

## Tutorial Redes Privadas Virtuales (VPNs sobre ADSL)

Cuando su empresa cuenta con más de una sucursal o mantiene intercambio constante de información entre sus proveedores y clientes, es vital encontrar una forma segura y económica de compartir información entre diferentes sucursales y ciudades.

Mantenga su operación informática de acuerdo a las exigencias del mundo moderno, donde la disponibilidad y presencia de la información en cualquier lugar forman parte del éxito de una empresa.

Una Red Privada Virtual en IP, es una conexión privada entre dos o más computadoras que intercambian tráfico privado a través de una red pública compartida como Internet (enlaces de banda ancha ADSL). Esta tecnología permite a las organizaciones extender sus servicios de red, a través de Internet, hacia sus sucursales y usuarios remotos creando una WAN (Wide Area Network) privada vía Internet.

Utilizando tunneling, encriptación, autenticación y tecnología de directorios, las Redes Privadas Virtuales en IP le ofrecen confidencialidad y el más alto nivel de seguridad en el intercambio de datos entre las diferentes sucursales de una empresa, además de grandes ahorros en los gastos de operación.

### ¿Qué es una Red Privada Virtual (VPN)?

Una VPN es una red privada que utiliza el Internet para conectar con seguridad usuarios o sitios remotos. En lugar de usar líneas dedicadas, una VPN utiliza una conexión "virtual" enrutada a través de Internet.

Desde la perspectiva del usuario, una VPN opera transparentemente, dándole la sensación como si estuviera trabajando en la oficina. El correo electrónico, bases de datos, Intranets, Voz sobre IP, Video o cualquier otra aplicación puede pasar a través de una conexión de VPN.

### Esto era antes...

#### **Red de Área Amplia (denominada WAN, por sus siglas en inglés Wide Area Networking)**

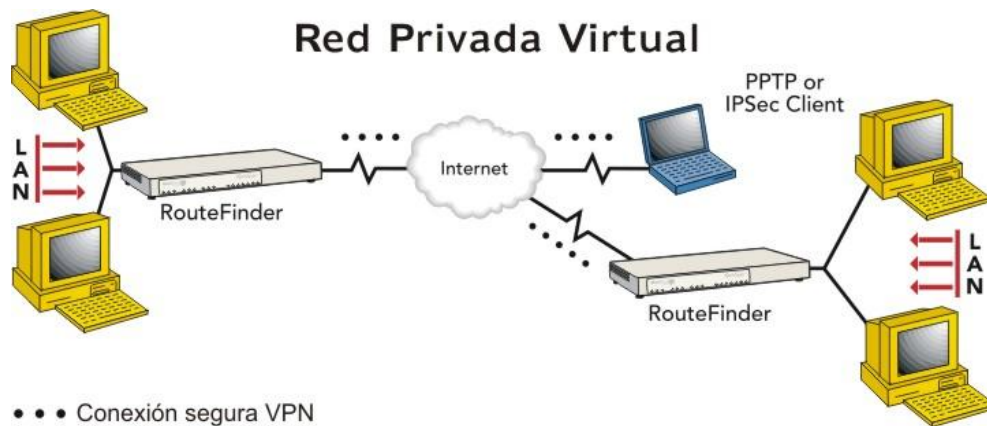
Las soluciones tradicionales de WAN requieren que las compañías mantengan enlaces directos entre la red corporativa y los sitios remotos. Para mantener esta conexión de Red-a-Red, las compañías típicamente tienen que contratar líneas privadas de datos, con costos elevados.

#### **Servicio de Acceso Remoto (denominado RAS, por sus siglas en inglés Remote Access Services)**

Las soluciones tradicionales de acceso remoto Cliente-a-Red, usan lentas conexiones de marcado telefónico a través de módems o complicados servidores de acceso remoto. Estas conexiones de marcado telefónico son caras considerando los cargos de larga distancia que generan, además de ser muy lentas en la transmisión y recepción.

## Esto es ahora...

Con la llegada más accesible de tecnologías de banda ancha (ADSL), los negocios pequeños y medianos ahora pueden usar el Internet y las Redes Privadas Virtuales (VPN) para evitar el alto costo de las conexiones tradicionales de acceso remoto y WAN. Una VPN permite a una compañía aprovechar los beneficios del acceso remoto, sin el alto costo de la infraestructura técnica compleja.



