

## Redes WLAN seguras con un túnel OpenVPN encriptado

# Secretitos en Reunión...

Las redes inalámbricas son prácticas pero al mismo tiempo peligrosas. La encriptación WEP es improbable que pueda detener a un atacante. La solución viene de la mano de medidas de seguridad adicionales, tales como un túnel OpenVPN encriptado.

POR ACHIM LEITNER



La tecnología WLAN es insegura. La mayoría de la gente no está al tanto de momento. La tecnología de encriptación integrada es fácil de romper o incluso deshabilitar en el peor de los casos posibles. Mientras que un cracker malintencionado tendría que acceder físicamente a su apartamento para robar datos de una red cableada, ahora con una red inalámbrica cualquier extraño podría ir por la calle armado con un portátil y un adaptador WLAN para acceder fácilmente a su red inalámbrica (de hecho, en este mismo número vemos como se hace utilizando un simple Zaurus). Antenas especiales y amplificadores de señal aumentan de forma considerable el rango de acción de la red en varios cientos de metros.

A pesar del riesgo, las redes inalámbricas están ya aquí y se van a quedar. La posibilidad de navegar por Internet con un portátil desde la terraza o desde el jardín, o copiar los ficheros del PC de sobremesa al portátil, mejoran la experiencia del usuario. Y esto es algo bueno, suponiendo que se tomen algunas medidas básicas de seguridad para eliminar el riesgo.

### Póntelo, Pónselo

Antes de decidir que clase de protección es mejor para un entorno, hay que mirar

detenidamente como el ordenador se conecta a la red y la clase de tráfico de red que va soportar el adaptador inalámbrico.

La protección integrada en la WLAN podría ser suficiente para algunos usuarios y otros incluso deshabilitarán deliberadamente cualquier clase de seguridad. Pero si se necesita más, las soluciones VPN como OpenVPN [1] son

una buena elección: simples de usar, pero seguras y modernas. OpenVPN encripta y autentifica los intercambios entre dos máquinas, ya sean Linux o Windows.

Fuera de la red particular, Internet está llena de los mismos peligros que las WLAN. Los atacantes pueden acceder o manipular los datos o incluso introducir contenidos dañinos. Hay que

### Cuadro 1: Un ordenador Aislado

El escenario más simple de todos es aquel formado por un sólo ordenador que usa un punto de acceso para conectarse a Internet (Véase la Figura 1). Además de los riesgos que afectan a las redes cableadas, tenemos que considerar el secuestro de la conexión, la denegación de servicios, el acceso no autorizado desde portátiles desde la calle o de nuestros vecinos. Aquellos que estén paranoicos con ser atacados por crackers, verán que las redes inalámbricas es un sector potencialmente fácil de atacar. Pero un ataque aleatorio puede venir tanto desde la

Web como desde unos metros a la redonda entre el portátil y el punto de acceso inalámbrico.

También es conveniente estar bastante paranoico por cualquier tipo de dato. La única forma de cerciorarse de que los datos no han sido manipulados es usar criptografía e impedir los accesos no autorizados. En otras palabras, usar SSL/TSL para obtener el contenido de la Web y habilitar la protección SSL en el cliente de correo. SSL encripta y autentifica los datos en la transmisión.

Para añadir una capa más de protección hay que usar PGP o S/MIME. Ambos encriptan los mensajes de correo, en vez de proteger el tráfico. Y usar SSH para las conexiones remotas seguras.



Figura 1: Conexión a Internet con un router WLAN.

distinguir entre dos casos: PCs aislados o portátiles que usen la red inalámbrica y un router WLAN para el acceso (Véase el Cuadro 1) y redes particulares protegidas donde una WLAN se ha instalado para ampliar su uso, o incluso reemplazar parte de la red cableada (Véase el Cuadro 2).

