(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 535 021**

(51) Int. CI.:

H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **13.10.2010 E 10187415 (4)**

(97) Fecha y número de publicación de la concesión europea: **21.01.2015 EP 2323334**

(54) Título: **Autorización de una conexión a través de un cortafuegos de un dispositivo de acceso a la red**

(30) Prioridad:

13.11.2009 DE 102009044525

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
04.05.2015

(73) Titular/es:

VODAFONE HOLDING GMBH (100.0%)
Mannesmannufer 2
40213 Düsseldorf, DE

(72) Inventor/es:

ACKERMANN, THOMAS

(74) Agente/Representante:

VALLEJO LÓPEZ, Juan Pedro

DESCRIPCIÓN

Autorización de una conexión a través de un cortafuegos de un dispositivo de acceso a la red

Campo técnico de la invención

La presente invención se refiere a un procedimiento con las características mencionadas en la reivindicación 1.

Adicionalmente, la invención se refiere a un dispositivo de acceso a la red que permite establecer por medio de una red de telecomunicaciones una conexión de datos basada en paquetes a través de una red de datos pública con orientación de paquetes, con una dirección de red asignada al dispositivo de acceso a la red y telefonía con un número de teléfono asignado al dispositivo de acceso a la red, en donde el dispositivo de acceso a la red presenta las características mencionadas en la reivindicación 9.

Estado de la técnica

Como redes de telecomunicaciones públicas se conocen sobre todo las redes fijas sujetas a líneas de acuerdo con el estándar analógico POTS (Plain Old Telefon Service) o el estándar digital ISDN (Integrated Services Digital Network) junto con el estándar DSL (Digital Subscriber Line), así como las redes de telefonía móvil con una red de acceso basada en radiotransmisión de acuerdo con el estándar GSM/GPRS (Global System for Mobile Communications / General Packet Radio Service), el estándar UMTS (Universal Mobile Telecommunications System) o el estándar LTE (Long Term Evolution). El estándar LTE es un estándar para redes de telefonía móvil de la cuarta generación (4G). Además de telefonía y otros servicios con orientación de línea, estas redes de telecomunicaciones también ofrecen a los usuarios servicios con orientación de paquetes, tales como, por ejemplo, el uso de Internet.

Para poder usar estos servicios, el usuario a nivel local requiere un terminal de usuario (CPE, por las siglas en inglés de Customer Premises Equipment). Teléfonos, dispositivos de fax y módems son dispositivos CPE frecuentemente usados y que le permiten al usuario tener acceso a una red de telefonía o a Internet. Los módems de DSL también se denominan como módems de CPE. En el marco de la transición que actualmente se está realizando de las redes de telecomunicaciones tradicionales con intermediación de líneas a una infraestructura de red con intermediación uniforme de paquetes, se están empleando con una frecuencia cada vez mayor los así denominados dispositivos de acceso integrados (IAD, por las siglas en inglés de Integrated Access Device). Estos dispositivos de acceso sustituyen en una NGN (Next Generation Network) no sólo al módem de DSL y al splitter de DSL, sino también a los dispositivos analógicos y o dispositivos terminales de red ISDN (por ejemplo un NTBS: Network Termination for ISDN Basic Rate Access) y normalmente disponen de interfaces correspondientes para aparatos de teléfono analógicos, tales como dispositivos de ISDN y ordenadores locales o redes locales. Para el uso de servicios a través de una red de telecomunicaciones, al usuario o al dispositivo de acceso a la red, respectivamente, además de un número de teléfono también se le asigna una dirección de red, normalmente una dirección de IP (dirección de protocolo de Internet).

Adicionalmente, los dispositivos de acceso a la red tales como los módems de CPE o los IAD comprenden un así llamado cortafuegos como protección contra los accesos no autorizados desde Internet. El cortafuegos vigila el tráfico de datos que pasa por el mismo y basándose en reglas predeterminadas decide si determinados paquetes de datos pueden pasar o no. Basándose en una dirección de origen o una dirección de destino y basándose en los servicios usados sólo se permiten determinadas conexiones de comunicación previamente determinadas, mientras que todas las demás se impiden.

En una conexión bidireccional entre dos ordenadores a través de Internet, se usa el protocolo TCP (Transmission Control Protocol) que a su vez se basa en el protocolo de Internet (IP). Una conexión de TCP se identifica de manera inequívoca con dos puntos terminales. Un punto terminal consiste en una dirección de IP y un puerto. Este par forma un interface bidireccional en un ordenador y también se denomina como Socket. Mediante el uso de direcciones de IP se identifican los ordenadores que participan en la conexión. En ambos ordenadores participantes, los puertos identifican a las aplicaciones o servicios que se comunican entre sí. Un cortafuegos vigila tanto las direcciones de IP como también los puertos y o bien permite o impide las conexiones dependiendo de las direcciones de IP y/o de un número de puerto.

El documento WO 2008/149126 A2 describe un dispositivo periférico para un ordenador que comprende un módem para conexiones de datos a través de una red de telefonía móvil. El dispositivo periférico preferentemente está realizado en forma de ratón y dispone de un medio de autorización para comprobar una solicitud de conexión entrante desde un segundo ordenador para el establecimiento de una conexión segura. La solicitud de conexión entra en el dispositivo periférico a través de una conexión de GSM basada en línea. El medio de autorización comprueba la identidad del segundo ordenador basándose en un número de teléfono recibido junto con la conexión de GSM y verifica si se desea establecer una conexión segura con el segundo ordenador. Si esto es el caso, a través de la conexión de GSM se intercambian claves digitales para establecer la conexión segura. A continuación, la conexión segura se establece usando las claves digitales a través de una red de telefonía móvil de la tercera

generación (por ejemplo, de acuerdo con el estándar UMTS) con elevada velocidad de transmisión de datos.

