(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 673 938**

(51) Int. CI.:

H04L 29/06 (2006.01)
G06F 21/44 (2013.01)
H04L 29/12 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **29.05.2015 PCT/ES2015/070423**

(87) Fecha y número de publicación internacional: **03.12.2015 WO15181431**

(96) Fecha de presentación y número de la solicitud europea: **29.05.2015 E 15735721 (1)**

(97) Fecha y número de publicación de la concesión europea: **28.03.2018 EP 3151505**

(54) Título: **Procedimiento y elemento de red para acceso mejorado a redes de comunicación**

(30) Prioridad:

29.05.2014 ES 201430822

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
26.06.2018

(73) Titular/es:

TECTECO SECURITY SYSTEMS, S.L. (100.0%)
Avda. Leguario nº 49 Planta 2 Ofic. 3
28981 Parla (Madrid), ES

(72) Inventor/es:

ENRIQUE SALPICO, JOSÉ ANTONIO

(74) Agente/Representante:

CARPINTERO LÓPEZ, Mario

DESCRIPCIÓN

Procedimiento y elemento de red para acceso mejorado a redes de comunicación

Campo técnico de la invención

La presente invención tiene su aplicación dentro del sector de las telecomunicaciones y, especialmente, se refiere al acceso de equipos (dispositivos) a una red de comunicaciones. Más específicamente, la invención descrita en la presente memoria descriptiva se refiere a un procedimiento y elemento (nodo) de acceso a una red de comunicaciones que incorpora mecanismos de mejora (particularmente de seguridad).

Antecedentes de la invención

Son conocidos en el estado de la técnica, diferentes elementos o mecanismos para controlar el acceso a redes de comunicaciones, estos elementos incorporan técnicas de seguridad para que la interconexión entre los dispositivos de una red sea únicamente para los usuarios y dispositivos autorizados para acceder a la misma y bajo las condiciones permitidas. El documento US 6393484 desvela un sistema de prevención de acceso a usuarios no autorizados en redes de IP públicas de medios compartidos. Sin embargo, hasta la fecha, ninguno estos elementos/mecanismos que gestionan el acceso a la red proporciona una protección global, es decir, actualmente no se puede confirmar que exista un elemento o mecanismo de control de acceso que cubra totalmente las necesidades del usuario y de los dispositivos conectados, ya que todos los elementos/mecanismos existentes tienen serias limitaciones y vulnerabilidades, algunas de las cuales se expondrán a continuación.

Habitualmente, la identificación de usuarios autorizados se realiza a nivel de la capa 3 del modelo OSI, mediante direcciones IP o en capas superiores. Por tanto, los elementos encargados de controlar el acceso a la red (e identificar a los usuarios) deben contar con dispositivos capaces de interpretar, al menos, datos a nivel 3 y superiores del modelo OSI. Adicionalmente, la identificación basándose en de direcciones IP resulta insuficiente para garantizar la identificación de un usuario ya que cualquier usuario mediante un dispositivo cualquiera puede configurar su dirección IP sin necesidad de tener un conocimiento exhaustivo de la red, por lo que las direcciones IP son fácilmente suplantables.

Un elemento principal para proporcionar conectividad entre dispositivos de una red de comunicaciones, es el enrutador. A día de hoy, los enrutadores tienen limitaciones hardware (falta de recursos tal como memorias, procesadores, interfaces/puertos necesarios para realizar las tareas del enrutador...), limitaciones de integración y particularmente limitaciones de seguridad ya que no existe una seguridad integral de los enrutadores (para los diferentes servicios que aloja y las comunicaciones que transcurren por este). Estas limitaciones van en detrimento de la escalabilidad, adaptabilidad y confiabilidad del enrutador en cuestión.

Las limitaciones de seguridad son aquellas vulnerabilidades detectadas en la actualidad en los diferentes protocolos o estándares soportados por un dispositivo enrutador. Estas vulnerabilidades se nutren de las debilidades de los protocolos y elementos usados a la hora de establecer entornos confiables de comunicaciones. La forma de destruir las capas de seguridad establecidas por los protocolos, se ejecutan con los denominados ataques de red con el objeto de obtener habitualmente los siguientes resultados: captura de paquetes en la red de datos (Sniffers), suplantación de identidad (Spoofing), Man In the Middle o Denegación de servicio (DoS), por ejemplo.

De esta manera, por ejemplo, en redes WIFI, se pueden producir, entre otros, ataques FMS (por fuerza bruta intenta romper el protocolo criptográfico RC4 en el que se basa el protocolo WEP, Privacidad equivalente a cableado), Chop-Chop (por el cual se inyecta un paquete cambiando el último byte tratando de descifrar este valor), de fragmentación, WPS (Wifi Protected Setup, esta función, bajo los estándares IEEE 802.11i, se utiliza para la aceptación y vinculación de nuevos clientes en redes inalámbricas sin tener que introducir las propias contraseñas criptográficas del protocolo Wifi de protección, lo cual supone una exposición del enrutador a ataque de suplantaciones de identidad), pueden tener lugar entre otros.

En redes Ethernet, existen mecanismos de protección basados en el identificador de red de los dispositivos conectados al enrutador. El enrutador deniega o permite las comunicaciones entre los extremos de la comunicación basándose en unas reglas basadas en el identificador de red. La decisión de interrumpir la conexión nunca se toma basándose en el enlace físico y, por lo tanto, discrimina situaciones de protección contra ataques de denegación de servicio o un uso fraudulento del dispositivo.

En redes IPV6 se pueden producir, entre otros, ataques de Router Advertising, DNSv6 Spoofing o ataques fragmentación de paquetes. Por su parte, Por su parte, en redes WAN, algunos de los principales problemas que se presentan pueden ser de Protección Antimalware (los enrutadores no dejan de ser sistemas de software que se pueden ver afectados por código malicioso para el control y uso ilícito del dispositivo y existen vulnerabilidades críticas que permite a los intrusos tomar control de muchos de los enrutadores que dan acceso a Internet) y de Flow Label (La etiqueta de "Flow Label" sirve para dar un tratamiento diferenciado a los flujos de datos que recorre una red por medio de IPv6, esto puede usarse por competidores y personas mal intencionadas para inyectar paquetes con direcciones IPv6 falsas o etiquetas "Flow Label" adulteradas. Esto es posible ya que las cabeceras de los paquetes que pasan por los nodos intermedios no se comprueban, por lo que no existe garantía que éstos datos

sean confiables y la red simplemente asume que la fecha es confiable).

El protocolo DHCP (siglas en inglés de "Dynamic Host Configuration Protocol", protocolo de configuración dinámica de hosts), se usa ampliamente en el estado de la técnica, para la configuración de equipos que se encuentran conectados por una red de comunicaciones. A pesar de todas las útiles funciones que ofrece el protocolo DHCP, existen diversos aspectos muy negativos al utilizar este sistema, principalmente de seguridad. Algunos de estos problemas de seguridad pueden ser:

Servidor malicioso: La automatización del protocolo DHCP es un gran riesgo de seguridad que permite que un servidor DHCP malicioso sea introducido en una red, que puede interceptar la información enviada por un usuario que se conecte al servidor.

Universalización del protocolo DHCP: Como la mayor parte de enrutadores y conmutadores tienen implementado el protocolo DHCP, cualquier usuario que quiera acceder a la red podría tener fácil el acceso a la misma si usa dicho protocolo.

Múltiples subredes o segmentos de red: Existen entornos donde cada segmento de red puede necesitar su propio servidor DHCP, o un agente de retransmisión de DHCP (lo que requiere una configuración adicional, lo que representa tiempo adicional y un incremento elevado de los costes). Si ninguna opción es viable, todos los elementos de red deben ser configurados como emisores del protocolo BOOTP, que es un protocolo más antiguo y menos avanzado que el protocolo DHCP (con los consiguientes problemas) y, además, no todos los sistemas pueden soportar dicho protocolo.

Control de flujos de información: El servidor de DHCP suele utilizar los puertos 67 y 68 a través de UDP para recibir y enviar datos a los clientes. El control de dichos flujos puede llevarse a cabo por un cortafuegos pero esto no descarta a aquellos intrusos de la red que pueden capturar los paquetes relacionados con dicha información sensible y que sea usada para la suplantación de un cliente. Actualmente, el único mecanismo que ofrece un control de este tipo de intrusión sería la integración de un IDS o detector de intrusos, con el consecuente coste y que en algunos casos no compense debido al tamaño y forma de la red.

Los cortafuegos son los elementos más ampliamente usados a la hora de establecer seguridad y se basan en que todo el tráfico de entrada o de salida de una red, tiene que pasar obligatoriamente por ellos, que imponen una serie de filtrado de políticas de seguridad. Sin embargo, estos elementos distan mucho de ser la solución final a los problemas de seguridad ya que presentan diversas vulnerabilidades

La limitación más grande, que tiene un cortafuegos son los huecos de seguridad que dejan y que pueden ser descubiertos por un intruso. Los cortafuegos no son sistemas inteligentes, ellos actúan de acuerdo con parámetros introducidos por su diseñador y el administrador, si un paquete de información no se encuentra dentro de estos parámetros como una amenaza de peligro, simplemente lo deja pasar a través. Más peligro aun es que el intruso deje puertas traseras, abriendo un hueco diferente y borre las pruebas o indicios del ataque original.

Otra limitación del cortafuegos es que, si un intruso logra entrar a la organización y descubrir la contraseña o los huecos del cortafuegos y difunde esta información, el cortafuegos no se dará cuenta. Adicionalmente, los cortafuegos solo protegen redes y dispositivos, pero no protegen usuarios ni personas físicas. El cortafuegos tampoco proporciona herramientas contra la filtración de software o archivos infectados por virus, aunque es posible dotar al sistema, donde se aloja el cortafuegos, de antivirus apropiados.

Además, los cortafuegos no protegen a las personas que están dentro de la red y no actúan de manera adecuada ante técnicas tal como la ingeniería social y ataque de Insiders.

Por otro lado, existen los servidores o sistemas de autenticación o NAS (Network Access Servers), que son los servidores de red de acceso en el punto de entrada inicial a una red para la mayoría de los usuarios de servicios de red. Es el primer dispositivo en la red que presta servicios al usuario final y actúa como una puerta de entrada para todos los servicios adicionales, aplicando ciertas políticas de autenticación de los usuarios que quieren acceder a la red. Algunos de los sistemas de autenticación más ampliamente usados en la actualidad pueden ser KERBEROS, RADIUS o TACATS, por ejemplo. Sin embargo, todos los sistemas de autenticación existentes en la actualidad tienen serias limitaciones.

En resumen, se puede decir que todos los elementos y mecanismos que forman parte de la seguridad del acceso a una red (por ejemplo, enrutadores, conmutadores, cortafuegos, sistemas de autentificación, antivirus) tienen serias limitaciones de seguridad y vulnerabilidades de seguridad. Adicionalmente, la mayoría de estos elementos/mecanismos no han evolucionado prácticamente en la última década (al menos no desde el punto de vista de gestión y mejora de la seguridad). Existe, por lo tanto, la necesidad de proporcionar una solución global y eficaz que cubra totalmente las necesidades actuales del usuario y de los dispositivos de la red, sin presentar las limitaciones y vulnerabilidades de los elementos/mecanismos de acceso existentes en la actualidad.

Breve descripción de la invención

La presente invención se define en las reivindicaciones independientes. Las realizaciones preferentes se definen en las reivindicaciones dependientes. El presente procedimiento y dispositivo resuelve los problemas que presentan las soluciones del estado de la técnica, proponiendo un mecanismo mejorado de acceso a redes de comunicaciones. Un

elemento que gestiona el acceso en la red de comunicaciones (por ejemplo, un enrutador) tendrá una nueva arquitectura física y lógica que ampliará la capacidad de dicho elemento con mayor protección para la red de comunicaciones a la que da acceso. Este elemento tendrá capacidad para gestionar y proporcionar los mecanismos necesarios para la protección de las comunicaciones de entrada y salida de la red, usuarios y dispositivos.

Para ello, en un primer aspecto, la presente invención propone un procedimiento o método para el acceso mejorado de un usuario en una red de comunicaciones usando un dispositivo electrónico, en el que el procedimiento comprende las siguientes etapas realizadas en un elemento de red:

a) recibir del dispositivo electrónico un mensaje de solicitud de acceso a la red que incluye un identificador del dispositivo;
b) si dicho identificador del dispositivo se encuentra en una base de datos interna del elemento de red como identificador de un dispositivo denegado (aparece en la tabla de dispositivos denegados de dicha base interna), denegar el acceso a la red a dicho dispositivo, en caso contrario, proceder a la etapa c);
c) si el identificador del dispositivo está registrado en la base de datos como identificador de un dispositivo con acceso permitido a la red (aparece en la tabla de dispositivos autorizados de dicha base interna), proceder a la etapa d) y, en caso contrario, almacenar la identificación del dispositivo en la base de datos interna como dispositivo no autorizado, denegar el acceso a la red a dicho dispositivo;
d) recibir del dispositivo electrónico (por ejemplo, previa solicitud del elemento de red al dispositivo), un identificador del usuario y una contraseña para dicho usuario;
e) si dicho identificador del usuario se encuentra en la base de datos, como un identificador de un usuario denegado (aparece en la tabla de usuarios denegados de dicha base interna), denegar el acceso a la red a dicho dispositivo y terminar el procedimiento, en caso contrario, proceder a la etapa f);
f) autenticar al usuario, realizando al menos las siguientes comprobaciones:

f1) comprobar que el identificador de usuario aparece en la base de datos como identificador de un usuario autorizado (o registrado, es decir que aparece en la tabla de control de usuarios y contraseña) y si la contraseña recibida corresponde a la vinculada (asignada) a dicho usuario en la base de datos;
f2) comprobar que el identificador del dispositivo aparece en la base de datos como vinculado a dicho usuario;

g) si todas las comprobaciones de todas las etapas de autenticación son positivas (la comprobación de usuario, comprobación de contraseña, comprobación de vinculación y, en su caso, tiempo de comprobación de acceso, comprobación de políticas de seguridad, comprobación de una página web permitida por el analizador semántico…), otorgar (permitir) el acceso a la red, en caso contrario, almacenar la identificación del usuario en la base de datos interna como un usuario no autorizado y denegar el acceso a la red a dicho usuario;
h) si se recibe del dispositivo un mensaje de capa 2, solicitando parámetros de configuración de red (normalmente en este mensaje también estará incluido el identificador del dispositivo), una medida adicional opcional de seguridad tiene la posibilidad de comprobar otra vez en este punto si el dispositivo está registrado en la base de datos como un dispositivo con acceso permitido a la red y, en caso contrario, se almacena la identificación del dispositivo como dispositivo no autorizado y se le deniega el acceso a la red (y no se procede a la etapa i).
i) asignar un conjunto de parámetros de configuración de red al dispositivo dependiendo al menos del identificador del dispositivo y enviar dicho conjunto de parámetros de configuración de red al dispositivo (dicho conjunto de parámetros de configuración de red incluye una dirección de red (IP) para el dispositivo, en el que dicha dirección de red pertenece a un rango de direcciones de red disponibles para el dispositivo, que depende del identificador del dispositivo).

La denegación del acceso a la red (basándose en la solicitud de acceso a la red que ha hecho el dispositivo/usuario) puede ser explícita (mediante un mensaje de capa 2 al dispositivo informándole de la denegación) o implícita (sin mensaje informándole de la denegación). En ambos casos, implica que el elemento de red no le permite el acceso a la red solicitada (o no hace las acciones necesarias para proporcionar acceso a la red) al dispositivo (y usuario) o, es decir, los paquetes que envíe el dispositivo van a ser bloqueados en el enrutador (y no van a alcanzar la red o no van a salir de la red si es tráfico de salida de la misma). Y, obviamente, como es lógico, si se llega un punto en que se deniega el acceso a la red, no se sigue con el resto de las comprobaciones y etapas del procedimiento.

Todas las comunicaciones entre el dispositivo y el enrutador descritas anteriormente se realizan mediante mensajes de capa 2 del modelo OSI; es decir o, en otras palabras, el control de acceso expuesto se hace en la capa 2 (capa de enlace de datos) del modelo OSI.

La etapa d) puede incluir: cuando se recibe del dispositivo electrónico un mensaje de capa 2 que incluye una solicitud de acceso a la red y un identificador del dispositivo, enviar al dispositivo un mensaje de capa 2 solicitando un identificador del usuario y una contraseña para dicho usuario y recibir del dispositivo un mensaje de capa 2 incluyendo un identificador del usuario y la contraseña para dicho usuario.

En una realización, en la que la etapa de autenticación del usuario además comprende las siguientes etapas de autenticación tras la etapa f2) y antes de la etapa g):

f3) obtener la hora (y opcionalmente la fecha) en que se está produciendo el acceso (la solicitud de acceso) y comprobar que dicha hora (y/o fecha) está dentro de los tiempos de acceso permitidos para dicho usuario y/o para dicho dispositivo, almacenados en la base de datos interna (por ejemplo, si el acceso se produce fuera de los tiempos de acceso permitidos o no aparecen tiempos de acceso permitidos para dicho usuario en la base de datos interna, la comprobación sería negativa) y/o
f4) comprobar que el acceso a la red que solicita el usuario está permitido por las políticas (416) de seguridad definidas para dicho usuario almacenadas en la base de datos interna;

Para obtener la fecha y hora para realizar la etapa f3) o para otras funciones (por ejemplo, conocer la edad actual del usuario, a partir de su fecha de nacimiento), se puede usar un servicio NTP.

En una realización, si el usuario es menor de edad se realizan las siguientes acciones después de la etapa f2):

- clasificar al usuario en una categoría determinada de acuerdo con la edad del usuario;
- comprobar si la página web a la que quiere acceder el usuario (si es que quiere acceder a alguna página web de acuerdo con la solicitud de acceso) está clasificada como accesible para dicha categoría en la que se ha clasificado al usuario, en la que para clasificar una página web como accesible dependiendo de la edad del usuario se realiza un análisis del contenido semántico de dicha página web. Si está clasificada como no accesible, denegar el acceso (a dicha página web). Al nivel de base de datos externa, existirá un módulo del servicio o sistema de clasificación de contenido que es el encargado de nutrir al analizador semántico, con el contenido de las páginas webs que este debe analizar.

En una realización, la etapa i) comprende:

i1) asignar al dispositivo un segundo perfil de acceso obtenido de la base de datos, en función del identificador de dicho dispositivo;
i2) asignar al dispositivo un conjunto de parámetros de configuración de red en función del segundo perfil de acceso asignado al mismo, incluyendo dicho conjunto de parámetros de configuración de red una dirección de red para el dispositivo; dicha dirección de red asignada puede otorgar un acceso restringido a la red, dependiendo del rango de direcciones de red a la que pertenezca dicha dirección asignada;
i3) enviar un mensaje de capa 2 al dispositivo con los parámetros de configuración de red asignados al dispositivo.

El acceso restringido a la red puede comprender al menos una de las siguientes restricciones:

- denegación de la emisión de datos al dispositivo;
- denegación de comunicación con el resto de dispositivos de la red;
- denegación de acceso a al menos un puerto;
- denegación de comunicación mediante al menos un protocolo;
- autorización de acceso únicamente a Internet;
- acceso a la red dentro de un determinado periodo de tiempo.

Si la información de antivirus del dispositivo ha cambiado, se puede cambiar el segundo perfil asignado al dispositivo y, por lo tanto, por lo tanto, el rango de direcciones de red disponibles para el mismo. Por ejemplo, si el dispositivo ahora está infectado por un virus o ha dejado de ser es correcta la versión de antivirus que tiene instalada el dispositivo, se le asignará un perfil más restrictivo y si el dispositivo ha dejado de estar infectado por un virus o ya es correcta la versión de antivirus que tiene instalada el dispositivo, se le asignará un perfil menos restrictivo. Opcionalmente, si el dispositivo ahora está infectado por un virus o ha dejado de ser es correcta la versión de antivirus que tiene instalada el dispositivo, se le deniega el acceso a la red al dispositivo.

La etapa i2) puede comprender:

i21) obtener de la base de datos, en función del segundo perfil de acceso asignado al mismo, un conjunto de parámetros de configuración de red disponibles para el dispositivo, incluyendo dichos parámetros un rango de direcciones de red disponibles para el dispositivo;
i22) enviar un mensaje de capa 2 al dispositivo, incluyendo dichos parámetros de configuración de red disponibles para el dispositivo;
i23) recibir del dispositivo un mensaje de capa 2, con los parámetros de configuración escogidos por el dispositivo de entre los parámetros de configuración de red disponibles enviados en la etapa i22, en la que dichos parámetros de configuración escogidos incluyen una dirección de red del conjunto de direcciones de red disponibles para el dispositivo y asignar al dispositivo los parámetros de configuración escogidos recibidos en la etapa.

En una realización, el procedimiento además comprende:

j) obtener periódicamente la ubicación del elemento de red;
k) comparar dicha ubicación con la anterior ubicación obtenida (o con un rango de ubicaciones permitidas) y si no coincide, bloquear el acceso a la red del elemento de red.

l) obtener periódicamente la ubicación del dispositivo, comparar dicha ubicación con un rango de ubicaciones permitidas y si no coincide, denegar el acceso a la red del dispositivo, y, opcionalmente, añadir la ubicación del dispositivo a todos los paquetes procedentes del dispositivo.

Opcionalmente, se puede añadir la ubicación del elemento de red a todos los paquetes procedentes de cualquier dispositivo electrónico que acceda a la red a través del elemento de red.

En una realización, para permitir el acceso a la red (por primera vez, es decir, cuando se registra en la red), el elemento de red le pide al usuario información de usuario y si el usuario no proporciona dicha información, el elemento de red le deniega el acceso a la red; en la que esta información de usuario incluye al menos uno de los siguientes parámetros: nombre completo del usuario, dirección postal, DNI, número de pasaporte, fecha de nacimiento y toda la información acerca del usuario que se encuentra en la base de datos interna, el elemento de red la envía dicha información a una base de datos externa a nivel mundial (para la gestión, sincronización y control de los usuarios a nivel mundial). Esta información puede enviarse a través de una red de comunicaciones externa (por ejemplo, Internet).

Los mensajes recibidos del y enviados al dispositivo en la etapa i) pueden ser mensajes de multidifusión, que usan una dirección de multidifusión de capa 2 de la red.

