UNIVERSIDAD NACIONAL PEDRO HENRIQUEZ UREÑA

Facultad de Ciencia y Tecnología
Escuela de Informática

VPN'S: ANÁLISIS DE SU IMPLEMENTACIÓN Y DESEMPEÑO BAJO WINDOWS, EN LA REPÚBLICA DOMINICANA

TRABAJO DE GRADO PRESENTADO POR

THANYA GUZMÁN RINCÓN

PARA LA OBTENCIÓN DEL GRADO DE

LICENCIADA EN INFORMÁTICA

Santo Domingo, D.N.
2003

DEDICATORIA

DEDICATORIA

A Tania:

Por ser tan especial, me has acompañado en este trayecto, estando ahí para mi. Tu gran ayuda ha sido un maravilloso aporte para alcanzar un eslabón más en la escalera de la vida; has formado parte activa en la culminación de mis estudios, tus aportes no tienen precio. Me has acompañado en todo momento importante en mi vida, desde mi nacimiento hasta el sol de hoy. Que Dios te siga iluminando siempre, para que con esa ternura que te caracteriza sigas siendo para mí, una excelente madre y una excelente amiga.

A William:

Mi querido viejito. Te dedico este trabajo de grado por que has sido un padre ejemplar, un gran vencedor de obstáculos, tu ejemplo de lucha y perseverancia me ha demostrado que aún cuando no se puede, tengo todo lo necesario para poder. Me has alentado en cada momento, cuando no tuve ni las fuerzas, ni el deseo para seguir, tu me ayudaste a seguir. Eres tremendo, que Dios Todopoderoso te siga ayudando a ser ese gran ser humano que siempre te ha caracterizado, lleno de valores y bondades.

A mi hermana Esther:

Mi querida Estelita, gracias por todo tu apoyo, gracias a ese apoyo debo una gran parte de este proyecto. Que tu bondad y tu buen ejemplo de lucha y perseverancia, siga caracterizando esa gran persona que hay en ti. Que Dios Todo Poderoso te siga bendiciendo.

A mi hermano Willy:

Has sido un maravilloso hermano, un verdadero ejemplo de servicio y entrega, que tu Dios te lo recompense. Tu ayuda ha sido de gran valor para hoy haber concluido airosamente este proyecto, que no es más que el principio de una vida de constante lucha por la superación, gracias por tu apoyo incondicional.

A mi hermano Edwin:

Tu ejemplo de disciplina, esfuerzo, trabajo tesonero, dedicación y perseverancia han sido impulsadores para que me haya forjado una meta, que hoy por hoy, ya no es un ideal, es un sueño hecho realidad. Tu, siendo el menor te has hecho el mayor, mostrándome tu humildad. Que el Señor Jesús guarde todas tus entradas y tus salidas.

A mi sobrino Wili:

Este logro te lo dedico con todo mi cariño y aprecio, que te sirva de guía e inspiración para tus estudios, y tu trabajo futuro. Eres una gran bendición de Dios, en nuestras vidas. Que Dios te siga bendiciendo y te guíe siempre por buen camino.

AGRADECIMIENTOS

AGRADECIMIENTOS

A Dios:

Mi benefactor, mi proveedor, mi fortaleza y mi escudo, el Dios en quien confío, gracias mi Señor, no sólo por traerme hasta aquí, sino también por acompañarme durante todo el trayecto, por devolverme a la vida, por que tu diestra me ha sostenido. Gracias por ser mi norte, ya que sin ti nada soy, todo te lo debo a ti, y por que hoy sé que: "Todo lo puedo en Cristo que me fortalece". (Filipenses 4:13)

A mis compañeros de Estudios:

A Wendy, Mónica, Carmen, Marlene, Mayra, Dayana, Luis, Arismendy, Franchy, Richard, Handell, Claudia, Fausto, Leo. Gracias por compartir conmigo esos momentitos tan agradables, pero también las penas, las luchas por el simple hecho de que hayamos saltado obstáculos juntos, gracias le doy a Dios por la oportunidad que nos brindó para compartir.

A mi Asesor Ing. Milton Reyes:

Has sido una gran ayuda, y no sólo en la realización de este trabajo de grado, ya que tus enseñanzas han sido clave en mi preparación. Maestros como tu, hacen una gran diferencia en el proceso de aprendizaje de todo estudiante, el alumno que pasa por tus manos no vuelve a ser el mismo jamás.

A mis apreciados Maestros:

Gracias por sus enseñanzas, por compartirme sus conocimientos y por exhortarme a extender mi aprendizaje. Por su vocación, dedicación y entrega. Que Dios les multiplique esa maravillosa labor, con la cual hacen grandes aportes a la sociedad.

A la UNPHU:

Por ser una institución forjadora de vencedores: hombres y mujeres de gran valor. Gracias por la oportunidad de estudiar en esta alta casa de estudio y por los conocimientos y experiencias que he adquirido.

A Paola:

Eres un verdadero ejemplo de "superación", te agradezco en el alma cada vez que has estado ahí para mí, por tu dedicación, tu hermosa amistad, tus palabras de aliento, no tengo palabras para agradecerte lo mucho que has hecho por mi.

A mis hermanos de Comunidad:

A ustedes mis queridos hermanos, que me han acompañado en cada parte de mi proceso, desde nacer de nuevo hasta el sol de hoy. Gracias por estar ahí para mí. Por alentarme a seguir, por enseñarme que dando es como recibimos, y que la fe sin obras es fe muerta. También quiero agradecerles que ustedes sean los instrumentos que ha usado mi gran Dios para darme una nueva vida. De todo corazón, gracias.

A Mariam:

Eres un angelito que el Señor ha puesto en mi camino, gracias por tenderme tu mano siempre que la he necesitado, y también por ser como eres, cómo tu bien dices: "Por fa, no cambies nunca, sólo lo necesario para ser feliz", desde lo más profundo de mi corazón recibe un ciber abrazote.

A Laura:

Mi querida princesa Laly, mi hermanaza del alma, tu apoyo incondicional ha sido vital para poder alcanzar esta meta, gracias por recordarme que: "Se puede!".

A Javier:

Gracias querido Rey XP, por toda tu ayuda, por ser como eres, por alentarme a seguir, por tu bella amistad, gracias.

Ana Luisa:

Gracias por ser como eres, por tu gran ejemplo, por ser un valioso instrumento que Dios usó y continua usando, para hablarme. Por tu gran apoyo, que Dios te lo pague.

A Ivelisse:

Gracias por tu ayuda, por el gran apoyo en la continuidad de mi "superación", especialmente en mis estudios. Que Dios te siga bendiciendo.

ÍNDICE DE CONTENIDO

Capítulo II: TÉCNICAS DE ENCRIPTACIÓN Y AUNTENTICACIÓN

Capítulo III: DISEÑO Y APLICACIONES DE REDES PRIVADAS VIRTUALES (VPN's)

JUSTIFICACIÓN Y MOTIVACIÓN

El potencial de la red en los momentos actuales es todavía ilimitado y muchos buscan aún la manera de explotar sus dos principales ventajas: Universalidad y bajo costo, donde caben perfectamente las redes VPN. Por lo que se hace idóneo conocer los grandes y agigantados avances y el alcance de aplicación, así como otros datos sobre su incidencia y soluciones que ofrece.

Es necesario que todo profesional tenga absoluto dominio de la tecnología VPN, ya que es una de las alternativas más ventajosas para las empresas, con la que se puede disminuir notablemente los costos en empresas que hacen uso de otras tecnologías como ATM y Frame Relay, a la vez que se robustece la seguridad de la información de las empresas.

Tiene gran aplicación en empresas que tienen sucursales en varios puntos del país, con las cuales se necesita mantener una confiable comunicación y es necesario accesar constantemente a determinadas bases de datos.

Es de gran utilidad en personal gerencial de mando, que necesitan tomar decisiones, estando viajando y accediendo a la información actualizada de la empresa.

Para asegurar la privacidad de la conexión de los datos transmitidos entre dos o más ordenadores, se hace un encriptamiento por el Point to Point Protocol (PPP), un protocolo de acceso remoto, y posteriormente son enrutados o encaminados sobre una conexión previa (también remota, LAN o WAN) por un dispositivo PPTP.

Una VPN, es una forma de compartir y transmitir información entre un círculo cerrado de usuarios que están situados en diferentes localizaciones geográficas.

La tecnología VPN ofrece múltiples variedades, que se adecuan a las necesidades de cada persona o empresa, tomando en cuenta que las diferencia entre una y otra están muy marcadas. Estas redes están basadas en estándares abiertos bajo Windows, Unix y Radius.

Las redes VPN ofrecen una seguridad confiable, la que se maneja de acuerdo a los accesos a implementar por los administradores del sistema.

Es necesario, explotar las grandes ventajas que ofrece esta tecnología, ya que las VPN's permiten:

- La administración y ampliación de la red corporativa al mejor costo-beneficio.
- La facilidad y seguridad para los usuarios remotos de conectarse a las redes corporativas.

En el campo de la tecnología de la información la computadora constituye uno de los medios más destacados, hasta el punto de ser identificado como la totalidad de los mismos. La importancia que adquiere desde el punto de vista virtual no requiere grandes justificaciones. En nuestros días y más en el futuro, cualquier individuo se ha de enfrentar a la informática, al menos como usuario de la misma y en cualquier caso y de forma pasiva, sufrirá sus efectos.

Esta tecnología es de gran importancia por el gran potencial que representa ahorrando costos, en un país donde la economía es un punto clave, sin necesidad de sacrificar la calidad, la integridad y la seguridad de la información. Es otro factor motivante, su diversidad de aplicación y que no requiere una gran inversión. Puede configurarse en sistemas operativos tan comunes como son la gama de windows, y para dispositivos móviles, sin mayores inconvenientes.

OBJETIVOS

General

Analizar las pautas básicas sobre la implementación y el desempeño de las Redes Virtuales Privadas (VPN) como una solución que permite extender su alcance de Aplicación, en un sistema operativo muy amigable, como lo es windows, haciendo grandes aportes, que de una u otra forma repercuten en la evolución de la tecnología en la República Dominicana.

Específicos

1. Conocer los aportes de esta tecnología y evaluar su funcionamiento, en la República Dominicana.
2. Comparar beneficios de estas Redes Virtuales Privadas con otras tecnologías .
3. Identificar los beneficios que ofrece a las empresas en el manejo de la información por Internet e Intranet.
4. Mostrar las dificultades y requerimientos de la instalación de una red VPN, en la República Dominicana.
5. Conocer los diferentes tipos de Enlaces de VPN's, con ejemplos de casos nacionales
6. Dominar las configuraciones de VPN's bajo cualquier Sistema Operativo Windows.
7. Conocer herramientas de Seguridad en las VPN's

INTRODUCCIÓN

En esta investigación se abarca la funcionabilidad, desglose de las Redes Privadas Virtuales (VPN's), basándose en la aplicación, desarrollo y evolución de las mismas, enfocando los aportes, costos, requerimientos, configuración, administración, versatilidad y de manera especial las ventajas que éstas ofrecen

En estos tiempos de constantes cambios, donde la tecnología evoluciona a pasos gigantes, se hace necesario que las empresas le saquen el mayor provecho posible a los aportes que hace la tecnología de hoy día.

Estamos viviendo una era que está marcada por los constantes avances de la tecnología, por tanto las empresas se ven obligadas a danzar al ritmo de la tecnología o dejarse sepultar por ésta. Por eso me permito decir que las VPN's son forman parte de la tecnología del futuro a nuestro alcance en el presente.

Una Red Privada Virtual, consiste en 2 computadoras (una de cada "extremo" de la conexión y una ruta o "túnel" que se crea dinámicamente en un red pública o privada.

Las VPN's permiten una comunicación de túnel seguro que puede proceder del ordenador de un usuario remoto, a través de Internet, y va directamente a la red privada de su empresa. Una red VPN permite que los usuarios accedan de forma segura a una red privada a través de la mayoría de tipos de conexión a internet.

ANTECEDENTES DEL TEMA

Las posibilidades de la realidad virtual, antes apenas un sueño, están al alcance de nuestras manos.

En los últimos años el ambiente virtual ha captado la atención de los medios. La idea es insertar al usuario en el mundo imaginario generado por la computadora, por lo que distintas tecnologías lo utilizan para el logro de este efecto, tal es el caso de la Red Virtual Privada (VPN).

Las redes virtuales privadas surgen dentro del marco de desarrollo de la realidad virtual, la cual fue utilizada por primera vez en el año 1982, convirtiéndose en la hija más joven de la informática.

La política industrial es comprendida en el Japón y en los países del Asia-Pacífico (A_P), como el uso de la autoridad y de los recursos del gobierno con el objeto de solucionar problemas de sectores e industrias específicos, a fin de elevar la productividad de los factores de producción. Por ejemplo, acelerar el proceso de industrialización; transformar las ventajas comparativas a las nuevas realidades del mercado y mantenerlas a través del tiempo, proteger las industrias jóvenes, trazar directrices para el desarrollo tecnológico y facilitar la transferencia de tecnología (Villamizar, 1995. p 92).

IMPORTANCIA

Actualmente existen varios tipos de redes de cómputo establecidas por las diferentes plataformas tecnológicas desarrolladas por los fabricantes a nivel mundial, por lo que se hace necesario conocer cada tecnología que surge en el mercado. Como es el caso de las Redes Privadas Virtuales (VPN's) que forman parte de los que es la nueva tecnología del mercado de las telecomunicaciones, en esta era de la información y el conocimiento.

Ya que las VPN's surgen como resultado de la explosión del Internet. Visto todo esto se produce la iniciativa que permite entender, de forma segura y económica, al alcance de aplicaciones y datos por todo el mundo: la implementación de las soluciones de una Red Privada Virtual (VPN) con el fin de asegurar o dar privacidad a ciertas informaciones que viajan a través de la red pública de Internet.

Es de suma importancia conocer que con este tipo de red 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.

PLANTEAMIENTO DEL PROBLEMA

El problema de la presente investigación se formula desde la siguiente consideración básica: "El estudio de Redes Virtuales Privadas, basada en la realidad virtual, como parte de la política científica y tecnológica que se concretiza en los procesos de la sociedad moderna".

Para un tratamiento adecuado el tema a investigar se planteará desde el marco general de la implementación tecnológica de la red en la República Dominicana y su desempeño.

Donde se evaluarán las distintas aplicaciones de las redes VPN, en la República Dominicana, así como los aportes de éstas para disminuir costos.

En tal sentido, la presente investigación deberá responder las siguientes cuestiones:

1. ¿Cuáles han sido los aportes y dificultades que las redes VPN presentan en la actualidad?

2. Principales Ventajas de las Redes VPN's y como se benefician las empresas en territorio nacional que usan está maravillosa tecnología?

3. Factores a tomar en cuenta para la configuración, administración de VPN y la fijación de costos.

4. Impacto que han tenido las redes virtuales en el desarrollo de la tecnología

MARCO TEÓRICO

Una Red Privada Virtual VPN (Virtual Private Network) es una extensión de una red interna o Intranet a través de una red pública como Internet, lo que forma una conexión privada segura, esencialmente por medio de un túnel. Este proceso esta basado en tecnología y protocolos de red comunes y corrientes, por lo que su instalación y configuración es sumamente sencilla.

El desempeño de las redes virtuales privadas VPN estarán en cualquier momento del día, relacionado directamente al tráfico de internet.

Esta tecnología ofrece una seguridad plena a sus usuarios, esta resguarda los datos a través de sus protocolos de seguridad IP Security situada en la capa de red del modelo OSI y utilizando la tunelización para asegurar los datos. Dentro de este tipo de redes la seguridad depende del control de acceso que implementen los administradores sobre sus redes.

Las redes privadas virtuales tienen la característica principal de ofrecer soluciones a gran parte de las necesidades de comunicación, proporcionando a las empresas diversas fórmulas para obtener un ahorro sustancial e inmediato en las conexiones remotas aprovechando las infraestructuras de red y los servicios de los proveedores de acceso a Internet y otros proveedores de servicio de red.

Las redes VPN explota dos grandes ventajas en la sociedad moderna, que fundamentan su gran avance y desarrollo, tanto a nivel personal como empresarial en casi todo el mundo, que son: ***Universalidad y bajo costo.***

Entre las principales aplicaciones del servicio que ofrecen las redes VPN están:

- Interconexión de Redes de Área Local (LAN)
- Acceso a Internet de las sucursales sin tener que enrutarse por la oficina central.
- Videoconferencia
- Redes privadas virtuales de voz sobre IP
- Televigilancia
- Aplicaciones host-terminal
- Aplicaciones cliente-servidor
- Acceso remoto a base de datos
- Construcción de bases de datos distribuidas.

DELIMITACIÓN DEL TEMA

La Aplicación, desempeño e implementación de las VPN's en la República Dominicana. Cómo esta tecnología reduce costos a la vez que proporciona seguridad y confiabilidad en el manejo de las informaciones.

En este trabajo de grado abarcaré los conceptos básicos que todo informático debe dominar con respecto a las VPN's, como configurar una Red VPN bajo los distintos sistemas operativos Windows.

Casos prácticos de empresas en territorio nacional usando esta moderna tecnología en los diferentes enlaces: Enlace Cliente-Red, Red-Red, Enlace Híbrido o compuesto. Incluyendo un caso de una empresa nacional usando esta tecnología combinada con dispositivos móviles (PDA).

Hipótesis

Las Redes Virtuales Privadas (VPN's) es una tecnología con un gran campo de explotación, donde se reducen los costos, se garantiza la seguridad de la data y se optimizan los recursos.

Variable independiente

Comunicación a través de las Redes Virtuales Privadas

Variable dependiente

Desempeño e Implementación bajo Windows en la República Dominicana, para reducir costos, garantizando la seguridad e integridad de la data, optimizando el manejo de los recursos de hardware, software, espacio físico, y los recursos humanos.

METODOLOGÍA

Esta investigación consiste en analizar la aplicación, la implementación y el desempeño que han experimentado las Redes Virtuales Privadas (VPN's) en la República Dominicana, los efectos de éstas en la tecnología, sus aportes reduciendo costos, así como una serie de conclusiones y recomendaciones.

Se hace pertinente, además, conocer los antecedentes o eventos que anteceden a esta nueva tecnología de red, como es la realidad virtual, el acceso remoto y los tipos de redes que utiliza para su operación.

Para el desarrollo e investigación de este tema, me baso en entrevistas y cuestionarios al personal de Telecomunicaciones de empresas que emplean esta tecnología, usando el método deductivo (de lo general a lo particular). Investigaciones, observaciones y consultas en los sites de los principales proveedores de equipos a nivel del caribe: Cisco System, manuales de productos, etc..

Se desarrollará un caso práctico de VPN para ilustrar y demostrar lo aprendido en base a estas investigaciones. En este caso implementaré una VPN, explicando los pasos que doy, y que otras alternativas se pueden utilizar.

En los casos prácticos que procedo a describir, haré un análisis de esos casos, describiendo brevemente la tecnología que es utilizada, para entender el desempeño de las VPN's.

Capítulo I

CONCEPTOS GENERALES DE VPN's

CAPITULO I CONCEPTOS GENERALES DE VPN's

1.1 Evolución de las Redes.

El avance tecnológico experimentado en los campos electrónicos y en la computación en los últimos 50 años, ha permitido el gran incremento en la capacidad y velocidad de los sistemas de comunicación de datos. Razón por lo cual es importante conocer las diversas etapas o evolución de las computadoras así como los distintos mecanismos para su interconexión.

Actualmente existen varios tipos de redes de computadoras establecidas por las diferentes plataformas tecnológicas desarrolladas por los fabricantes a nivel mundial, por lo que se hace necesario conocer cada tecnología que surge en el mercado. Tal es el caso de las Redes Privadas Virtuales (VPN's) que son prácticamente una tecnología nueva en el mercado de las telecomunicaciones.

Las Redes Privadas Virtuales han surgido como resultado de la explosión del Internet. Visto todo esto surge la iniciativa que permite entender, de forma segura y económica, al alcance de aplicaciones y datos por todo el mundo: la implementación de las soluciones de una Red Privada Virtual (VPN) con el fin de asegurar o dar privacidad a ciertas informaciones que viajan a través de la red pública de Internet.

1.2 Definiciones.

Una Red Privada Virtual (Virtual Private Network) es una expresión que se entiende mediante un proceso de encapsulación, y en su caso, de encriptación, de los paquetes de datos a distintos puntos remotos mediante el uso de infraestructuras públicas de transporte. Los paquetes de datos de las VPN's viajan por medio de un "túnel" definido en la red pública.

Con este tipo de red 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.

El enlace en el cual los datos son encapsulados y encriptados se conoce como una conexión de Red Privada Virtual (VPN). La figura No.1 muestra el concepto lógico de una VPN y su equivalente local.

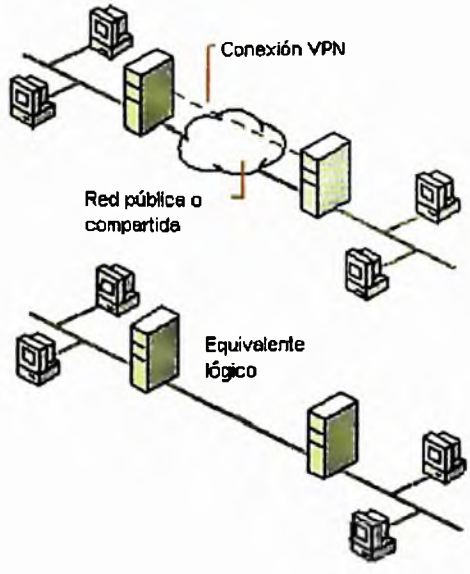


Fig.1 Concepto lógico de una VPN y su equivalente local.

Con las conexiones VPN, los usuarios que trabajan en casa o de manera móvil, pueden tener una conexión de acceso remoto a un servidor de la organización, utilizando la infraestructura proporcionada por una red pública como Internet.

A través de este tipo de red las organizaciones también pueden tener conexiones enruptadas (router connections) con oficinas separadas geográficamente o con otras organizaciones por una red pública como Internet, manteniendo a la vez una comunicación segura. Una conexión VPN enruptada a través del Internet opera desde el punto de vista lógico como un enlace WAN dedicado.

1.3 Elementos de una Conexión VPN.

Una conexión sencilla de Redes Privadas Virtuales incluye los siguientes componentes (ver figura No.2 que muestra los componentes de una VPN):

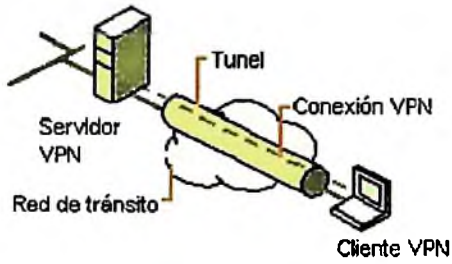


Fig.2. Componentes de una VPN

1) Servidor VPN

Es una computadora que acepta conexiones VPN de clientes VPN. Un servidor VPN puede proporcionar una conexión de acceso remoto VPN o una conexión de una Intranet a otra.

2) Cliente VPN

Una computadora que inicia una conexión VPN con un servidor VPN. Por ejemplo, las computadoras Microsoft Windows NT versión 4.0, Microsoft Windows 95, Microsoft Windows 98, Me, Xp, 200, pueden crear conexiones de acceso remoto VPN a un servidor VPN con Windows NT 4.0. Las computadoras con Windows NT Server 4.0 que ejecutan el servicio de enrutamiento y acceso remoto, pueden crear conexiones VPN de Intranet a Intranet con un servidor VPN con Windows NT 4.0 con RAS.

3) Túnel VPN

Es la porción de la conexión en la cual sus datos son encapsulados.

4) Datos Tunelizados

Son aquellos datos que generalmente son enviados a través de un enlace punto a punto.

5) Conexión VPN

Es la porción de la conexión en la que sus datos son encriptados. Para conexiones VPN's seguras, los datos son encriptados y encapsulados en la misma porción de la conexión.

6) Protocolos de Túnel

Se utilizan para administrar los túneles y encapsular los datos privados (los datos que son enviados por el túnel también deben ser encriptados para que sea una conexión VPN). Windows NT 4.0 incluye el protocolo de túnel PPTP.

7) Red de Tránsito

Es la red pública o compartida que es cruzada por los datos encapsulados. Para Windows NT 4.0, la red de tránsito es siempre una red IP. La red de tránsito puede ser Internet o una Intranet IP privada.

1.4 Tipos de Enlaces en las VPN's.

A) Enlaces Cliente-Red

En estos enlaces se encapsula, típicamente, PPP (Point-to-Point Protocol). Las tramas del cliente se encapsulan en PPP, y el PPP resultante se encapsula para crear la VPN. Se emplea entre, otras cosas, para:

- Acceso seguro de un cliente a la red
- Clientes móviles
- Puntos de acceso remoto.
- Tuteado de tramas no utilizables en Internet, por ejemplo, tramas NetBEUI, IPX, SNA o DECNET.

B) Enlaces Red-Red

En estos casos se está encapsulando el tráfico de una red local, por lo que nos ahorramos el paso PPP anterior. Las tramas de la LAN se encapsulan directamente para crear la VPN. Se utiliza para:

- Fundir dos redes locales a través de Internet, para que parezca una sola.
- Establecer canales con privacidad, autenticidad y control de integridad, entre dos redes independientes.
- Ruteado de tramas no utilizables en Internet.

Existen variedades de redes privadas virtuales que prestan un servicio más amplio a la compañía que busca este acceso. Entre ellas están:

a) Las redes privadas virtuales completamente controladas por el proveedor o "outsource VPN's". Este tipo de VPN controla todo el aspecto de seguridad, interoperabilidad y eficiencia junto con la mayoría de requisitos del usuario. La única excepción sería el "Firewall" que divide la Intranet de Internet controlado por la compañía. Funciona de la siguiente manera: el usuario se conecta al POP (punto de presencia) donde el servidor del proveedor intercepta esta llamada y hace una "búsqueda" a una base de datos que se mantiene en un servidor de seguridad, como RADIUS, TACACS, de la compañía donde todos los parámetros individuales y privilegios de cada persona son almacenados para validar la conexión. El túnel creado es completamente transparente y el tráfico creado es encapsulado y desencapsulado en el POP local.

b) Las VPNs controladas por la misma compañía, o "in-house VPN". Aquí todo lo relacionado con seguridad, verificación y acceso es manejado por los administradores de Internet. El rol del proveedor es solamente ese, proveer la conexión al Internet y garantizar el ancho de banda. Todo el tráfico es encapsulado y desencapsulado en la red privada o Intranet y es también transparente para el usuario.

c) Por último, esta la VPN compuesto o híbrido, "hybrid VPN". Esta, como el nombre lo explica, es una combinación de los dos tipos de VPN's anteriores. El proveedor y la compañía se complementan facilitando acceso para el cliente móvil.