El documento US 2006/291502 A1 desvela un procedimiento y un sistema para el establecimiento de una conexión de IP entre un nodo de red inicial en una república y un nodo de red terminal en una red de telecomunicaciones privada. El nodo de red terminal está adaptado para recibir una solicitud de conexión del nodo de red inicial a través de una conexión no IP. Basándose en la solicitud de conexión, el nodo de red terminal inicia entonces una conexión de IP con el nodo de red inicial.

El documento US 2007/147399 A1 desvela un sistema y un procedimiento entre dos dispositivos para el establecimiento de una conexión de IP, en donde un primer dispositivo envía su dirección de IP al otro dispositivo a través de un segundo canal de conexión de uso temporal, para entonces establecer una conexión de IP a través de un primer canal de conexión con el otro dispositivo en una red pública de ordenadores. A este respecto, el segundo canal de conexión puede estar configurado, por ejemplo, como una línea de red fija o como un intermediario de línea o como un canal de diálogo con intermediación de paquetes en una red de telefonía móvil, por el que mediante telefonía o mensaje corto (SMS) se transmite la dirección de IP.

Una desventaja de los procedimientos conocidos para la autorización de una conexión a través de un dispositivo de acceso a la red con un cortafuegos consiste en que para las conexiones entrantes deseadas siempre tienen que estar disponibles determinados puertos a través del cortafuegos. Por ejemplo, si un usuario quiere establecer en cualquier momento una conexión con otro dispositivo terminal a través de Internet con su dispositivo de acceso a la red o con un ordenador conectado con el mismo, el cortafuegos debe mantener los puertos correspondientes permanentemente abiertos.

Si adicionalmente el usuario quiere realizar esto con cualquier dispositivo terminal de su elección, por ejemplo, en un café Internet o en el domicilio de personas conocidas o allegadas, los puertos se deben mantener abiertos para cualesquiera direcciones de IP. Debido a este procedimiento, sin embargo, se crean importantes riesgos de seguridad. Personas no autorizadas podrían usar los puertos abiertos desde la Internet para contrarrestar el cortafuegos y de esa manera obtener acceso a datos sensibles.

Revelación de la invención

Por lo tanto, el objetivo de la presente invención consiste en evitar las desventajas del estado de la técnica y aumentar la seguridad en conexiones a través de una red de datos pública con orientación de paquetes a través de un cortafuegos de un dispositivo de acceso a la red.

De acuerdo con la presente invención, dicho objetivo se logra con un procedimiento con las características mencionadas en la reivindicación 1.

Adicionalmente, el objetivo se logra con un dispositivo de acceso a la red con las características mencionadas en la reivindicación 9.

La presente invención se basa en el principio de que las conexiones entrantes primeros son bloqueadas por el cortafuegos y sólo después de la verificación positiva de una característica de identificación se permite el establecimiento de una conexión a través del cortafuegos. Para esto, la característica de identificación es transmitida mediante una llamada o un mensaje de texto corto dirigido al número de teléfono asignado al dispositivo de acceso a la red. Como mensaje de texto corto se usa, por ejemplo, un mensaje de SMS (Short Message Service). La conexión de transmisión telefónica o de mensaje de texto corto hacia el dispositivo de acceso a la red que se usa para ello no es bloqueada por el cortafuegos, ya que el mismo sólo controla las conexiones con orientación de paquete a través de la red de datos pública. En otras palabras, a través de una conexión telefónica o de mensajes cortos y una característica de identificación transmitida a través de dicha conexión, el cortafuegos autoriza una conexión desde la red de datos pública.

A través del procedimiento de acuerdo con la presente invención y el dispositivo de acceso a la red conforme a la presente invención, una conexión desde la red de datos pública al dispositivo de acceso a la red o a otros dispositivos conectados al mismo sólo se permite cuando ellos se solicite por medio de una correspondiente llamada o mensaje de texto corto. Previamente, el cortafuegos no permite ninguna o sólo algunas pocas conexiones entrantes seguras y se encarga así de proveer una protección óptima contra ataques provenientes de la red de datos pública. Cuando se produce una llamada como la que se ha descrito previamente, en primer lugar se verifica la existencia de un derecho correspondiente basándose en una característica de identificación transmitida. Si el resultado de la verificación expositivo, el cortafuegos permite que se establezcan conexiones con, o que se envíe el respectivo paquete de datos a, los puertos autorizados, respectivamente. De esta manera se asegura una seguridad muy elevada frente a los accesos no autorizados provenientes de la red de datos pública, y al mismo tiempo se asegura que un acceso autorizado se pueda realizar sin complicaciones.

En una forma de realización ventajosa del procedimiento de acuerdo con la presente invención para la autorización de una conexión a través de una red de datos pública con orientación de paquetes en un cortafuegos de un

dispositivo de acceso a la red, se comprueba la coincidencia de la característica de identificación transmitida con una característica de identificación almacenada en el dispositivo de acceso a la red. De esta manera se puede realizar una rápida y segura comprobación de la autorización del autor de la llamada o del remitente para la autorización de una conexión desde la red de datos pública. De manera preferente, el usuario del dispositivo de acceso a la red puede efectuar por sí mismo el almacenamiento o la modificación de la característica de identificación almacenada. De esta manera, la verificación de la autorización puede ser adaptada de forma muy flexible a los deseos y necesidades de aplicación del usuario.

