



19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA

11 Número de publicación: **2 323 244**

51 Int. Cl.:
H04L 12/26 (2006.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

96 Número de solicitud europea: **05291044 .5**

96 Fecha de presentación : **13.05.2005**

97 Número de publicación de la solicitud: **1722509**

97 Fecha de publicación de la solicitud: **15.11.2006**

54 Título: **Análisis del tráfico en redes de alta velocidad.**

45 Fecha de publicación de la mención BOPI:
09.07.2009

45 Fecha de la publicación del folleto de la patente:
09.07.2009

73 Titular/es: **Qosmos**
Immeuble le Cardinet, 5 Impasse Chalabre
75017 Paris, FR

72 Inventor/es: **Harmel, Gautier;**
Horlait, Eric y
Tollet, Jérôme

74 Agente: **Carpintero López, Mario**

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

DESCRIPCIÓN

Análisis del tráfico en redes de alta velocidad.

5 **Campo técnico**

La presente invención se refiere al campo de las redes informáticas y en particular, al análisis del flujo del tráfico en enlaces de conexión de alta velocidad.

10 **Antecedentes**

El flujo del tráfico de investigación puede consumir mucho tiempo y energía de procesamiento de vigilancia y clasificación, y están aumentado de una manera tremenda tanto la cantidad como la velocidad de los datos del tráfico, especialmente los datos del tráfico en Internet. Los sistemas de análisis del flujo del tráfico muy a menudo tropiezan con diversos obstáculos, los cuales tienen lugar al nivel del paso del flujo del tráfico debido a los diversos tipos de procesamiento densos requeridos con el fin de obtener una clasificación y un procesamiento semánticos, fiables, y útiles del tráfico de las redes.

La clasificación del tráfico que se desplaza alrededor de una red de datos hace posible decidir sobre los comportamientos que se van a adoptar para cada flujo de tráfico como una función de su clasificación. Esto es, antes de que un paquete de datos pueda ser satisfactoriamente procesado, la clasificación del flujo del tráfico permite que los componentes de la red clasifiquen los paquetes del tráfico de acuerdo con las características de los paquetes y con la información contenida en el paquete. Por tanto, un procesamiento preciso y eficiente de los datos depende en gran medida de los procedimientos fiables de clasificación de los paquetes. Después de que el paquete ha sido clasificado, los componentes de la red pueden determinar cómo manejar y procesar adecuadamente los paquetes.

Por ejemplo, en un cortafuegos, un sistema de seguridad establecido se basa en términos generales en el reconocimiento de las propiedades del protocolo para impedir determinadas transferencias, y en los dispositivos de gestión de la calidad del servicio; dichos dispositivos asignan unas prioridades a los datos como una función de normas complejas que describen diversos escenarios. Una correspondencia entre estos escenarios y los paquetes de datos transmitidos dentro de unas conexiones utiliza determinadas técnicas para clasificar estas conexiones.

De nuevo aquí, las operaciones de control y gestión de las redes requieren la clasificación de las conexiones entre diversos emisores y receptores los cuales generan flujos de datos digitales a través de estas redes. Esto requiere unos procedimientos de clasificación potentes y fiables, y con ello el análisis del tráfico.

Así mismo, el análisis y la clasificación de los paquetes a menudo comportan la tarea compleja de construir atributos de protocolo, esto es, determinar la secuencia ordenada de los nombres del protocolo utilizados en el flujo semántico de los datos y en los nombres de los parámetros acarreados por un protocolo. La generación de dicha base gráfica o de conocimiento para reconocer diferentes protocolos es una tarea muy engorrosa debido al número creciente de nuevos protocolos utilizados en las redes de comunicación de paquetes, así como al número de modificaciones de protocolos y de nuevos enlaces de dependencia.

