

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Resolución N° 25465

Ref. Expediente N° NC2017/0003283

Por la cual se deniega una Patente de Invención

EL SUPERINTENDENTE DE INDUSTRIA Y COMERCIO
en ejercicio de sus facultades legales, en especial de las conferidas en el numeral 26 del artículo 3° del Decreto 4886 de 2011, y

CONSIDERANDO:

PRIMERO: Que mediante escrito radicado en esta Superintendencia el 4 de abril de 2017, con el N° NC2017/0003283, por CRYPTZONE NORTH AMERICA INC., entró a fase nacional la solicitud de patente de invención titulada "SISTEMAS Y MÉTODOS PARA PROTEGER DISPOSITIVOS DE RED", que corresponde a la solicitud internacional PCT/US2015/050485 del 16 de septiembre de 2015.

SEGUNDO: Que la solicitud fue publicada en la Gaceta de la Propiedad Industrial N° 797 el 30 de junio de 2017, sin que se hubieran presentado oposiciones por parte de terceros.

TERCERO: Que realizado el examen de fondo mediante Oficio N° 12572, notificado 19 de octubre de 2018, se requirió al solicitante en los términos del artículo 45 de la Decisión 486 de la Comisión de la Comunidad Andina para que presentara respuesta a las observaciones de carácter técnico, relacionadas con la patentabilidad o cumplimiento de los requisitos establecidos por esta Decisión para la concesión de la patente.

CUARTO: Que el solicitante mediante escrito radicado bajo el N° NC2017/0003283 el 27 de febrero de 2019, respondió oportunamente el requerimiento formulado sin presentar nuevo capítulo reivindicatorio. Por lo tanto, se tendrá en cuenta el capítulo reivindicatorio presentado con el radicado N° NC2017/0003283 el 14 de agosto de 2018.

QUINTO: Que en virtud de lo dispuesto en el artículo 14 de la Decisión 486 expedida por la Comisión de la Comunidad Andina *"Los países miembros otorgarán patentes para las invenciones, sean de producto o de procedimiento, en todos los campos de la tecnología, siempre que sean nuevas, tengan nivel inventivo y sean susceptibles de aplicación industrial."*

SEXTO: Que en el presente caso las reivindicaciones 1 a 15 incluidas en el radicado bajo el N° NC2017/0003283 del 14 de agosto de 2018, no cumplen los requisitos indicados. Lo anterior, de acuerdo con las siguientes consideraciones:

6.1 Objeto de la invención

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



Ref. Expediente N° NC2017/0003283

permitido. Tales modalidades incluyen varios métodos, aparatos (incluyendo sistemas informáticos) que realizan tales métodos, y medios legibles por computadora que contienen instrucciones que, cuando se ejecutan pos sistemas de cómputo, provocan que los sistemas de cómputo realicen tales métodos.

6.2 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 Hethod for secure application communication between networked processors”	2014/septiembre/18
D2	US2008028436	“Generalized policy server”	2008/enero/31
D3	US6381631	“Method and apparatus for controlling client computer systems”	2002/abril/30

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 sistema de aplicación de políticas en el que la tarea de la aplicación de políticas se comparte entre dos componentes: un servidor de políticas que incluye una base de datos extensible de políticas y un ejecutor de políticas (Párr. 31).

El documento D3³ 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 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).

6.3 Novedad (Art 16 Decisión 486)

Según lo dispuesto en el artículo 16 de la Decisión 486: *“Una invención se considerará nueva cuando no está comprendida en el estado de la técnica.*

¹https://worldwide.espacenet.com/publicationDetails/biblio?CC=US&NR=2014282914A1&KC=A1&FT=D&ND=3&date=20140918&DB=&locale=en_EP

²https://worldwide.espacenet.com/publicationDetails/biblio?CC=US&NR=2008028436A1&KC=A1&FT=D&ND=3&date=20080131&DB=&locale=en_EP

³https://worldwide.espacenet.com/publicationDetails/biblio?CC=US&NR=6381631B1&KC=B1&FT=D&ND=3&date=20020430&DB=&ocale=en_EP

Resolución N° 25465

Ref. Expediente N° NC2017/0003283

El estado de la técnica comprenderá todo lo que haya sido accesible al público por una descripción escrita u oral, utilización, comercialización o cualquier otro medio antes de la fecha de presentación de la solicitud de patente o, en su caso, de la prioridad reconocida”.