En una forma de realización preferente de la presente invención, como característica de identificación se usa un número telefónico del autor de la llamada o del remitente de un mensaje de texto corto transmitido al dispositivo de acceso a la red. Esto puede realizarse, por ejemplo, a través de una CLIP (Calling Line Identification Presentation). La CLIP se usa en redes telefónicas analógicas y de ISDN, así como en redes de telefonía móvil, para transmitir el número telefónico de un abonado previamente a la aceptación de la llamada en el dispositivo terminal llamado. En mensajes cortos de texto, tales como, por ejemplo, un mensaje SMS, normalmente el número de teléfono del remitente es transmitido en el mensaje corto de texto al destinatario. La CLIP y el número de teléfono del remitente en un mensaje SMS se consideran como muy seguros frente a falsificaciones. Por lo tanto, cuando se usa un número de teléfono transmitido de esta manera como característica de identificación, se alcanza un grado muy elevado de seguridad. Adicionalmente, en una llamada de la transmisión del número de teléfono también se realiza sin que se acepte la llamada, por lo que resulta muy económico para el usuario.

Una forma de realización adicional del procedimiento de acuerdo con la presente invención emplea ventajosamente una característica introducida por el autor de la llamada o el remitente y transmitida mediante la llamada o el mensaje de texto como característica de identificación. Debido a esta medida también es posible la transmisión de una característica de identificación válida incluso si se suprime la transmisión del número de teléfono (por ejemplo, CLIR: Calling Line Identification Restriction), o si se usa un dispositivo terminal ajeno. El usuario obtiene así la posibilidad muy ventajosa de usar numerosos dispositivos terminales para autorizar una conexión a través del cortafuegos del dispositivo de acceso a la red.

Adicionalmente, en una forma de realización ventajosa del procedimiento de acuerdo con la presente invención, para la autorización de una conexión con la característica de identificación se transmite a través de la llamada o el mensaje de texto la dirección de un dispositivo terminal usado para la conexión. Con la dirección disponible es posible autorizar solamente conexiones desde el dispositivo terminal empleado. Por ejemplo, el cortafuegos sólo permite el paso de paquetes de datos desde el dispositivo terminal a través de un puerto abierto. Debido a esto se optimiza la seguridad frente a los accesos no autorizados.

En una forma de realización preferente del procedimiento de acuerdo con la presente invención se prevé la especificación de las propiedades de conexión antes de que se autorice la conexión. Preferentemente, esto es realizado por el usuario o por un operador de la red de telecomunicaciones antes o durante la puesta en servicio del dispositivo de acceso a la red. También es posible la especificación o modificación posterior de las propiedades de conexión durante el uso. A este respecto se especifican en particular las posibles actividades a través de una conexión autorizada hacia una red de datos pública. Con esta medida, la conexión a ser autorizada por el cortafuegos del dispositivo de acceso a la red puede ser adaptada de manera óptima a múltiples aplicaciones. El procedimiento de acuerdo con la presente invención puede ser aplicado de forma universal. Con la especificación de las posibles actividades, se incrementa tradicionalmente de forma sustancial la seguridad frente a los accesos no autorizados desde la red de datos pública a través de la conexión autorizada.

Preferentemente, en una forma de realización del procedimiento de acuerdo con la presente invención se transmiten instrucciones de mando para el dispositivo de acceso a la red a través de la llamada o el mensaje de texto. El dispositivo de acceso a la red y las características de la conexión se pueden adaptar a los deseos y requerimientos actuales del usuario inmediatamente antes de la autorización por el dispositivo de acceso a la red. De manera muy ventajosa para el usuario, esta adaptación es posible en todo momento desde lugares remotos. A través de la configuración inmediatamente antes de la autorización de una conexión, se incrementa adicionalmente la seguridad contra accesos no autorizados, debido a que la conexión no va a ser autorizada desde un principio para todos los posibles deseos de uso del usuario.

Adicionalmente, otra forma de realización ventajosa del procedimiento de acuerdo con la presente invención prevé que la dirección de red asignada al dispositivo de acceso a la red sea transmitida al autor de la llamada o al remitente después de autorizar la conexión desde un módulo de transmisión de direcciones por medio de un correo electrónico o un mensaje de texto corto. De esta manera, también en caso de que se desconozca la dirección de red del dispositivo de acceso a la red, es posible establecer una conexión rápida y sin problemas con el dispositivo de acceso a la red. Este procedimiento resulta particularmente práctico en el caso de direcciones de red que son asignadas dinámicamente durante la puesta en servicio del dispositivo de acceso a la red o a intervalos regulares y que por lo tanto no son conocidas de antemano por el usuario. Asimismo, tampoco es necesario ya que el usuario memorice o recuerde de manera complicada y susceptible a errores las direcciones de red que se asignan de forma estática.

