identificación de asociación y una segunda regla de identificación de asociación, donde la primera regla de identificación de asociación incluye el identificador de la aplicación, y una 3-tupla que incluye una dirección de destino, un puerto de destino y un identificador de protocolo de un primer tren de datos, y la segunda regla de identificación de asociación incluye el identificador de la aplicación, y una 3-tupla que incluye una dirección de origen, un puerto de origen y el identificador de protocolo del primer tren de datos.

Cuando el dispositivo de seguridad de red posteriormente recibe otro tren de datos, por ejemplo, un segundo tren de datos, si al menos una de una 3-tupla de destino o una 3-tupla de origen del segundo tren de datos es coherente con una 3-tupla incluida en cualquiera de la primera regla de identificación de asociación y la segunda regla de identificación de asociación, el dispositivo de seguridad de red determina que un identificador de una aplicación que envía el segundo tren de datos es un identificador de una aplicación incluida en cualquiera de las reglas de identificación de asociación.

En la presente realización, la primera regla de identificación de asociación es "tcp 201.6.8.30:6682 Sogou input method", y la segunda regla de identificación de asociación es "tcp 192.168.1.211:3020 Sogou input method".

Posteriormente, otro dispositivo terminal envía un segundo tren de datos. Cuando recibe un paquete P3 en el segundo tren de datos, el dispositivo de seguridad de red extrae un identificador "tcp 192.168.1.100:3020-201.6.8.30:6682" del segundo tren de datos y una 3-tupla de destino "tcp 201.6.8.30:6682" del segundo tren de datos según el paquete P3. Dado que la 3-tupla de destino del segundo tren de datos es igual a una 3-tupla en la primera regla de identificación de asociación, el dispositivo de seguridad de red puede directamente determinar, según la primera regla de identificación de asociación sin interacción con el dispositivo terminal nuevamente, que una aplicación que envía el segundo tren de datos es "Sogou input method".

En el sistema para identificar información de aplicación en el tráfico de red provisto en la presente realización de la presente solicitud, cuando recibe un tren de datos, el dispositivo de seguridad de red obtiene un identificador del tren de datos, y envía el identificador del tren de datos al dispositivo terminal. El dispositivo terminal encuentra, en la primera tabla de correspondencia almacenada, un identificador que es de un proceso y que corresponde al identificador del tren de datos no identificado; encuentra un identificador de una aplicación en la segunda tabla de correspondencia, donde el identificador de la aplicación corresponde al identificador que es del proceso y que corresponde al identificador del tren de datos no identificado; y envía el identificador encontrado de la aplicación al dispositivo de seguridad de red. El dispositivo de seguridad de red determina un resultado de identificación de aplicación del tren de datos según una realimentación del dispositivo terminal. En comparación con la técnica anterior, en el sistema anterior, más aplicaciones pueden identificarse por medio de la interacción entre el dispositivo de seguridad de red y el dispositivo terminal, de modo que una proporción del tráfico no identificado en el tráfico total se reduce, y un efecto de identificación de tráfico de red se mejora.

Con referencia a la Figura 3A, el dispositivo terminal en la realización anterior puede obtener la primera tabla de correspondencia que se muestra en la Tabla 1 de la siguiente manera.

Etapa 31: El dispositivo terminal obtiene una lista de procesos.

El dispositivo terminal obtiene, mediante el uso de una interfaz provista por un sistema operativo (sistema operativo, OS, por sus siglas en inglés) que se ejecuta en el dispositivo terminal, la lista de procesos que se ejecutan en el dispositivo terminal. Un "proceso" en la presente solicitud se refiere a una instancia de un programa que se está ejecutando, y es una actividad que se está ejecutando, sobre un conjunto de datos, de un programa que tiene una función independiente particular. Un proceso es una unidad básica para la ejecución dinámica por el OS. En un OS convencional, un proceso no es solo una unidad de asignación de recursos básica, sino que también es una unidad de ejecución básica.

La mayoría de los OS pueden proveer una interfaz de programación de aplicaciones (Interfaz de Programación de Aplicaciones, API, por sus siglas en inglés) o un comando de línea de comandos, para una aplicación o un operador para obtener una lista de procesos que se ejecutan en un dispositivo terminal. Por ejemplo, una lista de procesos que se ejecutan puede obtenerse mediante la invocación de un comando "ps" en un sistema operativo Linux; y una lista de procesos que se ejecutan puede obtenerse mediante la invocación de una función EnumProcesses en un sistema operativo Windows.

Etapa 32: El dispositivo terminal obtiene un identificador de un tren de datos creado por cada proceso.

Para cada proceso en la lista de procesos, el dispositivo terminal obtiene, mediante el uso de una interfaz provista por el OS, una conexión actualmente activa que se establece por el proceso mediante la habilitación de un puerto. Por ejemplo, las conexiones habilitadas por el proceso pueden cruzarse mediante el uso de un sistema de archivo virtual "/proc" en el sistema operativo Linux. En el sistema operativo Windows, todas las correspondencias entre trenes de datos TCP y procesos pueden obtenerse mediante el uso de una función GetExtendedTcpTable, y todas las correspondencias entre trenes de datos UDP y procesos pueden obtenerse mediante el uso de una función GetExtendedUdpTable.

Cada conexión actualmente activa se usa como un tren de datos, y una 5-tupla de la conexión activa se usa como el identificador del tren de datos.

Etapa 33: El dispositivo terminal genera, para cada identificador obtenido de un proceso, un registro que incluye un identificador del proceso y el identificador del tren de datos, y almacena el registro en la primera tabla de correspondencia. Por lo tanto, la primera tabla de correspondencia se obtiene.

De manera opcional, el sistema OS puede crear o abandonar un proceso en cualquier momento según una actividad de uso de un usuario. Con el fin de actualizar y mantener la primera tabla de correspondencia en tiempo real, para mejorar una probabilidad de que el dispositivo terminal encuentre una aplicación correspondiente según un identificador, enviado por el dispositivo de seguridad de red, de un tren de datos no identificado, el dispositivo terminal monitorea un estado del proceso mediante el uso de una función de gancho y, por consiguiente, actualiza el registro en la primera tabla de correspondencia. La Figura 3B-1 y Figura 3B-2 son un diagrama de flujo de un proceso de actualización de la primera tabla de correspondencia según la presente realización.

La etapa 31 a la etapa 33 en la Figura 3B-1 y Figura 3B-2 son similares a aquellas en la Figura 3A. En aras de la brevedad, la descripción no se repite en la presente memoria.

Etapa 34: El dispositivo terminal obtiene, mediante el uso de una función de gancho, un episodio en el que el sistema operativo crea un proceso.

La función de gancho es una parte de un mecanismo de procesamiento de mensajes Windows. Mediante el establecimiento de un "gancho", el agente u otra aplicación pueden filtrar todos los mensajes y episodios a nivel de sistema, y acceder a un mensaje al que no puede accederse en una circunstancia normal. La función de gancho es, esencialmente, un programa usado para procesar mensajes de sistema. La función de gancho se carga en un sistema por medio de la invocación del sistema.

Etapa 35: El dispositivo terminal obtiene un identificador de un proceso recientemente creado del episodio de creación de un proceso. El dispositivo terminal obtiene, mediante el uso de la interfaz provista por el OS, una conexión actualmente activa establecida por el proceso recientemente creado mediante la habilitación de un puerto. Cada conexión actualmente activa se usa como un tren de datos, y una 5-tupla de la conexión actualmente activa se usa como un identificador del tren de datos.

Etapa 36: El dispositivo terminal obtiene un identificador de un tren de datos creado por el proceso recientemente creado, genera un registro que incluye el identificador del proceso recientemente creado y el identificador del tren de datos creado por el proceso recientemente creado, y almacena el registro en la primera tabla de correspondencia.

Etapa 37: El dispositivo terminal obtiene, mediante el uso de la función de gancho, un episodio en el que el sistema operativo abandona un proceso.

Etapa 38: El dispositivo terminal obtiene un identificador de un proceso abandonado del episodio de abandono de un proceso, y elimina, de la primera tabla de correspondencia, un registro que incluye el identificador del proceso abandonado.

De manera opcional, con el fin de actualizar y mantener la primera tabla de correspondencia en tiempo real, el dispositivo terminal puede además monitorear un paquete de red mediante el uso de la función de gancho y, de esta manera, actualizar el registro en la primera tabla de correspondencia, y añadir información sobre un tiempo de creación y un último tiempo de actividad del tren de datos a cada registro. Puede aprenderse de las etapas posteriores de la presente realización que el último tiempo de actividad del tren de datos puede usarse para envejecer el registro en la primera tabla de correspondencia, y el tiempo de creación del tren de datos puede usarse para el análisis de otro propósito, como se muestra en la etapa 39 a la etapa 315.

Etapa 39: El dispositivo terminal obtiene, mediante el uso de la función gancho, un paquete transmitido, que puede ser específicamente un paquete enviado o un paquete recibido. Con el fin de además reducir una cantidad de procesamiento de datos posterior, solo los paquetes cuyo tipo de protocolo es el Protocolo de Control de Transmisión (Protocolo de Control de Transmisión, TCP, por sus siglas en inglés) o el Protocolo de Datagramas de Usuario (Protocolo de Datagramas de Usuario, UDP, por sus siglas en inglés) pueden capturarse.

Etapa 310: El dispositivo terminal analiza el paquete obtenido para obtener un identificador de estado de paquete y un identificador de un tren de datos al cual el paquete pertenece. De manera específica, el identificador de estado en la presente realización es un identificador de estado de un protocolo de capa 4. El protocolo de capa 4 puede obtenerse de un campo de protocolo de un encabezamiento IP del paquete, y puede ser, por ejemplo, el TCP o el UDP. Un identificador de estado del TCP puede obtenerse de un campo de banderas de un encabezamiento TCP del paquete. El identificador de estado puede ser FIN, RST o similares. Para una descripción más detallada del identificador de estado de paquete, es preciso remitirse a un documento RFC como, por ejemplo, RFC 793.

El dispositivo terminal extrae una 5-tupla del paquete obtenido, y usa la 5-tupla extraída como el identificador del tren de datos al cual el paquete pertenece.

Etapa 311: El dispositivo terminal determina si el identificador de estado de paquete del paquete es FIN, y si el identificador de estado de paquete del paquete es FIN, lleva a cabo la etapa 312, o si el identificador de estado de paquete del paquete no es FIN, lleva a cabo la etapa 313.

Etapa 312: Si el identificador de estado de paquete es FIN, eliminar, de la primera tabla de correspondencia, un registro que incluye el identificador del tren de datos al cual el paquete pertenece, y el procesamiento finaliza.

Etapa 313: El dispositivo terminal consulta, según el identificador obtenido del tren de datos, la primera tabla de correspondencia que se muestra en la Tabla 1 para el registro que incluye el identificador del tren de datos. Si el registro se encuentra, ello indica que el paquete pertenece a un tren de datos creado, y la etapa 314 se lleva a cabo. Si el registro no se encuentra, ello indica que el paquete pertenece a un tren de datos recientemente creado, y la etapa 315 se lleva a cabo.

Etapa 314: El dispositivo terminal actualiza, en el registro encontrado, un último tiempo de actividad del tren de datos a un tiempo actual.

En realidad, una manera de eliminar un registro caducado según el último tiempo de actividad del tren de datos y una manera de eliminar un registro según el identificador de estado de paquete FIN son dos maneras de eliminación de registro opcionales que pueden coexistir.

Por ejemplo, un paquete P4 TCP se obtiene mediante el uso de la función de gancho, y una 5-tupla extraída del paquete P4 es "tcp 192.168.1.211:6122-168.3.56.120:1138". Un registro que incluye la 5-tupla "tcp 192.168.1.211:6122-168.3.56.120:1138" y que se encuentra en la Tabla 1 es el noveno registro. Un último tiempo de actividad en el noveno registro se actualiza a un tiempo actual 21:00:3456. Una primera tabla de correspondencia actualizada se muestra en la Tabla 3.

Tabla 3

Identificador de un proceso	Identificador de un tren de datos	Tiempo de creación	Último tiempo de actualización
SogouCloud.exe	tcp 192.168.1.211:3020-201.6.8.30:6682	...	...
	tcp 192.168.1.211:3021-201.6.8.30:6682	...	...

	tcp 192.168.1.211:3022-201.6.8.30:6682	...	...
SogouSmartInfo.exe	tcp 192.168.1.211:3023-201.6.8.30:6683	...	...
	tcp 192.168.1.211:3024-201.6.8.30:6683	...	...
	tcp 192.168.1.211:3025-201.6.8.30:6683	...	...
kxescore.exe	tcp 192.168.1.211:6120-168.3.56.120:1138	...	...
kxetray.exe	tcp 192.168.1.211:6121-168.3.56.120:1138	...	...
	tcp 192.168.1.211:6122-168.3.56.120:1138	...	21:00:3456

Etapa 315: El dispositivo terminal actualiza la primera tabla de correspondencia, encuentra, en una primera tabla de correspondencia actualizada, un registro que incluye el identificador del tren de datos que se obtiene en la etapa 310, y establece un tiempo de creación y un último tiempo de actividad del tren de datos en el registro en el tiempo actual.

Para la mayoría de los OS, un proceso que crea un tren de datos identificado por una 5-tupla no puede encontrarse directamente según la 5-tupla. En el presente caso, el sistema OS necesita actualizar una lista de procesos nuevamente; vuelve a obtener, para cada proceso en una lista de procesos actualizada, todas las conexiones establecidas por el proceso, para obtener una primera tabla de correspondencia actualizada; y luego encuentra, en la primera tabla de correspondencia actualizada según el identificador del tren de datos que se obtiene en la etapa 310, el registro que incluye el identificador del tren de datos que se obtiene en la etapa 310.

Por ejemplo, el dispositivo terminal obtiene un paquete P5 TCP mediante el uso de la función de gancho, y una 5-tupla extraída del paquete P5 es "tcp 192.168.1.211:6123-168.3.56.120:1138". Un registro que incluye la 5-tupla "tcp 192.168.1.211:6123-168.3.56.120:1138" no se encuentra en la Tabla 1, y la primera tabla de correspondencia se actualiza. Como se muestra en la Tabla 4, un registro que incluye la 5-tupla "tcp 192.168.1.211:6123-168.3.56.120:1138" y que se encuentra en la Tabla 4 es el décimo registro, y un tiempo de creación y un último tiempo de actividad en el décimo registro se establecen, ambos, en un tiempo actual 21:01:3456. Una primera tabla de correspondencia actualizada se muestra en la Tabla 4.

Tabla 4

Identificador de un proceso	Identificador de un tren de datos	Tiempo de creación	Último tiempo de actualización
SogouCloud.exe	tcp 192.168.1.211:3020-201.6.8.30:6682	...	...
	tcp 192.168.1.211:3021-201.6.8.30:6682	...	...
	tcp 192.168.1.211:3022-201.6.8.30:6682	...	...
SogouSmartInfo.exe	tcp 192.168.1.211:3023-201.6.8.30:6683	...	...
	tcp 192.168.1.211:3024-201.6.8.30:6683	...	...
	tcp 192.168.1.211:3025-201.6.8.30:6683	...	...
kxescore.exe	tcp 192.168.1.211:6120-168.3.56.120:1138	...	...
kxetray.exe	tcp 192.168.1.211:6121-168.3.56.120:1138	...	...

Identificador de un proceso	Identificador de un tren de datos	Tiempo de creación	Último tiempo de actualización
	tcp 192.168.1.211:6122-168.3.56.120:1138	...	21:00:3456
	tcp 192.168.1.211:6123-168.3.56.120:1138	21:01:3456	21:01:3456

De manera opcional, para reducir el espacio de almacenamiento ocupado por la primera tabla de correspondencia en el dispositivo terminal, el dispositivo terminal puede eliminar, de forma periódica, un registro caducado según un último tiempo de actividad que es de un tren de datos y que se encuentra en la primera tabla de correspondencia. Un registro caducado es un registro en el cual un intervalo de tiempo entre un último tiempo de actividad que es de un tren de datos y que se incluye en el registro caducado y un tiempo actual supera un intervalo de tiempo predeterminado. Es decir, el registro caducado es un registro correspondiente a un tren de datos que está inactivo durante un largo tiempo.

El dispositivo terminal determina si un tiempo predeterminado que se determina según un período de detección se alcanza, y si el tiempo predeterminado se alcanza, ejecuta una tarea de eliminación periódica, es decir, para cada registro en la primera tabla de correspondencia en la Tabla 4, el dispositivo terminal determina si un intervalo de tiempo entre un último tiempo de actividad de un tren de datos y un tiempo actual supera un umbral especificado. Si el intervalo de tiempo supera el umbral especificado, el dispositivo terminal elimina el registro. Si el tiempo predeterminado no se alcanza, el dispositivo terminal regresa a la etapa 301.

Se debe notar que, en la Figura 3B-1 y Figura 3B-2, un primer subprocedimiento que incluye la etapa 31 a la etapa 33, un segundo subprocedimiento que incluye la etapa 34 a la etapa 36, un tercer subprocedimiento que incluye la etapa 37 a la etapa 38, y un cuarto subprocedimiento que incluye la etapa 39 a la etapa 315 son independientes entre sí, y pueden llevarse a cabo de manera opcional. Por ejemplo, solo el primer subprocedimiento y el segundo subprocedimiento pueden llevarse a cabo, o solo el primer subprocedimiento y el tercer subprocedimiento pueden llevarse a cabo.

De manera opcional, según la solución provista en la presente realización, una proporción de tráfico que no puede identificarse en el tráfico total puede reducirse ampliamente por medio de la interacción entre el dispositivo de seguridad de red y el dispositivo terminal. Sin embargo, en comparación con una manera en la técnica anterior en la cual el dispositivo de seguridad de red lleva a cabo la identificación de aplicación según una regla localmente almacenada, la solución provista en la presente realización requiere la interacción entre el dispositivo de seguridad de red y el dispositivo terminal y, en consecuencia, un retardo requerido es relativamente largo, y un recurso de transmisión de red particular se consume. Si múltiples trenes de daos completos enviados por un proceso que envía trenes de datos que no pueden identificarse por el dispositivo de seguridad de red pueden obtenerse, una regla puede obtenerse por medio del análisis manual. Para una regla de identificación basada en las características obtenida por medio del análisis manual, o una regla de identificación heurística, la obtención de múltiples trenes de datos completos enviados por una misma aplicación se esencial. El tren de datos completo se refiere a todos los paquetes de un primer paquete enviado por dos partes de comunicación durante una etapa de negociación de establecimiento de conexión a un último paquete enviado antes de que una conexión se desconecte. Sin embargo, para consideraciones de espacio de almacenamiento y rendimiento, un dispositivo de seguridad de red existente no puede almacenar en caché múltiples paquetes de un tren de datos. Por ejemplo, en una tecnología de identificación basada en las características existente o tecnología de identificación heurística, una característica extraída se almacena en caché normalmente después de que la característica se extrae de un paquete recibido y, de esta manera, se reenvía el paquete. La captura de un tren de datos no identificado completo mediante el uso de una tecnología de captura de paquetes de un dispositivo terminal existente es relativamente difícil, dado que qué tren de datos se capturará no puede determinarse, y es difícil ubicar, de forma correcta, un inicio y un fin de un tren de datos no identificado. Si todos los paquetes enviados y recibidos por un dispositivo terminal dentro de un período bastante largo se almacenan para capturar un tren de datos no identificado, un recurso de almacenamiento y un recurso de procesamiento del dispositivo terminal se ocupan ampliamente. Sin embargo, si se usa una tecnología de captura de paquetes de muestreo, un recurso se guarda, pero una gran parte de los paquetes de datos de un tren de datos se pierden. Ello provoca la extracción de regla difícil o incorrecta. Para este problema, la presente solicitud provee una solución que se muestra en la Figura 4A y Figura 4B. Según la solución, todos los paquetes de un tren de datos enviado por un proceso pueden capturarse en una manera dirigida, y la ocupación de una gran cantidad de recursos en el dispositivo terminal se evita.

De manera opcional, en la Figura 4A y Figura 4B, que se basa en la Figura 2A y Figura 2B, después de la etapa 206, es decir, después de que el dispositivo terminal recibe el paquete P1 enviado por un dispositivo de seguridad de red, y determina que el identificador del proceso que crea el tren de datos cuyo identificador es "tcp 192.168.1.211:3020-201.6.8.30:6682" es SogouCloud.exe, las siguientes etapas además se incluyen.

