(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 690 474**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04L 29/08 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **11.05.2015 PCT/US2015/030223**

(87) Fecha y número de publicación internacional: **19.11.2015 WO15175438**

(96) Fecha de presentación y número de la solicitud europea: **11.05.2015 E 15726433 (4)**

(97) Fecha y número de publicación de la concesión europea: **11.07.2018 EP 3143746**

(54) Título: **Conexión de nube pública con recursos de red privada**

(30) Prioridad:

12.05.2014 US 201461992073 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
21.11.2018

(73) Titular/es:

MICROSOFT TECHNOLOGY LICENSING, LLC (100.0%)
One Microsoft Way
Redmond, WA 98052-6399, US

(72) Inventor/es:

CHANDWANI, SANTOSH y
KATTI, JAYTEERTH NARASINGRAO

(74) Agente/Representante:

CARPINTERO LÓPEZ, Mario

DESCRIPCIÓN

Conexión de nube pública con recursos de red privada

Antecedentes

Plataformas de alojamiento de nube pública alojan aplicaciones que usan recursos, tal como bases de datos y servicios. Convencionalmente, los recursos usados por tales aplicaciones alojadas en la nube pública también se ubican dentro de la nube pública. Si los recursos se ubican dentro de una red privada, entonces esos recursos se moverían a la nube pública para ser usador por tales aplicaciones. Sin embargo, por seguridad, razones de conformidad o legales, algunos recursos no pueden moverse a la nube pública.

Para permitir acceso a estos recursos en redes privadas, a menudo se requiere que administradores de red abran puertos en sus cortafuegos para permitir tráfico desde la internet en su red, desplegar intermediarios y/o pasarelas en la Zona Desmilitarizada (DMZ) de red que reenvía el tráfico externo al recurso o usa una Red Privada Virtual (VPN) para conectar la aplicación a su red privada.

La materia objeto revindicada en el presente documento no se limita a realizaciones que solucionan algunas desventajas o que operan únicamente en entornos tal como los descritos anteriormente. En su lugar, estos antecedentes se proporcionan únicamente para ilustrar un área de tecnología ilustrativa en la que pueden practicarse algunas realizaciones descritas en el presente documento.

La memoria descriptiva de la Patente US2012331528 desvela procedimientos de provisión a aplicaciones autorizadas que se ejecutan en una nube pública de acceso seguro a servicios seleccionados que se ejecutan en una infraestructura privada.

La memoria descriptiva de la Patente EP2228968 desvela mecanismo de puente seguro de interconexión de un entorno empresarial y un entorno informático en la nube.

Breve resumen

Al menos algunas realizaciones descritas en el presente documento se refieren a la provisión automática de una conexión entre una nube pública y un recurso local en una red privada. Esto permite que una conexión se haga más fácilmente cuando una aplicación en la nube pública tiene que acceder a ese recurso local en la red privada. La provisión automática se inicia tras la determinación de que una aplicación que se ejecuta en la nube pública tiene que acceder al recurso local. Ejemplos de recursos locales incluyen bases de datos, almacenamientos de datos, servicios web, servidores de aplicación y así sucesivamente.

La provisión se produce mediante la identificación de una infraestructura de puente que proporciona acceso al recurso local. La infraestructura de puente es parte de la infraestructura de nube pública y puede aprovisionarse o asignarse por un servicio designado para este fin. Seleccionar elementos de esta infraestructura de puente puede asignarse o crearse bajo demanda si se requiere. Se accede a continuación a credenciales usadas para acceder a la infraestructura de puente para uso posterior en conexión a la infraestructura de puente. Se proporcionan de forma segura y automáticamente credenciales específicas de la aplicación con derechos de envío al tiempo de ejecución de aplicación para la aplicación que tiene que acceder al recurso en la red privada. Las credenciales específicas de la aplicación son usables por un agente embebido en el tiempo de ejecución de la aplicación en la nube pública para conectar a la infraestructura de puente identificada. A continuación se crea un paquete de configuración incluyendo credenciales específicas del recurso, la identidad del recurso local y un ejecutable. Un usuario puede interactuar con el ejecutable para desplegar un intermediario en la red privada que proporciona conectividad segura entre el recurso local y la infraestructura de puente usando las credenciales específicas del recurso. El intermediario se ubica dentro de la red privada y usa comunicación saliente desde la red privada para conectar a la infraestructura de puente. Por lo tanto, los administradores de red no tienen que abrir puertos de cortafuegos o establecer conexiones VPN para que el intermediario se conecte a la infraestructura de puente.

Al menos algunas realizaciones descritas en el presente documento se refieren al establecimiento automático de la conexión entre una aplicación en la nube pública y el recurso local. En primer lugar, se accede a la infraestructura de puente automáticamente. La infraestructura de puente se configura para interactuar con un primer control dentro de la red privada. Por ejemplo, este primer control puede representarse como un intermediario alojado en la red privada y que se despliega mediante un ejecutable dentro del paquete de configuración usado en la provisión de la conexión. El intermediario se conecta de forma segura a la infraestructura de puente y reenvía tráfico entre la infraestructura de puente y el recurso local. Se proporciona un segundo control a la aplicación que se ejecuta en la nube pública. El segundo control se estructura de tal forma que la al menos una aplicación puede usarse para conectarse de forma segura a través de la infraestructura de puente con un recurso local de la red privada.

En un ejemplo, el segundo control puede realizarse como un agente embebido en el tiempo de ejecución de aplicación, ese control intercepta mensajes de la aplicación destinados para el recurso local, entrama el mismo en un mensaje de red apropiado o protocolo de tunelización y redirige los mismos a través de la infraestructura de puente hasta el primer control, que a su vez reenvía el mismo al recurso local. La respuesta sigue la trayectoria

inversa de vuelta a la aplicación en la nube pública.

Este resumen no se pretende para identificar características clave o características esenciales del objeto reivindicado, ni pretende usarse como una ayuda en la determinación del alcance del objeto reivindicado. La invención se define mediante las reivindicaciones adjuntas.

Breve descripción de los dibujos

Para describir la manera en que pueden obtenerse las ventajas y características anteriormente descritas y otras, se presentará una descripción más particular de diversas realizaciones mediante referencia a los dibujos adjuntos. Entendiendo que estos dibujos representan únicamente realizaciones de muestra y por lo tanto no deben considerarse como que limitan el alcance de la invención, las realizaciones se describirán y explicarán con especificación y detalle adicionales a través del uso de los dibujos adjuntos en los que:

la Figura 1 ilustra de forma abstracta un sistema informático en el que pueden emplearse algunas realizaciones descritas en el presente documento;
la Figura 2 ilustra un entorno en el que pueden operar los principios descritos en el presente documento, y que incluye una nube pública y una red privada interconectada con una infraestructura de puente;
la Figura 3 ilustra tres etapas temporales asociadas con la infraestructura de puente;
la Figura 4 ilustra un diagrama de flujo de un procedimiento de provisión de una conexión entre una nube pública y un recurso local en una red privada;
la Figura 5 ilustra un ejemplo específico de flujos de datos asociados con la provisión de una conexión entre una nube pública y un recurso local en una red privada;
la Figura 6 ilustra un diagrama de flujo de un procedimiento de establecimiento de acceso desde una nube pública a un recurso local en una red privada;
la Figura 7 ilustra un diagrama de flujo de un procedimiento de uso de la infraestructura de puente una vez conectada a la aplicación y el recurso local en la nube privada; y
la Figura 8 ilustra un procedimiento de tiempo de ejecución que muestra un ejemplo más específico de cómo la aplicación en la nube pública puede entonces acceder al recurso en la red privada usando la infraestructura de puente.

Descripción detallada

Al menos algunas realizaciones descritas en el presente documento se refieren a la provisión automática de una conexión entre una nube pública y un recurso local en una red privada. Esto permite que una conexión se haga más fácilmente cuando una aplicación en la nube pública tiene que acceder a ese recurso local en la red privada. La provisión automática se inicia tras la determinación de que una aplicación que se ejecuta en la nube pública tiene que acceder al recurso local. Ejemplos de recursos locales incluyen bases de datos, almacenamientos de datos, servicios web, servidores de aplicación y así sucesivamente.

