(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 625 542**

(51) Int. CI.:

H04L 12/26 (2006.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **21.03.2013 PCT/US2013/033361**

(87) Fecha y número de publicación internacional: **03.10.2013 WO13148472**

(96) Fecha de presentación y número de la solicitud europea: **21.03.2013 E 13717364 (7)**

(97) Fecha y número de publicación de la concesión europea: **08.03.2017 EP 2832043**

(54) Título: **Vigilancia de desempeño de red de comunicaciones cifradas**

(30) Prioridad:

28.03.2012 US 201213432847

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
19.07.2017

(73) Titular/es:

BMC SOFTWARE, INC. (100.0%)
2103 City West Boulevard
Houston,Texas 77042, US

(72) Inventor/es:

DESCHENES, DANNY;
HSY, JOE PEI-WEN y
LAROSE, PIERRE

(74) Agente/Representante:

ISERN JARA, Jorge

DESCRIPCIÓN

Vigilancia de desempeño de red de comunicaciones cifradas

CAMPO TÉCNICO

Esta descripción se refiere al desempeño de una red y más específicamente la vigilancia y análisis del desempeño de comunicaciones entre dos dispositivos de red.

ANTECEDENTES

En un modelo de software tradicional, los grupos de tecnología de información (TI) corporativos compran software, desplegar el software, y gestionar el software en su propio centro de datos. En dicho modelo, el grupo TI es responsable del desempeño y disponibilidad de aplicaciones o del software comprado. Tradicionalmente, dichos grupos de TI utilizan herramientas para vigilar las aplicaciones de software con el fin de asegurar la disponibilidad y desempeño consistentes.

El software como un servicio (SaaS), se denomina en ocasiones como “software bajo demanda” o “software en la nube”, normalmente es un modelo de suministro de software en que el software y sus datos asociados se alojan centralmente (normalmente en Internet o la nube) y normalmente los usuarios tienen acceso a partir de un dispositivo de cómputo (por ejemplo, ordenadores de escritorios, laptops, netbooks, ordenadores tipo tableta, teléfonos inteligentes, etcétera) que utilizan un explorador de red sobre la internet. El SaaS ha llegado a ser un modelo de suministro común para muchas aplicaciones comerciales, que incluyen contabilidad, cooperación, gestión de relación con el cliente (CRM), planeación de recursos de la empresa (ERP), facturación, gestión de recursos humanos (HRM), gestión de contenidos (CM) y gestión de servicios, etc. El SaaS se ha incorporado en la estrategia de muchas compañías líderes de software empresarial.

Sin embargo, en el modelo de servicios SaaS, en el que el software se proporciona frecuentemente como un servicio de un tercero, las organizaciones de usuario final frecuentemente se suscriben directamente con un proveedor de software. Como tal, un usuario final hace contacto directamente en general con el proveedor SaaS para proporcionar el software con un determinado nivel de disponibilidad o desempeño.

Sin embargo, frecuentemente los usuarios finales ni tienen las habilidades ni los recursos económicos para rastrear activamente dichos niveles de servicio SaaS. Ni en general tendrían las herramientas para hacer seguimiento a dichos niveles incluso si lo desearan. Frecuentemente, no existen acuerdo de nivel de servicio consistente (SLA) de una perspectiva corporativa e incluso cuando existen SLA, existen pocas herramientas para hacer seguimiento al desempeño y mucho menos para hacer cumplir los niveles de servicio. Como tal, las empresas frecuentemente no pueden contar con sus grupos de TI para que sean responsables de las operaciones y gestión de las aplicaciones de misiones críticas. Frecuentemente, el grupo TI se reduce para soportar solamente la red y el acceso de escritorio a los proveedores SaaS, y no el desempeño de las aplicaciones SaaS propiamente dichas. Frecuentemente, los proveedores SaaS son ahora responsables del desempeño de las aplicaciones y los grupos de TI corporativos incluso pueden no tener una relación directa con el proveedor SaaS.

RESUMEN

De acuerdo con un aspecto general, un método para utilizar un primer dispositivo de sondeo puede incluir vigilar una o más sesiones de comunicaciones cifradas entre un primer dispositivo de cómputo y un segundo dispositivo de cómputo. En algunas implementaciones del método, cada sesión de comunicaciones cifradas incluye transmitir una pluralidad de objetos de datos cifrados entre el primero y segundo dispositivos de cómputo. El método puede incluir derivar, mediante el primer dispositivo de sondeo, información de tiempo con respecto a una sesión de comunicaciones cifradas. El método puede incluir también transmitir, desde un primer dispositivo de sondeo hasta un segundo dispositivo de sondeo, la información de tiempo derivada.

De acuerdo con otro aspecto general, un sistema puede incluir unos primeros y segundos puntos de conexión de red y un dispositivo de sondeo del lado del cliente. El primer punto de conexión de red se puede configurar para duplicar, de en una forma no intrusiva, por lo menos porción de una comunicación de red cifrada transmitida hacia y desde un dispositivo de punto de acceso que forma el límite entre una primera red y una segunda red. El segundo punto de acceso de red se puede configurar para duplicar, en una forma no intrusiva, por lo menos porción de una comunicación de red cifrada transmitida hacia y desde un dispositivo de cómputo servidor colocado dentro de, en un sentido de topología de red, la segunda red. El dispositivo de sondeo de lado del cliente se puede configurar para vigilar las sesiones de comunicaciones cifradas entre el dispositivo de cómputo del servidor y el dispositivo de cómputo del cliente, en el que cada sesión de comunicaciones cifradas incluye transmitir una pluralidad de objetos de datos cifrados entre los dispositivos de cómputo de cliente y de servidor. El dispositivo de sondeo de lado del cliente se puede configurar para derivar información de tiempo con respecto a sesiones de comunicación cifradas basadas en uno o más objetos de datos cifrados recibidos incluidos por la sesión de comunicaciones cifradas. El dispositivo de sondeo de lado del cliente se puede configurar para transmitir, a un dispositivo de sondeo de lado del servidor, la información de tiempo derivada.

De acuerdo con otro aspecto general, un producto de programa de ordenador para gestionar una red se puede incorporar en forma tangible y no transitoria sobre un medio legible por ordenador. El programa de ordenador puede incluir un código ejecutable que, cuando se ejecuta, se configura para provocar que un aparato vigile sesiones de comunicaciones cifradas entre un primer dispositivo de cómputo y un segundo dispositivo de cómputo, en el que cada sesión de comunicaciones cifradas incluye transmitir una pluralidad de objetos de datos cifrados entre los primeros y segundos dispositivos de cómputo. El código ejecutable provoca que el aparato derive, mediante el aparato, información de tiempo con respecto a una sesión de comunicaciones cifradas basadas en uno o más objetos de datos cifrados recibidos incluidos por la sesión de comunicaciones cifrada. El código ejecutable puede provocar que el aparato transmita, desde un aparato hasta un segundo aparato, la información de tiempo derivada.

Los detalles de una o más implementaciones se establecen en los dibujos acompañantes y la descripción adelante. Otras características serán evidentes a partir de la descripción y dibujos, y de las reivindicaciones.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

La figura 1 es un diagrama de bloques de una realización de ejemplo de un sistema de acuerdo con la materia objeto divulgada.

La figura 2 es un diagrama de bloques de una realización de ejemplo de un sistema de acuerdo con la materia objeto divulgada.

La figura 3 es un diagrama de bloques de una realización de ejemplo de un sistema de acuerdo con la materia objeto divulgada.

La figura 4 es un diagrama de tiempo de una realización de ejemplo de un sistema de acuerdo con la materia objeto divulgada.

La figura 5 es un diagrama de tiempo de una realización de ejemplo de un sistema de acuerdo con la materia objeto divulgada.

La figura 6 es un diagrama de flujo de una realización de ejemplo de una técnica de acuerdo con la materia objeto divulgada.

Símbolos de referencia similares en los diversos dibujos indican elementos similares.

DESCRIPCIÓN DETALLADA

La figura 1 es un diagrama de bloques de una realización de ejemplo de un sistema 100 de acuerdo con la materia objeto divulgada. En diversas realizaciones, el sistema 100 puede incluir dos o más redes de comunicaciones. En la realización ilustrada, el sistema 100 puede incluir una intranet 196 y una internet 195. Sin embargo, se entiende que lo anterior solamente es un ejemplo ilustrativo al que no se limita la materia objeto divulgada. Adicionalmente, se entiende que, aunque se ilustran dos redes o segmentos 195 y 106 de red, la materia objeto divulgada no se limita a cualquier número de dichos segmentos de red o redes.

En diversas realizaciones, el sistema 100 puede incluir una primera red de comunicaciones (por ejemplo, intranet 196, etc.) que incluye un dispositivo 102 de cómputo de cliente. Normalmente, esta primera red 196 de comunicaciones puede estar bajo el control de un grupo TI único o unidad de negocio. En diversas realizaciones, el sistema 100 puede incluir una segunda red de comunicaciones (por ejemplo, internet 195, etc.) que incluye, por lo menos desde el punto de vista del dispositivo 102 de cómputo de cliente, el dispositivo 106 de cómputo de servidor. Normalmente, esta segunda red 195 de comunicaciones puede no estar bajo el control del grupo TI o unidad de negocio. Se entiende que lo anterior solamente son pocos ejemplos ilustrativos a los que no se limita la materia objeto divulgada.

En diversas realizaciones, el sistema 100 puede incluir un dispositivo de cómputo de servidor o servidor 106 configurado para proporcionar un servicio (por ejemplo, un servidor web, una aplicación SaaS, etc.). En una realización, el dispositivo 106 de cómputo servidor puede incluir un procesador, memoria e interfaz de red (no mostrado, pero análogo aquellos del dispositivo 104 o 108). En la realización ilustrada, el dispositivo 106 de cómputo servidor puede proporcionar e incluir la aplicación 180 de negocios y los datos de 182 aplicación de negocios. En diversas realizaciones, esta aplicación 180 de negocios puede incluir una aplicación SaaS (por ejemplo, una CRM, una ERP, una HRM, un CM, etc.). Se entiende que, aunque se ilustra un servidor 106, la materia objeto divulgada no se limita a ningún número de dichos dispositivos.

En una realización, el dispositivo de cómputo ilustrado como servidor 106 puede incluir cualquier dispositivo de pares (por ejemplo, cliente o servidor, etcétera) que comunica, por lo menos parcialmente, sobre una vía de un protocolo cifrado (por ejemplo, protocolo de Capa de Conexión Segura (SSL), protocolo de seguridad de capa de transporte (TLS), etc.). Adicionalmente, aunque la comunicación entre los dispositivos 106 y 102 se describen en general que implican el protocolo de transferencia de hipertexto (HTTP) y/o el protocolo seguro HTTP (HTTPS), se entiende que lo

anterior son sólo pocos ejemplos ilustrativos a los que no se limita materia objeto divulgada. Finalmente, se entiende que los dispositivos 102, 104, 106, 108, 108b, y 109 pueden incluir ejemplos de dichos dispositivos incluidos en entornos virtuales o modulares respectivos (por ejemplo, un sistema de servidor blade, máquinas virtuales, etc.).

En diversas realizaciones, el sistema 100 puede incluir un dispositivo de cómputo cliente o cliente 102 configurado para consumir o hacer uso de servicio (por ejemplo, aplicación 180 de negocios aplicación SaaS, etcétera) proporcionado por el servidor 106. En una realización, el cliente 102 puede incluir un procesador, memoria, e interfaz de red (no mostrada, pero análoga a aquellas del dispositivo 104 o 108). En diversas realizaciones, el cliente 102 puede incluir o ejecutar una aplicación 130 (por ejemplo, un explorador web, etc.) que tiene acceso o visualiza el servicio o aplicación 180 proporcionada por el servidor 106. En algunas realizaciones, el cliente 102 puede ser controlado o utilizado por un usuario 190. En diversas realizaciones, el cliente 102 puede incluir un ordenador tradicional (por ejemplo, un ordenador de escritorio, laptop, netbook, etc.) o un dispositivo de cómputo no tradicional (por ejemplo, teléfono inteligente, ordenador tipo tableta, terminal de ordenador, cliente delgado, etc.). Se entiende que, aunque sólo se ilustra un cliente 102 la materia objeto divulgada no se limita a ningún número particular de dispositivos 102 de cliente.

En diversas realizaciones, el sistema 100 puede incluir un dispositivo de punto de acceso (PA) o dispositivo 104 PA intranet/internet. En dicha realización, el dispositivo 104 PA se puede configurar para separar la primera y segunda redes (por ejemplo, intranet 196 e internet 195, etc.). En diversas realizaciones, el dispositivo 104 PA puede incluir un enrutador, un cortafuego, un servidor proxy, etc., o una combinación de los mismos. Se entiende que los anteriores son sólo unos pocos ejemplos ilustrativos a los que no se limita la materia objeto divulgada.

En diversas realizaciones, el dispositivo 104 PA puede incluir un procesador 152 configurado para ejecutar una un flujo de datos o instrucciones ejecutables por maquina (por ejemplo, sistema operativo, aplicación 158, etc.). El dispositivo 104 PA puede incluir una memoria 154 configurada para almacenar datos y/o instrucciones. En diversas realizaciones, la memoria 154 puede incluir memoria volátil, memoria no volátil, o una combinación de las mismas. La memoria 154 o porciones de las mismas se pueden configurar para almacenar datos en forma temporal (por ejemplo, memoria de acceso aleatorio (RAM), etc.) como porción de la ejecución de instrucciones por porción del procesador 152. La memoria 154 o porciones de la misma se pueden configurar para almacenar datos en una forma semipermanente o a largo plazo (por ejemplo, una unidad física, memoria de estado sólido, memoria flash, almacenamiento óptico, etcétera).

En diversas realizaciones, el dispositivo 104 PA puede incluir uno o más interfaces 156 de red configuradas para comunicarse con otros dispositivos (por ejemplo, servidor 106, cliente 102, etc.) a través de una red de comunicaciones. En diversas realizaciones, esta red de comunicaciones puede emplear protocolos cableados (por ejemplo, Ethernet, Canal de Fibra, etc.) o inalámbricos (por ejemplo, Wi-Fi, celular, etc.) o protocolos estándares o una combinación de los mismos.

