(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 644 338**

(51) Int. CI.:

H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **24.09.2013 PCT/EP2013/069790**

(87) Fecha y número de publicación internacional: **03.04.2014 WO14048900**

(96) Fecha de presentación y número de la solicitud europea: **24.09.2013 E 13774093 (2)**

(97) Fecha y número de publicación de la concesión europea: **19.07.2017 EP 2901652**

(54) Título: **Procedimiento de segurización de un canal de transmisión de datos de voz y dispositivo de segurización asociado**

(30) Prioridad:

26.09.2012 FR 1202553

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
28.11.2017

(73) Titular/es:

THALES (100.0%)
45, rue de Villiers
92200 Neuilly-sur-Seine, FR

(72) Inventor/es:

ALLARD, FABIEN

(74) Agente/Representante:

SALVA FERRER, Joan

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín Europeo de Patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre Concesión de Patentes Europeas).

DESCRIPCIÓN

Procedimiento de segurización de un canal de transmisión de datos de voz y dispositivo de segurización asociado.

[0001] La presente invención concierne a un procedimiento de segurización de un canal de transmisión de datos entre al menos una red de partida y una red de destino a través de una red de tránsito de un nivel de seguridad más débil que las redes de partida y destino,

[0002] Las redes de partida y de destino tienen como condición previa una conexión protegida según un proceso de tratamiento IPsec que comprende una política de seguridad IPsec y que pone en marcha al menos un protocolo de IPsec,

[0003] Los datos comprenden los primeros datos y los segundos datos. Los primeros datos comprenden datos de voz y están protegidos por un protocolo de segurización diferente a los protocolos del proceso de tratamiento IPsec,

[0004] El procedimiento que comprende las siguientes etapas, cuando los datos son transmitidos de la red de partida a la red de tránsito:

- Si los datos son los segundos datos, desvío de los segundos datos hacia una etapa de encriptación según al menos un protocolo de IPsec del proceso de tratamiento IPsec para obtener los segundos datos encriptados; y
- Transmisión de los segundos datos encriptados hacia la red de tránsito

[0005] La invención se aplica, en particular, a la transmisión de datos de voz, en medios restringidos como, por ejemplo, las redes de radio a baja velocidad, típicamente a algunos kilobits por segundo, o las redes filiares donde los datos transmitidos están modulados como, por ejemplo, las redes RTC (Red Telefónica Conmutada).

[0006] En adelante, por “red de partida” y “red de destino” entendemos las redes informáticas que tienen niveles de seguridad elevados, como las redes locales, por ejemplo, las redes informáticas de tipo LAN (del inglés, *Local Area Network,* o Red de Área Local)

[0007] En lo sucesivo, por “red de tránsito” entenderemos una red que tiene un nivel de seguridad más débil que las redes de partida y de destino, como por ejemplo una red pública de un operador de telecomunicaciones.

[0008] Para asegurar un canal de comunicación entre dos redes seguras, a través de una red de tránsito de nivel de seguridad más débil, se sabe que, si se coloca un dispositivo de segurización en los alrededores de cada red segura, por ejemplo, un cifrador IP (del inglés, *Internet Protocol),* con objeto de cifrar y descifrar, respectivamente, los datos emitidos por estas redes. De esta forma, todos los datos emitidos por estas redes son transmitidos a través de la red de tránsito en forma cifrada, y ningún dato final de estas redes seguras transitan de forma clara, es decir, bajo una forma no cifrada en la red de tránsito.

[0009] También se sabe igualmente cómo establecer una conexión segura entre dos redes seguras conforme a un proceso de tratamiento IPsec que comprende una política de seguridad IPsec (del inglés, *Internet Protocol SECurity)*, poniendo en marcha al menos un protocolo IPsec.

[0010] Este proceso de tratamiento IPsec comprende un conjunto de protocolos y está definidos en la norma IETF RFC 4301. El conjunto de protocolos IPsec está destinado a asegurar que las comunicaciones estén protegidas en las redes IP. Más concretamente, IPsec es un conjunto de protocolos que utilizan algoritmos que permiten el transporte de datos seguros en una red IP mediante la utilización de servicios de seguridad criptográficos. IPsec es típicamente puesto en marcha por un dispositivo se segurización emplazado en los alrededores de cada red segura.

[0011] De ahora en adelante, entenderemos por “protocolo IPsec” un protocolo que forma parte de conjunto de protocolos IPsec. Los protocolos IPsec operan en la capa de red del modelo OSI (del inglés, *Open System Interconnection)* es decir, en la capa 3.

[0012] En el protocolo IPsec, una base de datos, normalmente llamada SPD (del inglés *Security Policy Database)* reagrupa el conjunto de comportamientos que el dispositivo de securización adopta en relación con las comunicaciones externas tales como la transmisión o no de datos entre redes seguras. Este conjunto de comportamientos es conocido como “política de seguridad de IPsec”.

[0013] Esta base de datos sirve para decidir, cuando se establece una comunicación, si esta última debe o no utilizar un protocolo IPsec y de qué forma debe ser securizada esta última.

[0014] En la base de datos SPD, las comunicaciones que deben utilizar el conjunto de protocolos IPsec son definidas por las informaciones disponibles a partir de la cabecera IP de los paquetes de la comunicación.

[0015] Las funcionalidades IPsec, con frecuencia llamadas asociaciones de seguridad, son después asociadas a estas comunicaciones, siguiendo el tipo de securización que se desee otorgar a la conexión. Por ejemplo, si los datos con confidenciales, la base de datos SPD especifica que hace falta utilizar la asociación de seguridad ESP (del inglés *Encapsulating Security Payloads)* de forma que los datos transmitidos sean cifrados. Si los la integridad de los datos debe ser protegida, se utiliza la asociación de seguridad AH (del inglés, *Authentication Headers).*

[0016] El conjunto de asociaciones de seguridad IPsec, definidas en la base de datos SPD, con contenidas en una base de datos comúnmente llamada SAD (del inglés, *Security Association Database).*

[0017] En la base de datos SAD, se identifica una asociación de seguridad de manera única por un índice de parámetros de seguridad, comúnmente llamado SPI (del inglés, *Secutiry Parameter Index)*

[0018] Por otra parte, con el fin de mejorar el rendimiento de las comunicaciones, es conocido por todos la utilización de protocolos de securización de comunicaciones diferentes siguiendo el tipo de datos intercambiados. Típicamente, para la transmisión de datos de voz, se utiliza otro tipo de protocolos, como el protocolo SCIP (del inglés, *Secure Communications Interoperability Porotocol*), o el protocolo SRTP (del inglés, *Secure Real-time Transport Protocol*). Estos protocolos son adaptados para securizar la transmisión de datos de voz, y permiten una comunicación fiable y segura, en particular en las redes limitadas. La securización de la transmisión de datos de voz, por ejemplo, por SCIP, consiste, por ejemplo, en el cifrado de los datos de voz destinados a transitar entre las redes seguras. Este tipo de protocolos opera típicamente en la capa de aplicación del modelo OSI, es decir, la capa7.

