

REIVINDICACIONES

1. Un método para calcular el análisis de red, caracterizado porque comprende las etapas de:

Recolectar (905), por un sistema de computadora (800), datos de múltiples diferentes tipos de fuentes, en donde los datos recolectados incluyen datos de la red y datos de recurso;

identificar, por el sistema de computadora (800) con base en los datos de la red en los datos recolectados, un evento de tráfico de la red y múltiples recursos de la red (915) relacionados con el evento de tráfico de la red;

identificar, por el sistema de computadora (800) con base en los datos de recurso en los datos recolectados, conexiones entre los múltiples recursos de la red (920); en el que una de las características de una conexión entre recursos de red o una característica de un recurso de red se identifica con base en un atributo seleccionado de los datos recolectados;

en respuesta a la detección, basada en los datos recolectados (905), un cambio en un atributo (420) de un primer recurso de red asociado con una primera zona lógica, moviendo (430) el primer recurso de red de la primera zona lógica a una segunda zona lógica, el movimiento comprende actualizar una base de datos para indicar que el primer recurso de red es un miembro de la segunda zona lógica, y en base a la membresía en la

segunda zona lógica, la comunicación entre el primer recurso de red y otros recursos de red está bloqueada;

generar, por el sistema de computadora (800), una gráfica de información de flujo (925) que representa los múltiples recursos de la red y las conexiones entre los múltiples recursos de la red, en donde los múltiples recursos de red incluyen el primer recurso de red y la información de flujo del gráfico representa el tráfico de red permitido entre los recursos de la red y el tráfico de la red que está bloqueado entre los recursos de la red;

presentar la gráfica de información de flujo (930) a través de una pantalla de una interfaz de usuario en comunicación con el sistema de computadora, en el que el gráfico de información de flujo representa conexiones entre los recursos de red empleando líneas de flujo direccional seleccionables; y

en respuesta a la selección (935), por un usuario a través de la interfaz de usuario, de una línea de flujo respectiva asociada a una conexión desde las múltiples conexiones, mostrando las características de la conexión seleccionada (940) incluyendo reglas de visualización para permitir y bloquear el tráfico sobre la conexión seleccionada.

2. El método de conformidad con la reivindicación 1, caracterizado porque los datos recolectados se obtienen de una fuente seleccionada del grupo que consiste de: un enrutador, un conmutador, un servidor de seguridad, un sistema de detección de intrusión, un sistema de protección de intrusión y combinaciones de los mismos.

3. El método de conformidad con la reivindicación 1, caracterizado además

porque comprende filtrar la información duplicada de los datos recolectados.

4. El método de conformidad con la reivindicación 1, caracterizado porque el atributo se selecciona por un usuario a través de la interfaz de usuario.

5. El método de conformidad con la reivindicación 1 caracterizado porque el atributo se selecciona automáticamente por el sistema de computadora.

6. El método de conformidad con la reivindicación 1, caracterizado porque las características de una conexión entre los recursos de la red y la característica de un recurso de la red se indica visualmente en la gráfica de información de flujo.

7. El método de conformidad con la reivindicación 1, caracterizado porque las líneas de flujo indican un tipo de la fuente de los datos recolectados empleados para identificar la conexión.

8. El método de conformidad con la reivindicación 1, caracterizado además porque comprende:

identificar características de las conexiones entre los recursos de la red (920).

9. El método de conformidad con la reivindicación 1, caracterizado además porque comprende:

recibir ediciones (945), del usuario a través de la interfaz de usuario, a las reglas mostradas para permitir y bloquear el tráfico sobre la conexión seleccionada; y aplicar las reglas editadas a la conexión seleccionada (950).

10. El método de conformidad con la reivindicación 1, caracterizado porque la generación de la gráfica de información de flujo (925) incluye:

identificar un recurso asociado con un tipo de vulnerabilidad de seguridad; e indicar visualmente el recurso identificado que se asocia con la vulnerabilidad de seguridad en la gráfica de información de flujo.

11. El método de conformidad con la reivindicación 1, caracterizado porque la gráfica de información de flujo representa la información en un recurso y uno o más de: los datos de la red asociados con el recurso, y un atributo operacional del sistema asociado con el recurso.

12. El método de conformidad con la reivindicación 1, caracterizado además porque comprende:

recolectar los datos actualizados (955);
actualizar la gráfica de información de flujo (960) basada en los datos actualizados;
y
presentar la gráfica de información de flujo actualizada (930) a través de la pantalla de la interfaz de usuario.

13. El método de conformidad con la reivindicación 1, caracterizado además porque comprende almacenar datos relacionados con la gráfica de información de flujo en respuesta a la entrada del usuario a través de la interfaz de usuario, en el que los datos relacionados con la gráfica de información de flujo incluyen uno de: los datos recolectados para generar la gráfica de información de flujo, y la gráfica de información de flujo misma.

14. El método de conformidad con la reivindicación 1, caracterizado además porque comprende:

analizar los datos recolectados (970); y

generar una alerta (975) en respuesta al análisis de los datos recolectados.

