(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 788 655**

(51) Int. CI.:

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

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **21.03.2013 E 17159345 (2)**

(97) Fecha y número de publicación de la concesión europea: **19.02.2020 EP 3208973**

(54) Título: **Supervisión de rendimiento de red de comunicaciones encriptadas**

(30) Prioridad:

28.03.2012 US 201213432847

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
22.10.2020

(73) Titular/es:

BLADELOGIC, INC. (100.0%)
2103 CityWest Blvd.
Houston, TX 77042, US

(72) Inventor/es:

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

(74) Agente/Representante:

ISERN JARA, Jorge

DESCRIPCIÓN

Supervisión de rendimiento de red de comunicaciones encriptadas

Campo técnico

Esta descripción se refiere al rendimiento de red, y más específicamente a supervisar y analizar el rendimiento de comunicación entre dos dispositivos de red.

Antecedentes

En un modelo de software tradicional, grupos de tecnología de información (IT) de empresa compran software, despliegan el software y gestionan el software en su propio centro de datos. En un modelo de este tipo, el grupo de IT es responsable del rendimiento y disponibilidad de las aplicaciones o software comprados. Tradicionalmente, tales grupos de IT usan herramientas para supervisar las aplicaciones de software para asegurar un rendimiento y disponibilidad consistentes.

Software como un Servicio (SaaS), en ocasiones denominado como "software bajo demanda" o "software en la nube", habitualmente es un modelo de distribución de software y sus datos asociados se alojan centralmente (habitualmente en la Internet o nube) y habitualmente se acceden por usuarios desde un dispositivo informático (por ejemplo, de sobremesa, portátil, de mano, tableta, teléfono inteligente, *etc.)* usando un navegador web a través de la Internet. SaaS se ha convertido en un modelo de distribución común para muchas aplicaciones empresariales, incluyendo contabilidad, colaboración, gestión de relaciones con clientes (CRM), planificación de recursos empresariales (ERP), facturación, gestión de recursos humanos (HRM), gestión de contenidos (CM) y gestión de servicio de asistencia, *etc.* SaaS se ha incorporado a la estrategia de muchas empresas líderes de software empresarial.

Sin embargo, en el modelo de servicios de SaaS, en el que el software a menudo se proporciona como un servicio por una tercera parte, organizaciones de usuarios finales frecuentemente se suscriben directamente con un proveedor de software. Como tal, un usuario final generalmente contacta directamente con el proveedor de SaaS para proporcionar el software con un cierto nivel de rendimiento o disponibilidad.

Sin embargo, a menudo los usuarios finales no tienen ni las capacitaciones ni los recursos económicos para rastrear activamente tales niveles de servicio de SaaS. Ni generalmente tendrían las herramientas para rastrear tales niveles incluso si quisieran. Frecuentemente, no existen acuerdos de nivel de servicios (SLA) consistentes desde una perspectiva de empresa e incluso donde existen SLA, existen pocas herramientas para rastrear el rendimiento y mucho menos para cumplir con los niveles de servicio. Como tal, frecuentemente las empresas ya no pueden depender de sus grupos de IT para que sean responsables de las operaciones y gestión de aplicaciones de misiones críticas. A menudo, el grupo de IT se reduce para soportar meramente acceso a red y escritorio a proveedores de SaaS y no el rendimiento de las propias aplicaciones de SaaS. Frecuentemente, proveedores de SaaS son ahora responsables del rendimiento de la aplicación y los grupos de IT de empresa pueden incluso no tener una relación directa con el proveedor de SaaS.

El documento US 2012 042064 A1 explica un enfoque de supervisión para dos redes, tal como una red de servidor y una red de cliente (es decir, Internet e Intranet), en el que la comunicación de redes con datos encriptados. Puntos de derivación en ambas redes recopilan datos encriptados, y un dispositivo de analizador procesa los datos desde ambos puntos para obtener métricas.

El documento US 5.521.907 explica mediciones de retardo de ida y vuelta en una red de comunicaciones durante operación en servicio. Se sitúan dos sondas como puntos de interés a lo largo de la red de comunicación. Las sondas reciben patrones de datos identificables transmitidos a través de la red de comunicaciones y generan una indicación de tiempo cuando el patrón llega o abandona el punto. Cada sonda adicionalmente genera un identificador de patrón y una indicación de tiempo como un par en una memoria intermedia interna. Una vez que la memoria intermedia interna excede una cantidad de datos predeterminada, se calcula un promedio de retardo de ida y vuelta basándose en indicaciones de tiempo de salida y llegada.

Jianbin Wei et al. "Measuring Client-Perceived Pageview Response Time of Internet Services" IDEE Transactions on Parallel and Distributed Systems, IEEE Service Center, Los Alamitos, California, Estados Unidos, vol. 22, n.º 5, mayo de 2011, página 773-785 investigan los tiempos de respuesta en las comunicaciones entre servidor y ordenadores de cliente que usan el protocolo HTTPS. El documento también introduce un supervisor que mide tiempos de respuesta percibidos por clientes para tráfico HTTP y HTTPS.

Sumario

La invención se define por las reivindicaciones adjuntas.

De acuerdo con un aspecto general, un método de uso de un primer dispositivo de sondeo puede incluir supervisar

una o más sesiones de comunicaciones encriptadas entre un primer dispositivo informático y un segundo dispositivo informático. En algunas implementaciones del método, cada sesión de comunicaciones encriptadas incluye transmitir una pluralidad de objetos de datos encriptados entre el primer y segundo dispositivos informáticos. El método puede incluir obtener, por el primer dispositivo de sondeo, información de temporización con respecto a una sesión de comunicaciones encriptadas. El método puede incluir también transmitir, desde el primer dispositivo de sondeo a un segundo dispositivo de sondeo, la información de temporización obtenida.

De acuerdo con otro aspecto general, un sistema puede incluir un primer y un segundo puntos de derivación de red y un dispositivo de sondeo de lado de cliente. El primer punto de derivación de red puede configurarse para duplicar, de una manera no intrusiva, al menos parte de una comunicación de red encriptada transmitida a y desde un dispositivo de punto de acceso que forma el límite entre una primera red y una segunda red. El segundo punto de derivación de red puede configurarse para duplicar, de una manera no intrusiva, al menos parte de una comunicación de red encriptada transmitida a y desde un dispositivo informático de servidor situado dentro de, en un sentido de topología de red, la segunda red. El dispositivo de sondeo de lado de cliente puede configurarse para supervisar sesiones de comunicaciones encriptadas entre el dispositivo informático de servidor y el dispositivo informático de cliente, en el que cada sesión de comunicaciones encriptadas incluye transmitir una pluralidad de objetos de datos encriptados entre el servidor y dispositivos informáticos de cliente. El dispositivo de sondeo de lado de cliente puede configurarse para obtener información de temporización con respecto a una sesión de comunicaciones encriptadas basándose en uno o más objetos de datos encriptados recibidos incluidos por la sesión de comunicaciones encriptadas. El dispositivo de sondeo de lado de cliente puede configurarse para transmitir, a un dispositivo de sondeo de lado de servidor, la información de temporización obtenida.

De acuerdo con otro aspecto general, un producto de programa informático para gestionar una red puede incorporarse de forma tangible y no transitoria en un medio legible por ordenador. El programa informático puede incluir código ejecutable que, cuando se ejecuta, se configura para provocar que un aparato supervise sesiones de comunicaciones encriptadas entre un primer dispositivo informático y un segundo dispositivo informático, en el que cada sesión de comunicaciones encriptadas incluye transmitir una pluralidad de objetos de datos encriptados entre el primer y segundo dispositivos informáticos. El código ejecutable provoca que el aparato obtenga, por el aparato, información de temporización con respecto a una sesión de comunicaciones encriptadas basándose en uno o más objetos de datos encriptados recibidos incluidos por la sesión de comunicaciones encriptadas. El código ejecutable puede provocar que el aparato transmita, desde el aparato a un segundo aparato, la información de temporización obtenida.

Los detalles de una o más implementaciones se exponen en los dibujos adjuntos y la descripción a continuación. Otras características serán evidentes a partir de la descripción y los 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 temporización de una realización de ejemplo de un sistema de acuerdo con la materia objeto divulgada.
La Figura 5 es un diagrama de temporización 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 es meramente un ejemplo ilustrativo al que no se limita la materia objeto. Además, se entiende que, mientras se ilustran dos redes o segmentos de red 195 y 106, la materia objeto divulgada no se limita a ningún número de tal red o segmentos de red.

En diversas realizaciones, el sistema 100 puede incluir una primera red de comunicaciones (por ejemplo, intranet 196, *etc.)* que incluye un dispositivo informático de cliente 102. Habitualmente, la primera red de comunicaciones 196 puede estar bajo el control de un único grupo de IT o unidad de negocio. En diversas realizaciones, el sistema 100 puede incluir una segunda red de comunicaciones (por ejemplo, internet 195, *etc.)* que incluye, al menos desde el punto de vista del dispositivo informático de cliente 102, el dispositivo informático de servidor 106. Habitualmente, esta segunda

red de comunicaciones 195 puede no estar bajo el control del grupo de IT o unidad de negocio. Se entiende que lo anterior son meramente unos pocos ejemplos ilustrativos a los que no se limita la materia objeto divulgada.

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

En una realización, el dispositivo informático ilustrado como el servidor 106 puede incluir cualquier dispositivo de pares (por ejemplo, cliente o servidor, *etc.)* que comunica, al menos parcialmente, a través de un protocolo encriptado (por ejemplo, protocolo de Capa de Conexiones Seguras (SSL), protocolo de Seguridad de Capa de Transporte (TLS), *etc.).* Además, mientras la comunicación entre los dispositivos 106 y 102 se describe generalmente como que implica el Protocolo de Transferencia de Hipertexto (HTTP) y/o el protocolo de HTTP Seguro (HTTPS), se entiende que lo anterior son meramente unos pocos ejemplos ilustrativos a los que no se limita la materia objeto divulgada. Finalmente, se entiende que los dispositivos 102, 104, 106, 108, 108b y 109 pueden incluir instanciaciones de tales dispositivos incluidos en respectivos entornos modulares o virtuales (por ejemplo, un sistema de servidor de tipo blade, máquinas virtuales, *etc.).*

En diversas realizaciones, el sistema 100 puede incluir un dispositivo informático de cliente o cliente 102 configurado para consumir o hacer uso del servicio (por ejemplo, aplicación empresarial 180, aplicación de SaaS, *etc.)* proporcionado por el servidor 106. En una realización, el cliente 102 puede incluir un procesador, memoria e interfaz de red (no mostrados, pero análogos a los 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 accede o visualiza el servicio o aplicación 180 proporcionado por el servidor 106. En algunas realizaciones, el cliente 102 puede controlarse o usarse por un usuario 190. En diversas realizaciones, el cliente 102 puede incluir un ordenador tradicional (por ejemplo, un ordenador de escritorio, portátil, de mano, *etc.)* o un dispositivo informático no tradicional (por ejemplo, teléfono inteligente, tableta, equipo con recursos limitados, terminal informático, *etc.).* Se entiende que mientras se ilustra únicamente un cliente 102 la materia objeto divulgada no se limita a ningún número particular de dispositivos de cliente 102.

En diversas realizaciones, el sistema 100 puede incluir un dispositivo de punto de acceso (AP) o dispositivo de AP de intranet/internet 104. En una realización de este tipo, el dispositivo de AP 104 puede configurarse para separar la primera y segunda redes (por ejemplo, intranet 196 e internet 195, *etc.).* En diversas realizaciones, el dispositivo de AP 104 puede incluir un encaminador, un cortafuegos, un servidor de intermediario, *etc.* o una combinación de los mismos. Se entiende que lo anterior son meramente unos pocos ejemplos ilustrativos a los que no se limita la materia objeto divulgada.

En diversas realizaciones, el dispositivo de AP 104 puede incluir un procesador 152 configurado para ejecutar un flujo o instrucciones ejecutables por máquina (por ejemplo, sistema operativo, aplicación 158, *etc.).* El dispositivo de AP 104 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 misma pueden configurarse para almacenar datos de una forma temporal (por ejemplo, Memoria de Acceso Aleatorio (RAM), *etc.)* como parte de la ejecución de instrucciones por el procesador 152. La memoria 154 o porciones de la misma pueden configurarse para almacenar datos de una forma semipermanente o a largo plazo (por ejemplo, un disco duro, memoria de estado sólido, memoria flash, almacenamiento óptico, *etc.*).

En diversas realizaciones, el dispositivo de AP 104 puede incluir una o más interfaces de red 156 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 o normas por cable (por ejemplo, Ethernet, Canal por Fibra, *etc.)* o inalámbricos (por ejemplo, Wi-Fi, celular, *etc.)* o una combinación de los mismos.

En una realización, el dispositivo de AP 104 puede incluir un dispositivo o aplicación de AP 158 que actúa como un intermediario entre el cliente 102 y el servidor 106. En la realización ilustrada, que ilustra el dispositivo de AP 104 como un servidor de intermediario, el cliente 102 puede hacer una petición al dispositivo de AP 104 para acceder al servidor 106 en nombre del cliente 102. En una realización de este tipo, el dispositivo de AP 104 puede reenviar a continuación (a menudo reempaquetando y encapsulando) la comunicación desde el cliente 102 al servidor 106. Análogamente, el servidor 106 puede contactar con el dispositivo de AP 104 con información o datos que tienen que reenviarse al cliente 102.