En un segundo aspecto, la presente invención propone un elemento de red (un enrutador, un conmutador, cortafuegos o splitter o cualquier otro elemento de red que pertenece a la red de comunicaciones y gestiona el acceso a la red de comunicaciones) para el acceso mejorado de un usuario a una red de comunicaciones usando un dispositivo electrónico, en el que el elemento de red comprende:

- una base de datos que comprende:
    - una tabla de identificadores de dispositivos con acceso denegado a la red y una tabla de identificadores de usuarios con acceso denegado a la red, una tabla de identificadores de usuarios autorizados que incluye la contraseña vinculada a cada usuario, una tabla de identificadores de aquellos dispositivos que tienen acceso autorizado a la red, una tabla de identificadores de usuario que están vinculados a cada identificador de dispositivo con acceso autorizado a la red y una tabla con el conjunto de parámetros de configuración de red disponibles para cada identificador de dispositivo con acceso autorizado a la red, en el que el conjunto de parámetros de configuración de red disponibles comprende un rango de direcciones de red disponibles para cada perfil;
- medios para recibir del dispositivo una solicitud de acceso a la red, un identificador del dispositivo, un identificador del usuario, una contraseña para dicho usuario
- medios para recibir del dispositivo un mensaje de capa 2, solicitando parámetros de configuración de red para acceder a la red;
- un procesador configurado para:
    - comprobar si dicho identificador del dispositivo se encuentra la tabla (registro) de dispositivos con acceso denegado a la red y, si es así, denegar el acceso a la red a dicho dispositivo;
    - comprobar si el identificador del dispositivo está registrado en la tabla de identificadores de aquellos dispositivos que tienen acceso autorizado a la red, si la comprobación es negativa, denegar el acceso a la red y almacenar la identificación del dispositivo en la tabla de dispositivos con acceso denegado a la red;
    - comprobar si dicho identificador de usuario se encuentra en la tabla de usuarios con acceso denegado a la red y, si es así, denegar el acceso a la red a dicho dispositivo;
    - autenticar al usuario, realizando al menos las siguientes comprobaciones:
        - comprobar que el identificador de usuario aparece en la tabla de usuarios autorizados y la contraseña recibida corresponde a la vinculada a dicho usuario en dicha tabla;
        - comprobar que el identificador del dispositivo aparece en la base de datos como vinculado a dicho usuario;
    - si alguna de las comprobaciones de autenticación es negativa, almacenar la identificación del usuario en la tabla de usuarios con acceso denegado a la red y denegar el acceso a la red a dicho usuario;
    - al recibir del dispositivo el mensaje solicitando parámetros de configuración de red, - comprobar si el identificador del dispositivo está registrado en la tabla de identificadores de aquellos dispositivos que tienen acceso autorizado a la red, si la comprobación es negativa, almacenar la identificación del dispositivo en la tabla de dispositivos con acceso denegado a la red y denegar el acceso a la red a dicho dispositivo y, si la comprobación es positiva, asignar un conjunto de parámetros de configuración de red al dispositivo dependiendo al menos del identificador del dispositivo;
- medios para enviar un mensaje de capa 2 al dispositivo con los parámetros de configuración de red asignados al dispositivo.

Finalmente, en un cuarto aspecto de la invención se presenta un programa de ordenador que comprende

instrucciones ejecutables por ordenador para implementar el procedimiento descrito, al ejecutarse en un ordenador, un procesador digital de la señal, un circuito integrado específico de la aplicación, un microprocesador, un microcontrolador o cualquier otra forma de hardware programable. Dichas instrucciones pueden estar almacenadas en un medio de almacenamiento de datos digitales.

Aspectos, realizaciones y detalles adicionales, específicos y preferentes, de la invención se enuncian en las reivindicaciones adjuntas, independientes y dependientes. Para un entendimiento más completo de la invención, sus objetos y ventajas, puede tenerse referencia a la siguiente memoria descriptiva y a los dibujos adjuntos.

Descripción de los dibujos

Para completar la descripción que se está haciendo, y con el objeto de asistir para una mejor comprensión de las características de la invención, de acuerdo con un ejemplo preferente de realización práctica de la misma, que acompaña dicha descripción como una parte integral de la misma, hay un conjunto de dibujos en los cuales, a modo de ilustración y no de manera restrictiva, ha sido representado lo siguiente:

La Figura 1 muestra un diagrama esquemático del funcionamiento de la denegación implícita en varios escenarios de acuerdo con una realización de la presente invención.
La Figura 2 muestra de manera esquemática un posible ejemplo de tabla de control de usuario y contraseña, de acuerdo con una realización de la presente invención.
La Figura 3 muestra de manera esquemática un posible ejemplo de tabla de control de dispositivos y usuarios, de acuerdo con una realización de la presente invención.
La Figura 4 muestra de manera esquemática un posible ejemplo de tabla de políticas de seguridad de acuerdo con una realización de la presente invención.
La Figura 5 muestra un diagrama de bloques de la arquitectura del mecanismo SDHCP propuesto de acuerdo con una realización de la presente invención.
La Figura 6 muestra un diagrama de mensajes intercambiados, entre un dispositivo o equipo cliente y un servidor SDHCP, en el caso de que dicho dispositivo no esté registrado en la base de datos interna, de acuerdo con una realización de la presente invención.
La Figura 7 muestra un diagrama de mensajes intercambiados, entre un dispositivo o equipo cliente y un servidor SDHCP para la obtención de los parámetros de red, en el caso de que dicho dispositivo esté registrado en la base de datos interna, de acuerdo con una realización de la presente invención.
La figura 8 muestra de manera esquemática la interacción entre los distintos elementos de la solución propuesta de acuerdo con un ejemplo de realización de la presente invención.

Descripción detallada de la invención

La presente invención propone un mecanismo mejorado de acceso a una red de comunicaciones. El elemento principal de este mecanismo será un elemento de red (también llamado nodo de red o dispositivo de red) que gestiona el acceso (de entrada, o salida) a la red de comunicaciones. Este elemento de red puede ser un enrutador, aunque en otras realizaciones puede ser otro tipo de elemento de red tal como, por ejemplo, un conmutador que opera en la capa 2 del modelo OSI u otro tipo de nodos que gestionan de alguna manera el acceso a la red. La presente invención propone una nueva arquitectura física y lógica para dicho elemento de red (que será programable con carácter distribuido, es decir, constituidos por varios componentes de hardware y software, para facilitar la implementación, escalabilidad y extensibilidad), que ampliará la capacidad de dicho elemento con mayor protección para la red de comunicaciones a la que da acceso. Este elemento tendrá capacidad para gestionar y proporcionar los mecanismos necesarios para la protección de las comunicaciones, protección de usuarios y dispositivos sin la colaboración de sistemas finales (es decir, de manera transparente para dichos sistemas finales).

Los dispositivos que quieren acceder a la red pueden ser ordenadores, tabletas, ordenadores personales, teléfonos móviles, teléfonos inteligentes, ordenadores portátiles y en general cualquier equipo o dispositivo electrónico que pueda conectarse a una red de comunicaciones.

La red de comunicaciones (por ejemplo, una red de datos) puede ser de cualquier tipo tanto desde el punto de vista de su estructura (puede ser una red de área local, LAN, una red de área extendida, WAN, o de cualquier otro tipo de red) y de la tecnología de comunicación que usa (puede ser una red cableada, una red WIFI, una red de telefonía móvil o usar cualquier otro tipo de tecnología de comunicaciones). Asimismo, puede ser una red privada o pública. Normalmente funcionará bajo el modelo OSI (del inglés "Open System Interconnection", en español "Sistema de Interconexión Abierto") y pila TCP/IP.

Este nuevo sistema de acceso global, presenta importantes retos a la hora de conseguir un comportamiento coordinado entre el elemento de red (por ejemplo, el enrutador), el dispositivo o equipo que quiere acceder a la red y el usuario en lo referente a la seguridad y protección de cada uno de ellos. Para ello se proponen varios mecanismos de comunicación enrutador, dispositivo y usuario. El desarrollo del mecanismo de control y gestión de la seguridad a nivel individual del usuario que accede a la red, que puede ser una persona física o un objeto (en el campo de "Internet de las Cosas" o IoT) define una interfaz abierta entre el plano de control y el plano de datos del enrutador.

Este elemento de red (enrutador) controlará el acceso a una red de comunicaciones (por ejemplo, una LAN) tanto de

entrada como de salida. En otras palabras, controlará el acceso desde una red (por ejemplo, Internet) o equipo (dispositivo) externo a la red de comunicaciones, que intenta acceder a la red de comunicaciones o desde un equipo que está en la red de comunicaciones y que intenta comunicarse con otro equipo de la red o con una red externa a la red de comunicaciones. En otras palabras, controla el uso de la red de comunicaciones para comunicarse con dispositivos o servicios de dentro o de fuera de la red.

Para ello, se define un modelo de los recursos del elemento de red y se identifican las funcionalidades de cada uno de los componentes. Se establece una jerarquía de confianza en tres niveles del elemento de red siendo el nivel 1 constituye el nivel más alto. Cada nivel de seguridad está compuesto por mecanismos, protocolos y tablas dinámicas o estáticas, estas tablas trabajan independientemente, pero todas ellas se sincronizan entre sí, con esto conseguimos un alto nivel de coordinación y seguridad. Estos niveles son: nivel 1 (Lógica de Enrutador, también llamado de denegación Implícita), nivel 2 (base de datos interna) y nivel 3 (base de datos externa, también llamada base de datos de acceso externo). Estos niveles jerárquicos se definen en el elemento de red para especificar mejor su funcionamiento, pero no hay que confundirlos con las capas del modelo OSI.

Los tres niveles de seguridad están sincronizados entre sí, pero el nivel 3 no podrá acceder a la base de datos de los niveles 1 y 2. Se ha desarrollado así porque el nivel 1 tiene datos que están expuesto al exterior (Internet) y para incrementar la seguridad se les deniega el acceso a los niveles 1 y 2. En otras palabras, los niveles 1 y 2 tienen acceso al resto de los niveles, pero el nivel 3 no tiene acceso a los datos de los niveles 1 y 2.

Nivel 1: Lógica de Enrutador (Denegación Implícita)

En este nivel se engloba los mecanismos para la denegación de dispositivos, usuarios y servicios, a los que se les llama de denegación implícita. La denegación implícita es el mecanismo por el cual el mecanismo o sistema de seguridad desarrollado deniega el acceso a cualquier dispositivo o usuario (persona física) que no esté registrado en la base de datos interna (BBDD) (del nivel 2), no contestando el enrutador a los mensajes de multidifusión de mensajes que provengan de un equipo o usuario, cuyo acceso haya sido denegado (porque no está en la base de datos interna del enrutador); con esto se consigue que el enrutador sea invisible a cualquier elemento o dispositivo que no esté en la lista de elementos confiables, (es decir, en la base de datos interna). Se trata de un mecanismo implícito debido a que no existe ninguna expresión ni configuración especifica del sistema. Con este mecanismo se otorga al equipo de inteligencia ya que es capaz de tomar decisiones sin la necesidad de interactuar con el ser humano.

La lógica de enrutador genera automáticamente los campos necesarios para aplicar una configuración segura, esto quiere decir que los campos de registros se generan automáticamente con la información y el tráfico existente en la red, que proporciona el sistema de autenticación, el protocolo de configuración dinámica de anfitriones y el sistema de geolocalización, por lo tanto, no es imprescindible la interlocución del ser humano. Para ello, el enrutador registra la actividad de todos los servicios, sistemas, dispositivos y usuarios que quieren acceder a la red y, en general, de las comunicaciones entrantes y salientes de la red y decide si las permite o no. Adicionalmente, basándose en este registro de actividad, se generan tablas en los contenedores que componen la lógica del enrutador. De esta manera, por ejemplo, cuando un usuario quiere acceder a la red y no está registrado, esta actividad se registra en el contenedor de "REGISTRO DE USUARIOS DENEGADOS" si por el contrario es un dispositivo que no está registrado, la actividad de este dispositivo se registra en el contendor de "REGISTROS DE DIRECCIONES MAC NO PERMITIDAS". El administrador de sistema recibirá periódicamente la información necesaria para la gestión de la lógica de enrutador. En otras palabras, en otras palabras, el administrador de la red recibe toda la información que genere el nivel 1 de "lógica de enrutador" y es el que decide qué hacer con dicha información (si es necesario realizar alguna acción a partir de dicha información). Por ejemplo; cuando un usuario ha olvidado su contraseña o simplemente ha caducado, esta actividad queda registrada en el contenedor de "REGISTROS DE USUARIOS DENEGADOS" y se le informará al administrador que el usuario que ha sido denegado se ha denegado el acceso porque ha caducado a la contraseña de dicho usuario, el administrador en este caso podrá otorgar al usuario una nueva contraseña, para poder acceder a la red.

La denegación implícita es un mecanismo totalmente automático de defensa que protege al enrutador contra los ataques de denegación de servicio. Las reglas implícitas, son un conjunto de reglas predefinidas para mayor protección. Estas reglas deniegan el acceso de usuarios y dispositivos que han sido denegados, por ejemplo, bien por el sistema de autenticación, por el protocolo de SDHCP (siglas en inglés de "Secure Dynamic Host Configuration Protocol", protocolo seguro de configuración dinámica de hosts) y por el sistema de geolocalización tal como se describirá más adelante. En otras palabras, se nutre de la información que proporciona el sistema de autenticación con los usuarios que no tienen acceso a red, con los denegados por el protocolo SDHCP y con el sistema de geolocalización que no están registrados en la BBDD. Basándose en la información que recibe y que se envía a las tablas de registros, el campo de reglas dentro de la denegación implícita decidirá si que usuario o el dispositivo tiene que ser eliminado del sistema de protección (es decir, se le deniega el acceso).

Las reglas que componen la denegación implícita deciden:

- Denegar el acceso temporalmente o permanentemente de un usuario.
- Denegar el acceso temporalmente o permanentemente de un dispositivo.

■ Cerrar los puertos del enrutador automáticamente y físicamente a los dispositivos que han sido denegados permanentemente (reabriendo automáticamente los puertos del enrutador para los dispositivos que están registrados).
■ Denegar el acceso a los dispositivos (y el elemento de red) si no cumplen con la normativa de geolocalización.

La denegación implícita no se aplica hasta que no se haya realizado la primera configuración del elemento de red (por ejemplo, el enrutador), una vez que se realice esa primera configuración, el sistema la aplicará por defecto de acuerdo con los parámetros de configuración del administrador del sistema.

Una de las ventajas de este mecanismo de denegación implícita, es que impide los ataques de denegación de servicio; estos ataques tienen como objeto imposibilitar el acceso a los servicios y recursos de la red durante un periodo determinado y el acceso no permitido a la red. Uno de estos ataques es el ataque "por saturación", en el que desde uno o varios dispositivos (maliciosos) se le envían a un elemento de la red (enrutador, conmutador…) de la red, de manera intencionada, un número tan alto de solicitudes que el elemento se satura y no puede responder a las solicitudes reales (es decir, a solicitudes de dispositivos de usuarios reales que quieren acceder a la red). Adicionalmente, al saturarse, el equipo que recibe el ataque normalmente se reinicia y es cuando el dispositivo agresor puede acceder a él y/o a la red. Usando el mecanismo propuesto por la presente invención, la denegación por defecto que se aplica en la capa baja del elemento de red atacado (por ejemplo, un enrutador) previene tales ataques, ya que el enrutador deniega el acceso a todos los dispositivos que no estén registrados en su base de datos interna. En otras palabras, usando el mecanismo propuesto, si el enrutador recibe una solicitud de un dispositivo o usuario al que ya se le haga denegado el acceso previamente, el enrutador ya ni siquiera le responde con una denegación, sino que hace caso omiso del mensaje. Esto da como resultado que por muchos mensajes que reciba el enrutador desde un dispositivo (en un intento de saturarlo), como ya a hace caso omiso de ellos, el enrutador no se va a saturar ni reiniciar, de tal manera que el ataque no tendría éxito.

Este mecanismo de denegación implícita se basa en al menos cuatro tablas (o registros, tal como son el registro de direcciones MAC, el registro de direcciones MAC denegadas, el registro de usuarios denegados y el registro de geolocalización (también llamado de coordenadas GPS).

- Registro (104) de direcciones MAC (también llamada registro de direcciones MAC autorizadas o permitidas o registro de dispositivos autorizados o permitidos):

Aquí se almacenan el identificador (normalmente la dirección MAC, de ahí su nombre, aunque puede ser otro identificador tal como el IMEI, MSISDN, IMSI, LTE_ID…) de los dispositivos (equipos) a los que está permitido el acceso a la red. Si el identificador del dispositivo no se encuentra en esta tabla, se considerará que el dispositivo no pertenece a la red (no tiene acceso permitido a la red).

Además del identificador principal (por ejemplo, la dirección MAC del equipo), este registro puede contener otras identificaciones del dispositivo (tal como el IMEI, IMSI, MSISDN o cualquier otro parámetro que identifique el dispositivo), es decir, almacena no sólo el identificador principal de los equipos autorizados sino también alguno o algunos de estos otros identificadores. En ciertos escenarios, en vez de la dirección MAC, el dispositivo puede enviar uno de estos otros identificadores; en esos casos la tabla se comprobará de igual manera, pero partiendo de este identificador del dispositivo, en vez de la dirección MAC del dispositivo.

Este registro se encuentra en la base de datos interna y, por lo tanto, se puede decir que pertenece al nivel 2 de seguridad del dispositivo (aunque es accesible desde el nivel 1).

En este registro, se registran automáticamente los identificadores de cualquier dispositivo que el enrutador considere que tiene acceso autorizado a la red (por ejemplo, porque aparezca en otros registros como autorizado, como se verá más adelante) se registran automáticamente. A su vez el administrador de la red puede introducir en esta tabla los identificadores de los dispositivos que él considere que deben tener acceso autorizado a la red (esto se puede hacer previamente a la iniciación del enrutador o durante su funcionamiento). Este registro permite abrir todos los puertos del enrutador. Todos los dispositivos que están registrados correctamente en esta tabla, tienen la capacidad de abrir los puertos físicos del enrutador que estén cerrados, si están en este registro, sin interactuar con el enrutador (es decir, sin tener que solicitárselo al enrutador).

Como se explicará más adelante, cuando un dispositivo que no está registrado en la base de datos, intenta acceder a la red, el enrutador lo registra en el "REGISTRO DE DIRECCIONES MAC DENEGADAS". Cuando dicho dispositivo intenta acceder más de un número determinado de veces (por ejemplo, tres), el mecanismo de denegación implícita cierra el puerto por el que quiere acceder físicamente porque entiende que es atacado por este dispositivo. Para cerrar el puerto físicamente usa por ejemplo el comando "port ETH1 shutdown", suponiendo que el puerto a cerrar es el puerto ETH1. Cuando un dispositivo confiable (es decir, que está registrado en este registro de direcciones MAC permitidas), quiere acceder a la red por el puerto que está cerrado (ETH1), el sistema de denegación implícita, al detectar corriente en el puerto, comprueba la dirección MAC del dispositivo y abre el puerto automáticamente con el comando "set policy ide mac xx.xx.xx.xx port not shutdown". Esta acción la realiza automáticamente la Denegación Implícita ya que se nutre de la información generada por el enrutador, es decir cuando la dirección MAC no está registrada el enrutador (e intenta acceder a la red más de un número determinado

de veces) realiza el comando de cierre automáticamente y si por el contrario la dirección MAC sí está registrada el enrutador realiza el comando de apertura automáticamente.

- Registro (108) de direcciones MAC denegadas:

En este campo, se registra automáticamente el identificador (normalmente, la dirección MAC, de ahí su nombre, aunque puede ser otro identificador tal como el IMEI, MSISDN, IMSI, LTE, ID…) de todos los equipos (dispositivos) de usuario que no tienen registradas sus identificadores de red como autorizados en la BBDD interna y/o han sido rechazados por el protocolo SDHCP (como se explicará más adelante). En otras palabras, cuando se recibe un intento de acceso de un dispositivo de usuario se comprueba si su dirección MAC (u otro identificador) está registrado en la base de datos interna como dispositivos autorizados. Si no es así, se registrará automáticamente como denegado en este registro. Igualmente, cuando se recibe una solicitud de acceso a la red de un equipo de usuario y se deniega mediante el protocolo SDHCP (como se explicará más adelante), pues también se registrará dicho equipo como denegado en este registro. Cuando se recibe un intento de acceso o una solicitud de acceso de un dispositivo que esté en esta tabla de dispositivos denegados (direcciones MAC denegadas), ya el enrutador le denegará automáticamente el acceso al dispositivo mediante denegación implícita (es decir, no contesta al dispositivo para permitirle el acceso, y el dispositivo no podrá acceder a la red).

En la figura 1 se muestra la metodología y funcionamiento del nivel 1 y la denegación implícita en varios escenarios/situaciones de denegación de acceso a la red.

A continuación, se explicará el escenario en que la dirección MAC del dispositivo no está registrada (y el usuario no solicita previamente la asignación de dirección IP, usando por ejemplo el protocolo SDHCP).

En un escenario, por ejemplo, por ejemplo, el equipo (102) o dispositivo 1 pertenece a un usuario (con alto conocimiento de las redes) que para acceder a la red no necesita solicitar los parámetros de configuración de red al protocolo SDHCP, con lo cual el usuario se asigna manualmente los parámetros de la red (dirección IP, máscara de red y puerta de enlace). Una vez que el usuario acceda a la red, el enrutador comprobará la dirección MAC del dispositivo y una vez realizada la comprobación verá que la MAC del dispositivo no está registrada (106) en la BBDD interna, no se le permite el acceso y automáticamente el enrutador enviará la información de la dirección MAC a la tabla de registro (108) de direcciones MAC denegadas, y el dispositivo no podrá acceder la próxima vez tampoco a la red porque será automáticamente rechazado por el mecanismo (112) de denegación implícita.

En otras palabras, cuando un dispositivo intenta acceder a la red, se hace una doble comprobación. En primer lugar, se comprueba si está registrado en el registro de direcciones MAC denegadas. Si es así, no se contestará ni tramitará el acceso, por lo que no podrá acceder a la red (denegación implícita). Si no está en este registro, se comprueba si está en el registro de direcciones MAC autorizadas. Si no es así, entonces se registrará el identificador en el registro de direcciones MAC denegadas y se le denegará el acceso. Esta primera denegación de acceso, es decir, cuando el dispositivo no está en el registro de dispositivos denegados, pero tampoco en el registro de dispositivos autorizados puede ser denegación implícita (es decir, no se le contesta al dispositivo y no se le permite el acceso) o una denegación explícita (se le envía un mensaje al dispositivo, informándole de que se le deniega el acceso).

Para mayor seguridad, en una realización, cuando el dispositivo intenta acceder a la red más de un número de veces, automáticamente el enrutador considera que la red está siendo amenazada y cierra el puerto físicamente (por ejemplo, mediante la instrucción "port ethe1 shutdown"). Una vez que el sistema ha cerrado el puerto físicamente y permanentemente, solo podrá abrir el puerto automáticamente cuando acceda un dispositivo que este registrado en la BBDD (por ejemplo, mediante la instrucción "port eth1 no shutdown 68:76:4F:BF:6A:0F") es decir, todos los dispositivos que estén registrados en la BBDD interna (en el registro de direcciones MAC autorizadas) tendrán la capacidad de abrir los puertos automáticamente.

Esta política de apertura y/o cierre de puertos las genera automáticamente el enrutador a partir de la información que recibe de las bases de datos internas. En otras palabras, si, por ejemplo, si, por ejemplo, de acuerdo con la base de datos interna figura que la dirección MAC "YYY" está autorizada, el enrutador puede generar una política de apertura de puerto que sea "enrutador № 1 set pólice id mac YYY ports not shutdown" y así para el dispositivo que tenga dicha dirección MAC el puerto estará abierto y habilitado cuando acceda a la red. Una instrucción análoga existirá para serán todas las direcciones MAC que estén en la tabla de direcciones MAC autorizadas.

