(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 806 379**

(51) Int. CI.:

***G06F 21/53*** (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **25.05.2017 PCT/US2017/034354**

(87) Fecha y número de publicación internacional: **07.12.2017 WO17210065**

(96) Fecha de presentación y número de la solicitud europea: **25.05.2017 E 17728376 (9)**

(97) Fecha y número de publicación de la concesión europea: **13.05.2020 EP 3465517**

(54) Título: **Aislamiento de seguridad virtualizado basado en hardware**

(30) Prioridad:

**02.06.2016 US 201615171917**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
**17.02.2021**

(73) Titular/es:

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

(72) Inventor/es:

**PAI, NAVIN NARAYAN;**
**JEFFRIES, CHARLES G.;**
**VISWANATHAN, GIRIDHAR;**
**SCHULTZ, BENJAMIN M.;**
**SMITH, FREDERICK J.;**
**REUTHER, LARS;**
**EBERSOL, MICHAEL B.;**
**DIAZ CUELLAR, GERARDO;**
**PASHOV, IVAN DIMITROV;**
**GADDEHOSUR, POORNANANDA R.;**
**PULAPAKA, HARI R. y**
**RAO, VIKRAM MANGALORE**

(74) Agente/Representante:

**ELZABURU, S.L.P**

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín Europeo de Patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre Concesión de Patentes Europeas).

## DESCRIPCIÓN

Aislamiento de seguridad virtualizado basado en hardware

### Antecedentes

Las infecciones de los dispositivos informáticos a menudo ocurren cuando los usuarios navegan por Internet a sitios web no de confianza o cuando descargan o abren recursos de red no de confianza, tales como aplicaciones y documentos. Estas infecciones permiten a los atacantes robar las credenciales del usuario o incluso tomar el control del dispositivo informático para reutilizarlo para los propios medios del atacante. Si bien una solución para combatir estos ataques a nivel de núcleo es cerrar el acceso de red al dispositivo informático, esto limita severamente la funcionalidad de muchos dispositivos informáticos modernos. Además, en un entorno de trabajo, deshabilitar el acceso a la red dificulta la productividad de los empleados y la satisfacción laboral. Como compromiso, muchos empleadores permiten un acceso limitado a la red impidiendo que los empleados accedan a recursos de red no de confianza. Sin embargo, este acceso limitado a la red da como resultado mayores costos de administración para el empleador, ya que el empleador debe actualizar constantemente la política que define qué recursos de la red no son de confianza. Esto puede llevar a la frustración con el uso de dispositivos informáticos tanto por los usuarios como por el empleador.

El documento US2015/150142 enseña un sistema informático y un método para interceptar una tarea desde una cuenta de usuario principal antes de la ejecución de la tarea por el dispositivo informático, donde la tarea se relaciona con un contenido no de confianza. Se proporciona un entorno de aislamiento de tareas para ejecutar la tarea, incluyendo la creación de manera programática de una cuenta de usuario secundaria en el dispositivo de informático.

El documento US9245108 enseña el ajuste dinámico del formato de un archivo para permitir que otras partes determinen la confiabilidad del archivo.

El documento US2011047613 enseña una herramienta de entorno aislado para cooperar con los componentes de un sistema operativo seguro para crear un entorno de ejecución aislado para acceder al contenido no de confianza sin exponer otros procesos y recursos del sistema informático al contenido no de confianza.

### Compendio

Según aspectos de la presente invención, se proporciona un método y dispositivo como se define en las reivindicaciones adjuntas.

### Breve descripción de los dibujos

La descripción detallada se describe con referencia a las figuras adjuntas. En las figuras, el dígito o los dígitos más a la izquierda de un número de referencia identifican la figura en la que aparece primero el número de referencia. El uso de los mismos números de referencia en diferentes instancias en la descripción y las figuras puede indicar elementos similares o idénticos. Las entidades representadas en las figuras pueden ser indicativas de una o más entidades y, por lo tanto, se puede hacer referencia indistintamente a formas individuales o plurales de las entidades en la discusión.

La Figura 1 ilustra un sistema de ejemplo que implementa el aislamiento de seguridad virtualizado basado en hardware de acuerdo con una o más realizaciones.

La Figura 2 ilustra una arquitectura de sistema de ejemplo para el aislamiento de seguridad virtualizado basado en hardware de acuerdo con una o más realizaciones.

La Figura 3 es un diagrama de flujo que ilustra un proceso de ejemplo para implementar el aislamiento de seguridad virtualizado basado en hardware de acuerdo con una o más realizaciones.

La Figura 4 es un diagrama de flujo que ilustra un proceso de ejemplo para activar un contenedor para el aislamiento de seguridad virtualizado basado en hardware de acuerdo con una o más realizaciones.

La Figura 5 es un diagrama de flujo que ilustra un proceso de ejemplo para gestionar un contenedor para el aislamiento de seguridad virtualizado basado en hardware de acuerdo con una o más realizaciones.

La Figura 6 es un diagrama de flujo que ilustra un proceso de ejemplo para implementar el aislamiento de seguridad virtualizado basado en hardware de acuerdo con una o más realizaciones.

La Figura 7 ilustra un sistema de ejemplo que incluye un dispositivo informático de ejemplo que es representativo de uno o más sistemas y/o dispositivos que pueden implementar las diversas técnicas descritas en la presente memoria.

**Descripción detallada**

El aislamiento de seguridad virtualizado basado en hardware se trata en la presente memoria. Un sistema operativo que se ejecuta en un dispositivo informático, también denominado en la presente memoria como sistema operativo central que se ejecuta en un dispositivo central, utiliza contenedores para la partición de recursos de hardware. A diferencia de muchos enfoques basados en máquinas virtuales o entorno aislado, el uso de contenedores junto con las técnicas de aislamiento de seguridad virtualizado basado en hardware descritas en la presente memoria protegen el dispositivo informático de los ataques al aislar los navegadores web, las aplicaciones relacionadas y los componentes del sistema operativo tales como el núcleo, el sistema de archivos y la red de recursos de red no de confianza. El aislamiento de los recursos de red no de confianza se aplica y supervisa a través de uno o más filtros del sistema operativo y gestores de políticas. De esta manera, cuando el dispositivo central solicita acceso a un recurso de red no de confianza, el dispositivo central contiene el recurso de red no de confianza dentro de uno o más contenedores que proporcionan un aislamiento completo del núcleo del sistema operativo host. Como se discute en la presente memoria, los recursos de red se refieren a ubicaciones (por ejemplo, de dispositivos o donde residen los datos) a las que el dispositivo central puede acceder a través de una red, así como a uno o más datos, ejecutables o conexiones de red proporcionados por uno o más de las ubicaciones. Por ejemplo, los recursos de red pueden ser archivos, aplicaciones, correos electrónicos, documentos, Localizadores Uniformes de Recursos (URL), direcciones de Protocolo de Internet (IP), puertos de Protocolo de Control de Transmisión (TCP), nombre del Sistema de Nombres de Dominio (DNS), almacenes de datos, dispositivos de hardware, o combinaciones de los mismos. Un recurso de red de confianza se refiere a un recurso de red que es de confianza para no tener software malicioso o ser utilizado por usuarios malintencionados, y está identificado por una o más políticas para el dispositivo central. Un recurso de red no de confianza se refiere a un recurso de red que no es de confianza (por ejemplo, que puede tener software malicioso o ser utilizado por usuarios malintencionados).

Para proteger el dispositivo central de ataques maliciosos, la política se utiliza para definir una lista enumerada de recursos de red de confianza. En un entorno empresarial en el que varios usuarios de la empresa están conectados y comparten acceso a redes y datos empresariales comunes, un administrador de la empresa puede definir esta política para asegurar que los usuarios individuales, así como los datos y redes compartidos de la empresa la empresa permanecen protegidos. Cuando un usuario del dispositivo central solicita acceso a un recurso de red, el recurso de red solicitado se compara con la política para determinar si el recurso de red solicitado es un recurso de red de confianza. Si la política indica que el recurso de red solicitado es un recurso de red de confianza, las técnicas de aislamiento de seguridad virtualizado basado en hardware descritas en la presente memoria permiten que el sistema operativo central acceda al recurso de red de confianza. La política se puede aprovechar además para aislar las interfaces de red de un dispositivo informático que implementa las técnicas de aislamiento de seguridad virtualizado descritas en la presente memoria al restringir el acceso a una o más comunicaciones de red del dispositivo central para recursos de red no de confianza. Por ejemplo, si un dispositivo central admite comunicaciones de red de área local inalámbrica (WLAN), comunicaciones de banda ancha móvil, conexiones de acceso por línea conmutada, conexiones de red privada virtual (VPN) y conexiones directas tales como cableado en serie, cableado directo o un enlace de infrarrojos, las comunicaciones de red pertenecientes a recursos de red no de confianza pueden restringirse a las comunicaciones WLAN.

Cuando la política no define un recurso de red solicitado como un recurso de red de confianza, se determina que el recurso de red solicitado no es de confianza. En respuesta a la determinación de que un recurso de red no es de confianza, las técnicas de aislamiento de seguridad virtualizado basado en hardware descritas en la presente memoria activan un contenedor que está aislado del sistema operativo central. Luego se accede al recurso de red no de confianza desde el contenedor para aislar cualquier actividad peligrosa asociada con el recurso de red no de confianza. Debido al aislamiento, cualquier contenido malicioso o ataques que resulten del recurso de red no de confianza no podrán salir del contenedor para infectar el sistema operativo central. Las técnicas de aislamiento de seguridad virtualizado basado en hardware descritas en la presente memoria están configuradas además para supervisar la actividad dentro de un contenedor para asegurar que el contenedor no obtenga acceso a ningún recurso de red de confianza.

En consecuencia, al activar contenedores para acceder a recursos de red no de confianza, las técnicas de aislamiento de seguridad virtualizado basado en hardware descritas en la presente memoria crean dos o más instancias separadas de un sistema operativo o entorno de tiempo de ejecución contenido, cada uno con conectividad de red. Al supervisar los datos y las operaciones realizadas dentro de estos entornos de tiempo de ejecución contenido, las técnicas de aislamiento de seguridad virtualizado basado en hardware descritas en este documento se configuran para evitar que el sistema operativo central acceda a los recursos de red no de confianza. Las técnicas de aislamiento de seguridad virtualizado basado en hardware descritas en la presente memoria además permiten que un sistema central escanee y comparta información de DNS y Protocolo de Transferencia de Hipertexto (HTTP) desde el sistema operativo central seguro para mejorar el rendimiento de navegación web u otra actividad de red dentro de uno o más de los contenedores aislados.

Las técnicas de aislamiento de seguridad virtualizado basado en hardware descritas en la presente memoria permiten adicionalmente que un sistema operativo central descargue y acceda a archivos de forma aislada, como en uno o más contenedores que están separados del núcleo del sistema operativo central. Esto permite que el sistema

operativo central escanee recursos de red individuales tales como archivos, aplicaciones, sitios web, etc. para determinar un nivel de riesgo asociado con los individuales del recurso de red escaneada.

Las técnicas de aislamiento de seguridad virtualizado basado en hardware discutidas en la presente memoria también están configuradas para conservar los recursos del sistema del dispositivo central. Por ejemplo, cuando uno o más recursos de red no de confianza dentro de un contenedor están inactivos, el contenedor aún puede ejercer presión sobre los recursos del sistema (por ejemplo, memoria) y afectar al rendimiento de cualquier otro contenedor o proceso que se ejecute en el dispositivo central que está compitiendo por estos recursos. En consecuencia, al supervisar la actividad dentro de contenedores individuales, las técnicas de aislamiento de seguridad virtualizado basado en hardware descritas en la presente memoria están configuradas para suspender o restablecer contenedores individuales para reducir la presión que ejerce el contenedor sobre los recursos del dispositivo central cuando los recursos de red no de confianza dentro del contenedor están inactivos. El estado de uno o más recursos de red dentro de un contenedor suspendido puede conservarse para que un usuario pueda volver rápidamente a interactuar con uno o más recursos de red no de confianza dentro del contenedor suspendido.

En respuesta a un evento desencadenado, tal como cuando un usuario del dispositivo central cierra la sesión, las técnicas de aislamiento de seguridad virtualizado basado en hardware descritas en la presente memoria descartan el contenedor y todos los datos asociados con él. De esta manera, los contenedores pueden estar dañados por uno o más recursos de red no de confianza sin ninguna repercusión negativa para el sistema operativo del dispositivo central.

Sistema de aislamiento de seguridad virtualizado basado en hardware

La Figura 1 ilustra un sistema 100 de ejemplo que implementa aislamiento de seguridad virtualizado basado en hardware según una o más realizaciones. El sistema 100 se implementa al menos en parte por un dispositivo central. Se puede usar cualquiera de una variedad de diferentes tipos de dispositivos informáticos para implementar el sistema 100, tales como un ordenador servidor, un ordenador de escritorio, un ordenador portátil o miniordenador portátil, un dispositivo móvil (por ejemplo, una tableta o dispositivo tabléfono, un teléfono celular o otro teléfono inalámbrico (por ejemplo, un teléfono inteligente), un ordenador de agenda, una estación móvil), un dispositivo que se puede llevar puesto (por ejemplo, anteojos, pantalla montada en la cabeza, reloj, brazalete, gafas o auriculares de realidad virtual, auriculares o gafas de realidad aumentada), un dispositivo de entretenimiento (por ejemplo, un dispositivo de entretenimiento, un decodificador acoplado comunicativamente a un dispositivo de visualización, una consola de juegos), un dispositivo de Internet de las Cosas (IoT) (por ejemplo, objetos o cosas con software, microprogramas y/o hardware para permitir la comunicación con otros dispositivos), un televisor u otro dispositivo de visualización, un ordenador automotriz, etc. Por lo tanto, el sistema de implementación del dispositivo informático 100 puede variar desde un dispositivo de recursos completos con recursos sustanciales de memoria y procesador (por ejemplo, ordenadores personales, consolas de juegos) hasta un dispositivo de bajos recursos con memoria limitada y/o recursos de procesamiento (por ejemplo, decodificadores tradicionales, consolas de juegos portátiles).

El sistema 100 incluye un sistema operativo central 102, un servicio de gestión y supervisión 104 y un intermediario web 106. El servicio de gestión y supervisión 104 es representativo de un servicio que proporciona una o más políticas administrativas para el dispositivo informático que implementa el sistema operativo central 102, como se discute en la presente memoria. El intermediario web 106 es representativo de la funcionalidad que controla el acceso a uno o más recursos de red 122(1), ..., 122(*m*) accedido de forma remota desde el dispositivo informático que implementa el sistema operativo central 102. Por ejemplo, en una o más realizaciones, el intermediario web 106 controla el acceso a uno o más recursos a los que se accede desde la red 108 al requerir la autenticación del sistema operativo central 102, como se describe con más detalle a continuación. Alternativamente, en una o más realizaciones, el dispositivo informático que implementa el sistema operativo central 102 accede a los recursos de red a través de la red 108 independiente de un intermediario web. La red 108 representa la funcionalidad de una red de datos, tal como Internet, una red de área local (LAN), una red telefónica pública, una intranet, otras redes públicas y/o propietarias, combinaciones de las mismas, etc. Como tal, los recursos de red 122(1), ..., 122(*m*) accedido a través de la red 108 puede incluir sitios web, aplicaciones web, correos electrónicos, documentos, etc.

En una o más realizaciones, el sistema operativo central 102, el servicio de gestión y supervisión 104 y el intermediario web 106 se implementan como parte del mismo dispositivo informático. Alternativamente, al menos parte del servicio de gestión y supervisión 104 y/o intermediario web 106 se puede implementar en un dispositivo que está separado y remoto del dispositivo que implementa el sistema operativo central 102. Por ejemplo, en una o más realizaciones, el servicio de gestión y supervisión 104 se implementa como un servicio de gestión de dispositivos móviles (MDM) ubicado de forma remota de un dispositivo informático que implementa el sistema operativo central 102. Alternativamente o adicionalmente, el servicio de gestión y supervisión 104 puede implementarse como un servidor de protocolo ligero de acceso a directorios (LDAP) ubicado remotamente de un dispositivo informático que implementa el sistema operativo central 102. De manera similar, el intermediario web 106 puede implementarse remotamente del dispositivo que implementa el sistema operativo central 102.

El servicio de gestión y supervisión 104 está configurado para proporcionar (por ejemplo, enviar) la política al sistema operativo central 102. En una o más realizaciones, el servicio de gestión y supervisión 104 está configurado para enviar la política al sistema operativo central 102 a intervalos regulares, tales como en el arranque del sistema,

diariamente, etc. Alternativamente, el servicio de gestión y supervisión 104 puede configurarse para enviar una política al sistema operativo central 102 siempre que haya una actualización de la política para el sistema operativo central. Aunque en la presente memoria se hace referencia a la política que se envía al sistema operativo central 102, el servicio de gestión y supervisión 104 está configurado para proporcionar una política al sistema operativo central a través de cualquier método de transmisión de datos adecuado (por ejemplo, difusión en forma continua). Alternativamente, en una o más realizaciones, el sistema operativo central 102 está configurado para obtener (por ejemplo, extraer) la política del servicio de gestión y supervisión 104. El servicio de gestión y supervisión 104 tiene dos papeles. Primero, el servicio de gestión y supervisión 104 recibe una configuración administrativa para recursos de red individuales 122(1), ..., 122(*m*) que generalmente son accesibles para un usuario del sistema operativo central 102. En una o más realizaciones, estos recursos de red están asociados con niveles individuales de confianza. Por ejemplo, un empleador puede definir cualquier recurso de red que está asociado con el sitio web del empleador como que tiene un alto nivel de confianza. En consecuencia, la política para el sistema operativo central 102 indica que cualquier recurso de red asociado con el sitio web del empleador son recursos de red de confianza. El segundo papel del servicio de gestión y supervisión 104 es recibir retroalimentación del sistema operativo central 102 con respecto a la actividad supervisada asociada con recursos de red individuales y compilar esa información supervisada en un informe para un administrador. Un administrador puede utilizar este informe compilado para actualizar la política perteneciente a los recursos de red de confianza para el sistema operativo central 102.

El servicio de gestión y supervisión 104 puede configurarse para recibir datos de configuración de políticas de un administrador del dispositivo que implementa el sistema operativo central 102. Como se discute en la presente memoria, la política describe información perteneciente a recursos de red de confianza tales como sitios web de confianza, ubicaciones de red de confianza, redes de confianza, etc. Cuando el servicio de gestión y supervisión 104 recibe la política de un administrador, el servicio de gestión y supervisión 104 está configurado para enviar una actualización de política a un conjunto de dispositivos informáticos de destino. El conjunto de dispositivos informáticos de destino a los que el servicio de gestión y supervisión 104 envía actualizaciones de políticas está definido por un administrador según una o más realizaciones. Por ejemplo, en un entorno empresarial como se discutió anteriormente, el servicio de gestión y supervisión 104 está configurado para enviar actualizaciones de políticas a cada dispositivo informático asociado con la empresa. Cada dispositivo informático que recibe una actualización de política está configurado para almacenar localmente la política para su uso cuando se intenta acceder a los recursos de la red.

