(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 546 136**

(51) Int. CI.:

H04L 12/46 (2006.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **27.11.2009 E 09828645 (3)**

(97) Fecha y número de publicación de la concesión europea: **03.06.2015 EP 2357763**

(54) Título: **Métodos y aparatos para cruzar un denominado 'cortafuegos' virtual con el fin de transmitir y recibir datos**

(30) Prioridad:

29.11.2008 CN 200810217797

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
18.09.2015

(73) Titular/es:

HUAWEI TECHNOLOGIES CO., LTD. (100.0%)
Huawei Administration Building, Bantian, Longgang District
Shenzhen, Guangdong 518129, CN

(72) Inventor/es:

ZHU, ZHIQIANG;
ZHANG, RIHUA;
HOU, GUIBIN;
XU, YONG;
XIE, WENHUI;
MA, BO;
GAO, GUOLU;
LU, XIAOPING y
FU, CUIHUA

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

DESCRIPCIÓN

Métodos y aparatos para cruzar un denominado 'cortafuegos' virtual con el fin de transmitir y recibir datos

CAMPO DE LA INVENCIÓN

La presente invención se refiere al campo de las tecnologías de comunicaciones y más en particular, a métodos y aparatos para enviar y recibir datos a través de 'cortafuegos' virtuales (VFWs).

ANTECEDENTES DE LA INVENCIÓN

Un denominado 'cortafuegos' es una combinación de una serie de componentes establecidos entre diferentes redes, tales como entre una red Intranet de confianza y una red pública de no-confianza, o entre zonas de seguridad de redes. Dicho 'cortafuegos' suele formular una política de seguridad basada en zonas de seguridad para supervisar, limitar o modificar datos a través del 'cortafuegos' y selecciona información interna, estructuras y situaciones operativas de una red hacia el exterior lo más posible, con el fin de proteger una red Intranet.

Recientemente, con la aparición y desarrollo de la tecnología de Red Privada Virtual (VPN), la tecnología del Cortafuegos Virtual (VFW) apareció consecuentemente. Un VFW es una sub-entidad lógica derivada de un sistema cortafuegos principal y se presenta a un usuario como un cortafuegos independiente. Después de que se establezca un VFW, el sistema cortafuegos principal presentado por un usuario se denomina un cortafuegos raíz. El número del cortafuegos raíz es uno y los VFWs pueden crearse de forma dinámica en conformidad con las configuraciones y el número de los VFWs es al menos uno. Cuando los VFWs lógicos se establecen sobre la base de un cortafuegos, se satisfacen las demandas del sistema y al mismo tiempo, los rendimientos restantes en el sistema se utilizan para proporcionar servicios de arrendamiento para conseguir más altos rendimientos. Actualmente la tecnología de VPN se ha convertido en una tecnología básica de la tecnología de VFW. Cada VFW es un complejo de una instancia de VPN, una instancia de seguridad y una instancia de configuración y es capaz de proporcionar a un usuario de los VFWs un plano de reenvío de rutas privadas, servicios de seguridad y plano de gestión de configuración.

Con el desarrollo rápido de las tecnologías de seguridad de redes, cada vez más empresas, a gran escala, utilizan las redes Internet para establecer redes VPN utilizando la tecnología de seguridad de protocolo Internet (IPSec). El protocolo IPSec proporciona datos IP con alta calidad, interoperables y un rendimiento de seguridad basado en la criptología. La encriptación y la autenticación origen de datos se realiza en la capa de IP entre partes de comunicaciones específicas para garantizar la confidencialidad, integridad y la autenticidad cuando se transmiten datos a través de las redes.

En la técnica anterior (según se ilustra, a modo de ejemplo, en el documento CN 1949741 A), cuando se procesa un flujo de datos a través de diferentes cortafuegos, una zona de seguridad privada y una zona de seguridad virtual (VZONE) para transmitir el flujo de datos se establecen en VFW y el cortafuegos raíz, respectivamente. Se establece un puerto en cualquiera de las zonas de seguridad privadas que se establecen en los VFWs y el cortafuegos raíz respectivamente y se establecen políticas de seguridad entre las zonas de seguridad de los VFWs y el cortafuegos raíz, respectivamente. Cuando un flujo de datos se envía a través de cortafuegos, un extremo transmisor filtra el flujo de datos utilizando una política de seguridad entre una zona de seguridad origen de un cortafuegos del flujo de datos y una VZONE del cortafuegos y envía el flujo de datos filtrado a un extremo receptor. El extremo receptor filtra el flujo de datos utilizando una política de seguridad entre una zona de seguridad de destino de un cortafuegos en donde llega el flujo de datos y una zona VZONE del cortafuegos.

En la técnica anterior, cuando se procesa un flujo de datos a través del cortafuegos, cada uno de los cortafuegos necesita configurarse con una VZONE. Además de las políticas de seguridad configuradas entre las zonas de seguridad existentes de los cortafuegos, necesitan configurarse, respectivamente, las políticas de seguridad entre zonas de seguridad privadas y la VZONE en los cortafuegos. Con el incremento de VFWs, el número de VZONEs que necesitan configurarse aumenta también continuamente, necesitándose configurar cada vez más políticas de seguridad y por ello, la configuración se hace muy complicada. Además, en la técnica anterior, cuando los flujos de datos se reenvían a través de cortafuegos, necesita realizarse un filtrado de seguridad sobre los flujos de datos en el extremo transmisor y en el extremo receptor para realizar el reenvío de los flujos de datos, con lo que no solamente es complicado el proceso, sino que también resulta muy difícil gestionar las relaciones inter-zonales entre los cortafuegos.

SUMARIO DE LA INVENCIÓN

Las formas de realización de la presente invención dan a conocer un método para el envío y la recepción de datos a través de VFWs y el método puede simplificar la gestión de las relaciones inter-zonales cuando se reenvían datos a través de diferentes VFWs.

La presente invención da a conocer un método para enviar datos a través de VFWs. Los VFWs se establecen con un túnel de seguridad correspondiente y el túnel de seguridad se establece con una zona de protección. El método

para enviar datos a través de VFWs incluye las etapas siguientes. Un filtrado de seguridad se realiza sobre los datos en el primer cortafuegos virtual utilizando una política de seguridad entre una zona de seguridad de un puerto de entrada de datos y una zona de protección de un túnel de seguridad del primer VFW. Los datos se envían al túnel de seguridad del primer VFW. El túnel de seguridad del primer VFW encripta los datos que pasan el filtrado de seguridad. Los datos encriptados se envían a un segundo VFW a través del túnel de seguridad del primer VFW. El segundo VFW está configurado para enviar los datos.

La presente invención da a conocer un método para recibir datos a través de VFWs. Los VFWs se establecen con un túnel de seguridad correspondiente y el túnel de seguridad se establece con una zona de protección. El método para recibir datos a través de VFWs incluye las etapas siguientes. Un primer VFW recibe los datos que han de desencriptarse, busca un túnel de seguridad para la desencriptación de los datos y envía los datos al túnel de seguridad para su desencriptación. El túnel de seguridad para la desencriptación realiza la desencriptación de los datos y modifica una zona de seguridad de un puerto de entrada de los datos desencriptados en la zona de protección del túnel de seguridad para su desencriptación. Un segundo VFW realiza un filtrado de seguridad sobre los datos utilizando una política de seguridad entre la zona de protección del túnel de seguridad para desencriptación y la zona de seguridad en donde llegan los datos.

La presente invención da a conocer, además, un aparato de envío, que incluye una primera unidad de procesamiento de seguridad, una unidad de encriptación y una unidad de envío. La primera unidad de procesamiento de seguridad se estable con zonas de seguridad, con el establecimiento de políticas de seguridad entre las zonas de seguridad, respectivamente. La unidad de encriptación se establece con una zona de protección.

La primera unidad de procesamiento de seguridad está configurada para realizar un filtrado de seguridad sobre los datos utilizando una política de seguridad entre una zona de seguridad de un puerto de entrada de datos y la zona de protección de la unidad de encriptación y para enviar los datos después del filtrado de seguridad a la unidad de encriptación.

La unidad de encriptación está configurada para encriptar los datos que pasan a través de la primera unidad de procesamiento de seguridad y para enviar los datos encriptados a la unidad de envío.

La unidad de envío está configurada para enviar los datos encriptados por la unidad de encriptación.

La presente invención da a conocer, además, un aparato de recepción, que incluye una unidad de recepción, una unidad de desencriptación y una segunda unidad de procesamiento de seguridad. La segunda unidad de procesamiento de seguridad se establece con zonas de seguridad y las políticas de seguridad se establecen entre las zonas de seguridad. La unidad de desencriptación se establece con una zona de protección.

La unidad de recepción está configurada para recibir datos que han de desencriptarse, para buscar la unidad de desencriptación de los datos y para enviar los datos a la unidad de desencriptación.

