

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Oficio N° 9107 de 28 de julio de 2020

Ref. Expediente N° NC2017/0003283

Señor(a)
CRYPTZONE NORTH AMERICA INC.

TÍTULO DE LA SOLICITUD: “SISTEMAS Y MÉTODOS PARA PROTEGER DISPOSITIVOS DE RED”

NÚMERO DE SOLICITUD INTERNACIONAL: PCT/US2015/050485

FECHA DE PRESENTACIÓN INTERNACIONAL: 16 de septiembre de 2015.

PRIORIDAD(ES): 6/10/2014, US (ESTADOS UNIDOS DE AMÉRICA), 62/060,427

19/12/2014, US (ESTADOS UNIDOS DE AMÉRICA), 14/578,140

17/08/2015, US (ESTADOS UNIDOS DE AMÉRICA), 14/828,357

Como resultado del examen de patentabilidad realizado a la solicitud indicada en la referencia, atendiendo a lo consagrado en el artículo 45 de la Decisión 486 de 2000, se le comunica que esta Dirección ha encontrado que la materia objeto de solicitud no cumple con algunos requisitos establecidos en la Decisión, con fundamento en los siguientes aspectos:

1. Modificaciones presentadas (Art. 34 Decisión 486)

Se aceptan las modificaciones radicadas el 22 de agosto de 2019, bajo el número NC2019/0009063, por ajustarse a los requisitos legales.

2. Objeto de la invención

De acuerdo con lo establecido en el numeral 1.2.2.2 del Capítulo Primero del Título X de la Circular Única para efectos del examen de patentabilidad, cuando la solicitud contenga más de diez (10) reivindicaciones y no se haya pagado la tasa complementaria, sólo se estudiarán las cubiertas por la tasa pagada al momento de realizar el examen de patentabilidad consagrado en el artículo 45 de la Decisión 486. Por lo tanto, se estudiarán las reivindicaciones 1 a 18 del radicado N° NC2019/0009063 del 22 de agosto de 2019.

El problema planteado en esta solicitud consiste en la necesidad de suministrar un método y un dispositivo capaz de implementar una puerta de enlace privada segura para toda la red y de fácil acceso para todos los usuarios que a su vez proteja los dispositivos del acceso no autorizado.

Para resolver este problema técnico, la solicitud en estudio proporciona modalidades que ayudan a proteger a los dispositivos de red contra acceso no autorizado. Entre otras cosas, las modalidades de la descripción permiten acceso completo a servidores de aplicaciones y otros dispositivos de red que un cliente tiene acceso permitido, mientras que evita acceso completo (o incluso conocimiento) de los dispositivos de red que el cliente no tiene acceso permitido (Resumen).

3. De la solicitud de patente

3.1. Título

El nombre de la invención de que se trata en el artículo 27 literal d) de la Decisión 486 deberá reflejar el objeto y el campo industrial con el cual se relaciona la misma y ser



Oficio N° 9107 de 28 de julio de 2020

Ref. Expediente N° NC2017/0003283

concordante con la materia descrita y las reivindicaciones de la solicitud. El nombre no podrá referirse a nombres personales, marcas de productos o nombres de fantasía.

El solicitante en el escrito radicado bajo el N° NC2017/0003283 el 4 de abril de 2017, tituló la invención como: “SISTEMAS Y MÉTODOS PARA PROTEGER DISPOSITIVOS DE RED”. Este título no se relaciona con el objeto de la solicitud contenido en la descripción y las reivindicaciones, por lo cual se sugiere el título siguiente: “SISTEMA, MÉTODO Y MEDIO LEGIBLE POR COMPUTADORA PARA PROTEGER DISPOSITIVOS DE RED”.

3.2. Reivindicaciones (Art. 30 Decisión 486)

El preámbulo de la reivindicación 1 no permite identificar con claridad el objeto a proteger porque se presenta de manera general en donde menciona: *“Un método implementado por computadora”* (Reiv. 1). Se recomienda presentar el preámbulo indicando cuál es el objeto de la invención, el cual suele coincidir con el título de la invención: *“Un método implementado por computadora para proteger dispositivos de red caracterizado porque comprende: (...)”*

4. Determinación del Estado de la Técnica

La fecha para determinar el estado de la técnica es el 6 de octubre de 2014 que corresponde a la fecha de presentación de la solicitud de prioridad.

Consultadas las fuentes de información con que se cuenta, se encontraron los siguientes documentos que anticipan el objeto de esta solicitud:

Ítem	Documento	Título	Fecha de Publicación
D1	US2014282914	“System and Method for secure application communication between networked processors”	18 de septiembre de 2014
D2	US6381631	“Method and apparatus for controlling client computer systems”	30 de abril de 2002

El documento D1¹ divulga un sistema y método para transportar datos de aplicaciones a través de un túnel de comunicaciones entre un dispositivo host y un dispositivo invitado que incluye procesadores en red cada uno. Los datos de la aplicación se pueden transportar entre el dispositivo host y el dispositivo invitado a través de un puerto permitido del dispositivo host, el túnel de comunicaciones y un puerto del dispositivo invitado. Según las credenciales de inicio de sesión, el dispositivo invitado puede ser autenticado por un servidor de seguridad y se puede determinar un rol. El rol puede incluir puertos permitidos y aplicaciones asociadas en el host al que el invitado puede acceder. El acceso remoto desde el dispositivo invitado a dispositivos host o dispositivos remotos puede habilitarse sin necesidad de conocer previamente sus configuraciones. El acceso seguro puede ser facilitado a dispositivos host remotos o dispositivos remotos, de acuerdo con políticas de seguridad que pueden variar por sesión y toma en cuenta varios factores (Resumen).

El documento D2² divulga un método y aparato que conectan a un usuario a una red remota e impone el funcionamiento del software de gestión antes de que el usuario pueda realizar otras tareas en la red remota. El método y el aparato también permiten la conexión del usuario a una red de terceros. El usuario puede tener restricciones para

¹ <https://patentimages.storage.googleapis.com/80/28/c2/c9b0c0ea1c61c5/US20140282914A1.pdf>

² <https://patentimages.storage.googleapis.com/99/c0/af/96a0b20ce0696d/US6381631.pdf>

Oficio N° 9107 de 28 de julio de 2020

Ref. Expediente N° NC2017/0003283

acceder a redes de terceros que no se encuentran en una lista confiable de redes, que pueden ser actualizadas por el software de administración. El método y el aparato imponen reglas de acceso para el software de terceros para evitar la recuperación no autorizada o la eliminación de información por parte del software de terceros (Resumen).

