(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 396 027**

(51) Int. CI.:

H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **15.04.2009 E 09749421 (5)**

(97) Fecha y número de publicación de la concesión europea: **07.11.2012 EP 2257024**

(54) Título: **Método, dispositivo de red y sistema de red para defenderse de un ataque de denegación distribuida de servicios**

(30) Prioridad:

23.05.2008 CN 200810067376

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
18.02.2013

(73) Titular/es:

CHENGDU HUAWEI SYMANTEC TECHNOLOGIES CO., LTD. (100.0%)
Qingshui River Zone West Hi-tech Zone Chengdu Sichuan 611731, CN

(72) Inventor/es:

LI, HONGXING

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

DESCRIPCIÓN

Método, dispositivo de red y sistema de red para defenderse de un ataque de denegación distribuida de servicios

Campo de la invención

La presente invención está relacionada con el campo de la tecnología de seguridad de las redes y, más en particular, con un método, un dispositivo de red y un sistema de red para defenderse de un ataque de Denegación Distribuida de Servicios (DDoS).

Antecedentes de la invención

El ataque DDoS utiliza principalmente el protocolo de Internet y las ventajas básicas de Internet, transfiriendo paquetes de datos desde cualquier fuente a cualquier destino sin desviación. El ataque DDoS puede ser clasificado en dos tipos: uno es para abrumar al dispositivo de red y al servidor con una gran cantidad de datos y tráfico alto, y el otro es para hacer una gran cantidad de peticiones incompletas que no pueden hacerse, a propósito, para agotar rápidamente los recursos del servidor.

El ataque DDoS es un tipo de ataque generado sobre la base del ataque DoS convencional. El ataque DDoS puede usar más ordenadores centrales marionetas para iniciar un ataque, y atacan a las víctimas a una escala mucho mayor que antes. Técnicamente, el ataque DDoS incluye una amenaza para la seguridad de los ordenadores en Internet y la colocación de programas de caballo troyano. Un gran número de programas de caballo troyano pueden iniciar un ataque simultáneamente en un momento especificado de una cierta manera, siguiendo las instrucciones de un servidor principal controlado por el atacante, para formar globalmente una vasta red de ataque Zombi.

Una característica importante del ataque DDoS es iniciar un ataque con muchos ordenadores centrales marioneta enviando una abundancia de paquetes de datos al lugar objetivo del ataque, de manera que destruyan, por ejemplo, el ancho de banda o la capacidad de transacción del lugar objetivo del ataque.

Con el fin de aliviar la presión del DDoS al objetivo atacado, se puede colocar un dispositivo de defensa antes del objetivo atacado. Cuando tiene lugar el ataque DDoS, el dispositivo defensor filtra automáticamente las corrientes de ataque, de manera que bloquean el ataque DDoS fuera del dispositivo de filtrado.

La detección de un ataque puede ser realizada individualmente por el dispositivo de defensa de DDoS, de acuerdo con las características del ataque DDoS, por ejemplo, cuando se considera que ocurre un ataque de SYN Flood (aluvión SYN, que es un tipo de ataque DDoS), si se detectan un gran número de paquetes SYN que excede un cierto umbral, independientemente de si el efecto del ataque sobre el objetivo atacado se lleva a cabo verdaderamente o no.

El dispositivo de defensa de DDoS puede filtrar los paquetes atacantes utilizando un método específico de acuerdo con el tipo de ataque, para filtrar un gran número de paquetes de ataque y permitir que los paquetes de acceso normales pasen a su través, suprimiendo con ello el ataque al objetivo atacado en cierta medida.

El documento US 2004148520 divulga un método para defenderse de los ataques DDoS contra una red de cliente, por medio de un sensor asociado con la red, el cual, al detectar un ataque, notifica a un motor de análisis en una red ISP con el fin de mitigar el ataque.

Debido a que la solución de defensa adopta un dispositivo independiente, solamente se detectan las características del tráfico de la red para determinar si tiene lugar o no un ataque. Para diferentes objetivos atacados, las características del ataque y el umbral para determinar un ataque no pueden ser definidas fácilmente. Por tanto, existen informes de errores y algunos ataques no son informados.

Sumario de la invención

Consecuentemente, la presente invención está dirigida a un método para defenderse de un ataque DDoS, que incluye los pasos siguientes:

Se detecta el estado en curso de un servidor en el lado del servidor, para determinar si está ocurriendo un ataque DDoS en el servidor. Se notifica a un limpiador de flujos de datos que necesita limpiar el flujo de datos de la red que fluye al servidor, si el ataque DDoS ocurre en el servidor.

La presente invención se dirige además a un dispositivo de red, que incluye un módulo de defensa contra ataques DDoS. El módulo incluye una unidad de detección y una unidad de notificación.

La unidad de detección está configurada para detectar el estado en curso del dispositivo de red en el lado del dispositivo de la red, para determinar si ocurre un ataque DDoS en el dispositivo de red.

La unidad de notificación está configurada para notificar a un limpiador de flujos de datos que el limpiador de flujos de datos necesita limpiar el flujo de datos de red que fluye hacia el dispositivo de red, si la unidad de detección detecta que ocurre un ataque DDoS en el dispositivo de red.

La presente invención está dirigida además a un sistema de red. El sistema de red incluye al menos un dispositivo de red y un limpiador de flujos de datos.

