(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 556 252**

(21) Número de solicitud: 201431060

(51) Int. CI.:

G06F 21/00 (2013.01)

(12) PATENTE DE INVENCIÓN B1

(22) Fecha de presentación:

14.07.2014

(43) Fecha de publicación de la solicitud:

14.01.2016

Fecha de modificación de las reivindicaciones:

27.04.2016

Fecha de la concesión:

20.12.2016

(45) Fecha de publicación de la concesión:

28.12.2016

(73) Titular/es:

NIETO FOMBELLA, Gabriel (100.0%)
Estrella Polar 18
41870 Bormujos (Sevilla) ES

(72) Inventor/es:

NIETO FOMBELLA, Gabriel

(74) Agente/Representante:

AGUDO HILL, Carlos

(54) Título: **Método de un cortafuegos con reglas dinámicas mediante SQL**

(57) Resumen:
Método de un cortafuegos con reglas dinámicas mediante SQL, constituido a partir de un dispositivo cortafuegos localizado entre dos redes: a un lado los usuarios y al otro los equipos o redes a proteger, disponiendo de conectividad a un servidor donde se encuentra alojada la base de datos de inventario de equipos, siendo en este servidor de base de datos relacional donde mediante tablas indexadas y relacionas por datos comunes se obtiene el conjunto de direcciones IP, gracias a un lenguaje estructurado de consultas conocido como SQL, asociando una o varias sentencias SQL al perfil de un usuario y ejecutando estas órdenes cuando el usuario inicie sesión en el cortafuegos, obteniéndose y volcando sobre un fichero el resultado con el conjunto de direcciones IP o redes IP, a las cuales, a ese usuario en concreto, se le permite o deniega el acceso mediante la aplicación de las reglas de filtrado.

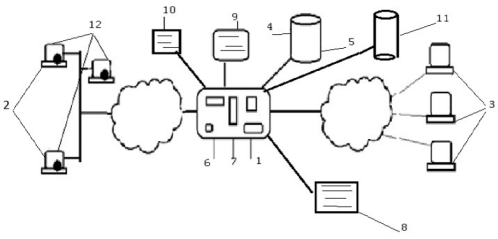

Fig.1

ES 2 556 252 B1

DESCRIPCIÓN

METODO DE UN CORTAFUEGOS CON REGLAS DINAMICAS MEDIANTE SQL

El método cortafuegos con reglas dinámicas mediante SQL, lenguaje estructurado de consulta, de la presente invención se refiere a un servidor de seguridad de red informática para usuarios remotos o internos, con capacidades de cortafuegos de tráfico IP de nivel 1,2 y 3 del modelo TCP/IP, protocolo de control de transmisión y protocolo de Internet, que se integra como complemento de seguridad y permite o bloquea a un usuario o host, computadora conectada a una red, el acceso a otros equipos o redes, basándose en la identidad del usuario y en consultar en un servidor de bases de datos relacional, los equipos permitido.. Para ello el método asocia a cada usuario dado de alta en el cortafuegos unos comandos SQL, con los cuales se extrae en tiempo real un conjunto de direcciones IP de host o direcciones IP de red. Con este conjunto, más la dirección IP del usuario o su Socket, identificador de conexión entre el usuario y el cortafuegos, se crean las reglas de dinámicas de acceso que filtrarán el tráfico IP. Esta invención soluciona el problema, dotando a un servidor de seguridad de red, la flexibilidad y potencia del lenguaje SQL.

Un cortafuegos de red en Informática o Firewall es un sistema o grupo de sistemas que impone una política de seguridad entre unos usuarios y la red de una la organización y determina cual de los servicios o equipos de red pueden ser usados dentro de ésta, es decir un

empleado puede o no puede utilizar dentro de su organización ciertos recursos o poseer acceso a cierta información. Para que un cortafuegos sea efectivo, todo el tráfico debe de pasar a través de éste donde se selecciona el sitio al que puede o no acceder. Siendo éste mismo inmune a la penetración. Actualmente se conocen los cortafuegos aplicados a redes que utilizan reglas que interceptan o no la entrada de usuarios o hosts a zonas o equipos dentro de una misma red. El lenguaje de alto nivel SQL es el estándar para el manejo de bases de datos relacionales y consigue mediante operadores sencillos como SELECT, WHERE, FROM, WHERE, GROUP BY, ORDER BY, extraer o modificar grupos de registros.