15. El método de conformidad con la reivindicación 14, caracterizado porque el análisis de los datos recolectados (970) incluye comparar los datos recolectados a uno o más de: una póliza de seguridad, una póliza de conformidad de normas y una norma de desempeño.

16. Un medio legible por computadora no transitorio, tangible (814), caracterizado porque almacena instrucciones que, cuando se ejecutan, provocan que un sistema de computadora (800):

recolecte datos (905) de múltiples diferentes tipos de fuentes, en donde los datos

recolectados incluyen datos de la red y datos de recursos;

identifique (915), con base en los datos de la red en los datos recolectados, un evento de tráfico de la red y múltiples recursos de la red relacionados con el evento del tráfico de la red;

identifique (920), con base en los datos de recursos en los datos recolectados, conexiones entre los múltiples recursos de la red, en el que una de las características de una conexión entre recursos de red o una característica de un recurso de red se identifica con base en un atributo seleccionado de los datos recolectados;

en respuesta a la detección, basada en los datos recolectados (905), un cambio en un atributo (420) de un primer recurso de red asociado con una primera zona lógica, moviendo (430) el primer recurso de red de la primera zona lógica a una segunda zona lógica, el movimiento comprende actualizar una base de datos para indicar que el primer recurso de red es un miembro de la segunda zona lógica, y en base a la membresía en la segunda zona lógica, la comunicación entre el primer recurso de red y otros recursos de red está bloqueada;

genere una gráfica de información de flujo (925) que representa los múltiples recursos de la red y las conexiones entre los múltiples recursos de la red, en donde los múltiples recursos de red incluyen el primer recurso de red y la información de flujo del gráfico representa el tráfico de red permitido entre los recursos de la red y el tráfico de la red que está bloqueado entre los recursos de la red;

presente la gráfica de información de flujo (930) a través de la pantalla de una interfaz de usuario en comunicación con el sistema de computadora, en el que el gráfico

de información de flujo representa conexiones entre los recursos de red empleando o líneas de flujo direccional seleccionables; y

en respuesta a la selección (935), por un usuario a través de la interfaz de usuario, de una línea de flujo respectiva asociada a una conexión desde las múltiples conexiones, mostrar las características de la conexión seleccionada (940) incluyendo reglas de visualización para permitir y bloquear el tráfico sobre la conexión seleccionada.

17. Un sistema de computadora (800), caracterizado porque comprende:

un procesador (812); y

memoria (814) en comunicación con el procesador y las instrucciones de almacenamiento que, cuando se ejecutan por el procesador, provocan que el sistema de computadora:

recolecte datos (905) de múltiples diferentes tipos de fuentes, en donde los datos recolectados incluyen datos de la red y datos de recursos;

identifique (915), con base en los datos de la red en los datos recolectados, un evento de tráfico de la red y múltiples recursos de la red relacionados con el evento de tráfico de la red;

identifique (920), con base en los datos de recursos en los datos recolectados, conexiones entre los múltiples recursos de la red, en el que una de las características de una conexión entre recursos de red o una característica de un recurso de red se identifica con base en un atributo seleccionado de los datos recolectados;

en respuesta a detectar, basado en los datos recolectados (905), un cambio en un atributo (420) de un primer recurso de red asociado con una primera zona lógica, moviendo (430) el primer recurso de red de la primera zona lógica a una segunda zona lógica, el movimiento comprende actualizar una base de datos para indicar que el primer recurso de red es un miembro de la segunda zona lógica, y en base a la membresía en la segunda zona lógica, la comunicación entre el primer recurso de red y otros recursos de red está bloqueada;

genere una gráfica de información de flujo (925) que representa los múltiples recursos de la red y las conexiones entre los múltiples recursos de la red, en donde los múltiples recursos de red incluyen el primer recurso de red y la información de flujo del gráfico representa el tráfico de red permitido entre los recursos de la red y el tráfico de la red que está bloqueado entre los recursos de la red; y

presente la gráfica de información de flujo (930) a través de una pantalla de una interfaz de usuario en comunicación con el sistema de computadora, en el que el gráfico de información de flujo representa conexiones entre los recursos de red empleando líneas de flujo direccional seleccionables; y

en respuesta a la selección (935), por un usuario a través de la interfaz de usuario, de una línea de flujo respectiva asociada a una conexión desde las múltiples conexiones, mostrar las características de la conexión seleccionada (940) incluyendo reglas de visualización para permitir y bloquear el tráfico sobre la conexión seleccionada.

