(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 290 148**

(51) Int. Cl.:
***H04L 29/06*** (2006.01)
***H04Q 7/24*** (2006.01)
***H04L 12/66*** (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Número de solicitud europea: **01945907 .2**
(86) Fecha de presentación : **06.07.2001**
(87) Número de publicación de la solicitud: **1314291**
(87) Fecha de publicación de la solicitud: **28.05.2003**

(54) Título: **Tunelización de una sesión de protocolo de aplicaciones inalámbricas (WAP).**

(30) Prioridad: **31.08.2000 US 652421**

(45) Fecha de publicación de la mención BOPI:
**16.02.2008**

(45) Fecha de la publicación del folleto de la patente:
**16.02.2008**

(73) Titular/es:
**TELEFONAKTIEBOLAGET LM ERICSSON (publ)**
**164 83 Stockholm, SE**

(72) Inventor/es: **Larsson, Pär y**
**Nilsson, Mikael**

(74) Agente: **Elzaburu Márquez, Alberto**

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



Venta de fascículos: Oficina Española de Patentes y Marcas. Pº de la Castellana, 75 – 28071 Madrid

## DESCRIPCIÓN

Tunelización de una sesión de protocolo de aplicaciones inalámbricas (WAP).

### Antecedentes de la invención

#### Campo técnico de la invención

La presente invención está relacionada con sesiones WAP entre un terminal móvil y una pasarela WAP y, más en particular, con la organización de capas de protocolos en una pasarela WAP.

#### Descripción de la técnica relacionada

Cuando se construye una red privada virtual para usuarios corporativos que es accesible por terminales móviles, tales como ordenadores portátiles, teléfonos móviles y similares, no existe una manera estandarizada para construir la denominada "zona desmilitarizada", que permita la autenticación de usuarios de terminales móviles que accedan a la red a través de un protocolo de aplicaciones inalámbricas (WAP), antes de dar acceso realmente a un usuario a la red corporativa. En Internet, puede utilizarse un mecanismo de pregunta/respuesta o de retos donde típicamente el protocolo punto a punto (PPP) o el servidor de acceso remoto solicita a un usuario su nombre de usuario, le indica al usuario un reto, y lee cualquier palabra de paso proporcionada por el usuario como respuesta al reto. Esto ocurre antes de proporcionar acceso realmente al usuario. Los mecanismos existentes para autorizar el acceso de un terminal WAP a la red son molestos y tienen varios problemas de seguridad.

La autenticación puede hacerse utilizando un mecanismo conocido como Autenticación Básica de HTTP, donde el servidor de origen (por ejemplo, un servidor de Internet) debe recibir primero una petición del dispositivo terminal con el fin de responder con una petición de autenticación al terminal. Esto, naturalmente, requiere que el terminal ya esté conectado a la red, e incluso a la red privada. La autenticación puede hacerse también en la pasarela, por ejemplo permitiendo a los usuarios de dispositivos terminales móviles configurar una palabra de paso y un identificador de usuario de la pasarela. Alternativamente, esto se hace en el servidor de acceso. Estos métodos son muy inflexibles, y si se utiliza un método más seguro, tal como la utilización de una palabra de paso cada vez, tarjetas seguras, etc., para entrar en la red corporativa, se requiere una cantidad de trabajo excesiva para el usuario. Los terminales actuales no permiten al usuario obtener una "ventana del terminal" similar a la que está disponible, por ejemplo, en Windows 98, donde se pueden introducir palabras de paso dinámicas. Por tanto, es deseable alguna manera de proporcionar un proceso de autorización no probado para terminales móviles que accedan a redes privadas virtuales.

El FORO DE APLICACIONES INALÁMBRICAS: "Wireless Aplication Protocol Wireless datagram Protocol specification", Especificación del Protocolo de aplicaciones inalámbricas, protocolo de datagramas inalámbricos, xx,xx, 30 de Abril de 1998, ilustra una pasarela WAP de acuerdo con la técnica anterior. Sin embargo, no proporciona un proceso de autorización no probado para terminales móviles que acceden a redes privadas virtuales.

### Sumario de la invención

La presente invención supera los problemas anteriores y otros problemas con una pasarela WAP que interconecta una red PLMN y una segunda red privada de datos.

