

**REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO**

Oficio N° 2178

Ref. Expediente N° NC2016/0000561

Señor(a)
ACCELERATION SYSTEMS, LLC
notificaciones@clarkemodet.com.co

Asunto: PATENTE DE INVENCION - PCT

Patente de Invención	PT	Patente de Modelo de Utilidad			
Vía Nacional					
Vía PCT (Fase Nacional)	PCT	Capítulo I		Capítulo II	
No. Solicitud Internacional	PCT/US2014/015035				
Fecha de Presentación Internacional	6 de febrero de 2014				

Como resultado del examen de fondo realizado, con fundamento en el Artículo 45 de la Decisión 486 de la Comisión de la Comunidad Andina, se comunica:

1. Documentos estudiados

Descripción	Radicado N° NC2016/0000561	02/Agosto/2016
Reivindicaciones:	Radicado N° NC2016/0000561	02/Agosto/2016
	Radicado N° NC2016/0000756	09/Agosto/2016
	Radicado N° NC2016/0000561	20/Diciembre/2016
Dibujos:	Radicado N° NC2016/0000561	02/Agosto/2016

2. Modificaciones presentadas (Art. 34 D 486 y Art. 19, 22 y 34 PCT)

**REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO**

Oficio N° 2178

Ref. Expediente N° NC2016/0000561

Se aceptan las modificaciones presentadas comoquiera que se ajustan a las prescripciones contenidas en el reglamento del PCT y en el Art 34 de la Decisión 486.

3. 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, se tendrá en cuenta la tasa pagada por la solicitante al momento de comenzar el examen para las reivindicaciones adicionales; esto es que 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. Por lo tanto, se estudiarán las reivindicaciones 1 a 19 del capítulo reivindicatorio (Radicado N° NC2016/0000561 del 20 de diciembre de 2016).

Título de la solicitud: "Anotación de contenidos de medios para la comprensión automática de contenidos" (Ver página 1 del radicado bajo el N° NC2016/0000561 del 02 de agosto de 2016).

El problema planteado en esta solicitud consiste en la necesidad de suministrar un sistema para etiquetar elementos en una trama de video o de audio en un punto dado en el tiempo como un anotador de flujo de medios. Si es suficientemente preciso, un sistema de reconocimiento de patrones genera automáticamente metadatos desde el flujo de medios que pueden utilizarse para reducir el tiempo y esfuerzo humanos requeridos para crear los metadatos de alta precisión.

Para resolver este problema técnico, la solicitud en estudio proporciona un sistema que consta de un acceso aleatorio a una trama o sección del flujo de medios archivado y de los metadatos asociados y la visualización o superposición gráfica en tiempo real de metadatos generados por el sistema de reconocimiento de patrones en la presentación de la trama de video.

El objeto de la presente solicitud se relaciona con la Clasificación Internacional de Patentes (CIP): H04L 12/28.

4. De la solicitud de patente

Página 2 de 22

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Oficio N° 2178

Ref. Expediente N° NC2016/0000561

Reivindicaciones (Art. 30 D 486, Art. 22 PCT)

- Las reivindicaciones 1 a 6, 10 a 13, 15 18 y 19 no son claras, debido a que poseen términos generales que no permiten establecer un concepto suficiente de la invención que se está reclamando. Estos términos se describen a continuación: reivs. 1, 2 y 18: “(...) *primera lógica* (...)”; reivs. 1, 4 y 5: “(...) *procesador* (...)”; reivs. 1, 2, 12, 13, 18 y 19: “(...) *compuerta de propietario* (...)”; reivs. 1, 3 y 6 “(...) *segunda lógica* (...)”; reivs. 4, 7, 8, 10, 11 y 15: “(...) *interfaz de usuario* (...)”; reiv. 4: “(...) *tercera lógica* (...)”; reiv. 5: “(...) *cuarta lógica* (...)”; reivs. 6, 8, 10, 11 y 17: “(...) *Proceso de Texto Claro limpio de estantería comercial* (...)”. Se sugiere hacer la aclaración respectiva.
- Las reivindicaciones 1, 18 y 19 no son claras porque los términos: reiv. 18: “*al menos*”; reivs. 1 y 19: “*por lo menos*”; son imprecisos, por lo cual no permiten distinguir la invención del estado de la técnica. Se sugiere sustituirlos por un término preciso o un rango concreto.

5. Determinación del Estado de la Técnica

El estado de la técnica se determinó con base en la fecha de solicitud internacional: febrero 06 de 2014 y se encontraron los siguientes documentos que anticipan el objeto de esta solicitud:

Ítem	Documento	Título	Fecha de Publicación
D1	US 2011/013641	“Method and Apparatus for Communication of Data Packets between Local Networks”	20/enero/2011
D2	US 2008/201486	“Dynamic system and method for virtual private network (VPN) packet level routing using dual-NAT method”	21/agosto/2008
D3	US 2012/159607	“Multi-Service VPN Network Client For Mobile Device”	21/junio/2012

**REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO**

Oficio N° 2178

Ref. Expediente N° NC2016/0000561

El documento D1¹ divulga un método y disposición para obtener un direccionamiento inequívoco para los paquetes de datos comunicados entre dispositivos (E1B, E3A) en dos redes locales diferentes (A, B) que utilizan espacios de direcciones IP privadas superpuestas (Fl. 1, resumen).

El documento D2² divulga un sistema y método para enrutamiento de nivel de paquetes de red privada virtual (VPN) utilizando una arquitectura Dual-NAT para proporcionar una conexión segura bidireccional entre aplicaciones, hosts o redes en dos sitios finales sin exponer las direcciones IP y topologías de red reales de los demás (Fl. 1, resumen).

