

REIVINDICACIONES

1. Un método implementado por computadora caracterizado porque comprende:
recibir, por un sistema informático que implementa una puerta de enlace (100) en una red privada (140), una solicitud de un dispositivo de cliente (121) para un túnel de red entre el dispositivo de cliente (121) y un dispositivo de red (141) en la red privada (140);

autenticar el dispositivo de cliente (121) por el sistema informático;

al autenticar el dispositivo cliente (121), recibir, de un servidor de autenticación (160) en comunicación con el sistema informático, una lista de accesos de cliente que incluye una lista de dispositivos de red con la que tiene permitido comunicarse el dispositivo de cliente (121);

al recibir la lista de accesos de cliente, verificar, por el sistema informático, que el dispositivo de red (141) en la red privada (140) sea parte de la lista de dispositivos de red con la que tiene permitido comunicarse el dispositivo de cliente (121); y

al verificar que el dispositivo de red (141) en la red privada (140) es parte de la lista de dispositivos de red con la que tiene permitido comunicarse el dispositivo de cliente (121), establecer, por el sistema informático, el túnel de red entre el dispositivo de cliente (121) y el dispositivo de red en la red privada a través de la puerta de enlace (100).

2. El método de conformidad con la reivindicación 1, caracterizado porque el dispositivo de red (141) en la red privada (140) incluye un servidor de aplicaciones que

proporciona un servicio, y en donde el servidor de aplicaciones (141) incluye uno o más de:

- un servidor de correo que proporciona un servicio de correo;
- un servidor de archivos que proporciona un almacén de datos conectado a red; y
- un servidor web que proporciona servicios de alojamiento.

3. El método de conformidad con la reivindicación 1, caracterizado porque el dispositivo de red (141) en la red privada incluye uno o más de un enrutador y un conmutador que proporciona acceso de administrador.

4. El método de conformidad con la reivindicación 1, caracterizado porque el sistema informático además implementa un cortafuegos (102) para bloquear de manera selectiva y permitir tráfico de red entre el dispositivo de cliente (121) y el dispositivo de red (141) en la red privada (140), y en donde el cortafuegos (102) bloquea todo el tráfico de red entre el dispositivo de cliente (121) y el dispositivo de red (141) en la red privada (140) por defecto.

5. El método de conformidad con la reivindicación 4, caracterizado además porque comprende:

obtener, por el sistema informático, una regla de cortafuegos para permitir el acceso de red entre el dispositivo de cliente (121) y el dispositivo de red (141) en la red privada (140); y

configurar el cortafuegos basándose en la regla de cortafuegos;

en donde la regla de cortafuegos se incluye en la lista de accesos de cliente.

6. El método de conformidad con la reivindicación 1, caracterizado porque establecer el túnel de red entre el dispositivo de cliente (121) y el dispositivo de red (141) en la red privada incluye establecer una red privada virtual.

7. El método de conformidad con la reivindicación 1, caracterizado porque la lista de accesos de cliente es legible, pero no alterable, por el cliente.

8. El método de conformidad con la reivindicación 1, caracterizado porque autenticar el dispositivo de cliente (121) incluye verificar una firma digital en la lista de accesos de cliente mediante una clave de firma compartida entre la puerta de enlace (100) y el servidor de autenticación (160).

9. El método de conformidad con la reivindicación 1, caracterizado además porque comprende recibir, por el sistema informático del servidor de autenticación (160), una lista de túneles de cliente que incluye información para establecer el túnel de conexión a red, en donde la lista de túneles de cliente sólo se recibe del servidor de autenticación (160) en respuesta a una autenticación exitosa del dispositivo de cliente, y no se recibe de otra manera.

10. El método de conformidad con la reivindicación 9, caracterizado porque la lista de túneles de cliente incluye una dirección de protocolo de Internet de destino y un número de puerto de destino de la puerta de enlace.

11. El método de conformidad con la reivindicación 1, caracterizado porque la lista de accesos de cliente incluye una primera selección de dispositivos de red y una segunda selección de dispositivos de red, la segunda selección de dispositivos de red tiene requerimientos de autenticación mejorados con respecto a la primera selección de dispositivos de red, y en donde los requerimientos de autenticación mejorados incluyen un requerimiento seleccionado del grupo que consiste de:

- un requerimiento de que todos los parches necesitan aplicarse a un sistema operativo en el cliente;

- un requerimiento de que un escáner de virus actualizado debe ejecutarse en el cliente; y

- un requerimiento de que el cliente no está intentando tener acceso al dispositivo de red en la red privada mediante una red inalámbrica pública.

12. El método de conformidad con la reivindicación 11, caracterizado porque los requerimientos de autenticación mejorados incluyen un requerimiento de que un usuario del dispositivo de cliente proporcione una credencial de autenticación seleccionada del grupo que consiste de:

- un escaneo de huella digital;

un escaneo del iris; y

una clave generada por un generador de claves externo.

13. El método de conformidad con la reivindicación 1, caracterizado además porque comprende:

recibir, por el sistema informático, información de estado de cliente del cliente; y

romper el túnel de red en respuesta a una no recepción de la información de estado de cliente del cliente en un intervalo de tiempo regular o en respuesta a la información de estado de cliente que no corresponde con requerimientos predefinidos para el cliente.

14. Un medio legible por computadora no transitorio caracterizado porque almacena instrucciones que, cuando se ejecutan, provocan que un sistema informático que implementa una puerta de enlace (100) a una red privada (140):

reciba una solicitud de un dispositivo de cliente (121) para un túnel de red entre el dispositivo de cliente y un dispositivo de red (141) en la red privada (140);

autenticar el dispositivo de cliente (121);

al autenticar el dispositivo cliente (121), reciba, de un servidor de autenticación (160) en comunicación con el sistema informático, una lista de accesos de cliente que incluye una lista de dispositivos de red con la que tiene permitido comunicarse el dispositivo de cliente (121);

al recibir la lista de accesos de cliente, verifique que el dispositivo de red (141) en la red privada (140) sea parte de la lista de dispositivos de red con la que tiene permitido

comunicarse el dispositivo de cliente (121); y

al verificar que el dispositivo de red (141) en la red privada (140) es parte de la lista de dispositivos de red con la que tiene permitido comunicarse el dispositivo de cliente (121), establezca el túnel de red entre el dispositivo de cliente (121) y el dispositivo de red (141) en la red privada (140) a través de la puerta de enlace (100).

15. Un sistema informático que implementa una puerta de enlace, el sistema informático caracterizado porque comprende:

un procesador; y

una memoria no transitoria en comunicación con el procesador y que almacena instrucciones que, cuando se ejecutan por el procesador, provocan que el sistema informático:

reciba una solicitud de un dispositivo de cliente (121) para un túnel de red entre el dispositivo de cliente (121) y un dispositivo de red (141) en la red privada (140);

autentique el dispositivo de cliente (121);

al autenticar el dispositivo cliente (121), reciba, de un servidor de autenticación (160) en comunicación con el sistema informático, una lista de accesos de cliente que incluye una lista de dispositivos de red con la que tiene permitido comunicarse el dispositivo de cliente (121);

al recibir la lista de accesos de cliente, verifique que el dispositivo de red (141) en la red privada (140) sea parte de la lista de dispositivos de red con la que tiene permitido comunicarse el dispositivo de cliente (121); y

al verificar que el dispositivo de red (141) en la red privada (140) es parte de la lista de dispositivos de red con la que tiene permitido comunicarse el dispositivo de cliente (121), establezca el túnel de red entre el dispositivo de cliente (121) y el dispositivo de red (141) en la red privada (140) a través de la puerta de enlace (100).

P-13175

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO
DIRECCIÓN DE NUEVAS CREACIONES

E. S. D.

Re: Expediente No. **NC2017/0003283**

Solicitud de patente a nombre de **CRYPTZONE NORTH AMERICA INC.**

Yo, CAROLINA DAZA MONTALVO identificada como aparece al pie de mi firma, domiciliada en la Carrera 11 No. 86-53, obrando como apoderada de la sociedad CRYPTZONE NORTH AMERICA INC., solicitante de la patente de la referencia, en respuesta al oficio No. **5813** notificado el 16 de mayo de 2018, relacionado con concepto técnico de fondo, atentamente me permito manifestar:

1. Modificación a las Reivindicaciones

Con fundamento en la facultad que confiere el artículo 34 de la Decisión 486 al solicitante para modificar la solicitud de patente en cualquier momento del trámite, presento junto con este memorial nuevo capítulo reivindicatorio, el cual consta de 15 reivindicaciones y reemplaza completamente el capítulo presentado anteriormente. En el nuevo capítulo reivindicatorio se realizaron las siguientes modificaciones:

- 1.1.** Se rescribió el contenido de la nueva reivindicación independiente 1, para establecer una relación técnica estructural entre sus componentes, y hacer referencia a *“... al autenticar el dispositivo cliente (121), recibir, de un servidor de autenticación (160) en comunicación con el sistema informático, una lista de accesos de cliente que incluye una lista de dispositivos de red con la que tiene permitido comunicarse el dispositivo de cliente (121); al recibir la lista de accesos de cliente, verificar, por el sistema informático, que el dispositivo de red (141) en la red privada (140) sea parte de la lista de dispositivos de red con la que tiene permitido comunicarse el dispositivo de cliente (121); y al verificar que el dispositivo de red (141) en la red privada (140) es parte de la lista de dispositivos de red con la que tiene permitido comunicarse el dispositivo de cliente (121), establecer, por el sistema informático, el túnel de red entre el dispositivo de cliente (121) y el dispositivo de red (141) en la red privada (140) a través de la puerta de enlace (100)”*, con base en el soporte que provee la Descripción original presentada, en particular párrafos 0046-0049 de la publicación internacional WO2016057177.

-
- 1.2. Se rescribió el contenido de la nueva reivindicación independiente 14 (antigua reivindicación 19), para establecer una relación técnica estructural entre sus componentes, y hacer referencia a *“... al autenticar el dispositivo cliente (121), reciba, de un servidor de autenticación (160) en comunicación con el sistema informático, una lista de accesos de cliente que incluye una lista de dispositivos de red con la que tiene permitido comunicarse el dispositivo de cliente (121); al recibir la lista de accesos de cliente, verifique, que el dispositivo de red (141) en la red privada (140) sea parte de la lista de dispositivos de red con la que tiene permitido comunicarse el dispositivo de cliente (121); y al verificar que el dispositivo de red (141) en la red privada (140) es parte de la lista de dispositivos de red con la que tiene permitido comunicarse el dispositivo de cliente (121), establezca, el túnel de red entre el dispositivo de cliente (121) y el dispositivo de red (141) en la red privada (140) a través de la puerta de enlace (100)”*, con base en el soporte que provee la Descripción original presentada, en particular párrafos 0046-0049 de la publicación internacional WO2016057177.
- 1.3. Se rescribió el contenido de la nueva reivindicación independiente 15 (antigua reivindicación 20), para establecer una relación técnica estructural entre sus componentes, y hacer referencia a *“... al autenticar el dispositivo cliente (121), reciba, de un servidor de autenticación (160) en comunicación con el sistema informático, una lista de accesos de cliente que incluye una lista de dispositivos de red con la que tiene permitido comunicarse el dispositivo de cliente (121); al recibir la lista de accesos de cliente, verifique, que el dispositivo de red (141) en la red privada (140) sea parte de la lista de dispositivos de red con la que tiene permitido comunicarse el dispositivo de cliente (121); y al verificar que el dispositivo de red (141) en la red privada (140) es parte de la lista de dispositivos de red con la que tiene permitido comunicarse el dispositivo de cliente (121), establezca, el túnel de red entre el dispositivo de cliente (121) y el dispositivo de red (141) en la red privada (140) a través de la puerta de enlace (100)”*, con base en el soporte que provee la Descripción original presentada, en particular párrafos 0046-0049 de la publicación internacional WO2016057177.
- 1.4. Se combinaron las antiguas reivindicaciones 2 y 3 en una nueva reivindicación 2; se combinaron las antiguas reivindicaciones 5 y 6 en una nueva reivindicación 4; se combinaron las antiguas reivindicaciones 7 y 8 en una nueva reivindicación 5; se combinaron las antiguas reivindicaciones 12 y 13 en una nueva reivindicación 9; se combinaron las antiguas reivindicaciones 15 y 16 en una nueva reivindicación 11.
- 1.5. Se eliminaron las antiguas reivindicaciones 3, 6, 8, 13 y 16.
- 1.6. En vista de lo anterior, se reenumeran las reivindicaciones y sus dependencias.

En cuanto a estas modificaciones, me permito decir que las mismas no amplían de ninguna manera la materia objeto de la presente solicitud y se realizaron con el ánimo de superar las objeciones de claridad planteadas por el examinador en su concepto técnico.

2. Descripción (Art. 28 y 29)

Solicito a ese Despacho tener en cuenta que el solicitante desea eliminar el primer párrafo titulado “Referencias Cruzadas a las Solicitudes Relacionadas” en la página 1 de la descripción original.

Por otra parte, solicito a ese Despacho tener en cuenta que el solicitante desea agregar un nuevo párrafo en la sección titulada “Antecedentes de la Invención” en la página 6 de la descripción original de la siguiente manera para añadir algunos documentos relevantes del estado de la técnica.

La solicitud de patente de los Estados Unidos US2014/282914 divulga transportar datos de aplicaciones a través de un túnel de comunicaciones entre un dispositivo host y un dispositivo invitado. US2008/028436 divulga un filtro de acceso escalable para uso en una red privada virtual. US2010/205657 revela comunicaciones informáticas protegidas. US 2007/1010405 divulga un sistema y método diseñados para asegurar que una conexión de red privada virtual cumpla con políticas de seguridad de red.

En cuanto a estas modificaciones, me permito decir que las mismas no amplían de ninguna manera la materia objeto de la presente solicitud y se realizaron con el ánimo de dar claridad a la invención.

3. Pago de tasas

Considerando que el presente memorial se presenta junto con modificaciones a las reivindicaciones, se adjunta recibo por concepto de examen de patentabilidad, según lo establecido en la Resolución 3719 del 2016.

En relación con el número de reivindicaciones, atentamente nos permitimos decir que no se adjunta tasa por reivindicaciones adicionales, toda vez que el nuevo capítulo

reivindicatorio tiene un menor número de cláusulas que el originalmente presentado y es en esencia el mismo objeto, pero más limitado y definido con mayor claridad.

4. Novedad/Nivel inventivo

El examinador establece en su concepto técnico la falta de novedad y nivel inventivo por parte de las antiguas reivindicaciones 1 a 20, a la luz de las enseñanzas técnicas descritas en el documento US2014282914 (D1) en combinación con los documentos US2008028436 (D2) y US6381631 (D3).

En primer lugar, me permito decir que el artículo 16 de la Decisión 486 de la Comisión de la Comunidad Andina establece que la invención se considera nueva cuando no está comprendida en el estado de la técnica. Si de acuerdo con el espíritu de la norma legal indicada, la invención no se considera como nueva si está “comprendida” en el estado de la técnica, dicha norma se está refiriendo, naturalmente, a la totalidad del invento y no a alguno o a algunos de los componentes.

Así, para que la invención pierda su calidad de novedosa, es claro que ella, TODA ELLA, ha de estar contenida en el “conjunto de conocimientos existentes que son aplicables al proceso industrial” como define el estado de la técnica el Tribunal de justicia del Acuerdo de Cartagena (Proceso No. 6-IP-89, sentencia de 31 de octubre de 1989, publicada en Jurisprudencia del Tribunal de Justicia del Acuerdo de Cartagena, Tomo 11, BID-INTAL, Buenos Aires, 1994, página 60).

Aplicando lo anterior al caso concreto, para que las razones que aduce ese despacho para desvirtuar la novedad fuesen ciertas, sería forzoso que se demostrara que la invención de mi mandante esté comprendida en el estado de la técnica, específicamente en forma individual en los documentos D1, D2 y D3 de forma TOTAL, lo cual no sucede con la materia reclamada en el nuevo capítulo reivindicatorio, como se demostrará con los argumentos a continuación.

Del mismo modo, el artículo 18 de la Decisión 486 establece que “*Se considerará que una invención tiene nivel inventivo, si para una persona del oficio normalmente versada en la materia técnica correspondiente, esa invención no hubiese resultado obvia ni se hubiese derivado de manera evidente del estado de la técnica*”.

Lo anterior significa que el análisis de nivel inventivo NO es una comparación de los objetos de las anterioridades y la solicitud en estudio. El análisis de nivel inventivo debe demostrar la obviedad de la invención y establecer cómo ésta no contiene un salto cualitativo, que demuestre su altura inventiva, teniendo en cuenta que se hace necesario

demostrar que la invención analizada carece de nivel inventivo y hubiese sido obvia para una persona versada en la materia.

Considerando la anterior definición, es deseo del solicitante señalar que la combinación de las enseñanzas de D1 y D2 y la combinación de las enseñanzas de D1 y D3 no hacen obvia la presente invención de acuerdo con las razones expuestas a continuación.

Así las cosas, se llama la atención del examinador frente a las modificaciones introducidas a las reivindicaciones, de forma que el método, dispositivo y sistema se encuentran definidos de forma más clara y completa.

En primer lugar, me permito llamar la atención del Examinador sobre la materia reclamada en el Capítulo Reivindicatorio Modificado adjunto, en el cual, y como se explicó en el numeral 1 del presente memorial, con referencia a la nueva reivindicación 1, donde se reclama específicamente: *“Un método implementado por computadora caracterizado porque comprende: recibir, por un sistema informático que implementa una puerta de enlace (100) en una red privada (140), una solicitud de un dispositivo de cliente (121) para un túnel de red entre el dispositivo de cliente (121) y un dispositivo de red (141) en la red privada (140); autenticar el dispositivo de cliente (121) por el sistema informático; al autenticar el dispositivo cliente (121), recibir, de un servidor de autenticación (160) en comunicación con el sistema informático, una lista de accesos de cliente que incluye una lista de dispositivos de red con la que tiene permitido comunicarse el dispositivo de cliente (121); al recibir la lista de accesos de cliente, verificar, por el sistema informático, que el dispositivo de red (141) en la red privada (140) sea parte de la lista de dispositivos de red con la que tiene permitido comunicarse el dispositivo de cliente (121); y al verificar que el dispositivo de red (141) en la red privada (140) es parte de la lista de dispositivos de red con la que tiene permitido comunicarse el dispositivo de cliente (121), establecer, por el sistema informático, el túnel de red entre el dispositivo de cliente (121) y el dispositivo de red en la red privada a través de la puerta de enlace (100)”*, con referencia a la nueva reivindicación 14, donde se reclama específicamente: *“Un medio legible por computadora no transitorio caracterizado porque almacena instrucciones que, cuando se ejecutan, provocan que un sistema informático que implementa una puerta de enlace (100) a una red privada (140): reciba una solicitud de un dispositivo de cliente (121) para un túnel de red entre el dispositivo de cliente y un dispositivo de red (141) en la red privada (140); autenticar el dispositivo de cliente (121); al autenticar el dispositivo cliente (121), reciba, de un servidor de autenticación (160) en comunicación con el sistema informático, una lista de accesos de cliente que incluye una lista de dispositivos de red con la que tiene permitido comunicarse el dispositivo de cliente (121); al recibir la lista de accesos de cliente, verifique que el dispositivo de red (141) en la red privada (140) sea parte de la lista de dispositivos de red con la que tiene permitido comunicarse el dispositivo de cliente (121); y al verificar que el dispositivo de red (141) en la red privada (140) es parte de la lista de dispositivos de red con la que tiene permitido comunicarse el dispositivo de cliente (121), establezca el túnel de red entre el dispositivo de cliente (121) y el dispositivo*

de red (141) en la red privada (140) a través de la puerta de enlace (100)”, con referencia a la nueva reivindicación 15, donde se reclama específicamente: “Un sistema informático que implementa una puerta de enlace, el sistema informático caracterizado porque comprende: un procesador; y una memoria no transitoria en comunicación con el procesador y que almacena instrucciones que, cuando se ejecutan por el procesador, provocan que el sistema informático: reciba una solicitud de un dispositivo de cliente (121) para un túnel de red entre el dispositivo de cliente (121) y un dispositivo de red (141) en la red privada (140); autentique el dispositivo de cliente (121); al autenticar el dispositivo cliente (121), reciba, de un servidor de autenticación (160) en comunicación con el sistema informático, una lista de accesos de cliente que incluye una lista de dispositivos de red con la que tiene permitido comunicarse el dispositivo de cliente (121); al recibir la lista de accesos de cliente, verifique que el dispositivo de red (141) en la red privada (140) sea parte de la lista de dispositivos de red con la que tiene permitido comunicarse el dispositivo de cliente (121); y al verificar que el dispositivo de red (141) en la red privada (140) es parte de la lista de dispositivos de red con la que tiene permitido comunicarse el dispositivo de cliente (121), establezca el túnel de red entre el dispositivo de cliente (121) y el dispositivo de red (141) en la red privada (140) a través de la puerta de enlace (100)”, cuyas características no se encuentran totalmente divulgadas en los documentos citados D1 y D2.