En una realización, el dispositivo 104 PA puede incluir un dispositivo o una aplicación 158 PA que actúa como intermediario entre el cliente 102 y el servidor 106. En una realización ilustrada, que ilustra el dispositivo 104 PA como un servidor proxy, el cliente 102 puede hacer una solicitud al dispositivo 104 PA para tener acceso al servidor 106 a nombre del cliente 102. En dicha una realización, el dispositivo 104 PA puede luego reenviar (frecuentemente reempacar o encapsular) la comunicación del cliente 102 al servidor 106. Del mismo modo, el servidor 106 puede hacer contacto con el dispositivo 104 PA con información o datos de que este se reenvía al cliente 102.

En dicha una realización, la comunicación entre el servidor 106 y el cliente 102 puede tener lugar en dos porciones. Una porción de lado del cliente o porción puede ocurrir entre el cliente 102 y el dispositivo 104 PA con la intranet 196. Puede ocurrir una porción del lado del servidor entre el servidor 106 y el dispositivo 104 PA a través de la internet 195. En combinación, estas porciones laterales cliente y servidor pueden constituir la comunicación entre dos dispositivos 102 y 106 a través de dos redes 195 y 196.

Frecuentemente, uno o ambos de estas porciones del lado del cliente y lado del servidor se pueden cifrar. En dicha una realización, cada una de las porciones cifradas respectivas de la comunicación de red pueden incluir sus claves de cifrado respectivas o credenciales de seguridad.

Por ejemplo, la comunicación entre el servidor 106 y el cliente 102 se puede cifrar a través del protocolo de transferencia de hipertexto (HTTP) protocolo seguro (HTTPS) que hace uso de los protocolos de Capa de Conexión Segura (SSL) y/o protocolos de seguridad de capa de transporte (TLS) para proporcionar comunicación cifrada y identificación segura entre dos dispositivos conectados en red. Se entiende que lo anterior sólo es un ejemplo ilustrativo al que la materia objeto divulgada no se limita.

En la realización ilustrada, un departamento TI u otra entidad puede desear vigilar y analizar las comunicaciones de red entre el cliente 102 y el servidor 106. Con el fin de hacer esto, el departamento de TI u otra entidad puede colocar una conexión de red o punto 107 de sonda en una red (por ejemplo, 196, etc.). En este contexto, un “punto de conexión de red” o “punto de sonda de red” incluye unos medios sustancialmente no invasivos de ver o vigilar las comunicaciones de red a través de una porción de la red en donde se ha colocado el punto 107 de conexión de red. En la realización ilustrada, el punto 107 de conexión de red se coloca de tal manera que cualquier comunicación de red transmitida o recibida por el servidor 106 se vigila y observa.

Sin embargo, colocar un único punto 107 de conexión de red en el lado 195 de internet del dispositivo 104 PA puede no ser una realización preferida. En diversas realizaciones, esto puede ser porque un único punto de conexión cerca al servidor (por ejemplo, punto 107 de conexión, etc.) puede no proporcionar visibilidad en cuanto a qué segmento de red de los segmentos múltiples potenciales entre 102 y 106 pueden ser el segmento de cuello de botella. Se entiende que lo anterior es sólo un ejemplo de ilustración al que no se limita la materia objeto divulgada. En diversas realizaciones, entre más segmentos de red existan se pueden desear más puntos de conexión.

Por ejemplo, en la realización ilustrada, un segundo punto 107b de sonda o de conexión se puede colocar de tal manera que cualquier comunicación de red que atraviese el dispositivo 104 PA se puede observar o vigilar. En diversas realizaciones, los puntos de conexión adicionales o una pluralidad o una pluralidad de puntos de conexiones se pueden agregar a través del sistema. Por ejemplo, se puede agregar un tercero o cuarto puntos de conexión (no mostrados) en puntos estratégicos o deseables dentro del sistema para controlar u obtener medidas de desempeño para segmentos de red adicionales (por ejemplo, entre el cliente 102 y el dispositivo 104 PA, etc.). En diversas realizaciones, el punto 107b y/o los puntos de conexión adicionales (no mostrados) pueden ser similares o análogos al punto 107 de conexión divulgado aquí. Otra realización se muestra y discute con referencia a la figura 2, como se describe adelante. Se entiende que lo anterior son sólo ejemplos de ilustración a los que no se limitan la materia objeto divulgada.

En diversas realizaciones, el punto 107 de sonda o conexión de red puede incluir una conexión física que divide o duplica una señal de red entrante y por lo tanto, cualquier comunicación de red transmitida a través de esa señal de red en dos o más señales de red salientes. En dicha una realización, una de las señales de red salientes se puede trasmitir a su destino normal (por ejemplo, dispositivo 104 PA o el dispositivo 102 de cliente, etc.) y la segunda señal de red saliente se puede trasmitir a un dispositivo de escucha intromisión o conexión (por ejemplo, dispositivo 108 de sondeo, etc.). En dicha realización, cualquier retardo agregado a la señal de comunicaciones de red puede ser mínimo o sustancialmente insignificante y la señal de red puede ser inalterada o no procesada. Como tal, el punto 107 de conexión de red se puede realizar en una forma sustancialmente no intrusiva.

En diversas realizaciones, los puntos 107 y 107b de conexión de red se pueden colocar cerca, en un sentido de topología de red, al dispositivo 106 servidor o, respectivamente, el dispositivo 104 PA con el fin de capturar o duplicar el pasaje de comunicación de red entre el dispositivo 106 servidor y el dispositivo 102 de cliente a través del dispositivo 104 PA o a través del límite entre las dos redes (por ejemplo, un límite de internet 195/intranet196, etc.). En la realización ilustrada, los puntos 107 y 107b de conexión de red pueden proporcionar una vista de la comunicación de la red de servidor106/cliente 102 desde un punto de vista más cercano al cliente 102 o al dispositivo 104 PA (punto 107b de conexión) y el servidor 106 (punto 107 de conexión). Se entiende que lo anterior es solamente un ejemplo de ilustración al que no se limita la materia objeto divulgada.

En una realización, el dispositivo 108 de sondeo puede incluir un procesador 112, memoria 114, e interfaz de red 116, análogos a aquellos descritos anteriormente. Como se describió anteriormente, en diversas realizaciones, la memoria 114 puede incluir almacenamiento volátil (por ejemplo, memoria de acceso aleatorio, etc.), almacenamiento no volátil (por ejemplo, una unidad física, una unidad de estado sólido, etc.) o una combinación de las mismas. En algunas realizaciones, el dispositivo 108 de sondeo puede incluir un punto 107 de sondeo o conexión de red.

En diversas realizaciones, el dispositivo 108 de sondeo se puede configurar para vigilar y analizar la comunicación de red cifrada y/o no cifrada. En dicha realización, el dispositivo 108 de sondeo puede generar un grupo de medidas 122 que se relacionan con el desempeño de la comunicación de red entre el cliente 102 y el servidor 106. Estas medidas 122 se pueden transmitir o visualizar dentro de una interfaz de usuario (IU) 142 de una aplicación 140 TI que se ejecuta por un dispositivo 109 de cómputo TI. En diversas realizaciones, él dispositivo 109 de cómputo de TI puede incluir un ordenador tradicional (por ejemplo, un ordenador escritorio, laptop, netbook, etc.) o un dispositivo de cómputo no tradicional (por ejemplo, teléfono inteligente, tableta, terminal de ordenador de cliente delgado, etc.).

En la realización ilustrada, el dispositivo 108 de sondeo se puede configurar para recibir o vigilar tráfico capturado mediante el punto 107 de contacto sobre el lado del servidor. Por el contrario, el dispositivo 108b de sondeo se puede configurar para recibir o vigilar tráfico capturado por el punto 107b de contacto sobre el lado del cliente. En diversas realizaciones, el dispositivo 108b de sondeo puede incluir elementos y realizar algunas o todas las funciones en forma similar dispositivo 108 de sondeo, como se describe aquí. En otra realización, tal como aquella tratada con referencia a la figura 2, los dispositivos 108 y 108b de sondeo pueden realizar funciones similares pero diferentes o incluir elementos diferentes. Se entiende que lo anterior sólo es un ejemplo de ilustración al que no se limita la materia objeto divulgada.

En una realización, el dispositivo 108 de sondeo puede incluir un monitor 118 de tráfico configurado para vigilar la comunicación de red capturada o duplicada por el punto 107 de contacto de red. En diversas realizaciones, esta comunicación de red puede incluir comunicación de red cifrada entre el cliente 102 y el servidor 106. En la realización ilustrada, la comunicación cifrada puede incluir una porción de la comunicación cliente/servidor que ocurre entre el cliente 102 y el dispositivo 104 PA. En una realización más preferida (por ejemplo, el sistema 200 de la figura 2), el punto 107 de contacto se puede colocar para capturar comunicación cifrada entre el servidor 106 y el dispositivo 102 de cliente. Se entiende que lo anterior sólo son unos ejemplos ilustrativos a los que no se limita la materia objeto divulgada.

En algunas realizaciones, como se describe adelante con referencia a la figura 2, el monitor 118 de tráfico del dispositivo 108 de sonde de servidores se puede configurar para descifrar todo o porción de la comunicación de red capturada por uno o más puntos de contacto de red. En otras realizaciones, como se describe adelante con referencia a la figura 2, el dispositivo 108 de sondeo se puede configurar para descifrar todo o porción de la comunicación de red capturada por el punto 107 de contacto de red y puede vigilar y analizar dicho tráfico.

Por el contrario, el dispositivo 108b de sondeo del lado del cliente puede no estar configurado para descifrar cualquiera o porción de la comunicación de red capturada por el punto 107b de contacto de red, pero puede aún vigilar y analizar dicho tráfico. En diversas realizaciones, se puede evitar que el dispositivo 108b de sondeo sea capaz de descifrar las comunicaciones de red debido a un cifrado privado clave asociado con el dispositivo 106 de servidor (ilustrado en la figura 2) que permanece dentro del dispositivo servidor por motivos de seguridad.

En dicha una realización, el dispositivo 108 de sondeo se puede configurar para descifrar la comunicación de red debido a que este se encuentra dentro del dominio (por ejemplo, centro de datos seguro del dispositivo 106 servidor, etc.) y se puede confiar con la clave de cifrado privada, mientras que el dispositivo 108b de sondeo del lado del cliente (y otros puntos de contacto, como se describe adelante) normalmente están afuera o en el exterior del dominio (por ejemplo ,fuera del centro de datos seguro, etc.) y no tienen acceso a la clave de cifrado privada que se utiliza para descifrar la comunicación de red. Esta capacidad para descifrar por lo menos el tráfico comunicación de red cifrado se contrastada con los esquemas de vigilancia de comunicación de red tradicionales que generalmente descartan o no vigilan las comunicaciones de red cifradas como el analizador 120 u otras porciones de los dispositivos 108 y/p 108b de sondeo que son incapaces de procesar comunicaciones de red cifradas.

En una realización, el dispositivo 108 de sondeo puede incluir un analizador 120 de tráfico configurado para analizar la comunicación de red vigilada y generar el grupo de medidas 122. En diversas realizaciones, el grupo de medidas 122 puede incluir información, tal como, la latencia agregada a la intranet 196 o el dispositivo 104 PA, el desempeño de diversos servidores 106, la disponibilidad del servidor 106, el número de accesos o páginas web requeridas de/proporcionadas por el servidor 106, el número de errores, retransmisiones, o interacciones de comunicación de red fallidas (por ejemplo, páginas web vistas, etc.) entre el dispositivo 102 de cliente y el servidor 106, un valor de calidad general de la comunicación de red (por ejemplo, una medición sintética o agregada de latencia y errores, etc.), el uso de ancho de banda que implica el servidor 106 o el cliente 102, una determinación de dónde en la red (por ejemplo, el servidor 106, el dispositivo 104 PA, el cliente 102, etc.) cualquier error ocurre, el número de veces que el servidor 106 es accesado (por ejemplo, vistas de página, etc.) en un período de tiempo dado, el número de dispositivos 102 de cliente que tienen acceso al servidor 106 en cualquier momento dado o período de tiempo, medidas de desempeño para cada uno de una pluralidad de servidores 106 o intranets 196, etc. En diversas realizaciones, estas medidas se pueden compiladas para la comunicación cliente/servidor general, comunicaciones que implican solo una de las redes (por ejemplo, dispositivo servidor a PA, dispositivo cliente a PA, etc.), o una combinación de los mismos. Se entiende que lo anterior son sólo unos pocos ejemplos ilustrativos a los que no se limita la materia objeto divulgada.

Como se describió anteriormente, en diversas realizaciones, se puede configurar el analizador 120 de tráfico para que coincida o se correlacione con la comunicación de red de un lado (por ejemplo, lado de cliente) del límite de internet 195/intranet 196 con la comunicación de red del otro lado (por ejemplo, lado del servidor) del límite de internet 195/intranet 196. Como se describe adelante, esto puede incluir comunicación de red de emparejamiento de dos puntos 107 y 107b de conexión (o puntos de conexión adicionales que dependen de la realización) basado en un grupo predeterminado de criterios. En diversas realizaciones, la comunicación de red vigilada o capturada (el lado del servidor) se puede cifrar y el dispositivo 108 de sondeo puede no ser capaz de descifrar esa porción de la comunicación de red vigilada. En dicha realización, el analizador 120 de tráfico puede aún ser configurado para que coincida o se correlacione, como mejor sea, las dos porciones (por ejemplo, lado del servidor y lado del cliente) de la comunicación de red.

En diversas realizaciones, el dispositivo 108 de sondeo puede incluir un Generador 124 de medidas configurado para generar un grupo de medidas 122 y, en algunas realizaciones, el Generador 124 de medidas también se puede configurar para generar un grupo de información 123 de tiempo (u otros estadísticos) que se relaciona con las comunicaciones vigiladas por el dispositivo 108 de sondeo.

En una realización, el dispositivo 108b de sondeo del lado del cliente también puede incluir un Generador 124 de medidas (y otros componentes similares al dispositivo 108 de sondeo, que no se muestran explícitamente debido a consideraciones de espacio). En dicha realización, el dispositivo 108b de sondeo del lado del cliente puede no configurarse para descifrar las comunicaciones de red cifradas, pero puede ser capaz de generar o derivar información 123b de tiempo en función de las comunicaciones de red cifradas vigiladas a través del punto 107b de conexión. Adelante se describen diversas técnicas para generar dicha información 123b de tiempo con referencia a las figuras 4 y 5.