Cuando en una empresa u organización el número de equipos a proteger supera un cierto valor o cambian su número frecuentemente, es complicado para los administradores de esa red aplicar políticas y reglas para que a unos empleados se les permita conectividad a ciertos equipos o servicios y a otros no. Si queremos agrupar los equipos por tener alguna característica común que se desea que un usuario haga uso, como todos los equipos de un departamento, o de tipo impresora o de la primera planta de un edificio, se acaba teniendo dos tipos de perfiles: los usuarios que se pueden conectar a todos los equipos y los que no. Con los consiguientes problemas de seguridad. Este tipo de agrupaciones se consiguen fácilmente mediante el lenguaje de consulta SQL aplicado a

una base de datos de inventario, donde cada equipo tiene asignadas unas características y una dirección de red conocida como IP.

Se encuadra en la industria de la informática y, dentro de ésta, en la de los cortafuegos.

ANTECEDENTES DE LA INVENCION

El documento WO03040923 describe un sistema de seguridad que se aplica a una base de datos que se estructura dentro del sistema y no en el servidor de red. El documento US2011231926 propone un aparato conectado a una red interior y/o exterior con objeto de que la barrera que se impone impida la conexión de un usuario de internet a la red interior. El documento ES2292737 describe una comunicación inalámbrica para producir una clave de acceso del usuario a la red configurando una biométrica de entrada que un procesador compara con el certificado de firma guardado en la memoria dejando acceder al usuario si coinciden ambos datos.

Esto que se conoce presenta los inconvenientes que a continuación se indican:

- Los cortafuegos convencionales están orientados a proteger a una red de otras redes o a proteger un pequeño grupo de equipos de otros equipos, pero no pueden proteger a un conjunto numeroso de equipos de ataques internos o usuarios negligentes por la imposibilidad de mantener largas listas de acceso aplicando reglas individuales.

– No solucionan el problema de actualizar las reglas de acceso cada vez que se incluyen nuevos equipos en el perfil de los usuarios y se dan de baja otros.

- El documento WO03040923 se ocupa de proteger información almacenada dentro de una base de datos relacional pero no impide la conectividad IP a equipos en una red informática.

- El documento US2011231926 posee la desventaja de que solo protege al ordenador donde está instalado y no a los equipos y redes de una organización.

-El documento ES2292737 tiene el inconveniente que se limita a proteger el punto de acceso a la red y no los equipos individuales de esa red .

Frente a estos inconvenientes la invención propuesta presenta las siguientes ventajas:

- El método cortafuegos no depende de conocer previamente las direcciones IP que pueda tener el equipo ordenador del usuario pues estas direcciones IP las extrae automáticamente en la sesión obligatoria de autorización que el usuario tiene que establecer con el cortafuego.

- No necesita conocer los equipos a proteger previamente, con el consiguiente problema si su número cambiase, pues estos equipos los obtiene automáticamente y en tiempo real en la sesión obligatoria de autorización, al ejecutar la consulta que el usuario tiene asignada en su perfil, sobre la base de datos de inventario.

- Es una protección orientada a usuarios con la ventaja de tener reglas personalizadas por usuario o por grupos de usuarios.

- Al conectar con bases de datos relacionales, la sentencias de consulta que un administrador debe crear en el perfil de un usuario son muy sencillas y flexibles.

-Se pueden crear perfiles con el mismo patrón de búsqueda.

- Permite la movilidad de los usuarios, pues al validar al usuario valida las direcciones IP de su dispositivo de conexión.

-Ahorra trabajo de administración pues no se necesita cambiar las reglas cuando cambia el inventario de equipos.

-Se puede asignar a un usuario una regla que le permite conectar con millones de equipos con una simple consulta SQL.

-Al usar SQL es compatible y adaptable a la mayoría de bases de datos relaciones existentes en el mercado.

-Es seguro pues la conexión desde los cortafuegos a la base de datos, solo necesita permisos de lectura.

- Permite una gran separación de tareas a los administradores al separar el inventario, propio de residir en un servidor de base de datos, de las reglas de tráfico, más acorde con un cortafuegos.

- Permite proteger equipos que no soportan RADIUS, protocolo de autentificación y autorización para aplicaciones de acceso a la red. Y es una primera línea de defensa para los que sí lo soportan, puesto que se interpone entre estos equipos finales y los usuarios,

evitando la conectividad IP directa entre ellos si no está autorizado por el servidor de seguridad de red.

