(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 764 783**

(51) Int. CI.:

G06F 21/53 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **02.12.2009 PCT/EP2009/066256**

(87) Fecha y número de publicación internacional: **10.06.2010 WO10063768**

(96) Fecha de presentación y número de la solicitud europea: **02.12.2009 E 09760915 (0)**

(97) Fecha y número de publicación de la concesión europea: **16.10.2019 EP 2359302**

(54) Título: **Equipo de seguridad**

(30) Prioridad:

05.12.2008 FR 0806839

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
04.06.2020

(73) Titular/es:

THALES (100.0%)
Tour Carpe Diem - Place des Corolles, Esplanade Nord
92400 Courbevoie, FR

(72) Inventor/es:

MAXIMILIEN, BENOÎT;
FREREBEAU, LAURENT;
WEBER, ERIC y
LACROIX, JEAN-MARC

(74) Agente/Representante:

CARPINTERO LÓPEZ, Mario

DESCRIPCIÓN

Equipo de seguridad

La invención se sitúa en el campo de la seguridad de los sistemas de información. Se refiere al diseño de equipos de seguridad, teniendo en cuenta sus limitaciones específicas (tipo y calidad del aislamiento, control de los flujos, ...) por medio de una capa de virtualización. El sistema según la invención está destinado a estar dispuesto entre dominios que tienen diferentes niveles de sensibilidad entre sí.

La invención se aplica, por ejemplo, a la compartimentación de tratamientos sensibles, al control de flujo de datos intercambiados entre dominios de diferentes niveles de seguridad, y a la restricción de acceso a recursos sensibles, tales como un componente criptográfico, un medio de comunicación, un dispositivo de almacenamiento, etc.

El diseño de equipos asegurados necesita separar la información de diferentes niveles de sensibilidad y evitar que puedan mezclarse o modificarse, o que su tratamiento esté afectado.

Esta información puede ser privada o pública, roja o negra, sensible o compartida, sin cifrar o cifrada.
La separación de estos datos necesita una separación de los tratamientos que los manipulan, así como espacios de almacenamiento (persistentes, volátiles, temporales, ...) que los contienen. La tarea resulta difícil si se considera que los medios usados para soportar estos tratamientos (procesadores, memorias, ...) son sistemas físicos que 1) tienen efectos de borde en su entorno (radiación electromagnética, consumo eléctrico, ...), 2) tienen características intrínsecas (memorias cachés, elementos de predicción de tratamiento, ...) susceptibles de mantener información sensible entre dos tratamientos y, 3) usan materiales que pueden presentar una cierta remanencia de la información después de un apagado.

En el campo de la seguridad, la técnica anterior propone soluciones técnicas basadas en principios de separación de hardware, o soluciones de software de baja resistencia a los intentos de intrusión (y, por lo tanto, de bajo nivel de seguridad). Las soluciones actuales, tales como las arquitecturas de hardware roja-negra, conocidas por el experto en la materia, son costosas de elaborar y de producir. Necesitan el diseño y la evaluación de varias tarjetas de hardware y, en general, de un entorno de software complejo para sincronizar los intercambios entre tarjetas, separar las funciones de administración, etc... Estas soluciones carecen de flexibilidad debido a que se trata de soluciones de hardware, necesariamente menos fáciles de corregir/actualizar en caso de corrección de anomalías informáticas (más conocidas como "error").

Varios industriales y laboratorios trabajan actualmente en las tecnologías de virtualización y, más particularmente, en sus problemáticas de seguridad específicas. Ahora son ampliamente usadas por los gestores de servidores y de forma más anecdótica en estaciones de trabajo, en general para necesidades de desarrollo y de elaboración de software. Todavía se usan poco por necesidades de seguridad.

La solicitud de patente WO 2008/108868 divulga un sistema y un método para implementar una plataforma virtual de seguridad. Esta patente se interesa en crear compartimentos lógicos en un servidor y en asociar cada uno de ellos con una red o con una subred de comunicación, con el objetivo de separar los tratamientos y los datos específicos de estas redes. Esta patente está relacionada con una problemática de red, y más específicamente con una problemática de separación de los espacios de direccionamiento y de enrutamiento.

La solicitud de patente WO 2007/106565 describe una arquitectura de tipo "request box", en español "cuadro de petición", en cabeza de puente.

No obstante, el uso de una tecnología de virtualización no permite resolver por sí sola uno o varios de los problemas mencionados anteriormente. Sin embargo puede permitir sistematizar la toma en cuenta de medios físicos o de procesos de seguridad específicos, y facilitar la evaluación de seguridad de un equipo sensible: la toma en cuenta de las limitaciones de seguridad de un equipo ya no se traslada al sistema operativo (o OS), potencialmente grande y complejo, y las aplicaciones que manipulan datos sensibles, sino a la tecnología de virtualización encargada de pilotar los recursos de hardware, de restringir el acceso a ellos y de aplicar una compartimentación (lógica y posiblemente física) fuerte entre los diferentes tratamientos y el raudal de información. Finalmente, usando una tecnología de virtualización, la problemática del diseñador de un equipo sensible se convierte en una problemática de diseño asegurado de un software de "bajo nivel" y de pequeño tamaño, y ya no el aseguramiento de una gran amalgama de líneas de código. Para dejar constancia, la virtualización es una capa de software que se coloca entre el material informático o hardware y el sistema operativo y la aplicación cliente. Permite compartimentar la aplicación con un OS en bloques lógicamente independientes entre sí; en otras palabras, la virtualización permite realizar una compartimentación "estanca" o manejada entre los compartimentos y lograr que solo los flujos autorizados puedan intervenir entre los bloques. La tecnología de virtualización ha sido imaginada inicialmente para poner en común y permitir un reparto equitativo y transparente de recursos de hardware (procesadores, recursos de medios de almacenamiento y de comunicación, ...) *a priori* costosos y poco usados. Esta tecnología, llamada de "virtualización", permite que varios entornos de software dedicados a diferentes usos o usuarios compartan los mismos recursos de hardware, mientras se da la impresión a cada uno de estos entornos de ser los únicos beneficiarios de los recursos de la plataforma que lo aloja. Con ello, las tecnologías de virtualización se distinguen de los sistemas operativos: un OS multitarea permite que varias aplicaciones se ejecuten simultáneamente en la misma plataforma de hardware, sin

buscar darles la impresión de que son las únicas usuarias de la plataforma.

La presente innovación se interesa en la descripción de una arquitectura compartimentada de confianza que permite compartimentar, intercambiar, tratar y filtrar información, posiblemente (y no solamente) relacionada con redes de comunicación, por medio de una tecnología: la virtualización. El equipo que implementa esta nueva arquitectura permite separar, disociar información de diferentes niveles de sensibilidad porque pertenece a dominios independientes.

El objeto de la presente invención se refiere a un equipo de seguridad ES dispuesto para posicionarse entre al menos un primer dominio que tiene un primer nivel de sensibilidad A y al menos un segundo dominio que tiene un segundo nivel de sensibilidad B, sabiendo que el nivel de seguridad A es diferente del nivel de seguridad B, caracterizado porque incluye al menos los siguientes elementos:

- una capa de hardware física H y varias interfaces I que permiten el intercambio de datos entre dicho equipo de seguridad y los diferentes dominios A, B, un flujo de datos que se emite desde el primer dominio que tiene un nivel de sensibilidad A, transita por la capa de hardware física H y por una capa de virtualización V, luego por un bloque de esclusa y finalmente llega al segundo dominio que tiene un nivel de sensibilidad B,
- la capa de virtualización V está implementada en la capa física H y dispuesta entre dicha capa física H y al menos un conjunto constituido por al menos tres bloques compartimentados, BLA, BLB, MDS, basándose dichos bloques compartimentados en la capa física H y la capa de virtualización, los al menos tres bloques compartimentados no están en la capa de virtualización, y estando dichos bloques constituidos por al menos uno de los elementos tomado de entre la lista siguiente:
    - un software de red A, BLA, que incluye el conjunto de las funciones de redes que permiten tratar datos de nivel de seguridad A,
    - un software de red B, BLB, que incluye el conjunto de las funciones de redes que permiten tratar datos de nivel de seguridad B
    - un bloque de software Módulo de seguridad, MDS, o esclusa dispuesto entre al menos un bloque de tipo BLA y al menos un bloque de tipo BLB, estando dicho módulo de seguridad adaptado para controlar los intercambios de datos entre dichos bloques BLA y BLB, incluyendo dicho módulo de seguridad el conjunto de las transformaciones de seguridad, de filtrado o de funciones criptográficas.

Las letras A y B se usan como referencia genérica para designar dominios que tienen diferentes niveles de seguridad. La expresión "al menos un segundo dominio de nivel de seguridad B", puede designar un segundo dominio de nivel de seguridad B, y un tercer dominio con un nivel de seguridad C diferente de B y A diferente de C.

El equipo de seguridad ES incluye, por ejemplo, las funciones adaptadas para gestionar el intercambio de los flujos de datos entre los diferentes bloques de la siguiente manera:

- los intercambios entre el dominio A y el bloque de software BLA,
- los intercambios entre el bloque de software BLA y un módulo de seguridad MDS,
- los intercambios entre un módulo de seguridad MDS y el bloque de software BLB,
- los intercambios entre el bloque de software BLB y el dominio B.

De este modo, los intercambios directos entre el dominio A y el dominio B están prohibidos. Los intercambios directos entre los bloques BLA y BLB están prohibidos en funcionamiento normal de dicho equipo de seguridad.
Cada uno de los dominios A, B está enlazado con una subred o una red LANi, WANi, siendo en este ejemplo dichos bloques de software BLA y BLB de aplicación de los bloques de redes BRA, BRB.

Un módulo de seguridad MDS incluye, por ejemplo, una o varias de las funcionalidades seleccionadas de entre una de las siguientes: un cifrador IP u otro y/o un contrafuegos y/o de un diodo y/o de detección de intrusión y/o de análisis de flujo. De hecho, el módulo MDS es un punto de control obligatorio de todos los flujos que transitan entre el dominio A y el dominio B.

El equipo de seguridad según la invención puede incluir un número x de bloques de seguridad A, un número de módulos de seguridad igual a x, un número y de bloques de seguridad de nivel B, con A diferente de B.

El módulo de seguridad MDS está dispuesto de tal forma que el recurrido de los flujos de datos en un equipo de seguridad ES el siguiente: el flujo FI que comprende inicialmente datos sensibles sin cifrar es un flujo saliente que va desde el dominio B al dominio A, pasa a través de la capa física H y la capa de virtualización V, antes de transitar por el bloque de red rojo, luego se transmite al bloque de seguridad de criptografía de los flujos salientes, los datos cifrados se transmiten a continuación al bloque de red negro antes de transmitirse al dominio A y un flujo Fil va desde el dominio A y se transmite a través de la capa física H y la capa de virtualización V en el bloque rojo, luego se transmite al bloque de seguridad o esclusa en el que se descifran los datos.

