(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 815 568**

(51) Int. CI.:

H04L 12/28 (2006.01)
H04L 29/12 (2006.01)
H04L 12/46 (2006.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **06.02.2014 PCT/US2014/015035**

(87) Fecha y número de publicación internacional: **13.08.2015 WO15119606**

(96) Fecha de presentación y número de la solicitud europea: **06.02.2014 E 14881946 (9)**

(97) Fecha y número de publicación de la concesión europea: **01.07.2020 EP 3103221**

(54) Título: **Sistemas y métodos para proporcionar una arquitectura de enlace seguro múltiple**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
30.03.2021

(73) Titular/es:

E^NAT TECHNOLOGIES, LLC (100.0%)
1520 S. Arlington Street
Akron, OH 44306, US

(72) Inventor/es:

MCKINNEY, JACK, DENNIS

(74) Agente/Representante:

PONS ARIÑO, Ángel

DESCRIPCIÓN

Sistemas y métodos para proporcionar una arquitectura de enlace seguro múltiple

Antecedentes de la técnica

La Internet en la actualidad soporta comunicación mundial entre ordenadores usando diversos protocolos de normas. Uno de estos protocolos, el Protocolo de Internet (IP), asigna una dirección única a cada ordenador conocida como la dirección IP. IP está disponible en la actualidad en dos versiones: IPv4 con direcciones de 32 bits, e IPv6 con direcciones de 128 bits. IPv4 es la versión más común en uso hoy.

El crecimiento de la Internet ha usado todas las direcciones de 32 bits disponibles en IPv4. Un resultado del limitado número de direcciones es que la mayoría de organizaciones ahora usan uno de los tres espacios de direcciones privadas definidos por IPv4. Estas direcciones IP privadas no pueden usarse en la Internet pública. Encaminadores de pasarela gestionan la interfaz entre la Internet privada y la Internet pública. Encaminadores de pasarela proporcionan diversas funciones para ocultar o enmascarar su IP interna privada cuando se desea una comunicación fuera de la red privada.

Un método común usado por encaminadores de pasarela en entornos comerciales es la creación de una Red Privada Virtual (VPN) para conectar usuarios externos a la red privada interna. Una VPN proporciona una envolvente o protocolo de envoltura que oculta las direcciones IP internas y datos mientras el paquete se encamina a través de la Internet pública a la estación de trabajo de cliente.

La VPN extiende la red privada interna asignando una dirección IP privada interna a la estación de trabajo de cliente a medida que la estación de trabajo de cliente se conecta a la pasarela de VPN. La VPN crea una red o túnel de VPN que conecta las aplicaciones en la estación de trabajo de cliente a la red privada interna detrás de la pasarela de VPN (o pasarela de propietario). La red privada local de la estación de trabajo de cliente y la Internet pública están ocultas para las aplicaciones en la estación de trabajo de cliente por el túnel de VPN. Como resultado, en versiones actuales de VPN, la estación de trabajo de cliente puede únicamente conectarse a una VPN a la vez. Si una estación de trabajo de cliente fuera capaz de conectarse a más de una VPN entonces, ya que los dominios de dirección privada internos para cada VPN no se garantizarían que fueran únicos, no se podrían encaminar de forma fiable paquetes a los destinos deseados.

El documento US 2008/201486 A1 (Hsu, Nai-Ting et al), publicado el 21 de agosto de 2008, divulga encaminamiento de nivel de paquetes de Red Privada Virtual (VPN) usando una arquitectura de NAT dual para proporcionar una conexión segura bidireccional entre aplicaciones, anfitriones o redes en dos sitios extremo cualquiera sin exponer las direcciones IP y topologías de red reales de cada uno. El método incluye proporcionar a un cliente una lista de recursos disponibles en una red remota; iniciar una petición por el cliente para al menos un recurso de la lista de recursos remotos disponibles como si el al menos un recurso es local al cliente; traducción de dirección de red de las direcciones IP de origen y destino a un par de direcciones de VPN Dinámica (DVPN) de recurso y cliente; encaminar la petición a la red remota; traducción de dirección de red de las direcciones de DVPN de recurso y cliente a direcciones IP locales en la red remota; emitir la petición al al menos un recurso; traducción de dirección de red/encaminamiento de la respuesta usando el proceso inverso.

El documento EP 2020799 A1 (Canon KK), publicado el 2 de febrero de 2009, divulga la transmisión de paquetes de datos en un túnel que interconecta dos subredes para formar una red de comunicaciones general, implementándose dicho túnel entre dos puntos de extremo de túnel, comprendiendo cada una de dichas subredes un punto de extremo de túnel distinto entre dichos puntos de túneles, implementando dicho túnel al menos dos canales de transmisión, implementándose dicho método por uno de dichos puntos de extremo de túnel, conocido como un punto de extremo entrada de túnel. El método comprende las siguientes etapas para cada paquete de datos: recepción de dicho paquete de datos procedentes de un dispositivo de origen que pertenece a la misma subred que el punto de extremo entrada de túnel; selección de un canal efectivo de entre los canales de transmisión, como una función de un protocolo asociado con los datos de carga útil contenidos en dicho paquete recibido, y de una pieza de información en calidad de transporte vinculado a condiciones actuales de transmisión en dichos canales de transmisión; encapsulación de dicho paquete recibido, de acuerdo con un protocolo de transporte asociado con el canal efectivo, usado para obtener un paquete a enviar; y transmisión (6) del paquete a enviar en el túnel en el canal efectivo seleccionado.

El documento US 7814541 B1 (Manvi, Rajendra), publicado el 12 de octubre de 2010, divulga el encaminamiento virtual de una dirección IP solapante usando un dispositivo de red privada virtual (VPN) conectado a una red privada virtual (VLAN). El método comprende la etapa de recibir una dirección de protocolo de internet (IP) solapante desde un sitio virtual, teniendo la dirección IP solapante una etiqueta de dirección de sitio virtual (Vsite) asociada con un cliente. La dirección IP solapante se convierte en una dirección IP no solapante. La dirección IP no solapante se convierte a continuación en una dirección IP solapante que tiene una etiqueta de red de área local virtual (Vlan), en el que la etiqueta de red de área local virtual (Vlan) se asocia con al menos una red de área local (LAN) dentro de la red privada virtual.

Sumario de la invención

Realizaciones divulgadas en este documento incluyen un sistema para proporcionar una arquitectura de enlace seguro múltiple (MSL). Algunas realizaciones del sistema incluyen un componente de red privada virtual (VPN) de MSL que incluye una primera lógica que, cuando se ejecuta por un procesador, provoca que el sistema cree un túnel de VPN entre una estación de trabajo de cliente y una pasarela de propietario, envíe un datagrama saliente desde la estación de trabajo de cliente a la pasarela de propietario, y reciba un datagrama entrante desde la pasarela de propietario a la estación de trabajo de cliente, en la que el datagrama entrante incluye una dirección IP de origen y una dirección de protocolo de internet (IP) de destino que se establece a una dirección IP privada de propietario de VPN. En algunas realizaciones, la primera lógica provoca que el sistema envíe el datagrama entrante con la dirección IP de destino. Realizaciones del sistema también puede incluir un traductor de dirección de red (NAT) doble de MSL que incluye una segunda lógica que, cuando se ejecuta por el procesador, provoca que el sistema reciba el datagrama entrante desde la VPN de MSL, registre una nueva dirección IP privada de propietario de VPN desde la dirección IP de origen en el datagrama entrante, asigne una nueva dirección de UPIP para el datagrama entrante y la estación de trabajo de cliente, y facilite enviar el datagrama entrante a la estación de trabajo de cliente.

De manera similar, algunas realizaciones divulgadas en este documento incluyen un componente de red privada virtual (VPN) de MSL que incluye lógica que, cuando se ejecuta por un procesador, provoca que la VPN de MSL cree un túnel de VPN entre una estación de trabajo de cliente y una pasarela de propietario y envíe un datagrama saliente desde la estación de trabajo de cliente a la pasarela de propietario. En algunas realizaciones, la lógica provoca que el componente de VPN de MSL reciba un datagrama entrante desde la pasarela de propietario a la estación de trabajo de cliente, en la que el datagrama entrante incluye una dirección IP de origen y una dirección de protocolo de internet (IP) de destino que se establece a una dirección IP privada de propietario de VPN y se envían el datagrama entrante con la dirección IP de destino.

Aún algunas realizaciones divulgadas en este documento incluyen un traductor de dirección de red (NAT) doble de MSL que incluye lógica que, cuando se ejecuta por un procesador, provoca que el NAT doble de MSL reciba datagrama entrante desde VPN de MSL y registre una nueva dirección IP privada de propietario de VPN desde una dirección IP de origen en el datagrama entrante. En algunas realizaciones la lógica provoca que el NAT doble de MSL asigne una nueva dirección de UPIP para el datagrama entrante y estación de trabajo de cliente y facilite enviar el datagrama entrante a la estación de trabajo de cliente.

Otras realizaciones y/o ventajas de esta divulgación serán o pueden ser evidentes para un experto en la materia tras el examen de los siguientes dibujos y descripción detallada. Se concibe que todos tales sistemas, métodos, características y ventajas adicionales se incluyen dentro de esta descripción y pertenecen al alcance de la presente divulgación.

Breve descripción de los dibujos

Muchos aspectos de la divulgación pueden entenderse mejor con referencia a los siguientes dibujos. Los componentes en los dibujos no están necesariamente a escala, situándose en su lugar énfasis en ilustrar claramente los principios de la presente divulgación. Además, en los dibujos, números de referencia similares designan correspondientes partes a través de las varias vistas.

La Figura 1 representa un entorno informático para proporcionar una arquitectura de enlace seguro múltiple en una estación de trabajo de cliente, de acuerdo con realizaciones divulgadas en este documento;
La Figura 2 representa un entorno informático para proporcionar una arquitectura de enlace seguro múltiple en un servidor de MSL, de acuerdo con realizaciones divulgadas en este documento;
La Figura 3 representa un entorno informático para proporcionar una arquitectura de enlace seguro múltiple en un encaminador de pasarela de MSL, de acuerdo con realizaciones divulgadas en este documento;
La Figura 4 representa un entorno informático para proporcionar una arquitectura de enlace seguro múltiple en una estación de trabajo de cliente, de acuerdo con realizaciones divulgadas en este documento;
La Figura 5 representa un entorno informático para proporcionar una arquitectura de enlace seguro múltiple en un centro de operaciones de red (NOC) de MSL, de acuerdo con realizaciones divulgadas en este documento;
La Figura 6 representa un diagrama de flujo para que un gestor de inicio de sesión proporcione una arquitectura de enlace seguro múltiple, de acuerdo con realizaciones divulgadas en este documento;
La Figura 7 representa un diagrama de flujo para que un gestor de sesión proporcione una arquitectura de enlace seguro múltiple, de acuerdo con realizaciones divulgadas en este documento;
Las Figuras 8A, 8B representan un diagrama de flujo para una pluralidad de componentes para proporcionar una arquitectura de enlace seguro múltiple, de acuerdo con realizaciones divulgadas en este documento; y
La Figura 9 representa un dispositivo informático que puede utilizarse para proporcionar una arquitectura de enlace seguro múltiple, de acuerdo con realizaciones divulgadas en este documento.

Descripción de las realizaciones

Realizaciones divulgadas en este documento incluyen un sistema y/o método para proporcionar una arquitectura de

enlace seguro múltiple. Específicamente, cada propietario de VPN define un dominio de red con direccionamiento de IPv4 privada definido por propietario de VPN. Se espera que dominios de red de propietario de VPN tengan direcciones que se solapan ya que todos los propietarios de VPN podrían usar 10.0.0.0/24 como su definición de red. Las realizaciones divulgadas en este documento definen dominio de red interna para usar mientras los paquetes están dentro del servicio de MSL. MSL proporciona funciones de NAT doble para traducir todas las direcciones de IP privadas definidas por propietario de VPN a y desde direcciones de dominio de IP privada única (UPIP) de MSL a medida que los paquetes entran o salen del servicio de MSL. A los servidores de propietario de VPN se asigna dinámicamente una dirección de dominio de UPIP de MSL a medida que se descubren en paquetes procesados.

Cuando la estación de trabajo de cliente abre la primera conexión de VPN, o bien la IP privada de propietario de VPN asignada a la estación de trabajo de cliente o la dirección de UPIP para la estación de trabajo de cliente puede usarse como la dirección IP para la estación de trabajo de cliente. Cuando se abre una segunda VPN (o más tarde), la dirección IP anteriormente usada para la IP de la estación de trabajo puede usarse como la UPIP para la estación de trabajo y se asignan nuevas UPIP a servidores de la segunda VPN. Aplicaciones de estación de trabajo de cliente se comunican con UPIP de MSL. NAT de origen y destino de MSL convierte entre UPIP y IP privada de propietario de VPN de modo que los servidores ven únicamente direcciones de IP privada de propietario de VPN. Esto permite que la estación de trabajo de cliente facilite simultáneamente una pluralidad de conexiones VPN independientes con diferentes pasarelas de propietario y/o VPN.