La pasarela WAP incluye un Proxy de la primera etapa y un Proxy de la segunda etapa. El Proxy de la primera etapa está situado en un primer lado de un cortafuegos de la segunda red e incluye la capa WDI de la pila de protocolos WAP. Las capas restantes de la pila de protocolos WAP están situadas dentro de un Proxy de segunda etapa situado en el otro lado del cortafuegos de la segunda red. Respondiendo a las peticiones proporcionadas desde un terminal móvil, la capa WDP del Proxy de la primera etapa puede comunicarse con capas de protocolo dentro del Proxy de la segunda etapa, utilizando la tunelización SSL/TLS. Como resultado, la autenticación solamente se necesita una vez, en la primera petición para acceder a la red privada de datos, y todas las peticiones posteriores dentro de la sesión son tunelizadas directamente a través del cortafuegos.

### Breve descripción de los dibujos

Se puede obtener una comprensión más completa del método y aparato de la presente invención, haciendo referencia a la siguiente Descripción Detallada, cuando se considera conjuntamente con los dibujos que se acompañan, en los que:

La figura 1 es una ilustración de un terminal móvil que accede a una pasarela WAP configurada de acuerdo con la presente invención;

La figura 2 es una pasarela WAP configurada de acuerdo con la presente invención, y

La figura 3 es un diagrama de flujo que ilustra la manera en la cual un terminal móvil accede a la pasarela WAP de la figura 2.

**Descripción detallada**

Haciendo referencia ahora a los dibujos y, más en particular, a la figura 1, se ilustra la manera en la que un terminal móvil 10 puede acceder a una red 15, tal como una red intranet privada, de acuerdo con el método y el aparato de la presente invención. Aunque la descripción siguiente se ha hecho con respecto a una pasarela WAP y a un protocolo WAP, debe observarse que la presente invención puede ser útil con cualquier pasarela de Internet para móviles y una configuración de Internet para móviles utilizando un dispositivo de usuario, una red principal (PLMN), una pasarela y una red secundaria (intranet). El terminal móvil 10 obtiene acceso a un servidor 25 de acceso, a través de una red PLMN 20. El enlace 26 entre el terminal móvil 10 y la red PLMN 20 comprende un enlace de comunicaciones inalámbricas. El terminal móvil 10 puede consistir en un ordenador portátil, un asistente personal digital (PDA), un teléfono móvil, un buscapersonas, etc.

Una vez que el terminal móvil 10 ha obtenido acceso al servidor 25 de acceso, a través de la red PLMN 20, el terminal móvil 10 puede intentar acceder a la red privada 15, por ejemplo, una red corporativa, utilizando una pasarela WAP 30. La pasarela 30 puede comprender físicamente múltiples entidades de máquinas que comprenden lógicamente una sola pasarela. La red privada 15 puede comprender una red privada virtual que haya sido establecida para usuarios de una compañía u organización particular.

La pasarela WAP 30 comprende una pasarela de protocolos que traduce las peticiones entre un protocolo WAP (WAE, WSP, WTP, WTLS y WDP) y un correspondiente protocolo de Internet (HTTP y TCP/IP) para la transmisión en ambas direcciones. La traducción se consigue a través de codificadores y descodificadores de contenidos (no ilustrados) dentro de la pasarela WAP 30. Dentro de la presente invención, la pasarela WAP 30 incluye dos componentes funcionales independientes, que son un Proxy 35 de primera etapa y un Proxy 40 de segunda etapa. El Proxy 35 de primera etapa contiene la capa más baja de la pila de protocolos WAP y es el responsable de conceder el acceso de un terminal móvil 10 a la red privada 15. El Proxy 40 de la segunda etapa incluye el resto de capas de la pila de protocolos WAP. El Proxy 35 de la primera etapa y el Proxy 40 de la segunda etapa están funcionalmente separados de forma que el Proxy de la primera etapa reside en el exterior del cortafuegos 37 (es decir, en el lado de la red PLMN) de la red privada 15, mientras que el Proxy 40 de la segunda etapa reside dentro del cortafuegos 37 (es decir, en el lado de la red privada) de la red privada 15.

Haciendo referencia ahora a la figura 2, se ilustra con más detalle la estructura y la funcionalidad de la pasarela WAP 30. Como se ha mencionado anteriormente, la pasarela WAP 30 incluye una funcionalidad 35 de Proxy de la primera etapa, que reside en el lado público del cortafuegos 37 asociado con la red PLMN 20, y la funcionalidad 40 del Proxy de la segunda etapa que reside en el lado privado del cortafuegos 37 asociado con la red privada 15.

