(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 364 946**

(51) Int. Cl.:
H04L 29/06 (2006.01)
H04L 12/22 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **08853480 .5**
(96) Fecha de presentación : **27.11.2008**
(97) Número de publicación de la solicitud: **2215801**
(97) Fecha de publicación de la solicitud: **11.08.2010**

(54) Título: **Procedimiento de protección de un canal bidireccional de comunicación y dispositivo de puesta en práctica del procedimiento.**

(30) Prioridad: **30.11.2007 FR 07 08397**

(45) Fecha de publicación de la mención BOPI:
19.09.2011

(45) Fecha de la publicación del folleto de la patente:
19.09.2011

(73) Titular/es: **THALES**
45, rue de Villiers
92200 Neuilly-sur-Seine, FR

(72) Inventor/es: **Breton, Sébastien;**
Cappy, Dominique y
Euzenat, Jean-Yves

(74) Agente: **Carpintero López, Mario**

DESCRIPCIÓN

Procedimiento de protección de un canal bidireccional de comunicación y dispositivo de puesta en práctica del procedimiento

La presente invención se refiere a un procedimiento de protección de un canal bidireccional de comunicación y un dispositivo de aplicación del procedimiento. La invención permite especialmente establecer comunicaciones entre varias redes con niveles de seguridad diferentes.

Las normas de seguridad relativas a las comunicaciones entre redes con niveles de seguridad diferentes imponen a menudo requisitos contradictorios respecto de las exigencias de interoperabilidad entre dichas redes, pero también con las prestaciones deseadas en términos de transporte de datos.

A título ilustrativo, se autoriza que una red interna de empresa reciba algunos datos de una red externa, pero ningún dato de la red interna debe transitar sin codificar hacia la red externa. De este modo, por ejemplo, cuando dos redes de empresa que comunican a través de una red intermedia pública, por ejemplo, Internet, desean intercambiar informaciones confidenciales, un dispositivo de encriptación/desencriptación se dispone a la salida de cada una de estas redes de empresa. Todos los datos se encriptan a la salida de la red de empresa emisora, siendo estos datos desencriptados por la red de empresa receptora, de tal manera que ningún dato procedente de una red de empresa transite sin codificar por la red intermedia pública.

Ahora bien, por una parte, para poder transferir datos en el sentido ascendente –de la red externa hacia la red interna de la empresa, es decir, de una red de baja visibilidad hacia una red de nivel sensiblemente más elevado-, los protocolos de transporte de datos necesitan generalmente emisiones de datos en el sentido descendente –de la red interna hacia la red externa-. En efecto, además de los datos útiles para encaminar (conjunto de datos a menudo calificado de “plano de tráfico de usuario”), existen datos de señalización y de control, inherentes a la gestión del transporte de datos por el protocolo, debiendo estos datos transitar a la vez en el sentido ascendente y en el sentido descendente. Los datos de señalización y de control, que existen especialmente para los protocolos IP (Internet Protocol) y Ethernet, son por ejemplo, acuses de recepción o marcadores de prioridad con el fin de administrar una calidad de servicio en sesiones de transmisiones de datos. Por otra parte, el tratamiento aplicado a los datos (una encriptación total) es idéntico cualquier que sea su naturaleza, lo cual, en un contexto de desarrollo de los canales de comunicaciones multimedia que reúnen voz, datos o también vídeo, es cada vez más molesto.

Asimismo, para beneficiar algunos servicios de base tales como la gestión de la calidad de servicio, es necesario establecer un canal de comunicación bidireccional, encriptado o no, que autoriza que los datos de señalización y/o de control transiten entre las redes protegidas y la red intermedia pública.

Por otra parte, la ausencia de medios que permitan intercambiar de manera protegida datos entre redes con niveles de seguridad dferentes induce igualmente duplicidades de equipos y de medios de gestión asociados. Por ejemplo, cada red debe comprender un servidor de nombres de dominios, un servidor de hora universal o cualquier otro tipo de servicio a priori aconfidencial, esencial para su funcionamiento. Además, el diagnóstico del estado de la red pública no se puede efectuar a través de los dispositivos de encriptación/desencriptación. Por ejemplo, es imposible señalar a una red pública, un incidente ocurrido en la red protegida, no pudiéndose transmitirse una simple alarma de disfunción, intrínsecamente no confidencial, desde la red protegida hacia una red de nivel de protección más bajo.

Una solución alternativa consiste en autorizar algunos tipos de datos elegidos para transitar sin codificar y sin control a través de la red publica, es decir, crear un canal de comunicación adicional para algunos tipos de datos. Pero esta solución incluye riesgos, ya que un malhechor podría explotar este canal para extraer información de una red protegida. El documento US 2006/0020800 describe un sistema para transferir datos entre redes con diferentes niveles de seguridad. Los datos se analizan en la interfaz de red y se comparan con una base de datos que contiene tipos de datos autorizados y sus políticas de seguridad.