Algo similar ocurre cuando se solicita previamente la asignación de dirección IP, usando, por ejemplo, el protocolo SDHCP y la dirección MAC no está registrada. El dispositivo 1 (102) solicita los parámetros de configuración de red, esta solicitud es recibida por el servidor (105) SDHCP, que puede ser el propio enrutador. El enrutador aplicando el protocolo SDHCP, realiza las comprobaciones necesarias y comprueba que el dispositivo (106) no está registrado en la BBDD, y enviará la información de la dirección MAC a la tabla de registro (108) de direcciones MAC denegadas. Una vez que la dirección MAC esté en el registro, la próxima vez que el dispositivo solicite los parámetros de red al protocolo SDHCP, el enrutador verá que la dirección MAC del dispositivo está en el registro de direcciones MAC denegadas y esta solicitud será rechazada por el sistema (112) de denegación implícita.

Una vez que el enrutador ha registrado al usuario en el registro de direcciones MAC denegados, dicho dispositivo al

volver a solicitar el acceso a la red, esta solicitud no llegara al sistema SDCHCP ya que la solicitud está denegada por el sistema de denegación implícita.

- Registro (107) de usuarios denegados:

En esta tabla (o registro), se registra automáticamente todos los usuarios que no están registrados en la BBDD interna o han sido denegados por el sistema de autenticación. Cuando se recibe un intento de acceso de un usuario que esté en esta tabla, ya el enrutador le denegará automáticamente el acceso mediante denegación implícita (es decir, no le contesta al dispositivo por lo que el dispositivo no podrá acceder a la red).

En la figura 1 también se muestra la metodología y funcionamiento del nivel 1 y la denegación implícita, con un usuario no registrado.

El usuario 1 (101), solicita acceso a la red, el sistema (103) de autenticación realiza las comprobaciones necesarias (que se explicarán más adelante) y comprueba que la autenticación es negativa, con lo cual es sistema de autenticación envía la información del usuario a la tabla de registros (107) de usuarios denegados que se encuentra en el nivel 1 de la capa de seguridad. La información queda almacenada en dicha tabla por un tiempo predeterminado, este tiempo es configurable por el administrador.

Una vez que se ha registrado el usuario en la tabla de registros de usuarios denegados, dicho usuario al volver a solicitar el acceso a la red, esta solicitud no llegara al sistema de autenticación ya que la solicitud esta denegada por el sistema (112) de denegación implícita.

Una vez que el usuario 1 no se encuentre en la tabla de registros de usuarios denegados, el usuario 1 podrá solicitar el acceso a la red al sistema de autenticación.

Existen dos formas de que el usuario 1 no esté en la tabla de registros de usuarios denegados aun habiéndosele denegado el acceso previamente:

- Porque el sistema haya borrado los datos de la tabla; en este caso si el usuario 1 sigue sin estar registrado en la BBDD, automáticamente volverá a la tabla.
- Porque el administrador del sistema ha autorizado al usuario explícitamente. En este caso, si previamente ha habido una autorización de acceso por parte del administrador, automáticamente el usuario 1, saldrá de la tabla si es que estaba registrado. Lo mismo puede pasar con el dispositivo que se borrará de la tabla de direcciones MAC denegadas si ha habido una autorización de acceso por parte del administrador de la red.

- Registro de geolocalización (llamado registro de coordenadas GPS si se está usando este sistema de geolocalización):

Aquí se registra automáticamente todos los dispositivos que no cumplan con la normativa de ubicación de geolocalización. Esto quiere decir que el mecanismo propuesto se puede definir una lista de ubicaciones (coordenadas) autorizadas para el enrutador (y/o para los dispositivos que acceden al enrutador) y si no está en esa lista o rango de coordenadas, se le deniega el acceso. Esto es útil, por ejemplo, en plataformas digitales que dan servicios de contenidos audiovisuales, ya que permite dar servicio sólo a dispositivos que se encuentren en determinadas ubicaciones (por ejemplo, no daría servicio a dispositivos que accedan desde fuera del país al que pertenece la plataforma).

En la Figura 1 también se muestra la metodología y funcionamiento del nivel 1 y la denegación implícita, cuando el enrutador se ha cambiado a una ubicación no autorizada. Cuando el enrutador (o el dispositivo), ha cambiado de ubicación, y está fuera de los rangos de coordenadas establecidas inicialmente, el sistema de geolocalización (109) registra las nuevas coordenadas de la nueva ubicación (111) y le envía las nuevas coordenadas al contenedor de la denegación implícita (112). Este al comprobar que las coordenadas no son las que él tiene establecidas inicialmente (o están fuera de un rango de ubicaciones permitidas), bloqueará el enrutador y el enrutador no podrá acceder a la red (por ejemplo, los contenidos audiovisuales).

Este bloqueo puede ser parcial, es decir, por ejemplo, sólo se bloquea el enrutador para cierto tipo de contenido (por ejemplo, contenido audiovisual o multimedia, por lo que no podría acceder a las plataformas digitales), pero un usuario o dispositivo que quiera acceder a la red podría hacerlo. Sin embargo, si un usuario y dispositivo de la red quiere acceder a un sitio o servicio determinado con una etiqueta de posición (credenciales de geolocalización, que puede ser la posición del enrutador o la posición exacta del dispositivo) que no sean las permitidas puede no tener acceso ya que a la hora de establecer la comunicación no se enviaría la ubicación correcta autorizada. Por ejemplo, un dispositivo en una sucursal bancaria quiere acceder a los recursos en la nube (por ejemplo, Google), donde puede existir una política de seguridad que diga que las coordenadas de acceso permitidas para esa sucursal son XXX (con estas coordenadas la sucursal tendrá acceso a la red). Si la sucursal cambia de ubicación, las coordenadas no serán las mismas y no podrán acceder a los servicios de Google.

Para localizar al elemento de red y/o los dispositivos, se puede usar cualquier sistema de geolocalización conocido tal como geolocalización por GPS, geolocalización por la dirección IP (ya sea del proveedor o de cliente

independiente), geolocalización por red móvil (ID célula de origen), GPS asistido, E-OTD, TOA, huella multicamino, potencia de la señal recibida…) o cualquier otro tipo de sistema que permita obtener la ubicación de un dispositivo.

Nivel 2: Base de datos interna

Este nivel abarca los mecanismos de control y autenticación que hacen que los recursos y servicios de la red tengan un mejor control, coordinación y protección. Para ello, se usan una serie de tablas (o registros) que se encuentran almacenados en una (o varias) base de datos interna del enrutador.

Estos mecanismos pueden comprender un mecanismo (o sistema) de autenticación, un mecanismo (o protocolo) seguro de configuración dinámica de anfitriones (SDHCP), un mecanismo antivirus y un mecanismo de geolocalización, que suelen actuar por ese orden, aunque otro orden es posible.

- Autenticación:

La implementación de un sistema de autenticación en el elemento de red (por ejemplo, enrutador) consigue minimizar las vulnerabilidades existentes y las futuras y no necesita ninguna colaboración de los sistemas finales

En una tabla en la base de datos interna llamada de control de usuarios y contraseña (también llamada tabla de autorización de usuarios), se almacena la información de todos los usuarios que están registrados y con sus respectivas contraseñas en el enrutador. En esta tabla pueden almacenarse datos concretos de la persona que crea dicho usuario, que permitan identificar a la persona real que hay tras ese nombre de usuario (tal como dirección postal, número de teléfono, DNI, pasaporte, fecha de nacimiento…). También permite establecer unos grupos predeterminados, es decir, se puede hacer grupos por usuario. Otra novedad importante es que, al nombre de usuario creado por el administrador de la red, se pueden añadir los nombres de usuario o sub-usuarios de los distintos servicios que están en Internet y vincularlos al usuario generado (a datos concretos personales de la persona que crea dicho usuario como dirección postal, teléfono, DNI, pasaporte...). Con este procedimiento se consigue una mayor seguridad tanto dentro de la red como fuera de ella, ya que se puede rastrear el nombre de usuario asociado al usuario del sistema, obteniendo la persona real que hay detrás de ese usuario o nombre de usuario. El usuario o nombre de usuario no podrá ser duplicado en ningún caso para evitar suplantaciones de identidad.

La primera vinculación se hace manualmente, es decir, cuando se crean los usuarios (por ejemplo, por el administrador del sistema), a estos se vinculan los servicios de terceros que usen y a su vez a los dispositivos de usuario registrados que utilizan para acceder a la red. Una vez que el usuario genera tráfico, esta vinculación la puede realizar y cambiar automáticamente el sistema. Para ello, el sistema realiza unos cálculos matemáticos y una serie de predicciones basándose en la información que genera el propio usuario de tal manera que a un usuario le puede vincular distintos servicios, dispositivos con los que se comunica. Esta vinculación también puede venir predefinida en las tablas o ser cambiada en cualquier momento por el administrador de red.

En la Figura 2 se muestra un ejemplo de la tabla de control de usuarios y contraseña (204) de la base de datos interna. Obviamente, los campos que aparecen en dicha tabla son sólo un ejemplo y otro tipo de campos pueden utilizarse.

Los campos de esta tabla se rellenan, por ejemplo, cuando el usuario se registra en la red (por primera vez) o cuando por algún motivo el usuario quiere cambiar alguno de estos datos. En el campo user ID (220) (identificador de usuario) se añade el identificador de los usuarios a los que se le autoriza el acceso a la red de comunicaciones. Para cada usuario se añadirá una contraseña (221). La contraseña suele tener un tiempo de validez limitado (por ejemplo, 90 días) y pasado ese tiempo el usuario tiene que cambiar la contraseña, si por cualquier circunstancia el usuario no cambiara la contraseña no podría tener acceso a la red. Una vez que se ha registrado la contraseña, en una realización la siguiente etapa es cumplimentar el campo (222) de fecha (o año) de nacimiento, este campo "fecha de nacimiento" es una innovación por si solo ya que este campo identifica la edad del usuario y dependiendo de esta edad el sistema añadirá automáticamente al usuario al perfil que le corresponda, es decir, si el usuario es mayor de edad (Figura 2, usuario 1a), se le asignará uno de los perfiles para adultos o perfiles estándar, pero si por el contrario el usuario es menor de edad (Figura 2, usuario 1m), se le puede asignar un perfil de control parental automáticamente basándose en la edad del usuario. Para hacer esto, la tabla puede tener comunicación directa, por ejemplo, con un servicio tal como el protocolo de tiempo de red (NTP) alojado en la base de datos externa, por ejemplo, y realiza la comprobación de la edad del usuario con la fecha de actual. Adicionalmente, se pueden incluir otra información sobre cada usuario como dirección postal, teléfono (223), DNI, número de pasaporte y cualquier otro dato que caracterice al usuario real o "físico". También se pueden vincular cuentas de correo, los nombres de usuario (224) de las redes sociales, las cuentas de video juegos (XBOX live y PlayStation) u otros servicios que emplee el usuario.

Cuando el usuario quiere acceder a la red, envía un mensaje de solicitud de acceso a red al enrutador y el enrutador le pide al dispositivo (y el dispositivo al usuario, mediante un interfaz de usuario) la contraseña (y el identificador del usuario si no lo ha recibido en el primer mensaje). El enrutador comprobará si el usuario está en esta tabla de control de usuarios y contraseña (es decir, comprobará que el usuario es un usuario previamente autorizado/registrado), si la contraseña que introduce el usuario coincide con la que tiene el enrutador en la tabla de control de usuarios y

contraseña y comprobará si el usuario está vinculado a este dispositivo (de acuerdo con la tabla de control de dispositivos). Si el usuario no aparece en la tabla (no está autorizado/registrado), a contraseña es incorrecta o si está accediendo a través de un dispositivo al que no está vinculado de acuerdo con la tabla correspondiente (como se explicará a continuación), se le deniega el acceso al usuario. Adicionalmente, el enrutador enviará un mensaje a la tabla de usuarios denegados, para almacenar la identificación del usuario al que se le ha denegado el acceso.

Todas las comunicaciones entre el dispositivo y el enrutador descritas anteriormente se realizan mediante mensajes de capa 2 (también llamado nivel o capa de enlace de datos) del modelo OSI (Open Systems Interconnection).

También existirá una tabla de control (310) de dispositivos; en esta tabla, se registran los dispositivos que tienen acceso autorizado a la red (mediante su dirección MAC, IMEI, el IMSI, IMSI, MSISDN que identifique a dicho dispositivo) y se añaden los usuarios que pueden acceder a la red con cada uno de los dispositivos autorizados. Se puede decir que esta tabla es una ampliación de la tabla de dispositivos autorizados (la tabla de direcciones MAC autorizadas que se ha explicado anteriormente) que incluye los usuarios que usan cada dispositivo para acceder a la red. O visto de otra forma, en esta tabla para cada usuario registrado aparecen los dispositivos con los que puede acceder a la red. Si el dispositivo no está en esta tabla, este no podrá ser vinculado a ningún usuario con lo cual no tendrá acceso a la red.

También hay que destacar la innovación en cuanto a la vinculación de los usuarios con los dispositivos. Todos los usuarios que estén registrados en la red, tienen que estar vinculados al menos a uno de los dispositivos autorizados, ya que, en caso contrario, no podrán acceder a la red. La metodología utilizada es que los usuarios están vinculados al identificador del dispositivo (dirección MAC, IMEI, IMSI, MSISDN o cualquier identificación existente en dicho dispositivo que lo identifica de manera unívoca), es decir, se aplica este enlace en la capa 2 del sistema OSI. Al utilizar el enlace entre el dispositivo y el usuario sobre la capa 2 del sistema OSI, no es necesaria la utilización de una aplicación externa en los dispositivos. Con esta innovación se minimizan los riesgos de vulnerabilidades en el sistema y la suplantación de identidad tanto de los identificadores de los dispositivos como de los usuarios.

En la figura 3 se muestra un ejemplo de la tabla control (310) de dispositivos de la base de datos interna. En este caso, los usuarios están vinculados al dispositivo 1 (que en la tabla estará identificado por su identificación única, tal como MAC, IMEI…) son usuario 1m y usuario 1a (331), estos usuarios pueden seguir con el procedimiento, en cambio el Usuario 2m al no estar vinculado al dispositivo no podrá acceder a la red usando el dispositivo 1 (es decir, si el enrutador comprueba que el dispositivo que está usando el usuario 2m es el dispositivo 1 no le dará acceso a la red). En el dispositivo 2 (332) el único usuario vinculado es el usuario 1a, (333) es decir usuario 1m, 2m y cualquier otro usuario no podrán acceder a la red desde el dispositivo 2. El dispositivo 3 (334) no tiene vinculado ningún usuario (335), con lo cual desde este dispositivo (aun cuando está en la lista de dispositivos autorizados a acceder a la red) no se podrá acceder a la red. Con esta doble comprobación (dispositivo y usuario/contraseña) se aumenta en gran medida la seguridad de acceso a la red.

Dentro de la base de datos, puede existir también una tabla de perfiles, donde se asignan o definen los perfiles a los distintos usuarios de la red. En otras palabras, en esta tabla aparecerán los perfiles asignados a cada usuario (a los usuarios autorizados, que aparezcan en las tablas de control de dispositivos).

En una realización, a los usuarios menores de edad (detectados basándose en los datos de usuario, como fecha de nacimiento, de la tabla de control de usuarios/contraseña) se les asigna automáticamente el perfil de control parental. Este perfil de control parental puede estar vinculado a un sistema de clasificación de contenido de Internet (páginas web, redes sociales…) por edades, con un servicio de analizador semántico. Una de las novedades de la presente invención es usar este sistema para otorgar el acceso a Internet. Usando el sistema de clasificación de contenido de redes externas (Internet) por edades, se consigue que el acceso a Internet presente un sistema de clasificación por edad a nivel de usuario. En el sistema de clasificación se pueden incluir varias categorías de acuerdo con la edad del usuario (por ejemplo, mayores de 7, de 12 o de 16 años, aunque se pueden añadir y configurar más categorías). También se puede definir una pluralidad de descripciones de diferente contenido (lenguaje soez, discriminatorio, de drogas, sexo, juego, terror, violencia, redes sociales…). Todos estos campos son totalmente configurables por el administrador del sistema. De manera que cuando el analizador semántico descubre que en la página web a la que se quiere conectar el usuario, se usa lenguaje de algunos de estos tipos, impide el acceso a la red (dependiendo de la categoría de edad a la que pertenezca el usuario). Para que esta clasificación de contenidos cumpla con los diferentes estándares culturales en la red de varios países europeos, se puede usar para la clasificación de contenidos de Internet un baremo parecido al que se usa en el sistema PEGI, iniciado y gestionado por la Federación Europea de Software Interactivo para software y video juegos (no para contenido de páginas web y redes sociales).

El usuario puede ser asignado en esta tabla a alguno de los perfiles que están predefinidos en la base de datos. Por ejemplo, un perfil estándar que sería el perfil por defecto (y estos usuarios no tendrían potestad para cambiar la configuración) o un perfil de administrador para los administradores de sistemas (usuarios que tienen más privilegios que los usuarios que son miembros del perfil estándar, teniendo la potestad de configurar y cambiar la configuración del sistema de autenticación). Si un usuario es menor de edad, se le puede asignar un perfil de control parental. En este perfil se le otorga el acceso dependiendo de la edad del usuario (por ejemplo, mayores de 7, de 12 o de 16 años). Estas vinculaciones al perfil de control parental y a la categoría de acuerdo con la edad del usuario el

enrutador las realiza automáticamente, ya que conoce la edad del usuario de la entrada para dicho usuario en la tabla de control de usuario. El enrutador puede detectar cuando el usuario pasa a ser mayor de edad y automáticamente se le eliminará del perfil de control parental y se añadirá al perfil de estándar, por ejemplo. En estos casos, pueden existir unas medidas de control tales como, por ejemplo, notificar al administrador de la red (mediante SMS, correo electrónico o similar) de estas situaciones, para que esté al tanto de las mismas.

Como se ha explicado, en el enrutador también existirá un analizador semántico, que es el encargado analizar las páginas web que quieren visitar por los usuarios con perfil de control parental, para analizar el contenido de la web y bloquear el acceso a la web dependiendo del contenido de la misma. Para ello, antes de mostrar el contenido de la página web, el analizador semántico analiza el contenido de la página y dicha información la guarda en memoria. Si es una página web que ya ha sido visitada, la información acerca de su contenido ya está almacenada en el enrutador y, si dicha información almacenada no es muy antigua (su antigüedad es menor que un determinado límite de tiempo), el enrutador puede utilizarla para denegar o no el acceso. Si es muy antigua, pues puede analizar otra vez el contenido de la página web en caso de haber cambiado. El analizador semántico tiene comunicación directa con la base de datos externa (que a su vez accederá a dichas páginas web) para realizar dichas comprobaciones online de los contenidos en las páginas web que desea visitar el usuario para restringirle o no el acceso. El analizador semántico no deniega el acceso completo, lo que hace es no permitir el acceso a las páginas web con contenido ilícito.

Además del perfil asociado a cada usuario, en la base de datos interna también puede existir una entrada o tabla de tiempo de acceso (llamada también tabla de políticas de tiempo). En esta tabla se definirá para cada usuario y/o dispositivo, los límites temporales de acceso a la red (es decir, los días y horas a las que puede acceder a la red). Estos límites de acceso están predefinidos por el sistema y se pueden configurar manualmente.

Todos los usuarios (directamente o a través de su perfil) y dispositivos (excepto los administradores) deberían estar definidos en esta tabla ya que si no están definidos no podrán acceder a la red. Este acceso temporal a nivel de enrutador, es una innovación ya que actualmente los enrutadores del mercado no hacen esta distinción.

Para poder aplicar dichos límites temporales, el enrutador debe saber el día y la hora y otros datos, tal como, por ejemplo, los festivos que hay que aplicar (ya que el acceso temporal puede estar vinculado a que sea un día festivo o laborable). Para ello, el enrutador tendrá que usar por ejemplo un servicio de NTP (la lógica de este servicio estaría en el nivel 3 de base de datos externa). Para saber los festivos que hay que aplicar, el servicio NTP tiene que conocer el código postal y aplica un calendario laboral u otro dependiendo de dicho código. Esta configuración se puede realizar, por ejemplo, a la hora de la primera configuración del enrutador, al que se solicita el código postal para poder registrar correctamente la fecha al dispositivo. Esta fecha solo puede ser configurada en el enrutador y ningún usuario excepto el administrador podrá acceder a ella; la fecha y hora puede refrescarse periódicamente accediendo al servicio de NTP.

El que esta tabla de tiempo de acceso esté conectada al servicio de NTP alojado en el propio enrutador (en el nivel de base de datos externa), es una innovación ya que actualmente no está implementado en ningún enrutador y permite una gestión más intuitiva y sencilla a la hora de gestionar la red. Con esto se le añade inteligencia al enrutador, ya que basándose en una serie de datos puede decidir y saber la fecha de la semana en la que estamos operando y poder decidir el límite de tiempo de uno o varios usuarios en concreto y, basándose en esos límites, decidir si permitirle el acceso a la red o no.

En una posible realización, en esta tabla, habría una entrada para cada dispositivo y para cada usuario vinculado a cada dispositivo indicando, para cada día, el (o los) rangos temporales en los que se puede acceder a la red (definiendo, por ejemplo, un tiempo de comienzo y tiempo de finalización de cada rango). Siguiendo con el ejemplo mostrado en la figura 3, el Dispositivo 1 tendría una entrada en esta tabla y a su vez, para cada usuario vinculado a este dispositivo (1a y 1m) habría otra entrada en la tabla. A los dispositivos registrados, también se les puede asignar un límite de tiempo independientemente del usuario. De esta manera, por ejemplo, el dispositivo 1 puede no tener ninguna limitación de tiempo (por lo que el rango de acceso que figuraría para este dispositivo sería para cada día de las 0:00 a las 24:00), mientras que los usuarios sí tienen limitación de tiempo, por ejemplo el usuario 1a puede acceder a la red desde las 08:00 hasta las 22:00 horas los días de diario, mientras que los fines de semana puede acceder a la red desde las 12:00 horas de la mañana hasta las 00:00 y el 1m desde las 19:00 a las 21:00 en días laborables y a las 22:00 en fines de semana (el usuario 1m tiene una política de acceso es más restrictiva ya que el sistema sabe que es un menor).

En una realización, si el dispositivo o usuario no aparece en esta tabla se supone que no tiene restricción de tiempo de acceso. En una realización alternativa, si el dispositivo o usuario no aparece en esta tabla, se supone que no está autorizado para acceder a la red y se le denegará el acceso. En una realización, si durante la comunicación establecida por el usuario, se rebasa el tiempo de acceso permitido (es decir, cuando se empezó la comunicación sí estaba dentro del tiempo de acceso permitido, pero en un determinado momento se rebasa dicho tiempo), el enrutador puede cortar la comunicación y denegar el acceso. Para ello, el enrutador puede comprobar periódicamente la tabla de tiempos de acceso para las comunicaciones en curso.