En el presente caso, el método reclamado en la solicitud no es nuevo, teniendo en cuenta que la reivindicación 1 está referida a: “Un método implementado por computadora caracterizado porque comprende: (...)” (Radicado N° NC2017/0003283 del 14 de agosto de 2018).

La siguiente tabla presenta la comparación entre las características técnicas esenciales de la solicitud estudiada, mencionadas en la reivindicación 1, y las reveladas en el documento D1 que representa el estado de la técnica:

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

Características esenciales	D1
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 (Párr. 2).
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) (Párr. 44); 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 (Párr. 71).
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) (Párr. 48).
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 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 (Párr. 26).
al recibir la lista de accesos de cliente, 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); y	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) (Párr. 48).
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	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) (Párr. 51).



Ref. Expediente N° NC2017/0003283

de red en la red privada a través de la puerta de enlace (100).	
---	--

De acuerdo con la tabla anterior, las características esenciales del método de la reivindicación 1 habían sido divulgadas previamente en el documento D1, por lo tanto, la materia reivindicada no es nueva.

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. 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 está activa y sus marcas de tiempo correspondientes se pueden registrar en el paso (424) (Párr. 35).
- Reivindicación 3: 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 (Párr. 37).
- Reivindicaciones 4 y 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). 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. (Párr. 39); 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 (Párr. 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) (Párr. 48).
- Reivindicación 7: Solo los puertos permitidos seleccionados se pueden utilizar para el acceso remoto, mientras que otros puertos tienen restricciones de uso (Párr. 8); 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

Ref. Expediente N° NC2017/0003283

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 (Párr. 26).

- Reivindicación 9: Si el dispositivo invitado (104) / dispositivo local (1004) no se ha autenticado con éxito en el paso (412), entonces el proceso (400) puede estar completo y la sesión puede finalizar. Sin embargo, si el dispositivo invitado (104) / dispositivo local (1004) se autentica satisfactoriamente en el paso 412, entonces el proceso (400) puede continuar al paso (414). En la etapa (414), la función del dispositivo invitado (104) / dispositivo local (1004) puede ser determinada por el servidor de seguridad (158) (...). El servidor de seguridad (158) puede determinar la función del dispositivo invitado (104) / dispositivo local (1004) en función de las políticas y estándares de seguridad establecidos dentro del servidor de seguridad (158) (Párr. 30); 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). 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) (Párr. 32).
- Reivindicación 10: 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 (Párr. 29); 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) (Párr. 32); 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 (Párr. 67).
- Reivindicación 11: FIG. 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 FIG. 4 o el proceso (500) de la FIG. 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

Resolución N° 25465

Ref. Expediente N° NC2017/0003283

(154), (254) (y a los dispositivos remotos asociados 262) (Párr. 52); 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. 24).

- Reivindicación 13: 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 correspondientes cuando los eventos ocurrieron en una base de datos (160) de registro (Párr. 25).

Las reivindicaciones dependientes 2 a 5, 7, 9 a 11 y 13 tampoco cumplen con el requisito de novedad.

Por otro lado, el medio legible reclamado en la solicitud no es nuevo, teniendo en cuenta que la reivindicación 14 está referida a: *“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° NC2017/0003283 del 14 de agosto de 2018).

La siguiente tabla presenta la comparación entre las características técnicas esenciales de la solicitud estudiada, mencionadas en la reivindicación 14, y las reveladas en el documento D1 que representa el estado de la técnica:

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

Características esenciales	D1
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 (Párr. 66).
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) (Párr. 44); 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 (Párr. 71).
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) (Párr. 48).
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 (Párr. 26).



Resolución N° 25465

Ref. Expediente N° NC2017/0003283

al recibir la lista de accesos de cliente, verifique 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); y	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) (Párr. 48).
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) (Párr. 51).

De acuerdo con la tabla anterior, las características esenciales del dispositivo de la reivindicación 14 habían sido divulgadas previamente en el documento D1, por lo tanto, la materia reivindicada no es nueva.