En algunas realizaciones, los dispositivos 108 y 108b analizadores de puntos de conexión se puede configurar para generar información 123 y 123b de tiempo para diversas porciones de la comunicación de red que son vigiladas por el dispositivo de sondeo particular. En dicha realización, un dispositivo de sondeo particular (dispositivo 108b de sondeo) puede no ser capaz de descifrar la comunicación de red cifrada y, por lo tanto, puede no ser capaz de generar medidas

122 detalladas o información 123 de tiempo como se desea. En dicha realización, el dispositivo de sondeo particular (por ejemplo, dispositivo 108b de sondeo) se puede configurar para transmitir esta información 123b de tiempo al segundo dispositivo de sondeo u otro dispositivo (por ejemplo, dispositivo 108 de sondeo).

Como se describe adelante con referencia a la figura 2, el segundo dispositivo de sondeo o sondeo de recepción (por ejemplo, dispositivo 108 de sondeo) se puede configurar para descifrar las comunicaciones de red cifradas que vigila. En dicha realización, esté o por lo menos su analizador 120 de tráfico se puede configurar para que coincida o se asocie con la información 123b de tiempo recibida con las comunicaciones de red descifradas que vigila o la información 123 de tiempo derivada del mismo. En dicha realización, al combinar la información proporcionada por la información 123 y 123b de tiempo recibida y las comunicaciones de red vigiladas localmente se puede generar un grupo más completa de medidas 122.

Por ejemplo, un objeto de dato sencillo o transacción de comunicaciones puede incluir una vista de página web que tienen una fase de solicitud, cumplimiento y reconocimiento. Esa comunicación de vista de página web puede incluir dos porciones: una porción del lado del cliente entre el cliente 102 y el dispositivo 104 PA, y una porción del lado del servidor entre el servidor 106 y el dispositivo 104 PA. Tanto la porción del lado del cliente y como la porción del lado del servidor pueden tener sus propias medidas de desempeño respectivas (por ejemplo, latencia, etc.). Debido a que la comunicación de vista de página web se divide en dos porciones (lado del cliente y lado del servidor) puede no ser posible medir directamente, por ejemplo, la latencia o el tiempo desde el inicio hasta el final de la comunicación de vista de página web como se mide del cliente 102 al servidor 106. Sin embargo, si los dos lados o porciones de la comunicación coinciden, se puede determinar la latencia de cliente/servidor con base en la latencia del dispositivo cliente/PA (latencia del lado del cliente) y la latencia del dispositivo PA/servidor (latencia del lado del servidor), ambas se pueden medir directamente. Se entiende que lo anterior es solamente un ejemplo ilustrativo al que no se limita la materia objeto divulgada.

La figura 2 es un diagrama de bloques de una realización de ejemplo de un sistema 200 de acuerdo con la materia objeto divulgada. En diversas realizaciones, el sistema 200 puede incluir un cliente 202, un dispositivo 204 PA del lado del cliente, un internet o segunda red 295, y un servidor 206 que se evalúa a través de o por vía de la red segunda 295. En diversas realizaciones, el sistema 200 puede incluir un dispositivo 204s PA del lado del servidor. El sistema 200 ilustrado muestra una realización en la que el dispositivo 204 PA (dispositivo 204s PA) puede no ser un proxy sino simplemente un enrutador u otro dispositivo. Se entiende que lo anterior es solamente un ejemplo ilustrativo al que no se limita la materia objeto divulgada.

En dicha realización, se puede colocar un punto 212 de conexión del lado del cliente cerca a, o en un sentido de topología de red, al lado del servidor del dispositivo 204 PA. De la misma manera, en la realización ilustrada, un punto 280 de conexión del lado del servidor se puede colocar cerca de a, o en un sentido de topología de red, al servidor 206. En la realización ilustrada, la comunicación de red entre el cliente 202 y el servidor 206 puede ocurrir en una forma cifrada o por lo menos parcialmente cifrada (ilustrado a través del gráfico de seguro cerrado).

Como se describió anteriormente, una pluralidad de puntos de sonda o conexión pueden, en algunas realizaciones, ser agregados en diversos puntos a través del sistema 200. En otras realizaciones, puede haber proxys de túnel entre el cliente 202 y servidor 206 que crea segmentación de red adicional. Se entiende que lo anterior es únicamente un ejemplo ilustrativo al que no se limita la materia objeto divulgada.

En una realización, la infraestructura del servidor puede utilizar un distribuidor de carga, un terminador SSL, o cualquier tipo de controlador de entrega de aplicación (ADC). En general, el detector del lado de servicio o punto 280 de conexión se puede instalar en frente de dicho dispositivo. Siempre que la infraestructura de cliente pueda utilizar un portal, proxy u otro dispositivo, el punto 212 de conexión puede estar lejos del cliente 202, en el punto que enfrenta el servidor 204. Se entiende que los anteriores son sólo pocos ejemplos ilustrativos a los que no se limita la materia objeto divulgada.

En diversas realizaciones, tanto el punto 280 de conexión del lado del servidor como el punto 212 de conexión del lado del cliente se pueden colocar para ver o vigilar cualquier tráfico de comunicaciones de red cifradas entre el cliente 202 y el servidor 206 (por ejemplo, tráfico SSL o TLS, etc.). Como se describe adelante, en diversas realizaciones, aunque los puntos 212 y 280 de solo un punto 280 de conexión (o un dispositivo asociado, tal como, dispositivo 208 de sondeo, etc.) se puede configurar para descifrar la comunicación de red cifrada vigilada.

Adicionalmente, en diversas realizaciones, puede existir un número de otros dispositivos dentro de una red interviniente (por ejemplo, la internet 295). En tal una realización, las comunicaciones de red (por ejemplo, paquetes, etc.) establecidas por el servidor 206 al cliente 202 se puede alterar suficientemente durante la transmisión de tal manera que cualquier encabezado de tiempo o información identificación incluida en los paquetes se puede perder, volverse poco fiables o más generalmente inutilizable para los propósitos de vigilancia de red. En dicha realización, los dispositivos 268 y 208 de sondeo se pueden configurar para no basarse en la información en los encabezados de paquete que puedan ser cambiados por un dispositivo interviniente.

En una realización, el sistema 200 puede incluir un dispositivo 208 de sondeo de red del lado del servidor y un dispositivo 268 de sonde de red del lado del cliente. En dicha una realización, el dispositivo 268 de sondeo de red se

puede configurar para recibir una copia de la comunicación 222 de red capturada o duplicada por el punto 212 de conexión de red. Del mismo modo, el dispositivo 208 de sondeo de red se puede configurar para recibir una copia de la comunicación 220 de red capturada o duplicada por el punto 280 de conexión de red.

En diversas realizaciones, el dispositivo 268 de sondeo de red puede no ser capaz de descifrar la comunicación 220 de red. Independientemente, el dispositivo 268 de sondeo de red se puede configurar para vigilar la comunicación 222 de red cifrada y no descartar o ignorar los objetos de datos o las comunicaciones de red cifradas. Sin embargo, como se describe adelante, en diversas realizaciones, las porciones de la comunicación de red cifrada u objetos de datos pueden no ser analizados o ignorados para propósitos analíticos.

En este contexto, un “objeto de datos” incluye una porción discreta de una comunicación de red y puede incluir un paquete de datos, datagrama, o marco, y se puede medir en términos de bytes, bits o caracteres. Como se utiliza aquí el término “paquete” se puede utilizar como una realización de ejemplo específica de un tipo de objeto de datos.

En diversas realizaciones, el objeto de datos puede incluir una porción de encabezado y una porción de carga útil. En dicha realización, la porción de encabezado puede, como mínimo, indicar la fuente inmediata y los dispositivos de destino a los cuales se trasmiten los objetos de datos desde/a, respectivamente (por ejemplo, dispositivo 202 de cliente y dispositivo 204 PA, dispositivo 204 PA y servidor 206, etc.). La porción de carga útil puede incluir cualquier información transmitida por los objetos de datos y también puede incluir información de encabezado o enrutamiento encapsulado (por ejemplo, en el caso donde se interrumpen comunicaciones de red por lo que implica un servidor proxy, una información de red de área local virtual, una información de red privada virtual, etc.). En algunas realizaciones, esta porción de carga útil puede ser cifrada. En diversas realizaciones, la comunicación de red puede incluir un flujo de datos o pluralidad de objetos de datos que transmiten piezas respectivas de información entre dos dispositivos (por ejemplo, cliente 202 y servidor 206, etc.).

En diversas realizaciones, en los que se vigilan comunicaciones de red cifradas, el dispositivo 268 de sondeo de cliente se puede configurar para proporcionar medidas de desempeño de red limitada (por ejemplo, latencia, etc., como se describió anteriormente, etc.) en función de la porción de red entre el punto 212 de conexión y el servidor de 206. En dicha realización, el dispositivo 268 de sondeo se puede configurar para proporcionar medidas limitadas sobre las estadísticas de desempeño de red.

En diversas realizaciones, se puede emplear un punto 280 de conexión del lado del servidor. En dicha realización, el sistema 200 puede incluir un dispositivo 208 de sondeo de servidor. El dispositivo 208 de sondeo de servidor se puede configurar para vigilar la comunicación 220 de red cifrada y no descartar o ignorar la comunicación de red cifrada o los objetos de datos.

A diferencia del dispositivo 268 de sondeo de cliente, el dispositivo 208 de sondeo de servidor puede estar más cercanamente integrado con uno más confiable. En dicha realización, el servidor 206 puede proporcionar el dispositivo 208 de sondeo de servidor con llaves privadas de servidor o credenciales 295 de seguridad. En dicha realización, el dispositivo 208 de sondeo de servidor puede, como porción de la vigilancia de la comunicación 220 de red, detectar cuando se inicia una nueva sesión de comunicación de red cifrada (por ejemplo, la fase de negociación SSL de la sesión SSL, etc.) y extraer (utilizando la llave 294 de servidor) la llave de cifrado de sesión o las credenciales 296 de seguridad de sesión para cada una de las sesiones de comunicación de red cifradas. En diversas realizaciones, esto puede permitir que el dispositivo 208 de sondeo de servidor descifre la comunicación 220 de red del lado del servidor vigilada.

En dicha realización, la comunicación 220 de red del lado de servidor cifrada se puede descifrar (por ejemplo, a través de una porción 218 descifradora del dispositivo 208 de sondeo, e indicada en la ilustración por la gráfica de seguro abierto). En diversas realizaciones, una porción de monitor de tráfico (mostrado en la figura 1) del dispositivo 208 de sondeo puede incluir el descifrador 218.

En la realización ilustrada, el analizador 219 se puede configurar para proporcionar un mayor análisis y medidas más exactas que aquellas del dispositivo 268 de sondeo de cliente que no es capaz de descifrar la comunicación de red cifrada. En dicha realización, el analizador 219 se puede configurar para correlacionar o hacer coincidir objetos de datos o porciones de la comunicación de red del lado del servidor descifrada con objetos de datos o porciones de las comunicaciones de red del lado del cliente cifradas. En diversas realizaciones, se pueden proporcionar diversas medidas en función de los objetos de datos que coinciden que incluyen medidas para las comunicaciones de red de cliente 202/servidor 206 como un todo, así como medidas para cada lado o porción (lado de cliente, lado de servidor) de la comunicación de red.

Como se describió anteriormente, el dispositivo 268 de sondeo de cliente puede no ser capaz de descifrar el tráfico de comunicaciones de red vigilada cifrada 222. En dicha realización, la información incluida por el tráfico 222 de comunicación de red vigilado que normalmente se analizaría (por ejemplo, identificadores de recursos uniformes (URI), ubicadores de recursos uniformes (URL), cookies, etc.) pueden no estar disponibles para las porciones del tráfico 222 vigilado cifrados. Sin embargo, el dispositivo 268 de sondeo de cliente se puede configurar para ver o examinar porciones de transacciones HTTPS u otras porciones definibles del tráfico 222 de comunicaciones de red vigilado

cifrado (por ejemplo, el inicio o el final de un registro SSL, como se describe adelante, etcétera). En diversas realizaciones, también se puede ver o examinar otra información, tal como, por ejemplo, información de nivel de TCP/IP o medidas de tiempo, etcétera. Se entiende que el uso del HTTP es sólo un ejemplo de ilustración al que no se limita la materia objeto divulgada no es limitada.

En diversas realizaciones, el dispositivo 268 de sondeo de cliente puede incluir un monitor 278 configurado para vigilar o registrar el tráfico 222 de red vigilado. En una realización, el dispositivo 268 de sondeo de cliente puede incluir un Generador 279 de medidas configurado para generar diversas medidas (por ejemplo, información 297 de tiempo) para porciones del tráfico 222 de red vigilado. En la realización ilustrada, el generador 279 de medidas genera información 297 de tiempo; sin embargo, se entiende que el tiempo es solamente un ejemplo de ilustración al que no se limita la materia objeto divulgada.

En diversas realizaciones, esta información 297 de tiempo se puede transmitir o enviar desde el dispositivo 268 de sonde de cliente hasta el dispositivo 208 de sondeo de servidor. En diversas realizaciones, las otras transacciones derivadas o vigiladas se pueden transmitir o enviar al servidor del dispositivo 208 de sondeo.

En algunas realizaciones, el Generador 279 de medidas se puede configurar para examinar las porciones no cifradas (por ejemplo, encabezaos, etc.) del tráfico 222 de red vigilado. Como se describió anteriormente, las porciones de carga útil pueden ser cifradas y no legibles por porción del dispositivo 268 de sondeo de cliente. Para cada paquete, unidad de datos, objeto de datos o porción discreta de otra forma de tráfico 222 de red, el dispositivo 268 de sondeo de cliente puede detectar en qué dirección (por ejemplo, cliente al servidor, servidor al cliente, etc.) se dirige el paquete. En diversas realizaciones, esto se puede hacer con base en el encabezado no cifrado.

