UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERIA EN CIENCIAS APLICADAS

ESCUELA DE INGENIERIA EN SISTEMAS COMPUTACIONALES

Tesis previa la obtención del título de Ingeniero en Sistemas Computacionales

Tema: Metodología para la Implementación de Redes Privadas Virtuales, con Internet como red de enlace.

AUTOR: **Cosme MacArthur Ortega B.**

DIRECTOR DE TESIS: **Ing. Msc. Rodrigo Naranjo**

Ibarra, Enero del 2003

TESIS DE GRADO

Metodología para la Implementación de Redes Privadas Virtuales, con Internet como red de enlace.

CAPITULO I

INTRODUCCIÓN A LAS REDES PRIVADAS VIRTUALES

Una red VPN es una extensión de una red privada que utiliza enlaces a través de redes públicas o compartidas (una red publica y compartida más común es Internet). Con una VPN se puede enviar datos entre dos computadoras a través de redes públicas o compartidas de una manera que emula las propiedades de un enlace punto a punto privado.

Para lograr esta funcionalidad, la tecnología de redes seguras, privadas y virtuales debe completar tres tareas:

- ✓ Deben ser capaces de transportar paquetes IP a través de un túnel en la red pública, de manera que dos segmentos de LAN remotos no parezcan estar separados por una red pública.
- ✓ La solución debe agregar encriptación, de manera que el tráfico que cruce por la red pública no pueda ser espiado, interceptado, leído o modificado.
- ✓ La solución debe ser capaz de autenticar positivamente cualquier extremo del enlace de comunicación de modo que un adversario no pueda acceder a los recursos del sistema.

Para emular un enlace punto a punto, los datos son encapsulados o envueltos, con una cabecera que proporciona la información de enrutamiento que le permite atravesar la red pública o compartida para llegar a su destino. Para emular un enlace privado, los datos enviados son encriptados para tener confidenciabilidad. Los paquetes que son interceptados en la red pública o compartida son indescifrables. El enlace en el cual los datos son encapsulados y encriptados se conoce como una conexión de red privada virtual (VPN).

Se define a una VPN como:

> *Un intercambio de información entre dos puntos de una forma segura a través de una red insegura y pública*

Elementos de una conexión VPN.

La tabla 1 y la figura 1 siguientes muestran los elementos de una conexión VPN.

Elemento	Detalle
Servidor VPN	Administra clientes VPN
Cliente VPN	Cliente Remotos
Túnel	Encapsulamiento de los datos
Conexión VPN	Encriptación de datos
Protocolos de Túnel	Administracíon de túneles
Datos de Túnel	Datos que se transmiten
Red de Tánsito	Red pública de enlace

Tabla 1- Elementos de una conexión VPN

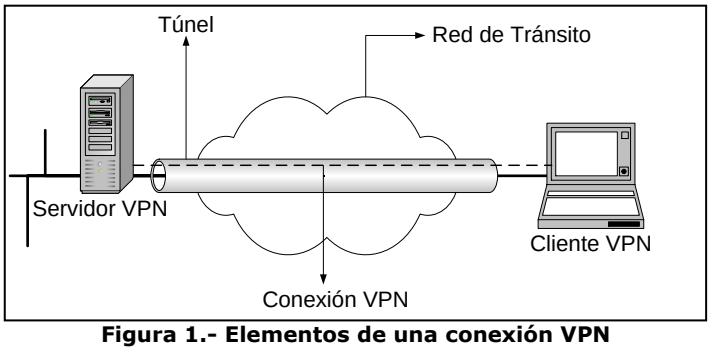

Figura 1.- Elementos de una conexión VPN

Implementaciones comunes de una VPN.

Entre las implementaciones más comunes se tiene 4 maneras claramente identificadas.

TIPO	DETALLE
VPN de Intranet	Creación de conexión entre las oficinas centrales y las oficinas remotas.
VPN de Acceso Remoto	Creación de conexión entre las oficinas centrales y los usuarios móviles remotos.
VPN de Extranet	Creación de conexión entre la empresa y sus socios comerciales.
VPN Interna	Creación de conexión dentro de una LAN

Tabla 2.- Implementaciones comunes de una VPN

Requisitos de una Red Privada Virtual.