En una realización de este tipo, la comunicación entre el servidor 106 y el cliente 102 puede tener lugar en dos partes. Puede producirse una porción o parte de lado cliente entre el cliente 102 y el dispositivo de AP 104 a través de la

intranet 196. Puede producirse una porción de lado de servidor entre el servidor 106 y el dispositivo de AP 104 a través de la internet 195. En combinación, estas porciones de lado de cliente y servidor pueden constituir la comunicación entre los dos dispositivos 102 y 106 a través de las dos redes 195 y 196.

A menudo, una o ambas de estas porciones de lado de cliente y lado de servidor pueden encriptarse. En una realización de este tipo, cada una de las respectivas porciones encriptadas de la comunicación de red puede incluir sus respectivas claves de encriptación o credenciales de seguridad.

Por ejemplo, la comunicación entre el servidor 106 y el cliente 102 puede encriptarse a través del protocolo de Protocolo de Transferencia de Hipertexto (HTTP) Seguro (HTTPS) que hace uso de los protocolos de Capa de Conexiones Seguras (SSL) y/o Seguridad de Capa de Transporte (TLS) para proporcionar comunicación encriptada e identificación segura entre dos dispositivos en red. Se entiende que lo anterior es meramente un ejemplo ilustrativo al que no se limita la materia objeto.

En la realización ilustrada, un departamento de IT u otra entidad puede desear supervisar y analizar la comunicación de red entre el cliente 102 y el servidor 106. Para hacer esto, el departamento de IT u otra entidad puede situar un punto de sonda o derivación de red 107 en una red (por ejemplo, 196, *etc.).* En este contexto, un "punto de derivación de red" o "punto de sonda de red" incluye un medio sustancialmente no invasivo de observación o supervisión de comunicación de red a través de la porción de la red en la que se ha situado el punto de derivación de red 107. En la realización ilustrada, el punto de derivación de red 107 se sitúa de tal forma que se supervisa u observa cualquier comunicación de red transmitida o recibida por el servidor 106.

Sin embargo, situar un único punto de derivación de red 107 en el lado de internet 195 del dispositivo de AP 104 puede no ser una realización preferida. En diversas realizaciones, esto puede ser porque un único punto de derivación cerca del servidor (por ejemplo, punto de derivación 107, *etc.)* puede no proporcionar visibilidad en cuanto a qué segmento de los múltiples segmentos potenciales entre 102 y 106 podría ser el segmento cuello de botella. Se entiende que lo anterior es meramente un ejemplo ilustrativo al que no se limita la materia objeto. En diversas realizaciones, cuantos más segmentos de red haya más puntos de derivación pueden desearse.

Por ejemplo, en la realización ilustrada, puede situarse un segundo punto de derivación o sonda 107b de tal forma que cualquier comunicación de red que atraviesa el dispositivo de AP 104 puede supervisarse u observarse. En diversas realizaciones, pueden añadirse por todo el sistema puntos de derivación adicionales o una pluralidad de puntos de derivación. Por ejemplo, un tercer y cuarto puntos de derivación (no mostrados) pueden añadirse en puntos estratégicos o deseables dentro del sistema para supervisar u obtener métricas de rendimiento para segmentos de red adicionales (por ejemplo, entre cliente 102 y dispositivo de AP 104, *etc*.). En diversas realizaciones, el punto de derivación 107b y/o cualquier punto de derivación adicional (no mostrado) puede ser similar o análogo al punto de derivación 107 descrito en este documento. Se muestra y analiza otra realización en referencia con la Figura 2, como se describe a continuación. Se entiende que lo anterior son meramente un ejemplo ilustrativo al que no se limita la materia objeto divulgada.

En diversas realizaciones, el punto de sonda o derivación de red 107 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 una realización de este tipo, una de las señales de red salientes puede transmitirse a su destino normal (por ejemplo, dispositivo de AP 104 o dispositivo de cliente 102, *etc.)* y la segunda señal de red saliente puede transmitirse a un dispositivo de escucha, intercepción o derivación (por ejemplo, dispositivo de sondeo 108, *etc.).* En una realización de este tipo, cualquier retardo añadido a la señal de comunicaciones de red puede ser mínimo o sustancialmente imperceptible y la señal de red puede no alterarse o procesarse. Como tal, el punto de derivación de red 107 puede funcionar de una manera sustancialmente no intrusiva.

En diversas realizaciones, los puntos de derivación de red 107 y 107b pueden situarse cerca, en un sentido de topología de red, al dispositivo de servidor 106 o, respectivamente, al dispositivo de AP 104 en cuanto a capturar o duplicar comunicación de red que pasa entre el dispositivo de servidor 106 y el dispositivo de cliente 102 a través del dispositivo de AP 104 o a través del límite entre las dos redes (por ejemplo, un límite de internet 195/intranet 196, *etc.).* En la realización ilustrada, los puntos de derivación de red 107 y 107b pueden proporcionar una vista de la comunicación de red del servidor 106/cliente 102 desde un punto de vista más cercano al cliente 102 o al dispositivo de AP 104 (punto de derivación 107b) y al servidor 106 (punto de derivación 107). Se entiende que lo anterior es meramente un ejemplo ilustrativo al que no se limita la materia objeto.

En una realización, el dispositivo de sondeo 108 puede incluir un procesador 112, memoria 114 e interfaz de red 116, análogos a los descritos anteriormente. Como se ha descrito anteriormente, en diversas realizaciones, la memoria 114 puede incluir almacenamiento volátil (por ejemplo, Memoria de Acceso Aleatorio *etc.),* almacenamiento no volátil (por ejemplo, un disco duro, una unidad de estado sólido, *etc.)* o una combinación de los mismos. En algunas realizaciones, el dispositivo de sondeo 108 puede incluir el punto de sonda o derivación de red 107.

En diversas realizaciones, el dispositivo de sondeo 108 puede configurarse para supervisar y analizar tanto comunicación de red encriptada como/o no encriptada. En una realización de este tipo, el dispositivo de sondeo 108

puede generar un conjunto de métricas 122 con respecto al rendimiento de la comunicación de red entre el cliente 102 y el servidor 106. Estas métricas 122 pueden transmitirse o visualizarse dentro de una interfaz de usuario (UI) 142 de una aplicación de IT 140 que se ejecuta por un dispositivo informático de IT 109. En diversas realizaciones, el dispositivo informático de IT 109 puede incluir un ordenador tradicional (por ejemplo, un ordenador de escritorio, portátil, de mano, *etc.)* o un dispositivo informático no tradicional (por ejemplo, teléfono inteligente, tableta, equipo con recursos limitados, terminal informático, *etc.).*

En la realización ilustrada, el dispositivo de sondeo 108 puede configurarse para recibir o supervisar tráfico capturado por el punto de derivación 107 en el lado de servidor. A la inversa, el dispositivo de sondeo 108b puede configurarse para recibir o supervisar tráfico capturado por el punto de derivación 107b en el lado de cliente. En diversas realizaciones, el dispositivo de sondeo 108b puede incluir elementos y realizar algunas o todas las funciones de forma similar al dispositivo de sondeo 108, como se describe en este documento. En otra realización, tal como la analizada en referencia con la Figura 2, los dispositivos de sondeo 108 y 108b pueden realizar funciones similares pero diferentes o incluir diferentes elementos. Se entiende que lo anterior es meramente un ejemplo ilustrativo al que no se limita la materia objeto.

En una realización, el dispositivo de sondeo 108 puede incluir un supervisor de tráfico 118 configurado para supervisar comunicación de red capturada o duplicada por el punto de derivación de red 107. En diversas realizaciones, esta comunicación de red puede incluir comunicación encriptada de red entre el cliente 102 y el servidor 106. En la realización ilustrada, la comunicación encriptada puede incluir una porción de la comunicación de cliente/servidor que se produce entre el cliente 102 y el dispositivo de AP 104. En una realización más preferida (por ejemplo, el sistema 200 de la Figura 2), el punto de derivación 107 puede situarse para capturar comunicación encriptada entre el servidor 106 y el dispositivo de cliente 102. Se entiende que lo anterior son meramente unos pocos ejemplos ilustrativos a los que no se limita la materia objeto divulgada.

En algunas realizaciones, como se describe a continuación en referencia con la Figura 2, el supervisor de tráfico 118 del dispositivo de sondeo de lado de servidor 108 puede configurarse para desencriptar toda o parte de la comunicación de red capturada por uno o más puntos de derivación de red. En otras realizaciones, como se describe a continuación en referencia con la Figura 2, el dispositivo de sondeo 108 puede configurarse para desencriptar toda o parte de la comunicación de red capturada por el punto de derivación de red 107 y puede supervisar y analizar tal tráfico.

A la inversa, el dispositivo de sondeo de lado de cliente 108b puede no configurarse para desencriptar ninguna o parte de la comunicación de red capturada por el punto de derivación de red 107b, pero aún puede supervisar y analizar tal tráfico. En diversas realizaciones, puede impedirse que el dispositivo de sondeo 108b sea capaz de desencriptar las comunicaciones de red porque una clave de encriptación privada asociada con el dispositivo de servidor 106 (ilustrado en la Figura 2) permanece dentro del dispositivo de servidor por razones de seguridad.

En una realización de este tipo, el dispositivo de sondeo 108 puede configurarse para desencriptar la comunicación de red porque está dentro del dominio (por ejemplo, centro de datos seguros del dispositivo de servidor 106, *etc.)* y se puede confiar con la clave de encriptación privada, mientras que el dispositivo de sondeo de lado de cliente 108b (y otros puntos de derivación, como se describe a continuación) están habitualmente sin o fuera del dominio (por ejemplo, fuera del centro de datos seguros, *etc.)* y no tienen acceso a la clave de encriptación privada que se usa para desencriptar la comunicación de red. Esta capacidad para desencriptar al menos parcialmente tráfico de comunicación encriptada de red contrasta con los esquemas de supervisión de comunicación de red tradicionales que generalmente descartan o no supervisan la comunicación encriptada de red ya que el analizador 120 u otras porciones de los dispositivos de sondeo 108 y/o 108b son incapaces de procesar comunicación encriptada de red.

En una realización, el dispositivo de sondeo 108 puede incluir un analizador de tráfico 120 configurado para analizar la comunicación de red supervisada y generar el conjunto de métricas 122. En diversas realizaciones, el conjunto de métricas 122 puede incluir información, tal como, la latencia añadida por la intranet 196 o el dispositivo de AP 104, el rendimiento de diversos servidores 106, la disponibilidad del servidor 106, el número de accesos o páginas web solicitadas desde/proporcionadas por el servidor 106, el número de errores, retransmisiones o, de otra manera, interacciones de comunicación de red fallidas (por ejemplo, vistas de páginas web, *etc.)* entre el dispositivo o dispositivos de cliente 102 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 cliente 102, una determinación de dónde se produce cualquier error en la red (por ejemplo, el servidor 106, el dispositivo de AP 104, el cliente 102, *etc.)*, el número de veces que se accede al servidor 106 (por ejemplo, vistas de páginas, *etc.)* en un periodo de tiempo dado, el número de dispositivos de cliente 102 que acceden al servidor 106 en cualquier momento dado o periodo de tiempo, métricas de rendimiento por cada uno de una pluralidad de servidores 106 o intranets 196, *etc.* En diversas realizaciones, estas métricas pueden compilarse para la comunicación de cliente/servidor general, comunicaciones que implican solo una de las redes (por ejemplo, AP de servidor a dispositivo, AP cliente a dispositivo, *etc*.), o una combinación de las mismas. Se entiende que lo anterior son meramente unos pocos ejemplos ilustrativos a los que no se limita la materia objeto divulgada.

Como se describe a continuación, en diversas realizaciones, el analizador de tráfico 120 puede configurarse para

emparejar o correlacionar comunicación de red desde un lado (por ejemplo, lado de cliente) del límite de internet 195/intranet 196 con comunicación de red desde el otro lado (por ejemplo, lado de servidor) del límite de internet 195/intranet 196. Como se describe a continuación, esto puede incluir emparejar comunicación de red desde dos puntos de derivación 107 y 107b (o puntos de derivación adicionales dependiendo de la realización) basándose en un conjunto predeterminado de criterios. En diversas realizaciones, la comunicación de red supervisada o capturada desde un lado (por ejemplo, el lado de servidor) puede encriptarse y el dispositivo de sondeo 108 puede no ser capaz de desencriptar esa porción de la comunicación de red supervisada. En una realización de este tipo, el analizador de tráfico 120 puede configurarse aún para emparejar o correlacionar, como mejor pueda, las dos porciones (por ejemplo, lado de servidor y lado de cliente) de la comunicación de red.

