Capítulo 3

VPN

Las redes virtuales privadas han existido desde hace un tiempo, y sus usos se han diversificado conforme estas se adaptan a las distintas tecnologías emergentes. Parte de esto hace necesario que se expongan sus características y posibilidadaes, por lo que en el presente capítulo mencionaremos sus principales características, requerimientos y algunas de sus ventajas y desventajas.

Capítulo 3 VPN

Una red privada virtual **VPN** (***Virtual Private Network***), se le conoce al tipo de red que permite una extensión de una red local sobre una red pública o no controlada, como por ejemplo Internet.

Las VPNs surgen ante la necesidad de las organizaciones o corporativos de proveer a su personal con la capacidad de acceder a su infraestructura de red interna, o intranet desde cualquier lugar y en cualquier momento de forma segura. Así las VPNs aparecen como las redes privadas con la capacidad de utilización de la infraestructura de Internet para el transporte de datos, implementando técnicas de seguridad para mantener la confidencialidad de los datos que se manejan entre los usuarios.

Ahora es posible implementar distintos tipos de VPNs, como las VPN sitio-a-sitio, VPNs de acceso remoto, VPNs LAN-2-LAN, VPNs confiables, VPNs seguras, L1VPNs, L2VPNs, L3VPNs, VPNs VPWS, VPNs VPLS, VPNs IPLS, VPNs basadas en esquemas de red, VPNs basadas en C(P)E, VPNs multiservicio, VPNs suministradas por el usuario, VPNs Internet, VPNs Intranet, VPN extranets, VPNs punto-a-punto, VPNs multipunto-a-multipunto, VPNs orientadas a la conexión, VPNs connectionless, etc. Además hay redes virtuales basadas en L2TPv3, AToM, capa 3 MPLS, L2F, L2TPv2, PPTP y SSL.

Una **VPN** da la capacidad de proveer los servicios de redes privadas para organizaciones tales como los proveedores de servicio de Internet **ISPs** (*Internet Service Providers*) o los proveedores de red en la dorsal que es conocido como la VPN dorsal (V*PN backbone*) y es usado para transportar tráfico de múltiples VPNs, así como posible tráfico no VPN.

Las VPNs suministradas usando tecnologías tales como **Frame Relay** y circuitos virtuales **VC**-**ATM** (*virtual circuit-Asynchronous Transfer Mode*) han estado disponibles por mucho tiempo, pero en los años recientes las VPNs IP son más y más populares.

Es importante destacar la seguridad como factor importante al establecer las VPN, así como proporcionar y garantizar la autenticación, confidencialidad e integridad dentro del canal de comunicación.

Esta autenticación se resume a saber quien se encuentra en el otro extremo, así como el nivel y facultades de acceso que debe de tener. Garantizar la integridad, es decir, que la información no sufra alteraciones y para eso se utilizan algoritmos especializados.

Debido a una posible interceptación de datos a través del canal se debe de garantizar la confidencialidad de esta información, por eso es necesario establecer un cifrado de los datos, y así la información sólo se entenderá para las partes involucradas, siendo inútil para el intruso a la red.

3.1 Clasificación de las VPN

3.1.1 VPN de acceso remoto

Este modelo consiste en que los usuarios se conectan desde un sitio remoto y se utiliza internet como un vínculo de acceso y después de ser autenticados se puede decir que el nivel de acceso que poseen es como el de una red local.

3.1.2 VPN punto a punto

En este modelo la arquitectura a seguir es la de conectar los nodos remotos con la matriz o punto central. El servidor VPN siempre debe de tener un vínculo permanente con Internet y debe de aceptar las conexiones provenientes de los sitios y establecer el llamado túnel VPN; mientras que los puntos externos deben de utilizar los servicios de su proveedor local de internet por medio de banda ancha, a este fenómeno también se le conoce como túneleo (tunneling).

Lo anterior permite tener una cuenta de acceso seguro en la máquina con la que se quiere comunicar los datos.

3.1.3 VPN interna

Esta opción tiene las mismas cualidades de una VPN tradicional, la única diferencia es que en lugar de utilizar internet como medio de acceso, utiliza la red local del edificio donde se encuentra, con lo cual su nivel de seguridad es mayor que cualquier red WiFi.

3.1.4 VPN basada en firewall

Este tipo de VPN aprovecha los mecanismos de seguridad del servidor de seguridad, incluyendo la restricción del acceso a la red interna, realiza la traducción de direcciones, satisfaciendo los requisitos de autenticación. La mayoría de los firewalls comerciales también optimizan al núcleo del sistema operativo al despojar a los servicios innecesarios o peligrosos, proporcionando seguridad adicional para el servidor VPN. La desventaja de este tipo de tecnología es poder optimizar su desempeño de manera eficiente sin mermar las aplicaciones del sistema operativo.

3.1.5 VPN basada en software

Estas VPNs son ideales en casos donde ambos extremos de la VPN no están controlados por la misma organización o cuando diferentes firewalls y enrutadores se implementan dentro de la misma. Por el momento, las VPNs independientes ofrecen mayor flexibilidad en cómo se gestiona el tráfico de red. Muchos productos basados en software permiten que el tráfico de túnel se dependa de la dirección o protocolo, a diferencia de los productos basados en hardware, que en general encapsulen el tráfico que manejan, independientemente del protocolo.

Pero el software de los sistemas en que están basados generalmente son más difíciles de manejar que el cifrado de los enrutadores. Ellos requieren familiaridad con el sistema operativo del Host, la propia solicitud, y los mecanismos de seguridad adecuados. Y algunos paquetes de software de VPN requieren cambios en las tablas de enrutamiento y sistemas de direccionamiento de red.