Para garantizar que una red privada virtual sea segura, este disponible y sea fácil de mantener es necesario cumplir con ciertos requisitos esenciales que una empresa debe tomar en cuenta antes de implementar una Red Privada Virtual.

Estos requisitos son los siguientes:

- ✓ Disponibilidad
- ✓ Control
- ✓ Compatibilidad
- ✓ Seguridad
- ✓ Interoperabilidad
- ✓ Confiabilidad
- ✓ Autenticación de datos y usuarios
- ✓ Sobrecarga de tráfico
- ✓ Mantenimiento
- ✓ Sin repudio

Beneficios de las Redes Privadas Virtuales.

El simple hecho de hablar de redes privadas virtuales, como se indicó anteriormente, viene a la mente el término de seguridad, así como también el bajo costo que esta tecnología necesita para implementarla y además su facilidad de uso.

En resumen se puede decir que la implementación de una red privada virtual nos hace pensar en tres aspectos fundamentales y beneficiosos para nuestra empresa que son:

- ✓ Seguridad
- ✓ Bajos costos
- ✓ Facilidad de uso

CAPITULO II

PROTOCOLOS TCP/IP

TCP/IP (Transmisión Control Protocol / Internet Protocol) es un grupo de protocolos estándares de la industria diseñados para redes. Se ha convertido en el protocolo más popular debido a que es utilizado por Internet y esta muy extendido en los sistemas operativos.

TCP/IP se ha convertido en el conjunto de protocolos de red disponible más adaptable por el medio del cual se puede trabajar casi en cualquier medio de Red, Hardware y Sistema Operativo existente, desde una pequeña LAN de grupo de trabajo, hasta la conexión de millones de sistemas que componen la propia Internet.

Arquitectura de TCP/IP.

Los protocolos TCP/IP mapean un modelo conceptual de cuatro capas conocido como el modelo DARPA, denominado así por la agencia del gobierno de los Estados Unidos que inicialmente desarrolló TCP/IP. Las cuatro capas en el modelo DARPA corresponden a una o más capas del modelo de siete capas de Interconexiones de Sistemas Abiertos (Open Systems Interconnection, OSI).

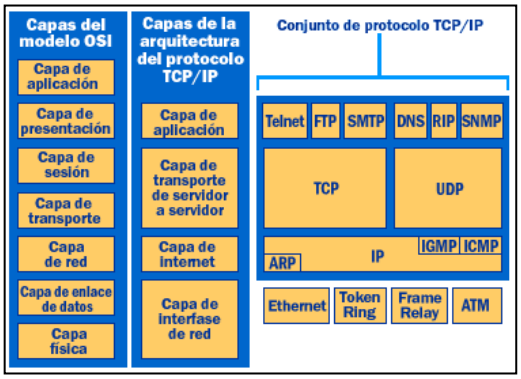

Figura 2.- Relación del modelo TCP/IP con el modelo OSI

Capa de Interfaz de red.- La capa de interfaz de red (también llamada la capa de acceso a la red) es responsable de colocar los paquetes TCP/IP en el medio de la red y de recibir los paquetes TCP/IP del medio de la red.

Capa de Internet.- La capa de Internet es el corazón de cualquier red basada en el protocolo TCP/IP. La capa de Internet en el modelo TCP/IP es análoga a la capa de red en el modelo ISO/OSI.

Capa de Transporte.- La capa de transporte es responsable de proporcionar a la capa de aplicación los servicios de comunicación de sesión y datagrama. Los protocolos base de la capa de transporte son el TCP y el Protocolo de Datagramas de Usuario (User Datagram Protocol, UDP).

Capa de Aplicación.- La capa de aplicación proporciona la habilidad de acceder a los servicios de otras capas y define los protocolos que las aplicaciones utilizan para intercambiar datos. Hay varios protocolos para la capa de aplicación y constantemente se están desarrollando nuevos protocolos.

