(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 687 049**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04L 29/08 (2006.01)
H04L 12/24 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **22.07.2014 PCT/EP2014/065714**

(87) Fecha y número de publicación internacional: **26.02.2015 WO15024722**

(96) Fecha de presentación y número de la solicitud europea: **22.07.2014 E 14747329 (2)**

(97) Fecha y número de publicación de la concesión europea: **27.06.2018 EP 3001884**

(54) Título: **Procedimiento, equipo y sistema para vigilar una pasarela de seguridad a la red**

(30) Prioridad:

23.08.2013 DE 102013216847

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
23.10.2018

(73) Titular/es:

SIEMENS MOBILITY GMBH (100.0%)
Otto-Hahn-Ring 6
81739 München, DE

(72) Inventor/es:

FALK, RAINER;
VON OHEIMB, DAVID y
BLÖCHER, UWE

(74) Agente/Representante:

LOZANO GANDIA, José

PROCEDIMIENTO, EQUIPO Y SISTEMA PARA VIGILAR UNA PASARELA DE SEGURIDAD A LA RED

DESCRIPCIÓN

La invención se refiere a un procedimiento, un equipo y un sistema, así como a un programa de computadora y a un medio de memoria para vigilar una pasarela a la red, que recibe un flujo de paquetes de datos a través de una primera interfaz, comprueba ese flujo de datos con respecto a reglas de filtrado y lo emite a una segunda interfaz.

Las pasarelas de seguridad a la red, por ejemplo firewalls (cortafuegos) se instalan en límites de la red, para realizar un acoplamiento controlado de distintas zonas críticas de la red. Se realiza entonces un filtrado del tráfico de datos, con lo que sólo se permite el paso del tráfico de datos admisible. En sistemas de automatización industriales, como por ejemplo un puesto de enclavamiento o un sistema de control del tren en la automatización ferroviaria, por ejemplo en naves de fabricación en la automatización de la producción, o por ejemplo en refinerías o fábricas de cerveza en la automatización de procesos, se acoplan zonas de la automatización críticas para la seguridad con redes generales, por ejemplo una red de oficina. Para ello se utilizan pasarelas (gateways) de seguridad o bien cortafuegos (firewalls) y se configuran tal que sólo puede atravesarlas un tráfico de datos permitido.

En estos casos se filtra el flujo de datos según reglas de filtrado que pueden configurarse. Al poder existir faltas en una implementación de la pasarela de seguridad a la red o faltas en su configuración, en particular en cuanto a sus reglas de filtrado, o también cuando se ve comprometida la pasarela de seguridad a la red debido a un ataque a esta misma unidad, existe la posibilidad de que una pasarela de seguridad a la red funcione incorrectamente y realmente permita el paso de paquetes de datos no admisibles.

Hasta hoy día se aminoran las posibles deficiencias de una pasarela de seguridad a la red conectando una tras otra varias pasarelas de seguridad a la red, por ejemplo varios firewalls. Al respecto se utilizan en particular pasarelas a la red de distintos fabricantes. Pero esto tiene el inconveniente de que al ser más largos los tiempos de procesamiento aumentan el retardo o la fluctuación del retardo y por lo tanto no se cumplen las exigencias para una comunicación en tiempo real.

El documento US 2003/105976 A1 da a conocer un sistema de detección de intrusión (Intrusion Detection System) basado en el flujo de datos, que asocia paquetes de datos de un flujo de datos a diversos enlaces de comunicación, en particular a los distintos interlocutores de comunicación. Para cada flujo de datos de un tal enlace de comunicación se determinan indicaciones estadísticas a partir de las cabeceras (header) de los paquetes de datos. Mientras dura el enlace de comunicación, los eventos sospechosos se reúnen en un coeficiente de preocupación y se asocian a los interlocutores de comunicación. Cuando se sobrepasa un valor de umbral predeterminado, se activa una alarma.

El documento US 2005/076235 A1 da a conocer un procedimiento de comprobación para una red de paquetes de IP para transmitir voz, que determina la facilidad de ser atacada de una red Voice over IP (de voz sobre IP) mediante apertura y cierre retardados de puertos de datos.

Por otro lado, en una pasarela de seguridad a la red deben actualizarse continuamente las reglas de filtrado, para poder defenderse mediante una protección en particular frente a nuevos ataques, por ejemplo mediante virus o gusanos. En algunos entornos de la automatización industrial rigen elevadas exigencias en cuanto a la integridad, por lo que tienen que autorizarse pasarelas de seguridad a la red y/o las reglas de filtrado implementadas en las mismas y no se admite una modificación y/o actualización de la configuración de las pasarelas de seguridad a la red o de las reglas de filtrado y/o del software antivirus. Además debe quedar asegurado que el flujo de datos no queda modificado mediante una pasarela de seguridad hacia la red de automatización, en particular que no se introduce ningún paquete de datos adicional a través de la pasarela a la red en la red de automatización.

En el documento DE 10 2011 007 387 se da a conocer por ejemplo una autovigilancia de una pasarela de seguridad a la red. Allí se comprueba si se ha recibido un paquete de datos entrante correspondiente a un paquete de datos emitido. De esta manera puede quedar asegurado que una pasarela a la red no genera por sí misma paquetes de datos cuando el funcionamiento es defectuoso.

Es por lo tanto el objetivo de la presente invención lograr un equipo y un sistema que filtren con fiabilidad un tráfico de datos inadmisible en la pasarela hacia una red de datos relevante para la seguridad y que incluso cuando la pasarela de seguridad a la red esté defectuosa, garantice una integridad de los datos en la red de datos relevante para la seguridad. Al respecto debe quedar asegurada la ausencia de retroacción de la pasarela de seguridad a la red, es decir, no debe introducirse ningún paquete de datos adicional a través de la pasarela de seguridad a la red en la red de seguridad.

El objetivo se logra mediante las medidas descritas en las reivindicaciones independientes. En las reivindicaciones secundarias se presentan ventajosos perfeccionamientos de la invención.

El procedimiento de acuerdo con la invención para vigilar una pasarela de seguridad a la red, por ejemplo un firewall, que recibe un flujo de paquetes de datos a través de una primera interfaz, comprueba este flujo de datos contrastándolo con reglas de filtrado y lo emite a una segunda interfaz, incluye las etapas del procedimiento de duplicar y desacoplar el flujo de datos en la segunda interfaz, de comprobar el flujo de datos desacoplado en cuanto a un posible tráfico de datos inadmisible, de enviar un mensaje de aviso a la pasarela de seguridad a la red cuando se detecte un tráfico de datos inadmisible en el flujo de datos y de limitar el flujo de datos mediante la pasarela de seguridad a la red cuando el mensaje de aviso se reciba en la pasarela de seguridad a la red (23).

