Juan A. León

Colegio Altair - Sevilla
Grado Superior Desarrollo de Aplicaciones Web
SSII - 2017/18

Servidor VPN basado en IPSec (CentOS)

Puedes ver este vídeo

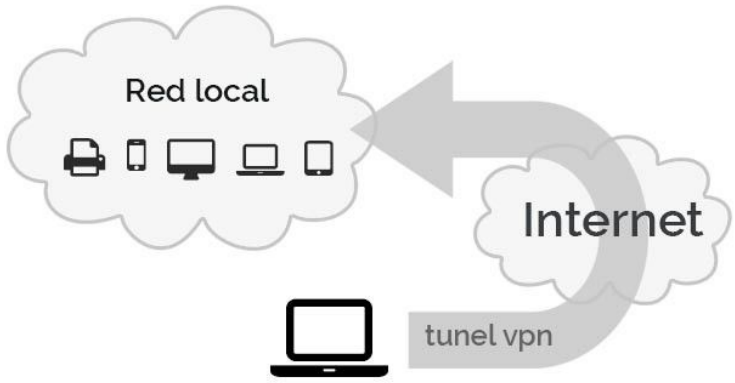
ÍNDICE

¿Qué es VPN?[1]

VPN son las siglas de *Virtual Private Network*, o **red privada virtual**.

Para conectarse a Internet, tu móvil, PC, televisión y demás dispositivos generalmente **se comunican con el router o módem** que conecta tu casa con tu proveedor de Internet, ya sea mediante cable o inalámbricamente. Los componentes son distintos si estás usando la conexión de datos de tu móvil (que incluye su propio módem y habla con la antena de telefonía) pero la esencia es la misma: tu dispositivo se conecta a otro, que le conecta a Internet.

Una conexión VPN lo que te permite es crear una red local **sin necesidad que sus integrantes estén físicamente conectados entre sí**, sino a través de Internet. Es el componente "virtual" del que hablábamos antes. Obtiene las ventajas de la red local (y alguna extra), con una mayor flexibilidad, pues la conexión es a través de Internet y puede por ejemplo ser de una punta del mundo a la otra.



Usos principales de VPN

- **Teletrabajo:** Empresas con sedes en varias poblaciones o trabajadores que no estén en su oficina en este momento pueden trabajar como si de una red local se tratase.
- **Evitar censuras y bloqueos geográfico de contenidos:** Usando un servidor VPN el cliente navega como si estuviera en la ubicación física del servidor. Supongamos que tenemos un servidor en Frankfurt (Hesse, Alemania) y a un cliente en Villanubla (Valladolid, España), nuestro cliente podrá navegar como si estuviera en Alemania, saltándose los filtros que haya en España, y pudiendo acceder al contenido tudesco.
- **Capa extra de seguridad:** Al conectarte por redes wifi públicas corres el riesgo de que tu información sea capturada por terceros que también están conectados a esa red, en cambio al usar la tecnología VPN, la comunicación servidor-cliente está cifrada.

[1]Ivan Ramirez en Xataka
https://www.xataka.com/seguridad/que-es-una-conexion-vpn-para-que-sirve-y-que-ventajas-tiene

¿Qué es IpSec?[2]

IpSec es una suite de protocolos de red, enfocados a la seguridad que trabajan a nivel de capa 3 y permiten autentificación, autenticación y cifrado mediante criptografía simétrica o asimétrica de un flujo de datos.

Esto quiere decir que cada paquete Ip de un flujo de datos es cifrado de una forma más flexible que SSH por ejemplo (ya que usan la capa 7)

IPsec consta de tres protocolos que han sido desarrollados para proporcionar seguridad a nivel de paquete, tanto para IPv4 como para IPv6:

- **Authentication Header (AH):** proporciona integridad, autenticación.
- **Encapsulating Security Payload (ESP):** proporciona confidencialidad y la opción -altamente recomendable- de autenticación y protección de integridad.
- **Internet key exchange (IKE):** emplea un intercambio secreto de claves de tipo Diffie-Hellman para establecer el secreto compartido de la sesión. Esta será el que usemos nosotros.

