# Tecnología VPN (1ª parte)

***Lic. María Teresa Lozano Hernández,***
***Lic. María de Lourdes Olvera Cárdenas,***
***Ing. María del Rocío Velázquez Serrano,***
***Profesoras del CIDETEC-IPN***

Desde hace mucho tiempo, el mundo empresarial se enfrenta a la necesidad de implementar sistemas eficientes de manejo de información. La solución para muchas de estas empresas, independientemente de su actividad, ha sido las redes de telecomunicaciones, a través de las cuales han abatido costos y gastos de operación, manufactura, recursos humanos, etc. El uso de la tecnología de telecomunicaciones benefició a las empresas para agilizar sus ventas y básicamente sus movimientos contables, así como el servicio y soporte a los equipos sin tener que viajar entre ciudades o países. Las compañías prestadoras de servicios de telecomunicaciones comenzaron a invertir cada vez más en infraestructura para poder ofrecer mayor cantidad y calidad de servicios (QOS).

Esto también generó altos gastos de equipamiento para las empresas que se iniciaron en estas áreas, dudando muchas de ellas en invertir en equipo de comunicaciones. Por otro lado, la industria de las telecomunicaciones se vio favorecida y, hasta hace poco todavía, monopolizada. En la actualidad el beneficio de las telecomunicaciones se ha hecho cada vez mayor de tal forma que el número de servicios privados de los proveedores se ha visto disminuido o le han dado un giro para aprovecharlo en otros servicios. Para las compañías clientes esto ha significado la reducción de hasta un 75% los gastos por renta de enlaces privados.

El porque de todo ello es el uso de las VPN's (Virtual Private Network) siendo estas la respuesta lógica al crecimiento de Internet; ya que permiten reemplazar líneas dedicadas por accesos a Internet con características adicionales. Se puede decir que una VPN es el uso de una infraestructura de telecomunicaciones pública para el uso privado o bien una conexión punto a punto de oficinas con usuarios remotos. Tal infraestructura pública está al alcance de casi cualquier persona o empresa a través de Internet. Sin embargo, por tratarse de una infraestructura pública es de esperase que los datos pasaran a través de muchos puntos inseguros.

El objetivo principal de las VPN's es la seguridad y cualquier VPN que se precie de serlo deberá manejar los datos privados y confidenciales con un alto índice de seguridad. Una VPN típica cuenta con oficinas corporativas, una o más sucursales, cada una con sus enlaces a Internet de algún proveedor de servicios, un usuario remoto y un usuario móvil.

Aún cuando pareciera que una VPN es insegura, por el medio que utiliza, no lo es. Estas redes manejan un protocolo de seguridad para Internet llamado IPSec y al mismo tiempo el protocolo estándar de IP, tanto para autentificar como para cifrar datos, de tal suerte que los equipos intermedios por donde pasa la información no distinguen entre un paquete IP y un paquete IPSec. Las VPN´s también manejan certificados de seguridad como los bancos y otras instituciones. Los protocolos empleados tienen compatibilidad con equipos y aplicaciones. La seguridad se efectúa de extremo a extremo, ya que solo los equipos que se interconectan conocen el cifrado.

La red privada se extiende mediante un proceso de encapsulación y 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 1**. Conexión VPN

Las topologías pueden tener lógicas punto a punto, punto a multipunto; dependiendo de ello se generan las políticas de acceso así como también se forma el esquema de equipamiento de protección contra intrusos.

Antes de analizar las ventajas hablemos del caso en que se desea enlazar las oficinas centrales con alguna sucursal u oficina remota utilizando:

Modem: La desventaja es el costo de la llamada, ya que el costo de esta llamada sería por minuto conectado,

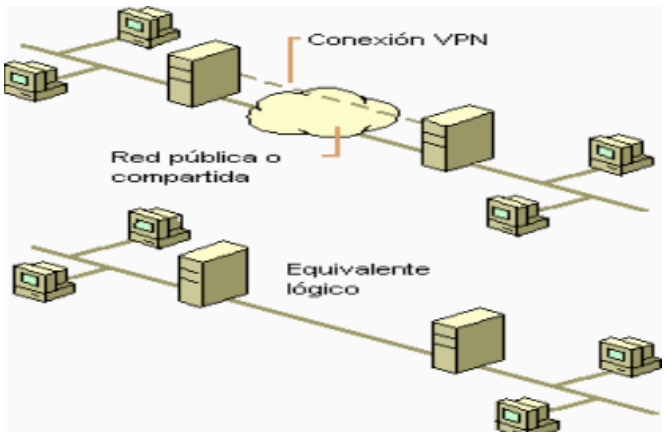


**Figura 1. Conexión VPN.**

además sería una llamada de larga distancia, a parte no se contaría con la calidad y velocidad adecuadas.

