Hackers y Programadores Hispanos

Redes VPN

- Que es
- Como funciona
- Para que sirve
- Ventajas

Ángel G. González R.

Redes VPN

Una red privada virtual (RPV), en inglés: Virtual Private Network (VPN) es una tecnología de red de computadoras que permite una extensión segura de la red de área local (LAN) sobre una red pública o no controlada como Internet. Permite que la computadora en la red envíe y reciba datos sobre redes compartidas o públicas como si fuera una red privada con toda la funcionalidad, seguridad y políticas de gestión de una red privada. La VPN además es una privada virtual capaz de conectar varios dispositivos como si se encontrasen físicamente en el mismo lugar, emulando las conexiones de redes locales. Virtual, porque conecta dos redes físicas; y privada, porque solo los equipos que forman parte de una red local de uno de los lados de la VPN pueden acceder.

Como funciona:

Al conectarnos a una VPN, lo haremos utilizando una suerte de túnel, un vocablo que se emplea para indicar que los datos se encuentran cifrados en todo momento, desde que entran hasta que salen de la VPN, y que se lleva a cabo mediante distintos protocolos que los protegen. Ahora bien, existe una excepción con el PPTP –utiliza una combinación de algoritmos inseguros como MS-CHAP v1/2-.

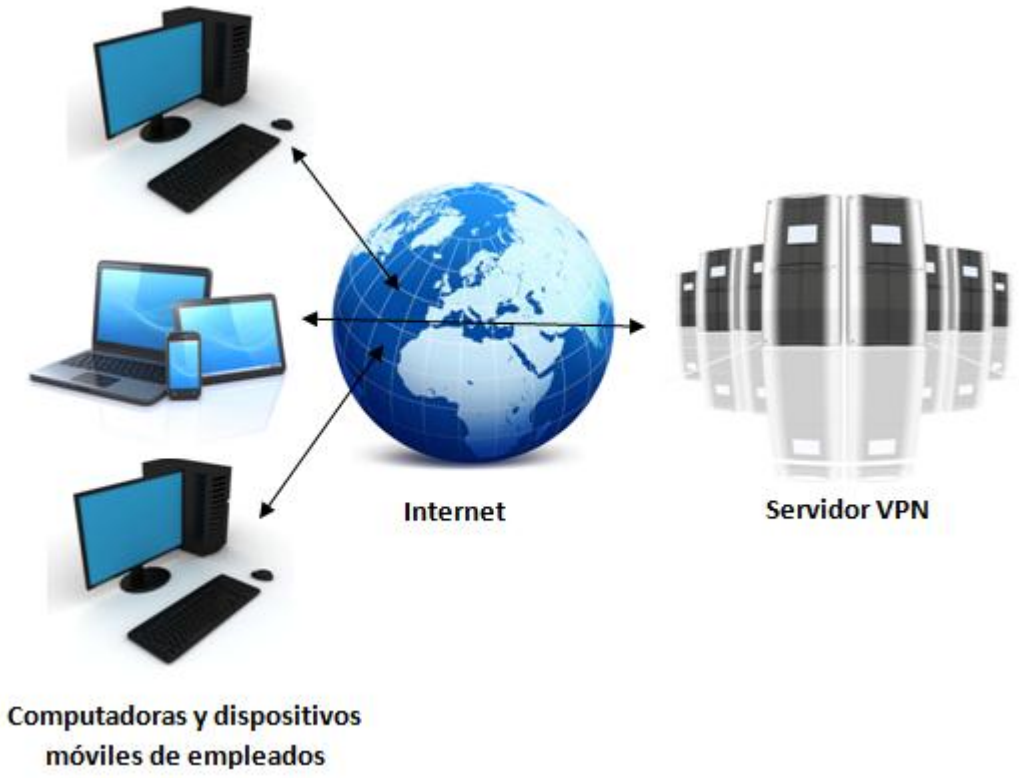
Lo que hará nuestro sistema al tratar de visitar una página es encapsular la petición y mandarla a través de Internet a nuestro proveedor de VPN. Este los desencapsulará haciendo que sigan su curso habitual: saldrán por su router de red y, posteriormente, se reenviará el paquete.

