

PROTECCIÓN DE LOS DISPOSITIVOS DE RED POR UN CORTAFUEGOS

REFERENCIA CRUZADA A SOLICITUDES RELACIONADAS

- 5 Esta solicitud reivindica el beneficio de y prioridad a la Solicitud de Patente de E.U.A. No. de Serie 15/053,422, presentada el 25 de febrero de 2016 y Solicitud Provisional de E.U.A. No. de Serie 62/292,702, presentada el 8 de febrero de 2016, por Glazemakers et al., los contenidos completos de cuya solicitud se incorpora como referencia como si se estableciera completamente en la presente.

CAMPO DE LA INVENCION

- 10 Al menos algunas modalidades generalmente se refieren al campo de protección de red y más particularmente, pero no limitado a, la protección de redes privadas por una puerta de enlace que incluye un servidor de túnel tal como un servidor VPN (siglas en inglés de Red Privada Virtual) y un cortafuegos (firewall, programa de seguridad).

ANTECEDENTES DE LA INVENCION

- 15 Con objeto de proteger las redes privadas del acceso a redes no deseadas, un cortafuegos puede implementarse en una puerta de enlace con objeto de filtrar selectivamente la comunicación desde y hasta la red privada. Al aplicar reglas del cortafuegos, el cortafuegos entonces deja pasar los paquetes de red, o los bloquea en una o ambas direcciones. Las reglas se definen típicamente por la fuente y/o direcciones de destino de los paquetes de red,
20 o la fuente y/o puertos de destino de los paquetes de red.

- Un cortafuegos puede realizar además inspección del paquete con control de estado por ello mantiene un seguimiento del estado de las conexiones de red tales como, por ejemplo, conexiones de red TCP o UDP. De esta manera, un control detallado es posible ya que las reglas se vuelven dependientes sobre la conexión de red y de esta manera dinámica.
- 25 El cortafuegos mantiene el seguimiento de todas las conexiones de red abiertas al mantener una tabla, la tabla de estado o lista de estado, con todas las conexiones pendientes.

- Con objeto de tener mejor control sobre el tráfico de red que pasa por una puerta de enlace, el cortafuegos puede realizar además inspección profunda de paquetes al controlar los datos de carga útil de los paquetes de red. De esta manera, pueden implementarse diferentes
- 30 tipos de control tales como, por ejemplo, acceso o autorización del usuario, cumplimiento del protocolo, filtrado de correo no solicitado y detección de virus.

- Con objeto de proteger una red privada adicional, el cortafuegos de puerta de enlace puede combinarse con túnel de red. El acceso a la red privada luego puede estabilizarse por una VPN (Red Privada Virtual) donde un túnel de red segura se establece entre un dispositivo
- 35 de cliente y la puerta de enlace. La configuración de dicho túnel se garantiza únicamente durante la autenticación exitosa con la puerta de enlace, que entonces funciona como un servidor VPN. Por la combinación de un cortafuegos y servidor de VPN en la puerta de enlace,

el acceso a los dispositivos en la red privada puede autorizarse sobre un nivel de cliente o uno de usuario por el servidor VPN y sobre un nivel de red por el cortafuegos.

BREVE DESCRIPCIÓN DE LA INVENCION

5 Diversos problemas pueden surgir con sistemas de puerta de enlace combinados como se describe anteriormente. Primero, la cantidad de reglas de cortafuegos incrementará con cada usuario adicional, haciendo la gestión de todas las reglas difíciles para sistemas grandes. Debido a esto, cada paquete entrante tendrá que procesarse contra todas estas reglas.

10 Un segundo problema se relaciona con el sistema de recuperación de fallos de la puerta de enlace. En un esquema de recuperación de fallos, conocido como sistema de recuperación de fallos pasivo, toda la información en la puerta de enlace (es decir, reglas de cortafuegos, lista de estado y túneles de red activos) se sincroniza constantemente con una segunda puerta de enlace redundante. Si existe una falla de la primera puerta de enlace, la segunda puerta de enlace se toma automáticamente de la primera puerta de enlace. Debido a la sincronización, no se pierden conexiones de red activas durante el sistema de recuperación
15 de fallos.

En otro esquema de recuperación de fallos, referido como sistema de recuperación de fallos activo, diversas puertas de enlace también se sincronizan uno con el otro, pero todas son activas al mismo tiempo de manera que la carga puede equilibrarse entre las puertas de enlace. También, en este caso, debido a la sincronización, una puerta de enlace puede tomar
20 todas las conexiones de otra puerta de enlace durante la falla sin perder las conexiones de red.

Un problema con los dos esquemas es la escalabilidad debido a que el sistema no se puede escalar al agregar solo nuevas puertas de enlace. Primero, el ancho de banda entre las puertas de enlace necesario para la sincronización incrementará exponencialmente con la cantidad o número de puertas de enlace. Segundo, debido a que la lista de estado se
25 mantiene sincronizada, el tamaño de la lista de estado y las reglas de cortafuegos para cada puerta de enlace también incrementarán linealmente cuando se escala. Debido a esto, el ancho de banda necesario, energía de procesamiento y espacio de memoria de cada puerta de enlace incrementará cuando se agrega una nueva puerta de enlace.

30 Varias modalidades se describen en la presente que alivian los problemas anteriores y proporcionan una puerta de enlace que puede graduarse y gestionarse en una manera fácil e inequívoca. Algunas modalidades se resumen en esta sección.

Las modalidades de la presente descripción ayudan a proteger los dispositivos de red de acceso no autorizado. Entre otras cosas, las modalidades de la descripción permiten el acceso completo a los servidores de la aplicación y otros dispositivos de red que un cliente
35 está autorizado para acceder, mientras que previene todo el acceso (o incluso el conocimiento) de los dispositivos de red al que el cliente no está autorizado para acceder.

Un método implementado en computadora de acuerdo con una modalidad de la

presente descripción incluye: luego de 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, luego de establecer el túnel de red, partiendo de un servicio de cortafuegos separado con un conjunto separado de reglas de 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.

La presente descripción incluye varios métodos, aparatos (que incluyen sistemas informáticos) que realizan dichos métodos, y medios legibles en computadora que contienen instrucciones que, cuando se ejecutan por sistemas informáticos, provoca que los sistemas informáticos realicen dichos métodos.

Otras características serán aparentes de los dibujos acompañantes y de la descripción detallada que sigue.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

Las modalidades se ilustran a manera de ejemplo y sin limitación en las figuras de los dibujos acompañantes en las cuales las referencias similares indican elementos similares.

La FIGURA 1 es un sistema ejemplar para la protección de los dispositivos de red de acceso a la red no deseada de acuerdo con varios aspectos de la presente descripción.

La FIGURA 2 es un proceso ejemplar para establecer un túnel de red entre un dispositivo de cliente y una red privada que puede ejecutarse por componentes de la presente descripción.

La FIGURA 3 es un proceso ejemplar para distribuir servicios de cortafuegos entre diferentes núcleos del procesador de un sistema informático que implementa una puerta de enlace de acuerdo con una modalidad.

La FIGURA 4 es un sistema ejemplar para el establecimiento de un túnel de red entre un dispositivo de cliente y una red privada separada por una puerta de enlace que implementa un servicio de cortafuegos de acuerdo con una modalidad.

La FIGURA 5 es un proceso ejemplar para sincronizar un cortafuegos implementado sobre una puerta de enlace que puede ejecutarse por componentes de la presente descripción.

La FIGURA 6 es un sistema ejemplar que incluye una pluralidad de puertas de enlace para la protección de los dispositivos de red de acceso a la red no deseada de acuerdo con varios aspectos de la presente descripción.

La FIGURA 7 es un proceso ejemplar para transferir sin problemas un servicio de cortafuegos de una puerta de enlace a otra puerta de enlace ejecutada por componentes de la presente descripción.

La FIGURA 8 ilustra un sistema informático ejemplar de acuerdo con varios aspectos de la presente descripción.

