

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Oficio N° 2073 de 11 de febrero de 2020

Ref. Expediente N° NC2018/0009316

Señor(a)
CRYPTZONE NORTH AMERICA INC.

TÍTULO DE LA SOLICITUD: “MÉTODO, SISTEMA Y MEDIO DE ALMACENAMIENTO LEGIBLE POR COMPUTADOR PARA PROTECCIÓN DE DISPOSITIVOS DE RED MEDIANTE UN CORTAFUEGOS”

NÚMERO DE SOLICITUD INTERNACIONAL: PCT/US2016/036053

FECHA DE PRESENTACIÓN INTERNACIONAL: 6 de junio de 2016.

PRIORIDAD(ES): US, 62/292,702, 08 de febrero de 2016.

US, 15/053,422, 25 de febrero de 2016.

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 24 de octubre de 2019, bajo el número NC2018/0009316, 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 20 del radicado N° NC2018/0009316 del 24 de octubre de 2019.

El problema planteado en esta solicitud consiste en la necesidad de introducir medidas de protección de red en redes privadas que incluyen un servidor de túnel como un servidor VPN permitiendo o bloqueado el tráfico que fluye a través de estas.

Para resolver este problema técnico, la solicitud en estudio proporciona sistemas y métodos para escalamiento y gestión de una puerta de enlace. En una modalidad, un método incluye: en respuesta a una petición de un dispositivo del cliente, establecer, por un sistema de computadora que implementa una puerta de enlace a una red privada, un túnel de red entre el dispositivo del cliente y la puerta de enlace; y después establecer el túnel de red, partiendo de un servicio de cortafuegos separado con un conjunto separado de reglas del cortafuegos sobre el sistema de computadora para selectivamente bloquear y permitir el tráfico de red entre el dispositivo del cliente y uno o más dispositivos de red en la red privada.

3. De la solicitud de patente



Oficio N° 2073 de 11 de febrero de 2020

Ref. Expediente N° NC2018/0009316

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 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.

De acuerdo con la modificación presentada por el solicitante en el escrito radicado bajo el N° NC2018/0009316 el 24 de octubre de 2019 y teniendo en cuenta el objeto de la solicitud, se acepta el título siguiente: “MÉTODO, SISTEMA Y MEDIO DE ALMACENAMIENTO LEGIBLE POR COMPUTADOR PARA PROTECCIÓN DE DISPOSITIVOS DE RED MEDIANTE UN CORTAFUEGOS”.

4. Determinación del Estado de la Técnica

La fecha para determinar el estado de la técnica es el 8 de febrero de 2016 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	US20150293756	“Software Deployment and Control Method and System”	15 de octubre de 2015
D2	US20040225895	“Method and apparatus for providing adaptive VPN to enable different security levels in virtual private networks (VPNs)”	11 de noviembre de 2004

El documento D1¹ divulga un método para monitorear un aparato informático por medio de un sistema de gestión a través de una red, comprendiendo el método: establecer una conexión entre el aparato informático y el sistema de gestión a través de la red, estando el aparato informático ubicado en una primera ubicación y la gerencia el sistema está ubicado en una segunda ubicación remota desde la primera ubicación; instalar un controlador y crear en el aparato de la computadora al menos una máquina virtual, la o cada máquina virtual que está siendo monitoreada por el controlador; monitorear una o más características del aparato de computadora y / o la o cada máquina virtual y generar resultados de monitoreo basados en las características; e informar los resultados del monitoreo al sistema de gestión a través de la red (...) (Resumen)

El documento D2² divulga un método y aparato para proporcionar al menos dos túneles VPN de red privada virtual desde un dispositivo cliente en una red VPN que tiene una puerta de enlace empresarial y una puerta de enlace VPN de red. El método y el aparato incluyen un dispositivo cliente que tiene un módulo de intercambio de claves de Internet (IKE) para establecer al menos dos túneles utilizando un protocolo IKE en el que un primer túnel es un túnel VPN de extremo a extremo hacia la puerta de enlace de la empresa, y un segundo túnel es un túnel basado en la red a la red VPN gateway. Una interfaz de controlador de red IPsec interactúa con el módulo IKE, que incluye una base de datos de autenticación de seguridad (SADB) que almacena las políticas de seguridad empresarial descargadas, respectivamente, para cada uno de los al menos dos túneles (...) (Resumen).

¹<https://patents.google.com/patent/US20150293756A1/en?q=US2015293756>

²<https://patents.google.com/patent/US20040225895A1/en?q=US2004225895>

Oficio N° 2073 de 11 de febrero de 2020

Ref. Expediente N° NC2018/0009316

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

5.1. Novedad (Art 16 Decisión 486)

La reivindicación 1 consiste en: “*Un método implementado en computadora, caracterizado porque comprende: (...)*” (Radicado N° NC2018/0009316 del 24 de octubre de 2019).