El documento D3³ divulga un cliente de red integrado y multiservicio para dispositivos móviles celulares (Fl. 1, resumen).

6. Examen de Patentabilidad (Art. 14 D486)

Novedad (Art 16 D286)

La reivindicación 12 consiste en: “*Un método para suministrar una arquitectura de vínculo seguro (...)*” (Ver página 4 del radicado N° NC2016/0000561 del 20 de diciembre de 2016).

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

Características esenciales	D1
Crear un primer túnel VPN entre una estación de trabajo de cliente	Una VPN se puede ver básicamente como un túnel encriptado a través de una red IP pública, para transferir paquetes de datos entre terminales y servidores (Pág. 1, Fl. 5, Párr. 006).

1https://worldwide.espacenet.com/publicationDetails/biblio?CC=US&NR=2011013641A1&KC=A1&FT=D&ND=3&date=20110120&DB=&locale=en_EP

2https://worldwide.espacenet.com/publicationDetails/biblio?II=1&ND=3&adjacent=true&locale=en_EP&FT=D&date=20080821&CC=US&NR=2008201486A1&KC=A1

3https://worldwide.espacenet.com/publicationDetails/biblio?II=0&ND=3&adjacent=true&locale=en_EP&FT=D&date=20120621&CC=US&NR=2012159607A1&KC=A1

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Oficio N° 2178

Ref. Expediente N° NC2016/0000561

y una primera compuerta de propietario.	
Enviar un datagrama de salida de la estación de trabajo de cliente a la primera compuerta de propietario.	En algún momento posterior en un paso adicional (304), se recibe un paquete de datos entrantes a través del túnel VPN, cuyo paquete se ha enviado desde el segundo dispositivo y tiene un encabezado interno con direcciones de origen y destino usadas en la segunda red para el primer y segundo dispositivos, respectivamente (Pág. 5, Fl. 9, Párr. 059).
Recibir un datagrama de entrada desde la primera compuerta de propietario a la estación de trabajo de cliente, en donde el datagrama de entrada incluye una dirección de protocolo de internet (IP) fuente y una dirección de protocolo de internet (IP) destino que se configura a una dirección IP privada de propietario de VPN.	Una vez recibido el paquete, la puerta de enlace (102) elimina el encabezado externo y cambia el encabezado interno traduciendo la dirección de destino privada a 10.0.0.11 y la dirección de origen a 10.0.1.4, que son válidas en la red (A) para los dispositivos (E1B) y (E3A), respectivamente (Pág. 4, Fl. 8, Párr. 055).
Registrar una nueva dirección IP privada de propietario de VPN de la dirección IP fuente en el datagrama de entrada.	Cuando se recibe el paquete de datos, el gateway (102) elimina el encabezado externo, habiendo cumplido su propósito, mientras que la red de envío puede deducirse del túnel VPN utilizado para transmitir el paquete. Debe recordarse que el paquete recibido contiene un destino privado y direcciones de origen válidas en la red emisora B, pero no en la red receptora A. Por lo tanto, el gateway (102) cambia las direcciones de origen y destino en el encabezado interno del paquete, en un paso (1): (6) adicional, traduciéndolos en direcciones usadas en la red receptora A (Pág. 4, Fl. 8, Párr. 050).
Asignar una nueva dirección IP privada única (UIP) para el datagrama de entrada y la estación de trabajo de cliente.	Una vez recibido el paquete, la puerta de enlace (102) elimina el encabezado externo y cambia el encabezado interno traduciendo la dirección de destino privada a 10.0.0.11 y la dirección de origen a 10.0.1.4, que son válidas en la red (A) para los dispositivos (E1B) y (E3A), respectivamente (Pág. 4, Fl. 8, Párr. 055).
Enviar el datagrama de entrada a la estación de trabajo de cliente.	En algún momento posterior en un paso adicional (304), se recibe un paquete de datos entrantes a través del túnel VPN,

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Oficio N° 2178

Ref. Expediente N° NC2016/0000561

	cuyo paquete se ha enviado desde el segundo dispositivo y tiene un encabezado interno con direcciones de origen y destino usadas en la segunda red para el primer y segundo dispositivos, respectivamente (Pág. 5, Fl. 9, Párr. 059).
Crear un segundo túnel VPN entre la estación de trabajo de cliente y una segunda compuerta de propietario mientras se está utilizando el primer túnel VPN.	De esta forma, una puerta de enlace en una red local puede establecer múltiples túneles VPN con puertas de enlace de otras redes locales, y se puede crear una tabla de traducción o similar en la puerta de enlace, que contenga al menos una identidad de túnel y un espacio de direcciones IP no superpuesto utilizado en la red para cada red local opuesta (Pág. 3, Fl. 7, Párr. 045).

De acuerdo con la tabla anterior, donde se comparan las características técnicas de la reivindicación 12 con la anterioridad D1, el método descrito en dicha reivindicación, ya era conocido en el estado de la técnica. Por lo tanto, la reivindicación 12 no es nueva.

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

- Reivindicación 14: Una vez recibido el paquete, la puerta de enlace (102) elimina el encabezado externo y cambia el encabezado interno traduciendo la dirección de destino privada a 10.0.0.11 y la dirección de origen a 10.0.1.4, que son válidas en la red (A) para los dispositivos (E1B) y (E3A), respectivamente (Pág. 4, Fl. 8, Párr. 055)
- Reivindicación 16: Una VPN se puede ver básicamente como un túnel encriptado a través de una red IP pública, para transferir paquetes de datos entre terminales y servidores (Pág. 1, Fl. 5, Párr. 006).