DESCRIPCIÓN DETALLADA DE LA INVENCION

La materia objeto ahora se describirá más completamente de aquí en adelante con referencia a los dibujos acompañantes, que forman una parte de la misma, y que muestran, a manera de ilustración, modalidades de ejemplo específico. La materia objeto puede, sin embargo, ser incorporado en una variedad de diferentes formas y, por lo tanto, la materia objeto cubierta o reivindicada se pretende para construirse ya que no se limita por ninguna de las modalidades ejemplares establecidas en la presente; las modalidades ejemplares se proporcionan meramente para ser ilustrativas. Del mismo modo, se pretende un alcance razonablemente amplio para la materia objeto reivindicada o cubierta. Entre otras cosas, por ejemplo, la materia objeto puede incorporarse como métodos, dispositivos, componentes, o sistemas. En consecuencia, las modalidades pueden, por ejemplo, tomar la forma de hardware, software, firmware o cualquier combinación de los mismos (diferentes de software en sí). La siguiente descripción detallada, por lo tanto, no se pretende para tomarse en un sentido limitante.

En los dibujos acompañantes, algunas características pueden exagerarse para mostrar detalles de componentes particulares (y cualquier tamaño, material y detalles similares mostrados en las figuras se pretenden para ser ilustrativos y no restrictivos). Por lo tanto, los detalles funcionales y estructurales específicos descritos en la presente no son para incorporarse como limitantes, sino meramente como una base representativa para enseñar a un experimentado en la técnica para emplear diversamente las modalidades descritas.

La referencia en esta especificación a “una modalidad” o “una modalidad” significa que una característica particular, estructura, o característica descrita en conexión con la modalidad se incluye en al menos una modalidad de la descripción. Las apariencias de la frase “en una modalidad” en varios lugares en la especificación no son necesariamente todas referidas en la misma modalidad, ni son separadas o modalidades alternativas mutuamente exclusivas de otras modalidades. Además, varias características se describen que pueden exhibirse por algunas modalidades y no por otras. De manera similar, varios requerimientos se describen que pueden ser requerimientos para algunas modalidades pero sin otras modalidades.

Cualquier combinación y/o subconjunto de los elementos de los métodos representados en la presente puede combinarse uno con el otro, selectivamente realizado o no realizado con base en varias condiciones, repetidas cualquier número deseado de veces, y practicadas en cualquier orden adecuado y en conjunto con cualquier sistema, dispositivo, y/o proceso adecuado. Los métodos descritos y representados en la presente pueden implementarse en cualquier manera adecuada, tal como a través de software que opera en uno o más sistemas informáticos. El software puede comprender instrucciones legibles en computadora almacenadas en un medio legible en computadora tangible (tal como la memoria de un sistema informático) y puede ejecutarse por uno o más procesadores para realizar los métodos de varias modalidades.

La FIGURA 1 ilustra un sistema ejemplar para la protección de los dispositivos de red de acceso a la red no deseada de acuerdo con varios aspectos de la presente descripción. En este ejemplo, tres dispositivos de red (servidores de aplicación 141, 142 y 143) son parte de una red privada 140. El acceso a los servidores 141-143 se obtiene desde dentro de la red privada 140 por medio de una dirección de red privada. En este contexto, el término “privada” se refiere al hecho de que los servidores de aplicación 141-143 no son enrutables globalmente. En otras palabras, los servidores de aplicación 141-143 no pueden ser direccionados por su dirección de red privada desde afuera de la red privada 140.

La red privada 140 y otros componentes en la FIGURA 1 puede utilizar cualquier número y tipo de protocolos de comunicación, también referido como el Protocolo de Internet (“IP”), o como el Protocolo de Control de Transmisión/Protocolo de Internet (“TCP/IP”). Por ejemplo, la red privada 140 puede tener intervalos de dirección como se establece por RFC 1918 para el Protocolo de Internet Versión 4 o IPv4 y RFC 4193 para el Protocolo de Internet Versión 6 o IPv6.

Los dispositivos de red 141-143 pueden corresponder a servidores de aplicación que proporcionan servicios sobre la red 140 a otros dispositivos de computación. Cualquier número y tipo de servidores de aplicación y servicios asociados pueden utilizarse en conjunto con modalidades de la presente descripción, tal como servidores de correo, servidores de campo, Gestión de Relaciones con Clientes o servicios CRM, Planeación de Recurso Empresariales o servicios ERP, y/o servicios de gestión de documentos.

Una conexión de datos luego puede establecerse con cualquiera de los servidores de aplicación 141-143 al abrir un enchufe de comunicación con el servidor de aplicación respectivo sobre un puerto (o intervalo de puerto) asociado con el servidor. Los servidores de aplicación 141-143 pueden corresponder a dispositivos físicos con una interfaz de red física asociada con una dirección de red privada. Alternativamente, los servidores de aplicación 141-143 también pueden corresponder a instancias de servidores virtuales que se ejecutan sobre uno o más servidores físicos. Las instancias del servidor virtual pueden cada uno tener una interfaz de red virtual con una dirección de red privada asociada. Las instancias del servidor virtual pueden incluir, así como operar en conjunto con, una o más instancias de espacio del usuario (también conocido como recipientes de software, motores virtuales, servidores privados virtuales, y/o cárceles). Dichas instancias de espacio del usuario pueden implementarse en cualquier manera adecuada, incluyendo, por ejemplo, por medio de la herramienta de software DOCKER.

En el ejemplo mostrado en la FIGURA 1, la red privada 140 se separa de una red externa por una puerta de enlace 100, por ello permite el tráfico de red entre la red externa y la red privada 140 en una forma controlada. El sistema de la FIGURA 1 puede identificar clientes 121-126 como “clientes de confianza” que tienen derechos de acceso a uno o más de los

servidores de aplicación 141-143 dentro de la red privada 140 con objeto de usar los servicios que se ejecutan en ellos. Los clientes 121-126 pueden ser, o incluir, hardware físico y/o componentes virtuales. Por ejemplo, un cliente 121-126 puede incluir un sistema operativo virtual que se ejecuta sobre un dispositivo físico, tal como un dispositivo móvil. El sistema también puede garantizar acceso a la red para una selección de los servidores de aplicación 141-143 los cuales los clientes 121-126 se permitieron acceder, y denegar el acceso a la red a cualquier servidor de aplicación a los clientes 121-126 no se les permitió el acceso.

Con objeto de controlar el acceso por los clientes 121-126 a los servidores de aplicación 141-143, los túneles de red 131-133 se establecen entre los clientes 121-126 y la puerta de enlace 100. De esta manera, la red privada 140 se extiende a los clientes 121-126. En algunas modalidades, una red privada virtual (o “VPN”) se establece a través de túneles 131-133. De esta manera, un cliente 121-126, aunque no físicamente en la red privada 140, se proporciona una dirección de red privada en el intervalo de la red privada 140, y puede de esta manera acceder potencialmente a todos los servidores de aplicación 141-143 por su dirección de red privada respectiva (se permite acceso proporcionado, como se discute en más detalle a continuación).

Todas las peticiones de la conexión de red inicial de los clientes 121-126 son manejados por el módulo de túnel 101 implementado en la puerta de enlace 100. En una modalidad, el módulo de túnel 101 mira en la conexión inicial (por ejemplo, típicamente un primer paquete TLS que está llegando) y luego determina si transfiere la conexión al módulo de gestión 102 (discutida a continuación) en el caso de metadatos, o para uno de los servicios de túnel 150, 151 (discutidos a continuación) en el caso del tráfico de túnel actual (es decir, datos) de los clientes. Una vez que la conexión se entrega (por ejemplo, esto puede hacerse al pasar sobre un descriptor de campo para el módulo de gestión 102 o uno de los módulos de servicio de túnel), el módulo de túnel 101 ya no se involucra. Luego, la conexión va directamente del cliente al módulo de gestión 102, o al servicio de túnel seleccionado 150, 151.

La petición de conexión de red inicial puede ser una petición de conexión para establecer un nuevo túnel por un nuevo dispositivo del cliente o una nueva petición de conexión de red dentro de un túnel existente. Los datos que viajan sobre las conexiones en los túneles 131-133 pueden protegerse además por encriptación, tal como de acuerdo con la Seguridad de Protocolo de Internet (o “protocolo IPsec,”) Seguridad de Capa de Transporte (o “TLS”) y/o Seguridad de Capa de Transporte de Datagram (o “DTLS”). En un ejemplo, el módulo de túnel 101 opera de acuerdo con TLS o SSL y establece las conexiones de red como conexiones de red TCP. Con objeto de hacerlo así, los clientes envían la petición a un puerto abierto o intervalo de puerto de la puerta de enlace 100, preferiblemente el puerto estándar 443 para conexiones TCP encriptadas TLS/SSL.

