UNIVERSIDAD CENTRAL "Marta Abreu" DE LAS VILLAS
FACULTAD DE INGENIERIA ELECTRICA
Departamento de Telecomunicaciones y Electrónica

PROPUESTA DE IMPLEMENTACION DE RED PRIVADA VIRTUAL PARA ETECSA.

Tesis presentada en opción al título académico de
Master en Telemática.

Autor: Ing. Leodan Salomé Lorente Leyva.
Gerencia Territorial ETECSA, GRANMA.

Tutor: Msc. Vitalio Alfonso Reguera.
Facultad de Ingeniería Eléctrica. UCLV.

Santa Clara. 2007
Cuba

PENSAMIENTO

"*Un sistema se vuelve inseguro simplemente con el mero hecho de encenderlo*. *El único sistema totalmente seguro sería uno que estuviese apagado, desconectado de cualquier red, metido dentro de una caja fuerte de titanio, rodeado de gas y vigilado por unos guardias armados insobornables. Aún así yo no apostaría mi vida por él*"

Gene Spafford, experto en seguridad

DEDICATORIA

`

A mi Madre,

a mi Papá,

a mi Esposa,

a mis Hijos,

a mis Hermanos.

AGRADECIMIENTOS

- A todos mis compañeros de la maestría por la amistad y el empuje en todo momento.
- A la Empresa de Telecomunicaciones de Cuba S.A., por darme la oportunidad de participar en esta maestría.
- Al claustro de profesores de la Universidad Central de Las Villas.
- A la gran familia del Centro de Capacitación por sus maravillosas atenciones.
- Al profesor Vitalio por sus métodos para hacer llegar sus conocimientos.
- A mi familia, que tanto ha impulsado mis pasos en la vida.

RESUMEN

En la Empresa de Telecomunicaciones Cuba, SA existen tres redes independientes físicamente, dedicada una a la Gestión Corporativa, otra a la Gestión de los elementos de conmutación, tráfico y abonados, y la otra a la Gestión de los elementos de Transmisión. Como característica fundamental se identifican las conexiones mediante la red Pública de Transmisión de Datos de las dos primeras y mediante un enlace dedicado de la última. Haciendo uso de la seguridad que se provee por defecto en cada caso. Esta tesis describe desde el punto de vista teórico los aspectos básicos de las Redes Privadas Virtuales y los protocolos que la implementan, escogiendo el protocolo IPSec para la tunelización y encriptación de la información que se intercambia. Se describen las principales características y topología de las distintas redes y se caracterizan los equipos de conectividad principales en la interconexión con las provincias, además se propone una guía para implementar las Redes Privadas virtuales de acuerdo a las condiciones actuales. Finalmente se aplica esta guía para dar una solución concreta y se obtiene una propuesta de integración y optimización de los recursos existentes, así como un esquema flexible para incorporación de nuevas redes al menor costo y menor gestión de administración.

INDICE

INTRODUCCIÓN

En los últimos años, las redes se han convertido en un factor crítico para cualquier organización. Cada vez en mayor medida, estas transmiten información vital para el éxito de una empresa que se encuentra más extendida geográficamente. Por tanto, dichas redes deben cumplir con atributos tales como seguridad, fiabilidad, alcance geográfico y ser económicas.

Anteriormente al desarrollo de las redes, los servicios de telecomunicaciones se gestionaban principalmente por puerto serie. Los protocolos eran en gran medida propietarios y no estandarizados. La seguridad de la gestión y supervisión se garantizaba desde una estación de trabajo y un especialista era el actor fundamental.

El crecimiento e instalación de las redes locales posibilitó la gestión remota con un elevado nivel de prestaciones. La seguridad de la información comienza a depender entonces de otros actores humanos y tecnológicos.

Las redes privadas virtuales (VPN, Virtual Private Networking) son redes que se construyen sobre una infraestructura pública y constituyen una poderosa solución con los requerimientos necesarios para garantizar seguridad y han sido la solución de conexión de los componentes de una red con otra red para resolver el inquietante problema de la seguridad, permitiendo realizar un túnel a través de Internet o a través de otra red y hacer mas adecuado el uso de las tecnologías.[1, 2]

Las búsquedas y consultas realizadas en ETECSA han reflejado que la aplicación de VPN es pobre y se está aplicando en la actualidad para conectar la Red de la Unidad de Negocios Datos con la Red Corporativa, mediante una conexión a un servidor que implementa la tunelización. Además se implementa en algunas redes privadas de la Red IP del ISP Enet.

En el mercado existen diversas técnicas que garantizan de diferentes modos los atributos de seguridad, fiabilidad, flexibilidad, agilidad y escalabilidad en la implementación de una VPN, que con el aumento de velocidad de procesamiento de datos y el desarrollo de algoritmos criptográficos posibilitan aumentar los niveles de seguridad.

Situación Problémica

Con la evolución de las tecnologías informáticas y las telecomunicaciones se comprueba que no es suficiente con procesar la información, sino que además, es preciso compartir esta información entre distintos equipos, así como los recursos que pueden ser muy costosos también se pueden compartir. ¿Qué ocurre en este caso cuando tenemos que transmitir información confidencial de un equipo a otro? La solución pasa por interconectar entre sí, aquellos equipos que comparten la información confidencial, separando físicamente la red confidencial de la red general.