Típicamente una tarea de observación de paquetes de datos es asignada a un nodo de una red, como por ejemplo un servidor apoderado a través del cual pasan las conexiones, las cuales generan estos paquetes de datos. Así, los análisis del flujo existentes se llevan en general a cabo en sistemas de redes informáticas como por ejemplo el ilustrado en la Figura 1. Un sistema de análisis del tráfico para el análisis del tráfico de alta velocidad (por ejemplo, paquetes o datagramas) entre varias computadoras, incluye una primera red 100 conectada a una segunda red 110 que utiliza un enlace de comunicaciones 200. El enlace 200 es utilizado por un analizador 300, el cual mide y analiza el tráfico que fluye en ambas o en una u otra dirección entre la primera red 100 y la segunda red 110. El tráfico entre la red 100 y la red 110 es generalmente de 1 Gbps en redes comerciales pero puede ser tan alto como un par de docenas de Gbps en el núcleo de una red del operador.

Como se indicó con anterioridad, en redes de tráfico intenso, el análisis continuo de todo el tráfico de una forma exacta y precisa es una tarea formidable. La capacidad de análisis y medición del analizador 300 se determina por el número de flujos simultáneos N (por ejemplo, el tamaño del flujo del tráfico) y por el rendimiento T de cada flujo (por ejemplo, la velocidad del flujo del tráfico). N directamente afecta a la cantidad de memoria requerida para gestionar el contexto de las aplicaciones registradas, mientras que T incide directamente en la potencia de procesamiento requerida para llevar a cabo el análisis sin pérdida significativa de paquetes. T define la cantidad de paquetes que van a ser procesados en un lapso de tiempo y define, como resultado de ello, la cantidad de procesamiento que puede ser asignada a cada paquete.

En sistemas conocidos, la cantidad de procesamiento aumenta de forma proporcional con el incremento del flujo N, en tanto en cuanto cada paquete contribuye al estado de un flujo y con ello impone una estructura de datos cuyo tamaño está relacionado con N. Es evidente, por tanto, que una estructura material determinada presentará un comportamiento relacionado con su rendimiento y configuración intrínsecos, lo que hará posible o bien incrementar N mediante la reducción de D, o bien incrementar D reduciendo N. En otras palabras, $N \times D$ permanece casi constante.

Sin embargo, la realidad y el progreso de las redes informáticas existentes es que N y T aumentan ambos proporcionalmente al mismo tiempo. Esto es, el tamaño y la velocidad del tráfico de red ya no es inversamente proporcional, sino que tanto N como T están aumentando. A ello se añade la vastedad y complejidad del flujo del tráfico que queda por vigilar y analizar.

La publicación de la solicitud de Patente estadounidense US2005/0083935 se refiere a un procedimiento y a un aparato para una clasificación de paquetes en dos etapas, incluyendo en el sistema de clasificación de paquetes en dos etapas una primera etapa y una segunda etapa. En la primera etapa de clasificación, un paquete es clasificado sobre la base de la trayectoria de red del paquete. En la segunda fase de clasificación, el paquete es clasificado sobre la base de uno o más campos de transporte (u otros) del paquete. Se divulgan también formas de realización de adaptación de filtros y de compartición de nivel de transporte de máxima concreción, y una u otra o ambas técnicas referidas pueden ser implementadas dentro del procedimiento de clasificación de dos etapas.

Por consiguiente, sería deseable desarrollar un procedimiento y un sistema novedosos para llevar a cabo análisis de flujo del tráfico eficientes, prácticos y mejorados destinados a redes informáticas para evaluar el flujo del tráfico denso y de alta velocidad, así como para llevar a cabo un análisis de protocolo mejorado para tecnologías emergentes, como por ejemplo aplicaciones VoIP (Voz sobre IP).