La puerta de enlace 100 implementa además servicios de cortafuegos 111-116. Cada servicio cortafuegos respectivo entonces implementa un cortafuegos para selectivamente bloquear y permitir el tráfico de red entre el dispositivo del cliente respectivo y los dispositivos de red 141-143 en la red privada. Cada servicio de cortafuegos también comprende un conjunto de reglas de cortafuegos que definen las reglas de acceso para un dispositivo del cliente respectivo. En otras palabras, la puerta de enlace 100 ejecuta un cortafuegos separado para cada cliente conectado 121-126. Una ventaja de esto es que el tamaño de las reglas de cortafuegos de un servicio de cortafuegos no crece con la cantidad de clientes conectados. De esta manera, un incremento en clientes conectados no resulta en una pérdida de rendimiento debido a un incremento en la cantidad de reglas de cortafuegos que tienen que ser gestionados por un servicio de cortafuegos sencillo.

La FIGURA 2 muestra un proceso ejemplar que puede ejecutarse por componentes de la presente descripción que incluye la puerta de enlace 100 de acuerdo con la FIGURA 1. Por este proceso, un dispositivo de cliente 121-126 se conecta a la red privada 140 a través de la puerta de enlace 100. Como un ejemplo, el proceso se describirá con referencia al dispositivo del cliente 121. En una primera etapa 201, el módulo de túnel 101 recibe una primera petición de conexión del dispositivo de red del cliente 121 para establecer una primera conexión de red con la puerta de enlace 100, por ejemplo una petición de conexión de red TCP asegurada recibida en el puerto 443 de la puerta de enlace. Luego, la conexión de red se establece bajo la etapa 202, por ejemplo, por un protocolo de intercambio de tres vías en el caso de una conexión de red TCP. Esta primera conexión de red se utiliza para intercambiar la información de control entre el cliente 121 y la puerta de enlace 100, y más particularmente con el módulo de gestión 102 implementado en la puerta de enlace 100. Con objeto de conocer que la conexión es para propósitos de control, el módulo de túnel puede inspeccionar el primer paquete de datos intercambiado sobre cada conexión de red recién establecida. Si el paquete de datos es un paquete de datos de control, el módulo de túnel 101 identifica la conexión de red como una conexión de control y redireccionará todos los paquetes adicionales recibidos sobre esta conexión para el módulo de gestión 102. El paquete de datos de control puede, por ejemplo, identificarse al inspeccionar un campo de extensión TSL específico en el encabezado del paquete TLS.

En la siguiente etapa 203, el módulo de gestión 102 recibe información del túnel del dispositivo del cliente 121 sobre la primera conexión de red. Esta información se refiere además como la lista de túnel del cliente. Esta lista de túnel del cliente incluye información con objeto de establecer el túnel de red 131 con la puerta de enlace tal como, por ejemplo, información de autenticación para autenticar el cliente con la puerta de enlace. Después de la autenticación exitosa por el módulo de gestión 102, el proceso procede a la etapa 204.

En la etapa 204, el módulo de gestión 102 recibe una lista de acceso de clientes del

cliente 121. Esta lista de acceso de clientes comprende una lista de los dispositivos de red o aplicaciones en la red privada 140 ya que el dispositivo del cliente se permite para acceder. Esta lista puede, por ejemplo, comprender una dirección de red tal como una dirección de red IPv4 o IPv6 que identifica el dispositivo de red respectivo en la red privada 140. También, un número de puerto o intervalo de número de puerto puede especificarse con objeto de limitar el acceso al dispositivo de red respectivo a una o más aplicaciones específicas. La lista también puede identificar el dispositivo de red respectivo por su nombre de host o por un nombre de dominio completamente calificado (FQDN). La lista también puede identificar el dispositivo de red respectivo indirectamente al especificar un servicio adicional de donde uno o más dispositivos de red respectivos pueden recibirse. Dicho servicio puede, por ejemplo, ser los Servicios Web Amazon que permiten recuperación de una lista de los dispositivos de red utilizando el AWS REST API de acuerdo con metadatos asignados a instancias virtuales en la nube Amazon.

El cliente 121 puede recuperar además esta lista de acceso de clientes y/o lista de túnel de un servicio de autenticación que gestiona el acceso del cliente a la red privada 140. Con objeto de evitar una situación en la cual el cliente compromete la lista de acceso de cliente y/o lista de túnel, las listas pueden hacerse inalterables (es decir, protegidos de manera que una alteración de una o ambas de las listas pueden detectarse por el módulo de gestión 102).

Varios métodos y sistemas para autenticar el cliente y proporcionar una lista de túnel y cliente se describen además en la Patente de E.U.A. No. US 9,148,408 B1, que se incorpora por ello como referencia en su totalidad.

Luego, en la etapa 205, el módulo de túnel 101 establece una segunda conexión de red con el cliente 121 durante la petición del cliente 121. Ya que esta es una nueva conexión, el módulo de túnel 101 inspecciona el primer paquete de datos recibido sobre esta segunda conexión. Esta segunda conexión se utiliza para el túnel de red actual 131 debido a que el cliente 121 ya ha establecido la primera conexión para el intercambio de control información con la puerta de enlace 100. El paquete de datos inspeccionado por lo tanto se identifica como un primer paquete para el túnel de red aún no establecido 131.

Más específicamente, en una modalidad, dos conexiones se requieren para cada túnel (131, 132, 133) (por ejemplo, dos conexiones TCP en el caso de un túnel TLS). Una conexión es para cargar las llaves electrónicas (metadatos), y la otra conexión es para el tráfico de túnel actual. El túnel 131 únicamente se establece después de la etapa 207 (ver a continuación), y únicamente se permite el tráfico después de la etapa 208 (ver a continuación), debido a que el cortafuegos se bloquea por omisión.

Por lo tanto, en la etapa 206, el módulo de túnel 101 pasa a la segunda conexión de red (conexión que es responsable para tener el efecto de túnel del tráfico que viene del cliente

121) al servicio del túnel 150. Los servicios de túnel 150 y 151 manejan el tráfico de túnel (131, 132, 133). Los servicios de túnel 150, 151 son responsables para descryptar/encryptar el tráfico que entra y sale del cliente respectivo (121, 122, ... 126) implementados sobre la puerta de enlace 100. El servicio de túnel entonces se verifica con el módulo de gestión 102 si el túnel de red 131 puede establecerse. En la siguiente etapa 207, el servicio de túnel 150 establece el túnel de red 131 al iniciar el servicio de cortafuegos 111. Desde este momento, todos los datos intercambiados sobre la segunda conexión de red y de esta manera sobre el túnel de red 131 pasan a través del servicio de cortafuegos 111. En otras palabras, los datos de carga del túnel de red 131 se reenvían al servicio de cortafuegos de partida 111. Este servicio de cortafuegos 111 implementa un cortafuegos que bloquea por omisión todo el tráfico entre el cliente 121 y red privada 140. En la siguiente etapa 208, el servicio de cortafuegos 111 aplica las reglas de cortafuegos apropiadas para el cortafuegos al recuperar las reglas de cortafuegos del módulo de gestión 102. El módulo de gestión 102 a su vez deriva estas reglas de cortafuegos de la lista de acceso del cliente.

Más específicamente, en una modalidad, las reglas de acceso son reglas de cortafuegos básicamente descritas, y el módulo de gestión 102 se ocupa en algunas de estas descripciones. Algunos ejemplos son como sigue:

Permitir el tráfico TCP para 1.1.1.1 puerto 80 (se tiene en cuenta que esto es una regla de acceso que es una coincidencia exacta con una regla de cortafuegos).

Permitir el tráfico TCP a www.google.com puerto 80 (se tiene en cuenta que esto es una regla de acceso que requiere traducción para múltiples reglas FW tales como:

Permitir el tráfico TCP para 173.194.71.103 puerto 80

Permitir el tráfico TCP para 173.194.71.105 puerto 80

Permitir el tráfico TCP para 173.194.71.99 puerto 80

...)