El dispositivo de red está configurado para recibir y procesar un flujo de datos de red desde el lado de la red, y comprende un módulo de defensa contra ataques DDoS. El módulo de defensa contra ataques DDoS está configurado para detectar el estado en curso del dispositivo de red o del flujo de datos de la red que fluye al dispositivo de red, para determinar si el ataque DDoS tiene lugar en el dispositivo de red; y notificar al limpiador de flujos de datos que el limpiador de flujos de datos necesita limpiar el flujo de datos de la red que fluye al dispositivo de red, si el ataque DDoS ocurre en el dispositivo de red. El limpiador de flujos de datos está configurado para negociar con el dispositivo de red y limpiar el flujo de datos de la red de acuerdo con el resultado de la negociación. La presente invención está dirigida además a otro dispositivo de red, que incluye un módulo de defensa contra ataques DDoS. El módulo incluye una unidad de detección y una unidad de notificación.

La unidad de detección está configurada para detectar el estado en curso del dispositivo de red y el flujo de datos de la red que fluye al dispositivo de red en el lado del dispositivo de red, para determinar si el ataque DDoS ocurre en el dispositivo de red.

La unidad de notificación está configurada para notificar al limpiador de flujos de datos que el limpiador de flujos de datos necesita limpiar el flujo de datos de la red que fluye al dispositivo de red, si la unidad de detección detecta que ocurre un ataque DDoS en el dispositivo de red.

De acuerdo con el método, el dispositivo de red y el sistema de red para defenderse del ataque DDoS, que están divulgados en los modos de realización de la presente invención, se puede llevar a cabo la detección y la defensa preliminar en el lado del objetivo atacado, para obtener el estado del ataque y proporcionar la información requerida para la defensa. Por tanto, el ataque puede ser defendido efectivamente.

Breve descripción de los dibujos

Para hacer más clara la solución técnica de la presente invención, se describen a continuación los dibujos que se acompañan, para ilustrar los modos de realización de la presente invención o de la técnica anterior. Evidentemente, los dibujos que se acompañan son solamente para la finalidad de servir como ejemplos, y la persona con experiencia normal en la técnica puede deducir otros dibujos a partir de los que se acompañan, sin ningún esfuerzo creativo.

La figura 1 es un diagrama esquemático de la arquitectura de un sistema de red, de acuerdo con el modo de realización 1 de la presente invención;

La figura 2 es un diagrama de flujo de un método para defenderse de un ataque DDoS, de acuerdo con el modo de realización 1 de la presente invención;

La figura 3 es un diagrama esquemático de la estructura de un ataque módulo de defensa contra ataques DDoS, de acuerdo con el modo de realización 1 de la presente invención;

La figura 4 es un diagrama esquemático de la arquitectura de un sistema de red de acuerdo con el modo de realización 2 de la presente invención;

La figura 5 es un diagrama de flujo de un método para la defensa contra un ataque DDoS, de acuerdo con el modo de realización 2 de la presente invención;

La figura 6 es un diagrama esquemático de la estructura de un módulo de defensa contra ataques DDoS, de acuerdo con el modo de realización 3 de la presente invención; y

La figura 7 es un diagrama esquemático de la estructura de un módulo de defensa contra ataques DDoS, de acuerdo con el modo de realización 4 de la presente invención.

Descripción detallada de los modos de realización

Se describe a continuación la solución técnica que subyace en la presente invención, con referencia a los dibujos que se acompañan. Evidentemente, los modos de realización descritos a continuación son solamente para la finalidad de servir como ejemplos, sin cubrir todos los modos de realización de la presente invención. Los expertos en la técnica pueden deducir otros modos de realización a partir de los modos de realización ofrecidos en esta memoria, sin realizar ningún esfuerzo creativo, y tales modos de realización están cubiertos en el ámbito de protección de la presente invención.

En los modos de realización siguientes, la red puede ser, por ejemplo, una red móvil, una red fija, una red de convergencia móvil-fija-móvil; o una red de área local, una red de área metropolitana, o una red de área amplia; o una red de acceso, una red básica, o una red de transporte; o una red punto a punto (P2P) o una red de arquitectura cliente/servidor (C/S).

Modo de realización 1

De acuerdo con este modo de realización, se monta un módulo de defensa contra ataques DDoS en un servidor objetivo del ataque. El módulo puede detectar el estado en curso del servidor y/o un flujo de datos de red que fluyen hacia el servidor, y retro-informar sobre el resultado de la detección a un limpiador de flujos de datos. El módulo de defensa contra ataques DDoS en el lado del servidor puede ser hardware o software, por ejemplo, pero sin limitarse a ello, una capa de interfaz de red, un nivel de Kernel o un software a nivel de aplicación. El módulo puede ser un software independiente o parte de un cierto software de seguridad y puede ser también defensor del hardware o software en diversos niveles.

El estado en curso del servidor incluye la carga en curso o el tráfico de red de una unidad central de proceso (CPU) o de una memoria.

Haciendo referencia a la figura 1, el sistema de red de acuerdo con este modo de realización incluye un detector 102 de ataques, un limpiador 104 de flujos de datos y al menos un servidor 106.

El detector 102 de ataques está configurado para detectar un flujo de datos de red desde el lado de la red; y si se detecta que tiene lugar un ataque DDoS en el servidor, dirigir el flujo atacante de datos de red que fluye en el objetivo atacado hacia el limpiador de flujos de datos para limpiarlo utilizando una tecnología de conducción de flujos, y enviar el flujo normal de datos de red al servidor. El objetivo atacado del ataque DDoS puede ser reconocido utilizando, por ejemplo, la dirección IP o la dirección MAC.

