(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 804 174**

(51) Int. CI.:

H04L 29/08 (2006.01)
H04L 29/06 (2006.01)
G06F 9/50 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **19.01.2016 PCT/US2016/013944**

(87) Fecha y número de publicación internacional: **28.07.2016 WO16118518**

(96) Fecha de presentación y número de la solicitud europea: **19.01.2016 E 16740600 (8)**

(97) Fecha y número de publicación de la concesión europea: **08.04.2020 EP 3248100**

(54) Título: **Plataforma de seguridad gradual**

(30) Prioridad:

20.01.2015 US 201562105685 P
17.09.2015 US 201514857775

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
04.02.2021

(73) Titular/es:

CYEMPTIVE TECHNOLOGIES, INC. (100.0%)
18433 22nd Way NE
Woodinville, WA 98077, US

(72) Inventor/es:

PIKE, ROBERT

(74) Agente/Representante:

IZQUIERDO BLANCO, María Alicia

DESCRIPCIÓN

Plataforma de seguridad gradual

REFERENCIA CRUZADA A SOLICITUDES RELACIONADAS

Esta solicitud reivindica la prioridad de la Solicitud de Patente Provisional de Estados Unidos Nº 62/105.685, presentada el 20 de enero de 2015 y la Solicitud de Patente de Estados Unidos Nº 14/857.775, presentada el 17 de septiembre de 2015.

ANTECEDENTES

1. Campo

La presente divulgación se refiere a la seguridad informática contra el acceso no autorizado a los recursos, y más específicamente a una plataforma de seguridad gradual para una seguridad aumentada.

2. Descripción de la técnica relacionada

En las comunicaciones de red hay muchas formas de seguridad de software y hardware, incluyendo cortafuegos y sistemas de detección y prevención de intrusos. Pero todos fallan en un asunto central, que si las reglas no se aplican correctamente pueden abrir oportunidades para el acceso no autorizado. Los sistemas operativos y las aplicaciones actuales también tienen muchos errores que, si están expuestos a Internet, pueden permitir el acceso remoto a los servidores que alojan las aplicaciones.

La publicación IEEE Mantenimiento y evolución de los sistemas orientados a servicios y basados en la nube (MESOCA) "Cloud software upgrades: Challenges and opportunities" por Iulian Neamtiu y Tudor Dumitras propone una agenda de investigación para el futuro de las actualizaciones de software en la nube.

SUMARIO

La presente invención se define por las reivindicaciones independientes adjuntas.

Las realizaciones de la presente divulgación incluyen métodos y sistemas inteligentes para proporcionar seguridad en línea contra hackers. En una realización, se divulga un sistema para seguridad gradual. El sistema comprende un primer grupo de servidores y un segundo grupo de servidores. Cada servidor en el primer grupo de servidores y el segundo grupo de servidores incluye software que incluye un sistema operativo y una aplicación que admite sesiones de usuario. Un medio legible por ordenador no transitorio almacena instrucciones que, cuando son ejecutadas por al menos un procesador, hacen que el por lo menos un procesador acceda a la información de cadencia gradual que indica los cadencias de reconstrucción para el primer grupo de servidores y las cadencias de reconstrucción para el segundo grupo de servidores.

Las cadencias de reconstrucción para el primer grupo de servidores se escalonan en el tiempo desde las cadencias de reconstrucción del segundo grupo de servidores. Las instrucciones también hacen que el procesador inicie periódicamente la reconstrucción del software de cada servidor del primer grupo de servidores de acuerdo con las cadencias de reconstrucción para el primer grupo de servidores. Las instrucciones también hacen que el procesador inicie periódicamente la reconstrucción del software de cada servidor en el segundo grupo de servidores de los servidores de acuerdo con las segundas cadencias de reconstrucción para el segundo grupo de servidores. La reconstrucción del primer grupo de servidores se escalona en el tiempo a partir de la reconstrucción del segundo grupo de servidores de los servidores.

En una realización, se divulga un método de seguridad gradual para un sistema que incluye múltiples grupos de servidores. El método incluye iniciar repetidamente la reconstrucción del primer grupo de servidores de uno o más servidores. El método también incluye iniciar repetidamente la reconstrucción del segundo grupo de servidores de uno o más servidores. La reconstrucción del primer grupo de servidores de uno o más servidores se escalona en el tiempo a partir de la reconstrucción del segundo grupo de servidores de uno o más servidores.

En una realización, cada uno de los servidores en el primer y el segundo grupo incluye software que se reconstruye repetidamente, como de manera periódica. El software que se reconstruye puede incluir un sistema operativo, una aplicación y otro software. En una realización, cada uno de los servidores en el primer y el segundo grupo de servidores incluye un firmware respectivo. Iniciar la reconstrucción repetidamente del primer grupo de servidores comprende iniciar una reconstrucción del firmware respectivo en cada servidor del primer grupo de servidores. Iniciar la reconstrucción del segundo grupo de servidores comprende iniciar una reconstrucción del firmware respectivo en cada servidor del segundo grupo de servidores.

En una realización, cada uno de los servidores en el primer y el segundo grupo de servidores incluye una contraseña respectiva. El método también comprende iniciar repetidamente un cambio de contraseña de cada servidor en el primer grupo de servidores cuando se reconstruye el primer grupo de servidores; e iniciar repetidamente un cambio de contraseña de cada servidor en el segundo grupo de servidores cuando se reconstruye el segundo grupo de servidores.

En una realización, el método comprende acceder a información de cadencia gradual que indica cadencias de reconstrucción para reconstruir el primer grupo de servidores y el segundo grupo de servidores. El primer grupo de servidores y el segundo grupo de servidores se reconstruyen repetidamente de acuerdo con la información de cadencia gradual. Además, cada uno de los servidores en el primer grupo de servidores y el segundo grupo de servidores alojan las aplicaciones respectivas y admiten sesiones de usuario para las aplicaciones, y el método comprende además monitorizar las duraciones de las sesiones de usuario para las aplicaciones respectivas; y generar la información de cadencia gradual que indica las cadencias de reconstrucción para el primer grupo de servidores y el segundo grupo de servidores en base a las duraciones monitorizadas de las sesiones de usuario.

En una realización, los servidores en el primer grupo de servidores y el segundo grupo de servidores que se reconstruyen repetidamente son servidores físicos. En una realización, los servidores en el primer grupo de servidores y el segundo grupo de servidores que se reconstruyen repetidamente son máquinas virtuales.

En una realización, el sistema comprende además uno o más equilibradores de carga para equilibrar el tráfico de red entre el primer grupo de servidores y el segundo grupo de servidores. El método también comprende iniciar repetidamente el modo de preparación de apagado del primer grupo de servidores antes de cada reconstrucción del primer grupo de servidores, los equilibradores de carga evitan que se establezcan nuevas sesiones con aplicaciones del primer grupo de servidores mientras el primer grupo de servidores está en modo de preparación de apagado. El método también comprende iniciar repetidamente el modo de preparación de apagado del segundo grupo de servidores antes de cada reconstrucción del segundo grupo de servidores, los equilibradores de carga evitan que se establezcan nuevas sesiones con aplicaciones del segundo grupo de servidores mientras el segundo grupo de servidores está en modo de preparación de apagado.

Otras realizaciones incluyen un medio legible por ordenador no transitorio que almacena instrucciones. Las instrucciones son ejecutables por al menos un procesador para hacer que por lo menos un procesador realice el método de seguridad gradual. Otras realizaciones pueden aplicar seguridad gradual a los contenedores de software. Otras realizaciones pueden aplicar seguridad gradual a dispositivos informáticos en red dentro de un centro de datos, o dispositivos informáticos fuera de un centro de datos.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

La Figura (FIG.) 1A es un diagrama de bloques del sistema de comunicación en red con componentes de un centro de datos seguro para seguridad gradual, de acuerdo con una realización.

La FIG. 1B es un diagrama de bloques del sistema de comunicación en red con componentes de un centro de datos seguro para seguridad gradual, de acuerdo con otra realización.

La FIG. 1C es un diagrama de bloques del sistema de comunicación en red con componentes de un centro de datos seguro para seguridad gradual, de acuerdo con otra realización.

La FIG. 2A es un diagrama de bloques de un servidor frontend de la FIG. 1A, de acuerdo con una realización.

La FIG. 2B es un diagrama de bloques de un servidor con máquinas virtuales, de acuerdo con una realización.

La FIG. 2C es un diagrama de bloques de un servidor con contenedores de software, de acuerdo con una realización.

La FIG. 3 es un diagrama de grupos de servidores graduales, de acuerdo con una realización.

La FIG. 4 es un diagrama de bloques de un módulo de control de seguridad, de acuerdo con una realización.

La FIG. 5 es un diagrama de flujo para un método de seguridad gradual, de acuerdo con una realización.

La FIG. 6 ilustra la arquitectura de hardware de un dispositivo informático.

DESCRIPCIÓN DETALLADA

Se hará referencia ahora en detalle a varias realizaciones de la presente divulgación, ejemplos de las

cuales se ilustran en las figuras acompañantes. Se observa que, siempre que sea posible, pueden usarse números de referencia similares o parecidos en las figuras y pueden indicar una funcionalidad similar o parecida. Las figuras representan realizaciones de la presente divulgación solo con propósitos ilustrativos. Un experto en la técnica reconocerá fácilmente a partir de la siguiente descripción que pueden emplearse realizaciones alternativas de las estructuras y métodos ilustrados en la presente sin apartarse de los principios, o beneficios ofrecidos, de la divulgación descrita en la presente.

La presente divulgación se refiere a una plataforma de sistema que evita que los hackers obtengan acceso a conjuntos de datos de backend y evita el acceso continuo a cualquier conjunto de datos. Más particularmente, esta invención puede detener el acceso creciente a recursos no autorizados para una solución de mayor seguridad.

En una realización, se divulga una plataforma de seguridad para un centro de datos. La plataforma de seguridad se reconstruye de forma continua y repetida de una manera gradual en base a métricas de tiempo específicas. La seguridad gradual reemplazará automáticamente el software del servidor en cortos períodos de tiempo para eliminar por completo cualquier configuración o agujeros encontrados en los sistemas operativos o aplicaciones, limitando de este modo el acceso a cualquier servidor a un corto período de tiempo. Por ejemplo, este tiempo puede ser tan corto como 10 segundos o tan largo como horas. En una realización, una configuración estándar tendrá un valor predeterminado de 10 minutos entre reconstrucciones. Los hackers tendrán una ventana tan corta en la que aprenderán el pirateo, descubrirán cuál es la arquitectura en el backend, comprometerán el servidor e intentarán instalar un kit raíz para un acceso adicional. Por tanto, no tiene sentido que los hackers intenten completar su pirateo ya que el reemplazo del servidor ocurre con tanta frecuencia. Cuando un hacker descubre una contraseña o una clave de infraestructura de clave pública (PKI), el sistema operativo (SO) está siendo reemplazado junto con nuevas contraseñas y claves.

El sistema puede, pero no se limita a, reemplazar toda la pila de software en un dispositivo, incluyendo el sistema operativo, las aplicaciones, el contenido, los datos y la caché en un corto período de tiempo. El sistema puede integrarse completamente con múltiples dispositivos en una red (por ejemplo, equilibrador de carga, cortafuegos, etc.) para administrar ininterrumpidamente tanto usuarios reales como usuarios hackers. En otras realizaciones, el recuento de sesiones, el recuento de conexiones, los disparadores de sensores únicos y otras indicaciones de seguridad pueden usarse para desencadenar reconstrucciones. En otras realizaciones, una sesión puede estar contenida dinámicamente en un entorno aislado y un tiempo de la sesión puede extenderse para aprender los pirateos realizados en un entorno aislado.

El sistema puede aprender dinámicamente el tiempo y el contador de sesión medio de las aplicaciones y ajustar dinámicamente la cadencia de reconstrucción o tener una configuración manual para permitir políticas de seguridad más estrictas. El sistema limita el tiempo que cualquier sesión individual puede estar conectada a una aplicación frontend y un conjunto de datos para evitar el acceso remoto a largo plazo a cualquier sistema.

La FIG. 1A es un diagrama de bloques del sistema de comunicación en red con componentes de un centro de datos seguro para seguridad gradual, de acuerdo con una realización. El sistema incluye varios dispositivos cliente 105, una red 110, un rúter 115, cortafuegos frontales 120A-C, equilibradores de carga 125A-C, grupos de servidores frontend 130A-130D, cortafuegos de backend o equilibradores de carga 132A-C, grupos de servidores de backend 135A-135D, sistemas de almacenamiento 140A-140D y el servidor de seguridad 148. Los rúters, los cortafuegos 120, el equilibrador de carga 125, los servidores frontend 130, el cortafuegos 132, el servidor de backend 135 y los sistemas de almacenamiento 140 pueden ser componentes de un centro de datos. En la FIG. 1A solo se muestra un número limitado de dispositivos. 1A, pero en otras realizaciones puede haber un mayor número de dispositivos (por ejemplo, >cuatro grupos de servidores frontend).