La funcionalidad 35 del Proxy de la primera etapa incluye la capa 45 del protocolo WDP. La capa WDP 45 comprende el protocolo de la capa de transporte, dentro de la arquitectura WAP. La capa WDP 45 opera por encima de los servicios portadores con capacidad de datos, soportados por la red PLMN 20. La capa WDP 45 actúa como un servicio de transporte general para los protocolos de las capas superiores de la arquitectura WAP y se comunica transparentemente sobre uno de los servicios portadores disponibles.

El resto de la pila de protocolos WAP reside dentro de la funcionalidad 40 del Proxy de la segunda etapa. La capa 50 de protocolos de sesión inalámbrica (WSP) proporciona servicios adecuados para aplicaciones de navegación. La capa 50 de WSP permite a la pasarela WAP 30 conectar un cliente con un servidor estándar de HTTP. La capa 50 de protocolos WSP proporciona la capa de la sesión de la pila de protocolos WAP y tiene un interfaz constante para los servicios de dos sesiones. El servicio de la primera sesión es un servicio orientado a la conexión, que opera por encima del protocolo de la capa de transacciones WTP. El servicio de la segunda sesión es un servicio sin conexiones que opera por encima de un servicio de datagramas seguros o no seguros (WDP).

Las capas adicionales de protocolos incluyen la capa 65 del entorno de aplicaciones inalámbricas (WAE), que es un entorno de aplicaciones de propósito general basado en una combinación de tecnologías W3C e IETF de Internet para móviles. La capa 65 de WAE proporciona un entorno de inter-operaciones que permite a los operadores y a los proveedores de servicios construir aplicaciones y servicios útiles en una amplia variedad de plataformas inalámbricas. La capa 55 del protocolo de transacciones inalámbricas (WTP) proporciona un protocolo orientado a las transacciones, que es adecuado para ser utilizado con estaciones móviles, y se utiliza para supervisar transacciones inalámbricas. La capa 60 de seguridad de las capas de transporte inalámbrico (WTLS) es un protocolo basado en la seguridad para ser utilizado con protocolos de transporte WAP. La capa 60 de WTLS asegura la integridad de los datos para transmisiones entre la pasarela WAP 30 y el terminal móvil 10, asegura la privacidad de los datos transmitidos entre el terminal móvil y la pasarela WAP para impedir la interceptación y la descodificación por partes intermedias, permite la autenticación del terminal móvil y protege contra la denegación de ataques al servicio.

El Proxy 35 de la primera etapa es capaz de comunicarse con el Proxy 40 de la segunda etapa utilizando la capa WDP 45 y la capa WSP 50. Se utiliza la capa WDP 45 porque solamente se pueden realizar operaciones inofensivas por un acceso concedido a esta capa. La capa WSP 50 se utiliza porque todas las configuraciones WAP incluyen esta capa de sesión. Sin embargo, la capa WTLS 60 podría ser utilizada como alternativa a la capa WSP 50. El software de estas capas se comunica con cada una de las demás utilizando la tunelización SSL/TLS 70. La tunelización SSL/TLS 70 comprende un canal de comunicaciones encriptadas entre las capas. El protocolo SSL utiliza una combinación de encriptación con clave pública y con clave simétrica. La encriptación con clave simétrica es mucho más rápida que la

encriptación con clave pública, pero la encriptación con clave pública proporciona mejores técnicas de autenticación. Una sesión SSL comienza siempre con un intercambio de mensajes llamado saludo inicial de SSL. El saludo inicial permite a un servidor autenticarse él mismo a un cliente utilizando técnicas de clave pública, después permite al cliente y al servidor cooperar en la creación de claves simétricas utilizadas para una rápida encriptación, desencriptación y detección de manipulaciones durante la sesión que sigue. Opcionalmente, el saludo inicial permite también al cliente autenticarse para el servidor.

La tunelización de SSL/TLS permite comunicarse entre sí a las capas WDP 45 y WSP 50 en lados opuestos del cortafuegos de la red privada. La capa WDP 45 hace un seguimiento de los usuarios y tuneliza las peticiones al Proxy 40 de la segunda etapa, donde otras capas de la pila de protocolos pueden funcionar bajo petición. La primera vez que un usuario intenta acceder a la pasarela WAP 30 a través del Proxy 35 de primera etapa, se requiere un proceso de autenticación para el usuario, antes de que la petición pueda ser procesada. Para las peticiones siguientes, el Proxy 35 de primera etapa puede tunelizar peticiones de la capa WDP 45 a la capa WSP 50 del Proxy 40 de la segunda etapa, utilizando un túnel SSL/TLS 70 seguro sin un proceso de autenticación adicional. Pueden utilizarse varios métodos por el Proxy de la primera etapa para hacer un seguimiento de los usuarios que han entrado previamente a través de la pasarela WAP 30. La pasarela 30 podría mantener una pequeña base de datos relacional (no ilustrada), una lista de un solo enlace (no ilustrada), un fichero plano (no ilustrado) o algún tipo de serie ordenada para hacer un seguimiento de los usuarios previamente autenticados del Proxy 35 de la primera etapa.

