(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 763 183**

(51) Int. CI.:

H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **19.12.2008 PCT/GB2008/004235**

(87) Fecha y número de publicación internacional: **25.06.2009 WO09077770**

(96) Fecha de presentación y número de la solicitud europea: **19.12.2008 E 08862287 (3)**

(97) Fecha y número de publicación de la concesión europea: **16.10.2019 EP 2232814**

(54) Título: **Seguridad de red informática**

(30) Prioridad:

19.12.2007 GB 0724758

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
27.05.2020

(73) Titular/es:

AIRBUS DEFENCE AND SPACE LIMITED (100.0%)
Gunnels Wood Road, Stevenage
Hertfordshire SG1 2AS, GB

(72) Inventor/es:

BENTALL, MARK

(74) Agente/Representante:

PONS ARIÑO, Ángel

DESCRIPCIÓN

Seguridad de red informática

La presente invención hace referencia al diseño de redes informáticas. En particular, la presente invención está dirigida a la seguridad en sistemas de redes informáticas y a la gestión de la solución de compromiso (del inglés "trade-off") entre seguridad y usabilidad de los sistemas de redes informáticas.

Es bien conocido en el campo de la seguridad de la tecnología de la información proporcionar uno o más cortafuegos como característica de seguridad de una red. Habitualmente, un cortafuegos se utiliza para controlar el tráfico de datos entre una red interna y el mundo exterior (a menudo bajo la forma de Internet). En uso, un cortafuegos permite habitualmente que los paquetes de datos que llegan al cortafuegos se introduzca en una red interna únicamente cuando esos datos cumplen con ciertos requerimientos. De esta manera, se reduce la exposición de la red interna a problemas tales como virus, y se reduce la probabilidad de que los datos dentro de la red sean vulnerables a partir de una acción realizada en el exterior de la red.

El documento W02006/093917 divulga un sistema de seguridad para un entorno de datos basados en una red móvil. La invención proporciona integración de seguridad, informática móvil, tecnología inalámbrica y de gestión de infraestructura IT.

El documento US2007/0261121 divulga un método y un aparato para el cumplimiento de la política de mantenimiento en una red informática. El sistema monitoriza electrónicamente el cumplimiento del usuario de red con una política de seguridad de la red almacenada en una base de datos, y emprende una acción para el cumplimiento de la política de red en respuesta al no cumplimiento de la política de seguridad de la red.

El documento US2007/0157286 divulga un método de análisis del cumplimiento de la seguridad dentro de una red. Una base de datos de la política de seguridad identifica las políticas de seguridad previstas dentro de una red. Un generador de tráfico proporciona un tráfico de prueba configurado para someter a prueba cada política de seguridad. A continuación un simulador simula la propagación del tráfico en un modelo de la red.

La Figura 1 muestra una disposición de red habitual, indicada en general con el número 2 de referencia, que incorpora un servidor 8 y un número de ordenadores usuarios de 10 a 15 conectados entre sí como una red interna. La red se conecta a una segunda red 4 (habitualmente una red externa, tal como Internet) a través de un cortafuegos 6; el cortafuegos 6 controla el flujo de datos entre la segunda red 4 y la red interna.

Claramente, cuanto más restrictivo es el cortafuegos 6, menos probable es que se generen problemas de seguridad por el flujo de datos entre la red interna y la segunda red 4. Sin embargo, tales restricciones restringen también la funcionalidad de los ordenadores 10 a 15 usuarios. Por ejemplo, un cortafuegos puede evitar que un usuario acceda a datos que están almacenados en un ordenador fuera de la red local. Si se requieren esos datos para una finalidad en particular, entonces la seguridad proporcionada por el cortafuegos 6 ocurre a expensas de restringir que un usuario obtenga los datos requeridos. Claramente, se necesita lograr un equilibrio entre seguridad y funcionalidad.

Los datos que el cortafuegos 6 permite pasar pueden depender del usuario que solicita el acceso a esos datos. Por tanto, puede permitirse que diferentes usuarios o grupos de usuarios dentro de una red tengan acceso a diferentes tipos de información. Dicha disposición puede ser gestionada proporcionando un conjunto de políticas de seguridad, donde se le asigna un perfil de seguridad diferente a diferentes usuarios.

A modo de ejemplo, podrían proporcionarse los siguientes niveles de seguridad:

Nivel 1 – No se permite que ningún dato traspase el cortafuegos en cualquier dirección.

Nivel 2 – Se permite que los datos salgan de la red desde un usuario de nivel 2, pero no se permite que se introduzcan en la red.

Nivel 3 – Se permite que los datos traspasen el cortafuegos en cualquier dirección hacia/desde un usuario de nivel 3.