1.5 Características de las VPN's.

Las Redes Privadas Virtuales (VPN's) tienen la característica principal de ofrecer soluciones a gran parte de las necesidades de comunicación, proporcionando a las empresas fórmulas diversas para obtener un ahorro sustancial e inmediato en las conexiones remotas, aprovechando las infraestructuras de red y los servicios de los proveedores de acceso a Internet y otros proveedores de servicios de red. Estas redes representan un sistema rentable, escalable, flexible, gestionable y seguro de controlar el crecimiento de la red, conectar nuevas unidades de negocio y obtener una comunicación instantánea con otros colaboradores de la empresa.

Las VPN's tienen, además otras características, entre las cuales están siguientes:

a) Ahorro en los costos
b) Escalabilidad y cooperación
c) Control absoluto
d) Acceso global a Internet
e) Subcontratación del acceso telefónico
f) Líneas alquiladas virtuales para la conectividad de sucursales.

a) Ahorro en los Costos

Este consiste en la reducción de los costos de comunicación entre puntos distantes, permitiendo a sus usuarios el aprovechamiento de los bajos costos de Internet, sin sacrificar la privacidad y seguridad de sus datos y con unos niveles adecuados y constantes de velocidad y fiabilidad en las comunicaciones.

Se pueden realizar ahorros significativos cambiando a Internet. Analistas indican que el cambiar a una VPN de una red de Frame Relay o de un enlace dedicado, puede reflejar un ahorro de hasta un 65% en cargos para estas comunicaciones. Cuando se involucran conexiones internacionales, los ahorros pueden ser significativamente mayores. Estos ahorros hacen de una VPN, una decisión estratégica de negocios para una corporación.

Internet, por otra parte, basa sus costos en la velocidad de acceso, esto significa que el costo es el mismo si se envía un paquete de Nueva York a Boston, que si lo hace de Nueva York a Tokio. Este hecho es uno de los núcleos de los conductos detrás de la economía de las redes privadas virtuales.

b) Escalabilidad y Cooperación

Las Redes Privadas Virtuales (VPN's) proporcionan escalabilidad con mínimo esfuerzo. Las empresas pueden ampliar la capacidad y el alcance de sus redes con sólo establecer una cuenta con nuevo proveedor de servicios de red o con ampliar su acuerdo con el proveedor ya contratado. Además, instalar funciones de acceso VPN en oficinas remotas es una tarea generalmente sencilla que no requiere la presencia de un especialista en la instalación. Las VPN's permiten, asimismo, enlazar a la red los diversos centros internacionales de una empresa de forma económica y sin la complejidad y retrasos asociados al establecimiento de circuitos Frame Relay entre varios países.

c) Control Absoluto

Las Redes Privadas Virtuales (VPN's) permiten a las empresas aprovechar las instalaciones y capacidades de los proveedores de servicios de conectividad y mantener al mismo tiempo control sobre su red.

Esto permite que las empresas puedan contratar el acceso telefónico y conservar las responsabilidades sobre autenticación del usuario, privilegios de acceso, direccionamiento de red, seguridad y gestión de cambios.

d) Acceso Global a Internet

Las empresas que utilizan Redes Privadas Virtuales (VPN's) para sustituir el acceso mediante líneas dedicadas por el acceso telefónico a Internet, pueden reducir gastos en las facturas de teléfono y en equipamiento.

Las VPN's permiten a los usuarios remotos acceder a la red corporativa efectuando una llamada local a un proveedor de servicios de red. Basta con elegir un proveedor de servicios con presencia global o establecer cuentas con distintos proveedores, y el usuario que se encuentra de viaje podrá conectarse a la red corporativa haciendo una llamada local. El acceso global a Internet puede utilizarse también para proporcionar a los clientes y proveedores de una empresa acceso seguro a los recursos de la Extranet.

e) Subcontratación del Acceso Telefónico

Las compañías que subcontraten servicio remoto a un proveedor de servicios de red, pueden reducir no sólo sus gastos de teléfono (tarifas, llamadas de larga distancia...) y costos de equipamiento, sino también los costos de soporte de usuarios finales, ya que esa responsabilidad se puede trasladar al nuevo proveedor como parte del paquete de servicios de Redes Privadas Virtuales (VPN's).

La ventaja de este servicio para los usuarios y los trabajadores es que no necesitan disponer de un software de red preparado para la tunelización. Sólo tienen que marcar para acceder a los servicios de su proveedor de la forma acostumbrada.

f) Línea Alquiladas Virtuales para la Conectividad de Sucursales

Las empresas que conectan sucursales a través de líneas alquiladas virtuales podrán ahorrar hasta un 65% con respecto al costo de las líneas dedicadas y beneficiarse al mismo tiempo de la posibilidad de conectar nuevas oficinas sin experimentar demoras. Las líneas virtuales alquiladas reducen los gastos de comunicación sustituyendo los enlaces a larga distancia por una conexión con proveedor de servicios de red local.

1.6 Beneficios.

Las Redes Privadas Virtuales (VPN's) ofrecen varios beneficios económicos que permiten el acceso rápido, seguro y constante utilizando infraestructura fuera de la red privada o Internet. En otro tipo de red la corporación tiene que mantener un número indefinido de modems, líneas agregadas de acceso, definidos anchos de banda, números telefónicos de tarifa gratis y altos cargos de larga distancia, que son impuestos cada vez que hay un acceso remoto al Intranet. En cambio, si se utilizan VPN's, el usuario o cliente remoto solamente tendría que llamar a un número telefónico de acceso local, conectando a Internet en la región donde estuviese creando un canal de información dedicado entre este y su respectiva compañía, garantizando desde ese momento, el ahorro prometido por las Redes Privadas Virtuales junto con la seguridad y eficiencia requeridas. Las VPN's son especialmente necesarias si el acceso al Intranet es internacional, cuando puede que no exista una extensión de la red privada que pueda proveer esta clase de acceso.

Mientras las Redes Privadas Virtuales ofrecen ahorro del costo directo sobre otros métodos de comunicaciones (como líneas alquiladas y llamadas de larga distancia), ellas también pueden ofrecer otras ventajas, incluyendo ahorro de costo indirecto como resultado del reducido equipo, al igual que los requisitos de entrenamiento, flexibilidad incrementada y escalabilidad.

Las líneas de Internet alquiladas en las VPN's presentan también la ventaja de que muchos proveedores ofrecen precios que están clasificados de acuerdo a su necesidad y uso.

Las Redes Privadas Virtuales, entre sus múltiples ventajas, ofrecen además:

- Velocidad mejorada
- Seguridad de la información
- Flexibilidad
- Simplicidad
- Estandarización mundial
- Conectividad
- Tiempo de vida útil prolongado, nueva tecnología en desarrollo.
- Bajos costos, efectividad. (Los clientes VPN remotos, no necesariamente tienen que estar en territorio dominicano, este concepto está basado en un diseño mundial usando Internet como medio, esto quiere decir que los clientes pueden estar en el interior o exterior del país, y no significará ningún costo adicional o diferencia. Esta ventaja permitirá acceso a los ejecutivos, empleados y/o funcionarios en los casos que esté fuera o dentro del país, con un mínimo de costos y una excelente velocidad y tiempo de respuesta).

1.7 Desventajas de las Redes Privadas Virtuales (VPN's)

Entre los inconvenientes podemos citar: una mayor carga en el cliente VPN puesto que debe realizar la tarea adicional de encapsular los paquetes de datos una vez más, situación que se agrava cuando además se realiza encriptación de los datos que produce una mayor relentización de la mayoría de conexiones.

También se produce una mayor complejidad en el tráfico de datos que puede producir efectos no deseados al cambiar la numeración asignada al cliente VPN y que puede requerir cambios en las configuraciones de aplicaciones o programas (proxy, servidor de correo, permisos basados en nombre o número IP).

Capítulo II

TÉCNICAS DE ENCRIPTACIÓN Y DE AUTENTICACIÓN

CAPITULO II TÉCNICAS DE ENCRIPTACIÓN Y AUTENTICACIÓN

2.1 Encriptación (Criptología).

Se entiende por ***criptología*** el estudio y práctica de los sistemas de cifrado destinados a ocultar el contenido de mensajes enviados entre dos partes: emisor y receptor.

La ***criptografía*** es la parte de la criptología que estudia como cifrar efectivamente los mensajes. Por ejemplo, el derecho a la privacidad que difícilmente se puede conseguir, si cuando uno se comunica con alguien, no sabemos quién o quiénes fue (fueron) los interlocutores, que realmente pueden estar leyendo el mensaje.

No estamos ante un problema trivial: es de vital importancia para que se desarrolle el comercio seguro en Internet que aunque nuestros mensajes puedan ser interceptados, resulten totalmente ininteligibles, lo que se consigue con la cripotología.

La criptología para asegurar la información utiliza los sistemas de clave:

- Simétrico
- Asimétrico

La tendencia de los ***sistemas de clave simétrica,*** actualmente, es utilizarlo, poco o simplemente para cuestiones que no necesiten un alto grado de protección. Los sistemas de clave asimétrica son los que se están imponiendo, ya que ofrecen un mayor grado de seguridad. Sobre todo porque no hace falta que la clave sea conocida nada más que por una persona. Ya se sabe que cuando un secreto se comparte, hay bastantes posibilidades para que deje de serlo (ver ilustración figura No.3).

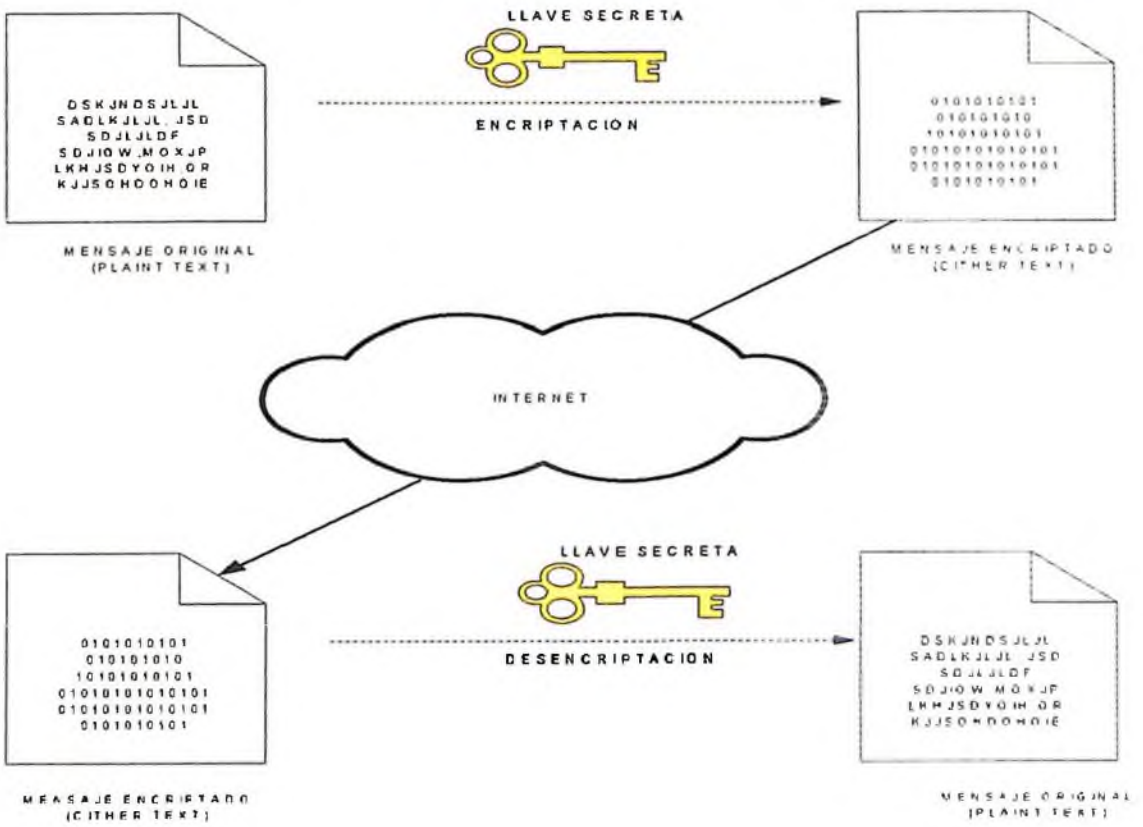


Fig.3 Encriptación Simétrica

Algunos de los problemas que surgen en las conexiones tradicionales, son los siguientes:

- Un usuario accede a unas páginas de una empresa, selecciona un producto para su compra, pero ¿cómo puede tener la seguridad de que esa empresa existe realmente?

- Los datos enviados, tales como el número de la tarjeta de crédito, pueden ser interceptados por terceros. ¿Cómo sabe la empresa que el cliente no negará la compra de los productos? ¿Cómo sabe el usuario que la información ha llegado correctamente y no ha sufrido alteraciones por el camino?

Para solucionar todos estos problemas se han adoptado métodos de encriptación que pueden ser de clave privada o de clave pública. Se podría decir simplemente que en general, el sistema consiste en codificar los datos que se envían para que cualquiera que los intercepte no los pueda entender.

Normalmente se utilizaba el sistema de clave secreta simétrica. En éste el remitente y el destinatario se ponen de acuerdo en una clave y es la que usan para codificar y descodificar la información tal y como se muestra en la *figura No.3.*

El segundo método es el ***sistema de clave asimétrica o pública.*** En este método se necesitan dos claves distintas. Una para encriptar la información y otra para descifrarla. La clave con que se encripta es conocida por todos, y la segunda clave para descifrar el mensaje sólo la conoce el destinatario , la empresa que vende los productos.

Una vez encriptado el mensaje por el usuario, ni siquiera éste tiene la posibilidad de poder leer su contenido. A su vez él tiene su propia clave que usan los demás usuarios para mandarle información y él usa la suya para descifrar los mensajes.

Entre los programas encriptadores de esta segunda clase, el que se está configurando como un standard (por lo menos en cuanto a los usuarios corrientes), y goza de mayor popularidad es el PGP (Pret Good Privacy) el cual es un programa criptográfico que permite a las personas intercambiar mensajes con privacidad y autenticación, fue creado por Phil Zimmermann.

2.1.1 Criptografía Digital.

La aparición de la computadoras y su increíble capacidad de procesamiento, hizo que la criptografía fuera digital. En 1976, IBM desarrolló un sistema criptográfico denominado DES (Data Eneryptice Standard), que luego fue aprobado por la Oficina de Estandarización de los Estados Unidos.

DES (Data Eneryptice Standard) se basa en complicados sistemas matemáticos de sustitución y reposición, los cuales hacen que sea particularmente difícil de romper. Sin embargo, DES depende de que tanto el que envía el mensaje como el que lo recibe conozcan la clave con la cual fue encriptada.

La seguridad de esta llave va a depender de su tamaño. Cuando tenemos un mensaje cifrado hay un número "n" de posibilidades de descubrir la llave con la cual se encriptó. Así, la confiabilidad de una llave depende de que ese número "n" sea tan alto que a un atacante le tome demasiado tiempo probar todas las posibilidades.

Para resolver este problema se creó la criptografía de llave pública. (Ver Figura No. 4) Bajo este sistema existen dos llaves: una privada y otra pública. Cuando A quiere enviar un mensaje a B, le solicita la llave pública (que como su nombre lo indica puede ser conocida por todo el mundo).

En la Figura No. 4, con la llave pública, A encripta el mensaje y lo envía a B, que luego procede a descifrarlo aplicándole su llave privada, que no debe dar a conocer a nadie (ver la figura No.4, donde PC-A y PC-B pertenecen al mismo CA, donde PC-A para identificar la entidad de PC-B simplemente necesita verificar la firma de CA's en el certificado de PC-B. La ventaja de este método es que no requiere que ambas partes conozcan la llave privada del otro.

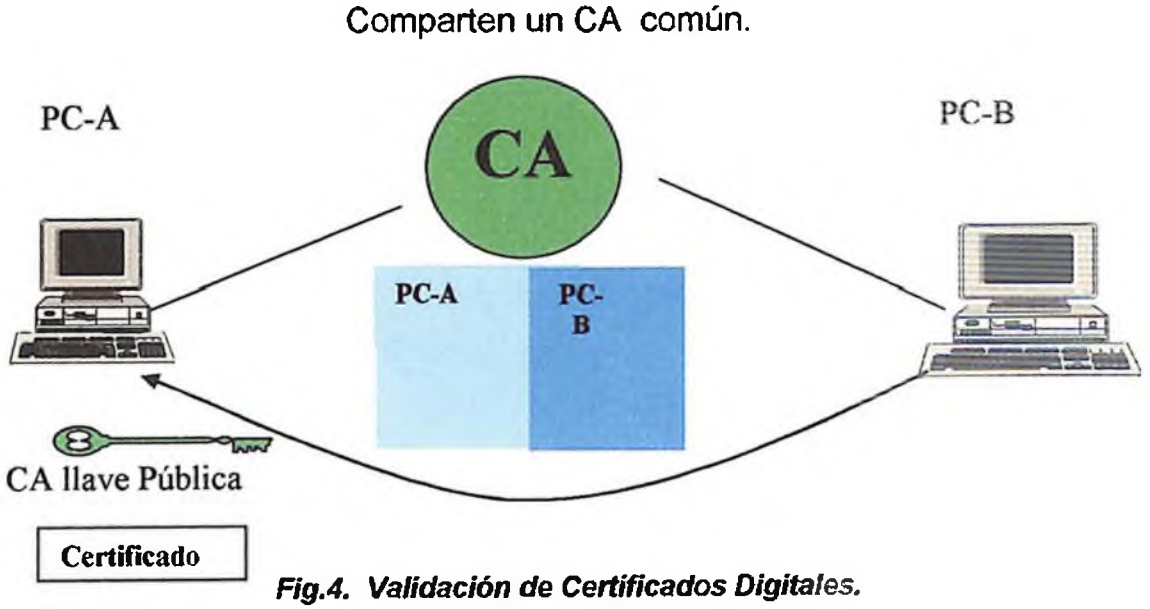


Fig.4. Validación de Certificados Digitales.

2.1.2 Criptografía en Internet.

La criptografía en Internet es de suma importancia, porque básicamente toda la estructura del comercio electrónico dependerá de ella. Como se sabe, Internet nació hace más de veinte años como una red militar y es insegura para transacciones comerciales, por la razón de que "desde sus inicios se decidió que la seguridad de la información que se transmitía no era una prioridad, lo más valioso en ese momento era interconectar computadoras de forma tal que pudiera resistir fallas severas." (Revista Negocios.com, junio/agosto 2001).

El protocolo principal por el cual se transmite la información que viaja por la red (TCP/IP, Transfer Control Protocol/Intenet Protocol) no ha variado en su esencia desde la creación de Internet.

Esta información se divide en paquetes más pequeños a los cuales se llama datagramas. Estos datagramas son enviados por la red sin ningún orden específico. Así, cuando enviamos un mensaje que contenga, por ejemplo, las letras ABCD, éste se dividirá en cuatro datagramas, cada uno con una letra. Estos datagramas viajarán de modo independiente, para luego recomponerse en la computadora de destino, sin que el receptor final pueda saber qué ruta tomó cada uno de ellos. Sin embargo, ninguno de estos datagramas está encriptado y cualquiera que los tome en su recorrido puede leerlos sin problema.

Y aquí es donde entra la criptografía como aliada del comercio en línea. La idea es encontrar un sistema en donde los datos comerciales y financieros puedan viajar de un modo seguro por la red. A ese sistema se le ha llamado SET (Secure Electrónic Transaction).

SET introduce un nivel superior de seguridad mediante el empleo de las denominadas firmas dobles. Una firma de este tipo se genera creando un compendio de ambos mensajes, encadenándolos entre sí, computando el compendio del resultado y cifrando este compendio con la clave privada de la firma original. El firmante debe incluir el compendio del otro mensaje para que el destinatario sea capaz de verificar la firma doble.

Para incrementar aún más la seguridad de estos procedimientos, SET utiliza la Certificate Authority (CA).

SET es un sistema de criptografía basado en el mecanismo de llave pública y en el cual participan las más importantes compañías de tarjetas de crédito a nivel mundial (Visa, Master Card y American Express) y varios colosos de la informática (Microsoft, IBM, Netscape, entre otros.).

SET cubre los tres tipos de principios básicos para asegurar el crecimiento del comercio en línea:

1. Que la información transmitida sea confidencial.
2. Transacciones que se lleven a cabo con total integridad, es decir, sin pérdida de datos.
3. Autentificar a los tarjeta habientes y a los comerciantes.

En el SET participan seis actores, cada uno con sus funciones bien definidas:

- ***El emisor:*** que en este caso es la institución que entrega la llamada tarjeta de crédito electrónica. Suele ser un banco.

- ***El tarjeta habiente:*** es la persona que dispone de la tarjeta electrónica para realizar transacciones.

- ***El comerciante:*** es el que dispone de un sitio Web para realizar ventas en línea.

- ***El pagador:*** es una institución que recibe del comerciante el certificado de pago (voucher) que certifica la transacción entre el comprador y el vendedor.

- ***La cámara de compensación o gateway:*** ésta es una institución que se encarga de procesar el pago al comerciante.

- ***La autoridad certificadora***, que son instituciones encargadas de generar las llaves públicas y privadas de cada uno de los miembros del sistema.

2.2 Autenticación.

La autenticación es la propiedad de conocer que los datos recibidos son los mismos que los datos enviados y que quien dice ser que los envío realmente lo es. En la comunicación de clave pública a un usuario, es necesario garantizar que no haya sido sustituida por la de algún intruso, con lo cual quien parece ser su propietario no lo es.

Un certificado de autenticación es expedido por las CAs (autoridades de Certificación) para mantener la autenticidad de las claves públicas definidas, y es un documento electrónico que lleva los datos de la entidad que quiere hacer pública su clave (lógicamente entre esos datos). Este documento se envía al usuario a quien se quiere comunicar la clave.

El usuario que recibe el certificado comprueba que la firma pertenece a la CA de la que posee la clave y confía en que los datos suministrados por ella en dicho certificado son los correctos, para mayor seguridad el certificado debe ir firmado además por la entidad que quiere dar a conocer su clave.

Las Redes Privadas Virtuales se auxilian de distintos productos para proporcionar seguridad en la transmisión de datos por Internet, como son los protocolos: SSL, IKP y SET.

2.2.1 SSL (Secured Sockets Layer).

Es un protocolo desarrollado por Netscape para proporcionar comunicación cifrada entre un cliente (navegador) y un servidor http. Utiliza de forma conjunta cifrado simétrico y asimétrico. Son capas situadas entre el nivel de aplicación y el conjunto TCP/IP. De esta forma proporciona a la comunicación propiedades de confidencialidad, integridad de los datos y autenticación.

Los esquemas de identificación son métodos mediante los que una entidad (usuario, máquina) puede probar su identidad a alguien distinto así mismo, sin revelar ningún dato propio esencial que permita a un intruso suplantarle. Los esquemas de identificación implican que el aspirante:

- ***Demuestre saber algo***: palabras de paso.
- ***Demuestre tener algo:*** una tarjeta magnética, por ejemplo.
- ***Muestra característica*** e indeleble: retina, ADN, ritmo de teclado.
- ***Existe un tercero de confianza que lo avala***: certificados.

2.2.2 Autenticación con RADIUS.

Si se selecciona y configura RADIUS como agente de autenticación en el servidor VPN, las credenciales de los usuarios y los parámetros de la conexión son enviados como una serie de mensajes de petición RADIUS al servidor RADIUS. Este servidor recibe una petición de conexión de usuario del servidor VPN y es donde autentifica a dicho usuario a utilizar su base de datos de autentificación. Como se muestra una auntenticación con RADIUS en la *figura No.6* RADIUS, autorizando un acceso remoto al servidor de autenticación usando RADIUS).

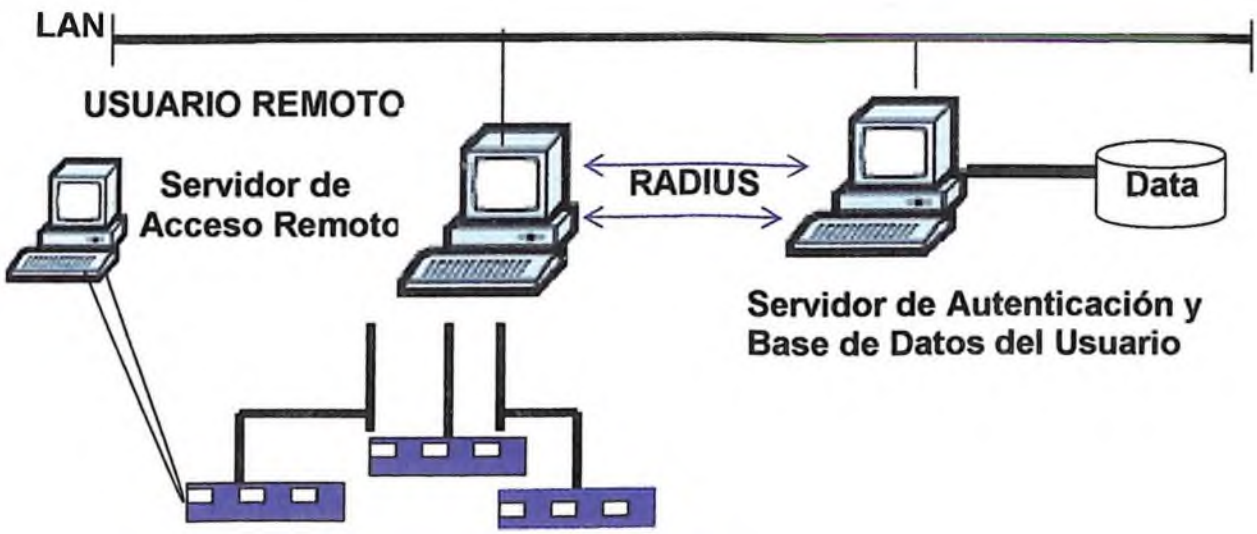


Fig. No.6. Autenticación con RADIUS.

