UNIVERSIDAD CATÓLICA DE CÓRDOBA
JESUITAS

VPNs - Virtual Private Networks

Seguridad Informática

Por: Ticiana Cobresi
Nara Abril Nanfara

Profesor: Mariano Aliaga

2020

Conceptos teóricos básicos de VPN

Definición

Analogía

Internet es como una autopista virtual por la que circulamos en unas motos luminosas tan llamativas como las de la película Tron. Visitamos nuestros sitios web favoritos, hacemos compras en tiendas, consultamos nuestras acciones, leemos las noticias de nuestras fuentes preferidas, jugamos y mucho más.

Cualquiera que desee lo puede seguir por estas autopistas y estos senderos digitales para ver su actividad en línea, quién es usted o los sitios que le gusta visitar, etc. Y puede ser peor: le pueden seguir hasta casa. Está localizable.

Una VPN sería como un velo que lo oculta y le permite usar la red de forma anónima. Es como cambiar la moto luminosa que va dejando un rastro por un coche alquilado con las ventanillas tintadas. El cifrado de datos oculta sus huellas y, de este modo, queda escondido detrás de una dirección IP falsa, sin nada que temer.

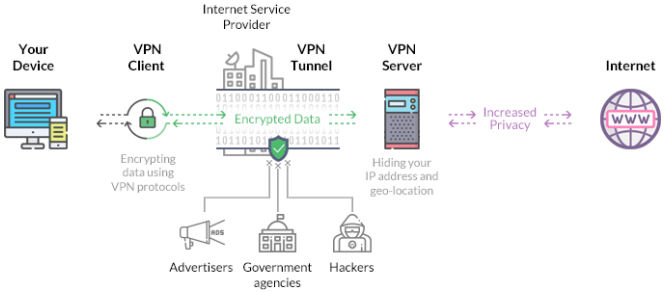
Formalmente

Una Red Privada Virtual (VPN, *Virtual Private Network*) es una red privada que utiliza la infraestructura de una red pública para poder transmitir información.

Las VPN más comunes son las VPN físicas, como la red de área local (LAN). Las grandes organizaciones implementan una red de área amplia que cubre múltiples áreas al mismo tiempo. Sin embargo, llega un momento en que ya no es factible colocar un cable físico para configurar una red física privada. Donde las oficinas están separadas por cientos o miles de millas, los costos y las dificultades involucradas hacen que una red física sea imposible. En tal caso, es mejor usar los recursos en Internet para crear una red privada. Por lo tanto, las empresas establecen una VPN (red privada virtual), que replica las características de una red física privada. Mediante el uso de una VPN, es posible que los empleados de la empresa accedan a la red de área local o amplia incluso cuando trabajan de forma remota. La VPN encripta el tráfico desde la computadora remota a la red de la compañía, manteniendo la información lejos de posibles hackers.

Una red privada virtual es una implementación o sistema que habilita una comunicación segura a través de un medio inseguro, siendo transparente para el usuario o aplicación que realiza y recibe la comunicación.

Cuando usa Internet, hay un proceso constante en el que su dispositivo intercambia datos con otras partes en la web. Una VPN crea un túnel seguro entre su dispositivo (por ejemplo, teléfono inteligente o computadora portátil) e Internet. La VPN le permite enviar sus datos a través de una conexión segura y encriptada a un servidor externo: el servidor VPN. Desde allí, sus datos se enviarán a su destino en Internet.



¿Cómo funciona?

Sin una VPN

Cuando accede a una página web sin una VPN, usted se conecta a esa página a través de su proveedor de servicios de internet o ISP, por sus siglas en inglés. El ISP le asigna una dirección IP única que puede ser utilizada para identificarle en la página web. Debido a que su ISP maneja y dirige todo su tráfico, este puede ver las páginas web que visita. Y su actividad puede ser vinculada a usted mediante esa dirección IP única.

Con una VPN

1. El software VPN en su computadora encripta su tráfico de datos y lo envía (a través de su proveedor de servicios de Internet) al servidor VPN a través de una conexión segura.
2. El servidor VPN descifra los datos cifrados de su computadora.
3. El servidor VPN enviará sus datos a Internet y recibirá una respuesta, que es para usted, el usuario.
4. A continuación, el servidor VPN vuelve a cifrar el tráfico y se lo envía de vuelta.
5. El software VPN de su dispositivo descifrará los datos para que pueda comprenderlos y utilizarlos.

Su tráfico todavía pasa por su ISP, pero su ISP ya no puede leerlo ni ver su destino final. Las páginas web que usted visita ya no pueden ver su dirección IP original, solo la dirección IP del servidor VPN, la cual es compartida por muchos otros usuarios y cambia regularmente.

Conceptos

Proxy

Suele confundirse VPN con proxy y hasta algunas proxies se autodenominan VPNs gratuitas para captar más usuarios. La diferencia es sustancial:

Si bien el servidor VPN actúa en cierto sentido como proxy, o suplente, para su actividad web: en lugar de su dirección IP y ubicación reales, las páginas web que usted visite solo verán la dirección IP y la ubicación del servidor VPN. Sin embargo, un proxy no le brinda ningún tipo de protección adicional, como la encriptación. De forma más específica el VPN tiene como fin velar por la seguridad de sus usuarios, el proxy es simplemente un intermediario.

Autenticación

Una vez autenticados, el cliente VPN y el servidor VPN pueden estar seguros de que solo están hablando entre sí y nadie más.

Tunelización

Las VPN también protegen la conexión entre el cliente y el servidor utilizando tunelización y encriptación. En algunas ocasiones se denomina a las redes privadas virtuales como túneles, ya que estas transportan la información por un canal público, pero aislando la información del resto y consecuentemente creando unas paredes virtuales que separan nuestra información de la del resto.

La tunelización es un proceso mediante el cual cada paquete de datos es encapsulado dentro de otro paquete de datos. Esto dificulta a que terceros puedan leerlos durante su tránsito. Estos paquetes contienen formatos específicos para coincidir con el tipo de protocolo en uso. Es decir, un paquete que sale de una «red A» se encapsula en un formato que se fija al protocolo de transmisión, atraviesa el túnel entre redes y al final, cuando llega a su destino «red B» se desencapsula.

Encriptación

Mediante la encriptación, el sistema será más seguro, cuanto mayor seguridad nos suministre el sistema criptográfico. Los datos dentro del túnel también son encriptados de tal manera que sólo el destinatario

previsto puede desencriptarlos. Esto mantiene completamente oculto al contenido de su tráfico en internet, incluso de su proveedor de servicios de internet.

Kill switch

Es una parada de emergencia. Esta función con el software de la mayoría de las VPN bloquea automáticamente todo el tráfico de Internet si la conexión de su VPN se cae. De esta manera, sus datos permanecerán seguros, protegidos y anónimos.

