(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 375 710**

(51) Int. CI.:
H04L 12/46 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **05292613 .6**
(96) Fecha de presentación: **08.12.2005**
(97) Número de publicación de la solicitud: **1672849**
(97) Fecha de publicación de la solicitud: **21.06.2006**

(54) Título: **PROCEDIMIENTO DE EXPLOTACIÓN DE UNA RED INFORMÁTICA LOCAL CONECTADA A UNA RED REMOTA PRIVADA MEDIANTE UN TÚNEL IPSEC.**

(30) Prioridad:
16.12.2004 FR 0413413

(45) Fecha de publicación de la mención BOPI:
05.03.2012

(45) Fecha de la publicación del folleto de la patente:
05.03.2012

(73) Titular/es:
FRANCE TELECOM
6 PLACE D'ALLERAY
75015 PARIS, FR

(72) Inventor/es:
Charles, Olivier;
Butti, Laurent y
Veysset, Franck

(74) Agente: **Pérez Barquín, Eliana**

DESCRIPCIÓN

Procedimiento de explotación de una red informática local conectada a una red remota privada mediante un túnel IPsec

La invención se refiere, de modo general, a la explotación de redes relacionadas entre sí, en particular de redes informáticas.

Más precisamente, la invención se refiere, según un primero de sus aspectos, a un procedimiento de explotación de una red local que incorpora un terminal local enlazado con una pasarela de una red remota mediante un túnel en modo de bloqueo, de manera tal que un flujo emitido por el terminal con destino a un equipo de la red local se encamina hacia la pasarela a través de dicho túnel.

Un procedimiento de este tipo queda descrito, por ejemplo, en la solicitud de patente US2003/182363.

Como sabe el experto en la materia, un enlace entre dos redes puede ser de tipo IP y puede estar constituido por la red Internet o por cualquier otra red que utiliza los protocolos de Internet.

Por otro lado, como sabe igualmente el experto en la materia, Internet utiliza un protocolo de seguridad conocido con la denominación "IPsec", que es el acrónimo obtenido del inglés "Internet Protocol Security".

La presente invención se refiere, en su principal aplicación concreta, a los ordenadores en situación de nomadismo cuando están conectados a una red privada de empresa mediante el protocolo IPsec. Es de aplicación particularmente adaptada cuando el nómada realiza teletrabajo, es decir, cuando está conectado desde su red doméstica (la red local de su domicilio) a la red remota privada de su empresa. El procedimiento, no obstante, sigue siendo operante para otros tipos de redes locales, como por ejemplo las zonas de conexión inalámbrica llamadas "hot spots wi-fi".

Por convención, la presente descripción utiliza los términos "terminal" o "terminal local" para designar el ordenador por el que el nómada se conecta a su red local y luego a la red remota privada del la empresa.

El término "equipo local" designa todo equipo informático conectado a la red local y al que es preciso dar acceso al terminal durante sus conexiones IPsec. Este equipo local podrá estar así constituido, de manera estadísticamente representativa, por una impresora, pero también podrá estar constituido por cualquier tipo de servidor de la red local (FTP, Telnet...) al que el terminal tendrá que tener acceso durante sus conexiones IPsec.

Los términos "encaminador", "encaminador local" y "encaminador doméstico" designan un equipo que está situado en la entrada de la red local (o doméstica, si se contempla al nómada como un teletrabajador) y cuyas funciones se definirán más precisamente con posterioridad.

El término "pasarela" y, particularmente, "pasarela IPsec", designa un equipo que está situado entre el terminal y la red remota privada de la empresa, que es el encargado en particular de dar fin a los túneles, particularmente a los túneles IPsec, procedentes de los terminales y cuyas funciones se definirán más precisamente con posterioridad. Éste puede estar situado en la frontera de la red remota y ser gestionado por la empresa o por un operador de redes de telecomunicaciones.

Por motivos de seguridad, la mayoría de las puestas en práctica del protocolo IPsec no permiten al terminal local acceder simultáneamente a la red local y a la red remota de la empresa. Sin esta prohibición, el terminal estaría en situación de "doble nexo" e interconectaría de este modo las dos redes, constituyendo una grave falla de seguridad.

Esta prohibición queda asegurada por un modo específico denominado "modo de bloqueo" y previsto en particular en el protocolo IPsec.