Otra tabla (o entrada o registro) que podría haber en la base de datos interna sería las tablas de política de

seguridad. Esta tabla definiría una serie de reglas que establecerían las políticas de seguridad, tales como, por ejemplo, con que destinatarios y/o que servicios y/o que puertos y/o qué páginas web y/o con qué protocolos (por ejemplo, FTP), puede acceder cada usuario o cada dispositivo. En las soluciones existentes, las políticas de seguridad de acceso se aplican en la capa 3 del sistema OSI y los elementos de red que aplican dicha seguridad son los cortafuegos o cortafuegos. En la presente invención, las políticas de seguridad se aplican en la capa 2 del sistema OSI (en el enrutador o conmutador), es decir, se aplican dichas políticas antes de obtener una dirección IP. Y además de aplicar estas políticas en la capa 2 del sistema OSI, también se aplican las políticas a nivel de usuario, es decir que independientemente del dispositivo y la dirección IP, el sistema aplica dichas políticas de seguridad a los usuarios registrados en el sistema. Estas políticas se aplicarían tanto en origen como en destino, es decir, tanto en entrada a la red (Inbound) como en la salida (Outbound), por lo que afectan tanto a la red de comunicaciones que gestiona el enrutador (a la que pertenece el enrutador, llamada red interna) como a redes externas/internet. Otra innovación de este sistema es que políticas también se aplican a puertos lógicos (TCP/UDP), actualmente no hay ningún equipo que apliquen estas políticas a usuarios y dispositivos sin necesidad de direccionamiento IP.

En la figura 4 se muestra un ejemplo de la tabla de políticas (416) de seguridad de la base de datos interna. Como se puede apreciar la regla 1 (460) dice que si el usuario 1a (461) que está vinculado al dispositivo 1, quiere acceder al dispositivo 2 (462) a los puertos lógicos SMB y TCP 25 (463). Esta comunicación está permitida por el enrutador (464), pero solo está permitida a estos puertos lógicos, esto quiere decir que si el dispositivo 1 (461) quiere acceder al dispositivo 2 (462) por otros puertos que no son estos, estas comunicaciones no se pueden establecer ya que no hay regla en el sistema que lo permita. En la regla número 2 hay definida una política de acceso a google que está permitida para el usuario 1m (161), esto quiere decir que el usuario menor de edad 1m puede acceder a google, pero si este usuario quisiera acceder a una página web con contenido ilícito, no podría acceder a ella a través de google (ya que al tener el usuario un perfil de menor de edad, el analizador semántico bloquearía el acceso). En otras palabras, en cuanto a las políticas de los usuarios menores de edad, se puede predeterminar el denegar o permitir el acceso a una dirección web mediante estas reglas de políticas de seguridad, pero aún si el acceso está permitido por las políticas de seguridad, si dentro de dicha web se quieren acceder a datos que están configurados en el sistema de clasificación de contenido por edades (en el analizador semántico) como datos no permitidos (por ejemplo, relacionados con sexo o violencia), el analizador semántico del enrutador los detectará, el enrutador bloqueará el acceso a esa página a este usuario, se etiquetará automáticamente la web como "prohibida" y se incluirá en el analizador semántico como página web prohibida.

La regla número 5 indica que aquellas comunicaciones que no estén recogidas explícitamente en la base de datos de política de seguridad, estarían automáticamente rechazadas por lo que automáticamente tira el tráfico y deniega el acceso. Como se ve, en la tabla hay dos tipos de acciones de rechazo "drop" y "reject", la diferencia es que DROP recibe el paquete y lo descarta (sin responder al emisor) y el REJECT recibe el paquete y lo procesa y procesa un paquete de rechazo y lo envía de vuelta al emisor. En otro ejemplo, en que la seguridad requerida fuera más baja, se podría decir que aquellas comunicaciones que no estén recogidas explícitamente en la base de datos de política de seguridad, estarían por defecto permitidas.

Por último, en la base de datos interna, podría existir una tabla (117) (llamada por ejemplo tabla de registro de actividad o "log") donde se guarde toda la actividad de todos usuarios y dispositivos del sistema (comunicaciones que han establecido, destinatarios, fecha y hora…). En una realización, se registran todos los intentos de acceso hayan sido autenticados con éxito o no.

- SDHCP:

Aparte del sistema o mecanismo de autenticación, otro mecanismo que se aplica en el sistema propuesto por la presente invención, es el protocolo seguro de configuración dinámica de anfitriones (SDHCP o secure DHPC). El SDHCP tiene como objeto asegurar el DHCP, de tal manera que la configuración, asignación y distribución de direcciones (IP) y parámetros de configuración de red (de capa 3) en una red de comunicaciones se realice de manera más óptima y segura.

Para ello se usan políticas basadas en roles (perfiles) vinculados directamente a la identificación física del dispositivo (por ejemplo, la dirección MAC). De esta manera, el servicio SDHCP podrá tomar decisiones de restricción o acceso, no solo por la asignación de identificador IP al dispositivo dotado de acceso, sino por la protección de nivel 2 (nivel de enlace de datos de modelo OSI) que ofrece al denegar cualquier negociación entre el cliente y servidor DHCP sin que haya sido dado de alta el cliente y gestionado en los roles previamente.

Esto es posible debido a la presencia de una base de datos en el elemento de red (por ejemplo, el enrutador) a la que se accede mediante un elemento funcional SDHCP, conocido como agente de seguridad y que actúa con el servidor de parámetros de configuración de red (servidor SDHCP). Esta base de datos relaciona los identificadores de red de nivel 2 (por ejemplo, dirección MAC) de los elementos de red con los identificadores de nivel 3 (IP) y a su vez con los roles (perfiles) de usuario. De esta manera la protección del servicio no solo se reduce al filtrado MAC o a políticas de asignación y reserva de direccionamiento IP, ya que proporciona un control y enlace estricto de cada cliente DHCP conectado en el mismo ámbito de red. Por lo tanto, el uso de esta nueva base de datos para el nuevo servicio SDHCP, mejora en aspectos de seguridad la estructura hasta ahora utilizada en el protocolo DHCP que usa dos bases de datos independientes que se describieron en el apartado de antecedentes de la invención (la

estructura del protocolo BOOTP y la estructura que almacena la pila o conjunto de direcciones disponibles ya descritas anteriormente en este mismo documento).

El agente de seguridad (también llamado agente seguro) es un módulo o elemento funcional que normalmente se encuentra físicamente en el mismo elemento de red (por ejemplo, enrutador o conmutador) que el servidor SDHCP. En una realización alternativa, puede encontrarse en otro nodo de red (con el que el servidor SDHCP se comunica a través de una red de comunicaciones).

Cabe destacar que se introduce como medida de seguridad en el SDHCP la denegación implícita de todas aquellas solicitudes de multidifusión de nivel 2 derivadas del procedimiento de solicitud y ofrecimiento entre cliente y servidor (mediante el registro de los dispositivos cuyo acceso haya sido denegado en el registro de direcciones MAC denegadas como se ha explicado anteriormente). Durante el procedimiento de asignación, el envío/recepción de datagramas con destino difundir la dirección MAC, se produce en todos los mensajes (DHCPDISCOVER, DHCPOFFER, DHCPREQUEST y DHCPACK) de tal manera que el control y descarte de aquellas solicitudes no autorizadas (cuyos dispositivos no están autorizados) supone una mejora, no solo en cuanto a la seguridad, sino en términos de consumo de recursos del dispositivo en el que está activo el servicio SDHCP. Adicionalmente, este procedimiento palia vulnerabilidades en el control de flujo de la información que se realizaba hasta ahora en la capa de red o nivel 3 mediante firewalls o cortafuegos.

Así, por ejemplo, en los sistemas existentes, un usuario de un dispositivo puede configurar los parámetros de red manualmente, (dirección IP, máscara de subred, puerta de enlace, DNS…) y con estos parámetros configurados en el dispositivo del usuario, este tendrá acceso a la red. Usando el mecanismo propuesto por la presente invención, si un usuario quiere configurar manualmente los parámetros de red y que estos parámetros permitan el acceso a la red del dispositivo, el dispositivo tiene que estar registrado en la base de datos del agente de seguridad SDHCP, porque si no es así, se le denegará el acceso y el dispositivo no podrá acceder a la red. Como se ha explicado antes, con esta denegación implícita se aumenta la seguridad de la red, impidiendo ataques de acceso tales como los ataques "por saturación".

La Figura 5 muestra esquemáticamente la arquitectura del protocolo SDHCP propuesto de acuerdo con una realización de la invención. En dicha figura, se muestra el dispositivo o equipo cliente que quiere operar en la red de comunicaciones, el servidor SDHCP encargado de suministrarle los parámetros de configuración necesarios para operar en dicha red (incluyendo la dirección de red, por ejemplo, una dirección IP), el agente de seguridad y la base de datos con datos para asignar los parámetros de configuración al equipo. Como se ha dicho, el servidor SDHCP puede estar en el mismo elemento de red que la base de datos y el agente de seguridad (en el elemento de red propuesto por la presente invención) o en un elemento de red distinto.

El protocolo SDHCP se basa en los siguientes elementos (o tablas de datos):

-- registro de direcciones MAC (también llamada registro de direcciones MAC autorizadas o permitidas o registro de dispositivos autorizados o permitidos): Esta tabla ya se ha definido anteriormente con detalle (en el apartado del nivel 1), por lo que no se va a repetir aquí su descripción. En esta tabla se almacenan las direcciones MAC (u otro identificador) de los dispositivos que pertenecen a la red en cuestión o, en otras palabras, dispositivos que tienen acceso autorizado a la misma.

El servicio SDHCP puede asignar direcciones IP de manera estática o dinámica. Ya sea la asignación estática o dinámica, la dirección MAC de cada dispositivo que tenga permiso de acceso a la red tiene que estar registrada en esta tabla, de tal manera que, si un dispositivo que solicita una dirección IP al SDHCP no está registrado en la base de datos, el SDHCP no procederá a asignarle ninguna dirección IP.

- Roles (perfiles) MAC: Almacena los perfiles (roles) en la red de los dispositivos. Se pueden configurar un número ilimitado de perfiles, dependiendo la capacidad de procedimiento del equipo. En esta tabla, a cada dispositivo de la red le corresponderá un perfil u otro (por ejemplo, dependiendo de su dirección MAC); en otras palabras, a partir de la dirección MAC del dispositivo (es decir, depende de la identificación del dispositivo, no de la identificación del usuario), a través de esta tabla se obtiene el perfil que le corresponde al dispositivo. En el caso expuesto en la Figura 5, estos perfiles serán, por ejemplo, GUEST (en español, huésped), HOME AUTOMATION (en español, domótica), QUARANTINE (en español, cuarentena), WIRED CONNECTION (en español, conexión cableada), WIRELESS (en español, conexión sin cable o WIFI); pero por supuesto, esto es sólo un ejemplo y puede haber muchos otros perfiles distintos.

Además, de la dirección MAC del dispositivo, las bases de datos de MAC registradas y de Roles MAC pueden contener otras identificaciones del dispositivo tales como el IMEI, IMSI, MSISDN o cualquier otro parámetro que identifique el dispositivo (es decir, almacena no sólo el perfil que le corresponde al dispositivo en función de su dirección MAC sino también en función de alguno o algunos de estos otros identificadores).

Roles (perfiles) de direcciones IP: Almacena las subredes IP existentes en toda la red, y se asigna automáticamente un rango de direcciones IP (definido, por ejemplo, por una dirección IP y una máscara de direcciones) de acuerdo con la subred a la que pertenezca cada dispositivo. El dispositivo pertenecerá a una subred u otra (es decir, se le asignará un rango de direcciones IP u otro), dependiendo del rol (perfil) que se le haya asignado en la tabla anterior;

en otras palabras, en la tabla anterior se obtiene el perfil de red que le corresponde al dispositivo de acuerdo con su dirección MAC y en esta tabla se obtiene el rango de direcciones que le corresponde a dicho perfil, y por lo tanto a dicho dispositivo. Se puede configurar un número determinado de subredes dependiendo de la capacidad del equipo. Estos rangos de red son configurables, al administrador del sistema solo tiene que decir cuántos dispositivos van a estar vinculados a cada subred y el agente de seguridad SDHCP configurara automáticamente el rango de red. Dependiendo de la subred (rango de red) donde este asignado el dispositivo (que, a su vez, dependerá de su perfil) tendrá una serie de reglas implícitas que permitirán o denegarán el acceso a otros dispositivos, como medida de seguridad. Por ejemplo, los dispositivos con el perfil asignado de "HUÉSPED", al no pertenecer a la red, es conveniente denegarles el acceso a los dispositivos de todos los demás perfiles. Estas denegaciones de acceso o configuraciones en general, se consiguen con las políticas que aplican el (los) enrutador(s) de la red. En otras palabras, en el enrutador (enrutador) de la red se configurará de tal manera que si la dirección del dispositivo pertenece a un determinado rango de direcciones (que corresponderá a un determinado perfil), no puede acceder a otros rangos de direcciones (que corresponderán a otros perfiles). Estas políticas de restricciones (o más generalmente hablando, de políticas de seguridad) también se pueden aplicar a nivel de puerto. De esta manera, el enrutador puede configurar que si la dirección del dispositivo pertenece a un determinado rango de direcciones (que corresponderá a un determinado perfil), dicho dispositivo podrá acceder por un determinado puerto y no por otro (lo que implicará que puede acceder a unos determinados dispositivos o servicios o no). De esta manera, por ejemplo, en el caso expuesto de la figura 5, a un dispositivo que tenga un perfil CUARENTENA le corresponderá el rango de direcciones IP 192.168.102.0/x. Se decide (el administrador de red) que los dispositivos que tienen este perfil, sólo tengan acceso a Internet y por un tiempo limitado, pero no tengan acceso a otros recursos de la red ni se puedan comunicar con otros dispositivos de la red. Para ello se configura el enrutador (o los enrutadores si hay más de uno) de la red, de tal manera que a un dispositivo cuya dirección esté en el rango de red correspondiente al perfil CUARENTENA, se le aplique una denegación de acceso a toda la red y dispositivo de la red. Adicionalmente, para conseguir que el acceso a Internet de este perfil sea limitado, el enrutador le puede añadir una política de tiempo. Siguiendo la figura 5, a un dispositivo que tenga un perfil HUÉSPED, le corresponderá el rango de direcciones IP 192.168.100 0/x. Se decide (el administrador de red) que los dispositivos que tienen este perfil (es decir que tienen una dirección en este rango de direcciones de red), tengan acceso a Internet, pero solo con la utilización del protocolo HTTP y HTTPS, pero que no tengan acceso a los demás perfiles o redes. Aquí se puede aplicar también la denegación o el acceso a los puertos lógicos, es decir, el dispositivo que pertenezca a este perfil podrá acceder a Internet por el puerto 80 (http) pero no podrá acceder a un servidor a través de ssh (puerto 22). En otro ejemplo, a un dispositivo que tenga un perfil HOME AUTOMATION le corresponderá el rango de direcciones IP 192.168.101.0/x. Se decide que los dispositivos que tienen este perfil (es decir que tienen una dirección en este rango de direcciones de red) tengan acceso a Internet con los protocolos HTTP, HTTPS, SSH, POP3 y desde Internet hacia a ellos.

Es decir, de acuerdo con las direcciones IP que se le asigne (de acuerdo con el perfil), va a tener un acceso a la red restringido o no. Y, si es restringido, generalmente hablando, puede comprender al menos una de las siguientes restricciones (o cualquier otro tipo de restricción):

- denegación del envío de datos al dispositivo;
- denegación de comunicarse con el resto de dispositivos de la red;
- denegación de acceso a al menos un puerto;
- denegación de comunicación mediante al menos un protocolo;
- autorización de acceso únicamente a Internet;
- acceso a la red dentro de un determinado periodo de tiempo.

Estas tablas (bases de datos) puede configurarlas el administrador de red y cambiar su contenido cuando sea necesario. El agente de seguridad SDHCP también puede tomar una serie de decisiones dinámicamente para añadir perfiles, modificar perfiles, cambiar el dispositivo del perfil al que está vinculado, cambiar los parámetros de configuración de cada perfil de acuerdo con las circunstancias de la comunicación o distintas condiciones que detecte en el dispositivo o en la red. Por ejemplo, cuando un dispositivo no tiene la base de datos de antivirus actualizada o que este tenga un virus o troyano, el agente SDHCP puede tomar la decisión de eliminarlo del perfil al que pertenece temporalmente y asignarle otro perfil (cuarentena) para que el dispositivo no infecte a los demás dispositivos dentro del perfil (y la red) al que ha sido asignado. En otras palabras, si el agente SDHCP detecta que las condiciones de seguridad del dispositivo están comprometidas puede asignarle un perfil de acceso más restringido a la red. Y viceversa, es decir, si el agente SDHCP detecta que las condiciones de seguridad del dispositivo dejan de estar comprometidas (por ejemplo, se actualiza su base de datos de antivirus) puede asignarle un perfil de acceso menos restringido a la red.

La Figura 6 muestra el flujo de mensajes que se intercambian, de acuerdo con una realización de la presente invención, entre un dispositivo o equipo cliente y un servidor DHCP usando el protocolo SDHCP propuesto, en el caso de que dicho dispositivo no esté registrado como dispositivo autorizado. Cada una de las etapas, en este escenario, se describirá y se enumerará a continuación, de acuerdo con una realización de la presente invención:

1. El dispositivo cliente (el que solicita los parámetros de configuración de red porque quiere acceder a la red) manda un mensaje solicitando los parámetros de configuración de red, que es captado por el servidor SDHCP (que está, por ejemplo, en el enrutador).
2. Una vez que la solicitud la tiene el servidor SDHCP, el servidor la envía al agente de seguridad SDHCP y éste

manda un mensaje, solicitando a la base de datos información sobre el dispositivo. Este mensaje se llama SDHCPAGENT.
3. Una vez realizadas las comprobaciones en la base de datos, y al no estar registrada la dirección MAC del dispositivo en la tabla correspondiente, el agente de seguridad SDHCP manda un mensaje llamado DHCPNULL al servidor SDHCP que contiene la información necesaria para denegar el acceso.
4. El enrutador (servidor SDHCP) manda el mensaje de DHCPNULLPACK, notificando al cliente que no se le puede asignar una dirección IP. Este mensaje puede incluir una notificación, diciendo que se ponga en contacto con el administrador de la red para que sea registrado debidamente. Adicionalmente, el servidor SDHCP o el mismo enrutador donde está el agente de seguridad enviará un mensaje a la tabla de direcciones MAC denegadas para almacenar la dirección MAC de este dispositivo al que se le ha denegado el acceso.

La Figura 7 muestra el flujo de mensajes que se intercambian, de acuerdo con una realización de la presente invención, entre un dispositivo o equipo cliente y un servidor DHCP para la distribución de los parámetros de red (incluyendo la dirección IP) usando el protocolo SDHCP. Tanto los mensajes a los que nos referimos en este escenario, como en el escenario anterior, son mensajes de capa 2 (también llamado capa de enlace) del modelo OSI. A continuación, se describen y enumeran a continuación cada una de las etapas a realizar para la asignación de direcciones IP y otros parámetros de configuración de red, de acuerdo con una realización de la presente invención:

1. El dispositivo cliente manda un mensaje solicitando los parámetros de configuración de red (por ejemplo, la dirección IP), que es captado por el servidor SDHCP.
Al igual que en el caso anterior, este mensaje será por ejemplo un mensaje DHCPDISCOVER y para enviarlo, el dispositivo usará una dirección de multidifusión ya que el cliente no tiene la dirección del servidor IP y, por lo tanto, no puede conectar directamente con él. Este mensaje incluye información que permite identificar al dispositivo cliente (por ejemplo, su dirección MAC u otro tipo de identificador).
2. Una vez que la solicitud la tiene el servidor SDHCP, el servidor la envía al agente de seguridad SDHCP y éste manda un mensaje solicitando a la base de datos (por ejemplo, al enrutador) información sobre el dispositivo que esta solicitado la asignación de parámetros de configuración de red y, en particular, la dirección IP (o, en otras palabras, el servidor SDHCP comprueba en la base de datos si el identificador del dispositivo está registrada consulta la base de datos).
3. Si el identificador (la dirección MAC) del dispositivo está registrada dentro de la base de datos (como es el caso de este escenario), se le asigna un perfil de usuario en la tabla de roles MAC de acuerdo con la identificación de dicho dispositivo. Como se ha indicado anteriormente, además, de la dirección MAC del dispositivo, la base de datos puede también tener registradas otras identificaciones del dispositivo. En ciertos escenarios, en vez de la dirección MAC, el dispositivo puede enviar uno de estos otros identificadores; en esos casos la tabla se comprobará de igual manera, pero partiendo de este identificador, en vez de la dirección MAC del dispositivo.
A partir del perfil asignado, en la tabla de roles de direcciones de red, se le asigna la configuración de red a la que pertenece el dispositivo. Esta configuración la obtiene el agente de seguridad y se la envía en un mensaje al servidor SDHCP. Este mensaje se llama DHCPACCES.
4. El servidor SDHCP manda un mensaje (DHCPOFFER) al dispositivo cliente con toda la configuración de red que se ha asignado a dicho dispositivo de acuerdo con la base de datos interna. Este mensaje puede incluir varias direcciones IP disponibles (o un pool de direcciones IP) y es el dispositivo cliente el que elige una dirección IP concreta de las que se le ofrece.
5. El dispositivo cliente recibe el DHCPOFFER y manda otro mensaje llamado DHCPREQUEST por multidifusión indicando la configuración de red que ha escogido (incluyendo la dirección IP que ha escogido) si ha recibido varias posibles.
6. El servidor SDHCP recibe el mensaje de DHCPREQUEST y crea un mensaje con toda la configuración de red que necesita el dispositivo cliente y el perfil que se ha asignado al dispositivo cliente. El servidor compila toda esta información en un mensaje llamado DHCPACK y lo envía al dispositivo cliente. En este momento el Servidor SDHCP ya tiene registrada la información del dispositivo. Este mensaje DHCPACK, por lo tanto, puede ser un mensaje dirigido expresamente al dispositivo que solicita la dirección IP, ya que el servidor SDHCP ya tiene toda la información del mismo.

Tanto en este escenario como en el anterior, si hubiera más de un servidor SDHCP, el comportamiento sería análogo. En ese caso, habría un servidor SDHCP y uno o más servidores secundarios, dependiendo de lo extensa que sea la red. Cada uno de esos servidores tendrían su agente de seguridad SDHCP y su base de datos; los servidores secundarios de SDHCP se sincronizarán entre ellos y entre el servidor principal, con lo cual las bases de datos de los agentes de seguridad SDHCP estarían sincronizadas correctamente y tendrían la misma información.

- Antivirus:

En una realización de la presente invención se contempla la integración de los sistemas antivirus de los clientes (dispositivos) conectados al elemento de red (por ejemplo, enrutador) con el sistema de acceso global propuesto. De esta manera se incluyen parámetros del estado de antivirus tales como la detección de amenazas.

Por otro lado, para el caso concreto de la comprobación del estado de las bases de datos de antivirus, se

establecerá un enlace similar con el proveedor de las bases de datos, es decir, con el fabricante del SW del Sistema Antivirus instalado en el cliente, con el que se cotejará dicho elemento para tener un grado superior de confianza en el entorno de red que aplica el enrutador. Hay que recordar que las bases de datos de antivirus son donde se encuentran registradas las amenazas potenciales actuales en Internet, y que, por lo tanto, la protección del Antivirus no será real si no se encuentra actualizada a la última versión disponible y distribuida por el desarrollador del SW Antivirus.

