(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 628 613**

(51) Int. CI.:

H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **17.09.2012 PCT/CN2012/081473**

(87) Fecha y número de publicación internacional: **20.03.2014 WO14040292**

(96) Fecha de presentación y número de la solicitud europea: **17.09.2012 E 12884731 (6)**

(97) Fecha y número de publicación de la concesión europea: **03.05.2017 EP 2790382**

(54) Título: **Método y dispositivo de protección contra ataques**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
03.08.2017

(73) Titular/es:

HUAWEI TECHNOLOGIES CO., LTD. (100.0%)
Huawei Administration Building Bantian, Longgang District
Shenzhen, Guangdong 518129, CN

(72) Inventor/es:

LIU, GAOQIANG;
PAN, YONGBO y
YANG, LI

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín Europeo de Patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre Concesión de Patentes Europeas).

DESCRIPCIÓN

Método y dispositivo de protección contra ataques

CAMPO DE LA INVENCIÓN

La presente invención se refiere a las tecnologías de la comunicación y en particular, a un método y dispositivo de defensa contra ataques.

ANTECEDENTES DE LA INVENCIÓN

El protocolo de capa de conexión segura (Secure Socket Layer, en adelante referido como SSL en forma abreviada) es un protocolo de comunicación segura de la red y se utiliza para proporcionar un canal seguro entre dos máquinas. Tiene funciones de protección de los datos transmitidos e identificar las máquinas de comunicaciones. Una comprobación de ataque del tipo de denegación de servicio (Denial of Service, en adelante referido como DOS en forma abreviada) de SSL es una manera de ataque en la que un ordenador de uso general está conectado a una línea de abonado digital (Digital Subscriber Line, en adelante referida como DSL en forma abreviada) y ataca un servidor SSL demandando de nuevo una clave de encriptación.

En la manera de ataque, puesto que una sobrecarga de una unidad central de procesamiento (central processing unit, en adelante referida como CPU en forma abreviada) del servidor SSL es aproximadamente 15 veces la de un cliente cuando se negocia un algoritmo de encriptación, dicha clase de comportamiento de ataque consume recursos de CPU del servidor en gran medida. Sin embargo, hasta ahora no existe ningún método efectivo que pueda realizar una defensa contra un comportamiento de ataque DOS de SSL.

THC: "thc-ssl-dos" (25 octubre 2011, https://www.thc.org/thc-ssl-dos/) da a conocer una herramienta denominada THC-SSL-DOS para verificar el comportamiento de SSL. Los ataques de DDoS tradicionales basados en inundación son sub-óptimos: servidores están preparados para gestionar una gran cantidad de tráfico y los clientes están enviando constantemente demandas al servidor incluso cuando no está bajo un ataque. El diálogo operativo de SSL se realiza solamente al inicio de una sesión segura y solamente si se requiere la seguridad. Los servidores no están preparados para gestionar una gran cantidad de diálogos operativos de SSL. El escenario de ataque más desfavorable es un ataque de Agotamiento de SSL montado desde miles de clientes. No existe ninguna solución real. Desactivar la función de Renegociación de SSL e instalar un Acelerador de SSL puede mitigar la importancia del problema, pero no lo resuelve.

El documento de Vincent Bernat: "Mitigación de DoS informática de SSL", 4 noviembre 2011, reconoce que no existe ninguna solución definitiva para los ataques de DoSs informáticos de DSL y examina algunos procedimientos de soluciones alternativas, a modo de ejemplo, desactivar la renegociación de SSL, limitación de las tasas de diálogos SSL, aumento de la potencia de procesamiento del lado del servidor y aplicar más trabajo en el lado del cliente.

SUMARIO DE LA INVENCIÓN

Formas de realización de la presente invención dan a conocer un método y dispositivo de defensa contra los ataques, con el fin de realizar efectivamente una defensa contra un comportamiento de ataque de denegación de servicio (Denial of Service, en adelante referido como DOS en forma abreviada) de una capa de conexión segura (Secure Socket Layer, en adelante referida como SSL en forma abreviada).

En un primer aspecto de la idea inventiva, una forma de realización de la presente invención da a conocer un método de defensa contra los ataques, que incluye:

supervisar una conexión de protocolo de control de transmisión (TCP) establecida entre un cliente y un servidor SSL;

contar un número de renegociaciones en la conexión TCP, en donde el número de las renegociaciones es un número de negociaciones repetidas entre el cliente y el servidor en la conexión TCP,

cuando el número de las renegociaciones en la conexión TCP es superior que un umbral preestablecido del número de renegociaciones, determinar que la conexión TCP es una conexión anormal; y

desconectar la conexión TCP;

en donde el método incluye, además:

determinar si una dirección IP del cliente en la conexión de protocolo de control de transmisión TCP está incluida en una lista negra, en donde la lista negra incluye una dirección IP de un cliente que inicia una conexión anormal;

cuando la dirección IP del cliente no está incluida en la lista negra, introducir la etapa de contar el número de las

renegociaciones en la conexión TCP; y

cuando la dirección IP del cliente está incluida en la lista negra, desconectar la conexión TCP.

En una primera manera de puesta en práctica posible del primer aspecto de la idea inventiva, la operación de contar el número de las renegociaciones en la conexión TCP incluye:

por intermedio de un tipo de un paquete intercambiado entre el cliente y el servidor en la conexión TCP, identificar si el paquete es un paquete de negociación; y

contar el número de las renegociaciones en la conexión TCP en conformidad con el número de paquetes de negociación en la conexión TCP.

En combinación con la primera manera de puesta en práctica posible del primer aspecto de la idea inventiva, en una segunda manera de puesta en práctica posible del primer aspecto, el paquete de negociación incluye un paquete de un tipo de cambio de especificación de cifrado Change Cipher Spec.

En una tercera manera de puesta en práctica posible del primer aspecto de la idea inventiva, la operación de contar el número de las renegociaciones en la conexión TCP incluye:

obtener el número de las renegociaciones en la conexión TCP contando el número de los paquetes de negociación del tipo de cambio de especificación de cifrado Change Cipher Spec que se intercambian entre el cliente y un servidor SSL en la conexión TCP.

En combinación con el primer aspecto de la idea inventiva, la primera manera de puesta en práctica posible del primer aspecto, la segunda manera de puesta en práctica posible del primer aspecto, o la tercera manera de puesta en práctica posible del primer aspecto, en una cuarta manera de puesta en práctica posible del primer aspecto, el método de defensa contra los ataques en la presente invención incluye, además:

contar el número de conexiones anormales iniciadas por el cliente en la conexión TCP; y

cuando el número de las conexiones anormales iniciadas por el cliente es superior a un umbral preestablecido del número de conexiones, añadir la dirección IP del cliente en la lista negra.

En un segundo aspecto de la idea inventiva, una forma de realización de la presente invención da a conocer un dispositivo de defensa contra los ataques, que incluye:

un módulo configurado para supervisar una conexión TCP establecida entre un cliente y un servidor SSL;

un primer módulo de conteo, configurado para contar un número de renegociaciones en la conexión TCP, en donde el número de las renegociaciones es un número de negociaciones repetidas entre el cliente y el servidor en la conexión TCP;

un módulo de determinación de conexión anormal, configurado para, cuando el número de las renegociaciones en la conexión TCP es superior a un umbral preestablecido del número de renegociaciones, determinar que la conexión TCP es una conexión anormal; y

un módulo de procesamiento, configurado para desconectar la conexión TCP;

en donde el dispositivo de defensa contra los ataques incluye, además:

un módulo de determinación, configurado para determinar si una dirección IP del cliente en la conexión TCP está incluida en una lista negra, en donde la lista negra incluye una dirección IP de un cliente que inicia una conexión anormal, iniciar operativamente el primer módulo de conteo cuando la dirección IP del cliente no está incluida en la lista negra, e iniciar el módulo de procesamiento cuando la dirección IP del cliente está incluida en la lista negra.

En una primera manera de puesta en práctica posible del segundo aspecto de la idea inventiva, el primer módulo de conteo incluye:

una unidad de identificación, configurada para, por intermedio de un tipo de un paquete intercambiado entre el cliente y el servidor en la conexión TCP, identificar si el paquete es un paquete de negociación; y

una unidad de conteo, configurada para contar el número de las renegociaciones en la conexión TCP en conformidad con el número de paquetes de negociación en la conexión TCP que se identifican por la unidad de identificación.

En combinación con la primera manera de puesta en práctica posible del segundo aspecto de la idea inventiva, en una segunda manera de puesta en práctica posible del segundo aspecto, el paquete de negociación incluye un paquete de un tipo de cambio de especificación de cifrado Change Cipher Spec.

En una tercera manera de puesta en práctica posible del segundo aspecto de la idea inventiva, el primer módulo de conteo está configurado concretamente para obtener el número de las renegociaciones en la conexión TCP contando el número de paquetes de negociación del tipo de cambio de especificación de cifrado Change Cipher Spec que se intercambian entre el cliente y un servidor SSL en la conexión TCP.

En combinación con el segundo aspecto de la idea inventiva, la primera manera de puesta en práctica posible del segundo aspecto, la segunda manera de puesta en práctica posible del segundo aspecto o la tercera manera de puesta en práctica posible del segundo aspecto, una cuarta manera de puesta en práctica posible del segundo aspecto, el dispositivo de defensa contra los ataques dado a conocer en la presente invención incluye, además:

un módulo de determinación, configurado para determinar si una dirección IP del cliente en la conexión TCP está incluida en una lista negra, en donde la lista negra incluye una dirección IP de un cliente que inicia una conexión anormal, iniciar operativamente el primer módulo de conteo cuando la dirección IP del cliente no está incluida en la lista negra, e iniciar el módulo de procesamiento cuando la dirección del IP del cliente está incluida en la lista negra.

En combinación con el segundo aspecto de la idea inventiva, la primera manera de puesta en práctica posible del segundo aspecto, la segunda manera de puesta en práctica posible del segundo aspecto o la tercera manera de puesta en práctica posible del segundo aspecto, en una cuarta manera de puesta en práctica posible del segundo aspecto, el dispositivo de defensa contra los ataques dado a conocer en la presente invención incluye, además:

un segundo módulo de conteo, configurado para contar el número de conexiones anormales iniciadas por el cliente en la conexión TCP; y

un módulo de gestión, configurado para, cuando el número de las conexiones anormales iniciadas por el cliente en la conexión TCP que se cuentan por el segundo módulo de conteo es superior que un umbral preestablecido del número de conexiones, añadir la dirección IP del cliente en la lista negra.

En esta forma de realización, en conformidad con una característica de que un ataque del tipo DOS de SSL consume los recursos de una unidad CPU de servidor negociando repetidamente de forma continua, el número de renegociaciones en la conexión TCP es objeto de conteo, y cuando el número contado de las renegociaciones en la conexión TCP es superior a un umbral del número de renegociaciones, se determina que la conexión TCP es una conexión anormal, y la conexión TCP se desconecta, con lo que se pone en práctica efectivamente la defensa contra un comportamiento de ataque de denegación de servicios DOS de SSL y se protege al servidor del ataque de SSL DOS.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

Para describir las soluciones técnicas en las formas de realización de la presente invención o en la técnica anterior con mayor claridad, a continuación se introducen brevemente los dibujos adjuntos requeridos para describir las formas de realización o la técnica anterior. Evidentemente, los dibujos adjuntos en la descripción siguiente ilustran algunas formas de realización de la presente invención, y los expertos en esta técnica pueden derivar todavía otros dibujos a partir de estos dibujos adjuntos sin necesidad de esfuerzos creativos.