Etapa 401: El dispositivo terminal establece, en la primera tabla de correspondencia que se muestra en la Tabla 1, una bandera de recolección de paquetes para el proceso SogouCloud.exe. La bandera de recolección de paquetes se usa para ordenar al dispositivo terminal que obtenga y almacene, después de capturar mediante el uso de la interfaz del sistema operativo un paquete transmitido por el proceso, un tren de datos completo posteriormente transmitido por el proceso. A continuación se describe una función de la bandera de recolección de paquetes con referencia a un ejemplo específico. Una primera tabla de correspondencia obtenida después de que la bandera de recolección de paquetes se establece se muestra en la Tabla 5.

Tabla 5

Identificador de un proceso	Bandera de recolección de paquetes	Identificador de un tren de datos
SogouCloud.exe	1	tcp 192.168.1.211:3020-201.6.8.30:6682
		tcp 192.168.1.211:3021-201.6.8.30:6682
		tcp 192.168.1.211:3022-201.6.8.30:6682
SogouSmartInfo.exe		tcp 192.168.1.211:3023-201.6.8.30:6683
		tcp 192.168.1.211:3024-201.6.8.30:6683
		tcp 192.168.1.211:3025-201.6.8.30:6683
kxescore.exe		tcp 192.168.1.211:6120-168.3.56.120:1138
kxetray.exe		tcp 192.168.1.211:6121-168.3.56.120:1138
		tcp 192.168.1.211:6122-168.3.56.120:1138

En la presente realización, que la bandera de recolección de paquetes es 1 se usa como un ejemplo en aras de la descripción. En un proceso de implementación específico, las banderas de recolección de paquetes correspondientes a identificadores de todos los procesos pueden establecerse en "0" cuando la primera tabla de correspondencia se genera inicialmente. Una bandera de recolección de paquetes correspondiente a un identificador de un proceso en un registro encontrado se actualiza a "1" después de la etapa 206. Por cierto, otra manera de establecimiento puede usarse, siempre que un valor de bandera diferente pueda establecerse para el identificador del proceso en el registro encontrado después de la etapa 206.

Etapa 49: El dispositivo terminal obtiene, mediante el uso de la función gancho, un paquete transmitido, que puede ser específicamente un paquete enviado o un paquete recibido. La presente etapa es similar a la etapa 39 en la Figura 3B-1 y Figura 3B-2, y los detalles no se describen en la presente memoria nuevamente.

Etapa 410: El dispositivo terminal extrae un identificador de un tren de datos del paquete obtenido. De manera específica, el dispositivo terminal extrae una 5-tupla del paquete obtenido.

Etapa 411: El dispositivo terminal consulta, según el identificador obtenido del tren de datos, la primera tabla de correspondencia que se muestra en la Tabla 5 para un registro que incluye el identificador del tren de datos. Si el registro se encuentra, el registro puede actualizarse según la etapa 314 en la Figura 3B-1 y Figura 3B-2. Si el registro no se encuentra, ello indica que el paquete pertenece a un tren de datos recientemente creado, y el dispositivo terminal actualiza la primera tabla de correspondencia, y encuentra, en una primera tabla de correspondencia actualizada, un registro que incluye el identificador del tren de datos que se obtiene en la etapa 310.

Por ejemplo, el dispositivo terminal obtiene un paquete P6 TCP mediante el uso de la función de gancho, y una 5-tupla extraída del paquete P6 es "tcp 192.168.1.211:3011-201.6.8.30:6682". Un registro que incluye la 5-tupla "tcp 192.168.1.211:3011-201.6.8.30:6682" no se encuentra en la Tabla 5, y el dispositivo terminal actualiza la primera tabla de correspondencia. Como se muestra en la Tabla 6, un registro que incluye la 5-tupla "tcp 192.168.1.211:3011-201.6.8.30:6682" es el primer registro.

Tabla 6

Identificador de un proceso	Bandera de recolección de paquetes	Identificador de un tren de datos
SogouCloud.exe	1	tcp 192.168.1.211:3011-201.6.8.30:6682
		tcp 192.168.1.211:3020-201.6.8.30:6682
		tcp 192.168.1.211:3021-201.6.8.30:6682
		tcp 192.168.1.211:3022-201.6.8.30:6682
SogouSmartInfo.exe		tcp 192.168.1.211:3023-201.6.8.30:6683
		tcp 192.168.1.211:3024-201.6.8.30:6683
		tcp 192.168.1.211:3025-201.6.8.30:6683
kxescore.exe		tcp 192.168.1.211:6120-168.3.56.120:1138
kxetray.exe		tcp 192.168.1.211:6121-168.3.56.120:1138
		tcp 192.168.1.211:6122-168.3.56.120:1138

Independientemente de si el registro que incluye el identificador del tren de datos se encuentra en la primera tabla de correspondencia, el registro que incluye el identificador del tren de datos puede obtenerse después de la etapa 411. Un identificador de un proceso se obtiene del registro. En la presente realización, el identificador obtenido del proceso es SogouCloud.exe.

Etapa 420: El dispositivo terminal determina si una bandera de recolección de paquetes se establece para el identificador SogouCloud.exe del proceso en el primer registro. Si la bandera de recolección de paquetes se establece para el identificador, la etapa 421 se lleva a cabo. Si la bandera de recolección de paquetes no se establece para el identificador, el procedimiento finaliza.

Etapa 421: El dispositivo terminal retira la bandera de recolección de paquetes, y empieza a llevar a cabo la captura de paquetes en el proceso cuyo identificador es SogouCloud.exe.

Según la presente realización, el dispositivo terminal retira la bandera de recolección de paquetes en la Tabla 6, para obtener la Tabla 7. Un propósito de retirar la bandera de recolección de paquetes es evitar la captura de paquetes a largo plazo para un proceso.

Tabla 7

Identificador de un proceso	Bandera de recolección de paquetes	Identificador de un tren de datos
SogouCloud.exe		tcp 192.168.1.211:3011-201.6.8.30:6682
		tcp 192.168.1.211:3020-201.6.8.30:6682
		tcp 192.168.1.211:3021-201.6.8.30:6682
		tcp 192.168.1.211:3022-201.6.8.30:6682

SogouSmartInfo.exe		tcp 192.168.1.211:3023-201.6.8.30:6683
		tcp 192.168.1.211:3024-201.6.8.30:6683
		tcp 192.168.1.211:3025-201.6.8.30:6683
kxescore.exe		tcp 192.168.1.211:6120-168.3.56.120:1138
kxetray.exe		tcp 192.168.1.211:6121-168.3.56.120:1138
		tcp 192.168.1.211:6122-168.3.56.120:1138

De manera opcional, para evitar además la captura de paquetes a largo plazo para un mismo proceso, un intervalo de tiempo de captura de paquetes puede establecerse. Antes de llevar a cabo la etapa 421, el dispositivo terminal determina si un intervalo de tiempo entre un tiempo actual y un tiempo cuando una acción de captura de paquetes se lleva a cabo previamente en el mismo proceso supera un intervalo de tiempo de captura de paquetes especificado; y si el intervalo de tiempo supera el intervalo de tiempo de captura de paquetes especificado, lleva a cabo la captura de paquetes; o si el intervalo de tiempo no supera el intervalo de tiempo de captura de paquetes especificado, se salta la presente etapa, es decir, se salta, de forma temporal, la retirada de una bandera de captura de paquetes y se salta, de forma temporal, el llevar a cabo la captura de paquetes, y finaliza el procesamiento actual.

Etapa 422: El dispositivo terminal almacena un resultado de captura de paquetes, para facilitar el posterior análisis manual. Cuando implementa, de manera específica, la captura de paquetes en un proceso particular, el dispositivo terminal puede llevar a cabo la captura de paquetes según una política de captura de paquetes especificada. Por ejemplo, el dispositivo terminal finaliza la captura de paquetes después de capturar paquetes de datos que se transmiten por el proceso dentro de un segmento de tiempo prestablecido, o finaliza la captura de paquetes después de que los paquetes de datos que se transmiten por el proceso y que se capturan alcanzan un volumen de datos prestablecido.

Debe notarse en la presente memoria que un método para actualizar la primera tabla de correspondencia que se muestra en la Figura 3B-1 y Figura 3B-2 y un método de captura de paquetes que se muestra en la Figura 4A y Figura 4B pueden llevarse a cabo de forma independiente, o pueden llevarse a cabo en una manera combinada.

Según el anterior método de captura de paquetes provisto en la presente realización, múltiples trenes de datos completos sobre un proceso particular pueden obtenerse en el dispositivo terminal para el análisis manual posterior, para obtener una regla de identificación basada en las características o una regla de identificación heurística. Después de que la regla obtenida se aplica al dispositivo de seguridad de red, un efecto de identificación de aplicación puede mejorarse.

Una realización de la presente solicitud además provee un dispositivo terminal. Como se muestra en la Figura 5A, el dispositivo terminal incluye una memoria 510, un procesador 520 y una interfaz 530 de red, y la memoria 510, el procesador 520 y la interfaz 530 de red se comunican entre sí mediante el uso de un bus 540.

La memoria 510 incluye, pero no se encuentra limitada a, una memoria de acceso aleatorio (RAM, por sus siglas en inglés), una memoria de solo lectura (ROM, por sus siglas en inglés), una memoria de solo lectura programable borrable (EPROM, por sus siglas en inglés, o una memoria flash), o una memoria de solo lectura portátil (CD-ROM, por sus siglas en inglés).

El procesador 520 puede ser una o más unidades de procesamiento centrales (Unidad de Procesamiento Central, CPU, por sus siglas en inglés). Cuando el procesador 520 es una CPU, la CPU puede ser una CPU de un solo núcleo, o puede ser una CPU de múltiples núcleos.

La interfaz 530 de red puede ser una interfaz cableada, por ejemplo, una interfaz de datos distribuida por fibra (Interfaz de Datos Distribuida por Fibra, FDDI, por sus siglas en inglés) o una interfaz Gigabit Ethernet (Gigabit Ethernet, GE); o la interfaz 530 de red puede ser una interfaz inalámbrica. Si el dispositivo terminal es un ordenador personal, la interfaz 530 de red puede ser la anterior interfaz cableada o un módulo de red de área local inalámbrica (Fidelidad Inalámbrica, WiFi, por sus siglas en inglés) basado en IEEE 802.11b. Si el dispositivo terminal es un terminal móvil como, por ejemplo, un teléfono móvil, la interfaz 530 de red puede ser un módulo de hardware que incluye un chip de banda base y una antena RF.

La memoria 510 se configura para almacenar un código de programa, una primera tabla de correspondencia y una segunda tabla de correspondencia. Para definiciones de la primera tabla de correspondencia y segunda tabla de correspondencia, es preciso remitirse a la descripción en la realización anterior. Los detalles no se describen nuevamente en la presente memoria.

La interfaz 530 de red se configura para recibir un identificador, enviado por un dispositivo de seguridad de red, de un primer tren de datos.

El procesador 520 lee el código de programa almacenado en la memoria 510, para llevar a cabo las siguientes etapas:

encontrar, en la primera tabla de correspondencia, un primer registro en el cual el identificador del primer tren de datos se almacena, para obtener un identificador de un proceso en el primer registro; y encontrar, en la segunda tabla de correspondencia, un segundo registro en el cual el identificador del proceso en el primer registro se almacena, para obtener un identificador de una aplicación del segundo registro.

La interfaz 530 de red se configura además para enviar el identificador de la aplicación obtenida por el procesador 520 al dispositivo de seguridad de red.

De manera opcional, el procesador 520 puede obtener la primera tabla de correspondencia y actualizar la primera tabla de correspondencia mediante el uso del método según la Figura 3A y Figura 3B y la descripción relacionada.

De manera opcional, el procesador 520 puede obtener paquetes de un tren de datos completo mediante el uso del método según la Figura 4A y Figura 4B y la descripción relacionada.

Una realización de la presente solicitud además provee un dispositivo terminal, como se muestra en la Figura 5B. El dispositivo terminal incluye un módulo 560 de almacenamiento, un módulo 570 de recepción, un módulo 580 de procesamiento y un módulo 590 de envío. Debe notarse que dichos módulos son módulos lógicos cuyas funciones son relativamente independientes, y pueden generarse después de que una CPU en el dispositivo terminal lee y ejecuta el código de software en una memoria, o pueden implementarse mediante el uso de un componente de hardware.

De manera específica: el módulo 560 de almacenamiento se configura para almacenar una primera tabla de correspondencia y una segunda tabla de correspondencia. La primera tabla de correspondencia almacena una correspondencia entre un identificador de un proceso que se ejecuta en el dispositivo terminal y un identificador de un tren de datos creado por el proceso. La segunda tabla de correspondencia almacena una segunda correspondencia entre un identificador de una aplicación y un identificador de un proceso creado por la aplicación. El identificador del tren de datos es una 5-tupla que incluye una dirección de origen, un puerto de origen, una dirección de destino, un puerto de destino y un identificador de protocolo.

El módulo 570 de recepción se configura para recibir un identificador, enviado por un dispositivo de seguridad de red, de un primer tren de datos.

El módulo 580 de procesamiento se configura para: encontrar, en la primera tabla de correspondencia almacenada en el módulo 560 de almacenamiento, un primer registro en el cual el identificador del primer tren de datos se almacena, para obtener un identificador de un proceso en el primer registro; y encontrar, en la segunda tabla de correspondencia, un segundo registro en el cual el identificador del proceso en el primer registro se almacena, para obtener un identificador de una aplicación del segundo registro.

El módulo 590 de envío se configura para enviar el identificador de la aplicación al dispositivo de seguridad de red.

De manera opcional, el módulo 580 de procesamiento puede obtener la primera tabla de correspondencia y actualizar la primera tabla de correspondencia mediante el uso del método según la Figura 3A y Figura 3B y la descripción relacionada.

De manera opcional, el módulo 580 de procesamiento puede obtener paquetes de un tren de datos completo mediante el uso del método según la Figura 4A y Figura 4B y la descripción relacionada.

El dispositivo terminal provisto en la Figura 5A y Figura 5B puede usarse como el dispositivo 110 terminal en la Figura 1A o la Figura 1B.

Después de recibir el identificador, enviado por el dispositivo de seguridad de red, del tren de datos, el dispositivo terminal provisto en la presente realización de la presente solicitud encuentra el identificador de la aplicación según la primera tabla de correspondencia y la segunda tabla de correspondencia que se almacenan por el dispositivo terminal, y envía el identificador encontrado de la aplicación al dispositivo de seguridad de red. Más aplicaciones pueden identificarse por medio de la interacción entre el dispositivo de seguridad de red y el dispositivo terminal, de

modo que una proporción del tráfico no identificado en el tráfico total se reduce, y un efecto de identificación de tráfico de red se mejora.

Una realización de la presente solicitud además provee un dispositivo de seguridad de red. Como se muestra en la Figura 6A, el dispositivo de seguridad de red incluye una memoria 610, un procesador 620 y una interfaz 630 de red, y la memoria 610, el procesador 620 y la interfaz 630 de red se comunican entre sí mediante el uso de un bus 640.

La memoria 610 incluye, pero no se encuentra limitada a, una memoria de acceso aleatorio (RAM), una memoria de solo lectura (ROM), una memoria de solo lectura programable borrable (EPROM, o una memoria flash), o una memoria de solo lectura portátil (CD-ROM).

El procesador 620 puede ser una o más unidades de procesamiento centrales (Unidad de Procesamiento Central, CPU). Cuando el procesador 620 es una CPU, la CPU puede ser una CPU de un solo núcleo, o puede ser una CPU de múltiples núcleos.

La interfaz 630 de red puede ser una interfaz cableada, por ejemplo, una interfaz de datos distribuida por fibra (Interfaz de Datos Distribuida por Fibra, FDDI) o una interfaz Gigabit Ethernet (Gigabit Ethernet, GE); o la interfaz 630 de red puede ser una interfaz inalámbrica.

La interfaz 630 de red se configura para recibir un primer tren de datos.

El procesador 620 se configura para obtener un identificador del primer tren de datos. El identificador del tren de datos es una 5-tupla que incluye una dirección de origen, un puerto de origen, una dirección de destino, un puerto de destino y un identificador de protocolo.

La interfaz 630 de red se configura además para enviar el identificador del tren de datos al dispositivo terminal según la dirección de origen o la dirección de destino en el identificador del primer tren de datos, donde una dirección del dispositivo terminal es la dirección de origen o la dirección de destino en el identificador del primer tren de datos.

De manera opcional, el procesador 620 ordena, cuando una aplicación que envía el primer tren de datos no puede identificarse mediante el uso de una tecnología de identificación de aplicación existente, a la interfaz 630 de red que envíe el identificador del tren de datos al dispositivo terminal.

La interfaz 630 de red se configura además para recibir un identificador de una aplicación enviada por el dispositivo terminal.

El procesador 620 se configura además para determinar que el identificador de la aplicación recibida por la interfaz 630 de red es el identificador de la aplicación que envía el primer tren de datos, para obtener un resultado de identificación de aplicación del primer tren de datos.

Una realización de la presente solicitud además provee un dispositivo de seguridad de red, como se muestra en la Figura 6B. El dispositivo de seguridad de red incluye un módulo 660 de recepción, un módulo 670 de procesamiento y un módulo 680 de envío. Debe notarse que dichos módulos son módulos lógicos cuyas funciones son relativamente independientes, y pueden generarse después de que una CPU en el dispositivo terminal lee y ejecuta el código de software en una memoria, o pueden implementarse mediante el uso de un componente de hardware. De manera específica:

El módulo 660 de recepción se configura para recibir un primer tren de datos.

El módulo 670 de procesamiento se configura para obtener un identificador del primer tren de datos. El identificador del tren de datos es una 5-tupla que incluye una dirección de origen, un puerto de origen, una dirección de destino, un puerto de destino y un identificador de protocolo.

El módulo 680 de envío se configura para enviar el identificador del tren de datos al dispositivo terminal según la dirección de origen o la dirección de destino en el identificador del primer tren de datos, donde una dirección del dispositivo terminal es la dirección de origen o la dirección de destino en el identificador del primer tren de datos.

De manera opcional, el módulo 670 de procesamiento ordena, cuando una aplicación que envía el primer tren de datos no puede identificarse mediante el uso de una tecnología de identificación de aplicación existente, al módulo 680 de envío que envíe el identificador del tren de datos al dispositivo terminal.

El módulo 660 de recepción se configura además para recibir un identificador de una aplicación enviada por el dispositivo terminal.

El módulo 670 de procesamiento se configura además para determinar que el identificador de la aplicación recibida por el módulo 660 de recepción es el identificador de la aplicación que envía el primer tren de datos, para obtener un resultado de identificación de aplicación del primer tren de datos.

El dispositivo de seguridad de red provisto en la Figura 6A y Figura 6B puede usarse como el dispositivo 120 de seguridad de red en la Figura 1A o la Figura 1B. Para un proceso de interacción entre el dispositivo de seguridad de red provisto en la Figura 6A y Figura 6B y el dispositivo terminal, es preciso remitirse a la Figura 2A y Figura 2B y a la descripción relacionada.

El dispositivo de seguridad de red provisto en la presente realización de la presente solicitud envía, cuando la aplicación que envía el tren de datos no puede identificarse mediante el uso de la tecnología de identificación de aplicación existente, el identificador del tren de datos al dispositivo terminal; recibe el identificador de la aplicación enviada por el dispositivo terminal; y usa el identificador recibido de la aplicación como el identificador de la aplicación que envía el tren de datos, para obtener el resultado de identificación de aplicación del tren de datos. Más aplicaciones pueden identificarse por medio de la interacción entre el dispositivo de seguridad de red y el dispositivo terminal, de modo que una proporción del tráfico no identificado en el tráfico total se reduce, y un efecto de identificación de tráfico de red se mejora.

Realización 2

La Figura 7 es un diagrama esquemático de un sistema para identificar información de aplicación en el tráfico de red según una realización de la presente solicitud. El sistema incluye un dispositivo 710 terminal, un dispositivo 720 de seguridad de red y un dispositivo 730 de procesamiento de datos. En comparación con el sistema de identificación que se muestra en la Figura 1A y Figura 1B, al sistema que se muestra en la Figura 7 se añade el dispositivo 730 de procesamiento de datos. El dispositivo 730 de procesamiento de datos puede usarse como un módulo lógico e integrarse en el dispositivo 720 de seguridad de red o el dispositivo 710 terminal, o puede desplegarse de forma separada como un dispositivo físico independiente siempre que la comunicación separada con el dispositivo 710 terminal y el dispositivo 720 de seguridad de red pueda asegurarse.