Como se discute con más detalle a continuación, el dispositivo informático que implementa el sistema operativo central 102 está configurado para supervisar dinámicamente la actividad asociada con los recursos de red a los que se accede 122(1), ..., 122(*m*). La actividad supervisada asociada con los recursos de red se actualiza localmente en el sistema operativo central 102 y se comunica de nuevo al servicio de gestión y supervisión 104. De esta manera, el servicio de gestión y supervisión 104 puede actualizarse continuamente para proveer a un usuario del sistema operativo central 102 con una lista precisa de recursos de red de confianza.

El sistema operativo central 102 también incluye un subsistema de aislamiento de seguridad virtualizado basado en hardware (HVSI) 110, un gestor de políticas 112, una o más aplicaciones 114, un filtro de red 116, un gestor de contenedores 118 y un subsistema de seguridad 120. El sistema operativo central 102 también gestiona uno o más contenedores, ilustrados como múltiples (*n*) contenedores 130(1), ..., 130(*n*).

El subsistema HVSI 110 es representativo de la funcionalidad para llamar a interfaces de programación de aplicaciones (API) de consulta de aislamiento de red para determinar si un recurso de red solicitado es de confianza. Estas API de consulta de aislamiento de red están expuestas, por ejemplo, por el gestor de políticas 112. Si el subsistema HVSI 110 determina que un recurso de red solicitado es de confianza, el subsistema HVSI 110 permite que el sistema operativo central 102 acceda al recurso de red solicitado. Alternativamente, si el subsistema HVSI 110 determina que un recurso de red solicitado no es de confianza, el subsistema HVSI 110 hace que el sistema operativo central 102 active uno o más de los contenedores 130(1), ..., 130(*n*) y permitir que uno o más contenedores activados accedan al recurso de red no de confianza. La funcionalidad del subsistema HVSI 110 se discutirá con más detalle a continuación. Según una o más realizaciones, el subsistema HVSI 110 determina si un recurso de red solicitado es de confianza comunicándose con el gestor de políticas 112.

El gestor de políticas 112 es representativo de la funcionalidad para obtener y almacenar una o más políticas para el dispositivo informático que implementa el sistema operativo central 102. Por ejemplo, en una o más realizaciones, un gestor de políticas 112 obtiene y almacena una o más políticas administrativas que definen una o más recursos de red de confianza para el sistema operativo central 102. Según una o más implementaciones, un gestor de políticas 112 obtiene y almacena políticas administrativas del servicio de gestión y supervisión 104. Alternativamente o adicionalmente, el gestor de políticas 112 obtiene y almacena una o más políticas administrativas de una fuente remota, tal como la red 108. Además o alternativamente, el gestor de políticas 112 recibe y almacena una o más políticas administrativas de un usuario del dispositivo que implementa el sistema operativo central 102.

Las aplicaciones 114 incluyen una o más aplicaciones que son ejecutables por uno o más procesadores del dispositivo informático que implementa el sistema operativo central 102. Por ejemplo, las aplicaciones 114 pueden incluir una aplicación de navegador web. Alternativa o adicionalmente, las aplicaciones 114 pueden incluir

aplicaciones tales como aplicaciones de correo electrónico, aplicaciones de procesamiento de texto, aplicaciones de hoja de cálculo, aplicaciones de presentación visual y similares.

El filtro de red 116 es representativo de la funcionalidad para conectar el dispositivo que implementa el sistema operativo central 102 a una red, tal como la red 108. El filtro de red 116 incluye al menos una tarjeta de interfaz de red física y al menos una tarjeta de interfaz de red virtual central. El filtro de red 116 incluye además un controlador de filtro, que está configurado para interceptar los recursos de red solicitados a medida que se transmiten desde la red 108 al sistema operativo central 102. El subsistema HVSI 110 compara entonces estos recursos de red interceptados con una o más políticas almacenadas en el gestor de políticas 112. De esta manera, el filtro de red 116 asegura que el sistema operativo central 102 se impida que acceda a ningún recurso de red no de confianza. De manera similar, el filtro de red 116 asegura que uno o más de los contenedores 130(1), ..., 130 (*n*) no pueden acceder a ningún recurso de red de confianza. Por ejemplo, en una o más realizaciones, el filtro de red 116 está configurado para cambiar los datos asociados con paquetes individuales de un recurso de red de confianza para asegurar que el recurso de red de confianza sea accedido solo por el sistema operativo central 102 y se impide que se acceda por cualquiera del uno o más de los contenedores 130(1), ..., 130(n).

El sistema operativo central 102 incluye adicionalmente un gestor de contenedores 118. El gestor de contenedores 118 gestiona la programación de los contenedores 130(1), ..., 130(*n*) en el sistema 100 y determina qué contenedores 130(1), ..., 130(*n*) se ejecutan en el sistema operativo central 102 a qué horas. El gestor de contenedores 118 también es responsable de activar uno o más contenedores 130(1), ..., 130(*n*) para un usuario individual del sistema 100 y para asegurar que otros usuarios del sistema 100 no puedan acceder al uno o más contenedores 130(1), ..., 130(*n*) creados para el usuario individual. El gestor de contenedores 118 también está configurado para recopilar registros y rastreos de uno o más contenedores creados 130(1), ..., 130(*n*) para telemetría e indicadores de seguridad. Por ejemplo, en una o más realizaciones, el gestor de contenedores 118 consulta las aplicaciones antivirus instaladas en el sistema operativo central 102 para interpretar la información recopilada y proporciona datos supervisados al subsistema HVSI 110. Dependiendo de la cantidad de procesadores físicos y/o núcleos de procesador en el dispositivo informático que ejecuta el sistema operativo central 102, un único contenedor 130(1), ..., 130(*n*) puede ejecutarse a la vez (por ejemplo, en el caso de un único procesador con un solo núcleo) o, alternativamente, múltiples contenedores 130(1), ..., 130(n) pueden ejecutarse simultáneamente (por ejemplo, en el caso de múltiples procesadores y/o múltiples núcleos de procesador). Además, en una o más realizaciones, el gestor de contenedores 118 está configurado para supervisar los cambios de configuración del usuario que se realizan dentro de uno o más de los contenedores 130(1), ..., 130(n). Por ejemplo, el gestor de contenedores 118 está configurado para detectar cambios en las preferencias del usuario asociadas con un sitio web al que se accede en uno de los contenedores 130(1), ..., 130(n). El sistema operativo central 102 está configurado para usar estos cambios detectados en el contenedor y aplicarlos a uno o más sitios web relacionados a los que se accede en el sistema operativo central.

El subsistema de seguridad 120 es representativo de la funcionalidad para hacer cumplir la política de seguridad en el sistema operativo central 102. El subsistema de seguridad 120 está configurado para verificar que un usuario inicie sesión en un dispositivo que implementa el sistema operativo central 102, manejar los cambios de contraseña para el usuario conectado, crear testigos de acceso para un usuario conectado, y así sucesivamente.

Cada contenedor 130(1), ..., 130(n) se puede implementar de diferentes maneras. Un tipo de contenedor en el que un contenedor 130 puede implementarse se denomina contenedor de procesos. Para un contenedor de procesos, los procesos de aplicación dentro del contenedor se ejecutan como si estuvieran operando en su propio sistema individual (por ejemplo, dispositivo informático), lo que se logra mediante el aislamiento del espacio de nombres. El sistema operativo central 102 implementa el aislamiento del espacio de nombres. El aislamiento del espacio de nombres proporciona a los procesos en un contenedor una vista compuesta que consta de las partes compartidas del sistema operativo central 102 y las partes aisladas del sistema operativo que son específicas de cada contenedor, tales como el sistema de archivos, la configuración, la red, etc.

Otro tipo de contenedor en el que un contenedor 130 puede implementarse se denomina contenedor virtualizado. Para un contenedor virtualizado, el contenedor virtualizado se ejecuta en una máquina virtual ligera que, en lugar de tener memoria física central específica asignada a la máquina virtual, tiene páginas de memoria respaldadas por dirección virtual. Por lo tanto, las páginas de memoria asignadas a la máquina virtual se pueden cambiar a un archivo de página. El uso de una máquina virtual ligera proporciona seguridad adicional y aislamiento entre procesos que se ejecutan en un contenedor. Por lo tanto, mientras que los contenedores de proceso usan aislamiento de proceso o aislamiento de proceso basado en silo para lograr su contención, los contenedores virtualizados usan protección basada en máquina virtual para lograr un mayor nivel de aislamiento más allá de lo que puede proporcionar un límite de proceso normal. Un contenedor también puede ejecutarse en una máquina virtual utilizando memoria física.

En una o más realizaciones, cada contenedor 130(1), ..., 130(n) incluye una o más aplicaciones virtuales 132(1), ..., 132(n). Las individuales de una o más aplicaciones virtuales 132(1), ..., 132(n) corresponden a instancias de individuales de las aplicaciones 114 en el sistema operativo central 102. Aplicaciones virtuales 132(1), ..., 132(n) pueden utilizarse por lo tanto para acceder a recursos de red no de confianza en uno o más de los contenedores

130(1), ..., 130(n) de manera similar a cómo una de las aplicaciones 114 accedería a un recurso de red de confianza en el sistema operativo central 102.

Habiendo considerado un sistema de ejemplo para implementar el aislamiento de seguridad virtualizado basado en hardware, considere ahora una arquitectura de ejemplo para el sistema que implementa el aislamiento de seguridad virtualizado basado en hardware según una o más realizaciones.

Arquitectura del sistema

La Figura 2 ilustra un ejemplo de arquitectura de sistema 200 para aislamiento de seguridad virtualizado basado en hardware según una o más realizaciones. Aunque se discute en la presente memoria como aislamiento de seguridad virtualizado basado en hardware, se debe apreciar y entender que las técnicas discutidas en la presente memoria también se pueden denominar aislamiento basado en virtualización (VBI). La arquitectura de sistema 200 se implementa al menos en parte mediante un dispositivo informático. Se puede usar cualquiera de una variedad de diferentes tipos de dispositivos informáticos para implementar la arquitectura del sistema 200, de forma análoga a la discusión anterior con respecto a los tipos que se pueden usar para implementar el sistema 100 de la Figura 1.

En el ejemplo ilustrado, el dispositivo informático que implementa la arquitectura del sistema 200 incluye dos partes separadas y aisladas: el sistema operativo central 102 y el contenedor 130. El sistema operativo central 102 está aislado de uno o más contenedores 130 para proteger el sistema operativo central de ataques o infecciones que pueden resultar de recursos de red no de confianza, como lo ilustra la línea discontinua en la Figura 2.

Se ilustra que el sistema operativo central 102 incluye el subsistema HVSI 110, el gestor de políticas 112, el filtro de red 116, el gestor de contenedores 118 y el subsistema de seguridad 120. Además, el sistema operativo central 102 incluye la aplicación 202, que puede ser una de las aplicaciones 114 ilustradas en Figura 1. La aplicación 202 incluye la biblioteca HVSI 204, cuya funcionalidad se discutirá con más detalle a continuación.

El contenedor 130 incluye la aplicación virtual 206, que es representativa de una instancia de la aplicación 202 incluida en el sistema operativo central 102. El contenedor 130 incluye adicionalmente un subsistema de seguridad virtual 210, cuya funcionalidad se discute con más detalle a continuación. Además, el contenedor 130 incluye un sistema de registro 214, que es representativo de la funcionalidad del gestor de contenido 118 para gestionar y supervisar la actividad de los recursos de red dentro de uno o más contenedores 130 activados por el dispositivo que implementa la arquitectura de sistema 200.

El sistema operativo central 102 y el contenedor 130, aunque aislados entre sí, están conectados comunicativamente a través del bus de máquina virtual 216. El bus de máquina virtual 216 es un canal de comunicación que permite que las partes central y de contenedor se comuniquen entre sí. Adicionalmente o alternativamente, el sistema operativo central 102 y el contenedor 130 están conectados comunicativamente a través de otros medios tales como una red física, una red virtual, un protocolo de bloque de mensajes simples (SMB) o interconexiones de llamada a procedimiento remoto (RPC).

Habiendo considerado una arquitectura de sistema para un sistema que implementa el aislamiento de seguridad virtualizado basado en hardware, considere ahora la funcionalidad de los componentes individuales ilustrados en la parte central y la parte de contenedor de la arquitectura de sistema 200.

Subsistema HVSI

El subsistema HVSI 110 es representativo de la funcionalidad para implementar el aislamiento de seguridad virtualizado basado en hardware en el dispositivo informático que implementa la arquitectura de sistema 200. Para implementar el aislamiento de seguridad virtualizado basado en hardware, el subsistema HVSI 110 está configurado para comunicarse con el gestor de políticas 112, el filtro de red 116, el gestor de contenedores 118, el subsistema de seguridad 120, la aplicación 202 y uno o más contenedores 130. En una o más realizaciones, el subsistema HVSI 110 se lanza automáticamente al arrancar el dispositivo informático que implementa la arquitectura de sistema 200. Alternativamente, el subsistema HVSI 110 se lanza en otros momentos, tales como por la biblioteca HVSI 204 de la aplicación 202 cuando el sistema operativo central lanza la aplicación 202.

Cuando se lanza el subsistema HVSI 110, llama al gestor de contenedores 118 para crear un contenedor para un usuario conectado al dispositivo informático que implementa la arquitectura de sistema 200, si el contenedor para el usuario aún no existe. El gestor de contenedores 118 creará una credencial de cuenta local única aleatoria o seudoaleatoria a usar para conectarse al contenedor. Esta credencial de cuenta local es conocida solo por el sistema operativo central 102 y se usa para conectar el sistema operativo central 102 al contenedor. Una transacción de la credencial de cuenta local entre el sistema operativo central 102 y el contenedor es transparente para un usuario del sistema operativo central 102 y evita que ataques maliciosos o infecciones se conecten al contenedor a través de la conexión a Internet de la red física del sistema operativo central 102. En realizaciones donde el sistema operativo central 102 tiene múltiples usuarios, el gestor de contenedores 118 está configurado para crear contenedores separados para usuarios individuales. Cada contenedor separado tiene una credencial de cuenta local única aleatoria o seudoaleatoria diferente, de modo que el sistema operativo central 102 se restrinja que acceda a ningún contenedor que no fuera creado para un usuario conectado. El gestor de contenedores 118

asegura la separación de este contenedor al autenticar las credenciales de usuario asociadas antes de permitir el acceso a uno o más contenedores.

El subsistema HVSI 110 entonces ordena al gestor de contenedores 118 que suspenda el contenedor hasta que el subsistema HVSI 110 detecte que una aplicación que se ejecuta en el dispositivo informático que implementa la arquitectura de sistema 200 está intentando acceder a uno o más recursos de red no de confianza. El subsistema HVSI 110 está configurado para supervisar las comunicaciones entre el sistema operativo central y una o más ubicaciones de recursos remotos en función de la información proporcionada al subsistema HVSI 110 por el filtro de red 116.

Cuando el sistema operativo central 102 intenta acceder a un recurso de red, el subsistema HVSI 110 se comunica con el gestor de políticas 112 para determinar si el recurso de red solicitado es un recurso de red de confianza. Si el subsistema HVSI 110 determina que el recurso de red solicitado es un recurso de red de confianza, el subsistema HVSI 110 permite que una aplicación en el sistema operativo central 102 acceda al recurso de red de confianza, tal como la aplicación 202. Información asociada con un recurso de red que el subsistema HVSI 110 puede usarse para determinar si el recurso de red es de confianza incluye, tipo de archivo, tipo de aplicación, resultados de un análisis antivirus del recurso de red, una firma de virus, información de fuente de correo electrónico, metadatos de documentos, URL, direcciones IP, puertos TCP, Nombre DNS, identificadores de dispositivo de hardware o combinaciones de los mismos. Por ejemplo, si el subsistema HVSI 110 confirma que la aplicación 202 está solicitando navegar a una página web particular, el subsistema HVSI 110 compara la información asociada con la página web particular con una o más políticas del gestor de políticas 112 y permite que la aplicación 202 acceda a la página web particular en respuesta a la determinación de que la página web particular es de confianza. El subsistema HVSI 110 determina que la página web en particular es de confianza, por ejemplo, basándose en uno o más de los nombres de dominio totalmente calificados (FQDN) de la página web particular, el nombre de dominio del sitio raíz que utiliza el servidor de nombres de dominio (DNS), la dirección de protocolo de Internet (IP), o un método similar de direccionamiento del localizador uniforme de recursos (URL). Según una o más realizaciones, el subsistema HVSI 110 está configurado adicionalmente para determinar si un recurso de red es de confianza al recibir información de un servicio basado en la nube implementado remotamente desde el dispositivo informático 102 que mantiene una lista de recursos de red maliciosos. Por ejemplo, si el subsistema HVSI 110 confirma que la aplicación 202 está solicitando navegar a una página web particular, el subsistema HVSI 110 consulta un servicio basado en la nube a través de la red 108 para comparar la página web particular con una lista de recursos de red potencialmente maliciosos almacenados en el servicio basado en la nube. Si el servicio basado en la nube indica que el sitio web particular está incluido en la lista de recursos de red potencialmente maliciosos, se determina que la página web particular no es de confianza.

Alternativamente, si el subsistema HVSI 110 determina que un recurso de red solicitado no es un recurso de red de confianza, el subsistema HVSI 110 hace que el gestor de contenedores 118 active el contenedor 130 para manejar el recurso de red no de confianza. Según el tipo de aplicación que está solicitando el recurso de red no de confianza en el sistema central, el subsistema HVSI 110 instruye al gestor de contenedores 118 para que lance una versión virtual de la aplicación dentro del contenedor 130. Por ejemplo, si el subsistema HVSI 110 determina que la aplicación 202 es solicitando acceso a un recurso de red no de confianza, el subsistema HVSI 110 instruye al gestor de contenedores 118 para crear la aplicación virtual 206 dentro del contenedor 130. De esta manera, el contenedor 130 está configurado para interactuar con uno o más recursos de red no de confianza tal como el sistema operativo central 102 interactuaría con uno o más recursos de red de confianza. En una o más realizaciones, el contenedor 130 es activado e implementado en el dispositivo que implementa el sistema operativo central 102. Alternativamente, el contenedor 130 es activado e implementado en un dispositivo que es diferente del dispositivo que implementa el sistema operativo central 102. Alternativamente, el contenedor 130 es implementado por un dispositivo que es diferente del dispositivo que implementa el sistema operativo 102 pero es activado por el dispositivo que implementa el sistema operativo central 102.

