(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 368 745**

(51) Int. CI.:
H04L 12/28 (2006.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **06701277 .3**
(96) Fecha de presentación: **23.01.2006**
(97) Número de publicación de la solicitud: **1977559**
(97) Fecha de publicación de la solicitud: **08.10.2008**

(54) Título: **ACCESO A RED DE COMUNICACIÓN.**

(45) Fecha de publicación de la mención BOPI:
21.11.2011

(45) Fecha de la publicación del folleto de la patente:
21.11.2011

(73) Titular/es:
Telefonaktiebolaget LM Ericsson (publ)
16483 Stockholm, SE

(72) Inventor/es:
ARKKO, Jari;
RINTA-AHO, Teemu y
MELÉN, Jan

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

DESCRIPCIÓN

Acceso a red de comunicación

Campo de la invención

La presente invención se refiere a un procedimiento y a un aparato para facilitar el acceso a una red de comunicación. La invención es aplicable, en particular, aunque no necesariamente, para facilitar el acceso a una red de comunicación a través de una red de acceso inalámbrico.

Antecedentes

Las redes de acceso inalámbrico permiten a los usuarios móviles acceder a los servicios ofrecidos por una variedad de redes de comunicación. Un buen ejemplo de dicha red de comunicación es Internet. Otro ejemplo es una red telefónica. En la actualidad, las redes de acceso inalámbrico usadas más ampliamente son las redes de acceso por radio de teléfonos celulares, tales como las proporcionadas por los operadores de redes GSM y 3G. Estas redes de acceso están disponibles al público en la medida en que cualquiera que tenga una suscripción válida (incluyendo cuentas de pre-pago) puede hacer uso de la red de acceso. También hay disponibles otros tipos de redes de acceso inalámbrico. Por ejemplo, la introducción de redes WLAN en cafés, bibliotecas, aeropuertos, etc., permite a los usuarios móviles hacer uso de los servicios WLAN de forma gratuita o por un módico precio.

Resumen

El número de redes de acceso inalámbrico que podrían ser usadas por los usuarios móviles itinerantes es mucho mayor que el número que se usa realmente. Considérese, por ejemplo el gran número de WLANs domésticas y corporativas que están, actualmente, cerca de usuarios que no "pertenecen" a los hogares o a las empresas en las que residen las WLAN, pero que ofrecen unas capacidades y unas velocidades relativamente altas. Estas están cerradas por una serie de razones, incluyendo:

- Un propietario de una red privada no quiere permitir que otros se aprovechen de su inversión o, peor aún, permitir que otros incurran en gastos para el propietario de la red privada;
- Con el fin de asegurar que hay disponible una capacidad de red suficiente para los usuarios domésticos/usuarios de la empresa;
- Para asegurar que la red de acceso no es usada para propósitos ilegales, y
- Razones técnicas que hacen que el acceso público a las redes privadas sea poco práctico.

Como ejemplo de una dificultad técnica, podría considerarse una red privada que requiere que los usuarios sean autenticados a la misma, en cuyo caso puede ser necesario configurar una clave en los terminales móviles itinerantes. Particularmente en el caso de redes domésticas, esto no es algo que el propietario de la casa (por ejemplo, una familia) o los usuarios móviles desearían hacer (de manera regular). Por supuesto, podría ser posible permitir a los operadores de redes privadas participar en los consorcios de itinerancia existentes y ser equipados con la tecnología necesaria (en base, por ejemplo al estándar de autenticación y autorización y contabilidad (AAA)). Sin embargo, en la práctica, esto es poco realista, debido a una serie de limitaciones técnicas y de otro tipo, concretamente:

- El establecimiento de conexiones AAA es exigente incluso para los expertos, no digamos ya para el público en general. Los protocolos existentes requieren un acuerdo sobre un gran número de parámetros, particularmente cuando se usa RADIUS [IETF RFC2865].
- Las características de los sistemas AAA no los hacen adecuados para conexiones de itinerancia a gran escala entre múltiples niveles de actores [problema l-D.ietf-eap-netsel]. Por ejemplo, se echa en falta un mecanismo de enrutamiento automático que fuerce un enrutamiento de transacciones dentro de la red de proveedores interconectados para ser configurados manualmente.
- Los requisitos comerciales para la aceptación en un consorcio de itinerancia (o ser capaz de proporcionar "peering" sobre AAA) son demasiado altos para la mayoría de redes privadas. Es poco probable que un proxy AAA de una red privada obtuviera permiso para conectarse a la red AAA de un proveedor principal, por ejemplo.