La reivindicación 18 consiste en: *“Un sistema para suministrar una arquitectura de vínculo seguro (...)”* (Ver página 6 del radicado N° NC2016/0000561 del 20 de diciembre de 2016).

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

Características esenciales	D1
----------------------------	----

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Oficio N° 2178

Ref. Expediente N° NC2016/0000561

Componente de red privada virtual (VPN) MSL que incluye primera lógica que se ejecuta en un procesador.	Una VPN se puede ver básicamente como un túnel encriptado a través de una red IP pública, para transferir paquetes de datos entre terminales y servidores (Pág. 1, Fl. 5, Párr. 006). Es pertinente aclarar que un servidor contiene un procesador que ejecuta instrucciones correspondientes a una lógica ⁴ .
Sistema para crear un primer túnel VPN entre una estación de trabajo de cliente y una primera compuerta de propietario.	Una VPN se puede ver básicamente como un túnel encriptado a través de una red IP pública, para transferir paquetes de datos entre terminales y servidores (Pág. 1, Fl. 5, Párr. 006).
Sistema para enviar un datagrama de salida de la estación de trabajo de cliente a la primera compuerta de propietario.	En algún momento posterior en un paso adicional (304), se recibe un paquete de datos entrantes a través del túnel VPN, cuyo paquete se ha enviado desde el segundo dispositivo y tiene un encabezado interno con direcciones de origen y destino usadas en la segunda red para el primer y segundo dispositivos, respectivamente (Pág. 5, Fl. 9, Párr. 059).
Sistema para recibir un datagrama de entrada desde la primera compuerta de propietario a la estación de trabajo de cliente, en donde el datagrama de entrada incluye una dirección de protocolo de internet (IP) fuente y una dirección de protocolo de internet (IP) destino que se configura a una dirección IP privada de propietario de VPN.	Una vez recibido el paquete, la puerta de enlace (102) elimina el encabezado externo y cambia el encabezado interno traduciendo la dirección de destino privada a 10.0.0.11 y la dirección de origen a 10.0.1.4, que son válidas en la red (A) para los dispositivos (E1B) y (E3A), respectivamente (Pág. 4, Fl. 8, Párr. 055).
Sistema para registrar una nueva dirección IP privada de propietario de VPN de la dirección IP fuente en el datagrama de entrada.	Cuando se recibe el paquete de datos, el gateway (102) elimina el encabezado externo, habiendo cumplido su propósito, mientras que la red de envío puede deducirse del túnel VPN utilizado para transmitir el paquete. Debe recordarse que el paquete recibido contiene un destino privado y direcciones de origen válidas en la red emisora B, pero no en la red receptora A. Por lo tanto, el gateway (102) cambia las direcciones de origen y destino en el encabezado interno del paquete, en un paso (1):

4 [https://en.wikipedia.org/wiki/Server_\(computing\)](https://en.wikipedia.org/wiki/Server_(computing))

**REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO**

Oficio N° 2178

Ref. Expediente N° NC2016/0000561

	(6) adicional, traduciéndolos en direcciones usadas en la red receptora A (Pág. 4, Fl. 8, Párr. 050).
Sistema para asignar una nueva dirección IP privada única (UIP) para el datagrama de entrada y la estación de trabajo de cliente.	Una vez recibido el paquete, la puerta de enlace (102) elimina el encabezado externo y cambia el encabezado interno traduciendo la dirección de destino privada a 10.0.0.11 y la dirección de origen a 10.0.1.4, que son válidas en la red (A) para los dispositivos (E1B) y (E3A), respectivamente (Pág. 4, Fl. 8, Párr. 055).
Sistema para enviar el datagrama de entrada a la estación de trabajo de cliente.	En algún momento posterior en un paso adicional (304), se recibe un paquete de datos entrantes a través del túnel VPN, cuyo paquete se ha enviado desde el segundo dispositivo y tiene un encabezado interno con direcciones de origen y destino usadas en la segunda red para el primer y segundo dispositivos, respectivamente (Pág. 5, Fl. 9, Párr. 059).
El sistema adicionalmente crea un segundo túnel VPN entre la estación de trabajo de cliente y una segunda compuerta de propietario mientras se está utilizando el primer túnel VPN.	De esta forma, una puerta de enlace en una red local puede establecer múltiples túneles VPN con puertas de enlace de otras redes locales, y se puede crear una tabla de traducción o similar en la puerta de enlace, que contenga al menos una identidad de túnel y un espacio de direcciones IP no superpuesto utilizado en la red para cada red local opuesta (Pág. 3, Fl. 7, Párr. 045).

De acuerdo con la tabla anterior, donde se comparan las características técnicas de la reivindicación 18 con la anterioridad D1, el sistema descrito en dicha reivindicación, ya era conocido en el estado de la técnica. Por lo tanto, la reivindicación 18 no es nueva.

Nivel inventivo (Art 18 D286)

La reivindicación 1 consiste en: “*Un sistema para suministrar una arquitectura de vínculo seguro simple (...)*” (Ver página 1 del radicado N° NC2016/0000561 del 20 de diciembre de 2016).