En un entorno IPv6, las direcciones de red de propietario de VPN se generan como UPIP de 128 bits y se usan en IPv6 como se describe en el párrafo anterior para IPv4. Ya que direcciones de unidifusión IPv6 locales únicas tienen una alta probabilidad de ser únicas, MSL puede generar una UPIP de IPv6 para la estación de trabajo y usar las direcciones IPv6 privadas para los nodos detrás de la pasarela de propietario de VPN. MSL debe verificar que cada nueva VPN de IPv6 no ha duplicado las direcciones de unidifusión IPv6 locales únicas de una VPN ya abierta. Si se encuentra un duplicado, se generarán UPIP para los nodos en esa VPN, como se describe en el párrafo anterior para IPv4. Las direcciones IPv6 locales se crean usando una ID global asignada pseudoaleatoriamente. Una realización puede tener el siguiente formato de la Tabla 1.

Tabla 1

7 bits	1	40 bits	16 bits	64 bits
Prefijo	L	ID global	ID de subred	ID de interfaz
1111110	1	pseudoaleatorio		

Haciendo referencia ahora a los dibujos, la Figura 1 representa un entorno informático para proporcionar una arquitectura de enlace seguro múltiple en una estación de trabajo de cliente 102, de acuerdo con realizaciones divulgadas en este documento. Como se ilustra, la arquitectura de MSL crea un dominio o espacio de dirección IP privada (dominio de IP privada única de MSL) que se aísla tanto de las direcciones IP de Internet pública y las direcciones IP privadas de propietarios de VPN.

Como se ilustra, la arquitectura de la Figura 1 incluye una estación de trabajo de cliente 102, una primera VPN (VPN A 104a) y una segunda VPN (VPN B 104b). La estación de trabajo de cliente 102 puede incluir una aplicación A de usuario 108a y una aplicación B de usuario 108b. Las aplicaciones de usuario 108a, 108b pueden utilizarse para comunicarse con la VPN A 104a y la VPN B 104b. También se incluyen en la estación de trabajo de cliente 102 un componente de NAT doble de MSL 110, un componente de interfaz de usuario de VPN de MSL 114 y un componente de gestión de MSL 116, que forman el dominio de UPIP de MSL 106. En la estación de trabajo de cliente 102 también se incluye un componente de VPN de MSL 112. Esta configuración puede permitir comunicaciones de VPN con la VPN A 104a y/o la VPN B 104b a través de una red de área extensa o pública 118. La red pública 118 puede incluir la Internet y/u otra red públicamente accesible.

Por consiguiente, la estación de trabajo de cliente 102 puede incluir una pluralidad de componentes, que pueden o pueden no incluirse en un software de cliente autónomo de MSL. Como un ejemplo, los componentes del software de cliente autónomo de MSL pueden incluir el componente de gestión de MSL 116, que puede operar como un gestor de sesión para mantener información de sesión para la estación de trabajo de cliente 102. El gestor de sesión puede configurarse para asignar UPIP y proporcionar información de coordinación de UPIP al componente de NAT doble de MSL 110. De manera similar, los componentes también pueden incluir el componente de interfaz de usuario de MSL 114, que proporciona una o más interfaces de usuario de modo que el usuario puede identificar una conexión de VPN, borrar una conexión de VPN, abrir una conexión de VPN o cerrar una conexión de VPN abierta. El componente de VPN de MSL 112 puede utilizarse para proporcionar la IP de origen en los paquetes externos desde la pasarela de propietario 120a, 120b para identificar la pasarela de propietario 120a, 120b y/o la VPN 104a, 104b. Paquetes desde el componente de NAT doble de MSL 110 pueden incluir la IP pública de destino para identificar la pasarela/VPN de destino. También se incluye el componente de NAT doble de MSL 110 y traduce ambas direcciones IP de origen y de destino en los paquetes de texto claro a y/o desde direcciones de UPIP asignadas. Para un datagrama entrante (incluyendo datagramas de respuesta), el componente de NAT doble de MSL 110 usa la IP de origen proporcionada por el componente de VPN de MSL 112 para identificar la pasarela de propietario 120a, 120b. Para datagramas salientes, el componente de NAT doble de MSL 110 usa la UIP de origen y destino para identificar la IP pública de

destino para la pasarela de propietario 120a, 120b, y/o VPN 104a, 104b.

Por consiguiente, con los componentes en la estación de trabajo de cliente 102, puede hacerse una comunicación segura con uno o más dispositivos informáticos en la VPN A 104a y la VPN B 104b. La VPN A 104a puede incluir una pasarela de propietario 120a, que se acopla a uno o más dispositivos informáticos (tales como el dispositivo informático remoto 124a) a través de una red local 122a. De manera similar, la VPN B 104b también puede incluir una pasarela de propietario 120b, que facilita la comunicación con uno o más dispositivos informáticos remotos, tales como el dispositivo informático remoto 124b a través de una red local 122b.

La arquitectura de enlace seguro múltiple asigna una dirección IP privada única (UPIP) para cada anfitrión, tal como un dispositivo informático remoto 124a, 124b, servidor, etc. que comunica con una estación de trabajo de cliente 102 usando tecnología de MSL, de modo que todos los anfitriones (sistemas) de la organización del usuario tienen direcciones IP únicas dentro del dominio de IP privada de MSL 106. La arquitectura de MSL proporciona una función de NAT doble para gestionar el dominio de IP privada de MSL 106. El NAT doble de MSL 110 traduce entre direcciones IP privadas asignadas por propietario de VPN y UPIP asignadas de modo que la estación de trabajo tiene direcciones IP únicas para todos los anfitriones de propietario de VPN incluso cuando múltiples propietarios de VPN tienen las mismas direcciones IP privadas.

Por consiguiente, la aplicación A de usuario 108a y la aplicación B de usuario 108b ven UPIP mientras los anfitriones de propietario de VPN ven únicamente las direcciones IP privadas internas del propietario de VPN. El NAT doble de MSL 110 se coordina para traducir entre direcciones IP privadas asignadas por propietario de VPN y UPIP asignadas por arquitectura de MSL de modo que la aplicación A de usuario 108a y la aplicación B de usuario 108b ven UPIP y los anfitriones del propietario de VPN ven únicamente las direcciones IP privadas internas del propietario de VPN.

La estación de trabajo de cliente 102 se conecta a la VPN A 104a usando la interfaz de usuario de MSL y las funciones de gestión. El componente de gestión de MSL 116 asigna UPIP a los nodos de VPN A 104a, incluyendo el dispositivo informático remoto 124a. La estación de trabajo de cliente 102 puede acceder ahora a la VPN A 104a de la manera habitual.

La estación de trabajo de cliente 102 puede conectarse adicionalmente a la VPN B 104b usando el componente de interfaz de usuario de MSL 114 y el componente de gestión de MSL 116. El componente de gestión de MSL 116 asigna UPIP a nodos en la VPN B 104b, tal como el dispositivo informático remoto 124b. Ya que la VPN A 104a ya ha asignado una UPIP a la estación de trabajo de cliente 102, el componente de gestión de MSL 116 usa el mismo valor de UPIP para la IP de VPN B 104b. La estación de trabajo de cliente 102 puede acceder ahora a dispositivos informáticos tales como el dispositivo informático remoto 124b en la VPN B 104b con las aplicaciones de usuario 108a, 108b de la manera habitual.

La Tabla 2, a continuación, muestra un ejemplo de las asignaciones de dirección IP. Se ha de observar que la IP puede haberse seleccionado para simplificar el rastreo de asignaciones.

Tabla 2

	IP privada de propietario de VPN	UPIP de MSL
Servidor de VPN A	10.0.0.10	192.168.0.10
Estación de trabajo de VPN A	10.0.1.1	192.168.1.1
Servidor de VPN B	10.0.2.20	192.168.2.20
Estación de trabajo de VPN B	10.0.3.30	192.168.1.1

La UPIP generada se asigna a la estación de trabajo de cliente 102 cuando la estación de trabajo de cliente 102 inicia sesión en la VPN A 104a. Cuando la estación de trabajo de cliente 102 inicia sesión en la VPN B 104b, se asignan UPIP a los dispositivos informáticos detrás de la VPN B 104b, pero la estación de trabajo de cliente 102 continúa usando la estación de trabajo UPIP generada para la VPN A 104a. Debería entenderse que las aplicaciones de usuario 108a, 108b operan ahora en el dominio de UPIP de MSL 106.

La Figura 2 representa un entorno informático para proporcionar una arquitectura de enlace seguro múltiple en un servidor de MSL 204, de acuerdo con realizaciones divulgadas en este documento. Como se ilustra, la realización de la Figura 2 incluye una estación de trabajo de cliente 202, un servidor de MSL 204, VPN A 206a y VPN B 206b. La estación de trabajo de cliente 202 puede incluir una aplicación A de usuario 210a, una aplicación B de usuario 210b, un cliente de procesamiento de texto claro de producto comercialmente disponible (COTS) 212, un primer componente de VPN de MSL 214, un componente de interfaz de usuario de VPN de MSL 216 y un primer componente de gestión de MSL 218. Estos componentes pueden comprender un dominio de UPIP de MSL 208 y puede configurarse para establecer comunicaciones VPN con la VPN A 206a y/o la VPN B 206b a través de una red pública 220, tal como la Internet.

Para facilitar esta comunicación, el servidor de MSL 204 puede incluir un componente de VPN de COTS 224, un componente de procesamiento de texto claro de COTS 226, un componente de NAT doble de MSL 228 y un segundo componente de gestión de MSL 230, que son también parte del dominio de UPIP de MSL 208. También puede incluirse un segundo componente de VPN de MSL 232. Por consiguiente, estos componentes también pueden ser remotos de la VPN A 206a y/o VPN B 206b y pueden enviar uno o más datagramas a una pasarela de propietario 234a, 234b, que se acopla a una red local 122a, 122b para enviar y/o recibir datos desde los dispositivos informáticos remotos 238a, 238b y/u otros dispositivos informáticos en la VPN A 206a, y/o VPN B 206b.

Por consiguiente, la realización de la Figura 2 puede operar de forma similar a lo descrito con respecto a la Figura 1, excepto que la realización de la Figura 2 utiliza un servidor de MSL 204 que está remoto de la estación de trabajo de cliente 202. Por consiguiente, esta configuración extiende el dominio de UPIP de MSL 208 al servidor de MSL 204, que puede albergar funciones de texto claro de COTS, tales como aceleración de modo que la función de texto claro de COTS puede aplicarse a cada VPN usada por una pluralidad de diferentes estaciones de trabajo de cliente. Adicionalmente, el componente de VPN de COTS 224 se proporciona conectando el servidor de MSL 204 y la estación de trabajo de cliente 202 para proteger datos a medida que se mueve entre la estación de trabajo de cliente 202 y el servidor de MSL 2044 a través de la red pública 220.

La Figura 3 representa un entorno informático para proporcionar una arquitectura de enlace seguro múltiple en un encaminador de pasarela de MSL 304, de acuerdo con realizaciones divulgadas en este documento. Como se ilustra, la realización de la Figura 3 incluye una estación de trabajo de cliente 302, un encaminador de pasarela de MSL 304, una VPN A 306a y una VPN B 306b. La estación de trabajo de cliente 302 incluye una aplicación A de usuario 310a, una aplicación B de usuario 310b, un primer componente de VPN de COTS 314, un componente de interfaz de usuario de VPN de MSL 316 y un componente de gestión de MSL 318, que comprenden una porción del dominio de UPIP de MSL 308.

Por consiguiente, la estación de trabajo de cliente 302 puede comunicarse con un encaminador de pasarela de MSL 304 a través de una red local y/o privada 320. El encaminador de pasarela de MSL 304 puede incluir un segundo componente de VPN de COTS 322, un componente de NAT doble de MSL 324 y un componente de gestión de servidor de MSL 326, que son también parte del dominio de UPIP de MSL 308. También se incluye una VPN de MSL 328 con el encaminador de pasarela de MSL 304 y puede facilitar comunicación con la VPN A 306a y/o VPN B 306b a través de una red pública 330.

Como se ha analizado anteriormente con respecto a otras VPN, la VPN A 306a incluye una pasarela de propietario 332a que se acopla a una red privada 334a. La red privada 334a puede acoplarse a uno o más dispositivos informáticos, tales como el dispositivo informático remoto 336a. De manera similar, la VPN B 306b incluye una pasarela de propietario 332a que se acopla a una red privada 334b. La red privada 334b puede acoplarse a uno o más dispositivos informáticos, tales como el dispositivo informático remoto 336b.