Los dispositivos cliente 105 pueden ser dispositivos informáticos, como teléfonos inteligentes, tabletas, ordenadores portátiles y ordenadores de escritorio, entre otros. Un usuario interactúa con el software de los dispositivos cliente 105 a través de una interfaz, como una pantalla táctil o un ratón y teclado. Los dispositivos cliente 105 son controlados por el usuario para establecer sesiones de aplicación y conexiones con varias aplicaciones alojadas por los grupos de servidores frontend 130.

El rúter 115 enruta el tráfico de red entre la red 110 y el resto de los componentes en el centro de datos. Los cortafuegos de frontend 120 son dispositivos de cortafuegos basados en hardware que controlan el tráfico de red entrante y saliente usando un conjunto de reglas aplicado. Un cortafuegos establece una barrera entre la red interna del centro de datos y la red externa 110. Los equilibradores de carga 125 distribuyen el tráfico de red en una gran cantidad de grupos de servidores frontend 130. Los equilibradores de carga aumentan la capacidad y la fiabilidad de las aplicaciones disminuyendo la carga sobre cualquier grupo de servidores frontend particular 130.

Cada grupo de servidores frontend 130 incluye varios servidores frontend físicos. Un servidor es un dispositivo informático de clase servidor que puede incluir uno o más procesadores y ejecuta un sistema operativo. Un servidor aloja varias aplicaciones de software. Los clientes 105 pueden establecer conexiones de red y sesiones de aplicaciones con las aplicaciones alojadas por los servidores frontend. Por razones de seguridad, cada grupo de

servidores puede transferirse (es decir, mediante la reconstrucción del grupo de servidores) después de la expiración de una cantidad de tiempo y los grupos de servidores pueden graduarse de manera escalonada. Las copias de la misma aplicación están alojadas por múltiples grupos de servidores 130 de modo que, incluso cuando los grupos de servidores se transfieren, la aplicación todavía está disponible para los dispositivos de cliente 105. En una realización hay un total de nueve grupos de servidores frontend 130 y cada grupo de servidores frontend 130 incluye miles de servidores frontend.

Los cortafuegos de backend 132 son dispositivos de cortafuegos basados en hardware, o cortafuegos virtuales, que controlan el tráfico entre los grupos de servidores de frontend 130 y los grupos de servidores de backend 135 usando un conjunto de reglas aplicado. Cada grupo de servidores de backend 135 incluye uno o más servidores de backend. Los servidores de backend permiten el acceso a los datos almacenados en los sistemas de almacenamiento 140. Los servidores de backend almacenan y recuperan datos de los sistemas de almacenamiento 140 como sea solicitado por las aplicaciones alojadas en los grupos de servidores frontend 130. Un ejemplo de un servidor de backend es un servidor SQL que proporciona acceso a una base de datos SQL.

El servidor de seguridad 148 incluye un módulo de control de seguridad 150 que coordina el funcionamiento gradual de los grupos de servidores de frontend 130. Específicamente, el módulo de control de seguridad 150 inicia repetidamente reconstrucciones de los grupos de servidores de frontend 130 a intervalos periódicos y escalonados. La reconstrucción de un servidor puede incluir reemplazar la pila de software completa de un servidor, incluyendo el sistema operativo (SO), las aplicaciones, el contenido, los datos y las cachés, reemplazando una imagen del disco duro del servidor con una imagen de reemplazo buena y conocida. Reconstruir un servidor también puede incluir reemplazar el firmware de un servidor. La reconstrucción también puede incluir otras operaciones además de estas operaciones. El tiempo entre reconstrucciones puede ser tan corto como 10 segundos o tan largo como horas. En otras realizaciones, el tiempo de reconstrucción estándar será por defecto de 10 min.

La reconstrucción repetida de servidores de forma periódica y frecuente obliga a los hackers a completar su pirateo en un corto período de tiempo (por ejemplo, menos de 5 segundos), lo que es casi imposible ya que los tiempos de respuesta y los tiempos de carga requieren habitualmente una mayor cantidad de tiempo. Por ejemplo, para un servidor DNS, el servidor DNS puede reconstruirse cada 10 segundos con un nuevo sistema operativo y caché de base de datos DNS. En esta situación, los hackers no tendrán tiempo de piratear el protocolo y cargar datos falsos mediante falsificación de caché. Cualquier código malicioso cargado por los hackers también será eliminado. Todo lo relacionado con el servidor será reemplazado, lo que hace que sea imposible acceder al SO desde el exterior. Al mismo tiempo, todo el contenido necesario para las solicitudes estándar de los clientes se sirve correctamente. Esto resuelve completamente cualquier agujero encontrado en el software actual.

El módulo de control de seguridad 150 también inicia las reconstrucciones de forma gradual escalonando la reconstrucción de cada grupo de servidores frontend (por ejemplo, 130A) a tiempo con respecto a los otros grupos de servidores frontend (por ejemplo, 130B). Cada grupo de servidores frontend 130 comenzará a atender las sesiones de los usuarios en diferentes momentos, creando un enfoque de escalonamiento para cuando un grupo de servidores 130 se conecte y comience a atender el tráfico. El proceso desde el cual una sesión comienza y finaliza sucede todo dentro de un único servidor o grupo de servidores 130. Esto permite un equilibrio de carga simple dentro del grupo, pero también permite la finalización de una sesión dentro del grupo. Los servidores dentro de un grupo de servidores 130 reemplazarán su sistema operativo al mismo tiempo, mientras que otros grupos de servidores 130 se están conectando y prestando servicio a las nuevas sesiones de usuario. El marco temporal para reconstruir un grupo de servidores 130 puede variar dependiendo de la funcionalidad de las aplicaciones en los grupos de servidores 130.

El módulo de control de seguridad 150 también se comunica con los equilibradores de carga 125 de tal manera que los equilibradores de carga 125 son conscientes del grupo de servidores que se está apagando para las nuevas instalaciones del sistema operativo, permitiendo de este modo que los equilibradores de carga 125 distribuyan el tráfico de red solo a los grupos de servidores 130 que están en línea. El módulo de control de seguridad 150 puede transmitir información a los equilibradores de carga 125 para indicar cuándo un grupo de servidores 130 está comenzando a prepararse para apagarse. En respuesta, los equilibradores de carga 125 desconectan el grupo de servidores 130 y evitan que se establezcan nuevas conexiones con el grupo de servidores 130. Una vez que se reconstruye el grupo de servidores 130, el módulo de control de seguridad 150 puede transmitir información a los equilibradores de carga 125 indicando que el grupo de servidores 130 está listo para aceptar nuevas conexiones. En respuesta, los equilibradores de carga 125 vuelven a poner el grupo de servidores 130 en línea y permite que se establezcan nuevas conexiones con el grupo de servidores 130.

El módulo de control de seguridad 150 también puede cambiar la contraseña de los grupos de servidores 130 al reconstruir los grupos de servidores 130. Los cambios de contraseña frecuentes hacen que sea imposible realizar ataques de contraseña en los servidores.

El módulo de control de seguridad 150 puede implementarse como software, hardware o como una combinación de hardware y software. En otras realizaciones, el módulo de control de seguridad 150 puede

distribuirse a través de uno o más componentes del centro de datos que no sea el servidor de seguridad 148.

La FIG. 1B es un diagrama de bloques del sistema de comunicaciones en red con componentes de un centro de datos seguro para seguridad gradual, de acuerdo con otra realización. La FIG. 1B es parecida a la FIG. 1A excepto que ahora incluye grupos 160 de máquinas virtuales (VM) frontend e hipervisores 190. Cada grupo de VM 160 incluye una o más VM. Una VM es una emulación de un sistema informático, como una emulación de un servidor informático. Cada VM puede estar conectada a su propio disco virtual. En la presente puede hacerse referencia a una VM como un servidor virtual.

El hipervisor 190 crea y gestiona los grupos de máquinas virtuales 160. Cada hipervisor 190 puede estar localizado en su propio servidor frontend físico 159, y también controlar un grupo de VM 160 que están localizadas en el mismo servidor frontend físico. Por ejemplo, el hipervisor 190A y el grupo de VM 160A están localizados en un único servidor físico 159A.

En esta realización, el módulo de control de seguridad 150 proporciona seguridad gradual al sistema de comunicación en red iniciando periódicamente las reconstrucciones de los grupos de VM de frontend 160 (es decir, grupos de servidores virtuales). Las copias de la misma aplicación están alojadas en múltiples grupos de VM 160 para que la aplicación esté siempre en línea, incluso cuando los grupos de VM 160 se están reconstruyendo. La reconstrucción de una VM puede incluir restaurar el estado de una VM a un estado bueno conocido original. La reconstrucción se explicará con mayor detalle a continuación.

De otro modo, el funcionamiento del módulo de control de seguridad 150 es el mismo que el descrito junto con la FIG. 1A. En una realización, el sistema de comunicación en red puede incluir tanto grupos de servidores físicos como grupos de servidores virtuales que se reconstruyen de forma periódica y escalonada.

La FIG. 1C es un diagrama de bloques del sistema de comunicación en red con componentes de un centro de datos seguro para seguridad gradual, de acuerdo con otra realización. La FIG. 1C es parecido a la FIG. 1B excepto que ahora incluye grupos de contenedores 960 y motores de contenedores 990 localizados en los servidores 159.

Cada grupo de contenedores 960 incluye uno o más contenedores de software usados para la virtualización a nivel del sistema operativo. Un contenedor de software incluye una aplicación, sus dependencias, bibliotecas y binarios agrupados en un único paquete. Un contenedor de software comparte un sistema operativo (no mostrado) con otros contenedores de software en el mismo servidor 159. Un contenedor de software se instancia dentro del núcleo del sistema operativo y virtualiza la instancia de la aplicación. Los contenedores de software permiten la creación rápida de una aplicación o servicio para ponerlo en un bloque de recursos. La implementación de un contenedor es rápida porque los contenedores pueden compartir archivos de la biblioteca central del sistema operativo central. Los contenedores de software son gestionados por un motor de contenedores 990. En una realización, los contenedores de software 960 son contenedores DOCKER o cumplen con el estándar del proyecto de contenedores estándar.

En esta realización, el módulo de control de seguridad 150 proporciona seguridad gradual al sistema de comunicación en red iniciando periódicamente reconstrucciones de los grupos de contenedores 960 de manera gradual. Se incluyen copias de la misma aplicación en múltiples grupos de contenedores 960 de tal manera que la aplicación esté siempre en línea, incluso cuando se están reconstruyendo algunos de los grupos de contenedores 960. Un contenedor puede reconstruirse restaurando el contenedor a un buen estado conocido. La reconstrucción se explicará con mayor detalle a continuación.
De lo contrario, el funcionamiento del módulo de control de seguridad 150 es el mismo que el descrito junto con las FIG. 1A y 1B. En una realización, la reconstrucción de contenedores puede ser más eficiente que la reconstrucción de servidores físicos y máquinas virtuales. Por ejemplo, los contenedores pueden restaurarse y desplegarse en ~30 segundos. Por el contrario, la reconstrucción de servidores y máquinas virtuales puede llevar mucho más tiempo. Aunque los contenedores graduales pueden ser más fáciles que los servidores físicos y las máquinas virtuales graduales, tienen mayores riesgos debido al uso de archivos compartidos del sistema operativo central. Las arquitecturas de hipervisor también tienen riesgo, pero debido a que el SO está dedicado a cada VM, reduce el riesgo en comparación con una plataforma de contenedores. El riesgo es menor de nuevo cuando se gradúan servidores físicos, ya que un hacker necesitará tener un control de nivel de BIOS de un servidor para realizar el secuestro del servidor, o el hacker necesitará acceso a herramientas de administración remoto.

La descripción en la presente puede centrarse principalmente en el graduación de servidores físicos o máquinas virtuales. Sin embargo, los principios de seguridad gradual descritos en la presente son aplicables al graduación de servidores físicos, máquinas virtuales o contenedores.

La FIG. 2A es un diagrama de bloques de un servidor frontend 200, de acuerdo con una realización. El servidor frontend 200 puede representar un servidor frontend de los grupos de servidores frontend 130 de la FIG. 1A. El servidor frontend 200 incluye varias aplicaciones de software 250A-C, un OS 152, firmware 154 y un módulo de

seguridad frontend 156. Los ejemplos de SO 152 incluyen LINUX y MICROSOFT WINDOWS, entre otros. Las aplicaciones 250 se ejecutan sobre el SO 152. El firmware 154 incluye software que está almacenado en un chip de memoria programable.

Los dispositivos cliente 105 pueden establecer conexiones de red C1-C6 con las aplicaciones 250. Una conexión se usa como un canal de comunicación bidireccional entre las conexiones en los dispositivos cliente 105 y el servidor 200. La conexión se establece en un momento determinado usando un proceso de protocolo de intercambio, y luego se termina en un momento posterior en el tiempo. La conexión puede incluir varios estados definidos por un protocolo. Un ejemplo de conexión es una conexión de protocolo de control de transmisión (TCP) de la capa de transporte del modelo de interconexión de sistemas abiertos (OSI).

