(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 784 203**

(51) Int. CI.:

H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **11.07.2014 E 14176736 (8)**

(97) Fecha y número de publicación de la concesión europea: **15.01.2020 EP 2966828**

(54) Título: **Método para detectar un ataque a un entorno de trabajo conectado a una red de comunicación**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
23.09.2020

(73) Titular/es:

DEUTSCHE TELEKOM AG (100.0%)
Friedrich-Ebert-Allee 140
53113 Bonn, DE

(72) Inventor/es:

OCHSE, MARCO

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Método para detectar un ataque a un entorno de trabajo conectado a una red de comunicación

La presente invención se refiere a un método para detectar un ataque a un entorno de trabajo conectado a una red de comunicación y se refiere a un sistema de seguridad de red con un entorno de trabajo y con un elemento de seguridad de red para la detección de tal ataque.

En los sistemas de terminales de trabajo o en los entornos de trabajo o en los entornos de los lugares de trabajo de las empresas están almacenados frecuentemente datos sensibles, que pueden ser interesantes para un atacante. El robo de secretos de empresa sucede a menudo de forma inadvertida mediante la introducción clandestina de programas maliciosos en la red informática propia de la empresa o espiando entornos de trabajo de grupos adecuados de personas, por ejemplo, de la junta directiva de una empresa o de personas públicas importantes. En este contexto se emplean en tales ataques a veces programas maliciosos de desarrollo propio y adaptados individualmente al uso concreto, que los productos antivirus disponibles en el mercado detectan muy tarde o no detectan. Si bien, como víctimas potenciales de un ataque espía digital, los grupos de personas que potencialmente estén en peligro en las empresas pueden prepararse, en la mayoría de los casos se desconocen las circunstancias exactas, como por ejemplo el lugar, el momento y la configuración.

Los documentos pertinentes US 2012/084866, US 2013/145465, US 2006/018466 y US 2004/172557 se refieren a sistemas para detectar ataques mediante tarros de miel. El documento “Martin Roesch: Snort Users Manua, I Snort Release: 1.8.3” describe un producto para detectar ataques a redes.

El objetivo de la presente invención es detectar un ataque en una red de ordenadores, en particular en un sistema de terminales de trabajo de la red de ordenadores. Este objetivo se logra mediante las características de las reivindicaciones independientes. Las reivindicaciones dependientes tienen por objeto formas de perfeccionamiento ventajosas.

Los métodos y sistemas presentados a continuación pueden utilizarse para proteger entornos de trabajo. Un entorno de trabajo designa en la presente memoria un sistema informático en una red de ordenadores, que está preparado para un usuario individual o un grupo individual de usuarios. Por ejemplo, los miembros del personal de una empresa pueden utilizar entornos de trabajo para realizar sus tareas relacionadas con la empresa. El entorno de trabajo puede comprender uno o varios terminales de trabajo, por ejemplo, un PC, una estación de trabajo, un ordenador portátil, un PDA, un teléfono inteligente, que estén conectados a una red de comunicación. La red de comunicación puede ser una red alámbrica, por ejemplo, utilizando Ethernet, USB o cable, etc. La red de comunicación puede ser una red inalámbrica, por ejemplo, utilizando WLAN, WiFi, Bluetooth, infrarrojos o un estándar de radiotelefonía móvil como por ejemplo LTE, UMTS, GSM, etc.

Los métodos y sistemas presentados a continuación pueden emplearse para proteger una red de ordenadores, en particular un entorno de trabajo en una red de ordenadores, contra ataques de *botnets* (redes de ordenadores esclavos), en particular contra ataques DDoS, ataques de *spamming*, ataques de *sniffing*, ataques de *phishing*, difusión de *malware*, *key-logging*, instalación de *software* no deseado, usurpación de identidad, manipulación de la red de ordenadores, etc.

Los métodos y sistemas presentados a continuación pueden emplearse en el campo de la tecnología de la información (TI). Tecnología de la información es un concepto genérico para el procesamiento de información y datos y para el *hardware* y el *software* necesarios para ello. La tecnología de la información de una empresa comprende todos los dispositivos técnicos para generar, procesar y transmitir información.

Los métodos y sistemas presentados a continuación pueden ser de diferentes tipos. Los distintos elementos descritos pueden estar realizados mediante componentes de *hardware* o componentes de *software*, por ejemplo, componentes electrónicos, que pueden producirse mediante diferentes tecnologías y comprenden por ejemplo chips semiconductores, ASIC, microprocesadores, procesadores digitales de señales, circuitos eléctricos integrados, circuitos electroópticos y/o componentes pasivos.

La idea fundamental, en la que se basa la invención, es la detección de un posible o inminente ataque a la red de ordenadores basándose en atraer a un atacante de forma dirigida a un objetivo, a modo de un tarro de miel, es decir, a un elemento de seguridad de red que emula un determinado entorno de trabajo valioso para el atacante. Mientras el atacante intenta acceder a este entorno de trabajo emulado, el sistema puede registrar las actividades del atacante así realizadas y, basándose en esto, determinar una característica del ataque o del atacante. Mediante esta característica pueden detectarse y/o frustrarse ataques similares.

Según un primer aspecto, la invención se refiere a un método para detectar un ataque a un entorno de trabajo conectado a una red de comunicación, con las etapas siguientes: emular electrónicamente el entorno de trabajo mediante un elemento de seguridad de red conectado a la red de comunicación; captar un tráfico de red en el elemento

de seguridad de red; comparar el tráfico de red captado con un tráfico de red predeterminado; y disparar una primera señal de aviso de ataque en caso de una diferencia entre el tráfico de red captado y el tráfico de red predeterminado.

La ventaja de tal método consiste en que a través de la emulación del entorno de trabajo mediante el elemento de seguridad de red se induce a un atacante a dirigir su ataque al elemento de seguridad de red, de manera que el entorno de trabajo real está protegido. Por lo tanto, el tráfico de red en el elemento de seguridad de red puede captarse y evaluarse. La comparación con un tráfico de red predeterminado ofrece una posibilidad sencilla de detectar una irregularidad que indique un ataque. La ventaja de tal método consiste por lo tanto en el efecto protector en relación con el entorno de lugar de trabajo real, así como en la capacidad de reacción rápida para detectar un ataque a un entorno de lugar de trabajo y prevenir contra el mismo.

Según una forma de realización, el captar el tráfico de red comprende captar una tasa de acceso al elemento de seguridad de red, y el comparar el tráfico de red captado con el tráfico de red predeterminado comprende comparar la tasa de acceso captada con una tasa de acceso predeterminada.

La ventaja consiste en que la tasa de acceso predeterminada puede determinarse fácilmente, por ejemplo, evaluando estadísticamente actividades de un usuario típico del entorno del trabajo. Si se realiza un ataque al entorno de trabajo o al elemento de seguridad de red, la tasa de acceso aumenta de manera significativa, lo que puede comprobarse de un modo fácil y fiable.

Según una forma de realización, el emular electrónicamente el entorno de trabajo comprende emular un entorno desprotegido de trabajo, que comprende al menos partes del mismo *software* que el instalado en el entorno de trabajo.

Esto tiene la ventaja de que un atacante encuentra entonces el mismo *software* en el elemento de seguridad de red y piensa que es un entorno de lugar de trabajo interesante para él. Así pues, el atacante dirigirá sus actividades a investigar el elemento de seguridad de red en la creencia de que es un entorno de lugar de trabajo real.

Según una forma de realización, el entorno de trabajo está protegido y la emulación electrónica comprende una simulación de un entorno desprotegido de trabajo.

Esto tiene la ventaja de que la simulación de un entorno desprotegido de trabajo distrae del o de los entornos protegidos de trabajo y puede atraer a un atacante.

Según una forma de realización, entre el entorno de trabajo y la red de comunicación está intercalado un elemento de conexión de red y el elemento de conexión de red tiene conectado un elemento de vigilancia de red y el método comprende copiar un tráfico de red existente en el elemento de conexión de red al elemento de vigilancia de red.

Esto tiene la ventaja de que todo el tráfico de red desde y hacia el entorno de trabajo pasa por el elemento de conexión de red, donde puede copiarse fácilmente y alimentarse al elemento de vigilancia de red para su posterior evaluación. De este modo, el elemento de vigilancia de red puede captar todas las actividades del atacante dirigidas al entorno de trabajo.

Según una forma de realización, el método comprende captar el tráfico de red en el elemento de conexión de red mediante el elemento de vigilancia de red; y disparar una segunda señal de aviso de ataque al detectarse una anomalía en el tráfico de red captado en el elemento de conexión de red.

Esto tiene la ventaja de que se genera una segunda señal de aviso de ataque independientemente de la primera señal de aviso de ataque y de este modo la detección de un ataque se realiza de una manera aún más fiable. La segunda señal de aviso de ataque se basa en la detección de una anomalía en el tráfico de red en el elemento de conexión de red, es decir, el tráfico de red de orden superior, mientras que la primera señal de aviso de ataque se basa en la comparación del tráfico de red relacionado con el lugar de trabajo en el elemento de seguridad de red con un tráfico de red predeterminado, es decir, un tráfico de red de referencia.