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

VPN: Los costos son bajos porque solo se realizan llamadas locales, contando con que los datos viajan encriptados y seguros, con una buena calidad y velocidad, ver **figura 2**.

Los datos a través de una VPN pasan por el servidor dedicado, del cual parten, llegando a un firewall que a su vez hace la función de una pared para engañar a los intrusos, después los datos llegan a la nube de Internet donde se genera un túnel dedicado por el cual únicamente pasan estos con una velocidad garantizada, ancho de banda, también garantizado; los datos lleguen a su vez al firewall remoto y terminan en el servidor remoto. Las VPN's pueden enlazar oficinas corporativas con los socios, con usuarios móviles, con oficinas remotas mediante los protocolos como Internet, IP, Ipsec, Frame Relay y/o ATM, como se muestra en la **figura 3**.

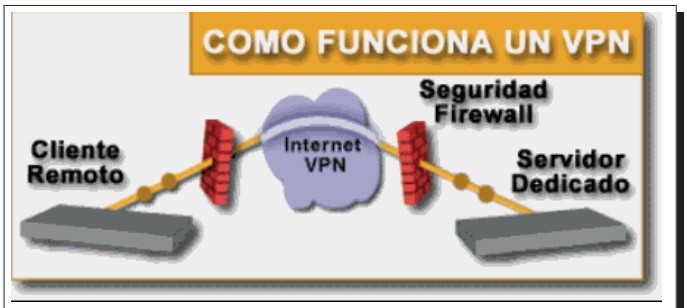


**Figura 2. Solución VPN.**

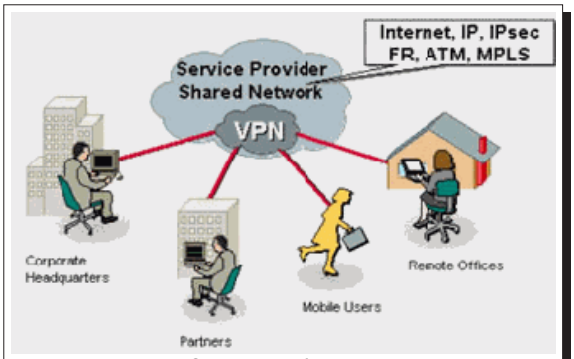


**Figura 3. Protocolos para VPN.**

## *1 Ventajas de una VPN*

Hasta el momento solo podemos hablar de las bondades que nos ofrece el uso de las VPN's en una comparativa con las redes tradicionales. Dentro de las ventajas más significativas podremos mencionar la integridad, confidencialidad y seguridad de los datos. A continuación se enlistan algunas de estas:

- Reducción de costos.
- Sencilla de usar.
- Sencilla instalación del cliente en cualquier PC Windows.
- Manipulación en otros Sistemas Operativos
- Creación a partir de software o hardware
- Control de Acceso basado en políticas de la organización
- Herramientas de diagnóstico remoto.
- Manejo de direccionamiento propio
- Los algoritmos de compresión optimizan el tráfico del cliente.
- Evita el alto costo de las actualizaciones y mantenimiento a las PC´s remotas.

Con respecto a la reducción de costo tenemos: reducción de costo de conectividad por líneas dedicadas eliminadas, menos accesos telefónicos, reducción de tiempo de configuración y mantenimiento ante una eventual caída del servidor o de la red misma, reducción de contratos de mantenimiento y configuración; eliminación de equipos PBX propiedad del cliente, sistemas de almacenamiento de energía o sistemas de energía ininterrumpible, sistemas de enfriamiento, etc., necesarios para el buen funcionamiento del cuarto de telecomunicaciones. Es importante recordar que el costo de los enlaces varía según la distancia.

## 2 Otras Ventajas

Incluyen la escalabilidad y flexibilidad de interconexión ya que permiten anexar nuevas conexiones o eliminar tantas conexiones como usuarios remotos se agreguen o dejen de utilizarla; la seguridad que involucra el cifrado de la información y la autentificación de los usuarios; diseño simplificado que reduce tiempos y costos de mantenimiento asociados a la gestión de la red; compatibilidad con protocolos de red más comunes (TCP/IP, IPX, NetBEUI), lo cual provoca el corrimiento de aplicaciones soportadas por estos protocolos, prioridad de tráfico ligado a las políticas de admi-

nistración de uso del ancho de banda a través de un administrador.