Los perfiles de seguridad son habitualmente más sofisticados que el simple sistema de tres niveles descrito anteriormente. Por ejemplo, puede darse acceso a diferentes usuarios para diferentes aplicaciones o para diferentes proyectos. Por ejemplo, los usuarios pueden ser capaces de acceder a datos que están almacenados fuera de una red local cuando utilizan una primera aplicación, para la cual ese acceso es esencial, pero pueden no ser capaces de acceder a datos fuera de la red local cuando utilizan una segunda aplicación para la cual dicho acceso no es esencial.

Un primer problema causado por las políticas de seguridad es que si éstas son demasiado restrictivas pueden evitar que algunas aplicaciones de software funcionen según está previsto o no funcionen en absoluto. Un segundo problema causado por las políticas de seguridad es que, si no son lo suficientemente restrictivas, pueden ocurrir brechas de seguridad. Por consiguiente, el objeto de cualquier política de seguridad es proporcionar un equilibrio entre la seguridad y la usabilidad de una red informática.

A modo de ejemplo, se considera el escenario que se muestra en la Figura 2.

La Figura 2 muestra un sistema, indicado en general con el número de referencia 20 que comprende un primer 21, un segundo 22 y un tercer 23 usuario, cada uno conectado a una primera red 24 interna. Cada uno de los usuarios 21 a 23 son parte del departamento de recursos humanos de una compañía y la primera red 24 interna es la red de recursos humanos. También conectada a la primera red 24 interna, se encuentra una base de datos 25 que contiene datos relativos al departamento de recursos humanos. Cada uno del primer, segundo y tercer usuario 21 a 23 tiene acceso a la base de datos 25 a través de la red 24.

La primera red 24 interna se conecta a una segunda red 27 interna a través de un cortafuegos 26. La segunda red 27 interna se conecta a una base de datos 28 que contiene datos relacionados con proyectos. La segunda red 27 interna también se conecta a una tercera red 30 interna a través de un segundo cortafuegos 29.

La tercera red 30 interna se conecta a una base de datos 31 que contiene datos relacionados con el sitio web de la compañía. La tercera red 30 interna se conecta a Internet 33 a través de un cortafuegos 32. Finalmente, un cuarto 34 y un quinto 35 usuario se conectan también a Internet 33.

Se asume que el primer usuario 21 es un miembro del personal administrativo del departamento de recursos humanos, el segundo y tercer usuarios 22 y 23 son empleados de más antigüedad que trabajan en una serie de proyectos, el cuarto usuario 34 es otro empleado que trabaja en una serie de proyectos y el quinto usuario 35 es un miembro público.

El primer usuario 21 puede únicamente necesitar acceso a la base de datos 25. Por consiguiente, el primer cortafuegos 26 puede evitar la transferencia de datos entre el primer usuario 21 y la segunda red 27.

El segundo y el tercer usuario 22 y 23 pueden necesitar acceso tanto a la primera base de datos 25 como a la segunda base de datos 28. Por consiguiente, el primer cortafuegos 26 puede permitir la transferencia de datos entre el segundo usuario 22 y la segunda red 27 y entre el tercer usuario 23 y la segunda red 27, pero el segundo cortafuegos 29 puede evitar la transferencia entre el segundo y el tercer usuario y la tercera red 30.

El cuarto usuario puede necesitar acceso a la segunda base de datos 28, pero puede no estar autorizado a acceder a la base de datos 25 de recursos humanos. Por lo tanto, el segundo y el tercer cortafuegos 29 y 32 pueden ambos permitir el paso de datos entre la base de datos 28 y el cuarto usuario 34. Al quinto usuario 35 se le puede permitir el acceso a la tercera base de datos 31 para ver el sitio web de la compañía. Por consiguiente, el tercer cortafuegos 32 puede permitir que se transfieran datos entre la tercera base de datos 39 y el quinto usuario 35, con el segundo cortafuegos 29 bloqueando el paso de datos hacia y desde el quinto usuario 35.

Habitualmente, las provisiones de seguridad de la disposición de sistemas tales como el sistema 20 se modifican de modo *ad hoc*. Por ejemplo, se considera el escenario en el que se da una responsabilidad al usuario 22 para alguna parte del sitio web de la compañía, los datos para lo cual están almacenados en la base de datos 31. En el escenario descrito anteriormente, el segundo cortafuegos 29 evitaría que ese usuario accediera a los datos en la base de datos 31. Para abordar este problema, puede requerirse un técnico experto para determinar que los ajustes de seguridad del usuario son la fuente del problema y para ajustar esos ajustes; por supuesto, puede requerirse permisos antes de que se puedan implementar tales cambios.