El modo de bloqueo es, por tanto, una técnica que permite evitar el doble nexo de un terminal local a la red remota accesible en IPsec (típicamente, la red privada de la empresa) y a la red local (típicamente la red doméstica). Para tal fin, el modo de bloqueo impide toda comunicación del terminal local al margen del túnel IPsec, lo que tiene como efecto el de limitar ampliamente los riesgos de ataques por rebote en el túnel IPsec (y, por tanto, hacia el sistema de información de la empresa).

Como el modo de bloqueo reviste el mayor interés para las empresas preocupadas por la seguridad, las políticas de seguridad de las empresas accesibles a distancia gracias a IPsec generalmente prevén activarlo por defecto.

En la práctica, el modo de bloqueo se pone en práctica en el soporte lógico IPsec del terminal y generalmente modifica la configuración de encaminamiento del cliente de manera que envía todos los paquetes hacia un camino por defecto que pertenece al plan de direccionamiento de la red remota de la empresa. Éste pone en práctica asimismo una función de filtrado de acceso (típicamente un cortafuegos personal) que impide toda comunicación

desde el exterior hacia el terminal.

La contrapartida de este funcionamiento de seguridad es que el terminal nómada, durante una conexión a una red remota (también llamada "intranet"), ya no puede acceder a las máquinas (equipos) que están presentes en la red local a la que está físicamente conectado. En particular, ya no tiene acceso a la impresora de su red local, puesto que todos los flujos de control y de datos son canalizados automáticamente por el túnel de bloqueo hacia la red remota de la empresa.

Una vía conocida a día de hoy para salvar este problema consiste en utilizar la técnica llamada de "túnel dividido" (o "split tunneling"), que ofrece al terminal local la posibilidad de direccionar directamente cualquier equipo de la red local pese a la existencia concomitante del túnel IPsec y, por tanto, de acceder a los servicios locales.

El problema está en que esta técnica hace que aparezca un serio riesgo de penetración pirata en la red remota de la empresa por rebote en el terminal, siendo fuertemente desaconsejado, e incluso prohibido, recurrir a esta técnica por la mayoría de los administradores de redes corporativas.

En este contexto, la presente invención tiene como objetivo, en particular, proponer un procedimiento que permite al terminal local direccionar un equipo local pese a la existencia concomitante de un enlace de este terminal con una pasarela IPsec a través de un túnel de bloqueo, funcionalidad esta que se obtiene sin degradación de la seguridad ofrecida por el túnel de bloqueo y sin modificación del terminal local ni del equipo local de interés ni, en particular, de la impresora.

Para este propósito, el procedimiento de la invención, por otro lado conforme a la definición genérica que le da el anterior preámbulo, está caracterizado esencialmente porque comprende una operación de reenvío, puesta en práctica en la pasarela, de un flujo emitido por el terminal, encaminado a través de dicho túnel y no destinado a dicha red remota, consistente en reenviar el flujo en cuestión hacia un encaminador perteneciente a la red local, a efectos de la redirección del flujo en cuestión por parte de dicho encaminador hacia un equipo de la red local al que está destinado el flujo en cuestión, identificándose dicho encaminador a partir de una información obtenida por la pasarela en el establecimiento del túnel.

Si bien la solicitud de patente US2004/177157 describe un procedimiento de gestión de direcciones, esta solicitud no enseña la redirección de un flujo de datos hacia un equipo de una red local.

La operación de reenvío puede incluir, por ejemplo, la recepción de dicho flujo por un encaminador de la red local y el encaminamiento automático de dicho flujo por parte de dicho encaminador hacia dicho equipo.

La operación de reenvío puede incluir asimismo el análisis de los flujos por parte de la pasarela al objeto de reconocer un flujo no destinado a dicha red remota.