El equipo puede incluir un módulo administrador del funcionamiento de dicho equipo de seguridad.

El número de bloque de módulo de seguridad MDS es igual al número de nivel de seguridad o al número de bloques

de nivel de seguridad presentes en dicho equipo de seguridad.

El número de nivel de seguridad es igual al número de nivel de bloque rojo.

La invención tiene por objeto un equipo de seguridad y su uso. En concreto, ofrece las siguientes ventajas:

1) disminuir el coste de producción de los equipos sensibles,
2) facilitar su evaluación (Ejemplo: Certificación Criterios Comunes EAL),
3) dar más flexibilidad en la gestión de las posibles anomalías de diseño o de implementación.

El equipo asegurado según la invención además permite:

- separar los entornos de software que tienen diferentes niveles de confianza, por el origen del código fuente que los constituye y debido al número y a la naturaleza de las pruebas que han permitido calificar estos compartimentos, por ejemplo,
- restringir el acceso a los recursos sensibles (y, en concreto, a los recursos criptográficos) solo a los compartimentos que realmente los necesitan,
- aplicar una política de seguridad que conste de reglas de control de acceso, independientemente de la naturaleza y de la estructura de los compartimentos soportados y, por lo tanto, independientemente de los sistemas operativos.

La invención se comprenderá mejor y otras ventajas aparecerán con la lectura de la descripción detallada hecha a título de ejemplo no limitativo y con la ayuda de las figuras de entre las que:

- la figura 1 representa un esquema de arquitectura de un equipo asegurado según la invención,
- la figura 2, una arquitectura en el caso de un equipo que comprende varios niveles de seguridad,
- las figuras 3A y 3B, un equipo de seguridad integrado en una estación cliente estándar con un solo nivel de seguridad y un equipo multiniveles,
- las figuras 4A y 4B, dos ejemplos de equipo de seguridad usado como tránsito,
- la figura 5 el esquema cogido los flujos de datos en el caso de un sistema, tal como el que se ha descrito en la figura 1,
- la figura 6, el esquema de la ruta cogida por los flujos en el caso de un equipo de seguridad multiniveles,
- las figuras 7A y 7B, un ejemplo de implementación del equipo de seguridad en un equipo criptográfico,
- la figura 8, un ejemplo de implementación concreto,
- la figura 9, un ejemplo de los detalles de los mecanismos de seguro de la ejecución de la transformación de seguridad,
- la figura 10, un ejemplo de protección espacial, empleada en el sistema según la invención,
- la figura 11, otro ejemplo que especifica las pasarelas que se pueden usar,
- la figura 12, un ejemplo de protección temporal,
- la figura 13, un ejemplo de sistema según la invención usado como una pasarela,
- la figura 14, un ejemplo de equipo de seguridad que contiene dos módulos de seguridad en los que se ejecutan los mismos tratamientos en paralelo con un ligero desfase temporal, y
- la figura 15, un ejemplo de equipo de seguridad que contiene tres módulos de seguridad con un mecanismo de votación mayoritaria.

Los ejemplos dados en la continuación de la descripción están relacionados con bloques de redes. Sin salir del marco, de la invención, los bloques de redes podrían ser remplazados por bloques de software anotados BLs, pudiendo estos últimos adaptarse para gestionar una interfaz hombre máquina, discos duros o incluso funciones de redes.

La figura 1 representa un ejemplo de equipo de seguridad ES compuesto por un conjunto de bloques compartimentados que comprenden cada uno una aplicación independiente con su sistema operativo. En la figura 1 se representan un primer bloque de red BRA de nivel de seguridad A, un segundo módulo de red BRB de nivel de seguridad B, un módulo de seguridad MDS que tiene, por ejemplo, una función de encriptación de los datos o cualquier otra función adaptada para controlar, filtrar, los datos. El módulo de seguridad o esclusa es una esclusa de seguridad que impide cualquier comunicación directa de datos entre dos niveles de seguridad diferentes; se coloca en corte de uno o varios flujos y aplica tratamientos de seguridad (inspección, descontaminación, control de acceso, cifrado, etiquetado, imputación,...) a cada uno de estos flujos con la ayuda en caso necesario de recursos de seguridad (elemento de almacenamiento, componente criptográfico, interfaz de confianza, ...) cuyo acceso le está reservado; su relativa complejidad, así como la posibilidad de poder hacer evolucionar su contenido (para añadir o suprimir funcionalidades, por ejemplo) justifica que esté separado de la tecnología de virtualización subyacente, más enfocada en la puesta en común y el control de acceso a los recursos materiales; su papel de seguridad, además de la necesidad de una evaluación de seguridad según criterios de seguro elevados justifican que esté separado de los bloques de software a los que ofrece sus servicios (BRA y BRB en el caso de la figura 1). De este modo, en la figura, el conjunto compuesto por los tres bloques compartimentados BRA, BRB y MDS) se implanta en una capa de software de virtualización V, estando esta capa implementada en material físico más conocido por la abreviatura anglosajona Hardware y permitiendo las interfaces I la comunicación de cada uno de los bloques con el exterior, por ejemplo, la red A y la red B en la figura 1.

La circulación de los flujos de datos entre los diferentes bloques BRA, BRB se hace de la siguiente manera. El bloque BRA intercambia datos o información a través de la capa de software de virtualización V y la capa física H a una red externa A que corresponde a un dominio de nivel de seguridad diferente de B, por medio de un enlace o según una ruta, FA. El mismo bloque BRA comunica con el módulo de seguridad MDS por la mediación de un enlace CA. Este bloque BRA nunca comunica directamente con el bloque BRB en el caso de un funcionamiento normal del equipo de seguridad. Los intercambios de datos siempre son filtrados o controlados por la esclusa de seguridad.

El bloque BRB intercambia datos con una red externa B de nivel de seguridad B diferente de A por la mediación de la capa de software de virtualización y de la capa física y a través de un enlace FB. Este mismo bloque BRB intercambia datos con el bloque de seguridad MDS a través de un enlace CB. En caso de funcionamiento normal, el bloque BRB no tiene intercambios directos con el bloque BRA.

Cada bloque o compartimento que se sitúa por encima de la capa de virtualización está compuesto, por ejemplo, un sistema operativo u OS sigla anglosajona Operating System u "OS" propio (opcional) y por su aplicación cliente (programa del usuario). Por supuesto, cada compartimento es independiente funcionalmente de los demás (es el objetivo de la virtualización): en otras palabras, es posible ejecutar, detener o reiniciar en cada uno de los compartimentos los programas que se ejecutan en ellos.

La solución propuesta proporciona, de este modo, una solución esencialmente de software que garantiza un nivel de seguridad elevado, esto con el fin de sustraerse a la obligación de proponer sistemáticamente una solución realizada con elementos físicos compartimentados, hoy en día costosa y tecnológicamente limitada. El uso de la capa de virtualización está dispuesto entre la capa de material informático o "hardware" y los compartimentos de software compuestos por un sistema operativo y por la aplicación del usuario. De este modo, la invención permite diseñar equipos sensibles, tales como cifradores IP, cifradores de arteria en redes de comunicación, cortafuegos o incluso recursos criptográficos, por ejemplo, con un coste menor y con un nivel de seguridad comparable (siempre que la tecnología de virtualización y el hardware subyacente posean ciertas propiedades esenciales) con respecto a una solución puramente de hardware.

De este modo, la tecnología de virtualización V es el punto de paso obligatorio para cualquier intercambio entre un componente de software y un recurso sensible, por un lado, y entre dos componentes de software, por otro lado. Asegura un manejo:

1) de los flujos entre componentes de software y recursos de hardware poniendo en común los recursos de la capa física entre varios componentes de software y controlando el acceso a estos recursos (ejemplo: componente criptográfico), y 2) de los flujos entre componentes de software. Autoriza la comunicación entre al menos dos componentes de software (o bloques).

En otras palabras, esta tecnología de virtualización (capa V) aplica:

* por un lado, una política de aislamiento espacial y temporal de los componentes de software que le están asociados, y
* por otro lado, una política de seguridad (autenticación, control de acceso, restricción de velocidades, restricción de las orientaciones de flujo, imputación,...).

Por consiguiente, la política de seguridad aplicada por la tecnología de virtualización permite reservar el acceso de ciertos recursos de hardware a una o varias implementaciones de un componente (de hardware o de software) de un tipo particular, llamado "esclusa de seguridad" o "módulo de seguridad (MDS)" que contiene las funciones de seguridad que a menudo son complejas, específicas y críticas.

La figura 2 esquematiza una arquitectura de equipo de seguridad según la figura 1, que comprende varios niveles de seguridad. En este ejemplo, se habla de bloques de red rojos BRi de nivel de seguridad A que constituyen cada uno individualmente una interfaz con el dominio sensible al que están dedicados (por ejemplo, una red local o LAN privada LAN1, LAN2, LAN3); los datos son sensibles y generalmente circulan sin cifrar. También se trata de bloque de red llamado negro BNi, que forma la interfaz con el dominio público (por ejemplo, una red de área amplia o WAN Wide Area Network); los datos están o bien cifrados, o bien no protegidos. Sin embargo, se puede imaginar que existen varios dominios negros BN1, BN2, BN3 conectados a varias LAN, LAN4, LAN5, LAN6 de sensibilidades inferiores a los dominios rojos. Los bloques MDS1, MDS2, MDS3 (o bloque de seguridad) tienen, en concreto, como función filtrar, analizar los únicos flujos autorizados a circular posiblemente después de haberles hecho experimentar un tratamiento criptográfico, una descontaminación, una desensibilización, términos comúnmente usados por el experto en la materia en el campo de la seguridad. De manera más precisa, un bloque de red rojo BRi va a comunicar datos a través de una esclusa de seguridad MDSi a un bloque BNj (o viceversa, pero siempre a través de un MDS). En el ejemplo de la figura 2, se encuentran las capas de virtualización, así como la capa física de la figura 1. El número de bloques rojos, que pueden presentar diferentes niveles de seguridad, BR1, BR2 ..., es al menos superior o igual al número de bloques esclusa o bloques de seguridad (MDS1, MDS2, MDS3…, por ejemplo). Del lado de los bloques negros, puede haber uno o varios niveles de seguridad.

La virtualización está adaptada para el uso del multiniveles:
Lado rojo: el equipo puede tratar varios flujos de diferentes niveles de seguridad conectados a varias redes locales o

LANi diferentes. En este caso, un nivel rojo está asociado con un bloque de esclusa MDS1.
En el lado negro, es común que el bloque negro BNi esté conectado a un solo dominio de sensibilidad (tal como una red de área amplia o una red pública, en ciertos contextos). También puede haber un solo nivel negro o bien varios niveles negros, no necesariamente en el dominio público.

