(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 738 106**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04L 29/12 (2006.01)
H04L 12/28 (2006.01)
H04W 12/12 (2009.01)
H04L 29/08 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **27.08.2013 PCT/CN2013/082397**

(87) Fecha y número de publicación internacional: **22.05.2014 WO14075485**

(96) Fecha de presentación y número de la solicitud europea: **27.08.2013 E 13854514 (0)**

(97) Fecha y número de publicación de la concesión europea: **24.04.2019 EP 2922263**

(54) Título: **Procedimiento de procesamiento para tecnología de traducción de direcciones de red, dispositivo de NAT y dispositivo de BNG**

(30) Prioridad:

14.11.2012 CN 201210456758

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
20.01.2020

(73) Titular/es:

ZTE CORPORATION (100.0%)
ZTE Plaza, Keji Road South, Hi-Tech Industrial Park, Nanshan District
Shenzhen, Guangdong 518057, CN

(72) Inventor/es:

FAN, LIANG y
YUAN, BO

(74) Agente/Representante:

LINAGE GONZÁLEZ, Rafael

DESCRIPCIÓN

Procedimiento de procesamiento para tecnología de traducción de direcciones de red, dispositivo de NAT y dispositivo de BNG

Campo técnico

La presente invención se refiere al campo de la comunicación y, en particular, a un procedimiento, un dispositivo de Traducción de Direcciones de Red (NAT) y un dispositivo de Pasarela de Red de Banda Ancha (BNG) para procesar una tecnología de traducción de direcciones de red.

Antecedentes

A medida que aumenta el número de usuarios que utilizan el acceso de banda ancha a Internet, los recursos de dirección de un Protocolo de Internet Versión 4 (IPv4) se están estirando, y las direcciones del IPv4 de una red pública que pueden transmitirse a través de Internet son cada vez más escasas; al parecer, las direcciones del IPv4 de la red pública que disminuyen continuamente no pueden satisfacer las demandas de los usuarios de la red, como resultado, surge la tecnología de Traducción de Direcciones de la Red (NAT).

La tecnología NAT, una tecnología para traducir una dirección del IPv4 de la red privada en una dirección del IPv4 de la red pública, se ha aplicado ampliamente a varios tipos de modalidades de acceso a Internet y varios tipos de redes. La tecnología de NAT puede resolver perfectamente el problema de la insuficiencia de direcciones del Protocolo de Internet (IP) y evitar efectivamente un ataque desde el exterior de la red, a fin de ocultar y proteger uno o más ordenadores en la red.

Como dispositivo para proporcionar una función de NAT, el dispositivo de NAT se clasifica en dos tipos:

(1) un dispositivo de NAT convergente está integrado con una pasarela de red de banda ancha (BNG) que proporciona un servicio de acceso de banda ancha y la función de NAT.

(2) Un dispositivo de NAT independiente simplemente proporciona la función de NAT. El dispositivo de NAT independiente está ubicado flujo arriba del BNG y simplemente proporciona una función de NAT pero no una función de acceso de banda ancha.

El proceso por el que un usuario accede a Internet utilizando la función de NAT es el siguiente:

(1) cuando está en línea, un usuario de banda ancha adquiere una dirección del IPv4 de la red privada desde una pasarela de red de banda ancha;

(2) cuando el usuario de banda ancha accede a Internet, la dirección de origen de uno o más paquetes del IPv4 del usuario de banda ancha es una dirección del IPv4 adquirida de la red privada, y los uno o más paquetes del IPv4 se envían al dispositivo de NAT;

(3) el dispositivo de NAT traduce una dirección del IP de origen y un puerto de origen de un mensaje de usuario a una dirección del IP de la red pública y un puerto de la red pública de acuerdo a una regla específica, genera una relación de correspondencia de sesiones entre 'la dirección del IP de origen + el puerto de origen' y 'una dirección del IP de origen traducida + un puerto de origen traducido' y envía el mensaje del usuario a Internet, completando así una NAT directa;

(4) un mensaje del IP devuelto al usuario por Internet busca la relación de correspondencia de sesiones entre las direcciones y los puertos de la red pública y las direcciones y los puertos de la red privada en el dispositivo de NAT, de acuerdo a una dirección de destino y un puerto de destino del mensaje del IP. La dirección de destino y el puerto de destino del mensaje del IP se traducen en la dirección del IP de origen de la red privada del mensaje de usuario y al puerto de origen de la red privada del mensaje de usuario, realizando así una NAT inversa;

(5) se envía un paquete inverso al anfitrión del usuario tomando la dirección del IP y el puerto de la red privada del mensaje del usuario como destino.

Por lo tanto, durante un proceso de NAT, el dispositivo de NAT genera la relación de correspondencia de sesiones entre "la dirección del IP de origen + el puerto de origen" y "la dirección del IP de origen traducida + el puerto de origen traducido de acuerdo al mensaje del usuario que accede a Internet. La relación se denomina Sesión y se genera un elemento de sesión en el dispositivo de NAT cada vez que el usuario accede a un servicio de Internet (identificado como una dirección del IP de destino + un puerto de destino). Cada elemento de sesión registra el siguiente contenido:

1) la dirección del IP de destino y el puerto de destino del servicio de Internet;

2) la dirección del IP de origen y el puerto de origen de la red privada del usuario y la dirección del IP de origen y el puerto de origen de la red pública, obtenidos por el usuario al usar la NAT; y

3) un protocolo usado.

El dispositivo de NAT establece un elemento de sesión siempre que el grupo de cinco elementos (la dirección del IP de origen, el puerto de origen, un protocolo, la dirección del IP de destino y el puerto de destino) de un mensaje del IP sea diferente cuando un usuario de la red privada accede a Internet, el dispositivo de NAT puede realizar una NAT directa o una NAT inversa según la relación de correspondencia entre la red pública y la red privada en el elemento de la sesión, y el usuario no puede acceder a Internet antes de reemplazar la dirección y el puerto de la red privada con la dirección y el puerto de la red pública mediante la realización de la NAT.

La capacidad de dichos uno o más elementos de sesión está limitada por los recursos de hardware en el dispositivo de NAT, es decir, el número de los elementos de sesión con soporte por parte del dispositivo de NAT es limitado. En esta situación, aparece un problema en cuanto a que cuando el anfitrión de un usuario de una red privada es atacado por uno o más virus, el host del usuario de la red privada envía continuamente a Internet uno o más mensajes de ataque con una dirección del IP de destino variable y un puerto de destino variable a una velocidad alta, por ejemplo, a una velocidad tan alta que las combinaciones de 1000 direcciones del IP de destino y puertos de destino diferentes se envíen cada segundo, ya que el grupo de cinco elementos de los uno o más mensajes de ataque sigue variando y es enviado por el anfitrión de un usuario legal, el dispositivo de NAT genera diferentes sesiones de acuerdo a los uno o más mensajes de ataque, ya que los uno o más mensajes de ataque se envían a una velocidad extremadamente alta, las sesiones generadas por los uno o más mensajes de ataque ocupan una gran cantidad de recursos de sesión e incluso pueden agotar todos los recursos de sesión de un dispositivo de NAT completo, lo que impide al usuario legal acceder a Internet legalmente.

De manera similar, como la capacidad de procesamiento del dispositivo de NAT para una nueva sesión es limitada, la sesión del usuario legal no se puede establecer cuando la velocidad de establecimiento de sesión de un usuario atacante está más allá de la capacidad de procesamiento del dispositivo de NAT, lo que también inhabilita al usuario legal para acceder a internet.

Hay tres soluciones proporcionadas para resolver los problemas anteriores:

1) un tiempo de antigüedad de una sesión de ataque está configurado para acelerar la antigüedad de una sesión inválida;

2) el número de sesiones disponibles para cada usuario está limitado, de modo que solo las sesiones del usuario de un anfitrión atacado por virus se agotan, sin causar ninguna influencia a otros usuarios legales;

3) una velocidad de establecimiento de la nueva sesión de cada usuario está limitada a fin de inhibir una conducta de ataque de alta velocidad.

Sin embargo, en las tres soluciones descritas anteriormente, las sesiones de un usuario se agotan en el caso de una conducta de ataque. Los dispositivos existentes solo pueden notificar al operador el agotamiento de las sesiones por medio de un administrador de red o una alarma de registro del sistema mientras la conexión de red de acceso telefónico de banda ancha del usuario aún funciona. Por lo tanto, el usuario no es consciente del hecho de que no se puede acceder a la red porque el ordenador del usuario es atacado por los uno o más virus y todavía presenta quejas contra el operador, lo que da como resultado que las quejas presentadas por el usuario por el comportamiento anormal del anfitrión del usuario aumentan significativamente.

No se han propuesto soluciones efectivas para resolver al menos uno de los problemas anteriores.

PERREAULT S ET AL: "Common requirements for Carrier Grade NATs (CGNs) [Requisitos comunes para las NAT de grado de portador (CGN)]; draft-ietf-behave-lsn-Requirements-09.txt" y FORD M ET AL: "Issues with IP Address Sharing; rfc6269.txt [Problemas con el intercambio de direcciones del IP; rfc6269,txt]" proporciona soluciones técnicas relacionadas; sin embargo, el problema mencionado anteriormente sigue sin resolverse.

El documento US 2004047356A1 divulga la "monitorización de tráfico de red", el documento US 2006206933 A1 divulga "seguridad para dispositivos móviles en una red inalámbrica" y el documento EP 1983721 A1 divulga "sistema y procedimiento para limitar la actividad del software espía".

Sumario

La presente invención está definida en las reivindicaciones independientes. Se definen modos de realización preferidos en las reivindicaciones dependientes. Las realizaciones de la presente invención proporcionan un procedimiento de procesamiento para la tecnología de traducción de direcciones de red, un dispositivo de NAT y

un dispositivo de BNG, a fin de resolver al menos el problema en la técnica relacionada en cuanto a que un usuario presenta quejas contra el operador por el comportamiento anormal del anfitrión del usuario.

El procedimiento de procesamiento para la tecnología de traducción de direcciones de red de acuerdo a un modo de realización de la presente invención incluye:

un dispositivo de NAT que determina si el establecimiento de sesión de un equipo de usuario (UE) alcanza o no un umbral predeterminado, y notifica a un dispositivo de pasarela de red de banda ancha (BNG) para ejecutar una estrategia de seguridad para el UE si el establecimiento de sesión del UE alcanza el umbral predeterminado, en donde la estrategia de seguridad se usa para detener la conducta de ataque del UE e informar al UE de la conducta de ataque del UE.

En un modo de realización ejemplar, el proceso en el que el dispositivo de BNG ejecuta la estrategia de seguridad precedente para el UE incluye: el dispositivo de BNG ejecutando una estrategia de presentación impuesta de páginas de la Red forzadas, para que el UE redirija una solicitud del HTTP enviada por el UE a una primera página de solicitud, en el que la primera página de solicitud se usa para informar al UE de la existencia de una conducta de ataque durante el acceso del UE.

En un modo de realización ejemplar, el proceso por el que el dispositivo de BNG redirige la solicitud HTTP enviada por el UE a la primera página de solicitud incluye: el dispositivo de BNG redirige la solicitud del HTTP enviada por el UE a la primera página de solicitud en el intervalo preestablecido.

En un modo de realización ejemplar, la primera página de solicitud se usa para recordar al UE que revise o elimine virus y/o troyanos.

En un modo de realización ejemplar, después de que el dispositivo de BNG ejecute la estrategia de seguridad para el UE, el procedimiento de procesamiento para la tecnología de traducción de direcciones de red incluye además: notificar el dispositivo de NAT al dispositivo de BNG que ejecute, apuntando a la conducta de acceso del UE, una operación para forzar al UE a estar fuera de línea o devolver el UE a un estado no autenticado y notificar a un servidor de Autenticación, Autorización y Contabilidad (AAA) para que marque o establezca al UE como un equipo de usuario con una conducta de ataque, en el que se utiliza adicionalmente la primera página de solicitud para recordarle al UE que debe ser forzado a estar fuera de línea o regresar al estado no autenticado; solicitar el UE estar en línea y/o ser autenticado nuevamente, autenticar el servidor de AAA al UE, después de que el UE aprueba la autenticación, notificar el servidor AAA al dispositivo de BNG que ejecute una estrategia forzada de presentación impuesta de página de la Red, para que el UE vuelva a dirigir una solicitud de acceso a página del UE a una segunda página de solicitud, en donde la segunda página de solicitud se usa para recordar que una razón por la que el UE fue forzado anteriormente a estar fuera de línea o ser devuelto a un estado no autenticado es la conducta de ataque del UE y, si el equipo de usuario aún tiene la conducta de ataque, el dispositivo de NAT le recuerda al UE que el UE será forzado a estar fuera de línea o volver al estado no autenticado nuevamente y le recuerda al equipo del usuario que debe verificar y eliminar virus y/o troyanos.

En un modo de realización ejemplar, el dispositivo de NAT incluye al menos uno de los siguientes: un dispositivo de NAT integrado con el dispositivo de BNG; y un dispositivo de NAT dispuesto por separado del dispositivo de BNG.

En un modo de realización ejemplar, en el caso de que el dispositivo de NAT esté integrado con el dispositivo de BNG, el dispositivo de NAT notificará al dispositivo de BNG para que ejecute la estrategia de seguridad para el UE de una de las siguientes maneras: el dispositivo de NAT envía la información de identificación del UE a un servidor de estrategia de seguridad, y el servidor de estrategia de seguridad notifica al dispositivo de BNG para que ejecute la estrategia de seguridad para el UE; y el dispositivo de NAT que envía la información de identificación del UE al dispositivo de BNG para notificar al dispositivo de BNG para que ejecute la estrategia de seguridad para el UE.