Las VPNs también pueden clasificarse de acuerdo a criterios de función:

Por su punto de terminación, pueden estar basadas en las CE (overlay) o en el PE (peer-to-peer); por el tipo de tráfico de cliente transportado (nivel 2 y nivel3 del modelo OSI); por el tipo de red del proveedor (IP, IP/MPLS, ATM, Frame Relay, SONET/SDH, pppoe, etc); por tecnología de túnel (IPSec, L2TP, PPTP, MPLS-LPS, ATM-VP/VC, Frame Relay VC, SONET/SDH VT, PPP/Dial-up), y por el número de nodos conectados en multipunto y punto a punto.

3.2 Arquitecturas de las VPNs

Dentro de las posibles arquitecturas que encontramos en las VPN se pueden mencionar las siguientes:

- *Proporcionada por un servidor de Internet*: El proveedor de Internet puede instalar en su oficina un dispositivo que se encargará de la creación del túnel para la organización.

- *Basadas en firewalls*: De la misma forma en que las VPN trabajan en los niveles más bajos del modelo OSI, el firewall actuará de la misma forma.

- *Basadas en Caja Negra*: Básicamente es un dispositivo con software de cifrado. No provee seguridad en la organización pero si en los datos. Para suplir esta carencia se pueden utilizar un firewall en serie o paralelo al dispositivo de VPN.

- *Basadas en Enrutadores*: Puede ser en este caso que el software de cifrado se añada al enrutador ya existente o bien que se utilice una salida exclusiva de otro proveedor.

- *Basadas en acceso remoto*: El cliente tiene software por el cual se conecta al servidor de VPN de la corporación a través de un túnel cifrado.

- *Basadas en software*: Por lo general se utiliza de un cliente a un servidor de VPN que está instalado en alguna estación de trabajo. Es necesario tener procesos de administración de claves y un emisor de certificados.

3.3 Protocolos

Algunos de las tecnologías y protocolos usados para habilitar las VPNs sitio-a-sitio incluyen **IPSec**, **GRE** (Generic *Routing Encapsulating*), **L2TPv3** (Layer *Two Tunneling Protocol version 3*), **Draft Martini pseudowires** (circuitos emulados), **IEEE 802.1Q tunneling** (*Q-en-Q*) y **MPLS** (Multiple *Label Switched Paths*). A continuación se describen estos protocolos y tecnologías:

IPSec: consiste en un conjunto de protocolos diseñados para proteger el tráfico del IP entre puertas de enlace seguras. Mientras este transita entre redes intermedias.

GRE: puede ser usado para construir túneles y transportar tráfico multiprotocolo entre dispositivos CE en una VPN. *GRE* tiene una pequeña o ninguna seguridad, pero los túneles GRE pueden ser protegidos usando IPSec.

Draft Martini (cualquier transporte sobre **MPLS** [**AToM**]): el trasporte de datos tipo Draft Martini habilita un trasporte de datos del tipo punto-a-punto de protocolos del tipo Frame Relay, ATM, Ethernet , Ethernet VLAN (802.1 Q), HDLC (High-Level Data Link Control) y tráfico PPP sobre MPLS.

L2TPv3: permite el transporte punto-a-punto de protocolos tales como Frame Relay, ATM, Ethernet, Ethernet VLAN, HDLC, y tráfico PPP sobre IP.

MPLS LSPs: Una LSP es una ruta a través de una **LSR** (*Label Switch Routers*) en una red MPLS. Los paquetes son entregados en base a etiquetas agregadas al paquete. LSP puede ser señalizado usando **TDP** (*Tag Distribution Protocol*), **LDP** (*Label Distribution Protocol*), o **RSVP** (*Resource Reservation Protocol*).

También se requieren otros protocolos y tecnologías para permitir el acceso remoto, tales como:

L2F (*Layer Two Forwarding*) : L2F es un protocolo propietario de Cisco que fue diseñado para permitir encapsulamiento de tramas **PPP** (o **SLIP** [*Serial Line Interface Protocol*]) entre un sistema ***NAS*** y un dispositivo de puerta de enlace VPN ubicado en un sitio central. Los usuarios de acceso remoto conectados a un sistema ***NAS***, y las tramas PPP de los usuarios de acceso remoto son entonces encapsulados sobre la red hacia la puerta de enlace VPN de origen y destino.

PPTP (*Point-to-Point Tunneling Protocol*): PPTP es un protocolo que fue desarrollado por un grupo de empresas, incluyendo Microsoft, 3Com, y Ascend Communications. Como *L2F*, *PPTP* permite el encapsulamiento de tramas PPP de clientes de acceso remoto entre sistemas ***NAS*** y una ***VPN*** *gateway*. Los paquetes encapsulados PPP llevados sobre túneles PPTP son usualmente protegidos usando ***MPPE*** (*Microsoft Point-to-Point Encryption*).

L2TPv2/L2TPv3 (*Layer 2 Tunneling Protocol versions 2 and 3*): L2TP es una norma de la **IETF** (*Internet Engineering Task Force*) que combina las mejores cualidades de *L2F* y *PPTP*. En un ambiente de acceso remoto, *L2TP* permite tanto encapsulamiento de las tramas PPP de los clientes de acceso remoto a través de sistemas ***NAS*** a una puerta de enlace *VPN* como encapsulamiento de tramas *PPP* directamente desde el cliente de acceso remoto al concentrador/puerta de enlace *VPN*. *L2TP* tiene una seguridad intrínseca limitada por lo cual los túneles *L2TP* son usualmente protegidos con IPSec.

IPSec: Así como se habilitan VPNs sitio-a-sitio, IPSec también puede ser usado para asegurar tráfico de datos a través de túneles entre usuarios tanto de acceso remoto como usuarios móviles y un concentrador o puerta de enlace VPN.

SSL (*Secure Sockets Layer*): es un protocolo de seguridad que originalmente fue desarrollado por *Netscape Communications* (SSL versiones 1, 2, y 3), y provee de acceso remoto seguro para usuarios móviles y usuarios. Puede estar limitado funcionalmente (comparado con *L2F, PPTP, L2TPv2,* o *IPSec*) si son desplegadas VPNs *clientless* con SSL de acceso remoto.