Así, el sistema de acceso propuesto en la presente invención, puede incluir una nueva mejora en relación al entorno de confianza del enrutador hacia sus clientes. El enrutador establece un enlace mediante la comprobación del estado y tipo de antivirus. El registro de la comprobación estará en la base de datos interna y por lo tanto interviene en el nivel 2 de la seguridad jerárquica del sistema de autenticación. El factor primordial para este tipo de comprobaciones es el estado propio de la protección del sistema operativo por el sistema antivirus residente en cada dispositivo. Los tipos de estados serán:

- En cuanto a la base de datos de antivirus, puede estar actualizada (la protección del antivirus dispone de la información más reciente de todos los tipos de amenazas para realizar análisis en tiempo real o no del sistema operativo en el dispositivo cliente) o no actualizada (en caso contrario).
- En cuanto al estado del sistema operativo del dispositivo, los estados pueden ser:
    - no Infectado:
        - Inmune: el sistema se encuentra totalmente protegido y dispondrá de las políticas en el enrutador que le permita las conexiones tanto en el entorno de red local como en el entorno de red externa o pública (Internet).
        - Preventivo: el sistema antivirus lleva tiempo sin ejecutar un análisis del sistema operativo instalado en el dispositivo cliente (por lo que no se puede asegurar que el dispositivo esté totalmente protegido).
    - *Infectado*:
        - Crítico: infección relacionada con virus o software malintencionado que necesita de las comunicaciones para su funcionamiento, propagación o envío de información a terceros.
        - Bajo: infección relacionada con virus o software malintencionado que no necesita de las comunicaciones para su funcionamiento y propagación.

Basándose en cada estado o circunstancia en la que se encuentre el sistema antivirus, el sistema de autenticación de acceso que alberga el enrutador, tomará una decisión de acceso en cuanto a las conexiones que gestiona de cada usuario/dispositivo registrado en el sistema:

- Permitido: existen garantías de seguridad para comunicaciones. Aprobación de todas las comunicaciones que requiera el dispositivo cliente (por supuesto, esta aprobación estará condicionada a que el dispositivo cliente y el usuario pasen el resto de controles de seguridad del enrutador que se han descrito en los apartados anteriores).
- Denegado: no existen garantías de seguridad para las comunicaciones. Se prohíben todas las comunicaciones relacionadas con ese dispositivo.
- Temporal: todavía no existen garantías integrales para las comunicaciones. Aprobación de permisos temporales para realizar tareas de actualización o análisis on-line del sistema antivirus residente.

Así, por ejemplo, en el caso de que el sistema esté en estado de base de datos antivirus actualizada, no infectado-inmune o infectado-baja, el acceso puede estar permitido, si está en estado Infectado-Crítico el acceso puede ser denegado y en el resto de casos el acceso puede ser temporal. La información sobre el estado de antivirus de cada dispositivo la puede solicitar la base de datos interna a la base de datos externa, como se explicará más adelante.

En el caso de que se haga una denegación de acceso (temporal o definitiva), se puede enviar un mensaje (por ejemplo, AV1CHANGE) al servidor SDHCP para que modifique el perfil del dispositivo y lo asigne al perfil de cuarentena. En el perfil de cuarentena, solo podrá tener acceso a la red externa y por un tiempo determinado para que pueda actualizar el software del antivirus o eliminar la infección del virus. Mientras que el dispositivo este en el perfil de cuarentena, no tendrá acceso a los servicios y recursos de la red interna. Normalmente, cuando el dispositivo está realizando las negociaciones para acceder a la red, pidiendo los parámetros de configuración de la misma (usando SDHCP), el servidor de antivirus realiza un chequeo y si comprueba que está infectado (o, por ejemplo, no tiene la base de datos de antivirus actualizada), le enviará el mensaje AV1CHANGE al servidor SDHCP y el perfil que se le asignará (y, por lo tanto, los parámetros de configuración de red que le asignará), será el perfil de cuarentena. Si, por otro lado, el cliente ya ha completado el procedimiento y está conectado a la red, si el cliente recibe un virus o troyano mientras esté conectado (o se le queda la base de datos de antivirus desfasada) y el antivirus lo detecta, el servicio de antivirus mandará el mensaje AV1CHANGE al SDHCP y este le cambiará el perfil a cuarentena. El SDHCP le enviará un mensaje al dispositivo de cambio de parámetros de configuración de red y le enviará unos nuevos parámetros de configuración (entre ellos una nueva dirección IP) que corresponderán al nuevo perfil (al perfil de cuarentena).

Cabe destacar que la comprobación del sistema antivirus será siempre en base siempre al dispositivo (MAC) y no al

usuario. Esto se debe a que el sistema antivirus coexiste con el sistema operativo del dispositivo y por lo tanto los estados están directamente relacionados para todos los usuarios de este.

Para informarse del estado del sistema antivirus en cada dispositivo, el enrutador puede ser capaz de distribuir a los dispositivos un software adicional que una vez instalado en el dispositivo cliente enviará la información del estado del sistema antivirus al enrutador (por ejemplo, periódicamente o cuando se produzca algún evento relacionado con el sistema antivirus). El enrutador entonces interpretará y tomará una decisión basándose en dicho estado.

Para distribuir la información del sistema antivirus de cada dispositivo cliente, puede usarse el protocolo SNMP (Protocolo Simple de Administración de Red) para los casos de entornos de centralización de Antivirus, es decir, cliente/servidor. Para que exista comunicación entre el enrutador y el servidor del antivirus debe estar soportado el protocolo en ambos extremos, de tal manera que se envíe la información de las bases de datos antivirus tal y como se hace con la comprobación de las MIB (Base de Información de Administración) de SNMP habituales. Para esto es necesaria la disponibilidad de un agente de SNMP que gestione el envío de mensajes, así como la gestión remota del dispositivo si fuera necesario.

Para los casos concretos en los que el sistema operativo del dispositivo cliente conectado al enrutador no soporte la instalación de un antivirus, se pueden contemplar comprobaciones adicionales para recabar información del usuario para el registro del usuario en el sistema de autenticación. Dicho tipo de información a reclamar al usuario, estará predeterminada en roles exclusivos para tal caso, en el que el propio rol de usuario requerirá una información distinta y que será interpretada por el Sistema de Acceso y por consiguiente detallada en la BBDD. La información a almacenar por los dispositivos que no soporten ningún tipo de SW Antivirus es:

- Versión del sistema operativo: para la comprobación si se encuentra actualizado a la última versión que contenga vulnerabilidades relacionadas con amenazas críticas del sistema.
- Estado del sistema operativo: si se encuentra bloqueado o no, tal como por el ejemplo para el caso de dispositivos móviles que se encuentran bloqueado por robo o pérdida. De esta manera se protegen también los datos legítimos del cliente.

En estos casos, el enrutador puede encargarse de distribuir el parche o software desarrollado para la comprobación de dicha información, tal y como sucede con los usuarios que soportan la instalación de sistemas antivirus.

Para mayor seguridad, las comunicaciones entre el sistema de acceso (enrutador) y los dispositivos clientes estarán cifradas para que el intercambio de información no sea capturado o se vea expuesto a ningún tipo de ataque malintencionado. Lo mismo ocurrirá en las comunicaciones entre el enrutador y los elementos de comprobación en Internet (Servidor Desarrollador y Servidor Centralizado) para el procedimiento de comprobación y constatación de las bases de datos del sistema antivirus.

Los puertos y protocolos utilizados para la seguridad en las comunicaciones dependerán del desarrollo del fabricante por un lado o bien por la seguridad implementada en el sistema centralizado por el organismo o empresa que explota las características del sistema de acceso.

- Geolocalización:

El sistema de acceso propuesto también puede incorporar mecanismos por los cuales será capaz de localizar el elemento de red (y en una realización también a los dispositivos) y relacionar la ubicación como una comprobación de estado y por consiguiente dotar de una protección añadida al dispositivo de red en el que esté albergado este nuevo sistema de acceso (por ejemplo, un enrutador o conmutador de la red).

El sistema de geolocalización aportará entonces el posicionamiento (por ejemplo, las coordenadas geográficas de latitud, longitud y altitud) para el tratado de los datos basándose en a la información del elemento de red o información del dispositivo y de los usuarios registrados en el sistema de autenticación. Supone una mejora de las capacidades del nuevo elemento de red para generar registros de los dispositivos cliente conectados, así como un nuevo procedimiento de protección en cuanto a los servicios prestados por el dispositivo a los clientes, ya sea acceso a Internet, TV, Telefonía, entre otros. En resumen, con el uso del nuevo elemento de red y los mecanismos software y hardware que incorpora, se introduce una nueva solución de trazabilidad que aporta mayor confiabilidad y protección, no solo a los usuarios conectados sino a los organismos que intervienen en la seguridad global de Internet.

Para localizar al dispositivo o elemento de red, se puede usar cualquier procedimiento de geolocalización conocido tal como, por ejemplo, GPS, geolocalización por la dirección IP, geolocalización por red móvil (ID célula de origen), GPS asistido, E-OTD, TOA, huella multicamino, potencia de la señal recibida… o cualquier otro tipo de sistema de geolocalización (es decir, cualquier tecnología que permita localizar geográficamente al dispositivo, dando su ubicación exacta o relativa).

En una realización, la geolocalización se realizará mediante un módulo GPS (Sistema de Posicionamiento Global) incorporado en el elemento de red e integrado con el resto de HW que lo compone. El GPS realizará comprobaciones de estado de las coordenadas cada periodo de tiempo predeterminado en la fabricación y puesta

en marcha del dispositivo. Normalmente, este valor no debería poder ser modificado por motivos de seguridad ya que el hecho de que se pudiera desactivar, supondría una vulneración de las políticas de seguridad y de la jerarquía de niveles sobre la que se sustenta la solución.

Existen casos en los que el GPS no podrá ofrecer los valores de posicionamiento. En tal caso se contemplan otros procedimientos tales como, por ejemplo: posicionamiento manual (introducir manualmente las coordenadas de geolocalización del dispositivo, que será certificada conectándose con un servidor que verifique dicha ubicación), Posicionamiento facilitado por terceros (por ejemplo, el proveedor de servicios facilita dicha información al enrutador mediante cualquier procedimiento utilizado por el proveedor, tal como, por ejemplo, por ejemplo, E-OTD, TOA, RSS,...) o GeoPing (permite posicionar dispositivos mediante la latencia del protocolo ICMP).

En estos aspectos, los dispositivos cliente (también llamados dispositivos de usuario) conectados con el elemento de red (enrutador) para acceder a la red, podrán ser móviles o estáticos. Si son móviles, se les asignará un perfil de usuario que contemple la variación de las coordenadas de geolocalización del dispositivo, mientras que los dispositivos estáticos se asociarán a perfiles de usuario que por sus características no tengan que sufrir en ningún caso comprobaciones en cuanto a las variaciones coordenadas. Esto es un factor importante a la hora determinar una decisión sobre las comunicaciones que gestiona el dispositivo ya que, por ejemplo, no se tratará de igual manera un Smartphone (móvil) que a un decodificador de señal de televisión o una SmartTV (estático). De esta manera, por ejemplo, si el dispositivo es móvil (tableta, teléfono inteligente…), podrá tener acceso a otro tipo de redes y puede ser gestionado por el software en la nube del centro de servicio y podrá tener unas coordenadas diferentes en cualquier momento, mientras que los sistemas estáticos tal como una SmartTV, siempre deben tener las mismas coordenadas. La información de que el dispositivo sea estático y dinámico, puede, por ejemplo, introducirla el administrador en el enrutador cuando registra dicho dispositivo en las tablas del enrutador durante su configuración.

Las funciones principales del sistema de geolocalización serán las de ubicación del enrutador (que estará geolocalizado) y la trazabilidad de las conexiones del usuario final. También se podrán ubicar los dispositivos asociados al enrutador, estén o no estén dentro del rango de red. En otras palabras, cuando los dispositivos están conectados a la misma red a la que pertenece el enrutador (red interna), a los dispositivos se le pueden asignar las coordenadas del enrutador, pero cuando no estén en a la misma red a la que pertenece el enrutador (es decir, están conectados al enrutador a través de una red externa) tendrán las coordenadas de ubicación que le corresponda (obtenidas por ejemplo a través de cualquier mecanismo de geolocalización que tenga el dispositivo, tal como GPS), pero en ningún caso será la del enrutador.

La ubicación de los dispositivos y/o elemento de red supone una mejora sustancial de seguridad para casos en los que el robo, pérdida o uso malintencionado se produzca. La información de la geolocalización del elemento de red o dispositivo será almacenada (por ejemplo, en los servidores ubicados en el centro de servicios centralizados del cliente) para que estén a disposición del enrutador cuando tenga que realizar tareas de comprobación o modificaciones autorizadas sobre la misma. Estos centros de servicio son plataformas donde se accede a los enrutadores de los clientes (usuarios) para poder gestionar los dispositivos y el enrutador de forma remota desde Internet. Se establecerá un enlace seguro con dichos servidores entre los cuales las comunicaciones serán cifradas evitando de esta manera que la información sea expuesta en entornos no deseados. Una vez se establezca la posición del dispositivo, se realizarán periódicamente chequeos para que en el caso de que haya alguna variación en las coordenadas, el sistema de autenticación de acceso determine la acción a tomar. Si la ubicación actual del enrutador o dispositivo no se corresponde con la última posición autorizada por los administradores de la red o bien por el instalador (que estará guardada en la base de datos de registro de coordenadas que se ha explicado anteriormente), normalmente el sistema de acceso tomará la decisión de bloqueo del dispositivo. Adicionalmente, en caso de que la ubicación actual corresponde con la última posición pues no se realizará ninguna acción.

Como punto adicional, y excepcionalmente, el nuevo elemento enviará un mensaje (a través de la información incorporada en el "Registro de coordenadas GPS" de la BBDD interna del sistema de autenticación) en el caso que haya alguna variación de estado de la geolocalización. Por ejemplo, cuando un cliente tiene los servicios contratados de plataformas de servicios (como DIGITAL PLUS), estos servicios, estarán asociados al enrutador y a las coordenadas del propio enrutador; si el enrutador cambiara su ubicación a una ubicación no permitida, el mecanismo de denegación Implícita bloqueará el acceso a dichos contenidos (como se ha explicado anteriormente) y se le enviará un mensaje a la plataforma de servicios advirtiéndole de dicho intento de acceso desde una ubicación no autorizada. Esto mismo se puede hacer a nivel de dispositivo, es decir, si el dispositivo tiene un mecanismo de geolocalización (por ejemplo, GPS), informará de su posición periódicamente al enrutador (o cada vez que quiera acceder a la red). Si el enrutador detecta que ha habido un cambio de posición y dicha posición no está dentro de las que tenga el enrutador en su base de datos como permitida, puede denegarle el acceso (a la red en general o a un servicio concreto).

Por otra parte, la trazabilidad de las conexiones del usuario se trata del mecanismo por el cual todas las comunicaciones de los dispositivos clientes (dispositivos de usuario) que gestiona el elemento de red propuesto (enrutador) dispositivo, no solo quedarán registradas, sino que existirá la posibilidad de enviar dicha información a terceros. Se encuentran los siguientes casos de trazabilidad:

■ Traza en paquete/datagrama: por el que la información de geolocalización de los dispositivos clientes viajará en la red en la que se encuentran. Es decir, el enrutador puede registrar periódicamente donde está ubicado el dispositivo (asignándole la propia posición del enrutador o la posición exacta del dispositivo obtenida a través de un sistema de geolocalización del dispositivo, por ejemplo, GPS), esta información de la ubicación puede incluirse en el datagrama del paquete o en la carga útil. Esta función, una vez se universalice el estándar, podría suponer el mayor control de las comunicaciones manteniendo el anonimato relativo, en cuanto a los usuarios de Internet.
■ Información de traza: el nuevo dispositivo registra las conexiones del dispositivo cliente y las almacena en una base de datos como medida de prevención de usos fraudulentos del dispositivo.

Se puede decir que este procedimiento de geolocalización tiene varias etapas:

- Cuando se inicia por primera vez el enrutador se toma la posición del mismo (mediante GPS o cualquier otro procedimiento). En una realización, el "registro de coordenadas GPS" tendrá predefinidas una serie de ubicaciones permitidas para el enrutador y se comprobará también si la ubicación del mismo está dentro de estas ubicaciones permitidas (si no es así, pues el enrutador se bloqueará).
- El nuevo enrutador guarda la información de geolocalización en el "registro de coordenadas GPS" y, opcionalmente, envía la información de la geolocalización al centro de servicios centralizados en el que se almacenará dicha información.
- Comprobación del posicionamiento: periódicamente, el dispositivo (por ejemplo, el enrutador) obtiene su ubicación actual y la envía a una base de datos para que se compare con la última posición del dispositivo guardada (es decir, compara la posición actual con la última posición autorizada), y si ha cambiado, se bloquea. En una realización, el "Registro de Coordenadas GPS" tendrá predefinidas una serie de ubicaciones permitidas para el enrutador y se comprobará también si la ubicación del mismo está dentro de estas ubicaciones permitidas.

En una realización, estas tres etapas también se aplican a la posición de los dispositivos que acceden a la red a través del enrutador (es decir, se obtiene la posición del dispositivo, se guarda dicha información o se envía al centro de servicios centralizados y periódicamente se comprueba si ha cambiado de ubicación y si la nueva ubicación está permitida; en caso contrario se le denegará el acceso).

Nivel 3: Bases de datos externa (base de datos de acceso externo)

Para poder otorgar al elemento de red propuesto en la presente invención (por ejemplo, enrutador) de una protección de alto nivel, existen una serie de mecanismos que tiene como objetivo principal apoyar a los mecanismos que pertenecen a la base de datos interna, para obtener información adicional de redes externas o indexar o correlacionar cualquier tipo de datos.

Al llamarlo Base de datos externa, quiere decir que este nivel tiene acceso al exterior y puede ser accedido desde el exterior, pero no quiere decir que las bases de datos que se encuentran en este nivel sean necesariamente externas al elemento de red (enrutador), sino que son bases de datos que se pueden encontrar en el enrutador y que pueden tener acceso a información exterior.

Para llevar a cabo estos mecanismos de apoyo, se usan una serie de tablas (o registros) que se encuentran almacenados en una (o varias bases de datos) del enrutador que tiene acceso a redes externas/internet (por eso se llama base de datos externa).

Estos mecanismos pueden comprender un servicio NTP, un servicio de clasificación de contenidos, un servicio de sincronización de usuario único, un servicio antivirus y un servicio de geolocalización.

- Servicio NTP:

El servicio o protocolo NTP (Network Time Protocol) es un protocolo que se utiliza para obtener y asegurar el tiempo y fecha) exacto. Para ello se puede consultar por ejemplo a un servidor externo (servidor NTP). En una realización, el enrutador puede tener una medición confiable del tiempo exacto y no haría falta consultar a un servidor externo. NTP es utilizado para el tiempo y la fecha del reloj en todos los dispositivos de una red y usa el horario universal coordinado (UCT) en el puerto 123 para establecer la comunicación entre el dispositivo cliente y el servidor. En la presente invención caso, el servicio NTP está orientado en proporcionar al enrutador, la fecha y hora exactas, lo que le posibilita la automatización de distintos mecanismos de seguridad especialmente del sistema de autenticación, como se ha explicado anteriormente (asignar perfiles de control parental, saber si el acceso a la red se produce dentro del horario autorizado), con esto se consigue maximizar la seguridad de la red y mejorar la gestión de la misma.

Así, por ejemplo, el servicio NTP permite:

- Sincronizar la fecha y la hora de todos los dispositivos y usuarios.
- Identificar las edades de los usuarios que estén registrados en la base de datos, para poder determinar las edades de los usuarios en cada momento, con esta metodología podemos saber la edad de un usuario y

basándose en esta edad aplicarle un filtro u otro (CONTROL PARENTAL). El sistema lo hace automáticamente y no es necesario la actuación del administrador del sistema.

- Identificar el calendario aplicable a la localidad de los usuarios y así poder ofrecer unos límites de tiempos individuales para cada perfil y usuario, es decir si el usuario de la red a la que está conectada se le asocia por ejemplo el código postal de una localidad en concreto, el servidor tendrá el calendario laboral local y el calendario festivo, con lo cual se le aplicaran las políticas de tiempo basándose en el calendario local.

En una realización, el enrutador puede tener configurado el servicio NTP en la dirección http://www.pool.ntp/tecteco.org. Cuando se solicita la fecha y hora, esta solicitud llega al servidor NTP y basándose en la localidad donde está ubicado el enrutador le asigna un perfil de fecha. El servidor NTP, a su vez se tiene comunicación constante con el servidor NTP global http://www.pool.ntp.org/, para adquirir los parámetros de configuración de hora.

Aunque el servicio NTP es el más común, por supuesto, el sistema de acceso propuesto puede usar otros servicios para obtener los datos de fecha y hora que necesita para aplicar los distintos mecanismos de seguridad.

- Servicio de clasificación de contenidos de redes:

Como se ha indicado existe un sistema de clasificación de contenido de redes externas (Internet) por edades que usa un analizador semántico, que descarga las páginas web que quieren visitar los usuarios de control parental, para analizar el contenido de la web y bloquear el acceso a la web dependiendo del contenido de la misma.

En este nivel de base de datos externa, existe un módulo del servicio o sistema de clasificación de contenidos de redes externas (Internet) que es el encargado de nutrir al analizador semántico, con el contenido de las páginas webs que este quiere analizar. Esta "descarga" de páginas web para el analizador semántico puede ser periódica. Una vez analizado el contenido de las páginas web, el analizador semántico actualizará su propia base de datos, indicando si el acceso a dichas páginas web está permitido o no a los usuarios con un determinado perfil y categoría (por ejemplo, control parental menor de 12 años).

- Servicio de sincronización de usuario único (también llamado servicio de sincronización de usuario a nivel global):

Este nuevo servicio o sistema que se puede incorporar a la presente invención, intenta resolver el problema que existe actualmente a la hora de perseguir e identificar a un usuario en la red, por ejemplo, cuando el usuario comete algún delito. Para ello, este sistema está dividido en dos componentes fundamentes uno de ellos es el identificar realmente a todos los usuarios (y a los dispositivos, pseudónimos (nombres de usuario), cuentas de correo y cuentas de servicios de estos usuarios) que se encuentran en Internet (en otras palabras, identificar a la persona física que hay detrás de cada usuario) y nutrir a una base de datos a nivel mundial (una base de datos internacional y/o sincronizada con bases de datos de otros países o de organismos gubernamentales…) con esta información para la gestión y control de dichos usuarios.