Una forma de realización ventajosa del dispositivo de acceso a la red de acuerdo con la presente invención comprende una memoria de datos para almacenar una característica de identificación que es utilizada por la unidad de verificación para comprobar la característica de identificación transmitida. Como característica de identificación se puede almacenar, por ejemplo, un número de teléfono u otra identificación. Con la característica de identificación almacenada se puede lograr una verificación rápida y confiable del derecho que tiene el autor de la llamada o el remitente para que se autorice la conexión desde la red de datos pública. De manera preferente, la memoria de datos está configurada como memoria reescribible. El usuario del dispositivo de acceso a la red puede efectuar entonces por sí mismo un almacenamiento o un cambio de la característica de identificación almacenada, por lo que la verificación de derechos se puede adaptar de manera sumamente flexible a los deseos y requerimientos de aplicación del usuario. Adicionalmente, una forma de realización preferente del dispositivo de acceso a la red de acuerdo con la presente invención prevé un dispositivo de configuración con una memoria de configuración para determinar y almacenar propiedades de conexión antes de que se autorice la conexión. La configuración es realizada, por ejemplo, por el usuario o por un operador de la red de telecomunicaciones, o durante la puesta en servicio del dispositivo de acceso la red. También es posible una especificación o un cambio posterior de las propiedades de conexión durante el uso. A este respecto se determinan en particular las posibles actividades a través de una conexión autorizada hacia una red de datos pública. Al igual que en la configuración correspondiente del procedimiento de acuerdo con la presente invención, de esta manera es posible adaptar de forma óptima una conexión a ser autorizada a una pluralidad de aplicaciones y actividades. Adicionalmente, se optimiza la seguridad frente a accesos no autorizados desde la red de datos pública debido a la especificación de las posibles actividades.

Otras formas de realización del dispositivo de acceso a la red de acuerdo con la presente invención se corresponden respectivamente con una forma de realización previamente descrita del procedimiento conforme a la presente invención y, por lo tanto, ofrecen las mismas ventajas.

Adicionalmente, otras formas de realización y ventajas se derivan del objeto de las reivindicaciones subordinadas, así como del dibujo con su correspondiente descripción.

Un ejemplo de realización de la presente invención se describe a continuación con referencia al dibujo correspondiente.

Breve descripción del dibujo

La Fig. 1 muestra en un diagrama de principio esquemático un ejemplo de realización del procedimiento de acuerdo con la presente invención y de un correspondiente dispositivo de acceso a la red para autorizar una conexión a través de la red de datos pública con orientación de paquetes en un cortafuegos.

Ejemplo de realización preferente

En la Fig. 1 se usa el numeral 10 para designar una red de telefonía móvil. La red de telefonía móvil es una red de telefonía móvil pública, celular, de 2.5ª, 3ª o 4ª generación y está configurada, por ejemplo, de acuerdo con el estándar GSM, GPRS, EDGE, UMTS, HSDPA, CDMA2000, FOMA, TD-SCDMA, LTE/SEA o WiMAX. Para el especialista en la materia son conocidas estas redes de telefonía móvil y sus correspondientes componentes. Por lo tanto, para una mayor simplicidad, la red de telefonía móvil 10 sólo se representa de forma estilizada mediante una nube con una torre de antena 12 comprendida en ella.

Adicionalmente, en las Fig. 1 se designa con el numeral 14 una red fija sujeta a líneas. La red fija 14 está configurada de acuerdo con el conocido estandarte analógico o el estándar ISDN y el estándar DSL. También la red fija 14 por razones de simplicidad se representa de manera estilizada mediante una nube con un mástil de telégrafo 16 comprendido en ella.

Tanto la red móvil 10 como también la red fija 14 le permiten al usuario establecer una telecomunicación. Por lo tanto, en lo sucesivo también se denominan como redes de telecomunicaciones 10, 14. Adicionalmente, las redes de telecomunicaciones 10, 14 le permiten al usuario tener acceso a la Internet como una red de datos pública con orientación de paquetes 18. La estructura y el modo de funcionamiento de la Internet 18 también son conocidas por los especialistas en la materia. Por lo tanto, la Internet 18 en la Fig. 1 también se representa de forma estilizada mediante una nube con ordenadores 20 interconectados, comprendidos en la misma.

Con un dispositivo de acceso a la red 22, el usuario puede tener acceso a por lo menos una de las redes de telecomunicaciones 10, 14 y usar servicios de la red de telecomunicaciones 10, 14, o, a través de la red de telecomunicaciones 10, 14, usar servicios de la Internet 18. Para conexiones sujetas a una línea con la red fija 14, el dispositivo de acceso a la red 22 dispone de un interface de red fija basado en cable 24 para un cable 26 de la red fija 14. Alternativamente, o adicionalmente, en el dispositivo de acceso a la red 22 se provee un interface de telefonía móvil 28 para conexiones con la red de telefonía móvil 10 a través de señales de radio 30.

El dispositivo de acceso a la red 22 es, por ejemplo, un módem de CPE (CPE: Customer Premises Equipment), un

módem de DSL (DSL: Digital Subscriber Line), un router de DSL, un router de DSL-WLAN (WLAN: Wireless Local Area Network) o un módem de IAD (IAD: Integrated Access Device). Sin embargo, el aparato de acceso a la red 22 también puede ser un dispositivo terminal de telefonía móvil, tal como un teléfono móvil o un teléfono inteligente, un ordenador estacionario (por ejemplo, un PC), un ordenador móvil (por ejemplo, un notebook, un netbook o un Personal Digital Assistent) o algún otro dispositivo con funcionalidad de módem integrada.

Para la conexión opcional de un aparato de teléfono analógico o de ISDN 32 se provee un interface de telefonía 34. A través de un interface de datos 36 (por ejemplo, basado en radiotransmisión o cable de acuerdo con un estandarte IEEE-802) se puede establecer una conexión con un ordenador 38 o con una red de área local no representada en la Fig. 1 para un intercambio de datos con el dispositivo de acceso a la red 22. De esta manera, los servicios de la red de telecomunicaciones 10, 14 o de la Internet 18 también están disponibles para el ordenador 38 o el aparato de teléfono 32. Para servicios mediados por línea, por ejemplo, telefonía, fax o mensajes SMS, la respectiva red de telecomunicaciones 10, 14 asigna un número de teléfono 40 al dispositivo de acceso a la red 22. Con una dirección de red 42, que también es asignada al dispositivo de acceso a la red 22 por la correspondiente red de telecomunicaciones 10, 14, se pueden establecer conexiones con orientación de paquetes a través de la Internet 18. A este respecto, la dirección de red 42 puede ser una dirección de red asignada de manera permanente o dinámica.

