(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 774 258**

(51) Int. CI.:

H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **05.09.2012 E 12183114 (3)**

(97) Fecha y número de publicación de la concesión europea: **04.12.2019 EP 2568681**

(54) Título: **Equipo de comunicación en red para la comunicación a través de una red de comunicación**

(30) Prioridad:

07.09.2011 DE 102011082237

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
20.07.2020

(73) Titular/es:

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

(72) Inventor/es:

KÖNIGSHOFEN, THOMAS;
PEUSQUENS, DR., RÜDIGER y
SCHUSTER, ANDREAS

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Equipo de comunicación en red para la comunicación a través de una red de comunicación

Campo técnico

La presente invención se refiere a un sistema y un procedimiento en el campo de la detección de ataques en una red de comunicación, así como a un equipo de comunicación en red para este fin.

Antecedentes de la técnica

Las redes de comunicación modernas están expuestas a un gran número de fuentes de peligros, cuya eliminación es de una importancia decisiva para la comunicación segura.

Una de las fuentes de peligros conocidas son las, así llamadas, *botnets* (redes de ordenadores esclavos), que se forman mediante un grupo de robots de *software* controlados por medio de un servidor de mando de *botnet*. Los robots se ejecutan habitualmente en ordenadores en red y utilizan sus recursos de comunicación.

Sin embargo, un problema en un ataque de una *botnet* es que éste no puede ser detectado con seguridad por los cortafuegos (*firewalls*) conocidos.

La escritura de declaración US 2010/202299 A1 muestra una arquitectura de vigilancia de red que comprende un servidor de análisis y una tarjeta de red que comprende varios sensores.

La escritura de declaración US 2010/115621 A1 muestra un sistema de detección para detectar contenido nocivo en una red de comunicación.

La escritura de declaración US 2010/050260 A1 muestra un dispositivo para determinar un ataque en una red de comunicación.

La escritura de declaración US 2011/154492 A1 muestra un procedimiento de filtrado para una red de comunicación.

La publicación Rehak M. et al.: “Adaptive Multiagent System for Network Traffic Monitoring” muestra un sistema de vigilancia de tráfico de red.

La publicación Zseby Fraunhofer Fokus M. Molina Dante N. Duffield AT (oeb_entity_ampersand) AMP T. et al.: "Sampling and filtering techniques for IP packet selection"; RFC 5475.txt" muestra un procedimiento de filtrado para paquetes IP.

Compendio

Por lo tanto, el objetivo de la presente invención es crear un sistema, un procedimiento y un equipo de comunicación en red para detectar ataques en una red de comunicación, en particular para detectar ataques de *botnet*.

Este objetivo se logra mediante las características de las reivindicaciones independientes. La descripción, los dibujos y las reivindicaciones dependientes tienen por objeto formas de realización ventajosas de la invención.

La presente invención se basa en el conocimiento de que el objetivo antes indicado puede lograrse mediante la observación de un comportamiento de un equipo de comunicación en red, por ejemplo de un CPE (CPE: *Consumer Premises Equipment*), en particular de un encaminador (*router*) o de otro equipo de acceso. Con este fin, el equipo de comunicación en red puede registrar estadísticamente el perfil de comunicación de un usuario y, sobre esta base, reconocer una desviación del perfil de comunicación registrado que indique un ataque de *botnet*. La desviación puede ser un parámetro de comunicación inesperado, como por ejemplo una tasa de datos de envío, que sea diferente de los parámetros de comunicación utilizados habitualmente. El parámetro de comunicación inesperado puede transmitirse como mensaje a una entidad de red, que por ejemplo puede ser un elemento de un sistema de reconocimiento de uso indebido. Si se acumulan mensajes del mismo tipo, es decir, mensajes que se refieran al mismo parámetro de comunicación, la entidad de red puede generar un mensaje de aviso que indique por ejemplo un ataque de *botnet*. Este mensaje de aviso puede enviarse a un centro de seguridad y ser evaluado en éste automáticamente o por personal especializado.

Según un primer aspecto, la invención se refiere a un equipo de comunicación en red para la comunicación a través de una red de comunicación, con un procesador que está configurado para registrar un valor actual de un parámetro de comunicación de la comunicación a través de la red de comunicación y determinar una desviación del valor actual del parámetro de comunicación con respecto a un valor medio del parámetro de comunicación; y con una interfaz de red que está configurada para transmitir el valor actual del parámetro de comunicación a través de la red de comunicación en caso de una desviación del valor actual del parámetro de comunicación con respecto al valor medio del parámetro de comunicación.

El procesador está preferiblemente preparado por técnica de programación para determinar el valor actual del parámetro de comunicación, así como la desviación. Sin embargo, según una forma de realización, el procesador puede estar cableado y presentarse por ejemplo en forma de un circuito integrado de aplicación específica.

La interfaz de red puede ser una interfaz de red inalámbrica o una interfaz de red alámbrica. Si la interfaz de red es una interfaz de red inalámbrica, ésta puede comunicarse según un estándar de comunicación inalámbrica, por ejemplo según DLAN, Bluetooth, GSM, UMTS o LTE. Si la interfaz de red es alámbrica, ésta puede comunicarse según un estándar de comunicación alámbrica, como DSL. La interfaz de red puede estar configurada para transmitir el valor actual del parámetro de comunicación a una dirección de comunicación predeterminada, en la que pueda contactarse por ejemplo con una entidad de red.

El procesador puede estar configurado para determinar la desviación sobre la base de una comparación del valor actual con el valor medio.

Según una forma de realización, la invención se refiere al equipo de comunicación en red en donde el procesador está configurado para ordenar a la interfaz de red que transmita el valor actual del parámetro de comunicación sólo si la desviación o el valor actual del parámetro de comunicación alcanzan un valor umbral predeterminado.

El valor actual del parámetro de comunicación se transmite preferiblemente sólo si éste o si la desviación sobrepasan o no llegan a un valor umbral predeterminado.

Según una forma de realización, la invención se refiere al equipo de comunicación en red en donde el procesador está configurado para determinar el valor umbral predeterminado en función del valor medio del parámetro de comunicación. El valor umbral predeterminado puede divergir del valor medio por ejemplo en un 5%, un 10% y un 50% o un 100%.

Según una forma de realización, la invención se refiere al equipo de comunicación en red en donde la interfaz de red está configurada para transmitir el parámetro de comunicación mediante uno de los protocolos de comunicación siguientes: *Internet Protocol, Internet Protocol Flow Information Export Protocol, User Datagram Protocol, Transmission Control Protocol*.

Según una forma de realización, la invención se refiere al equipo de comunicación en red en donde el procesador está configurado para registrar el valor actual del parámetro de comunicación dentro de un intervalo de tiempo de observación predeterminado. El intervalo de tiempo de observación puede ser por ejemplo de 1 segundo, 2 segundos, 5 segundos, 10 segundos, 30 segundos, 1 minuto, 2 minutos, 5 minutos o 10 minutos. El intervalo de tiempo de observación puede también ser móvil.