La Figura 1 es un diagrama esquemático de una arquitectura de red de aplicación de un método de defensa contra los ataques de conformidad con una forma de realización de la presente invención,

La Figura 2 es un diagrama de flujo de un método de defensa contra los ataques en conformidad con una forma de realización de la presente invención;

La Figura 3 es un diagrama de flujo de otro método de defensa contra los ataques en conformidad con una forma de realización de la presente invención,

La Figura 4 es un diagrama de flujo de todavía otro método de defensa contra los ataques en conformidad con una forma de realización de la presente invención;

La Figura 5 es un diagrama estructural esquemático de un dispositivo de defensa contra los ataques en conformidad con una forma de realización de la presente invención;

La Figura 6 es un diagrama estructural esquemático de otro dispositivo de defensa contra los ataques en conformidad con una forma de realización de la presente invención; y

La Figura 7 es un diagrama estructural esquemático de otro dispositivo de defensa contra los ataques en

conformidad con una forma de realización de la presente invención.

DESCRIPCIÓN DETALLADA DE LAS FORMAS DE REALIZACIÓN

Para hacer más claros los objetivos, las soluciones técnicas y las ventajas de las formas de realización de la presente invención, a continuación se describe, de forma clara y completa, las soluciones técnicas en las formas de realización de la presente invención haciendo referencia a los dibujos adjuntos en las formas de realización de la presente invención. Evidentemente, las formas de realización descritas son simplemente una parte y no la totalidad de las formas de realización de la presente invención. Todas las demás formas de realización obtenidas por expertos en esta técnica sobre la base de las formas de realización de la presente invención sin necesidad de esfuerzos creativos, caerán dentro del alcance de protección de la presente invención.

Un método de defensa contra los ataques dado a conocer en esta forma de realización puede ponerse en práctica en un producto de pasarela, en donde el producto de pasarela se desarrolla en frente de un servidor de capa de conexión segura (Secure Socket Layer, en adelante referida como SSL en forma abreviada) con lo que se realiza una protección del servidor SSL; y se puede desarrollar también en un servidor SSL en la forma de software para realizar la detección sobre una demanda de SSL, con lo que se impide un comportamiento de ataque del tipo de denegación de servicio (Denial of Service, en adelante referido como DOS en forma abreviada) de SSL. La Figura 1 es un diagrama esquemático de una arquitectura de red de aplicación de un método de defensa contra los ataques en conformidad con una forma de realización de la presente invención. Según se ilustra en la Figura 1, un intruso atacante puede utilizar un ordenador generar para interaccionar con un servidor SSL como si fuera un usuario normal. El intruso atacante establece una conexión de protocolo de control de transmisión (Transmission Control Protocol, en adelante referido como TCP en forma abreviada) con el servidor SSL y luego, negocia, de forma repetida, una clave rápidamente sin una interrupción en la conexión TCP establecida, con el fin de atacar al servidor SSL. En este caso, el intruso atacante puede iniciar un ataque sobre el servidor SSL por intermedio de una conexión TCP establecida con el servidor SSL y puede iniciar también un ataque sobre el servidor SSL por intermedio de múltiples conexiones TCP establecidas con el servidor SSL. Por supuesto, cuanto mayor sea el número de conexiones TCP, tanto mayores serán los daños para el servidor SSL. Además, pueden existir también múltiples intrusos de ataque. El método de defensa contra los ataques, en esta forma de realización, puede ponerse en práctica en un producto de pasarela tal como un enrutador o un cortafuegos que se pueden poner en práctica también por intermedio de un enrutador y un cortafuegos, y puede aplicarse también a un dispositivo de limpieza de denegación de servicio del tipo distribuido (Distributed Denial of Service, en forma abreviada referido como DDOS en forma abreviada), en donde el producto de pasarela tal como el enrutador o el cortafuegos o el dispositivo de limpieza DDOS se desarrolla en frente de un servidor SSL, con lo que es capaz de bloquear un ataque en el servidor SSL iniciado por un intruso.

La Figura 2 es un diagrama de flujo de un método de defensa contra los ataques en conformidad con una forma de realización de la presente invención. Según se ilustra en la Figura 2, esta forma de realización da a conocer un método de defensa contra los ataques. El método de defensa contra los ataques puede utilizarse para la defensa contra un ataque del tipo de denegación de servicio (Denial of service, en adelante referida como DOS en forma abreviada) de una capa de conexión segura (Secure Socket Layer, en adelante referida como SSL en forma abreviada). Puede entenderse que, en una aplicación real, un mismo cliente puede establecer también múltiples conexiones con un servidor. Para una descripción clara, la forma de realización de la presente invención toma, a modo de ejemplo, para fines de descripción, una conexión TCP establecida entre un cliente y un servidor. El método puede incluir las etapas siguientes:

Etapa 201: Contar el número de renegociaciones en una conexión de protocolo de control de transmisión TCP.

En una aplicación real, cuando un cliente y un servidor interaccionan entre sí de forma normal, solamente una conexión TCP puede existir entre el cliente y el servidor, o pueden existir múltiples conexiones TCP al mismo tiempo. Un intruso puede atacar al servidor por intermedio de una conexión TCP establecida con el servidor y puede atacar también al servidor a través de múltiples conexiones TCP establecidas con el servidor. Cuando múltiples conexiones TCP se establecen con el servidor, cada conexión TCP puede supervisarse por separado, y el número de renegociaciones entre el cliente y el servidor en cada conexión TCP puede contarse por separado. La forma de realización de la presente invención toma, a modo de ejemplo, para su descripción, una conexión TCP establecida entre un cliente y un servidor SSL. Más concretamente, una supervisión puede realizarse sobre una sola conexión TCP y el número de renegociaciones en la conexión TCP puede ser objeto de conteo, en donde el número de las renegociaciones es el número de negociaciones repetidas entre el cliente y el servidor en la conexión TCP.

Un paquete de negociación del tipo de cambio de especificación de cifrado Change Cipher Spec existe junto con cada proceso de negociación clave entre el cliente y el servidor SSL en una conexión TCP, en donde una primera negociación es una negociación normal y la otra no primera negociación es una negociación repetida; por lo tanto, cuando el número de renegociaciones en la conexión de protocolo de control de transmisión TCP es objeto de conteo, si el paquete es un paquete de negociación puede identificarse por intermedio de un tipo de un paquete intercambiado entre el cliente y el servidor en la conexión TCP, y el número de las renegociaciones en la conexión TCP puede contarse en conformidad con el número de paquetes de negociación en la conexión TCP. Más

concretamente, el número de las renegociaciones en la conexión TCP puede obtenerse contando el número de paquetes de negociación del tipo de cambio de especificación de cifrado Change Cipher Spec, que se intercambian entre el cliente y el servidor SSL en la conexión TCP.

Puesto que el ataque de SSL DOS se refiere a que un intruso atacante inicia rápidamente negociaciones repetidas dentro de un corto intervalo de tiempo después de establecer una conexión con el servidor, con el fin de atacar al servidor, el número de las renegociaciones en la conexión TCP dentro de un tiempo preestablecido puede obtenerse en función de una diferencia entre el número de paquetes de negociación en la conexión TCP dentro del intervalo temporal preestablecido y 1.

Etapa 202: Si el número de las renegociaciones en la conexión TCP es superior a un umbral preestablecido del número de renegociaciones, determinar que la conexión TCP es una conexión anormal.

Más concretamente, el umbral del número de renegociaciones es un número máximo preestablecido de renegociaciones permitidas dentro de un determinado tiempo en una conexión TCP. En un caso normal, el número de renegociaciones en una conexión TCP dentro de un tiempo preestablecido no supera el umbral del número de renegociaciones; cuando el número de las renegociaciones supera el umbral del número de renegociaciones, ello indica que un proceso de renegociación en la conexión TCP puede ser un ataque iniciado por un intruso malintencionado exterior y luego, se determina que la conexión TCP es una conexión anormal. Puede entenderse que, en una aplicación real, si existen múltiples conexiones TCP, si el número de renegociaciones en cada conexión TCP es superior que el umbral preestablecido del número de renegociaciones puede determinarse por separado, con el fin de determinar por separado si cada conexión TCP es, o no, una conexión anormal.

Etapa 203: Desconectar la conexión TCP.

Cuando se determina que la conexión TCP es una conexión anormal, con el fin de garantizar que el servidor está protegido contra un ataque de intruso, se desconecta la conexión TCP.

Puede entenderse que, en la forma de realización de la presente invención, el número de negociaciones en la conexión TCP puede obtenerse contando directamente el número de paquetes de negociación en la conexión TCP, y si la conexión TCP es una conexión anormal, puede determinarse también en conformidad con un umbral establecido del número de negociaciones. Más concretamente, en la etapa 201, el número de las negociaciones puede obtenerse directamente en función del número de paquetes de negociación de un tipo de cambio de especificación de cifrado, Change Cipher Spec, que se intercambia entre el cliente y el servidor en la conexión TCP dentro de un período de tiempo preestablecido. En la etapa 202, se puede determinar si el número de las negociaciones en la conexión TCP es superior que el umbral preestablecido del número de negociaciones, en donde el umbral del número de negociaciones es un número preestablecido de negociaciones permitidas dentro de un período de tiempo establecido en una conexión TCP.

En esta forma de realización, en conformidad con una característica de que una ataque de SSL DOS consume recursos de CPU del servidor renegociando continuamente una clave en una conexión TCP establecida, el número de renegociaciones en la conexión TCP es objeto de conteo, y cuando el número contado de las renegociaciones en la conexión TCP es superior que a un umbral de número de renegociaciones, se determina que la conexión TCP es una conexión anormal, y se desconecta la conexión TCP, con lo que se realiza efectivamente una defensa contra un comportamiento de ataque de tipo DOS de SSL y se protege al servidor contra el ataque SSL DOS.

La Figura 3 es un diagrama de flujo de otro método de defensa contra los ataques en conformidad con una forma de realización de la presente invención. La forma de realización de la presente invención toma a modo de ejemplo, para su descripción, una conexión TCP establecida entre un cliente y un servidor SSL. Puede entenderse que, en una aplicación real, cuando existen múltiples conexiones TCP entre el cliente y el servidor SSL, cada conexión TCP puede procesarse con referencia al método descrito en esta forma de realización. Según se ilustra en la Figura 3, el método incluye:

Etapa 300: Determinar si una dirección IP de un cliente en una conexión TCP está incluida en una lista negra; si la dirección IP del cliente está incluida en la lista negra, realizar la etapa 303 y si no lo está, realizar la etapa 301.

Más concretamente, una lista negra de intrusos de ataque puede prestablecerse en un producto de pasarela tal como un enrutador o un cortafuegos, o en un dispositivo de limpieza de DDOS. La lista negra incluye una dirección IP detectada de un intruso atacante. Cuando un paquete enviado por el cliente es recibido, si la dirección IP del cliente en la conexión TCP está en la lista negra prestablecida puede determinarse en conformidad con una dirección IP origen incluida en el paquete. Si la dirección IP no está en la lista negra, realizar la etapa 301, de no ser así, realizar la etapa 303, en donde la conexión TCP se desconecta directamente.

Conviene señalar que, en un caso en el que la dirección IP del cliente en la conexión TCP está incluida en la lista negra, después de realizar la etapa 303 para desconectar la conexión TCP, resulta innecesario realizar la etapa 304 para contar el número de conexiones anormales iniciadas por el cliente en la conexión TCP. En tal caso, se

determina ya, en función de la lista negra, que el cliente es un intruso atacante, con lo que resulta innecesario determinar, además, si añadir, o no, la dirección IP del cliente en la lista negra.