## Gorrones y Alborotadores

Las redes WLAN presentan un nuevo tipo de riesgo: toda clase de desconocidos pueden aprovecharse del punto de acceso de la WLAN para obtener acceso gratuito a Internet. La extensión del daño que esto puede causar depende de la clase de tarifa de Internet que se tenga contratada. Si se tiene tarifa plana, puede ser que no le importe que su vecino se le cuele por la WLAN y compartan la Web. Pero si se tiene una tarifa basada en el tráfico de datos, el compartir el acceso puede afectar de forma negativa su cartera. La forma de evitar que esto suceda es habilitando el filtrado basado en MAC del router WLAN y, adicionalmente, el uso de la encriptación WEP.

Ninguna de estas medidas proporciona una protección perfecta, pero al menos levanta una barrera extra contra los crackers y se asegura de que nadie pueda acceder de forma accidental a la WLAN o negar que se está compartiendo el acceso de forma deliberada. Hay que cerciorarse de que la encriptación WEP y el filtrado MAC estén activados en todo momento; el no tenerlos es una

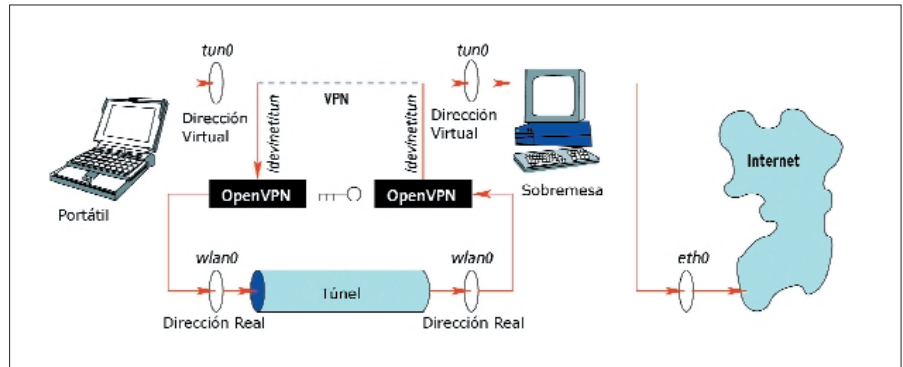


Figura 2: La Red Privada Virtual (VPN) funciona a través de un túnel, en los extremos es donde están las direcciones IPs reales del portátil y del PC.

invitación para los crackers, gorrones y espías.

Más protección implica mayor trabajo, pero al menos WEP ya tiene sucesor designado. En el pasado mes de junio del 2004, IEEE presentó un estándar más seguro llamado 802.11i, también conocido como WPA-2. Desafortunadamente, esta tecnología está limitada a los nuevos adaptadores y es difícil hacer las cosas bien. El nuevo estándar especifica un número de técnicas, pero no todas ellas son seguras. Se recomiendan AES-CCMP para la encriptación y 802.1x para autenticación y gestión de claves.

## Protección VPN

Linux soporta un sistema de seguridad para WLAN con operaciones anti-intrusos sin la necesidad de una tarjeta nueva. Si su tarjeta no le proporciona la clase de protección que necesita, la solución está en añadir software de

seguridad. El protocolo VPN (Virtual Private Network) encripta y autentifica datos en la capa IP. Un terminal VPN acepta sus datos, los encripta, los firma y los transmite por el enlace de radio. El receptor desempaqueta los paquetes entrantes.

Una VPN usará los recursos de una WLAN tradicional pero parecerá como una red nueva (una red virtual) desde el punto de vista del cliente. La Figura 2 explica el principio: El portátil y el PC de sobremesa tienen una conexión WLAN. Ambos son accesibles a través de sus direcciones IP reales sobre la red inalámbrica.

La VPN le da al portátil y al PC de sobremesa direcciones IP adicionales. Los datos enviados a las direcciones virtuales se encapsulan por la VPN y se envían a la IP real de destino. El destino desempaqueta los datos y los trata como si hubiesen llegado por la dirección virtual, así se crea un túnel entre el portátil y el PC de sobremesa.

Las reglas del cortafuegos se aseguran de que ambas máquinas sólo aceptan datos provenientes del túnel. Esto significa que los paquetes insertados directamente dentro de la WLAN por algún cracker malintencionado serán inofensivos.