La unidad de desencriptación está configurada para desencriptar los datos que han de desencriptarse y se reciben por la unidad de recepción y para modificar una zona de seguridad de un puerto de entrada de los datos en la zona de protección de la unidad de desencriptación.

La segunda unidad de procesamiento de seguridad está configurada para realizar un filtrado de seguridad sobre los datos utilizando una política de seguridad entre la zona de protección y la unidad de desencriptación y la zona de seguridad donde llegan los datos.

Puede deducirse de las soluciones técnicas que, en conformidad con las soluciones técnicas de la presente invención, se adopta el método anterior para reenviar datos a través de VFWs usando un túnel de seguridad, de modo que se garantice la seguridad de la transmisión de datos y al mismo tiempo, se simplifica la gestión de las relaciones inter-zonales entre diferentes VFWs. Una política de seguridad entre dos zonas en el interior de un VFW se usa directamente para realizar un filtrado de seguridad sobre un flujo de datos y de este modo, las relaciones inter-zonales se gestionan de una manera simple cuando el flujo de datos cruza los VFWs. Por lo tanto, el reenvío de datos a través de los VFWs se consigue sin adoptar un método de adición de políticas de seguridad entre zonas de seguridad en varios VFWs diferentes en la configuración para procesar la relación interzonal en la técnica anterior, cuando se reenvían los datos a través de los VFWs y por ello, la configuración es simple y es cómoda de gestionar. Mediante este método, se realiza efectivamente la reutilización de puertos de los VFWs y se economizan recursos en gran medida.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

Para ilustrar las soluciones técnicas en conformidad con las formas de realización de la presente invención o en la técnica anterior con mayor claridad, se introducen brevemente a continuación los dibujos adjuntos para describir las formas de realización de la técnica anterior. Evidentemente, los dibujos adjuntos en la siguiente descripción son solamente algunas formas de realización de la presente invención y los expertos ordinarios en esta técnica pueden

derivar otros dibujos a partir de los dibujos adjuntos sin necesidad de esfuerzos creativos.

La Figura 1 es una vista estructural esquemática de los denominados cortafuegos en conformidad con una forma de realización de la presente invención;

La Figura 2 es un diagrama de flujo esquemático de envío de datos a través de cortafuegos en conformidad con una forma de realización de la presente invención;

La Figura 3 es un diagrama de flujo esquemático de recepción de datos a través de cortafuegos en conformidad con una forma de realización de la presente invención;

La Figura 4 es una vista esquemática de un aparato de envío en conformidad con una forma de realización de la presente invención;

La Figura 5 es una vista esquemática de un aparato de recepción en conformidad con una forma de realización de la presente invención; y

La Figura 6 es una vista esquemática de un sistema de redes de utilidad para el entendimiento de la presente invención.

DESCRIPCIÓN DETALLADA DE LAS FORMAS DE REALIZACIÓN DE LA INVENCIÓN

La solución técnica de la presente invención se describirá, con mayor claridad, a continuación, haciendo referencia a los dibujos adjuntos. Es evidente que las formas de realización que se describen son solamente una parte y no la totalidad de las formas de realización de la presente invención. Todas las demás formas de realización obtenidas por expertos en esta técnica, sobre la base de las formas de realización de la presente invención sin necesidad de esfuerzos creativos, caerán dentro del alcance de protección de la presente invención.

Con el fin de poner en práctica las formas de realización de la presente invención, en primer lugar, una vista esquemática de configuración de los cortafuegos necesarios en las soluciones técnicas en las formas de realización de la presente invención necesita entenderse. Para facilidad de la descripción, se describe, a modo de ejemplo, la creación de 3 VFWs en un cortafuegos raíz. Conviene señalar que el cortafuegos raíz puede considerarse como un VFW especial.

Según se ilustra en la Figura 1, VFW0, VFW1 y VFW2 son tres VFWs del cortafuegos raíz. El Puerto 0, el Puerto 1 y el Puerto 2 se establecen en VFW0, VFW1 y VFW2 respectivamente. Cada VFW tiene múltiples zonas de seguridad divididas respectivamente. En la forma de realización de la presente invención, el VFW, a modo de ejemplo, está dividido en 2 zonas de seguridad, que incluyen una zona de no-confianza y una zona de confianza. Políticas de seguridad se establecen entre las zonas de seguridad de cada VFW.

Una línea de trazos a en la Figura 1 representa una dirección de flujo de datos enviados por VFW1 y los datos se envían a través del Puerto 0 de VFW0. Una línea de trazos a' en la Figura 1 representa los datos de respuesta que se proporcionan en respuesta a los datos que se representan por la línea de trazos a y se reciben por VFW1 y los datos entran a través del Puerto 0 de VFW0. Con el fin de proteger los datos enviados por VFW1, se configura un túnel IPSec1 y una salida de IPSec1 es el Puerto 0 de VFW0. Conviene señalar que IPSec1 es "unidireccional". En este caso, el término "unidireccional" significa que IPSec1 protege los datos (que se representan por la línea de trazos a en la Figura 1) que se envían por VFW1 y necesitan enviarse a una red pública a través de VFW0 y los datos de respuesta en respuesta a los datos que se envían por VFW1 y necesitan enviarse a una red pública a través de VFW0 (según se ilustra en la Figura 1, los datos de respuesta en respuesta a los datos representados por la línea de trazos a se representa por la línea de trazos a'). Es decir, solamente los datos que se envían por VFW1 y necesitan enviarse a la red pública por VFW0 o los datos de respuesta en respuesta a los datos recibidos por VFW0 les está permitido entrar en IPSec1 para su encriptación o desencriptación. Los datos que se envían desde VFW0 e intentan pasar a través de VFW1 solamente pueden protegerse por otro túnel IPSec que está configurado para VFW0 y pasan a través de VFW1. Con el fin de gestionar las relaciones inter-zonales cuando los datos cruzan los VFWs, una zona de protección está configurada para IPSec1 y la zona de protección de IPSec1 es la zona de no-confianza de VFW1. Conviene señalar que la zona de protección del IPSec1 no está limitada a la zona de no-confianza en VFW1 y puede ser cualquier zona de seguridad en VFW1.

En consecuencia, una línea de trazos b en la Figura 1 representa una dirección de flujo de datos enviados por VFW2 y los datos se envían también a través del Puerto0 de VFW0. Una línea de trazos b' en la Figura 1 representa datos de respuesta en respuesta a los datos que se representan por la línea de trazos b y se reciben por VFW2 y los datos de respuesta entran a través del Puerto0 de VFW0. Con el fin de proteger los datos enviados por VFW2, se configura un túnel IPSec2 y una salida del IPSec2 es el Puerto0 de VFW0. Conviene señalar también que IPSec2 es también "unidireccional" es decir, IPSec2 solamente protege los datos que se envían desde VFW2 y necesitan enviarse a la red pública a través de VFW0 (según se representa por la línea de trazos b en la Figura 1) y los datos de respuesta en respuesta a los datos (según se ilustra en la Figura 1, los datos de respuesta en respuesta a los

datos representados por la línea de trazos *b* se representa por la línea de trazos *b'*). Con el fin de gestionar las relaciones inter-zonales cuando los datos cruzan los VFWs, se configura una zona de protección para IPSec2 y la zona de protección de IPSec2 es la zona de no-confianza de VFW2. La zona de protección de IPSec2 no está limitada a la zona de no-confianza en VFW2 y puede ser cualquier zona de seguridad en VFW2.

La Figura 2 es un diagrama de flujo esquemático de envío de datos a través de VFWs en conformidad con una forma de realización de la presente invención e ilustra el proceso del procesamiento de datos cuando lo datos se envían por los VFWs en la forma de realización de la presente invención. En adelante, el proceso de procesamiento se describe concretamente con referencia al procedimiento de envío de los flujos de datos representados por las líneas de trazos a y b en la Figura 1 a través de los VFWs.

En la etapa 201, se realiza un filtrado de seguridad sobre los datos en un primer VFW utilizando una política de seguridad entre una zona de seguridad de un puerto de entrada de datos una zona de protección de un túnel IPSec de un primer VFW y los datos después del filtrado de seguridad se envían a un túnel IPSec del primer VFW;

Según se ilustra en la Figura 1, en la línea de trazos a en la Figura 1 representa los datos enviados por VFW1 y los datos necesitan pasar a través de VFW0. Cuando se envían los datos, VFW1 realiza primero el procesamiento de seguridad y defensa sobre los datos que han de enviarse y reciben por el Puerto1 de VFW1. Durante la configuración, VFW1 se configura con IPSec1 para protección de datos y una zona de seguridad de no-confianza de VFW1 se establece como una zona de protección de IPSec1. Por lo tanto, cuando los datos se envían desde VFW1, se realiza un filtrado de seguridad sobre los datos utilizando la política de seguridad entre la zona de confianza del Puerto1 en donde los datos entran y la zona de protección de IPSec1 de VFW1. La línea de trazos b, en la Figura 1, representa los datos enviados por VFW2 y los datos necesitan pasar a través de VFW0. Durante la configuración, VFW2 se configura con IPSec2 para protección de datos y una zona de seguridad de no-confianza de VFW2 se establece como una zona de protección del IPSec2. Por lo tanto, cuando se envían los datos desde VFW2, se realiza un filtrado de seguridad sobre los datos utilizando la política de seguridad entre la zona de confianza del Puerto2 en donde los datos entran y la zona de protección de IPSec2 de unidad de VFW2.