[2] IpSec - Wikipedia https://es.wikipedia.org/w/index.php?title=IPsec&oldid=105381650

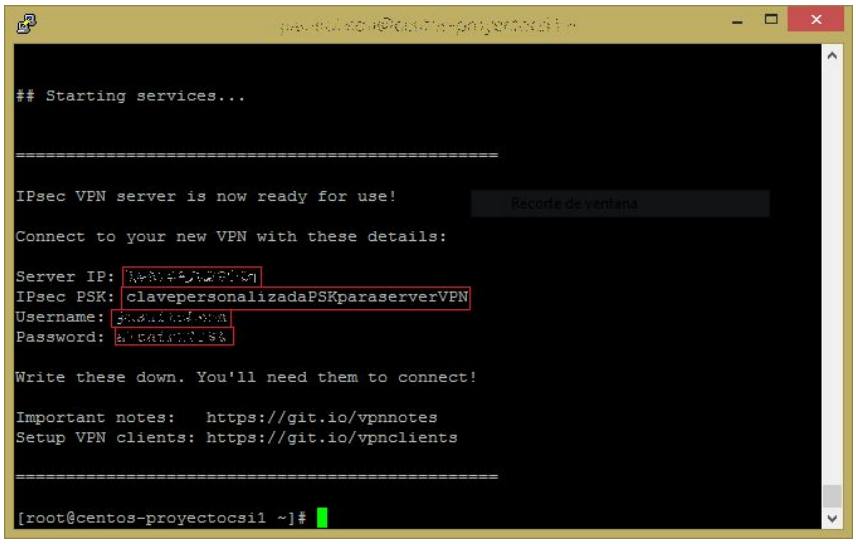
Proceso de Instalación

En nuestro caso vamos a usar un script de Lin Song basado en un trabajo de Thomas Sarlandie.

Este script, el cual analizaremos posteriormente descarga o actualiza los paquetes necesarios desde repositorio y configura el servidor VPN.

1. Descargamos como root el script desde el git del autor.
   - wget https://git.io/vpnsetup-centos -O vpnsetup.sh
2. **(Opcional)** Modificamos el script para usar nuestra propia configuración.
   - vi vpnsetup.sh
   - modificamos los campos: *[YOUR_IPSEC_PSK*[3]*, YOUR_USERNAME y YOUR_PASSWORD]*
3. Ejecutamos el script.
   - sh vpnsetup.sh

Una vez finalizado el script, nos mostrará en pantalla la configuración de acceso al servidor.



Recomendaciones de seguridad:

- Generar una clave PSK segura, puedes ver esta información de Microsoft.
- Crear distintos usuarios para cada dispositivo que se vaya a conectar, en lugar de un solo usuario para todos los dispositivos.
- Usar diferentes contraseñas en todas las cuentas y usuarios de VPN.

[3] Este script está optimizado para claves PSK de 32bits, todos nuestros clientes deberán tener la misma clave precompartida PSK.

Contenido del script

De forma ordenada realizará las siguientes acciones.

- Instalará o actualizará:
  - wget, bind-utils, openssl, iproute, grep, net-tools (requeridos para trabajos de red)
  - epel-release
  - nspr-devel, pkgconfig, pam-devel libcap-ng-devel, libselinux-devel, curl-devel (requeridos para VPN)
  - fail2ban (para protección SSH)
- Librerías que descargara:
  - Libreswan (en la que se basa el trabajo original de Thomas Sarlandie.
- Creará o modificará los siguientes archivos de configuración:
  - /etc/ipsec.conf - Configuración general de IpSec
  - /etc/ipsec.secrets - Almacenará la clave PSK
  - /etc/xl2tpd/xl2tpd.conf - Configuración XL2TPD
  - /etc/ipsec.d/passwd - Almacenará usuarios-contraseñas de forma segura
  - /etc/sysctl.conf - Añadiendo reglas para servicio VPN
- Actualizará la tabla de redireccionamiento IP para VPN.
- Creará reglas básicas de fail2ban:
  - /etc/fail2ban/jail.local
- Para terminar añadirá el inicio automático del servicio con el sistema y mostrará en pantalla la configuración creada para el usuario
- Por nuestra parte tendremos que abrir los siguientes puertos:
  - UDP: 500-1194-4500
  - TCP: 1701-1723

Archivos[4]

Estos parámetros serán creados directamente por el script, adaptados a nuestra configuración del servidor, no es necesario que lo alteremos nosotros.