Cualquier solución que facilite un acceso externo a una red de comunicación a través de una red privada debería cumplir los requisitos siguientes:

- Dicho servicio de red debería ser establecido automáticamente, es decir, sin la participación del propietario o de los usuarios (quizás con la excepción de activar la característica).
- Deberían soportarse diferentes modelos de negocio y compensación, en caso de que los operadores de las redes privadas requieran una compensación.

- La solución debería acomodar el seguimiento de actividades ilegales en un grado similar a las soluciones de acceso a Internet existentes, desplegadas comercialmente.

- La solución debería ser adecuada tanto para soluciones de salto único como para soluciones multi-salto, es decir, la entidad que proporciona acceso a red puede estar conectada directamente a una red de acceso público real o accede a través de alguna otra red o redes privadas.

Según un primer aspecto de la presente invención, se proporciona un procedimiento de enrutamiento de tráfico entre usuarios externos y una red de comunicación, a través de una red de acceso privado, comprendiendo el procedimiento:

establecer un túnel exterior seguro entre la red privada y una pasarela de una red de acceso público a la que está acoplada la red privada;

en base a la autenticación de la red privada a la red de acceso público, acoplando dicha pasarela a dicha red de comunicación;

para cada usuario externo que desea conectarse a la red de comunicación a través de la red privada, establecer un túnel interior seguro entre el usuario externo y la pasarela en base a la autenticación del usuario externo a la pasarela, estando el túnel interior dentro de dicho túnel exterior;

hacer que el tráfico fluya entre los usuarios externos y la pasarela a través de los túneles interiores respectivos;

dentro de dicha red de acceso público, usar dichos túneles interiores y exteriores para determinar una cantidad de tráfico exterior enrutado entre los usuarios externos e Internet por medio de la red de acceso privado; y

aplicar una compensación apropiada a un operador de dicha red de acceso privado dependiendo de dicha cantidad determinada de tráfico exterior.

El término "usuarios externos" abarca un rango de entidades, incluyendo pero no limitándose a, dispositivos, suscriptores que utilizan uno o más dispositivos, y tarjetas SIM/USIM usadas en uno o más dispositivos.

Las realizaciones de la invención permiten a la red de acceso público de la red privada determinar exactamente qué tráfico asociado con los usuarios externos es enrutado a través de la red privada. Esto permite a la red de acceso público, por ejemplo, asignar un crédito monetario apropiado, u otra bonificación, al operador de la red privada. Por otro lado, la red de acceso público es capaz de determinar la identidad del usuario externos asociado con un tráfico particular en base al propietario del túnel interior a través del cual se realiza ese tráfico.

El papel de la red privada es hacer que el tráfico recibido desde un usuario externo fluya a través del túnel exterior. Esto implica encapsular el tráfico recibido según los procedimientos de seguridad del túnel exterior. De manera similar, la red privada desencapsula el tráfico que llega desde la pasarela y que está destinado para un usuario externo. Por otro lado, la pasarela encapsula y desencapsula según ambos túneles interior y exterior, mientras que el usuario externo encapsula y desencapsula sólo según el túnel interior.

En algunas realizaciones de la invención, el túnel exterior lleva sólo el tráfico que viaja a través de los túneles interiores. Otras realizaciones pueden permitir que la red privada envíe su propio tráfico a través del túnel exterior, no dentro de un túnel interior. En este caso, la pasarela reconocerá que este tráfico pertenece a la red privada, ya que no es transportado a través de un túnel interior.

La red de comunicación a la que la red privada facilita el acceso puede ser Internet.

La red de acceso público de la red privada puede ser una línea fija o una red de telecomunicación celular.

Preferentemente, dichos túneles interior y exterior son túneles IPSec, definidos por IKE SAs, negociados entre la red privada y una pasarela de la red de acceso público y entre los usuarios externos y esa pasarela.

La autenticación de un usuario externo a una pasarela puede realizarse dentro de dicha red de acceso público, o puede implicar que la red de acceso público se comunica con una red adicional, donde el usuario es un abonado de esa red adicional.

En su forma más simple, la red privada es un solo nodo conectado a la red de acceso público a través de una conexión inalámbrica o por cable. La red privada puede consistir también en un conjunto de nodos, conectados internamente, sobre enlaces inalámbricos o por cable.