Así la presente invención se constituye a partir de un cortafuego localizados entre dos redes o segmentos de red, localizándose de la siguiente forma: a un lado los usuarios de una organización y al otro los equipos o redes a proteger, disponiendo de conectividad a un servidor donde se encuentra alojada la base de datos de inventario de equipos pudiendo ser este servidor el propio cortafuegos siendo en este servidor de base de datos donde mediante tablas indexadas y relacionas entre sí por datos comunes, una empresa u organización administra sus equipos informáticos, registra altas, bajas, modificaciones, y los clasifica según su criterio, como localización geográfica, situación, si está en avería o no, grupo o usuario que tiene acceso a él, contrato en vigor, tipo. y por supuesto la red o dirección IP de estos equipos, dato, éste último ,imprescindible para obtener el conjunto de direcciones IP o redes gracias a un lenguaje estructurado de consultas conocido como SQL que debe soportar este servidor de base de datos y un interfaz ,o programa cliente de ejecución de estas instrucciones, que se aloja en el cortafuegos asociando una o varias sentencias SQL al perfil de un usuario y ejecutando estas órdenes cuando el usuario inicie sesión en el cortafuegos, obteniéndose y volcando sobre un fichero el resultado con el conjunto de direcciones IP o redes IP, a las cuales, a ese usuario en

concreto, se le permite o deniega el acceso mediante la aplicación de las reglas de filtrado.

El funcionamiento del método consta de las siguientes etapas; en una primera etapa, el usuario, con un proceso llamado login, se conecta al cortafuego mediante una sesión SSH, intérprete de comandos y protocolo seguro de acceso a máquinas remotas. En una segunda etapa, el cortafuegos valida al usuario con una clave local o consulta la clave en otros servidores externos como es un LDPA corporativo, protocolo ligero de acceso a directorios. En la tercera etapa y si el proceso de login es correcto, el cortafuegos obtiene la dirección IP del host del usuario, su Socket. En una cuarta etapa se obtiene las sentencias SQL del perfil del usuario, ejecuta las ordenes SQL contra la base de datos de inventario, almacena la respuesta del conjunto de direcciones IP en un fichero persona. En una quinta etapa aplica las reglas extraídas del perfil del usuario sobre estos dos extremos: Las direcciones IP del usuario o su Socket y el fichero de direcciones IP o redes IP. En la sexta etapa el cortafuego informa al usuario que ya puede cursar tráfico hacia las direcciones IP permitidas. El usuario en ese momento puede trabajar normalmente como si no existiese el cortafuego y establecer otras sesiones independientes con los equipos permitidos.

Cuando el usuario cierra la sesión SSH con el cortafuego todas las reglas personalizadas sobre sus direcciones IP o sobre su Socket desaparecen.

En una realización diferente los ficheros de comandos SQL y los ficheros de reglas personalizadas ubicados en el cortafuegos, se extraen igualmente mediante SQL, de la base de datos de inventario.

En otra realización distinta es factible que el dispositivo sea virtualizado dentro de otro servidor.

En otra realización distinta es factible que la sesión obligatoria de login se use otro programa distinto a SSH como HTTPS, protocolo seguro de transferencia de hipertexto.

Para una mejor comprensión de cuanto se expresa en esta memoria descriptiva se acompaña a continuación un dibujo que a modo de ejemplo no limitativo representa un modo de realización preferida y su funcionamiento

Figura 1.- Esquema del funcionamiento del método

1) Cortafuegos
2) Usuarios
3) Equipos o redes
4) Servidor de base de datos de inventario
5) Tablas indexadas
6) Conjunto de direcciones IP
7) Interfaz
8) Sentencias SQL
9) Fichero
10) Reglas de filtrado

11)Protocolo ligero de acceso a directorios.