5. Examen de Patentabilidad (Art. 14 Decisión 486)

5.1. Nivel Inventivo (Art. 18 Decisión 486)

La reivindicación 1 consiste en: “Un método implementado por computadora caracterizado porque comprende: recibir, por un sistema informático que implementa una puerta de enlace (100) en una red privada (140), una solicitud de un dispositivo de cliente (121) para un túnel de red entre el dispositivo de cliente (121) y un dispositivo de red (141) en la red privada (140) (...)” (Radicado N° NC2019/0009063 del 22 de agosto de 2019).

Tabla 1. Comparación de las características técnicas esenciales, con las del estado de la técnica:

Características esenciales	D1	D2
Un método implementado por computadora caracterizado porque comprende.	Un sistema y método para transportar datos de aplicaciones a través de un túnel de comunicaciones entre un dispositivo host y un dispositivo invitado (Pág. 1, Párr. 0002).	Un método y un aparato conectan a un usuario a una red remota y hacen cumplir la operación del software de administración antes de que el usuario pueda realizar otras tareas en la red remota (Resumen, líneas 1 a 4).
Recibir, por un sistema informático que implementa una puerta de enlace (100) en una red privada (140), una solicitud de un dispositivo de cliente (121) para un túnel de red entre el dispositivo de cliente (121) y un dispositivo de red (141) en la red privada (140).	En la etapa (502), se puede recibir una solicitud de conexión desde el dispositivo invitado (204) en el servidor de facilitación de conexión (220) que denota que el dispositivo invitado (204) desea establecer el túnel de comunicaciones (222) con el dispositivo host (254) y un dispositivo remoto (262) (Pág. 5, Párr. 0044, líneas 4 a 9). El dispositivo remoto (1062) y el dispositivo host (1054) pueden estar en comunicación a través de una red de área local (1064) (...) El dispositivo local (1004) y el dispositivo invitado (1002) pueden estar en comunicación a través de una red (1070), tal como una red de área local, por ejemplo, u otro tipo de red o camino o túnel de comunicaciones (Pág. 9, Párr. 0071).	No menciona.
Autenticar el dispositivo de cliente (121) por el sistema informático.	Puede determinarse en el paso (514) si el dispositivo invitado (204) ha sido autenticado por el servidor de seguridad (258) (Pág. 6, Párr. 0048, líneas 1 a 2).	No menciona.
Al autenticar el dispositivo cliente (121), recibir, de un servidor de autenticación (160) en comunicación con el sistema informático, una lista de accesos de cliente que incluye una lista de dispositivos de	Si el dispositivo invitado (104) es autenticado y validado para el servidor de facilitación de conexión (120), el dispositivo invitado (1049) puede recibir una lista de servidores entre los que también podría estar el dispositivo anfitrión (154). De la lista de dispositivos de host (154), un usuario en el dispositivo de invitado (104) puede seleccionar un	No menciona.

Oficio N° 9107 de 28 de julio de 2020

Ref. Expediente N° NC2017/0003283

red con la que tiene permitido comunicarse el dispositivo de cliente (121).	dispositivo de host particular (154) al que el usuario desea acceder (Párr. 0026).	
En donde la autenticación del dispositivo cliente incluye el sistema informático que verifica una firma digital en la lista de acceso del cliente a través de una clave de firma compartida entre la puerta de enlace y el servidor de autenticación.	No menciona.	El autenticador (230) también puede usar otros procesos de autenticación, como las técnicas de autenticación convencionales. Comparación de firma digital. El autenticador (230) puede enviar un acuse de recibo a través de la misma ruta a la red remota si el proceso de autenticación descrito anteriormente es exitoso, y puede recibir un acuse de recibo de la red remota a través de la misma ruta (Col. 6, líneas 45 a 51).
Al recibir la lista de accesos de cliente y en respuesta a que la firma digital es correcta, verificar, por el sistema informático, que el dispositivo de red (141) en la red privada (140) sea parte de la lista de dispositivos de red con la que tiene permitido comunicarse el dispositivo de cliente (121).	Puede determinarse en el paso (514) si el dispositivo invitado (204) ha sido autenticado por el servidor de seguridad (258). Si el dispositivo invitado (204) no se ha autenticado con éxito en el paso (514), entonces el proceso (500) puede estar completo y la sesión puede finalizar. Sin embargo, si el dispositivo invitado (204) se autentica satisfactoriamente en el paso (514), entonces el proceso (500) puede continuar al paso (516) (...) Las credenciales de inicio de sesión pueden indicar una identidad del usuario del dispositivo invitado (204) y, por lo tanto, el nivel de acceso, por ejemplo, puertos y aplicaciones, que el usuario debería tener en el dispositivo remoto (262) (Pág. 6, Párr. 0048).	No menciona.
Al verificar que el dispositivo de red (141) en la red privada (140) es parte de la lista de dispositivos de red con la que tiene permitido comunicarse el dispositivo de cliente (121), establecer, por el sistema informático, el túnel de red entre el dispositivo de cliente (121) y el dispositivo de red en la red privada a través de la puerta de enlace (100).	Después de recibir la selección del puerto deseado y su aplicación asociada, los datos de la aplicación pueden reenviarse en la etapa (524) entre el puerto en el dispositivo remoto (262) y un puerto del dispositivo invitado a través del dispositivo host (254) y el túnel de comunicaciones (222) (Pág. 6, Párr. 0051, líneas 1 a 5).	No menciona.

El documento D1 se considera el estado de la técnica más cercano a la invención definida en la reivindicación 1 porque divulga un sistema y método para la comunicación segura de aplicaciones entre procesadores en red, incluidos dispositivos basados en procesadores con capacidad de red. Más particularmente, esta invención proporciona un sistema y un método para transportar datos de la aplicación a través de un túnel de comunicaciones entre un dispositivo host y un dispositivo invitado, y los datos de la aplicación pueden reenviarse entre el dispositivo host y el dispositivo invitado a través de

Oficio N° 9107 de 28 de julio de 2020

Ref. Expediente N° NC2017/0003283

un puerto permitido del dispositivo host, el túnel de comunicaciones y un puerto del dispositivo invitado durante una sesión activa (Pág. 1, Párr. 0002).