En un modo de realización ejemplar, después de que el dispositivo de NAT notifique al dispositivo de BNG que ejecute la estrategia de seguridad para el UE, el procedimiento de procesamiento para la traducción de la dirección de red incluye además: si el dispositivo de NAT determina que el establecimiento de la sesión del UE no alcanza el valor predeterminado de umbral o el UE cancela la ejecución de la estrategia de seguridad mediante una página de la Red presentada forzadamente, el dispositivo de NAT notifica al dispositivo de BNG que cancele la ejecución de la estrategia de seguridad para el UE.

En un modo de realización ejemplar, en el caso en que el dispositivo de NAT esté integrado con el dispositivo de BNG, el dispositivo de NAT notifica al dispositivo de BNG cancelar la ejecución de la estrategia de seguridad para el UE de una de las siguientes maneras: el dispositivo de NAT envía la información de identificación del UE al servidor de la estrategia de seguridad, y el servidor de la estrategia de seguridad notifica al dispositivo de BNG cancelar la ejecución de la estrategia de seguridad para el UE; y el dispositivo de NAT envía la información de

identificación del UE al dispositivo de BNG para notificar al dispositivo de BNG que cancele la ejecución de la estrategia de seguridad para el UE.

En un modo de realización ejemplar, en el caso en que una página de la Malla Máxima Mundial (la Red) presentada forzadamente está en una red pública y el dispositivo de NAT ejecuta una operación de presentar forzadamente la página de la Red, apuntando a la conducta de acceso del UE, una sesión establecida por el dispositivo de NAT para el UE incluye: una sesión establecida entre el UE y una conexión del HTTP de la página de la Red presentada a la fuerza.

En un modo de realización ejemplar, una sesión para el dispositivo de NAT para determinar si el establecimiento de sesión del UE alcanza o no el umbral preestablecido incluye al menos uno de los siguientes: una sesión establecida por una conexión del Protocolo de Control de Transmisión (TCP) del UE; una sesión establecida por una conexión del Protocolo de mensajes de control de Internet (ICMP) del UE; y una sesión establecida por una conexión del Protocolo de Datagramas de Usuario (UDP) del UE.

En un modo de realización ejemplar, el umbral preestablecido incluye al menos uno de los siguientes: el número total de sesiones establecidas por el UE y la velocidad de las sesiones de establecimiento por el UE.

En un modo de realización ejemplar, el procedimiento incluye además: el dispositivo de NAT acelera el envejecimiento de una o más sesiones del UE cuando el dispositivo de NAT notifica al dispositivo de BNG para ejecutar la estrategia de seguridad para el UE.

Un dispositivo de NAT de acuerdo a otro modo de realización de la presente invención incluye: un componente de determinación configurado para determinar si el establecimiento de sesión de un equipo de usuario alcanza o no un umbral preestablecido; y un primer componente de notificación configurado para notificar a un dispositivo de BNG para ejecutar una estrategia de seguridad para el UE si el establecimiento de la sesión del UE alcanza el umbral preestablecido, en donde la estrategia de seguridad se usa para detener la conducta de ataque del UE e informar al equipo de usuario de la conducta de ataque del UE.

En un modo de realización ejemplar, el dispositivo de NAT incluye además: un segundo componente de notificación configurado para notificar al dispositivo de BNG que ejecute, apuntando a la conducta de acceso del UE, una operación para forzar al UE a estar fuera de línea o devolver el UE a un estado no autenticado y notificar a un servidor de Autenticación, Autorización y Contabilidad (AAA) para que marque o configure el equipo de usuario como un UE con una conducta de ataque, en donde la primera página de solicitud se usa además para recordar al UE que está forzado a estar fuera de línea o ser devuelto a un estado no autenticado; el UE solicita estar en línea y/o ser autenticado nuevamente por el servidor de AAA; una vez que el UE aprueba la autenticación, el servidor de AAA notifica al dispositivo de BNG que ejecute una estrategia forzada de presentación impuesta de página de la Red, para que el UE redirija la solicitud de acceso a la página del UE a una segunda página de solicitud, en donde la segunda página de solicitud se usa para recordar al UE que una razón por la cual el equipo de usuario fue forzado anteriormente a estar fuera de línea o ser devuelto a un estado no autenticado es la conducta de ataque del UE, y si el UE aún tiene la conducta de ataque, el UE se verá obligado nuevamente a estar fuera de línea o ser devuelto a un estado no autenticado, y recordar al UE que revise y mate los virus y/o los troyanos.

En un modo de realización ejemplar, el dispositivo de NAT incluye además: un tercer componente de notificación configurado para notificar al dispositivo de BNG para cancelar la ejecución de la estrategia de seguridad para el UE si se determina que el establecimiento de sesión del UE no alcanza el umbral preestablecido o el UE cancela la ejecución de la estrategia de seguridad mediante una página de la Red presentada forzadamente.

En un modo de realización ejempla, el dispositivo de NAT incluye además: un componente de procesamiento configurado para notificar al dispositivo de BNG para acelerar el envejecimiento de la sesión del UE cuando se ejecuta la estrategia de seguridad para el UE.

Un dispositivo de pasarela de red de banda ancha (BNG) de acuerdo a otro modo de realización de la presente invención incluye: un primer componente receptor configurado para recibir una primera notificación que es enviada por un dispositivo de NAT para indicar la ejecución de una estrategia de seguridad para un UE, en donde, cuando el establecimiento de sesión del UE alcanza un umbral predeterminado, la estrategia de seguridad se utiliza para detener la conducta de ataque del UE e informar al UE de la conducta de ataque del UE; y un componente de redirección, configurado para ejecutar una estrategia de presentación forzada de una página de la Red, para que el UE redirija una solicitud del HTTP enviada por el UE a una primera página de solicitud, en donde la primera página de solicitud se usa para recordar al UE la existencia de la conducta de ataque en el acceso del UE.

En un modo de realización ejemplar, el dispositivo de BNG incluye además: un segundo componente receptor configurado para recibir una segunda notificación que es enviada por el dispositivo de NAT para indicar la ejecución de una operación para forzar al UE a estar fuera de línea o devolver el UE a un estado no autenticado,

apuntando a la conducta de acceso del UE; y un componente de procesamiento configurado para ejecutar, apuntando a la conducta de acceso del UE, una operación para forzar al UE a estar fuera de línea o devolver el UE al estado no autenticado, de acuerdo a la segunda notificación, y notificar a un servidor de Autenticación, Autorización y Contabilidad (AAA) para marcar o configurar el UE como un UE que tiene una conducta de ataque, en el que la primera página de solicitud se usa además para recordar al UE que está forzado a estar fuera de línea o regresar al estado no autenticado, para permitir que el UE solicite estar en línea y/o ser autenticado nuevamente. El componente de procesamiento está configurado además para ejecutar una estrategia de presentación forzada de páginas de la Red para que el UE redirija la solicitud de acceso a páginas del UE a una segunda página de solicitud después de que el UE apruebe la autenticación realizada por el servidor de AAA, en donde la segunda página de solicitud se usa para recordar al UE que una razón por la cual el UE fue forzado anteriormente a estar fuera de línea o a regresar a un estado no autenticado es la conducta de ataque del UE, y si el UE todavía tiene la conducta de ataque, recordar al UE que está forzado a estar fuera de línea o devuelto al estado no autenticado nuevamente y recordar al UE que revise y elimine virus y/o troyanos.

En los modos de realización de la presente invención, el dispositivo de NAT determina si el establecimiento de sesión del UE alcanza o no el umbral preestablecido, que se refiere al número o la frecuencia del establecimiento de sesión. Si el establecimiento de sesión del UE alcanza el umbral preestablecido, el dispositivo de NAT notifica al dispositivo de BNG que ejecute la estrategia de seguridad para el UE, en donde la estrategia de seguridad se usa para detener la conducta de ataque del UE y notificar al UE sobre la conducta de ataque del UE. Se observa cuando el UE tiene la conducta de ataque, por notificar el dispositivo de NAT al dispositivo de BNG que ejecute la estrategia de seguridad para que el UE detenga la conducta de ataque del UE, y por recordar el dispositivo de NAT al UE la conducta de ataque, a fin de recordar al UE que revise y elimine posibles virus o troyanos, se evitan las quejas presentadas por el usuario contra el operador y se mejoran tanto la tasa de utilización del dispositivo de NAT como la experiencia del usuario.

Breve descripción de los dibujos

Los dibujos ilustrados aquí proporcionan una comprensión adicional de la presente invención y forman parte de la presente solicitud. Las realizaciones ejemplares y la descripción de las mismas se utilizan para explicar la presente invención sin limitar indebidamente el alcance de la presente invención, en la que:

la figura 1 es un diagrama de flujo de un procedimiento de procesamiento para una tecnología de traducción de direcciones de red, de acuerdo a un modo de realización de la presente invención;

la figura 2 es un primer diagrama esquemático de una arquitectura de red, de acuerdo a un modo de realización de la presente invención;

la figura 3 es un segundo diagrama esquemático de la arquitectura de red, de acuerdo a un modo de realización de la presente invención;

la figura 4 es un tercer diagrama esquemático de la arquitectura de red, de acuerdo a un modo de realización de la presente invención;

la figura 5 es un diagrama estructural de un dispositivo de NAT, de acuerdo a un modo de realización de la presente invención;

la figura 6 es un diagrama estructural de un dispositivo de BNG, de acuerdo a un modo de realización de la presente invención;

la figura 7 es un primer diagrama esquemático de una red, de acuerdo a un modo de realización de la presente invención;

la figura 8 es un diagrama de flujo de un procedimiento de procesamiento para la tecnología de traducción de direcciones de red, de acuerdo a un modo de realización de la presente invención;

la figura 9 es un diagrama de flujo de un procedimiento de procesamiento para la tecnología de traducción de direcciones de red, de acuerdo a otro modo de realización de la presente invención;

la figura 10 es un diagrama de flujo de un procedimiento de procesamiento para la tecnología de traducción de direcciones de red, de acuerdo a otro modo de realización de la presente invención;

la figura 11 es un segundo diagrama esquemático de la red, de acuerdo a un modo de realización de la presente invención;

la figura 12 es un diagrama de flujo de un procedimiento de procesamiento para la tecnología de traducción de direcciones de red, de acuerdo a otro modo de realización de la presente invención;

la figura 13 es un diagrama de flujo de un procedimiento de procesamiento para la tecnología de traducción de direcciones de red, de acuerdo a otro modo de realización de la presente invención;

la figura 14 es un tercer diagrama esquemático de la red, de acuerdo a un modo de realización de la presente invención; y

la figura 15 es un diagrama de flujo de un procedimiento de procesamiento para la tecnología de traducción de direcciones de red, de acuerdo a otro modo de realización de la presente invención.

Descripción detallada de los modos de realización

La presente invención se describirá a continuación en detalle con referencia a los dibujos y junto con los modos de realización. Se debe señalar que los modos de realización de la presente solicitud y las características en los modos de realización se pueden combinar entre sí si no existe ningún conflicto.

Se proporciona un procedimiento de procesamiento para una tecnología de conversión de direcciones de red de acuerdo a un modo de realización de la presente invención y, como se muestra en la Figura 1, el procedimiento de procesamiento para la tecnología de direcciones de red incluye la etapa S102 y la etapa S104:

Etapa S102: un dispositivo de NAT determina si el establecimiento de sesión de un UE alcanza o no un umbral preestablecido;

Etapa S104: si el establecimiento de sesión del UE alcanza el umbral preestablecido, el dispositivo de NAT notifica a un dispositivo de BNG para que ejecute una estrategia de seguridad para el UE, en donde la estrategia de seguridad se usa para detener la conducta de ataque del UE e informar al UE de la conducta de ataque del UE.

Con las etapas de procesamiento mencionadas anteriormente, el dispositivo de NAT determina si el establecimiento de sesión del UE alcanza o no el umbral preestablecido, que se refiere al número o la frecuencia del establecimiento de sesión; si el UE alcanza el umbral preestablecido, el dispositivo de NAT notifica al dispositivo de BNG para ejecutar la estrategia de seguridad para el UE, en donde la estrategia de seguridad se usa para detener la conducta de ataque del UE e informar al UE de la conducta de ataque del UE. Se observa que, cuando el UE tiene la conducta de ataque, por ejecutar el dispositivo de BNG la estrategia de seguridad para detener la conducta de ataque del UE y por informar el dispositivo de NAT al UE de la conducta de ataque del UE y recordar al UE que debe verificar y matar virus potenciales o troyanos, se evitan las quejas presentadas por el usuario contra el operador y se mejoran tanto la tasa de utilización del dispositivo de NAT como la experiencia del usuario.

Para hacer que la estrategia de seguridad se ejecute convenientemente, en un modo de realización ejemplar de la presente invención, el dispositivo de BNG ejecuta la estrategia de seguridad para el UE, que incluye: el dispositivo de BNG ejecuta una estrategia de presentación forzada de páginas de la Red para que el UE redirija una solicitud del HTTP enviada por el UE a una primera página de solicitud, en donde la primera página de solicitud se usa para recordar al UE sobre la existencia de la conducta de ataque en el acceso del UE.