El limpiador 104 de flujos de datos está configurado para negociar con el detector de ataques y con el servidor, y limpiar el flujo de datos de red, de acuerdo con el resultado de la negociación.

El al menos un servidor 106 está configurado para recibir y procesar el flujo de datos de red desde el lado de la red, e incluye un módulo de defensa contra ataques DDoS. El módulo de defensa contra ataques DDoS está configurado para detectar un estado en curso del servidor y/o del flujo de datos de red que fluye hacia el servidor, para determinar si tiene lugar un ataque DDoS, y enviar el resultado de la detección al limpiador de flujos de datos, y notificar al limpiador de flujos de datos que el limpiador de flujos de datos necesita limpiar el flujo de datos de red que fluye al dispositivo de red, si la unidad de detección detecta que ocurre un ataque DDoS en el dispositivo de la red. El módulo de defensa contra ataques DDoS puede limpiar además el flujo de datos que ha sido limpiado por el limpiador de flujos de datos.

El limpiador de flujos de datos puede ser instalado en cualquier posición antes del servidor. Como se ilustra en la figura 1, el limpiador de flujos de datos se instala entre un enrutador 108 y un conmutador 110.

El limpiador y el módulo de defensa contra ataques DDoS en el lado del servidor pueden tener un interfaz de unión.

Haciendo referencia a la figura 2, el método para defenderse de un ataque DDoS de acuerdo con este modo de realización incluye los pasos siguientes:

En el paso S202, el detector de ataques detecta si tiene lugar un ataque DDoS en el servidor, de acuerdo con las características del flujo de datos de red, y si se detecta el ataque DDoS, dirige el flujo atacante de datos de red que fluye en el objetivo atacado al limpiador de flujos de datos, para limpiarlo utilizando la tecnología de conducción de flujos, y envía el flujo normal de datos de red al servidor. El objetivo atacado puede ser reconocido, por ejemplo, a través de la dirección IP o de la dirección MAC.

En el paso S204, el módulo de defensa contra ataques DDoS del lado del servidor detecta el estado en curso del servidor y/o el flujo de datos de red en el lado del servidor, para determinar si ocurre un ataque DDoS. Se adoptan diversos motores y algoritmos en la detección del módulo, con el fin de averiguar si hay ataque DDoS lo antes posible. El módulo de defensa contra ataques DDoS trabaja conjuntamente con el módulo detector en el lado de la red.

La detección en el lado del servidor puede realizar un análisis basado en flujos, ficheros o protocolos. Debido a que la detección se lleva a cabo en el lado del servidor, se consigue una mayor sensibilidad que la del dispositivo en el lado de la red, y por tanto se pueden encontrar más características DDoS que en el lado de la red.

En el paso S206, cuando se determina que tiene lugar un ataque DDoS en el servidor, el módulo de defensa contra ataques DDoS en el lado del servidor notifica al limpiador de flujos de datos a través del interfaz de unión, o por otros medios, al limpiador de flujos de datos, que el limpiador de flujos de datos necesita limpiar el flujo de datos de red que fluye hacia el servidor para su limpieza. El módulo de defensa contra ataques DDoS puede extraer las características de los paquetes de red atacantes, para notificar al limpiador de flujos de datos que el limpiador de flujos de datos necesita limpiar el flujo de datos.

El flujo de datos de red que ha sido limpiado puede seguir conteniendo una parte del ataque DDoS, de manera que el método de este modo de realización puede incluir además los pasos siguientes:

En el paso S208, el módulo de defensa contra ataques DDoS limpia el flujo de datos de red que fluye hacia el servidor y que ha sido limpiado por el limpiador de flujos de datos.

El módulo de defensa contra ataques DDoS, de acuerdo con este modo de realización, incluye una unidad 302 de detección, una unidad 304 de notificación y una unidad 306 de limpieza.

La unidad 302 de detección está configurada para detectar el estado en curso del servidor y/o el flujo de datos de red que fluye hacia el servidor en el lado del servidor, para determinar si tiene lugar un ataque DDoS en el servidor.

La unidad 304 de notificación está configurada para notificar al limpiador de flujos de datos que el limpiador de flujos de datos necesita redirigir el flujo de datos de red que fluye al servidor, hacia el limpiador de flujos de datos para limpiar el flujo de datos, si la unidad de detección detecta que ocurre un ataque DDoS en el servidor.

La unidad 306 de limpieza está configurada para limpiar el flujo de datos de red que fluye hacia el servidor.

De acuerdo con este modo de realización, la detección y defensa preliminares pueden ser llevadas a cabo en el lado del objetivo atacado, para obtener el estado del ataque y proporcionar información requerida para la defensa. Por tanto, el ataque puede ser defendido eficazmente.

Modo de realización 2

De acuerdo con este modo de realización, el detector de ataques no necesita ser montado en el lado de la red, y en lugar de eso, se monta el módulo de defensa contra ataques DDoS en el servidor objetivo del ataque.

Haciendo referencia a la figura 4, un sistema de red de acuerdo con este modo de realización incluye un limpiador 402 del flujo de datos y al menos un servidor 404.

El limpiador 402 del flujo de datos está configurado para negociar con el detector de ataques y con el servidor y para limpiar el flujo de datos de red, de acuerdo con el resultado de la negociación.