## *Tecnología de Túnel*

Las redes privadas virtuales crean un túnel (**figura 4**) 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.

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

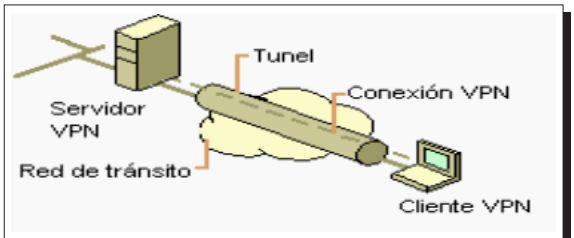


**Figura 4. Tecnología de túnel.**

## *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

### 2 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.

### 2 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.

### 2 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.

### 2 Administración de Claves

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

### 2 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.

## *Herramientas de una VPN*

Las herramientas típicas de una VPN son:

- VPN Gateway
- Software
- Firewall
- Router

Los datos transitan codificados por Internet en «Túneles Virtuales» creados por los dispositivos VPN que utilizan criptografía; estos dispositivos son capaces de «entender» los datos codificados y forman una «red virtual» sobre la red pública. Es esa red virtual la que es conocida como VPN.

Los dispositivos responsables para la formación y administración de la red virtual, para propiciar una comunicación con seguridad, deben ser capaces de garantizar:

*La seguridad de los datos*, en el caso que fuesen interceptados durante la transmisión, no pueden ser decodificados.

*Integridad de los datos*, además de no ser decodificados (seguridad), los datos no pueden ser modificados durante la transmisión.

*La autenticación*, garantía de que los datos están siendo trasmitidos o recibidos del dispositivo remoto autorizado y no de un equipamiento cualquiera, o sea, garantía de que el dispositivo remoto con el cual fue establecido el túnel, es el dispositivo remoto autorizado y no otro equipamiento haciéndose pasar por él.

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

## *IP's Públicas, Privadas y sus Clases*

Las IP's de todo el mundo son clasificadas en públicas y privadas. Las IP's públicas también conocidas como IP's homologadas, y se consiguen de manera permanente pagando una cantidad por la renta de cada IP que la compañía solicita. Éstas IP's tienen la característica de ser globalmente ruteables, mientras que las IP's no homologadas solo pueden ser ruteadas en un ambiente totalmente privado.

La división para las IP's versión 4 se lleva a cabo por una división en clases.

| Formato | Bits de orden superior | Rango de direcciones | Número de bits de red y host | Máximo de hots |
|---|---|---|---|---|
| RH.H.H | 1/0 | 1.0.0.0 a | 7/24 | $2^{24}$-2 |
| RRH.H | 2/10 | 128.1.0.0 a 191.254.0.0 | 14/16 | $2^{16}$-2 |
| RRRH | 3/110 | 192.0.1.0 a 223.255.254.0 | 22/8 | $2^{8}$-2 |
| No utilizado | 4/1110 | 224.0.0.0 a 239.255.255.255 | No se utilizan | No utilizados |
| No utilizados | 4/1111 | 240.0.0.0 a 254.255.255.255 | No se utilizan | No utilizados |

**Tabla 1. Clases de redes IP's.**

| Rango de direcciones | Clase | Número de redes |
|---|---|---|
| 10.0.0.0 10.255.255.255 | A | 1 |
| 172.16.0.0 172.31.255.255 | B | 16 |
| 192.168.0.0 192.168.255.255 | C | 256 |

**Tabla 2. Rango para direcciones privadas.**

Las clases de redes IP's se muestran en la **tabla 1** y el rango para direcciones privadas se muestra en la **tabla 2**.

## *Infraestructura Para Una VPN*

### Equipamiento

Para poder crear una VPN debemos tener acceso a Internet mediante cualquier tecnología disponible en nuestro centro de trabajo ya sea inalámbrica, mediante POTS, ISDN, ADLS o algún otro medio de acceso hacia la red. Es de hacer notar que la velocidad de acceso irá estrechamente relacionada con la cantidad de información que se desee pasar por el túnel de la VPN, es obvio que las oficinas centrales deberán contar con un enlace de mayor capacidad ya que estas proveerán la mayor parte de la información para ser accesadas por los usuarios y las oficinas remotas.

Teniendo el enlace se requiere una solución para manejar la(s) VPN('s), esto puede llevarse a cabo mediante software o hardware, las soluciones por hardware son más recomendables, ya que son las que tienen un mejor performance, además permiten un mejor rendimiento del enlace que utilice para acceder a servicios públicos y a las VPN's.