Por consiguiente, la realización de la Figura 3 extiende el dominio de UPIP de MSL 308 a un encaminador de pasarela de MSL 304 que soporta una pluralidad de estaciones de trabajo de cliente. Una configuración de este tipo puede ser económica donde pueda utilizarse un único componente para una pluralidad de estaciones de trabajo de cliente (tales como en una red escolar, una red empresarial, etc.). Adicionalmente, el componente de VPN de COTS 332 se acopla la estación de trabajo de cliente 302 para proteger datos a medida que se mueven entre la estación de trabajo y el encaminador de MSL a través de la red privada 320.

También debería entenderse que mientras las aplicaciones de usuario 310 pueden ser una pluralidad de aplicaciones separadas que operan de forma completamente independiente, esto es solo una realización. Específicamente, algunas realizaciones están configuradas de tal forma que una aplicación de navegador común puede servir tanto a la aplicación A 310a como a la aplicación B 310b visualizando diferentes pestañas o páginas.

La Figura 4 representa un entorno informático para proporcionar una arquitectura de enlace seguro múltiple en una estación de trabajo de cliente 402, de acuerdo con realizaciones divulgadas en este documento. Como se ilustra, la realización de la Figura 4 incluye una estación de trabajo de cliente 402, un aparato de MSL 404, un servidor de MSL 406, una VPN A 408a y una VPN B 408b. La estación de trabajo de cliente 402 puede incluir una aplicación A de usuario 412a, una aplicación B de usuario 412b, un primer componente de VPN de COTS 414, así como un componente de interfaz de usuario de VPN de MSL 418, que comprenden una porción de un dominio de UPIP de MSL 410. Adicionalmente, la estación de trabajo de cliente 402 puede acoplarse al aparato de MSL 404 a través de un túnel encriptado y/o en una forma encriptada en una red privada 416.

El aparato de MSL 404 puede incluir un segundo componente de VPN de COTS 422, un primer cliente de procesamiento de texto claro de COTS 424, un tercer componente de VPN de COTS 426 y un primer componente de gestión de servidor de MSL 430, que son también parte del dominio de UPIP de MSL 410. El aparato de MSL 404 puede acoplarse a una red pública 428 para comunicarse con una VPN 408a, 408b a través del servidor de MSL 406.

También se acopla a la red pública 428 el servidor de MSL 406. El servidor de MSL 406 incluye un cuarto componente de VPN de COTS 432, un proceso de texto claro de COTS 434 y un segundo componente de gestión de servidor de

MSL 438, que son también parte del dominio de UPIP de MSL 410. Un componente de VPN de MSL 439 también es parte del servidor de MSL 406 y se acopla a la red pública 428.

También se acoplan a la red pública 428 la VPN A 408a y la VPN B 408b. La VPN A 408a incluye una pasarela de propietario 440a, una red privada 442a y uno o más dispositivos informáticos, tales como un dispositivo informático remoto 444a. La VPN B 408b incluye una pasarela de propietario 440b, una red privada 442b y uno o más dispositivos informáticos, tales como un dispositivo informático remoto 444b.

Por consiguiente, la realización de la Figura 4 proporciona una implementación que extiende el dominio de UPIP de MSL 410 a un aparato de MSL 404 que soporta una pluralidad de diferentes estaciones de trabajo de cliente (similar a la Figura 3), pero también utiliza el servidor de MSL 406. Debería entenderse que en algunas realizaciones, el aparato de MSL 404 puede implementarse dentro de un encaminador de pasarela que soporta una pequeña oficina. Adicionalmente, el tercer componente de VPN de COTS 426 y el cuarto componente de VPN de COTS 432 se acoplan entre el servidor de MSL 406 y el aparato de MSL 404 para proteger datos a medida que se mueven entre el aparato de MSL 404 y el servidor de MSL 406 a través de la red pública 428. El primer componente de VPN de COTS 414 y el segundo componente de VPN de COTS 422 se proporcionan entre el aparato de MSL 404 y la estación de trabajo de cliente 402 para proteger datos a medida que se mueven entre la estación de trabajo de cliente 402 y el aparato de MSL 404 a través de la red privada 416.

La Figura 5 representa un entorno informático para proporcionar una arquitectura de enlace seguro múltiple en un centro de operaciones de red (NOC) de MSL 504, de acuerdo con realizaciones divulgadas en este documento. Como se ilustra, la realización de la Figura 5 incluye una estación de trabajo de cliente 502, un centro de operaciones de red (NOC) de MSL 504, una VPN A 506a y una VPN B 506b. Los componentes de COTS incluyen: VPN de COTS y procesamiento de texto claro de COTS.

La estación de trabajo de cliente 502 incluye una aplicación A de usuario 510a y una aplicación B de usuario 510b. También se incluyen en la estación de trabajo de cliente 502, como parte de lógica de cliente de MSL, un cliente de procesamiento de texto claro de COTS 512, un cliente de VPN de COTS 514, un componente de interfaz de usuario de VPN de MSL 516 y un componente de gestión de MSL 518. Estos componentes comprenden parte de un dominio de IP privada de MSL 508.

Acoplar la estación de trabajo de cliente 502 con el NOC de MSL 504 es una red pública 520. Por consiguiente, el NOC de MSL 504 incluye un componente de VPN de COTS 524, un componente de procesamiento de texto claro de COTS 526, un componente de NAT doble de MSL 528, un componente de gestor de inicio de sesión 529 y un componente de gestor de sesión 530, que son también parte del dominio de IP privada de MSL 508. Un componente de VPN de MSL 531 también es parte del NOC de MSL 504. El componente de procesamiento de texto claro de COTS 526 puede implementarse como un producto de aceleración de red y puede implementarse como una función no modificada que opera en paquetes de texto claro para proporcionar el servicio para el cliente de usuario.

Adicionalmente, algunas realizaciones incluyen un gestor de sesión de cliente en la estación de trabajo de cliente 502 que comunica con el componente de gestor de sesión 530 y mantiene información de sesión para la estación de trabajo de cliente 502. La VPN A 506a y la VPN B 506b incluyen pasarela de propietario 532a, 532b, una red privada 534a, 534b y un dispositivo informático remoto 536a, 536b. El componente de gestor de sesión 530 puede configurarse para mantener información de sesión para cada estación de trabajo de cliente que ha iniciado sesión en el servicio. El componente de gestor de sesión 530 puede proporcionar información de coordinación de UPIP al componente de NAT doble de MSL 528 y puede actualizar el gestor de sesión de cliente con UPIP asignada para cada pasarela de propietario 532a, 532b. El gestor de sesión también puede configurarse para mantener la relación entre UPIP e IP pública de la pasarela de propietario 532a, 532b y/o VPN 506a, 506b. El componente de gestor de inicio de sesión 529 puede configurarse para procesar peticiones de inicio de sesión desde un gestor de inicio de sesión de cliente (que puede ser parte del componente de gestión de MSL 518) para validar el acceso de cliente al servicio y para establecer el túnel de VPN.

Como se ha descrito anteriormente, el componente de VPN de MSL 531 puede utilizarse para proporcionar la IP de origen en los paquetes externos desde la pasarela de propietario 532a, 532b para identificar la pasarela y/o VPN de origen. Por el contrario, datagramas salientes desde el componente de NAT doble de MSL 528 incluyen la IP pública de destino para identificar la pasarela y/o VPN de destino. El componente de interfaz de usuario de VPN de MSL 516 gestiona el proceso de puesta en marcha para la estación de trabajo de cliente 502. El componente de interfaz de usuario de VPN de MSL 516 comunica con el gestor de inicio de sesión para validar la licencia de cliente y establecer la VPN al NOC de MSL 504. Además, el componente de interfaz de usuario de VPN de MSL 516 puede configurarse para usar el componente de gestor de sesión 530 para la puesta en marcha y apagado de cada una de las conexiones de VPN solicitadas por la estación de trabajo de cliente 502.

De manera similar, el componente de NAT doble de MSL 528 puede configurarse para traducir ambas direcciones IP de origen y de destino en los paquetes de texto claro a y/o desde direcciones de UPIP asignadas. Para paquetes entrantes, el componente de NAT doble de MSL 528 usa la IP de origen proporcionada por el componente de VPN de MSL 531 para identificar al propietario de VPN. Para paquetes salientes, el componente de NAT doble de MSL 528

utiliza la UIP de origen y destino para identificar la IP pública de destino para la pasarela y/o VPN de destino. Debería entenderse que en el enlace entre el componente de NAT doble de MSL 528 y el componente de VPN de MSL 531, los paquetes pueden envolverse en un protocolo IP definido por la arquitectura de MSL privada que incluye las IP de origen y destino públicas. También debería entenderse que realizaciones descritas en este documento pueden asignar una UPIP que se solapa con una dirección IP privada asignada a cliente. Esto no crea problemas de encaminamiento porque la dirección asignada es única dentro del dominio de IP privada de MSL 508 y se correlaciona con la IP pública de la pasarela de propietario 532a, 532b mediante el componente de gestor de sesión 530. Como se entenderá, realizaciones descritas en este documento pueden configurarse de tal forma que no se requerirán cambios en la red del propietario de VPN.

Debería entenderse que en algunas realizaciones descritas anteriormente se representa una única estación de trabajo. Mientras tales realizaciones pueden soportar una estación de trabajo, cada una de las realizaciones descritas anteriormente puede configurarse para acomodar una pluralidad de estaciones de trabajo, dependiendo de la configuración particular.

La Figura 6 representa un diagrama de flujo para que un gestor de inicio de sesión proporcione una arquitectura de enlace seguro múltiple, de acuerdo con realizaciones divulgadas en este documento. Como se ilustra en el bloque 652, el gestor de inicio de sesión puede validar un ID de licencia para acceder al sistema. En el bloque 654, un cliente puede identificarse para el servicio. En el bloque 656, puede utilizarse un gestor de sesión para crear una sesión para rastrear a un usuario. En el bloque 658, puede utilizarse un componente de VPN de COTS para crear un túnel de VPN para crear un túnel de VPN a la estación de trabajo de cliente y asignar la UPIP para el ID de licencia a la estación de trabajo de cliente. En el bloque 660, un gestor de sesión de cliente en la estación de trabajo de cliente puede actualizarse con UPIP a las correlaciones de IP privada de cliente asignadas a la licencia. En el bloque 662, puede utilizarse una VPN de MSL para crear el túnel de VPN a la pasarela de cliente. En el bloque 664, puede proporcionarse un mensaje a la estación de trabajo de cliente que indica que el sistema está listo y proporciona el servicio solicitado.

La Figura 7 representa un diagrama de flujo para un gestor de sesión para proporcionar una arquitectura de enlace seguro múltiple, de acuerdo con realizaciones divulgadas en este documento. Como se ilustra en el bloque 752, un gestor de sesión de cliente en la estación de trabajo de cliente puede actualizarse con la UPIP asignada a la licencia. En el bloque 754, puede utilizarse un componente de VPN de MSL para crear el túnel de VPN a la pasarela de cliente. En el bloque 756, puede realizarse una emulación del inicio de sesión del usuario en la pasarela de cliente. En el bloque 758, puede enviarse de vuelta una página de inicio de sesión de VPN de cliente a la interfaz de usuario para que el usuario introduzca credenciales de inicio de sesión. En el bloque 760, puede actualizarse un gestor de sesión de cliente con los resultados de inicio de sesión. En el bloque 762, puede actualizarse un componente de NAT doble de MSL con la UPIP para la pasarela de propietario.

Las Figuras 8A, 8B representan un diagrama de flujo para una pluralidad de componentes para proporcionar una arquitectura de enlace seguro múltiple, de acuerdo con realizaciones divulgadas en este documento. Como se ilustra en el bloque 850 de la Figura 8A, una aplicación de usuario puede crear un datagrama de petición basándose en una entrada de usuario. En el bloque 852, un cliente de procesamiento de COTS procesa el datagrama. En el bloque 854, un cliente de VPN de COTS y un VPN de COTS transfieren el datagrama a un NOC de MSL. En el bloque 856, un proceso de texto claro de COTS procesa el datagrama y genera un datagrama nuevo para el servidor de propietario de VPN. En el bloque 858, un NAT doble de MSL correlaciona direcciones de UPIP en el datagrama con direcciones IP privadas definidas por cliente. En el bloque 860, la VPN de MSL puede encriptar el datagrama nuevo y, a continuación, transferir el datagrama nuevo a la pasarela de propietario. En el bloque 862, la pasarela de propietario desencripta el datagrama nuevo y reenvía el datagrama nuevo al dispositivo informático remoto de propietario de VPN para procesamiento. En el bloque 864, el dispositivo informático remoto de propietario de VPN genera un datagrama de respuesta con una dirección IP de destino establecida a la IP privada de propietario de VPN para la estación de trabajo de cliente solicitante. En el bloque 866, la pasarela de propietario de VPN encripta el datagrama de respuesta y reenvía el datagrama de respuesta al componente de VPN de MSL. En el bloque 868, la VPN de MSL desencripta el datagrama de respuesta y reenvía el datagrama de respuesta con las direcciones de IP de origen originales al NAT doble de MSL.