La invención, en una definición particular y muy detallada, puede adoptar así la forma de un procedimiento de explotación de una red informática local en una configuración que comprende, además de esa red local,

- una red informática remota privada a la que está conectada la red local a través de una red de enlace de tipo IP,

- un encaminador local dispuesto en la interfaz entre la red local y la red de enlace, y

- una pasarela IPsec dispuesta en la interfaz entre la red remota y la red de enlace,

comprendiendo la red local al menos un terminal local y un equipo informático local y estando enlazado el terminal con la pasarela IPsec mediante un túnel IPsec en modo de bloqueo,

permitiendo este procedimiento el reencaminamiento automático, hacia la pasarela y a través del túnel en modo de bloqueo, de un flujo de control y/o de datos proveniente del terminal con destino al equipo local, y comprendiendo para tal fin:

- una operación de análisis, puesta en práctica en la pasarela a la recepción por parte de ella de un flujo de control y/o de datos proveniente del terminal con destino al equipo local y consistente en reconocer que ese flujo no está destinado a la red remota,

- una operación de reenvío puesta en práctica en la pasarela y consistente en reenviar hacia el encaminador local el flujo de control y/o de datos proveniente del terminal y

- una operación de encaminamiento automático, puesta en práctica en el encaminador local y consistente en encaminar automáticamente hacia dicho equipo local el flujo de control y/o de datos procedente del terminal local y reenviado por la pasarela hacia el encaminador local.

En el caso en que el encaminador local, al que se asigna una dirección encaminable, sustituye una dirección del terminal interna a la red local por su propia dirección encaminable en una petición de conexión a la red remota privada proveniente del terminal con destino a la pasarela y en que la pasarela IPsec asigna al terminal local una dirección interna a la red remota en el establecimiento del túnel de bloqueo, el procedimiento puede comprender además una operación de correlación puesta en práctica en la pasarela en el establecimiento del túnel de bloqueo y consistente en memorizar una tabla de consulta que establece una correspondencia mutua entre la dirección encaminable del encaminador local y la dirección del terminal interna a la red remota, utilizando la operación de reenvío del flujo de control y/o de datos la tabla de consulta y consistiendo ésta en reenviar hacia la dirección encaminable del encaminador local el flujo de control y/o de datos proveniente del terminal identificado mediante la dirección interna a la red remota.

La operación de encaminamiento automático preferentemente se pone en práctica mediante una técnica de traducción de puerto.

El flujo de control y/o de datos puede comprender por ejemplo un mandato de impresión.

El procedimiento puede comprender una operación suplementaria, puesta en práctica por la pasarela, y consistente en establecer un segundo túnel, de tipo IPsec o SSL, que enlaza esta pasarela con el encaminador local.

Como variante, la operación puesta en práctica por la pasarela puede consistir en establecer un segundo túnel, de tipo IPsec o SSL, que enlaza esta pasarela con el equipo local, en el presente caso constituido por una impresora.

Por otro lado, el procedimiento de la invención puede comprender una operación puesta en práctica por el encaminador local y consistente en reservar a la pasarela el acceso al equipo local, en el presente caso constituido por una impresora.

La invención se refiere asimismo a un módulo de soporte lógico que comprende instrucciones que, una vez cargado este módulo en una pasarela IPsec, ponen en práctica al menos la operación de correlación del procedimiento tal y como se ha definido anteriormente, pudiendo además estas instrucciones poner en práctica la operación de análisis y la operación de reenvío de este procedimiento.

Aún se refiere la invención a una pasarela IPsec para una red remota, comprendiendo esta pasarela un módulo de soporte lógico tal y como se ha definido anteriormente.

Otras características y ventajas de la invención se desprenderán claramente de la descripción que de ella se hace a continuación, a título indicativo y sin carácter limitativo alguno, haciendo referencia a la figura única, que representa esquemáticamente la arquitectura y los medios puestos en práctica en la invención.

Como se ha indicado anteriormente, la invención se refiere en particular a un procedimiento de explotación de una red informática local RES_L, por ejemplo una red doméstica, en la configuración representada en la figura y comprendiendo, además de esta red local RES_L, una red informática remota privada RES_D, por ejemplo una red o "intranet" corporativa, un encaminador local ROUT_L y una pasarela IPsec PASS_D, comprendiendo la propio red local RES_L al menos un terminal local T_L y un equipo informático local E_L tal como una impresora o un servidor adaptado a cualquier tipo de servicio doméstico por IP al que el terminal T_L tiene que poder acceder permanentemente, por ejemplo FTP, Telnet, etc.

El terminal T_L está configurado con una lista de periféricos E_L, tal como impresoras en las que puede iniciar impresiones y, en particular, la impresora de la red local. Éste pone en práctica asimismo el protocolo IPsec para conectarse a la pasarela IPsec PASS_D.