TLS (*Transport Layer Security*), que es un estándar IETF muy similar a *SSLv3*.

Una ventaja es que no se requiere ningún tipo de software adicional porque SSL es incluido en cualquier navegador Web.

3.4 Requerimientos

Una VPN es una versión modificada de una red privada que permite incrementar la tradicional red de área local o la configuración de la Intranet a lo largo de la Internet y otras redes públicas. Para comunicarse de una manera económica y segura.

Como resultado, muchos de los requerimientos de una VPN y las redes privadas tradicionales son esencialmente los mismos. Los siguientes son requerimientos específicos de las VPNs:

- Seguridad
- Disponibilidad
- Calidad de Servicio
- Confiabilidad
- Compatibilidad
- Manejabilidad

A) Seguridad

Las redes privadas y las Intranets ofrecen un entorno altamente seguro porque los recursos de la red no están accesibles al público en general. Por lo tanto, la probabilidad de accesos desautorizados a sus recursos es altamente improbable. Pero esta certeza no es totalmente cierta para las VPNs, ya que estas hacen uso de los recursos públicos de la Internet y de las redes compartidas. Por lo tanto la seguridad en las VPNs no deberá tomarse a la ligera y las medidas de protección deberán plantearse muy seriamente.

Los recursos y la información localizados en la red pueden asegurarse de las siguientes maneras mediante:

Implementación de mecanismos de defensa periféricos.- que permitan sólo tráfico autorizado de fuentes confiables al interior de la red y que bloqueen el demás tráfico. *Firewalls* y *NAT's* son ejemplos de mecanismos de defensa que son implementados en los puntos donde una red privada o Intranet es conectada a la red en general. Los *firewalls* no sólo analizan el tráfico entrante, sino también el saliente. Los NAT's impiden revelar la IP real de los recursos localizados dentro de la red. Con el resultado de que los atacantes no pueden focalizar un recurso en específico ni los datos ahí almacenados.

Implementación de autenticación de usuarios y paquetes.- sirve para establecer la identidad del usuario y determinar si él o ella serán autorizados a ingresar a los recursos accesibles de la VPN. El modelo AAA (*Authentication Authorization Accounting*) es un ejemplo de uno de esos sistemas de autenticación de usuarios. Primero se autentica al usuario en la red, después de que el usuario ha sido autenticado exitosamente, el usuario puede acceder sólo a esos recursos que ha sido autorizado a usar. Adicionalmente, una detallada bitácora de actividades de todos los usuarios de la red es mantenida, lo cual permite a los administradores de la red descubrir y seguir los accesos no autorizados.

Implementación de mecanismos de cifrado.- se utiliza para garantizar la autenticidad, integridad y confidencialidad de la información cuando la misma es transmitida a través de las redes no autorizadas. IPSec ha emergido como uno de los más poderosos mecanismos de cifrado de datos. Este no solo cifra la información transmitida usando el encabezado ESP, también permite la autenticación de cada usuario y de cada paquete.

B) Disponibilidad y Confiabilidad

La *disponibilidad* se refiere al tiempo total que el sistema está disponible, en las redes privadas y las Intranets el tiempo de producción es relativamente alto porque toda la infraestructura es particular y está en completo control de la organización. Las VPNs usan redes intermedias como la Internet, por lo que las redes basadas en VPNs son altamente dependientes de las mismas.

Es en este tipo de escenarios que el factor de disponibilidad es altamente dependiente del proveedor de servicio de Internet. Si alguna organización está buscando una alta disponibilidad, tiene que contactar un ISP que ofrezca una infraestructura de intercambio altamente recuperable que incluya:

Poderosas capacidades de enrutamiento.- útiles para realizar el re-enrutamiento de tráfico a través de una ruta alternativa en caso de que la ruta principal falle o esté congestionada. Para garantizar la máxima eficiencia, esta capacidad de enrutamiento deberá soportar opciones para designar rutas preferenciales cuando sean requeridas.

Redundancia en las líneas de acceso, la cuál puede ser utilizada para acomodar el incremento en la demanda de ancho de banda.

Infraestructura redundante completa con recuperación automática,

Ésta infraestructura no solo debe de incluir dispositivos de intercambio como servidores y dispositivos de almacenamiento y de acceso, sino también plantas de engría y sistemas de enfriamiento.

La *confiabilidad* es otro de los requerimientos importantes de las VPNs y está íntimamente ligado al factor de *disponibilidad*. La confianza en las transacciones de las VPNs asegura la entrega de la información en los puntos finales en todas las situaciones. Como casi todas las otras configuraciones de red, la *confiabilidad* en los entornos VPNs puede ser logrado al intercambiar los paquetes de información por distintas rutas, si el dispositivo o vínculo en la ruta pudiera fallar. Este proceso por completo es transparente para el usuario y puede lograrse implementando redundancia en los vínculos así como hardware dedicado.

C) Calidad de servicio

La calidad de servicio (QoS) es la capacidad de la red para responder a situaciones críticas asignando un alto porcentaje del ancho de banda y recursos a las aplicaciones sensibles a los retrasos y de misión crítica. Las aplicaciones, tales como transacciones financieras y procesamiento de peticiones, son más importantes desde el punto de vista financiero que las actividades del usuario que incluyen el navegar por la red. Similarmente, aplicaciones tales como las videoconferencias son extremadamente sensibles a los retardos y requieren el suficiente ancho de banda para evitar la pobre calidad en la transmisión y la desincronía.

La calidad de servicio está comprometida con dos dimensiones, *latencia* y *rendimiento.* La *latencia* es el retraso en una comunicación saliente y es extremadamente importante para aplicaciones de audio y vídeo. El rendimiento (*throughput*) se refiere a la disponibilidad del apropiado ancho de banda para todas las aplicaciones, especiales de misión crítica y de uso intensivo de ancho de banda.