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

Características esenciales	D1	D2
En respuesta a una petición de un dispositivo del cliente, establecer, por un primer sistema informático que implementa una primera puerta de enlace a una red privada, un primer túnel de red entre el dispositivo del cliente y la primera puerta de enlace, en donde la red privada comprende uno o más dispositivos de red.	Un método y un sistema para establecer una conexión entre un aparato informático y un sistema de gestión a través de una red, (...) que comprende establecer un túnel entre un nodo asociado con el aparato informático y un nodo maestro asociado con el sistema de gestión (...) (Párr. 0017). El maestro de túneles (71), (...) da instrucciones a la respectiva puerta de enlace en cada uno de los dos sitios A, B para establecer una conexión directa entre ellos (...) (Párr. 0072).	(...) El método y el aparato incluyen un dispositivo cliente que tiene un módulo de intercambio de claves de Internet (IKE) para establecer al menos dos túneles utilizando un protocolo IKE en el que un primer túnel es un túnel VPN de extremo a extremo a la puerta de enlace VPN de la empresa, y un segundo túnel es un túnel basado en la red a la red VPN gateway (Párr. 0007).
Recibir, por el primer sistema informático, desde el dispositivo del cliente, una lista de acceso del cliente que indica las de los dispositivos de red en la red privada que pueden comunicarse con el dispositivo del cliente.	(...) Esta segunda máquina virtual (102) tiene la responsabilidad de proteger el tráfico de red del escritorio y puede ser controlada por un administrador del sistema central. Esto permite que un administrador del sistema central defina una política de cortafuegos por escritorio, que la misma computadora implemente esa política y que confíe en que la política no puede ser interferida (...) (Párr. 0081).	(...) Este controlador incluye una base de datos de autenticación de seguridad (SADB) que almacena las políticas de seguridad empresarial descargadas respectivamente para cada uno de los al menos dos túneles. (...) Esta información incluye las direcciones IP de los puntos finales de al menos dos túneles en las respectivas puertas de enlace VPN y políticas que especifican las direcciones IP de los hosts detrás de los túneles, así como los puertos TCP de destino en estos hosts para los cuales este túnel debe usarse para transportar tráfico (...) (Párr. 0008).
Iniciar, para el primer túnel de red, un servicio de cortafuegos separado con un conjunto separado de reglas de cortafuegos en el primer sistema informático para bloquear selectivamente y permitir el tráfico de red entre el dispositivo del cliente y el uno o más dispositivos de red en la red privada, en donde cada una de las reglas del cortafuegos se derivan de la lista de acceso del cliente.	(...) Esta política de firewall podría usarse para restringir el acceso de los usuarios a ciertos servicios en lugar de darles un amplio acceso a la red corporativa. También se puede usar para monitorear el tráfico de red hacia y desde el escritorio en busca de patrones de tráfico inusuales, como una infección por gusanos / virus o la penetración de la red por parte de terceros (...) (Párr. 0081).	(...) La red empresarial (120) comprende una puerta de enlace / firewall VPN empresarial (en adelante, "puerta de enlace VPN"), que sirve como punto final del lado del servidor para el túnel VPN (...) (Párr. 0025). (...) El Firewall Engine (254) aplica la política de firewall configurada. El módulo de proceso IKE (224) descarga la política de firewall desde el SMS (126) durante la negociación de IKE (...) (Párr. 0047). Un noveno servicio de valor agregado proporciona bloqueo / filtrado de URL. Una empresa normalmente restringe el acceso a algunos sitios web para sus usuarios (...) (Párr. 0103).

Oficio N° 2073 de 11 de febrero de 2020

Ref. Expediente N° NC2018/0009316

De acuerdo con la tabla anterior, las características esenciales del método de la reivindicación 1 habían sido divulgadas previamente en los documentos D1 y D2, por lo tanto, la materia reivindicada no es nueva.