Según una forma de realización, la invención se refiere al equipo de comunicación en red en donde el parámetro de comunicación es al menos uno de los parámetros de comunicación siguientes: volumen de datos recibido por el equipo del cliente, volumen de datos transmitido por el equipo del cliente, relación entre el volumen de datos recibido por el equipo del cliente y un volumen de datos transmitido por el equipo del cliente, caudal de datos, tasa de datos de envío, tasa de datos de recepción, relación entre tasa de datos de envío y tasa de datos de recepción, cantidad de paquetes de envío, cantidad de paquetes de recepción, tamaño de un paquete de envío, tamaño de un paquete de recepción, momento inicial y momento final de un flujo de información, dirección de destino, en particular una dirección de destino IPv4 o IPv6, dirección de origen, en particular una dirección de origen IPv4 o IPv6, ubicación geográfica de una dirección de destino, ubicación geográfica de una dirección de origen, puerto de origen para un protocolo de comunicación, puerto de destino para un protocolo de comunicación.

Según una forma de realización, la invención se refiere al equipo de comunicación en red en donde el procesador está configurado para determinar el valor medio del parámetro de comunicación mediante una promediación de valores del parámetro de comunicación, en particular mediante una promediación móvil, o mediante la determinación de una frecuencia media, en particular de una frecuencia media de un valor de un parámetro de comunicación, o la determinación de una varianza media de los valores del parámetro de comunicación.

Según una forma de realización, la invención se refiere al equipo de comunicación en red en donde el valor medio del parámetro de comunicación es al menos uno de los valores medios siguientes: volumen de datos medio recibido por el equipo del cliente, volumen de datos medio transmitido por el equipo del cliente, relación entre un volumen de datos medio recibido por el equipo del cliente y un volumen de datos medio transmitido por el equipo del cliente, caudal de datos medio, tasa media de datos de envío, tasa media de datos de recepción, relación media entre tasa de datos de envío y tasa de datos de recepción, cantidad media de paquetes de envío, cantidad media de paquetes de recepción, tamaño medio de un paquete de envío, tamaño medio de un paquete de recepción, momento inicial medio y momento final medio de un flujo de información, frecuencia de una dirección de destino, en particular de una dirección de destino IPv4 o IPv6, frecuencia de una dirección de origen, en particular de una dirección de origen IPv4 o IPv6, ubicación geográfica media de una dirección de destino, ubicación geográfica media de una dirección de origen, frecuencia de un puerto de origen para un protocolo de comunicación, frecuencia de un puerto de destino para un protocolo de comunicación.

Según una forma de realización, la invención se refiere al equipo de comunicación en red en donde la interfaz de red está configurada para recibir una descripción de filtro a través de la red de comunicación en respuesta a la transmisión del parámetro de comunicación y en donde el procesador está configurado para, según la descripción de filtro, bloquear un enlace de comunicación a una dirección de red predeterminada.

La descripción de filtro puede por ejemplo comprender una dirección de destino que haya de bloquearse.

Según una forma de realización, la invención se refiere al equipo de comunicación en red en donde el procesador está configurado para generar un mensaje, que pueda mostrarse a un usuario del equipo de comunicación en red, sobre el bloqueo del enlace de comunicación a la dirección de red predeterminada.

El mensaje mostrable puede presentarse por ejemplo en forma de una página web depositada en una dirección de red predeterminada.

Según una forma de realización, la invención se refiere al equipo de comunicación en red en donde el procesador está configurado para implementar un resolutor de sistema de nombres de dominio (*Domain Name System Resolver*), comprendiendo el resolutor de sistema de nombres de dominio una lista de filtros, en particular una lista de filtros configurable, con al menos un criterio de filtrado.

La lista de filtros puede por ejemplo ser transmitida al equipo de comunicación en red por una entidad de red remota.

Según una forma de realización, la invención se refiere al equipo de comunicación en red en donde el resolutor de sistema de nombres de dominio está configurado para, en respuesta a una petición de emitir para un alias una dirección de red asignada al alias, emitir una dirección de red predeterminada en lugar de la dirección de red asignada al alias cuando el alias corresponda a un criterio de filtrado de la lista de filtros.

De este modo se impide la resolución del alias, existiendo la posibilidad de que en la dirección de red predeterminada pueda llamarse una página web que indique que se ha impedido la resolución del alias.

Según una forma de realización, la invención se refiere al equipo de comunicación en red en donde el criterio de filtrado comprende una coincidencia al menos parcial de un alias con una descripción de filtro.

En la descripción de filtro pueden por ejemplo mencionarse varios alias cuya resolución haya de impedirse.

Según una forma de realización, la invención se refiere al equipo de comunicación en red que es un encaminador de red.

Según una forma de realización, la invención se refiere al equipo de comunicación en red que está preparado por técnica de programación.

Con este fin, el equipo de comunicación en red puede comprender una memoria con un programa informático depositado en la misma, al que pueda acceder el procesador.

Según otro aspecto, la invención se refiere a un procedimiento para la comunicación a través de una red de comunicación, con: registro de un valor actual de un parámetro de comunicación de la comunicación a través de la red de comunicación, determinación de una desviación del valor actual del parámetro de comunicación con respecto a un valor medio del parámetro de comunicación y transmisión del valor actual del parámetro de comunicación a través de la red de comunicación en caso de una desviación del valor actual del parámetro de comunicación con respecto al valor medio del parámetro de comunicación.

De la funcionalidad del equipo de comunicación en red, en particular de la funcionalidad de al menos uno de los elementos del equipo de comunicación en red, resultan directamente otras características del procedimiento.

Según otro aspecto, la invención se refiere al sistema de red que comprende una entidad de red que está configurada para recibir al menos un valor actual de un parámetro de comunicación de al menos un equipo de comunicación en red según la invención, y evaluar el valor actual del parámetro de comunicación por medio de un criterio mensurable para averiguar si el valor actual del parámetro de comunicación indica un comportamiento de comunicación inesperado del equipo de comunicación en red, estando el procesador configurado además para emitir un mensaje de aviso en caso de que exista un comportamiento de comunicación inesperado del equipo de comunicación en red.

Según una forma de realización, la invención se refiere al sistema de red en donde el criterio mensurable comprende al menos unas de las indicaciones siguientes: indicación sobre una distribución temporal de una presencia del valor del parámetro de comunicación, una indicación sobre una probabilidad de una presencia del valor del parámetro de comunicación, una indicación sobre la acumulación de los valores del parámetro de comunicación dentro de un intervalo de tiempo.

Según una forma de realización, la invención se refiere al sistema de red en donde la entidad de red está configurada además para transmitir un mensaje de aviso a un centro de seguridad a través de la red de comunicación.

Según una forma de realización, la invención se refiere al sistema de red que además comprende un servidor de agregación, que está configurado para agregar una pluralidad de valores del mismo género del parámetro de comunicación y transmitir a la entidad de red la pluralidad de parámetros de comunicación agregados.

Según una forma de realización, la invención se refiere al sistema de red que además comprende el equipo de comunicación en red según la invención y un centro de seguridad, estando el centro de seguridad configurado para recibir el mensaje de aviso de la entidad de red y, en respuesta a la recepción del mensaje de aviso, transmitir una descripción de filtro al equipo de comunicación en red y estando el equipo de comunicación en red configurado para, según la descripción de filtro, bloquear un enlace de comunicación.

Según otro aspecto, la invención se refiere a un programa informático para realizar al menos uno de los procedimientos según la invención en un ordenador.

La invención puede realizarse en *software* y/o en *hardware*.

Descripción de las figuras

Con referencia a los dibujos adjuntos se explican más detalladamente otros ejemplos de realización. Se muestran:

Figura 1 un sistema de red según una forma de realización;

Figura 2 un sistema de red según una forma de realización;

Figura 3 un diagrama de bloques de un equipo de comunicación en red según una forma de realización;

Figura 4 un diagrama de bloques de un equipo de comunicación en red según una forma de realización; y

Figura 5 un diagrama de operaciones de un procedimiento para la comunicación a través de una red de comunicación según una forma de realización.

