

VPN (Redes Privadas Virtuales)

Índice

- [1. Introducción](#)
- [2. ¿Por qué una VPN?](#)
- [3. ¿Que es una VPN?](#)
- [4. Tecnología de túnel](#)
- [5. Requerimientos básicos de una VPN](#)
- [6. Herramientas de una VPN](#)
- [7. Ventajas de una VPN](#)
- [8. Conclusión](#)
- [9. Bibliografía](#)

1. Introducción

Una RED se extiende sobre un área geográfica amplia, a veces un país o un continente; contiene una colección de máquinas dedicadas a ejecutar programas de usuario (aplicaciones).

En los últimos años las redes se han convertido en un factor crítico para cualquier organización. Cada vez en mayor medida, las redes transmiten información vital, por tanto dichas redes cumplen con atributos tales como seguridad, fiabilidad, alcance geográfico y efectividad en costos.

Se ha demostrado en la actualidad que las redes reducen en tiempo y dinero los gastos de las empresas, eso ha significado una gran ventaja para las organizaciones sobre todo las que cuentan con oficinas remotas a varios kilómetros de distancia, pero también es cierto que estas redes remotas han despertado la curiosidad de algunas personas que se dedican a atacar los servidores y las redes para obtener información confidencial. Por tal motivo la seguridad de las redes es de suma importancia, es por eso que escuchamos hablar tanto de los famosos firewalls y las VPN

2. ¿Por qué una VPN?

Cuando deseo enlazar mis oficinas centrales con alguna sucursal u oficina remota tengo tres opciones:

Modem: Las desventajas es el costo de la llamada, ya que el costo de esta llamada sería por minuto conectado, además sería una llamada de larga distancia, a parte no contaría con la calidad y velocidad adecuadas.

Línea Privada: Tendría que tender mi cable ya sea de cobre o fibra óptica de un punto a otro, en esta opción el costo es muy elevado porque si por ejemplo necesito enlazar mi oficina central con una sucursal que se encuentra a 200 Kilómetros de distancia el costo sería por la renta mensual por Kilómetro. Sin importar el uso.

VPN: Los costos son bajos porque solo realizo llamadas locales, además de tener la posibilidad de que mis datos viajen encriptados y seguros, con una buena calidad y velocidad.

3. ¿Que es una VPN?

Es una red privada que se extiende, mediante un proceso de encapsulación y en su caso de encriptación, de los paquetes de datos a distintos puntos remotos mediante el uso de unas infraestructuras públicas de transporte.

Los paquetes de datos de la red privada viajan por medio de un "túnel" definido en la red pública. (ver figura siguiente)