## OpenVPN

El principio en el que se basa VPN es usado por diversos protocolos, productos y proyectos. OpenVPN [1] es un método probado y verificado, siendo estable y simple, funciona sin manipular ni el kernel ni la pila IP. Como este programa se basa en el popular protocolo criptográfico TLS y la implementación es clara, OpenVPN se

## Cuadro 2: Redes Particulares

Una red para una pequeña empresa o para una casa con un grupo de ordenadores conectados es algo más complicado de proteger que un simple PC aislado, comentado en el Cuadro 1. Las redes de esta clase usan un cortafuegos para proteger la conexión de Internet y los usuarios se sienten seguros detrás de él. Los cortafuegos a menudo impiden cualquier clase de conexión desde Internet. Pero este tipo de ambiente puede provocar que los usuarios se descuiden.

Los daños potenciales incluyen los servicios de NFS o Samba que permiten acceso compartido anónimo de los directorios privados, los servicios de impresión que envían datos sin encriptar y las conexiones basadas en Telnet y Rlogin. Se supone que cada ordenador confía en la red y en los equipos conectados

en ella. La confianza es peligrosa en las LAN tradicionales, así que mucho más en las redes WLAN. El atacante está detrás del cortafuegos y puede lanzar ataques desde dentro. En una red cableada tradicional, un espía o saboteador tendría que tener acceso físico a las instalaciones para poder lanzar el ataque. Con las WLAN, el atacante tan sólo tiene que estar en las proximidades. Ya no hacen falta ni los cables ni puntos de acceso.

La única manera de protegerse en las redes inalámbricas contra los atacantes es usando la criptografía. El primer intento por estandarizar la criptografía para las redes LAN inalámbricas ha fallado miserablemente: WEP es fácil de romper y no ha sido un buen trabajo. Sin embargo, VPN permite añadir una capa más de protección.

ha ganado la reputación de ser extremadamente seguro.

A ambos lados del túnel, OpenVPN recoge los paquetes destinados al otro lado, y usando una clave local encripta los paquetes antes de enviarlos. En el punto de recepción tan solo se aceptarán datos que hayan sido encriptados usando la clave válida. Cualquier otro paquete se ignorará. Con esta solución los datos se transportan en contenedores seguros a través de ambientes hostiles.

El siguiente ejemplo supone que *wlan0* es la conexión de red inalámbrica. El PC de sobremesa tiene además una NIC cableada, *eth0*. Las otras máquinas de la red y de Internet son accesibles vía conexión Ethernet (Véase la Figura 2).

## Empezando

Si aún no lo ha hecho, instale el paquete OpenVPN antes de continuar (Véase el Cuadro 3). OpenVPN no modifica el kernel. En vez de ello, para ser capaz de reenviar los paquetes, usa el driver TUN/TAP [4]. La mayoría de las distribuciones instalan el módulo del kernel por defecto, así que lo único que hay que hacer es cargar el módulo. Como root, tecléese lo siguiente para hacerlo:

```
modprobe tun
```

Linux normalmente no usa ficheros de dispositivo para los interfaces de red; es decir, no hay */dev/eth0*. Esto podría parecer inconsistente, pero es innecesario ya que la interfaz socket maneja la comunicación. El interfaz TUN se aprovecha de esto y rompe las reglas creando un fichero de dispositivo, que permite a un servicio de usuario tomar

los paquetes IP, reempaquetarlos y reenviarlos.

El servicio escribe el paquete en */dev/tun0* o en */dev/tun* (Véase el Cuadro 3), y llegan al kernel por el interfaz *tun0*. Cada paquete que el kernel envía a *tun0* llega al servicio por */dev/tun0* o en */dev/tun* (Véase la Figura 2). El interfaz funciona como cualquier otro interfaz de red; se le puede asignar una dirección IP, usarse para encaminamiento y aplicársele las reglas del cortafuegos. La única diferencia está en que no usa la tarjeta Ethernet para poner los datos en el cable, sino que usa el dispositivo para enviarle los datos a un proceso.