Descripción detallada

La Figura 1 muestra un sistema de red con una pluralidad de equipos 101 de comunicación en red, así como con una entidad 103 de red. El escenario de red representado en la Figura 1 ilustra un ataque de *botnet* utilizando un servidor 105 de mando de *botnet* representado a modo ejemplo en la Figura 1.

Los equipos 101 de comunicación en red pueden ser encaminadores de red. Los equipos 101 de comunicación en red envían según un esquema de comunicación usual por ejemplo datos a unos destinos 107 usuales, para por ejemplo llamar contenidos web de una revista *online*.

Sin embargo, en caso de un ataque de *botnet*, los equipos 101 de comunicación en red se comportan de forma anómala, desviándose del esquema de comunicación usual, y envían por ejemplo datos al servidor 105 de mando de *botnet* representado a modo de ejemplo en la Figura 1. Esta desviación puede reconocerse en forma de un parámetro de comunicación actual diferente de los parámetros de comunicación utilizados usualmente. El parámetro de comunicación actual diferente puede por ejemplo ser una dirección de destino diferente o un volumen de datos de envío elevado.

Los equipos 101 de comunicación en red pueden determinar esta desviación del valor actual del parámetro de comunicación con respecto a un valor medio del parámetro de comunicación y enviarla por ejemplo de forma anónima a una entidad 103 de red, que transmite un mensaje de aviso por ejemplo a un centro 109 de seguridad.

La Figura 2 muestra un sistema de red según una forma de realización con los equipos 101 de comunicación en red, así como con la entidad 103 de red. Entre los equipos 101 de comunicación en red y la entidad 103 de red se halla un servidor 201 de agregación, que está configurado para agregar una pluralidad de valores umbral del mismo género de un parámetro de comunicación y transmitirlos a la entidad 103 de red. La entidad 103 de red constituye, según una forma de realización, un servidor de correlación.

Opcionalmente, el sistema de red representado en la Figura 2 puede comprender un servidor 203 de autoconfiguración (ACS, por sus siglas en inglés). El ACS 203 puede ser un componente dentro de una red de banda ancha explotada por un proveedor de servicios de Internet y comunicarse mediante el protocolo TR-069. Con este fin, el ACS 203 puede aceptar de los equipos 101 de comunicación en red por ejemplo mensajes de estado, que comprendan los valores del parámetro de comunicación actual respectivo, así como opcionalmente actualizar un *firmware* y repartir datos de configuración a los equipos 101 de comunicación en red. Según una forma de realización, el ACS 203 sirve de interfaz entre los equipos 101 de comunicación en red y el servidor 201 de agregación.

Según una forma de realización, el ACS 203 puede realizar un colector de flujo (*Flow Collector*) en el sentido de RFC 5101. La transmisión del flujo puede realizarse periódicamente por ejemplo cada 60 minutos, pudiendo por ejemplo un proveedor de servicios configurar un intervalo diferente. Además, los flujos pueden transmitirse en los casos siguientes:

- cuando la memoria de trabajo disponible en un equipo 101 de comunicación en red para el almacenamiento intermedio de flujos esté utilizada en más de un 90%

- cuando el proveedor de servicios inicie una transmisión mediante el ACS 203

- en los casos previstos según el protocolo TR-069

Según una forma de realización, la transmisión de los datos al ACS 203 se realiza según RFC 5101 y 5102, sirviendo TR-069 de protocolo de transporte.

Según una forma de realización, el ACS 203 elimina toda información sobre la procedencia del registro de flujo (*Flow Record*) y transmite éste a un servidor 201 de agregación. Habitualmente, un servidor 201 de agregación da servicio a un gran número de equipos 101 de comunicación en red adyacentes por lo que se refiere a la topología de red, por ejemplo todos los equipos de comunicación en red de un PoP de banda ancha.

Los equipos 101 de comunicación en red pueden transmitir los valores del parámetro de comunicación actual por ejemplo utilizando flujos según las normas RFC5101, 5102 y 5470. Según una forma de realización, el ACS 203 puede comprobar la autorización del equipo 101 de comunicación en red respectivo para la entrega de tales flujos. Según una forma de realización, el ACS 203 puede eliminar referencias al equipo 101 de comunicación en red que entrega el flujo respectivo, como por ejemplo una identificación de acceso.

Según una forma de realización, el servidor 201 de agregación acepta flujos del ACS 203, los comprime y transmite los datos resultantes al servidor 103 de correlación, que puede almacenarlos en una base de datos. El servidor 103 de correlación puede recibir datos de una pluralidad de servidores 201 de agregación, como se indica en la Figura 2. Según una forma de realización, el servidor 201 de agregación está asignado al ACS 203. Según una forma de realización, el servidor 201 de agregación da servicio a un PoP de banda ancha y, por lo tanto, a varios equipos 101 de comunicación en red adyacentes por lo que se refiere a la topología de red.

Según una forma de realización, el servidor 201 de agregación almacena en una memoria intermedia los flujos antes mencionados durante un lapso de tiempo predeterminado, que por ejemplo puede ser de 5 minutos y ser configurable. Los valores idénticos o similares de un parámetro de comunicación que se reciban varias veces durante este lapso de tiempo, que se diferencien por ejemplo en un puerto de origen o un puerto de destino, se reúnen, añadiéndose a los mensajes reunidos, según una forma de realización, una indicación sobre la cantidad de mensajes individuales con los que se transmiten los valores del parámetro de comunicación.

Según una forma de realización, el servidor 201 de agregación transmite de manera continua al servidor 103 de correlación los flujos reunidos.

Los datos pueden examinarse en cuanto a fluctuaciones en la frecuencia de aparición de una de las características registradas en los flujos. Además, para el conjunto de datos respectivamente actual se calculan correlaciones entre las características.

Según una forma de realización, el servidor 103 de correlación calcula de manera continua, por ejemplo, tendencias para la correlación entre los valores comunicados de uno o varios parámetros de comunicación. En este contexto pueden registrarse por ejemplo una inversión de signo, que por ejemplo puede ocurrir en caso de invertirse una relación entre el volumen de datos de envío y el volumen de datos de recepción, un gran aumento o una disminución de una correlación. Según una forma de realización, los resultados pueden visualizarse y/o transmitirse al centro 109 de seguridad. Según una forma de realización, los datos pueden borrarse de la base de datos del servidor 103 de correlación una vez transcurrido un lapso de tiempo por ejemplo configurable.

Según una forma de realización, el centro 109 de seguridad está previsto para llevar a cabo el control de la distribución del *firmware* utilizable para una detección de anomalías, que puede comprender por ejemplo descripciones de filtros, y su actualización.

Según una forma de realización, el control de la agregación de los flujos de los equipos 101 de comunicación en red, incluida la parametrización de componentes de *hardware* y *software* configurables de los equipos 101 de comunicación en red, puede ser llevado a cabo también por el centro 109 de seguridad. En este contexto pueden implementarse por ejemplo reglas de filtrado. Según otra forma de realización, el centro 109 de seguridad puede llevar a cabo el control de la agregación, llevar a cabo el control de la detección de anomalías en una zona del proveedor de servicios de Internet, incluyendo una adaptación continua de los procedimientos para la detección de una anomalía, es decir, de una desviación anómala de un valor de un parámetro de comunicación con respecto a un valor medio del parámetro de comunicación, a modelos de comunicación cambiantes de las *botnets*, llevar a cabo una verificación de mensajes de aviso o alarmas, efectuar una conversión de las alarmas en listas de filtros, efectuar un aseguramiento de la calidad de las listas de filtros, encargarse de un control de una distribución de las listas de filtros a los equipos 101 de comunicación en red.