La provisión se produce mediante la identificación de una infraestructura de puente que proporciona acceso al recurso local. La infraestructura de puente es parte de la infraestructura de nube pública y puede aprovisionarse o asignarse por un servicio designado para este fin. La identidad de red del recurso local se configura como metadatos para la infraestructura de puente. Elementos seleccionados de esta infraestructura de puente pueden asignarse o crearse bajo demanda si se requiere. Se accede a continuación a credenciales usadas para acceder a la infraestructura de puente para uso posterior en conexión a la infraestructura de puente. Se proporcionan de forma segura y automáticamente credenciales específicas de la aplicación con derechos de envío al tiempo de ejecución de aplicación para la aplicación que tiene que acceder al recurso en la red privada. Las credenciales específicas de la aplicación son usables por un agente embebido en el tiempo de ejecución de aplicación en la nube pública para conectar a la infraestructura de puente identificada. A continuación se crea un paquete de configuración incluyendo credenciales específicas del recurso, la identidad del recurso local y un ejecutable. Por ejemplo, el ejecutable puede identificarse mediante un Identificador de Recurso Uniforme (URI) que contiene la identidad de la infraestructura de puente y una contraseña de un único uso con los derechos recibidos que pueden usarse para acceder a la infraestructura de puente. Un usuario puede interactuar con el ejecutable para desplegar un intermediario en la red privada que proporciona conectividad entre el recurso local y la infraestructura de puente usando las credenciales específicas del recurso.

Al menos algunas realizaciones descritas en el presente documento se refieren al establecimiento automático de la conexión entre una aplicación en la nube pública y el recurso local. En primer lugar, se accede a la infraestructura de puente automáticamente. La infraestructura de puente se configura para interactuar con un primer control dentro de la red privada. Por ejemplo, este primer control puede representarse como un ejecutable dentro del paquete de configuración usado en la provisión de la conexión. El intermediario se conecta de forma segura a la infraestructura de puente y reenvía tráfico entre la infraestructura de puente y el recurso local. Se proporciona un segundo control a la aplicación que se ejecuta en la nube pública. El segundo control se estructura de tal forma que la al menos una aplicación puede usarse para conectarse de forma segura a través de la infraestructura de puente con un recurso local de la red privada.

En un ejemplo, el segundo control puede realizarse como un agente embebido en el tiempo de ejecución de aplicación, ese control intercepta mensajes de la aplicación destinados para el recurso local, entrama el mismo en un mensaje de red apropiado o protocolo de tunelización y redirige los mismos a través de la infraestructura de puente hasta el primer control, que a su vez reenvía el mismo al recurso local. La respuesta sigue la trayectoria inversa de vuelta a la aplicación en la nube pública.

Se describirá una descripción introductoria de un sistema informático con respecto a la Figura 1. A continuación, se describirán los principios de la provisión y utilización de una infraestructura de puente para permitir que una nube pública use recursos en una red privada con respecto a posteriores Figuras.

Sistemas informáticos ahora están tomando cada vez más una amplia variedad de formas. Sistemas informáticos pueden ser, por ejemplo, dispositivos portátiles, aplicaciones, ordenadores portátiles, ordenadores de sobremesa, ordenadores centrales, sistemas informáticos distribuidos, centros de datos o incluso dispositivos que convencionalmente no se han considerado un sistema informático, tal como dispositivos llevables (por ejemplo, gafas). En esta descripción y en las reivindicaciones, la expresión "sistema informático" se define ampliamente incluyendo cualquier dispositivo o sistema (o combinación de los mismos) que incluye al menos un procesador físico y tangible y una memoria física y tangible capaz de tener en la misma instrucciones ejecutables por ordenador que pueden ejecutarse mediante el procesador. La memoria puede tomar cualquier forma y puede depender de la naturaleza y forma del sistema informático. Un sistema informático puede distribuirse en un entorno de red y puede incluir múltiples sistemas informáticos constituyentes.

Como se ilustra en la Figura 1, en su configuración más básica, un sistema 100 informático habitualmente incluye al menos una unidad 102 de procesamiento de hardware y memoria 104. La memoria 104 puede ser una memoria de sistema física, que puede ser volátil, no volátil o alguna combinación de las dos. El término "memoria" también puede usarse en el presente documento para referirse a almacenamiento masivo no volátil tal como medio de almacenamiento físico. Si el sistema informático es distribuido, el procesamiento, memoria y/o capacidad de almacenamiento también puede ser distribuido. Como se usa en el presente documento, la expresión "módulo ejecutable" o "componente ejecutable" puede referirse a objetos de software, rutinas, o procedimientos que pueden ejecutarse el sistema informático. Los diferentes componentes, módulos, motores y servicios descritos en el presente documento pueden implementarse como objetos o procedimientos que se ejecutan en el sistema informático (por ejemplo, hilos separados).

En la descripción que sigue, se describen realizaciones con referencia a actos que se realizan por uno o más sistemas informáticos. Si tales actos se implementan en software, uno o más procesadores (del sistema informático asociado que realiza el acto) dirigen la operación del sistema informático en respuesta a haber ejecutado instrucciones ejecutables por ordenador. Por ejemplo, tales instrucciones ejecutables por ordenador pueden incorporarse en uno o más medios legibles por ordenador que forman un producto de programa informático. Un ejemplo de una operación de este tipo implica la manipulación de datos. Las instrucciones ejecutables por ordenador (y los datos manipulados) pueden almacenarse en la memoria 104 del sistema 100 informático. El sistema 100 informático también puede contener canales 108 de comunicación que permiten que el sistema 100 informático se comunique con otros sistemas informáticos a través de, por ejemplo, la red 110. El sistema 100 informático también incluye un visualizador, que puede usarse para visualizar representaciones visuales a un usuario.

Realizaciones descritas en el presente documento pueden comprender o utilizar un sistema informático de fin especial o fin general que incluye hardware informático, tal como, por ejemplo, uno o más procesadores y memoria de sistema, como se ha analizado en mayor detalle a continuación. Realizaciones descritas en el presente documento también incluyen medios físicos y otros legibles por ordenador para transportar o almacenar instrucciones ejecutables por ordenador y/o estructuras de datos. Tales medios legibles por ordenador pueden ser cualquier medio disponible que puede accederse mediante un sistema informático de fin general o fin especial. Medios legibles por ordenador que almacenan instrucciones ejecutables por ordenador son medios de almacenamiento físicos. Medios legibles por ordenador que transportan instrucciones ejecutables por ordenador son medios de transmisión. Por lo tanto, a modo de ejemplo, y no como limitación, realizaciones de la invención pueden comprender al menos dos distintivamente diferentes clases de medios legibles por ordenador: medios de almacenamiento y medios de transmisión.

Medio de almacenamiento legible por ordenador incluye RAM, ROM, EEPROM, CD-ROM u otro almacenamiento de disco óptico, almacenamiento de disco magnético u otros dispositivos de almacenamiento magnético, o cualquier otro medio de almacenamiento físico y tangible que puede usarse para almacenar medios de código de programa deseados en forma de instrucciones ejecutables por ordenador o estructuras de datos y que puede accederse mediante un sistema informático de fin general o fin especial.

Una "red" se define como uno o más enlaces de datos que habilitan el transporte de datos electrónicos entre sistemas informáticos y/o módulos y/o otros dispositivos electrónicos. Cuando se transfiere o proporciona información a través de una red u otra conexión de comunicaciones (ya sea por cable, inalámbrica o una combinación de cable o inalámbrica) a un sistema informático, el sistema informático ve apropiadamente la conexión como un medio de transmisión. Medio de transmisión puede incluir una red y/o enlaces de datos que pueden usarse para transportar medios de código de programa deseados en forma de instrucciones ejecutables por ordenador o

estructuras de datos y que pueden accederse mediante un sistema informático de fin general o fin especial. Combinaciones de lo anterior deberían incluirse también dentro del alcance de medios legibles por ordenador.

Además, tras alcanzar diversos componentes de sistema informático, medios de código de programa en forma de instrucciones ejecutables por ordenador o estructuras de datos pueden transferirse automáticamente desde medios de transmisión hasta medios de almacenamiento (o viceversa). Por ejemplo, instrucciones ejecutables por ordenador o estructuras de datos recibidos a través de una red o enlace de datos pueden almacenarse en memoria intermedia en RAM dentro de una módulo de interfaz de red (por ejemplo, una "NIC"), y a continuación finalmente transferirse a RAM de sistema informático y/o a menos medios de almacenamiento volátiles en un sistema informático. Por lo tanto, debería entenderse que medios de almacenamiento pueden incluirse en componentes de sistema informático que también (o incluso esencialmente) utilizan medios de transmisión.