Si su VPN fallara temporalmente, quedaría desprotegido. Sus datos se enviarán a Internet sin la protección adicional de un túnel VPN. Como resultado, su dirección IP será visible para el mundo exterior de todos modos. Aquí es donde entra el interruptor de apagado.

Un kill switch de VPN le asegura que nunca se conectará a Internet sin protección. Si su VPN no funciona bien mientras navega, el interruptor de apagado apagará su conexión a Internet por completo.

Ventajas

Si bien es un recurso maravilloso, Internet también está plagado de malware, cookies, piratas informáticos, censura en todo el estado y delitos cibernéticos de alto nivel. Por lo tanto, un poco más de seguridad en línea es una adición bienvenida.

Usar una VPN tiene varias ventajas.

- Brindarle más **libertad** en Internet al sortear las barreras nacionales.
- Brindarle más **seguridad** mediante el cifrado de su tráfico de Internet
- Proporcionarle algo de **anonimato** ocultando su dirección IP

Tu dirección IP real está oculta

Al conectarse a uno de los servidores VPN, su dirección IP se oculta y se reemplaza por la del servicio VPN. La VPN falsifica su ubicación y, por lo tanto, lo anonimiza parcialmente en la web. La dirección IP observada es la dirección del servidor VPN. Con una nueva dirección IP, usted puede navegar por internet como si se encontrase en el Reino Unido, Alemania, Canadá, Japón o prácticamente en cualquier país, si el servicio VPN cuenta con servidores allí

El tráfico de datos se cifra

Una VPN cifra su tráfico de datos. Esto evita que los piratas informáticos y otras partes malintencionadas se apoderen de nuestros datos importantes (o al menos, puedan descifrarlos). Esto también permite que el usuario se conecte de forma segura a puntos de acceso wifi públicos que de otro modo serían inseguros.

Mayor seguridad

Utilizar una VPN lo protege de las violaciones de seguridad en muchas formas, como los análisis de paquetes, las redes Wi-Fi clandestinas y los ataques de intermediarios. Los viajeros, los empleados remotos y todo tipo de personas en constante movimiento utilizan una VPN cada vez que se conectan una red que no es de confianza, como las redes Wi-Fi públicas gratuitas.

Evite las restricciones geográficas

Con una VPN es posible conectarse a un servidor en un país diferente y, por lo tanto, permitir que todo su tráfico de datos pase por este otro país. Esto a menudo permite que ciertos sitios web bloqueados, servicios de transmisión y redes sociales sean accesibles.

Por ejemplo, con un servidor VPN en Gran Bretaña, los no británicos de repente pueden ver BBC iPlayer. Si se encuentra en alguna parte del mundo que restringe el acceso a Google, Wikipedia, YouTube u otras páginas y servicios, utilizar una VPN le permitirá recuperar el acceso a la internet libre. Usted también puede utilizar una VPN para atravesar los cortafuegos de las redes escolares o de oficina.

Los usuarios pueden descargar de forma segura y anónima

Debido a que la dirección IP está oculta y la conexión está encriptada, los terceros ya no podrán averiguar qué se está descargando exactamente o quién lo está descargando. Debido al túnel VPN cifrado, no pueden registrar lo que se descarga a través de la conexión VPN segura. Cuando descarga archivos importantes o confidenciales (por ejemplo, para el trabajo), nadie puede interceptar y ver esta información. Las buenas VPN también le ocultan su actividad a su proveedor de internet, a su operador de telefonía móvil y a cualquier otra persona que pueda estar escuchando, gracias a una capa de encriptación fuerte.

Evitar la censura del gobierno

En países donde el gobierno controla y regula Internet, como China, Irán o Eritrea, no todos los sitios web están disponibles. Es así como los regímenes totalitarios se acostumbran a silenciar a los medios de comunicación escépticos de dicho régimen bloqueándolos en el país. Este tipo de censura se puede eludir, como todas las demás restricciones geográficas, utilizando una VPN. Por tanto, una VPN es una herramienta importante en la batalla por la libertad de prensa.

Comprar en línea por menos

Los precios de las compras en línea a veces pueden diferir según el país desde el que se realiza la compra. Al visitar una tienda web en línea desde una conexión a Internet dentro de Inglaterra, por ejemplo, los productos a veces pueden ser drásticamente más caros que cuando se compran en otro país, como por ejemplo, India. Una conexión VPN permite al usuario conectarse a servidores VPN de todo el mundo. Esto hace que los sitios web registren a los usuarios como visitantes del país donde se encuentra el servidor VPN, lo que permite al usuario beneficiarse de las mejores tarifas internacionales.

Las VPN mejoran los juegos en línea

Así como esto puede darle acceso a ciertos sitios, también le permitirá jugar juegos en línea que pueden estar restringidos en su país de origen. O quizás el juego que quieres jugar está programado para una fecha de lanzamiento posterior. Con una VPN, no tienes que esperar más.

Las VPN evitarán que su ISP limite su conexión a Internet

La limitación del ancho de banda es la limitación deliberada de su ancho de banda por parte de su proveedor de servicios de Internet. Ocasionalmente, a los ISP no les gustará el hecho de que esté descargando grandes cantidades de datos. Sin embargo, cuando encripta sus datos con una VPN, los proveedores de servicios de Internet no podrán ver lo que está haciendo en línea. Tampoco podrán aislarte en particular.

Desventajas

Una VPN puede parecer la solución perfecta para muchos problemas de privacidad en línea. Después de todo, una VPN oculta su dirección IP, cifra sus datos y desbloquea el contenido protegido por dirección IP. En resumen, le brinda seguridad, anonimato y libertad.

Sin embargo, todo tiene sus inconvenientes y diferencias entre lo gratuito y pago.

Una VPN puede disminuir su velocidad

Debido a que la conexión a Internet con una VPN se redirige y encripta a través del servidor VPN, es posible que su conexión a Internet se ralentice ligeramente. La mayoría de los usuarios de Internet no notarán la diferencia. Pero por ejemplo, los jugadores que quieran jugar juegos multijugador en línea deben buscar las mejores VPN para juegos, para asegurarse de que no experimentarán ningún retraso.

Puede correr el riesgo de ser bloqueado por ciertos servicios

Las VPN también están bloqueadas por servicios de transmisión como Netflix y Hulu. Debido a que estas empresas tienen contratos con distribuidores de películas que solo les permiten mostrar contenido en países específicos. Dado que Netflix puede no tener los derechos para mostrar ese contenido en su país, están luchando contra el uso de una VPN. Lo hacen bloqueando las direcciones IP que acceden a su servicio con grandes cantidades de personas al mismo tiempo.

Una VPN no es legal en todos los países

Aunque pueda considerarse sospechoso, el uso de una VPN es legal en la mayoría de los países. De hecho, la mayoría de las grandes empresas y corporaciones utilizan una VPN como parte de su seguridad. Sin embargo, existen algunas excepciones. Algunos países quieren tener un control total sobre las cosas que sus ciudadanos ven en Internet. En algunos países, como Rusia y China, solo puede usar VPN aprobadas por el gobierno.