Puesto que el flujo de datos se toma en la segunda interfaz, que se encuentra detrás de la pasarela de seguridad a la red y dentro de la red de datos relevante para la seguridad, puede detectarse un funcionamiento incorrecto de la pasarela de seguridad a la red mediante comprobación de este flujo de datos filtrado. Una ventaja adicional es que cuando existe una tal sospecha, la pasarela de seguridad a la red es informada de ello y con ello pueden iniciarse muy rápidamente medidas para limitar el flujo de datos. Entonces se evita la introducción de mensajes en la red de datos relevante para la seguridad es decir, en la segunda interfaz, ya que simplemente como consecuencia del anuncio de la sospecha se realiza una limitación del flujo de datos mediante la pasarela de seguridad a la red, en particular el firewall. Así puede por ejemplo vigilarse una pasarela de seguridad a la red de autorización obligatoria o certificada mediante software de filtrado actualizado en una unidad de vigilancia, sin tener que adaptar y con ello autorizar o certificar de nuevo la configuración o bien la versión de software de la propia pasarela a la red. Cuando hay un aviso relativo a un tráfico de datos inadmisible, se limita el tráfico de datos mediante la pasarela de seguridad a la red. La pasarela de seguridad a la red puede, dado el caso mediante informaciones adicionales, tomar medidas adecuadas en el mensaje de aviso, en función de la información adicional.

Además incluye el procedimiento de acuerdo con la invención las etapas adicionales en el procedimiento de duplicar y desacoplar el flujo de datos en la primera interfaz, comparar el flujo de datos en la primera interfaz con el flujo de datos en la segunda interfaz y enviar un mensaje de aviso a la pasarela de seguridad a la red cuando el flujo de datos de la segunda interfaz es diferente del flujo de datos de la primera interfaz.

Esto tiene la ventaja de que también mediante la pasarela de seguridad a la red se detecta un flujo de datos inadmisible rechazado con éxito. Puede entonces realizarse la configuración tal que, en función de las prescripciones que se tienen, se configure tal que se realice un cambio a una forma de funcionamiento restrictiva de la pasarela de seguridad a la red, por ejemplo un firewall. De esta manera se detecta también cuando se introducen nuevos paquetes de datos que no existían en la primera interfaz en la red de datos relevante para la seguridad y se limita inmediatamente el flujo de datos mediante la pasarela de seguridad a la red.

En una forma de realización ventajosa se realiza la limitación del flujo de datos activando reglas de filtrado sustitutorias de la pasarela de seguridad a la red. Así pueden definirse con antelación reglas de filtrado que se hayan acordado y que por ejemplo estén permitidas y/o reglas de filtrado restrictivas para un funcionamiento limitado y cuando se sospecha que hay una entrada de datos inadmisible en la red de datos relevante para la seguridad, se activan inmediatamente estas reglas.

Así puede prevenirse rápidamente el peligro con un tiempo de fallo lo más reducido posible en el paso a la red.

En una forma de realización ventajosa se realiza la limitación del flujo de datos mediante un rearranque de la pasarela de seguridad a la red con un software de arranque protegido o mediante un rearranque de la pasarela de seguridad a la red con un firmware sustitutorio o mediante un cambio de una máquina virtual activa a una máquina virtual sustitutoria en un firewall.

Mediante un rearranque de la pasarela de seguridad a la red puede cancelarse en muchos casos una manipulación en el software de la pasarela a la red, ya que cuando se produce un rearranque se retrotrae el software a su estado inicial de partida. En sistemas embebidos, los llamados Embedded Systems, puede retrotraerse un rearranque con un firmware sustitutorio, que bien corresponde al estado inicial de la pasarela a la red primitiva o bien que incluye reglas de filtrado más estrictas. El firmware sustitutorio puede estar archivado entonces en una memoria de sólo lectura (Read Only Memory) o en una memoria flash, que durante el funcionamiento regular del firewall no puede modificarse. Cuando se implementa una pasarela de seguridad a la red como máquina virtual, puede lograrse el correspondiente efecto mediante un cambio de una máquina virtual activa a una máquina virtual sustitutoria. Entonces los tiempos de fallo durante el cambio son especialmente reducidos. El tráfico de datos hacia la red de datos relevante para la seguridad se interrumpe así sólo muy brevemente.

En otra forma de realización ventajosa se realiza la limitación del flujo de datos desactivando la segunda y/o desactivando la primera interfaz del firewall.

Cuando se desactiva la segunda interfaz, queda asegurado definitivamente que ya no puede penetrar ningún dato más en la red de seguridad. Desactivando la primera interfaz de la pasarela a la red, se evita un desbordamiento de los filtros o bien que se dañe la pasarela de seguridad a la red debido al flujo de datos entrante.

En otra forma de realización ventajosa se limita el flujo de datos desactivando una alimentación eléctrica de la pasarela de seguridad a la red.

Así queda asegurada una interrupción física del flujo de datos hasta más allá del límite de la red. Esta medida tiene la ventaja de que la misma puede utilizarse para cualquier pasarela de seguridad a la red, independientemente de las posibilidades eventualmente existentes o no existentes de limitación de datos en la pasarela a la red. De esta manera queda asegurado con muy elevada fiabilidad que no se realiza ninguna comunicación de datos a través de la pasarela de seguridad a la red. También puede lograrse de esta manera que los registros de datos y el estado del software dado el caso memorizados de forma permanente en la pasarela de seguridad a la red queden disponibles para una evaluación posterior, es decir, no se sobrescriban o se borren.

En una forma de realización permanece activa la limitación en la pasarela de seguridad a la red mientras se reciba el mensaje de aviso en el firewall.

Esto tiene la ventaja de que tras eliminarse el hueco de seguridad puede conectarse de nuevo inmediatamente a activa la comunicación de datos hasta más allá del límite de la red.

En otra forma de realización permanece activa la limitación de la pasarela a la red hasta que se recibe una señal explícita de eliminación de la limitación, con preferencia mediante una operación del personal de administración, en la pasarela de seguridad a la red.

Esto tiene la ventaja de que la pasarela a la red sólo vuelve a estar en servicio una vez que quede asegurada la eliminación del defecto o bien tras realizarse todas las medidas deseadas. En una variante está prevista para ello una interfaz de entrada local en la pasarela de seguridad a la red, que está realizada en forma de un pulsador o interruptor de llave.