CAPITULO III

PROTOCOLOS DE TUNEL

Un sistema de túnel, es un método para utilizar una infraestructura de red para transferir datos de una red sobre otra. Los datos que serán transferidos (carga útil) pueden ser tramas (paquetes) de otro protocolo. En lugar de enviar una trama a medida que es producida por el nodo originador, el protocolo de túnel encapsula la trama en un encabezado adicional. El encabezado adicional proporciona información de enrutamiento de tal manera que la carga útil encapsulada pueda viajar a través de la red intermedia.

Protocolos de túnel.

Para que se establezca un túnel el cliente del túnel como el servidor del túnel deberán utilizar el mismo protocolo de túnel.

Protocolo	Detalle
PPTP	Point to Point Tunneling Protocol (Microsoft)
L2F	Layer Two Forwarding (Cisco)
L2TP	Layer Two Tunneling Protocol (Cisco)

Tabla 3.- Protocolos de Túnel

Túneles Voluntarios.- Una computadora de usuario o de cliente puede emitir una solicitud VPN para configurar y crear un túnel voluntario. En este caso, la computadora del usuario es un punto terminal del túnel y actúa como un cliente del túnel.

Túneles Obligatorios.- Un servidor de acceso de marcación capaz de soportar una VPN configura y crea un túnel obligatorio. Con un túnel obligatorio, la computadora del usuario deja de ser un punto terminal del túnel. Otro dispositivo, el servidor de acceso remoto, entre la computadora del usuario y el servidor del túnel, es el punto terminal del túnel y actúa como el cliente del túnel.

CAPITULO IV

ARQUITECTURA DE RED PRIVADA VIRTUAL

Existen innumerables tipos de tecnología para la instalación de una VPN, cada una con su propio lugar y función, y cada uno con sus propias ventajas y desventajas asociadas. En el presente capitulo examinaremos algunas de las distintas arquitecturas de la tecnología VPN, incluyendo las VPN proporcionadas por los proveedores de servicio de red, las VPN basadas en cortafuegos, las VPN basadas en caja negra, las VPN basadas en acceso remoto / enrutador, las VPN consientes de las aplicaciones, las VPN de servicios múltiples y las VPN basadas en software. Con esta muestra de productos el lector podrá apreciar que existe una VPN para cada organización y cualquier infraestructura de red.

A continuación empezaremos a describir cada arquitectura de las VPN más populares:

VPN proporcionada por un Proveedor de Servicios de Red.

Este tipo de servicio son proporcionados por los Proveedores de Servicio de Internet (ISP), el cual se encarga de mantener el túnel entre nuestra organización y el ISP. Correspondería al ISP mantener la VPN funcionando adecuadamente, y para esto el ISP se haría cargo de la instalación y configuración de la VPN, y si así lo requiere el ISP puede instalar un dispositivo en las oficinas de nuestra organización o en su compañía, el cual creará el túnel por nosotros.

VPN basadas en Cortafuegos.

Las VPN basadas en cortafuego son la forma más común de implementación de VPN hoy en día, y muchos proveedores ofrecen este tipo de configuración; esto no significa que sean mejores, sino más bien se trata de una base establecida a partir de la cual crecer.

VPN basadas en Caja Negra.

Se trata de un dispositivo cargado con software de cifrado para crear un túnel de VPN. Algunas cajas negras vienen equipadas con software que se ejecuta en el cliente, para ayudar a administrar el dispositivo, y otras se las puede administrar mediante el explorador de Internet. Por ser un dispositivo de hardware se cree que las VPN instaladas con estos equipos son mucho más rápidas que los tipos basados en software, ya que crean túneles más rápidos bajo demanda y ejecutan el proceso de cifrado mucho más rápido. Aunque esto puede ser verdad, no todos ofrecen una característica de administración centralizada.

VPN basadas en enrutador.