Etapa 301: Contar el número de renegociaciones en la conexión TCP y realizar la etapa 302.

Más concretamente, un paquete de negociación de un tipo de cambio de especificación de cifrado, Change Cipher Spec, existe junto con cada proceso de negociación clave de un cliente y un servidor SSL en una conexión TCP, en donde una primera negociación es una negociación normal y la otra no primera negociación es una negociación repetida; por lo tanto, el número de las renegociaciones en la conexión TCP puede obtenerse contando el número de paquetes de negociación del tipo de cambio de especificación de cifrado, Change Cipher Spec, que se intercambian entre el cliente y el servidor SSL en la conexión TCP. Puesto que el ataque del tipo de denegación de servicio DOS de SSL se refiere a que un intruso atacante inicia rápidamente negociaciones repetidas dentro de un corto intervalo de tiempo después de establecer una conexión con el servidor con el fin de atacar al servidor, el número de renegociaciones en la conexión TCP dentro de un período de tiempo preestablecido puede obtenerse en conformidad con una diferencia entre el número de paquetes de negociación en la conexión TCP dentro del tiempo preestablecido y 1. A modo de ejemplo, si el número de paquetes de negociación del tipo de cambio de especificación de cifrado, Change Cipher Spec, que aparece en una determinada conexión TCP dentro de una hora es 10, puede obtenerse que el número de renegociaciones en la conexión TCP dentro de una hora es 9.

Más concretamente, en una aplicación real, cuando el número de renegociaciones en la conexión TCP dentro de un tiempo preestablecido es objeto de conteo, se puede prestablecer un tiempo para la operación de conteo. En una aplicación real, un período de conteo puede establecerse a 30 segundos o 1 minuto. El establecimiento del tiempo específico puede realizarse en conformidad con un requisito de servicio real y puede determinarse también en función del tráfico de red. Durante el conteo, cuando se recibe un paquete de negociación, el número de paquetes de negociación se registra una vez y se registra una marca temporal, de modo que cuando se reciba posteriormente un paquete de negociaciones, el período de conteo puede determinarse de conformidad con la marca temporal anteriormente registrada, y el número de renegociaciones dentro del período de conteo puede contarse de conformidad con el período de conteo determinado. A modo de ejemplo, cuando se recibe un primer paquete de negociaciones, el número del paquete de negociaciones se registra como 1 y se registra una marca temporal, y cuando se recibe un segundo paquete de negociaciones, se añade 1 al número de paquetes de negociaciones y se registra una segunda marca temporal, de modo que el número de paquetes de negociaciones recibido dentro de este período de tiempo pueda determinarse en función de las dos marcas temporales registradas.

Etapa 302: Si el número de las renegociaciones en la conexión TCP es superior que un umbral preestablecido del número de renegociaciones, determinar que la conexión TCP es una conexión anormal e iniciar la etapa 303.

En este caso, el umbral del número de renegociaciones es un número máximo preestablecido de renegociaciones permitidas dentro de un determinado tiempo en una conexión TCP. En un caso normal, el número de renegociaciones en una conexión TCP dentro de un tiempo preestablecido no supera el umbral del número de renegociaciones; cuando el número de renegociaciones supera el umbral del número de renegociaciones, ello indica que un proceso de renovación en la conexión TCP puede ser un ataque iniciado por intruso malintencionado exterior, y entonces, se determina que la conexión TCP es una conexión anormal. A modo de ejemplo, se prestablece que el número máximo de renegociaciones dentro de una hora en una conexión TCP es 10, el umbral del número de renegociaciones de la conexión TCP se establece a 10. Cuando el número de renegociaciones en la conexión TCP supera el número de 10 dentro de una hora, la conexión TCP se toma como una conexión anormal. Por supuesto, puede entenderse que el umbral del número de renegociaciones se determina en función de un valor empírico del número normal de negociaciones que pueden existir en una conexión TCP normal en una aplicación real. Durante una determinación específica, el ajuste puede realizarse en función de requerimiento de servicio o del tráfico de la red. En una aplicación real, el umbral del número de renegociaciones puede establecerse a tres veces por treinta segundos (3 veces/30 s).

Etapa 303: Desconectar la conexión TCP e iniciar la etapa 304.

En la etapa 302, cuando se determina que la conexión TCP es una conexión anormal, puede desconectarse la conexión TCP, con el fin de impedir que el intruso realice el ataque del tipo SSL DOS sobre el servidor SSL por intermedio de la conexión TCP. Más concretamente, la conexión TCP puede desconectarse enviando paquetes de reposición bidireccionales (Reset, en adelante referido como RST en forma abreviada), es decir, enviar un paquete RST a un cliente con una dirección IP origen dirigida a la conexión TCP y enviar un paquete RST a un servidor cuya dirección IP de destino apunta a la conexión TCP, con el fin de desconectar la conexión TCP entre el cliente y el servidor SSL.

Etapa 304: Contar el número de conexiones anormales iniciadas por el cliente en la conexión TCP, e iniciar la etapa 305.

Después de que se determine que la conexión TCP es una conexión anormal y se desconecta la conexión TCP, puede realizarse una supervisión sobre la dirección IP del cliente en la conexión TCP, con el fin de determinar,

además, si el cliente en la conexión TCP es un intruso atacante. Más concretamente, puede establecerse una tabla de supervisión de conexión anormal. La tabla de supervisión de conexión anormal registra una dirección IP de un cliente y el número de las conexiones anormales iniciadas por el cliente a las que apunta la dirección IP. Más concretamente, después de identificar que una determina conexión TCP es una conexión anormal en la etapa 302, en la tabla de supervisión de conexión anormal puede buscarse una dirección IP que sea la misma que la dirección IP del cliente en la conexión TCP. Si se encuentra una dirección IP que es la misma que la dirección IP del cliente, se añade 1 al número de conexiones anormales correspondientes a la dirección IP. Si no se encuentra la misma dirección IP, se añade un nuevo registro en la tabla de supervisión de conexiones anormales, se registra la dirección IP y el número de conexiones anormales correspondientes a la dirección IP se registra como 1. Puede entenderse que el conteo del número de las conexiones anormales iniciadas por el cliente en la conexión TCP se refiere también a contar el número de conexiones anormales dentro de un período de conteo establecido. Más concretamente, cuando se determina la presencia de una conexión anormal, puede registrarse una marca temporal, un período de conteo se determina en función de la marca temporal registrada, y el número de las conexiones anormales dentro del período de conteo establecido es objeto de conteo. Para un método de conteo específico, puede hacerse referencia a la descripción del conteo del número de renegociaciones en la etapa 301, que no se describe aquí de nuevo en detalle.

Etapa 305: Si el número de conexiones anormales iniciadas por el cliente en la conexión TCP es superior que un umbral preestablecido del número de conexiones, añadir la dirección IP del cliente en la lista negra.

Más concretamente, el umbral del número de conexiones puede ser un número máximo de conexiones anormales iniciadas por el cliente que la dirección IP apunta a que se permita dentro de un período de tiempo preestablecido. Cuando el número de conexiones anormales iniciadas por el cliente en la conexión TCP que son objeto de conteo en la etapa 304, es superior al umbral preestablecido del número de conexiones, se determina que el cliente es un intruso atacante y la dirección IP del cliente se añade en la lista negra, con el fin de actualizar dinámicamente dicha lista negra. En este caso, en la siguiente ocasión en que se reciba un paquete enviado desde la dirección IP, el paquete puesta en práctica desecharse directamente, o puede desconectarse directamente una conexión TCP iniciada por la dirección IP, con lo que se mejora la eficiencia de la detección. En este caso, la lista negra establecida registra una dirección IP detectada de un intruso atacante.

Puede entenderse que, en la forma de realización de la presente invención, el número de negociaciones en la conexión TCP puede obtenerse mediante un conteo directo del número de paquetes de negociaciones en la conexión TCP, y si la conexión TCP es una conexión anormal puede determinarse en conformidad con un umbral preestablecido del número de negociaciones. Más concretamente, en la etapa 301, el número de las negociaciones puede obtenerse directamente en función del número de paquetes de negociaciones del tipo de cambio de especificación de cifrado, Change Cipher Spec que se intercambian entre el cliente y el servidor SSL en la conexión TCP dentro de un período de tiempo preestablecido. En la etapa 302, se puede determinar si el número de negociaciones en la conexión TCP es superior que un umbral preestablecido del número de negociaciones, en donde el umbral del número de negociaciones es el número preestablecido de negociaciones permitidas dentro de un período de tiempo establecido en una conexión TCP.,

En el método de defensa contra los ataques dado a conocer en la forma de realización de la presente invención, antes de que se cuente el número de renegociaciones en una conexión TCP, en primer lugar, si una dirección IP de un cliente en la conexión TCP está en una lista negra se determina; si la dirección IP está en la lista negra, la conexión TCP se desconecta directamente; si la dirección IP no está en la lista negra, si la conexión TCP es una conexión anormal se determina contando el número de renegociaciones en la conexión TCP; si la conexión TCP es una conexión anormal, la conexión TCP se desconecta y el número de conexiones anormales iniciadas por el cliente en la conexión TCP se registra en una tabla de supervisión de conexiones anormales establecida; y cuando el número de las conexiones anormales iniciadas por el cliente en la conexión TCP supera un umbral preestablecido del número de conexiones, la dirección IP del cliente se añade a la lista negra, con el fin de actualizar la lista negra a su debido tiempo, con lo que no solamente es capaz de impedir al cliente iniciar un ataque SSL DOS sobre un servidor SSL, sino que también es capaz de mejorar la eficiencia de la defensa.

La Figura 4 es un diagrama de flujo de otro método de defensa contra los ataques en conformidad con una forma de realización de la presente invención. Según se ilustra en la Figura 4, esta forma de realización da a conocer un método de defensa contra los ataques que puede incluir específicamente las etapas siguientes.

Etapa 400: Recibir un paquete enviado por un cliente e iniciar la etapa 401.

Etapa 401: Determinar si el paquete recibido accede a una sesión; si la respuesta es afirmativa, realizar la etapa 402 y en caso contrario, realizar la etapa 410.

Después de que se reciba un paquete enviado por un cliente, se determina si el paquete contiene información de una sesión. Más concretamente, si puede determinarse si una sesión establecida es objeto de acceso, en función de una quíntuple información del paquete, en donde la quíntuple información es: una dirección IP origen, una dirección IP de destino, un puerto origen, un puerto de destino y un tipo de protocolo. Si la sesión es alcanzada, ello indica

que la dirección IP origen del paquete es una dirección IP real y en tal caso, se realiza la etapa 402. Si no se accede a la sesión, ello indica que la dirección IP origen del paquete es una dirección IP virtual y en tal caso, puede realizarse la etapa 410 y se desecha el paquete.

Etapa 402: En conformidad con el paquete recibido, determinar si una dirección IP del cliente está, o no, en una lista negra; si la respuesta es afirmativa, realizar la etapa 410, de no ser así, realizar la etapa 403.

Cuando el paquete recibido muestra información de la sesión, si la dirección IP del cliente que envía el paquete está, o no, en una lista negra se determina de forma adicional, con el fin de impedir que un intruso utilice una dirección IP para iniciar un ataque sobre el servidor, en donde la lista negra registra una dirección IP detectada de un intruso atacante. Si la respuesta es afirmativa, se realiza la etapa 410 y se desecha el paquete; de no ser así, se realiza la etapa 403.