Haciendo referencia ahora a la figura 3, se ilustra un proceso por el cual se actúa sobre las peticiones por medio de la pasarela WAP 30. La petición, que puede comprender una Conexión WSP, una Continuación, una Suspensión, una Obtención y similares, se recibe inicialmente en el paso 75 desde el terminal móvil 10. El Proxy 35 de la primera etapa de la pasarela WAP 30 analiza la petición recibida para determinar en el paso 80 de interrogación, si esta petición comprende la primera petición del terminal móvil 10 a la pasarela WAP 30. Si la petición recibida comprende una primera petición desde el terminal móvil 10, el Proxy 35 de primera etapa devuelve un paquete WML 85 al terminal móvil forzando un proceso de entrada por el usuario del terminal móvil 10. Como respuesta al paquete WML devuelto, el terminal móvil intenta entrar en el paso 90 al Proxy 35 de la primera etapa de la pasarela WAP 30. La entrada del usuario es aprobada en el paso 95 por el Proxy de la primera etapa (suponiendo que es un usuario válido), y la petición es tunelizada en el paso 100 al Proxy 40 de la segunda etapa, utilizando la tunelización SSL/TLS 70, como se ha descrito anteriormente con respecto a la figura 2. Si el paso 80 de interrogación determina que la petición recibida no es la primera petición desde el terminal 10, la petición puede ser tunelizada directamente en el paso 100 al Proxy 40 de la segunda etapa sin el procedimiento de entrada.

La descripción anterior es de un modo de realización preferido para implementar la invención, y el alcance de la invención no debe estar necesariamente limitado por esta descripción. El alcance de la presente invención está definido, en lugar de eso, por las reivindicaciones siguientes.

## REIVINDICACIONES

1. Un método, que comprende los pasos de:

recibir (75) una petición desde un terminal móvil en una pasarela WAP; **caracterizado** por

acceder solamente a una capa WDP de una pila de protocolos WAP en un Proxy de primera etapa, que responde a la petición del terminal móvil; y

comunicarse entre la capa WDP de la pila de protocolos WAP de un Proxy de primera etapa y al menos alguna otra capa de la pila de protocolos WAP en un Proxy de segunda etapa, utilizando un canal de comunicaciones encriptadas, donde la capa WDP del Proxy de la primera etapa está situada en un primer lado de un cortafuegos y la otra capa de la pila de protocolos WAP del Proxy de la segunda etapa está situada sobre un segundo lado del cortafuegos.

2. El método de la reivindicación 1, en el que el paso de acceder comprende además los pasos de

determinar si la petición es una primera petición desde el terminal móvil a la pasarela;

si la petición es la primera petición desde el terminal móvil al servidor, solicitar autenticación desde el terminal móvil.

3. El método de la reivindicación 2, en el que si la petición es una petición subsiguiente desde la estación móvil, el método comprende el paso adicional de acceder a la capa WDP para comunicarse con la otra capa de la pila de protocolos sin ninguna autenticación.

4. El método de la reivindicación 2, en el que el paso de solicitar comprende además devolver un paquete WML al terminal móvil.

5. El método de la reivindicación 2, en el que el paso de acceder incluye además aprobar los datos de entrada proporcionados por el terminal móvil.

6. El método de la reivindicación 1, en el que la otra capa comprende una capa WSP de la pila de protocolos.

7. El método de la reivindicación 1, en el que el canal de comunicaciones encriptadas es un túnel SSL/TLS.

8. Una pasarela WAP (30), que comprende:

una primera conexión a una primera red PLMN;

una segunda conexión a una segunda red privada; **caracterizada** por un Proxy (35) de primera etapa asociado con la primera conexión y sobre un primer lado de un cortafuegos (37), asociado con la segunda red, incluyendo dicho Proxy (35) de la primera etapa una capa WDP de una pila de protocolos WAP; un Proxy (40) de la segunda etapa asociado con la segunda conexión y sobre un segundo lado del cortafuegos (37), asociado con la segunda red privada, incluyendo dicho Proxy (40) de la segunda etapa una parte de la capa WSP de la pila de protocolos WAP; y donde la capa WDP del Proxy de la primera etapa y la capa WSP del Proxy de la segunda etapa se comunican entre sí utilizando un canal de comunicaciones encriptadas.