Este tipo de arquitectura es adecuada para organizaciones que ya tiene instaladas una base de enrutadores, y que además soporten VPN. Existen dos tipos de VPN basadas en enrutadores. En uno de ellos el software se añade al enrutador para permitir que el proceso de cifrado ocurra. En el segundo método se inserta una tarjeta externa de otro proveedor en el mismo chasis del enrutador, este método esta diseñado para que la tarjeta insertada realice el proceso de cifrado y liberar de esta tarea al CPU del enrutador.

VPN basadas en acceso remoto.

El acceso remoto significa que alguien de afuera esta tratando de crear un flujo de paquetes cifrados hacia su organización. Este túnel podría venir de Internet, pero también podría venir de una línea de marcación. La figura 4.5 muestra un escenario típico de acceso remoto.

VPN con herramientas proxy.

En la actualidad con las aplicaciones recientes, como la telefonía IP y las tele conferencias, cuando se hace una conexión para una aplicación específica en un puerto determinado, la respuesta que el servidor envía de regreso llega a varios puertos. Así que, ¿cómo se debe configurar la VPN para que se maneje varias conexiones de entrada que se originan desde una solicitud de salida? ¿Qué sucede si se tiene un producto de cortafuego / VPN? ¿Qué puertos se abrirán?.

VPN basadas en software.

Una VPN basada en software básicamente es un programa para establecer túneles o cifrado a otro anfitrión. Por lo general se utiliza desde un cliente a un servidor. Por ejemplo, en una VPN de PPTP,

el software cargado en el cliente se conecta al software cargado en el servidor y establece una sesión de VPN.

CAPITULO V

TOPOLOGIAS DE RED PRIVADA VIRTUAL

En el presente capitulo se tratará de mostrar donde se debe colocar el dispositivo VPN en la topología de su red. Todas las opciones disponibles dan la oportunidad de aprovechar completamente la tecnología VPN. Los dispositivos VPN pueden ser internos, lo que significa que puede dejar que pasen los paquetes cifrados a su red sin necesidad de ser modificados por un enrutador o cortafuegos (Siempre y cuando el permiso este garantizado).

Además se tratará de explicar muchas de las topologías más comunes como por ejemplo: VPN de cortafuego a equipo portátil, VPN de LAN a LAN, topologías anidadas y topologías de túneles son sólo algunas de las configuraciones de topologías que se tratará de analizarlas.

Las topologías son las siguientes:

Topología de cortafuego/VPN a Cliente.

En la actualidad casi todas las organizaciones conectadas a Internet tienen un cortafuego instalado, y todo lo que se necesita es agregar software de VPN al cortafuego. Este tipo de topología es la más común y posiblemente la más fácil de configurar para los que tienen un cortafuego colocado, y sólo desean aumentar la funcionalidad de la VPN.

Topología de VPN/LAN a LAN.

Luego de haber utilizado la topología de Cortafuego/VPN a cliente las organizaciones se han dado cuenta que pueden extender sus VPN para brindar servicios a distintas oficinas remotas. Este tipo de topología es la segunda más comúnmente utilizada; teóricamente, se pueden utilizar tanto un cortafuego basado en Windows NT como uno basado en Unix, pero ambos utilizando un cifrado común, por ejemplo DES, y deberán ser capaces de comunicarse entre sí.

En la figura aparece una organización con una oficina remota, las dos tiene su cortafuego propio, una es una máquina basada en Windows NT y la otra es una máquina basada en Unix. Ambas ejecutan software de VPN de distintos fabricantes y el algoritmo de cifrado utilizado en los productos VPN de los fabricantes es DES.