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

Características esenciales	D2	D1

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Oficio N° 2178

Ref. Expediente N° NC2016/0000561

Componente de red privada virtual (VPN) MSL que incluye primera lógica que se ejecuta en un procesador.	Además, puede apreciarse que el nodo de VPN cliente (50) puede configurarse para hospedar al menos un recurso, de modo que el nodo de VPN de recurso también puede ser un nodo de cliente, y el nodo de cliente puede utilizarse como un nodo de recurso (Pág. 3, Fl. 16, Párr. 027). Puede apreciarse que el intercambio de datos entre el recurso y los nodos de cliente (20), (50) del sistema de red (10) (figura 1) puede ser entre una máquina cliente o cliente (70) tal como un dispositivo informático (por ejemplo, una computadora, PDA, teléfono celular, cualquier dispositivo con una CPU/software incrustado) (Pág. 3, Fl. 16, Párr. 028). Es pertinente aclarar que un dispositivo con una CPU comprende un procesador ⁵ .	Una VPN se puede ver básicamente como un túnel encriptado a través de una red IP pública, para transferir paquetes de datos entre terminales y servidores (Pág. 1, Fl. 5, Párr. 006). Es pertinente aclarar que un servidor contiene un procesador que ejecuta instrucciones correspondientes a una lógica ⁴ .
Sistema para crear un primer túnel VPN entre una estación de trabajo de cliente y una primera compuerta de propietario.	Además, puede apreciarse que el nodo de VPN cliente (50) puede configurarse para hospedar al menos un recurso, de modo que el nodo de VPN de recurso también puede ser un nodo de cliente, y el nodo de cliente puede utilizarse como un nodo de recurso (Pág. 3, Fl. 16, Párr. 027). Puede apreciarse que el intercambio de datos entre el recurso y los nodos de cliente (20), (50) del sistema de red (10) (figura 1) puede ser entre una máquina cliente o cliente (70) tal como un dispositivo informático (por ejemplo, una computadora, PDA, teléfono celular, cualquier dispositivo con una CPU/software incrustado) (Pág. 3, Fl. 16, Párr. 028).	Una VPN se puede ver básicamente como un túnel encriptado a través de una red IP pública, para transferir paquetes de datos entre terminales y servidores (Pág. 1, Fl. 5, Párr. 006).
Sistema para enviar un	La figura 5 muestra una tabla que se refiere a la regla de solo NAT para el flujo de	En algún momento posterior en un paso adicional (304), se recibe un

5 https://es.wikipedia.org/wiki/Unidad_central_de_procesamiento



REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Oficio N° 2178

Ref. Expediente N° NC2016/0000561

datagrama de salida de la estación de trabajo de cliente a la primera compuerta de propietario.	paquetes de acceso a recursos remotos entre dos nodos VPN iguales de acuerdo con la realización. En el sitio de recursos DVPN gateway (30) (Gateway A), el número de puerto fuente (cliente) (2000) no se modifica en la traducción de direcciones. En consecuencia, cada conexión requiere una nueva dirección IP local como 10.1.0.102 (Pág. 7, Fl. 20, Párr. 079). Es pertinente aclarar que un paquete de datos es un datagrama ⁶ . Como se muestra en la figura 2 (y la figura 1), el cliente (70) emite una solicitud de un recurso (40) dentro del nodo (50) de red privada virtual del cliente en forma de un paquete IP que tiene una IP de origen (IP src), una dirección IP de destino (dst IP) y Datos, que es recibido por el cliente DVPN gateway (60) (Gateway B) (Pág. 4, Fl. 17 a Pág. 5, Fl. 18, Párr. 044).	paquete de datos entrantes a través del túnel VPN, cuyo paquete se ha enviado desde el segundo dispositivo y tiene un encabezado interno con direcciones de origen y destino usadas en la segunda red para el primer y segundo dispositivos, respectivamente (Pág. 5, Fl. 9, Párr. 059).
Sistema para recibir un datagrama de entrada desde la primera compuerta de propietario a la estación de trabajo de cliente, en donde el datagrama de entrada incluye una dirección de protocolo de internet (IP) fuente y una dirección de	La figura 5 muestra una tabla que se refiere a la regla de solo NAT para el flujo de paquetes de acceso a recursos remotos entre dos nodos VPN iguales de acuerdo con la realización. En el sitio de recursos DVPN gateway (30) (Gateway A), el número de puerto fuente (cliente) (2000) no se modifica en la traducción de direcciones. En consecuencia, cada conexión requiere una nueva dirección IP local como 10.1.0.102 (Pág. 7, Fl. 20, Párr. 079). Como se muestra en la figura 2 (y la figura 1), el cliente (70) emite una solicitud de un recurso (40) dentro del nodo (50) de red privada virtual del cliente en forma de un paquete IP que tiene una IP de origen (IP	Una vez recibido el paquete, la puerta de enlace (102) elimina el encabezado externo y cambia el encabezado interno traduciendo la dirección de destino privada a 10.0.0.11 y la dirección de origen a 10.0.1.4, que son válidas en la red (A) para los dispositivos (E1B) y (E3A), respectivamente (Pág. 4, Fl. 8, Párr. 055).