2.2.3 Password de uso único (One-Time Password).

Este password actúa como su nombre lo indica. Se usa una sola vez y no vuelve a ser empleado. Lo que proporciona una gran seguridad frente al intruso que utilice la repetición a ciega de password.

2.3 Tecnología de Tunelización en VPN.

Esta tecnología esta basada en estándares establecidos. Esta tecnología es un modo de transferir datos entre dos redes similares sobre una red intermedia. También se llama "Encapsulación", a la tecnología de túneles que encierra un tipo de paquete de datos dentro del paquete de otro protocolo, que en este caso sería TCP/IP. En el caso de las VPN los paquetes están encriptados de forma que los datos son ilegibles para los extraños. Los paquetes encapsulados viajan a través de Internet hasta que alcanzan su destino, donde los datos se separan y vuelven a su formato original. (*Ver figura No.7*)

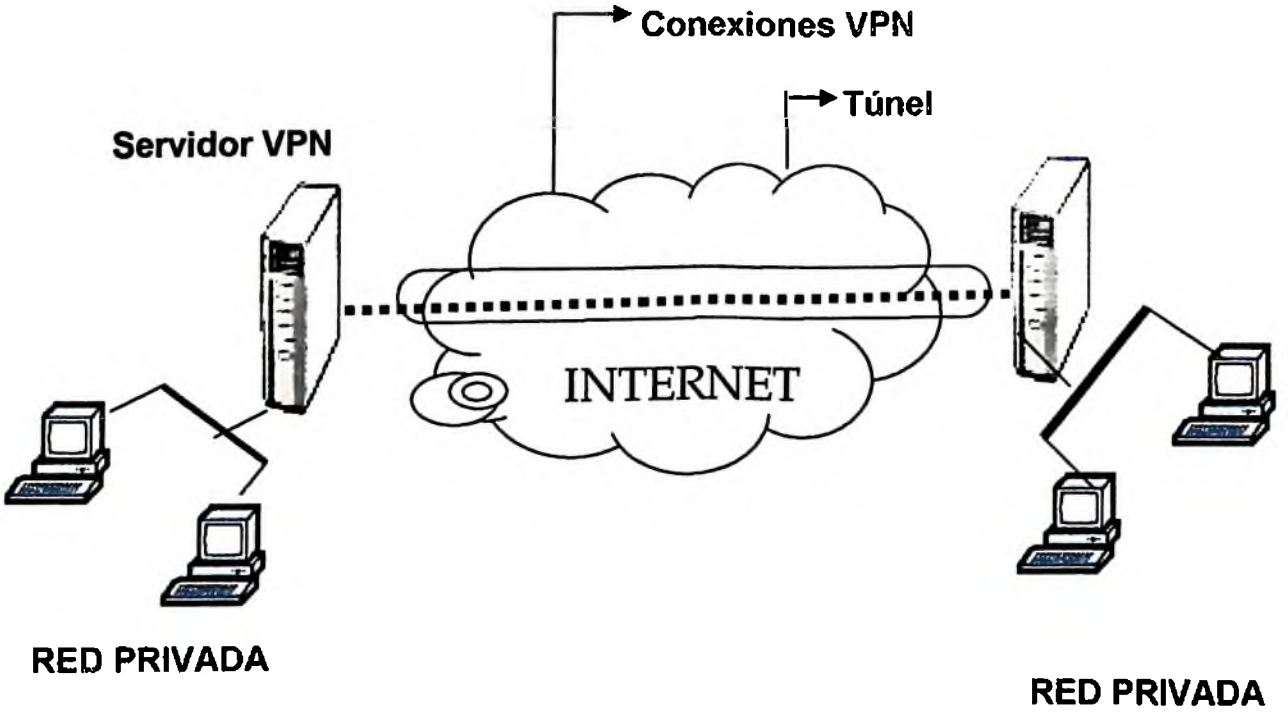


Fig.7. Como viajan los paquetes encapsulados

Para utilizar estos túneles propiamente es necesario tener en cuenta ciertos aspectos como seguridad, calidad de servicio, disponibilidad e interoperación. Estos túneles virtuales privados deben utilizar las mismas técnicas de seguridad que en una Intranet con métodos de autenticación y verificación con "Password" y encriptación que faciliten la administración, mantenimiento y facilidad de uso para el usuario.

En el cuadro No.1 se presentan los métodos de seguridad que utilizan las Redes Privadas Virtuales (VPN) para reguardar las informaciones y los objetivos que persiguen con cada método:

Objetivos	Método
Confidencialidad 	Encriptación
Autenticación 	Certificado Digital/Firma Digital
Autorización 	Passwords, PAP, CHAP, RADIUS, TACAS+
Integridad 	Interprete de Algoritmo de seguridad

Cuadro No.1: Objetivos y métodos de seguridad VPN

2.4 Protocolos utilizados por las VPN's.

Una razón para el número de protocolos es que para algunas compañías, una VPN es un sustituto para los servidores de acceso remoto, permitiéndole a los usuarios móviles y a las oficinas ramificadas marcar en la red incorporada protegida vía su ISP local. Para otras, una VPN podría consistir en el tráfico que viaja en túneles seguros sobre Internet entre las LANs protegidas.

Entre los protocolos más utilizados para la creación de VPN's sobre Internet, están:

1. El Point-to-Point Tunneling Protocol (PPTP)
2. Layer 2 Forwarding (L2F)
3. Layer 2 Tunneling Protocol (L2TP)
4. IP Security Protocol (IPSec)

2.4.1 El Point-to-Point Tunneling Protocol (PPTP).

El Protocolo de Túnel de Punto a Punto, originalmente desarrollado por la Ascend y la Microsoft y uno de los primeros utilizados por las VPN's. Es un protocolo de red que permite el tráfico seguro de datos desde un cliente remoto a un servidor corporativo privado, estableciéndose así una Red Privada Virtual (VPN) basada en TCP/IP.

Como protocolo de túnel, PPTP encapsula datagramas de cualquier protocolo de red en datagramas IP, que luego son tratados como cualquier otro paquete IP. La gran ventaja de este tipo de encapsulamiento es que cualquier protocolo puede ser ruteado a través de una red IP, como Internet.

El PPTP encapsula los paquetes PPP usando una versión modificada del protocolo GRE, el cual otorga al PPTP la flexibilidad del manejo de otros protocolos que no sea IP, como Internet Packet Exchange (IPX) y el sistema NetBEUI, tal y como se ilustra en la *figura No.8*.

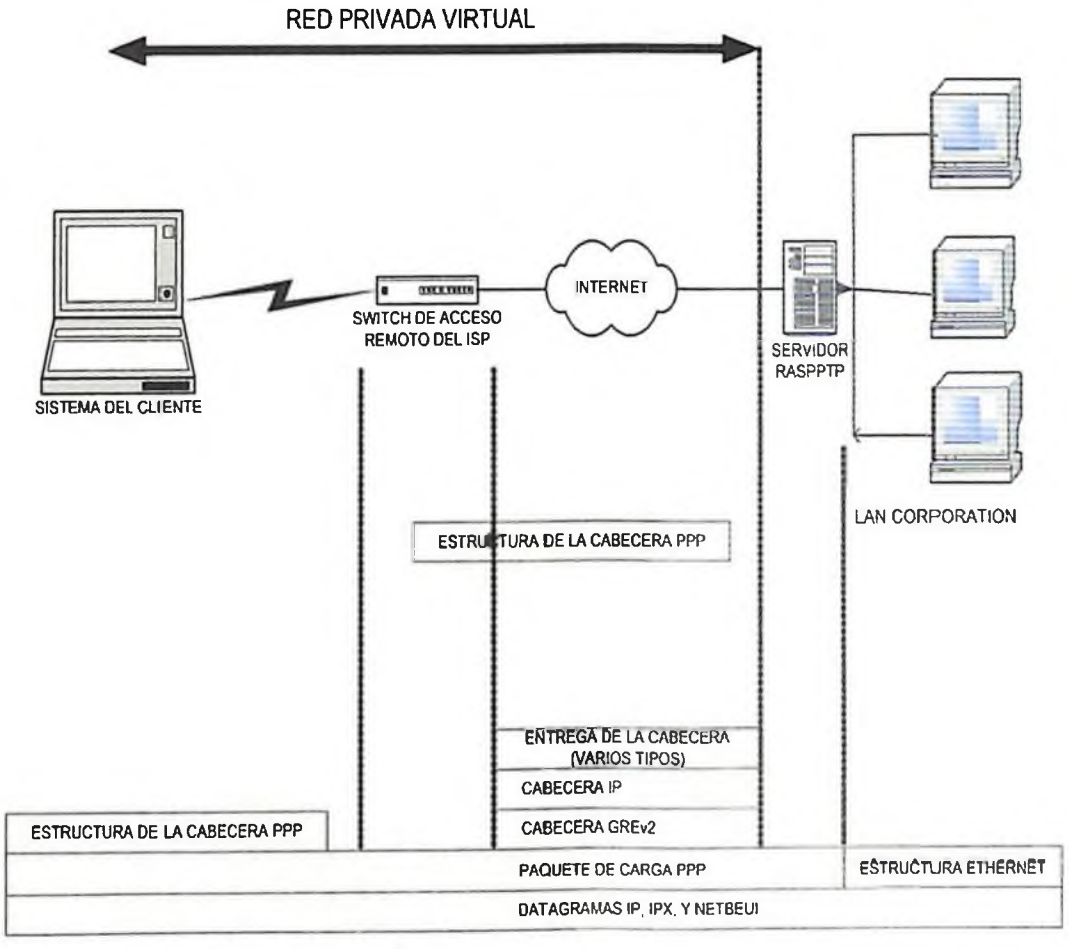


Fig.8 Protocolos usados en la conexión PPTP

PPTP fue diseñado para permitir a los usuarios conectarse a un servidor RAS desde cualquier punto en Internet para tener la misma autenticación, encriptación y los mismos accesos de LAN como si discaran directamente al servidor. En vez de discar a un modem conectado al servidor RAS, los usuarios se conectan a su proveedor y luego "llaman" al servidor RAS a través de Internet utilizando PPTP.

El hardware que se requiere en el servidor es una máquina configurada como PPTP server, debe tener la configuración mínima requerida para correr Windows NT 4.0 Server. Debe tener además dos adaptadores de red, uno conectado a la red local LAN y otro a Internet.

Este protocolo es el más comúnmente usado para el acceso remoto a Internet. El PPTP constituye una funcionalidad del PPP para proveer acceso remoto que puede ser tunelizado a través de Internet a su sitio de destino.

El direccionamiento público y privado en los datos del túnel PPTP para clientes VPN de acceso telefónico que se conectan a Internet antes de crear la conexión VPN con un servidor VPN en Internet, es asignado mediante dos direcciones IP:

Cuando se crea la dirección PPP, la negación IPCP con el NAS del ISP asigna una dirección IP pública.

1. Cuando se crea la conexión VPN, la negación IPCP con el servidor VPN asigna una dirección IP de la Intranet, ya sea en una dirección pública o privada.

Un ejemplo del direccionamiento de un cliente de acceso telefónico se muestra en la ***figura No.9*** donde la organización utiliza direcciones privadas en Intranet y los datos enviados por el túnel están dentro de un datagrama IP.

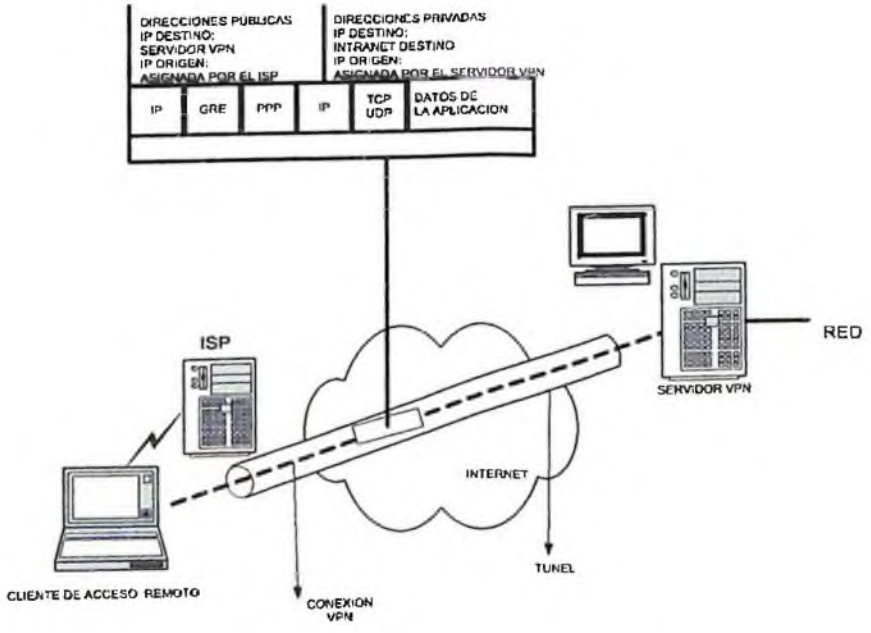


Fig.9. Direccionamiento público y privado en los datos del túnel PPTP

2.4.1.1 Seguridad de la información transmitida en PPTP.

La autenticación de usuarios se realiza a través de los protocolos existentes en el servidor de acceso remoto (PAP y CHAP).

Por otro lado también puede existir una seguridad adicional establecida por el proveedor de servicios de Internet TCP/IP. PPTP hace uso de la seguridad que da el protocolo PPP. Mientras que la autenticación la toma de MS-CHAP que valida las credenciales del usuario remoto contra dominios NT, ya que sólo los usuarios autorizados pueden realizar la conexión.

2.4.1.2 Mantenimiento del túnel con el control de conexión PPTP.

Este se encuentra entre direcciones IP del cliente PPTP que utiliza el puerto TCP asignado. Este lleva a cabo el control de la llamada del PPTP y la administración de mensajes que son utilizados para mantener el túnel PPTP. Los paquetes de control de conexión PPTP consisten de una cabecera IP, una cabecera TCP y un mensaje de control PPTP como se muestra en la figura No.8 el paquete de control de conexión PPTP en el cuadro No.2, también incluye una cabecera de la capa de enlace de datos y una cola.

CABECERA DEL ENLACE DE DATOS	**IP**	**TCP**	**MENSAJE DE CONTROL PPTP**	**COLA DEL ENLACE DE DATOS**

Cuadro No.2. Paquetes de conexión PPTP.

2.4.1.3 Procesamientos de los datos enviados con PPTP.

Al recibir los datos enviados por el túnel PPTP, el cliente o el servidor PPTP, ejecuta las siguientes acciones:

1. Procesa y elimina la cabecera y la cola del enlace de datos.
2. Procesa y elimina la cabecera IP.
3. Procesa y elimina las cabeceras GRE y PPP.
4. Desencripta, descomprime o ambas procesos, la carga PPP, siempre que sea necesario.
5. Procesa la carga para recepción o reenvío de información.

2.4.1.4 Configurando el PPTP en Windows para establecer una VPN.

El PPTP viene como una característica de Windows NT 4.0 (Server y Wokstation), incluida en el propio producto. No existe para versiones anteriores de NT.

A. Si todavía no se ha hecho, Se debe proceder a instalar el Acceso Telefónico a Redes. Para ello, se puede basar en el siguiente artículo de la Base de Conocimientos de Microsoft:

   ARTICLE.ID : Q171015

   TITLE : How to install and configure Windows NT 4.0
   : Dial-Up Networking.

B. Se agrega el protocolo PPTP, a través del Panel de control, icono de Red, pestaña Protocolos, botón Agregar.

C. Después de que el protocolo se agregue, el Servidor de Acceso Remoto (RAS) aparecerá. Se debe agregar al menos un puerto de Red Privada Virtual (VPN). Se puede especificar hasta 256 de ellos. Cada uno puede conectarse a una red distinta.

D. En este punto, se especifica qué protocolos se usarán en cada puerto.

E. Debe asegurarse de que al menos un puerto VPN está configurado para realizar llamadas.

F. Si todavía no se ha hecho, debe crear una entrada de Acceso telefónico a Redes al Proveedor de Servicios de Internet. Para ello, puede basarse en el siguiente artículo de la Base de Conocimientos de Microsoft:

ARTICLE-ID	:	E10281
TITLE	:	Cómo conectar a Infovía desde Windows NT 4.0

G. Cree una entrada de Acceso Telefónico a Redes para su servidor PPTP. Utilice como número de teléfono el nombre o mejor aún la dirección IP de dicho servidor. Asegúrese de que esta entrada está utilizando un puerto RASPPTPM VPM en la caja de diálogo "Marcar una X."

H. Realice la conexión a Internet a través de su proveedor, y una vez establecida con éxito, realice la conexión al servido PPTP.[1]

[1] Si la computadora suele estar conectada mediante un adaptado de red a la red remota, como pudiera ser el caso de una laptop, tendrá que agregar una ruta a la tabla de enruptado para asegurar que los paquetes se envían al adaptado de red adecuado.

2.5 Layer 2 fowarding (L2F).

Protocolo de túnel, originalmente creado por Cisco. La tecnología L2F permite el proceso de túnel multiprotocolo, y es sustentada por muchos vendedores, es excelente para el acceso remoto en POP (Point of Presence, punto de presencia: Punto de acceso a una red de comunicación nacional o internacional). El L2F también se despierta en las primeras etapas de desarrollo de VPN. Como el PPTP, el L2F fue diseñado como un protocolo para llevar el tráfico en los túneles desde los usuarios a sus sites incorporados. El L2F usa el PPP para la autenticación del usuario remoto, pero también incluye soporte para la autenticación de TACACS+ y RADIUS.

2.6 Layer 2 Tunneling Protocol (L2TP).

Fue creado como sucesor de dos (2) protocolos de túnel, PPTP y L2F. En vez de desarrollar dos protocolos competentes para realizar esencialmente la misma labor, PPTP de la Microsoft versus L2F de la Cisco, lograron un acuerdo para trabajar juntos en un solo protocolo, L2TP, el cual sometieron a la IETF[2].

Las características del L2F han sido llevadas al L2TP. Como el PPTP, el Layer2 fowarding Protocol utiliza la funcionalidad del PPP para proveer acceso **Dial-up** que puede ser transmitida por túnel a través de Internet hacia una localidad de destino. Aunque el L2TP define su propio protocolo de túnel, basado en el trabajo del L2F.

[2] IETF (Internet Engineering Task Force; Misión Especial de Ingeniería Internet: Organización Mundial que desarrolla nuevas tecnologías y estándares para la Internet.) para la estandarización.

El L2TP es un protocolo de comunicación entre dispositivos de datos y es transparente a las aplicaciones de usuarios existentes. No hay necesidad de invertir en programas nuevos para aprovechar las ventajas del L2TP. Los túneles L2TP residen exclusivamente en la capa PPP, por lo que es posible transportar de forma sencilla otros protocolos además de IP. Este permite al punto de presencia (POP) estar situado lejos de los servidores de la empresa. Ello permite a los usuarios y redes remotas acceder a la red corporativa a un precio reducido, y no restringirlo a aplicaciones TCP/IP (ver figura No.10).

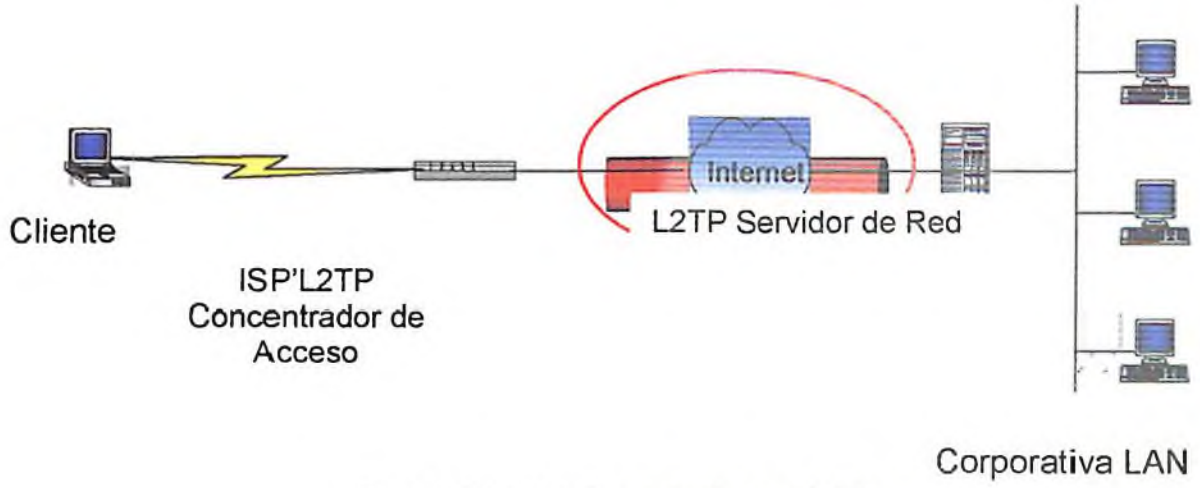


Fig.10. Muestra de un protocolo L2TP

La figura No. 11 muestra la relación entre los marcos PPP y los mensajes de control a través de los canales de control y datos de L2TP.

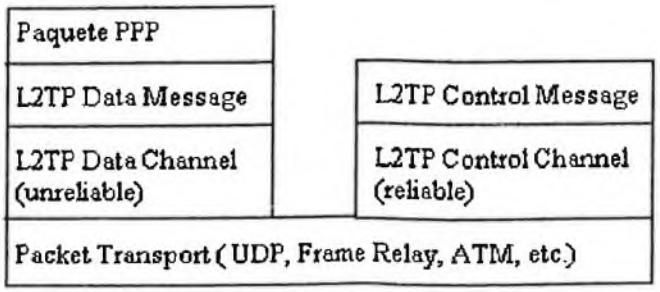


Fig.11. Relación entre los marcos PPP y los Mensajes de Control a través de LTP

Los marcos PPP son enviados a través de un canal de datos no confiable, encapsulado primero por un encabezado L2TP y luego por un transporte de paquetes como UDP, Frame Relay o ATM. Los mensajes de control son enviados a través de un canal de control L2TP confiable que transmite los paquetes sobre el mismo transporte de paquete.

2.7 IP Security Protocol (IPSec).

El ultimo protocolo, pero quizás el más importante, el IPSec, incrementó sus esfuerzos para asegurar los paquetes IP como la próxima generación de IP (Ipv6); ahora puede usarse con los protocolos Ipv4 de igual modo.

El IPSec permite al emisor (o a un gateway de seguridad que actúe por su cuenta) autenticar o encriptar cada paquete IP o aplicar ambas operaciones al paquete. Al separar la aplicación de la autenticación de paquete y la encriptación se ha delegado a dos modos: en el modo de transporte, sólo el segmento de nivel de transporte de un paquete IP es autenticado o encriptado. En el modo de túnel se autentica o encripta todo el paquete IP, mientras el modo de transporte IPSec puede probar ser útil en muchas situaciones, provee incluso más protección contra ciertos ataques y monitoreos de tráfico que podría ocurrir en la Internet. Está construido alrededor de un número de tecnologías criptográficas estandarizadas para proveer confidencialidad, integridad y autenticación.

Por ejemplo, el IPSec usa:

- Criptografía de clave pública para señalar los intercambios, para garantizar las identidades de las dos partes y previene los ataques Than in the middle.
- DES y otro volumen de algoritmo de encriptación para encriptar la data.
- Keyed hash algoritms (HMAC, MD5, SHA) para autenticación de paquete.
- Certificados digitales para la validación de las claves públicas.

Esencialmente, el IPSec maneja dos tipos de problemas:

- Considera esos casos donde una red contiene información que debería permanecer en una base de datos confidencial; Recursos Humanos, Información Médica, e Información Financiera, por ejemplo.

- Hay veces en que el acceso a la red debería estar limitado a usuarios autorizados y la entrada a través de equipos autorizados (esto es importante si la compañías construyen).

2.8 Interconexión Firewall en Redes Privadas Virtuales.

Los Firewalls (cortafuegos) son una colección de filtros que proporcionan un punto donde concentrar las medidas de seguridad. Ellos verifican que el tráfico no autorizado fuera de su red no pueda entrar en la misma. Por ende, los firewall protegen los puntos de entrada de un ataque externo y sólo permiten el paso al tráfico autorizado. Entre dos redes solo permiten el paso a los paquetes de información autorizados. Generalmente los firewall se dividen en dos lados: ***un lado externo y otro interno.***

- ***El lado externo de un firewall*** incluye servicios que están disponibles para el público en general y generalmente incluye la habilidad de recibir E-mail, así como servicios de directorio (DNS) para los recursos públicos, como un site de Web.

- ***El lado interno*** provee un conjunto de servicios separado para aquellos que están dentro del firewall. Esto puede incluir servicios de directorio para encontrar servidores de archivo confidenciales, sites de Web, y otros. Así también servicios para retirar mensajes. Todos estos recursos están pensados para uso privado y es importante que se mantengan alejados de la red pública externa.

Para prevenir que intrusos de la red pública accedan a recursos corporativos, el firewall bloquea el tráfico de la red pública para que no entre en la red interna. Pero, algún tipo de tráfico debe pasar a través del firewall, para permitir cierto, los firewall proveen a los administradores reglas y proxies. Con los que, los administradores pueden configurar que tráfico puede pasar y bajo que circunstancias. Desde el punto de vista de configuración, el objetivo es minimizar la cantidad de diferentes tipos de tráfico pasando a través del firewall y así limitar el número de agujeros.

2.8.1 Tipos Básicos de Firewall.

a) Nivel de red.