Continuando en el bloque 870 de la Figura 8B, el NAT doble de MSL correlaciona direcciones de IP privadas definidas por propietario de VPN en el datagrama de respuesta con direcciones de UPIP. En el bloque 872, el NAT doble de MSL registra la nueva IP privada de propietario de VPN desde la IP de origen en el datagrama de respuesta desencriptado en el gestor de sesión y asigna una nueva UPIP. En el bloque 874, el NAT doble de MSL reenvía el datagrama de respuesta al componente de procesamiento de texto claro de COTS. En el bloque 876, el componente de procesamiento de texto claro de COTS procesa el datagrama de respuesta y genera un nuevo datagrama de respuesta para la aplicación de usuario. En el bloque 878, la VPN de COTS y el cliente de VPN de COTS transfieren el nuevo datagrama de respuesta a la estación de trabajo de cliente. En el bloque 880, el cliente de procesamiento de COTS procesa el nuevo datagrama de respuesta. En el bloque 882, la aplicación de usuario presenta resultados en el nuevo datagrama de respuesta al usuario.

La Figura 9 representa un dispositivo informático que puede utilizarse para proporcionar una arquitectura de enlace seguro múltiple, de acuerdo con realizaciones divulgadas en este documento. En la realización ilustrada, el servidor

de MSL 204 incluye uno o más procesador 930, hardware de entrada/salida 932, hardware de interfaz de red 934, un componente de almacenamiento de datos 936 (que almacena datos de inicio de sesión 938a y datos de sesión 938b), y el componente de memoria 940. El componente de memoria 940 puede configurarse como memoria volátil y/o no volátil y, como tal, puede incluir memoria de acceso aleatorio (incluyendo SRAM, DRAM y/u otros tipos de RAM), memoria flash, registros, discos compactos (CD), discos versátiles digitales (DVD) y/u otros tipos de medios legibles por ordenador no transitorios. Dependiendo de la realización particular, el medio legible por ordenador no transitorio puede residir dentro del servidor de MSL 204 y/o externo al servidor de MSL 204.

Adicionalmente, el componente de memoria 940 puede configurarse para almacenar lógica de operación 942, la lógica de VPN de MSL 944a, la lógica de NAT doble de MSL 944b y otra lógica, tal como se ha descrito anteriormente, cada una de las cuales puede incorporarse como un programa informático, firmware y/o hardware, como un ejemplo. En la Figura 9 también se incluye una interfaz de comunicación local 946 y puede implementarse como un bus u otra interfaz para facilitar la comunicación entre los componentes del servidor de MSL 204.

El procesador 930 puede incluir cualquier componente de procesamiento operable para recibir y ejecutar instrucciones (tales como desde el componente de almacenamiento de datos 936 y/o componente de memoria 940). El hardware de entrada/salida 932 puede incluir y/o configurarse para interactuar con un monitor, teclado, ratón, impresora, cámara, micrófono, altavoz y/u otro dispositivo para recibir, enviar y/o presentar datos. El hardware de interfaz de red 934 puede incluir y/o configurarse para comunicarse con cualquier hardware de red por cable o inalámbrico, un satélite, una antena, un módem, puerto LAN, tarjeta de fidelidad inalámbrica (Wi-Fi), tarjeta de WiMax, hardware de comunicación móvil, fibra y/u otro hardware para comunicarse con otras redes y/o dispositivos. A partir de esta conexión, puede facilitarse la comunicación entre el servidor de MSL 204 y otros dispositivos informáticos, como se ha descrito anteriormente.

De manera similar, debería entenderse que el componente de almacenamiento de datos 936 puede residir local a y/o remoto del servidor de MSL 204 y puede configurarse para almacenar una o más piezas de datos para acceso por el servidor de MSL 204 y/u otros componentes. En algunas realizaciones, el componente de almacenamiento de datos 936 puede ubicarse remotamente del servidor de MSL 204 y, por lo tanto, ser accesible a través de una conexión de red. En algunas realizaciones sin embargo, el componente de almacenamiento de datos 936 puede ser meramente un dispositivo periférico, pero externo al servidor de MSL 204.

En el componente de memoria 940 se incluyen la lógica de operación 942, la lógica de VPN de MSL 944a y la lógica de NAT doble de MSL 944b, y la otra lógica 944c. La lógica de operación 942 puede incluir un sistema operativo y/u otro software para gestionar componentes del servidor de MSL 204. De manera similar, la lógica de VPN de MSL 944a puede incluir lógica para realizar la funcionalidad de VPN de MSL descrita anteriormente. La lógica de NAT doble de MSL 944b puede incluir lógica para realizar la funcionalidad de NAT doble de MSL descrita anteriormente. La otra lógica 944c se incluye en este documento para representar la otra lógica y funcionalidad descritas anteriormente.

Debería entenderse que los componentes ilustrados en la Figura 9 son meramente ilustrativos y no pretenden limitar el alcance de esta divulgación. Mientras los componentes en la Figura 9 se ilustran como que residen dentro del servidor de MSL 204, esto es meramente un ejemplo. En algunas realizaciones, uno o más de los componentes pueden residir externos al servidor de MSL 204. También debería entenderse que mientras el servidor de MSL 204 se representa en la Figura 9, otros dispositivos informáticos descritos en las Figuras 1-6 u otros dibujos pueden incluir hardware y software similares para proporcionar la funcionalidad descrita. Como un ejemplo, las estaciones de trabajo de cliente 102, 202, 302, 402 y/o 502 pueden incluir parte o todo el hardware y componentes de software descritos anteriormente. Por consiguiente, en la medida de lo aplicable, los componentes descritos en las Figuras 1-6 pueden incorporarse como lógica y/o software que se ejecutan dentro de un dispositivo informático que incluye el hardware necesario, parte del cual se representa en la Figura 9.

Debería observarse que los diagramas de flujo incluidos en este documento muestran la arquitectura, funcionalidad y operación de una posible implementación de software. En este sentido, cada bloque puede interpretarse para representar un módulo, segmento o porción de código, que comprende una o más instrucciones ejecutables para implementar la función o funciones lógicas especificadas. Debería observarse también que en algunas implementaciones alternativas, las funciones indicadas en los bloques pueden producirse fuera del orden y/o no producirse. Por ejemplo, dos bloques mostrados en sucesión pueden ejecutarse de hecho de forma sustancialmente simultánea o los bloques pueden ejecutarse en ocasiones en el orden inverso, dependiendo de la funcionalidad implicada.

REIVINDICACIONES

1. Un sistema para proporcionar una arquitectura de enlace seguro múltiple, MSL, comprendiendo dicho sistema:
un componente de red privada virtual, VPN, de MSL (112) que incluye primera lógica que, cuando se ejecuta por un procesador de dicho sistema, provoca que el sistema realice lo siguiente:

crear un primer túnel de VPN entre una estación de trabajo de cliente (106) y una primera pasarela de propietario (120a); enviar un datagrama saliente desde la estación de trabajo de cliente (106) a la primera pasarela de propietario (120a);
recibir un datagrama entrante desde la primera pasarela de propietario (120a) a la estación de trabajo de cliente (106), en el que el datagrama entrante incluye una dirección de protocolo de internet, IP, de origen y una dirección IP de destino que se establece a una dirección IP privada de propietario de VPN; y
enviar el datagrama entrante con la dirección IP de destino; y un traductor de dirección de red, NAT, doble de MSL (110) que incluye segunda lógica que, cuando se ejecuta por el procesador, provoca que el sistema realice al menos lo siguiente:
recibir el datagrama entrante desde la VPN de MSL (112);
registrar una nueva dirección IP privada de propietario de VPN desde la dirección IP de origen en el datagrama entrante;
asignar una nueva dirección IP privada única, UPIP, para el datagrama entrante y la estación de trabajo de cliente (106); y enviar el datagrama entrante a la estación de trabajo de cliente (106),
en el que el sistema crea adicionalmente un segundo túnel de VPN entre la estación de trabajo de cliente (106) y una segunda pasarela de propietario (120b) mientras se está utilizando el primer túnel de VPN.

2. El sistema de la reivindicación 1, en el que la primera lógica provoca adicionalmente que el sistema realice lo siguiente:

encriptar el datagrama saliente y transferir el datagrama saliente a la primera pasarela de propietario (120a); y
recibir el datagrama entrante en una forma encriptada desde la primera pasarela de propietario (120a) y desencriptar el datagrama entrante.

3. El sistema de la reivindicación 1, en el que la segunda lógica provoca adicionalmente que el sistema correlacione una dirección de UPIP en el datagrama saliente con una dirección IP privada.

4. El sistema de la reivindicación 1, comprendiendo adicionalmente un componente de gestión de MSL (116) que incluye tercera lógica que, cuando se ejecuta por el procesador, provoca que el sistema cree el primer túnel de VPN.

5. El sistema de la reivindicación 1, comprendiendo adicionalmente un servidor de MSL (204), en el que la VPN de MSL (112) y el NAT doble de MSL (110) residen en el servidor de MSL (204) que está remoto desde la estación de trabajo de cliente (106), en el que el sistema comprende además incluye un componente de interfaz de usuario de VPN de MSL (114), un primer componente de VPN de MSL (112) y un primer componente de gestión de MSL (116) que residen en la estación de trabajo de cliente (106), y en el que el sistema comprende además un componente de procesamiento de texto claro de producto comercialmente disponible, COTS, (226), un componente de VPN de COTS (224) y un segundo componente de gestión de MSL (116) que residen en el servidor de MSL (204).

6. El sistema de la reivindicación 1, comprendiendo adicionalmente un encaminador de pasarela de MSL (304) que incluye la VPN de MSL (112) y el NAT doble de MSL (110), en el que el sistema comprende además un primer componente de VPN de COTS (326), un componente de gestión de MSL (116) que residen en la estación de trabajo de cliente (106), y en el que el sistema comprende además un segundo componente de VPN de COTS (326) y un componente de gestión de servidor de MSL (326) que residen en el encaminador de pasarela de MSL (304).

7. El sistema de la reivindicación 1, comprendiendo adicionalmente un aparato de MSL (404) y un servidor de MSL (204), en el que el componente de VPN de MSL (112) y el NAT doble de MSL (110) residen en el servidor de MSL (204), en el que el sistema comprende además un primer componente de VPN de COTS (326) y un componente de interfaz de usuario de VPN de MSL (114) que residen en la estación de trabajo de cliente (106), en el que el sistema comprende además un primer componente de gestión de servidor de MSL (326), un segundo componente de VPN de COTS (326), un tercer componente de VPN de COTS (326) y un cliente del componente de procesamiento de texto claro de COTS (226) que residen en el aparato de MSL (404), y en el que el sistema comprende además un segundo componente de gestión de servidor de MSL (326), un cuarto componente de VPN de COTS (326) y un segundo cliente de procesamiento de texto claro de COTS (226) que residen en el servidor de MSL (204).

8. El sistema de la reivindicación 1, comprendiendo adicionalmente un centro de operaciones de red, NOC, de MSL (504) en el que el NAT doble de MSL (110) y el componente de VPN de MSL (112) residen en el NOC (504), en el que el sistema comprende además un cliente de VPN de COTS (326), un componente de interfaz de usuario de VPN de MSL (114) y un componente de gestión de MSL (116) que residen en la estación de trabajo de cliente (106), y en el que el sistema comprende además un componente de VPN de COTS (326), un componente de procesamiento de texto claro de COTS (226), un componente de gestor de sesión (530) y un componente de gestor de inicio de sesión

(529) que residen en el NOC de MSL (504).

9. Un método para proporcionar una arquitectura de enlace seguro múltiple, MSL, comprendiendo dicho método las etapas de:

creación de un primer túnel de VPN entre una estación de trabajo de cliente (106) y una primera pasarela de propietario (120a);
envío de un datagrama saliente desde la estación de trabajo de cliente (106) a la primera pasarela de propietario (120a);
recepción de un datagrama entrante desde la primera pasarela de propietario (120a) a la estación de trabajo de cliente (106), en el que el datagrama entrante incluye una dirección de protocolo de internet, IP, de origen y una dirección IP de destino que se establece a una dirección IP privada de propietario de VPN;
registro de una nueva dirección IP privada de propietario de VPN desde la dirección IP de origen en el datagrama entrante; asignación de una nueva dirección IP privada única, UPIP, para el datagrama entrante y la estación de trabajo de cliente (106); y envío del datagrama entrante a la estación de trabajo de cliente (106), en el que el sistema crea adicionalmente un segundo túnel de VPN entre la estación de trabajo de cliente (106) y una segunda pasarela de propietario (120b) mientras se está utilizando el primer túnel de VPN.

10. El método de la reivindicación 9, comprendiendo adicionalmente las etapas de:

encriptación del datagrama saliente y transferencia del datagrama saliente a la primera pasarela de propietario (120a); y
recepción del datagrama entrante en una forma encriptada desde la primera pasarela de propietario (120a) y desencriptación el datagrama entrante.

11. El método de la reivindicación 9, comprendiendo adicionalmente la etapa de correlación de una dirección de UPIP en el datagrama saliente con una dirección IP privada.