En este ejemplo, se han representado 6 redes locales más conocidas por la sigla anglosajona "LAN". Están conectadas al equipo sensible a través de un puerto Ethernet. Es interesante anotar que las LAN representan diferentes niveles de sensibilidades o diferentes niveles de confianza (es decir, niveles de sensibilidad idénticos pero cuya información es de naturaleza diferente: por ejemplo, información de mismos niveles "secreto", pero de un país A y de un país B que no desean mezclar sus flujos, lo que implica un diferente nivel de confianza).

Las figuras 3A y 3B representan dos ejemplos de equipo asegurado según la invención que tiene una función de terminal, por ejemplo, en una aplicación de red.

La figura 3A muestra un ejemplo de equipo asegurado integrado en una estación cliente estándar 10 que comunica con una red R. La estación cliente que puede ser un PC de usuario comprende una capa física H, una capa de virtualización V, un bloque de red negro 12, un bloque de interfaz hombre máquina que constituye el bloque rojo 13, y una esclusa 14 que separa los dos bloques 12, 13, bloque de red negro y el bloque de red rojo.

La figura 3B, representa un ejemplo de equipo asegurado implementado en una estación de cliente multiniveles. La estación de cliente 20 está en relación con una red 21. La estación de cliente 20 comprende una capa de hardware física H, una capa de virtualización V, una red negra 22, una primera interfaz hombre máquina (1er cliente del servidor) que tiene un nivel de sensibilidad NR1, 23, enlazada con una primera esclusa 24, una segunda interfaz hombre máquina 25 (2º cliente del servidor) que tiene un segundo nivel de seguridad NR2 que comunica con una segunda Esclusa 26. Las líneas punteadas en la figura 3B representan la separación de software de los diferentes módulos mencionados anteriormente. De este modo, el segundo bloque 25 no puede comunicar con el primer bloque directamente, ya que no tienen el mismo nivel de sensibilidad. Las esclusas no comunican entre sí.

Los compartimentos sensibles se multiplican por el número de niveles gestionados por el terminal.

La línea de compartimentación LC muestra la separación de software y funcional de los dominios de redes: en otras palabras, la información diferente de nivel de sensibilidad nunca se mezcla. Esta separación de software está tan comprobada como una separación de hardware convencional.

La figura 4A esquematiza un ejemplo de equipo de seguridad usado como una pasarela o tránsito entre una primera red de área amplia conocida por la sigla anglosajona "WAN" 30 y una segunda red local LAN, 31. El equipo de seguridad está compuesto por una parte negra 32, enlazada con la WAN 30, de una parte roja 33, enlazada con la LAN 31 y por una esclusa 34 que actúa como línea de compartimentación entre las dos redes de diferentes niveles de sensibilidad. El equipo siempre comprende, la capa física H y la capa de virtualización V. En este ejemplo, las comunicaciones con las redes se hacen a través de las partes negra o roja. Una línea de compartimentación LC entre dos niveles de seguridad está esquematizada en la figura: esta línea de compartimentación no es física. Sin embargo, indica que lógica y funcionalmente ningún dato pasa de un dominio al otro sin pasar por una esclusa (o MDS: Módulo de Seguridad).

La figura 4B representa una aplicación de la figura 4A para una parte roja que comprende varios niveles de seguridad. En este caso, a cada bloque rojo de nivel de seguridad NRi corresponde una parte de esclusa Si. Las líneas punteadas en la figura representan las líneas de compartimentación LC, LC2 entre las redes formadas de este modo que presentan diferentes niveles de sensibilidad.

La figura 4 B puede considerarse como una pasarela o un cortafuego, o un cifrador, o un diodo de redes, etc...

Una parte Negra o una parte roja está compuesta por los siguientes elementos: un OS (Operating System), pilotos, aplicaciones cliente que ofrecen servicios (posiblemente con bibliotecas DLL (Dynamic Link Library, en español, biblioteca de enlace dinámico), etc...). Las aplicaciones pueden ser diversas: un agente SNMP (Simple Network Management Protocol, en español, protocolo simple de administración de redes), una función de árbol de extensión, una función de coloración de flujo, una función de gestión de pila IP (Internet Protocol, en español, protocolo de internet), función de gestión QoS (Quality of Service, en español, calidad de servicio), función ARP (Address resolution protocol, en español, protocolo de resolución de direcciones), función NAT transversal (Network Address Translation, en español, traducción de direcciones de red), función de fragmentación, función de orientación DSCP (Differentiated Services Code Point, en español, punto de código de servicios diferenciados) función de gestión de congestión, función de alarmas y de registro, función DHCP (Dynamic Host Configuration Protocol, en español, protocolo de configuración dinámica de host), función VLAN (Virtual Local Area Network, en español, red de área local virtual), función de reparto de cargas (load balancing), función de movilidad (Mobike), función de enrutamiento (RIP: Routing Information Protocol, en español, protocolo de información de enrutamiento), OSPF (Open Shortest Path First, en español, abrir el camino más corto primero), etc. básicamente todas las funciones de redes estándar.

En la parte Módulo de Seguridad MDSi se implementan, en concreto, las siguientes funciones:

- funciones de filtrado (filtrado de números de puerto, filtrado de protocolos, Antivirus, filtrado IP, IDS, etc...),
- o funciones de criptográficas o de seguridad (cifrado, descifrado, función de protocolo IPSEC conocida por el experto en la materia, función de contador anti-reproducción, función de gestión de claves simétricas, función de certificados, función de tratamiento de borrado de emergencia, función de seguridad de antiintrusión, etc.).

La figura 5 esquematiza el recurrido de los flujos de datos en un equipo de seguridad, tal como el que se ha descrito en la figura 1 o incluso en la figura 4A. En este ejemplo, el equipo de seguridad es un cifrador IP. El flujo FI que comprende inicialmente datos sensibles sin cifrar es un flujo saliente que va desde el dominio B al dominio A. Pasa a través de la capa física H y la capa de virtualización V, antes de transitar por el bloque de red rojo 52, luego se transmite al bloque de esclusa 51 de criptografía de los flujos salientes, por ejemplo, este bloque puede cifrar los datos del flujo. Los datos cifrados se transmiten a continuación al bloque de red negro 50 antes de transmitirse al dominio A. El recurrido de los flujos entrantes se hace de la siguiente manera: el flujo FII va desde el dominio A y se transmite a través de la capa física H y la capa de virtualización V en el bloque rojo 52, luego se transmite al bloque de esclusa 53 en el que los datos son descifrados, por ejemplo. Los datos descifrados se transmiten a continuación al bloque rojo 52 antes de enviarse a la red de dominio B.
El bloque negro como el bloque rojo contiene funciones de redes conocidas por el experto en la materia. Los módulos criptográficos o módulo de seguridad (MDS) contienen funciones de seguridad o las funciones críticas (tales como el cifrado o el descifrado).
En cada paso de un bloque rojo o negro al otro, los flujos pasan a través de la capa de virtualización V. La descomposición de los módulos criptográficos en este ejemplo de aplicación o MDS en dos partes distintas (cifrado / descifrado) permite separar los flujos entrantes de los flujos salientes. Ello tiene la ventaja de mejorar la seguridad, ya que cada esclusa se convierte en un diodo dedicado a un sentido unidireccional del flujo de datos (se especializan las funciones) y de aumentar también la fiabilidad de funcionamiento y de autorizar mecanismos de autoprueba (véase figura 9 A).
De este modo, cada MDS se asigna a un sentido dado y cada bloque BRi está dedicado a un enrutamiento particular según el sentido del flujo. El bloque de red BRi orienta el mensaje o bien hacia el exterior (la red LAN o WAN a la que está conectado) o bien hacia el bloque de seguridad MDS correcto.
Los bloques de redes BRi no pueden comunicar directamente entre sí. Conteniendo los módulos de seguridad las funciones críticas de seguridad, la política de seguridad, aseguran las comunicaciones entre los bloques de redes BRi.

La figura 6 representa el recurrido seguido por flujos de datos en un equipo de seguridad con varios niveles de seguridad diferentes, tal como el que se ha descrito en la figura 4B, por ejemplo.

El recorrido F1 representa un primer flujo saliente que va desde el dominio C al dominio A. El flujo F1 recorre la siguiente ruta; pasa por las capas de hardware y las interfaces físicas y de virtualización para pasar a continuación en el bloque de red rojo 62. Después se transmite a un primer bloque de esclusa 61 dentro del que los datos se cifran, por ejemplo, los datos cifrados repasan por la capa de virtualización V antes de pasar a través del bloque de red negro 60, luego a través de la capa de virtualización, estos datos cifrados se transmiten a la red de dominio A.

La línea F2 representa el recorrido de un flujo de datos salientes que va desde el dominio B a una red de dominio A. Los flujos de datos pasan a través de la capa física H y de virtualización al bloque de red rojo 64. A continuación, se transmiten a un bloque de esclusa 63 de cifrado de los datos antes de transmitirse a través de la capa de virtualización a un bloque negro 60. Los datos cifrados se transmiten a continuación a través de la capa de virtualización y la capa física al dominio C.

La flecha F3 corresponde al recorrido seguido por un flujo entrante que va desde el dominio A y que va al dominio B. El flujo de datos se va a transmitir a través de las capas físicas y de virtualización al bloque negro 60, luego en el bloque de esclusa 65, con el fin de que los datos sean descifrados, por ejemplo. Los datos descifrados pueden transmitirse a través de la capa de virtualización y la capa física al bloque de red rojo 64, luego a la red B a través de la capa de virtualización y la capa física.

La flecha F4 esquematiza el recorrido de un flujo entrante que va desde el dominio A para desembocar en el dominio C. Los datos del flujo se transmiten desde la red A al bloque de red negro 60 antes de descifrarse en el bloque de esclusa 66. Los datos descifrados se transmiten a continuación a través de la capa de virtualización y la capa física al bloque de red rojo 62 antes de enviarse al dominio C a través de la capa de virtualización y la capa física.

Cada comunicación entre dos bloques autorizados a comunicar entre sí pasa obligatoriamente por la capa de virtualización que garantiza la compartimentación y el control de sus intercambios entre los bloques. Los bloques de redes contienen las funciones estándar de redes. Aseguran los intercambios entre el exterior y los MDS. No pueden comunicar entre sí. Los bloques MDS siempre tienen la función de seguridad descrita anteriormente y aseguran la comunicación entre los bloques de redes BRi exclusivamente.

Las figuras 7A y 7B esquematizan dos ejemplos de implementación en un equipo criptográfico.