[0019] Cuando los datos de voz previamente securizados por un protocolo de securización como el SCIP son emitidos por una red de partida y son transmitidos hacia una red de tránsito a través de un dispositivo de securización IPsec situado en la interfaz entre la red de partida y la red de tránsito, estas últimas son enfrentadas con la política de seguridad IPsec contenida en el dispositivo de securización. De manera tradicional, estos datos de voz securizados son reconocidos por la política de seguridad IPsec como datos que no tienen que ser protegidos por un protocolo IPsec con el fin de evitar sobrecargar las tramas de datos. En consecuencia, estos datos de voz son transmitidos a nivel de la capa de red en la cual opera IPsec hacia la red de destino. A la llegada a la red de destino, la política de seguridad IPsec conduce a transmitir sin tratamiento los datos de voz hacia la red de destino (política de seguridad IPsec “BYPASS”) o a suprimir estos datos de la pila IPsec y por tanto a no transmitirlos a la red de destino (política de seguridad IPsec “DISCARD”).

[0020] En la práctica, los datos de voz son transmitidos hacia la red de destino, lo que constituye un fallo de seguridad dado que el canal no está controlado, antes de atravesar las capas superiores de la capa de red.

[0021] Existe por tanto una necesidad de un procedimiento de securización de un canal de transmisión de datos de voz securizados entre dos redes seguras a través de una red de tránsito de un nivel de seguridad más débil que las redes seguras, teniendo las redes seguras como condición previa establecida una conexión segura según un proceso de tratamiento IPsec.

[0022] A tal fin, está definido en las reivindicaciones, 1,5,9, 10 y 11. Las formas de realización particulares están definidas en las reivindicaciones dependientes. La invención tiene como objeto un procedimiento del tipo precitado anteriormente, caracterizado en que la política de seguridad IPsec prevea, en el proceso de tratamiento

IPsec, un protocolo de tratamiento IPsec propio a tratar los primeros datos y en que comprende además las siguientes etapas:

- Si los datos no son los primeros datos, desvío de los primeros datos a una etapa de codificación según el protocolo de tratamiento IPsec del proceso de tratamiento IPsec para obtener los primeros datos codificados; siendo dicho protocolo de tratamiento IPsec diferente del protocolo de tratamiento IPsec o de cada uno de ellos, según el cual los segundos datos son encriptados,
- Transmisión de los primeros datos codificados hacia la red de tránsito.

[0023] El procedimiento de segurización según la invención comprende además las características siguientes, consideradas separadamente o en combinación:

- Comprende, cuando se transmite un paquete de primeros datos de la red de partida a la red de tránsito y previamente a la etapa de desvío del paquete de primeros datos, una etapa de adición de una cabecera de dicho paquete, correspondiendo dicho cabecera a un protocolo de segurización de los primeros datos;
- Todos los primeros datos pasan por la etapa de codificación
- La etapa de codificación comprende una etapa de adición de una cabecera a los primeros datos para obtener los primeros datos codificados.

[0024] La invención tiene igualmente por objeto un procedimiento de segurización del canal de transmisión de datos entre al menos una red de partida y una red de destino a través de una red de tránsito de un nivel de seguridad más débil que las redes de partida y de destino.
Las redes de partida y de destino que tienen como condición previa una conexión segura según un proceso de tratamiento IPsec que comprende una política de seguridad IPsec que pone en marcha al menos un protocolo IPsec, los datos que comprenden los primeros datos y los segundo datos, los primeros datos comprenden los datos de voz y están segurizados por un protocolo de segurización diferente a los protocolos del proceso de tratamiento IPsec,
El procedimiento que comprende las siguientes etapas, cuando los datos son transmitidos a la red de tránsito hacia la red de destino:

- Si los datos son los segundos datos encriptados, el desvío de los segundos datos encriptados hacia una etapa de descifrado según al menos un protocolo IPsec del proceso de tratamiento IPsec para obtener los segundos datos descifrados;
- Transmisión de los segundos datos descifrados hacia la red de destino;
-
- El procedimiento se caracteriza en que la política de seguridad IPsec prevé, en el proceso del tratamiento IPsec, un protocolo de tratamiento IPsec propio a tratar los primeros datos codificados, y en que comprende además las siguientes etapas:
- Si los datos son los primeros datos codificados, el desvío de los primeros datos codificados hacia una etapa de decodificación según el protocolo de tratamiento IPsec del proceso de tratamiento IPsec para obtener los primeros datos decodificados; dicho protocolo de tratamiento IPsec siendo diferente del protocolo IPsec según el cual los segundos datos son descifrados;
- Transmisión de los primeros datos decodificados hacia la red de destino

[0025] El procedimiento de segurización según la invención comprende además las características siguientes, consideradas por separado o en conjunto:

- Todos los primeros datos codificados pasan por la etapa de decodificación;
- La etapa de decodificación para obtener los primeros datos decodificados comprende una etapa de supresión de una cabecera de los primeros datos codificados.

[0026] Asimismo, la invención tiene como objeto un dispositivo de segurización de un canal de transmisión de datos entre al menos una red de partida y una red de destino a través de una red de tránsito con un nivel de seguridad más débil que las redes de partida y de destino,
Las redes de partida y destino tienen como condición previa una conexión segura según un proceso de tratamiento IPsec que comprende una política de seguridad IPsec y que pone en marcha al menos un protocolo IPsec, los datos que comprenden los primeros datos y los segundos datos, los datos primeros datos comprenden los datos de voz y están segurizados por un protocolo de segurización diferente a los protocolos del proceso de tratamiento IPsec,
El dispositivo que comprende, cuando los datos son transmitidos de la red de partida a la red de tránsito:

- - si los datos son los segundos datos, los primeros medios de desvío de los segundos datos hacia los medios de encriptación según al menos un protocolo IPsec del proceso de tratamiento IPsec para obtener los segundos datos encriptados; y
- - medios de transmisión de los segundos datos encriptados hacia la red de tránsito;
- El dispositivo estando caracterizado en que la política de seguridad IPsec prevé, en el proceso de tratamiento IPsec, un protocolo de tratamiento IPsec propio a tratar los primeros datos y en que comprende, además:
- si los datos son los primeros datos, los primeros medios de desvío de los primeros datos hacia los medios de codificación según el protocolo de tratamiento IPsec del proceso de tratamiento IPsec para obtener los primeros datos codificados; dicho protocolo de tratamiento IPsec siendo diferente del protocolo IPsec según el cual los segundos datos están encriptados,
- Los medios de transmisión de los primeros datos hacia la red de tránsito.

[0027] El dispositivo de segurización según la invención comporta, igualmente, las características siguientes, tomadas por separado o en conjunto:

- Los medios de codificación comprenden medios de adición de una cabecera a los primeros datos;
- Los medios de encriptación comprenden medios de protección de la integridad de los segundos datos y de los medios de cifrado de los segundos datos.

[0028] La invención tiene igualmente como objeto un dispositivo de segurización de un canal de transmisión de datos entre al menos una red de partida y una red de destino a través de una red de tránsito de un nivel de seguridad más débil que las redes de partida y de destino,

Las redes de partida y de destino teniendo como condición previa una conexión segura según un proceso de tratamiento IPsec que comprende una política de seguridad IPsec y que pone en marcha al menos un protocolo IPsec, siendo los primeros datos de voz y estando segurizados por un protocolo de segurización diferente de los protocolos del proceso de tratamiento IPsec,

El dispositivo que comprende, cuando los datos son transmitidos de la red de tránsito hacia la red de destino:

- Si los datos son los segundos datos cifrados, los segundos medios de desvío de los segundos datos encriptados hacia los medios de desciframiento según al menos un protocolo IPsec del proceso de tratamiento IPsec para obtener los segundos datos descifrados.
- Los medios de transmisión de los segundos datos descifrados hacia la red de destino
- El dispositivo estando caracterizado en que la política de seguridad de IPsec prevé, en el proceso de tratamiento IPsec, un protocolo de tratamiento IPsec propio a tratar los primeros datos codificados, y en que comprende, además:
- Si los datos son los primeros datos codificados, los segundos medios de desvío de los primeros datos codificados hacia los medios de descodificación según el protocolo de tratamiento IPsec del proceso de tratamiento IPsec para obtener los primeros datos descodificados, dicho protocolo de tratamiento IPsec siendo diferente del protocolo IPsec según el cual los segundos datos son descifrados;
- Los medios de transmisión de los primeros datos descodificados hacia la red de destino.