Según una forma de realización, la detección de la anomalía se basa en una detección de procesos de búsqueda anómalos en el tráfico de red captado.

Esto tiene la ventaja de que la detección de procesos de búsqueda anómalos indica de manera fiable un ataque que está teniendo lugar o que es inminente. Los ordenadores de una red de ordenadores generan siempre un gran número de mensajes de aviso, por ejemplo en caso de no funcionar una actualización de *software*, cuando el procesador está sobrecargado, cuando no se ha realizado hasta el momento una actualización del *software*, cuando se ha introducido incorrectamente una contraseña, cuando temporalmente no es posible acceder a Internet, cuando no es posible acceder a determinados datos, etc. Estos mensajes de aviso están causados por determinadas anomalías de la red de ordenadores, que durante el funcionamiento se producen con mayor o menor frecuencia y en la mayoría de los casos requieren una interacción del usuario para subsanarlas. En cambio, los procesos de búsqueda anómalos no

son funciones típicas del sistema. Deben considerarse críticos e indican un uso indebido del ordenador. Por medio de los procesos de búsqueda anómalos así detectados puede detectarse de manera fiable un ataque.

Según una forma de realización, el método comprende, al detectarse la anomalía, registrar en tiempo real el tráfico de red captado en el elemento de conexión de red.

Esto tiene la ventaja de que las acciones del atacante pueden registrarse y analizarse de inmediato en cuanto una anomalía indique un ataque inminente. El sistema de seguridad puede actuar rápidamente, los tiempos de reacción son muy cortos.

Según una forma de realización, el método comprende generar un mensaje de aviso basándose en la primera señal de aviso de ataque y en la segunda señal de aviso de ataque.

Esto tiene la ventaja de que el mensaje de aviso es particularmente fiable cuando se basa en dos señales de aviso de ataque determinadas independientemente una de otra, concretamente la primera señal de aviso de ataque y la segunda señal de aviso de ataque.

Según una forma de realización, la generación del mensaje de aviso se basa además en señales de aviso de ataque adicionales de entornos de trabajo adicionales de la red de comunicación.

Cuando la generación del mensaje de aviso se basa además en señales de aviso de ataque adicionales de entornos de trabajo adicionales de la red de comunicación, el mensaje de aviso es aún más fiable, dado que para ello se recurre a información adicional.

Según una forma de realización, el método comprende además protocolizar el tráfico de red captado en el elemento de seguridad de red mediante un servidor de protocolo al dispararse la primera señal de aviso de ataque; y protocolizar el tráfico de red captado en el elemento de conexión de red mediante el servidor de protocolo al dispararse la segunda señal de aviso de ataque.

Esto tiene la ventaja de que, al protocolizar el tráfico de red captado en ambos elementos de red, éste está disponible para análisis posteriores. De este modo, el análisis del patrón de ataque puede realizarse con mayor exactitud y pueden hacerse predicciones más fiables en relación con futuros ataques.

Según una forma de realización, el método comprende detectar atributos característicos del ataque basándose en el tráfico de red protocolizado del elemento de seguridad de red y en el tráfico de red protocolizado del elemento de conexión de red.

Esto tiene la ventaja de que los atributos característicos del ataque pueden utilizarse para detectar fácilmente y sin un gran esfuerzo otros ataques basados en la misma característica de ataque.

Según un segundo aspecto, la invención se refiere a un sistema de seguridad de red con: un elemento 105 de conexión de red, que está diseñado para establecer una conexión con una red 115 de comunicación; y un elemento 103 de seguridad de red conectado al elemento 105 de conexión de red, pudiendo al menos un entorno 101 de trabajo conectarse al elemento 105 de conexión de red, para conectar el al menos un entorno 101 de trabajo a la red 115 de comunicación, y estando el elemento 103 de seguridad de red diseñado para detectar un ataque al o a los entornos 101 de lugar de trabajo basándose en una emulación del o de los entornos 101 de lugar de trabajo.

La ventaja de tal sistema de seguridad de red consiste en que a través de la emulación del entorno de lugar de trabajo mediante el elemento de seguridad de red se induce a un atacante a dirigir su ataque al elemento de seguridad de red, de manera que el entorno de lugar de trabajo real está protegido. Por lo tanto, el tráfico de red en el elemento de seguridad de red puede captarse y evaluarse. La ventaja de tal sistema de seguridad de red consiste por lo tanto en el efecto protector en relación con el entorno de lugar de trabajo real, así como en la capacidad de reacción rápida para detectar un ataque a un entorno de lugar de trabajo.

Según una forma de realización, el elemento de seguridad de red comprende lo siguiente: un emulador, que está diseñado para emular electrónicamente el o los entornos de trabajo; una unidad de captación, que está diseñada para captar el tráfico de red en el elemento de seguridad de red; y una unidad de aviso de ataque, que está diseñada para comparar el tráfico de red captado con un tráfico de red predeterminado y, en caso de una diferencia entre el tráfico de red captado y el tráfico de red predeterminado, disparar una primera señal de aviso de ataque.

La ventaja de tal sistema de seguridad de red consiste en que la comparación del tráfico de red captado con un tráfico de red predeterminado ofrece una posibilidad sencilla y fiable de detectar una irregularidad que indique un ataque. El disparo de la primera señal de aviso de ataque puede realizarse con una rapidez tal que el usuario no sea sorprendido por el ataque o lo detecte demasiado tarde, de manera que tenga suficiente tiempo para tomar las medidas de precaución correspondientes.

Según una forma de realización, el sistema de seguridad de red comprende un elemento de vigilancia de red que está conectado al elemento de conexión de red, estando el elemento de vigilancia de red diseñado para captar un tráfico de red en el elemento de conexión de red y, en caso de detectarse una anomalía en el tráfico de red captado en el elemento de conexión de red, disparar una segunda señal de aviso de ataque.

Esto tiene la ventaja de que se genera una segunda señal de aviso de ataque independientemente de la primera señal de aviso de ataque y de este modo la detección de un ataque se realiza de una manera aún más fiable. La segunda señal de aviso de ataque se basa en la detección de una anomalía en el tráfico de red en el elemento de conexión de red, es decir, el tráfico de red de orden superior, mientras que la primera señal de aviso de ataque se basa en la comparación del tráfico de red relacionado con el lugar de trabajo en el elemento de seguridad de red con un tráfico de red predeterminado, es decir, un tráfico de red de referencia.

Según una forma de realización, el sistema de seguridad de red comprende un servidor de protocolo, que está diseñado para generar un mensaje de aviso basándose en la primera señal de aviso de ataque y la segunda señal de aviso de ataque y protocolizar el tráfico de red captado en el elemento de seguridad de red y el tráfico de red captado en el elemento de conexión de red y, basándose en el tráfico de red protocolizado, detectar un atributo característico del ataque.

Esto tiene la ventaja de que, al protocolizar el tráfico de red captado en ambos elementos de red, éste está disponible para análisis posteriores. De este modo, el análisis del patrón de ataque puede realizarse con mayor exactitud y pueden hacerse predicciones más fiables en relación con futuros ataques. Además, los atributos característicos del ataque pueden utilizarse para detectar fácilmente y sin un gran esfuerzo otros ataques basados en la misma característica de ataque. La invención se define mediante la reivindicación 1 de método y la reivindicación 8 de sistema y sus reivindicaciones dependientes.

Haciendo referencia a los dibujos adjuntos se explican otros ejemplos de realización. Se muestran:

- La Figura 1, una representación esquemática de un sistema 100 de seguridad de red según una forma de realización;
- la Figura 2, una representación esquemática de un elemento 103 de seguridad de red según una forma de realización;
- la Figura 3, una representación esquemática de un elemento 107 de vigilancia de red según una forma de realización;
- la Figura 4, una representación esquemática de un servidor 109 de protocolo según una forma de realización;
- la Figura 5, una representación esquemática de un método 500 para detectar un ataque a un entorno de trabajo según una forma de realización; y
- la Figura 6, una representación esquemática de un método 600 para detectar un ataque a un entorno de trabajo según otra forma de realización.

En la descripción detallada siguiente se hace referencia a los dibujos adjuntos, que forman parte de la misma y en los que, a modo de ilustración, se muestran formas de realización específicas en las que la invención puede realizarse. Se entiende que también pueden utilizarse otras formas de realización y que pueden efectuarse modificaciones estructurales o lógicas sin apartarse del concepto de la presente invención. Por lo tanto, la descripción detallada siguiente no debe entenderse en un sentido limitativo. Además, se entiende que las características de los distintos ejemplos de realización descritos en la presente memoria pueden combinarse entre sí, siempre que no se indique específicamente otra cosa.

Los aspectos y las formas de realización se describen haciendo referencia a los dibujos, en donde en general los símbolos de referencia iguales se refieren a elementos iguales. En la descripción siguiente se exponen numerosos detalles específicos con fines de explicación, para transmitir una comprensión en profundidad de uno o varios aspectos de la invención. Sin embargo, para un experto puede ser evidente que uno o varios aspectos o formas de realización pueden realizarse con un menor grado de los detalles específicos. En otros casos se representan en forma esquemática estructuras y elementos conocidos, para facilitar la descripción de uno o varios aspectos o formas de realización. Se entiende que pueden utilizarse otras formas de realización y que pueden efectuarse modificaciones estructurales o lógicas sin apartarse del concepto de la presente invención.