Se entiende que la descripción y uso del HTTP y HTTPS es solamente un ejemplo de ilustración al que no se limita la materia objeto divulgada. En diversas realizaciones, se pueden emplear otros protocolos de cifrado y esquema de comunicaciones. Por ejemplo, dichos protocolos pueden incluir el protocolo de transferencia de correo simple (SMTP), protocolo de transferencia de archivos SSH (SFTP), etc. Se entiende que los anteriores son sólo unos pocos ejemplos de ilustración a los que no se limita la materia objeto divulgada.

En la realización ilustrada, los paquetes u objetos de datos y sus medidas asociadas se pueden hacer coincidir entre el lado del cliente y la información 297 y 298 de tiempo que utiliza del lado del servidor. En algunas realizaciones, esta información de tiempo se puede derivar de marcas temporales colocadas en o incluidas por los paquetes u objetos de datos. En otra realización, como se describe adelante, las marcas temporales se pueden incluir con una serie de paquetes u objetos de datos.

En este contexto, una “sesión de comunicaciones de datos” puede incluir una serie de objetos de datos o paquetes agrupados a través de un protocolo de comunicaciones. En una realización, una sesión de comunicaciones de datos puede incluir un registro SSL/TLS que define una serie de paquetes u objetos de datos que pertenecen al registro SSL/TLS y tiene un punto de inicio definible y punto final. En tal realización, un registro SSL/TLS establece un grupo de credenciales de cifrado para una serie de objetos de datos o paquetes. En diversas realizaciones, una sesión SSL/TLS puede incluir una pluralidad de registros SSL/TLS. Se entiende que los anteriores son solamente unos pocos ejemplos de ilustración a los que no se limita la materia objeto divulgada.

En una realización, la información 297 de tiempo se puede grabar o determinar (por ejemplo, a través de marcas temporales, etc.) por el dispositivo 268 de sondeo de cliente para todos los objetos de datos o paquetes. En otra realización, el dispositivo 268 de sondeo de cliente puede sólo generar información 297 de tiempo a porciones particulares de las comunicaciones vigiladas o para determinados tipos de objetos de datos o paquetes. Por ejemplo, en una realización, el dispositivo 268 de sondeo de cliente se puede configurar para ignorar o no determinar información 297 de tiempo para determinados tipos de paquetes (por ejemplo, paquetes de reconocimiento (ACK), paquetes de negociación SSL/TLS intermedios, etc.) que se considera (por ejemplo, a través de configuraciones predeterminadas, etc.) no son útiles o deseables para medir latencias u otra información de medida. En otra realización, sólo algunas porciones de la sesión de comunicaciones de datos se pueden analizar.

Por ejemplo, se puede establecer el tiempo final SSL/TLS en razón a que es generalmente es llevado por cargas útiles no cifradas. Los paquetes de negociación de SSL intermedios no son interesantes y pueden no ser vigilados. Por el contrario, el tiempo de paquete ACK de negociación SSL/TLS final se puede analizar, con el fin de medir el tiempo SSL/TLS, percibido en el lado del cliente. En dicha realización, los mensajes de negociación SSL/TLS tal como el servidor SSL/TLS HELLO, transfiere certificados, intercambia claves, etcétera pueden no ser analizadas o incluidas en la información 297 de tiempo. En otra realización, la comunicación cifrada puede incluir acceso a gran cantidad de datos tal como filas o campos de una base de datos. En dicha realización, algunas de las filas pueden no ser consideradas interesantes y puede ser ignoradas o no vigiladas. En otras realizaciones, porciones de las comunicaciones cifradas se pueden ignorar o no vigilar basado en el protocolo o forma de la comunicación. Se entiende que los anterior son sólo unos pocos ejemplos de ilustración a los que no se limita la materia objeto divulgada.

En diversas realizaciones, una vez el dispositivo 268 de sonde de cliente ha determinado un número de medidas basado en o derivado de las comunicaciones 222 cifradas esta información 297 de tiempo (u otra información de medida

vigilada) se puede transmitir al dispositivo 208 de sondeo de servidor. Se entiende que lo anterior es sólo un ejemplo ilustrativo al que no se limita la materia objeto divulgada.

En diversas realizaciones, el analizador 219 puede incluir un generador de medidas que se utiliza o emplea para generar un segundo grupo de información de medidas (por ejemplo, información 298 de tiempo, etc.) que se basa en las comunicaciones 221 de red descifradas. Esta información 298 de tiempo basada en descifrado se puede comparar luego con la información 297 de tiempo basada en cifrado para correlacionar o asociar porciones o transacciones dentro de las comunicaciones de red. En diversas realizaciones, si una porción de información de tiempo substancialmente basada en descifrado y una porción de información de tiempo basada en cifrado coinciden, el analizador 219 puede determinar que la porción subyacente de las comunicaciones de red coincide para una porción dada de las comunicaciones de red. El analizador 219 se puede configurar para generar un grupo de medidas 299 en función de la información disponible en las comunicaciones 221 de red descifradas (por ejemplo, encabezados de paquetes, vistas cleartext de mensajes de solicitud/respuesta, etc.) y el dispositivo 268 de sonde de cliente que proporciona información 297 de tiempo. Se entiende que lo anterior es sólo uno ejemplo ilustrativo al que no se limita la materia objeto divulgada.

En una realización, la información 221 que va desde el dispositivo 218 o 318 de descifrado al analizador 219 puede no simplemente ser la carga útil de comunicaciones descifradas. En dicha realización, la información 221 puede incluir un modelo de evento (por razones de eficiencia) y material de unión.

En este contexto, el término “modelo de eventos” puede incluir información de resumen (por ejemplo, en el caso HTTP: URI, tiempo de inicio y fin, algún encabezado particular, tamaño de bytes, etc.) pero no toda la carga útil del cleartext. En una realización, el modelo puede incluir o ser representado como un archivo de valores separados por comas (CSV) o tablas de bases de datos. En diversas realizaciones, el modelo de evento puede incluir una reducción esencial de la entropía de información del mensaje cleartext actual.

En este contexto, el “material de unión” del evento puede incluir el material de emparejamiento de sesión SSL/TLS del evento (por ejemplo, números aleatorios hello cliente/servidor, etc.) y el paquete de bytes o números de registro SSL/TLS “de interés” (dependiendo de la técnica utilizada). Se entiende que lo anterior es sólo uno ejemplo ilustrativo al que no se limita la materia objeto divulgada.

En dicha realización, el material de unión y/o modelo de evento se puede utilizar mediante el analizador 219 para emparejar o hacer coincidir los tiempos 297 observados en forma remota con el evento observado localmente o (en una realización) tiempos 298 y asignar (unir) los tiempos remotos a los puntos de interés equivalentes en este evento.

En diversas realizaciones, el analizador 219 también puede generar oportunistamente o transferir) otras medidas 299. Por ejemplo, en una realización TCP relacionada con medidas puede incluir tiempo de ida y vuelta (RTT), conteo fuera de orden (OOO), retransmisiones, conteo de paquetes, etcétera. En diversas realizaciones, las medidas 299 también pueden incluir medidas relacionadas con envoltura cifrada (por ejemplo, detalles de negociación SSL/TLS, etc.) basado en el modelo de evento.

En diversas realizaciones, que el descifrador 218 puede requerir que contribuyan con al “material de unión”, debido a que el descifrador 218 puede proporcionar solamente o por lo menos la oportunidad difícil de realizar dichas observaciones en las comunicaciones cifradas y proporcionar aquellas operaciones en relación con el modelo de evento. Se entiende que lo anterior es solamente un ejemplo de ilustración al que no se limita la materia objeto divulgada.

En diversas realizaciones, el analizador 219 se puede configurar para determinar que dos objetos de datos (por ejemplo, una porción de tráfico de red cifrada y una porción de tráfico de red descifrada, etc.) coinciden o se relacionan si se cumple un grupo de criterios predefinidos. Se entiende que lo de adelante es solamente un ejemplo ilustrativo a que no se limita la materia objeto divulgada.

La figura 3 es un diagrama de bloques de una realización de ejemplo de un sistema 300 de acuerdo con la materia objeto divulgada. El sistema 300 puede incluir una variación de un sistema similar al sistema 200 de la figura 2.

En la realización ilustrada, el sistema 300 puede incluir un distribuidor 304 de carga en lugar del punto 204s de acceso de la figura 2. Aunque se muestra un distribuidor de carga, se entiende que lo anterior es solamente un ejemplo ilustrativo al que no se limita la materia objeto divulgada y se pueden utilizar otros dispositivos.

En la realización ilustrada, el distribuidor 304 de carga puede incluir un descifrador 318 configurado para cifrar/descifrar las comunicaciones de red cifradas entre el servidor 206 y cliente 202. En diversas realizaciones, se puede configurar el descifrador 318 para que utilice o emplee la claves 296 de sesión como porción del proceso de descifrado.

En dicha realización, dispositivo 308 de sondeo de servidor puede no incluir un descifrador 218, a diferencia del dispositivo 208 de sondeo de servidor de la figura 2. En dicha realización, el punto 280 de conexión puede proporcionar una versión 320 descifrada de las comunicaciones 321 de red cifradas. En dicha realización, las comunicaciones 320 de red descifradas pueden ser iguales que o sustancialmente equivalentes a las comunicaciones 221 de red descifradas

(por ejemplo, permitiendo el almacenamiento en búfer o el proceso auxiliar mediante el dispositivo 308 de sondeo de servidor, etc.). En diversas realizaciones, las comunicaciones 320 de red pueden incluir el modelo de eventos y el material de unión, como se describió anteriormente en relación con las comunicaciones 221 descifradas de la figura 2. Se entiende que lo anterior es solamente un ejemplo de ilustración al que no se limita la materia objeto divulgada.

Se entiende que mientras las realizaciones muestran una sonda del lado del servidor haciendo descifrado cómo se muestra en las figuras 1, 2 y 3, la materia objeto no se limita a esa realización. Se entiende que lo anterior es sólo uno ejemplo de ilustración al que no se limita la materia objeto.

En una realización preferida, la sonda que no descifra se puede configurar para enviar datos a la sonda que descifra. En diversas realizaciones, esto puede tener la ventaja relacionada con razones de seguridad y también para una topología SaaS. Por ejemplo, puede no ser deseable llevar todos los otros poseedores SaaS a una única ubicación de poseedor SaaS. Se entiende que los anteriores son sólo unos pocos ejemplos ilustrativos a los que no se limita la materia objeto divulgada.

En una realización, en un sistema cerrado en donde se vigilan las comunicaciones cifradas sin puntos de ventaja preferibles (por ejemplo, comunicaciones cifradas dentro de un puente de red privada virtual (VPN) en una compañía), es concebible que cualquiera de todas las sondas que envía sus tiempos a un tercero (u otra) entidad que analiza no está sondeando e incluso no en proximidad a sus sondas. Se entiende que lo anterior es solamente un ejemplo de ilustración al que no se limita la materia objeto divulgada.

En diversas realizaciones, los fabricantes de equipos de red pueden desear divulgar dichos tiempos de envoltura cifrados como un bloque fundamental de herramientas de vigilancia de desempeño. En dicha realización, los routers, distribuidores de carga, servidores Web, puntos de acceso VPN, u otros dispositivos de red, etcétera se puede configurar para producir los tiempos de envoltura de cifrado (por ejemplo, SSL/TLS, etc.). En dicha realización, se puede configurar una sonda de descifrado para enriquecer su modelo de datos con aquellos puntos de ventaja (por ejemplo, información de tiempo, etc.).

En una realización, el dispositivo 308 de sondeo de servidor puede incluir el analizador 219. En diversas realizaciones, el analizador 219 se puede configurar para que coincida con las comunicaciones 221 de red descifradas con la información 297 de tiempo, como se describió anteriormente. En dicha realización, el analizador 219 se puede configurar para generar las medidas 299 en función de la información disponible de las comunicaciones de red 221 descifrada monitoreados y la información 297 de tiempo proporcionada por el dispositivo 268 de sondeo de cliente.

La figura 4 es un diagrama de tiempo de una realización de ejemplo de un sistema de acuerdo con la materia objeto divulgada. Como se describió anteriormente, en diversas realizaciones, los dispositivos de intervención pueden alterar o cambiar los objetos o paquetes de datos entre el tiempo en que ellos se transmiten desde el servidor y son recibidos por el cliente (o viceversa). En dicha realización, las marcas temporales de un objeto de datos o paquete pueden no estar disponible o puede haber sido cambiado. En dicha realización, se puede emplear un identificador posiblemente no cifrado alterno. En la realización ilustrada, se puede emplear una información a partir de un registro SSL para identificar diversas transferencias de datos. Se entiende que lo anterior es solamente un ejemplo de ilustración al que no se limita la materia objeto divulgada.

En la realización ilustrada, se muestran 3 transferencias de datos A, B y C. En la realización ilustrada, cada transferencia de datos incluye un mensaje de solicitud (por ejemplo, Get 412 para transferencia de datos A, etc.) y un mensaje de respuesta (por ejemplo, Object A 416 para transferencia de datos A, etc.). En diversas realizaciones, puede ocurrir estas transferencias substancialmente concurrentemente o en una forma segmentada, de tal manera que la transferencia de datos B empieza antes que se complete la transferencia de datos A. Se entiende que lo anterior es solamente un ejemplo de ilustración al que no se limita la materia objeto divulgada

En una realización, los mensajes de solicitud 412, 413 y 414 se pueden transmitir a través de los paquetes, 421, 422, 423, 424 y 425. De la misma manera, los mensajes de respuesta, 416, 417 y 418 se pueden transmitir a través de los paquetes, 431, 432, 433, 434 y 435. En la realización ilustrada, se muestra el inicio y el fin de los paquetes mediante líneas que conectan los paquetes a los registros SSL. En la realización ilustrada, cada paquete 421, etc., se asocia con incluye una marca temporal 452, etc. En dicha realización, de paquetes (por ejemplo, paquetes, 421, 422 y 423, etc.) requeridos para formar un registro SSL (por ejemplo, registro SSL 402, etc.), el tiempo de paquete más temprano (por ejemplo, tiempo 452, etc.) puede llegar a ser el registro SSL 402 de tiempo de inicio mientras que el último paquete de tiempo (por ejemplo, tiempo 453, etc.) pueden llegar a ser el tiempo final del registro SSL 402'.