El equipo de acuerdo con la invención para vigilar una pasarela de seguridad a la red, que recibe un flujo de paquetes de datos a través de una primera interfaz, comprueba este flujo de datos en función de reglas de filtrado y lo emite a una segunda interfaz, incluye una unidad de desacoplamiento, que está configurada para duplicar el flujo de datos en la segunda interfaz y desacoplarlo en una línea, una unidad de comprobación, que está configurada para comprobar el flujo de datos desacoplado en cuanto a si se trata de un tráfico de datos inadmisible y una unidad de comunicación que está configurada para enviar un mensaje de aviso a la pasarela de seguridad a la red cuando se detecta un tráfico de datos inadmisible en el flujo de datos.

Este equipo puede comprobar ventajosamente una pasarela de seguridad a la red con por ejemplo reglas de filtrado fijamente prescritas y difícilmente adaptables mediante comprobación del flujo de datos emitido por la pasarela a la red con un equipo dotado de las reglas de seguridad más modernas y con ello también detectar nuevos métodos de ataque o bien datos inadmisibles. Puesto que el equipo no tiene influencia alguna sobre el flujo de datos en la segunda interfaz, funciona el equipo sin retroalimentación, es decir, sin intervenir en la red de datos relevante para la seguridad, a la que se transmiten los datos. No obstante, resulta una reacción rápida para limitar el flujo de datos en la segunda interfaz. Esto es especialmente ventajoso cuando la pasarela de seguridad a la red propiamente dicha no puede actualizarse o sólo puede hacerlo limitadamente, es decir, pueden actualizarse o parchearse reglas de filtrado, por ejemplo en base a un certificado o permiso que se exija, que tiene que repetirse en una actualización. El equipo, denominado también a continuación equipo de vigilancia, puede actualizarse flexiblemente, ya que no tiene retroalimentación respecto a la comunicación admisible. Entonces siempre que la pasarela de seguridad a la red “activa” sea suficientemente buena, puede permanecer en servicio una pasarela de seguridad a la red no actualizada. Pero tan pronto como se observa la presencia de tráfico de datos inadmisible, se limita la conectividad desde fuera.

Además incluye el equipo una unidad de desacoplamiento adicional, que está configurada para duplicar y desacoplar el flujo de datos en la primera interfaz y una unidad de comparación, que está configurada para comparar el flujo de datos desacoplado de la primera interfaz con el flujo de datos de la segunda interfaz y, cuando se detectan diferencias entre el flujo de datos de la segunda interfaz y el flujo de datos de la primera interfaz, dar lugar a que la unidad de comunicación envíe un mensaje de aviso a la pasarela de seguridad a la red.

Ventajosamente se detecta de esta manera que la pasarela a la red rechaza con éxito un tráfico de datos inadmisible y por otro lado se detecta cuando la propia pasarela a la red funciona defectuosamente, por

ejemplo debido a manipulación y por ejemplo emite a la segunda interfaz paquetes de datos adicionales que no se recibieron a través de la primera interfaz.

El sistema ventajoso para vigilar una pasarela de seguridad a la red incluye una pasarela de seguridad a la red que está configurada para recibir un flujo de paquetes de datos a través de una primera interfaz, comprobar estos datos en cuanto a reglas de filtrado y emitirlos a una segunda interfaz y una unidad de vigilancia con una unidad de desacoplamiento, que está configurada para duplicar y desacoplar el flujo de datos en la segunda interfaz, con una unidad de comprobación para comprobar si en el flujo de datos desacoplado existe un tráfico de datos inadmisible y una unidad de comunicación que está configurada para enviar un mensaje de aviso a la pasarela de seguridad a la red cuando se detecta un tráfico de datos inadmisible en el flujo de datos, después de lo cual la pasarela de seguridad a la red está preparada para limitar el flujo de datos.

El mensaje de aviso puede proporcionarse en una variante como señal de conexión eléctrica.

La unidad de vigilancia incluye adicionalmente una unidad de desacoplamiento, que está configurada para duplicar y desacoplar el flujo de datos en la primera interfaz y una unidad de comparación, que está configurada para comparar el flujo de datos desacoplado de la primera interfaz con el flujo de datos de la segunda interfaz y, cuando se detectan diferencias entre el flujo de datos de la segunda interfaz y el flujo de datos de la primera interfaz, dar lugar a que la unidad de comunicación envíe un mensaje de aviso a la pasarela de seguridad a la red.

Adicionalmente se reivindica un programa de computadora con órdenes de programa para realizar el procedimiento, así como un soporte de datos que memoriza el programa de computadora.

En los dibujos se representan a modo de ejemplo ejemplos de realización del procedimiento de acuerdo con la invención, del equipo de acuerdo con la invención y del sistema de acuerdo con la invención y se describirán más en detalle en base a la siguiente descripción. Se muestra en:

figura 1a una forma de realización a modo de ejemplo de un procedimiento conocido, como diagrama secuencial;
figura 1b una segunda forma de realización a modo de ejemplo del procedimiento de acuerdo con la invención, como diagrama secuencial;
figura 1c una tercera forma de realización a modo de ejemplo del procedimiento de acuerdo con la invención, como diagrama secuencial;
figura 2 un ejemplo de realización de un sistema con un desacoplamiento del flujo de datos solamente en una segunda interfaz, en representación esquemática y
figura 3 un ejemplo de realización de un sistema de acuerdo con la invención con un desacoplamiento del flujo de datos en una primera y en una segunda interfaz en representación esquemática.

Las partes que se corresponden entre sí se han dotado en todas las figuras de las mismas referencias. A continuación se denominará a la pasarela de seguridad a la red simplemente pasarela a la red.

La figura 1a muestra el procedimiento propuesto para vigilar el funcionamiento correcto de una pasarela a la red sin retroalimentación. Al respecto significa “sin retroalimentación” que la red de datos a la que se transfiere el flujo de datos no se ve influida por la pasarela a la red. En particular no se generan ni se emiten paquetes de datos adicionales hacia una tal red de automatización por ejemplo relevante para la seguridad debido a la pasarela a la red.

En el estado 10 del procedimiento recibe la pasarela de seguridad a la red en una primera interfaz un flujo de datos de una primera red de datos y emite el flujo de datos, una vez comprobado, a una segunda interfaz hacia una segunda red de datos, por ejemplo una red de automatización relevante para la seguridad.

En la primera etapa 11 del procedimiento se duplica y por ejemplo se desacopla en una línea separada el flujo de datos en la segunda interfaz, es decir, ya dentro de la segunda red de datos. Entonces debe quedar asegurado que el flujo de datos se desacopla dentro de la red relevante para la seguridad y frente a componentes que modifican el flujo de datos. A continuación, en la etapa 12 del procedimiento, se comprueba el flujo de datos desacoplado en cuanto a si contiene tráfico de datos inadmisible. La comprobación 12 puede realizarse por ejemplo mediante reglas de filtrado correspondientes a las reglas de filtrado activas de la pasarela a la red. No obstante, con preferencia se comprueba el flujo de datos desacoplado mediante reglas de filtrado actualizadas, por ejemplo con los más modernos parches antivirus. Usualmente se comprueban entonces una dirección de IP de los paquetes de datos y/o los números de puerto en el paquete de datos o los contenidos en datos útiles en el paquete de datos o bien se investiga el flujo de datos según patrones de ataque específicos, a lo largo de varios paquetes de datos.