6 <https://es.wikipedia.org/wiki/Datagrama>



REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Oficio N° 2178

Ref. Expediente N° NC2016/0000561

protocolo de internet (IP) destino que se configura a una dirección IP privada de propietario de VPN.	src), una dirección IP de destino (dst IP) y Datos, que es recibido por el cliente DVPN gateway (60) (Gateway B) (Pág. 4, Fl. 17 a Pág. 5, Fl. 18, Párr. 044). Para la regla NAT de sitio de cliente: en el sitio de inicio de sesión (es decir, típicamente el Sitio de cliente), la regla NAT de sitio de cliente se usa para traducir la dirección de destino (recurso virtual) a una dirección de DVPN de destino específico (por ejemplo, 10.2.0.100: 8080 => 198.1.0.200:80, figura 3) que es parte del conjunto de direcciones DVPN del sitio de recursos DVPN gateway (30) (Gateway A) (Pág. 6, Fl. 18, Párr. 050). Es pertinente aclarar que la dirección IP 10.2.0.100 es parte del rango de direccionamiento privado IP ⁷ .	
Sistema para enviar el datagrama de entrada con la dirección IP destino; y un traductor de dirección de red (NAT) gemelo MSL que incluye segunda lógica que se ejecuta por un procesador.	Para la regla NAT de sitio de cliente: en el sitio de inicio de sesión (es decir, típicamente el Sitio de cliente), la regla NAT de sitio de cliente se usa para traducir la dirección de destino (recurso virtual) a una dirección de DVPN de destino específico (por ejemplo, 10.2.0.100: 8080 => 198.1.0.200:80, figura 3) que es parte del conjunto de direcciones DVPN del sitio de recursos DVPN gateway (30) (Gateway A) (Pág. 6, Fl. 18, Párr. 050). Es pertinente aclarar que la dirección IP 10.2.0.100 es parte del rango de direccionamiento privado IP ⁷ . Como se muestra en la figura 1, el recurso y los gateways cliente DVPN (red privada virtual dinámica) (30) y (60) están configuradas de modo que las aplicaciones	No se menciona

⁷ https://es.wikipedia.org/wiki/Red_privada

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Oficio N° 2178

Ref. Expediente N° NC2016/0000561

	y otros recursos relacionados tales como el correo electrónico en un nodo VPN (20), (50) son accesibles por el otro nodo VPN (20), (50) en de tal manera que los recursos sean seguros, sin revelar las topologías de red local de dos nodos VPN, ya que son transportados o accedidos al proporcionar enrutamiento a nivel de paquete y proporcionando un método y sistema para un NAT dual dinámico para direcciones de origen y destino (Pág. 3, Fl. 16, Párr. 029). Realizaciones alternativas de la invención también pueden implementarse como un producto de programa de computadora para uso con un sistema de computadora (Pág. 9, Fl. 22, Párr. 099). Es pertinente aclarar que un computador posee un procesador⁸.	
Sistema para recibir el datagrama de entrada de VPN MSL.	La figura 5 muestra una tabla que se refiere a la regla de solo NAT para el flujo de paquetes de acceso a recursos remotos entre dos nodos VPN iguales de acuerdo con la realización. En el sitio de recursos DVPN gateway (30) (Gateway A), el número de puerto fuente (cliente) (2000) no se modifica en la traducción de direcciones. En consecuencia, cada conexión requiere una nueva dirección IP local como 10.1.0.102 (Pág. 7, Fl. 20, Párr. 079). Como se muestra en la figura 2 (y la figura 1), el cliente (70) emite una solicitud de un recurso (40) dentro del nodo (50) de red privada virtual del cliente en forma de un paquete IP que tiene una IP de origen (IP src), una dirección IP de destino (dst IP) y Datos, que es recibido por el cliente DVPN	En algún momento posterior en un paso adicional (304), se recibe un paquete de datos entrantes a través del túnel VPN, cuyo paquete se ha enviado desde el segundo dispositivo y tiene un encabezado interno con direcciones de origen y destino usadas en la segunda red para el primer y segundo dispositivos, respectivamente (Pág. 5, Fl. 9, Párr. 059).

⁸ <https://es.wikipedia.org/wiki/Computadora>



REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Oficio N° 2178

Ref. Expediente N° NC2016/0000561

	gateway (60) (Gateway B) (Pág. 4, Fl. 17 a Pág. 5, Fl. 18, Párr. 044).	
Sistema para registrar una nueva dirección IP privada de propietario de VPN de la dirección IP fuente en el datagrama de entrada.	Como se muestra en la figura 2 (y la figura 1), el cliente (70) emite una solicitud de un recurso (40) dentro del nodo (50) de red privada virtual del cliente en forma de un paquete IP que tiene una IP de origen (IP src), una dirección IP de destino (dst IP) y Datos, que es recibido por el cliente DVPN gateway (60) (Gateway B) (Pág. 4, Fl. 17 a Pág. 5, Fl. 18, Párr. 044).	Cuando se recibe el paquete de datos, el gateway (102) elimina el encabezado externo, habiendo cumplido su propósito, mientras que la red de envío puede deducirse del túnel VPN utilizado para transmitir el paquete. Debe recordarse que el paquete recibido contiene un destino privado y direcciones de origen válidas en la red emisora B, pero no en la red receptora A. Por lo tanto, el gateway (102) cambia las direcciones de origen y destino en el encabezado interno del paquete, en un paso (1): (6) adicional, traduciéndolos en direcciones usadas en la red receptora A (Pág. 4, Fl. 8, Párr. 050).
Sistema para asignar una nueva dirección IP privada única (UIP) para el datagrama de entrada y la estación de trabajo de cliente.	Para la regla de NAT del sitio de recursos: cuando el sitio de recursos DVPN (30) (puerta de enlace A) recibe los paquetes IP traducidos del túnel SSL (90), el sitio de recursos DVPN gateway (30) traduce la dirección DVPN de destino (recurso) de los paquetes recibidos a la real dirección IP del recurso (198.1.0.200:80=>10.1.0.200:80, figura 3) y selecciona una dirección IP local adecuada, en el sitio de recurso (20), ya sea desde un rango de IP o desde un servidor DHCP como la dirección IP de origen, para el cliente (198.2.0.10 => 10.1.0.101) (Pág. 5, Fl. 18, Párr. 005).	Una vez recibido el paquete, la puerta de enlace (102) elimina el encabezado externo y cambia el encabezado interno traduciendo la dirección de destino privada a 10.0.0.11 y la dirección de origen a 10.0.1.4, que son válidas en la red (A) para los dispositivos (E1B) y (E3A), respectivamente (Pág. 4, Fl. 8, Párr. 055).