La invención es aplicable, en particular, a redes inalámbricas privadas. La red privada puede ser una red WLAN, por ejemplo, doméstica o corporativa, o una red proporcionada por un único dispositivo que tiene conectividad inalámbrica. A los usuarios externos que tienen una conectividad inalámbrica apropiada se les permite itinerar entre las redes inalámbricas privadas y las redes inalámbricas públicas, tales como redes GSM y 3G.

Dicha pasarela puede ser configurada para rechazar solicitudes de establecimiento de túneles seguros con usuarios externos que no pasarán a través de dicho túnel externo.

Según un segundo aspecto de la presente invención, se proporciona una pasarela para controlar el acceso por parte de usuarios externos a una red de comunicación, estando localizada la pasarela dentro de una red de acceso público, comprendiendo la pasarela:

medios para establecer un túnel exterior seguro entre una red privada y la pasarela,

medios para establecer un túnel interior seguro entre cada usuario externo que desee conectarse a la red de comunicación a través de la red privada y la pasarela, en base a una autenticación del usuario externo a la pasarela, estando el túnel interior dentro de dicho túnel exterior,

medios para asociar el tráfico que viaja a través de un túnel interior con un usuario externo correspondiente y con la red privada, y dichos medios para asociar el tráfico están dispuestos también para determinar una cantidad de tráfico externo enrutado entre los usuarios externos e Internet por medio de la red de acceso privado.

Breve descripción de los dibujos

La Figura 1 ilustra esquemáticamente un escenario en el que un usuario externo accede a Internet a través de una red privada, y

La Figura 2 es un diagrama de flujo que ilustra un procedimiento para permitir a un usuario externo acceder a una red de comunicación a través de una red de acceso privado.

Descripción detallada

Tal como se ha expuesto anteriormente, en algunas circunstancias, es deseable permitir que un usuario móvil itinerante, que posee un terminal con función inalámbrica habilitada (o posiblemente conectado por cable), por ejemplo, un teléfono inteligente, PDA, portátil, etc., acceda a una red de comunicación a través de lo que es, esencialmente, una red de acceso privado. Un ejemplo de una red privada es una WLAN doméstica o corporativa. Las redes privadas adecuadas estarán conectadas a una red de acceso público, tal como una red que es propiedad de y es operada por un operador de red de telecomunicación, para permitir a los usuarios conectarse al "mundo exterior". El operador de la red privada pagará al operador de la red de telecomunicación por este servicio, típicamente, en base a una suscripción regular y/o en base a un pago por uso.

La definición de una red privada abarca las WLANs domésticas y corporativas típicas. Sin embargo, se extiende también para abarcar cualquier dispositivo o sistema adecuado que proporciona cobertura inalámbrica en un área circundante. Los ejemplos incluyen dispositivos habilitados para Bluetooth® y WLAN. La red privada establecerá un túnel o unos túneles con la red de acceso público para enrutar el tráfico originado dentro de la red privada y con destino a la red privada, es decir, asociado con el propio cliente o clientes de las redes privadas, según la práctica convencional.

Una etapa preliminar necesaria en el procedimiento de permitir a los usuarios móviles itinerantes ("externos") hacer uso de una red de acceso privado, es el establecimiento de un túnel a nivel IP (el túnel "exterior") entre la red privada y su red de acceso público. Dicho túnel IP significa que la red privada no necesita estar conectada directamente a su red de acceso público. Esto es relevante, por ejemplo, cuando la red privada es proporcionada mediante un dispositivo tal como un teléfono inteligente o una PDA, que es capaz de conectarse a una red de acceso público a través de una red visitada (o "extranjera"). El túnel es establecido usando un intercambio de claves de Internet (Internet Key Exchange) (IKEv2) [ID.ietf-ipsec-IKEv2] a un nodo pasarela dentro de la red de acceso público. La dirección del nodo pasarela está preconfigurada o es calculada según algún procedimiento conocido (véase, por ejemplo, [3GPP.24.234]). IKEv2 puede usar posiblemente su protocolo de autenticación extensible (Extensible Authentication Protocol, EAP) de manera pueden emplearse las credenciales de acceso a red típicas. Por ejemplo, un teléfono inteligente LAN inalámbrico celular podría usar tarjetas SIM o USIM para autenticarse a sí mismo cuando se conecta a una red particular, así como cuando se comunica con la pasarela (IKEv2). La primera ejecución del procedimiento IKE resulta en el establecimiento de un par de Asociaciones de Seguridad (Security Associations, SA) IKE entre la red privada y la red de acceso público.