En diversas realizaciones, el dispositivo de sondeo 108 puede incluir un generador de métricas 124 configurado para generar un conjunto de métricas 122 y, en algunas realizaciones, el generador de métricas 124 también puede configurarse para generar un conjunto de información de temporización (u otra estadística) 123 con respecto a las comunicaciones supervisadas el dispositivo de sondeo 108.

En una realización, el dispositivo de sondeo de lado de cliente 108b también puede incluir un generador de métricas 124 (y otros componentes similares al dispositivo de sondeo 108, que no se muestran explícitamente debido a consideraciones de espacio). En una realización de este tipo, el dispositivo de sondeo de lado de cliente 108b puede no configurarse para desencriptar las comunicaciones encriptadas de red, pero puede ser capaz de generar u obtener información de temporización 123b basándose en las comunicaciones encriptadas de red supervisadas a través del punto de derivación 107b. A continuación se describen diversas técnicas para generar tal información de temporización 123b en referencia con las Figuras 4 y 5.

En algunas realizaciones, ambos dispositivos de analizador de punto de derivación 108 y 108b pueden configurarse para generar información de temporización 123 y 123b para diversas porciones de la comunicación de red que se supervisan por el dispositivo de sondeo particular. En una realización de este tipo, un dispositivo de sondeo particular (dispositivo de sondeo 108b) puede no ser capaz de desencriptar la comunicación encriptada de red y, por lo tanto, puede no ser capaz de generar métricas 122 o información de temporización 123 tan detalladas como se desean. En una realización de este tipo, el dispositivo de sondeo particular (por ejemplo, el dispositivo de sondeo 108b) puede configurarse para transmitir esta información de temporización 123b al segundo u otro dispositivo de sondeo (por ejemplo, dispositivo de sondeo 108).

Como se describe a continuación en referencia con la Figura 2, el segundo dispositivo de sondeo o dispositivo de sondeo de recepción (*por ejemplo*, dispositivo de sondeo 108) puede configurarse para desencriptar las comunicaciones encriptadas de red que supervisa. En una realización de este tipo, este o al menos su analizador de tráfico 120 puede configurarse para emparejar o asociar la información de temporización recibida 123b con las comunicaciones de red desencriptadas que supervisa o información de temporización 123 obtenida de las mismas. En una realización de este tipo, combinando la información proporcionada por la información de temporización recibida 123 y 123b y las comunicaciones de red supervisadas localmente puede generarse un conjunto más completo de métricas 122.

Por ejemplo, un único objeto de datos o transacción de comunicación puede incluir una vista de página web que tiene unas fases de petición, cumplimiento y acuse de recibo. Esa comunicación de vista de página web puede incluir dos porciones: una porción de lado de cliente entre el cliente 102 y el dispositivo de AP 104, y una porción de lado de servidor entre el servidor 106 y el dispositivo de AP 104. Tanto la porción de lado de cliente como la porción de lado de servidor pueden tener sus propias respectivas métricas de rendimiento (por ejemplo, latencia, *etc.).* Debido a que la comunicación de vista de página web se divide en dos partes (lado de cliente y lado de servidor) puede no ser posible medir directamente, por ejemplo, la latencia o tiempo desde el inicio hasta la finalización de la comunicación de vista de página web como se mide desde el cliente 102 al servidor 106. Sin embargo, si los dos lados o porciones de la comunicación se emparejan, la latencia de cliente/servidor puede determinarse basándose en la latencia de cliente/dispositivo de AP (latencia de lado de cliente) y la latencia de dispositivo de AP/servidor (latencia de lado de servidor), ambas de las cuales pueden medirse directamente. Se entiende que lo anterior es meramente un ejemplo ilustrativo al que no se limita la materia objeto.

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 de AP de lado de cliente 204, una internet o segunda red 295 y un servidor 206 al que se accede a través de o por medio de la segunda red 295. En diversas realizaciones, el sistema 200 puede incluir un dispositivo de AP de lado de servidor 204s. El sistema ilustrado 200 muestra una realización en la que el dispositivo de AP 204 (dispositivo de AP 204s) puede no ser un intermediario, sino simplemente un encaminador u otro dispositivo. Se entiende que lo anterior es meramente un ejemplo ilustrativo al que no se limita la materia objeto.

En una realización de este tipo, un punto de derivación de lado de cliente 212 puede situarse cerca de, en un sentido de topología de red, el lado de servidor del dispositivo de AP 204. Análogamente, en la realización ilustrada, un punto de derivación de lado de servidor 280 puede situarse cerca de, en un sentido de topología de red, el servidor 206. En la realización ilustrada, la comunicación de red entre el cliente 202 y el servidor 206 puede producirse de una manera

encriptada o al menos parcialmente encriptada (ilustrada a través del gráfico de candado cerrado).

Como se ha descrito anteriormente, pueden añadirse una pluralidad de puntos de derivación o sonda, en algunas realizaciones, a diversos puntos por todo el sistema 200. En otras realizaciones, pueden existir intermediarios de tunelización entre el cliente 202 y servidor 206 que crea segmentación de red adicional. Se entiende que lo anterior es meramente un ejemplo ilustrativo al que no se limita la materia objeto.

En una realización, la infraestructura de servidor puede usar un equilibrador de carga, un terminador de SSL o cualquier clase de controlador de entrega de aplicación (ADC). En general, el punto de rastreador o derivación de lado de servidor 280 puede instalarse en frente de tal dispositivo. Siempre que la infraestructura de cliente pueda usar una pasarela, intermediario u otro dispositivo, el punto de derivación 212 puede estar alejado del cliente 202, en el punto enfrentado al servidor 204. Se entiende que lo anterior son meramente unos pocos ejemplos ilustrativos a los que no se limita la materia objeto divulgada.

En diversas realizaciones, tanto el punto de derivación de lado de servidor 280 como el punto de derivación de lado de cliente 212 pueden situarse para ver o supervisar cualquier tráfico de comunicación encriptada de red entre el cliente 202 y el servidor 206 *(por ejemplo,* tráfico de SSL o TLS, *etc.).* Como se describe a continuación, en diversas realizaciones, mientras ambos puntos de derivación 212 y 280 pueden ser capaces de supervisar u observar las comunicaciones encriptadas de red, únicamente puede configurarse un punto de derivación 280 (o un dispositivo asociado, tal como, dispositivo de sondeo 208, *etc.)* para desencriptar la comunicación encriptada de red supervisada.

Además, en diversas realizaciones, puede existir un número de otros dispositivos dentro de una red intermedia (por ejemplo, la internet 295). En una realización de este tipo, las comunicaciones de red (por ejemplo, paquetes, *etc.)* establecidas por el servidor 206 al cliente 202 pueden alterarse de forma suficiente durante la transmisión de tal forma que el cualquier temporizador de encabezamiento o información de identificación incluida en los paquetes puede perderse, convertirse en no fiable o más generalmente no utilizable para propósitos de supervisión de red. En una realización de este tipo, los dispositivos de sondeo 268 y 208 pueden configurarse para no depender de información en los encabezamientos de paquete que pueden cambiarse por un dispositivo intermedio.

En una realización, el sistema 200 puede incluir un dispositivo de sondeo de red de lado de servidor 208 y un dispositivo de sondeo de red de lado de cliente 268. En una realización de este tipo, el dispositivo de sondeo de red 268 puede configurarse para recibir una copia de la comunicación de red 222 capturada o duplicada por el punto de derivación de red 212. Análogamente, el dispositivo de sondeo de red 208 puede configurarse para recibir una copia de la comunicación de red 220 capturada o duplicada por el punto de derivación de red 280.

En diversas realizaciones, el dispositivo de sondeo de red 268 puede no ser capaz de desencriptar la comunicación de red 220. Independientemente, el dispositivo de sondeo de red 268 puede configurarse para supervisar la comunicación encriptada de red 222 y no descartar o ignorar la comunicación encriptada de red u objetos de datos. Sin embargo, como se describe a continuación, en diversas realizaciones, porciones de la comunicación encriptada de red u objetos de datos pueden no analizarse o ignorarse 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 trama, y puede medirse en términos de bytes, bits o caracteres. Usado en este documento el término "paquete" puede usarse como una realización específica de ejemplo de un tipo de objeto de datos.

En diversas realizaciones, el objeto de datos puede incluir una porción de encabezamiento y una porción de carga útil. En una realización de este tipo, la porción de encabezamiento puede indicar, como mínimo, los dispositivos de destino y fuente intermedios desde/a los que se transmite el objeto de datos, respectivamente (por ejemplo, dispositivo de cliente 202 y dispositivo de AP 204, dispositivo de AP 204 y servidor 206, *etc.).* La porción de carga útil puede incluir cualquier información transmitida por el objeto de datos y también puede incluir información de encabezamiento o encaminamiento encapsulada (por ejemplo, en el caso en el que la comunicación de red se interrumpe por o implica un servidor de intermediario, una información de red área local virtual, una información de red privada virtual, *etc.).* En algunas realizaciones, esta porción de carga útil puede encriptarse. En diversas realizaciones, comunicación de red puede incluir un flujo o pluralidad de diversos objetos de datos que transmiten respectivas piezas de información entre dos dispositivos (por ejemplo, cliente 202 y servidor 206, *etc.).*

En diversas realizaciones, en las que se supervisa la comunicación encriptada de red, el dispositivo de sondeo de cliente 268 puede configurarse para proporcionar métricas de rendimiento de red limitadas (por ejemplo, latencia, *etc.,* como se ha descrito anteriormente, *etc.)* basándose en la porción de red entre el punto de derivación 212 y el servidor 206. En una realización de este tipo, el dispositivo de sondeo 268 puede configurarse para proporcionar métricas limitadas o estadísticas de rendimiento de red.

En diversas realizaciones, puede emplearse un punto de derivación de lado de servidor 280. En una realización de este tipo, el sistema 200 puede incluir un dispositivo de sondeo de servidor 208. El dispositivo de sondeo de servidor 208 puede configurarse para supervisar la comunicación encriptada de red 220 y no descartar o ignorar la

comunicación encriptada de red u objetos de datos.

A diferencia del dispositivo de sondeo de cliente 268, el dispositivo de sondeo de servidor 208 puede integrarse de forma más estricta o más confiable. En una realización de este tipo, el servidor 206 puede proporcionar al dispositivo de sondeo de servidor 208 con las claves privadas del servidor o credenciales de seguridad 295. En una realización de este tipo, el dispositivo de sondeo de servidor 208 puede, como parte de la supervisión de la comunicación de red 220, detectar cuándo se está iniciando una nueva sesión de comunicación de red encriptada (por ejemplo, la fase de negociación de SSL de la sesión de SSL, *etc.),* y extraer (usando la clave de servidor 294) la clave de encriptación de sesión o credenciales de seguridad de sesión 296 para cada sesión de comunicación de red encriptada. En diversas realizaciones, esto puede permitir que el dispositivo de sondeo de servidor 208 desencripte la comunicación de red de lado de servidor supervisada 220.

En una realización de este tipo, la comunicación de red de lado de servidor encriptada 220 puede desencriptarse (por ejemplo, a través de una porción del desencriptador 218 del dispositivo de sondeo 208, e indicada en la ilustración por el gráfico de candado abierto). En diversas realizaciones, una porción de supervisor de tráfico (mostrada en la Figura 1) del dispositivo de sondeo 208 puede incluir el desencriptador 218.

En la realización ilustrada, el analizador 219 puede configurarse para proporcionar un mayor análisis y métricas más precisas que las del dispositivo de sondeo de cliente 268, que es incapaz de desencriptar comunicación encriptada de red. En una realización de este tipo, el analizador 219 puede configurarse para correlacionar o emparejar objetos de datos o porciones desde la comunicación de red de lado de servidor desencriptada con objetos de datos o porciones desde las comunicaciones de red de lado de cliente encriptadas. En diversas realizaciones, pueden proporcionarse diversas métricas basándose en estos objetos de datos emparejados que incluyen métricas para la comunicación de red de cliente 202/servidor 206 como un todo, así como métricas para cada lado o porción (lado de cliente, lado de servidor) de la comunicación de red.

Como se ha descrito anteriormente, el dispositivo de sondeo de cliente 268 puede no ser capaz de desencriptar el tráfico de comunicación de red supervisada encriptada 222. En una realización de este tipo, la información incluida por el tráfico de comunicación de red supervisada 222 que se analizaría normalmente (por ejemplo, Identificadores de Recursos Uniformes (URI), Localizadores de Recursos Uniformes (URL), cookies, *etc.)* puede no estar disponible para las porciones del tráfico supervisado 222 que están encriptadas. Sin embargo, el dispositivo de sondeo de cliente 268 puede configurarse para observar o examinar porciones de transacciones de HTTPS u otras porciones definibles del tráfico de comunicación de red supervisada encriptada 222 (por ejemplo, el inicio o final de un registro de SSL, como se describe a continuación, *etc.).* En diversas realizaciones, también puede observarse o examinarse otra información, tal como, por ejemplo, información de nivel de TCP/IP o métricas de temporización, *etc.* Se entiende que el uso de HTTP es meramente un ejemplo ilustrativo al que la materia objeto divulgada no está limitada.