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

- ❑ Reivindicación 2: (...) Esto le permite a un administrador del sistema central definir una política de firewall por escritorio, tener esa política implementada por el propio equipo y tener la confianza de que la política no puede ser interferida. (...) También se puede usar para monitorear el tráfico de la red hacia y desde el escritorio en busca de patrones de tráfico inusuales, como una infección de gusanos / virus o una penetración de la red por parte de terceros (...) (Párr. 0081). (...) La supervisión puede involucrar a un servidor centralizado que regularmente envía solicitudes de determinación de estado a máquinas virtuales en dispositivos para obtener información de estado de los mismos (...) (Párr. 0055).
- ❑ Reivindicación 3: (...) La actividad de monitoreo se delega ventajosamente a los dispositivos de procesamiento de datos (16,17) que tienen una buena conectividad con las máquinas virtuales (32,33,34,35). De acuerdo con las realizaciones de la presente invención, el agente del dispositivo puede monitorear los estados de las máquinas virtuales. El agente de dispositivo de un dispositivo de procesamiento de datos con regularidad, por ejemplo, cada minuto, solicita información relacionada con el estado de cada máquina virtual de la que es responsable, e incorpora la información respectiva en un paquete. El agente del dispositivo luego envía la información agregada dentro de un solo paquete al servidor de monitoreo central (...) (Párr. 0056).
- ❑ Reivindicación 4: (...) El agente de dispositivo de un dispositivo de procesamiento de datos con regularidad, por ejemplo, cada minuto, solicita información relacionada con el estado de cada máquina virtual de la que es responsable, e incorpora la información respectiva en un paquete (...) (Párr. 0056). (...) Si no ha cambiado ningún estado dentro de un intervalo de monitoreo, entonces el agente del dispositivo (16) envía una notificación explícita que indica que no se ha producido ningún cambio para que el servidor de monitoreo central (31) sepa que todavía está en contacto con el dispositivo (16) (Párr. 0058).
- ❑ Reivindicaciones 7 y 8: Todas o parte de las operaciones descritas anteriormente pueden llevarse a cabo en virtud de un programa de computadora que incluye las instrucciones de código apropiadas. Este programa se puede cargar y ejecutar en medios informáticos de un dispositivo de procesamiento de datos, p. Ej. una caja independiente, o una pluralidad de tales dispositivos (Párr. 0101). Es posible enrutar el tráfico de red desde la interfaz de la red física (96) a través de máquinas virtuales separadas (102) antes de pasar a la interfaz de la red virtual (104). (...) Esto le permite a un administrador del sistema central definir una política de firewall por escritorio, tener esa política implementada por el propio equipo y tener la confianza de que la política no puede ser interferida. Esta política de cortafuegos podría utilizarse para restringir el acceso de los usuarios a ciertos servicios en lugar de darles un amplio acceso a la red corporativa (...) (Párr. 0081).
- ❑ Reivindicación 9: (...) Comprende establecer un túnel entre un nodo asociado con el aparato informático y un nodo maestro asociado con el sistema de gestión, en el que la conexión comprende establecer una conexión segura entre el aparato informático y



Oficio N° 2073 de 11 de febrero de 2020

Ref. Expediente N° NC2018/0009316

el sistema de gestión a través del túnel y la conexión segura se establece entre el nodo asociado con el aparato informático y el nodo maestro asociado con el sistema de gestión mediante una conexión de red privada virtual, en la que la conexión virtual privada de red protege los datos con cifrado y / o autenticación y / o protección de integridad (Párr. 0017). (...) El flujo de datos entre los medios y la máquina virtual de escritorio se puede procesar, cifrando los datos a medida que se escriben en los medios y desenscriptándolos a medida que se leen desde los medios (...) (Párr. 0085).

- ❑ Reivindicación 10: (...) El flujo de datos entre los medios y la máquina virtual de escritorio se puede procesar, cifrando los datos a medida que se escriben en los medios y desenscriptándolos a medida que se leen desde los medios (...) (Párr. 0085). (...) Es posible automatizar el proceso de integración de dos aplicaciones que se ejecutan en máquinas virtuales separadas dentro del sistema, acelerando el proceso, haciéndolo más confiable y simplificándolo (...) (Párr. 0074).

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

- ❑ Reivindicación 2: Reivindicación 2: (...) Normalmente, una empresa permitirá que los paquetes TCP salgan de la empresa, pero permitirá que los paquetes TCP ingresen a la empresa solo si la conexión TCP correspondiente se inició desde dentro de la empresa. Este es un ejemplo de una funcionalidad de firewall de estado y requiere que el estado de TCP se mantenga por sesión. Dado que el encabezado TCP (y el encabezado IP) en los paquetes son visibles en el IPSS (104), el mantenimiento del estado TCP es posible en el IPSS (104) y, por lo tanto, el IPSS (104) puede proporcionar una funcionalidad de firewall de estado completo (Párr. 0099).

- ❑ Reivindicación 5: Además, se observa que cuando el dispositivo cliente (130) intenta establecer un túnel de red (158), pero falla, los paquetes que deberían haberse reenviado a través del túnel de red (158) se reenvían a través del túnel de extremo a extremo (156). Para Para lograr esto, la política en el cliente SADB (260) se modifica adecuadamente. Además, el dispositivo (130) del cliente envía información al SMS (126), de modo que el SMS (126) puede cambiar el firewall y otras políticas en el Enterprise VPN Gateway (122) para permitir que se acepten estos paquetes en este Gateway. En consecuencia, la presente invención proporciona tolerancia a fallos en el caso de que no se pueda establecer un túnel de red (158) (Párr. 0075).