Estos diversos objetos de datos o paquetes se pueden cifrar a través de envolturas de cifrado 402, 404, 406 y/o 408. En la realización ilustrada, las envolturas de cifrado 402, 404, 406 y 408 se muestran como registros SSL. Se entiende que lo anterior es solo un ejemplo de ilustración al que no se limita la materia objeto divulgada

En diversas realizaciones, incluso el dispositivo de sondeo incapaz de descifrado puede ser capaz de determinar el inicio y el fin de cada registro SSL. Como tal, al examinar el inicio o el final de los registros SSL el dispositivo sondeo

incapaz de descifrado puede ser capaz de estimar o derivar la información de tiempo con respecto a los mensajes de solicitud/respuesta.

Por el contrario, en una realización, el dispositivo de sondeo incapaz de descifrado puede no ser capaz de determinar cuando ocurre una solicitud (por ejemplo, Get A 412, etc.) o respuesta (Object A 416, etc.). Sin embargo, cuando el dispositivo de sondeo capaz de descifrado puede ser capaz de discernir esta información o por lo menos que se encapsule la solicitud/respuesta o incluya mediante una envoltura de cifrado. Por ejemplo, el dispositivo de sondeo capaz de descifrado puede ser capaces de determinar que el mensaje Get A 412 se encapsula o incluye por el registro SSL 402. En dicha realización, el dispositivo de sondeo capaz de descifrado puede ser capaz de determinar esto porque puede descifrar el registro SSL 402 y ver los contenidos, mientras que dispositivo de sondeo incapaz de descifrado no puede ser capaz de hacer esto.

En diversas realizaciones, el dispositivo de sondeo capaz de descifrado se puede configurar para recibir la información de tiempo (por ejemplo, tiempo de inicio, tiempo de finalización, etcétera) de diversos registros SSL 402, 404, 406 y 408 desde el dispositivo de sondeo incapaz de descifrado. En una realización, el dispositivo de sondeo capaz de descifrado se puede configurar para utilizar esa información de tiempo en adición a lo que sabe el dispositivo de sondeo capaz descifrado o es capaz de determinar que son los contenidos de los registros SSL 402, 404, 406 y 408 para estimar o determinar cuándo ocurren varias solicitudes/respuestas de mensajes.

En la realización ilustrada, el dispositivo de sondeo capaz de descifrado puede reconocer que el registro SSL 402 incluye el mensaje 412 de solicitud A y, través de la información de tiempo proporcionada por el dispositivo de sondeo incapaz de descifrado, que el registro SSL 402 inicia en el tiempo 452. El dispositivo de sondeo incapaz de descifrado puede reconocer que el paquete 422 incluye un extremo o inicio de un registro SSL, pero que el paquete 423 incluye el final del registro SSL 402 en el momento 453, y por lo tanto no se puede generar información de tiempo con base en el paquete 422. Pero, la información de tiempo se puede generar en función del final del registro SSL 402 en el momento 453. Por lo tanto, el dispositivo de sondeo capaz de descifrado puede inferir o estimar que el mensaje 412 de solicitud A ocurre durante el período de tiempo 462, entre los tiempos 452 y 453.

En la realización ilustrada, el dispositivo de sondeo capaz de descifrado puede reconocer que el registro SSL 406 incluye el mensaje 416 de respuesta A y a través de la información de tiempo, que el registro SSL 406 empieza en el tiempo 456. El dispositivo de sondeo incapaz de descifrado puede reconocer que el paquete 432 incluye un fin o inicio de un registro SSL (y por lo tanto no se puede generar información de tiempo), pero que el paquete 433 incluye el final del registro SSL 406 en el tiempo 457. Por lo tanto, el dispositivo de sondeo capaz de descifrado puede inferir o estimar que el mensaje 416 de respuesta A ocurre durante el período de tiempo 466 (y tiempo entre los tiempos 456 y 457), y el servidor o anfitrión toma el período de tiempo 464 (entre los tiempos 453 y 456) para procesar la solicitud A 412.

De la misma manera, el dispositivo de sondeo capaz de descifrado puede reconocer que el registro SSL 402 incluye el inicio del mensaje 413 de solicitud B y, a través de la información de tiempo suministrada por el dispositivo de sondeo incapaz de descifrado, que inicia el registro SSL 402 en el momento 452. El dispositivo de sondeo incapaz de descifrado puede reconocer que el registro SSL 404 incluye el final del mensaje 413 de la solicitud B y, a través de la información de tiempo, que el registro SSL 404 finaliza en el momento 454. El dispositivo de sondeo capaz de descifrado puede reconocer que el registro SSL 406 incluye el inicio del mensaje 417 de respuesta B y, a través de la información de tiempo, que el registro SSL 406 inicia en el tiempo 456. El dispositivo de sondeo capaz de descifrado puede reconocer que el registro SSL 408 incluye la finalización del mensaje 417 de respuesta B y, a través de la información de tiempo, que el registro SSL 408 finaliza en el tiempo 458. Por lo tanto, el dispositivo de sondeo capaz de descifrado puede inferir o estimar que el mensaje 413 de solicitud B ocurre durante el periodo de tiempo 472. El dispositivo de sondeo capaz de descifrado puede inferir o estimar que el mensaje 417 de respuesta B ocurre durante el período de tiempo 476. Por lo tanto, el servidor o anfitrión toma el período 474 (entre los tiempos 454 y 456) para procesar la solicitud B 413.

Del mismo modo, el dispositivo de sondeo capaz de descifrado puede reconocer que el registro SSL 404 incluye el mensaje 414 de solicitud C y, a través de la información de tiempo, que el registro SSL 404 inicia en el momento 453 y finaliza en el momento 454. El dispositivo de sondeo capaz de descifrado puede reconocer que el registro SSL 408 incluye el mensaje 418 de respuesta B y, a través de la información de tiempo, que el registro SSL 408 inicia en el momento 457 y finaliza en el momento 458. Por lo tanto, el dispositivo de sondeo capaz de descifrado puede inferir o estimar que el mensaje 414 de solicitud C ocurre durante el período de tiempo 482. El dispositivo de sondeo capaz de descifrado puede inferir o estimar que el mensaje 418 de respuesta C ocurre durante el período de tiempo 486. Por lo tanto, el servidor o anfitrión toma el período 484 (entre los tiempos 454 y 457) para procesar la solicitud C 414.

En diversas realizaciones, el dispositivo de sondeo incapaz de descifrado se puede configurar para transmitir información de tiempo con respecto a los registros SSL, en lugar de paquetes del dispositivo de sondeo capaz de descifrado. En dicha realización, el dispositivo de sondeo capaz de descifrado se puede configurar para asociar estos tiempos de registro SSL con varios mensajes de solicitud/respuesta.

En diversas realizaciones, el mensaje de información de tiempo enviado al dispositivo de sondeo capaz de descifrado puede incluir un identificador de registro SSL que indica que el registro SSL se asocia con una solicitud particular o

mensaje de respuesta. Se entiende que lo anterior es solamente un ejemplo de ilustración al que no se limita la materia objeto divulgada.

En diversas realizaciones, a envoltura de comunicación cifrada (por ejemplo, registro SSL, etc.) puede, dependiendo del protocolo de comunicaciones empleado, no incluir un identificador o esquema de numeración. En dicha realización, un identificador o número se puede asignar mediante los dispositivos de sondeo a cada uno de las envolturas de comunicación cifradas (por ejemplo, registro SSL, etc.). En una realización, esta numeración puede ser secuencial; Aunque, se entiende que lo anterior es solamente un ejemplo ilustrativo al que no se limita la materia objeto divulgada.

La figura 5 es un diagrama de tiempo de una realización de ejemplo de un sistema de acuerdo con la materia objeto divulgada. En otra realización, las sesiones de comunicación cifradas pueden tener una relación conocida (por ejemplo, 1 a 1, etc.) para comunicación descifrada. Por ejemplo, cada byte de un dato no cifrado puede solicitar un byte de datos cifrados. En dicha realización, el dispositivo de sondeo incapaz de descifrado se puede configurar para transmitir o determinar la información de tiempo en función de los bytes de la comunicación cifrada.

En diversas realizaciones, el cifrado o protocolo de transmisión puede agregar bytes adicionales o datos de relleno a la sesión de comunicación cifrada que no existe en la comunicación plaintext o no cifrada. Sin embargo, la cantidad o el tamaño de los bytes adicionales se conocen en general y por lo tanto, se puede explicar. Por ejemplo, la carga útil de un registro SSL puede ser de 5 bytes de la carga útil de plaintext debido al encabezado de registro SSL. Se entiende que lo anterior es solamente un ejemplo de ilustración al que no se limita la materia objeto divulgada

En una realización, el dispositivo de sondeo incapaz de descifrado puede recibir una lista o serie de bytes (u otra medida, por ejemplo, kilobytes, etc.) para el que se desea la información de tiempo. En una realización, la lista de bytes puede ser recibida del dispositivo de sondeo capaz de descifrado. Basado en esta lista el dispositivo de sondeo incapaz de descifrado puede vigilar la sesión de comunicaciones cifradas y derivar la información de tiempo al contar los bytes en la sesión de comunicación cifrada y registrar el tiempo cuando los bytes de interés se reciben/envían.

Por ejemplo, en una realización, la sesión 502 de comunicaciones cifradas se puede dividir y trasmitir como una serie de objetos de datos o paquetes 504. En la realización ilustrada, la serie de paquetes 504 puede incluir paquetes 521, 522, 523, 524 y 525.

La sesión 502 de comunicaciones cifradas también puede incluir una porción 512 de encabezado no cifrado (cuyo dispositivo de sondeo incapaz de descifrado puede leer los contenidos) y una porción 514 de carga útil cifrada (cuyo dispositivo de sondeo incapaz de descifrado no puede leer los contenidos). En diversas realizaciones, la sesión 502 de comunicaciones cifradas también puede incluir una porción 516 de pie de página.

En una realización, el dispositivo de sondeo incapaz de descifrado puede recibir el paquete 521 que empieza en el byte 530 de la sesión 502 de comunicaciones cifradas y finaliza en el byte 532. En dicha realización, el dispositivo de sondeo incapaz de descifrado puede contar el tamaño o número de bytes del encabezado 512 y determinar que el desfase 531 de la sesión 502 de comunicaciones cifradas de la lista de serie de bytes para el cual se desea la información de tiempo.

En diversas realizaciones, cada paquete (por ejemplo, paquete 522, etc.) llega el número de bytes del paquete 522 (byte 532a byte 534) que se puede agregar a un conteo de bytes dentro de la sesión 502 de comunicaciones cifradas. Este conteo de bytes se puede comparar con la lista de bytes para el cual se desea información de tiempo.

Si el paquete 522 incluye uno de los bytes para el cual se desea información de tiempo, la información de tiempo del paquete 522 se puede registrar. En una realización, el tiempo de llegada del paquete 522 se puede registrar y eventualmente trasmitir al dispositivo de sondeo capaz de descifrado como información de tiempo, como se describió anteriormente.

En una realización, la información de tiempo puede incluir información del tiempo para cada uno de los bytes dentro de la lista de bytes para el que se desea información de tiempo. En otra realización, la información de tiempo puede incluir información de tiempo no para los bytes específicos dentro de la lista, sino en cambio la información del tiempo para los paquetes que incluyen los bytes para el cual se desea la información de tiempo. En aún otra realización, la información de tiempo puede incluir información del tiempo para el inicio o finalización de bytes (por ejemplo, bytes 530, 532, 534, 536, 538 y 539) o un rango de bytes para los paquetes que incluyen los bytes para el cual se desea la información de tiempo.

En diversas realizaciones, los datos cleartext o plaintext, no cifrados se pueden comprimir antes de cifrado y eventual transmisión como comunicaciones de red cifradas. En dicha realización, la relación de 1 a 1 bytes entre las comunicaciones de red cifradas y descifradas, descritas anteriormente, pueden no existir. Esto puede complicar el análisis de tiempo, como una carga útil 514 cifrada puede no ser descifrada y descomprimida por el dispositivo de sondeo incapaz de descifrado. En dicha realización, el dispositivo de sondeo capaz de descifrado puede generar la lista de bytes para que se desea la información de tiempo en función de los datos comprimidos y no los datos no comprimidos. En dicha realización, la lista de bytes para los que se desea la información de tiempo se puede basar en los bytes dentro de la carga útil 514 cifrada y no en los datos plaintext o no cifrados, como se describió anteriormente.

En algunas realizaciones, la lista de bytes puede ser aproximada ya que el dispositivo de sondeo capaz de descifrado puede no ser capaz de medir exactamente los bytes entre las etapas de compresión y cifrado o transmisión. Se entiende que lo anterior es solamente un ejemplo ilustrativo al que no se limita la materia objeto divulgada

La figura 6 es un diagrama de flujo de una realización de ejemplo de una técnica de acuerdo con la materia objeto divulgada. En diversas realizaciones, la técnica 600 se puede utilizar o producir por los sistemas tal como aquellos de las figuras 1, 2 o 3. Adicionalmente, las porciones de la técnica 600 se pueden utilizar para producir objetos de datos tal como aquellos de las figuras 4, o 5. Aunque se entiende que lo anterior son sólo unos pocos ejemplos ilustrativos a los que no se limita la materia objeto divulgada. Se entiende que la materia objeto divulgada no se limita a ordenar una serie de acciones ilustradas por la técnica 600.

El bloque 602 ilustra que, en una realización, la sesión de comunicaciones cifradas entre un primer dispositivo de cómputo y un segundo dispositivo de cómputo se puede vigilar, como se describió anteriormente. En diversas realizaciones, cada sesión de comunicaciones cifradas puede incluir trasmitir una pluralidad de objetos de datos cifrados entre un primer y un segundo dispositivo de cómputo, como se describió anteriormente. En diversas realizaciones, uno o más de las acciones ilustradas por este Bloque se pueden realizar por los aparatos o sistemas de las figuras 1, 2 o 3, los puntos de conexión de lado del cliente de las figuras 1, 2 o 3, como se describió anteriormente.

El bloque 604 ilustra que, en una realización, la información de tiempo con respecto a una sesión de comunicaciones cifradas se puede derivar, como se describió anteriormente. En una realización, la derivación se puede basar en uno o más objetos de datos cifrados recibidos incluidos por la sesión de comunicaciones cifradas, como se describió anteriormente. En algunas realizaciones, la derivación puede incluir determinar el inicio de una envoltura de cifrado incluida por la sesión de comunicaciones de cifrado vigilada, y determinar el fin de la envoltura de cifrado, como se describió anteriormente.