Etapa 403: Contar el número de renegociaciones en una conexión TCP correspondiente al paquete e iniciar la etapa 404.

Esta etapa se refiere a que, cuando la dirección IP del cliente que envía el paquete no está en la lista negra, se supervisa una conexión TCP establecida entre un cliente al que apunta la dirección IP del cliente y un servidor SSL, con el fin de contar el número de renegociaciones en la conexión TCP que corresponden al paquete recibido. Durante la identificación de un comportamiento de renegociación en la conexión TCP, la identificación puede realizarse concretamente por intermedio de un paquete intercambiado entre el cliente y el servidor SSL en la conexión TCP. Un paquete de negociación de un tipo de cambio de especificación de cifrado, Change Cipher Spec, existe junto con cada proceso de renegociación entre el cliente y el servidor SSL en una conexión TCP, en donde una primera negociación es una negociación normal la otra no primera negociación es una negociación repetida; de este modo, en esta forma de realización, si el paquete es, o no, un paquete de negociaciones puede determinarse mediante la determinación de si el tipo del paquete recibido es del tipo de cambio de especificación de cifrado, Change Cipher Spec. Además, puesto que el ataque de SSL DOS se refiere a que un intruso atacante inicia rápidamente negociaciones repetidas dentro de un período de tiempo corto después de establecer una conexión con el servidor con el fin de atacar al servidor, el número de renegociaciones en la conexión TCP puede obtenerse en función de una diferencia entre el número el paquetes de negociaciones en la conexión TCP dentro de un período de tiempo preestablecido y 1. A modo de ejemplo, si el número de paquetes de negociaciones del tipo de cambio de especificación de cifrado, Change Cipher Spec, que aparece en una determinada conexión TCP dentro de una hora es 10, puede obtenerse que el número de renegociaciones en la conexión TCP dentro de una hora es 9.

Más concretamente, en una aplicación real, cuando el número de renegociaciones en la conexión TCP dentro de un tiempo preestablecido es objeto de conteo, se puede prestablecer un tiempo para dicho conteo. En una aplicación real, un período de conteo puede establecerse a 30 segundos o 1 minuto. El establecimiento del tiempo específico puede realizarse en función del requerimiento de servicio real y puede determinarse también en función del tráfico de la red. Durante el conteo, cuando se recibe un paquete de negociaciones, el número de paquetes de negociaciones se registra una vez y se registra también una marca temporal, de modo que cuando se reciba posteriormente un paquete de negociaciones, pueda determinarse un período de conteo en conformidad con la marca temporal anteriormente registrada, y el número de renegociaciones dentro del período de conteo puede contarse en función del período de conteo determinado. A modo de ejemplo, cuando se recibe un primer paquete de negociación, el número del paquete de negociación registra como 1 y también se registra una marca temporal, y cuando se recibe un segundo paquete de negociaciones, se añade 1 al número de los paquetes de negociaciones y se registra una segunda marca temporal, de modo que el número de paquetes de negociaciones recibidos dentro de este período de tiempo pueda determinarse en función de las dos marcas temporales registradas.

Etapa 404: Determinar si el número de las renegociaciones en la conexión TCP es superior que un umbral preestablecido del número de renegociaciones; si la respuesta es afirmativa, realizar la etapa 405, de no ser así, volver a realizar la etapa 400.

Después del proceso de conteo de la etapa 403, se determina si el número contado de las renegociaciones en la conexión TCP es superior que el umbral preestablecido del número de las renegociaciones. Más concretamente, si el número de las renegociaciones en la conexión TCP es superior que el umbral preestablecido del número de renegociaciones puede determinarse después de cada vez que se actualiza el número de las renegociaciones en la conexión TCP. A modo de ejemplo, cuando se determina que el paquete recibido es un paquete de negociación del tipo de cambio de especificación de cifrado, Change Cipher Spec, se añade 1 al número de paquetes de negociaciones en la conexión TCP a la que pertenece el paquete, es decir, se añade 1 al número de las renegociaciones en la conexión TCP, en consecuencia. Si el número actualizado de las renegociaciones es superior al umbral preestablecido del número de renegociaciones, puede realizarse la etapa 405 y se determina que la conexión TCP es una conexión anormal; de no ser así, hay que volver a realizar la etapa 400 y continuar recibiendo otro paquete enviado por el cliente.

En esta forma de realización, antes de que se realice la etapa 403, el método incluye, además: preconfigurar el umbral del número de renegociaciones y un umbral del número de conexiones. Más concretamente, los dos

umbrales pueden establecerse en conformidad con una situación real. En este caso, el umbral del número de renegociaciones se refiere a un número máximo permitido configurado por el usuario de renegociaciones dentro de un período de tiempo establecido y el umbral del número de conexiones se refiere a un número máximo permitido configurado por el usuario de conexiones anormales dentro del período de tiempo establecido. Durante una determinación específica, el establecimiento puede realizarse en función de un requerimiento de servicio o del tráfico de la red. En una aplicación real, el umbral del número de renegociaciones puede establecerse a tres veces por treinta segundos (3 veces/30 s) y el umbral del número de conexiones puede establecerse a tres veces por quince segundos (3 veces/15 s).

Etapa 405: Determinar que la conexión TCP es una conexión anormal e iniciar la etapa 406.

Cuando el número de las renegociaciones en la conexión TCP es superior que el umbral preestablecido del número de renegociaciones, ello indica que un proceso de renegociación en la conexión TCP puede iniciarse por un intruso de un ataque malintencionado externo y puede determinarse que la conexión TCP es una conexión anormal. A modo de ejemplo, se prestablece que el número máximo de renegociaciones dentro de una hora en una conexión TCP es 10, en cuyo caso el umbral del número de renegociaciones de la conexión TCP se establece a 10. Cuando el número de renegociaciones en la conexión TCP supera el valor de 10 dentro de una hora, la conexión TCP se considera como una conexión anormal. Por supuesto, puede entenderse que el umbral del número de renegociaciones se determina en conformidad con un valor empírico del número normal de negociaciones que pueden existir en una conexión TCP normal en una aplicación real.

Etapa 406: Enviar un paquete de reposición a un cliente cuya dirección IP origen apunta a la conexión TCP, enviar un paquete de reposición a un servidor al que apunta la dirección IP de destino en la conexión TCP, desconectar, mediante los paquetes de reposición, la conexión TCP entre el cliente y el servidor e iniciar la etapa 407.

En esta forma de realización, cuando se determina que una conexión TCP es una conexión anormal, la conexión TCP puede desconectarse, con el fin de impedir que un intruso realice un ataque de tipo SSL DOS sobre el servidor SSL por intermedio de la conexión TCP. La conexión TCP puede desconectarse enviando paquetes RST. En esta etapa, después de que se determine que una conexión TCP es una conexión anormal, se envía un paquete RST a un cliente cuya dirección IP origen apunta a la conexión TCP. El cliente desconecta automáticamente la conexión TCP correspondiente después de recibir el paquete RST y el servidor desconecta automáticamente la conexión TCP correspondiente después de recibir el paquete RST, de modo que la conexión TCP entre el cliente y el servidor SSL se desconecte por intermedio de los paquetes RST.

Etapa 407: Contar el número de conexiones anormales iniciadas por el cliente en la conexión TCP e iniciar la etapa 408.

Después de que se determine que la conexión TCP es una conexión anormal y se desconecte la conexión TCP, puede realizarse una supervisión sobre la dirección IP del cliente en la conexión TCP, con el fin de determinar, además, si el cliente en la conexión TCP es un intruso atacante. Más concretamente, puede establecerse una tabla de supervisión de conexiones anormales. La tabla de supervisión de conexiones anormales registra el número de las conexiones anormales iniciadas por el cliente. En esta forma de realización, después de que se determine que la conexión TCP es una conexión anormal, si la conexión TCP es una primera conexión anormal iniciada por el cliente en la conexión TCP, resulta necesario establecer una tabla de supervisión de conexiones anormales, con el fin de supervisar la dirección IP del cliente en la conexión TCP y contar el número de conexiones anormales iniciadas por el cliente. Por supuesto, si la conexión TCP no es la primera conexión anormal iniciada por el cliente, el número de las conexiones anormales iniciadas por el cliente puede actualizarse en la tabla de supervisión de conexiones anormales. Debe entenderse que la operación de contar el número de conexiones anormales iniciadas por el cliente en la conexión TCP es también contar el número de las conexiones anormales dentro de un período de conteo establecido. Más concretamente, cuando se determina la presencia de una conexión anormal, se puede registrar una marca temporal, se determina un período de conteo en función de las marcas temporales registradas y se cuenta el número de conexiones anormales dentro del período de conteo establecido. Además, en esta forma de realización, cuando se detecta que una determinada conexión TCP es una conexión anormal, el resultado de la detección puede registrarse también como información de registro en un registro para su uso en una consulta posterior.

Etapa 408: Determinar si el número de las conexiones anormales iniciadas por el cliente en la conexión TCP es superior que un umbral preestablecido del número de conexiones; si la respuesta es afirmativa, realizar la etapa 409, de no ser así, volver a realizar la etapa 400.

Si el número contado de las conexiones anormales iniciadas por el cliente en la conexión TCP es superior al umbral preestablecido del número de conexiones se determina a este respecto. Si la respuesta es afirmativa, realizar la etapa 409 y añadir la dirección IP del cliente en la lista negra; de no ser así, volver a realizar la etapa 400 y continuar recibiendo un paquete enviado por el cliente.

Etapa 409: Añadir la dirección IP del cliente en la lista negra.

Cuando el número contado de conexiones anormales iniciadas por el cliente en la tabla de supervisión de conexiones anormales es superior que el umbral preestablecido del número de conexiones, ello indica que el cliente puede ser un intruso atacante y la dirección IP del cliente se añade a la lista negra, con el fin de actualizar dinámicamente dicha lista negra. En la siguiente ocasión en que se reciba un paquete enviado desde la dirección IP, el paquete puede desecharse directamente, o iniciarse una conexión TCP por la dirección IP que se puede desconectar también de forma directa, con lo que se mejora la eficiencia de la detección. En esta forma de realización, cuando se detecta que una determinada dirección IP se añade a la lista negra, el resultado de la detección puede registrarse también como información de registro en un registro para uso en una consulta posterior.

Etapa 410: Desechar el paquete.

Cuando se recibe un paquete desde el cliente, y si el paquete no accede a una sesión o una dirección IP origen del paquete está en la lista negra, se desecha el paquete.

Esta forma de realización da a conocer un método de defensa contra los ataques. Después de que se reciba un paquete enviado por un cliente, en primer lugar, se determina si el paquete accede a una sesión; si la sesión es objeto de acceso, si una dirección IP del cliente está en una lista negra sigue determinándose en función del paquete recibido; si la dirección IP no está en la lista negra y el número contado de renegociaciones en una conexión TCP es superior a un umbral del número de renegociaciones, se determina que la conexión TCP es una conexión anormal, se desconecta la conexión TCP, y el número de conexiones anormales iniciadas por el cliente en la conexión TCP se registra en una tabla de supervisión de conexiones anormales establecida; y cuando el número de las conexiones anormales iniciadas por el cliente en la conexión TCP supera un umbral preestablecido del número de conexiones, la dirección IP del cliente se añade en la lista negra, con el fin de actualizar la lista negra establecida a su debido tiempo, con lo que no solamente es capaz de impedir al cliente inicial un ataque del tipo SSL DOS sobre un servidor, sino que también es capaz de mejorar la eficiencia de la defensa.

