

**UNIVERSIDAD TÉCNICA FEDERICO SANTA MARÍA**

**DEPARTAMENTO DE ELECTRÓNICA**

**V**irtual **P**rivate **N**etwork

Integrantes: Marcela Barria 201002019-3

Nicole Bernal 201030013-7

Arturo Reyes 201030026-9

Profesor: Agustín González

Fecha: 30 de Julio de 2012

**Resumen**

Una red privada virtual (VPN) es una red virtual creada dentro de otra red, generalmente internet, por lo que los requerimientos de seguridad son de alto nivel e importancia. El intercambio efectivo de paquetes y la calidad son servicio importan mucho en el manejo de redes virtuales. La necesidad de acceder a recursos de la universidad o el trabajo es probable que aumente dramáticamente con la ejecución de nuevos proyectos y VPN ofrece soluciones a este tipo de necesidades conocidas como “acceso remoto”. Además, los servicios de VPN proporcionan un método seguro para mejorar este tipo de acceso a los materiales con licencia y otros recursos universitarios que restringe a los sistemas foráneos, por lo que si se conectan a través de un VPN asigna una dirección IP del campus, dando así comodidad y acceso a los servicios internos de una red.

**Introducción**

Hace unos años atrás no era tan necesario conectarse a internet por motivos de trabajo, pero hoy en día con el auge del internet, las empresas, universidades y distintas áreas de trabajo han visto la necesidad traspasar las redes locales LAN permitiendo la conectividad a su lugar de trabajo desde distintos lugares geográficos con acceso a internet. Esto es posible gracias a las Redes Virtuales Privadas o mejor dicho VPN.

En el siguiente informe detallaremos más sobre su uso y funcionamiento como también de la seguridad requerida para el tipo de información que circula por este tipo de red.

**¿Qué es una red virtual privada?**

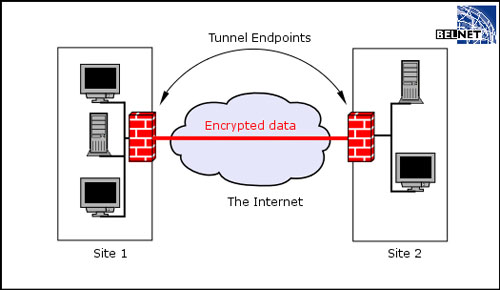
Hoy en día es habitual almacenar información en servidores, para hacerla accesible por los trabajadores de una empresa. Cualquier persona autorizada podrá consultar o modificar esta información, siempre que esté dentro de la red de la empresa, o cuando existen oficinas separadas de la sede central, se utilizan conexiones VPN para que la red de dichas oficinas se incorpore de forma segura a la Intranet. Cada uno de los emplazamientos utilizará la conexión a Internet para conectarse de forma segura a la Intranet constituida pasando a formar parte de la misma. De esta forma todo el personal de su empresa dispondrá de la misma información independientemente de su ubicación, eliminando las cuotas  por NetLan y similares.

Por lo tanto, se puede definir a una Red Privada Virtual VPN (sigla del inglés Virtual Private Network) como  una tecnología de red que permite la extensión de una red interna de una Organización sobre una red pública o no controlada (red insegura), externa a la Organización, como por ejemplo Internet, otorgando al usuario los mismos privilegios y nivel de acceso a la información que tendría si estuviese dentro de la Organización (físicamente).

**¿Cómo funciona una Red Virtual Privada?**

La comunicación entre los dos extremos de la red privada a través de la red pública se hace estableciendo túneles virtuales entre esos dos puntos y usando sistemas de encriptación y autentificación que aseguren la confidencialidad e integridad de los datos transmitidos a través de esa red pública. Debido al uso de estas redes públicas, generalmente Internet, es necesario prestar especial atención a las cuestiones de seguridad para evitar accesos no deseados.

La tecnología de túneles (Tunneling) es un modo de envío de datos en el que se encapsula un tipo de paquetes de datos dentro del paquete de datos propio de algún protocolo de comunicaciones, y al llegar a su destino, el paquete original es desempaquetado volviendo así a su estado original.

En el traslado a través de Internet, los paquetes viajan encriptados, por este motivo, las técnicas de autenticación son esenciales para el correcto funcionamiento de las VPNs, ya que se aseguran a emisor y receptor que están intercambiando información con el usuario o dispositivo correcto.   
  


**Ventajas de una VPN**

Hoy en dia las redes virtuales están siendo muy utilizadas debido a las ventajas que esta ofrece. Una de las más importantes que se pueden mencionar es la integridad, confidencialidad y seguridad de los datos. Aparte de que es muy sencilla de usar.

Por otro lado, la particularidad de VPN es que es posible conectarse desde una casa a la red de trabajo, o sea que hay flexibilidad con el trabajo con respecto a la comodidad. Otros de los beneficios es la seguridad que este emplea, ya que encripta los datos y los envía de forma segura sin ser intervenidos, por ende mantiene la integridad y la confiabilidad de los datos.

