Panasonic Electric Works España, S.A.
San Severo, 20, Barajas Park, 28042 Madrid, España
Tel.:+34 902 414 140 • Fax: +34 913 292 976

Número	**ITE0120090**
Título	**FPWEB. OpenVPN. Conceptos Redes Virtuales**
Versión	**1.0**

0. Sobre Este Documento

Este documento tiene como único objetivo el facilitar la ejecución de las funciones más comunes. En ningún caso, este documento tiene carácter oficial ni se podrá responsabilizar a Panasonic por las erratas o información errónea contenida en el mismo.
Panasonic declina toda responsabilidad por el uso de este documento

1. Descripción

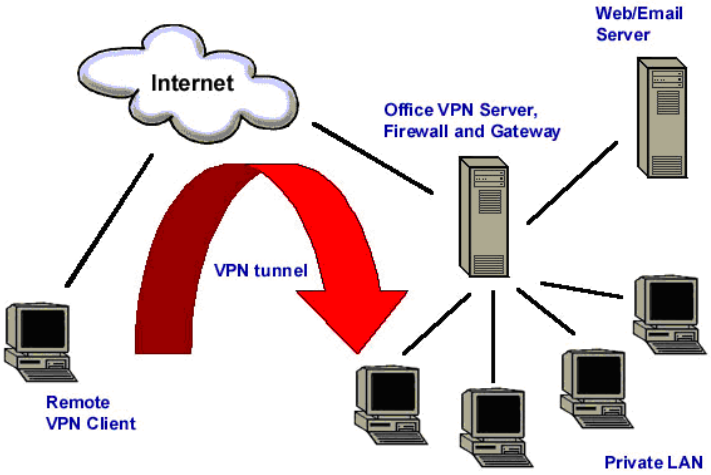
Una red privada virtual o VPN (Virtual Private Network) es una forma barata y segura para permitir el acceso a una red local desde cualquier parte del mundo. Las posibilidades de su aplicación son múltiples, que van desde solución de hardware a la solución software o mixta. Para cada uno de estos a su vez, hay muchas soluciones que no se van a tratar en este documento.

En nuestro caso estamos interesados sólo en el caso del software VPN y más particularmente a soluciones de software gratuito o mejor aún OpenSource. Su elección se deriva de su facilidad de instalación, por la gran variedad de posibles configuraciones, y finalmente, por su compatibilidad con casi todos los sistemas operativos en el mercado.

En primer lugar, vamos a empezar por decir lo que es una red VPN y que problemática resuelve.

Muchas compañías tienen la necesidad de dar a sus empleados la posibilidad de acceso a la LAN corporativa remota. Este hecho permite la posibilidad a cualquier empleado de la empresa a utilizar todos los servicios ofrecidos por la red LAN corporativa desde cualquier lugar del mundo para así poder hacer su trabajo como si estuviera realmente conectado directamente a la red LAN de la empresa. Este acceso se puede lograr a través de líneas dedicadas o por medio de un servidor de acceso remoto (RAS). El RAS (Remote Access Server) está constituido por un número de módems conectados a una máquina que actúa como un servidor. Cada módem a su vez tendrá su propia línea telefónica que permita a los empleados de la compañía conectarse a través de ella. Esta solución sin duda ofrece un alto grado de fiabilidad y seguridad, pero es, sin duda, una de las más caras.

Una solución alternativa a los RAS que parece ser flexible, económica y segura es la red privada virtual (VPN).



Una VPN permite utilizar Internet para conectarse a la LAN corporativa. Básicamente, se crea un túnel virtual en la que viajan los paquetes destinados a la LAN.

La información transmitida a través del túnel está cifrada para que nadie pueda acceder a los datos que pasan por dentro. A través de la VPN, los clientes remotos "lógicamente" pertenecen a la misma red local que la oficina central y pueden tener acceso a todas las aplicaciones y bases de datos que residen en cualquiera de los servidores de la compañía como si estuvieran físicamente en la misma LAN.