Además, el sistema informático reclamado en la solicitud no es nuevo, teniendo en cuenta que la reivindicación 15 está referida a: *“Un sistema informático que implementa una puerta de enlace, el sistema informático caracterizado porque comprende: (...)”* (Radicado N° NC2017/0003283 del 14 de agosto de 2018).

La siguiente tabla presenta la comparación entre las características técnicas esenciales de la solicitud estudiada, mencionadas en la reivindicación 15, y las reveladas en el documento D1 que representa el estado de la técnica:

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

Características esenciales	D1
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 (Párr. 65).
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) (Párr. 44); 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 (Párr. 71).
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) (Párr. 48).
al autenticar el dispositivo cliente (121), reciba, de un servidor de	Si el dispositivo invitado (104) es autenticado y validado para el servidor de facilitación de conexión (120), el dispositivo invitado



Resolución N° 25465

Ref. Expediente N° NC2017/0003283

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);	(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 (Párr. 26).
al recibir la lista de accesos de cliente, verifique 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); y	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) (Párr. 48).
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) (Párr. 51).

De acuerdo con la tabla anterior, las características esenciales del sistema de la reivindicación 15 habían sido divulgadas previamente en el documento D1, por lo tanto, la materia reivindicada no es nueva.

6.4 Nivel Inventivo (Art. 18 Decisión 486)

Según lo dispuesto en el artículo 18 de la Decisión 486: *“Se considerará que una invención tiene nivel inventivo, si para una persona del oficio normalmente versada en la materia técnica correspondiente, esa invención no hubiese resultado obvia ni se hubiese derivado de manera evidente del estado de la técnica”.*

En el presente caso, el método reclamado en la solicitud no tiene nivel inventivo, teniendo en cuenta que la reivindicación 6 está referida a: *“El método de conformidad con la reivindicación 1, caracterizado porque establecer el túnel de red entre el dispositivo de cliente (...)”* (Radicado N° NC2017/0003283 del 14 de agosto de 2018).

La siguiente tabla presenta la comparación entre las características técnicas esenciales de la solicitud estudiada, mencionadas en la reivindicación 6, y las reveladas en los documentos D1 y D2 que representan el estado de la técnica:

Tabla 4. Comparación de las características técnicas esenciales, con las del estado de la técnica:

Reiv.	Características esenciales	D1	D2
1	El método de conformidad con la reivindicación 1,	Ver tabla 1.	No lo menciona.
6	Caracterizado porque establecer el túnel de red entre el dispositivo de cliente (121) y el dispositivo de red (141) en la red privada incluye establecer una red privada virtual.	No lo menciona.	La siguiente descripción detallada proporcionará primero una descripción general de los filtros de acceso que son fácilmente escalables, de cómo se usan para controlar el acceso en intranets y de cómo se pueden usar para construir redes privadas virtuales (Párr. 76); Fig. 2 muestra una red privada virtual (VPN) (201) en la que el acceso a los datos está controlado por filtros de acceso

Resolución N° 25465

Ref. Expediente N° NC2017/0003283

			que están diseñados para evitar los problemas planteados por los filtros de acceso múltiple (Párr. 77).
--	--	--	---

El documento D1 se considera el estado de la técnica más cercano a la invención definida en la reivindicación 6 porque divulga un sistema y un método para la comunicación segura de aplicaciones entre procesadores en red, que incluyen dispositivos basados en procesadores con capacidad de interconexión en red (Párr. 2).

La diferencia entre la invención definida en la reivindicación 6 y el método divulgado en D1 consiste en que la invención incluye establecer una red privada virtual.

El efecto que se logra por el hecho de que la invención incluya establecer una red privada virtual es lograr la comunicación y el control seguro de una red privada puesta sobre una red pública no controlada como internet.

Por lo tanto, el problema técnico objetivo que pretende resolver esta invención se puede formular así: ¿cómo modificar el método conocido en D1 para lograr la comunicación y el control seguro de una red privada puesta sobre una red pública no controlada como internet?

Sin embargo, lo que permite lograr la comunicación y el control seguro de una red privada puesta sobre una red pública no controlada como internet ya está divulgado en el documento D2 que se refiere a que la VPN (201) está compuesta por cuatro redes internas (103) que están conectadas entre sí por Internet (121). También conectado a la VPN (201) a través de Internet (121) se encuentra un itinerante (217), es decir, un sistema informático que está siendo utilizado por una persona que puede acceder a los datos en la intranet (201), pero está conectado a las redes internas únicamente por Internet (121) (Párr. 77).