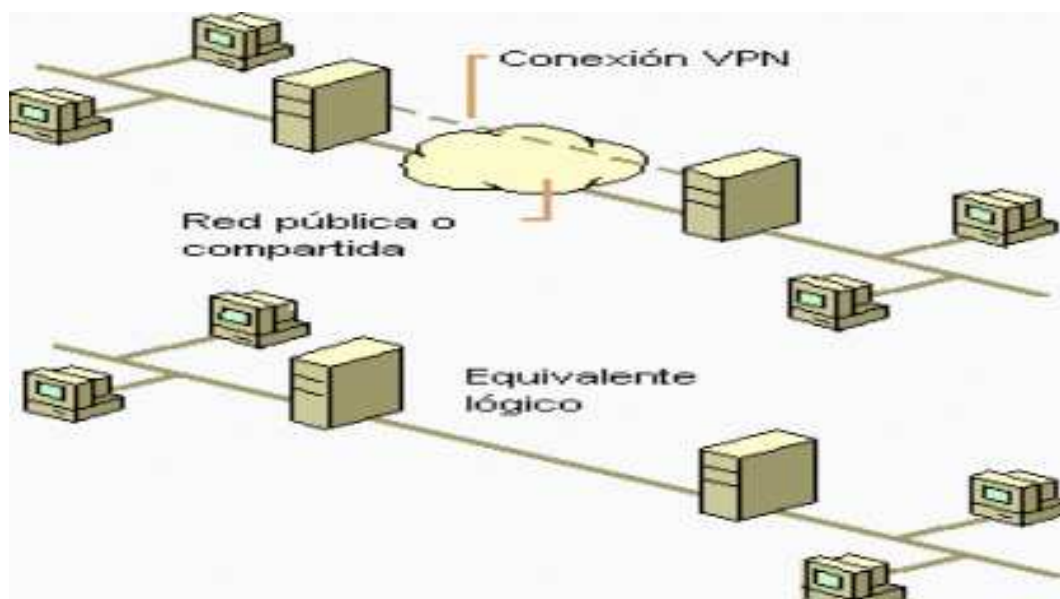


Figura 1



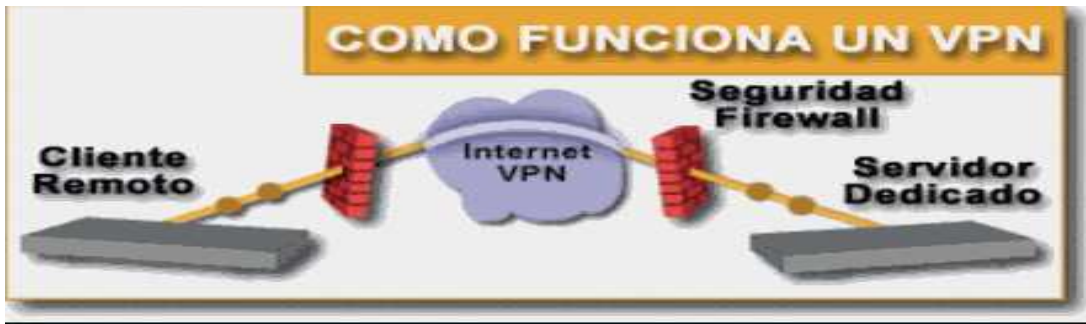


Figura 2

En la figura anterior (figura 2) se muestra como viajan los datos a través de una VPN ya que el servidor dedicado es del cual parten los datos, llegando a firewall que hace la función de una pared para engañar a los intrusos a la red, después los datos llegan a nube de internet donde se genera un túnel dedicado únicamente para nuestros datos para que estos con una velocidad garantizada, con un ancho de banda también garantizado y lleguen a su vez al firewall remoto y terminen en el servidor remoto. Las VPN pueden enlazar mis oficinas corporativas con los socios, con usuarios móviles, con oficinas remotas mediante los protocolos como internet, IP, Ipsec, Frame Relay, ATM como lo muestra la figura siguiente.

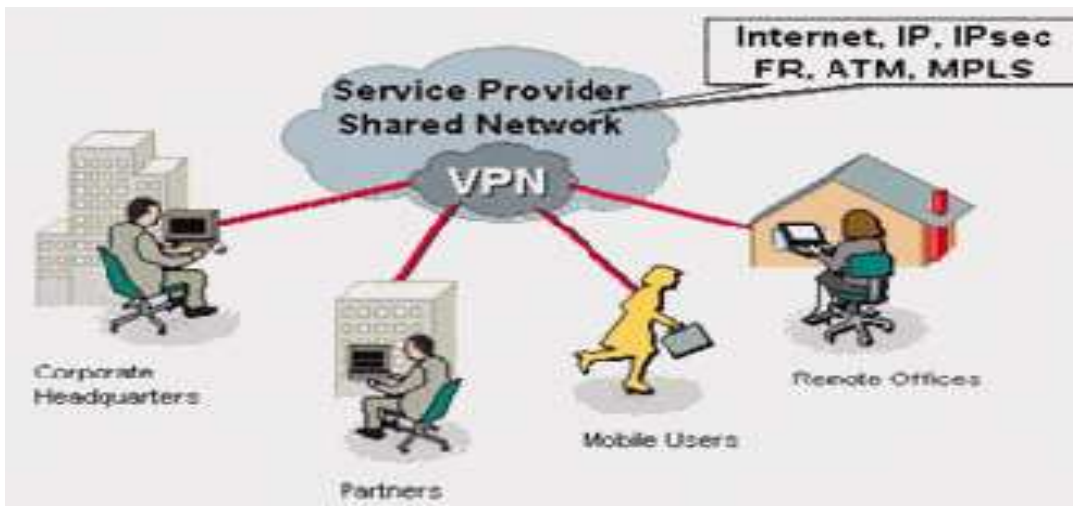


Figura 3

4. Tecnología de túnel

Las redes privadas virtuales crean un túnel o conducto de un sitio a otro para transferir datos a esto se le conoce como encapsulación además los paquetes van encriptados de forma que los datos son ilegibles para los extraños.

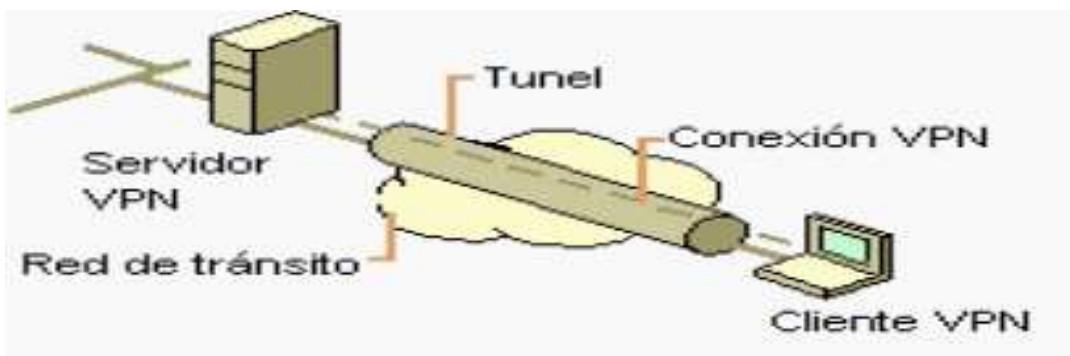


Figura 4

El servidor busca mediante un ruteador la dirección IP del cliente VPN y en la red de tránsito se envían los datos sin problemas.