2.- Tipos de redes VPN

Haciendo una búsqueda en google se localizan tres soluciones VPN que se basan en los siguientes protocolos: IPSec, PPTP y SSL / TSL. Este último no es un protocolo, sino más bien un conjunto de librerías para el cifrado de datos y es en lo que se basa el OpenVPN.

PPTP

PPTP es un estándar emitido por el IETF y documentado en el RFC 2637. Esta norma permite establecer una conexión punto a punto entre dos anfitriones (o **hosts**) usando el encapsulado en paquetes IP y pasando este último dentro de un túnel. El protocolo PPTP se encargara de autentificar los datos de acceso del cliente y de la codificación de los datos. El protocolo PPP es el que administra los métodos utilizados para la autentificación de usuarios que serán los habitualmente utilizados por el punto-a-punto (PAP o CHAP). En cuanto a la encriptación de datos que no es proporcionada por el PPP tendrá que añadir un módulo de compresión de datos y, a continuación, parchear el sistema de modo que admita el cifrado. Esta solución es la solución utilizada por Windows para la realización de VPN entre máquinas de Microsoft y también hay hardware que soporta de forma nativa las VPN basadas en PPTP. Para utilizar VPN basada en PPTP en Linux es necesario utilizar un software específico y luego el parche en el kernel (núcleo del sistema operativo) para que sea posible el cifrado y descifrado de datos. Una solución gratuita que nos permite implementar este protocolo en Linux es el software PopTop. Con este software, varios servidores, Linux y Windows, pueden trabajar juntos en una VPN basada en PPTP. PopTop cliente está disponible para todas las versiones de Windows y Linux.

IPSec

Este es quizás el protocolo más utilizado en esta área, de hecho la mayor parte del hardware que soporta VPN lo utiliza. Este protocolo opera en la capa de red (capa 3) y nace como una parte integral de IPv6, pero también se puede utilizar IPv4. La IPSec protege cualquier protocolo que se encuentra por encima del nivel de la red. Proporciona servicios de cifrado que se utilizan para la autenticación, la integridad y la confidencialidad de los datos. Esta solución nos permite intercambiar datos cifrados con usuarios remotos y autenticados: por lo tanto, es posible crear un túnel cifrado que nos permite establecer nuestra VPN.
Este protocolo también ha sido estandarizado por la IETF. Aunque se le ha definido como un protocolo, sería más correcto referirse a ella como una arquitectura de seguridad que funciona en la capa IP. Esta arquitectura se basa en otros tres protocolos que son:

• Encabezado de autenticación (AH-Autentification Header) que se ocupa de la autenticación e integridad del mensaje;
• Carga de seguridad encapsuladora (ESP- Encapsulating Security Payload) que se encarga de la autenticación, confidencialidad e integridad de la comprobación de los mensajes;
• IKE (Internet Key Exchange), que se ocupa del intercambio de claves;

Primero entran en juego el AH y ESP, que negocian entre las dos partes una "Asociación de Seguridad" (SA) mediante la clave IKE. El SA contiene información acerca de los mecanismos de protección, y las claves que se utilizarán durante la transferencia de datos.
Además de todo lo que visto en la IPSec también incluye dos bases de datos:

• La base de datos de directivas de seguridad (SPD): contiene todas las directivas IPSec;
• La base de datos de la Asociación de Seguridad (SAD). Contiene todos los datos relacionados con SA.

IPSec soporta dos modos de funcionamiento:

- Método por Túnel
- Método de Transporte

Dependiendo del modo elegido, están protegidos sólo los protocolos de capa superior o todo el paquete IP. En el modo de transporte IPSec sólo está cifrada la carga útil (datos) del paquete IP. El enrutamiento permanece intacto, ya que no se modifica ni se cifra la cabecera IP. En modo túnel, IPsec encapsula el paquete IP original en un nuevo paquete IP. Los dos modos son compatibles con AH y ESP. Una solución de software que nos permite implementar el IPSec bajo Linux es **freeswan**.