Aunque es posible que una determinada característica o un determinado aspecto de una forma de realización se describan en relación con sólo una de varias implementaciones, tal característica o tal aspecto pueden además combinarse con una o varias otras características o aspectos de las otras implementaciones, como pueda ser deseable y ventajoso para una aplicación dada o determinada. Además, en la medida en que se utilicen los términos “contienen”, “tienen”, “con” u otras variantes de los mismos bien en la descripción detallada, bien en las reivindicaciones, tales términos han de ser inclusivos de manera similar al término “comprenden”. Los términos “acoplado” y “conectado” pueden haberse utilizado junto con derivaciones de los mismos. Se entiende que tales términos se utilizan para indicar que dos elementos cooperan o interactúan entre sí independientemente de que estén en contacto directo físico o

eléctrico o que no estén en contacto directo uno con otro. Además, el término “ejemplar” debe interpretarse solamente como un ejemplo, en lugar de la designación para lo mejor u óptimo. Por lo tanto, la descripción siguiente no debe entenderse en un sentido limitativo.

La Figura 1 muestra una representación esquemática de un sistema 100 de seguridad de red según una forma de realización.

El sistema 100 de seguridad de red comprende un elemento 105 de conexión de red, que sirve para establecer una conexión con una red 115 de comunicación, así como un elemento 103 de seguridad de red conectado al elemento 105 de conexión de red. Al menos un entorno 101 de trabajo es conectable al elemento 103 de conexión de red o puede conectarse al elemento 103 de conexión de red, para conectar el al menos un entorno 101 de trabajo a la red 115 de comunicación.

El elemento 105 de conexión de red puede conectar el entorno 101 de trabajo, el elemento 103 de seguridad de red y el elemento 107 de vigilancia de red a la red 115 de comunicación. El elemento 105 de conexión de red puede ser por ejemplo un conmutador, una pasarela o un encaminador, siendo posible, mediante distintos puertos, conectar los distintos elementos de red al conmutador, la pasarela o el encaminador y transmitirlos correspondientemente. El tipo de transmisión puede configurarse mediante protocolos de encaminador o protocolos de pasarela o ajustes de conmutador correspondientes.

El elemento de seguridad de red sirve para detectar un ataque al, al menos un, entorno 101 de lugar de trabajo basándose en una emulación del, al menos un, entorno 101 de lugar de trabajo. En este contexto, puede ser un entorno 101 de lugar de trabajo o varios de tales entornos 101 de lugar de trabajo distintos.

El elemento 103 de seguridad de red puede estar construido como se describe después más detalladamente en la Figura 2. El elemento 103 de seguridad de red puede presentar un emulador 201, una unidad 203 de captación y una unidad 205 de aviso de ataque. Con el emulador pueden emularse electrónicamente el o los entornos 101 de trabajo. Con la unidad 203 de captación puede captarse el tráfico 202 de red en el elemento 103 de seguridad de red. Con la unidad 205 de aviso de ataque se puede comparar el tráfico 202 de red captado con un tráfico 204 de red predeterminado y, en caso de una diferencia entre el tráfico 202 de red captado y el tráfico 204 de red predeterminado, disparar una primera señal 110 de aviso de ataque.

El entorno 101 de trabajo puede ser un sistema informático en una red de ordenadores, que esté preparado para un usuario individual o un grupo individual de usuarios. Por ejemplo, el entorno de trabajo puede estar asignado a un miembro del personal de una empresa para que éste pueda cumplir en el mismo sus tareas relacionadas con la empresa. El entorno de trabajo puede comprender uno o varios terminales de trabajo, por ejemplo, un PC, una estación de trabajo, un ordenador portátil, un PDA, un teléfono inteligente u otros tipos de ordenadores o procesadores. La red 115 de comunicación puede ser una red alámbrica, por ejemplo, una red por Ethernet, USB o cable. La red 115 de comunicación puede ser una red inalámbrica, por ejemplo, una red por WLAN, WiFi, Bluetooth, infrarrojos, o una red de comunicación de un estándar de radiotelefonía móvil, como por ejemplo LTE, UMTS, GSM, etc.

El sistema 100 de seguridad de red puede presentar además un elemento 107 de vigilancia de red. El elemento 107 de vigilancia de red puede estar construido como se describe posteriormente en la Figura 3 con mayor detalle. El elemento 107 de vigilancia de red puede servir para captar un tráfico 302 de red en el elemento 105 de conexión de red y, en caso de detectarse una anomalía 304 en el tráfico 302 de red captado en el elemento 105 de vigilancia de red, disparar una segunda señal 112 de aviso de ataque.

El sistema 100 de seguridad de red puede presentar además un servidor 109 de protocolo, que por ejemplo puede estar construido como se describe posteriormente en la Figura 4 con mayor detalle. El servidor 109 de protocolo puede generar un mensaje 114 de aviso basándose en la primera señal 110 de aviso de ataque y la segunda señal 112 de aviso de ataque. El servidor 109 de protocolo puede protocolizar el tráfico 202 de red captado en el elemento 103 de seguridad de red y el tráfico 302 de red captado en el elemento 105 de conexión de red y, basándose en el tráfico 402 de red protocolizado, detectar un atributo característico 404 del ataque.

La emulación del entorno 101 de lugar de trabajo por parte del elemento 103 de seguridad de red tiene como fin inducir a un atacante 113 a dirigir su ataque al elemento 103 de seguridad de red, de manera que el entorno 101 de lugar de trabajo real está protegido. El tráfico de red en el elemento 103 de seguridad de red puede ser captado y evaluado eficazmente por éste. De este modo se logra un efecto protector en relación con el entorno 101 de lugar de trabajo real. El elemento 103 de seguridad de red puede estar equipado con procesadores rápidos que permitan al elemento 103 de seguridad de red detectar muy rápidamente un ataque al entorno 101 de lugar de trabajo.

En este contexto, un método para detectar un ataque puede desarrollarse como se describe a continuación:

1. Un atacante (interno) 113 examina la red 115 en busca de objetivos atacables;
2. el lugar de trabajo o el entorno 101 de trabajo está protegido;

3. el elemento 103 de seguridad de red simula un lugar de trabajo desprotegido y atrae al atacante 113;
4a. el atacante 113 encuentra en (3) un objetivo atacable en una zona de red interesante, es decir, el elemento 103 de seguridad de red;
4b. el elemento 107 de vigilancia de red detecta procesos de búsqueda anómalos en el tráfico de red en tiempo real e informa de los mismos de manera centralizada;
4c. el servidor 109 de protocolo protocoliza mensajes entrantes relativos a procesos de búsqueda anómalos;
5a. el atacante inicia un intento de intrusión en (3), es decir, en el elemento 103 de seguridad de red;
5b. el elemento 103 de seguridad de red detecta un intento de intrusión, registra las entradas del atacante 113 en tiempo real e informa de las mismas de manera centralizada; el elemento 107 de vigilancia de red detecta atributos de un ataque en el tráfico de red e informa de los mismos de manera centralizada; el servidor 109 de protocolo protocoliza mensajes entrantes relativos a atributos de un ataque;
6. el servidor 109 de protocolo relaciona los mensajes de (5b), es decir, del elemento 103 de seguridad de red y del elemento 107 de vigilancia de red, y genera un informe de aviso;
7. el analista de seguridad analiza en el dispositivo 111 de análisis el informe de aviso para adoptar medidas adecuadas.

La Figura 2 muestra una representación esquemática de un elemento 103 de seguridad de red según una forma de realización.

El elemento 103 de seguridad de red comprende un emulador 201, una unidad 203 de captación y una unidad 205 de aviso de ataque. Con el emulador 201 puede emularse electrónicamente el entorno 101 de trabajo representado anteriormente en la Figura 1, es decir, el emulador 201 puede generar o emular un entorno emulado 101a de trabajo. El emulador 201 puede por ejemplo instalar en el elemento 103 de seguridad de red al menos partes del mismo *software* que el instalado en el entorno 101 de trabajo. El atacante 113 encuentra entonces el mismo *software* en el elemento 103 de seguridad de red y piensa que es un entono 101 de lugar de trabajo interesante para él. De este modo se simula frente al atacante 113 que el elemento 103 de seguridad de red es un entorno 101 de trabajo real, para inducirle a continuar sus actividades de ataque, de manera que sea posible seguir sus huellas. Así pues, el atacante 113 dirigirá sus actividades a examinar el elemento 103 de seguridad de red en la creencia de que es un entorno 101 de lugar de trabajo real.

Con la unidad 203 de captación puede captarse tráfico 202 de red en el elemento 103 de seguridad de red. Con la unidad 205 de aviso de ataque se puede comparar el tráfico 202 de red captado con un tráfico 204 de red predeterminado y, en caso de una diferencia entre el tráfico 202 de red captado y el tráfico 204 de red predeterminado, disparar una primera señal 110 de aviso de ataque. La captación del tráfico 202 de red en el elemento 103 de seguridad de red puede realizarse por ejemplo captando una tasa de acceso al elemento 103 de seguridad de red. La tasa de acceso así captada puede entonces compararse con una tasa de acceso predeterminada.

