(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 747 380**

(51) Int. CI.:

H04L 12/58 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **26.06.2013 PCT/CN2013/077995**

(87) Fecha y número de publicación internacional: **31.12.2014 WO14205669**

(96) Fecha de presentación y número de la solicitud europea: **26.06.2013 E 13887614 (9)**

(97) Fecha y número de publicación de la concesión europea: **07.08.2019 EP 2985957**

(54) Título: **Dispositivo de red y método de procesamiento de solicitud de correo electrónico**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
10.03.2020

(73) Titular/es:

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

(72) Inventor/es:

ZHENG, NENGHONG y
GUO, XIANZHI

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

DESCRIPCIÓN

Dispositivo de red y método de procesamiento de solicitud de correo electrónico

Campo técnico

La presente invención se refiere al campo de las tecnologías de la comunicación, y en particular a un dispositivo de red y a un método para procesar una solicitud de correo electrónico.

Antecedentes de la invención

Un correo electrónico (correo electrónico, email) es una forma de comunicación que permite el intercambio de información por medios electrónicos. Al utilizar un sistema de correo electrónico en una red, un usuario puede ponerse en contacto con un usuario de la red en cualquier parte del mundo de una manera muy rápida. Un mensaje de correo electrónico puede presentar varias formas como texto, imagen y sonido. El Protocolo de acceso a mensajes de Internet 4 (Protocolo de acceso a mensajes de Internet 4, IMAP4) es un protocolo que especifica cómo un ordenador personal accede de forma remota a un servidor de correo electrónico en Internet para enviar y recibir un correo. El IMAP4 admite que un cliente, en línea o sin conexión, puede acceder y leer un mensaje de correo electrónico en un servidor. Un usuario puede realizar directamente una operación en el mensaje de correo electrónico en el servidor utilizando un dispositivo cliente. Aquí, la operación incluye: leer un mensaje de correo electrónico en línea o comprobar información en línea como el asunto de un correo electrónico, el tamaño, o una dirección de remitente. El usuario puede además mantener (incluyendo operaciones como mover, crear, borrar, renombrar, compartir o capturar texto) un directorio de correo del usuario en el servidor. El IMAP4 admite que el usuario pueda determinar, al navegar por un encabezado de correo electrónico, ya sea para recibir o borrar una parte específica de un correo, y crear o cambiar una carpeta o un buzón en el servidor de correo electrónico. Además, aparte de admitir un modo de operación sin conexión POP3 (Protocolo de oficina de correo 3, Protocolo de oficina de correo 3), el IMAP4 además admite una operación en línea y en modo sin conexión. Por lo tanto, IMAP4 proporciona al usuario la función de recibir selectivamente un mensaje de correo electrónico del servidor de correo electrónico, una función de procesamiento de información basada en el servidor, y una función de intercambio de buzón. Actualmente, el IMAP4 ha sido aplicado ampliamente como un importante protocolo de correo.

En la actualidad, muchos dispositivos de pasarela de seguridad son compatibles con el IMAP4. Los dispositivos de pasarela de seguridad generalmente implementan, basados en el IMAP4, el proxy de un servidor de correo electrónico. Una pasarela de seguridad recibe una solicitud de operación de correo enviada por un cliente, y reenvía, al cliente de acuerdo con la solicitud de operación de correo, un mensaje de correo electrónico adquirido desde el servidor de correo electrónico. Además, la pasarela de seguridad puede implementar, en el proceso de proxy, procesos de seguridad como el procesamiento de antivirus o la filtración de correos en el mensaje de correo electrónico, con el fin de proteger la seguridad del cliente.

Sin embargo, en la técnica anterior, en una situación en la que un usuario recibe solamente una parte de un mensaje de correo electrónico (por ejemplo, un archivo adjunto de un correo electrónico), una pasarela de seguridad no puede obtener el contenido de la parte, en forma decodificada, del mensaje de correo electrónico. Por lo tanto, la pasarela de seguridad puede reenviar, al usuario, solo la parte del mensaje de correo electrónico que no se somete a un proceso de seguridad y que es devuelta por un servidor de correo electrónico.

El documento JP2007151159A proporciona un dispositivo servidor proxy de correo electrónico para llevar a cabo un proceso de eliminación de correo electrónico, sin verse afectado por la desconexión de la comunicación, en lugar de un servidor de correo electrónico.

El documento US 6 654 787 B1 (ARONSON DANIEL ALEX [US] ET AL) 25 de noviembre de 2003 (25/11/2003), describe un método y un aparato mediante el cual se aplican técnicas de filtración dinámica para filtrar los mensajes de correo electrónico no deseados en diversas etapas de transmisión a través de una o más redes.

Compendio

Los problemas de la técnica anterior se resuelven mediante el método para procesar una solicitud de que un dispositivo cliente adquiera un mensaje de correo electrónico de un servidor de correo electrónico según la reivindicación 1 y la pasarela de seguridad según la reivindicación 7. Las reivindicaciones dependientes describen realizaciones ventajosas del método según la reivindicación 1.

Breve descripción de los dibujos

A fin de describir las soluciones técnicas en las realizaciones de la presente invención o en la técnica anterior con mayor claridad, a continuación se presentan brevemente los dibujos que la acompañan necesarios para describir las realizaciones o la técnica anterior.

La FIG. 1 es un diagrama de un escenario de aplicación de un método para procesar una solicitud de correo electrónico según una realización de la presente invención;

La FIG. 2 es un diagrama estructural esquemático de un mensaje de correo electrónico según una realización de la presente invención;

La FIG. 3 es un diagrama esquemático de una estructura física de una pasarela de seguridad según una realización de la presente invención;

La FIG. 4 es un diagrama de flujo de un método para procesar una solicitud de correo electrónico según una realización de la presente invención;

La FIG. 5 es un diagrama de flujo de otro método para procesar una solicitud de correo electrónico según una realización de la presente invención; y

La FIG. 6 es un diagrama esquemático de señalización de otro método para procesar una solicitud de correo electrónico según una realización de la presente invención.

Descripción de las realizaciones

Para hacer que un experto en la técnica comprenda mejor las soluciones técnicas de la presente invención, lo siguiente describe de manera clara y completa las soluciones técnicas en las realizaciones de la presente invención con referencia a los dibujos que la acompañan en las realizaciones de la presente invención. Aparentemente, las realizaciones descritas son más bien una parte en lugar de la totalidad de las realizaciones de la presente invención.

La FIG. 1 es un diagrama de un escenario de aplicación de un método para procesar una solicitud de correo electrónico de acuerdo con una realización de la presente invención. En el escenario de aplicación mostrado en la FIG. 1, se incluye un dispositivo 100 cliente, un conmutador 105, una pasarela 110 de seguridad, un enrutador 115 y un servidor 120 de correo electrónico. Todos, el dispositivo 100 cliente, la pasarela 110 de seguridad, y el servidor 120 de correo electrónico, pueden admitir el Protocolo de acceso a mensajes de Internet 4 (Protocolo de acceso a mensajes de Internet 4, IMAP4). La pasarela 110 de seguridad puede desplegarse en una salida de una intranet, una salida de Internet, o un extremo frontal del servidor 120 de correo electrónico. La pasarela 110 de seguridad puede establecer una conexión entre el dispositivo 100 cliente y el servidor 120 de correo electrónico en forma de proxy transparente o proxy no transparente. La pasarela 110 de seguridad puede realizar el procesamiento de seguridad, como la detección del virus y la filtración de correo, en un mensaje de correo electrónico enviado por el servidor 120 de correo electrónico al dispositivo 100 cliente, con el fin de proteger la seguridad del dispositivo 100 cliente en la intranet. El proxy transparente se refiere a que el dispositivo 100 cliente no conoce la existencia de un dispositivo proxy (por ejemplo, la pasarela 110 de seguridad en la FIG. 1), y el dispositivo 100 cliente y el servidor 120 de correo electrónico pueden comunicarse entre sí utilizando un canal transparente establecido por la pasarela 110 de seguridad. El proxy no transparente se refiere a que el dispositivo 100 cliente conoce la existencia de la pasarela 110 de seguridad, y el dispositivo 100 cliente solo puede acceder al servidor 120 de correo electrónico utilizando la pasarela 110 de seguridad.

Por ejemplo, en el escenario de aplicación mostrado en la FIG. 1, la pasarela 110 de seguridad se despliega en la salida de la intranet, y establece la conexión entre el dispositivo 100 cliente y el servidor 120 de correo electrónico en forma de proxy transparente. El dispositivo 100 cliente accede, basado en el IMAP4, al servidor 120 de correo electrónico en Internet. Una solicitud de acceso del dispositivo cliente 100 llega a la pasarela de seguridad 110 mediante el uso del conmutador 105. Sirviendo como dispositivo proxy del servidor 120 de correo electrónico, la pasarela 110 de seguridad puede determinar, de acuerdo con la solicitud de acceso del dispositivo cliente 100 si la pasarela 110 de seguridad ha almacenado en memoria caché un mensaje de correo electrónico requerido por el dispositivo 100 cliente. Si el mensaje de correo electrónico requerido por el dispositivo 100 cliente se almacena en la memoria caché, la pasarela 110 de seguridad puede enviar directamente el mensaje de correo electrónico al dispositivo 100 cliente. Si no se almacena ningún mensaje de correo electrónico requerido por el dispositivo 100 cliente, la pasarela 110 de seguridad puede enviar la solicitud de acceso del dispositivo 100 cliente al servidor 120 de correo electrónico utilizando el enrutador 115, y reenviar el mensaje de correo electrónico al dispositivo 100 cliente después de realizar el procesamiento de seguridad, como la detección de virus y la filtración de correo, en mensaje de correo electrónico devuelto por el servidor 120 de correo electrónico.

En esta realización de la presente invención, se pueden incluir múltiples dispositivos 100 cliente. El dispositivo 100 cliente puede ser un dispositivo que puede implementar el acceso a la red, por ejemplo, un teléfono móvil o un ordenador. Cabe señalar que la pasarela 110 de seguridad en esta realización de la presente invención es solo un ejemplo de un dispositivo de red. Esta realización de la presente invención también se puede aplicar a otro dispositivo de red que puede implementar, basado en el IMAP4, una función de proxy de correo, por ejemplo, un cortafuegos. Además, el dispositivo de red puede desplegarse por separado en una red como un dispositivo independiente, o puede estar ubicado en otro dispositivo, como un cortafuegos o una pasarela de seguridad, que no está limitada en esta realización.