La comprobación 12 se realiza por completo desacoplada de la comprobación del flujo de datos en la pasarela a la red. El flujo de datos en la segunda interfaz no sufre ningún retraso ni se modifica su contenido. Así permanece la comprobación 12 del paquete de datos desacoplado completamente invisible y con ello sin retroalimentación para la red que recibe el flujo de datos. Si se detecta el flujo de datos como flujo de datos admisible, se emiten los paquetes de datos a la segunda interfaz y el procedimiento finaliza así; véase la etapa 13 del procedimiento.

Si se detecta en el flujo de datos un tráfico de datos inadmisible, se emite en la etapa 14 del procedimiento un mensaje de aviso a la pasarela a la red. Cuando recibe la pasarela a la red el mensaje de aviso, origina la misma una limitación del flujo de datos. El procedimiento finaliza así; véase la etapa 13 del procedimiento.

En una variante del procedimiento que se representa en la figura 1b, se realiza para un paquete de datos de la segunda interfaz, que no se ha reconocido ya en la etapa 12 como admisible, una comprobación adicional en función del flujo de datos recibido en la primera interfaz. Para ello se capta un flujo de datos duplicado y desacoplado en la primera interfaz de la pasarela a la red; véase la etapa 16 del procedimiento. En la siguiente etapa del procedimiento 17 se toma a continuación el flujo de datos desacoplado de la primera interfaz para la comprobación adicional del paquete de datos.

Puede emitirse por ejemplo en la segunda interfaz un mensaje de estado, por ejemplo un mensaje de sobrecarga o un mensaje de modo de mantenimiento, a través de la pasarela a la red, lo cual sólo es admisible en este ejemplo cuando en la primera interfaz de la pasarela a la red se han recibido determinados paquetes de datos. Puede comprobarse por ejemplo si existe un patrón de ataque Denial-of-Service (de denegación de servicio) en la primera interfaz de la pasarela a la red o bien si tiene lugar un acceso de mantenimiento (Remote Service Access) hacia la pasarela a la red a través de la primera interfaz de la pasarela a la red, por ejemplo mediante un enlace HTTPS o SSH.

Si se reconoce el flujo de datos en la comprobación realizada en la etapa 17 del procedimiento como tráfico de datos admisible, se emiten los paquetes de datos a la segunda interfaz y el procedimiento finaliza; véase la etapa 13 del procedimiento. Si se reconoce el paquete de la segunda interfaz como inadmisible, se envía también aquí un mensaje de aviso a la pasarela a la red en la etapa 14 del procedimiento, a continuación de lo cual la pasarela a la red origina una limitación del flujo de datos; véase la etapa 15 del procedimiento.

En otra forma de realización del procedimiento se duplica y desacopla el flujo de datos entrante en la pasarela de seguridad a la red en la primera interfaz y a continuación adicionalmente se compara el flujo de datos desacoplado de la primera interfaz con el flujo de datos desacoplado de la segunda interfaz. Esta comprobación puede realizarse en paralelo a las comprobaciones representadas en la figura 1a ó 1b.

En la variante representada en la figura 1c, se realiza esta comprobación adicional 18 en el caso de que en la etapa 12 se detecte el flujo de datos como tráfico de datos inadmisible. Para ello se capta un flujo de datos duplicado y desacoplado en la primera interfaz de la pasarela a la red; véase la etapa 16 del procedimiento. En la siguiente etapa del procedimiento 18, se utiliza el flujo de datos desacoplado de la primera interfaz para una comprobación adicional del paquete de datos. Para el paquete de datos recibido en la segunda interfaz, se comprueba entonces si existió un paquete idéntico en el flujo de datos de la primera interfaz o bien existía en una determinada ventana de tiempo anterior en el flujo de datos de la primera interfaz. Si es éste el caso, entonces ha finalizado esta comprobación; véase la etapa 13 del procedimiento. Pero si se detecta una inconsistencia en ambos flujos de datos, se envía también aquí un mensaje de aviso a la pasarela a la red en la etapa 14' del procedimiento, a continuación de lo cual origina la pasarela a la red una limitación del flujo de datos; véase la etapa 15 del procedimiento.

Esta comprobación adicional, representada en la figura 1c, puede complementarse también según la variante representada en la figura 1b.

Mediante la comparación del flujo de datos entrante con el flujo de datos saliente, puede detectarse por un lado que se ha realizado un filtrado mediante la pasarela a la red, es decir, que no se incluyen paquetes de datos entrantes inadmisibles en el flujo de datos saliente. Si por el contrario se detectan en el flujo de datos saliente en la segunda interfaz paquetes de datos que no han entrado en la primera interfaz en la pasarela a la red, entonces puede deducirse igualmente que existe una falta en la pasarela a la red. En particular puede detectarse así cuando la pasarela a la red no bloquea un paquete de datos o lo retransmite sin modificar, sino que envía un paquete de datos modificado o un paquete de datos adicional. Pueden entonces por lo tanto detectarse cuando la pasarela a la red envía un paquete de datos que la misma no ha recibido en realidad previamente.

Mediante el mensaje de aviso se hace que la pasarela a la red pase por ejemplo también a un modo de filtrado restrictivo, por ejemplo activando reglas de filtrado sustitutorias. Mediante el mensaje de aviso puede hacerse en una variante que la pasarela a la red realice un rearranque, que con preferencia se

ejecuta con un estado de software no modificado, apoyado, o bien boot-image (imagen de arranque), con lo que de nuevo se activa una configuración por defecto (default) o bien configuración de recuperación (recovery) admisible fijamente archivada. Si está configurada la pasarela a la red como un sistema embebido, se repone la memoria de trabajo en un rearranque a un estado inicial. Así puede desactivarse una versión de software defectuosa o manipulada.

Alternativamente puede estar previsto un rearranque de la pasarela a la red con una imagen de firmware sustitutorio. Pueden estar previstas por ejemplo dos particiones del sistema de ficheros con distintas implementaciones de la pasarela a la red. Cuando se recibe un mensaje de aviso en la pasarela a la red, se realiza un rearranque, arrancándose la partición del sistema de ficheros con la implementación restrictiva.