Para aumentar la tasa de utilización del dispositivo de BNG, en un modo de realización ejemplar de la presente invención, el dispositivo de BNG redirige una solicitud del HTTP enviada por el UE a la primera página de solicitud, que incluye: el dispositivo de BNG redirige la solicitud del HTTP enviada por el UE a la primera página de solicitud cada período preestablecido. Es decir, el dispositivo de BNG puede interceptar cada mensaje de solicitud del HTTP del UE y redirigir cada mensaje de solicitud del HTTP a la primera página de solicitud, o el dispositivo de BNG intercepta el mensaje de solicitud del HTTP del UE cada período preestablecido y redirige el mensaje de solicitud del HTTP a la primera página de solicitud.

Para permitir que el UE termine la conducta de ataque rápidamente, en un modo de realización ejemplar, la primera página de solicitud se usa además para recordar al UE que revise o elimine virus y/o troyanos.

Para detener la conducta de ataque del UE de manera efectiva, en un modo de realización ejemplar, después de que el dispositivo de BNG ejecute la estrategia de seguridad para el UE, el procedimiento de procesamiento para la tecnología de traducción de direcciones de red incluye además: el dispositivo de NAT notifica al dispositivo de BNG para que ejecute, apuntando a la conducta de acceso del UE, una operación para forzar al UE a estar fuera de línea o devolver el UE a un estado no autenticado, y notifica a un servidor de AAA que marque o establezca al UE como un UE que tiene la conducta de ataque, en donde la primera página de solicitud se utiliza además para recordar al UE que está forzado a estar fuera de línea o a regresar a un estado no autenticado. El UE solicita estar en línea y/o ser autenticado nuevamente. Después de que el UE aprueba la autenticación ejecutada por el servidor de AAA, el servidor de AAA notifica al dispositivo de BNG que ejecute una estrategia de presentación forzada de páginas de la Red, para que el UE redirija la solicitud de acceso a páginas del UE a una segunda

página de solicitud, en donde la segunda página de solicitud se usa para recordar al UE que una razón por la cual el UE fue forzado anteriormente a estar fuera de línea o regresar al estado no autenticado es la conducta de ataque del UE, y si el UE todavía tiene la conducta de ataque, el dispositivo de NAT recuerda al UE que está forzado a estar fuera de línea o a regresar a un estado no autenticado nuevamente y recuerda al UE revisar y eliminar virus y/o troyanos.

En un modo de realización ejemplar, el dispositivo de NAT puede incluir al menos uno de los siguientes: un dispositivo de NAT integrado con el dispositivo de BNG; y un dispositivo de NAT dispuesto por separado del dispositivo de BNG.

En un modo de realización ejemplar, en el caso en que el dispositivo de NAT esté integrado con el dispositivo de BNG, una arquitectura de red para realizar el procedimiento de procesamiento mencionado anteriormente para la tecnología de traducción de direcciones de red puede ser la que se muestra en la Figura 2, y el dispositivo de NAT puede notificar al dispositivo de BNG para realizar la estrategia de seguridad para el UE de una de las siguientes formas: el dispositivo de NAT envía la información de identificación (por ejemplo, la dirección del IP de la red pública y la gama de puertos de la red pública del UE que resulta de una traducción) del UE al servidor de estrategia de seguridad, y el servidor de estrategia de seguridad notifica al dispositivo de BNG para que ejecute la estrategia de seguridad para el UE; y el dispositivo de NAT envía la información de identificación del UE al dispositivo de BNG para notificar al dispositivo de BNG que ejecute la estrategia de seguridad para el UE.

En un modo de realización ejemplar, cuando el dispositivo de NAT es un dispositivo de NAT dispuesto por separado del dispositivo de BNG, la arquitectura de red para realizar el procedimiento de procesamiento mencionado anteriormente para la tecnología de traducción de direcciones de red puede ser como se muestra en la Figura 3 o 4.

Con el fin de satisfacer las demandas de los diferentes escenarios de aplicación, en un modo de realización ejemplar, después de que el dispositivo de NAT notifica al dispositivo de BNG para que ejecute la estrategia de seguridad para el UE, el procedimiento de procesamiento para la tecnología de traducción de direcciones de red incluye: si el dispositivo de NAT determina que el establecimiento de sesión del UE no alcanza el umbral preestablecido o que el UE cancela la ejecución de la estrategia de seguridad mediante una página de la Red de presentación forzada, el dispositivo de NAT notifica al dispositivo de BNG para cancelar la ejecución de la estrategia de seguridad para el UE.

En un modo de realización ejemplar, en el caso en que el dispositivo de NAT esté integrado con el dispositivo de BNG, el dispositivo de NAT puede notificar al dispositivo de BNG para cancelar la ejecución de la estrategia de seguridad para el UE de una de las siguientes maneras: el dispositivo de NAT envía la información de identificación del UE al servidor de la estrategia de seguridad, y el servidor de la estrategia de seguridad notifica al dispositivo de BNG que cancele la ejecución de la estrategia de seguridad para el UE; y el dispositivo de NAT envía la información de identificación del UE al dispositivo de BNG para notificar al dispositivo de BNG que cancele la ejecución de la estrategia de seguridad para el UE.

En un modo de realización ejemplar, el UE cancela la ejecución de la estrategia de seguridad mediante la página de la Red de presentación forzada, que puede incluir: un servidor de la Red envía una estrategia de usuario al dispositivo de NAT mediante el servidor de la estrategia de seguridad para cancelar la ejecución de la estrategia de seguridad; o el servidor de la Red notifica al dispositivo de NAT que distribuya la estrategia del usuario para cancelar la ejecución de la estrategia de seguridad.

En una forma de realización ejemplar, en el caso en el que la página de la Red presentada forzadamente está en una red pública y el dispositivo de NAT ejecuta una operación de presentar forzadamente una página de la Red que apunta a la conducta de acceso del UE, la sesión establecida por el dispositivo de NAT para el UE puede incluir: una sesión establecida entre el UE y la conexión del HTTP que presenta forzadamente la página de la Red.

Para determinar con precisión si el establecimiento de sesión del UE alcanza o no el umbral preestablecido, en un modo de realización ejemplar, la sesión del dispositivo de NAT para determinar si el establecimiento de sesión del UE alcanza o no el umbral preestablecido puede incluir al menos una de las siguientes: la sesión establecida por la conexión del TCP del UE; la sesión establecida por la conexión del ICMP del UE; y la sesión establecida por la conexión del UDP del UE.

En un modo de realización ejemplar, el umbral preestablecido incluye al menos uno de los siguientes: el número total de sesiones establecidas por el UE y la velocidad de las sesiones establecidas por el UE.

Para acortar el tiempo de antigüedad de la sesión del usuario y liberar oportunamente los recursos de la sesión, en un modo de realización ejemplar, el procedimiento incluye además: cuando se notifica al dispositivo de BNG que ejecute la estrategia de seguridad para el UE, el dispositivo de NAT acelera el envejecimiento de la sesión de la UE.

En un modo de realización ejemplar, con el fin de informar de manera flexible y oportuna al UE que el UE tiene una conducta de ataque, el dispositivo de NAT notifica al servidor de estrategia la información de identificación (por ejemplo, la dirección del IP de ataque) del UE mientras ejecuta una estrategia de seguridad del usuario, y luego, a través de la interfaz de terceros del servidor de estrategia, el dispositivo de NAT notifica al UE sobre la conducta de ataque del UE de otras maneras, por ejemplo, enviando un mensaje corto al UE, haciendo una llamada al UE o utilizando otras herramientas de mensajería instantánea.

Se proporciona un dispositivo de NAT de acuerdo a un modo de realización ejemplar; como se muestra en la Figura 5, el dispositivo de NAT incluye: un componente de determinación 502 configurado para determinar si el establecimiento de sesión de un UE alcanza o no un umbral preestablecido; y un primer componente de notificación 504 conectado al componente de determinación 502 y configurado para notificar a un dispositivo de BNG para ejecutar una estrategia de seguridad para el UE si el establecimiento de sesión del UE alcanza el umbral preestablecido, en donde la estrategia de seguridad se usa para detener la conducta de ataque del UE y notificar al UE sobre la conducta de ataque del UE.

En un modo de realización ejemplar, el componente de determinación 502 determina si el establecimiento de sesión del UE alcanza o no el umbral preestablecido, en donde el umbral preestablecido se refiere al número de la sesión establecida por el UE o la frecuencia de la sesión establecida por el UE, y si el establecimiento de sesión del UE alcanza el umbral preestablecido, el primer componente de notificación 504 notifica al dispositivo de BNG para que ejecute una estrategia de seguridad para el UE, en donde la estrategia de seguridad se usa para detener la conducta de ataque del UE y notificar al UE sobre la conducta de ataque del UE. Por lo tanto, cuando el UE tiene la conducta de ataque, por ejecutar el dispositivo de BNG la estrategia de seguridad para detener la conducta de ataque y por recordar el dispositivo de NAT al UE el comportamiento del ataque y recordar al UE verificar y eliminar posibles virus o troyanos, se evitan las quejas presentadas por el usuario contra el operador y se mejoran tanto la tasa de utilización del dispositivo de NAT como la experiencia del usuario.

Para detener efectivamente la conducta de ataque del UE, en un modo de realización ejemplar, el dispositivo de NAT incluye además: un segundo componente de notificación configurado para notificar al dispositivo de BNG para que ejecute, con el objetivo de la conducta de acceso del UE, una operación de forzar al UE a estar fuera de línea o devolver el UE a un estado no autenticado y notificar a un servidor de AAA para que marque o configure el UE como un UE que tiene la conducta de ataque, en donde la primera página de solicitud se usa adicionalmente para recordar al UE que está forzado a estar fuera de línea o a ser devuelto a un estado no autenticado. El UE solicita estar en línea y/o ser autenticado nuevamente. Después de que el UE aprueba la autenticación ejecutada por el servidor de AAA, el servidor de AAA notifica al dispositivo de BNG que ejecute una estrategia de presentación forzada de páginas de la Red, para que el UE redirija la solicitud de acceso a páginas del UE a una segunda página de solicitud, en donde la segunda página de solicitud se usa para recordar al UE que una razón por la que el UE fue forzado anteriormente a estar fuera de línea o ser devuelto a un estado no autenticado es la conducta de ataque del UE, y si el UE todavía tiene la conducta de ataque, el dispositivo de NAT recuerda al UE que está forzado a estar fuera de línea o ser devuelto al estado no autenticado nuevamente y le recuerda al UE que revise y elimine virus y/o troyanos.

En un modo de realización ejemplar, en el caso en que el dispositivo de NAT esté integrado con el dispositivo de BNG, el primer componente de notificación 504 incluye: una primera unidad de envío configurada para enviar la información de identificación (por ejemplo, la dirección del IP de la red pública y la gama de puertos de la red pública del UE resultante de una traducción) del UE a un servidor de estrategia de seguridad, y el servidor de estrategia de seguridad notifica al dispositivo de BNG para que ejecute la estrategia de seguridad para el UE; y/o una segunda unidad de envío configurada para enviar la información de identificación del UE al dispositivo de BNG para notificar al dispositivo de BNG que ejecute la estrategia de seguridad para el UE.

En un modo de realización ejemplar, para satisfacer las demandas de diferentes escenarios de aplicación, el dispositivo de NAT incluye además: un tercer componente de notificación configurado para notificar al dispositivo de BNG para cancelar la ejecución de la estrategia de seguridad para el UE si se determina que el establecimiento de sesión del UE no alcanza el umbral preestablecido o que el UE cancela la ejecución de la estrategia de seguridad mediante una página de la Red de presentación forzada.

En un modo de realización ejemplar, en el caso en que el dispositivo de NAT esté integrado con el dispositivo de BNG, el tercer componente de notificación incluye: una tercera unidad de envío configurada para enviar la información de identificación del UE al servidor de estrategia de seguridad, y el servidor de estrategia de seguridad notifica al dispositivo de BNG para cancelar la ejecución de la estrategia de seguridad para el UE; y/o una cuarta unidad de envío configurada para enviar la información de identificación del UE al dispositivo de BNG para notificar al dispositivo de BNG que cancele la ejecución de la estrategia de seguridad para el UE.

En un modo de realización ejemplar, para acortar el tiempo de antigüedad de la sesión del usuario y liberar oportunamente los recursos de sesión, el dispositivo de NAT incluye además: un componente de procesamiento

configurado para notificar al dispositivo de BNG para acelerar el envejecimiento de la sesión del UE cuando el dispositivo de BNG esté ejecutando la estrategia de seguridad para la UE.

Se proporciona un dispositivo de BNG de acuerdo a un modo de realización ejemplar. Como se muestra en la Figura 6, el dispositivo de BNG incluye: un primer componente receptor 602 configurado para recibir una primera notificación que es enviada por un dispositivo de NAT para indicar la ejecución de una estrategia de seguridad para el UE, en donde, cuando el establecimiento de sesión del UE alcanza un umbral preestablecido, la estrategia de seguridad se usa para detener la conducta de ataque del UE y notificar al UE sobre la conducta de ataque del UE; y un componente de redirección 604 conectado al primer componente receptor 602 y configurado para ejecutar una estrategia de presentación forzada de páginas de la Red, para que el UE redirija una solicitud del HTTP enviada por el UE a una primera página de solicitud, en donde la primera página de solicitud es utilizada para recordar al UE la existencia de la conducta de ataque en el acceso del UE.