Como protección contra accesos no autorizados o malintencionados hacia o desde la Internet 18, en el dispositivo de acceso a la red 22 se provee un así llamado cortafuegos 44. El cortafuegos 44 filtra los paquetes de datos que son intercambiados a través de una conexión entre la Internet 18 y el dispositivo de acceso a la red 22, basándose en un puerto de destino, una dirección de origen y una dirección de destino. Estos datos están incluidos en cada paquete de datos. La verificación de los paquetes de datos se efectúa de acuerdo con un reglamento predeterminado. También es posible el uso de filtros adicionales en el cortafuegos 44, tales como, por ejemplo, filtros de contenido.

El dispositivo de acceso a la red 22 comprende además un dispositivo de recepción 46 para recibir una llamada o un mensaje de texto, por ejemplo, un mensaje de SMS, EMS (Enhanced Message Service) o MMS (Multimedia Messaging Service), con por lo menos una característica de identificación 48. La llamada o el mensaje de texto se dirige a un número de teléfono 40 del dispositivo de acceso a la red 22. Como característica de identificación 48, el dispositivo de recepción 46 recibe un número de teléfono transmitido mediante CLIP y/o un código de identificación transmitido como contenido de la llamada o del mensaje de texto. Adicionalmente, el dispositivo de recepción 46 puede recibir instrucciones de mando 50 comprendidas en el contenido de la llamada o del mensaje de texto para el dispositivo de acceso a la red 22, o una dirección de red 88 de un dispositivo terminal 74 usado para establecer una conexión a través de la Internet. Para esto, el dispositivo de acceso a la red 22 en una llamada puede emplear, por ejemplo, un procedimiento de DTMF (Dual Tone Multiple Frequency) o un sistema de reconocimiento de voz.

Con una unidad de verificación 52 se verifica por lo menos una característica de identificación 48 recibida basándose en las características de identificación 56 almacenadas en una memoria de datos 54. La memoria de datos 54 está configurada como memoria de reescritura para la modificación de las características de identificación 56 almacenadas por parte del usuario. Durante la verificación, se comprueba la coincidencia entre por lo menos una característica de identificación 48 recibida y una característica de identificación 56 almacenada. En caso de una comprobación positiva por la unidad de verificación 52, un dispositivo de autorización 58 del dispositivo de acceso a la red 22 permite una conexión entrante desde la Internet 18 o el paso de los correspondientes paquetes de datos a través del cortafuegos 44. Para esto, el dispositivo de autorización 58 modifica el reglamento del cortafuegos 44. A este respecto se puede tomar en cuenta la dirección de red 88 del dispositivo terminal 74 transmitida opcionalmente.

Adicionalmente, en el dispositivo de acceso a la red 22 se provee un dispositivo de configuración 60 y una memoria de configuración 62. El dispositivo de configuración 60 determina las propiedades de conexión de una conexión autorizada a la Internet 18 y las actividades permitidas a través de la misma antes de la autorización. Como propiedades de conexión se pueden definir, por ejemplo, una duración máxima, un volumen de datos o una velocidad de transmisión de datos. Mediante la autorización de puertos, que se asignan a determinados procesos o aplicaciones, se pueden especificar las actividades posibles. El dispositivo de configuración 60 provee para esto los correspondientes parámetros operativos del dispositivo de acceso a la red 22 y del cortafuegos 44. Para la configuración de una conexión a ser autorizada, el dispositivo de configuración 60 usa los datos de configuración almacenados en la memoria de configuración 62 o transmitidos como instrucciones de mando 50. Los datos de configuración almacenados en la memoria de configuración 62 son definidos previamente por el usuario, por un operador de la red de telecomunicaciones 10, 14 o por el fabricante del dispositivo de acceso a la red 22.

Adicionalmente, el dispositivo de configuración 60, con los datos de configuración correspondientes causa la transmisión de la dirección de red estática o dinámicamente asignada 42 del dispositivo de acceso a la red 22 mediante mensaje de texto o correo electrónico a través de un módulo de transmisión de direcciones 64. A este respecto, como dirección de destino se puede usar un número de teléfono o una dirección de correo electrónico almacenada la memoria de configuración 62. Sin embargo, también es posible el uso de un número de teléfono o de una dirección de correo electrónico que se haya transmitido con la llamada o con el mensaje de texto para la autorización de una conexión a Internet.

A continuación se describe el modo de funcionamiento y la colaboración de los componentes previamente mencionados del dispositivo de acceso a la red 22 conjuntamente con un procedimiento ejemplar correspondiente para autorizar una conexión por medio de la red de datos pública con orientación de paquetes 18 a través del cortafuegos 44.

En primer lugar, por medio del cortafuegos 44 se bloquean todas las conexiones 70, o exceptuando sólo algunas pocas conexiones seguras, a través de la Internet 18 y una de las redes de telecomunicaciones 10, 14 al dispositivo de acceso a la red 22, cruz 72. El cortafuegos 44 reconoce los correspondientes paquetes de datos en la dirección de origen, la dirección de destino y el número de puerto y no permite el paso de estos paquetes de datos. De esta manera se obtiene una seguridad muy elevada contra accesos no autorizados desde la Internet 18.