## Claves

OpenVPN necesita las claves para proporcionar la seguridad. En el caso más simple, ambos usuarios confiarían en una clave secreta compartida. El siguiente comando crea una clave y la almacena en un fichero llamado *secret.key*:

```
openvpn --genkey
--secret secret.key
```

Sólo las dos máquinas deberían conocer las claves y sólo el root debería tener acceso de lectura a ellas. Si alguien conoce la clave, podría irrumpir fácilmente en el túnel. Es muy importante asegurarse de que las claves no sean pirateadas por el cable cuando se copien entre las dos máquinas. Alguien podría estar escuchando en la línea. Lo mejor sería usar un disquete; ¡sin olvidarse de formatear el disquete una vez que se haya terminado la copia! Si se tiene OpenSSH, PGP, GnuPG o una he-

rramienta similar, se podría usar alguno de estos programas para transferir el fichero de forma segura.

## Cavando el Túnel

Lo siguiente que hay que hacer es crear el túnel. Para ello, OpenVPN necesita la dirección IP (estática) de la máquina destino, el nombre del dispositivo del túnel (por defecto *tun0*), las dos direcciones virtuales de VPN y el fichero de la clave. En el portátil, el comando a introducir sería como:

```
openvpn --dev tun0 --remote
[Real_DesktopIP] --ifconfig
[Virtual_LaptopIP]
[Virtual_DesktopIP]
--secret secret.key
```

Hay que ser root para ejecutar este comando y todos los siguientes. En el PC de sobremesa, el comando con la IP modificada sería:

```
openvpn --dev tun0 --remote
[Real_LaptopIP] --ifconfig
[Virtual_DesktopIP]
[Virtual_LaptopIP]
--secret secret.key
```

Las direcciones virtuales del túnel son más o menos arbitrarias; pero tienen que ser **direcciones privadas**. Las direcciones virtuales deberían ser de un bloque diferente de las reales para facilitar el enrutamiento y hacerlas fácilmente distinguibles de las direcciones reales de la red.

## Asignación de Direcciones

Supongamos que la tarjeta WLAN en el portátil tiene la dirección IP real

## Glosario

**S/MIME:** Secure/Multipurpose Internet Mail Extensions es otra forma de encriptar y firmar digitalmente los mensajes de correo, una alternativa a PGP.

**WEP:** Wired Equivalent Privacy fue el primer intento de los desarrolladores de WLAN de estandarizar un protocolo cripto-seguro para darle al tráfico inalámbrico la misma clase de protección que el tráfico cableado. Pronto se comprobó que el protocolo tenía fallos y era además inseguro.

**SSL/TLS:** Secure Sockets Layer es un protocolo criptográfico desarrollado por Netscape. SSL

es un método probado en el que se puede confiar para las transmisiones encriptadas. Transport Layer Security es un desarrollo sobre SSL.

**VPN:** Virtual Private Network. Usa una red existente para emular una red diferente dentro de un entorno de red. El software VPN encripta el tráfico de datos antes de enviarlos.

**SSH:** El Secure Shell permite a los usuarios de Linux conectarse de forma segura desde un ordenador remoto. Las sesiones completas, incluido el intercambio de claves, se encripta con SSH.

**PGP:** Pretty Good Privacy se usa para encriptar y firmar los mensajes de correo. OpenPGP es una implementación estándar y GnuPG es una alternativa más actual.

**Private address:** Las direcciones IPs públicas son únicas. Esta es la única forma de asegurarse de que los paquetes puedan encontrar el camino al destino. Las direcciones IP privadas sólo son válidas en una red local y no son enrutadas dentro de la Internet pública. Esto permite que varias redes puedan usar las mismas direcciones privadas.