En un modo de realización ejemplar, para aumentar la tasa de utilización del dispositivo de BNG, el componente de redirección 604 está configurado para redirigir la solicitud del HTTP enviada por el UE a la primera página de solicitud cada período preestablecido. Es decir, el dispositivo de BNG puede interceptar cada mensaje de solicitud del HTTP del UE y redirigir cada mensaje de solicitud del HTTP a la primera página de solicitud, o el dispositivo de BNG intercepta el mensaje de solicitud del HTTP del UE cada período preestablecido y redirige el mensaje de solicitud del HTTP a la primera página de solicitud.

En un modo de realización ejemplar, para detener efectivamente la conducta de ataque del UE, el dispositivo de BNG incluye además: un segundo componente de recepción configurado para recibir una segunda notificación, que es enviada por el dispositivo de NAT para indicar la ejecución de una operación para forzar al UE para que esté fuera de línea o devolver el UE a un estado no autenticado que apunta a la conducta de acceso del UE; y un componente de procesamiento conectado al segundo componente receptor y configurado para ejecutarse, apuntando a la conducta de acceso del UE, una operación para forzar al UE a estar fuera de línea o devolver el UE al estado no autenticado, de acuerdo a la segunda notificación, y notificar a un servidor de AAA para marcar o configurar el UE como un UE con conducta de ataque, en donde la primera página de solicitud se utiliza además para recordar al UE que está forzado a estar fuera de línea o ser devuelto al estado no autenticado, para permitir que el UE solicite estar en línea y/o ser autenticado de nuevo. El componente de procesamiento está configurado además para ejecutar una estrategia de presentación forzada de páginas de la Red, para que el UE redirija la solicitud de acceso a páginas del UE a una segunda página de solicitud cuando el servidor de AAA notifica al dispositivo de BNG después de que el UE aprueba la autenticación ejecutada por el servidor de AAA, en donde la segunda página de solicitud se usa para recordar al UE que una razón por la que el UE fue forzado anteriormente a estar fuera de línea o ser devuelto al estado no autenticado es la conducta de ataque del UE, y recordar al UE que está forzado a estar fuera de línea o a ser devuelto a un estado no autenticado nuevamente si el UE aún tiene la conducta de ataque, y recordar al UE que revise y elimine virus y/o troyanos.

En un modo de realización ejemplar, el UE es uno cualquiera de los siguientes: un UE que usa un Protocolo de Punto a Punto sobre Ethernet (PPPoE), un UE que usa el Protocolo de Internet sobre Ethernet (IPoE) y un UE en una Internet móvil.

Cada uno de los modos de realización mencionados anteriormente se describe a continuación en detalle con referencia a los dibujos adjuntos.

En un modo de realización ejemplar, al tomar un escenario de red como se muestra en la Figura 7, por ejemplo, el dispositivo de NAT es un dispositivo de NAT convergente, una página de la Red siempre es de presentación forzada cuando el número de sesiones consumidas por el ataque del TCP de un usuario de la NAT alcanza un umbral de activación de la estrategia de seguridad (equivalente al umbral preestablecido) de manera que el usuario cancele la estrategia de seguridad de forma iniciativa mediante la página de la Red y, según el escenario de red, el diagrama de flujo de un procedimiento de procesamiento para la tecnología de traducción de direcciones de red, como se muestra en Figura 8, incluye las siguientes etapas:

etapa S802: el dispositivo de NAT preestablece que el umbral de activación de la estrategia de seguridad sea el 80% del número máximo de sesiones admitidas del usuario;

etapa S804: el dispositivo de NAT determina que el umbral de activación de la estrategia de seguridad se alcanza cuando el usuario tiene un conducta de ataque del TCP;

paso S806: el dispositivo de NAT distribuye una marca de presentación forzada al usuario y luego intercepta todas las conexiones del TCP del usuario al puerto 80 y redirige todos los accesos del HTTP del usuario a la página de solicitud de la Red (equivalente a la primera página de solicitud) del operador, mediante una marca de redirección del HTTP, para recordar al usuario que revise y elimine posibles virus y troyanos; mientras tanto, el dispositivo de NAT acelera dinámicamente el envejecimiento de una sesión inválida del usuario.

etapa S808: después de verificar y eliminar virus y troyanos, el usuario solicita cancelar la estrategia de seguridad en la página de la Red del operador;

etapa S810: el servidor de la Red del operador notifica a un servidor de estrategia que notifique al dispositivo de NAT para cancelar la estrategia de seguridad;

etapa S812: el servidor de estrategia notifica al dispositivo de NAT para cancelar la estrategia de seguridad; y

etapa S814: el usuario accede a la red mediante el dispositivo de NAT.

En un modo de realización ejemplar, al tomar el escenario de red como se muestra en la Figura 7, por ejemplo, el dispositivo de NAT es un dispositivo de NAT convergente, una página de la Red se presenta de manera forzada periódicamente cuando las sesiones consumidas por el ataque del UDP de un usuario de la NAT alcanzan un umbral de activación de la estrategia de seguridad (equivalente al umbral preestablecido anterior) de modo que el dispositivo de NAT cancele de manera iniciativa la estrategia de seguridad después de que se termine la conducta de ataque del usuario y, basándose en el escenario de la red, el diagrama de flujo de un procedimiento de procesamiento para la tecnología de traducción de direcciones de red, como se muestra en la Figura 9, incluye las siguientes etapas:

etapa S902: el dispositivo de NAT preestablece el umbral de activación de la estrategia de seguridad en el 80% de la velocidad máxima admitida de establecimiento de nueva sesión del usuario;

etapa S904: el dispositivo de NAT determina que el umbral de activación de la estrategia de seguridad se alcanza cuando el usuario tiene una conducta de ataque FLOOD del UDP;

etapa S906: el dispositivo de NAT establece una marca de presentación forzada para el usuario e intercepta secuencialmente la conexión del TCP del usuario al puerto 80 y redirige periódicamente la solicitud de acceso del HTTP del usuario a la página de solicitud de la Red del operador, mediante una marca de redirección del HTTP; una parte de las solicitudes del HTTP del usuario para solicitar el acceso a una página de la Red se redireccionan periódicamente a la página de solicitud de la Red del operador para recordar al usuario que revise y elimine posibles virus y troyanos;

etapa S908: la conducta de ataque FLOOD del UDP del usuario desaparece después de que el terminal de usuario comprueba y elimina virus y troyanos;

etapa S910: el dispositivo de NAT determina que la nueva velocidad de establecimiento de sesión del usuario está por debajo del umbral y cancela la estrategia de seguridad del usuario; y

etapa S912: el usuario accede a la red a través del dispositivo de NAT.

En un modo de realización ejemplar, al tomar el escenario de red como se muestra en la Figura 7, por ejemplo, el dispositivo de NAT es un dispositivo de NAT convergente, una página de la Red se presenta forzadamente y el usuario se ve obligado a estar fuera de línea cuando el número de sesiones consumidas por el ataque del TCP de un usuario de la NAT alcanza un umbral de activación de estrategia de seguridad (equivalente al umbral preestablecido anterior), y el diagrama de flujo de un procedimiento de procesamiento para la tecnología de traducción de direcciones de red, como se muestra en la Figura 10, incluye las siguientes etapas:

etapa S1002: el dispositivo de NAT preestablece el umbral de activación de la estrategia de seguridad en el 80% del número máximo de sesiones admisibles del usuario;

etapa S1004: el dispositivo de NAT determina que el umbral de activación de la estrategia de seguridad se alcanza cuando el usuario tiene una conducta de ataque del TCP;

etapa S1006: el dispositivo de NAT obliga al usuario a estar fuera de línea o volver a un estado no autenticado y notifica a un servidor de autenticación que el usuario está fuera de línea debido a un ataque de sesión de la NAT;

Optativamente, antes de forzar al usuario a estar fuera de línea o regresar a un estado no autenticado, el dispositivo de NAT presenta forzadamente una página de la Red para recordar al usuario que está fuera de línea o devuelto al estado no autenticado, y que está en línea o autenticado nuevamente, después de verificar o eliminar posibles virus o Troyanos;

etapa S1008: el usuario marca línea telefónica para estar en línea o inicia una solicitud de autenticación y vuelve a estar en línea después de aprobar la autenticación;

etapa S1010: un servidor de AAA notifica al dispositivo de NAT para redirigir la solicitud del HTTP del usuario a la segunda página de solicitud de la Red (equivalente a la segunda página de solicitud) del operador;

etapa S1012: el dispositivo de NAT redirige la solicitud del HTTP del usuario a la segunda página de solicitud de la Red del operador, para recordar al usuario la razón de la desconexión anterior y recordar al usuario que revise y elimine posibles virus y troyanos potenciales; y

etapa S1014: la segunda página de solicitud de la Red solo se presenta forzadamente una vez, y luego el usuario accede a la red a través del dispositivo de NAT.

Si la operación de verificación y eliminación de virus o troyanos no está implementada o no está completamente implementada por el usuario, entonces la conducta de ataque continúa y el usuario se ve obligado a estar fuera de línea nuevamente cuando el número de sesiones del usuario alcanza el umbral de activación de la estrategia de seguridad de nuevo.

Si el usuario comprueba y elimina con éxito los virus y los troyanos, la conducta de ataque finaliza y el usuario puede continuar accediendo a la red a través del dispositivo de NAT.

En un modo de realización ejemplar, al tomar el escenario de red como se muestra en la Figura 11, por ejemplo, el dispositivo de NAT es un dispositivo de NAT independiente o un encaminador de transición de familias de direcciones (AFTR), un servidor de estrategia notifica a una BNG para ejecutar una estrategia de seguridad del usuario cuando el número de sesiones consumidas por el ataque del TCP de un usuario de la NAT alcanza un umbral de activación de la estrategia de seguridad (equivalente al umbral preestablecido anterior), y el diagrama de flujo de un procedimiento de procesamiento para la tecnología de traducción de direcciones de red, como se muestra en la Figura 12, Incluye las siguientes etapas:

etapa S1202: el dispositivo de NAT preestablece que el umbral de activación de la estrategia de seguridad sea el 80% del número máximo de sesiones admisibles del usuario;

etapa S1204: el dispositivo de NAT determina que el umbral de activación de la estrategia de seguridad se alcanza cuando el usuario tiene una conducta de ataque del TCP;

etapa S1206: el dispositivo de NAT notifica al servidor de estrategia la dirección del IP del usuario;

etapa S1208: el servidor de estrategia notifica al BNG para ejecutar una estrategia de seguridad del usuario;

etapa S1210: el BNG ejecuta la estrategia de seguridad del usuario y redirige la solicitud del HTTP del usuario para recordar al usuario que revise y elimine posibles virus y troyanos;

etapa S1212: después de que el terminal de usuario verifique y elimine virus y troyanos, la conducta de ataque FLOOD del UDP del usuario desaparecerá; y el dispositivo de NAT determina que la conducta de ataque del usuario desaparece y notifica al servidor de estrategia la dirección del IP del usuario;

etapa S1214: el servidor de estrategia notifica a la BNG que cancele la estrategia de seguridad; y

etapa S1216: el usuario accede a la red mediante el dispositivo de NAT.

En un modo de realización ejemplar, al tomar el escenario de red como se muestra en la Figura 11, por ejemplo, el dispositivo de NAT es un dispositivo de NAT independiente o un AFTR, se notifica a una BNG para que ejecute una estrategia de seguridad del usuario cuando el número de las sesiones consumidas por el ataque del TCP de un usuario de la NAT alcanza un umbral de activación de estrategia de seguridad (equivalente al umbral preestablecido anterior), y el diagrama de flujo de un procedimiento de procesamiento para la tecnología de traducción de direcciones de red, como se muestra en la Figura 13, incluye las siguientes etapas:

etapa S1302: el dispositivo de NAT preestablece el umbral de activación de la estrategia de seguridad en el 80% de la velocidad máxima permitida de establecimiento de nueva sesión del usuario;

etapa S1304: el dispositivo de NAT determina que el umbral de activación de la estrategia de seguridad se alcanza cuando el usuario tiene una conducta de ataque del TCP;

etapa S1306: el dispositivo de NAT envía la dirección del IP del usuario a la BNG para notificar a la BNG que ejecute la estrategia de seguridad del usuario;

etapa S1308: la BNG ejecuta la estrategia de seguridad del usuario y redirige la solicitud del HTTP del usuario para recordar al usuario que revise y elimine posibles virus y troyanos;

etapa S1310: después de que el terminal de usuario verifique y elimine virus y troyanos, la conducta de ataque FLOOD del UDP del usuario desaparece; y el dispositivo de NAT determina que la conducta de ataque del

usuario desaparece y envía la dirección del IP del usuario a la BNG para notificar a la BNG que cancele la estrategia de seguridad; y

etapa S1312: el usuario accede a la red mediante el dispositivo de NAT.