El acceso a los recursos de la red privada puede ser controlado por el operador de la red privada para garantizar que hay suficiente capacidad disponible para los usuarios domésticos. Sin embargo, cuando la situación de los recursos lo permite, la red privada puede ofrecer acceso a red a otros usuarios móviles externos. No se requiere autenticación para estos usuarios externos en la capa de enlace (es decir, en el establecimiento de un enlace de radio entre el usuario externo y la red privada). Sin embargo, la red privada fuerza todo el tráfico originado externamente a través del túnel exterior establecido sobre el enlace entre la red de acceso privado y público. De la misma manera, la pasarela forzará todo el tráfico destinado a un usuario externo a través del mismo túnel. El nodo de procesamiento apropiado dentro de la red privada y la pasarela realizan papeles emisor-receptor recíprocos.

Sin embargo, previamente a enrutar cualquier tráfico relacionado con el exterior a través del túnel exterior, un

usuario externo debe ser autenticado a la pasarela dentro de la red de acceso público. Esto puede realizarse haciendo que la pasarela contacte con el Registro de Ubicación Doméstica (Home Location Register) de la red troncal asociada, usando procedimientos AAA estándar. Si el usuario externo pertenece a alguna otra red, la pasarela debe autenticar el usuario externo contactando con la red doméstica del usuario, usando de nuevo procedimientos AAA. Suponiendo que la autenticación tiene éxito, se establece un nuevo par IPsec SA en IKEv2, usando Create Child SA Exchange, y la red privada asigna una dirección IP al usuario externo. Como resultado, para cada usuario externo, se crea un túnel "interior" dentro del túnel exterior que se extiende entre el usuario y la pasarela. Una vez establecido el túnel interior, el usuario externo puede empezar a enviar tráfico a Internet o a otra red de comunicación, a través de la pasarela. Esto se ilustra en la Figura 1, donde la red privada se ilustra como un ordenador portátil con WLAN habilitada, que pertenece a "Alice", mientras que el usuario externo que hace uso de la red privada de Alicia es "Nancy". La red de comunicación a la que accede Nancy es Internet. Los paquetes son "encapsulados" en el nivel más externo con las SA asociadas con el túnel exterior, y en un segundo nivel con las SA asociadas con el túnel interior apropiado. La pasarela rechazará cualquier solicitud recibida desde un usuario externo, a través del túnel exterior, de establecimiento de un túnel que no está dentro del túnel exterior. El diagrama de flujo de la Figura 2 ilustra adicionalmente este procedimiento.

Como resultado del procedimiento descrito anteriormente, la red de acceso público usada por la red privada puede asociar todo el tráfico que pasa por la misma tanto con una red privada como con un usuario externo. La red de acceso público puede determinar, de esta manera, la cantidad de tráfico externo enrutado por una red privada y puede aplicar una compensación apropiada al operador de la red privada (la compensación puede ser monetaria créditos de tráfico, etc.). Además, o de manera alternativa, la red de acceso público puede usar el acceso proporcionado por la red privada para autorizar a los usuarios de la red privada para que itineren en otras redes privadas (es decir, para permitir itinerancia recíproca entre redes privadas). Al mismo tiempo, la red de acceso público será capaz de distinguir entre el tráfico originado en la red privada y el tráfico externo enrutado a través de la red de acceso público. Esto es importante, por ejemplo, para facilitar una interceptación legal y determinar la responsabilidad por un tráfico ilícito.

Aunque es conocido el establecimiento de túneles encadenados entre puntos extremos y nodos intermedios (véase, por ejemplo, EP1280300 y “A Public Key based Secure Mobile IP”, Zao et al), no se conoce el uso de dichos túneles encadenados como un medio de enrutar un tráfico que fluye entre los usuarios externos y una pasarela a través de una red de acceso intermedia, en este caso la red de acceso privado. Al usar túneles tal como se ha explicado anteriormente, es posible para la red de acceso público determinar que cierto tráfico está originado desde un usuario externo y no está asociado directamente con la red de acceso privado. Por lo tanto, dicho mecanismo puede ser usado para aplicar una compensación monetaria o de otro tipo al operador de la red de acceso privado.