Tales disposiciones ad hoc tienen como resultado unos incrementos en los periodos de tiempo durante los cuales no están disponibles nuevas aplicaciones para los usuarios, requieren profesionales expertos para identificar y corregir problemas, y requieren tiempo de gestión a la hora de determinar si las normas de acceso de seguridad pueden suavizarse o no. Además, es probable que dichas disposiciones ad hoc conduzcan a políticas de seguridad que son suavizadas sin una completa consideración de las implicaciones de realizar tal acción.

El sistema 20 descrito anteriormente en referencia a la Figura 2 es relativamente simple. Queda claro que a medida que los sistemas se vuelven más complicados, se vuelve imposible rápidamente para los técnicos individuales recordar y mantener los procedimientos de seguridad requeridos.

La presente invención busca abordar al menos parte de los problemas identificados anteriormente.

La presente invención proporciona un método según se define en la reivindicación independiente 1. Se definen realizaciones específicas en las reivindicaciones dependientes.

La presente invención permite que el impacto de una o más políticas de seguridad en una aplicación sea determinado gestionando una evaluación del impacto. De esta manera, puede realizarse una determinación de si una aplicación en particular funcionará o no según se requiera antes de que se introduzca en la red. De hecho, dichas determinaciones pueden ser realizadas incluso si la red no ha sido implementada. La evaluación de impacto puede realizarse utilizando una herramienta automática, tal como el software o motor de comportamiento Erudine Behaviour Engine.

El nodo de la red puede hacer referencia a una parte de la red, tal como un usuario en particular, un grupo de usuarios en particular, un terminal de ordenador en particular o un grupo en particular de terminales de ordenador.

La etapa de determinación del modelo puede comprender definir dicho modelo. De forma alternativa, la etapa de determinación de dicho modelo puede comprender recibir dicho modelo; por ejemplo, como un archivo de entrada o conjunto de archivos de entrada. El método puede comprender además la etapa de ajustar el modelo de dicha red.

La etapa de determinación de dicha política de seguridad puede comprender definir dicha política de seguridad. Alternativamente, la etapa de determinación de dicha política de seguridad puede comprender recibir dicha política de seguridad; por ejemplo, como un archivo de entrada o un conjunto de archivos de entrada. El método puede además comprender la etapa de ajustar la política de seguridad. En una forma de la invención, la política de seguridad es endurecida o suavizada dependiendo del resultado del análisis de impacto.

La etapa de determinación de dichos requerimientos de comunicaciones puede comprender definir dichos requerimientos de comunicaciones. Alternativamente, la etapa de determinación de dichos requerimientos de comunicaciones puede comprender recibir dichos requerimientos de comunicaciones; por ejemplo como un archivo de entrada o un conjunto de archivos de entrada. El método puede además comprender la etapa de ajuste de los requerimientos de comunicaciones. En una forma de la invención, el archivo o conjunto de archivos de requerimientos de comunicaciones forma parte de un archivo o archivos de aplicación que están asociados con la propia aplicación (o aplicaciones).

El método puede comprender las etapas de ajuste a una, dos o todos de entre la representación del sistema, la política de seguridad y los requerimientos de comunicaciones. En algunas realizaciones, uno o más de esos requerimientos pueden ser fijos.

Los datos pueden tener que poseer transversalidad en diversos nodos entre su fuente y su destino. Uno o más nodos pueden ser agrupados en un único dominio de seguridad, con una política de seguridad común para todos los nodos dentro del dominio. En un ejemplo de realización, para cada servicio de la aplicación, la compatibilidad de los requerimientos de comunicación de la aplicación y las políticas de seguridad de los nodos se determina:

- buscando el dominio de seguridad para la fuente;

- buscando el dominio de seguridad para el destino o destinos definidos por los requerimientos de comunicación de la aplicación;

- buscando los dominios de seguridad que van a poseer transversalidad entre el dominio fuente y el dominio destino;

- determinando si los requerimientos de comunicaciones se comunicaran a través de las políticas de dominio de seguridad de cada dominio de seguridad que van a poseer transversalidad;

- si no se permite la comunicación a través de los dominios de seguridad que van a poseer transversalidad, generar un informe de la aplicación (o al servicio relevante asociado con la aplicación), y el dominio o dominios que tienen políticas de seguridad que evitan la comunicación.

Puede ser que el sistema asuma que cada ordenador central pertenece a una red, y que cada red está en un dominio de seguridad completo.

Puede ser que una política de “bloquear todo excepto” sea adoptada por al menos uno o todos los dominios de seguridad.