## APLICACIONES

### VPN en Sucursal (reemplaza una WAN)

La aplicación de una VPN de Red-a-Red envía tráfico de red sobre la conexión de Internet de la Sucursal, en lugar de depender de conexiones de líneas dedicadas. Esto puede ahorrar miles de pesos en costos de líneas y reducir los altos costos en hardware y administración.

### VPN de Usuario Remoto (reemplaza un Servicio de Acceso Remoto)

La aplicación de una VPN Cliente-a-Red envía el tráfico del usuario remoto sobre su conexión de Internet. La ventaja es que el usuario remoto puede hacer una llamada local a un proveedor de servicio de Internet, en comparación con una llamada de larga distancia al servidor de acceso remoto de la compañía.

## VENTAJAS DE LA VPN

Además de reducir los costos de comunicaciones, una solución VPN también proporciona las siguientes ventajas:

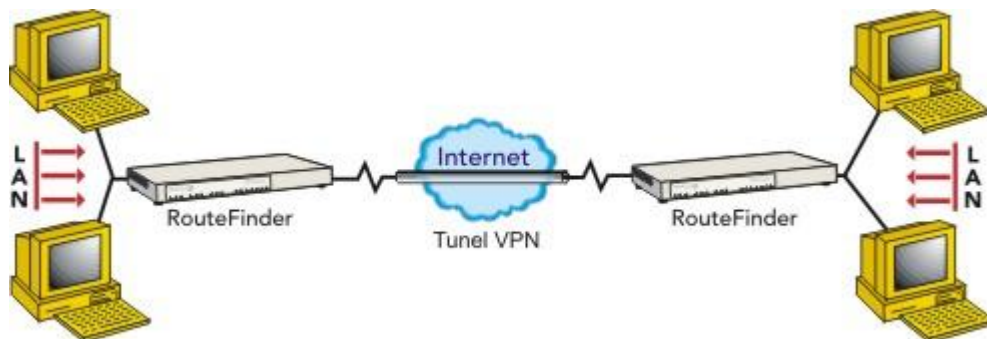
- **Extiende la conectividad geográfica** - Una VPN conecta a empleados remotos a los recursos centrales.

- **Crecimiento en productividad de empleados** - Una solución de VPN permite a los empleados remotos aumentar su productividad un 22% - 45% (Gallup Organization and Opinion Research) eliminando tiempo.
- **Mejora la seguridad de Internet** - Siempre en una conexión de banda ancha a Internet, hace a una red vulnerable a ataques de hacker's. Muchas soluciones de VPN incluyen medidas de seguridad adicional, tales como dispositivos de seguridad ("firewall") y anti-virus de chequeo para contrarrestar los diferentes tipos de amenazas a la seguridad de la red.
- **Fácilmente escalable** - Una VPN permite a las compañías utilizar la infraestructura de los accesos remotos dentro de los ISP's. Por lo tanto, las compañías pueden agregar virtualmente una cantidad ilimitada de capacidad sin añadir infraestructura que sea significativa.
- **Simplifica la topología de Red** - La eliminación de módems y una infraestructura de red privada, simplifica la administración de la red.

### ¿Cómo trabaja una VPN?

En una VPN, una compañía usa el ancho de banda de Internet para establecer conexiones privadas y seguras entre sus empleados y oficinas remotas. Cada usuario remoto se conecta con el proveedor de servicio de Internet local en la misma forma que accesa a Internet por marcado telefónico, cable, DSL, ISDN, T1 o wireless.

Un proceso llamado "túnel" es usado para llevar la información sobre Internet. Sin embargo, el túnel por si solo no asegura la privacidad. Para asegurar una transmisión de túnel contra interceptaciones, todo el tráfico sobre una VPN es encriptado para su seguridad.



### ¿Qué es "hacer un túnel"?

Esencialmente, "hacer un túnel" es el proceso de colocar todo un paquete dentro de otro (el cual proporciona información de ruteo) y enviarlo sobre Internet. La ruta a través de la cual los paquetes viajan es llamada túnel. Para que un túnel sea establecido, el túnel del servidor y del cliente debe estar usando el mismo protocolo de túnel.