12. El método de la reivindicación 9, comprendiendo adicionalmente la etapa de creación del primer túnel de VPN.

13. El método de la reivindicación 9, comprendiendo adicionalmente la etapa de reenvío del datagrama entrante a un componente de procesamiento de texto claro de producto comercialmente disponible, COTS, (226) para procesar el datagrama entrante.

14. Un medio legible por ordenador no transitorio para proporcionar una arquitectura de enlace seguro múltiple, MSL, que incluye lógica que, cuando se ejecuta por un dispositivo informático, provoca que el dispositivo informático realice al menos lo siguiente:

crear un primer túnel de VPN entre una estación de trabajo de cliente (106) y una primera pasarela de propietario (120a);
enviar un datagrama saliente desde la estación de trabajo de cliente (106) a la primera pasarela de propietario (120a);
recibir un datagrama entrante desde la primera pasarela de propietario (120a) a la estación de trabajo de cliente (106), en el que el datagrama entrante incluye una dirección de protocolo de internet, IP, de origen y una dirección IP de destino que se establece a una dirección IP privada de propietario de VPN;
registrar una nueva dirección IP privada de propietario de VPN desde la dirección IP de origen en el datagrama entrante;
asignar una nueva dirección IP privada única, UPIP, para el datagrama entrante y la estación de trabajo de cliente (106); y
enviar el datagrama entrante a la estación de trabajo de cliente (106),
en el que el sistema crea adicionalmente un segundo túnel de VPN entre la estación de trabajo de cliente (106) y una segunda pasarela de propietario (120b) mientras se está utilizando el primer túnel de VPN.

15. El medio legible por ordenador no transitorio de la reivindicación 14, en el que la lógica, que cuando se ejecuta por dicho dispositivo informático, provoca adicionalmente que el dispositivo informático realice al menos lo siguiente:

encriptar el datagrama saliente y transferir el datagrama saliente a la primera pasarela de propietario (120a); y
recibir el datagrama entrante en una forma encriptada desde la primera pasarela de propietario (120a) y desencriptar el datagrama entrante.

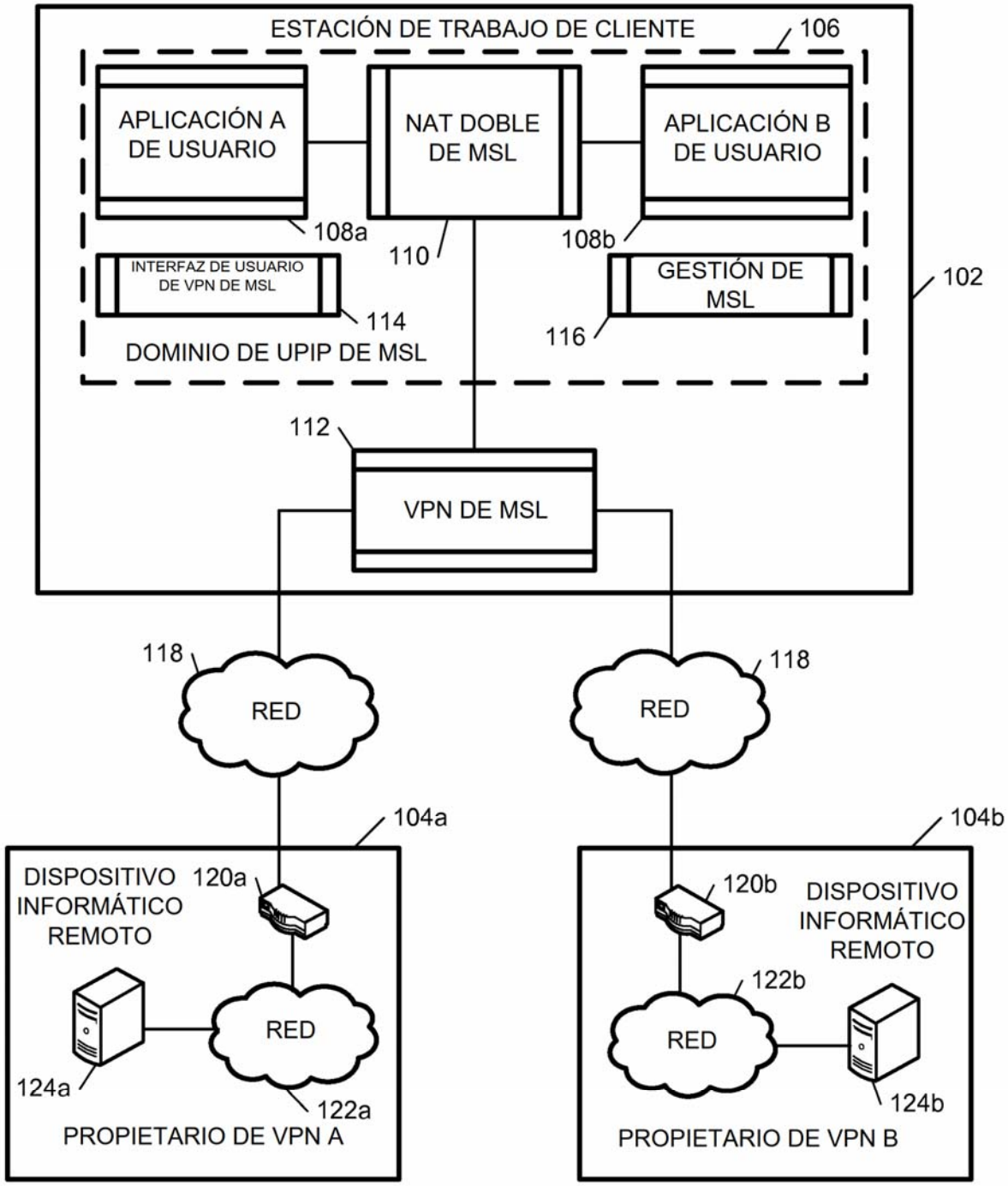
ESTACIÓN DE TRABAJO DE CLIENTE
106
APLICACIÓN A DE USUARIO
NAT DOBLE DE MSL
APLICACIÓN B DE USUARIO
108a
110
108b
INTERFAZ DE USUARIO DE VPN DE MSL
114
GESTIÓN DE MSL
116
DOMINIO DE UPIP DE MSL
102
112
VPN DE MSL
118
RED
118
RED
104a
104b
DISPOSITIVO INFORMÁTICO REMOTO
120a
120b
DISPOSITIVO INFORMÁTICO REMOTO
122b
RED
RED
124a
122a
124b
PROPIETARIO DE VPN A
PROPIETARIO DE VPN B

FIG. 1

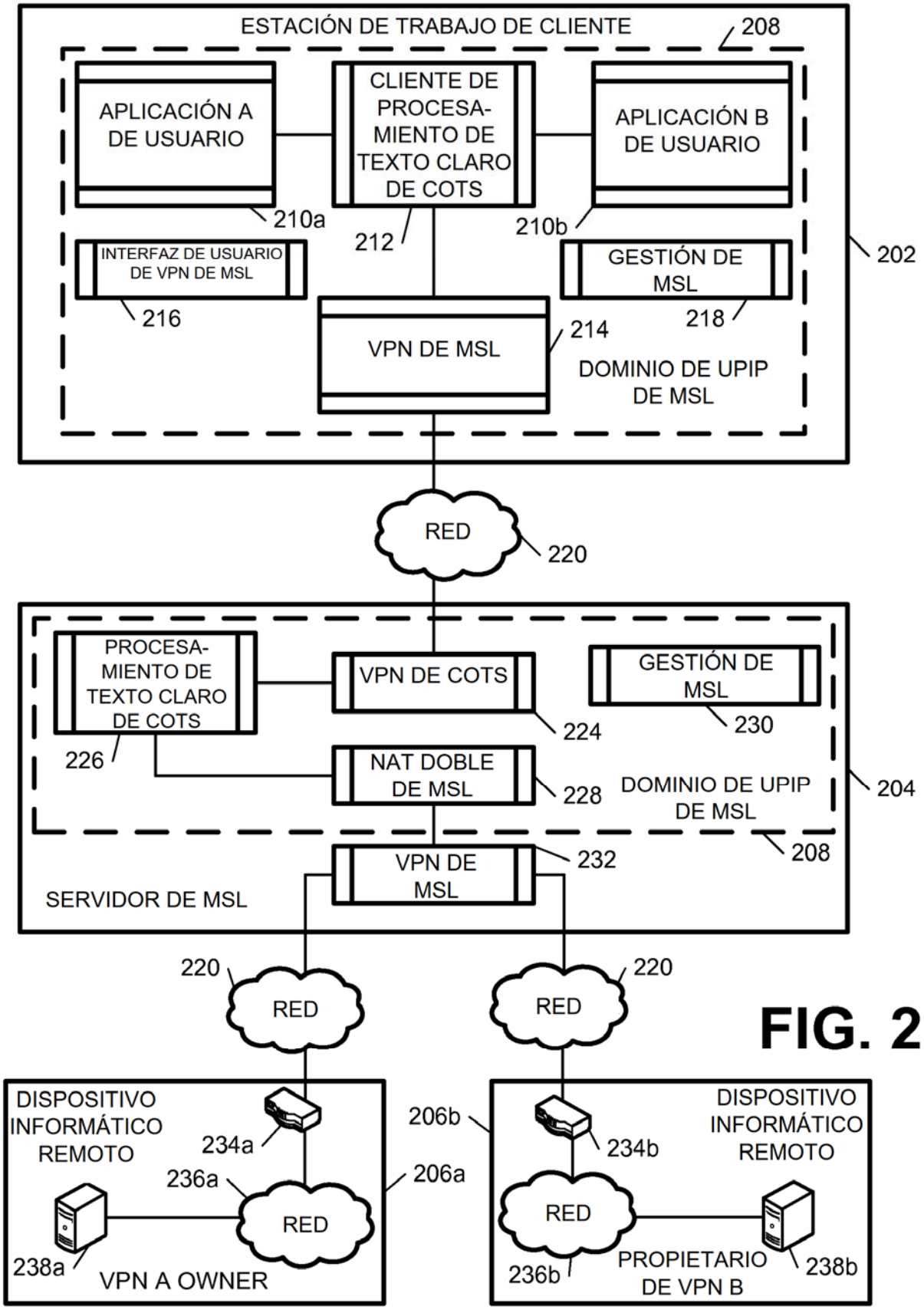
ESTACIÓN DE TRABAJO DE CLIENTE
208
APLICACIÓN A DE USUARIO
CLIENTE DE PROCESA-MIENTO DE TEXTO CLARO DE COTS
APLICACIÓN B DE USUARIO
210a
212
210b
INTERFAZ DE USUARIO DE VPN DE MSL
GESTIÓN DE MSL
202
216
218
VPN DE MSL
214
DOMINIO DE UPIP DE MSL
RED
220
PROCESA-MIENTO DE TEXTO CLARO DE COTS
VPN DE COTS
GESTIÓN DE MSL
224
230
226
NAT DOBLE DE MSL
228
DOMINIO DE UPIP DE MSL
204
208
VPN DE MSL
232
SERVIDOR DE MSL
220
RED
220
RED
DISPOSITIVO INFORMÁTICO REMOTO
234a
206b
234b
DISPOSITIVO INFORMÁTICO REMOTO
236a
206a
RED
RED
238a
VPN A OWNER
236b
PROPIETARIO DE VPN B
238b