De esta manera, una regla de acceso puede, por ejemplo, resultar en muchas reglas de cortafuegos. En algunos casos, una regla de acceso puede ser una llamada a un proveedor IAAS tipo servicios web AWS y permitir el tráfico TCP para, por ejemplo lo siguiente: [todas las instancias que tienen finanzas en su descripción].

Por el proceso de acuerdo con la FIGURA 2, un túnel de red 131 entre el dispositivo del cliente 121 y la puerta de enlace 100 de esta manera se establece junto con un cortafuegos separado con un conjunto separado de reglas de cortafuegos para selectivamente bloquear y permitir el tráfico de red entre el dispositivo del cliente 121 y los dispositivos de red 141-143 en la red privada 140. Este proceso se realiza para cada 121-126 que se conecta a la red privada 140 por ello obtiene los servicios de cortafuegos respectivos 111-116.

De acuerdo con una modalidad adicional, la puerta de enlace 100 se implementa sobre un sistema informático que comprende múltiples núcleos de procesador. El módulo de gestión

102, el módulo de túnel 101, servicio de túnel 150 y servicios de cortafuegos 111, 112 y 113 luego pueden implementarse sobre el sistema de computadora por instrucciones ejecutables en computadora ejecutadas sobre los núcleos del procesador. La puerta de enlace 100 entonces incluye un servicio de túnel separado que se ejecuta sobre cada núcleo del
5 procesador. Esto se ilustra por la modalidad ejemplar de la FIGURA 1 donde el servicio de túnel 150 y servicios de cortafuegos 111, 112 y 113 se implementan sobre el primer núcleo del procesador 160 y el servicio de túnel 151 y servicios de cortafuegos 114, 115 y 116 se implementan sobre un segundo núcleo del procesador 161. Los servicios de túnel 150 y 151 pueden, por ejemplo, implementarse como procesos de software que se ejecutan sobre los
10 núcleos del procesador respectivos. Los servicios de cortafuegos pueden implementarse como procesos de software ejecutados por el proceso de software respectivo (es decir, los servicios de túnel respectivos).

Una ventaja de ejecución que separa los servicios de túnel sobre cada núcleo del procesador es que la comunicación inter-proceso entre los servicios de cortafuegos y
15 comunicación entre un servicio de cortafuegos y el servicio de túnel se limita al mismo núcleo. Como un resultado, cuando la puerta de enlace 100 aumenta al agregar más núcleos del procesador, no habrá pérdida en rendimiento debido a la comunicación inter-proceso incrementada.

La FIGURA 3 muestra un proceso ejemplar que puede ejecutarse por componentes de
20 la presente descripción que incluyen la puerta de enlace 100 de acuerdo con la FIGURA 1. Por el proceso, las conexiones del cliente y, de esta manera, los túneles de red pueden distribuirse sobre los diferentes núcleos 160, 161. El proceso inicia durante el establecimiento de la segunda conexión en la etapa 305 como se establece arriba con referencia a la etapa 205 de la FIGURA 2. El proceso luego procede a la etapa 306 donde el módulo de túnel
25 selecciona uno de los servicios de túnel 150, 151 a los cuales reenviará la segunda conexión. Esto puede hacerse en diversas formas. Por ejemplo, el módulo de túnel puede distribuir la conexión en una manera de retorno al punto de origen al reenviar la conexión cada vez para el siguiente núcleo del procesador. Alternativamente, puede reenviarse la conexión al
30 procesador que tiene la mayor cantidad de recursos disponibles tales como, por ejemplo, energía de procesamiento, memoria o cualquier combinación de los mismos. Cuando el núcleo del procesador se selecciona, el módulo de túnel 101 reenvía la segunda conexión al servicio de túnel seleccionado bajo la etapa 307, ya que también se establece arriba con referencia a la etapa 206 de la FIGURA 2.

La FIGURA 4 ilustra los detalles de un servicio de cortafuegos ejemplar 411 que puede
35 implementarse en una puerta de enlace 100 de acuerdo con la presente descripción, por ejemplo como el servicio de cortafuegos 111 a 116 de la FIGURA 1. Por el bien de la ilustración ejemplar, se asumirá que el servicio de cortafuegos 411 corresponde al servicio de

cortafuegos 111, que proporciona el túnel de red 131 entre el cliente 121 y red privada 140. Cuando el servicio de cortafuegos 411 se inicia, esto comprende un componente cortafuegos 420 para selectivamente bloquear y permitir el tráfico de red entre el dispositivo del cliente respectivo 121 y los dispositivos de red 141-143 en la red privada 140. Las reglas utilizadas por el cortafuegos 420 de acuerdo con las cuales el tráfico se bloquea o permite, se almacenan como reglas de cortafuegos 421. Estas reglas pueden, por ejemplo, almacenarse en un campo o base de datos que reside en la memoria del sistema informático que implementa la puerta de enlace 100.

El cortafuegos 420 puede ser un cortafuegos con control de estado configurado para realizar la inspección de paquetes con control de estado, por ello mantiene un seguimiento del estado de las conexiones de red establecidas sobre el túnel de red 131 entre el cliente 121 y los dispositivos de red 141-143 en la red privada 140. Cada una de dicha conexión puede relacionarse con conexiones de red TCP o UDP. De esta manera, un control detallado es posible ya que las reglas se vuelven dependientes de la conexión de red y son de esta manera dinámicas. El cortafuegos mantiene el seguimiento de todas las conexiones de red abiertas al mantener una lista, la lista de estado 422, con todas las conexiones pendientes. Estos estados pueden, por ejemplo, almacenarse en un campo o base de datos que residen en la memoria del sistema informático que implementa la puerta de enlace 100.

Cada servicio de cortafuegos 411 de esta manera mantiene una lista de estado separada 422. Una ventaja de esto es que el tamaño de la lista de estado del servicio de cortafuegos 411 no crece con la cantidad de clientes conectados con la puerta de enlace 100. De esta manera, un incremento en los clientes conectados no resulta en una pérdida de rendimiento debido a un incremento en la cantidad de estados que tienen que ser gestionados por un servicio de cortafuegos sencillo.

El servicio de cortafuegos 411 puede incluir además un componente de encriptación y/o desencriptación 423 para encriptar y desencriptar respectivamente datos transmitidos a o recibidos del cliente 121. La encriptación y desencriptación puede realizarse además de acuerdo con la Seguridad del Protocolo de Internet (o "protocolo IPsec,") Seguridad de Capa de Transporte (o "TLS") y/o Seguridad de Capa de Transporte de Datagram (o "DTLS"). La encriptación y desencriptación puede además ser hardware acelerado por un componente de hardware en el núcleo del procesador sobre el cual el servicio de cortafuegos 411 se ejecuta.

La FIGURA 5 muestra un proceso ejemplar que puede ejecutarse por componentes de la presente descripción, por ejemplo por el servicio de cortafuegos 411 de la FIGURA 4. Por este proceso, una copia de seguridad del servicio de cortafuegos se hace de manera que puede utilizarse durante una falla del sistema informático, y de esta manera la puerta de enlace sobre la cual el servicio de cortafuegos 411 se ejecuta. En la etapa 501, el cortafuegos 420 permite el establecimiento de una conexión de red entre el cliente 121 y un dispositivo de

red o aplicación de red en la red privada 140. Esta conexión de red de esta manera se establece sobre el túnel de red ya establecido 131. Con objeto de mantener el seguimiento del tráfico sobre esta nueva conexión y, de esta manera, permitir el tráfico de esta conexión para pasar el cortafuegos 420, el cortafuegos registra la conexión con la lista de estado de cortafuegos 422 bajo la etapa 501. Luego, en la etapa 502, el cortafuegos 420 copia la lista de estado 422 y firma la copia en la etapa 503 con una clave de firma secreta. De esta manera, luego puede verificarse que la copia no fue alterada por una parte no autorizada. En la etapa 504, la copia luego se transmite al cliente 121. De esta manera, la lista de estado y de esta manera el estado del cortafuegos 420 se sincroniza con el cliente 121. Ya que la lista de estado se firma bajo la etapa 502, las modificaciones a la lista de estado pueden descubrirse al verificar la firma.