La mayoría de los mensajes de correo electrónico se transmiten en un formato especificado por extensiones multipropósito de correo de Internet (Multipurpose Internet Mail Extensions, MIME). El protocolo MIME es un estándar de correo electrónico extendido y puede admitir mensajes de correo electrónico de varios formatos como un carácter no ASCII y un archivo adjunto de formato binario. Para la claridad de la descripción, en esta realización

de la presente invención, el mensaje de correo electrónico se divide en tres partes: un encabezado del correo electrónico, un cuerpo principal del correo y un archivo adjunto. El encabezado del correo electrónico incluye información como la fecha de envío, la dirección del remitente, la dirección del destinatario, y el asunto del correo electrónico.

Un experto en la técnica puede aprender que el protocolo MIME se implementa mediante campos adicionales de encabezado (campos) de un mensaje de correo electrónico estándar. Estos campos adicionales del encabezado describen el contenido y una forma organizativa de un nuevo tipo de mensaje. En esta realización de la presente invención, un mensaje de correo electrónico en un formato MIME se divide en un encabezado de información MIME y un cuerpo MIME. El encabezado de información MIME se implementa agregando campos adicionales de encabezado de un encabezado de correo electrónico del mensaje de correo electrónico. De esta manera, el encabezado de información MIME incluye el contenido del encabezado del correo electrónico. La información de campo registrada en los campos adicionales del encabezado de información MIME actúa sobre todo el mensaje de correo electrónico. El encabezado de información MIME puede incluir los siguientes campos:

MIME version: la versión MIME, que se utiliza para indicar una versión de un protocolo MIME con el que un paquete cumple, por ejemplo, Mime version: 1.0;

Content-Type: tipo de contenido, que se utiliza para especificar un tipo de paquete. En general, el tipo de contenido puede incluir texto, imagen, audio, vídeo, aplicaciones, multiparte, mensaje y similares, por ejemplo, Content-Type: multipart/mixed. El tipo de contenido puede incluir además un conjunto de caracteres (char set) de una forma de codificación de texto de un cuerpo principal o similar, donde el conjunto de caracteres (char set) puede incluir tipos de caracteres como ASCII, GB2312, Times New Roman y Arial;

Content-Transfer-Encoding: codificación de transferencia de contenido, que se utiliza para especificar una forma de codificación ejecutada para datos e incluye tipos de codificación de transferencia como 7 bits 8 bits, base64, binario, codificación QP, y personalizado, por ejemplo, Content-Transfer-Encoding: base64;

Content-Disposition: disposición del contenido, que se utiliza para incitar al cliente a decidir si un archivo adjunto se presenta en línea o actúa como un archivo adjunto independiente, por ejemplo, Content-Disposition: archivo adjunto; y

Content-Description: descripción del contenido, que es un texto libre utilizado para describir cualquier contenido de segmentos de información.

El cuerpo MIME puede incluir múltiples segmentos MIME. Cada segmento MIME se implementa añadiendo campos adicionales al encabezado de un cuerpo principal o un archivo adjunto de un correo electrónico. De esta manera, los segmentos MIME incluyen por separado el cuerpo principal o el archivo adjunto del correo electrónico. En esta realización de la presente invención, cada segmento MIME se divide en un encabezado de segmento MIME y un cuerpo de segmento MIME. El encabezado de segmento MIME puede incluir cualquier otro campo, excepto la MIME version, en el encabezado de información MIME. La información de campo registrada en el encabezado de segmento MIME solo puede actuar en el segmento MIME. Por ejemplo, si existe Content-Transfer-Encoding en el encabezado de información MIME, se aplica a todo el cuerpo de información. Sin embargo, si el Content-Transfer-Encoding se presenta en un encabezado de segmento MIME de un segmento MIME, se puede aplicar solamente al segmento MIME. Debido a que cualquier dato que no sea de 7 bits en un mensaje de correo electrónico puede pasar a través de una pasarela de correo de Internet solamente después de codificarse en un modo de codificación, un dispositivo cliente puede decodificar un mensaje de correo electrónico recibido utilizando información del Content-Transfer-Encoding. El cuerpo de segmento MIME incluye un cuerpo principal o un archivo adjunto de correo electrónico que se codifica utilizando el Content-Transfer-Encoding en el encabezado de segmento MIME. Ciertamente, se puede comprender que, si el encabezado de segmento MIME no incluye la información del Content-Transfer-Encoding, el cuerpo de segmento MIME será un cuerpo principal o un archivo adjunto de un correo electrónico que se codifica utilizando la información del Content-Transfer-Encoding incluida en el encabezado de información MIME.

La FIG. 2 es un diagrama estructural esquemático de un mensaje de correo electrónico según una realización de la presente invención. Como se muestra en la FIG. 2, un mensaje 200 de correo electrónico incluye un encabezado 202 de correo electrónico, un cuerpo 204 principal de correo, y un archivo adjunto 206 de correo electrónico. El archivo adjunto 206 de correo electrónico incluye dos archivos adjuntos: un archivo adjunto 1 y un archivo adjunto 2. Después de que el mensaje 200 de correo electrónico se procesa utilizando un formato especificado en un protocolo MIME, el mensaje 200 de correo electrónico puede dividirse en dos partes: un encabezado 208 de información MIME y un cuerpo 210 MIME. El encabezado 208 de información MIME incluye información en el encabezado 202 de correo electrónico, y puede incluir específicamente información como una fecha de envío del mensaje de correo electrónico, una dirección del remitente, una dirección del destinatario y un asunto de correo electrónico. El cuerpo 210 MIME incluye además tres segmentos MIME: un segmento 1 MIME, un segmento 2 MIME, y un segmento 3 MIME. El segmento 1 MIME incluye el contenido del cuerpo 204 principal de correo; el segmento 2 MIME incluye el contenido del archivo adjunto 1; y el segmento 3 MIME incluye el contenido del archivo adjunto 2. Cada segmento

MIME se divide además en dos partes: un encabezado de segmento MIME y un cuerpo de segmento MIME. Por ejemplo, el segmento 1 MIME se divide en un encabezado de segmento 1 MIME y un cuerpo de segmento 1 MIME; el segmento 2 MIME se divide en un encabezado de segmento 2 MIME y un cuerpo de segmento 2 MIME; y el segmento 3 MIME se divide en un encabezado de segmento 3 MIME y un cuerpo de segmento 3 MIME. El encabezado de segmento 1 MIME puede incluir información de campos como Content-Type y Content-Transfer-Encoding, donde un campo Content-Type puede incluir además un conjunto de caracteres (char set) del cuerpo 204 principal de correo; y el cuerpo de segmento 1 MIME incluye el contenido del cuerpo 204 principal de correo que está codificado de una forma especificada por un campo de Content-Transfer-Encoding en el encabezado de segmento 1 MIME. El encabezado de segmento 2 MIME puede incluir información de campos como Content-Type, Content-Transfer-Encoding, y Content-Disposition. En un campo Content-Disposition, se puede especificar además un nombre de archivo de un archivo adjunto y el cuerpo de segmento 2 MIME incluye el contenido del archivo adjunto 1 que está codificado de una forma especificada por un campo Content-Transfer-Encoding en el encabezado de segmento 2 MIME. Una estructura de segmento 3 MIME es similar a la del segmento 2 MIME, y los detalles no se describen repetidamente en esta realización.

Debido a que el IMAP4 permite que un dispositivo cliente adquiera la totalidad o parte de un mensaje de correo electrónico, cuando el dispositivo cliente desea adquirir solamente un cuerpo principal de correo o un archivo adjunto, un servidor de correo electrónico devuelve solo el cuerpo de segmento 1 MIME, el cuerpo de segmento 2 MIME, o el cuerpo de segmento 3 MIME que se muestra en la FIG. 2, pero no devuelve información en el encabezado de segmento 1 MIME, el encabezado de segmento 2 MIME, o el encabezado de segmento 3 MIME. Por lo tanto, un dispositivo de red como un cortafuegos o una pasarela no puede aprender a codificar la información del cuerpo principal del correo o del archivo adjunto. El dispositivo de red no puede realizar una operación de decodificación para aprender el cuerpo principal del correo o del archivo adjunto que está en forma decodificada; y, además, el dispositivo de red no puede realizar el procesamiento de seguridad, como el procesamiento de antivirus o filtración de correo, en el contenido del mensaje de correo que está en forma decodificada.

La FIG. 3 es un diagrama esquemático de una estructura física de la pasarela 110 de seguridad de la FIG. 1 de acuerdo con una realización de la presente invención. Como se muestra en la FIG. 3, la pasarela 110 de seguridad incluye: una interfaz 310 de comunicaciones (interfaz de comunicaciones), una memoria 320 (memoria), un procesador 330 (procesador), y un bus 340 de comunicaciones. La interfaz 310 de comunicaciones, la memoria 320 y el procesador 330 se comunican entre sí utilizando el bus 340 de comunicaciones.

La interfaz 310 de comunicaciones está configurada para comunicarse con otro dispositivo. El otro dispositivo puede incluir un dispositivo como un dispositivo cliente, un conmutador, un enrutador o un servidor de correo electrónico.

La memoria 320 está configurada para almacenar un programa 322, almacenar en caché una solicitud 326 de adquisición de correo electrónico enviada por el dispositivo 100 cliente, y almacenar en caché un mensaje 324 de correo electrónico enviado por el servidor 120 de correo electrónico. La memoria 320 puede incluir una memoria RAM de alta velocidad, y puede incluir además una memoria no volátil (memoria no volátil), por ejemplo, al menos una memoria de disco magnético. Se puede comprender que, la memoria 320 puede ser cualquier medio no transitorio (no transitorio) legible por máquina que pueda almacenar el código de programa, como una ROM, una RAM, un disco magnético, un disco duro, un disco óptico, o una memoria no volátil. La memoria 320 puede además almacenar en caché otra solicitud de operación de correo electrónico, como una solicitud de lectura de un mensaje de correo electrónico.

El programa 322 puede incluir un código de programa, donde el código de programa incluye una instrucción de operación de ordenador.

El procesador 330 puede ser una unidad central de procesamiento CPU o un circuito integrado de aplicaciones específicas ASIC (Application-Specific Integrated Circuit), o puede configurarse como uno o más circuitos integrados que implementan las realizaciones de la presente invención.

En esta realización de la presente invención, el procesador 330 está configurado para ejecutar el programa 322, y puede ejecutar específicamente los pasos relacionados en las realizaciones del método mostradas en la FIG. 4 a la FIG. 5.

La FIG. 4 es un diagrama de flujo de un método para procesar una solicitud de correo electrónico de acuerdo con una realización de la presente invención. El método puede ser ejecutado por la pasarela 110 de seguridad según la FIG. 1 y la FIG. 3. La pasarela 110 de seguridad está configurada para procesar una solicitud de adquisición de correo enviada por un dispositivo cliente, donde la solicitud de adquisición de correo se utiliza para adquirir un correo de un servidor de correo electrónico. A continuación, se describe el método en la FIG. 4 con referencia a la FIG. 1 y la FIG. 6. El método puede incluir:

En la etapa 400, la pasarela 110 de seguridad recibe una primera solicitud enviada por el dispositivo 100 cliente, donde la primera solicitud se utiliza para adquirir una parte de un mensaje de correo electrónico, y la parte del mensaje de correo electrónico no incluye un encabezado de correo electrónico del mensaje de correo electrónico.