En la técnica anterior, para implementar un objetivo de encontrar un resultado de identificación incorrecto de un dispositivo de seguridad de red, solo el tráfico no mixto que solo incluye tráfico generado por una aplicación que se identificará y que no incluye tráfico generado por otra aplicación puede usarse para probar un efecto de identificación, por el dispositivo de seguridad de red, de la aplicación que se identificará. Además, un efecto de identificación en un caso de tráfico mixto no puede estimarse.

Un objetivo principal de añadir el dispositivo 730 de procesamiento de datos en la presente realización es identificar un resultado de identificación incorrecto del dispositivo 720 de seguridad de red mediante el análisis, de manera integral, de la información del dispositivo 710 terminal y de la información del dispositivo 720 de seguridad de red.

En primer lugar, debe notarse que el dispositivo 710 terminal tiene una similitud particular con el dispositivo 110 terminal en la realización 1, y el dispositivo 720 de seguridad de red tiene una similitud particular con el dispositivo 120 de seguridad de red en la realización 1. En aras de la brevedad, una diferencia con respecto a la realización 1 se describe, de manera enfática, en detalle en la presente realización, y el contenido que es similar al contenido en la realización 1 se describe brevemente.

En el sistema de identificación que se muestra en la Figura 7, el dispositivo 720 de seguridad de red se configura para: recibir un primer tren de datos; generar un primer registro de identificación después de determinar un identificador de una aplicación que envía el primer tren de datos, donde el primer registro de identificación incluye un identificador del primer tren de datos y el identificador de la aplicación, y el identificador del tren de datos es una 5-tupla que incluye una dirección de origen, un puerto de origen, una dirección de destino, un puerto de destino y un identificador de protocolo; y enviar el primer registro de identificación al dispositivo de procesamiento de datos. El dispositivo 720 de seguridad de red puede identificar el primer tren de datos mediante el uso de una tecnología de identificación de aplicación existente como, por ejemplo, una tecnología de identificación basada en las características, una tecnología de identificación heurística o una tecnología de identificación de asociación, para determinar el identificador de la aplicación que envía el primer tren de datos.

El dispositivo 710 terminal se configura para: obtener un identificador de un proceso que se ejecuta en el dispositivo terminal y un identificador de un segundo tren de datos creado por el proceso, para generar un segundo registro de identificación, donde el segundo registro de identificación incluye el identificador del segundo tren de datos y el identificador del proceso; obtener una tabla de correspondencia, donde cada registro en la tabla de correspondencia almacena un identificador de una aplicación y un identificador de un proceso creado por la aplicación; y enviar el segundo registro de identificación y la tabla de correspondencia al dispositivo de procesamiento de datos. Se comprende inmediatamente que la tabla de correspondencia en la presente realización es la segunda tabla de correspondencia en la realización 1. Con el fin de mantener la coherencia con un nombre de cada tabla de correspondencia en la realización 1, un nombre de la segunda tabla de correspondencia aún se retiene en la presente realización.

El segundo registro de identificación en la presente realización puede ser un registro en la primera tabla de correspondencia en la realización 1. Para un proceso de obtención de la primera tabla de correspondencia por el dispositivo 710 terminal, es preciso remitirse al contenido relacionado en la realización 1. Después de obtener la

primera tabla de correspondencia, el dispositivo 710 terminal envía, de forma integral, la primera tabla de correspondencia como un archivo al dispositivo 730 de procesamiento de datos, o envía, de forma selectiva, un registro o múltiples registros en la primera tabla de correspondencia al dispositivo 730 de procesamiento de datos. Ello no se encuentra limitado en la presente memoria.

El dispositivo 730 de procesamiento de datos se configura para recibir el primer registro de identificación del dispositivo 720 de seguridad de red, y recibir el segundo registro de identificación y la tabla de correspondencia del dispositivo 710 terminal; si el identificador del primer tren de datos incluido en el primer registro de identificación es igual al identificador del segundo tren de datos incluido en el segundo registro de identificación, consultar si un primer registro de asociación existe en la tabla de correspondencia, donde el primer registro de asociación almacena el identificador de la aplicación incluida en el primer registro de identificación y el identificador del proceso incluido en el segundo registro de identificación; y si el primer registro de asociación no existe, determinar que el primer registro de identificación es un registro de identificación incorrecto.

De manera opcional, después de determinar que el primer registro de identificación es el registro de identificación incorrecto, el dispositivo 730 de procesamiento de datos puede además enviar el identificador del proceso incluido en el segundo registro de identificación al dispositivo 710 terminal, de modo que el dispositivo 710 terminal establece una bandera de captura de paquetes para el identificador del proceso, y posteriormente captura múltiples trenes de datos completos enviados por el proceso representado por el identificador del proceso para llevar a cabo el análisis manual. Para un proceso de captura de paquetes detallado, es preciso remitirse a la Figura 4A y Figura 4B en la realización 1 y a la descripción relacionada. Los detalles no se describen nuevamente en la presente memoria.

De manera opcional, con el fin de reducir la ocupación de un recurso de transmisión entre el dispositivo de procesamiento de datos y el dispositivo de seguridad de red provocado debido a que el dispositivo de seguridad de red posteriormente envía un mismo registro de identificación incorrecto de forma repetida al dispositivo de procesamiento de datos debido a una misma regla de identificación de asociación, el dispositivo de seguridad de red puede añadir un identificador de una manera de identificación al primer registro de identificación enviado al dispositivo de procesamiento de datos. Después de determinar que el registro de identificación incorrecto se provoca por la regla de identificación de asociación, el dispositivo de procesamiento de datos ordena al dispositivo de seguridad de red que elimine una regla de identificación de asociación relacionada. Por lo tanto, un registro de identificación incorrecto posteriormente provocado por un mismo motivo se evita.

De manera específica: el primer registro de identificación del dispositivo 720 de seguridad de red además incluye el identificador de la manera de identificación, donde la manera de identificación incluye identificación de asociación, identificación de características e identificación heurística.

La manera de identificación de asociación significa que el dispositivo 720 de seguridad de red identifica, según las correspondencias entre una dirección IP y un número de puerto de un paquete y la aplicación, una aplicación que envía el paquete. Por ejemplo, el dispositivo 720 de seguridad de red puede obtener, mediante el análisis de un paquete de control en un canal de control FTP, una dirección IP y un número de puerto que se usan por un canal de datos que se creará, y añadir correspondencias entre la dirección IP obtenida y el número de puerto, y un nombre de un cliente FTP como, por ejemplo, FileZilla, a una tabla de asociación. Después de recibir un paquete posterior, el dispositivo 720 de seguridad de red consulta si una dirección IP y un número de puerto llevado en el paquete existen en la tabla de asociación; y si la dirección IP y el número de puerto llevado en el paquete existen en la tabla de asociación, usa FileZilla correspondiente a la dirección IP y al número de puerto que se llevan en el paquete y que se encuentran en la tabla de asociación como una aplicación que envía el paquete.

Cuando el primer registro de identificación además incluye el identificador de la manera de identificación, después de determinar que el primer registro de identificación es un registro de identificación incorrecto, el dispositivo 730 de procesamiento de datos puede además enviar un mensaje de notificación al dispositivo de seguridad de red si el identificador de la manera de identificación en el primer registro de identificación es un identificador de la manera de identificación de asociación. El mensaje de notificación se usa para ordenar al dispositivo de seguridad de red que elimine una primera regla de identificación de asociación, y la primera regla de identificación de asociación incluye el identificador del primer tren de datos incluido en el primer registro de identificación.

En el sistema para identificar información de aplicación en el tráfico de red provisto en la presente realización de la presente solicitud, el dispositivo de procesamiento de datos recibe el primer registro de identificación del dispositivo de seguridad de red, y el segundo registro de identificación y la tabla de correspondencia del dispositivo terminal; si el identificador del primer tren de datos incluido en el primer registro de identificación es igual al identificador del segundo tren de datos incluido en el segundo registro de identificación, consulta si un primer registro de asociación existe en la tabla de correspondencia, donde el primer registro de asociación almacena el identificador de la aplicación incluida en el primer registro de identificación y el identificador del proceso incluido en el segundo registro de identificación; y si el primer registro de asociación no existe, determina que el primer registro de identificación es un registro de identificación incorrecto. El dispositivo de procesamiento de datos puede identificar, mediante comparación de un registro de identificación del dispositivo terminal con el del dispositivo de seguridad de red, un

registro de identificación incorrecto que es del dispositivo de seguridad de red y que es difícil de encontrar mediante el uso de la técnica anterior. Por lo tanto, un efecto de identificación de tráfico de red se mejora.

A continuación se describe, mediante referencia a la Figura 8A-1 a la Figura 8A-3 y a la Figura 8B-1 y Figura 8B-2 y con referencia a un ejemplo específico, un método para identificar información de aplicación en el tráfico de red provisto en una realización. En la presente realización, un dispositivo terminal puede ser el dispositivo 710 terminal en la Figura 7, un dispositivo de seguridad de red puede ser el dispositivo 720 de seguridad de red en la Figura 7, un dispositivo de procesamiento de datos puede ser el dispositivo 730 de procesamiento de datos en la Figura 7.

En la Figura 8A-1 a la Figura 8A-3, el método de identificación provisto en la presente realización se describe en la forma de un diagrama de interacción de secuencias de tiempo detallado.

Etapa 801: Después de recibir un paquete P10 de un primer tren de datos, el dispositivo de seguridad de red lleva a cabo, según una tecnología de identificación de asociación, la identificación de aplicación en el primer tren de datos, para obtener un resultado de identificación, es decir, un primer registro de identificación "tcp 192.168.1.211:3020-201.6.8.30:6682 Storm Codec A".

El primer registro de identificación puede obtenerse después de que el dispositivo de seguridad de red recibe el primer tren de datos y luego identifica el primer tren de datos mediante el uso de una regla obtenida mediante el uso de una tecnología de identificación basada en las características, una tecnología de identificación heurística o una tecnología de identificación de asociación. El dispositivo de seguridad de red puede usar varias tecnologías de identificación existentes de forma sucesiva para identificar el paquete hasta que un resultado de identificación pueda obtenerse. Por ejemplo, el dispositivo de seguridad de red primero usa una regla basada en las características para identificar el paquete; cuando no puede obtenerse ningún resultado de identificación, es decir, una característica en el paquete es incoherente con cualquier característica en la regla basada en las características, usa una regla heurística para identificar el paquete; y cuando no puede obtenerse ningún resultado de identificación, entonces usa una regla de identificación de asociación para intentar identificar el paquete. Por cierto, si el resultado de identificación puede obtenerse cuando el dispositivo de seguridad de red primero usa la regla basada en las características para identificar el paquete, un registro de identificación se genera, y el procesamiento finaliza. Una secuencia de selección de tecnologías de identificación por el dispositivo de seguridad de red no se encuentra, en particular, limitada.

En la presente realización, el primer registro de identificación se identifica por el dispositivo de seguridad de red según una primera regla de identificación de asociación, y la primera regla de identificación de asociación es "tcp 201.6.8.30:6682 Storm Codec". Después de recibir el paquete P10, el dispositivo de seguridad de red obtiene una 3-tupla de destino y una 3-tupla de origen del paquete, combina la 3-tupla de destino o la 3-tupla de origen con la primera regla de identificación de asociación, y si cualquiera de la 3-tupla de destino y una 3-tupla de origen es coherente con una 3-tupla en la primera regla de identificación de asociación, determina que el primer tren de datos al cual el paquete P10 pertenece se envía por Storm Codec en el dispositivo terminal.

En la presente realización, un identificador de una manera de identificación de asociación es A, un identificador de una manera de identificación basada en características es B, y un identificador de una manera de identificación heurística es C.

Etapa 802: El dispositivo de seguridad de red añade el primer registro de identificación "tcp 192.168.1.211:3020-201.6.8.30:6682 Storm Codec A" a un paquete P11, y envía el P11 al dispositivo de procesamiento de datos.

Etapa 803: Después de recibir el paquete P11, el dispositivo de procesamiento de datos analiza el paquete P11, para obtener el primer registro de identificación "tcp 192.168.1.211:3020-201.6.8.30:6682 Storm Codec A" llevado en el paquete P11.

Etapa 804: El dispositivo de procesamiento de datos recibe un segundo registro de identificación "tcp 192.168.1.211:3020-201.6.8.30:6682 SogouCloud.exe" y una segunda tabla de correspondencia del dispositivo terminal.

Debe notarse que el segundo registro de identificación y la segunda tabla de correspondencia pueden enviarse de manera separada. Por ejemplo, la segunda tabla de correspondencia se envía después de que la inicialización del agente en el dispositivo terminal se haya completado, o se envía después de que el agente en el dispositivo terminal detecta que la segunda tabla de correspondencia que se muestra en la Tabla 2 en la realización 1 cambia.

Si el dispositivo terminal se configura para enviar, de manera regular, la primera tabla de correspondencia mantenida que se muestra en la Tabla 1 en la realización 1 como un paquete de archivos integral al dispositivo de procesamiento de datos, el segundo registro de identificación puede ser un registro en la primera tabla de correspondencia enviada por el dispositivo terminal.

De manera alternativa, después de recibir el primer registro de identificación del dispositivo de seguridad de red, el dispositivo de procesamiento de datos puede extraer una 5-tupla del primer registro de identificación, y enviar la 5-tupla al dispositivo terminal, para ordenar al dispositivo terminal que devuelva un registro que incluye la 5-tupla y que se encuentra en la primera tabla de correspondencia al dispositivo de procesamiento de datos.

Una manera específica en la cual el dispositivo terminal envía el segundo registro de identificación al dispositivo de procesamiento de datos no se encuentra limitada en la presente memoria.

Etapa 805: El dispositivo de procesamiento de datos determina que el identificador del primer tren de datos incluido en el primer registro de identificación es igual a un identificador de un segundo tren de datos incluido en el segundo registro de identificación.

De manera específica, si el dispositivo terminal se configura para enviar, de manera regular, la primera tabla de correspondencia mantenida que se muestra en la Tabla 1 en la realización 1 como un paquete de archivos integral al dispositivo de procesamiento de datos, el dispositivo de procesamiento de datos encuentra, en el paquete de archivos integral según la 5-tupla en el primer registro de identificación, un registro que incluye una 5-tupla "tcp 192.168.1.211:3020-201.6.8.30:6682" como el segundo registro de identificación.

Si el dispositivo terminal envía, de manera independiente, el segundo registro de identificación, después de recibir el primer registro de identificación enviado por el dispositivo de seguridad de red, el dispositivo de procesamiento de datos compara el primer registro de identificación con al menos un registro de identificación que se recibe previamente del dispositivo terminal dentro de un segmento de tiempo prestablecido; determina que un registro de identificación que lleva un tren de datos cuyo identificador es igual a un identificador de un tren de datos incluido en el primer registro de identificación existe; y usa el registro de identificación como el segundo registro de identificación.

Etapa 806: El dispositivo de procesamiento de datos consulta si un primer registro de asociación existe en la segunda tabla de correspondencia, donde el primer registro de asociación almacena un identificador de una aplicación incluida en el primer registro de identificación y un identificador de un proceso incluido en el segundo registro de identificación.

Si el primer registro de asociación existe, ello indica que el primer registro de identificación es un registro de identificación correcto, y el dispositivo de procesamiento de datos continúa procesando un registro de identificación siguiente enviado por el dispositivo de seguridad de red; o si el primer registro de asociación no existe, ello indica que el primer registro de identificación es un registro de identificación incorrecto.

De manera específica, el dispositivo de procesamiento de datos determina si un registro de asociación existe en la segunda tabla de correspondencia, donde el registro de asociación almacena el identificador "Storm Codec" de la aplicación en el primer registro de identificación y el identificador "SogouCloud.exe" del proceso en el segundo registro de identificación. En la presente realización, un registro que incluye tanto "Storm Codec" como "SogouCloud.exe" no existe en la segunda tabla de asociación que se muestra en la Tabla 2.

Si el dispositivo de procesamiento de datos determina que un registro de identificación del dispositivo de seguridad de red es un registro de identificación incorrecto, al menos una de la etapa 807, etapa 810 o un subprocedimiento que incluye la etapa 808 a la etapa 809 puede llevarse a cabo. En otras palabras, la etapa 807, etapa 810 o el subprocedimiento que incluye la etapa 808 a la etapa 809 son opcionales, y ello no se encuentra, en particular, limitado en una secuencia de ejecución.

Etapa 807: El dispositivo de procesamiento de datos envía, al dispositivo terminal, un paquete P12 que lleva el identificador "SogouCloud.exe" del proceso incluido en el segundo registro de identificación, de modo que el dispositivo terminal establece una bandera de captura de paquetes para el identificador del proceso, y posteriormente captura múltiples trenes de datos completos enviados por el proceso representado por el identificador del proceso para llevar a cabo el análisis manual. Para un proceso de captura de paquetes detallado, es preciso remitirse a la descripción en la etapa 49 a la etapa 422 en la Figura 4A y Figura 4B.

Etapa 808: El dispositivo de procesamiento de datos determina si un identificador de una manera de identificación llevada en el primer registro de identificación es un identificador de una manera de identificación de asociación; y si el identificador de la manera de identificación llevada en el primer registro de identificación es el identificador de la manera de identificación de asociación, lleva a cabo la etapa 809; o si el identificador de la manera de identificación llevada en el primer registro de identificación no es el identificador de la manera de identificación de asociación, finaliza el procesamiento actual.

Etapa 809: El dispositivo de procesamiento de datos envía un mensaje de notificación P13 al dispositivo de seguridad de red, donde el mensaje de notificación se usa para ordenar al dispositivo de seguridad de red que elimine una primera regla de identificación de asociación "tcp 201.6.8.30:6682 Storm Codec".

De manera específica, el mensaje de notificación puede llevar el identificador del tren de datos incluido en el primer registro de identificación y una instrucción de eliminar, por ejemplo, "201.6.8.30:6682 D", y D es la instrucción de eliminar.

Etapa 810: El dispositivo de procesamiento de datos además cuenta una cantidad de registros de identificación incorrectos, y aumenta una cantidad actual de registros de identificación incorrectos en 1 cada vez después de que un registro de identificación incorrecto se determina.

De manera opcional, cuando se determina que el primer registro de identificación es un registro de identificación correcto en la etapa 806, el dispositivo de procesamiento de datos puede también aumentar una cantidad actual de registros de identificación correctos en 1. De esta manera, una tasa de informes falsos en el segmento de tiempo prestablecido puede calcularse según una cantidad de registros de identificación incorrectos y una cantidad de registros de identificación correctos.

El dispositivo de procesamiento de datos puede además, de forma regular, producir los registros de identificación incorrectos y la tasa de informes falsos mediante el uso de una interfaz de salida, por ejemplo, una pantalla o una impresora, para el análisis por el personal de gestión.

Etapa 811: Después de recibir el mensaje de notificación P13, el dispositivo de seguridad de red elimina la primera regla de identificación de asociación "tcp 201.6.8.30:6682 Storm Codec" o una segunda regla de identificación de asociación "tcp 192.168.1.211:3020 Storm Codec".

De manera opcional, en la etapa 806, después de determinar que el primer registro de identificación es un registro de identificación incorrecto, el dispositivo de procesamiento de datos además genera una regla de identificación de asociación correcta para el dispositivo de seguridad de red, para mejorar un efecto de identificación posterior del dispositivo de seguridad de red. De manera específica:

Etapa 812: El dispositivo de procesamiento de datos consulta si un segundo registro de asociación existe en la tabla de correspondencia, donde el segundo registro de asociación almacena el identificador del proceso incluido en el segundo registro de identificación. Si el segundo registro de asociación existe, la etapa 813 se lleva a cabo. Si el segundo registro de asociación no existe, el procesamiento finaliza.

Etapa 813: El dispositivo de procesamiento de datos genera una tercera regla de identificación de asociación o una cuarta regla de identificación de asociación, donde la tercera regla de identificación de asociación incluye un identificador de una aplicación en el segundo registro de asociación, y una 3-tupla que incluye una dirección de destino, un puerto de destino y un identificador de protocolo del primer tren de datos, y la cuarta regla de identificación de asociación incluye el identificador de la aplicación en el segundo registro de asociación, y una 3-tupla que incluye una dirección de origen, un puerto de origen y el identificador de protocolo del primer tren de datos.