- ❑ Reivindicación 6: Es decir, IKE se utiliza para establecer el túnel (156) de la empresa y el túnel (158) de la red. Las políticas para los dos túneles se descargan desde la puerta de enlace (122) de la empresa y se rellenan en la base de datos (260) de SA del dispositivo (130) del cliente (Párr. 0076). Además, se observa que cuando el dispositivo cliente (130) intenta establecer un túnel de red (158), pero falla, los paquetes que deberían haberse reenviado a través del túnel de red (158) se reenvían a través del túnel de extremo a extremo (156). Para Para lograr esto, la política en el cliente SADB (260) se modifica adecuadamente. Además, el dispositivo (130) del cliente envía información al SMS (126), de modo que el SMS (126) puede cambiar el firewall y otras políticas en el Enterprise VPN Gateway (122) para permitir que se acepten estos paquetes en este Gateway. En consecuencia, la presente invención proporciona tolerancia a fallos en el caso de que no se pueda establecer un túnel de red (158) (Párr. 0075).

- ❑ Reivindicación 7 y 8: (...) Como tal, se contempla que algunos de los pasos del proceso discutidos en este documento como procesos de software pueden implementarse



Oficio N° 2073 de 11 de febrero de 2020

Ref. Expediente N° NC2018/0009316

- dentro del hardware, por ejemplo, como un circuito que coopera con el procesador (202) para realizar varios pasos (...) (Párr. 0034). (...) La red empresarial (120) comprende una puerta de enlace / firewall VPN empresarial (en adelante, "puerta de enlace VPN"), que sirve como punto final del lado del servidor para el túnel VPN (...) (Párr. 0025).
- 7 Reivindicación 9: El método de la reivindicación (13), en el que en un caso en el que dicha información de encabezado de paquete coincide con dichos valores de SADB, dicho método comprende además: recuperar la dirección IP de destino del túnel y una clave de cifrado de dicha SADB; cifrar dicho paquete; adjuntando un encabezado IPsec; y realizar el procesamiento de IP convencional (Reivindicación 15). El método de la reivindicación 11, en el que para un paquete recibido a través de una conexión de Internet en dicho dispositivo cliente, dicho método comprende además: consultar a dicha SADB por una clave de descifrado; descifrar dicho paquete recibido; y realizar el procesamiento de IP convencional (Reivindicación 18).

Las reivindicaciones dependientes 2 a 10 tampoco cumplen con el requisito de novedad.

La reivindicación 11 consiste en: *“Un sistema, caracterizado porque comprende: (...)”* (Radicado N° NC2018/0009316 del 24 de octubre de 2019).

Tabla 2. Comparación de las características técnicas esenciales, con las del estado de la técnica		
Características esenciales	D1	D2
Al menos un núcleo del procesador, cada núcleo configurado para ejecutar un proceso.	Todas o parte de las operaciones descritas anteriormente pueden llevarse a cabo en virtud de un programa de computadora que incluye las instrucciones de código apropiadas. Este programa se puede cargar y ejecutar en medios informáticos de un dispositivo de procesamiento de datos, p. Ej. una caja independiente, o una pluralidad de tales dispositivos (Párr. 0101).	(...) Como tal, se contempla que algunos de los pasos del proceso discutidos en este documento como procesos de software pueden implementarse dentro del hardware, por ejemplo, como un circuito que coopera con el procesador (202) para realizar varios pasos (...) (Párr. 0034).
Instrucciones almacenadas en memoria configuradas para indicar al, al menos un núcleo del procesador a:	(...) Comprendiendo el producto de programa informático un medio de almacenamiento legible por ordenador que tiene un código de programa legible por ordenador incorporado (...) (Párr. 0015).	Específicamente, el dispositivo cliente (130) comprende un procesador (202), así como una memoria (208) para almacenar diversos programas de control. El procesador (202) coopera con los circuitos de soporte convencionales (204), (...) así como los circuitos que ayudan a ejecutar las rutinas de software almacenadas en la memoria (208) (...) (Párr. 0034).
En respuesta a una petición de un dispositivo del cliente, establecer un túnel de red entre el dispositivo del cliente y una puerta de enlace a una red privada, en donde la red privada comprende uno o más dispositivos de red.	Un método y un sistema para establecer una conexión entre un aparato informático y un sistema de gestión a través de una red, (...) que comprende establecer un túnel entre un nodo asociado con el aparato informático y un nodo maestro asociado con el sistema de gestión (...) (Párr. 0017). El maestro de túneles (71), (...) da instrucciones a la respectiva puerta de enlace en cada uno de los dos sitios A, B para establecer una	(...) El método y el aparato incluyen un dispositivo cliente que tiene un módulo de intercambio de claves de Internet (IKE) para establecer al menos dos túneles utilizando un protocolo IKE en el que un primer túnel es un túnel VPN de extremo a extremo a la puerta de enlace VPN de la empresa, y un segundo túnel es un túnel basado en la red a la red VPN gateway (Párr. 0007).