En diversas realizaciones, el dispositivo de sondeo de cliente 268 puede incluir un supervisor 278 configurado para supervisar o registrar el tráfico de red supervisado 222. En una realización, el dispositivo de sondeo de cliente 268 puede incluir un generador de métricas 279 configurado para generar diversas métricas (por ejemplo, información de temporización 297) para porciones del tráfico de red supervisado 222. En la realización ilustrada, el generador de métricas 279 generó información de temporización 297; sin embargo, se entiende que temporización es meramente un ejemplo ilustrativo al que la materia objeto divulgada no está limitada.

En diversas realizaciones, esta información de temporización 297 puede transmitirse o enviarse desde el dispositivo de sondeo de cliente 268 al dispositivo de sondeo de servidor 208. En diversas realizaciones, las otras transacciones o métricas supervisadas u obtenidas pueden transmitirse o enviarse al dispositivo de sondeo de servidor 208.

En algunas realizaciones, el generador de métricas 279 puede configurarse para examinar las porciones no encriptadas (por ejemplo, encabezamientos, *etc.)* del tráfico de red supervisado 222. Como se ha descrito anteriormente, las porciones de carga útil pueden encriptarse y no ser legibles por el dispositivo de sondeo de cliente 268. Para cada paquete, unidad de datos, objeto de datos o, de otra manera, porción discreta del tráfico de red 222, el dispositivo de sondeo de cliente 268 puede detectar en qué dirección (por ejemplo, cliente a servidor, servidor a cliente, *etc.)* se dirige el paquete. En diversas realizaciones, esto puede hacerse basándose en el encabezamiento no encriptado.

Se entiende que la descripción y uso de HTTP y HTTPS es meramente un ejemplo ilustrativo al que la materia objeto divulgada no está limitada. En diversas realizaciones, pueden emplearse otros esquemas de protocolos y comunicaciones encriptados. Por ejemplo, tales protocolos pueden incluir Protocolo de Transferencia de Correo Simple (SMTP), Protocolo de Transferencia de Archivos de SSH (SFTP), *etc.* Se entiende que lo anterior son meramente unos pocos ejemplos ilustrativos a los que la materia objeto divulgada no está limitada.

En la realización ilustrada, paquetes u objetos de datos y sus métricas asociadas pueden emparejarse entre el lado de cliente y el lado de servidor usando la información de temporización 297 y 298. En algunas realizaciones, esta información de temporización puede obtenerse a partir de indicaciones de tiempo situadas en o incluidas por los objetos de datos o paquetes. En otra realización, como se describe a continuación, las indicaciones de tiempo pueden

incluirse con una serie de objetos de datos o paquetes.

En este contexto, una "sesión de comunicaciones de datos" puede incluir una serie de objetos de datos o paquetes agrupados juntos a través de un protocolo de comunicaciones. En una realización, una sesión de comunicaciones de datos puede incluir un registro de SSL/TLS que define un número de objetos de datos o paquetes como pertenecientes al registro de SSL/TLS y tiene un punto de inicio y punto de finalización definibles. En una realización de este tipo, un registro de SSL/TLS establece un conjunto de credenciales de encriptación para una serie de objetos de datos o paquetes. En diversas realizaciones, una sesión de SSL/TLS puede incluir una pluralidad de registros de SSL/TLS. Se entiende que lo anterior son meramente unos pocos ejemplos ilustrativos a los que no se limita la materia objeto divulgada.

En una realización, la información de temporización 297 puede registrarse o determinarse (por ejemplo, a través de indicaciones de tiempo, *etc.)* por el dispositivo de sondeo de cliente 268 para todos los objetos de datos o paquetes. En otra realización, el dispositivo de sondeo de cliente 268 puede generar únicamente información de temporización 297 a porciones particulares de las comunicaciones supervisadas o para ciertos tipos de objetos de datos o paquetes. Por ejemplo, en una realización, el dispositivo de sondeo de cliente 268 puede configurarse para ignorar o no determinar información de temporización 297 para ciertos tipos de paquetes (por ejemplo, paquetes de acuse de recibo (ACK), paquetes de negociación SSL/TLS intermedios, *etc.)* que se consideran (por ejemplo, a través de ajustes predeterminados, *etc.)* que no son útiles o deseables para medir latencias u otra información de métricas. En otra realización, pueden analizarse únicamente algunas porciones de una sesión de comunicaciones de datos.

Por ejemplo, el tiempo de finalización de SSL/TLS puede ser detectable ya que se transporta generalmente a través de cargas útiles no encriptadas. Los paquetes de negociación de SSL intermedios no son interesantes y pueden no supervisarse. A la inversa, la temporización de paquete de ACK de negociación de SSL/TLS final puede analizarse, para medir el tiempo de SSL/TLS, percibido en el lado de cliente. En una realización de este tipo, mensajes de negociación de SSL/TLS tales como SALUDO INICIAL de servidor de SSL/TLS, transferencias de certificados, intercambios de clave, *etc.* pueden no analizarse o incluirse en la información de temporización 297. En otra realización, la comunicación encriptada puede incluir accesos a grandes datos tales como filas o campos de una base de datos. En una realización de este tipo, algunas de las filas pueden no considerarse que son interesantes y pueden ignorarse o no supervisarse. En otras realizaciones más, porciones de las comunicaciones encriptadas pueden ignorarse o no supervisarse basándose en el protocolo o forma de la comunicación. Se entiende que lo anterior son meramente unos pocos ejemplos ilustrativos a los que no se limita la materia objeto divulgada.

En diversas realizaciones, una vez que el dispositivo de sondeo de cliente 268 ha determinado un número de métricas basadas en u obtenidas a partir de comunicaciones encriptadas 222, esta información de temporización 297 (u otra información de métricas supervisadas) puede transmitirse al dispositivo de sondeo de servidor 208. Se entiende que lo anterior es meramente un ejemplo ilustrativo al que no se limita la materia objeto.

En diversas realizaciones, el analizador 219 puede incluir un generador de métricas que se usa o emplea para generar un segundo conjunto de información de métricas (por ejemplo, información de temporización 298, *etc.)* que se basan en las comunicaciones de red desencriptadas 221. Esta información de temporización basada en desencriptación 298 puede compararse, a continuación, con la información de temporización basada en encriptación 297 para correlacionar o asociar porciones o transacciones dentro de las comunicaciones de red. En diversas realizaciones, si una porción de información de temporización sustancialmente basada en desencriptación y una porción de información de temporización basada en encriptación coinciden, el analizador 219 puede determinar que la porción subyacente de las comunicaciones de red coincide con una porción dada de las comunicaciones de red. El analizador 219 puede configurarse para generar un conjunto de métricas 299 basándose en la información disponible en las comunicaciones de red desencriptadas 221 (por ejemplo, encabezamientos de paquetes, vista de texto claro de mensajes de petición/respuesta, *etc.)* y el dispositivo de sondeo de cliente 268 dada la información de temporización 297. Se entiende que lo anterior es meramente un ejemplo ilustrativo al que no se limita la materia objeto.

En una realización, la información 221 que va desde el dispositivo de desencriptación 218 o 318 al analizador 219 puede no ser simplemente la carga útil de comunicación desencriptada. En una realización de este tipo, la información 221 puede incluir el modelo de un evento (por razones de eficiencia) y material vinculante.

En este contexto, el término "modelo de evento" puede incluir información de resumen (por ejemplo, en el caso de HTTP: URI, tiempo de inicio y finalización, algún encabezamiento particular, tamaño de byte, *etc.)* pero no la carga útil de texto claro completa. En una realización, el modelo puede incluir o representarse como archivos de valores separados por comas (CSV), o tablas de base de datos. En diversas realizaciones, el modelo de evento puede incluir una reducción esencial de la entropía de información del mensaje de texto claro real.

En este contexto, el "material vinculante" del evento puede incluir el material de emparejamiento de sesión de SSL/TLS del evento (por ejemplo, los números aleatorios de saludo inicial de cliente/servidor, *etc.)* y el paquete o bytes o números de registro de SSL/TLS "de interés" (dependiendo de la técnica usada). Se entiende que lo anterior es meramente un ejemplo ilustrativo al que no se limita la materia objeto.

En una realización de este tipo, el material vinculante y/o modelo de evento pueden usarse por el analizador 219 para emparejar o hacer coincidir las temporizaciones observadas remotamente 297 con el evento observado localmente o (en una realización) temporizaciones 298 y para asignar (vincular) las temporizaciones remotas a los puntos de interés equivalentes en este evento.

En diversas realizaciones, el analizador 219 también puede generar o transferir) de forma oportunista otras métricas 299. Por ejemplo, en una realización métricas relacionadas con TCP pueden incluir tiempo de ida y vuelta (RTT), recuento de fuera de orden (OOO), retransmisiones, recuento de paquetes, *etc.* En diversas realizaciones, las métricas 299 también pueden incluir métricas relacionadas con envolventes encriptadas (por ejemplo, detalles de negociación de SSL/TLS, *etc.)* basándose en el modelo del evento.

En diversas realizaciones, que puede requerirse que el desencriptador 218 contribuya al "material vinculante", porque el desencriptador 218 puede proporcionar la única o la oportunidad menos difícil para realizar tales observaciones en las comunicaciones encriptadas y proporcionar esas operaciones en relación con el modelo de evento. Se entiende que lo anterior es meramente un ejemplo ilustrativo al que no se limita la materia objeto.

En diversas realizaciones, el analizador 219 puede configurarse para determinar que dos objetos de datos (por ejemplo, una porción de tráfico de red encriptada y una porción de tráfico de red desencriptada, *etc.)* se emparejan o correlacionan si se cumplen un conjunto de criterios predefinidos. Se entiende que lo siguiente son meramente unos pocos criterios de ejemplo ilustrativos a los que la materia objeto divulgada no está limitada.

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 o un sistema similar al sistema 200 de la Figura 2.

En la realización ilustrada, el sistema 300 puede incluir un equilibrador de carga 304 en lugar del punto de acceso 204s de la Figura 2. Mientras se muestra un equilibrador de carga, se entiende que lo anterior es meramente un ejemplo ilustrativo al que la materia objeto no está limitada y pueden usarse otros dispositivos.

En la realización ilustrada, el equilibrio de cargar 304 puede incluir un desencriptador 318 configurado para desencriptar/encriptar las comunicaciones encriptadas de red entre el servidor 206 y cliente 202. En diversas realizaciones, el desencriptador 318 puede configurarse para hacer uso de o emplear la clave de sesión 296 como parte del proceso de desencriptación.

En una realización de este tipo, el dispositivo de sondeo de servidor 308 puede no incluir un desencriptador 218, a diferencia del dispositivo de sondeo de servidor 208 de la Figura 2. En una realización de este tipo, el punto de derivación 280 puede proporcionar una versión desencriptada 320 de las comunicaciones encriptadas de red 321. En una realización de este tipo, las comunicaciones de red desencriptadas 320 pueden ser las mismas que o sustancialmente equivalentes a (por ejemplo, permitiendo el almacenamiento en memoria intermedia o procesamiento auxiliar por el dispositivo de sondeo de servidor 308, *etc.)* las comunicaciones de red desencriptadas 221. En diversas realizaciones, las comunicaciones de red 320 pueden incluir el modelo de evento y material vinculante, como se ha descrito anteriormente en relación con las comunicaciones desencriptadas 221 de la Figura 2. Se entiende que lo anterior es meramente un ejemplo ilustrativo al que no se limita la materia objeto.

Se entiende que mientras se han mostrado en las Figuras 1, 2 y 3 realizaciones que muestran una sonda de lado de servidor que hace el desencriptado, la materia objeto divulgada no se limita a esa realización. Se entiende que lo anterior es meramente un ejemplo ilustrativo al que no se limita la materia objeto.

En una realización preferida, la sonda de no desencriptación puede configurarse para enviar datos a la sonda de desencriptación. En diversas realizaciones, esto puede tener ventajas relacionadas con razones de seguridad y también para una topología de SaaS. Por ejemplo, puede no desearse traer a todos los otros arrendatarios de SaaS a una única ubicación de arrendatarios de SaaS. Se entiende que lo anterior son meramente unos pocos ejemplos ilustrativos a los que no se limita la materia objeto divulgada.

En una realización, en un sistema cerrado en el que la comunicación o comunicaciones encriptadas se supervisan sin puntos de ventaja preferibles (por ejemplo, comunicaciones encriptadas dentro de un puente de red Privada Virtual (VPN) en una empresa), es concebible que cualquier sonda de todas envía sus temporizaciones a una tercera (u otra) entidad de análisis que no están sondeado en absoluto y ni siquiera en proximidad a cualquier sonda. Se entiende que lo anterior es meramente un ejemplo ilustrativo al que no se limita la materia objeto.