Tras un tiempo configurable por un proveedor de servicios, los flujos pueden borrarse del conjunto de datos del servidor de correlación. Si cambian las frecuencias o las correlaciones más allá de unos valores umbral respectivamente configurables, se genera una alarma.

Las alarmas pueden ser examinadas o automáticamente o por miembros expertos del personal en un centro de operaciones de seguridad (*Security Operating Center* (SOC)). Con este fin pueden examinarse los flujos que se hallen en el conjunto de datos. Un ejemplo de búsqueda es: lista con dirección IP y puerto de todos los flujos con el protocolo IP TCP, un puerto > 50000, una duración >= 3σ y una tasa de transmisión de datos <= 3σ.

Si la comprobación de la alarma por parte de un usuario o un miembro del personal del centro 109 de seguridad confirma la sospecha de una actividad maliciosa, un usuario o un miembro del personal del centro 109 de seguridad genera una o más reglas de filtrado como defensa. Según una forma de realización, las reglas de filtrado se transmiten al ACS 203 y desde éste, mediante TR-069, al CPE. La transmisión es realizada usualmente a continuación de la transmisión de los flujos por el equipo 101 de comunicación en red o en los casos mencionados en TR-069. Además, el proveedor de servicios puede iniciar una transmisión, como está previsto en la norma TR-069.

La Figura 3 muestra un diagrama de bloques de un equipo 300 de comunicación en red según una forma de realización. El equipo 300 de comunicación en red comprende un procesador 301, que está configurado para registrar un valor actual de un parámetro de comunicación de la comunicación del equipo de comunicación en red a través de una red de comunicación y determinar una desviación del valor actual del parámetro de comunicación del tipo anteriormente mencionado con respecto a un valor medio del parámetro de comunicación. El equipo de comunicación en red comprende además una interfaz 303 de red, que está configurada para transmitir el valor actual del parámetro de comunicación a través de la red de comunicación, por ejemplo a una dirección de comunicación predeterminada, en caso de una desviación del valor actual del parámetro de comunicación con respecto al valor medio del parámetro de comunicación.

La Figura 4 muestra un diagrama de bloques de un equipo 400 de comunicación en red según una forma de realización con un servidor HTTP 401 para la configuración y la información de bloqueo, que puede presentarse en forma de un filtro o de una descripción de filtro, con un encaminador 403 para tareas de encaminamiento, que está conectado a un dispositivo 405 de detección de anomalías. Además, está previsto un resolutor 407 de DNS, que también se comunica con el dispositivo 405 de detección de anomalías.

El dispositivo 405 de detección de anomalías puede estar configurado por ejemplo para detectar una desviación de un valor actual de un parámetro de comunicación con respecto a un valor medio del parámetro de comunicación y ordenar a la interfaz 409 de red que transmita un valor actual del parámetro de comunicación a través de una red de comunicación. Opcionalmente está previsto un cortafuegos 411.

La interfaz 409 de red puede estar configurada para comunicarse mediante una red WAN (WAN: *Wide Area Network*). En el lado del usuario o de la intranet, el equipo de comunicación en red puede presentar por ejemplo una interfaz inalámbrica (WiFi) o una interfaz alámbrica (LAN: *Local Area Network*).

Los dispositivos 401, 403, 405, 407 y 411 pueden realizarse mediante un procesador, por ejemplo mediante el procesador 301 representado en la Figura 3, en el que se ejecute un *firmware* que implemente los dispositivos 401, 403, 405, 407 y 411.

El equipo 400 de comunicación en red está dispuesto preferiblemente en la zona de influencia de un cliente y, según una forma de realización, forma un CPE con dos interfaces de red: una interfaz de red de cliente para la comunicación por WiFi o LAN y la interfaz 409 WAN hacia Internet para la comunicación por WAN. La transmisión de paquetes de datos entre estas interfaces y en caso dado la modificación de los paquetes en el curso de la transmisión pueden realizarse mediante *hardware*, que esté controlado mediante un *software*, por ejemplo mediante el *firmware* antes mencionado.

El equipo 400 de comunicación en red está previsto preferiblemente para realizar la transmisión de datos entre el ISP (proveedor de servicios de Internet) y la red local o las redes locales del cliente.

El *firmware* puede realizar el cortafuegos 411, que, basándose en la dirección IPv4/IPv6 remota, el protocolo IP y, en el caso de los protocolos IP UDP y TCP, también el puerto, impide o permite la comunicación según reglas configurables por el ISP. Siempre que se impida la comunicación, el cortafuegos 411 envía un mensaje ICMP (protocolo de mensajes de control de Internet) según RFC 792 con el código 10 según RFC 1122 al equipo en red que inicia la comunicación en la red del cliente.

El *firmware* puede además realizar el servidor HTTP 401, que, mediante el protocolo de transferencia de hipertexto (*Hypertext Transfer Protocol* (HTTP, véase RFC 2068)), presenta al usuario información de estado y acepta cambios de configuración.

El *firmware* puede además realizar el resolutor 407 de DNS, que determina la dirección IP correspondiente para nombres de dominio incompletos y completamente calificados. Los resultados pueden almacenarse en una memoria de trabajo del equipo 400 de comunicación en red. El resolutor 407 de DNS desecha una entrada cuando ha de

conseguir espacio de memoria para un nuevo juego de datos. Con este fin, el resolutor 407 de DNS lleva una lista ordenada según el tiempo transcurrido desde la última llamada (*Most Recently Used List*, MRU). El resolutor 407 de DNS desecha una entrada también cuando se alcanza el tiempo de vida (*Time To Live*, TTL) fijado por el servidor de nombre respondedor sin que se haya llamado de nuevo el juego de datos. Según una forma de realización, el intervalo en el que el resolutor 407 de DNS comprueba un juego de datos durante su tiempo de vida es configurable, en particular es configurable por un proveedor de servicios.

Según una forma de realización, el resolutor 407 de DNS comprende una lista de filtros configurable. Si el alias completamente calificado consultado corresponde a un criterio de filtrado, el resolutor 407 de DNS interrumpe la resolución de nombre y responde con una dirección IP fija, por ejemplo dependiente de la instalación, en la red del cliente. Bajo esta dirección IP y el puerto estándar para HTTP (80/tcp), un servidor web del equipo 400 de comunicación en red puede emitir mediante el protocolo de transferencia de hipertexto una página web que informe del hecho y del motivo del bloqueo. Toda comunicación de otro tipo dirigida a esta dirección puede responderse con el código ICMP 10 (“host administratively prohibited”), véase RFC 792 y 1122.

Según una forma de realización, el *firmware* amplía el equipo 400 de comunicación en red en la capacidad para crear y transmitir flujos según RFC 5101, 5102 y 5470. El *firmware* puede por ejemplo comunicar sólo valores de un parámetro de comunicación detectados como nuevos o modificados en un intervalo de observación.