FIG. 2

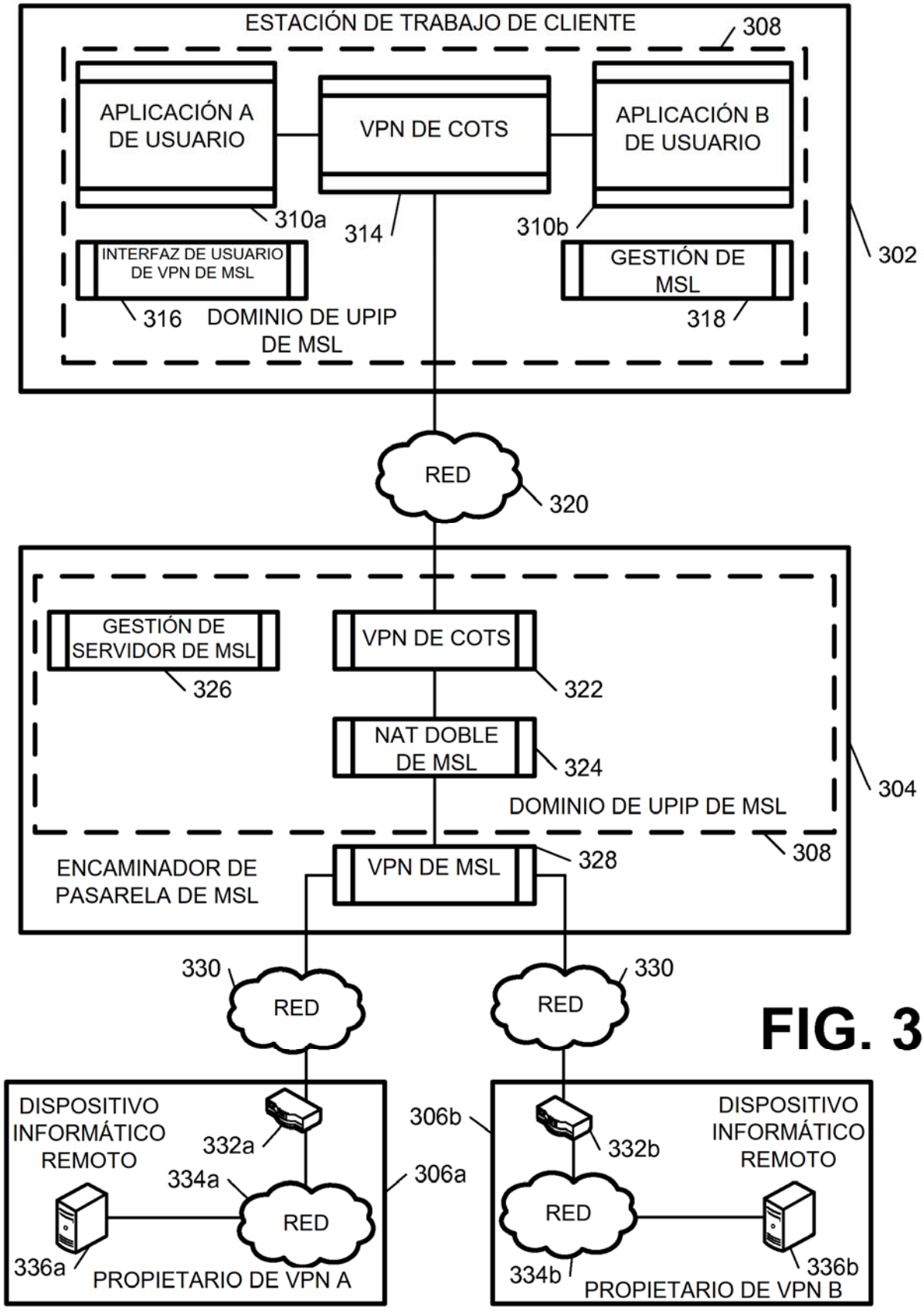
ESTACIÓN DE TRABAJO DE CLIENTE
308
APLICACIÓN A DE USUARIO
VPN DE COTS
APLICACIÓN B DE USUARIO
310a
314
310b
INTERFAZ DE USUARIO DE VPN DE MSL
GESTIÓN DE MSL
316
DOMINIO DE UPIP DE MSL
318
302
RED
320
GESTIÓN DE SERVIDOR DE MSL
VPN DE COTS
326
322
NAT DOBLE DE MSL
324
304
DOMINIO DE UPIP DE MSL
308
ENCAMINADOR DE PASARELA DE MSL
VPN DE MSL
328
330
RED
330
RED
DISPOSITIVO INFORMÁTICO REMOTO
332a
306b
332b
DISPOSITIVO INFORMÁTICO REMOTO
334a
306a
RED
RED
336a
PROPIETARIO DE VPN A
334b
336b
PROPIETARIO DE VPN B

FIG. 3

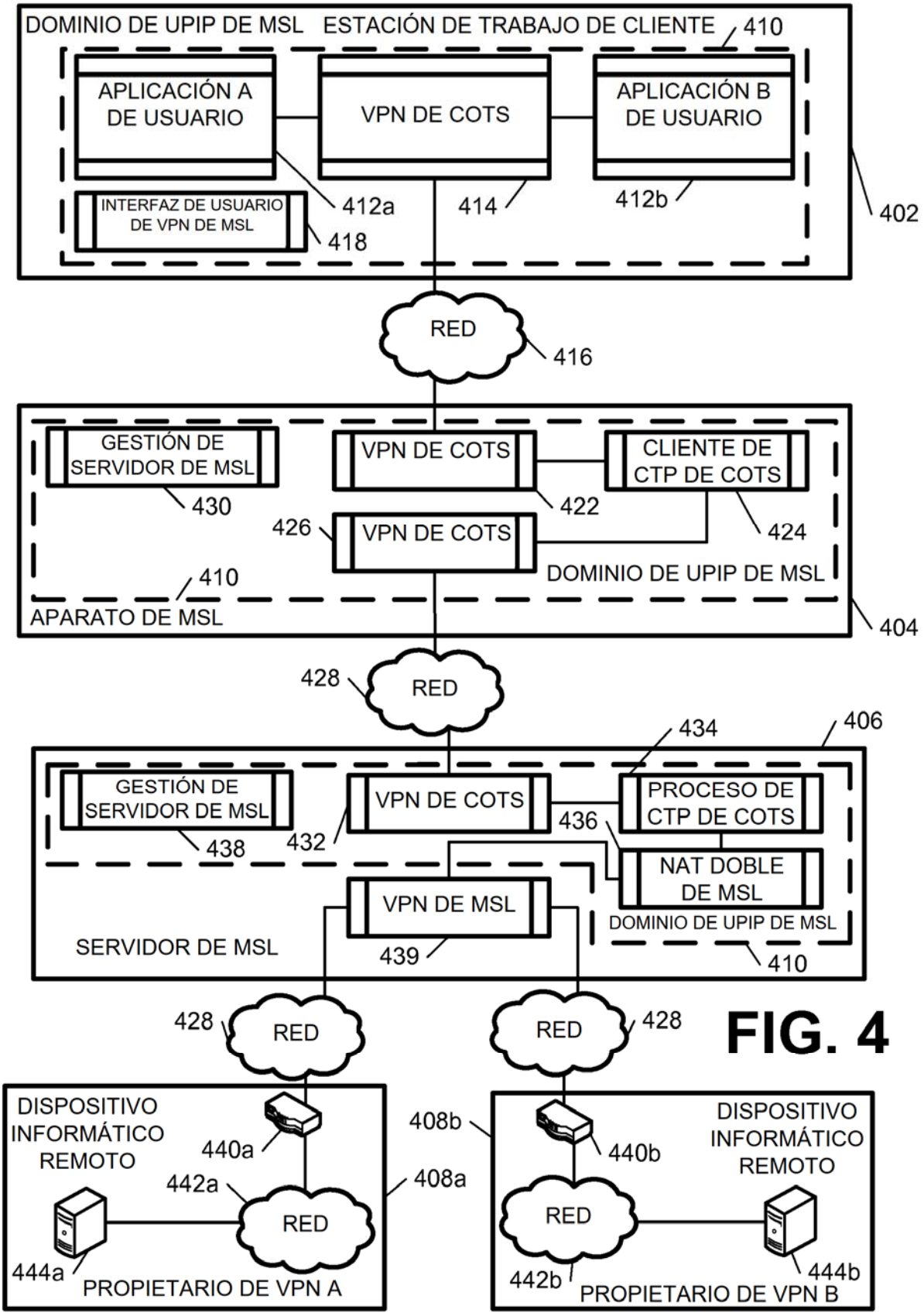
DOMINIO DE UPIP DE MSL
ESTACIÓN DE TRABAJO DE CLIENTE
410
APLICACIÓN A DE USUARIO
VPN DE COTS
APLICACIÓN B DE USUARIO
INTERFAZ DE USUARIO DE VPN DE MSL
412a
414
412b
418
402
RED
416
GESTIÓN DE SERVIDOR DE MSL
VPN DE COTS
CLIENTE DE CTP DE COTS
430
422
424
426
VPN DE COTS
DOMINIO DE UPIP DE MSL
410
APARATO DE MSL
404
428
RED
434
406
GESTIÓN DE SERVIDOR DE MSL
VPN DE COTS
PROCESO DE CTP DE COTS
438
432
436
NAT DOBLE DE MSL
VPN DE MSL
DOMINIO DE UPIP DE MSL
SERVIDOR DE MSL
439
410
428
RED
RED
428
DISPOSITIVO INFORMÁTICO REMOTO
440a
442a
RED
408a
444a
PROPIETARIO DE VPN A
408b
440b
DISPOSITIVO INFORMÁTICO REMOTO
RED
442b
444b
PROPIETARIO DE VPN B

FIG. 4

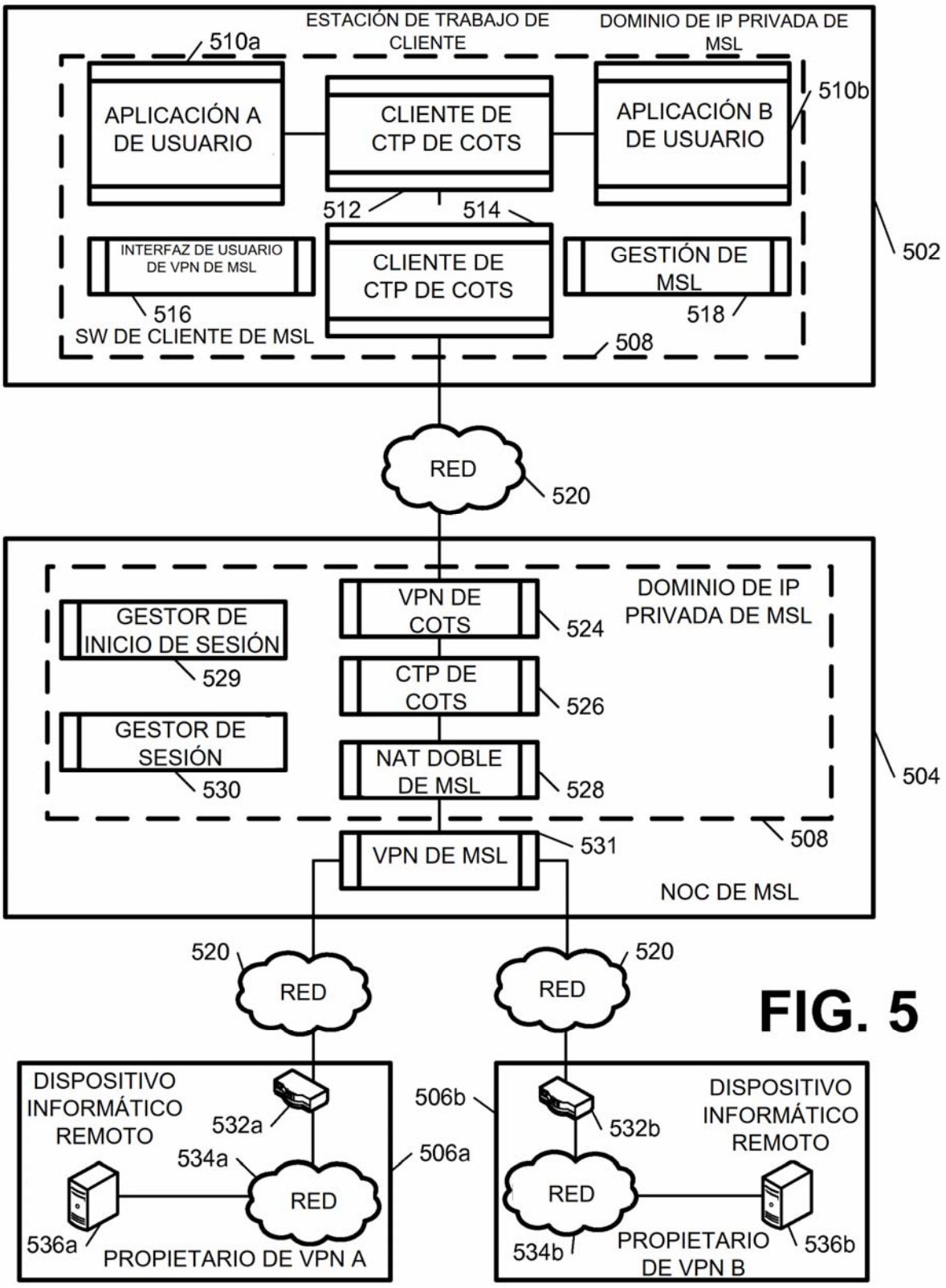
ESTACIÓN DE TRABAJO DE CLIENTE
DOMINIO DE IP PRIVADA DE MSL
510a
APLICACIÓN A DE USUARIO
CLIENTE DE CTP DE COTS
APLICACIÓN B DE USUARIO
510b
512
514
INTERFAZ DE USUARIO DE VPN DE MSL
CLIENTE DE CTP DE COTS
GESTIÓN DE MSL
502
516
518
SW DE CLIENTE DE MSL
508
RED
520
GESTOR DE INICIO DE SESIÓN
529
VPN DE COTS
524
DOMINIO DE IP PRIVADA DE MSL
CTP DE COTS
526
GESTOR DE SESIÓN
530
NAT DOBLE DE MSL
528
504
508
VPN DE MSL
531
NOC DE MSL
520
RED
520
RED
DISPOSITIVO INFORMÁTICO REMOTO
532a
506b
532b
DISPOSITIVO INFORMÁTICO REMOTO
534a
506a
RED
RED
536a
PROPIETARIO DE VPN A
534b
PROPIETARIO DE VPN B
536b