Para que un usuario del dispositivo informático que implementa el sistema operativo central 102 pueda ver e interactuar de otro modo con cualquiera de los recursos de red no de confianza a los que accede una aplicación virtual dentro del contenedor 130, el subsistema HVSI 110 está configurado para comunicarse con el contenedor 130 para causar visualización de una interfaz para la aplicación virtual 206. Por ejemplo, en una o más realizaciones, el subsistema HVSI 110 usa un modo de aplicaciones remotas integradas localmente (RAIL) de un protocolo de escritorio remoto (RDP) usando el bus de máquina virtual 216. De esta manera, el sistema operativo central 102 puede mostrar una interfaz de aplicación virtual 206 en un dispositivo de visualización del dispositivo que implementa el sistema operativo central 102. En una o más realizaciones, la interfaz está configurada para que un usuario del sistema operativo central 102 perciba que la interfaz es parte del sistema operativo central en sí. Alternativamente, el subsistema HVSI 110 está configurado para mostrar una interfaz correspondiente a la aplicación virtual 206 con una indicación visual de que la interfaz mostrada corresponde a uno o más recursos de red no de confianza. En otras realizaciones, el subsistema HVSI 110 usa un sistema X Window o una implementación alternativa de escritorio remoto para mostrar una interfaz correspondiente a la aplicación virtual 206.

Después de que el gestor de contenedores 118 active el contenedor 130, el filtro de red 116 filtra todas las llamadas de recursos de red del sistema operativo central 102 y el contenedor 130. Por ejemplo, el subsistema HVSI 110 instruye al filtro de red 116 para que bloquee todas las llamadas a recursos de red no de confianza del sistema

operativo central 102 y permita solo llamadas de recursos de red de confianza desde el sistema operativo central 102. De manera similar, el subsistema HVSI 110 instruye al filtro de red 116 para que permita todas las llamadas a recursos de red no de confianza desde el contenedor 130 y bloquee todas las llamadas a recursos de red de confianza desde el contenedor 130.

El subsistema HVSI 110 está configurado para instruir al gestor de contenedores 118 para que supervise toda la actividad asociada con los recursos de red no de confianza a los que accede el contenedor 130. Cuando el subsistema HVSI 110 recibe una indicación del gestor de contenedores 118 de que todas las instancias de aplicaciones virtuales 206 que se ejecutan en el contenedor 130 están terminadas, el subsistema HVSI 110 finaliza cualquier conexión entre el sistema operativo central 102 y cualquier contenedor 130 al que acceda el sistema operativo central 102. El subsistema HVSI 110 entonces o bien suspenderá o bien terminará uno o más contenedores 130. Por ejemplo, en una o más realizaciones cuando el subsistema HVSI 110 comprueba que el procesamiento de la aplicación virtual 206 ha finalizado, el subsistema HVSI 110 termina una conexión con el contenedor 130 y suspende el contenedor para esperar solicitudes adicionales de recursos de red no de confianza. Alternativamente, si el subsistema HVSI 110 determina que un usuario ha cerrado la sesión del dispositivo que implementa la arquitectura de sistema 200, el subsistema HVSI 110 termina uno o más contenedores 130 que fueron activados por el sistema operativo central 102.

Al comunicarse con los componentes del sistema operativo central 102, tal como el gestor de políticas 112, el filtro de red 116, el gestor de contenedores 118 y el subsistema de seguridad 120, el subsistema HVSI 110 está configurado para determinar si un recurso de red solicitado es de confianza, restringir la apertura de los recursos de red no de confianza a un contenedor aislado y gestionar uno o más procesos que se ejecutan dentro del contenedor aislado. Esto permite que el subsistema HVSI 110 realice técnicas de aislamiento de seguridad virtualizado basado en hardware para proteger el dispositivo que implementa el sistema operativo central 102 de ataques a nivel de núcleo o infecciones que pueden ser causadas por recursos de red no de confianza.

Habiendo considerado una arquitectura de sistema de ejemplo de un sistema operativo central que realiza aislamiento de seguridad virtualizado basado en hardware, considere ahora los componentes individuales de un sistema operativo central según una o más realizaciones.

Gestor de Políticas

El gestor de políticas 112 representa la funcionalidad del sistema operativo central 102 para obtener y almacenar una o más políticas para un dispositivo informático que implementa el sistema operativo central. Por ejemplo, el gestor de políticas 112 está configurado para obtener y almacenar una o más políticas del servicio de gestión y supervisión 104 ilustrado en la Figura 1. Cada una de las políticas especifica uno o más recursos de red de confianza que se permite que el sistema operativo central 102 acceda. Además, una política puede especificar uno o más objetos de política y uno o más parámetros de seguridad correspondientes para el objeto de política. Estos objetos de política y los parámetros de seguridad correspondientes proporcionan restricciones que definen cómo el sistema operativo central puede interactuar con uno o más recursos de red no de confianza.

Por ejemplo, un objeto de política puede identificar si el sistema operativo central 102 se permite que implemente aplicaciones virtuales en contenedores aislados, tales como el contenedor 130. Si el parámetro de seguridad correspondiente para este objeto de política indica que se permite que el sistema operativo central 102 implemente aplicaciones virtuales y contenedores aislados, entonces el sistema operativo central puede abrir uno o más recursos de red no de confianza en la aplicación virtual 206 del contenedor aislado 130. Alternativa o adicionalmente, un objeto de política indica ciertas aplicaciones virtuales que se permite que se abran en un contenedor aislado. El parámetro de seguridad correspondiente para este objeto de política puede identificar una o más aplicaciones específicas que se permite que se abran virtualmente en un contenedor aislado. Alternativa o adicionalmente, un objeto de política indica qué sistema operativo central 102 puede copiar entre el contenedor aislado 130 y el propio sistema operativo central 102. El parámetro de seguridad correspondiente especifica uno o más tipos de archivos que pueden copiarse entre el contenedor aislado 130 y el sistema operativo central 102. Alternativamente o adicionalmente, un objeto de política indica la configuración de impresión para aplicaciones virtuales abiertas en el contenedor aislado 130. El parámetro de seguridad correspondiente para este el objeto de política indica si la aplicación virtual 206 que se ejecuta en el contenedor aislado 130 puede imprimir y, de ser así, una o más impresoras, aplicaciones o tipos de archivo en los que se permite imprimir la aplicación virtual 206. Alternativa o adicionalmente, un objeto de política indica si el tráfico de red para la aplicación virtual 206 está permitido. El parámetro de seguridad correspondiente para este objeto de política puede especificar una o más aplicaciones virtuales para las cuales se permite el tráfico de red dentro de un contenedor aislado. Alternativa o adicionalmente, un objeto de política indica si se permiten tareas en segundo plano para la aplicación virtual 206. El parámetro de seguridad correspondiente especifica una o más aplicaciones virtuales para las cuales se permiten tareas en segundo plano dentro del contenedor aislado 130. Alternativa o adicionalmente, un objeto de política indica si la aplicación virtual 206 que se ejecuta en el contenedor se permite que aproveche uno o más recursos de hardware del dispositivo informático que implementa el sistema operativo central 102, tal como la GPU del dispositivo informático para la aceleración de gráficos.

La siguiente tabla proporciona un conjunto de ejemplos de objetos de política y parámetros de seguridad correspondientes, tales como los discutidos anteriormente. Según los procedimientos de seguridad estándar, esta política de ejemplo tiene implícita una regla de denegación predeterminada, que no se ilustra. Sin embargo, debe apreciarse y comprenderse que los objetos de política discutidos y los parámetros de seguridad correspondientes son ejemplares y no exhaustivos en su alcance.

| **Objeto de política** | **Parámetro de seguridad** |
|---|---|
| ¿Permitir aislamiento de aplicaciones virtuales en contenedor? | Sí |
| Aplicaciones virtuales para aislamiento de contenedores | Navegador web, agenda, aplicación de procesamiento de textos, aplicación de correo electrónico. |
| Configuraciones del portapapeles | Texto e imágenes permitidas |
| Configuraciones de impresión | Impresora 1; Imprimir en PDF; Imprimir a XPS |
| ¿Tráfico de red para aplicaciones virtuales aisladas? | Habilitado para navegador web |
| ¿Tareas en segundo plano para aplicaciones virtuales aisladas? | Habilitado para la aplicación de correo electrónico |

Cuando se arranca el sistema operativo central 102, el subsistema HVSI 110 contacta al gestor de políticas 112 para obtener una lista de recursos de red de confianza para el sistema operativo central, junto con cualquier objeto de política y parámetros de seguridad correspondientes. El subsistema HVSI 110 agrega estos recursos de red de confianza, objetos de política y parámetros de seguridad correspondientes y aplica esta política agregada al sistema operativo central 102. En una o más realizaciones, esta política agregada se consulta cada vez que el sistema operativo central 102 solicita realizar una acción o intenta acceder a un recurso de red. Por ejemplo, cuando el sistema operativo central 102 solicita abrir la aplicación 202 que está incluida en el parámetro de seguridad correspondiente al objeto de política "Aplicaciones virtuales para el aislamiento de contenedores", el subsistema HVSI 110 hace que el sistema operativo central 102 abra una versión virtual de esa aplicación 206 en contenedor aislado 130.

El subsistema HVSI 110 está configurado adicionalmente para supervisar la actividad dentro de uno o más de los contenedores aislados 130 para asegurar que el contenedor o los contenedores no tengan acceso a ningún recurso de red de confianza. Por ejemplo, si una versión virtual de un navegador web está ejecutándose en un contenedor aislado 130, y el subsistema HVSI 110 detecta que el navegador web virtual está intentando acceder a un recurso de red que el gestor de políticas 112 indica como recurso de red de confianza, el subsistema HVSI 110 puede evitar que el navegador web virtual abra o acceda de otro modo a este recurso de red de confianza y, en cambio, haga que el recurso de red de confianza se abra dentro de un navegador web correspondiente en el sistema operativo central 102. Al restringir el acceso y la apertura de recursos de red de confianza al sistema operativo central 102 y restringiendo el acceso y la apertura de recursos de red no de confianza a uno o más contenedores aislados 130, el subsistema HVSI 110 asegura que los recursos de red de confianza no sean corrompidos por ningún recurso de red no de confianza.

Además de recibir la lista de recursos de red de confianza, objetos de política y parámetros de seguridad correspondientes del gestor de políticas 112, el sistema operativo central 102 está configurado para observar uno o más eventos locales que podrían afectar a la política para el sistema operativo central. Por ejemplo, considere un escenario en el que un navegador web virtual está ejecutándose dentro del contenedor aislado 130. El subsistema HVSI 110 supervisa el comportamiento de cada recurso de red al que accede el navegador web virtual dentro del contenedor aislado 130. Cuando la aplicación web virtual navega a un recurso de red no de confianza, descargar el recurso de red no de confianza puede hacer que se escriba un registro del contenedor 130 de manera inesperada. Usando el gestor de contenedores 118, que se discute con más detalle a continuación, el subsistema HVSI 110 obtiene datos del contenedor 130 y calcula una política local actualizada para el recurso de red no de confianza. Por ejemplo, en una o más realizaciones, el subsistema HVSI 110 actualiza la política local para el recurso de red no de confianza inhabilitando las configuraciones de impresión y copia asociadas con el recurso de red no de confianza. El subsistema HVSI 110 se configura luego para agregar estos datos obtenidos e informar de los datos obtenidos a un servicio remoto, tal como el servicio de gestión y supervisión 104 ilustrado en la Figura 1. Según una o más realizaciones, el subsistema HVSI 110 consulta localmente las aplicaciones instaladas del sistema operativo central 102, tales como aplicaciones antivirus para obtener información adicional al actualizar esta política local. Por ejemplo, el subsistema HVSI 110 usa una o más aplicaciones antivirus para escanear un recurso de red no de confianza en el contenedor 130 y asignar un nivel de seguridad al recurso de red no de confianza. De esta manera, el subsistema HVSI 110 está configurado para actualizar continuamente la política y proteger aún más el dispositivo informático que implementa el sistema operativo central 102 contra recursos de red no de confianza.

En una o más realizaciones, el subsistema HVSI 110 implementa un motor de políticas independiente basado en ordenador central que responde a la actividad local en el sistema operativo central 102 y el contenedor 130. Este

motor de políticas independiente basado en ordenador central reduce los viajes de ida y vuelta al servicio de gestión y supervisión 104, permitiendo el servicio de gestión y supervisión para gestionar muchos clientes. En una o más realizaciones, el gestor de políticas 112 obtiene una plantilla o una firma del servicio de gestión y supervisión 104. El gestor de políticas 112 proporciona esta plantilla o firma al subsistema HVSI 110. Cuando se activa el contenedor 130, el subsistema HVSI 110 calcula la política requerida basándose en un patrón de la plantilla de política o firma que coincide con la actividad observada en el contenedor 130. Por ejemplo, si una aplicación web virtual se está ejecutando en el contenedor 130 y un recurso de red a la que la aplicación web virtual está intentando acceder a medida que un URL coincide con un patrón en la plantilla de política, el subsistema HVSI 110 calcula un nivel de riesgo y actualiza la política. Esto da como resultado dinámicamente una acción específica aplicada a la aplicación virtual en el contenedor 130, tal como una acción de permiso, una acción de bloqueo o una acción de redireccionamiento. En esta realización, la política es dinámica, descargando la evaluación y política local del servicio de gestión y supervisión 104 al subsistema HVSI 110.

Como ejemplo alternativo, considere un escenario donde un usuario descarga e instala una nueva aplicación desde un sitio web no de confianza dentro del contenedor 130. En este ejemplo, el subsistema HVSI 110 evalúa la aplicación descargada contra la política existente y calcula la política que se aplica a la aplicación descargada en un contenedor aislado 130. En una o más realizaciones, esta política calculada se basa en uno o más objetos de política y parámetros de seguridad correspondientes de aplicaciones similares. Por ejemplo, si la aplicación descargada es una aplicación de correo electrónico, el subsistema HVSI 110 identifica uno o más objetos de política y parámetros de seguridad correspondientes pertenecientes a otras aplicaciones de correo electrónico y aplica configuraciones de política similares para la aplicación de correo electrónico descargada. El subsistema HVSI 110 está configurado para supervisar la actividad asociada con la aplicación descargada dentro del contenedor 130 y está configurado para recalcular la política local basada en esta actividad observada. Adicionalmente o alternativamente, la información que describe la actividad observada de una o más aplicaciones descargadas o recursos de red accedidos dentro del contenedor 130 se agrega y comunica a un servicio remoto, tal como el servicio de gestión y supervisión 104 ilustrado en la Figura 1. En algunas realizaciones, el sistema operativo central 102 realiza un análisis local de la información que describe la actividad observada dentro del contenedor 130 y calcula una política de seguridad adicional. Por ejemplo, si una aplicación descargada está exhibiendo un comportamiento anómalo, la aplicación descargada puede terminar y el contenedor restablecerse a su estado operativo anterior antes de descargar la aplicación. Como se discute en la presente memoria, el comportamiento anómalo en el contenedor se refiere, por ejemplo, a un indicador que el subsistema HVSI 110 interpreta como un intento de comprometer un núcleo o sistema operativo del contenedor 130.

Para hacer cumplir la política del sistema operativo central 102, el subsistema HVSI 110 emplea uno o más filtros de red, tales como el filtro de red 116.

Filtro de red

El filtro de red 116 es representativo de la funcionalidad para interceptar e inspeccionar el tráfico de red entrante y saliente para el sistema operativo central 102. El filtro de red 116 tiene una funcionalidad de cumplimiento para el tráfico de red que incluye reenvío, bloqueo y/o modificación del tráfico de red, entre otras capacidades. Por ejemplo, el filtro de red 116 está configurado para interceptar e inspeccionar todo el tráfico de red y la comunicación de datos entre el sistema operativo central 102 y uno o más contenedores aislados 130. De manera similar, el filtro de red 116 está configurado para interceptar e inspeccionar todo el tráfico de red y la comunicación de datos entre el sistema operativo central 102 y cualquier ubicación de recursos remotos a los que se acceda a través de la red, tal como la red 108 ilustrada en la Figura 1. En una o más realizaciones, para interconectar el sistema operativo central 102 con uno o más contenedores aislados 130, filtro de red 116 incluye un conmutador virtual, al menos una tarjeta de interfaz de red para el sistema operativo central y una o más tarjetas de interfaz de red virtual para el uno o más contenedores aislados.

Usando la política recibida del gestor de políticas 112, el subsistema HVSI 110 interactúa con el filtro de red 116 para asegurar que el contenedor 130 no pueda acceder a recursos de red de confianza. De manera similar, el subsistema HVSI 110 interactúa con el filtro de red 116 para asegurar que el sistema operativo central 102 no pueda acceder o de otra manera abrir uno o más recursos de red no de confianza. En una o más realizaciones, el filtro de red 116 está configurado para cambiar datos de paquetes individuales asociados con recursos de red de confianza para asegurar que los datos de confianza permanezcan en el sistema operativo central 102 y no fluyan al contenedor 130. Como se discute con más detalle a continuación, en un escenario de autenticación de intermediario, el filtro de red 116 inyecta información de credenciales en el tráfico de red para asegurar el recorrido del intermediario y evitar que las credenciales se filtren o de otro modo que se acceda por el contenedor. En algunas realizaciones, el filtro de red 116 valida que el tráfico de red esté originándose o terminándose en un recurso de red que se consultó durante la búsqueda de DNS. Para lograr esto, los identificadores basados en los recursos de red permitidos se conectan dentro del contenedor y se asocian con uno o más nombres de recursos de red. Una pila de red en el contenedor incluye estos identificadores en el tráfico de red. El filtro de red 116 valida si un identificador coincide con un nombre de recurso de red. Si la validación es exitosa, el tráfico se reenvía; si falla, el tráfico se descarta. En algunas realizaciones, el filtro de red 116 elimina el identificador del tráfico de red reenviado.

Según una o más realizaciones, el filtro de red 116 se implementa como una extensión de conmutador virtual. Alternativamente, el filtro de red 116 se implementa como cualquier módulo que tenga múltiples capacidades, incluyendo interceptar, inspeccionar, reenviar, modificar y bloquear el tráfico de red. En otras realizaciones, el filtro de red está integrado en el cortafuegos u otro software de seguridad del dispositivo informático que implementa el sistema operativo central 102. Según una o más realizaciones, el filtro de red 116 se instala en el sistema operativo central 102 cuando se recibe la política en el sistema operativo central. Por ejemplo, el filtro de red 116 puede instalarse cuando el gestor de políticas 112 recibe la política del servicio de gestión y supervisión 104 ilustrado en la Figura 1. Sin embargo, debido a que el filtro de red 116 requiere recursos (por ejemplo, memoria) del dispositivo que implementa el sistema operativo central 102, en una o más realizaciones, el filtro de red 116 no está instalado cuando no hay una política presente en el sistema operativo central. De esta manera, cuando no existe una política para desviar recursos de red no de confianza a contenedores aislados, tal como el contenedor 130, el filtro de red 116 no se instala para reducir la sobrecarga de recursos.