En el presente ejemplo, un registro en una primera fila en la segunda tabla de correspondencia que se muestra en la Tabla 2 incluye "SogouCloud.exe", y un identificador de una aplicación incluida en el registro en la primera fila es "Sogou input method".

La tercera regla de identificación de asociación generada es "tcp 201.6.8.30:6682 Sogou input method", y la cuarta regla de identificación de asociación generada es "tcp 192.168.1.211:3020 Sogou input method".

Etapa 814: El dispositivo de procesamiento de datos envía la tercera regla de identificación de asociación o la cuarta regla de identificación de asociación al dispositivo de seguridad de red.

La Figura 8B-1 y Figura 8B-2 muestran otro diagrama de flujo de un método de identificación ejecutado por un dispositivo de procesamiento de datos. Debe comprenderse que, según la Figura 8A-1 a la Figura 8A-3, la etapa 821 a la etapa 829 en la Figura 8B-1 y Figura 8B-2 son una descripción provista para otros dos registros de identificación enviados por el dispositivo de seguridad de red y el dispositivo terminal.

Etapa 821: Después de recibir un paquete P20 de un tercer tren de datos, el dispositivo de seguridad de red lleva a cabo la identificación de aplicación en el tercer tren de datos según una tecnología de identificación basada en las características existente, y si no puede obtenerse ningún resultado de identificación, genera un tercer registro de identificación "tcp 192.168.1.211:6120-168.3.56.120:1138 Unidentified", donde *Unidentified* es una bandera no identificada y se usa para indicar que el dispositivo de seguridad de red no ha identificado una aplicación que envía el tercer tren de datos.

Etapa 822: El dispositivo de seguridad de red añade el tercer registro de identificación "tcp 192.168.1.211:6120-168.3.56.120:1138 Unidentified" a un paquete P21, y envía el P21 al dispositivo de procesamiento de datos.

Etapa 823: Después de recibir el paquete P21, el dispositivo de procesamiento de datos obtiene el tercer registro de identificación transportado "tcp 192.168.1.211:6120-168.3.56.120:1138 Unidentified" del paquete P21.

Etapa 824: El dispositivo de procesamiento de datos recibe un cuarto registro de identificación "tcp 192.168.1.211:6120-168.3.56.120:1138 kxescore.exe" del dispositivo terminal.

En la presente memoria, se supone que la segunda tabla de correspondencia que se muestra en la Tabla 2 ya se encuentra almacenada en el dispositivo de procesamiento de datos.

Etapa 825: El dispositivo de procesamiento de datos determina que un identificador del tercer tren de datos incluido en el tercer registro de identificación es igual a un identificador de un cuarto tren de datos incluido en el cuarto registro de identificación.

Etapa 826: El dispositivo de procesamiento de datos consulta si un tercer registro de asociación existe en la segunda tabla de correspondencia, donde el tercer registro de asociación almacena un identificador de un proceso incluido en el cuarto registro de identificación.

Si el tercer registro de asociación existe, ya sea de un subprocedimiento que incluye la etapa 827 a la etapa 828 y un subprocedimiento que incluye la etapa 829 a la etapa 830 puede seleccionarse para la ejecución.

En la presente realización, un tercer registro en la Tabla 2 es "kxescore.exe".

Etapa 827: El dispositivo de procesamiento de datos genera una quinta regla de identificación de asociación o una sexta regla de identificación de asociación, donde la quinta regla de identificación de asociación incluye un identificador de una aplicación incluida en un tercer registro de asociación, y una 3-tupla que incluye una dirección de destino, un puerto de destino y un identificador de protocolo del tercer tren de datos, y la sexta regla de identificación de asociación incluye el identificador de una aplicación en el tercer registro de asociación, y una 3-tupla que incluye una dirección de origen, un puerto de origen y el identificador de protocolo del tercer tren de datos.

En la presente realización, la quinta regla de identificación de asociación es "tcp 168.3.56.120:1138 Huawei Security Guard", y la sexta regla de identificación de asociación es "tcp 192.168.1.211:6120 Huawei Security Guard".

Etapa 828: El dispositivo de procesamiento de datos envía la quinta regla de identificación de asociación o la sexta regla de identificación de asociación al dispositivo de seguridad de red.

Etapa 829: El dispositivo de procesamiento de datos añade el identificador del tercer tren de datos y el identificador de la aplicación incluida en el tercer registro de asociación a un paquete 22, y envía el paquete P22 al dispositivo de seguridad de red.

Etapa 830: Después de recibir el paquete P22, el dispositivo de seguridad de red genera la quinta regla de identificación de asociación o la sexta regla de identificación de asociación según el paquete P22.

La quinta regla de identificación de asociación incluye el identificador de la aplicación llevada en el paquete P22, y una 3-tupla que incluye la dirección de destino, el puerto de destino y el identificador de protocolo del tercer tren de datos y que se lleva en el paquete P22. La sexta regla de identificación de asociación incluye el identificador de la aplicación llevada en el paquete P22, y la 3-tupla que incluye la dirección de origen, el puerto de origen y el identificador de protocolo del tercer tren de datos.

Debe notarse, en la presente memoria, que, en una manera de generación de una nueva regla de identificación de asociación según un registro de identificación, como se muestra en la etapa 212 en la Figura 2A y Figura 2B en la realización 1, la etapa 813 en la Figura 8A-1 a la Figura 8A-3 en la realización 2, y la etapa 827 a la etapa 828, o la etapa 829 a la etapa 830 en la Figura 8B-1 y Figura 8B-2 en la realización 2, con el fin de reducir, en una implementación específica, una probabilidad de identificación incorrecta posteriormente generada debido a una regla de identificación de asociación, una regla de identificación de asociación puede generarse según múltiples registros de identificación que tienen una similitud particular, en lugar de generar la regla de identificación de asociación inmediatamente después de que un registro de identificación se obtiene.

Por ejemplo, cuando se determina un registro de identificación correcto en la etapa 826, el dispositivo de procesamiento de datos genera y almacena una regla de identificación de asociación temporal, y establece un valor de recuento para cada regla de identificación de asociación temporal, como se muestra en la Tabla 8.

Tabla 8

Número de serie	Regla de identificación de asociación temporal	Valor de recuento
1	tcp 168.3.56.120:1138 Huawei Security Guard	1
2	tcp 192.168.1.211:6120 Huawei Security Guard	1

Número de serie	Regla de identificación de asociación temporal	Valor de recuento
3	...	...

Cuando el dispositivo de procesamiento de datos lleva a cabo, posteriormente, el procedimiento que se muestra en la Figura 8B-1 y Figura 8B-2 nuevamente para generar otra regla de identificación de asociación temporal, y almacena la regla de identificación de asociación temporal en la Tabla 8, el dispositivo de procesamiento de datos primero consulta si una misma regla de identificación de asociación temporal existe en la Tabla 8; y si la misma regla de identificación de asociación temporal existe, aumenta un valor de recuento correspondiente a la regla de identificación de asociación temporal en 1; o si la misma regla de identificación de asociación temporal no existe, añade un nuevo registro a la Tabla 8, y establece un valor de recuento en 1.

El dispositivo de procesamiento de datos establece un umbral, por ejemplo, 10. Cuando un valor de recuento de un registro en la Tabla 8 supera el umbral, ello indica que la regla de identificación de asociación temporal tiene universalidad, y la regla de identificación de asociación temporal se usa entonces como una regla de identificación de asociación formal que puede usarse por el dispositivo de seguridad de red para llevar a cabo la identificación de aplicación en un tren de datos posteriormente recibido.

En el método para identificar la información de aplicación en el tráfico de red provisto en la presente realización de la presente solicitud, el dispositivo de procesamiento de datos recibe el primer registro de identificación del dispositivo de seguridad de red, y el segundo registro de identificación y la tabla de correspondencia del dispositivo terminal; si el identificador del primer tren de datos incluido en el primer registro de identificación es igual al identificador del segundo tren de datos incluido en el segundo registro de identificación, consulta si un registro de asociación existe en la tabla de correspondencia, donde el registro de asociación almacena el identificador de la aplicación incluida en el primer registro de identificación y el identificador del proceso incluido en el segundo registro de identificación; y si el registro de asociación no existe, determina que el primer registro de identificación es un registro de identificación incorrecto. Según el proceso anterior, el registro de identificación incorrecto del dispositivo de seguridad de red puede encontrarse, y un efecto de identificación de aplicación puede mejorarse.

Una realización de la presente solicitud además provee un dispositivo de procesamiento de datos, como se muestra en la Figura 9A. El dispositivo de procesamiento de datos incluye una memoria 910, un procesador 920 y una interfaz 930 de red, y la memoria 910, el procesador 920 y la interfaz 930 de red se comunican entre sí mediante el uso de un bus 940.

La memoria 910 incluye, pero no se encuentra limitada a, una memoria de acceso aleatorio (RAM), una memoria de solo lectura (ROM), una memoria de solo lectura programable borrable (EPROM, o una memoria flash), o una memoria de solo lectura portátil (CD-ROM).

El procesador 920 puede ser una o más unidades de procesamiento centrales (Unidad de Procesamiento Central, CPU). Cuando el procesador 920 es una CPU, la CPU puede ser una CPU de un solo núcleo, o puede ser una CPU de múltiples núcleos.

La interfaz 930 de red puede ser una interfaz cableada, por ejemplo, una interfaz de datos distribuida por fibra (Interfaz de Datos Distribuida por Fibra, FDDI) o una interfaz Gigabit Ethernet (Gigabit Ethernet, GE); o la interfaz 930 de red puede ser una interfaz inalámbrica.

La interfaz 930 de red se configura para recibir un primer registro de identificación de un dispositivo de seguridad de red, donde el primer registro de identificación incluye un identificador de un primer tren de datos y un identificador de una aplicación; y recibir un segundo registro de identificación y una tabla de correspondencia de un dispositivo terminal, donde el segundo registro de identificación incluye un identificador de un segundo tren de datos y un identificador de un proceso, y cada registro en la tabla de correspondencia almacena un identificador de una aplicación y un identificador de un proceso creado por la aplicación.

El procesador 920 lee el código de programa almacenado en la memoria 910, para llevar a cabo las siguientes etapas:

si el identificador del primer tren de datos incluido en el primer registro de identificación es igual al identificador del segundo tren de datos incluido en el segundo registro de identificación, consultar si un primer registro de asociación existe en la tabla de correspondencia, donde el primer registro de asociación almacena el identificador de la aplicación incluida en el primer registro de identificación y un identificador del proceso incluido en el segundo registro de identificación; y si el primer registro de asociación no existe, determinar que el primer registro de identificación es un registro de identificación incorrecto.

De manera opcional, la interfaz 930 de red se configura además para: si un identificador de una manera de identificación en el primer registro de identificación es un identificador de una manera de identificación de asociación, cuando el primer registro de asociación no existe, enviar un mensaje de notificación al dispositivo de seguridad de red, donde el mensaje de notificación se usa para ordenar al dispositivo de seguridad de red que elimine una primera regla de identificación de asociación o una segunda regla de identificación de asociación, la primera regla de identificación de asociación incluye una 3-tupla que incluye una dirección de destino, un puerto de destino y un identificador de protocolo del primer tren de datos, y la segunda regla de identificación de asociación incluye una 3-tupla que incluye una dirección de origen, un puerto de origen y el identificador de protocolo del primer tren de datos.

El dispositivo de procesamiento de datos puede además interactuar con el dispositivo de seguridad de red y el dispositivo terminal, para identificar el tráfico que no puede identificarse en la técnica anterior. De manera opcional, la interfaz 930 de red se configura además para: recibir un tercer registro de identificación del dispositivo de seguridad de red, donde el tercer registro de identificación incluye un identificador de un tercer tren de datos y una bandera no identificada, y la bandera no identificada se usa para indicar que el dispositivo de seguridad de red no ha identificado una aplicación que envía el tercer tren de datos; y recibir un cuarto registro de identificación del dispositivo terminal, donde el cuarto registro de identificación incluye un identificador de un cuarto tren de datos y un identificador de un proceso.

El procesador 920 se configura además para: determinar si el identificador del tercer tren de datos incluido en el tercer registro de identificación es igual al identificador del cuarto tren de datos incluido en el cuarto registro de identificación; y si el identificador del tercer tren de datos incluido en el tercer registro de identificación es igual al identificador del cuarto tren de datos incluido en el cuarto registro de identificación, consultar si un tercer registro de asociación existe en la tabla de correspondencia, donde el tercer registro de asociación almacena el identificador del proceso incluido en el cuarto registro de identificación.

La interfaz 930 de red se configura además para: si el procesador determina que el tercer registro de asociación existe, enviar un identificador de una aplicación incluida en el tercer registro de asociación y el identificador del tercer tren de datos al dispositivo de seguridad de red.

Una realización de la presente solicitud además provee un dispositivo de procesamiento de datos, como se muestra en la Figura 9B. El dispositivo de procesamiento de datos incluye un módulo 970 de recepción y un módulo 980 de procesamiento. Debe notarse que dichos módulos son módulos lógicos cuyas funciones son relativamente independientes, y pueden generarse después de que una CPU en el dispositivo de procesamiento de datos lee y ejecuta el código de software en una memoria, o pueden implementarse mediante el uso de un componente de hardware.

De manera específica:

El módulo 970 de recepción se configura para recibir un primer registro de identificación de un dispositivo de seguridad de red, donde el primer registro de identificación incluye un identificador de un primer tren de datos y un identificador de una aplicación; y recibir un segundo registro de identificación y una tabla de correspondencia de un dispositivo terminal, donde el segundo registro de identificación incluye un identificador de un segundo tren de datos y un identificador de un proceso, y cada registro en la tabla de correspondencia almacena un identificador de una aplicación y un identificador de un proceso creado por la aplicación.

El módulo 980 de procesamiento se configura para: si el identificador del primer tren de datos incluido en el primer registro de identificación recibido por el módulo 970 de recepción es igual al identificador del segundo tren de datos incluido en el segundo registro de identificación recibido por el módulo 970 de recepción, consultar si un primer registro de asociación existe en la tabla de correspondencia, donde el primer registro de asociación almacena el identificador de la aplicación incluida en el primer registro de identificación y el identificador del proceso incluido en el segundo registro de identificación; y si el primer registro de asociación no existe, determinar que el primer registro de identificación es un registro de identificación incorrecto.

De manera opcional, el dispositivo de procesamiento de datos que se muestra en la Figura 9B además incluye un módulo 990 de envío, configurado para: si un identificador de una manera de identificación en el primer registro de identificación es un identificador de una manera de identificación de asociación, cuando el primer registro de asociación no existe, enviar un mensaje de notificación al dispositivo de seguridad de red, donde el mensaje de notificación se usa para ordenar al dispositivo de seguridad de red que elimine una primera regla de identificación de asociación o una segunda regla de identificación de asociación, la primera regla de identificación de asociación incluye una 3-tupla que incluye una dirección de destino, un puerto de destino y un identificador de protocolo del primer tren de datos, y la segunda regla de identificación de asociación incluye una 3-tupla que incluye una dirección de origen, un puerto de origen y el identificador de protocolo del primer tren de datos.

El dispositivo de procesamiento de datos puede además interactuar con el dispositivo de seguridad de red y el dispositivo terminal, para identificar el tráfico que no puede identificarse en la técnica anterior. De manera opcional, el módulo 970 de recepción se configura además para: recibir un tercer registro de identificación del dispositivo de

seguridad de red, donde el tercer registro de identificación incluye un identificador de un tercer tren de datos y una bandera no identificada, y la bandera no identificada se usa para indicar que el dispositivo de seguridad de red no ha identificado una aplicación que envía el tercer tren de datos; y recibir un cuarto registro de identificación del dispositivo terminal, donde el cuarto registro de identificación incluye un identificador de un cuarto tren de datos y un identificador de un proceso.

El módulo 980 de procesamiento e configura además para: determinar si el identificador del tercer tren de datos incluido en el tercer registro de identificación es igual al identificador del cuarto tren de datos incluido en el cuarto registro de identificación; y si el identificador del tercer tren de datos incluido en el tercer registro de identificación es igual al identificador del cuarto tren de datos incluido en el cuarto registro de identificación, consultar si un tercer registro de asociación existe en la tabla de correspondencia, donde el tercer registro de asociación almacena el identificador del proceso incluido en el cuarto registro de identificación.

El módulo 990 de envío se configura además para: si el módulo 980 de procesamiento determina que el tercer registro de asociación existe, enviar un identificador de una aplicación incluida en el tercer registro de asociación y el identificador del tercer tren de datos al dispositivo de seguridad de red.

El dispositivo de procesamiento de datos provisto en la Figura 9A y 9B puede usarse como el dispositivo 730 de procesamiento de datos en la Figura 7.

Para otras funciones adicionales del dispositivo de procesamiento de datos y de un proceso detallado de interacción entre el dispositivo de seguridad de red y el dispositivo terminal, es preciso remitirse a la Figura 8A-1 a la Figura 8A-3 y a la Figura 8B-1 y Figura 8B-2, y a la descripción relacionada. Los detalles no se describen nuevamente en la presente memoria.

El dispositivo de procesamiento de datos provisto en la presente realización de la presente solicitud recibe el primer registro de identificación del dispositivo de seguridad de red, y el segundo registro de identificación y la tabla de correspondencia del dispositivo terminal; si el identificador del primer tren de datos incluido en el primer registro de identificación es igual al identificador del segundo tren de datos incluido en el segundo registro de identificación, consulta si un registro de asociación existe en la tabla de correspondencia, donde el registro de asociación almacena el identificador de la aplicación incluida en el primer registro de identificación y el identificador del proceso incluido en el segundo registro de identificación; y si el registro de asociación no existe, determina que el primer registro de identificación es un registro de identificación incorrecto. Según el proceso anterior, el registro de identificación incorrecto del dispositivo de seguridad de red puede encontrarse, y un efecto de identificación de aplicación puede mejorarse.

De manera obvia, una persona con experiencia en la técnica puede realizar varias modificaciones y variaciones en la presente invención sin apartarse del alcance de la presente invención. Por lo tanto, la presente invención se interpretará como una que incluye dichas modificaciones y variaciones, siempre que dichas modificaciones y variaciones caigan dentro del alcance de las reivindicaciones de la presente invención.

REIVINDICACIONES

1. Un método para identificar información de aplicación en el tráfico de red, en donde el método se ejecuta por un dispositivo terminal; una primera tabla de correspondencia en el dispositivo terminal almacena, en una forma de registro, una correspondencia entre un identificador de un proceso que se ejecuta en el dispositivo terminal y un identificador de un tren de datos creado por el proceso; una segunda tabla de correspondencia en el dispositivo terminal almacena, en una forma de registro, una correspondencia entre un identificador de una aplicación y un identificador de un proceso creado por la aplicación; y el identificador del tren de datos es una 5-tupla que comprende una dirección de origen, un puerto de origen, una dirección de destino, un puerto de destino y un identificador de protocolo; y

el método comprende:

recibir (204) un identificador, enviado por un dispositivo de seguridad de red, de un primer tren de datos;

consultar (205), en la primera tabla de correspondencia, un primer registro en el cual el identificador del primer tren de datos se almacena;

si el primer registro se encuentra, obtener (206) un identificador de un proceso en el primer registro, y consultar (207), en la segunda tabla de correspondencia, un segundo registro en el cual el identificador del proceso en el primer registro se almacena;

si el segundo registro se encuentra, obtener (208) un identificador de una aplicación del segundo registro, y enviar (209) el identificador de la aplicación al dispositivo de seguridad de red.

2. El método según la reivindicación 1, en donde el dispositivo terminal obtiene la primera tabla de correspondencia mediante el uso de las siguientes etapas:

obtener (31), por el dispositivo terminal mediante el uso de una interfaz provista por un sistema operativo, un identificador de al menos un proceso que se ejecuta en el dispositivo terminal; y

para cada identificador obtenido de un proceso, obtener (32), por el dispositivo terminal, un identificador de un tren de datos creado por el proceso, generar (33) un registro que comprende el identificador del proceso y el identificador del tren de datos, y almacenar el registro en la primera tabla de correspondencia.