P-13166

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO
DIRECCIÓN DE NUEVAS CREACIONES

E. S. D.

Re: Expediente No. **NC2017/0003261**
Solicitud de patente a nombre de **CATBIRD NETWORKS INC.**

Yo, CAROLINA DAZA MONTALVO identificada como aparece al pie de mi firma, domiciliada en la Carrera 11 No. 86-53, obrando como apoderada de la sociedad CATBIRD NETWORKS INC., solicitante de la patente de la referencia, en respuesta al oficio No. **12997** notificado el 31 de octubre de 2018, relacionado con concepto técnico de fondo, atentamente me permito manifestar:

1. Modificación a las Reivindicaciones

Con fundamento en la facultad que confiere el artículo 34 de la Decisión 486 al solicitante para modificar la solicitud de patente en cualquier momento del trámite, presento junto con este memorial nuevo capítulo reivindicatorio, el cual consta de 17 reivindicaciones y reemplaza completamente el capítulo presentado anteriormente. En el nuevo capítulo reivindicatorio se realizaron las siguientes modificaciones:

- 1.1.** Se modificó la dependencia de la antigua reivindicación 8, para ahora depender de la reivindicación independiente 1.
- 1.2.** En el nuevo capítulo reivindicatorio se eliminaron los términos imprecisos y que hacían referencia a un uso.

En cuanto a estas modificaciones, me permito decir que las mismas no amplían de ninguna manera la materia objeto de la presente solicitud y se realizaron con el ánimo de superar las objeciones de claridad planteadas por el examinador en su concepto técnico.

2. Pago de tasas

En relación con el número de reivindicaciones, atentamente nos permitimos decir que no se adjunta tasa por reivindicaciones adicionales, toda vez que el nuevo capítulo

reivindicatorio tiene un menor número de cláusulas que el originalmente presentado y es en esencia el mismo objeto, pero más limitado y definido con mayor claridad.

Por otra parte, no se adjunta recibo por concepto de examen de patentabilidad considerando que, aunque el presente memorial de respuesta se presenta junto con modificaciones al capítulo reivindicatorio, en donde dichas modificaciones a las reivindicaciones no son de carácter sustancial y no se incluye materia que no haya sido estudiada previamente.

3. Claridad

El artículo 30 de la Decisión 486 de la Comunidad Andina establece:

***Artículo 30.-** Las reivindicaciones definirán la materia que se desea proteger mediante la patente. Deben ser claras y concisas y estar enteramente sustentadas por la descripción.*

3.1 En relación a los términos referidos como términos relativos e imprecisos como “uno o más”, “pluralidad”, la solicitante desea manifestar respetuosamente que estos términos son usados para elementos en las antiguas reivindicaciones 1, 16 y 13, respectivamente, difiero respetuosamente de la opinión del Examinador en tanto que las expresiones “uno o más”, “pluralidad” o similares, establecen un alcance perfectamente entendible para cualquier persona medianamente versada en la materia, puesto que indican inequívocamente la cantidad mínima necesaria de elementos posibles que deben estar presentes en cada una de las configuraciones posibles de la invención reclamada. El uso de estos términos y otros análogos que indican la posibilidad de obtener la invención en diversas modalidades, es una práctica aceptada a nivel mundial en el ámbito de las patentes, ya que como el Examinador debe saberlo, una patente de invención no se limita a una única modalidad, si no que cubre un concepto inventivo global que abarca diferentes modalidades (diversas materializaciones de la invención) ligadas por un efecto técnico común que finalmente delimita el alcance de la invención.

Por ejemplo, este lenguaje se utiliza en situaciones donde se quiere evitar que un infractor trate de argumentar, por ejemplo, que un método para calcular el análisis de red comprenda una o más de las características de una conexión entre los recursos de la red, en lugar de todas las características de una conexión entre los recursos de la red reivindicado. Si se reclamara todas las características de una conexión entre los recursos de la red para el método para calcular el análisis de red, se estaría violando el derecho de un inventor de reclamar protección sobre la totalidad de su concepto inventivo, que en

este caso está soportado por la divulgación del Capítulo Descriptivo. En conclusión, en los casos donde se está haciendo uso de dicha expresión en el Capítulo Reivindicatorio Modificado adjunto, necesariamente la expresión corresponde a los elementos mínimos sobre las que actúan los componentes de la presente invención.

Por lo tanto, no debería existir problema alguno en el uso de las expresiones “uno o más”, “pluralidad”, pues es perfectamente entendible por cualquier persona medianamente versada en la materia, de tal manera que, a la luz del Capítulo Descriptivo, es perfectamente claro el alcance y los límites de la protección solicitada.

3.2 En relación con la objeción del uso de términos generales, me permito señalar respetuosamente que el Manual Andino de Patentes (MAP) y la Guía de Examen de Solicitudes de Patente y Modelos de Utilidad de la SIC, establecen que el lenguaje utilizado en una solicitud de patente debe ser el lenguaje común del campo técnico relacionado y su significado y alcance en las reivindicaciones, debe ser el que normalmente se da en el área técnica de la solicitud, siendo claro para la persona versada en la materia con su sola lectura, lo que cumple a cabalidad la presente solicitud. Así las cosas, las reivindicaciones de la presente solicitud son lo suficientemente claras y concisas precisando la materia reclamada, pues el uso de frases como *“de diferentes tipos de fuentes”*, *“atributo seleccionado de los datos recolectados”*, *“una primera zona lógica”*, *“segunda zona lógica”*, de la reivindicación 1, entre otros, pues a la luz del Capítulo Descriptivo resultan completamente reconocibles por cualquier persona medianamente versada en la materia.