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Oficio N° 2178

Ref. Expediente N° NC2016/0000561

Sistema para enviar el datagrama de entrada a la estación de trabajo de cliente.	Luego, el gateway DVPN (60) (Gateway B) envía el paquete, en nombre del servidor FTP, al Cliente en el Sitio de nodo de red privada virtual B (Pág. 8, Fl. 21, Párr. 092).	En algún momento posterior en un paso adicional (304), se recibe un paquete de datos entrantes a través del túnel VPN, cuyo paquete se ha enviado desde el segundo dispositivo y tiene un encabezado interno con direcciones de origen y destino usadas en la segunda red para el primer y segundo dispositivos, respectivamente (Pág. 5, Fl. 9, Párr. 059).
El sistema adicionalmente crea un segundo túnel VPN entre la estación de trabajo de cliente y una segunda compuerta de propietario mientras se está utilizando el primer túnel VPN.	No se menciona	De esta forma, una puerta de enlace en una red local puede establecer múltiples túneles VPN con puertas de enlace de otras redes locales, y se puede crear una tabla de traducción o similar en la puerta de enlace, que contenga al menos una identidad de túnel y un espacio de direcciones IP no superpuesto utilizado en la red para cada red local opuesta (Pág. 3, Fl. 7, Párr. 045).

El documento D2 se considera el estado de la técnica más cercano a la invención definida en la reivindicación 1 porque divulga un sistema y método para enrutamiento de nivel de paquetes de red privada virtual (VPN) utilizando una arquitectura Dual-NAT para proporcionar una conexión segura bidireccional entre aplicaciones, hosts o redes en dos sitios finales sin exponer las direcciones IP y topologías de red reales de los demás (Fl. 1, resumen).

La diferencia entre la invención, definida en la reivindicación 1 y el sistema de D2 consiste en que el sistema de la reivindicación 1 posee la creación de un segundo túnel VPN entre la estación de trabajo de cliente y una segunda compuerta de propietario.

**REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO**

Oficio N° 2178

Ref. Expediente N° NC2016/0000561

El efecto que logra el incluir la creación de un segundo túnel VPN entre la estación de trabajo de cliente y una segunda compuerta de propietario es poder utilizar diferentes túneles VPN al mismo tiempo entre la estación del cliente y las diferentes compuertas de propietario.

Por lo tanto, el problema técnico objetivo que pretende resolver esta invención se puede formular así: “¿cómo modificar el sistema conocido en D2 para lograr utilizar diferentes túneles VPN al mismo tiempo entre la estación del cliente y las diferentes compuertas de propietario?”.

Sin embargo, la utilización de la creación de un segundo túnel VPN entre la estación de trabajo de cliente y una segunda compuerta de propietario, ya está divulgada en el documento D1 que se refiere a que una puerta de enlace en una red local puede establecer múltiples túneles VPN con puertas de enlace de otras redes locales, y se puede crear una tabla de traducción o similar en la puerta de enlace, que contenga al menos una identidad de túnel y un espacio de direcciones IP no superpuesto utilizado en la red para cada red local opuesta (Pág. 3, Fl. 7, Párr. 045).

En consecuencia, la persona del oficio normalmente versada en la materia, incluiría la creación de un segundo túnel VPN del documento D1 en el sistema divulgado en el documento D2 para llegar así al objeto de la reivindicación 1 de la solicitud. Por lo cual se considera obvia.

Asimismo, los documentos D2 y D1 divulgan las características de las siguientes reivindicaciones dependientes así:

- Reivindicación 3: Una vez recibido el paquete, la puerta de enlace (102) elimina el encabezado externo y cambia el encabezado interno traduciendo la dirección de destino privada a 10.0.0.11 y la dirección de origen a 10.0.1.4, que son válidas en la red (A) para los dispositivos (E1B) y (E3A), respectivamente (D1, Pág. 4, Fl. 8, Párr. 055).
- Reivindicación 5: Además, puede apreciarse que el nodo de VPN cliente (50) puede configurarse para hospedar al menos un recurso, de modo que el nodo de VPN de recurso también puede ser un nodo de cliente, y el nodo de cliente puede utilizarse como un nodo de recurso (D2, Pág. 3, Fl. 16, Párr. 027). Puede apreciarse que el intercambio de datos entre el recurso y los nodos de cliente (20), (50) del sistema de red (10) (figura 1) puede ser entre una máquina cliente o cliente

Página 15 de 22

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Oficio N° 2178

Ref. Expediente N° NC2016/0000561

(70) tal como un dispositivo informático (por ejemplo, una computadora, PDA, teléfono celular, cualquier dispositivo con una CPU/software incrustado) (D2, Pág. 3, Fl. 16, Párr. 028).

La reivindicación 13 consiste en: *“El método de la reivindicación 12, que además comprende: (...)”* (Ver página 5 del radicado N° NC2016/0000561 del 20 de diciembre de 2016).