En una aplicación real, un usuario puede decidir, al navegar por el encabezado de correo electrónico del mensaje de correo electrónico, recibir o navegar solamente por otras partes, excepto el encabezado de correo electrónico, del mensaje de correo electrónico. Por ejemplo, se puede recibir un cuerpo principal o un archivo adjunto del mensaje de correo electrónico, o se puede recibir un cuerpo principal y un archivo adjunto del mensaje de correo electrónico. Como se muestra en la FIG. 6, la FIG. 6 es un diagrama esquemático de señalización de otro método para procesar una solicitud de correo electrónico según una realización de la presente invención. En el diagrama esquemático de señalización mostrado en la FIG. 6, el dispositivo 100 cliente envía la primera solicitud 600 utilizada para adquirir la parte del mensaje de correo electrónico a la pasarela 110 de seguridad. La primera solicitud 600 enviada por el dispositivo 100 cliente lleva un ID de correo electrónico del mensaje de correo electrónico y un ID de la parte del mensaje de correo electrónico que debe adquirirse.

La primera solicitud 600 puede formatearse según el IMAP4. Específicamente, la primera solicitud 600 puede formatearse basándose en un comando FETCH del IMAP4. Por ejemplo, la primera solicitud puede ser fhn6 UID FETCH 77 (BODY.PEEK[2]), y la primera solicitud se utiliza para obtener un primer archivo adjunto de un mensaje de correo electrónico cuyo ID de correo electrónico es 77, donde: "fhn6" es una etiqueta de la solicitud y se utiliza para identificar la solicitud; "UID" es el ID de correo electrónico del mensaje de correo electrónico y puede identificar de manera únicamente el mensaje de correo electrónico; un UID puede ser un valor específico, o puede ser una lista o un rango, donde cuando un valor del UID es una lista o un rango, se utiliza para indicar múltiples mensajes de correo electrónico; "FETCH" es un comando especificado por el IMAP4 y que se utiliza para adquirir el mensaje de correo electrónico; "77" es un valor del ID de correo electrónico UID; "2" es un ID de una parte del mensaje de correo electrónico que debe adquirirse y representa el primer archivo adjunto del mensaje de correo electrónico; y "(BODY.PEEK [2])" indica que se solicita adquirir el primer archivo adjunto del mensaje de correo electrónico. Se puede comprender que, el ID de la parte del mensaje de correo electrónico que se va a adquirir también puede ser un valor específico, una lista o un rango. Cuando el ID de la parte adquirida del mensaje de correo electrónico es una lista o un rango, se utiliza para indicar que se han adquirido varias partes del mensaje de correo electrónico. Por ejemplo, "(BODY.PEEK [2-4]) se utiliza para indicar que se le solicita adquirir los primeros y terceros archivos adjuntos del mensaje de correo electrónico.

Un experto en la técnica puede aprender que, cuando la pasarela 110 de seguridad realiza el proxy de una forma de proxy transparente, la pasarela 110 de seguridad puede interceptar una solicitud de adquisición de mensajes de correo electrónico enviada por el dispositivo 100 cliente al servidor 120 de correo electrónico. Cuando la pasarela 110 de seguridad realiza el proxy de forma de proxy no transparente, el dispositivo 100 cliente puede enviar directamente una solicitud de adquisición de mensajes de correo electrónico a la pasarela 110 de seguridad. Esta realización de la presente invención no establece ningún límite en una forma proxy de la pasarela 110 de seguridad.

En la etapa 405, la pasarela 110 de seguridad convierte la primera solicitud 600 en una solicitud 605 utilizada para adquirir el mensaje de correo electrónico completo. Después de recibir la primera solicitud 600 del dispositivo 100 cliente, la pasarela 110 de seguridad puede construir, de acuerdo con un formato de comando especificado por un protocolo IMAP4 y de acuerdo con la primera solicitud 600, la solicitud 605 utilizada para adquirir el mensaje de correo electrónico completo. Por ejemplo, la solicitud 605, fhn6 UID FETCH 77 (BODY.PEEK []), utilizada para adquirir el mensaje de correo electrónico completo puede formatearse de acuerdo con la primera solicitud 600: fhn6 UID FETCH 77 (BODY.PEEK [2]). En la presente memoria, la solicitud 605 utilizada para adquirir el mensaje de correo electrónico completo puede ser referida como una primera solicitud 605 convertida.

En esta etapa, la pasarela 110 de seguridad puede almacenar en caché la primera solicitud 600 enviada por el dispositivo 100 cliente, y construir, de acuerdo con el ID que se encuentra en el mensaje de correo electrónico y que está en la primera 600 solicitud, la solicitud 605 utilizada para adquirir el mensaje de correo electrónico completo.

En la etapa 410, la pasarela 110 de seguridad envía la primera solicitud 605 convertida al servidor 120 de correo electrónico. Por ejemplo, la pasarela 110 de seguridad puede enviar la primera solicitud 605 convertida, fhn6 UID FETCH 77 (BODY.PEEK []), al servidor 120 de correo electrónico, para solicitar al servidor 120 de correo electrónico que devuelva, de acuerdo con la primera solicitud 605 convertida, el mensaje de correo electrónico completo.

En la etapa 415, la pasarela 110 de seguridad recibe el mensaje 610 de correo electrónico devuelto por el servidor 120 de correo electrónico, donde el mensaje 610 de correo electrónico es un mensaje de correo electrónico en forma codificada. Después de recibir la primera solicitud convertida, el servidor 120 de correo electrónico devuelve, de acuerdo con la primera solicitud convertida, el mensaje 610 de correo electrónico indicado por un UID. El mensaje 610 de correo electrónico devuelto por el servidor 120 de correo electrónico es un mensaje de correo electrónico que cumple con un formato especificado por el protocolo MIME. El mensaje de correo electrónico en un formato MIME incluye contenido de correo codificado. El contenido de correo codificado se refiere al contenido de correo codificado que se genera después de que el contenido de correo se codifica utilizando información de codificación de transferencia de contenido. Para una estructura específica del mensaje 610 de correo electrónico devuelto por el servidor 120 de correo electrónico, se hace referencia a la FIG. 2 y a las descripciones relacionadas.

Un encabezado de información MIME del mensaje 610 de correo electrónico devuelto por el servidor 120 de correo electrónico puede incluir el contenido de un encabezado de correo electrónico y campos de encabezado MIME como MIME version y Content-Type. Por ejemplo, un encabezado de información MIME del mensaje de correo electrónico

cuyo UID es 77 y que es devuelto de acuerdo con la primera solicitud 605 convertida por el servidor 120 de correo electrónico es:

Fecha: domingo, 17 Feb 2013 11:10:02 +0800 fecha de envío de correo:

De: "123" 123@123.com información del remitente

Para: "456" 456@123.com información del destinatario

Asunto: prueba asunto del correo electrónico

Versión Mime: MIME version 1.0

Tipo de contenido: multiparte/mezclado; tipo de contenido

Delimitación="=====001_Dragon664320174586_=====" delimitador, indica un comienzo y un final de un segmento MIME.

Un segmento 1 MIME del mensaje de correo electrónico cuyo UID es 77 y que es devuelto por el servidor 120 de correo electrónico incluye un cuerpo principal que es del mensaje de correo electrónico y que está codificado, donde un encabezado de segmento 1 MIME incluye la información de codificación del cuerpo principal del mensaje de correo electrónico, y un cuerpo de segmento 1 MIME incluye el contenido del cuerpo principal del mensaje de correo electrónico codificado. Por ejemplo, el segmento 1 MIME del mensaje de correo electrónico cuyo UID es 77 es:

--=====001_Dragon664320174586_===== indica un comienzo de segmento 1 MIME;

Content-Type: text/plain;

char set="gb2312" indica que un tipo de contenido de segmento 1 MIME es un tipo de texto/simple, y un conjunto de caracteres de texto en el segmento 1 MIME es "gb2312";

Content-Transfer-Encoding: base64 indica que un tipo de codificación de transferencia de segmento 1 MIME es base64; y

vPu4vbz+DQo= indica un cuerpo principal codificado del mensaje de correo electrónico.

Un segmento 2 MIME del mensaje de correo electrónico cuyo UID es 77 y que es devuelto por el servidor 120 de correo electrónico incluye un primer archivo adjunto que es del mensaje de correo electrónico y que está codificado, donde un encabezado de segmento 2 MIME incluye la información de codificación del primer archivo adjunto del mensaje de correo electrónico, y un cuerpo de segmento 2 MIME incluye el contenido codificado del primer archivo adjunto. Un segmento 3 MIME incluye un segundo archivo adjunto que es del mensaje de correo electrónico y que está en forma codificada, donde un encabezado de segmento 3 MIME incluye la información de codificación del segundo archivo adjunto del mensaje de correo electrónico, y un cuerpo de segmento 3 MIME incluye el contenido codificado del segundo archivo adjunto. Por ejemplo, el segmento 2 MIME del mensaje de correo electrónico cuyo UID es 77 es:

--=====001_Dragon664320174586_===== indica un comienzo de segmento 2 MIME;

Content-Type: application/octet-stream;

name="file1.txt" indica que un tipo de contenido de segmento 2 MIME es cualquier dato binario, y recibe el nombre de "file1.txt";

Content-Transfer-Encoding: base64 indica que un tipo de codificación de transferencia de segmento 2 MIME es base64;

Content-Disposition: archivo adjunto;

filename="file1.txt" indica que el contenido de segmento 2 MIME es un archivo adjunto, y recibe el nombre de "file1.txt"; y

xPq6w6Ohuty439DLvPu1vcT6o6E= indica el contenido codificado del primer archivo adjunto.

En la etapa 420, la pasarela 110 de seguridad analiza el mensaje 610 de correo electrónico para obtener la información de codificación del mensaje 610 de correo electrónico, donde la información de codificación incluye información del Content-Transfer-Encoding. Como se muestra en la FIG. 2, debido a que el mensaje 610 de correo electrónico devuelto por el servidor 120 de correo electrónico está en el formato especificado por MIME, la pasarela 110 de seguridad puede obtener la información del Content-Transfer-Encoding del mensaje 610 de correo electrónico analizando el encabezado de información MIME o un encabezado de segmento MIME del mensaje 610 de correo electrónico y puede decodificar una parte correspondiente del mensaje 610 de correo electrónico

utilizando la información del Content-Transfer-Encoding del mensaje 610 de correo electrónico. Por ejemplo, la pasarela 110 de seguridad puede obtener el Content-Transfer-Encoding: base64 del encabezado de segmento 2 MIME del mensaje 610 de correo electrónico cuyo UID es 77, para aprender que la información de codificación de transferencia del primer archivo adjunto del mensaje de correo electrónico es base64.