9. La pasarela WAP (30) de la reivindicación 8, en la que la primera capa WDP transmite un paquete WML a un terminal móvil, como respuesta a una primera petición desde el terminal móvil.

10. La pasarela WAP (30) de la reivindicación 9, en la que la capa WDP aprueba los datos de entrada recibidos desde el terminal móvil, como respuesta al paquete WML.

11. La pasarela WAP (30) de la reivindicación 8, en la que el canal de comunicaciones encriptadas es un túnel SSL/TLS.

12. La pasarela WAP (30) de la reivindicación 8, en la que el Proxy de la primera etapa está adaptado para transmitir una petición de autenticación a un terminal móvil, como respuesta a una primera petición desde el terminal móvil.

13. La pasarela WAP (30) de la reivindicación 12, en la que la petición de autenticación comprende un paquete WML.

14. La pasarela WAP (30) de la reivindicación 12, en la que el Proxy de la primera etapa está adaptado para aprobar los datos de entrada recibidos desde el terminal móvil, como respuesta a la petición de autenticación.

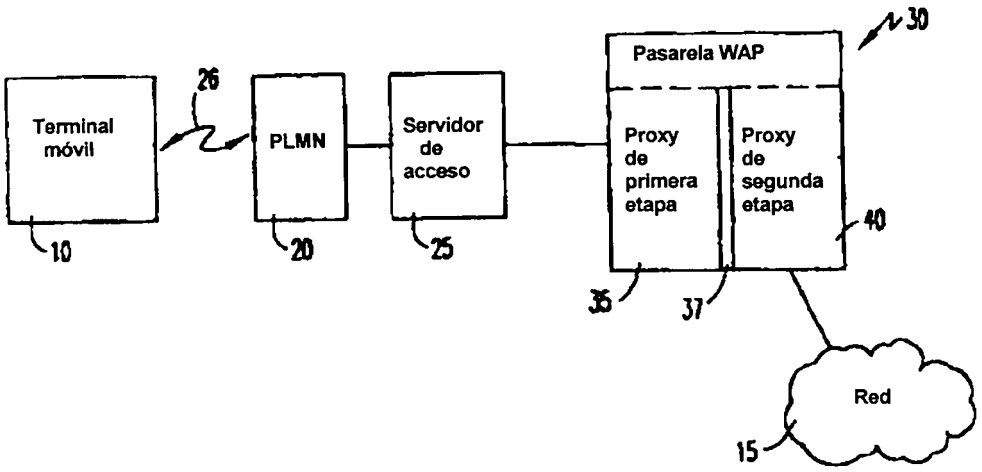

Terminal móvil
26
PLMN
Servidor de acceso
Pasarela WAP
30
Proxy de primera etapa
Proxy de segunda etapa
40
10
20
25
35
37
Red
15

