Revista de Marina Nº 962, pp. 90-91
ISSN 0034-8511

PROTEJAMOS NUESTRA PRIVACIDAD

Eduardo Fainé Celis*

En el artículo anterior vimos que las redes inalámbricas públicas y privadas adolecen de una falla de seguridad que permitiría a quien tenga los conocimientos, acceder al tráfico de información de los usuarios para fines ilícitos. El viajero del ejemplo ingresaba a una red pública y ponía en riesgo sus datos personales al hacerlo.

Afortunadamente, existen herramientas para reducir el peligro de que nuestros movimientos en la red sean interceptados por terceros. Una de estas herramientas se denomina *Virtual Private Network*, abreviado VPN.

Este acrónimo, que aparece frecuentemente en los textos técnicos, consiste en un método para encriptar la información que se mueve entre dos puntos de una red, de manera que los otros participantes no sean capaces de interpretar su contenido.

De acuerdo con el sitio www.welivesecurity.com, una VPN se define como "una tecnología de red que se utiliza para conectar una o más computadoras a una red privada utilizando Internet. Las empresas suelen utilizar estas redes para que sus empleados, desde sus casas, hoteles, etc., puedan acceder a recursos corporativos que, de otro modo, no podrían. Sin embargo, conectar la computadora de un empleado a los recursos corporativos es solo una función de una VPN".

En primer término, una VPN permite conectarse de manera segura y remota a redes privadas. Asimismo permite enlazar diferentes redes o servidores, de manera más segura. En concreto, y para los nuestros fines, nos permite navegar seguros en redes WiFi públicas como las de las cafeterías, aeropuertos u hoteles. En ciertos casos pueden servir para eludir restricciones a la navegación o censuras en determinados sitios.

Una conexión opera como una ruta con puntos de inicio y término y puntos de control de la integridad de los paquetes de información que viajan por ésta. Lo que hace una VPN es agregar una capa de cifrado y autenticación a la ruta, creando un túnel (VPN *tunneling*) dentro de la red. Así, aun cuando estos paquetes cifrados de información pasen por múltiples nodos en su tránsito de un computador a otro, su contenido solo podrá ser descifrado por el receptor final, evitando la posibilidad de ser leídos en el camino. Por otra parte, la capa de autenticación permite verificar la identidad del emisor y del receptor, dejando fuera a cualquier intruso.

Según el sitio www.xataca.com, la ventaja de una VPN es que permite crear una red local sin que sus componentes estén físicamente conectados entre sí, empleando para esto a la Internet.

No siendo un método infalible para proteger la información, la VPN agrega un par de capas de seguridad que nos ayudarán a lograrlo. Sin embargo, hay que tener en cuenta que, como todas las tecnologías, tiene ventajas y desventajas. Aquí enumero las que se menciona en www.xataca.com.

Ventajas

➢ El teletrabajo, que permite a empleados fuera de una oficina acceder a los

* Capitán de Navío. Magister en Ciencias Navales y Marítimas. Magister en Diseño y Comunicación Multimedia. Magno Colaborador de la Revista de Marina desde 2014. (eduardofaine@hotmail.com).

contenidos de los servidores corporativos desde redes remotas.
- Evitar la censura y los bloqueos geográficos en aquellos lugares donde se aplican, como por ejemplo en países totalitarios.
- Una capa de seguridad. No es que todas las VPN tengan el servicio de encriptación, pero una gran parte de ellas sí lo hace, proveyendo esta seguridad adicional a nuestro tráfico.
- Descargas de contenidos P2P, como es el caso de *bitTorrent*. Dado que esta práctica significa la transferencia de grandes cantidades de datos, algunos servicios de Internet los bloquean o reducen su ancho de banda para disuadir de su uso. Las VPN pasan por encima de estos bloqueos, ya que su contenido es desconocido.
- Funciona en todos los dispositivos y sistemas operativos.
- Se activa y desactiva tan solo con abrir o cerrar el programa.
- Permite falsear la ubicación del usuario, esto es ideal para ver contenidos de Netflix que solo están disponibles en otras latitudes.
- El proveedor de Internet no puede conocer el contenido del tráfico.

Desventajas

- Hay servicios gratis y otros pagados. Como es obvio, los gratis son más limitados, o más lentos, o menos confiables, aun cuando pueda haber honrosas excepciones.
- Hay pérdidas en velocidad. Como la conexión pasa por un módem virtual que puede estar en cualquier parte del mundo, es esperable que los tiempos de subida y descarga aumenten.
- Son seguros, pero no perfectos. Existen diferentes protocolos para crear VPN. El más seguro según el mismo sitio mencionado es IPsec (*Internet Protocol Security*). Otros son PPTP/MPPE y L2TP/IPsec (L2TP sobre IPsec). En estos dos últimos casos, podemos decir que el nombre representa la tecnología de túnel y el apellido aporta el cifrado.
- No siempre logran ocultar o falsear la localización del usuario, en especial con equipos móviles.
- No garantizan el anonimato durante la navegación.

Yendo a la práctica

Existen numerosos proveedores del servicio de VPN en el mercado, demasiados para la extensión de este artículo y asimismo para analizar cada uno de ellos. Los hay pagados como NordVPN, ExpressVPN, CyberGhost, IPVanish, TrustZone y otros que cobran cifras razonablemente bajas por su servicio; también los hay gratis, como Opera, TunnelBear, Windscribe, HotspotShield, Speedify y una larga lista de etcétera. Como es de suponer, los sistemas gratis tienen bastantes limitaciones en cuanto a velocidad o al volumen de data mensual que permiten manejar; por otra parte, nada es gratis en esta vida y los proveedores deben encontrar una forma de financiarse, la cual puede ser mediante cuentas premium pagadas, o bien vendiendo cierta información que pueda serle útil a una tercera parte. Por esto, antes de decidir si pagar o no por este servicio, es bueno analizar cuán segura queremos que esté nuestra cuenta bancaria cuando la revisemos en el café de la esquina durante las vacaciones.

Una última opción, más avanzada y para valientes, es crear nuestro propio servidor de VPN, descargando el programa OpenVPN desde el sitio https://openvpn.net/index.php/open-source/downloads.html, que tiene instrucciones en línea para hacerlo tanto en ambiente Windows (https://community.openvpn.net/openvpn/wiki/Easy_Windows_Guide) como para Mac (http://www.podfeet.com/blog/tutorials-5/how-to-set-up-a-vpn-server-using-a-mac-2/).

Por lo tanto, si los lectores se animan a intentarlo, pueden llegar a obviar las limitaciones de los servicios gratuitos y obtener su propia red virtual y segura sin pagarle un dólar a nadie.

* * *