Cabe señalar que, si la Información del Content-Transfer-Encoding se incluye en el encabezado de información MIME, la información del Content-Transfer-Encoding puede utilizarse para decodificar el mensaje de correo electrónico completo. Si la información del Content-Transfer-Encoding se incluye en un encabezado de segmento MIME, la información del Content-Transfer-Encoding puede actuar solamente en el segmento MIME, y utilizarse para decodificar un cuerpo de segmento MIME del segmento MIME.

Además, la pasarela 110 de seguridad puede obtener más información sobre el conjunto de caracteres (char set) que se encuentra en el mensaje 610 de correo electrónico analizando el mensaje 610 de correo electrónico. Específicamente, la pasarela 110 de seguridad puede obtener, a partir del mensaje 610 de correo electrónico devuelto por el servidor 120 de correo electrónico, información del tipo de contenido de cada segmento MIME del mensaje 610 de correo electrónico de manera que la pasarela 110 de seguridad puede determinar un tipo de paquete de segmento MIME de acuerdo con la información del tipo de contenido obtenida. Por ejemplo, el tipo de paquete puede ser texto, imagen, audio o similar. Además, la información del tipo de contenido puede incluir además un conjunto de caracteres (char set) de una forma de codificación de texto del segmento MIME. Por ejemplo, en el mensaje de correo electrónico cuyo UID es 77 descrito anteriormente, en el segmento 1 MIME, char set ="gb2312" indica que un conjunto de caracteres de texto en el segmento 1 MIME es "gb2312". Ni el encabezado de información MIME ni el segmento 2 MIME incluyen información sobre el conjunto de caracteres y, por lo tanto, un tipo de conjunto de caracteres en el segmento 2 MIME es un tipo de conjunto de caracteres por defecto: ASCII.

En la etapa 425, la pasarela 110 de seguridad decodifica el mensaje 610 de correo electrónico de acuerdo con la información de codificación, para obtener la parte, en forma decodificada, del mensaje de correo electrónico. De manera específica, se puede aprender qué forma de codificación se utiliza siempre que se obtiene la información de codificación, y luego se utiliza una forma de decodificación correspondiente a la forma de codificación para realizar la decodificación para obtener el contenido de correo que sea de la parte, en forma decodificada, del mensaje de correo electrónico.

Por ejemplo, la pasarela 110 de seguridad puede decodificar el contenido de un archivo adjunto codificado "xPq6w6Ohuty439DLvPu1vcT6o6E =" que se encuentra en el segmento 2 MIME de acuerdo con la forma de codificación de transferencia base64, para obtener el contenido, en forma decodificada, del primer archivo adjunto en el mensaje de correo electrónico cuyo UID es 77: "¡Hola! ¡Encantado de conocerte!"

Se puede comprender que, la pasarela 110 de seguridad puede decodificar el mensaje 610 de correo electrónico completo, o puede decodificar solo la parte, requerida por el dispositivo 100 cliente, del mensaje de correo electrónico, que no está limitada en esta realización. Por ejemplo, la pasarela 110 de seguridad puede decodificar el mensaje 610 de correo electrónico completo de acuerdo con la información del Content-Transfer-Encoding en el encabezado de información MIME, o puede decodificar el contenido de un cuerpo de un segmento MIME en el segmento MIME de acuerdo con la información del Content-Transfer-Encoding en un encabezado de segmento MIME. Si el encabezado de segmento MIME no incluye información del Content-Transfer-Encoding, la pasarela 110 de seguridad puede decodificar el contenido del cuerpo de segmento MIME de acuerdo con la información del Content-Transfer-Encoding en el encabezado de información MIME.

En la etapa 430, la pasarela 110 de seguridad realiza el procesamiento de seguridad en la parte, en forma decodificada, del mensaje de correo electrónico, para determinar si la parte del mensaje de correo electrónico es segura. En una aplicación real, después de que la pasarela 110 de seguridad decodifica el mensaje de correo electrónico, la pasarela 110 de seguridad puede realizar además, de acuerdo con una política de seguridad establecida, el procesamiento de seguridad en la parte, en forma decodificada, del mensaje de correo electrónico. Si se determina, después de realizar el procesamiento de seguridad, que el mensaje 610 de correo electrónico es un mensaje de correo electrónico seguro, diríjase a la etapa 435; de lo contrario, diríjase a la etapa 440.

La política de seguridad establecida puede incluir una política de detección y eliminación de virus, una política de filtración, etc. Por ejemplo, se puede realizar una operación de seguridad como la detección y eliminación de virus en el mensaje de correo electrónico descodificado de acuerdo con la política de detección y eliminación de virus preestablecida, o la filtración de contenido se puede realizar en el mensaje de correo electrónico descodificado de acuerdo con la información del conjunto de caracteres (char set) en el mensaje de correo electrónico y la política de filtración preestablecida, para evitar que el dispositivo 100 cliente reciba un mensaje de correo electrónico con un virus, un correo de basura, o un mensaje de correo electrónico con un campo sensible, protegiendo de este modo la seguridad del dispositivo cliente.

En una situación, cuando se requiere filtrar un mensaje de correo electrónico recibido por el dispositivo 100 cliente, se puede generar una política de filtración por adelantado con una cadena que necesita ser filtrada y un conjunto de caracteres preestablecido. En un proceso de filtración de correo electrónico, primero se determina si la información de conjunto de caracteres en la parte del mensaje de correo electrónico es coherente con la información del conjunto

de caracteres en la política de filtración. Si la información del conjunto de caracteres en la parte del mensaje de correo electrónico es coherente con la información del conjunto de caracteres en la política de filtración, el contenido de correo decodificado de la parte del mensaje de correo electrónico se ajusta directamente a la cadena que debe filtrarse y que se encuentra en la política de filtración. Si la información del conjunto de caracteres en la parte del mensaje de correo electrónico no es coherente con la información del conjunto de caracteres en la política de filtración, el contenido de correo decodificado de la parte del mensaje de correo electrónico debe convertirse de acuerdo con la información del conjunto de caracteres en la política de filtración, y luego debe coincidir con la cadena que debe filtrarse y que se encuentra en la política de filtración, para determinar si la parte del mensaje de correo electrónico incluye la cadena que se debe filtrar.

Por ejemplo, la pasarela 110 de seguridad puede filtrar, de acuerdo con la política de filtración establecida, el contenido, en forma decodificada, del primer archivo adjunto del mensaje de correo electrónico cuyo UID es 77. El conjunto de políticas de filtración en la pasarela 110 de seguridad puede ser: filtrar un mensaje de correo electrónico con una cadena de "publicidad", y la información del conjunto de caracteres que se establece para filtrar una cadena es "gb2312". Ciertamente, se puede comprender que, la pasarela 110 de seguridad puede generar, mediante la compilación, un equipo de estado de acuerdo con la cadena que necesita ser filtrada y que está configurada en la política de filtración y de acuerdo con la información del conjunto de caracteres. Debido a que la información del conjunto de caracteres del primer archivo adjunto del mensaje de correo electrónico cuyo UID es 77 es ASCII, y la información del conjunto de caracteres en el equipo de estado generada es "gb2312", la información del conjunto de caracteres del primer archivo adjunto no es coherente con la información del conjunto de caracteres en el equipo de estado. Por lo tanto, cuando el primer archivo adjunto del mensaje de correo electrónico se filtra de acuerdo con la política de filtración establecida, el contenido del primer archivo adjunto debe convertirse en contenido en formato "gb2312"; y luego el contenido convertido debe coincidir utilizando el equipo de estado, para determinar si el primer archivo adjunto incluye la cadena de "publicidad" que debe ser filtrada. Si el primer archivo adjunto no incluye la cadena "publicidad" que se va a filtrar, se considera que el mensaje 610 de correo electrónico es seguro; de lo contrario, se considera que el mensaje 610 de correo electrónico no es un mensaje de correo electrónico seguro.

Cabe señalar que, después de que la pasarela 110 de seguridad obtiene el contenido de correo de la parte del mensaje de correo electrónico, el procesamiento de seguridad, como el procesamiento antivirus o la filtración de correo, realizada en el contenido de correo de la parte del mensaje de correo electrónico es solamente una de tantas formas de procesamiento enumeradas en esta realización de la presente invención. En una aplicación actual, se puede realizar además otro procesamiento en el contenido de correo, que no se limita en esta realización.

En la etapa 435, la pasarela 110 de seguridad reenvía la parte 615 del mensaje de correo electrónico al dispositivo 100 cliente. Después de determinar que la parte 615 del mensaje de correo electrónico es segura, la pasarela 110 de seguridad puede reenviar la parte 615 del mensaje de correo electrónico al dispositivo 100 cliente. Por ejemplo, si la pasarela 110 de seguridad determina, después de realizar el procesamiento de seguridad en el mensaje 610 de correo electrónico, que el mensaje 610 de correo electrónico es un mensaje de correo electrónico seguro, o la pasarela 110 de seguridad determina, después de realizar el procesamiento como la detección y la eliminación de virus en el mensaje 610 de correo electrónico, que el mensaje 610 de correo electrónico procesado es un mensaje de correo electrónico seguro, la pasarela 110 de seguridad puede reenviar la parte 615 del mensaje de correo electrónico al dispositivo 100 cliente de acuerdo con el ID de la parte del mensaje de correo electrónico y que se lleva a cabo en la primera solicitud 600 de la misma, para terminar el proceso del método. Por ejemplo, la pasarela 110 de seguridad puede devolver el primer archivo adjunto en el mensaje de correo electrónico cuyo UID es 77 al dispositivo 100 cliente de acuerdo con un ID "2"·del archivo adjunto en la primera solicitud fhn7 UID FETCH 77 (BODY.PEEK [2]).

En la etapa 440, la pasarela 110 de seguridad rechaza reenviar la parte del mensaje de correo electrónico al dispositivo cliente. Si la pasarela 110 de seguridad determina, después de realizar el procesamiento de seguridad en el mensaje 610 de correo electrónico, que el mensaje 610 de correo electrónico no es un correo electrónico seguro, la pasarela 110 de seguridad puede rechazar el reenvío de la parte 615 del mensaje de correo electrónico al dispositivo 100 cliente. Por ejemplo, la pasarela 110 de seguridad puede enviar, al dispositivo 100 cliente, la información de que la adquisición del mensaje de correo electrónico falla, para descartar el mensaje 610 de correo electrónico, o enviar un mensaje 610 de correo electrónico modificado al dispositivo 100 cliente. Por ejemplo, la pasarela 110 de seguridad puede eliminar o modificar algunas frases del mensaje 610 de correo electrónico y después enviar el mensaje 610 de correo electrónico al dispositivo 100 cliente para realizar protección de seguridad en el dispositivo 100 cliente.