Sumario de la invención

De acuerdo con ello, constituye un objetivo de la invención proporcionar un sistema de análisis del tráfico para análisis del tráfico sobre un enlace de comunicaciones, y que ofrece unos circuitos analizadores conectados entre sí por una pluralidad de enlaces, donde cada circuito analizador tiene una velocidad de transmisión de datos menor que la velocidad de transmisión de datos del enlace de comunicaciones, y están adaptados para llevar a cabo unos respectivos niveles diferentes de análisis sobre los paquetes. La información extraída de los paquetes analizados en un primer nivel de análisis por un primer circuito analizador es reenviada a un segundo nivel de análisis llevado a cabo en un segundo circuito analizador, y del análisis adicional llevado a cabo por el segundo circuito analizador depende del análisis llevado a cabo por el primer circuito analizador.

Pueden también incluirse uno o más de los siguientes rasgos distintivos.

En un aspecto de la invención, los primero y segundo circuitos analizadores adaptados para llevar a cabo los respectivos diferentes niveles de análisis incluyen una memoria para recibir información del estado proporcionada por el análisis llevado a cabo por los primero y segundo circuitos analizadores.

En otro aspecto, los primero y segundo circuitos analizadores adaptados para llevar a cabo los respectivos niveles diferentes de análisis incluyen unos circuitos analizadores de niveles más bajo y más alto, respectivamente, donde el circuito analizador de nivel más bajo está adaptado para llevar un nivel explícito de análisis, mientras que el circuito analizador de nivel más alto está adaptado para llevar a cabo un nivel de análisis implícito.

En otro aspecto adicional más, el nivel explícito de análisis está adaptado para reconocer los protocolos para los cuales en la cabecera de los paquetes identifica suficientemente la información útil para formular una signature de los paquetes.

Así mismo, la invención proporciona también un procedimiento para el examen del flujo del tráfico de la red mediante la realización del análisis de los paquetes sobre un enlace de comunicaciones que conecta diversas redes, en el que el procedimiento establece unos niveles sucesivos de análisis dentro de un sistema de análisis del tráfico que incorpora unos circuitos analizadores adaptados para llevar a cabo unos niveles de análisis respectivos diferentes en diferentes gamas, y los circuitos analizadores están conectados entre sí mediante enlaces, cada uno de los cuales tiene una velocidad de transmisión de datos inferior que una velocidad de transmisión de datos del enlace de comunicaciones. El procedimiento así mismo reenvía los paquetes analizados por los circuitos analizadores, donde la información extraída de los paquetes analizados en un primer nivel de análisis por un primer circuito analizador es reenviada a un segundo nivel de análisis llevada a cabo en un segundo circuito analizador, y así sucesivamente, y el procedimiento utiliza el análisis llevado a cabo por el primer circuito analizador por el análisis llevado a cabo por el segundo circuito analizador subsecuente.

Otros rasgos distintivos de la invención se exponen con mayor detenimiento en las reivindicaciones dependientes.

Estos y otros aspectos del sistema y el procedimiento mejorados se pondrán de manifiesto a partir de la descripción subsecuente, de los dibujos, y a partir de las reivindicaciones.

Breve descripción de las figuras

La Figura 1 es un diagrama esquemático de un típico sistema de análisis del tráfico;

la Figura 2 es un diagrama esquemático de una primera implementación de acuerdo con la presente invención; y

la Figura 3 es un diagrama esquemático de otra implementación de la presente invención.

Descripción detallada

Con referencia a la Figura 2, un sistema 10 de análisis del tráfico incluye un analizador jerárquico 310 que sustituye al analizador 300 del sistema de análisis del tráfico de la Figura 1.

El analizador jerárquico 310 define unas capas sucesivas de análisis para el flujo del tráfico que atraviesa un enlace de comunicaciones 200' entre una primera red 100' y una segunda red 110'. Como resultado de ello, el analizador jerárquico 310 lleva a cabo un primer nivel de análisis sobre el flujo del tráfico, un segundo nivel de análisis es llevado a cabo por los analizadores 320a a 320n, y un tercer nivel de análisis se lleva a cabo por los analizadores 330i a 330j. El sistema 10 de análisis del tráfico puede tener tantos niveles y analizadores como sean necesarios para analizar y clasificar satisfactoriamente el tráfico que depende del tamaño y de la velocidad del flujo de los paquetes sobre el enlace de comunicaciones 200'.