5. Requerimientos básicos de una VPN

Por lo general cuando se desea implantar una VPN hay que asegurarse que esta proporcione:

Identificación de usuario
Administración de direcciones
Codificación de datos
Administración de claves
Soporte a protocolos múltiples

Identificación de usuario
La VPN debe ser capaz de verificar la identidad de los usuarios y restringir el acceso a la VPN a aquellos usuarios que no estén autorizados. Así mismo, debe proporcionar registros estadísticos que muestren quien acceso, que información y cuando.

Administración de direcciones

La VPN debe establecer una dirección del cliente en la red privada y debe cerciorarse que las direcciones privadas se conserven así.

Codificación de datos

Los datos que se van a transmitir a través de la red pública deben ser previamente encriptados para que no puedan ser leídos por clientes no autorizados de la red.

Administración de claves

La VPN debe generar y renovar las claves de codificación para el cliente y el servidor.

Soporte a protocolos múltiples

La VPN debe ser capaz de manejar los protocolos comunes que se utilizan en la red pública. Estos incluyen el protocolo de internet(IP), el intercambio de paquete de internet(IPX) entre otros.

6. Herramientas de una VPN

VPN Gateway

Software

Firewall

Router

VPN Gateway

Dispositivos con un software y hardware especial para proveer de capacidad a la VPN

Software

Esta sobre una plataforma PC o Workstation, el software desempeña todas las funciones de la VPN.

7. Ventajas de una VPN

Dentro de las ventajas más significativas podremos mencionar la integridad, confidencialidad y seguridad de los datos.

Reducción de costos.

Sencilla de usar.

Sencilla instalación del cliente en cualquier PC Windows.

Control de Acceso basado en políticas de la organización

Herramientas de diagnostico remoto.

Los algoritmos de compresión optimizan el tráfico del cliente.

Evita el alto costo de las actualizaciones y mantenimiento a las PC's remotas.

8. Conclusión

Las VPN representan una gran solución para las empresas en cuanto a seguridad, confidencialidad e integridad de los datos y practicamente se ha vuelto un tema importante en las organizaciones, debido a que reduce significativamente el costo de la transferencia de datos de un lugar a otro, el unico inconveniente que pudieran tener las VPN es que primero se deben establecer correctamente las políticas de seguridad y de acceso porque si esto no esta bien definido pueden existir consecuencias serias.

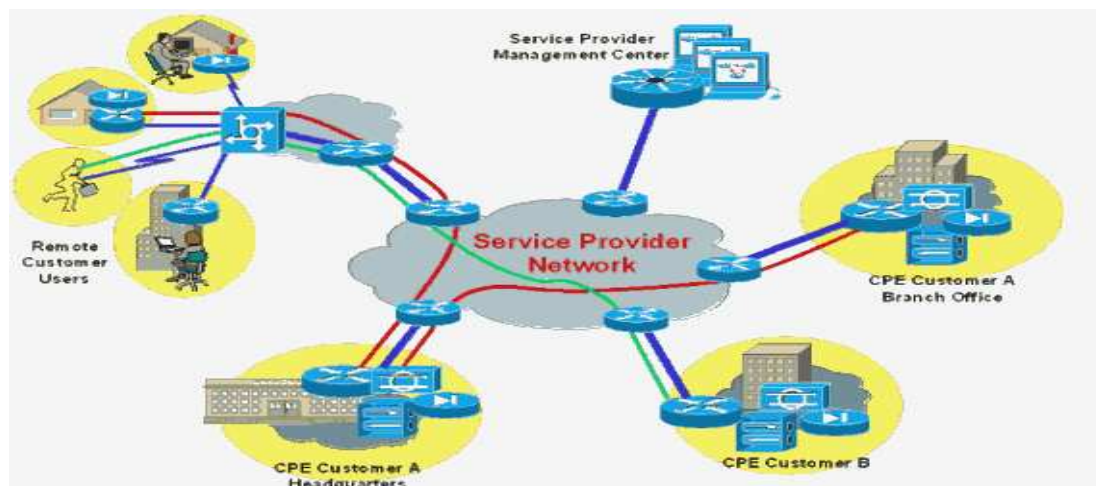


Figura 5

9. Bibliografía

Internet

<http://www.entarasys.com/la>

<http://www.cisco.com/warp/public/44/solutions/network/vpn.shtml>

Trabajo enviado por:

Roberto Nader Carreon

robertonader@hotmail.com

Edad: 30 años

Estudiante de maestría