Los expertos en esta técnica deben entender que la totalidad o parte de las etapas del método en las formas de realización pueden ponerse en práctica por un programa que da instrucciones a un hardware pertinente. El programa puede memorizarse en un soporte de memorización legible por ordenador. Cuando se ejecuta el programa, se realizan las etapas anteriores del método en la forma de realización. El soporte de memorización puede ser cualquier soporte capaz de memorizar códigos de programa, tal como una memoria ROM, una memoria RAM, un disco magnético o un disco óptico y similares.

La Figura 5 es un diagrama estructural esquemático de un dispositivo de defensa contra los ataques en conformidad con una forma de realización de la presente invención. Según se ilustra en la Figura 5, esta forma de realización da a conocer un dispositivo de defensa contra los ataques 50. El dispositivo de defensa contra los ataques 50 puede utilizarse para defensa contra un comportamiento de ataque del tipo de denegación de servicio (Denial of service, en adelante referido como DOS en forma abreviada) de una capa de conexión segura (Secure Socket Layer, en adelante referida como SSL en forma abreviada). El dispositivo de defensa contra los ataques 50 puede incluir un primer módulo de conteo 501, un módulo de determinación de conexión anormal 502 y un módulo de procesamiento 503.

El primer módulo de conteo 501 está configurado para contar el número de renegociaciones en una conexión de protocolo de control de transmisión (Transmission Control Protocol, en adelante referida como TCP en forma abreviada) en donde el número de las renegociaciones es el número de negociaciones repetidas entre un cliente y un servidor en la conexión TCP.

Un paquete de negociaciones de un tipo de cambio de especificación de cifrado, Change Cipher Spec, existe junto con cada proceso de negociación clave entre un cliente y un servidor SSL en una conexión TCP, en donde una primera negociación es una negociación normal y la otra no primera negociación es una negociación repetida; de este modo, el número de las renegociaciones en la conexión TCP que se cuentan por el primer módulo de conteo 501 puede identificarse contando el número de paquetes de negociaciones del tipo de cambio de especificación de cifrado, Change Cipher Spec, que se intercambian entre el cliente y el servidor SSL en la conexión TCP. Más concretamente, el número de las renegociaciones en la conexión TCP puede obtenerse restando 1 del número de paquetes de negociaciones en la conexión TCP dentro de un tiempo preestablecido. Más concretamente en una aplicación real, cuando el primer módulo de conteo 501 cuenta el número de renegociaciones en la conexión TCP dentro del tiempo preestablecido, puede prestablecerse un período de conteo. Es decir, el número de renegociaciones dentro del período de conteo preestablecido se cuenta a este respecto. En una aplicación real, el período de conteo puede establecerse a 30 segundos o 1 minuto. El establecimiento del tiempo específico puede realizarse de conformidad con un requerimiento de servicio real y puede determinarse también en función del tráfico de la red. Durante el conteo, cuando se recibe un paquete de negociaciones, el número de paquetes de negociaciones se registra una vez y se registra también una marca temporal, de modo que cuando se reciba un paquete de negociaciones posteriormente, pueda determinase un período de conteo en función de la marca temporal anteriormente registrada, y el número de renegociaciones dentro del período de conteo puede contarse de conformidad con el período de conteo determinado. A modo de ejemplo, cuando se recibe un primer paquete de

negociaciones, el número del paquete de negociación se registra como 1 y se registra también una marca temporal, y cuando se recibe un segundo paquete de negociaciones, se añade 1 al número del paquete de negociaciones, y se registra una segunda marca temporal, de modo que el número de paquetes de negociaciones recibido dentro de este período de tiempo pueda determinarse en conformidad con las dos marcas temporales registradas.

El módulo de determinación de conexión anormal 502 está configurado para, cuando el número de renegociaciones en la conexión TCP que se cuentan por el primer módulo de conteo 501 es superior que un umbral preestablecido del número de renegociaciones, determinar que la conexión TCP es una conexión anormal.

Más concretamente, el umbral del número de renegociaciones es un número máximo preestablecido de renegociaciones permitidas dentro de un tiempo determinado en una conexión TCP. En un caso real, el número de renegociaciones en una conexión TCP dentro de un período preestablecido no supera el umbral del número de renegociaciones; cuando el número de renegociaciones supera el umbral del número de renegociaciones, ello indica que un proceso de renegociación en la conexión TCP puede ser un ataque iniciado por un intruso malintencionado exterior y luego, el módulo de determinación de conexión anormal 502 determina que la conexión TCP es una conexión anormal. En una aplicación real, el umbral del número de renegociaciones puede establecerse en conformidad con un requerimiento de servicio o un tráfico de la red. A modo de ejemplo, el umbral del número de renegociaciones puede establecerse a tres veces por treinta segundos (3 veces/30 s).

El módulo de procesamiento 503 está configurado para, cuando el módulo de determinación de conexión anormal 502 determina que la conexión TCP es una conexión anormal, desconectar la conexión TCP.

Más concretamente, cuando el módulo de determinación de conexión anormal 502 determina que la conexión TCP es una conexión anormal, con el fin de garantizar que el servidor esté protegido del ataque de un intruso, se desconecta la conexión TCP.

El dispositivo de defensa contra los ataques 50 dado a conocer en estas formas de realización puede realizar específicamente las etapas pertinentes en las formas de realización del método ilustradas en la Figura 2 a la Figura 4.

El dispositivo de defensa contra los ataques en la forma de realización de la presente invención, de conformidad con una característica de que un ataque del tipo SSL DOS se realiza por un intruso consumiendo recursos de CPU del servidor mediante la negociación continua de una clave en una conexión TCP establecida con el servidor de forma repetida, cuenta el número de renegociaciones en la conexión TCP, de termina que la conexión TCP es una conexión anormal cuando el número contado de renegociaciones en la conexión TCP es superior a un umbral del número de renegociaciones, y desconecta la conexión TCP, con lo que se realiza efectivamente una defensa contra un comportamiento de ataque del tipo SSL DOS y se protege al servidor del ataque de SSL DOS.

La Figura 6 es un diagrama estructural esquemático de otro dispositivo de defensa contra los ataques en conformidad con una forma de realización de la presente invención. Según se ilustra en la Figura 6, esta forma de realización da a conocer un dispositivo de defensa contra los ataques 60, que puede realizar específicamente etapas pertinentes en las formas de realización del método que se ilustran en la Figura 2 a la Figura 4, por lo que no se describe aquí de nuevo en detalle. Sobre la base de la forma de realización ilustrada en la Figura 5, el dispositivo de defensa contra los ataques 60 dado a conocer en esta forma de realización puede incluir, además, un módulo de determinación 601.

El módulo de determinación 601 está configurado para determinar si una dirección IP del cliente en la conexión TCP está incluida en una lista negra, en donde la lista negra incluye una dirección IP de un cliente que inicia una conexión anormal, iniciar el primer módulo de conteo 501 cuando la dirección IP del cliente no está en la lista negra, e iniciar el módulo de procesamiento 503 cuando la dirección IP del cliente está en la lista negra.

Más concretamente, una lista negra de intrusos de ataque puede prestablecerse en el dispositivo de defensa contra los ataques. La lista negra incluye una dirección IP detectada de un intruso atacante, en donde el dispositivo de defensa contra los ataques, en esta forma de realización, puede ser un producto de pasarela tal como un enrutador o un cortafuegos, o puede ser un dispositivo de red tal como un dispositivo de limpieza de DDOS. Cuando se recibe un paquete enviado por el cliente, el módulo de determinación 601 puede determinar, en conformidad con una dirección IP origen incluida en el paquete, si la dirección IP del cliente en la conexión TCP está en la lista negra prestablecida; si no es así, iniciar el primer módulo de conteo 501, de no ser así, iniciar el módulo de procesamiento 503 y desconectar directamente la conexión TCP con lo que se mejora la eficiencia de la defensa contra los ataques.

Además, el dispositivo de defensa contra los ataques dado a conocer en esta forma de realización puede incluir, además, un segundo módulo de conteo 602 y un módulo de gestión 603.

El segundo módulo de conteo 602 está configurado para contar el número de conexiones anormales iniciadas por el cliente en la conexión TCP.

Más concretamente, se puede establecer una tabla de supervisión de conexiones anormales en el dispositivo de defensa contra los ataques, y se utiliza para contar el número de conexiones anormales iniciadas por el cliente. La tabla de supervisión de conexiones anormales registra una dirección IP de un cliente y el número de conexiones anormales iniciadas por el cliente al que apunta la dirección IP. Más concretamente, después de que el módulo de determinación de conexión anormal 502 determina que una determina conexión TCP es una conexión anormal, el segundo módulo de conteo 602 puede buscar en la tabla de supervisión de conexiones anormales una dirección IP que sea la misma que una dirección IP de un cliente en la conexión TCP y contar el número de conexiones anormales bajo la dirección IP. Más concretamente, si la dirección IP que es la misma que la dirección IP del cliente se encuentra, el segundo módulo de conteo 602 añade 1 al número de conexiones anormales correspondiente a la dirección IP. Si no se encuentra la misma dirección IP, el segundo módulo de conteo 602 añade un nuevo registro en la tabla de supervisión de conexiones anormales, registra la dirección IP y registra el número de conexiones anormales correspondiente a la dirección IP como 1.

Puede entenderse que el conteo del número de conexiones anormales iniciadas por el cliente en la conexión TCP se refiere también a contar el número de conexiones anormales dentro de un período de conteo establecido. Más concretamente, cuando se determina una conexión anormal, puede registrarse una marca temporal, se determina un período de conteo en conformidad con las marcas temporales registradas y es objeto de conteo el número de conexiones anormales dentro del período de conteo establecido. Para un método de conteo específico, puede hacerse referencia a la descripción de las formas de realización del método antes citadas, por lo que no se describe aquí de nuevo en detalle.

El módulo de gestión 603 está configurado para, cuando el número de conexiones anormales iniciadas por el cliente en la conexión TCP que es objeto de conteo por el segundo módulo de conteo 602 es superior a un umbral preestablecido del número de conexiones, añadir la dirección IP del cliente a la lista negra.

En este caso, el umbral del número de conexiones puede ser un número máximo de conexiones anormales iniciadas por un cliente al que apunta la dirección IP para que se permita dentro de un período preestablecido. En una aplicación real, el umbral del número de conexiones puede establecerse en conformidad con un requerimiento de servicio o un tráfico de la red. A modo de ejemplo, el umbral del número de conexiones puede establecerse a tres veces por treinta segundos (3 veces/30 s). Cuando el número de conexiones anormales iniciadas por el cliente en la conexión TCP que es objeto de conteo por el segundo módulo de conteo 602 es superior al umbral preestablecido del número de conexiones, el módulo de gestión 603 determina que el cliente es un intruso atacante, y añade la dirección IP del cliente a la lista negra, con el fin de actualizar dinámicamente la lista negra. En este caso, en la siguiente ocasión en que se reciba un paquete enviado desde la dirección IP, el paquete puede desecharse directamente, o se puede desconectar directamente una conexión TCP iniciada por la dirección IP, con lo que se mejora la eficiencia de la detección.

Además, en otra puesta en práctica, el primer módulo de conteo 501 puede incluir específicamente una unidad de identificación 511 y una unidad de conteo 521.

La unidad de identificación 511 está configurada para, mediante un tipo de un paquete intercambiado entre el cliente y el servidor en la conexión TCP, identificar si el paquete es un paquete de negociación o no lo es.