De acuerdo con el método de procesamiento de una solicitud de correo electrónico mostrada en la FIG. 4, una pasarela 110 de seguridad convierte una solicitud 600 que se utiliza para adquirir otras partes, excepto un encabezado de correo electrónico de un mensaje de correo electrónico y que es de un dispositivo 100 cliente en una solicitud 605 para adquirir el mensaje de correo electrónico completo, de manera que la pasarela 110 de seguridad pueda adquirir, a partir del mensaje 610 de correo electrónico completo devuelto por un servidor 120 de correo electrónico, la información de codificación de transferencia de contenido de la parte 615, para ser adquirida por el dispositivo 100 cliente, del mensaje de correo electrónico. Además, la pasarela 110 de seguridad puede utilizar la información de codificación de transferencia de contenido de la parte del mensaje de correo electrónico para decodificar la parte 615 del mensaje de correo electrónico, de manera que la pasarela 110 de seguridad pueda

también obtener el contenido de la parte, en forma decodificada, del mensaje de correo electrónico en un escenario de aplicación en el que el dispositivo 100 cliente adquiere solamente la parte, excepto el encabezado de correo electrónico, del mensaje de correo electrónico, mejorando así la protección del dispositivo 100 cliente.

En otra situación, para mejorar una velocidad del dispositivo 100 cliente en la adquisición de un mensaje de correo electrónico, la pasarela 110 de seguridad puede almacenar además un mensaje de correo electrónico obtenido del servidor 120 de correo electrónico. Específicamente, la pasarela de seguridad puede seguir procesando, utilizando el método que se muestra en la FIG. 5, una solicitud de adquisición de correo enviada por el dispositivo 100 cliente, donde se utiliza la solicitud de adquisición de correo para adquirir, desde el servidor 120 de correo electrónico, una parte del mensaje de correo electrónico. La FIG. 5 es un diagrama de flujo de otro método para procesar una solicitud de correo electrónico de acuerdo con una realización de la presente invención. El método también puede ser ejecutado por la pasarela 110 de seguridad en la FIG. 1, la FIG. 3, y la FIG. 6. A continuación se describe el método mostrado en la FIG. 5 con referencia a la FIG. 1 y la FIG. 6. Como se muestra en la FIG. 5, el método puede incluir:

En la etapa 500, la pasarela 110 de seguridad recibe una segunda solicitud enviada por el dispositivo 100 cliente, donde la segunda solicitud se utiliza para adquirir una parte de un mensaje de correo electrónico, y la parte del mensaje de correo electrónico no incluye un encabezado de correo electrónico del mensaje de correo electrónico.

La segunda solicitud también se formatea basándose en un comando FETCH del IMAP4. Por ejemplo, la segunda solicitud puede ser fhn7 UID FETCH 77 (BODY.PEEK [3]), y se utiliza para solicitar al servidor de correo electrónico que devuelva un segundo archivo adjunto de un mensaje de correo electrónico cuyo ID de correo electrónico es 77, donde "77" es el ID de correo electrónico del mensaje de correo electrónico, y "3" es un ID de una parte del mensaje de correo electrónico que debe ser adquirida. Para obtener descripciones detalladas acerca de la solicitud enviada por el dispositivo cliente, consulte las descripciones relacionadas con la realización de la FIG. 4.

Cabe señalar que, la primera y la segunda en la primera solicitud, la segunda solicitud, la primera solicitud convertida y la segunda solicitud convertida en las realizaciones de la presente invención son solo para mayor claridad de la descripción y para distinguir las solicitudes enviadas por el dispositivo cliente en lugar de para establecer cualquier límite en un tiempo, una secuencia, o similar de las solicitudes enviadas por el dispositivo cliente.

En la etapa 505, la pasarela 110 de seguridad determina si la pasarela 110 de seguridad ha almacenado en caché el mensaje de correo electrónico. Debido a que en un sistema de red mostrado en la FIG. 1, la pasarela 110 de seguridad generalmente procesa, mediante proxy, una solicitud de operación de correo enviada por el dispositivo 100 cliente. La pasarela 110 de seguridad tiene una función de almacenamiento en caché. Por ejemplo, la pasarela 110 de seguridad puede almacenar en caché continuamente un mensaje de correo electrónico adquirido del servidor 120 de correo electrónico en una caché local. Después de recibir la segunda solicitud del dispositivo 100 cliente, la pasarela 110 de seguridad determina, de acuerdo con la segunda solicitud, si la pasarela 110 de seguridad ha almacenado el mensaje de correo electrónico requerido para ser adquirido por el dispositivo 100 cliente. Si la pasarela 110 de seguridad no almacena el mensaje de correo electrónico requerido para ser adquirido por el dispositivo 100 cliente, la pasarela 110 de seguridad puede ejecutar la etapa 510. Si la pasarela 110 de seguridad ha almacenado el mensaje de correo electrónico requerido para ser adquirido por el dispositivo 100 cliente, la pasarela 110 de seguridad puede ejecutar directamente la etapa 550 y enviar directamente la parte del mensaje de correo electrónico, almacenada por la pasarela 110 de seguridad, al dispositivo 100 cliente. De esta manera, se puede mejorar significativamente la velocidad y eficiencia del dispositivo 100 cliente en la adquisición del mensaje de correo electrónico.

Específicamente, cuando se determina si el mensaje de correo electrónico está almacenado en caché, la pasarela 110 de seguridad puede determinar, de acuerdo con un ID de correo electrónico llevada en la segunda solicitud, si el mensaje de correo electrónico está almacenado en caché.

En la etapa 510, la pasarela 110 de seguridad convierte la segunda solicitud en una solicitud utilizada para adquirir el mensaje de correo electrónico completo. La pasarela 110 de seguridad puede construir, de acuerdo con el ID de correo electrónico transportada en la segunda solicitud y un formato de comando especificado por el IMAP4, la solicitud 605 utilizada para adquirir el mensaje de correo electrónico completo. Por ejemplo, la solicitud, fhn7 UID FETCH 77 (BODY.PEEK []), utilizada para adquirir el mensaje de correo electrónico completo puede formatearse de acuerdo con la segunda solicitud: fhn7 UID FETCH 77 (BODY.PEEK [3]); en este caso la solicitud utilizada para adquirir el mensaje de correo electrónico completo puede referirse a una segunda solicitud convertida.

Se puede comprender que, en esta etapa, la pasarela 110 de seguridad puede almacenar primero la segunda solicitud enviada por el dispositivo 100 cliente en la memoria 320 y luego construir, de acuerdo con el ID de correo electrónico en la segunda solicitud, la solicitud 605 utilizada para adquirir el mensaje de correo electrónico completo.

En la etapa 515, la pasarela 110 de seguridad envía la segunda solicitud convertida al servidor de correo electrónico. Por ejemplo, la pasarela 110 de seguridad puede enviar la segunda solicitud convertida fhn7 UID FETCH 77

(BODY.PEEK []) al servidor 120 de correo electrónico, para solicitar al servidor 120 de correo electrónico que devuelva, de acuerdo con la segunda solicitud convertida, el mensaje de correo electrónico completo cuyo UID es 77.

En la etapa 520, la pasarela 110 de seguridad recibe el mensaje 610 de correo electrónico, en forma codificada, que es devuelto por el servidor 120 de correo electrónico. El mensaje 610 de correo electrónico devuelto por el servidor 120 de correo electrónico tiene un formato especificado por MIME, y para más detalles, consulte las descripciones relacionadas en las realizaciones mostradas en la FIG. 2 y la FIG. 4.

En la etapa 525, la pasarela 110 de seguridad analiza el mensaje 610 de correo electrónico para obtener información de codificación del mensaje de correo electrónico.

En la etapa 530, la pasarela 110 de seguridad decodifica el mensaje 610 de correo electrónico de acuerdo con la información de codificación, para obtener la parte, en forma decodificada, del mensaje de correo electrónico.

En la etapa 535, la pasarela 110 de seguridad realiza el procesamiento de seguridad en la parte, en forma decodificada, del mensaje de correo electrónico, para determinar si la parte del mensaje de correo electrónico es segura. Si la pasarela 110 de seguridad determina, después de realizar el procesamiento de seguridad, que el mensaje de correo electrónico es un mensaje de correo electrónico seguro, diríjase a la etapa 545; de lo contrario, diríjase a la etapa 540.

En la etapa 540, la pasarela 110 de seguridad rechaza reenviar la parte del mensaje de correo electrónico al dispositivo cliente.

En la etapa 545, la pasarela 110 de seguridad almacena el mensaje de correo electrónico en la caché de la pasarela 110 de seguridad. Específicamente, cuando se determina, en la etapa 505 de acuerdo con el ID de correo electrónico llevada en la segunda solicitud, que la pasarela 110 de seguridad no ha almacenado en caché el mensaje 610 de correo electrónico, significa que la pasarela 110 de seguridad no ha obtenido el mensaje 610 de correo electrónico del servidor 120 de correo electrónico. Cuando se realiza el procesamiento de seguridad en el mensaje 610 de correo electrónico decodificado y determinar que el mensaje 610 de correo electrónico es seguro, la pasarela 110 de seguridad puede almacenar el mensaje 610 de correo electrónico en la caché de la pasarela 110 de seguridad. Cuando la pasarela 110 de seguridad recibe nuevamente una solicitud para adquirir el mensaje 610 de correo electrónico, la pasarela 110 de seguridad puede enviar directamente el mensaje 610 de correo electrónico o cualquier parte del mensaje 610 de correo electrónico en la caché al dispositivo 100 cliente, con el fin de mejorar la velocidad y eficiencia del dispositivo 100 cliente en la obtención del mensaje de correo electrónico.

En la etapa 550, la pasarela 110 de seguridad reenvía la parte 615 del mensaje de correo electrónico al dispositivo cliente. En una situación, si la pasarela 110 de seguridad determina, después de realizar el procesamiento de seguridad en el mensaje 610 de correo electrónico, que el mensaje 610 de correo electrónico es un mensaje de correo electrónico seguro, o la pasarela 110 de seguridad determina, después de realizar el procesamiento como la detección y la eliminación de virus en el mensaje 610 de correo electrónico, que el mensaje de correo electrónico procesado es un mensaje de correo electrónico seguro, la pasarela 110 de seguridad puede enviar la parte 615 del mensaje de correo electrónico al dispositivo 100 cliente de acuerdo con el ID de la parte del mensaje de correo electrónico y que se lleva a cabo en la segunda solicitud de la misma. Por ejemplo, la pasarela 110 de seguridad puede devolver el segundo archivo adjunto en el mensaje de correo electrónico cuyo UID es 77 al dispositivo 100 cliente de acuerdo con un ID "3" del archivo adjunto en la segunda solicitud fhn7 UID FETCH 77 (BODY.PEEK [3]).

