(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 758 927**

(51) Int. CI.:

H04L 29/06 (2006.01)
G06F 9/455 (2008.01)
G06F 9/50 (2006.01)
G06F 15/177 (2006.01)
G06F 21/53 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **11.12.2013 PCT/IB2013/060822**

(87) Fecha y número de publicación internacional: **19.06.2014 WO14091431**

(96) Fecha de presentación y número de la solicitud europea: **11.12.2013 E 13828986 (3)**

(97) Fecha y número de publicación de la concesión europea: **04.09.2019 EP 2932682**

(54) Título: **Cortafuegos híbrido para seguridad de centro de datos**

(30) Prioridad:

11.12.2012 US 201213710642

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
07.05.2020

(73) Titular/es:

TELEFONAKTIEBOLAGET LM ERICSSON (PUBL) (100.0%)
Stockholm
164 83 Stockholm, SE

(72) Inventor/es:

ZHU, ZHONGWEN y
POURZANDI, MAKAN

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Cortafuegos híbrido para seguridad de centro de datos

Campo técnico

Esta invención se refiere en general a la seguridad informática en la nube. En particular, los sistemas y métodos para administrar cortafuegos de hardware y software y otros requisitos de servicio de una aplicación virtualizada.

Antecedentes

Con la rápida evolución de Computación en la Nube ("Cloud Computing"), se ha hecho cada vez más común ejecutar programas de ordenador en máquinas virtuales que operan en servidores. Una máquina virtual (VM) es una implementación de software de una máquina (es decir, un ordenador) que ejecuta programas como una máquina física. El hardware físico en el que funcionan las máquinas virtuales se denomina como anfitrión u ordenador/ordenadores anfitriones y puede residir en instalaciones de centros de datos.

Los centros de datos son instalaciones utilizadas para alojar sistemas informáticos y componentes asociados, que generalmente incluyen rúters y conmutadores para transportar el tráfico entre los sistemas informáticos y las redes externas. Los centros de datos generalmente incluyen fuentes de alimentación redundantes y conexiones de comunicaciones de datos redundantes para proporcionar una infraestructura fiable para las operaciones y minimizar cualquier posibilidad de interrupción. La seguridad de la información también es una preocupación y, por esta razón, un centro de datos debe ofrecer un entorno seguro para minimizar cualquier posibilidad de violación de la seguridad.

La virtualización tiene varias ventajas sobre los entornos informáticos convencionales. El sistema operativo y las aplicaciones que se ejecutan en una máquina virtual a menudo requieren solo una fracción de los recursos completos disponibles en el hardware físico subyacente en el que está funcionando la máquina virtual. Un sistema anfitrión puede emplear múltiples ordenadores físicos, cada uno de los cuales ejecuta múltiples máquinas virtuales. Las máquinas virtuales se pueden crear y apagar según sea necesario, utilizando solo así los recursos del ordenador u ordenadores físicos según sea necesario. Una aplicación virtual puede ejecutarse en una o varias máquinas virtuales que pueden ampliarse o reducirse según lo requiera la aplicación.

Otra ventaja de la virtualización es la flexibilidad proporcionada por la capacidad de manipular y mover una máquina virtual de un sitio físico a otro, o mover una máquina virtual entre anfitriones dentro del mismo centro de datos. Las máquinas virtuales se pueden mover para utilizar mejor las máquinas anfitrionas y proporcionar la elasticidad para aumentar o disminuir de tamaño.

Muchos centros de datos usan dispositivos, que emplean hardware y software dedicados, para proporcionar diversos servicios en el centro de datos. Dichos servicios pueden incluir servicios de cortafuegos, servicios de equilibrio de carga, servicios de Administración Unificada de Amenazas (UTM), sistemas de detección y prevención de intrusos (IDS/IPS), sistemas de prevención de pérdida de datos (DLP), servicios de Proxy/Pasarela y otros servicios de seguridad.

La Figura 1 ilustra un centro 100 de datos con un dispositivo 102 de hardware desplegado frente al centro 100 de datos que proporciona servicios de cortafuegos y seguridad. El centro 100 de datos tiene 7 servidores "blade" 104, 106, 108, 110, 112, 114, 116. Los servidores "blade" 1 - 5, 104 - 112, ejecutan máquinas virtuales VM1 - VM10 gestionadas por la capa 118 de virtualización. Los servidores "blade" 6 y 7, 114 y 116, ejecutan componentes de almacenamiento virtual VS1 - VS4 gestionados por la capa 120 de virtualización. El cortafuegos 102 de hardware inspecciona y filtra el tráfico procedente de la red 122 al centro 100 de datos. La capacidad de este cortafuegos 102 es determinada en función del rendimiento máximo para el centro 100 de datos. En la práctica, esto a menudo conduce al sobredimensionamiento del cortafuegos 102.

Si en el futuro, el centro 100 de datos de hardware se actualiza y la capacidad total del centro 100 de datos se incrementa, también tendrá que ser actualizado el dispositivo cortafuegos 102 para satisfacer la demanda creciente de tráfico. Este tipo de operación puede requerir la interrupción del servicio, una inversión en actualizaciones de hardware/software y un alto costo operativo.

La virtualización de los servicios proporcionados por los dispositivos de hardware también está ganando impulso. Por ejemplo, un cortafuegos virtual (VF) es un servicio de cortafuegos de red que funciona por completo dentro de un entorno virtual que puede proporcionar el mismo filtrado y monitorización de paquetes que el que proporciona tradicionalmente un cortafuegos de red físico o dispositivo de servicio de cortafuegos.

La Figura 2 ilustra un centro 200 de datos que emplea un cortafuegos puramente virtual. El centro 200 de datos tiene 7 servidores "blade" 204, 206, 208, 210, 212, 214 y 216. Los servidores "blade" 1 - 5, 204 - 212, ejecutan máquinas virtuales VM1 - VM10 gestionadas por la capa 218 de virtualización. Los servidores "blade" 6 y 7, 214 y 216, ejecutan componentes de almacenamiento virtual VS1 - VS4 gestionados por la capa 220 de virtualización. Los servidores "blade" 4 y 5, 210 y 212, se pueden aprovisionar en máquinas virtuales VM7 - VM10 que ejecutan aplicaciones de cortafuegos, o más simplemente llamados "cortafuegos virtuales". Los servidores "blade" 4, 210, puede dedicarse a cortafuegos virtuales en todo momento, mientras que los servidores "blade" 5, 212, pueden asignarse al cortafuegos cuando aumenta

el tráfico. Estas máquinas virtuales, VM9 y VM10, se pueden liberar cuando el tráfico disminuye. El cortafuegos virtual puede inspeccionar y filtrar el tráfico desde la red 222 al centro 200 de datos de forma similar al cortafuegos 102 de hardware de la Figura 1. Un servicio de cortafuegos virtualizado permite escalar los recursos con los requisitos de tráfico.

Por lo tanto, sería deseable proporcionar un sistema y un método para integrar hardware y componentes de cortafuegos virtual y mitigar los problemas de escalabilidad asociados.

La exposición que no es una patente de Hasan M.Z. et al: "Integrated and Autonomic Cloud Resource Scaling" ("Escalado de Recursos en la Nube Integrados y Autonómicos"), 2012 IEEE Network Operations and Management Symposium (NOMS 2012), 16 de Abril de 2012, XP032448820, ISBN: 978-1-4673-0267-8, páginas 1327-1334, describe un sistema de auto-escalado de recursos en la nube que proporciona una técnica de auto-escalado integrada que impide el escalado falso y reduce el número de sistemas de auto-escalado que han de ser soportados en un sistema de administración en la nube. Ejemplos de recursos pueden incluir máquinas virtuales y cortafuegos virtuales. La exposición aborda recursos de red de escalado con relación a recursos de cálculo y almacenamiento, por ejemplo, cuando se escalan recursos de cálculo virtuales, pueden también ser auto-escalados equilibradores de carga o cortafuegos.

La exposición de bibliografía que no es una patente de Ho-Yu Lam et al: "Hybrid Security Architecture for Data Center Networks" ("Arquitectura Híbrida de Seguridad para Redes de Centros de Datos"), IEEE International Conference on Communications (ICC), 10 de Junio de 2012, XP032274347, ISBN: 978-1-4577-2052-9, páginas 2939-2944, se refiere al problema de que, cuando se escala un centro de datos, el sistema de seguridad necesita ser actualizado consecuentemente. La exposición presenta una así llamada Arquitectura de Seguridad Híbrida (HSA) que representa un diseño para desacoplar servicios de seguridad de enrutamiento y permitir la integración de hardware y dispositivos de red de software de modo complementario.

La Solicitud de Patente US 2011/0258621 A1 se refiere al escalado autonómico de máquinas virtuales en un entorno de computación en la nube. Según una realización, un método incluye desplegar, mediante un sistema que opera en la nube, un ejemplo de una máquina virtual, transmitir el ejemplo de la máquina virtual para escalado autonómico, monitorizar una o más características operativas del ejemplo de la máquina virtual, y desplegar un ejemplo adicional de la máquina virtual si un valor de una característica operativa excede un primer valor umbral predeterminado, incluyendo ejecutar una parte de la carga de trabajo de procesamiento de datos en el ejemplo adicional de la máquina virtual.

Compendio

Es un objeto de la presente invención obviar o mitigar al menos una desventaja de la técnica anterior.

En un primer aspecto de la presente invención, se proporciona un método para gestionar los requisitos de cortafuegos relacionados con una aplicación virtualizada. Una entidad de administración de computación en la nube, que incluye un procesador, determina que una aplicación virtualizada, asociada con una primera pluralidad de máquinas virtuales de aplicación y una segunda pluralidad de máquinas virtuales de cortafuegos, requiere un número incrementado de máquinas virtuales de aplicación en la primera pluralidad. Se determina que se requiere un número incrementado de máquinas virtuales de cortafuegos por el número incrementado de máquinas virtuales de aplicación. Se ejemplifica una máquina virtual de aplicación; y se ejemplifica una máquina virtual de cortafuegos.

El umbral de relación de cortafuegos se puede incluir en un perfil de aplicación configurado en el despliegue de la aplicación virtualizada. La aplicación virtualizada se puede alojar en la primera pluralidad de máquinas virtuales de aplicación y la segunda pluralidad de máquinas virtuales de cortafuegos puede proporcionar servicios de cortafuegos para el tráfico asociado con la aplicación virtualizada.

En otra realización, el método comprende además comparar el número incrementado requerido de máquinas virtuales de aplicación con el número de máquinas virtuales de cortafuegos en la segunda pluralidad.

En otra realización, el método comprende además calcular una relación del número incrementado requerido de máquinas virtuales de aplicación al número de máquinas virtuales de cortafuegos en la segunda pluralidad; y comparar la relación calculada con un requisito de relación de cortafuegos asociado con la aplicación virtualizada.