En un modo de realización ejemplar, por tomar el escenario de red como se muestra en la Figura 14, por ejemplo, el dispositivo de NAT anterior es un dispositivo de NAT independiente o integrado con una CA, un servidor de estrategia notifica a una BNG para que ejecute una estrategia de seguridad del usuario cuando el número de las sesiones consumidas por el ataque del TCP de un usuario de una NAT alcanza un umbral de activación de la estrategia de seguridad (equivalente al umbral preestablecido anterior), y el diagrama de flujo de un procedimiento de procesamiento para la tecnología de traducción de direcciones de red, como se muestra en la Figura 15, incluye las siguientes etapas:

etapa S1502: el dispositivo de NAT preestablece el umbral de activación de la estrategia de seguridad en el 80% del número máximo de sesiones admisibles del usuario y asigna una dirección de red pública y una gama de puertos de red públicos traducidos por una dirección de usuario a la dirección de red privada del usuario;

etapa S1504: el dispositivo de NAT determina que el umbral de activación de la estrategia de seguridad se ha alcanzado cuando el usuario tiene una conducta de ataque del TCP;

etapa S1506: el dispositivo de NAT notifica al servidor de estrategia la dirección del IP de la red pública y la gama de puertos de la red pública, traducidos por la dirección del usuario;

etapa S1508: el servidor de estrategia envía la dirección del IP de la red pública y la gama de puertos de la red pública, traducidos por la dirección del usuario, a la BNG para notificar a la BNG que ejecute una estrategia de seguridad del usuario;

etapa S1510: la BNG ejecuta una estrategia de seguridad del usuario y redirige la solicitud del HTTP del usuario para recordar al usuario que revise y elimine posibles virus y troyanos;

etapa S1512: después de que el terminal de usuario verifique y elimine virus y troyanos, la conducta de ataque FLOOD del UDP del usuario desaparece; y el dispositivo de NAT determina que la conducta de ataque del usuario desaparece y notifica al servidor de estrategia la dirección del IP del usuario;

etapa S1514: el servidor de estrategia notifica a la BNG que cancele la estrategia de seguridad; y

etapa S1516: el usuario accede a la red mediante el dispositivo de NAT y la BNG.

Se puede ver por lo que antecede que los modos de realización ejemplares realizan el siguiente efecto técnico que, por medio del dispositivo de NAT, determina si el establecimiento de sesión del UE alcanza o no el umbral preestablecido que se refiere al número de sesión establecido por el UE o a la frecuencia de la sesión establecida por el UE, el dispositivo de NAT notifica al dispositivo de BNG que ejecute una estrategia de seguridad para el UE si el establecimiento de sesión del UE alcanza el umbral predeterminado, en donde la estrategia de seguridad se usa para detener la conducta de ataque del UE y notificar al UE sobre la conducta de ataque del UE. Cuando el UE tiene la conducta de ataque, por ejecutar el dispositivo de BNG la estrategia de seguridad para detener la conducta de ataque, por recordar el dispositivo de NAT al UE la conducta de ataque y recordar comprobar y eliminar posibles virus o troyanos, se evitan las quejas presentadas por el usuario contra el operador y mejoran tanto la tasa de utilización del dispositivo de NAT como la experiencia del usuario.

Obviamente, los expertos en la técnica entenderán que los componentes y las etapas anteriormente mencionadas de la presente invención se pueden realizar mediante el uso de un dispositivo de cálculo de propósito general, se pueden integrar en un dispositivo de cálculo o distribuirse en una red que consiste en una pluralidad de dispositivos de cálculo. 26

Alternativamente, los componentes y las etapas de la presente invención se pueden realizar mediante el uso del código de programa ejecutable del dispositivo de cálculo. En consecuencia, se pueden almacenar en el dispositivo de almacenamiento y ejecutarse mediante el dispositivo de cálculo, o se hacen componentes de circuito integrado, respectivamente, o una pluralidad de componentes o etapas de los mismos se hacen componentes de un circuito integrado. De esta manera, la presente invención no se limita a ninguna combinación particular de hardware y software.

Aplicabilidad Industrial

La solución técnica proporcionada en el presente documento se puede aplicar al campo de la traducción de direcciones de red para resolver el problema de que el usuario presenta quejas contra el operador debido al comportamiento anormal de su propio anfitrión, detener la conducta de ataque de un UE ejecutando un

estrategia de seguridad cuando el UE tiene la conducta de ataque, recordar al UE su propia conducta de ataque y recordar al usuario que revise y elimine posibles virus y troyanos y, por consiguiente, evita las quejas presentadas por el usuario contra el operador y mejora la tasa de utilización de un dispositivo de NAT.

REIVINDICACIONES

1. Un procedimiento de procesamiento para una tecnología de traducción de direcciones de red, NAT, que comprende:

determinar, mediante un dispositivo de NAT, si el establecimiento de sesión de un equipo de usuario, UE, alcanza o no un umbral preestablecido (S 102);

notificar, mediante el dispositivo de NAT, a un dispositivo de Pasarela de Red de Banda Ancha, BNG, para ejecutar una estrategia de seguridad para el UE si el establecimiento de sesión del UE alcanza el umbral preestablecido, en donde la estrategia de seguridad se usa para detener la conducta de ataque del UE e informar el UE de la conducta de ataque del UE (S104);

en donde ejecutar, mediante el dispositivo de BNG, la estrategia de seguridad para el UE comprende: ejecutar, el dispositivo de BNG, una estrategia de presentación forzada de páginas de la Red para que el UE redirija una solicitud del protocolo de transferencia de hipertexto, HTTP, enviada por el UE a una primera página de solicitud, en donde la primera página de solicitud se utiliza para informar al UE de la existencia de la conducta de ataque durante el acceso del UE.

2. El procedimiento de acuerdo a la reivindicación 1, en el que la redirección, mediante el dispositivo de BNG, de la solicitud del HTTP enviada por el UE a la primera página de solicitud comprende:

redirigir, mediante el dispositivo de BNG, la solicitud del HTTP enviada por el UE a la primera página de solicitud en el intervalo preestablecido; o

la primera página de solicitud se usa para recordar al UE que revise o elimine virus y/o troyanos; o

después de la ejecución, mediante el dispositivo de BNG, de la estrategia de seguridad para el UE, el procedimiento comprende además:

notificar, mediante el dispositivo de NAT, al dispositivo de BNG para ejecutar, apuntando a la conducta de acceso del UE, una operación para forzar al UE a estar fuera de línea o devolver el UE a un estado no autenticado; y notificar, mediante el dispositivo de NAT, a un servidor de Autenticación, Autorización y Contabilidad, AAA, para marcar o configurar el UE como un UE que tiene la conducta de ataque, en donde la primera página de solicitud se usa para recordar al UE que el UE ha de ser forzado a estar fuera de línea o ser devuelto al estado no autenticado;

solicitar, mediante el UE, estar en línea y/o ser autenticado nuevamente; autenticar, mediante el servidor de AAA, al UE; después de que el UE aprueba la autenticación, notificar, mediante el servidor de AAA, al dispositivo de BNG que ejecute una estrategia de presentación forzada de páginas de la Red para que el UE vuelva a dirigir una solicitud de acceso a páginas del UE a una segunda página de solicitud, en donde la segunda página de solicitud se usa para recordar al UE que una razón por la que el UE fue forzado anteriormente a estar fuera de línea o ser devuelto al estado no autenticado es la conducta de ataque del UE y, si el UE aún tiene la conducta de ataque, el UE se verá obligado a estar fuera de línea o ser devuelto al estado no autenticado, y recordar al UE que revise y elimine los virus y/o los troyanos.

3. Un procedimiento de acuerdo a la reivindicación 1, en el que el dispositivo de NAT comprende al menos uno de los siguientes:

un dispositivo de NAT integrado con el dispositivo de BNG; y

un dispositivo de NAT dispuesto por separado del dispositivo de BNG;

preferiblemente, en el caso en que el dispositivo de NAT esté integrado con el dispositivo de BNG, notificar, mediante el dispositivo de NAT, al dispositivo de BNG que ejecute la estrategia de seguridad para el UE de una de las siguientes maneras:

enviar, mediante el dispositivo de NAT, información de identificación del UE a un servidor de estrategia de seguridad y notificar, mediante el servidor de estrategia de seguridad, al dispositivo de BNG para que ejecute la estrategia de seguridad para el UE; y

enviar, mediante el dispositivo de NAT, la información de identificación del UE al dispositivo de BNG para notificar al dispositivo de BNG para que ejecute la estrategia de seguridad para el UE.

4. El procedimiento de acuerdo a la reivindicación 3, en el que, después de notificar, mediante el dispositivo de NAT, al dispositivo de BNG para ejecutar la estrategia de seguridad para el UE, el procedimiento comprende además:

si el dispositivo de NAT determina que el establecimiento de sesión del UE no alcanza el umbral preestablecido o que el UE cancela la ejecución de la estrategia de seguridad mediante una página de la Red de presentación forzada, notificar, mediante el dispositivo de NAT, al dispositivo de BNG para cancelar la ejecución de la estrategia de seguridad para la UE.

5. El procedimiento de acuerdo a la reivindicación 4, en el que, en el caso de que el dispositivo de NAT esté integrado con el dispositivo de BNG, notificar, mediante el dispositivo de NAT, al dispositivo de BNG que cancele la ejecución de la estrategia de seguridad para el UE de una de las siguientes maneras:

enviar, mediante el dispositivo de NAT, información de identificación del UE a un servidor de estrategia de seguridad y notificar, mediante el servidor de estrategia de seguridad, al dispositivo de BNG para cancelar la ejecución de la estrategia de seguridad para el UE; y

enviar, mediante el dispositivo de NAT, la información de identificación del UE al dispositivo de BNG, para notificar al dispositivo de BNG que cancele la ejecución de la estrategia de seguridad para el UE.

6. El procedimiento de acuerdo a una cualquiera de las reivindicaciones 1 a 3, en el que, en el caso de que una página de la Red presentada forzadamente esté en una red pública y el dispositivo de NAT ejecute una operación de presentar forzadamente una página de la Red que apunta a la conducta de acceso del UE, una sesión establecida por el dispositivo de NAT para el UE comprende:

una sesión establecida entre el UE y una conexión del HTTP de la página de la Red de presentación forzada.

7. El procedimiento de acuerdo a una cualquiera de las reivindicaciones 1 a 3, en el que una sesión para que el dispositivo de NAT determine si el establecimiento de sesión del UE alcanza o no el umbral preestablecido comprende al menos uno de los siguientes:

una sesión establecida por una conexión del Protocolo de Control de Transmisión, TCP, del UE;

una sesión establecida por una conexión del Protocolo de Mensajes de Control de Internet, ICMP, del UE; y

una sesión establecida por una conexión del Protocolo de Datagramas de Usuario, UDP, del UE.

8. El procedimiento de acuerdo a una cualquiera de las reivindicaciones 1 a 3, en el que el umbral preestablecido comprende al menos uno de los siguientes:

el número total de sesiones establecido por el UE y la velocidad para establecer sesiones por el UE; o

acelerar, mediante el dispositivo de NAT, el envejecimiento de una o más sesiones del UE cuando el dispositivo de NAT notifica al dispositivo de BNG para ejecutar la estrategia de seguridad para el UE.

9. Un dispositivo de traducción de direcciones de red, NAT, que comprende:

un componente de determinación (502) configurado para determinar si el establecimiento de sesión de un UE alcanza o no un umbral preestablecido; y

un primer componente de notificación (504) configurado para notificar a un dispositivo de Pasarela de Red de Banda Ancha, BNG, para ejecutar una estrategia de seguridad para el UE si el establecimiento de sesión del UE alcanza el umbral preestablecido, en donde la estrategia de seguridad se utiliza para detener la conducta de ataque del UE e informar al UE de la conducta de ataque del UE;

en el que la etapa de ejecutar, mediante el dispositivo de BNG, la estrategia de seguridad para el UE comprende: ejecutar, mediante el dispositivo de BNG, una estrategia de presentación forzada de páginas de la Red para que el UE redirija una solicitud del protocolo de transferencia de hipertexto, HTTP, enviada por el UE a una primera página de solicitud, en la que la primera página de solicitud se utiliza para informar al UE de la existencia de la conducta de ataque durante el acceso del UE.

10. El dispositivo de NAT de acuerdo a la reivindicación 9, en el que el dispositivo comprende además:

un segundo componente de notificación configurado para notificar al dispositivo de BNG para ejecutar, apuntando a la conducta de acceso del UE, una operación para forzar al UE a estar fuera de línea

o devolver el UE a un estado no autenticado y notificar a un servidor de Autenticación, Autorización y Contabilidad, AAA, para marcar o configurar el UE como un UE que tiene la conducta de ataque, en donde la primera página de solicitud se usa además para recordar al UE que el UE ha de ser forzado a estar fuera de línea o devuelto al estado no autenticado, para permitir que el UE solicite estar en línea y/o ser autenticado nuevamente;

estando el segundo componente de notificación configurado además para notificar al dispositivo de BNG que ejecute una estrategia de presentación forzada de páginas de la Red, para que el UE redirija la solicitud de acceso a la página del UE a una segunda página de solicitud después de que el UE apruebe la autenticación ejecutada por el servidor de AAA, en donde la segunda página de solicitud se usa para informar al UE que una razón por la que el UE fue forzado anteriormente a estar fuera de línea o devuelto al estado no autenticado es la conducta de ataque del UE, y recordar al UE que el UE se verá obligado a estar fuera de línea o devuelto nuevamente al estado no autenticado si el UE aún tiene la conducta de ataque, y recordar al UE que revise y elimine virus y/o troyanos.

11. El dispositivo de NAT de acuerdo a la reivindicación 9 o 10, en donde el dispositivo de NAT comprende además:

un tercer componente de notificación configurado para notificar al dispositivo de BNG para cancelar la ejecución de la estrategia de seguridad para el UE si se determina que el establecimiento de sesión del UE no alcanza el umbral predeterminado o que el UE cancela la ejecución de la estrategia de seguridad mediante una página de la Red de presentación forzada.

