

## i-VPN

# Servicio de redes privadas virtuales dinámicas sobre Internet

Internet se ha convertido en una infraestructura de bajo costo para las comunicaciones. Su alcance universal ha llevado a muchas organizaciones a considerar la construcción de una red privada virtual segura (VPN) sobre esta red pública. Para conseguir esta seguridad, usando los estándares IETF, necesitamos soluciones VPN basadas en el protocolo de seguridad a nivel de red IPSec (IPSecurity), y protocolos de intercambio de claves de alto nivel, como IKE (Internet Key Exchange).

Si bien existen soluciones tanto comerciales como de código abierto para la construcción de VPN's, la mayoría de estas requieren que algunos (o todos) los nodos de la VPN cuenten con direcciones de red IP fijas y conocidas de antemano.

Muchas de estas soluciones permiten que los usuarios que tienen acceso remoto utilicen direcciones dinámicas, pero siempre requieren al menos un nodo central con dirección fija.

Debido a la actual profusión de enlaces de banda ancha, cada vez es mayor la cantidad de organizaciones pequeñas y medianas que tienen accesos de este tipo. Sin embargo, en general, obtener una dirección IP fija con este tipo de acceso incrementa bastante los costos, al menos comparado con los servicios más económicos.

**i-VPN** es una solución a este problema, permitiendo que organizaciones que tienen múltiples nodos, todos con direcciones dinámicas, puedan establecer redes privadas virtuales encriptadas utilizando estas conexiones.

## Red privada virtual

En la Figura 1 se presenta un diseño de VPN que consta de dos redes privadas que van a ser protegidas por dos Gateways Seguros (SG), los cuales se encargarán de controlar la información que circula entre la red A y la red B a través de Internet. De este modo, una oficina que se encuentre situada en la red A podrá enviar o recibir información de otra oficina situada en la red B de modo seguro, es decir, se proporcionará confidencialidad (la información enviada no será vista por otras personas), autenticación (la información enviada es realmente de quien dice ser) e integridad (seguridad de que cualquier alteración de la información será detectada).

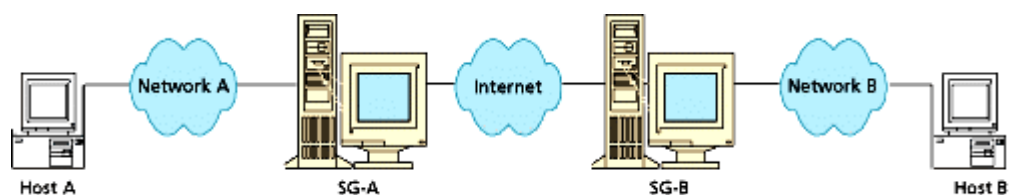


Figura 1

Figura 1

Para ofrecer esta conexión, los SGs establecen un canal seguro basado en los protocolos IPsec e IKE. La autenticación entre los extremos será realizada usando un esquema de clave pública/privada.

La implementación IPsec/IKE utilizada está basada en Linux FreeS/WAN ya que es una solución para IPv4 completa, robusta, usada ampliamente y no esta sujeta a controles de exportación.



## Seguridad IP (IPSec)

IPSec se ha convertido en el estándar criptográfico para los servicios de nivel IP, ofreciendo confidencialidad, integridad y autenticación de los extremos. El estándar es obligatorio para soluciones IPv6, para el cual fue definido, y ha sido adaptado para soluciones IPv4, en las que es optativo.

El principal concepto que define IPSec es el de Asociación de Seguridad (SA). Una SA representa una conexión lógica unidireccional entre dos entidades IPSec, y ofrece servicios de seguridad al tráfico mantenido por ellas. Estos servicios de seguridad son proporcionados por dos cabeceras que son añadidas al nivel IP: AH (Authentication Header) y ESP (Encapsulating Security Payload). La primera ofrece integridad en las conexiones, autenticación de origen y opcionalmente servicio anti-reenvío. La segunda es más completa y además de los servicios ofrecidos por AH ofrece confidencialidad. **i-VPN** utiliza ESP.

La implementación IPSec utilizada ha sido KLIPS (Kernel IP Security) incluida en el software FreeS/WAN. Esta solución permite establecer túneles seguros sobre redes no confiables, siendo los paquetes IP enrutados entre los SGs separados por cualquier topología de red. El resultado es una conexión IP virtual que nos permite definir nuestra VPN.

## Intercambio de claves: IKE

Los mecanismos de seguridad de IPSec se basan en que las oficinas deben establecer una negociación, en la cual ambas partes se ponen de acuerdo en los algoritmos criptográficos utilizados, en qué claves utilizar, y otros parámetros. Esta negociación no se puede establecer a nivel de red, por lo que es necesario un protocolo de nivel superior. El estándar actual es IKE (Internet Key Exchange), también conocido como Internet Security Association and Key Management Protocol (ISAKMP/Oakley). Este protocolo se basa en una negociación en dos fases. En la primera se establece una SA ISAKMP con la cual las entidades realizan la negociación y autenticación. En la segunda se establece una SA que será usada para la comunicación entre los extremos.

El software utilizado ha sido Pluto, la solución IKE que ofrece Linux FreeS/WAN. Pluto es un daemon que maneja intercambios de claves, verifica identidades y establece una política de seguridad para KLIPS.

## Direcciones dinámicas

**i-VPN** consiste de un servidor, alojado en Pert Consultores, que funciona como colector y distribuidor de información de ruteo y direcciones.

A cada oficina o "nodo" se le asigna un nombre lógico en la red privada virtual y cada uno de estos nodos es responsable de informarle al servidor **i-VPN** su dirección IP cada vez que arranca o su dirección cambia. A su vez, cada nodo solicita al server **i-VPN** las direcciones IP de los demás nodos de su VPN.

Con esta información, todos los nodos de la VPN establecen las conexiones entre sí.

Debe notarse que:

- ♦ El server **i-VPN** no forma parte de ninguna VPN y, de hecho, no pasa tráfico IPSec a través de él. El server se limita a recabar y redistribuir información de direcciones IP y ruteo de los nodos.
- ♦ La conexión entre los nodos y el server **i-VPN** se realiza por medio del protocolo SSH en forma segura y encriptada a través de un par de claves pública/privada distinto del que se utiliza para establecer las conexiones de la VPN. De este modo, un nodo no puede "hacerse pasar por otro" para engañar al server **i-VPN**.



Pert Consultores SRL  
Tucumán 340 4º Of. "14" - C1049AAH Buenos Aires, Argentina  
Tel/Fax: +(5411) 4311 9431  
E-mail: info@pert.com.ar  
www.pert.com.ar