Se supone que el soporte lógico IPsec tan sólo funciona en modo de bloqueo y, por tanto, que no autoriza los túneles divididos (split tunneling).

El encaminador local ROUT_L, que está situado en la entrada de la red local RES_L, cumple varias funciones, a saber:

- establecer la conexión física (RNIS, cable, XDSL...) del terminal T_L con Internet;

- aceptar las comunicaciones de los diferentes equipos E_L de la red local RES_L (PC, impresora, escáner, decodificadores...); generalmente estas conexiones se hacen por Ethernet alámbrico o inalámbrico ([IEEE802.11]);

- traducir las direcciones internas ([RFC1918]) del terminal T_L y de los equipos E_L a una dirección encaminable; si, por ejemplo, el terminal T_L y una impresora E_L tienen en la red local RES_L unas respectivas direcciones internas ad_1 y ad_2, el encaminador ROUT_T traduce, en una conexión por Internet, estas direcciones internas a la dirección encaminable AD_1 que es la que este encaminador ha obtenido en su conexión a la red del proveedor de acceso a Internet. Este procedimiento de traducción es conocido por el experto en la materia con el nombre de

NAT/NAPT (Network Address Translation, Network Address Port Translation), [RFC3022]. Consiste en mantener una tabla de consulta entre los pares (dirección IP interna, número de puerto interno) y los pares (dirección IP externa, número de puerto externo). Para cada paquete de información direccionado al encaminador ROUT_L o emitido por él, la traducción se efectúa según esta tabla; y

- poner en práctica una técnica de traducción de puerto (conocida por el experto en la materia con el nombre de "port forwarding"), que consiste en definir estáticamente una asociación entre un puerto externo del encaminador y un puerto interno de ese encaminador, y que permite a las máquinas externas a la red local RES_L acceder a servidores internos a esa red local consultándolos sobre números de puertos conocidos por el encaminador.

La pasarela IPsec PASS_D, que está situada entre el terminal T_L y la red RES_D de la empresa, es la encargada de terminar los túneles IPsec procedentes de los terminales. Ésta posee funciones de encaminamiento de los paquetes y por tanto está abierta a Internet por una interfaz y a la red privada RES_D por otra interfaz.

La pasarela PASS_D, a la que por ejemplo se adscribe una dirección encaminable AD_2, adscribe al terminal T_L una dirección ad_3 interna a la red remota RES_D en el establecimiento del túnel IPsec de bloqueo entre este terminal y esta pasarela.

Además de las pasarelas IPsec convencionales, la pasarela de la invención incorpora un módulo de soporte lógico MTI que ofrece al terminal T_L un acceso al equipo E_L o a los equipos locales de la red RES_L, de un modo que es específico de la invención y que se describirá con mayor detalle posteriormente.

La puesta en práctica del procedimiento de la invención se fundamenta en los siguientes supuestos.

La red local RES_L utiliza un plan de direccionamiento llamado "privado", es decir, conforme a la norma RFC1918. Esto corresponde de hecho a la elección que por defecto hacen los fabricantes de encaminadores domésticos ROUT_L; esta red pone en práctica un servidor DHCP que asigna direcciones IP en un intervalo de direcciones "privadas".

La red remota RES_D, por ejemplo la red de la empresa, no utiliza el mismo direccionamiento de subred que el utilizado en la red doméstica RES_L. En todo caso, si existe tal solape, la ambigüedad en lo que respecta a la red solicitada es despejada con la toma en cuenta del origen de la petición.

Por ejemplo, si la red 10.0.0.X es utilizada a la vez en la empresa y en la red doméstica, entonces:

- si es una máquina de la red corporativa RES_D la que envía un paquete a la dirección 10.0.0.3, entonces el equipo destinatario es una máquina de la red corporativa RES_D, y

- si es una máquina de la red local RES_L la que envía un paquete a la dirección 10.0.0.3, entonces el equipo destinatario es una máquina de la red local RES_L.

La pasarela IPsec PASS_D puede hacer esta distinción por cuanto que está en conocimiento de los dos planes de direccionamiento y que está al corte entre las dos redes.

El procedimiento de la invención se base en los siguientes principios.