Es difícil para los consumidores comprobar la calidad del cifrado

Averiguar qué registros dice un proveedor que mantienen y leer más sobre la calidad y seguridad generales de la VPN. Esto incluye una breve explicación de qué protocolos y tipos de cifrado emplea el proveedor de VPN.

La conexión se rompe

Cuando la conexión a su servidor VPN se desconecta, de repente se queda sin protección y su comportamiento en línea está vinculado a su dirección IP real. Para evitar esto, el interruptor de interrupción interrumpe inmediatamente toda su conexión a Internet y solo se restaura una vez que se restablece la conexión a la VPN.

Una sensación injustificada de impunidad en línea

Hay algunas personas que creen que su conexión VPN las hace completamente anónimas y no se ven afectadas por el malware.

Incluso con una conexión VPN estable y fuertemente encriptada, aún puede:

- Sea seguido en la web por anunciantes, rastreadores, piratas informáticos, agencias de inteligencia, etc.
- Sea objetivo y sea víctima de ataques de phishing
- Infectarse con algún tipo de malware
- Queda bloqueado de ciertas redes, bases de datos, páginas web, etc.

VPN gratuitas: a veces peor que ninguna

Algunas personas optan por probar un servicio VPN gratuito. No hay nada de malo en esto. Sin embargo, desafortunadamente, muchos proveedores de VPN gratuitos no fueron diseñados para brindar al usuario promedio más privacidad y anonimato en Internet, sino únicamente para ganar dinero. Un buen ejemplo es

Hola VPN, un servicio VPN del que debe mantenerse alejado. Este tipo de VPN no se dedica a vender un servicio de VPN, sino a vender sus datos personales a terceros. Muchos servicios VPN gratuitos ganan dinero vendiendo sus datos a, por ejemplo, anunciantes. Además, muchas aplicaciones VPN gratuitas no son seguras y contienen software espía o malware en la descarga.

El registro y la posible reventa de sus hábitos de Internet a terceros

La idea de obtener una suscripción de un proveedor de VPN es que enrutes tu tráfico de Internet a través de sus servidores. Cifran sus datos y le permiten utilizar uno de sus muchos servidores para ocultar también su dirección IP. Esto significa que debe tener confianza en su VPN para que no abusen de los datos que viajan a través de sus servidores. Básicamente, ha comprado seguridad y anonimato. Muchos proveedores de VPN mantienen su parte del trato e ignoran por completo sus datos personales. No registran lo que haces ni almacenan tus datos. Sin embargo, algunos proveedores de VPN registran sus datos. Muchas VPN gratuitas hacen esto y por supuesto, anula todo el propósito de obtener un servicio VPN. Pero estos no son los peores infractores. Los casos realmente preocupantes son los proveedores de VPN pagados que afirman que no inician sesión, pero que más tarde se ha descubierto que lo hacen. Por ejemplo, el FBI le pidió a un proveedor de VPN (HideMyAss) que proporcionara información sobre uno de sus clientes debido a la sospecha de actividades ilegales en la web oscura. Aunque la empresa se negó inicialmente, terminaron entregando registros muy específicos sobre el usuario, incluidos los tiempos de inicio de sesión, las descargas, el uso de ancho de banda, etc.

El caso de Onavo Protect: Onavo protect era un proveedor de servicios VPN diseñado exclusivamente para equipos móviles, fundada en el 2010 y subsidiada por Facebook se encargaba de proteger las sesiones en internet de sus usuarios. La realidad es que este proveedor es poco confiable, en su momento y antes de ser eliminada esta herramienta se demostró que este proveedor usaba la información registrada sobre las sesiones de sus usuarios para servir de espía a Facebook y determinar el tiempo que dedicaba estos usuarios en la competencia. Se rumorea que Facebook usó estos datos para tomar varias decisiones comerciales, incluida la adquisición de WhatsApp en 2014.

Tipos de VPN

Hay dos tipos fundamentales de VPN:

VPN de acceso remoto

La VPN de acceso remoto (Remote Access VPN) permite a los usuarios conectarse a una red privada para acceder a servicios y recursos de forma remota. Esta conexión es segura y se realiza a través de internet mediante un remote access server.

Resulta útil para usuarios comerciales como domésticos. Por ejemplo, un empleado corporativo, mientras está fuera de las instalaciones de la compañía, puede utilizar una VPN para conectarse a la red privada de la empresa y acceder a archivos de esa misma red.

Los usuarios privados de este tipo de VPN utilizan principalmente estos servicios para eludir las restricciones regionales en internet y acceder a sitios web bloqueados. Otro caso es proteger la privacidad mientras se navega en internet.

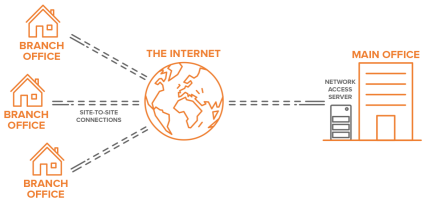
VPN site-to-site

Una VPN site-to-site o de sitio a sitio se utiliza principalmente en las empresas. Las organizaciones con instalaciones en diferentes ubicaciones geográficas utilizan esta VPN para conectar la red de una instalación a la red en otra, y en otra ubicación geográfica.

Nos permitirían conectar 2 o más hogares entre sí, y tener acceso a todos los recursos compartidos, como si estuviéramos físicamente en todas las casas. El servidor VPN es el que posee un vínculo permanente a internet, acepta todas las conexiones que provienen de los sitios, y establece el túnel VPN.

La VPN de sitio a sitio crea un puente virtual entre las redes, en oficinas geográficamente distantes, y las conecta a través de internet para mantener una comunicación segura y privada entre las redes.

La VPN de sitio a sitio se basa en la comunicación de enrutador a enrutador; uno actúa como un cliente VPN y otro enrutador como un servidor VPN. La comunicación entre los dos enrutadores comienza después de validar una autenticación entre los dos.



Protocolos VPN

Los protocolos VPN son los métodos mediante los cuales se conecta su dispositivo al servidor VPN. Algunos protocolos favorecen la velocidad, otros favorecen la seguridad y algunos simplemente funcionan mejor en determinadas condiciones de red.

Los protocolos determinan qué algoritmo de encriptación utilizar, cómo establecer y verificar las claves de encriptación y cómo manejar los potenciales errores. Los protocolos de VPN pueden estar diseñados para redirigir todos sus datos a través de este túnel encriptado, o como ocurre con los proxy de HTTP, redirigir solamente su tráfico web.

La mayoría de proveedores de servicios VPN dan a sus usuarios a elegir entre varios protocolos VPN. Algunos de los más utilizados son: Point to Point Tunnelling Protocol (PPTP), Layer Two Tunnelling Protocol (L2TP), Internet Protocol Security (IPSec) y OpenVPN (SSL/TLS).