SSL/TSL OPENVPN

SSL (Secure Sockets Layer) / TSL (Transport Sockets Layer) es la solución en la que se basa el OpenVPN. OpenVpn es un software gratuito que nos permite de una manera muy simple crear una VPN, ya sea Cliente-a-Cliente o Gateway-a-Cliente o Gateway-a-Gateway. La peculiaridad de OpenVPN es que no se va a afectar el funcionamiento del sistema operativo y por lo tanto no se requiere ningún tipo de parche. De hecho OpenVPN hace uso de varias soluciones de conexión en red proporcionada por el sistema operativo en sí mismo. OpenVPN existe para casi todas las plataformas existentes y se integra perfectamente con el sistema.

Para usarlo en Windows, sólo tiene que descargar el instalador que lo hace todo, crea un adaptador de red virtual e instalar todos los paquetes virtuales para el correcto funcionamiento del software.
El mismo paquete de la aplicación puede funcionar como servidor y cliente. Lo que cambia es sólo la configuración. OpenVPN utiliza los dispositivos TUN / TAP que son interfaces virtuales que permiten a los programas intercambiar paquetes.
Los paquetes son encriptados antes de ser enviados. La elección del tipo de dispositivo que se utilice dependerá de qué tipo de infraestructura se quiere lograr.

Con el dispositivo TUN se crea una conexión punto a punto entre el cliente y el servidor y es como si los dos están conectados a través de una interfaz PPP, en este caso OpenVPN opera en la capa IP. Es el método **Túnel IP**

> Modo Túnel. Todos los paquetes IP son encapsulados en un nuevo paquete y enviados a través del túnel siendo desempaquetados en el otro extremo y posteriormente dirigidos a su destinatario final. En este modo, se protegen las direcciones IP de emisor y receptor así como el resto de los metadatos de los paquetes.

Con el dispositivo de TAP se crea una interfaz de red virtual similar a una interfaz Ethernet que transporta tramas de Ethernet. Es el método **Puente Ethernet**

> Modo Transporte. Solo la carga útil (payload) de la sección de datos es cifrada y encapsulada. La sobrecarga entonces, es sensiblemente menor que en el caso anterior, pero se exponen los metadatos a posibles atacantes que podrán ver quien se está comunicando con quien.

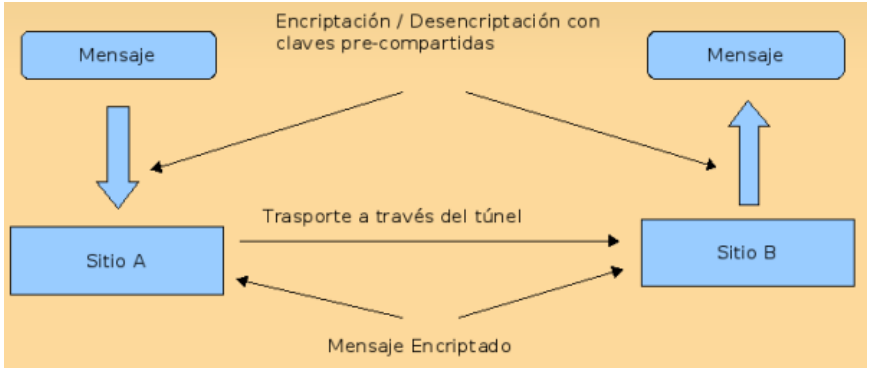
3.- Seguridad en Redes Virtuales VPN

Para cifrar datos se usan contraseñas o claves de cifrado.

OpenVPN tiene dos modos considerados seguros, uno basado en claves estáticas pre-compartidas y otro en SSL/TLS usando certificados y claves RSA.
Cuando ambos lados usan la misma clave para cifrar y descifrar los datos, estamos usando el mecanismo conocido como “clave simétrica” y dicha clave debe ser instalada en todas las máquinas que tomarán parte en la conexión VPN. Si bien SSL/TLS + claves RSA es de lejos la opción más segura, las claves estáticas cuentan con la ventaja de la simplicidad. Veremos a continuación ese método y otros que aportan mayor seguridad y facilidad de distribución.