172.16.0.1 y el PC de sobremesa 172.16.0.2. La VPN necesita direcciones de un espacio privado de direcciones, tales como 10.0.0.1 para la dirección virtual del portátil y 10.0.0.2 para el PC de sobremesa. En este caso, el comando en el portátil sería:

```
openvpn --dev tun0 --remote 172.16.0.2 --ifconfig 10.0.0.1 10.0.0.2 --secret secret.key
```

y en el PC de sobremesa:

```
openvpn --dev tun0 --remote 172.16.0.1 --ifconfig 10.0.0.2 10.0.0.1 --secret secret.key
```

Se puede usar el comando ping para comprobar que el túnel está funcionando. En el portátil, `ping 10.0.0.2` debería funcionar e indicar que la dirección virtual del PC de sobremesa es alcanzable.

Si todo funciona tal y como se ha planeado, se querrá ejecutar el servidor de OpenVPN en segundo plano; el servidor enviará mensajes de salida a syslog. Para conseguirlo se usa la opción `--daemon`. Nótese que se necesita indicar la ruta absoluta al fichero con la clave secreta.

## El Camino Seguro

El túnel ya está listo y los paquetes llegan al otro lado. Pero tanto el portátil como el PC de sobremesa necesitan conocer qué paquetes tienen que enviar por el túnel. En otras palabras, necesitan saber la dirección IP virtual del otro lado del túnel. El comando de OpenVPN establece la ruta para reflejar esta dirección. Todas las otras direcciones serán enrutadas como se hacía anteriormente, sin el túnel.

La ruta desde el PC de sobremesa al portátil funcionará bien, si se usa la nueva dirección IP virtual para comunicarse con el portátil. De hecho, las antiguas direcciones reales asignadas a las tarjetas WLAN en el portátil y en el PC de sobremesa sólo sirven para un propósito: son los extremos del túnel. No se usarán con las conexiones normales salvo para esta tarea.

El camino de regreso desde el portátil hasta el PC de sobremesa (y desde allí hasta los demás PC de la red cableada e

Internet) necesita editarse de forma manual. La ruta por defecto tiene que ser reconfigurada. El siguiente comando le indica la portátil que envíe todos los paquetes por el túnel:

```
route del default
route add default gw 10.0.0.2
```

Los paquetes que se direccionan a la dirección IP real de la WLAN del PC de sobremesa (172.16.0.2) no se ven afectados por esta configuración. Y está bien porque el túnel usa esta dirección. Ahora, el PC de sobremesa necesita saber que debe reenviar los paquetes que ha desempaqueado si fuera necesario. El siguiente comando se encarga de ello:

```
echo "1" > /proc/sys/net/ipv4/ip_forward
```

## Combatiendo el Fuego

Casi hemos terminado a ambos lados del túnel. El portátil y el PC de sobremesa ya usan felizmente el túnel, los datos están protegidos y nadie puede hacerse con ellos. Pero aún es posible infiltrar paquetes dañinos y permitir a un atacante compartir la conexión a Internet.

Incluso si se está pagando una tarifa plana para acceder a Internet, no se querrá compartir el ancho de banda. Todos los servicios de red que el PC de sobremesa y el portátil comparten (Web, SSH, FTP,...) pueden ser atacados por la WLAN. Y si se tiene una red, también existe otra fuente de peligro: cualquier paquete infiltrado a través de la WLAN se salta el cortafuegos, que típicamente está instalado entre Internet y la red local, donde la WLAN está conectada.

La solución está en proporcionar alguna clase de protección de cortafuegos para la WLAN. La distribución de OpenVPN [1] tiene un script de ejemplo de cortafuegos. Pero se necesitan reglas adicionales para el túnel de la WLAN. La Figura 3 muestra cómo se aplican estas reglas.