### Seguridad en los Enlaces

#### Redundancia

Para una VPN que corre aplicaciones críticas es necesario manejar algún tipo de redundancia, existen proveedores de equipo que manejan una redundancia en sus equipos al hacer que soporten un sistema de fail-over.

Un sistema de fail-over consiste en tener un equipo con redundancia en la comunicación WAN, de tal suerte que se pueda detectar cuando falla el enlace principal y de esta manera conmutar la comunicación al enlace de respaldo, el enlace principal seguirá siendo censado para detectar cuando vuelva a estar arriba para volver a éste.

#### Encriptamiento

Las redes VPN basadas en IPsec son de mayor demanda en estos días, por lo tanto nos enfocaremos a describir el estándar de IPsec.

## *Protocolos de VPN (IPSec)*

Las redes se diseñan normalmente para impedir el acceso no autorizado a datos confidenciales desde fuera de la intranet de la empresa mediante el cifrado de la información que viaja a través de líneas de comunicación pública. Sin embargo, la mayor parte de las redes manejan las comunicaciones entre los hosts de la red interna como texto sin formato. Con acceso físico a la red y un analizador de protocolos, un usuario no autorizado puede obtener datos privados.

IPsec autentifica los equipos y cifra los datos para su transmisión entre hosts en una red, intranet o extranet, incluidas la comunicaciones entre estaciones de trabajo y servidores, y entre servidores. El objetivo principal de IPsec es proporcionar protección a los paquetes IP. IPsec esta basado en un modelo de seguridad de extremo a extremo, lo que significa que los únicos hosts que tienen que conocer la protección de IPsec son el que envía y el que recibe. Cada equipo controla la seguridad por sí mismo en su extremo, bajo la hipótesis de que el medio por el que se establece la comunicación no es seguro.

IPsec aumenta la seguridad de los datos de la red mediante:

- La autenticación mutua de los equipos antes del intercambio de datos. IPsec puede utilizar kerberos V5 para la autenticación de los usuarios.
- El establecimiento de una asociación de seguridad entre los dos equipos. IPsec se puede implementar para proteger las comunicaciones entre usuarios remotos y redes, entre redes e incluso, entre equipos cliente dentro de una red de área local (LAN).
- El cifrado de los datos intercambiados mediante **Cifrado de datos estándar** (DES, Data Encryption Standard), triple DES (3DES) o DES de bits. IPsec usa formato de paquete IP estándar en la autenticación o el cifrado de los datos. Por tanto, los dispositivos de

red intermedios, como los enrutadores, no pueden distinguir los paquetes de IPsec de los paquetes IP normales.

El protocolo también proporciona las siguientes ventajas:

- Compatibilidad con la infraestructura de claves públicas. También acepta el uso de certificados de claves públicas para la autenticación.
- Compatibilidad con claves compartidas. Si la autenticación mediante kerberos V5 o certificados de claves públicas no es posible, se puede configurar una clave compartida (una contraseña secreta compartida) para proporcionar autenticación y confianza entre equipos.
- Transparencia de IPsec para los usuarios y las aplicaciones. Como IPsec opera al nivel de red, los usuarios y las aplicaciones no interactúan con IPsec.
- Administración centralizada y flexible de directivas mediante directiva de grupo. Cuando cada equipo inicia una sesión en el dominio, el equipo recibe automáticamente su directiva de seguridad, lo que evita tener que configurar cada equipo individualmente. Sin embargo, si un equipo tiene requisitos exclusivos o es independiente, se puede asignar una directiva de forma local.
- Estándar abierto del sector. IPsec proporciona una alternativa de estándar industrial abierto ante las tecnologías de cifrado IP patentadas. Los administradores aprovecha la interoperabilidad resultante.

## *Ataques a la Seguridad*

A continuación se presenta una lista parcial de los ataques más comunes a las redes tradicionales:

- Rastreo. Un rastreo de red es una aplicación o un dispositivo que puede supervisar y leer los paquetes de la red. Si los paquetes no están cifrados, un rastreo de red obtiene una vista completa de los datos del paquete. El monitor de red de Microsoft es un ejemplo de rastreador de red.
- Modificación de datos. Un atacante podría modificar un mensaje en tránsito y enviar datos falsos, que podrían impedir al destinatario recibir la información correcta o permitir al atacante conseguir la información protegida.
- Contraseñas. El atacante podría usar una contraseña o clave robada, o intentar averiguar la contraseña si es fácil.
- Suplantación de direcciones. Este ataque va dirigido a servidores de aplicaciones al explotar las debilidades del sistema operativo y de las aplicaciones del servidor.
- Intermediario. En este tipo de ataque, alguien entre los dos equipos comunicantes esta supervisando activamente, capturando y controlando los datos de forma desapercibida, (el atacante puede estar cambiando el encaminamiento de un intercambio de datos).
- Denegación de servicio. El objetivo de este ataque es impedir el uso normal de equipos o recursos de la red. Por ejemplo, cuando las cuentas de correo electrónico se ven desbordadas con mensajes no solicitados.