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

Reiv.	Características esenciales	D1	D3
12	Un método para suministrar una arquitectura de vínculo seguro (...)	Ver Tabla 1.	Cliente de red integrado y multiservicio para dispositivos móviles celulares.
13	Encriptar el datagrama de salida y transferir el datagrama de salida a la primera compuerta de propietario.	Una VPN se puede ver básicamente como un túnel encriptado a través de una red IP pública, para transferir paquetes de datos entre terminales y servidores (Pág. 1, Fl. 5, Párr. 006).	El cliente de red multiservicio proporciona un controlador de red privada virtual (VPN) para establecer una conexión VPN con un dispositivo de seguridad VPN remoto, donde el manejador de VPN encripta los paquetes de red salientes y descifra los paquetes de red entrantes para tunelizar de forma segura los paquetes de red entre el dispositivo móvil y el dispositivo de seguridad VPN remoto (Pág. 1, Fl. 16, Párr. 009).
13	Recibir el datagrama de entrada en una forma encriptada de la primera compuerta de propietario (120a) y descifrar el datagrama de entrada.	No se menciona	

El documento D1 se considera el estado de la técnica más cercano a la invención definida en la reivindicación 13 porque divulga un método y disposición para obtener un direccionamiento inequívoco para los paquetes de datos comunicados entre

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Oficio N° 2178

Ref. Expediente N° NC2016/0000561

dispositivos (E1B, E3A) en dos redes locales diferentes (A, B) que utilizan espacios de direcciones IP privadas superpuestas (Fl. 1, resumen).

La diferencia entre la invención, definida en la reivindicación 13 y el método de D1 consiste en que el método de la reivindicación 13 posee la descripción del datagrama de entrada.

El efecto que logra el incluir la descripción del datagrama de entrada es poder descifrar el contenido del paquete que ha sido enviado de forma segura por medio del túnel VPN.

Por lo tanto, el problema técnico objetivo que pretende resolver esta invención se puede formular así: “¿cómo modificar el sistema conocido en D1 para lograr descifrar el contenido del paquete que ha sido enviado de forma segura por medio del túnel VPN?”.

Sin embargo, la utilización de la descripción del datagrama de entrada, ya está divulgada en el documento D3 que se refiere a que el cliente de red multiservicio proporciona un controlador de red privada virtual (VPN) para establecer una conexión VPN con un dispositivo de seguridad VPN remoto, donde el manejador de VPN encripta los paquetes de red salientes y descifra los paquetes de red entrantes para tunelizar de forma segura los paquetes de red entre el dispositivo móvil y el dispositivo de seguridad VPN remoto (Pág. 1, Fl. 16, Párr. 009).

En consecuencia, la persona del oficio normalmente versada en la materia, incluiría la descripción del datagrama de entrada del documento D3 en el método divulgado en el documento D1 para llegar así al objeto de la reivindicación 13 de la solicitud. Por lo cual se considera obvia.

La reivindicación 15 consiste en: “El método de la reivindicación 12, que además comprende (...)” (Ver página 5 del radicado N° NC2016/0000561 del 20 de diciembre de 2016).

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

Reiv.	Características esenciales	D1	D3

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Oficio N° 2178

Ref. Expediente N° NC2016/0000561

12	Un método para suministrar una arquitectura de vínculo seguro (...)	Ver Tabla 1.	Cliente de red integrado y multiservicio para dispositivos móviles celulares.
15	Suministrar una interfaz de usuario para establecer el primer túnel VPN a la estación de trabajo de cliente.	No se menciona	El cliente de red multiservicio comprende además un administrador de seguridad para recibir los paquetes de red entrantes descifrados del manejador VPN y aplicar al menos un servicio de seguridad a los paquetes de red descifrados, y una aplicación de control VPN que proporciona una interfaz de usuario unificada que permite al usuario para configurar tanto el controlador de VPN como el administrador de seguridad (Pág. 2, Fl. 17, Párr. 011).

El documento D1 se considera el estado de la técnica más cercano a la invención definida en la reivindicación 15 porque divulga un método y disposición para obtener un direccionamiento inequívoco para los paquetes de datos comunicados entre dispositivos (E1B, E3A) en dos redes locales diferentes (A, B) que utilizan espacios de direcciones IP privadas superpuestas (Fl. 1, resumen).

La diferencia entre la invención, definida en la reivindicación 13 y el método de D1 consiste en que el método de la reivindicación 15 posee una interfaz de usuario.

El efecto que logra el incluir una interfaz de usuario es poder establecer el primer túnel VPN a la estación de trabajo de cliente.

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Oficio N° 2178

Ref. Expediente N° NC2016/0000561

Por lo tanto, el problema técnico objetivo que pretende resolver esta invención se puede formular así: “¿cómo modificar el sistema conocido en D1 para lograr establecer el primer túnel VPN a la estación de trabajo de cliente?”.

Sin embargo, la utilización de una interfaz de usuario, ya está divulgada en el documento D3 que se refiere a que el cliente de red multiservicio comprende además un administrador de seguridad para recibir los paquetes de red entrantes descifrados del manejador VPN y aplicar al menos un servicio de seguridad a los paquetes de red descifrados, y una aplicación de control VPN que proporciona una interfaz de usuario unificada que permite al usuario para configurar tanto el controlador de VPN como el administrador de seguridad (Pág. 2, Fl. 17, Párr. 011).

En consecuencia, la persona del oficio normalmente versada en la materia, incluiría la interfaz de usuario del documento D3 en el método divulgado en el documento D1 para llegar así al objeto de la reivindicación 15 de la solicitud. Por lo cual se considera obvia.