La tasa de acceso predeterminada puede determinarse fácilmente, por ejemplo, evaluando estadísticamente actividades de un usuario típico del entorno 101 de trabajo. Si se realiza un ataque al entorno 101 de trabajo o al elemento 103 de seguridad de red, la tasa de acceso aumenta significativamente, lo que puede comprobarse de una manera fácil y fiable.

La Figura 3 muestra una representación esquemática de un elemento 107 de vigilancia de red según una forma de realización.

El elemento 107 de vigilancia de red está conectado al elemento 105 de conexión de red y puede captar el tráfico 302 de red en el elemento 105 de conexión de red. Así pues, todo el tráfico de red desde y hacia el entorno 101 de trabajo puede pasar por el elemento 105 de conexión de red, desde donde puede copiarse fácilmente y alimentarse al elemento 107 de vigilancia de red para su posterior evaluación. De este modo, el elemento 107 de vigilancia de red puede captar todas las actividades del atacante 113 dirigidas al entorno 101 de trabajo.

Al detectarse una anomalía 304 en el tráfico 302 de red captado en el elemento 105 de conexión de red, el elemento de vigilancia de red puede disparar una segunda señal 112 de aviso de ataque. Así pues, la segunda señal 112 de aviso de ataque puede generarse independientemente de la primera señal 110 de aviso de ataque, de manera que la detección de un ataque puede realizarse de una manera aún más fiable. La segunda señal 112 de aviso de ataque puede basarse en la detección de una anomalía en el tráfico de red en el elemento de conexión de red, es decir, el tráfico de red de orden superior, mientras que la primera señal 110 de aviso de ataque puede basarse en la comparación del tráfico de red relacionado con el lugar de trabajo en el elemento de seguridad de red con un tráfico de red predeterminado, es decir, un tráfico de red de referencia.

La detección de la anomalía 304 puede realizarse mediante una detección de procesos de búsqueda anómalos en el tráfico 302 de red captado. La detección de procesos de búsqueda anómalos puede indicar de manera fiable un ataque que esté teniendo lugar o que sea inminente. Los ordenadores de una red de ordenadores generan siempre un gran número de mensajes de aviso, por ejemplo, en caso de no funcionar una actualización de *software*, cuando el procesador está sobrecargado, cuando no se ha realizado hasta el momento una actualización del *software*, cuando

se ha introducido incorrectamente una contraseña, cuando temporalmente no es posible acceder a Internet, cuando no es posible acceder a determinados datos, etc. Estos mensajes de aviso están causados por determinadas anomalías de la red de ordenadores, que durante el funcionamiento se producen con mayor o menor frecuencia y en la mayoría de los casos requieren una interacción del usuario para subsanarlas. En cambio, los procesos de búsqueda anómalos no son funciones típicas del sistema. Deben considerarse críticos e indican un uso indebido del ordenador. Por medio de los procesos de búsqueda anómalos así detectados puede detectarse de manera fiable un ataque.

El elemento 107 de vigilancia de red puede presentar una unidad de captación, por ejemplo, una memoria, con la que pueda captarse el tráfico 302 de red en el elemento 105 de conexión de red. El elemento 107 de vigilancia de red puede presentar una unidad de detección, por ejemplo, un correlacionador de datos, para detectar una anomalía 304 en el tráfico 302 de red captado en el elemento 105 de conexión de red, por ejemplo, mediante la aplicación de métodos de correlación. El elemento 107 de vigilancia de red puede presentar una unidad de aviso, con la que pueda generarse una señal 112 de aviso de ataque en caso de detectarse una anomalía 304. El elemento 107 de vigilancia de red puede presentar una interfaz de notificación mediante la cual sea posible transmitir la señal 112 de aviso de ataque a otros componentes en el sistema 100 de seguridad de red, por ejemplo, como se muestra en la Figura 1, a través del elemento 105 de conexión de red y la red 115 de comunicación al servidor 109 de protocolo y/o al dispositivo 111 de análisis o, como no se muestra en la Figura 1, a través de una interfaz propia, eludiendo la red 115 de comunicación, al servidor 109 de protocolo y/o al dispositivo 111 de análisis.

La Figura 4 muestra una representación esquemática de un servidor 109 de protocolo según una forma de realización.

El servidor 109 de protocolo puede generar un mensaje 114 de aviso basándose en la primera señal 110 de aviso de ataque y la segunda señal 112 de aviso de ataque. El servidor 109 de protocolo puede protocolizar el tráfico 202 de red captado en el elemento 103 de seguridad de red y el tráfico 302 de red captado en el elemento 105 de conexión de red, por ejemplo, en una memoria de protocolo, y, basándose en el tráfico 402 de red protocolizado, detectar un atributo característico 404 del ataque.

Mediante la protocolización del tráfico 202, 302 de red captado en ambos elementos 103, 105 de red, éste está disponible para análisis posteriores. De este modo, el análisis del patrón de ataque puede realizarse con mayor exactitud y pueden hacerse predicciones más fiables en relación con futuros ataques. Los atributos característicos del ataque detectados mediante el servidor 109 de protocolo pueden utilizarse para detectar fácilmente y sin un gran esfuerzo otros ataques basados en la misma característica de ataque.

Los protocolos registrados por el servidor 109 de protocolo y los atributos característicos 404 del ataque detectados por el servidor 109 de protocolo pueden ponerse a disposición de un dispositivo 111 de análisis, como está representado en la Figura 1.

El dispositivo 111 de análisis puede estar realizado por ejemplo como sistema SIEM (*Security Information and Event Management* o Gestión de Eventos e Información de Seguridad). El dispositivo 111 de análisis puede por ejemplo combinar una gestión de información de seguridad (“security information management”, SIM) con una gestión de eventos de seguridad (“security event management”, SEM) y realizar un análisis en tiempo real de alarmas de seguridad. El dispositivo 111 de análisis y/o el servidor 109 de protocolo pueden utilizarse para registrar datos relevantes en cuanto a la seguridad y generar informes para aplicaciones de conformidad.

La Figura 5 muestra una representación esquemática de un método 500 para detectar un ataque a un entorno de trabajo según una forma de realización.

El método 500 puede comprender, en una primera etapa 501 del método, configurar un elemento de conexión de red, por ejemplo, un elemento 105 de conexión de red según la descripción relativa a la Figura 1. El elemento 105 de conexión de red puede tener conectados sistemas de lugar de trabajo protegidos, por ejemplo, sistemas 101 de lugar de trabajo según la representación de la Figura 1, que puedan ser interesantes para un atacante 113. La configuración del elemento 105 de conexión de red puede prever que todo el “Traffic”, es decir, tráfico de red, se copie en un puerto en el que esté conectado un elemento de vigilancia de red, por ejemplo, un elemento 107 de vigilancia de red según la representación de la Figura 1.

Como alternativa, el método 500 puede realizarse ya con un elemento de conexión de red configurado.

El método 500 puede comprender, en una segunda etapa 502 del método, simular un sistema de lugar de trabajo, por ejemplo, de un entorno 101 de trabajo según la descripción relativa a la Figura 1, mediante un elemento 103 de seguridad de red. La simulación de un sistema de lugar de trabajo desprotegido tiene como fin distraer de los sistemas de lugar de trabajo protegidos y atraer al mismo a un atacante.

El método 500 puede comprender, en una tercera etapa 503 del método, comprobar el tráfico de red entrante y saliente, por ejemplo, con un elemento 107 de vigilancia de red, como se describe detalladamente en la Figura 1. El

elemento 107 de vigilancia de red es capaz de inspeccionar el tráfico de red entrante y saliente del elemento 105 de conexión de red en cuanto a patrones sospechosos.

Si el tráfico de red está codificado, sólo están disponibles para el análisis los datos de red y protocolo de la conexión. El contenido de un dato codificado mediante la transmisión puede analizarse posteriormente cuando el elemento 107 de vigilancia de red tenga a su disposición la información de codificación que sirve de base a la conexión.

El método 500 puede comprender, en una cuarta etapa 504 del método, un análisis y una creación de informes de aviso. Si el elemento 103 de seguridad de red detecta un intento de intrusión, es posible protocolizar y captar de manera centralizada las entradas del atacante. Si el elemento 107 de vigilancia de red descubre patrones sospechosos, pueden generarse alarmas y transmitirse éstas a un sistema central para la consolidación, por ejemplo, el servidor 109 de protocolo, como se describe en las Figuras 1 y 4.

Mediante la combinación de la simulación de un lugar de trabajo desprotegido con un elemento de vigilancia de red y la protocolización centralizada, ahora es posible de manera centralizada relacionar de forma causal los sucesos y sacar conclusiones sobre el atacante.

Pueden reunirse de manera centralizada mensajes de otras zonas de red según el mismo diseño. Cuantos más datos puedan recopilarse en esta forma, tanto más cualitativa será la información en relación con un ataque realizado, es decir, pueden reducirse recopilaciones erróneas.