Instrucciones ejecutables por ordenador comprenden, por ejemplo, instrucciones y datos que, cuando se ejecutan en un procesador, provocan que sistema informático de fin general, sistema informático de fin especial o dispositivo de procesamiento de fin especial realice una cierta función o grupo de funciones. Las instrucciones ejecutables por ordenador pueden ser, por ejemplo, binarias o incluso instrucciones que experimentan algo de traducción (tal como compilación) antes de ejecución directa por el procesador, tal como instrucciones de formato intermedio tal como lenguaje de ensamblaje o incluso código fuente. Aunque la materia objeto se ha descrito en lenguaje específico para características estructurales y/o actos metodológicos, se ha de entender que la materia objeto definida en las reivindicaciones adjuntas no necesariamente se limita a las características descritas o actos descritos anteriormente. En su lugar, las características descritas y actos se desvelan como formas de ejemplo de implementación de las reivindicaciones.

Los expertos en la materia apreciarán que la invención puede ponerse en práctica en entornos informáticos de red como muchos tipos de configuraciones de sistema informático, incluyendo, ordenadores personales, ordenadores de sobremesa, ordenadores portátiles, procesadores de mensajes, dispositivos portátiles, sistemas multiprocesador, electrónica basada en microprocesadores o de consumo programable, PC de red, miniordenadores, ordenadores centrales, teléfonos móviles, PDA, buscapersonas, encaminadores, conmutadores, centros de datos, dispositivos llevables (tal como gafas) y similares. La invención también puede practicarse en entornos de sistemas distribuidos en los que sistemas informáticos locales y remotos, que están vinculados (o bien por enlaces de datos por cable, enlaces de datos inalámbricos o por una combinación de enlaces de datos por cable e inalámbricos) a través de una red, realizan ambos tareas. En un entorno de sistema distribuido, módulos de programa pueden ubicarse tanto en dispositivos de almacenamiento de memoria locales como remotos.

De acuerdo con los principios described en el presente documento, aplicaciones que se alojan en nubes públicas se comunican con recursos en redes privadas remotas como si la aplicación estuviera ejecutándose localmente en es red privada. Adicionalmente, tal conectividad puede configurarse con solo unos pocos gestos. Teniendo un agente embebido en el tiempo de ejecución en el que la aplicación se aloja, tal conectividad puede establecerse con literalmente unos pocos gestos de configuración que incluyen 1) crear una representación lógica del recurso remoto con la infraestructura de puente asociada, 2) instalación de un intermediario para ese recurso remoto en la red privada que automáticamente se conecta a la infraestructura de puente y 3) automáticamente configurar el agente en el tiempo de ejecución de aplicación para interceptar el tráfico para el recurso remoto y dirigir el mismo a la infraestructura de puente. Una capacidad única de este mecanismo es que agrupaciones de aplicaciones enteras (o niveles) tal como los niveles web o móviles pueden moverse de redes privadas a nubes públicas sin ningún código o cambio de configuración mientras mantiene otros niveles críticos tal como bases de datos en las redes privadas seguras.

En esta descripción y las siguientes reivindicaciones, "informática en la nube" se define como un modelo para habilitar acceso de red bajo demanda a una agrupación compartida de recursos informáticos configurables (por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios). La definición de "informática en la nube" no se limita a ninguna de las otras numerosas ventajas que pueden obtenerse a partir de un modelo de este tipo cuando se despliegan apropiadamente.

Por ejemplo, informática en la nube se emplea en la actualidad en el mercado para ofrecer acceso bajo demanda conveniente y ubicuo a la agrupación compartida de recursos informáticos configurables. Adicionalmente, la agrupación compartida de recursos informáticos configurables puede aprovisionarse rápidamente a través de virtualización y liberarse con un esfuerzo de gestión o interacción de proveedor de servicio bajos y a continuación escalarse en consecuencia.

Un modelo informático en la nube puede componerse de diversas características tal como autoservicio bajo demanda, acceso de red ancho, agrupamiento de recursos, elasticidad rápida, servicio medido, y así sucesivamente. Un modelo informático en la nube puede venir también en forma de diversos modelos de servicio tal como, por ejemplo, Software como un Servicio ("SaaS"), Plataforma como un Servicio ("PaaS") e Infraestructura como un Servicio ("IaaS"). El modelo informático en la nube también puede desplegarse usando diferentes modelos de despliegue tal como nube privada, nube comunitaria, nube pública, nube híbrida y así sucesivamente. En esta descripción y en las reivindicaciones, un "entorno informático en la nube" es un entorno en el que se emplea informática en la nube.

La Figura 2 ilustra un entorno 200 en el que pueden operar los principios descritos en el presente documento. El entorno 200 incluye una nube 210 pública y una red 220 privada. La nube 210 pública tiene operando en la misma una diversidad de aplicaciones 211. Por ejemplo, la nube 210 pública se ilustra como que opera en la misma las aplicaciones 211A, 211B y 211C, aunque la elipse 211D representa flexibilidad en el número de aplicaciones operadas por una nube 210 pública. La aplicación 211A se ilustra ligeramente más grande ya que se usará como un ejemplo primario descrito en el presente documento. La nube 210 pública puede implementar un modelo informático en la nube que tiene muchos clientes - de ahí el término "público".

La red 220 privada tiene operando en la misma, recursos 221 locales. Por ejemplo, los recursos 221 locales se ilustran incluyendo los recursos 221A y 221B, aunque la elipse 221C representa que puede existir una gran diversidad de recursos operando dentro de la red 220 privada. El recurso 221A se ilustra ligeramente más grande ya que se usará como un ejemplo primario descrito en el presente documento. Ejemplos de recursos que pueden accederse incluyen, por ejemplo, bases de datos, servidores, almacenamiento, archivos, directorios y así sucesivamente. Existe también una infraestructura 230 de puente a usar por la aplicación 211A en la nube 210 pública para acceder al recurso 221A en la red 220 privada. Las flechas 231 a 238 representan un flujo de datos de ejemplo asociado con el uso de la infraestructura 230 de puente y se describirá adicionalmente a continuación en conjunción con la Figura 7.

Como se ilustra en la Figura 3, existen tres etapas 300 temporales asociadas con la infraestructura de puente. La etapa 310 de provisión se sigue por la etapa 320 de conexión, que se sigue por la etapa 330 de uso. El fin de la etapa 310 de provisión es hacer más fácil la etapa 320 de conexión y más automática de realizar. De hecho, la etapa 320 de conexión puede diferirse justo antes de la etapa 330 de uso, en el momento que la nube pública realmente usa la infraestructura 230 de puente para comunicarse con el recurso 221A local.

La Figura 4 ilustra un diagrama de flujo de un procedimiento 400 de provisión automática de una conexión entre una nube pública y un recurso local en una red privada. El procedimiento 400 es un ejemplo de la etapa 310 de provisión de la Figura 3. Ya que el procedimiento 400 puede realizarse en el entorno 200 de red de la Figura 2, el procedimiento 400 de la Figura 4 se describirán ahora con referencia frecuente a la Figura 2.

El procedimiento 400 se inicia tras la determinación de que una aplicación que se ejecuta en la nube pública tiene que acceder a un recurso local de la red privada (acto 401). Por ejemplo, un usuario dentro de la red 220 privada puede determinar que la aplicación 211A de la nube 210 pública tiene que acceder al recurso 221A de la red privada 210. Por ejemplo, la aplicación 211A puede requerir acceso al recurso 221A ubicado dentro de la red 220 privada para servir información o para procesar peticiones. Tal intento de acceder al recurso remoto puede indicarse o configurarse por el desarrollador de la aplicación 211A durante el desarrollo de la aplicación. Como alternativa, este intento puede determinarse durante el despliegue o configuración de la aplicación 211A por el administrador.

El procedimiento 400 se realiza mediante realización automática del contenido por debajo de la línea 410 tras la interacción del usuario con el control (por ejemplo, el hiperenlace). Específicamente, se identifica una estructura de puente que proporciona acceso al recurso local (acto 411). Esto podría incluirse como argumentos dentro del hiperenlace. Por consiguiente, el sitio web podría asignar la infraestructura de puente tras la provisión del usuario de la identidad del recurso local al sitio web. A continuación se accede a las credenciales usadas para conectar a la infraestructura de puente (acto 412). Esto incluye la credencial 251 específica de la aplicación que se proporciona a la aplicación 211A en la nube 210 pública (acto 413). Por ejemplo, en la Figura 2, la credencial 241 específica del recurso puede usarse para establecer un primer control 242 que conecta la infraestructura 230 de puente con el recurso 221A local. La credencial 242 específica de la aplicación puede usarse para establecer un segundo control 252 que conecta la infraestructura 230 de puente con la aplicación 211A.