La reivindicación 19 consiste en: “*El sistema de la reivindicación 18, en donde la lógica además (...)*” (Ver página 7 del radicado N° NC2016/0000561 del 20 de diciembre de 2016).

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

Reiv.	Características esenciales	D1	D3
18	Un sistema para suministrar una arquitectura de vínculo seguro (...)	Ver Tabla 2.	Cliente de red integrado y multiservicio para dispositivos móviles celulares.
19	Encriptar el datagrama de salida y transferir el datagrama de salida a la primera compuerta de propietario.	Una VPN se puede ver básicamente como un túnel encriptado a través de una red IP pública, para transferir paquetes de datos entre terminales y servidores (Pág. 1, Fl. 5, Párr. 006).	El cliente de red multiservicio proporciona un controlador de red privada virtual (VPN) para establecer una conexión VPN con un dispositivo de seguridad VPN remoto, donde el manejador de VPN encripta los paquetes
19	Recibir el datagrama de entrada en una forma	No se menciona	

Página 19 de 22

**REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO**

Oficio N° 2178

Ref. Expediente N° NC2016/0000561

	encriptada de la primera compuerta de propietario (120a) y descifrar el datagrama de entrada.		de red salientes y descifra los paquetes de red entrantes para tunelizar de forma segura los paquetes de red entre el dispositivo móvil y el dispositivo de seguridad VPN remoto (Pág. 1, Fl. 16, Párr. 009).
--	---	--	---

El documento D1 se considera el estado de la técnica más cercano a la invención definida en la reivindicación 19 porque divulga un método y disposición para obtener un direccionamiento inequívoco para los paquetes de datos comunicados entre dispositivos (E1B, E3A) en dos redes locales diferentes (A, B) que utilizan espacios de direcciones IP privadas superpuestas (Fl. 1, resumen).

La diferencia entre la invención, definida en la reivindicación 13 y el método de D1 consiste en que el sistema de la reivindicación 19 posee la descrición del datagrama de entrada.

El efecto que logra el incluir la descrición del datagrama de entrada es poder descifrar el contenido del paquete que ha sido enviado de forma segura por medio del túnel VPN.

Por lo tanto, el problema técnico objetivo que pretende resolver esta invención se puede formular así: “¿cómo modificar el sistema conocido en D1 para lograr descifrar el contenido del paquete que ha sido enviado de forma segura por medio del túnel VPN?”.

Sin embargo, la utilización de la descrición del datagrama de entrada, ya está divulgada en el documento D3 que se refiere a que el cliente de red multiservicio proporciona un controlador de red privada virtual (VPN) para establecer una conexión VPN con un dispositivo de seguridad VPN remoto, donde el manejador de VPN encripta los paquetes de red salientes y descifra los paquetes de red entrantes para tunelizar de forma segura los paquetes de red entre el dispositivo móvil y el dispositivo de seguridad VPN remoto (Pág. 1, Fl. 16, Párr. 009).

**REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO**

Oficio N° 2178

Ref. Expediente N° NC2016/0000561

En consecuencia, la persona del oficio normalmente versada en la materia, incluiría la descripción del datagrama de entrada del documento D3 en el método divulgado en el documento D1 para llegar así al objeto de la reivindicación 19 de la solicitud. Por lo cual se considera obvia.

7. Conclusión

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

Ítem	Documento	Reivindicaciones afectadas	Requisito que afecta
D1	US 2011/013641	12, 14, 16 y 18	Novedad/ Nivel inventivo
		1, 3, 13, 15 y 19	Nivel Inventivo
D2	US 2008/201486	1 y 5	Nivel inventivo
D3	US 2012/159607	13, 15 y 19	Nivel inventivo

En cumplimiento del artículo 45, de la Decisión 486 de la Comisión de la Comunidad Andina, 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 la solicitante llegara a modificar: i) el capítulo reivindicatorio, ii) la descripción de la invención a proteger, iii) o presente un nuevo capítulo reivindicatorio, y desee que se realice un nuevo examen de patentabilidad a esta modificación, no deberá pagar la tasa de modificación voluntaria pero sí la correspondiente a la tasa de examen de patentabilidad. En todo caso, el número de requerimientos por no patentabilidad estará supeditado a que el término del estudio de patentabilidad no sea superior a 18 meses, contados desde la publicación de la solicitud de patente de invención. Adicionalmente, se le recuerda a la solicitante que si como respuesta a este requerimiento llegara a modificar el capítulo reivindicatorio y éste contenga más de diez (10) reivindicaciones deberá pagar la tasa por reivindicación adicional.

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

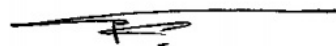
Oficio N° 2178

Ref. Expediente N° NC2016/0000561

Se invita a la solicitante se sirva indicar, si así lo considera, su renuncia al término faltante para los sesenta (60) días.

Notifíquese el presente oficio conforme a lo dispuesto en el Título I, Actuaciones ante la Superintendencia de Industria y Comercio; Capítulo sexto, publicación, comunicación, notificación y ejecutoria de las decisiones de la Superintendencia de Industria y Comercio, informándoles que contra el mismo no procede el recurso de la vía gubernativa.

Atentamente,



[DirectorName]
DIRECTOR DE NUEVAS CREACIONES

Elaborado: FERNANDO NICOLÁS VARGAS PLAZAS
Revisado: FERNANDO NICOLÁS VARGAS PLAZAS
Aprobado: JOSÉ LUIS SALAZAR LÓPEZ