Dependiendo del nivel de latencia y del rendimiento, la calidad de servicio puede ser definida en alguna de las siguientes tres categorías:

1) *Mejor esfuerzo en calidad de servicio*: este tipo de servicio, en el mejor de los casos, indica la ausencia de calidad de servicio, porque el proveedor de servicios no garantiza la ausencia de latencia y de rendimiento en ningún caso. Es por esto que es el servicio menos costoso y no debe de ser usado para tráfico sensible al retraso o de uso intensivo de conexión.

2) *Calidad de servicio relativa*: esta clase de servicio es capaz de priorizar el tráfico de información. Por esta razón, al menos el rendimiento se garantiza. De cualquier manera, esta garantía no es absoluta y depende de la carga en la red y el porcentaje del tráfico que se necesita priorizar en algún momento dado. Adicionalmente, esta clase de servicio no tiene priorización para minimizar la latencia. Esta clase de servicio es moderadamente costoso para aplicaciones de uso intensivo de ancho de banda.

3) *Calidad de servicio absoluta*: esta clase garantiza ambas propiedades, *latencia* y *rendimiento*. Por lo tanto es el tipo de servicio más costoso y que soporta uso intensivo de ancho de banda y aplicaciones sensibles al retardo.

D) Manejabilidad

El control completo de los recursos de la red y sus operaciones, junto con la administración adecuada, han sido temas muy importantes para todas las organizaciones que tienen redes por todo el mundo. En este escenario la mayoría de las organizaciones están conectadas a sus servicios mundiales por medio de los proveedores de servicios (*ISP's*) como resultado, el control de una Intranet en el punto final no es posible por la presencia de intermediarios.

Con la actual disposición de dispositivos y software de VPNs, ha sido posible eliminar los límites tradicionales en el manejo de recursos y la administración de la red privada así como la parte pública de la VPN en sus puntos finales.

Una organización puede ahora administrar, monitorear, probar y localizar fallas, y mantener su red con el paradigma tradicional. La organización tiene el completo control del acceso a la red, y puede monitorear en tiempo real el estado de la red, ajustar la configuración de la VPN, etcétera.

E) Compatibilidad

Como ya se ha mencionado las VPNs usan las redes públicas como una extensión de la propia infraestructura, y esas redes intermedias pueden estar basadas en IP o en otras tecnologías de redes, tales como FR (*Frame Relay*) y ATM (*Asynchronous Transfer Mode*). Como resultado las VPNs deberían de ser capaces de hacer uso de todos los tipos de protocolos y tecnologías.

Para garantizar la compatibilidad con la infraestructura basada en IP, los siguientes métodos pueden ser integrados a las VPNs:

Uso de puertas de enlace IP:

Las puertas de enlace IP convierten o traducen los protocolos no-IP en IP y viceversa. Estos dispositivos pueden ser dispositivos de red dedicados o pueden ser soluciones basadas en software. Como dispositivos de hardware, las puertas de enlace son implementadas en las orillas de la Intranet de la organización. Como soluciones de software, las puertas de enlace son instaladas en cada servidor y son usadas para convertir de protocolos no-IP a IP.

Uso de túneles:

Los túneles se basan en la técnica de encapsulamiento de paquetes no-IP o IP en paquetes IP para su transmisión a través de la infraestructura IP existente. En el punto final receptor, donde se reciben estos paquetes mandados por el túnel, se remueve el encabezado IP para recuperar la información original, que en la terminología de los túneles se refiere como la carga útil (*payload*).

En la imagen 1 se esquematiza la forma en que las redes privadas virtuales hacen uso de la infraestructura de la Internet, como media de transmisión a través de ella y conservando su característica principal de privacía en los puntos finales respectivos.

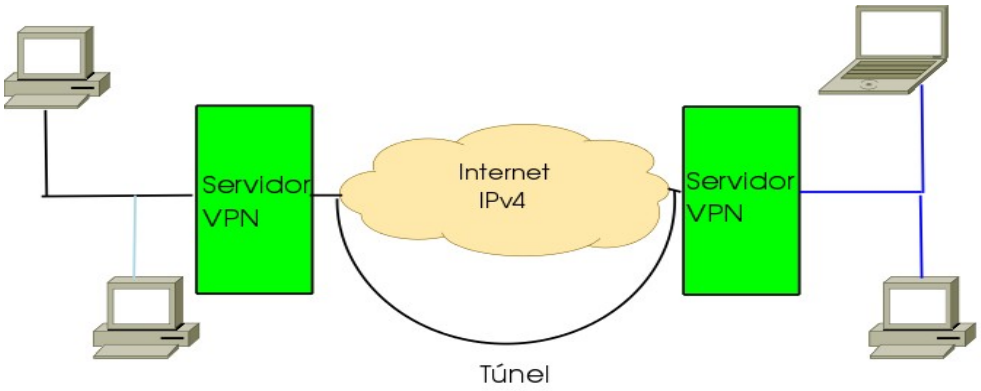

Imagen 1 “Túneles a través de la Internet”.

3.5 Conexiones

La conectividad que las VPNs puedan tener estará en función de qué tipo de políticas de seguridad se implementen y las respectivas herramientas que se utilicen para lograrlo. Será importante tomar en cuenta las ventajas y desventajas que cada opción pueda ofrecernos a fin de poder elegir aquella de acuerdo a nuestros requerimientos.

3.6 Seguridad en las VPN

Una VPN sin seguridad deja de ser privada, la cual es uno de los principales objetivos de las mismas. La seguridad en las TIs y en las VPNs se describe con tres aspectos:

1. *Privacidad (Confidencialidad):* los datos transmitidos sólo deberán estar disponibles para el receptor autorizado.

2. *Confiabilidad (Integridad)*: la información transmitida no deberá cambiar entre el receptor y el emisor.

3. *Disponibilidad*: la información trasferida deberá estar disponible cuando sea necesaria.

Todas estas metas deberán lograrse usando software confiable, hardware, IPS's y políticas de seguridad.