Para la detección de anomalías en una capa de transporte, el equipo 300, 400 de comunicación en red puede utilizar un *Observation Point* (punto de observación) en el sentido de RFC 5101 como interfaz del lado del ISP para la capa de transporte OSI. Según una forma de realización, es posible medir y reunir en flujos valores de los siguientes parámetros de comunicación:

- dirección de origen IPv4/IPv6

- dirección de destino IPv4/IPv6

- puerto de origen para los protocolos IP UDP y TCP

- puerto de destino para los protocolos IP UDP y TCP

- protocolo IP

- volumen de datos, separado según sentido

- cantidad de paquetes, separada según sentido

- momento inicial y final del flujo, medido por ejemplo en milisegundos desde la última inicialización del equipo 300, 400 de comunicación en red.

Según una forma de realización, la comunicación de datos dentro de la red del lado del cliente no se tiene en cuenta. Sin embargo, según una forma de realización, el ISP puede configurar excepciones adicionales, para por ejemplo asegurar la comunicación con los servidores de entrada de correo explotados por el ISP.

Según una forma de realización, el equipo 300, 400 de comunicación en red, en particular su procesador 301, calcula, por protocolo IP (TCP y UDP) y puerto de destino, valores medios móviles y la varianza de los siguientes parámetros de comunicación:

- relación entre volumen de datos entrante y saliente

- tamaño de paquetes de datos entrantes y salientes

- duración del flujo

- caudal de datos

Según una forma de realización, el ISP puede configurar una desviación tolerada. Si el flujo actualmente procesado está fuera del intervalo tolerado, el equipo 300, 400 de comunicación en red prepara el juego de datos para la exportación. En este contexto puede desecharse la dirección IP del flujo del lado del cliente. La dirección IP remanente se denomina “dirección remota” (*remote address*).

El ISP puede además configurar reglas adicionales que lleven a la exportación o la supresión de un flujo en la forma anteriormente descrita. Para la detección de anomalías en el servicio de nombres de dominio (*domain name service*), el resolutor 407 de DNS puede utilizar un punto de observación en el sentido de RFC 5101. Según una forma de realización pueden medirse valores de los siguientes parámetros de comunicación:

- nombre de anfitrión completamente calificado

- dirección IPv4/IPv6

- duración de la validez de la asignación (*Time To Live*, TTL)

- dirección IPv4/IPv6 del servidor de nombre del que se ha obtenido la respuesta

Según una forma de realización, el punto de observación en el sentido de RFC 5101 es el equipo 300, 400 de comunicación en red mismo.

Según una forma de realización pueden prepararse para la exportación nuevos juegos de datos incluidos en una memoria intermedia opcional del resolutor 407 de DNS o juegos de datos actualizados durante su tiempo de vida.

La Figura 5 muestra un diagrama de operaciones de un procedimiento para la comunicación a través de una red de comunicación con el registro 501 de un valor actual de un parámetro de comunicación de la comunicación a través de la red de comunicación, la determinación 503 de una desviación del valor actual del parámetro de comunicación con respecto a un valor medio del parámetro de comunicación, y la transmisión 505 del valor actual del parámetro de comunicación a través de la red de comunicación, por ejemplo a una dirección de comunicación predeterminada, en caso de una desviación del valor actual del parámetro de comunicación con respecto al valor medio del parámetro de comunicación.

El procedimiento representado en la Figura 5 puede realizarse por ejemplo mediante el equipo 300 de comunicación en red representado en la Figura 3 y/o en la Figura 4.

Según una forma de realización, un cliente puede aprobar la detección de anomalías y el filtrado por ejemplo encargando o modificando la configuración de los componentes de red y/o los programas de aplicación del equipo 300, 400 de comunicación en red. El primer nivel de la detección de anomalías se realiza por ejemplo de forma descentralizada y en el lado del cliente, para poder llevar a cabo la carga de cálculo y almacenamiento, así como para comprimir y anonimizar datos y por lo tanto seguir el principio de la minimización de datos. La conversión de la comunicación de anomalías en un filtro se realiza por ejemplo de forma desplazada en el tiempo y tras una comprobación por parte de un experto. Así pues, el cliente, o sea, el usuario del equipo 101, 300, 400 de comunicación en red, puede activar o desactivar la detección de anomalías. En este contexto, el usuario del equipo 300, 400 de comunicación en red puede activar o desactivar el filtrado de la comunicación de datos basada en IP con presuntos servidores de instrucciones y control de una *botnet*. Según una forma de realización, los ajustes se aplican a todos los equipos en la red del cliente que, de forma mediada por el equipo 300, 400 de comunicación en red, se comuniquen con un punto terminal fuera de la red del cliente.

REIVINDICACIONES

1. Equipo de comunicación en red para la comunicación a través de una red de comunicación con:

un procesador (301), que está configurado para registrar un valor actual de un parámetro de comunicación de la comunicación a través de la red de comunicación y determinar una desviación del valor actual del parámetro de comunicación con respecto a un valor medio del parámetro de comunicación; y

una interfaz (303) de red, que está configurada para, en caso de una desviación del valor actual del parámetro de comunicación con respecto al valor medio del parámetro de comunicación, transmitir el valor actual del parámetro de comunicación a través de la red de comunicación a una entidad de red para evaluar el parámetro de comunicación y detectar un comportamiento de comunicación inesperado del equipo de comunicación en red, en donde el procesador (301) está configurado para ordenar a la interfaz de red que transmita el valor actual del parámetro de comunicación sólo cuando la desviación alcance un valor umbral predeterminado,

en donde el parámetro de comunicación es al menos uno de los parámetros de comunicación siguientes: volumen de datos recibido por un equipo de cliente, volumen de datos transmitido por el equipo de cliente, relación entre un volumen de datos recibido por el equipo de cliente y un volumen de datos transmitido por el equipo de cliente, caudal de datos, tasa de datos de envío, tasa de datos de recepción, relación entre tasa de datos de envío y tasa de datos de recepción, cantidad de paquetes de envío, cantidad de paquetes de recepción, tamaño de un paquete de envío, tamaño de un paquete de recepción, momento inicial y momento final de un flujo de información.

2. Equipo de comunicación en red según la reivindicación 1, en donde el procesador (301) está configurado para determinar el valor umbral predeterminado en función del valor medio del parámetro de comunicación.

3. Equipo de comunicación en red según una de las reivindicaciones precedentes, en donde la interfaz (303) de red está configurada para transmitir el parámetro de comunicación mediante uno de los protocolos de comunicación siguientes: *Internet Protocol, Internet Protocol Flow Information Export Protocol, User Datagram Protocol, Transmission Control Protocol*.

4. Equipo de comunicación en red según una de las reivindicaciones precedentes, en donde el procesador (301) está configurado para registrar el valor actual del parámetro de comunicación dentro de un intervalo de tiempo de observación predeterminado.

5. Equipo de comunicación en red según una de las reivindicaciones precedentes, en donde el procesador (301) está configurado para determinar el valor medio del parámetro de comunicación mediante una promediación de valores del parámetro de comunicación o mediante la determinación de una frecuencia media de un valor de un parámetro de comunicación o la determinación de una varianza media de los valores del parámetro de comunicación.

6. Equipo de comunicación en red según una de las reivindicaciones precedentes, en donde el valor medio del parámetro de comunicación es al menos uno de los valores medios siguientes: volumen de datos medio recibido por el equipo de cliente, volumen de datos medio transmitido por el equipo de cliente, relación entre un volumen de datos medio recibido por el equipo de cliente y un volumen de datos medio transmitido por el equipo de cliente, caudal de datos medio, tasa media de datos de envío, tasa media de datos de recepción, relación media entre tasa de datos de envío y tasa de datos de recepción, cantidad media de paquetes de envío, cantidad media de paquetes de recepción, tamaño medio de un paquete de envío, tamaño medio de un paquete de recepción, momento inicial medio y momento final medio de un flujo de información.