12. El dispositivo de NAT de acuerdo a la reivindicación 9 o 10, en donde el dispositivo de NAT comprende además:

un componente de procesamiento configurado para acelerar el envejecimiento de una o más sesiones del UE cuando el dispositivo de NAT notifica al dispositivo de BNG para ejecutar la estrategia de seguridad para el UE.

13. Un dispositivo de pasarela de red de banda ancha, BNG, que comprende:

un primer componente receptor (602) configurado para recibir una primera notificación que es enviada por un dispositivo de NAT para indicar la ejecución de una estrategia de seguridad para un UE, en donde, cuando el establecimiento de la sesión del UE alcanza un umbral preestablecido, la estrategia de seguridad se usa para detener la conducta de ataque del UE e informar al UE de la conducta de ataque del UE; y

un componente redirigido (604) configurado para ejecutar una estrategia de presentación forzada de páginas de la Red para que el UE redirija una solicitud del HTTP enviada por el UE a una primera página de solicitud, en donde la primera página de solicitud se usa para informar al UE de la existencia de la conducta de ataque en el acceso de la UE.

14. El dispositivo magnético de acuerdo a la reivindicación 13, en donde el dispositivo de BNG comprende además:

un segundo componente de recepción configurado para recibir una segunda notificación que es enviada por el dispositivo de NAT para indicar la ejecución de una operación para forzar al UE a estar fuera de línea o devolver al UE a un estado no autenticado que apunta a la conducta de acceso del UE; y

un componente de procesamiento configurado para ejecutar, apuntando a la conducta de acceso del UE, una operación para forzar al UE a estar fuera de línea o devolver el UE al estado no autenticado de acuerdo a la segunda notificación y notificar a un Servidor de Autentificación, Autorización y Contabilidad, AAA para marcar o configurar el UE como un UE que tiene la conducta de ataque, en el que la primera página de solicitud se usa además para recordar al UE que el UE debe ser forzado a estar fuera de línea o ser devuelto al estado no autenticado para permitir que el UE solicite estar en línea y/o ser autenticado nuevamente;

el componente de procesamiento configurado además para ejecutar una estrategia de presentación forzada de páginas de la Red para que el UE redirija una solicitud de acceso a páginas del UE a una segunda página de solicitud, cuando el servidor AAA notifica al dispositivo de BNG, después de que el UE aprueba la autenticación ejecutada por el servidor de AAA, en donde la segunda página de solicitud le recuerda al UE que una razón por la que el UE fue forzado anteriormente a estar fuera de línea o devuelto a un estado no autenticado es la conducta de ataque del UE, y le recuerda al UE que el UE se verá obligado a estar fuera de línea o volver a un estado no autenticado nuevamente si el UE aún tiene la conducta de ataque, y recuerda al UE que revise y elimine virus y/o troyanos.

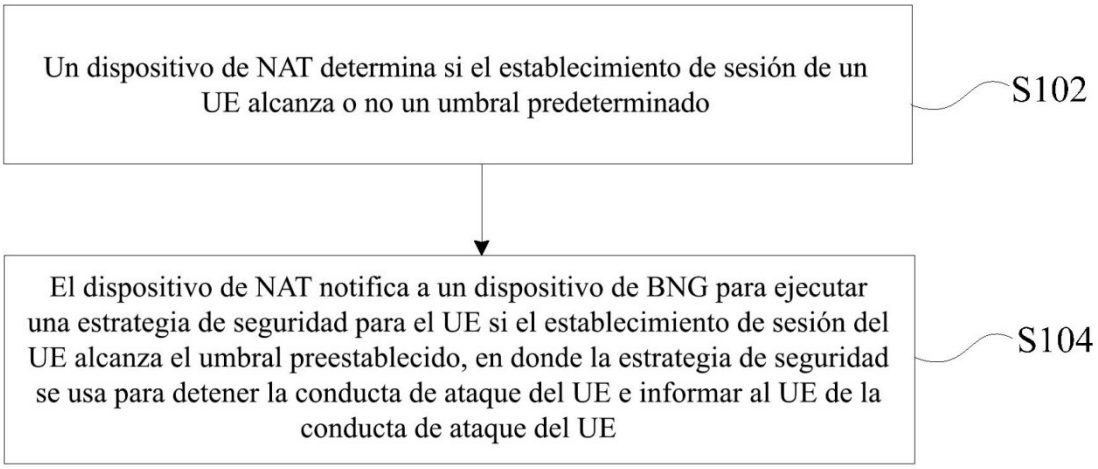
Un dispositivo de NAT determina si el establecimiento de sesión de un UE alcanza o no un umbral predeterminado
S102
El dispositivo de NAT notifica a un dispositivo de BNG para ejecutar una estrategia de seguridad para el UE si el establecimiento de sesión del UE alcanza el umbral preestablecido, en donde la estrategia de seguridad se usa para detener la conducta de ataque del UE e informar al UE de la conducta de ataque del UE
S104

Fig. 1

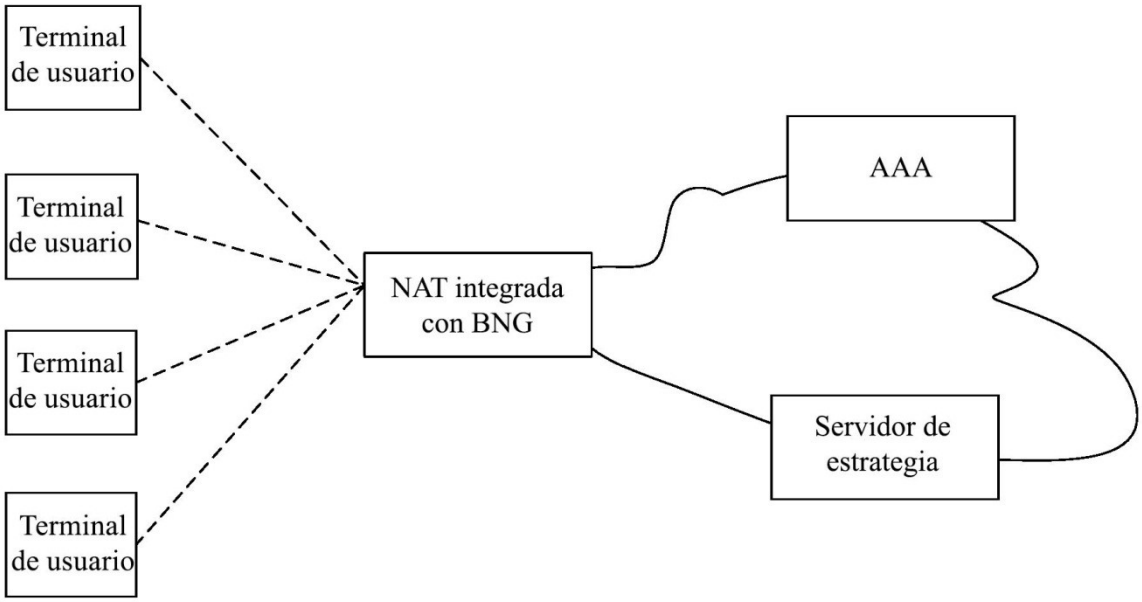
Terminal de usuario
Terminal de usuario
Terminal de usuario
Terminal de usuario
NAT integrada con BNG
AAA
Servidor de estrategia

Fig. 2

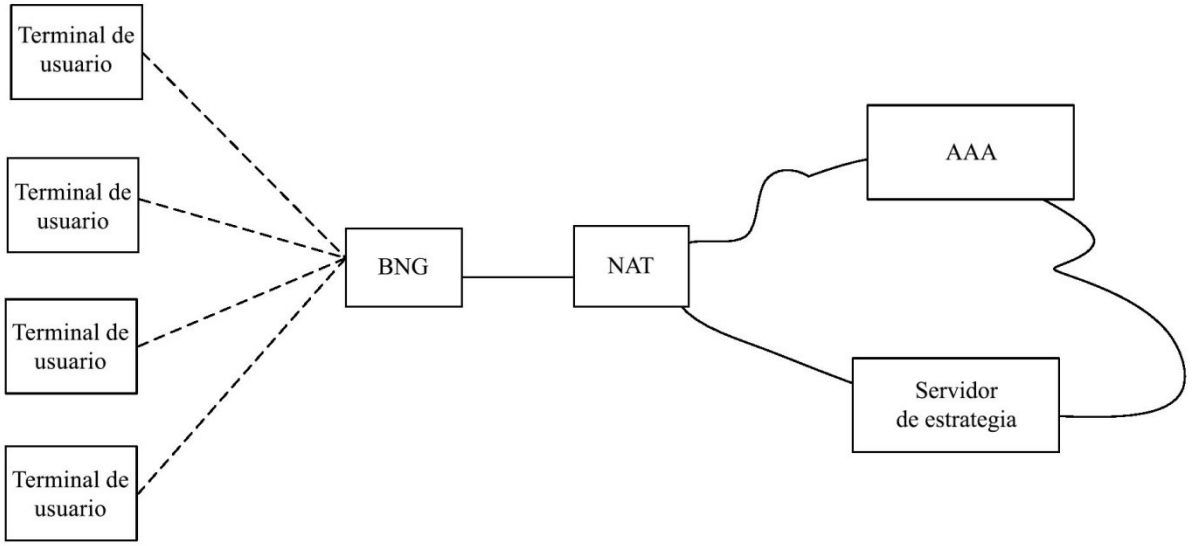
Terminal de usuario
Terminal de usuario
Terminal de usuario
Terminal de usuario
BNG
NAT
AAA
Servidor de estrategia

Fig. 3

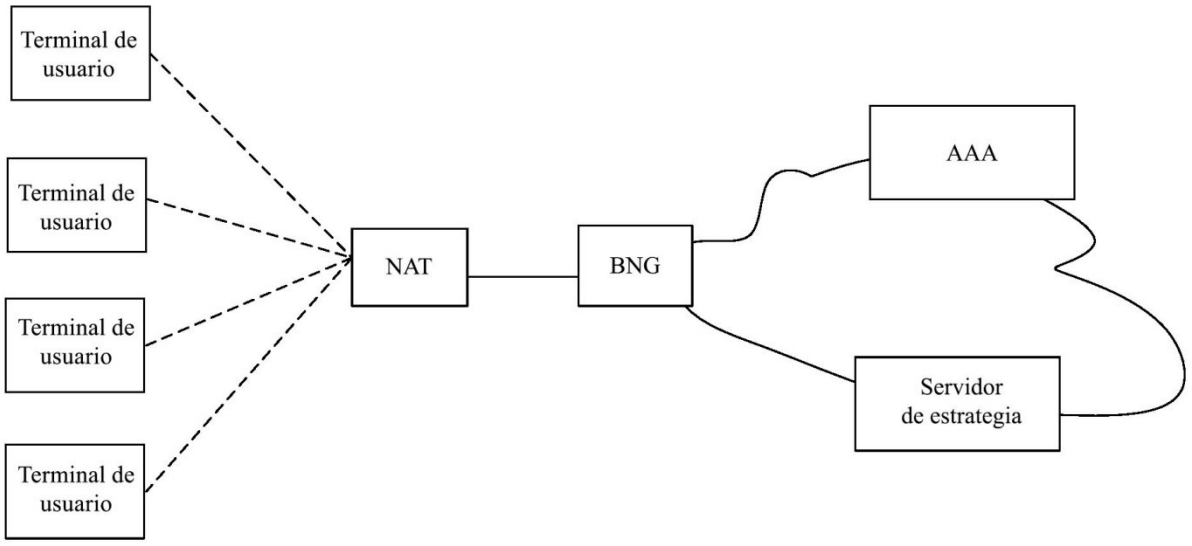
Terminal de usuario
Terminal de usuario
Terminal de usuario
Terminal de usuario
NAT
BNG
AAA
Servidor de estrategia