La diferencia entre la invención definida en la reivindicación 1 y el método divulgado de D1 consiste en que la autenticación del dispositivo cliente incluye que el sistema informático verifica una firma digital en la lista de acceso del cliente a través de una clave de firma compartida entre la puerta de enlace y el servidor de autenticación.

El efecto que se logra al incluir que la autenticación del dispositivo cliente incorpore que el sistema informático verifica una firma digital en la lista de acceso del cliente a través de una clave de firma compartida entre la puerta de enlace y el servidor de autenticación es identificar los dispositivos de los clientes evitando suplantaciones.

Por lo tanto, el problema técnico objetivo que pretende resolver esta invención se puede formular así: ¿Cómo modificar el método conocido en D1 para identificar los dispositivos de los clientes evitando suplantaciones?

Sin embargo, el incluir que la autenticación del dispositivo cliente incorpore que el sistema informático verifique una firma digital en la lista de acceso del cliente a través de una clave de firma compartida entre la puerta de enlace y el servidor de autenticación para identificar los dispositivos de los clientes evitando suplantaciones, ya está divulgado en el documento D2 que se refiere a un método y un aparato conectan a un usuario a una red remota y hacen cumplir la operación del software de administración antes de que el usuario pueda realizar otras tareas en la red remota (Resumen, líneas 1 a 4). El autenticador (230) también puede usar otros procesos de autenticación, como las técnicas de autenticación convencionales. Comparación de firma digital. El autenticador (230) puede enviar un acuse de recibo a través de la misma ruta a la red remota si el proceso de autenticación descrito anteriormente es exitoso, y puede recibir un acuse de recibo de la red remota a través de la misma ruta (Col. 6, líneas 45 a 51).

En consecuencia, la persona normalmente versada en la materia estaría motivada a incluir que la autenticación del dispositivo cliente incorpore que el sistema informático verifique una firma digital en la lista de acceso del cliente a través de una clave de firma compartida entre la puerta de enlace y el servidor de autenticación del documento D2 en el método de D1, para así llegar al objeto de la reivindicación 1. Por lo cual se considera obvia.

Asimismo, el documento D1 divulga las características de las reivindicaciones dependientes así:

- Reivindicación 2: Los datos de la aplicación pueden incluir datos gráficos, datos de texto, datos binarios y/u otros datos que permiten al usuario del dispositivo invitado (104) ejecutar e interactuar con la aplicación en el dispositivo invitado (104) basándose en los datos de la aplicación recibida (Pág. 4, Párr. 0035, líneas 1 a 5).
- Reivindicación 3: Por ejemplo, si la aplicación deseada es un navegador web, los datos de la aplicación pueden incluir el código fuente HTML que define el contenido y el diseño de las páginas web. Como otro ejemplo, si la aplicación deseada es una ventana de comando, entonces los datos de la aplicación pueden incluir datos de texto para avisos, opciones de menú, etc. Los eventos que se han producido mientras la sesión están activa y sus marcas de tiempo correspondientes se pueden registrar en el paso (424). El servidor de seguridad (158) puede registrar



Oficio N° 9107 de 28 de julio de 2020

Ref. Expediente N° NC2017/0003283

los eventos en una base de datos de registro (160), por ejemplo (Pág. 4, Párr. 0035, líneas 5 a 13).

- Reivindicación 4: El dispositivo remoto (262) puede incluir, por ejemplo, un sistema de control de edificios (por ejemplo, sistema HVAC, sistema de iluminación, etc.), un sistema de control industrial (por ejemplo, sistema de control de potencia, sistema de control de equipos de fabricación, etc.), una impresora, una copiadora, un componente de red (por ejemplo, conmutador, enrutador, etc.) y / u otro dispositivo con capacidad de red (Pág. 4, Párr. 0037, líneas 6 a 12).
- Reivindicaciones 5: Un cortafuego (206) puede controlar el tráfico entre el dispositivo invitado (204) y los dispositivos externos a la ubicación (202), y de manera similar, un cortafuegos (256) puede controlar el tráfico entre el dispositivo remoto (262) y el dispositivo host (254) y los dispositivos externos a la ubicación (252) (Pág. 5, Párr. 0039, líneas 6 a 10).
- Reivindicación 6: Los cortafuegos (106) y (156) pueden estar basados en software o basados en hardware, como se conoce en la técnica. Los firewalls (106) y (156) no necesitan tener ningún puerto de entrada abierto, lo que puede eliminar las vulnerabilidades de las violaciones de red (Pág. 2, Párr. 21, líneas 12 a 15).
- Reivindicación 7: Además, se puede facilitar el acceso seguro a dispositivos host o dispositivos remotos, de acuerdo con políticas de seguridad que pueden variar por sesión y tienen en cuenta varios factores. Solo los puertos permitidos seleccionados se pueden utilizar para el acceso remoto, mientras que otros puertos tienen restricciones de uso (Pág. 1, Párr. 8, líneas 4 a 9).
- Reivindicación 8: El servidor de seguridad (258) puede determinar la función del dispositivo invitado (204) en base a las políticas y estándares de seguridad establecidos dentro del servidor de seguridad (258). Las credenciales de inicio de sesión pueden indicar una identidad del usuario del dispositivo invitado (204) y, por lo tanto, el nivel de acceso, por ejemplo, puertos y aplicaciones, que el usuario debería tener en el dispositivo remoto (262) (Pág. 6, Párr. 48, líneas 14 a 19).
- Reivindicación 10: Solo los puertos permitidos seleccionados se pueden utilizar para el acceso remoto, mientras que otros puertos tienen restricciones de uso (Pág. 1, Párr. 8, líneas 7 a 9); Cada uno de los dispositivos de invitado (104) y el dispositivo de host (154) puede realizar una comunicación inicial con el servidor de facilitación de conexión (120), que incluye la conexión y la autenticación al servidor de facilitación de conexión (120). El dispositivo de host (154) puede transmitir al servidor de facilitación de conexión (120) una identificación del dispositivo de host (154). El dispositivo invitado (104) puede solicitar una lista de dispositivos de host (154) desde el servidor de facilitación de conexión (120) que son accesibles a la computadora de invitado (104). Si el dispositivo invitado (104) es autenticado y validado para el servidor de facilitación de conexión (120), el dispositivo invitado (104) puede recibir una lista de servidores entre los que también podría estar el dispositivo anfitrión (154). De la lista de dispositivos de host (154), un usuario en el dispositivo de invitado (104) puede seleccionar un dispositivo de host particular (154) al que el usuario desea acceder (Pág. 3, Párr. 0026).
- Reivindicación 11: La función del dispositivo invitado (104) / dispositivo local (1004)