En otra realización, el método comprende además comparar las etapas de determinar que se requiere un número incrementado de máquinas virtuales de equilibrio de carga por el número incrementado de máquinas virtuales de aplicación, y ejemplificar una máquina virtual de equilibrio de carga.

En otra realización, el método comprende además las etapas de determinar que la aplicación virtualizada requiere un número reducido de máquinas virtuales de aplicación en la primera pluralidad; determinar que un número reducido de máquinas virtuales de aplicación es requerido por el número reducido de máquinas virtuales de aplicación; apagar una máquina virtual de aplicación; y apagar una máquina virtual de cortafuegos.

En un segundo aspecto de la presente invención, se proporciona una entidad de administración de la nube según la reivindicación 9. La entidad de administración de la nube comprende una memoria para almacenar instrucciones y un motor de procesamiento configurado para ejecutar las instrucciones. El motor de procesamiento está configurado para determinar que una aplicación virtualizada, asociada con una primera pluralidad de máquinas virtuales de aplicación y

una segunda pluralidad de máquinas virtuales de cortafuegos, requiere un número incrementado de máquinas virtuales de aplicación en la primera pluralidad. El motor de procesamiento determina que se requiere un número incrementado de máquinas virtuales de cortafuegos por el número incrementado de máquinas virtuales de aplicación. El motor de procesamiento ejemplifica una máquina virtual de aplicación y ejemplifica una máquina virtual de cortafuegos.

En una realización del segundo aspecto de la presente invención, la entidad de administración en la nube comprende además una interfaz de comunicación para comunicarse con la primera pluralidad de máquinas virtuales de aplicación y la segunda pluralidad de máquinas virtuales de cortafuegos.

El umbral de relación de cortafuegos se puede incluir en un perfil de aplicación configurado en el despliegue de la aplicación virtualizada por el motor de procesamiento. La aplicación virtualizada se puede alojar en la primera pluralidad de máquinas virtuales de aplicación y la segunda pluralidad de máquinas virtuales de cortafuegos puede proporcionar servicios de cortafuegos para el tráfico asociado con la aplicación virtualizada.

En otra realización, el motor de procesamiento compara el número incrementado requerido de máquinas virtuales de aplicación en la primera pluralidad con el número de máquinas virtuales de cortafuegos en la segunda pluralidad.

En otra realización, el motor de procesamiento calcula una relación del número incrementado requerido de máquinas virtuales de aplicación en la primera pluralidad al número de máquinas virtuales de cortafuegos en la segunda pluralidad; y compara la relación calculada con un umbral de relación de cortafuegos asociado con la aplicación virtualizada.

Otros aspectos y características de la presente invención resultarán evidentes para los expertos en la técnica tras la revisión de la siguiente descripción de realizaciones específicas de la invención en combinación con las figuras adjuntas.

Breve descripción de los dibujos

A continuación se describirán realizaciones de la presente invención, solo a modo de ejemplo, con referencia a las Figuras adjuntas, en las que:

La Figura 1 es un diagrama de bloques de un centro de datos de la técnica anterior con un cortafuegos de hardware;

La Figura 2 es un diagrama de bloques de un centro de datos de la técnica anterior con un cortafuegos virtual;

La Figura 3 es un diagrama de bloques de un centro de datos con un cortafuegos híbrido;

La Figura 4a es un ejemplo de asignaciones de máquinas virtuales por primera vez;

La Figura 4b es un ejemplo de asignaciones de máquinas virtuales por segunda vez;

La Figura 5 es un diagrama de flujo que ilustra una realización;

La Figura 6 es un diagrama de flujo de llamadas que ilustra una realización;

La Figura 7 es un diagrama de flujo de un método de acuerdo con una o más realizaciones; y

La Figura 8 es un diagrama de bloques de un ejemplo de dispositivo de administración en la nube.

Descripción detallada

Se puede hacer referencia a continuación a elementos específicos, numerados de acuerdo con las Figuras adjuntas. La exposición a continuación debe considerarse de naturaleza ejemplar y no como limitante del alcance de la presente invención. El alcance de la presente invención se define en las reivindicaciones, y no debe considerarse limitado por los detalles de implementación descritos a continuación, que como apreciará un experto en la técnica, pueden modificarse reemplazando elementos con elementos funcionales equivalentes.

La presente invención está dirigida a un sistema y método para administrar una solución de cortafuegos híbrido que emplea tanto hardware como componentes de cortafuegos virtual. La parte de hardware puede ser muy especializada en operaciones básicas y, por lo tanto, no es necesario que se actualice a menudo. La capacidad de la parte de cortafuegos virtual puede variar con la capacidad de las aplicaciones que se ejecutan en un centro de datos en un momento dado. Se puede aplicar una relación predefinida entre el cortafuegos virtual y las aplicaciones virtualizadas para evitar cuellos de botella o bloqueos en el manejo del tráfico del servicio. La adición de cortafuegos virtuales adicionales se puede lograr mediante el lanzamiento de máquinas virtuales adicionales dedicadas a ejecutar el servicio de cortafuegos.

Las diferentes aplicaciones virtuales pueden tener diferentes requisitos y, por lo tanto, cada aplicación puede tener un perfil de relación de seguridad diferente que se puede configurar en el despliegue de la aplicación. Este perfil de relación de seguridad se puede usar para verificar la relación entre la cantidad de cortafuegos virtuales y la cantidad de máquinas virtuales que proporcionan la aplicación. Alternativamente, el perfil de seguridad puede definir un requisito de relación para la capacidad de ancho de banda, el tipo de máquinas virtuales, la potencia de procesamiento, el almacenamiento/memoria, o una combinación de los mismos, entre las máquinas virtuales de cortafuegos y las máquinas virtuales de aplicación asociadas con la aplicación.

La Figura 3 ilustra un centro 300 de datos que emplea un cortafuegos híbrido. Un cortafuegos 302 de hardware y un cortafuegos 303 virtual están integrados para proteger el centro 300 de datos. El centro 300 de datos tiene 7 servidores “blade” 304, 306, 308, 310, 312, 314 y 316. Los servidores “blade” 1 - 5, 304 - 312, proporcionan máquinas virtuales VM1 - VM10 administradas por la capa 318 de virtualización. Los servidores “blade” 6 y 7, 314 y 316, proporcionan componentes de almacenamiento virtual VS1 - VS4 administrados por la capa 320 de virtualización. El servidor “blade” 5, 312, proporciona máquinas virtuales VM9 y VM10 dedicadas a ejecutar el servicio de cortafuegos virtual. La capacidad del cortafuegos 302 de hardware puede diseñarse originalmente para manejar todo el tráfico esperado desde la red 322 al centro 300 de datos. A medida que pasa el tiempo, se puede actualizar parte del hardware en los servidores “blade” del centro 300 de datos y el centro 300 de datos total es capaz de manejar más tráfico. En este escenario, se puede exceder la capacidad del cortafuegos y el cortafuegos 302 de hardware se convierte en un cuello de botella. Para manejar el aumento del tráfico, el cortafuegos virtual 303 se puede iniciar en el servidor “blade” 5, 312. Una parte del tráfico entrante puede encaminarse a continuación hacia el cortafuegos virtual 303 para descargar la demanda en el dispositivo 302 de hardware.

Aunque la Figura 3 solo está relacionada con un hardware híbrido y un cortafuegos virtual, los expertos en la técnica apreciarán que los mismos conceptos se pueden aplicar a otros servicios en el centro de datos, tales como el equilibrio de carga. En una realización adicional, la parte de hardware puede comprender un equilibrador de carga "superficial", un cortafuegos superficial y un componente de correspondencia de patrones de hardware. Todos estos elementos son conocidos por implementarse eficientemente en hardware. Al implementar estos elementos en el hardware, el sistema puede beneficiarse de años de desarrollo en tecnología de hardware para el filtrado basado en el Protocolo de Internet (IP) y mecanismos para la correspondencia de patrones para detectar firmas de malware en los paquetes. Estos elementos se configuran principalmente en el momento del despliegue de la aplicación virtual asociada. No es necesario que la parte de hardware conozca el perfil de seguridad de la aplicación virtual, ya que el filtrado se realiza en función de la información de la capa L3-L5 y la parte de hardware no analiza la capa de aplicación, L7. Por ejemplo, el equilibrador de carga superficial puede equilibrar la carga utilizando solo la tupla IP 5 de un paquete (dirección IP de origen, puerto de origen, dirección IP de destino, puerto de destino, protocolo). El cortafuegos superficial también puede filtrar utilizando solo la tupla IP 5. La correspondencia de patrones de hardware puede utilizar expresiones regulares de hardware y reconocimiento de patrones utilizando componentes de hardware en paquetes IP. Se puede probar un conjunto predefinido de firmas de malware en todos los paquetes IP, sin requerir el conocimiento del perfil de seguridad de la aplicación virtual asociada.

La parte de software de este ejemplo incluye un cortafuegos virtual y un equilibrador de carga virtual que se ejecuta en máquinas virtuales y ajustado al perfil de seguridad de la aplicación virtual específica. Estos componentes generalmente pueden operar sobre la capa de aplicación, L7. Por lo tanto, existe un requisito en el despliegue para establecer parámetros predefinidos para el perfil de seguridad de la aplicación virtual. Por lo tanto, es posible crear un cortafuegos virtual y/o equilibrador de carga bien ajustado para cada aplicación específica y aumentarlos o disminuirlos de manera independiente para cada aplicación. No existe una necesidad urgente de hardware especializado para estos componentes, ya que los mecanismos de seguridad se basan en algoritmos tales como la monitorización de comportamiento que generalmente son monitorizados por computadoras generales y no se implementan de manera tan eficiente en hardware en la industria.

Cabe señalar que la parte de hardware de este enfoque híbrido es común para todas las aplicaciones virtuales en el centro de datos, incluso aunque los perfiles de seguridad para varias aplicaciones virtuales pueden diferir. La parte de software está dedicada a cada aplicación virtual y puede ajustarse a su perfil de seguridad. Aunque la parte de hardware puede considerarse como no elástica y no escalable, si el tráfico aumenta a un nivel inmanejable para la parte de hardware, se pueden crear máquinas virtuales de cortafuegos adicionales para manejar el tráfico adicional antes de encaminarlo a los componentes de software.

Con el fin de proporcionar una escalabilidad adicional y forzar perfiles de relación de seguridad de la aplicación, como se expuso anteriormente, se prevé un mecanismo para asignar máquinas virtuales para diferentes aplicaciones en el centro de datos. Las figs. 4a y 4b ilustran asignaciones ejemplares de máquinas virtuales en el centro 300 de datos en dos puntos diferentes de tiempo, t1 y t2.