Los dispositivos cliente 105 también establecen sesiones de usuario de aplicación S1-S6 con las aplicaciones 250 a través de las conexiones C1-C6. Una sesión de usuario es un intercambio de información interactivo entre dos o más entidades comunicantes para una aplicación determinada. La sesión del usuario se establece en un momento determinado y luego se termina en un momento posterior. Durante la sesión del usuario, pueden enviarse uno o más mensajes en cada dirección a través de una conexión que se ha establecido para la sesión. En una realización, las sesiones de aplicación son sesiones de la capa de sesión OSI que se encuentran por encima de la capa de transporte.

En un ejemplo, puede iniciarse una sesión de autenticación de tarjeta de crédito (por ejemplo, S1, S2) cuando un usuario desliza una tarjeta de crédito en un dispositivo cliente 105A, y el dispositivo cliente 105A establece una conexión y sesión con la aplicación de pago con tarjeta de crédito 250A. La aplicación de pago con tarjeta de crédito 250A se comunica con el dispositivo cliente 105A para obtener el número de tarjeta de crédito y el importe del cargo del dispositivo cliente 105A. La aplicación de pago con tarjeta de crédito 250 accede luego a la base de datos 140 a través del servidor de backend 135 para determinar si el número de tarjeta de crédito tiene crédito suficiente para procesar el pago. La aplicación de pago con tarjeta de crédito 250 proporciona luego una respuesta sí/no al dispositivo cliente 105A. La conexión y la sesión se terminan después de proporcionar la respuesta al dispositivo cliente 105A.

En otro ejemplo, puede iniciarse una sesión de formulario web (por ejemplo, S3, S4) cuando un usuario introduce una URL en un navegador en un cliente 105B. El dispositivo cliente 105B establece una sesión con el sitio web 250B. El servidor 200 puede estar procesando múltiples sesiones. El servidor 200 inicia un contador de tiempo por sesión. El usuario tiene x cantidad de tiempo para completar un formulario antes de que se cierre la sesión. Un servidor diferente puede procesar el envío del formulario desde la sesión inicial debido al tiempo que lleva completar los datos del formulario web.

En un ejemplo adicional, se puede iniciar una sesión de banca en línea (por ejemplo, S5, S6) cuando un usuario abre una aplicación de banca móvil en el dispositivo cliente 105B, y el dispositivo cliente 105B establece una conexión y sesión con la aplicación de banca en línea 250C. La aplicación de banca en línea 250C se comunica con el dispositivo cliente 105B para obtener información de autenticación del dispositivo cliente 105B. Una vez autenticado, el dispositivo cliente 105B puede solicitar saldos de cuenta, cargar copias de cheques para depósito y hacer otras solicitudes bancarias. La aplicación bancaria 250C puede acceder a la información de la cuenta almacenada en la base de datos 140 a través del servidor de backend 135 para procesar estas solicitudes. La conexión y la sesión terminan finalmente al final de la sesión.

El módulo de seguridad de frontend 156 puede comunicarse con el módulo de control de seguridad 150 para enviar y recibir información de seguridad para implementar la seguridad gradual. El módulo de seguridad 156 puede recibir comandos para iniciar una reconstrucción del servidor frontend 200. Los comandos pueden incluir el nombre de una imagen preferida, que es una imagen de software maestro buena conocida que se usará como plantilla para la reconstrucción. El módulo de seguridad 156 reconstruye luego el servidor frontend 200 de acuerdo con los comandos, como reemplazando el OS 152, las aplicaciones y/o el firmware 154. El OS 152, las aplicaciones 250 y/o el firmware 154 pueden reemplazarse sobrescribiendo el software existente en el servidor 200 con la imagen preferida, eliminando el software existente en el servidor 200 y copiando el nuevo software en el servidor 200 desde la imagen preferida, etc. La imagen preferida puede almacenarse localmente en un disco dentro del servidor 200 o en otro lugar en una red.

Pueden usarse diferentes técnicas de reconstrucción con tiempos de reconstrucción variables. En una realización, puede usarse una sola imagen preferida para reconstruir múltiples servidores 200. Los datos de la imagen preferida pueden copiarse en el servidor frontend 200, y luego las configuraciones posteriores al proceso se ejecutan en cada servidor frontend 200 para configurar el SO 152 o las aplicaciones 250. Por ejemplo, puede ejecutarse un script diferente en cada servidor frontend 200 para establecer un nombre único para el servidor y una dirección IP para el servidor. En una realización, puede haber múltiples imágenes preferidas que son específicas y únicas para cada servidor frontend 200. Los datos de una imagen preferida pueden copiarse en un servidor respectivo sin la necesidad de configuraciones posteriores al proceso, lo que reduce el tiempo de reconstrucción.

En otra realización, se usa una técnica de diferenciación de datos para reconstruir el servidor frontend 200. Específicamente, los bloques de datos o archivos del software de un servidor frontend 200 pueden compararse con bloques de datos o archivos de una imagen preferida. Solo los bloques de datos o archivos que son diferentes se restauran de la imagen preferida. Al aprovechar la diferenciación basada en bloques o archivos, es posible la implementación rápida de configuraciones preconfiguradas del SO y aplicaciones a través de un disco local, discos SAN remotos o discos NAS. Cabe señalar que otras técnicas de reconstrucción pueden ser posibles y estar aún dentro del alcance de la divulgación.

En una realización, pueden aplicarse varios modelos de cifrado o hash o comparaciones de estado de bloque a una imagen de software reconstruida para verificar que la reconstrucción tenga la configuración estándar esperada y el estado tenga una buena configuración conocida. Por ejemplo, el software reconstruido puede cifrarse y luego compararse con el hash de la imagen preferida para verificar que la reconstrucción se realizó como se esperaba.

En una realización, el módulo de seguridad frontend 156 coloca un servidor frontend 200 en un modo de seguridad de bloqueo durante las reconstrucciones para protección contra la manipulación. Durante las reconstrucciones, el módulo de seguridad frontend 156 puede establecer sus listas de control de acceso de cortafuegos interno (ACL) con permisos que bloquean cualquier tráfico a ciertos puertos que no sean las comunicaciones con el módulo de control de seguridad 150 del servidor de seguridad 148. Una ACL puede ser una lista de puertos de red, junto con entidades específicas autorizadas para usar los puertos de red. Otra aplicaciones de terceros también pueden tener acceso en base a una necesidad para la verificación del estado de cumplimiento.

El módulo de seguridad 156 también puede recibir un comando para cambiar la contraseña del SO 152 y luego reemplazar la contraseña de acuerdo con el comando. En una realización, la información de seguridad se comunica a través de una interfaz de gestión de plataforma inteligente (IPMI).

La FIG. 2B es un diagrama de bloques de un servidor frontend 202 con máquinas virtuales 204, de acuerdo con una realización. El servidor frontend 202 puede representar un servidor frontend 159 de la FIG. 1B. El servidor frontend 202 incluye varias VM 204, hipervisor 208, SO 152 y el módulo de seguridad frontend 156A. Cada VM incluye un SO virtualizado 206 y aplicaciones 250.

El módulo de seguridad frontend 156A es similar al módulo frontend 156, pero ahora reconstruye las VM en respuesta a los comandos para reconstruir las VM 204. La reconstrucción de las VM 204 es similar a la reconstrucción descrita con respecto a la FIG. 2A, y también puede utilizar una imagen preferida de una VM 204 para generar una VM 204, utilizar la diferenciación de datos y/o realizar una verificación de reconstrucción después de reconstruir la VM 204.

La FIG. 2C es un diagrama de bloques de un servidor frontend 290 con contenedores 292, de acuerdo con una realización. El servidor frontend 290 puede representar un servidor frontend 159 de la FIG. 1C. El servidor frontend 290 incluye varios contenedores 292, motor de contenedor 294, SO 152 y módulo de seguridad frontend 156B. Cada contenedor incluye aplicaciones virtualizadas 250.

El módulo de seguridad frontend 156B es similar al módulo frontend 156, pero ahora reconstruye los contenedores 292 en una base gradual en respuesta a los comandos para reconstruir los contenedores 292. La reconstrucción de los contenedores 292 es similar a la reconstrucción descrita con respecto a la FIG. 2A, y también puede utilizar una imagen preferida de un contenedor 292 para generar un contenedor 292, utilizar la diferenciación de datos y/o realizar una verificación de reconstrucción después de reconstruir el contenedor 292.

La FIG. 3 es un diagrama de grupos de servidores graduales, de acuerdo con una realización. La operación gradual de cuatro grupos de servidores 130A-130D se ilustra en la FIG. 3. En otras realizaciones, la operación gradual mostrada en la FIG. 3 también es aplicable para la graduación de los grupos de máquinas virtuales 160 y los grupos de contenedores de software 960.

Cada grupo de servidores 130 opera en diferentes modos de seguridad gradual: (1) un modo de operación normal (2) un modo de preparación de apagado y (3) un modo de reconstrucción. Durante el modo de funcionamiento normal, un grupo de servidores 130 acepta y da servicio a nuevas sesiones de usuario y conexiones. Durante el modo de preparación de apagado, el grupo de servidores 130 no acepta nuevas sesiones y conexiones. Se permite que las sesiones y conexiones existentes finalicen. En una realización, los equilibradores de carga 125 pueden ser notificados de que un grupo de servidores particular 130 se está poniendo en modo de preparación de apagado y no está aceptando nuevas sesiones y conexiones. Los equilibradores de carga 125 responden eliminando el grupo de servidores 130 de los posibles grupos de servidores 130 en los que pueden realizarse nuevas sesiones y conexiones. Durante el modo de reconstrucción el grupo de servidores 130 se elimina del servicio y se reconstruye reemplazando el software del grupo de servidores 130. Los modos se repiten periódicamente, como cada 60 segundos.

Los grupos de servidores 130 se operan de manera gradual, de tal manera que la reconstrucción de diferentes grupos de servidores se inicia en diferentes momentos. Por ejemplo, el grupo de servidores 130A se reconstruye a las 1:00:50, el grupo de servidores 130B se reconstruye a las 1:01:00, el grupo de servidores 130C se reconstruye a las 1:01:10 y el grupo de servidores 130D se reconstruye a las 1:01:20. Los tiempos de reconstrucción se escalonan entre sí durante diez segundos. El escalonamiento de los tiempos de reconstrucción asegura que siempre haya por lo menos un grupo de servidores 130 en servicio y disponible para aceptar nuevas conexiones y sesiones de usuario para aplicaciones alojadas por el grupo de servidores 130. En otras palabras, siempre hay por lo menos un grupo de servidores 130 que está en modo de funcionamiento normal.

En una realización, el modo de preparación de apagado puede retrasarse para un grupo de servidores 130 si se activa una condición de seguridad que indica la presencia de un hacker. Puede desencadenarse una condición de seguridad, por ejemplo, si la sesión está asociada con una IP sospechosa o ha mantenido la sesión abierta durante demasiado tiempo. En esa situación, el módulo de control de seguridad 150 puede implementar análisis profundos de la sesión, contención de la sesión y registro de la sesión para comprender mejor las acciones de un hacker. Alternativamente, si se activa una condición de seguridad, el módulo de seguridad 150 puede tomar un servidor pirateado, en el que se detecta la sesión pirateada, fuera del grupo de servidores 130. Un nuevo servidor se intercambia en caliente en lugar del servidor pirateado de tal manera que no se interrumpe la graduación de los grupos de servidores 130.

La FIG. 4 es un diagrama de bloques de un módulo de control de seguridad 130, de acuerdo con una realización. El módulo de control de seguridad 130 incluye un módulo de comunicación 405, un módulo de cadencia gradual 410, un módulo de control gradual 415 y un módulo de cambio de contraseña 420. En otras realizaciones, el módulo de control de seguridad 130 puede tener módulos adicionales no mostrados en la FIG. 4.

El módulo de cadencia gradual 410 mantiene información de la cadencia gradual que indica las cadencias escalonadas para cuando los grupos de servidores físicos 130, los grupos de VM 160 o los grupos de contenedores 960 (referidos colectivamente en la presente como "grupos de entidades graduales") deben introducir modos diferentes, como el modo de funcionamiento normal, modo de preparación de apagado y modo de reconstrucción. La información de cadencia puede tener la forma de un programa de cadencia que incluye una lista de grupos de entidades graduales y tiempos específicos para cuando cada grupo de entidades graduales debe introducir modos diferentes. La siguiente tabla es un ejemplo de un programa de cadencia.

Grupo de Servidores	Modo: Funcionamiento Normal	Modo: Preparación de Apagado	Modo: Reconstrucción
1	1:00:00 1:01:00 ...	1:00:30 1:01:30 ...	1:00:50 1:01:50 ...
2	1:00:10 1:01:10 ...	1:00:40 1:01:40 ...	1:01:00 1:02:00 ...
3	1:00:20 1:01:20 ..	1:00:50 1:01:50 ...	1:01:10 1:02:10 ...
4	1:00:30 1:01:30 ...	1:01:00 1:02:00 ...	1:01:20 1:02:20 ...