Si está implementada la pasarela a la red como máquina virtual con un hipervisor o bien microvisor, entonces existen varias particiones lógicas separadamente como máquinas virtuales o también particiones. Un filtrado de paquetes de datos se realiza entonces en una máquina virtual. Cuando está presente el mensaje de aviso, se desactiva una primera máquina virtual y se activa una máquina virtual sustitutoria con reglas de filtrado restrictivas y/o una realización de filtrado alternativa. Un tal cambio es posible en menos de un segundo, en particular en la gama de milisegundos y permite así un funcionamiento casi sin interrupción de la pasarela a la red.

En una variante está realizada al respecto la unidad de vigilancia como componente físico separado. En otra variante está realizada la unidad de vigilancia como máquina virtual, realizada mediante el mismo hipervisor o microvisor que la pasarela a la red.

Además cuando está presente o se recibe el mensaje de aviso, pueden desactivarse una o ambas interfaces. Con preferencia se desactiva la segunda interfaz, con lo que no se emite ningún paquete de datos hacia la segunda interfaz. Es igualmente ventajoso desactivar la primera interfaz para evitar un desbordamiento de las memorias en la pasarela a la red. Igualmente puede provocar una desactivación de la primera interfaz una interrupción del tráfico de datos hacia la red de datos relevante para la seguridad.

Una variante que puede aplicarse universalmente para limitar el tráfico de datos es la desactivación de la alimentación eléctrica de la pasarela a la red, es decir, la conexión sin corriente. Esto es posible con un coste muy reducido por ejemplo mediante una fuente de alimentación conmutable de la pasarela a la red sin modificar la configuración o implementación de la propia pasarela a la red. Así pueden vigilarse mediante este procedimiento también pasarelas a la red que no apoyan ningún mecanismo de limitación explícito y limitarse el tráfico de datos.

En una forma de realización del procedimiento permanece activado el modo restrictivo, limitativo de la pasarela a la red mientras permanece el mensaje de aviso en la pasarela a la red. No obstante, con preferencia permanece el modo restrictivo hasta que se realiza un cambio explícito a un modo regular mediante una operación de administración. Por ejemplo puede activarse el modo regular accionando un pulsador en un pulsador físico o accionando un interruptor de llave o realizando una entrada a través de una interfaz de administración lógica por parte de personal de administración. Al respecto puede incluir el modo regular también una regla de filtrado nueva actualizada. El procedimiento pasa entonces a un estado final designado como parada (stop).

En la figura 2 se representa ahora un sistema compuesto por una pasarela a la red 23 y una unidad de vigilancia 24. La pasarela a la red separa dos redes de datos con por ejemplo distintos grados de seguridad. Entonces se conecta por ejemplo un flujo de datos procedente de una red con bajas exigencias de seguridad, como una red de oficina, a través de una primera interfaz 21 a la pasarela de red 23. La pasarela de red 23 comprueba los paquetes de datos o bien el flujo de paquetes de datos y emite los mismos a través de una segunda interfaz 22 a una segunda red, que por ejemplo presenta mayores exigencias de seguridad.

En la forma de realización de la figura 2 se duplica solamente el flujo de datos saliente en la segunda interfaz mediante una unidad de desacoplamiento 25 y se desacopla en una línea separada. El flujo de datos desacoplado se retransmite a la unidad de comprobación 26 de la unidad de vigilancia 24 y se comprueba allí en cuanto a si existe un tráfico de datos inadmisible. Entonces pueden comprobarse en particular los campos de direcciones en la cabecera del paquete de datos en cuanto a si hay direcciones de origen y/o direcciones de destino inadmisibles o bien se comparan los número de puerto frente a números de puerto admisibles. Si el contenido útil del paquete de datos no está encriptado, encontrándose por lo tanto en texto explícito, entonces puede comprobarse también el contenido de los paquetes en cuanto a si existen por ejemplo patrones sospechosos y/o inadmisibles y se impide su retransmisión incluso antes de la finalización de la comprobación del paquete de datos.

La unidad de comprobación 26 está conectada con una unidad de comunicación 27. Si se detecta en la unidad de comprobación 26 un tráfico de datos inadmisible, lo señaliza la unidad de comprobación 26 a la

unidad de comunicación 27, que a su vez emite o introduce un mensaje de aviso 28 en la pasarela a la red 23. El mensaje de aviso puede proporcionarse por ejemplo como señal de conexión eléctrica.

La figura 3 muestra una variante del sistema de la figura 2, duplicándose aquí, además del tráfico de datos saliente en la segunda interfaz 22, también el flujo de datos entrante en la primera interfaz 21 mediante una unidad de desacoplamiento adicional 31 y se desacopla sobre una línea hacia la unidad de vigilancia 24. Las unidades de desacoplamiento 25 y 31 se encuentran con preferencia directamente en la pasarela a la red 23, con lo que en particular no se incluye ningún componente adicional en el flujo de datos que podría modificar el mismo.

El flujo de datos desacoplado de la primera interfaz 21 se compara en la unidad de comparación 32 con el flujo de datos de la segunda interfaz 22. El flujo de datos de la segunda interfaz 22 puede retransmitirse a través de la unidad de prueba 26, por ejemplo a la unidad de comparación 32. La unidad de comparación 32 está conectada a su vez con la unidad de comunicación 27. Si se detecta una diferencia entre el flujo de datos de la primera y de la segunda interfaz 21, 22, envía la unidad de comunicación 27 un mensaje de aviso 28 a la pasarela a la red 23. La conexión entre unidad de vigilancia 24 y pasarela a la red 23 puede entonces estar realizada en forma de una conexión por hilo, pero también como conexión inalámbrica o como una conexión lógica.

Todas las características descritas y/o señaladas pueden combinarse entre sí ventajosamente en el marco de la invención. Además puede está realizada la unidad de vigilancia como componente separado, pero también integrada con la pasarela a la red.

REIVINDICACIONES

1. Procedimiento para vigilar una pasarela de seguridad a la red (23), que recibe un flujo de paquetes de datos a través de una primera interfaz (21), comprueba ese flujo de datos con respecto a reglas de filtrado y lo emite a una segunda interfaz (22), con las etapas del procedimiento:
   - duplicar y desacoplar (11) el flujo de datos en la segunda interfaz (22),
   - comprobar (12) el flujo de datos desacoplado en cuanto a si contiene un tráfico de datos inadmisible,
   - enviar (14) un mensaje de aviso (28) a la pasarela de seguridad a la red (23) cuando se detecta un tráfico de datos (12) inadmisible en el flujo de datos y
   - duplicar y desacoplar (16) el flujo de datos en la primera interfaz (21),
   - comparar (18) el flujo de datos en la primera interfaz (21) con el flujo de datos en la segunda interfaz (22),
   - enviar (14') un mensaje de aviso (28) a la pasarela de seguridad a la red (23) cuando el flujo de datos de la segunda interfaz (22) es diferente del flujo de datos de la primera interfaz (21) y
   - limitar (15) el flujo de datos mediante la pasarela de seguridad a la red (23) cuando el mensaje de aviso (28) se recibe en la pasarela de seguridad a la red (23),

   realizándose la comprobación (12) mediante reglas de filtrado correspondientes a las reglas de filtrado activas de la pasarela a la red (23) o mediante reglas de filtrado ampliadas.