En la Figura 4a, en un primer momento t1, se asignan cuatro máquinas virtuales para las aplicaciones 400a de administración en la nube, se asignan tres máquinas virtuales para los servicios 402a de cortafuegos, se asignan dos máquinas virtuales para los servicios 404a de equilibrio de carga, y se utilizan diecinueve máquinas virtuales para la aplicación o aplicaciones 406a. En la Figura 4b, en un segundo momento t2, se asignan cuatro máquinas virtuales para aplicaciones 400b de administración en la nube, se asignan cinco máquinas virtuales para servicios 402b de cortafuegos, se asignan tres máquinas virtuales para servicios 404b de equilibrio de carga, y se utilizan veintiocho máquinas virtuales para la aplicación o aplicaciones 406b. A partir de este ejemplo, los expertos en la técnica apreciarán la relación entre el número de máquinas virtuales asignadas entre el cortafuegos, el equilibrio de carga y las aplicaciones.

En un entorno privado de computación en la nube, al contrario que en un centro de datos público, los tipos exactos de aplicaciones que se han de desplegar son conocidos y finitos. Se supone que los desarrolladores de aplicaciones pueden definir perfiles para sus aplicaciones que detallen un conjunto de parámetros que deben cumplirse en el momento de la implementación. Se puede suponer que en cualquier momento, muchas aplicaciones virtuales diferentes con diferentes perfiles de seguridad predefinidos pueden ejecutarse en la nube privada. Por ejemplo, en una nube de

telecomunicaciones, un perfil de Subsistema Multimedia de IP (IMS), un perfil de Voz sobre IP (VoIP), un perfil de televisión de Protocolo de Internet (IPTV), un perfil de Pasarela de Red de Datos por Paquetes (PDN GW) y un perfil de Protocolo de Transferencia de Hipertexto (HTTP) para aplicaciones web pueden ser todos definidos.

Como los requisitos de estas aplicaciones de telecomunicaciones convencionales son bien conocidos, es posible definir una relación de cortafuegos que establece cuántos cortafuegos virtuales deben desplegarse para manejar el tráfico de un número X de máquinas virtuales asociadas con la aplicación virtual. Cabe señalar que esta relación puede ser una función del número de máquinas virtuales que ejecutan diferentes tipos de aplicaciones dentro de la misma aplicación virtual o tipo de aplicación virtual. Por ejemplo, una aplicación IMS virtual puede incluir máquinas virtuales que ejecutan procesadores de tráfico, cargadores de entrada/salida y rúters. La relación de cortafuegos para la aplicación IMS se puede definir como una función del número total de máquinas virtuales que ejecutan las distintas sub-aplicaciones dentro de la aplicación virtual.

La relación de cortafuegos se puede utilizar como base para asignar o distribuir máquinas virtuales para diferentes aplicaciones. A diferencia de esperar simplemente a que la carga de tráfico alcance un umbral y luego lanzar cortafuegos virtuales adicionales, el enfoque expuesto aquí es proactivo y crea nuevos cortafuegos virtuales en paralelo con la creación de nuevos ejemplos de máquinas virtuales para la aplicación. Por lo tanto, el componente o los componentes de software de los requisitos de seguridad pueden ampliarse y reducirse al mismo tiempo que la propia aplicación se amplia y se reduce. Basado en la combinación de las diferentes relaciones para las diversas aplicaciones virtuales, también se puede definir una relación total para el centro de datos.

Los perfiles de relación también se pueden crear con respecto a otros servicios virtualizados, tales como el equilibrio de carga. Por ejemplo, una aplicación virtual puede tener una relación de cortafuegos y una relación de equilibrio de carga que define la cantidad de máquinas virtuales de cortafuegos y la cantidad de máquinas virtuales de equilibrio de carga necesarias para una determinada cantidad de máquinas virtuales de aplicación.

La Figura 5 es un diagrama de flujo que ilustra una realización de la presente invención para escalar nuevos ejemplos de cortafuegos virtuales y equilibradores de carga virtuales para una aplicación virtual. Este proceso puede ser realizado por un sistema de administración en la nube o una aplicación en un centro de datos. El proceso comienza al recibir una solicitud de al menos una máquina virtual adicional para una aplicación (etapa 500). En respuesta a la solicitud, se lanzan una o más máquinas virtuales de aplicación (etapa 502). Se verifica la relación entre el número de máquinas virtuales que ejecutan servicios de cortafuegos y el número de máquinas virtuales que ejecutan la aplicación (etapa 504) para determinar si se requieren máquinas virtuales de cortafuegos adicionales (etapa 506). Si no se necesitan nuevas máquinas virtuales de cortafuegos, la máquina o máquinas virtuales de aplicación recién lanzadas se pueden asociar con las máquinas virtuales de cortafuegos existentes (etapa 508). Si se requiere una máquina virtual de cortafuegos adicional, se lanza (etapa 510) y se asocia con la nueva máquina o máquinas virtuales de aplicación (etapa 512). Opcionalmente, la máquina virtual de cortafuegos recién lanzada puede asociarse tanto con las máquinas virtuales de cortafuegos existentes como con las máquinas virtuales de aplicación existentes.

Después de satisfacer la relación de cortafuegos para la aplicación virtual, también se puede verificar la relación de equilibrio de carga entre el número de máquinas virtuales que ejecutan servicios de equilibrio de carga y el número de máquinas virtuales que ejecutan la aplicación (etapa 514). Se determina si se requieren máquinas virtuales de equilibrio de carga adicionales para satisfacer la relación (516). Si no se necesitan nuevas máquinas virtuales de equilibrio de carga, la máquina o máquinas virtuales de aplicación recién lanzadas pueden asociarse con las máquinas virtuales de equilibrio de carga existentes (etapa 518). Si se requiere una máquina virtual de equilibrio de carga adicional, se lanza (etapa 520) y se asocia con la nueva o nuevas máquinas virtuales de aplicación (etapa 522) De forma similar a las máquinas virtuales de cortafuegos, la máquina virtual de equilibrio de carga recién lanzada se puede asociar opcionalmente tanto con las máquinas virtuales de equilibrio de carga existentes como con las máquinas virtuales de aplicaciones existentes.

En algunas realizaciones, puede ser necesario determinar si es posible lanzar máquinas virtuales adicionales en el/los anfitriones antes de lanzar una nueva máquina virtual de cortafuegos en la etapa 510 o una nueva máquina virtual de equilibrio de carga en la etapa 520. En el caso de que no se pueda cumplir con las máquinas virtuales adicionales requeridas, se puede entregar una alarma o notificación correspondiente. El operador del centro de datos puede considerar aumentar la capacidad general del centro de datos o aprovechar recursos adicionales.

La Figura 6 es un diagrama de flujo de llamadas que ilustra otra realización de la presente invención. Para el propósito de este ejemplo, se supondrá que este proceso ocurre en un solo centro de datos. En realizaciones alternativas, los componentes de computación en la nube pueden estar ubicados en múltiples anfitriones en múltiples centros de datos sin apartarse del alcance de la invención. Se proporciona un dispositivo o entidad 600 de administración en la nube en el centro de datos. En algunas realizaciones, la entidad 600 de administración en la nube puede residir físicamente fuera de los centros de datos o estar distribuida entre varios centros de datos. La entidad 600 de administración en la nube se puede implementar como un servidor “blade” dedicado para aprovisionar la administración de configuración en los centros de datos y controlar la capa 650 de virtualización y el hardware físico subyacente. La capa 650 de virtualización actúa como el administrador de la máquina virtual, proporcionando virtualización de hardware que permite que una plataforma operativa virtual administre múltiples o diferentes sistemas operativos y aplicaciones. La virtualización 650 puede comprender uno o más hipervisores. Un cortafuegos 630 de dispositivo de servicio de hardware y un cortafuegos

640 virtual también están previstos en el centro de datos. El cortafuegos 640 virtual se muestra como un solo bloque en la Figura 6, pero puede estar compuesto por varias máquinas virtuales.

La entidad 600 de administración de nube recibe un activador para ejemplificar una nueva máquina virtual para una aplicación virtual (etapa 601). La administración 600 en la nube puede decidir que se requiere una nueva máquina virtual en función de una serie de factores, incluido el ancho de banda de tráfico que es manejada por la aplicación virtual. La administración 600 en la nube solicita una instantánea del tráfico manejado por el cortafuegos 630 de hardware (etapa 602) y el cortafuegos virtual 640 (etapa 604). El cortafuegos 630 de hardware y el cortafuegos virtual 640 devuelven la información solicitada a la administración 600 en la nube (etapas 603 y 605). En la etapa 606, se compara la relación entre el número de máquinas virtuales de cortafuegos y el número de máquinas virtuales de aplicación para determinar si se requieren máquinas virtuales de cortafuegos adicionales. La relación se puede comparar con un parámetro de seguridad predefinido asociado con la aplicación virtual. El parámetro puede definir un umbral o requisito para una cantidad de máquinas virtuales dedicadas a ejecutar la aplicación correspondiente a una cantidad de máquinas virtuales que ejecutan el servicio de cortafuegos asociado con la aplicación. Alternativamente, el parámetro puede definir un requisito de relación de tráfico o ancho de banda entre las máquinas virtuales de aplicación y las máquinas virtuales de cortafuegos.

La administración 600 en la nube ordena a la virtualización 650 que lance una nueva máquina virtual de aplicación (etapa 607). La virtualización 650 ejemplifica la nueva máquina virtual 670 (etapa 608). La ejemplificación satisfactoria de la máquina virtual 670 se le reconoce a la virtualización 650 (etapa 609) y a la administración 600 en la nube (etapa 610).

De acuerdo con la determinación de que la relación de cortafuegos para la aplicación no se satisface en la etapa 606, la administración 600 en la nube ordena a la virtualización 650 que lance una nueva máquina virtual de cortafuegos (etapa 611). La virtualización 650 ejemplifica la nueva máquina virtual 680 de cortafuegos (etapa 612). La ejemplificación satisfactoria de la máquina virtual 680 de cortafuegos se le reconoce a la virtualización 650 (etapa 613) y a la administración 600 en la nube (etapa 614).

Tras la ejemplificación satisfactoria de la nueva máquina virtual 670 de aplicación y de la nueva máquina virtual 680 de cortafuegos, la administración 600 en la nube puede ordenar a la virtualización 650 que asocie el cortafuegos virtual 680 con la máquina virtual 670 (etapa 615). La virtualización 650 envía instrucciones de configuración (etapas 616 y 618) a la máquina virtual 670 y al cortafuegos virtual 680 respectivamente. La configuración y asociación satisfactorias se reconocen en la virtualización 650 (etapas 617 y 619) y la virtualización 650, a su vez, reconoce el éxito de la administración 600 en la nube (etapa 620).

En algunas realizaciones, las etapas 606-620 se pueden repetir para otros servicios hechos virtuales, como el equilibrio de carga. Como se expuso con respecto a la Figura 5, se puede verificar una relación de equilibrio de carga entre el número de máquinas virtuales que ejecutan servicios de equilibrio de carga y el número de máquinas virtuales que ejecutan la aplicación para determinar si se requiere un número incrementado de máquinas virtuales de equilibrio de carga.