El funcionamiento consiste en que todos los usuarios registrados en el nuevo sistema de autenticación nutran a la entrada del nivel de base de datos externa del enrutador con información que identifique a la persona física detrás del usuario (y esta información se envíe a una base de datos a nivel mundial). Para ello, en una tabla del enrutador (por ejemplo, en la tabla de control de usuarios/contraseña) se guarda y registra información del usuario tal como, por ejemplo: nombre y apellidos, DNI u otra identificación, número de teléfono, fecha de nacimiento, servicios en la red, tal como por ejemplo XBOX LIVE, PSN PLUS, Facebook, etc., correos electrónicos, conexiones externas, vinculación de dispositivos etc. Esta información se le pide al usuario, por ejemplo, cuando el usuario se registra en la red (que puede ser cuando intenta el usuario acceder al enrutador por primera vez o con anterioridad). En una realización, si el usuario no proporciona esta información se le puede denegar el alta como usuario (es decir, no se registra como usuario autorizado) y, por lo tanto, no podrá acceder a la red. Esta información sobre los usuarios es enviada para que quede registrada en una tabla alojada en el nivel de base de datos externa al enrutador, por ejemplo, en una tabla SYN_USERID_WORLD que, preferentemente, tiene un formato que la hace exportable y entendible por dispositivos a nivel global. De esta manera esta información que está alojada en la base de datos externa, pueda ser enviada y sincronizada con una base de datos a nivel mundial. Para el correcto funcionamiento y para no corromper los datos extraídos de la base de datos que contiene dicha información, puede ser necesaria la instalación de una segunda base de datos esclava dentro de la infraestructura de los distintos operadores de servicios de Internet (que se comunicará con otros organismos institucionales/gubernamentales). De esta manera, el servidor o servidores principales de esta base de datos a nivel mundial, estarán alojados en los distintos centros de datos de los edificios gubernamentales y tendrán acceso a datos que identifican a las personas físicas que hay detrás de todos los usuarios de todas las redes.

- Servicio de antivirus:

El servicio de antivirus a este nivel, es un servicio para chequear la versión del antivirus que está corriendo en los dispositivos, también tiene la labor de contrastar la lista de virus en tiempo real. Con esta información, como se ha explicado anteriormente, se podrá ofrecer el servicio de antivirus que se explicó en el nivel 2, en el que el enrutador podrá tomar una decisión de acceso en cuanto a las conexiones que gestiona de cada dispositivo.

Así, la base de datos interna, solicitará la información que necesite de estado antivirus de cada dispositivo al servicio de antivirus de nivel 3 (por ejemplo, información sobre la versión de antivirus de un dispositivo cliente). Una vez que la solicitud es recibida por el servicio de antivirus, este servicio consulta sus tablas (de actualización de bases de datos de aplicación antivirus y de virus y troyanos) y los fabricantes de antivirus y el centro de servicio. Una vez obtenida la información, por sus fuentes es puesta a disposición de la base de datos interna que no cierra la comunicación con el servicio de antivirus, hasta que este no le contesta. Por seguridad, el servicio de antivirus que reside en la BBDD Externa, no puede acceder a los elementos que componen la BBDD Interna

- Servicio de geolocalización:

Igualmente, el servicio de geolocalización a este nivel realizará las acciones que impliquen comunicación con una red externa, que sean necesarias para ofrecer el servicio de geolocalización que se explicó en el nivel 2.

Una vez explicados los distintos elementos que existen en el elemento de red (por ejemplo, enrutador) y su funcionamiento, para ayudar a aclarar el procedimiento completo de acceso a la red y la interacción entre los distintos elementos, se va a exponer a continuación un ejemplo de modo de funcionamiento de acuerdo con una realización de la invención. Para ello, se usará la Figura 8 que muestra de manera esquemática la interacción entre los distintos elementos en un ejemplo de funcionamiento de la invención propuesta.

En el ejemplo expuesto en la Figura 8, un usuario (usuario 1) quiere acceder a la red de comunicaciones usando un dispositivo electrónico (dispositivo 1), para ello, cuando el dispositivo quiere acceder a la red, le envía una solicitud de acceso (en un mensaje de capa 2 del modelo OSI) al enrutador y este, una vez recibida la solicitud de acceso, le solicitara una serie de datos. El dispositivo puede estar conectado a una red de comunicaciones externa a la red de comunicaciones a la que pertenece el enrutador y, en ese caso, la solicitud de acceso vendrá a través de esa red externa. Si el dispositivo está conectado a la red de comunicaciones a la que pertenece el enrutador, en ese caso, la solicitud de acceso vendrá a través de esa red.

En primer lugar el enrutador comprueba si el identificador del dispositivo (dirección MAC, IMEI, IMSI, MSISDN u otra identificación) está registrado en el "Registro de direcciones MAC Denegadas". Si lo está, el dispositivo no se le dará acceso a la red. Si no es así, se comprueba si el identificador está en el registro de direcciones MAC autorizadas. Si no está, entonces se registrará el identificador en el registro de direcciones MAC denegadas y se le denegará el acceso al dispositivo. Sin embargo, si está registrada en el "registro de direcciones MAC Autorizadas" comenzará el procedimiento de autenticación.

El registro en dicha tabla de dispositivos autorizados, permitirá abrir los puertos físicamente de las direcciones MAC que están registradas, como se ha descrito anteriormente. En otras palabras, si un dispositivo autorizado (su dirección MAC está en la tabla de dirección MAC autorizadas) se conecta a través de un puerto que se ha cerrado anteriormente (porque un dispositivo no autorizado ha intentado acceder a través de él), este puerto se abrirá automáticamente. Cuando el dispositivo autorizado finaliza la conexión de red y deja el puerto libre, el puerto permanecerá abierto, pero si el dispositivo que no está registrado (que ha accedido antes), quiere volver acceder ahora ya que el puerto 1 está libre (sin uso), el sistema volverá a cerrar el puerto.

Para la autenticación, en primera instancia el enrutador solicita la identificación del usuario que está accediendo y su contraseña para proseguir con la negociación (esto lo solicita el enrutador al dispositivo a través de la propia red de comunicaciones o de la red externa si el dispositivo está conectado a la red de comunicaciones a través de una red externa). El sistema de autenticación realizará las comprobaciones necesarias y contrastará la información recibida por el usuario y tomará las decisiones correspondientes. Por lo tanto, si el usuario, está registrado en el "registro de usuarios denegados", o no está registrado en la base de datos como usuario autorizado (en la tabla de "control de usuario/contraseña") o la contraseña es incorrecta, no continuará el procedimiento. En ese caso, dicho usuario se registrará en el "registro de usuarios denegados" como medida de protección, ya que, si el usuario quiere volver a acceder a la red, el servicio de denegación implícita denegará el acceso al usuario indefinidamente. Si el usuario está registrado en la base de datos continuará el procedimiento.

Una vez que el usuario esté registrado correctamente, el procedimiento de autenticación comprueba el siguiente nivel, control de dispositivos. En la tabla de control de dispositivos, el enrutador comprueba la vinculación del usuario con los dispositivos registrados, es decir comprueba que el dispositivo 1 que está utilizando, esté registrado en dicha tabla y vinculado con dicho usuario que está solicitando el acceso. Si el usuario no está vinculado al dispositivo con el que esta solicitado el acceso, no continuará el procedimiento de autenticación y no podrá acceder a la red y dicho usuario se registrará en el "registro de usuarios denegados". Si el usuario está vinculado al dispositivo proseguirá el procedimiento de autenticación.

Asimismo, como medida de protección, un usuario tiene que estar vinculado a algún dispositivo registrado de la red, si el usuario que está creado correctamente (es decir, la contraseña que ha introducido coincide con la contraseña que el enrutador tiene guardada para dicho usuario) no ha sido vinculado a ningún dispositivo, dicho usuario no tendrá acceso a la red y se le apuntará en el registro de usuarios denegados.

Una vez comprobado que el usuario está vinculado al dispositivo con el que accede a la red, el procedimiento de autenticación continúa y procederá a comprobar los datos en la entrada (tabla) de perfiles de usuario. En esta

entrada se asignará al usuario un perfil de acceso a la red. Estos perfiles estarán predefinidos en el enrutador y pueden ser, por ejemplo, administrador, estándar, control parental o cualquier otro tipo de perfil predefinido. Si el usuario es considerado menor de edad, el enrutador automáticamente añade dicho usuario al perfil de control parental, (perfil de clasificación por edades).

Una vez que se le ha asignado un perfil, el usuario, continúa con el procedimiento, el siguiente procedimiento es el tiempo de acceso a la red. Para ello, se usa la tabla de políticas de tiempo (o tiempo de acceso) que se ha explicado anteriormente (ver Figura 3). Si el usuario no está definido o registrado en esta tabla, el procedimiento no continuará y no el usuario tendrá acceso a la red (y se registrará en el registro de usuarios denegados). Si el usuario está definido en la tabla, se aplicará el tiempo de acceso configurado en dicha tabla y continuará el procedimiento de acceso. Si el usuario es menor de edad, se le asignará las políticas de tiempo de acuerdo con la edad de cada usuario menor de edad. Estas políticas de tiempo pueden ser predefinidas por el sistema, definidas por el administrador del sistema o predefinidas por la edad del usuario. Una vez terminado el procedimiento de tiempo de acceso, los usuarios tendrán acceso a la red durante el tiempo que este estipulado en la entrada correspondiente de tiempo de acceso (si intentan acceder fuera de las horas estipuladas en esta tabla, el enrutador le denegará el acceso).

La siguiente etapa es gestionar el acceso a los servicios usando las políticas de seguridad definidas en la tabla de políticas de seguridad explicada anteriormente (ver por ejemplo Figura 4). Aquí se definen los accesos a la red, ya sea interna o externa, que están permitidos para cada usuario. Estas reglas son análogas a las que existirían en un cortafuegos de la red, es decir, se puede establecer una comunicación determinada dependiendo del origen, destino, servicio y/o puerto lógico. En una realización, en estas reglas de seguridad, tienen que aparecer los usuarios, dispositivos, grupos de usuarios y perfiles, para poder acceder a la red. Toda comunicación que no esté definida en estas reglas o políticas, se le denegará el tráfico, tanto como de dentro hacia fuera, como de fuera hacia dentro.

Con esto se termina el procedimiento de autenticación. Una vez terminado, todas las actividades de los usuarios y dispositivos se pueden registrar y almacenar en una tabla de registro de actividad (LOG).

Pasada la autenticación, si todas las comprobaciones de autenticación son positivas se otorgará el acceso a la red. Si el usuario no tiene asignada la dirección de red (y otros parámetros de configuración de red de capa 3, necesarios para acceder a la red), el usuario para acceder a la red, deberá solicitarlos al elemento de red y se pasa al procedimiento que se explica a continuación. Si el usuario ya tiene asignados estos parámetros de configuración de red de capa 3 (porque el usuario tiene estos parámetros de un acceso anterior o porque el usuario ha introducido estos parámetros en el dispositivo manualmente) no es necesario que el dispositivo los solicite al enrutador.

Para solicitar y obtener los parámetros de configuración de red, se usará el servicio SDHCP. Como se ha explicado anteriormente, se recibirá del usuario información del dispositivo desde el que está accediendo (MAC, IMEI, IMSI, MSISDN, u otra identificación del dispositivo), una vez que el SDHCP reciba la identificación del dispositivo, el SDHCP decidirá:

si la identificación del dispositivo no está registrada en la base de datos (en la tabla correspondiente, en este caso, en el contenedor de "registros de direcciones MAC permitidas"), no continuará con el procedimiento, no se le asignará los parámetros de red y, como resultado, no tendrá acceso a la red. Este dispositivo se registrará en el contenedor de "registros de direcciones MAC denegadas" como medida de protección, ya que si el dispositivo quiere volver a acceder a la red (más de un determinado número de veces), el servicio de "denegación implícita" bloqueará el puerto físicamente. El comprobar aquí otra vez, si el dispositivo está registrado en la base de datos, es optativo ya que ya se ha comprobado al principio del procedimiento, antes de la autenticación. Sin embargo, como medida de seguridad, en una realización se realiza esta comprobación aquí también.
Si la identificación (identidad) del dispositivo está registrada en la base de datos, el servidor SDHCP (el enrutador) le asignará los parámetros de red basándose en los perfiles o roles de cada dispositivo.

Como se ha explicado anteriormente estos perfiles o roles pueden ser, por ejemplo, de Invitados, domótica, cuarentena, red cableada o red WIFI. Dependiendo del identificador (por ejemplo, de la dirección MAC del dispositivo), se le asignará un perfil u otro, lo que implicará que se le asigne un rango de direcciones IP u otro.

Una vez terminado este procedimiento de obtención de parámetros de configuración de red, el dispositivo tendrá dirección IP (capa 3 del modelo OSI), con lo cual, el dispositivo ya tendrá acceso a la red parcialmente. La siguiente comprobación que realiza el enrutador es chequear si el dispositivo está infectado por un virus o troyano y si es correcta la versión de antivirus que tiene instalada, para ello el servicio de antivirus podrá realizar las siguientes acciones, de acuerdo con una realización de la invención:

Si el dispositivo está infectado o no tiene instalada la última versión del software de antivirus se le puede denegar el acceso o el servicio de antivirus al dispositivo puede enviar un mensaje al servidor SDHCP para que modifique el perfil del dispositivo y lo asigne al perfil de cuarentena.
Si el dispositivo no está infectado y tiene la versión del software actualizada, tendrá acceso a la red y a todos los servicios y recursos de la red interna.

Cuando el dispositivo ha terminado el procedimiento de autenticación, solicitud de parámetros de configuración y

comprobación de estado de antivirus, si el dispositivo quiere acceder a Internet o una red externa, el Servicio de Geolocalización, podría etiquetar el tráfico de salida con las coordenadas del enrutador, estas coordenadas servirán para identificar el usuario en el destino. El servicio de geolocalización también tendrá la opción de denegar el servicio del enrutador o del dispositivo si el enrutador o dispositivo cambia de ubicación (a una ubicación no autorizada). Si fuera el caso que se cambiará de ubicación del enrutador, el servicio de geolocalización registrará el cambio en el "registro de coordenadas GPS", y la "denegación implícita" denegará el acceso (por ejemplo, a plataformas de medios digitales).

En una realización, el procedimiento completo anteriormente descrito (con autenticación completa y solicitud de parámetros de configuración de red) sólo se hará la primera vez que el dispositivo y usuario accede a la red y cada vez que el dispositivo y el usuario establezca una comunicación nueva con la red. Si el dispositivo y usuario, está usando una comunicación ya establecida, ya tendrá parámetros de configuración de red (dirección IP) y ya estará autenticado, por lo que no hará falta hacer el procedimiento completo otra vez sino sólo parte de él. En una realización, una vez que el usuario este correctamente autenticado y con su dirección IP, solo se comprueban las políticas de tiempo y de seguridad (y opcionalmente se comprueba la geolocalización y el antivirus) cada vez que accede a la red, para asegurar que está accediendo a la red dentro del plazo temporal autorizado y que el acceso es a páginas web, destinatarios o servicios autorizados por las políticas de seguridad (incluyendo las políticas de control parental).

Resumiendo, se puede decir que el mecanismo de acceso a una red de comunicaciones propuesto ofrece unas capacidades de protección, gestión y automatización mucho mayor de los sistemas que hay en la actualidad. Se puede decir, que con esta nueva generación de enrutadores, la administración y la gestión es mucho más sencilla que la actual, ya que el administrador de la red o del sistema (a la hora de un posible problema o una modificación de los parámetros de configuración) no tendrá necesariamente que interactuar con el enrutador de nueva generación, si no que basándose en los mecanismos que incluye dicho enrutador, el propio enrutador automáticamente buscará y aplicará la mejor solución para dichos problemas, notificando opcionalmente al administrador el problema y la solución dada. Con esta nueva generación de enrutadores se han evolucionado estándares, protocolos y elementos de red que llevaban más de una década sin evolución, tal como pueden ser los enrutadores, conmutadores o cortafuegos.

Las ventajas que ofrece el elemento de red propuesto (con el sistema de acceso global objeto de la presente invención) son, entre otras:

- Mayor protección de acceso externo a la red ya que se detecta la intrusión en el primer segmento de la red más expuesto conectado al enrutador (Internet o redes extensas con un gran número de usuarios). Una de las técnicas de ataque informático más ampliamente utilizadas para la recolección de información sensible del usuario, es el de suplantación de identidad o phishing. Con la protección que otorga el sistema de autenticación de la nueva solución, los usuarios no estarán expuestos a tales ataques debido a la jerarquía por niveles diseñada para que exista correlación entre elementos de las dos BBDD que alberga la solución. La jerarquía añade además aislamiento y control de cada uno de los campos u objetos almacenados en las BBDD de tal manera que únicamente existan los flujos determinados internamente en el propio sistema y que han sido concebidos para que no puedan ser manipulados por terceros de forma malintencionada.
- Aumento de confiabilidad con todos los dispositivos de una LAN: debido a las comprobaciones de estado de cada uno de los dispositivos mediante los controles de seguridad aplicados en cada nivel y el chequeo de antivirus, que nunca se han integrado en ningún enrutador o equipo de acceso a la red.
- Desaparición de "anonimato relativo" en la red, vinculando usuarios con información real del mismo (información del cliente final tal como nombre y apellidos, correo, teléfono, coordenadas GPS, servicios a terceros, DNI…). Toda la información referente al usuario podrá ser trasladada a los organismos que regulan la red sin que esto suponga una vulneración de la intimidad sino un elemento adicional para la seguridad de sus comunicaciones. Hoy en día existen datos públicos de los usuarios proporcionados por los proveedores de servicios, pero no llegan al nivel de detalle que los servicios de Internet reclaman para la seguridad de sus clientes. Esto afecta directamente a la confiabilidad cliente/servidor que es el pilar que sustenta la seguridad en las comunicaciones dentro de una red.
- Fácil gestión de roles o perfiles: El enrutador detecta los diferentes identificadores de los dispositivos de la red y los sistemas operativos que los alberga (MAC, asignación, NetBIOS etc., por lo que la creación de usuarios no supondrá ningún reto para el administrador de la red. Los roles incorporarán reglas predeterminadas en las políticas del módulo de cortafuegos con relación al sistema de control parental. Con esta acción prestablecida se ejecuta una relación entre la comprobación automática del perfil de usuario y los sitios y servicios ofertados en Internet sin que el usuario administrador tenga que tener altos conocimientos de seguridad y comunicaciones.
- Automatismo de protección: gracias a la correlación y los registros de los datos de la red, la denegación implícita está capacitada para tomar una serie de decisiones para mejorar la protección a la red, denegando automáticamente aquellas comunicaciones que puedan tener carácter fraudulento: esto añade inteligencia al enrutador para procesar y ejecutar acciones sobre los elementos hardware del dispositivo o el perfil de usuario. Tal y como ocurre con las BBDD, la denegación implícita forma parte de la estructura jerárquica de niveles de seguridad, que en este caso concreto siempre estará al margen de los datos de los usuarios que contienen las BBDD. Por lo tanto, el blindaje de este automatismo está garantizado.
- Control de contenidos: aplicación de políticas de seguridad y filtrados de contenidos basándose en el perfil de

usuario totalmente integrado en el sistema de autenticación, otorgándole una inteligencia ya que el sistema de autenticación es totalmente automático y aprende basándose en las amenazas detectadas en el transcurso de las comunicaciones del usuario además de establecer las políticas a nivel de usuario basándose en dicho aprendizaje.

- Única instancia de identificación: Podemos decir que se produce un SSO (Single Sing On) entre los diferentes elementos del enrutador. El usuario solo tiene una única identificación para las diferentes funciones del enrutador y sus componentes, cortafuegos W, clasificación de contenidos... Habitualmente la relación número de autenticaciones con el número de servicios es de 1 a 1 mientras que, con este único procedimiento de autenticación, el usuario podrá validar mediante una única autenticación numerosas acciones en los diferentes módulos del dispositivo. A diferencia de las soluciones actuales no utiliza un único elemento que valide la autenticación sino varios identificadores únicos que se relacionan específicamente entre sí.
- Interoperabilidad con los protocolos actuales: El enrutador propuesto, sus mecanismos y sus componentes, funcionan correctamente con los protocolos y estándares actuales y pueden coexistir con los elementos externos del proveedor de servicios y los organismos gubernamentales. La compatibilidad con los protocolos de comunicaciones actuales será total debido a que no hay manipulación de los paquetes de datos y por consiguiente de las cabeceras de estos que son los que contienen la información referente a los protocolos de comunicaciones. Respecto a la integración, sirva de ejemplo la opción que tendrán los operadores de red para que, el usuario que se valide en este nuevo dispositivo y sus credenciales, puedan ser heredadas por los sistemas de acceso a la red de servicio que el operador administra.
- Funciona con cualquier tipo de dispositivo con acceso a redes (por ejemplo, Internet), con cualquier tipo de conexión (actuales y futuras) y con cualquier tipo de capa de Transporte (ADSL, VDSL, FTTH, RDSI, Frame relay, Macrolan…).
- Mejoras en las capas del modelo OSI, mejorando los estándares y protocolo de cada una de las capas. Las mejoras más considerables se efectúan en la capa o nivel 2 y 3 del modelo OSI donde se incorporan nuevos elementos de seguridad que transformarán los protocolos que actúan sobre estas añadiendo protección al usuario final, así como a la propia infraestructura de la red. Protocolos tales como Spanning Tree o DHCP requerirán la validación del sistema de autenticación para un funcionamiento de acuerdo con el nivel de seguridad exigido en la nueva solución.
- Nuevos vínculos entre las capas del modelo OSI, haciendo posible un solo punto de control de las comunicaciones en el acceso a una red sea o no de confianza. Se garantiza un control de las comunicaciones aunando identificadores de red de los protocolos de los diferentes niveles OSI, respetando la jerarquía del modelo de referencia actual. En otras palabras, mediante la solución propuesta, se asocian elementos identificadores del nivel 2 OSI con información del usuario final referente a otros niveles del modelo OSI tales como IP, puertos TCP/UDP, así como protocolos de la última capa (aplicación) tal como puede ser el usuario de correo. Esto no quiere decir que la información viaje dentro del paquete de datos, sino que se utiliza la relación de cada elemento identificador para dotar de protección al usuario. Sirva como ejemplo el hecho de establecer un enlace entre la MAC y el usuario de correo electrónico para permitir o denegar las comunicaciones que atraviesan el dispositivo con la nueva solución implementada.
- Obtención de trazabilidad de manera más exacta y con menos recursos, tiempo y costes mediante el nuevo sistema de autenticación y geolocalización. Se incorporan datos unívocos de cada usuario que utiliza la infraestructura de red, así como de los servicios alojados en esta. Los datos únicos del usuario tienen como objeto proporcionar registros de actividad que puedan determinar la ubicación del usuario. Esto supone, no solo una etapa para validar el acceso del usuario en los diferentes entornos de red a los que esté conectado el dispositivo, sino un aporte de información para la administración y protección de los recursos de la red. Esto se debe considerar como un funcionamiento similar al estándar AAAA en el que la auditoría de red queda reflejada como acción preventiva para el uso malintencionado de los elementos que componen la red.

Hay que indicar que no todos los elementos incluidos en el enrutador, que se han expuesto en este documento son obligatorios para el funcionamiento de la solución de acceso global a la red propuesta por la presente invención; muchos de ellos son opcionales y dependiendo de la aplicación particular y de las prestaciones que se deseen pueden incluirse o no.