En la etapa 202, el túnel IPSec del primer VFW encripta los datos que pasan a través del filtrado de seguridad y los datos encriptados se envían a un segundo VFW a través del túnel IPSec.

Según se ilustra en la Figura 1, después de que los datos representados por la línea de trazos a pasen por el filtrado de seguridad, IPSec1 de VFW1 encripta los datos y los datos encriptados se reenvían desde VFW0 a la red pública. De forma similar, después de que los datos representados por la línea de trazos b pasen por el filtrado de seguridad, IPSec2 de VFW2 encripta los datos y los datos encriptados se reenvían desde VFW0 a la red pública.

Un método para enviar los datos encriptados al segundo VFW en la etapa 202 puede incluir, sin limitación, a: etiquetado de los datos encriptados con una etiqueta del segundo VFW o marcado del segundo VFW de los datos en una lista de reenvío de los datos.

En la etapa 203, el segundo VFW envía los datos.

En esta forma de realización, se configura el túnel IPSec, se garantiza la seguridad del reenvío de los datos a través de los VFWs. Además, IPSec1 e IPSec2 se configuran, respectivamente con la zona de protección de IPSec1 y la zona de protección de IPSec2 y la zona de protección de IPSec1 es la zona de seguridad de no-confianza original de VFW1 y la zona de protección de IPSec2 es también la zona de seguridad de no-confianza original de VFW2. Por lo tanto, cuando VFW1 envía los datos, se realiza el filtrado de seguridad sobre los datos utilizando la política de seguridad entre las zonas de seguridad de VFW1 es decir, todas las relaciones inter-zonales para realizar el procesamiento de seguridad y de defensa son las relaciones inter-zonales de VFW1 y de este modo, se simplifica el proceso para gestionar las relaciones inter-zonales durante el envío de VFW en la técnica anterior. De forma similar, cuando VFW2 envía los datos, el filtrado de seguridad se realiza también sobre los datos utilizando la política de seguridad entre las zonas de seguridad de VFW2. Cuando se toman algunas medidas al respecto, los datos encriptados por IPSec1 e IPSec2 pueden entrar en VFW0 para el reenvío, de modo que los datos en múltiples VFWs puedan reenviarse a través del mismo puerto y de este modo, se reutiliza el puerto y se economizan recursos.

La Figura 3 es un diagrama de flujo esquemático de recepción de datos a través de VFWs en conformidad con una forma de realización de la presente invención e ilustra el proceso de procesamiento de los datos cuando los VFWs reciben los datos en conformidad con la forma de realización de la presente invención. Todos los datos son los datos que han de desencriptarse y la dirección de destino de los datos se dirige a un terminal local. Para facilidad de descripción, a modo de ejemplo, el proceso del procesamiento de datos de respuesta (según se representa por las líneas de trazos a' y b' en la Figura 1) de los datos (según se representa por las líneas de trazos a y b en la Figura 1) enviados por VFW1 y VFW2 en la forma de realización anterior, se describen, en detalle, a continuación.

En la etapa 301, un primer VFW recibe datos que han de desencriptarse y un túnel IPSec para desencriptación de los datos que han de desencriptarse se busca a este respecto, y luego, los datos se envían al túnel IPSec.

Según se ilustra en la Figura 1, la línea de trazos a' en la Figura 1 representa los datos de respuesta en respuesta a los datos que se representan por la línea de trazos a y se reciben por VFW1 y los datos de respuesta entran a través del Puerto0 de VFW0. La línea de trazos b' representa los datos de respuesta en respuesta a los datos que se representan por la línea de trazos b y se reciben por VFW2 y los datos de respuesta entran también a través del Puerto0 de VFW0. Por lo tanto, el VFW0 origen realiza la operación de búsqueda por túneles para la desencriptación sobre los datos de respuesta que entran y envía los datos de respuesta representados por a' al túnel IPSec1 para su desencriptación y envía los datos de respuesta representados por b' al túnel IPSec2 para su desencriptación.

En la etapa 302, el túnel IPSec desencripta los datos y modifica una zona de seguridad de un puerto de entrada de los datos desencriptados en una zona de protección del túnel IPSec.

Según se ilustra en la Figura 1, después de desencriptar los datos de respuesta representados por a', IPSec1 modifica un parámetro que indica la zona de seguridad a la que pertenece el puerto de entrada de los datos (es decir, la zona de confianza del Puerto0 de VFW0) en la zona de protección de IPSec1 (es decir, la zona de no-confianza de VFW1). Después de desencriptar los datos de respuesta representados por b', IPSec2 modifica un parámetro que indica la zona de seguridad a la que pertenece el puerto de entrada de los datos (es decir, la zona de confianza del Puerto0 de VFW0) en la zona de protección de IPSec2 (es decir, la zona de no-confianza de VFW2).

En la etapa 303, un segundo VFW realiza un filtrado de seguridad sobre los datos utilizando una política de seguridad entre la zona de protección del túnel IPSec y la zona de seguridad en donde llegan los datos.

Según se ilustra en la Figura 1, después de que los datos de respuesta representados por la línea de trazos a' entran en VFW1, se realiza un filtrado de seguridad sobre los datos usando la política de seguridad entre la zona de protección de IPSec1 (es decir, la zona de seguridad de no-confianza de VFW1) y la zona de seguridad en donde llegan los datos (es decir, la zona de confianza de VFW1); y después de que los datos de respuesta representados por la línea de trazos b' entran en VFW2, se realiza el filtrado de seguridad sobre los datos usando la política de seguridad entre la zona de protección de IPSec2 (es decir, la zona de seguridad de no-confianza de VFW2) y la zona de seguridad en donde llegan los datos (es decir, la zona de confianza de VFW2).

Un método para la búsqueda de túneles para desencriptar los datos en la etapa 301 se pone en práctica buscando un IP de destino de los datos, una interfaz Periférica Serie (SPI, es decir, un campo de protocolo en el protocolo de Cabecera de Autenticación (AH), un protocolo de Carga Útil de Seguridad de Encapsulación (ESP)) y un tipo de protocolo. Los túneles que necesitan los datos para entrar se buscan por intermedio del IP de destino, la SPI y el tipo de protocolo.

Un método para modificar la zona de seguridad del puerto de entrada de los datos desencriptados en la etapa 302 puede incluir, sin limitación, a: etiquetado de los datos con una etiqueta de la zona de protección del túnel IPSec o la indicación en una lista de reenvío de los datos que la zona de seguridad a la que pertenece el puerto de entrada de los datos es la zona de protección del túnel IPSec.

Puede deducirse de la forma de realización anterior, en las soluciones técnicas de las formas de realización de la presente invención, que cuando un VFW recibe los datos de respuesta como un cortafuegos de terminal local, el túnel IPSec utilizando cuando el VFW envía los datos puesto que se utiliza un cortafuegos de terminal local y de este modo, se garantiza la seguridad de los datos. Además, cuando se modifica la zona de entrada con los datos, con el fin de gestionar la relaciones inter-zonales cuando los datos cruzan los VFWs, solamente la política de seguridad entre la zona de seguridad existente del segundo VFW en donde los datos que llegan necesitan utilizarse para realizar un filtrado de seguridad sobre los datos, por lo que se simplifica el proceso complicado para gestionar las relaciones inter-zonales en la técnica anterior.

En los métodos para enviar y recibir datos a través de los VFWs en conformidad con las formas de realización anteriores de la presente invención, el número de los puertos de VFWs se controla por el equipo de cortafuegos que se utiliza y no está limitado a 3 puertos según se ilustra en la Figura 1. Los puertos en las formas de realización de la presente invención no están limitados a los puertos físicos o puertos virtuales, solamente si los puertos pueden establecerse en los VFWs. El número de VFWs se determina en función del número de puertos, es decir, cada puerto virtual está configurado con un VFW. En las formas de realización de la presente invención, un puerto en cualquier VFW puede utilizarse como un puerto de entrada común de otros VFWs, tal como el Puerto0 en la Figura 1.

En las soluciones técnicas para enviar y recibir datos a través de los VFWs en conformidad con las formas de realización de la presente invención, cualquier salida puede establecerse para los datos que necesitan reenviarse a través de los VFWs, solamente se configura un túnel IPSec correspondiente para los VFWs antes de que se reenvíen los datos. A modo de ejemplo, los datos en VFW1 pueden enviarse a través de VFW0 y pueden enviarse también a través de VFW2. De forma similar, los datos enviados por VFW0 pueden enviarse también a través de VFW1 o VFW2.