En otra realización, la derivación puede incluir recibir una indicación, desde el segundo dispositivo de sondeo, de una ubicación dentro de una sesión de comunicaciones cifradas para el que se va a derivar la información de tiempo, como se describió anteriormente. En dicha realización, la derivación puede incluir adicionalmente determinar cuándo la ubicación indicada dentro de una sesión de comunicaciones cifradas ha sido recibida por el dispositivo 102 de cómputo de cliente, como se describió anteriormente. En diversas realizaciones, la derivación también puede incluir almacenar una marca temporal asociada con la ubicación indicada recibida dentro de una sesión de comunicaciones cifradas, como se describió anteriormente.

En algunas realizaciones, la ubicación dentro de la sesión de comunicaciones cifradas se puede indicar a través de un desfase de bytes desde el inicio de una porción de la sesión de comunicaciones cifradas, como se describió anteriormente. En dicha realización, determinar cuándo se ha recibido la ubicación indicada dentro de una sesión de comunicaciones cifradas puede incluir, para cada objeto de datos cifrados recibidos, determinar si el objeto de datos cifrados recibidos está incluido con la sesión de comunicaciones cifrada indicadas, determinar el rango de bytes dentro de la sesión de comunicaciones cifradas indicadas asociada con el objeto de datos cifrados recibidos, y comparar el rango de bytes asociados con el objeto de datos cifrados recibidos para indicar el desfase de bytes, como se describió anteriormente.

En algunas realizaciones, la sesión de comunicaciones cifradas puede incluir objetos de datos están comprimidos y cifrados. En dicha realización, la derivación puede incluir recibir una indicación, mediante el primer dispositivo de sondeo y desde el segundo dispositivo de sondeo, de una ubicación dentro de una sesión de comunicaciones cifradas para el que se va a derivar información, en el que la ubicación se basa en los objetos de datos comprimidos y cifrados, como se describió anteriormente.

En algunas realizaciones, la sesión de comunicación de cifrado incluye uno o más envolturas de cifrado, como se describió anteriormente. En dicha realización, la derivación puede incluir basar la información de tiempo sobre una marca temporal asociada con las envolturas cifradas, como se describió anteriormente. En otra realización, la derivación puede incluir ignorar, para propósitos de derivar la información de tiempo, uno o más objetos de datos cifrados recibidos incluidos por la sesión de comunicaciones cifradas que se indican, por el primer dispositivo de cómputo, como ignorables, como se describió anteriormente recibieron. En diversas realizaciones, una o más de las acciones ilustradas por este bloque se pueden realizar por los aparatos o sistemas de las figuras 1, 2 o 3, los puntos de conexión de lado de cliente de las figuras 1, 2 o 3, como se describió anteriormente.

El bloque 606 ilustra que, en una realización, la información de tiempo derivada se puede trasmitir a otro dispositivo, como se describió anteriormente. En una realización, la información de tiempo se puede trasmitir a un dispositivo de sondeo de lado del servidor, como se describió anteriormente. En diversas realizaciones, una o más de las acciones ilustradas por este bloque se pueden realizar por los aparatos o sistemas de las figuras 1, 2 o 3, los puntos de conexión del lado del cliente de las figuras 1, 2 o 3, como se describió anteriormente.

El bloque 608 ilustra que, en una realización, por lo menos una porción de la sesión de comunicación cifrada se puede descifrar por un segundo dispositivo de sondeo, como se describió anteriormente. En diversas realizaciones, una o más

de las acciones ilustradas por este bloque se pueden realizar por los aparatos o sistemas de las figuras 1, 2 o 3, los puntos de conexión del lado del cliente de las figuras 1, 2 o 3, como se describió anteriormente.

El bloque 610 ilustra que, en una realización, el grupo de medidas relacionadas con la sesión de comunicaciones cifradas se puede crear. En diversas realizaciones, estas medidas se pueden basar en la porción descifrada de la sesión de comunicación cifrada y la información de tiempo derivada, como se describió anteriormente. En algunas realizaciones, la creación puede incluir correlacionar el inicio del mensaje de datos con la información de tiempo derivada, proporcionada por el primer dispositivo de sondeo, que indica el tiempo de inicio de la envoltura de cifrado, y correlacionar el fin del mensaje de datos con la información de tiempo derivada, proporcionada por el primer dispositivo de sondeo, que indica el tiempo del final de la envoltura de cifrado, como se describió anteriormente. En diversas realizaciones, una o más de las acciones ilustradas por este bloque se pueden realizar por los aparatos o sistemas de las figuras 1, 2 o 3, los puntos de conexión del lado del cliente de las figuras 1, 2 o 3, como se describió anteriormente.

Las implementaciones de diversas técnicas descritas aquí se pueden implementar en circuitos electrónicos digitales, o en hardware de ordenador, firmware, software, o en combinaciones de ellos. Las implementaciones se pueden implementar como un producto de programa de ordenador, es decir, un programa de ordenador incorporado tangiblemente en un portador de información por ejemplo, en un dispositivo de almacenamiento legible por máquina o en una señal programada, para ejecución por, o para controlar la operación de, aparatos de procesamiento de datos, por ejemplo, un procesador programable, un ordenador, o múltiples ordenadores. Un programa de ordenador, tal como el programa de ordenador descrito anteriormente, puede ser escrito en cualquier forma de lenguaje de programación, que incluye lenguajes interpretados o compilados, y se puede desplegar en cualquier forma, que incluye un programa independiente o como un módulo, componente, subrutina, u otra unidad adecuada para uso en un entorno computacional. Un programa de ordenador se puede desplegar para ser ejecutado en un ordenador o múltiples ordenadores en un sitio o distribuido a través de múltiples sitios e interconectado a través de una red de comunicación.

Las etapas de método se pueden realizar mediante uno o más procesadores programables que ejecutan un programa de ordenador para realizar funciones al operar datos de entrada y generar salidas. Las etapas de método también se pueden realizar por, y un aparato se puede implementar como, circuitos lógicos de propósito especial, por ejemplo, una FPGA (matriz de puerta programable de campo) o un ASIC (circuito integrado específico de aplicación).

Los procesadores adecuados para la ejecución de un programa de ordenador incluyen, por vía de ejemplo, microprocesadores de propósito especial y general, y uno cualquiera de uno o más procesadores de cualquier tipo de ordenador digital. En general, un procesador recibirá instrucciones y datos de una memoria de acceso aleatorio o una memoria de solo lectura o ambos. Los elementos de un ordenador pueden incluir por lo menos un procesador para ejecutar instrucciones y uno o más dispositivos de memoria para almacenar instrucciones y datos. En general, un ordenador puede incluir, o ser acoplado funcionalmente a datos recibidos de o datos trasferidos a, o ambos, de uno o más dispositivos de almacenamiento masivos para almacenar datos, por ejemplo, discos magnéticos, magneto ópticos, u ópticos. Los portadores de información adecuados para incorporar las instrucciones de programa de ordenador y datos incluyen todas las formas de memoria no volátiles, que incluyen por vía de ejemplo dispositivos de memoria de semiconductor, por ejemplo, EPROM, EEPROM, y dispositivos de memoria flash; discos magnéticos, por ejemplo, discos duros internos o discos removibles; discos magneto ópticos; y discos CD-ROM y DVD-ROM. El procesador y la memoria se pueden complementar mediante, o incorporar en circuitos lógicos de propósito especial.

Para proporcionar interacción con un usuario, se pueden establecer implementaciones sobre un ordenador que tiene un dispositivo de visualización, por ejemplo, un tubo de rayos catódicos (CRT) monitor de pantalla de cristal líquido (LCD) para visualizar información al usuario y un teclado y un dispositivo de indicación, por ejemplo, un mouse, o un trackball, mediante el cual el usuario puede proporcionar entrada al ordenador. Otros tipos de dispositivos se pueden utilizar para proporcionar también interacción con un usuario por ejemplo, la retroalimentación proporcionada al usuario puede ser de cualquier forma de retroalimentación sensorial, por ejemplo, retroalimentación visual, retroalimentación auditiva, o retroalimentación táctil; y una entrada del usuario puede ser recibida de cualquier forma, incluyendo entrada acústica, de voz o táctil.

Se pueden incorporar implementaciones en un sistema de ordenador que incluye componente back-end, por ejemplo, como un servidor de datos, que incluye un componente middleware, por ejemplo, un servidor de aplicación, o que incluye un componente de front-end, por ejemplo, un ordenador de cliente que tiene una interfaz de usuario gráfica o un navegador Web a través del cual un usuario puede interactuar con una implementación, o cualquier combinación dichos componentes back-end, middleware, o front-end. Los componentes se pueden interconectar mediante cualquier forma o medio de comunicación de datos digital, por ejemplo, una red de comunicación. Ejemplos de redes de comunicación incluyen una red de área local (LAN) y una red de área amplia (WAN), por ejemplo, la internet.

Aunque determinadas características de las implementaciones descritas se han ilustrado como descritas aquí, muchas modificaciones, sustituciones, cambios y equivalentes ocurrirán a aquellos expertos en la técnica. Por lo tanto, se entiende que las reivindicaciones adjuntas pretenden cubrir todas dichas modificaciones y cambios como caen dentro del alcance de las realizaciones.

REIVINDICACIONES

1. Un método (600) implementado por ordenador para utilizar un dispositivo (108b) de sondeo del lado del cliente, el método que comprende:

vigilar (602) el dispositivo (108b) de sondeo del lado del cliente, una o más sesiones de comunicaciones cifradas entre un dispositivo (102) de cómputo de cliente y un dispositivo (106) de cómputo de servidor en donde cada sesión de comunicaciones cifradas incluye transmitir una pluralidad de objetos de datos cifrados entre los dispositivos de cómputo de cliente y servidor;

derivar, (604) por el dispositivo (108b) de sondeo del lado del cliente, información de tiempo con respecto a una sesión de comunicaciones cifradas; y

transmitir, (606) del dispositivo (108b) de sondeo del lado del cliente a un dispositivo (108) de sondeo de servidor, la información de tiempo derivada,

en el que derivar la información de tiempo incluye:

recibir una indicación, del dispositivo (108) de sondeo del lado del servidor, de una ubicación dentro de una sesión de comunicaciones cifradas para el que se va a derivar información de tiempo en el que la ubicación dentro de la sesión de comunicaciones cifrada se indica a través de un desfase de bytes desde el inicio de una porción de la sesión de comunicaciones cifradas;

determinar cuándo la ubicación indicada dentro de una sesión de comunicaciones cifradas ha sido recibida por el dispositivo (102) de cómputo de cliente; y

almacenar una marca temporal asociada con la ubicación indica recibida dentro de una sesión de comunicaciones cifradas; y

en el que determinar cuándo la ubicación indicada dentro de una sesión de comunicación cifrada ha sido recibida incluye:

para cada objeto de datos cifrados recibidos, determinar si el objeto de datos cifrados recibidos se incluye con la sesión de comunicaciones cifradas indicas,

determinar el rango de bytes dentro de la sesión de comunicaciones cifradas indicadas asociadas con el objeto de datos cifrados recibidos, y

comparar el rango de bytes asociados con el objeto de datos cifrados recibidos al desfase de bytes indicado.

2. El método de la reivindicación 1, que incluye adicionalmente:

descifrar, (608) por el dispositivo (108) de sondeo del lado del servidor, por lo menos una porción de la sesión de comunicaciones cifradas; y

crear (610) por el dispositivo (108) de sondeo del lado del servidor, un grupo de medidas relacionadas con la sesión de comunicaciones cifradas basadas en la porción descifrada de la sesión de comunicaciones cifradas y la información de tiempo derivada.

3. El método de la reivindicación 2, en el que el mensaje de datos se incluye dentro de una primera envoltura de cifrado incluida por la sesión de comunicaciones de cifrado; y

crear un grupo de medidas incluye:

correlacionar un inicio del mensaje de datos con la información de tiempo derivada, suministrada por el (108b) dispositivo de sondeo del lado del cliente, que indica el tiempo de inicio de la envoltura de cifrado, y

correlacionar un fin del mensaje de datos con la información de tiempo derivada, proporcionada por el dispositivo de sondeo de lado del cliente, que indica el tiempo del fin de la envoltura de cifrado.

4. El método de una cualquiera de las reivindicaciones anteriores, en el que derivar la información de tiempo incluye:

determinar un inicio de una envoltura de cifrado incluida por la sesión de comunicaciones cifrado vigiladas; y

determinar un fin de la envoltura de cifrado.

5. El método de una cualquiera de las reivindicaciones anteriores, en el que la sesión de comunicaciones cifradas incluye objetos de datos que se comprimen y encriptan; e incluyendo adicionalmente:

recibir una indicación, por el dispositivo (108b) de sondeo de lado del cliente y de un dispositivo (108) de sondeo del servidor, de una ubicación dentro de una sesión de comunicación cifrada para el que la información de tiempo se va a derivar, en el que la ubicación se basa en los objetos de datos comprimidos y cifrados.

6. El método de una cualquiera de las reivindicaciones anteriores, en donde la sesión de comunicación de cifrado incluye uno o más envolturas de cifrado; y

en el que derivar la información de tiempo incluye:

basar la información de tiempo en una marca temporal asociada con las envolturas cifradas.

7. El método de una cualquiera de las reivindicaciones anteriores, en donde derivar la información de tiempo incluye:

ignorar, para propósitos de derivar la información de tiempo, uno o más objetos de datos cifrados recibidos incluidos por la sesión de comunicaciones cifradas que se indican, mediante el dispositivo (102) de cómputo del lado del cliente, como ignorable.

8. Un producto de programa de ordenador para manejar una red, el producto de programa de ordenador se incorpora tangiblemente un medio legible por ordenador y código ejecutable incluido que, cuando se ejecuta por el procesador de un ordenador, se configura para provocar que el computador ejecute las etapas del método implementado por ordenador de acuerdo con una cualquiera de las reivindicaciones anteriores.