Un objetivo de la invención es proponer medios para mejorar la interoperabilidad entre las redes de niveles de seguridad diferentes, limitando a la vez los riesgos de descubrimiento de datos sensibles. Con este fin, la invención tiene por objeto un procedimiento de protección de un canal de comunicación bidireccional entre al menos una red N1 y una red N2 de un nivel de seguridad más bajo que N1, caracterizado porque incluye al menos las siguientes etapas:

- definir uno o varios tipos de datos autorizados a transitar de N1 hacia N2;
- para un dato transmitido de N1 hacia N;
- si el dato es de un tipo autorizado a transitar entre N1 y N2, dirigir el dato hacia una primera etapa de filtrado, en caso contrario dirigir el dato hacia una etapa de encriptación,

- si el dato se dirige hacia la primera etapa de filtrado:

  salvaguardar el contexto asociado a este dato,

  aplicar uno o varios filtros de análisis al dato para impedir la creación de un canal de comunicación oculto,

- para un dato transmitido de N2 hacia N1:

  si el dato es de un tipo autorizado a transitar entre N1 y N2, dirigir el dato hacia una segunda etapa de filtrado, en caso contrario, dirigir el dato hacia una etapa de desencriptación;

- si el dato es dirigido hacia la segunda etapa de filtrado:

  comparar el contexto del dato con el contexto salvaguardado durante la primera etapa de filtrado y bloquear el dato si los contextos son incoherentes,

  en caso contrario, aplicar uno o más filtros de análisis al dato.

Según una realización, la etapa de filtrado incluye una fase de análisis sintáctico de los datos, controlando dicha fase la validez del formato del dato en función del protocolo utilizado para la transmisión de este dato.

Según una realización, la etapa de filtrado incluye una fase de análisis semántico de los datos, controlando dicha fase la coherencia de las respuestas emitidas desde la red N2 hacia la red N1 respecto de las peticiones emitidas por la red N1 hacia la red N2.

Según una realización, la etapa de filtrado incluye una fase de análisis comportamental de los datos, evaluando dicha fase la probabilidad de inocuidad de los intercambios de datos entre la red N1 y la red N2 respecto de escenarios predefinidos de interconexión que definen, a partir de los estados del autómata del protocolo de transmisión de los datos, duraciones esperadas de transición entre estos estados.

Según una realización, la etapa de filtrado incluye una fase de retranscripción de un dato formateado por un primer protocolo para volver a traducirlo en un dato formateado por un segundo protocolo.

La invención tiene también por objeto un dispositivo para establecer un canal de comunicación bidireccional entre al menos una primera red N1 y una segunda red N2 de nivel de seguridad más bajo que N1, comprendiendo el dispositivo un módulo de encriptación y un módulo de desencriptación, comprendiendo el dispositivo al menos un primer módulo de direccionamiento, un segundo módulo de direccionamiento y un módulo de filtrado, orientando el primer módulo de direccionamiento los paquetes de datos procedentes de la primera red N1, bien hacia el módulo de encriptación , bien hacia el módulo de filtrado, orientando el segundo módulo de direccionamiento los paquetes de datos procedentes de la segunda red N2, bien hacia el módulo de desencriptación, bien hacia el módulo de filtrado, aplicando el módulo de filtrado el procedimiento tal como se ha descrito anteriormente.

Otras características irá apareciendo durante la siguiente descripción detallada dada a título de ejemplo y no limitativa respecto de dibujos anexos que representan:

- figura 1, un cuadro sinóptico que ilustra las etapas de tránsito de un dato de una primera red hacia una segunda red de un nivel de seguridad inferior a la primera aplicando un procedimiento de protección según la invención (sentido descendente);

- figura 2, un cuadro sinóptico que ilustra las etapas de tránsito de un dato entre las mismas redes que la figura 1, pero en sentido opuesto, aplicando un procedimiento de protección según la invención (sentido ascendente);

- figura 3, un ejemplo de arquitectura de un dispositivo que aplica el procedimiento de protección según la invención;

- figura 4, un cuadro sinóptico que ilustra la utilización de un dispositivo de protección según la invención para permitir que dos redes protegidas comuniquen entre sí a través de una red pública intermedia.

Por razones de claridad, los elementos con las mismas referencias en diferentes figuras son los mismos.

La figura 1 presenta un cuadro sinóptico que ilustra las etapas de tránsito de un dato de una primera red 111 hacia una segunda red 112 con un nivel inferior según la invención.

En un primer tiempo, un dato 101 procedente de la primera red 111 es recibido por un módulo de direccionamiento 102, el cual orienta dicho dato 101, bien hacia una etapa de encriptación 103, bien hacia una etapa de filtrado 104.