Cifrado simétrico y claves pre-compartidas

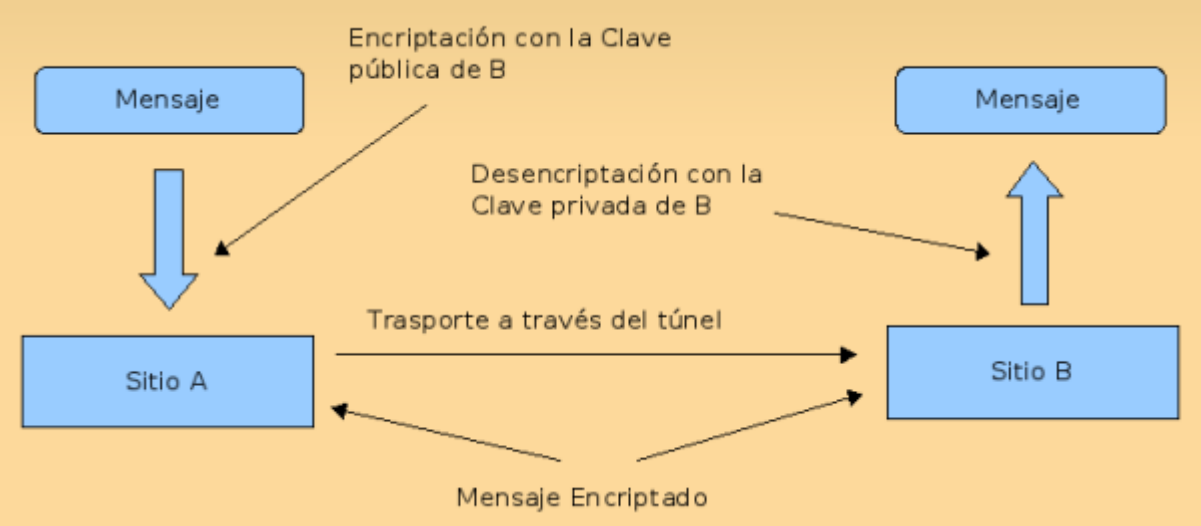
Cualquiera que posea la clave podrá descifrar el tráfico, por lo que si un atacante la obtuviese comprometería el tráfico completo de la organización ya que tomaría parte como un integrante más de la VPN.



Es por ello que se han de prever mecanismos para el cambio de las claves cada cierto período, asociando a las mismas ciertos períodos de validez, llamados “tiempo de vida” o “lifetime”. Una buena combinación de tiempo de vida y longitud de la clave asegurarán que un atacante no pueda descifrar la clave a tiempo, haciendo que cuando finalmente la obtenga (porque lo hará), ya no le sirva por estar fuera de vigencia.

Cifrado asimétrico con SSL/TLS

SSL/TLS usa una de las mejores tecnologías de cifrado para asegurar la identidad de los integrantes de la VPN.
Cada integrante tiene dos claves, una pública y otra privada.
La pública es distribuida y usada por cualquiera para cifrar los datos que serán enviados a la contraparte quien conoce la clave privada que es imprescindible para descifrar los datos. El par de clave pública/privada es generado a partir de algoritmos matemáticos que aseguran que solo con la clave privada es posible leer los datos originales.
Si se encontrase un modo de quebrar la seguridad que estos algoritmos proporcionan, todas las conexiones cuya integridad depende de ellos se verían potencialmente comprometidas.



Es de destacar que la clave privada debe permanecer secreta mientras que la clave pública debe ser intercambiada para que nos puedan enviar mensajes.