Oficio N° 9107 de 28 de julio de 2020

Ref. Expediente N° NC2017/0003283

puede incluir los puertos en el dispositivo host (154) a los que se permite el acceso del dispositivo invitado (104) / dispositivo local (1004), y las aplicaciones asociadas que utilizan esos puertos en el dispositivo host (154). Aunque las aplicaciones son capaces de ejecutarse en el dispositivo host (154), una vez que los datos de la aplicación se envían a través del túnel de comunicaciones (122), como se describe más adelante, una aplicación seleccionada particular se ejecuta en el dispositivo invitado (104) usando los datos de la aplicación recibidos del dispositivo host (154) (Pág. 4, Párr. 0032).

- Reivindicación 12: Por ejemplo, el tipo de autenticación puede basarse en protocolos tales como Active Directory, LDAP (Protocolo ligero de acceso a directorios), RADIUS (Servicio de usuario de marcado de autenticación remota), RSA y/u otros protocolos (Pág. 3, Párr. 29, líneas 16 a 20). La función del dispositivo invitado (104) / dispositivo local (1004) puede incluir los puertos en el dispositivo host (154) a los que se permite el acceso del dispositivo invitado (104) / dispositivo local (1004), y las aplicaciones asociadas que utilizan esos puertos en el dispositivo host (154) (Pág. 4, Párr. 32, líneas 1 a 5). En un entorno de red preferido, cada uno de la pluralidad de dispositivos informáticos (300) en la red está configurado para usar el conjunto de protocolos de Internet (TCP/IP) para comunicarse entre sí (Pág. 8, Párr. 67, líneas 6 a 9).
- Reivindicación 13: La figura 6 muestra una realización de un proceso (600) para recibir credenciales de inicio de sesión y autenticar un dispositivo invitado (104), (204) junto con el proceso (400) de la figura 4 o el proceso (500) de la figura 5. El proceso (600) puede realizar la autenticación desde el dispositivo invitado (104), (204) a través del dispositivo host (154), (254) y el servidor de seguridad (158), (258). El proceso (600) puede incluir realizaciones de los pasos (408), (410), (508) y (510), como se describió anteriormente. En la etapa (602), el servidor de seguridad (158), (258) puede determinar un tipo de autenticación para el dispositivo invitado (104), (204), basándose en configuraciones predefinidas asociadas con el dispositivo invitado (104), (204) en el servidor de seguridad (158). Un tipo de autenticación particular, tal como basado en protocolos tales como Active Directory, LDAP, RADIUS, RSA, etc., puede estar asociado con el dispositivo invitado (104), (204). En la etapa (604), el tipo de autenticación determinado puede transmitirse desde el dispositivo host (154), (254) al dispositivo invitado (104), (204) a través del túnel de comunicaciones (122), (222). De esta manera, se informará a un usuario del dispositivo invitado (104), (204) en cuanto a qué credenciales de inicio de sesión y tipo de autenticación son necesarios para acceder con éxito al dispositivo host (154), (254) (y a los dispositivos remotos asociados 262) (Págs. 6 y 7, Párr. 0052, líneas 1 a 21).
- Reivindicación 14: Como otro ejemplo, los empleados pueden tener mayor acceso a recursos informáticos si se conectan al dispositivo host (154) desde una computadora de escritorio en la casa del empleado, y pueden tener un acceso más restringido a recursos informáticos si se conectan al dispositivo host (154) desde una computadora portátil en una red inalámbrica pública (Párr. 0024, líneas 12 a 17).
- Reivindicación 16: El dispositivo invitado (104) y el dispositivo host (154) pueden comunicar solicitudes de conexión, mantener señales vivas y/u otros datos e información en el servidor de facilitación de conexión (120) (Párr. 22); El servidor de seguridad (158) puede almacenar y registrar eventos y las marcas de tiempo



Oficio N° 9107 de 28 de julio de 2020

Ref. Expediente N° NC2017/0003283

correspondientes cuando los eventos ocurrieron en una base de datos (160) de registro (Pág. 3, Párr. 0025).

Asimismo, el documento D2 divulga las características de las reivindicaciones dependientes así:

- Reivindicación 9: Si el usuario se autentica localmente, o de lo contrario si no se realiza una autenticación local, se conecta una red remota (318), por ejemplo, marcando un número de acceso VPN o proveedor de servicios de Internet u otra parte y transmitiendo un identificador de la red remota que se recupera de una base de datos o archivo como se describe anteriormente. Los identificadores que corresponden a la información de identificación del usuario recibida en el Paso (310) se proporcionan a la red remota como parte del paso (318). (Col. 11, líneas 15 a 23).

Las reivindicaciones dependientes 2 a 8, 10 a 14 y 16 no mencionan alguna característica que, junto con las características de la reivindicación independiente, aporte nivel inventivo al método de la reivindicación 1, por lo cual se considera que no tienen nivel inventivo.

La reivindicación 17 consiste en: *“Un medio legible por computadora no transitorio caracterizado porque almacena instrucciones que, cuando se ejecutan, provocan que un sistema informático que implementa una puerta de enlace (100) a una red privada (140) (...)”* (Radicado N° NC2019/0009063 del 22 de agosto de 2019).