Es más, a lo largo del Capítulo Descriptivo, dichos términos tienen los significados asociados explícitamente aquí, con el ánimo de establecer el alcance de ciertos términos y delimitar la interpretación de las características reclamadas en el presente invento.

Debe recordarse que la Descripción de una solicitud de patente debe servir para interpretar las reivindicaciones. En conclusión, una persona medianamente versada en la materia puede entender perfectamente el alcance y los límites de la protección solicitada, entendiendo qué elementos estructurales deben usarse para reproducir el invento y cuáles elementos están cobijados por las reivindicaciones y cuáles no.

Adicionalmente, es importante recordar que un inventor está en su derecho de reclamar

protección para la totalidad de un concepto inventivo desarrollado sin importar la amplitud de éste, siempre y cuando se guarde unidad de invención. Así las cosas, respetuosamente considero errada la objeción que el Examinador presenta en relación con los términos objetados, pues éstos indican claramente y de manera directa que tipo de característica estructural debe estar incluida en el método, sistema y producto reclamado.

Esto es, dentro del concepto inventivo desarrollado se contemplan modalidades sin apartarse del espíritu y alcance de la materia reivindicada. De nuevo, una persona versada en la materia puede entender perfectamente el alcance y los límites de la protección solicitada, entendiendo qué modalidades incluyen sustituciones y cuáles no, con base en la información divulgada en el Capítulo Descriptivo. Por lo demás, vale la pena anotar que el uso de estos términos y otros análogos que indican la posibilidad de obtener la invención en diversas modalidades, es una práctica aceptada a nivel mundial en el ámbito de las patentes, ya que como el Examinador debe saberlo, una patente de invención no se limita a una única modalidad, sino que cubre un concepto inventivo global que abarca diferentes modalidades (diversas materializaciones de la invención) ligadas por un efecto técnico común que finalmente delimita el alcance de la invención. Así las cosas, insisto respetuosamente que los términos objetados son perfectamente entendibles por cualquier persona medianamente versada en la materia, de tal manera que a la luz del Capítulo Descriptivo es perfectamente claro el alcance y los límites de la protección solicitada, entendiendo cuáles materializaciones están cobijadas por las reivindicaciones y cuáles no.

Adicionalmente, en línea con las modificaciones realizadas al Capítulo Reivindicatorio adjunto, se debe entender que el esquema de reivindicaciones de producto responde a una aproximación de “medios más función”, que define elementos estructurales mediante la relación funcional entre dichos elementos. Como el Examinador bien debe saberlo, este tipo de caracterización es permitido por los lineamientos de examen en Colombia. Específicamente, la Guía de Examen de Patentes y Modelos de Utilidad de la SIC, establece en el Capítulo 2.6.5.15 que se puede redactar una reivindicación por su función, siempre y cuando se precisen sus elementos estructurales. En el presente caso, se está reclamando el método y producto por sus características técnicas estructurales, y adicionalmente se le está añadiendo el carácter funcional de cada elemento estructural

reclamado.

3.3 En relación a la objeción del examinador en contra de las antiguas reivindicaciones 1, 4, 6, 10, 11, 12, 13, 14, 16 y 17, según la cual estas comprenden fragmentos considerados no patentables por referirse a formas de presentar información. Es deseo del solicitante manifestar respetuosamente su desacuerdo con la opinión del examinador, teniendo en cuenta que la invención se refiere a un método, un sistema y un medio legible por computador, en donde *el sistema, el medio legible y el método está definido por una secuencia lógica de pasos que definen elementos estructurales mediante la relación funcional entre dichos elementos y además comprende elementos estructurales tangibles, tales como un procesador, una memoria, entre otras, pero en la que además el aspecto de la gráfica de información de flujo es crucial, dado que el método, el sistema y el medio legible se basan en generar y presentar una gráfica de información de flujo.* En este sentido, la eliminación de los fragmentos en los cuales se hace referencia a dicha gráfica de información de flujo generaría una falta de claridad en las reivindicaciones, por cuanto *el objeto del método, sistema y medio legible, el cual consiste en calcular el análisis de red en respuesta a la detección, basada en los datos recolectados en la red, no podría ser explicado apropiadamente.* En otras palabras, *no se pretende reclamar protección sobre la presentación de una gráfica de información de flujo, teniendo en cuenta que la invención se relaciona con un método, sistema y medio legible, sin embargo, hacer referencia a esta es vital para que una persona versada en la materia entienda el funcionamiento y el propósito de dicho método, sistema y medio legible por computador.*

Adicional a lo anterior, de acuerdo con nuestra práctica actual, se permite una invención implementada por computador en Colombia siempre que dicha invención esté relacionada con un elemento tangible, que en el presente caso es aplicable. Por consiguiente, es deseo del solicitante manifestar su desacuerdo contra la opinión del examinador, *para indicar que las supuestas formas de presentar información corresponden a características esenciales de la invención, teniendo en cuenta que la invención está relacionada con el procesamiento de datos o el procesamiento de información a través de un medio o una computadora.* Además, podemos indicar que *el método es realizado por una máquina y está definido por una serie de pasos*

que llevan a obtener un resultado, como se define en la reivindicación 1, en donde el resultado corresponde a información diferente a la ingresada, es decir, hay una transformación, lo cual es claro para el experto en la materia. De igual forma, el medio legible por computadora al ejecutar sus instrucciones por medio de la computadora produce un efecto técnico que forma parte de la solución al problema técnico planteado. Teniendo en cuenta lo anterior, se solicita amablemente que la objeción formulada a este respecto se debe tener por superada.