La pasarela IPsec PASS_D es el encaminador por defecto de todos los terminales T_L de las redes domésticas tales como RES_L. Así, cuando un terminal T_L va a ordenar por ejemplo un trabajo de impresión en su impresora local E_L, la orden de impresión será enviada sistemáticamente hacia la pasarela IPsec PASS_D, puesto que no se puede establecer comunicación con la impresora E_L a causa del túnel establecido en modo de bloqueo entre el terminal T_L y la pasarela PASS_D. Este comportamiento es el comportamiento normal de una pila IP porque el modo de bloqueo IPsec modifica la tabla de encaminamiento del cliente forzando a todos los paquetes a ir hacia la red corporativa RES_D.

La pasarela IPsec PASS_D, cuando ve llegar paquetes IP direccionados por el terminal T_L al equipo local E_L identificado mediante su dirección interna ad_2, comprueba que no puede encaminarlos por la red corporativa RES_D. En efecto, habida cuenta de los anteriores supuestos, la dirección ad_2 de destino solicitada no pertenece a la red RES_D de la empresa o cuando menos, un terminal doméstico T_L no tiene ningún motivo para solicitar tal dirección. Por donde la pasarela PASS_D deduce entonces que tiene que reenviar los paquetes hacia la red doméstica RES_L.

Para poder reencaminar ese tráfico, la pasarela PASS_D necesita saber sin embargo hacia qué encaminador doméstico ROUT_L tiene que serlo.

De acuerdo con la invención, esta información es construida por el módulo de soporte lógico MTI, en el momento del montaje del túnel IPsec previamente establecido entre el terminal T_L y la pasarela IPsec PASS_D.

En efecto, en el establecimiento de este túnel IPsec, y a causa del mecanismo de NAT puesto en práctica en el encaminador doméstico ROUT_L, la dirección pública AD_1 de este encaminador es la que se ha utilizado en el establecimiento del túnel IPsec.

A raíz de ello, la pasarela IPsec PASS_D ha asignado al terminal T_L una dirección interna ad_3 del plan de direccionamiento de la empresa. La pasarela IPsec PASS_D conoce por tanto el enlace entre la dirección ad_3 del terminal T_L en el plan de dirección interna de la empresa y la dirección pública AD_1 del encaminador doméstico ROUT_L, teniendo en particular como función el módulo de soporte lógico MTI el mantener un registro de esta correspondencia.

Consecuentemente, la pasarela IPsec PASS_D, cuando recibe paquetes IP provenientes del terminal nómada T_L y tiene que reenviar esos paquetes hacia la red doméstica RES_L, conoce perfectamente la dirección pública AD_1 del encaminador doméstico ROUT_L.

El encaminador doméstico ROUT_L convencionalmente pone en práctica un mecanismo de traducción de puerto (o "port forwarding"), de modo que es capaz, cuando recibe conexiones desde Internet por un puerto particular, de hacer una traducción de dirección hacia un equipo local E_L interno en un número de puerto particular. Por ejemplo en este punto, todos los paquetes recibidos provenientes de Internet y en el puerto de impresión correspondiente a la dirección ad_2 pueden ser directamente retransmitidos por el puerto de la impresora interna E_L.

Esta técnica puede ser utilizada con todos los protocolos de impresión existentes, en particular IPP descrito a continuación.

Se han definido nuevos estándares en el ámbito de trabajos en el IETF, en el presente caso en el grupo de trabajo PWG (the Printer Working Group [IETF-IPP]), donde el protocolo IPP (Internet Printing Protocol, [RFC 2910], [RFC 2911]) especifica ampliaciones al protocolo HTTP/1.1 y ofrece, por tanto, soluciones modernas y eficientes de impresión local y remota.

Un estado de la técnica de los protocolos de impresión está disponible en el sitio Internet http://www.cups.org/overview.html.

Uno de los protocolos más utilizados actualmente es el protocolo IPP anteriormente referido, ya que en particular es soportado por una mayoría de equipos. Su funcionamiento es simple, por ser muy cercano al protocolo HTTP. Funciona como este último según una modalidad cliente-servidor, accediendo el cliente a la impresora remota generalmente por el puerto 80/TCP.