En conjunto con lo anterior, una implementación correcta de esta tecnología permite asegurar la confidencialidad e integridad de la información.

Diagrama red VPN

Como puede suponerse, a través de una VPN pasa información privada y confidencial que en las manos equivocadas, podría resultar perjudicial para cualquier empresa. Esto se agrava aún más si el empleado en cuestión se conecta utilizando un Wi-Fi público sin protección. Afortunadamente, este problema

puede ser mitigado cifrando los datos que se envían y reciben. Para poder lograr este objetivo, se pueden utilizar los siguientes protocolos:



IPsec (Internet Protocol Security): permite mejorar la seguridad a través de algoritmos de cifrado robustos y un sistema de autentificación más exhaustivo. IPsec posee dos métodos de encriptado, modo transporte y modo túnel. Asimismo, soporta encriptado de 56 bit y 168 bit (triple DES).

PPTP/MPPE: tecnología desarrollada por un consorcio formado por varias empresas. PPTP soporta varios protocolos VPN con cifrado de 40 bit y 128 bit utilizando el protocolo Microsoft Point to Point Encryption (MPPE). PPTP por sí solo no cifra la información.

L2TP/IPsec (L2TP sobre IPsec): tecnología capaz de proveer el nivel de protección de IPsec sobre el protocolo de túnel L2TP. Al igual que PPTP, L2TP no cifra la información por sí mismo.

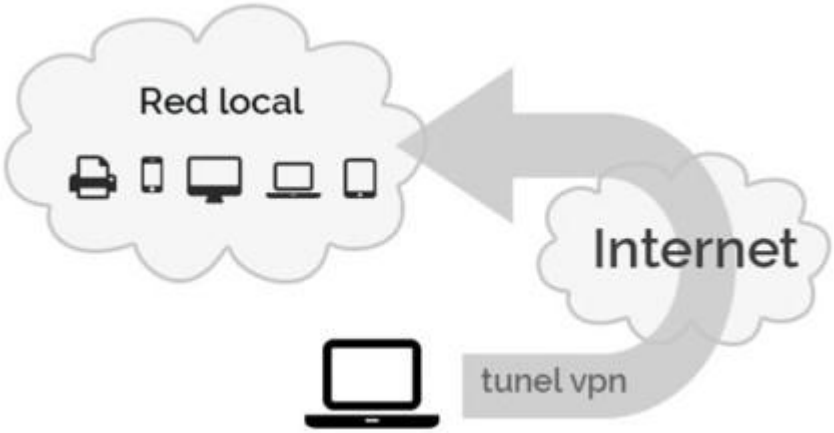
Parte de la protección de la información que viaja por una VPN es el cifrado, no obstante, verificar que la misma se mantenga íntegra es igual de trascendental. Para lograr esto, IPsec emplea un mecanismo que si detecta alguna modificación dentro de un paquete, procede a descartarlo. Proteger la confidencialidad e integridad de la información utilizando una VPN es una buena medida para navegar en Wi-Fi públicos e inseguros incluso si no se desea acceder a un recurso corporativo.

Por otro lado, aquellos usuarios hogareños que deseen utilizar una red VPN, pueden elegir entre servicios gratuitos y otros de pago. Es importante mencionar que aquellos libres suelen funcionar más

lento que uno que no lo es. También, recomendamos la lectura de nuestra Guía de Seguridad en redes inalámbricas en donde se repasan otras medidas que se pueden adoptar para utilizar una conexión inalámbrica pública de forma más segura.