El analizador jerárquico 310 y los analizadores 320a a 320n están conectados por los enlaces 202a a 202n, y el número de paquetes que pasa a través del enlace de comunicaciones 200' es mayor que el número de paquetes que pasa a través de los enlaces 202a a 202n.

Por ejemplo, en el primer nivel de análisis, el analizador jerárquico 310 lleva a cabo un primer nivel de clasificación, esto es, lleva a cabo las primeras operaciones para clasificar los paquetes de acuerdo con el tipo de paquetes, la identificación de cabecera, y operaciones similares. Así mismo, el analizador jerárquico 310 puede llevar a cabo un tipo explícito de análisis de protocolo como por ejemplo las técnicas de reconocimiento de patrones o la búsqueda de patrones.

Entre dichos protocolos explícitos se encuentra el protocolo Ethernet, donde una cabecera de paquetes de Ethernet especifica si el protocolo siguiente de la pila de protocolos es, por ejemplo, un protocolo de LLC o un protocolo de IP posiblemente junto con su versión. Así mismo, la cabecera de los paquetes bajo el control del IP especifica si el protocolo siguiente de la pila de protocolos es un Protocolo TCP, UDP, o ICMP. Aunque el primer nivel de análisis podría pertenecer a tipos explícitos de análisis de protocolo no está necesariamente limitado a ellos.

Una vez que el primer nivel de análisis llevado a cabo en el nivel inferior es llevado a cabo por el analizador jerárquico 310, los analizadores de segundo nivel, a saber, los analizadores 320a a 320n pueden examinar también los paquetes de acuerdo con la clasificación anterior efectuada por el analizador jerárquico 310 de primer nivel. En otras palabras, los analizadores 320a a 320n llevarán a cabo un tipo implícito de análisis a niveles más altos, lo que significa el reconocimiento de la presencia de protocolos implícitos. Se dice que un protocolo es implícito cuando no es fácilmente identificable de manera definida por una cabecera de protocolo que precede a este protocolo dentro de la pila de protocolos. Tal es el caso de los numerosos protocolos de los niveles de aplicación, como por ejemplo Pointcast o Kazaa, cuyo uso en la pila de protocolos de una conexión, depende del contexto de sus conexiones genéricamente establecido mediante negociaciones previas, que son difíciles de compilar con un escaneo en tiempo real a lo largo del flujo de paquetes que se desplaza alrededor de la conexión. Por ejemplo, determinados protocolos conocidos, como por ejemplo los protocolos HTTP, Telnet, FTP están en el límite de los protocolos implícitos y explícitos. Estos protocolos pueden considerarse como explícitos cuando un número de puerto reservado que figura en una cabecera de protocolo TCP proporciona un indicador de destino que hace posible identificar de manera definida el protocolo que es transportado, por ejemplo, un número 80 correspondiente al protocolo HTTP, un número 23, correspondiente al protocolo Telnet, un número 21 correspondiente al protocolo FTP. Una estación de cliente utiliza, por ejemplo, bajo el TCP, un número de puerto 80 para establecer una conexión de consulta del HTTP con una estación de servidor mediante la asignación de un número de puerto dinámico a una conexión entre pares que posibilite que la estación de servidor responda a la estación de cliente. La naturaleza explícita del protocolo HTTP a través de la conexión entre pares para acarrear las respuestas de la situación de servidor a la estación de cliente queda disminuida a través de la asignación dinámica de un número de puerto, relacionado con el contexto de la conexión de consulta. Así mismo, nada impide que una estación de cliente negocie de antemano con la estación de servidor, un número de puerto distinto del número 80 para la conexión de consulta del HTTP. En este caso, el protocolo HTTP es más implícito que explícito. Esto sigue siendo verdad para otros protocolos y la tecnología es capaz de gestionar esta situación.

