UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

Redes Privadas Virtuales (VPN)

Integrantes:
- Diego Álvarez Delgado
- Carolina Jorquera Cáceres
- Gabriel Sepúlveda Jorquera
- Camila Zamora Esquivel

Fecha: 28 de Julio de 2014

Profesor: Agustín González V.

Resumen

El mundo ha cambiado últimamente y ya no solo interesa tratar asuntos locales o regionales, ahora muchas empresas tienen que lidiar con mercados de logística globales, pero siempre hay algo que necesitan: comunicación segura, confiable y rápida sin importar dónde estén sus oficinas.

Los datos transmitidos a través de Internet son mucho más vulnerables que cuando viajan por una red interna de una organización, están expuestos ante cualquier usuario. Una solución para satisfacer esta necesidad de comunicación segura implica conectar redes remotas mediante líneas dedicadas, sin embargo, el costo es alto. Para esto se crean las Redes Privadas Virtuales (VPN).

Redes artificiales que utilizan Internet como medio de transmisión junto a un protocolo de túnel garantizando confidencialidad, bajo costo, autenticación y que la información recibida sea la enviada son algunas de las características de VPN, además de su sistema de cifrado de mensajes.

Para implementar una red privada virtual es necesario una base con las políticas de seguridad, servidor de acceso y autenticación, administración de direcciones y soporte para múltiples protocolos, para poder compartir datos, aplicaciones y recursos.

Se debe tener en cuenta que no hay solo un tipo de VPN, esta puede ser de Acceso Remoto que ofrece un nivel de acceso similar al de estar dentro de la red local, Punto a Punto que intenta eliminar las conexiones punto a punto tradicionales, y VPN Interna que funciona dentro de la misma red local LAN.

Utilizando software como LogMeIn Hamachi se puede crear una VPN. Al final de este informe se muestra la implementación de una con un límite de 5 usuarios máximos, puesto que se utiliza la versión gratuita de la aplicación mencionada anteriormente. Así, nos damos cuenta que con el software apropiado podemos hacer las cosas más simples, rápidas y seguras obteniendo los resultados requeridos.

Introducción

Dentro de la gran diversidad de usos del Internet, el principal y medular es la comunicación de equipos, la red en sí, mas ¿Cómo podemos asegurarnos de conectar terminales remotos? ¿Cómo podemos acercar computadoras para facilitar el trabajo? Tenemos las redes locales que permiten compartir archivos, recursos, información en general de forma rápida, y como bien dice, local. Ahora el reto es hacerlo a través de Internet, poder crear un ambiente en que las máquinas compartan como si estuvieran en la misma red a largas distancias.

Explicaremos cómo funcionan las Redes Virtuales Privadas, o VPN por sus siglas en inglés, los tipos de redes virtuales, protocolos empleados a grandes rasgos, mecanismos de seguridad, el software utilizado para facilitar la implementación de éstas, y las principales y potenciales aplicaciones en el ámbito doméstico/usuario final, empresarial e industrial.

¿Qué es y qué ofrecen las VPN?

VPN es una tecnología de red que permite una extensión segura de la red local (LAN) sobre una red pública o no controlada como Internet, mediante un proceso de encapsulación y de encriptación, de los paquetes de datos a distintos puntos remotos mediante el uso de unas infraestructuras públicas de transporte. Permite que la computadora en la red envíe y reciba datos sobre redes compartidas o públicas como si fuera una red privada.

VPN ofrece una solución de bajo costo para implementar la red a larga distancia al basarse sobre Internet, además de ofrecer autenticación de usuarios o equipos a través de cifrados, firmas digitales o claves de acceso para una identificación inequívoca; ofrece también integridad, garantizando que los datos enviados por el emisor sean exactos a los que se reciben, y confidencialidad, el cifrado hace posible que nada de lo transmitido sea interceptado o interpretada por nadie más que emisor y destino.

Requerimientos básicos de una VPN

Las redes privadas virtuales deben contar con ciertas bases antes de su implementación, tales son un set de **políticas de seguridad** para la codificación de datos, pues no deben ser visibles por clientes no autorizados en la red; **administración de claves**, para asegurar la codificación entre clientes y servidor; **compartir datos, aplicaciones y recursos**; un **servidor de acceso y autenticación**, para que en la red se tenga control de quiénes ingresan, verificar su identidad y tener registro estadístico sobre accesos; **administración de direcciones**, pues la VPN debe establecer una dirección para el cliente dentro de la red privada y debe asegurar que estas direcciones privadas se mantengan así; y finalmente **soporte para múltiples protocolos**, pues debe manejar los protocolos comunes a la red Internet, como IP, por ejemplo.