[0029] El dispositivo de segurización según la invención comprende igualmente las características siguientes, tomadas por separado o en conjunto:

- Los medios de decodificación comprenden medios de supresión de una cabecera de los primeros datos codificados;
- Los medios de descodificación comprenden los medios de control de la integridad de los segundos datos cifrados y de los medios de desciframiento de los segundos datos cifrados.

[0030] La invención tiene igualmente por objeto un programa informático caracterizado en que comprende las instrucciones propias a poner en marcha las etapas del procedimiento como se ha descrito arriba.

[0031] La invención comporta un soporte de datos sobre los cuales está guardado el programa informático como se ha descrito arriba.

[0032] La invención comporta igualmente una trama de datos propia a transitar en un canal de transmisión de datos entre al menos una red de partida y una red de destino a través de una red de tránsito de un nivel de seguridad más débil que las redes de partida y destino,
Las redes de partida y de destino teniendo como condición previa establecida una conexión segura según un proceso de tratamiento IPsec que comprende una política de seguridad IPsec y pone en marcha al menos un protocolo IPsec, los datos que comprenden los primeros datos y los segundos datos, los primeros datos que comprenden los datos de voz y que están segurizados por un protocolo de segurización diferente del protocolo del proceso de tratamiento IPsec,
dicha trama que comprende sucesivamente:

- Una cabecera IP que comprende las direcciones de origen y de destino de la trama;
- Una cabecera IPsec que corresponde a un protocolo IPsec del proceso de tratamiento IPsec;
- Una cabecera indicando al menos un puerto de destino de la trama, y
- Los datos.
- Dicha trama estando caracterizada en que la política de seguridad IPsec prevé, en el proceso de tratamiento IPsec, un protocolo de tratamiento IPsec propio a tratar los primeros datos y en que la cabecera IPsec corresponde a dicho protocolo de tratamiento IPsec;

En que los datos de la trama son los primeros datos; y
En que la trama comprende además una cabecera correspondiente al protocolo de segurización de los primeros datos, situado entre el cabecera que indica cada puerto de destino y los primeros datos.

[0033] La trama de datos según la invención comporta igualmente la característica según la cual la cabecera IPsec comporta:

- Un identificador del protocolo de tratamiento IPsec;
- Una identificación correspondiente al puerto o a cada puerto de destino; y
- La longitud total de la trama.

[0034] La invención será ventajosamente comprendida en relación con los ejemplos de realización de la invención que serán ahora descritos haciendo referencia a las figuras anexadas entre las cuales:

- La figura 1 es un esquema que ilustra la arquitectura global de las redes adaptadas a la puesta en marcha del procedimiento según la invención;
- La figura 2 es un esquema de un dispositivo de segurización según la invención, situada en un corte entre una red de partida y una red de tránsito o entre una red de tránsito y una red de destino y adaptado para poner en marcha las etapas del procedimiento según la invención;
- La figura 3 es un sinóptico que ilustra las etapas del procedimiento según la invención, cuando los datos son transmitidos de la red de partida a la red de tránsito;
- La figura 4 es un sinóptico que ilustra las etapas del procedimiento según la invención, cuando los datos son transmitidos de la red de tránsito hacia la red de destino; y
- La figura 5 es una representación simplificada de los formatos de una trama de un paquete de datos durante las etapas del procedimiento según la invención, cuando los datos son transmitidos de una red de partida hacia una red de tránsito.

[0035] Se ha representado sobre la figura 1 la arquitectura global de las redes adaptadas a la puesta en marcha del procedimiento según una forma de realización de la invención.

[0036] Dos redes de telecomunicaciones seguras N1 y N3, llamadas tras la red de partida N1 y la red de destino N3, son propias a comunicar a través de una red de tránsito N2, de nivel de seguridad más débil que las redes seguras N1 y N3. Se establece una conexión segura entre la red N1 y la red N3, según un proceso de tratamiento IPsec. El proceso de tratamiento IPsec comprende una política de seguridad IPsec y pone en marcha al menos un protocolo IPsec.

[0037] Las redes seguras N1 y N3 son por ejemplo redes locales tales como las redes internas de las empresas, y la red de tránsito N2, una red pública como una red pública de un operador de telecomunicaciones o como internet.

[0038] La red N1 de partida comprende al menos un terminal emisor 2 y un dispositivo de segurización 4, conectado por una unión 6 con cableado o sin cableado al terminal emisor 2.

[0039] El terminal emisor 2, por ejemplo, un teléfono móvil, está destinado a intercambiar datos, principalmente datos de voz, con la red N2 de tránsito y la red N3 de destino por el intermediario del dispositivo de segurización 4.

[0040] El dispositivo de segurización 4 está en corte entre la red N1 de partida y la red N2 de tránsito, de forma que todos los datos intercambiados entre el terminal emisor 2 y la red N2 de tránsito pasan obligatoriamente por el dispositivo de segurización 4.

[0041] El dispositivo de segurización 4 está destinado a cifrar los datos emitidos por el terminal emisor 2 y a transmitir estos datos, una vez cifrados, hacia la red N3 de destino a través de la red N2 de tránsito.

[0042] Además, el dispositivo de segurización 4 está destinado a recibir los datos cifrados emitidos por la red N3 de destino a través de la red N2 de tránsito hacia el terminal emisor 2 y a transmitir esos datos al terminal emisor 2 después de un desciframiento de esos datos. Más concretamente, el dispositivo de segurización está destinado a descifrar los datos cifrados emitidos por la red N3 de destino y a transmitir los datos descifrador al terminal emisor 2.

[0043] Este dispositivo de segurización 4 será descrito en más detalle en referencia a la figura 2.

[0044] La red N3 de destino comprende al menos un terminal receptor 8 y un dispositivo de segurización 10, conectado por una unión 12 de cableado o no al terminal recetor 8.

[0045] El terminal receptor 8, por ejemplo, un teléfono móvil, está destinado a intercambiar los datos con la red N2 de tránsito y la red N3 de destino por el intermediario del dispositivo de segurización 10.

[0046] El dispositivo de segurización 10 está dispuesto en corte entre la red N2 de tránsito y la red N3 de destino, de forma que todos los datos intercambiados entre el terminal emisor 2 y la red N2 de tránsito pasan obligatoriamente por el dispositivo de segurización 10. La estructura y el funcionamiento del dispositivo 10 son idénticas a aquellos del dispositivo de segurización 4 de la red N1 de partida.

[0047] La figura 2 ilustra, de manera simplificada, la estructura de segurización 4 que pone en marcha el procedimiento según la invención.

[0048] El dispositivo 4 está instalado en corte entre la red de partida N1 y la red de tránsito N2. Comporta, de la red N1 hacia la red N2, un primer módulo de desvío 14 y un primer módulo de tratamiento IPsec 16 que comprende un módulo de codificación 18 y un módulo de encriptación 20.

[0049] Simétricamente, la red N2 hacia la red N1, el dispositivo 4 comporta un segundo módulo de tratamiento IPsec 24 que comprende un módulo de decodificación 26 y un módulo de encriptación 20.