Los expertos en la técnica apreciarán que el orden de las etapas mostradas en la Figura 6 no es esencial para cada realización de la presente invención. Por ejemplo, la entidad 600 de administración en la nube puede optar por lanzar el cortafuegos virtual 680 adicional (etapas 611-614) antes de lanzar la máquina virtual 670 de aplicación adicional (etapas 607-610) sin afectar al alcance de la invención.

La Figura 7 es un diagrama de flujo de un método de acuerdo con una o más realizaciones de la presente invención. El proceso comienza en el bloque 700 determinando que una aplicación virtualizada, asociada con una primera pluralidad de máquinas virtuales de aplicación y una segunda pluralidad de máquinas virtuales de cortafuegos, requiere un número incrementado de máquinas virtuales de aplicación en la primera pluralidad. Esta determinación puede hacerse de acuerdo con un aumento en el tráfico asociado con la aplicación virtualizada o cualquier otro número de factores. La aplicación virtualizada se puede alojar en la primera pluralidad de máquinas virtuales de aplicación. La segunda pluralidad de máquinas virtuales de cortafuegos puede proporcionar servicios de cortafuegos para el tráfico asociado con la aplicación virtualizada.

En el bloque 710, opcionalmente, se detecta que un umbral de relación de cortafuegos asociado con la aplicación virtualizada es superado por el número incrementado de máquinas virtuales de aplicación que se determina que se requieren en el bloque 700. La relación de cortafuegos puede ser un requisito de perfil de seguridad predefinido asociado con la aplicación virtualizada. El perfil de seguridad de la aplicación se puede configurar en el despliegue de la aplicación virtualizada.

En algunas realizaciones, la detección del bloque 710 se realiza de acuerdo con la comparación del número incrementado requerido de máquinas virtuales de aplicación en la primera pluralidad con el número de máquinas virtuales de cortafuegos en la segunda pluralidad. El número total de máquinas virtuales de aplicación que se determina que requiere la aplicación virtualizada puede compararse con el número de máquinas virtuales de cortafuegos actualmente en la segunda pluralidad para determinar si se supera un umbral de relación de cortafuegos. Si se excede la relación de cortafuegos, se necesita un número incrementado de máquinas virtuales de cortafuegos.

En otras realizaciones, la detección del bloque 710 se realiza de acuerdo con la comparación de la capacidad de ancho

de banda del número incrementado de máquinas virtuales de aplicación con la capacidad de ancho de banda de las máquinas virtuales de cortafuegos en la segunda pluralidad. La capacidad de ancho de banda de la cantidad incrementada de máquinas virtuales de aplicación puede ser una suma de cada una de las capacidades de la cantidad requerida de máquinas virtuales de aplicación. La capacidad de ancho de banda de las máquinas virtuales de cortafuegos puede ser una suma de las capacidades de las máquinas virtuales de cortafuegos actualmente en la segunda pluralidad. Las capacidades de ancho de banda respectivas se pueden comparar para determinar si se supera el umbral de la relación de cortafuegos. Opcionalmente, también se puede considerar el ancho de banda de un cortafuegos de hardware que se ha aprovisionado para su uso con la aplicación virtualizada. Se puede comparar una suma de la capacidad de ancho de banda aprovisionada del cortafuegos de hardware y la capacidad de ancho de banda de la pluralidad de máquinas virtuales de cortafuegos con la capacidad de ancho de banda total del número incrementado requerido de máquinas virtuales de aplicación para determinar si se supera un umbral de relación de cortafuegos. Si se supera la relación del cortafuegos, se necesita un número incrementado de máquinas virtuales de cortafuegos.

En el bloque 720, se determina que se requiere un número incrementado de máquinas virtuales de cortafuegos por el número incrementado de máquinas virtuales de aplicación. La determinación de que la aplicación virtualizada requiere al menos una máquina virtual de cortafuegos adicional se puede determinar de acuerdo con la detección de que se ha superado una relación de cortafuegos (en el bloque 710). Alternativamente, la determinación de que la aplicación virtualizada requiere al menos una máquina virtual de cortafuegos adicional puede determinarse en respuesta a la determinación de que se requiere un número incrementado de máquinas virtuales de aplicación (en el bloque 700).

En el bloque 730, se ejemplifica una máquina virtual de aplicación adicional. La máquina virtual de aplicación ejemplificada se puede añadir a la primera pluralidad de máquinas virtuales de aplicación. La máquina virtual de aplicación adicional ejemplificada puede requerir estar conectada o asociada con la primera pluralidad inicial de máquinas virtuales de aplicación a través de su proceso de configuración.

En el bloque 740, se ejemplifica una máquina virtual de cortafuegos adicional. La máquina virtual de cortafuegos ejemplificada se puede añadir a la segunda pluralidad de máquinas virtuales de cortafuegos. La máquina virtual de cortafuegos adicional ejemplificada puede requerir estar conectada o asociada con la segunda pluralidad inicial de máquinas virtuales de cortafuegos a través de su proceso de configuración.

En una realización alternativa, puede determinarse que se requiere un número incrementado de máquinas virtuales de equilibrio de carga por el número incrementado de máquinas virtuales de aplicación. De manera similar a la exposición relacionada con la relación de cortafuegos, un perfil de seguridad asociado con la aplicación virtualizada puede definir un requisito de relación para la cantidad de máquinas virtuales de equilibrio de carga en comparación con las máquinas virtuales de aplicación. Esta relación se puede verificar en respuesta a la determinación de que se requiere un número incrementado de máquinas virtuales de aplicación. En consecuencia, se puede ejemplificar una máquina virtual de equilibrio de carga.

En otra realización alternativa, se puede determinar que la aplicación virtualizada requiere un número reducido de máquinas virtuales de aplicación en la primera pluralidad. De acuerdo con la verificación de la relación de cortafuegos, se puede determinar que se requiere un número reducido de máquinas virtuales de cortafuegos por el número reducido de máquinas virtuales de aplicación. Una máquina virtual de aplicación y una máquina virtual de cortafuegos se pueden apagar según sea necesario.

Como será evidente para un experto en la técnica, en algunas realizaciones, el orden de etapas en la Figura 7 puede modificarse sin apartarse del alcance previsto de la presente invención. Por ejemplo, se puede ejemplificar una máquina virtual adicional (bloque 730) antes de verificar la relación de cortafuegos o determinar que se requiere un número incrementado de máquinas virtuales de cortafuegos. La determinación del bloque 720, de que se requiere un número incrementado de máquinas virtuales de cortafuegos, se desencadena por la determinación de que la aplicación virtual requiere un número incrementado de máquinas virtuales de aplicación y puede realizarse antes o después del lanzamiento de cualquier máquina o máquinas virtuales adicionales. De modo similar, la relación del cortafuegos se puede verificar utilizando el número incrementado requerido de máquinas virtuales de aplicación, se el número incrementado se ha lanzado o no.

La Figura 8 es un diagrama de bloques que ilustra detalles funcionales asociados con un ejemplo de entidad de administración en la nube o dispositivo 800. El dispositivo 800 de administración en la nube puede incluir un motor 810 de procesamiento, una memoria 820 y una interfaz 830 de comunicación. El dispositivo 800 de administración en la nube puede implementarse utilizando hardware subyacente dedicado o, alternativamente, puede implementarse por sí mismo, como una máquina virtual en un centro de datos. El dispositivo 800 de administración en la nube puede realizar las distintas realizaciones, como se describe en la presente memoria descriptiva, relacionadas con la administración de aplicaciones virtuales y sus servicios virtuales asociados. El dispositivo 800 de administración en la nube puede realizar estas operaciones en respuesta a un motor 810 de procesamiento que ejecuta instrucciones almacenadas en un depósito de datos tal como la memoria 820. Las instrucciones pueden ser instrucciones de software y el depósito de datos puede ser cualquier medio lógico o físico legible por ordenador. El dispositivo 800 de administración en la nube, aunque se muestra en la Figura 8 como una sola entidad, puede implementarse mediante varios dispositivos diferentes que están distribuidos geográficamente, como se expuso anteriormente.

El motor 810 de procesamiento determina que una aplicación virtualizada, asociada con una primera pluralidad de máquinas virtuales de aplicación y una segunda pluralidad de máquinas virtuales de cortafuegos, requiere un número incrementado de máquinas virtuales de aplicación en la primera pluralidad. En respuesta a la determinación del número incrementado requerido de máquinas virtuales de aplicación, el motor 810 de procesamiento determina que la aplicación virtualizada también requiere un número incrementado de máquinas virtuales de cortafuegos. Por consiguiente, el motor 810 de procesamiento ejemplifica una nueva máquina virtual de aplicación y una nueva máquina virtual de cortafuegos.

El motor 810 de procesamiento puede determinar que la aplicación virtualizada requiere un número incrementado de máquinas virtuales de cortafuegos en respuesta a la detección de que se supera un umbral de relación de cortafuegos. El umbral de relación de cortafuegos puede ser un requisito de seguridad, asociado con la aplicación virtualizada, que define la cantidad de máquinas virtuales de cortafuegos requeridas por máquina virtual de aplicación. Alternativamente, el umbral de relación de cortafuegos puede definir un requisito de capacidad de ancho de banda para las máquinas virtuales de cortafuegos en comparación con la capacidad de ancho de banda del número incrementado de máquinas virtuales de aplicación. Opcionalmente, también se puede considerar una capacidad de ancho de banda de un cortafuegos de hardware aprovisionado para su uso por la aplicación virtualizada al verificar el umbral de la relación del cortafuegos.

La interfaz 830 de comunicación se puede usar para comunicarse con la primera pluralidad de máquinas virtuales de aplicación y la segunda pluralidad de máquinas virtuales de cortafuegos, o con su hipervisor o hipervisores asociados. El motor 810 de procesamiento puede emitir y recibir instrucciones a través de la interfaz 830 de comunicación. El dispositivo 800 de administración en la nube es capaz de comunicarse con las diversas entidades, tanto físicas como virtuales, en el entorno de la computación en la nube.

Las realizaciones descritas en este documento se han dirigido a servicios virtuales tales como cortafuegos y servicios de equilibrio de carga. Los expertos en la técnica apreciarán que los mecanismos presentados en este documento pueden aplicarse a cualquier servicio que se ejecute en máquinas virtuales. Los ejemplos de otros servicios virtuales incluyen un servicio de Seguridad de Protocolo de Internet (IPSec), un servicio de Red Privada Virtual (VPN), un servicio de equilibrio de carga, un sistema de detección y prevención de intrusiones (IDS/IPS) o un servicio de Administración Unificada de Amenazas (UTM) .