PPTP

PPTP (del inglés Point to Point Tunneling Protocol) significa: Protocolo de Tunelización de Punto a Punto. El PPTP, que opera en el puerto TCP 1723, es uno de los protocolos VPN más antiguos en uso, siendo contemporáneo con Windows 95, y estándar en todas las versiones de Windows desde entonces. PPTP fue desarrollado gracias a una iniciativa de Microsoft para encapsular otro protocolo llamado PPP (Protocolo Punto a Punto).

De todos los protocolos VPN, PPTP es uno de los más comunes, más fáciles de configurar, y computacionalmente rápidos. Por esa razón, el PPTP es particularmente útil para aplicaciones en las cuales la velocidad es fundamental, como streaming de audio o video, o en dispositivos más antiguos y lentos, con procesadores más limitados. Sin embargo, el PPTP también está expuesto a serias vulnerabilidades de seguridad. Sus protocolos de autenticación subyacentes, típicamente MS-CHAP-v1/v2, son fundamentalmente inseguros, y han sido descifrados en análisis de seguridad una y otra vez desde que el PPTP se introdujo por vez primera.

La carga útil de PPP se cifra mediante el protocolo de cifrado punto a punto (MPPE) de Microsoft. MPPE implementa el algoritmo de cifrado RSA RC4 con un máximo de claves de sesión de 128 bits.

Con RC4 y claves de 128 bits, la sobrecarga de cifrado es menos que todos los protocolos, lo que hace que PPTP sea el más rápido.

Por esta razón, el PPTP no se recomienda, excepto en los casos en los que la seguridad es absolutamente prescindible.

Pros: Rápido y Compatible con dispositivos más antiguos

Contras: Menos seguro

IPsec

Este protocolo proporciona servicios de seguridad a la capa IP y a todos los protocolos superiores, como TCP y UDP (capa de transporte en internet). IPsec proporciona todos los servicios necesarios para que la comunicación sea segura (autenticación, confidencialidad, integridad y no repudio). Gracias a estos servicios, la seguridad de las comunicaciones está garantizadas. Por supuesto, también tenemos control de acceso, calidad de servicio y registro de actividad.

En cuanto a la negociación de la criptografía, IPsec integra un sistema de negociación para que los equipos finales negocien el mejor cifrado posible que soporten, acordar las claves de intercambio, y elegir los algoritmos de cifrado que tengan en común. Dependiendo de la cabecera de IPsec usada (AH o ESP), podremos comprobar solamente la autenticidad del paquete, o cifrar la carga útil de todo el paquete IP y comprobar también su autenticidad.

El protocolo IPsec tiene una arquitectura con varias cabeceras, dependiendo de lo que nos interese «asegurar», podremos elegir una cabecera u otra, no podemos elegir ambas cabeceras simultáneamente en un mismo túnel de IPsec. Las cabeceras que tenemos en este protocolo son las siguientes:

- Cabecera de Autenticación (AH)
    - Esta cabecera proporciona al receptor de los paquetes IP un método para autenticar el origen de los datos, y verificar que dichos datos no han sido alterados en la comunicación. Un detalle muy importante, es que esta cabecera no proporciona confidencialidad porque no cifra los datos del paquete IP, por tanto, la información intercambiada puede ser vista por terceros a no ser que usen protocolos como HTTPS por ejemplo
- Carga de Seguridad Encapsulada (ESP)
    - La Carga de Seguridad Encapsulada, o también conocida como ESP, ofrece autenticación, integridad y confidencialidad de los datos transmitidos a través de IPsec. Es decir, en este caso sí estaremos cifrando todo el campo de datos para que todas las comunicaciones sean confidenciales, a diferencia de AH que no cifra el mensaje transmitido. Para conseguir estas

características de seguridad, se hace un intercambio de llaves públicas haciendo uso de Diffie-Hellmann para asegurar la comunicación entre ambos hosts. El cifrado de los datos se realiza mediante algoritmos de clave simétrica

Existen dos modos básicos de operación de IPsec:

- Modo transporte: sólo la carga útil (los datos que se transfieren) del paquete IP es cifrada o autenticada. El enrutamiento permanece intacto, ya que no se modifica ni se cifra la cabecera IP.
- Modo túnel: todo el paquete IP (datos más cabeceras del mensaje) es cifrado o autenticado. Debe ser entonces encapsulado en un nuevo paquete IP para que funcione el enrutamiento. Este es el utilizado por las VPNs.

Pros: Más seguro que PPTP

Contras: Más lento que OpenPVN, a veces bloqueado por los firewalls y solo es moderadamente seguro

OpenVPN

OpenVPN es un protocolo altamente configurable y relativamente nuevo. Lo mejor de OpenVPN es que es de código abierto. Aunque la palabra “abierto” tal vez no suene muy atractiva para una herramienta de privacidad, verdaderamente representa una enorme ventaja. Si hubiese fallos de seguridad en el código, la comunidad del código abierto las identificaría rápidamente. En combinación con un robusto algoritmo de encriptación, OpenVPN es uno de los protocolos de VPN más seguros que existen.

Es compatible con sistemas operativos Microsoft Windows, GNU/Linux, macOS e incluso tiene aplicaciones gratuitas para Android y iOS. Otro punto fuerte de OpenVPN es que algunos fabricantes de routers lo están incorporando en sus equipos, por lo que se puede tener la posibilidad de configurar un servidor OpenVPN en el router. Otro aspecto destacable es que, por ejemplo, sistemas operativos orientados a cortafuegos también lo incorporan.

Este software nos permite configurar dos tipos de arquitecturas de VPN:

- VPN de acceso remoto: tenemos un servidor VPN central, y varios clientes VPN con el software instalado en su ordenador, smartphone, tablet u otro dispositivo, y todos se conectan de manera centralizada al servidor VPN.

- VPN Site-to-Site: esta arquitectura nos permite intercomunicar diferentes sedes para compartir los recursos a través de una red segura, protegida con cifrado punto a punto. Este tipo de VPN nos permite interconectar oficinas, sedes de empresas etc.

Algunas características muy importantes de OpenVPN son que soporta una amplia configuración, tanto para mejorar el rendimiento como también la seguridad. Está basado en SSL/TLS, por tanto, se crean certificados digitales para la autenticación de los clientes VPN, además, también permite autenticarse con certificados más un usuario/contraseña que se agregue al sistema. OpenVPN es mucho más fácil de configurar que IPsec y parte de eso gracias al gran soporte de la comunidad.

OpenVPN utiliza la biblioteca OpenSSL para proporcionar cifrado. OpenSSL implementa una gran cantidad de algoritmos criptográficos como 3DES, AES, RC5, Blowfish.

IKEv2

Desarrollado por Microsoft y Cisco, IKEv2 es la siguiente versión del protocolo Internet Key Exchange. Este protocolo VPN también se conoce como IKEv2/IPsec, pero como IKEv2 nunca es implementado sin la capa de encriptación IPsec, generalmente solo se abrevia IKEv2.