Los métodos para enviar o recibir datos a través de los VFWs, en conformidad con las formas de realización de la

presente invención no son solamente aplicables a los datos que se reenvían entre VFWs, sino que también son aplicables a datos que se reenvían entre un cortafuegos raíz y un VFW cuando el cortafuegos raíz se considera como un VFW especial.

En las soluciones técnicas en conformidad con las formas de realización de la presente invención, cuando se procesan los datos a través de los VFWs, puesto que se utiliza la tecnología de IPSec y el túnel IPSec está configurado con la zona de protección, la seguridad está garantizada cuando los datos se envían a través de los VFWs, sin necesidad de que tenga que configurarse ninguna VZONE adicional y el filtrado de seguridad se realiza sobre los datos utilizando las zonas de seguridad existentes de los VFWs y la política de seguridad entre las zonas. Por lo tanto, se elimina la configuración complicada de las políticas de seguridad inter-zonales y solamente se requiere un tiempo de filtrado de seguridad para garantizar la seguridad de los datos durante la transmisión de datos y se reduce los procesos para gestionar las relaciones inter-zonales. Además, puesto que se utiliza la tecnología IPSec, los datos pueden reenviarse desde un VFW a otro VFW y los puertos se pueden compartir, con lo que se reutilizan los puertos de cortafuegos y se consigue una gran económica de recursos.

Los expertos ordinarios en esta técnica pueden entender que la totalidad o parte de las etapas del método dado a conocer por las formas de realización de la presente invención puede ponerse en práctica por un programa que proporcione instrucciones al hardware pertinente. El programa puede memorizarse en un soporte de memorización legible por ordenador. Cuando se ejecuta el programa, pueden incluirse los procedimientos de las formas de realización de los métodos anteriores. El soporte de memorización puede ser un disco magnético, una memoria de solamente lectura-disco compacto (CD-ROM), una memoria de solamente lectura (ROM) o una memoria de acceso aleatorio (RAM).

La Figura 4 es una vista esquemática de un aparato de envío en conformidad con una forma de realización de la presente invención. El aparato de envío incluye una primera unidad de procesamiento de seguridad 401, una unidad de encriptación 402 y una unidad de envío 403. La primera unidad de procesamiento de seguridad 401 y la unidad de envío 403 se establecen con zonas de seguridad (incluyendo una zona de no-confianza y una zona de confianza). Se establecen políticas de seguridad entre las zonas de seguridad de la primera unidad de procesamiento de seguridad 401 y entre las zonas de seguridad de la unidad de envío 403, respectivamente. La unidad de encriptación 402 incluye un módulo de encriptación 4021 y un módulo de etiquetado 4022. El módulo de encriptación 4021 está configurado para encriptar datos en la primera de unidad de procesamiento de seguridad 401. El módulo de etiquetado 4022 está configurado para hacer que los datos encriptados entren en la unidad de envío. La unidad de encriptación 402 se establece con una zona de protección y la zona de protección es la zona de no-confianza de la primera unidad de procesamiento de seguridad 401. Conviene señalar que la zona de protección no está limitada a la zona de no-confianza de la primera unidad de procesamiento de seguridad 401 y puede ser cualquier zona de seguridad de la primera unidad de procesamiento de seguridad 401.

La primera unidad de procesamiento de seguridad 401 está configurada para realizar el filtrado de seguridad sobre los datos utilizando una política de seguridad entre una zona de seguridad de un puerto de entrada de datos y la zona de protección de la unidad de encriptación 402 y envía los datos después del filtrado de seguridad a la unidad de encriptación 402.

La unidad de encriptación 402 está configurada para encriptar los datos que pasan por la primera unidad de procesamiento de seguridad 401 y para enviar los datos encriptados a la unidad de envío 403.

La unidad de encriptación 402 incluye el módulo de encriptación 4021 y el módulo de etiquetado 4022. El módulo de encriptación 4021 está configurado para encriptar los datos procedentes de la primera unidad de procesamiento de seguridad 401. El módulo de etiquetado 4022 está configurado para enviar los datos encriptados por el módulo de encriptación 4021 a la unidad de envío 403. Un método para enviar los datos a la unidad de envío 403 incluye, sin limitación, a: etiquetado de los datos encriptados con una etiqueta de la unidad de envío 403 o la indicación a la unidad de envío 403 en una lista de reenvío de los datos por el módulo de etiquetado 4022.

La unidad de envío 403 está configurada para enviar los datos encriptados por la unidad de encriptación 402.

En este caso, el aparato de envío incluye cortafuegos o equipos del tipo de cortafuegos y la unidad de encriptación puede ser un túnel IPSec.

La Figura 5 es una vista esquemática de un aparato de recepción en conformidad con una forma de realización de la presente invención. El aparato de recepción incluye una unidad de recepción 501, una unidad de desencriptación 502 y una segunda unidad de procesamiento de seguridad 503. La unidad de recepción 501 y la segunda unidad de procesamiento de seguridad 503 se establecen con zonas de seguridad (incluyendo una zona de no-confianza y una zona de confianza). Se establecen políticas de seguridad entre las zonas de seguridad de la unidad de recepción 501 y entre las zonas de seguridad de la segunda unidad de procesamiento de seguridad 503, respectivamente. La unidad de desencriptación 502 incluye un módulo de desencriptación 5021 y un módulo de modificación 5022. El módulo de desencriptación 502 se establece con una zona de protección. La zona de protección es la zona de no-confianza de la segunda unidad de procesamiento de seguridad 503. Conviene señalar que la zona de protección no

está limitada a la zona de no-confianza de la segunda unidad de procesamiento de seguridad 503 y puede ser cualquier zona de seguridad de la segunda unidad de procesamiento de seguridad 503.

La unidad de recepción 501 está configurada para recibir los datos que han de desencriptarse, para buscar la unidad de desencriptación de los datos y para enviar los datos a la unidad de desencriptación 502. Una dirección de destino de los datos que han de desencriptarse es un terminal local.

Un método para la búsqueda de la unidad de desencriptación incluye la búsqueda de un IP de destino de los datos, una SPI (un campo de protocolo en el protocolo AH, protocolo ESP) y un tipo de protocolo son todos ellos objeto de búsqueda. La unidad de desencriptación 502 a la que se requiere que entren los datos se busca a través de IP de destino, la SPI y el tipo de protocolo.

La unidad de desencriptación 502 está configurada para desencriptar los datos que han de desencriptarse y se reciben por la unidad de recepción 501 y para cambiar una zona de seguridad de un puerto de entrada de los datos a la zona de protección de la unidad de desencriptación 502.

La unidad de desencriptación 502 incluye un módulo de desencriptación 5021 y un módulo de modificación 5022. El módulo de desencriptación 5021 desencripta los datos que han de desencriptarse. El módulo de modificación 5022 está configurado para modificarla zona de seguridad a la que pertenece el puerto de entrada de los datos desencriptados por el módulo de desencriptación 5021 en la zona de protección de la unidad de desencriptación 502. Un método para modificar la zona de seguridad a la que pertenece el puerto de entrada de los datos por el módulo de modificación 5022 puede incluir, sin limitación, a: etiquetado de los datos con una etiqueta de la zona de protección de la unidad de desencriptación 502 o la indicación en una lista de reenvío de los datos de que la zona de seguridad del puerto de entrada de los datos es la zona de protección de la unidad de desencriptación 502.

La segunda unidad de procesamiento de seguridad 503 está configurada para realizar un procesamiento de seguridad y defensa sobre los datos desencriptados por la unidad de desencriptación 502. El procesamiento de seguridad y de defensa se consigue realizando un filtrado de seguridad sobre los datos utilizando una política de seguridad entre la zona de protección de la unidad de desencriptación 502 y la zona de seguridad en donde llegan los datos.

En este caso, el aparato de recepción incluye los denominados cortafuegos o equipos del tipo de cortafuegos y la unidad de desencriptación puede ser un túnel IPSec.

La primera unidad de procesamiento de seguridad del aparato de envío y la segunda unidad de procesamiento de seguridad del aparato de recepción pueden ser físicamente una misma unidad. De forma similar, la unidad de encriptación del aparato de envío y la unidad de desencriptación del aparato de recepción pueden ser también una misma unidad y la unidad de envío del aparato emisor y la unidad de recepción del aparato receptor puede ser también la misma unidad.

La Figura 6 es una vista esquemática de un sistema de redes que es de utilidad para entender la presente invención. El sistema de redes incluye un aparato de envío 601 y un aparato de recepción 602.

El aparato de envío 601 está configurado para enviar datos.

El aparato de recepción 602 está configurado para recibir datos de respuesta que son en respuesta a los datos enviados por el aparato de envío 601. Los datos de respuesta son los datos que han de desencriptarse con una dirección de destino dirigida a un terminal local.