Por el proceso de la FIGURA 5, una copia de seguridad separada puede hacerse de cada cortafuegos en la puerta de enlace 100. Esto tiene diversas ventajas. Ante todo, esto puede hacerse rápidamente como solo un conjunto limitado de estados necesarios para transmitirse cada vez. Como un resultado, cuando el sistema se escala, el tiempo para la sincronización de un servicio de cortafuegos sencillo 411 no incrementa. Segundo, esto se permite una disposición de conmutación de falla que es escalable como se demostrará a continuación.

La FIGURA 6 ilustra un sistema de acuerdo con una modalidad para proteger el acceso a una red privada 140. El acceso se controla por puertas de enlace 600, 601 y 602 correspondientes a la puerta de enlace 100 también por que implementa el módulo de túnel 101 (no se muestra), módulo de gestión 102 (no se muestra), y uno o más servicios de túnel 150, 151 (no se muestran) cada uno que implementa uno o más servicios de cortafuegos. Por motivos de claridad, sólo dos servicios de cortafuegos 611A y 616A se muestran en la puerta de enlace 600.

La FIGURA 7 muestra un proceso ejemplar que puede ejecutarse por los componentes de la FIGURA 6 en el caso de una falla de una de las puertas de enlace 600-602 (en el siguiente ejemplo, una falla de puerta de enlace 600 se discute). En la etapa 701 del proceso, puerta de enlace 600 establece un primer túnel de red 631 con el dispositivo del cliente 621 con objeto de proporcionar al cliente 621 acceso a los dispositivos de red 141-143 en la red privada. Por esto, el servicio de cortafuegos 611A por ello se inicia implementando un cortafuegos de control de estado y que incluye además las reglas de cortafuegos y la lista de estado. La etapa 701 puede, por ejemplo, realizarse de acuerdo con la FIGURA 2.

Después del establecimiento del túnel de red 631, el servicio de cortafuegos 611A continuamente sincroniza la lista de estado con el cliente 621 al enviar regularmente una copia o actualización 650 de la lista de estado para el dispositivo del cliente 621. Por ejemplo, el estado sólo necesita sincronizarse si el estado actual se cambia. De esta manera, si el cliente

no abre nuevas conexiones a los servidores protegidos, no ocurrirá la sincronización del estado. También, esta sincronización es configurable y puede hacerse, por ejemplo, continuamente, o al menos cada 1-5 segundos, etc. Siempre que el túnel de red está en el lugar 631, la sincronización se activa como se ilustra en el ciclo 703-702. La sincronización de la lista de estado puede además realizarse de acuerdo con el proceso como se ilustra en la FIGURA 5.

Para propósitos de discusión ejemplar, se considera que en un cierto momento en tiempo, el túnel de red 631 se interrumpe. Como un resultado de esta interrupción, el proceso procede a la etapa 704. La interrupción del túnel de red 631 puede provocarse por diversos factores tales como, por ejemplo, por una falla en la trayectoria de la red entre el cliente 621 y la puerta de enlace 600, o por una falla de la puerta de enlace 600 por sí misma. Cuando el cliente detecta la falla del túnel de red, este establece un nuevo túnel de red 632 con la segunda puerta de enlace 601, que también proporciona acceso a la red privada 140. Esto puede, por ejemplo, hacerse por el proceso como se ilustra por la FIGURA 2 al reenviar el túnel información de autenticación 653 y lista de acceso de clientes 652 para la segunda puerta de enlace 601.

Más específicamente, en una modalidad, la información sobre todas de las puertas de enlace disponibles (600, 601, 602) es parte de las listas de túnel descritas arriba. Esta información puede venir de, por ejemplo, un servidor de autenticación central (controlador) tal como se describe en la Patente de E.U.A. No. US 9,148,408 B1, la cual se incorpora como referencia arriba. Esta información está disponible en la primera conexión (es decir, antes de que la primera conexión pueda fallar). El servidor de autenticación central simplemente elige otro candidato de la lista de túnel y establece la conexión. La única información de fuente que viene de la copia o actualización 650 es el estado de conexión actual del servicio de cortafuegos que se sincronizará una vez que el nuevo túnel se establezca.

Durante el establecimiento del túnel 632, el servicio de cortafuegos 611B se inicia sobre la puerta de enlace 601 con idénticas reglas de cortafuegos como se utilizan en el servicio de cortafuegos 611A debido a que la misma lista de acceso 652 se utiliza por el módulo de gestión de la puerta de enlace 601 para derivar las reglas de cortafuegos.

Durante el establecimiento del segundo túnel de red 632, el cliente 621 también transmite la lista de estado 651 para la puerta de enlace 601 bajo la etapa 705 del proceso. En una modalidad, la copia o actualización 650 es la fuente de la lista de estado 651. Las conexiones iban al túnel 631 antes del sistema de recuperación de fallos. Durante las conexiones activas, el estado se ha sincronizado continuamente para el cliente 621, y también se actualiza cuando los estados se actualizaron para el servicio de cortafuegos 611A. Cuando el túnel se cae, un nuevo túnel se establece y el último estado recibido 651 se sincroniza con el servicio de cortafuegos 611B.

La lista de estado 651 puede, por ejemplo, reenviarse al módulo de gestión. El módulo de gestión verifica que la lista de estado no se cambió por el cliente, y luego proporciona la lista de estado para el servicio de cortafuegos 611B que utiliza esto como su lista de estado con objeto de restaurar el estado del cortafuegos bajo la etapa 706. Después de restaurar el estado del cortafuegos, el cliente reanuda, bajo la etapa 707, su comunicación con la red privada 140, por ello alcanza un conmutación por fallos continua (es decir, sin una pérdida de las conexiones de red pendientes establecidas sobre el túnel de red inicial 631).

Alternativamente, la lista de estado también puede enviarse sobre el túnel de red directamente al servicio de cortafuegos 611B, en donde este servicio verificará que la lista de estado no se alteró. Esta verificación puede hacerse al utilizar la misma clave de firma secreta (compartida) entre las puertas de enlace. En una modalidad, debido a que los estados del cortafuegos se almacenan temporalmente en memoria sobre el cliente, existe un riesgo potencial de manipulación no autorizada con los estados. Con objeto de evitar este riesgo, los estados se firman con una clave compartida secreta entre las puertas de enlace. Así, si los estados son manipulados, la firma se rompe y los estados no se aceptarán.

El proceso de la FIGURA 7 tiene la ventaja de que no hay sincronización de las reglas del cortafuegos y los estados entre las puertas de enlace 600 y 601 se necesitan. Por lo tanto, el sistema puede aumentarse fácilmente al agregar una puerta de enlace (por ejemplo, puerta de enlace 602) sin requerimientos del ancho de banda entre las puertas de enlace (se tiene en cuenta que no existen requerimientos para cualquier ancho de banda que se utiliza entre la puerta de enlaces). Además, durante la falla de la puerta de enlace 600, los túneles de red pueden transferirse a través de las puertas de enlace 601 y 602. Por ejemplo, el servicio de cortafuegos 616A puede moverse a la puerta de enlace 602 como el servicio 616B mientras que el cortafuegos 616A se transfiere a la puerta de enlace 601 como el servidor 611B.

La FIGURA 8 muestra un sistema informático ejemplar adecuado 800 para que implemente la puerta de enlace de acuerdo con las modalidades anteriores. El sistema informático 800 puede en general formarse como una computadora de propósitos general adecuado y comprende un bus 810, uno o más procesos del procesador 802, una memoria local 804, una o más interfaces de salida opcionales 814, una o más interfaces de salida opcionales 816, una o más interfaces de comunicación 812, una interfaz de elemento de almacenamiento 806 y uno o más elementos de almacenamiento 808. El bus 810 puede comprender uno o más conductores que permiten la comunicación entre los componentes del sistema informático 800. Los procesos del procesador 802 pueden incluir cualquier tipo de procesador convencional o microprocesador que interpreta y ejecuta las instrucciones de programación. La memoria local 804 puede incluir una memoria de acceso aleatorio (RAM) u otro tipo de dispositivo de almacenamiento dinámico que almacena información e instrucciones para la ejecución por procesos del procesador 802 y/o una memoria de sólo

lectura (ROM) u otro tipo de dispositivo de almacenamiento estático que almacena la información estática e instrucciones para uso por el procesador 802. La interfaz de entrada 814 puede comprender uno o más mecanismos convencionales que permiten a un operador ingresar información al dispositivo informático 800, tal como un teclado 820, un ratón 830, un bolígrafo, reconocimiento de voz y/o mecanismos biométricos, etc. La interfaz de salida 816 puede comprender uno o más mecanismos convencionales que sacan la información al operador, tal como una pantalla 840. La interfaz de comunicación 812 puede comprender cualquier mecanismo tipo transceptor tal como, por ejemplo, una o más interfaces Ethernet que permiten al sistema informático 800 comunicarse con otros dispositivos y/o sistemas 801.