Por lado derecho entendemos la parte remota de la conexión -es decir el acceso a internet- y por lado izquierdo la parte local (la propia VPN).

El servidor creará una interfaz y red virtuales en el lado izquierdo, (por defecto en nuestro script 192.168.40/) en la cual se asignará una IP para cada conexión o servicio que abra el cliente. (Esto se edita en la configuración de xl2tpd)

En el lado derecho usará una de salida a internet, la cual puede ser virtual o física, pudiendo poner incluso todas las interfaces disponibles.

/etc/ipsec/ipsec.conf[5]

Los parámetros más destacables son:

- **virtual-private**: Indica las redes privadas con las que puede trabajar.
- **interfaces**: Elige qué interfaz de conexión se desea usar para el servicio.
- **uniqueid**: Cada cliente tendrá un ID único para la conexión, permite elegir si se sobrescribirá la lista por cada conexión, si forzará a todos a usar el mismo o si permite la conexión independientemente del id de sesión.
- **left**: (parte local) indica por qué interfaz se hará la conexión.
- **left id**: dirección IP del servidor.
- **right**: (parte externa) indica por qué interfaz se hará la conexión.
- **authby**: secret o psk son los aceptables, indican que la comprobación en ambas partes se hará por PSK. pubkey (valor por defecto) indica que la verificación se hará por huella RSA o PSK.
- **dpddelay/dpdtimeout:** Ajusta los tiempos de reenvío en caso de un paquete perdido. (frecuencia de envío, máximo tiempo de intento)
- **dpdaction**: En caso de superar el dpdtimeout indica qué hacer con la información a enviar, clear (por defecto) limpia el buffer de salida y cierra conexión, hold lo mantiene para realizar el envío en caso de detectar una nueva conexión entrante del mismo dispositivo, restart reinicia la conexión y envío.
- **left | rightprotoport:** Indica en qué puerto o servicio se hará la conexión en cada lado.
- **rightaddresspool:** Rango de direcciones del lado derecho.
- **modecfgdns:** Permite elegir qué DNS usar.

/etc/xl2tpd/xl2tpd.conf[6]

- **port:** Puerto UDP para el servicio xl2tpd.
- **ip range:** Rango IP (red virtual) válido para el servicio.
- **local ip**: Dirección IP asignada al servicio.
- **pppoptfile:** Configuración pppd

Hay muchos más parámetros de configuración, pero para nuestra VPN básica no son necesario.

[4] https://wiki.strongswan.org/projects/strongswan/wiki/
[5] Este script usa ipsec 2.0, tras la versión 5.0 algunos de estos parámetros fueron deshabilitados
[6] https://linux.die.net/man/5/xl2tpd.conf

Administrar usuarios

Para añadir, modificar o eliminar usuarios **NO EJECUTAREMOS NUEVAMENTE EL SCRIPT,** ya que esto restablecerá el servidor VPN.

- Añadir usuarios:
  - Accederemos a /etc/ppp/chap-secrets y añadiremos los usuarios-contraseñas.
  - Accederemos a /etc/ipsec.d/passwd y añadiremos la siguiente estructura por cada usuario:

    user_VPN:pass_VPN_Cifrada:xauth-psk

  - La contraseña deberá estar cifrada por el protocolo correspondiente, podemos obtener la cadena cifrada mediante:

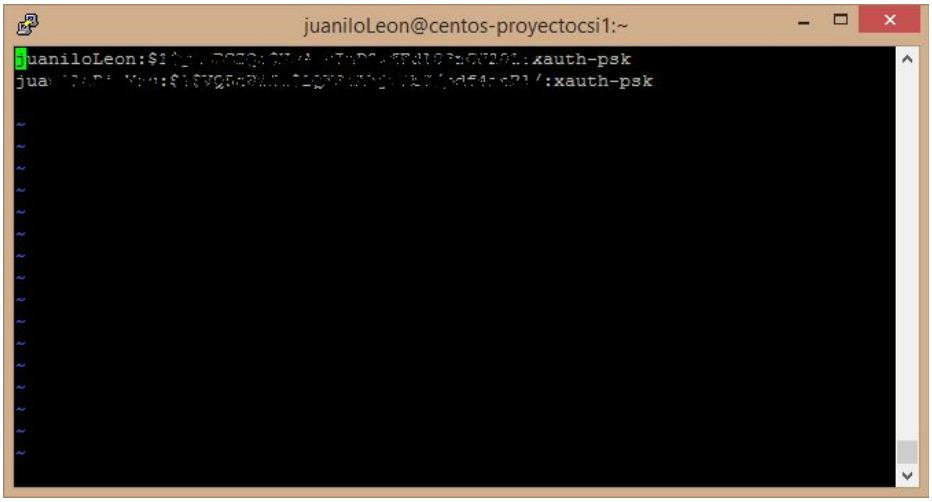
    openssl passwd -1 'pass_VPN'