Tabla 2. Comparación de las características técnicas esenciales, con las del estado de la técnica:

Características esenciales	D1	D2
Un medio legible por computadora no transitorio caracterizado porque almacena instrucciones que, cuando se ejecutan, provocan que un sistema informático que implementa una puerta de enlace (100) a una red privada (140).	Un "medio legible por computadora" puede ser cualquier medio que pueda almacenar, comunicar, propagar o transportar objetos de datos para su uso por o en conexión con el facilitador (310) de comunicación segura. El medio legible por ordenador puede ser, por ejemplo, un sistema, aparato, dispositivo, medio de propagación electrónico, magnético, óptico, electromagnético, infrarrojo o semiconductor, o cualquier otro dispositivo con funcionalidad similar (Pág. 8, Párr. 0066, líneas 1 a 8).	El producto de programa de computadora (174) ha codificado en él dispositivos de código de programa legibles por computadora (176), tales como cargas magnéticas en el caso de un disquete o codificaciones ópticas en el caso de un CD-ROM que se codifican como instrucciones de programa, datos o ambos para configurar la computadora sistema (150) para operar como se describe a continuación (Col. 4, líneas 38 a 43).
Reciba una solicitud de un dispositivo de cliente (121) para un túnel de red entre el dispositivo de cliente y un dispositivo de red (141) en la red privada (140).	En la etapa (502), se puede recibir una solicitud de conexión desde el dispositivo invitado (204) en el servidor de facilitación de conexión (220) que denota que el dispositivo invitado (204) desea establecer el túnel de comunicaciones (222) con el dispositivo host (254) y un dispositivo remoto (262) (Pág. 5, Párr. 0044, líneas 4 a 9). El dispositivo remoto (1062) y el dispositivo host (1054) pueden estar en comunicación a través de una red de área local (1064) (...) El dispositivo local (1004) y el dispositivo invitado (1002) pueden	No menciona.

Oficio N° 9107 de 28 de julio de 2020

Ref. Expediente N° NC2017/0003283

	estar en comunicación a través de una red (1070), tal como una red de área local, por ejemplo, u otro tipo de red o camino o túnel de comunicaciones (Pág. 9, Párr. 0071, líneas 6 a 12).	
Autenticar el dispositivo de cliente (121).	Puede determinarse en el paso (514) si el dispositivo invitado (204) ha sido autenticado por el servidor de seguridad (258) (Pág. 6, Párr. 0048, líneas 1 a 2).	No menciona.
al autenticar el dispositivo cliente (121), reciba, de un servidor de autenticación (160) en comunicación con el sistema informático, una lista de accesos de cliente que incluye una lista de dispositivos de red con la que tiene permitido comunicarse el dispositivo de cliente (121).	Si el dispositivo invitado (104) es autenticado y validado para el servidor de facilitación de conexión (120), el dispositivo invitado (1049) puede recibir una lista de servidores entre los que también podría estar el dispositivo anfitrión (154). De la lista de dispositivos de host (154), un usuario en el dispositivo de invitado (104) puede seleccionar un dispositivo de host particular (154) al que el usuario desea acceder (Pág. 3, Párr. 0026, líneas 9 a 14).	No menciona.
En donde la autenticación del dispositivo cliente incluye el sistema informático que verifica una firma digital en la lista de acceso del cliente a través de una clave de firma compartida entre la puerta de enlace y el servidor de autenticación.	No menciona.	El autenticador (230) también puede usar otros procesos de autenticación, como las técnicas de autenticación convencionales. Comparación de firma digital. El autenticador (230) puede enviar un acuse de recibo a través de la misma ruta a la red remota si el proceso de autenticación descrito anteriormente es exitoso, y puede recibir un acuse de recibo de la red remota a través de la misma ruta (Col. 6, líneas 45 a 51).
Al recibir la lista de accesos de cliente y en respuesta a que la firma digital es correcta, verificar, por el sistema informático, que el dispositivo de red (141) en la red privada (140) sea parte de la lista de dispositivos de red con la que tiene permitido comunicarse el dispositivo de cliente (121).	Puede determinarse en el paso (514) si el dispositivo invitado (204) ha sido autenticado por el servidor de seguridad (258). Si el dispositivo invitado (204) no se ha autenticado con éxito en el paso (514), entonces el proceso (500) puede estar completo y la sesión puede finalizar. Sin embargo, si el dispositivo invitado (204) se autentica satisfactoriamente en el paso (514), entonces el proceso (500) puede continuar al paso (516) (...) Las credenciales de inicio de sesión pueden indicar una identidad del usuario del dispositivo invitado (204) y, por lo tanto, el nivel de acceso, por ejemplo, puertos y aplicaciones, que el usuario debería tener en el dispositivo remoto (262) (Pág. 6, Párr. 0048, líneas 1 a 10).	No menciona.
Al verificar que el dispositivo de red (141) en la red privada (140) es parte de la lista de dispositivos de red con la	Después de recibir la selección del puerto deseado y su aplicación asociada, los datos de la aplicación pueden reenviarse en la etapa (524) entre el puerto en el dispositivo	No menciona.

Oficio N° 9107 de 28 de julio de 2020

Ref. Expediente N° NC2017/0003283

que tiene permitido comunicarse el dispositivo de cliente (121), establezca el túnel de red entre el dispositivo de cliente (121) y el dispositivo de red (141) en la red privada (140) a través de la puerta de enlace (100).	remoto (262) y un puerto del dispositivo invitado a través del dispositivo host (254) y el túnel de comunicaciones (222) (Pág. 6, Párr. 0051, líneas 1 a 5).	
--	--	--

El documento D1 se considera el estado de la técnica más cercano a la invención definida en la reivindicación 17 porque divulga un sistema y método para la comunicación segura de aplicaciones entre procesadores en red, incluidos dispositivos basados en procesadores con capacidad de red. Más particularmente, esta invención proporciona un sistema y un método para transportar datos de la aplicación a través de un túnel de comunicaciones entre un dispositivo host y un dispositivo invitado, y los datos de la aplicación pueden reenviarse entre el dispositivo host y el dispositivo invitado a través de un puerto permitido del dispositivo host, el túnel de comunicaciones y un puerto del dispositivo invitado durante una sesión activa (Pág. 1, Párr. 0002).

La diferencia entre la invención definida en la reivindicación 17 y el medio legible divulgado de D1 consiste en que la autenticación del dispositivo cliente incluye que el sistema informático verifica una firma digital en la lista de acceso del cliente a través de una clave de firma compartida entre la puerta de enlace y el servidor de autenticación.

El efecto que se logra al incluir que la autenticación del dispositivo cliente incorpore que el sistema informático verifique una firma digital en la lista de acceso del cliente a través de una clave de firma compartida entre la puerta de enlace y el servidor de autenticación es identificar los dispositivos de los clientes evitando suplantaciones.