FIG. 5

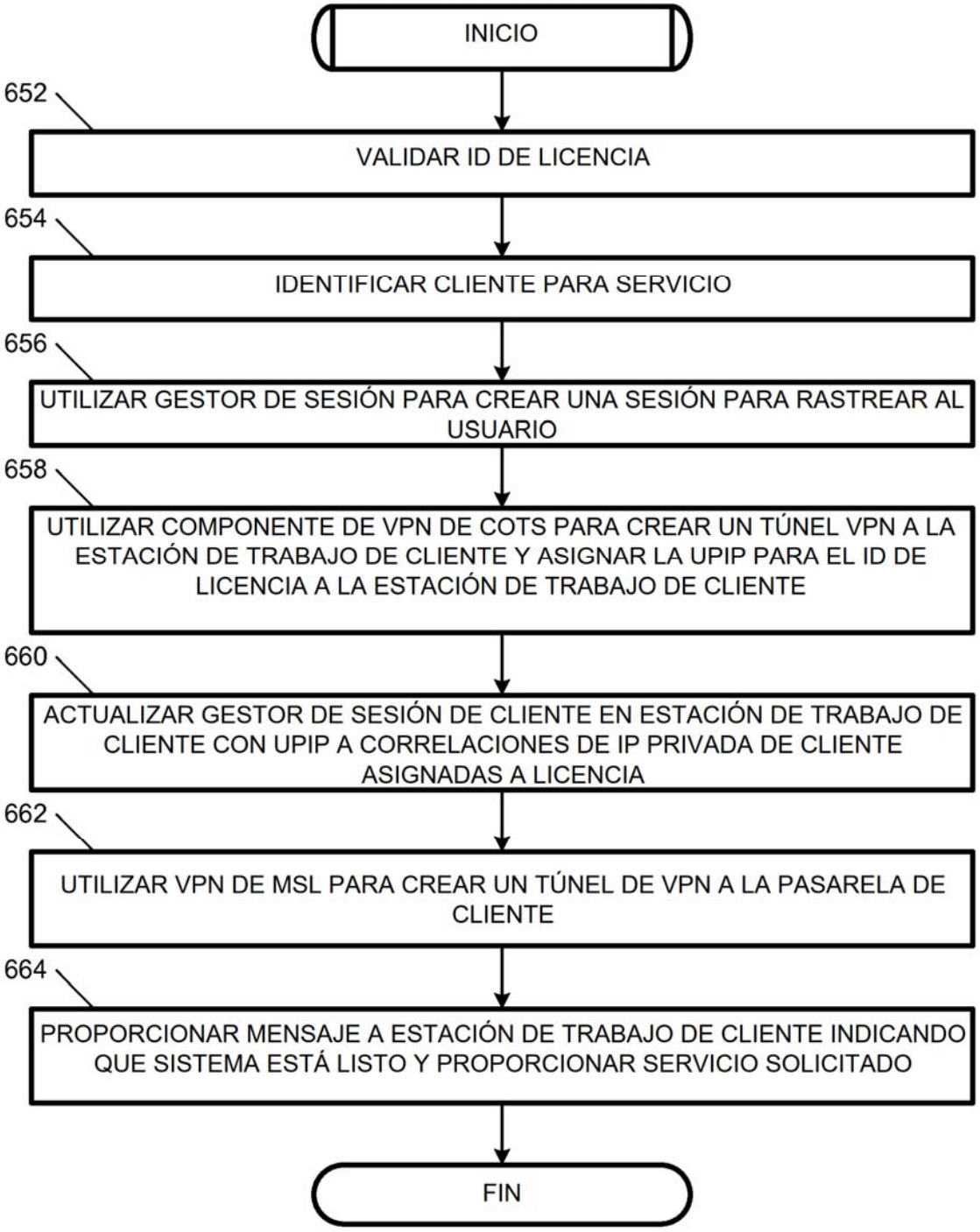
INICIO
652
VALIDAR ID DE LICENCIA
654
IDENTIFICAR CLIENTE PARA SERVICIO
656
UTILIZAR GESTOR DE SESIÓN PARA CREAR UNA SESIÓN PARA RASTREAR AL USUARIO
658
UTILIZAR COMPONENTE DE VPN DE COTS PARA CREAR UN TÚNEL VPN A LA ESTACIÓN DE TRABAJO DE CLIENTE Y ASIGNAR LA UPIP PARA EL ID DE LICENCIA A LA ESTACIÓN DE TRABAJO DE CLIENTE
660
ACTUALIZAR GESTOR DE SESIÓN DE CLIENTE EN ESTACIÓN DE TRABAJO DE CLIENTE CON UPIP A CORRELACIONES DE IP PRIVADA DE CLIENTE ASIGNADAS A LICENCIA
662
UTILIZAR VPN DE MSL PARA CREAR UN TÚNEL DE VPN A LA PASARELA DE CLIENTE
664
PROPORCIONAR MENSAJE A ESTACIÓN DE TRABAJO DE CLIENTE INDICANDO QUE SISTEMA ESTÁ LISTO Y PROPORCIONAR SERVICIO SOLICITADO
FIN

FIG. 6

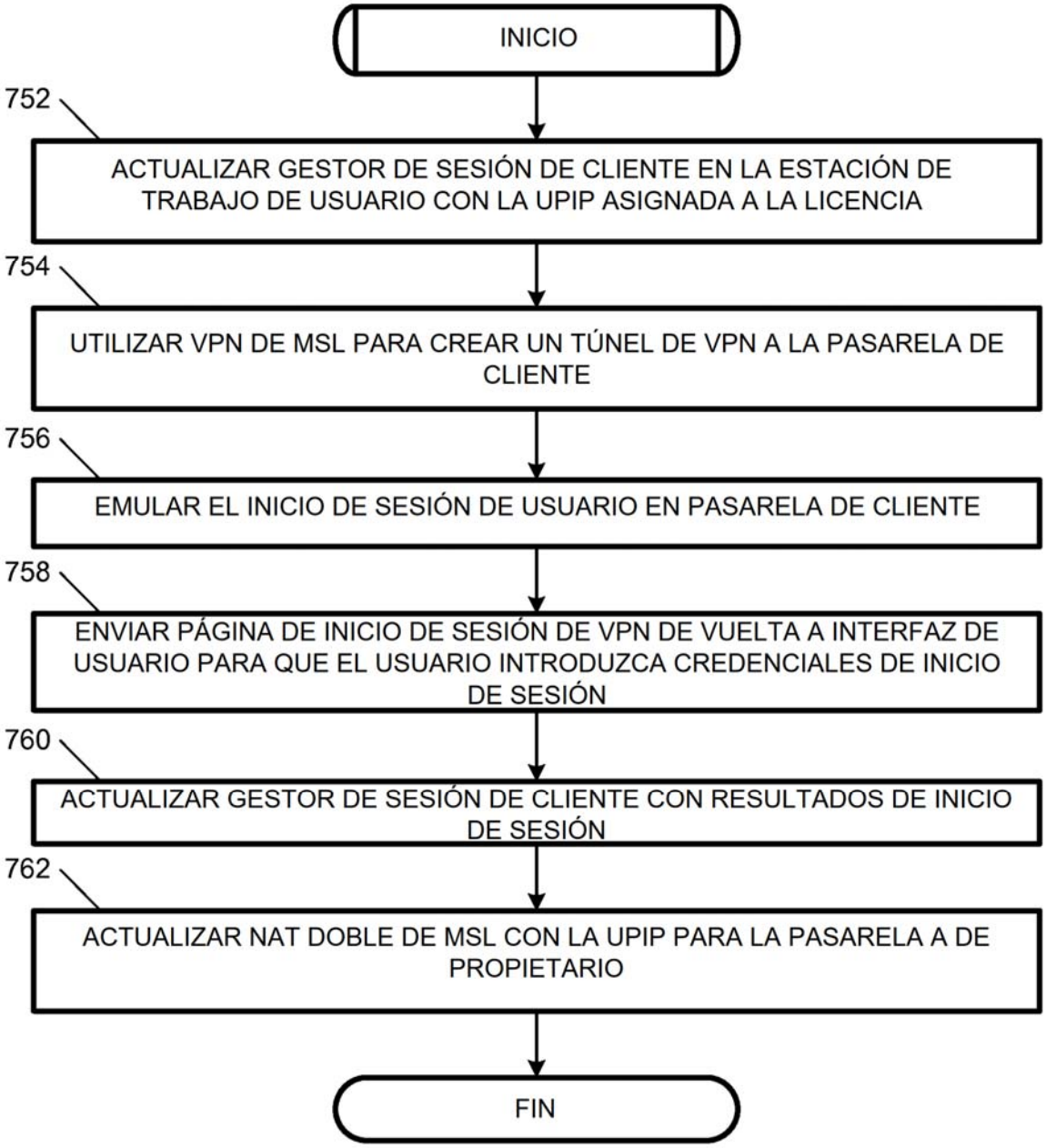
INICIO
752
ACTUALIZAR GESTOR DE SESIÓN DE CLIENTE EN LA ESTACIÓN DE TRABAJO DE USUARIO CON LA UPIP ASIGNADA A LA LICENCIA
754
UTILIZAR VPN DE MSL PARA CREAR UN TÚNEL DE VPN A LA PASARELA DE CLIENTE
756
EMULAR EL INICIO DE SESIÓN DE USUARIO EN PASARELA DE CLIENTE
758
ENVIAR PÁGINA DE INICIO DE SESIÓN DE VPN DE VUELTA A INTERFAZ DE USUARIO PARA QUE EL USUARIO INTRODUZCA CREDENCIALES DE INICIO DE SESIÓN
760
ACTUALIZAR GESTOR DE SESIÓN DE CLIENTE CON RESULTADOS DE INICIO DE SESIÓN
762
ACTUALIZAR NAT DOBLE DE MSL CON LA UPIP PARA LA PASARELA A DE PROPIETARIO
FIN