  - Reiniciamos el servicio

    service ipsec restart

    service xl2tpd restart

- Eliminar usuarios:
  - Accederemos a /etc/ipsec.d/passwd y eliminaremos al usuario correspondiente:



Desinstalar el servidor

Si has decidido desinstalar el servidor VPN debes seguir los siguientes pasos:

- Parar el servicio y eliminar dependencias
  - ejecutamos el siguiente script:

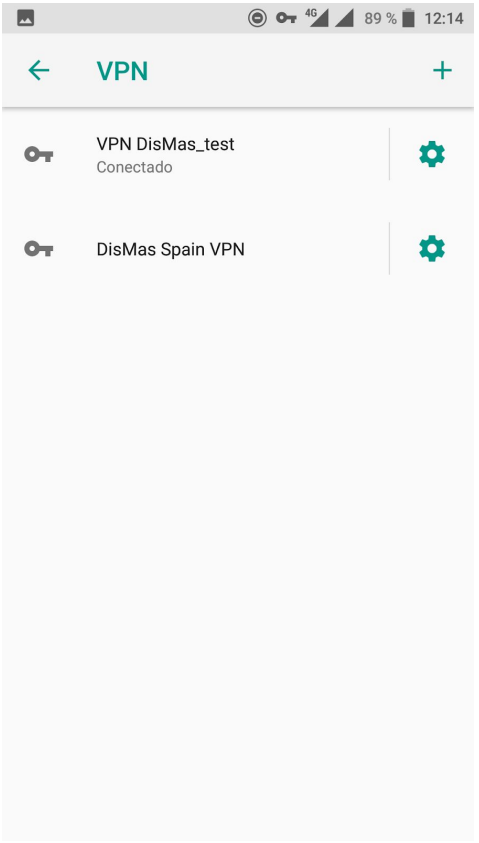
```
service ipsec stop
service xl2tpd stop
rm -rf /usr/local/sbin/ipsec /usr/local/libexec/ipsec
rm -f /etc/init/ipsec.conf /lib/systemd/system/ipsec.service \
    /etc/init.d/ipsec /usr/lib/systemd/system/ipsec.service
```

- Eliminar paquetes no necesarios
  - yum remove xl2tpd
- Modificar configuración del sistema
  - Editar /etc/sysctl.conf eliminar líneas tras *# Added by hwdsl2 VPN script*.
  - Editar /etc/rc.local eliminar líneas tras *# Added by hwdsl2 VPN script*. **Mantener la regla** *remove exit 0*
- (**OPCIONAL)** Eliminar las siguientes configuraciones
  - rm -f /etc/ipsec.conf* /etc/ipsec.secrets* /etc/ppp/chap-secrets* /etc/ppp/options.xl2tpd*
  - rm -rf /etc/ipsec.d /etc/xl2tpd
- Reiniciar el sistema.

Conexión de clientes

- Usuarios Android:
  - Accedemos a Ajustes>Red e Internet>VPN y seleccionamos la opción de *añadir nuevo VPN*.
    - *Nombre:* Campo para identificar VPN
    - *Tipo:* Seleccionamos L2TP/IPSec PSK
    - *Dirección del servidor:* URL o IP de nuestro servidor
    - *Clave precompartida de IPSec*: Nuestra clave PSK pre-compartida.
    - *Nombre de usuario:* nuestro nombre de usuario.
    - *Contraseña*: nuestra contraseña.
  - Seleccionamos la conexión que hemos creado y pulsamos *Conectar*.

Si todo ha salido bien aparecerá “conectado” y el icono VPN en la barra de notificaciones.



- Usuarios Windows.
  - La tecnología IPSec no está optimizada para Windows Vista y superior, en el caso de XP será necesario añadir al registro unos parámetros que podemos encontrar en git.io/vpnclients