7. Equipo de comunicación en red según una de las reivindicaciones precedentes, en donde la interfaz (303) de red está configurada para recibir una descripción de filtro a través de la red de comunicación en respuesta a la transmisión del parámetro de comunicación y en donde el procesador (301) está configurado para, según la descripción de filtro, bloquear un enlace de comunicación a una dirección de red predeterminada.

8. Equipo de comunicación en red según la reivindicación 7, en donde el procesador (301) está configurado para generar un mensaje, que pueda mostrarse a un usuario del equipo de comunicación en red, sobre el bloqueo del enlace de comunicación a la dirección de red predeterminada.

9. Equipo de comunicación en red según una de las reivindicaciones precedentes, en donde el procesador (301) está configurado para implementar un resolutor de sistema de nombres de dominio (*Domain Name System Resolver*), comprendiendo el resolutor de sistema de nombres de dominio una lista de filtros con al menos un criterio de filtrado.

10. Equipo de comunicación en red según la reivindicación 9, en donde el resolutor de sistema de nombres de dominio está configurado para, en respuesta a una petición de emitir para un alias una dirección de red asignada al alias, emitir una dirección de red predeterminada en lugar de la dirección de red asignada al alias cuando el alias corresponda a un criterio de filtrado de la lista de filtros.

11. Equipo de comunicación en red según la reivindicación 9 o 10, en donde el criterio de filtrado comprende una coincidencia al menos parcial de un alias con una descripción de filtro.

12. Equipo de comunicación en red según una de las reivindicaciones precedentes, que es un encaminador (*router*) de red.

13. Equipo de comunicación en red según una de las reivindicaciones precedentes, en donde el procesador (301) está preparado por técnica de programación para determinar el valor actual del parámetro de comunicación, así como la desviación.

14. Procedimiento para la comunicación a través de una red de comunicación, con:

registro (501) de un valor actual de un parámetro de comunicación de la comunicación a través de la red de comunicación;

determinación (503) de una desviación del valor actual del parámetro de comunicación con respecto a un valor medio del parámetro de comunicación; y

transmisión (505) del valor actual del parámetro de comunicación a través de la red de comunicación, en caso de una desviación del valor actual del parámetro de comunicación con respecto al valor medio del parámetro de comunicación, a una entidad de red para evaluar el parámetro de comunicación y detectar un comportamiento de comunicación inesperado cuando la desviación alcanza un valor umbral predeterminado,

en donde el parámetro de comunicación es al menos uno de los parámetros de comunicación siguientes: volumen de datos recibido por un equipo de cliente, volumen de datos transmitido por el equipo de cliente, relación entre un volumen de datos recibido por el equipo de cliente y un volumen de datos transmitido por el equipo de cliente, caudal de datos, tasa de datos de envío, tasa de datos de recepción, relación entre tasa de datos de envío y tasa de datos de recepción, cantidad de paquetes de envío, cantidad de paquetes de recepción, tamaño de un paquete de envío, tamaño de un paquete de recepción, momento inicial y momento final de un flujo de información.

15. Sistema de red, que comprende una entidad (103) de red que está configurada para recibir al menos un valor actual de un parámetro de comunicación de un equipo de comunicación en red según una de las reivindicaciones 1 a 13 a través de una red de comunicación y evaluar el valor actual del parámetro de comunicación por medio de un criterio mensurable para averiguar si el valor actual del parámetro de comunicación indica un comportamiento de comunicación inesperado del equipo de comunicación en red, en donde el procesador está configurado además para emitir un mensaje de aviso en caso de que exista un comportamiento de comunicación inesperado del equipo de comunicación en red, comprendiendo el sistema de red además el equipo (101) de comunicación en red según una de las reivindicaciones 1 a 13 y un centro (109) de seguridad, estando el centro (109) de seguridad configurado para recibir el mensaje de aviso de la entidad (103) de red y, en respuesta a la recepción del mensaje de aviso, transmitir una descripción de filtro al equipo (101) de comunicación en red, y estando el equipo (101) de comunicación en red configurado para, según la descripción de filtro, bloquear un enlace de comunicación.

16. Sistema de red según la reivindicación 15, en donde el criterio mensurable comprende al menos una de las indicaciones siguientes: indicación sobre una distribución temporal de una presencia del valor del parámetro de comunicación, una indicación sobre una probabilidad de una presencia del valor del parámetro de comunicación, una indicación sobre la acumulación de los valores del parámetro de comunicación dentro de un intervalo de tiempo.

17. Sistema de red según una de las reivindicaciones 15 o 16, en donde la entidad (103) de red está configurada además para transmitir un mensaje de aviso a un centro (109) de seguridad a través de la red de comunicación.

18. Sistema de red según una de las reivindicaciones 15 a 17, que además comprende un servidor (203) de agregación, que está configurado para agregar una pluralidad de valores del mismo género del parámetro de comunicación y transmitir a la entidad (103) de red la pluralidad de parámetros de comunicación agregados.

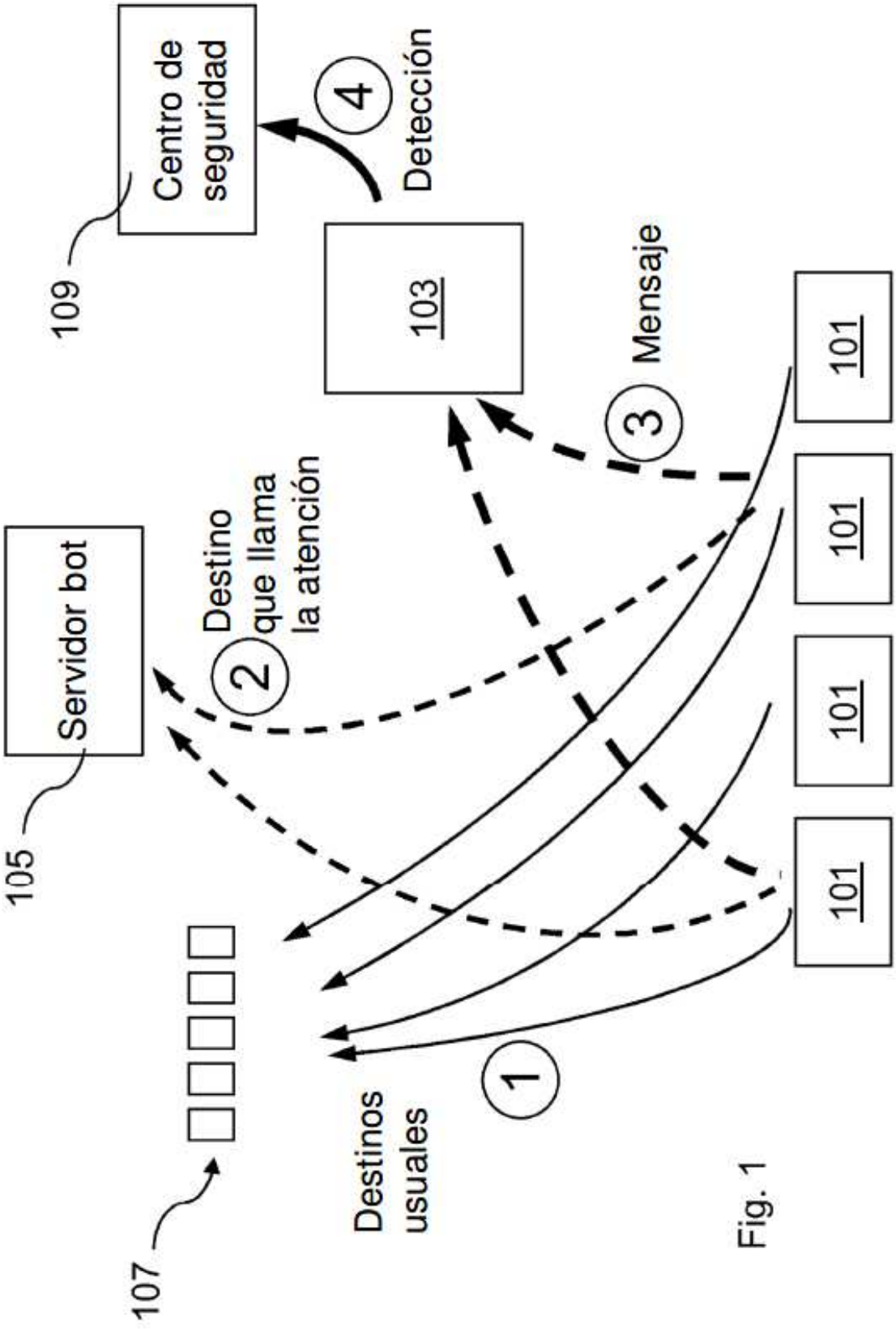
Centro de seguridad
109
4
Detección
103
Mensaje
3
Servidor bot
105
Destino que llama la atención
2
101
101
101
101
1
Destinos usuales
107

