

VPN, LA INFORMACIÓN DE SU EMPRESA DONDE LA NECESITE

El mundo está cambiando aceleradamente en las últimas décadas y de relacionarse simplemente con asuntos a nivel local o regional, las empresas están, en este momento, pensando en mercados y negocios a nivel global. Muchas compañías tienen oficinas o instalaciones en distintos puntos del país o del mundo y hay una cosa que todas ellas necesitan: una forma de tener comunicaciones rápidas, seguras y confiables dondequiera que sus oficinas, instalaciones o empleados estén.

Las redes privadas virtuales (VPN) deben su creciente popularidad al hecho que las empresas, especialmente las Pymes, han buscado la forma de utilizar una red pública, ampliamente extendida y de bajo costo como Internet para aumentar la movilidad, mejorar la productividad de los empleados y contribuir al desarrollo. Y las VPN han demostrado que lo pueden lograr, cuando les permiten a los trabajadores remotos que desarrollan sus actividades en la calle, en el hogar o en otras oficinas, tener acceso a una única red privada de la compañía desde cualquier parte del mundo utilizando su computadora portátil, hogareña o de oficina y el Internet público.

Básicamente, una VPN es una red privada que utiliza un red pública (generalmente Internet) para conectar varios lugares o usuarios remotos entre ellos. En vez de utilizar una conexión dedicada o líneas alquiladas, una VPN usa una "conexión virtual" a través de Internet desde la red privada de la compañía hasta el sitio o empleado remoto. En este artículo intentaremos llegar a un entendimiento más acabado sobre las redes privadas virtuales y sus diferentes usos.

TRES PUNTOS CLAVES

Las redes locales tradicionales son esencialmente restringidas, por lo cual se puede intercambiar información entre las computadoras usualmente sin pensar en la seguridad de la información como un asunto crítico. Sin embargo, con las VPN la situación es preocupante debido principalmente a que Internet es intrínsecamente abierto e inseguro. Por lo tanto, las VPN se implementan usando protocolos especiales que le permiten a los usuarios comunicarse de manera segura y comprobar que la transmisión se hace desde una fuente confiable. Cuando un empleado se conecta a Internet, la configuración de las VPN les permite "perforar" la red privada de la compañía y navegar en la red como si estuvieran en su propia oficina.

Para esto, los dispositivos responsables para la formación y administración de la red virtual, deben ser capaces de garantizar:

- La Confidencialidad de los datos, en el caso que fuesen interceptados durante la transmisión, no pueden ser decodificados. De este modo, la información no debe poder ser interpretada por nadie más que los destinatarios de la misma.
- Integridad de los datos, además de no ser interpretados, los datos no deben ser modificados o alterados durante la transmisión.
- La Autenticación y Autorización, garantiza que los datos están siendo transmitidos o recibidos desde dispositivos remotos autorizados y no desde un equipo cualquiera haciéndose pasar por él. Además, administra los distintos niveles de accesos y derechos de cada uno de los usuarios que utilizan la VPN.

VENTAJAS DE LAS VPN

La principal motivación del uso y difusión de esta tecnología es la reducción de los costos de comunicaciones directos, tanto en costos de llamados de larga distancia como en vínculos dedicados. Anterior a la ubicuidad de Internet, las compañías que querían que las redes de sus empresas trascendieran más allá del ámbito de la oficina e incluyeran a los trabajadores y centros de información

de otros edificios, ciudades, estados o incluso otros países, tenían que invertir en hardware y servicios de telecomunicaciones costosos y proporcionales a las distancias implicadas para crear redes amplias de servicio. Sin embargo, con Internet, las compañías tienen la posibilidad de crear una VPN que demanda una inversión relativamente pequeña de hardware y prácticamente independiente de las distancias, utilizando esta posibilidad de alcance global para la conexión entre los puntos de la red.

Cada usuario remoto de la red empresarial puede comunicarse de manera segura y confiable utilizando Internet para conectarse a su red privada local. Una VPN puede crecer para adaptarse a más usuarios y diferentes lugares mucho más fácil que las líneas dedicadas. De hecho, la escalabilidad es otra de las grandes ventajas de una VPN sobre las líneas rentadas.