En consecuencia, nos permitimos indicar que el presente capítulo reivindicatorio, que incluye 17 reivindicaciones, se ajusta a las disposiciones del artículo 30 de la Decisión 486/00.

4. Novedad

El examinador establece en su concepto técnico la falta de novedad por parte de las antiguas reivindicaciones 1 a 17, a la luz de las enseñanzas técnicas descritas en los documentos US 2009/327903 (D3), US7849497 (D4), US2008005784 (D5) y US 2005/193430 (D6).

En primer lugar, nos permitimos informar que el artículo 16 de la Decisión 486 establece que “Una invención se considerará nueva cuando no está comprendida en el estado de la técnica”.

Así las cosas, queda claro para el experto en la materia que el cumplimiento del requisito de novedad debe ser de forma TOTAL, lo que se conoce en el medio como Novedad Absoluta, esto significa que cuando existe por lo menos una diferencia entre la invención a analizar y el estado del arte, dicha invención definida en la reivindicación independiente cumplirá con el requisito en mención y se ajustará a las disposiciones del artículo 16 de la Decisión 486.

Aplicando lo anterior al caso concreto, para que las razones que aduce ese despacho para desvirtuar la novedad fuesen ciertas, sería forzoso que se demostrara que la invención de mi mandante esté comprendida en el estado de la técnica, específicamente en forma individual en los documentos D3 a D6 de forma TOTAL, lo cual no sucede con la materia reclamada en el nuevo capítulo reivindicatorio.

Considerando las anteriores definiciones, es deseo de la solicitante manifestar su desacuerdo con dichas objeciones y presentar argumentos que demuestran la novedad de la invención que se reclama en las reivindicaciones 1 a 17.

En primer lugar, se llama la atención del examinador frente a las modificaciones introducidas a las reivindicaciones, de forma que el método, el sistema y el medio legible por computadora se encuentran definidos de forma más clara y completa.

Las nuevas reivindicaciones independientes 1, 16 y 17 modificadas de la solicitud incluyen características técnicas esenciales no divulgadas o sugeridas en los documentos citados como D3, D4, D5 o D6. Como tal, las reivindicaciones de la presente invención son patentables sobre D3, D4, D5 y D6. En particular, las reivindicaciones independientes 1, 16 y 17 incluyen los elementos reivindicados de: presente la gráfica de información de flujo (930) a través de la pantalla de una interfaz de usuario en comunicación con el sistema de computadora, en el que el gráfico de información de flujo representa conexiones entre los recursos de red empleando o líneas de flujo direccional seleccionables; y en respuesta a la selección (935), por un usuario a través de la interfaz de usuario, de una línea de flujo respectiva asociada a una conexión desde las múltiples conexiones, mostrar las características de la conexión seleccionada (940) incluyendo reglas de visualización para permitir y bloquear el tráfico sobre la conexión seleccionada.

Ahora bien, el examinador usa el documento D3 únicamente para intentar mostrar las características reclamadas por el solicitante. Sin embargo, D3 no revela o sugiere las características reivindicadas por el solicitante de ***presentar la gráfica de información de flujo (930) a través de la pantalla de una interfaz de usuario en comunicación con el sistema de computadora, en el que el gráfico de información de flujo representa conexiones entre los recursos de red empleando o líneas de flujo direccional seleccionables; y en respuesta a la selección (935), por un usuario a través de la interfaz de usuario, de una línea de flujo respectiva asociada a una conexión desde las múltiples conexiones, mostrar las características de la conexión seleccionada (940) incluyendo reglas de visualización para permitir y bloquear el tráfico sobre la conexión seleccionada.*** Más bien, D3 simplemente se limita a revelar una vista de topología de una red. En particular, el objetivo de D3 es identificar y mostrar un flujo de red común mostrando una flecha para cada segmento de ruta de transmisión atravesado por la comunicación a través de la red (Ver Pars. 004-007 de D3).

El examinador hace referencia específicamente a D3 (Pars. 0087-0096) y a las Figuras 16-17 como la divulgación del reclamo del solicitante que presenta el gráfico de información

de flujo a través de una pantalla de una interfaz de usuario, **en respuesta a la selección (935), por un usuario a través de la interfaz de usuario, de una línea de flujo respectiva asociada a una conexión desde las múltiples conexiones, mostrar las características de la conexión seleccionada incluyendo reglas de visualización para permitir y bloquear el tráfico sobre la conexión seleccionada.**

Sin embargo, las Figuras 16-17 de D3 no son de una calidad aceptable para una solicitud de patente de EE. UU., Seguramente han sido rechazadas por la USPTO y no pueden utilizarse como base para un rechazo. Las figuras utilizan de forma inadmisiblemente el sombreado de los datos, lo que las hace ininteligibles. No se puede esperar que una persona razonable identifique la divulgación de los datos que se pretendía revelar en las figuras 16-17 de D3.