Esto presenta varios problemas, el primero es la duplicidad de recursos de red que se necesitan, ya que tendremos que montar y mantener varias redes. La segunda es que aún así la confidencialidad no se puede considerar segura, puesto que la seguridad viene impuesta por la separación física de las dos redes, pero nada impide que en una determinada parte de la instalación alguien se pueda conectar a dicha red y leer los datos que circulan. La solución pasa por usar una misma red para transmitir la información confidencial junto a la información abierta. Este es un escenario típico de las redes de ETECSA. Las soluciones de interconexión son principalmente por la Red Pública de Transmisión de Datos, en este caso la información se puede considerar hasta cierto punto segura, ya que los conocimientos necesarios para poder acceder a las líneas, no se encuentra al alcance de cualquier persona, además de los equipos necesario para ello. No obstante, el crecimiento y la automatización empresarial, nos lleva a un escenario, donde las oficinas y el equipamiento tecnológico se despliegan por la geografía, haciéndose necesario además el acceso a la información en las oficinas centrales.

Por ser el servicio que interconecta las distintas redes de carácter público, parece lógico pensar que es un sistema inseguro donde la información que circula por la misma está al alcance de personas que pueden actuar sobre ellas.

Esto define la necesidad de la propuesta de un escenario donde aparezcan las Redes Privadas Virtuales, haciendo uso de la encriptación de la información como la forma para impedir la lectura y/o modificación de la información y por la cual pueden confluir varias redes optimizando el uso del equipamiento, los enlaces y la gestión de administración.

Problema

La seguridad de la información que se intercambia por las redes requiere mantener su integridad, confidencialidad y disponibilidad y la que le proveen las aplicaciones resultan insuficientes. La utilización de un enlace por cada red instalada y equipamiento tecnológico incrementa los costos, la gestión de administración para poder soportarlas y no es una solución flexible a incorporar nuevas redes.

Interrogantes

¿Cuáles son los distintos protocolos que soportan las redes para garantizar la confidencialidad de la información?

¿Cuál es la situación actual de las redes privadas virtuales soportadas en Internet u otras redes públicas de transmisión de datos?

¿Qué equipamiento existe en ETECSA para garantizar mecanismos de encriptación de los datos?

¿Cuáles son las redes existentes en ETECSA para los distintos entornos de trabajo?

¿Qué aplicaciones se utilizan en cada red y que nivel de seguridad necesitan?

¿Cuál puede ser el protocolo para garantizar la seguridad de la información que transita por la red?

¿Cuales son las etapas que deben considerarse para implementar las redes privadas virtuales en ETECSA que garanticen una solución de extremo a extremo de los equipos de borde instalados?

Objetivo general:

Proponer una implementación de seguridad que garantice disponibilidad, confidencialidad e integridad de la información que viaja por las principales redes de ETECSA.

Objetivos específicos:

1. Revisar las diferentes alternativas de Redes Privadas Virtuales.
2. Analizar que algoritmo es el mas adecuado de acuerdo al estado actual de los elementos de conectividad en la redes existente en la empresa.
3. Realizar una propuesta de implementar Redes Privadas Virtuales que integren las distintas redes por un mismo enlace, haciendo uso del equipamiento disponible o la actualización de este.

Para alcanzar los objetivos propuestos se definieron las siguientes tareas de investigación:

1. Estudio de los diferentes variantes de Redes Privadas Virtuales.
2. Estudio de los diferentes protocolos de encriptación que funcionan en las Redes Privadas Virtuales.
3. Revisión del estado actual de las distintas redes instaladas en la empresa.
4. Caracterización de los distintos equipos de conectividad principales utilizados.
5. Guía para implementar las VPN especificas para resolver la situación actual.
6. Propuesta de implementación de las Redes Privadas Virtuales en la empresa a partir de la guía propuesta.

En el proceso de investigación se utilizaron los métodos de investigación teóricos de análisis y síntesis para el estudio del fundamento teórico de las Redes Privadas Virtuales y la elaboración de la estrategia de implementación de varias redes sobre un mismo enlace de conectividad.

Impacto Económico

Reducir las interrupciones provocadas por la de alteración de la información que viaja por la red con el consiguiente ahorro de recursos en su solución. Enlaces disponibles para la comercialización de otros servicios. Evita la adquisición de nuevo equipamiento al integrarse al ya existente.

Impacto Tecnológico

Utilización de prestaciones disponibles no utilizadas. Ahorro de enlaces de datos que pueden ser utilizados para otras necesidades.

Defensa

Continuidad de la operación de la red de telecomunicaciones al minimizar la afectación de integridad, disponibilidad y confidencialidad de la información que viaja por la red, objetivo priorizado por la Dirección de la Empresa y del país.

El trabajo cuenta con la siguiente estructura:

INTRODUCCION: Se definen los antecedentes, justificación y problema que determinan la propuesta de trabajo científico, el objetivo general y objetivos específicos a lograr.

DESARROLLO.

CAPITULO I: Estado de arte de las Redes Privadas Virtuales.

CAPITULO II: Estado actual de las redes en ETECSA. Caracterización del equipamiento y enlaces. Propuesta para el diseño de la VPN.

CAPITULO III: Propuesta de implementación de la VPN en ETECSA aprovechando el uso del equipamiento y enlaces disponibles.

CONCLUSIONES
RECOMENDACIONES.
GLOSARIO.
BIBLIOGRAFIAS.
ANEXOS.

CAPITULO 1. Estado del arte de las Redes Privadas Virtuales

En este capítulo se describen las Redes Privadas Virtuales y se establecen los criterios para su clasificación. Se discuten las ventajas de utilizarlas y problemas que son comunes a todas la VPN. Se estudia como han evolucionado sus protocolos y se hace una breve de su introducción en Cuba a nivel de proveedores de servicio.