Por lo tanto, el problema técnico objetivo que pretende resolver esta invención se puede formular así: ¿Cómo modificar el medio legible por computadora conocido en D1 para identificar los dispositivos de los clientes evitando suplantaciones?

Sin embargo, el incluir que la autenticación del dispositivo cliente incorpore que el sistema informático verifique una firma digital en la lista de acceso del cliente a través de una clave de firma compartida entre la puerta de enlace y el servidor de autenticación para identificar los dispositivos de los clientes evitando suplantaciones, ya está divulgado en el documento D2 que se refiere a un método y un aparato conectan a un usuario a una red remota y hacen cumplir la operación del software de administración antes de que el usuario pueda realizar otras tareas en la red remota (Resumen, líneas 1 a 4). El autenticador (230) también puede usar otros procesos de autenticación, como las técnicas de autenticación convencionales. Comparación de firma digital. El autenticador (230) puede enviar un acuse de recibo a través de la misma ruta a la red remota si el proceso de autenticación descrito anteriormente es exitoso, y puede recibir un acuse de recibo de la red remota a través de la misma ruta (Col. 6, líneas 45 a 51).

En consecuencia, la persona normalmente versada en la materia estaría motivada a incluir que la autenticación del dispositivo cliente incorpore que el sistema informático verifique una firma digital en la lista de acceso del cliente a través de una clave de firma compartida entre la puerta de enlace y el servidor de autenticación del documento D2 en el medio legible por computadora de D1, para así llegar al objeto de la reivindicación 17. Por lo cual se considera obvia.

Oficio N° 9107 de 28 de julio de 2020

Ref. Expediente N° NC2017/0003283

La reivindicación 18 consiste en: “*Un sistema informático que implementa una puerta de enlace, el sistema informático caracterizado porque comprende (...)*” (Radicado N° NC2019/0009063 del 22 de agosto de 2019).

Tabla 3. Comparación de las características técnicas esenciales, con las del estado de la técnica:

Características esenciales	D1	D2
Un sistema informático que implementa una puerta de enlace, el sistema informático caracterizado porque comprende: un procesador; y una memoria no transitoria en comunicación con el procesador y que almacena instrucciones que, cuando se ejecutan por el procesador, provocan que el sistema informático:	Cuando el dispositivo informático (300) está en funcionamiento, el procesador (302) está configurado para ejecutar software almacenado en la memoria (304), para comunicar datos hacia y desde la memoria (304), y para controlar en general las operaciones del dispositivo informático (300) de acuerdo con el software. El facilitador de comunicación segura (310) y el sistema operativo (312), en su totalidad o en parte, pueden ser leídos por el procesador (302), almacenados en el procesador (302), y luego ejecutados (Pág. 8, Párr. 0065).	El producto de programa de computadora (174) ha codificado en él dispositivos de código de programa legibles por computadora (176), tales como cargas magnéticas en el caso de un disquete o codificaciones ópticas en el caso de un CD-ROM que se codifican como instrucciones de programa, datos o ambos para configurar la computadora sistema (150) para operar como se describe a continuación (Col. 4, líneas 38 a 43).
Reciba una solicitud de un dispositivo de cliente (121) para un túnel de red entre el dispositivo de cliente (121) y un dispositivo de red (141) en la red privada (140)	En la etapa (502), se puede recibir una solicitud de conexión desde el dispositivo invitado (204) en el servidor de facilitación de conexión (220) que denota que el dispositivo invitado (204) desea establecer el túnel de comunicaciones (222) con el dispositivo host (254) y un dispositivo remoto (262) (Pág. 5, Párr. 0044, líneas 4 a 9). El dispositivo remoto (1062) y el dispositivo host (1054) pueden estar en comunicación a través de una red de área local (1064) (...) El dispositivo local (1004) y el dispositivo invitado (1002) pueden estar en comunicación a través de una red (1070), tal como una red de área local, por ejemplo, u otro tipo de red o camino o túnel de comunicaciones (Pág. 9, Párr. 0071, líneas 6 a 12).	No menciona.
Autentique el dispositivo de cliente (121).	Puede determinarse en el paso (514) si el dispositivo invitado (204) ha sido autenticado por el servidor de seguridad (258) (Pág. 6, Párr. 0048, líneas 1 a 2).	No menciona.
Al autenticar el dispositivo cliente (121), reciba, de un servidor de autenticación (160) en comunicación con el sistema informático, una lista de accesos de cliente que incluye una lista de dispositivos de red con la	Si el dispositivo invitado (104) es autenticado y validado para el servidor de facilitación de conexión (120), el dispositivo invitado (1049) puede recibir una lista de servidores entre los que también podría estar el dispositivo anfitrión (154). De la lista de dispositivos de host (154), un usuario en el dispositivo de invitado (104) puede seleccionar un	No menciona.

Oficio N° 9107 de 28 de julio de 2020

Ref. Expediente N° NC2017/0003283

que tiene permitido comunicarse el dispositivo de cliente (121).	dispositivo de host particular (154) al que el usuario desea acceder (Pág. 3, Párr. 0026, líneas 9 a 14).	
En donde la autenticación del dispositivo cliente incluye el sistema informático que verifica una firma digital en la lista de acceso del cliente a través de una clave de firma compartida entre la puerta de enlace y el servidor de autenticación.	No menciona.	El autenticador (230) también puede usar otros procesos de autenticación, como las técnicas de autenticación convencionales. Comparación de firma digital. El autenticador (230) puede enviar un acuse de recibo a través de la misma ruta a la red remota si el proceso de autenticación descrito anteriormente es exitoso, y puede recibir un acuse de recibo de la red remota a través de la misma ruta (Col. 6, líneas 45 a 51).
Al recibir la lista de accesos de cliente y en respuesta a que la firma digital es correcta, verificar, por el sistema informático, que el dispositivo de red (141) en la red privada (140) sea parte de la lista de dispositivos de red con la que tiene permitido comunicarse el dispositivo de cliente (121).	Puede determinarse en el paso (514) si el dispositivo invitado (204) ha sido autenticado por el servidor de seguridad (258). Si el dispositivo invitado (204) no se ha autenticado con éxito en el paso (514), entonces el proceso (500) puede estar completo y la sesión puede finalizar. Sin embargo, si el dispositivo invitado (204) se autentica satisfactoriamente en el paso (514), entonces el proceso (500) puede continuar al paso (516) (...) Las credenciales de inicio de sesión pueden indicar una identidad del usuario del dispositivo invitado (204) y, por lo tanto, el nivel de acceso, por ejemplo, puertos y aplicaciones, que el usuario debería tener en el dispositivo remoto (262) (Pág. 6, Párr. 0048, líneas 1 a 10).	No menciona.
Al verificar que el dispositivo de red (141) en la red privada (140) es parte de la lista de dispositivos de red con la que tiene permitido comunicarse el dispositivo de cliente (121), establezca el túnel de red entre el dispositivo de cliente (121) y el dispositivo de red (141) en la red privada (140) a través de la puerta de enlace (100).	Después de recibir la selección del puerto deseado y su aplicación asociada, los datos de la aplicación pueden reenviarse en la etapa (524) entre el puerto en el dispositivo remoto (262) y un puerto del dispositivo invitado a través del dispositivo host (254) y el túnel de comunicaciones (222) (Pág. 6, Párr. 0051, líneas 1 a 5).	No menciona.