Entonces, IKE es un protocolo de tunelización basado en IPSec que proporciona un canal de comunicación VPN seguro y define los medios automáticos de negociación y autenticación para las asociaciones de seguridad IPSec de forma segura. Hay una serie de diferencias entre IKEv1 e IKEv2, una de las cuales es la reducción de los requisitos de ancho de banda de IKEv2, otra la compatibilidad con MOBIKE (Protocolo de movilidad y multihoming IKEv2) una función que permite que el protocolo resista los cambios de red.

IKEv2 emplea autenticación de certificados de servidor, lo que significa que no realizará ninguna acción hasta que determine la identidad del solicitante. Esto desvía la mayoría de los intentos de ataques de intermediario y DoS.

En la primera versión del protocolo, si se intentaba cambiar a una conexión de Internet diferente, (p. ej. de WiFi a Datos) con la VPN activada, interrumpiría la conexión VPN y requeriría una reconexión. Esto tiene ciertas consecuencias negativas, como caídas de rendimiento y cambio a una dirección IP anterior.

Se le considera más liviano y estable que OpenVPN, al tiempo que conserva cierto nivel de personalización. Sin embargo, solo está disponible a través de UDP, que a su vez es bloqueado por algunos firewalls.

IKEv2 es uno de los protocolos más nuevos y tiene fortalezas significativas, particularmente su velocidad. IKEv2 implementa una gran cantidad de algoritmos criptográficos, incluidos 3DES, AES, Blowfish, Camellia. IVPN implementa IKEv2 usando AES con claves de 256 bits.

IKE se basa en los protocolos de seguridad subyacentes, como Internet Security Association and Key Management Protocol (ISAKMP), A Versatile Secure Key Exchange Mechanism for Internet (SKEME) y Oakley Key Determination Protocol.

Oakley permite que las partes autenticadas intercambien material de claves usando conexiones inseguras utilizando el algoritmo de intercambio de claves Diffie-Hellman. Este método convierte estas claves de forma segura, creando una mayor protección de la identidad y autentificación.

Si bien es más seguro que L2TP/IPsec, es más lento que OpenVPN

Wireguard

Si bien es un protocolo joven, superó numerosas auditorías de seguridad y desde marzo 2020 está disponible su versión estable. Es extremadamente sencillo de configurar, diseñado para consumir menos recursos, rápido (más rápido que IPsec y OpenVPN) y que utiliza la criptografía moderna por defecto, sin necesidad de seleccionar entre diferentes algoritmos de cifrado simétrico, asimétrico y de hashing. El objetivo de WireGuard VPN es convertirse en un estándar, y que más usuarios domésticos y empresas comiencen a utilizarlo, en lugar de usar IPsec o el popular OpenVPN que son más difíciles de configurar y más lentos. Este software está diseñado para ser utilizado por todos los públicos, tanto para usuarios domésticos como en súper ordenadores. El protocolo de capa transporte utilizado por WireGuard es UDP únicamente.

Con los protocolos IPsec y OpenVPN, es necesario que tanto los clientes como el servidor «acuerden» los protocolos criptográficos a utilizar. WireGuard proporciona un «paquete» criptográfico entero, garantizando la conectividad sin necesidad de seleccionar nosotros nada.

WireGuard presenta una construcción más liviana (solo 4k lineas de código) que la mayoría de los protocolos VPN, bueno, al menos los de código abierto (OpenVPN, SoftEther, IKEv2) donde todo el código es visible.

Como desventaja encontramos que el uso de WireGuard podría obligar a un proveedor de VPN a almacenar registros de IP de forma indefinida dado a que las direcciones IP de VPN autorizadas se

combinan con claves de cifrado públicas para una mayor seguridad. Sin embargo, los proveedores que comenzaron a ofrecer este protocolo encontraron soluciones alternativas seguras.

SSL/TLS

SSL es el acrónimo de Secure Sockets Layer (capa de sockets seguros), la tecnología estándar para mantener segura una conexión a Internet, así como para proteger cualquier información confidencial que se envía entre dos sistemas e impedir que los delincuentes lean y modifiquen cualquier dato que se transfiera, incluida información que pudiera considerarse personal. Los dos sistemas pueden ser un servidor y un cliente (por ejemplo, un sitio web de compras y un navegador) o de servidor a servidor (por ejemplo, una aplicación con información que puede identificarse como personal o con datos de nóminas).

Considerando un modelo OSI (Arquitectura de redes por capas), el protocolo SSL se utiliza entre la capa de aplicación y la capa de transporte. Uno de sus usos más extendidos, es el que se realiza junto al protocolo HTTP, dando lugar al HTTPS o versión segura de HTTP. Se utiliza para la transferencia de hipertexto (Sitios web) de manera segura. De esta forma se consigue que la información transmitida entre un sitio web y un usuario (en ambos sentidos), sea segura, especialmente importante cuando se trata de información sensible: datos confidenciales, contraseñas, información bancaria, imágenes personales, etc

¿Cómo funciona el Protocolo SSL?

En el protocolo SSL se utiliza tanto criptografía asimétrica como simétrica. La primera se utiliza para realizar el intercambio de las claves, que a su vez serán usadas para cifrar la comunicación mediante un algoritmo simétrico.

En el caso de los sitios web, para el funcionamiento de este protocolo, lo que se necesita utilizar es un certificado SSL. El servidor web tendrá instalado uno y cuando un cliente intente acceder a él, le remitirá el mismo con la clave pública del servidor, para enviar de esta forma la clave que se usará para realizar la conexión de manera segura mediante un cifrado simétrico.

Si hablamos de diferencias entre SSL y TLS podríamos decir que radican principalmente en que SSL se ubica en la capa de sesión del modelo OSI, sin embargo, TLS se encuentra en la capa de transporte y es el protocolo sucesor de SSL. TLS es una versión mejorada de SSL. Funciona de un modo muy parecido a SSL, utilizando cifrado que protege la transferencia de datos e información.

Se debe tomar una decisión de arquitectura para determine el método apropiado para proteger los datos cuando se está transmitiendo. Las opciones más comunes disponibles para las empresas son las redes privadas virtuales (VPN) o un modelo SSL / TLS comúnmente utilizado por las aplicaciones web. El modelo seleccionado está determinado por las necesidades empresariales de la organización en particular. Por ejemplo, una conexión VPN puede ser el mejor diseño para una asociación entre dos empresas que incluye el acceso mutuo a un servidor compartido a través de una variedad de protocolos. A la inversa, una aplicación web para empresas que se enfrenta a Internet probablemente sería mejor atendida por un modelo SSL / TLS. Sin embargo, aunque te encuentres en un sitio web con SSL/TLS, usando una VPN tendrias otra capa de protección.

En otras palabras, las VPN con protocolos como IPsec conectan hosts o redes a una red privada protegida, mientras que las VPN SSL / TLS conectan de forma segura la sesión de aplicación de un usuario a los servicios dentro de una red protegida.