La decisión de transmitir el dato hacia una u otra de estas dos etapas 103, 104 es tomada por el módulo de direccionamiento 102 en función de la naturaleza de este dato 101. La naturaleza del dato 101 se determina, gracias a un análisis de los metadatos asociados al mismo por el protocolo de transporte. Por ejemplo, los metadatos del protocolo IP relativos a la capa 3 del modelo OSI ("Open System Interconnection"), como dirección IP del emisor y/o del destinatario o el puerto de comunicación empleado, son examinados para determinar hacia qué etapa 103, 104 el módulo de direccionamiento 102 debe orientar el dato 101. En efecto, en el ejemplo, algunas direcciones y/o puertos de comunicación están asociados a servicios autorizados para hacer transitar informaciones por otro canal de comunicación a través la segunda red 112, estando las otras direcciones y/o puertos de comunicación dedicados a transferencias de informaciones sensibles, que necesitan por lo tanto una encriptación sistemática.

Por ejemplo, una petición emitida por la primera red 111 con destino a un servidor de nombres de datos situado e la segunda red 112 es orientada hacia la etapa de filtrado 104 y no hacia la etapa de encriptación 103, ya que los datos contenidos en esta petición pueden no ser considerados como sensibles. El ejemplo se puede extender a una multitud de servicios –por ejemplo, servicio de reserva de recursos en pasabanda, anuarios, servidores de tiempo universal- en función, especialmente, de los requisitos de seguridad relativos a las redes en cuestión. El procedimiento se puede ver entonces como un procedimiento de encriptación con opacidad controlada, estando el nivel de opacidad configurado según la proporción de servicios autorizados a transmitir informaciones por la etapa de filtrado 104 y según el contexto de empleo y del nivel de amenazas asociadas. La opacidad se mantiene naturalmente a un nivel elevado para las redes que necesitan niveles de protección elevados. El caso clásico de la encriptación total se puede obtener asimismo no autorizando ninguna transmisión mediante la etapa de filtrado 104, es decir, imponiendo al módulo de direccionamiento 102 el hecho de orientar los datos recibidos sistemáticamente hacia la etapa de encriptación 103.

Sin embargo, la autorización para hacer transitar datos entre redes con niveles de seguridad diferentes debe ir acompañada de medidas de protección. En efecto, es posible desviar una comunicación de aspecto anodino para crear un canal de comunicación oculto o auxiliar. Especialmente, para una serie de paquetes de datos, cada paquete tomado por separado puede no contener información sensible, mientras que la sucesión de estos paquetes puede desembocar en la creación de un código de comunicación. Por ejemplo, durante la emisión de una serie de peticiones de igual naturaleza de la primera red 111 hacia la segunda red 112, la presencia de un intervalo temporal más o menos largo entre cada petición puede constituir un código explotable para sacar informaciones al exterior de la primera red 111. En el caso, por ejemplo, de un marcaje de paquetes para gestionar la calidad de servicio en el encaminamiento de dichos paquetes, una variación anormal del valor del marcador de calidad de servicio durante la emisión de una sucesión de paquetes también puede constituir un canal de comunicación oculto.

En un segundo tiempo, si el dato es orientado hacia una etapa de encriptación 103, el dato encriptado 101' producido por dicha etapa es emitido hacia la segunda red 112; si el dato es orientado hacia la etapa de filtrado 104, experimenta un tratamiento para contrarrestar cualquier tentativa de creación, por un malhechor, de un canal de comunicación oculto. El dato 101 "resultante de este tratamiento es por lo tanto un dato filtrado y depurado de los eventuales canales auxiliares resultantes. El tratamiento de la etapa de filtrado 104 incluye, en el ejemplo, una fase de análisis sintáctico, una fase de análisis semántico y una fase de análisis comportamental. La naturaleza del dato se determina en primer lugar para iniciar los parámetros de cada una de las fases de análisis.

El análisis sintáctico verifica que el dato a transmitir respeta escrupulosamente las normas, por ejemplo los documentos RFC ("Request For Comments") o la norma del protocolo utilizado, y que ningún campo sea desviado de su objeto. Especialmente, se detectan las anomalías en los valores de los campos. Por ejemplo, en el caso de una petición DNS ("Domain Name System"), es conveniente asegurarse que el nombre de huésped a resolver respeta el formato descrito por los RFC 1034 y 1035. En particular, dado que el nombre de huésped a resolver es independiente de la caja, es decir de las minúsculas o mayúsculas, la etapa de filtrado 104 podrá entonces, según a una realización volver a escribir la petición bien en mayúscula, bien en minúscula, o también combinando los dos con el fin de reducir los canales ocultos en la tipografía utilizada.

El análisis semántico cumple varias funciones. Por una parte, verifica el autómata de los posibles estados para un protocolo dado y la coherencia de los encadenamientos de dichos estados. Por otra parte, el análisis semántico detecta un eventual sentido oculto disimulado en una petición o una respuesta a esta petición. Además, el análisis semántico gestiona los contextos de conexión que permiten garantizar que una respuesta procedente de la segunda red 112 de menor sensibilidad está efectivamente asociado a una petición activa emitida desde la primera red 111 de mayor sensibilidad.