El mecanismo de cortafuegos híbrido de la presente invención desacopla la porción de hardware de la porción de software para una mayor flexibilidad y escalabilidad. Este enfoque disocia la tecnología de unidad de procesamiento central (CPU) general que cambia rápidamente de la de hardware especializado. A medida que los servidores “blade” del centro de datos se actualizan con el tiempo a la última tecnología, este enfoque permite al administrador del centro de datos cambiar las relaciones de cortafuegos de las aplicaciones virtuales para acomodar las actualizaciones. No es necesario actualizar el cortafuegos de hardware especializado, ya que los cortafuegos virtuales mejorarán tanto como las máquinas virtuales utilizadas para las aplicaciones virtuales.

Las realizaciones de la invención pueden representarse como un producto de software almacenado en un medio legible por máquina (también denominado medio legible por ordenador, medio legible por procesador o un medio utilizable por ordenador que tiene un código de programa legible por ordenador incorporado en él). El medio legible por máquina puede ser cualquier medio tangible adecuado, incluido un medio de almacenamiento magnético, óptico o eléctrico, incluido un disquete, un disco compacto de memoria de solo lectura (CD-ROM), un disco versátil digital de memoria solo de lectura (DVD-ROM) (volátil o no volátil), o mecanismo de almacenamiento similar. El medio legible por máquina puede contener varios conjuntos de instrucciones, secuencias de códigos, información de configuración u otros datos que, cuando se ejecutan, hacen que un procesador realice etapas en un método de acuerdo con una realización de la invención. Los expertos en la técnica apreciarán que otras instrucciones y operaciones necesarias para implementar la invención descrita también pueden almacenarse en el medio legible por máquina. El software que se ejecuta desde el medio legible por máquina puede interactuar con los circuitos para realizar las tareas descritas.

Las realizaciones de la presente invención descritas anteriormente pretenden ser solo ejemplos. Los expertos en la técnica pueden realizar alteraciones, modificaciones y variaciones a las realizaciones particulares sin apartarse del alcance de la invención, que se define únicamente por las reivindicaciones adjuntas.

REIVINDICACIONES

1. Un método para gestionar los requisitos de cortafuegos relacionados con una aplicación virtualizada por una entidad (600; 800) de administración en la nube que tiene un motor (810) de procesamiento, que comprende:

- determinar (700), por el motor (810) de procesamiento, que una aplicación virtualizada, asociada con una primera pluralidad de máquinas virtuales (406a; 406b) de aplicación y una segunda pluralidad de máquinas virtuales (402a; 402b) de cortafuegos, requiere un número incrementado de máquinas virtuales de aplicación en la primera pluralidad;

- determinar (720) mediante el motor (810) de procesamiento, que se requiere un número incrementado de máquinas virtuales de cortafuegos por el número incrementado de máquinas virtuales de aplicación;

- ejemplificar (730) una máquina virtual de aplicación; y

- ejemplificar (740) una máquina virtual de cortafuegos,

en donde el número incrementado requerido de máquinas virtuales de cortafuegos es determinado de acuerdo con la detección (710) de que se ha superado un umbral de relación de cortafuegos asociado con la aplicación virtualizada por el número incrementado de máquinas virtuales de aplicación, en donde la detección de que se ha superado el umbral de relación de cortafuegos se realiza de acuerdo con la comparación de una capacidad de ancho de banda del número incrementado requerido de máquinas virtuales de aplicación en la primera pluralidad con una suma de una capacidad de ancho de banda de las máquinas virtuales de cortafuegos en la segunda pluralidad y un ancho de banda de un cortafuegos de hardware aprovisionado para usar por la aplicación virtualizada.

2. El método de la reivindicación 1, en el que el umbral de la relación de cortafuegos se incluye en un perfil de aplicación configurado en el despliegue de la aplicación virtualizada.

3. El método de la reivindicación 1, que incluye además la etapa de comparar el número incrementado requerido de máquinas virtuales de aplicación con el número de máquinas virtuales de cortafuegos en la segunda pluralidad.

4. El método de la reivindicación 1, que incluye además las etapas de:

calcular una relación del número incrementado requerido de máquinas virtuales de aplicación al número de máquinas virtuales de cortafuegos en la segunda pluralidad; y

comparar la relación calculada con un requisito de relación de cortafuegos asociado con la aplicación virtualizada.

5. El método de la reivindicación 1, en donde la aplicación virtualizada está alojada en la primera pluralidad de máquinas virtuales (406a; 406b) de aplicación y la segunda pluralidad de máquinas virtuales (402a; 402b) de cortafuegos proporciona servicios de cortafuegos para el tráfico asociado con la aplicación virtualizada.

6. El método de la reivindicación 1, incluyendo además las etapas de añadir la máquina virtual de aplicación ejemplificada a la primera pluralidad; y añadir la máquina virtual de cortafuegos ejemplificada a la segunda pluralidad.

7. El método de la reivindicación 1, que incluye además las etapas de:

- determinar que se requiere un número incrementado de máquinas virtuales de equilibrio de carga por el número incrementado de máquinas virtuales de aplicación; y

- ejemplificar una máquina virtual de equilibrio de carga.

8. El método de la reivindicación 1, que incluye además las etapas de:

- determinar que la aplicación virtualizada requiere un número reducido de máquinas virtuales de aplicación en la primera pluralidad;

- determinar que se requiere un número reducido de máquinas virtuales de aplicación por el número reducido de máquinas virtuales de aplicación;

- apagar una máquina virtual de aplicación; y

- apagar una máquina virtual de cortafuegos.

9. Una entidad (600; 800) de administración en la nube, que comprende:

- una memoria (820) para almacenar instrucciones; y

- un motor (810) de procesamiento, configurado para ejecutar las instrucciones, para determinar (700) que una aplicación virtualizada, asociada con una primera pluralidad de máquinas virtuales (406a; 406b) de aplicación y una segunda pluralidad de máquinas virtuales (402a; 402b) de cortafuegos, requiere un número incrementado de máquinas virtuales

de aplicación en la primera pluralidad; para determinar (720) que un número incrementado de máquinas virtuales de cortafuegos es requerido por el número incrementado de máquinas virtuales de aplicación para ejemplificar (730) una máquina virtual de aplicación; y para ejemplificar (740) una máquina virtual de cortafuegos,

en donde la determinación de se requiere el número incrementado de máquinas virtuales de cortafuegos es en respuesta a la detección (710) de que se supera un umbral de relación de cortafuegos asociado con la aplicación virtualizada, en donde la detección de que se ha superado el umbral de relación de cortafuegos se realiza de acuerdo con la comparación de una capacidad de ancho de banda del número incrementado requerido de máquinas virtuales de aplicación en la primera pluralidad con una suma de una capacidad de ancho de banda de las máquinas virtuales de cortafuegos en la segunda pluralidad y una capacidad de ancho de banda de un cortafuegos de hardware aprovisionado para utilizar por la aplicación virtualizada.

10. La entidad de administración en la nube de la reivindicación 9, que comprende además una interfaz de comunicación para comunicarse con la primera pluralidad de máquinas virtuales de aplicación y la segunda pluralidad de máquinas virtuales de cortafuegos.

11. La entidad (600; 800) de administración en la nube de la reivindicación 9, en donde el umbral de la relación de cortafuegos se incluye en un perfil de aplicación configurado en el despliegue de la aplicación virtualizada por el motor (810) de procesamiento.

12. La entidad (600; 800) de administración en la nube de la reivindicación 9, en donde el motor (810) de procesamiento compara el número incrementado requerido de máquinas virtuales de aplicación en la primera pluralidad con el número de máquinas virtuales de cortafuegos en la segunda pluralidad.

13. La entidad (600; 800) de administración en la nube de la reivindicación 9, en donde el motor (810) de procesamiento calcula una relación del número incrementado requerido de máquinas virtuales de aplicación en la primera pluralidad al número de máquinas virtuales de cortafuegos en la segunda pluralidad; y compara la relación calculada con un umbral de relación de cortafuegos asociado con la aplicación virtualizada.

14. La entidad (600; 800) de administración en la nube de la reivindicación 9, en donde la aplicación virtualizada está alojada en la primera pluralidad de máquinas virtuales (406a; 406b) de aplicación y la segunda pluralidad de máquinas virtuales (402a; 402b) de cortafuegos proporciona servicios de cortafuegos para el tráfico asociado con la aplicación virtualizada.

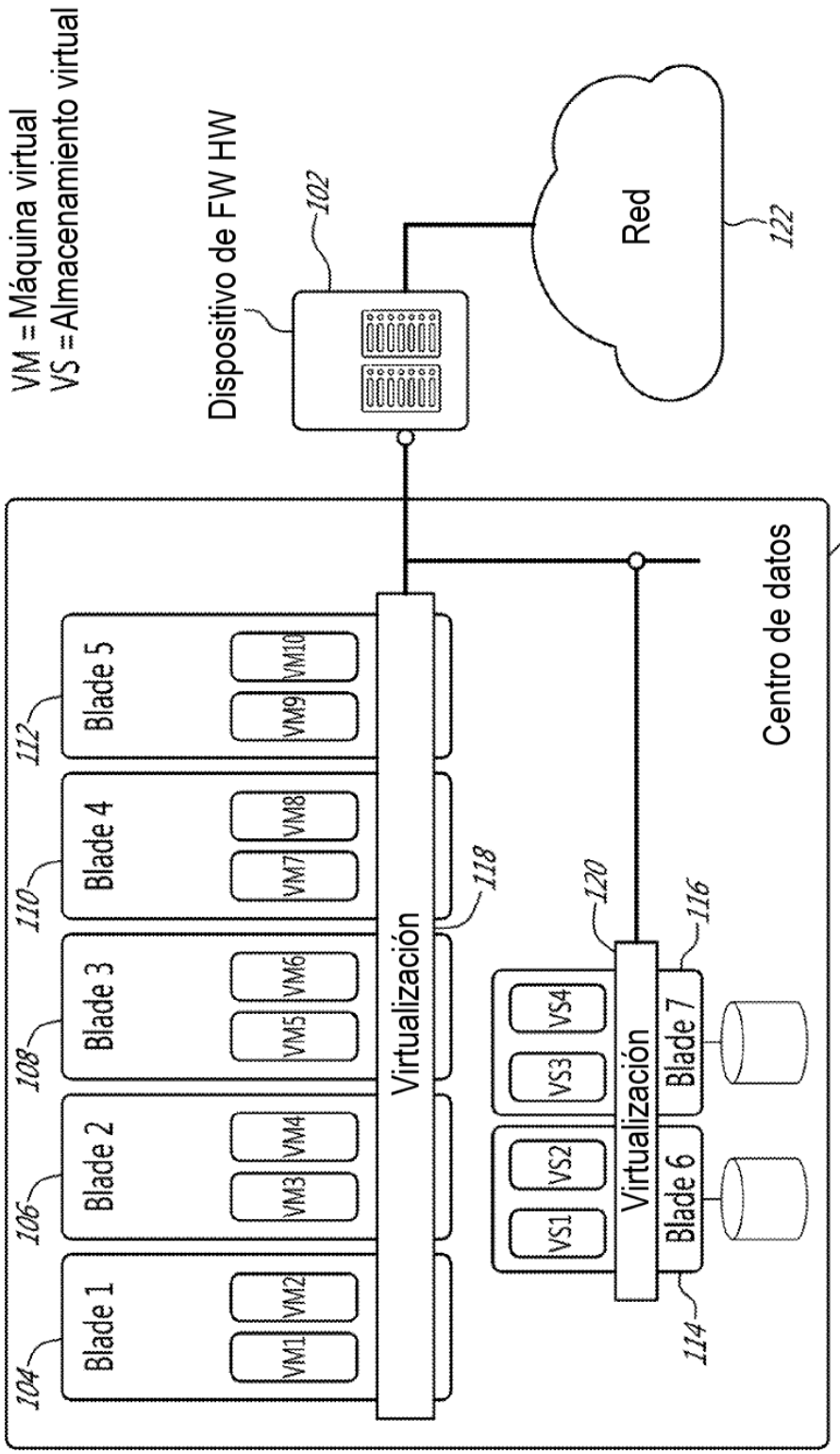

Fig. 1 (Técnica Anterior)