Oficio N° 2073 de 11 de febrero de 2020

Ref. Expediente N° NC2018/0009316

	conexión directa entre ellos (...) (Párr. 0072).	
Recibir, del dispositivo del cliente, una lista de acceso del cliente que indica las de los dispositivos de red en la red privada que pueden comunicarse con el dispositivo del cliente.	(...) Esta segunda máquina virtual (102) tiene la responsabilidad de proteger el tráfico de red del escritorio y puede ser controlada por un administrador del sistema central. Esto permite que un administrador del sistema central defina una política de cortafuegos por escritorio, que la misma computadora implemente esa política y que confíe en que la política no puede ser interferida (...) (Párr. 0081).	(...) Este controlador incluye una base de datos de autenticación de seguridad (SADB) que almacena las políticas de seguridad empresarial descargadas respectivamente para cada uno de los al menos dos túneles. (...) Esta información incluye las direcciones IP de los puntos finales de al menos dos túneles en las respectivas puertas de enlace VPN y políticas que especifican las direcciones IP de los hosts detrás de los túneles, así como los puertos TCP de destino en estos hosts para los cuales este túnel debe usarse para transportar tráfico (...) (Párr. 0008).
Iniciar, para el túnel de red, un servicio de cortafuegos separado con un conjunto separado de reglas de cortafuegos para bloquear selectivamente y permitir el tráfico de red entre el dispositivo del cliente y el uno o más dispositivos de red en la red privada, en donde cada una de las reglas del cortafuegos se derivan de la lista de acceso del cliente.	(...) Esta política de firewall podría usarse para restringir el acceso de los usuarios a ciertos servicios en lugar de darles un amplio acceso a la red corporativa. También se puede usar para monitorear el tráfico de red hacia y desde el escritorio en busca de patrones de tráfico inusuales, como una infección por gusanos / virus o la penetración de la red por parte de terceros (...) (Párr. 0081).	(...) La red empresarial (120) comprende una puerta de enlace / firewall VPN empresarial (en adelante, "puerta de enlace VPN"), que sirve como punto final del lado del servidor para el túnel VPN (...) (Párr. 0025). (...) El Firewall Engine (254) aplica la política de firewall configurada. El módulo de proceso IKE (224) descarga la política de firewall desde el SMS (126) durante la negociación de IKE (...) (Párr. 0047). Un noveno servicio de valor agregado proporciona bloqueo / filtrado de URL. Una empresa normalmente restringe el acceso a algunos sitios web para sus usuarios (...) (Párr. 0103).

De acuerdo con la tabla anterior, las características esenciales del sistema de la reivindicación 11 habían sido divulgadas previamente en los documentos D1 y D2, por lo tanto, la materia reivindicada no es nueva.

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

Reivindicaciones 12 a 14: Todas o parte de las operaciones descritas anteriormente pueden llevarse a cabo en virtud de un programa de computadora que incluye las instrucciones de código apropiadas. Este programa se puede cargar y ejecutar en medios informáticos de un dispositivo de procesamiento de datos, p. Ej. una caja independiente, o una pluralidad de tales dispositivos (Párr. 0101). Es posible enrutar el tráfico de red desde la interfaz de la red física (96) a través de máquinas virtuales separadas (102) antes de pasar a la interfaz de la red virtual (104). (...) Esto le permite a un administrador del sistema central definir una política de firewall por escritorio, tener esa política implementada por el propio equipo y tener la confianza de que la política no puede ser interferida. Esta política de cortafuegos podría utilizarse para restringir el acceso de los usuarios a ciertos servicios en lugar de darles un amplio acceso a la red corporativa (...) (Párr. 0081).

Oficio N° 2073 de 11 de febrero de 2020

Ref. Expediente N° NC2018/0009316

Reivindicación 15: (...) Esto le permite a un administrador del sistema central definir una política de firewall por escritorio, tener esa política implementada por el propio equipo y tener la confianza de que la política no puede ser interferida. Esta política de cortafuegos podría utilizarse para restringir el acceso de los usuarios a ciertos servicios en lugar de darles un amplio acceso a la red corporativa (...) (Párr. 0081).

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

Reivindicaciones 12 a 14: (...) Como tal, se contempla que algunos de los pasos del proceso discutidos en este documento como procesos de software pueden implementarse dentro del hardware, por ejemplo, como un circuito que coopera con el procesador (202) para realizar varios pasos (...) (Párr. 0034). (...) La red empresarial (120) comprende una puerta de enlace / firewall VPN empresarial (en adelante, "puerta de enlace VPN"), que sirve como punto final del lado del servidor para el túnel VPN (...) (Párr. 0025).

Reivindicación 15: La Fig. 4 muestra un diagrama de flujo para descargar las políticas de VPN adaptativas de la presente invención. La FIG. 4 es la misma que se muestra en la FIG. 3, excepto que se proporcionan direcciones IP físicas ejemplares de los puntos finales, así como una tabla (400) que ilustra las reglas de políticas almacenadas en la memoria (no se muestra) en el servidor AAA (106) (...) (Párr. 0055).

Las reivindicaciones dependientes 12 a 15 tampoco cumplen con el requisito de novedad.