Los firewalls a nivel de red generalmente, toman las decisiones basándose en la fuente, dirección de destino y puertos, todo ello en paquetes individuales IP. Un simple router es un "tradicional" firewall a nivel de red, particularmente, desde el momento que no puede tomar decisiones sofisticadas en relación con quien está enviando un paquete ahora o desde donde está llegando en este momento. Los firewalls modernos a nivel de red se han sofisticado ampliamente, y ahora mantienen información interna sobre el estado de las conexiones que están pasando a través de ellas, los contenidos de algunos datagramas y más cosas.

b) Nivel de aplicación.

Los Firewalls a nivel de aplicación son generalmente, hosts que corren en servidores proxy, no permiten tráfico directo entre redes y realizan logins elaborados auditando el tráfico que pasa a través de ellos. Los firewalls a nivel de aplicación se pueden usar como traductores de direcciones de red. Los primeros firewalls a nivel de aplicación eran poco transparentes a los usuarios finales, pero los firewalls modernos a nivel de aplicación son bastante transparentes. Los firewalls a nivel de aplicación, tienden a proporcionar mayor detalle en los informes auditados e implementan modelos de conservación de la seguridad. Esto los hace diferenciarse de los firewalls a nivel de red.

2.8.2 Puntos que permite el Firewall

Entre estos puntos están:

1. Permiten desactivar servicios que se consideran inseguros desde Internet.
2. Permiten restringir fácilmente el acceso o la salida desde/hacia determinadas máquinas.
3. Permiten el registro de información sobre la actividad entre la red interna y el exterior.
4. Bloquea el acceso para NFS.
5. Aislar unas secciones internas de la red de otras.

2.8.3 Tecnologías de los Firewalls

Existen tres tipos de tecnologías:

1. ***Filtros de paquetes:***

   En esta tecnología el firewall trabaja a nivel de TCP/IP. No tiene control de los paquetes que está filtrando y es totalmente transparente al usuario.

2. ***Gateway a nivel de Circuitos:***

   Estos interceptan las secciones y las pasan a través de los firewalls. Los gateways son una definición segura, y todo el tráfico de entrada y salida está gobernado por ellos.

3. ***Gateway a nivel de Aplicaciones:***

   Efectúa el mismo tipo de función de los gateways nivel de circuitos con una adicción; examinan los contenidos de cada paquete cuando pasa por ellos. Es el protocolo de filtro más seguro.

2.8.4 Configuración del Firewall y el Servidor VPN.

Existen dos abordajes para utilizar un firewall con un servidor VPN:

- **Servidor VPN frente al Firewall**

Con el servidor VPN en frente al firewall conectado a Internet, como se muestra en la figura No.11, se necesita agregar los filtros de paquetes a la interfase con Internet que solamente permitan tráfico de la VPN hacia y desde la dirección IP de la interfase del servidor VPN en Internet.

Para el tráfico que entra, una vez que los datos enviados por el túnel son desencriptados por el servidor VPN, son redirigidos al firewall, el cual utiliza sus filtros para permitir que el tráfico sea redirigido a los recursos de la Intranet. Debido a que solamente el tráfico que está cruzando el servidor VPN en tráfico generado por clientes VPN autentificados, el filtrado del firewall en este escenario puede ser utilizado para evitar que los usuarios VPN tengan acceso a recursos específicos de la Intranet.

Debido a que el único tráfico de Internet que es permitido el paso a la Intranet debe pasar a través del servidor VPN, este abordaje también evita que se puedan compartir recursos de la Web y del Protocolo de Transferencia de Archivos (File Transfer Protocol, FTP) con usuarios que no estén en la VPN. (Ver la *Figura No.12*, donde se conecta un Servidor VPN frente a un firewall).

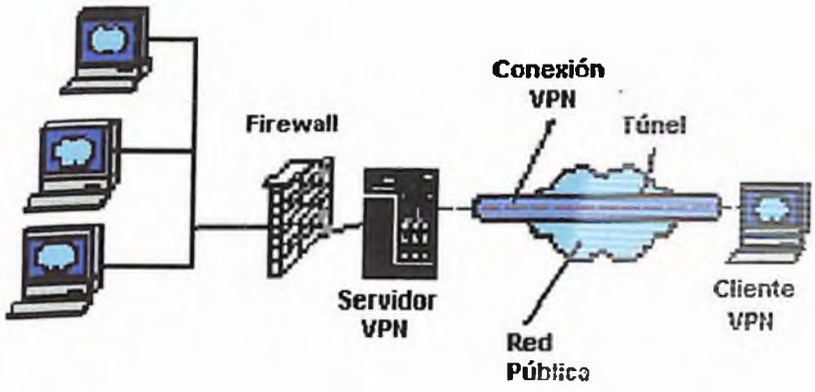


Fig. 12. Conexión de un servidor VPN frente a un firewall

- **Servidor VPN detrás del Firewall**

Con este abordaje, el firewall debe de configurarse con filtros de entrada y salida en su interfase con Internet para permitir el paso del tráfico de mantenimiento del túnel y los datos del túnel hacia el servidor VPN. Debido a que el firewall no tiene las claves de encriptación para cada conexión VPN, solamente puede filtrar las cabeceras no encriptadas de los datos del túnel, dando como resultado que todos los datos del túnel pasan por el firewall. Sin embargo, esto no afecta la seguridad debido a que la conexión VPN requiere un proceso de autentificación que previene el acceso no autorizado más allá del servidor VPN (ver figura No.13).

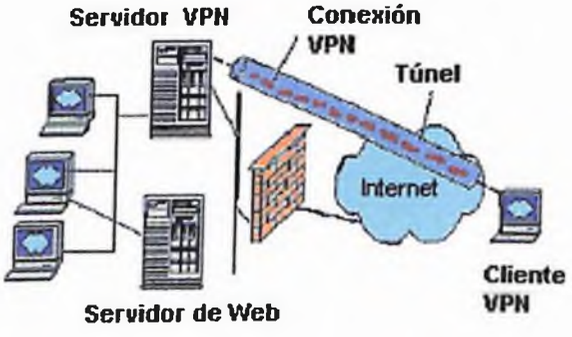


Fig.13. Servidor VPN detrás del firewall

Capítulo III

DISEÑO Y APLICACIONES DE REDES PRIVADAS VIRTUALES (VPN's)

CAPITULO III DISEÑO Y APLICACIONES DE REDES PRIVADAS VIRTUALES (VPN´S)

3.1 Diseño de una VPN.

El diseño de una Red Privada Virtual (VPN) deberá hacerse con mucho cuidado porque no solo afecta la conectividad entre las diferentes partes de la organización y seguridad de los datos, sino también que puede afectar el tráfico de la red en cada site. Un diseño apropiado, un alineamiento autorizado de las necesidades futuras, además le ayudará a resolver cualquier problema que se presente en el camino. A continuación presento las principales consideraciones al momento del diseño de este tipo de red.

3.1.1 Determinación de Requerimientos.

Al diseñar una red lo primero, es determinar los requerimientos, tener una idea clara de la demanda que recaerá sobre ésta; qué tipo de tráfico de datos o información se transmitirá, qué aplicaciones se usarán y con qué frecuencia, además, estar conciente del nivel de seguridad requerido por el tipo de data y por usuario.

El diseñador de la red debe realizar las siguientes preguntas por cada lugar a ser conectado:

1. ¿Cuántos usuarios existen en cada sitio que requerirá interconexión?

2. ¿Qué tipo de conexión al Internet se requiere? ¿Será acceso continuo o de demanda?

3. Si se requiere conexión continua a Internet, ¿Cuál es el tiempo mínimo de disponibilidad que el sitio requiere? ¿Será necesaria una segunda conexión de respaldo?

4. Si se requiere una conexión en demanda, ¿Con qué frecuencia se conectará? ¿Qué tipo de confiabilidad se requeriría, con qué frecuencia?

5. ¿Cuánto tráfico genera cada sitio específico? ¿Cómo varía el tráfico de hora en hora?

6. ¿Se requiere dar acceso a usuarios remotos en este sitio? ¿A cuántos?

Una vez contestadas estas preguntas, se debe proceder a determinar y analizar cómo acomodar las mismas a través de los enlaces WAN. Las estimaciones del ancho de banda y la arquitectura de los enlaces WAN es crucial para determinar el requerimiento de enlace de sitio del proveedor de Internet.

3.1.2 Dispositivos en la Red.

En un segundo lugar se recomienda que al diseñar una VPN, una vez ponderadas las consideraciones por cada sitio a ser conectado vía VPN, se proceda a considerar toda la red corporativa con todos los sitios en conjunto, donde se debe:

a) Determinar la localización geográfica de cada sitio, ver cuáles sitios requieren comunicación entre sí.

b) Determinar el tipo de seguridad de acuerdo al tipo de datos a ser transmitido, a fin de ver que necesita encriptación y qué puede ser transmitido como texto normal.

c) Tomar en cuenta el uso de los certificados digitales, considerando los tipos de usuarios dentro de la organización.

d) Verificar que el ISP garantice el punto de presencia (POP) en todos o en la mayoría de los lugares que necesite conectarse la organización.

e) Considerar la posibilidad del uso de Back-up (hasta en segundos) dependiendo del tipo de información a ser transmitido.

Se debe considerar muy bien los equipos a utilizar, tales como el Router o Firewall, el tipo de encriptación, así como los servidores de acceso remoto y los bancos de modems, también ver el sistema de autenticación a utilizar. Velar además que la VPN cumpla con las políticas de seguridad establecidas por la organización, también se debe dar participación en el diseño de la VPN, al proveedor de servicio de acceso a Internet.

El IPS debe garantizar el punto de presencia (POP) en todos o en la mayoría de los lugares que necesite conectarse la organización. Si se piensa en transmitir información sumamente importante por VPN, se debe considerar la posibilidad de Back-up (que pueda guardar información por segundos).

Tan pronto como se haya obtenido este conjunto de información se tiene la base sobre la cual se levantaría el diseño requerido.

3.1.3 Plan Pre-Implementación.

Por último, está la pre-implementación del sistema diseñado, la cual debe ser sometida a una auditoria del nivel de seguridad existente en la organización, garantizando así que no haya hoyos que permitan ataques externos. En caso de descubrir debilidades de seguridad, se deben corregir antes del despliegue de la VPN diseñada.

3.1.4 Configuración de VPN's de Acceso Remoto.

El primer paso es ver qué tipo de conexión WAN se necesita, la cual cae en dos categorías: *enlaces de Intranet* y *enlaces de Extranet*.

- En Intranet, la VPN conecta direcciones confiables y usuarios en la misma organización.

- En Extranet, la VPN debe equipar el mismo acceso a la red corporativa como si el usuario o la oficina ramificada estuvieran conectados físicamente.

Al configurar la VPN, los diseñadores de red necesitan fijar los parámetros para longitud de clave; los servidores de autenticación primario y secundario; la conexión y el tiempo de ocio; la generación certificada y generación de clave, así como los mecanismos de distribución. Además, los certificados digitales que se encargarán de verificar la identidad de las máquinas en puntos finales de VPN (en vez de usuarios). Para usuarios remotos también será necesario fijar password, y establecer procedimientos de autenticación.

Los administradores de red también necesitan sincronizar las rutinas de autenticación y autorización. La autenticación debe probar que un usuario remoto es quien dice ser; la autorización determina cuales recursos de red son a los que el usuario tiene derecho. También se debe chequear los protocolos y la exportabilidad de claves de encriptación.

3.1.5 Configuración de una VPN Bajo Windows.

Para configurar una VPN bajo Windows se necesita lo siguiente:

- Conexión a Internet tanto para el servidor local de NT como para las computadoras remotas.
- Una dirección IP estática para el servidor NT.
- Proxy que se ejecute en el servidor NT, para evitar el acceso desautorizado al sistema.
- Direcciones IP para los recursos a compartir.
- Adaptador virtual de la red instalado en la máquina remota o cliente.

La secuencia de pasos es:

1. Hacer una lista de las direcciones IP de los recursos que serán compartidos a través de Internet.
2. Instalación y ejecución del proxy.
3. En el servidor NT, se deben configurar los archivos del usuario NT para que pueda llamar y conectarse al servidor, garantizando su acceso al sistema con los permisos de la VPN.

4. Luego de estos pasos, se deberá instalar el adaptador privado de la red en la computadora cliente, como se indica:

5. Dentro del Diálogo de Red, que se muestra debajo (Figura No.14), y al cual se accede a través de la opción Propiedades del icono Entorno de Red, se presiona el botón Add.

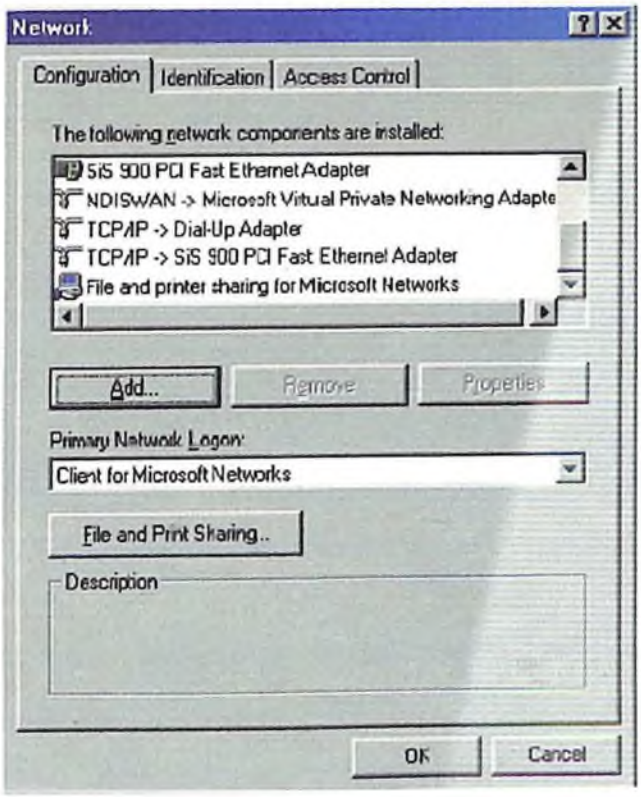


Fig. 14. Pantalla diálogo de red

Aparecerá la siguiente pantalla, se deberá seleccionar Adapter y luego presionar el botón Add. ***(Figura No. 15)***

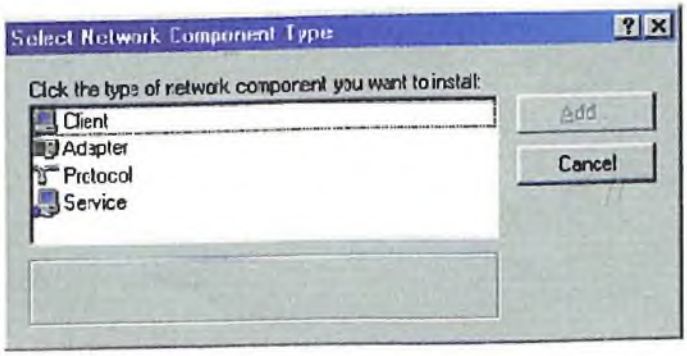


Fig.15. Pantalla para seleccionar el tipo de componente.

Aparece el cuadro Select Network adapters, donde se deberá elegir el fabricante y el adaptador como se muestra en la figura No. 16:

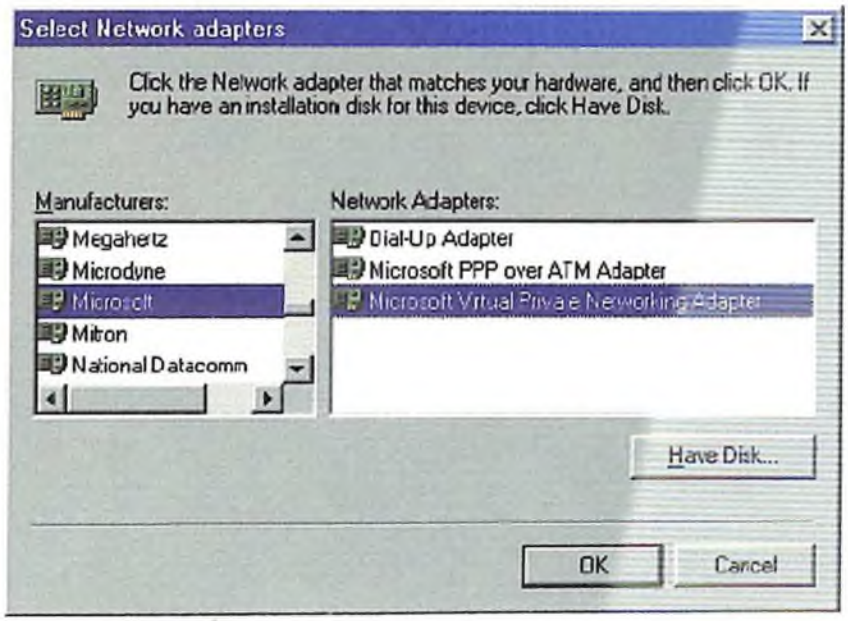


Fig.16. Pantalla para seleccfonar adaptadores de red.

Posteriormente, para instalar la conexión a la LAN, se deberá acceder al Acceso Remoto a Redes (Ver Figura No. 17)

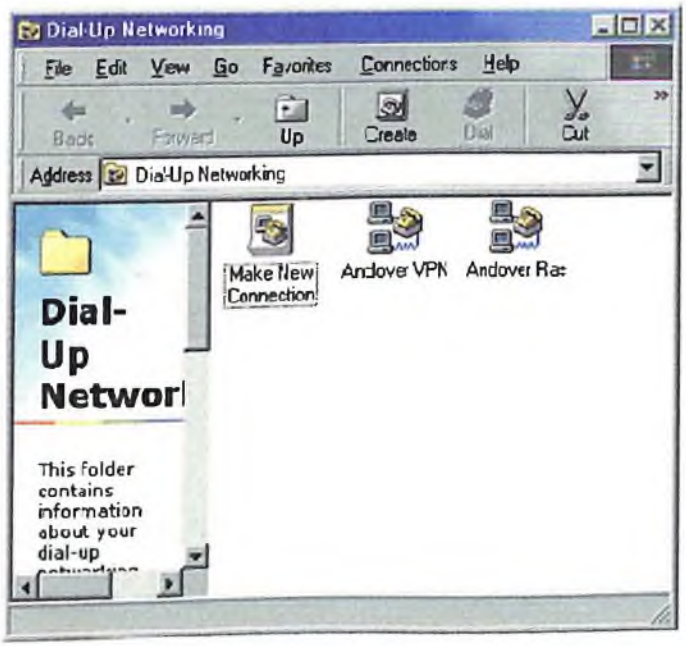


Fig.17. Pantalla de acceso remoto a redes.

Se selecciona Make a New Connection, apareciendo la siguiente pantalla, donde se podrá elegir el adaptador de VPN, como se muestra en la Figura No. 18:

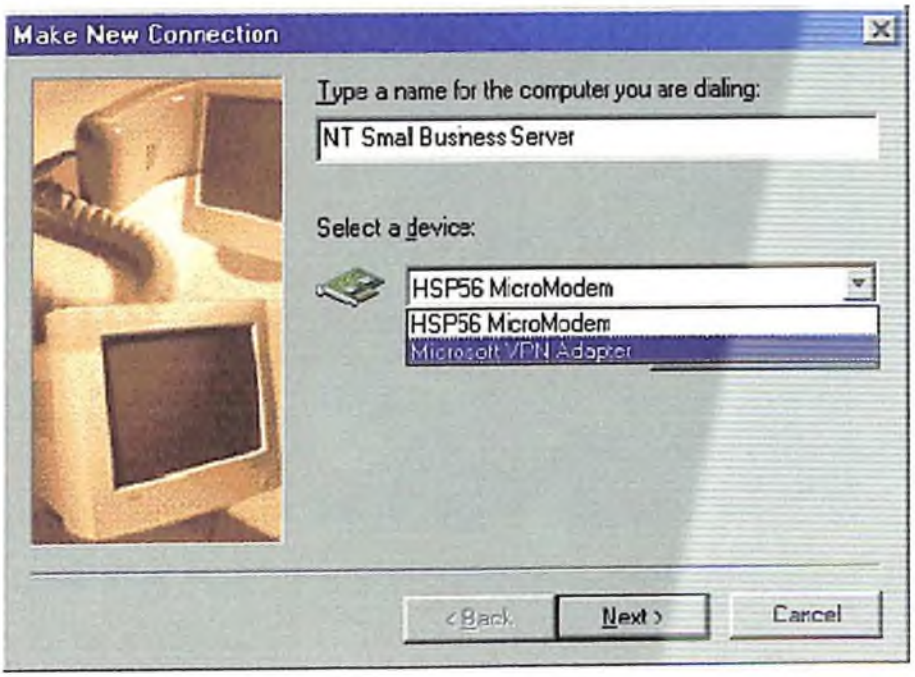


Fig.18. Pantalla para crear una nueva conexión.

Luego de presionar el botón Next, se deberá introducir la dirección IP del servidor VPN en la Figura No. 19:

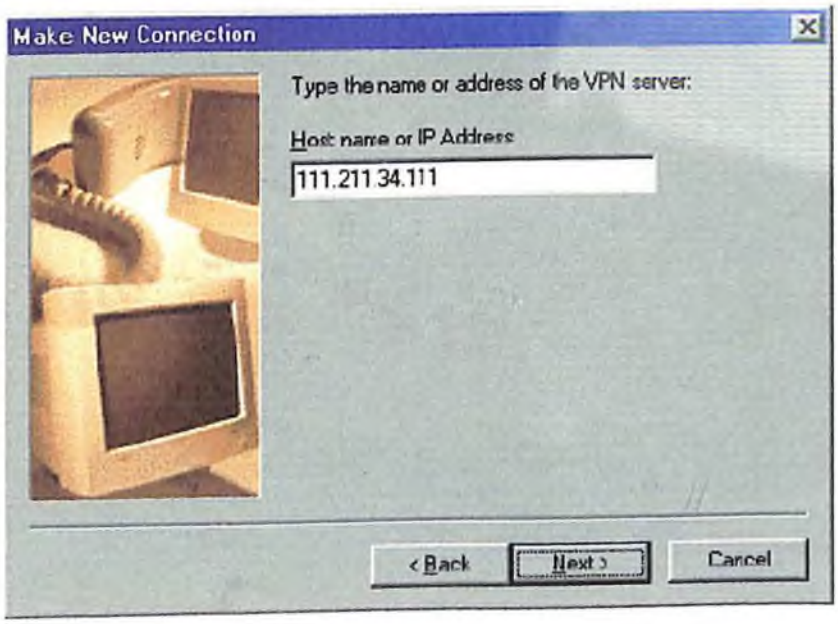


Fig.19. Pantalla con la dirección IP del servidor VPN

Así se finaliza la creación de la nueva conexión (Figura 20):

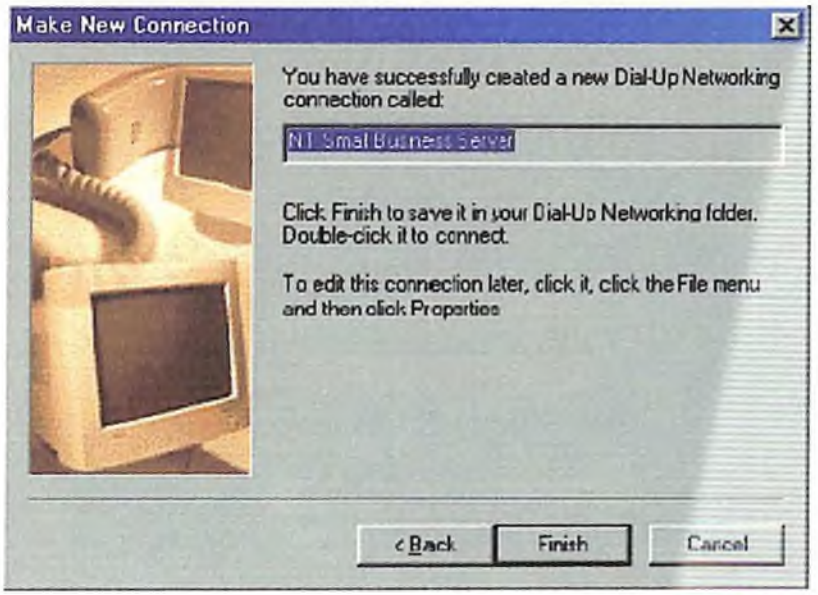


Fig.20. Muestra de cómo finaliza la creación de la conexión nueva.

Para acceder al servidor NT, se abre el Acceso Remoto a Redes (Figura 21):

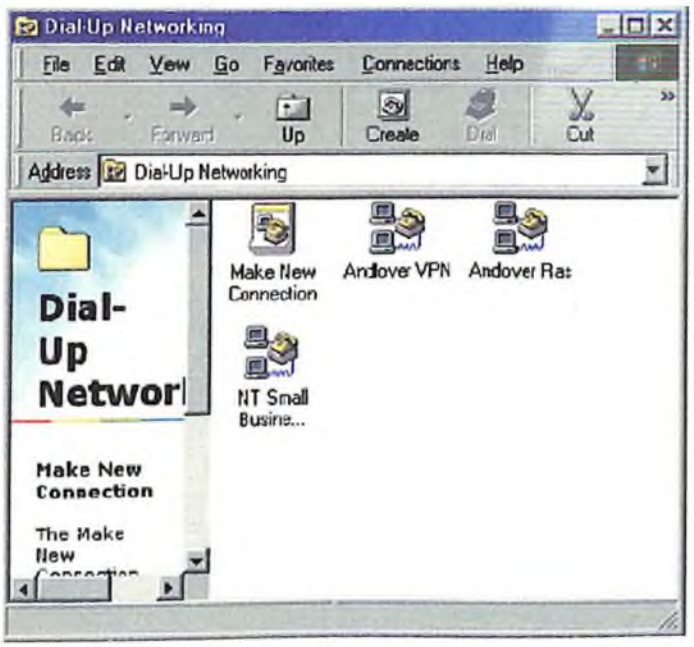


Fig. 21. Como acceder al servidor VPN

Al hacer doble-click en el icono de la conexión VPN, aparecerá la siguiente pantalla, donde se debe introducir el nombre de usuario, la contraseña y la dirección IP del servidor NT (Figura No. 22):

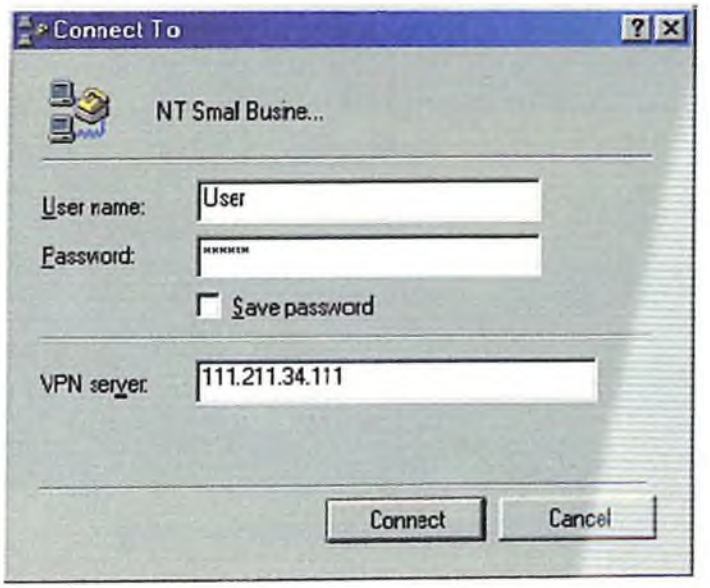


Fig.22 Pantalla de acceso a l servidor VPN

Para configurar el servidor VPN, se deberá configurar PPTP, activar el filtro PPTP y activar el soporte PPTP en los clientes.