1.1 Distintos tipos de VPN

Para comenzarse a definir lo que son las Redes Privadas Virtuales se analiza la siguiente frase:

Es de noche. La calle está llena de gente. Estamos esperando a cruzar la acera, cuando de repente vemos pasar una limusina. Tiene los cristales tintados, que reflejan las luces del neón, pero no podemos ver quién hay dentro ni lo que está haciendo. Estamos acostumbrados a ver otro tipo de coches, así que nos preguntamos ¿quién viajará ahí dentro? ¿Un político? ¿Un actor? De repente las luces del semáforo cambian y nos vemos arrastrados por la multitud al otro lado de la calle. La limusina se desvanece en la noche, dejando atrás todas nuestras especulaciones.

Si se traslada esta experiencia al mundo IP (Internet Protocol), nos daremos cuenta de las ventajas de las VPN (Virtual Private Network). La analogía reside en que al igual que la limusina viaja por la calle sin mostrar que ocurre en su interior, la comunicación en una VPN viaja a través de Internet, pero está encapsulada y encriptada por lo que su contenido es secreto. Sólo el emisor y el receptor legítimo del mensaje pueden verla en su estado normal. Así el camino de un mensaje a través de una VPN tiene luz en los extremos, y oscuridad entre ellos, por lo que también se le llama, metafóricamente hablando, un túnel VPN.[3, 4]

Una red privada virtual (Virtual Private Network) es una red que se extiende, mediante un proceso de encapsulamiento y de encriptación de los paquetes de datos a distintos puntos remotos mediante el uso de infraestructuras públicas de transporte. Los paquetes de datos de la red privada viajan por medio de un “túnel” definido en la red pública.[5]

En definitiva, las definiciones que podemos encontrar del significado e implicación de una red privada virtual, son múltiples, que se puede concretar en:

"Una red privada virtual es una implementación o sistema que habilita una comunicación segura a través de un medio inseguro, siendo transparente para el usuario u aplicación que realiza y recibe la comunicación." [6]

Esta definición que es perfectamente válida, se puede ampliar y podremos decir que siempre que queramos asegurar una comunicación entre dos puntos, podremos utilizar una red privada virtual, independientemente del potencial de privacidad que tengamos en la comunicación, si la información ha de ser preservada de terceros por su importancia. Véase Figura 1.

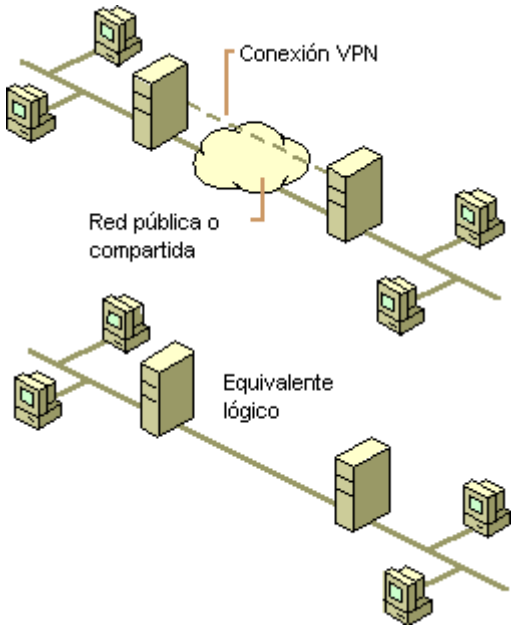

Figura 1 Definición de Red Privada Virtual pública

En el caso de acceso remoto, la VPN permite al usuario acceder a su red corporativa, asignándole a la computadora remota las direcciones y privilegios de la misma, aunque la conexión la haya realizado por medio de un acceso a Internet público. Véase Figura 2.

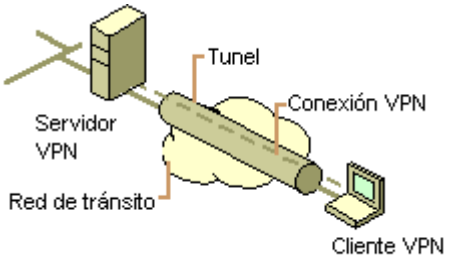

Figura 2 Acceso Remoto

Desde una perspectiva muy simple, una VPN es un método para conectar redes, utilizando redes públicas para la transportación de datos. Es decir, enlaza computadoras y redes entre sí.

Es **virtual**, porque toda la información que viaja a través de ella se realiza mediante una red pública y no sobre una LAN. P**rivada**, debido a que los datos se encapsulan por medio de un protocolo de túnel.[7]

Normalmente usa la red Internet como transporte para establecer enlaces seguros, extendiendo las comunicaciones a oficinas aisladas. Significativamente, decrece el costo de las comunicaciones porque el acceso a Internet es generalmente local y mucho más barato que las conexiones mediante Acceso Remoto a Servidores.[8]

Así, las VPN constituyen una buena combinación entre la seguridad y garantía que ofrecen las costosas redes privadas y el gran alcance, lo asequible y lo escalable del acceso a través de Internet o una red pública. Esta combinación hace de las Redes Privadas Virtuales una **infraestructura confiable y de bajo costo** que satisface las necesidades de comunicación y seguridad de cualquier organización.

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.

Los requisitos indispensables para esta interconectividad son:

Políticas de seguridad.

Requerimiento de aplicaciones en tiempo real.

Compartir datos, aplicaciones y recursos.

Servidor de acceso y autenticación.

Aplicación de autenticación.

Las organizaciones instalan las VPN por tres razones principales:

Reducir los costos de acceso remoto y las comunicaciones dedicadas entre las empresas y sus filiales o socios comerciales.

Mejorar el rendimiento para el acceso distribuido.

Crear políticas de seguridad consistentes con todos los medios heterogéneos de la empresa.

Hay algunos modelos de empresa en los que la tecnología VPN proporciona notables beneficios.

Direcciones aisladas de una misma empresa.