La reivindicación 16 consiste en: *“Un medio de almacenamiento legible por computadora no transitorio que almacena instrucciones legibles por computadora, caracterizado porque cuando se ejecutan, hacen que un primer sistema informático a: (...)”* (Radicado N° NC2018/0009316 del 24 de octubre de 2019).

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

Características esenciales	D1	D2
En respuesta a una petición de un dispositivo del cliente, establezca un primer túnel de red entre el dispositivo del cliente y una primera puerta de enlace.	Un método y un sistema para establecer una conexión entre un aparato informático y un sistema de gestión a través de una red, (...) que comprende establecer un túnel entre un nodo asociado con el aparato informático y un nodo maestro asociado con el sistema de gestión (...) (Párr. 0017). El maestro de túneles (71), (...) da instrucciones a la respectiva puerta de enlace en cada uno de los dos sitios A, B para establecer una conexión directa entre ellos (...) (Párr. 0072).	(...) El método y el aparato incluyen un dispositivo cliente que tiene un módulo de intercambio de claves de Internet (IKE) para establecer al menos dos túneles utilizando un protocolo IKE en el que un primer túnel es un túnel VPN de extremo a extremo a la puerta de enlace VPN de la empresa, y un segundo túnel es un túnel basado en la red a la red VPN gateway (Párr. 0007).
Recibir, por el primer sistema informático, del dispositivo del cliente, una lista de acceso del cliente.	(...) Esta segunda máquina virtual (102) tiene la responsabilidad de proteger el tráfico de red del escritorio y puede ser controlada por un administrador del sistema central. Esto permite que un administrador del sistema central defina una política de cortafuegos por escritorio, que la misma computadora implemente esa	(...) Este controlador incluye una base de datos de autenticación de seguridad (SADB) que almacena las políticas de seguridad empresarial descargadas respectivamente para cada uno de los al menos dos túneles. (...) Esta información incluye las direcciones IP de los puntos finales de al menos dos túneles en

Oficio N° 2073 de 11 de febrero de 2020

Ref. Expediente N° NC2018/0009316

	política y que confíe en que la política no puede ser interferida (...) (Párr. 0081).	las respectivas puertas de enlace VPN y políticas que especifican las direcciones IP de los hosts detrás de los túneles, así como los puertos TCP de destino en estos hosts para los cuales este túnel debe usarse para transportar tráfico (...) (Párr. 0008).
Iniciar, para el primer túnel de red, un servicio de cortafuegos separado con un conjunto separado de reglas del cortafuegos en el primer sistema informático para bloquear selectivamente y permitir el tráfico de red entre el dispositivo del cliente y uno o más dispositivos de red en una red privada, en donde cada una de las reglas del cortafuegos se derivan de la lista de acceso del cliente.	(...) Esta política de firewall podría usarse para restringir el acceso de los usuarios a ciertos servicios en lugar de darles un amplio acceso a la red corporativa. También se puede usar para monitorear el tráfico de red hacia y desde el escritorio en busca de patrones de tráfico inusuales, como una infección por gusanos / virus o la penetración de la red por parte de terceros (...) (Párr. 0081).	(...) La red empresarial (120) comprende una puerta de enlace / firewall VPN empresarial (en adelante, "puerta de enlace VPN"), que sirve como punto final del lado del servidor para el túnel VPN (...) (Párr. 0025). (...) El Firewall Engine (254) aplica la política de firewall configurada. El módulo de proceso IKE (224) descarga la política de firewall desde el SMS (126) durante la negociación de IKE (...) (Párr. 0047). Un noveno servicio de valor agregado proporciona bloqueo / filtrado de URL. Una empresa normalmente restringe el acceso a algunos sitios web para sus usuarios (...) (Párr. 0103).

De acuerdo con la tabla anterior, las características esenciales del medio de almacenamiento legible por computadora de la reivindicación 16 habían sido divulgadas previamente en los documentos D1 y D2, por lo tanto, la materia reivindicada no es nueva.

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

- Reivindicación 19: (...) Esto le permite a un administrador del sistema central definir una política de firewall por escritorio, tener esa política implementada por el propio equipo y tener la confianza de que la política no puede ser interferida. (...) También se puede usar para monitorear el tráfico de la red hacia y desde el escritorio en busca de patrones de tráfico inusuales, como una infección de gusanos / virus o una penetración de la red por parte de terceros (...) (Párr. 0081). (...) La supervisión puede involucrar a un servidor centralizado que regularmente envía solicitudes de determinación de estado a máquinas virtuales en dispositivos para obtener información de estado de los mismos (...) (Párr. 0055).
- Reivindicación 20: (...) Comprende establecer un túnel entre un nodo asociado con el aparato informático y un nodo maestro asociado con el sistema de gestión, en el que la conexión comprende establecer una conexión segura entre el aparato informático y el sistema de gestión a través del túnel y la conexión segura se establece entre el nodo asociado con el aparato informático y el nodo maestro asociado con el sistema de gestión mediante una conexión de red privada virtual, en la que la conexión virtual privada de red protege los datos con cifrado y / o autenticación y / o protección de integridad (Párr. 0017).