Los túneles (interior y exterior) no siempre tienen que ser establecidos a partir de cero después de movimientos de los usuarios externos y de la red privada, si es que también es móvil. Por ejemplo, cuando la red privada se mueve, puede reconectarse a su pasarela usando MOBIKE. MOBIKE es una extensión de IKEv2, que permite cambiar la dirección IP del cliente sin recrear el túnel. De manera similar, un usuario externo puede mantener su túnel interior existente incluso cuando se mueve a una red privada diferente, siempre que la red de acceso público de las redes privadas sea la misma (ya que si no, estaría implicada una pasarela diferente).

Un conjunto de mecanismos de publicidad pueden ser empleados en el nivel de la capa de enlace para indicar a los usuarios externos el tipo de servicio proporcionado por una red privada y bajo qué condiciones es proporcionado. Dicha publicidad puede proporcionar, por ejemplo, una indicación de las tarifas aplicables. Un usuario externo se conecta a la red privada en base a la publicidad.

Una persona con conocimientos en la materia apreciará que pueden realizarse diversas modificaciones a la realización descrita anteriormente, sin alejarse del alcance de la presente invención.

Referencias

[I-D.ietf-ipsec-ikev2] Kaufman, C., "Internet Key Exchange (IKEv2) Protocol", draft-ietf-ipsec-ikev2-17 (trabajo en curso), Octubre 2004.

[I-D.ietf-mobike-protocol] Eronen, P., "IKEv2 Mobility and Multihoming Protocol (MOBIKE)", draft-ietfmobike- protocol-00 (trabajo en curso), Junio 2005.

[I-D.arkko-eap-service-identity-auth] Arkko, J. y P. Eronen, "Authenticated Service Identities for the Extensible Authentication Protocol (EAP)", draft-arkko- eap-service-identity-auth-00 (trabajo en curso), Abril 2004.

[RFC2865] Rigney, C., Willens, S., Rubens, A., y W. Simpson, "Remote Authentication Dial In User Service (RADIUS)". RFC 2865, Junio 2000.

[RFC3588] Calhoun, P., Loughney, J., Guttman, E., Zorn, G., y J. Arkko, "Diameter Base Protocol", RFC 3588, Septiembre 2003.

[RFC3748] Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., y H. Levkowetz, "Extensible Authentication Protocol

(EAP)", RFC 3748, Junio 2004.

[I-D.ietf-eap-netsel-probfem] Arkko, J. y B. Aboba, "Network Discovery and Selection Problem", draft-ietf-eap-netsel-problem-01 (trabajo en curso), Julio 2004.

[3GPP.24.234] 3GPP, "3GPP system to Wireless Local Area Network (WLAN)"

REIVINDICACIONES

1. Procedimiento para enrutar tráfico entre usuarios externos e Internet a través de una red de acceso privado, comprendiendo el procedimiento:

establecer un túnel exterior seguro entre la red de acceso privado y una pasarela de una red de acceso público a la que está acoplada la red de acceso privado, en base a una autenticación de la red de acceso privado a la red de acceso público, estando dicha pasarela acoplada a Internet;

para cada usuario externo que desee conectarse a Internet a través de la red de acceso privado, establecer un túnel interior seguro entre el usuario externo y la pasarela, en base a una autenticación del usuario externo a la pasarela, estando el túnel interior dentro de dicho túnel exterior, y

hacer que el tráfico fluya entre los usuarios externos y la pasarela a través de los túneles internos respectivos,

dentro de dicha red de acceso público, usar dichos túneles interior y exterior para determinar una cantidad de tráfico externo enrutado entre los usuarios externos e Internet por medio de la red de acceso privado, y

aplicar una compensación apropiada a un operador de dicha red de acceso privado dependiendo de dicha cantidad determinada de tráfico externo.

2. Procedimiento según la reivindicación 1, en el que dicho túnel exterior transporta sólo tráfico que viaja a través de los túneles interiores.

3. Procedimiento según la reivindicación 1, en el que la red de acceso privado puede enviar su propio tráfico a través del túnel exterior, que no está dentro de un túnel interior.

4. Procedimiento según una cualquiera de las reivindicaciones anteriores, en el que dicha pasarela está configurada para rechazar solicitudes de establecimiento de túneles seguros con usuarios externos que no pasarán a través de dicho túnel exterior.