La capa de transporte permite el cifrado de extremo a extremo, por lo que la capa de aplicación es siempre una implementación del protocolo estándar superior TLS. HTTPS es, por ejemplo, una aplicación de TLS. Lo mismo se aplica a POP3S, SMTPS e IMAPS, todos los cuales permiten una transmisión segura de correo electrónico. Para otras aplicaciones, como chats, conexiones VPN o transferencia de datos FTP, existen

protocolos adaptados que hacen que TLS sea aplicable en la práctica. TLS es un concepto básico que puede tener muchas aplicaciones o instancias diferentes.

SSH

SSH o Secure Shell, es un protocolo de administración remota que le permite a los usuarios controlar y modificar sus servidores remotos a través de Internet a través de un mecanismo de autenticación.

Es un protocolo que facilita las comunicaciones seguras entre dos sistemas usando una arquitectura cliente/servidor y que permite a los usuarios conectarse a un host remotamente. A diferencia de otros protocolos de comunicación remota tales como FTP o Telnet, SSH encripta la sesión de conexión, haciendo imposible que alguien pueda obtener contraseñas no encriptadas.

El protocolo funciona en el modelo cliente-servidor, lo que significa que la conexión la establece el cliente SSH que se conecta al servidor SSH. El cliente SSH dirige el proceso de configuración de la conexión y utiliza criptografía de clave pública para verificar la identidad del servidor SSH. Después de la fase de configuración, el protocolo SSH utiliza un cifrado simétrico fuerte y algoritmos hash para garantizar la privacidad y la integridad de los datos que se intercambian entre el cliente y el servidor.

La principal diferencia entre VPN y SSH es que SSH se conecta a una computadora en particular mientras que una VPN se conecta a una red. Cada uno de ellos proporciona una capa adicional de seguridad al navegar en línea.

SSH cifra las aplicaciones en lugar de todo el tráfico procedente de su dispositivo. Eso significa que debe configurar cada aplicación por separado para el túnel SSH. Una VPN, por otro lado, se asegurará automáticamente de que todo su tráfico esté encriptado, por lo que no es necesario configurar el cifrado para aplicaciones específicas.

Con VPN se puede comunicar con compañeros de trabajo e intercambiar archivos como si estuviera sentado en el cubículo de al lado. Esto no funciona con SSH. Además, no necesita terminales de comando para comunicarse con otros sitios web.

La idea de usar SSH y una VPN en combinación asegura un nivel más profundo de seguridad. Es decir, incluso si la VPN se ve comprometida, un atacante/investigador aún necesitaría penetrar en la conexión SSH para obtener algo de valor.

Utilización de criptografía en VPN

¿Puede alguien hackear y acceder a una VPN?

Hackear una conexión VPN implica vulnerar la criptografía de esta, ya sea descodificando el cifrado mediante algún tipo de vulnerabilidad, o bien robando la clave mediante algún método fraudulento; de allí la importancia de la criptografía utilizada. Los hackers y criptoanalistas utilizan ataques criptográficos para recuperar la información en forma de texto de la versión cifrada de ésta, sin la clave. No obstante, descodificar el cifrado es una tarea que demanda mucho en cuanto a computación y tiempo, y puede llevar años.

La mayoría de los esfuerzos en hacerlo se centran en robar las claves, lo cual es mucho más fácil que descodificar el cifrado.

Las revelaciones del conocido informante Edward Snowden y de investigadores de seguridad mostraron que la agencia de espionaje de EE.UU. (la NSA) consiguió descodificar el cifrado de una cantidad enorme de tráfico de internet, incluyendo el de VPN. Los documentos de Snowden informan de que el método de

descodificación de VPN de la NSA consiste en interceptar el tráfico cifrado, y mandar parte de los datos a unos superordenadores que averiguan la clave.

Los investigadores de seguridad Alex Halderman y Nadia Heninger también presentaron una investigación convincente que sugería que era cierto que la NSA desarrolló una forma de descifrar una enorme cantidad de tráfico HTTPS, SSH y VPN mediante un ataque Logjam, el cual estaba basado en implementaciones comunes del algoritmo Diffie-Helman.

Recomendaciones

En general, estas son las principales cosas que debe buscar si desea asegurarse de obtener la experiencia en línea más segura:

- Una clave de cifrado larga, de al menos 128 bits de tamaño.
- Protocolos confiables de intercambio de claves, como ECDH o RSA-2048.
- Cifrados VPN fuertes como AES, Twofish o Camellia.
- Potentes protocolos de VPN como OpenVPN, SoftEther e IKEv2.
- Un hash SHA-2 para la autenticación HMAC: idealmente 256 bits, 384 bits o 512 bits. La autenticación HMAC significa Código de Autenticación de Mensajes Basado en Hash, y es un Código de Autenticación de Mensajes (MAC) que se utiliza para verificar la integridad de los datos y la autenticación de un mensaje al mismo tiempo para asegurarse de que no haya sido modificado por terceros.
- Perfect Forward Secrecy

Como dijo Edward Snowden: «El cifrado funciona. Los sistemas de cifrado fuertes debidamente implementados son una de las pocas cosas en las que se puede confiar».

Perfect Forward Secrecy

Perfect Forward Secrecy (también llamado Forward Secrecy o secreto perfecto hacia adelante) es una característica de varios protocolos de acuerdo de clave. Básicamente, el cifrado PFS funciona generando una clave de sesión única para cada sesión de comunicación iniciada por un usuario entre un cliente y un servidor. Si, por cualquier motivo, una clave de sesión se ve comprometida, los datos de cualquier otra sesión de comunicación estarán seguros. Una vez que se agota la clave privada generada, desaparece, por lo que ya no puede verse comprometida.

Además, las claves de cifrado PFS pueden incluso actualizarse dentro de una sola sesión de comunicación, lo que limita aún más la cantidad de datos que un ciberdelincuente puede robar si la clave privada temporal se ve comprometida.

En comparación con Perfect Forward Secrecy, el cifrado normal suele hacer que el cliente utilice la misma clave privada para todas las sesiones cliente-servidor. Básicamente, eso significa que hay una "clave maestra" que se puede utilizar para descifrar todo el tráfico. Si esa clave se ve comprometida, todos los datos encontrados en todas las sesiones de comunicación entre el cliente y el servidor también se verán comprometidos.

PFS se usa normalmente con ciertos protocolos VPN específicos como OpenVPN, SoftEther, L2TP / IPSec, IKEv2 / IPSec, SSTP o Wireguard.

Algoritmos criptográficos soportados por protocolo

Cada protocolo mencionado anteriormente soporta/recomienda algoritmos de cifrado específicos:

PPTP: La carga útil de PPP se cifra mediante MPPE (Microsoft's Point-to-Point Encryption protocol). MPPE implementa el algoritmo de cifrado RSA RC4 con un máximo de claves de sesión de 128 bits.