En algunas realizaciones, el filtro de red 116 impone qué interfaz de red se usa para conectarse a un recurso. Por ejemplo, mientras el sistema operativo central 102 está en una empresa, se asume la seguridad. En la empresa, la aplicación 202 que se ejecuta en el sistema operativo central 102 puede simplemente usar cualquier interfaz física disponible (por ejemplo, Ethernet, Wi-Fi, etc.). Sin embargo, cuando el sistema operativo central 102 está en una red pública (por ejemplo, fuera de la empresa en el Wi-Fi público de una cafetería), el filtro de red 116 solo puede permitir que la aplicación 202 y otras aplicaciones que se ejecutan en el sistema operativo central 102 usen una cierta interfaz de red, tal como una interfaz VPN, que mejora la seguridad de la red. En algunas configuraciones, el filtro de red 116 permite que una o más aplicaciones que se ejecutan en el contenedor 130 accedan a la red pública sin usar VPN. En realizaciones en las que una interfaz de red está aislada para las comunicaciones del sistema operativo central 102 y una interfaz de red diferente está aislada para las comunicaciones del contenedor 130, el filtro de red 116 está configurado para proporcionar una indicación a una pila de red del contenedor 130 de que las comunicaciones de red para el contenedor están aisladas a la interfaz de red diferente.

El subsistema HVSI 110 llama al filtro de red 116 y hace que el filtro de red 116 se conecte él mismo a los puertos de red del dispositivo que implementa el sistema operativo central 102. Una vez que el filtro de red 116 está conectado a los puertos de red, puede supervisar, filtrar y/o bloquear tráfico de red. En una o más realizaciones, el filtro de red 116 incluye un servidor DNS local para aplicar aún más la política para el sistema operativo central 102. Por ejemplo, en una o más realizaciones, el servidor DNS del filtro de red 116 asigna recursos de red a las direcciones IP correspondientes para verificar un origen de recursos de red individuales. En una o más implementaciones, el filtro de red 116 incluye uno o más sistemas de control de entrada/salida (IOCTL) que están configurados para permitir o bloquear un tráfico de red tanto para el sistema operativo central 102 como para uno o más contenedores 130. En otras implementaciones esta configuración se realiza a través de una API, un archivo o un intérprete de comandos.

El filtro de red 116 está configurado para supervisar el tráfico de red (por ejemplo, tráfico HTTP) para asegurar que el sistema operativo central 102 y el contenedor 130 no accedan a los recursos de red que no están permitidos para el respectivo sistema operativo central o contenedor. Para supervisar el tráfico HTTP, el filtro de red 116 realiza una inspección de encabezado HTTP con uno o más intermediarios web que facilitan el tráfico de red entre el sistema operativo central 102 y/o cualquiera de los contenedores aislados 130, tales como el intermediario web 106 ilustrado en la Figura 1. Alternativamente, según una o más realizaciones, el filtro de red 116 está configurado para implementar su propio intermediario HTTP.

Para admitir funciones de comunicación de red en entornos intermediarios y a través de cambios de red, el filtro de red 116 incluye un traductor de direcciones de red (NAT). El NAT provee el contenedor 130 con una red privada y una pasarela para llegar a una red fuera del sistema operativo central 102. Según una o más realizaciones, el NAT está configurado para reenviar la configuración del intermediario de la red externa y reenviar notificaciones de cambio de la red externa al sistema operativo central 102. Por ejemplo, en una o más realizaciones, el filtro de red 116 usa un NAT para reenviar notificaciones de cambio de red al sistema operativo central 102 cuando cambia el estado de una conexión de red, tal como cuando un adaptador de red Wi-Fi (IEEE 802.11) sale o entra en el alcance de una red Wi-Fi. Además, el NAT del filtro de red 116 está configurado para emular una identidad de red externa para asegurar que el contenedor 130 pueda identificar diferentes redes correctamente. Por ejemplo, el NAT puede tomar la dirección de control de acceso a medios (MAC) de la pasarela de red externa central y reutilizarla como la dirección MAC de la pasarela de red privada proporcionada por NAT. Esto asegura que el software HTTP del contenedor 130 alineará adecuadamente la caché HTTP y asegurará que el descubrimiento de intermediario no se duplique cuando vuelve a conectarse a la misma red. Al emular una identidad de red externa, el NAT del filtro de red 116 mejora significativamente el rendimiento de reconexión de la red y mejora la experiencia del usuario para un usuario del sistema operativo central 102. Además, el NAT del filtro de red 116 está configurado para reenviar configuraciones de "espera conectada de baja potencia" al sistema operativo central 102 para una o más aplicaciones virtuales 206 que se ejecutan en uno o más contenedores aislados, tales como el contenedor 130. Esto permite que el sistema operativo central 102 mantenga viva cualquier aplicación virtual 206 que se ejecute en uno o más contenedores aislados 130 activos. En una o más realizaciones, la funcionalidad del NAT se descarga a un componente diferente del sistema operativo central 102. Por ejemplo, el aprovisionamiento de una red privada y una pasarela para llegar a una red fuera del sistema operativo central 102, el reenvío de notificaciones de cambio de red, emulando una identidad de red externa, y el reenvío de la configuración de espera conectada de baja potencia se

pueden realizar mediante uno o una combinación de filtro de red 116, subsistema HVSI 110 o gestor de contenedores 118.

El subsistema HVSI 110 está configurado para interactuar con el filtro de red 116 para realizar la autenticación de intermediario web según una o más realizaciones. Por ejemplo, muchos sistemas empresariales utilizan uno o más intermediario web para controlar el acceso a Internet de usuarios individuales de la empresa. Estos intermediarios web requieren autenticación antes de permitir que usuarios individuales o aplicaciones accedan a recursos de red, tales como sitios web, solicitando credenciales de usuario tales como nombre de usuario y contraseña asociada. En consecuencia, el filtro de red 116 está configurado para identificar un intermediario web que se requiere para facilitar el acceso a un sitio web, tal como el intermediario web 106 ilustrado en la Figura 1. Sin embargo, en escenarios donde una aplicación virtual que se ejecuta en un contenedor aislado requiere autenticación de intermediario web, surgen problemas de seguridad. Por ejemplo, uno o más recursos de red no de confianza que están abiertos y ejecutándose en el contenedor aislado 130 pueden obtener acceso no autorizado a las credenciales de usuario y comprometer la seguridad de las cuentas de usuario asociadas.

Para proporcionar una experiencia de usuario sin problemas para las aplicaciones virtuales 206 que se ejecutan en el contenedor 130 que requieren autenticación de intermediario web, el subsistema HVSI 110 está configurado para proporcionar credenciales de usuario a un intermediario web desde el sistema operativo central 102 sin proporcionar las credenciales de usuario al contenedor 130. El subsistema HVSI 110 está configurado para proporcionar credenciales de usuario a un intermediario web para la aplicación virtual 206 que se ejecuta en el contenedor 130 mediante la implementación del subsistema de seguridad virtual 210 dentro del contenedor aislado. El subsistema de seguridad virtual 210 está configurado para interactuar con el subsistema de seguridad 120 del sistema operativo central 102. Por ejemplo, en una o más realizaciones, el subsistema HVSI 110 detecta que la aplicación web virtual 206 está llamando a un recurso de red que requiere autenticación de intermediario web. El subsistema HVSI 110 está configurado para implementar el subsistema de seguridad virtual 210 dentro del contenedor aislado para que el subsistema de seguridad virtual 210 pueda interactuar con el subsistema de seguridad 120 del sistema operativo central 102. La comunicación entre el subsistema de seguridad virtual 210 y el subsistema de seguridad 120 puede realizarse a través de la conexión establecida por el subsistema HVSI 110, tal como a través del bus de máquina virtual 216.

Cuando la aplicación web virtual 206 en el contenedor 130 intenta acceder a un recurso de red a través de un intermediario web, el intermediario web regresa con un desafío para las credenciales de usuario. En este escenario, el subsistema de seguridad virtual 210 está configurado para llamar al subsistema de seguridad 120 del sistema operativo central 102 para proporcionar autenticación al intermediario web. En respuesta a la recepción de esta llamada, el subsistema de seguridad 120 está configurado para generar un objeto binario grande de credenciales ficticio que indica la propiedad de las credenciales de usuario sin contener realmente las credenciales de usuario dentro del objeto binario grande de credenciales. Como se discute en la presente memoria, un objeto binario grande ficticio también puede denominarse una seudo autenticación de las credenciales de usuario. El subsistema de seguridad 120 devuelve el objeto binario grande de credenciales ficticio generado al subsistema de seguridad virtual 210. El subsistema de seguridad virtual 210 luego proporciona el objeto binario grande de credenciales ficticio a la aplicación web virtual 206 para que la aplicación web virtual pueda incrustar el objeto binario grande de credenciales ficticio en una respuesta HTTP al intermediario web. De esta manera, el contenedor 130 está configurado para probar la propiedad de las credenciales de usuario sin recibir las credenciales de usuario reales del sistema operativo central 102. Según una o más realizaciones, la prueba de propiedad de credenciales dentro del objeto binario grande ficticio se realiza aplicando una función de seguridad de comprobación aleatoria a las credenciales reales e incluyendo las credenciales comprobadas aleatoriamente dentro del objeto binario grande ficticio. Esto asegura que las credenciales de usuario no se vean comprometidas por ningún recurso de red no de confianza que pueda estar ejecutándose en el contenedor 130.

Alternativamente, si el subsistema de seguridad virtual 210 reenvía una solicitud de intermediario web para credenciales de usuario al subsistema de seguridad 120 del sistema operativo central 102, el subsistema de seguridad 120 está configurado para generar dos objetos binarios grandes de credenciales. El primer objeto binario grande de credenciales generado por el subsistema de seguridad 120 es un objeto binario grande de credenciales ficticio como se describe anteriormente. El segundo objeto binario grande de credenciales generado por el subsistema de seguridad 120 contiene las credenciales de usuario reales solicitadas por el intermediario web. En este escenario, el objeto binario grande de credenciales ficticio se proporciona al subsistema de seguridad virtual 210 en el contenedor 130, y el objeto binario grande que contiene las credenciales de usuario reales se proporciona al filtro de red 116 en el sistema operativo central 102. Como se discutió anteriormente, la aplicación web virtual 206 está configurada para recibir el objeto binario grande de credenciales ficticio del subsistema de seguridad virtual 210 e incrustar el blob de credenciales ficticio en una respuesta HTTP al intermediario web. Debido a que todo el tráfico de red del sistema operativo central 102 y el contenedor 130 se filtra a través del filtro de red 116, el filtro de red 116 está configurado para interceptar la respuesta HTTP del contenedor y reemplazar el objeto binario grande ficticio con el objeto binario grande de credenciales de usuario real antes de transmitir la respuesta HTTP al intermediario web. Según una o más realizaciones, donde el sistema operativo central 102 está funcionando en un entorno informático anidado, este reemplazo de objeto binario grande de credenciales se puede realizar múltiples veces, en cada capa del entorno anidado. Alternativamente, en una o más realizaciones, el filtro de red 116 sondea los identificadores de

recursos de red permitidos dentro del contenedor 130 para validar que el tráfico de red se origina y termina en un recurso de red que se consultó durante la búsqueda de DNS, como se discutió anteriormente.

Cuando el subsistema HVSI 110 determina que el sistema operativo central 102 está intentando acceder a un recurso de red no de confianza, utilizando el gestor de políticas 112, el filtro de red 116 y el subsistema de seguridad 110 como se describe en la presente memoria, el subsistema HVSI 110 se comunica con el gestor de contenedores 118 para gestionar y supervisar uno o más contenedores 130 para acceder al recurso de red no de confianza.

Gestor de contenedores

El gestor de contenedores 118 es responsable de activar uno o más contenedores 130 que están aislados del sistema operativo central 102 para acceder a recursos de red no de confianza. Como se discute en el presente documento, la activación de un contenedor tal como el contenedor 130 incluye crear uno o más contenedores nuevos o reanudar el funcionamiento de uno o más contenedores suspendidos. El gestor de contenedores 118 está configurado adicionalmente para activar uno o más contenedores para un usuario individual conectado al sistema operativo central 102 y asegurar que cualquier otro usuario del sistema operativo central tenga restringido el acceso a uno o más contenedores activados para el usuario individual. El gestor de contenedores 118 asegura una asignación del usuario conectado al sistema operativo central 102 al contenedor 130. En algunas realizaciones en las que hay múltiples usuarios del sistema operativo central 102 y múltiples contenedores, el gestor de contenedores 118 está configurado para ver una identidad del usuario conectado y asociarla directamente con uno o más contenedores correspondientes. Esta restricción evita que otros usuarios vean o interactúen de otro modo con los contenedores.

El gestor de contenedores 118 está configurado además para recopilar registros y rastreos que describen la actividad dentro del contenedor 130. El gestor de contenedores 118 está configurado para usar estos registros y rastreos para supervisar el uso del contenedor para telemetría e indicadores de seguridad. Según una o más realizaciones, el gestor de contenedores 118 consulta con las aplicaciones locales instaladas en el sistema operativo central 102, tales como una aplicación antivirus, para interpretar cualquier problema de seguridad asociado con la actividad supervisada en el contenedor 130. El gestor de contenedores 118 está configurado para agregar esta información supervisada y proporcionar la información supervisada al subsistema HVSI 110. Alternativamente o adicionalmente, el gestor de contenedores 118 está configurado para proporcionar esta información supervisada a una o más fuentes remotas, tales como el servicio de gestión y supervisión 104 ilustrado en la Figura 1.

Cuando se arranca el sistema operativo central 102, el subsistema HVSI 110 determina si la política está presente. En una o más realizaciones, el subsistema HVSI 110 determina si la política está presente comunicándose con el gestor de políticas 112, como se discute en la presente memoria. Si el subsistema HVSI 110 determina que la política está presente en el sistema operativo central 102, el gestor de contenedores 118 está configurado para activar el contenedor 130 para manejar cualquier recurso de red no de confianza que solicite el sistema operativo central. El gestor de contenedores 118 está configurado para activar el contenedor 130 comunicándose con el sistema operativo central 102 para determinar si existe una imagen base del contenedor. Si el gestor de contenedores 118 determina que no existe una imagen base del contenedor, el gestor de contenedores 118 está configurado para crear una imagen base del contenedor. Si el gestor de contenedores 118 determina que existe una imagen base del contenedor, o después de que el gestor de contenedores 118 cree una imagen base del contenedor, el gestor de contenedores 118 espera a que un usuario inicie sesión en el sistema operativo central 102.

Una imagen base del contenedor contiene información requerida para crear y activar un contenedor aislado que incluye su propio sistema operativo, tal como el contenedor 130. Por ejemplo, en una o más realizaciones, una imagen base del contenedor contiene información que describe cómo el sistema operativo central 102 debe establecer la configuración del registro para un contenedor. Se requiere información con respecto a la configuración del registro porque algunas aplicaciones virtuales que se abren dentro del contenedor 130 se comportan de manera diferente que una versión de la aplicación que se abriría en el sistema operativo central 102. Además o alternativamente, una imagen base del contenedor incluye información que describe cómo crear una cuenta de usuario dentro de una aplicación virtual ejecutada en el contenedor 130. Además o alternativamente, la imagen base del contenedor incluye información con respecto a una cantidad de recursos asignados, tales como memoria, procesadores, discos o redes, que el contenedor 130 puede requerir cuando está activo.

Cuando un usuario inicia sesión en el sistema operativo central 102, el gestor de contenedores 118 determina si existe un contenedor correspondiente a la imagen base del contenedor. Si el gestor de contenedores 118 determina que no existe un contenedor para la imagen base del contenedor, el gestor de contenedores 118 puede crear un contenedor, tal como el contenedor 130. Para asegurar que una imagen base del contenedor represente con precisión el sistema operativo central 102, el gestor de contenedores 118 está configurado para invalidar cualquier imagen base del contenedor existente y crear una o más imágenes base de contenedor nuevas después de una actualización del sistema operativo. De esta manera, el gestor de contenedores 118 asegura que una imagen base del contenedor incluya cualquier archivo binario del sistema operativo central actualizado, manteniendo así actualizados los contenedores creados a partir de la imagen base del contenedor con el sistema operativo central 102. En el caso de una actualización del sistema operativo central 102, el gestor de contenedores 118 está configurado o bien para forzar el cierre de cualquier contenedor abierto o bien esperar hasta que la actividad del

usuario en el contenedor haya dejado de eliminar la imagen base del contenedor y crear una nueva imagen base del contenedor. Después de crear el contenedor, el gestor de contenedores 118 coloca el contenedor en un modo suspendido. Cuando un contenedor está en modo suspendido, el contenedor consume menos recursos del dispositivo que implementa el sistema operativo central 102, reduciendo así la sobrecarga de recursos. El gestor de contenedores 118 está configurado para mantener uno o más contenedores aislados 130 en un modo suspendido hasta que el sistema operativo central 102 solicite acceso a uno o más recursos de red no de confianza.

Cuando el subsistema HVSI 110 detecta que el sistema operativo central 102 está solicitando acceso a uno o más recursos de red no de confianza, el subsistema HVSI 110 instruye al gestor de contenedores 118 a activar uno o más contenedores suspendidos para manejar uno o más recursos de red no de confianza. En una o más realizaciones, el uno o más contenedores están alojados en el dispositivo informático que está implementando el sistema operativo central 102. Alternativamente, al menos uno de los uno o más contenedores puede estar alojado en un dispositivo informático que está remoto del dispositivo informático que implementa el sistema operativo central 102. En un escenario en el que un contenedor está alojado en un dispositivo informático diferente, el gestor de contenedores 118 está configurado para comunicarse con los diferentes dispositivos informáticos para gestionar y supervisar los contenedores remotos. Debido a que el gestor de contenedores 118 puede activar un contenedor suspendido más rápido de lo que puede crear un contenedor, mantener uno o más contenedores suspendidos permite que el sistema operativo central 102 responda rápidamente a las solicitudes de recursos de red no de confianza.