A continuación, el segundo nivel de análisis enriquece el conocimiento proporcionado por el primer nivel de análisis, y así sucesivamente. A continuación, añadiendo niveles adicionales de análisis, como por ejemplo los analizadores 330i a 330j de tercer nivel, los analizadores 330i a 330j utilizan el análisis llevado a cabo en el segundo nivel precedente de análisis y enriquecen el nivel precedente con análisis adicionales propios.

Así mismo, como otro ejemplo de un primer nivel de análisis, podemos imaginar un primer nivel de análisis llevado a cabo por el primer analizador jerárquico 310 de primer nivel mediante el cálculo de una clave de refundición sobre el origen del IP, las direcciones de destino del IP, el código de transporte, el puerto de origen y el puerto de destino, y enviar los paquetes a los analizadores 320a a 320n para un segundo nivel de análisis donde se efectúe una clasificación utilizando los puertos de clasificación, dejando a los analizadores 330i a 330j la tarea de llevar a cabo un tercer nivel de clasificación perteneciente al reconocimiento semántico del flujo del tráfico. Por ejemplo, un reconocimiento semántico del flujo puede comportar la utilización de un gráfico del protocolo y un mecanismo de autoidentificación modular asociado con el protocolo para obtener elementos importantes de los paquetes a partir del tráfico, tal y como se describe en el documento WO 2004/017595.

Con referencia todavía a la Figura 2, todos los analizadores del sistema 10 de análisis del tráfico pueden compartir una memoria 400 que almacene el estado de la información relacionada con los análisis llevados a cabo. Por ejemplo, en el escenario anteriormente descrito, sería necesario que los analizadores 320a a 320n y los analizadores 330i a 330j compartieran la memoria común 400. De hecho, sería necesario que los analizadores 310, 320a a 320n, y 330i a 330j y todos los analizadores de niveles diferentes subsecuentes compartieran la misma memoria 400. Un ejemplo se produce cuando la visión de la tarea analítica se basa en el empleo de estadísticas de recursos procedentes de cada sensor.

Con referencia ahora a la Figura 3, en ella se representa otro sistema 20 de análisis del tráfico en el que un nivel jerárquico de análisis es implementado utilizando unidades de procesamiento independientes, ya sea combinando varias CPUs, como por ejemplo computadoras PC, mediante la utilización de una arquitectura de procesamiento paralela, por ejemplo, procesadores de red, ya sea de forma más global, mediante la utilización de otro tipo de mecanismo que posibilite la organización de capas de análisis sucesivas y la compartición de los datos relacionados.

La Figura 3 muestra un tráfico de datos bidireccional sobre un enlace de comunicación 200'' que pasa a través de un procesador de red 500 que agrega unos procesadores elementales 510a a 510x, conectados a una memoria 600, un módulo de almacenaje 700, y un microprocesador tradicional 800 por medio de un bus 900 de alto rendimiento.

Como se ilustra así mismo en la Figura 3, al analizar el tráfico de datos bidireccional para el análisis jerárquico, el análisis de comunicaciones 200'' recibe los paquetes entrantes 1000 en su extremo de entrada 205. Estos paquetes entrantes 1000 son primeramente analizados por uno de los procesadores elementales 510a a 510x en una etapa (210). Los paquetes entrantes 1000 son a continuación enviados en la memoria 600 en una etapa (220). Por ejemplo, si es necesario, los paquetes entrantes 1000 son a continuación duplicados sobre el enlace de comunicación 200'' en su extremo de salida 215 en una etapa (230). Este puede ser el caso cuando el análisis positivo se lleve a cabo, por ejemplo, con fines de vigilancia, pero no es el caso en otras aplicaciones como en aplicaciones de cortafuegos. En paralelo, las mismas etapas son acarreadas para los demás paquetes. A continuación, los paquetes 1000 almacenados en la memoria 600 son procesados por el microprocesador tradicional 800 en una etapa (240), el cual analizará los paquetes y describirá la información de estado en el módulo de almacenaje 700 en una etapa (250). Esta parte del análisis no implica a todos los paquetes, sino solo a una porción de ellos. Así mismo, el análisis de todos los paquetes entrantes 1000 puede efectuarse en paralelo y de manera independiente de la copia y duplicación así como del procesamiento de los paquetes utilizando el microprocesador tradicional 800.