En un ejemplo de realización, se realiza una verificación para asegurar que las políticas de seguridad de los dominios no son demasiado abiertas. Para cada política en un dominio, al menos una de las siguientes verificaciones puede tener lugar:

- se realiza una verificación de que se utiliza la política; si no, entonces la política se considera demasiado abierta (o se desconoce su necesidad);

- se realiza una verificación de qué capas de protocolos se permiten, y si las capas permitidas no se utilizan, la amplitud de la política se considera demasiado extensa, y se puede realizar una verificación para determinar si los protocolos dentro de la capa se utilizan o no se utilizan (p.ej., pueden permitirse los servicios de la capa 3 y 4, pero solo se utiliza la TCP y la política se considera por lo tanto nuevamente demasiado amplia);

- se realiza una verificación para determinar los puertos abiertos.

La política de seguridad del dominio puede ajustarse entonces en vista de los resultados de al menos una de esas verificaciones.

Los dispositivos y métodos de acuerdo con la invención se describirán a continuación, únicamente a modo de ejemplo, en referencia a los dibujos esquemáticos anexos, en los que:

La Fig. 1 es un diagrama de bloques de una red informática conocida;

La Fig. 2 es un diagrama de bloques de una red informática conocida;

La Fig. 3 es un diagrama de bloques que demuestra un aspecto de la presente invención;

y la Fig. 4 es un diagrama de flujo que muestra un algoritmo de acuerdo con un aspecto de la presente invención.

La Figura 3 muestra una red informática, indicada en general con el número de referencia 40, de acuerdo con una primera realización de la presente invención. La red 40 comprende un ordenador 42 usuario, que está acoplado a Internet 46 (o a alguna otra red) a través de un cortafuegos 44. El ordenador 42 usuario incluye una aplicación 50. La aplicación 50 está ligada a un archivo 52 de requerimientos de comunicaciones. La aplicación 50 y su archivo 52 de requerimientos de comunicaciones asociado forman un archivo 48 de la aplicación. Las partes constituyentes del archivo 48 de la aplicación pueden estar ligadas entre sí de tal manera que, si el proveedor de la aplicación 50 es fiable, entonces el archivo 52 de requerimientos de comunicaciones también es fiable. En algunas realizaciones de la invención, para que sea implementado el archivo de requerimientos de comunicaciones, éste debe proceder de una fuente fiable.

El archivo 52 de requerimientos de comunicaciones establece los requerimientos de comunicaciones que la red 40 debe proporcionar para que la aplicación 50 funcione correctamente.

La presente invención hace uso del archivo de requerimientos de comunicaciones cuando se considera el efecto de incluir la aplicación 50 en la red 40.

La Figura 4 es un diagrama de flujo que demuestra la funcionalidad de un aspecto de la presente invención. El diagrama de flujo, indicado en general con el número de referencia 60 comienza en la etapa 62, etapa en la que se obtiene o se determina una representación de la red relevante. El diagrama de flujo entonces continúa hacia la etapa 64, etapa en la cual se obtiene o se determina el requerimiento de comunicaciones de la aplicación relevante; por ejemplo el requerimiento de comunicaciones puede obtenerse de uno o más archivos 52 de requerimiento de comunicaciones. El diagrama de flujo continúa entonces a la etapa 66, etapa en la cual se obtiene o se determina la política de seguridad relevante.

De la etapa 66, el diagrama de flujo continúa hacia la etapa 68. En la etapa 68, una técnica de análisis de impacto se utiliza para determinar si la política de seguridad obtenida en 66 es compatible con el requerimiento de comunicaciones obtenido en la etapa 64. Si no se cumplen los requerimientos de comunicaciones, el diagrama de flujo continúa hacia la etapa 70: si se cumplen los requerimientos de comunicaciones, el diagrama de flujo continúa hacia la etapa 72.

En esta etapa 72, la técnica de análisis de impacto se utiliza para determinar si se exceden los requerimientos de comunicaciones. Si es así, el diagrama de flujo continúa a la etapa 70; de otro modo, el algoritmo 60 termina en la etapa 74.

En la etapa 70, la política de seguridad se ajusta de la siguiente forma. Si, en la etapa 68, se determinó que los requerimientos de comunicaciones no se cumplieron, entonces la política de seguridad se suaviza. Alternativamente, si, en la etapa 72, se determinó que se excedieron los requerimientos de comunicaciones, entonces la política de seguridad se endurece. Una vez que la política de seguridad se haya ajustado, el algoritmo regresa a la etapa 68 y la etapa de análisis de impacto se repite.

El análisis de impacto al que se hace referencia anteriormente puede implementarse en una variedad de formas. Un ejemplo de sistema es el que se describe en el documento EP 1 758 025. Un sistema adecuado que se encuentra disponible en el comercio es el motor de comportamiento Erudine Behaviour Engine, disponible en Erudine Limited, 54 East Parade, Harrogate, North Yorkshire HG1 5LT, Reino Unido (www.erudine.com).