## ¡Fuera!

OpenVPN usa UDP para enviar los paquetes encriptados al puerto 5000 al otro lado del túnel. Como usa la interfaz de WLAN `wlan0` para ello, hay que admitir los paquetes UDP que van al puerto 5000 del interfaz. La siguiente sintaxis maneja esto para los paquetes entrantes:

```
iptables -A INPUT -i wlan0 -p udp --dport 5000 -j ACCEPT
iptables -A INPUT -i wlan0 -j DROP
```

## Cuadro 3: Instalación

OpenVPN es muy fácil de instalar. El paquete de código fuente para la versión estable 1.6.0 está disponible en la página web del proyecto [1]. Los siguientes comandos descomprimen el paquete, compilan el software y lo instala con los privilegios de root:

```
tar -xvzf openvpn-1.6.0.tar.gz
cd openvpn-1.6.0
./configure --disable-lzo
make
su
make install
```

Necesita ejecutar `configure` con el parámetro `--disable-lzo` para deshabilitar la compresión. Como los datos no pueden comprimirse después de encriptarse, esta librería está recomendada sobre todo para las conexiones lentas. La librería está disponible en [2]. Lo que se necesita aquí es la librería OpenSSL y los ficheros de desarrollo, que están localizados en dos paquetes separados en Suse: `openssl` y `openssl-devel`. Otras dis-

tribuciones también contienen el paquete SSL o puede mirarse la página web del proyecto OpenSSL [3] para obtener más detalles y productos relacionados.

El kernel actual tiene el dispositivo túnel por defecto; el paquete disponible en [4] es para las versiones más antiguas del kernel. Si compilas tu propio kernel, el módulo TUN está localizado en la sección "Network device support" bajo "Universal TUN/TAP device driver support" de `make xconfig`. Desde luego que se puede compilar e instalar el módulo sin sustituir el kernel al completo. Después de configurar el kernel, tecléese:

```
make modules
make modules_install
El siguiente paso es crear el fichero de dispositivo /dev/net/tun. Si /dev/net/ no existe, teclee primero mkdir /dev/net/ y luego cree el dispositivo:
mknod /dev/net/tun c 10 200
```

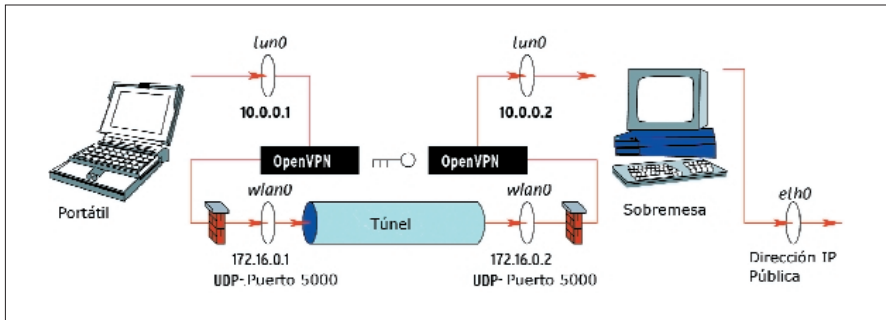


Figura 3: Las reglas de los cortafuegos impiden a los intrusos entrar en la WLAN. Sólo al túnel OpenVPN se le permite enviar paquetes a través de la WLAN.

La última línea se asegura de que la máquina no aceptare ningún otro paquete entrante. La primera regla de entrada podría incluso ser más estricta y especificar `-s RealIP` para restringir la dirección IP fuente, donde los paquetes se permiten que sean originados. Esta tendría que ser la dirección IP real del otro extremo del túnel, es decir, `-s 172.16.0.2` en el portátil. También es necesario restricciones para el envío y reenvío de paquetes:

```
iptables -A OUTPUT -o wlan0 -p udp --dport 5000 -j ACCEPT
```

```
iptables -A OUTPUT -o wlan0 -j DROP
iptables -A FORWARD -i wlan0 -j DROP
```

Los extremos del túnel sólo reenvían los paquetes que son originados por un compañero conocido y sólo si este compañero conocido usa la clave (secreta) correcta. Esto significa que podemos confiar, aceptar y procesar los paquetes que vienen desde el dispositivo `tun`. Naturalmente, aún falta permitir a las máquinas el envío de paquetes por el túnel. El siguiente

comando permite la recepción y envío de paquetes:

```
iptables -A INPUT -i tun0 -j ACCEPT
iptables -A OUTPUT -o tun0 -j ACCEPT
```

Esto es todo lo que necesitamos para el portátil; que no está conectado a otras redes ni necesita reenviar paquetes.