Si el usuario o una persona autorizada ahora quiere tener acceso desde un dispositivo terminal con capacidad de Internet 74 a través de la Internet 18 y una red de telecomunicaciones 10, 14 al dispositivo de acceso a la red 22 o a un ordenador 38 conectado al mismo, o a una red de área local o a otro dispositivo terminal con capacidad de Internet, el cortafuegos 44 primero tendrá que permitirlo. Para esto, el usuario o la persona autorizada efectúan una llamada, flecha 78, con el dispositivo terminal de telefonía móvil 76 al dispositivo de acceso a la red 22 o envía un mensaje de texto 80 al dispositivo de acceso a la red 22. En ambos casos se usa para esto el número de teléfono 40 del dispositivo de acceso a la red 22. Alternativamente, la llamada o el envío del mensaje de texto también se pueden efectuar con un dispositivo terminal de red fija, no representado en la Fig. 1, para la red fija 14. Un número de teléfono 82 asignado al dispositivo de telefonía móvil 76 es transmitido en una llamada 78 a través de un procedimiento de CLIP o en el envío de un mensaje de texto 80 junto con el mensaje de texto 80 al dispositivo de acceso a la red 22. Algo equivalente rige también para el uso de un dispositivo terminal de red fija.

Con una llamada 78, el dispositivo de recepción 46 recibe el número de teléfono 82 del terminal de telefonía móvil 76 que efectúa la llamada, o de un dispositivo terminal de red fija mediante un procedimiento de CLIP, sin que se tenga que aceptar la llamada 78. Con un mensaje de texto 80, el dispositivo de recepción 46 recibe el número de teléfono 82 del remitente junto con el mensaje de texto 80.

En una primera alternativa de realización, la unidad de verificación 52 verificar la coincidencia del número de teléfono 82 o recibido con un número de teléfono almacenado en la memoria de datos 54 como característica de identificación almacenada 56. En caso de coincidencia, el dispositivo de autorización 58 libera el cortafuegos 44 para una conexión 84 desde el dispositivo terminal 74 al dispositivo de acceso a la red 22. Para esto, el número de teléfono 82 del dispositivo terminal de telefonía móvil 76 o de un dispositivo terminal de red fija usado para la autorización previamente tiene que haber sido almacenado por el usuario o por una persona autorizada en la memoria de datos 54. Por lo tanto, para la autorización sólo se puede usar un dispositivo terminal de telefonía móvil 76 o un dispositivo terminal de red fija previamente especificado. En la memoria de datos 54 también es posible almacenar varios números de teléfono 82 como características de identificación almacenadas 56 para diferentes dispositivos terminales. De esta manera se obtiene una elevada seguridad en una autorización.

Si el usuario desea efectuar una autorización desde cualquier dispositivo de telefonía móvil o de red fija, de acuerdo con una segunda alternativa de realización deberá transmitir un código de identificación 86, por ejemplo, un número PIN (número de identificación personal) o una contraseña junto con la llamada 78 o el mensaje de texto 80. El código de identificación 86 por su parte es recibido por el dispositivo de recepción 46 y transferido a la unidad de verificación 52. La unidad en de verificación 52 comprueba la coincidencia del código de identificación recibido 86 como característica de identificación 48 con un código de identificación almacenado en la memoria de datos 54 como característica de identificación almacenada 56. Si el resultado de la verificación es positivo, el dispositivo de autorización 58 libera el cortafuegos 44 para la conexión entrante 84. Por lo tanto, el uso de cualquier dispositivo terminal para una autorización es muy flexible y seguro.

En una tercera alternativa de realización, el dispositivo de recepción 46 recibe tanto el número de teléfono 82 como también el código de identificación 86 como características de identificación 48. La unidad de verificación 52 verifica la coincidencia del número de teléfono 82 y del código de identificación 86 con las características de identificación 56 almacenadas en la memoria de datos 54. Solamente si en ambos casos se obtiene un resultado de verificación positivo, el dispositivo de autorización 58 libera el cortafuegos 44 para la conexión entrante 84. De esta manera, también en el caso de un uso no autorizado del terminal de telefonía móvil 76 (por ejemplo, en caso de pérdida o robo) o de un dispositivo de red fija se asegura un alto grado de seguridad contra ataques procedentes de la Internet 18.

Antes de autorizarse la conexión 84, la misma es configurada por el dispositivo de configuración 60. Para esto se usan los ajustes previamente almacenados en la memoria de configuración 62 para el dispositivo de acceso a la red 22 y el cortafuegos 44. El almacenamiento de estos ajustes es realizado con el dispositivo de configuración 60 por el usuario o por otra persona autorizada. Opcionalmente, junto con la llamada 78 o el mensaje de texto 80 se pueden transmitir instrucciones de mando 50 para la conexión 84. Éstas son recibidas igualmente por el dispositivo de recepción 46 y transferidas al dispositivo de configuración 60. Por ejemplo, se puede especificar una duración, una velocidad de transmisión de datos o un volumen de datos de la conexión 84, una dirección de red 88 del dispositivo terminal 74 usado para la conexión 84 o un número de puerto permitido. Con la dirección de red 88 es posible limitar

la autorización de conexiones al dispositivo terminal 74 empleado. Junto con el número de puerto, frecuentemente se especifica también una aplicación asignada al respectivo puerto. Con semejante configuración de la conexión 84 se optimiza la protección contra ataques desde la Internet 18.

En caso de una autorización, es posible adicionalmente la transmisión de la dirección de red 42 del dispositivo de acceso a la red 22 por medio de un mensaje de texto 90 al dispositivo terminal de telefonía móvil 76 o a un dispositivo de red fija correspondiente. Alternativamente, esto también se puede realizar mediante un correo electrónico. Por lo tanto, también en el caso de una dirección de red 42 asignada de manera dinámica, y que por esta razón cambia con frecuencia, el establecimiento de la conexión 84 es posible sin problema alguno.