El algoritmo 60 descrito anteriormente en referencia a la Figura 4 supone que los requerimientos de comunicaciones y la configuración de red son algo fijo y que el perfil de seguridad es variable. Por supuesto, este puede no ser el caso, ya que un diseñador de sistemas puede ser capaz de modificar uno o más de los requerimientos de comunicaciones de la aplicación y el diseño de la propia red además, o en lugar de, modificar el perfil de seguridad.

De esta manera, puede evaluarse el impacto de la introducción de una nueva aplicación en la red antes de que la aplicación se introduzca en la red real. Esto permite que se realice una evaluación completa del impacto de cualquier aplicación de este tipo de forma rápida y con un bajo coste, sin interrumpir un sistema real. De hecho, dicho análisis puede ser realizado antes de que el propio sistema se implemente.

En diferentes formas de la presente invención, uno o más de entre la red, la política de seguridad y los archivos de requerimientos de comunicaciones son fijos, por tanto son limitados los ajustes que pueden realizarse para alojar una nueva aplicación en la red. La presente invención proporciona un método sistemático para predecir el efecto de introducir una aplicación de este tipo, independientemente de dichas restricciones.

REIVINDICACIONES

1. Un método de diseño de redes informáticas que comprende evaluar el impacto de la introducción de una aplicación en una red antes de que la aplicación se introduzca en la red real, comprendiendo el método las etapas de:

determinar una representación de la red (62);

determinar una política de seguridad para un nodo de la red (66);

determinar los requerimientos de comunicaciones para la aplicación en particular que se desea ejecutar dentro de dicho nodo de la red (64); y

realizar un análisis de impacto para determinar si dichos requerimientos de comunicaciones se cumplen (68) y/o se exceden (72) en dicho nodo, determinando de este modo si la aplicación en particular funcionará o no según se requiere;

el método que además comprende al menos uno de:

ajustar la representación de dicha red; y

ajustar dicha política de seguridad.

2. Método según se reivindica en la reivindicación 1, en donde dicha etapa de determinación de dicha representación (62) comprende definir dicha representación.

3. Método según se reivindica en la reivindicación 1, en donde dicha etapa de determinación de dicha representación (62) comprende recibir dicha representación.

4. Método según se reivindica en una cualquiera de las reivindicaciones 1 a 3, en donde dicha etapa de determinación de dicha política de seguridad (66) comprende definir dicha política de seguridad.

5. Método según se reivindica en una cualquiera de las reivindicaciones 1 a 3, en donde dicha etapa de determinación de dicha política de seguridad (66) comprende recibir dicha política de seguridad.

6. Método según se reivindica en una cualquiera de las reivindicaciones 1 a 5, en donde dicha etapa de determinación de dichos requerimientos de comunicaciones comprende definir dichos requerimientos de comunicaciones.

7. Método según se reivindica en una cualquiera de las reivindicaciones 1 a 5, en donde dicha etapa de determinación de dichos requerimientos de comunicaciones (64) comprende recibir dichos requerimientos de comunicaciones.

8. Método según se reivindica en la reivindicación 7, en donde los requerimientos de comunicaciones se proporcionan como parte de un archivo de aplicación.

9. Método según se reivindica en la reivindicación 1, en donde, en el caso de que dichos requerimientos de comunicaciones no se cumplan en dicho nodo, dicha política de seguridad se suaviza.

10. Método según se reivindica en la reivindicación 1 o reivindicación 9, en donde, en el caso de que dichos requerimientos de comunicaciones se excedan en dicho nodo, dicha política de seguridad se endurece.

11. Método según se reivindica en una cualquiera de las reivindicaciones 1 a 10, que además comprende la etapa de ajustar dichos requerimientos de comunicaciones.

12. Método según se reivindica en una cualquiera de las reivindicaciones 1 a 11, en donde dicha etapa de realizar un análisis de impacto comprende el uso de un motor de comportamiento.