## Reenvío

El PC de sobremesa necesita reglas de reenvío y necesita usar enmascaramiento para permitir que el portátil llegue al otro lado del mundo:

```
iptables -A FORWARD -i tun0 -j ACCEPT
iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
```

La regla de enmascaramiento le indica al PC de sobremesa que inserte su propia dirección IP pública en vez de la dirección privada de la VPN. La dirección privada no puede ser enrutada en Internet, pero con esta configuración, el PC de sobremesa enrutará cualquier paquete que el portátil envíe a través del túnel a su propio interfaz LAN y a Internet. Si el PC de sobremesa tiene una conexión DSL o módem simplemente hay que sustituir `ppp0` por `eth0`.

## Limitaciones de Seguridad

Una red es tan segura como lo puedan ser los ordenadores conectados a ella. Una persona no autorizada podría acceder al portátil OpenVPN, leer la clave y usarla para romper la seguridad de la red virtual. Las redes inalámbricas necesitan una mejor protección ante los ladrones.

Si se atiende a las reglas básicas descritas en este artículo, encontrará que OpenVPN es un producto de VPN seguro y al mismo tiempo de uso sencillo. ■

## Cuadro 4: Variedad de Funciones en OpenVPN

Además del sencillo ejemplo mostrado de una conexión VPN, OpenVPN también permite conectar sitios completos. Simplemente cambiando la configuración de enrutamiento se consigue esto. En el modo puente, OpenVPN puede incluso conectar dos secciones de LAN de forma transparente, permitiéndoles usar el mismo espacio de direcciones.

La solución de la clave secreta descrita en este artículo no funciona bien si la red tiene múltiples nodos. Pero esto es una de las mejores características de TLS. Está diseñada para usarse con certificados X.509. La versión 2.0 (actualmente en fase beta) hace que el trabajo sea mucho más sencillo para los administradores: no hace falta crear una configuración de servidor para cada cliente VPN; tan sólo se necesita un certificado X.509 válido. Además, el nuevo servidor debería realizar la mayor parte del trabajo duro.

En modo UDP, OpenVPN no distingue entre clientes y servidores pero ejecuta aplicaciones peer-to-peer. Estableciendo la opción `--float` se permite que el túnel pueda transportar flujos sin interrupciones incluso si las direcciones IP reales de un extremo cambian,

por ejemplo, debido a un reseteo forzoso diario. Las conexiones TCP se mantendrían, lo que es útil si se necesita transferir grandes ficheros mediante FTP.

Si lo que se necesita es enviar grandes ficheros a través del túnel, podría especificarse la opción `--shaper [ancho de banda]`. La opción restringe la velocidad de entrada al túnel a un número específico de bytes por segundo. Para restringir el ancho de banda en ambas direcciones se necesita especificar la misma opción a ambos lados. OpenVPN puede abrir múltiples túneles entre dos compañeros al mismo tiempo y asignar diferentes anchos de banda a cada túnel: esto puede ser útil para tareas administrativas. La configuración del router especifica qué datos se envía por cada túnel.

La versión 1.5 de OpenVPN y posteriores también soportan TCP. Si está detrás de un cortafuegos que sólo acepta TCP no habrá otra alternativa posible. La desventaja de esto, si hay problemas en la red, es que la combinación de VPN sobre TCP haría que las cosas empeorasen. A pesar de todo, se debería configurar OpenVPN para que usase la solución tradicional basada en UDP.

## RECURSOS

- [1] OpenVPN: <http://openvpn.sourceforge.net>
- [2] Proyecto OpenSSL: <http://www.openssl.org/>
- [3] Librería LZO: <http://www.oberhumer.com/opensource/lzo/>
- [4] Driver TUN/TAP: <http://vtun.sourceforge.net/tun/>