Según una realización, además de garantizar que la respuesta corresponde a un contexto activo que, por ejemplo, se puede definir mediante un par (dirección IP fuente – puerto fuente; dirección IP destino – puerto destino), el análisis semántico verifica que la respuesta tiene sentido, es decir que la respuesta corresponde a casos de respuestas verosímiles al nivel del protocolo. Si se toma el ejemplo de una petición DNS ("Domain Nane System") emitida por la primera red 111 hacia un servidor DNS presente en la segunda red 112, no hay más que una sola

respuesta esperada por parte de la primera red 111. Asimismo, esta respuesta debe ser coherente con la petición emitida. Si la petición emitida DNS apunta a la obtención la resolución del nombre de un huésped, la fase de análisis semántico debe verificar que la respuesta obtenida es coherente con la petición planteada (si la resolución tiene éxito, se debe obtener aquí la dirección IP del huésped resuelto), y por ejemplo, que la dirección IP obtenida corresponde a un huésped efectivamente unible, es decir accesible por un simple encaminamiento IP.

El análisis comportamental es, preferiblemente ejecutado después de las fases de análisis sintáctico y semántico anteriormente mencionados. La fase de análisis comportamental se apoya en un esquema cognitivo, es decir en una estructura que apunta a dar un sentido a un proceso de intercambio de información. Para ilustrar este nuevo enfoque en los análisis de filtrado, se puede apoyar en tramas verosímiles de escenarios de interconexión, donde cada escenario podría corresponder a un uso predeterminado de un protocolo dato teniendo en cuenta a la vez los aspectos secuenciales pero también los aspectos temporales de las comunicaciones. Un muestreo estadístico se puede por ejemplo ejecutar para controlar el volumen de datos que transitan entre la primera red 111 y la segunda red 112, para un protocolo elegido y durante un cierto periodo temporal. Un volumen de dato anormalmente elevado puede entonces indicar un ataque. Asimismo, los espacios temporales entre una primera transmisión de datos de la primera red 111 hacia la segunda red 112 y una segunda transmisión de datos entre dichas redes se pueden analizar. De este modo, durante intercambios de datos mediante un protocolo, si la transición entre dos estados del autómata del protocolo es de una duración anormalmente corta o elevada respecto de las duraciones esperadas, se activa un índice de ataque.

Por ejemplo, es totalmente aceptable, en el caso de un análisis de las peticiones de tipo DNS, que un mismo usuario envíe varias veces de seguida peticiones DNS que apuntan a la resolución de varios nombres de dominios, incluso en un lapso de tiempo muy corto. Por el contrario, si este mismo usuario, identificado, por ejemplo, por su dirección IP fuente, enviase varias veces de seguida peticiones que apuntan a la resolución de la dirección IP de un mismo huésped DNS e un lapso de tiempo inferior a la duración de su caché DNS, mientras abría sospecha de acto malintencionado ya que su terminal de trabajo debería conservar normalmente la dirección IP resuelta durante una duración definida parametrizable (en general algunos minutos). Para limitar las falsas alarmas, se aconseja definir umbrales parametrizables a partir de los cuales se recomienda quitar las alertas. En otro ejemplo relativo a un análisis comportamental dedicado a las peticiones DHCP (“Dynamic Host Configuration Protocol”, que permite la asignación de una dirección IP para un arrendamiento limitado), es totalmente aceptable que un huésped cliente, identificado por ejemplo, por su dirección MAC (Ethernet) envíe una petición DHCP varias veces al día para obtener una dirección IP (teniendo en cuenta, por ejemplo, las múltiples desconexiones del cable de red), mientras que un huésped servidor no hará la petición más que una sola vez,, y a continuación durante la renovación de su arrendamiento o durante su reinicio.

Cuando se detecta una anomalía, el dato no se transmite hacia la segunda red 112. Otros tratamientos son posibles durante la detección de una anomalía. Por ejemplo, se puede activar una alarma para impedir que los datos de naturaleza igual al dato en cuestión transiten entre las redes de sensibilidad diferentes. Esto se puede efectuar modificando la configuración del módulo de direccionamiento 102.

Según otra realización, la etapa de filtrado 104 ejecuta solamente una parte de las fases de análisis anteriormente mencionadas, por ejemplo únicamente las fases de análisis sintáctico y de análisis semántico.

Según otra realización, la etapa de filtrado 104 aplica, además, una etapa de retranscripción de los datos para disminuir los riesgos de fuga de información de la primera red 111. De este modo, en el caso de una serie de peticiones (por ejemplo, peticiones SIP, acrónimo de “Session Initialization Protocol”) emitidas por la primera red 111, algunas peticiones de dicha serie se reformulan en el formato de otro protocolo en funciones análogas (por ejemplo, las peticiones SIP se vuelven a traducir en peticiones de tipo H.323), para eliminar las informaciones redundantes y/o variar el formato de la petición, permitiendo de este modo aumentar las dificultades de creación de un canal de comunicación oculto.