12)Host del usuario

DESCRIPCION DE UNA REALIZACION PREFERIDA

Así la presente invención se constituye a partir de un cortafuego (1) localizado entre dos redes o segmentos de red, localizándose de la siguiente forma: a un lado los usuarios (2) de una organización y al otro los equipos o redes a proteger (3), disponiendo de conectividad a un servidor (4) donde se encuentra alojada la base de datos de inventario de equipos pudiendo ser este servidor (4) el propio cortafuegos (1) siendo en este servidor (4) de base de datos donde mediante tablas indexadas (5) y relacionas entre sí por datos comunes, una empresa u organización administra sus equipos informáticos, registra altas, bajas, modificaciones, y los clasifica según su criterio, como localización geográfica, situación, si está en avería o no, grupo o usuario que tiene acceso a él, contrato en vigor, tipo. y por supuesto la red o dirección IP (12) de estos equipos, dato, éste último ,imprescindible para obtener el conjunto de direcciones IP o redes (6) gracias a un lenguaje estructurado de consultas conocido como SQL que debe soportar este servidor (4) de base de datos y un interfaz (7) ,o programa cliente de ejecución de estas instrucciones, que se aloja en el cortafuegos asociando una o varias sentencias SQL (8) al perfil de un usuario (8) y ejecutando estas órdenes cuando el usuario (2) inicie sesión en el cortafuegos (1), obteniéndose y volcando sobre un

fichero (9) el resultado con el conjunto de direcciones IP o redes IP (6), a las cuales, a ese usuario en concreto, se le permite o deniega el acceso mediante la aplicación de las reglas de filtrado (10).

El funcionamiento del método consta de las siguientes etapas; en una primera etapa, el usuario (2), con un proceso llamado login, se conecta al cortafuego (1) mediante una sesión SSH, intérprete de comandos y protocolo seguro de acceso a máquinas remotas. En una segunda etapa, el cortafuegos valida al usuario con una clave local o consulta la clave en otros servidores externos como es un LDPA (11) corporativo, protocolo ligero de acceso a directorios. En la tercera etapa y si el proceso de login es correcto, el cortafuegos obtiene la dirección IP del host (12) del usuario, su Socket. En una cuarta etapa se obtiene las sentencias SQL (8) del perfil del usuario, ejecuta las ordenes SQL contra la base de datos de inventario, almacena la respuesta del conjunto de direcciones IP en un fichero (9) personal. En una quinta etapa aplica las reglas extraídas del perfil del usuario (8) sobre estos dos extremos: las direcciones IP del usuario o su Socket y el fichero de direcciones IP o redes IP (6). En la sexta etapa el cortafuego informa al usuario que ya puede cursar tráfico hacia las direcciones IP permitidas. El usuario en ese momento puede trabajar normalmente como si no existiese el cortafuego y establecer otras sesiones independientes con los equipos permitidos (6).

Cuando el usuario cierra la sesión SSH con el cortafuego (1) todas las reglas personalizadas sobre sus direcciones IP o sobre su Socket (12) desaparecen.

REIVINDICACIONES

1. Método de un cortafuegos con reglas dinámicas mediante SQL constituido a partir de un cortafuego de trafico IP de los niveles 2 y 3 del modelo TCP/IP (1) localizado entre dos redes o segmentos de red, focalizándose de la siguiente forma: a un lado los usuarios (2) de una organización y al otro los equipos o redes a proteger (3), disponiendo de conectividad a un servidor (4) donde se encuentra alojada la base de datos de inventario de equipos pudiendo ser este servidor (4) el propio cortafuegos (1) siendo en este servidor (4) de base de datos donde mediante tablas indexadas (5) y relacionas entre sí por datos comunes, una empresa u organización administra sus equipos informáticos, registra altas, bajas, modificaciones, y los clasifica según su criterio, como localización geográfica, situación, si está en avería o no, grupo o usuario que tiene acceso a él, contrato en vigor, tipo. y por supuesto la red o dirección IP (12) de estos equipos, dato, éste último ,imprescindible para obtener el conjunto de direcciones IP o redes (6) gracias a un lenguaje estructurado de consultas conocido como SQL que debe soportar este servidor (4) de base de datos y un interfaz (7) ,o programa cliente de ejecución de estas instrucciones, que se aloja en el cortafuegos asociando una o varias sentencias SQL (8) al perfil de un usuario (8) y ejecutando estas órdenes cuando el usuario (2) inicie sesión en el cortafuegos (1), obteniéndose y volcando sobre un fichero (9) el resultado con el conjunto de direcciones IP o redes IP (6), a las cuales, a

ese usuario en concreto, se le permite o deniega el acceso mediante la aplicación de las reglas de filtrado (10).