3. El método según la reivindicación 1 o 2, en donde el dispositivo terminal obtiene la primera tabla de correspondencia mediante el uso de las siguientes etapas:

obtener (34), por el dispositivo terminal mediante el uso de una función de gancho, un episodio en el que el sistema operativo crea un proceso;

obtener (35) un identificador del proceso recientemente creado del episodio de creación de un proceso; y

obtener (36) un identificador de un tren de datos creado por el proceso recientemente creado, generar un registro que comprende el identificador del proceso recientemente creado y el identificador del tren de datos creado por el proceso recientemente creado, y almacenar el registro en la primera tabla de correspondencia; y

el dispositivo terminal obtiene la primera tabla de correspondencia que además comprende:

obtener (37), por el dispositivo terminal mediante el uso de la función de gancho, un episodio en el que el sistema operativo abandona un proceso; y

obtener (38) un identificador del proceso abandonado del episodio de abandono de un proceso, y eliminar, de la primera tabla de correspondencia, un registro que comprende el identificador del proceso abandonado.

4. El método según cualquiera de las reivindicaciones 1 a 3, en donde un registro en la primera tabla de correspondencia además comprende un último tiempo de actividad de un tren de datos; y el método además comprende:

determinar, por el dispositivo terminal, un registro caducado en la primera tabla de correspondencia, en donde el registro caducado es un registro en el cual un intervalo de tiempo entre un último tiempo de actividad que es de un tren de datos y que está comprendido en el registro caducado y un tiempo actual supera un intervalo de tiempo predeterminado; y

eliminar el registro caducado.

5. El método según la reivindicación 4, en donde después de que el dispositivo terminal obtiene la primera tabla de correspondencia, el método además comprende:

obtener (39), por el dispositivo terminal mediante el uso de la función de gancho, un paquete transmitido por el dispositivo terminal;

obtener (310), del paquete obtenido, un identificador de un tren de datos al cual el paquete pertenece; y

actualizar (314) un último tiempo de actividad de un tren de datos en un registro que se encuentra en la primera tabla de correspondencia y que comprende el identificador del tren de datos al cual el paquete pertenece al tiempo actual.

6. El método según cualquiera de las reivindicaciones 1 a 3, en donde después de que el dispositivo terminal obtiene la primera tabla de correspondencia, el método además comprende:

obtener (39), por el dispositivo terminal mediante el uso de la función de gancho, un paquete transmitido por el dispositivo terminal;

obtener (310), del paquete obtenido, un identificador de estado de paquete y un identificador de un tren de datos al cual el paquete pertenece; y

si el identificador de estado de paquete es FIN, eliminar (312), de la primera tabla de correspondencia, un registro que comprende el identificador del tren de datos al cual el paquete pertenece.

7. Un dispositivo terminal, en donde el dispositivo terminal comprende una memoria (510), un procesador (520) y una interfaz (530) de red, y la memoria (510), el procesador (520) y la interfaz (530) de red se comunican entre sí mediante el uso de un bus (540);

la memoria (510) se configura para almacenar un código de programa, una primera tabla de correspondencia, y una segunda tabla de correspondencia, en donde la primera tabla de correspondencia almacena, en una forma de registro, una correspondencia entre un identificador de un proceso que se ejecuta en el dispositivo terminal y un identificador de un tren de datos creado por el proceso, la segunda tabla de correspondencia almacena, en una forma de registro, una correspondencia entre un identificador de una aplicación y un identificador de un proceso creado por la aplicación, y el identificador del tren de datos es una 5-tupla que comprende una dirección de origen, un puerto de origen, una dirección de destino, un puerto de destino, y un identificador de protocolo;

la interfaz (530) de red se configura para recibir un identificador, enviado por un dispositivo de seguridad de red, de un primer tren de datos;

el procesador (520) se adapta para consultar, en la primera tabla de correspondencia, un primer registro en el cual el identificador del primer tren de datos se almacena; si el primer registro se encuentra, obtener un identificador de un proceso en el primer registro, y consultar, en la segunda tabla de correspondencia, un segundo registro en el cual el identificador del proceso en el primer registro se almacena; si el segundo registro se encuentra, obtener un identificador de una aplicación del segundo registro; y

la interfaz (530) de red se configura además para, si el segundo registro se encuentra, enviar el identificador de la aplicación obtenida por el procesador (520) al dispositivo de seguridad de red.

8. El dispositivo terminal según la reivindicación 7, en donde

el procesador (520) se configura además para obtener la primera tabla de correspondencia mediante el uso de las siguientes operaciones: obtener, mediante el uso de una interfaz provista por un sistema operativo, un identificador de al menos un proceso que se ejecuta en el dispositivo terminal; y para cada identificador obtenido de un proceso, obtener, por el dispositivo terminal, un identificador de un tren de datos creado por el proceso, generar un registro que comprende el identificador del proceso y el identificador del tren de datos, y almacenar el registro en la primera tabla de correspondencia.

9. El dispositivo terminal según la reivindicación 7 u 8, en donde

el procesador (520) se configura además para obtener la primera tabla de correspondencia mediante el uso de las siguientes operaciones:

obtener, mediante el uso de una función de gancho, un episodio en el que el sistema operativo crea un proceso;

obtener un identificador del proceso recientemente creado del episodio de creación de un proceso;

y obtener un identificador de un tren de datos creado por el proceso recientemente creado, generar un registro que comprende el identificador del proceso recientemente creado y el identificador del tren de datos creado por el proceso recientemente creado, y almacenar el registro en la primera tabla de correspondencia; y

obtener, mediante el uso de la función de gancho, un episodio en el que el sistema operativo abandona un proceso;

y obtener un identificador del proceso abandonado del episodio de abandono de un proceso, y eliminar, de la primera tabla de correspondencia, un registro que comprende el identificador del proceso abandonado.

10. El dispositivo terminal según cualquiera de las reivindicaciones 7 a 9, en donde un registro en la primera tabla de correspondencia además comprende un último tiempo de actividad de un tren de datos; y

el procesador (520) se configura además para: determinar un registro caducado en la primera tabla de correspondencia, en donde el registro caducado es un registro en el cual un intervalo de tiempo entre un último tiempo de actividad que es de un tren de datos y que está comprendido en el registro caducado y un tiempo actual supera un intervalo de tiempo predeterminado; y eliminar el registro caducado.

11. El dispositivo terminal según la reivindicación 10, en donde

el procesador (520) se configura además para: después de obtener la primera tabla de correspondencia, obtener, por el dispositivo terminal mediante el uso de la función de gancho, un paquete transmitido por el dispositivo terminal;

obtener, del paquete obtenido, un identificador de un tren de datos al cual el paquete pertenece; y

actualizar un último tiempo de actividad de un tren de datos en un registro que se encuentra en la primera tabla de correspondencia y que comprende el identificador del tren de datos al cual el paquete pertenece al tiempo actual.

12. El dispositivo terminal según cualquiera de las reivindicaciones 7 a 9, en donde

el procesador (520) se configura además para: después de obtener la primera tabla de correspondencia, obtener, por el dispositivo terminal mediante el uso de la función de gancho, un paquete transmitido por el dispositivo terminal;

obtener, del paquete obtenido, un identificador de estado de paquete y un identificador de un tren de datos al cual el paquete pertenece; y

si el identificador de estado de paquete es FIN, eliminar, de la primera tabla de correspondencia, un registro que comprende el identificador del tren de datos al cual el paquete pertenece.

13. Un sistema para identificar información de aplicación en el tráfico de red, que comprende un dispositivo (120) de seguridad de red y un dispositivo (110) terminal, en donde

el dispositivo (120) de seguridad de red se configura para: recibir un primer tren de datos, y obtener un identificador del primer tren de datos, en donde el identificador del primer tren de datos es una 5-tupla que comprende una dirección de origen, un puerto de origen, una dirección de destino, un puerto de destino, y un identificador de protocolo; enviar el identificador del primer tren de datos al dispositivo (110) terminal según la dirección de origen o la dirección de destino en el identificador del primer tren de datos, en donde una dirección del dispositivo (110) terminal es la dirección de origen o la dirección de destino en el identificador del primer tren de datos; recibir un identificador de una aplicación enviada por el dispositivo (110) terminal; y determinar que el identificador recibido de la aplicación es un identificador de una aplicación que envía el primer tren de datos;

el dispositivo (110) terminal se configura para almacenar una primera tabla de correspondencia y una segunda tabla de correspondencia, en donde la primera tabla de correspondencia almacena, en una forma de registro, una correspondencia entre un identificador de un proceso que se ejecuta en el dispositivo (110) terminal y un identificador de un tren de datos creado por el proceso, la segunda tabla de correspondencia almacena, en una forma de registro, una segunda correspondencia entre un identificador de una aplicación y un identificador de un proceso creado por la aplicación, y el identificador del tren de datos es una 5-tupla que comprende una dirección de origen, un puerto de origen, una dirección de destino, un puerto de destino, y un identificador de protocolo; y

el dispositivo (110) terminal se configura para: recibir el identificador, enviado por el dispositivo (120) de seguridad de red, del primer tren de datos; consultar, en la primera tabla de correspondencia, un primer registro en el cual el identificador del primer tren de datos se almacena; si el primer registro se encuentra, obtener un identificador de un proceso en el primer registro, y consultar, en la segunda tabla de correspondencia, un segundo registro en el cual el identificador del proceso en el primer registro se almacena; si el segundo registro se encuentra, obtener un identificador de una aplicación del segundo registro y enviar el identificador de la aplicación al dispositivo de seguridad de red.

14. Un sistema para identificar información de aplicación en el tráfico de red, que comprende:

un dispositivo (710) terminal, un dispositivo (720) de seguridad de red y un dispositivo (730) de procesamiento de datos;

el dispositivo (720) de seguridad de red se configura para recibir un primer tren de datos, generar un primer registro de identificación después de determinar un identificador de una aplicación que envía el primer tren de datos, en donde el primer registro de identificación incluye un identificador del primer tren de datos y el identificador de la aplicación, y el identificador del tren de datos es una 5-tupla que incluye una dirección de origen, un puerto de origen, una dirección de destino, un puerto de destino y un identificador de protocolo; y enviar el primer registro de identificación al dispositivo de procesamiento de datos;

el dispositivo (710) terminal se configura para obtener un identificador de un proceso que se ejecuta en el dispositivo (710) terminal y un identificador de un segundo tren de datos creado por el proceso, para generar un segundo registro de identificación, en donde el segundo registro de identificación incluye el identificador del segundo tren de datos y el identificador del proceso; obtener una tabla de correspondencia, en donde cada registro en la tabla de correspondencia almacena un identificador de una aplicación y un identificador de un proceso creado por la aplicación; y enviar el segundo registro de identificación y la tabla de correspondencia al dispositivo de procesamiento de datos;

el dispositivo (730) de procesamiento de datos se configura para recibir el primer registro de identificación del dispositivo (720) de seguridad de red, recibir el segundo registro de identificación y la tabla de correspondencia del dispositivo (710) terminal; determinar si el identificador del primer tren de datos comprendido en el primer registro de identificación es igual al identificador del segundo tren de datos comprendido en el segundo registro de identificación; si el identificador del primer tren de datos comprendido en el primer registro de identificación es igual al identificador del segundo tren de datos comprendido en el segundo registro de identificación, consultar si un primer registro de asociación existe en la tabla de correspondencia, en donde el primer registro de asociación almacena el identificador de la aplicación comprendida en el primer registro de identificación y el identificador del proceso comprendido en el segundo registro de identificación, y si el primer registro de asociación no existe, determinar que el primer registro de identificación es un registro de identificación incorrecto.

15. El sistema según la reivindicación 14, en donde el dispositivo (730) de procesamiento de datos comprende una memoria (910), aun procesador (920) y una interfaz (930) de red, y la memoria (910), el procesador (920) y la interfaz (930) de red se comunican entre sí mediante el uso de un bus (940);

la memoria (910) almacena un código de programa;

la interfaz (930) de red se configura para: recibir el primer registro de identificación del dispositivo (720) de seguridad de red, y recibir el segundo registro de identificación y la tabla de correspondencia del dispositivo (710) terminal;

el procesador (920) se adapta para, si el identificador del primer tren de datos comprendido en el primer registro de identificación es igual al identificador del segundo tren de datos comprendido en el segundo registro de identificación, consultar si un primer registro de asociación existe en la tabla de correspondencia, en donde el primer registro de asociación almacena el identificador de la aplicación comprendida en el primer registro de identificación y un identificador de un proceso comprendido en el segundo registro de identificación; y si el primer registro de asociación no existe, determinar que el primer registro de identificación es un registro de identificación incorrecto.

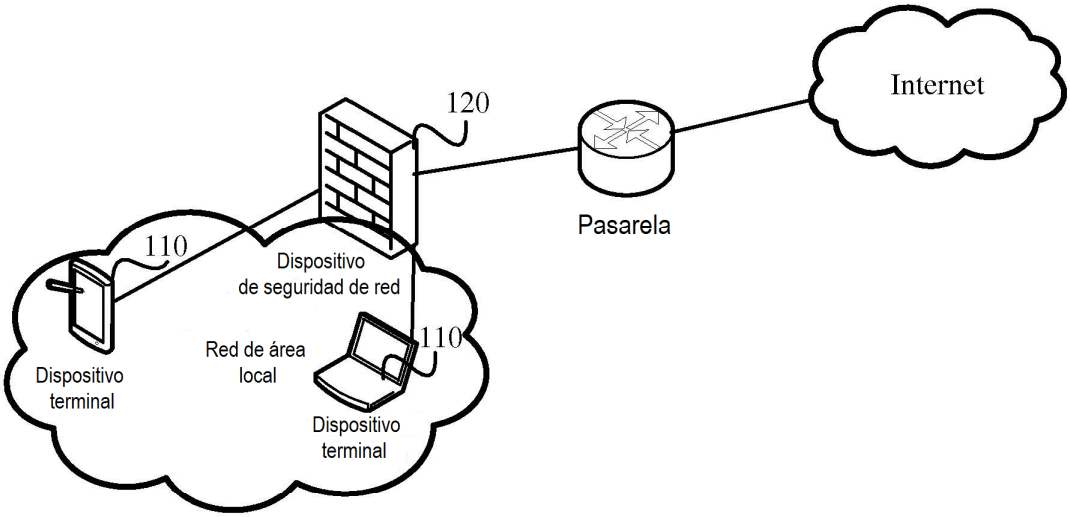
Internet
120
Pasarela
110
Dispositivo
de seguridad de red
Red de área
local
110
Dispositivo
terminal
Dispositivo
terminal

FIG. 1A

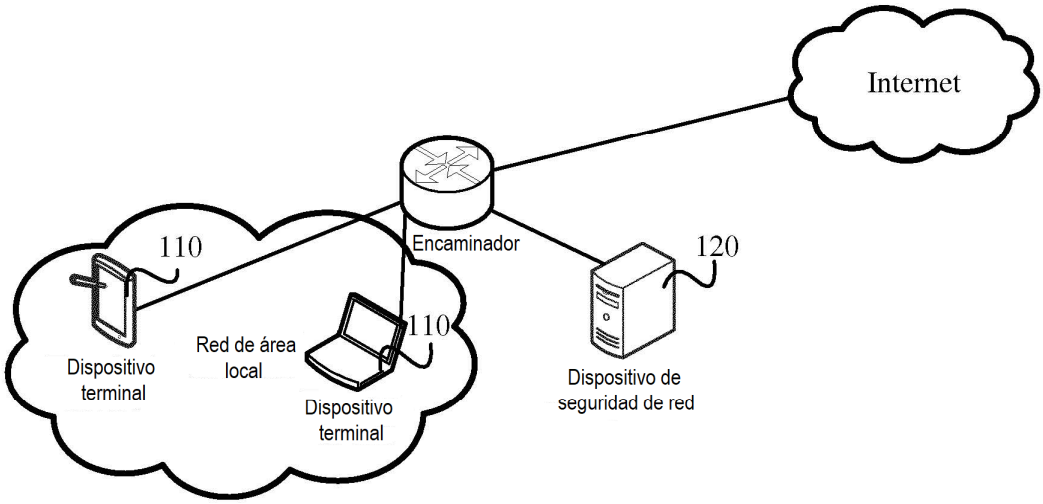
Internet
Encaminador
120
110
110
Dispositivo
terminal
Red de área
local
Dispositivo
terminal
Dispositivo de
seguridad de red

FIG. 1B

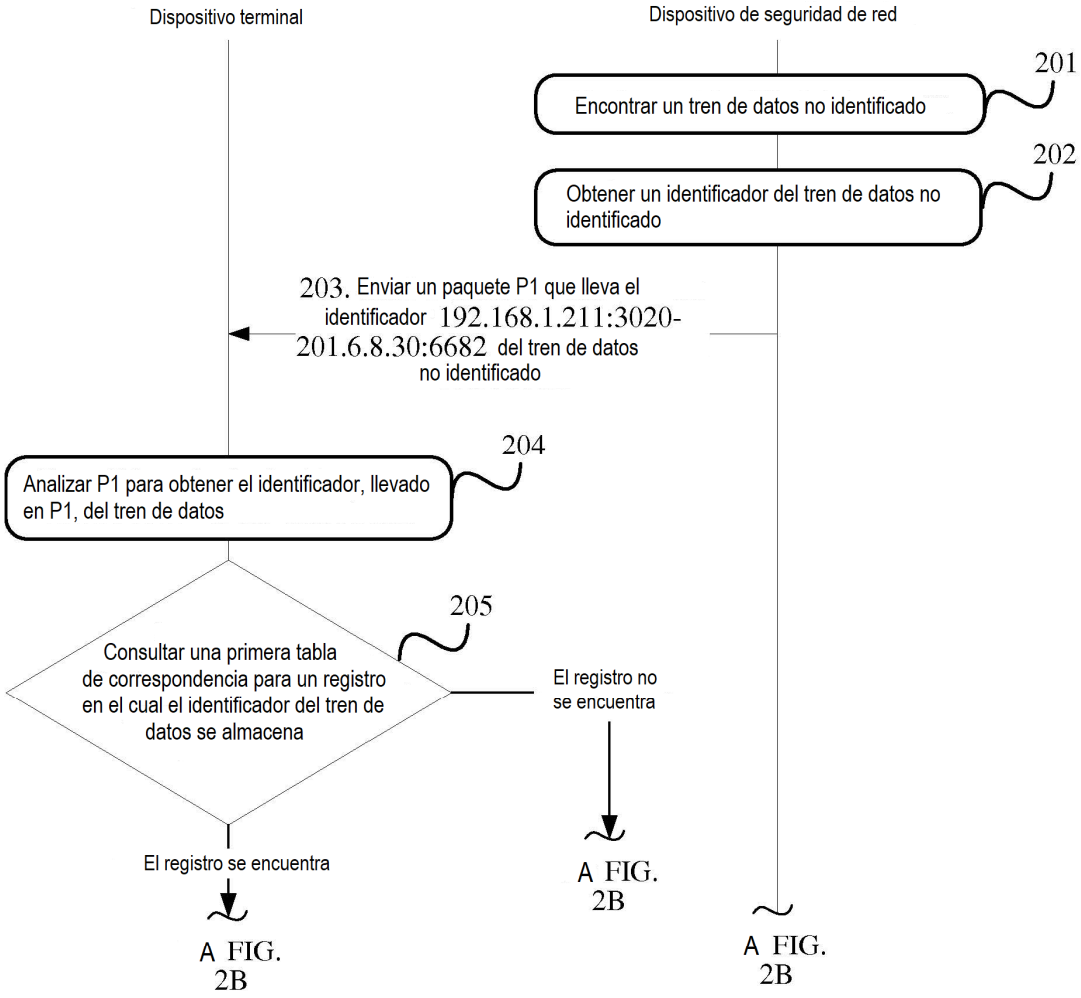
Dispositivo terminal
Dispositivo de seguridad de red
201
Encontrar un tren de datos no identificado
202
Obtener un identificador del tren de datos no identificado
203. Enviar un paquete P1 que lleva el identificador 192.168.1.211:3020-201.6.8.30:6682 del tren de datos no identificado
204
Analizar P1 para obtener el identificador, llevado en P1, del tren de datos
205
Consultar una primera tabla de correspondencia para un registro en el cual el identificador del tren de datos se almacena
El registro no se encuentra
A FIG. 2B
El registro se encuentra
A FIG. 2B
A FIG. 2B