En otra situación, cuando la pasarela 110 de seguridad determina, en la etapa 505, que la pasarela 110 de seguridad ha almacenado en caché el mensaje 610 de correo electrónico, la pasarela 110 de seguridad también puede ejecutar directamente la etapa 550, y reenviar la parte 615 del mensaje de correo electrónico en caché en la pasarela 110 de seguridad, al dispositivo 100 cliente de acuerdo con el ID que es de la parte 615 del mensaje de correo electrónico y que se lleva en la segunda solicitud para mejorar la velocidad y eficiencia del dispositivo 100 cliente en la obtención del mensaje de correo electrónico.

Cabe señalar que, la etapa de almacenar en caché el mensaje 610 de correo electrónico (por ejemplo, etapa 545 en la FIG. 5) se puede ejecutar después de que el mensaje 610 de correo electrónico se obtenga del servidor 120 de correo electrónico, o se puede ejecutar después de que se realice el procesamiento de seguridad en el mensaje 610 de correo electrónico, o puede ejecutarse antes de que la parte 615 del mensaje de correo electrónico sea enviada al dispositivo 100 cliente, o puede ejecutarse al mismo tiempo que la parte 615 del mensaje de correo electrónico se reenvía al dispositivo 100 cliente, que no se limita a esta realización. Se puede comprender que, si el mensaje 610 de correo electrónico se almacena después de que se obtenga el mensaje 610 de correo electrónico y antes de que se realice el procesamiento de seguridad en el mensaje 610 de correo electrónico, cuando se encuentre, después de que se realice el procesamiento de seguridad en el mensaje 610 de correo electrónico, que el mensaje de correo electrónico no es seguro, el mensaje 610 de correo electrónico se puede eliminar de la caché.

Puede comprenderse claramente por un experto en la técnica que, en aras de la facilidad y brevedad de la descripción, para descripciones de algunas etapas en la realización mostrada en la FIG. 5, se refieren a las descripciones detalladas del procedimiento correspondiente en la realización mostrada en la FIG. 4.

De acuerdo con el método de procesamiento de una solicitud de correo electrónico mostrado en la FIG. 5, una pasarela 110 de seguridad puede determinar primero, después de recibir una solicitud para adquirir una parte de un mensaje de correo electrónico y que es enviada por un dispositivo 100 cliente, si el mensaje de correo electrónico requerido para ser adquirido por el dispositivo 100 cliente está almacenado en una caché. Si la pasarela 110 de seguridad ha almacenado el mensaje de correo electrónico requerido para ser adquirido por el dispositivo 100 cliente, la pasarela 110 de seguridad puede enviar directamente la parte del mensaje de correo electrónico almacenada por la pasarela 110 de seguridad, al dispositivo 100 cliente, de manera que se pueda mejorar significativamente la velocidad y eficiencia del dispositivo 100 cliente en la adquisición del mensaje de correo electrónico. Si la pasarela 110 de seguridad no almacena el mensaje de correo electrónico requerido para ser adquirido por el dispositivo 100 cliente, la pasarela 110 de seguridad convierte la solicitud del dispositivo 100 cliente en una solicitud para adquirir el mensaje de correo electrónico completo, de manera que la pasarela 110 de seguridad pueda adquirir, a partir del mensaje de correo electrónico completo devuelto de acuerdo con la solicitud convertida por el servidor 120 de correo electrónico, información de codificación de transferencia de contenido de la parte, para ser adquirida por el dispositivo 100 cliente, del mensaje de correo electrónico. Además, la pasarela 110 de seguridad puede descodificar la parte del mensaje de correo electrónico utilizando la información de codificación de transferencia de contenido de la parte del mensaje de correo electrónico, de manera que la pasarela 110 de seguridad también pueda identificar y obtener contenido de la parte, adquirida por el dispositivo 100 cliente, del mensaje de correo electrónico. Además, la pasarela 110 de seguridad puede realizar una operación de procesamiento de seguridad como la filtración de correo o detección de virus y eliminación del contenido de la parte decodificada del mensaje de correo electrónico, y después reenviar la parte del mensaje de correo electrónico al dispositivo 100 cliente, para asegurar la seguridad del dispositivo 100 cliente. Más aún, la pasarela 110 de seguridad puede almacenar en caché, después de determinar que el mensaje de correo electrónico es seguro, el mensaje de correo electrónico adquirido del servidor 120 correo electrónico, de manera que la pasarela 110 de seguridad pueda devolver el mensaje de correo electrónico almacenado en caché al dispositivo 100 cliente después de recibir una solicitud de operación de correo del dispositivo 100 cliente, con el fin de mejorar la velocidad y eficiencia del dispositivo 100 cliente en la adquisición del mensaje de correo electrónico.

Cabe señalar que, las realizaciones proporcionadas por la aplicación son solamente ejemplares, y la pasarela de seguridad en las realizaciones de la presente invención es también solamente un ejemplo del dispositivo de red; las realizaciones de la presente invención también se pueden aplicar a otro dispositivo de red, por ejemplo, un cortafuegos, con la condición de que el dispositivo de red pueda implementar, basándose en el IMAP4, una función de proxy de correo, la cual no está limitada en la presente. Además, el dispositivo de red en las realizaciones de la presente invención se puede utilizar por separado en una red como un dispositivo independiente, o puede estar situado en otro dispositivo como un cortafuegos o una pasarela, lo cual no está limitado en la presente memoria.

REIVINDICACIONES

1. Un método, ejecutado por una pasarela (110) de seguridad, para procesar una solicitud de que un dispositivo cliente adquiera un mensaje de correo electrónico de un servidor de correo electrónico, el método comprende las etapas de:

recibir (400) una primera solicitud (600) enviada por el dispositivo cliente, en donde la primera solicitud (600) se utiliza para adquirir una parte del mensaje de correo electrónico, y la parte del mensaje de correo electrónico no incluye un encabezado de correo electrónico del mensaje de correo electrónico;

convertir (405) la primera solicitud (600) en una primera solicitud (605) convertida utilizada para adquirir el mensaje (610) de correo electrónico completo, en donde la primera solicitud enviada por el dispositivo cliente y la primera solicitud (605) convertida se formatean de acuerdo con el Protocolo de acceso a mensaje de Internet 4, IMAP4;

enviar (410) la primera solicitud (605) convertida al servidor de correo electrónico;

recibir (415) el mensaje (610) de correo electrónico devuelto por el servidor de correo electrónico, en donde el mensaje de correo electrónico es un mensaje de correo electrónico en forma codificada;

analizar (420) el mensaje (610) de correo electrónico para obtener información de codificación del mensaje de correo electrónico, en donde la información de codificación incluye información del Content-Transfer-Encoding y la información del Content-Transfer-Encoding se obtiene analizando una extensión multipropósito de correo de Internet, MIME, un encabezado de información o un encabezado de segmento MIME del mensaje (610) de correo electrónico;

decodificar (425) el mensaje (610) de correo electrónico de acuerdo con la información de codificación, para obtener la parte, en forma decodificada, del mensaje de correo electrónico;

realizar (430) el procesamiento de seguridad en la parte, en forma decodificada, del mensaje de correo electrónico, para determinar si la parte del mensaje de correo electrónico es segura; y

reenviar (435) la parte del mensaje (615) de correo electrónico al dispositivo cliente si se determina que la parte del mensaje de correo electrónico es segura; o rechazar (440) el reenvió la parte del mensaje de correo electrónico al dispositivo cliente si se determina que el mensaje de correo electrónico no es un correo electrónico seguro.

2. El método según la reivindicación 1, en donde la primera solicitud comprende un ID de correo electrónico del mensaje de correo electrónico y un ID de la parte del mensaje de correo electrónico; y en donde la etapa de convertir la primera solicitud en una primera solicitud (605) convertida utilizada para adquirir el mensaje de correo electrónico completo comprende la etapa de:

convertir, de acuerdo con el ID de correo electrónico, la primera solicitud en la primera solicitud (605) convertida utilizada para adquirir el mensaje de correo electrónico completo; y

en donde la etapa de reenviar la parte del mensaje de correo electrónico al dispositivo cliente comprende la etapa de: reenviar la parte del mensaje de correo electrónico al dispositivo cliente de acuerdo con el ID de la parte del mensaje de correo electrónico.

3. El método según la reivindicación 1, comprende además la etapa de: realizar el procesamiento de seguridad en la parte, en forma decodificada, del mensaje de correo electrónico, para determinar si la parte del mensaje de correo electrónico es segura; en donde la etapa de reenviar la parte del mensaje de correo electrónico al dispositivo cliente comprende la etapa de: reenviar la parte del mensaje de correo electrónico al dispositivo cliente cuando se determina que la parte del mensaje de correo electrónico es segura.

4. El método según la reivindicación 3, comprende además la etapa de: adquirir información del conjunto de caracteres en el mensaje de correo electrónico devuelto por el servidor de correo electrónico; en donde la etapa de realizar el procesamiento de seguridad en la parte, en forma decodificada, del mensaje de correo electrónico para determinar si la parte del mensaje de correo electrónico es segura comprende la etapa de: realizar, de acuerdo con una política de seguridad y la información del conjunto de caracteres, el procesamiento de seguridad sobre la parte, en forma decodificada, del mensaje de correo electrónico, para determinar si la parte del mensaje de correo electrónico es segura.

5. El método según la reivindicación 1, comprende además la etapa de: almacenar el mensaje de correo electrónico en una caché de la pasarela (110) de seguridad.

6. El método según la reivindicación 5, comprende además las etapas de:

recibir una segunda solicitud enviada por el dispositivo cliente, en donde la segunda solicitud es utilizada para adquirir una segunda parte del mensaje de correo electrónico, la segunda parte del mensaje de correo electrónico no comprende el encabezado de correo electrónico del mensaje de correo electrónico, y la segunda solicitud comprende un ID de correo electrónico del mensaje de correo electrónico y un ID de la segunda parte del mensaje de correo electrónico;

determinar, de acuerdo con el ID de correo electrónico, que la pasarela (110) de seguridad ha almacenado en caché el mensaje de correo electrónico; y

reenviar la segunda parte del mensaje de correo electrónico al dispositivo cliente de acuerdo con el ID de la segunda parte del mensaje de correo electrónico.

7. Una pasarela (110) de seguridad, que comprende:

una interfaz (310) de comunicaciones, configurada para comunicarse con un dispositivo cliente y un servidor de correo electrónico; y

un procesador (330) configurado para realizar las etapas del método de cualquiera de las reivindicaciones 1 a 6.