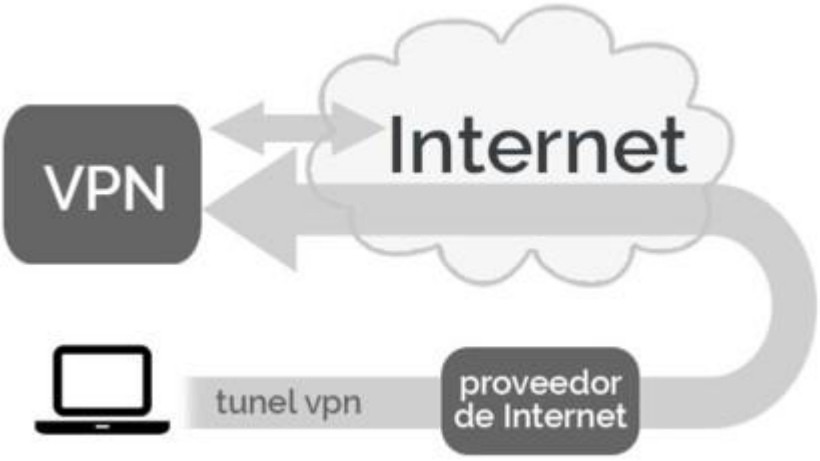
También podemos ver este video donde se explica que es la red VPN y cómo es que funciona: https://youtu.be/IzxC6UPilqQ

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. Obtienes 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.



Sin embargo, es otra peculiaridad de las conexiones VPN la que las está volviendo tan de moda hoy en día: los túneles de datos. Normalmente, mientras usas Internet tu dispositivo se pone en contacto con tu proveedor de Internet, que es el que conecta con los distintos servicios web para ofrecerte, por ejemplo, los vídeos de YouTube.

Cuando te conectas a una conexión VPN, esto cambia. Todo tu tráfico de red sigue yendo desde tu dispositivo a tu proveedor de Internet, pero de ahí se dirige directo al servidor VPN, desde donde partirá al destino. Idealmente la conexión está cifrada, de modo que tu proveedor de Internet realmente no sabe a qué estás accediendo. A efectos prácticos, tu dirección IP es la del servidor VPN: en muchos aspectos es como si estuvieras físicamente ahí, conectándote a Internet.



Para que sirve

Las redes VNP también son empleadas habitualmente para saltarse restricciones geográficas de determinados servicios. Por ejemplo, pongamos el caso de que la visualización de un contenido en vídeo únicamente se encuentra disponible para usuarios de los Estados Unidos. Pues bien, este tipo de conexión nos permitirá decirle a la web que nos encontramos en este país.

Cuando hablamos de restricciones, no podemos dejar de referirnos a las que tienen que ver con la censura impuesta por determinados gobiernos totalitarios a sus ciudadanos. Una manera de ver las noticias e información del mundo exterior sin vetos que, no obstante, tampoco es perfecta.

Es un secreto a voces que son especialmente importantes en el entorno corporativo, pero sus usos no acaban ni mucho menos ahí. Estos son los principales usos de las conexiones VPN.

1. Teletrabajo

El uso más obvio de una conexión VPN es la interconectividad en redes que no están físicamente conectadas, como es el caso de trabajadores que están en ese momento fuera de la oficina o empresas con sucursales en varias ciudades que necesitan acceder a una única red privada.

Desde el punto de vista de la seguridad, permitir el acceso indiscriminado a la red propia de una empresa desde Internet es poco menos que una locura. Aunque el acceso esté protegido con una contraseña, podría ser capturada en un punto de acceso WiFi público o avistada por un observador malintencionado.

Teletrabajo Teletrabajo y VPN son conceptos que con frecuencia van de la mano

Por el contrario, el riesgo disminuye si el trabajador y la empresa se conectan mediante una conexión VPN. El acceso está protegido, la conexión está previsiblemente cifrada y el trabajador tiene el mismo acceso que si estuviera presencialmente ahí.