El aparato de envío 601 incluye una primera unidad de procesamiento de seguridad 6011, una unidad de encriptación 6012 y una unidad de envío 6013. La unidad de encriptación 6012 incluye un módulo de encriptación 60121 y un módulo de etiquetado 60122.

La primera unidad de procesamiento de seguridad 6011 y la unidad de envío 6013 se establecen con zonas de seguridad (que incluye una zona de no-confianza y una zona de confianza). Se establecen políticas de seguridad entre las zonas de seguridad de la primera unidad de procesamiento de seguridad 6011. De forma similar, se establecen también políticas de seguridad entra la zona de seguridad de la unidad de envío 6013. La unidad de encriptación 6012 se establece con una zona de protección. La zona de protección de la unidad de encriptación 6012 es la zona de no-confianza de la primera unidad de procesamiento de seguridad 6011. Conviene señalar que la zona de protección de la unidad de encriptación 6012 no está limitada a la zona de no-confianza de la primera unidad de procesamiento de seguridad 6011 y puede ser cualquier zona de seguridad de la primera unidad de procesamiento de seguridad 6011.

La primera unidad de procesamiento de seguridad 6011 está configurada para realizar un filtrado de seguridad sobre los datos utilizando una política de seguridad entre una zona de seguridad de un puerto de entrada de datos y la zona de protección de la unidad de encriptación 6012 y para enviar los datos a los que se ha realizado un filtrado de

seguridad a la unidad de encriptación 6012.

La unidad de encriptación 6012 está configurada para encriptar los datos que pasan por la primera unidad de procesamiento de seguridad 6011 y para enviar los datos a la unidad de envío 6013.

La unidad de encriptación 6012 incluye un módulo de encriptación 60121 y el módulo de etiquetado 60122. El módulo de encriptación 60121 está configurado para encriptar datos procedentes de la primera unidad de procesamiento de seguridad 6011. El módulo de etiquetado 60122 está configurado para enviar los datos encriptados por el módulo de encriptación 60121 a la unidad de envío 6013. Un método para enviar los datos a la unidad de envío 6013 incluye, sin limitación, a: el etiquetado de los datos encriptados con una etiqueta de la unidad de envío o la indicación de la unidad de envío 6013 en una lista de reenvío de los datos por el módulo de etiquetado 60122.

La unidad de envío 6013 está configurada para enviar los datos encriptados por la unidad de encriptación 6012.

El aparato de recepción 602 incluye una unidad de recepción 6021, una unidad de desencriptación 6022 y una segunda unidad de procesamiento de seguridad 6023. La unidad de desencriptación 6022 incluye un módulo de desencriptación 60221 y un módulo de modificación 60222.

La unidad de recepción 6021 y la segunda unidad de procesamiento de seguridad 6023 se establecen también con zonas de seguridad (que incluyen una zona de no-confianza y una zona de confianza). Se establecen políticas de seguridad entre las zonas de seguridad de la unidad de recepción 6021. De forma similar, se establecen también políticas de seguridad entre las zonas de seguridad de la unidad de procesamiento 6023. La unidad de desencriptación 6022 se estable con una zona de protección. La zona de protección de la unidad de desencriptación 6022 es la zona de no-confianza de la segunda unidad de procesamiento de seguridad 6023. Conviene señalar que la zona de protección de la unidad de desencriptación 6022 no está limitada a la zona de no-confianza de la segunda unidad de procesamiento de seguridad 6023 y puede ser cualquier zona de seguridad de la segunda unidad de procesamiento de seguridad 6023.

La unidad de recepción 6021 está configurada para recibir datos que han de desencriptarse, para buscar la unidad de desencriptación de los datos y para enviar los datos a la unidad de desencriptación 6022. Una dirección de destino de los datos que han de desencriptarse es un terminal local.

Un método para buscar la unidad de desencriptación incluye la búsqueda de un IP de destino de los datos, una SPI (un campo de protocolos en protocolo AH, protocolo ESP) y un tipo de protocolo. La unidad de desencriptación 6022 a la que necesitan introducirse los datos se busca a través del IP de destino, de la SPI y del tipo de protocolo.

La unidad de desencriptación 6022 está configurada para desencriptar los datos que han de desencriptarse y se reciben por la unidad de recepción 6021 y para modificar una zona de seguridad de un puerto de entrada de los datos desencriptados en la zona de protección de la unidad de desencriptación 6022.

La unidad de desencriptación 6022 incluye un módulo de desencriptación 60221 y un módulo de modificación 60222. El módulo de desencriptación 60221 está configurado para desencriptar los datos que han de desencriptarse. El módulo de modificación 60222 está configurado para modificar la zona de seguridad a la que pertenece el puerto de entrada de los datos desencriptados por el módulo de desencriptación 60221 en la zona de protección de la unidad de desencriptación 6022. Un método para modificar la zona de seguridad la que pertenece el puerto de entrada de los datos por el módulo de modificación 60222 incluye, sin limitación, a: el etiquetado de los datos con una etiqueta de la zona de protección de la unidad de desencriptación 6022 o la indicación en una lista de reenvío de los datos de que la zona de seguridad del puerto de entrada de datos es la zona de protección de la unidad de desencriptación 6022.

La segunda unidad de procesamiento de seguridad 6023 está configurada para realizar el procesamiento de seguridad y de defensa sobre los datos desencriptados por la unidad de desencriptación 6022. El procesamiento de seguridad y de defensa se consigue realizando un filtrado de seguridad sobre los datos utilizando una política de seguridad entre la zona de protección de la unidad de desencriptación 6022 y la zona de seguridad en donde llegan los datos.

En este caso, el aparato de envío y el aparato de recepción incluyen los denominados cortafuegos o equipos del tipo cortafuegos y la unidad de encriptación y la unidad de desencriptación pueden ser un túnel IPSec.

En el sistema de redes, la primera unidad de procesamiento de seguridad del aparato de envío y la segunda unidad de procesamiento de seguridad del aparato de recepción pueden ser físicamente una misma unidad. De forma similar, la unidad de encriptación del aparato de envío y la unidad de desencriptación del aparato de recepción pueden ser también una misma unidad y la unidad de envío del aparato emisor y la unidad de recepción del aparato receptor puede ser también una misma unidad.

REIVINDICACIONES

1. Un método para enviar datos a través de los denominados 'cortafuegos' virtuales, VFWs, en donde los VFWs se establecen con un túnel de seguridad correspondiente, estableciéndose el túnel de seguridad con una zona de protección y el método para enviar datos a través de los VFWs comprende:

la realización de un filtrado de seguridad (201) de datos en un primer VFW utilizando una política de seguridad entre una zona de seguridad de un puerto de entrada de datos y una zona de protección de un túnel de seguridad del primer VFW y el envío de los datos después del filtrado de seguridad al túnel de seguridad del primer VFW; y

la encriptación (202), por el túnel de seguridad del primer VFW, de los datos que pasan a través del filtrado de seguridad; y el envío, por el túnel de seguridad del primer VFW, de los datos encriptados a un segundo VFW, en donde el segundo VFW está configurado para enviar los datos (203).

2. El método de envío según la reivindicación 1, en donde la zona de protección del túnel de seguridad es una zona de seguridad en un 'cortafuegos' protegido por el túnel de seguridad.

3. El método de envío según la reivindicación 1, en donde un método para enviar los datos encriptados al segundo VFW por el túnel de seguridad comprende: el etiquetado de los datos con una etiqueta del segundo VFW.

4. El método de envío según la reivindicación 1, en donde un método para enviar los datos encriptados al segundo VFW por el túnel de seguridad comprende, además: el marcado del segundo VFW en una lista de reenvío de los datos.

5. Un método para la recepción de datos a través de los denominados 'cortafuegos' virtuales, VFWs, en donde los VFWs se establecen con un túnel de seguridad correspondiente, estableciéndose el túnel de seguridad con una zona de protección y el método para la recepción de datos a través de los VFWs comprende:

la recepción (301), por un primer VFW, de los datos que han de desencriptarse, la búsqueda de un túnel de seguridad para la desencriptación de los datos y el envío de los datos al túnel de seguridad para la desencriptación;

la desencriptación (302), por el túnel de seguridad para desencriptación de los datos, y la modificación de una zona de seguridad de un puerto de entrada de los datos desencriptados en una zona de protección del túnel de seguridad para la desencriptación; y

la realización, por un segundo VFW, del filtrado de seguridad (303) sobre los datos utilizando una política de seguridad entre la zona de protección del túnel de seguridad para la desencriptación y la zona de seguridad en donde llegan los datos.

6. El método de recepción según la reivindicación 5, en donde la zona de protección del túnel de seguridad es una zona de seguridad en un denominado 'cortafuegos' protegido por el túnel de seguridad.