La interfaz de comunicación 812 del sistema informático 800 puede conectarse con otro sistema informático por medio de una red de área local (LAN, por sus siglas en inglés) o una red de área amplia (WAN, por sus siglas en inglés) tal como, por ejemplo, la internet. La interfaz del elemento de almacenamiento 806 puede comprender una interfaz de almacenamiento tal como, por ejemplo, una interfaz de Unión de Tecnología Avanzada en Serie (SATA) o una Interfaz de Sistema informático Pequeño (SCSI) para conectar el bus 810 a uno o más elementos de almacenamiento 808, tal como uno o más discos locales, por ejemplo unidades de disco SATA, y controlar la lectura y escritura de datos a y/o de estos elementos de almacenamiento 808. Aunque los elementos de almacenamiento 808 de arriba se describen como, por ejemplo, un disco local, en general cualquier otro medio legible en computadora adecuado tal como un disco magnético removible, medio de almacenamiento óptico tal como discos de CD-ROM o DVD-ROM, unidades de estado sólido, tarjetas de memoria flash, etc., podrían utilizarse. El sistema 800 descrito arriba también puede ejecutarse como una máquina virtual por encima del hardware físico.

Las etapas realizadas de acuerdo con los procesos de arriba pueden implementarse como instrucciones ejecutables en computadora. Estas instrucciones luego pueden ejecutarse sobre procesos del procesador 802 al realizar los procesos. De esta manera, las etapas ejecutadas por el módulo de túnel 101, módulo de gestión 102, servicios de túnel 150, 151 y servicios de cortafuegos 111-116 pueden, por ejemplo, implementarse como instrucciones sobre el sistema informático 800 por ello implementa la puerta de enlace 100. Los procesos del procesador 802 pueden corresponder a procesos del procesador 160, 161 de la puerta de enlace 100. Un servicio de túnel 150, 151 luego se ejecuta sobre cada uno de los núcleos del procesador 802. Cada núcleo del procesador 802 luego ejecuta servicios de cortafuegos separados respectivamente iniciados por uno de los servicios de túnel. La comunicación del paquete de datos entre los dispositivos cliente 121-126 y la puerta de enlace 100 pueden realizarse sobre una interfaz de red 812. También, los paquetes de datos comunicados entre la puerta de enlace 100 y la red privada 140 pueden intercambiarse sobre una interfaz de red 812. Las instrucciones ejecutables en computadora pueden formar o ser parte de un producto

de programa de computadora que se almacena sobre el elemento de almacenamiento 808 o cualquier medio de almacenamiento legible en computadora.

La comunicación entre los sistemas, dispositivos, y componentes que operan en conjunto con modalidades de la presente descripción pueden realizarse utilizando cualquier método de comunicación adecuado, tal como, por ejemplo, una red de teléfono, una extranet, una intranet, la Internet, punto de dispositivo de interacción (punto de dispositivo de venta, asistente digital personal (por ejemplo, iPhone®, Palm Pilot®, Blackberry®), teléfono celular, quiosco, etc.), comunicaciones en línea, comunicaciones por satélite, comunicaciones fuera de línea, comunicaciones inalámbricas, comunicaciones del transpondedor, red de área local (LAN), red de área amplia (WAN), red privada virtual (VPN), dispositivos en red o conectados, teclado, ratón y/o cualquier comunicación adecuado o modalidad de entrada de datos. Los sistemas y dispositivos de la presente descripción pueden utilizar protocolos de comunicaciones TCP/IP así como IPX, Appletalk, IP-6, NetBIOS, OSI, cualquier protocolo con efecto de túnel (por ejemplo IPsec, SSH), o cualquier número de protocolos existentes o futuros.

Aunque algunas modalidades pueden implementarse en sistemas informáticos y computadoras que funcionan completamente, varias modalidades son capaces de ser distribuidos como un producto informático en una variedad de formas y son capaces de ser aplicados con respecto al tipo particular de máquina o medio legible en computadora utilizado para efectuar actualmente la distribución.

Un medio legible en máquina puede utilizarse para almacenar software y datos que cuando se ejecutan por un sistema de procesamiento de datos provoca al sistema para realizar varios métodos. Los datos y software ejecutable pueden almacenarse en varios lugares incluyendo, por ejemplo, ROM, RAM volátil, memoria no volátil y/o caché. Las porciones de este software y/o datos pueden almacenarse en cualquiera de uno de estos dispositivos de almacenamiento. Además, los datos e instrucciones pueden obtenerse de servidores centralizados o redes punto a punto. Diferentes porciones de los datos e instrucciones pueden obtenerse de diferentes servidores centralizados y/o redes punto a punto en diferentes tiempos y en diferentes sesiones de comunicación o en una misma sesión de comunicación. Los datos e instrucciones pueden obtenerse en su totalidad antes de la ejecución de las aplicaciones. Alternativamente, las porciones de los datos e instrucciones pueden obtenerse dinámicamente, justo en tiempo, cuando se necesitan para ejecución. De esta manera, no se requiere que los datos ni instrucciones estén sobre un medio legible en máquina en su totalidad en una instancia particular de tiempo.

Los ejemplos de medios legibles en computadora incluyen pero no se limitan a medios de tipo legibles y no legibles tal como dispositivos de memoria volátil y no volátil, memoria de solo lectura (ROM), memoria de acceso aleatorio (RAM), dispositivos de memoria flash,

flexible y otros discos removibles, medios de almacenamiento de disco magnético, medios de almacenamiento óptico (por ejemplo, Discos Compactos de Memoria de Solo Lectura (CD ROMS), Discos Versátiles Digitales (DVDs), etc.), entre otros. Los medios legibles en computadora pueden almacenar las instrucciones.

5 En varias modalidades, el circuito de conexión permanente puede utilizarse en combinación con las instrucciones del software para implementar las técnicas. De esta manera, las técnicas no son limitadas a cualquier combinación específica de circuito de hardware y software ni a ninguna fuente particular para las instrucciones ejecutadas por el sistema de procesamiento de datos.

10 Aunque algunos de los dibujos ilustran un número de operaciones en un orden particular, las operaciones que no son dependientes del orden pueden reordenarse y otras operaciones pueden combinarse o romperse. Aunque algunos reordenamientos u otras agrupaciones se mencionan específicamente, otras serán aparentes para aquellos de experiencia ordinaria en la técnica y por lo tanto presentan una lista exhaustiva de alternativas.

15 Además, deberá reconocerse que las etapas podrían implementarse en hardware, firmware, software o cualquier combinación de los mismos.

Por motivos de brevedad, la red de datos convencional, el desarrollo de la aplicación y otros aspectos funcionales de los sistemas (y componentes de los componentes de operación individuales de los sistemas) no pueden describirse en detalle en la presente. Además, las

20 líneas de conexión mostradas en las varias figuras contenidas en la presente se pretenden para representar las relaciones funcionales ejemplares y/o acoplamientos físicos entre los varios elementos. Deberá señalarse que muchas relaciones funcionales adicionales o alternativas o conexiones físicas pueden presentarse en un sistema práctico.

Los varios componentes del sistema discutidos en la presente pueden incluir uno o

25 más de los siguientes: un servidor anfitrión u otros sistemas informáticos que incluyen un procesador para procesar datos digitales; una memoria acoplada al procesador para almacenar los datos digitales; un digitalizador de entrada acoplado al procesador para ingresar datos digitales; un programa de aplicación almacenado en la memoria y accesible por el procesador para un procesamiento de dirección de datos digitales por el procesador; un

30 dispositivo de visualización acoplado al procesador y memoria para visualizar información derivada de datos digitales procesados por el procesador; y una pluralidad de bases de datos. Varias bases de datos utilizadas en la presente pueden incluir: datos de envío, datos del paquete, y/o cualquiera de los datos útiles en la operación del sistema.