IPSec/IKEv2: implementa una gran cantidad de algoritmos criptográficos, incluidos 3DES, AES, Blowfish, Camellia.

OpenVPN: utiliza la biblioteca OpenSSL para proporcionar cifrado. OpenSSL implementa una gran cantidad de algoritmos criptográficos como 3DES, AES, RC5, Blowfish.

WireGuard: ChaCha20 para cifrado simétrico. Curve25519 para acuerdo de clave ECDH. BLAKE2s para hashing. SipHash24 para hashtable key. HKDF para key derivation.

SSTP: utiliza certificados SSL/TLS de 2048 bits para autenticación y una clave SSL de 256 bits para el cifrado.

SSH Tunnel/Socks Proxy usa cifrado AES con 128 bits o 256 bits (Opcional).

AES-256

La gran mayoría de proveedores VPN para empresas utilizan este algoritmo de encriptación para autoproclamarse seguros, lo cual es de esperar dado a que está aprobado por la Agencia Nacional de Seguridad de Estados Unidos (NSA) para información ultra-secreta, es usado por gobiernos y fuerzas militares. AES significa Advanced Encryption Standard. Aunque sus raíces se remontan a 1997, actualmente sigue siendo el único algoritmo en la lista del National Institute of Standards and Technology (NIST) para proteger datos clasificados.

AES-256 es el primer cifrado públicamente accesible y abierto aprobado por la NSA. Su tamaño de clave mayor hace que sea esencialmente irrompible, lo que significa que, incluso si los servidores VPN fueran hackeados, los datos serían imposibles de descifrar. AES-256 también tiene la ventaja de ser rápido.

El cifrado de 256 bits hasta donde sabemos sigue inexpugnable y aunque ha habido intentos con AES-128 bits, intentar romper una clave 256 bits requiere 2128 veces más potencia de cómputo por fuerza bruta, y aun teniendo semejante potencia de cálculo y con el hardware actual, el tiempo para descifrar una sola clave sería más del doble de la edad total del universo.

Modos de procesamiento AES-256

Uno de los modos de operación más utilizados y conocidos para AES es el modo CBC (cipher-block chaining). Ahora Cloudflare ha mostrado que la utilización de este modo de operación CBC está decayendo, en favor de otras suites de cifrado más actuales. La cuota de la suite de cifrados AES-GCM (Galois/Counter Mode) es del 71,2%, una mayoría absoluta y es que esta suite de cifrado es una de las más seguras que hay actualmente, ya que no solo proporciona confidencialidad sino también autenticidad (integridad).

Los modos GCM y CBC funcionan internamente de manera bastante diferente; ambos involucran un cifrado de bloque y OR exclusivo, pero los usan de diferentes maneras.

En el modo CBC, usted encripta un bloque de datos tomando el bloque de texto plano actual y haciendo una operación ORX con el bloque de texto cifrado anterior (o IV, initial vector), y luego envía el resultado de eso a través del cifrado de bloque; la salida del cifrado de bloque es el bloque de texto cifrado.

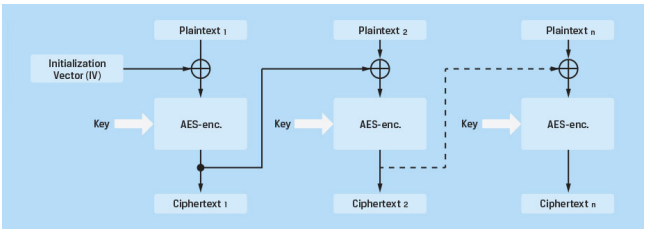
El modo GCM para proporcionar cifrado mantiene un contador; para cada bloque de datos, envía el valor actual del contador a través del cifrado de bloque. Luego, toma la salida del cifrado de bloque y los ORX con el texto plano para formar el texto cifrado.

AES-GCM es un cifrado más seguro que AES-CBC, porque AES-CBC, opera por XOR (eXclusive OR) cada bloque con el bloque anterior y no se puede escribir en paralelo. Esto afecta el rendimiento debido a las complejas matemáticas involucradas que requieren cifrado en serie. AES-CBC también es vulnerable a los ataques padding oracle, que explotan la tendencia de los cifrados de bloque a agregar valores arbitrarios al final del último bloque de una secuencia para cumplir con el tamaño de bloque especificado.

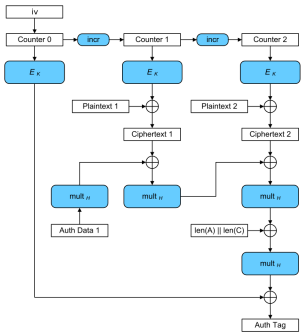
El Modo Galois/Contador (GCM) de procesamiento (AES-128-GCM) funciona de manera bastante diferente; está diseñado para convertir los cifrados de bloque en cifrados de flujo, donde cada bloque se cifra con un valor pseudoaleatorio de un "flujo de claves". Este concepto logra esto mediante el uso de valores sucesivos de un "contador" creciente de modo que cada bloque se cifra con un valor único que es poco probable que vuelva a ocurrir. El componente de multiplicación de campos de Galois lleva esto al siguiente nivel al conceptualizar cada bloque como su propio campo finito para el uso de cifrado sobre la base del estándar AES. Además, AES-GCM incorpora la autenticación de protocolo de enlace en el cifrado de forma nativa y, como tal, no requiere un protocolo de enlace.

AES-GCM se escribe en paralelo, lo que significa que el rendimiento es significativamente mayor que AES-CBC al reducir los gastos generales de cifrado. Cada bloque con AES-GCM se puede cifrar de forma independiente. El modo de funcionamiento AES-GCM se puede ejecutar en paralelo tanto para el cifrado como para el descifrado. La seguridad adicional que proporciona este método también permite que la VPN use solo una clave de 128 bits, mientras que AES-CBC generalmente requiere una clave de 256 bits para considerarse segura.

Cipher Block Chaining (CBC)



Galois/Counter Mode (GCM)



Productos empresariales de VPN

En los últimos años se ha producido un aumento significativo del número de ciberataques a empresas. Y el negocio del ciberdelito solo está creciendo: se espera que cueste al mundo $ 6 billones para 2021, según The Herjavic Group.

Un informe reciente de Verizon afirmó que casi el 43% de las pequeñas empresas fueron blanco de ataques cibernéticos. El informe se basó en una investigación realizada en más de 86 países en todo el mundo, y sus hallazgos han llevado a un aumento en la demanda de soluciones de seguridad más sólidas, como los servicios VPN.

Perimeter 81

Perimeter 81 es una specialist business VPN de origen Israelei. Permite a las empresas implementar servidores VPN privados a los que el personal puede conectarse de forma segura desde cualquier parte del mundo. Puede administrar fácilmente la actividad de la red para todo su personal sin un título en IT desde

un dashboard en línea. Esto permitirá a los empleados acceder de forma segura a archivos, aplicaciones y otros recursos de forma segura desde ubicaciones remotas.