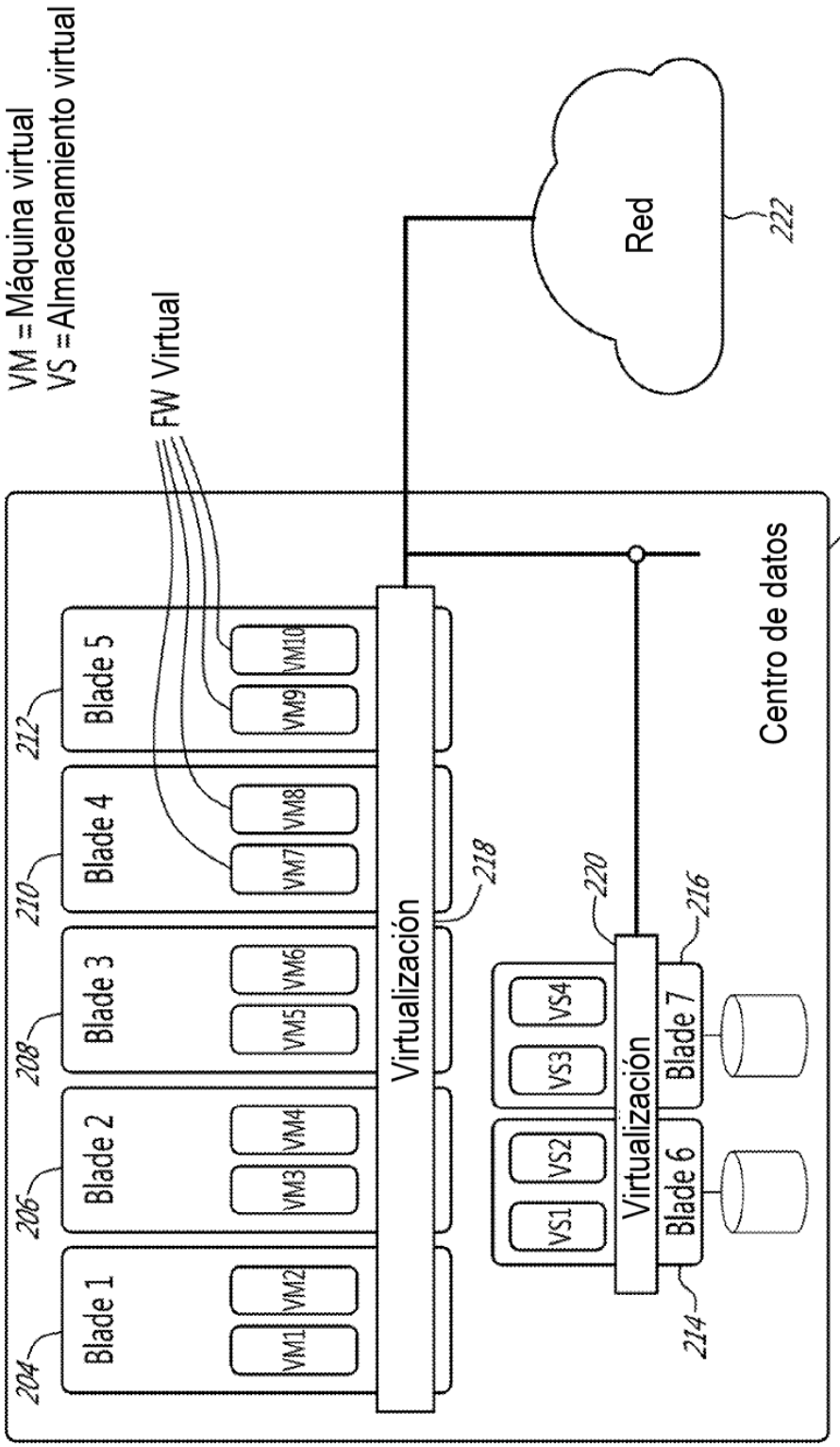

FIG. 2 (Técnica Anterior)

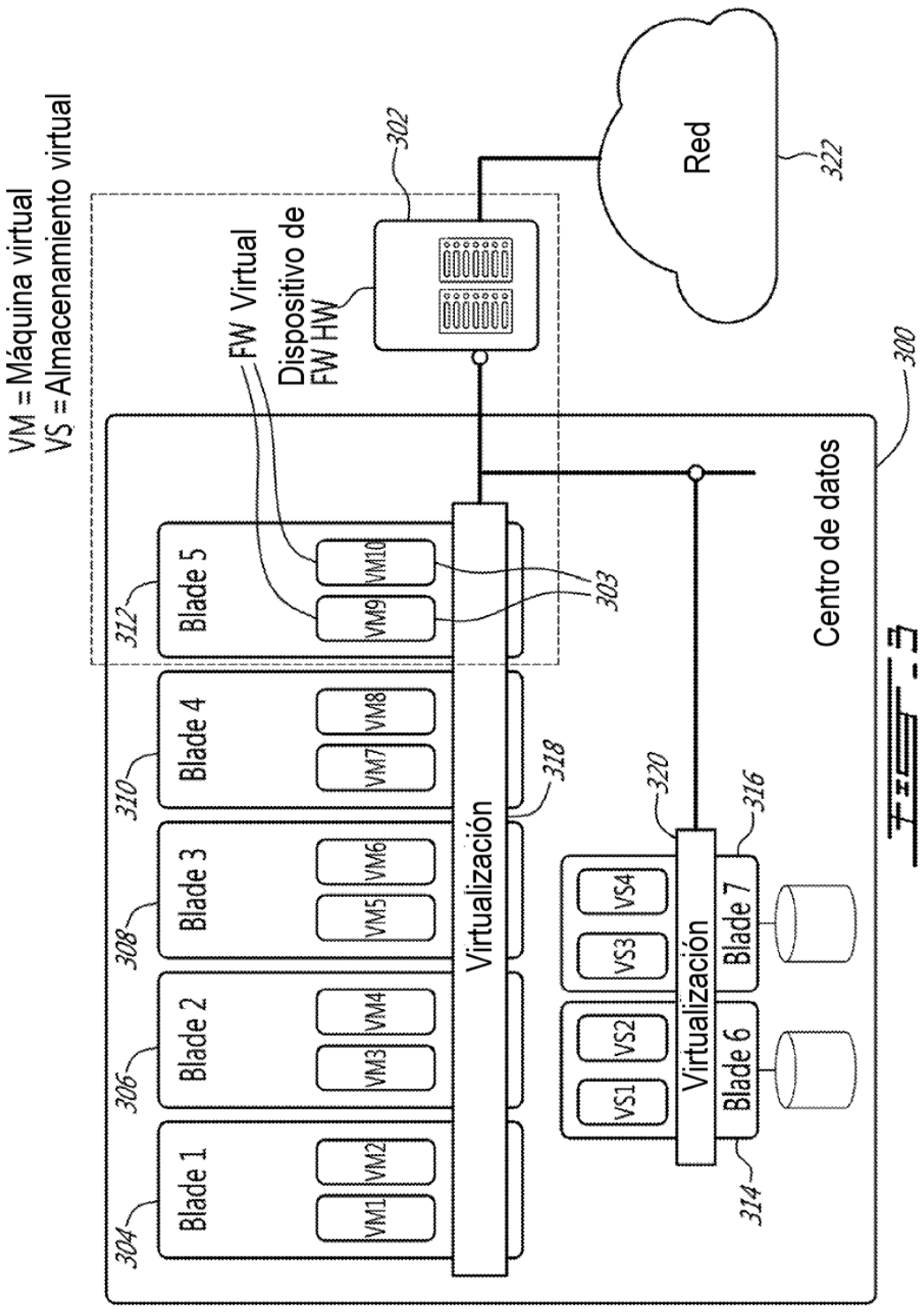
VM = Máquina virtual
VS = Almacenamiento virtual
Red
322
302
FW Virtual
Dispositivo de FW HW
300
Centro de datos
312
Blade 5
VM9
VM10
303
310
Blade 4
VM7
VM8
308
Blade 3
VM5
VM6
306
Blade 2
VM3
VM4
304
Blade 1
VM1
VM2
318
Virtualización
320
VS1
VS2
VS3
VS4
316
Blade 7
Virtualización
Blade 6
314