Varias funcionalidades pueden realizarse por medio de un navegador web y/o

35 aplicación de interfaz que utiliza un navegador web. Tales aplicaciones del navegador pueden comprender software de navegación por Internet instalado dentro de una unidad de computación o un sistema para realizar varias funciones. Estas unidades de computación o

sistemas pueden tomar la forma de una computadora o conjunto de computadoras, y cualquier tipo de dispositivo de computación o sistemas pueden utilizarse, que incluyen laptops, notebooks, tabletas, computadoras portátiles, asistentes digitales personales, decodificadores, estaciones de trabajo, computadora-servidores, ordenadores centrales, mini-computadoras, servidores de PC, conjuntos de red de computadoras, computadoras personales y tabletas, tal como iPads, iMACs, y MacBooks, quioscos, terminales, punto de dispositivos y/o terminales de venta (POS), televisiones, o cualquier otro dispositivo capaz de recibir datos sobre una red. Varias modalidades pueden utilizar Microsoft Internet Explorer, Mozilla Firefox, Google Chrome, Apple Safari, Opera, o cualquier otro de los innumerables paquetes de software disponibles para navegar en la internet.

Varias modalidades pueden operar en conjunto con cualquier sistema operativo adecuado (por ejemplo, Windows NT, 95/98/2000/CE/Mobile/, Windows 7/8, OS2, UNIX, Linux, Solaris, MacOS, PalmOS, etc.) así como varios controladores y software de soporte convencional típicamente asociados con las computadoras. Varias modalidades pueden incluir cualquier computadora personal adecuada, computadora de red, estación de trabajo, asistente digital personal, teléfono celular, teléfono inteligente, minicomputadora, procesador central o los similares. Las modalidades pueden implementar protocolos de seguridad, tal como Secure Sockets Layer (SSL), Transport Layer Security (TLS), y Secure Shell (SSH). Las modalidades pueden implementar cualquier protocolo de capa de aplicación deseada, que incluye http, https, ftp, y sftp.

Los varios componentes del sistema pueden estar independientemente, separadamente o colectivamente de manera adecuada acoplados a una red por medio de datos ligados que incluyen, por ejemplo, una conexión a un Proveedor de Servicio de Internet (ISP) sobre el ciclo local como se utiliza típicamente en conexión con comunicación de módem estándar, módem de cable, redes de satélite, ISDN, Línea del Suscriptor Digital (DSL), o varios métodos de comunicación inalámbrica. Se señala que las modalidades de la presente descripción pueden operar en conjunto con cualquier tipo adecuado de red, tal como una red de televisión interactiva (ITV).

El sistema puede implementarse parcialmente o completamente utilizando computación en la nube. "Nube" o "computación en la nube" incluye un modelo para permitir el acceso a la red bajo pedido, conveniente a un grupo compartido de recursos de computación configurables (por ejemplo, redes, servidores, almacenamiento, aplicaciones, y servicios) que pueden aprovisionarse rápidamente y liberarse con el esfuerzo de la gestión mínima o interacción del proveedor de servicio. La computación en la nube puede incluir computación independiente de la ubicación, por ello los servidores compartidos proporcionan recursos, software, y datos para computadoras y otros dispositivos bajo pedido.

Varias modalidades pueden utilizarse en conjunto con servicios web, computación de

utilidad, computación persuasiva e individualizada, seguridad y soluciones de identidad, computación autónoma, computación en la nube, computación de productos básicos, movilidad y soluciones inalámbricas, fuente abierta, biométrica, computación de red y/o computación de malla.

5 Cualquiera de las bases de datos discutidas en la presente puede incluir estructura relacional, jerárquica, gráfica, u orientada a objetos y/o cualquiera de las otras configuraciones de base de datos. Además, las bases de datos pueden organizarse de cualquier manera adecuada, por ejemplo, como tablas de datos o tablas de búsqueda. Cada registro puede ser un campo sencillo, una serie de campos, una serie ligada de campos de datos o cualquier otra
10 estructura de datos. La asociación de ciertos datos puede realizarse a través de cualquier técnica de asociación de datos deseada tal como aquellos conocidos o practicados en la técnica. Por ejemplo, la asociación puede realizarse ya sea manualmente o automáticamente.

Cualquiera de las bases de datos, sistemas, dispositivos, servidores u otros componentes del sistema pueden ubicarse en una ubicación sencilla o en ubicaciones
15 múltiples, en donde cada base de datos o sistema incluye cualquiera de varias características de seguridad adecuadas, tal como servidores de seguridad, códigos de acceso, encriptación, desenscriptación, compresión, descompresión, y/o los similares.

La encriptación puede realizarse a manera de cualquiera de las técnicas ahora disponibles en la técnica o que pueden volverse disponibles—por ejemplo, Twofish, RSA, El Gamal, firma Schorr, DSA, PGP, PKI, y criptosistemas simétricos y asimétricos.
20

Las modalidades pueden conectar a la Internet o una intranet utilizando acceso telefónico estándar, cable, DSL o cualquier protocolo de Internet conocido en la técnica. Las transacciones pueden pasar a través de un cortafuegos con objeto de prevenir el acceso no autorizado de usuarios de otras redes.

25 Las computadoras discutidas en la presente pueden proporcionar un sitio web adecuado u otra interfaz del usuario gráfica con base en Internet que es accesible por los usuarios. Por ejemplo, el servidor de Información de Internet de Microsoft (IIS), Servidor de Transacción de Microsoft (MTS), y Servidor Microsoft SQL, pueden utilizarse en conjunto con el sistema operativo Microsoft, software de servidor web Microsoft NT, un sistema de base de
30 datos del Servidor Microsoft SQL, y un Servidor de Comercio de Microsoft. Adicionalmente, los componentes tales como Access o Microsoft SQL Server, Oracle, Sybase, Informix MySQL, Interbase, etc., pueden utilizarse para proporcionar un sistema de gestión de base de datos compatible con Objetos de Datos Activos (ADO). En otro ejemplo, un servidor web Apache puede utilizarse en conjunto con un sistema operativo Linux, una base de datos MySQL, y los
35 programas de programación Perl, PHP, y/o Python.

Cualquiera de las comunicaciones, entradas, almacenamiento, bases de datos o visualizaciones discutidas en la presente pueden facilitarse a través de un sitio web que tienen

páginas web. El término “página web” como se utiliza en la presente no está destinado para limitar el tipo de documentos y aplicaciones que podrían utilizarse para interactuar con el usuario. Por ejemplo, un sitio web típico podría incluir, además de los documentos HTML estándares, varias formas, miniaplicaciones Java, JavaScript, páginas del servidor activas (ASP), secuencias de comandos comunes de puerta de enlace interface (CGI), lenguaje de marcado extensible (XML), HTML dinámico, hojas de estilo en cascada (CSS), AJAX (Asíncrono de Javascript y XML), aplicaciones de ayuda, complementos, y los similares. Un servidor puede incluir un servidor web que recibe una petición de un servidor web, la petición que incluye una URL y una dirección IP. El servidor web recupera las páginas web apropiadas y envía los datos o aplicaciones para las páginas web para la dirección IP. Los servicios web son aplicaciones que son capaces de interactuar con otras aplicaciones sobre los medios de comunicación, tal como la Internet.

Varias modalidades pueden emplear cualquier número deseado de métodos para visualizar los datos dentro de un documento con base en el navegador. Por ejemplo, los datos pueden representarse como texto estándar o dentro de una lista fija, lista desplazable, lista desplegable, campo de texto editable, campo de texto fijo, ventana emergente, y los similares. Del mismo modo, las modalidades pueden utilizar cualquier número deseado de métodos para modificar los datos en una página web tal como, por ejemplo, entrada de texto libre utilizando un teclado, selección de elementos del menú, casillas de verificación, cajas de opciones, y los similares.