El método 500 puede comprender, en una quinta etapa 505 del método, una adopción de medidas adecuadas por parte de un analista de seguridad. El analista de seguridad puede recibir de forma automatizada un mensaje de aviso, por ejemplo, en forma de un correo electrónico, un SMS, una aplicación (*App*), etc. y puede adoptar entonces medidas adecuadas.

La Figura 6 muestra una representación esquemática de un método 600 para detectar un ataque a un entorno de trabajo conectado a una red 115 de comunicación, por ejemplo, un entorno 101 de trabajo como el representado en la Figura 1, según otra forma de realización.

El método 600 comprende emular electrónicamente 601 el entorno 101 de trabajo mediante un elemento de seguridad de red conectado a la red 115 de comunicación, por ejemplo, un elemento 103 de seguridad de red como el representado en la Figura 1. El método 600 comprende captar 602 un tráfico 202 de red en el elemento 103 de seguridad de red. El método 600 comprende comparar 603 el tráfico 202 de red captado con un tráfico 204 de red predeterminado. El método 600 comprende disparar 604 una primera señal 110 de aviso de ataque en caso de una diferencia entre el tráfico 202 de red captado y el tráfico 204 de red predeterminado, por ejemplo, según la descripción relativa a las Figuras 1 y 2.

El captar 602 el tráfico de red puede comprender captar una tasa de acceso al elemento 103 de seguridad de red. El comparar 603 el tráfico 202 de red captado con el tráfico 204 de red predeterminado puede comprender comparar la tasa de acceso captada con una tasa de acceso predeterminada.

El emular electrónicamente 601 el entorno 101 de trabajo puede comprender emular un entorno desprotegido 101a de trabajo, que comprenda al menos partes del mismo *software* que el instalado en el entorno 101 de trabajo.

Entre el entorno 101 de trabajo y la red 115 de comunicación puede estar intercalado un elemento 105 de conexión de red, por ejemplo, según la representación de la Figura 1, y el elemento 105 de conexión de red puede tener conectado un elemento 107 de vigilancia de red. El método 600 puede comprender copiar un tráfico de red existente en el elemento 105 de conexión de red al elemento 107 de vigilancia de red.

El método 600 puede comprender además captar el tráfico 302 de red en el elemento 105 de conexión de red mediante el elemento 107 de vigilancia de red; y disparar una segunda señal 112 de aviso de ataque en caso de detectarse una anomalía 304, por ejemplo, según la descripción relativa a la Figura 3, en el tráfico 302 de red captado en el elemento 105 de conexión de red. La detección de la anomalía 304 puede basarse en una detección de procesos de búsqueda anómalos en el tráfico 302 de red captado.

El método 600 puede comprender además registrar en tiempo real el tráfico 302 de red captado en el elemento 105 de conexión de red en caso de detectarse la anomalía 304. El método 600 puede comprender generar un mensaje 114 de aviso basándose en la primera señal 110 de aviso de ataque y la segunda señal 112 de aviso de ataque, por ejemplo, según la descripción relativa a las Figuras 1 a 3. El generar el mensaje 114 de aviso puede basarse además en señales de aviso de ataque adicionales de entornos de trabajo adicionales de la red 115 de comunicación.

El método 600 puede comprender además protocolizar el tráfico 202 de red captado en el elemento 103 de seguridad de red mediante un servidor 109 de protocolo al dispararse la primera señal 110 de aviso de ataque, por ejemplo según la descripción relativa a las Figuras 1 y 4. El método 600 puede comprender protocolizar el tráfico 302 de red

captado en el elemento 105 de conexión de red mediante el servidor 109 de protocolo al dispararse la segunda señal 112 de aviso de ataque, por ejemplo según la descripción relativa a las Figuras 1 y 4. El método 600 puede comprender además detectar atributos característicos 404 del ataque basándose en el tráfico 202 de red protocolizado existente en el elemento 103 de seguridad de red y el tráfico 302 de red protocolizado existente en el elemento 105 de conexión de red.

El método 600 describe una generalización de las etapas 1 a 7 de método explicadas al final de la descripción relativa a la Figura 1, así como del método 500 descrito en la Figura 5.

Un aspecto de la invención comprende también un producto de programa informático que puede cargarse directamente en la memoria interna de un ordenador digital y que comprende secciones de código de *software* con las que puede realizarse el método 500, 600 descrito en relación con la Figura 5 o la Figura 6 cuando el producto se ejecuta en un ordenador. El producto de programa informático puede estar almacenado en un medio adecuado para un ordenador y comprender lo siguiente: recursos de programa legibles por ordenador que induzcan a un ordenador a emular electrónicamente 601 un entorno de trabajo mediante un elemento de seguridad de red conectado a la red de comunicación; captar 602 un tráfico de red en el elemento de seguridad de red; comparar 603 el tráfico de red captado con un tráfico de red predeterminado; y disparar 604 una primera señal de aviso de ataque en caso de una diferencia entre el tráfico de red captado y el tráfico de red predeterminado. El ordenador puede ser un PC, por ejemplo, un PC de una red de ordenadores. El ordenador puede estar realizado como un chip, un ASIC, un microprocesador o un procesador de señales y estar dispuesto en una red de ordenadores, por ejemplo, en una red de ordenadores como se describe en las Figuras 1 a 4.

Es evidente que las características de las distintas formas de realización descritas a modo de ejemplo en la presente memoria pueden combinarse entre sí, excepto cuando se indique específicamente otra cosa. Como se presenta en la descripción y los dibujos, los distintos elementos representados como conectados no han de estar conectados entre sí directamente; entre los elementos conectados pueden estar previstos elementos intermedios. Además, es evidente que las formas de realización de la invención pueden estar implementadas en circuitos individuales, circuitos parcialmente integrados o circuitos completamente integrados o herramientas de programación. El concepto “por ejemplo” se refiere solamente a un ejemplo y no a lo mejor u óptimo. En la presente memoria se han ilustrado y descrito determinadas formas de realización, pero para el experto es evidente que pueden realizarse una pluralidad de implementaciones alternativas y/o similares en lugar de las formas de realización mostradas y descritas, sin apartarse del concepto de la presente invención.

Lista de símbolos de referencia

100: Sistema de seguridad de red
101: Entorno de trabajo
101a: Entorno emulado de trabajo
103: Elemento de seguridad de red
105: Elemento de conexión de red
107: Elemento de vigilancia de red
109: Servidor de protocolo
110: Primera señal de aviso de ataque
111: Dispositivo de análisis
112: Segunda señal de aviso de ataque
113: Atacante
114: Mensaje de aviso
115: Red de comunicación
201: Emulador
203: Unidad de captación
205: Unidad de aviso de ataque
202: Tráfico de red captado en el elemento de seguridad de red
204: Tráfico de red predeterminado
302: Tráfico de red captado en el elemento de conexión de red
304: Anomalía
402: Tráfico de red protocolizado
404: Atributos característicos del ataque
500: Método para detectar un ataque a un entorno de trabajo
501: Primera etapa del método: configurar el elemento de conexión de red
502: Segunda etapa del método: simular un sistema de lugar de trabajo
503: Tercera etapa del método: comprobar el tráfico de red entrante y saliente
504: Cuarta etapa del método: análisis y creación de informes de aviso
505: Quinta etapa del método: adopción de medidas adecuadas por parte de un analista de seguridad
600: Método para detectar un ataque a un entorno de trabajo
601: Primera etapa del método: emular electrónicamente el entorno de trabajo
602: Segunda etapa del método: captar un tráfico de red en el elemento de seguridad de red

603: Tercera etapa del método: comparar el tráfico de red captado con un tráfico de red predeterminado
604: Cuarta etapa del método: disparar una primera señal de aviso de ataque

REIVINDICACIONES

1. Método (600) para detectar un ataque a un entorno (101) de trabajo conectado a una red (115) de comunicación, en donde entre el entorno (101) de trabajo y la red (115) de comunicación está intercalado un elemento (105) de conexión de red y en donde el elemento (105) de conexión de red tiene conectado un elemento (107) de vigilancia de red, con las etapas siguientes:

emular electrónicamente (601) el entorno (101) de trabajo mediante un elemento (103) de seguridad de red conectado a la red (115) de comunicación;
captar (602) un tráfico (202) de red en el elemento (103) de seguridad de red;
comparar (603) el tráfico (202) de red captado con un tráfico (204) de red predeterminado;
disparar (604) una primera señal (110) de aviso de ataque mediante el elemento (103) de seguridad de red en caso de una diferencia entre el tráfico (202) de red captado y el tráfico (204) de red predeterminado;
copiar un tráfico de red existente en el elemento (105) de conexión de red al elemento (107) de vigilancia de red;
captar el tráfico (302) de red en el elemento (105) de conexión de red mediante el elemento (107) de vigilancia de red; y
disparar una segunda señal (112) de aviso de ataque mediante el elemento (107) de vigilancia de red en caso de detectarse una anomalía (304) en el tráfico (302) de red captado en el elemento (105) de conexión de red;
generar un mensaje (114) de aviso basándose en la primera señal (110) de aviso de ataque y la segunda señal (112) de aviso de ataque;
basándose la generación del mensaje (114) de aviso además en señales de aviso de ataque adicionales de entornos de trabajo adicionales de la red (115) de comunicación.