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

Oficio N° 2073 de 11 de febrero de 2020

Ref. Expediente N° NC2018/0009316

- Reivindicación 17: Además, se observa que cuando el dispositivo cliente (130) intenta establecer un túnel de red (158), pero falla, los paquetes que deberían haberse reenviado a través del túnel de red (158) se reenvían a través del túnel de extremo a extremo (156). Para Para lograr esto, la política en el cliente SADB (260) se modifica adecuadamente. Además, el dispositivo (130) del cliente envía información al SMS (126), de modo que el SMS (126) puede cambiar el firewall y otras políticas en el Enterprise VPN Gateway (122) para permitir que se acepten estos paquetes en este Gateway. En consecuencia, la presente invención proporciona tolerancia a fallos en el caso de que no se pueda establecer un túnel de red (158) (Párr. 0075).
- Reivindicación 18: Es decir, IKE se utiliza para establecer el túnel (156) de la empresa y el túnel (158) de la red. Las políticas para los dos túneles se descargan desde la puerta de enlace (122) de la empresa y se rellenan en la base de datos (260) de SA del dispositivo (130) del cliente (Párr. 0076). Además, se observa que cuando el dispositivo cliente (130) intenta establecer un túnel de red (158), pero falla, los paquetes que deberían haberse reenviado a través del túnel de red (158) se reenvían a través del túnel de extremo a extremo (156). Para Para lograr esto, la política en el cliente SADB (260) se modifica adecuadamente. Además, el dispositivo (130) del cliente envía información al SMS (126), de modo que el SMS (126) puede cambiar el firewall y otras políticas en el Enterprise VPN Gateway (122) para permitir que se acepten estos paquetes en este Gateway. En consecuencia, la presente invención proporciona tolerancia a fallos en el caso de que no se pueda establecer un túnel de red (158) (Párr. 0075).
- Reivindicación 19: (...) Normalmente, una empresa permitirá que los paquetes TCP salgan de la empresa, pero permitirá que los paquetes TCP ingresen a la empresa solo si la conexión TCP correspondiente se inició desde dentro de la empresa. Este es un ejemplo de una funcionalidad de firewall de estado y requiere que el estado de TCP se mantenga por sesión. Dado que el encabezado TCP (y el encabezado IP) en los paquetes son visibles en el IPSS (104), el mantenimiento del estado TCP es posible en el IPSS (104) y, por lo tanto, el IPSS (104) puede proporcionar una funcionalidad de firewall de estado completo (Párr. 0099).
- Reivindicación 20: El método de la reivindicación (13), en el que en un caso en el que dicha información de encabezado de paquete coincide con dichos valores de SADB, dicho método comprende además: recuperar la dirección IP de destino del túnel y una clave de cifrado de dicha SADB; cifrar dicho paquete; adjuntando un encabezado IPsec; y realizar el procesamiento de IP convencional (Reivindicación 15).

Las reivindicaciones dependientes 17 a 20 tampoco cumplen con el requisito de novedad.

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	US20150293756	1 a 4, 7 a 16, 19 y 20	Novedad
D2	US20040225895	1, 2, 5 a 9 y 11 a 20	Novedad

7. Respuesta a los argumentos del solicitante

El solicitante argumenta que “(...) La reivindicación 1 se ha modificado anteriormente para ahora recitar la recepción de una lista de acceso del cliente desde un dispositivo

Oficio N° 2073 de 11 de febrero de 2020

Ref. Expediente N° NC2018/0009316

cliente y derivar las reglas del cortafuegos de la lista de acceso del cliente.

Al objetar la reivindicación dependiente 6, que se relaciona con la recepción de una lista de acceso del cliente y la determinación de las reglas del cortafuegos de la lista de acceso del cliente, el examinador cita a D1 en los párrafos [0017], [0055] y [0081]. Al menos por las siguientes razones, D1 no enseña o sugiere las características anteriores de la reivindicación 1 (...)."

Se aclara que el documento D1 se utilizó para afectar la novedad de las reivindicaciones independientes 1, 11 y 16 y las reivindicaciones dependientes relacionadas en la sección 6 del presente oficio, asimismo, es importante mencionar que el documento D1 se refiere a una máquina virtual controlada por un sistema central encargada de proteger el tráfico de la red, donde dicho sistema define una política de cortafuegos a ser aplicada y restringir así el acceso de usuarios a ciertos servicios (Párr. 0081), por lo tanto D1, si revela la recepción de una lista de acceso del cliente³ y la determinación de las reglas del cortafuegos, al referirse a las políticas definidas por el sistema central, como ocurre en la solicitud de patente, anticipando de esta manera las características reclamadas.