En donde D3, tampoco divulga los elementos reclamados por el solicitante. La sección más relevante de D3 (Ver Pars. 0087-0096) está limitada a revelar la terminación de una conexión. No hay nada en D3 que divulgue la presente reclamación de un gráfico de información a través de una pantalla de una interfaz de usuario, **en donde, en respuesta a la selección, de una línea de flujo respectiva asociada a una conexión desde las múltiples conexiones, mostrar las características de la conexión seleccionada incluyendo reglas de visualización para permitir y bloquear el tráfico sobre la conexión seleccionada.**

FIG. 16A muestra un ejemplo de la GUI 1300 que representa flujos de comunicación de red comunes sobre la vista de topología en la primera región de visualización 1303, de acuerdo con una realización de la presente invención. Los flujos de la red se visualizan mostrando la dirección de origen y destino como puntos finales y dibujando una cantidad de flechas 1601 que se extienden a través de la red entre las direcciones de origen y destino. Más específicamente, una flecha se dibuja desde una dirección de origen a una nube de subred. Luego, se dibuja una flecha desde la nube de subred a una interfaz de ingreso de un dispositivo de red. Luego, se dibuja una flecha a través del dispositivo de red desde la interfaz de ingreso a una interfaz de egreso. Luego, si es necesario, se dibujan flechas adicionales en otra nube de subred, y en otro dispositivo de red, y a través del otro dispositivo de red, etc. **Finalmente, se dibuja una flecha desde un dispositivo de red a la dirección de destino. Algunos flujos de red terminarán dentro de un enrutador al que está destinado o dentro del cual está bloqueado. Estos flujos de red mostrarán su punto de terminación dentro de la interfaz local o nula dentro del enrutador.** (énfasis añadido) (D3 [0087]).

Las reivindicaciones independientes 1, 16 y 17 del solicitante también incluyen las características reivindicadas de *identificar, por el sistema de computadora con base en los datos de recurso en los datos recolectados, conexiones entre los múltiples recursos de la red; en el que una de las características de una conexión entre recursos de red o una característica de un recurso de red se identifica con base en un atributo seleccionado de los datos recolectados.*

D3, D4, D5 y D6 *no revelan* reivindicadas de *identificar, por el sistema de computadora con base en los datos de recurso en los datos recolectados, conexiones entre los múltiples recursos de la red; en el que una de las características de una conexión entre recursos de red o una característica de un recurso de red se identifica con base en un atributo seleccionado de los datos recolectados.*

Específicamente, D3, D4, D5 y D6 simplemente proporcionan un sistema de mitigación de intrusión de seguridad que muestra información de configuración del árbol de red para determinar una acción para mitigar la difusión de ataques intrusivos.

En consecuencia, las reivindicaciones independientes 1, 16 y 17 del solicitante son patentables sobre los documentos D3, D4, D5 y D6, citados como la técnica anterior.

Las reclamaciones dependientes 2 a 15 del solicitante dependen de la reivindicación independiente 1 y respetuosamente son patentables al menos por las mismas razones discutidas anteriormente.

De esta forma, se demuestra que las nuevas reivindicaciones 1 a 17 cumplen con el requisito de novedad y nivel inventivo según los lineamientos del artículo 16 y 18 de la Decisión 486/00.

5. Conclusión

Con las modificaciones introducidas y los argumentos presentados puede concluirse que:

- i) La presente solicitud es clara, concisa y está debidamente soportada en la descripción, cumpliendo con los requerimientos del Artículo 30 de la Decisión 486; y
- ii) Las reivindicaciones actuales son patentables sobre D1 y D2, cumpliendo así con los requerimientos del Artículo 18 de la Decisión 486.

En consecuencia, se solicita atentamente otorgar el privilegio de patente solicitado, toda vez que esta solicitud cumple con los requerimientos de la Decisión 486.

Habiendo atendido cabalmente las objeciones presentadas por ese despacho, atentamente solicitamos se conceda el privilegio de patente de invención a la solicitud en estudio o si el señor examinador considera que subsisten razones para objetar la presente invención, rogamos expedir otro examen de fondo con los debidos motivos y razones que sustenten su objeción con el fin de que nuestro mandante tenga la posibilidad de exponer sus argumentos con base en la interpretación de los artículos 45 de la Decisión 486 -el cual otorga la facultad al examinador para emitir los exámenes de fondo- y 42 del Código de Procedimiento Administrativo y de lo Contencioso Administrativo que señala que: *“Habiéndose dado oportunidad a los interesados para expresar sus opiniones, y con base en las pruebas e informes disponibles, se tomará la decisión, que será motivada. La decisión resolverá todas las peticiones que hayan sido oportunamente planteadas dentro de la actuación por el peticionario y por los terceros reconocidos”*, (el subrayado es nuestro).