2. Método (600) según la reivindicación 1,
en donde el captar (602) el tráfico (202) de red comprende captar una tasa de acceso al elemento de (103) de seguridad de red; y
en donde el comparar (603) el tráfico (202) de red captado con el tráfico (204) de red predeterminado comprende comparar la tasa de acceso captada con una tasa de acceso predeterminada.

3. Método (600) según la reivindicación 1 o 2,
en donde el emular electrónicamente (601) el entorno (101) de trabajo comprende emular un entorno desprotegido (101a) de trabajo, que comprende al menos partes del mismo *software* que el instalado en el entorno (101) de trabajo.

4. Método (600) según una de las reivindicaciones precedentes,
en donde la detección de la anomalía (304) se basa en una detección de procesos de búsqueda anómalos en el tráfico (302) de red captado.

5. Método (600) según una de las reivindicaciones precedentes, que comprende:

registrar en tiempo real el tráfico de red (302) captado en el elemento (105) de conexión de red en caso de detectarse la anomalía (304).

6. Método (600) según una de las reivindicaciones precedentes, que comprende además:

protocolizar el tráfico (202) de red captado en el elemento (103) de seguridad de red mediante un servidor (109) de protocolo al dispararse la primera señal (110) de aviso de ataque; y protocolizar el tráfico (302) de red captado en el elemento (105) de conexión de red mediante el servidor (109) de protocolo al dispararse la segunda señal (112) de aviso de ataque.

7. Método (600) según la reivindicación 6, que comprende:

detectar atributos característicos (404) del ataque basándose en el tráfico (202) de red protocolizado existente en el elemento (103) de seguridad de red y el tráfico (302) de red protocolizado existente en el elemento (105) de conexión de red.

8. Sistema (100) de seguridad de red con:

un elemento (105) de conexión de red, que está diseñado para establecer una conexión con una red (115) de comunicación; y
un elemento (103) de seguridad de red conectado al elemento (105) de conexión de red,
en donde al menos un entorno (101) de trabajo está conectado al elemento (105) de conexión de red, para conectar el al menos un entorno (101) de trabajo a la red (115) de comunicación, y

en donde el elemento (103) de seguridad de red está diseñado para detectar un ataque al o a los entornos (101) de lugar de trabajo basándose en una emulación del o de los entornos (101) de lugar de trabajo, comprendiendo el elemento (103) de seguridad de red lo siguiente:

un emulador (201), que está diseñado para emular electrónicamente el o los entornos (101) de trabajo;
una unidad (203) de captación, que está diseñada para captar el tráfico (202) de red en el elemento (103) de seguridad de red; y
una unidad (205) de aviso de ataque, que está diseñada para comparar el tráfico (202) de red captado con un tráfico (204) de red predeterminado y, en caso de una diferencia entre el tráfico (202) de red captado y el tráfico (204) de red predeterminado, disparar la primera señal (110) de aviso de ataque, y además con:
un elemento (107) de vigilancia de red, que está conectado al elemento (105) de conexión de red,
estando el elemento (107) de vigilancia de red diseñado para captar un tráfico (302) de red en el elemento (105) de conexión de red y, en caso de detectarse una anomalía (304) en el tráfico (302) de red captado en el elemento (105) de conexión de red, disparar una segunda señal (112) de aviso de ataque; y
estando el sistema de seguridad de red diseñado para generar un mensaje (114) de aviso basándose en la primera señal (110) de aviso de ataque, la segunda señal de aviso de ataque y señales de aviso de ataque adicionales de entornos de trabajo adicionales de la red (115) de comunicación.

9. Sistema (100) de seguridad de red según la reivindicación 8, con:

un servidor (109) de protocolo, que está diseñado para generar un mensaje (114) de aviso basándose en la primera señal (110) de aviso de ataque y la segunda señal (112) de aviso de ataque y protocolizar el tráfico (202) de red captado en el elemento (103) de seguridad de red y el tráfico (302) de red captado en el elemento (105) de conexión de red y, basándose en el tráfico (402) de red protocolizado, detectar un atributo característico (404) del ataque.