La figura 2 presenta un cuadro sinóptico que ilustra las etapas de tránsito de un dato entre las mismas redes que la figura 1, pero en sentido opuesto. El dato 201 se transmite de la segunda red 112 hacia la primera red 111, la cual es de un nivel de seguridad superior a la segunda, aplicando un procedimiento de protección según la invención.

En un primer tiempo, el dato 201 es recibido por un módulo de direccionamiento 202 que lo orienta, bien hacia una etapa de desencriptación 203, bien hacia una etapa de verificación de contexto 204.

Si el dato 201 está encriptado (si se trata, por ejemplo, de un dato transportado por los protocolos de tipo IPSec (“Internet Protocolo Security”), el dato 201 se orienta hacia la etapa de desencriptación 203. Si el desencriptado se desarrolla correctamente, el dato desencriptado 201’ procedente de esta etapa de desencriptación 203 se emite a continuación hacia la primera red 111.

En el caso contrario, si el dato 201 no está encriptado, se orienta hacia la etapa de verificación de contexto 204. Esta etapa analiza el contexto del dato respecto de los parámetros del contexto salvaguardado durante la etapa de filtrado 104 (figura 1). Se trata, por ejemplo, de verificaciones en los campos relativos a la capa 3 del modelo OSI, como por ejemplo, la verificación de un campo DSCP ("Differentiated Services Code Point") utilizado para la gestión de la calidad de servicio, o la verificación de una dimensión MTU ("Maximum Transmission Unit") y variaciones de dimensión de MTU autorizadas. Puede tratarse asimismo de verificaciones al nivel de la capa aplicativa (capa 7 del modelo OSI), por ejemplo para analizar peticiones de reserva de recursos RSVP ("Resource ReSerVation Protocol") o peticiones DNS. Si el contexto es incoherente con el contexto previamente registrado durante la etapa de filtrado 104, entonces el dato se bloquea, 206, y se puede activar una alarma. Por ejemplo, si se recibe una respuesta de la segunda red 112 sin que se haya emitido ninguna petición por la primera red 111 hacia la segunda red 112 (sin la creación de ningún contexto), esta respuesta se bloquea. En caso contrario, si el contexto es coherente con el contexto registrado, el dato 201 se transmite a una etapa de filtrado 205, la cual aplica las fases de análisis anteriormente mencionadas para la figura 1.

La figura 3 presente un ejemplo de arquitectura de un dispositivo que aplica el procedimiento según la invención. El dispositivo 300 se instala con corte entre una red confidencial 311 y una red pública 312. Incluye un primer módulo de direccionamiento 301, un módulo de encriptación 302, un módulo de desencriptación 303, un módulo de filtrado 304 y un segundo módulo de direccionamiento 305.

El dispositivo 300 incluye una primera entrada 300a conectada a la red confidencial 311, una segunda entrada 300a' conectada a la red pública 312, una primera salida 300b y una segunda salida 300c conectadas a la red confidencial 311, una tercera salida 300b' y una cuarta salida 300c' conectadas a la red pública 312.

El primer módulo de direccionamiento 301 comprende una entrada 301a y dos salidas 301b, 301c, estando su entrada 301a conectada a la primera entrada 300a del dispositivo 300. El segundo módulo de direccionamiento 305 comprende una entrada 305a y dos salidas 305b, 305c, estando su entrada 305a conectada a la segunda entrada 300a' del dispositivo 300.

El módulo de encriptación 302 comprende una entrada 302a, conectada a la primera salida 301b del primer módulo de direccionamiento 301, y una salida 302b conectada a la tercera salida 300b' del dispositivo 300. El módulo de desencriptación 303 comprende una entrada 303a, conectada a la primera salida 305b del segundo módulo de direccionamiento 305, y una salida 303b conectada a la primera salida 300b del dispositivo 300. Los módulos de encriptación 302 y de desencriptación 303 se apoyan en las técnicas clásicas de criptografía.

El módulo de filtrado 304 comprende dos entradas 304a, 304b y dos salidas 304c, 304d, estando su primera entrada 304a conectada a la segunda salida 301c del primer módulo de direccionamiento 301, estando su segunda entrada 304b conectada a la segunda salida 305c del segundo módulo de direccionamiento 305, estando su primera salida 304c conectada a la segunda salida 300c del dispositivo 300, estando su segunda salida 304d conectada a la cuarta salida 300c' del dispositivo 300.

El módulo de filtrado 304 se apoya especialmente en una base de datos de filtros, correspondiendo cada filtro a un tipo de datos a controlar. Cada filtro aplica un tipo o más de fases de análisis de la etapa de filtrado 104 (figura 1). Un filtro está constituido por ejemplo, por un conjunto de parámetros y/o de componentes de software, Cuando se ha identificado la naturaleza del dato, los parámetros y eventualmente, los componentes de software que corresponden a la naturaleza del dato a controlar son cargados y ejecutados por el módulo de filtrado 304.