El al menos un servidor 404 está configurado para recibir y procesar el flujo de datos de red desde el lado de la red, e incluye un módulo de defensa contra ataques DDoS. El módulo de defensa contra ataques DDoS está configurado para detectar el estado en curso del servidor y/o el flujo de datos de red, y retro-informar sobre el resultado de la detección al limpiador de flujos de datos. El módulo de defensa contra ataques DDoS puede limpiar además el flujo de datos que ha sido limpiado por el limpiador de flujos de datos.

El limpiador de flujos de datos puede ser instalado en cualquier posición antes del servidor. Como se ilustra en la figura 4, el limpiador de flujos de datos se instala entre un enrutador 406 y un conmutador 408.

El limpiador y el módulo de defensa contra ataques DDoS del lado del servidor pueden tener un interfaz de unión.

Haciendo referencia a la figura 5, el método de este modo de realización incluye los pasos siguientes:

En el paso S502, el módulo de defensa contra ataques DDoS del lado del servidor detecta el estado en curso del servidor y/o del flujo de datos de red en el lado del servidor, para determinar si ocurre un ataque DDoS. Se adoptan diversos motores y algoritmos en la detección del módulo, con el fin de averiguar si hay ataque DDoS lo antes posible. El módulo de defensa contra ataques DDoS trabaja conjuntamente con el detector de ataques en el lado de la red.

La detección en el lado del servidor puede realizar un análisis basado en flujos, ficheros o protocolos. Debido a que la detección se lleva a cabo en el lado del servidor, se consigue una mayor sensibilidad que la del dispositivo en el lado de la red, y por tanto se pueden averiguar más características DDoS que en el lado de la red.

En el paso S504, cuando se determina que ocurre un ataque DDoS en el servidor, el módulo de defensa contra ataques DDoS del lado del servidor notifica al limpiador de flujos de datos a través del interfaz de unión, o por otros medios, que el flujo de datos de red necesita redirigir el flujo de datos de red que fluye a la dirección IP del servidor, hacia el limpiador de flujos de datos para limpiar el flujo de datos. El módulo de defensa contra ataques DDoS puede extraer las características de los paquetes de red atacantes, para notificar al limpiador de flujos de datos que el limpiador de flujos de datos necesita limpiar el flujo de datos.

El flujo de datos de red que ha sido limpiado puede seguir conteniendo parte del ataque DDoS, de manera que el método de este modo de realización puede incluir además los pasos siguientes:

En el paso S506, el módulo de defensa contra ataques DDoS limpia el flujo de datos de red que fluye al servidor y que ha sido limpiado por el limpiador de flujos de datos.

De acuerdo con este modo de realización, la detección y defensa preliminares pueden ser llevadas a cabo en el lado del objetivo atacado, para obtener el estado del ataque y proporcionar la información requerida para la defensa. Por tanto, el ataque puede ser defendido eficazmente. Más aún, no necesita instalarse ningún detector de ataques, y los costes se reducen aún más.

Modo de realización 3

De acuerdo con este modo de realización, se añade al servidor un mecanismo de alarma de la carga. Como se ilustra en la figura 6, el módulo de defensa contra ataques DDoS incluye además una unidad 602 de alarma de la carga.

La unidad 602 de alarma de la carga está configurada para supervisar el tráfico del flujo de datos de red que fluye al servidor, y producir una alarma para el limpiador de flujos de datos cuando el tráfico del flujo de datos de red alcanza un valor prefijado, por ejemplo un nivel de riesgo autodefinido.

La detección del tráfico que fluye en el servidor es acompañada por la detección del tráfico en la tarjeta de red. La detección puede estar vinculada a la fortaleza de limpieza y filtrado del limpiador de flujos de datos, de acuerdo con los grados clasificados por la capacidad de soporte. Cuando el tráfico que pasa a través de la tarjeta de red alcanza un nivel de riesgo, se produce una alarma para el limpiador de flujos de datos.

De acuerdo con este modo de realización, la alarma y defensa del ataque DDoS puede llevarse a cabo de acuerdo con el tráfico en el lado del servidor, de manera que se refuerza la seguridad.

Modo de realización 4

De acuerdo con este modo de realización, se establece un vínculo por impulsos entre el servidor y el detector, y el detector puede ser un limpiador de flujos de datos.

Cuando los recursos de la CPU del servidor han sido agotados, el ordenador central no puede enviar ningún mensaje, y puede determinarse si el servidor se viene abajo detectando el impulso. El limpiador de flujos de datos comienza el rescate del servidor al detectar que el ordenador central se ha venido abajo. Las medidas del rescate se describen en lo que sigue:

(1) Limitar el tráfico que fluye hacia el servidor en el limpiador de flujos de datos, en el cual el límite del tráfico puede ser a nivel de rescate; detectar si se recupera el impulso; y reiniciar el servidor si no se recupera el impulso.

(2) Tras haber recuperado el impulso, el detector analiza la “razón de venirse abajo” y mejora las reglas de filtrado, en el cual el detector puede ser un limpiador.

Como se ilustra en la figura 7, el módulo de defensa contra ataques DDoS incluye además una unidad 702 de envío del impulso.

La unidad 702 de envío del impulso está configurada para enviar impulsos al limpiador de flujos de datos.

De acuerdo con este modo de realización, el limpiador de flujos de datos es notificado por medio de los impulsos que necesita limitar el tráfico cuando el lado del servidor se viene abajo con un ataque DDoS, defendiendo con ello eficazmente el ataque DDoS y mejorando la seguridad.