La primera columna de la tabla identifica un grupo de servidores. La segunda columna identifica las horas de inicio para cuando el grupo de servidores debe introducir el modo de funcionamiento normal. La tercera columna identifica cuándo el grupo de servidores debe introducir el modo de preparación de apagado. La cuarta columna identifica cuándo debe comenzar el proceso de reconstrucción.

En otras realizaciones, la información de cadencia puede estar en forma de límites de tiempo máximos en lugar de un programa de cadencia. Por ejemplo, la información de cadencia puede incluir un tiempo de actividad máximo de un grupo de entidades graduales, una duración máxima de un modo de funcionamiento normal, una duración máxima de un modo de preparación de apagado y/o una duración máxima de un modo de reconstrucción. La información de cadencia también puede incluir información que describe una cantidad de retraso de escalonamiento entre los grupos de entidades graduales.

La información de cadencia gradual para los modos graduales puede ser configurada manualmente por un usuario. En otra realización, la información de cadencia puede aprenderse de forma automática monitorizando las duraciones de sesiones o conexiones de aplicaciones anteriores en los servidores y la generación de perfiles de aplicaciones que incluyen las duraciones monitorizadas. Puede determinarse una medida estadística de las duraciones (por ejemplo, duración media, duración máxima) a partir de las duraciones monitorizadas. La medida estadística se multiplica luego por un multiplicador (por ejemplo, 8x, 10x) para determinar la duración máxima de cada modo gradual. El resultado es que el tiempo entre reconstrucciones es suficiente para que se establezcan y completen nuevas sesiones de usuario y conexiones antes de que se reconstruya un grupo de entidades graduales. Por ejemplo, si las sesiones de usuario tienden a durar 6 segundos, este valor puede multiplicarse por 8x para dar como resultado una duración entre reconstrucciones periódicas de 48 segundos, que es mucho mayor que la duración de la sesión.

El módulo de control gradual 415 controla la operación de gradual de los grupos de entidades graduales de acuerdo con la información de cadencia gradual, como el programa de cadencia de gradual o los límites de tiempo máximos descritos anteriormente. El módulo de control gradual 415 usa la información de cadencia gradual para determinar el modo gradual en el que debe estar un grupo de servidores. El módulo de control gradual 415 envía luego comandos de control a los equilibradores de carga 125 y grupos de entidades graduales a través del módulo de comunicación 405 que hacen que los grupos de entidades graduales funcionen de una manera gradual como se muestra en la FIG. 3. Los comandos para cada grupo de entidades graduales pueden escalonarse en el tiempo con respecto a los comandos para los otros grupos de entidades graduales para garantizar que los grupos de entidades graduales se gradúen en tiempos controlados y escalonados.

Para iniciar el modo de funcionamiento normal, el módulo de control gradual 415 puede transmitir un comando de inicio de funcionamiento normal a los equilibradores de carga 125. El comando identifica un grupo de entidades graduales particular y también indica que el modo de funcionamiento normal debe comenzar para ese grupo de entidades graduales. El equilibrador de carga 125 responde al comando permitiendo que se establezcan sesiones y conexiones con el grupo de entidades graduales identificado. En una realización, el comando de inicio de funcionamiento normal también puede transmitirse al grupo de entidades graduales apropiado para el que se está iniciando el funcionamiento normal.

Para iniciar el modo de preparación de apagado, el módulo de control gradual 415 puede transmitir un comando de inicio de preparación de apagado a los equilibradores de carga 125. El comando identifica un grupo de entidades graduales particular y también indica que el modo de preparación de apagado debe comenzar para ese grupo de entidades graduales. El equilibrador de carga 125 responde al comando evitando que se establezcan nuevas sesiones y conexiones con el grupo de entidades graduales identificado. Se permite que las sesiones y conexiones existentes del grupo de entidades graduales se completen. En una realización, el comando de inicio de preparación de apagado también puede transmitirse a los servidores apropiados para un grupo de entidades graduales.

Para iniciar la reconstrucción, el módulo de control gradual 415 puede enviar un comando de inicio de reconstrucción a los servidores frontend apropiados asociados con un grupo de entidades graduales que se va a reconstruir. El comando puede incluir un nombre de una imagen de software buena conocida que se usará para la reconstrucción. En respuesta, el grupo de entidades graduales puede reconstruirse con la imagen de software buena conocida. El módulo de control gradual 415 también puede recibir información de confirmación de reconstrucción de los servidores frontend apropiados una vez que se ha completado la reconstrucción.

Además, antes de la reconstrucción, el módulo de control gradual 415 puede copiar datos de un grupo de entidades graduales a una unidad de almacenamiento separada. Puede usarse aprendizaje automático para monitorizar los cambios en los datos y hacer un análisis en línea de los cambios para la comparación global con otros servidores. Esto permite comprender todos los cambios realizados por un hacker en el SO, las aplicaciones o los archivos mientras una entidad estaba en línea. El aprendizaje automático del estado y la cadencia de reconstrucción es importante, pero retrasar el estado de reconstrucción en una situación de pirateo para permitir un aprendizaje más avanzado también es parte de los controles del sistema administrados a través del módulo de control gradual 415. El módulo de control gradual 415 también puede comunicarse con los grupos de servidores locales, el rúter 115 y el cortafuegos 120 para continuar dando servicio a un hacker con la intención de aprender y recopilar más datos para aprender las capacidades de los hackers y aprender más sobre nuevos ataques.

El módulo de cambio de contraseña 420 inicia cambios de contraseña para los grupos de servidores 130. Las contraseñas pueden ser contraseñas de SO, base de datos o aplicación, entre otras. Las contraseñas pueden cambiarse con cada reconstrucción, como lo indica la información de cadencia gradual, o pueden reconstruirse en marcas temporales específicas (es decir, en ciertos intervalos). La frecuencia de los cambios de contraseña puede ser igual o diferente a la frecuencia de las reconstrucciones del grupo de entidades graduales. En una realización, el módulo de cambio de contraseña 420 puede iniciar un cambio de contraseña generando nuevas contraseñas y transmitiendo las contraseñas a los servidores. En otra realización, el módulo de cambio de contraseña 420 puede iniciar un cambio de contraseña enviando un comando de cambio de contraseña a los servidores. Los servidores

generan nuevas contraseñas en respuesta al comando. Puede usarse cualquiera de una serie de algoritmos para generar la contraseña. En una realización, una marca temporal es uno de los elementos usados para generar la contraseña.

El módulo de comunicación 405 se comunica con los servidores, los equilibradores de carga 125 y otros dispositivos en el sistema de comunicación en red. El módulo de comunicación 405 puede transmitir comandos de seguridad graduales que hacen que los grupos de entidades graduales funcionen de manera gradual y escalonada. El módulo de comunicación 405 puede enviar comandos que inician cambios de contraseña en los grupos de entidades graduales. El módulo de comunicación 405 también puede recibir otros tipos de información de los dispositivos en el sistema de comunicación en red.

La FIG. 5 es un diagrama de flujo para un método de seguridad gradual, de acuerdo con una realización. En el paso 505, se supervisan las conexiones o sesiones de usuario anteriores para aplicaciones alojadas por los grupos de entidades graduales. Las duraciones se almacenan en los perfiles de la aplicación. Una vez que se recopila suficiente información, las duraciones de las conexiones y las sesiones de usuario anteriores se usan para generar información de cadencia gradual que describe las cadencias escalonadas para diferentes modos de seguridad gradual de los grupos de entidades graduales, como la cadencia escalonada para cuando se deben reconstruir diferentes grupos de entidades graduales.

En el paso 510, el módulo de control de seguridad 150 inicia el funcionamiento normal del primer grupo de entidades graduales en un momento especificado por la información de cadencias graduales. En el paso 512, el módulo de control de seguridad 150 inicia el modo de preparación de apagado del grupo de entidades graduales a una cadencia especificada por la información de cadencias graduales. En el paso 514, el módulo de control de seguridad 150 inicia la reconstrucción del primer grupo de entidades graduales a una candencia especificada por la información de cadencias graduales. Además, el módulo de control de seguridad 150 inicia un cambio de contraseña del primer grupo de entidades graduales al mismo tiempo. Los pasos 510-514 se repiten continuamente, como a intervalos periódicos.

En el paso 520, el módulo de control de seguridad 150 inicia el funcionamiento normal del segundo grupo de entidades graduales a una cadencia especificada por la información de cadencias graduales. En el paso 522, el módulo de control de seguridad 150 inicia el modo de preparación de apagado del segundo grupo de entidades graduales a una cadencia especificada por la información de cadencias graduales. En el paso 524, el módulo de control de seguridad 150 inicia la reconstrucción del segundo grupo de entidades graduales a una cadencia especificada por la información de cadencias graduales. Además, el módulo de control de seguridad 150 inicia un cambio de contraseña del primer grupo de entidades graduales al mismo tiempo. Los pasos 520-524 se repiten continuamente, como a intervalos periódicos.

Otros grupos de entidades graduales también pueden controlarse de manera similar a los pasos 510-514 y 520-524. Además, para cada grupo de entidades graduales, el inicio de la reconstrucción, los modos de funcionamiento normal y los modos de preparación de cierre se escalonan en el tiempo con respecto a otros grupos de entidades graduales. El escalonamiento de los modos de seguridad da como resultado la seguridad gradual ilustrada en la FIG. 3.

La FIG. 6 ilustra la arquitectura de hardware de un dispositivo informático, como un cortafuegos 120, un rúter 115, un equilibrador de carga 125, un dispositivo cliente 105, un servidor de frontend 130 o 159, un servidor de backend 135 o un servidor de seguridad 148, de acuerdo con una realización. En una realización, el dispositivo informático es un ordenador que incluye componentes como un procesador 602, una memoria 603, un módulo de almacenamiento 604, un módulo de entrada (por ejemplo, teclado, ratón y similares) 606, un módulo de visualización 607 y una interfaz de comunicación 605, intercambiando datos y señales de control entre sí a través de un bus 601. El módulo de almacenamiento 604 se implementa como uno o más medios de almacenamiento legibles por ordenador no transitorios (por ejemplo, disco duro o unidad de estado sólido), y almacena las instrucciones de software 640 (por ejemplo módulos) que son ejecutados por el procesador 602 junto con la memoria 603 para implementar las características de seguridad graduales descritas en la presente. El software del sistema operativo y otro software de aplicación también pueden almacenarse en el módulo de almacenamiento 604 para ejecutarse en el procesador 602.

La seguridad gradual descrita en el presente no solo se limita a los servidores de frontend 130, las máquinas virtuales 160 y los contenedores 960. En otras realizaciones, la seguridad gradual puede usarse para reconstruir periódicamente otros grupos de sistemas informáticos en un centro de datos, como cortafuegos 120, equilibradores de carga 125, conmutadores, servidores de backend 135 y almacenamiento de backend 140. Además, las funciones de los módulos descritos en la presente pueden combinarse en un solo módulo o distribuirse a través de módulos adicionales.

En otras realizaciones, la seguridad gradual descrita en la presente puede aplicarse a otros grupos de sistemas informáticos fuera de los centros de datos que proporcionan una funcionalidad de software común. Los

sistemas informáticos pueden ser ordenadores de escritorio, portátiles, ipads, iphones y sistemas informáticos en vehículos (automóviles, trenes, aviones) y sistemas informáticos en centrales eléctricas, generadores, etc. En el ejemplo de un avión, el avión puede incluir varios sistemas de control de vuelo paralelos, cada uno de los cuales puede proporcionar control de vuelo para el avión. Graduar los sistemas de control de vuelo de manera escalonada puede proteger del pirateo a los sistemas de control de vuelo, a la vez que garantiza que por lo menos un sistema de control de vuelo esté siempre en línea.

Tras leer esta divulgación, los expertos en la técnica pueden apreciar más diseños alternativos adicionales para la seguridad gradual. Por tanto, aunque se han ilustrado y descrito realizaciones y aplicaciones particulares de la presente divulgación, debe entenderse que la divulgación no se limita a la construcción precisa y los componentes precisos divulgados en la presente. Pueden hacerse varias modificaciones, cambios y variaciones que pueden ser evidentes para los expertos en la técnica en la disposición, funcionamiento y detalles del método y aparato de la presente divulgación en la presente sin apartarse del alcance de la divulgación tal como se define en las reivindicaciones adjuntas.

REIVINDICACIONES

1. Un medio legible por ordenador no transitorio que almacena instrucciones para implementar seguridad gradual para un sistema que incluye un primer grupo de servidores y un segundo grupo de servidores, cada servidor en el primer grupo de servidores y segundo grupo de servidores incluyendo software que incluye un sistema operativo y una aplicación que admite sesiones de usuario, las instrucciones cuando son ejecutadas por al menos un procesador hacen que el por lo menos un procesador:

acceda a la información de cadencia gradual generada en base a las duraciones monitorizadas de las sesiones de usuario anteriores establecidas entre la aplicación y los dispositivos del cliente, la información de cadencia gradual indicando las primeras cadencias de reconstrucción para reconstruir el primer grupo de servidores y las segundas cadencias de reconstrucción para reconstruir el segundo grupo de servidores, las primeras cadencias de reconstrucción escalonadas en el tiempo desde las segundas cadencias de reconstrucción;
iniciar repetidamente la reconstrucción del primer grupo de servidores de los servidores de acuerdo con las primeras cadencias de reconstrucción; y
iniciar repetidamente la reconstrucción del segundo grupo de servidores de los servidores de acuerdo con las segundas cadencias de reconstrucción, la reconstrucción del primer grupo de servidores estando escalonadas en el tiempo desde la reconstrucción del segundo grupo de servidores de los servidores.