Por ejemplo, la base de datos comprende un filtro para controlar las peticiones DHCP, un filtro para las peticiones DNS, y un filtro para las solicitudes de reserva de recursos del protocolo RSVP ("Resource ReSerVation Protocol"). Asimismo, es muy deseable una arquitectura abierta y modular, permitiendo dicha arquitectura integrar un nuevo filtro y/o retirar un filtro de la base de datos sin afectar al funcionamiento de los otros filtros. De este modo, se pueden operar homologaciones de seguridad filtro por filtro, integrándose solamente un filtro homologado en la base de datos de los filtros. Según otra realización, algunos filtros son realizados por circuitos electrónicos, sobre componentes programables por ejemplo.

Asimismo, el dispositivo de protección 300 se instala preferiblemente en un espacio controlado, por ejemplo, en el recinto de la red confidencial 311, con el fin de proteger físicamente su segunda entrada 300a' y su segunda salida 300c contra potenciales malhechores.

Ventajosamente, el dispositivo de protección 300 está físicamente blindado, especialmente para evitar los ataques por canales auxiliares, mediante especialmente el análisis de la corriente eléctrica consumida por el dispositivo o la radiación electromagnética emitida por el dispositivo.

La figura 4 presenta un cuadro sinóptico que ilustra la utilización de un dispositivo según la invención para permitir que dos redes protegidas 401, 402 se comuniquen entre sí a través de una red pública intermedia 403.

Una primera red de empresa 401 debe comunicar con una segunda red de empresa 402. Estas dos redes 401, 402 se comunican a través de la red pública 403. Siendo los datos presentes en las dos redes de empresa 401, 402 confidenciales, ninguna de estos datos debe transitar sin codificar en la red pública 403. Se establece entonces un enlace protegido entre las dos redes de empresa 401, 402 colocando en la salida de cada uno de ellos un dispositivo de protección 411, 412 según la invención, de tal manera que todos los datos entrantes o salientes de una red de empresa estén bien encriptadas/desencriptadas 411a, 412a, bien filtrados 411b, 412b. El dispositivo de protección según la invención permite entonces establecer un canal de comunicación paralelo al canal de comunicación encriptado clásico, autorizando este canal de comunicación paralelo una interoperabilidad controlada entre una red de empresa 401, 402 y la red pública 403.

En el caso en que las dos redes de empresa 401, 402 ya están conectadas por un enlace protegido clásico que comprende un encriptador en la salida de cada red de empresa 401, 402, basta generalmente con sustituir cada encriptador por un dispositivo de protección según la invención. De este modo, una de las ventajas de la invención es la facilidad de su aplicación en el seno de una arquitectura protegida preexistente.

El dispositivo según la invención incluye varias ventajas. Permite mutualizar equipamientos y reducir los equipos así como las operaciones de explotación y de mantenimiento. Asimismo, proponiendo una solución de intercambios controlados de datos de señalización entre redes de diferentes niveles de seguridad, permite ofrecer una mayor reactividad de las redes de niveles de seguridad elevados respecto de los cambios de carga o de topología de las redes circundantes.

REIVINDICACIONES

1.- Procedimiento de protección de un canal de comunicación bidireccional entre al menos una red N1 y una red N2 de un nivel de seguridad menor que N1, **caracterizado porque** comprende las siguientes etapas:

- definir uno o varios tipos de datos autorizados a transitar de N1 hacia N2;
- para un dato transmitido de N1 hacia N;

. si el dato es de un tipo autorizado a transitar entre N1 y N2, dirigir el dato hacia una primera etapa de filtrado (104), en caso contrario dirigir el dato hacia una etapa de encriptación (103),

. si el dato se dirige hacia la primera etapa de filtrado (104):

º salvaguardar el contexto asociado a este dato,

º aplicar uno o varios filtros de análisis al dato para impedir la creación de un canal de comunicación oculto,

- para un dato transmitido de N2 hacia N1:

. si el dato es de un tipo autorizado a transitar entre N1 y N2, dirigir el dato hacia una segunda etapa de filtrado (204, 205), en caso contrario, dirigir el dato hacia una etapa de desencriptación (203);

. si el dato es dirigido hacia la segunda etapa de filtrado (204, 205):

º comparar el contexto del dato con el contexto salvaguardado durante la primera etapa de filtrado (104) y bloquear el dato si los contextos son incoherentes,

º en caso contrario, aplicar uno o más filtros de análisis al dato.

2.- Procedimiento de protección según la reivindicación 1, **caracterizado porque** la etapa de filtrado (104) incluye una fase de análisis sintáctico de los datos, controlando dicha fase la validez del formato del dato en función del protocolo utilizado para la transmisión de este dato.