En los modos de realización anteriores, el servidor objetivo del ataque en distintos entornos de red puede ser otro tipo de dispositivo, tal como un ordenador, un teléfono móvil, un nodo de red (por ejemplo, un enrutador, un conmutador o una estación base), o un electrodoméstico.

En vista de lo anterior, de acuerdo con el método, el dispositivo de red y el sistema de red para defenderse de un ataque DDoS de la presente invención, la detección y la defensa preliminar, pueden llevarse a cabo en el lado del objetivo atacado, para obtener con precisión el estado del ataque y proporcionar la información requerida para la defensa. Por tanto, el ataque puede ser defendido eficazmente.

Las personas expertas en la técnica puede además darse cuenta que, en combinación con los modos de realización presentes, las unidades y los pasos de algoritmo de cada ejemplo descrito, pueden ser implementados con hardware electrónico, software informático, o combinación de los mismos. Con el fin de describir claramente la intercambiabilidad entre el hardware y el software, se han descrito generalmente con profusión las composiciones y pasos de cada ejemplo, de acuerdo con las funciones de las descripciones precedentes. Que las funciones se ejecuten en un modo de hardware o software depende de las aplicaciones particulares y las condiciones restrictivas del diseño de las soluciones técnicas. Las personas expertas en la técnica pueden utilizar distintos métodos para implementar las funciones descritas para cada aplicación particular, pero no debe considerarse que la implementación sobrepase el alcance de la presente invención.

En combinación con los modos de realización presentes, los pasos del método o algoritmo descritos pueden ser implementados directamente utilizando hardware, un módulo de software ejecutado por un procesador o

combinación de los mismos. El módulo de software puede ser colocado en una memoria de acceso aleatorio (RAM), una memoria, una memoria de sólo lectura (ROM), una ROM programable eléctricamente (EPROM), una ROM programable eléctricamente que pueda borrarse (EEPROM), un registrador, un disco duro, un disco magnético extraíble, un CD-ROM, o cualquier medio de almacenamiento de otras formas bien conocidas en el campo de la técnica.

Las descripciones anteriores son meramente modos de realización preferidos de la presente invención, pero no pretenden limitar la presente invención. Cualquier modificación, sustitución equivalente o mejora hechas sin apartarse del principio de la presente invención deben caer dentro del alcance de la presente invención.

REIVINDICACIONES

1. Un método para defenderse de un ataque de denegación distribuida de servicios, DDoS, caracterizado porque comprende:

detectar el estado en curso de un servidor en el lado del servidor, para determinar si ocurre un ataque DDoS en el servidor (204); y

notificar a un limpiador de flujos de datos que el limpiador de flujos de datos necesita limpiar el flujo de datos de red que fluye al servidor, si ocurre el ataque DDoS en el servidor (206).

2. El método de acuerdo con la reivindicación 1, caracterizado porque comprende además:

limpiar el flujo de datos de red que ha sido limpiado por el limpiador de flujos de datos en el lado del servidor (208).

3. El método de acuerdo con la reivindicación 1, caracterizado porque, antes de detectar el estado en curso del servidor o del flujo de datos de red que fluye en el servidor en el lado del servidor, el método comprende además:

detectar, por medio de un detector de ataques en el lado de la red, el flujo de datos de red, para determinar si ocurre un ataque DDoS en el servidor, y si ocurre un ataque DDoS en el servidor, dirigir el flujo de datos de red que fluye al servidor, hacia el limpiador de flujos de datos para su limpieza (202).

4. Un dispositivo (106) de red, caracterizado porque comprende un módulo de defensa contra un ataque de denegación distribuida de servicios, DDoS, donde el módulo comprende:

una unidad (302) de detección, configurada para detectar un estado curso del dispositivo de red en el lado del dispositivo de red, para determinar si ocurre un ataque DDoS en el dispositivo de red; y

una unidad (304) de notificación, configurada para notificar a un limpiador de flujos de datos que el limpiador de flujos de datos necesita limpiar el flujo de datos de red que fluye hacia el dispositivo de red, si la unidad de detección detecta que ocurre un ataque DDoS en el dispositivo de red.

5. El dispositivo de red de acuerdo con la reivindicación 4, caracterizado porque el módulo de defensa contra ataques DDoS comprende además:

una unidad (306) de limpieza, configurada para limpiar el flujo de datos de red que fluye hacia el dispositivo de red.

6. El dispositivo de red de acuerdo con la reivindicación 4, caracterizado porque en módulo de defensa contra ataques DDoS comprende además:

una unidad (602) de alarma de la carga, configurada para supervisar el tráfico del flujo de datos de red que fluye hacia el dispositivo de red, y cuando el tráfico del flujo de datos de red alcanza un valor prefijado, enviar una alarma al limpiador de flujos de datos.

7. El dispositivo de red de acuerdo con la reivindicación 4, caracterizado porque el módulo de defensa contra ataques DDoS comprende además:

una unidad (702) de envío de impulsos configurada para enviar impulsos al limpiador de flujos de datos.