2. Procedimiento de acuerdo con la reivindicación 1, en el que la limitación del flujo de datos se realiza activando reglas de filtrado sustitutorias de la pasarela de seguridad a la red (23).

3. Procedimiento de acuerdo con la reivindicación 1, en el que la limitación del flujo de datos se realiza mediante un rearranque de la pasarela de seguridad a la red (23) con un software de arranque protegido o mediante un rearranque de la pasarela de seguridad a la red (23) con una imagen de firmware sustitutorio o mediante un cambio de una máquina virtual activa a una máquina virtual sustitutoria en una pasarela de seguridad a la red (23).

4. Procedimiento de acuerdo con una de las reivindicaciones 1 a 3, en el que la limitación del flujo de datos se realiza desactivando la segunda interfaz (22) y/o desactivando la primera interfaz (21) de la pasarela de seguridad a la red (23).

5. Procedimiento de acuerdo con una de las reivindicaciones 1 a 4, en el que se realiza la limitación del flujo de datos desactivando una fuente de alimentación eléctrica de la pasarela de seguridad a la red (23).

6. Procedimiento de acuerdo con una de las reivindicaciones 1 a 5, en el que la limitación en la pasarela de seguridad a la red (23) permanece activa mientras se reciba el mensaje de aviso (23) en la pasarela de seguridad a la red (23).

7. Procedimiento de acuerdo con una de las reivindicaciones 1 a 5, en el que la limitación de la pasarela de seguridad a la red (23) permanece activa hasta que se recibe una señal explícita para eliminar la limitación, con preferencia mediante una operación del personal de administración, en la pasarela de seguridad a la red (23).

8. Equipo para vigilar una pasarela de seguridad a la red (23), que recibe un flujo de paquetes de datos a través de una primera interfaz (21), comprueba este flujo de datos en función de reglas de filtrado y lo emite a una segunda interfaz (22), incluyendo:
   - una unidad de desacoplamiento (25), que está configurada para duplicar el flujo de datos en la segunda interfaz (22) y desacoplarlo,
   - una unidad de comprobación (26), que está configurada para comprobar el flujo de datos desacoplado en cuanto a si se trata de un tráfico de datos inadmisible y
   - una unidad de comunicación (27), que está configurada para enviar un mensaje de aviso (28) a la pasarela de seguridad a la red (23) cuando se detecta un tráfico de datos inadmisible en el flujo de datos,

   incluyendo adicionalmente
   - una unidad de desacoplamiento (31), que está configurada para duplicar y desacoplar el flujo de datos en la primera interfaz (21) y
   - una unidad de comparación (32), que está configurada para comparar el flujo de datos desacoplado de la primera interfaz (21) con el flujo de datos de la segunda interfaz (22) y, cuando se detectan diferencias entre el flujo de datos de la segunda interfaz (22) y el flujo de datos de la primera interfaz (21), dar lugar a que la unidad de comunicación (27) envíe un mensaje de aviso (28) a la pasarela de seguridad a la red (23),

   realizándose la comprobación (12) mediante reglas de filtrado correspondientes a las reglas de filtrado activas de la pasarela a la red (23) o mediante reglas de filtrado ampliadas.

9. Equipo de acuerdo con la reivindicación 8,
tal que el equipo está constituido para realizar el procedimiento de acuerdo con las reivindicaciones 3 a 7.

10. Sistema para vigilar una pasarela de seguridad a la red (23) que incluye
- una pasarela de seguridad a la red (23), que está configurada para recibir un flujo de paquetes de datos a través de una primera interfaz (23), comprobar este flujo de datos frente a reglas de filtrado y emitirlo a una segunda interfaz (22),
- una unidad de vigilancia (24) con una unidad de desacoplamiento (25), que está configurada para duplicar y desacoplar el flujo de datos en la segunda interfaz (22), con una unidad de comprobación (26), para comprobar si en el flujo de datos desacoplado existe un tráfico de datos inadmisible y una unidad de comunicación (27), que está configurada para enviar un mensaje de aviso (28) a la pasarela de seguridad a la red (23) cuando se detecta un tráfico de datos inadmisible en el flujo de datos, a continuación de lo cual la pasarela de seguridad a la red (23) está preparada para limitar el flujo de datos, incluyendo la unidad de vigilancia (24)
- una unidad de desacoplamiento (31) adicional, que está configurada para duplicar y desacoplar el flujo de datos en la primera interfaz (21) y
- una unidad de comparación (32), que está configurada para comparar el flujo de datos desacoplado de la primera interfaz (21) con el flujo de datos de la segunda interfaz (22) y, cuando se detectan diferencias entre el flujo de datos de la segunda interfaz (22) y el flujo de datos de la primera interfaz (21), dar lugar a que la unidad de comunicación (27) envíe un mensaje de aviso (28) a la pasarela de seguridad a la red (23),

realizándose la comprobación (12) mediante reglas de filtrado correspondientes a las reglas de filtrado activas de la pasarela a la red (23) o mediante reglas de filtrado ampliadas.

11. Sistema de acuerdo con la reivindicación 10,
en el que la pasarela de seguridad a la red (23) y la unidad de vigilancia (24) están configuradas para realizar el procedimiento de acuerdo con las reivindicaciones 3 a 8.

12. Programa de computadora con órdenes de programa para realizar el procedimiento de acuerdo con las reivindicaciones 1- 7.