2. Evitar censura y bloqueos geográficos de contenido

Con el apogeo de Internet y la picaresca tanto de los proveedores de contenidos como de los usuarios, se han ido popularizando otros usos más lúdicos de las conexiones VPN, muchos de ellos relacionados con un concepto muy sencillo: falsear dónde estás.

Al conectarte con VPN, tu dispositivo se comunica con el servidor VPN, y es éste el que habla con Internet. Si tú estás en China y el servidor VPN está en Estados Unidos, generalmente los servidores web creerán que estás navegando desde este país, dejándote acceder a los contenidos disponibles solo allí, como podría ser Netflix.

De igual modo, esta misma lógica se puede usar para acceder a aquellos contenidos que estuvieran censurados o bloqueados en tu país, pero no allí donde se encuentra el servidor VPN. Así es como millones de ciudadanos chinos logran conectarse a Facebook y otras 3.000 webs bloqueadas en el país.

Desbloqueo Geografico El firewall de China impide la conexión con Facebook, pero no con un VPN (que después conecte con Facebook)

3. Capa extra de seguridad

Aunque no es estrictamente necesario, sí es común que las conexiones VPN vengan acompañadas de un cifrado de los paquetes que se transmiten con ellas, por lo que es normal oir la recomendación de que, si necesitas conectarte a un punto de acceso Wi-Fi público, al menos uses te conectes con una VPN.

Iniciar sesión en tus cuentas bancarias mientras estás conectado a una red WiFi pública en la que no confías probablemente no sea la mejor idea del mundo, pues es relativamente sencillo para un ladrón capturar los paquetes sin cifrar y hacerse con tus cuentas de usuario. Aquí es donde entra la capa extra de seguridad que puedes conseguir mediante una conexión VPN, pues los paquetes se enviarían cifrados, de modo que aquel que está escuchando probablemente no podría hacer nada con ellos.

No obstante, hay letra pequeña en esto, pues mientras estás desconfiando de la red pública Wi-Fi, estás poniendo toda tu fé en el servidor de VPN, que puede de igual modo capturar todo tu tráfico, guardar registros de lo que haces o incluso vender tu ancho de banda al mejor postor. Una VPN es tan segura y

útil como su proveedor. Si no confías en tu VPN, no la uses, pues en vez de tener una capa de seguridad adicional, tendrás al enemigo en casa y mirando absolutamente todo lo que haces en Internet.

4. Descargas P2P

Otro uso común de las conexiones VPN se encuentra en las descargas P2P, lo cual en estos tiempos generalmente es sinónimo de descargar desde BitTorrent. Antes de que me pongas un parche en el ojo, una pata de palo y me obligues a pasar por la quilla, las conexiones VPN también tienen usos en la descarga P2P aunque bajes torrents completamente legales.

Desgraciadamente es cada vez común que los proveedores de Internet decidan meter las narices en cómo enviamos y recibimos los ceros y unos en la Red, y aunque les encanta que visitemos páginas web normales, que descarguemos no les hace tanta gracia: demasiado tráfico, y además probablemente te estás descargando algo ilegal.

Algunos proveedores bloquean por completo las descargas P2P, mientras que otros simplemente la boicotean para que funcione mal y te rindas por ti mismo. Igual que puedes usar una conexión VPN para evitar la censura de tu país, también puedes en ocasiones evitar que tu proveedor de Internet boicotee tus descargas P2P.

Ventajas de una red VPN

Usar una VPN implica que podremos acceder a prácticamente cualquier lugar de la red sin ningún tipo de restricción geográfica, **sin importar dónde nos encontremos físicamente**. ¿La razón? Que nos permitirá acceder a través de varios servidores emplazados en otro lugar del mundo distinto al que nos hallamos.

La **seguridad y privacidad** son otros puntos a su favor, en especial si necesitamos enviar o recibir información de carácter sensible a través de la red. Y si bien siempre podemos decantarnos por servicios proxy y herramientas que ocultan la IP de nuestro dispositivo, al decantarnos por una VPN estamos escogiendo establecer una conexión segura entre el ordenador y el servidor.