Es deseo del solicitante también respetuosamente manifestar que, si bien varias características enumeradas en las reivindicaciones dependientes de la invención pueden ser patentablemente distintas por sí mismas, cada una de estas reivindicaciones dependientes es patentablemente distinta por al menos las mismas razones que la reivindicación independiente 1, de la cual dependen.

Ahora bien, D1 no divulga varios de los elementos de la reivindicación 1. Por ejemplo, la reivindicación 1 requiere implementar una **“puerta de enlace a una red privada”** entre un **“dispositivo cliente y un dispositivo de red en la red privada”**. Estos dispositivos, como se reivindica, forman parte de la red privada. Por el contrario, D1 se limita a divulgar un dispositivo invitado 204 que no es parte de una red privada que intenta conectarse con un dispositivo host 254.

Específicamente, el párrafo [0044] de D1, por ejemplo, revela la recepción de “una solicitud de conexión... desde un dispositivo invitado 204... para establecer... con el dispositivo host 254”.

De acuerdo con las anteriores limitaciones distintivas, la reivindicación 1 requiere “Verificar... que el dispositivo de red (141) en la red privada (140) sea parte de la lista de dispositivos de red con la que tiene permitido comunicarse el dispositivo de cliente (121)”. Sin embargo, D1 está limitado a divulgar el acceso que se determina en base a las credenciales de un usuario del dispositivo invitado. “Las credenciales de inicio de sesión pueden indicar una identidad del usuario del dispositivo invitado 204 y, por lo tanto, el

nivel de acceso... que el usuario debería tener en el control remoto del dispositivo” (véase párrafo [0024] de D1). Determinar el acceso basado en las credenciales de un usuario del dispositivo invitado ejemplifica que D1 no revela nada de forma remotamente cercano de un dispositivo cliente que tiene acceso a un dispositivo de red dentro de una red privada, como se requiere en la reivindicación 1.

Sin embargo, D1 no divulga *"...implementa una puerta de enlace (100) en una red privada (140), una solicitud de un dispositivo de cliente (121) para un túnel de red entre el dispositivo de cliente (121) y un dispositivo de red (141) en la red privada (140) ... verificar, por el sistema informático, que el dispositivo de red (141) en la red privada (140) sea parte de la lista de dispositivos de red con la que tiene permitido comunicarse el dispositivo de cliente (121); y al verificar que el dispositivo de red (141) en la red privada (140) es parte de la lista de dispositivos de red con la que tiene permitido comunicarse el dispositivo de cliente (121), establecer, por el sistema informático, el túnel de red entre el dispositivo de cliente (121) y el dispositivo de red en la red privada a través de la puerta de enlace (100)"* como se menciona en la reivindicación independiente 1 enmendada actualmente.

Del mismo modo, D2 tampoco cumple con el requisito de “Verificar... que el dispositivo de red (141) en la red privada (140) sea parte de la lista de dispositivos de red con la que tiene permitido comunicarse el dispositivo de cliente (121)”. Este documento se refiere a un “nivel de confianza para un usuario” (véase párrafo [0160]) y “relaciona los niveles de confianza ordenados con los algoritmos criptográficos ordenados” (véase párrafo [0166]). De nuevo, esto es completamente diferente a un dispositivo cliente que tiene acceso a un dispositivo de red en una red privada, basado en una lista de dispositivos de red en la red privada con la que el dispositivo cliente puede comunicarse.

De forma similar, D3 no describe estos elementos de las presentes reivindicaciones. El examinador cita los párrafos [0043] y [0063] de este documento sin hacer un adecuado análisis, pero el enfoque de D3 está en “reglas de acceso a la red 124” que “pueden ser en apoyo de las políticas de acceso 102 a la red de una instalación empresarial, tales como denegar el acceso a ciertos tipos de sitios web 158” (véase párrafo [0043]). Esto no aborda el control de acceso a un dispositivo de red en una red privada o proporciona una lista de dispositivos de red en la red privada con la que el dispositivo cliente puede comunicarse.

Las distinciones también están presentes entre los requisitos de la reivindicación 1 y D3. D3 no revela: “Verificar... que el dispositivo de red (141) en la red privada (140) sea parte de la lista de dispositivos de red con la que tiene permitido comunicarse el dispositivo de

cliente (121)”. Más bien, D3 está limitado a divulgar el funcionamiento del software de gestión después de que un usuario inicia sesión en una red remota y antes de que el usuario pueda realizar otras funciones en la red remota. La información recibida del usuario para autenticar al usuario a la red remota también se puede usar para autenticar al usuario al software de administración, eliminando la necesidad de que el usuario se autentique nuevamente al software de administración después de autenticarse en la red remota. El sistema informático del cliente mantiene una lista de redes de terceros de confianza, y el método y el aparato solo permiten al usuario conectarse a redes de terceros en la lista de confianza, lo que elimina la necesidad de que los usuarios remotos pasen a través de la red corporativa. De nuevo, esto es completamente diferente a un dispositivo cliente que tiene acceso a un dispositivo de red en una red privada, basado en una lista de dispositivos de red en la red privada con la que el dispositivo cliente puede comunicarse, como se requiere en la reivindicación 1.

Las nuevas reivindicaciones independientes 14 y 15 se distinguen de la técnica anterior citadas como D1, D2 y D3, por las mismas razones identificadas anteriormente para la reivindicación independiente 1.

Las presentes reivindicaciones proporcionan así un enfoque fundamentalmente distinto a los descritos en el arte citado. Ventajosamente, un enfoque en una puerta de enlace a un dispositivo de red en una red privada se puede formar basada en una lista de dispositivos de red a los que un dispositivo cliente se le proporciona acceso. Un problema técnico objetivo derivado de estos efectos se puede formular como la forma de proporcionar una implementación de puerta de enlace mejorada. Una persona experta en la técnica que enfrenta este problema comenzando con D1 o cualquier otra de las referencias citadas no encontraría enseñanza que los conduzca a las características distintivas de las presentes reivindicaciones.

Las presentes reivindicaciones son, por lo tanto, novedosas e inventivas sobre la técnica citada.

Para llegar a la invención reivindicada basada en cualquiera de los documentos citados, tomados solos o en combinación, una persona experta tendría que modificar drásticamente las soluciones citadas, lo que es imposible sin implicar una actividad inventiva.

Por lo tanto, los documentos citados D1, D2 y D3, solos o en combinación, no divulgan el objeto de las reivindicaciones independientes y no proporcionan a un experto en la

materia la orientación para la implementación de la solución técnica reivindicada en la presente solicitud.

En consecuencia, los documentos de la técnica anterior citados no pueden hacer obvio el objeto reivindicado. Por lo tanto, la invención reivindicada se basa en una etapa inventiva sobre los documentos de la técnica anterior citados.

Así las cosas, es claro que existe por lo menos una diferencia entre la presente invención y los documentos D1, D2 y D3, ajustándose de este modo a las disposiciones del artículo 16 de la Decisión 486 y cumpliendo con el principio de novedad absoluta, razón por la cual dichas reivindicaciones independientes 1, 14 y 15, se considera como novedosa a la luz de las anterioridades D1, D2 y D3.

De acuerdo con lo definido en los párrafos anteriores, queda claro que la combinación de los documentos D1 y D2 y/o D1 y D3 no llevaría a obtener la presente invención como se encuentra definida en las reivindicaciones independientes 1, 14 y 15, ya que dichas divulgaciones son insuficientes y la única forma de llegar a la presente invención es por medio de un análisis de tipo retrospectivo o "hindsight", el cual es totalmente inaceptable y no se puede aplicar.

De esta forma, se demuestra que las nuevas reivindicaciones 1 a 15 cumplen con el requisito de nivel inventivo según los lineamientos del artículo 18 de la Decisión 486/00.

5. Conclusión

Con las modificaciones introducidas y los argumentos presentados puede concluirse que:

- i) La presente solicitud es clara, concisa y está debidamente soportada en la descripción, cumpliendo con los requerimientos del Artículo 30 de la Decisión 486; y
- ii) Las reivindicaciones actuales son patentables sobre D1, D2 y 32, cumpliendo así con los requerimientos de los Artículos 16 y 18 de la Decisión 486.

En consecuencia, se solicita atentamente otorgar el privilegio de patente solicitado, toda vez que esta solicitud cumple con los requerimientos de la Decisión 486.

Habiendo atendido cabalmente las objeciones presentadas por ese despacho, atentamente solicitamos se conceda el privilegio de patente de invención a la solicitud en

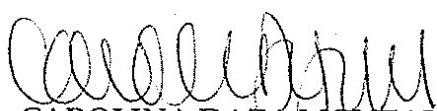
estudio o si el señor examinador considera que subsisten razones para objetar la presente invención, rogamos expedir otro examen de fondo con los debidos motivos y razones que sustenten su objeción con el fin de que nuestro mandante tenga la posibilidad de exponer sus argumentos con base en la interpretación de los artículos 45 de la Decisión 486 -el cual otorga la facultad al examinador para emitir los exámenes de fondo- y 42 del Código de Procedimiento Administrativo y de lo Contencioso Administrativo que señala que: *“Habiéndose dado oportunidad a los interesados para expresar sus opiniones, y con base en las pruebas e informes disponibles, se tomará la decisión, que será motivada. La decisión resolverá todas las peticiones que hayan sido oportunamente planteadas dentro de la actuación por el peticionario y por los terceros reconocidos”*, (el subrayado es nuestro).

Finalmente, solicitamos a ese Despacho pronunciarse en relación con todos los argumentos presentados en este memorial dando estricta aplicación al principio del debido proceso consagrado en el artículo 29 de la Constitución Nacional.

6. Anexos

- Nuevo capítulo reivindicatorio que incluye 15 reivindicaciones.
- Nuevo capítulo Descriptivo Modificado.
- Recibo de pago por concepto de examen de patentabilidad.

Señor Director,



CAROLINA DAZA MONTALVO

C.C. 66.783.790 de Palmira Valle

TP-141563 CSJ

notificaciones@clarkemodet.com.co

REIVINDICACIONES

1. Un método implementado por computadora caracterizado porque comprende: recibir, por un sistema informático que implementa una puerta de enlace (100) en una red privada (140), una solicitud de un dispositivo de cliente (121) para un túnel de red entre el dispositivo de cliente (121) y un dispositivo de red (141) en la red privada (140);

autenticar el dispositivo de cliente (121) por el sistema informático;

al autenticar el dispositivo cliente (121), recibir, de un servidor de autenticación (160) en comunicación con el sistema informático, una lista de accesos de cliente que incluye una lista de dispositivos de red con la que tiene permitido comunicarse el dispositivo de cliente (121);

al recibir la lista de accesos de cliente, verificar, por el sistema informático, que el dispositivo de red (141) en la red privada (140) sea parte de la lista de dispositivos de red con la que tiene permitido comunicarse el dispositivo de cliente (121); y

al verificar que el dispositivo de red (141) en la red privada (140) es parte de la lista de dispositivos de red con la que tiene permitido comunicarse el dispositivo de cliente (121), establecer, por el sistema informático, el túnel de red entre el dispositivo de cliente (121) y el dispositivo de red en la red privada a través de la puerta de enlace (100).

2. El método de conformidad con la reivindicación 1, caracterizado porque el dispositivo de red (141) en la red privada (140) incluye un servidor de aplicaciones que proporciona un servicio, y en donde el servidor de aplicaciones (141) incluye uno o más de:

un servidor de correo que proporciona un servicio de correo;

un servidor de archivos que proporciona un almacén de datos conectado a red; y

un servidor web que proporciona servicios de alojamiento.

3. El método de conformidad con la reivindicación 1, caracterizado porque el dispositivo de red (141) en la red privada incluye uno o más de un enrutador y un conmutador que proporciona acceso de administrador.

4. El método de conformidad con la reivindicación 1, caracterizado porque el sistema informático además implementa un cortafuegos (102) para bloquear de manera selectiva y permitir tráfico de red entre el dispositivo de cliente (121) y el dispositivo de red (141) en la red privada (140), y en donde el cortafuegos (102) bloquea todo el tráfico de red entre el dispositivo de cliente (121) y el dispositivo de red (141) en la red privada (140) por defecto.

5. El método de conformidad con la reivindicación 4, caracterizado además porque comprende:

obtener, por el sistema informático, una regla de cortafuegos para permitir el acceso de red entre el dispositivo de cliente (121) y el dispositivo de red (141) en la red privada (140); y

configurar el cortafuegos basándose en la regla de cortafuegos;

en donde la regla de cortafuegos se incluye en la lista de accesos de cliente.

6. El método de conformidad con la reivindicación 1, caracterizado porque establecer el túnel de red entre el dispositivo de cliente (121) y el dispositivo de red (141) en la red privada incluye establecer una red privada virtual.

7. El método de conformidad con la reivindicación 1, caracterizado porque la lista

de accesos de cliente es legible, pero no alterable, por el cliente.

8. El método de conformidad con la reivindicación 1, caracterizado porque autenticar el dispositivo de cliente (121) incluye verificar una firma digital en la lista de accesos de cliente mediante una clave de firma compartida entre la puerta de enlace (100) y el servidor de autenticación (160).

9. El método de conformidad con la reivindicación 1, caracterizado además porque comprende recibir, por el sistema informático del servidor de autenticación (160), una lista de túneles de cliente que incluye información para establecer el túnel de conexión a red, en donde la lista de túneles de cliente sólo se recibe del servidor de autenticación (160) en respuesta a una autenticación exitosa del dispositivo de cliente, y no se recibe de otra manera.

10. El método de conformidad con la reivindicación 9, caracterizado porque la lista de túneles de cliente incluye una dirección de protocolo de Internet de destino y un número de puerto de destino de la puerta de enlace.

11. El método de conformidad con la reivindicación 1, caracterizado porque la lista de accesos de cliente incluye una primera selección de dispositivos de red y una segunda selección de dispositivos de red, la segunda selección de dispositivos de red tiene requerimientos de autenticación mejorados con respecto a la primera selección de dispositivos de red, y en donde los requerimientos de autenticación mejorados incluyen un requerimiento seleccionado del grupo que consiste de:

un requerimiento de que todos los parches necesitan aplicarse a un sistema operativo en el cliente;

un requerimiento de que un escáner de virus actualizado debe ejecutarse en el cliente; y

un requerimiento de que el cliente no está intentando tener acceso al dispositivo de red en la red privada mediante una red inalámbrica pública.

12. El método de conformidad con la reivindicación 11, caracterizado porque los requerimientos de autenticación mejorados incluyen un requerimiento de que un usuario del dispositivo de cliente proporcione una credencial de autenticación seleccionada del grupo que consiste de:

un escaneo de huella digital;

un escaneo del iris; y

una clave generada por un generador de claves externo.

13. El método de conformidad con la reivindicación 1, caracterizado además porque comprende:

recibir, por el sistema informático, información de estado de cliente del cliente; y

romper el túnel de red en respuesta a una no recepción de la información de estado de cliente del cliente en un intervalo de tiempo regular o en respuesta a la información de estado de cliente que no corresponde con requerimientos predefinidos para el cliente.

14. Un medio legible por computadora no transitorio caracterizado porque almacena instrucciones que, cuando se ejecutan, provocan que un sistema informático que implementa una puerta de enlace (100) a una red privada (140):

reciba una solicitud de un dispositivo de cliente (121) para un túnel de red entre el dispositivo de cliente y un dispositivo de red (141) en la red privada (140);

autenticar el dispositivo de cliente (121);

al autenticar el dispositivo cliente (121), reciba, de un servidor de autenticación (160) en comunicación con el sistema informático, una lista de accesos de cliente que incluye una lista de dispositivos de red con la que tiene permitido comunicarse el dispositivo de cliente (121);

al recibir la lista de accesos de cliente, verifique que el dispositivo de red (141) en la red privada (140) sea parte de la lista de dispositivos de red con la que tiene permitido comunicarse el dispositivo de cliente (121); y

al verificar que el dispositivo de red (141) en la red privada (140) es parte de la lista de dispositivos de red con la que tiene permitido comunicarse el dispositivo de cliente (121), establezca el túnel de red entre el dispositivo de cliente (121) y el dispositivo de red (141) en la red privada (140) a través de la puerta de enlace (100).

15. Un sistema informático que implementa una puerta de enlace, el sistema informático caracterizado porque comprende:

un procesador; y

una memoria no transitoria en comunicación con el procesador y que almacena instrucciones que, cuando se ejecutan por el procesador, provocan que el sistema informático:

reciba una solicitud de un dispositivo de cliente (121) para un túnel de red entre el dispositivo de cliente (121) y un dispositivo de red (141) en la red privada (140);

autentique el dispositivo de cliente (121);

al autenticar el dispositivo cliente (121), reciba, de un servidor de autenticación (160) en comunicación con el sistema informático, una lista de accesos de cliente que incluye una lista de dispositivos de red con la que tiene permitido comunicarse el dispositivo de cliente (121);

al recibir la lista de accesos de cliente, verifique que el dispositivo de red (141) en

la red privada (140) sea parte de la lista de dispositivos de red con la que tiene permitido comunicarse el dispositivo de cliente (121); y

al verificar que el dispositivo de red (141) en la red privada (140) es parte de la lista de dispositivos de red con la que tiene permitido comunicarse el dispositivo de cliente (121), establezca el túnel de red entre el dispositivo de cliente (121) y el dispositivo de red (141) en la red privada (140) a través de la puerta de enlace (100).

SISTEMAS Y MÉTODOS PARA PROTEGER DISPOSITIVOS DE RED

ANTECEDENTES DE LA INVENCION

En un modelo de red de cliente-servidor, empresas o
5 proveedores de servicios típicamente ofrecen servicios y/o
aplicaciones a computadoras de cliente y a otros servicios
sobre una red de computadoras. Servidores y servicios
asociados pueden incluir, por ejemplo, servidores de correo,
servidores de archivos, servicios de Gestión de Relaciones de
10 Cliente o de CRM, servicios de Planificación de Recursos
Empresariales o de ERP, servicios de gestión de documentos, y
similares.