Una política de seguridad define las responsabilidades, procedimientos estandarizados, y los controles de daños además de los escenarios de recuperación que se prepararán para la peor situación posible.

Entendiendo que el daño máximo posible y el costo de la recuperación de la peor catástrofe posible pueden dar una idea de cuánto esfuerzo deberá gastarse en la seguridad.

La seguridad en las VPNs se logrará protegiendo el tráfico con modernos y fuertes métodos de cifrado, técnicas de autenticación segura y *firewalls* controlando el tráfico que se genera desde y hacia el túnel. Cifrar el tráfico no es suficiente, hay grandes diferencias en seguridad dependiendo del método que se implemente.

3.7 Criptografía

Usualmente se solía usar el cifrado de palabras claves o llaves como medio para garantizar el medio o cifrar datos. Si ambos lados usaban la misma llave para cifrar y descifrar la información se llama ***cifrado simétrico***. La llave de cifrado tiene que ser puesta en todas las máquinas que van a ser parte de la conexión VPN.

En el caso del cifrado simétrico y las llaves pre-establecidas, estas son estáticas por lo tanto pueden ser descifradas o adivinadas por ataques de fuerza bruta. Es sólo cuestión de tiempo para un atacante obtener la llave y leer, o en el peor de los casos escribir y destruir la información del sistema.

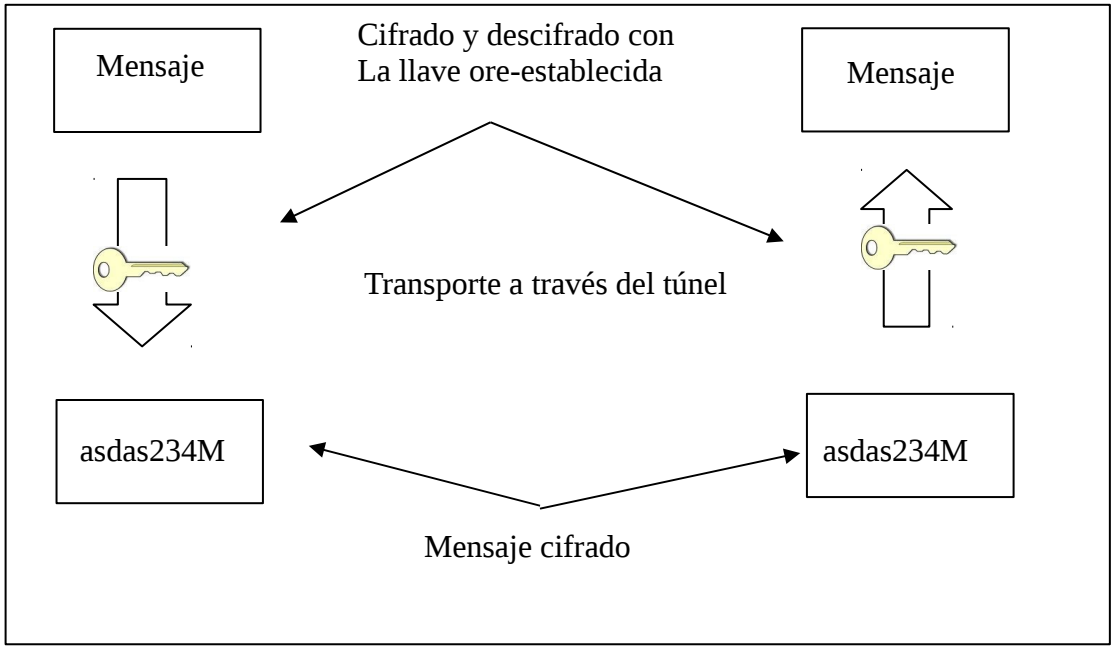

Imagen 2 “Gráfico del mecanismo de intercambio de llaves”.

En la imagen 2, esquematizamos un intercambio de llaves que se utilizan para conocer o sellar el contenido de un mensaje enviado/recibido para el caso del cifrado simétrico.
Así, protocolos como IPSec cambian las llaves en ciertos intervalos de tiempo, según se hayan configurado. Cada llave es válida sólo para cierto *periodo de tiempo*, llamado *tiempo de vida de la llave*. Una buena combinación del periodo de tiempo de la llave y la longitud de la misma, garantizarán que el atacante no pueda obtenerla cuando esta es aún válida.

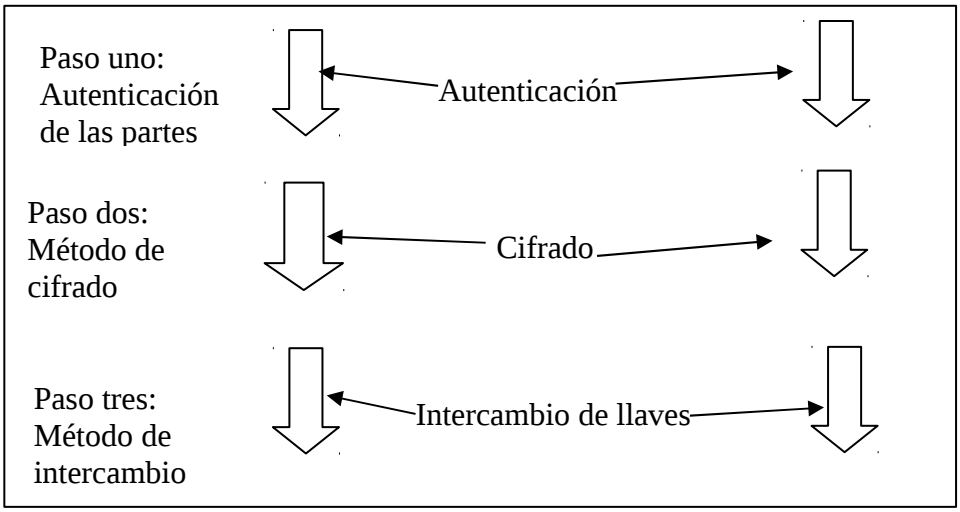

Imagen 3 “Pasos a seguir en un proceso de autenticación”.