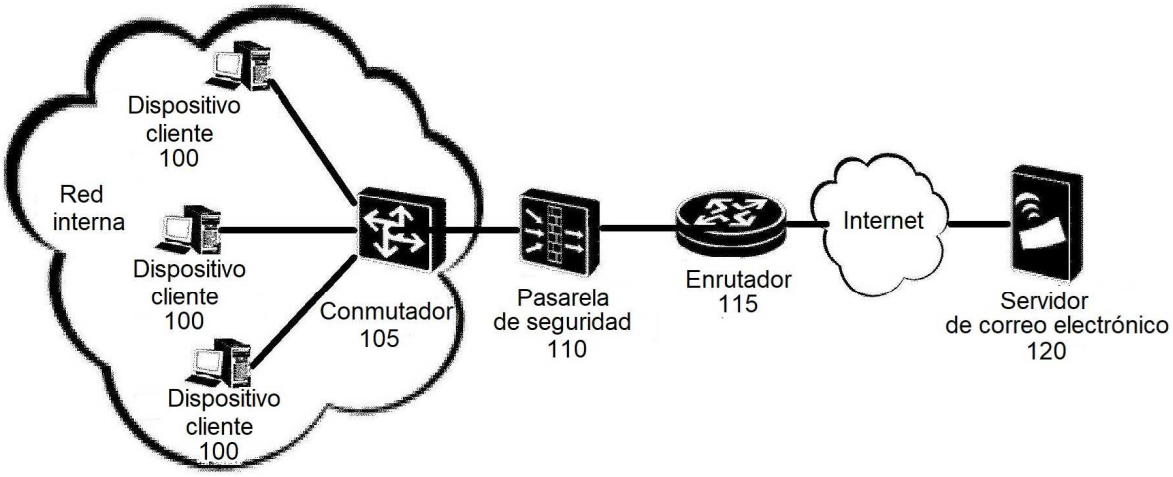
Dispositivo cliente 100
Red interna
Dispositivo cliente 100
Dispositivo cliente 100
Conmutador 105
Pasarela de seguridad 110
Enrutador 115
Internet
Servidor de correo electrónico 120

FIG. 1

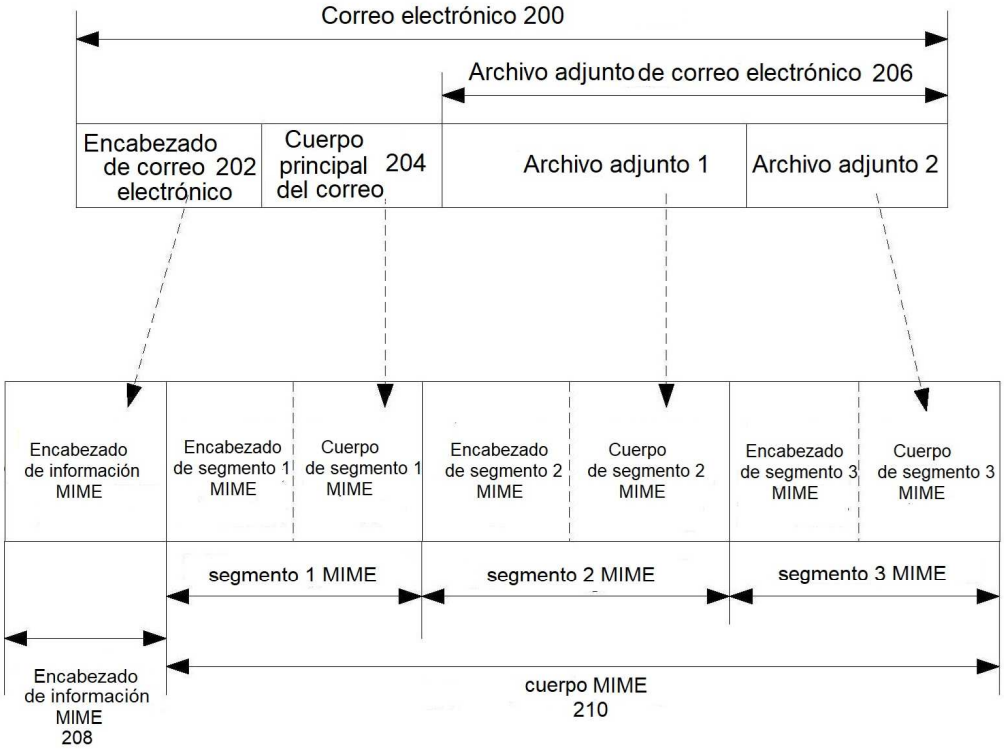
Correo electrónico 200
Archivo adjunto de correo electrónico 206
Encabezado de correo electrónico 202
Cuerpo principal del correo 204
Archivo adjunto 1
Archivo adjunto 2
Encabezado de información MIME
Encabezado de segmento 1 MIME
Cuerpo de segmento 1 MIME
Encabezado de segmento 2 MIME
Cuerpo de segmento 2 MIME
Encabezado de segmento 3 MIME
Cuerpo de segmento 3 MIME
segmento 1 MIME
segmento 2 MIME
segmento 3 MIME
Encabezado de información MIME 208
cuerpo MIME 210

FIG. 2

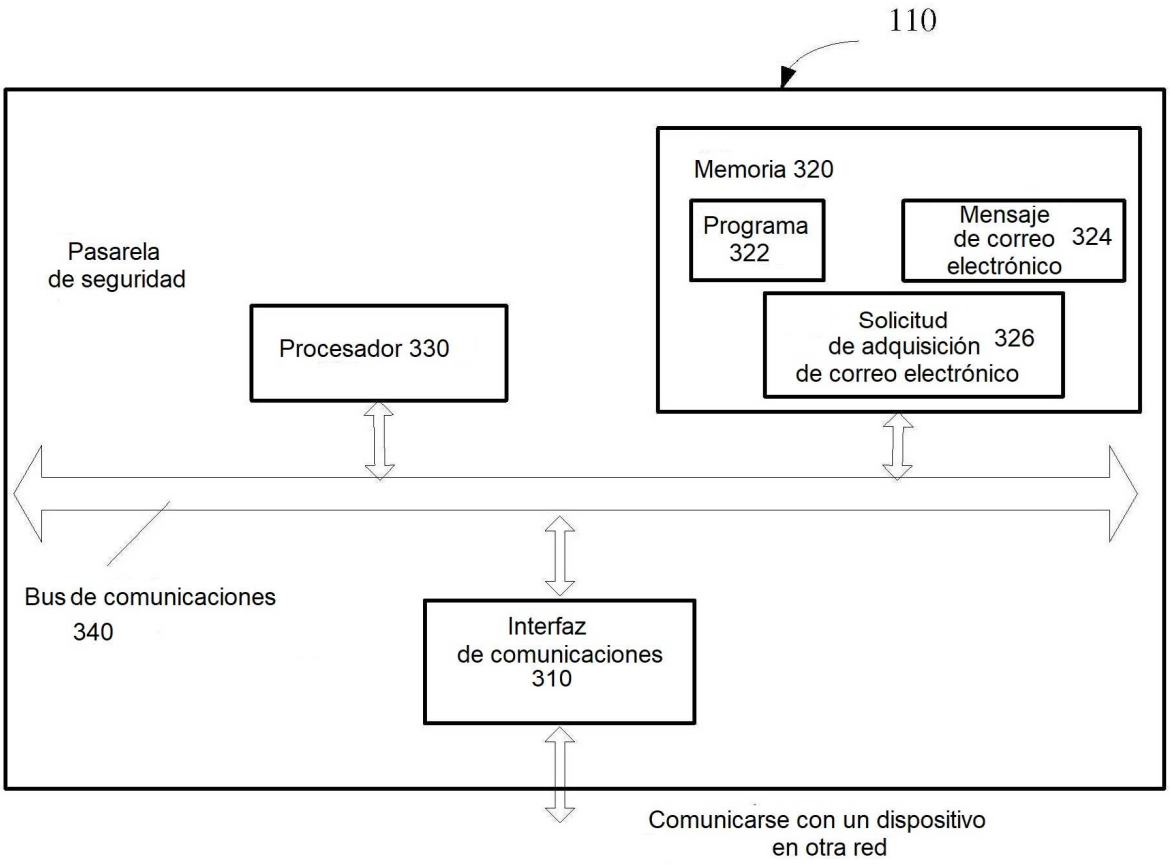
110
Memoria 320
Programa 322
Mensaje de correo electrónico 324
Solicitud de adquisición de correo electrónico 326
Pasarela de seguridad
Procesador 330
Bus de comunicaciones 340
Interfaz de comunicaciones 310
Comunicarse con un dispositivo en otra red