[0050] El módulo de encriptación 20 comprende un módulo de protección en integridad 30 y un módulo de cifrado 32. El módulo de protección en integridad 30 pone en marcha el protocolo AH y el módulo de cifrado 32 pone en marcha el protocolo ESP.

[0051] El módulo de descifrado 28 comprende un módulo de control de integridad 34 y un módulo de descifrado 36. El módulo de control de integridad pone en marcha el protocolo AH y el módulo de descifrado 36 pone en marcha el protocolo ESP.

[0052] El dispositivo comporta entre otros un modelo de supresión de datos 38.

[0053] El dispositivo de segurización 4 comporta una primera entrada 4a unida a una red de partida N1, una segunda entrada 4b unida a la red de tránsito N2, una primera salida 4c y una segunda salida 4d unidas a la red de tránsito N2, una tercera salida 4e y una cuarta salida 4f unidas a una red de partida N1.

[0054] El primer módulo de desvío 14 comprende una entrada 14ª y tres salidas 14b, 14c, 14d, la entrada 14a siendo conectada a la primera entrada 4ª del dispositivo 4. La segunda salida 14c del primer módulo de desvío 14 está directamente conectada a la segunda salida 4d del dispositivo 4. La tercera salida 14d del primer módulo de desvío 14 está conectada al módulo de supresión de datos 38.

[0055] El segundo módulo de desvío 22 comprende una entrada 22a y tres salidas 22b, 22c y 22d, siendo la entrada 22a conectada a la segunda entrada 4b del dispositivo 4. La segunda salida 22c del segundo módulo de desvío 22 está directamente conectada a la cuarta salida 4f del dispositivo 4. La tercera salida 22d del segundo módulo de desvío 22 está conectada al módulo de supresión de datos 38.

[0056] El primer módulo de tratamiento IPsec 16 comprende una entrada 16a conectada a la primera salida 14b del primer módulo de desvío 14, y una salida 16b conectada a la primera salida 4c del dispositivo 4.

[0057] EL segundo módulo de tratamiento 24 comprende una entrada 24a conectada a la primera salida 22b del segundo módulo de desvío 22, y una salida 24b conectada a la tercera salida 4e del dispositivo 4.

[0058] El módulo de supresión de datos 38 comprende dos entradas 38a y 38b, una primera entrada 38a conectada a la tercera salida 14d del primer módulo de desvío 14, y una segunda entrada 38b conectada a la tercera salida 22d del segundo módulo de desvío 22.

[0059] El primer módulo de desvío 14 está destinado a recibir los datos emitidos por la red de partida N1 hacia la red de tránsito N2 en dirección de la red de destino N3, y a analizar estos datos para determinar si deben ser transmitidos o no con destino de la red de tránsito N2. Por ejemplo, el primer módulo de desvío 14 está destinado a analizar los metadatos asociados a estos datos por el protocolo de transporte utilizado, y a determinar, a partir de estos metadatos, la naturaleza de los datos emitidos por la red de partida N1. Estos metadatos son por ejemplo los metadatos del protocolo IPsec relativos a la capa de red del modelo OSI, que comprende las direcciones IP, los números de protocolo de los terminales emisor 2 y receptor 8 y los puertos de comunicación empleados.

[0060] El primer módulo de desvío 14 comprende la base de datos SPD y los medios para la puesta en marcha de la política de seguridad IPsec. El primer módulo de desvío 14 determina qué datos deben ser transmitidos hacia la red de tránsito N2 en función de la política de seguridad predefinida y contenida en la base de datos SPD.

[0061] El primer módulo de desvío 14 está destinado a desviar los datos hacia el módulo de supresión 38 de datos si estos no deben alcanzar la red de tránsito N2.

[0062] Por otra parte, el primer módulo de desvío 14 está destinado a enviar los datos directamente hacia la segunda salida 4d del dispositivo 4, si estos deben ser transmitidos hacia la red de tránsito N2 sin tratamiento IPsec.

[0063] Finalmente, el primer módulo de desvío 14 está, por otra parte, destinado a desviar los datos hacia el primer módulo de tratamiento IPsec 16 si estos deben ser tratados antes de ser transmitidos hacia la red de tránsito N2.

[0064] El módulo de codificación 18 está destinado a codificar los primeros datos que comprenden los datos de voz. Más concretamente, el módulo de codificación está destinado a aplicar una cabecera a los datos de voz. Esta cabecera será denominado de ahora en adelante “SVHP” (del inglés, “Secure Voice Header Protocol”).

[0065] El módulo de supresión 38 de datos está destinado a suprimir los datos si ellos no deben ser transmitidos hacia la red de tránsito N2.

[0066] El segundo módulo de desvío 22 está destinado a recibir los datos emitidos, por ejemplo, por la red de destino N3 hacia la red de tránsito N2 en dirección de la red de partida N1. Estos datos son, por ejemplo, datos cifrados emitidos por la red de destino N3, a través del dispositivo de segurización 4. El segundo módulo de desvío 22 está destinado así a desviar los datos y a analizar estos datos para determinar si deben ser transmitidos o no hacia la red N1.

[0067] El segundo módulo de desvío 22 está destinado así a desviar los datos hacia el módulo de supresión de datos 38 si no debían llegar a la red N1, a desviar los datos directamente hacia la cuarta salida 4f del dispositivo 4 si debían ser transmitidos hacia la red N1 sin tratamiento IPsec, y a desviar los datos hacia el segundo módulo de tratamiento IPsec 24 si estos debían ser tratados antes de ser transmitidos hacia la red N1. El segundo módulo de tratamiento IPsec 24 comprende un módulo de decodificación 26 y un módulo de descifrado 28. El módulo de decodificación 26 está destinado a decodificar los primeros datos que comprenden los datos de voz. Más concretamente, el módulo de decodificación está destinado a suprimir la cabecera SVHP de los primeros datos. El módulo de descifrado 28 comprende un módulo de control de integridad 34 y un módulo de descifrado 36, destinados respectivamente a controlar la integridad según el protocolo AH y a descifrar según le protocolo ESP los datos transmitidos después de la red N2.

[0068] Se ha representado sobre la figura 3 un sinóptico que ilustra las etapas puestas en marcha por el dispositivo de segurización 4 cuando recibe un paquete de primeros datos que comprenden datos de voz, y un paquete de segundos datos diferentes a los datos de voz, emitidos por la red de partida N1, por ejemplo, por el terminal emisor 2.

[0069] Inicialmente, los paquetes de los primeros datos presentan una trama como la representada y diseñada por la referencia 200 en la figura 5. La trama 200 comprende una cabecera IP que comprende las direcciones de origen y de destino de la trama, un cabecera que indica los puertos de comunicación (TCP/UDP) empleados y los primeros datos.

[0070] Durante la primera etapa de cifrado 100, el paquete de primeros datos es encriptado, por ejemplo, por el terminal 2 según un protocolo de segurización diferente a los protocolos IPsec y optimizado para proteger los datos de voz en las redes limitadas, como el protocolo SCIP. Durante la primera etapa de cifrado, una cabecera SCIP es añadido a los primeros datos. La trama de un paquete de primeros datos encriptados por el protocolo SCIP es representado y diseñado por la referencia 202 sobre la figura 5. Al principio de la trama 200, la trama 202 comprende una cabecera IP que comprende las direcciones de origen y de destino de la trama, una cabecera que indica los puertos de comunicación (TCP/UDP) empleados y los primeros datos. La trama 202 comprende además una cabecera SCIP.