Como un ejemplo, el microprocesador tradicional 800 puede llevar a cabo análisis pertenecientes a protocolos diferentes de análisis y analizar los paquetes en el contexto de diferentes protocolos, por ejemplo, protocolos implícitos vs. explícitos, con el fin de identificar con rapidez los paquetes y extraer información semántica útil sobre el flujo del tráfico, como por ejemplo la clasificación de una conexión de red mediante una estructura progresiva de una secuencia ordenada de los protocolos utilizados.

REIVINDICACIONES

1. Un sistema (10) de análisis del tráfico para llevar a cabo un análisis del tráfico de paquetes sobre un enlace de comunicaciones (200') que conecta una pluralidad de redes, en el que el sistema comprende:

- una pluralidad de circuitos analizadores (310; 320a a 320n; 330i a 330j) conectados entre sí por una pluralidad de enlaces (202a a 202n), teniendo cada uno de los cuales una velocidad de transmisión de datos inferior a una velocidad de transmisión de datos de dicho enlace de comunicaciones; y
- en el que la pluralidad de circuitos analizadores está adaptada para llevar a cabo unos niveles diferentes respectivos de un análisis de paquetes que circulan a lo largo de dicho enlace de comunicaciones, en el que la información extraída de los paquetes analizados en un primer análisis en un primer circuito analizador es reenviada a un segundo circuito de análisis llevado a cabo en un segundo nivel analizador, comprendiendo el segundo nivel al menos dos analizadores (320a a 320n) dispuestos para llevar a cabo un análisis paralelo, y el análisis adicional llevado a cabo por el segundo circuito analizador depende del análisis llevado a cabo por el primer circuito analizador, en el que los primero y segundo circuitos analizadores adaptados para llevar a cabo los niveles respectivos diferentes de un análisis comprenden unos circuitos analizadores de niveles más bajo y más alto, respectivamente, en el que el circuito analizador de nivel más bajo está adaptado para llevar a cabo un nivel de análisis explícito, mientras que el segundo analizador de nivel más alto está adaptado para llevar a cabo el nivel de análisis implícito, en el que el nivel de análisis implícito comprende el reconocimiento de la presencia de un protocolo, el cual no es fácilmente identificable de una manera definida mediante una cabecera de protocolo, la cual precede a este protocolo dentro de una pila de protocolos, mientras que el nivel de análisis explícito comprende el reconocimiento de la presencia de un protocolo, el cual es fácilmente identificable de una manera definida por la cabecera del protocolo, la cual precede a este protocolo dentro de la pila de protocolos.

2. El sistema de acuerdo con la reivindicación 1, en el que los primero y segundo circuitos analizadores adaptados para llevar a cabo los niveles de análisis respectivos diferentes comprenden una memoria común (400) para recibir la información de estado proporcionada por el análisis llevado a cabo por los primero y segundo circuitos analizadores.

3. El sistema de acuerdo con la reivindicación 1, en el que el nivel de análisis explícito está adaptado para reconocer unos protocolos para los cuales la cabecera de un paquete identifica de manera suficiente la información útil para formular una signature de paquete.

4. El sistema de acuerdo con la reivindicación 1, que comprende así mismo un procesador de red (500) que agrega unos procesadores elementales (510a a 510x); una memoria (600); y un módulo de almacenaje (700) conectados por medio de un bus de comunicación (900).