2. El medio legible por ordenador de la reivindicación 1, en el que los servidores en el primer grupo de servidores y el segundo grupo de servidores que se reconstruyen repetidamente son servidores físicos o máquinas virtuales.

3. El medio legible por ordenador de la reivindicación 1, en el que el sistema comprende además uno o más equilibradores de carga para equilibrar el tráfico de red entre el primer grupo de servidores y el segundo grupo de servidores, y las instrucciones cuando son ejecutadas por el por lo menos un procesador hacen que el por lo menos un procesador:

inicie repetidamente el modo de preparación de apagado del primer grupo de servidores antes de cada reconstrucción del primer grupo de servidores, los equilibradores de carga evitan que se establezcan nuevas sesiones con aplicaciones del primer grupo de servidores mientras el primer grupo de servidores está en modo de preparación de apagado; y
inicie repetidamente el modo de preparación de apagado del segundo grupo de servidores antes de cada reconstrucción del segundo grupo de servidores, los equilibradores de carga evitan que se establezcan nuevas sesiones con aplicaciones del segundo grupo de servidores mientras el segundo grupo de servidores está en modo de preparación de apagado.

4. El medio legible por ordenador de la reivindicación 1, en el que
la reconstrucción que se inicia repetidamente del primer grupo de servidores comprende iniciar periódicamente la reconstrucción del primer grupo de servidores; y
la reconstrucción que se inicia repetidamente del segundo grupo de servidores comprende iniciar periódicamente la reconstrucción del segundo grupo de servidores.

5. Un método implementado por ordenador de seguridad gradual para un sistema que incluye un primer grupo de servidores y un segundo grupo de servidores, cada servidor en el primer grupo de servidores y el segundo grupo de servidores, incluyendo software que incluye un sistema operativo y una aplicación que admite sesiones de usuario, el método comprendiendo:

acceder a la información de cadencia gradual generada en base a las duraciones monitorizadas de las sesiones de usuario anteriores establecidas entre la aplicación y los dispositivos del cliente, la información de cadencia gradual indicando las primeras cadencias de reconstrucción para reconstruir el primer grupo de servidores y las segundas cadencias de reconstrucción para reconstruir el segundo grupo de servidores, las primeras cadencias de reconstrucción escalonadas en el tiempo de las segundas cadencias de reconstrucción
iniciar repetidamente la reconstrucción del primer grupo de servidores de los servidores de acuerdo con las primeras cadencias de reconstrucción; y
iniciar repetidamente la reconstrucción del segundo grupo de servidores de los servidores de acuerdo con las segundas cadencias de reconstrucción, la reconstrucción del primer grupo de servidores estando escalonada en el tiempo desde la reconstrucción del segundo grupo de servidores.

6. El medio legible por ordenador de la reivindicación 1 o el método de la reivindicación 5, en el que:

la reconstrucción que se inicia repetidamente del primer grupo de servidores comprende iniciar la reconstrucción de software de cada servidor del primer grupo de servidores; y

la reconstrucción que se inicia repetidamente del segundo grupo de servidores comprende iniciar el software de reconstrucción de cada servidor del segundo grupo de servidores.

7. El medio legible por ordenador de la reivindicación 1 o el método de la reivindicación 5, en el que:

la reconstrucción que se inicia repetidamente del primer grupo de servidores comprende iniciar una reconstrucción de firmware en cada servidor del primer grupo de servidores; y
la reconstrucción que se inicia repetidamente del segundo grupo de servidores comprende iniciar una reconstrucción de firmware en cada servidor del segundo grupo de servidores.

8. El método de la reivindicación 5, que comprende además:

iniciar repetidamente un cambio de contraseña de cada servidor en el primer grupo de servidores cuando se reconstruye el primer grupo de servidores; y
iniciar repetidamente un cambio de contraseña de cada servidor en el segundo grupo de servidores cuando se reconstruye el segundo grupo de servidores.

9.. El medio legible por ordenador de la reivindicación 1 o el método de la reivindicación 6 que comprende además:

monitorizar las duraciones de las sesiones de usuario; y
generar la información de cadencia gradual que indica las cadencias de reconstrucción para el primer grupo de servidores y el segundo grupo de servidores en base a las duraciones monitorizadas de las sesiones de usuario.

10. Un medio legible por ordenador no transitorio que almacena instrucciones para implementar la seguridad gradual de un sistema que incluye un primer grupo de contenedores de software y un segundo grupo de contenedores de software, cada contenedor de software en el primer grupo de contenedores de software y el segundo grupo de contenedores de software incluyendo software que incluye una aplicación que admite sesiones de usuario, las instrucciones cuando son ejecutadas por el al menos un procesador hacen que el por lo menos un procesador:

acceda a la información de cadencia gradual generada en base a las duraciones monitorizadas de las sesiones de usuario anteriores establecidas entre la aplicación y los dispositivos cliente, la información de cadencia gradual indicando las primeras cadencias de reconstrucción para reconstruir el primer grupo de contenedores de software y las segundas cadencias de reconstrucción para reconstruir el segundo grupo de contenedores de software, las primeras cadencias de reconstrucción escalonadas en el tiempo a partir de las segundas cadencias de reconstrucción;
iniciar repetidamente la reconstrucción del primer grupo de contenedores de software de acuerdo con las primeras cadencias de reconstrucción; y
iniciar repetidamente la reconstrucción del segundo grupo de contenedores de software de acuerdo con las segundas cadencias de reconstrucción, la reconstrucción del primer grupo de contenedores de software estando escalonada en el tiempo a partir de la reconstrucción del segundo grupo de contenedores de software.

11. Un método para implementar la seguridad gradual de un sistema que incluye un primer grupo de contenedores de software y un segundo grupo de contenedores de software, cada contenedor de software en el primer grupo de contenedores de software y el segundo grupo de contenedores de software, incluyendo software que incluye una aplicación que admite sesiones de usuario, el método comprendiendo:

accediendo a la información de cadencia gradual generada en base a las duraciones monitorizadas de las sesiones de usuario anteriores establecidas entre la aplicación y los dispositivos del cliente, la información de cadencia gradual que indica los primeras cadencias de reconstrucción para reconstruir el primer grupo de contenedores de software y las segundas cadencias de reconstrucción para reconstruir el segundo grupo de contenedores de software, las primeras cadencias de reconstrucción escalonadas en el tiempo a partir de las segundas cadencias de reconstrucción;
iniciar repetidamente la reconstrucción del primer grupo de contenedores de software de acuerdo con las primeras cadencias de reconstrucción; y
iniciar repetidamente la reconstrucción del segundo grupo de contenedores de software de acuerdo con las segundas cadencias de reconstrucción, la reconstrucción del primer grupo de contenedores de software estando escalonada en el tiempo a partir de la reconstrucción del segundo grupo de contenedores de software.

12. Un sistema para seguridad gradual, que comprende:

un primer grupo de servidores de los servidores;
un segundo grupo de servidores de los servidores, cada servidor en el primer grupo de servidores y el

segundo grupo de servidores, incluyendo software que incluye un sistema operativo y una aplicación que admite sesiones de usuario; y
un medio legible por ordenador no transitorio que almacena instrucciones, las instrucciones cuando son ejecutadas por el al menos un procesador hacen que el por lo menos un procesador:

acceda a la información de cadencia gradual generada en base a las duraciones monitorizadas de las sesiones de usuario anteriores establecidas entre la aplicación y los dispositivos del cliente que indican las primeras cadencias de reconstrucción para el primer grupo de servidores y las segundas cadencias de reconstrucción para el segundo grupo de servidores, las primeras cadencias de reconstrucción estando escalonadas en el tiempo a partir de las segundas cadencias de reconstrucción;
inicie repetidamente la reconstrucción del software de cada servidor del primer grupo de servidores de los servidores de acuerdo con las primeras cadencias de reconstrucción; y
inicie repetidamente la reconstrucción del software de cada servidor en el segundo grupo de servidores de los servidores de acuerdo con las segundas cadencias de reconstrucción, la reconstrucción del primer grupo de servidores estando escalonada a partir de la reconstrucción del segundo grupo de servidores.

13. El sistema de la reivindicación 12, en el que las instrucciones hacen además que el por lo menos un procesador:

monitorice las duraciones de las sesiones de usuario; y
genere la información de cadencia gradual que indica las cadencias de reconstrucción para el primer grupo de servidores y las cadencias de reconstrucción para el segundo grupo de servidores en base a las duraciones monitorizadas de las sesiones de usuario.

14. El medio legible por ordenador de la reivindicación 1, en el que las instrucciones cuando son ejecutadas por el al menos un procesador hacen que el por lo menos un procesador:

inicie repetidamente un cambio de contraseña de cada servidor en el primer grupo de servidores cuando se reconstruye el primer grupo de servidores; y
inicie repetidamente un cambio de contraseña de cada servidor en el segundo grupo de servidores cuando se reconstruye el segundo grupo de servidores.

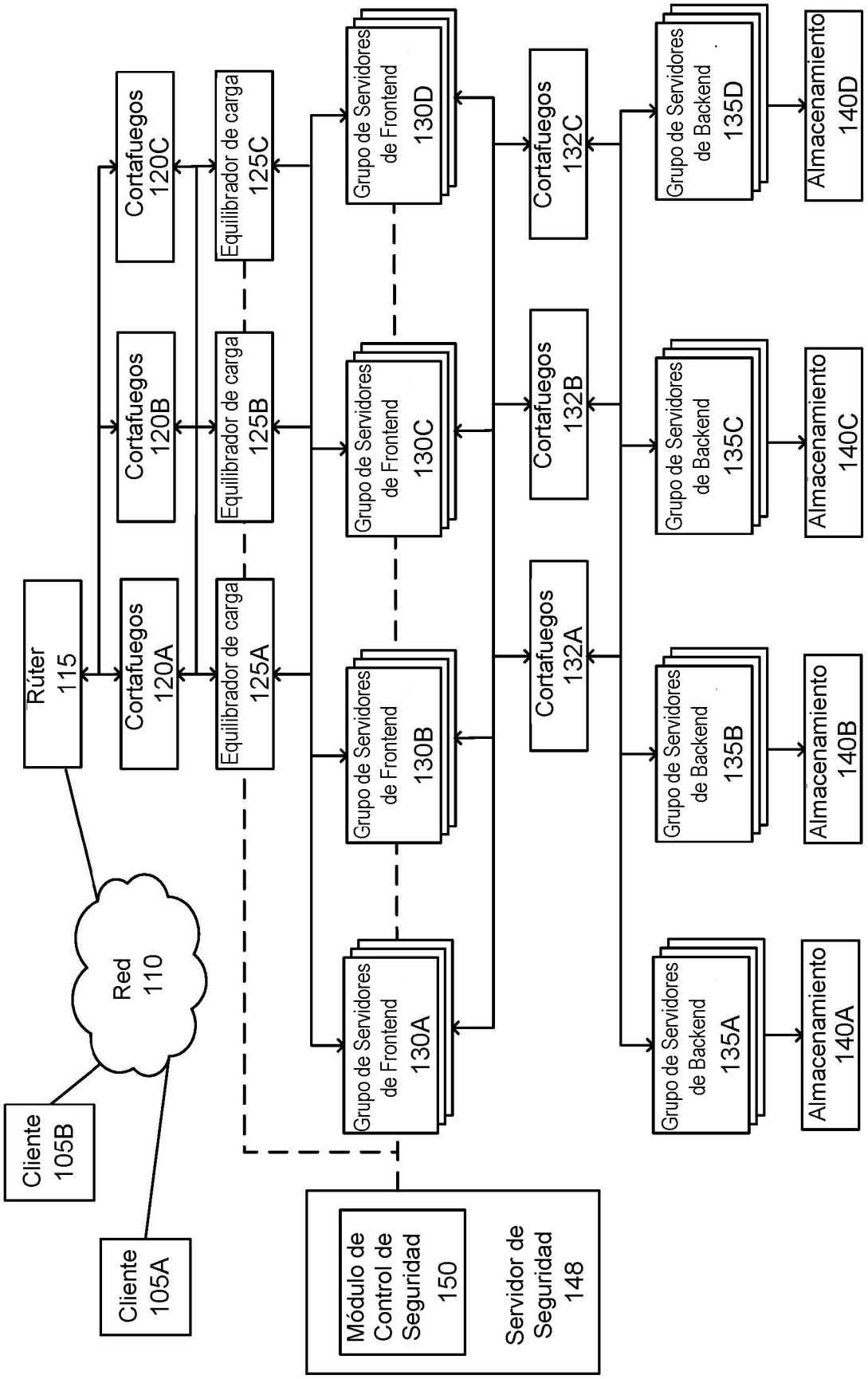
Cliente 105A
Cliente 105B
Red 110
Rúter 115
Cortafuegos 120A
Cortafuegos 120B
Cortafuegos 120C
Equilibrador de carga 125A
Equilibrador de carga 125B
Equilibrador de carga 125C
Grupo de Servidores de Frontend 130A
Grupo de Servidores de Frontend 130B
Grupo de Servidores de Frontend 130C
Grupo de Servidores de Frontend 130D
Cortafuegos 132A
Cortafuegos 132B
Cortafuegos 132C
Grupo de Servidores de Backend 135A
Grupo de Servidores de Backend 135B
Grupo de Servidores de Backend 135C
Grupo de Servidores de Backend 135D
Almacenamiento 140A
Almacenamiento 140B
Almacenamiento 140C
Almacenamiento 140D
Servidor de Seguridad 148
Módulo de Control de Seguridad 150