[0071] Los datos de voz y los segundos datos son recibidos por el primer módulo de desvío 14. En una etapa de desvío 102, este últimos analiza los datos para determinar si deben ser transmitidos o no hacia la red N2 y para determinar si debe aplicarse un protocolo IPsec o no a los datos antes de ser transmitidos a la red N2 según la política de seguridad memorizada en la SPD.

[0072] Según la invención, la política de seguridad IPsec prevé, en el proceso de tratamiento IPsec, un protocolo de tratamiento IPsec, como el protocolo SVHP, destinado a tratar los primeros datos. El protocolo SVHP es diferente a los protocolos AH y ESP.

[0073] Si los datos son datos de voz encriptados previamente por el protocolo SCIP, el primer módulo de desvío 14 los envía, durante la etapa de desvío 102, hacia el módulo de codificación 18 del primer módulo de tratamiento IPsec 16.

[0074] Durante la etapa de tratamiento IPsec 104, los datos de voz segurizados son codificados según el protocolo IPsec SVHP por el módulo de codificación 18 durante la etapa 106 de codificación. Más concretamente, durante la etapa 106 de codificación, el módulo 18 añade una cabecera SVHP a los paquetes de datos de voz segurizados por el protocolo SCIP. No se efectúa ningún otro tratamiento o cifrado siguiendo un protocolo IPsec puesto que los datos ya están cifrados por el protocolo SCIP.

[0075] La trama de un paquete de primeros datos codificados está representada y diseñada por la referencia 204 de la figura 5. La trama de datos 204 está destinada a transitar en el canal de transmisión de datos entre la red N1 y la red N3 hacia la red N2.

[0076] Según la invención, la trama 204 comprende sucesivamente una cabecera IP que comprende las direcciones de origen y de destino de la trama 204, un cabecera IPsec correspondiente al protocolo de tratamiento IPsec, un cabecera indicando al menos un puerto de destino de la trama 204 (TCP/UDP) y los primeros datos.

[0077] Ventajosamente, la cabecera IPsec comprende un identificador SPI del protocolo SVHP, una identificación correspondiente a cada puerto de destino, como un número de identificación y la longitud total de la trama.

[0078] Según la invención, todos los datos de voz emitidos por la red de partida N1 pasan por el módulo de codificación 18 para ser codificados y posteriormente transmitidos en la red de tránsito N2.

[0079] Los primeros datos codificados son después transmitidos durante una etapa 114 de transmisión hacia la red N2.

[0080] Si los datos son los segundos datos, es decir, todos aquellos datos que no son los datos de voz, el primer módulo de desvío 14 los envía, durante una etapa de desvío 102, hacia el módulo de cifrado 20 del primer módulo de tratamiento IPsec 16. Durante la etapa de cifrado 108, el módulo de cifrado 20 cifra los segundos datos durante una etapa cifrado, y/o protege la integridad de los segundos datos durante una etapa de 112 de protección en integridad. La trama de un paquete de segundos datos cifrados está representada y diseñada en la referencia general 206 en la figura 5.

[0081] La etapa 110 de cifrado es realizada según un protocolo IPsec como el protocolo ESP.

[0082] La etapa 112 de protección en integridad está realiza según un protocolo IPsec como el protocolo AH.

[0083] Después, durante una etapa 114 de transmisión de segundos datos cifrados, el primer módulo de tratamiento IPsec 16 transmite los segundos datos cifrados hacia la red N2 de tránsito.

[0084] Los datos que no deben ser transmitidos hacia la red de tránsito N2 son suprimidos durante una etapa de supresión 116 de datos.

[0085] Los datos que deben ser transmitidos hacia la red de tránsito N2 sin pasar por la etapa de tratamiento IPsec 104 son directamente transmitidos hacia la red N2 durante una etapa 118 de transmisión.

[0086] Por otra parte, se ha representado sobre la figura 4 un sinóptico que ilustra las etapas puestas en marcha por el dispositivo de segurización 10 cuando recibe los datos emitidos por la red N1 hacia la red N3 a través de la red N2, después de una emisión de datos como la descrita en referencia a la figura 3.

[0087] Los datos son recibidos por el segundo módulo de desvío 22. EN una etapa de desvío 120, este analiza los datos para determinar si deben ser transmitidos o no hacia la red N3 y para determinar si debe aplicarse un protocolo IPsec o o a los datos antes de ser transmitidos hacia la red N3.

[0088] Según la invención, la política de seguridad IPsec prevé, en el proceso de tratamiento IPsec, un protocolo de tratamiento IPsec propio a tratar los primeros datos codificados.

[0089] SI los datos son los primeros datos cifrados por el protocolo SCIP y codificados por el protocolo SVHP, estos últimos contienen la cabecera SVHP. El segundo módulo de desvío 22 envía estos últimos hacia el módulo de decodificación 26 del segundo módulo de tratamiento IPsec 24 debido a la presencia de la cabecera SVHP. Durante una segunda etapa de tratamiento IPsec 122, los primeros datos codificados son decodificados según el protocolo IPsec SVHP por el módulo de decodificación 26 durante una etapa de decodificación 124. Más concretamente, durante la etapa 124 de decodificación, el módulo de decodificación 26 suprime la cabecera SVHP de los primeros datos codificados y los envía directamente hacia la capa de aplicación del modelo OSI en la cual opera el protocolo de segurización SCIP.

[0090] Según la invención, todos los primeros datos codificados pasan por la etapa de decodificación 124.

[0091] Una vez que los primeros datos decodificados son transmitidos en la red de destino N3, estos son descifrados durante una etapa de descifrado 126 según el protocolo SCIP al nivel de la capa 7. Más concretamente, durante la etapa de descifrado de los primeros datos, la cabecera correspondiente al protocolo SCIP está suprimido de los primeros datos de forma que estos últimos son seguidamente transmitidos en claro en la red de destino N3 durante una etapa 128 de transmisión de los primeros datos descifrados.

[0092] Si los datos son los segundos datos, el primer módulo de desvío 12 los envía hacia el segundo módulo de tratamiento IPsec 24. Durante una etapa de descifrado 130, el módulo de descifrado 28 descifra los segundos datos durante una etapa 132 de descifrado y/o efectúa un control de integridad, después transmite estos datos descifrados hacia la red N3 de destino durante una etapa 136 de transmisión. Así, los segundos datos transitan en claro en la red N3.

[0093] Los datos que no deben ser transmitidos hacia la red de tránsito N3 son suprimidos durante una etapa de supresión 138 de datos.

[0094] Los datos que deben ser transmitidos hacia la red de tránsito N2 sin pasar por la etapa de tratamiento IPsec 122 son transmitidos directamente hacia la red N2 durante una etapa 142 de transmisión.

[0095] El procedimiento de segurización según la invención es puesto en marcha de forma ventajosa por un solo y único programa informático. El programa informático comprende las instrucciones propias a poner en marcha las etapas del procedimiento según la invención. Asimismo, el programa informático es ventajosamente grabado sobre un soporte de datos.

[0096] Se comprende la descripción que precede como el procedimiento y el dispositivo según la invención que permite mejorar la seguridad de la transmisión de datos como los datos de voz entre redes seguras que comunican a través de una red de seguridad más débil.

[0097] Particularmente, la codificación de cualquier dato de voz previamente segurizado por el protocolo de segurización, por ejemplo, SCIP, entre la red N1 y la red N2, permite orientar sistemáticamente tras la capa red hacia la capa de aplicación en la cual opera el protocolo de segurización. Así se evita que estos datos de voz puedan ser considerados como un vector de ataque de capas comprendidas entre la capa red, en la cual opera el protocolo IPsec, y la capa de aplicación, en la cual opera el protocolo de segurización.