Para configurar PPTP en el servidor RAS y en los clientes que vayan a utilizarlo, se deberán realizar los siguientes pasos:

Dentro de Red en el Panel de Control, seleccionando Protocolos, se deberá presionar el botón Agregar (Figura No. 23):

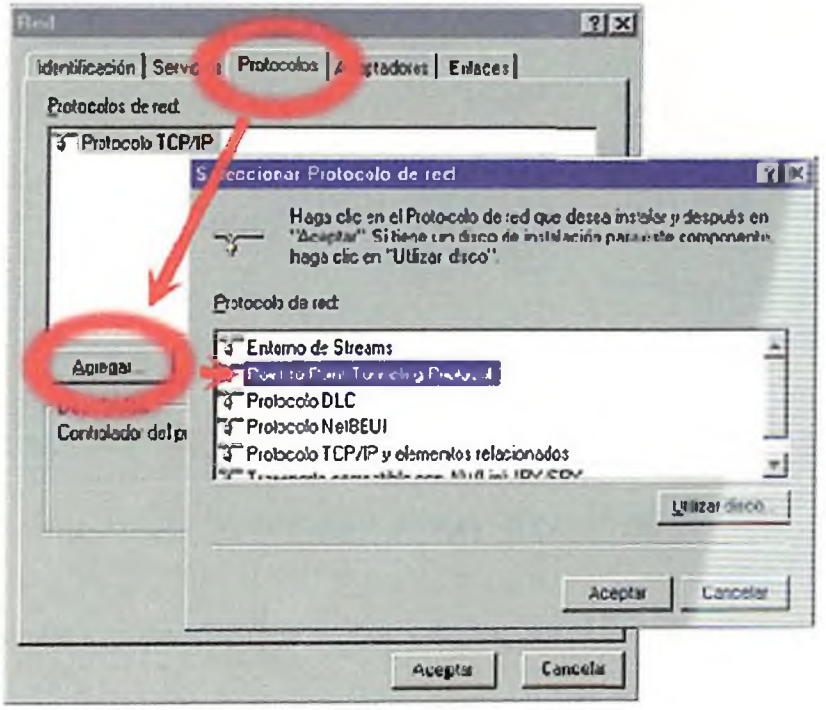


Fig.23. Pantalla para agregar protocolo

Se selecciona Point to Point Tunneling Protocol, y luego de copiados los archivos, aparecerá el cuadro de diálogo Configuración de PPTP. El campo Número de redes privadas virtuales indica el número de conexiones PPTP admitidas. En el ejemplo, se establecen 2 VPN (ver Figura No. 24):

Fig.24. Pantalla que indica el número de conexiones PPTP admitidas

Luego, se inicia la herramienta de configuración RAS, donde se deben añadir los puertos virtuales que darán servicio a las redes privadas virtuales que se deseen establecer. Al presionar el botón Agregar, se accede al dialogo Agregar dispositivo RAS (Figura 25):

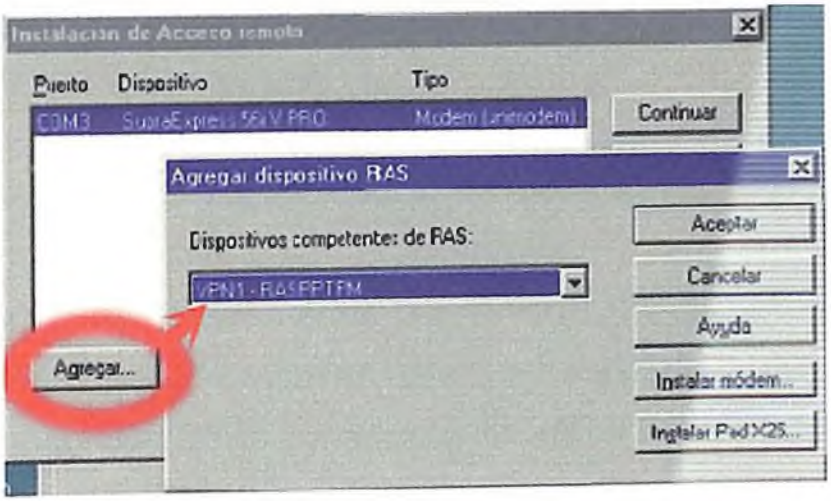


***Fig.25. Pantalla para agregar dispositivo** RAS*

Después de ingresadas las entradas, se presiona Aceptar. Luego se podrá seleccionar cada entrada del diálogo Instalación de Acceso Remoto, para configurar el uso del puerto. Las opciones son: Sólo recibir llamadas o Hacer y recibir llamadas.

Después de añadir todos los dispositivos virtuales, se podrá cerrar este diálogo para volver a la ficha Protocolos. Al reiniciar la computadora, ya estará configurado el server.

Para la activación del filtro PPTP, se debe selecciona la solapa Protocolos de Panel de Configuración / Red. Dentro de esta pantalla, se elige Protocolo TCP/IP, luego Propiedades. En la solapa Dirección IP, se selecciona el adaptador de red sobre el que se aplicará el filtro. Luego de presionar el botón Avanzadas, se marca la casilla Activar filtro PPTP y, por último, se reinicia la máquina para activar la configuración.

Cuando un cliente se conecta a Internet, el procedimiento para establecer un túnel VPN consta de dos pasos:

1. Establecimiento por parte del cliente mediante una conexión de acceso telefónico a través de un ISP.

2. Establecimiento de una conexión PPTP con el servidor RAS.

Cuando un cliente se conecta directamente a Internet, no es necesario establecer una conexión de acceso telefónico. Sin embargo, el procedimiento para iniciar la conexión PPTP con el servidor RAS es idéntico. Para establecer una conexión PPTP es necesario crear una entrada especial en la guía telefónica. Esta entrada se distingue por dos características:

El campo Marcar utilizado tiene uno de los dispositivos virtuales VPN añadidos a la configuración RAS al instalar PPTP. Esta lista sólo muestra los VPN configurados para hacer llamadas.

El campo Presentación preliminar de número telefónico contiene el nombre DNS o la dirección IP del servidor PPTP.

La creación de una conexión PPTP implica también dos pasos:

1. Se abre la aplicación Acceso telefónico a redes, utilizando la guía telefónica que permite acceder al ISP a través de un número de teléfono y un modem.

2. Establecida la conexión, se debe abrir la entrada de la guía telefónica que se conecta al túnel PPTP mediante un nombre DNS o una dirección IP.

Si el cliente está conectado directamente a Internet, sólo es necesario el segundo paso.

3.1.3 Aplicaciones de VPN.

Es difícil anticipar los requerimientos especiales de cada tipo de red y para diseñar una Red Privada Virtual útil, se necesita tener algunas ideas de las demanda que tomarán lugar en la red, o sea que tipo de datos será transmitido, que aplicaciones serán usadas, cuántas veces la red será usada, entre otras cosas. Para comprender mejor estas demanda se detallan las aplicaciones más utilizadas en el diseño de una VPN.

3.2.1 Extranet VPN.

Esta permita conexiones seguras con socios de negocios, suplidores y clientes para propósitos de comercio en línea. El Extranet VPN es una especie de extensión de Internet VPN con la adición de firewalls para proteger la red interna.

La Extranet VPN permite a las redes privadas extenderse a través de Internet u otro servicio público de red, en una forma segura. Es como la evolución lógica de su antecedente la Intranet. Una Intranet consiste en una red privada que tiene acceso total a Internet, pero Internet tiene un acceso restringido a ella, comportamiento que se consigue mediante elementos que se instalan como las firewalls, routers o servidores (ver *figura No. 26*).

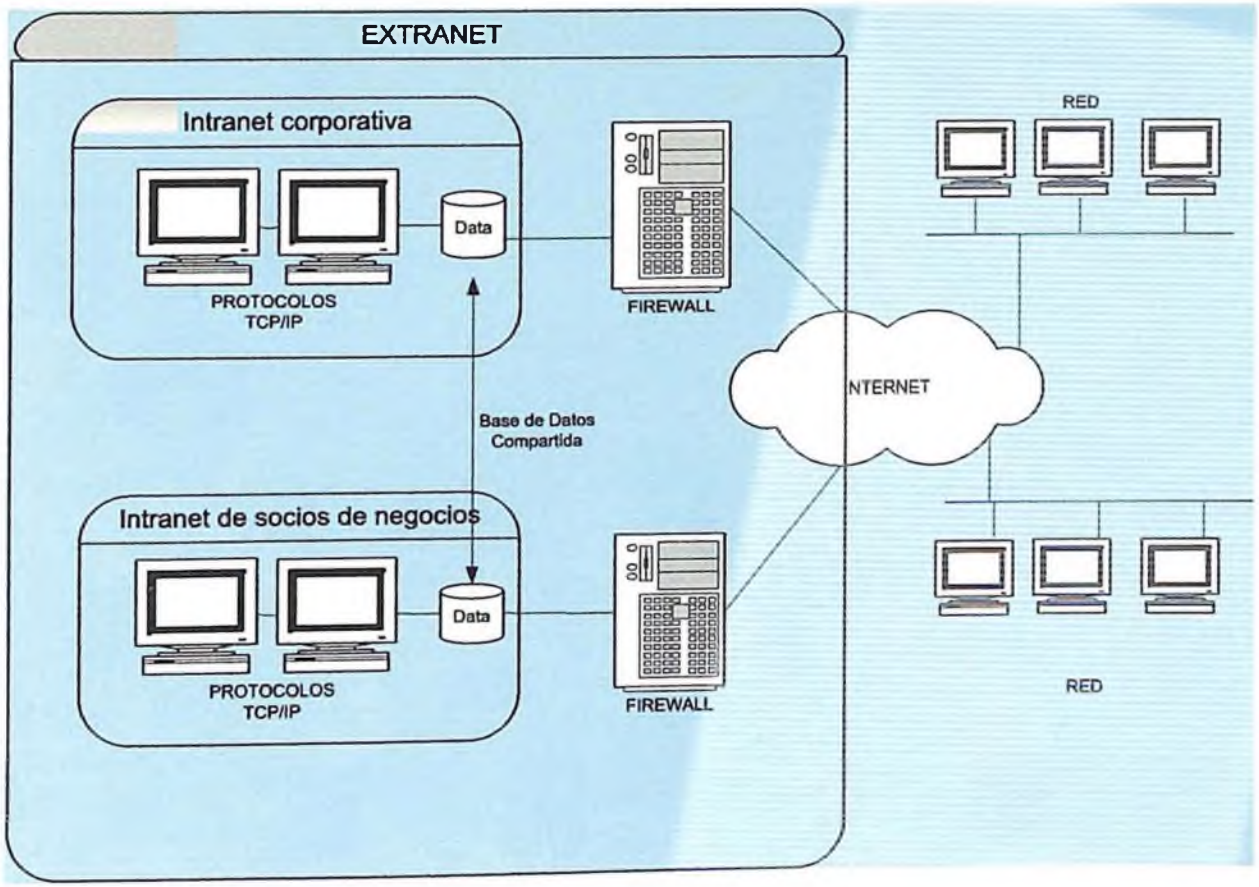


Fig.26 Intranets, Extranets

La Extranet ha surgido como solución (conexión independiente) para preservar la seguridad de la información que guarda la red a través del Internet, conocida como la tercera fase de Internet, cuyo fin es más económico y comercial.

En ese sentido podemos definir a una Extranet como una red comercial creada sobre Internet que enlaza a un grupo privado de usuarios formado por distintas organizaciones, de modo que comparten una serie de objetivos, generalmente económicos, y que de alguna manera nace como solución a la rápida evolución del comercio electrónico. En la figura No.27 se presenta una Extranet en VPN.

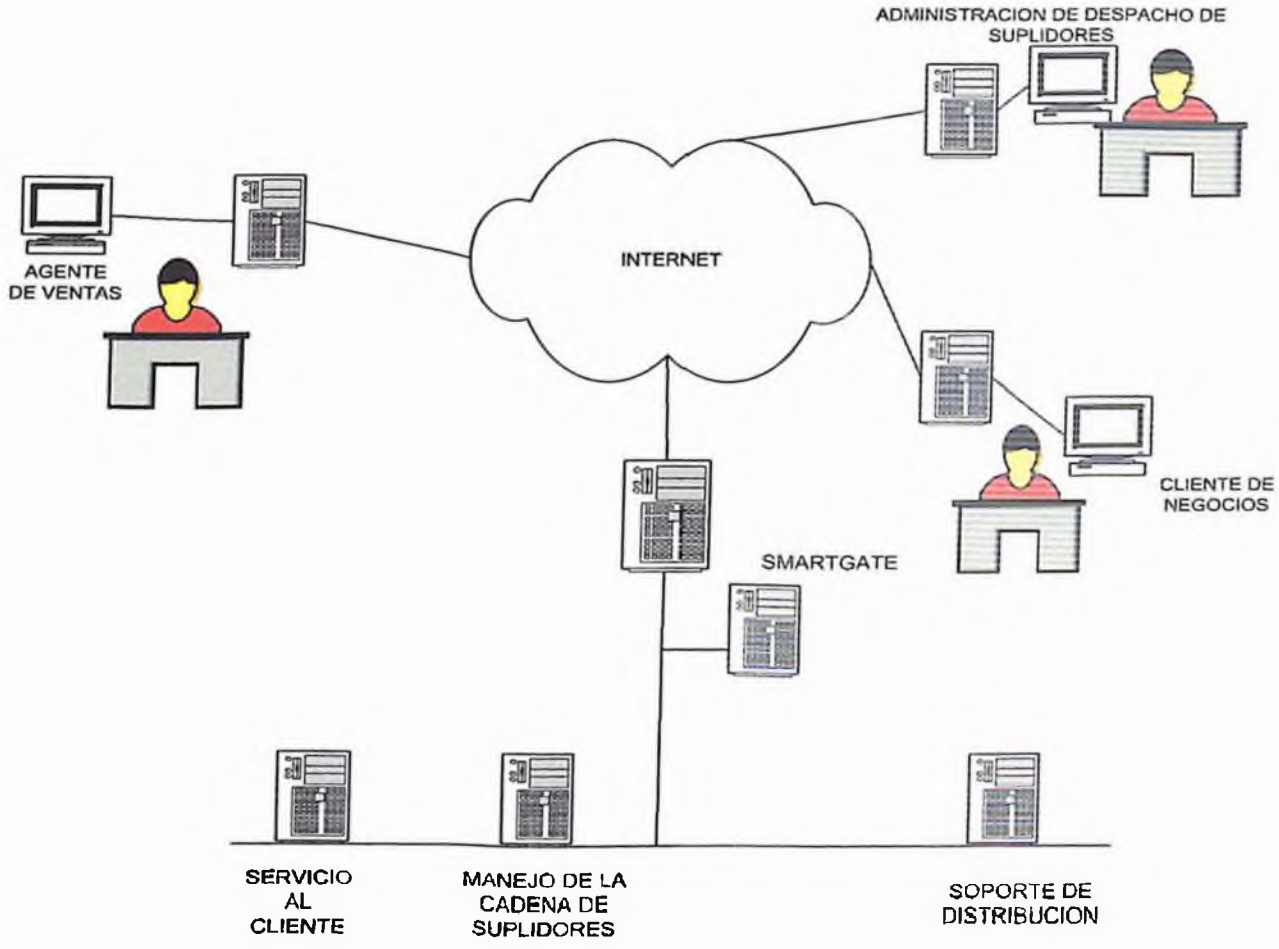


***Figura No. 27 Ejemplo** de una Extranet VPN*

3.2.2 Intranet VPN.

Permite a las redes privadas extenderse a través del Internet u otro servicio público de red en una forma segura.

La Intranet tiene como beneficio el ahorro de dinero sustituyendo la conexión de línea arrendadas por las conexiones locales de ISP .

La VPN permite a la Intranet privada ser extendida a través de Internet, facilitando así el comercio seguro en línea y conexiones Extranet con socios de negocios, suplidores y clientes (Ver figura No.28).

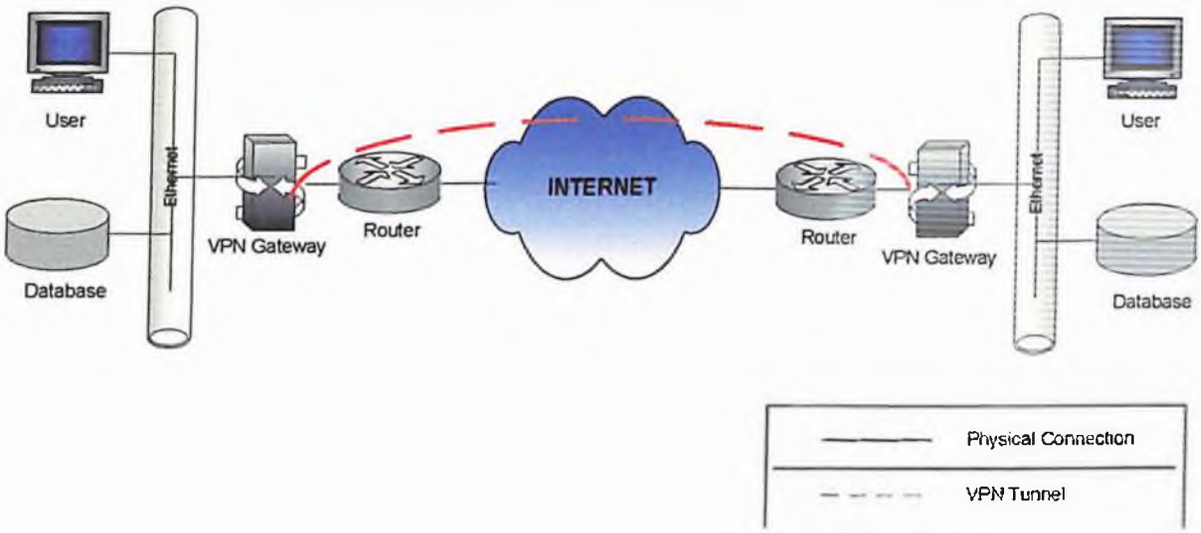


Figura No.28. Ejemplo del funcionamiento de una Intranet VPN

3.2.3 Acceso Remoto (Usuarios Móviles).

Una conexión VPN de acceso remoto la hace un cliente fuera de la empresa, desde una computadora personal conectándose a través de una red privada. El servidor VPN proporciona acceso a los recursos del servidor VPN o a la red completa a la cual está conectada el servidor VPN. Los paquetes (packets) enviados desde el cliente remoto a través de la conexión VPN se originan en la computadora cliente de acceso remoto según se puede apreciar en la figura No.30.

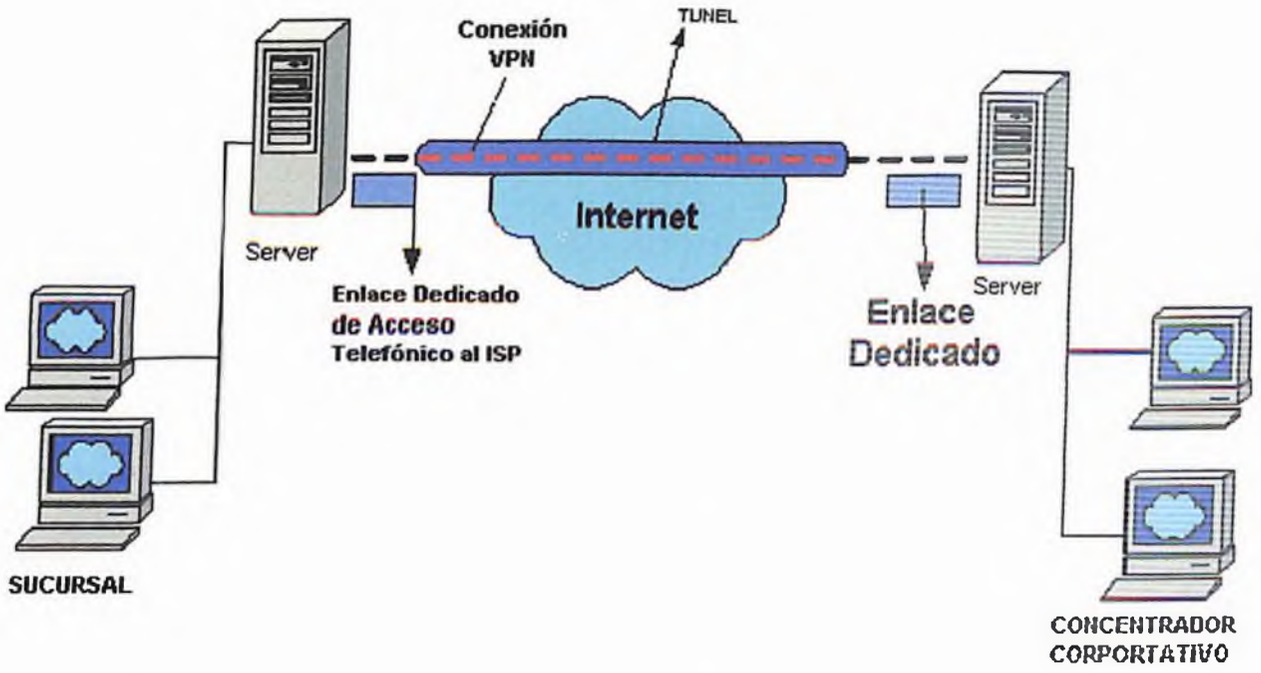


Fig.29. Una conexión VPN conectando dos sitios remotos a través de Internet

Con las conexiones VPN los usuarios que trabajan en casa o de manera móvil, pueden tener una conexión de acceso remoto a un servidor de la organización utilizando infraestructura proporcionada por una red pública como Internet.

En lugar de que un cliente de acceso remoto tenga que hacer una llamada de larga distancia a un servidor de acceso remoto de redes (Network Access Server, NAS), corporativo o contratado, el cliente puede llamar a un ISP local. Al utilizar la conexión física establecida con el ISP local, el cliente de acceso remoto inicia una conexión a través de Internet hacia el servidor VPN de la organización. Una vez que la conexión VPN es creada, el cliente de acceso remoto tiene acceso a los recursos de la Intranet privada (tal y como se muestra en la figura No.30).

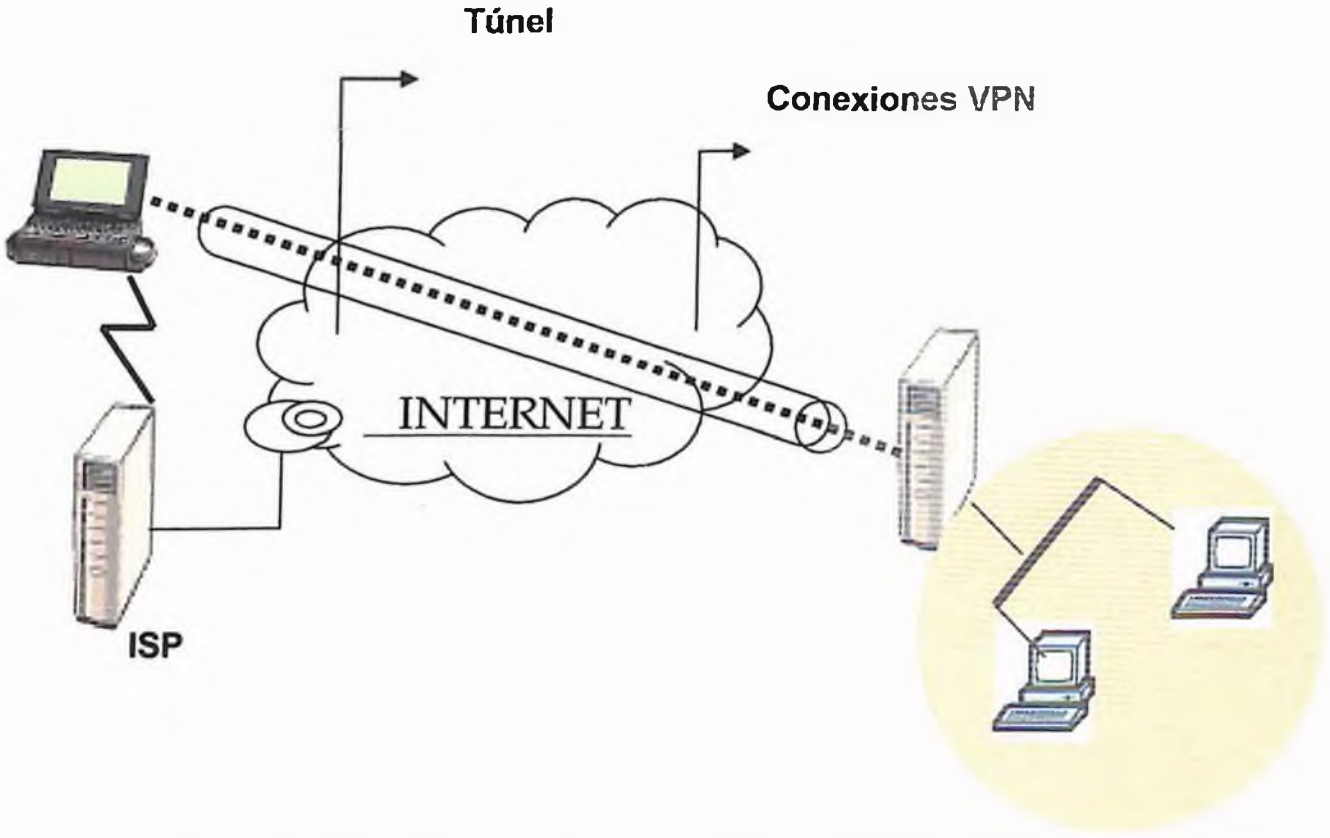


Figura No.30. Conexión VPN conectando un cliente remoto con una intranet privada.