En diversas realizaciones, fabricantes de equipo de red pueden querer divulgar tales temporizadores de envolvente encriptados como un bloque componente de herramientas de supervisión de rendimiento. En una realización de este tipo, encaminadores, equilibradores de carga, servidores web, puntos de acceso VPN u otros dispositivos de interconexión en red, *etc.* pueden configurarse para producir las temporizaciones de envolvente de encriptación (por ejemplo*.,* SSL/TLS, *etc.)*... En una realización de este tipo, una sonda de desencriptación puede configurarse para enriquecer su modelo de datos con esos puntos de ventaja (por ejemplo, la información de temporización, *etc.).*

En una realización, el dispositivo de sondeo de servidor 308 puede incluir el analizador 219. En diversas realizaciones, el analizador 219 puede configurarse para emparejar las comunicaciones de red desencriptadas 221 a la información de temporización 297, como se ha descrito anteriormente. En una realización de este tipo, el analizador 219 puede configurarse para generar las métricas 299 basándose en la información disponible de las comunicaciones de red desencriptadas supervisadas 221 y la información de temporización 297 proporcionada por el dispositivo de sondeo de cliente 268.

La Figura 4 es un diagrama de temporización de una realización de ejemplo de un sistema de acuerdo con la materia objeto divulgada. Como se ha descrito anteriormente, en diversas realizaciones, los dispositivos intermedios pueden alterar o cambiar los objetos de datos o paquetes entre el momento en que se transmiten desde el servidor y se reciben por el cliente (o viceversa). En una realización de este tipo, las indicaciones de tiempo de un objeto de datos o paquete pueden no estar disponibles o pueden haber cambiado. En una realización de este tipo, puede emplearse un posible identificador no encriptado alternativo. En la realización ilustrada, puede emplearse información desde un registro de SSL para identificar diversas transferencias de datos. Se entiende que lo anterior es meramente un ejemplo ilustrativo al que no se limita la materia objeto.

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 petición (por ejemplo, Conseguir A 412 para transferencia de datos A, *etc.)* y un mensaje de respuesta (por ejemplo, Objeto A 416 para transferencia de datos A, *etc.).* En diversas realizaciones, estas transferencias de datos pueden producirse sustancialmente simultáneamente o de una forma canalizada, de tal forma que la transferencia de datos B comienza antes de que se complete la transferencia de datos A. Se entiende que lo anterior es meramente un ejemplo ilustrativo al que no se limita la materia objeto.

En una realización, los mensajes de petición 412, 413 y 414 pueden transmitirse a través de los paquetes 421, 422, 423, 424 y 425. Análogamente, los mensajes de respuesta 416, 417 y 418 pueden transmitirse a través de los paquetes 431, 432, 433, 434 y 435. En la realización ilustrada, el inicio y final de los paquetes se ilustra mediante líneas que conectan los paquetes a los registros de SSL. En la realización ilustrada, cada paquete 421, *etc.* se asocia con o incluye una indicación de tiempo 452, *etc.* En una realización de este tipo, de los paquetes (por ejemplo, paquetes 421, 422, y 423, *etc.)* requeridos para formar un registro de SSL (por ejemplo, registro de SSL 402, *etc.),* el primer tiempo de paquete (por ejemplo, momento 452, *etc.)* puede convertirse en el tiempo de inicio del registro de SSL 402 mientras que el último tiempo de paquete (por ejemplo, momento 453, *etc.)* puede convertirse en el tiempo de finalización del registro de SSL 402's.

Estos diversos objetos de datos o paquetes pueden encriptarse a través de las envolventes de encriptación 402, 404, 406 y/o 408. En la realización ilustrada, las envolventes de encriptación 402, 404, 406 y 408 se muestran como registros de SSL. Se entiende que lo anterior es meramente un ejemplo ilustrativo al que no se limita la materia objeto.

En diversas realizaciones, incluso el dispositivo de sondeo sin capacidad de desencriptación puede ser capaz de determinar el inicio y final de cada registro de SSL. Como tal, examinando el inicio o final de los registros de SSL, el dispositivo de sondeo sin capacidad de desencriptación puede ser capaz de estimar u obtener información de temporización con respecto a los mensajes de petición/respuesta.

A la inversa, en una realización, el dispositivo de sondeo sin capacidad de desencriptación puede no ser capaz de determinar cuándo se produce una petición (por ejemplo, Conseguir A 412, *etc.)* o respuesta (Objeto A 416, *etc.)*. Sin embargo, el dispositivo de sondeo con capacidad de desencriptación puede ser capaz de discernir esta información o al menos qué petición/respuesta se encapsuló o incluyó por qué envolvente de encriptación. Por ejemplo, dispositivo de sondeo con capacidad de desencriptación puede ser capaz de determinar que el mensaje de Conseguir A 412 se encapsula o incluye por el registro de SSL 402. En una realización de este tipo, el dispositivo de sondeo con capacidad de desencriptación puede ser capaz de determinar esto porque puede desencriptar el registro de SSL 402 y observar los contenidos dentro del mismo, mientras que el dispositivo de sondeo sin capacidad de desencriptación puede no ser capaz de hacer esto.

En diversas realizaciones, el dispositivo de sondeo con capacidad de desencriptación puede configurarse para recibir la información de temporización (por ejemplo, tiempo de inicio, tiempo de finalización, *etc.)* de los diversos registros de SSL 402, 404, 406 y 408 desde el dispositivo de sondeo sin capacidad de desencriptación. En una realización, el dispositivo de sondeo con capacidad de desencriptación puede configurarse para usar esa información de temporización además de lo que sabe el dispositivo de sondeo con capacidad de desencriptación o es capaz de determinar que son los contenidos de los registros de SSL 402, 404, 406 y 408 para estimar o determinar cuándo se produjeron los diversos mensajes de petición/respuesta.

En la realización ilustrada, el dispositivo de sondeo con capacidad de desencriptación puede reconocer que el registro de SSL 402 incluye el mensaje 412 de respuesta A y, a través de la información de temporización proporcionada por el dispositivo de sondeo sin capacidad de desencriptación, que el registro de SSL 402 se inicia en el momento 452. El dispositivo de sondeo sin capacidad de desencriptación puede reconocer que el paquete 422 no incluye ni un final o inicio de un registro de SSL, sino que el paquete 423 incluye el final de registro de SSL 402 en el momento 453 y, por lo tanto, no puede generarse ninguna información de temporización basándose en el paquete 422. Sin embargo, puede

generarse información de temporización basándose en el final de registro de SSL 402 en el momento 453. Por lo tanto, el dispositivo de sondeo con capacidad de desencriptación puede inferir o estimar que el mensaje 412 de respuesta A se produce durante el periodo de tiempo 462, entre los momentos 452 y 453.

En la realización ilustrada, el dispositivo de sondeo con capacidad de desencriptación puede reconocer que el registro de SSL 406 incluye el mensaje 416 de respuesta A y, a través de la información de temporización, que el registro de SSL 406 se inicia en el momento 456. El dispositivo de sondeo sin capacidad de desencriptación puede reconocer que paquete 432 no incluye ni un final o inicio de un registro de SSL (y, por lo tanto, no puede generarse ninguna información de temporización), sino que paquete 433 incluye el final de registro de SSL 406 en el momento 457. Por lo tanto, el dispositivo de sondeo con capacidad de desencriptación puede inferir o estimar que el mensaje 416 de respuesta A se produce durante el periodo de tiempo 466 (el tiempo entre los momentos 456 y 457), y el servidor o anfitrión tomó el periodo de tiempo 464 (entre los momentos 453 y 456) para procesar la petición A 412.

Análogamente, el dispositivo de sondeo con capacidad de desencriptación puede reconocer que el registro de SSL 402 incluye el comienzo del mensaje 413 de petición B y, a través de la información de tiempo suministrada por el dispositivo de sondeo sin capacidad de desencriptación, que el registro de SSL 402 se inicia en el momento 452. El dispositivo de sondeo sin capacidad de desencriptación puede reconocer que el registro de SSL 404 incluye la finalización de mensaje 413 de petición B y, a través de la información de temporización, que el registro de SSL 404 finaliza en el momento 454. El dispositivo de sondeo con capacidad de desencriptación puede reconocer que el registro de SSL 406 incluye el comienzo del mensaje 417 de respuesta B y, a través de la información de temporización, que el registro de SSL 406 se inicia en el momento 456. El dispositivo de sondeo con capacidad de desencriptación puede reconocer que el registro de SSL 408 incluye la finalización de mensaje 417 de respuesta B y, a través de la información de temporización, que el registro de SSL 408 finaliza en el momento 458. Por lo tanto, el dispositivo de sondeo con capacidad de desencriptación puede inferir o estimar que el mensaje 413 de petición B se produce durante el periodo de tiempo 472. El dispositivo de sondeo con capacidad de desencriptación puede inferir o estimar que el mensaje 417 de respuesta B se produce durante el periodo de tiempo 476. Por lo tanto, el servidor o anfitrión tomó el periodo de tiempo 474 (entre los momentos 454 y 456) para procesar la petición B 413.

Análogamente, el dispositivo de sondeo con capacidad de desencriptación puede reconocer que el registro de SSL 404 incluye el mensaje 414 de petición C y, a través de la información de temporización, que el registro de SSL 404 se inicia en el momento 453 y finaliza en el momento 454. El dispositivo de sondeo con capacidad de desencriptación puede reconocer que el registro de SSL 408 incluye el mensaje 418 de respuesta B y, a través de la información de temporización, que el registro de SSL 408 se inicia en el momento 457 y finaliza en el momento 458. Por lo tanto, el dispositivo de sondeo con capacidad de desencriptación puede inferir o estimar que el mensaje 414 de petición C se produce durante el periodo de tiempo 482. El dispositivo de sondeo con capacidad de desencriptación puede inferir o estimar que el mensaje 418 de respuesta se produce durante el periodo de tiempo 486. Por lo tanto, el servidor o anfitrión tomó el periodo de tiempo 484 (entre los momentos 454 y 457) para procesar la petición C 414.

En diversas realizaciones, el dispositivo de sondeo sin capacidad de desencriptación puede configurarse para transmitir información de temporización con respecto a los registros de SSL, en lugar de los paquetes al dispositivo de sondeo con capacidad de desencriptación. En una realización de este tipo, el dispositivo de sondeo con capacidad de desencriptación puede configurarse para asociar estas temporizaciones de registro de SSL con diversos mensajes de petición/respuesta.

En diversas realizaciones, los mensajes de información de temporización enviados al dispositivo de sondeo con capacidad de desencriptación pueden incluir un identificador de registro de SSL que indica qué registro de SSL se asocia con un mensaje de petición o respuesta particular. Se entiende que lo anterior es meramente un ejemplo ilustrativo al que no se limita la materia objeto.

En diversas realizaciones, la envolvente de comunicación encriptada (por ejemplo, registro de SSL, *etc.)* puede no incluir, dependiendo del protocolo de comunicaciones empleado, un identificador o esquema de numeración. En una realización de este tipo, los dispositivos de sondeo pueden asignar un identificador o número a cada una de la envolvente de comunicación encriptada (por ejemplo, registro de SSL, *etc.).* En una realización, esta numeración puede ser secuencial; aunque, se entiende que lo anterior es meramente un ejemplo ilustrativo al que la materia objeto no está limitada.

La Figura 5 es un diagrama de temporización de una realización de ejemplo de un sistema de acuerdo con la materia objeto divulgada. En otra realización, las sesiones de comunicación encriptada pueden tener una relación conocida (por ejemplo, 1 a 1, *etc.)* con la comunicación no encriptada. Por ejemplo, cada byte de datos no encriptados puede solicitar en un byte de datos encriptados. En una realización de este tipo, el dispositivo de sondeo sin capacidad de desencriptación puede configurarse para transmitir o determinar información de temporización basándose en los bytes de la comunicación encriptada.

En diversas realizaciones, el protocolo de encriptación o transmisión puede añadir bytes o datos de relleno adicionales a la sesión de comunicación encriptada que no existen en la comunicación de texto plano o no encriptada. Sin embargo, generalmente se conoce la cantidad o tamaño de los bytes adicionales y, por lo tanto, pueden tenerse en

cuenta. Por ejemplo, la carga útil de un registro de SSL puede desviarse 5 bytes de la carga útil de texto plano debido al encabezamiento de registro de SSL. Se entiende que lo anterior es meramente un ejemplo ilustrativo al que no se limita la materia objeto.

En una realización, el dispositivo de sondeo sin capacidad de desencriptación puede recibir una lista o serie de bytes (u otra medida, por ejemplo, kilobytes, *etc*.) para los que se desea la información de temporización. En una realización, esta lista de bytes puede recibirse desde el dispositivo de sondeo con capacidad de desencriptación. Basándose en esta lista, el dispositivo de sondeo sin capacidad de desencriptación puede supervisar la sesión de comunicaciones encriptadas y obtener información de temporización contando los bytes en la sesión de comunicaciones encriptadas y registrar el momento en el que se recibieron/enviaron los bytes de interés.

Por ejemplo, en una realización, la sesión de comunicaciones encriptadas 502 puede descomponerse y transmitirse como una serie de objetos de datos o paquetes 504. En la realización ilustrada, la serie de paquetes 504 puede incluir los paquetes 521, 522, 523, 524 y 525.

La sesión de comunicaciones encriptadas 502 también puede incluir una porción de encabezamiento no encriptada 512 (de la que el dispositivo de sondeo sin capacidad de desencriptación puede leer los contenidos) y una porción de carga útil encriptada 514 (de la que dispositivo de sondeo sin capacidad de desencriptación puede no leer los contenidos). En diversas realizaciones, la sesión de comunicaciones encriptadas 502 también puede incluir una porción de pie 516.