FIG. 3

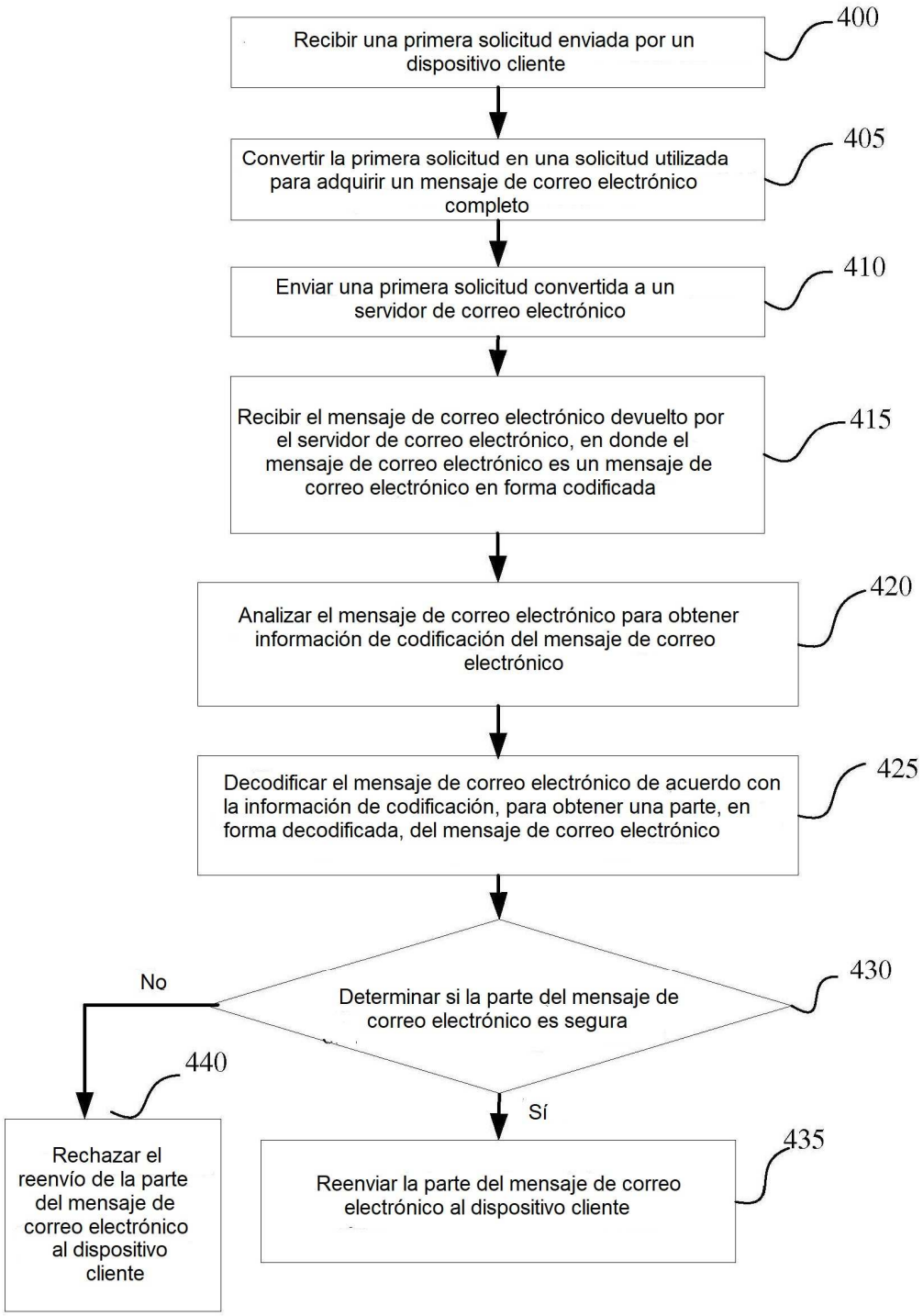
Recibir una primera solicitud enviada por un dispositivo cliente
400
Convertir la primera solicitud en una solicitud utilizada para adquirir un mensaje de correo electrónico completo
405
Enviar una primera solicitud convertida a un servidor de correo electrónico
410
Recibir el mensaje de correo electrónico devuelto por el servidor de correo electrónico, en donde el mensaje de correo electrónico es un mensaje de correo electrónico en forma codificada
415
Analizar el mensaje de correo electrónico para obtener información de codificación del mensaje de correo electrónico
420
Decodificar el mensaje de correo electrónico de acuerdo con la información de codificación, para obtener una parte, en forma decodificada, del mensaje de correo electrónico
425
Determinar si la parte del mensaje de correo electrónico es segura
430
No
Sí
Rechazar el reenvío de la parte del mensaje de correo electrónico al dispositivo cliente
440
Reenviar la parte del mensaje de correo electrónico al dispositivo cliente
435

FIG. 4

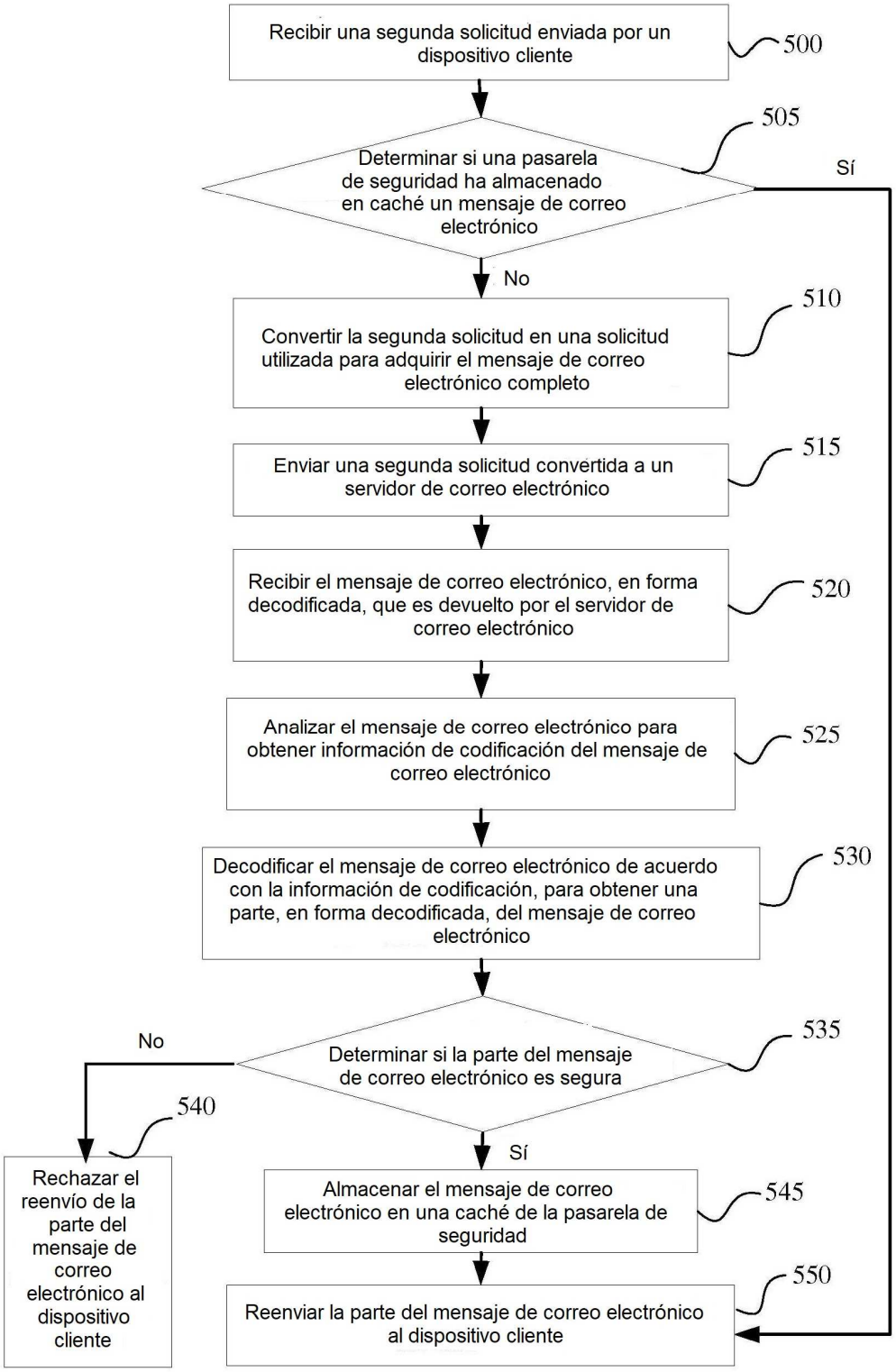
Recibir una segunda solicitud enviada por un dispositivo cliente
500
Determinar si una pasarela de seguridad ha almacenado en caché un mensaje de correo electrónico
505
Sí
No
Convertir la segunda solicitud en una solicitud utilizada para adquirir el mensaje de correo electrónico completo
510
Enviar una segunda solicitud convertida a un servidor de correo electrónico
515
Recibir el mensaje de correo electrónico, en forma decodificada, que es devuelto por el servidor de correo electrónico
520
Analizar el mensaje de correo electrónico para obtener información de codificación del mensaje de correo electrónico
525
Decodificar el mensaje de correo electrónico de acuerdo con la información de codificación, para obtener una parte, en forma decodificada, del mensaje de correo electrónico
530
Determinar si la parte del mensaje de correo electrónico es segura
535
No
Sí
Rechazar el reenvío de la parte del mensaje de correo electrónico al dispositivo cliente
540
Almacenar el mensaje de correo electrónico en una caché de la pasarela de seguridad
545
Reenviar la parte del mensaje de correo electrónico al dispositivo cliente
550

FIG. 5

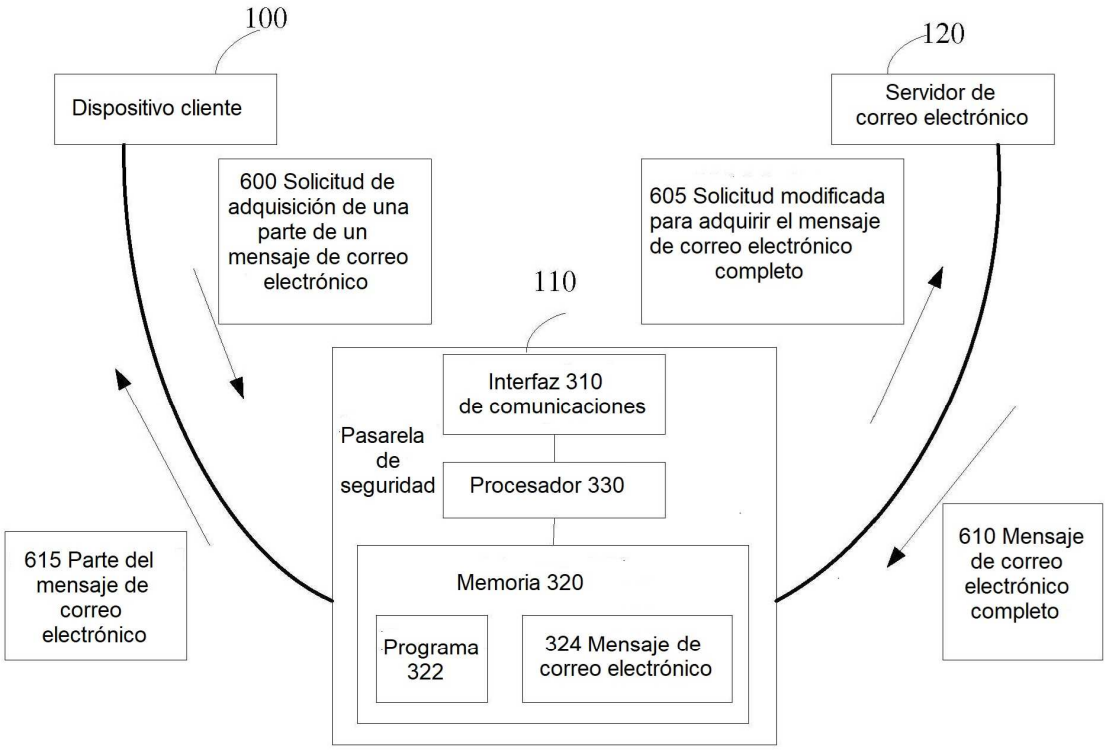
100
Dispositivo cliente
120
Servidor de correo electrónico
600 Solicitud de adquisición de una parte de un mensaje de correo electrónico
605 Solicitud modificada para adquirir el mensaje de correo electrónico completo
110
Interfaz 310 de comunicaciones
Pasarela de seguridad
Procesador 330
Memoria 320
Programa 322
324 Mensaje de correo electrónico
615 Parte del mensaje de correo electrónico
610 Mensaje de correo electrónico completo

FIG. 6