3.2.4 Redes Corporativas (Site to Site).

Las nuevas modalidades de trabajo han creado una creciente demanda para el teletrabajo. Existen dos modalidades principales: la primera es la necesidad de acceder a una red corporativa desde el exterior (ya sea directamente o a través de Internet). La segunda es la posibilidad de acceder a datos y sistemas locales desde cualquier punto de una red corporativa dentro o fuera de ella, (ver figura No.31).

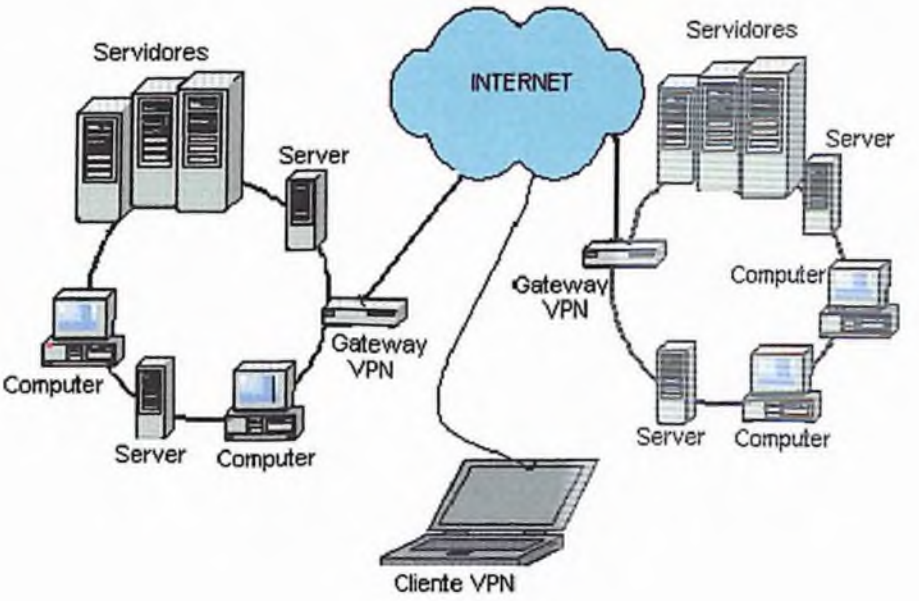


Fig. 31. VPN site to site

Capítulo IV

CASOS PRÁCTICOS DE VPN's EN LA REPÚBLICA DOMINICANA

CAPITULO IV CASOS PRÁCTICOS DE VPN's EN LA REPÚBLICA DOMINICANA

4.1 Las VPN's en la República Dominicana.

Los avances de las VPN en el país en estos momentos están en las manos de las dos empresas líder en las telecomunicaciones Codetel y Tricom, que son las únicas empresas que están autorizadas por los grandes desarrolladores de redes mundiales como Cisco System, Microsoft, entre otras, y éstas a su vez tienen otros vendedores autorizados que pueden vender este tipo de redes a través de sus grandes servidores.

En relación a los avances de las redes de comunicación. El Sr. Manuel E. Bonilla, Ejecutivo de Codetel; declara a la Revista Mercado, lo siguiente:

"Es muy posible que la década de los 90 sea recordada como el decenio en que tuvieron lugar la más profundas transformaciones relacionadas con las telecomunicaciones en toda la historia".

"...Todo nuestro desarrollo en este aspecto tiene que ver con las redes de telecomunicaciones de larga distancia que van a unir, ya sea por satélite, por cable de fibra óptica o por cable de cobre a todos los puntos del país con cualquier parte del mundo" (Revista Mercado, junio 2002, p.26)

En la actualidad la navegación de usuarios en el Internet alcanza unos 602.63 millones a nivel mundial y más de 25 millones en América Latina (donde se enmarca la República Dominicana), y en este aumento desmedido de usuarios donde las redes privadas intervienen reguardando las informaciones que viajan a través de las redes públicas, que es donde verdaderamente se puede colocar el servicio de las Redes Privadas Virtuales (VPN), que vienen a proteger de una forma extremadamente segura esa informaciones que viajan de un sitio a otro y que son confidenciales o que simplemente quien la envía no quiere que sea de uso público o que cualquier intruso trate de penetrar a ella.

El comercio mundial por Internet estima tener un alcance de casi $700 mil millones de dólares para el presente año, con el fin de señalar la gran diferencia en relación a años anteriores, cuando apenas en el año 1998 este comercio alcanzó sólo $32,000.00 mil millones de dólares, crecimiento que aumenta con grandes márgenes para este año (2003), según un estudio realizado por la International Data Cortporation y claro la República Dominicana también juega su rol como país que esta siguiendo los pasos a los avances tecnológicos mundiales del presente milenio.

Codetel como empresa líder en comunicación en República Dominicana, es la empresa que introduce por primera vez la tecnología de Internet en el país, esto lo hace a través del Centro de Operaciones de la Red (COR), a partir de ese momento esta compañía pone a servicio de todos los dominicanos el "servicio de Internet" y en especial para el sector empresarial.

La entrada de Codetel a Internet la mayor red de computadoras del mundo, trajo significativos aportes a la sociedad dominicana.

República Dominicana es actualmente uno de los países latinoamericanos número uno en el área de telecomunicaciones, gracias a las grandes inversiones de sus principales compañías de telecomunicaciones, es razón por la que los servicios de Extranet buscan ayudar a los clientes a evaluar de manera rápida y económica desde su propia PC, las ofertas de los distintos distribuidores ganando transacciones, ya que el cliente interviene de manera más activa, en la operación de venta; por lo que las Extranet son consideradas suficientemente flexibles, escalables, portables y extensibles reduciendo e incluso eliminando las barreras que supone trabajar a través de distintas organizaciones.

Indudablemente las VPN incorporan una solución práctica, para los ejecutivos de negocios y para las sucursales de una empresa o corporación, que necesitan de intercambio de información relevante. En general, sus aplicaciones van desde acceso remoto, hasta la ejecución de los conceptos de autenticar los usuarios y sistemas, empleo de algoritmo de encriptación según lo necesario y transporte IP seguro IPsec.

Hoy el comercio electrónico negocio-negocio, empresa-consumidor es la forma más común de expresarse y comunicarse en los contextos tecnológicos. Toda empresa o corporación tiene como fin incorporarse a la ola de los negocios y, para ello se deben enfocar hacia lo que se ha llamado el proceso de "transformación o globalización".

Debido al auge de la comunicaciones a través de Internet, las compañía se están decidiendo por realizar sus transacciones sobre redes públicas consiguiendo de este modo un ahorro en los costos. La principal solución utilizada hasta el momento en el establecimiento de redes privadas virtuales (VPN's) es que consiguen confidencialidad en las comunicaciones sobre un canal público gracias a los protocolos IPSec(1) e IKE(6).

Una de las grandes posibilidades de la World Wide Web es que posibilita a las organizaciones a ser protagonista en los mercados globales, apuntando a sus compradores e interactuando directamente con ellos y los proveedores; sin importar su ubicación geográfica. No importa el lugar del mundo donde se encuentre el usuario, los negocios son una realidad a través de este medio virtual.

Llegados a este punto es donde las Redes Virtuales Privadas (VPN's) hacean su mayor aporte, ya que juegan un papel protagónico, ofreciendo a quienes buscan incorporarse al comercio electrónico un ambiente seguro y eficaz. Otro de los grandes aportes que ofrecen las VPN's es que se adecuan a las necesidades de toda empresa, sin importar cual sea su tamaño, implementando una solución a la medida y convirtiéndola en un modelo costo-eficiencia para el comercio electrónico y la interacción con sucursales remotas.

No cabe duda que el mayor aporte de las VPN's es la seguridad más allá de un firewall, entendiendo que éste actúa como un protector bajo reglas de negocios y políticas de acceso a las redes corporativas.

Seis posibles razones por las cuales usar una VPN, informaciones presentadas por Codetel, en el marco de uno de los seminarios ofrecido por esta empresa al personal de venta de este tipo de tecnología.

4.2 ¿Porqué usar una VPN?

- Ahorro considerables en las facturas telefónicas de larga distancia
- Buena seguridad en integridad de la data
- Menos equipos que comprar para conectarse a la red
- Fácil mantenimiento a los equipos de acceso remoto.
- Los usuarios pueden usar varios tipos de servicios de mercado.
- Facilidad para añadir usuarios a las VPN's

Codetel ofrece al público una serie de consideraciones para las Redes Privadas Virtuales (VPN's) debido al alto grado de seguridad que oferta especialmente para las entidades bancarias nacionales como es el manejo de las informaciones de las tarjetas de créditos y los acceso a sitio de negocios.

En estos momentos los usuarios dominicanos en general tienen acceso a los siguientes servicios, en los cuales las VPN's ofrecen su máxima seguridad en las informaciones utilizadas, estos son:

4.3 Caso Codetel.

Ofrece la aplicación de filtro de contenido, exclusivo de *Codetel,* que es un programa que permite administrar el acceso de los niños a páginas no deseadas en Internet, bloqueando más de 40 páginas o direcciones, el cual se puede bajar de la dirección www.codetel.net.do/fltrodecontenido que utilizan las técnicas de autenticación de VPN.

4.4 Caso Banco Mercantil.

Presenta merca@net del Banco *Mercantil* donde usted puede hacer toda las transacciones bancarias a través de la red y claro son informaciones que necesitan de autenticación y encriptación de datos cuya seguridad sólo es garantizable a través de las Redes Privadas Virtuales (VPN's).

4.6 Caso Banco Popular.

El Banco Popular en soluciones financieras en línea donde al igual que en la demás entidades bancarias usted puede realizar todas sus transacciones bancarias en su PC, o celular, además de los métodos tradicionales.

4.7 Caso Tricom.

Tricom considerada como la segunda empresa líder en telecomunicaciones en República Dominicana, juega gran papel en el los avances de las VPN's en el país, por lo que cuenta con los equipos y el personal necesario para el desarrollo de esta nueva tecnología de redes.

La Figura No.32 es una muestra de la forma en que Tricom ilustra una Red Privada Virtual Corporativa en territorio dominicano.

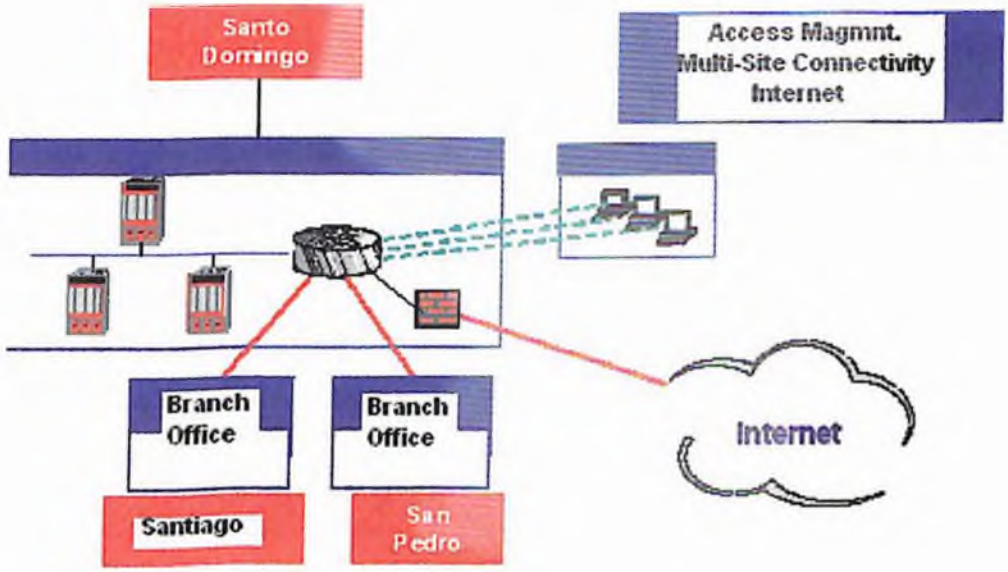


Fig.32. Ilustración de Tricom, sobre VPN

En la actualidad esta empresa se considera pionera en los siguientes avances tecnológicos sobre redes:

a) En instalar un nodo de Internet en R.D. www.tricom.net

b) Desarrollar un portal de comercio electrónico, que es donde verdaderamente las VPN juegan su papel, El proteger los datos comerciales que viajan a través de la red.

c) Desarrollar una red nacional de acceso vía satélite a Internet.

d) En ofrecer el servicio de oficina virtual.

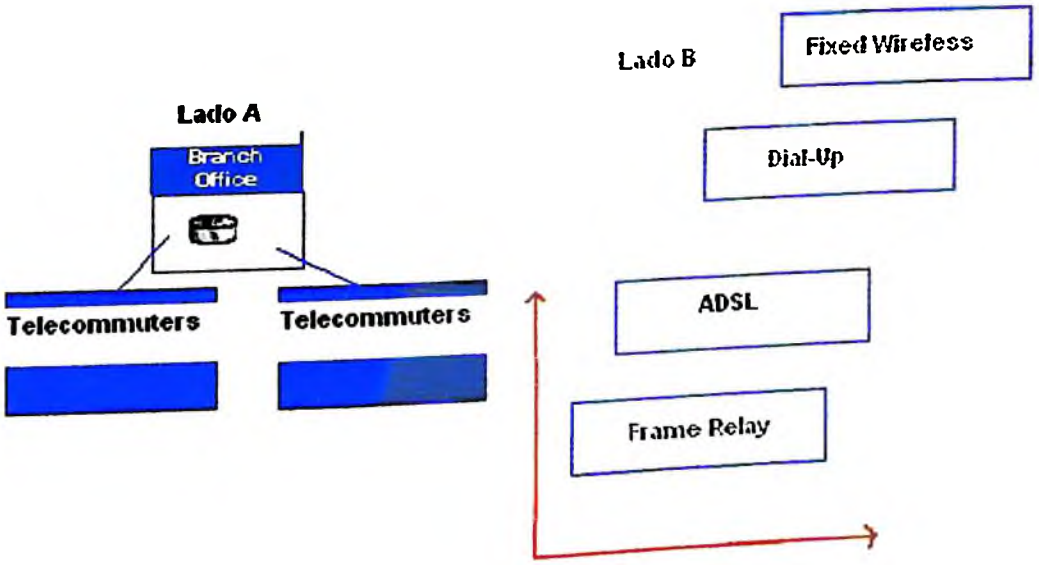


Fig 33. Una VPN de acceso universal mostrado en el lado A de la figura, y una VPN independiente del medio de acceso, mostrado en el lado B de la figura.

Los planes presentados por Tricom en la actualidad de Redes Privadas Virtuales:

1. Plan VPN de Línea Dedicada / ADSL / Frame Relay
2. Plan VPN Dial Up (con acceso a Internet).

4.8 Caso VPN con PPC2002.

La VPN, es una Extranet, es decir, una mezcla entre Internet e Intranet, que sirve para definir una red privada virtual que utiliza a Internet como medio de transporte de la información entre sus propios nodos.

La utilidad de esto, es increíble, se puede acceder a la información del ordenador tanto de la empresa como al de la casa, desde cualquier parte del mundo, al costo de una llamada a Internet, en la mayoría de los casos una llamada local.

Usando el cliente de Terminal Server que trae incorporado el Ipaq, y la posibilidad de conectar a una VPN, con el protocolo de punto a punto que trae también el Ipaq, aunque esta mejor dicho, el PPC 2002.

Hay un problema añadido: la empresa conecta a Internet mediante una línea ADSL, conectada a un router 3COM 812; el primer inconveniente a superar.

4.8.1 La VPN.

El router está configurado en multipuesto, esto es que cada uno de los equipos que están conectados al router (cinco en este caso) se conectan a el de forma directa, sin pasar por ningún servidor proxy, ni ningún firewalls. Es el propio router quien hace de firewalls.

Para que todo esto funcione, hay que hacer NAT (Traducción de Direcciones de Red) de forma correcta, esto es: el router tiene una dirección publica única, la dirección con la que vamos a intentar conectar desde cualquier parte a través de Internet. (Ver figura 37 y 38) para las configuraciones de acceso remoto, y permitir modificaciones de un site remoto. Para permitir la conexión a cualquier equipo de la empresa, cada uno debería de tener una dirección publica única (una línea por cada equipo). Como todos conectan a través del router, es este quien tiene la dirección pública. Los equipos están configurados en una pequeña red, cada uno con su dirección privada, es decir, la que el administrador le ha asignado dentro de la red de la empresa (ver figura No. 34).

Fig. 34. Administrador remoto de conexión a oficina

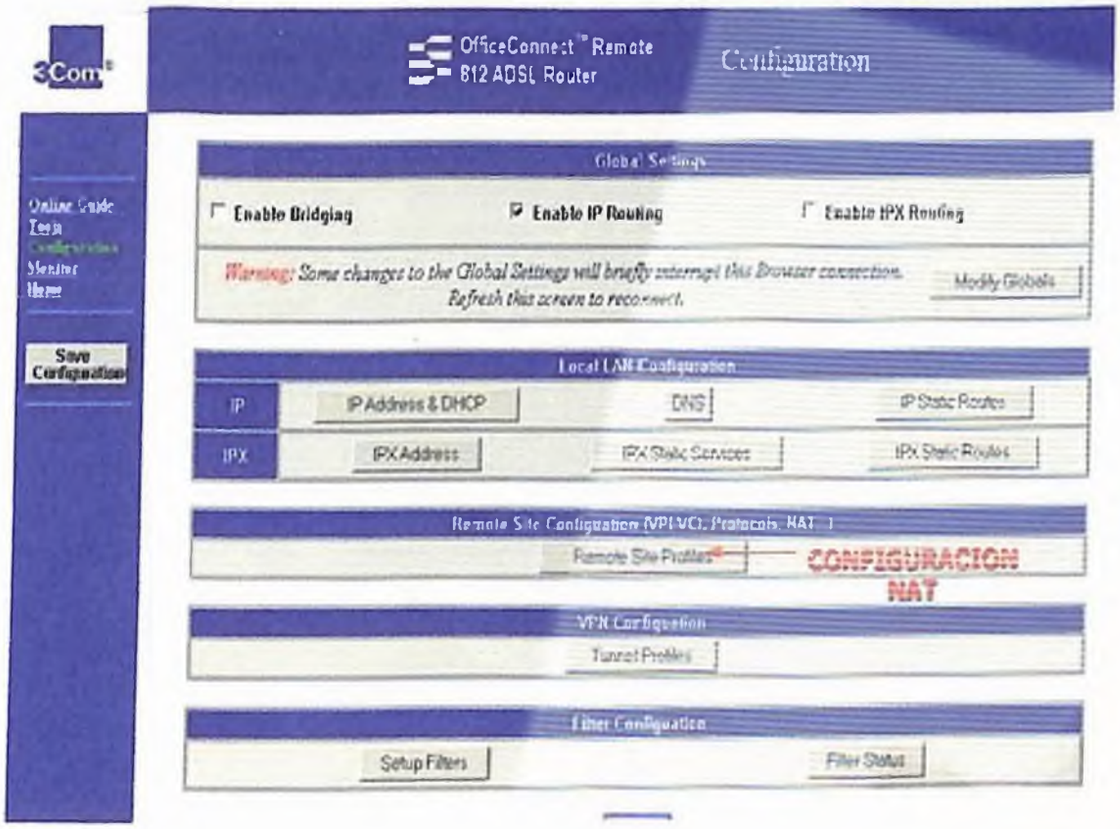


Fig.35. Configurando el NAT

El NAT, traduce la direcciones IP pública y los números de puerto TCP/IP de los paquetes que se reenvían entre Internet y la red privada a una dirección IP privada, se configura como se muestra en la figura 35.

En el caso que nos ocupa, comunicamos los datos de los puertos 47 y 1723 a la dirección privada en el servidor. (Ver figura 39).

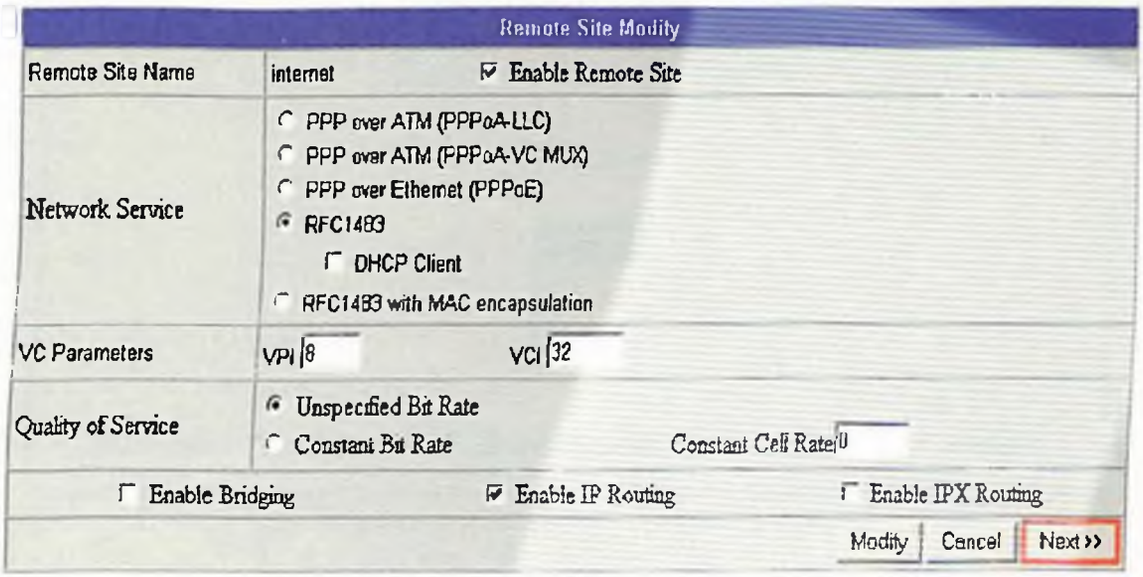


Fig.37. Pantalla para configurar la opción de modificar desde un site remoto.

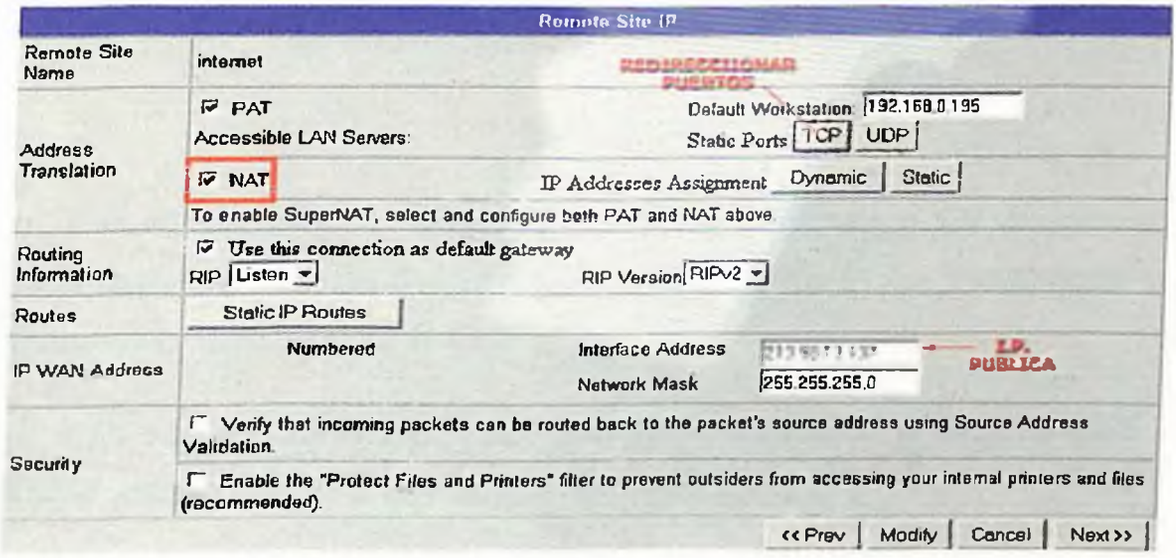


Fig.38. Pantalla para introducir el Ip del site remoto

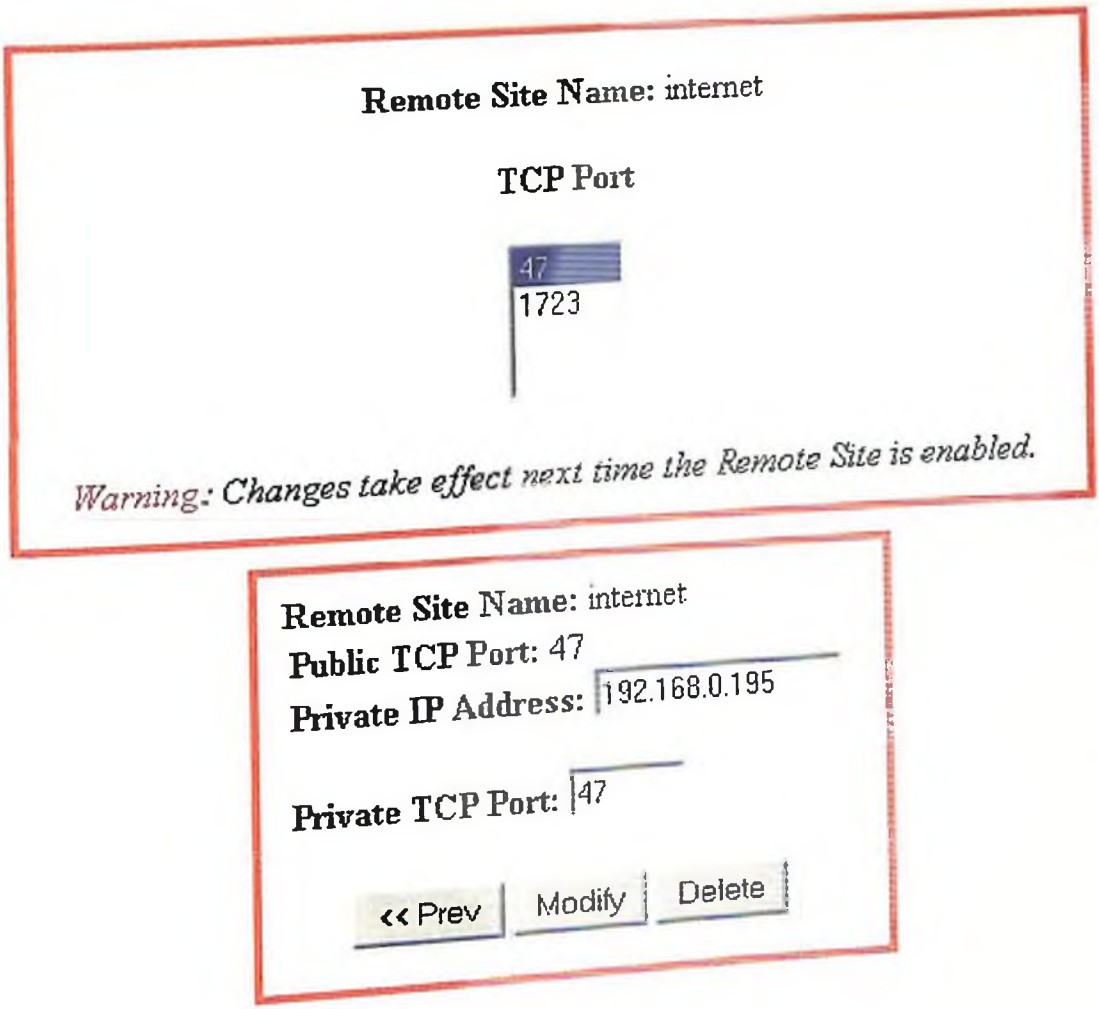


Figura No. 39

Por simplicidad, en esta red, no se ha configurado los equipos como clientes DHCP, si no, que tiene asignada una dirección IP fija. Tampoco se tiene configurado ningún servidor DNS.