Por una parte, la seguridad necesita garantizarse al
restringir el acceso a estos servicios a usuarios y clientes
15 de confianza solamente. Por otra parte, los usuarios de
confianza necesitan acceso a los servicios de una manera
fácil y directa. De preferencia, puede llegarse a los
servicios desde cualquier lugar en cualquier momento. Con la
política de "Trae tu propio dispositivo" (o "BYOD") se
20 encuentra más y más aceptación en empresas, también se debe
llegar a los servicios desde "cualquier cosa", es decir,
desde cualquier dispositivo propiedad de un usuario de
confianza como por ejemplo, una computadora tipo Tablet, una
computadora tipo laptop, su computadora en casa o un teléfono

inteligente.

Varios procedimientos convencionales existen para intentar evitar acceso no autorizado a tales servidores de aplicaciones o a los servicios o aplicaciones atendidos por estos servidores de aplicaciones. Por ejemplo, poner servidores de aplicaciones dentro de una red privada es en sí una medida de seguridad ya que aísla la red de las empresas, la Red de Área Local (o "LAN") de la Internet y otras redes públicas externas. Los dispositivos, y de esta manera los servicios, dentro de la red privada, no son visibles desde la red pública. El contenido del tráfico en la red pública, y la forma en la cual el tráfico puede recorrer los límites de red de la empresa, pueden regularse y monitorearse al utilizar Traducción de Direcciones de Red (NAT), reglas del cortafuegos y proxies en los dispositivos de puerta de enlace que separan la WAN de la red privada de la empresa. Las redes privadas además pueden subdividirse física o virtualmente por ejemplo, por LANs Virtuales con el fin de separar adicionalmente servidores de aplicaciones del acceso potencial no autorizado por clientes dentro de la red privada de la empresa.

La seguridad de nivel de red puede ejecutarse en una base de usuario por usuario o de cliente por cliente, tal como al configurar el cortafuegos de un cliente para sólo

tener acceso (por defecto) a un servidor de autenticación. Cuando el cliente tiene autorización, se abre el cortafuegos del cliente y todos los dispositivos de red se configuran para dejar pasar el tráfico de red del cliente a los
5 servidores de aplicaciones a los que se le ha concedido el acceso.

La seguridad de nivel de red en un nivel de cliente o de usuario también puede intentarse por un controlador que genera derechos de acceso para usuarios basándose en perfiles
10 de identidad y perfiles de funcionamiento. El controlador entonces configura un dispositivo de protección por lo que proporciona acceso de red a un conjunto de servidores.

La aplicación de seguridad de nivel de red en un ordenador central de aceptación puede intentarse al
15 configurar el ordenador central por un controlador. Cuando un ordenador central de inicio tiene acceso autorizado a un ordenador central de aceptación, el controlador configura el ordenador central de aceptación para que acepte las conexiones de red del ordenador central de inicio.

20 La seguridad dentro de una red privada además puede ejecutarse por la seguridad de nivel de aplicación donde el usuario o clientes sólo pueden tener acceso a los servicios en los servidores después de la autenticación. En tal caso, un cliente puede encontrar el servidor de aplicaciones dentro

de la red, por ejemplo, por su dirección de red de IP y puede encontrar el servicio que se ejecuta en el servidor de aplicaciones por su número de puerto de TCP o UDP, pero el servicio o aplicación en sí puede rechazar al cliente o

5 usuario basándose en las credenciales de autenticación. Tal autenticación puede manejarse localmente por los servicios individuales o de manera central por un servidor de autenticación. Los servicios entonces comprueban las credenciales de autenticación con tal servidor de

10 autenticación antes de conceder acceso a un usuario y/o cliente a un cierto servicio.

El acceso a una red privada de una empresa puede establecerse por una Red Privada Virtual o VPN donde un túnel en red asegurado se configura entre un dispositivo de cliente

15 y la red privada. La configuración de tal túnel sólo se concede por autenticación con un servidor de VPN. Diferentes esquemas de autorización existen para garantizar que sólo usuarios y/o clientes de confianza puedan unirse a una VPN.

20 Otra solución para proporcionar acceso a servicios en la red privada de una empresa es al abrir un acceso exterior a algunos servicios. Por ejemplo, un servidor de correo electrónico puede permitir conexiones desde el exterior de modo que usuarios puedan comprobar su correo electrónico

cuando no se encuentren en la empresa. Estos servicios algunas veces se restringen sólo al proporcionar acceso a través de una interfaz específica tal como, por ejemplo, a través del sitio web de la empresa de manera que el cliente
5 no tiene acceso de red físico al servidor que ejecuta el servicio sino sólo a un servidor web que proporciona un subconjunto de los servicios.

En autenticación basada en riesgo, el acceso a servicios no sólo se concede basándose en identificación del
10 usuario y/o cliente por credenciales de autenticación, sino también basándose en métricas adicionales con el fin de derivar un nivel de confianza adecuado para el nivel de riesgo. Tales métricas por ejemplo, son: la ubicación del usuario, el tipo de cliente, el sistema operativo, si todos
15 los parches de seguridad se han instalado, el historial de inicio de sesión del usuario, etc. De esta manera, un usuario que inicia sesión por VPN puede tener restricción de servicios de los que no tendría restricción al iniciar sesión desde dentro de la red privada. O un usuario que inicia
20 sesión desde dentro de la red privada con su propio dispositivo puede tener algunos servicios rechazados.

La solicitud de patente de los Estados Unidos US2014/282914 divulga transportar datos de aplicaciones a través de un túnel de comunicaciones entre un dispositivo

host y un dispositivo invitado. US2008/028436 divulga un filtro de acceso escalable para uso en una red privada virtual. US2010/205657 revela comunicaciones informáticas protegidas. US 2007/1010405 divulga un sistema y método
5 diseñados para asegurar que una conexión de red privada virtual cumpla con políticas de seguridad de red.

BREVE DESCRIPCIÓN DE LA INVENCION

Modalidades de la presente descripción ayudan a proteger a
10 los dispositivos de red contra acceso no autorizado. Entre otras cosas, las modalidades de la descripción permiten completo acceso a servidores de aplicaciones y otros dispositivos de red que un cliente tiene acceso permitido, mientras que evita todo el acceso (o incluso conocimiento) de
15 los dispositivos de red que el cliente no tiene acceso permitido.

Un método implementado por computadora de acuerdo con una modalidad de la presente descripción incluye: recibir, por un sistema informático que implementa una puerta de
20 enlace a una red privada, una solicitud de un dispositivo de cliente para un túnel de red entre el dispositivo de cliente y un dispositivo de red en la red privada; autenticar al dispositivo de cliente por el sistema informático; recibir, de un servidor de autenticación en comunicación con el

sistema informático, una lista de accesos de cliente que incluye una lista de dispositivos de red con la que tiene permiso de comunicarse el dispositivo de cliente; verificar, por el sistema informático, que el dispositivo de red en la red privada es parte de la lista de dispositivos de red con la que tiene permiso de comunicarse el dispositivo de cliente; y establecer, por el sistema informático, el túnel de red entre el dispositivo de cliente y el dispositivo de red en la red privada a través de la puerta de enlace.

La presente descripción incluye varios métodos, aparatos (incluyendo sistemas informáticos) que realizan tales métodos, y medios legibles por computadora que contienen instrucciones que, cuando se ejecutan por sistemas de cómputo, provocan que los sistemas de cómputo realicen tales métodos.

Otras características serán aparentes a partir de los dibujos anexos y a partir de la descripción detallada que sigue.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

La Figura 1 es un sistema ejemplar para proteger dispositivos de red contra acceso de red por dispositivos de cliente no confiables de acuerdo con varios aspectos de la descripción.

La Figura 2 es un proceso ejemplar ejecutado por un

dispositivo de cliente para tener acceso de red a dispositivos de red protegidos de acuerdo con varios aspectos de la descripción.

La Figura 3 es un proceso ejemplar ejecutado por un
5 servidor de autenticación para proporcionar una lista de accesos y túneles de cliente a un dispositivo de cliente que permite a este cliente el acceso de red a dispositivos de red protegidos de acuerdo con varios aspectos de la descripción.

La Figura 4 es un proceso ejemplar ejecutado por una
10 puerta de enlace para proporcionar un acceso de cliente a dispositivos de red protegidos detrás de un cortafuegos en esta puerta de enlace de acuerdo con varios aspectos de la descripción.

La Figura 5 es un proceso ejemplar ejecutado por el
15 dispositivo de cliente para tener acceso de red a una segunda sección de dispositivos de red detrás de un cortafuegos de una puerta de enlace después de haber tenido acceso a una primera selección de estos dispositivos de red de acuerdo con varios aspectos de la descripción.

20 La Figura 6 ilustra un cambio ejemplar de un mensaje de mantener vivo entre un dispositivo de cliente y una puerta de enlace con el fin de mantener un túnel de red entre el cliente y el dispositivo de cliente de acuerdo con varios aspectos de la descripción.

La Figura 7 ilustra un sistema ejemplar para proteger dispositivos de red contra acceso de red por dispositivos de cliente no confiables de acuerdo con varios aspectos de la descripción.

5 La Figura 8 ilustra un sistema ejemplar para proteger dispositivos de red contra acceso de red por dispositivos de cliente no confiables de acuerdo con varios aspectos de la descripción.

10 La Figura 9 ilustra un sistema ejemplar para proteger dispositivos de red contra acceso de red por dispositivos de cliente no confiables donde la carga de conexión a red de una puerta de enlace se equilibra por una segunda puerta de enlace de acuerdo con varios aspectos de la descripción.

15 La Figura 10 ilustra un sistema de cómputo ejemplar de acuerdo con varios aspectos de la descripción.

DESCRIPCIÓN DETALLADA DE LA INVENCION

20 La materia objeto ahora se describirá más completamente en adelante con referencia a los dibujos anexos, los cuales forman parte de la misma, y los cuales muestran, a manera de ilustración, modalidades ejemplares específicas. La materia objeto, sin embargo, puede representarse en una variedad de formas diferentes y, por lo tanto, se pretende que la materia objeto cubierta o reclamada sea interpretada como no limitada

a ninguna de las modalidades ejemplares establecidas en la presente; se proporcionan modalidades ejemplares solamente para ser ilustrativas. De igual manera, se pretende un alcance razonablemente amplio para la materia objeto
5 reclamada o cubierta. Entre otras cosas, por ejemplo, la materia objeto puede representarse como métodos, dispositivos, componentes, o sistemas. Por consiguiente, las modalidades, por ejemplo, adoptan la forma de hardware, software, firmware o cualquier combinación de los mismos
10 (distinto a software en sí). Por lo tanto, no se pretende que la siguiente descripción detallada sea tomada en un sentido limitante.

En los dibujos anexos, algunas figuras pueden exagerarse para mostrar detalles de componentes particulares (y
15 cualquier tamaño, material y detalles similares mostrados en las figuras se pretenden para ser ilustrativos y no restrictivos). Por lo tanto, la estructura específica y detalles funcionales descritos en la presente no deberán interpretarse como limitantes, sino únicamente como una base
20 representativa para enseñar a alguien de experiencia en la técnica a emplear de forma variada las modalidades descritas.

La referencia en esta especificación a "la modalidad" o "una modalidad", significa que un rasgo, estructura o característica particular descrita junto con la modalidad se

incluye en al menos una modalidad de la descripción. Las apariciones de la frase "en una modalidad" en varios lugares en la especificación no necesariamente todas se refieren a la misma modalidad, ni son modalidades separadas o alternativas
5 mutuamente exclusivas de otras modalidades. Por otra parte, varias características se describen las cuales pueden mostrarse por algunas modalidades y no por otras. De manera similar, varios requerimientos se describen los cuales pueden ser requerimientos para algunas modalidades pero no para
10 otras modalidades.

Cualquier combinación y/o subconjunto de elementos de los métodos representados en la presente pueden combinarse entre sí, realizarse o no realizarse de manera selectiva basándose en varias condiciones, repetirse cualquier número
15 deseado de veces y practicarse en cualquier orden adecuado y junto con cualquier sistema, dispositivo, y/o proceso adecuado. Los métodos descritos y representados en la presente pueden implementarse en cualquier forma adecuada, tal como a través de software que opera en uno o más sistemas
20 informáticos. El software puede comprender instrucciones legibles por computadora almacenadas en un medio legible por computadora tangible (tal como la memoria de un sistema informático) y puede ejecutarse por uno o más procesadores para realizar los métodos de varias modalidades.

La Figura 1 ilustra un sistema ejemplar para la protección de dispositivos de red contra acceso de red no deseado de acuerdo con varios aspectos de la presente descripción. En este ejemplo, tres dispositivos de red (servidores de aplicaciones 141, 142 y 143) son parte de una red privada 140. El acceso a los servidores 141-143 se obtiene desde dentro de la red privada 140 mediante una dirección de red privada. En este contexto, el término "privada" se refiere al hecho de que los servidores de aplicaciones 141-143 no son globalmente enrutables. En otras palabras, los servidores de aplicaciones 141-143 no pueden dirigirse por su dirección de red privada desde el exterior de la red privada 140.

La red privada 140 y otros componentes en la Figura 1 pueden utilizar cualquier número y tipo de protocolos de comunicación, también denominados como el protocolo de Internet ("IP"), o como el Protocolo de Control de Transformación/Protocolo de Internet ("TCP/IP"). Por ejemplo, la red privada 140 puede tener márgenes de dirección como se establece por RFC 1918 para la Versión 4 de Protocolo de Internet o IPv4 y RFC 4193 para la Versión 6 de Protocolo de Internet 6 o IPv6.

Los servidores de aplicaciones 141-143 proporcionan servicios sobre la red 140 a otros dispositivos de cómputo.

Cualquier número y tipo de servidores de aplicaciones y servicios asociados pueden utilizarse junto con modalidades de la presente descripción, tal como servidores de correo, servidores de archivos, servicios de Gestión de Relaciones de
5 Cliente o de CRM, servicios de Planificación de Recursos Empresariales o de ERP, y/o servicios de gestión de documentos.

Una conexión de datos puede establecerse con cualquiera de los servidores de aplicaciones 141-143 al abrir una
10 extremo de comunicación con el servidor de aplicaciones respectivo en un puerto (o margen de puertos) asociado con el servicio. Los servidores de aplicaciones 141-143 pueden corresponder a dispositivos físicos con una interfaz de conexión a red física asociada con una dirección de red
15 privada. Alternativamente, los servidores de aplicaciones 141-143 también pueden corresponder a casos de servidores virtuales que se ejecutan en uno o más servidores físicos. Los casos de servidores virtuales cada uno puede tener una interfaz de red virtual con una dirección asociada de red
20 privada. Los casos de servidores virtuales pueden incluir, así como operar junto con, uno o más casos de espacio de usuario (también conocidos como contenedores de software, motores virtuales, servidores privados virtuales, y/o cárceles). Tales casos de espacio de usuario pueden

implementarse en cualquier forma adecuada, incluyendo mediante la herramienta de software DOCKER.

En el ejemplo mostrado en la Figura 1, la red privada 140 se separa de la red externa 180 por una puerta de enlace 100, por lo que permite tráfico de conexión a red entre la red externa 180 y la red privada 140 en una forma controlada. El sistema de la Figura 1 puede identificar clientes 121, 122 como "clientes de confianza" que tienen derechos de acceso a uno o más de los servidores de aplicaciones 141-143 dentro de la red privada 140 con el fin de utilizar los servicios que se ejecutan en los mismos. Los clientes 121, 122 pueden ser, o incluir, hardware físico y/o componentes virtuales. Por ejemplo, un cliente 121, 122 puede incluir un sistema operativo virtual que se ejecuta en un dispositivo físico, tal como un dispositivo móvil. El sistema también puede conceder acceso de red a una selección de servidores de aplicaciones 141-143 con la cual los clientes 121, 122, tienen acceso permitido y rechazar acceso de red a cualquier servidor de aplicaciones que los clientes 121, 122 no tienen acceso permitido.

Para controlar el acceso por los clientes 121, 122 a los servidores de aplicaciones 141-143, la puerta de enlace 100 incluye un módulo de túnel 101 para establecer túneles de conexión a red con la solicitud por los clientes 121, 122 en

la red externa 180. En el ejemplo mostrado en la Figura 1, se establecen túneles de conexión a red 181, 182 entre el módulo de túnel 101 y los clientes 121, 122 respectivamente, por lo que se extiende la red privada 140 a los clientes 121, 122.

5 En algunas modalidades, una red privada virtual (o "VPN") se establece a través de túneles 181, 182. De esta manera, un cliente 121, 122, aunque dentro de la red 180, se proporciona con una dirección de red privada en el margen de la red privada 140, y de este modo puede acceder potencialmente a
10 todos los servidores de aplicaciones 141-143 por su dirección respectiva de red privada (siempre y cuando tenga acceso permitido, como se discute en mayor detalle a continuación).

Se establece un túnel con la solicitud de un cliente 121, 122, por lo que se proporciona información de
15 autenticación de túnel al módulo de túnel 101. Cualquier cantidad y tipo de información de autenticación puede utilizarse junto con modalidades de la presente descripción, tal como nombre de usuario y contraseña. La información de autenticación de túnel también puede (o alternativamente)
20 incluir biometría, autenticación de dos factores, y/u otros métodos criptográficos. Los datos que viajan en los túneles 181, 182 además pueden protegerse por encriptación, tal como de acuerdo con la Seguridad de Protocolo de Internet (o "protocolo de IPsec"), Seguridad de Capa de Transporte (o

"TLS") y/o Seguridad de Capa de Transporte de Datagrama (o "DTLS"). El módulo de autenticación de túnel 105 verifica la información de autenticación de túnel y, si la autenticación tiene éxito, el túnel de conexión a red se establece con el cliente respectivo.

La puerta de enlace 100 en la Figura 1 incluye un cortafuegos 102 para controlar el tráfico de red entre los clientes 121, 122 y los servidores de aplicaciones 141-143 después de que se han establecido los túneles respectivos 181, 182. El cortafuegos 102 puede controlar tal tráfico de acuerdo con las reglas del cortafuegos proporcionadas por el módulo de configuración del cortafuegos 103 o de otra fuente. En algunas modalidades, el módulo de configuración del cortafuegos 103 obtiene las reglas del cortafuegos de las listas de accesos de cliente recibidas de los clientes respectivos 121, 122 los cuales, a su vez, reciben la lista de accesos de cliente del servidor de autenticación 160.

Entre otras cosas, las reglas del cortafuegos permiten a un cliente 121, 122 establecer y mantener conexiones de red con los servidores de aplicaciones 141, 142 y 143. La selección de servidores de aplicaciones 141-143 de la cual puede acceder el cliente 121, 122 puede determinarse de la lista de accesos de cliente de la cual también pueden obtenerse las reglas del cortafuegos. Las reglas del

cortafuegos pueden incluir cualquier información deseada. En algunas modalidades, por ejemplo, las reglas del cortafuegos incluyen fichas de derecho adquirido que definen la información a la que los clientes pueden tener acceso. Tales

5 fichas de derecho adquirido pueden utilizarse para configurar un cortafuegos no sólo para conceder/rechazar acceso de tráfico de red, sino también acceso a varios archivos (por ejemplo, que se clasifican (contienen metadatos) como altamente confidenciales).