Seguridad SSL/TLS

Las bibliotecas SSL/TLS son parte del sofware OpenSSL que viene instalado en cualquier sistema moderno e implementa mecanismos de cifrado y autenticación basados en certificados. Los certificados generalmente son emitidos por entidades de reconocida confiabilidad aunque también podemos emitirlos nosotros mismos y usarlos en nuestra propia VPN. Con un certificado firmado, el dueño del mismo es capaz de demostrar su identidad a todos aquellos que confíen en la autoridad certificadora que lo emitió.

Panasonic

4.- Motivos para seleccionar OpenVPN

Se opta por OpenVPN. Se descarta la solución PPTP ya que se considera la menos segura y se considera que la seguridad y confidencialidad de los datos parece ser una prioridad para las empresas que desean establecer una VPN.

En cuanto a la solución basada en IPSec, a pesar de ser considerado muy segura en comparación con otras soluciones, parece ser complicada su instalación y configuración.

Para crear una VPN con IPSec se tienen que hacer muchos cambios en el sistema que se va a conectar y en particular en Linux se debe aplicar una serie de parches y luego continuar con la configuración del sistema que ya de por si es difícil de entender.

Asimismo, no se sabe en qué medida existen soluciones que funcionen correctamente en diferentes sistemas operativos.

Diferencias entre IPSec y OpenVPN

IPsec	OpenVPN
Estándar de la tecnología VPN	No compatible con IPsec
Plataformas de hardware (dispositivos, aparatos)	Solo en computadoras, pero en todos los sistemas operativos disponibles, ya comienzan a encontrarse dispositivos que cuentan con OpenVPN
Tecnología conocida y probada	Probada y sigue en crecimiento
Muchas interfaces gráficas disponibles	Sin interfaces gráficas profesionales, aunque ya existen algunos proyectos prometedores
Modificación compleja del stack IP	Tecnología sencilla
Necesidad de modificaciones críticas al kernel	Interfaces de red y paquetes estandarizados
Necesidad de permisos de administrador	Ejecuta en el espacio del usuario y puede ser chroot-ed
Diferentes implementaciones de distintos proveedores pueden ser incompatibles entre si	Tecnologías de cifrado estandarizadas
Configuración compleja y tecnología compleja	Facilidad, buena estructuración, tecnología modular y facilidad de configuración
Curva de aprendizaje muy pronunciada	Fácil de aprender e implementar (incluso para principiantes)
Necesidad de uso de múltiples puertos y protocolos en el firewall	Utiliza sólo un puerto del firewall
Problemas con direcciones dinámicas en ambas puntas	Trabaja con servidores de nombres dinámicos como DynDNS o No-IP con reconexiones rápidas y transparentes
Problemas de seguridad de las tecnologías IPsec	SSL/TLS como estándar de criptografía
	Control de tráfico (Traffic shaping)
	Velocidad (más de 20 Mbps en máquinas de 1Ghz)
	Compatibilidad con firewall y proxies
	Ningún problema con NAT (ambos lados puede ser redes NATeadas)
	Posibilidades para road warriors

OpenVPN ha sido la solución que era más adecuada para nuestro caso, de hecho la fase de instalación y configuración es comprensible.

Existen versiones para casi todas las plataformas o sistemas operativos.

También en internet se puede encontrar mucha información que explica detalladamente todo lo relativo a OpenVPN, desde la fase de instalación, configuración y gestión de la aplicación.

Otra ventaja de este software es que el mismo paquete se puede ejecutar de forma independiente desde el servidor o desde el cliente, lo que cambia es la forma de configurarlos.

Ayúdenos a Mejorar

Si lo desea puede ponerse en contacto con nosotros en la siguiente dirección de correo:

soporte.tecnico@eu.panasonic.com

Si desea realizar cualquier consulta sobre este informe que no le haya quedado claro, indicar una errata, corregir la información o simplemente evaluar la utilidad de este informe, le rogamos que incluya en el asunto del mail el número del mismo.

Así mismo, estaremos encantados de atender sus solicitudes sobre futuros informes o acciones que considere que Panasonic debería realizar por lo que le ruego utilice este mail como buzón de sugerencias.