FIG. 1A

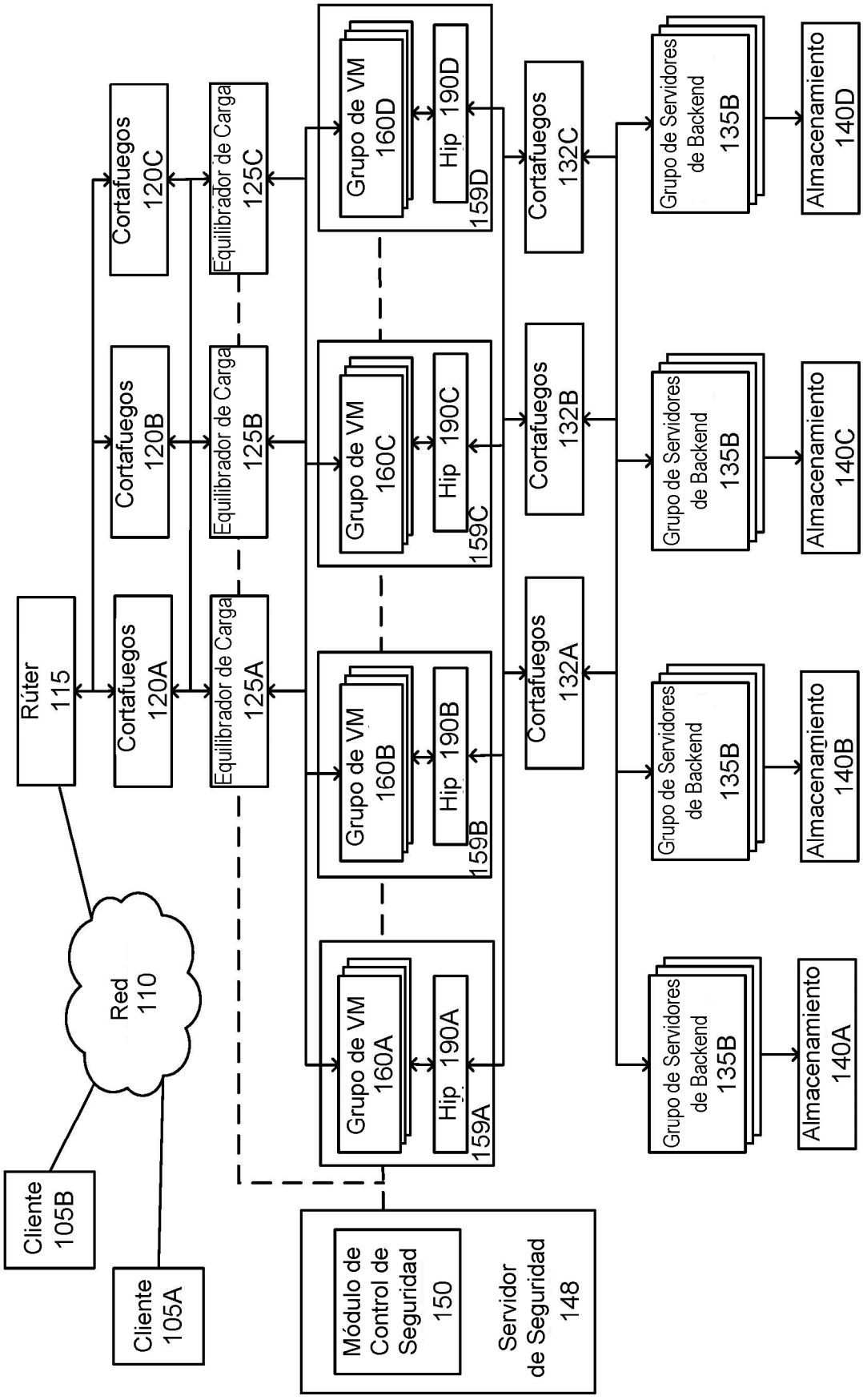
Cliente 105A
Cliente 105B
Red 110
Rúter 115
Módulo de Control de Seguridad 150
Servidor de Seguridad 148
Cortafuegos 120A
Cortafuegos 120B
Cortafuegos 120C
Equilibrador de Carga 125A
Equilibrador de Carga 125B
Equilibrador de Carga 125C
Grupo de VM 160A
Hip 190A
159A
Grupo de VM 160B
Hip 190B
159B
Grupo de VM 160C
Hip 190C
159C
Grupo de VM 160D
Hip 190D
159D
Cortafuegos 132A
Cortafuegos 132B
Cortafuegos 132C
Grupo de Servidores de Backend 135B
Grupo de Servidores de Backend 135B
Grupo de Servidores de Backend 135B
Grupo de Servidores de Backend 135B
Almacenamiento 140A
Almacenamiento 140B
Almacenamiento 140C
Almacenamiento 140D

FIG. 1B

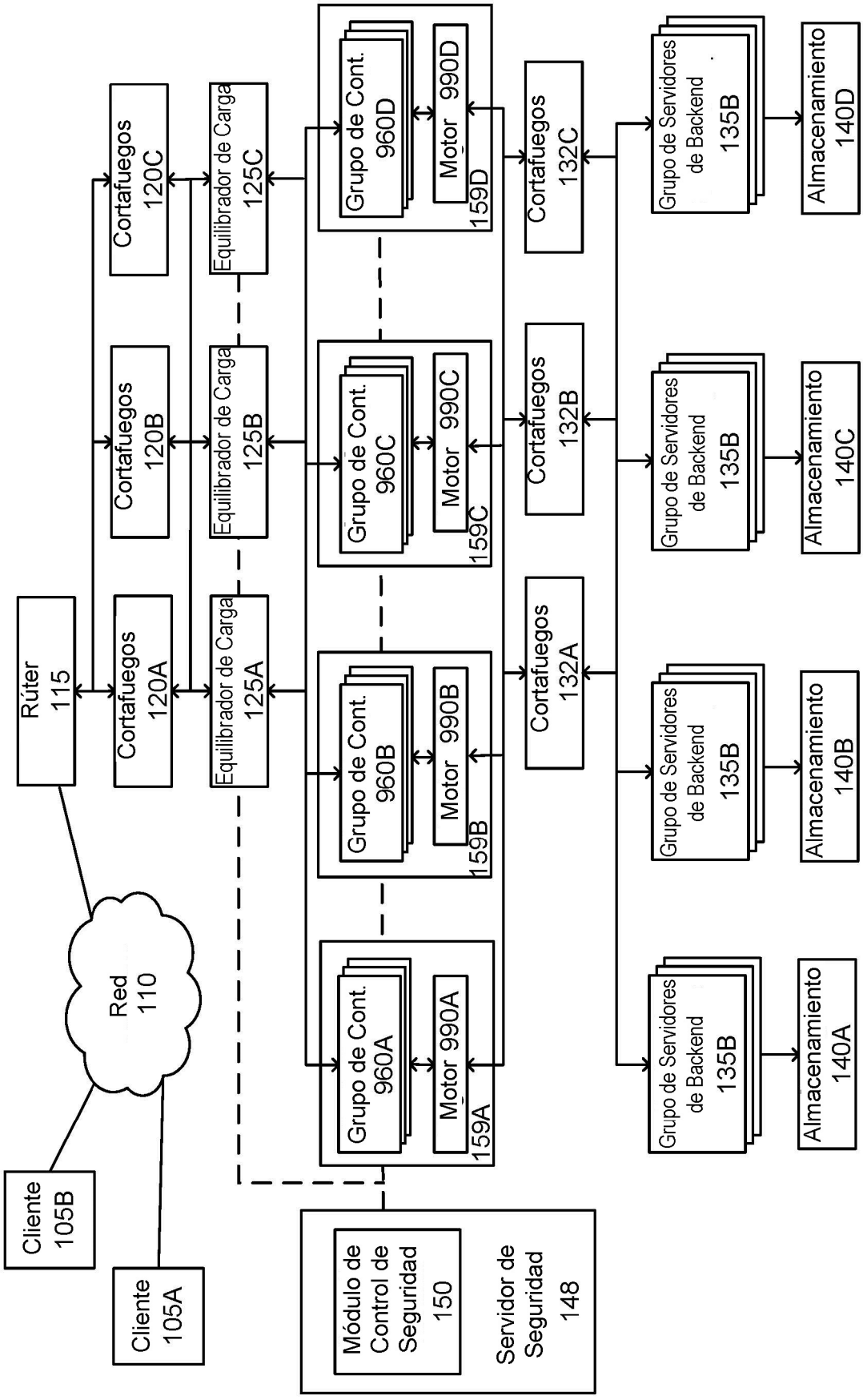
Cliente 105A
Cliente 105B
Red 110
Rúter 115
Cortafuegos 120A
Cortafuegos 120B
Cortafuegos 120C
Equilibrador de Carga 125A
Equilibrador de Carga 125B
Equilibrador de Carga 125C
Grupo de Cont. 960A
Motor 990A
159A
Grupo de Cont. 960B
Motor 990B
159B
Grupo de Cont. 960C
Motor 990C
159C
Grupo de Cont. 960D
Motor 990D
159D
Cortafuegos 132A
Cortafuegos 132B
Cortafuegos 132C
Grupo de Servidores de Backend 135B
Grupo de Servidores de Backend 135B
Grupo de Servidores de Backend 135B
Grupo de Servidores de Backend 135B
Almacenamiento 140A
Almacenamiento 140B
Almacenamiento 140C
Almacenamiento 140D
Módulo de Control de Seguridad 150
Servidor de Seguridad 148

FIG. 1C

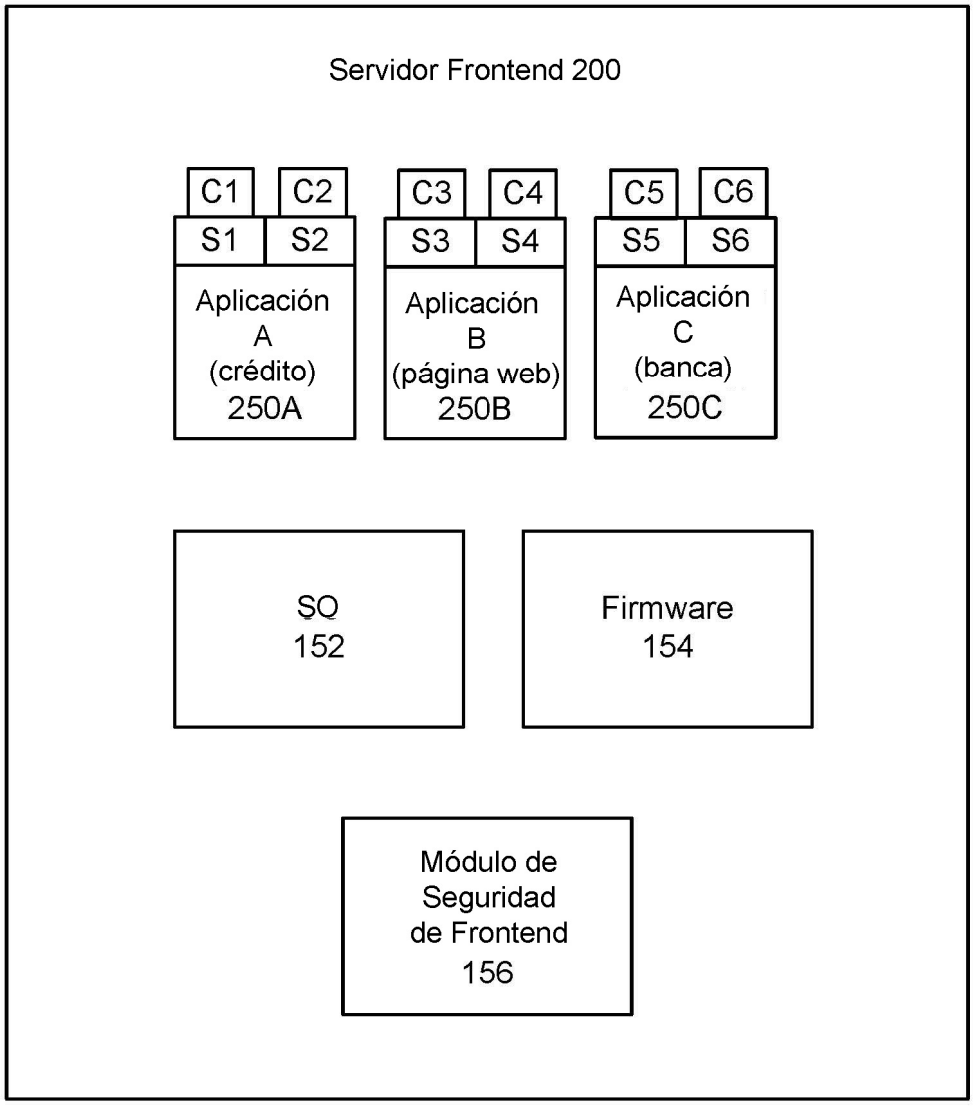
Servidor Frontend 200
C1
C2
S1
S2
Aplicación A (crédito) 250A
C3
C4
S3
S4
Aplicación B (página web) 250B
C5
C6
S5
S6
Aplicación C (banca) 250C
SO 152
Firmware 154
Módulo de Seguridad de Frontend 156