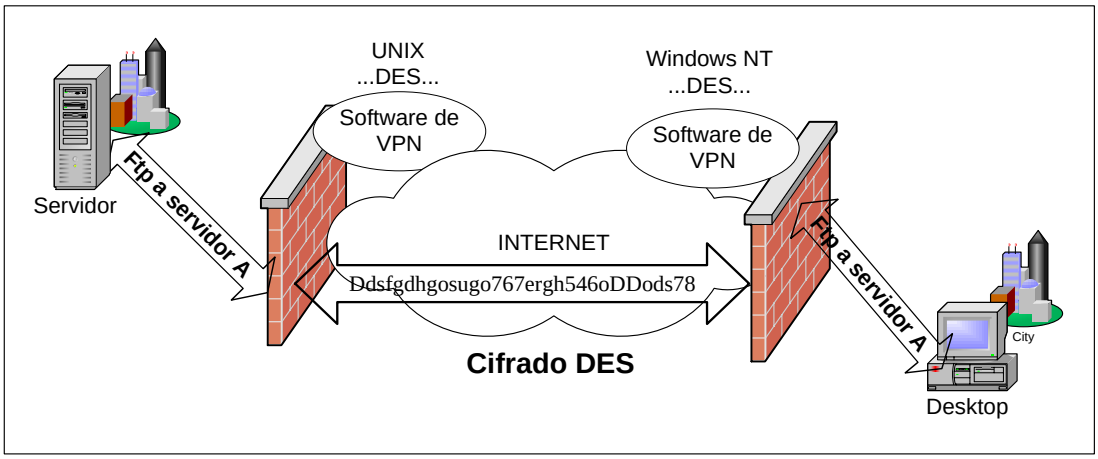

Figura 3.- Topología de VPN de LAN a LAN

Topología de VPN/Cortafuego a Intranet / Extranet.

En la actualidad las Intranet y Extranet son cada vez más populares. Normalmente las Intranet se utilizan internamente por el personal de la organización, y las Extranet se utilizan externamente por los clientes de la compañía.

En la tecnología VPN estos servicios no han cambiado, pero ahora se ha agregado un nivel adicional de seguridad, y se puede tener acceso internamente o externamente a cualquier servicio. Esto tiene dos condiciones. En primer lugar se cuenta con flexibilidad para que una máquina se encargue de la Intranet y Extranet y por lo tanto se reduce la redundancia, y en segundo lugar se debe tener presente la seguridad, ya que existe una forma para que los usuarios externos tengan acceso a estos servidores.

Topología de VPN/Tramas o ATM.

Si hay algo que agradecer a Internet es su flexibilidad casi en cualquier ámbito, y uno de ellos es la de habilitar comunicaciones instantáneas; pero siempre hay que tener en consideración un asunto de mucha importancia como es la seguridad. Es debido a la seguridad que muchas compañías construyen intranets empleando sólo líneas rentadas o enlaces basados en retransmisión de tramas para conectarse a sus sitios.

Por lo tanto las VPN pueden configurarse sobre una infraestructura compartida tal como ATM o topologías de redes basadas en tramas. Loas organizaciones que ejecutan sus propias intranets sobre esta topología de VPN tienen la misma seguridad, facilidad de administración y confiabilidad que en sus propias redes privadas.

Topología de VPN de hardware (Caja Negra).

Las VPN de hardware, o cajas negras, son dispositivos independientes que implementan algoritmos de tecnología VPN.

Algunos soportan normas de cifrado como DES de 40 bits (internacional) y 3DES (Estados Unidos y Canadá).

Topología de VPN/NAT.

Aunque la Traducción de Direcciones de Red (NAT) no es una VPN, se debe discutirla ya que muchas organizaciones lo tienen implementado, y los dispositivos VPN se ven afectados directamente por los procesos de NAT. La traducción de direcciones de red es el proceso de cambiar una dirección IP (por lo general la dirección privada de una organización) a una dirección IP pública enrutable. NAT proporciona un mecanismo para ocultar la estructura de la dirección privada de una organización. Utilizar la traducción de direcciones de red no es complicado, pero la ubicación del dispositivo VPN es importante.

Túneles de VPN anidados.

Los túneles de VPN anidados pueden considerarse como un túnel dentro de otro túnel. Existen muchas formas para hacer túneles anidados, una forma de emplearlos es cuando una organización requiere implantar seguridad punto a punto.

CAPITULO VI

SEGURIDADES DE RED PRIVADA VIRTUAL

Los computadores son hoy en día una parte fundamental de la sociedad de la información en la que vivimos, han supuesto una revolución total en la forma de comunicarnos, de llevar a cabo nuestras necesidades básicas diarias, y que sin ellos la vida, tal como la concebimos hoy por hoy, sería imposible.