El paquete de negociaciones identificado en la unidad de identificación 511 de esta forma de realización incluye un paquete del tipo de cambio de especificación de cifrado, Change Cipher Spec. Más concretamente, un paquete de negociaciones del tipo de cambio de especificación de cifrado, Change Cipher Spec, existe junto con cada proceso de renegociación entre el cliente y el servidor SSL en una conexión TCP, en donde una primera negociación es una negociación normal y la otra no primera negociación es una negociación repetida; por lo tanto, la unidad de identificación 511 puede identificar si el paquete es un paquete de negociaciones, determinando si el tipo del paquete intercambiado entre el cliente y el servidor es del tipo Change Cipher Spec .

La unidad de conteo 521 está configurada para contar el número de renegociaciones en la conexión TCP en conformidad con el número de paquetes de negociaciones en la conexión TCP que se identifican por la unidad de identificación 511.

En una aplicación real, el número de las renegociaciones en la conexión TCP puede obtenerse contando el número de paquetes de negociaciones del tipo Change Cipher Spec que se intercambian entre el cliente y el servidor SSL en la conexión TCP. Más concretamente, la unidad de conteo 521 puede obtener el número de las renegociaciones en la conexión TCP restando 1 del número de paquetes de negociaciones del tipo Change Cipher Spec dentro de un tiempo preestablecido. A modo de ejemplo, si el número de paquetes de negociaciones del tipo Change Cipher Spec que aparecen en una determina conexión TCP dentro de una hora es 10, puede obtenerse que el número de renegociaciones en la conexión TCP dentro de una hora es 9.

Además, en otro caso, el dispositivo de defensa contra los ataques 60 puede incluir, además.

un módulo de recepción 600, configurado para recibir un paquete enviado por un cliente.

El módulo de determinación 601 está configurado, además, para determinar si el paquete recibido por el módulo de recepción 600 accede a una sesión; si la sesión es objeto de acceso, continuar determinando si una dirección IP del cliente del paquete recibido está en una lista negra; si la respuesta es afirmativa, iniciar operativamente el módulo de procesamiento 503 y en caso contrario, iniciar el primer módulo de conteo 501.

El dispositivo de defensa contra los ataques dado a conocer en esta forma de realización, después de recibir un paquete enviado por un cliente, determina, en primer lugar, mediante un módulo de determinación, si el paquete accede a una sesión, si la sesión es objeto de acceso, continuar determinando, en función del paquete recibido, si una dirección IP del cliente está en una lista negra o no lo está; si la dirección IP no está en la lista negra y el número contado de renegociaciones en una conexión TCP es superior a un umbral del número de renegociaciones, determina que la conexión TCP es una conexión anormal, desconecta la conexión TCP, registra el número de conexiones anormales iniciadas por el cliente en la conexión TCP en una tabla de supervisión de conexiones anormales establecida, y cuando el número de las conexiones anormales iniciadas por el cliente en la conexión TCP supera un umbral preestablecido del número de conexiones, añade la dirección IP del cliente en la lista negra, con el fin de actualizar la lista negra establecida a su debido tiempo, con lo que no solamente es capaz de impedir que el cliente tenga una dirección IP real que tenga su iniciación en un ataque de tipo SSL DOS en un servidor SSL, sino que también es capaz de impedir que un intruso inicie un ataque sobre el servidor mediante una dirección IP virtual. Más adelante, el paquete recibido se filtra mediante la lista negra establecida, con lo que se mejora la eficiencia de la defensa.

La Figura 7 es un diagrama estructural esquemático de otro dispositivo de defensa contra los ataques en conformidad con una forma de realización de la presente invención. El dispositivo de defensa contra los ataques puede ser un enrutador, un cortafuegos o un dispositivo de limpieza de DDOS y puede ser también un servidor host que incluye una capacidad de defensa contra los ataques. La forma de realización específica de la presente invención no limita la puesta en práctica específica del dispositivo de defensa contra los ataques. Según se ilustra en la Figura 7, el dispositivo de defensa contra los ataques puede incluir:

un procesador (processor) 710, una interfaz de comunicaciones (Communications Interface) 720, una memoria (memory) 730 y un bus de comunicaciones 740.

El procesador 710, la interfaz de comunicaciones 720 y la memoria 730 se comunican entre sí por intermedio del bus de comunicaciones 740.

La interfaz de comunicaciones 720 está configurada para la comunicación con un elemento de red, tal como un cliente o un servidor SSL.

El procesador 710 está configurado para realizar un programa 732 y más concretamente, puede realizar las etapas pertinentes en las formas de realización del método ilustradas en la Figura 2 a la Figura 4.

Más concretamente, el programa 732 puede incluir códigos de programa, y los códigos de programa incluyen una instrucción de operación informática.

El procesador 710 puede ser una unidad central de procesamiento CPU, un circuito integrado específico de la aplicación ASIC (Application Specific Integrated Circuit) o uno o más circuitos integrados configurados para poner en práctica las formas de realización de la presente invención.

La memoria 730 está configurada para memorizar el programa 732. La memoria 730 puede incluir una memoria RAM de alta velocidad y puede incluir, además, una memoria no volátil (non-volatile memory), a modo de ejemplo, al menos una memoria de disco magnético. El programa 732 puede incluir, concretamente.

un primer módulo de conteo, configurado para contar el número de renegociaciones en una conexión TCP, en donde el número de las renegociaciones es el número de negociaciones repetidas entre un cliente y un servidor en la conexión TCP;

un módulo de determinación de conexión anormal configurado para, cuando el número de renegociaciones en la conexión TCP que se cuentan por el primer módulo de conteo es superior a un umbral preestablecido del número de renegociaciones, determinar que la conexión TCP es una conexión anormal; y

un módulo de procesamiento, configurado para, cuando el módulo de determinación de conexión anormal determina que la conexión TCP es una conexión anormal, desconectar la conexión TCP.

Para la puesta en práctica específica de cada módulo en el programa 732, puede hacerse referencia a los módulos correspondientes en las formas de realización ilustradas en la Figura 5 a la Figura 6, por lo que no se describe aquí de nuevo en detalle.

Puede entenderse claramente por expertos en esta técnica que, para la finalidad de una descripción breve y adecuada, en cuanto a un proceso de trabajo específico del dispositivo anterior y del módulo, puede hacerse referencia al proceso correspondiente en las formas de realización del método anteriores y por ello aquí no se describen aquí de nuevo en detalle.

En las formas de realización dadas a conocer en la presente solicitud, debe entenderse que el dispositivo y el método dados a conocer pueden ponerse en práctica en otras maneras. A modo de ejemplo, la forma de realización del dispositivo descrita con anterioridad es simplemente a modo de ejemplo. Por ejemplo, la división de unidades es simplemente una división de funciones lógicas y pueden ser otras maneras de división en las aplicaciones reales. A modo de ejemplo, una pluralidad de unidades o componentes pueden combinarse o pueden integrarse con otro sistema, o algunas características pueden ignorarse o no realizarse. Además, los acoplamientos mutuos ilustrados o examinados o los acoplamientos directos o conexiones de comunicaciones pueden realizarse mediante algunas interfaces. Los acoplamientos indirectos o las conexiones de comunicaciones entre aparatos o unidades pueden realizarse en una forma eléctrica, forma mecánica u otras formas.

Las unidades descritas como partes separadas pueden estar, o no, físicamente separadas, y las partes mostradas como unidades pueden ser, o no, unidades físicas, pueden estar situadas en una sola posición o pueden distribuirse en una pluralidad de unidades de red. Una parte o la totalidad de los módulos puede seleccionarse en función de las necesidades reales para conseguir los objetivos de las soluciones de las formas de realización.

Además, las unidades funcionales en las formas de realización de la presente invención pueden integrarse en un solo módulo de procesamiento o cada uno de los módulos puede existir por sí solo físicamente o dos o más módulos se integran en un módulo.

Por último, conviene señalar que las formas de realización anteriores están simplemente previstas para describir las soluciones técnicas de la presente invención y no para limitar el alcance de la presente invención. Aunque la presente invención se describe en detalle haciendo referencia a las formas de realización anteriores, los expertos en esta técnica deben entender que pueden realizarse modificaciones a las soluciones técnicas descritas en las formas de realización anteriores o realizar sustituciones equivalentes para algunas o la totalidad de sus características técnicas; no constituyendo dichas modificaciones o sustituciones una parte esencial de las soluciones técnicas correspondientes ni por ello desviarse del alcance de las soluciones técnicas de las formas de realización de la presente invención.

REIVINDICACIONES

1. Un método de defensa contra los ataques, que comprende:

supervisar una conexión de protocolo de control de transmisión, TCP, establecida entre un cliente y un servidor SSL;

contar (201, 301, 403) un número de renegociaciones en la conexión TCP, en donde el número de las renegociaciones es un número de negociaciones repetidas entre el cliente y el servidor en la conexión TCP;

cuando el número de renegociaciones en la conexión TCP es superior a un umbral preestablecido del número de renegociaciones, determinar (202, 302, 405) que la conexión TCP es una conexión anormal; y

desconectar (203, 303) la conexión TCP;

en donde el método comprende, además:

determinar (300, 402) si una dirección IP del cliente en la conexión TCP está incluida en una lista negra establecida, en donde la lista negra comprende una dirección IP de un cliente que inicia una conexión anormal;

cuando la dirección IP del cliente no está en la lista negra, introducir la etapa de contar (301, 403) el número de renegociaciones en la conexión TCP; y

cuando la dirección IP del cliente está en la lista negra, desconectar (303) la conexión TCP.

2. El método según la reivindicación 1, en donde la operación de contar el número de renegociaciones en la conexión TCP comprende:

a través de un tipo de un paquete intercambiado entre el cliente y el servidor en la conexión TCP, identificar si el paquete es un paquete de negociación; y

contar el número de renegociaciones en la conexión TCP en conformidad con el número de paquetes de negociación en la conexión TCP.

3. El método según la reivindicación 2, en donde el paquete de negociaciones comprende un paquete del tipo de cambio de especificación de cifrado Change Cipher Spec.

4. El método según la reivindicación 1, en donde la operación de contar el número de renegociaciones en la conexión TCP comprende:

obtener el número de las renegociaciones en la conexión TCP contando el número de paquetes de negociaciones de un tipo de cambio de especificación de cifrado Change Cipher Spec que se intercambia entre el cliente y un servidor SSL en la conexión TCP.

5. El método según cualquiera de las reivindicaciones 1 a 4, que comprende, además:

contar (304) el número de conexiones anormales iniciadas por el cliente; y

cuando el número de las conexiones anormales iniciado por el cliente es superior a un umbral preestablecido del número de conexiones, añadir (305) la dirección IP del cliente en la lista negra.

6. El método según cualquiera de las reivindicaciones 1 a 5, en donde el método de defensa contra los ataques se utiliza para la defensa contra un comportamiento de ataque por denegación de servicio, DOS, de la capa de conexión segura, SSL.