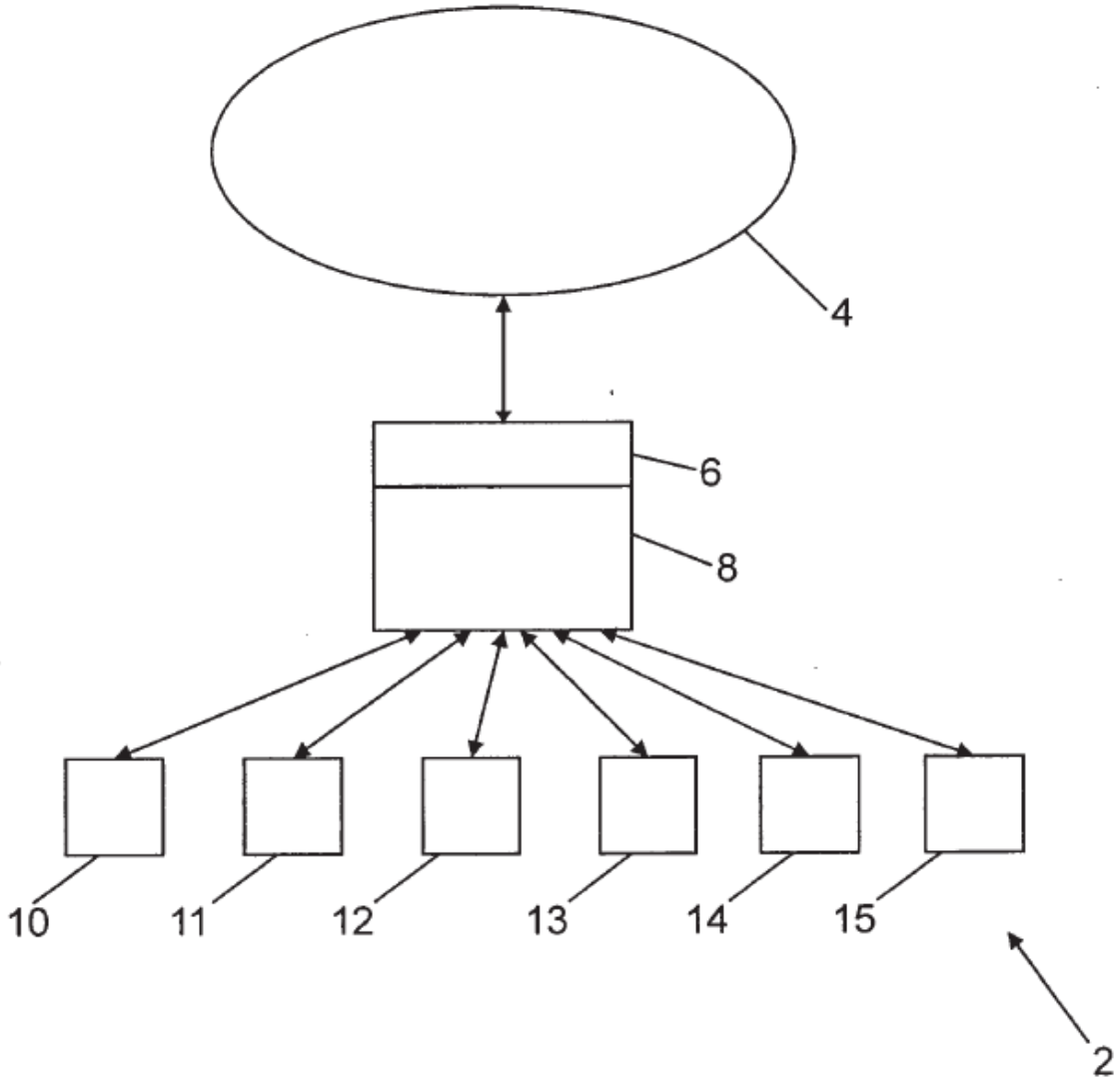

Fig. 1

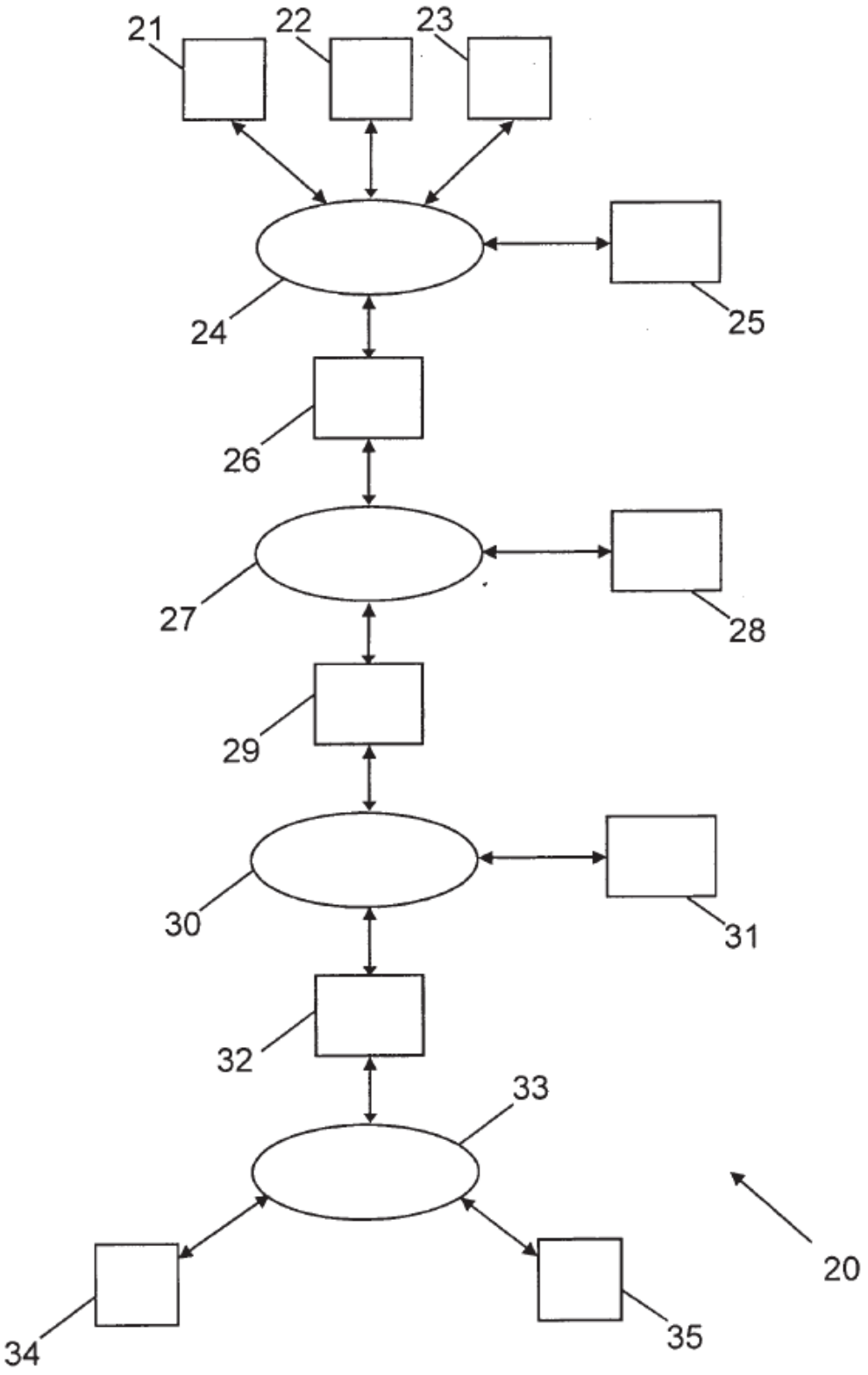

Fig. 2

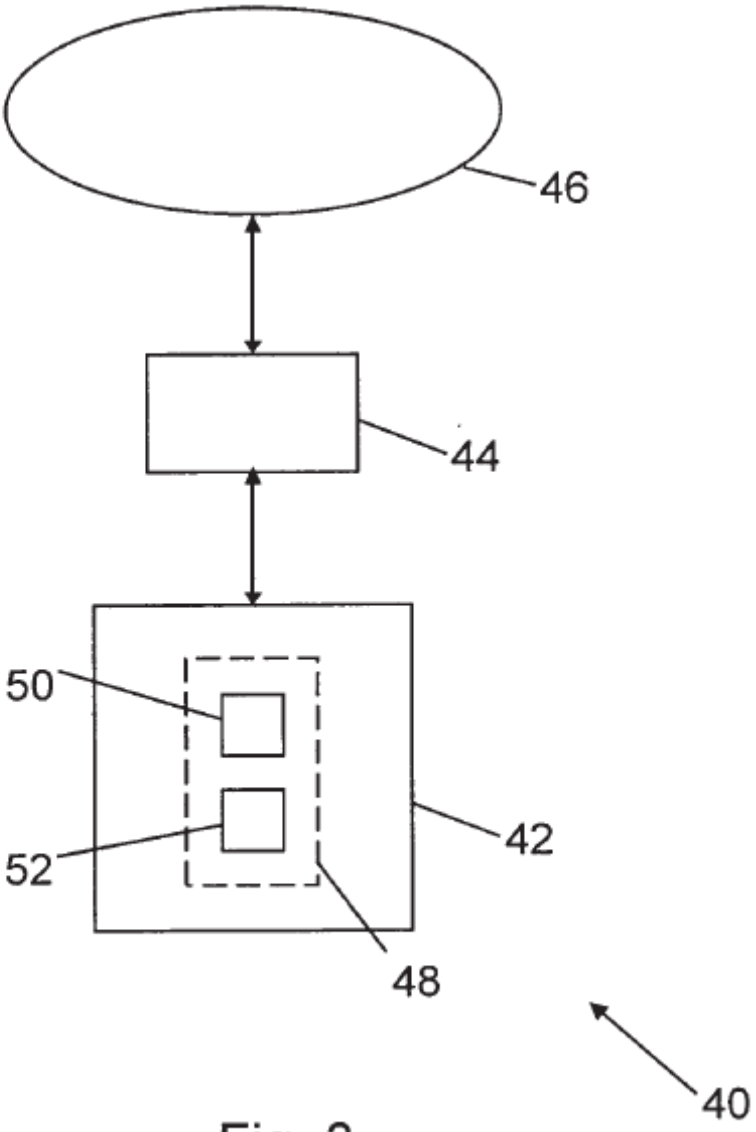

Fig. 3