10 El cortafuegos 102 puede ser, o incluir, cualquier número y tipo de sistema, dispositivo, componente de hardware, y/o componente de software. Por ejemplo, el cortafuegos 102 puede implementarse como cortafuegos distribuido que incluye múltiples componentes de hardware y/o

15 software. En algunas modalidades, el cortafuegos 102 bloquea todo el tráfico de los clientes 121, 122 sobre los túneles seguros 180, 181 por defecto, pero pueden configurarse para permitir tráfico en respuesta a una regla de cortafuegos. Por ejemplo, si una lista de accesos de cliente indica que el

20 cliente 121 puede tener acceso al servidor de aplicaciones 141, el módulo de configuración del cortafuegos 103 obtiene la regla correspondiente y la activa en el cortafuegos 102. Después de la activación de la regla, el cortafuegos 102 ya no bloquea el tráfico de red en la red privada 140 entre el

cliente 121 y el servidor de aplicaciones 141.

El sistema de la Figura 1 incluye un servidor de autenticación 160, el cual a su vez incluye un módulo de autenticación 162 para autenticar clientes 121, 122 y
5 generar información de cliente. En el ejemplo mostrado en la Figura 1, con el fin de que un cliente 121, 122 tenga acceso a un servidor de aplicaciones 141-143 en la red privada 140, primero necesita autenticarse a sí mismo con el servidor de autenticación 160.

10 El servidor de autenticación 160 puede implementarse utilizando cualquier combinación deseada de componentes de hardware y software, y puede comunicarse con otros componentes de hardware y software en cualquier forma deseada. En el sistema ejemplar mostrado en la Figura 1, el
15 servidor de autenticación 160 no es parte de la red privada 140, pero es accesible por los clientes 121, 122 sobre la red 180. La información de autenticación proporcionada por los clientes 121, 122 identifica únicamente el cliente o al usuario del cliente, tal como al proporcionar un nombre de
20 usuario y contraseña (la cual puede verificarse por el módulo de autenticación 162).

Los clientes 121, 122 pueden autenticarse utilizando cualquier número y tipo de diferentes métodos de autenticación. Por ejemplo, además (o como alternativa) de

la autenticación por contraseña, la autenticación puede utilizar una autenticación basándose en el hardware del cliente 121, 122, tal como el historial de uso de los atributos de hardware y hardware de cliente del cliente. En una modalidad, tal información puede almacenarse en un registro en el dispositivo de cliente, por lo que la detección de movimiento del registro en una máquina diferente resulta en una falla de autenticación. El registro puede encriptarse y/o firmarse con clave para proporcionar integridad adicional. La autenticación también puede basarse en una ventana de tiempo, de manera que la autenticación se rechaza (o autenticación adicional requerida) si un cliente 121, 122 intenta autenticación fuera de una ventana de tiempo predeterminada.

La autenticación puede realizarse basándose en la información basada en ubicación, tal como basada en la dirección de protocolo de Internet (IP) del cliente 121, 122 o la información de posicionamiento global asociada con el cliente 121, 122. Por ejemplo, la ubicación física del cliente 121, 122 puede determinarse a partir de la información de posicionamiento global, una dirección de IP específica, o incluso el código de país de la dirección de IP de un cliente, y utilizarse para determinar si el cliente 121, 122 es un cliente de buena fe o un tercero (tal como un

hacker) que intenta hacerse pasar como el cliente. Direcciones de IP (individuales o márgenes basados en código de país, etc.) pueden estar en la lista negra o estar en la lista blanca basándose en historial previo (es decir, 5 intentos de hackeo, fallas de autenticación, etc.). De igual manera, información basada en ubicación utilizada para autenticación también puede derivarse de la o las redes físicas utilizadas por el cliente 121, 122 al intentar una conexión.

10 El módulo de autenticación 162 también puede recibir la información de contexto o de estado directamente de los clientes 121, 122. Cuando tal información se recibe directamente del cliente, y de este modo no puede verificarse por el servidor de autenticación, puede tratarse como 15 "información de contexto de cliente" no confiable. La información de contexto de cliente la cual puede incluirse en la información de cliente puede incluir información tal como: un nombre de ordenador central el cual puede tener la forma de un nombre de dominio completamente calificado (o "FQDN"), 20 por ejemplo, "host.domain.com"; una familia y un nombre de versión del sistema operativo que se ejecuta en el ordenador central; un nivel de parche indicativo para el sistema operativo al cual se han aplicado los parches; un estado de software anti-virus instalado en el cliente; y/o cuánto

tiempo el usuario del dispositivo de cliente ha iniciado sesión en el cliente.

El módulo de autenticación 162 también puede agregar "información de cliente de confianza" a la información de cliente, la cual puede incluir información tal como información de membresía de usuario indicativa de grupos de usuarios y departamentos a los que pertenece el usuario. La información de cliente de confianza puede proporcionarse por sistemas de directorio de usuarios utilizando los servicios de protocolo ligero de acceso a directorios ("LDAP") o de Directorio Activo ("AD"). La información de cliente de confianza también puede incluir información tal como información de historial sobre sesiones previas del cliente con el servidor de autenticación 160 (por ejemplo, una marca de tiempo del último inicio de sesión y una cantidad de intentos fallidos de inicio de sesión).

En el ejemplo mostrado en la Figura 1, el módulo de autenticación 162 comprende un motor de lista de clientes 163 y un motor de lista de túneles 165. Tras la autenticación exitosa por el módulo de autenticación 162, el motor de lista de túneles 165 genera una lista de túneles de cliente y el motor de lista de clientes 163 genera una lista de accesos de cliente basadas en la información de cliente proporcionada por el módulo de autenticación.

La lista de túneles de cliente puede incluir toda la información para que un cliente autenticado 121, 122 establezca el túnel respectivo 181, 182. La lista de túneles de cliente puede incluir, por ejemplo, la información de dirección de red (tal como la dirección de IP de destino y/o el número de puerto de destino de la puerta de enlace 100) con el fin de que el cliente 121, 122 inicie el establecimiento del túnel respectivo 181, 182 al solicitar la configuración de un túnel en la dirección de IP y el número de puerto especificado en la lista de túneles de cliente. La lista de túneles de cliente también puede incluir la información de autenticación de túnel con el fin de autenticar al cliente 121, 122 con el módulo de autenticación 105 en la puerta de enlace 100. La lista de túneles de cliente puede incluir, por ejemplo, fichas de red privada virtual (VPN) que contienen la información necesaria para conectar al cliente a varias puertas de enlace.

La información de autenticación de túnel generada por el motor de lista de túneles 165 puede ser dinámica (es decir, no conocida por el módulo de autenticación 105 de la puerta de enlace 100 con anticipación). En tales casos, el servidor de autenticación puede reenviar la información de autenticación de túnel a la puerta de enlace 100 por un enlace de comunicación 168 entre el servidor de

autenticación 160 y la puerta de enlace 100. El enlace de comunicación 168 de esta manera proporciona un canal entre la puerta de enlace 100 y el servidor de autenticación 160 que permite actualizaciones de configuración que se intercambian y permiten el acceso por un usuario o que la sesión sea revocada si el usuario y/o sesión se borra en el servidor de autenticación 160. Existe una variedad de razones por las que un usuario o sesión puede removerse, tal como: 1) la base de datos de servicio cambia y el administrador desea ejecutar el cambio en todos los usuarios; 2) un usuario cambia su método de autenticación; o 3) un usuario o cliente se prohíbe en el sistema. El enlace de comunicación 168 puede implementarse en cualquier forma deseada, tal como mediante un canal de protocolo seguro de transferencia de hipertexto (HTTPS) que sólo permite comunicación entre el servidor de autenticación 160 y una o más de una o puertas de enlace.

La lista de accesos de cliente identifica una selección de los servidores de aplicaciones 141-143 a los cuales tiene acceso concedido un cliente. En algunas modalidades, el motor de lista de clientes 163 genera las reglas del cortafuegos para el cortafuegos 102 e incluye estas reglas en la lista de accesos de cliente. Las reglas del cortafuegos entonces se extraen de la lista de accesos de cliente por el módulo de configuración del cortafuegos 103 en la puerta de enlace 100

y se aplican al cortafuegos 102. La lista de accesos de cliente además puede agregar condiciones a la información de dirección de los servidores de aplicaciones 141-143. Un ejemplo ilustrativo de una lista de accesos de cliente se muestra en la siguiente tabla.

Tabla 1: Lista de accesos de cliente con servidores de aplicaciones condicionales

Dirección de IP	Condición
10.0.0.1	Intervalo de Tiempo (09.00-17.00)
10.0.0.11	Dominio ("domain.com")
10.0.0.3	Prefijo de Cadena (nombre de usuario, "adm_")

La primera columna de la Tabla 1 especifica la dirección de IP del servidor de aplicaciones a la cual tiene acceso concedido de red el cliente. La segunda columna además especifica una condición que necesita cumplirse con el fin de tener acceso. La primera condición especifica un intervalo de tiempo específico durante el cual el cliente tiene acceso concedido al servidor de aplicaciones 10.0.0.1. La segunda condición especifica un dominio específico del cual la solicitud debe originarse (es decir, especifica el dominio del cual el cliente puede tener acceso a la aplicación). La segunda condición puede utilizarse, por ejemplo, por una

empresa para permitir sólo acceso desde su propio dominio (es decir, desde dentro de la red de la empresa). La tercera condición podría utilizarse para identificar un usuario o grupo específico, (tal como los administradores de una empresa), que son los únicos que deben poder acceder a un servidor de aplicaciones dado u otro dispositivo de red.

En el sistema ejemplar mostrado en la Figura 1, el servidor de autenticación 160 incluye un módulo de firma 164 para crear listas digitalmente firmadas, tales como una lista de accesos de cliente firmada y lista de túneles de cliente firmada. Las firmas digitales generadas por el módulo de firma 164 pueden verificarse por el módulo de verificación de firma 104 en la puerta de enlace 100 tras la recepción de la lista de accesos y túneles de cliente. La firma puede generarse y verificarse por una clave de firma compartida entre la puerta de enlace y el servidor de autenticación 160 de manera que la lista de accesos de cliente y la lista de túneles de cliente no es alterable por los clientes 121, 122 sin que la puerta de enlace 100 notifique al servidor de autenticación 160. En una modalidad ejemplar, se emplean X.509 certificados utilizando un mecanismo de clave privada/pública para verificar el certificado.

En algunas modalidades, si la puerta de enlace 100, mientras se intenta verificar la firma, determina que la

lista de accesos de cliente o la lista de túneles de cliente se cambió, la puerta de enlace 100 puede notificar al servidor de autenticación 160 de los cambios y/o romper el túnel de red con el cliente. El servidor de autenticación 5 160 puede utilizar tales notificaciones como parte de la "información de cliente de confianza" asociada con el cliente en interacciones futuras con el cliente. En algunas modalidades, la puerta de enlace 100 puede romper un túnel de conexión a red establecido 181, 182 por su propia voluntad 10 (por ejemplo, en respuesta a detectar un cambio en la lista de accesos de cliente o lista de túneles de cliente como se describe en lo anterior). Adicional o alternativamente, el servidor de autenticación 160 puede adaptarse para provocar que la puerta de enlace 100 rompa túneles de conexión a red 15 181, 182 establecidos al detectar un mensaje en la puerta de enlace 100 sobre el enlace de comunicación 168 que instruye al módulo de túnel 101 para romper un túnel de conexión a red y para remover las reglas del cortafuegos del cortafuegos que permiten el acceso de cliente respectivo a los servidores de 20 aplicaciones.

Las Figuras 2, 3 y 4 muestran procesos ejemplares que pueden ejecutarse por varios componentes que operan junto con modalidades de la presente descripción, incluyendo los componentes del sistema ejemplar mostrado en la Figura 1,

particularmente el cliente 121, 122, el servidor de autenticación 160 y la puerta de enlace 100, respectivamente. Los procesos descritos en la presente pueden realizarse (completamente o en parte) por cualquier otra
5 combinación de diferentes componentes de hardware y/o software.

Los procesos en las Figuras 2, 3, y 4 pueden implementarse en una variedad de contextos y situaciones, tales como donde los servidores de aplicaciones 141, 142 y
10 143 todos pertenecen a una empresa cuyo objetivo es proporcionar los servicios de los servidores de aplicaciones en una forma segura a los clientes de confianza 121, 122. En tales casos, un "cliente de confianza" es un dispositivo de cliente del cual el usuario o el dispositivo en sí se conocen
15 por la empresa y puede tener acceso proporcionado a uno o más de los servidores de aplicaciones. Cada cliente 121, 122 puede implementarse como cualquier combinación de hardware hardware y/o software de computadora que pueda acceder y utilizar un servicio hecho disponible por los servidores de
20 aplicaciones 141-143. Un cliente, por ejemplo, puede ser (o incluir) una computadora de escritorio, una computadora tipo laptop, un teléfono inteligente y/o una computadora tipo Tablet. El cliente también podría ser (o incluir) un servidor que, por ejemplo, utilice un certificado para autenticarse

a sí mismo. Los procesos en las Figuras 2, 3, y 4 ayudan a evitar que clientes 121, 122 accedan la red pública directamente, en lugar de sólo proporcionar acceso a través de la puerta de enlace, (tal como la puerta de enlace 100 en la Figura 1). Tales restricciones también pueden ejecutarse con respecto a los clientes que operan dentro de la red privada de la empresa. Para un ejemplo de tal escenario, con referencia nuevamente a la Figura 1, la red 180 y la red 140 podrían ser "redes privadas" separadas, pero la comunicación de red entre los clientes 121, 122 y los servidores de aplicaciones 141-143 aún se controla por la puerta de enlace 100.

La Figura 2 muestra un proceso ejemplar que puede ejecutarse por cualquiera de los clientes 121, 122 para acceder a uno o más servicios en los servidores de aplicaciones 141-143. El proceso en la Figura 2 puede implementarse en cualquier forma adecuada, tal como mediante una aplicación de software en el dispositivo de cliente que se ejecute automáticamente en segundo plano cuando el cliente se encuentre activo. La aplicación de software puede ejecutarse automáticamente en el tiempo de arranque del cliente, o puede iniciarse manualmente por el usuario u otro proceso que opera en el cliente. El cliente 121, 122 monitorea (201) el acceso de red de los dispositivos de

cliente a uno de los servidores de aplicaciones 141-143. La dirección de red de los servidores de aplicaciones 141-143 puede ser una opción de configuración en las aplicaciones de cliente utilizando los servicios de los servidores de aplicaciones. Por ejemplo, el servidor de aplicaciones puede ser (o incluir): un servidor de correo con la dirección de red y puertos configurados en la aplicación de cliente de correo; un servidor de archivos configurado con su dirección de red como un recurso compartido de red; un servicio de CRM y el cliente tiene una aplicación de cliente dedicada instalada para acceder al servicio de CRM; y/o un servicio web y el usuario especifica la dirección en la barra de direcciones de una aplicación de navegador.

El cliente puede detectar (202) que una aplicación de cliente trata de tener acceso a servidores de aplicaciones dentro de la red privada 140 basada en la dirección de red de destino. El cliente recupera (203) información de autenticación para enviar al servidor de autenticación 160. La recuperación de la información de autenticación puede realizarse automáticamente tal como al utilizar las credenciales de autenticación de un usuario enviado previamente para iniciar sesión. Alternativamente, la recuperación de la información de autenticación puede incluir solicitar al usuario que proporcione credenciales de

autenticación, tal como nombre de usuario y una contraseña. Alternativamente a las etapas 201-203 de la Figura 2, el cliente puede autenticarse directamente a si mismo con el servidor de autenticación 160 sin esperar que un acceso de red pruebe uno de los servidores de aplicaciones 141-143. Por ejemplo, el cliente puede autenticar con el servidor de autenticación 160 cuando el usuario del cliente inicia sesión en el cliente o cuando el cliente arranca.

La autenticación del cliente puede realizarse en cualquier forma deseada, tal como al utilizar credenciales de autenticación almacenadas, las credenciales de inicio de sesión del usuario y/o se solicitan credenciales de autenticación separadas del usuario. Cualquier número y tipo de proveedor de identidad también puede utilizarse junto con modalidades de esta descripción, incluyendo RSA, Oauth, certificados, Radius, SAML, y similares. Las credenciales de autenticación se utilizan para autenticar (204) al cliente 121, 122 con el servidor de autenticación 160. En respuesta, el cliente recibe (205) la lista de túneles de cliente y la lista de accesos de cliente del servidor de autenticación 160.

El cliente 121, 122 establece (206) el túnel de red 181, 182 con la puerta de enlace 100, por ejemplo, al recuperar la dirección de red de la puerta de enlace 100 de la lista de

túneles de cliente y enviar una solicitud a la puerta de enlace 100 para establecer el túnel. Tras establecer (206) el túnel, el cliente puede proporcionar la lista de túneles de cliente a la puerta de enlace como una autenticación. La
5 lista de túneles de cliente porta la firma del servidor de autenticación 160, de la cual la puerta de enlace 100 puede verificar que el cliente es de confianza y establece el túnel sin intercambio adicional de credenciales de autenticación. Después de que el túnel de red se establece, la red privada
10 140 se extiende hasta el cliente a través del túnel, pero el cliente aún puede no ser capaz de acceder a ninguno de los servidores de aplicaciones 141-143, ya que el acceso de red a los servidores puede bloquearse por el cortafuegos 102 de la puerta de enlace 100.

15 El cliente envía (207) la lista de accesos de cliente recibida desde el servidor de autenticación 160 hasta la puerta de enlace 100 y registra (211) a qué servidores de aplicaciones puede tener acceso el cliente desde la lista de accesos de cliente. El cliente también puede señalar o
20 visualizar los servidores de aplicaciones accesibles o servicios al usuario del dispositivo de cliente. Suponiendo una autenticación exitosa, la puerta de enlace 100 proporciona al cliente acceso de red a todos los servidores de aplicaciones o servicios en los servidores de aplicaciones

que se listan en la lista de accesos de cliente.

La Figura 3 es un proceso ejemplar para proporcionar listas de accesos y túneles de cliente a los clientes que puedan ejecutarse por un servidor de autenticación, tal como el servidor de autenticación 160 en la Figura 1. En este proceso ejemplar, el servidor de autenticación recibe una solicitud de un cliente respectivo (301). En la solicitud, el cliente proporciona información de autenticación para autenticación con el servidor de autenticación tal como en la etapa 204 de la Figura 2. El servidor de autenticación intenta identificar (302) al cliente. Si el cliente no se conoce por el servidor de autenticación y de este modo no es confiable, el servidor detiene el flujo (303). Si el cliente se conoce, el servidor de autenticación recupera (304) la información de cliente de confianza y la agrega a la información de cliente. La información de contexto de cliente recibida con la información de autenticación en la etapa 301 también puede agregarse a la información de cliente.

El módulo de autenticación identifica (310) una selección de servidores de aplicaciones a la que tiene acceso permitido el cliente. La selección de servidores de aplicaciones, junto con la información de cliente, entonces puede reenviarse al motor de lista de clientes 163 y al motor

de lista de túneles 165 del servidor de autenticación 160. El motor de lista de túneles 165 genera (305) la lista de túneles basándose en la información de cliente por ejemplo, al proporcionar la dirección de IP de la puerta de enlace 100
5 junto con credenciales de autenticación después de configurar el túnel de conexión a red con la puerta de enlace 100. La lista de túneles de cliente se firma (306) por el motor de firma 164. El servidor de autenticación genera (307) la lista de accesos de cliente basada en la selección
10 de servidores que tiene acceso permitido el cliente. Basándose en la información de cliente, restricciones condicionales adicionales pueden agregarse a la lista de accesos de cliente. Después, también la lista de accesos de cliente se firma 308. El servidor de autenticación entonces
15 envía 309 el acceso de cliente y la lista de túneles al cliente.