7. El método de recepción según la reivindicación 5, en donde un método para la búsqueda del túnel de seguridad para la desencriptación de los datos comprende: la búsqueda de un IP de destino de los datos, una Interfaz Periférica Serie, SPI y un tipo de protocolo y la búsqueda del túnel de seguridad para la desencriptación en donde se requiere que entren los datos en función del IP de destino, de la SPI y del tipo de protocolo.

8. El método de recepción según la reivindicación 5, en donde un método para modificar la zona de seguridad del puerto de entrada de los datos desencriptados comprende: el etiquetado de los datos con una etiqueta de la zona de protección del túnel de seguridad para desencriptación.

9. El método de recepción según la reivindicación 5, en donde un método para modificar una zona de seguridad origen de los datos desencriptados comprende además: el marcado en una lista de reenvío de los datos debido a que la zona de seguridad a la que pertenece el puerto de entrada de los datos es la zona de protección del túnel de seguridad para la desencriptación.

10. Un aparato de envío, que comprende una primera unidad de procesamiento de seguridad (401), una unidad de encriptación (402) y una unidad de envío (403), en donde la primera unidad de procesamiento de seguridad se establece con zonas de seguridad, estableciéndose políticas de seguridad entre las zonas de seguridad respectivamente y la unidad de encriptación se establece con una zona de protección, en donde

la primera unidad de procesamiento de seguridad está configurada para realizar el filtrado de seguridad sobre los datos utilizando una política de seguridad entre una zona de seguridad de un puerto de entrada de datos y la zona de protección de la unidad de encriptación y para enviar los datos después del filtrado de seguridad a la unidad de encriptación;

la unidad de encriptación está configurada para encriptar los datos procedentes de la primera unidad de procesamiento de seguridad y para enviar los datos encriptados a la unidad de envío; y

la unidad de envío está configurada para enviar los datos encriptados por la unidad de encriptación.

11. El aparato de envío según la reivindicación 10, en donde la zona de protección de la unidad de encriptación es la zona de seguridad de la primera unidad de procesamiento de seguridad.

12. El aparato de envío según la reivindicación 10, en donde la unidad de encriptación comprende un módulo de encriptación (4021) y un módulo de etiquetado (4022);

el módulo de encriptación está configurado para encriptar los datos procedentes de la primera unidad de procesamiento de seguridad; y

el módulo de etiquetado está configurado para etiquetar los datos encriptados por el módulo de encriptación con una etiqueta de la unidad de envío y para enviar los datos encriptados a la unidad de envío; o

el módulo de etiquetado está configurado para marcar la unidad de envío de los datos encriptados en una lista de reenvío de los datos y para enviar los datos encriptados a la unidad de envío.

13. Un aparato de recepción que comprende una unidad de recepción (501), una unidad de desencriptación (502) y una segunda unidad de procesamiento de seguridad (503), en donde la segunda unidad de procesamiento de seguridad se establece con zonas de seguridad y se establecen políticas de seguridad entre las zonas de seguridad, estando la unidad de desencriptación establecida con una zona de protección, en donde

la unidad de recepción está configurada para recibir datos que han de desencriptarse, para buscar la unidad de desencriptación de los datos y para enviar los datos a la unidad de desencriptación;

la unidad de desencriptación está configurada para desencriptar los datos que han de desencriptarse procedentes de la unidad de recepción y para modificar una zona de seguridad de un puerto de entrada de los datos en la zona de protección de la unidad de desencriptación; y

la segunda unidad de procesamiento de seguridad está configurada para realizar un filtrado de seguridad sobre los datos utilizando una política de seguridad entre la zona de protección de la unidad de desencriptación y la zona de seguridad en donde llegan los datos.

14. El aparato de recepción según la reivindicación 13, en donde la zona de protección de la unidad de encriptación es la zona de seguridad de la segunda unidad de procesamiento de seguridad.

15. El aparato de recepción según la reivindicación 13, en donde la unidad de desencriptación comprende un módulo de desencriptación (5021) y un módulo de modificación (5022), en donde

el módulo de desencriptación está configurado para desencriptar los datos que han de desencriptarse recibidos por la unidad de recepción; y

el módulo de modificación está configurado para modificar la zona de seguridad a la que pertenece el puerto de entrada de los datos desencriptados por el módulo de desencriptación en la zona de protección de la unidad de desencriptación.

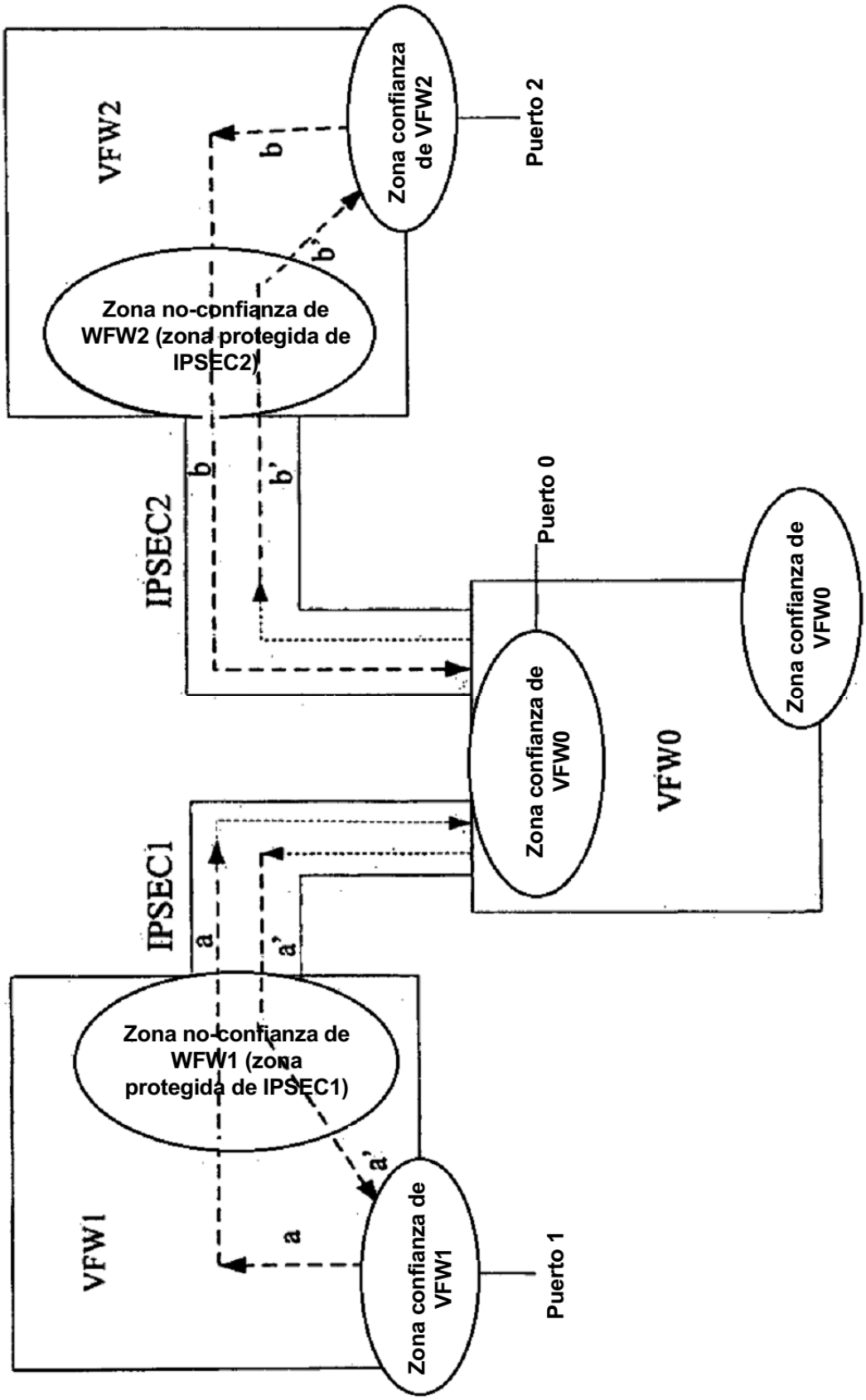
VFW2
Zona confianza de VFW2
Puerto 2
b
b'
Zona no-confianza de WFW2 (zona protegida de IPSEC2)
IPSEC2
Puerto 0
Zona confianza de VFW0
Zona confianza de VFW0
VFW0
IPSEC1
a
a'
Zona no-confianza de WFW1 (zona protegida de IPSEC1)
VFW1
Zona confianza de VFW1
Puerto 1