El documento D1 se considera el estado de la técnica más cercano a la invención definida en la reivindicación 18 porque divulga un sistema y método para la comunicación segura de aplicaciones entre procesadores en red, incluidos dispositivos basados en procesadores con capacidad de red. Más particularmente, esta invención proporciona un sistema y un método para transportar datos de la aplicación a través de un túnel de comunicaciones entre un dispositivo host y un dispositivo invitado, y los datos de la aplicación pueden reenviarse entre el dispositivo host y el dispositivo invitado a través de

Oficio N° 9107 de 28 de julio de 2020

Ref. Expediente N° NC2017/0003283

un puerto permitido del dispositivo host, el túnel de comunicaciones y un puerto del dispositivo invitado durante una sesión activa (Pág. 1, Párr. 0002).

La diferencia entre la invención definida en la reivindicación 18 y el sistema informático divulgado de D1 consiste en que la autenticación del dispositivo cliente incluye que el sistema informático verifica una firma digital en la lista de acceso del cliente a través de una clave de firma compartida entre la puerta de enlace y el servidor de autenticación.

El efecto que se logra al incluir que la autenticación del dispositivo cliente incorpore que el sistema informático verifique una firma digital en la lista de acceso del cliente a través de una clave de firma compartida entre la puerta de enlace y el servidor de autenticación es identificar los dispositivos de los clientes evitando suplantaciones.

Por lo tanto, el problema técnico objetivo que pretende resolver esta invención se puede formular así: ¿Cómo modificar el medio legible por computadora conocido en D1 para identificar los dispositivos de los clientes evitando suplantaciones?

Sin embargo, el incluir que la autenticación del dispositivo cliente incorpore que el sistema informático verifique una firma digital en la lista de acceso del cliente a través de una clave de firma compartida entre la puerta de enlace y el servidor de autenticación para identificar los dispositivos de los clientes evitando suplantaciones, ya está divulgado en el documento D2 que se refiere a un método y un aparato conectan a un usuario a una red remota y hacen cumplir la operación del software de administración antes de que el usuario pueda realizar otras tareas en la red remota (Resumen, líneas 1 a 4). El autenticador (230) también puede usar otros procesos de autenticación, como las técnicas de autenticación convencionales. Comparación de firma digital. El autenticador (230) puede enviar un acuse de recibo a través de la misma ruta a la red remota si el proceso de autenticación descrito anteriormente es exitoso, y puede recibir un acuse de recibo de la red remota a través de la misma ruta (Col. 6, líneas 45 a 51).

En consecuencia, la persona normalmente versada en la materia estaría motivada a incluir que la autenticación del dispositivo cliente incorpore que el sistema informático verifique una firma digital en la lista de acceso del cliente a través de una clave de firma compartida entre la puerta de enlace y el servidor de autenticación del documento D2 en el medio legible por computadora de D1, para así llegar al objeto de la reivindicación 18. Por lo cual se considera obvia.

6. Conclusión con respecto a novedad y/o nivel inventivo

Los requisitos de Patentabilidad de la presente solicitud están afectados así:

Ítem	Documento	Reivindicaciones afectadas	Requisito que afecta
D1	US2014282914	1 a 8, 10 a 14 y 16 a 18	Nivel Inventivo
D2	US6381631	1, 9, 17 y 18	Nivel Inventivo

En cumplimiento del artículo 45 de la Decisión 486 de 2000, se le indica que debe dar respuesta dentro del término de sesenta (60) días contados a partir de la fecha de notificación de la presente comunicación. En caso de no dar respuesta al presente requerimiento, o si a pesar de la respuesta subsistieran los impedimentos para la concesión, se denegará la patente.

Si como respuesta a este requerimiento, el solicitante modifica: i) el capítulo reivindicatorio, ii) la descripción de la invención a proteger, iii) o presenta un nuevo

Oficio N° **9107** de **28 de julio de 2020**

Ref. Expediente N° NC2017/0003283

capítulo reivindicatorio deberá observar las instrucciones contenidas en el numeral 1.2.2.1.1., del Capítulo Primero del Título X de la Circular Única y la Dirección de Nuevas Creaciones seguirá el procedimiento descrito en el numeral 1.2.2.5.1.

Notifíquese el presente oficio conforme a lo dispuesto en el numeral 6.2 del Capítulo Sexto del Título I de la Circular Única, informándoles que contra el mismo no procede recurso alguno en actuación administrativa.