En consecuencia, la persona del oficio normalmente versada en la materia incluiría establecer una red privada virtual como en el documento D2 en el método divulgado en el documento D1 para llegar así al objeto de la reivindicación 6 de la solicitud. Por lo cual se considera obvia.

Por otro lado, el método reclamado en la solicitud no tiene nivel inventivo, teniendo en cuenta que la reivindicación 8 está referida a: *“El método de conformidad con la reivindicación 1, caracterizado porque autenticar el dispositivo de cliente (121) incluye verificar una firma digital (...)”* (Radicado N° NC2017/0003283 del 14 de agosto de 2018).

La siguiente tabla presenta la comparación entre las características técnicas esenciales de la solicitud estudiada, mencionadas en la reivindicación 8, y las reveladas en los documentos D1 y D2 que representan el estado de la técnica:

Tabla 5. Comparación de las características técnicas esenciales, con las del estado de la técnica:

Reiv.	Características esenciales	D1	D2
1	El método de conformidad con la reivindicación 1,	Ver tabla 1.	No lo menciona.
8	Caracterizado porque autenticar el dispositivo de cliente (121) incluye verificar una firma digital en la lista de accesos de cliente mediante una clave de firma compartida entre la	No lo menciona.	Los filtros de acceso (203) están diseñados de tal manera que la decisión de otorgar a un usuario acceso a un recurso de información solo se necesita en uno de los filtros de acceso (203). La clave de esta característica de los filtros de acceso (203) es su capacidad para autenticarse entre sí. SKIP se usa para hacer esto. Cada filtro de acceso (203) tiene un certificado X (509) que vincula las claves del filtro de acceso (203) al nombre del filtro de acceso y está



Resolución N° 25465

Ref. Expediente N° NC2017/0003283

	puerta de enlace (100) y el servidor de autenticación (160).		firmado por la Autoridad de certificación para la VPN. Cada filtro de acceso (203) tiene los nombres y direcciones IP de todos los otros filtros de acceso en la VPN (201) en la base de datos (301), y al llegar una sesión cifrada usando SKIP, cada filtro de acceso usa el nombre del sujeto de los certificados como se describió anteriormente en la discusión de SKIP para determinar si el tráfico de red cifrado SKIP es de otro filtro de acceso (203) en VPN (201) (Párr. 148).
--	--	--	--

El documento D1 se considera el estado de la técnica más cercano a la invención definida en la reivindicación 8 porque divulga un sistema y un método para la comunicación segura de aplicaciones entre procesadores en red, que incluyen dispositivos basados en procesadores con capacidad de interconexión en red (Párr. 2).

La diferencia entre la invención definida en la reivindicación 8 y el método divulgado en D1 consiste en que la invención incluye verificar una firma digital en la lista de accesos de cliente mediante una clave de firma compartida entre la puerta de enlace y el servidor de autenticación.

El efecto que se logra por el hecho de que la invención incluya verificar una firma digital en la lista de accesos de cliente mediante 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, lo que permite identificar los dispositivos de los clientes evitando suplantaciones ya está divulgado en el documento D2 que se refiere a que la información de identificación identifica a sus usuarios por medio de un conjunto de técnicas de identificación extensibles. En la actualidad, estas técnicas de identificación incluyen certificados X (509), identificación de dominio de Windows NT, tokens de autenticación y dirección IP / nombre de dominio. El tipo de técnica de identificación utilizada para identificar a un usuario determina el nivel de confianza de la identificación (Párr. 106).

En consecuencia, la persona del oficio normalmente versada en la materia incluiría verificar una firma digital en la lista de accesos de cliente mediante una clave de firma compartida entre la puerta de enlace y el servidor de autenticación como en el documento D2 en el método divulgado en el documento D1 para llegar así al objeto de la reivindicación 8 de la solicitud. Por lo cual se considera obvia.

Por último, el método reclamado en la solicitud no tiene nivel inventivo, teniendo en cuenta que la reivindicación 12 está referida a: *“El método de conformidad con la reivindicación 15, caracterizado porque los requerimientos de autenticación mejorados incluyen un requerimiento de que un usuario (...)”* (Radicado N° NC2017/0003283 del 14 de agosto de 2018).