La Figura 4 muestra un proceso ejemplar para proporcionar acceso de red a un cliente que puede ejecutarse por una puerta de enlace que opera junto con modalidades de
20 la presente descripción, tal como una puerta de enlace 100 en la Figura 1. En este proceso ejemplar, la puerta de enlace 101 recibe (401) una solicitud de un cliente 121 o 122 para configurar el túnel de conexión a red (por ejemplo, una conexión de VPN) con ese cliente. En respuesta, la puerta de

enlace solicita (402) credenciales de autenticación del cliente y recibe (403) las credenciales de autenticación en forma de la lista de túneles de cliente. Para autenticar al cliente, la puerta de enlace 100 verifica (404) la firma en la lista de túneles de cliente utilizando una clave de firma compartida con el servidor de autenticación 160. Si la firma es correcta y la lista de túneles de cliente no se modificó por el cliente, la puerta de enlace 100 establece (405) el túnel de conexión a red con el cliente, de este modo extendiendo la red privada 140 al cliente sobre el túnel. El cortafuegos de la puerta de enlace se configura adicionalmente para bloquear todo el acceso de red del cliente por defecto. La puerta de enlace recibe (406) la lista de accesos de cliente del cliente que se generó por el servidor de autenticación y verifica (407) la firma de esta lista de accesos de cliente. A partir de la lista de accesos de cliente, la puerta de enlace obtiene (408) la reglas del cortafuegos para permitir acceso de red a los servidores de aplicaciones listados en la lista de accesos de cliente (y las condiciones de tal éxito, que también se proporcionaron en la lista de accesos de cliente). La puerta de enlace activa (409) las reglas, por lo que permite que el cliente tenga acceso a la selección de servidores de aplicaciones listados en la lista de accesos de cliente.

En algunas modalidades, el servidor de autenticación puede agregar requerimientos de autenticación mejorada a la lista de accesos de cliente junto con una segunda selección de servidores de aplicaciones que pueden accederse tras cumplir con estos requerimientos de autenticación mejorada. Estos requerimientos mejorados pueden relacionarse con el mecanismo de autenticación en sí y pueden, por ejemplo, establecer que un mecanismo de autenticación más seguro (con respecto a la primera selección de servidores de aplicaciones) debe utilizarse. Por ejemplo, en lugar de suministrar una combinación de usuario/contraseña (la cual puede cumplir con los requerimientos de autenticación para el primer conjunto de servidores de aplicaciones), los requerimientos mejorados pueden especificar que se requiere una autenticación de dos factores para tener acceso al segundo conjunto de servidores de aplicaciones. Los requerimientos también pueden relacionarse con el contexto o la información de estado del cliente en sí. Cualesquier requerimientos deseados pueden utilizarse, tal como el requerimiento de: que todos los parches necesitan aplicarse a los clientes que operan el sistema con el fin de acceder a un cierto servidor de aplicaciones; que un escáner de virus debe ejecutarse y actualizarse para acceder a un cierto servidor de aplicaciones; y/o que un servidor de aplicaciones puede no

accederse desde una red inalámbrica pública.

Tras la autenticación con el servidor de autenticación, el servidor de autenticación 160 (por ejemplo, mediante el motor de lista de clientes 163) proporciona una lista firmada de accesos de cliente que comprende los requerimientos de autenticación mejorada junto con una segunda selección de servidores de aplicaciones que requieren tal autenticación mejorada. Cuando el cliente autentifica y cumple con los requerimientos de autenticación mejorada, el servidor de autenticación puede emitir una lista de accesos de cliente actualizada al cliente donde la segunda selección de servidores de aplicaciones se lista entre los servidores de aplicaciones a los que el cliente tiene acceso permitido. Múltiples niveles de requerimientos de autenticación mejorada (y conjuntos correspondientes de servidores de aplicaciones) pueden listarse en una lista de accesos de cliente.

La Figura 5 muestra un proceso ejemplar que puede ejecutarse por un cliente con el fin de obtener acceso de red a los servidores de aplicaciones con requerimientos de autenticación mejorada. En este proceso ejemplar, el cliente establece acceso de red (501) en una primera selección de servidores de aplicaciones en la red privada 140 listada en una primera lista de accesos de cliente, también

denominada en la presente como la "lista de accesos de cliente base". La etapa 501 además puede implementarse de acuerdo con el flujo presentado en la Figura 2 con la diferencia de que la lista de accesos de cliente base además
5 comprende una segunda selección de servidores de aplicación y requerimientos de autenticación mejoradas con el fin de obtener acceso de red en esta segunda selección.

El cliente monitorea (502) las aplicaciones que se ejecutan en el dispositivo de cliente y el acceso de red de
10 tales aplicaciones a en la red privada 140. Si una aplicación de cliente trata de conectarse a un servidor de aplicaciones el cual no es parte de la primera selección, el cliente comprueba (503) si el servidor de aplicaciones es parte de la segunda selección. Si no, el cliente no puede obtener acceso
15 a este servidor de aplicaciones y un usuario del cliente o la aplicación se le puede notificar del acceso denegado (504). Si el servidor de aplicaciones es parte de la segunda selección, el cliente inicia el proceso de autenticación mejorada con el servidor de autenticación (505), el cual
20 puede incluir solicitar que el usuario proporcione credenciales de autenticación mejorada tales como escaneo de huella digital, un escaneo de iris, información biométrica adicional sobre el usuario, y/o una clave generada por un generador de claves externo. El cliente también puede

solicitar que el usuario actualice el contexto y/o estado del dispositivo de cliente mismo. Por ejemplo, puede solicitarse al usuario que: conecte el cliente a una red alámbrica; que no conecte el cliente a través de una red inalámbrica pública; que instale los últimos parches del sistema operativo del cliente; que instale un escáner de virus; y/o que actualice la base de datos del escáner de virus.

Cuando el usuario cumple con éxito los requerimientos de autenticación mejorada (506) el cliente recibe (507) una segunda lista de accesos de cliente o actualizada del servidor de autenticación 160. Si la autenticación mejorada no tuvo éxito, el usuario o aplicación de software que requiere acceso de red se señala o alerta (504) de que la red de acceso se denegó. La lista de accesos de cliente actualizada lista la primera selección y la segunda selección de servidores de aplicaciones que el cliente puede acceder, y se envía (508) a la puerta de enlace 100, la cual configura su cortafuegos 102 por consiguiente. El cliente entonces puede señalar (509) a las aplicaciones de cliente y al usuario qué aplicaciones o servicios se permiten.

La Figura 6 representa un sistema ejemplar de acuerdo con varios aspectos de la presente descripción. En este sistema ejemplar, la puerta de enlace 600 incluye un módulo de mantener vivo 605. La puerta de enlace 600 se conecta al

túnel de conexión a red establecido 182 con el cliente 621, y el módulo de mantener vivo se configura para comprobar que el mensaje de mantener vivo se reciba a intervalos regulares del cliente 621. Si el mensaje de mantener vivo no se recibe a tiempo, el módulo de mantener vivo instruye al módulo de configuración del cortafuegos 103 a que borre las reglas del cortafuegos para el cliente 621 del cortafuegos 102, e instruye al módulo de túnel 101 a romper el túnel de conexión a red 182. El módulo de mantener vivo 605 además puede configurarse para comprobar si cierto estado predefinido o información de contexto sobre el cliente 621 se presenta en el mensaje de mantener vivo y cumple con ciertos requerimientos predefinidos. Tales requerimientos pueden incluir, por ejemplo, que el escáner de virus de cliente y/o cortafuegos debe encontrarse activo.

El cliente 621 puede llevar a cabo el proceso ilustrado por etapas 601-604 con el fin de enviar los mensajes de mantener vivo a la puerta de enlace 600. En la primera etapa 601, un túnel de conexión a red 182 a la puerta de enlace 600 se establece. El túnel de conexión a red 182 puede establecerse en cualquier forma deseada, incluyendo utilizar el proceso (o porciones de la misma) ilustrada en las Figuras 2 y 5. El cliente recolecta (602) el contexto requerido e información de estado y formatos en un mensaje de mantener

vivo. El mensaje de mantener vivo se envía (603) sobre el túnel de conexión a red 182 hasta el módulo de mantener vivo 605 de la puerta de enlace 600. Cuando el mensaje se envía, se activa un cronómetro (604) para hacer conteo regresivo a
5 partir de un intervalo de tiempo predefinido. Cuando el cronómetro termina, se realiza un nuevo ciclo de las etapas 602-604 con el fin de enviar el siguiente mensaje de mantener vivo.

La Figura 7 ilustra un sistema ejemplar para proteger
10 los servidores de aplicaciones 741 a 746 contra acceso no autorizado de acuerdo con varios aspectos de la presente descripción. En este ejemplo, los servidores de aplicaciones 741-746 son parte de las redes privadas 750, 751 y 752 protegidas por las puertas de enlace 700, 701 y 702,
15 respectivamente. Un cliente 721 puede autenticar con el servidor de autenticación 760 y por consiguiente obtener una lista de túneles de cliente y una lista de accesos de cliente. La lista de túneles de cliente comprende información necesaria para establecer un túnel de conexión a red con cada
20 una de las puertas de enlace 700-702 con el fin de extender todas las redes privadas 740-744 al cliente 721. La lista de túneles de cliente puede tener cualquier formato adecuado, tal como un objeto de datos simple, un archivo con una sola firma que identifica todas las puertas de enlace, objetos de

datos separados firmados, y/o archivos que identifican cada una de las puertas de enlace 700-702. Con la recepción de la lista de túneles de cliente, el cliente 721 establece un túnel de conexión a red 781, 782 y 783 con cada una de las
5 puertas de enlace 700-702.

La lista de accesos de cliente incluye una selección de los servidores de aplicaciones 741-747 al que puede conectarse el cliente mediante los túneles de conexión a red 781, 782 y 783. El cliente 721 envía la lista de accesos de
10 cliente a las puertas de enlace que, a su vez, configuran su cortafuegos de acuerdo con la lista de accesos de cliente recibida, por lo que permite al cliente 721 el acceso a la selección de servidores de aplicaciones.

En algunas modalidades, el servidor de autenticación
15 760 puede acceder a otros servidores para autenticación del cliente 721 o para recuperar la información sobre el cliente 721. Esto también se ilustra por la Figura 7, donde el servidor de autenticación 760 puede acceder al servidor de radio 762 que sirve como terminal de salida de
20 autenticación para el servidor de autenticación 760. El módulo de autenticación 162 en el servidor de autenticación 760 entonces sirve como interfaz de autenticación para el cliente 721 mientras que el servidor 762 realiza la autenticación real. El servidor de

autenticación 760 también puede conectarse al servidor 761 que proporciona un servicio de Directorio Activo al servidor de autenticación 760 para recuperar la información de perfil adicional sobre el usuario del cliente 721.

5 La Figura 8 ilustra aún otros sistema ejemplar donde el servidor de radio 846 y el servidor de Directorio Activo 847 corresponden a servidores de aplicaciones dentro de la red privada 744 detrás de la puerta de enlace 702, por lo que ayuda a proteger a los servidores 846-847 contra acceso no
10 autorizado. Para acceder a los servidores 846-847, el servidor de autorización 760 puede incluir túnel de conexión a red permanente 884 con la puerta de enlace 702 protegiendo a los servidores 846 y 847. Alternativamente, el servidor de autorización 760 puede utilizar otro mecanismo para
15 proporcionar acceso a los servidores 846-847, tales como LDAP sobre JSON con el fin de hacer uso de tráfico estándar de HTTPS en lugar de utilizar un túnel de red. Las reglas del cortafuegos que permiten que el servidor de autenticación 760 tenga acceso a los servidores entonces puede configurarse
20 en la puerta de enlace 702 con anticipación de manera que ninguna lista de túneles de cliente o lista de accesos de cliente se necesita para establecer la conexión de red entre el servidor de autenticación 760 y los servidores 846-847.

La Figura 9 ilustra un ejemplo donde múltiples puertas

de enlace 900, 901 se utilizan para proteger a los servidores de aplicaciones 941-944 dentro de una misma red privada 940. Esta topología puede utilizarse para equilibrar la carga de tráfico de red entre las múltiples puertas de enlace 900, 5 901. El servidor de autenticación 960 proporciona listas de túneles de cliente que especifican una puerta de enlace diferente a los clientes 921 y 922. En particular, el cliente 921 establece un túnel de conexión a red 981 con la puerta de enlace 900 y el cliente 922 establece el túnel de conexión a 10 red 982 con la puerta de enlace 901.

Las modalidades ejemplares en la presente ilustran modalidades de la descripción que protege a servidores de aplicaciones contra acceso no autorizado. Además de los servidores de aplicaciones, cualquier otro tipo de 15 dispositivo de red que proporcione un servicio y se pueda dirigir sobre una red puede protegerse por las modalidades de esta descripción. De igual manera, los dispositivos de red que pueden protegerse por modalidades de la descripción incluyen equipo de conexión a red que proporciona una 20 interfaz de administrador a enrutadores y conmutadores de nivel de red.

La Figura 10 ilustra un sistema de cómputo ejemplar 1000 que puede utilizarse junto con las modalidades descritas en la presente. El sistema de cómputo 1000 puede utilizarse como

dispositivo de cliente, puerta de enlace, servidor de autenticación, y/o cualquier otro sistema adecuado. El sistema de cómputo 1000 comprende un bus 1010, un procesador 1002, una memoria local 1004, una o más interfaces de entrada 5 opcionales 1014, una o más interfaces de salida opcionales 1016, una interfaz de comunicación 1012, una interfaz de elemento de almacenamiento 1006 y uno o más elementos de almacenamiento 1008.

El bus 1010 puede comprender uno o más conductores que 10 permitan comunicación entre los componentes del sistema de cómputo 1000. El procesador 1002 puede incluir cualquier tipo de procesador que interprete y ejecute las instrucciones de programación. La memoria local 1004 puede incluir una memoria de acceso aleatorio (RAM) u otro tipo de dispositivo de 15 almacenamiento dinámico que almacena información e instrucciones para ejecución por el procesador 1002 y/o una memoria de sólo lectura (ROM) u otro tipo de dispositivo de almacenamiento estático que almacena información estática e instrucciones para su uso por el procesador 1002. La interfaz 20 de entrada 1014 puede comprender uno o más mecanismos convencionales que permiten a un operador ingresar información en el dispositivo de cómputo 1000, tal como un teclado 1020, un ratón 1030, una pluma, mecanismos de reconocimiento de voz y/o biométricos, etc.

La interfaz de salida 1016 puede comprender uno o más mecanismos convencionales que producen información al operador, tal como una pantalla 1040, una impresora 1050, un altavoz, etc. La interfaz de comunicación 1012 puede
5 comprender cualquier mecanismo similar a un transceptor tal como por ejemplo una o más interfaces de Ethernet que permiten al sistema de cómputo 1000 comunicarse con otros dispositivos y/o sistemas 1100. La interfaz de comunicación 1012 del sistema de cómputo 1000 puede conectarse a tal sistema de
10 cómputo por medio de una red de área local (LAN) o una red de área extensa (WAN) tal como, por ejemplo, la Internet. La interfaz de elemento de almacenamiento 1006 puede comprender una interfaz de almacenamiento tal como por ejemplo, una Interfaz de Unión de Tecnología Avanzada Serial (SATA) o una
15 Interfaz Pequeña de Sistema Informático (SCSI) para conectar el bus 1010 a uno o más elementos de almacenamiento 1008, tal como uno o más discos locales, por ejemplo, unidades de disco SATA, y control de lectura y escritura de datos en y desde estos elementos de almacenamiento 1008. Aunque los elementos
20 de almacenamiento 1008 anteriores se describen en un disco local, en general cualquier otro medio legible por computadora adecuado tal como un disco magnético removible, medio de almacenamiento óptico, tal como CD o DVD, -disco ROM, unidades de estado sólido, unidades de memoria flash,...

podrían utilizarse. El sistema 1000 descrito en lo anterior también puede ejecutarse como motor virtual por encima del hardware físico.

Los métodos ilustrados en la presente pueden
5 implementarse mediante instrucciones de programación almacenadas en memoria local 1004 del sistema de cómputo 1000 para ejecución por su procesador 1002. Alternativamente, las instrucciones pueden almacenarse en el elemento de almacenamiento 1008 o ser accesibles desde otro sistema de
10 cómputo a través de la interfaz de comunicación 1012.

El sistema 1000 puede corresponder al cliente 121, 122, 621, 721, 921, 922 de las modalidades ilustradas por la Figura 1, Figura 6, Figura 7, Figura 8 y Figura 9, respectivamente. En tales casos, el sistema 1000 puede
15 conectarse a la puerta de enlace y el servidor de autorización por la interfaz de comunicación 1012. Etapas de los métodos ilustrados en la Figura 2, Figura 5 y Figura 6 pueden realizarse como instrucciones en el procesador 1002 durante la ejecución y pueden almacenarse en el almacén de
20 memoria 1004 o 1008.

El sistema 1000 puede corresponder al cliente 100, 600, 700, 701, 702, 900 y 901 de las modalidades ilustradas por la Figura 1, Figura 6, Figura 7, Figura 8 y Figura 9, respectivamente. En tales casos, el sistema puede comprender

dos interfaces de comunicación 1012, una interfaz de comunicación para conectarse a la red privada y una para conectarse a la otra red mediante la cual se conecta a los clientes. Las etapas del método ilustrado en la Figura 4
5 pueden realizarse como instrucciones en el procesador 1002 durante la ejecución y pueden almacenarse en el almacén de memoria 1004 o 1008.

El sistema 1000 puede corresponder al servidor de autenticación 160, 760 y 960 de las modalidades ilustradas
10 por la Figura 1, Figura 6, Figura 7, Figura 8 y Figura 9. En tales casos, la interfaz de comunicación 1012 puede utilizarse para conectar el sistema 1000 a los clientes y puertas de enlace. Las etapas del método ilustrado en la Figura 3 entonces pueden realizarse como instrucciones en el
15 procesador 1002 durante la ejecución y pueden almacenarse en el almacén de memoria 1004 o 1008.

Métodos realizados por el servidor de autenticación y la puerta de enlace además pueden ejecutarse en un mismo sistema informático, en sistemas informáticos separados, o
20 como sistemas informáticos virtuales separados en los mismos sistemas informáticos físicos o diferentes.

La comunicación entre los sistemas, dispositivos y componentes que operan junto con modalidades de la presente descripción pueden realizarse utilizando cualquier método de

comunicación adecuado, tal como por ejemplo, una red telefónica, una extranet, una intranet, la internet, el punto de dispositivo de interacción (punto de dispositivo de venta, asistente digital personal (por ejemplo, iPhone®, Palm Pilot®, Blackberry®) teléfono celular, quiosco, etc.), comunicaciones en línea, comunicaciones satelitales, comunicaciones fuera de línea, comunicaciones inalámbricas, comunicaciones por transpondedor, red de área local (LAN), red de área extensa (WAN), red privada virtual (VPN), dispositivos conectados a red o enlazados, teclados, ratones y/o cualquier comunicación adecuada o modalidad de entrada de datos. Los sistemas y dispositivos de la presente descripción pueden utilizar protocolos de comunicación de TCP/IP, así como IPX, Appletalk, IP-6, NetBIOS, OSI, cualquier protocolo de canalización (por ejemplo, IPsec, SSH) o cualquier número de protocolos existentes o futuros.