También evita el alto costos frente a otras soluciones WAN, ya que internet es una de las herramientas principales de VPN, se reduce considerablemente el costo de los enlaces físicos.

Otras ventajas pero no de menor importancia son:

* Reduce los tiempos y costos de tránsito para usuarios remotos
* Aumenta la productividad
* Simplifica la topología de red
* Provee oportunidades de trabajo en red globales
* Hace posible el soporte a esos trabajadores remotos
* Provee un retorno de inversión más rápido que una WAN tradicional

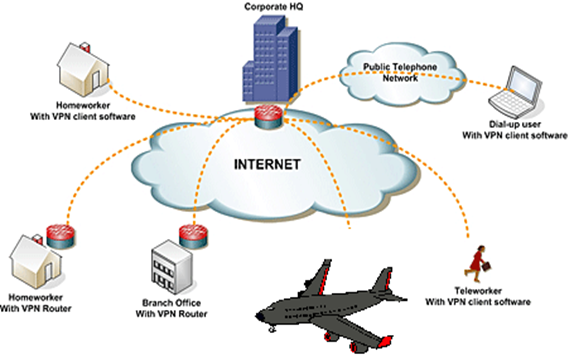
**Requerimientos de una VPN**

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

* **Identificación de usuario**: La VPN debe ser capaz de verificar la [identidad](http://www.monografias.com/trabajos14/cambcult/cambcult.shtml) de los usuarios y restringir el acceso a la VPN a aquellos usuarios que no estén autorizados. Así mismo, debe proporcionar [registros](http://www.monografias.com/trabajos7/regi/regi.shtml) 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](http://www.monografias.com/trabajos11/sercli/sercli.shtml) 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](http://www.monografias.com/trabajos12/mncerem/mncerem.shtml) de Internet (IP), el intercambio de paquete de Internet(IPX) entre otros.

**Tipos de VPN**

Según la utilidad que se le quiera dar a la red privada virtual es el tipo de VPN que utilizaremos:

* **De acceso remoto**: Es el modelo mas usado actualmente, ya que muchas empresas han remplazado con esta tecnología su infraestructura “dial-up”, donde el cliente utiliza un módem para llamar a través de la Red Telefónica Conmutada a un nodo proveedor de Servicios de Internet y este con un servidor establecía un enlace modem-a-modem, que permite entonces que se enrute a Internet. Pero hoy en día se conectan con la empresa desde sitios remotos, utilizando internet como vínculo de acceso. Una vez autentificados tienen un nivel de acceso muy similar al que tienen en la red local de la empresa.   
    
    
   
* **VPN de acceso remoto**: Este esquema se utiliza para conectar oficinas remotas con la sede central de organización. El servidor VPN, que posee vinculo permanente a Internet, acepta las conexiones vía Internet provenientes de los sitios y establece el túnel VPN. Los servidores de las sucursales se conectan a Internet, típicamente mediante conexiones de banda ancha. Esto permite eliminar los costosos vínculos punto a puntos tradicionales, sobre todo en las comunicaciones internacionales.
* **VPN over LAN**: También conocida como VPN interna. Es una aplicación realmente desconocida pero muy útil y potente consiste en establecer redes privadas virtuales dentro de una misma red local. El objetivo último es aislar partes de la red y sus servicios entre sí, aumentando la seguridad. Una aplicación muy típica de este modelo se utiliza para aumentar la seguridad en redes de acceso inalámbrico, separándolas así de la red física para evitar posibles fugas de información o accesos no autorizados.

**Conclusión**

Internet ha cambiado la forma como las personas se comunican, acortando distancias geográficas y acelerando la globalización del planeta.

Al apreciar las redes privadas virtuales nos podemos dar cuenta de cuan efectivas son. Se ha demostrado en la actualidad que las VPN 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 además dichas empresas demandan un alto rango de seguridad. Hoy en día es de vital importancia que se cumplan ciertos requisitos mínimos de seguridad y confiabilidad al momento de usar internet, ya sea para evitar usos maliciosos o simplemente porque no es algo que el usuario común deba preocuparse cada vez que trabaje en la web, es por eso que VPN resulta ser una muy buena solución, ya que por medio de su encriptación de datos mediante algoritmos como  *Data Encryption Standard* (DES), *Triple DES* (3DES) y *Advanced Encryption Standard* (AES) se logra que solo el usuario y el destinatario puedan hacer uso correcto de los datos.

**Anexo**

* <http://es.wikipedia.org/wiki/Red_privada_virtual>
* <http://www.configurarequipos.com/doc499.html>
* <http://www.monografias.com/trabajos11/repri/repri.shtml>
* <http://campusvirtual.unex.es/cala/cala/course/view.php?id=128>