FIG. 2A

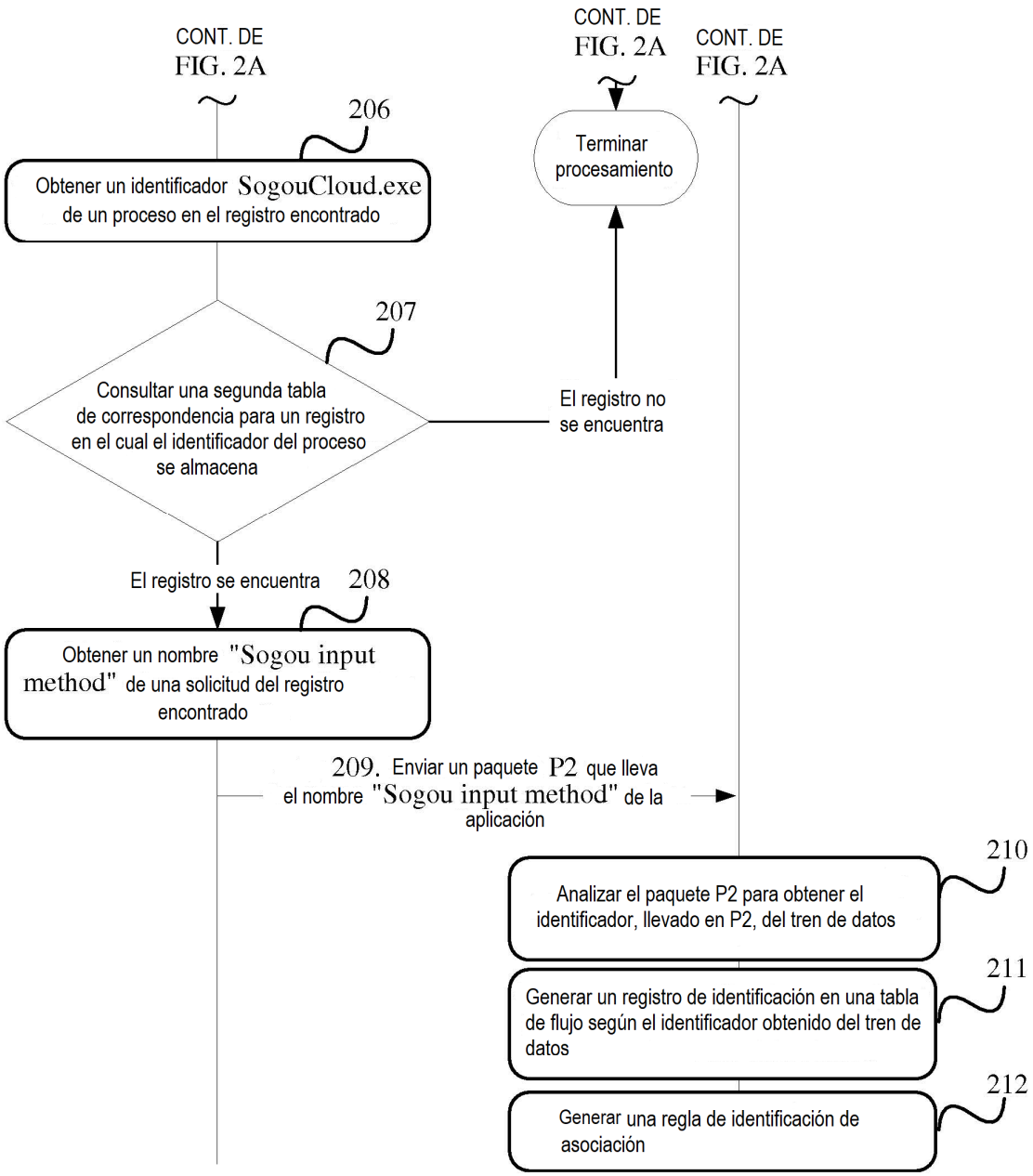
CONT. DE FIG. 2A
206
Obtener un identificador SogouCloud.exe de un proceso en el registro encontrado
207
Consultar una segunda tabla de correspondencia para un registro en el cual el identificador del proceso se almacena
El registro no se encuentra
CONT. DE FIG. 2A
Terminar procesamiento
El registro se encuentra
208
Obtener un nombre "Sogou input method" de una solicitud del registro encontrado
209. Enviar un paquete P2 que lleva el nombre "Sogou input method" de la aplicación
CONT. DE FIG. 2A
210
Analizar el paquete P2 para obtener el identificador, llevado en P2, del tren de datos
211
Generar un registro de identificación en una tabla de flujo según el identificador obtenido del tren de datos
212
Generar una regla de identificación de asociación

FIG. 2B

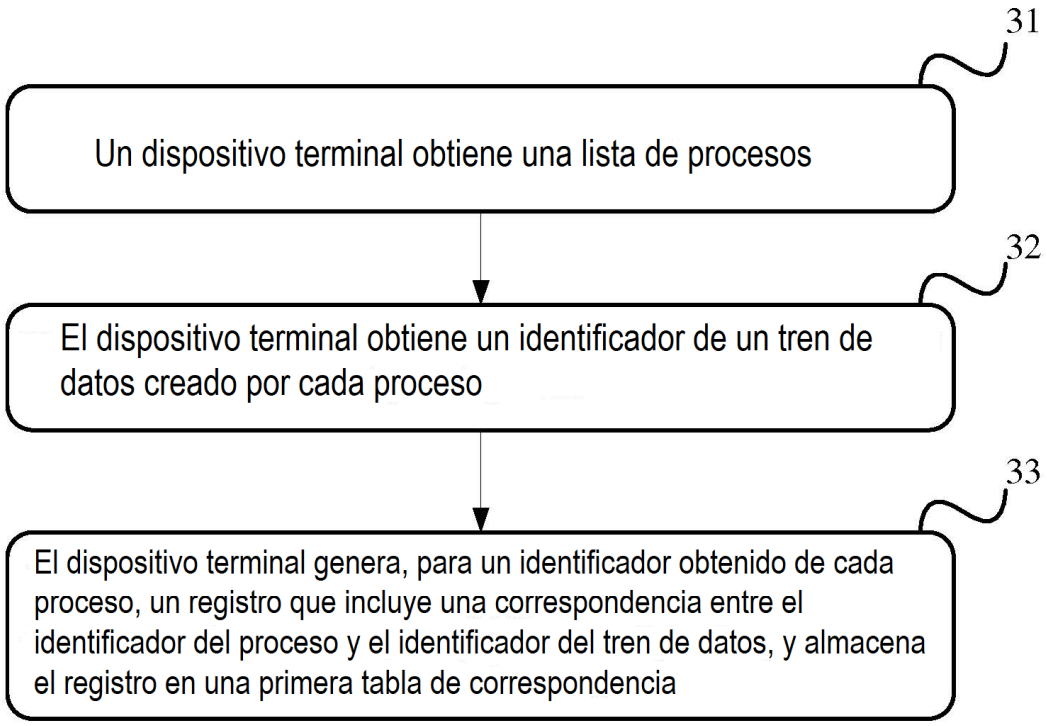
31
Un dispositivo terminal obtiene una lista de procesos
32
El dispositivo terminal obtiene un identificador de un tren de datos creado por cada proceso
33
El dispositivo terminal genera, para un identificador obtenido de cada proceso, un registro que incluye una correspondencia entre el identificador del proceso y el identificador del tren de datos, y almacena el registro en una primera tabla de correspondencia

FIG. 3A

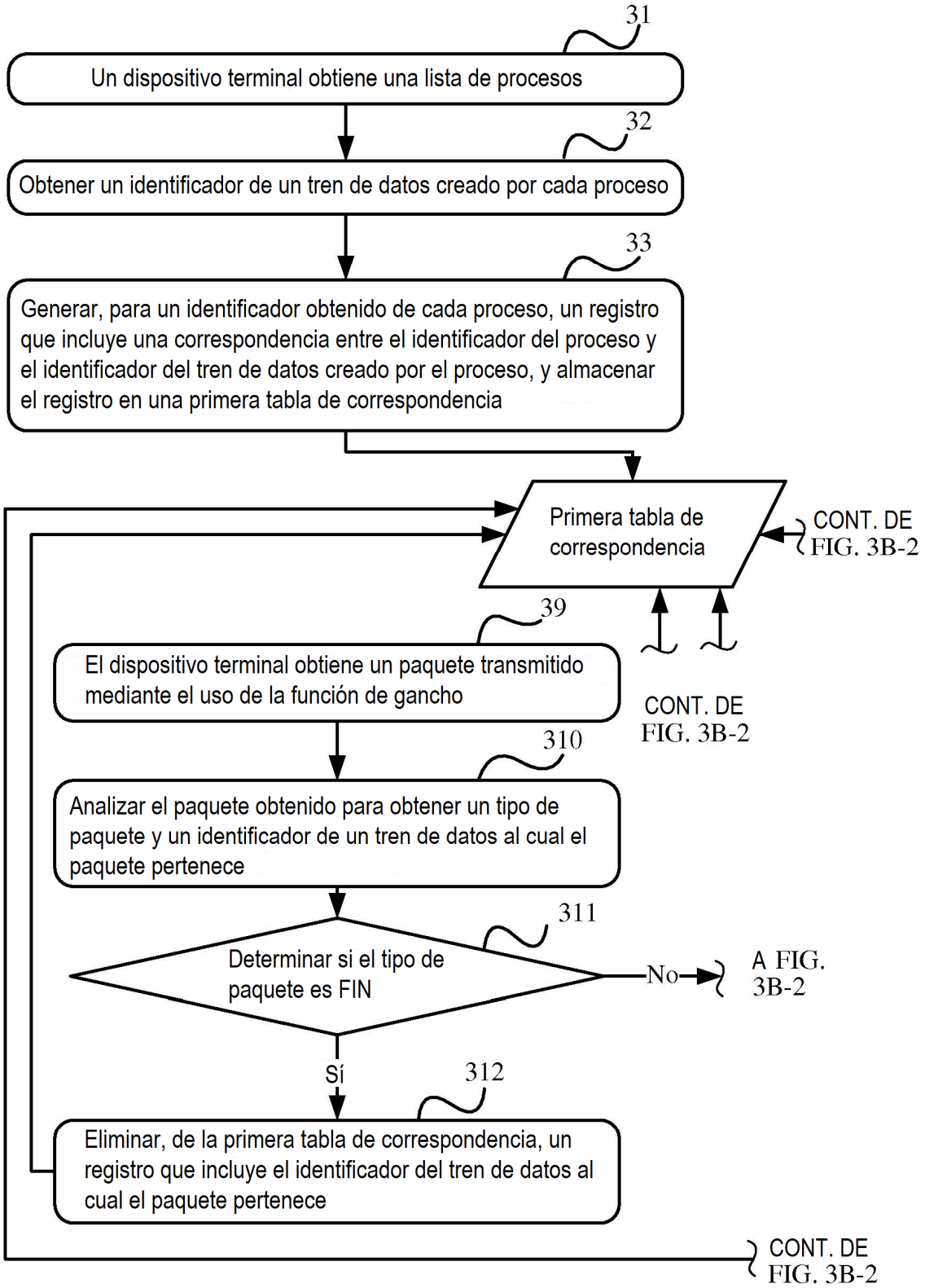
31
Un dispositivo terminal obtiene una lista de procesos
32
Obtener un identificador de un tren de datos creado por cada proceso
33
Generar, para un identificador obtenido de cada proceso, un registro que incluye una correspondencia entre el identificador del proceso y el identificador del tren de datos creado por el proceso, y almacenar el registro en una primera tabla de correspondencia
Primera tabla de correspondencia
CONT. DE FIG. 3B-2
39
El dispositivo terminal obtiene un paquete transmitido mediante el uso de la función de gancho
CONT. DE FIG. 3B-2
310
Analizar el paquete obtenido para obtener un tipo de paquete y un identificador de un tren de datos al cual el paquete pertenece
311
Determinar si el tipo de paquete es FIN
No
A FIG. 3B-2
Sí
312
Eliminar, de la primera tabla de correspondencia, un registro que incluye el identificador del tren de datos al cual el paquete pertenece
CONT. DE FIG. 3B-2

FIG. 3B-1

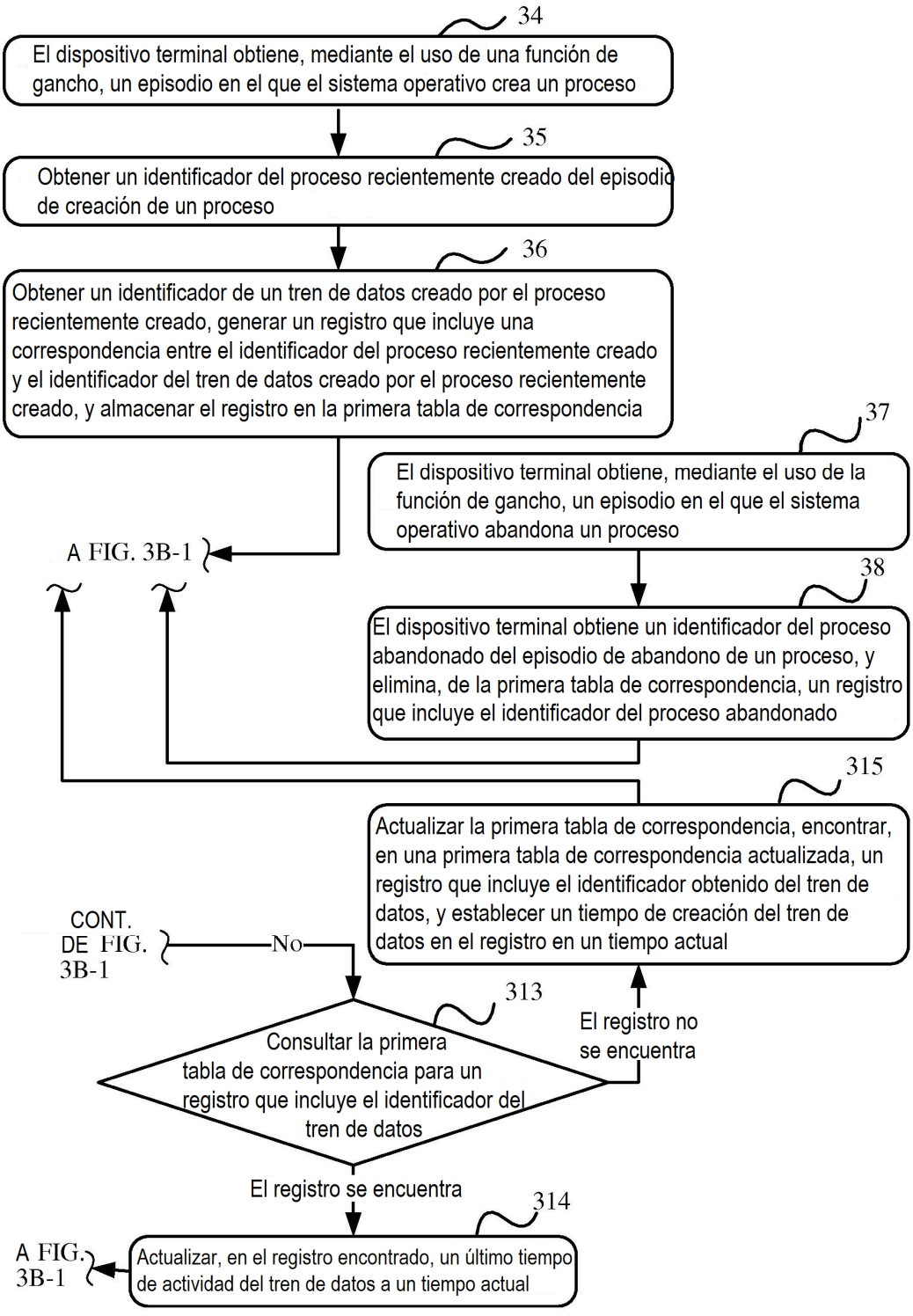
34
El dispositivo terminal obtiene, mediante el uso de una función de gancho, un episodio en el que el sistema operativo crea un proceso
35
Obtener un identificador del proceso recientemente creado del episodio de creación de un proceso
36
Obtener un identificador de un tren de datos creado por el proceso recientemente creado, generar un registro que incluye una correspondencia entre el identificador del proceso recientemente creado y el identificador del tren de datos creado por el proceso recientemente creado, y almacenar el registro en la primera tabla de correspondencia
37
El dispositivo terminal obtiene, mediante el uso de la función de gancho, un episodio en el que el sistema operativo abandona un proceso
A FIG. 3B-1
38
El dispositivo terminal obtiene un identificador del proceso abandonado del episodio de abandono de un proceso, y elimina, de la primera tabla de correspondencia, un registro que incluye el identificador del proceso abandonado
315
Actualizar la primera tabla de correspondencia, encontrar, en una primera tabla de correspondencia actualizada, un registro que incluye el identificador obtenido del tren de datos, y establecer un tiempo de creación del tren de datos en el registro en un tiempo actual
CONT. DE FIG. 3B-1
No
313
Consultar la primera tabla de correspondencia para un registro que incluye el identificador del tren de datos
El registro no se encuentra
El registro se encuentra
314
A FIG. 3B-1
Actualizar, en el registro encontrado, un último tiempo de actividad del tren de datos a un tiempo actual

FIG. 3B-2

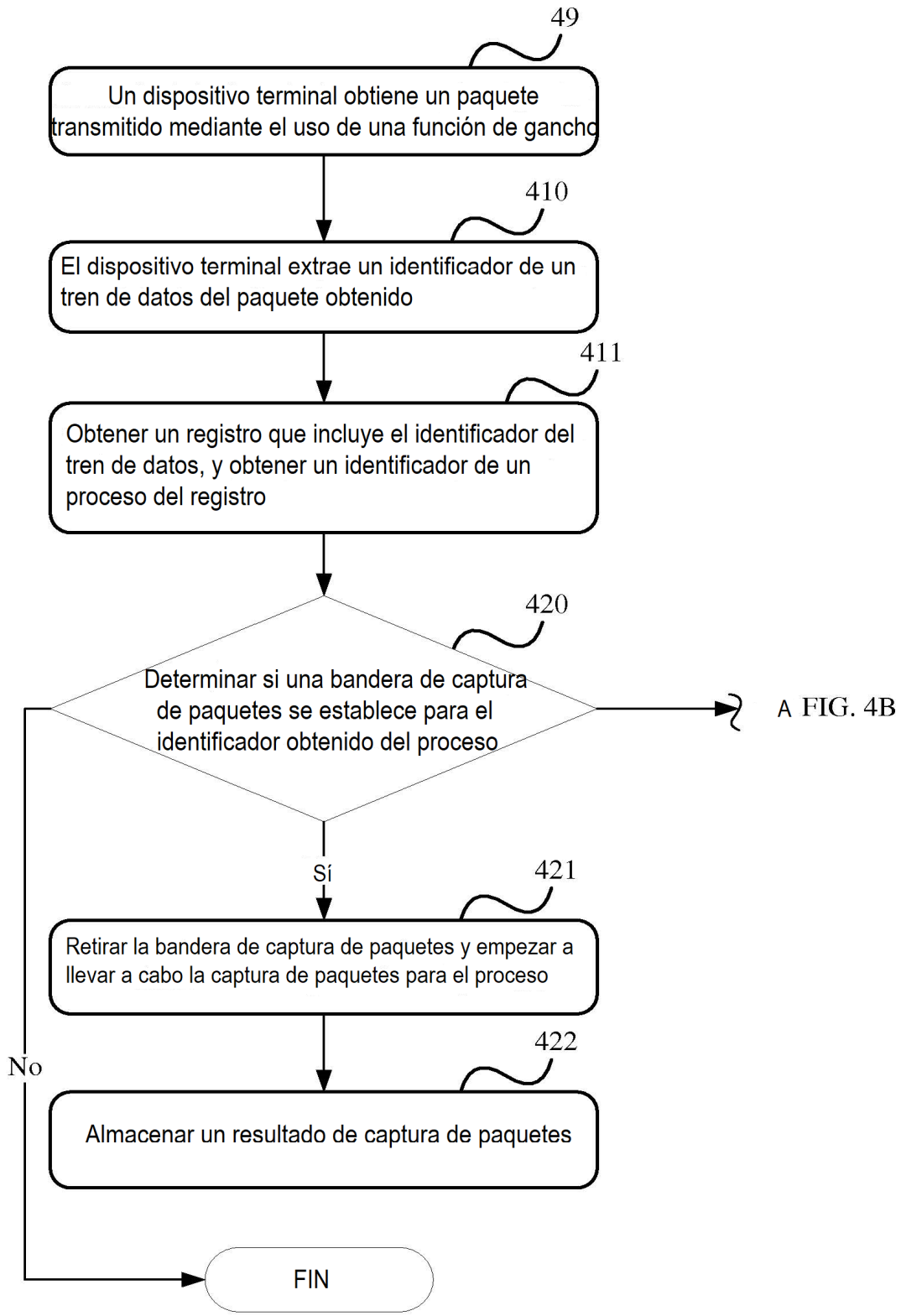
49
Un dispositivo terminal obtiene un paquete transmitido mediante el uso de una función de gancho
410
El dispositivo terminal extrae un identificador de un tren de datos del paquete obtenido
411
Obtener un registro que incluye el identificador del tren de datos, y obtener un identificador de un proceso del registro
420
Determinar si una bandera de captura de paquetes se establece para el identificador obtenido del proceso
A FIG. 4B
Sí
421
Retirar la bandera de captura de paquetes y empezar a llevar a cabo la captura de paquetes para el proceso
422
Almacenar un resultado de captura de paquetes
No
FIN