El solicitante afirma que "(...) Otros párrafos de D1 citados por el examinador respetuosamente no remedian las deficiencias anteriores. Por ejemplo, el párrafo [0072] de D1 describe un maestro tunelizador que forma parte del sistema de administración **central** e instruye a una puerta de enlace para establecer una conexión. Sin embargo, este maestro de túnel **no enseña ni sugiere** que se establezca un primer túnel de red en respuesta a la solicitud de un dispositivo cliente, que este dispositivo cliente proporcione una lista de acceso de cliente y que las reglas del cortafuegos se deriven de esta lista de acceso de cliente para la primera red túnel, como se reclama (...)."

Se aclara que el documento D1 menciona la creación de túneles entre los dispositivos y las puertas de enlace para establecer una conexión entre nodos tunelizadores debido a una instrucción del maestro tunelizador (Párr. 0072), donde una vez es establecida la conexión del túnel el resto del proceso puede desarrollarse automáticamente (Párr. 0073), es decir, que el sistema central puede definir las políticas cortafuegos a la máquina virtual para que estas sean aplicadas a la conexión (Párr. 0081), por lo tanto D1, revela el establecimiento de un primer túnel de red, donde adicionalmente se definen o determinan las listas de acceso o políticas de cortafuegos para dicho primer túnel de red, tal como lo define el capítulo reivindicatorio allegado, afectando así las características de la solicitud de patente.

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 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.

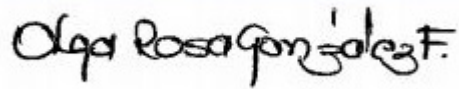
³ https://www.ibm.com/support/knowledgecenter/SSPREK_9.0.0/com.ibm.isam.doc/wrp_config/concept/con_acl.html



Oficio N° 2073 de 11 de febrero de 2020

Ref. Expediente N° NC2018/0009316

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.



OLGA ROSA GONZÁLEZ FONSECA
DIRECTORA DE NUEVAS CREACIONES (E)



Oficio N° 2073 de 11 de febrero de 2020

Ref. Expediente N° NC2018/0009316

INFORME DE BÚSQUEDA
EXAMEN DE PATENTABILIDAD

Solicitud No.		Examen de patentabilidad							
NC2018/0009316		1°		2°	X	3°		Revoca	
Solicitud Internacional No.		Fecha solicitud internacional: (DD/MM/AÑO)							
PCT/US2016/036053		6 de junio de 2016							
Fecha de determinación estado de la técnica (DD/MM/AÑO)				Prioridad		Presentación			
08/02/2016				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 20
Palabras clave utilizadas	VPN, Virtual Private Network, Tunnel, Establishment, Firewall, Policy, Rules, Filter, Allow, Block, Tunnel Failure, Primary, Secondary.
Clasificaciones utilizadas para la búsqueda	CIP: H04L 29/06

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	14231894	23/10/2014	-	-	A
ISA	US20150293756	15/10/2015	1 a 4, 7 a 16, 19 y 20	1 Párr. 0017, Párr. 0072, Párr. 0081. 2 Párr. 0081, Párr. 0055. 3 Párr. 0056. 4 Párr. 0056, Párr. 0058. 7 y 8 Párr. 0101, Párr. 0081. 9 Párr. 0017, Párr. 0085. 10 Párr. 0085, Párr. 0074. 11 Párr. 0101, Párr. 0015, Párr. 0017, Párr. 0072, Párr. 0081. 12 a 14 Párr. 0101, Párr. 0081. 15 Párr. 0081. 16 Párr. 0017, Párr. 0072, Párr. 0081. 19 y 20 Párr. 0081, Párr. 0055.	X
Patbase	US20040225895	11/11/2004	1, 2, 5 a 9 y 11 a 20	1 Párr. 0007, Párr. 0008, Párr. 0025, Párr. 0047, Párr. 0103. 2 Párr. 0099.	X

Oficio N° 2073 de 11 de febrero de 2020

Ref. Expediente N° NC2018/0009316

				5 Párr. 0075. 6 Párr. 0076, Párr. 0075. 7 y 8 Párr. 0025. Párr. 0034 9 Reivindicación 15, Reivindicación 18. 11 Parr. 0034, Párr. 0007, Párr. 0008, Párr. 0025, Párr. 0047, Párr. 0103. 12 a 14 Párr. 0034, Párr. 0025. 15 Párr. 0055. 16 Párr. 0007, Párr. 0008, Párr. 0025, Párr. 0047, Párr. 0103. 17 Párr. 0075. 18 Párr. 0076, Párr. 0075. 19 Párr. 0099. 20 Reivindicación 15.	
(1) Cita completa literatura no patente (LNP)					
Apellido, A. A. (Fecha). Título del artículo. <i>Nombre de la revista. Volumen</i> (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: (28/01/2020)					
Examinador: CARLOS EDUARDO GUEVARA NICHROY					