En este ejemplo, el equipo criptográfico está compuesto por una parte de usuario 70 y por una parte de supervisor 71. El equipo comprende una capa física H, un núcleo de un sistema operativo más conocido por la sigla anglosajona micro kernel. Este núcleo es en sí mismo un software, que tiene, en concreto, como función permitir la comunicación

entre los diferentes elementos del sistema. Una capa de configuración o de partición C específica para el usuario. La tecnología de virtualización permite la creación de los siguientes compartimentos lógicos:

- un compartimento rojo 72 trata datos sin cifrar, no cifrados. Estos datos de usuario deben ser protegidos, por ejemplo, en confidencialidad y en integridad. El compartimento rojo comunica con el exterior a través de 2 puertos Ethernet 73 y las capas de hardware, de particionamiento y el micro kernel,
- un módulo de seguridad (MDS) o esclusa criptográfica 74. Este compartimento llamado de confianza o de seguridad asegura, en concreto, todos los tratamientos, los más sensibles, tales como la firma de software, el cifrado o incluso el filtrado, requerido durante la transferencia de información entre un compartimiento rojo y un compartimiento negro,
- un compartimento negro 75 para los datos negros, es decir, los datos cifrados. Este compartimento negro está conectado al mundo exterior a través de 2 puertos 76 Ethernet, por ejemplo, y las capas de hardware, de particionamiento y el micro kernel,
- un compartimento 77 de Administración que tiene, en concreto, para funciones de mantenimiento, de actualización de software, de traslado de supervisión, de búsqueda de anomalías de funcionamiento o "corrección de error", de interfaz hombre máquina o "IHM", con el fin de mostrar ciertos resultados parciales o estados de funcionamiento del equipo. Su uso no es limitativo. Su aislamiento en un compartimento específico por medio de la tecnología subyacente se justifica por el nivel de confianza requerido en la ejecución de las funciones de administración. Además, este compartimento no efectúa ningún tratamiento en el flujo de datos (el tráfico) entre el dominio A y el dominio B.

Cada compartimento es independiente de los otros, debido a la presencia de la capa de virtualización en el caso de la figura 7A, la capa de virtualización v está representada por las capas del gestor de particionamiento y el hipervisor que asigna las asignaciones de recursos de hardware. En otras palabras, un compartimento puede tener su propio sistema operativo, ser capaz de reiniciar sin perturbar a los otros compartimentos, tener sus propios tratamientos y sus propias aplicaciones. La tecnología de virtualización emplea todos los mecanismos requeridos para asegurar esta independencia, incluso para permitir que dos compartimentos se intercambien información de forma asegurada. De este modo, los intercambios entre compartimentos rojo y negro pasan obligatoriamente por el compartimento MDS, estando estos intercambios esquematizados con las flechas F_R y F_N.

La figura 7B representa un ejemplo de implementación real de la arquitectura de un equipo diseñado según la invención. Esta figura hace aparecer los puertos Ethernet correspondientes a las interfaces E1, E2, E3, E4 y E5. Estas interfaces están conectadas a una entidad llamada "hardware" que constituye la plataforma de hardware de alojamiento de tipo COTS o de tipo tarjeta dedicada. Los elementos de software de la tecnología de virtualización están presentes a través de las dos entidades de tipo "microkernel" OS-kernel y gestión de partición u OS-G más conocido por la sigla anglosajona "partition Manager". Este conjunto ofrece un servicio de sistema operativo compartimentado para diferentes aplicaciones representadas a través de:

- El enrutador o tarjeta de red R_1 y sus dos interfaces E_1 y E_2 conformes del esquema anterior, circulando el flujo de tipo F_1 entonces entre las interfaces E_1 y E_2;
- El enrutador R_2 o tarjeta de red y sus dos interfaces E_3 y E_4 conformes del esquema de la figura 8B;
- El compartimento de pasarela P, responsable del flujo F_3 a través de las dos medias conexiones de tipo F3.1, F_N (figura 7A) y F3.2 o F_R (figura 7A);
- La gestión G que implementa el terminal T asociado con su interfaz E0. Por un lado, las propiedades de planificación temporal de la tecnología de virtualización permiten privilegiar un compartimento en detrimento de otro en función de los objetivos del sistema a alcanzar, por otro lado, el aislamiento de memoria aportado por la compartimentación estática empleada en las fases de ingeniería y gestionado por el gestor de partición permite obtener una interconexión de diferentes zonas de sensibilidad (dominio A y dominio B en la figura 9). Esta interconexión está bajo el control exclusivo del software de la pasarela P más conocida por la sigla anglosajona "gateway", que implementa una política de seguridad definida. La capacidad de emplear una pasarela de software exclusivamente en la interfaz de bajo nivel del gestor de partición o, más bien, a través de un sistema operativo OS de tipo Linux u otro ya no depende más que de los objetivos asociados con la estrategia de certificación de la pasarela y de la tecnología de virtualización asociada.

Las dos figuras 7A y 7B muestran las transferencias a través de la capa de virtualización y el número de conmutaciones. Se distinguen de este modo dos tipos de flujos:

- los flujos que conectan los bloques de redes y el exterior del equipo (flujo de comunicación / interequipo),
- Los flujos que conectan los Bloques de redes y los módulos de seguridad MDS (flujo intraequipo).

La línea de compartimentación LC se presenta con el fin de mostrar que ninguna comunicación es posible entre los dos dominios A y B aparte de los intercambios autorizados en el módulo de seguridad MDS (o Gateway / esclusa).

La figura 8 presenta un equipo de seguridad según la invención a través de un equipo de pasarela con sistema operativo particionado que incluye una capa de virtualización, tal como la que se ha descrito en las figuras anteriores, que corresponde a un enrutador lógico que contiene 5 interfaces físicas anotadas E1, E2, E3, E4 y E5.
Las zonas "área A" y "área B" corresponden a redes locales independientes constituidas por los servidores S1, S2 en

la red NET1 en la zona A y S3, S4 en la red NET3 en la zona B.
Cada zona constituida de este modo corresponde a una arquitectura de red tradicional que permite establecer flujos de información de tipo F1, F2. Por lo tanto, estos flujos corresponden al tráfico asociado con los protocolos intercambiados entre los terminales y los servidores. En ausencia de flujo F3, las redes constituidas de este modo están totalmente aisladas y en tal caso, el enrutador con parte de sistema operativo podría estar constituido por dos equipos independientes de tipo enrutador convencional. El terminal T en una interfaz dedicada E0 representa la capacidad de administración del equipo. En el esquema propuesto, el flujo F3 forma parte de un artículo de la invención, se caracteriza, por ejemplo, por dos diodos de software y de hardware (F3.1 y F3.2 no representados en la figura por razones de simplificación) que implementan, por lo tanto, un tráfico unidireccional. Estos diodos tienen por objeto evitar que el tráfico procedente del área A pueda transitar al área B.
Este esquema da un ejemplo de conectividad de un equipo que integra una arquitectura de seguridad virtualizada.

La figura 9 A representa un modo de realización que implementa un mecanismo de autocontrol del sistema de seguridad. Con el fin de asegurarse de la garantía de ejecución de la función de seguridad implementada en una esclusa dispuesta en corte de un bloque rojo 81 y de un bloque negro, es posible establecer un mecanismo de autocontrol que consiste en aplicar la función de seguridad, o bien una función de cifrado S_1 o bien de descifrado S_{-1} al mensaje o datos al que se ha aplicado la misma función durante una etapa anterior.
De este modo, en la figura en el caso de que se desee transmitir datos desde el dominio A al dominio B de nivel de seguridad más bajo que el de A, los datos se van a transmitir en primer lugar al bloque rojo 81 a través de la capa de hardware y de virtualización 82 antes de pasar primero a la primera esclusa de cifrado 83, luego a la segunda esclusa de descifrado 84. El flujo de datos cifrados, luego descifrados se transmite a continuación a un módulo de control y de pruebas 85 adaptado para verificar que los datos descifrados son efectivamente idénticos a los datos iniciales cifrados. El control puede consistir en un análisis y una comparación del código descifrado. De este modo, esta prueba garantiza que el flujo de datos que sale del dominio A está efectivamente protegido en el dominio B después de paso en el bloque negro 86 y el bloque 83.

El mecanismo figura 9B esquematiza las etapas del organigrama de la figura 9A. La figura 9A con su mecanismo descrito en 9B muestra un sistema que garantiza que los flujos están protegidos correctamente (en este caso, cifrado) antes de ir a un WAN (dominio público / dominio negro). Otros sistemas de control, de pruebas o de autoprueba pueden mejorar la seguridad o la fiabilidad de funcionamiento del equipo de seguridad.

Se pueden implementar otros mecanismos de control como en las figuras 10, 11 y 12. Las figuras 10, 11 y 12 representan un mecanismo de separación espaciotemporal de los flujos de diferentes niveles de sensibilidad. Es importante emplear mecanismos que garanticen que la información contenida en el ES virtualizado nunca se mezclará tanto en el espacio como en el tiempo, mientras se asegura que la configuración de la herramienta de virtualización está efectivamente implementada. Es una propiedad esencial en la que se basa la invención. El establecimiento de esta propiedad se basa en 1) mecanismos de hardware específicos (controlador de acceso a memoria, paginación / segmentación, gestión centralizada de las interrupciones, ...) y, 2) mecanismos de software apropiados. El funcionamiento de estos mecanismos conocidos por el experto en la materia no se describe en la invención. Dicho de otro modo, esto impone dos tipos de protección que se completan:

- una protección espacial: Figura 10. Controladores (o en este ejemplo autómatas de control ACi: especie de cortafuego o filtro de software) están en la entrada de cada bloque BR, MDS y controla cada trama de los flujos entrantes o salientes (por medio de tags o de etiquetas contenidas en las tramas). Estos controladores son, por ejemplo:

    ○ Módulos de control de memorias: las memorias no deben compartirse (partición, memoria diferentes, diferentes rangos ...),
    ○ Módulos de núcleo procesador (en el caso de un procesador multinúcleos) asignado a un cierto nivel de seguridad. Se puede asignar un núcleo de procesador a un bloque,
    ○ una protección espacial de seguridad: En este ejemplo el MDS puede contener todas las funciones de seguridad o incluso el equipo de seguridad puede incluir un MDS por servicio, (ejemplo: figura 11).

- una protección temporal: figura 12

    ○ usa un secuenciador S / temporizador que impide que un mismo bus compartido B o que una CPU trabaje tanto en los datos rojos como negros. El temporizador asigna divisiones temporales a cada compartimento con el fin de que no se mezcle ningún flujo con otro de un nivel de seguridad diferente al suyo,
    ○ permite evitar la creación de canales temporales ocultos y la explotación de canales auxiliares que se basan en una medición de tiempo de tratamiento o de la tasa de disponibilidad de un recurso,

- una protección de configuración.

Los autómatas de control filtran todos los flujos entrantes o salientes de cada uno de los bloques/compartimentos.
En la figura 12, el secuenciador asigna un tiempo CPU o de acceso al bus interno de intercambios de datos.

La figura 11 esquematiza un ejemplo de aplicación del equipo de seguridad para una pasarela. En este ejemplo, la virtualización y más particularmente los bloques de filtrado permiten distinguir los flujos entre sí: separación espacial.