En una realización, el dispositivo de sondeo sin capacidad de desencriptación puede recibir el paquete 521 que comienza en el byte 530 de la sesión de comunicaciones encriptadas 502 y finaliza en el byte 532. En una realización de este tipo, el dispositivo de sondeo sin capacidad de desencriptación puede contar el tamaño o número de bytes del encabezamiento 512 y determinar que la compensación 531 de la sesión de comunicaciones encriptadas 502 de la lista o series de bytes para la que se desea la información de temporización.

En diversas realizaciones, a medida que cada paquete (por ejemplo, paquete 522, *etc.)* llega, el número de bytes del paquete 522 (byte 532 a byte 534) puede añadirse a un recuento de bytes dentro de la sesión de comunicaciones encriptadas 502. Este recuento de bytes puede compararse con la lista de bytes para la que se desea la información de temporización.

Si el paquete 522 incluye uno de los bytes para los que se desea la información de temporización, la información de temporización de paquete 522 puede registrarse. En una realización, el tiempo de llegada del paquete 522 puede registrarse y finalmente transmitirse al dispositivo de sondeo con capacidad de desencriptación como información de temporización, como se ha descrito anteriormente.

En una realización, la información de temporización puede incluir información de tiempo para cada uno de los bytes dentro de la lista de bytes para la que se desea la información de temporización. En otra realización, la información de temporización puede incluir información de tiempo no para los bytes específicos dentro de la lista, sino en su lugar la información de tiempo para los paquetes que incluyen los bytes para los que se desea la información de temporización. En otra realización más, la información de temporización puede incluir información de tiempo para los bytes de comienzo o finalización (por ejemplo, bytes 530, 532, 534, 536, 538 o 539) o un intervalo de bytes para los paquetes que incluyen los bytes para los que se desea la información de temporización.

En diversas realizaciones, datos de texto claro, texto plano o no encriptados pueden comprimirse antes de la encriptación y transmisión final como las comunicaciones encriptadas de red. En una realización de este tipo, la relación de bytes de 1 a 1 entre las comunicaciones de red encriptadas y desencriptadas, descrita anteriormente, puede no existir. Esto puede complicar el análisis de temporización, ya que una carga útil encriptada 514 puede no desencriptarse y descomprimirse por el dispositivo de sondeo sin capacidad de desencriptación. En una realización de este tipo, el dispositivo de sondeo con capacidad de desencriptación puede generar la lista de bytes para la que se desea la información de temporización basándose en los datos comprimidos y no en los datos no comprimidos. En una realización de este tipo, la lista de bytes para la que se desea la información de temporización puede basarse en los bytes dentro de la carga útil encriptada 514 y no en los datos de texto plano o no encriptados, como se ha descrito anteriormente. En algunas realizaciones, la lista de bytes puede ser aproximada ya que el dispositivo de sondeo con capacidad de desencriptación puede no ser capaz de medir con precisión los bytes entre las etapas de compresión y encriptación o transmisión. Se entiende que lo anterior es meramente un ejemplo ilustrativo al que no se limita la materia objeto.

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 puede usarse o producirse por los sistemas tales como los de las Figuras 1, 2 o 3. Adicionalmente, pueden usarse porciones de la técnica 600 para producir objetos de datos tal como los de las Figuras 4 o 5. Aunque, se entiende que lo anterior son meramente unos pocos ejemplos ilustrativos a los que la materia objeto divulgada no está limitada. Se entiende que la materia objeto divulgada no está limitada a la ordenación de o número de acciones ilustradas por la técnica 600.

El bloque 602 ilustra que, en una realización, puede supervisarse una sesión de comunicaciones encriptadas entre un primer dispositivo informático y un segundo dispositivo informático, como se ha descrito anteriormente. En diversas realizaciones, cada sesión de comunicaciones encriptadas puede incluir transmitir una pluralidad de objetos de datos encriptados entre el primer y segundo dispositivos informáticos, como se ha descrito anteriormente. En diversas realizaciones, una o más de la acción o acciones ilustradas por este bloque pueden realizarse por los aparatos o sistemas de las Figuras 1, 2 o 3, los puntos de derivación de lado de cliente de las Figuras 1, 2 o 3, como se ha descrito anteriormente.

El bloque 604 ilustra que, en una realización, puede obtenerse información de temporización con respecto a una sesión de comunicaciones encriptadas, como se ha descrito anteriormente. En una realización, la obtención puede basarse en uno o más objetos de datos encriptados recibidos incluidos por la sesión de comunicaciones encriptadas, como se ha descrito anteriormente. En algunas realizaciones, la obtención puede incluir determinar un inicio de una envolvente de encriptación incluida por la sesión de comunicaciones de encriptación supervisada, y determinar un final de la envolvente de encriptación, como se ha descrito anteriormente.

En otra realización, la obtención puede incluir recibir una indicación, desde el segundo dispositivo de sondeo, de una ubicación dentro de una sesión de comunicación encriptada para la que tiene que obtenerse información de temporización, como se ha descrito anteriormente. En una realización de este tipo, la obtención puede incluir adicionalmente determinar cuándo se ha recibido la ubicación indicada dentro de una sesión de comunicación encriptada por el dispositivo informático de cliente 102, como se ha descrito anteriormente. En diversas realizaciones, la obtención también puede incluir almacenar una indicación de tiempo asociada con la ubicación indicada recibida dentro de una sesión de comunicación encriptada, como se ha descrito anteriormente.

En algunas realizaciones, la ubicación dentro de la sesión de comunicaciones encriptadas puede indicarse a través de una compensación de bytes del inicio de una porción de la sesión de comunicaciones encriptadas, como se ha descrito anteriormente. En una realización de este tipo, la determinación de cuándo se ha recibido la ubicación indicada dentro de una sesión de comunicación encriptada puede incluir, para cada objeto de datos encriptados recibido, determinar si el objeto de datos encriptados recibido se incluye con la sesión de comunicaciones encriptadas indicada, determinar el intervalo de bytes dentro de la sesión de comunicaciones encriptadas indicada asociada con el objeto de datos encriptados recibido, y comparar el intervalo de bytes asociado con el objeto de datos encriptados recibido con la compensación de bytes indicada, como se ha descrito anteriormente.

En algunas realizaciones, la sesión de comunicaciones encriptadas puede incluir objetos de datos que están tanto comprimidos como encriptados. En una realización de este tipo, la obtención puede incluir recibir una indicación, por el primer dispositivo de sondeo y desde el segundo dispositivo de sondeo, de una ubicación dentro de una sesión de comunicación encriptada para la que tiene que obtenerse información de temporización, en el que la ubicación se basa en los objetos de datos encriptados y comprimidos, como se ha descrito anteriormente.

En algunas realizaciones, la sesión de comunicación de encriptación incluye una o más envolventes de encriptación, como se ha descrito anteriormente. En una realización de este tipo, la obtención puede incluir basar la información de temporización en una indicación de tiempo asociada con las envolventes encriptadas, como se ha descrito anteriormente. En otra realización, la obtención puede incluir ignorar, para propósitos de la obtención de la información de temporización, uno o más objetos de datos encriptados recibidos incluidos por la sesión de comunicaciones encriptadas que se indican, por el primer dispositivo informático, como que pueden ignorarse, como se ha descrito anteriormente. En diversas realizaciones, una o más de la acción o las acciones ilustradas por este bloque pueden realizarse por los aparatos o sistemas de las Figuras 1, 2 o 3, los puntos de derivación de lado de cliente de las Figuras 1, 2 o 3, como se ha descrito anteriormente.

El bloque 606 ilustra que, en una realización, la información de temporización obtenida puede transmitirse a otro dispositivo, como se ha descrito anteriormente. En una realización, la información de temporización puede transmitirse a un dispositivo de sondeo de lado de servidor, como se ha descrito anteriormente. En diversas realizaciones, una o más de la acción o las acciones ilustradas por este bloque pueden realizarse por los aparatos o sistemas de las Figuras 1, 2 o 3, los puntos de derivación de lado de cliente de las Figuras 1, 2 o 3, como se ha descrito anteriormente.

El bloque 608 ilustra que, en una realización, al menos una porción de la sesión de comunicación encriptada puede desencriptarse por un segundo dispositivo de sondeo, como se ha descrito anteriormente. En diversas realizaciones, una o más de la acción o las acciones ilustradas por este bloque pueden realizarse por los aparatos o sistemas de las Figuras 1, 2 o 3, los puntos de derivación de lado de servidor de las Figuras 1, 2 o 3, como se ha descrito anteriormente.

El bloque 610 ilustra que, en una realización, puede crearse un conjunto de métricas relacionadas con la sesión de comunicaciones encriptadas. En diversas realizaciones, estas métricas pueden basarse en la porción desencriptada de la sesión de comunicación encriptada y la información de temporización obtenida, como se ha descrito anteriormente. En algunas realizaciones, la creación puede incluir correlacionar un inicio del mensaje de datos con información de temporización obtenida, proporcionada por el primer dispositivo de sondeo, que indica la temporización de un inicio de la envolvente de encriptación, y correlacionar un final del mensaje de datos con información de temporización obtenida, proporcionada por el primer dispositivo de sondeo, que indica la temporización de un final de

la envolvente de encriptación, como se ha descrito anteriormente. En diversas realizaciones, una o más de la acción o las acciones ilustradas por este bloque pueden realizarse por los aparatos o sistemas de las Figuras 1, 2 o 3, los puntos de derivación de lado de servidor de las Figuras 1, 2 o 3, como se ha descrito anteriormente.

Las implementaciones de las diversas técnicas descritas en el presente documento pueden implementarse en circuitería electrónica digital, o en hardware, firmware, software informático o en combinaciones de los mismos. Implementaciones pueden implementarse como un producto de programa informático, es decir, un programa informático incorporado tangiblemente en una portadora de información, por ejemplo, en un dispositivo de almacenamiento legible por máquina o en una señal propagada, para su ejecución por, o para controlar la operación de, un aparato de procesamiento de datos, por ejemplo, un procesador programable, un ordenador o múltiples ordenadores. Un programa informático, tal como el programa o programas informáticos descritos anteriormente, puede escribirse en cualquier forma de lenguaje de programación, incluyendo lenguajes compilados o interpretados, y puede desplegarse en cualquier forma, incluyendo como un programa autónomo o como un módulo, componente, subrutina u otra unidad adecuada para su uso en un entorno informático. Un programa informático puede desplegarse para ejecutarse en un ordenador o en múltiples ordenadores en un sitio o distribuirse a través de múltiples sitios e interconectarse por una red de comunicación.

Etapas de método pueden realizarse por uno o más procesadores programables que ejecutan un programa informático para realizar funciones operando en datos de entrada y generando salida. Etapas de método también puede realizarse por, y un aparato puede implementarse como, circuitería de lógica de fin especial, por ejemplo, un FPGA (campo de matriz de puertas programables) o un ASIC (circuito integrado específico de aplicación).

Los procesadores adecuados para la ejecución de un programa informático incluyen, a modo de ejemplo, microprocesadores de fin tanto general como especial, y uno o más procesadores cualesquiera de cualquier tipo de ordenador digital. En general, un procesador recibirá instrucciones y datos de una memoria de solo lectura o una memoria de acceso aleatorio o ambas. Los elementos de un ordenador pueden incluir al menos un procesador para ejecutar instrucciones y uno o más dispositivos de memoria para almacenar instrucciones y datos. En general, un ordenador también puede incluir, o acoplarse operativamente para recibir datos desde o transferir datos a, o ambos, uno o más dispositivos de almacenamiento masivo para almacenar datos, por ejemplo, magnéticos, discos magneto-ópticos o discos ópticos. Portadoras de información adecuadas para incorporar instrucciones de programa informáticas y datos incluyen todas las formas de memoria no volátil, incluyendo a modo de ejemplo dispositivos de memoria de semiconductores, por ejemplo, EPROM, EEPROM, y dispositivos de memoria flash; discos magnéticos, por ejemplo, discos duros internos o discos extraíbles; discos magneto-ópticos; y discos de CD ROM y DVD-ROM. El procesador y la memoria pueden complementarse mediante, o incorporarse en circuitería de lógica de fin especial.

Para proporcionar interacción con un usuario, implementaciones pueden implementarse en un ordenador que tiene un dispositivo de visualización, por ejemplo, un monitor de tubo de rayos catódicos (CRT) o de pantalla de cristal líquido (LCD), para visualizar información al usuario y un teclado y un dispositivo apuntador, por ejemplo, un ratón o una bola de mando, mediante el cual el usuario puede proporcionar una entrada al ordenador. También pueden usarse otros tipos de dispositivos para proporcionar interacción con un usuario; por ejemplo, realimentación proporcionada al usuario puede ser cualquier forma de realimentación sensorial, por ejemplo, realimentación visual, realimentación auditiva o realimentación táctil; y la entrada del usuario puede recibirse en cualquier forma, incluyendo acústica, voz o entrada táctil.