En respuesta a la determinación de que el sistema operativo central 102 está solicitando acceso a uno o más recursos de red no de confianza, el gestor de contenedores 118 está configurado para identificar una aplicación en el sistema operativo central que está solicitando el recurso de red no de confianza. El gestor de contenedores 118 está configurado para lanzar una versión virtual de la aplicación dentro del contenedor 130 para manejar el recurso de red no de confianza. Después de que el gestor de contenedores 118 active una versión virtual de la aplicación dentro del contenedor 130, el subsistema HVSI 110 se configura de forma remota en el contenedor 130 para mostrar una interfaz de la aplicación virtual en una pantalla del dispositivo que implementa el sistema operativo central 102.

El gestor de contenedores 118 está configurado para comunicarse con el subsistema HVSI 110 para asegurar que exista la tecnología de virtualización de hardware adecuada en el sistema operativo central 102 y en el contenedor 130, si el contenedor está alojado en un dispositivo informático remoto. Para que el gestor de contenedores 118 funcione correctamente, el gestor de contenedores 118 está configurado para verificar que las interfaces de programación de aplicaciones (API) del sistema operativo central 102 estén disponibles para gestionar ciclos de vida de contenedores aislados y pilas de red asociadas.

El gestor de contenedores 118 está configurado para supervisar la actividad dentro del contenedor 130 usando el sistema de registro 214. De esta manera, el gestor de contenedores 118 está configurado para detectar cualquier comportamiento sospechoso de una red o recurso de red al que se accede dentro del contenedor 130, ya sea que el contenedor 130 también esté ocupando demasiado espacio en disco, y así sucesivamente. En base a la información obtenida del sistema de registro 214, el gestor de contenedores 118 puede informar al subsistema HVSI 110 de cómo gestionar uno o más contenedores 130. Por ejemplo, en una o más realizaciones, el gestor de contenedores 118 comprueba que el acceso a uno o más recursos de red no de confianza dentro el contenedor 130 se ha completado y comunica esta información al subsistema HVSI 110. En respuesta a la recepción de esta información, el subsistema HVSI 110 coloca el contenedor 130 en modo suspendido hasta que posteriormente sea necesario manejar un recurso de red no de confianza adicional.

El gestor de contenedores 118 también está configurado para supervisar y determinar cuándo un usuario del sistema operativo central 102 se desconecta. En respuesta a la determinación de que un usuario del sistema operativo central 102 se ha desconectado, el gestor de contenedores 118 proporciona esta información al subsistema HVSI 110. El subsistema HVSI 110 está configurado para eliminar uno o más contenedores 130 en respuesta al cierre de sesión del usuario. Como se discute en la presente memoria, eliminar un contenedor también borra cualquier información incluida dentro del contenedor.

El gestor de contenedores 118 también está configurado para compartir información de DNS y Protocolo de Transferencia de Hipertexto (HTTP) del sistema operativo central 102 para mejorar el rendimiento de navegación web u otra actividad de red dentro de uno o más de los contenedores aislados. En una o más realizaciones, el gestor de contenedores 118 mantiene una memoria caché de consultas DNS realizadas desde instancias anteriores en las que el contenedor 130 accedió a recursos de red, así como datos HTTP tales como archivos de datos de Internet o cookies de sitios web que permiten que solicitudes futuras en un contenedor accedan a sitios web no de confianza para recordar una o más de las preferencias, configuraciones o ajustes anteriores del usuario.

Además de recibir información con respecto a la actividad supervisada dentro del contenedor 130 del gestor de contenedores 118, el subsistema HVSI 110 también está configurado para recibir información con respecto a la actividad del contenedor desde una o más bibliotecas HVSI 208.

Biblioteca HVSI

Como se discute en la presente memoria, una biblioteca HVSI es una biblioteca asíncrona pequeña, ligera, que está configurada para vincularse o bien estática o bien dinámicamente dentro de una aplicación. Por ejemplo, en la arquitectura de sistema 200 ilustrada de la Figura 2, la aplicación 202 incluye la biblioteca HVSI 204 y la aplicación virtual 206 incluye la biblioteca virtual HVSI 208. Cada biblioteca HVSI está configurada para ejecutarse dentro de su aplicación respectiva y es responsable de interceptar y reenviar llamadas de recursos de red desde la aplicación al subsistema HVSI 110.

Cuando un usuario del sistema operativo central 102 intenta abrir un recurso de red a través de la aplicación 202, la biblioteca HVSI 204 comunica información con respecto al recurso de red solicitado al subsistema HVSI 110. El subsistema HVSI 110 compara esta información con una o más políticas obtenidas del gestor de políticas 112 a determinar si el recurso de red solicitado es un recurso de red de confianza. Si el subsistema HVSI 110 determina que el recurso de red solicitado es un recurso de red de confianza, el subsistema HVSI 110 permite que la aplicación 202 acceda al recurso de red solicitado. Alternativamente, si el subsistema HVSI 110 determina que el recurso de red solicitado no es un recurso de red de confianza, el subsistema HVSI 110 reenvía el recurso de red no de confianza a la aplicación virtual 206 en el contenedor 130.

La biblioteca virtual HVSI 208 en el contenedor 130 está configurada para interceptar solicitudes de recursos de red de la aplicación virtual 206 y comunicar información con respecto a los recursos de red solicitados al subsistema HVSI 110. El subsistema HVSI 110 está configurado de manera similar para comparar esta información con cualquier política para el sistema operativo central 102 para asegurar que no se proporcionen recursos de red de confianza al contenedor 130. En una o más realizaciones, una aplicación virtual no se vinculará a la biblioteca virtual HVSI 208 para asegurar la compatibilidad. En estas realizaciones, el sistema de registro 214 y el filtro de red 116 funcionan para interceptar las solicitudes de recursos de red de la aplicación virtual y comunicar información con respecto a los recursos de red solicitados al subsistema HVSI 110.

Habiendo considerado una arquitectura de sistema para un sistema que implementa aislamiento de seguridad virtualizado basado en hardware para proteger un dispositivo informático de ataques o infecciones asociadas con recursos de red no de confianza, considere ahora procedimientos de ejemplo según una o más realizaciones.

Procedimientos de ejemplo

La Figura 3 es un diagrama de flujo que ilustra un proceso 300 de ejemplo para implementar aislamiento de seguridad basado en hardware según una o más realizaciones. El proceso 300 se lleva a cabo mediante un sistema, tal como el sistema 100 de la Figura 1, y puede implementarse en software, microprogramas, hardware o combinaciones de los mismos. El proceso 300 se muestra como un conjunto de actos y no se limita al orden que se muestra para realizar las operaciones de varios actos. El proceso 300 es un proceso de ejemplo para implementar el aislamiento de seguridad virtualizado basado en hardware; En la presente memoria se incluyen discusiones adicionales de la implementación del aislamiento de seguridad virtualizado basado en hardware con referencia a diferentes figuras.

En el proceso 300, se detecta el intento de acceso a un recurso de red (acto 302). El intento de acceso se detecta cuando un usuario, administrador, programa, aplicación u otra entidad del sistema solicita uno o más recursos de red desde una o más ubicaciones que se ubican de forma remota desde el sistema. Por ejemplo, el intento de acceso a un recurso de red se detecta cuando un usuario del sistema intenta navegar a una página web utilizando una aplicación web.

En respuesta a la detección del intento de acceso a un recurso de red, el proceso 300 procede a determinar si el recurso de red es de confianza (acto 304). La determinación de si el recurso de red es de confianza se realiza comparando el recurso de red con la política que o bien está almacenada en el sistema operativo central o bien que el sistema operativo central accede de forma remota. Por ejemplo, en una o más realizaciones, el sistema operativo central almacena localmente la política, tal como en el gestor de políticas 112 de la Figura 1, que enumera una lista de recursos de red de confianza. Alternativa o adicionalmente, la política se recibe de un servicio de gestión y supervisión que está alejado del sistema operativo central, como el servicio 104 de gestión y supervisión de la Figura 1. Además o alternativamente, el sistema operativo central actualiza la política local en función de la actividad supervisada asociada con la actividad de recursos de red en el sistema operativo central y los contenedores asociados. Como se discute en la presente memoria, la política puede actualizarse continuamente para mantener una lista actual de recursos de red de confianza.

En respuesta a la determinación de que el recurso de red es un recurso de red de confianza, el proceso 300 permite que una aplicación en el sistema operativo central acceda al recurso de red (acto 312). Por ejemplo, si el proceso 300 se lleva a cabo por el sistema 100 de la Figura 1, y se determina que el recurso de red es un recurso de red de confianza, el proceso 300 permitirá que una de las aplicaciones 114 en el sistema operativo central 102 acceda al recurso de red de confianza.

En respuesta a la determinación de que el recurso de red no es un recurso de red de confianza, el proceso 300 determina si el aislamiento de seguridad virtualizado basado en hardware está habilitado en el sistema operativo

central (acto 306). Si el proceso determina que el aislamiento de seguridad virtualizado basado en hardware no está habilitado, el proceso permite que una aplicación en el sistema operativo central acceda al recurso de red no de confianza (acto 312). En consecuencia, un sistema operativo central que no habilita el aislamiento de seguridad virtualizado basado en hardware como se discute en la presente memoria permite que una aplicación en el sistema operativo central acceda a un recurso de red no de confianza, exponiendo así un dispositivo que implementa el sistema operativo central a ataques maliciosos o infecciones del recurso de red no de confianza.

Alternativamente, si el proceso 300 determina que el aislamiento de seguridad virtualizado basado en hardware está habilitado, el proceso continúa para activar un contenedor (acto 308). Como se discute en la presente memoria, la activación de un contenedor incluye crear un contenedor según una o más realizaciones. Alternativa o adicionalmente, activar un contenedor incluye identificar un contenedor suspendido y reanudar el procesamiento del contenedor suspendido. Como se discute en la presente memoria, un contenedor representa un entorno de tiempo de ejecución aislado que está separado del sistema operativo central, tal como el sistema operativo central 102. El contenedor incluye su propio núcleo que está separado de un núcleo del sistema operativo central y, por lo tanto, lo protege de ataques a nivel de núcleo asociados con el recurso de red no de confianza que pueden dirigirse al sistema operativo central. En consecuencia, incluso si el contenedor se ve comprometido, el sistema operativo central está aislado y protegido de cualquier infección o ataque asociado con recursos de red no de confianza.

En respuesta a la activación del contenedor, el sistema operativo central permite que el contenedor acceda al recurso de red (acto 310). El sistema operativo central continúa supervisando la actividad en el contenedor asociado con el recurso de red y uno o más recursos de red adicionales que son llamados por el contenedor para asegurar que el contenedor no acceda a ningún recurso de red de confianza. Del mismo modo, el sistema asegura que el sistema operativo central no acceda a ningún recurso de red no de confianza.

Habiendo considerado un procedimiento de ejemplo para implementar el aislamiento de seguridad virtualizado basado en hardware en un sistema operativo central para proteger un dispositivo que implementa el sistema operativo central de ataques o infecciones asociadas con recursos de red no de confianza, considere ahora un procedimiento de ejemplo que puede utilizarse para activar un contenedor para aislamiento de seguridad virtualizado basado en hardware.

La Figura 4 es un diagrama de flujo que ilustra un proceso 400 de ejemplo para activar un contenedor para aislamiento de seguridad virtualizado basado en hardware según una o más realizaciones.

El proceso 400 se lleva a cabo mediante un sistema operativo central, tal como el sistema operativo central 102 de la Figura 1, y puede implementarse en software, microprogramas, hardware o combinaciones de los mismos. El proceso 400 se muestra como un conjunto de actos y no se limita al orden que se muestra para realizar las operaciones de varios actos. El proceso 400 es un proceso de ejemplo para activar un contenedor para el aislamiento de seguridad virtualizado basado en hardware; en la presente memoria se incluyen discusiones adicionales sobre la activación de un contenedor para el aislamiento de seguridad virtualizado basado en hardware con referencia a diferentes figuras.

En el proceso 400, se arranca el sistema operativo central (acto 402). Después de que el sistema operativo central se haya arrancado, el sistema operativo central procede a determinar si existe una imagen base del contenedor (acto 404).

Si el sistema operativo central determina que no existe una imagen base del contenedor, el sistema operativo central procede a crear una imagen base del contenedor (acto 406). Si el sistema operativo central determina que existe una imagen base del contenedor, o en respuesta a la creación de una imagen base del contenedor, el sistema operativo central espera hasta que un usuario inicie sesión (acto 408). Un usuario puede iniciar sesión en el sistema operativo central ingresando una o más credenciales que están asociadas de forma exclusiva con el usuario, tales como un nombre de usuario, una contraseña, etc.

Después de que un usuario inicia sesión, el sistema operativo central determina si existe un contenedor para el usuario conectado (acto 410). Como se discute en la presente memoria, el contenedor es exclusivo de un usuario individual y permite al usuario interactuar con recursos de red no de confianza en un entorno de tiempo de ejecución aislado que es independiente del sistema operativo central.

Si el sistema operativo central determina que no existe un contenedor para el usuario conectado, el sistema operativo central procede a crear un contenedor para el usuario conectado (acto 412). El sistema operativo central está configurado para crear un contenedor para el usuario conectado según una o más de las técnicas discutidas en la presente memoria.

Si el sistema operativo central determina que existe un contenedor para el usuario conectado, o después de que el sistema operativo central haya creado un contenedor para el usuario conectado, el sistema operativo central procede a activar el contenedor para el usuario conectado (acto 414). De esta manera, el sistema operativo central activa un contenedor cuando un usuario inicia sesión en el sistema operativo central que está preparado para procesar cualquier recurso de red no de confianza que solicite el sistema operativo central.

Habiendo considerado un procedimiento de ejemplo para activar un contenedor para aislamiento de seguridad virtualizado basado en hardware para proteger un sistema operativo central de recursos de red no de confianza, considere ahora un procedimiento de ejemplo para gestionar un contenedor para aislamiento de seguridad virtualizado basado en hardware.

La Figura 5 es un diagrama de flujo que ilustra un proceso 500 de ejemplo para gestionar un contenedor para aislamiento de seguridad virtualizado basado en hardware según una o más realizaciones.

El proceso 500 se lleva a cabo mediante un sistema operativo central, tal como el sistema operativo central 102 de la Figura 1, y puede implementarse en software, microprogramas, hardware o combinaciones de los mismos. El proceso 500 se muestra como un conjunto de actos y no se limita al orden que se muestra para realizar las operaciones de varios actos. El proceso 500 es un proceso de ejemplo para gestionar un contenedor para el aislamiento de seguridad virtualizado basado en hardware; en la presente memoria se incluyen discusiones adicionales sobre la gestión de un contenedor para el aislamiento de seguridad virtualizado basado en hardware con referencia a diferentes figuras.

En el proceso 500, después de que un usuario ha iniciado sesión en un sistema operativo central y se ha activado un contenedor para el usuario conectado, el sistema operativo central suspende el contenedor (acto 502). Al suspender el contenedor, el sistema operativo central reduce la cantidad de recursos del sistema para un dispositivo que implementa el sistema operativo central que se requiere para mantener un contenedor activo. Debido a que la reanudación de un contenedor suspendido puede realizarse más rápidamente que la creación de un contenedor, el proceso de implementación del sistema operativo central 500 está configurado para responder rápidamente a una solicitud de acceso a un recurso de red no de confianza.

El proceso de implementación del sistema operativo central 500 continúa supervisando las solicitudes de recursos de red hasta que detecta el intento de acceso a un recurso de red no de confianza (acto 504). La detección del intento de acceso a un recurso de red no de confianza se realiza comparando la información que describe el recurso de red solicitado con la política para el proceso de implementación del sistema operativo central 500, como se discute en la presente memoria. Por ejemplo, en una o más realizaciones, un usuario del sistema operativo central que implementa el proceso 500 intenta acceder a un sitio web que no está definido por política como un sitio web de confianza.

En respuesta a la detección de acceso a un recurso de red no de confianza, el proceso de implementación del sistema operativo central 500 activa el contenedor suspendido (acto 506). Una vez que se activa el contenedor suspendido, el sistema operativo central permite que una instancia virtual de una aplicación que se ejecuta en el contenedor acceda al recurso de red no de confianza. El sistema operativo central puede configurarse para comunicarse con el contenedor a través de un bus de máquina virtual para instalar y activar la instancia virtual de la aplicación y para hacer una visualización de una interfaz de la instancia virtual de la aplicación. De esta manera, el contenedor permite a un usuario del proceso de implementación del sistema operativo central 500 interactuar con uno o más recursos de red no de confianza mientras que uno o más recursos de red no de confianza se operan dentro de un entorno de tiempo de ejecución contenido que está aislado del sistema operativo central.

El proceso de implementación del sistema operativo central 500 está configurado para mantener el contenedor en un estado activo hasta que se detecte un evento desencadenante (acto 508) o hasta que el sistema operativo central determine que el acceso a uno o más recursos de red no de confianza ha finalizado (acto 510). Por ejemplo, si el proceso de implementación del sistema operativo central 500 identifica uno o más sitios web abiertos en una aplicación web como recursos de red no de confianza, el sistema puede identificar que el acceso a uno o más recursos de red no de confianza ha finalizado en respuesta al usuario cerrando la aplicación web. Si el sistema operativo central determina que el acceso a uno o más recursos de red no de confianza ha finalizado, el sistema operativo central suspende el contenedor (acto 502). Al suspender el contenedor cuando el contenedor no está accediendo a ningún recurso de red no de confianza, el sistema operativo central reduce la cantidad de recursos del sistema necesarios para mantener un contenedor activo. De manera similar, al suspender el contenedor en lugar de eliminarlo, el sistema operativo central puede activar fácilmente el contenedor suspendido al detectar el intento de acceso a uno o más recursos de red adicionales no de confianza.

En respuesta a la detección de un evento desencadenante, el sistema operativo central está configurado para eliminar el contenedor (acto 512). Como se discute en la presente memoria, un evento desencadenante puede referirse a la detección de que un usuario del proceso de implementación del sistema operativo central 500 se ha desconectado. Además o alternativamente, se detecta un evento desencadenante cuando se detecta un comportamiento anómalo en el contenedor.

Habiendo considerado un procedimiento de ejemplo para gestionar un contenedor de aislamiento de seguridad virtualizado basado en hardware para proteger un dispositivo que implementa el sistema operativo central de ataques e infecciones asociadas con recursos de red no de confianza, considere ahora un procedimiento de ejemplo que puede utilizarse para implementar aislamiento de seguridad virtualizado basado en hardware en un sistema operativo central.

La Figura 6 es un diagrama de flujo que ilustra el proceso 600 para implementar el aislamiento de seguridad virtualizado basado en hardware en un sistema operativo central según una o más realizaciones.

El proceso 600 se lleva a cabo mediante un sistema operativo central, tal como el sistema operativo central 102 de la Figura 1, y puede implementarse en software, microprogramas, hardware o combinaciones de los mismos. El proceso 600 se muestra como un conjunto de actos y no se limita al orden que se muestra para realizar las operaciones de varios actos. El proceso 600 es un proceso de ejemplo para usar uno o más contenedores para el aislamiento de seguridad virtualizado basado en hardware; en la presente memoria se incluyen discusiones adicionales sobre el uso de uno o más contenedores para el aislamiento de seguridad virtualizado basado en hardware con referencia a diferentes figuras.