Aunque muchas de las realizaciones presentadas están referidas a enrutadores, la presente invención no está limitada a su aplicación en enrutadores, pero también en otros elementos de red como, por ejemplo, conmutadores, cortafuegos, splitters y en general a cualquier elemento que se considere que realice las funciones de gestión del acceso a la red, bien en su totalidad o en parte. Véase, por ejemplo, el caso en el que la puerta de enlace de la red sea un cortafuegos, denominado así por incorporar capacidades de seguridad, que al realizar las funciones de segmentación (conmutador) o delimitar redes (enrutador), entre otras funciones, puedan aplicarse los mecanismos de seguridad detallados.

Obsérvese que, en este texto, términos relacionales tales como primero y segundo, superior e inferior y similares, pueden ser usados únicamente para distinguir una entidad o acción de otra, sin necesariamente requerir o implicar realmente esa relación u orden entre dichas entidades o acciones. Adicionalmente, el término "comprende" y sus derivaciones (tales como "comprendiendo", etc.) no deberían ser entendidos en un sentido de exclusión, es decir, estos términos no deberían ser interpretados como excluyentes de la posibilidad de que lo que se describe y define pueda incluir elementos, etapas, etc., adicionales.

Algunas realizaciones preferentes de la invención se describen en las reivindicaciones dependientes que se incluyen seguidamente.

Descrita suficientemente la naturaleza de la invención, así como la manera de realizarse en la práctica, hay que hacer constar la posibilidad de que sus diferentes partes podrán fabricarse en variedad de materiales, tamaños y formas, pudiendo igualmente introducirse en su constitución o procedimiento, aquellas variaciones que la práctica aconseje, siempre y cuando las mismas, no alteren el principio fundamental de la presente invención. La descripción y los dibujos simplemente ilustran los principios de la invención. Por lo tanto, debe apreciarse que los expertos en la técnica podrán concebir varias disposiciones que, aunque no se hayan descrito o mostrado explícitamente en este documento, representan los principios de la invención y están incluidas dentro de su ámbito. Adicionalmente, todos los ejemplos descritos deben considerarse como no limitativos con respecto a tales ejemplos y condiciones descritos de manera específica. Adicionalmente, todo lo expuesto en este documento relacionado con los principios, aspectos y realizaciones de la invención, así como los ejemplos específicos de los mismos, abarcan equivalencias de los mismos.

REIVINDICACIONES

1. Procedimiento para el acceso mejorado de un usuario (101) a una red de comunicaciones usando un dispositivo (102) electrónico, en el que el procedimiento comprende las siguientes etapas realizadas en la capa 2 del modelo OSI en un elemento de red, en el que el elemento de red es un enrutador o conmutador que gestiona el acceso a la red de comunicaciones:

a) recibir del dispositivo electrónico, un mensaje de capa 2 del modelo OSI que incluye una solicitud de acceso a la red y un identificador del dispositivo electrónico;
b) si dicho identificador del dispositivo electrónico está registrado en una base de datos interna del elemento de red como un identificador de un dispositivo (108) electrónico denegado, denegar el acceso a la red a dicho dispositivo electrónico y terminar el procedimiento, en caso contrario, proceder a la etapa c);
c) si el identificador del dispositivo electrónico está registrado en la base de datos interna como identificador de un dispositivo electrónico con acceso permitido a la red (104), proceder a la etapa d), y en caso contrario, almacenar la identificación del dispositivo electrónico en la base de datos interna como dispositivo (108) electrónico denegado, denegar el acceso a la red a dicho dispositivo electrónico y terminar el procedimiento;
d) recibir del dispositivo electrónico un identificador del usuario y una contraseña para dicho usuario en uno o más mensajes de capa 2 del modelo OSI;
e) si dicho identificador del usuario está registrado en la base de datos interna como identificador de un usuario (107) denegado, denegar el acceso a la red y terminar el procedimiento, en caso contrario, proceder a la etapa f);
f) autenticar al usuario, realizando al menos las siguientes comprobaciones:

f1) comprobar que el identificador del usuario está registrado en la base de datos interna como un identificador de un usuario autorizado y si la contraseña recibida corresponde a la vinculada a dicho usuario en la base (204) de datos interna;
f2) comprobar que el identificador del dispositivo electrónico está en la base (310) de datos interna como vinculado a dicho usuario;

g) si alguna de las comprobaciones realizadas en las etapas de autenticación es negativa, almacenar la identificación del usuario en la base de datos interna como usuario denegado, denegar el acceso a la red a dicho usuario y terminar el procedimiento; en caso contrario, proceder a la etapa h);
h) si se recibe del dispositivo electrónico un mensaje de capa 2 solicitando parámetros de configuración de red, comprobar si el dispositivo electrónico está registrado en la base de datos interna como un dispositivo electrónico con acceso permitido a la red; si es así, proceder a la etapa i), y en caso contrario, almacenar la identificación del dispositivo electrónico como dispositivo electrónico denegado, denegar el acceso a la red y terminar el procedimiento;
i) si la comprobación de la etapa h) es positiva, asignar un conjunto de parámetros de configuración de red al dispositivo electrónico dependiendo al menos del identificador del dispositivo electrónico y enviar dicho conjunto de parámetros de configuración de red al dispositivo electrónico.

2. Procedimiento de acuerdo con la reivindicación 1, en el que la etapa de autenticación del usuario además comprende las siguientes etapas de autenticación tras la etapa f2) y antes de la etapa g):

f3) obtener la fecha y/u hora en que se está produciendo el acceso y comprobar que dicha fecha y/u hora está dentro de los tiempos de acceso permitidos para dicho usuario y/o para dicho dispositivo electrónico, almacenados en la base de datos interna;
f4) comprobar que el acceso a la red que solicita el usuario está permitido por las políticas (416) de seguridad definidas para dicho usuario almacenadas en la base de datos interna;

3. Procedimiento de acuerdo con la reivindicación 2, en el que después de la etapa f2) se realiza una etapa de asignar un primer perfil de acceso al usuario, basándose al menos en la información almacenada en la base de datos interna para dicho usuario y, en el que, las políticas de seguridad y/o los tiempos de acceso permitidos para dicho usuario van a depender al menos del perfil que se le ha asignado.

4. Procedimiento de acuerdo con cualquiera de las reivindicaciones anteriores 2-3, en el que la etapa de comprobar que el acceso a la red está permitido por las políticas de seguridad en la etapa f4), comprende:

- comprobar que el destinatario y/o la página web y/o el servicio y/o el puerto al que quiere acceder dicho usuario de acuerdo con la solicitud de acceso recibida, está permitido en las políticas de seguridad definidas para dicho usuario almacenadas en la base de datos interna.

5. Procedimiento de acuerdo con cualquiera de las reivindicaciones 2-4, en el que después de la etapa f2) se calcula la edad del usuario basándose al menos en la información almacenada en la base de datos interna y si el usuario es menor de edad, se aplican unos tiempos de acceso permitidos específicos para usuarios menores de edad en la etapa f3) y se restringe el acceso a ciertas páginas web de acuerdo con la edad del usuario.

6. Procedimiento de acuerdo con la reivindicación 5, en el que si el usuario es menor de edad se realizan las siguientes acciones después de la etapa f2):

- clasificar al usuario en una categoría determinada de acuerdo con la edad del usuario;
- comprobar si la página web a la que quiere acceder el usuario está clasificada como accesible para dicha categoría en la que se ha clasificado al usuario y si no está clasificada como accesible, denegar el acceso y terminar el procedimiento; en el que para clasificar una página web como accesible se realiza un análisis del contenido semántico de dicha página web.

7. Procedimiento de acuerdo con cualquiera de las reivindicaciones anteriores que además comprende:

j) obtener periódicamente la ubicación del elemento de red;
k) comparar dicha ubicación con la ubicación obtenida previamente y si no coincide, bloquear el acceso a la red del elemento de red.

8. Procedimiento de acuerdo con cualquiera de las reivindicaciones anteriores, en el que la etapa i) comprende:

i1) asignar al dispositivo electrónico un segundo perfil de acceso obtenido de la base de datos interna, en función del identificador de dicho dispositivo electrónico;
i2) asignar al dispositivo electrónico un conjunto de parámetros de configuración de red en función del segundo perfil de acceso asignado al mismo, incluyendo dicho conjunto de parámetros de configuración de red una dirección de red para el dispositivo electrónico, en el que dicha dirección de red pertenece a un rango de direcciones de red disponibles para el dispositivo electrónico que depende del segundo perfil de acceso asignado al mismo;
i3) enviar un mensaje de capa 2 al dispositivo electrónico con los parámetros de configuración de red asignados al dispositivo electrónico.

9. Procedimiento de acuerdo con la reivindicación 8, en el que el segundo perfil asignado en la etapa i1) dependerá al menos de si el dispositivo electrónico está infectado por un virus y de si es correcta la versión de antivirus que tiene instalada el dispositivo electrónico, y en el que el procedimiento además comprende:

l) recibir información acerca del antivirus del dispositivo electrónico, en el que dicha información incluye si el dispositivo electrónico está infectado por un virus y/o si es correcta la versión de antivirus que tiene instalada el dispositivo electrónico;
m) si la información acerca del antivirus del dispositivo electrónico ha cambiado, cambiar el segundo perfil asignado al dispositivo electrónico en la etapa i1) y, por lo tanto, el rango de direcciones de red disponibles para el mismo.

10. Procedimiento de acuerdo con cualquiera de las reivindicaciones anteriores, en el que para permitir el acceso a la red, el elemento de red solicita al usuario información de usuario y si el usuario no proporciona dicha información, el elemento de red deniega el acceso a la red; en el que esta información de usuario incluye al menos uno de los siguientes parámetros: nombre completo del usuario, dirección postal, DNI, número de pasaporte, fecha de nacimiento y toda la información sobre el usuario que se encuentra en la base de datos interna, el elemento de red envía dicha información a una base de datos externa al elemento de red.

11. Procedimiento de acuerdo con cualquiera de las reivindicaciones anteriores, en el que la comunicación entre el dispositivo electrónico y el elemento de red se lleva a cabo en la etapa i) usando mensajes del protocolo DHCP.

12. Procedimiento de acuerdo con cualquiera de las reivindicaciones anteriores, en el que el identificador del dispositivo electrónico es al menos uno de entre los siguientes: la dirección MAC del dispositivo electrónico, el IMEI, el IMSI, el MSISDN o algún otro parámetro identificativo del dispositivo electrónico y en el que el elemento de red es un enrutador.

13. Procedimiento de acuerdo con cualquiera de las reivindicaciones anteriores, en el que el dispositivo electrónico quiere acceder a la red a través de un determinado puerto y que además comprende:

si en la etapa b) o c) se deniega el acceso al dispositivo electrónico, cerrar el puerto a través del que quiere acceder el dispositivo electrónico, y si, en las etapas b) y c) no se deniega el acceso al dispositivo electrónico y el puerto a través del que quiere acceder a la red el dispositivo electrónico está cerrado, abrir el puerto automáticamente.

14. Elemento de red para el acceso mejorado de un usuario (101) a una red de comunicaciones usando un dispositivo (102) electrónico, en el que el elemento de red realiza el control de acceso a la red en la capa 2 del modelo OSI y es un enrutador o conmutador que gestiona el acceso a la red de comunicaciones y en el que el elemento de red comprende:

- una base de datos que comprende:

  - una tabla de identificadores de dispositivos electrónicos con acceso (108) denegado a la red y una tabla de identificadores de usuarios con acceso (107) denegado a la red, una tabla de identificadores de usuarios autorizados que incluye la contraseña vinculada a cada usuario (204), una tabla de identificadores de

aquellos dispositivos electrónicos que tienen acceso autorizado a la red (104), una tabla de identificadores de usuario que están vinculados a cada identificador de dispositivo electrónico con acceso (310) autorizado a la red y una tabla con el conjunto de parámetros de configuración de red disponibles para cada identificador de dispositivo electrónico con acceso autorizado a la red, en el que el conjunto de parámetros de configuración de red disponibles comprende un rango de direcciones de red disponibles para cada perfil;

- medios para recibir del dispositivo electrónico una solicitud de acceso a la red, un identificador del dispositivo electrónico, un identificador de usuario y una contraseña para dicho usuario mediante uno o más mensajes de capa 2 del modelo OSI;
- medios para recibir del dispositivo electrónico un mensaje de capa 2 del modelo OSI, solicitando parámetros de configuración de red para acceder a la red;
- un procesador configurado para:

  - comprobar si dicho identificador del dispositivo electrónico se encuentra en la tabla de dispositivos electrónicos con acceso (108) denegado a la red y si es así, denegar el acceso a la red a dicho dispositivo electrónico;
  - comprobar si el identificador del dispositivo electrónico está registrado en la tabla de identificadores de aquellos dispositivos electrónicos (104) que tienen acceso autorizado a la red, si la comprobación es negativa, denegar el acceso a la red y almacenar la identificación del dispositivo electrónico en la tabla de dispositivos electrónicos con acceso (108) denegado a la red;
  - comprobar si dicho identificador de usuario se encuentra en la tabla de usuarios con acceso (107) denegado a la red y si es así, denegar el acceso a la red a dicho usuario;
  - autenticar al usuario, realizando al menos las siguientes comprobaciones:

    - comprobar que el identificador de usuario aparece en la tabla de usuarios (204) autorizados y la contraseña recibida corresponde a la vinculada a dicho usuario en dicha tabla;

  - comprobar que el identificador del dispositivo electrónico aparece en la base de datos como vinculado a dicho usuario;
  - si alguna de las comprobaciones de autenticación es negativa, almacenar la identificación del usuario en la tabla de usuarios con acceso denegado a la red y denegar el acceso a la red a dicho usuario;
  - al recibir del dispositivo electrónico el mensaje solicitando parámetros de configuración de red, comprobar si el identificador del dispositivo electrónico está registrado en la tabla de identificadores de aquellos dispositivos electrónicos que tienen acceso autorizado a la red, si la comprobación es negativa, almacenar la identificación del dispositivo electrónico en la tabla de dispositivos con acceso (108) denegado a la red y denegar el acceso a la red a dicho dispositivo electrónico, y si la comprobación es positiva, asignar un conjunto de parámetros de configuración de red al dispositivo electrónico dependiendo al menos del identificador del dispositivo electrónico;

- medios para enviar un mensaje de capa 2 al dispositivo electrónico con los parámetros de configuración de red asignados al dispositivo electrónico.

15. Medio de almacenamiento digital para almacenar un programa informático que comprende instrucciones ejecutables por ordenador que provocan que un ordenador que ejecute el programa implemente el procedimiento de acuerdo con cualquiera de las reivindicaciones 1-13.

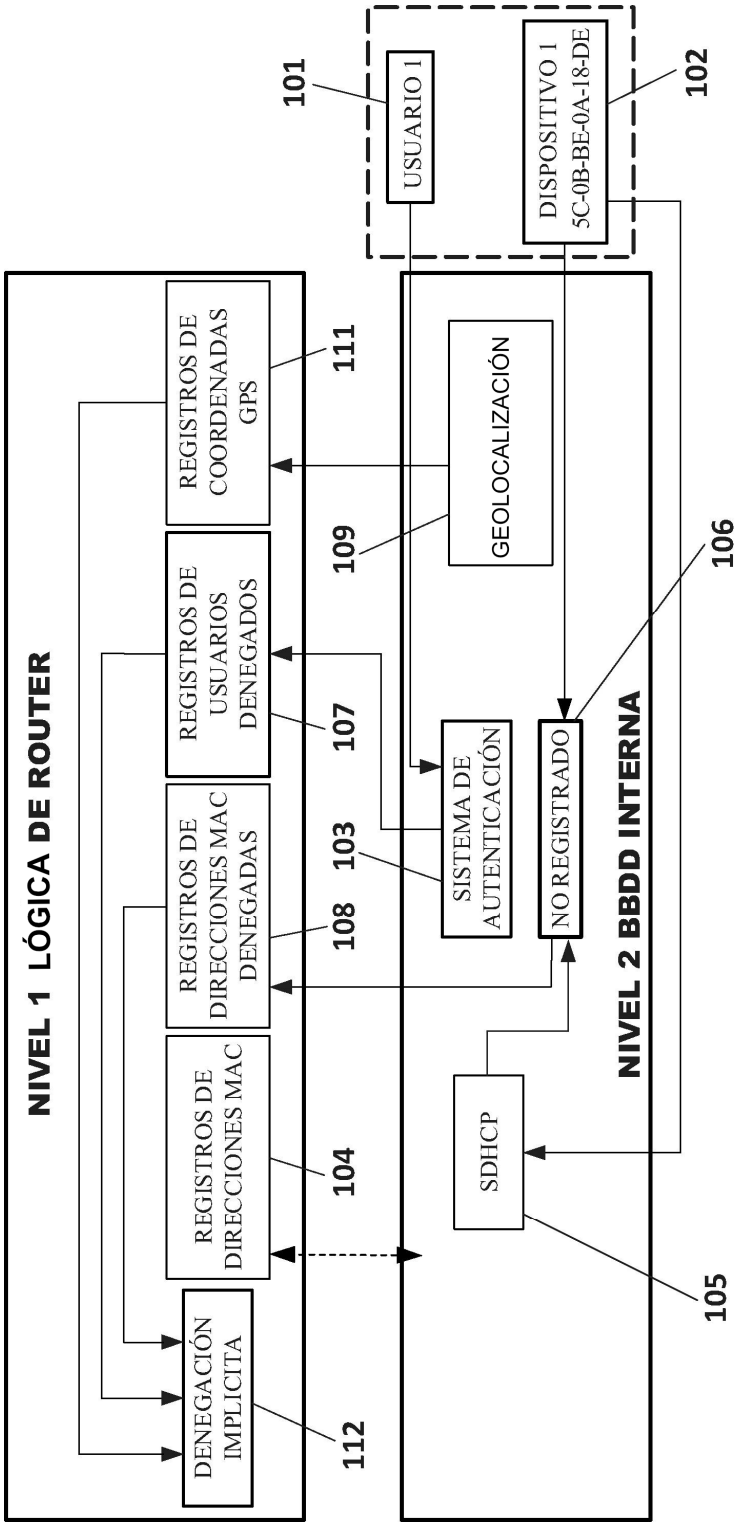
NIVEL 1 LÓGICA DE ROUTER
REGISTROS DE COORDENADAS GPS
REGISTROS DE USUARIOS DENEGADOS
REGISTROS DE DIRECCIONES MAC DENEGADAS
REGISTROS DE DIRECCIONES MAC
DENEGACIÓN IMPLICITA
NIVEL 2 BBDD INTERNA
GEOLOCALIZACIÓN
SISTEMA DE AUTENTICACIÓN
NO REGISTRADO
SDHCP
USUARIO 1
DISPOSITIVO 1
5C-0B-BE-0A-18-DE
101
102
103
104
105
106
107
108
109
111
112

FIG. 1

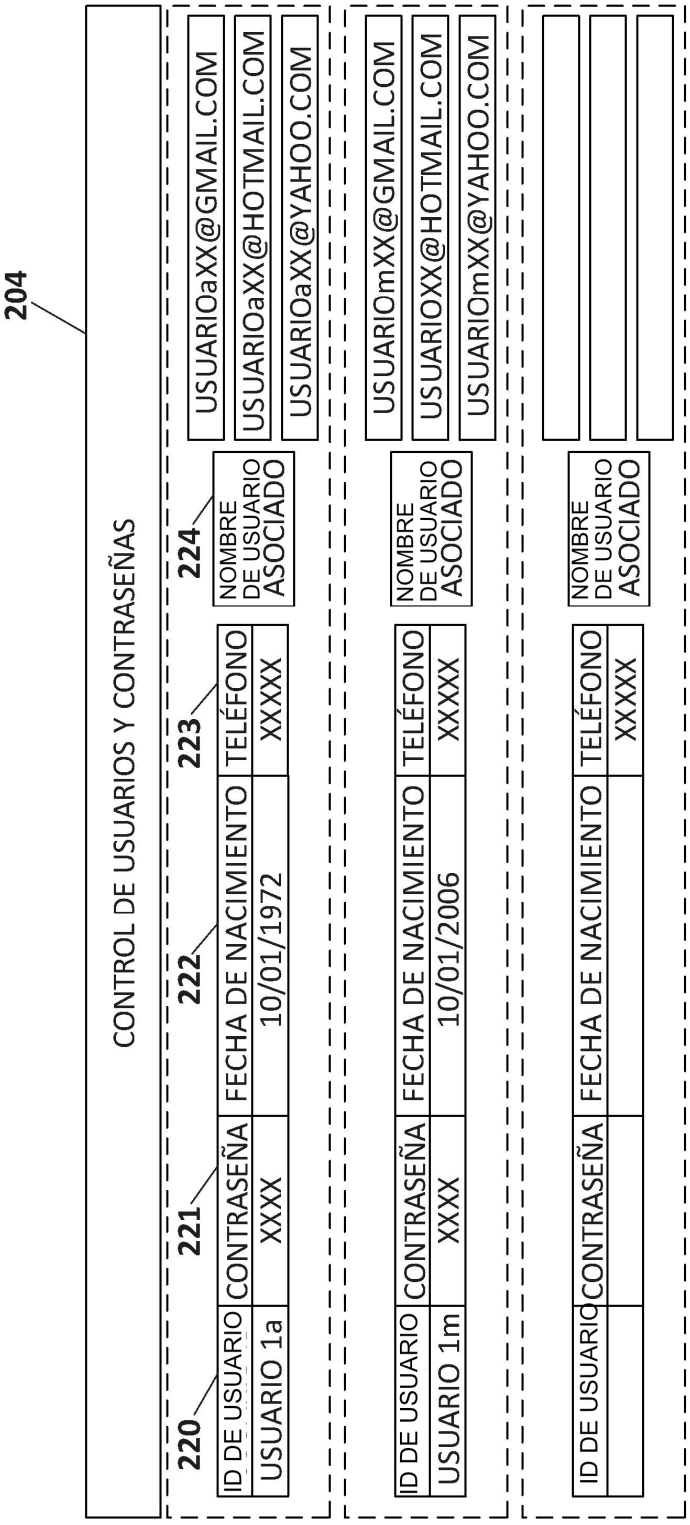
204
CONTROL DE USUARIOS Y CONTRASEÑAS
220
221
222
223
224
ID DE USUARIO
CONTRASEÑA
FECHA DE NACIMIENTO
TELÉFONO
NOMBRE DE USUARIO ASOCIADO
USUARIO 1a
XXXX
10/01/1972
XXXXX
USUARIOaXX@GMAIL.COM
USUARIOaXX@HOTMAIL.COM
USUARIOaXX@YAHOO.COM
USUARIO 1m
XXXX
10/01/2006
XXXXX
USUARIOmXX@GMAIL.COM
USUARIOXX@HOTMAIL.COM
USUARIOmXX@YAHOO.COM

