Implementación de VPNs en Linux
Roberto Gómez Cárdenas

Las VPNs (Redes Virtuales Privadas, por sus siglas en inglés) proporcionan confidencialidad, integridad y autenticación a dos entidades conectadas sobre una red insegura Hace algunos años la implementación de una VPN sobre Internet requería conocimientos difíciles de adquirir, y tenía un costo alto. Poco a poco fueron surgiendo alternativas para poder crear redes virtuales, pudiendo obtener aplicaciones para conectar diferentes subredes remotas sobre cualquier enlace WAN o Internet. Hoy en día varias compañías ofrecen diversas soluciones basadas en el estándar IPSec.

IPSec es un protocolo que usa mecanismos de criptografía para proporcionar servicios de autenticación y encriptación que permiten construir túneles seguros a través de entornos no fiables. La autenticación asegura que los paquetes son del emisor adecuado y que no han sido alterados. Por otro lado, la encriptación previene la lectura no autorizada del contenido de los paquetes. IPSec es totalmente transparente para los usuarios.

IPSec esta compuesto por tres protocolos, AH (Authentication Header) que proporciona un servicio de autenticación a nivel paquete, ESP (Encapsulating Security Payload) que permite contar con encripción más autenticación e IKE (Internet Key Exchange) encargado de negociar parámetros de conexión, incluyendo llaves para los otros dos protocolos.

Free Secure Wide Area Network (FreeS/Wan) es una implementación de IPSec para Linux, disponible libremente en la página http://www.freeswan.org. La primera versión fue liberada en abril de 1999. La implementación de IPSec esta basada en tres elementos. El primero de ellos, KLIPS (Kernel IPSec), se encarga de los protocolos AH y ESP así como del manejo de paquetes dentro del núcleo. Pluto es el elemento que lleva a cabo todas las funciones de IKE. Por último se cuentan con varios scripts que ayudan con la administración de todo el sistema.

FreeS/Wan va mas allá del protocolo IPSec proporcionando un modo de operación conocido como OE (Oportunistic Encription). Este modo permite encriptar de forma automática el tráfico entre dos gateways FreeS/Wan, incluso si los administradores nunca han tenido contacto previo y ninguno de los sistemas tiene predefinida información del otro.

El sistema proporciona dos tipos de conexiones de conexiones seguras y confiables. La primera, denominada punto a red, permite que un host que soporta IPSec se conecte a una red entera y pueda acceder a cualquier punto de la misma. En el segundo tipo, red a red, una red entera puede acceder a otra conectándose con IPSec. Esto último permite acceder a cualquier maquina de ambas redes.

Debido a las restricciones en las leyes de exportación de algunos países, el código de FreeS/Wan no se incluye en el núcleo estándar de Linux, y no es incluido en muchas distribuciones. Sin embargo, la distribución brasileña conectiva (http://www.conectiva.com.br) lo incluye. Si se desea implementarlo en distribuciones como RedHat, Debian, Slackware u otras, se puede adquirir el código de la página de FreeS/Wan. Esta página ofrece una guía para su instalación, así como ligas a páginas del manual de sus principales comandos. También cuenta con rpms para las últimas versiones del núcleo de RedHat que facilitan su instalación en esta distribución.

Es posible utilizar FreeS/Wan para asegurar ambientes inalámbricos, y no preocuparnos por habilitar la función de seguridad WEP (no activada por default). Lo anterior requiere de un diseño especial de la red y de tener instalado FreeS/Wan en las todas computadoras que componen la red.

Para los usuarios de Windows, buenas noticias, FreeW/Wan puede interactuar con máquinas clientes Windows, particularmente 2000 y XP. La mala noticia es que no es una tarea trivial configurar FreeS/Wan sobre Windows.

FreeS/Wan es una opción, como otras, para asegurar las comunicaciones de una organización. Dependerá de los objetivos de la organización el utilizarla o no, pero recordemos que si la información viaja sin encriptar es relativamente simple que un atacante capture esta información y la use para su propio beneficio.