Tipos de VPN

VPN de acceso remoto: Consiste en usuarios que se conectan a una empresa desde sitios remotos utilizando Internet como vínculo de acceso. Una vez autenticados tienen un nivel de acceso similar a estar dentro de la red local.

VPN punto a punto: Este esquema es el empleado para conectar oficinas remotas con una sede central. El servidor VPN está conectado permanentemente a Internet, acepta conexiones entrantes desde los sitios y establece el túnel VPN. Los servidores de las oficinas remotas se conectan a Internet y a través de ésta al túnel VPN de la oficina central. Se utiliza para eliminar las conexiones punto a punto tradicionales.

VPN interna (over LAN): Funciona tal cual una red VPN normal, salvo que dentro de la misma red local LAN en lugar de a través de Internet. Sirve para aislar zonas y servicios de la misma red interna. Sirve también para mejorar las características de seguridad de una red inalámbrica WiFi.

Protocolos usados en VPN

Dentro de la multiplicidad de protocolos disponibles para su uso en las VPN, el conjunto estándar es **IPSec**, encontrándose además otros protocolos como PPTP, L2F, SSL/TLS, SSH, etc.

IPSec es un conjunto de estándares para incorporar seguridad en IP, actúa a nivel de capa de red, protegiendo y autenticando los paquetes IP entre los equipos participantes de la red. Proporciona confidencialidad, integridad y autenticación a través de algoritmos de cifrado, hash, llaves públicas y certificados digitales. IPSec tiene tres grandes componentes, dos protocolos de seguridad, como son Autenticación de cabecera IP (AH) y Carga de seguridad de encapsulado (ESP); y uno de seguridad de llaves, Intercambio de llaves de Internet (IKE).

En el protocolo AH es la porción de datos del mensaje emitido pasa a través de un algoritmo de hashing junto a la clave de autenticación de cabecera y se anexa como cabecera al paquete IPSec; al llegar a destino los datos también se calculan por el mismo proceso de llave con el hash, y si es igual al que venía en la cabecera AH, el paquete está autenticado. (fig. 1)

El protocolo ESP tiene un funcionamiento similar, cuya principal diferencia con AH es que el mensaje es ahora cifrado a través de un proceso criptográfico con la llave ESP, por lo que solo puede ser descifrado luego por un receptor que conozca de la llave. (fig. 2)

El protocolo IKE tiene dos modos de funcionamiento, uno en modo trasporte y uno en modo túnel. En modo transporte, el contenido dentro de un datagrama AH o ESP son datos de la capa de transporte, por lo tanto la cabecera IPSec se inserta luego de la cabecera IP y antes de los datos que se desean proteger; asegura la comunicación extremo a extremo, pero entendiendo ambos el protocolo IPSec. En cambio, en modo túnel, son datagramas IP completos, incluyendo la cabecera IP original. Al datagrama IP se le adjunta la cabecera AH o ESP y luego otra cabecera IP para dirigir los paquetes a través de la red. Es el protocolo IKE el estándar para la configuración de las VPN por sus características. (fig. 3)

Implementaciones y tipos de conexión

Dentro de las implementaciones tenemos dos grandes divisiones que son vía hardware y vía software. Tal cual el nombre lo dice, vía hardware es emplear configuraciones a nivel de routers o cortafuegos para conectarse de forma remota a una red privada virtual, y vía software es emplear un programa o conjunto de programas en un equipo final para hacer la conexión a la VPN.

A partir de esto, tenemos tres tipos de conexiones hacia una VPN, primeramente la **conexión de acceso remoto**, que es realizada por un cliente o usuario a través de un computador a la red privada, los paquetes enviados a través de la conexión VPN son originados al cliente de acceso remoto, autenticándose éste al servidor y el servidor al cliente, generalmente por software.

El otro tipo de **conexión es router a router**, y tal como el nombre dice, es un router el que se conecta a la red privada; en éste tipo de conexión, los paquetes enviados desde cualquier router no se originan en los routers, y es el router quien se autentifica ante el router de la red privada y viceversa, sirve también para red interna.

El tercer tipo es **conexión firewall a firewall**, en la cual un cortafuego de origen se conecta a la red privada virtual. En este tipo de conexión, los paquetes son enviados desde cualquier usuario en Internet. El firewall que realiza la conexión se autentifica ante el que responde y viceversa.