REIVINDICACIONES

1. Procedimiento para autorizar una conexión entrante (84), bloqueada en un principio por un cortafuegos (44), a través de una red de datos pública con orientación de paquetes (18) en el cortafuegos (44) de un dispositivo de acceso a la red (22), que por medio de por lo menos una red de telecomunicaciones (10, 14) permite establecer una conexión de datos con orientación de paquetes (84) a través de la red de datos pública (18) mediante una dirección de red (42) asignada al dispositivo de acceso a la red (22), así como telefonía por medio de un número de teléfono (40) asignado al dispositivo de acceso a la red (22) con las etapas de procedimiento

a) Recepción de una llamada (78) dirigida al número de teléfono (40) por una persona que hace la llamada, o de un mensaje de texto corto (80) dirigido al número de teléfono (40) por un remitente por medio de la red de telecomunicaciones (10) a través del dispositivo de acceso a la red (22), en donde con la llamada (78) o con el mensaje de texto corto (80) se transmite una característica de identificación (48) y
b) Verificación de la característica de identificación (48) por el dispositivo de acceso a la red (22),
c) Modificación de un reglamento en el cortafuegos (44) por un dispositivo de autorización (58) del dispositivo de acceso a la red (22) y autorización por el dispositivo de autorización (58) de una conexión (84) proveniente de la red de datos pública con orientación de paquetes (18), bloqueada en un principio por el cortafuegos (22), en caso de un resultado de verificación positivo de la característica de identificación (48).

2. Procedimiento de acuerdo con la reivindicación 1, **caracterizado por que** una coincidencia de la característica de identificación (48) transmitida se verifica con una característica de identificación (56) almacenada en el dispositivo de acceso a la red (22).

3. Procedimiento de acuerdo con la reivindicación 1 o la reivindicación 2, **caracterizado por que** como característica de identificación (48) se usa un número de teléfono (82) transmitido al dispositivo de acceso a la red (22) de la persona que hace la llamada o del remitente de un mensaje de texto corto (80).

4. Procedimiento de acuerdo con cualquiera de las reivindicaciones 1 a 3, **caracterizado por que** como característica de identificación (48) se usa un código de identificación (86) introducido por la persona que hace la llamada o por el remitente y transmitido a través de la llamada (78) o el mensaje de texto corto (80).

5. Procedimiento de acuerdo con cualquiera de las reivindicaciones 1 a 4, **caracterizado por que** con la característica de identificación (48) se transmite una dirección de red (88) de un dispositivo terminal (74) usado para la conexión (84) por medio de la llamada (78) o el mensaje de texto corto (80).

6. Procedimiento de acuerdo con cualquiera de las reivindicaciones 1 a 5, **caracterizado por** la especificación de propiedades de conexión antes de autorizarse la conexión (84).

7. Procedimiento de acuerdo con cualquiera de las reivindicaciones 1 a 6, **caracterizado por** la transmisión de instrucciones de mando (50) para el dispositivo de acceso a la red (22) a través de la llamada (78) o del mensaje de texto corto (80).

8. Procedimiento de acuerdo con cualquiera de las reivindicaciones 1 a 7, **caracterizado por que** la dirección de red (42) asignada del dispositivo de acceso a la red (22) después de autorizarse la conexión (84) es transmitida por medio de un módulo de transmisión de direcciones (64) en un correo electrónico o un mensaje de texto corto (90) a la persona que hace la llamada o al remitente.

9. Dispositivo de acceso a la red (22) que por medio de por lo menos una red de telecomunicaciones (10, 14) permite establecer una conexión de datos con orientación de paquetes (84) a través de una red de datos pública con orientación de paquetes (18) con una dirección de red (42) asignada al dispositivo de acceso a la red (22), así como telefonía con un número de teléfono (40) asignado al dispositivo de acceso a la red (22), en donde el dispositivo de acceso a la red (22) contiene

a) Un cortafuegos (44) para el bloqueo de conexiones (70) que provienen de la red de datos pública con orientación de paquetes (18),
b) Un dispositivo de recepción (46) para la recepción de una llamada (78) dirigida al número de teléfono (40) por una persona que hace la llamada o de un mensaje de texto corto (80) dirigido al número de teléfono (40) por un remitente, así como una característica de identificación (48) transmitida con la llamada (78) o con el mensaje de texto corto (80),
c) Una unidad de verificación (52) para verificar la característica de identificación (48) y
d) Un dispositivo de autorización (58) para modificar un reglamento en el cortafuegos (44) y para autorizar una conexión (84) proveniente de la red de datos pública con orientación de paquetes (18), bloqueada en un principio por el cortafuegos (44), en caso de un resultado de verificación positivo de la característica de identificación (48) por la unidad de verificación (52).

10. Dispositivo de acceso a la red (22) de acuerdo con la reivindicación 9, **caracterizado por que** se provee una memoria de datos (54) para almacenar una característica de identificación (56) que es usada por la unidad de verificación (52) para verificar la característica de identificación transmitida (48).

11. Dispositivo de acceso a la red (22) de acuerdo con las reivindicaciones 9 o 10, **caracterizado por que** el dispositivo de recepción (46) está configurado para recibir un número de teléfono (82) de la persona que hace la llamada o del remitente del mensaje de texto corto, transmitido al dispositivo de acceso a la red (22) como característica de identificación (48).