Adicionalmente, el procedimiento 400 incluye crear (acto 414) un paquete de configuración que incluye credenciales específicas del recurso, un ejecutable para un control 242 y la identidad del recurso local. El ejecutable para el control 242 se configura para ejecutarse tras la selección del control por un usuario y proporciona conectividad entre el recurso local en red privada y la infraestructura de puente usando las credenciales específicas del recurso. En otras palabras, el ejecutable puede usarse para establecer el primer control 242.

Por consiguiente, tras la finalización del procedimiento 400, la red 220 privada del entorno 200 tiene credenciales 241 específicas del recurso y un control 242 con el que puede interactuarse (en el contexto de tener las credenciales 241 específicas del recurso) para establecer una conexión entre el recurso 221A y la infraestructura 230 de puente. Adicionalmente, la nube 210 pública tiene credenciales 251 específicas de la aplicación y un control 252 que puede usarse por la nube pública (en el contexto de tener las credenciales 251específicas de la aplicación) para establecer una conexión entre la aplicación 211A y la infraestructura 230 de puente.

El procedimiento puede realizarse múltiples veces para recursos diferentes en la red 220 privada para establecer una infraestructura de puente diferente para cada recurso local. Podría existir un control específico de recurso para cada recurso. En algunas realizaciones, si múltiples aplicaciones tienen que usar el mismo recurso local, el correspondiente control 242 puede usarse para conectar al recurso local para múltiples aplicaciones que se ejecutan en la nube pública. También podría existir un control específico de aplicación diferente para cada aplicación que se conecta al recurso local. En algunas realizaciones, si múltiples aplicaciones tienen que usar el mismo recurso local,

pueden compartir el mismo control 252. Las elipses 225 representan que infraestructuras de puente similares pueden establecerse entre la nube 210 pública y también otras redes privadas.

La Figura 5 ilustra un entorno de ejemplo en el que se provisiona la infraestructura de puente con el control 242 de intermediario de recurso establecido para alijarse en la red privada. En este diagrama, una nube pública se etiqueta como "Azure". Sin embargo, los principios described en el presente documento pueden aplicarse a cualquier nube pública para habilitar conectividad con recursos en una red privada, independientemente del proveedor o identidad de la nube pública. La frontera de confianza de la red privada se etiqueta como "Frontera de Confianza de Corpnet". La conexión entre la nube pública y la red privada para permitir que la aplicación en la nube pública acceda al recurso en la red privada se denominará en este documento como una "conexión híbrida".

En primer lugar, el usuario crea una conexión híbrida lógica que especifica la dirección de red del recurso remoto en la red privada. Esto automáticamente genera dos credenciales; una primera credencial (es decir, la credencial específica del recurso) con derechos de recepción en el intermediario local y una segunda credencial (es decir, la credencial específica de la aplicación) con derechos de envío para la aplicación en la nube pública. Esto también genera automáticamente una contraseña de un único uso efímera (OTP), e incorpora la contraseña como un parámetro de consulta en un enlace al intermediario de intermediario de recurso para la red privada (véase la flecha 1 en la Figura 5).

El usuario puede a continuación clicar en el enlace al intermediario local desde la red privada (véase la flecha 2 en la Figura 5). Esto provoca que la aplicación se descargue (véase la flecha 3 en la Figura 5). La aplicación extrae la contraseña de un único uso efímera (OTP) del parámetro de petición del enlace y usa la contraseña para adquirir la credencial con el derecho de recepción. La aplicación a continuación configura el servicio de intermediario ("Aplicación CO de gestor de conexión híbrida" en la Figura 5) en la red privada y proporciona a la misma la credencial con el derecho de recepción.

El servicio de intermediario en la red privada se inicia automáticamente a continuación. El servicio de intermediario usa la credencial con el derecho de recepción para determinar qué recurso local se diseña a intermediario, y a continuación se configura a sí mismo como un intermediario para ese servicio. Las flechas 4 a 10 en la Figura 5 muestran como podría producirse esto para una implementación particular, pero otra

La aplicación en la nube pública se configura con un enlace a la conexión híbrida lógica deseada que representa el recurso remoto en la red privada. La credencial con el derecho de envío se configura en la aplicación, y la aplicación conecta a la conexión híbrida lógica.

La Figura 6 ilustra un diagrama de flujo de un procedimiento 600 de establecimiento de acceso desde una nube pública a un recurso local en una red privada. El procedimiento 600 puede realizarse como parte de la etapa 320 de conexión de la Figura 3 y puede realizarse en el contexto del entorno 200 de la Figura 2. Por consiguiente, el procedimiento 600 de la Figura 6 se describirá ahora con referencia frecuente al entorno 200 de la Figura 2.

El procedimiento incluye automáticamente acceder (acto 601) a una infraestructura de puente que tiene que operar entre la nube pública y la red privada. Por ejemplo, haciendo referencia a la Figura 2, la infraestructura 230 de puente se configura para interactuar con un sistema de usuario dentro de la red 220 privada usando un primer control 242. El primer control 242 se estructura de tal forma que, cuando se configura con las credenciales específicas del recurso para la infraestructura de puente, el primer control 242 automáticamente establece una conexión segura a la infraestructura 230 de puente. Cuando se establece una conexión de este tipo, el primer control 242 identifica el recurso 221A local que la infraestructura 230 de puente se aprovisionó para acceder. Además, el primer control 242 se estructura para recibir tráfico interceptado desde la infraestructura 230 de puente, en la que se tráfico interceptado se reenvió en la infraestructura 230 de puente mediante el segundo control 252. El primer control 242 se configura a sí mismo para reenviar tráfico interceptado desde la infraestructura 230 de puente al recurso 221A. El segundo control 252 asimismo se configura para interceptar tráfico desde la aplicación 211A y destina para el recurso 221A local, entramando el mismo en un mensaje de entramado apropiado y reencaminando el mismo en la infraestructura 230 de puente. Adicionalmente, el segundo control 252 se proporciona (acto 602) a la aplicación que se ejecuta en la nube 210 pública. El segundo control 252 se estructura de tal forma que la aplicación 221A puede conectarse de forma segura a través de la infraestructura 230 de puente con un recurso local de la red privada. El segundo control 252 puede mantener siempre la conexión con la infraestructura 230 de puente o como alternativa la conexión puede establecerse bajo demanda. Si la conexión se establece bajo demanda, entonces como la aplicación 211A intenta acceder al recurso 221A (acto 603), el segundo control 252 finaliza la trayectoria comunicativa entre la aplicación 211A y el recurso 221A local.

La Figura 7 ilustra un diagrama de flujo de un procedimiento 700 de uso de la infraestructura de puente una vez conectada a la aplicación y el recurso local en la nube privada. El procedimiento 700 representa un ejemplo de la etapa 630 de uso de la Figura 6. El procedimiento 700 puede realizarse dentro del entorno 200 de la Figura 2 para provocar un número de flujos de datos 231 a 238 referenciados en la Figura 2. Por consiguiente, el procedimiento 700 de la Figura 7 se describirá ahora con respecto al entorno 200 de la Figura 2. Actos realizados por el segundo control se referencian en la columna izquierda de la Figura 7 bajo el encabezamiento ("Segundo Control") y se etiquetan en los 710. Actos realizados por el primer control se referencian en la columna derecha de la Figura 7 bajo

el encabezamiento ("Primer Control") y se etiquetan en los 720.

El segundo control intercepta primero (acto 711) una comunicación desde la aplicación que se destina para el recurso local. Por ejemplo, en la Figura 2, el segundo control 252 recibe (como se representa mediante la flecha 231) la comunicación desde la aplicación 211A. Esta comunicación puede estructurarse igual que sería si el recurso fuera a accederse desde dentro de la nube pública. Por consiguiente, la propia aplicación 211A puede ser completamente agnóstica acerca de donde se ubica realmente el recurso. La existencia del canal de comunicación establecido por el primer control 242, el segundo control 252 y la infraestructura 230 de puente puede ser algo que se abstrae de la vista de la aplicación 211A.