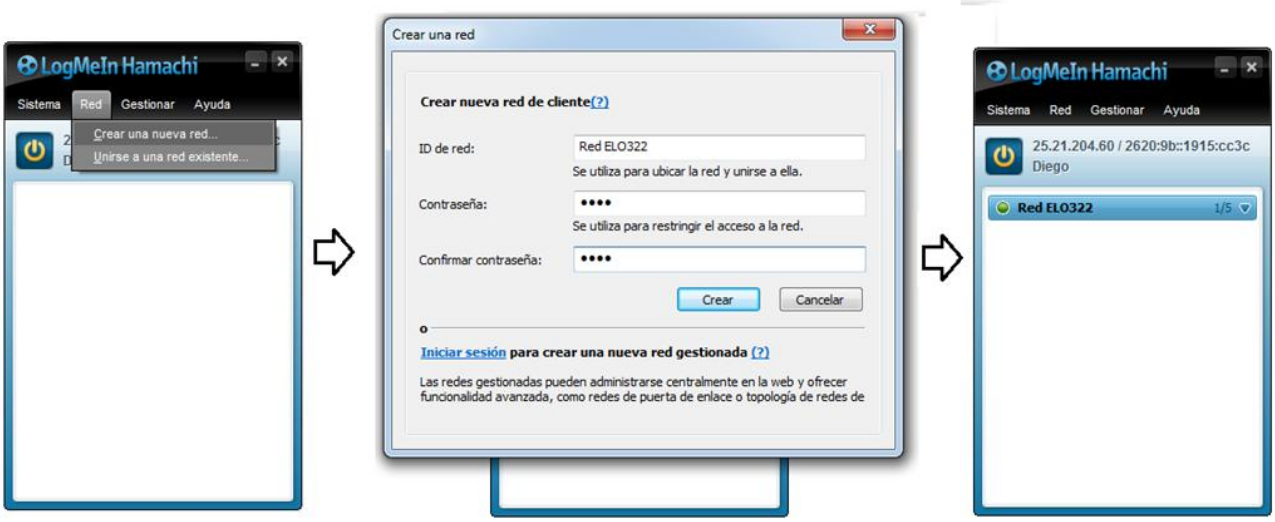
Resultados parte práctica

De manera sencilla se creó un servidor VPN en Windows 7 (Panel de control\Redes e Internet\Conexiones de red), donde el computador en uso pasa a ser el servidor. Para esto se crea una conexión entrante donde definimos los usuarios (cada usuario con una clave asignada) que podrán acceder a la VPN (equipo en uso) y especificando que puedan acceder desde Internet. Al elegir los tipos de conexiones que aceptará, generalmente descartamos la opción TCP/IPv6, ya que con TCP/IPv4 será suficiente. Una buena opción es especificar las direcciones IP, ya que se pueden acarrear conflictos con la conexión de puertos o hasta autentificación usando DHCP (ERROR 619-645-930 por ejemplo) y dándole así un rango máximo de usuarios. Finalmente se da autorización a las personas seleccionadas, posteriormente los usuarios pueden ser borrados, agregados y/o editados durante la administración de permisos de la VPN.

La segunda parte importante es la conexión de los usuarios a la VPN, para esto debemos saber cuál es nuestra IP del área local y así conectar algún equipo con alguna cuenta autorizada en esta red. Hay varias maneras de encontrar nuestra IP, podemos acceder a nuestro router y obtenerla desde ahí o poniendo en la consola el comando “ipconfig”, usaremos la IPv4 en el adaptador Ethernet conexión de área local (notar que es para conectarse sin pasar por la Internet), la conexión a través de la Internet es más compleja, pues se deben otorgar permisos del Firewall en el router y de los usuarios para evitar errores de conexión (ERROR 789-800). Finalmente introducimos un usuario y contraseña conectándonos a la VPN.