Estos últimos también permiten tener una separación temporal que se puede implementar de forma diferente según las limitaciones de seguridad y de redes. El equipo de seguridad está posicionado entre un dominio A de nivel de seguridad A y un dominio B de nivel de seguridad o sensibilidad B. Los flujos procedentes de A pasan a través de un bloque de red A a un módulo de filtrado FWA. En la salida del módulo de filtrado, los datos se transmiten al MDS que contiene los diferentes servicios. Los bloques de filtrado FWx sirven entonces de orientador de flujo a los servicios deseados. Puede haber tantos compartimentos como servicios. También puede haber agrupaciones de servicio en un solo compartimento. Luego, los datos se transmiten a un segundo módulo de filtrado FWB antes de enviarse a una parte B de la red y al dominio B.

La figura 12 ilustra más particularmente la capa de virtualización, con el secuenciador S, el bus de intercambios B.

La figura 13 muestra que un compartimento adicional puede ser agregado con el fin de ofrecer servicios de administración G del equipo de seguridad (como la IHM, el traslado de supervisión con el fin de que el operario o el administrador de red pueda verificar el correcto funcionamiento del equipo, etc...).

La figura 14 muestra un equipo de seguridad virtualizado que tiene un compartimento adicional para aumentar la fiabilidad y, por consiguiente, la seguridad de funcionamiento de la transformación de seguridad (figura cercana a la figura 9A). En las dos esclusas MDS1, MDS2, que separan el bloque rojo y el bloque negro BR, BN, los mismos programas o tratamiento de seguridad se ejecutan con un ligero desfase en el tiempo: de este modo, una vez completados los tratamientos, se comparan los resultados. Cuando los resultados son idénticos, entonces el flujo (por ejemplo, cifrados) sale del equipo, si no es idéntico, entonces no sale del equipo. De este modo, si experimentan un ataque o una intrusión en un momento dado, los dos procesos no se ven perturbados de la misma manera, ya que no ejecutan el mismo tratamiento en un momento t debido al pequeño desfase temporal.

Unos mecanismos similares ilustrados en la figura 15, pueden usarse con tres esclusas (o MDS) Esclusa1, Esclusa2, Esclusa3, que separan el bloque rojo BR y el bloque negro BN que ejecutan los mismos tratamientos, pero se efectúa una votación mayoritaria al final de estos: si al menos dos resultados son idénticos, entonces el tratamiento ha tenido éxito, de lo contrario es el fracaso y el equipo se congela (bloquea cualquier comunicación después de haber enviado una alarma a su centro de gestión o de supervisión).

REIVINDICACIONES

1. Equipo de seguridad ES dispuesto para posicionarse entre al menos un primer dominio que tiene un primer nivel de sensibilidad A y al menos un segundo dominio que tiene un segundo nivel de sensibilidad B, sabiendo que el nivel de seguridad A es diferente del nivel de seguridad B, **caracterizado porque** incluye al menos los siguientes elementos:

- una capa de hardware física H y varias interfaces I que permiten el intercambio de datos entre dicho equipo de seguridad y los diferentes dominios A, B, un flujo de datos que se emite desde el primer dominio que tiene un nivel de sensibilidad A, transita por la capa de hardware física H y por una capa de virtualización V, luego por un bloque de esclusa y finalmente llega al segundo dominio que tiene un nivel de sensibilidad B,
- la capa de virtualización V está implementada en la capa física H y dispuesta entre dicha capa física H y al menos un conjunto constituido por al menos tres bloques compartimentados, BLA, BLB, MDS, basándose dichos bloques compartimentados en la capa física H y la capa de virtualización, los al menos tres bloques compartimentados no están en la capa de virtualización, y estando dichos bloques constituidos por al menos uno de los elementos tomado de entre la lista siguiente:

    - un bloque de software A, BLA, que incluye el conjunto de las funciones de redes que permiten tratar datos de nivel de seguridad A,
    - un bloque de software B, BLB, que incluye el conjunto de las funciones de redes que permiten tratar datos de nivel de seguridad B,
    - un bloque de software Módulo de seguridad, MDS, o esclusa dispuesto entre al menos un bloque de tipo BLA y al menos un bloque de tipo BLB, estando dicho módulo de seguridad adaptado para controlar los intercambios de datos entre dichos bloques BLA y BLB, incluyendo dicho módulo de seguridad MDS el conjunto de las transformaciones de seguridad, de filtrado o de funciones criptográficas.

2. Equipo de seguridad según la reivindicación 1, **caracterizado porque** un equipo de seguridad incluye las funciones adaptadas para gestionar el intercambio de los flujos de datos entre los diferentes bloques de la siguiente manera:

- los intercambios entre el dominio A y el bloque de software BLA,
- los intercambios entre el bloque de software BLA y un módulo de seguridad MDS,
- los intercambios entre un módulo de seguridad MDS y el bloque de software BLB,
- los intercambios entre el bloque de software BLB y el dominio B.

3. Equipo de seguridad según una de las reivindicaciones 1 o 2, **caracterizado porque** cada uno de los dominios A, B está enlazado con una subred o una red LANi, WANi y **porque** los bloques de software BLA y BLB son bloques de Redes BRA y BRB.

4. Equipo de seguridad según una de las reivindicaciones 1 a 3, **caracterizado porque** un módulo de seguridad MDS incluye funcionalidades seleccionadas de entre las siguientes: un cifrador IP u otro y/o un cortafuego y/o de un diodo y/o de detección de intrusión y/o de análisis de flujo.

5. Equipo de seguridad según una de las reivindicaciones 1 a 4, **caracterizado porque** incluye un número x de bloques de seguridad A, un número de módulos de seguridad igual a x, un número y de bloques de seguridad de nivel B, con A diferente de B.

6. Equipo de seguridad según una de las reivindicaciones 1 a 5, **caracterizado porque** el módulo de seguridad MDS está dispuesto de tal forma que el recorrido de los flujos de datos en un equipo de seguridad ES es el siguiente: el flujo FI que comprende inicialmente datos sensibles sin cifrar es un flujo saliente que va desde el dominio B al dominio A, pasa a través de la capa física H y la capa de virtualización V, antes de transitar por el bloque de red rojo (52), luego se transmite al bloque de seguridad (51) de criptografía de los flujos salientes, los datos cifrados se transmiten a continuación al bloque de red negro (50) antes de transmitirse al dominio A y **porque** un flujo FII va desde el dominio A y se transmite a través de la capa física H y la capa de virtualización V en el bloque rojo (52), luego se transmite al bloque MDS (53) en el que se descifran los datos.

7. Equipo de seguridad según una de las reivindicaciones anteriores, **caracterizado porque** incluye un módulo administrador (77, G) de dicho equipo de seguridad.

8. Equipo de seguridad según una de las reivindicaciones anteriores, **caracterizado porque** el número de bloque de módulo de seguridad MDS es igual al número de nivel de seguridad o al número de bloques de nivel de seguridad presentes en dicho equipo de seguridad.

9. Equipo de seguridad según la reivindicación 8, **caracterizado porque** el número de nivel de seguridad es igual al número de nivel de bloque rojo.

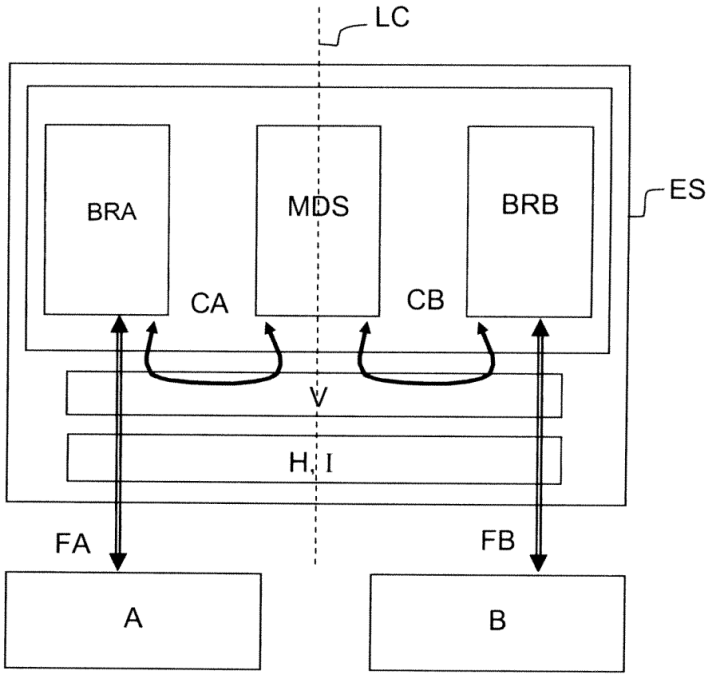
LC
BRA
MDS
BRB
ES
CA
CB
V
H, I
FA
FB
A
B

FIG.1

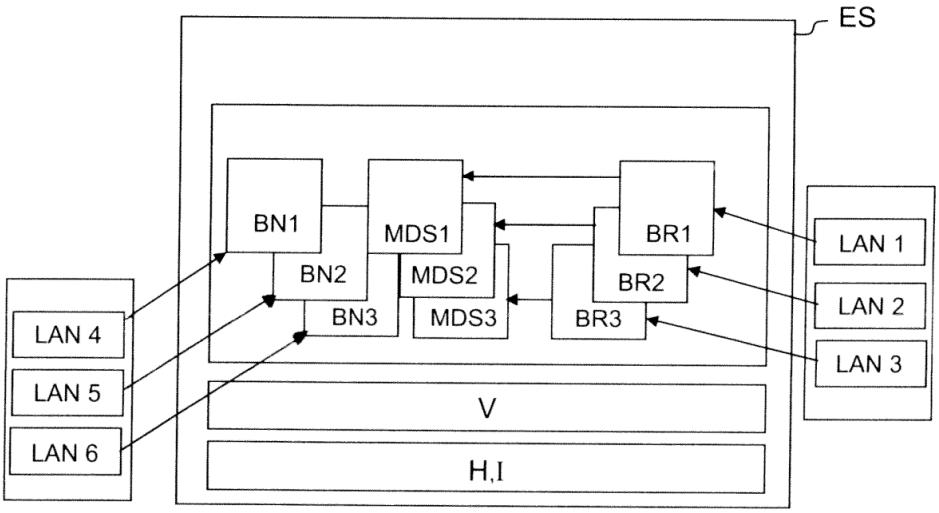
ES
BN1
MDS1
BR1
BN2
MDS2
BR2
BN3
MDS3
BR3
LAN 1
LAN 2
LAN 3
LAN 4
LAN 5
LAN 6
V
H,I