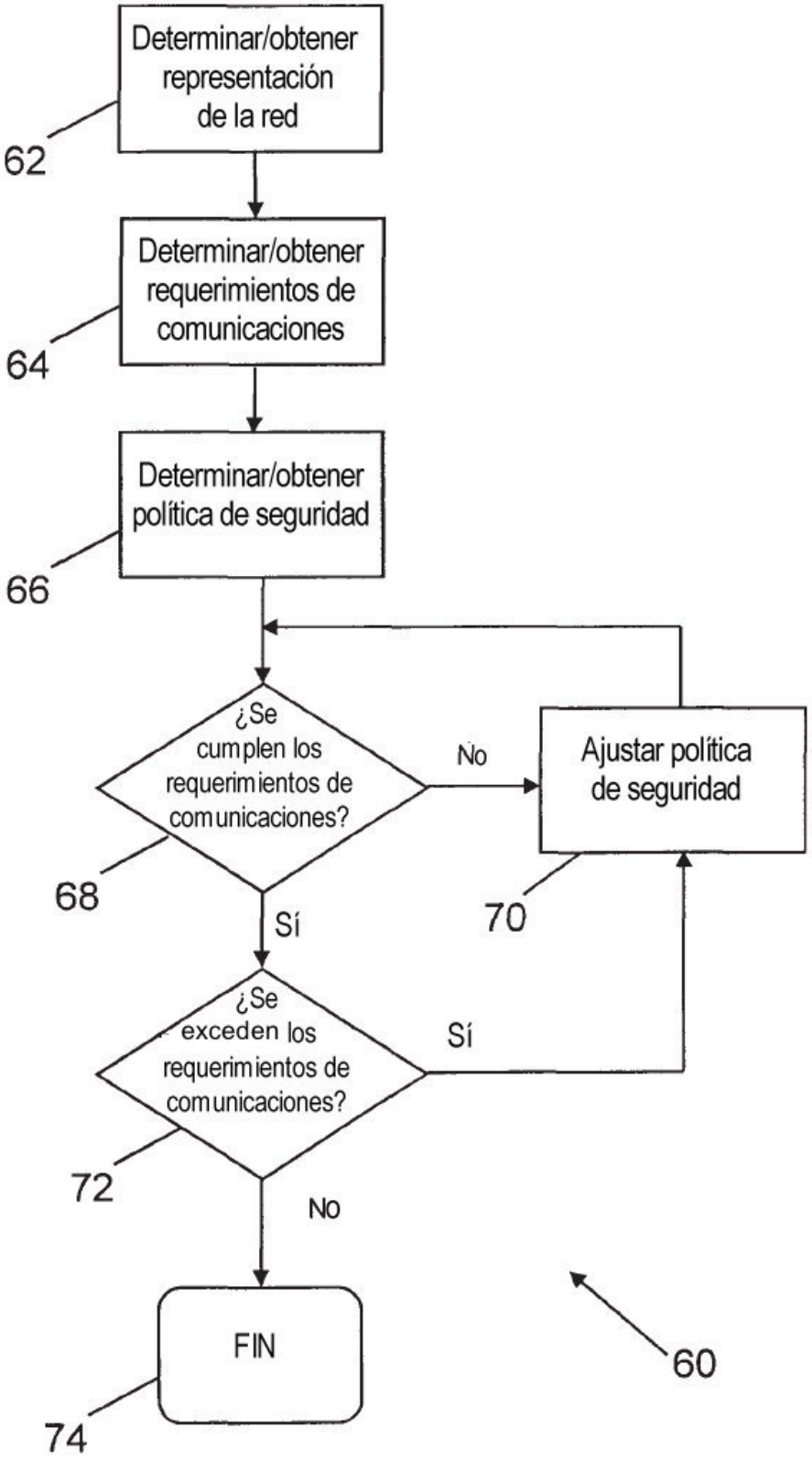
Determinar/obtener representación de la red
62
Determinar/obtener requerimientos de comunicaciones
64
Determinar/obtener política de seguridad
66
¿Se cumplen los requerimientos de comunicaciones?
68
No
Ajustar política de seguridad
70
Sí
¿Se exceden los requerimientos de comunicaciones?
72
Sí
No
FIN
74
60

Fig. 4