8. Un sistema de red, caracterizado porque comprende al menos un dispositivo (106) de red, de acuerdo con la reivindicación 4, y un limpiador (104) de flujos de datos, donde

el dispositivo (106) de red está configurado para recibir y procesar un flujo de datos de red desde el lado de la red y comprende un módulo de defensa contra ataques de denegación distribuida de servicios, DDoS, configurado para detectar el estado en curso del dispositivo de red, para determinar si al ataque DDoS ocurre en el dispositivo de red; y notificar al limpiador de flujos de datos que el limpiador de flujos de datos necesita limpiar el flujo de datos de red que fluye hacia el dispositivo de red, si ocurre un ataque DDoS en el dispositivo de red; y

el limpiador (104) de flujos de datos está configurado para negociar con el dispositivo de red y limpiar el flujo de datos de red, de acuerdo con el resultado de la negociación.

9. El sistema de red de acuerdo con la reivindicación 8, caracterizado porque comprende además:

un detector (102) de ataques, configurado para detectar el flujo de datos de red desde el lado de la red, para determinar si ocurre un ataque DDoS en el dispositivo de red, y si ocurre un ataque DDoS en el dispositivo de red, dirigir el flujo de datos de red que fluye al dispositivo de red, hacia el limpiador de flujos de datos para su limpieza.

10. El sistema de red de acuerdo con la reivindicación 8, caracterizado porque el tipo de dispositivo de red comprende:

un ordenador, un servidor, un teléfono móvil, un enrutador, un conmutador o una estación base.

11. Un dispositivo (106) de red, caracterizado porque comprende un módulo de defensa contra ataques de denegación distribuida de servicios, DDoS, donde el módulo comprende:

una unidad (302) de detección, configurada para detectar un estado en curso del dispositivo de red en el lado del dispositivo de red, y el flujo de datos de red que fluye hacia el dispositivo (106) de red, para determinar si ocurre un ataque DDoS en el dispositivo de red; y

una unidad (304) de notificación, configurada para notificar a un limpiador de flujos de datos que el limpiador de flujos de datos necesita limpiar el flujo de datos de red que fluye hacia el dispositivo de red, si la unidad de detección detecta que ocurre un ataque DDoS en el dispositivo de red.

12. El dispositivo de red de acuerdo con la reivindicación 11, caracterizado porque el módulo de defensa contra ataques DDoS comprende además:

una unidad (306) de limpieza, configurada para limpiar el flujo de datos de red que fluye hacia el dispositivo de red.

13. El dispositivo de red de acuerdo con la reivindicación 11, caracterizado porque el módulo de defensa contra ataques DDoS comprende además:

una unidad (602) de alarma de la carga, configurada para supervisar el tráfico del flujo de datos de red que fluye hacia el dispositivo de red, y cuando el tráfico del flujo de datos alcanza un valor prefijado, enviar una alarma al limpiador de flujos de datos.

14. El dispositivo de red de acuerdo con la reivindicación 11, caracterizado porque el módulo de defensa contra ataques DDoS comprende además:

una unidad (702) de envío de impulsos, configurada para enviar impulsos al limpiador de flujos de datos.

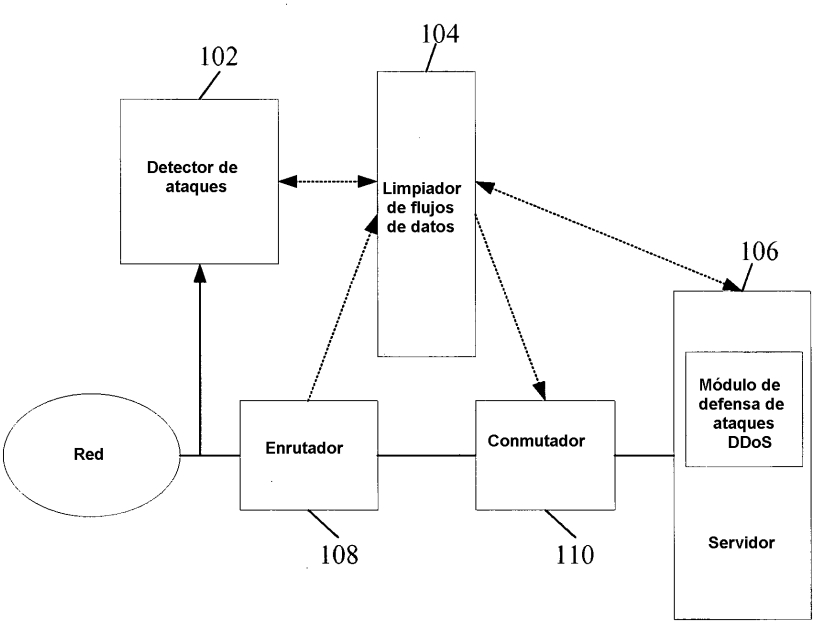
102
104
Detector de ataques
Limpiador de flujos de datos
106
Módulo de defensa de ataques DDoS
Red
Enrutador
Conmutador
Servidor
108
110