Finalmente, solicitamos a ese Despacho pronunciarse en relación con todos los argumentos presentados en este memorial dando estricta aplicación al principio del debido proceso consagrado en el artículo 29 de la Constitución Nacional.

6. Anexos

- Nuevo capítulo reivindicatorio que incluye 17 reivindicaciones.

Señor Director,


CAROLINA DAZA MONTALVO
C.C. 66.783.790 de Palmira Valle
TP-141563 CSJ
notificaciones@clarkemodet.com.co

www.clarkemodet.com

ESPAÑA · PORTUGAL · ARGENTINA · BRASIL · CHILE · COLOMBIA · MÉXICO · PERÚ · URUGUAY · VENEZUELA

REIVINDICACIONES

1. Un método para calcular el análisis de red, caracterizado porque comprende las etapas de:

Recolectar (905), por un sistema de computadora (800), datos de múltiples diferentes tipos de fuentes, en donde los datos recolectados incluyen datos de la red y datos de recurso;

identificar, por el sistema de computadora (800) con base en los datos de la red en los datos recolectados, un evento de tráfico de la red y múltiples recursos de la red (915) relacionados con el evento de tráfico de la red;

identificar, por el sistema de computadora (800) con base en los datos de recurso en los datos recolectados, conexiones entre los múltiples recursos de la red (920); en el que una de las características de una conexión entre recursos de red o una característica de un recurso de red se identifica con base en un atributo seleccionado de los datos recolectados;

en respuesta a la detección, basada en los datos recolectados (905), un cambio en un atributo (420) de un primer recurso de red asociado con una primera zona lógica, moviendo (430) el primer recurso de red de la primera zona lógica a una segunda zona lógica, el movimiento comprende actualizar una base de datos para indicar que el primer recurso de red es un miembro de la segunda zona lógica, y en base a la membresía en la segunda zona lógica, la comunicación entre el primer recurso de red y otros recursos de red está bloqueada;

generar, por el sistema de computadora (800), una gráfica de información de flujo (925) que representa los múltiples recursos de la red y las conexiones entre los múltiples

recursos de la red, en donde los múltiples recursos de red incluyen el primer recurso de red y la información de flujo del gráfico representa el tráfico de red permitido entre los recursos de la red y el tráfico de la red que está bloqueado entre los recursos de la red;

presentar la gráfica de información de flujo (930) a través de una pantalla de una interfaz de usuario en comunicación con el sistema de computadora, en el que el gráfico de información de flujo representa conexiones entre los recursos de red empleando líneas de flujo direccional seleccionables; y

en respuesta a la selección (935), por un usuario a través de la interfaz de usuario, de una línea de flujo respectiva asociada a una conexión desde las múltiples conexiones, mostrando las características de la conexión seleccionada (940) incluyendo reglas de visualización para permitir y bloquear el tráfico sobre la conexión seleccionada.

2. El método de conformidad con la reivindicación 1, caracterizado porque los datos recolectados se obtienen de una fuente seleccionada del grupo que consiste de: un enrutador, un conmutador, un servidor de seguridad, un sistema de detección de intrusión, un sistema de protección de intrusión y combinaciones de los mismos.

3. El método de conformidad con la reivindicación 1, caracterizado además porque comprende filtrar la información duplicada de los datos recolectados.

4. El método de conformidad con la reivindicación 1, caracterizado porque el atributo se selecciona por un usuario a través de la interfaz de usuario.

5. El método de conformidad con la reivindicación 1 caracterizado porque el atributo se selecciona automáticamente por el sistema de computadora.

6. El método de conformidad con la reivindicación 1, caracterizado porque las características de una conexión entre los recursos de la red y la característica de un recurso de la red se indica visualmente en la gráfica de información de flujo.

7. El método de conformidad con la reivindicación 1, caracterizado porque las líneas de flujo indican un tipo de la fuente de los datos recolectados empleados para identificar la conexión.

8. El método de conformidad con la reivindicación 1, caracterizado además porque comprende:

identificar características de las conexiones entre los recursos de la red (920).

9. El método de conformidad con la reivindicación 1, caracterizado además porque comprende:

recibir ediciones (945), del usuario a través de la interfaz de usuario, a las reglas mostradas para permitir y bloquear el tráfico sobre la conexión seleccionada; y

aplicar las reglas editadas a la conexión seleccionada (950).

10. El método de conformidad con la reivindicación 1, caracterizado porque la generación de la gráfica de información de flujo (925) incluye:

identificar un recurso asociado con un tipo de vulnerabilidad de seguridad; e

indicar visualmente el recurso identificado que se asocia con la vulnerabilidad de seguridad en la gráfica de información de flujo.

11. El método de conformidad con la reivindicación 1, caracterizado porque la gráfica de información de flujo representa la información en un recurso y uno o más

de: los datos de la red asociados con el recurso, y un atributo operacional del sistema asociado con el recurso.

12. El método de conformidad con la reivindicación 1, caracterizado además porque comprende:

recolectar los datos actualizados (955);

actualizar la gráfica de información de flujo (960) basada en los datos actualizados;

y

presentar la gráfica de información de flujo actualizada (930) a través de la pantalla de la interfaz de usuario.