5. Procedimiento según una cualquiera de las reivindicaciones anteriores, en el que la red de acceso público es una línea fija o una red de telecomunicación celular.

6. Procedimiento según una cualquiera de las reivindicaciones anteriores, en el que dichos túneles exterior e interior son túneles IPSec definidos por IKE Sas negociados entre la red de acceso privado y una pasarela de la red de acceso público y entre los usuarios externos y esa pasarela.

7. Procedimiento según una cualquiera de las reivindicaciones anteriores, en el que la autenticación de un usuario externo a la pasarela es realizada dentro de dicha red de acceso público, o implica que la red de acceso público se comunica con una red adicional, donde el usuario es un abonado de esa red adicional.

8. Procedimiento según una cualquiera de las reivindicaciones anteriores, en el que dicha red de acceso privado es un solo nodo conectado a la red de acceso público a través de una conexión inalámbrica o por cable.

9. Procedimiento según una cualquiera de las reivindicaciones 1 a 7, en el que dicha red de acceso privado es una red inalámbrica privada.

10. Pasarela para controlar el acceso de usuarios externos a Internet, estando localizada la pasarela dentro de una red de acceso público y acoplada a Internet, comprendiendo la pasarela:

medios para establecer un túnel exterior seguro entre una red de acceso privado y la pasarela;

medios para establecer un túnel interior seguro entre cada usuario externo que desea conectarse a Internet a través de la red de acceso privado y la pasarela en base a una autenticación del usuario a la pasarela, estando el túnel interior dentro de dicho túnel exterior; y

medios para asociar el tráfico que viaja a través de un túnel interior con un usuario externo correspondiente y con la red de acceso privado,

dichos medios para asociar el tráfico están dispuestos también para determinar una cantidad de tráfico externo enrutado entre los usuarios externos e Internet por medio de la red de acceso privado.

11. Pasarela según la reivindicación 10, que comprende medios para rechazar solicitudes de establecimiento de túneles seguros con usuarios externos que no pasarán a través de dicho túnel externo.

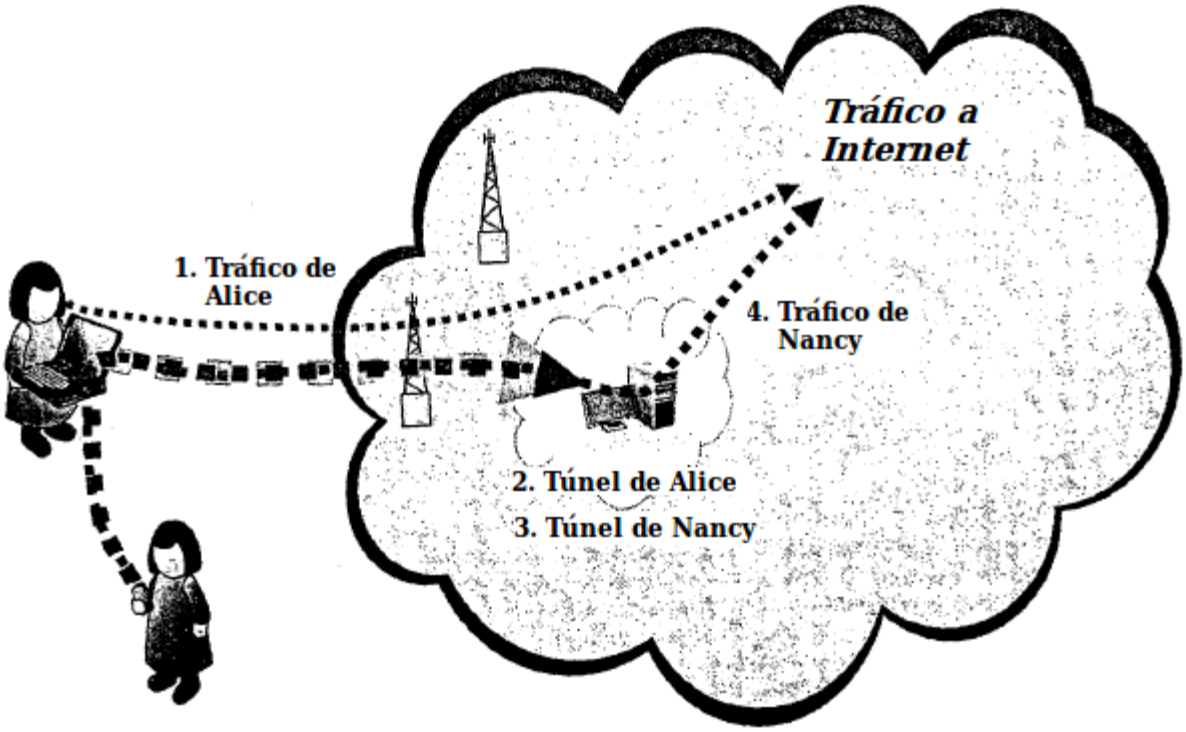
Tráfico a Internet
1. Tráfico de Alice
4. Tráfico de Nancy
2. Túnel de Alice
3. Túnel de Nancy