FIG. 1

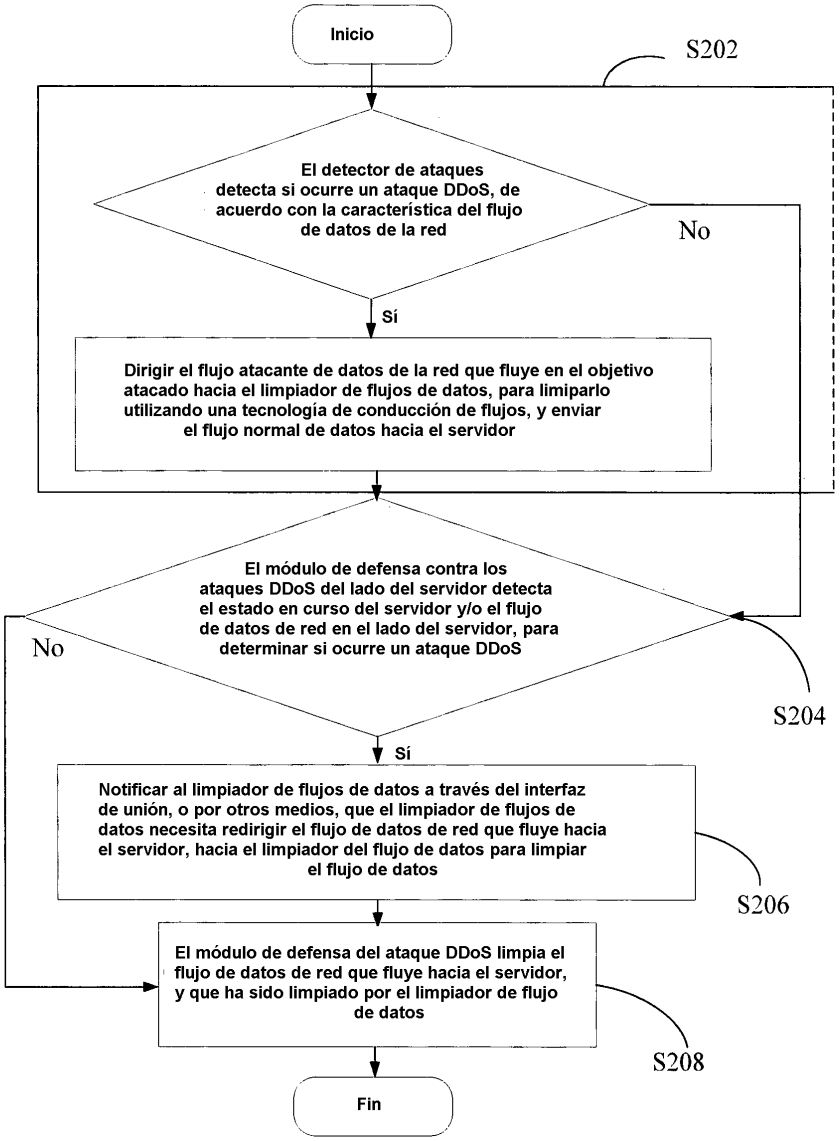
Inicio
S202
El detector de ataques detecta si ocurre un ataque DDoS, de acuerdo con la característica del flujo de datos de la red
No
Sí
Dirigir el flujo atacante de datos de la red que fluye en el objetivo atacado hacia el limpiador de flujos de datos, para limiparlo utilizando una tecnología de conducción de flujos, y enviar el flujo normal de datos hacia el servidor
El módulo de defensa contra los ataques DDoS del lado del servidor detecta el estado en curso del servidor y/o el flujo de datos de red en el lado del servidor, para determinar si ocurre un ataque DDoS
No
S204
Sí
Notificar al limpiador de flujos de datos a través del interfaz de unión, o por otros medios, que el limpiador de flujos de datos necesita redirigir el flujo de datos de red que fluye hacia el servidor, hacia el limpiador del flujo de datos para limpiar el flujo de datos
S206
El módulo de defensa del ataque DDoS limpia el flujo de datos de red que fluye hacia el servidor, y que ha sido limpiado por el limpiador de flujo de datos
S208
Fin

FIG. 2

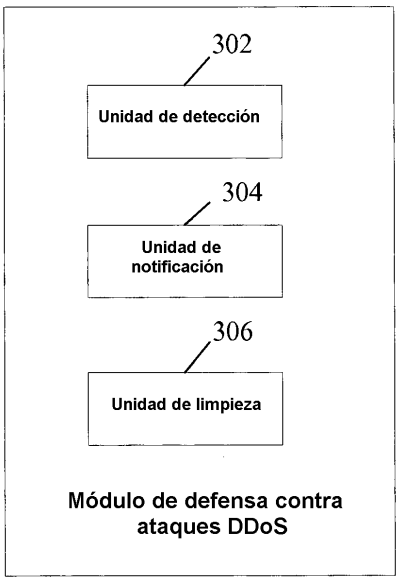
302
Unidad de detección
304
Unidad de notificación
306
Unidad de limpieza
Módulo de defensa contra ataques DDoS

FIG. 3

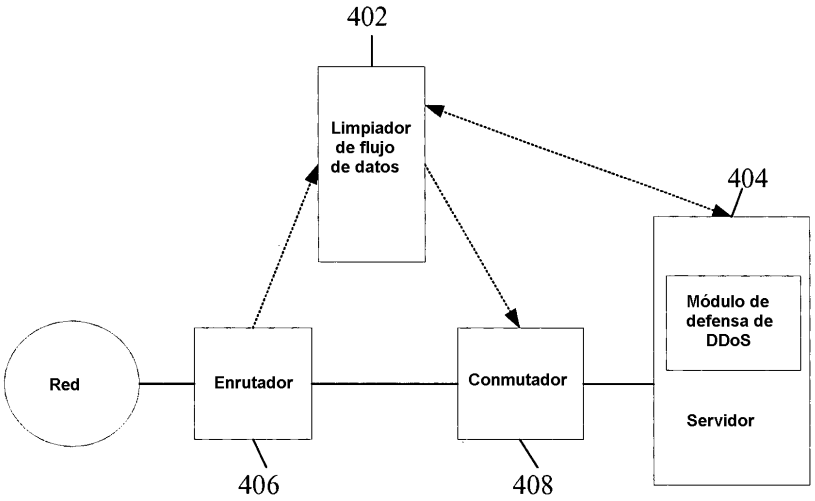
402
Limpiador de flujo de datos
404
Módulo de defensa de DDoS
Red
Enrutador
Conmutador
Servidor
406
408