FIG. 7

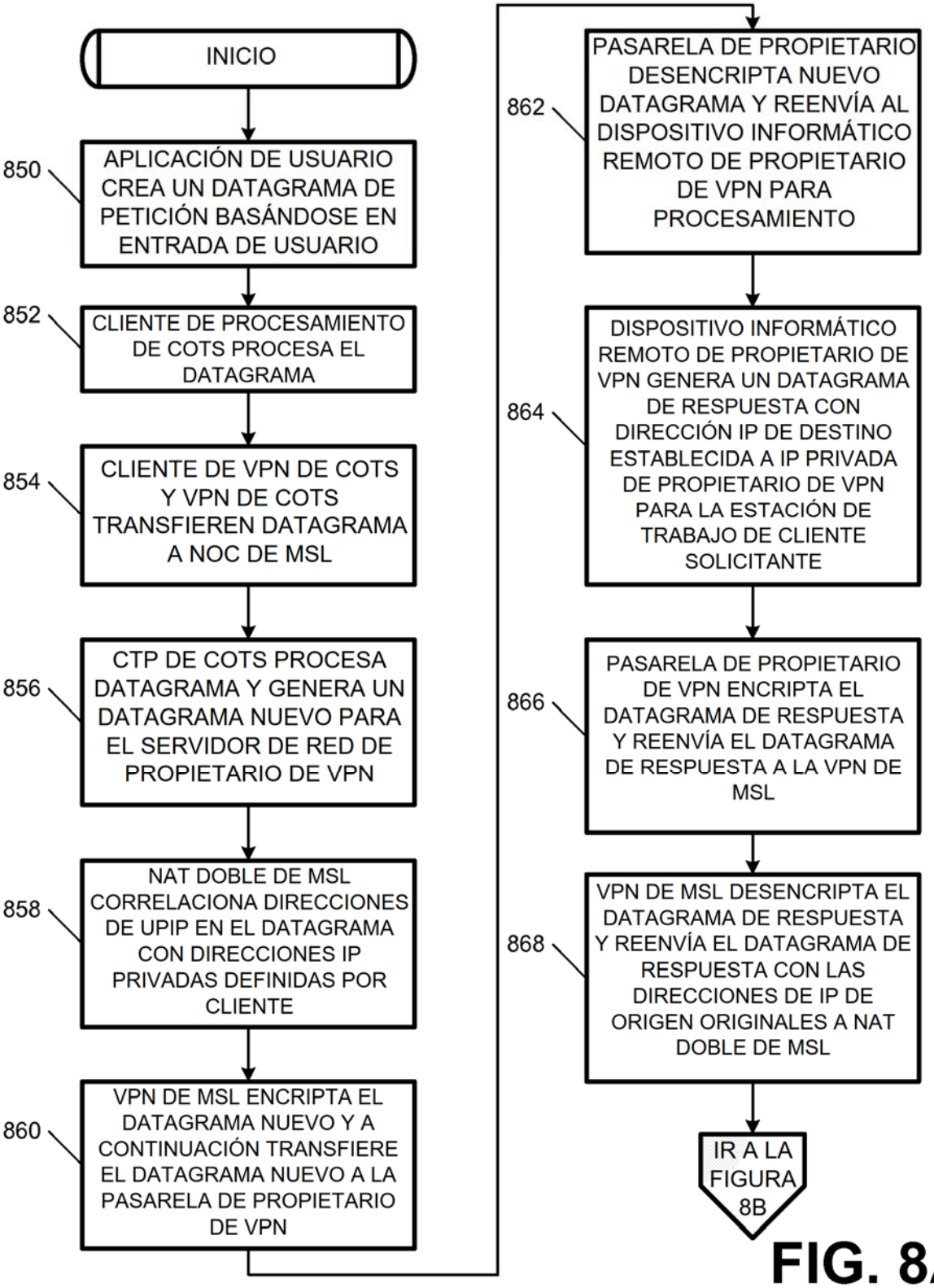
INICIO
850
APLICACIÓN DE USUARIO CREA UN DATAGRAMA DE PETICIÓN BASÁNDOSE EN ENTRADA DE USUARIO
852
CLIENTE DE PROCESAMIENTO DE COTS PROCESA EL DATAGRAMA
854
CLIENTE DE VPN DE COTS Y VPN DE COTS TRANSFIEREN DATAGRAMA A NOC DE MSL
856
CTP DE COTS PROCESA DATAGRAMA Y GENERA UN DATAGRAMA NUEVO PARA EL SERVIDOR DE RED DE PROPIETARIO DE VPN
858
NAT DOBLE DE MSL CORRELACIONA DIRECCIONES DE UPIP EN EL DATAGRAMA CON DIRECCIONES IP PRIVADAS DEFINIDAS POR CLIENTE
860
VPN DE MSL ENCRIPTA EL DATAGRAMA NUEVO Y A CONTINUACIÓN TRANSFIERE EL DATAGRAMA NUEVO A LA PASARELA DE PROPIETARIO DE VPN
862
PASARELA DE PROPIETARIO DESENCRIPTA NUEVO DATAGRAMA Y REENVÍA AL DISPOSITIVO INFORMÁTICO REMOTO DE PROPIETARIO DE VPN PARA PROCESAMIENTO
864
DISPOSITIVO INFORMÁTICO REMOTO DE PROPIETARIO DE VPN GENERA UN DATAGRAMA DE RESPUESTA CON DIRECCIÓN IP DE DESTINO ESTABLECIDA A IP PRIVADA DE PROPIETARIO DE VPN PARA LA ESTACIÓN DE TRABAJO DE CLIENTE SOLICITANTE
866
PASARELA DE PROPIETARIO DE VPN ENCRIPTA EL DATAGRAMA DE RESPUESTA Y REENVÍA EL DATAGRAMA DE RESPUESTA A LA VPN DE MSL
868
VPN DE MSL DESENCRIPTA EL DATAGRAMA DE RESPUESTA Y REENVÍA EL DATAGRAMA DE RESPUESTA CON LAS DIRECCIONES DE IP DE ORIGEN ORIGINALES A NAT DOBLE DE MSL
IR A LA FIGURA 8B

FIG. 8A

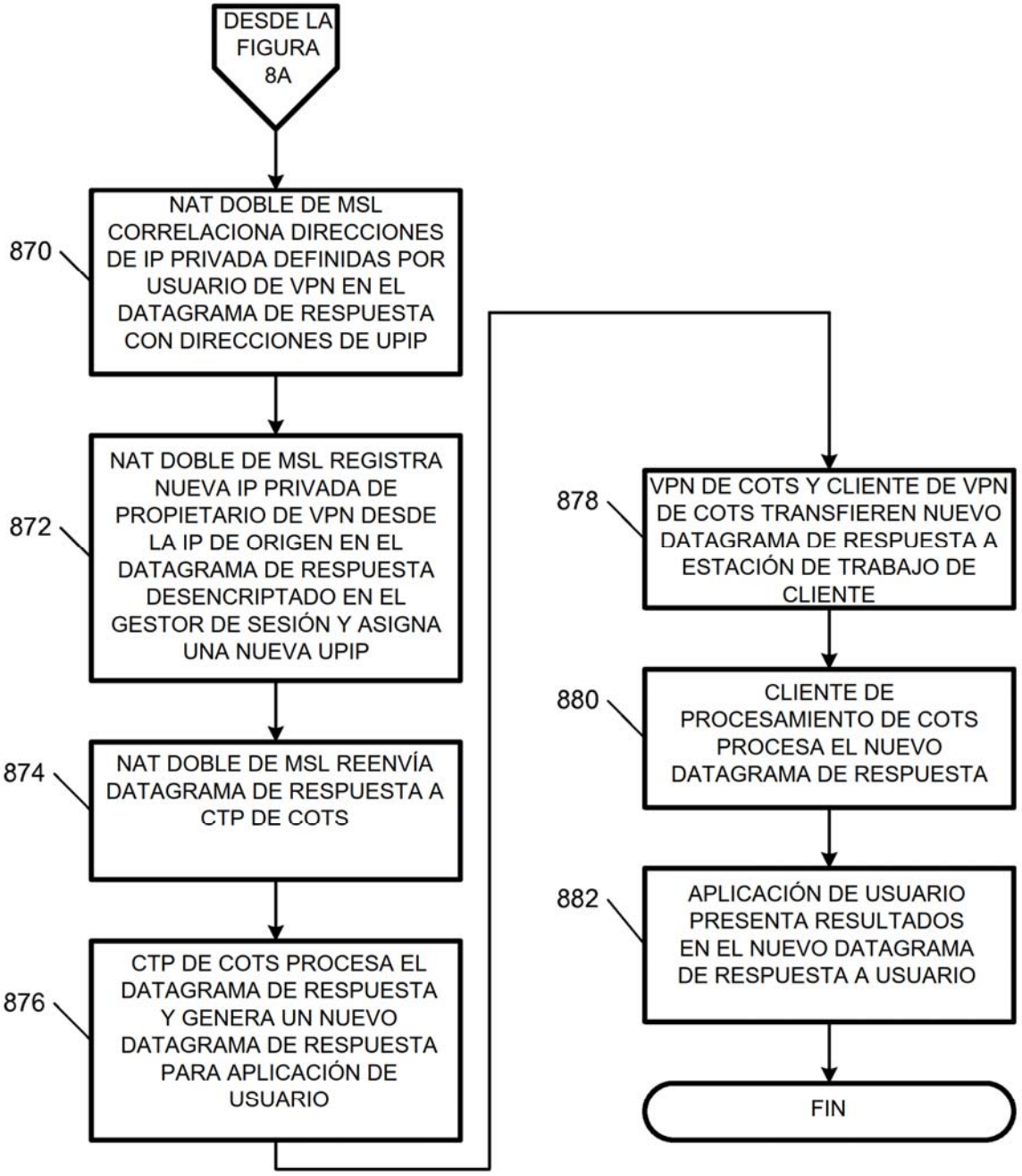
DESDE LA FIGURA 8A
870
NAT DOBLE DE MSL CORRELACIONA DIRECCIONES DE IP PRIVADA DEFINIDAS POR USUARIO DE VPN EN EL DATAGRAMA DE RESPUESTA CON DIRECCIONES DE UPIP
872
NAT DOBLE DE MSL REGISTRA NUEVA IP PRIVADA DE PROPIETARIO DE VPN DESDE LA IP DE ORIGEN EN EL DATAGRAMA DE RESPUESTA DESENCRIPTADO EN EL GESTOR DE SESIÓN Y ASIGNA UNA NUEVA UPIP
874
NAT DOBLE DE MSL REENVÍA DATAGRAMA DE RESPUESTA A CTP DE COTS
876
CTP DE COTS PROCESA EL DATAGRAMA DE RESPUESTA Y GENERA UN NUEVO DATAGRAMA DE RESPUESTA PARA APLICACIÓN DE USUARIO
878
VPN DE COTS Y CLIENTE DE VPN DE COTS TRANSFIEREN NUEVO DATAGRAMA DE RESPUESTA A ESTACIÓN DE TRABAJO DE CLIENTE
880
CLIENTE DE PROCESAMIENTO DE COTS PROCESA EL NUEVO DATAGRAMA DE RESPUESTA
882
APLICACIÓN DE USUARIO PRESENTA RESULTADOS EN EL NUEVO DATAGRAMA DE RESPUESTA A USUARIO
FIN

FIG. 8B

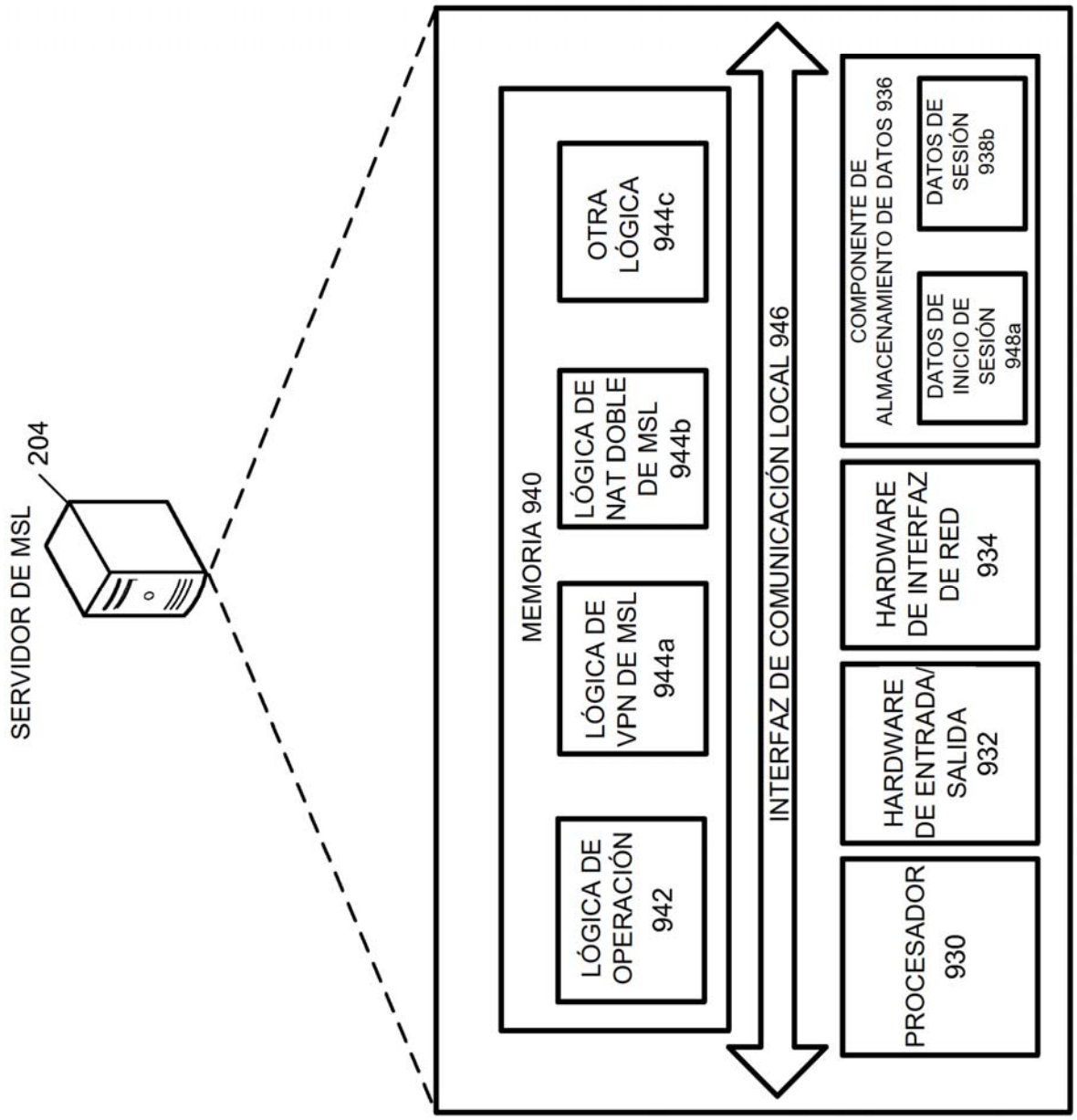
SERVIDOR DE MSL
204
MEMORIA 940
LÓGICA DE OPERACIÓN 942
LÓGICA DE VPN DE MSL 944a
LÓGICA DE NAT DOBLE DE MSL 944b
OTRA LÓGICA 944c
INTERFAZ DE COMUNICACIÓN LOCAL 946
PROCESADOR 930
HARDWARE DE ENTRADA/SALIDA 932
HARDWARE DE INTERFAZ DE RED 934
COMPONENTE DE ALMACENAMIENTO DE DATOS 936
DATOS DE INICIO DE SESIÓN 948a
DATOS DE SESIÓN 938b

FIG. 9