## *IPsec*

### Características de Seguridad de IPsec

Las siguientes características de IPsec afrontan todos estos métodos de ataque:

- Protocolo Carga de seguridad de encapsulación (ESP, Encapsulating Security Payload). ESP proporciona privacidad a los datos mediante el cifrado de los paquetes IP.
- Claves basadas en criptografía. Las claves cifradas, que se comparten entre los sistemas que se comunican, crean una suma de comprobación digital para cada paquete IP. Cualquier modificación del paquete altera la suma de comprobación, mostrando al destinatario que el paquete ha sido cambiado en su tránsito. Se utiliza material de claves diferentes para cada segmento del esquema de protección global y se puede generar un nuevo material de claves con la frecuencia especificada en la directiva de IPsec.
- Administración automática de claves. Las claves largas y el cambio dinámico de claves durante las comunicaciones ya establecidas protegen contra los ataques. IPsec usa el protocolo Asociación de seguridad en internet y administración de claves (ISAKMP, Internet Security Association and Key Management Protocol) para intercambiar y administrar claves cifradas entre los equipos que se comunican.
- Negociación de seguridad automática. IPsec usa ISAKMP para negociar de forma dinámica un conjunto de requisitos de seguridad mutuos entre los equipos que se comunican. No es necesario que los equipos tengan directivas idénticas, solo una directiva configurada con las opciones de negociación necesarias para establecer un conjunto de requisitos con otro equipo.
- Seguridad a nivel de red. IPsec existe en el nivel de red, proporcionando seguridad automática a todas las aplicaciones.
- Autenticación mutua. IPsec permite el intercambio y la comprobación de identidades sin exponer

la información a la interpretación de un atacante. La comprobación mutua (autenticación) se utiliza para establecer la confianza entre los sistemas que se comunican. Sólo los sistemas de confianza se pueden comunicar entre sí. Los usuarios no tienen que estar en el mismo dominio para comunicarse con la protección de IPsec. Pueden estar en cualquier dominio de confianza de la empresa. La comunicación se cifra, lo que dificulta la identificación e interpretación de la información.

- Filtrado de paquetes IP. Este proceso de filtrado habilita, permite o bloquea las comunicaciones según sea necesario mediante la especificación de intervalos de direcciones, protocolos o, incluso, puertos de protocolo específicos.

### Componentes de IPsec

En el proceso de autenticación y cifrado de IPsec intervienen varios componentes. Su conocimiento y el de los procesos en que consiste la comunicación IPsec le ayudará a encontrar soluciones a los problemas de implementación.

### El proceso de Negociación y Filtrado

Cuando un equipo configurado con una directiva de IPsec intenta comunicarse con otro equipo, comienza el proceso siguiente:

1. Las directivas de IPsec se entregan al controlador de IPsec y el intercambio de clave ISAKMP/Oakley a través de directivas locales o configuraciones de directivas de grupo.
2. ISAKMP supervisa las negociaciones entre los hosts y proporciona claves que se usan con algoritmos de seguridad.
3. El controlador de IPsec supervisa, filtra y protege el tráfico entre el nivel de transporte y el nivel de red.

## *Conclusión*

Las VPN representan una gran solución para las empresas en cuanto a seguridad, confidencialidad e integridad de los datos y prácticamente 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, así como el de omitir gastos en telefonía local y de larga distancia y otros servicios, el único 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 de interferencia por intrusos. En la siguiente publicación abordaremos otros temas relacionados con la puesta en pie de una VPN.

## *Bibliografía*


**[1]** Uyless Black, *"Tecnologías Emergentes de Telecomunicaciones"*, 2a. edic. Prentice Hall.

**[2]** Williams Stallings, *"Handbook of Computer – Communications Standards Vol. 3"*, Stallings / Macmillan Books.

**[3]** Stephen J. Bigelow, *"Herramientas, mantenimiento y reparación de Redes"*, Mc Graw Hill