FIG.2

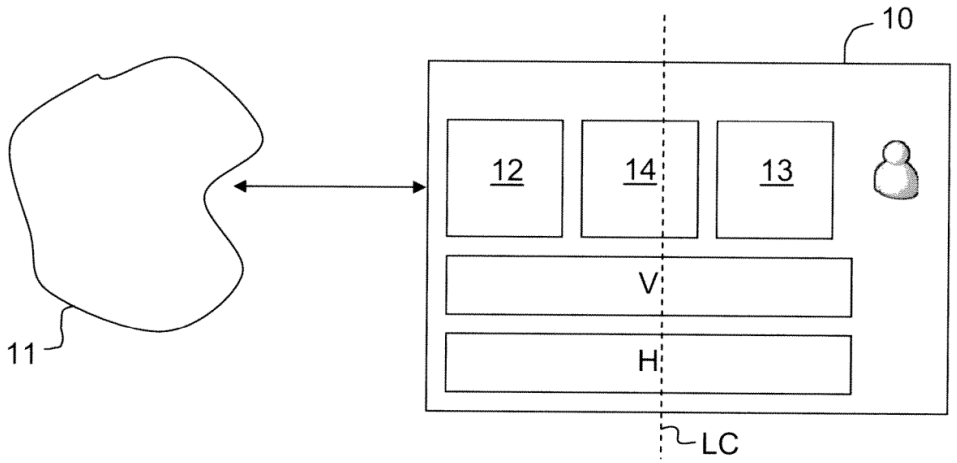

FIG.3A

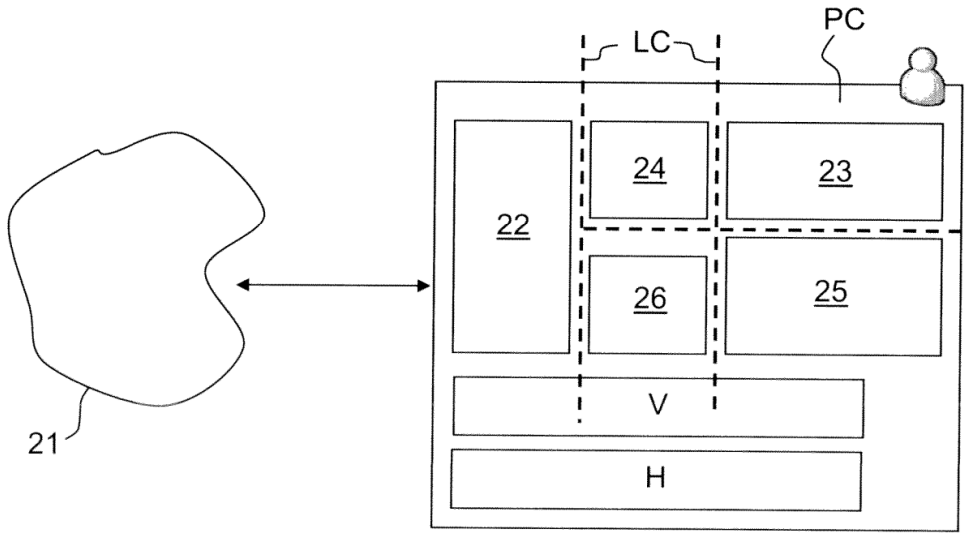

FIG.3B

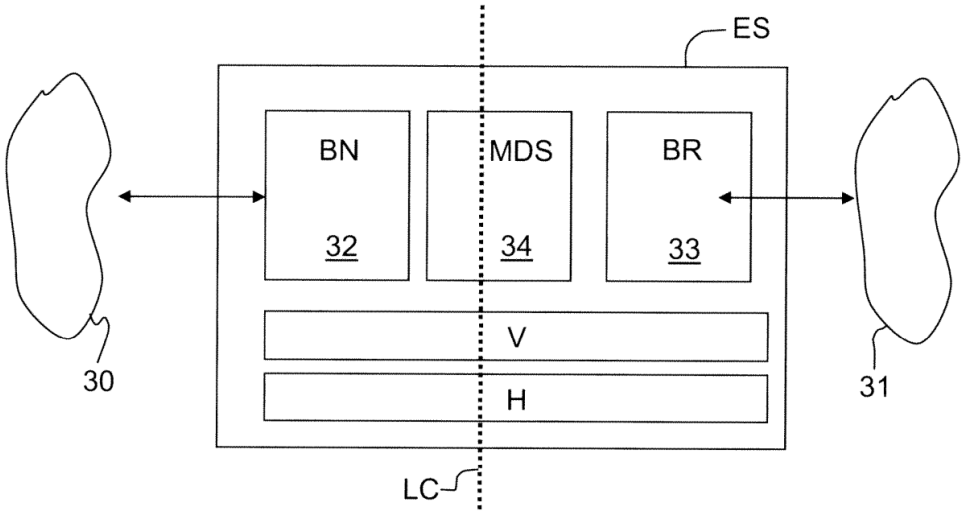
ES
BN
32
MDS
34
BR
33
V
H
30
31
LC

FIG.4A

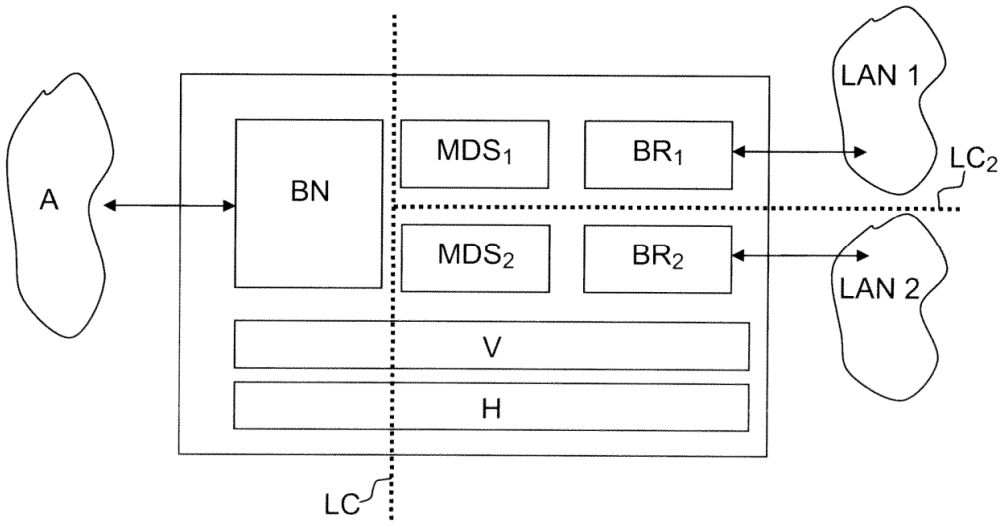
A
BN
MDS1
BR1
LAN 1
LC2
MDS2
BR2
LAN 2
V
H
LC

FIG.4B

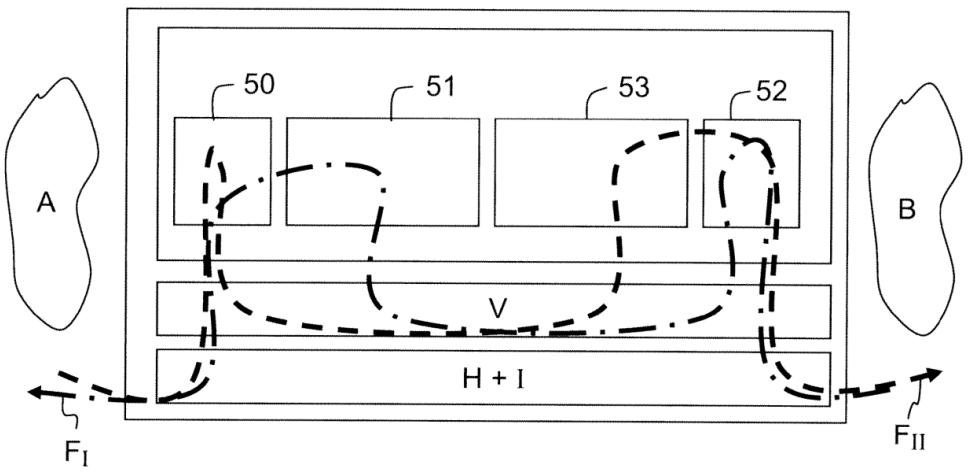

FIG.5

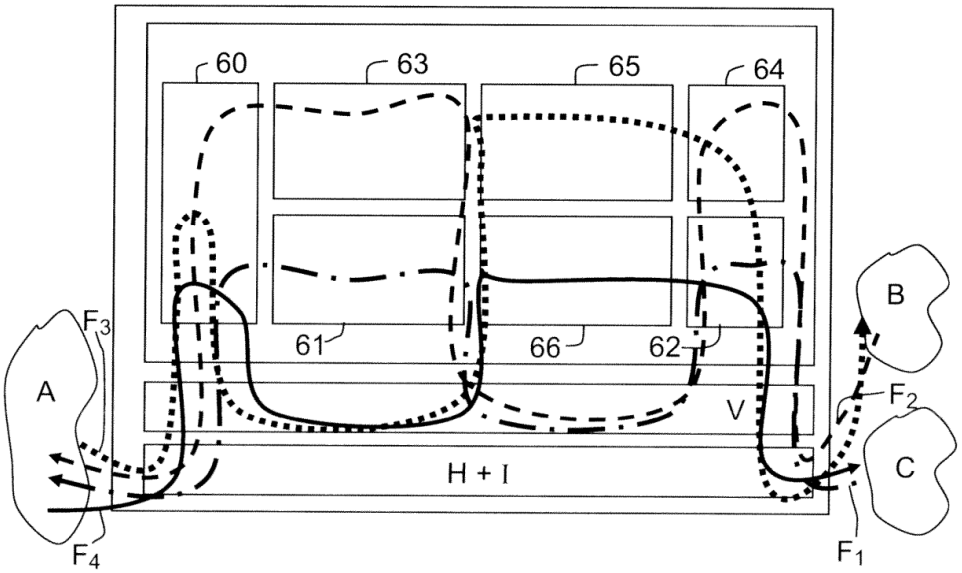

FIG.6

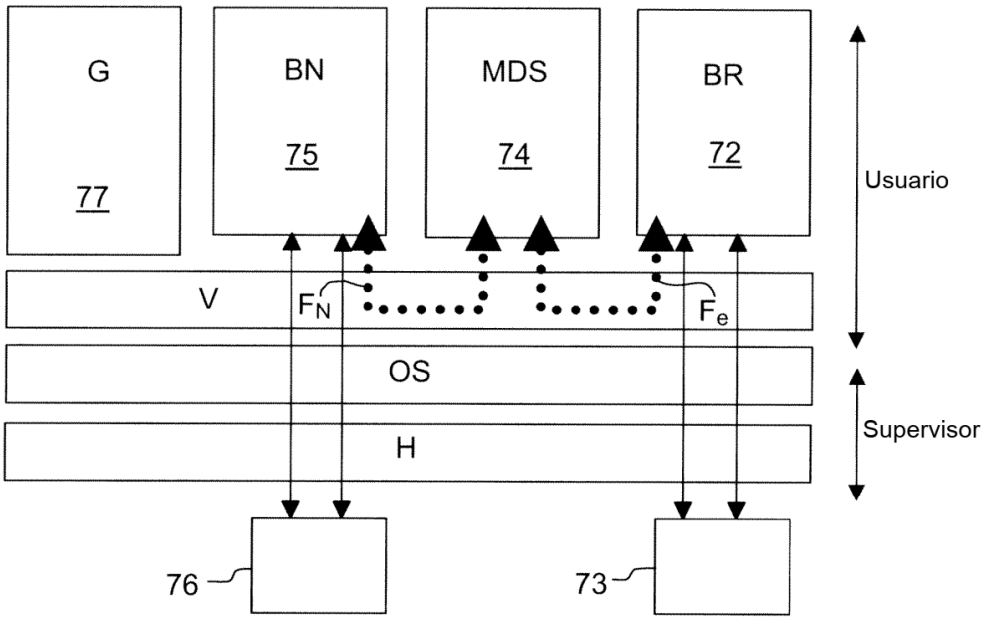
G
77
BN
75
MDS
74
BR
72
Usuario
V
F_N
F_e
OS
Supervisor
H
76
73