13. El método de conformidad con la reivindicación 1, caracterizado además porque comprende almacenar datos relacionados con la gráfica de información de flujo en respuesta a la entrada del usuario a través de la interfaz de usuario, en el que los datos relacionados con la gráfica de información de flujo incluyen uno de: los datos recolectados para generar la gráfica de información de flujo, y la gráfica de información de flujo misma.

14. El método de conformidad con la reivindicación 1, caracterizado además porque comprende:

analizar los datos recolectados (970); y

generar una alerta (975) en respuesta al análisis de los datos recolectados.

15. El método de conformidad con la reivindicación 14, caracterizado porque el análisis de los datos recolectados (970) incluye comparar los datos recolectados a uno o más de: una póliza de seguridad, una póliza de conformidad de normas y una norma

de desempeño.

16. Un medio legible por computadora no transitorio, tangible (814), caracterizado porque almacena instrucciones que, cuando se ejecutan, provocan que un sistema de computadora (800):

recolecte datos (905) de múltiples diferentes tipos de fuentes, en donde los datos recolectados incluyen datos de la red y datos de recursos;

identifique (915), con base en los datos de la red en los datos recolectados, un evento de tráfico de la red y múltiples recursos de la red relacionados con el evento del tráfico de la red;

identifique (920), con base en los datos de recursos en los datos recolectados, conexiones entre los múltiples recursos de la red, en el que una de las características de una conexión entre recursos de red o una característica de un recurso de red se identifica con base en un atributo seleccionado de los datos recolectados;

en respuesta a la detección, basada en los datos recolectados (905), un cambio en un atributo (420) de un primer recurso de red asociado con una primera zona lógica, moviendo (430) el primer recurso de red de la primera zona lógica a una segunda zona lógica, el movimiento comprende actualizar una base de datos para indicar que el primer recurso de red es un miembro de la segunda zona lógica, y en base a la membresía en la segunda zona lógica, la comunicación entre el primer recurso de red y otros recursos de red está bloqueada;

genere una gráfica de información de flujo (925) que representa los múltiples recursos de la red y las conexiones entre los múltiples recursos de la red, en donde los múltiples recursos de red incluyen el primer recurso de red y la información de flujo del gráfico representa el tráfico de red permitido entre los recursos de la red y el tráfico de la red que está bloqueado entre los recursos de la red;

presente la gráfica de información de flujo (930) a través de la pantalla de una interfaz de usuario en comunicación con el sistema de computadora, en el que el gráfico de información de flujo representa conexiones entre los recursos de red empleando o líneas de flujo direccional seleccionables; y

en respuesta a la selección (935), por un usuario a través de la interfaz de usuario, de una línea de flujo respectiva asociada a una conexión desde las múltiples conexiones, mostrar las características de la conexión seleccionada (940) incluyendo reglas de visualización para permitir y bloquear el tráfico sobre la conexión seleccionada.

17. Un sistema de computadora (800), caracterizado porque comprende:

un procesador (812); y

memoria (814) en comunicación con el procesador y las instrucciones de almacenamiento que, cuando se ejecutan por el procesador, provocan que el sistema de computadora:

recolecte datos (905) de múltiples diferentes tipos de fuentes, en donde los datos recolectados incluyen datos de la red y datos de recursos;

identifique (915), con base en los datos de la red en los datos recolectados, un evento de tráfico de la red y múltiples recursos de la red relacionados con el evento de tráfico de la red;

identifique (920), con base en los datos de recursos en los datos recolectados, conexiones entre los múltiples recursos de la red, en el que una de las características de una conexión entre recursos de red o una característica de un recurso de red se identifica con base en un atributo seleccionado de los datos recolectados;

en respuesta a detectar, basado en los datos recolectados (905), un cambio en un atributo (420) de un primer recurso de red asociado con una primera zona lógica,

moviendo (430) el primer recurso de red de la primera zona lógica a una segunda zona lógica, el movimiento comprende actualizar una base de datos para indicar que el primer recurso de red es un miembro de la segunda zona lógica, y en base a la membresía en la segunda zona lógica, la comunicación entre el primer recurso de red y otros recursos de red está bloqueada;

genere una gráfica de información de flujo (925) que representa los múltiples recursos de la red y las conexiones entre los múltiples recursos de la red, en donde los múltiples recursos de red incluyen el primer recurso de red y la información de flujo del gráfico representa el tráfico de red permitido entre los recursos de la red y el tráfico de la red que está bloqueado entre los recursos de la red; y

presente la gráfica de información de flujo (930) a través de una pantalla de una interfaz de usuario en comunicación con el sistema de computadora, en el que el gráfico de información de flujo representa conexiones entre los recursos de red empleando líneas de flujo direccional seleccionables; y

en respuesta a la selección (935), por un usuario a través de la interfaz de usuario, de una línea de flujo respectiva asociada a una conexión desde las múltiples conexiones, mostrar las características de la conexión seleccionada (940) incluyendo reglas de visualización para permitir y bloquear el tráfico sobre la conexión seleccionada.