1. **VPN PPTP**

PPTP es la abreviatura de Protocolo de Túnel Punto a Punto (en inglés, Point-to-Point Tunneling Protocol). Como su nombre lo indica, una VPN PPTP crea un túnel y captura los datos. Un nombre bastante largo para la VPN más utilizada. Las VPN PPTP son empleadas por usuarios remotos para conectarse a la red de VPN mediante su red de internet existente. Resulta útil para empresas y uso hogareño. Para acceder a la VPN, los usuarios inician sesión con una contraseña aprobada. Las VPN PPTP son ideales para uso personal y empresarial porque no requieren la compra o instalación de hardware adicional y funciones habitualmente ofrecidas como programas complementarios baratos. Las VPN PPTP se usan ampliamente también por su compatibilidad con Windows, Mac y Linux.

Aunque parezca tener muchos beneficios, hay una desventaja de esta VPN, y es que no brinda codificación, que es usualmente la razón por la que uno conseguiría una VPN. Otra desventaja es que depende del PPP o Protocolo de Punto a Punto para implementar medidas de seguridad.

1. **VPN Sitio a Sitio**

Una VPN de sitio a sitio, también llamada VPN de rúter a rúter, y se usa mayormente en operaciones corporativas. Debido al hecho de que muchas empresas tienen oficinas ubicadas dentro y fuera del país, una VPN de sitio a sitio se utiliza para conectar la red de la oficina principal con otras oficinas diferentes. Esto también se conoce como VPN basada en intranet. Lo opuesto también es posible con una VPN de sitio a sitio. Las empresas la utilizan para conectarse con otras compañías de la misma manera, y esto clasifica como una VPN basada en extranet. En términos simples, una VPN sitio a sitio crea un puente virtual que une redes en diferentes lugares para conectarlas a internet y mantener una comunicación segura y privada entre ellas.

De forma similar a una VPN PPTP, la VPN Sitio a sitio crea una red segura. Sin embargo, no hay una línea dedicada en uso que permita que los diferentes sitios dentro de una empresa se conecten para formar una VPN, como mencionamos anteriormente. Además, a diferencia de la PPTP, el direccionamiento, codificación y decodificación se realiza con rúters en forma de hardware o software en ambos lados.

1. **VPN L2TP**

L2TP es la abreviatura de Protocolo de Establecimiento de Túneles (en inglés, Layer to Tunneling Protocol) y fue desarrollado por Microsoft y Cisco. Las VPN L2TP típicamente están combinadas con otro protocolo de seguridad de VPN para establecer una conexión más segura. Una VPN L2TP forma un túnel entre dos puntos de conexión L2TP, y otra VPN como el protocolo IPSec encripta los datos y se focaliza en asegurar la comunicación entre los túneles.

Una L2TP también es similar a PPTP. Las similitudes existen en términos de su falta de encriptación y en que ambas dependen de protocolos PPP para hacerlo. Comienzan a diferenciarse en relación a la confidencialidad e integridad de los datos. Las VPN L2TP brindan ambos, mientras que las VPN PPTP no.

1. **IPsec**

IPsec es una abreviación de Protocolo de Seguridad en Internet. IPsec es un protocolo de VPN que se usa para proteger la comunicación por internet a través de una red IP. Se establece un túnel en un sitio remoto que permite el acceso a tu sitio central. Una IPsec funciona protegiendo la comunicación del protocolo de internet verificando cada sesión y codificando individualmente los paquetes de datos durante la conexión. Hay dos modos en los que opera una VPN IPsec, y son el de transporte y el de túnel. Ambos modos protegen la transferencia de datos entre dos redes diferentes. Durante el modo transporte, se codifica el mensaje en el paquete de datos. En el modo túnel, todo el paquete de datos está encriptado. Un beneficio de usar una VPN IPsec es que también se puede emplear junto con otros protocolos de seguridad para brindar un sistema más robusto.

Aunque una IPsec es una VPN valiosa, una gran desventaja de utilizar este protocolo son las instalaciones costosas y que demoran mucho tiempo en el lado del cliente que deben existir antes del uso.

1. **SSL y TLS**

SSL significa Secure Sockets Layer y TLS es la abreviatura de Transport Layer Security. Ambas funcionan como un protocolo, utilizadas para crear una conexión VPN. Se trata de una conexión de VPN donde el navegador web funciona como cliente, y el acceso del usuario está restringido a aplicaciones específicas en lugar de poder acceder a toda la red. El protocolo SSL y TLS se utiliza principalmente en sitios web de compras y proveedores de servicios. Una VPN SSL y TLS te brinda una sesión segura desde el navegador de tu PC hacia el servidor de la aplicación. Esto se debe a que los navegadores web cambian a SSL fácilmente y casi no requieren ninguna acción por parte del usuario. Los navegadores ya vienen con SSL y TLS integrado. Las conexiones SSL tienen https al inicio de la dirección URL en lugar de http.