Fig. 4

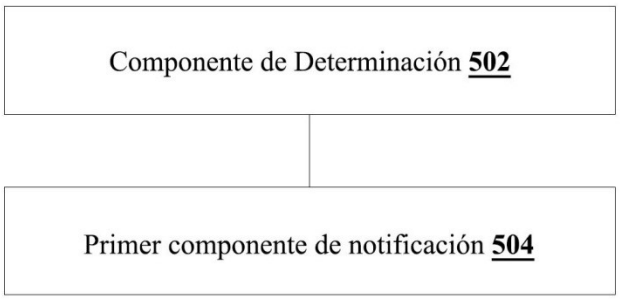

Fig. 5

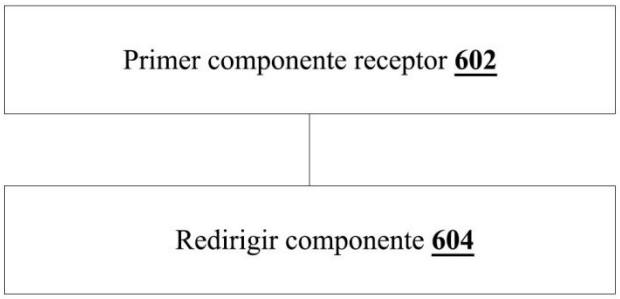

Fig. 6

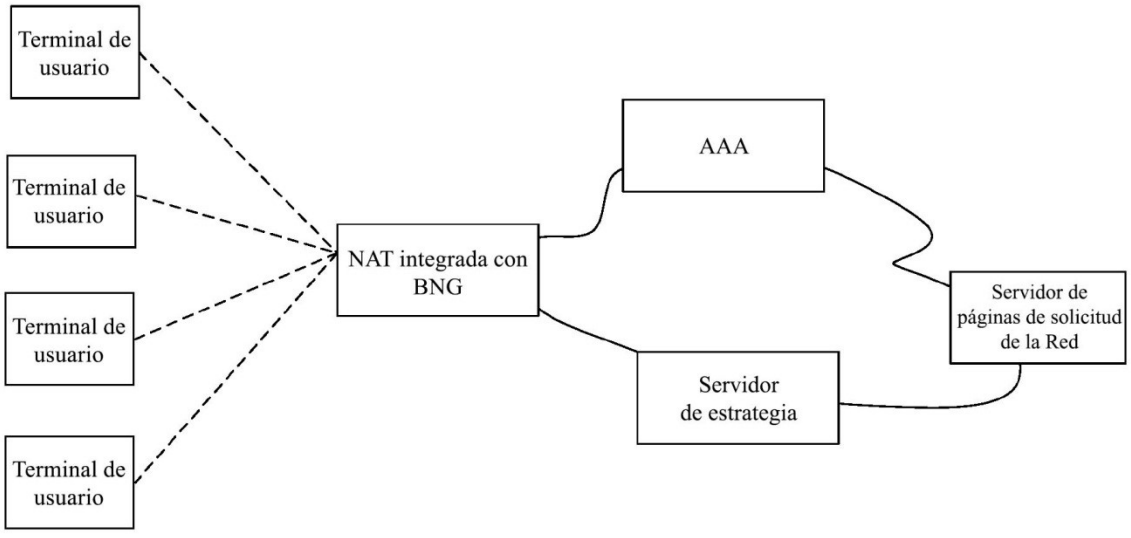

Fig. 7

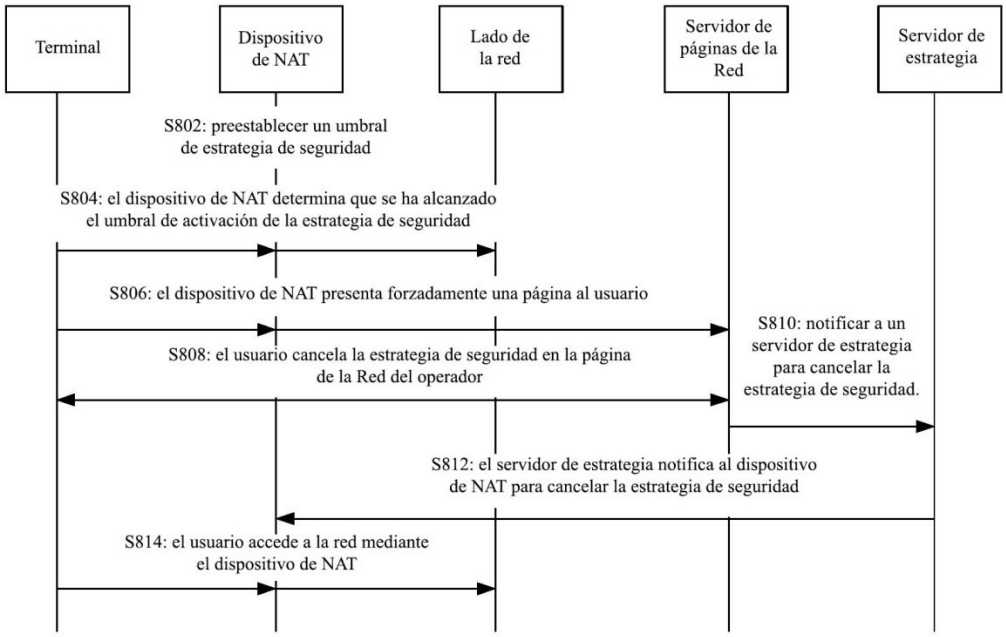
Terminal
Dispositivo de NAT
Lado de la red
Servidor de páginas de la Red
Servidor de estrategia
S802: preestablecer un umbral de estrategia de seguridad
S804: el dispositivo de NAT determina que se ha alcanzado el umbral de activación de la estrategia de seguridad
S806: el dispositivo de NAT presenta forzadamente una página al usuario
S808: el usuario cancela la estrategia de seguridad en la página de la Red del operador
S810: notificar a un servidor de estrategia para cancelar la estrategia de seguridad.
S812: el servidor de estrategia notifica al dispositivo de NAT para cancelar la estrategia de seguridad
S814: el usuario accede a la red mediante el dispositivo de NAT

Fig. 8

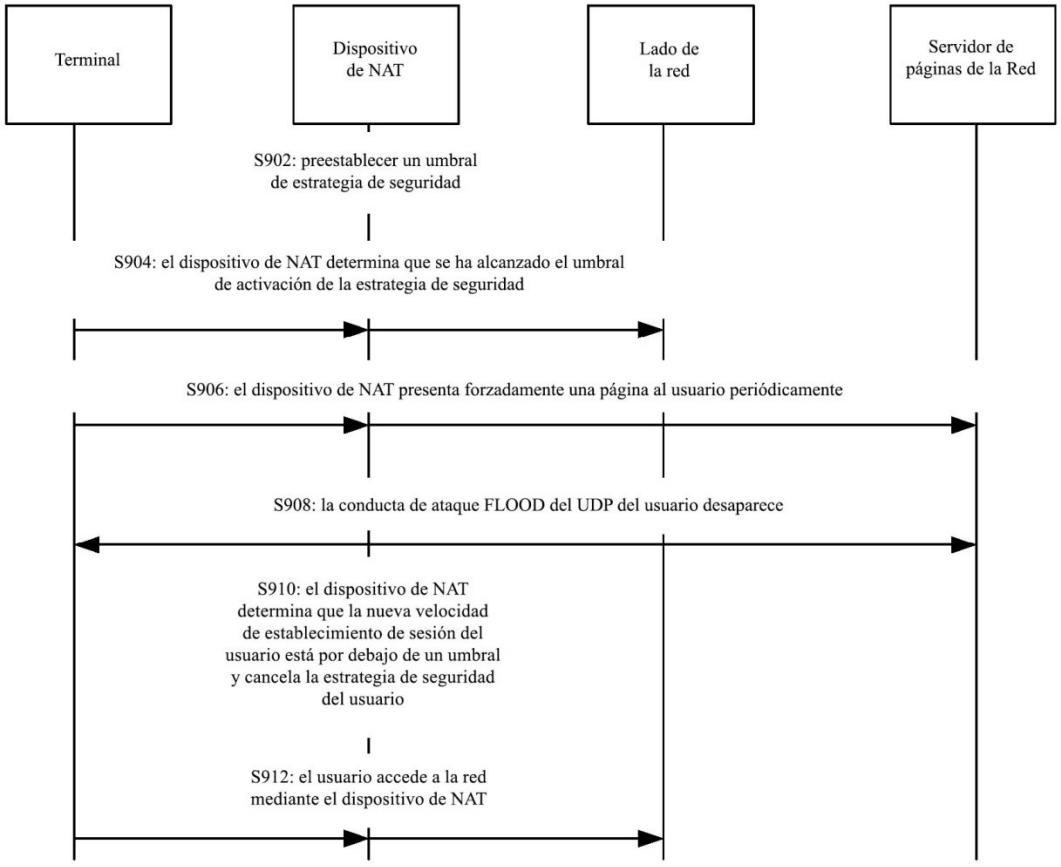
Terminal
Dispositivo de NAT
Lado de la red
Servidor de páginas de la Red
S902: preestablecer un umbral de estrategia de seguridad
S904: el dispositivo de NAT determina que se ha alcanzado el umbral de activación de la estrategia de seguridad
S906: el dispositivo de NAT presenta forzadamente una página al usuario periódicamente
S908: la conducta de ataque FLOOD del UDP del usuario desaparece
S910: el dispositivo de NAT determina que la nueva velocidad de establecimiento de sesión del usuario está por debajo de un umbral y cancela la estrategia de seguridad del usuario
S912: el usuario accede a la red mediante el dispositivo de NAT

Fig. 9

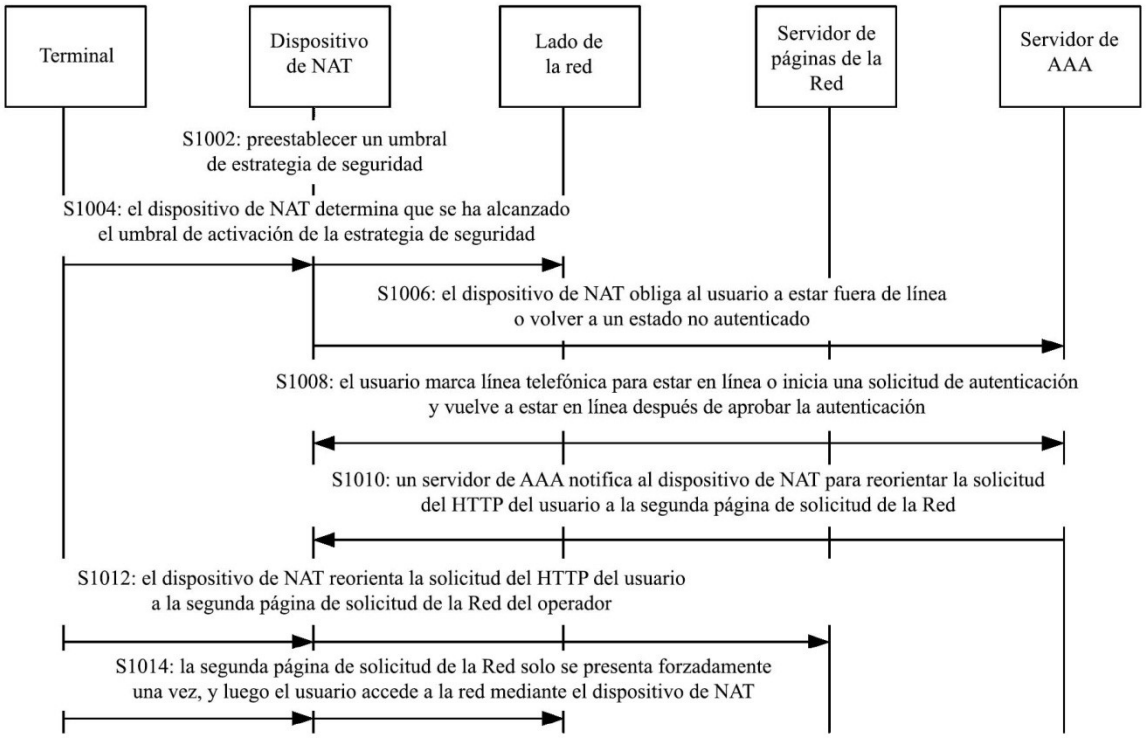
Terminal
Dispositivo de NAT
Lado de la red
Servidor de páginas de la Red
Servidor de AAA
S1002: preestablecer un umbral de estrategia de seguridad
S1004: el dispositivo de NAT determina que se ha alcanzado el umbral de activación de la estrategia de seguridad
S1006: el dispositivo de NAT obliga al usuario a estar fuera de línea o volver a un estado no autenticado
S1008: el usuario marca línea telefónica para estar en línea o inicia una solicitud de autenticación y vuelve a estar en línea después de aprobar la autenticación
S1010: un servidor de AAA notifica al dispositivo de NAT para reorientar la solicitud del HTTP del usuario a la segunda página de solicitud de la Red
S1012: el dispositivo de NAT reorienta la solicitud del HTTP del usuario a la segunda página de solicitud de la Red del operador
S1014: la segunda página de solicitud de la Red solo se presenta forzadamente una vez, y luego el usuario accede a la red mediante el dispositivo de NAT

Fig.10

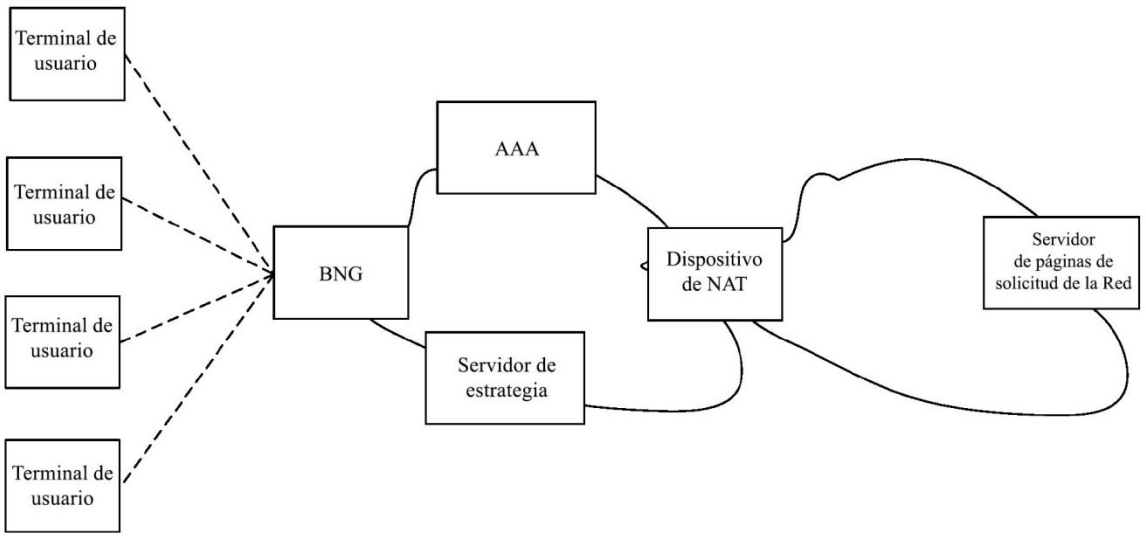
Terminal de usuario
Terminal de usuario
Terminal de usuario
Terminal de usuario
BNG
AAA
Dispositivo de NAT
Servidor de estrategia
Servidor de páginas de solicitud de la Red