Figura 1

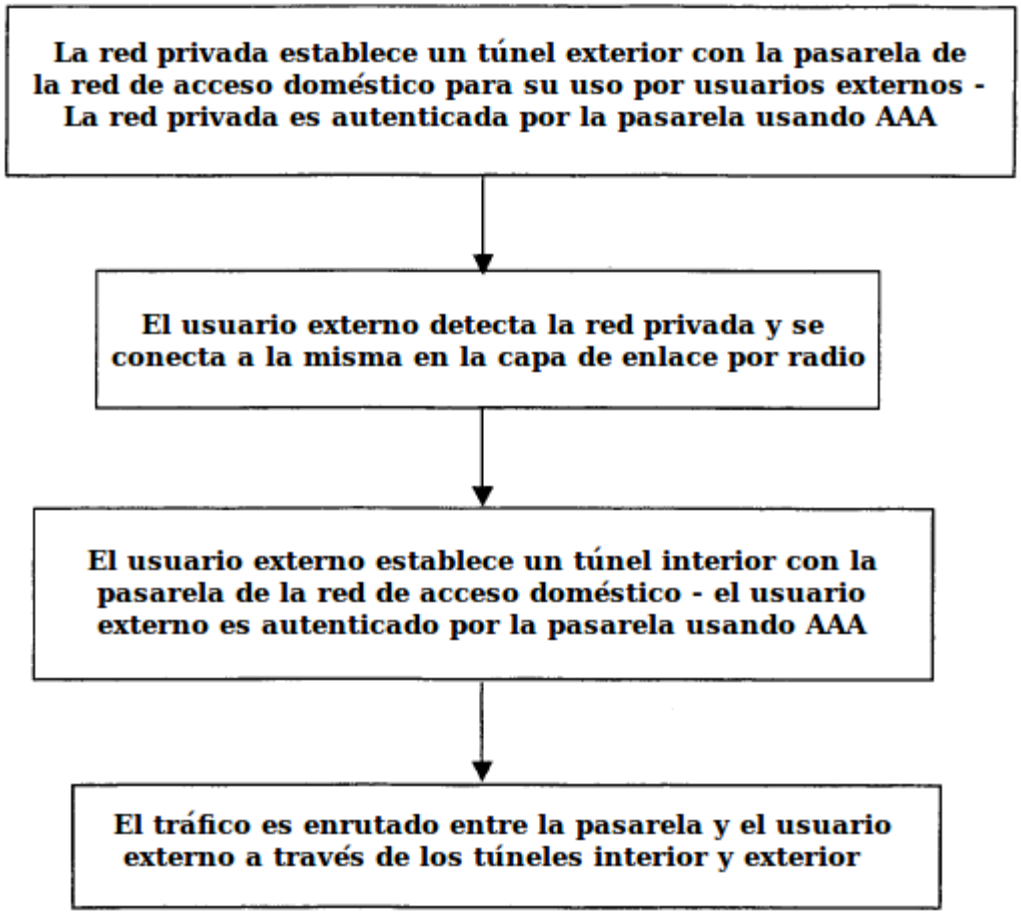
La red privada establece un túnel exterior con la pasarela de la red de acceso doméstico para su uso por usuarios externos - La red privada es autenticada por la pasarela usando AAA
El usuario externo detecta la red privada y se conecta a la misma en la capa de enlace por radio
El usuario externo establece un túnel interior con la pasarela de la red de acceso doméstico - el usuario externo es autenticado por la pasarela usando AAA
El tráfico es enrutado entre la pasarela y el usuario externo a través de los túneles interior y exterior

Figura 2