3.- Procedimiento de protección según cualquiera de las reivindicaciones anteriores, **caracterizado porque** la etapa de filtrado (104) incluye una fase de análisis semántico de los datos, controlando dicha fase la coherencia de las respuestas emitidas desde la red N2 hacia la red N1 respecto de las peticiones emitidas por la red N1 hacia la red N2.

4.- Procedimiento de protección según cualquiera de las reivindicaciones anteriores, **caracterizado porque** la etapa de filtrado (104) incluye una fase de análisis comportamental de los datos, evaluando dicha fase la probabilidad de inocuidad de los intercambios de datos entre la red N1 y la red N2 respecto de escenarios predefinidos de interconexión que definen, a partir de los estados del o de los autómatas definidos por el protocolo de transmisión de los datos, duraciones esperadas de transición entre estos estados.

5.- Procedimiento de protección según cualquiera de las reivindicaciones anteriores, **caracterizado porque** la etapa de filtrado (104) incluye una fase de retranscripción de un dato formateado por un primer protocolo para volver a traducirlo en un dato formateado por un segundo protocolo.

6.- Dispositivo para establecer un canal de comunicación bidireccional entre al menos una primera red N1 y una segunda red N2 con nivel de seguridad menor que N1, comprendiendo el dispositivo un módulo de encriptación (302) y un módulo de desencriptación (303), **caracterizado porque** incluye al menos un primer módulo de direccionamiento (301), un segundo módulo de direccionamiento (305) y un módulo de filtrado (304), orientando el primer módulo de direccionamiento (301) los paquetes de datos procedentes de la primera red N1, bien hacia el módulo de encriptación (304) , bien hacia el módulo de filtrado (304), orientando el segundo módulo de direccionamiento (305) los paquetes de datos procedentes de la segunda red N2, bien hacia el módulo de desencriptación (303), bien hacia el módulo de filtrado (304), aplicando el módulo de filtrado (304) el procedimiento de protección según una de las reivindicaciones anteriores.

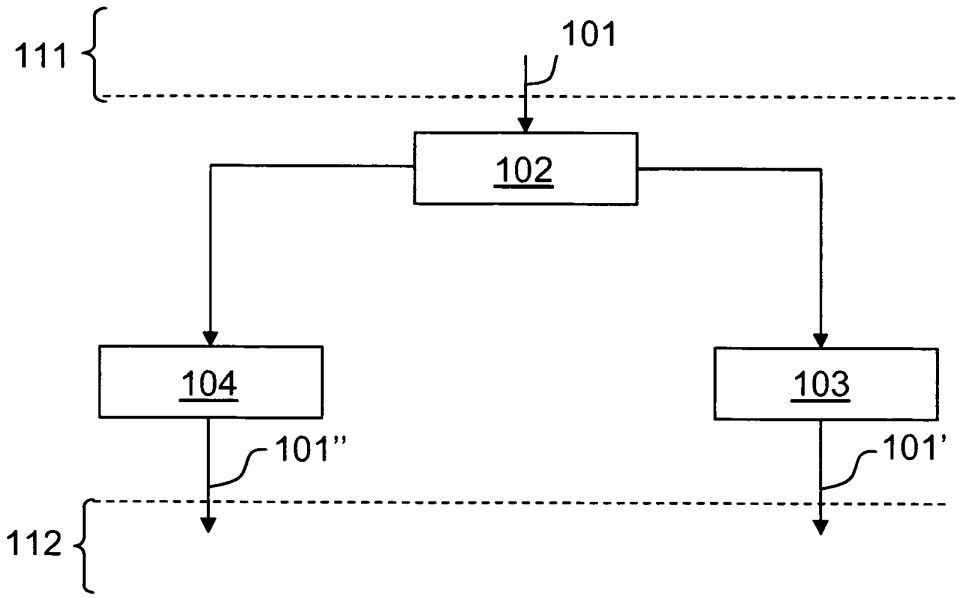
111
101
102
104
103
101''
101'
112

FIG.1

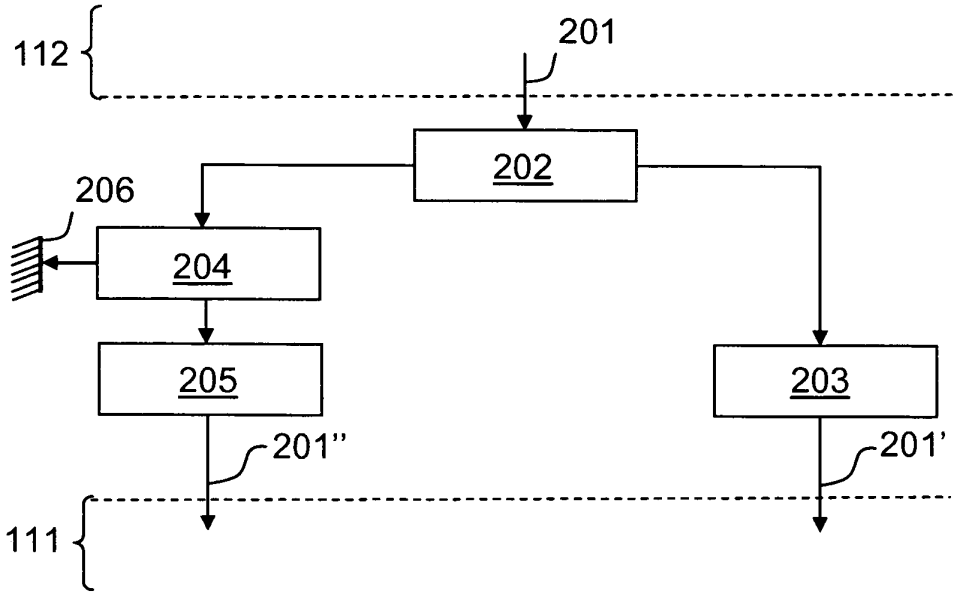
112
201
202
206
204
205
203
201''
201'
111