Perimeter 81 está dirigido a empresas con características de seguridad únicas como la segmentación de la red para aislar los datos confidenciales. Si su empresa tiene oficinas en diferentes ubicaciones, puede configurar VPN de sitio a sitio para conectar las dos redes. Las VPN en la nube permiten el acceso remoto y se pueden ampliar fácilmente según sea necesario.

Todos los datos están encriptados con 256-bits AES. Si no implementa su propia VPN, puede elegir entre 700 servidores públicos en 36 ubicaciones en todo el mundo. Las empresas pueden monitorear el acceso a la VPN registrando e inspeccionando todo el tráfico que pasa a través de ella.

Las aplicaciones están disponibles para Windows, MacOS, Linux, iOS, Android y Chrome.

Su costo parte de $8 usd mensuales y soporta los protocolos IKEv2/IPsec, OpenVPN y WireGuard.

Como contra tenemos que no funciona en China.

NordVPN

Es el servicio centrado en el negocio de NordVPN para pequeñas y medianas empresas. Puede configurar fácilmente un acceso remoto seguro tanto a la red de la oficina como a Internet. Cada cuenta de usuario se puede administrar desde un único panel de control centralizado. Agregar usuarios es fácil y no complicará la facturación.

La autenticación de terceros funciona con GSuite, OneLogin, Okta y Azure. Un cifrado sólido y kill switch garantizan que los datos de su organización estén protegidos en todo momento. Nord Teams promete ayudar a las empresas que necesitan soporte en menos de tres horas.

Pros:

- Conexiones rápidas y fiables
- Cifrado AES con claves de 256 bits
- Política estricta de no logs. Tiene su sede en Panamá, ya que el país no tiene leyes de retención de datos obligatorias
- Ancho de banda ilimitado y sin límites de datos
- Aplicaciones para Windows, MacOS, iOS, Linux y Android
- Costo (desde $3.71 mensual) y prueba gratuita
- Consta con +5500 servidores en 62 países

Contras:

- La aplicación de escritorio no es del todo intuitiva

Usa los protocolos IKEv2/IPsec, OpenVPN y NordLynx.

NordLynx: el único punto débil de Wireguard es que no puede garantizar la privacidad completa del usuario. Por eso Nord desarrolllo en su mismo núcleo un sistema de sobre NAT (Network Address Translation) que permite una conexión VPN segura y no almacena ningún dato identificable en el servidor VPN.

ExpressVPN

ExpressVPN tiene más de 1,500 ubicaciones de servidores repartidas en 94 países, lo que significa que es una muy buena opción para los empleados que pueden tener que viajar con frecuencia o trabajar de forma remota. La selección más grande se encuentra en Europa, América del Norte y Asia Pacífico, con un número menor en África y Medio Oriente.

El servicio VPN es uno de los favoritos de los usuarios, ya que ofrece velocidades rápidas junto con encriptación sólida. Los usuarios conscientes de la privacidad estarán felices de que ExpressVPN no almacene ningún registro de tráfico. La única pequeña retención de metadatos se refiere a la fecha (no a la hora) de la conexión, la elección de la ubicación del servidor y el ancho de banda total utilizado.

Ayuda que la sede de ExpressVPN esté en las Islas Vírgenes Británicas y, por lo tanto, no tiene que cumplir con ninguna ley de retención de datos obligatoria. Esto significa que también está fuera de la jurisdicción de las agencias gubernamentales occidentales.

Los estándares de cifrado son estrictos. El proveedor utiliza AES de 256 bits como su protocolo de cifrado predeterminado, así como la autenticación HMAC y perfect forward secrecy. Se incluye un kill switch de Internet, al que la compañía se refiere como un 'bloqueo de red'.

Las aplicaciones están disponibles para iOS y Android, así como software de escritorio para Windows, MacOS y Linux.

Otro punto a favor es que posee excelentes capacidades para desbloquear contenido bloqueado geográficamente

Su costo parte de $6.67 usd mensual

Protocolos que ofrece: Lightway, OpenVPN, IKEv2, WireGuard, L2TP/IPsec, PPTP, SSTP

Práctica

Se mostrará y desarrollará en exposición:

Servidor y cliente VPN mediante OpenVPN

- Servidor VPN corriendo en una máquina virtual Ubuntu en sede remota.
- Cliente VPN en sistema macOS.
- Captura de tráfico por parte de cliente VPN.

Uso de un servidor VPN de tercero (Hide.me)

- Conexión mediante protocolo IKEv2 a servidor de Hide.me.
- Configuración cliente VPN en Android.
- Test de VPN en https://ipleak.net
- Comando tracert a www.google.com con y sin conexión a VPN

Fuentes

Definición

https://uaeh.edu.mx/docencia/Tesis/icbi/licenciatura/documentos/Redes%20privadas%20virtuales.pdf
http://eprints.rclis.org/13992/1/fernandez2006redes.pdf
https://vpnoverview.com/vpn-information/what-is-a-vpn/

Ventajas y desventajas

https://vpnoverview.com/vpn-information/disadvantages-vpn/
https://vpnoverview.com/vpn-information/advantages-vpn/
https://en.wikipedia.org/wiki/Onavo

Protocolos VPN

http://eprints.rclis.org/13992/1/fernandez2006redes.pdf
https://www.cactusvpn.com/beginners-guide-to-vpn/what-is-wireguard/
https://revista.seguridad.unam.mx/numero-10/el-cifrado-web-ssltls
https://es.ryte.com/wiki/Transport_Layer_Security_(TLS)

Utilización de criptografía en VPN

https://es.vpnmentor.com/blog/se-pueden-hackear-las-vpn-analizamos-el-tema-en-detalle/
https://www.ivpn.net/pptp-vs-ipsec-ikev2-vs-openvpn-vs-wireguard/
https://www.earthvpn.com/faq-items/what-encryption-do-you-use/#:~:text=PPTP%20encryption%20uses%20MPPE%20128bit,will%20be%20used%20for%20encryption.

Cadenas VPN

https://www.cactusvpn.com/beginners-guide-to-vpn/double-vpn-chain/

Productos empresariales VPN

https://www.forbes.com/sites/forbestechcouncil/2020/01/07/why-have-vpns-become-so-important-to-corporations/?sh=38a2398d7462
https://www.perimeter81.com/next-gen-business-vpn?a_bid=5e851971&chan=code1&data1=business-vpn&data2=image_dt_d__post__40713&data3=&a_aid=158
https://support.perimeter81.com/docs/openvpn-protocol
https://www.comparitech.com/blog/vpn-privacy/business-vpn/
https://nordvpn.com/es/features/next-generation-encryption/#:~:text=Para%20garantizar%20la%20protección%20de,para%20su%20revisión%20y%20modificación.
https://www.comparitech.com/blog/vpn-privacy/business-vpn/
https://www.expressvpn.com/what-is-vpn/vpn-encryption