En el proceso 600, un sistema operativo central ejecuta una aplicación (acto 602). La aplicación puede ser cualquier tipo de aplicación, tal como una aplicación web, una aplicación de procesamiento de texto, una aplicación de correo electrónico, etc.

El sistema operativo central detecta que la aplicación está intentando acceder a un recurso de red (acto 604). El sistema operativo central está configurado para detectar que la aplicación está solicitando acceso a un recurso de red mediante la supervisión de las comunicaciones de red utilizando un filtro de red, como se discute en la presente memoria.

En respuesta a la detección de que la aplicación que se ejecuta en el sistema operativo central está solicitando acceso a un recurso de red, el sistema operativo central determina que el recurso de red es un recurso de red no de confianza (acto 606). El sistema operativo central está configurado para determinar que el recurso de la red no es de confianza comparando el recurso de la red con una o más políticas para el sistema operativo central, como se discute en la presente memoria.

En respuesta a la determinación de que el recurso de red es un recurso de red no de confianza, el sistema operativo central está configurado para activar un contenedor que está aislado del sistema operativo central (acto 608). Como se discute en la presente memoria, un contenedor que está aislado del sistema operativo central incluye su propio núcleo que está separado y aislado de un núcleo del sistema operativo central, protegiendo así el sistema operativo central de los ataques del núcleo.

Después de que el sistema operativo central activa el contenedor aislado, el sistema operativo central lanza una versión virtual de la aplicación que solicitó el recurso de red no de confianza dentro del contenedor aislado (acto 610). La versión virtual de la aplicación lanzada dentro del contenedor aislado está configurada para manejar el recurso de red solicitado de manera similar a cómo la aplicación que se ejecuta en el sistema operativo central manejaría el recurso de red solicitado.

En respuesta al lanzamiento de la versión virtual de la aplicación en el contenedor aislado, el sistema operativo central pasa el recurso de red no de confianza al contenedor aislado y permite que la versión de la aplicación que se ejecuta en el contenedor aislado acceda al recurso de red no de confianza (acto 612). En respuesta al lanzamiento de la versión de la aplicación en el contenedor aislado, el sistema operativo central también está configurado para mostrar una interfaz para la versión de la aplicación que opera dentro del contenedor aislado en una pantalla del dispositivo que implementa el sistema operativo central (acto 614) Por lo tanto, el sistema operativo central permite al usuario interactuar con la versión virtual de la aplicación lanzada dentro del contenedor aislado sin exponer el sistema operativo central a uno o más recursos de red no de confianza a los que accede el contenedor aislado.

Mientras que está ejecutándose la versión virtual de la aplicación dentro del contenedor aislado, el sistema operativo central está configurado para permitir que la versión virtual de la aplicación en el contenedor aislado acceda a uno o más recursos de red adicionales no de confianza (acto 618). El sistema operativo central está configurado para permitir que la versión de la aplicación que se ejecuta dentro del contenedor aislado acceda a recursos de red no de confianza mediante la supervisión de las comunicaciones de red entre el contenedor aislado y una o más ubicaciones de recursos de red.

De manera similar, mientras que está ejecutándose la versión virtual de la aplicación dentro del contenedor aislado, el sistema operativo central está configurado para evitar que la versión virtual de la aplicación en el contenedor aislado acceda a uno o más recursos de red de confianza (acto 620). De esta manera, el sistema operativo central se configura para asegurar que solo el sistema operativo central acceda a los recursos de red de confianza y que solo uno o más contenedores aislados accedan a los recursos de la red no de confianza.

En respuesta a la determinación de que la versión virtual de la aplicación que se ejecuta dentro del contenedor aislado ya no está accediendo a uno o más recursos de red no de confianza, o en respuesta a la determinación de que un usuario del sistema operativo central ha cerrado la sesión, el sistema operativo central está configurado suspender uno o más contenedores aislados (acto 622). Por ejemplo, en respuesta a la determinación de que la versión de la aplicación dentro del contenedor ya no está accediendo a uno o más recursos de red no de confianza, el sistema operativo central suspende el contenedor hasta que sea necesario para manejar uno o más recursos de red no de confianza adicionales. Si el sistema operativo central detecta que un usuario ha cerrado la sesión, el sistema operativo central elimina uno o más contenedores, ya sean activos o suspendidos.

Sistema de ejemplo

Aunque la funcionalidad particular se discute en la presente memoria con referencia a módulos particulares, se debe tener en cuenta que la funcionalidad de los módulos individuales discutidos en la presente memoria se puede separar en múltiples módulos, y/o al menos alguna funcionalidad de múltiples módulos se puede combinar en un solo módulo. Además, un módulo particular discutido en la presente memoria como realizar una acción incluye ese módulo particular en sí mismo que realiza la acción, o alternativamente ese módulo particular que invoca o accede de otro modo a otro componente o módulo que realiza la acción (o realiza la acción junto con ese módulo particular). Por lo tanto, un módulo particular que realiza una acción incluye ese módulo particular en sí mismo que realiza la acción y/u otro módulo invocado o al que accede de otro modo ese módulo particular que realiza la acción.

La Figura 7 ilustra un sistema de ejemplo generalmente en 700 que incluye un dispositivo de cálculo 702 de ejemplo que es representativo de uno o más sistemas y/o dispositivos que pueden implementar las diversas técnicas descritas en la presente memoria. El dispositivo informático 702 puede ser, por ejemplo, un servidor de un proveedor de servicios, un dispositivo asociado con un cliente (por ejemplo, un dispositivo cliente), un sistema en chip y/o cualquier otro dispositivo informático o sistema informático adecuado.

El dispositivo informático 702 de ejemplo como se ilustra incluye un sistema de procesamiento 704, uno o más medios legibles por ordenador 706, y una o más interfaces de I/O 708 que están acopladas comunicativamente, una a otra. Aunque no se muestra, el dispositivo informático 702 puede incluir además un bus del sistema u otro sistema de transferencia de datos y comandos que acople los diversos componentes, unos a otros. Un bus del sistema puede incluir una cualquiera o una combinación de diferentes estructuras de bus, tales como un bus de memoria o controlador de memoria, un bus periférico, un bus serie universal y/o un procesador o bus local que utiliza cualquiera de una variedad de arquitecturas de bus. También se contempla una variedad de otros ejemplos, tales como líneas de control y datos.

El sistema de procesamiento 704 es representativo de la funcionalidad para realizar una o más operaciones usando hardware. En consecuencia, se ilustra que el sistema de procesamiento 704 incluye elementos de hardware 710 que pueden configurarse como procesadores, bloques funcionales, etc. Esto puede incluir la implementación en hardware como un circuito integrado de aplicación específica u otro dispositivo lógico formado usando uno o más semiconductores. Los elementos de hardware 710 no están limitados por los materiales a partir de los cuales se forman o los mecanismos de procesamiento empleados en ellos. Por ejemplo, los procesadores pueden estar compuestos por semiconductor o semiconductores y/o transistores (por ejemplo, circuitos integrados (IC) electrónicos). En dicho contexto, las instrucciones ejecutables por procesador pueden ser instrucciones ejecutables electrónicamente.

Los medios legibles por ordenador 706 se ilustran incluyendo memoria/almacenamiento 712. La memoria/almacenamiento 712 representa la capacidad de memoria almacenamiento asociada con uno o más medios legibles por ordenador. La memoria/almacenamiento 712 puede incluir medios volátiles (tales como memoria de acceso aleatorio (RAM)) y/o medios no volátiles (tales como memoria de solo lectura (ROM), RAM resistiva (ReRAM), memoria Flash, discos ópticos, discos magnéticos, etc.). La memoria/almacenamiento 712 puede incluir medios fijos (por ejemplo, RAM, ROM, un disco duro fijo, etc.) así como medios extraíbles (por ejemplo, memoria Flash, un disco duro extraíble, un disco óptico, etc.). Los medios legibles por ordenador 706 pueden configurarse de una variedad de otras formas como se describe además a continuación.

La una o más interfaces de entrada salida 708 son representativas de la funcionalidad para permitir que un usuario ingrese comandos e información al dispositivo informático 702, y también permiten que se presente información al usuario y/u otros componentes o dispositivos que utilizan varios dispositivos de entrada/salida. Los ejemplos de dispositivos de entrada incluyen un teclado, un dispositivo de control del cursor (por ejemplo, un ratón), un micrófono (por ejemplo, para entradas de voz), un escáner, funcionalidad táctil (por ejemplo, sensores capacitivos u otros que están configurados para detectar el tacto físico), una cámara (por ejemplo, que puede emplear longitudes de onda visibles o no visibles, tales como frecuencias de infrarrojos para detectar movimientos que no implican el tacto como gestos), un sensor (por ejemplo, un sensor de luz ambiental o un sensor de movimiento), etc. Los ejemplos de dispositivos de salida incluyen un dispositivo de visualización (por ejemplo, un monitor o proyector), altavoces, una impresora, una tarjeta de red, un dispositivo de respuesta táctil, etc. Por lo tanto, el dispositivo informático 702 puede configurarse de varias maneras, como se describe además a continuación para apoyar la interacción del usuario.

El dispositivo informático 702 también incluye un sistema operativo central 714. El sistema operativo central 714 proporciona diversas gestiones de aislamiento de seguridad virtualizado basado en hardware, como se discutió anteriormente. El sistema operativo central 714 puede implementar, por ejemplo, el sistema operativo central 102 de la Figura 1.

Se pueden describir varias técnicas en la presente memoria en el contexto general de software, elementos de hardware o módulos de programa. En general, dichos módulos incluyen rutinas, programas, objetos, elementos, componentes, estructuras de datos, etc., que realizan tareas particulares o implementan tipos de datos abstractos particulares. Los términos "módulo", "funcionalidad" y "componente" como se usan en la presente memoria generalmente representan software, microprogramas, hardware o una combinación de los mismos. Las

características de las técnicas descritas en la presente memoria son independientes de la plataforma, lo que significa que las técnicas pueden implementarse en una variedad de plataformas informáticas que tienen una variedad de procesadores.

Una implementación de los módulos y técnicas descritos puede almacenarse o transmitirse a través de algún tipo de medio legible por ordenador. Los medios legibles por ordenador pueden incluir una variedad de medios a los que puede acceder el dispositivo informático 702. A modo de ejemplo, sin limitación, los medios legibles por ordenador pueden incluir "medios de almacenamiento legibles por ordenador" y "medios de señal legibles por ordenador".

"Medios de almacenamiento legibles por ordenador" se refiere a los medios y/o dispositivos que permiten el almacenamiento persistente de información y/o almacenamiento que es tangible, en contraste con la simple transmisión de señal, ondas portadoras o señales per se. Por lo tanto, los medios de almacenamiento legibles por ordenador se refieren a medios sin portador de señal. Los medios de almacenamiento legibles por ordenador incluyen hardware tal como medios volátiles y no volátiles, medios extraíbles y no extraíbles y/o dispositivos de almacenamiento implementados en un método o tecnología adecuada para el almacenamiento de información, tal como instrucciones legibles por ordenador, estructuras de datos, módulos de programa, elementos/circuitos lógicos u otros datos. Los ejemplos de medios de almacenamiento legibles por ordenador pueden incluir, entre otros, RAM, ROM, EEPROM, memoria flash u otra tecnología de memoria, CD-ROM, discos versátiles digitales (DVD) u otro almacenamiento óptico, discos duros, casetes magnéticos, cinta magnética, almacenamiento en disco magnético u otros dispositivos de almacenamiento magnético, u otro dispositivo de almacenamiento, medio tangible o artículo de fabricación adecuado para almacenar la información deseada y a la que puede acceder un ordenador.

"Medios de señal legibles por ordenador" se refiere a un medio portador de señal que está configurado para transmitir instrucciones al hardware del dispositivo informático 702, tal como a través de una red. Los medios de señal generalmente pueden incorporar instrucciones legibles por ordenador, estructuras de datos, módulos de programa u otros datos en una señal de datos modulada, tales como ondas portadoras, señales de datos u otro mecanismo de transporte. Los medios de señal también incluyen cualquier medio de entrega de información. El término "señal de datos modulados" significa una señal que tiene una o más de sus características establecidas o cambiadas de tal manera que codifique información en la señal. A modo de ejemplo, y no limitativo, los medios de comunicación incluyen medios cableados tales como una red cableada o conexión cableada directa, y medios inalámbricos como acústicos, RF, infrarrojos y otros medios inalámbricos.

Como se describió anteriormente, los elementos de hardware 710 y los medios legibles por ordenador 706 son representativos de instrucciones, módulos, lógica de dispositivo programable y/o lógica de dispositivo fijo implementada en una forma de hardware que puede emplearse en algunas realizaciones para implementar al menos algunos aspectos de las técnicas descritas en la presente memoria. Los elementos de hardware pueden incluir componentes de un circuito integrado o sistema en chip, un circuito integrado de aplicación específica (ASIC), una agrupación de puertas programables en campo (FPGA), un dispositivo lógico programable complejo (CPLD) y otras implementaciones en silicio u otros dispositivos de hardware En este contexto, un elemento de hardware puede funcionar como un dispositivo de procesamiento que realiza tareas de programa definidas por instrucciones, módulos y/o lógica incorporados por el elemento de hardware, así como un dispositivo de hardware utilizado para almacenar instrucciones de ejecución, por ejemplo, los medios de almacenamiento legibles por ordenador descritos anteriormente.

Las combinaciones de lo anterior también pueden emplearse para implementar diversas técnicas y módulos descritos en la presente memoria. En consecuencia, los módulos de software, hardware o programa y otros módulos de programa pueden implementarse como una o más instrucciones y/o lógica incorporadas en alguna forma de medios de almacenamiento legibles por ordenador y/o por uno o más elementos de hardware 710. El dispositivo informático 702 puede configurarse para implementar instrucciones particulares y/o funciones correspondientes a los módulos de software y/o hardware. En consecuencia, la implementación de módulos como un módulo que es ejecutable por el dispositivo informático 702 como software puede lograrse al menos parcialmente en hardware, por ejemplo, mediante el uso de medios de almacenamiento legibles por ordenador y/o elementos de hardware 710 del sistema de procesamiento. Las instrucciones y/o funciones pueden ser ejecutables/operables por uno o más artículos de fabricación (por ejemplo, uno o más dispositivos informáticos 702 y/o sistemas de procesamiento 704) para implementar técnicas, módulos y ejemplos descritos en la presente memoria.

Como se ilustra adicionalmente en la Figura 7, el sistema 700 de ejemplo habilita entornos ubicuos para una experiencia de usuario sin problemas cuando se ejecutan aplicaciones en un ordenador personal (PC), un dispositivo de televisión y/o un dispositivo móvil. Los servicios y las aplicaciones se ejecutan de manera sustancialmente similar en los tres entornos para una experiencia de usuario común cuando se pasa de un dispositivo al siguiente mientras que se utiliza una aplicación, jugar un videojuego, mirar un video, etc.

En el sistema 700 de ejemplo, múltiples dispositivos están interconectados a través de un dispositivo informático central. El dispositivo informático central puede ser local para los múltiples dispositivos o puede estar ubicado de forma remota desde los múltiples dispositivos. En una o más realizaciones, el dispositivo informático central puede ser una nube de uno o más ordenadores de servidor que están conectados a los múltiples dispositivos a través de una red, Internet u otro enlace de comunicación de datos.

En una o más realizaciones, esta arquitectura de interconexión permite que la funcionalidad se entregue a través de múltiples dispositivos para proporcionar una experiencia común y sin problemas al usuario de los múltiples dispositivos. Cada uno de los múltiples dispositivos puede tener diferentes requisitos y capacidades físicas, y el dispositivo informático central utiliza una plataforma para permitir la entrega de una experiencia al dispositivo que tanto se adapta al dispositivo como, sin embargo, es común a todos los dispositivos. En una o más realizaciones, se crea una clase de dispositivos objetivo y las experiencias se adaptan a la clase genérica de dispositivos. Una clase de dispositivos puede definirse por características físicas, tipos de uso u otras características comunes de los dispositivos.

En diversas implementaciones, el dispositivo informático 702 puede asumir una variedad de configuraciones diferentes, tales como para los usos del ordenador 716, el móvil 718 y la televisión 720. Cada una de estas configuraciones incluye dispositivos que pueden tener construcciones y capacidades generalmente diferentes, y por lo tanto el dispositivo informático 702 puede configurarse según una o más de las diferentes clases de dispositivos. Por ejemplo, el dispositivo informático 702 puede implementarse como la clase de ordenador 716 de un dispositivo que incluye un ordenador personal, un ordenador de escritorio, un ordenador de pantallas múltiples, un ordenador portátil, un miniordenador portátil, etc.

El dispositivo informático 702 también puede implementarse como la clase de dispositivo móvil 718 que incluye dispositivos móviles, tales como un teléfono móvil, un reproductor de música portátil, un dispositivo de juegos portátil, una tableta, un ordenador con pantallas múltiples, etc. El dispositivo informático 702 también puede implementarse como la clase de dispositivo de televisión 720 que incluye dispositivos que tienen o están conectados a pantallas generalmente más grandes en entornos de visualización casuales. Estos dispositivos incluyen televisores, decodificadores, consolas de juegos, etc.

Las técnicas descritas en la presente memoria pueden estar respaldadas por estas diversas configuraciones del dispositivo informático 702 y no se limitan a los ejemplos específicos de las técnicas descritas en la presente memoria. Esta funcionalidad también puede implementarse total o parcialmente mediante el uso de un sistema distribuido, tal como a través de una "nube" 722 a través de una plataforma 724 como se describe a continuación.

La nube 722 incluye y/o es representativa de una plataforma 724 para los recursos 726. La plataforma 724 abstrae la funcionalidad subyacente del hardware (por ejemplo, servidores) y los recursos de software de la nube 722. Los recursos 726 pueden incluir aplicaciones y/o datos que pueden ser utilizados mientras que el procesamiento informático se ejecuta en servidores que están remotos del dispositivo informático 702. Los recursos 726 también pueden incluir servicios proporcionados a través de Internet y/o a través de una red de abonado, tal como una red celular o Wi-Fi.