Una vez realizado esto, configuramos e instalamos el servidor para que acepte el acceso remoto a través de la VPN (ver figura 37).

Para ello vamos a inicio: programas: herramientas administrativas: enrutamiento y acceso remoto. Pinchamos en el nombre del servidor, con el botón derecha, y seleccionamos: configurar y habilitar el enrutamiento y acceso remoto. Seleccionamos la opción de conexión VPN, y configuramos según necesidades, según se ilustra en la figura No. 40.

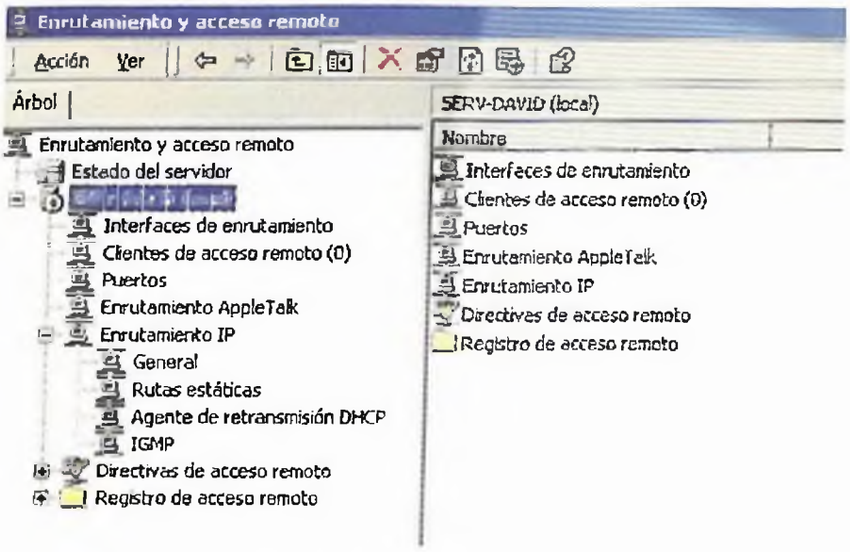


Fig.40. Configuración y habilitación del enrutamiento remoto

El router que utilizamos en cuestión, tiene en su versión de Firmware 2.1, una sección llamada "Túnel Profiles" que simplifica bastante la configuración.

Si se presenta algún problema para hacer funcionar el cliente de la PPC de Terminal Server, y no se posee esta versión del Firmware, seria aconsejable que se abra en el router, el puerto que utiliza el servicio de Terminal Server (3389) .

4.8.2 El PPC, (Ipaq 3870).

En nuestro caso vamos a utilizar y configurar para la VPN, el protocolo punto a punto de los PPC´s.

Primero, configuramos una conexión a Internet. (Ver pantalla de la figura no. 41). Es realmente útil la posibilidad de poder tener diferentes configuraciones para cada tipo de conexión, en una lista, y sólo tener que seleccionar la mas idónea en cada caso, de la lista, y picar en conectar. De esta forma tenemos configuradas conexiones para cuando lo hago a través del T68i, con el bluetooth, para la base de sincronización USB, para el MODEM de sobremesa con un cable Null-Modem.

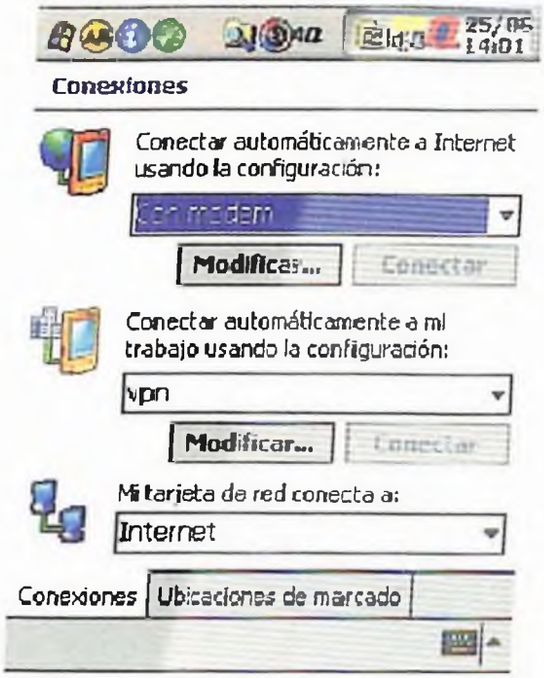


Fig.41. Configuración de conexión a internet

En el caso que nos ocupa, hay configurada una conexión dial up, que se realiza por el MODEM, un CF MODEM de Compaq, de 56K.

Una vez que tenemos la cuenta, tenemos que crear una conexión nueva el "Conectar automáticamente a mi trabajo usando la configuración:", en este caso la llamamos VPN, lo único que tenemos que hacer es dar clic en la pestaña de VPN y poner la dirección pública de nuestro router. (Ver figura 42)

4.9 Caso Remesas Vimenca.

Enlace Cliente-Red: Usa el cliente PPTP y L2TP para acceder tienen un equipo de seguridad marca Cisco modelo Pix 506E Enhanced. Este equipo es el firewall de las conexiones a internet utilizadas para los servicios de Proxy y de Email-Server y además es el VPN Gateway por el que accesan los funcionarios de alto nivel, desde sus casas para trabajo de oficina, o cuando se encuentran de viaje y también el personal que da soporte técnico, debido a que esta empresa labora 24 horas por su naturaleza de remesadora, de banco y de cadena de centro de llamadas y a su vez sirve de enlace de backup a Western Union por la eventualidad de que la línea dedicada que los conecta salga de servicio.

4.10 Caso Distribuidora Corripio.

Enlace Cliente-Red: Tiene una red VPN Wireless Móvil, cuyo gateway es un servidor windows 2000 server con una conexión a internet wireless y los clientes (vendedores móviles) son PDA's Compaq Ipaq PCC2000. Los clientes accesan a una base de datos donde colocan sus órdenes de compras, verifican disponibilidad de inventario y actualizaciones de precio y oferta, realizan cotizaciones. Estos vendedores no tienen la necesidad de pasar por la oficina a realizar ninguna de estas labores y la pueden realizar desde la oficina de sus propios clientes, brindando un servicio más profesional, más rápido y más preciso. La empresa a su vez no tiene que disponer de oficinas para este personal, ahorrándose dinero, por el espacio físico por energía, mobiliario de oficina, material gastable, facilidades, de energía alterna, impresoras, scanners, parqueos, etc.

4.11 Caso Viajes Barceló.

Enlace Red-Red: Esta compañía posee una conexión VPN con su matriz en España para eso utiliza como VPN Gateway un equipo marca Cisco, modelo Pix 501 y a su vez le sirve de firewall. Esta conexión se enfrenta a un equipo Cisco VPN 3000 concentrator que es un hardware dedicado, con un software de manejo a través de httpo tel net. Es el mismo equipo de la conexión de la empresa Sadomoco con SAP. Además, permite que los costos bajen mucho porque pagan el costo de una línea ADSL (más o menos RD$4,000.00 mensuales) en vez de una línea dedicada, que de Santo Domingo a España tiene un costo de más de RD$30,000.00; utilizándola también para el acceso a internet de los usuarios internos y de los servicios de email.

4.12 Caso Celso Pérez.

Enlace Red-Red. Tiene una cadena de tiendas en todo el país (Bella Vista Mall, Diamond Mall, Megacentro, Plaza Internacional en Santiago, Plaza Central, Plaza Naco, Unicentro Plaza, etc.). Estas tiendas tienen una línea ADSL con routers Cisco 1710 Bundele (Estos equipos tienen la peculiaridad que tienen más memoria RAM y un módulo integrado de encriptación por hardware, que aumenta su capacidad de conexiones simultáneas ya que no utiliza la capacidad de procesamiento del CPU.

Todas las conexiones se realizan desde cada tienda a la oficina principal en Villa Juana. Esto evita las conexiones Frame Relay cuyo costo mínimo sería alrededor de RD$50,000.00 mensuales contra los RD$4,000.00 mensuales que cuesta la línea ADSL.

4.13 Caso Santo Domingo Motors.

Enlace VPN Compuesto o híbrido: Esta empresa tiene una red VPN híbrida con equipo un router, marca Cisco modelo 1721 con una conexión Frame Relay T1 al internet. Se conecta a la casa matriz de SAP (en Filadelfia) a través de esa conexión. También usa una segunda conexión a la empresa Grupo Ámbar en Puerto Rico y a la vez sirve de VPN Gateway para clientes móviles que son altos funcionarios del grupo que accesan desde su casa, o cuando están de viaje, además del personal de soporte técnico de la empresa.

La conexión con la casa matriz de SAP ha permitido la implementación desarrollo, corrección de fallas incluidas en el contrato de mantenimiento desde la casa matriz, lo que anteriormente le ocasionaba unos gastos por pasajes, alojamiento, dietas y compensaciones al personal corporativo de SAP.

4.14 Caso de Frame Relay como Ahorrar en Costos Aplicando VPN.

AFP Siembra: Actualmente esta empresa consta de una oficina principal, una sucursal en la Romana, una sucursal en La Vega, una Sucursal en Santiago y una en Puerto Plata. Esta compañía enlaza todas las sucursales con su oficina principal a través de líneas Frame Relay a 128 Kbps.

Entonces la renta mensual por concepto de servicio para Frame Relay es de RD$30,000.00, mientras que para la VPN, es de RD$8,000.00. En un año estaríamos hablando de una diferencia de RD$264,000.00.

Para ambas tecnologías: VPN o Frame Relay, se considera apropiado un equipo Firewall CISCO PIX 501 Con licencias para 10 Usuarios 3DES, con un Switch Integrated 4-Port 10/100 and 10/100 Port. Dicho equipo tiene un costo de UD$1,560.00 (PIX-501-BUN-K9) y el (PIX-501-50-BUN-K9 de UD$755.00, cuya labor de instalación, configuración, prueba y puesta en operación de Acceso VPN y seguridad vía Firewall tiene un costo que asciende US$700.00, en total estamos hablando de US$3,099.00 (Precios de lista sujetos a cambio).

PRESUPUESTO IMPLEMENTACION
DE LA TECNOLOGIA FRAME RELAY
AFP Siembra
Septiembre, 2003

Cant.	Detalle	Equipos	Instalación	Manten.
5	Servicio de Interconexión entre los Puntos a 128Kbps: Santo Domingo - Puerto Plata - La Romana - Santiago y La Vega. Costo Mensual			30,000.00
10	Licencias para 10 Usuarios Firewall CISCO PIX 501 Usuarios 3DES, con un Switch Integrated 4 Port 10/100 and 10/100 Port (PIX-501-BUN-K9)		54,600.00	
1	Firewall Cisco PIX-501-50-BUN-K9	26,425.00		
1	Labor de Instalación, Configuración, prueba y puesta en operación de Acceso Frame Relay		45,500.00	
	*Totales	26,425.00	100,100.00	30,000.00

* Estos son precios de listas. Están sujetos a cambios. El equipo Cisco incluye 1 año de garantía del fabricante.

PRESUPUESTO IMPLEMENTACION DE LA TECNOLOGIA VPN

AFP Siembra

Septiembre, 2003

Cant.	Detalle	Equipos	Instalación	Manten.
5	Servicio de Interconexión entre los Puntos ADSL Santo Domingo - La Romana - Santiago - Puerto Plata y La Vega. Costo Mensual			8,000.00
10	Licencias para 10 usuarios Firewall CISCO PIX 501 Usuarios 3DES, con un Switch Integrated 4 Port 10/100 and 10/100 Port (PIX-501-BUN-K9)		54,600.00	
1	Firewall CISCO PIX-501-50-BUN-K9	26,425.00		
1	Labor de Instalación, Configuración, prueba y puesta en operación de Acceso VPN y seguridad via Firewall		24,500.00	
	Totales	**26,425.00**	**79,100.00**	**8,000.00**

* Estos son precios de lista. Están sujetos a cambios. El equipo Cisco incluye 1 año de garantía del fabricante.

Descripción del Equipo: Firewall CISCO PIX 501.

El Firewall Cisco PIX 501 trae seguridad de clase emprendedora para oficinas pequeñas y teletrabajadores, aplicación plug and play. Ideal para asegurar alta velocidad "siempre" entorno de banda ancha, el Firewall Cisco PIX 501, el cual es parte del mercado lidereado por la serie de Firewall Cisco PIX , provee capacidad de seguridad robusta, funciones en redes de oficinas de trabajo pequeñas y un manejo poderoso de capacidades compactos, todo en una solución.

Seguridad de Clase Emprendedora para Ambiente de Oficinas pequeñas.

El Firewall PIX 501 de Cisco está construido para aplicaciones de propósito completo lo cual provee una gran seguridad en los servicios incluyendo una inspección completa de estado de corta fuegos (firewalling), Virtual Private Network (VPN) y protección contra intrusos en un simple dispositivo. Usando el estado de Cisco del arte adoptado de algoritmo de seguridad (Adaptive Security Algorithm, ASA) y el sistema operativo PIX, el PIX 501 asegura que todos los usuarios detrás de él están salvos y seguros de las amenazas que están al acecho en el internet. Es poderosamente segura la inspección de la tecnología del firewall, guarda el rastro de los usuarios autorizados, los requerimientos de la red y previene de acceso desautorizados a la red. Por su acceso flexible y las capacidad de control del PIX 501, los administradores pueden enfocarse en políticas personalizadas en el tráfico de la red a través del Firewall.

El Firewall Cisco PIX 501 también puede asegurar todas las comunicaciones de red desde oficinas remotas a oficinas corporativas a través del Internet usando su llave de intercambio estándar (IKE)/IP capacidad de VPN, (Internet Key Exchange IKE/IP security VPN). Encriptando la data con una encriptación estándar de 56-bit (DES) o una opción avanzada encriptación de 168-bit Triple DES (3DES), ojos fisgones no pueden ver la data sensitiva de la empresa mientras esta viaja de manera segura a través del Internet.

La capacidad integrada de protección de intrusos del PIX 501 puede proteger la red de varias maneras de ataques populares. Buscando sobre 55 maneras diferentes de ataque "firmados," PIX se mantiene con una vigilante mirada a a taques y opcionalmente los bloquea o los notifica en tiempo real.

Empaquetando todas las funciones de seguridad contenidas en el Firewall Cisco high-end gigabit PIX, el PIX 501 provee gran protección que todos los usuarios de banda ancha buscan en una solución fácil de usar y fácil de desplegar.

Sencillo, Oficinas Pequeña de Gran Velocidad.

El Firewall Cisco PIX 501 provee una forma conveniente para múltiples computadoras compartir una misma conexión de banda ancha vía su integrado, alto rendimiento cuatros puertos 10/100 MBbps Switch. Además PIX 501 provee Traducción de Dirección de Red (NAT) y Traducción de Dirección de Puertos (PAT) para ocultar la dirección de dispositivos de red actual. También los usuarios pueden disfrutar del plug and play tomando la ventaja de la configuración del protocolo de Invitado Dinámico (Dinamic Host Configuration Protocol, DHCP) del servidor con PIX, el cual automáticamente asigna a las computadoras direcciones de red cuando están encendidas. El PIX 501 provee las funciones necesarias para integrar la mayoría de ambientes de red de banda ancha.

Robusto Manejo de Capacidades Remotas.

El PIX 501 es confiable, con una plataforma fácil de mantener que provee una amplia variedad de métodos para configurar, monitorear y solucionar problemas. La administración del rango de soluciones PIX desde una integrada, herramienta basada en web a centralizada, herramienta basada en políticas para soportar el protocolo de monitoreo remoto como un Simple Protocolo de Administración de Red (SNMP, Simple Network Management Protocol) y logeo al sistema.

El Administrador de Dispositivos PIX (PDM, PIX Device Manager) provee una intuitiva, interfase basada en web para los administradores fácilmente configurar y monitorear un PIX 501, sin requerir que ningún software (más que un browser de web) esté instalado en la computadora del administrador.

Los administradores también puede configurar, monitorear y resolver problemas del PIX 501 usando su interfase de línea de comando (CLI, command-line interface) a través de una variedad de métodos incluyendo Telnet, Secure Shell (SSH) sin acceso de banda vía el puerto de consola.

Firewall Cisco PIX 501

Caracteristicas	Beneficios
Clase de Seguridad Emprendedora	
Aplicación de Seguridad Real	▪ Usa su propio sistema operativo robusto que elimina los riesgos de seguridad asociados con los sistemas operativos de propósito general
Firewall de Inspección de Estado	▪ Provee un perímetro de seguridad en la red para prevenir los accesos desautorizados a la red ▪ Usa el estado de el arte de Algoritmo de Adaptación Seguridad (ASA) para un estado del firewall para la inspección de servicios. ▪ Provee capacidad de acceso-control flexible para más de 105 aplicaciones, servicios y protocolos predefinidos, con la habilidad de definir aplicaciones y servicios personalizados. ▪ Incluye numerosas aplicaciones-precavidas de "reparo" que aseguran un avanzado protocolo de red como H.323, SIP, Skinny, RTSP y más. ▪ Incluye contenido de filtro para aplicaciones Java applets y Active X control.
VPN	▪ Soporta los estándares IKE además del Ipsec VPN. ▪ Asegura la privacidad/integridad de la data y una robusta autenticación para las redes remotas sobre el Internet. ▪ Soporta 56-bits DES y 168-bit 3DES encriptación de data para asegurar la privacidad.
Protección de Intrusos	▪ Provee protección para más de 55 tipos diferentes de ataques basados en redes de telecomunicación que van desde paquetes mal formados a ataque de denegación de servicios (denial-of-service, DoS attack). ▪ Se integra con el Cisco Network Intrusión ▪ Sensores de Detección de Sistema (IDS) para la habilidad de dinámicamente bloquear/rescatar los nodos de red hostiles vía el firewall
AAA Support	▪ Integrado con la autenticación popular, autorización y contabilización se servicios vía TACACS+ y soporte de RADIUS
Certificado X.509 y soporte CRL	▪ Suporta SCEP-basado en el protocolo de las soluciones líderes X.509 de Baltimore, Entrust, Microsoft y Veri Sign
Integración con las soluciones líderes de Terceras-Fiestas	▪ Soporta el rango de banda de CISCO AVVID (Arquitectura para Voz, Vídeo y Data integrada) solución que provee filtro de URL, filtro de contenido, protección de virus, administración remota escalable, y más.
La seguridad de un Slot para candado integrado	▪ Provee la capacidad de asegurar físicamente el PIX 501 usando un candado standard de seguridad de cable (el candado no está incluido)
Redes Robustas para pequeñas	**Oficinas**
Switch integrado de 4 puertos 10/100	▪ Provee un conveniente ambiente de alta velocidad para entornos de oficina pequeña en una plataforma simple y compacta. ▪ El soporte de Auto-MDIX elimina la necesidad de atravesar cables con los dispositivos conectador al Switch.
DHCP Cliente y Servidor	▪ Obtiene dirección IP automáticamente para la interfase del firewall del proveedor de servicios. ▪ Provee direcciones IP a los dispositivos dentro de la red del firewall
Soporte de NAT/PAT	▪ Provee la habilidad de traducir direcciones de red dinámicas/estáticas (NAT) y traducir de direcciones de puertos (PAT) ▪ Permite a múltiples usuarios compartir una conexión de banda ancha usando una simple dirección IP pública.

Características	Beneficio
PPPoE (Disponible Q1 2002)	▪ Asegura la compatibilidad con las redes que requieren PPP o Ethernet (PPPoE)
Gran Capacidad de Administración	
Administrador de Dispositivo PIX (PDM)	▪ Basado en la intuitiva web GUI, permite de manera simple, administración remota y segura de los Firewalls PIX ▪ Provee un amplio rango informativo, en tiempo real, y reportes históricos con los cuales dan una vista a las tendencias usadas, el rendimiento, y los eventos de seguridad.
Soportado por el Cisco Secure Policy Manager (CSPM)	▪ Provee escalabilidad, administración consistente de toda la línea de productos Firewall Cisco PIX y desempeño usando la infraestructura de políticas de CSPM.
Cisco PIX CLI	▪ Permite a los clientes usar los conocimiento previos de PIX CLI para una fácil instalación y administración sin entrenamiento adicional. ▪ Accesibilidad a través de la variedad de métodos incluyendo puertos de consola, Telnet y SSH.
Soporte de SNMP y de syslog	▪ Provee capacidad de monitoreo remoto y de identificación, con una integración en el Cisco y las aplicaciones de administración de tercera fiesta. (Third-party management applications).

Cuadro No.3. Principales características del Firewall Cisco PIX 501

Licencias de Software:

Licencia de 10 Usuarios

La licencia de 10 Usuarios del Firewall Cisco PIX 501, soporta hasta 10 concurrentes direcciones IP fuentes desde la red interna para atravesar el PIX 501. El servidor integrado DHCP soporta hasta 32 DHCP.

Licencia de 50 Usuarios

La licencia de 50 Usuarios del Firewall Cisco PIX 501, soporta hasta 50 concurrentes direcciones IP fuentes desde la red interna para atravesar el PIX 501. El servidor integrado DHCP soporta hasta 128 DHCP. Según las necesidades crecen, de 10 a 50 usuarios hay una licencia de actualización (upgrade) disponible, lo cual permite extender la inversión los equipos PIX501.

Las licencias 3DES y DES

El PIX 501 tienes dos licencias opcionales de encriptación (168-bit 3DES y de 56-bit DES) disponible en a cualquier momento de hacer la orden, o como una licencia de actualización que puede ser comprada luego. Las restricciones de los Estados Unidos pudieran aplicar a estas licencias.

Sumario de Rendimiento

56-bit DES IPsec VPN : 6 Mbps

168-bit 3DES Ipsec VPN: 3 Mbps

Simultáneo VPN: 5*

* Número máximo de asociaciones simultáneas seguras VPN/IKE (VPN/IKE Security Associations, SAS supported)

Especificaciones Técnicas:

Procesador: Procesador 133-MHZ AMD SC520

RAM: 16 MB of SDRAM

Memoria Flash: 8 MB

Sistema de Bus: Simple de 32-bit, 33-MHZ PCI

Rango de Ambiente de Operación

Temperatura: 32 a 104° F (0 a 40° C)

Humedad Relativa: 10 a 90%, noncodensing

Altitud: 0 a 6500 pies (2000 m)

Shock: 250 G, < 2 ms

Vibración: 0.41 Grms2 (3-500 Hz) entrada aleatoria

4.15 Costos Implementación de VPN y Frame Relay, para la Universidad de la Tercera Edad (UTE).

Para enlazar los tres Centros Regionales de la UTE, con el Recinto Principal, viendo la necesidad de Expansión y Desarrollo que tiene esta Alta Casa de Estudios, que provee un gran apoyo a su metodología andragógica, donde las clases son una vez a la semana, y se está trabajando en la implementación del método de clases a distancia..

Usando el Firewall Cisco PIX 501, con un costo de UD$755.00.00* con licencia D para 10- Usuarios, más la instalación con un costo de UD$700.00* para un total de UD$1,455.00*., para la tecnología VPN. Más el mantenimiento mensual que asciende a la suma de RD$6,400.00.

Sin embargo, resulta mucho más costosa la tecnología Frame Relay, utilizando el mismo Firewall de Cisco con un costo de UD$755.00* con licencia D, para 10- Usuarios, más los costos de instalación que ascieden a UD$1,300.00*. Esto sin considerar el mantenimiento mensual que asciende a RD$24,000.00.