En la imagen 3 vemos los pasos que se llevan a cabo durante la autenticación en un intercambio de cifrado simétrico.

3.8 Certificados y autenticación

Existen otros métodos para asegurar las comunicaciones entre los puntos involucrados, como es el uso de SSL/TSL. Estas capas usan el cifrado asimétrico, el cuál funciona de manera distinta que el cifrado simétrico. Para este caso, ambos puntos de comunicación tienen dos llaves cada uno: una pública y otra privada. La llave pública es la que se maneja sobre las comunicaciones, con la cual se cifra la información. Y sólo aquel que posea el otro par de las llaves, en este caso la llave privada, podrá descifrar los datos.

La autenticación de usuarios es un mecanismo implementado en las VPNs en el punto de acceso de las mismas, el cual es usado para garantizar que solo las personas que se autentican pueden acceder a la red y a sus recursos. Los esquemas que se pueden implementar individualmente o en combinación con otros incluyen los siguientes.

Identificación de usuario y clave de acceso (Login ID y password): este esquema usa la autenticación basada en la identificación del usuario y la clave de acceso basada en el sistema para verificar la identidad del usuario que accede al nodo VPN.

Clave de acceso secreta: en este esquema el usuario inicia la clave secreta seleccionando una palabra clave secreta y un número entero, n. Este número entero denota el número de veces que una función hash (actualmente MD4) será aplicada a la clave misma. El resultado es almacenado en el servidor correspondiente. Cuando los usuarios intenten acceder al sistema, el servidor llevará a cabo el procedimiento de autenticación. El software que el usuario usa para intentar la conexión solicitará la palabra clave, aplicará n-1 iteraciones de la función hash a la palabra clave, y se la enviará al servidor.

El servidor aplicará la función hash a esta respuesta, si el resultado obtenido es el mismo que el valor almacenado anteriormente, la autenticación fue exitosa. El usuario es entonces autorizado a ingresar al sistema.

RADIUS:

Es un protocolo de seguridad de Internet que está fuertemente basado en el modelo cliente/servidor, donde la máquina que ingresa a la red es el cliente y el servidor RADIUS, en el punto de acceso, autentica al cliente. Generalmente los servidores RADIUS autentican al usuario usando una lista de nombres de usuario y claves de acceso que mantienen internamente. RADIUS puede también actuar como un cliente para autenticar usuarios de los sistemas operativos, tales como UNIX, NT y NetWare. Adicionalmente, los servidores RADIUS pueden actuar como clientes para otros servidores RADIUS. Para asegurar aún más la información durante las transacciones entre los clientes y los servidores RADIUS esta puede ser cifrada usando mecanismos de autenticación, tales como el protocolo de autenticación de claves (*Password Authenticaction Protocol PAP*) y el protocolo de autenticación por aviso mutuo (*CHAP Challenge Handshake Authentication Protocol*)

Como este nombre lo sugiere, el esquema implementa la autenticación dual para verificar las credenciales del usuario. Combina el uso de un *token* y de una clave de acceso. Durante el proceso de autenticación, un dispositivo electrónico sirve como *token* y como identificador único, tales como el número personal de identificación (*PIN Personal Identification Number*) que es usado como la clave de acceso.

Control de acceso:

Después de que los usuarios se han autenticado exitosamente, estos ganan acceso a los recursos permitidos, servicios de red y aplicaciones localizadas en la misma. Esto puede ser un problema de seguridad porque el usuario, incluso el que ya esta autenticado, puede encontrarse con la información almacenada en varios dispositivos, sabiéndolo o no.

Los permisos de control de accesos son una parte integral del propio control. Los problemas de seguridad pueden ser manejados otorgando privilegios limitados a los usuarios. Por ejemplo, la información puede ser salvaguardada permitiendo a los usuarios no privilegiados sólo permisos de lectura de cierta información. Sólo los usuarios autorizados y el administrador deben de tener los privilegios para escribir, modificar o borrar información.

El control de accesos está basado en la identificación del usuario. Aunque otros parámetros, tales como la dirección IP de origen y la de destino, los puertos, y grupos, juegan un papel importante en el esquema tradicional de control de accesos.

Los mecanismos modernos y avanzados de control de accesos se basan en otros parámetros tales como el tiempo, día, aplicaciones, servicios, métodos de autenticación, URLs, y mecanismos de cifrado.

Cifrando Información

El cifrado de información o la criptografía es uno de los componentes más importantes de la seguridad de las VPNs y juega un papel primordial en la seguridad de la información durante su tránsito por las redes. Es el mecanismo de convertir la información a un formato ilegible, conocido como texto cifrado (*ciphertext*), así los intentos desautorizados de acceder a la información se pueden prevenir mientras la información es transmitida a través de un medio inseguro.

El cifrado de información previene algunas cuestiones como:

- Interceptación de la información y su lectura.
- Modificación de la información y su robo detectable.
- Fabricación de información.
- No-repudio de información.

Certificados Digitales

Un certificado digital es el equivalente electrónico de una identificación y es usado para identificar a una entidad única durante la transmisión. Además de establecer la identidad del dueño, los certificados digitales también eliminan las oportunidades de suplantaciones, reduciendo la oportunidad de la fabricación de información, y adicionalmente previenen efectivamente el rechazo de pertenencia de la información.

Un certificado digital consiste en información que ayuda a validar al emisor e incluye la siguiente información:

- El número de serie del certificado
- La fecha de finalización del certificado
- La firma digital del certificado de autorización (*CA*)
- La llave pública del propietario (*PKI*)

Durante la transacción, el emisor debe de enviar su certificado digital durante la transmisión con un mensaje cifrado para autenticarse a sí mismo. Como en el caso de las llaves públicas, la llave pública CA es ampliamente publicada y disponible a todo el mundo.