La plataforma 724 puede abstraer recursos y funciones para conectar el dispositivo informático 702 con otros dispositivos informáticos. La plataforma 724 también puede servir para abstraer el escalado de recursos para proporcionar un nivel de escala correspondiente a la demanda encontrada para los recursos 726 que se implementan a través de la plataforma 724. Por consiguiente, en una realización de dispositivo interconectado, la implementación de la funcionalidad descrita en la presente memoria puede distribuirse a lo largo del sistema 700. Por ejemplo, la funcionalidad puede implementarse en parte en el dispositivo informático 702, así como a través de la plataforma 724 que abstrae la funcionalidad de la nube 722. Cabe señalar que la nube 722 se puede organizar en una miríada de configuraciones. Por ejemplo, la nube 722 se puede implementar como una sola nube, como múltiples instancias de la nube 722, todas comportándose como una sola nube, o con una o más instancias de la plataforma 724 implementadas detrás de la nube 722 y comportándose como si la una o más instancias de la plataforma 724 se implementaron en la nube.

En las discusiones en la presente memoria, se describen diversas realizaciones diferentes. Debe apreciarse y entenderse que cada realización descrita en la presente memoria puede usarse por sí misma o en conexión con una o más de las otras realizaciones descritas en la presente memoria.

Aunque el tema se ha descrito en un lenguaje específico para características estructurales y/o actos metodológicos, debe entenderse que el tema definido en las reivindicaciones adjuntas no se limita necesariamente a las características o actos específicos descritos anteriormente. Más bien, las características y los actos específicos descritos anteriormente se describen como formas de ejemplo de implementación de las reivindicaciones. La invención se define por el alcance de las reivindicaciones adjuntas.

**REIVINDICACIONES**

1. Un método realizado por un sistema operativo central que se ejecuta en un dispositivo central que comprende:

ejecutar (602), una aplicación en el sistema operativo central;

detectar (604) que la aplicación que se ejecuta en el sistema operativo central está intentando acceder a un recurso de red accesible al dispositivo central a través de una red;

determinar (606) que el recurso de red es un recurso de red no de confianza; y en respuesta a la determinación de que el recurso de red es un recurso de red no de confianza:

activar (608) un contenedor que está aislado del sistema operativo central y configurado para ejecutar una versión de la aplicación; y

permitir (612) que la versión de la aplicación que se ejecuta en el contenedor acceda al recurso de red no de confianza; y

en respuesta a la determinación de que el acceso al recurso de red no de confianza ha finalizado, suspender (622) el contenedor hasta que sea necesario para manejar uno o más recursos de red no de confianza adicionales.

2. El método según la reivindicación 1, que comprende además permitir que la versión de la aplicación que se ejecuta en el contenedor acceda a uno o más recursos de red no de confianza adicionales y evitar que la aplicación que se ejecuta en el contenedor acceda a recursos de red de confianza.

3. El método según la reivindicación 1 o la reivindicación 2, en donde el contenedor incluye una instancia del sistema operativo central y un núcleo que está separado y aislado de un núcleo del sistema operativo central.

4. El método según cualquiera de las reivindicaciones 1 a 3, que comprende además recibir al menos una política que incluye al menos una lista enumerada de recursos de red de confianza, en donde determinar que el recurso de red es un recurso de red no de confianza comprende comparar el recurso de red con la lista enumerada de recursos de red de confianza, la lista enumerada de recursos de red de confianza que se identifica en base a uno o más de un tipo de archivo del recurso de red, una ubicación de red asociada con el recurso de red o un tipo de aplicación que está intentando acceder al recurso de red.

5. El método según cualquiera de las reivindicaciones 1 a 4, en donde el contenedor se activa para un usuario que ha iniciado sesión en el sistema operativo central, el método que comprende además determinar que un usuario diferente ha iniciado sesión en el sistema operativo central y activar, para el usuario diferente, un contenedor diferente que está aislado del sistema operativo central y el contenedor.

6. El método según cualquiera de las reivindicaciones 1 a 5, que comprende además determinar que la aplicación está intentando acceder al recurso de red a través de una interfaz de red no de confianza y, en respuesta a determinar que la aplicación está intentando acceder al recurso de red a través de la interfaz de red no de confianza:

restringir las comunicaciones de red para la aplicación en el sistema operativo central a una interfaz de red privada virtual (VPN);

permitir que la versión de la aplicación que se ejecuta en el contenedor realice comunicaciones de red a través de la interfaz de red no de confianza; e

indicar a una pila de red del contenedor que las comunicaciones de red para el contenedor están aisladas de la interfaz de red no de confianza.

7. El método según en cualquiera de las reivindicaciones 1 a 6, que comprende además interceptar una respuesta a una solicitud de intermediario web para credenciales de usuario e insertar una o más credenciales de usuario en la respuesta a la solicitud de intermediario web sin comunicar la una o más credenciales de usuario al contenedor.

8. El método según cualquiera de las reivindicaciones 1 a 7, que comprende además escanear uno o más recursos de red no de confianza a los que se accede en el contenedor y usar software antivirus en el sistema operativo central para asignar uno o más niveles de riesgo al uno o más recursos de red no de confianza y poner en cuarentena, limpiar o eliminar uno del uno o más recursos de red no de confianza si el nivel de riesgo asignado indica que el recurso de red no de confianza es malicioso.

9. El método según cualquiera de las reivindicaciones 1 a 8, que comprende además la actividad de supervisión asociada con el recurso de red no de confianza en el contenedor y la actualización de la política local en el sistema operativo central en función de la actividad supervisada.

10. El método según cualquiera de las reivindicaciones anteriores, en donde suspender el contenedor comprende conservar el estado de uno o más recursos de red dentro del contenedor.

11. El método según cualquiera de las reivindicaciones anteriores, en donde activar un contenedor comprende identificar un contenedor suspendido y reanudar el procesamiento del contenedor suspendido.

12. El método según cualquiera de las reivindicaciones 1 a 11, en donde el contenedor se activa para comunicaciones de recursos de red a través de una primera interfaz de comunicación de red, comprendiendo además el método activar un segundo contenedor para comunicaciones de recursos de red a través de una segunda interfaz de comunicación de red.

13. Un dispositivo que comprende:

uno o más procesadores (704); y

uno o más medios de almacenamiento legibles por ordenador (706) que almacenan instrucciones legibles por ordenador que son ejecutables por uno o más procesadores para realizar operaciones que comprenden:

ejecutar una aplicación web en un sistema operativo central del dispositivo;

detectar, mediante el sistema operativo central, que la aplicación que se ejecuta en el sistema operativo central está intentando acceder a un recurso de red accesible al dispositivo a través de una red;

determinar, por el sistema operativo central, que el recurso de red es un recurso no de confianza comparando el recurso de red con una política recibida de un servicio de gestión y supervisión que se encuentra remotamente desde el dispositivo;

en respuesta a la determinación de que el recurso de red es un recurso de red no de confianza:

activar, mediante el sistema operativo central, un contenedor que está aislado del sistema operativo central y configurado para ejecutar una versión de la aplicación web;

permitir, por el sistema operativo central, la versión de la aplicación web que se ejecuta en el contenedor para acceder al recurso de red no de confianza;

en respuesta a la determinación de que el acceso al recurso de red no de confianza ha finalizado, suspender, por el sistema operativo central, el contenedor hasta que sea necesario para manejar uno o más recursos de red no de confianza adicionales.

14. El dispositivo según la reivindicación 13, las operaciones que comprenden además detectar una actualización del sistema operativo central y, en respuesta a detectar la actualización del sistema operativo central, eliminar el contenedor y crear un nuevo contenedor que refleje uno o más archivos binarios actualizados del sistema operativo central.

15. El dispositivo según la reivindicación 13 o la reivindicación 14, en donde el sistema operativo central está configurado para determinar que el recurso de red y uno o más recursos de red no de confianza adicionales no están basados en uno o más de un tipo de archivo del recurso de red, un ubicación de red asociada con el recurso de red, un tipo de aplicación que está intentando acceder al recurso de red, escaneo antivirus del recurso de red o basado en la consulta de un servicio basado en la nube que mantiene una lista de recursos de red maliciosos.

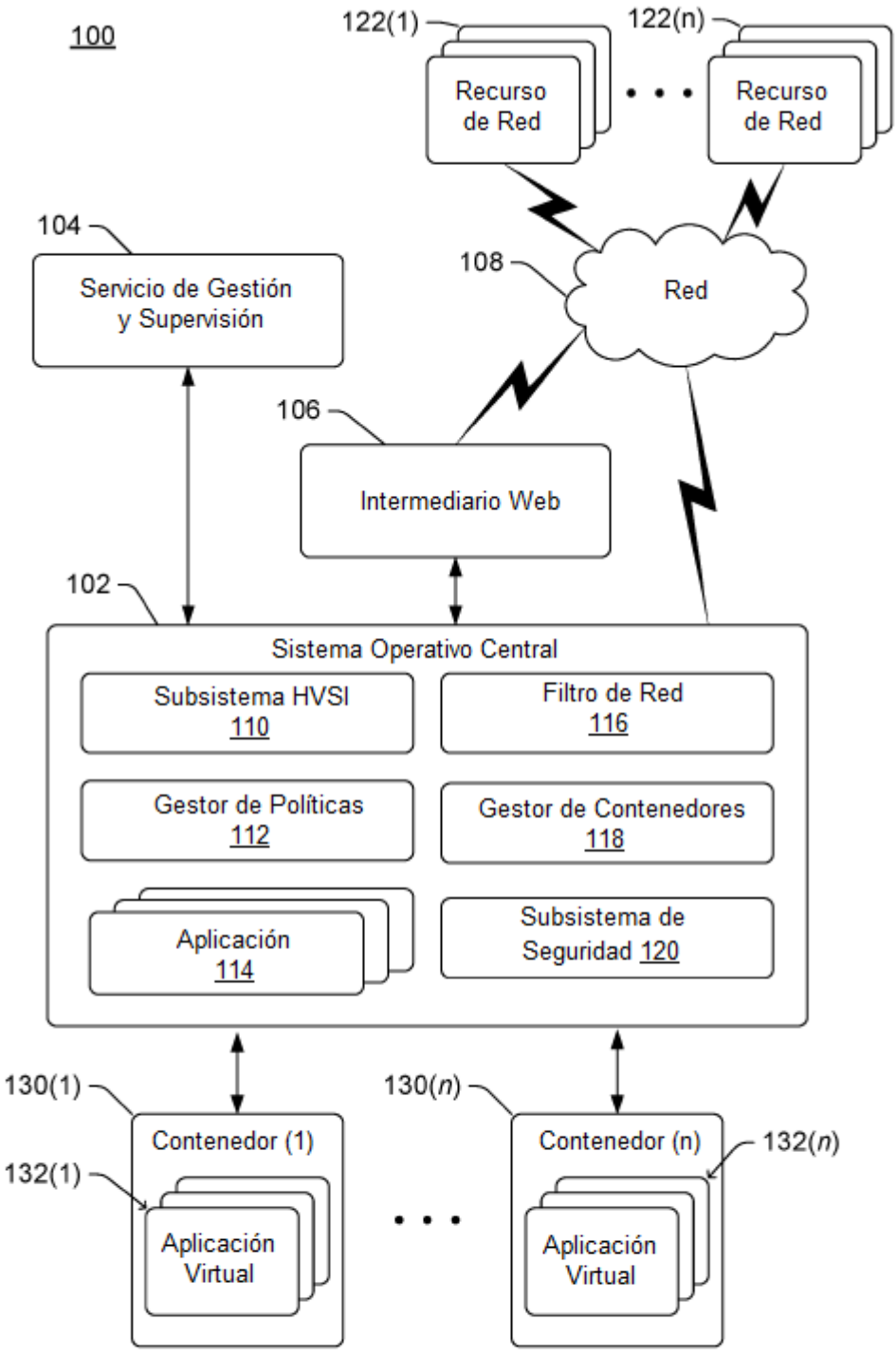
100
122(1)
122(n)
Recurso de Red
Recurso de Red
104
Servicio de Gestión y Supervisión
108
Red
106
Intermediario Web
102
Sistema Operativo Central
Subsistema HVSI 110
Filtro de Red 116
Gestor de Políticas 112
Gestor de Contenedores 118
Aplicación 114
Subsistema de Seguridad 120
130(1)
130(n)
Contenedor (1)
Contenedor (n)
132(1)
132(n)
Aplicación Virtual
Aplicación Virtual

**Fig. 1**

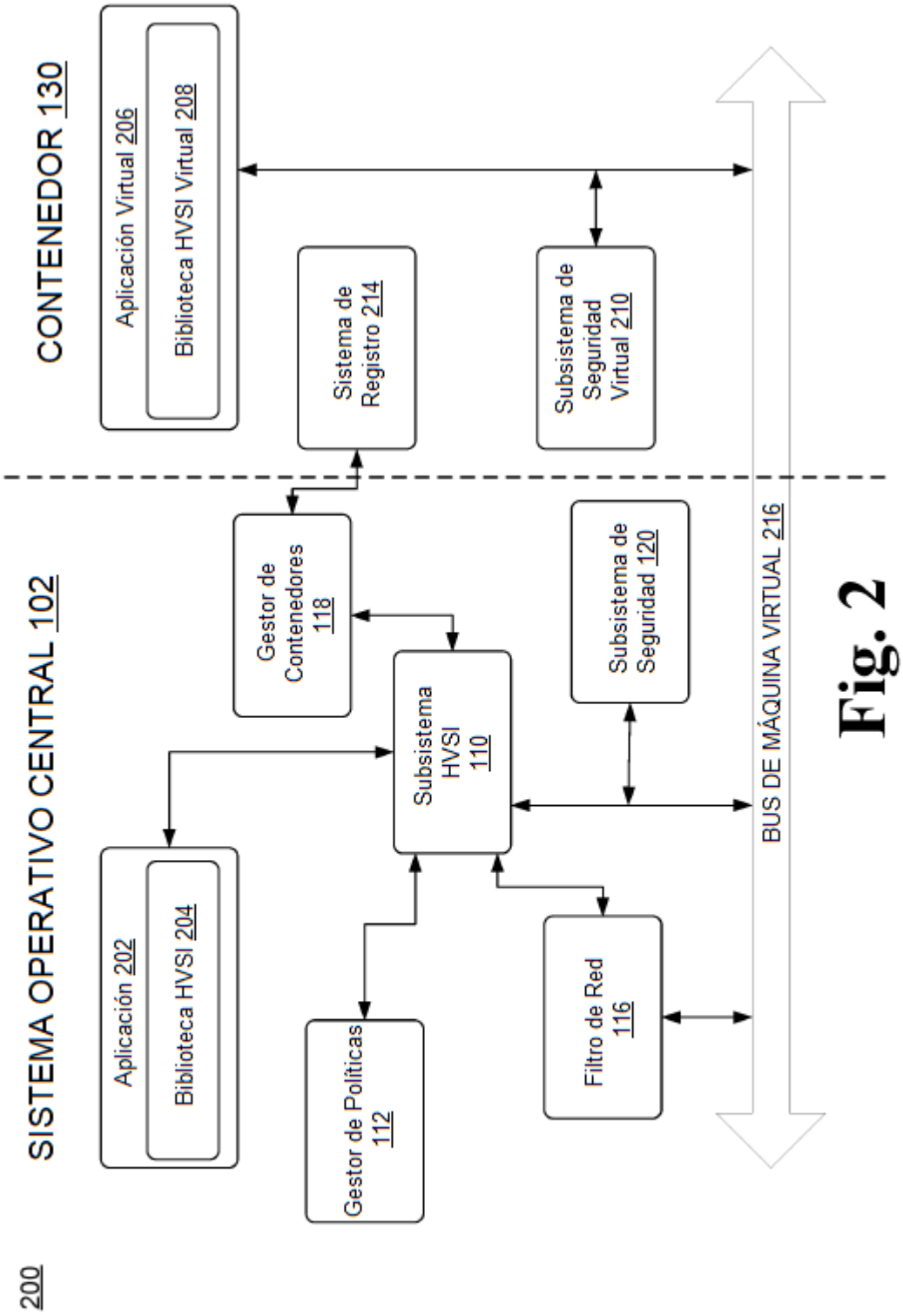
200
SISTEMA OPERATIVO CENTRAL 102
CONTENEDOR 130
Aplicación 202
Biblioteca HVSI 204
Aplicación Virtual 206
Biblioteca HVSI Virtual 208
Gestor de Políticas 112
Gestor de Contenedores 118
Subsistema HVSI 110
Filtro de Red 116
Sistema de Registro 214
Subsistema de Seguridad 120
Subsistema de Seguridad Virtual 210
BUS DE MÁQUINA VIRTUAL 216

Fig. 2

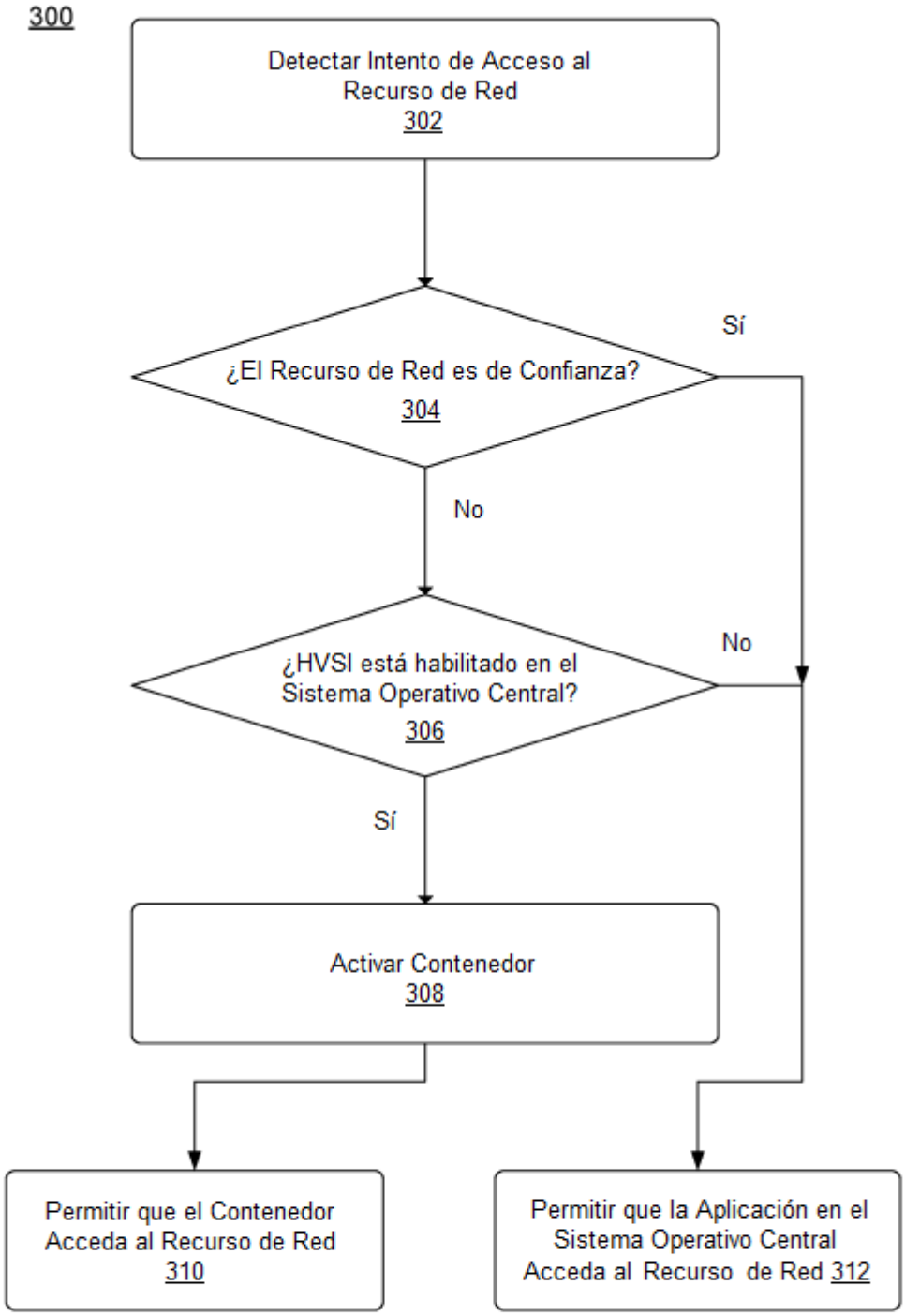
300
Detectar Intento de Acceso al Recurso de Red 302
¿El Recurso de Red es de Confianza? 304
Sí
No
¿HVSI está habilitado en el Sistema Operativo Central? 306
No
Sí
Activar Contenedor 308
Permitir que el Contenedor Acceda al Recurso de Red 310
Permitir que la Aplicación en el Sistema Operativo Central Acceda al Recurso de Red 312