5. El sistema de la reivindicación 4, en el que el procesador de red comprende una arquitectura de procesamiento en paralelo.

6. Un procedimiento para examinar el flujo del tráfico de una red mediante la realización de un análisis de paquetes sobre un enlace de comunicaciones (200') que conecta una pluralidad de redes, en el que el procedimiento comprende:

- el establecimiento de unos niveles sucesivos de análisis dentro de un sistema (10) de análisis del tráfico que comprende una pluralidad de circuitos analizadores adaptados para llevar a cabo unos niveles respectivos diferentes de análisis en diferentes capas, en el que varios circuitos analizadores (310; 320a a 320n; 330i a 330j), están conectados entre sí por una pluralidad de enlaces (202a a 202n), cada uno de los cuales tiene una velocidad de transmisión de datos inferior a una velocidad de transmisión de datos de dicho enlace de comunicaciones;
- el reenvío de los paquetes analizados por los diferentes circuitos analizadores, en el que la información extraída de los paquetes analizados en un primer nivel de análisis por un primer circuito analizador es reenviado a un segundo nivel de análisis llevado a cabo en un segundo circuito analizador, comprendiendo el segundo nivel al menos dos analizadores (320a a 320n) dispuestos para llevar a cabo análisis paralelos, y así sucesivamente; y
- la utilización del análisis llevado a cabo por el primer circuito analizador para el análisis llevado a cabo por el segundo circuito analizador en los que los primero y segundo circuitos analizadores están adaptados para llevar a cabo unos respectivos niveles diferentes de análisis que comprenden unos circuitos analizadores de nivel más bajo y más alto, respectivamente, en el que el circuito analizador de nivel más bajo está adaptado para llevar a cabo un nivel explícito de análisis, mientras que el circuito analizador de nivel más alto está adaptado para llevar a cabo un nivel implícito de análisis, en el que el nivel implícito de análisis comprende el reconocimiento de la presencia de un protocolo, el cual no es fácilmente identificable de manera definida por una cabecera de protocolo, el cual precede a este protocolo dentro de una pila de protocolos, mientras que el nivel explícito de análisis comprende el reconocimiento de la presencia de un protocolo; el cual es fácilmente identificable de manera definida mediante una cabecera de protocolo, el cual precede a este protocolo dentro de la pila de protocolos.

ES 2 323 244 T3

7. El procedimiento de la reivindicación 6, en el que el establecimiento de niveles sucesivos de análisis comprende la definición del primer nivel de análisis llevado a cabo por el primer circuito analizador mediante la clasificación de los paquetes por refundición de su dirección de origen o signatura y el reenvío de los paquetes clasificados hasta el circuito analizador de segundo nivel en el segundo nivel de análisis.

8. El procedimiento de las reivindicaciones 6 y 7, en el que el procedimiento comprende así mismo la provisión de un reconocimiento semántico del flujo del tráfico en base al análisis llevado a cabo por los primero y segundo niveles de análisis.

9. El procedimiento de las reivindicaciones 6 a 8, que comprende así mismo las etapas de:

- el análisis (210) de los paquetes entrantes (1000) que llegan al extremo entrante (205) del enlace de comunicaciones, mediante al menos uno de los procesadores elementales (510a a 510x);
- la copia (220) de los paquetes dentro de la memoria;
- el procesamiento (240) de los paquetes almacenados en la memoria utilizando un procesador para analizar los paquetes e inscribir (250) la información de estado en un módulo de almacenaje; y
- la realización del análisis para todos los paquetes entrantes en paralelo y con independencia de la copia, la duplicación, y las etapas de procesamiento.

10. El procedimiento de la reivindicación 9, en el que el procedimiento comprende así mismo la duplicación (230) de los paquetes sobre un enlace de salida (215) del enlace de comunicaciones.