Los sistemas ejemplares y métodos ilustrados en la presente pueden describirse en términos de componentes de bloque funcional, capturas de pantalla, selecciones de opción y varias etapas de procesamiento. Deberá apreciarse que tales bloques funcionales pueden realizarse por cualquier número de componentes de hardware y/o software configurados para realizar las funciones específicas. Por ejemplo, el sistema puede emplear varios componentes de circuito integrado, por ejemplo, elementos de memoria, elementos de procesamiento, elementos lógicos, tablas de búsqueda, y los similares, que pueden llevar a cabo una variedad de funciones bajo el control de uno o más microprocesadores u otros dispositivos de control. De manera similar, los elementos de software del sistema pueden implementarse con cualquier lenguaje de programación o secuencia de comandos tal como C, C++, C#, Java, JavaScript, VBScript, Macromedia Cold Fusion, COBOL, Páginas de Microsoft Active Server, conjunto de programas, PERL, PHP, AWK, Python, Visual Basic, Procedimientos de Almacenamiento SQL, PL/SQL, cualquier archivo de comandos de secuencia de comando UNIX, y lenguaje de marcado extensible (XML) con los varios algoritmos siendo implementados con cualquier combinación de estructuras de datos, objetos, procesos, rutinas u otros elementos de programación. Además, deberá señalarse que el sistema puede emplear cualquier número de técnicas convencionales para la transmisión de datos, señalización,

procesamiento de datos, control de red, y los similares. Todavía además, el sistema podría utilizarse para detectar o prevenir problemas de seguridad con un lenguaje de secuencia de comandos del lado del cliente, tal como JavaScript, VBScript o los similares.

Los sistemas y métodos de la presente descripción pueden incorporarse como una personalización de un sistema existente, un producto complementario, un aparato de procesamiento que ejecuta el software actualizado, un sistema independiente, un sistema distribuido, un método, un sistema de procesamiento de datos, un dispositivo para el procesamiento de datos, y/o un producto del programa de computadora. En consecuencia, cualquier porción del sistema o un módulo puede tomar la forma de un aparato de procesamiento que ejecuta el código, una realización con base en internet, una realización de hardware completamente, o una modalidad que combina aspectos del internet, software y hardware. Además, el sistema puede tomar la forma de un producto de programa de computadora sobre un medio de almacenamiento legible en computadora que tiene medio de código de programa legible en computadora incorporado en el medio de almacenamiento. Cualquier medio de almacenamiento legible en computadora adecuado puede utilizarse, que incluye discos duros, CD-ROM, dispositivos de almacenamiento óptico, dispositivos de almacenamiento magnético, y/o los similares.

El sistema y método se describe en la presente con referencia a las capturas de pantalla, diagramas en bloque e ilustraciones de diagramas de flujo de los métodos, aparatos (por ejemplo, sistemas), y productos del programa de computadora de acuerdo con varias modalidades. Se entenderá que cada bloque funcional de los diagramas en bloque y las ilustraciones de los diagramas de flujo, y combinaciones de bloques funcionales en los diagramas en bloque e ilustraciones de los diagramas de flujo, respectivamente, pueden implementarse por instrucciones del programa de computadora.

Estas instrucciones del programa de computadora pueden cargarse en una computadora de propósito general, computadora de propósito especial, u otros aparatos de procesamiento de datos programables para producir una máquina, de manera que las instrucciones que se ejecutan sobre la computadora u otro aparato de procesamiento de datos programable crean medios para implementar las funciones específicas en el bloque o bloques del diagrama de flujo. Estas instrucciones del programa de computadora también pueden almacenarse en una memoria legible en computadora que puede dirigir una computadora u otro aparato de procesamiento de datos programable para funcionar en una manera particular, de manera que las instrucciones almacenadas en la memoria legible en computadora producen un artículo de fabricación que incluye medios de instrucción que implementan la función específica en el bloque o bloques del diagrama de flujo. Las instrucciones del programa de computadora también pueden cargarse en una computadora u otro aparato de procesamiento de datos programable para provocar una serie de etapas operacionales para

realizarse sobre la computadora u otro aparato programable para producir un proceso implementado en computadora de manera que las instrucciones que se ejecutan sobre la computadora u otro aparato programable proporciona etapas para implementar las funciones específicas en el bloque o bloques del diagrama de flujo.

5 En consecuencia, los bloques funcionales de los diagramas en bloque e ilustraciones del diagrama de flujo soportan combinaciones de medios para realizar las funciones específicas, combinaciones de etapas para realizar las funciones específicas, y medios de instrucción del programa para realizar las funciones específicas. También se entenderá que cada bloque funcional de los diagramas en bloque e ilustraciones del diagrama de flujo, y
10 combinaciones de bloques funcionales en los diagramas en bloque e ilustraciones del diagrama de flujo, pueden implementarse por cualquiera de los sistemas informáticos con base en hardware de propósito especial que realizan las funciones o etapas específicas, o combinaciones adecuadas de instrucciones de computadora y hardware de propósito especial. Además, las ilustraciones de los flujos de proceso y las descripciones de las mismas pueden
15 hacer referencia a las ventanas de usuario, páginas web, sitios web, formas web, instrucciones, etc. Los practicantes apreciarán que las etapas ilustradas descritas en la presente pueden comprender en cualquier número de configuraciones que incluyen el uso de ventanas, páginas web, formas web, ventanas emergentes, instrucciones y los similares. Deberá apreciarse además que las múltiples etapas como se ilustra y describe pueden
20 combinarse en páginas web sencillas y/o ventanas pero se han expandido para mayor simplicidad. En otros casos, las etapas ilustradas y descritas como etapas de proceso sencillo pueden separarse en múltiples páginas web y/o ventanas pero se han combinado para simplicidad.

El término “no transitorio” es para entenderse que remueve sólo señales transitorias propagadas per se del alcance de la reivindicación y no renuncia a los derechos para todos los
25 medios legibles en computadora estándares que no son únicamente señales transitorias propagadas per se. Establecido de otra manera, el significado del término “medio legible en computadora no transitorio” deberá construirse para excluir sólo aquellos tipos de medios legibles en computadora transitorios que se encontraron en In Re Nuijten para quedar fuera
30 del alcance de la materia objeto patentable bajo 35 U.S.C. §101.

Los beneficios, otras ventajas, y soluciones a los problemas se han descrito en la presente con respecto a las modalidades específicas. Sin embargo, los beneficios, ventajas, soluciones a problemas, y cualquiera de los elementos que pueden provocar cualquier beneficio, ventaja, o solución que ocurren o se vuelven más pronunciados no son para
35 construirse como características o elementos críticos, requeridos, o esenciales de la descripción.

Aunque la descripción incluye un método, se contempla que puede incorporarse como

instrucciones del programa de computadora sobre un portador legible en computadora tangible, tal como una memoria magnética u óptica o como un disco magnético u óptico. Todos los equivalentes estructurales, químicos, y funcionales a los elementos de las modalidades ejemplares descritas arriba que se conocen para aquellos de experiencia ordinaria en la técnica se incorporan expresamente en la presente como referencia y se pretenden para abarcarse por las presentes reivindicaciones. Además, no es necesario para un dispositivo o método direccionar cada uno y cada problema que se intenta resolver por la presente descripción, para abarcarse por las presentes reivindicaciones. Adicionalmente, la etapa de elemento, componente, o método en la presente descripción no se pretende para dedicarse al público independientemente de si la etapa de elemento, componente, o método se recita explícitamente en las reivindicaciones. No es para construirse el elemento de la reivindicación en la presente bajo las provisiones de 35 U.S.C. 112, sexto párrafo, a menos que el elemento se recite expresamente utilizando la frase “medios para.” Como se utiliza en la presente, los términos “comprende”, “que comprende”, o cualquier otra variación de los mismos, se pretenden para cubrir una inclusión no exclusiva, de manera que un proceso, método, artículo, o aparato que comprende una lista de elementos no incluye sólo aquellos elementos sino pueden incluir otros elementos no enlistados expresamente o inherentes a dicho proceso, método, artículo, o aparato.

Donde una frase similar a “al menos uno de A, B, o C,” “al menos uno de A, B, y C,” “uno o más A, B, o C,” o “uno o más de A, B, y C” se utiliza, se pretende que la frase se interprete para significar que A solo puede presentarse en una modalidad, B solo puede presentarse en una modalidad, C solo puede presentar en una modalidad, o que cualquier combinación de los elementos A, B y C puede presentarse en una modalidad sencilla; por ejemplo, A y B, A y C, B y C, o A y B y C.

Pueden hacerse cambios y modificaciones a las modalidades descritas sin alejarse del alcance de la presente descripción. Estos y otros cambios o modificaciones se pretenden para incluirse dentro del alcance de la presente descripción, como se expresa en las siguientes reivindicaciones.