7. Un dispositivo de defensa contra los ataques que comprende:

un módulo configurado para supervisar una conexión de protocolo de control de transmisión, TCP, establecida entre un cliente y un servidor SSL;

un primer módulo de conteo (501), configurado para contar un número de renegociaciones en la conexión TCP, en donde el número de renegociaciones es un número de negociaciones repetidas entre el cliente y el servidor en la conexión TCP;

un módulo de determinación de conexión anormal (502) configurado para, cuando el número de las renegociaciones en la conexión TCP es superior a un umbral preestablecido del número de renegociaciones, determinar que la conexión TCP es una conexión anormal; y

un módulo de procesamiento (503), configurado para desconectar la conexión TCP;

en donde el dispositivo de defensa contra los ataques comprende, además:

un módulo de determinación (601), configurado para determinar si una dirección IP del cliente en la conexión TCP está incluida en una lista negra, en donde la lista negra comprende una dirección IP de un cliente que inicia una conexión anormal, iniciar operativamente el primer módulo de conteo (501) cuando la dirección IP del cliente no está incluida en la lista negra, e iniciar el módulo de procesamiento (503) cuando la dirección IP del cliente está incluida en la lista negra.

8. El dispositivo de defensa contra los ataques según la reivindicación 7, en donde el primer módulo de conteo comprende:

una unidad de identificación (511), configurada para, a través de un tipo de un paquete intercambiado entre el cliente y el servidor en la conexión TCP, identificar si el paquete es un paquete de negociación; y

una unidad de conteo (521), configurada para contar el número de las renegociaciones en la conexión TCP en conformidad con el número de paquetes de negociación en la conexión TCP que se identifican por la unidad de identificación.

9. El dispositivo de defensa contra los ataques según la reivindicación 8, en donde el paquete de negociación comprende un paquete de un tipo de cambio de especificación de cifrado Change Cipher Spec.

10. El dispositivo de defensa contra los ataques según la reivindicación 7, en donde el primer módulo de conteo (501) está concretamente configurado para obtener el número de las renegociaciones en la conexión TCP contando el número de paquetes de negociación de un tipo de cambio de especificación de cifrado Change Cipher Spec que se intercambia entre el cliente y un servidor SSL en la conexión TCP.

11. El dispositivo de defensa contra los ataques según cualquiera de las reivindicaciones 7 a 10 que comprende, además:

un segundo módulo de conteo (602), configurado para contar el número de conexiones anormales iniciadas por el cliente en la conexión TCP; y

un módulo de gestión (603), configurado para, cuando el número de las conexiones anormales iniciadas por el cliente en la conexión TCP que se cuentan por el segundo módulo de conteo (602) es superior a un umbral preestablecido del número de conexiones, añadir la dirección IP del cliente en la lista negra.

12. El dispositivo de defensa contra los ataques según cualquiera de las reivindicaciones 7 a 11, en donde el dispositivo de defensa contra los ataques se utiliza para la defensa contra un comportamiento de ataque del tipo de denegación de servicio DOS de la capa de conexión segura SSL.

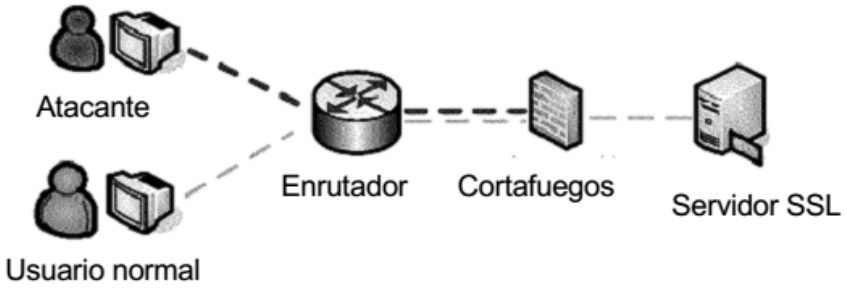
Atacante
Usuario normal
Enrutador
Cortafuegos
Servidor SSL

FIG. 1

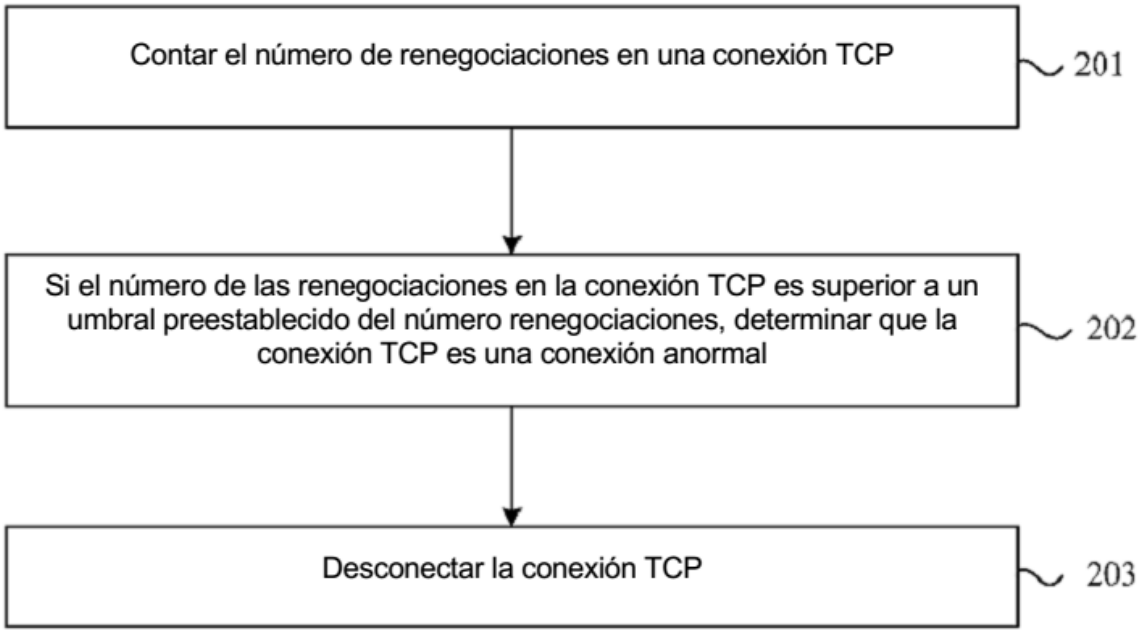
Contar el número de renegociaciones en una conexión TCP
201
Si el número de las renegociaciones en la conexión TCP es superior a un umbral preestablecido del número renegociaciones, determinar que la conexión TCP es una conexión anormal
202
Desconectar la conexión TCP
203

FIG. 2

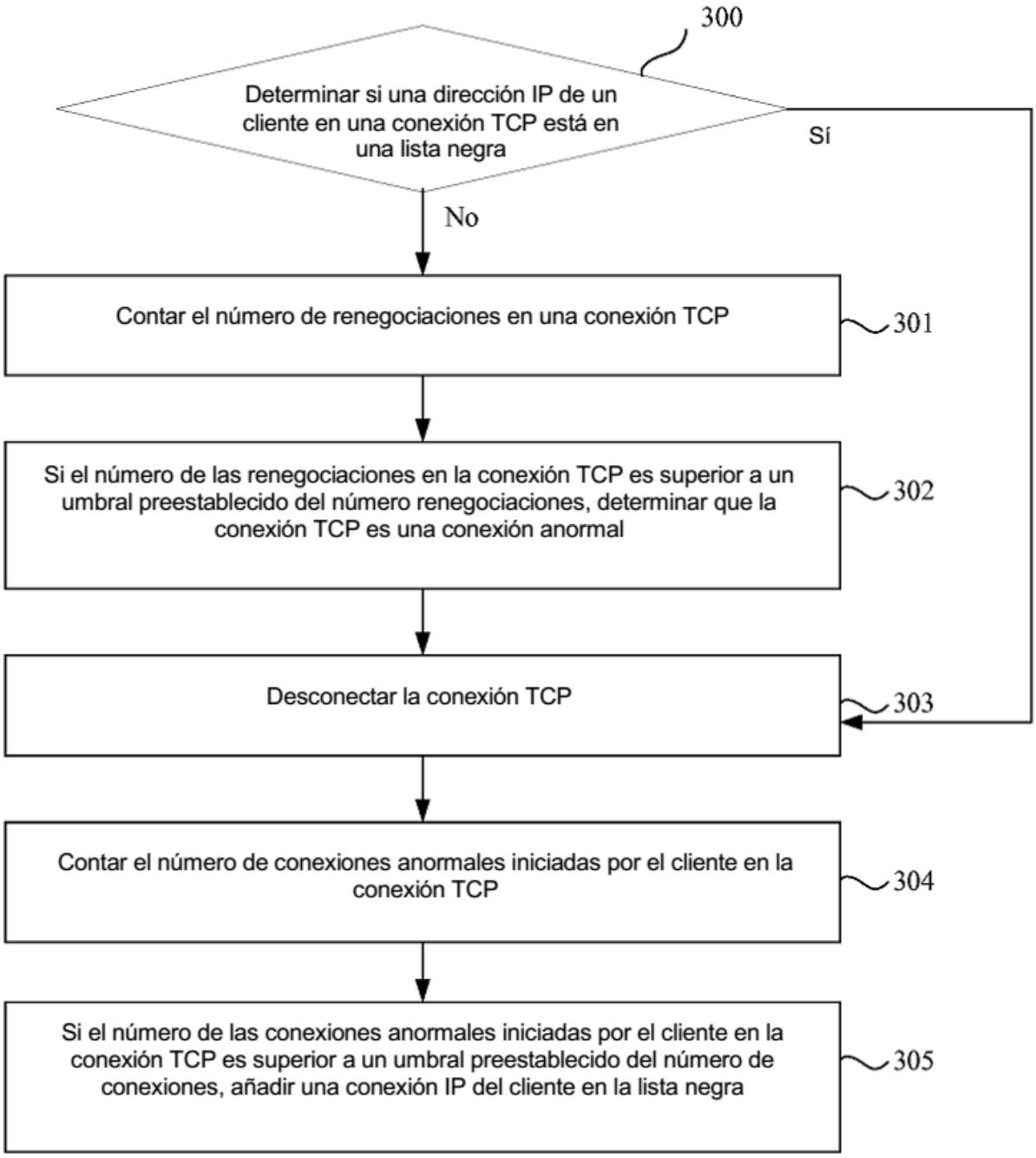
300
Determinar si una dirección IP de un cliente en una conexión TCP está en una lista negra
Sí
No
Contar el número de renegociaciones en una conexión TCP
301
Si el número de las renegociaciones en la conexión TCP es superior a un umbral preestablecido del número renegociaciones, determinar que la conexión TCP es una conexión anormal
302
Desconectar la conexión TCP
303
Contar el número de conexiones anormales iniciadas por el cliente en la conexión TCP
304
Si el número de las conexiones anormales iniciadas por el cliente en la conexión TCP es superior a un umbral preestablecido del número de conexiones, añadir una conexión IP del cliente en la lista negra
305