Dos protocolos populares para hacer túnel son el Protocolo de Túnel Punto a Punto (denominado PPTP, por sus siglas en inglés Point-to-Point Tunneling Protocol) y el Protocolo de Seguridad de Internet (denominado IPSec, por sus siglas en inglés Internet Protocol Security). La ventaja de usar PPTP es que está integrado dentro del sistema operativo de Windows® permitiendo a cualquier cliente correr Windows® para conectarse con seguridad al ruteador VPN de la oficina corporativa. Por otra parte, IPSec requiere software de Cliente para usuarios remotos. La ventaja de IPSec es que provee mejor seguridad con una encriptación más fuerte y de más alto desempeño que PPTP.

### ¿Qué es Encriptación?

Encriptación es el proceso de tomar toda la información que una computadora está enviando a otra y codificarla de una manera que sólo la otra computadora será capaz de descifrarla. El paquete de datos IP que está siendo enviado a través de Internet es primero encriptado y luego envuelto dentro de otro paquete IP. La Oficina corporativa y los ruteadores de Internet ven a los paquetes "envueltos", mientras que la información interna se mantiene segura en la sección de carga del primer paquete IP.

El protocolo IPSec usa el método Estándar de Encriptación de Información (Data Encryption Standard, DES) para codificar y decodificar información. El rango de longitud de la llave de encriptación es de 56 bits (DES) a 168 bits (3DES). Hasta la fecha, triple DES es el nivel más fuerte de encriptación pública disponible. Es exponencialmente más difícil de descifrar que DES; no es sólo tres veces más difícil. Microsoft's PPTP usa llaves de encriptación de 40 o 128 bits.

### AUTENTIFICACION

Uno de los más importantes elementos de seguridad para una VPN es identificar al usuario. Esto es esencial para determinar a qué recursos la persona está autorizada a usar. IPSec permite a los dispositivos usar un procedimiento llamado Intercambio de Llave de Internet (Internet Key Exchange, IKE) para transferir llaves de seguridad.

### TERMINOS COMUNES DE VPN

**Autenticación** - establecer la identidad de un usuario para transacciones seguras de e-commerce y VPN.

**DES (Estándar de Encriptación de Información, 3DES, Data Encryption Standard)** - Un método de criptografía estándar del NIST de clave secreta que usa una llave de 56 bits (DES) o una llave de 168 bits (3DES).

**Rechazo de Servicio (denominado DoS, por sus siglas en inglés Denial of Service)** - un ataque de hacker diseñado para deshabilitar un servidor o red al saturarlo con solicitudes de servicio el cual previene a usuarios legítimos de acceder a los recursos de la red.

**Encriptación** - el proceso de tomar toda la información que una computadora está enviando a otra y codificarla de una manera que sólo la otra computadora será capaz de decodificarla.

**Firewall** - a dispositivo de seguridad que controla el acceso desde Internet a una red local usando información asociada con paquetes TCP/IP para hacer decisiones sobre si se permiten o niegan accesos.



**Asociación Internacional de Seguridad Computacional (denominada ICSA, por sus siglas en inglés International Computer Security Association)** - fija estándares de desempeño para productos de seguridad de información y certifica cerca del 95% de la base instalada de dispositivos de seguridad ("firewall"), antivirus, criptografía y productos IPSec.

**Protocolo de Seguridad de Internet (IPSec, Internet Protocol Security)** - un estándar IETF robusto de VPN que abarca autenticación y encriptación de tráfico de datos sobre Internet.

**Traductor de dirección de red (denominada NAT, por sus siglas en inglés Network Address Translation)** - un estándar de seguridad que convierte múltiples direcciones IP en la red local privada a una dirección pública que es enviada al Internet.

**Protocolo de Túnel Punto a Punto (denominado PPTP, por sus siglas en inglés Point-to-Point Tunneling Protocol)** - un protocolo que está integrado en el sistema operativo Windows de Microsoft que permite acceso remoto con seguridad a redes corporativas sobre Internet (VPNs).

**Inspección de Estado de Paquetes (Stateful Packet Inspection)** - un dispositivo de seguridad ("firewall"), basado en la tecnología avanzada de filtrado de paquetes, que es transparente para los usuarios de la red local, no requiere configuración del cliente y asegura el arreglo más amplio de protocolos IP.

**Túnel** - la ruta a través de la cual un paquete de datos VPN con seguridad, viaja a través de la red interna.

**Virus** - programas de software dañino que atacan aplicaciones y archivos en memoria o discos.

## Grupo ACT

<http://www.grupoact.com>