FIG. 1

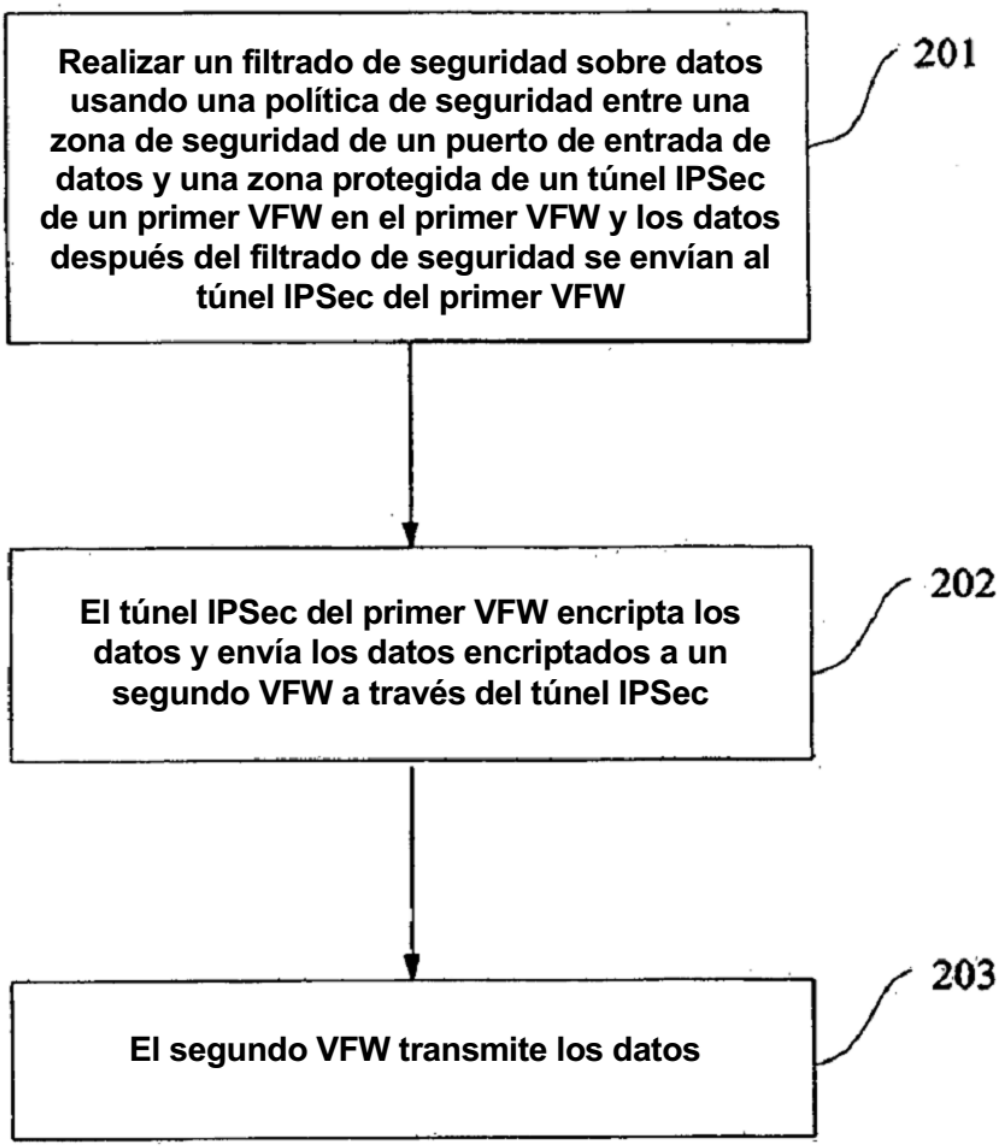
Realizar un filtrado de seguridad sobre datos usando una política de seguridad entre una zona de seguridad de un puerto de entrada de datos y una zona protegida de un túnel IPSec de un primer VFW en el primer VFW y los datos después del filtrado de seguridad se envían al túnel IPSec del primer VFW
201
El túnel IPSec del primer VFW encripta los datos y envía los datos encriptados a un segundo VFW a través del túnel IPSec
202
El segundo VFW transmite los datos
203

FIG. 2

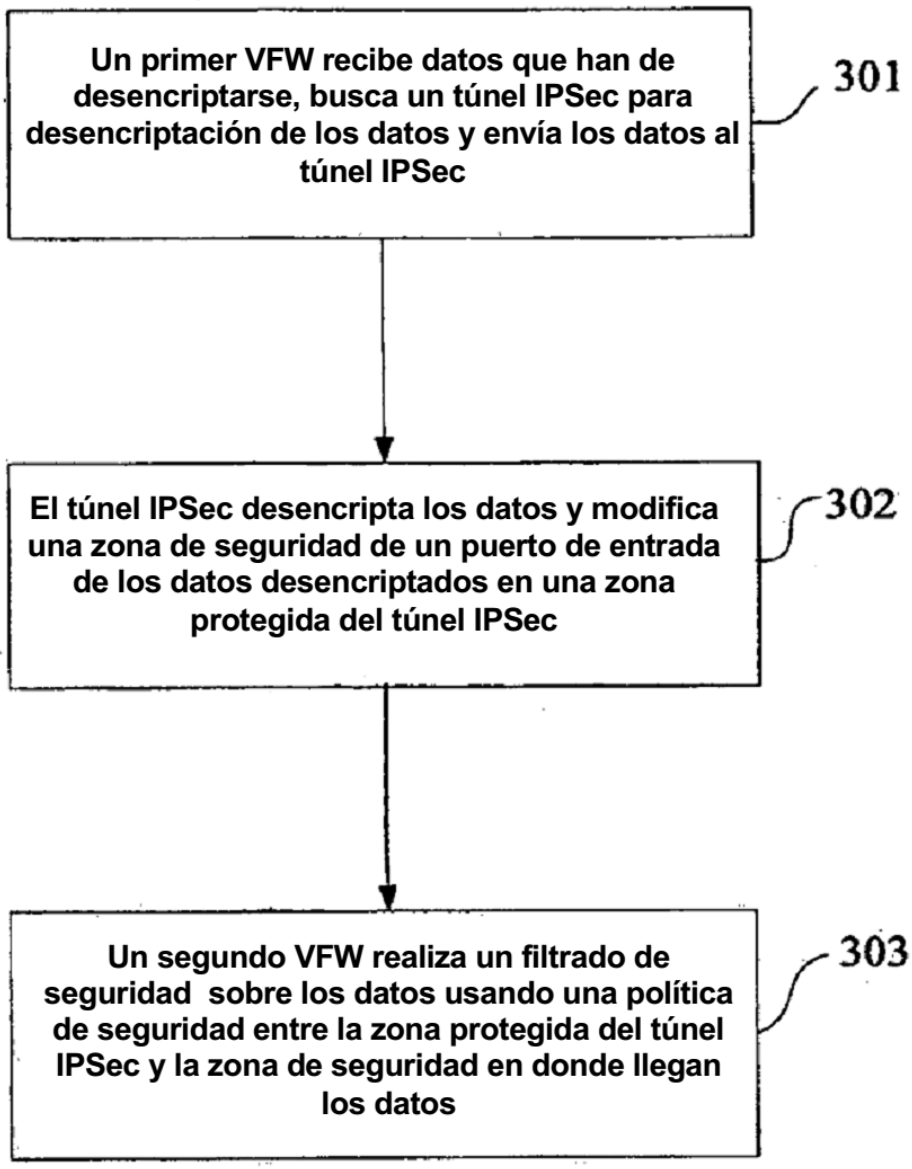
Un primer VFW recibe datos que han de desencriptarse, busca un túnel IPSec para desencriptación de los datos y envía los datos al túnel IPSec
301
El túnel IPSec desencripta los datos y modifica una zona de seguridad de un puerto de entrada de los datos desencriptados en una zona protegida del túnel IPSec
302
Un segundo VFW realiza un filtrado de seguridad sobre los datos usando una política de seguridad entre la zona protegida del túnel IPSec y la zona de seguridad en donde llegan los datos
303