**Fig. 3**

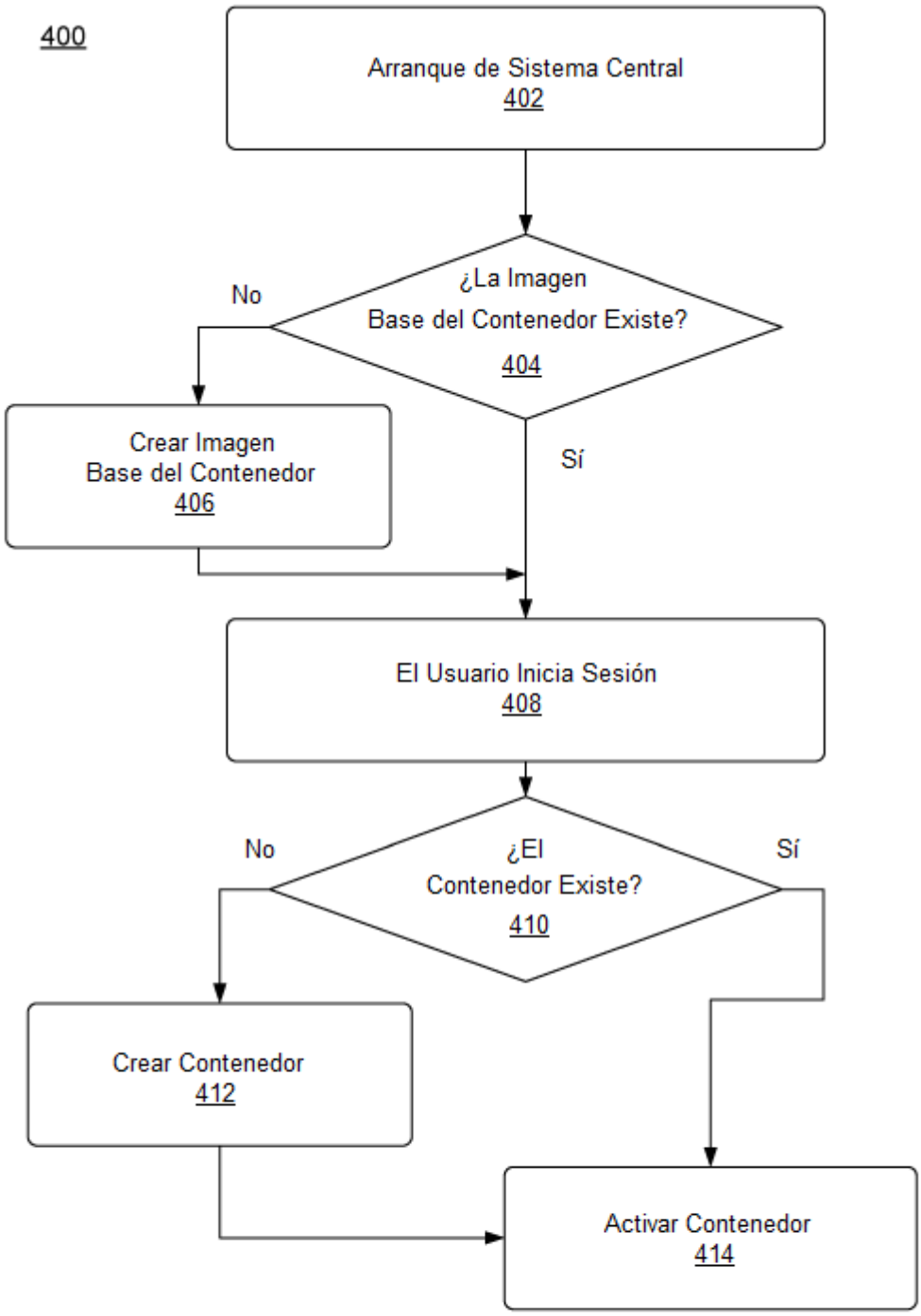
400
Arranque de Sistema Central
402
¿La Imagen
Base del Contenedor Existe?
404
No
Sí
Crear Imagen
Base del Contenedor
406
El Usuario Inicia Sesión
408
¿El
Contenedor Existe?
410
No
Sí
Crear Contenedor
412
Activar Contenedor
414

**Fig. 4**

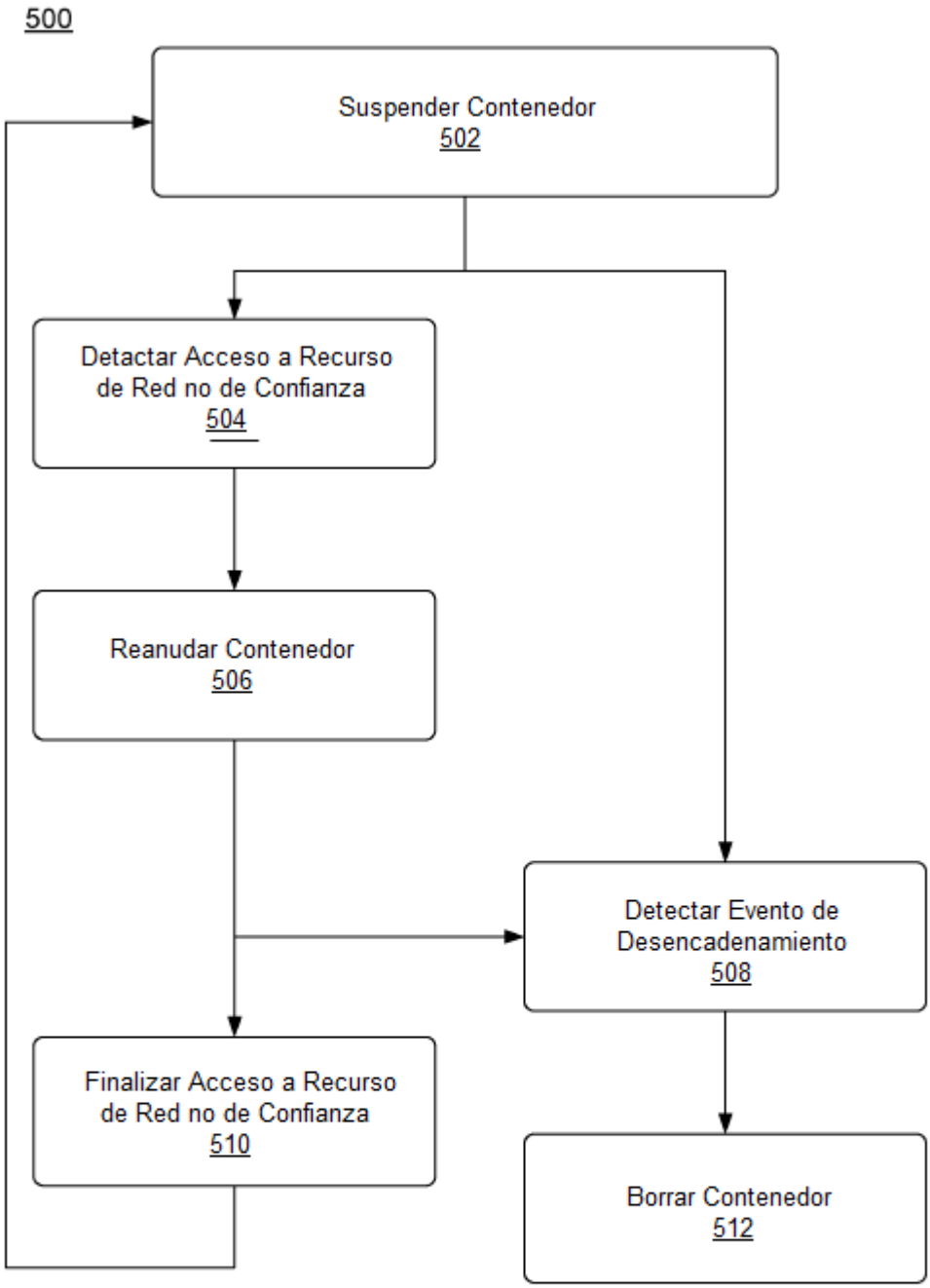
500
Suspender Contenedor
502
Detactar Acceso a Recurso de Red no de Confianza
504
Reanudar Contenedor
506
Detectar Evento de Desencadenamiento
508
Finalizar Acceso a Recurso de Red no de Confianza
510
Borrar Contenedor
512

**Fig. 5**

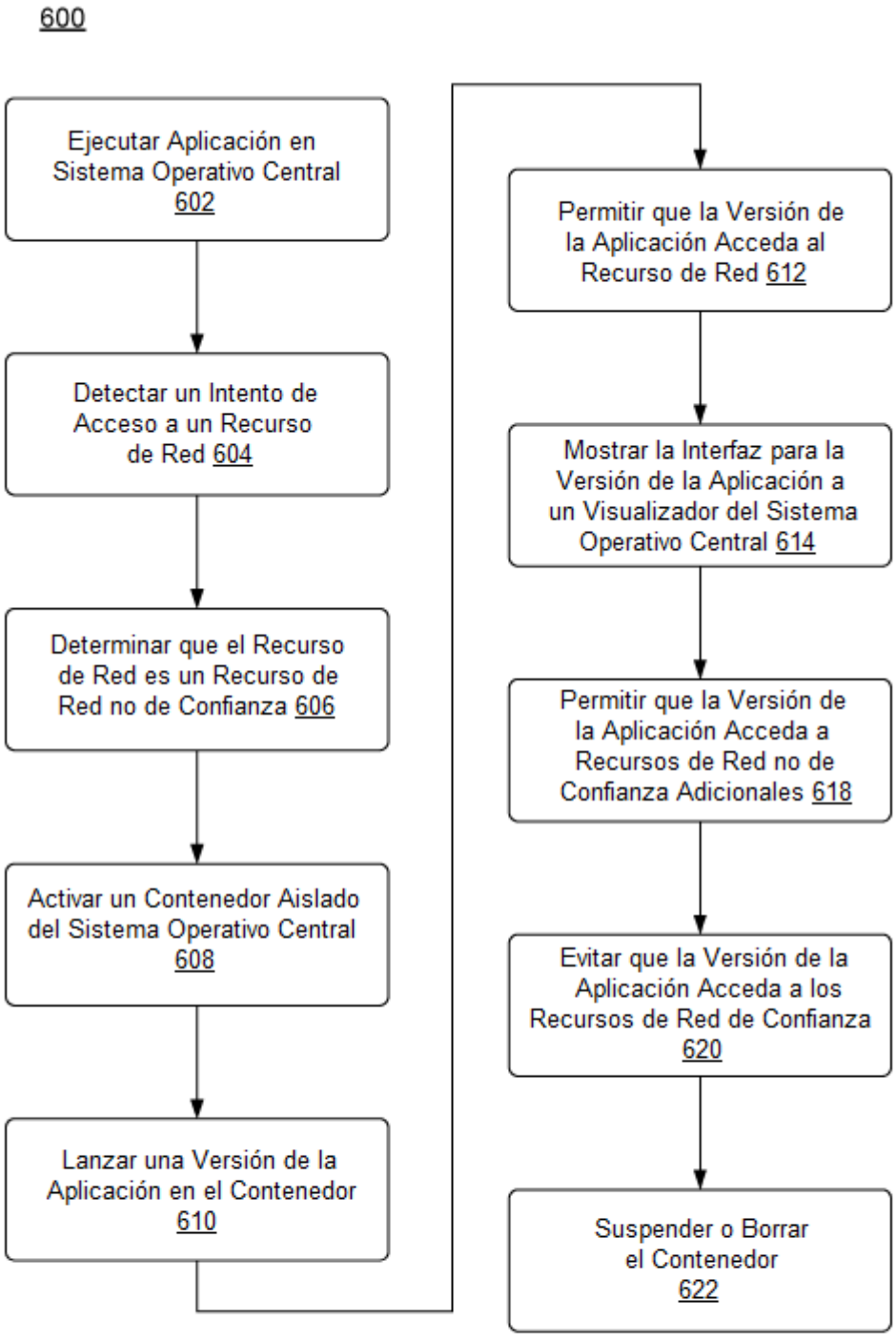
600
Ejecutar Aplicación en Sistema Operativo Central 602
Detectar un Intento de Acceso a un Recurso de Red 604
Determinar que el Recurso de Red es un Recurso de Red no de Confianza 606
Activar un Contenedor Aislado del Sistema Operativo Central 608
Lanzar una Versión de la Aplicación en el Contenedor 610
Permitir que la Versión de la Aplicación Acceda al Recurso de Red 612
Mostrar la Interfaz para la Versión de la Aplicación a un Visualizador del Sistema Operativo Central 614
Permitir que la Versión de la Aplicación Acceda a Recursos de Red no de Confianza Adicionales 618
Evitar que la Versión de la Aplicación Acceda a los Recursos de Red de Confianza 620
Suspender o Borrar el Contenedor 622

**Fig. 6**

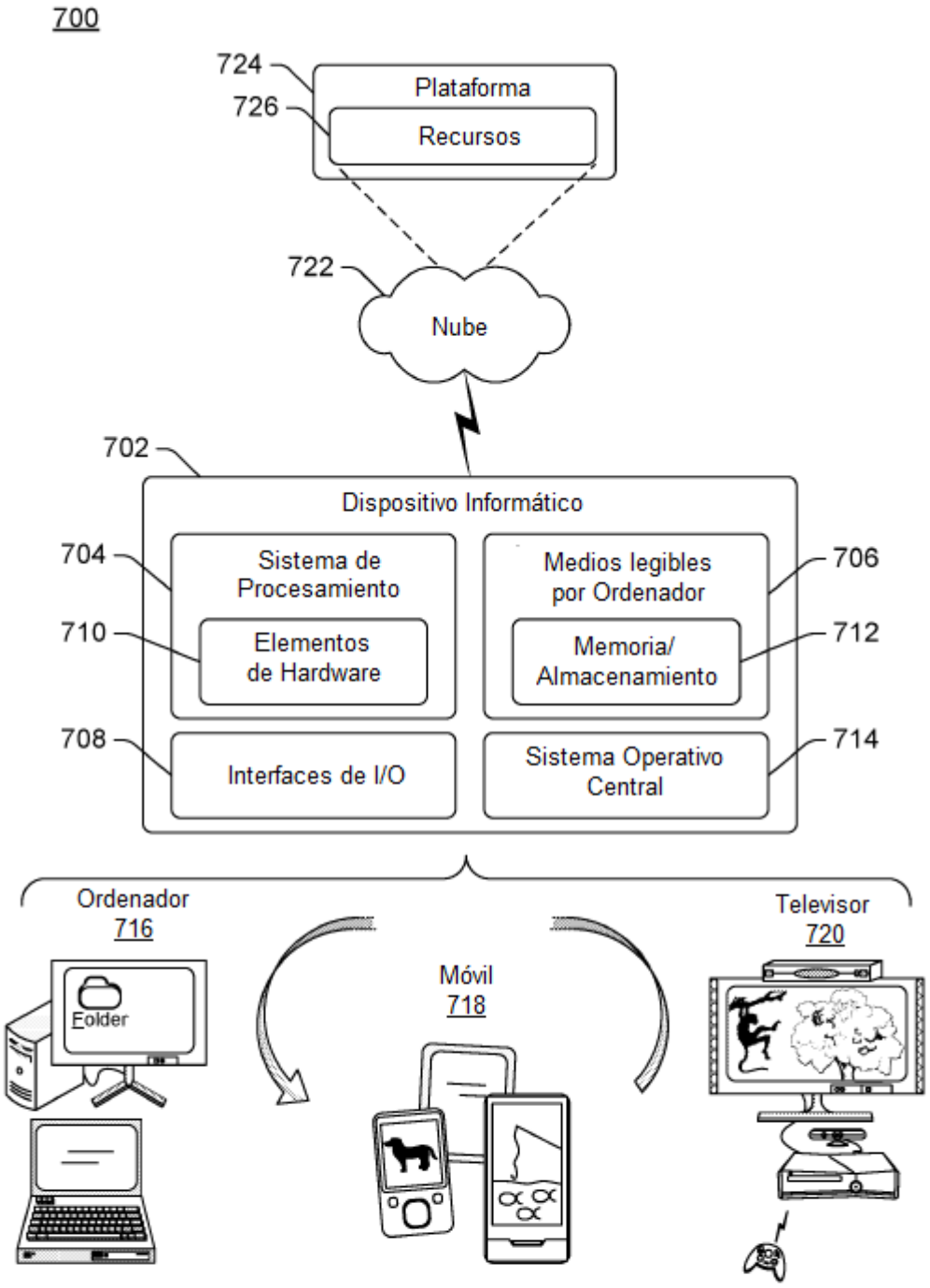
700
724
Plataforma
726
Recursos
722
Nube
702
Dispositivo Informático
704
Sistema de Procesamiento
710
Elementos de Hardware
706
Medios legibles por Ordenador
712
Memoria/ Almacenamiento
708
Interfaces de I/O
714
Sistema Operativo Central
Ordenador
716
Folder
Móvil
718
Televisor
720

**Fig. 7**