El segundo control a continuación entrama el mensaje original desde la aplicación 211A usando un mecanismo de entramado o tunelización apropiado y redirige (acto 712) la comunicación a través de la infraestructura de puente de encaminamiento mediante el primer control al recurso local. El entramado del mensaje original conserva cualquier encabezamiento de mensaje u otra información de control que puede adquirirse para control de acceso o para procesar correctamente el mensaje original mediante el recurso local. Por supuesto esta comunicación puede cifrarse por seguridad. Por ejemplo, en la Figura 2, el segundo control 252 se ilustra como que redirige (representado por la flecha 232) la comunicación a través de la infraestructura 230 de puente.

El primer control a continuación recibe la comunicación redirigida a través de la infraestructura de puente (acto 721). Por ejemplo, en la Figura 2, el primer control 242 se ilustra como que recibe la comunicación (representado mediante la flecha 233). El primer control a continuación elimina el entramado del mensaje original y redirige la comunicación al recurso local (acto 722). Por ejemplo, en la Figura 2, el primer control 242 se ilustra como que redirige la comunicación (representado mediante la flecha 234) al recurso 221A local. Si no hay respuesta a la comunicación desde el recurso local ("No" en el bloque de decisión 723), entonces el procedimiento 700 puede finalizar a continuación.

Si hay una respuesta a la comunicación ("Sí" en el bloque de decisión 723), entonces el primer control recibe esa respuesta (acto 724), la entrama usando el mecanismo de entramado elegido y reenvía esa respuesta a través de la infraestructura de puente (acto 725). Por ejemplo, en la Figura 2, el primer control 242 recibe una respuesta (como se representa mediante la flecha 235) desde el recurso 221A local y redirige la respuesta (como se representa mediante la flecha 236) en la infraestructura 230 de puente.

El segundo control recibe la respuesta (acto 713) a través de la infraestructura de puente, elimina el entramado añadido por el primer control y redirige la respuesta original desde el recurso local a la aplicación 211A (acto 714). Por ejemplo, en la Figura 2, el segundo control 242 recibe la respuesta (como se representa mediante la flecha 237) a través de la infraestructura 230 de puente y redirige la respuesta (como se representa mediante la flecha 238) de vuelta a la aplicación. En algunas realizaciones, la respuesta 1 puede parecer la misma o tener el mismo esquema independientemente de si el recurso local estaba dentro de la nube pública o la red privada.

La Figura 8 ilustra un procedimiento de tiempo de ejecución que muestra un ejemplo más específico de cómo la aplicación en la nube pública puede entonces acceder al recurso en la red privada usando la infraestructura de puente. En este caso, la aplicación es un sitio web. De nuevo, aunque la aplicación se etiqueta como un sitio web de "Azure", los principios descritos en el presente documento no se limitan a ninguna identidad o proveedor de nuble pública particulares y no se limita al proveedor o identidad de aplicación que está solicitando el recurso de red privada. En cualquier caso, la aplicación se dirige a un recurso remoto (que no puede alcanzarse directamente desde la nube pública) como si se ubicase proximalmente y si fuera directamente accesible:

La plataforma de nube pública en la que se aloja la aplicación incorpora un agente en el tiempo de ejecución de aplicación. El agente (el agente de conexión híbrida en la Figura 8) determina la conexión híbrida lógica a la que se vincula la aplicación y la información de dirección/puerto del recurso remoto que representa. El agente intercepta todo el tráfico desde la aplicación destinada para ese recurso remoto, usa el NetTcpRelayBinding para el entramado del mensaje original y lo envía a la conexión híbrida. Mientras se usa el NetTcpRelayBinding en este ejemplo específico, pueden usarse otros mecanismos de entramado o protocolos de tunelización.

La conexión híbrida reenvía todas las peticiones enviadas por la aplicación al intermediario de recurso ("servicio de gestor de conexión híbrida" en la Figura 8) alojado en la red privada para el reenvío adicional al recurso remoto. Adicionalmente, la conexión híbrida reenvía a la aplicación todas las respuestas enviadas por el recurso remoto.

El servicio de intermediario en la red privada usa conectividad de red saliente (por ejemplo, a través de TCP, HTTP, HTTPS o WebSockets) para escuchar en busca de peticiones de conexión desde la nube pública. Peticiones de conexión desde aplicaciones en la nube pública se reenvían continuación al recurso en la red privada y las respuestas se devuelven a las aplicaciones en la nube pública. El intermediario elimina el entramado del NetTcpRelayBinding del mensaje original antes de reenviar el mismo al recurso, y a la inversa añade el entramado cuando revuelve la respuesta desde el recurso a la aplicación.

Por consiguiente, los principios descritos en el presente documento proporcionan un mecanismo conveniente un altamente automatizado de provisión, conexión y uso de una infraestructura de puente que permite que una aplicación en una nube pública se conecte a un recurso local. Las realizaciones descritas deben considerarse en

todos los respectos únicamente como ilustrativas y no restrictivas. El alcance de la invención se indica, por lo tanto, mediante las reivindicaciones adjuntas en lugar de mediante la descripción anterior. Todos los cambios que entran dentro del significado y alcance de equivalencia de las reivindicaciones deben incluirse dentro de su ámbito.

REIVINDICACIONES

1. Un procedimiento de provisión automática de una conexión entre una nube pública y un recurso local en una red privada, comprendiendo el procedimiento:

un acto de determinación de que una aplicación que se ejecuta en la nube pública tiene que acceder a un recurso local de la red privada;
un acto de realización automática de lo siguiente en respuesta al acto de determinación:

un acto de identificación de una infraestructura de puente que proporciona acceso al recurso local;
un acto de acceso a credenciales usadas para conectar a la infraestructura de puente;
un acto de provisión de forma segura de credenciales específicas de la aplicación a la aplicación en la nube pública, siendo las credenciales específicas de la aplicación usables por un

agente en la nube pública para conectar a la infraestructura de puente identificada; **caracterizado porque** el acto de realización automática comprende además un acto de creación de un paquete de configuración que incluye credenciales específicas del recurso, un ejecutable para un control y la identidad del recurso local, estando el ejecutable para el control configurado para ejecutarse tras selección por un usuario y proporciona conectividad entre el recurso local en red privada y la infraestructura de puente usando las credenciales específicas del recurso.

2. El procedimiento de acuerdo con la reivindicación 1, siendo el recurso local en la red privada un primer recurso local en la red privada, siendo la infraestructura de puente una primera infraestructura de puente, siendo las credenciales primeras credenciales, siendo las credenciales específicas de la aplicación primeras credenciales específicas de la aplicación, siendo las credenciales específicas del recurso primeras credenciales específicas del recurso, el procedimiento comprendiendo además:

un acto de determinación de que la aplicación que se ejecuta en la nube pública tiene que acceder a un segundo recurso local de la red privada;
un acto de realización automática de lo siguiente en respuesta al acto de determinación de que la aplicación que se ejecuta en la nube pública tiene que acceder al segundo recurso local de la red privada:

un acto de identificación de una segunda infraestructura de puente que proporciona acceso al segundo recurso local;
un acto de acceso a segundas credenciales usadas para conectar a la segunda infraestructura de puente;
un acto de provisión de forma segura de segundas credenciales específicas de la aplicación a la aplicación en la nube pública, siendo las segundas credenciales específicas de la aplicación usables por un agente en la nube pública para conectar a la segunda infraestructura de puente; y
un acto de creación de un paquete de configuración que incluye segundas credenciales específicas del recurso y la identidad del segundo recurso local, proporcionando la ejecución del ejecutable para el control conectividad entre el segundo recurso local en red privada y la segunda infraestructura de puente usando las segundas credenciales específicas del recurso.

3. El procedimiento de acuerdo con la reivindicación 1, siendo el recurso local un servidor.

4. El procedimiento de acuerdo con la reivindicación 1, siendo el recurso local una base de datos.

5. El procedimiento de acuerdo con la reivindicación 1, siendo el recurso local almacenamiento.

6. El procedimiento de acuerdo con la reivindicación 1, comprendiendo el acto de determinación de que una aplicación que se ejecuta en la nube pública tiene que acceder a un recurso local de la red privada:
un acto de navegación a un sitio web e indicación a ese sitio web que el recurso local tiene que hacerse disponible a la nube pública.

7. El procedimiento de acuerdo con la reivindicación 6, comprendiendo el acto de determinación además:
un acto de recepción de un control que es único a la infraestructura de puente y recurso local, y que es seleccionable para obtener la credencial específica del recurso.