Aunque algunas modalidades pueden implementarse en computadoras de funcionamiento completo y sistemas informáticos, varias modalidades son capaces de distribuirse como producto de cómputo en una variedad de formas y son capaces de aplicarse independientemente del tipo particular de máquina o medio legible por computadora utilizado para efectuar realmente la distribución.

Un medio legible por máquina puede utilizarse para

almacenar software y datos que cuando se ejecutan por un sistema de procesamiento de datos provoca que el sistema realice varios métodos. El software ejecutable y datos pueden almacenarse en varios lugares incluyendo por ejemplo, ROM, RAM volátil, memoria no volátil y/o caché. Porciones de este software y/o datos pueden almacenarse en cualquiera de estos dispositivos de almacenamiento. Además, los datos e instrucciones pueden obtenerse de servidores centralizados o redes de igual a igual. Diferentes porciones de los datos e instrucciones pueden obtenerse a partir de diferentes servidores centralizados y/o redes de igual a igual en diferentes momentos y en diferentes sesiones de comunicación o en una misma sesión de comunicación. Los datos e instrucciones pueden obtenerse totalmente antes de la ejecución de las aplicaciones. Alternativamente, porciones de los datos e instrucciones pueden obtenerse dinámicamente, justo a tiempo, cuando se necesiten para ejecución. De esta manera, no se requiere que los datos e instrucciones se encuentren en un medio legible por máquina en su totalidad en un caso particular de tiempo.

Ejemplos de medios legibles por computadora incluyen pero no se limitan a medios tipo grabable y no grabable tales como dispositivos de memoria volátil y no volátil, memoria de solo lectura (ROM), memoria de acceso aleatorio (RAM)

dispositivos de memoria flash, discos flexibles y otros removibles, medios de almacenamiento en disco magnético, medios de almacenamiento óptico (por ejemplo, Memoria de Solo Lectura-Disco Compacto (CD ROM), Discos Versátiles Digitales (DVD), etc.), entre otros. Los medios legibles por computadora pueden almacenar las instrucciones.

En varias modalidades, circuitería alámbrica puede utilizarse en combinación con instrucciones de software para implementar las técnicas. De esta manera, las técnicas no se limitan a ninguna combinación específica de circuitería de hardware y software ni a ninguna fuente particular para las instrucciones ejecutadas por el sistema de procesamiento de datos.

Aunque algunos de los dibujos ilustran un número de operaciones en un orden particular, operaciones las cuales no dependen del orden pueden registrarse y otras operaciones pueden combinarse o descomponerse. Aunque en cierto reordenamiento u otras agrupaciones se mencionan específicamente, otras serán aparentes para aquellos de experiencia ordinaria en la técnica y no representan una lista exhaustiva de alternativas. Además, debe reconocerse que las fases podrían implementarse en hardware, firmware, software o cualquier combinación de los mismos.

Para brevedad, conexión a red de datos convencionales,

desarrollo de aplicaciones y otros aspectos funcionales de los sistemas (y componentes de los componentes operativos individuales de los sistemas) pueden no describirse en detalle en la presente. Además, se pretende que las líneas de
5 conexión mostradas en las diversas figuras contenidas en la presente representen relaciones funcionales ejemplares y/o acoplamientos físicos entre los diversos elementos. Debe observarse que muchas relaciones funcionales alternativas o adicionales o conexiones físicas pueden presentarse en un
10 sistema práctico.

Los diversos componentes de sistema discutidos en la presente pueden incluir uno o más de lo siguiente: un servidor central u otros sistemas de cómputo que incluyen un procesador para procesar datos digitales; una memoria
15 acoplada al procesador para almacenar datos digitales; un digitalizador de entrada acoplado al procesador para ingresar datos digitales; un programa de aplicación almacenado en la memoria y accesible por el procesador para dirigir procesamiento de datos digitales por el procesador; un
20 dispositivo de visualización acoplado al procesador y a la memoria para visualizar información derivada a partir de datos digitales procesados por el procesador; y una pluralidad de bases de datos. Varias bases de datos utilizadas en la presente pueden incluir: datos de envío,

datos de embalaje y/o cualesquier datos útiles en la operación del sistema.

Una funcionalidad variada puede realizarse mediante un navegador web y/o aplicación que se interconecta utilizando un navegador web. Tales aplicaciones de navegador pueden comprender software de navegación por internet instalado dentro de una unidad de cómputo o un sistema para realizar varias funciones. Estas unidades de cómputo o sistemas pueden adoptar la forma de una computadora o conjunto de computadoras, y cualquier tipo de dispositivo de cómputo o sistemas pueden utilizarse, incluyendo computadoras tipo laptop, computadoras tipo notebook, computadoras tipo tablet, computadoras portátiles, asistentes digitales personales, cajas de convertidor-descodificador, estaciones de trabajo, servidores informáticos, computadoras principales, mini computadoras, servidores PC, conjuntos de computadoras en red, computadoras personales y computadoras tipo tablet, tales como iPads, iMacs, y MacBooks, quioscos, terminales, dispositivos de punto de venta (POS), y/o terminales, televisiones, o cualquier otro dispositivo capaz de recibir datos sobre una red. Varias modalidades pueden utilizar el Microsoft Internet Explorer, Mozilla Firefox, Google Chrome, Apple Safari, Opera o cualquier otro de los miles de paquetes de software disponibles para navegar la internet.

Varias modalidades pueden operar junto con cualquier sistema operativo adecuado (por ejemplo, Windows NT, 95/98/2000/CE/Mobile/, Windows 7/8, OS2, UNIX, LINUX, Solaris, MacOS, PalmOS, etc.) así como software de soporte
5 convencional variado y controladores típicamente asociados con computadoras. Varias modalidades pueden incluir cualquier computadora personal adecuada, computadora de red, estación de trabajo, asistente digital personal, teléfono celular, teléfono inteligente, mini computadora, computadora principal
10 o similares. Modalidades pueden implementar protocolos de seguridad, tales como Capa de Terminal Segura (SSL), Seguridad de Capa de Transporte (TLS), y Protección Segura (SSH). Modalidades pueden implementar cualquier protocolo de capa de aplicación deseado, incluyendo http, https, ftp, y
15 sftp.

Los diversos componentes de sistema pueden acoplarse de manera independiente, separada o colectiva y adecuada a una red mediante enlaces de datos que incluye, por ejemplo, una conexión a un Proveedor de Servicios por Internet (ISP) sobre
20 bucle local como se utiliza típicamente junto con comunicación moderna estándar, módem de cable, redes satelitales, ISDN, Línea de Suscriptor Digital (DSL), o varios métodos de comunicación inalámbrica. Se observa que modalidades de la presente descripción pueden operar junto

con cualquier tipo adecuado de red, tal como una red de televisión interactiva (ITV).

El sistema puede implementarse parcial o completamente utilizando informática en la nube. "Nube" o "Informática en la nube" incluyen un modelo para permitir acceso de red a solicitud, conveniente en un grupo compartido de recursos de cómputo configurables (por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios) que pueden proveerse rápidamente y liberarse con mínimo esfuerzo de gestión o interacción de proveedores de servicio. La informática en la nube puede incluir informática independiente de ubicación, por lo que servidores compartidos proporcionan recursos, software y datos a computadoras y otros dispositivos a solicitud.

Varias modalidades pueden utilizarse junto con servicios web, informática de utilidad, informática pervasiva e individualizada, soluciones de seguridad de identidad, informática autónoma, informática en la nube, informática de bienes, soluciones de movilidad e inalámbrica, fuente abierta, biométrica, informática de rejilla y/o informática de malla.

Cualesquier bases de datos discutidas en la presente pueden incluir estructura de relación, jerárquica, gráfica u orientada a objeto y/o cualquier otras configuraciones de

bases de datos. Además, las bases de datos pueden organizarse en cualquier forma adecuada, por ejemplo, como tablas de datos o tablas de consulta. Cada registro puede ser un archivo simple, una serie de archivos, una serie enlazada de campos de datos o cualquier otra estructura de datos. La asociación de ciertos datos puede lograrse a través de cualquier técnica de asociación de datos deseada tal como aquella conocida o practicada en la técnica. Por ejemplo, la asociación puede lograrse ya sea manualmente o de forma automática.

Cualesquier bases de datos, sistemas, dispositivos, servidores u otros componentes del sistema pueden ubicarse en una sola ubicación o en múltiples ubicaciones, en donde cada base de datos o sistema incluye cualquiera de varias características de seguridad adecuadas, tales como cortafuegos, códigos de acceso, encriptación, descifrado, compresión, descompresión, y/o similares.

La encriptación puede realizarse por medio de cualquiera de las técnicas ahora disponibles en la arte o que puedan volverse disponibles - por ejemplo, Twofish, RSA, El Gamal, Schorr signature, DSA, PGP, PKI y criptosistemas simétricos y asimétricos.

Modalidades pueden conectarse al Internet o a una intranet utilizando marcación estándar, cable, DSL o

cualquier otro protocolo de internet conocido en la técnica. Transacciones pueden pasar a través de un cortafuegos con el fin de evitar acceso no autorizado de usuarios de otras redes.

5 Las computadoras discutidas en la presente pueden proporcionar un sitio web adecuado u otra interfaz de usuario gráfica basada en internet la cual sea accesible por usuarios. Por ejemplo, el Servidor de Información de Microsoft Internet (IIS), Servidor de Transacción Microsoft 10 (MTS), y Microsoft SQL Server, puede utilizarse junto con el sistema operativo Microsoft, software de servidor web de Microsoft NT, o sistema de base de datos de Microsoft SQL Server, y un Servidor de Comercio Microsoft. Adicionalmente, componentes tales como Access o Microsoft SQL Server, Oracle, 15 Sybase, Informix MySQL, Interbase, etc., pueden utilizarse para proporcionar un sistema de gestión de bases de datos con descendiente de objeto de datos activo (ADO). En otro ejemplo, un servidor web Apache puede utilizarse junto con un sistema operativo Linux, una base de datos MySQL y los 20 lenguajes de programación de Perl, PHP y/o Python.

Cualquiera de las comunicaciones, entradas, almacenamiento, bases de datos o visualizaciones discutidas en la presente pueden facilitarse a través de un sitio web que tiene páginas web. El término "páginas web" como se

utiliza en la presente no se pretende para limitar el tipo de documentos y aplicaciones que pueden utilizarse para interactuar con el usuario. Por ejemplo, un sitio web típico puede incluir, además de documentos estándar de HTML, varias formas, mini aplicaciones Java, JavaScript, páginas de servidor activo (ASP), programas de instrucciones de interfaz de puerta de enlace común (CGI), lenguaje de marcación extensible (XML), HTML dinámico, hojas de estilo en cascada (CSS), AJAX (Javascript Asincrónica y XML), aplicaciones de ayuda, plug-ins, y similares. Un servidor puede incluir un servicio web que recibe una solicitud de un servidor web, la solicitud incluye una dirección de URL y de IP. El servidor web recupera las páginas web adecuadas y envía los datos o aplicaciones para las páginas web a la dirección de IP. Los servicios web son aplicaciones que son capaces de interactuar con otras aplicaciones sobre un medio de comunicación tal como la Internet.

Varias modalidades pueden emplear cualquier número deseado de métodos para visualizar datos dentro de un documento basado en explorador. Por ejemplo, datos pueden representarse como texto estándar o dentro de una lista fija, lista desplegable, lista abatible, campo de texto editable, campo de texto fijo, ventana emergente, y similares. De igual manera, modalidades pueden utilizar cualquier número deseado

de métodos para modificar datos en una página web tal como por ejemplo, entrada de datos libre utilizando un teclado, selección de artículos de menú, cajas de comprobación, cajas de opción, y similares.

5 Los sistemas ejemplares y métodos ilustrados en la presente pueden describirse en términos de componentes de bloque funcional, capturas de pantalla, selecciones opcionales y varias etapas de procesamiento. Debe apreciarse que tales bloques funcionales pueden realizarse por cualquier
10 número de componentes de hardware y/o software configurados para realizar las funciones específicas. Por ejemplo, el sistema puede emplear varios componentes de circuito integrado, por ejemplo, elementos de memoria, elementos de procesamiento, elementos lógicos, tablas de consulta, y
15 similares, que pueden llevar a cabo una variedad de funciones bajo el control de uno o más microprocesadores u otros dispositivos de control. De manera similar, los elementos de software de sistema pueden implementarse con cualquier lenguaje de programación o lenguaje de escritura como C, C++,
20 C#, Java, JavaScript, VBScript, Macromedia Cold Fusion, COBOL, Microsoft Active Server Pages, assembly, PERL, PHP, AWK, Python, Visual Basic, Procedimientos Almacenados en SQL, PL/SQL, cualquier secuencia de comandos UNIX, y lenguaje de marcación extensible (XML) con varios algoritmos que se

implementan con cualquier combinación de estructuras de datos, objetos, procesos, rutinas u otros elementos de programación. Además, debe observarse que el sistema puede emplear cualquier número de técnicas convencionales para
5 transmisión de datos, señalización, procesamiento de datos, control de red y similares. Además, el sistema podría utilizarse para detectar o evitar cuestiones de seguridad con un lenguaje de escritura de lado de cliente, tal como JavaScript, VBScript o similares.

10 Los sistemas y métodos de la presente descripción pueden representarse como una personalización de un sistema existente, un producto de adición, un aparato de procesamiento que ejecuta software actualizado, un sistema autónomo, un sistema distribuido, un método, un sistema de
15 procesamiento de datos, un dispositivo para procesamiento de datos, y/o un producto de programa de computadora. Por consiguiente, cualquier porción del sistema o módulo puede adoptar la forma de un código de ejecución de aparato de procesamiento, una modalidad basada en Internet, una
20 modalidad totalmente de hardware, o una modalidad que combina aspectos del Internet, software y hardware. Además, el sistema puede adoptar la forma de un producto de programa de computadora en un medio de almacenamiento legible por computadora que tiene medio de código de programación legible

por computadora representado en el medio de almacenamiento. Cualquier medio de almacenamiento legible por computadora adecuado puede utilizarse, incluyendo discos duros, CD-ROM, dispositivos de almacenamiento óptico, dispositivos de
5 almacenamiento magnético, y/o similares.

El sistema y método se describe en la presente con referencia a capturas de pantalla, diagramas de bloque e ilustraciones de diagrama de flujo de métodos, aparatos (por ejemplo, sistemas), y productos de programa de computadora de
10 acuerdo con varias modalidades. Se entenderá que cada bloque funcional de los diagramas de bloque y las instrucciones de diagrama de flujo, y combinaciones de bloques funcionales y los diagramas de bloque e ilustraciones de diagrama de flujo, respectivamente, pueden implementarse por instrucciones de
15 programa de computadora.

Estas instrucciones de programa de computadora pueden cargarse en una computadora de propósito general, computadora de propósito especial u otro aparato de procesamiento de datos programable para producir una máquina de modo que las
20 instrucciones que se ejecuten en la computadora u otro aparato de procesamiento de datos programable cree medios para implementar las funciones especificadas en el bloque o bloques de diagrama de flujo. Estas instrucciones de programa de computadora también pueden almacenarse en una memoria

legible por computadora que puede dirigir a una computadora u otro aparato de procesamiento de datos programable a funcionar en una forma particular, de manera que las instrucciones almacenadas en la memoria legible por computadora produzcan un artículo de fabricación que incluya medios de instrucción que implementan la función especificada en el bloque o bloques del diagrama de flujo. Las instrucciones de programa de computadora también pueden cargarse en una computadora u otro aparato de procesamiento de datos programable para provocar que una serie de etapas operacionales se realicen en la computadora u otro aparato programable para producir un proceso implementado por computadora de manera que las instrucciones que se ejecutan en la computadora u otro aparato programable proporcionan etapas para implementar las funciones especificadas en el bloque o bloques de diagrama de flujo.

Por consiguiente, bloques funcionales de los diagramas de bloque y las ilustraciones de diagramas de flujo soportan combinaciones de medios para realizar las funciones especificadas, combinaciones de etapas para realizar las funciones especificadas, y los medios de instrucción de programación para realizar las funciones especificadas. También se entenderá que cada bloque funcional de los diagramas de bloque e ilustraciones de diagrama de flujo y

combinaciones de bloques funcionales en los diagramas de bloque e ilustraciones del diagrama de flujo, pueden implementarse por cualesquier sistemas informáticos basados en hardware de propósito especial que realizan las funciones o etapas especificadas, o combinaciones adecuadas de hardware de propósito especial e instrucciones de computadora. Además, ilustraciones de los flujos de proceso y las descripciones de los mismos pueden hacer referencia a ventanas de usuario, páginas web, sitios web, formularios web, indicaciones, etc.

Los practicantes apreciarán que las etapas ilustradas descritas en la presente pueden comprender en cualquier número de configuraciones que incluyen el uso de ventanas, páginas web, formularios web, ventanas emergentes, indicaciones y similares. Debe apreciarse además que múltiples etapas como se ilustra y describe pueden combinarse en páginas web simples y/o ventanas pero se ha expandido para simplicidad. En otros casos, etapas ilustradas y descritas como etapas de procesos simples pueden separarse en múltiples páginas web y/o ventanas pero se han combinado para simplicidad.

El término "no transitorio" se entenderá para remover solo señales transitorias de propagación en sí del alcance de la reivindicación y no renuncia a los derechos de todos los medios legibles por computadora estándar que no son solo

señales transitorias de propagación en sí. Establecido de otra manera, el significado del término "medio legible por computadora no transitorio" debe interpretarse para excluir solo estos tipos de medios legibles por computadora transitorios que se encontraron en In Re Nuijten que caen fuera del alcance de la materia objeto patentable bajo 35 U.S.C. § 101.

Los beneficios, otras ventajas, y las soluciones a los problemas se han descrito en la presente con respecto a las modalidades específicas. Sin embargo, los beneficios, ventajas, soluciones a problemas, y cualesquier elementos que puedan provocar cualquier beneficio, ventaja, o solución que se produzca o se vuelva más pronunciada no se interpretarán como críticos, requeridos o características esenciales o elementos de la descripción.

Aunque la descripción incluye un método, se contempla que puede representarse como instrucciones de programa de computadora en un portador legible por computadora tangible, tal como una memoria magnética u óptica o un disco magnético u óptico. Todos los equivalentes estructurales, químicos y funcionales de los elementos de las modalidades ejemplares antes descritas que se conocen por aquellos de experiencia ordinaria en la técnica se incorporan expresamente en la presente para referencia y se pretenden abarcar por las

presentes reivindicaciones. Además, no es necesario que un dispositivo o método aborde todos y cada uno de los problemas que se buscan resolver por la presente descripción, ya que se abarcará por las presentes reivindicaciones. Además, ningún elemento, componente, o etapa de método en la presente descripción se pretende dedicar al público independientemente de si el elemento, componente o etapa de métodos se narra explícitamente en las reivindicaciones. Ningún elemento de reivindicación en la presente se interpretará bajo las disposiciones de 35 U.S.C. 112, párrafo sexto, a menos que el elemento se narre expresamente utilizando la frase "medios para". Como se utiliza en la presente, los términos "comprende", "que comprende" o cualquier otra variación del mismo, se pretenden para cubrir una inclusión no exclusiva, de modo que un proceso, método, artículo o aparato que comprende una lista de elementos no incluye sólo estos elementos sino puede incluir otros elementos no listados expresamente o inherentes para tal proceso, método, artículo o aparato.