Ya **en un contexto más empresarial**, hace posible que los empleados de una compañía **accedan remotamente a sus redes y servidores** sin que se vea comprometida la seguridad. Otra de sus virtudes es que no se trata de servicios demasiado caros y que incluso encontramos opciones que merecen la pena de manera gratuita.

Para acabar, son **fáciles de utilizar**, nos dejan conectarnos y desconectarnos fácilmente a nuestro antojo (una vez configurada) y funciona con múltiples aplicaciones enrutando todo el tráfico de Internet.

Ahora que ya sabemos qué es una conexión VPN y para qué sirve, es hora de resumir una lista de las ventajas e inconvenientes que te supone el uso de esta tecnología. Primero, la parte positiva:

- **Funciona en todas las aplicaciones**, pues enruta todo el tráfico de Internet, a diferencia de los servidores proxy, que solo puedes usar en el navegador web y un puñado de aplicaciones más que te dejan configurar las opciones de conexión avanzadas.
- **Se conecta y desconecta fácilmente**. Una vez configurado, puedes activar y desactivar la conexión a tu antojo.
- **Seguridad adicional** en puntos de acceso WiFi, siempre y cuando la conexión esté cifrada, claro
- **Falseo de tu ubicación**, como ya hemos visto en el apartado anterior, una conexión VPN es un modo eficaz de evitar la censura o acceder a contenido limitado a cierta región.
- **Tu proveedor de Internet** no puede saber a qué te dedicas en Internet. ¿No te apetece que tu proveedor de Internet sepa que te pasas horas viendo vídeos de gatitos en YouTube? Con una VPN no sabrán a que te dedicas, pero ojo, que sí lo sabrá la compañía que gestiona el VPN.

Consideraciones que debes tomar en cuenta

Hasta ahora todo muy bonito, usar conexiones VPN parece estar lleno de ventajas: más seguridad, privacidad mejorada, salto de los bloqueos geográficos... Antes de que te lances a comprar un servicio de VPN o registrarte en uno gratuito, hay unos cuantos apartados que debes tener en cuenta:

- **El precio**. Aunque hay servicios VPN gratuitos, obviamente no puedes esperar mucho de ellos, pues con frecuencia estarán muy limitados, serán muy lentos o no sean muy de fiar. Hay algunas excepciones, no obstante.
- **La velocidad se resiente**. La diferencia entre conectarte a Internet directamente o que tus datos tracen una ruta que atraviesa medio mundo puede ser abrumadora. Si tu servidor VPN está muy lejos, experimentarás mucha latencia a la hora de navegar por la red. Además de latencia, es normal que la velocidad de descarga y subida máxima estén limitadas.
- **Su seguridad no es infalible**. Esto ya lo hemos dicho varias veces, pero nunca está de más repetirlo. Solo porque el icono de la conexión tenga un candado no quiere decir que la conexión sea segura, especialmente si estamos hablando de conexiones VPN basadas en el protocolo PPTP.
- **No siempre pueden falsear tu ubicación**. Especialmente en el móvil, cada vez hay más tecnologías por las cuales se puede triangular y aproximar tu ubicación más allá de tu dirección IP.

- **No te proporcionan anonimato**. Usar una VPN no supone que la navegación sea anónima. La combinación ganadora para un mayor anonimato, si hacemos caso a Edward Snowden, es usar a la vez una conexión VPN y Tor.

Referencias:

https://www.nobbot.com/tecnologia/mi-conexion/vpn-%C2%BFque-es-y-para-que-sirve/

https://www.welivesecurity.com/la-es/2012/09/10/vpn-funcionamiento-privacidad-informacion/

https://es.wikipedia.org/wiki/Red_privada_virtual#Características_básicas_de_la_seguridad

https://www.xatakandroid.com/sistema-operativo/como-configurar-y-para-que-sirve-usar-una-vpn-en-android

Autor: Ángel Gabriel González Rodríguez