Implementaciones pueden implementarse en un sistema informático que incluye un componente de extremo final, por ejemplo, como un servidor de datos, o que incluye un componente de soporte intermedio, por ejemplo, un servidor de aplicación, o que incluye un componente de extremo frontal, por ejemplo, un ordenador cliente que tiene una interfaz gráfica de usuario o un explorador web a través del cual un usuario puede interactuar con una implementación, o cualquier combinación de tales componentes de extremo final, soporte intermedio o extremo frontal. Componentes pueden interconectarse mediante cualquier forma o medio de comunicación de datos digital, *por ejemplo*, una red de comunicación. Ejemplos de las redes de comunicación incluyen una red de área local (LAN) y una red de área extensa (WAN), por ejemplo, la internet.

Aunque se han ilustrado ciertas características de las implementaciones descritas como se describen en el presente documento, muchas modificaciones, sustituciones, cambios y equivalentes se les ocurrirá a los expertos en la materia. Por lo tanto, deberá apreciarse que las reivindicaciones adjuntas se conciben para cubrir todas tales modificaciones y cambios como pertenecientes al alcance de las realizaciones.

REIVINDICACIONES

1. Un sistema que tiene un dispositivo de servidor (106, 206) que proporciona una aplicación (180) como un servicio a través de una red a un dispositivo informático de cliente (102), comprendiendo el sistema:
un primer dispositivo de sondeo (108, 208) configurado para:

supervisar una sesión de comunicación de red en una red de lado de servidor (195);
generar primera información de temporización (123, 298) con respecto a la sesión de comunicación de red en la red de lado de servidor (195);
un segundo dispositivo de sondeo (108b, 268) configurado para:

supervisar una sesión de comunicación de red en una red de lado de cliente (196);
generar segunda información de temporización (123b, 297) con respecto a la sesión de comunicación de red en la red de lado de cliente (196);
enviar la información de temporización (123b, 297) al primer dispositivo de sondeo (108, 208),
en el que el primer dispositivo de sondeo (108, 208) se configura para generar métricas de rendimiento de extremo a extremo basándose en la primera y segunda información de temporización.

2. El sistema de acuerdo con la reivindicación 1, en el que las métricas de rendimiento de extremo a extremo incluyen latencia de lado de cliente y latencia de lado de servidor.

3. El sistema de acuerdo con cualquiera de las reivindicaciones 1-2, en el que las métricas de rendimiento de extremo a extremo incluyen tasas de error.

4. El sistema de acuerdo con cualquiera de las reivindicaciones 1-3, en el que las métricas de rendimiento de extremo a extremo incluyen tiempos de carga de página.

5. El sistema de acuerdo con cualquiera de las reivindicaciones 1-3, en el que se encripta al menos una porción de la sesión de comunicación de red en la red de lado de servidor (195), y en el que el primer dispositivo de sondeo (108, 208) se configura para desencriptar la al menos una porción de la sesión de comunicación de red en la red de lado de servidor (195); y en el que el segundo dispositivo de sondeo (108b) se configura para generar la información de temporización (123b) basándose en la sesión de comunicación de red encriptada supervisada a través de un punto de derivación (107b) en la red de lado de cliente (196).

6. El sistema de acuerdo con la reivindicación 5, en el que el segundo dispositivo de sondeo (108b) se configura para generar la información de temporización empleando un identificador no encriptado.

7. El sistema de acuerdo con la reivindicación 6, en el que el segundo dispositivo de sondeo (108b) se configura para generar la información de temporización empleando un identificador no encriptado determinando el inicio y el final de registros de SSL.

8. El sistema de acuerdo con cualquiera de las reivindicaciones 1-4, en el que se encripta al menos una porción de la sesión de comunicación de red en la red de lado de servidor (195), el primer dispositivo de sondeo (108, 208) se configura para:

desencriptar la al menos una porción de la sesión de comunicación de red en la red de lado de servidor (195); y
generar la primera información de temporización (123, 298) con respecto a la sesión de comunicación de red en la red de lado de servidor (195) basándose en la porción desencriptada.

9. El sistema de acuerdo con cualquiera de las reivindicaciones 1-4, en el que el segundo dispositivo de sondeo (108b, 268) se configura para:

recibir una indicación, desde el primer dispositivo de sondeo (108, 208), de una ubicación dentro de la sesión de comunicación de red en la red de lado de cliente (196) para la que tiene que obtenerse la información de temporización (123b, 297);
determinar cuándo se ha recibido la ubicación indicada por el dispositivo informático de cliente (102); y
almacenar una indicación de tiempo asociada con la ubicación indicada recibida.

10. Un método implementado por ordenador de generación de métricas de rendimiento de extremo a extremo dentro de un sistema que tiene un dispositivo de servidor (106, 206) que proporciona una aplicación (180) como un servicio a través de una red a un dispositivo informático de cliente (102), comprendiendo el método:

supervisar, por un primer dispositivo de sondeo (108, 208), una sesión de comunicación de red en una red de lado de servidor (195);
generar, por el primer dispositivo de sondeo (108, 208), primera información de temporización (123, 298) con respecto a la sesión de comunicación de red en la red de lado de servidor (195);

supervisar, por un segundo dispositivo de sondeo (108b, 268), una sesión de comunicación de red en una red de lado de cliente (196);
generar, por el segundo dispositivo de sondeo (108b, 268), segunda información de temporización (123b, 297) con respecto a la sesión de comunicación de red en la red de lado de cliente (196);
enviar, por el segundo dispositivo de sondeo (108b, 268), la información de temporización (123b, 297) al primer dispositivo de sondeo (108, 208); y
generar, por el primer dispositivo de sondeo (108, 208), métricas de rendimiento de extremo a extremo basándose en la primera y segunda información de temporización.

11. El método de acuerdo con la reivindicación 10, en el que las métricas de rendimiento de extremo a extremo incluyen latencia de lado de cliente y latencia de lado de servidor.

12. El método de acuerdo con cualquiera de las reivindicaciones 10-11, en el que las métricas de rendimiento de extremo a extremo incluyen tasas de error.

13. El método de acuerdo con cualquiera de las reivindicaciones 11-12, en el que las métricas de rendimiento de extremo a extremo incluyen tiempos de carga de página.

14. El método de acuerdo con cualquiera de las reivindicaciones 11-13, en el que las métricas de rendimiento de extremo a extremo incluyen una medición agregada de latencia y errores.

FIG. 1

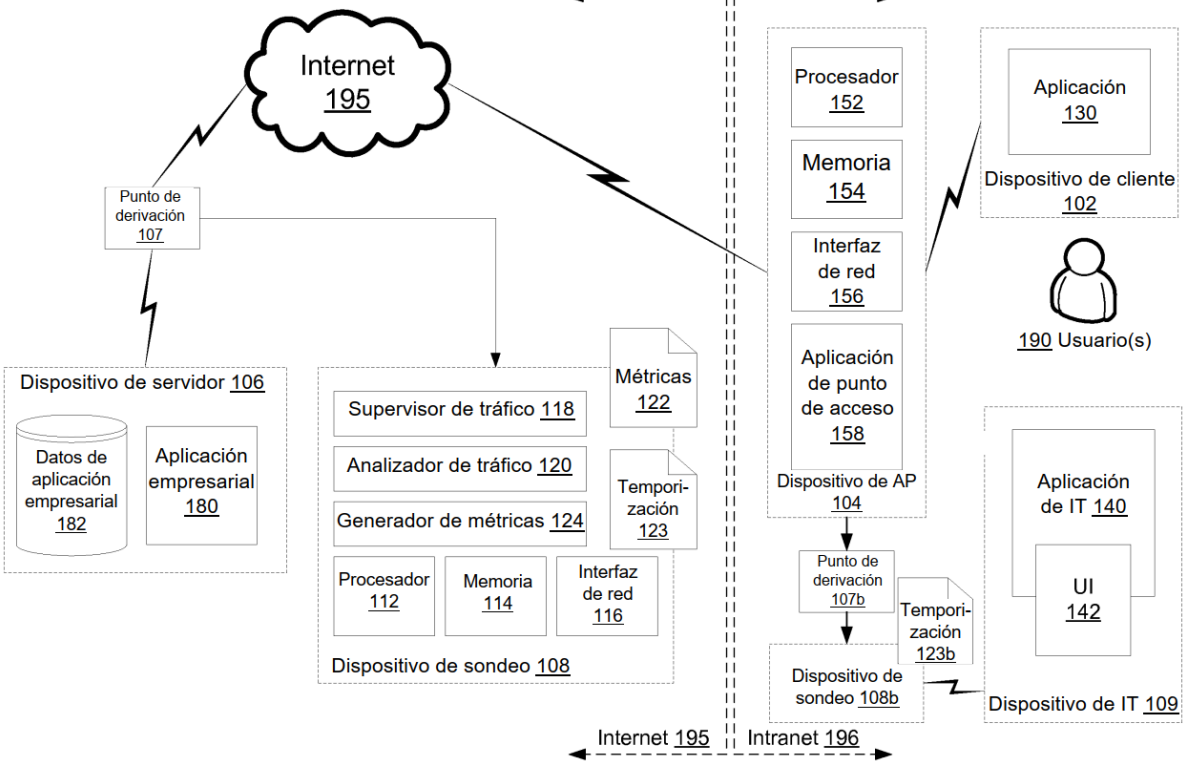

100
Internet 195
Punto de derivación 107
Dispositivo de servidor 106
Datos de aplicación empresarial 182
Aplicación empresarial 180
Métricas 122
Supervisor de tráfico 118
Analizador de tráfico 120
Generador de métricas 124
Tempori-zación 123
Procesador 112
Memoria 114
Interfaz de red 116
Dispositivo de sondeo 108
Procesador 152
Memoria 154
Interfaz de red 156
Aplicación de punto de acceso 158
Dispositivo de AP 104
Punto de derivación 107b
Tempori-zación 123b
Dispositivo de sondeo 108b
Aplicación 130
Dispositivo de cliente 102
190 Usuario(s)
Aplicación de IT 140
UI 142
Dispositivo de IT 109
Internet 195
Intranet 196

FIG. 2

200

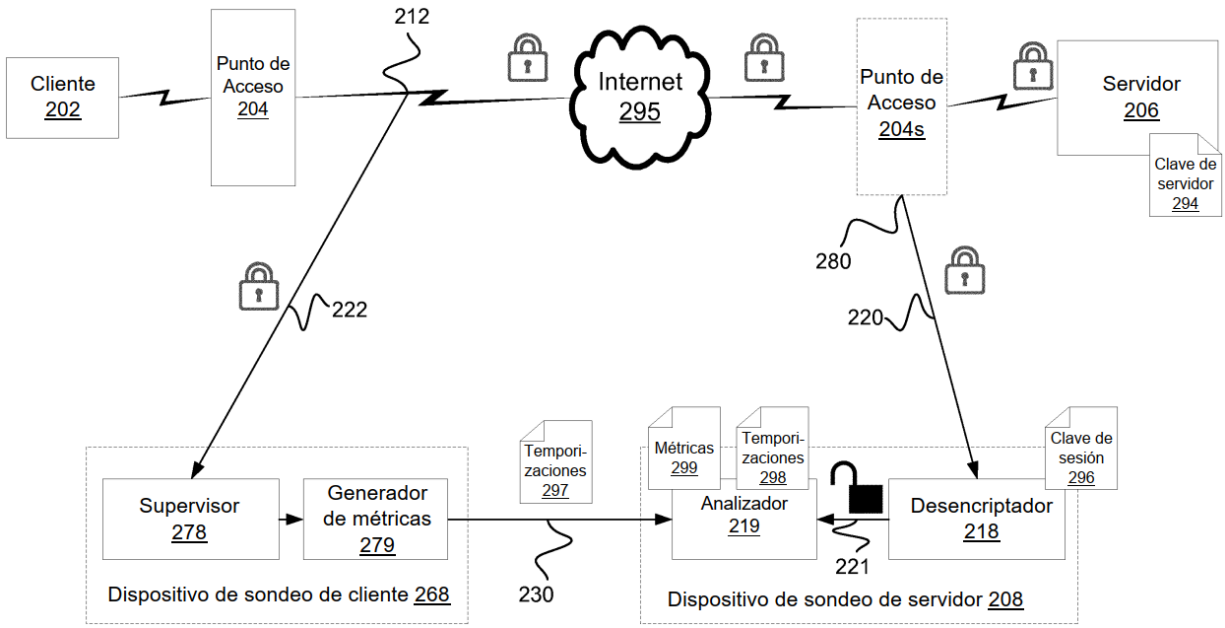

Cliente
202
Punto de Acceso
204
212
Internet
295
Punto de Acceso
204s
Servidor
206
Clave de servidor
294
280
220
222
Supervisor
278
Generador de métricas
279
Tempori-zaciones
297
Métricas
299
Tempori-zaciones
298
Analizador
219
Desencriptador
218
Clave de sesión
296
221
230
Dispositivo de sondeo de cliente 268
Dispositivo de sondeo de servidor 208