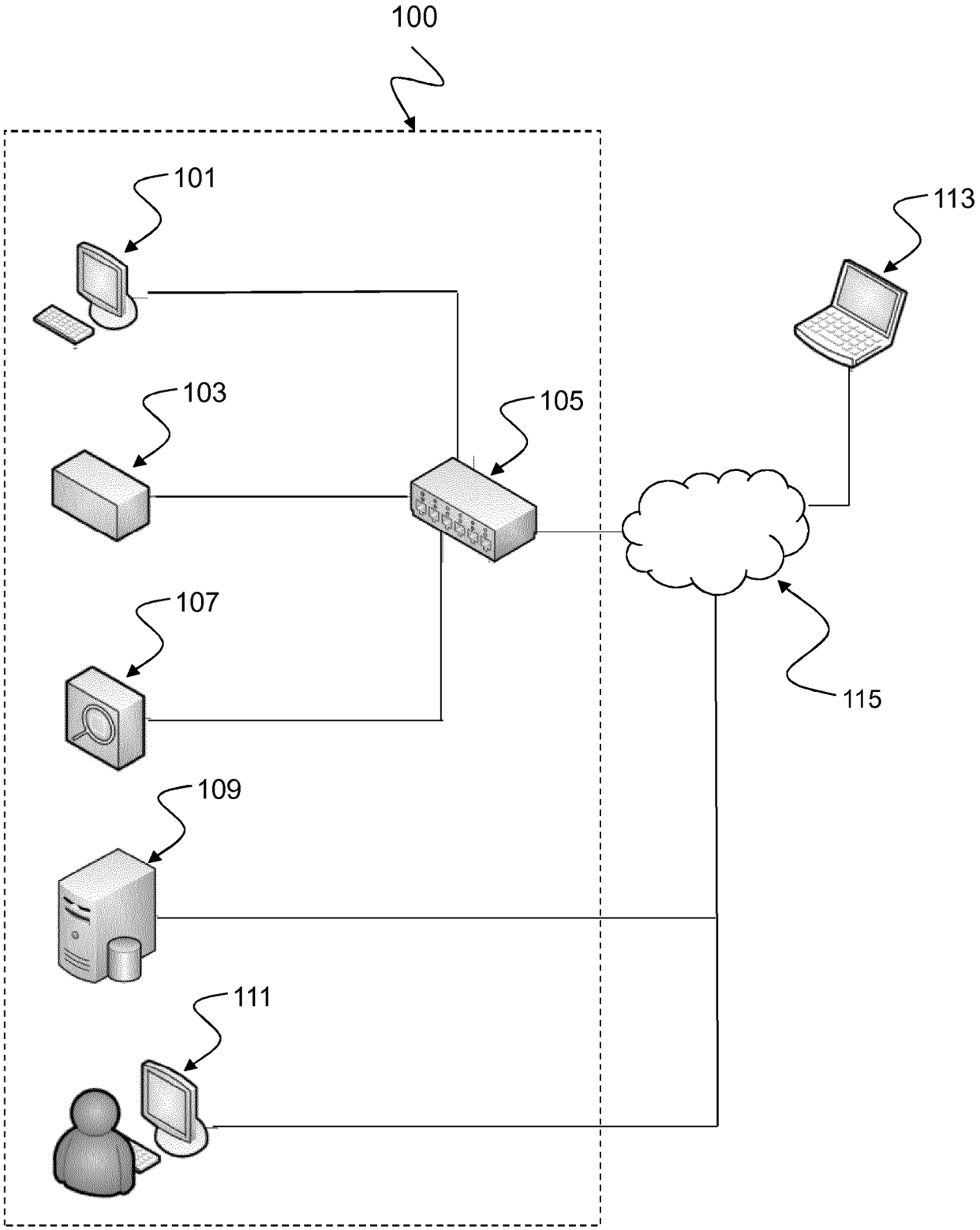

Fig. 1

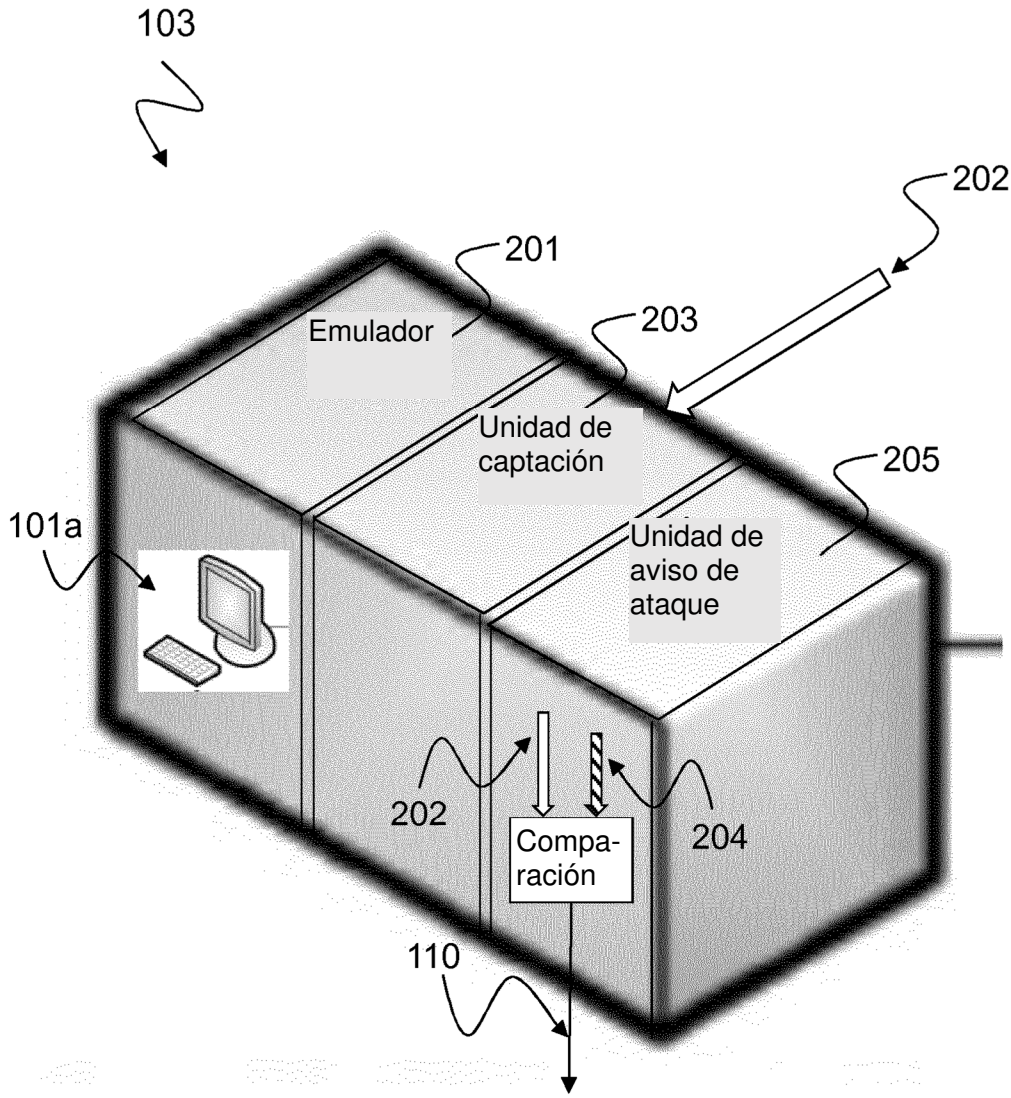
103
202
201
Emulador
203
Unidad de captación
205
101a
Unidad de aviso de ataque
202
Compa-ración
204
110
1ª señal de aviso de ataque

Fig. 2

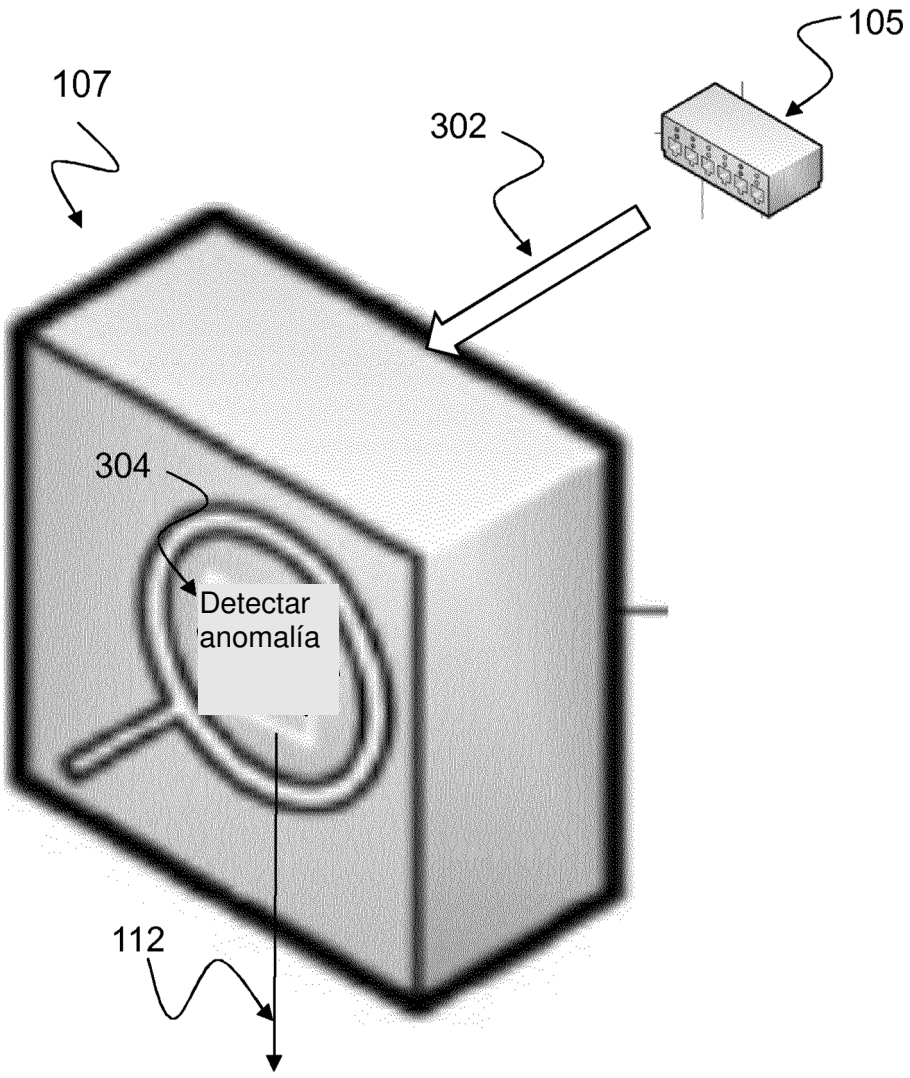
105
107
302
304
Detectar
anomalía
112
2ª señal de aviso de ataque

Fig. 3

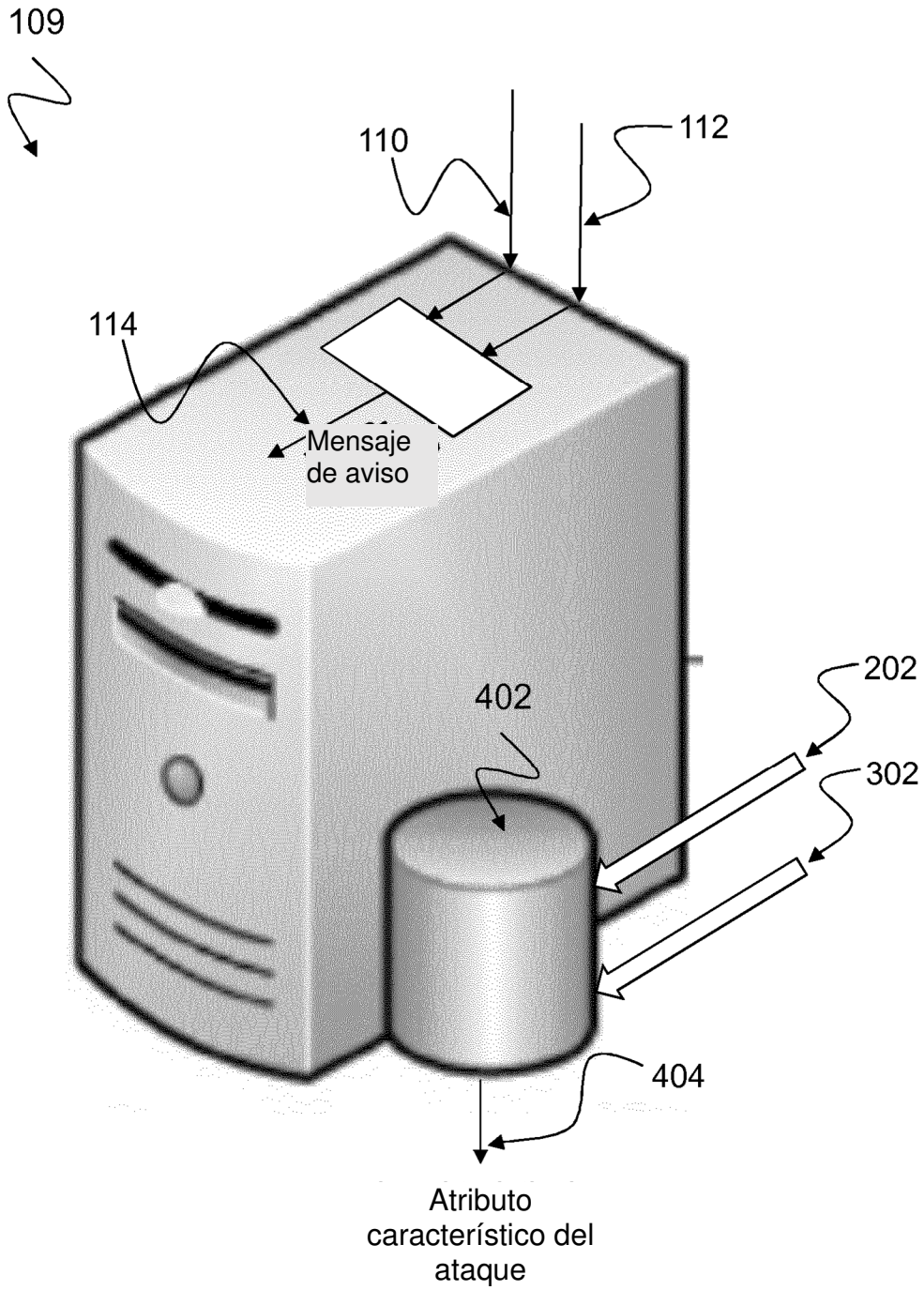
109
110
112
114
Mensaje
de aviso
202
402
302
404
Atributo
característico del
ataque