[0098] Por otra parte, el procedimiento y el dispositivo según la invención permiten explotar el modo túnel de IPsec, y de segurizar las comunicaciones tanto entre los terminales como en las redes que comprenden cada una de ellas una pluralidad de terminales.

[0099] Particularmente, según otras formas de realización, el procedimiento de segurización es puesto en marcha entre más de dos redes seguras, a través de varias redes de niveles de seguridad más débiles, estando cada una de las redes seguras equipadas de al menos un dispositivo de segurización según la invención.

REIVINDICACIONES

1. Procedimiento de segurización de un canal de transmisión de datos entre al menos una red de partida (N1) y una red de destino (N3) a través de una red de tránsito (N2) de un nivel de seguridad más débil que las redes de partida y destino,
Las redes de partida y de destino teniendo como condición previa establecida una conexión segura según un proceso de tratamiento IPsec que comprende una política de seguridad IPsec que pone en marcha al menos un protocolo IPsec,
Los datos que comprenden los primeros datos y los segundos datos, los primeros datos comprenden datos de voz y estando segurizados por un protocolo de segurización diferente a los protocolos del proceso de tratamiento IPsec,
El procedimiento que comprende las siguientes etapas, cuando los datos son transmitidos de una red de partida (N1) hacia una red de tránsito (N2):
Si los datos son los segundos datos, desvío (102) de los segundos datos hacia una etapa de cifrado (108) según al menos un protocolo IPsec del proceso de tratamiento IPsec para obtener los segundos datos cifrados; y
Transmisión (114) de los segundos datos cifrados hacia la red (N2) de tránsito;

El procedimiento que comprende una política de seguridad IPsec que prevé en el proceso de tratamiento IPsec, un protocolo de tratamiento IPsec destinado a tratar los primeros datos, y el procedimiento que comprende además las siguientes etapas, cuando los datos son los primeros datos:
Añadir una cabecera a los paquetes correspondientes a los primeros datos, dicho cabecera correspondiente al protocolo de segurización de los primeros datos para obtener los primeros datos seguros.
Desvío (102) de los primeros datos seguros hacia una etapa (106) de codificación según el protocolo de tratamiento IPsec del proceso de tratamiento IPsec para obtener los primeros datos codificados, dicho protocolo de tratamiento IPsec siendo diferente de o de cada protocolo IPsec según el cual los segundos datos son cifrados y consistiendo en añadir una cabecera a los primeros datos seguros;
Transmisión (114) de los primeros datos codificados hacia la red (N2) de tránsito.

2. Procedimiento según la reivindicación 1, **caracterizado en que** los primeros datos pasan por la etapa de codificación (106).

3. Procedimiento según la reivindicación 1 o la reivindicación 2, **caracterizado en que** comprende las siguientes etapas, cuando los datos son transmitidos de la red de tránsito (N2) hacia la red de destino (N3):
Si los datos son los segundos datos cifrados, desvío (120) de los segundos datos cifrados a una etapa de descifrado (126) según al menos un protocolo IPsec del proceso de tratamiento IPsec para obtener los segundos datos descifrados,
Transmisión (136) de los segundos datos descifrados hacia la red de destino;

El procedimiento estando **caracterizado en que** la política de seguridad IPsec prevé, en el proceso de tratamiento IPsec un protocolo de tratamiento IPsec destinado a tratar los primeros datos codificados, y **en que** comprende además las siguientes etapas cuando los datos son los primeros datos codificados:
Desvío (120) de los primeros datos codificados hacia una etapa de decodificación (124) según el protocolo de tratamiento IPsec del proceso de tratamiento IPsec para obtener los primeros datos decodificados, dicho protocolo de tratamiento IPsec siendo diferente del protocolo IPsec según el cual los segundos datos son descifrados y que consiste en suprimir la cabecera de los datos codificados;
Transmisión (128) de los primeros datos decodificados hacia la red (N1) de destino.

4. Procedimiento según la reivindicación 3, **caracterizado en que** todos los primeros datos codificados pasan por la etapa de decodificación (124).

5. Dispositivo de segurización (4) de un canal de transmisión de datos entre al menos una red de partida (N1) y una red de destino (N3) a través de una red de tránsito (N2) de un nivel de seguridad más débil que las redes de partida y de destino, las redes de partida y de destino teniendo como condición previa establecida una conexión segura según un proceso de tratamiento IPsec que comprende una política de seguridad IPsec que pone en marcha al menos un protocolo IPsec,

Los datos, que comprenden los primeros datos y los primeros datos, comprendiendo los primeros datos los datos de voz y estando segurizados por un protocolo de segurización diferente a los protocolos del proceso de tratamiento IPsec,
El dispositivo que comprende, cando los datos son transmitidos de la red de partida (N1) a la red de tránsito (N2):
Si los datos son los segundos datos, los primeros medios de desvío (14) de los segundos datos hacia los medios de cifrado (20) según al menos un protocolo IPsec del proceso de tratamiento IPsec para obtener los segundos datos encriptados, y
Los medios de transmisión de los segundos datos encriptados hacia la red (N2) de tránsito;

El dispositivo que comprende una política de seguridad IPsec que prevé en el proceso de tratamiento IPsec, un protocolo de tratamiento IPsec destinado a tratar los primeros datos, y el dispositivo que comprende, además, cuando los datos son los primeros datos:
Los medios de adición de u cabecera a los paquetes correspondientes a los primeros datos de forma que se obtenga los primeros datos seguro;
Los primeros medios de desvío (14) de los primeros datos seguros hacia los medios de codificación (18) según el protocolo de tratamiento IPsec del proceso de tratamiento IPsec para obtener los primeros datos codificados, dicho protocolo de tratamiento IPsec siendo diferente del protocolo IPsec según el cual los segundos datos son cifrados y que consisten en añadir una cabecera a los primeros datos seguros;
Los medios de transmisión de los primeros datos codificados hacia la red de tránsito (N2).

6. Dispositivo según la reivindicación 5, **caracterizado en que** los medios de cifrado (20) comprenden los medios de protección en integridad (30) de los segundos datos y de los medios de cifrado (32) de los segundos datos.

7. Dispositivo según la reivindicación 6, cuando los datos son transmitidos de la red de tránsito (N2) hacia la red de destino (N3):
Si los datos son los segundos datos encriptados, los segundos medios de desvío (22) de los segundos datos encriptados hacia los medios de descifrado (28) según al menos un protocolo IPsec del proceso de tratamiento IPsec para obtener los segundos datos descifrados;
Los medios de transmisión de los segundos datos descifrados hacia la red de destino;
El dispositivo estando **caracterizado en que** la política de seguridad IPsec prevé, en el proceso de tratamiento IPsec, un protocolo de tratamiento IPsec destinado a tratar los primeros datos codificados, y **en que** comprende, además, cuando los datos son los primeros datos codificados:
Los segundos medios de desvío (22) de los primeros datos codificados hacia los medios de decodificación (26) según el protocolo de tratamiento IPsec del proceso de tratamiento IPsec para obtener los primeros datos decodificados, dicho protocolo de tratamiento IPsec siendo diferente del protocolo IPsec según el cual los segundos datos son descifrados y que consiste en suprimir el cabecera de los primeros datos codificados, los medios de decodificación (26) comprenden los medios de supresión de un cabecera de los primeros datos codificados;
Los medios de transmisión de los primeros datos decodificados hacia la red de destino (N1).