13. Soporte de datos que memoriza el programa de computadora de acuerdo con la reivindicación 12.

FIG 1A

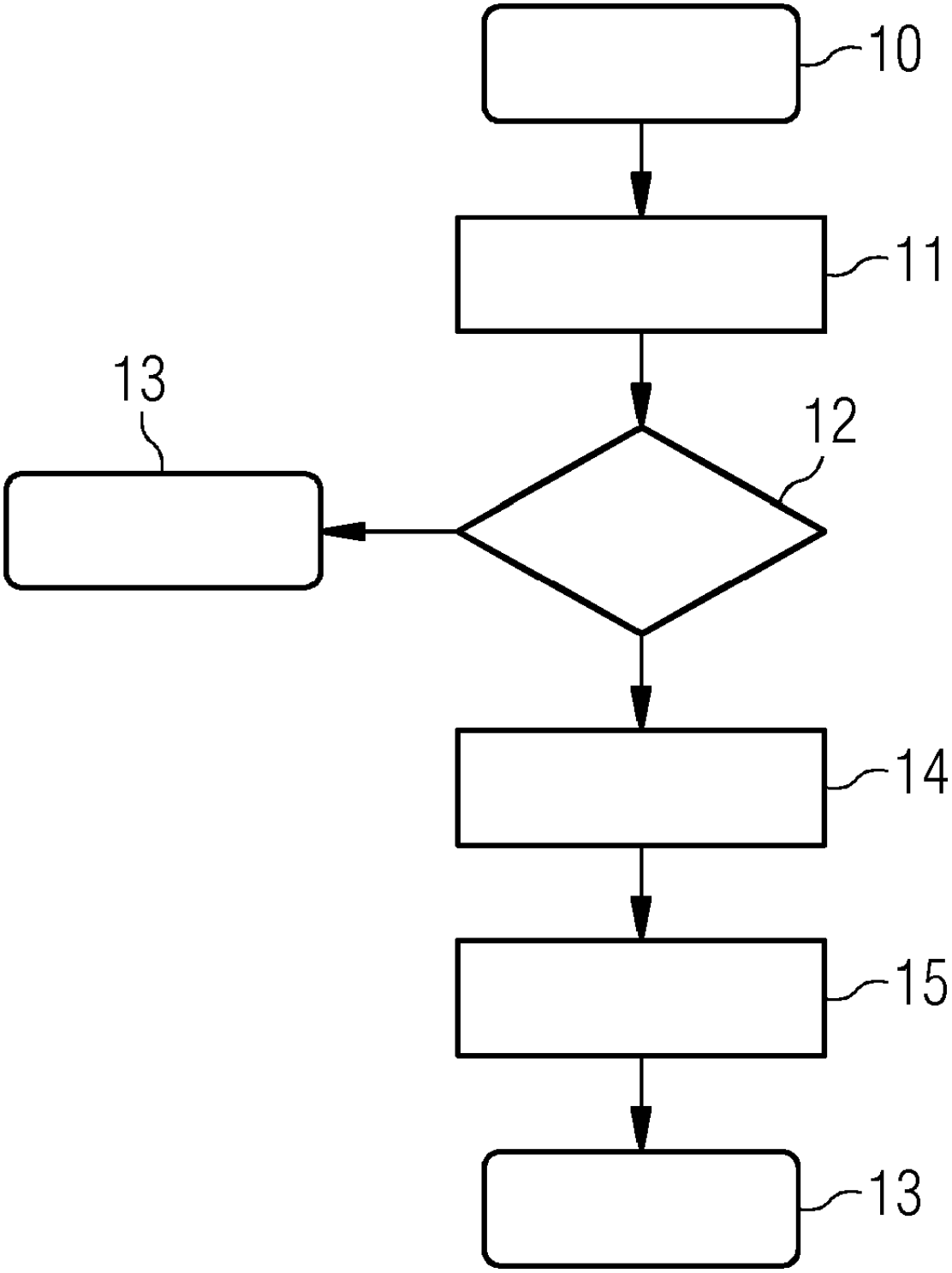