8. El procedimiento de acuerdo con la reivindicación 7, comprendiendo el acto de determinación además:
un acto del usuario seleccionando el control iniciando de este modo el acto de realización automática.

9. El procedimiento de acuerdo con la reivindicación 7, siendo el control un hiperenlace.

10. Un producto de programa informático que comprende uno o más medios de almacenamiento legible por ordenador que tiene en el mismo instrucciones ejecutables por ordenador que están estructuradas de tal forma que, cuando se ejecutan por uno o más procesadores del sistema informático, provocan que el sistema informático realice el procedimiento de la reivindicación 1.

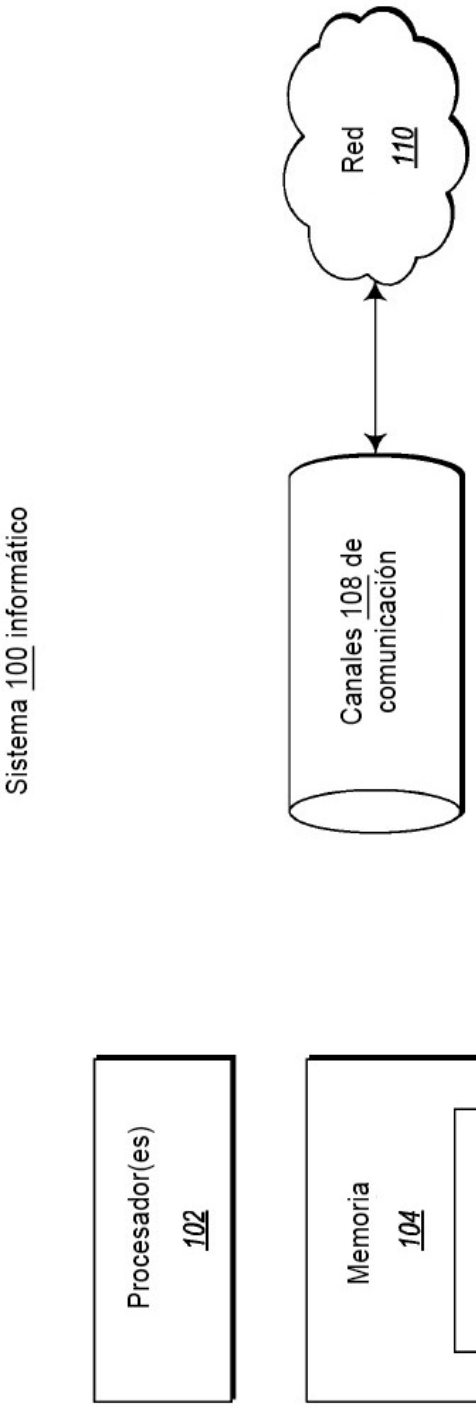
Sistema 100 informático
Red 110
Canales 108 de comunicación
Procesador(es) 102
Memoria 104
Volátil
No volátil

Figura 1

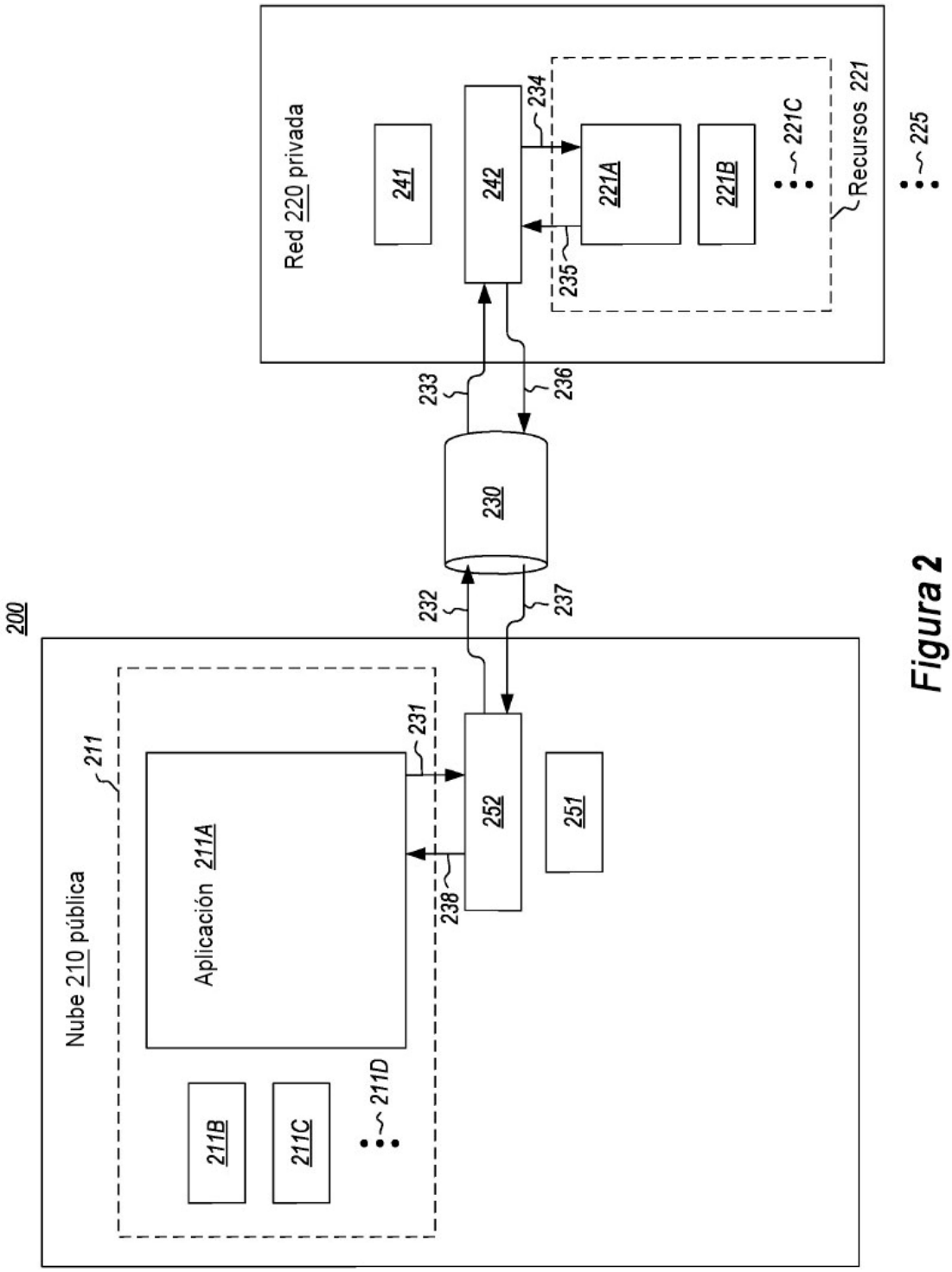
200
Nube 210 pública
211
Aplicación 211A
211B
211C
211D
231
252
251
238
232
237
230
233
236
Red 220 privada
241
242
234
235
221A
221B
221C
Recursos 221
225