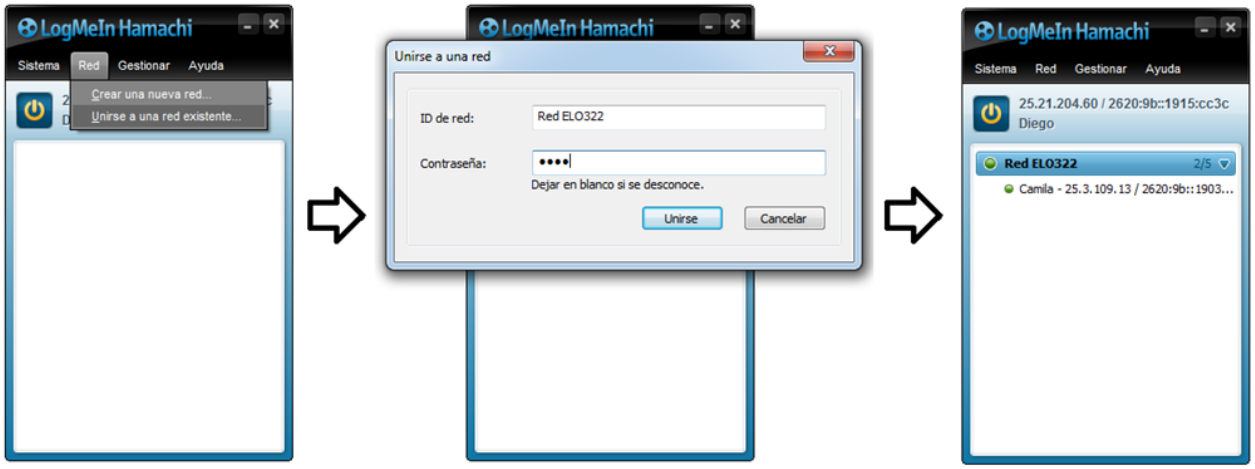
Para facilitar el uso e implementación de las VPN existen aplicaciones como LogMeIn Hamachi. Un servicio de VPN alojada que permite ampliar de forma segura la conectividad de redes tipo LAN a equipos distribuidos, teletrabajadores y jugadores. No hay necesidad de modificar el Firewall para conectarse, la seguridad es alta (SSL de 256 bits) y posee una rápida transmisión.

La utilización es muy simple, después de instalarlo se tendrá un nombre de usuario y se podrá crear una VPN :



Debemos darle un nombre que no esté en uso y asignarle una clave. Ahora otros usuarios pueden conectarse a ella pero como es la versión gratuita tiene un máximo de 5 usuarios, estos pueden ser administrados fácilmente en la aplicación, además se pueden bloquear nuevos clientes limitando el acceso.

Para conectarnos necesitamos saber el nombre y clave de la red:



Con el software apropiado podemos hacer las cosas más simples, rápidas y seguras obteniendo los resultados requeridos.

Conclusiones

En definitiva, las redes privadas virtuales resultaron un tema bastante sencillo de abordar en primera instancia, pues la información es relativamente abundante y fácil de entender, mas lo complejo vino al ir entendiendo y profundizando en el tema. Estas redes artificiales nacieron para poder abaratar costos a nivel empresarial, reemplazando las conexiones dedicadas punto a punto por cables físicos al utilizar la Internet como su estructura y camino esencial.

¿Cómo poder controlar todo lo que se trafica? En la red son solo algunos los participantes, no cualquier usuario en la Internet puede aparecer en ésta, y así nacen una serie de protocolos que ayudan a las bases de la VPN, aportando confidencialidad, integridad y autenticación. Siendo IPSec el estándar "de-facto" para las VPN, nuestro foco se mantuvo en comprender sus componentes y cómo actúa el set de protocolos y cómo los datos son transmitidos entre emisor y receptor.

Los tipos de conexiones, implementaciones y de redes privadas virtuales en sí son las que ayudan a resolver distintos escenarios y necesidades de conexión tanto para clientes finales como grandes empresas, siendo esto lo que nos llevó a nuestra parte práctica. Configurar un cliente y servidor VPN a nivel Internet es complejo, son muchas variables de seguridad en el equipo los que hay que manejar y comprender para que otros usuarios puedan participar de nuestra red, mas con ayuda de Hamachi, que es un VPN personal con directorio y servidor centralizado, estos problemas son fácilmente solucionables para un usuario estándar.

Siendo que las configuraciones de VPN actuales disponibles en routers, firewalls, y en los mismos sistemas operativos parecen simples, queda el reto de hacerlas disponibles para usuarios finales, así sería más eficiente y sencillo el uso para cualquiera con nociones de redes de computadores, pues la multiplicidad de protocolos y opciones parecen aturdir el proceso. Pero, es ésta misma la que facilita la disponibilidad para un amplio espectro de dispositivos.