La seguridad general abarca un sinnúmero de aspectos de la organización y este capitulo solo esta enfocado a la seguridad de la información, el cual abarca la seguridad de redes, la seguridad de las computadoras, la seguridad de acceso y la seguridad física, entre otras.

Con toda esta seguridad, es la administración superior de la organización quién decide que información es crítica y que información no lo es?. Ya que es aquí donde se decide dar un valor a la información y proporcionar los recursos necesarios para protegerla. Además no todos los datos son confidenciales y no todos los datos comerciales son críticos.

La seguridad informática se ocupa de elaborar las normas y procedimientos que hacen al procesamiento seguro de la información en todos sus aspectos.

La seguridad persigue tres objetivos básicos:

Confidencialidad:

- ✓ Proteger la revelación de información a personas no autorizadas
- ✓ Restringir el acceso a información confidencial
- ✓ Proteger el sistema contra usuarios curiosos internos y externos

Integridad:

- ✓ Proteger los datos de cambios no autorizados
- ✓ Restringir la manipulación de datos a programas autorizados
- ✓ Proveer información verídica y consistente

Disponibilidad:

- ✓ Asegurar la continuidad operativa del sistema y proveer planes alternativos de contingencia
- ✓ Proteger el sistema contra acciones o accidentes que detengan los servicios o destruyan la información que brinda

La seguridad informática es asociada siempre con amenazas externas (como hackers o espías), pero la prevención de accidentes de usuarios autorizados (internos) es uno de los principales beneficios de una seguridad bien diseñada.

Ataques a la red privada virtual.

En esta parte se tratará de explicar rápidamente los tipos de ataques a las que pueden estar expuestas las redes privadas virtuales.

- ✓ Ataques a los algoritmos criptográficos.
- ✓ Ataques al generador de números aleatorios.
- ✓ Ataques a la recuperación de claves.
- ✓ Ataques al Protocolo de Seguridad de Internet (IPSec).
- ✓ Ataques al protocolo PPTP.
- ✓ Ataques a la autoridad emisora de certificados.
- ✓ Ataques a radius.
- ✓ Ataques a kerberos.
- ✓ Ataques a pretty good privacy (PGP).
- ✓ Ataques de negación de servicio.
- ✓ Ataques de Autentificación.

Como identificar los ataques.

Una buena política de seguridad tiene auditorias y registros como pasos principales de sus procesos, ya que nunca se sabe de antemano cuando se va ha ser atacado. Es por esta razón que es bueno tener registros de quién ha ingresado o ha intentado introducirse y no tuvo éxito. Cuando se tiene intrusiones extrañas es necesario rastrear la intrusión y ver si los archivos de registro pueden identificar de donde vino el intruso, cuál es su dirección IP, y si es posible quién es su proveedor de Internet.

Importancia de la Seguridad en las VPN.

Para que las Redes Privadas Virtuales puedan ser un medio efectivo para el comercio electrónico, para las aplicaciones de Intranet, Extranet y para las transacciones financieras a través de Internet, deben utilizarse tecnologías de autenticación seguras, las más recientes y sofisticadas, así como criptografía y cifrado en cada extremo del túnel de las Redes Privadas Virtuales. Por los motivos expuestos con anterioridad es importante para cualquier configuración de seguridad lo siguiente.

Requisitos de seguridad en las Redes Privadas Virtuales.

Una red Privada Virtual esta basada en una red tradicional, así que los requisitos de seguridad son los mismos que se utilizan en las redes tradicionales y de algunas técnicas más, propias de la Red Privada Virtual. El mismo hecho de querer instalar una Red Privada Virtual significa que se quiere añadir un nivel más de seguridad a la red que se posee actualmente.

La seguridad de las Redes Privadas Virtuales es de suma importancia para cualquier compañía que realice negocios a través de Internet o de cualquier red pública. Estos requisitos de seguridad incluyen el cifrado, los dispositivos de Red Privada Virtual, la autenticación, el proceso sin rechazos,

el cifrado punto a punto, la administración centralizada de la seguridad y los procedimientos de respaldo restauración. A continuación se revisarán algunos de estos componentes.