FIG. 3

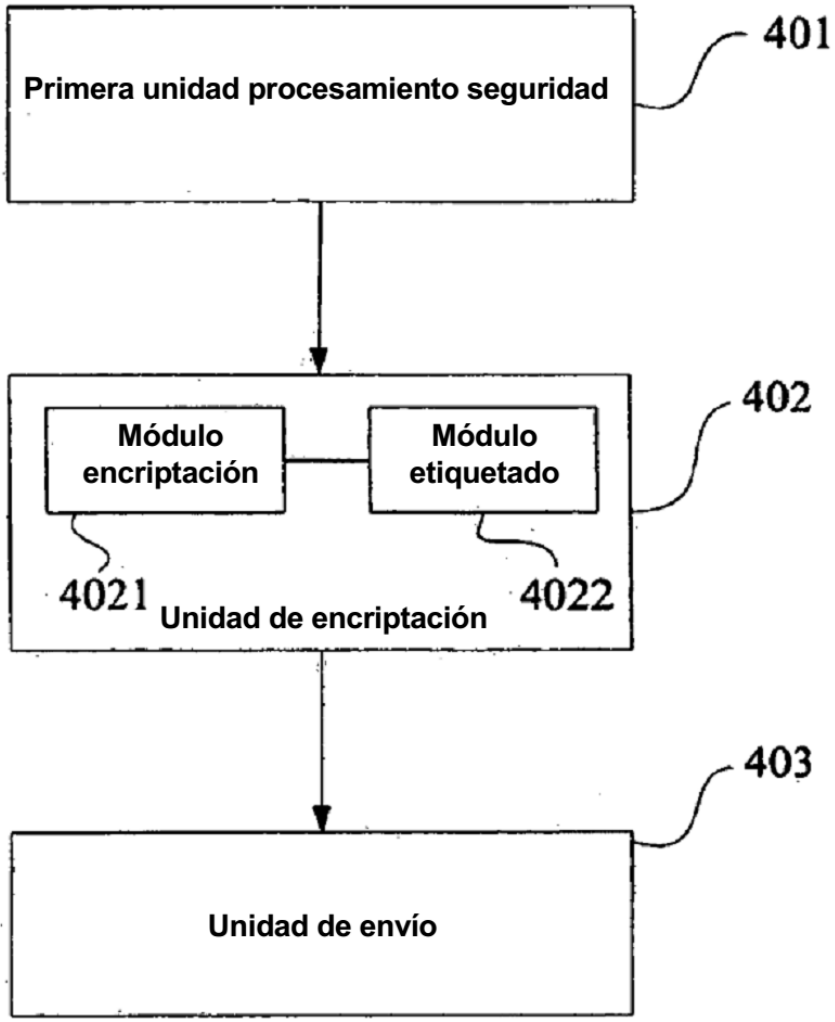
Primera unidad procesamiento seguridad
401
Módulo encriptación
Módulo etiquetado
402
4021
4022
Unidad de encriptación
403
Unidad de envío

FIG. 4

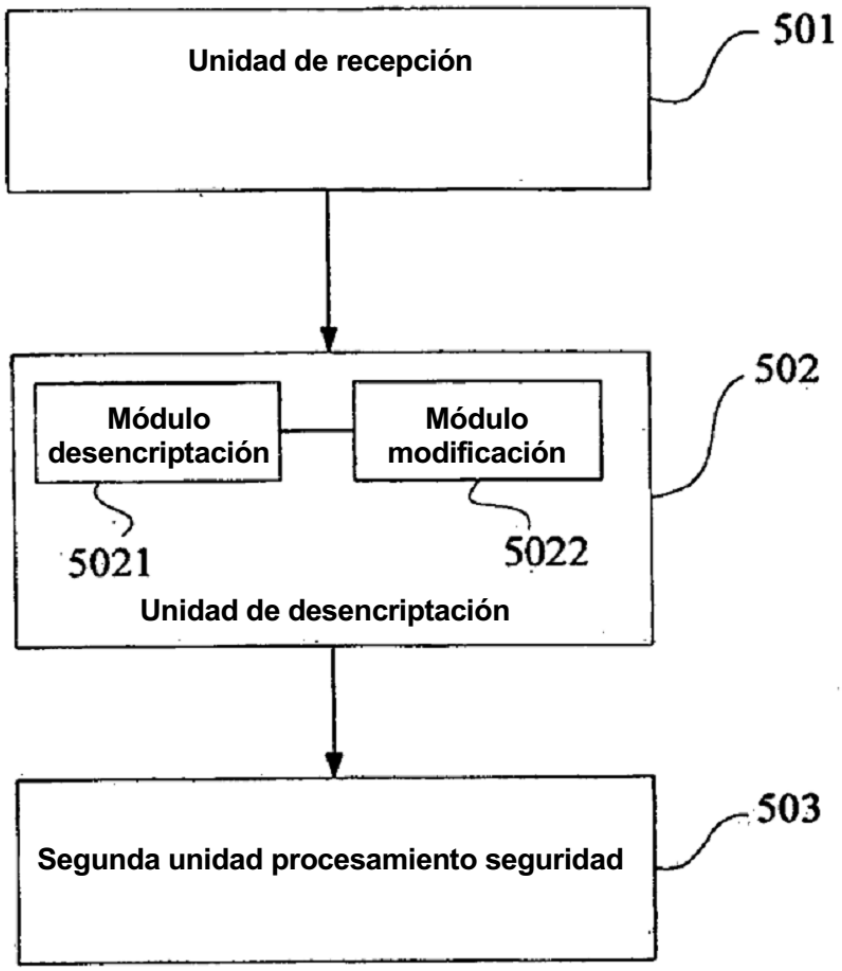
Unidad de recepción
501
Módulo desencriptación
Módulo modificación
502
5021
5022
Unidad de desencriptación
Segunda unidad procesamiento seguridad
503

FIG. 5

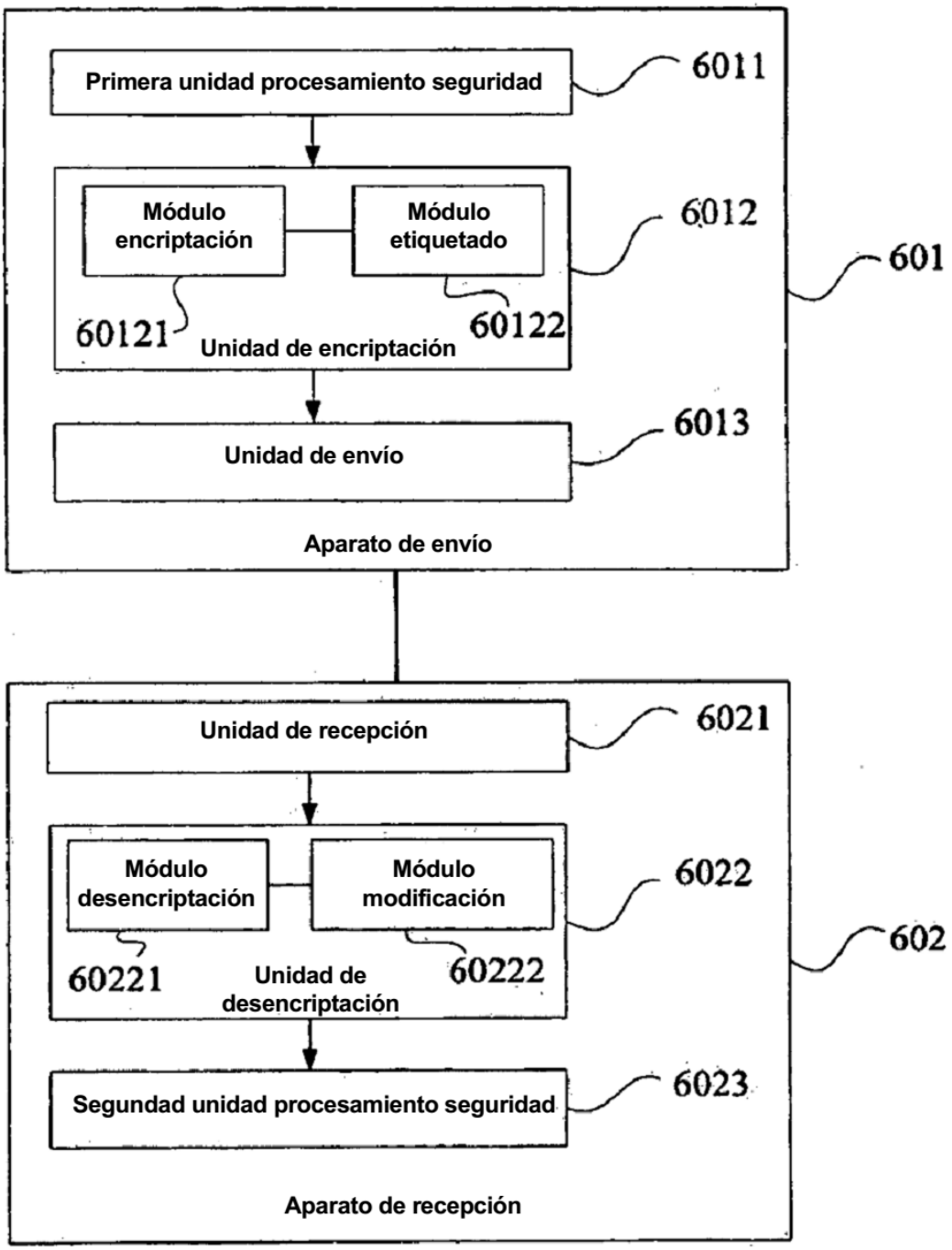
Primera unidad procesamiento seguridad
6011
Módulo encriptación
Módulo etiquetado
6012
60121
60122
Unidad de encriptación
601
Unidad de envío
6013
Aparato de envío
Unidad de recepción
6021
Módulo desencriptación
Módulo modificación
6022
60221
60222
Unidad de desencriptación
602
Segundad unidad procesamiento seguridad
6023
Aparato de recepción

FIG. 6