Edna Marcela Ramirez Orozco
DIRECTORA DE NUEVAS CREACIONES



Oficio N° 9107 de 28 de julio de 2020

Ref. Expediente N° NC2017/0003283

INFORME DE BÚSQUEDA
EXAMEN DE PATENTABILIDAD

Solicitud No.		Examen de patentabilidad							
NC2017/0003283		1°		2°		3°		Revoca	X
Solicitud Internacional No.		Fecha solicitud internacional: (DD/MM/AÑO)							
PCT/US2015/050485		16 de septiembre de 2015							
Fecha de determinación estado de la técnica (DD/MM/AÑO)				Prioridad		Presentación			
6/10/2014				X					
Solicitante									
CRYPTZONE NORTH AMERICA INC.									
Reivindicaciones que no son objeto de búsqueda por:									
Art. 14	-	Art. 15	-	Art. 20	-	Art. 25 (Falta de unidad de invención)		-	

CRITERIOS DE BÚSQUEDA	
Reivindicaciones objeto de búsqueda	1 a 18
Palabras clave utilizadas	Systems, methods, protect*, network, devices, help, network, unauthorized, access, application, server, prevent, client, signature, digital, private.
Clasificaciones utilizadas para la búsqueda	CIP: H04L 29/06, H04L 12/22

DOCUMENTOS CONSIDERADOS RELEVANTES (Documentos patente, Literatura no patente (LNP): Artículos, catálogos, etc.)					
Informes de búsqueda / Bases de datos consultadas	N° de solicitud de patente / N° de patente / Autor LNP (¹)	Fecha de Publicación /Presentación (DD/MM/AAAA)	Reivindicaciones /Secuencias afectadas	Citas relevantes del estado de la técnica	Categoría del documento citado (²)
SIPI	14279002	19/12/2014	-	-	A
ISA	US2014282914	18/09/2014	1 a 8, 10 a 14 y 16 a 18	1 Pág. 1, Párr. 0002; Pág. 5, Párr. 0044, líneas 4 a 9; Pág. 9, Párr. 0071; Pág. 6, Párr. 0048, líneas 1 a 2; Párr. 0026; Pág. 6, Párr. 0048; Pág. 6, Párr. 0051, líneas 1 a 5. 2 Pág. 4, Párr. 0035, líneas 1 a 5. 3 Pág. 4, Párr. 0035, líneas 5 a 13. 4 Pág. 4, Párr. 0037, líneas 6 a 12. 5 Pág. 5, Párr. 0039, líneas 6 a 10. 6 Pág. 2, Párr. 21, líneas 12 a 15. 7 Pág. 1, Párr. 8, líneas 4 a 9. 8 Pág. 6, Párr. 48, líneas 14 a 19. 10	Y

Oficio N° 9107 de 28 de julio de 2020

Ref. Expediente N° NC2017/0003283

				Pág. 1, Párr. 8, líneas 7 a 9; Pág. 3, Párr. 0026. 11 Pág. 4, Párr. 0032. 12 Pág. 8, Párr. 67, líneas 6 a 9; Pág. 3, Párr. 29, líneas 16 a 20. 13 Págs. 6 y 7, Párr. 0052, líneas 1 a 21. 14 Párr. 0024, líneas 12 a 17. 16 Pág. 3, Párr. 0025. 17 Pág. 8, Párr. 0066, líneas 1 a 8; Pág. 5, Párr. 0044, líneas 4 a 9; Pág. 9, Párr. 0071, líneas 6 a 12; Pág. 6, Párr. 0048, líneas 1 a 2; Pág. 3, Párr. 0026, líneas 9 a 14; 18 Pág. 8, Párr. 0066, líneas 1 a 8; Pág. 5, Párr. 0044, líneas 4 a 9; Pág. 9, Párr. 0071, líneas 6 a 12; Pág. 6, Párr. 0048, líneas 1 a 2; Pág. 3, Párr. 0026, líneas 9 a 14;	
	US6381631	30/04/2022	1, 9, 17 y 18	1 Resumen, líneas 1 a 4; Col. 6, líneas 45 a 51. 9 Col. 11, líneas 15 a 23 17 Col. 4, líneas 38 a 43; Col. 6, líneas 45 a 51; Pág. 6, Párr. 0048, líneas 1 a 10; Pág. 6, Párr. 0051, líneas 1 a 5. 18 Col. 4, líneas 38 a 43; Col. 6, líneas 45 a 51; Pág. 6, Párr. 0048, líneas 1 a 10; Pág. 6, Párr. 0051, líneas 1 a 5.	Y
EPO	US2008028436 US2010205657 US2007101405 US2008092223	31/01/2008 12/08/2010 03/05/2007 17/04/2008	- - - -	- - - -	A A A A
USPTO	US7574737 US8549300 US9992185	11/08/2009 01/10/2013 05/06/2013	- - -	- - -	A A A
Patbase	US2003055962	20/03/2003	-	-	A
Orbit	EP1526472	27/04/2005	-	-	A
JPO	US2008046995 US2002026503	21/02/2008 28/02/2002	- -	- -	A A
Googlepatent	US10187426	22/01/2019	-	-	E
(¹) Cita completa literatura no patente (LNP) Apellido, A. A. (Fecha). Título del					

Oficio N° 9107 de 28 de julio de 2020

Ref. Expediente N° NC2017/0003283

artículo. Nombre de la revista. Volumen(Número), pp-pp.	
O	
Apellido, A. A. (Fecha). Título del artículo. Nombre de la revista. Recuperado de http://xxxxxxx.	
(2) Categorías de documentos citados	
“A” Documento que define el estado general de la técnica no considerado como particularmente relevante. “E” Solicitud de patente o patente anterior pero publicada en la fecha de presentación internacional o en fecha posterior. “L” Documento citado para llamar la atención sobre por ejemplo, dudas acerca de una reivindicación de prioridad o para determinar la fecha de publicación de otra cita, siempre van acompañados de una explicación, por la cual se citan. “O” Documento del tipo actas de conferencia, este tipo de documentos siempre estará acompañado por otra letra que indique la pertinencia del documento, por ejemplo, O,X, O,Y o bien O,A. “P” Documento publicado antes de la fecha de presentación internacional pero con posterioridad a la fecha de prioridad reivindicada. “T” Documento publicado en fecha posterior a la de presentación o la de prioridad de la solicitud internacional y no entra en conflicto con dicha solicitud, pero puede ser útil para la mejor comprensión del principio o teoría en que se basa la invención, o para demostrar que el razonamiento o los hechos en los que se basa dicha invención son incorrectos. “X” Documento particularmente relevante; la invención reivindicada no puede considerarse nueva o que implique una actividad inventiva por referencia al documento aisladamente considerado. “Y” Documento particularmente relevante; la invención reivindicada no puede considerarse que implique una actividad inventiva cuando el documento se asocia a otro u otros documentos de la misma naturaleza, cuya combinación resulta evidente para un experto en la materia.	
Fecha del reporte de búsqueda: 24/06/2020	
Examinador: FREDDY ALEXANDER VELANDIA VIVAS	