FIG. 2

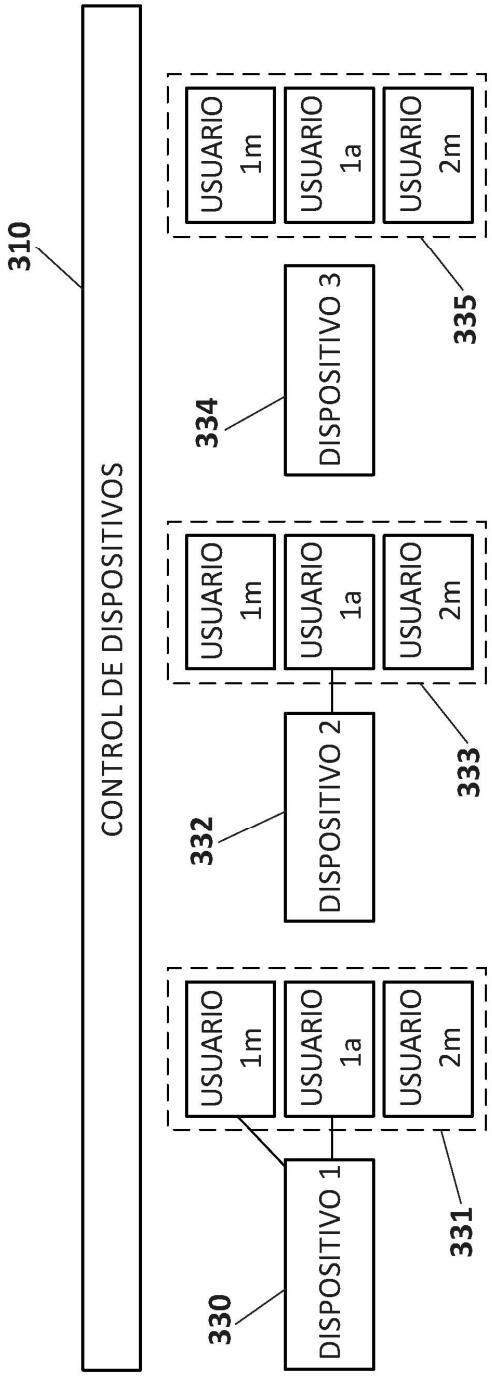
310
CONTROL DE DISPOSITIVOS
330
DISPOSITIVO 1
USUARIO 1m
USUARIO 1a
USUARIO 2m
331
332
DISPOSITIVO 2
USUARIO 1m
USUARIO 1a
USUARIO 2m
333
334
DISPOSITIVO 3
USUARIO 1m
USUARIO 1a
USUARIO 2m
335

FIG. 3

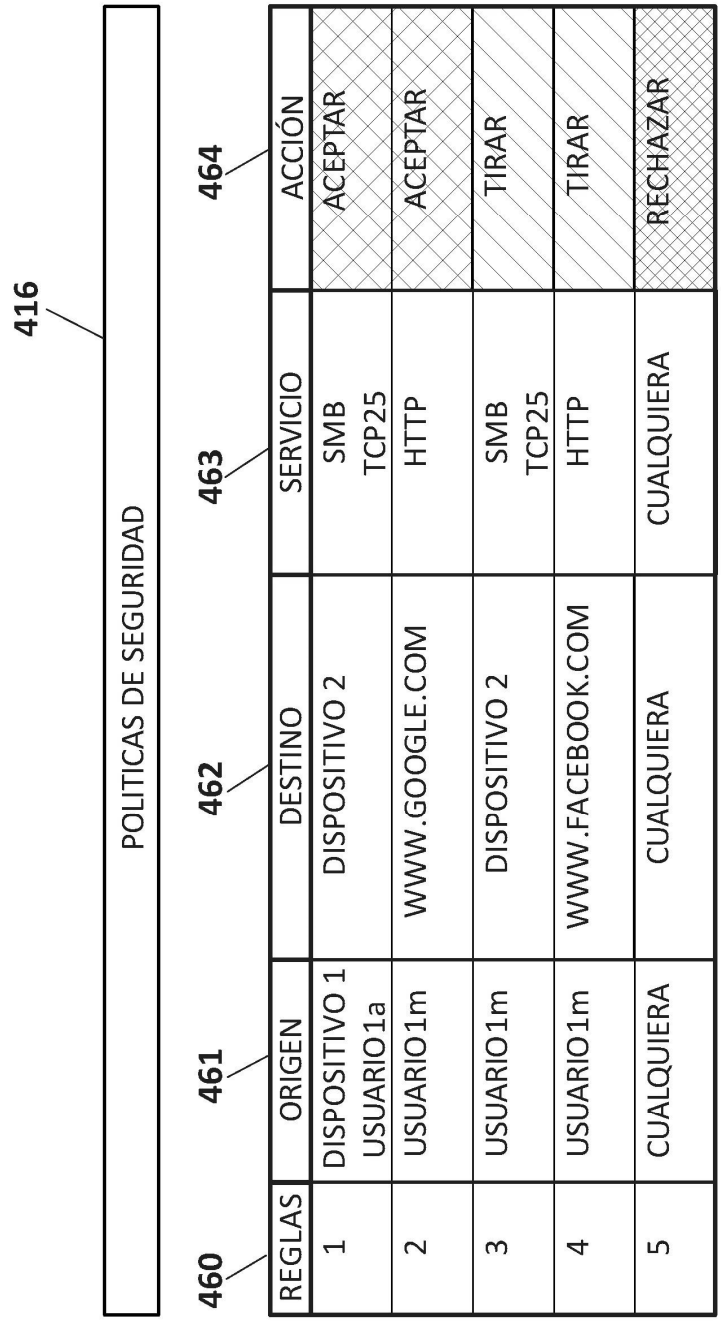
416
POLITICAS DE SEGURIDAD
460
461
462
463
464
REGLAS
ORIGEN
DESTINO
SERVICIO
ACCIÓN
1
DISPOSITIVO 1 USUARIO1a
DISPOSITIVO 2
SMB TCP25
ACEPTAR
2
USUARIO1m
WWW.GOOGLE.COM
HTTP
ACEPTAR
3
USUARIO1m
DISPOSITIVO 2
SMB TCP25
TIRAR
4
USUARIO1m
WWW.FACEBOOK.COM
HTTP
TIRAR
5
CUALQUIERA
CUALQUIERA
CUALQUIERA
RECHAZAR

FIG. 4

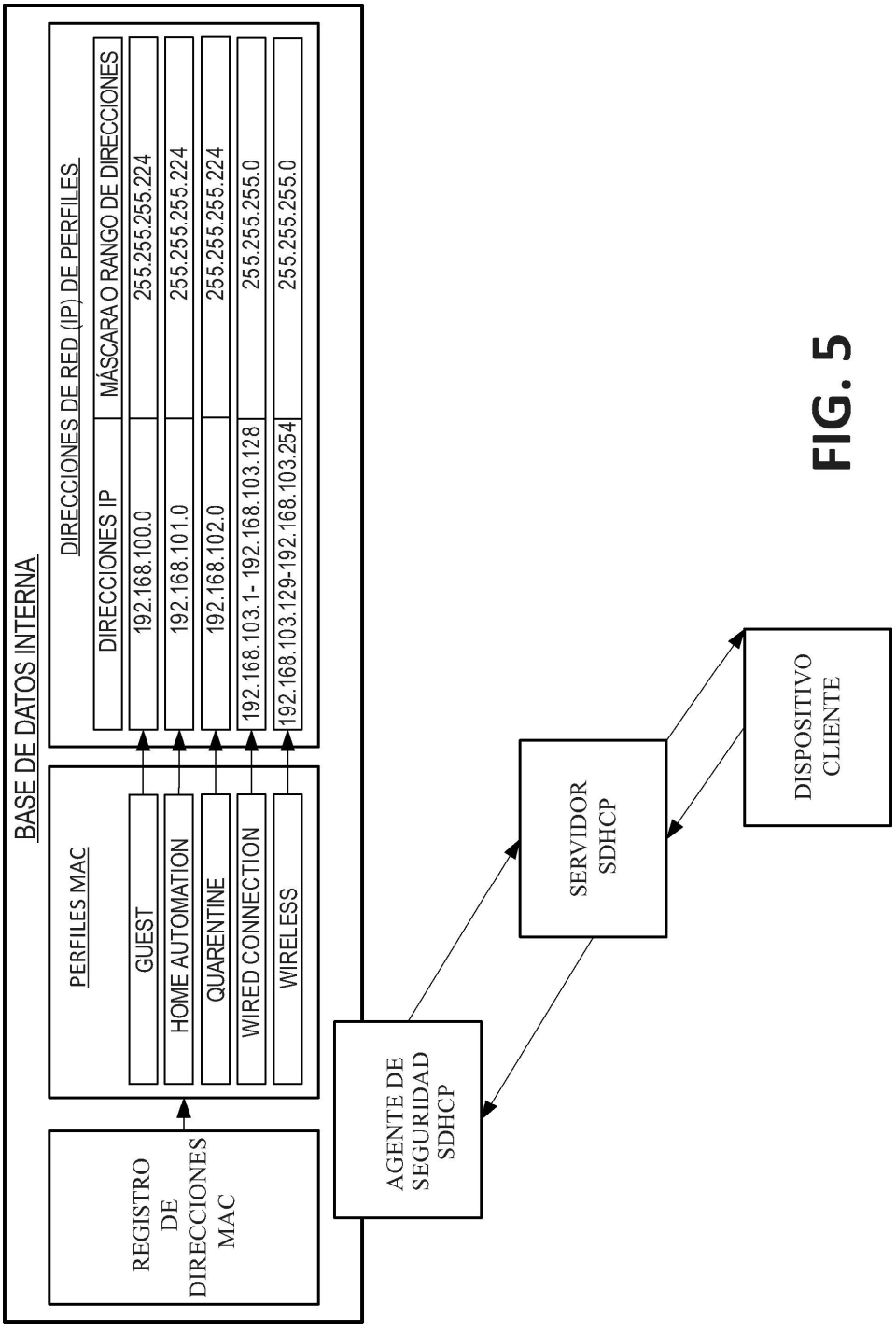
BASE DE DATOS INTERNA
DIRECCIONES DE RED (IP) DE PERFILES
DIRECCIONES IP
MÁSCARA O RANGO DE DIRECCIONES
192.168.100.0
255.255.255.224
192.168.101.0
255.255.255.224
192.168.102.0
255.255.255.224
192.168.103.1- 192.168.103.128
255.255.255.0
192.168.103.129-192.168.103.254
255.255.255.0
PERFILES MAC
GUEST
HOME AUTOMATION
QUARENTINE
WIRED CONNECTION
WIRELESS
REGISTRO DE DIRECCIONES MAC
AGENTE DE SEGURIDAD SDHCP
SERVIDOR SDHCP
DISPOSITIVO CLIENTE

FIG. 5

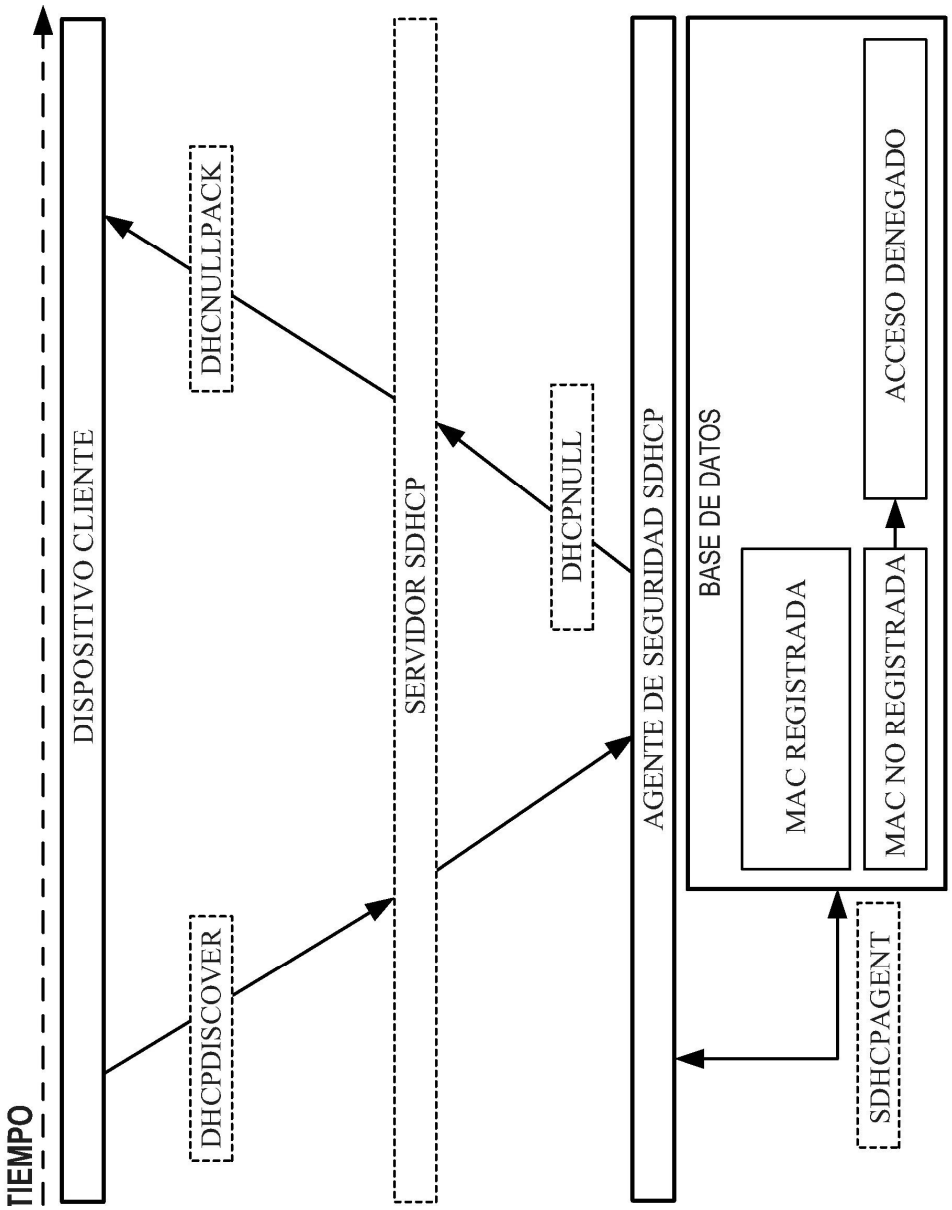
TIEMPO
DISPOSITIVO CLIENTE
DHCPDISCOVER
DHCNULLPACK
SERVIDOR SDHCP
DHCPNULL
AGENTE DE SEGURIDAD SDHCP
BASE DE DATOS
MAC REGISTRADA
MAC NO REGISTRADA
ACCESO DENEGADO
SDHCPAGENT

FIG. 6

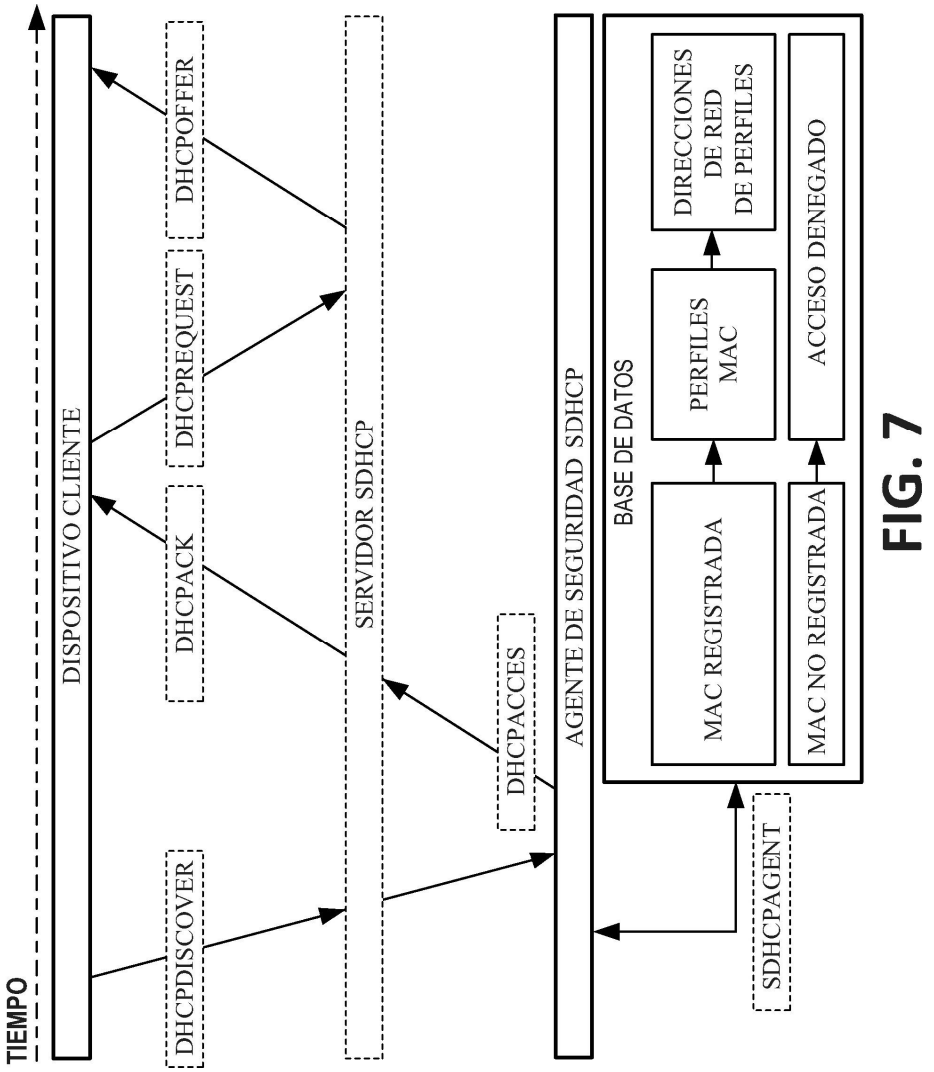
TIEMPO
DISPOSITIVO CLIENTE
DHCPDISCOVER
DHCPOFFER
DHCPREQUEST
DHCPACK
SERVIDOR SDHCP
DHCPACCES
AGENTE DE SEGURIDAD SDHCP
SDHCPAGENT
BASE DE DATOS
MAC REGISTRADA
MAC NO REGISTRADA
PERFILES MAC
DIRECCIONES DE RED DE PERFILES
ACCESO DENEGADO

FIG. 7

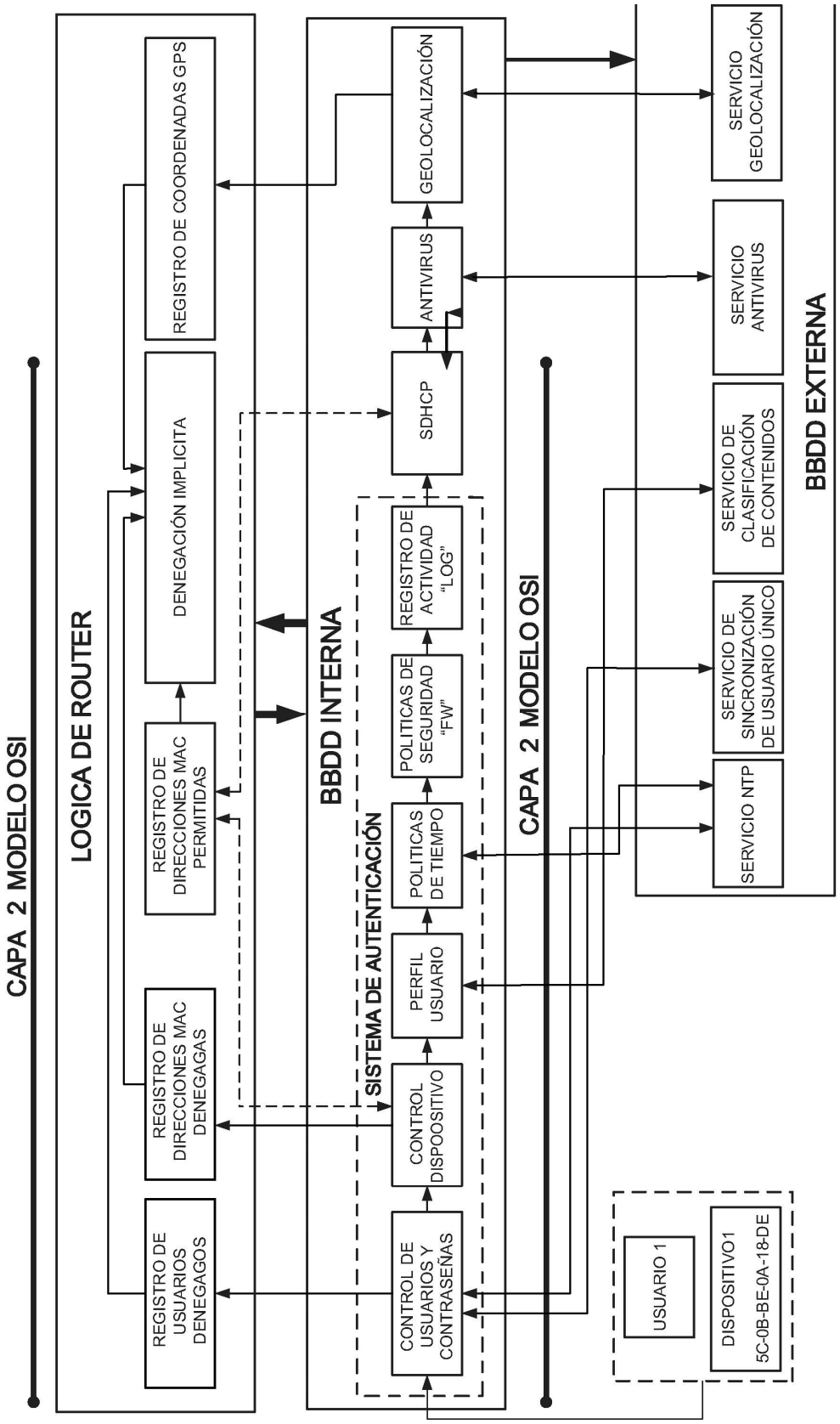
CAPA 2 MODELO OSI
LOGICA DE ROUTER
REGISTRO DE USUARIOS DENEGAGOS
REGISTRO DE DIRECCIONES MAC DENEGAGAS
REGISTRO DE DIRECCIONES MAC PERMITIDAS
DENEGACIÓN IMPLICITA
REGISTRO DE COORDENADAS GPS
BBDD INTERNA
SISTEMA DE AUTENTICACIÓN
CONTROL DE USUARIOS Y CONTRASEÑAS
CONTROL DISPOOSITIVO
PERFIL USUARIO
POLITICAS DE TIEMPO
POLITICAS DE SEGURIDAD "FW"
REGISTRO DE ACTIVIDAD "LOG"
SDHCP
ANTIVIRUS
GEOLOCALIZACIÓN
CAPA 2 MODELO OSI
USUARIO 1
DISPOSITIVO1
5C-0B-BE-0A-18-DE
SERVICIO NTP
SERVICIO DE SINCRONIZACIÓN DE USUARIO ÚNICO
SERVICIO DE CLASIFICACIÓN DE CONTENIDOS
SERVICIO ANTIVIRUS
SERVICIO GEOLOCALIZACIÓN
BBDD EXTERNA

FIG. 8