12. Dispositivo de acceso a la red (22) de acuerdo con cualquiera de las reivindicaciones 9 a 11, **caracterizado por que** el dispositivo de recepción (46) está configurado para recibir un código de identificación (86) introducido por la persona que hace la llamada o por el remitente y transmitido a través de la llamada (78) o el mensaje de texto corto (80) como característica de identificación (48).

13. Dispositivo de acceso a la red (22) de acuerdo con cualquiera de las reivindicaciones 9 a 12, **caracterizado por que** se provee un dispositivo de configuración (60) con una memoria de configuración (62) para especificar y almacenar propiedades de conexión antes de autorizarse la conexión (84).

14. Dispositivo de acceso a la red (22) de acuerdo con cualquiera de las reivindicaciones 9 a 13, **caracterizado por que** el dispositivo de recepción (46) está configurado para recibir instrucciones de mando (50) transmitidas por medio de la llamada (78) o el mensaje de texto corto (80) para el dispositivo de acceso a la red (22).

15. Dispositivo de acceso a la red (22) de acuerdo con cualquiera de las reivindicaciones 9 a 14, **caracterizado por** un módulo de transmisión de direcciones (64) para transmitir la dirección de red (42) asignada al dispositivo de acceso a la red (22) por medio de un correo electrónico o de un mensaje de texto corto (90) a la persona que hace la llamada o al remitente después de autorizarse la conexión (84).

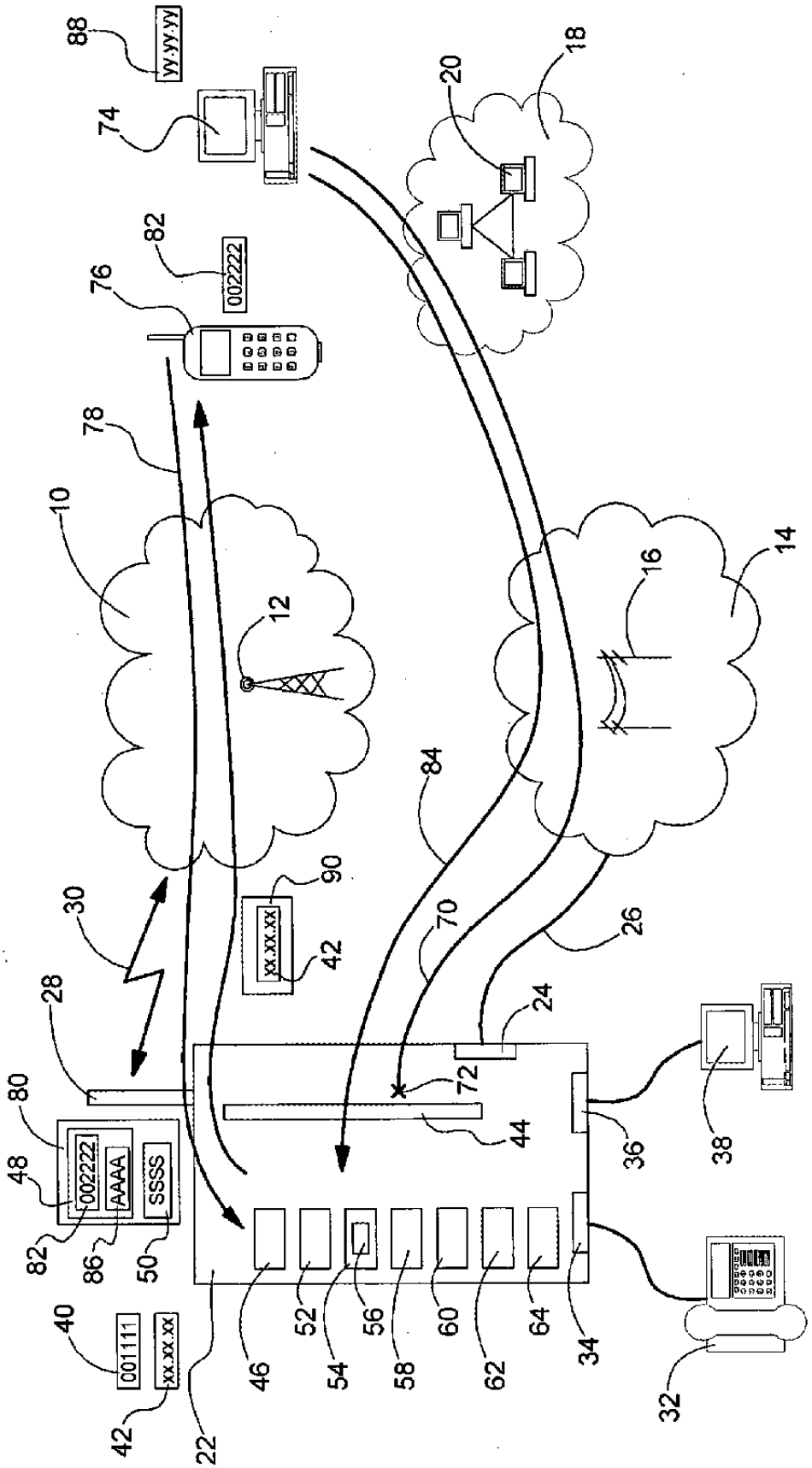
88
yy.yy.yy
74
18
20
82
002222
76
78
10
12
14
16
84
90
xx.xx.xx
42
30
70
26
28
24
72
80
48
002222
AAAA
SSSS
82
86
50
44
36
38
40
001111
xx.xx.xx
42
22
46
52
54
56
58
60
62
64
34
32

Fig. 1