Fig. 11

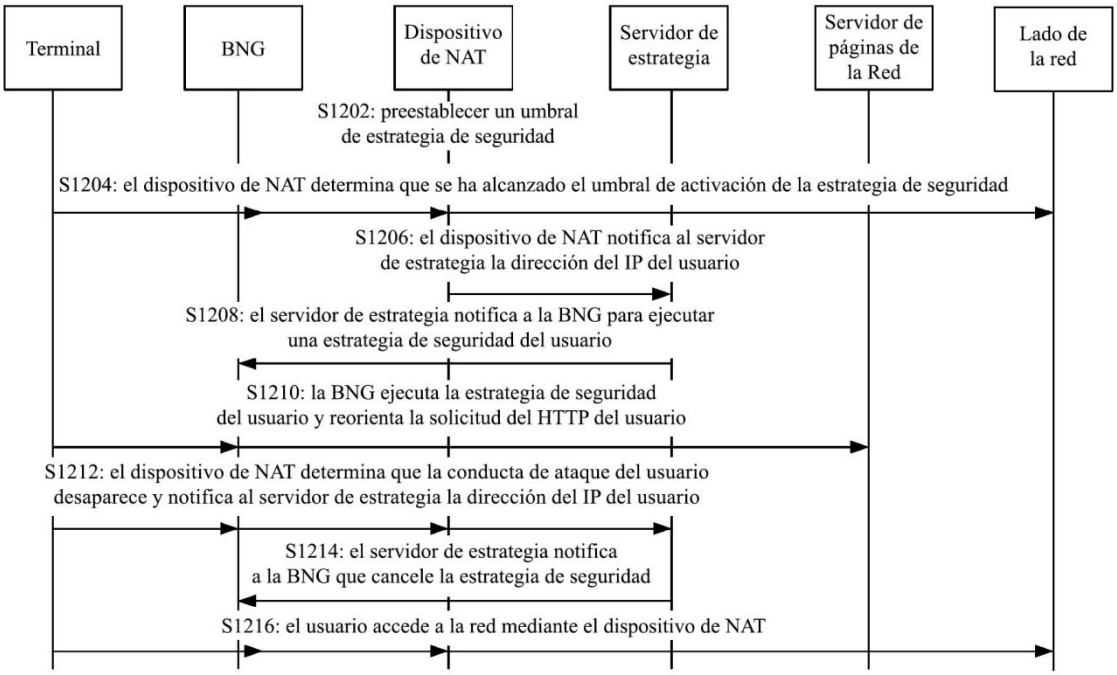
Terminal
BNG
Dispositivo de NAT
Servidor de estrategia
Servidor de páginas de la Red
Lado de la red
S1202: preestablecer un umbral de estrategia de seguridad
S1204: el dispositivo de NAT determina que se ha alcanzado el umbral de activación de la estrategia de seguridad
S1206: el dispositivo de NAT notifica al servidor de estrategia la dirección del IP del usuario
S1208: el servidor de estrategia notifica a la BNG para ejecutar una estrategia de seguridad del usuario
S1210: la BNG ejecuta la estrategia de seguridad del usuario y reorienta la solicitud del HTTP del usuario
S1212: el dispositivo de NAT determina que la conducta de ataque del usuario desaparece y notifica al servidor de estrategia la dirección del IP del usuario
S1214: el servidor de estrategia notifica a la BNG que cancele la estrategia de seguridad
S1216: el usuario accede a la red mediante el dispositivo de NAT

Fig. 12

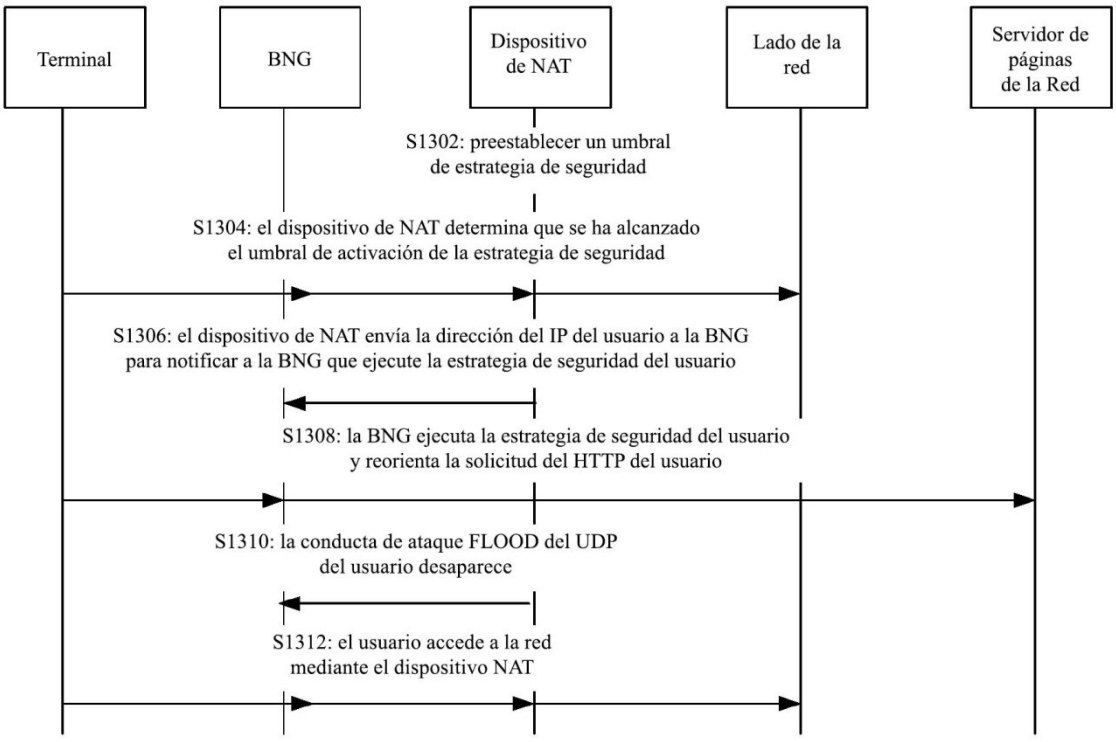
Terminal
BNG
Dispositivo de NAT
Lado de la red
Servidor de páginas de la Red
S1302: preestablecer un umbral de estrategia de seguridad
S1304: el dispositivo de NAT determina que se ha alcanzado el umbral de activación de la estrategia de seguridad
S1306: el dispositivo de NAT envía la dirección del IP del usuario a la BNG para notificar a la BNG que ejecute la estrategia de seguridad del usuario
S1308: la BNG ejecuta la estrategia de seguridad del usuario y reorienta la solicitud del HTTP del usuario
S1310: la conducta de ataque FLOOD del UDP del usuario desaparece
S1312: el usuario accede a la red mediante el dispositivo NAT

Fig. 13

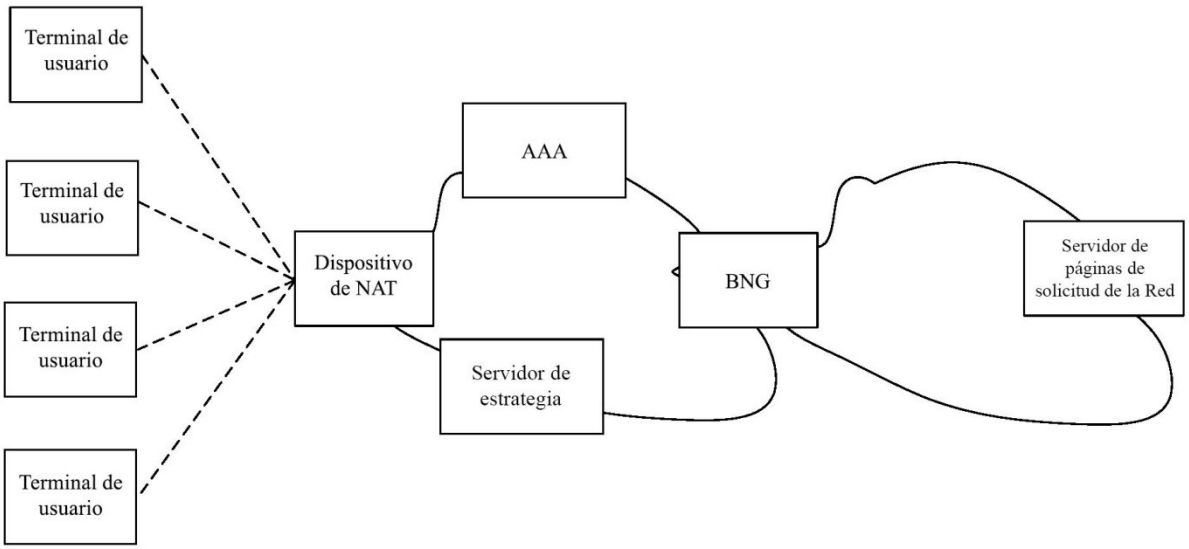
Terminal de usuario
Terminal de usuario
Terminal de usuario
Terminal de usuario
Dispositivo de NAT
AAA
Servidor de estrategia
BNG
Servidor de páginas de solicitud de la Red

Fig. 14

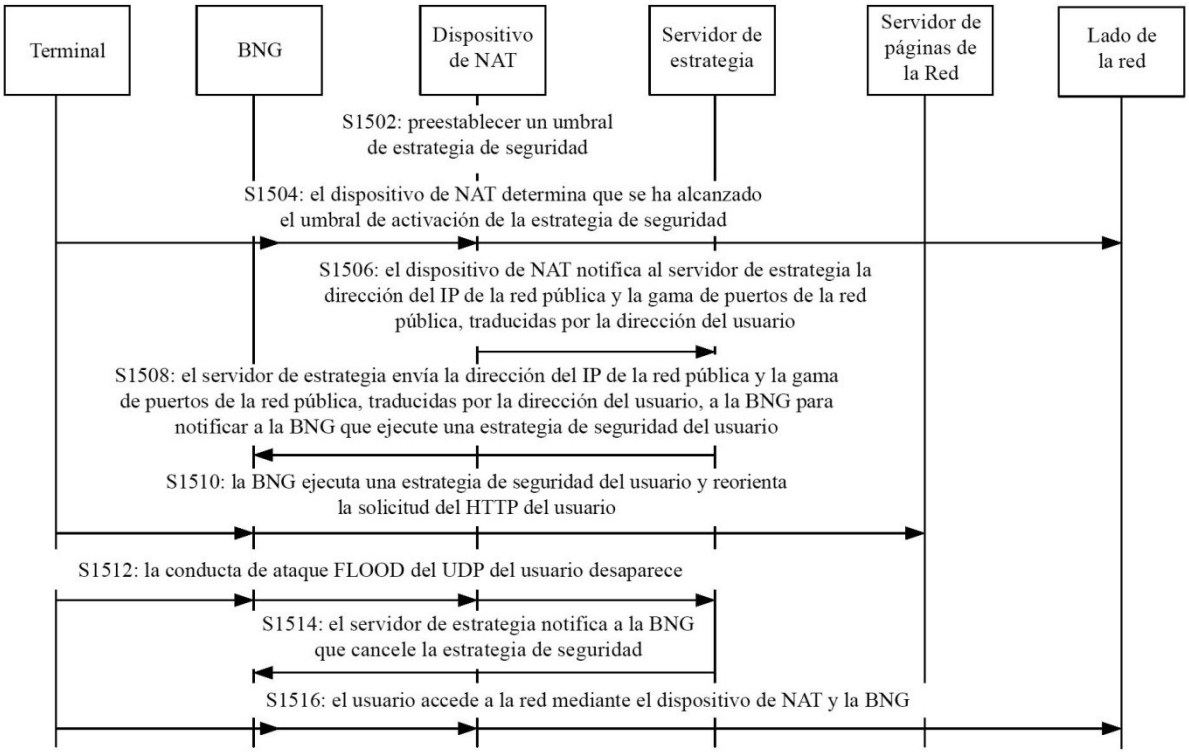
Terminal
BNG
Dispositivo de NAT
Servidor de estrategia
Servidor de páginas de la Red
Lado de la red
S1502: preestablecer un umbral de estrategia de seguridad
S1504: el dispositivo de NAT determina que se ha alcanzado el umbral de activación de la estrategia de seguridad
S1506: el dispositivo de NAT notifica al servidor de estrategia la dirección del IP de la red pública y la gama de puertos de la red pública, traducidas por la dirección del usuario
S1508: el servidor de estrategia envía la dirección del IP de la red pública y la gama de puertos de la red pública, traducidas por la dirección del usuario, a la BNG para notificar a la BNG que ejecute una estrategia de seguridad del usuario
S1510: la BNG ejecuta una estrategia de seguridad del usuario y reorienta la solicitud del HTTP del usuario
S1512: la conducta de ataque FLOOD del UDP del usuario desaparece
S1514: el servidor de estrategia notifica a la BNG que cancele la estrategia de seguridad
S1516: el usuario accede a la red mediante el dispositivo de NAT y la BNG

Fig. 15