Referencias

· Curso de VPN del Aula Libre y Abierta de la Universidad de Extremadura.
http://cala.unex.es/cala/cala/course/view.php?id=128
· Virtual Private Network, an overview.
http://technet.microsoft.com/en-us/library/bb742566.aspx
· LogMeIn Hamachi
https://secure.logmein.com/products/hamachi/

Anexos

Fig. 1: Funcionamiento del protocolo AH

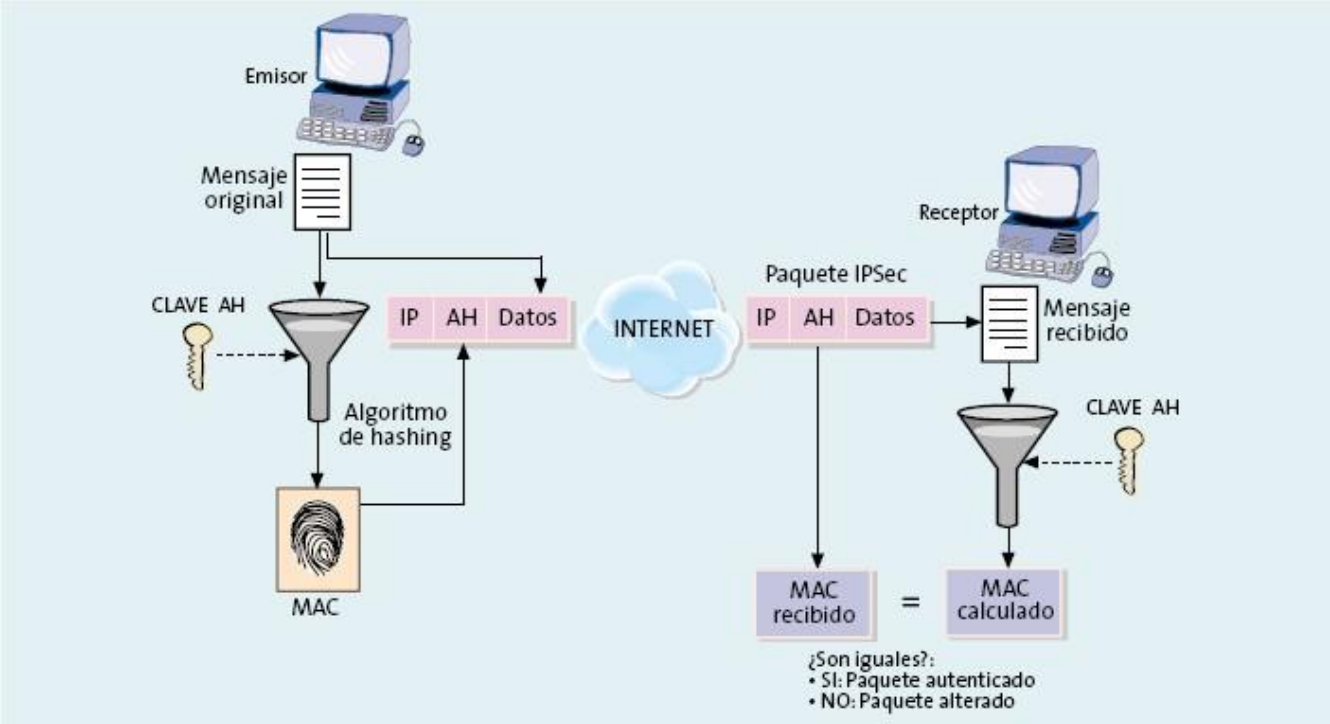


Fig. 2: Funcionamiento del protocolo ESP

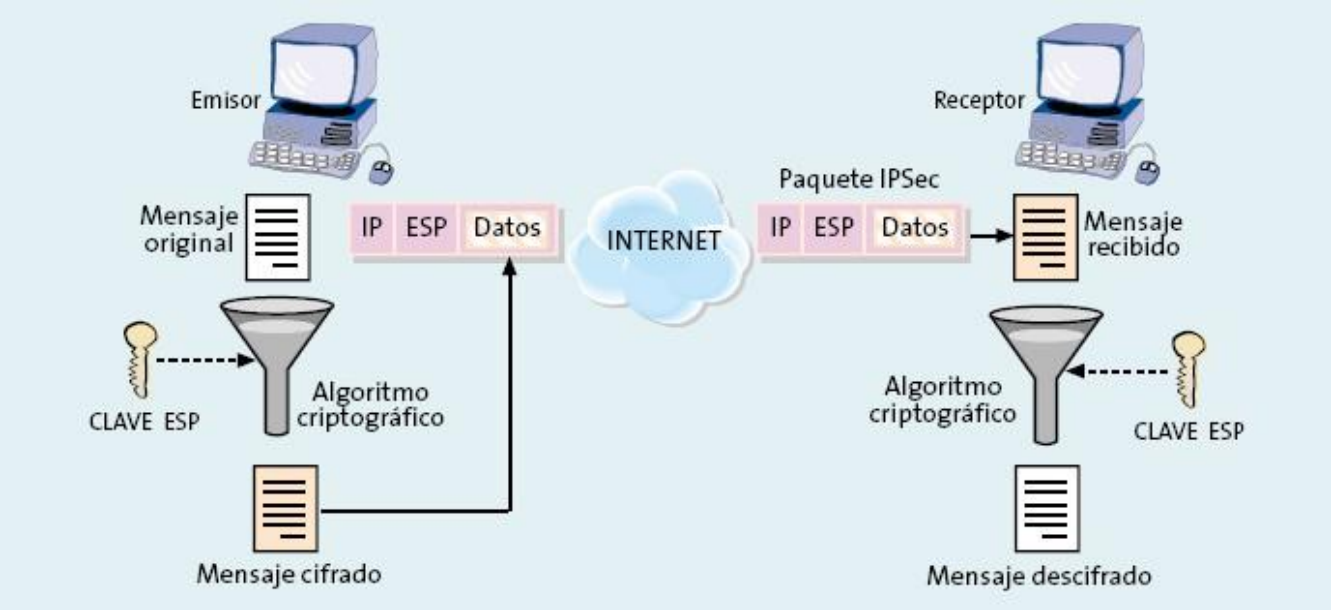
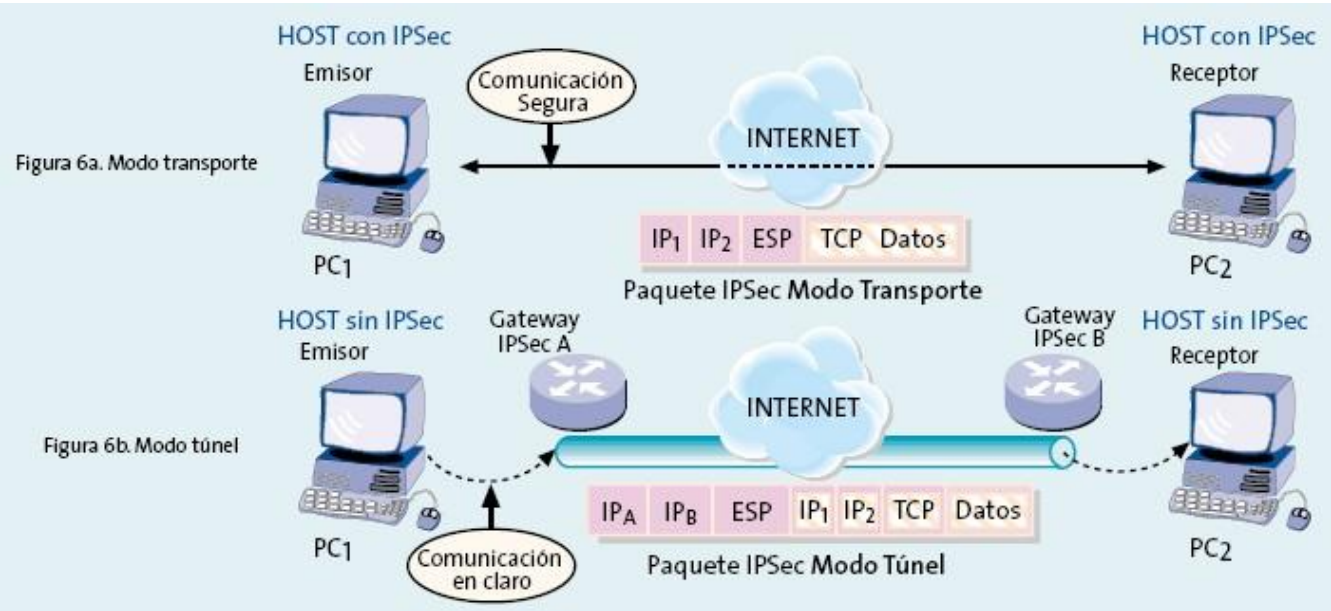


Fig. 3: Funcionamiento del protocolo IKE



Fuente: Curso de Redes Privadas Virtuales, Aula Libre y Abierta de la Universidad de Extremadura, España.