Sistema de distribución de certificados (*CDS Certificate Distribution System*)

El sistema de distribución de certificados es un repositorio para los usuarios y las organizaciones, adicionalmente un CDS genera y almacena pares de llaves, firma llaves públicas después de validarlas y almacena y remueve las llaves perdidas y caducas.

3.9 Aplicaciones específicas

El hardware VPN es básicamente para servidores VPN, clientes VPN y otros dispositivos de hardware, tales como enrutadores VPN y concentradores.

a) Servidores VPN

Generalmente, los servidores VPN son hardware dedicado corriendo software de servidores. Dependiendo de los requerimientos de la organización, puede haber uno o más servidores VPN. Como los servidores VPN deben de proveer servicio a los clientes remotos y locales, estos están siempre operativos y listos para las peticiones.

Las principales funciones de los servidores VPN incluyen las siguientes:

• Escuchar peticiones de conexión VPN.

• Negociar parámetros y requerimientos de conexión, tales como los mecanismos de cifrado y autenticación.

• Autenticación y autorización de clientes VPN.

• Aceptar información del cliente o la petición de reenvío de información del cliente.

• Actuar como el punto final del túnel VPN y la conexión. El otro punto de conexión se provee por las peticiones del usuario a la conexión VPN.

Los servidores VPN deben de poder soportar dos o más tarjetas de red (*NIC*). Una o más son usadas para conectarse con las organizaciones en la Intranet, mientras que las demás son usadas para conectarse a la Internet.

b) Clientes VPN

Los clientes VPN son máquinas locales o remotas que inicializan la conexión VPN a un servidor VPN y se introducen a la red remota después de haberse autenticado en el extremo de la misma. Después de un acceso exitoso pueden comunicarse mutuamente el servidor VPN y el cliente. Generalmente un cliente VPN es basado en software.

Aunque también puede ser un dispositivo de hardware dedicado. Un enrutador VPN basado en hardware con capacidades de conexión en demanda que se comunica con otro dispositivo VPN es un ejemplo de hardware dedicado. Con el incremento de una plantilla de trabajo móvil, muchos usuarios (clientes VPN) pueden tener perfiles de *roaming*. Estos usuarios pudieran haber usado una VPN para comunicarse con la Intranet del corporativo como por ejemplo:

•Usuarios móviles con laptops, palmtops, y notebooks los cuales usan redes públicas para conectarse con la Intranet de la organización accediendo a los correos y otros recursos de la Intranet.

• Administradores remotos los cuales usan las redes intermedias, tales como la Internet, para conectarse a una red remota para administrar, monitorear, diagnosticar, o configurar servicios y dispositivos.

c) Enrutadores VPN, Concentradores, y gateways

En el caso de la configuración de una VPN pequeña, el servidor VPN puede tomar una ruta para conectarse. Generalmente, un enrutador es el último extremo de una red privada a menos que esté detrás de un firewall. El papel de un enrutador VPN es hacer accesible las partes remotas de una Intranet. Por lo cual, los enrutadores son responsables de hallar posibles rutas hacia la red de destino y de escoger la ruta más corta del conjunto de rutas, como en el caso de las redes tradicionales.

Aunque los enrutadores tradicionales pueden ser usados en las VPNs, los expertos recomiendan usar enrutadores especialmente optimizados para las VPNs. Estos enrutadores, adicionalmente al enrutamiento, proveen seguridad, escalabilidad, y calidad de servicio (*QoS*) en la forma de redundancia en las rutas.

3.10 Administración

Para mantener a una VPN en óptimo estado de trabajo y con un rendimiento adecuado, deberán cuidarse algunos aspectos importantes. Debe recordarse que el desempeño de una VPN depende en gran medida del desempeño de los servidores VPN y de la infraestructura que se utilice. Se deberá revisar el desempeño de los servidores cuando menos una vez a la semana, para evitar cualquier imprevisto que baje el desempeño.

Es recomendable tener bitácoras detalladas de cada actividad relacionada con la VPN. Adicionalmente se deberán transferir dichas bitácoras a otra máquina para que en caso de que un intruso gane acceso este no pueda alterarlas.

Finalmente se deberá monitorear el desempeño de la red en general. Esto ayudará a identificar potenciales cuellos de botella y a identificar cuantos usuarios puede soportar su configuración de VPN antes de que los usuarios noten una degradación del rendimiento de la misma.

Los esquemas de cifrado, autenticación y de algoritmos pueden generar un considerable consumo de rendimiento, y se puede incrementar el propio de la red al analizar cuidadosamente las opciones a favor y en contra de los esquemas a utilizar, balanceando seguridad y rendimiento.

Los clientes son otro aspecto negativo de las VPNs. Será necesario controlar los clientes locales que estén en la intranet y avisar a los clientes remotos con perfiles de transferencia, de qué software para cliente VPN y qué sistema operativo usar para no afectar las transacciones a realizar.

3.11 Direccionamiento y enrutamiento

Otros puntos importantes en el diseño e implementación de las VPNs son el direccionamiento y el enrutamiento, esto es garantizar que las direcciones IP que se necesiten asignar a dispositivos VPN están bien planeadas y correctamente asignadas. -
También es necesario asegurarse que el esquema de enrutamiento no sólo tendrá conectividad IP con la dirección asignada, sino que será capaz de adaptarse a cambios en el esquema de direccionamiento futuro. Además deberán ser tomadas las medidas adecuadas para garantizar que colegas de negocios externos y clientes remotos son capaces de conectarse a la VPN sin problemas. Algunos de los temas comunes son:

1. Si se usan líneas dedicadas para conectarse a un ISP, en los dispositivos VPN deberían tenerse direcciones estáticas. Pero del otro lado, si usa una conexión telefónica para conectarse a un proveedor de conexión, deberían usarse direcciones dinámicas, especialmente clientes que usen dispositivos móviles o viejos teleconmutadores. El problema de usar direcciones dinámicas es que se generan problemas de seguridad, ya que un atacante puede pasar por un usuario plenamente autorizado.