Una VPN bien diseñada puede traer, además, los siguientes beneficios a una empresa:

- Extender su alcance geográfico.
- Mejorar la seguridad de la información.
- Reducir costos operativos en relación con aquellos producidos por una red tradicional.
- Reducir tiempos y costos de transporte para los usuarios remotos.
- Mejorar la productividad de la empresa.
- Simplificar la topología de la red empresarial.
- Encontrar oportunidades de negocios a nivel global.
- Proveer facilidades de telecomunicaciones.
- Permitir un mejor uso de redes con buen ancho de banda.
- Mejorar el tiempo de ROI (retorno de la inversión) con respecto a las redes WAN tradicionales.

TIPOS DE VPN

Existen varios tipos de arquitecturas de conexión VPN:

1. Acceso remoto

También denominadas VPDN (Virtual Private Dial-up Network), es quizás uno de los modelos más usados actualmente y consiste en usuarios -generalmente empleados- que se conectan con la empresa desde sitios remotos (oficinas comerciales, domicilios, hoteles, aviones, etc.) utilizando Internet como vínculo de acceso. Una vez que han sido autenticados tienen un nivel de acceso muy similar al que tienen en la red local de la empresa. A menudo, una empresa que necesita configurar una gran cantidad de accesos remotos VPN, tercerizan esta función a una empresa proveedora de servicios (Enterprise Service Provider, ESP). La ESP configura un servidor de acceso a la red (network access server, NAS) y proporciona a cada usuario remoto un programa cliente de escritorio para sus computadoras. Los usuarios pueden entonces discar un número gratuito para acceder al NAS y utilizar sus programas clientes para conectarse a la red privada de la compañía.

Un buen ejemplo de empresas que utilizan esta configuración podría ser una empresa con vendedores que recorren los clientes y se conectan a Internet a través de sus teléfonos móviles y utilizan esta conexión para acceder a sus redes empresariales a través de una VPN.

2. Sitio a sitio

Mediante la utilización de equipamiento dedicado, una empresa puede conectar múltiples sitios con ubicación fija a través de una red pública como Internet. Este esquema se utiliza para conectar, por ejemplo, oficinas o sucursales remotas de una empresa con su sede central. Un equipo en la central, que

posee un vínculo a Internet permanente, acepta las conexiones vía Internet provenientes de los otros sitios. A su vez, las sucursales se conectan a Internet utilizando los servicios de su proveedor local de Internet, típicamente mediante conexiones de banda ancha. Esto permite eliminar los costosos vínculos punto a punto tradicionales, sobre todo en las comunicaciones internacionales.

Esta configuración puede ser de dos tipos:

Tipo Intranet, si la empresa tiene una o más sucursales remotas que quiere unir en una única red privada, puede hacerlo creando una VPN para conectar ambas redes locales.

Tipo Extranet, cuando la empresa tiene una relación cercana con otra compañía (por ejemplo, una empresa asociada, un proveedor o cliente), entonces pueden desarrollar una VPN que conecte sus redes y permita a estas empresas trabajar en un ambiente compartido.

3. Interna

Es una variante del tipo "acceso remoto" pero, en vez de utilizar Internet como medio de conexión, emplea la misma red local de la empresa. Sirve para aislar zonas y servicios de la red interna. Esta capacidad también la hace muy conveniente para mejorar las prestaciones de seguridad de las redes inalámbricas.

Un ejemplo clásico es un servidor con información sensible, como las nóminas de sueldos, ubicado detrás de un equipo VPN, el cual provee autenticación adicional más el agregado del cifrado, haciendo posible que sólo el personal habilitado pueda acceder a la información.

CONCLUSIÓN

Si su empresa tiene varias oficinas, instalaciones distribuidas, trabajadores móviles que viajen frecuentemente como, por ejemplo, representantes de ventas, o si tiene empleados que ocasionalmente pueden trabajar desde sus hogares, las redes privadas virtuales pueden ayudarlo a mejorar su eficiencia y productividad. La tecnología de las VPN está, hoy en día, al alcance de prácticamente cualquier Pyme que quiera hacer uso de ellas y aprovechar sus beneficios. Sin embargo, ante la creciente amenaza a la seguridad a que está siendo sometida constantemente la Internet, una empresa que implemente estos avances debe incluir soluciones de cortafuegos y antivirus como parte de su plan integral de implementación.

Como se puede ver, una VPN es una buena forma de mantener a los empleados y socios de su compañía, conectados sin importar de dónde ellos están.