En este supuesto, se trata de localizaciones de una misma empresa separadas geográficamente, que necesitan intercambiar datos entre ellas, acceder a una misma base de datos y aplicación. Véase Figura 3.

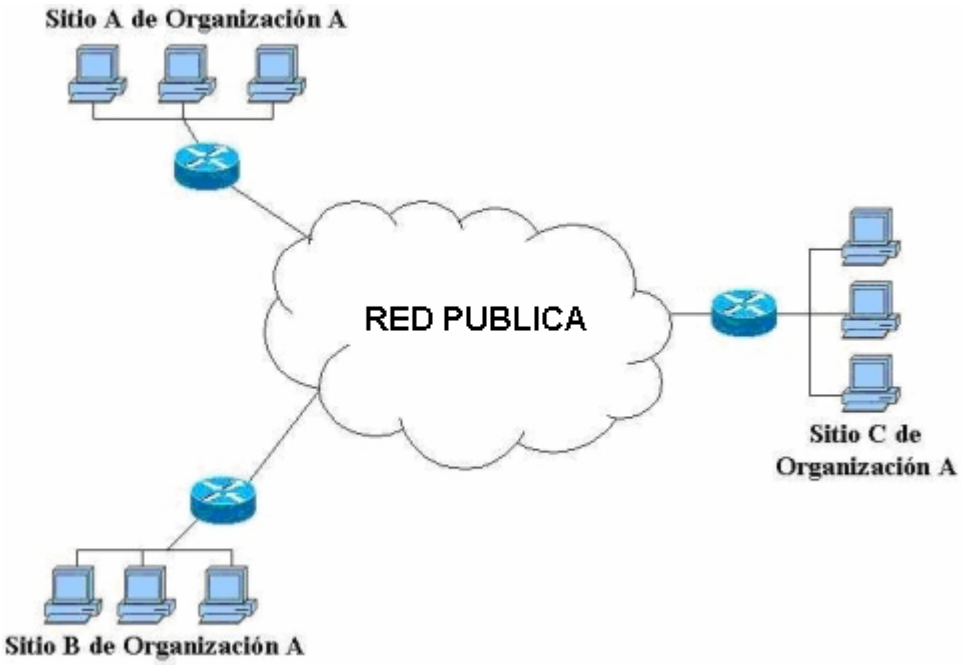

Figura 3 Extremo a extremo de equipos de borde.

1.2 Clasificación de las VPN

Se pueden clasificar las Redes Privadas Virtuales atendiendo a varios criterios:

Red pública que la soporta.

Uso de la VPN.

VPN por hardware.

VPN por software.

1.2.1 Red pública que la soporta

Las redes privadas virtuales pueden establecerse sobre varias redes públicas Frame Relay, Internet, ISDN, ATM, MPLS o sobre cualquier red de infraestructura pública.

Ahora bien, no se debe perder de vista que las redes privadas virtuales son redes privadas construidas sobre la infraestructura de una red pública. Es decir una buena idea es, que en lugar de utilizarse enlaces dedicados a redes de paquetes (como el X.25 y Frame Relay, ATM, y MPLS) para conectar redes remotas, se utilice la infraestructura de Internet o un enlace sobre la red pública, teniendo en cuenta que para los usuarios la forma como las redes están conectadas es transparente.

1.2.2 Uso de la VPN

En este enfoque existen dos variantes:

- VPN para acceso remoto (*VPN for Remote Acces*)

- VPN como *Extranet* e *Intranet* (*VPN as Extranet and Intranet*)

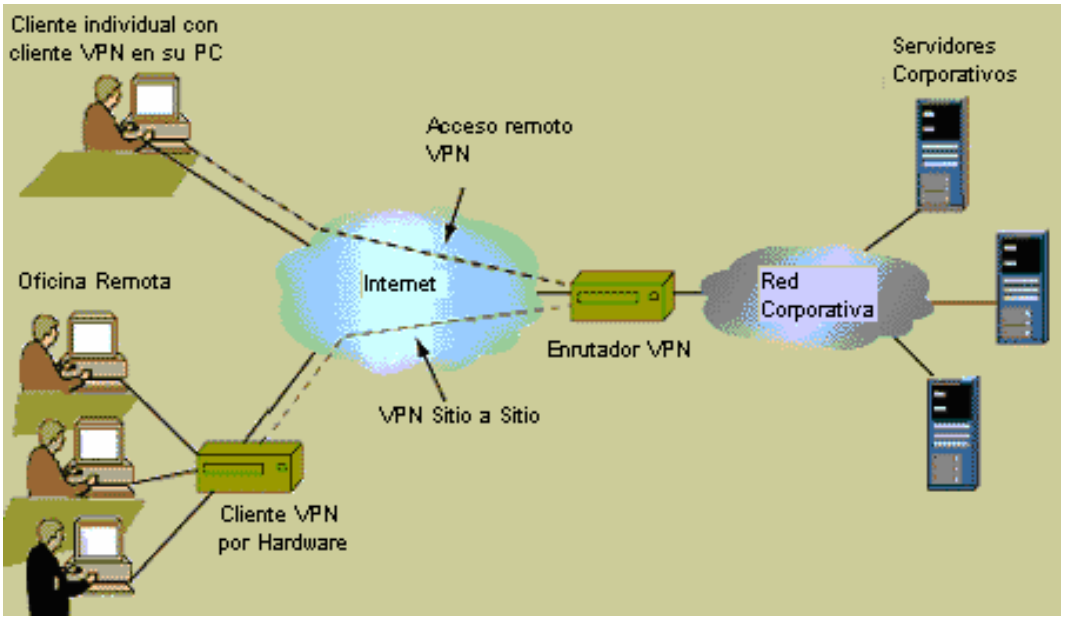

Figura 4 VPN para acceso remoto y VPN como Extranet[8]