Fig. 3

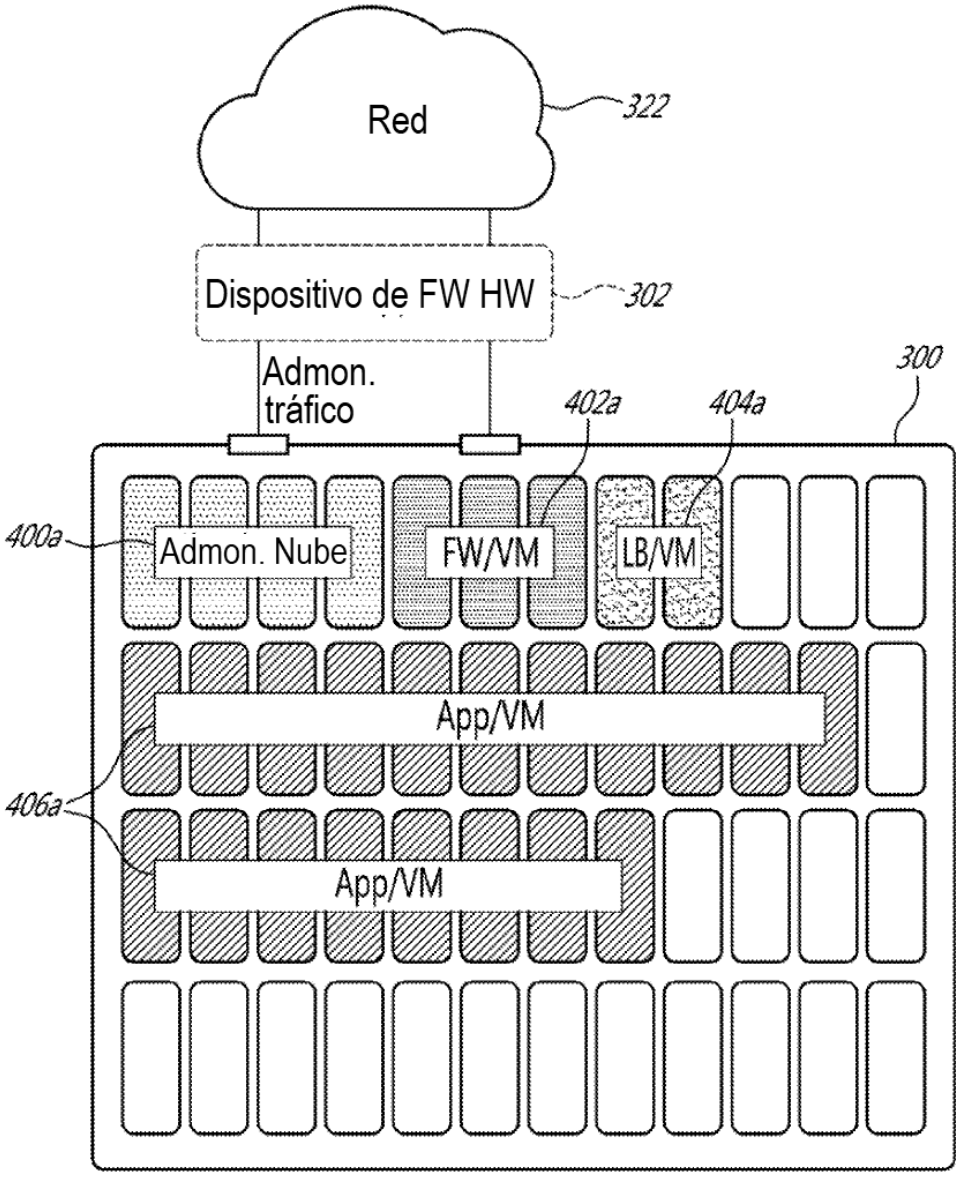
Red
322
Dispositivo de FW HW
302
Admon.
tráfico
300
402a
404a
400a
Admon. Nube
FW/VM
LB/VM
App/VM
406a
App/VM

Fig. 4a

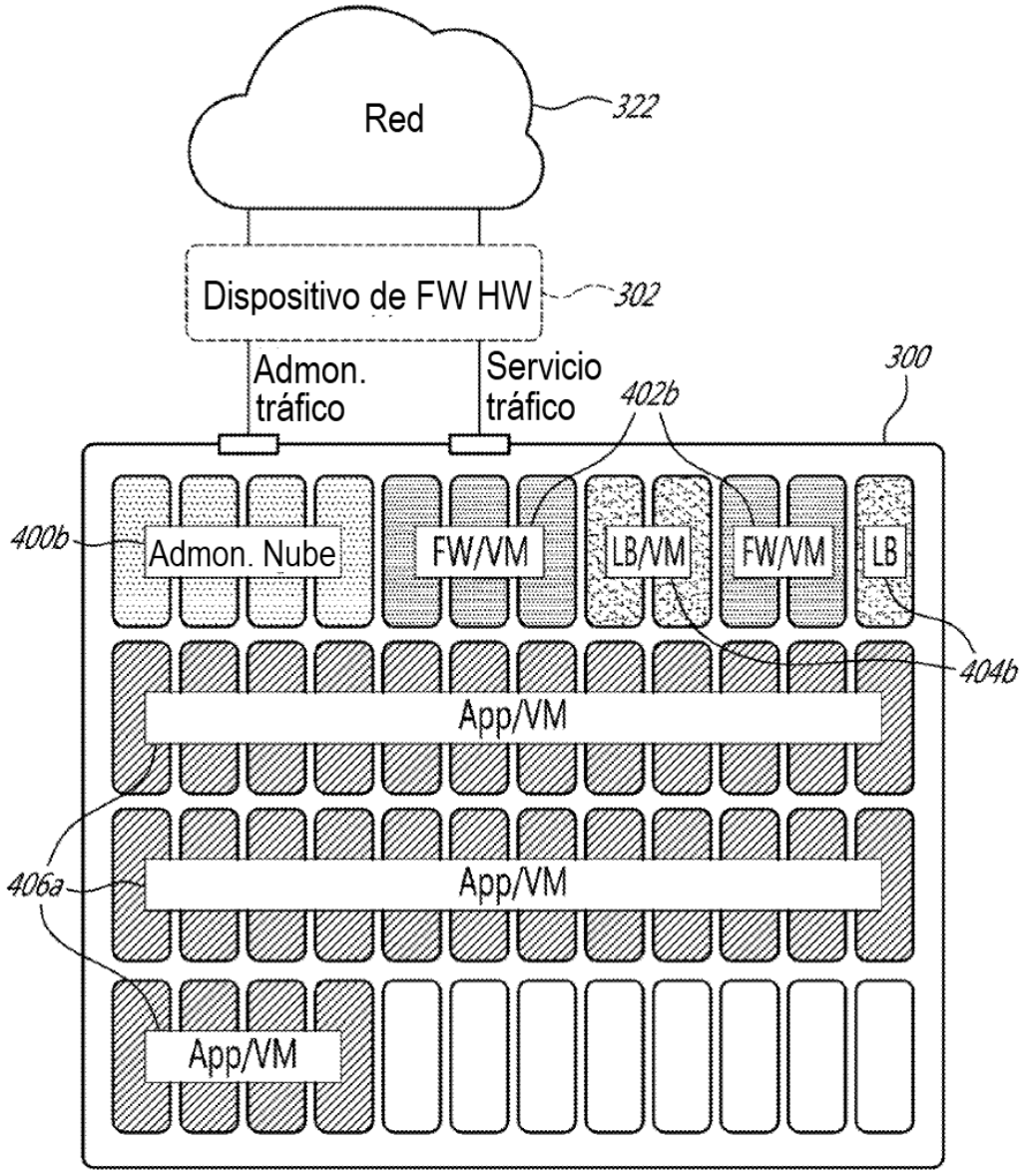
Red
322
Dispositivo de FW HW
302
Admon. tráfico
Servicio tráfico
300
402b
400b
Admon. Nube
FW/VM
LB/VM
FW/VM
LB
404b
App/VM
406a
App/VM
App/VM

Fig. 4b

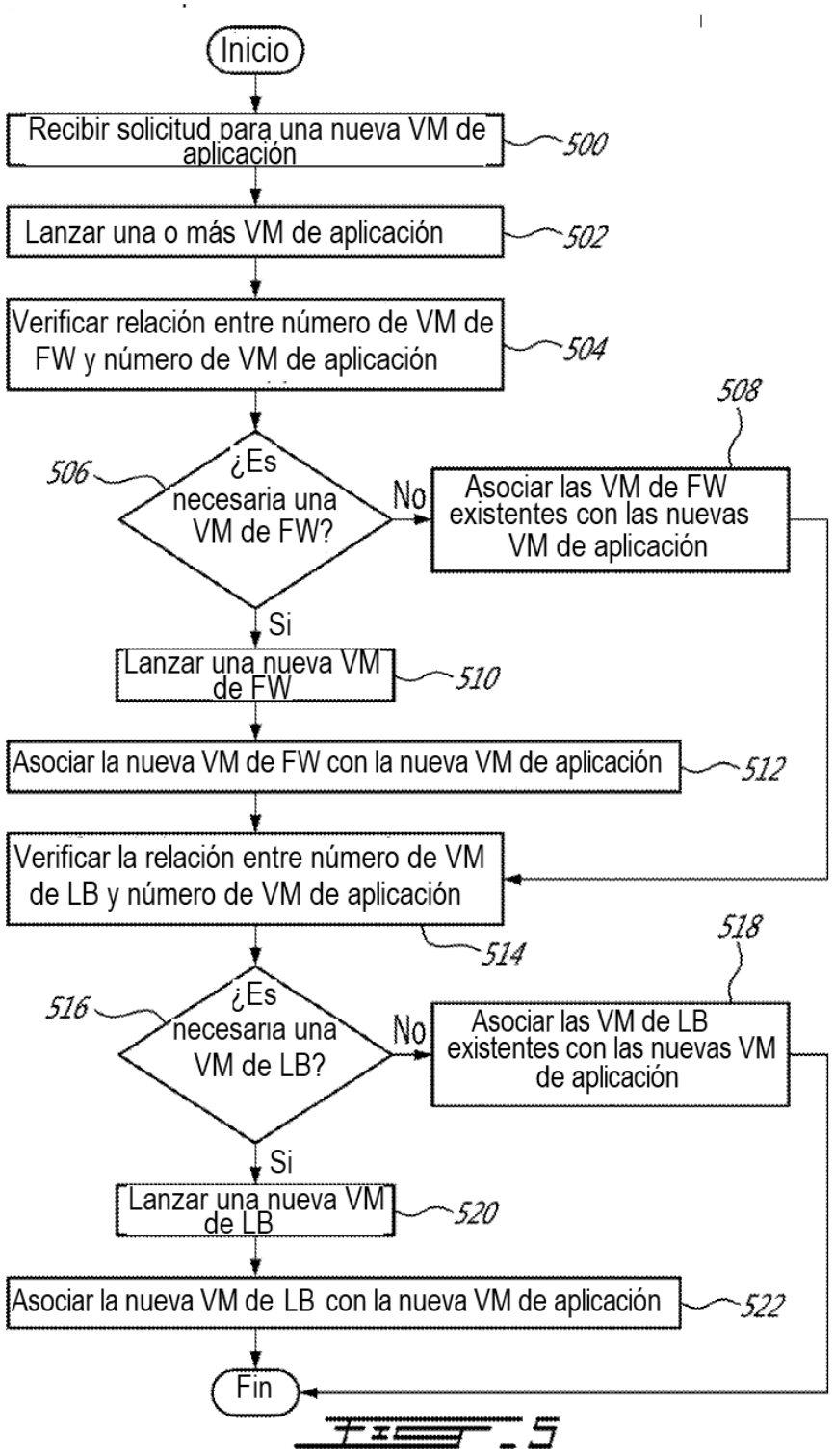
Inicio
Recibir solicitud para una nueva VM de aplicación
500
Lanzar una o más VM de aplicación
502
Verificar relación entre número de VM de FW y número de VM de aplicación
504
506
¿Es necesaria una VM de FW?
No
508
Asociar las VM de FW existentes con las nuevas VM de aplicación
Si
Lanzar una nueva VM de FW
510
Asociar la nueva VM de FW con la nueva VM de aplicación
512
Verificar la relación entre número de VM de LB y número de VM de aplicación
514
516
¿Es necesaria una VM de LB?
No
518
Asociar las VM de LB existentes con las nuevas VM de aplicación
Si
Lanzar una nueva VM de LB
520
Asociar la nueva VM de LB con la nueva VM de aplicación
522
Fin