El funcionamiento del método consta de las siguientes etapas; en una primera etapa, el usuario (2), con un proceso llamado login, se conecta al cortafuego (1) mediante una sesión SSH, intérprete de comandos y protocolo seguro de acceso a máquinas remotas. En una segunda etapa, el cortafuegos valida al usuario con una clave local o consulta la clave en otros servidores externos como es un LDPA (11) corporativo, protocolo ligero de acceso a directorios. En la tercera etapa y si el proceso de login es correcto, el cortafuegos obtiene la dirección IP del host (12) del usuario, su Socket. En una cuarta etapa se obtiene las sentencias SQL (8) del perfil del usuario, ejecuta las ordenes SQL contra la base de datos de inventario, almacena la respuesta del conjunto de direcciones IP en un fichero (9) personal. En una quinta etapa aplica las reglas extraídas del perfil del usuario (8) sobre estos dos extremos: las direcciones IP del usuario o su Socket y el fichero de direcciones IP o redes IP (6). En la sexta etapa el cortafuego informa al usuario que ya puede cursar tráfico hacia las direcciones IP permitidas. El usuario en ese momento puede trabajar normalmente como si no existiese el cortafuego y establecer otras sesiones independientes con los equipos permitidos (6).

2.- Método de un cortafuegos con reglas dinámicas mediante SQL, según reivindicación 1, caracterizado porque cuando el usuario cierra la

sesión SSH con el cortafuego (1) todas las reglas personalizadas sobre sus direcciones IP o sobre su Socket (12) desaparecen.

3.- Método de un cortafuegos con reglas dinámicas mediante SQL, según reivindicación 1, caracterizado porque los ficheros de comandos SQL y los ficheros de reglas personalizadas ubicados en el cortafuegos, se extraen igualmente mediante SQL, de la base de datos de inventario.

4.- Método de un cortafuegos con reglas dinámicas mediante SQL, según reivindicación 1, caracterizado porque el dispositivo se virtualiza dentro de otro servidor.

5.- Método de un cortafuegos con reglas dinámicas mediante SQL, según reivindicación 1, caracterizado porque en la sesión obligatoria de login se usa otro programa distinto a SSH como HTTPS, protocolo seguro de transferencia de hipertexto.