- ✓ Criptografía.
- ✓ Certificados Digitales.
- ✓ Autenticación.
- ✓ Sin Repudio.
- ✓ Cifrado Punto a Punto.
- ✓ Administración de seguridad centralizada.
- ✓ Procedimientos de respaldo/restauración.
- ✓ Sistemas Operativos.

CAPITULO 7

Metodología para la implementación de una VPN.

La información es una ventaja crítica para cualquier compañía, y poseer ésta a tiempo y con seguridad es fundamental para el desarrollo de cualquier organización. Además se debe tomar en consideración que la fuerza laboral del futuro será móvil, y una compañía u organización no estarán en capacidad de construir o rentar suficientes líneas a través de todo el mundo para garantizar conexiones seguras. Y es aquí donde toma importancia la implementación de una red privada virtual, ya que como se mencionó en los capítulos anteriores, una red privada virtual utiliza Internet como medio de transmisión de datos, lo que permite un considerable ahorro en términos económicos.

Para obtener una Red Privada Virtual exitosa es necesario tomar en cuenta algunos factores que son de vital importancia los mismos que se convertirán en pasos para el análisis y posterior implementación de una Red Privada Virtual, los mismos que se describen a continuación:

- ✓ Formación de un equipo de trabajo
- ✓ Fijación del Alcance
- ✓ Estudio y Análisis
- ✓ Elección de la Plataforma
- ✓ Propuestas de Soluciones
- ✓ Seguridades
- ✓ Plan de contingencia
- ✓ Costos
- ✓ Implementación
- ✓ Mantenimiento
- ✓ Medición

Cada uno de estos puntos serán detallados a continuación:

Formación de un Equipo Ejecutor

Si se toma en consideración de que una Red Privada Virtual es un conjunto de aplicaciones de software cliente-servidor basados en tecnología Internet para la transmisión y recepción de datos, y que utilizan las plataformas de red local (LAN), redes a nivel mundial (WAN), protocolos TCP/IP y los servidores de su organización para prestar servicios de una red privada, entonces en el momento que se emprende la tarea de poner en marcha una Red Privada Virtual se hace necesario la formación de un Equipo Ejecutor, el cual debe ser conformado por un pequeño grupo de

especialistas y a este agregar un número pequeño de personal con capacidad de decisión y conocimiento de la organización o empresa, de tal manera que se pueda asignar responsabilidades al personal, además que el equipo debe tener una gran capacidad de liderazgo y responsabilidad para asumir el reto de poner en marcha un proyecto de Redes Privadas Virtuales.

Fijación del Alcance

Una vez que se ha tomado la decisión de implementar una Red Privada Virtual es necesario definir argumentos que serán tomados en cuenta para la implementación, y que deberán cumplirse en lo posterior. Temas como los que se describen a continuación deberían ser tomados en consideración:

- ✓ ¿Para qué tener una Red Privada Virtual?
- ✓ ¿Quiénes serán los usuarios?
- ✓ ¿Qué conocimientos, información o datos se van a poner en la Red Privada Virtual?
- ✓ ¿Utilizará la Redes Privadas Virtuales para comercio global?
- ✓ ¿Instalará una extranet?
- ✓ ¿Su organización posee la capacidad técnica adecuada para mantener e instalar una Red Privada Virtual?
- ✓ ¿Cómo se integrará la Red Privada Virtual con la Red de la compañía?
- ✓ ¿Qué respuesta o resultados se desea obtener?
- ✓ ¿Qué tipo de seguridad de utilizara en la red privada virtual?
- ✓ ¿Cómo se construirá?
- ✓ ¿Qué servicios se colocarán primero, cuales después?
- ✓ ¿Su gobierno como considera al cifrado? . Se debe tener en cuenta que algunos gobiernos consideran al cifrado como arma, por lo tanto regula su uso.