*Para fines de presupuesto se unificó la moneda considerando la tasa del dólar a RD$35.00 x UD$1.00,

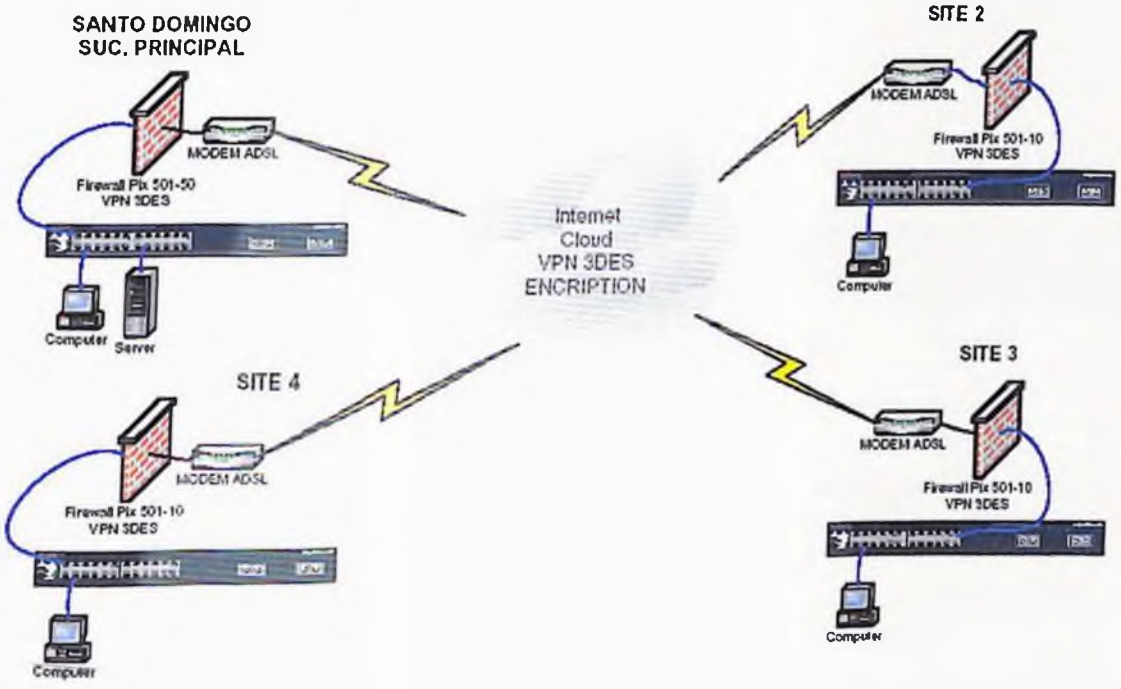
PRESUPUESTO IMPLEMENTACION DE LA TECNOLOGIA FRAME RELAY UTE

Septiembre, 2003

Cant.	Detalle	Equipos	Instalación	Manten.
4	Servicio de Interconexión entre los Puntos a 128Kbps: Santo Domingo - Zona Oriental - Barahona - Santiago Costo Mensual			24,000.00
1	Firewall CISCO PIX-501-50-BUN-K9	26,425.00		
1	Labor de Instalación, Configuración, prueba y puesta en operación de Acceso Frame Relay		45,500.00	
	Totales	**26,425.00**	**45,500.00**	**24,000.00**

* Estos son precios de lista. Están sujetos a cambios. El equipo Cisco incluye 1 año de garantía del fabricante.

DIAGRAMA VIRTUAL PRIVATE NETWORK (VPN) - 3DES
4 LOCALIDADES UNIVERSIDAD DE LA TERCERA EDAD



PRESUPUESTO IMPLEMENTACION
DE LA TECNOLOGIA VPN
UTE
Septiembre, 2003

Cant.	Detalle	Equipos	Instalación	Manten.
4	Servicio de Interconexión entre los Puntos ADSL Santo Domingo - Barahona - Santiago - Zona Oriental Costo Mensual			6,400.00
1	Firewall CISCO PIX-501-50-BUN-K9	26,425.00		
1	Labor de Instalación, Configuración, prueba y puesta en operación de Acceso VPN y seguridad via Firewall		24,500.00	
	Totales	**26,425.00**	**24,500.00**	**6,400.00**

* *Estos son precios de lista. Están sujetos a cambios. El equipo Cisco incluye 1 año de garantía del fabricante.*

CONCLUSIÓN

CONCLUSIÓN

Este proyecto ha sido desarrollado con la finalidad de analizar las pautas básicas basadas en el análisis de la Implementación y Desempeños de la tecnología de ***Redes Privadas Virtuales (VPN)***, en ambiente Windows, en la República Dominicana como solución para asegurar la información que navega a través del Internet (acceso seguro), reducción de costos, su aplicación, aportes, avances, etc..

Como resultado de las investigaciones realizadas se demuestra que esta tecnología ofrece a las empresas múltiples beneficios y ventajas. Las Redes Privadas Virtuales poseen la característica principal de ofrecer soluciones a gran parte de la necesidad de comunicación, proporcionando a las empresas diversas fórmulas para obtener un ahorro sustancial e inmediato de las conexiones remotas, aprovechando la infraestructura de red de servicios de los proveedores de acceso a Internet, todo a muy bajo costo, de fácil implementación y obteniendo un gran desempeño.

Los diferentes protocolos que utilizan la Redes Privadas Virtuales, especialmente los que la utilizan para ofrecer un alto nivel de seguridad, se podría decir que es su gran fuerte, lo que logra especialmente en la técnica de encriptación y autenticación de los datos que viajan por la red pública de Internet, haciendo que esta información se convierta en privada y que la misma sólo pueda ser leída por la persona a quien es dirigida y que para los intrusos y piratas del Internet sólo apareciera como un código de máquina imposible de descodificar al menos que se posea la llave autorizada.

He planteado lo que son las consideraciones de diseño de una VPN, lo que el diseñador de red debe saber, cuál es la necesidad real de la organización, seguridad de la información que va a viajar por la red pública para que no sufra ninguna alteración por persona no autorizada. Sin duda alguna la tecnología de red ha contribuido de una manera importante en el desarrollo de sociedad actual especialmente en el campo de las telecomunicaciones.

Las VPN's tienen garantizado un gran número de usuarios, es una tecnología que aporta grandes niveles de seguridad, además de aportar la movilidad.

Las VPN's son imprescindibles en la República Dominicana, y es fácil llegar a esta conclusión sólo hay que pensar en la muestra de casos citados en el capítulo IV este trabajo, que son grandes y medianas empresas que actualmente explotan los beneficios de ésta maravillosa tecnología, y hacerse la pregunta que sería del Banco Mercantil, del Banco Popular, de Santo Domingo Motors, Remesas Vimenca, Distribuidora Corripio, Celso Pérez, donde cada vez más la data online se convierte en una necesidad, se requiere de información actualizada al instante, donde el flujo de transacciones bancarias, el gran auge que tienen los servicios bancarios online es vital en el día a día; la movilidad de los gerentes, funcionarios, vendedores, etc. la seguridad con que es tratada la información, el gran desempeño que aportan las VPN's a un costo tan bajo, en comparación con otras tecnologías, sin sacrificar la integridad y seguridad de la data.

BIBLIOGRAFÍA

BIBLIOGRAFÍA

Albáu Muñoz, A. ***Telemática y Redes de Computador.***
Editorial Boixerau, Macombo, S.A. España, 1984.

Black Uyless. ***Redes de Transmisión de Datos y Procesos Distribuidos***
Ediciones Díaz Santos. Madrid, 1987.

Browm, Steven ***Implementing Virtual Network,*** 1999;McGraw Hill.

Chez Checo, J. ***La Telefonía Presencia y Desarrollo en la República Dominicana.*** Impreso Codetel. Rep. Dom., 2000

Grec, K.C.E. ***Introducción a las Redes Locales de Informática Aplicada.***
Editorial Díaz de Santos, S.A. Madrid, España, 1984.

Isaacs, M. **Internet User's Guide to Network Resource Tools**

Kent S., Atkinson R.,RFC 2409, ***IP Authentication Header,*** november
España, 1998.

Kent S., Atkinson R., RFC 2409, ***IP Encapsulating Security Payload.***
España, 1999.

Maughan D.,Schertler M., Tuner J., RFC 2408, ***Internet security(ISAKMP),***
NOVEMBER 1998.

PC Magazine Español, enero 1994, año 5 #1

Redes de Computadores.
Prentice-Hall, Tanebaun, A.S.

Revista mercado #7, julio 2002, Sto. Dgo. Rep.Dom.

Revista Negocios.com, enero/febrero 2001.

Revista Ciber Guia (Revista Exclusiva de Internet) enero/marzo; 2001.

Revista Giber Guia (abril/junio 2001)

Revista Magazine, suplemento 27 de Windows 2000 **enero , 2001.**

Sandere, D., **Informática Presente y Futuro**
Editorial McGraw-Hill. México, 1986.

INTERNETGRAFÍA

INTERNETGRAFÍA

www.cis.ohio_state.edu/~jain/cis677-8ip.htm/
TCP/IP Protocol suite e internetworking

www.cis.ohio_state.edu/~jain/cis677-98/69tcp.htm/
Protocolos de Transporte (TCP y UDP)

www.cisco.com/warp/public/44/aolutions/network/vpn.shtml
Redes Privadas Virtuales y sus Beneficios

www.cisco.com/warp/public/779/largeent/issues/vpn
Creación de una VPN

www.cisco.com/warp/public/779/smbiz/netsolutions/find/wan/vpn-solution
Soluciones de VPN

www.cisco.com/warp/public/cc/pd/wr2k/vpmnso/
Equipos

www.cisco.com/warp/public/cc/so/neso/vpn/vpne/vpn21-rg.htm
Implementación de una VPN

www.eia.udg.es/~atm/tcp.up/tema456.htm
Configurando un Servidor de VPN y una PDA

www.codetel.net.do/flash/negocios/welcome.htm
Internet Flash Negocios

www.monografias.com/trabajos12/monvpn/monvpn.shtml
Necesidades y Surgimiento de las VPN-S, Estructura, Protocolos, Configuraci'on Bajo Windows.

www.redaccionvirtual.com/redaccion/glosario/default.asp?letra=D&offset=2
Descripción de Términos

www.techweb.com/encyclopedia
Descripción de Términos

www.techguide.com
(Redes y comunicaciones, seguridad, plataformas, Sistemas Operativos)

www.uv.es/ciu/cas/vpn (Definición VPN, Ventajas e Inconvenientes, cuando usar VPN, Configuración de Acceso Remoto).

www.vpncon.com
(Encriptación y Autenticación)

GLOSARIO DE TÉRMINOS

GLOSARIO DE TÉRMINOS

A

Access Control: Control de acceso; propiedad usada en los sistemas de autenticación que asegura que individuos con ciertos derechos solo puedan realizar operaciones basadas en esos derechos.

Acceso Remoto: es el acceso que se la da los usuario que trabaja geográficamente en lugares diferentes

Address Resolutión Protocol (ARP): Protocolo de Resolución de Dirección; es un protocolo utilizado en el TCP/IP para determinar la dirección MAC se hardware de 48 bit dada a una dirección IP de 32 bit particular.

Analógico: Un modo de transmisión en el cual los datos se representan por una variación continua de señales eléctricas. Comparar con digital.

Ancho de Banda: La gama de frecuencias disponible para señalizar la diferencia entre las frecuencias más altas y las más bajas de una banda, se miden en Herzios.

ANSI (American National Standards Institute): El cuerpo principal de desarrollo de estándares en U.S.A. ANSI es una asociación sin ánimo de lucro, no gubernamental, mantenida por organizaciones comerciales, sociedades profesionales e industrias. Es el representante americano ante la ISO (Organización Internacional de Estándares).

ATM (Asynchronous Transfer Mode) — Una tecnología de red de alta velocidad que maneja datos, voz y video en tiempo real. ATM se define en el estándar Broadband RDSI (BISDN) y proporciona un ancho de banda "bajo demanda" cargando a los clientes por la cantidad de datos que envían. Las velocidades son escalables, empezando con velocidades lentas de 2.048 Mbps con velocidades intermedias de 25, 51, y 100 Mbps, y con velocidades altas de 155, 622 Mbps, y hasta la gama Gigabit.

Autenticación: Proceso de identificar positivamente el acceso de entidad requerido. Suele hacerse por medio de una función criptográfica.

Authentication Header (AH): Cabecera de autenticación; es uno de los estándares de IPSce que permite la integridad de la data en los paquetes de datos.

B

Block: Bloque; usualmente se refiere a un grupo de bits en los que opera un cifrado –por ejemplo, bloque de 40,64,128,512,y,1024bits.

Backup: es una copia de seguridad de los datos y/o procesos que se realizan en la red.

Bit: Es una cadena de caracteres que pueden usarse para crear claves de acceso.

C

Certificate: Certificado; es un documento digital firmado por una autoridad certificadora y es referente a un mensaje enviado por un individuo . El certificado le asegura al receptor que el emisor es quien dice ser.

Certificate Authority (CA): Autoridad Certificadora; Es un tercero confiable que avala la identidad de un usuario y su clave pública.

Certificado Digital: Es un certificado electrónico que identifica un usuario a una clave criptográfica pública.

CHAP: Es un protocolo asistente para el acceso remoto de NT4.0

Conexiones: Es el paso que se da a los usuarios de la red, para que puedan conectarse a cierta áreas en la red.

Conexión Punto a Punto: En ATM, conexión unidireccional o bidireccional entre dos sistemas ATM.

Criptografía: Es la parte de la criptología que estudia como cifrar efectivamente los mensajes.

Criptología: Es el estudio y práctica de los sistemas de cifrado destinado a ocultar el contenido de mensajes enviado entre dos partes: emisor y receptor.

Cipher text: Texto cifrado; Es el texto que ha pasado bajo el proceso de encriptación.

Clear Text: Texto limpio; Son los caracteres humanamente legible.

Criptación: Es el proceso de encriptar los datos de una forma ilegible durante su paso por la red publica.

Comunicación: es la forma de transmitir un mensaje sea mediante una red .

D

Data: Es el contenido de los paquetes de información que transita por la red de información.

Data Encriptión Estándar (DES): Desarrollado por IBM en 1977, es un bloque de 64 bit de un bloque de encriptación de un cipher que usa una clave de 56 bit.

Datagrama: Es el grupo de pequeño paquetes de datos que se colocan en la red pública.

Desencriptación: Consiste en invertir el proceso de criptación, haciendo que el texto ilegible sea un texto legible

DMZ: Zona de Datos Desmilitarizada: son los datos que no poseen gran seguridad.

Domain Name System (DNS): Es el protocolo estándar de Internet para mapear entre los nombre y las direcciones IP.

Desencriptar: Es el proceso de descodificar los datos de forma ilegible a legible.

E

E-mail: Correo electrónico por donde se envían y se reciben información mediante la red pública Internet.

Encapsulación: Es el proceso de ubicar un datagrama dentro del paquete de data de otra red de paquete de data; puede usarse con el mismo protocolo o con protocolo distinto.

Encapsulating Security Payload (ESP): Es uno de los estándares del IPSec que provee la confidencialidad de los paquetes de datos.

Encriptación: Es el proceso de convertir un texto legible a formatos ilegible por medio de una función criptográfica.

Estandarización: Es el estándar que debe contener todos los datos.

Extranet: Es un servidor de Internet usado por clientes externo ,suplidores y demás.

F

Firewall: Es una maquina que conecta el perimetro de la red confiable de una compañía con una red no confiable. Provee protección contra ataque usando port-filtterring, traducción de dirección y tecnología de inspección estatal, y puede presentar proxing para búsqueda interna.

Firma Digital: Es el equivalente a una firma manuscrita donde un usuario firma su clave con un valor hash para asegurar la no repudiación.

Frame Relay: Es una tecnología de comunicación rápida de tramas, basada en estándares internacionales, que pueden utilizarse como un protocolo de acceso en redes públicas o privadas proporcionando servicios de comunicación.

File transmitión Protocol (FTP): Protocolo de transmisión de archivos; es el protocolo utilizado para movilizar los archivos de un lugar a otro.

G

Gateway: es un sistema que implementa los servicios IPSec. Los gateway de seguridad provee servicios IPSec a su host y subredes interna.

GRE, Protocol Generic Router Encapsulation: Este otorga flexibilidad al PPTP de manejo de productos que no sean IP.

I

Internet Engineering Task Force (IETF): Es una organización que usa grupos de trabajo y que desarrolla nuevos estándares y tecnología para la Internet.

Internet Assigned Number Authority (IANA): Es la agencia responsable de asignar direcciones IP de Internet.

Interoperabilidad: es el mecanismo donde diferente sistema pueden comunicarse efectivamente con otro.

Internet Protocol (IP): Es el protocolo estándar para enviar data sobre el Internet.

Internet Service Provider (ISP): Proveedor de servicio de Internet; es una compañía comercial que provee acceso a Internet.

Intranet: Es un servidor o conjunto de servidores conectados dentro de la red de una compañía.

Internet Protocolo Security (IPSec): Es el protocolo de seguridad de Internet que especifica un modelo del nivel de red de encriptación y autenticación de paquete de data IP.

Internet Segurity Associatión and Key Management protocolo (ISAKMP): Asociación de seguridad de Internet y protocolo de manejo de clave; provee la estructura para manejo de para el IPSec.

Internet Key Exchange (IKP): Intercambio de clave de Internet; es un protocolo híbrido que implementa cambio de clave.

Internet Packet Exchange (IPX): Es un protocolo de alto nivel que no es IP.

K

Key: Clave; Es una combinación de dígitos usados en una función criptográfica para producir cipher tex(text cifrado).

Key Públic (KP): Llave pública; Es la llave que se utiliza para encriptar y desencriptar los datos que se transmiten en la red pública o compartida.

L

LAN: Red de Área Local: es una red que trabaja de forma local, es decir internamente en un territorio determinado.

Layer 2 Fowarding (L2F): Es un protocolo desarrollado por Cisco System que provee protocolo de alto nivel para tunelizado como IPX, IP Y SNA.

Layer 2 Tuneling Protocolo (L2TP): Es una combinación de los protocolos point to point y layer 2 que permite tunelizado de alto nivel como IPX,IP Y SNA y provee encriptación a eso flujo de datos usados en las VPN's.

Línea Punto a Punto: Una línea telefónica reservada para uso exclusivo de los que la contratan, sin conmutación. También se denomina Línea Privada.

Líneas Dedicada: Línea de comunicaciones point to point que es fijada por dos puntos finales.

Línea Local: Un canal que conecta los equipos de abonados a equipos terminales de línea en la oficina central. Normalmente circuitos metálicos (para 2 ó 4 hilos).

Línea Multipunto: Una sola línea de comunicación o circuito que interconecta varias estaciones; normalmente necesita algún tipo de mecanismo poleable para direccionar cada terminal conectado con un único código de dirección.

M

MD5: Es un algoritmo de resumen comunes que producen un mensaje de 128-bis desde una entrada de longitud arbitraria, desarrollada por Ron Rivest.

MS-CHAP: Es el que valida las credenciales del usuario remoto contra dominio de NT, ya que solo usuario con permiso pueden realizar las conexiones.

N

Network Access Point (NAP) : Punto de acceso de red; uno de los principales de apoyo donde las ISPs transfieren data entre redes.

Network Address Translation (NAT): Traducción de dirección de red; proceso de convertir un espacio de dirección IP en otro espacio de dirección IP; la NATs disponible son de una a una , mucha a mucha y mucha a una

No Repudiación: Es el proceso que se utiliza para que las firmas digitales no sean rechazada.

Network Access Securv (NAS): acceso seguro a la red; es para asegurar que los clientes y/o usuario tengan acceso seguro a la red.

Network File Secure (NFS): Seguridad de los archivos en la red; es utilizado para no permitir el acceso indebido en los archivos.

P

Packet Assembler/Disassembler (PAD): Dispositivo que ensambla o desensambla las filas del caracteres en bloques de data para transportarlos y luego ensamblar o desensamblar en el extremo receptor.

Password, Passcode: Medida Básica de seguridad para provee autenticación de usuario ;o el usuario usa un password común de una palabra o usa alguna combinación de palabras separadas como un passcode.

Permanent Virtual Circuit (PVC): Circuito virtual permanente; Son conexiones virtuales fijada entre dos punto finales que está establecida de manera permanente.

Point-Of-Point (POP): Punto de presencia; Facilita localizar un terreno de ISP que provee acceso al Internet

Point to Point protocol (PPP): protocolo punto a punto; permite el establecimiento del protocolo TCP/Ip sobre una serie de línea telefónica dial-up y líneas dedicada como ISDN.

Point to point tunneling protocol (PPTP): Protocolo de túnel punto a punto; protocolo para proveer encriptación a paquete de datos sobre una red usando en las VPN.

Pret Good Privacy (PGP): Privacidad bastante buena ; programa que permite la encriptación de documentos y E-mail, y permite el uso de firmas digitales usando el RSA.

Protocolo: Un conjunto formal de convenciones que gobiernan el formateado y el tiempo relativo del intercambio de mensajes entre dos sistemas de comunicaciones.

Proxy Server: Es una máquina que atrapa previamente los items buscados para aumentar la velocidad de acceso en el futuro; también puede ser usado como firewall con filtro de paquete y guardar y adelantar capacidades.

Public Key: Llave pública; una de las dos clave s que son usadas en un sistema criptográfico asimétrico o de clave pública.

R

Server Access Remote (RAS): Servidor de acceso remoto; son los servidores que permiten un acceso remoto a los usuarios que trabajan se forma móvil.

Remote Authentication Dial In User Service (RADIUS): es un protocolo para el manejo y autenticación de usuario remoto.

Router: es una maquina que se utiliza para enrutar las informaciones en la dirección correcta.

S

Secure Electonic Transmisión (SET): Transmisión electrónica segura; protocolo que especifica el intercambio seguro de números de tarjeta de créditos sobre la Internet.

Secure Sockets Layer (SSL): Estándar abierto de netscape para proveer servicio de encriptación y autenticación a las aplicaciones de nivel superior, como http,ftp

Secure Association (SA): Es una asociación de seguridad IPSec la cual especifica cuales servicios serán aplicado a los paquetes que estén viajando en una red no confiable entre los gateway de seguridad.

Sistema de Determinación de Intruso (IDS): Es un sistema para decretar el acceso no deseado y/o detectar algún intruso.

Server: Servidor: Estos es un equipo que se utiliza para asegurar los datos y evitar el acceso no autorizado.

T

Transmiting control protocol/Internet protocol (TCP/IP): Es un protocolo de red de comunicación de datos que provee la entrega confiable de paquetes de data; la Internet esta basada en TCP/IP.

Terminal Access Controller Control System (TACACS): Es un sistema de autenticación usado en el modulo cliente-servidor para administrar el acceso de usuarios de manera remota.

Tunneling: **Tunelización**: proceso el cual se crea una conexión lógica entre dos puntos finales.

Túnel Lan to Lan: usado en la terminología de VPN, define un conjunto de punto finales de comunicaciones que están comprometidas a pasarse los datos encriptados entre cada uno.

Túnel: es el medio por donde transitan los datos.

U

User Datagrama Protocol (VDP): Protocolo de datagrama de usuario; protocolo de transporte.

V

Valor Hash: Es un conjunto de dígitos único producido por un flujo de entrada de data.

Virtual LAN (VLAN): Dispositivo en una Red o Redes que están configurados como si estuviesen conectados al mismo cable, cuando en realidad estan localizados en un número diferente de segmento de red.

W

Wide Area Network (WAN): Red de área amplia; Una red que consta de dos o más LANs, conectadas por una infraestructura de comunicación.

World Wide Web (WWW): Servicio de Internet que habilita a un browser para ver data tomado como vía el protocolo http.

ANEXOS

CUESTIONARIO:
(Empresas proveedoras de servicios de data)

1.- ¿Cuáles Servicios ofrecen en la actualidad basados en VPN?

2.- ¿Qué alternativa(s) a VPN ofrecen?

3.- ¿Cuál es el costo de Implementación, renta mensual y de mantenimiento de cada alternativa que ofrecen?

4.- ¿Las alternativas que ofrecen, requiere un contratación mínima de tiempo? ¿Si es así cuál es el tiempo de contratación mínimo para cada alternativa?

CUESTIONARIO:
(Empresas Utilizando VPN, en República Dominicana)

1.- ¿Qué servicio(s) de comunicación utilizan a nivel de WAN? ¿Cuál es el ancho de banda de cada servicio?

2.- ¿Cuál(es) equipo(s) ustedes utilizan para la interconexión VPN?

3.- ¿Cuál tipo de VPN utilizan? ¿con qué fin?

4.- ¿Con cuáles localidades se interconectan a través de VPN?

5.- ¿Para que usan la VPN? ¿Quiénes la usan?

6.- ¿Qué tipo de Cliente usa en la VPN?

7.- ¿Contra que equipo se enfrenta el túnel de VPN?

8.- ¿Por qué usan VPN y no otra tecnología?

CUESTIONARIO:
(Para implementar la VPN)

1.- ¿Qué sistema de información utilizan en cada punto? ¿Con qué frecuencia utilizan cada sistema?

3.- ¿Cómo actualizan los sistemas?

4.- ¿Qué equipos de cómputos utiliza la empresa?

5.- ¿Cuáles de sus oficinas tienen acceso a Internet? ¿Qué tipo de acceso a Internet tienen?

6.- ¿Cuál(es) servicio(s) de sistema tienen en la oficina principal que no tienen en las otras oficinas?

7.- ¿Qué crecimiento prevén en todas sus oficinas (sucursales y principal)?

8.- ¿Cuántos usuarios necesitarían conectar VPN?

HOJA DE CALIFICACIÓN

Franklin Objio
Decano Facultad de Ingeniería

José Felipe Guillén Sarita
Director Escuela de Informática

Sustentante
Thanya Guzmán Rincón

Miembro del Jurado

Miembro del Jurado

Presidente del Jurado

Consejero

Calificación 91

Fecha 27/10/03