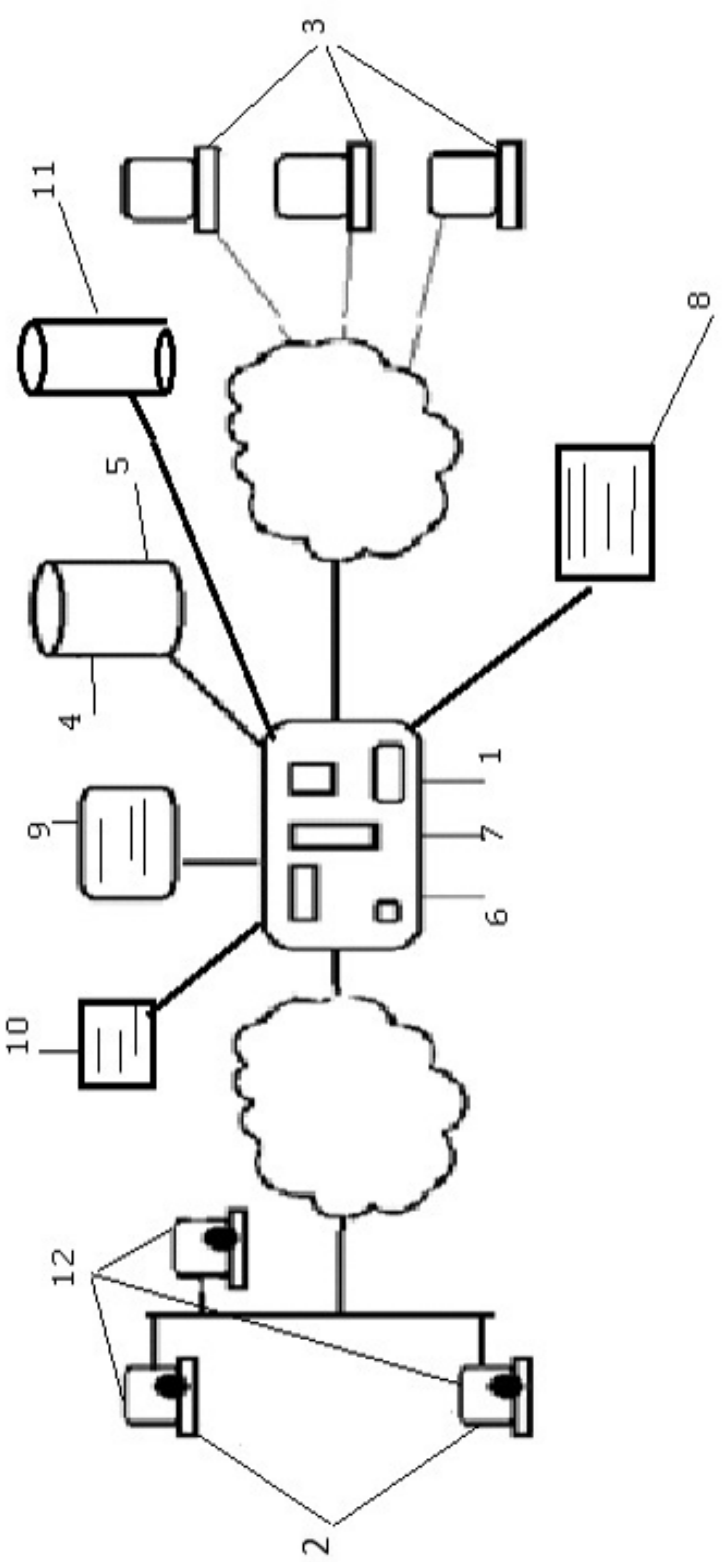

Fig.1

OFICINA ESPAÑOLA
DE PATENTES Y MARCAS

ESPAÑA

(21) N.º solicitud: 201431060

(22) Fecha de presentación de la solicitud: 14.07.2014

(32) Fecha de prioridad:

INFORME SOBRE EL ESTADO DE LA TECNICA

(51) **Int. Cl. :** ***G06F21/00*** (2013.01)

DOCUMENTOS RELEVANTES

Categoría	(56) **Documentos citados**	**Reivindicaciones afectadas**
X	US 2007245409 A1 (HARRIS JAMES et al.) 18.10.2007, párrafos 4-6,152-153,183-199,508-509,536; figuras 4A-E.	1-5
A	US 2011277027 A1 (HAYTON RICHARD et al.) 10.11.2011, todo el documento.	1
A	WO 02052767 A2 (OBLIX INC) 04.07.2002, todo el documento.	1

Categoría de los documentos citados

X: de particular relevancia
Y: de particular relevancia combinado con otro/s de la misma categoría
A: refleja el estado de la técnica
O: referido a divulgación no escrita
P: publicado entre la fecha de prioridad y la de presentación de la solicitud
E: documento anterior, pero publicado después de la fecha de presentación de la solicitud

El presente informe ha sido realizado

☒ para todas las reivindicaciones ☐ para las reivindicaciones nº:

Fecha de realización del informe	**Examinador**	**Página**
04.05.2015	M. Muñoz Sánchez	1/4

Documentación mínima buscada (sistema de clasificación seguido de los símbolos de clasificación)

G06F

Bases de datos electrónicas consultadas durante la búsqueda (nombre de la base de datos y, si es posible, términos de búsqueda utilizados)

INVENES, EPODOC, WPI

Fecha de Realización de la Opinión Escrita: 04.05.2015

Declaración

Novedad (Art. 6.1 LP 11/1986)	Reivindicaciones	1-5	**SI**
	Reivindicaciones		**NO**
Actividad inventiva (Art. 8.1 LP11/1986)	Reivindicaciones		**SI**
	Reivindicaciones	1-5	**NO**

Se considera que la solicitud cumple con el requisito de aplicación industrial. Este requisito fue evaluado durante la fase de examen formal y técnico de la solicitud (Artículo 31.2 Ley 11/1986).

Base de la Opinión.-

La presente opinión se ha realizado sobre la base de la solicitud de patente tal y como se publica.

1. Documentos considerados.-

A continuación se relacionan los documentos pertenecientes al estado de la técnica tomados en consideración para la realización de esta opinión.