Donde una frase similar a "al menos uno de A, B, o C", "al menos uno de A, B y C", "uno o más de A, B, o C", o "uno o más de A, B y C" se utilice, se pretende que la frase se interprete para significar que A sola puede representarse en una modalidad, B sola puede presentarse en una modalidad, C

sola puede presentarse en una modalidad, o que cualquier combinación de los elementos A, B y C pueden presentarse en una sola modalidad; por ejemplo A y B, A y C, B y C, o A y B y C.

5 Cambios y modificaciones pueden hacerse a las modalidades descritas sin apartarse del alcance de la presente descripción. Estos y otros cambios o modificaciones se pretenden para incluirse dentro del alcance de la presente descripción, como se expresa en las siguientes
10 reivindicaciones.

RESUMEN DE LA INVENCIÓN

Modalidades de la presente descripción ayudan a proteger a los dispositivos de red contra acceso no autorizado. Entre
5 otras cosas, las modalidades de la descripción permiten acceso completo a servidores de aplicaciones y otros dispositivos de red que un cliente tiene acceso permitido, mientras que evita acceso completo (o incluso conocimiento) de los dispositivos de red que el cliente no tiene acceso
10 permitido.

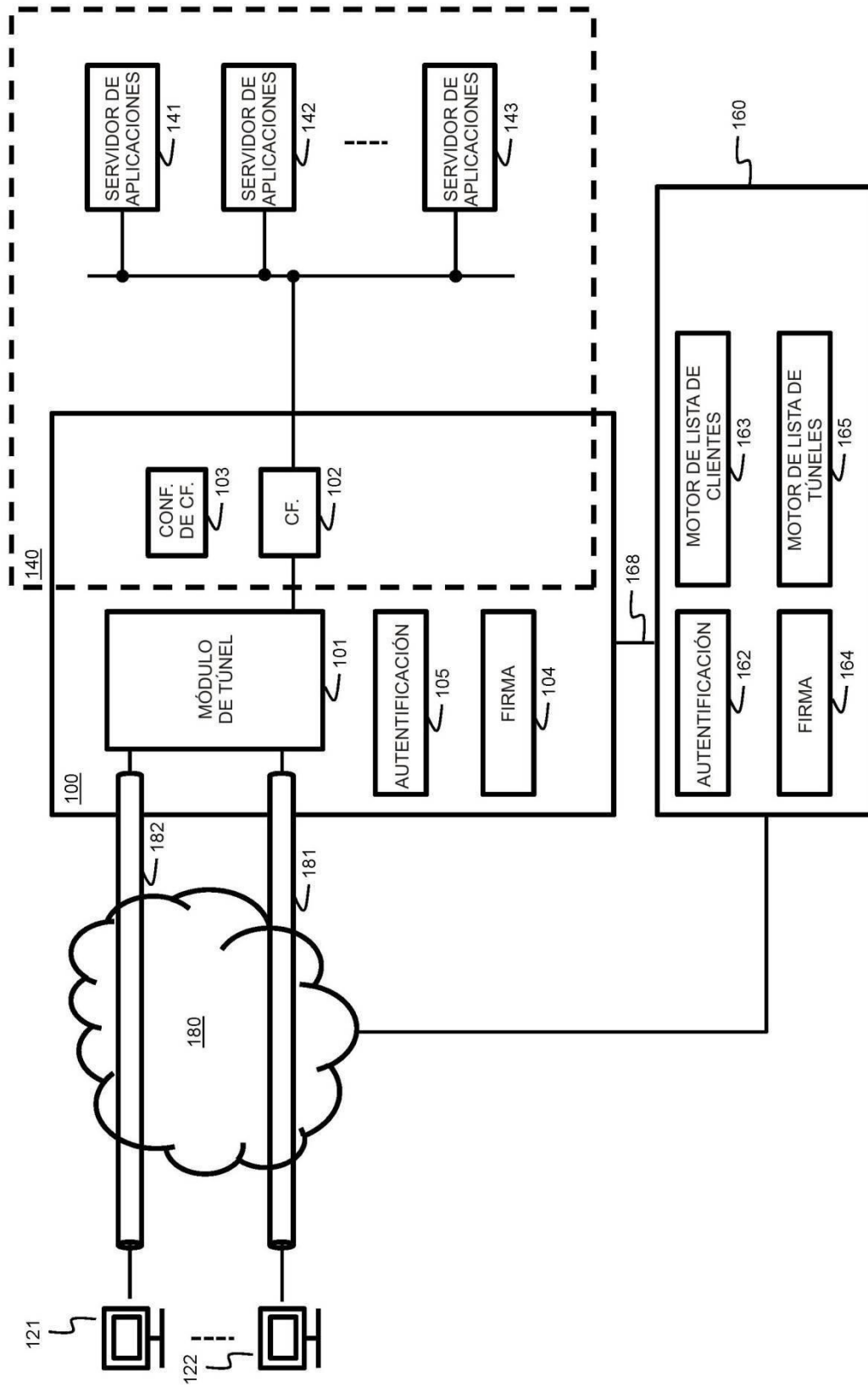


Figura 1

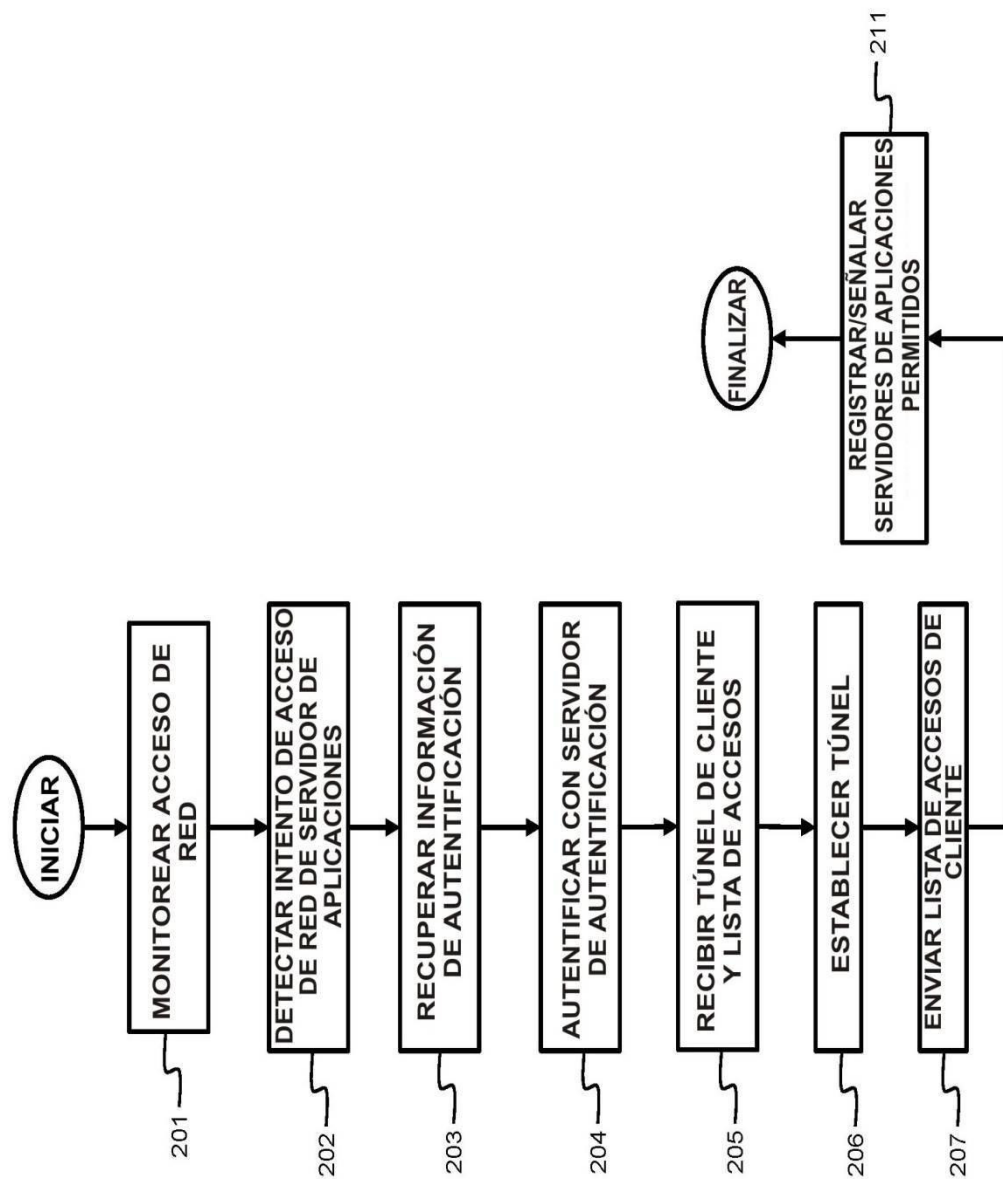


Figura 2

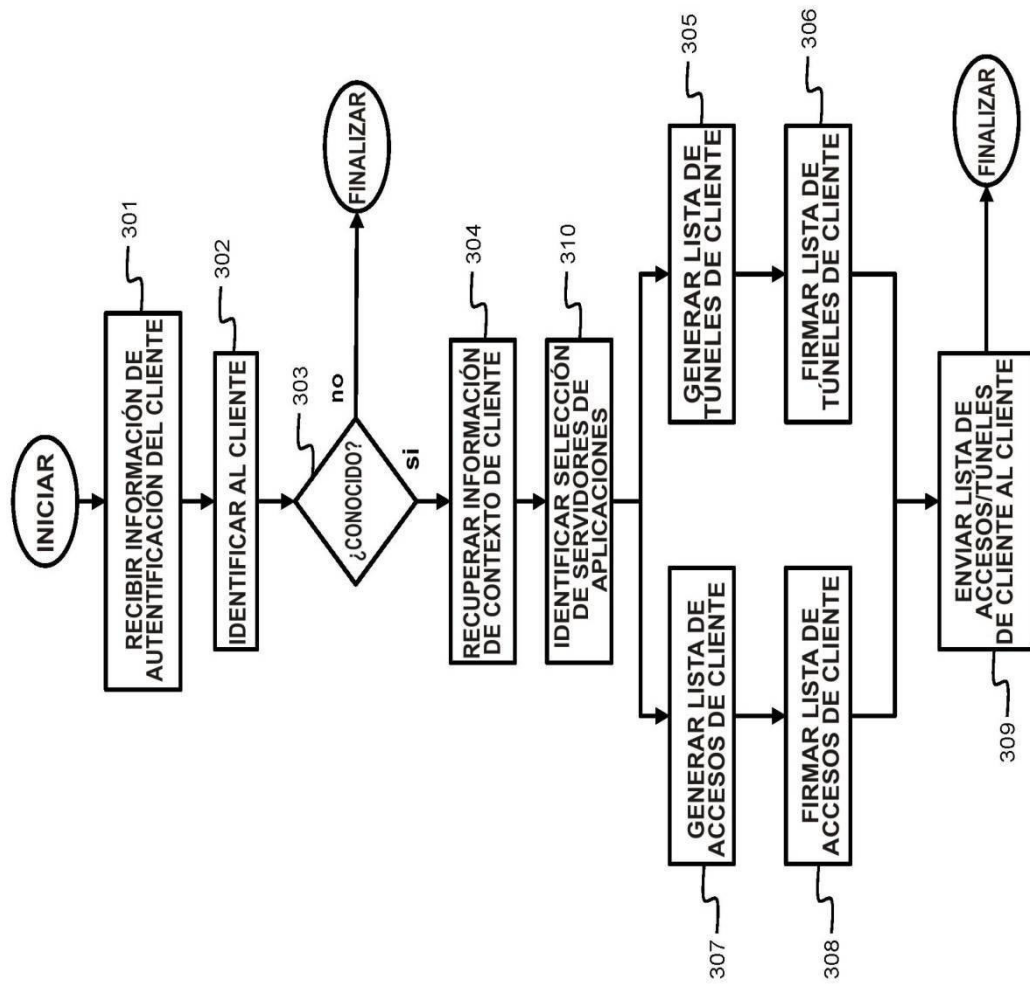


Figura 3

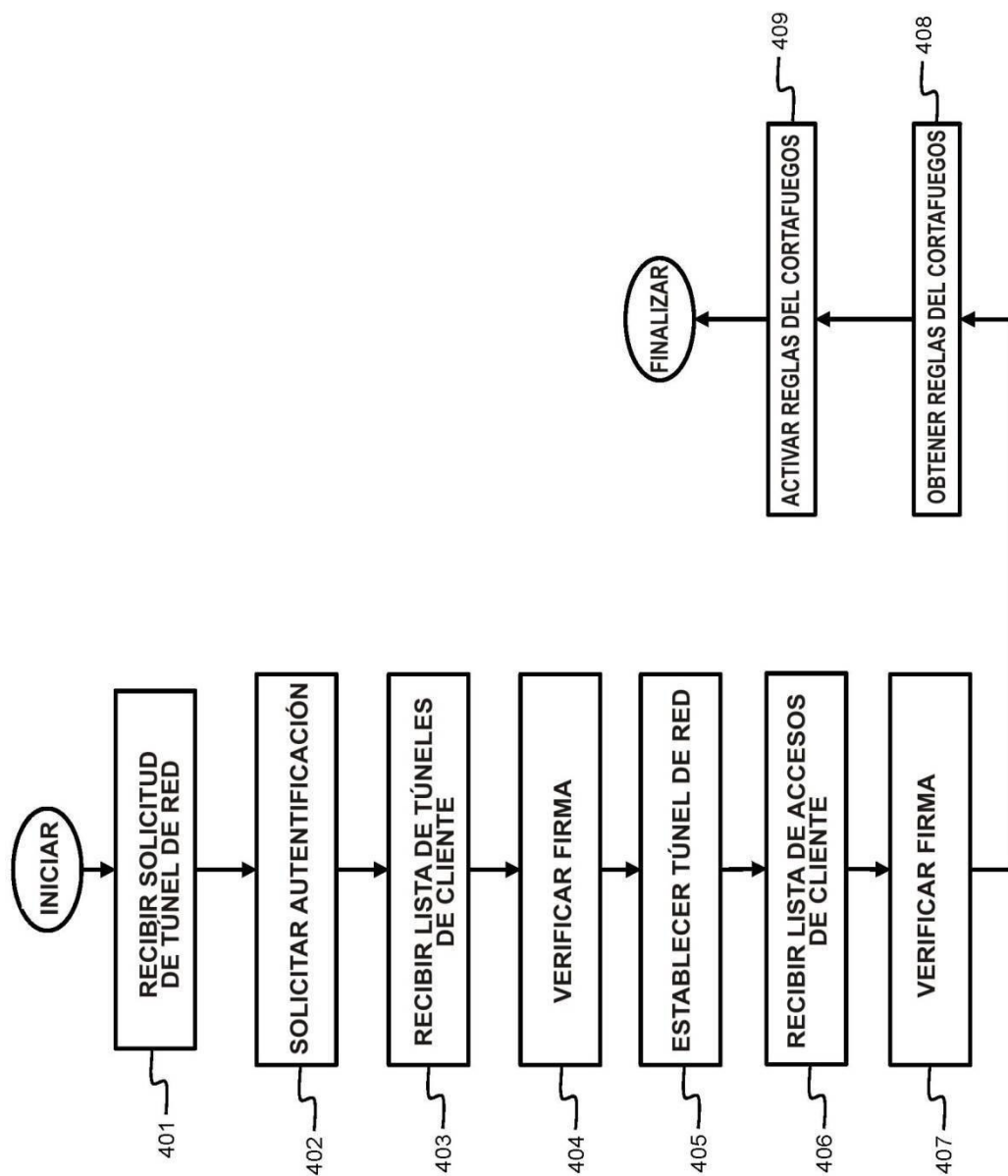


Figura 4

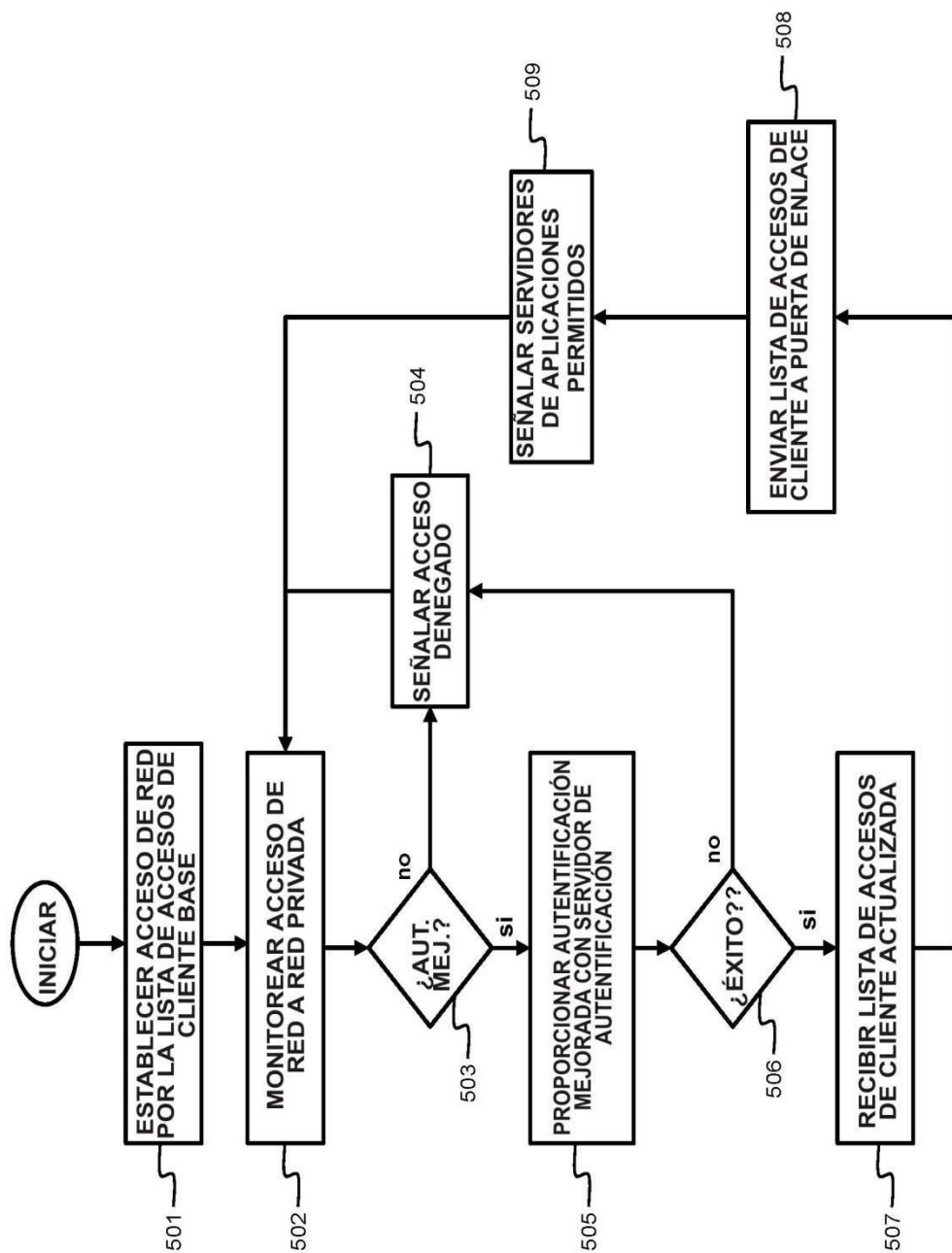


Figura 5

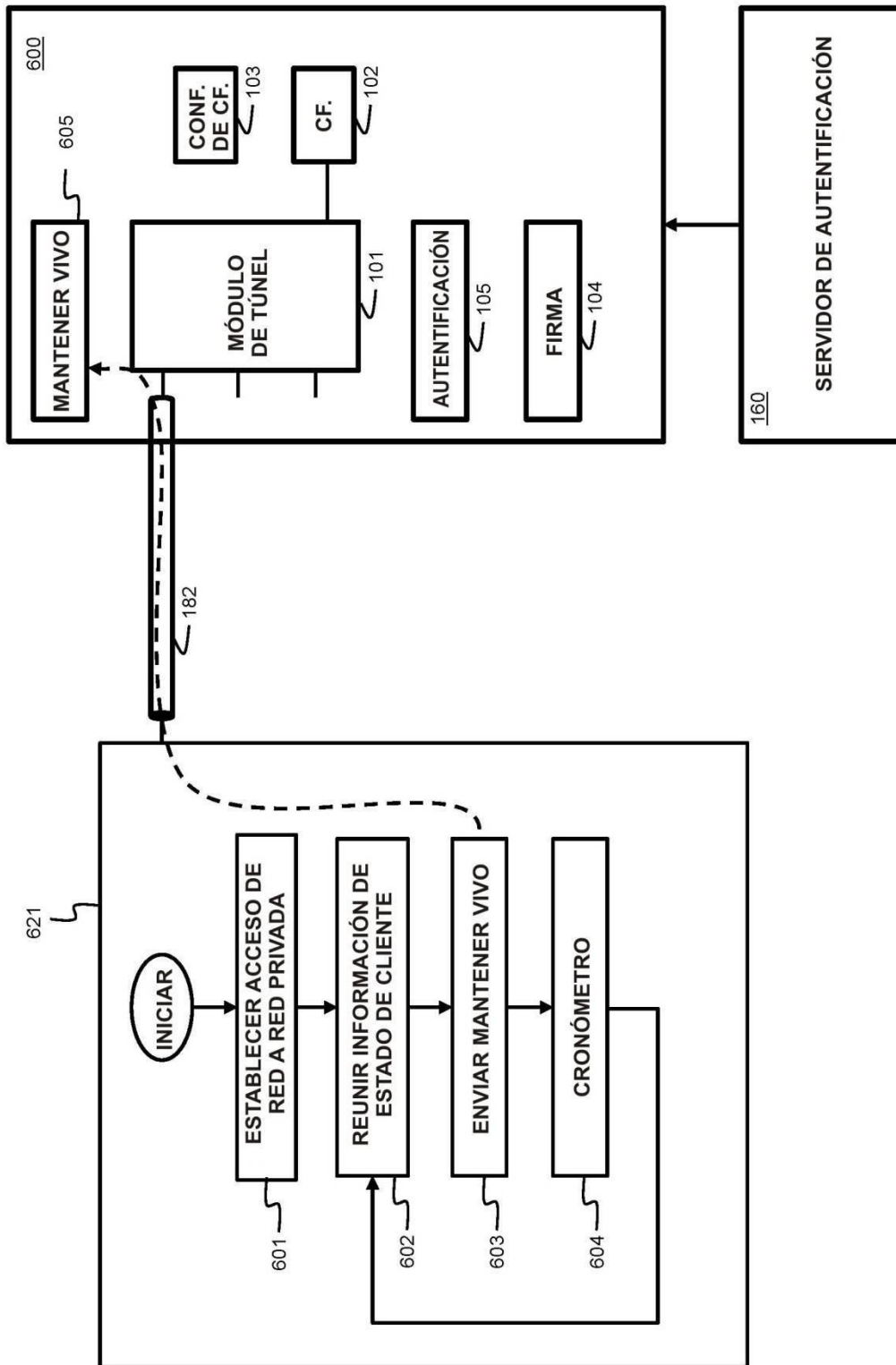


Figura 6

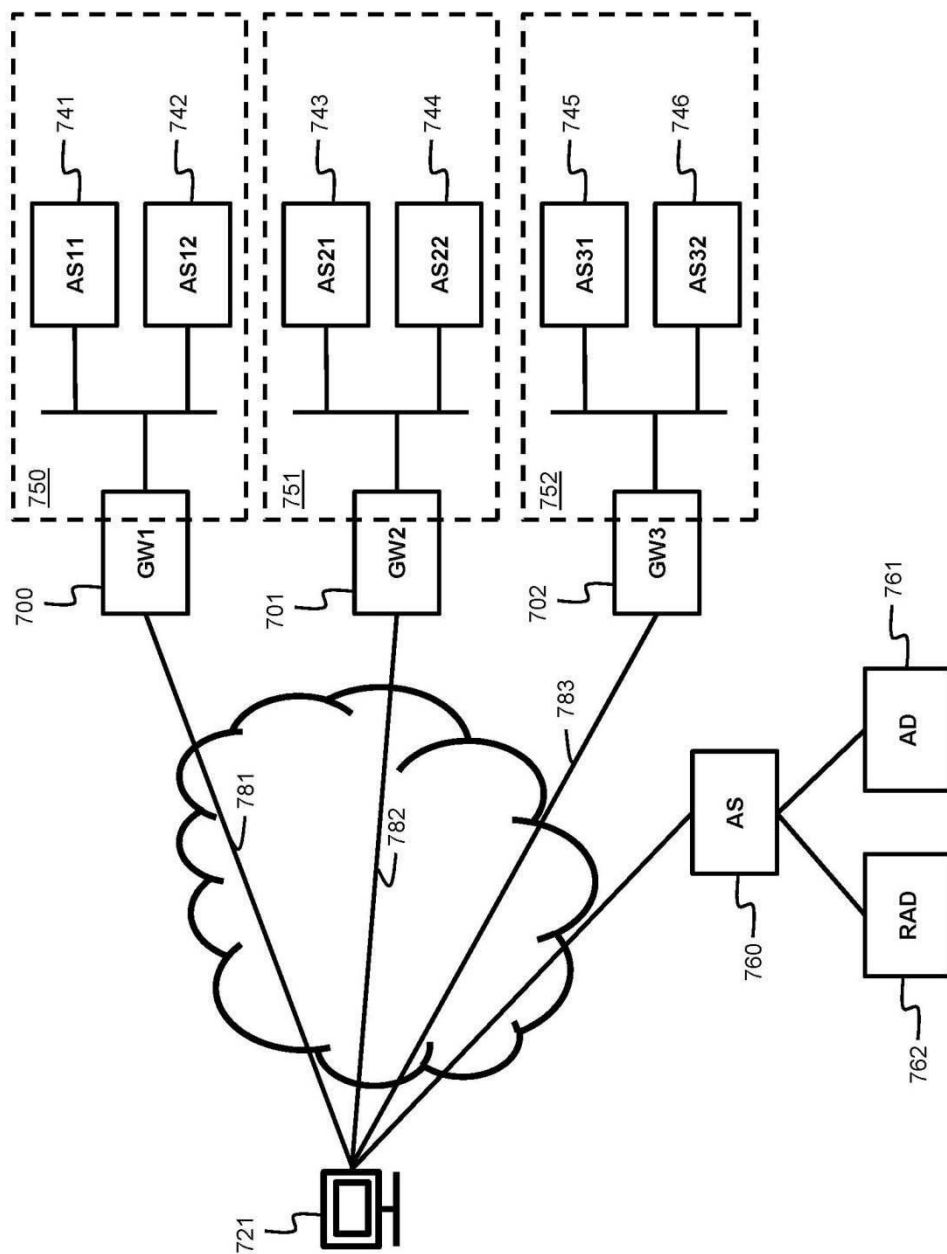


Figura 7

5

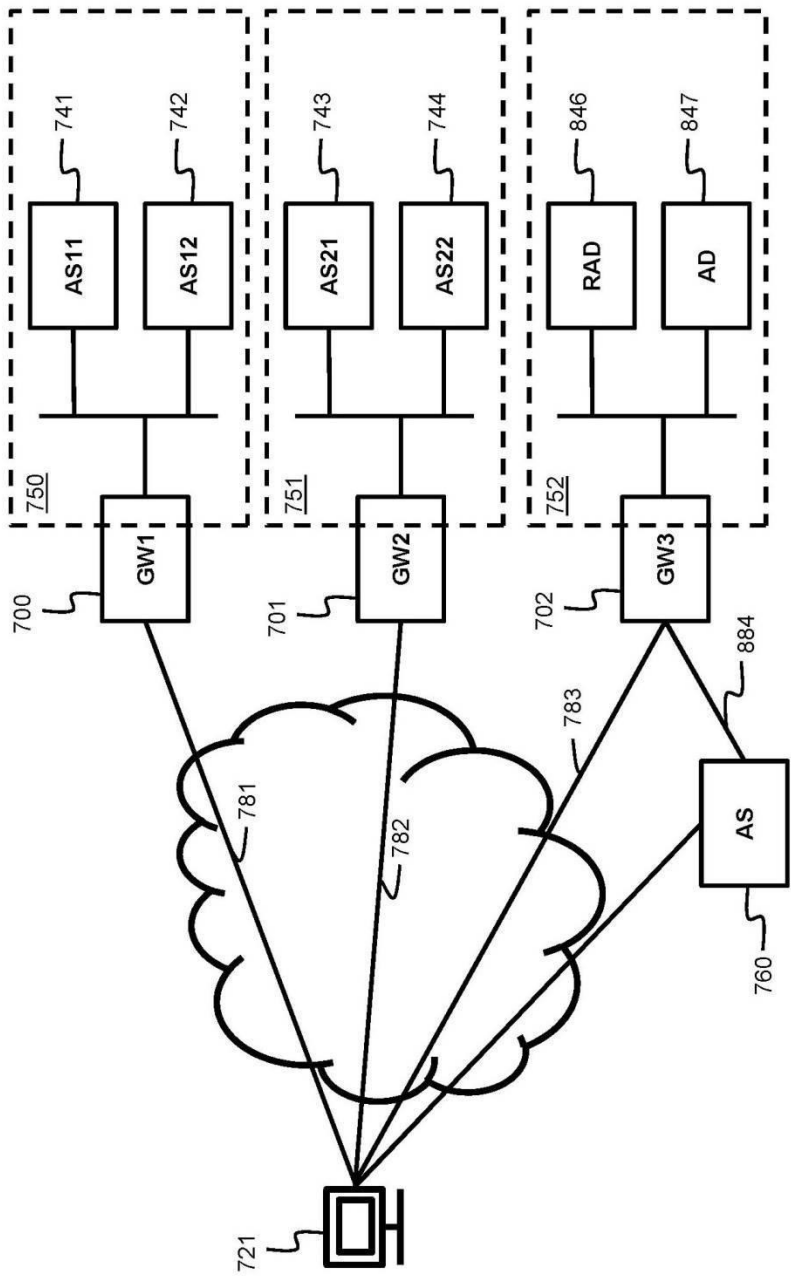


Figura 8

5

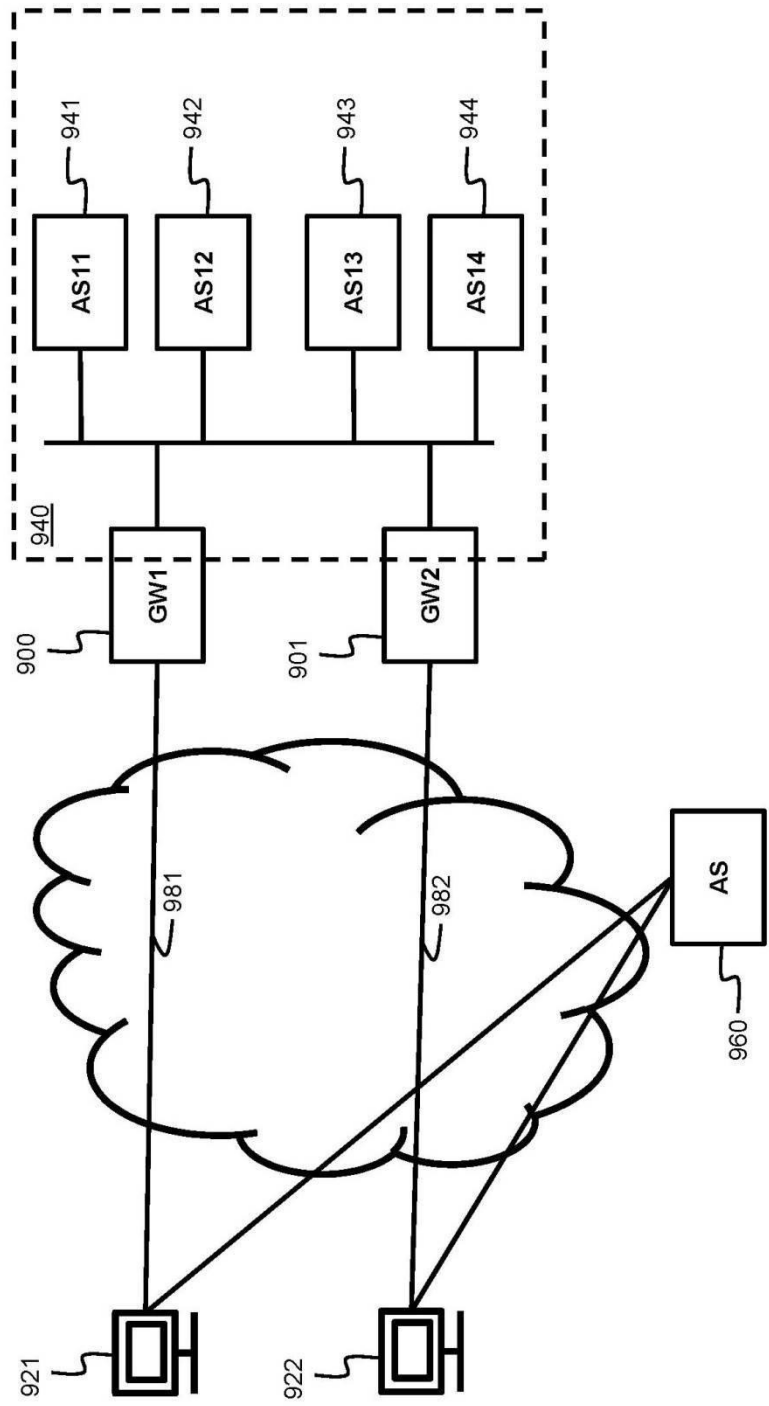


Figura 9

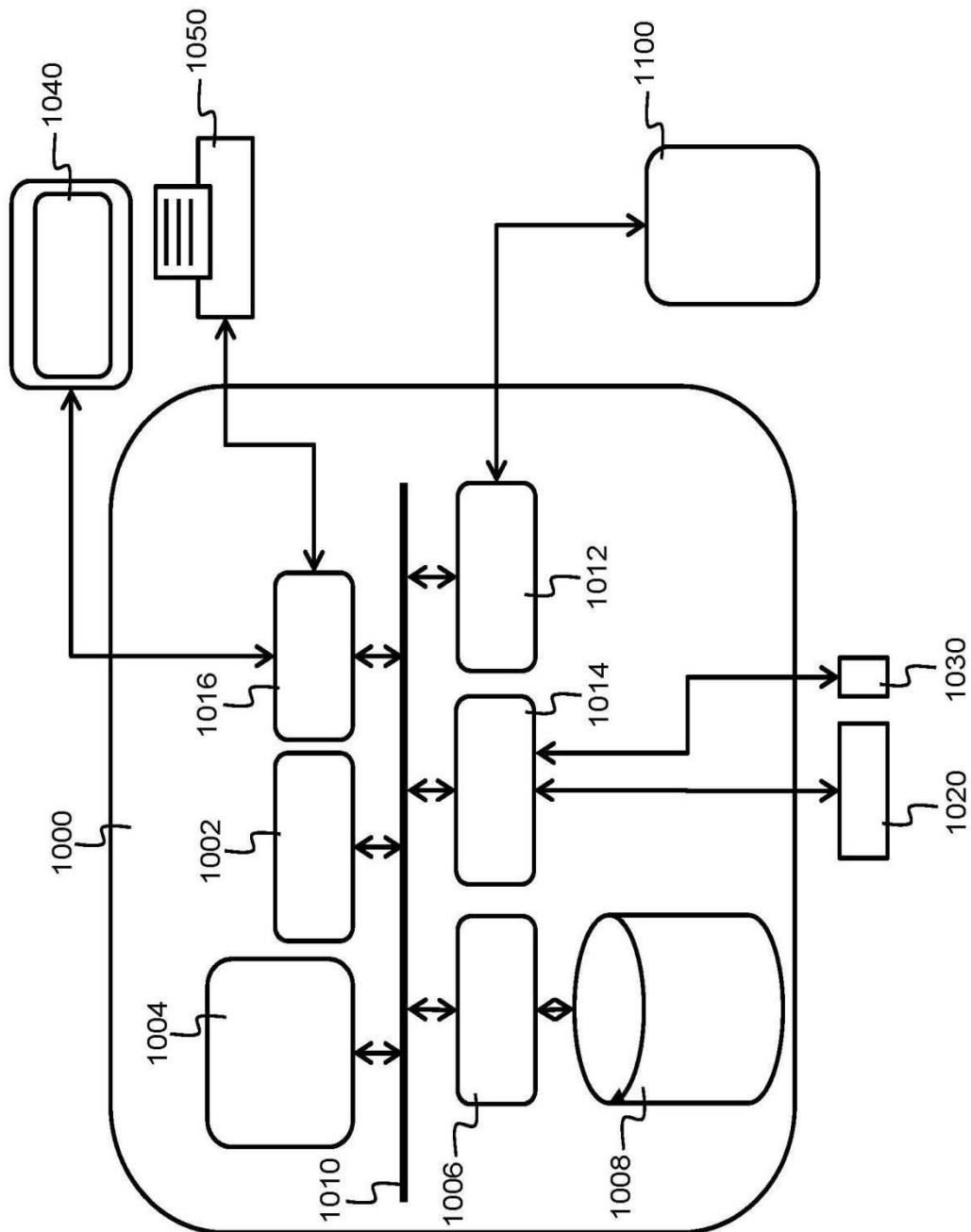


Figura 10



SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

NIT: 800.176.089-2

COMPROBANTE DE RECAUDO SISTEMA SIPI

Radicado: NC2017/0003283

Recibo: 18-60672

Fecha: 14/08/2018

CAROLINA MERCEDES DAZA MONTALVO

CC: 66.783.790

Pago PSE No: 206847

CUS: 360710539

Patente PCT

SISTEMAS Y MÉTODOS PARA PROTEGER DISPOSITIVOS DE RED

Detalle del pago

Id.	Rentístico	Concepto y Servicio	Cant.	Val. Unit.	Subtotal
1	50005-01-01	Solicitud examen de patentabilidad Patente de Invención (DESCUENTO INTERNET)	1	\$ 1,053,500	\$ 1,053,500
TOTAL					\$ 1,053,500