FIG. 2A

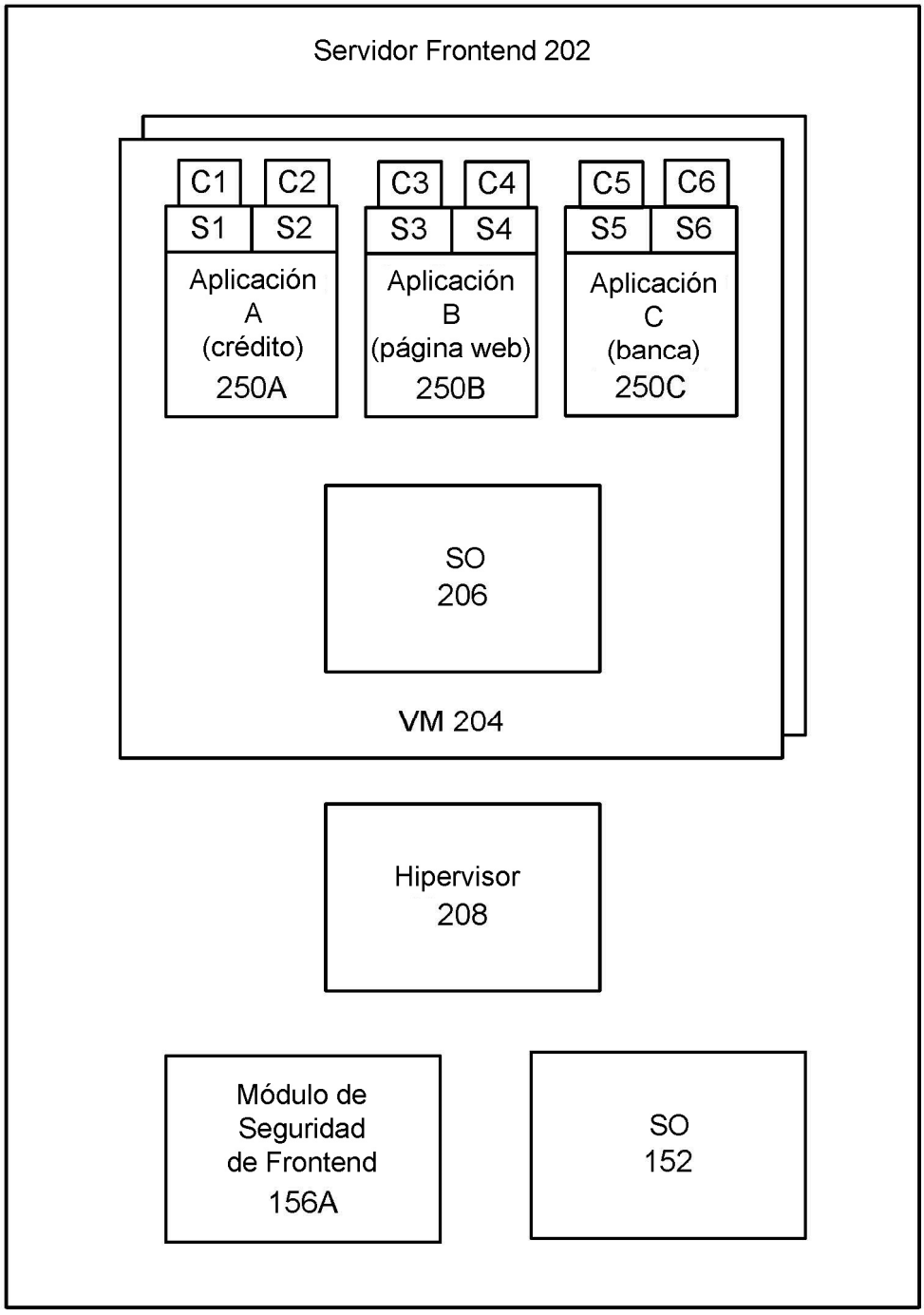
Servidor Frontend 202
C1
C2
S1
S2
Aplicación A (crédito) 250A
C3
C4
S3
S4
Aplicación B (página web) 250B
C5
C6
S5
S6
Aplicación C (banca) 250C
SO 206
VM 204
Hipervisor 208
Módulo de Seguridad de Frontend 156A
SO 152

FIG. 2B

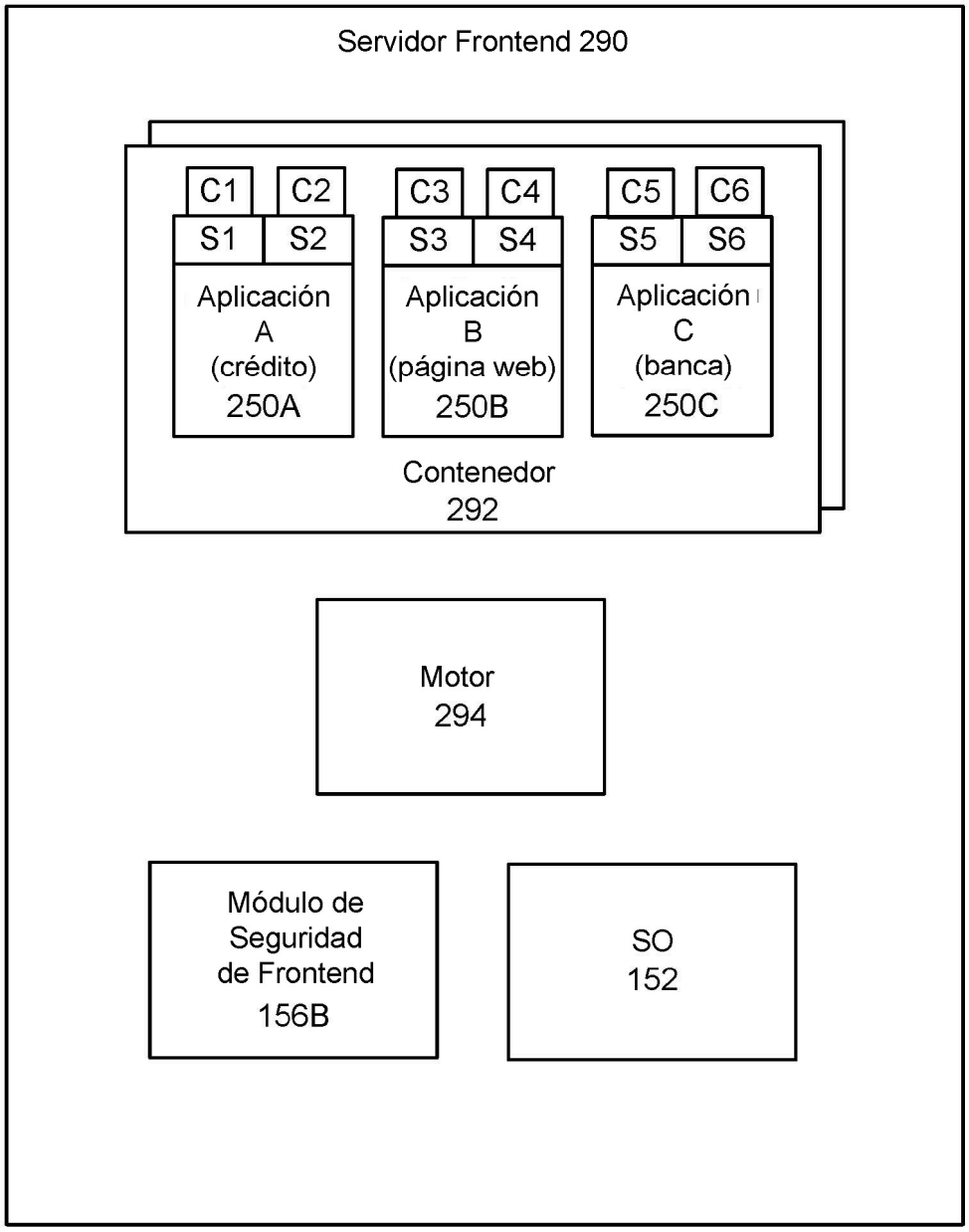
Servidor Frontend 290
C1
C2
S1
S2
Aplicación A (crédito) 250A
C3
C4
S3
S4
Aplicación B (página web) 250B
C5
C6
S5
S6
Aplicación C (banca) 250C
Contenedor 292
Motor 294
Módulo de Seguridad de Frontend 156B
SO 152

FIG. 2C

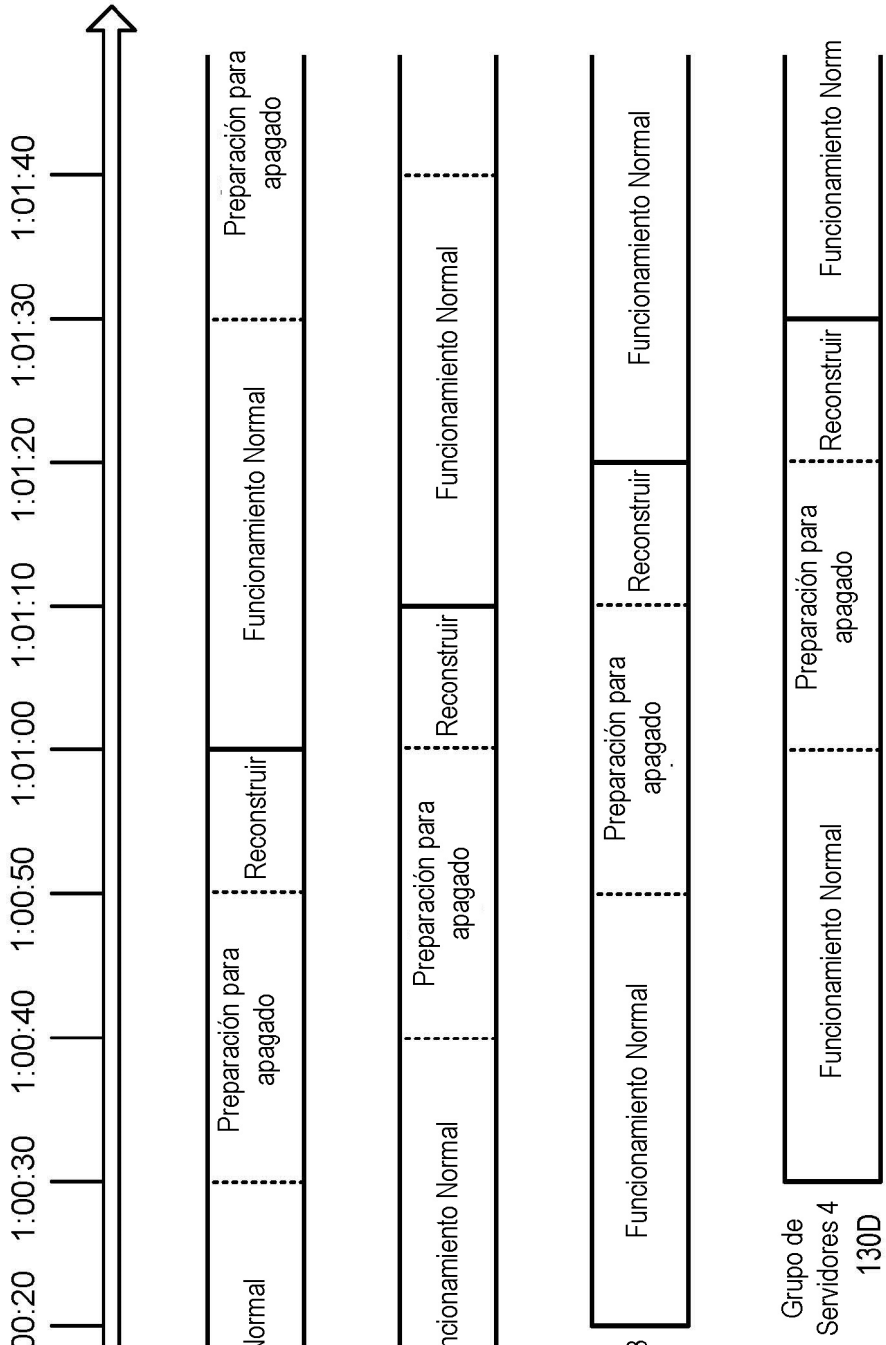
hora
1:00:00
1:00:10
1:00:20
1:00:30
1:00:40
1:00:50
1:01:00
1:01:10
1:01:20
1:01:30
1:01:40
Grupo de Servidores 1 130A
Funcionamiento Normal
Preparación para apagado
Reconstruir
Funcionamiento Normal
Preparación para apagado
Grupo de Servidores 2 130B
Funcionamiento Normal
Preparación para apagado
Reconstruir
Funcionamiento Normal
Grupo de Servidores 3 130C
Funcionamiento Normal
Preparación para apagado
Reconstruir
Funcionamiento Norm
Grupo de Servidores 4 130D