FIG 1B

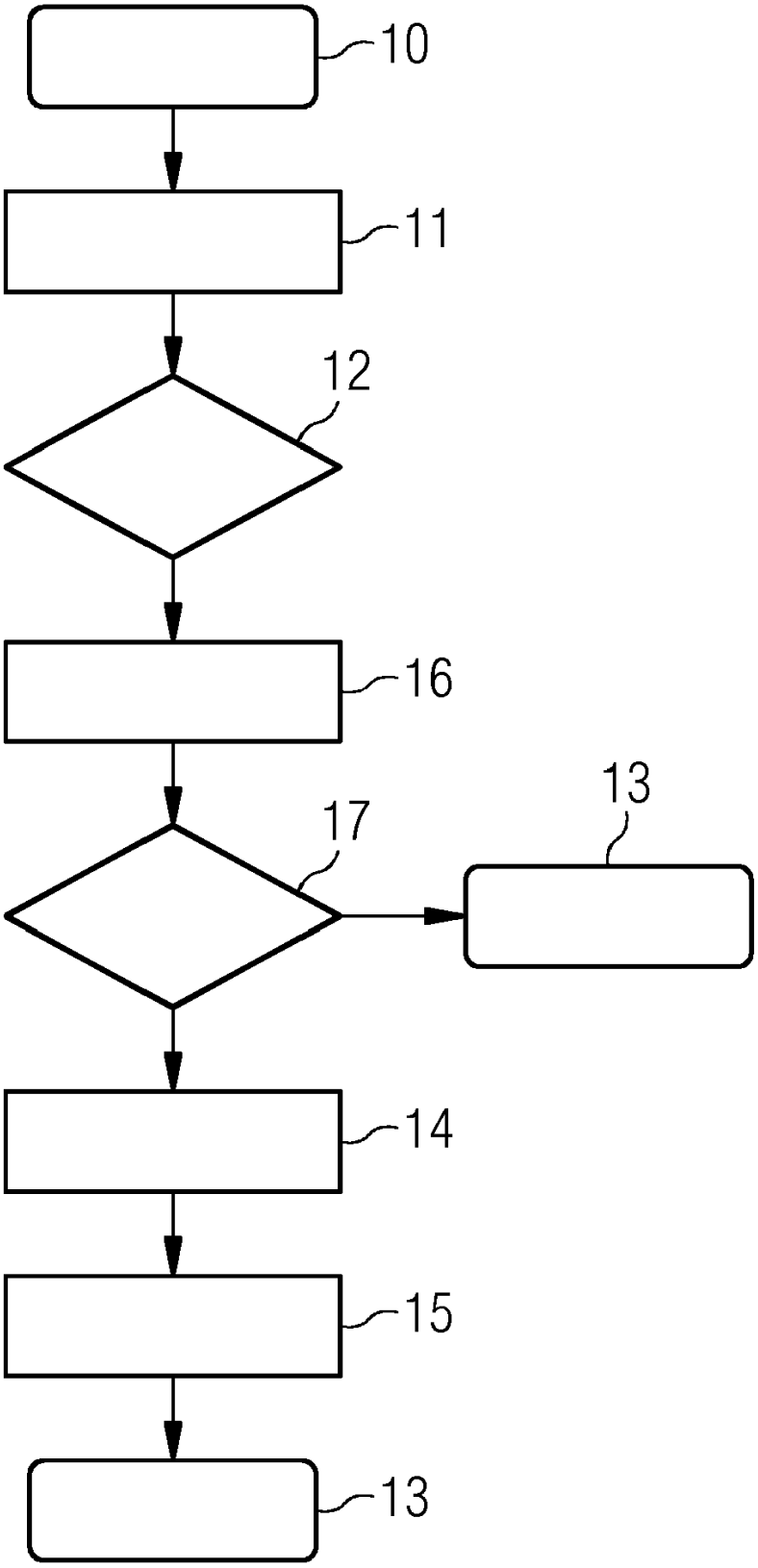

FIG 1C

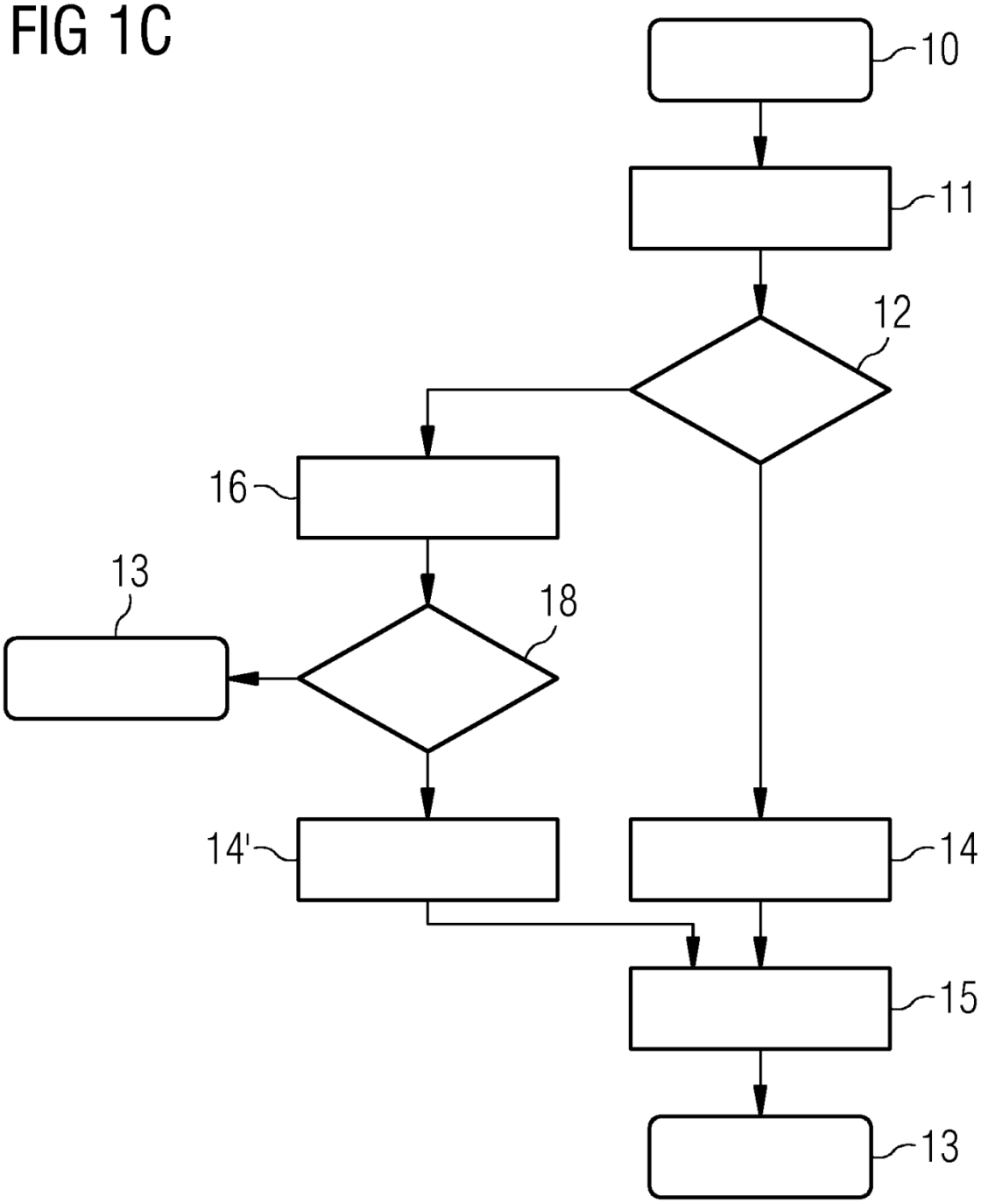

FIG 2

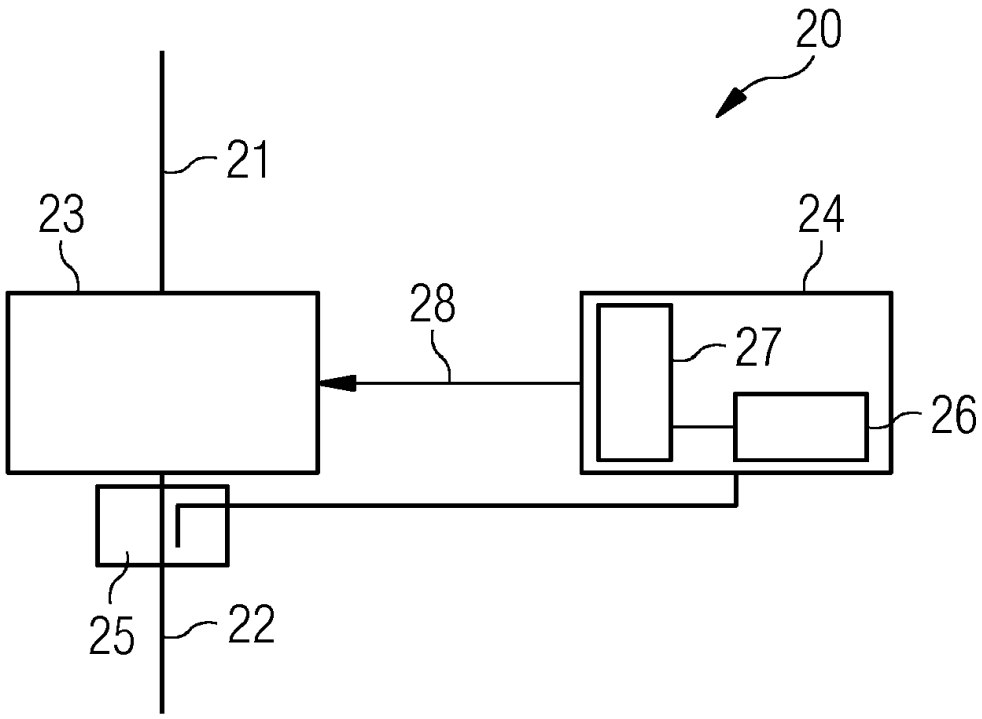

FIG 3