8. Dispositivo según cualquiera de las reivindicaciones 5 a 7, **caracterizado en** que los medos de descifrado (28) comprende los medios de control de la integridad (34) de los segundos datos encriptados y de los medios de descifrado (36) de los segundos datos encriptados.

9. Programa informático **caracterizado en que** comprende las instrucciones propias a poner en marcha las etapas del procedimiento según cualquiera de las reivindicaciones 1 a 4.

10. Soporte de datos sobre los cuales se graba el programa informático según la reivindicación 9.

11. Trama (204) de datos propia a transitar en un canal de datos entre al menos una red de partida (N1) y una red de destino (N3) a través de una red de tránsito (N2) de un nivel de seguridad más bajo que las redes de partida y de destino,
Las redes de partida y de destino teniendo como condición previa establecida una conexión segura según un proceso de tratamiento IPsec que comprende una política de seguridad IPsec y que pone en marcha al menos un protocolo IPsec,

Los datos que comprenden los primeros datos y los segundos datos los primeros datos que comprenden los datos de voz y que están segurizados por un protocolo de segurización diferente del protocolo del proceso de tratamiento IPsec, dicha trama que comprende sucesivamente:
Una cabecera IP que comprende las direcciones de origen y de destino de la trama;
Una cabecera IPsec que corresponde a un protocolo IPsec del proceso de tratamiento IPsec;
Una cabecera que indica al menos un puerto de destino de la trama; y
Los datos;

Dicha trama (204) estando como se prevé en la política de seguridad IPsec, en el proceso de tratamiento IPsec, un protocolo de tratamiento IPsec destinado a tratar los primeros datos y que el cabecera IPsec corresponde a dicho protocolo de tratamiento IPsec, los datos de la trama siendo los primeros datos; y la trama (204) que comprende además un cabecera que corresponde al protocolo de segurización de los primeros datos, situado entre el cabecera que indica el puerto o cada puerto de destino y los primeros datos.

12. Trama (204) de datos según la reivindicación 11, **caracterizada en que** la cabecera IPsec comprende:
Un identificador del protocolo de tratamiento IPsec;
Una identificación correspondiente al puerto o a cada puerto de destino; y
La longitud total de la trama (204).

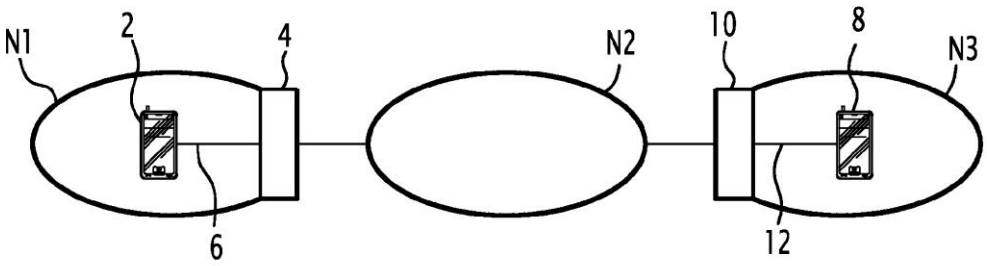
N1
2
4
N2
10
8
N3
6
12

FIG.1

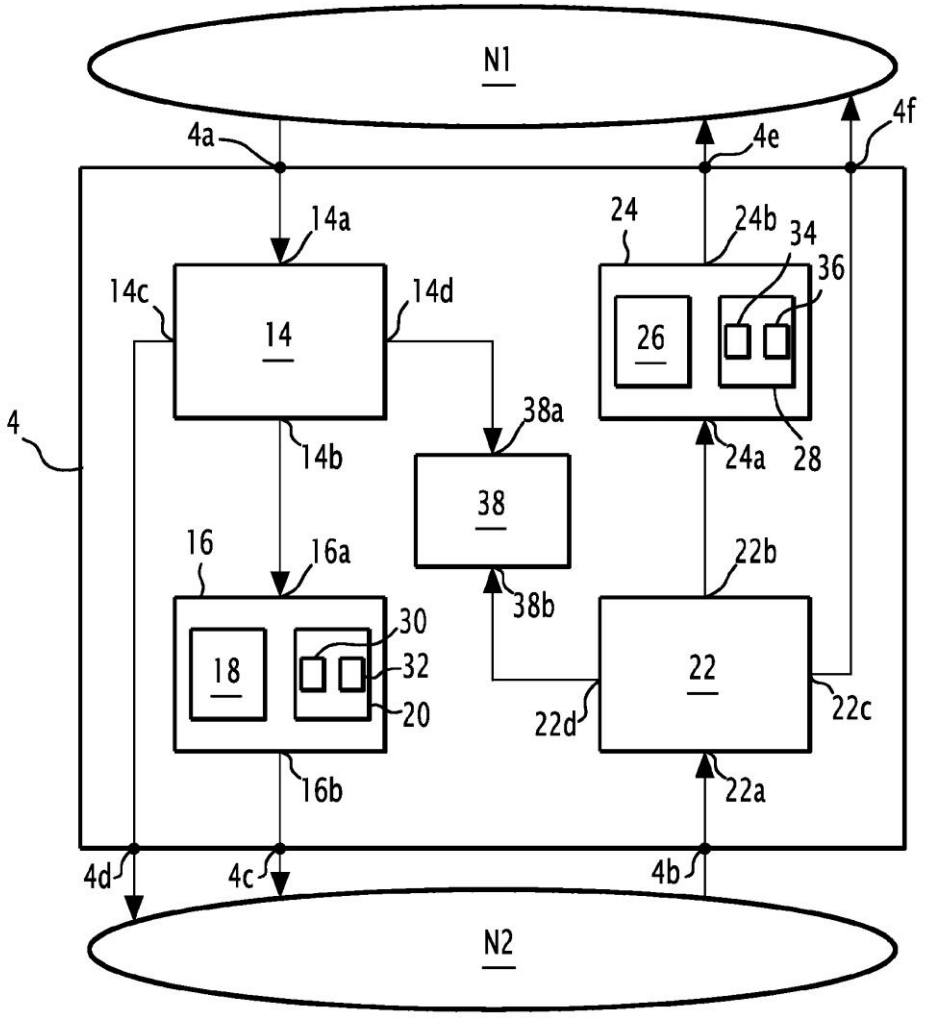
N1
4a
4e
4f
14a
24
24b
34
36
14c
14d
14
26
4
38a
14b
24a
28
38
16
16a
22b
38b
30
18
32
20
22
22d
22c
16b
22a
4d
4c
4b
N2