VPN para acceso remoto

La VPN para brindar acceso remoto, es muy usada para usuarios móviles que requieren acceso remoto para conectarse a través de llamadas: xDSL, ISDN, Wi-Fi. Los proveedores ofrecen ese servicio para ayudar a los clientes a conectarse a intranets y extranets donde se encuentren físicamente situados.[9]

VPN como Extranet e Intranet

Una VPN como extranet e intranet enlaza oficinas remotas, socios comerciales, clientes y comunidades de intereses sobre una infraestructura compartida con la misma política de que una red privada. Ambos servicios crean túneles sobre la red IP, tomando los estándares para establecer una conexión segura punto a punto. [10]

1.2.3 VPN por Hardware

El proceso de encriptación y desencriptación se realiza a nivel físico en los puntos inmediatamente anterior e inmediatamente posterior al comienzo de la línea de comunicación. Por realizarse a nivel físico, necesitamos unos equipos que permitan realizar esta tarea de forma transparente. Por lo general los elementos utilizados son los routers con VPN incorporada. Estos dispositivos llevan incorporado un procesador y algoritmos de encriptación y desencriptación. Tienen la ventaja de que el fabricante nos da realizada la implementación y su instalación y uso es extremadamente sencillo, ya que solo tenemos que intercalar los routers en los puntos de salida y entrada de la línea de comunicación y activar en los routers la encriptación-desencriptación, así como configurar la contraseña, certificación o medio que servirá para la encriptación y desencriptación de la información. [11]

Las VPN implementadas por hardware, presentan el inconveniente, de que el sistema de encriptación viene impuesto por el fabricante, y depende del mismo para las actualizaciones.

Dentro de esta categoría se puede incluir los routers wireless con encriptación, bien mediante WPA o/y WEP, ya que crean un túnel entre el router y la tarjeta wireless que impiden en cierta forma la lectura y modificación de la información.

En este caso el medio de transporte son las ondas electromagnéticas y por tener el router y la tarjeta inalámbrica la antena, la encriptación se realiza a nivel de capa física.

Las ventajas e inconvenientes que presenta este tipo de configuración son:

1. Ventajas[12]

- La instalación y la configuración son relativamente sencillas.
- No necesita personal especializado y su mantenimiento es mínimo.
- Un único elemento puede habilitar varias VPNs ubicadas en distintos sitios.
- El sistema es independiente de las máquinas conectadas a la red.
- No necesitamos máquinas dedicadas para realizar la VPN.

2. Inconvenientes.[13]

- Depende de una tecnología externa y cerrada.
- El firmware de los sistemas es cerrado y dependemos del fabricante para poder cambiarlo.
- Los sistemas de encriptación suelen ser cerrados y el fabricante suele utilizar un único tipo.
- En mucha de las ocasiones los elementos hardware de los extremos que componen la red privada virtual, deben ser iguales o por lo menos del mismo fabricante.

- La seguridad sólo se implementa desde los dos extremos de la VPN, siendo inseguro el camino que recorre la información desde el ordenador hasta el dispositivo VPN.

1.2.4 VPN por Software

Cada día se está imponiendo más la utilización de Redes Privadas Virtuales por software. La explicación radica en la necesidad que cada vez más tienen los medianos y pequeños usuarios implementar sistemas de seguridad en el acceso a sus máquinas. Como además son sistemas que tienden a crecer de forma rápida, es mucho mas barato la utilización de VPN por software que por hardware.

Las ventajas y desventajas que pueden presentar este tipo de redes son:

1. Ventajas:[14]

- Existe una gran variedad de Redes Privadas Virtuales desarrolladas por software, donde elegir y que están continuamente mejorando sus prestaciones.
- El número de usuarios de este tipo de red es mucho mayor que el número de usuarios de VPNs realizadas por hardware, con lo que la posibilidad de encontrar documentación y ayuda para estos elementos es mayor.
- Pueden dar cobertura tanto a redes internas (intranet) como redes externas.

- La seguridad puede cubrir de máquina a máquina, donde se encuentren colocados los extremos de la VPN.

2. Desventajas.

- Es necesario instalar el software en una máquina, pudiendo ser necesario una carga muy grande de información y tener que dedicar una máquina para esta tarea.
- El sistema de claves y certificados están en máquinas potencialmente inseguras, que pueden ser atacadas.
- Si el software es de libre distribución, éste puede estar modificado y contener puertas traseras.

1.2.5 Arquitectura de la VPN

Según sus arquitecturas las Redes Privadas Virtuales se pueden ser:

Dependiente

Independiente

Híbrida

Dependiente

Son aquellas en las cuales el proveedor de servicios brinda completamente la solución VPN y se encarga de controlar el túnel, el rendimiento, la seguridad y los requerimientos de administración.

Por supuesto que para estas arquitecturas, es necesario que el proveedor de servicios garantice la disponibilidad de la VPN.

Entre sus características se encuentran:

- Todos los sitios VPN tiene una interfaz con un punto de presencia del proveedor de servicios, ya sea mediante una línea arrendada o un servicio conmutado.
- Cuando un miembro de la VPN se conecta al servidor de acceso del proveedor de servicios, este le pregunta a su servidor RADIUS los datos del usuario (clave, privilegios, parámetros del túnel).
- Todo el tráfico de y hacia el usuario final es encapsulado/desencapsulado en el punto de presencia.

- El proceso de túnel entre este y la infraestructura de Internet es transparente al usuario final quien sólo ve el tráfico nativo.
- La organización se encarga de la seguridad de los usuarios y de sus posibilidades de acceso.