*FIG. 1*

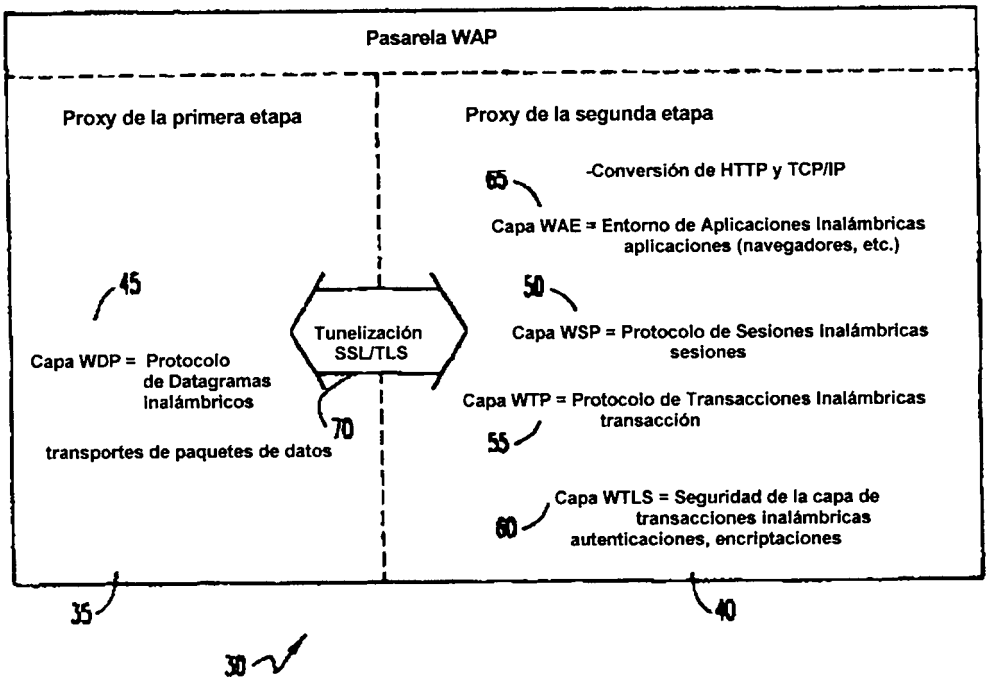

Pasarela WAP
Proxy de la primera etapa
Proxy de la segunda etapa
-Conversión de HTTP y TCP/IP
65
Capa WAE = Entorno de Aplicaciones Inalámbricas
aplicaciones (navegadores, etc.)
45
50
Tunelización SSL/TLS
Capa WDP = Protocolo de Datagramas Inalámbricos
Capa WSP = Protocolo de Sesiones Inalámbricas
sesiones
70
Capa WTP = Protocolo de Transacciones Inalámbricas
transacción
transportes de paquetes de datos
55
Capa WTLS = Seguridad de la capa de transacciones inalámbricas
autenticaciones, encriptaciones
60
35
40
30

*FIG. 2*

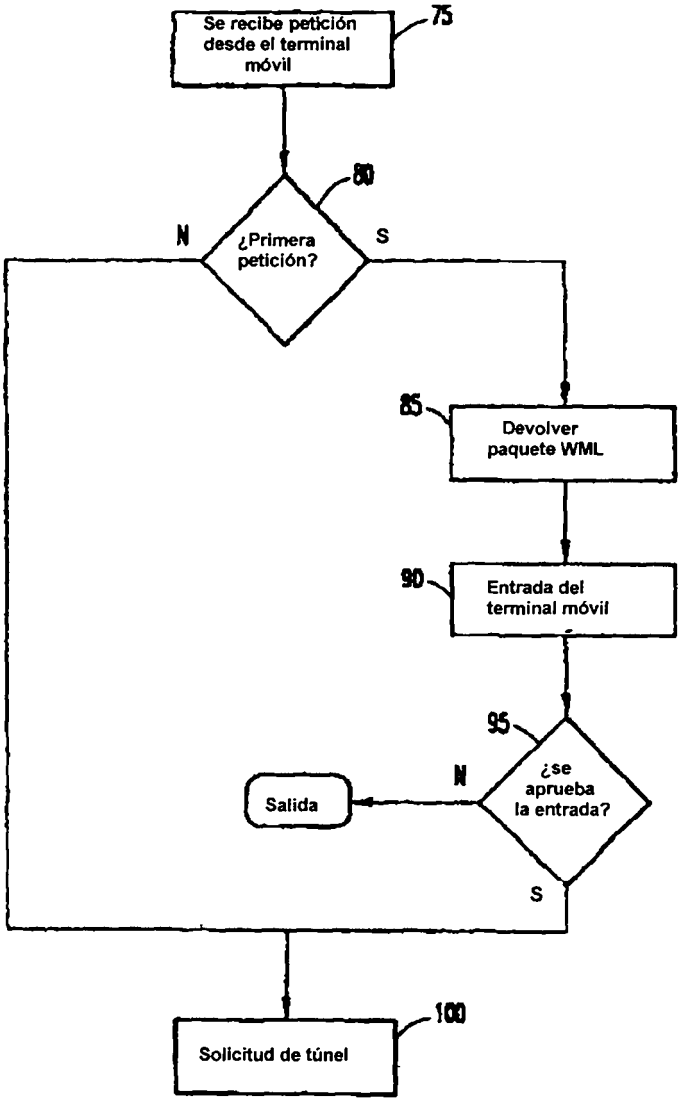

Se recibe petición desde el terminal móvil
75
80
¿Primera petición?
N
S
85
Devolver paquete WML
90
Entrada del terminal móvil
95
¿se aprueba la entrada?
N
Salida
S
100
Solicitud de túnel

*FIG. 3*