FIG. 4A

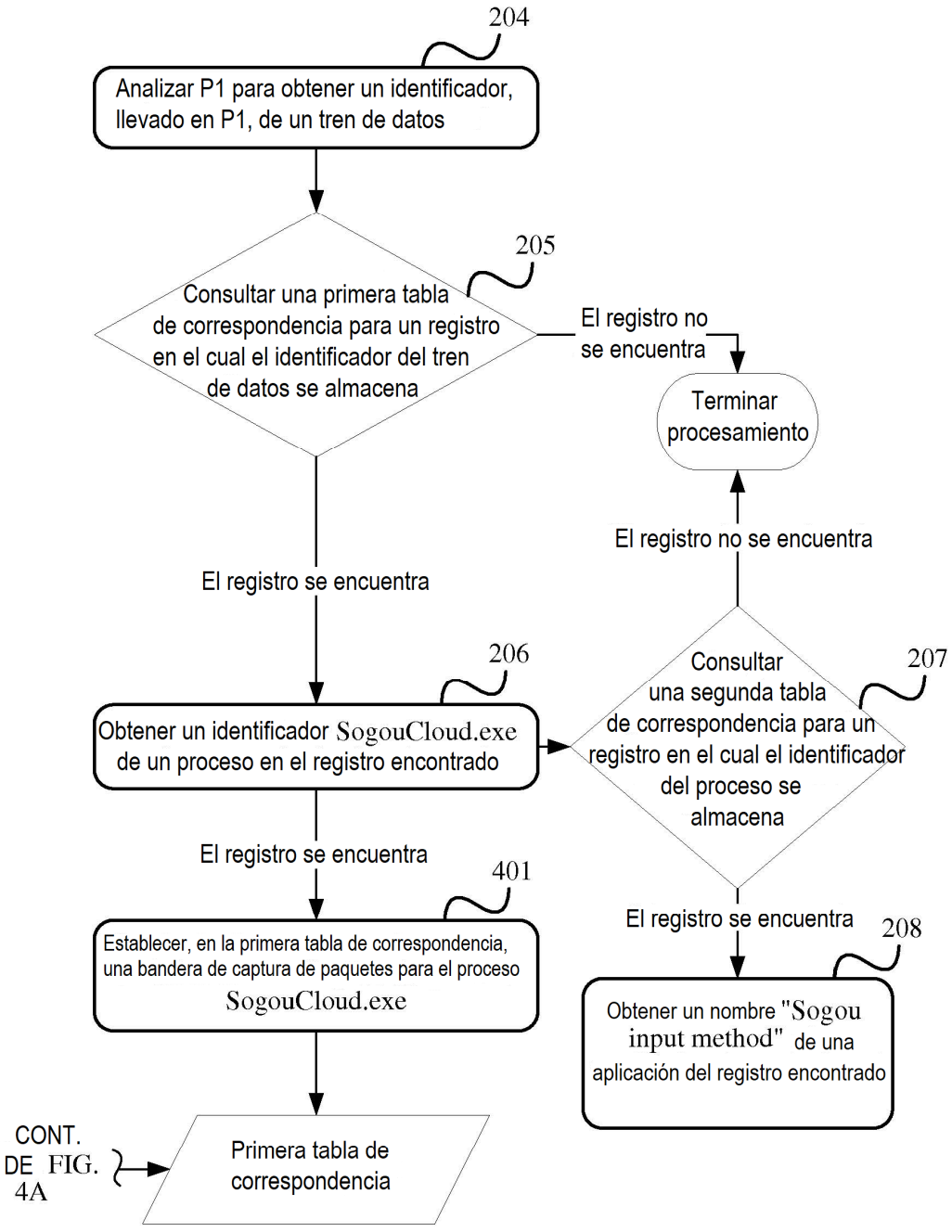
204
Analizar P1 para obtener un identificador, llevado en P1, de un tren de datos
205
Consultar una primera tabla de correspondencia para un registro en el cual el identificador del tren de datos se almacena
El registro no se encuentra
Terminar procesamiento
El registro no se encuentra
El registro se encuentra
206
Obtener un identificador SogouCloud.exe de un proceso en el registro encontrado
207
Consultar una segunda tabla de correspondencia para un registro en el cual el identificador del proceso se almacena
El registro se encuentra
401
Establecer, en la primera tabla de correspondencia, una bandera de captura de paquetes para el proceso SogouCloud.exe
El registro se encuentra
208
Obtener un nombre "Sogou input method" de una aplicación del registro encontrado
CONT. DE FIG. 4A
Primera tabla de correspondencia

FIG. 4B

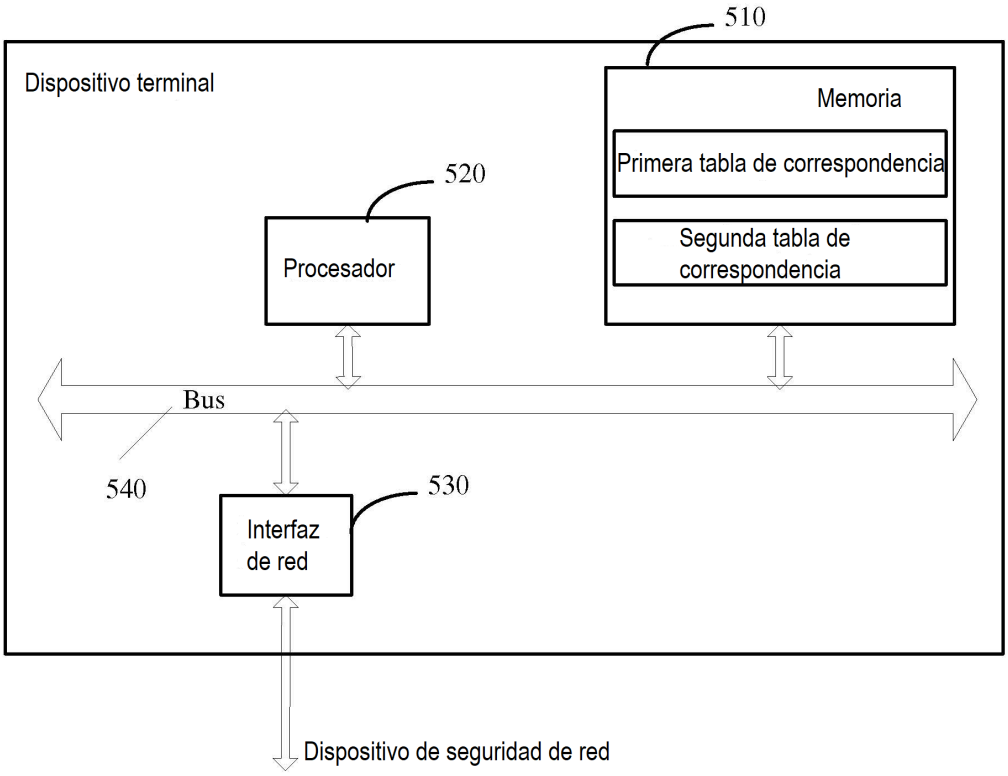
510
Dispositivo terminal
Memoria
Primera tabla de correspondencia
Segunda tabla de correspondencia
520
Procesador
Bus
540
530
Interfaz de red
Dispositivo de seguridad de red

FIG. 5A

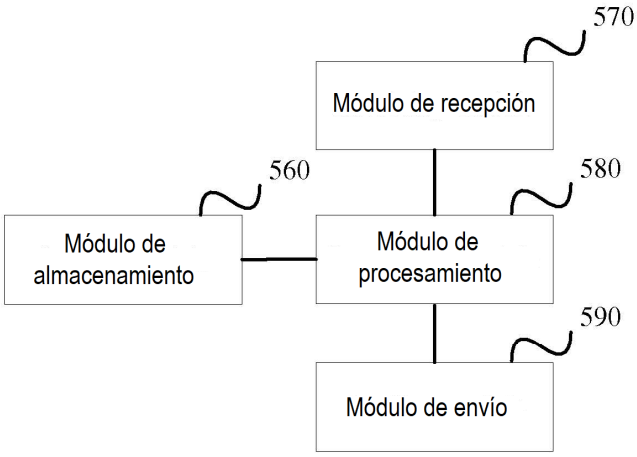
570
Módulo de recepción
560
580
Módulo de almacenamiento
Módulo de procesamiento
590
Módulo de envío

FIG. 5B

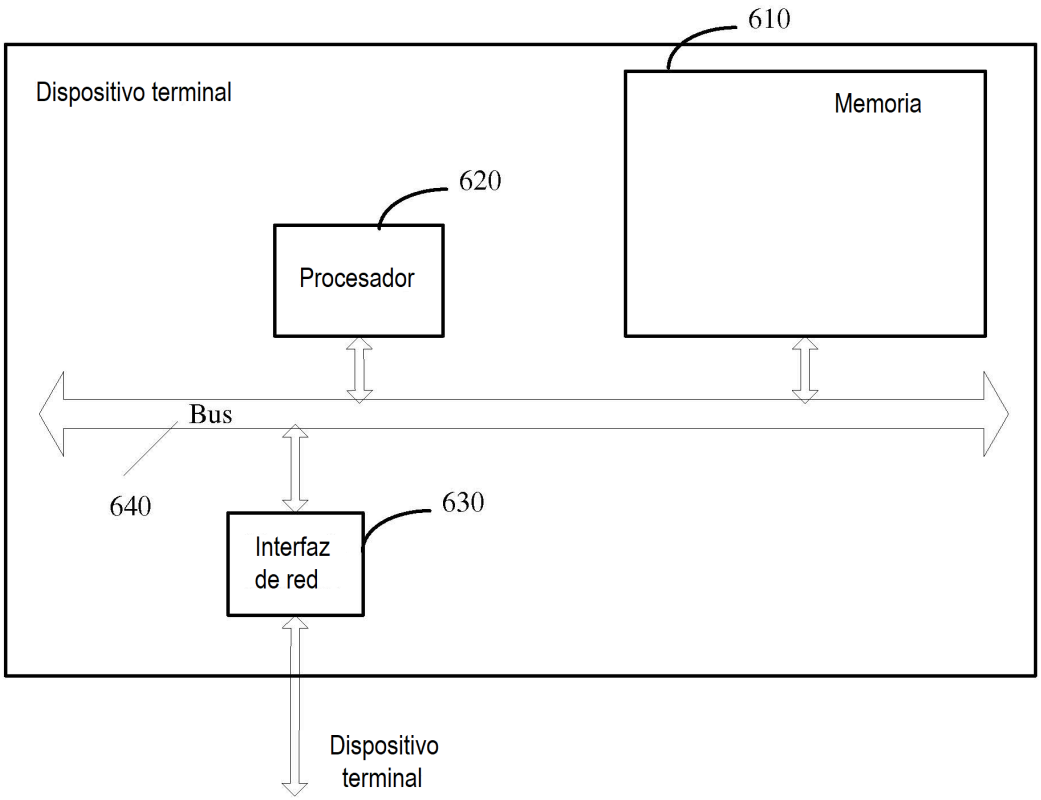
610
Dispositivo terminal
Memoria
620
Procesador
Bus
640
630
Interfaz de red
Dispositivo terminal

FIG. 6A

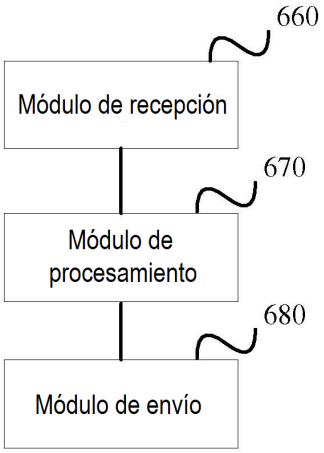
660
Módulo de recepción
670
Módulo de procesamiento
680
Módulo de envío

FIG. 6B

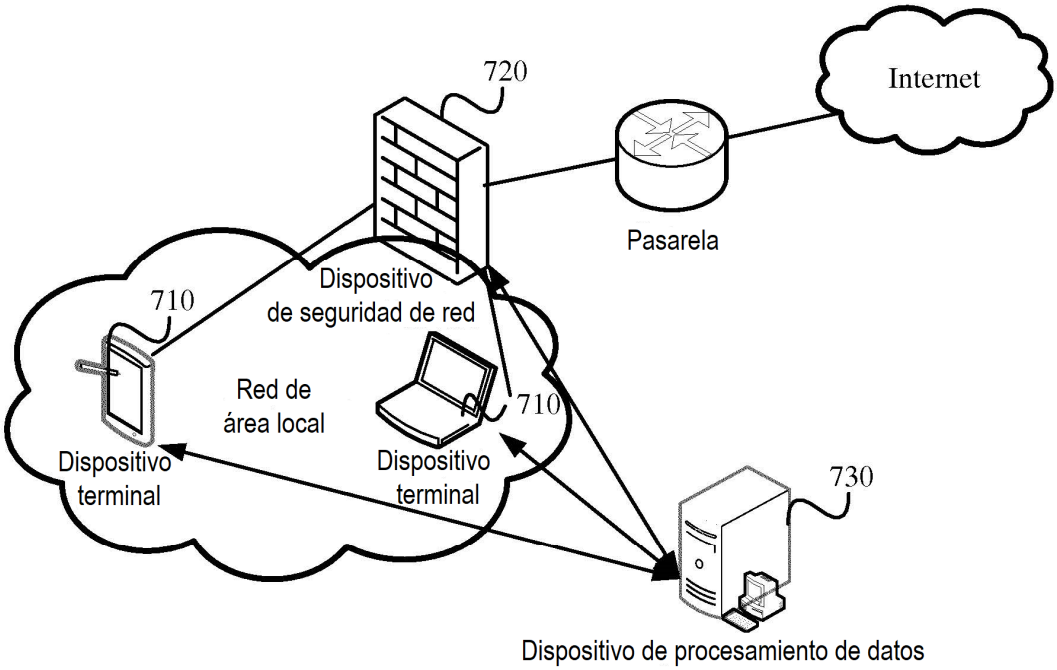
720
Internet
Pasarela
Dispositivo
de seguridad de red
710
Red de
área local
710
Dispositivo
terminal
Dispositivo
terminal
730
Dispositivo de procesamiento de datos

FIG. 7

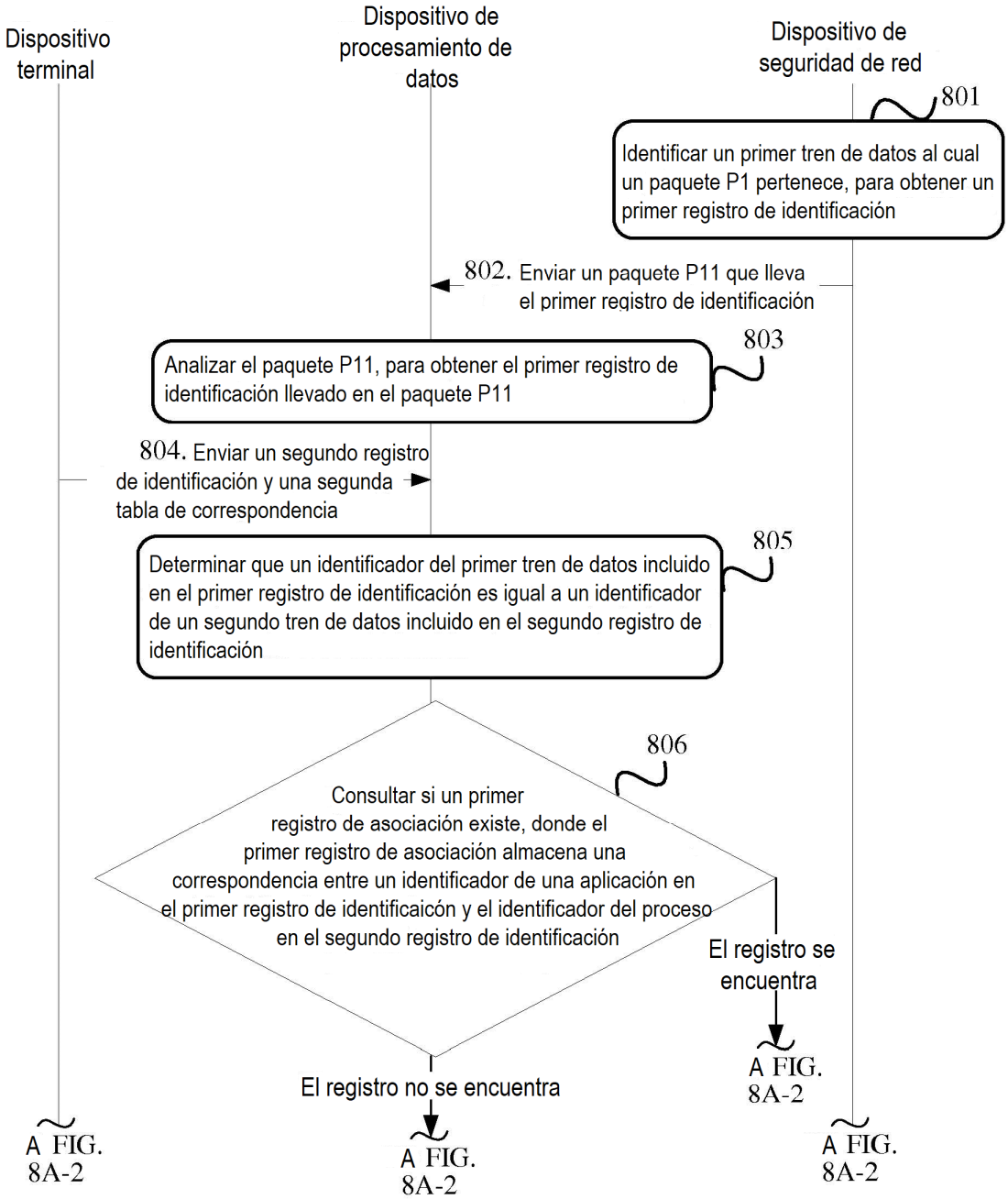
Dispositivo terminal
Dispositivo de procesamiento de datos
Dispositivo de seguridad de red
801
Identificar un primer tren de datos al cual un paquete P1 pertenece, para obtener un primer registro de identificación
802. Enviar un paquete P11 que lleva el primer registro de identificación
803
Analizar el paquete P11, para obtener el primer registro de identificación llevado en el paquete P11
804. Enviar un segundo registro de identificación y una segunda tabla de correspondencia
805
Determinar que un identificador del primer tren de datos incluido en el primer registro de identificación es igual a un identificador de un segundo tren de datos incluido en el segundo registro de identificación
806
Consultar si un primer registro de asociación existe, donde el primer registro de asociación almacena una correspondencia entre un identificador de una aplicación en el primer registro de identificaicón y el identificador del proceso en el segundo registro de identificación
El registro se encuentra
El registro no se encuentra
A FIG. 8A-2
A FIG. 8A-2
A FIG. 8A-2
A FIG. 8A-2