Figura 2

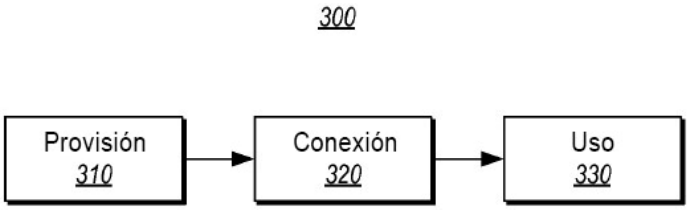

Figura 3

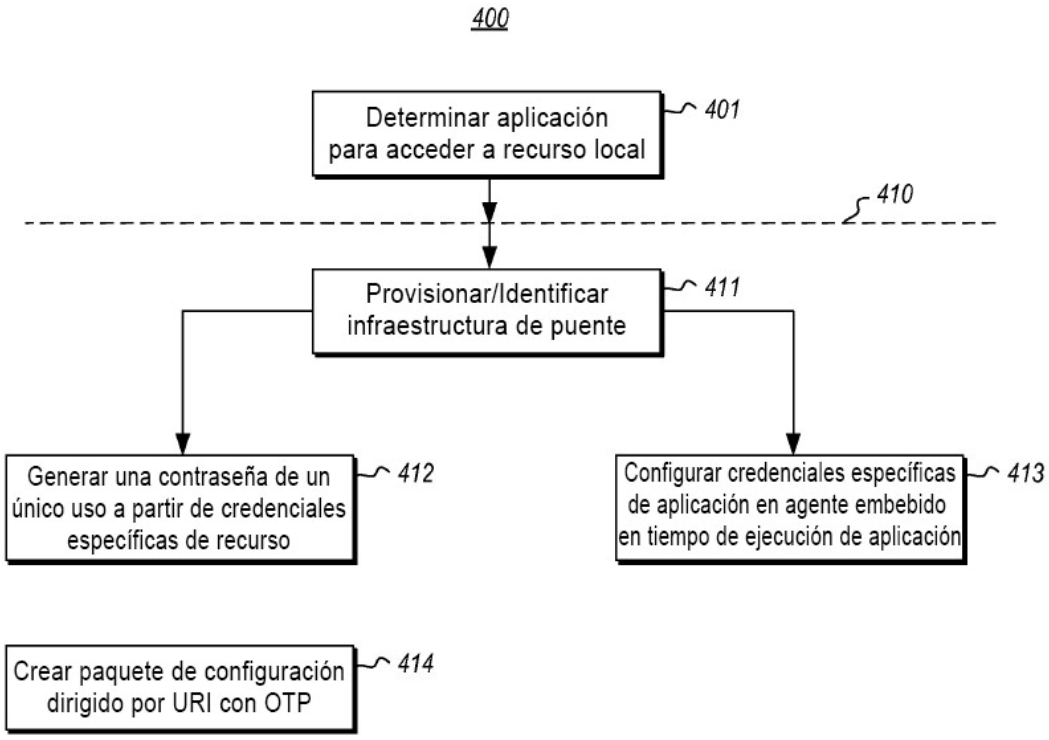

Figura 4

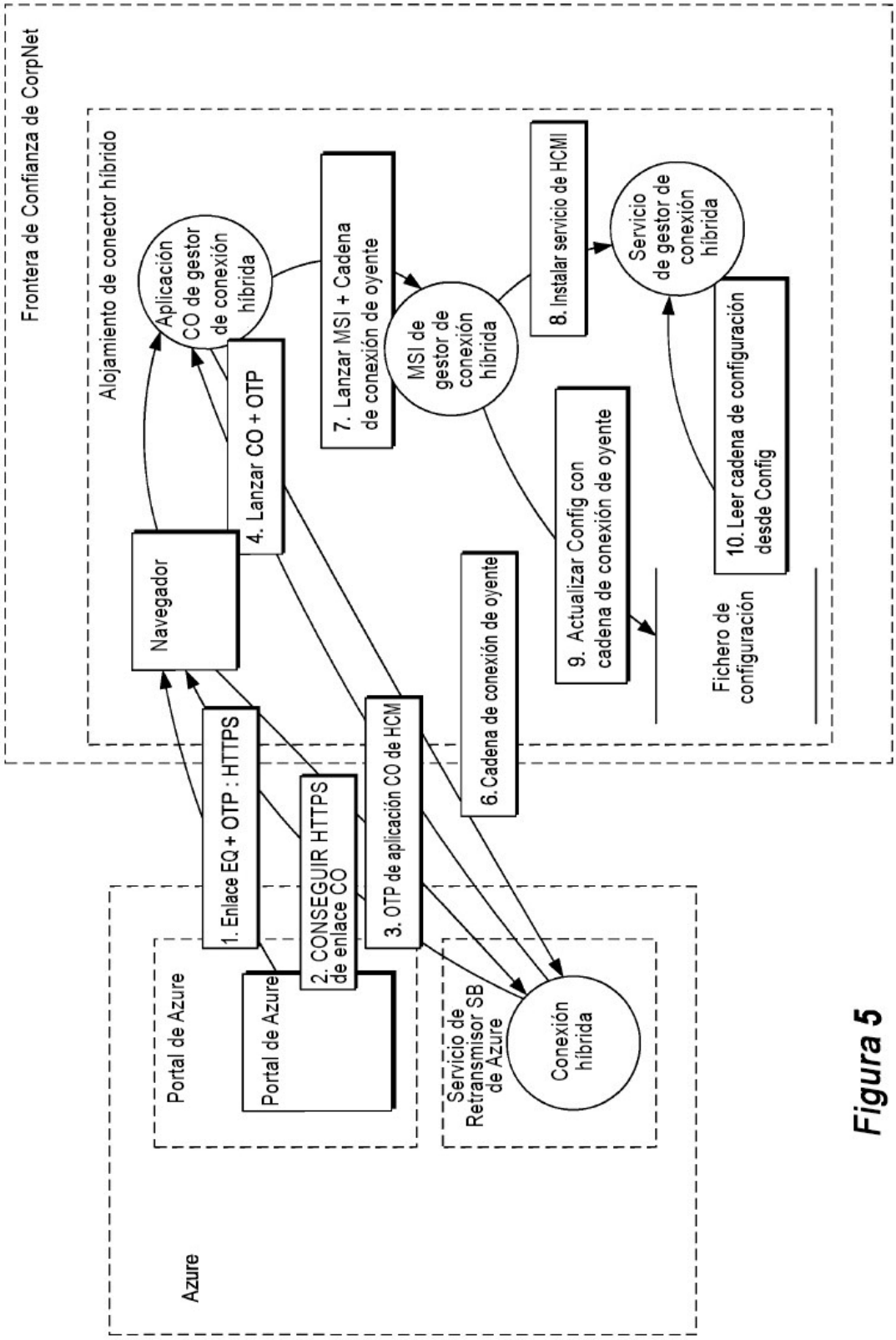
Frontera de Confianza de CorpNet
Alojamiento de conector híbrido
Aplicación CO de gestor de conexión híbrida
4. Lanzar CO + OTP
7. Lanzar MSI + Cadena de conexión de oyente
MSI de gestor de conexión híbrida
8. Instalar servicio de HCMI
Servicio de gestor de conexión híbrida
Navegador
9. Actualizar Config con cadena de conexión de oyente
10. Leer cadena de configuración desde Config
Fichero de configuración
6. Cadena de conexión de oyente
1. Enlace EQ + OTP : HTTPS
2. CONSEGUIR HTTPS de enlace CO
3. OTP de aplicación CO de HCM
Portal de Azure
Portal de Azure
Servicio de Retransmisor SB de Azure
Conexión híbrida
Azure

Figura 5

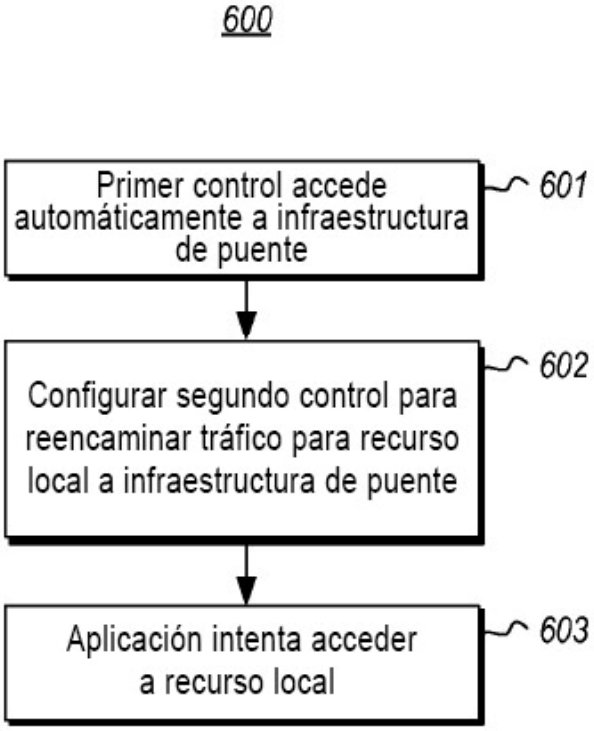
600
Primer control accede automáticamente a infraestructura de puente
601
Configurar segundo control para reencaminar tráfico para recurso local a infraestructura de puente
602
Aplicación intenta acceder a recurso local
603