9. Un sistema comprende:

un primer punto (107b) de conexión de red configurado para duplicar, en una forma no intrusiva, por lo menos porción de una comunicación de red cifrada transmitida hacia y desde un dispositivo (104) de punto de acceso que forma un límite entre la primera red y la segunda red;

un segundo punto (107) de conexión de red configurado para duplicar, en una forma no intrusiva, por lo menos porción de una comunicación de red cifrada transmitida hacia y desde un dispositivo (106) de cómputo servidor colocado dentro, en un sentido de topología de red, de la segunda red;

un dispositivo (108b) de sondeo del lado del cliente configurado para:

vigilar las sesiones de comunicaciones cifradas entre los dispositivos (106) de cómputo de servidor y un dispositivo (102) de cómputo de cliente, en el que cada sesión de comunicaciones cifradas incluye transmitir una pluralidad de objetos de datos cifrados entre los dispositivos de cómputo de cliente y servidor;

derivar información de tiempo con respecto a una sesión de comunicaciones cifradas basado en uno o más objetos de datos cifrados recibidos incluidos por la sesión de comunicaciones cifradas; y

transmitir, a un dispositivo (108) de sondeo del lado del servidor, información de tiempo derivada, en el que el dispositivo (108b) de sondeo del lado del cliente para:

recibir indicación, del dispositivo (108) de sondeo del lado del servidor, de una ubicación dentro de una sesión de comunicaciones cifradas para que la información de tiempo se va a derivar en el que la ubicación dentro de la sesión de comunicaciones cifradas se indica a través de un desfase de bytes del inicio de una porción de la sesión de comunicaciones cifradas;

determinar cuándo la ubicación indicada dentro de una sesión de comunicaciones cifradas ha sido recibida por el dispositivo (102) de cómputo del cliente; y

almacenar una temporal asociada con la ubicación indicada recibida dentro de una sesión de comunicaciones cifradas;

para cada objeto de datos cifrados recibidos, determinar si el objeto de datos cifrados recibidos se incluye con la sesión de comunicaciones cifradas indicas,

determinar el rango de bytes dentro de la sesión de comunicaciones cifradas indicas asociadas con el objeto de datos cifrados recibidos, y

comparar los rangos de bytes asociados con el objeto de datos cifrados recibidos al desfase de bytes indicado.

10. El sistema de la reivindicación 9, incluye adicionalmente el dispositivo (108) de sondeo del lado del servidor configurado para:

descifrar por lo menos una porción de la sesión de comunicaciones cifradas; y

crear un grupo de medidas relacionadas con la sesión de comunicaciones cifradas basado en la porción descifrada de la sesión de comunicaciones cifradas y la información de tiempo derivada.

11. El sistema de la reivindicación 10, en el que la comunicación de red cifrada incluye por lo menos una envoltura de cifrado, en el que la envoltura de cifrado incluye un mensaje de datos; y

en él que el dispositivo (108) de sondeo de lado del servidor se configura para:

correlacionar un inicio del mensaje de datos con la información de tiempo derivada, proporcionada por el dispositivo (108b) de sondeo de lado del cliente, que indica el tiempo de inicio de la envoltura de cifrado, y

correlacionar un fin de mensaje de datos con la información de tiempo derivada, proporcionada por el dispositivo (108b) de sondeo de lado del cliente, que indica el tiempo de un fin de la envoltura de cifrado.

12. El sistema de una cualquiera de las reivindicaciones 9 a 11, en el que el dispositivo (108b) de sondeo del lado del cliente se configura para:

determinar un inicio de una envoltura de cifrado incluida por la sesión de comunicaciones cifrado vigiladas; y

determinar un fin de la envoltura de cifrado.

13. El sistema de una cualquiera de las reivindicaciones 9 a 12, en el que la sesión de comunicaciones cifradas incluye objetos de datos que se comprimen y encriptan; y en el que el dispositivo de sondeo del lado del cliente se configura para:

recibir una indicación, de un dispositivo de sondeo del lado del servidor, de una ubicación dentro de una sesión de comunicaciones cifradas para que la información de tiempo se va a derivar, en el que la ubicación se basa en los objetos de datos cifrados y comprimidos.

14. El sistema de una cualquiera de las reivindicaciones 9 a 13, en el que el dispositivo de sondeo del lado del cliente donde se configura para:

basar la información de tiempo en una marca temporal asociada con la sesión de comunicaciones cifradas como un todo en lugar de una marca temporal asociada con uno de los objetos de datos cifrados.

15. El sistema de una cualquiera de las reivindicaciones 9 a 14, en el que el dispositivo (108b) de sondeo del lado del cliente se configura para:

ignorar, para propósitos de derivar la información de tiempo, uno o más objetos de datos cifrados recibidos incluidos por la sesión de comunicaciones cifradas que se indica, por el dispositivo (102) de cómputo de cliente, como ignorable.

FIG. 1 100

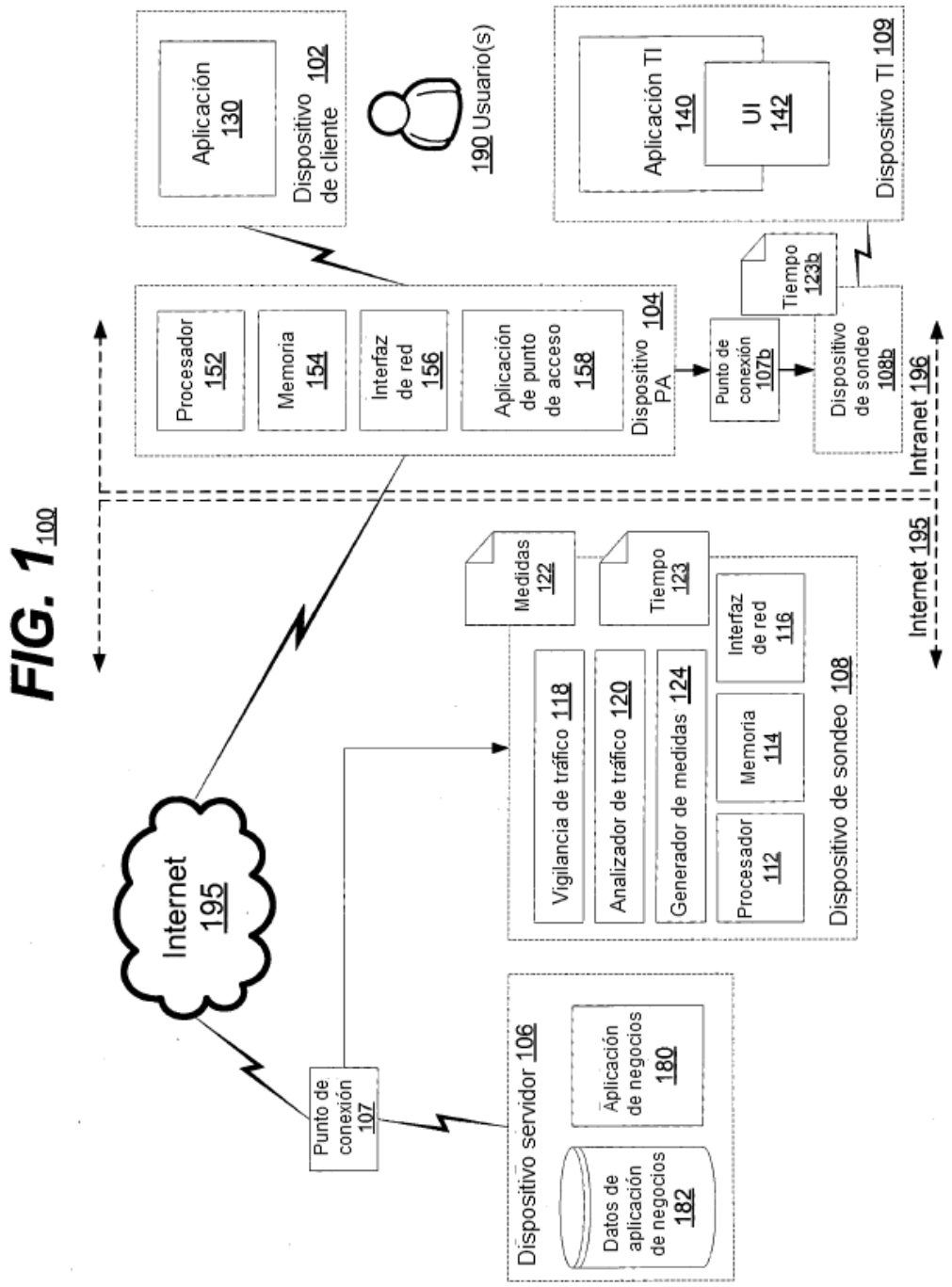

Aplicación 130
Dispositivo de cliente 102
190 Usuario(s)
Aplicación TI 140
UI 142
Dispositivo TI 109
Procesador 152
Memoria 154
Interfaz de red 156
Aplicación de punto de acceso 158
Dispositivo PA 104
Punto de conexión 107b
Tiempo 123b
Dispositivo de sondeo 108b
Intranet 196
Internet 195
Medidas 122
Tiempo 123
Vigilancia de tráfico 118
Analizador de tráfico 120
Generador de medidas 124
Interfaz de red 116
Memoria 114
Procesador 112
Dispositivo de sondeo 108
Internet 195
Punto de conexión 107
Aplicación de negocios 180
Datos de aplicación de negocios 182
Dispositivo servidor 106

FIG. 2

200

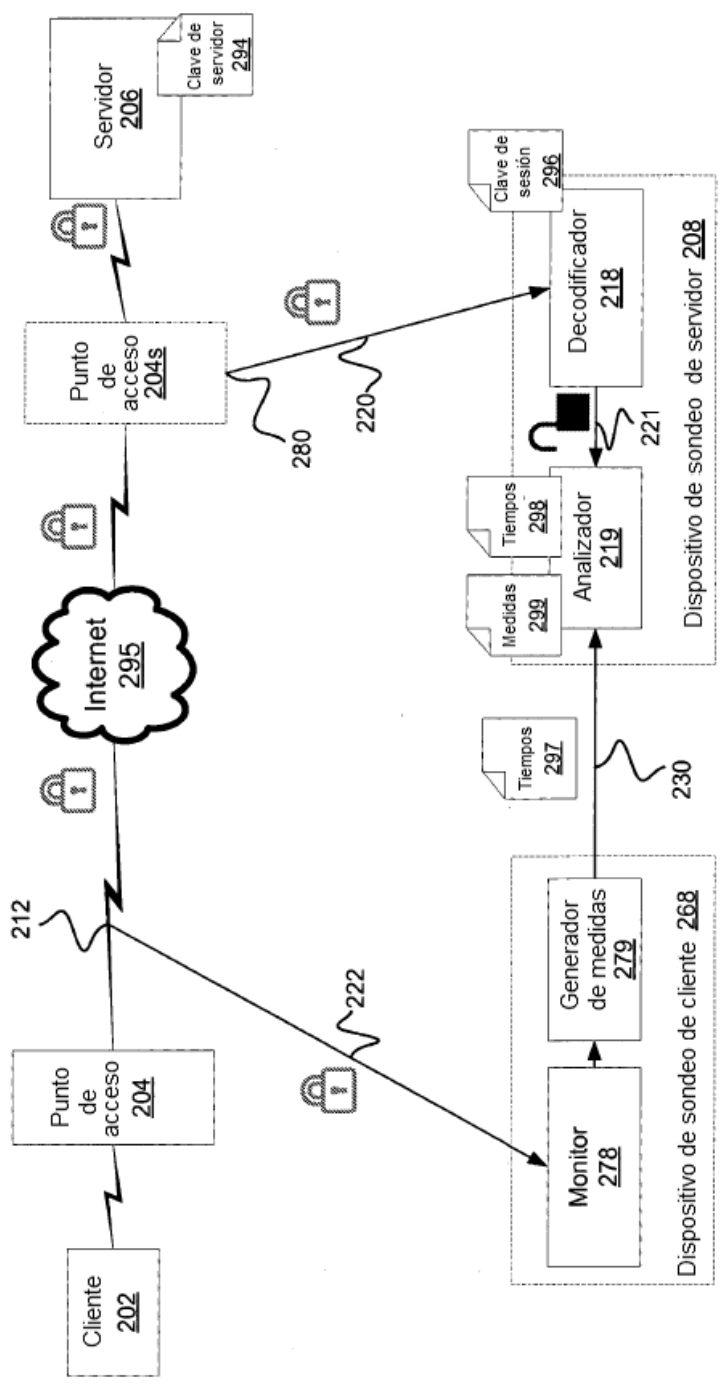

Servidor 206
Clave de servidor 294
Punto de acceso 204s
Internet 295
Punto de acceso 204
Cliente 202
212
222
280
220
Clave de sesión 296
Decodificador 218
221
Tiempos 298
Medidas 299
Analizador 219
Dispositivo de sondeo de servidor 208
Tiempos 297
230
Generador de medidas 279
Monitor 278
Dispositivo de sondeo de cliente 268