FIG. 8A-1

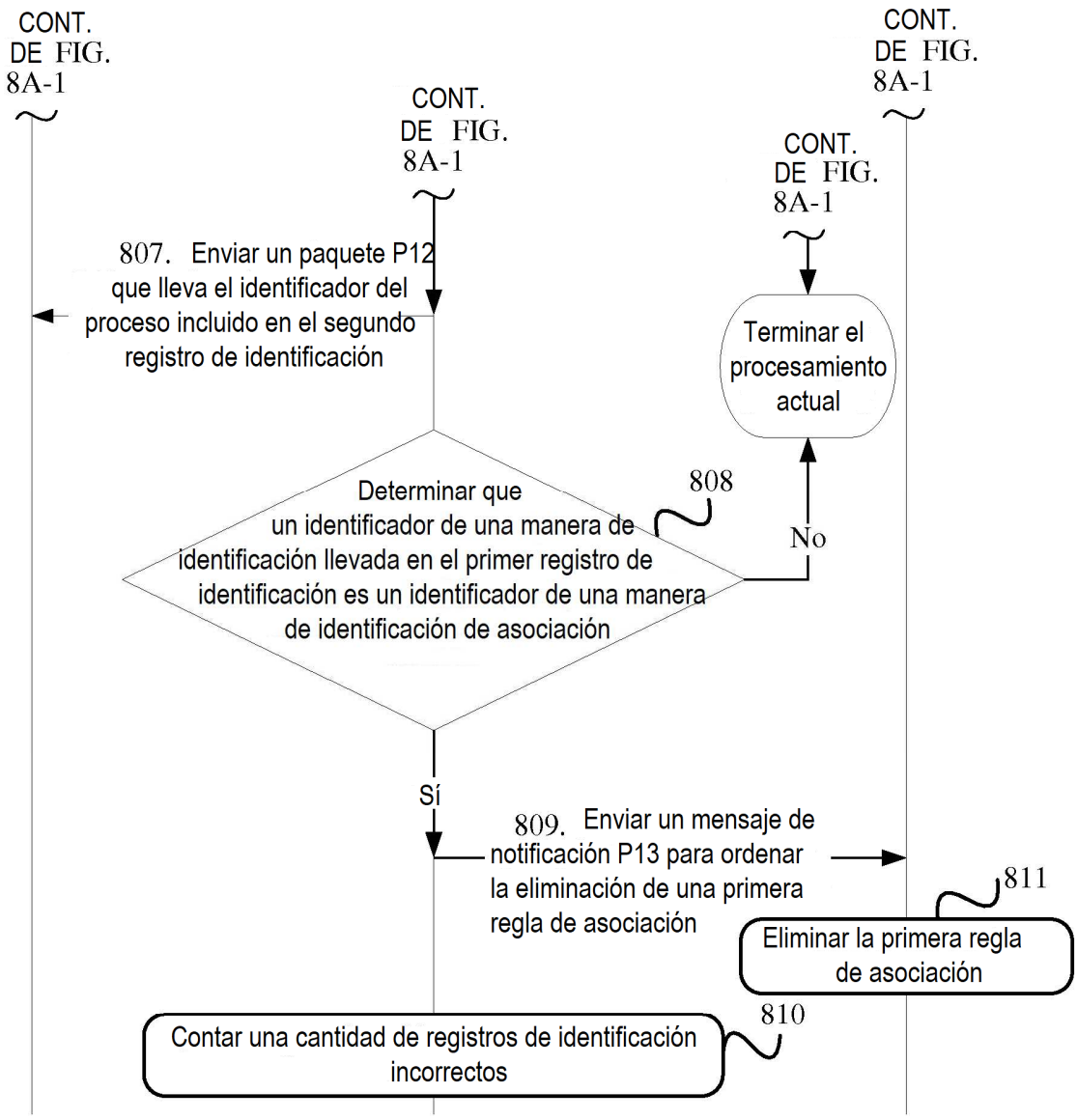
CONT. DE FIG. 8A-1
CONT. DE FIG. 8A-1
CONT. DE FIG. 8A-1
CONT. DE FIG. 8A-1
807. Enviar un paquete P12 que lleva el identificador del proceso incluido en el segundo registro de identificación
Terminar el procesamiento actual
808
Determinar que un identificador de una manera de identificación llevada en el primer registro de identificación es un identificador de una manera de identificación de asociación
No
Sí
809. Enviar un mensaje de notificación P13 para ordenar la eliminación de una primera regla de asociación
811
Eliminar la primera regla de asociación
810
Contar una cantidad de registros de identificación incorrectos

FIG. 8A-2

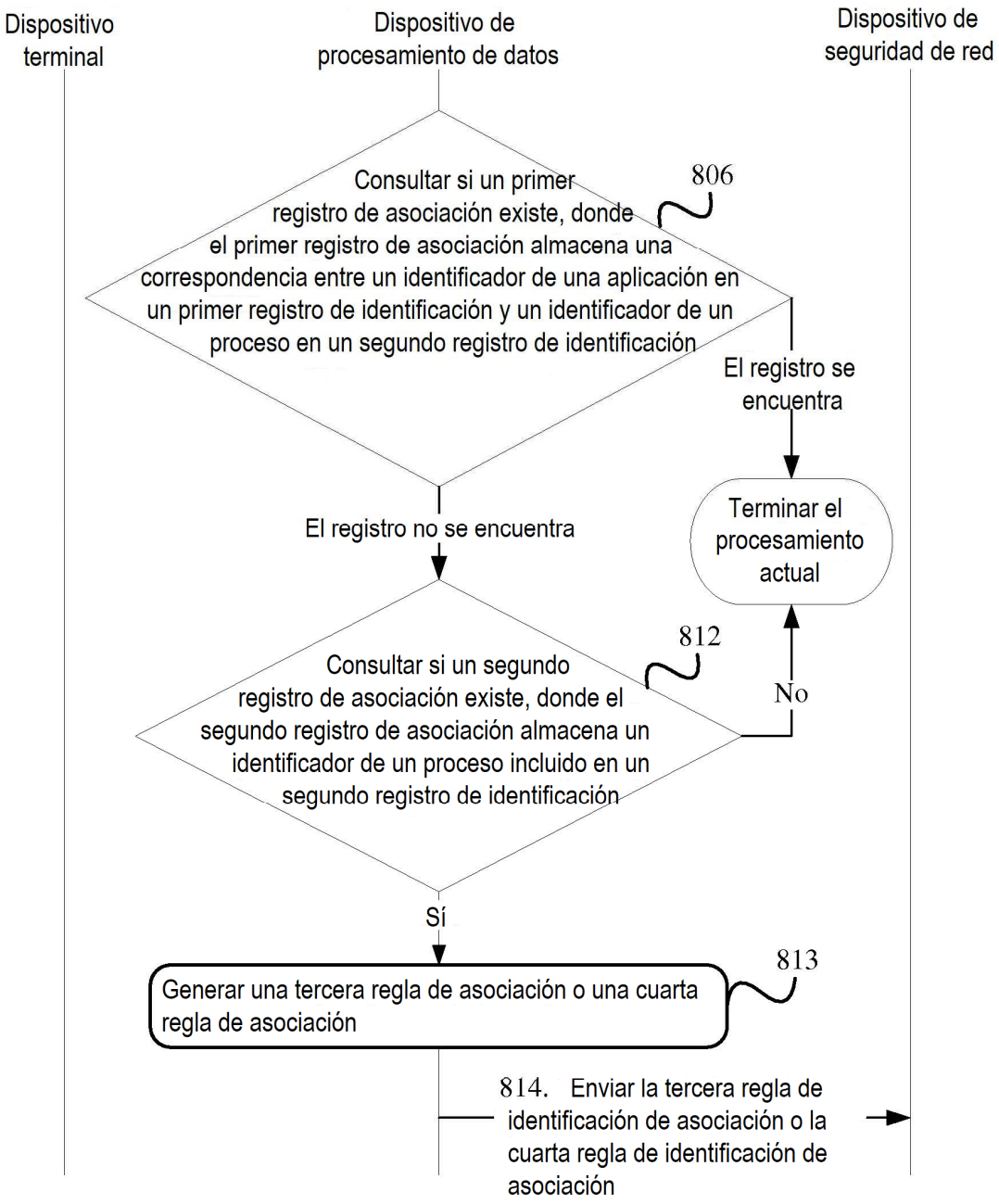
Dispositivo terminal
Dispositivo de procesamiento de datos
Dispositivo de seguridad de red
Consultar si un primer registro de asociación existe, donde el primer registro de asociación almacena una correspondencia entre un identificador de una aplicación en un primer registro de identificación y un identificador de un proceso en un segundo registro de identificación
806
El registro se encuentra
El registro no se encuentra
Terminar el procesamiento actual
Consultar si un segundo registro de asociación existe, donde el segundo registro de asociación almacena un identificador de un proceso incluido en un segundo registro de identificación
812
No
Sí
Generar una tercera regla de asociación o una cuarta regla de asociación
813
814. Enviar la tercera regla de identificación de asociación o la cuarta regla de identificación de asociación

FIG. 8A-3

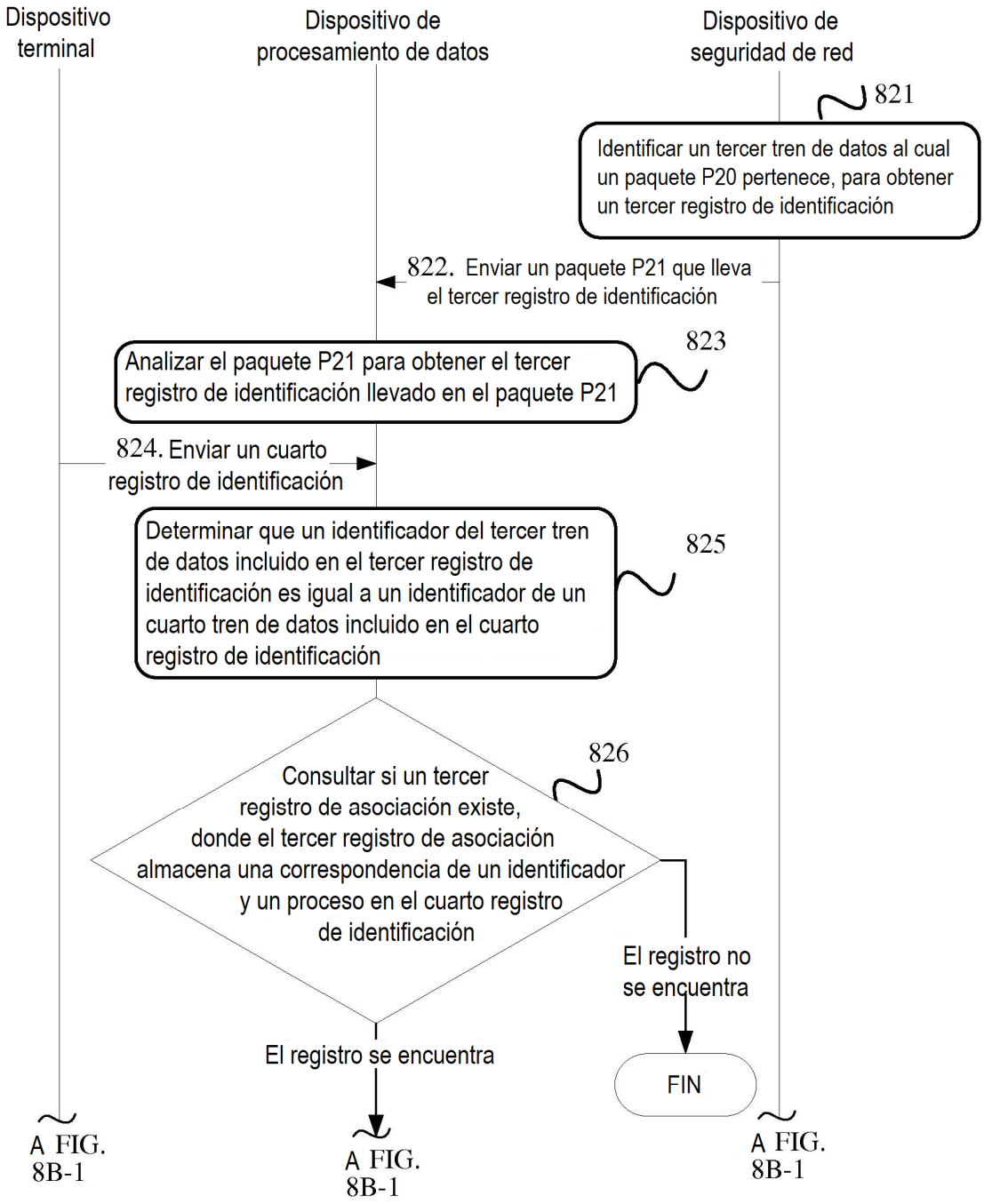
Dispositivo terminal
Dispositivo de procesamiento de datos
Dispositivo de seguridad de red
821
Identificar un tercer tren de datos al cual un paquete P20 pertenece, para obtener un tercer registro de identificación
822. Enviar un paquete P21 que lleva el tercer registro de identificación
823
Analizar el paquete P21 para obtener el tercer registro de identificación llevado en el paquete P21
824. Enviar un cuarto registro de identificación
825
Determinar que un identificador del tercer tren de datos incluido en el tercer registro de identificación es igual a un identificador de un cuarto tren de datos incluido en el cuarto registro de identificación
826
Consultar si un tercer registro de asociación existe, donde el tercer registro de asociación almacena una correspondencia de un identificador y un proceso en el cuarto registro de identificación
El registro no se encuentra
El registro se encuentra
FIN
A FIG. 8B-1
A FIG. 8B-1
A FIG. 8B-1

FIG. 8B-1

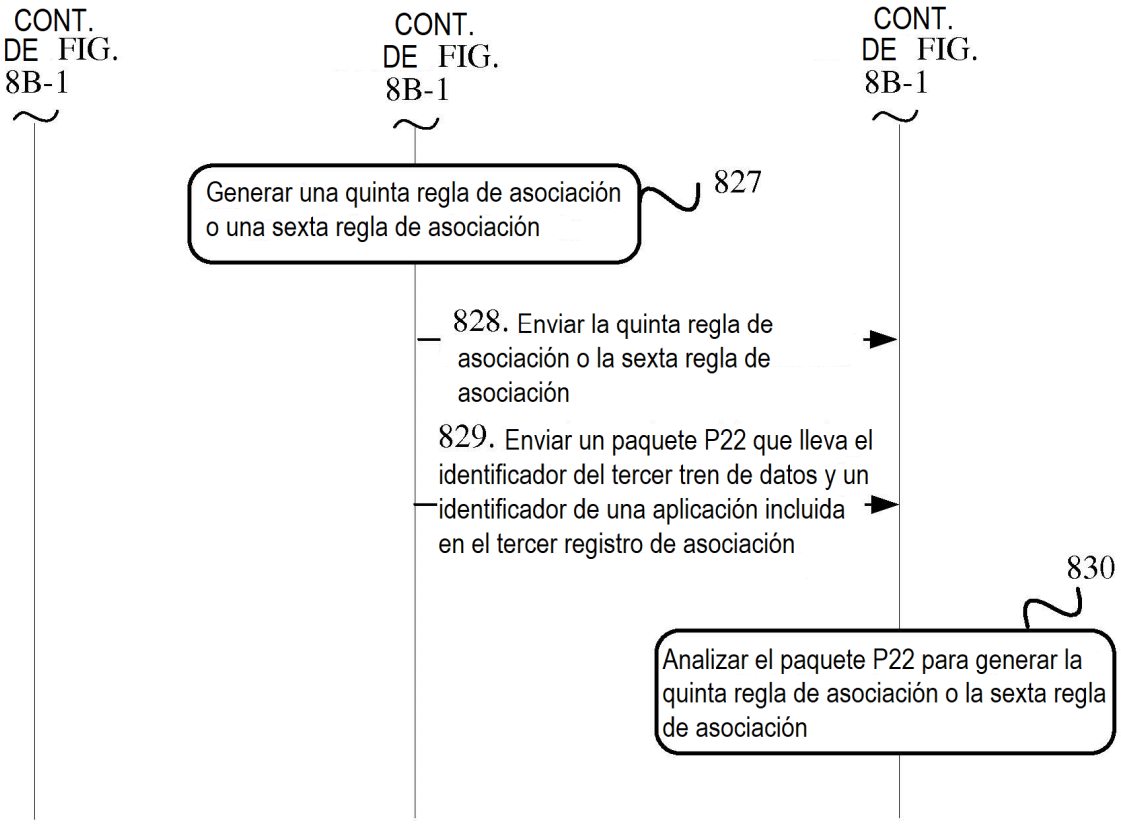
CONT. DE FIG. 8B-1
CONT. DE FIG. 8B-1
CONT. DE FIG. 8B-1
Generar una quinta regla de asociación o una sexta regla de asociación
827
828. Enviar la quinta regla de asociación o la sexta regla de asociación
829. Enviar un paquete P22 que lleva el identificador del tercer tren de datos y un identificador de una aplicación incluida en el tercer registro de asociación
830
Analizar el paquete P22 para generar la quinta regla de asociación o la sexta regla de asociación

FIG. 8B-2

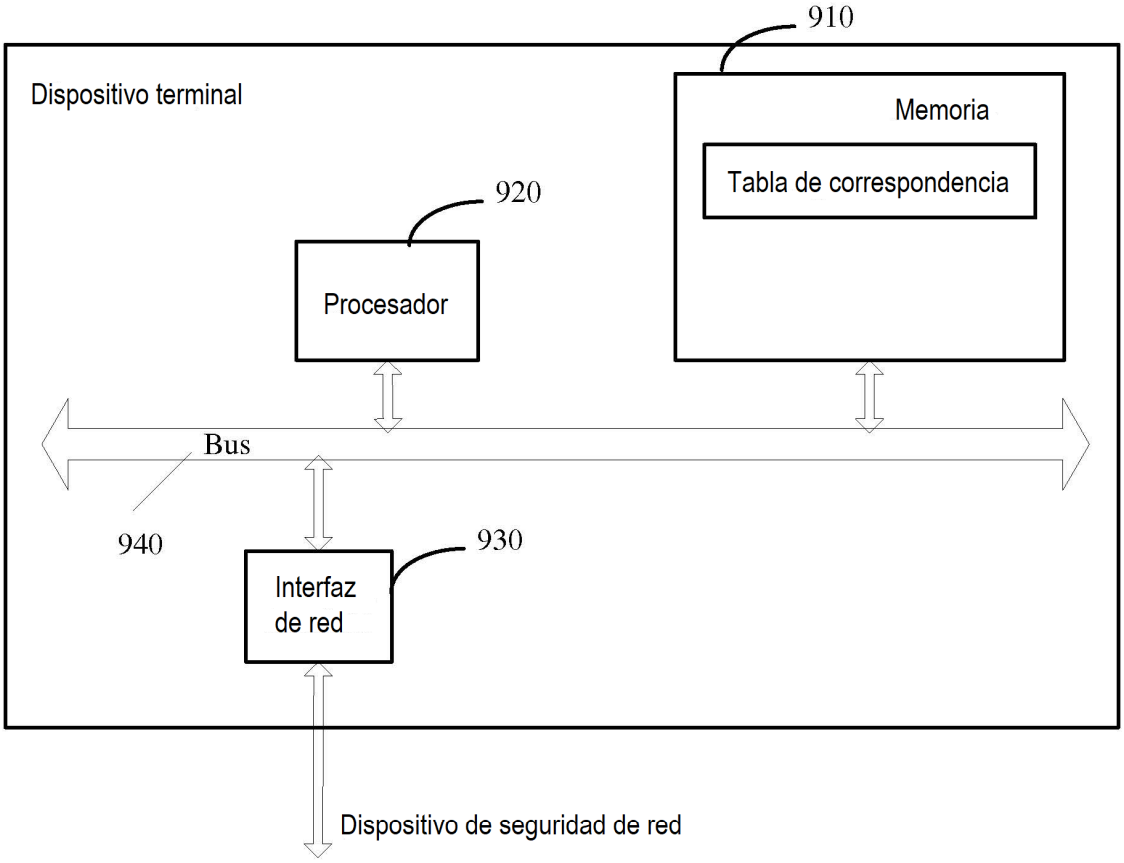
910
Dispositivo terminal
Memoria
Tabla de correspondencia
920
Procesador
Bus
940
930
Interfaz de red
Dispositivo de seguridad de red

FIG. 9A

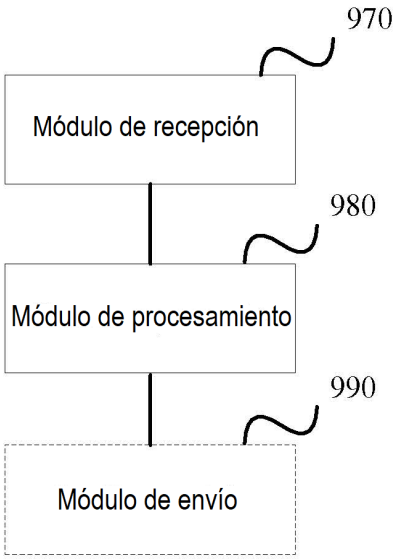
970
Módulo de recepción
980
Módulo de procesamiento
990
Módulo de envío

FIG. 9B