FIG.2

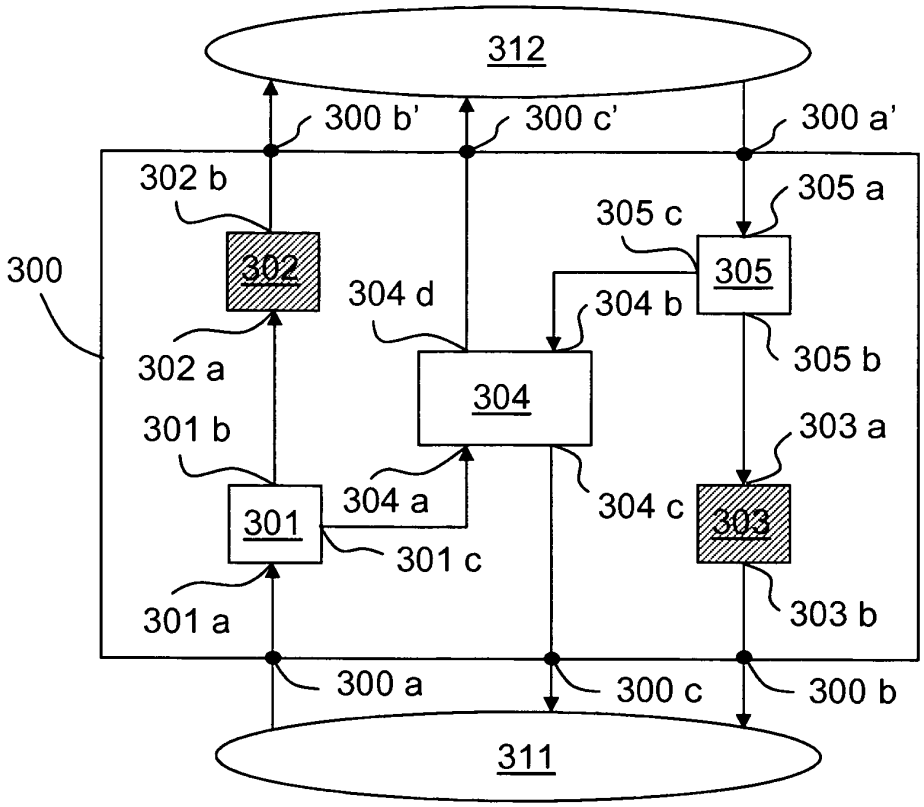
312
300 b'
300 c'
300 a'
302 b
305 a
305 c
300
302
305
304 d
304 b
302 a
305 b
304
301 b
303 a
304 a
304 c
301
303
301 c
303 b
301 a
300 a
300 c
300 b
311

FIG.3

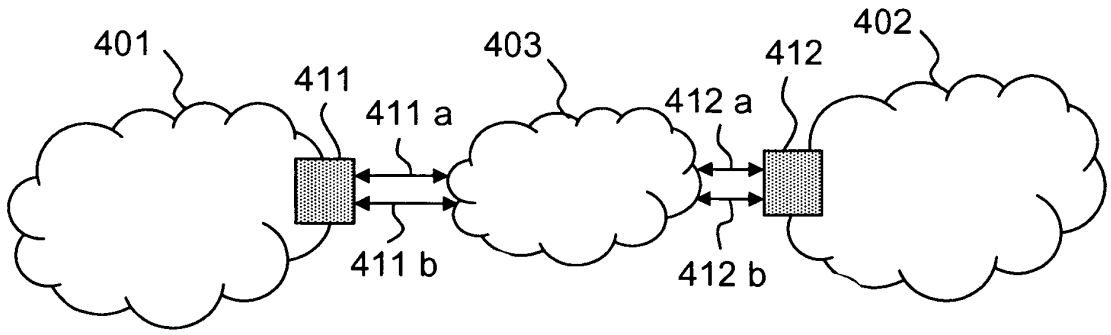
401
403
402
411
412
411 a
412 a
411 b
412 b

FIG.4