FIG. 3

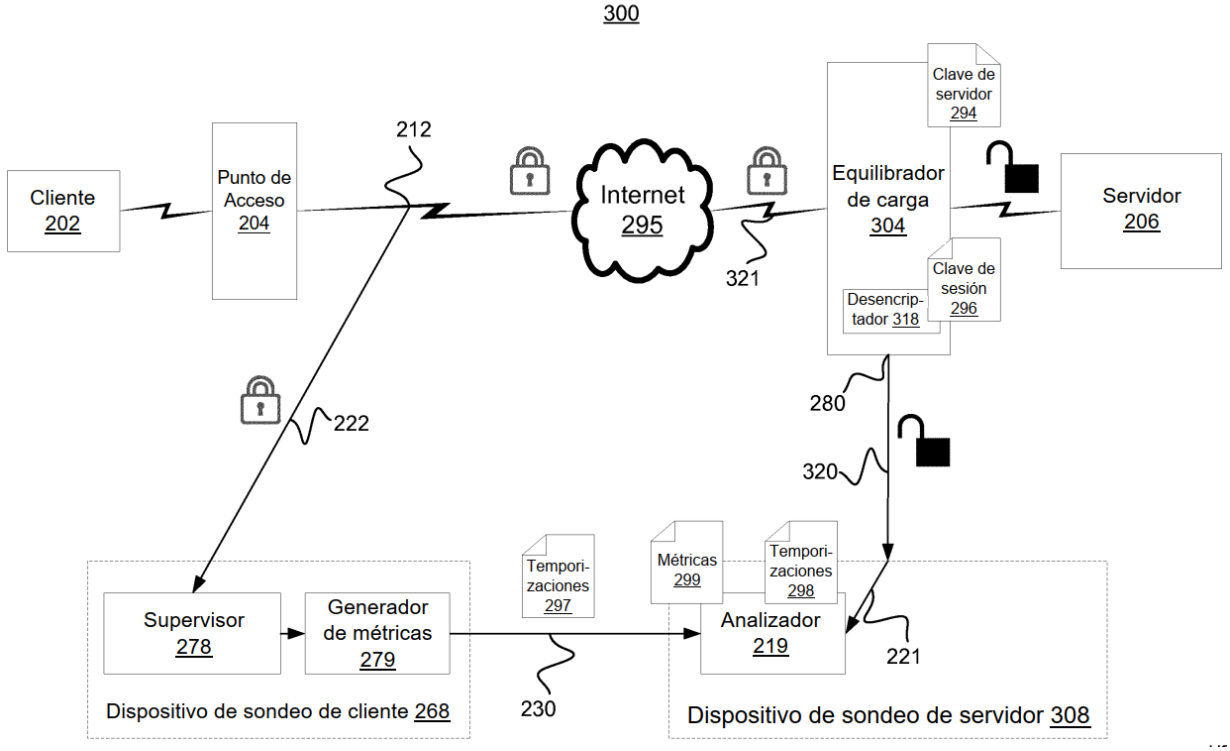

300
Cliente 202
Punto de Acceso 204
212
Internet 295
321
Equilibrador de carga 304
Clave de servidor 294
Servidor 206
Clave de sesión 296
Desencrip-tador 318
280
320
222
Supervisor 278
Generador de métricas 279
Tempori-zaciones 297
Métricas 299
Tempori-zaciones 298
Analizador 219
221
230
Dispositivo de sondeo de cliente 268
Dispositivo de sondeo de servidor 308

FIG. 4

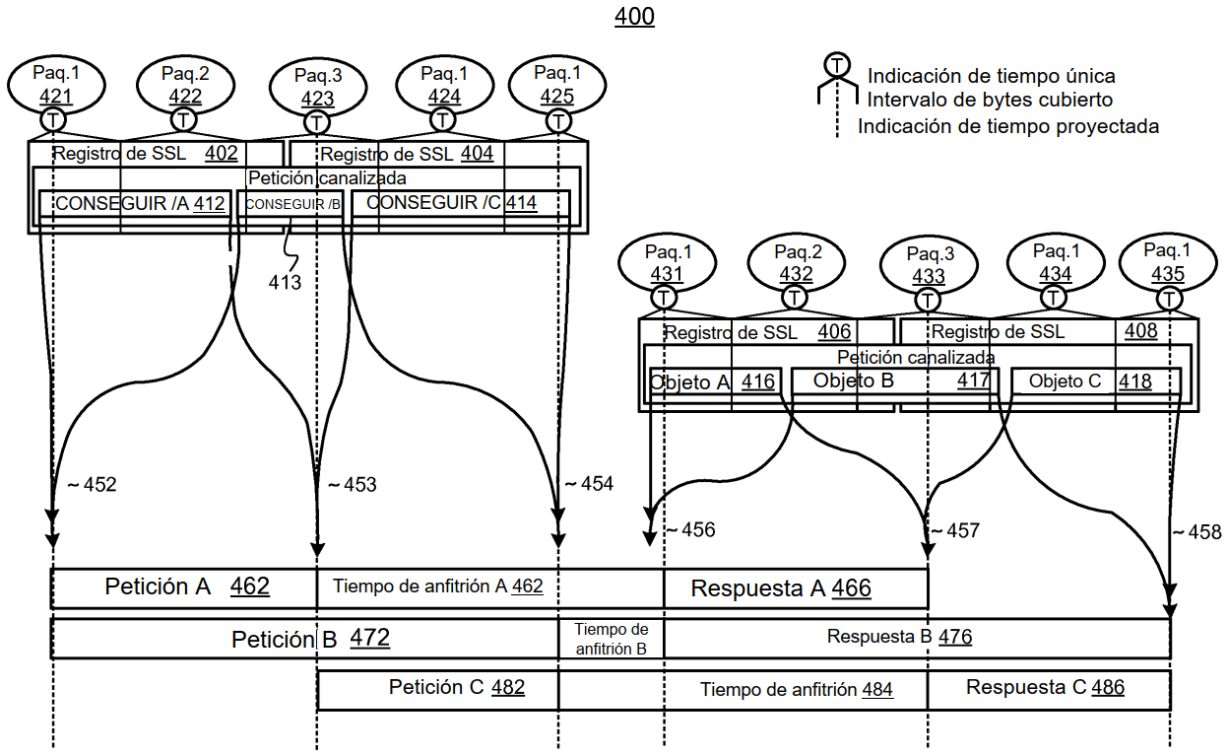
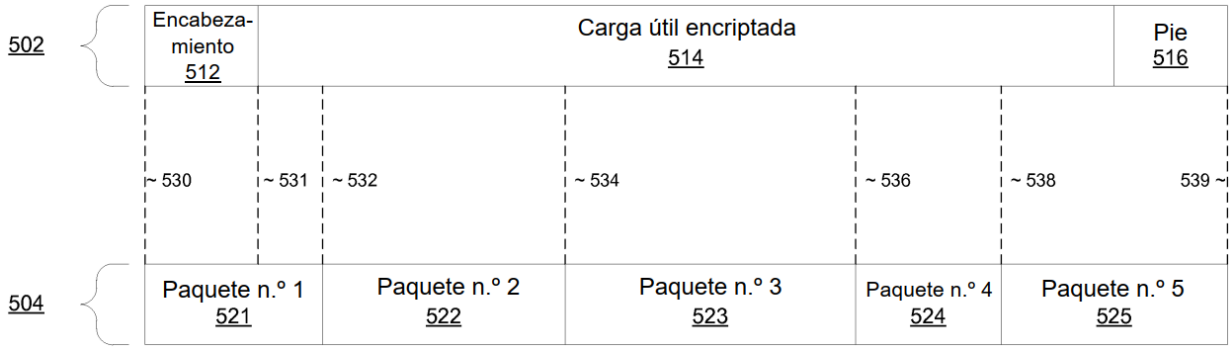

400
Indicación de tiempo única
Intervalo de bytes cubierto
Indicación de tiempo proyectada
Paq.1 421
Paq.2 422
Paq.3 423
Paq.1 424
Paq.1 425
Registro de SSL 402
Registro de SSL 404
Petición canalizada
CONSEGUIR /A 412
CONSEGUIR /B
CONSEGUIR /C 414
413
Paq.1 431
Paq.2 432
Paq.3 433
Paq.1 434
Paq.1 435
Registro de SSL 406
Registro de SSL 408
Petición canalizada
Objeto A 416
Objeto B 417
Objeto C 418
~452
~453
~454
~456
~457
~458
Petición A 462
Tiempo de anfitrión A 462
Respuesta A 466
Petición B 472
Tiempo de anfitrión B
Respuesta B 476
Petición C 482
Tiempo de anfitrión 484
Respuesta C 486

FIG. 5

500


502
Encabeza-miento 512
Carga útil encriptada 514
Pie 516
~ 530
~ 531
~ 532
~ 534
~ 536
~ 538
539 ~
504
Paquete n.º 1 521
Paquete n.º 2 522
Paquete n.º 3 523
Paquete n.º 4 524
Paquete n.º 5 525

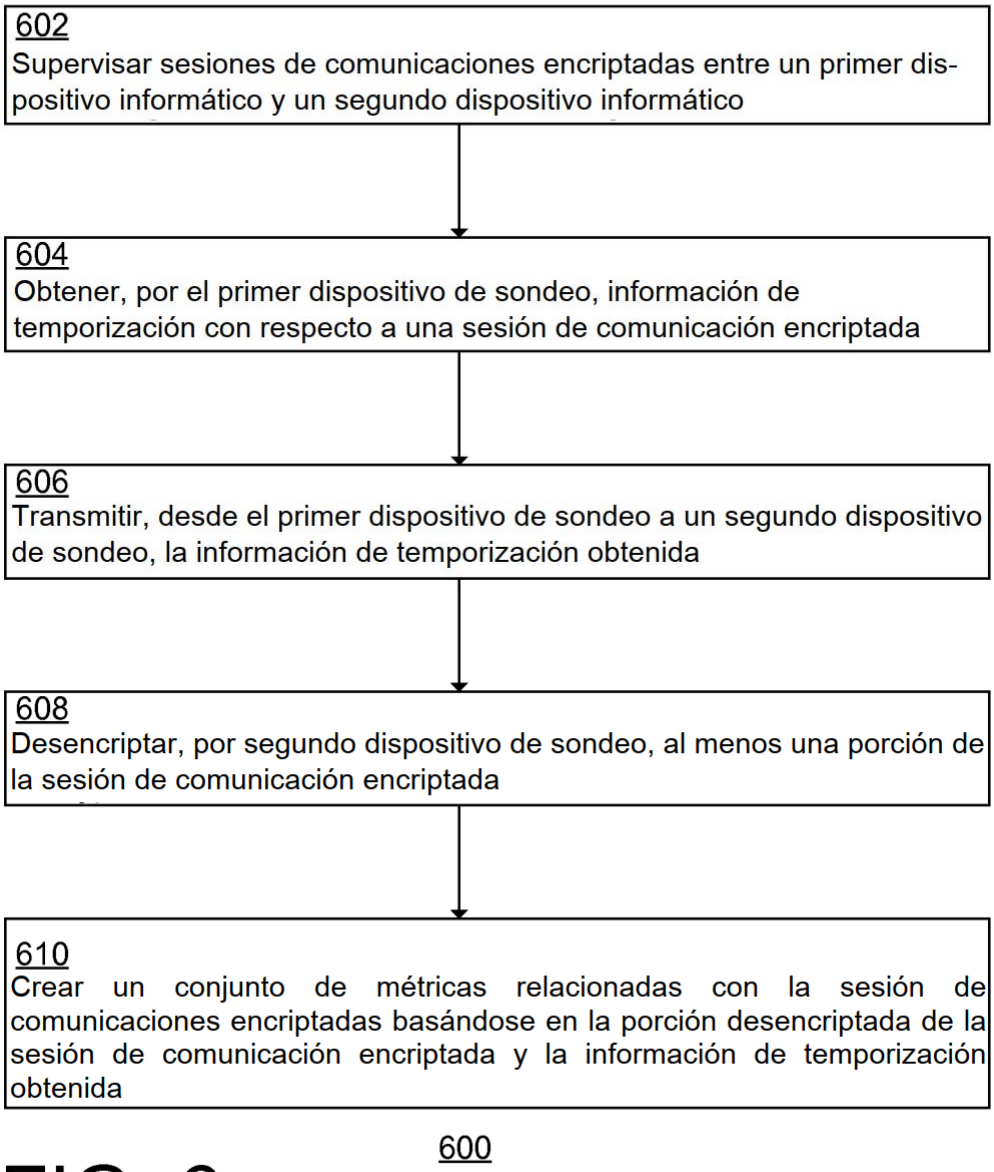

602
Supervisar sesiones de comunicaciones encriptadas entre un primer dispositivo informático y un segundo dispositivo informático
604
Obtener, por el primer dispositivo de sondeo, información de temporización con respecto a una sesión de comunicación encriptada
606
Transmitir, desde el primer dispositivo de sondeo a un segundo dispositivo de sondeo, la información de temporización obtenida
608
Desencriptar, por segundo dispositivo de sondeo, al menos una porción de la sesión de comunicación encriptada
610
Crear un conjunto de métricas relacionadas con la sesión de comunicaciones encriptadas basándose en la porción desencriptada de la sesión de comunicación encriptada y la información de temporización obtenida
600

FIG. 6