FIG. 4

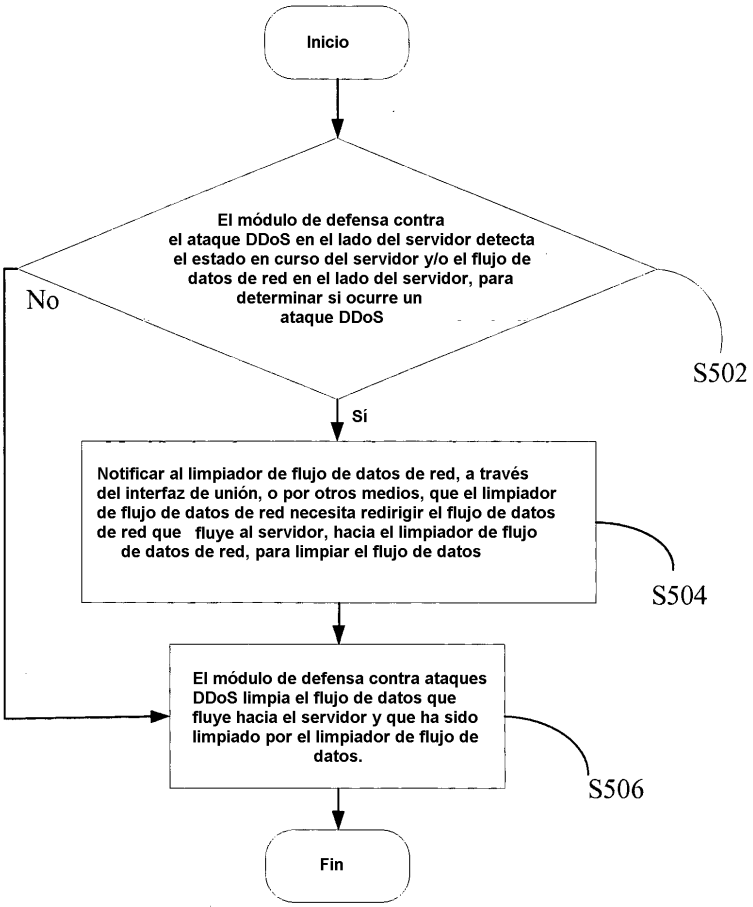
Inicio
El módulo de defensa contra el ataque DDoS en el lado del servidor detecta el estado en curso del servidor y/o el flujo de datos de red en el lado del servidor, para determinar si ocurre un ataque DDoS
No
S502
Sí
Notificar al limpiador de flujo de datos de red, a través del interfaz de unión, o por otros medios, que el limpiador de flujo de datos de red necesita redirigir el flujo de datos de red que fluye al servidor, hacia el limpiador de flujo de datos de red, para limpiar el flujo de datos
S504
El módulo de defensa contra ataques DDoS limpia el flujo de datos que fluye hacia el servidor y que ha sido limpiado por el limpiador de flujo de datos.
S506
Fin

FIG. 5

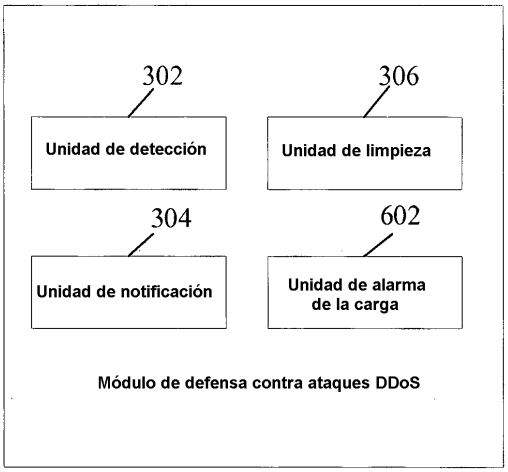
302
306
Unidad de detección
Unidad de limpieza
304
602
Unidad de notificación
Unidad de alarma de la carga
Módulo de defensa contra ataques DDoS

FIG. 6

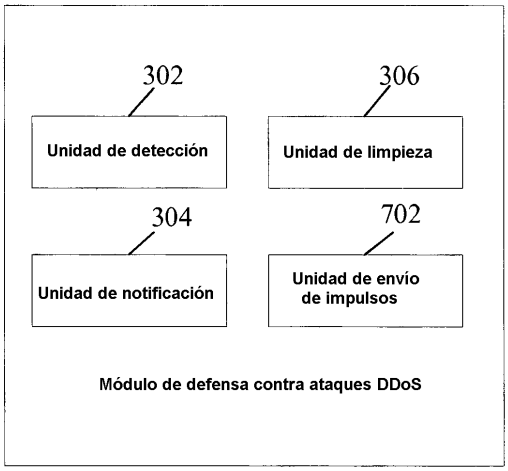
302
306
Unidad de detección
Unidad de limpieza
304
702
Unidad de notificación
Unidad de envío de impulsos
Módulo de defensa contra ataques DDoS

FIG. 7