Independiente

La organización se encarga de todos los requisitos de la VPN, dejándole al Proveedor de Servicios el transporte. El proveedor de servicios sólo ve el tráfico de Internet, sin poder determinar cuál pertenece a Internet y cuál a la VPN.

Todos los sitios participantes intercambian tráfico IP con el punto de presencia del proveedor. El tráfico se encapsula/desencapsula en los sitios de la organización. Es útil para las organizaciones que deseen asegurar el total de su tráfico.

Híbrida

Las VPN Híbridas son una combinación de las VPN dependientes y las independientes, que pueden establecerse cuando el ISP, implementa y administra algunos de los dispositivos VPN, mientras que otros los debe manipular la organización.

1.4 Ventajas de la utilización de las VPN

La principal ventaja de usar una VPN es que permite disfrutar de una conexión a red con todas las características de la red privada a la que se quiere acceder. El cliente VPN adquiere totalmente la condición de miembro de esa red, con lo cual se le aplican todas las directivas de seguridad y permisos de una computadora en esa red privada, pudiendo acceder a la información publicada para esa red privada: bases de datos, documentos internos, etc. a través de un acceso público. Al mismo tiempo, todas las conexiones de acceso a Internet desde el ordenador cliente VPN se realizaran usando los recursos y conexiones que tenga la red privada. [15]

Desde el punto de vista económico, una red privada virtual ayuda en la reducción de gastos de administración, pues “el costo de una red se divide en: equipo 20%, implementación 30 y administración 50%. Al utilizar una VPN se delega la administración y el mantenimiento de la red al proveedor de servicios”[16]. Claro que en ese caso se está refiriendo a una VPN dependiente.

De esta forma, una empresa se ahorra en inversión de infraestructura tecnológica, administración y mantenimiento, y además, puede integrar varios servicios en un solo enlace. Como ejemplo, se eliminan las llamadas de larga distancia, las cuales son sustituidas por llamadas locales al servidor de Internet, por lo que también desaparecen los pagos por concepto de enlaces dedicados para la interconexión de oficinas remotas.

Beneficios para las empresas

Según estudios realizados por CISCO “las organizaciones que adoptan VPN ahorran alrededor de un 60% a sus equivalentes redes privadas”, ya que:[16]

- Eliminan las líneas arrendadas entre sitios separados largas distancias.
- Eliminan las llamadas de larga distancia a través de la red telefónica conmutada, mediante modems.
- Les permite pagar solo por el uso actual de la red o por el tráfico enviado.
- Requieren menos equipamiento ya que es una solución brindada por Internet y el acceso VPN, por tanto se elimina la necesidad de bancos de modems, adaptadores de terminal, servidores de acceso remoto, etc.
- Minimiza el diseño de la red y las responsabilidades de administración.
- Las VPN explotan las nuevas generaciones de redes públicas de infraestructuras robustas para proporcionar más capacidades y alternativas confiables a las redes privadas.
- La presencia global de Internet hace a las VPN más flexibles que las redes privadas, pues con las VPN las empresas pueden:
    . Adicionar y borrar conexiones instantáneamente.
    . Brindar conexiones permanentes, periódicas o temporales, según se necesite.
    . Seleccionar las velocidades de datos óptimas, desde la de modems analógicos a T1/E1, y más allá de las tecnologías xDSL.

Beneficios para los proveedores de servicios

En el caso de los Proveedores de Servicio de Internet adoptar esta tecnología le trae beneficios, relacionados fundamentalmente, con la ampliación de sus ofertas y el establecimiento de un ambiente seguro con poco costo y la gran dependencia de sus clientes que realizan comercio electrónico.[17]

- Posibilidad de brindar una gran cantidad de servicios de valor añadido.
- Una gran oportunidad de negocio con ingresos sustanciales.
- Posibilidad para atraer y expandir clientes corporativos.
- Oportunidad para establecer relaciones con grandes organizaciones.
- Influencia de la infraestructura existente para el rápido establecimiento de nuevos servicios con poca inversión.

Los servicios de valor añadido sobre VPN dan más ganancia que los establecidos sobre líneas privadas.

1.5 Encapsulamiento (Tunneling) en las VPN

Una red privada virtual de Internet combina conceptos en conflicto: una zona privada dentro de una red privada dentro de una red pública. Pero la metáfora de la privacidad va demasiado lejos cuando los proveedores dicen cosas como que las VPN establecen túneles seguros a través de Internet. [18]

La definición mezcla un concepto técnico el encapsulamiento, también llamado "*tunneling*", con el concepto de la seguridad, dando como resultado la connotación de que las VPN se encuentran en una zona de robustez, con un túnel especial alrededor de ellas. Este es un mito de mercado, mientras las VPN son seguras contra piratas de la red (*hackers*) e intrusos, no hay túneles, no hay circuitos virtuales a través de Internet, tampoco se les dan a los paquetes del túnel prioridades especiales, siguen siendo datagramas como los otros paquetes.

Hay varios usos para el término "*tunneling*" en las redes. El significado más común y técnico de los túneles en Internet, se refiere a introducir un paquete dentro de otro; IPX dentro de IP, PPP dentro de IP. En este proceso el "*tunneling*" es meramente un proceso de transporte. El IP no añade seguridad al IPX o al PPP cuando las encapsula, meramente los porta.

Lo que añade seguridad son los procesos de encriptación y autenticación, que se pueden utilizar con los paquetes en el túnel y con los paquetes en no-túnel. Algunos enfoques de VPN encapsulan todos los paquetes antes de encriptarlos. Otros encriptan sólo los contenidos de los paquetes y los contenidos de los paquetes encapsulados, no las cabeceras.[4, 6]

De cualquier manera es la encriptación, no el encapsulamiento la que añade seguridad.