El contenido funcional del módulo de soporte lógico MTI de tratamiento de las peticiones de impresión y de la pasarela IPsec PASS_D en la que está cargado este módulo se describirá ahora con mayor detalle.

El terminal T_L, cuando monta su túnel IPsec, participa en un intercambio IKE (RFC2409) con la pasarela IPsec PASS_D, durante el cual la pasarela IPsec recibe paquetes IP cuya dirección de origen es la dirección IP pública del encaminador doméstico ROUT_L, es decir, AD_1.

En efecto, al atravesar el encaminador ROUT_L, la dirección AD_1 de este encaminador pasa a sustituir sistemáticamente a la dirección interna ad_1 del terminal T_L.

La pasarela IPsec PASS_D asigna al terminal T_L una dirección IP dinámica, señalada con ad_3, que pertenece al plan de direccionamiento de la red RES_D de la empresa.

La pasarela IPsec, que conoce la dirección pública AD_1 del encaminador ROUT_L de la red local RES_L y la dirección ad_3 asignada dinámicamente al terminal T_L, envía al módulo MTI un mensaje de actualización de la tabla de consulta que asocia estas dos direcciones.

A la recepción del mensaje de actualización de la tabla de consulta con las direcciones AD_1 y ad_3, el módulo de soporte lógico MTI realiza la actualización de la tabla.

El terminal T_L, cuando inicia un trabajo de impresión, elige como impresora de destino la impresora E_L de la red local RES_L, al igual que haría en una situación más simple en la que no hay establecido ningún túnel IPsec.

Por motivo del modo de bloqueo del túnel IPsec, el flujo de control y de datos proveniente del terminal T_L con destino a la impresora E_L es canalizado por el túnel hacia la pasarela IPsec PASS_D.

La pasarela IPsec PASS_D, cuando ve llegar ese tráfico encaminado a través del túnel IPsec y con destino a una máquina cuya dirección ad_2 pertenece a una red que no es la red RES_D de la empresa, pregunta al módulo de soporte lógico MTI hacia qué encaminador doméstico redirigir ese tráfico. Para tal fin, la pasarela PASS_D indica al

módulo MTI la dirección del terminal T_L tal como es visto en la red RES_D de la empresa, es decir, con la dirección ad_3 que se le ha asignado en el intercambio IKE.

El módulo MTI consulta la tabla de consulta y, a partir de la dirección ad_3 del terminal T_L, deduce la dirección pública AD_1 del encaminador doméstico ROUT_L.

La pasarela IPsec actualiza su tabla de encaminamiento con este nuevo destino y transmite la orden de impresión al encaminador doméstico ROUT_L. Dicho de otro modo, la pasarela PASS_D realiza entonces el relevo de todos los paquetes recibidos hacia la dirección IP pública, es decir, AD_1, del encaminador doméstico ROUT_L.

Cuando recibe este flujo, el encaminador doméstico lo redirige hacia la impresora E_L gracias al mecanismo de traducción de puerto ("port forwarding").

Cuando el terminal T_L cierra la sesión IPsec, o cuando la pasarela IPsec PASS_D detecta que el terminal T_L está desconectado, esta última pide al módulo MTI que elimine de su tabla la entrada que corresponde al terminal T_L y también purga de su tabla de encaminamiento la línea correspondiente a este terminal.

Como comprenderá el experto en la materia con la lectura de cuanto antecede, el procedimiento de la invención permite obviar el mecanismo de túnel dividido (o "split tunneling") ofreciendo al propio tiempo la posibilidad de entrar en contacto con máquinas locales pertenecientes a la red RES_L del terminal T_L, y todo ello de manera perfectamente segura. Éste no abre ninguna brecha en la seguridad de la red de la empresa.

Este procedimiento no obliga a modificación o configuración alguna ni sobre la impresora E_L, ni sobre el encaminador doméstico ROUT_L, ni sobre el terminal T_L.

Además, permite contar con las funciones avanzadas de las impresoras, puesto que los parámetros de la impresora local siguen siendo válidos, aun si la impresión pasa por la red RES_D de la empresa.