FIG.2

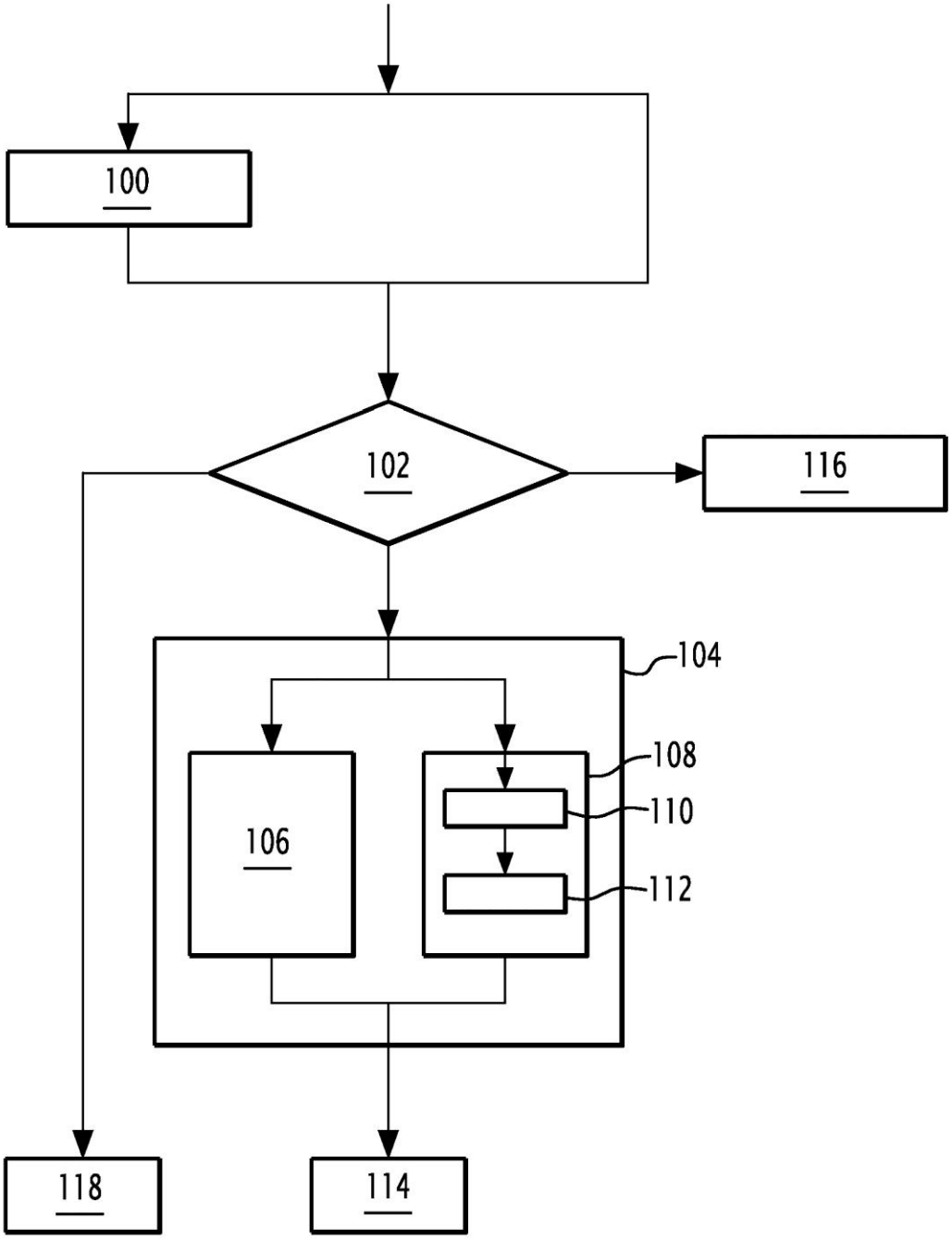

FIG.3

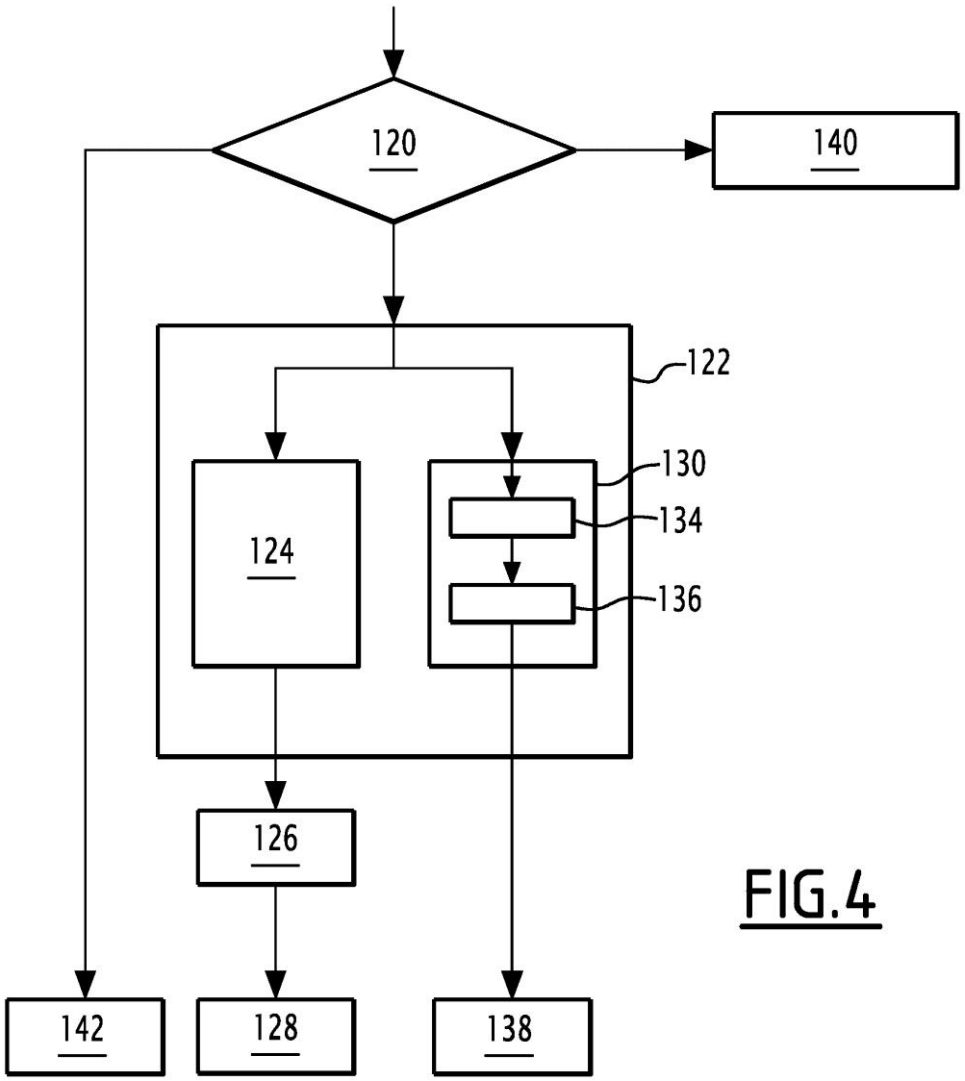
120
140
122
124
130
134
136
126
142
128
138

FIG.4

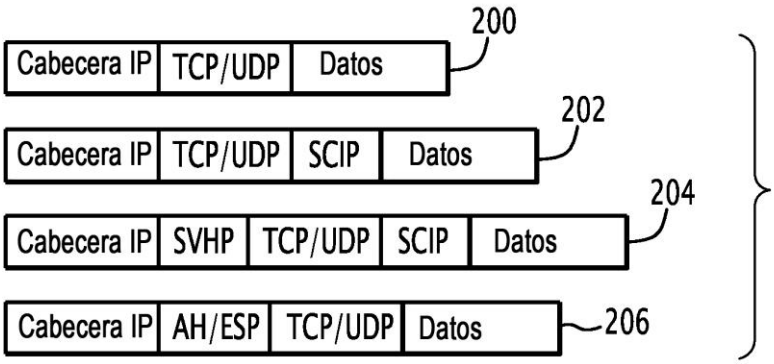
200
Cabecera IP
TCP/UDP
Datos
202
Cabecera IP
TCP/UDP
SCIP
Datos
204
Cabecera IP
SVHP
TCP/UDP
SCIP
Datos
Cabecera IP
AH/ESP
TCP/UDP
Datos
206

FIG.5