Fig. 1

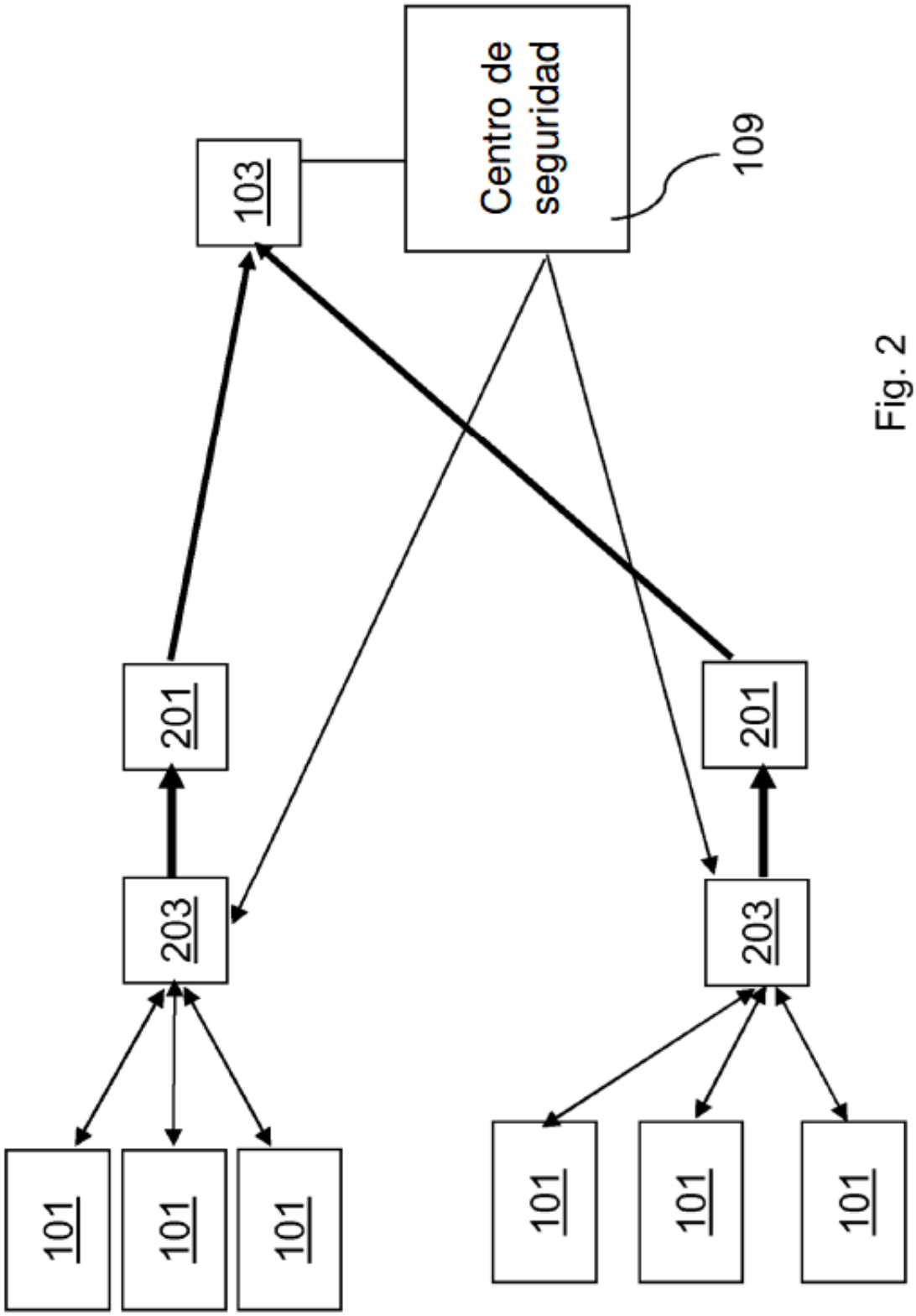
Centro de seguridad
109
103
201
201
203
203
101
101
101
101
101
101