FIG.7A

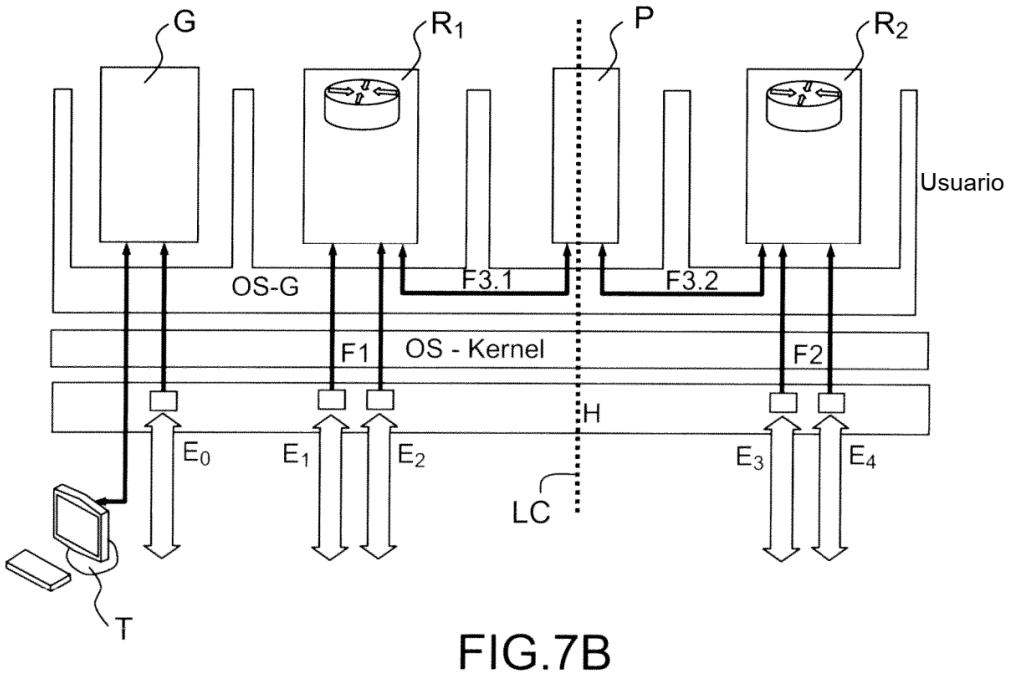
G
R_1
P
R_2
Usuario
OS-G
F3.1
F3.2
F1
OS - Kernel
F2
H
E_0
E_1
E_2
E_3
E_4
LC
T

FIG.7B

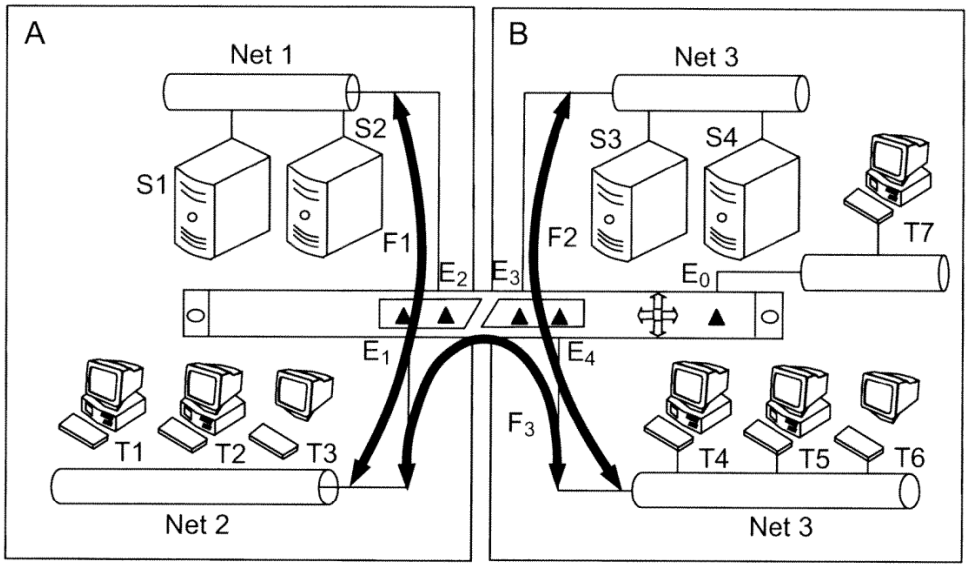
A
Net 1
S1
S2
F1
E2
E1
T1
T2
T3
Net 2
B
Net 3
S3
S4
F2
E3
E0
T7
E4
F3
T4
T5
T6
Net 3

FIG.8

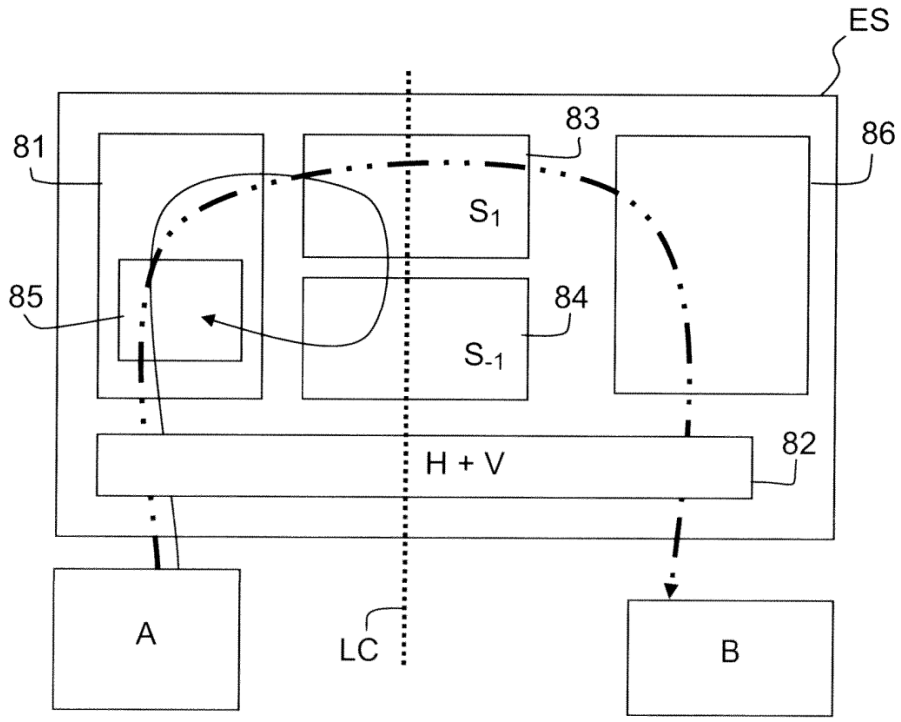
ES
81
83
86
S1
85
84
S-1
H + V
82
A
LC
B

FIG.9A

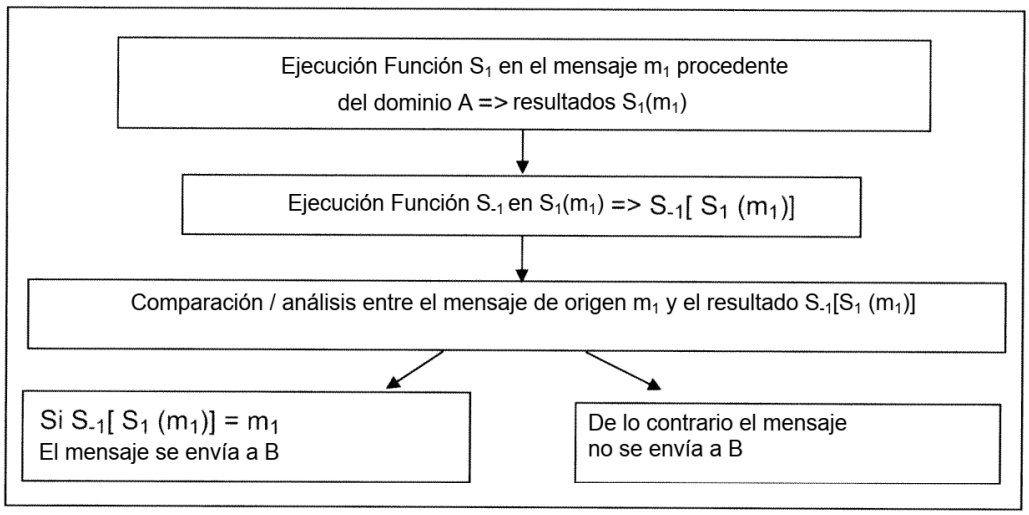
Ejecución Función S_1 en el mensaje m_1 procedente del dominio A => resultados $S_1(m_1)$
Ejecución Función S_{-1} en $S_1(m_1)$ => $S_{-1}[S_1(m_1)]$
Comparación / análisis entre el mensaje de origen m_1 y el resultado $S_{-1}[S_1(m_1)]$
Si $S_{-1}[S_1(m_1)] = m_1$ El mensaje se envía a B
De lo contrario el mensaje no se envía a B

FIG.9B

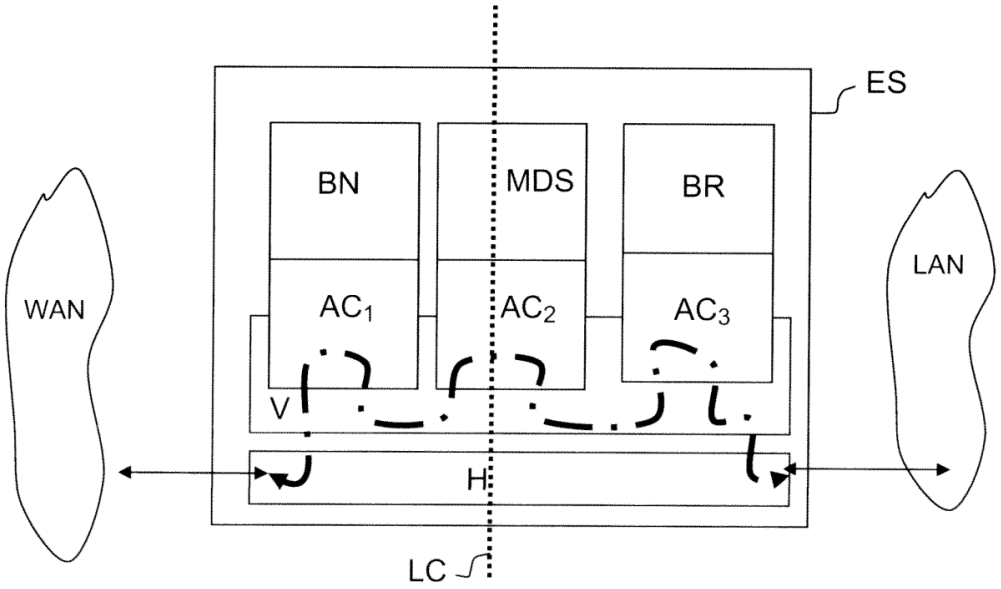
ES
BN
MDS
BR
WAN
LAN
AC_1
AC_2
AC_3
V
H
LC