FIG. 3

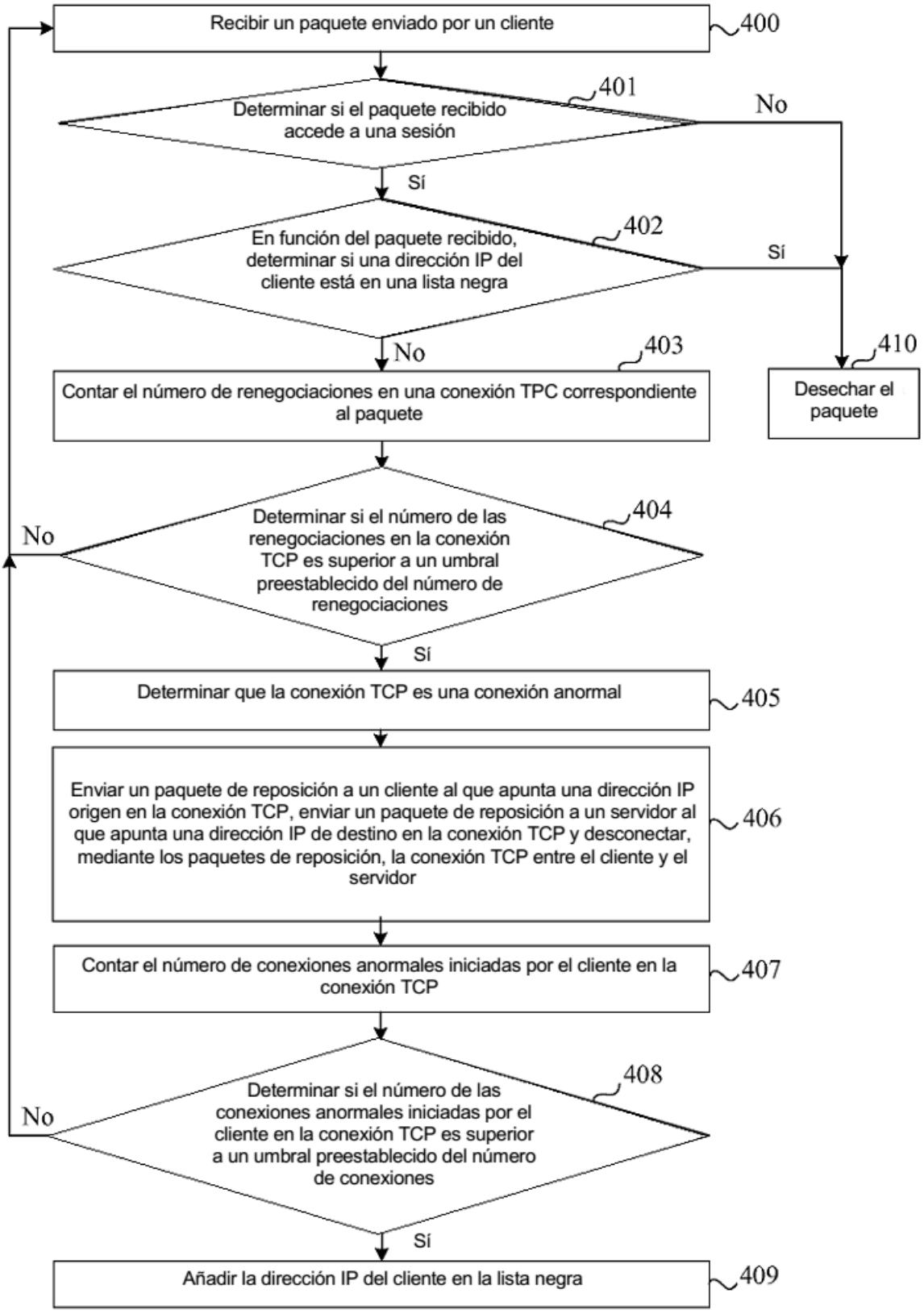
Recibir un paquete enviado por un cliente
400
Determinar si el paquete recibido accede a una sesión
401
No
Sí
En función del paquete recibido, determinar si una dirección IP del cliente está en una lista negra
402
Sí
No
Contar el número de renegociaciones en una conexión TPC correspondiente al paquete
403
Desechar el paquete
410
Determinar si el número de las renegociaciones en la conexión TCP es superior a un umbral preestablecido del número de renegociaciones
404
No
Sí
Determinar que la conexión TCP es una conexión anormal
405
Enviar un paquete de reposición a un cliente al que apunta una dirección IP origen en la conexión TCP, enviar un paquete de reposición a un servidor al que apunta una dirección IP de destino en la conexión TCP y desconectar, mediante los paquetes de reposición, la conexión TCP entre el cliente y el servidor
406
Contar el número de conexiones anormales iniciadas por el cliente en la conexión TCP
407
Determinar si el número de las conexiones anormales iniciadas por el cliente en la conexión TCP es superior a un umbral preestablecido del número de conexiones
408
No
Sí
Añadir la dirección IP del cliente en la lista negra
409

FIG. 4

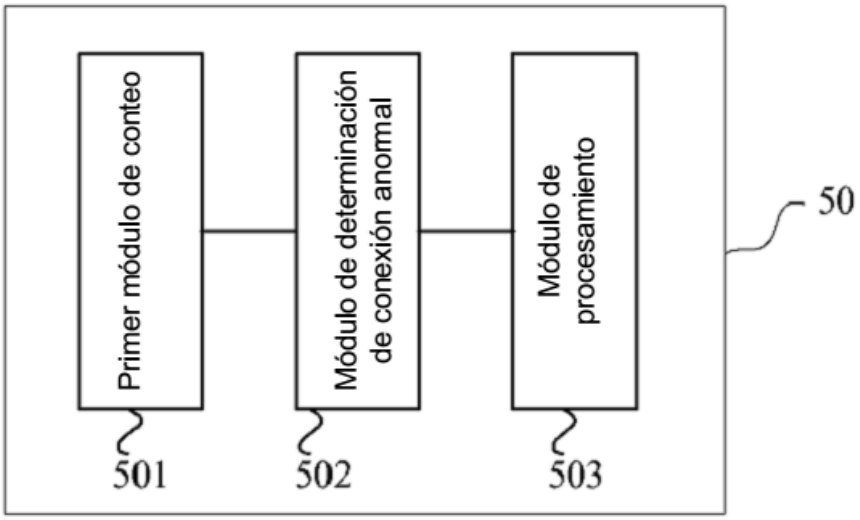
Primer módulo de conteo
Módulo de determinación de conexión anormal
Módulo de procesamiento
50
501
502
503

FIG. 5

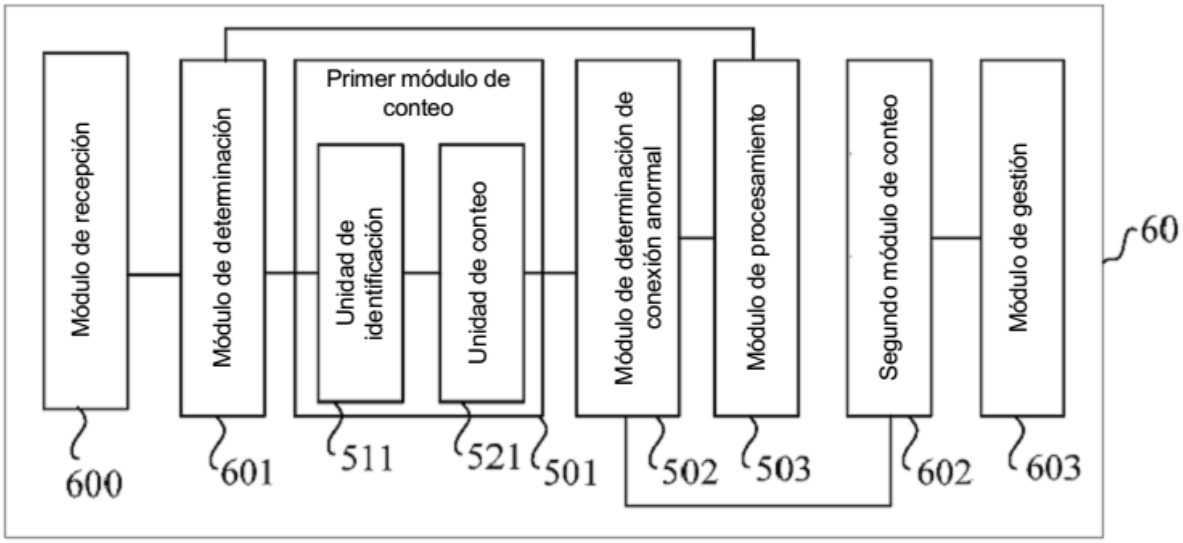
Módulo de recepción
Módulo de determinación
Primer módulo de conteo
Unidad de identificación
Unidad de conteo
Módulo de determinación de conexión anormal
Módulo de procesamiento
Segundo módulo de conteo
Módulo de gestión
60
600
601
511
521
501
502
503
602
603

FIG. 6

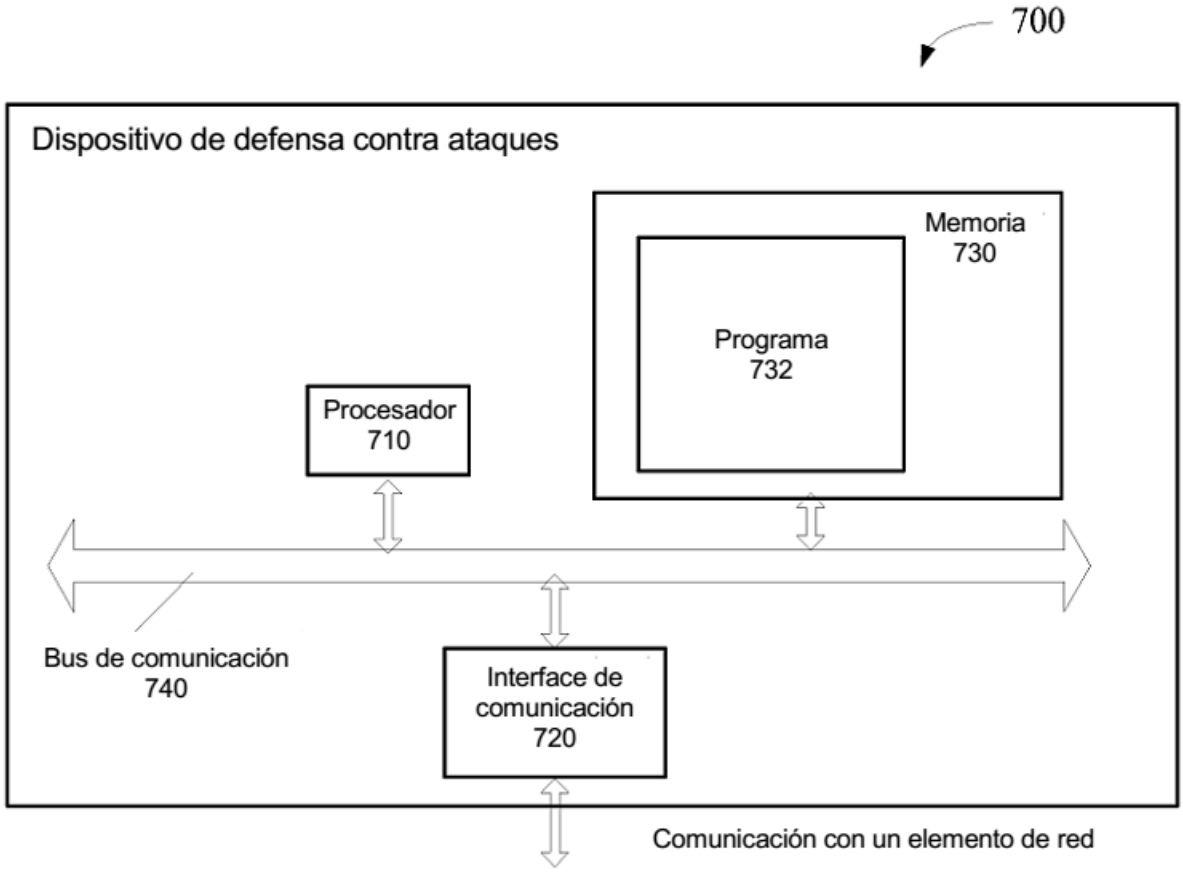
700
Dispositivo de defensa contra ataques
Memoria
730
Programa
732
Procesador
710
Bus de comunicación
740
Interface de
comunicación
720
Comunicación con un elemento de red

FIG. 7