La siguiente tabla presenta la comparación entre las características técnicas esenciales de la solicitud estudiada, mencionadas en la reivindicación 12, y las reveladas en los documentos D1 y D3 que representan el estado de la técnica:

Tabla 6. Comparación de las características técnicas esenciales, con las del estado de la técnica:

Reiv.	Características esenciales	D1	D3
1	El método de conformidad con la reivindicación 11,	Ver tabla 1.	No lo menciona.



Ref. Expediente N° NC2017/0003283

12	Caracterizado porque los requerimientos de autenticación mejorados incluyen un requerimiento de que un usuario del dispositivo de cliente proporcione una credencial de autenticación seleccionada del grupo que consiste de: un escaneo de huella digital; un escaneo del iris; y una clave generada por un generador de claves externo.	No lo menciona.	El usuario se comunica con el sistema (200) a través del sistema operativo (210) tal como Windows (98), a través de la entrada / salida (206), que puede acoplarse a dispositivos de entrada/salida convencionales tales como un teclado/monitor/mouse convencional, y también puede incluir entrada óptica o de audio o dispositivos de entrada/salida para registrar una huella digital, escaneo de iris, escaneo de retina, huella de voz, geometría de la mano, geometría de dedo, firma, datos de patrón de cara u otros datos biométricos (Col 4, Lin 64 – Col 5, Lin 4).
----	---	-----------------	---

El documento D1 se considera el estado de la técnica más cercano a la invención definida en la reivindicación 12 porque divulga un sistema y un método para la comunicación segura de aplicaciones entre procesadores en red, que incluyen dispositivos basados en procesadores con capacidad de interconexión en red (Párr. 2).

La diferencia entre la invención definida en la reivindicación 12 y el método divulgado en D1 consiste en que la invención incluye que un requerimiento de un usuario del dispositivo de cliente proporcione una credencial de autenticación seleccionada del grupo que consiste de: un escaneo de huella digital; un escaneo del iris; y una clave generada por un generador de claves externo.

El efecto que se logra por el hecho de que la invención incluya que un requerimiento de un usuario del dispositivo de cliente proporcione una credencial de autenticación seleccionada del grupo que consiste de: un escaneo de huella digital; un escaneo del iris; y una clave generada por un generador de claves externo es mejorar la autenticación de usuario 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 mejorar la autenticación de usuario evitando suplantaciones?

Sin embargo, lo que permite mejorar la autenticación de usuario evitando suplantaciones ya está divulgado en el documento D3 que se refiere a que el usuario puede identificarse usando un nombre de usuario y contraseña convencionales, un nombre de usuario solo o simplemente puede proporcionar una forma de identificación biométrica física o de otra índole, como reconocimiento de huellas digitales, reconocimiento de voz, escaneo del iris, exploración de la retina, geometría de la mano o del dedo reconocimiento, reconocimiento facial u otra identificación física o biométrica utilizando el escáner óptico o el micrófono o el teclado y el mouse acoplados a la entrada (206) (...) El administrador de inicio de sesión (232) recibe esta información de identificación a través del sistema operativo (210) y envía la información a la red remota a través del administrador de conexión (220) para la autenticación o autentica la información localmente usando el autenticador (230) (Col 5, Lin 9 – 26).

En consecuencia, la persona del oficio normalmente versada en la materia incluiría que un requerimiento de un usuario del dispositivo de cliente proporcione una credencial de autenticación seleccionada del grupo que consiste de: un escaneo de huella digital; un escaneo del iris; y una clave generada por un generador de claves externo como en el documento D3 en el método divulgado en el documento D1 para llegar así al objeto de la reivindicación 12 de la solicitud. Por lo cual se considera obvia.

6.5 Respuesta a los argumentos del solicitante

Argumentos respecto al análisis de Novedad

Ref. Expediente N° NC2017/0003283

El solicitante argumenta que: *“El examinador había argumentado que la reivindicación 1 carecía de novedad en cada uno de los documentos D1 a D3. Sin embargo, estos comentarios no dieron el debido peso a los puntos significativos de diferencia entre las reivindicaciones presentes y las divulgaciones de esos documentos”* a lo que este Despacho aclara que D1 afecta la novedad de la presente invención en sus reivindicaciones independientes y, D2 y D3 afectan el nivel Inventivo de las reivindicaciones dependientes no afectadas por novedad con el documento D1; por lo que dicho argumento no es procedente.