FIG. 3

300

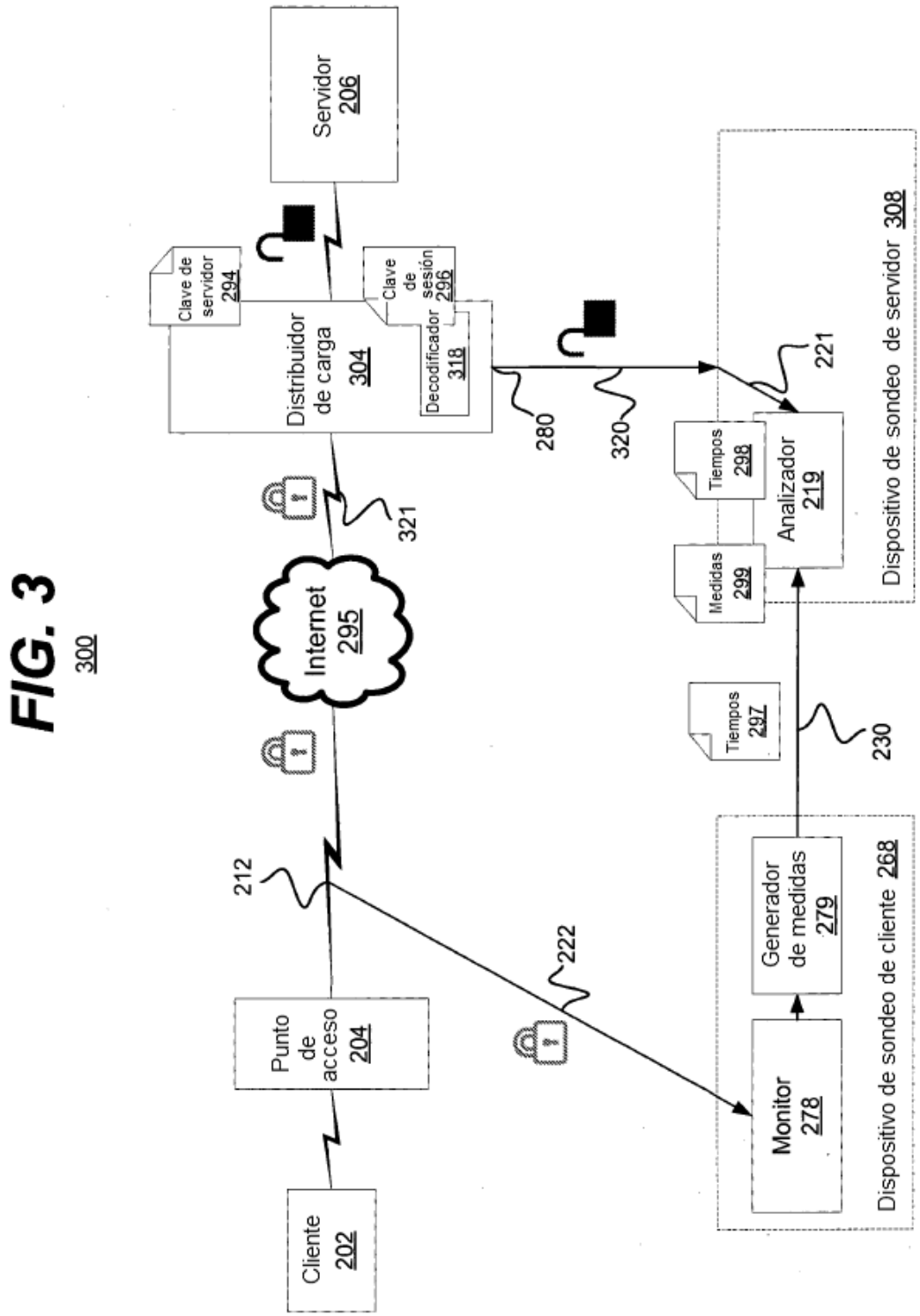

Servidor 206
Clave de servidor 294
Clave de sesión 296
Distribuidor de carga 304
Decodificador 318
280
320
221
Tiempos 298
Analizador 219
Medidas 299
Dispositivo de sondeo de servidor 308
321
Internet 295
Tiempos 297
230
212
222
Punto de acceso 204
Generador de medidas 279
Monitor 278
Dispositivo de sondeo de cliente 268
Cliente 202

FIG. 4

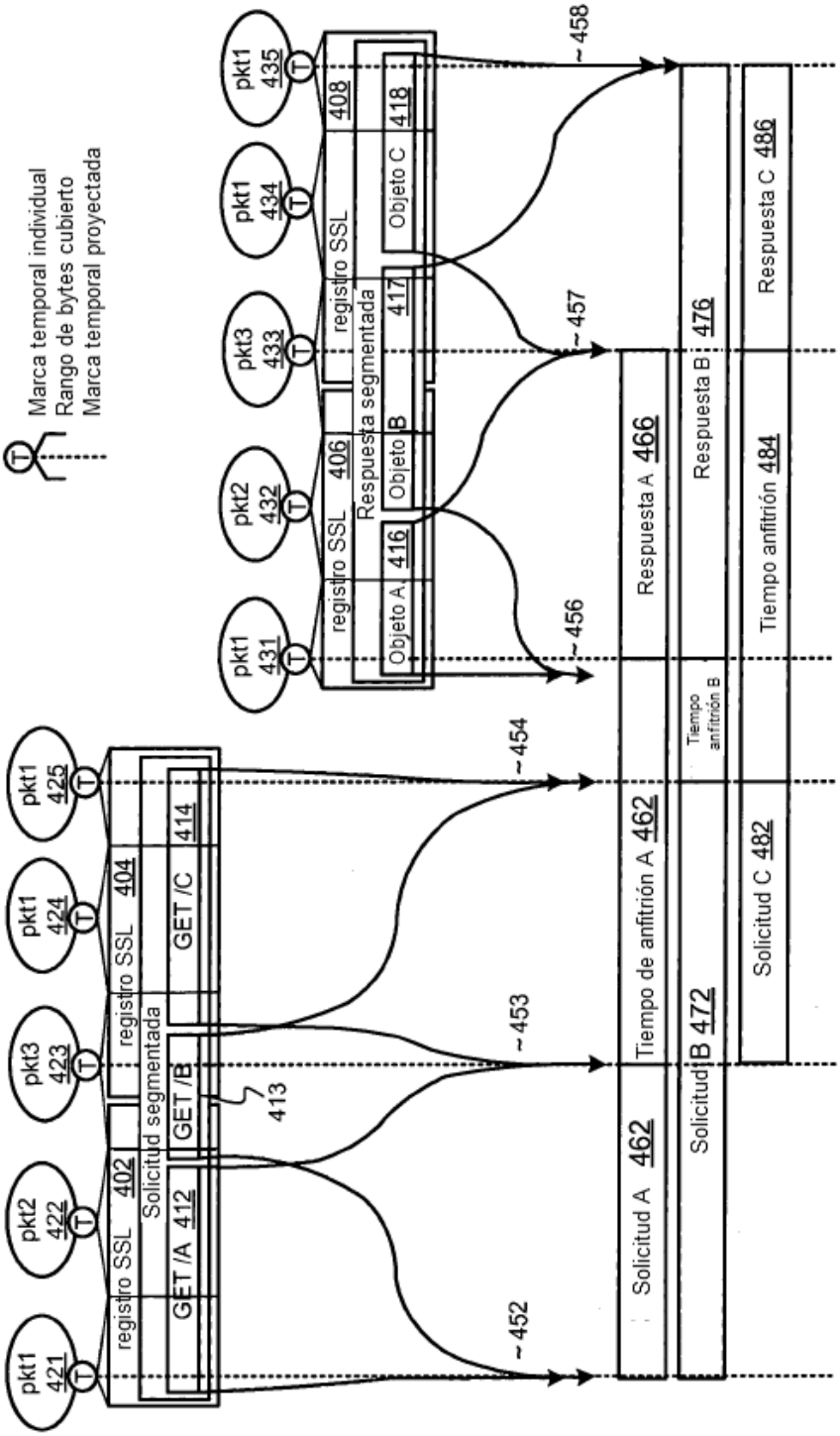

400
Marca temporal individual
Rango de bytes cubierto
Marca temporal proyectada
pkt1 421
pkt2 422
pkt3 423
pkt1 424
pkt1 425
registro SSL 402
Solicitud segmentada
GET /A 412
GET /B
GET /C 414
registro SSL 404
413
~452
~453
~454
pkt1 431
pkt2 432
pkt3 433
pkt1 434
pkt1 435
registro SSL 406
Respuesta segmentada
Objeto A 416
Objeto B 417
Objeto C 418
registro SSL 408
~456
~457
~458
Solicitud A 462
Tiempo de anfitrión A 462
Respuesta A 466
Solicitud B 472
Tiempo anfitrión B
Respuesta B 476
Solicitud C 482
Tiempo anfitrión 484
Respuesta C 486

FIG. 5

500

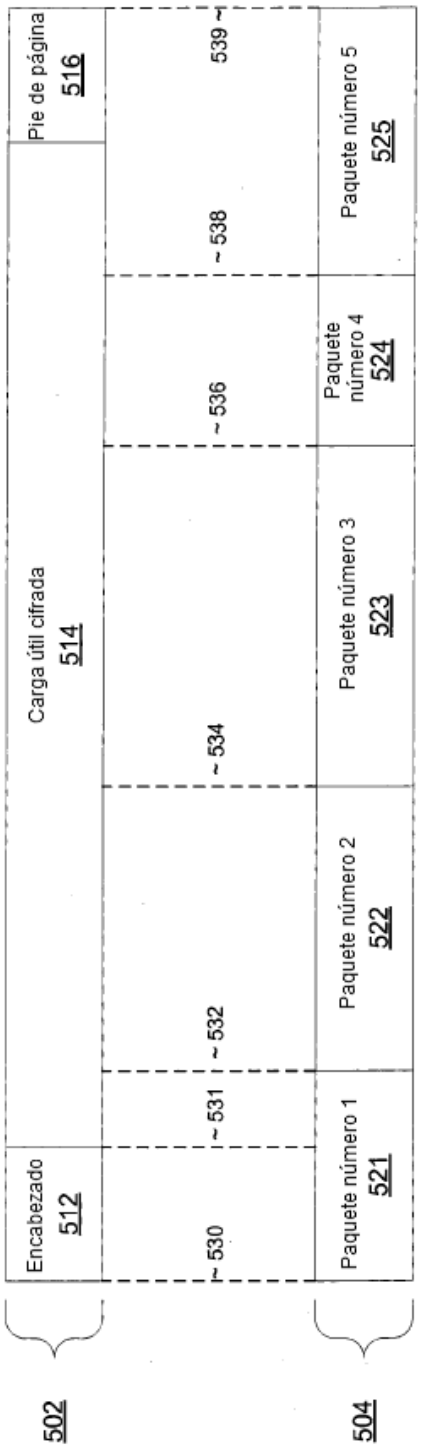
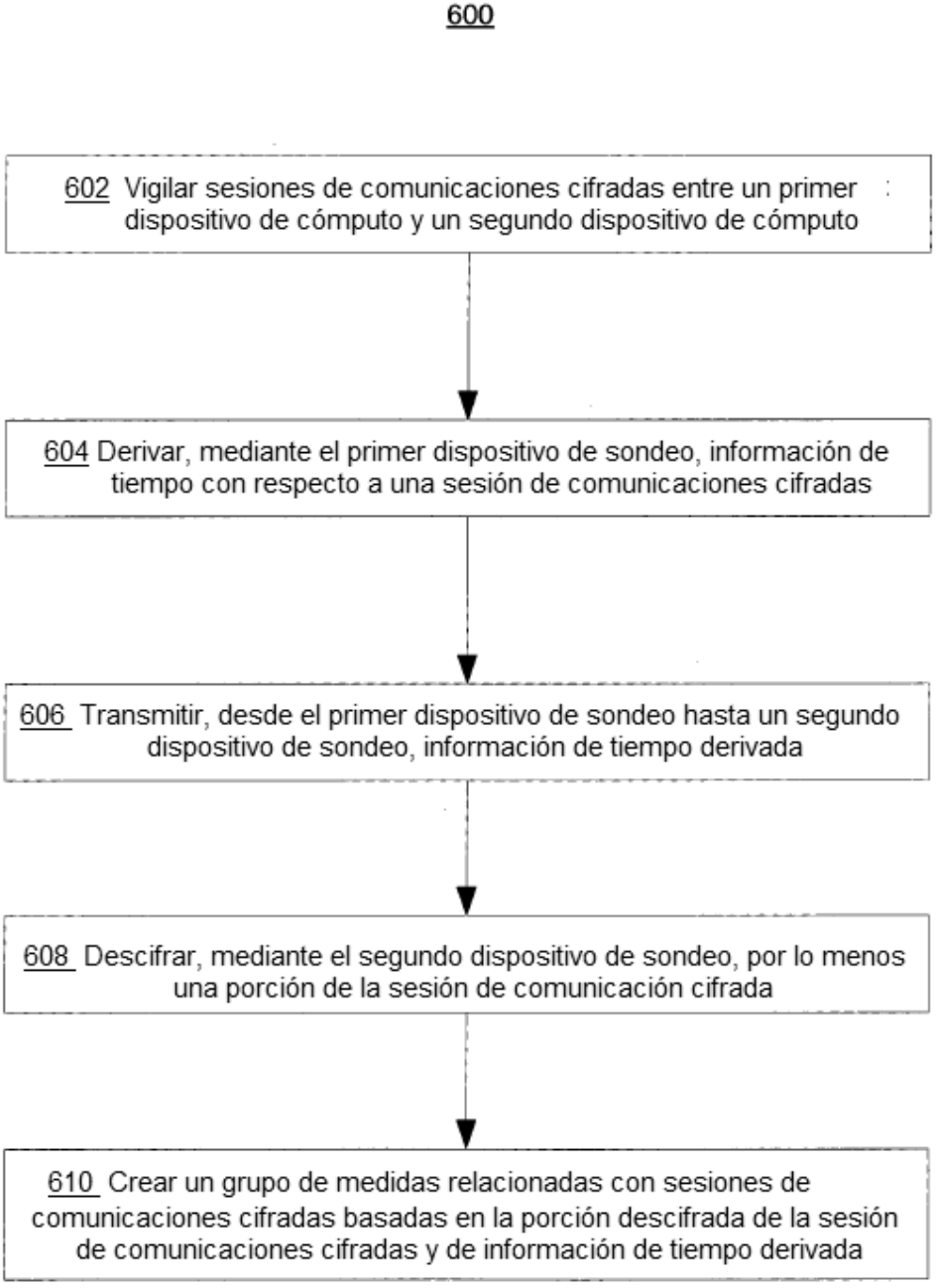

Encabezado
512
Carga útil cifrada
514
Pie de página
516
~ 530
~ 531
~ 532
~ 534
~ 536
~ 538
~ 539
Paquete número 1
521
Paquete número 2
522
Paquete número 3
523
Paquete número 4
524
Paquete número 5
525
502
504

FIG. 6


600
602 Vigilar sesiones de comunicaciones cifradas entre un primer dispositivo de cómputo y un segundo dispositivo de cómputo
604 Derivar, mediante el primer dispositivo de sondeo, información de tiempo con respecto a una sesión de comunicaciones cifradas
606 Transmitir, desde el primer dispositivo de sondeo hasta un segundo dispositivo de sondeo, información de tiempo derivada
608 Descifrar, mediante el segundo dispositivo de sondeo, por lo menos una porción de la sesión de comunicación cifrada
610 Crear un grupo de medidas relacionadas con sesiones de comunicaciones cifradas basadas en la porción descifrada de la sesión de comunicaciones cifradas y de información de tiempo derivada