1.6 Problemas comunes a todas las VPN

Algunos problemas son comunes a todas las VPNs:

Seguridad: Casi todas las Redes Privadas Virtuales usan redes públicas. Sin embargo, con cualquier servicio público hay preocupaciones en cuanto a privacidad de los datos. Hoy estas se manejan a través de la encriptación, y a través de técnicas que proporcionan separación lógica o física de tráfico de los diferentes clientes. Se tienen en cuenta, por ejemplo otros elementos, el alcance geográfico, ancho de banda disponible y eficiencia de ancho de banda**,** pero las preocupaciones de seguridad tienden a ser las principales.

Rendimiento: Una empresa puede vigilar o dar proporción al tráfico que entra en una red privada, y configurar la red para satisfacer los parámetros de rendimiento. Ése no es el caso de las redes públicas dónde los clientes están a merced del proveedor de servicios, y el tráfico de cada cliente compite por el ancho de banda. Los VPNs deben incluir mecanismos para asegurar el rendimiento.

Administración: El manejo, las adiciones y los cambios se hacen más difíciles en las VPNs en caso de que las redes no coincidan con sus políticas de seguridad. La facilidad de administración de VPN es primordial.

1.7 Protocolos para la implementación de VPN

El enfoque general del VPN IP tradicional es envolver (o encapsular) cada paquete IP en otro paquete IP antes de ponerlo en la Internet. El paquete saliente se dirige a la pasarela (*gateway)* VPN o cliente VPN, creando un túnel a través de la Internet escondiendo la dirección del último destino.

Dos protocolos VPN iniciales son L2F[19], desarrollado por Cisco, y PPTP[20], desarrollado por Microsoft. El IETF[21] (*Internet Engineering Task of Force*) diseñó un tercer protocolo, L2TP[22], como una alternativa para el vendedor neutral. Posteriormente, debido mayormente a las preocupaciones de seguridad, los tres protocolos se adecuaron a IPSec[23], este último también creado por IETF[21].

1.7.1 Point-to-Point Tunneling Protocol (PPTP)

PPTP es una especificación de protocolo desarrollada por varias compañías. Normalmente, se asocia PPTP con Microsoft, ya que Windows incluye soporte para este protocolo. Los primeros inicios de PPTP para Windows contenían características de seguridad demasiado débiles para usos serios. Por eso, Microsoft continúa mejorando el soporte PPTP. La mejor característica de PPTP radica en su habilidad para soportar protocolos no IP. Sin embargo, el principal inconveniente de PPTP es su fallo a elegir una única encriptación y autentificación estándar: dos productos que acceden con la especificación PPTP pueden llegar a ser completamente incompatibles simplemente porque la encriptación de los datos sea diferente.

Este protocolo tiene grandes problemas de seguridad, en pocas palabras: PPTP es un protocolo que puede evitar al curioso casual, pero no es rival ante un adversario determinado a acceder a la información que circule por el túnel. Este hecho es especialmente importante para las empresas que emplean PPTP para interconectar sus intranets entre sí, a través de infraestructuras públicas como es Internet.

1.7.2 Layer Two Tunneling Protocol (L2TP)

El principal competidor de PPTP en soluciones VPN fue L2F, desarrollado por Cisco. Con el fin de mejorar L2F, se combinaron las mejores características de PPTP y L2F para crear un nuevo estándar llamado L2TP[22]. L2TP pertenece al nivel de enlace del modelo OSI. L2TP, al igual que PPTP soporta clientes no IP, pero también da problemas al definir una encriptación estándar.

1.7.3 Internet Protocol Security (IPSec)

IPsec es en realidad una colección de múltiples protocolos relacionados. Puede ser usado como una solución completa de protocolo VPN o simplemente como un esquema de encriptación para L2TP o PPTP. IPsec se encuentra en el nivel de red en OSI, para a extender IP el propósito de soportar servicios más seguros basados en Internet.[24]

Los protocolos IPSec[24] combinan IP *tunneling* con la autenticación reforzada, encriptación e integridad-comprobación. La autenticación asegura que los remitentes y receptores son quién ellos dicen que ellos son, la encriptación mantiene en secreto datos de usuario y las verificaciones de integridad aseguran que nadie altera los datos del paquete que viaje por la VPN. IPSec ofrece múltiples niveles de seguridad y varios

algoritmos de encriptación y de autenticación. Lo más común es utilizar los certificados digitales para autenticar los extremos del enlace y los protocolos de Intercambio de claves (*Internet Key Exchange*, IKE[25]) para negociar las conexiones e intercambio de las claves criptográficas.

1.7.4 SSL/TLS

SSL[26]/TLS[27] Secure Sockets Layer/Transport Layer Security existen pequeñas diferencias entre SSL 3.0 y TLS 1.0, pero el protocolo permanece sustancialmente igual. El término "SSL" según se usa aquí, se aplica a ambos protocolos a menos que el contexto indique lo contrario. SSL proporciona autentificación y privacidad de la información entre extremos sobre Internet mediante el uso de criptografía. Habitualmente, sólo el servidor es autentificado (es decir, se garantiza su identidad) mientras que el cliente se mantiene sin autentificar; la autentificación mutua requiere un despliegue de infraestructura de claves públicas [28](o PKI) para los clientes. Los protocolos permiten a las aplicaciones cliente-servidor comunicarse de una forma diseñada para prevenir escuchas, la falsificación de la identidad del remitente y mantener la integridad del mensaje.

SSL implica una serie de fases básicas:

- Negociar entre las partes el algoritmo que se usará en la comunicación.
- Intercambio de claves públicas y autenticación basada en certificados digitales.
- Encriptación del tráfico basado en cifrado simétrico.