Documento	Número Publicación o Identificación	Fecha Publicación
D01	US 2007245409 A1 (HARRIS JAMES et al.)	18.10.2007
D02	US 2011277027 A1 (HAYTON RICHARD et al.)	10.11.2011
D03	WO 02052767 A2 (OBLIX INC)	04.07.2002

2. Declaración motivada según los artículos 29.6 y 29.7 del Reglamento de ejecución de la Ley 11/1986, de 20 de marzo, de Patentes sobre la novedad y la actividad inventiva; citas y explicaciones en apoyo de esta declaración

Se considera D01 el documento más próximo del estado de la técnica al objeto de la solicitud.

Reivindicaciones independientes

Reivindicación 1: El documento D01 plantea un sistema de control de acceso con diferentes niveles de acceso y seguridad a documentos y/o aplicaciones empresariales (pár. 4). El sistema utiliza la tecnología SSL VPN para la conexión del usuario y el control de sus acciones sobre el recurso basándose en el nivel de acceso identificado (pár. 6).
Un agente recolector de datos (collection agent) transmitido a la máquina local recopila las credenciales de la máquina local, por ejemplo, nombre de usuario y contraseña (pár. 152). Las credenciales pueden estar asociadas con la máquina local o un usuario, (pár. 153).
En una realización concreta la máquina local 10 transmite una solicitud 410 al motor de políticas para acceder a una aplicación, el agente recolector 404 se comunica con la máquina local para obtener información de ella y se la envía al motor de políticas 406. El motor de políticas aplica una decisión basando en la base de datos de políticas 408 y la información recibida 412, (pár. 183). El motor de políticas puede ser una máquina remota (pár. 184).
En una realización el motor de políticas, tiene varios componentes el primero formado por una base de datos de condiciones 422 y un agente de inicio de sesión 424, y el segundo formado por una base de datos de políticas 432. El primer componente aplica una condición de la base de datos de condiciones a la información recibida sobre la máquina local 10. (pár. 193). Una de las condiciones posibles es que la máquina local establezca un cierto tipo de conexión de red. (pár. 194).
En una realización el agente de inicio de sesión 424 ejecuta el agente de recolección 404.En otra realización el primer componente puede comprender una pluralidad de agentes de inicio de sesión, uno por cada dominio de red; (pár. 198). Las bases de datos de condiciones y de políticas pueden ser SQL (pár. 199).
El documento D01 detalla también el filtrado de una solicitud a un servidor web, interceptado por un proceso en ejecución en un servidor proxy. La solicitud se examina según unas reglas que se aplican a ella, que pueden modificarla, dejarla tal cual o denegarla. Las reglas pueden filtrar la solicitud de un archivo de contenido basándose en información de un perfil de usuario obtenida en el inicio de sesión de éste (por ejemplo el puesto que ocupa en la empresa; [pár. 0508 y 0509]). Estas reglas pueden formar parte del motor de políticas 3236. Estas reglas pueden controlar el acceso a contenido almacenado. Este motor de políticas puede estar integrado en la funcionalidad del motor de políticas 406; (pár. 536).
Las diferencias entre la reivindicación 1 y el documento D01 se refieren a:

- el volcado en un fichero del conjunto de direcciones a las que se permite o no se permite acceder al usuario
- se asocian una o varias sentencias SQL al perfil del usuario

Sin embargo, no se considera que estas diferencias tengan un efecto técnico sino que serían meras implementaciones alternativas a las del documento D01 y, por tanto, evidentes para el experto en la materia:

- el volcado en un archivo sería totalmente equivalente en funcionalidad a su almacenamiento en una base de datos (o en una tabla, por ejemplo)
- la asociación de una o varias sentencias SQL equivaldría totalmente al mantenimiento de la base de datos de condiciones (sentencias tipo Select más concretamente) en las que se basa el motor de políticas del documento D01 (usando la información obtenida en el inicio de sesión del usuario)

En conclusión el documento D01 afecta a la actividad inventiva de la reivindicación 1 según el art. 8.1 de la Ley de Patentes.

Reivindicaciones dependientes

Reivindicaciones 2 y 3: las características de estas reivindicaciones responden al carácter dinámico/ volátil intrínseco de la información generada en la ejecución del método y, por tanto, se consideran evidentes para el experto en la materia.
Reivindicaciones 4 y 5: el contenido de estas reivindicaciones se recoge en D01.

En conclusión el documento D01 afecta a la actividad inventiva de las reivindicaciones 2-5 según el art. 8.1 de la Ley de Patentes.