FIG.10

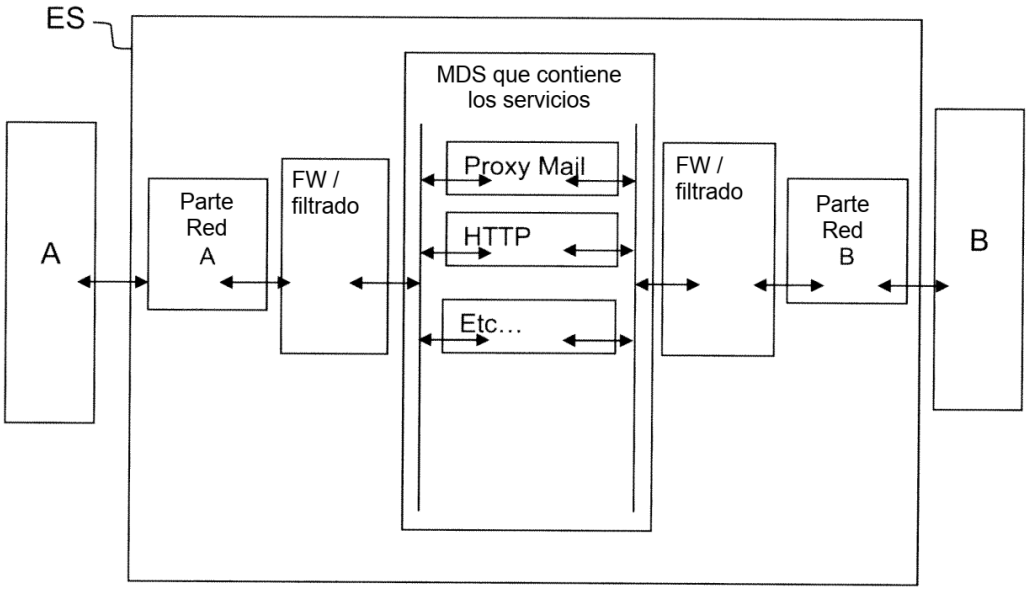
ES
MDS que contiene los servicios
Proxy Mail
HTTP
Etc…
A
Parte Red A
FW / filtrado
FW / filtrado
Parte Red B
B

FIG.11

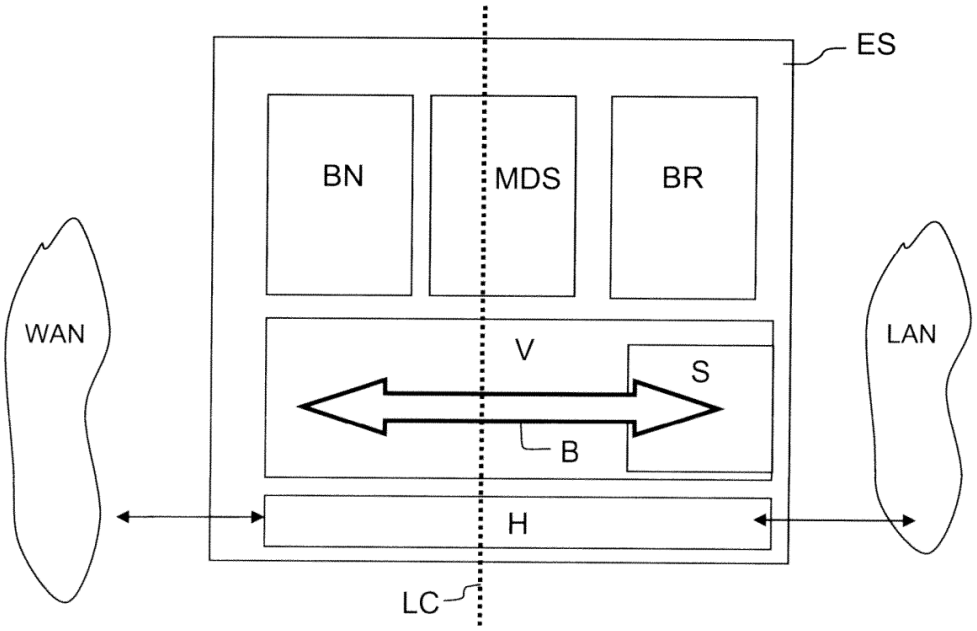
ES
BN
MDS
BR
WAN
V
S
B
H
LAN
LC

FIG.12

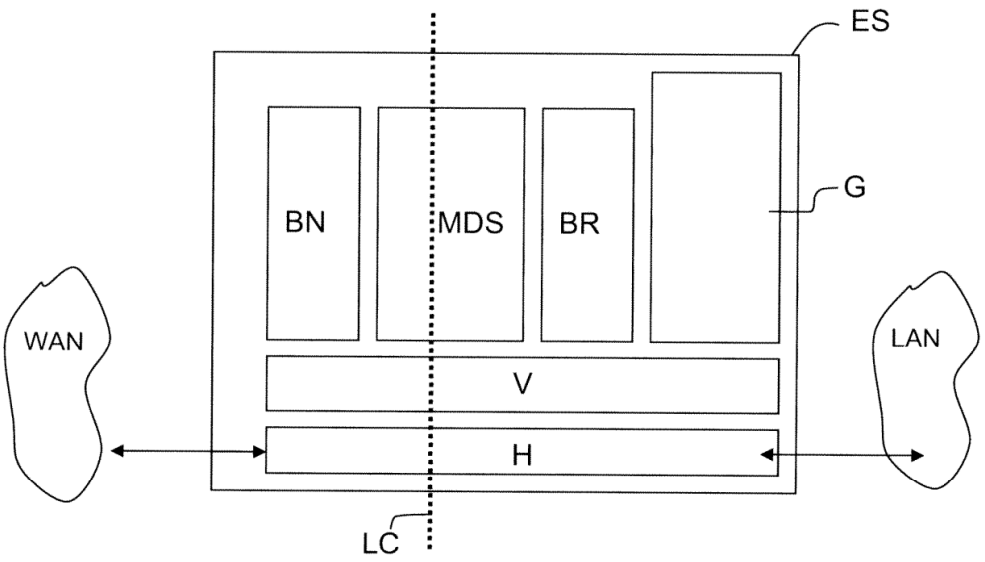
ES
BN
MDS
BR
G
WAN
LAN
V
H
LC

FIG.13

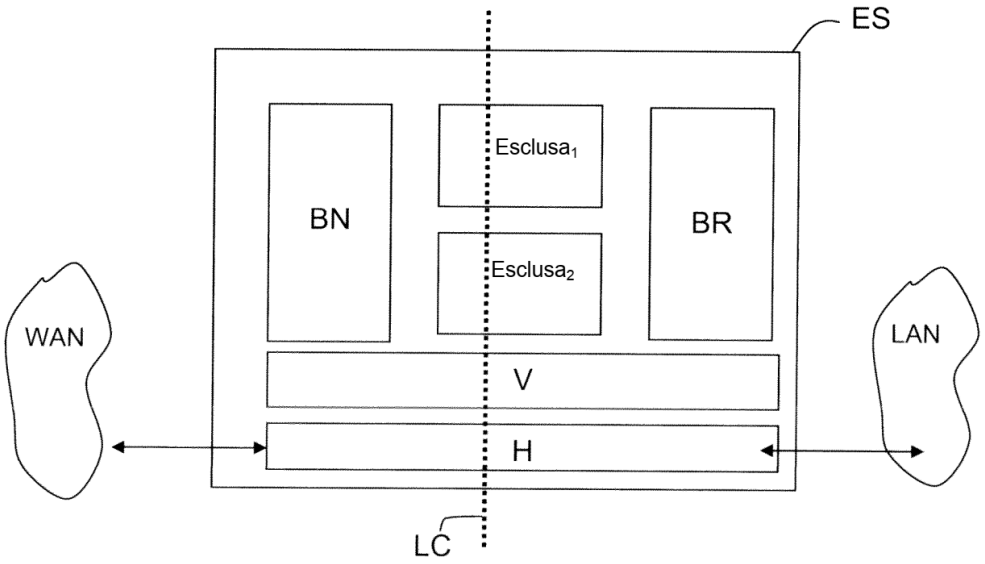
ES
BN
Esclusa1
Esclusa2
BR
WAN
LAN
V
H
LC

FIG.14

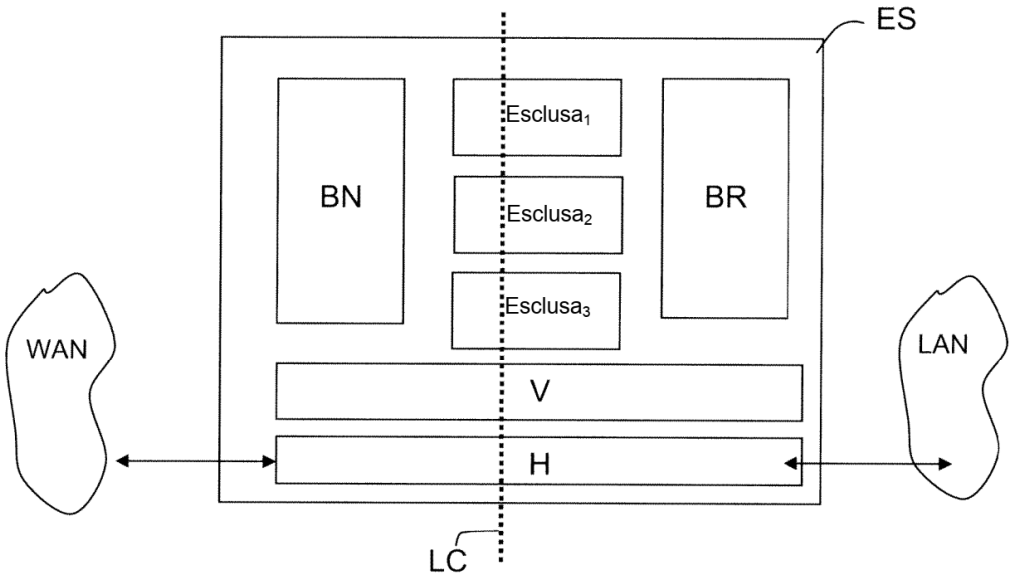

FIG.15