En lugar de pasar sin encriptar por Internet, el flujo circulante desde la pasarela IPsec PASS_D hacia la red doméstica RES_L puede estar protegido contra las escuchas mediante otro túnel IPsec establecido entre esta pasarela y el encaminador ROUT_L. Este túnel se monta a iniciativa de la pasarela IPsec cuando ésta desea reencaminar un flujo hacia la red doméstica RES_L. En tal caso, el encaminador doméstico tiene que estar configurado de forma que acepte el montaje del túnel sin la intervención del usuario.

El flujo circulante desde la pasarela IPsec PASS_D hacia la red doméstica RES_L también puede estar protegido contra las escuchas mediante un túnel SSL establecido entre la pasarela IPsec y la impresora E_L, en el caso en que esta impresora tenga la capacidad de dialogar por SSL. Por tanto, en la presente invención se puede sacar partido de esta funcionalidad.

En ambos casos, ello permite proteger la red doméstica RES_L de las intrusiones autenticando la pasarela IPsec, y garantizar la confidencialidad de los datos intercambiados gracias al cifrado.

Finalmente, como la mayoría de los encaminadores domésticos ROUT_L habilitan la implantación de reglas de cortafuegos básico (firewall simple), es posible implantar una regla estática de forma que se reserve a la pasarela IPsec PASS_D el acceso a la impresora E_L (a través del mecanismo de traducción de puerto), lo cual aporta un nivel de seguridad superior protegiendo la red local RES_L.

REIVINDICACIONES

1. Procedimiento de explotación de una red local (RES_L) que incluye un terminal local (T_L) enlazado con una pasarela (PASS_D) de una red remota (RES_D) mediante un túnel en modo de bloqueo, de manera tal que un flujo emitido por el terminal (T_L) con destino a un equipo (E_L) de la red local (RES_L) se encamina hacia la pasarela (PASS_D) a través de dicho túnel, caracterizado porque comprende:

- una operación de reenvío, puesta en práctica en la pasarela (PASS_D), de un flujo emitido por el terminal (T_L), encaminado a través de dicho túnel y no destinado a dicha red remota, consistente en reenviar el flujo en cuestión hacia un encaminador (ROUT_L) perteneciente a la red local, a efectos de la redirección del flujo en cuestión por parte de dicho encaminador hacia un equipo de la red local al que está destinado el flujo en cuestión, identificándose dicho encaminador (ROUT_L) a partir de una información obtenida por la pasarela (PASS_D) en el establecimiento del túnel.

2. Procedimiento según la reivindicación 1, caracterizado porque la operación de reenvío incluye:

- la recepción de dicho flujo por dicho encaminador (ROUT_L),

- el encaminamiento automático de dicho flujo por parte de dicho encaminador (ROUT_L) hacia dicho equipo (E_L).

3. Procedimiento según una cualquiera de las reivindicaciones precedentes, caracterizado porque la operación de reenvío incluye:

- el análisis de los flujos por la pasarela (PASS_D) al objeto de reconocer un flujo no destinado a dicha red remota (RES_D).

4. Procedimiento según una cualquiera de las reivindicaciones 1 a 3, en el que el encaminador local (ROUT_L), al que se asigna una dirección encaminable (AD_1), sustituye una dirección (ad_1) del terminal (T_L) interna a la red local por su propia dirección encaminable (AD_1) en una petición de conexión a la red remota privada (RES_D) proveniente del terminal (T_L) con destino a la pasarela (PASS_D) y en el que la pasarela (PASS_D) asigna al terminal local una dirección (ad_3) interna a la red remota (RES_D) en el establecimiento del túnel de bloqueo, comprendiendo además este procedimiento una operación de correlación puesta en práctica en la pasarela (PASS_D) en el establecimiento del túnel de bloqueo y consistente en memorizar una tabla de consulta que establece una mutua correspondencia entre la dirección encaminable (AD_1) del encaminador local y la dirección (ad_3) del terminal interna a la red remota, utilizando la operación de reenvío del flujo la tabla de consulta y consistiendo ésta en reenviar hacia la dirección encaminable (AD_1) del encaminador local el flujo proveniente del terminal (T_L) identificado mediante la dirección (ad_3) interna a la red remota.

5. Procedimiento según una cualquiera de las reivindicaciones precedentes combinada con la reivindicación 2, caracterizado porque la operación de encaminamiento automático se pone en práctica mediante una técnica de traducción de puerto.

6. Procedimiento según una cualquiera de las reivindicaciones 1 a 5, caracterizado porque el flujo reenviado comprende un mandato de impresión.