Fig. 2

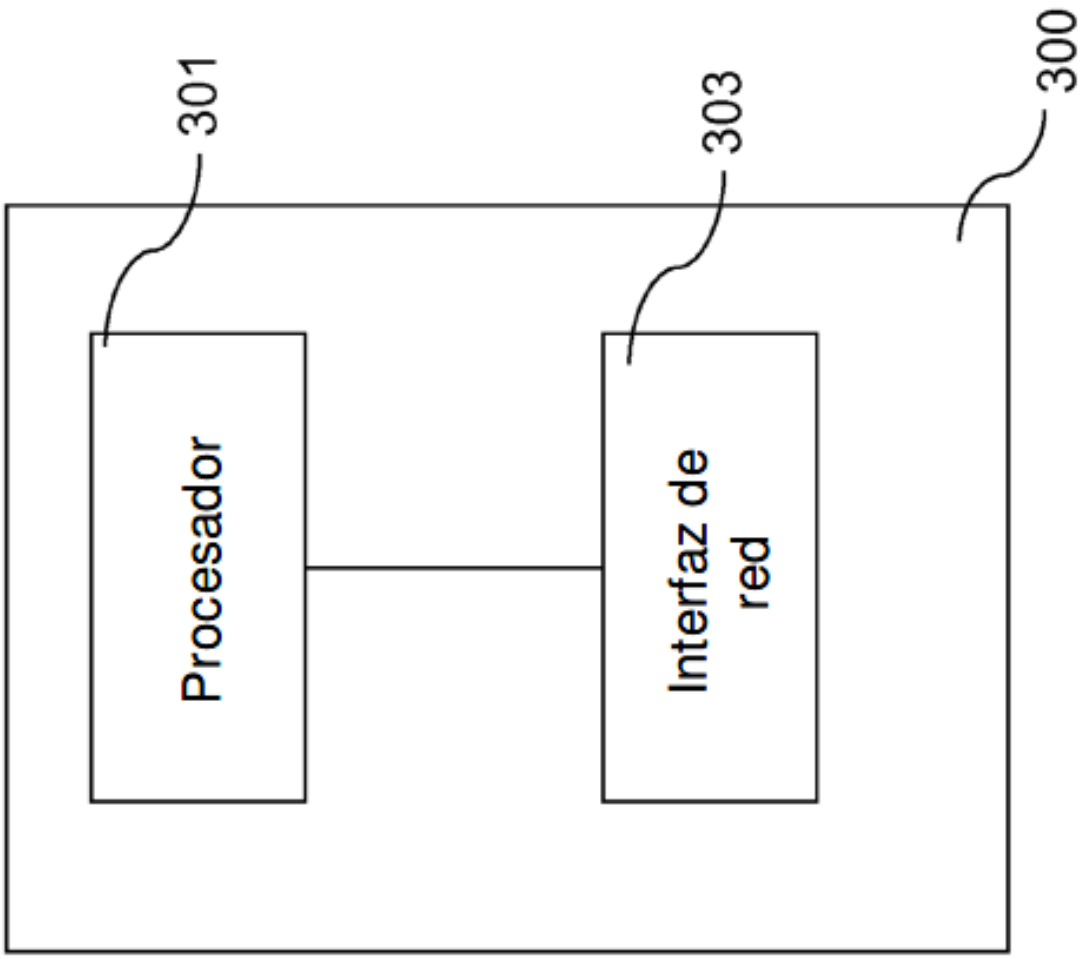

Fig. 3

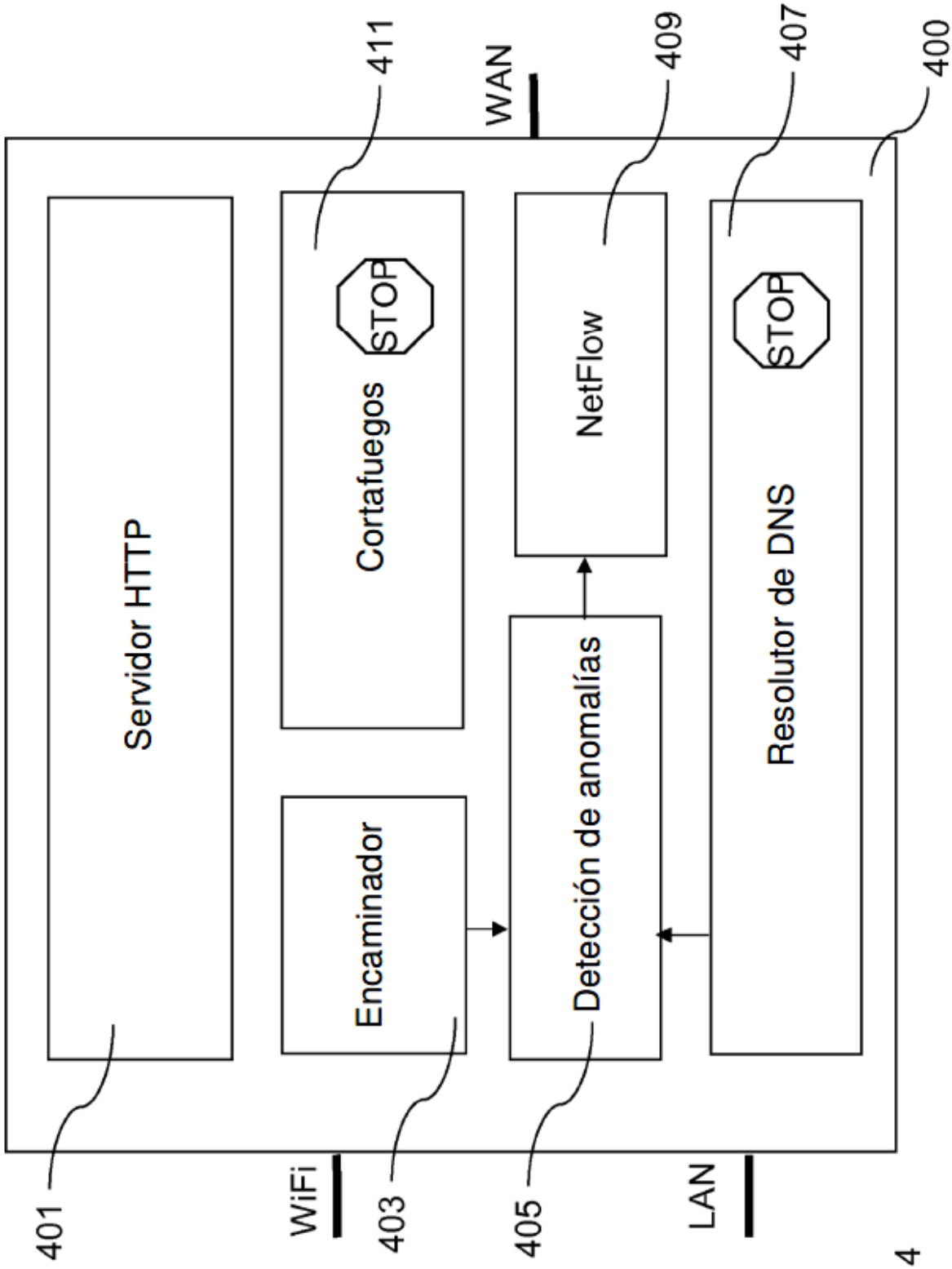
Servidor HTTP
Cortafuegos
STOP
Encaminador
NetFlow
Detección de anomalías
Resolutor de DNS
STOP
WAN
WiFi
LAN
401
403
405
407
409
411
400

Fig. 4

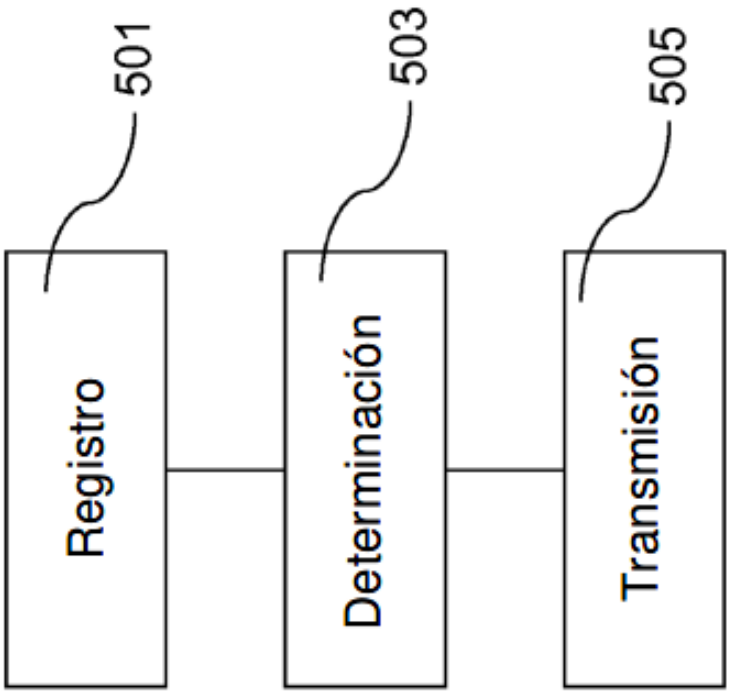

Fig. 5