1. **VPN MPLS**

Las VPN de conmutación por etiquetas multi-protocolo o MPLS (por sus siglas en inglés) son usadas con mayor eficacia para conexiones del tipo sitio a sitio. Esto se debe principalmente por el hecho de que las MPLS son la opción más flexible y adaptable. Se trata de un recurso de base estándar que se usa para acelerar la distribución de paquetes de red en múltiples protocolos. Las VPN MPLS son sistemas que están ajustados a ISP. Una VPN ajustada a ISP es cuando dos o más sitios están conectados para formar una VPN utilizando el mismo ISP. Sin embargo, la mayor desventaja de usar una VPN MPLS es el hecho de que la red no es tan fácil de configurar en comparación con otras VPN. Tampoco es sencillo hacer modificaciones. Por eso, este tipo de VPN generalmente es más costoso.

1. **VPN Híbrida**

Una VPN híbrida combina MPLS y VPN basada en protocolo de seguridad de internet o IPsec, aunque estos dos tipos de VPN se usan por separado en diferentes sitios. Sin embargo, es posible usar ambas en el mismo sitio. Esto se haría con la intención de utilizar la VPN IPsec como un respaldo de la VPN MPLS.

Las IPsec son VPN que requieren un equipamiento por parte del cliente de algunas cosas mencionadas anteriormente. Este equipamiento generalmente viene en forma de rúter o aparato de seguridad multipropósito. A través de este rúter o aparato se codifican los datos y se forma el túnel VPN tal como mencionamos antes. Comparativamente, las VPN MPLS son utilizadas por un operador, mediante el equipamiento en su red.

Para conectarse a estas dos VPN, se establece un portal para eliminar el túnel IPsec en un lado y trazarlo hacia la VPN MPLS en el otro extremo mientras se preserva la seguridad que esta red se propone brindar.

Las VPN híbridas son utilizadas por empresas principalmente porque utilizar MPLS para sus sitios no sería la opción más apropiada. Hay una gran cantidad de ventajas que las MPLS tienen sobre las conexiones de internet públicas, pero su costo es alto. Por eso, utilizar una VPN híbrida te permite acceder al sitio central a través de un sitio remoto. Las VPN híbridas son en general costosas, pero ofrecen gran flexibilidad.

**Resumen**

En conclusión, tomar la decisión correcta respecto a qué VPN es para ti podría ser algo difícil. Para determinar qué VPN es la adecuada, primero decide qué tipo de seguridad te gustaría tener. Elegir tu VPN dependerá de si eres un estudiante, un propietario de una pequeña empresa, o si tienes varias oficinas corporativas. Otra idea que debes considerar es cuán grande debe ser tu seguridad en términos de si te conviene conseguir algo simple o más complejo como una VPN híbrida. El costo es otro factor que entra en juego en este proceso de decisión. ¿Cuánto dinero estás dispuesto a pagar y vale la pena gastar en proteger tu conexión de internet? Una vez que puedas responder estas preguntas, decidir qué tipo de VPN es adecuada para ti será mucho más sencillo. Una idea que podría ayudarte es investigar más esta área. ¡Te deseo suerte!

Sistemas y medidas que ayudan a garantizar la seguridad de la red:

Antivirus: Este software ayuda a proteger de los virus que llegan por cualquier medio de almacenamiento u otra fuente.

Firewalls (cortafuegos): Es un sistema que ejerce la política de seguridad establecida, filtrando los accesos a la red y bloqueando el acceso a personas no autorizadas. Una vez instalado se debe mantener el Firmware actualizado en todo momento.

Proxy: El servidor Proxy se considera un complemento del firewall ya que es un intermediario que permite el control de acceso, el registro del tráfico, la mejora de rendimiento, el anonimato de la comunicación entre otros.

Listas de control de acceso (ACL): Estas listas permiten determinar los permisos de acceso apropiados a usuarios y grupos concretos. Por ejemplo, puede definirse sobre un Proxy una lista de los usuarios a quienes se les permite el acceso a Internet, FTP, etc.

Redes privadas virtuales (VPN): Una extensión de red segura que se crea sin que los dispositivos estén conectados entre sí físicamente. Cuando utilizamos una VPN nos conectamos a los servicios de Internet de nuestro proveedor y no de manera directa. La VPN garantiza la confidencialidad de los datos.

Sistema de prevención de intrusos (SPI): Es un sistema que soporta los dispositivos inalámbricos para evitar los puntos de acceso no autorizados y otras amenazas inalámbricas.

Cifrado de discos locales: Esto se puede hacer por medio del cifrado de Windows nativo o un cifrado con soluciones a terceros.