Figura 6

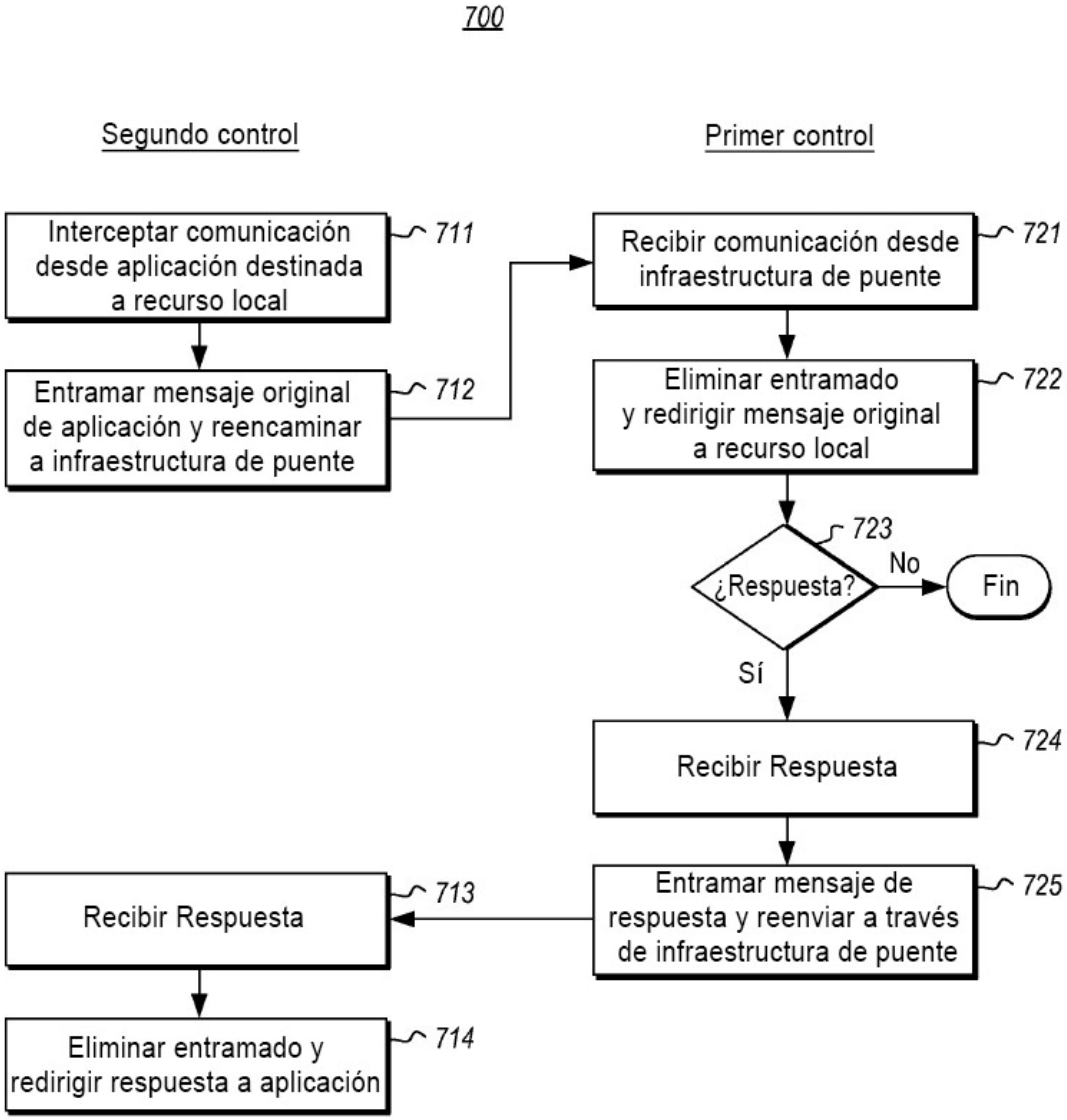
700
Segundo control
Primer control
Interceptar comunicación desde aplicación destinada a recurso local
711
Entramar mensaje original de aplicación y reencaminar a infraestructura de puente
712
Recibir comunicación desde infraestructura de puente
721
Eliminar entramado y redirigir mensaje original a recurso local
722
723
¿Respuesta?
No
Fin
Sí
Recibir Respuesta
724
Entramar mensaje de respuesta y reenviar a través de infraestructura de puente
725
Recibir Respuesta
713
Eliminar entramado y redirigir respuesta a aplicación
714

Figura 7

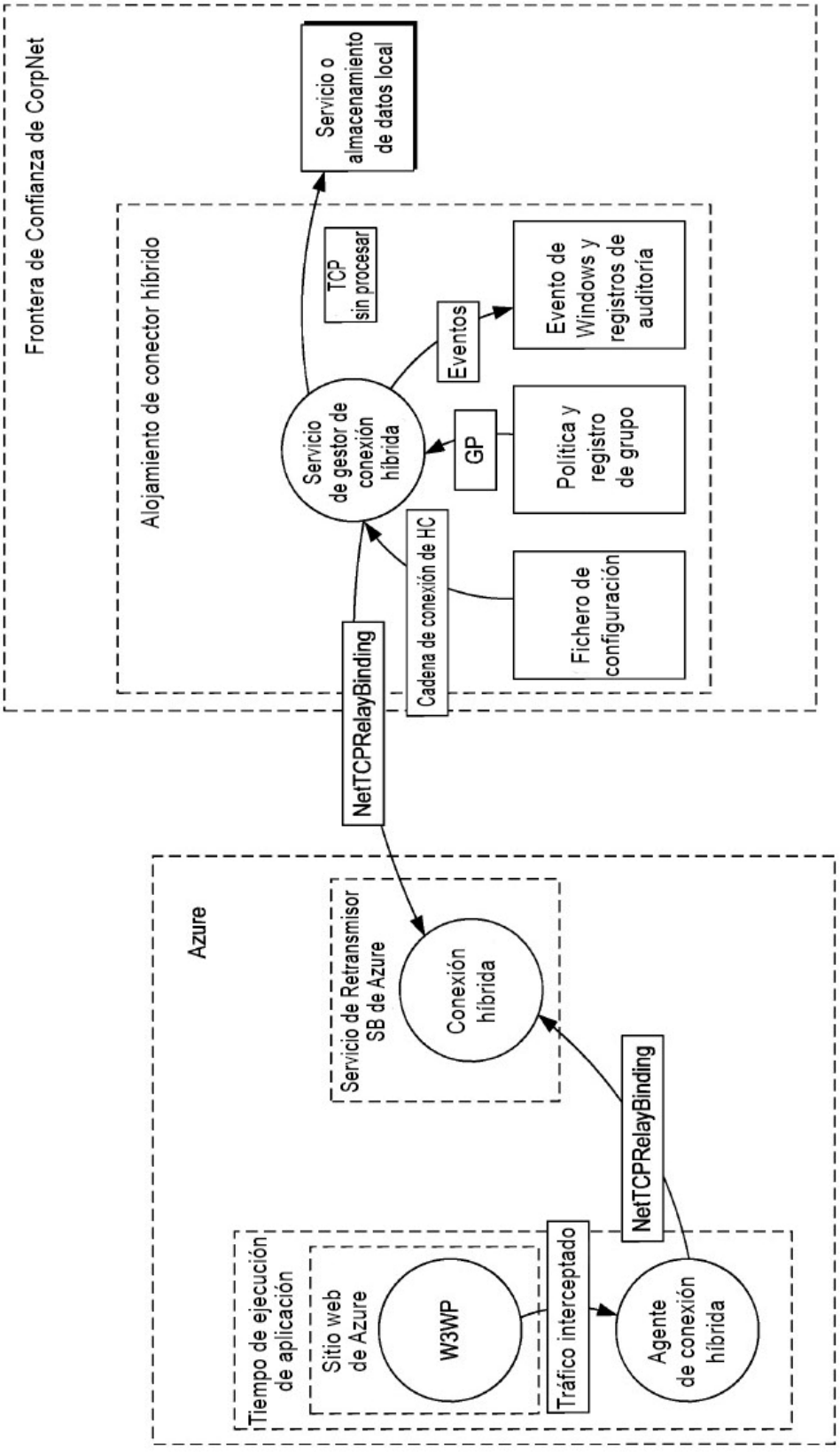
Frontera de Confianza de CorpNet
Alojamiento de conector híbrido
Servicio o almacenamiento de datos local
TCP sin procesar
Eventos
Evento de Windows y registros de auditoría
Servicio de gestor de conexión híbrida
GP
Política y registro de grupo
Cadena de conexión de HC
Fichero de configuración
NetTCPRelayBinding
Azure
Servicio de Retransmisor SB de Azure
Conexión híbrida
NetTCPRelayBinding
Tiempo de ejecución de aplicación
Sitio web de Azure
W3WP
Tráfico interceptado
Agente de conexión híbrida

Figura 8