Fig. 5

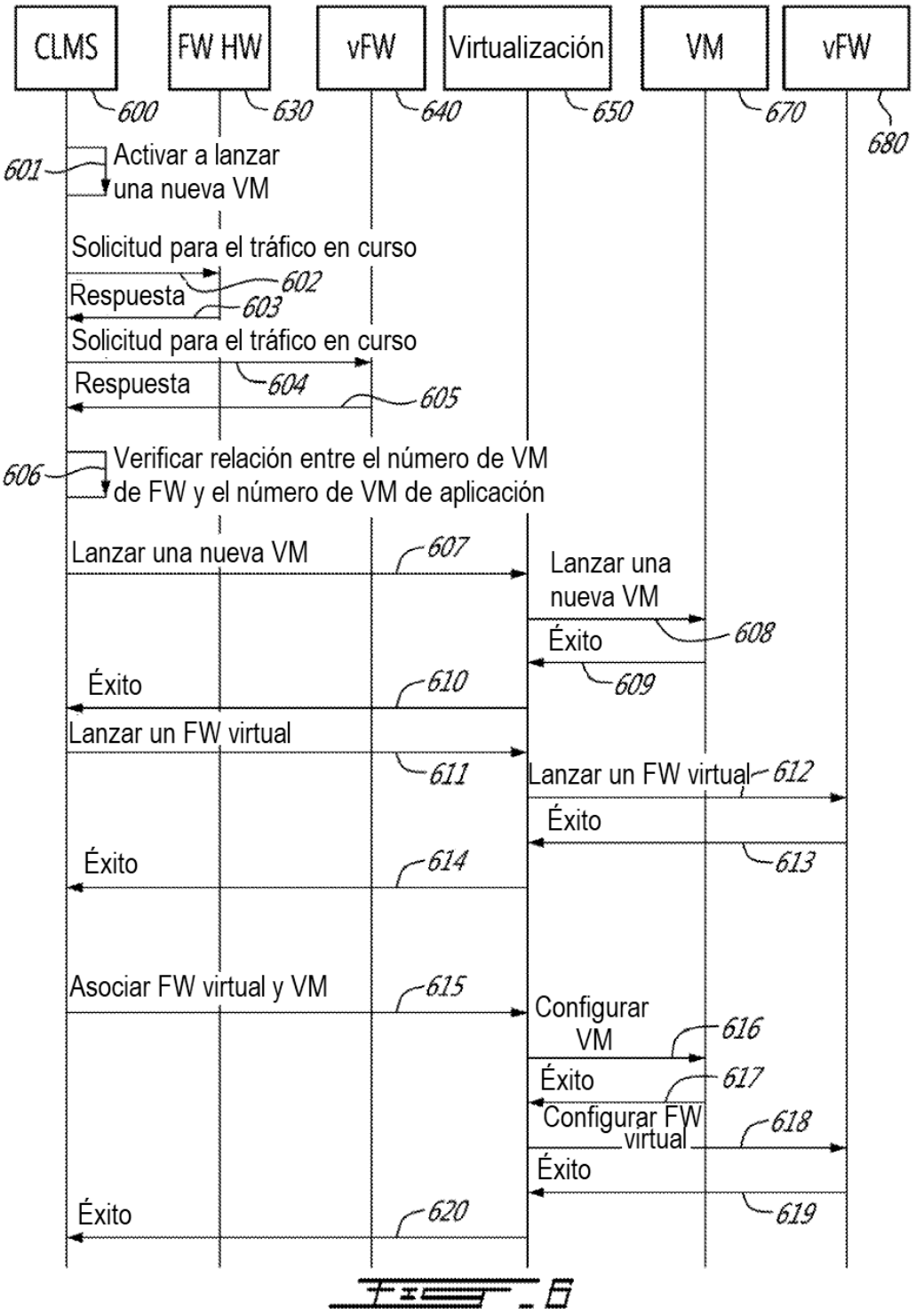
CLMS
FW HW
vFW
Virtualización
VM
vFW
600
630
640
650
670
680
601
Activar a lanzar una nueva VM
Solicitud para el tráfico en curso
602
Respuesta
603
Solicitud para el tráfico en curso
604
Respuesta
605
606
Verificar relación entre el número de VM de FW y el número de VM de aplicación
Lanzar una nueva VM
607
Lanzar una nueva VM
608
Éxito
609
Éxito
610
Lanzar un FW virtual
611
Lanzar un FW virtual
612
Éxito
613
Éxito
614
Asociar FW virtual y VM
615
Configurar VM
616
Éxito
617
Configurar FW virtual
618
Éxito
619
Éxito
620

Fig. 6

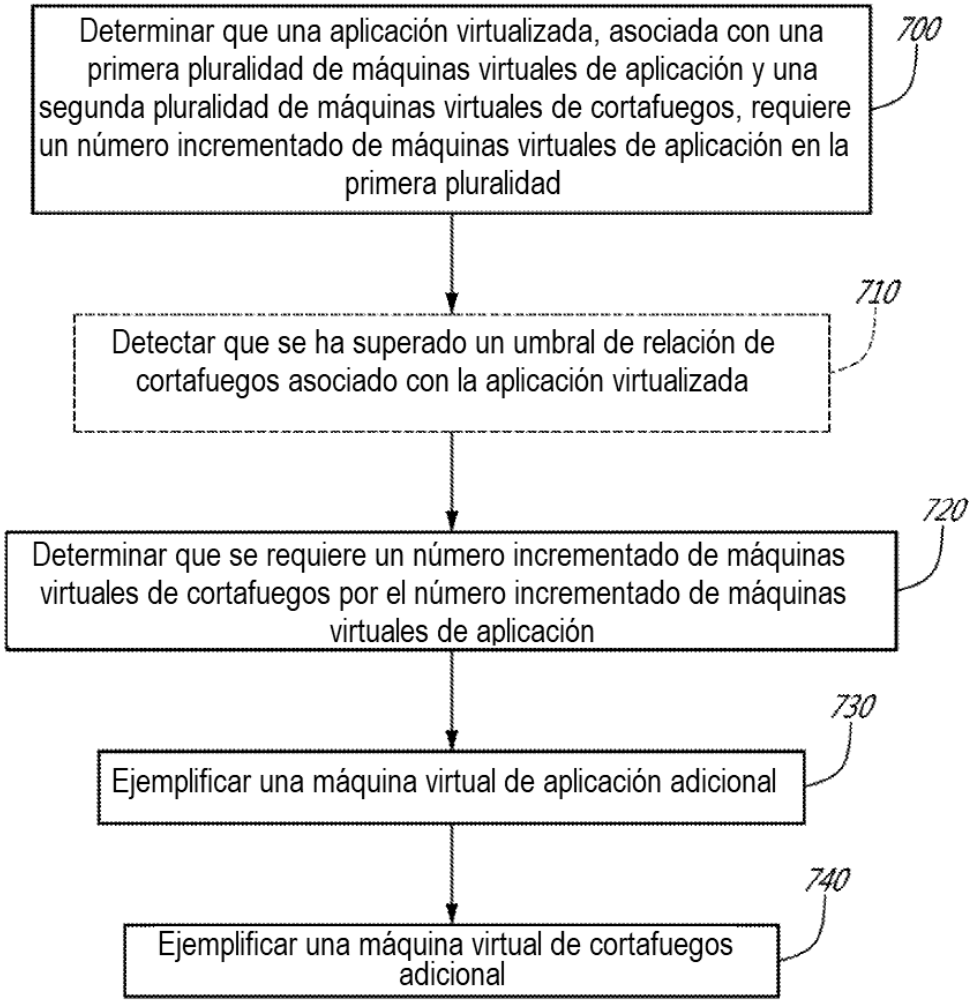
Determinar que una aplicación virtualizada, asociada con una primera pluralidad de máquinas virtuales de aplicación y una segunda pluralidad de máquinas virtuales de cortafuegos, requiere un número incrementado de máquinas virtuales de aplicación en la primera pluralidad
700
Detectar que se ha superado un umbral de relación de cortafuegos asociado con la aplicación virtualizada
710
Determinar que se requiere un número incrementado de máquinas virtuales de cortafuegos por el número incrementado de máquinas virtuales de aplicación
720
Ejemplificar una máquina virtual de aplicación adicional
730
Ejemplificar una máquina virtual de cortafuegos adicional
740

Fig. 7

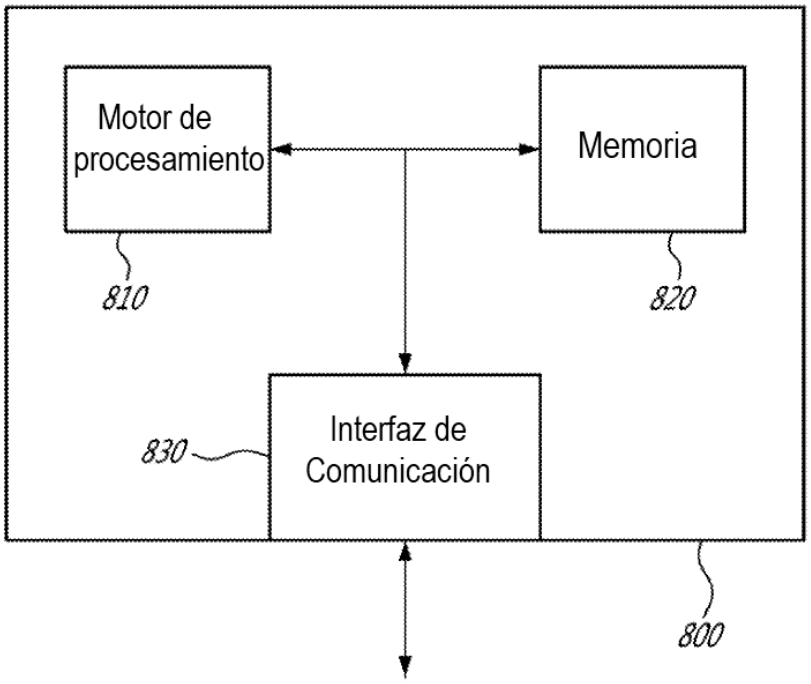
Motor de procesamiento
Memoria
810
820
830
Interfaz de Comunicación
800

Fig. 8