Fig. 4

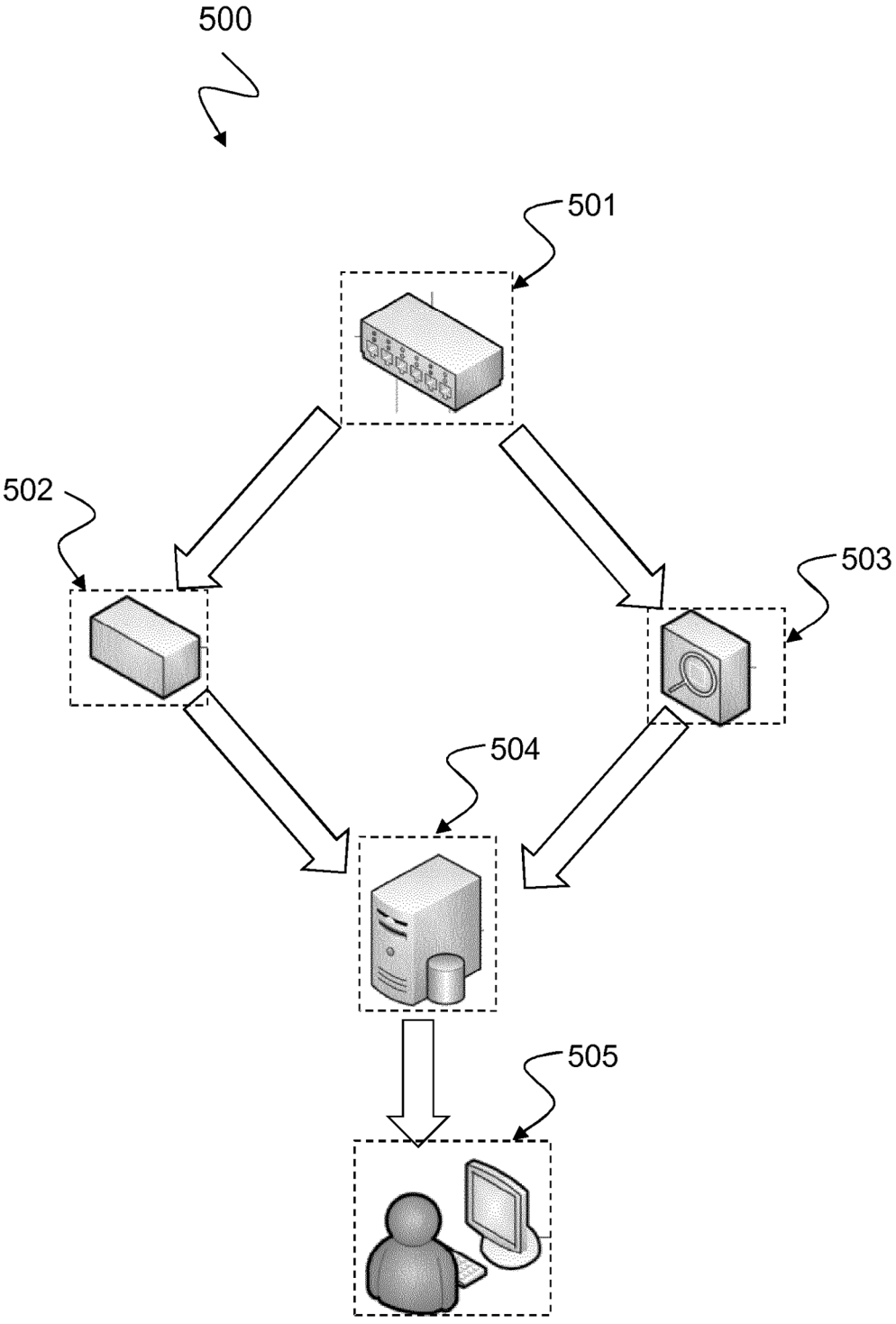

Fig. 5

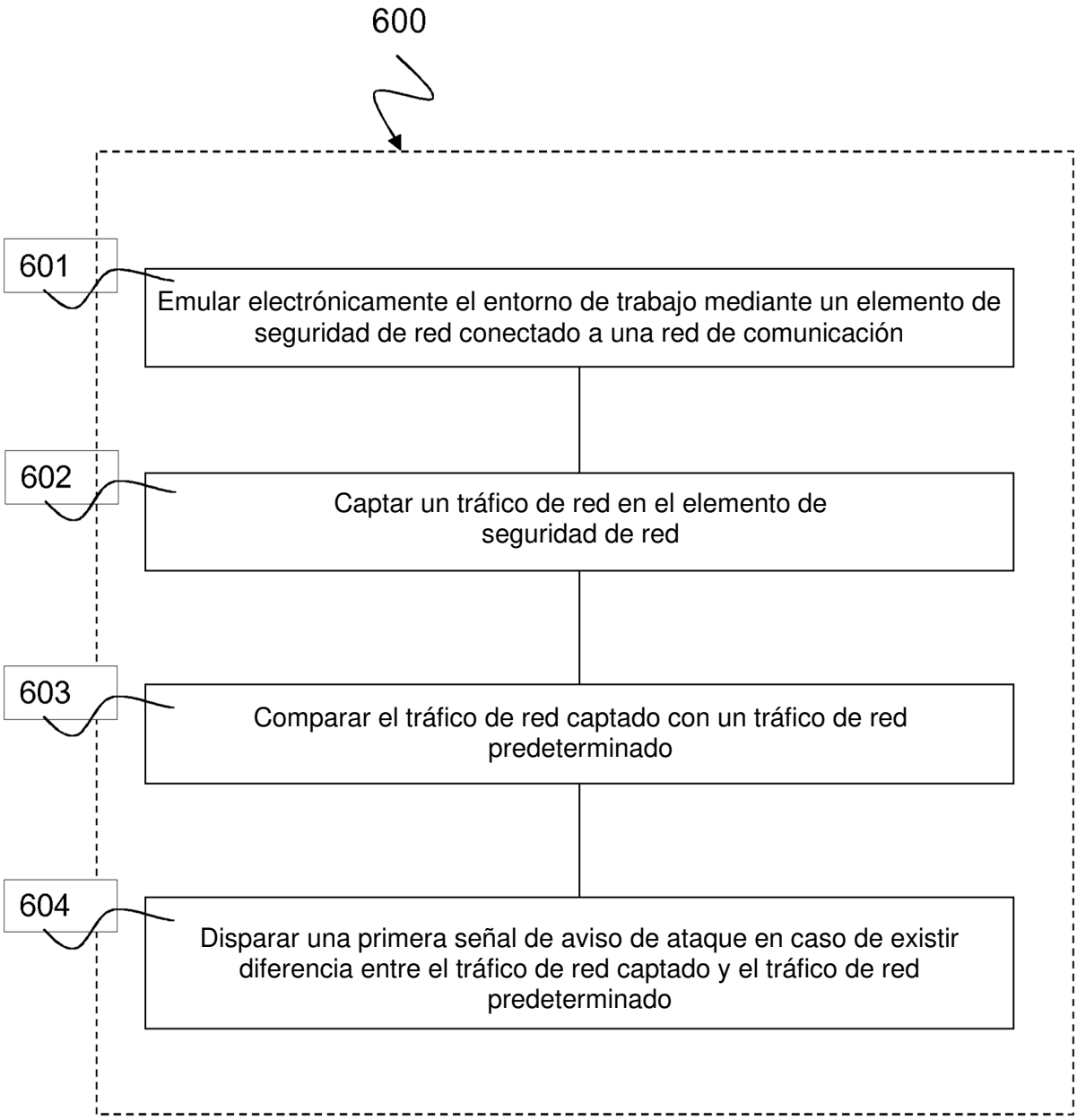
600
601
Emular electrónicamente el entorno de trabajo mediante un elemento de seguridad de red conectado a una red de comunicación
602
Captar un tráfico de red en el elemento de seguridad de red
603
Comparar el tráfico de red captado con un tráfico de red predeterminado
604
Disparar una primera señal de aviso de ataque en caso de existir diferencia entre el tráfico de red captado y el tráfico de red predeterminado

Fig. 6