7. Procedimiento según una cualquiera de las reivindicaciones precedentes combinada con la reivindicación 2, caracterizado porque comprende una operación puesta en práctica por la pasarela (PASS_D) y consistente en establecer un segundo túnel, de tipo IPsec o SSL, que enlaza esta pasarela (PASS_D) con el encaminador local (ROUT_L).

8. Procedimiento según una cualquiera de las reivindicaciones 1 a 6, caracterizado porque comprende una operación puesta en práctica por la pasarela (PASS_D) y consistente en establecer un segundo túnel, de tipo IPsec o SSL, que enlaza esta pasarela (PASS_D) con el equipo local (E_L, ad_2), constituido por una impresora.

9. Procedimiento según una cualquiera de las reivindicaciones precedentes combinada con la reivindicación 2, caracterizado porque comprende una operación puesta en práctica por el encaminador local (ROUT_L) y consistente en reservar a la pasarela (PASS_D) el acceso al equipo local (E_L, ad_2), constituido por una impresora.

10. Módulo de soporte lógico (MTI), caracterizado porque comprende instrucciones que, una vez cargado este módulo en una pasarela (PASS_D) de una red remota, ponen en práctica al menos la operación de reenvío del procedimiento según una cualquiera de las reivindicaciones 1 a 9.

11. Pasarela para una red remota, caracterizada porque comprende un módulo de soporte (MTI) según la reivindicación 10.

12. Pasarela según la reivindicación 11, caracterizada porque la pasarela es una pasarela (PASS_D) IPsec.

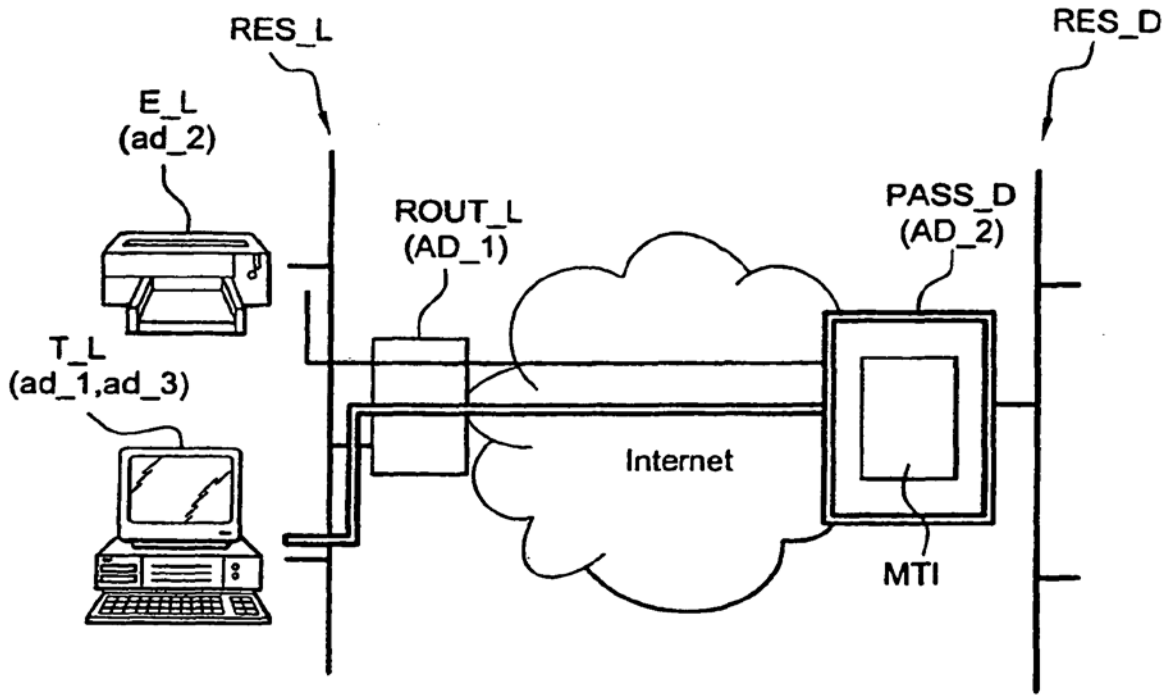

Figura única