Estudio y Análisis

Luego de que se ha completado con la formación del equipo ejecutor, y la fijación del alcance del proyecto, es necesario realizar un estudio y análisis detenido para saber a ciencia cierta que parámetros deben cumplir las Redes Privadas Virtuales que se desea implementar.

Elección de la Plataforma

Para la implementación de una Red Privada Virtual es muy importante la elección de la plataforma en cual se la va ha desarrollar. En el mercado existe una gran variedad de soluciones, por lo que se hace necesario elegir una. También es necesario mencionar que las Redes Privadas Virtuales pueden ser construidas tanto por software, como por hardware o una combinación de éstas. Para realizar la elección de que tipo de Redes Privadas Virtuales instalar es necesario analizar los siguientes puntos:

- ✓ Software existente en la empresa.
- ✓ Aplicaciones existentes en la empresa.
- ✓ Plataforma existente en la empresa.
- ✓ Servicios que posee la plataforma.
- ✓ Seguridades que brinda la plataforma.
- ✓ Soporte técnico que posee la plataforma.
- ✓ Tipo de servidores que posee la empresa.
- ✓ Costo de la plataforma.

Propuestas de Soluciones. (Diseño)

El diseño se lo pone como quinto punto, ya que luego de realizar el análisis se puede realizar el diseño, pero el diseño se ve afectado por la plataforma elegida, con esto se quiere decir que el

diseño se lo debe realizar sólo después de haber realizado el análisis y de haber elegido una plataforma, ya que existen muchas opciones para instalar una red privada virtual.

En la propuesta de soluciones se debe tener en consideración los siguientes aspectos:

- ✓ ¿Que aplicaciones van a pasar por la Red Privada Virtual?
- ✓ ¿Qué tipo de infraestructura de hardware soporta su organización?
- ✓ ¿Cuántos usuarios estima que utilizarán la Red Privada Virtual?
- ✓ ¿El tráfico que pasará por la VPN es pesado?
- ✓ ¿Qué tipo de seguridades se utilizarán en la Red Privada Virtual?

Seguridades.

Cómo la construcción de una Red Privada Virtual se basa en las seguridades, en este punto se debe ser muy exigente para poder disminuir a cero el riesgo de pérdida o daño de información en la Red Privada Virtual, y para esto se hace necesaria la implantación de una política de Seguridad basándose en los siguientes parámetros:

- ✓ Fijación de Objetivos
- ✓ Relación Costos vs Riesgos

Plan de Contingencia.

Cuando se tiene grandes volúmenes de información, y es de vital importancia para la organización el correcto funcionamiento de la red privada virtual, resulta necesario, por no decir imprescindible, el tener un plan de contingencia tanto durante la fase de desarrollo y durante el funcionamiento de la red privada virtual.

Costos.

Puesto que la parte económica juega un papel muy importante en el éxito de una Red Privada Virtual, se considera muy importante analizar los siguientes puntos para determinar los costos de implementar una Red privada virtual.

- ✓ Hardware
- ✓ Software
- ✓ Capacitación
- ✓ Contratación de Servicios

Implementación

Durante la implementación se utilizarán especialmente la fase del análisis y la fase del diseño, es necesario aclarar que antes de empezar con este punto, el personal que va a implementar la red privada virtual ya debe estar lo suficientemente capacitado acerca de esta tecnología para poder finalizar con éxito las Redes Privadas Virtuales.

Mantenimiento

El mantenimiento se centra en el cambio que va asociado a la corrección de errores, a las adaptaciones requeridas a medida que evoluciona el entorno de la red privada virtual, y a cambios debidos a las mejoras producidas por los requisitos cambiantes de la organización.

Medición de Resultados.

Este punto es necesario para poder realizar una evaluación del trabajo realizado en la institución, por tanto la evaluación se realizará en todo momento, se evaluará a partir de la puesta en marcha del proyecto y se podrá medir como se está avanzando en la ejecución, en lo posterior se evaluará la utilización de los servicios y por defecto se estará evaluando la conformidad, la aceptación por parte de los usuarios hacia la nueva implementación.