No importa si usa un servidor VPN o múltiples servidores, *todos* deberán tener direcciones IP estáticas. Si se usan direcciones dinámicas con los servidores, los clientes no podrán localizar el servidor incluso localmente.

Las colisiones de direcciones IP saltarán a la vista si se intenta mezclar dos redes privadas, como en el caso de la fusión de dos entidades. Cambiar el esquema de direccionamiento consume mucho tiempo generalmente en su lugar se deberá considerar usar un esquema de direccionamiento dinámico, como el que provee el protocolo de direccionamiento dinámico (a) *DHCP*.

Si no se tienen suficientes direcciones IP globales-únicas, el mejor esquema de aprovechamiento de la red corporativa será usar direcciones privadas en la red interna y usar *NAT* en la red externa para realizar la conexión global. Este esquema le ayudará a garantizar que no ocurrirán conflictos cuando se establezcan conexiones internas con el exterior.

3.12 Ventajas y desventajas

Las VPNs ofrecen muchos beneficios. En la siguiente lista se mencionan algunos de ellos:

- *Reducción de costos de implementación*: las VPNs son considerablemente menos costosas que las soluciones tradicionales, las cuales están basadas en líneas alquiladas, Frame Relay, ATM o ISDN. Esto es porque VPN elimina la necesidad de conexiones a larga distancia, remplazándola con conexiones a un portador (carrier) local o ISP.

- *Reducción de costos por administración y manejo*: al reducir los costos de comunicaciones a larga distancia, las VPNs también bajan los costos de las redes amplias (***WAN***) considerablemente. Además, una organización puede reducir los costos totales de la operación si sus dispositivos de red VPN son manejados por el ISP. La razón para esta afirmación es que la organización no necesitará contratar personal altamente entrenado y calificado para el mantenimiento de la VPN si ella misma la maneja.

- *Incrementa la conexión*: las VPNs emplean la estructura de la Internet para la interconectividad de partes remotas de redes distintas. Así como la Internet es mundialmente accesible, incluso las oficinas más lejanas, los usuarios móviles y los agentes viajeros podrán conectarse a la red interna (*Intranet*) corporativa.

- *Seguridad en las transacciones*: las VPNs usan las tecnologías de túneles para transmitir datos a través de las redes públicas 'inseguras'. Además las VPNs usan medidas de seguridad en extenso, tales como cifrados, autenticación y autorización para garantizar la seguridad, confiabilidad e integridad de los datos transmitidos. Como resultado una VPN ofrece un alto grado de seguridad en las transacciones.

Servicio	De acceso remoto	Punto a punto	Punto– multipunto
Provee protección entre el cliente y el gateway local	No	No disponible	No disponible
Provee protección entre los punto finales de la VPN	Sí	Sí	Sí
Provee protección entre el gateway remoto y el servidor remoto (a través del gateway)	No	No	No disponible
Transparente a los usuarios	Sí	No	No
Transparente a los usuarios del sistema	Sí	No	No
Transparente a los servidores	Sí	Sí	No

Tabla 3. “Comparativa de distintos tipos de VPN y algunas de sus características generales.”

- *Uso eficiente del ancho de banda*: En el caso de las conexiones a Internet basadas en líneas alquiladas, el ancho de banda es desperdiciado enteramente cuando no existe una conexión activa. Por otro lado, las VPNs crean túneles lógicos cuando son requeridas. Como resultado, el ancho de banda es usado únicamente cuando hay una conexión activa. Por lo tanto hay menos oportunidades de un desperdicio del ancho de banda.

- Alta escalabilidad: como las VPNs están basadas en las conexiones a Internet, permiten a la red interna (Intranet) corporativa evolucionar y crecer, cuando y como el negocio cambie, con el mínimo de equipo extra o expansiones. Esto hace de las redes internas, altamente escalables y adaptables para futuros crecimientos, sin poner demasiada tensión en la infraestructura de red de la organización. A pesar de las numerosas ventajas que ofrecen las VPNs, algunas desventajas están asociadas a su uso, lo que ha provocado escepticismo entre los usuarios para su adopción. Las desventajas incluyen algunas de las siguientes:

- *Alta dependencia de la conexión a Internet*: el desempeño de las redes virtuales privadas es altamente dependiente del desempeño de la Internet. En cambio, en las líneas de alquiler garantizan el ancho de banda que está especificado en un contrato entre el ISP y la organización.

• *Ausencia de soporte para protocolos legados*: las VPNs del presente están basadas enteramente en el IP. Sin embargo, muchas organizaciones continúan usando mainframes además de otros dispositivos y protocolos anteriores en sus operaciones diarias. Como resultado, las VPNs son incompatibles con dispositivos y protocolos previos. Este problema puede ser resuelto, ampliamente, con el uso de mecanismos de túneles. Pero empaquetar SNA y otros protocolos no-IP, puede disminuir considerablemente el desempeño de la red entera.

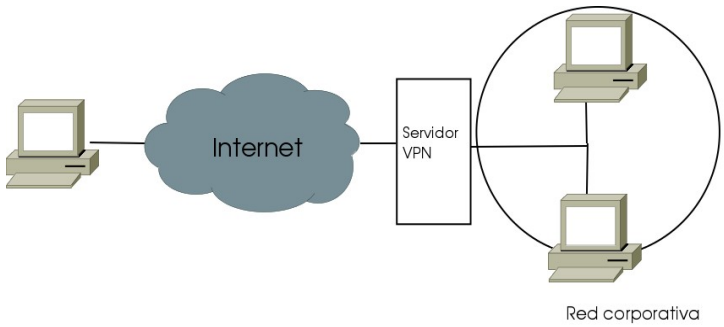

Imagen 4 “Operación de una VPN por un cliente remoto”

La imagen 4 muestra cómo un cliente remoro se conecta al servidor VPN de una red corporativa haciendo uso de la infraestructura de la Internet.