Por otro lado, el solicitante argumenta sobre las objeciones por falta de novedad que *“(…) D1 no revela varios de los elementos de la reivindicación 1. Por ejemplo, la reivindicación 1 requiere la implementación de una ‘puerta de enlace a una red privada’ entre un ‘dispositivo cliente y un dispositivo de red en la red privada’. Estos dispositivos, según se afirma, forman parte de la red privada.*

*Por el contrario, D1 se limita a divulgar un dispositivo cliente **que no es parte de una red privada** que intenta conectarse con un dispositivo host 254. Específicamente, el párrafo [0044] de D1, por ejemplo, revela haber recibido ‘una solicitud de conexión... desde un dispositivo cliente 204... para establecer... con el dispositivo host 254’”* esta Oficina aclara que el párrafo 71 presente en el documento D1 divulga que el dispositivo invitado y el host pueden estar en comunicación por medio de una red de área local, la cual es una red privada. Por lo tanto el argumento no es procedente.

También argumenta que: *“(…) La determinación del acceso en función de las credenciales de un usuario del dispositivo cliente ejemplifica que D1 no revela nada remotamente cercano a un dispositivo cliente que tenga acceso a un dispositivo de red dentro de una red privada, como lo exige la reivindicación independiente 1”* a lo que se aclara que igual como se menciona en el párrafo anterior, el documento D1 divulga que el dispositivo invitado y el host pueden estar en comunicación por medio de una red de área local, la cual es una red privada y el host es un dispositivo de red; también el párrafo 48 presente en D1 se divulga la verificación del dispositivo en la lista de dispositivos permitidos dado que si se autentican las credenciales de inicio de sesión del dispositivo es porque este está dentro de la lista de dispositivos; y el párrafo 51 también presente en D1 divulga el establecimiento del túnel de comunicaciones, lo que debe suceder después de la verificación para que pueda existir comunicación entre dichos dispositivos, por lo cual este argumento tampoco es admisible.

Respecto a D2 y D3 el solicitante argumenta que ninguno de los dos documentos revelan la característica técnica de *“verificar... el dispositivo de red en la red privada es parte de la lista de dispositivos de red con los que el dispositivo cliente puede comunicarse”* a lo que se reitera que dichos documentos D2 y D3 son usados para afectar las características por las cuales difiere la invención del documento D1 mencionadas en las reivindicaciones dependientes 6, 8 y 12, y no la característica que menciona el solicitante dado que ya el documento D1 la está divulgando como ya se mencionó. Por lo tanto este argumento tampoco es válido.

En conclusión, teniendo en cuenta que los argumentos del solicitante no desvirtúan de manera alguna las objeciones a la patentabilidad ya sustentadas, el Superintendente de Industria y Comercio,

RESUELVE

ARTÍCULO PRIMERO: Denegar la patente de invención a la creación titulada “SISTEMAS Y MÉTODOS PARA PROTEGER DISPOSITIVOS DE RED”.

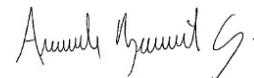
Página 12 de 13

Ref. Expediente N° NC2017/0003283

ARTÍCULO SEGUNDO: Notificar el contenido de la presente resolución a CRYPTZONE NORTH AMERICA INC., advirtiéndole que contra ella procede el recurso de reposición, ante el Superintendente de Industria y Comercio, el cual podrá ser interpuesto en el momento de la notificación o dentro de los diez (10) días hábiles siguientes a ella.

NOTIFÍQUESE Y CÚMPLASE

Dada en Bogotá D.C., el 2 de julio de 2019



ANDRÉS BARRETO GONZÁLEZ
SUPERINTENDENTE DE INDUSTRIA Y COMERCIO

Firmado digitalmente
por: ANDRÉS
BERNARDO BARRETO
GONZÁLEZ
Fecha: 2019.07.05
17:06:11 COT
Razón: Validez jurídica.
Ubicación: Bogotá,
Colombia.