FIG. 3

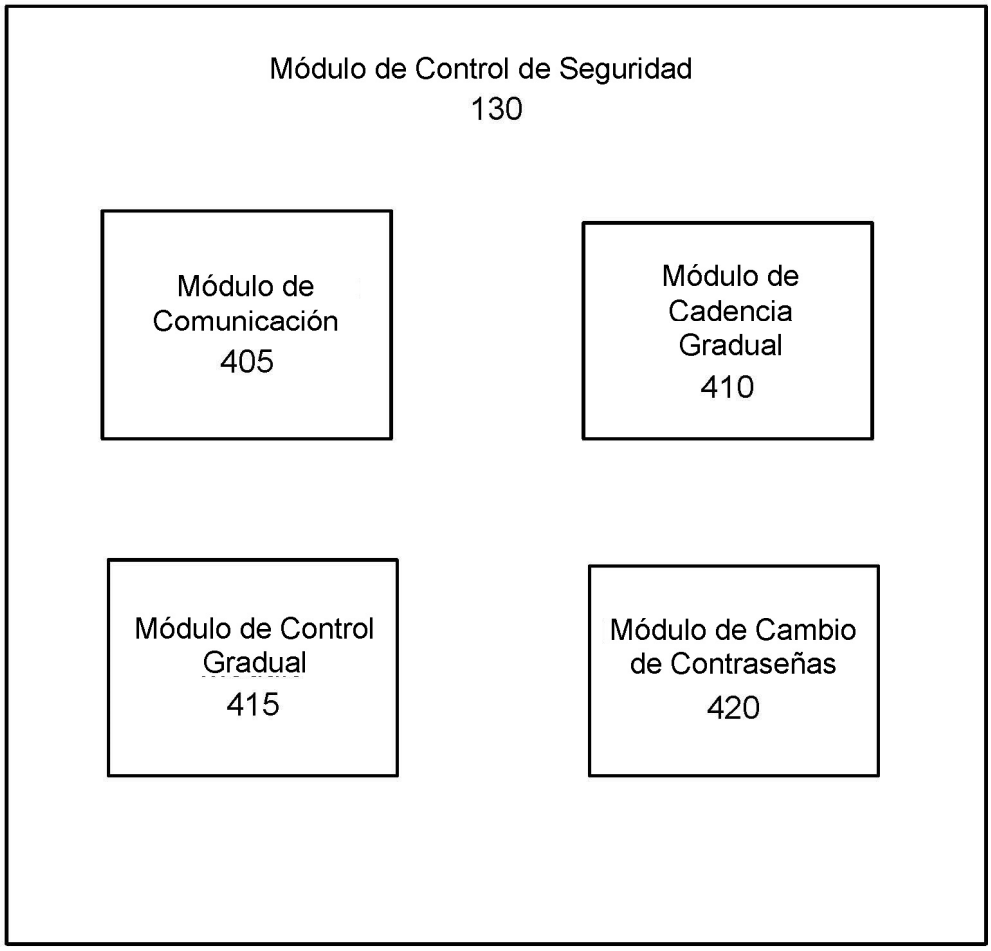
Módulo de Control de Seguridad
130
Módulo de Comunicación
405
Módulo de Cadencia Gradual
410
Módulo de Control Gradual
415
Módulo de Cambio de Contraseñas
420

FIG. 4

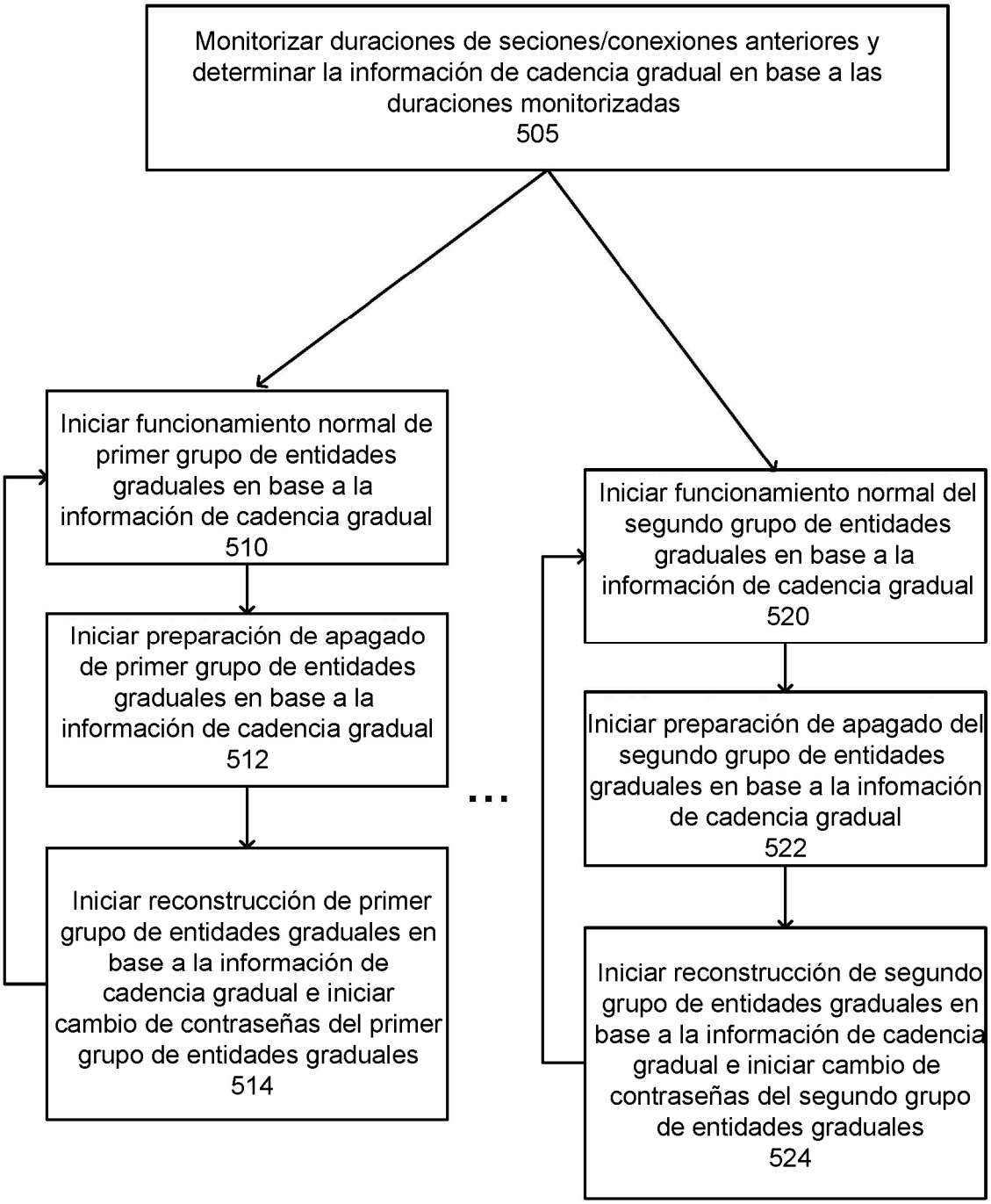
Monitorizar duraciones de seciones/conexiones anteriores y determinar la información de cadencia gradual en base a las duraciones monitorizadas
505
Iniciar funcionamiento normal de primer grupo de entidades graduales en base a la información de cadencia gradual
510
Iniciar preparación de apagado de primer grupo de entidades graduales en base a la información de cadencia gradual
512
Iniciar reconstrucción de primer grupo de entidades graduales en base a la información de cadencia gradual e iniciar cambio de contraseñas del primer grupo de entidades graduales
514
...
Iniciar funcionamiento normal del segundo grupo de entidades graduales en base a la información de cadencia gradual
520
Iniciar preparación de apagado del segundo grupo de entidades graduales en base a la infomación de cadencia gradual
522
Iniciar reconstrucción de segundo grupo de entidades graduales en base a la información de cadencia gradual e iniciar cambio de contraseñas del segundo grupo de entidades graduales
524

FIG. 5

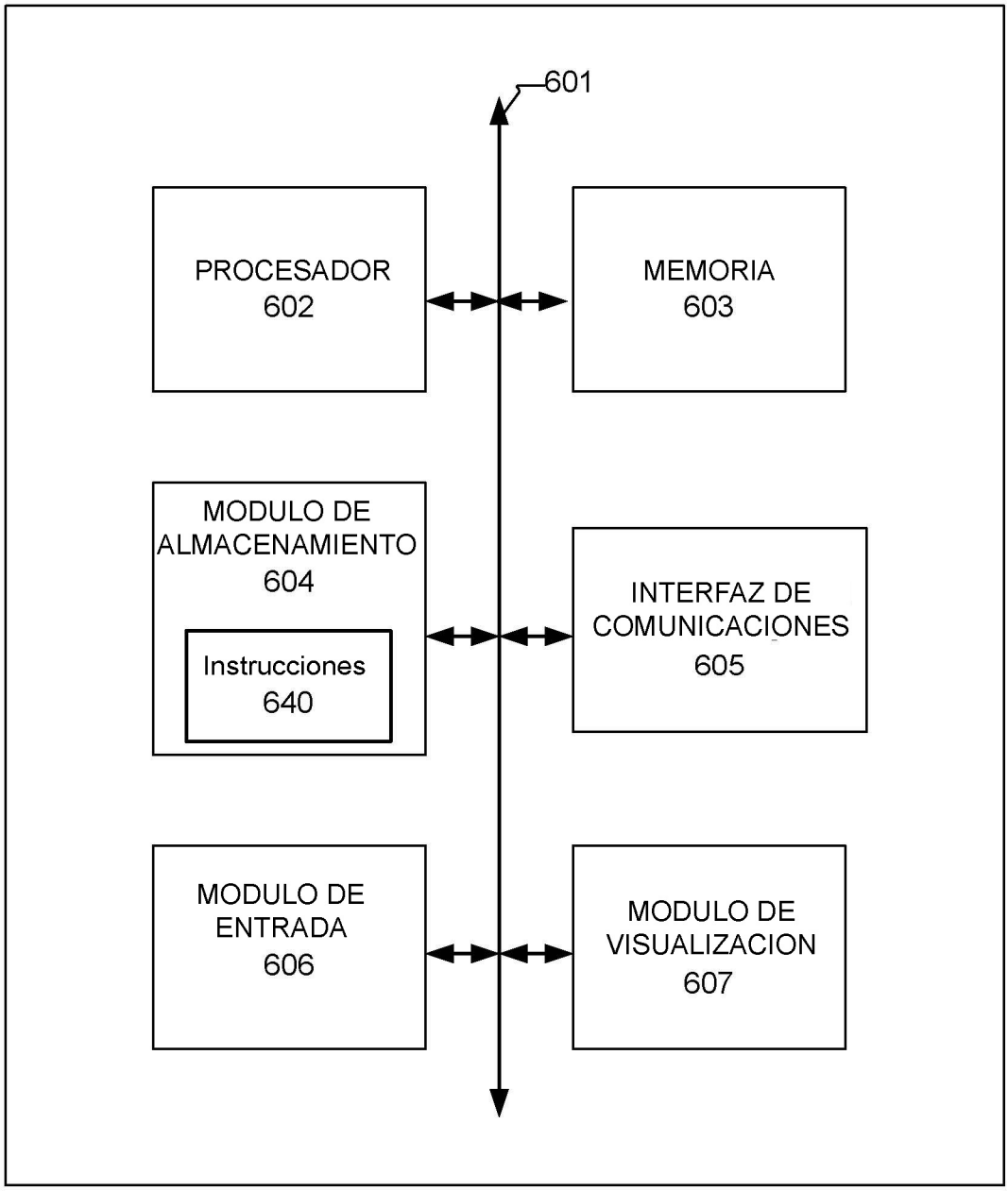
601
PROCESADOR
602
MEMORIA
603
MODULO DE
ALMACENAMIENTO
604
Instrucciones
640
INTERFAZ DE
COMUNICACIONES
605
MODULO DE
ENTRADA
606
MODULO DE
VISUALIZACION
607

FIG. 6