Durante la primera fase, el cliente y el servidor negocian qué algoritmos criptográficos se van a usar[29]. Las implementaciones actuales proporcionan las siguientes opciones:

- Para criptografía de clave pública: RSA, Difie-Hellman, DSA (Digital Signatura Algorithm) o Fortezza.
- Para cifrado simétrico: RC2, RC4, IDEA (International Data Encryption Algorithm), DES (Data Encryption Standard), Triple DES[30] o AES (Advanced Encryption Standard).[31]
- Con funciones hash: MD5[32] o de la familia SHA.

SSL se ejecuta en una capa entre los protocolos de aplicación como HTTP, SMTP[33], NNTP y sobre el protocolo de transporte TCP, que forma parte de la familia de protocolos TCP/IP. Aunque pueda proporcionar seguridad a cualquier protocolo que use conexiones de confianza (tal como TCP), se usa en la mayoría de los casos junto

a HTTP para formar HTTPS[34]. También puede ser usado para hacer túneles en una red completa y crear una red privada virtual (VPN), como en el caso de OpenVPN[35].

1.8 Calidad de Servicio (QoS) en las VPN

Es posible definir calidad de servicio (QoS) como la posibilidad de asegurar y medir una serie de parámetros que describen el grado de servicio recibido por el usuario. Teniendo esto en cuenta, la problemática de la calidad de servicio (*QoS*) en las VPN está ligada al tipo de tecnología subyacente utilizada. Los parámetros que definen la calidad de servicio en este entorno son básicamente: ancho de banda, retardo, variación de retardo, pérdida de paquetes y disponibilidad.[36]

Las VPN sobre servicios portadores nivel 2 (ATM, FR) disfrutan de los mecanismos de estos protocolos para asegurar estos parámetros. Por tanto, la verdadera problemática, que no es exclusiva de las VPNs, reside en la capacidad de IP para ir más allá de un servicio del mejor esfuerzo (*best-effort)*.

De una manera sintética, es posible decir que existen dos aproximaciones para abordar la problemática de la calidad de servicio: el Modelo de Servicios Integrados (IntServ) y el Modelo de Servicios Diferenciados (Diffserv). El modelo IntServ adopta lo que se pude denominar “aproximación por flujo”. Se envían peticiones de reserva de ancho de banda por cada comunicación o flujo que establece. Este modelo utiliza RSVP (*Resource Reservation Protocol*) como protocolo de señalización. El requerimiento de que RSVP deba ser interpretado por el conjunto de equipos atravesados y la carga que esta señalización puede suponer sobre los mismos, ha hecho que se cuestione su capacidad para ser desplegado en grandes redes.

El Modelo DiffServ adopta lo que se puede denominar “aproximación por Clase de Servicio”. Mediante la codificación del byte ToS de los paquetes IP (rebautizado DS), en los extremos de la red se clasifican los paquetes como pertenecientes a diferentes Clases de Servicio, cada una de las cuales está caracterizada por un tratamiento diferente en el núcleo de la red. Este tratamiento hace referencia básicamente a cómo se ubican en las colas, los paquetes en diferentes *buffers*, cómo se gestionan y priorizan cada uno de ellos (*scheduling*) y qué política se sigue en caso de congestión de *buffers* (adaptación de tráfico (*shaping*), descarte selectivo).[37]

Las limitaciones de escalabilidad del modelo IntServ[38], hacen de DiffServ la opción más aceptada en el mercado. De hecho, su principio de funcionamiento es la base de

las políticas de gestión de tráfico IP (clasificación de tráfico sobre la base de parámetros, como dirección IP origen, dirección IP destino, puerto…, y tratamiento de *buffers* diferenciado) que actualmente implementan las redes. Sólo un trabajo de ingeniería de red y un dimensionamiento correcto de la misma podrán hacer que se respeten determinados valores de retardo o pérdida de paquetes.

1.9 Introducción de las VPN en Cuba

Proveedores de Acceso a Internet

El Proveedor de Acceso a Internet (ISP), desempeña un rol en las implementaciones de Redes Privadas Virtuales. Al brindar este servicio a una empresa, es el encargado de transportar todo el tráfico que entra y sale de la misma.

En el caso de Cuba existen 2 Proveedores de Servicios a Internet, según regulaciones del Ministerio de Informática y Comunicaciones (MIC), organismo rector en esta esfera. Estos proveedores, en cuanto a VPN brindan lo siguiente:

La Empresa de Telecomunicaciones de Cuba S.A. (ETECSA) con la introducción de la Red IP/MPLS esta comenzando a brindar servicios de conectividad mediante la implementación de VPN, tal es el caso del Gobierno, Organización Básica Eléctrica y el Partido

Red **CENIAl** de la Empresa CITMATEL del Ministerio de Ciencia, Tecnología y Medio Ambiente: no ofrece soluciones VPN.

Otras redes

Además de lo analizado en cuanto a lo que ofrecen los Proveedores de Servicio Internet en Cuba, es importante señalar que existen muchas redes nacionales, pero en general soportadas sobre X.25, Frame Relay, ATM y no implementan Redes Privadas Virtuales. En las consultas realizadas se arrojó que la Corporación CIMEX en su Red Privada ha implementado VPN para garantizar la seguridad de algunos de sus servicios, aunque pueden existir otras que la utilicen.

Esta última, también utiliza la tecnología VPN pero para la comunicación con empresas *partners* en el extranjero. Esta empresa tiene aplicaciones de VPN desde 1997, primero lo hacían a través de un protocolo de encapsulamiento llamado “AltaVista tunneling” pero luego por razones de seguridad se implementó sobre IPSec.

Existen otras instituciones que sobre Internet para garantizar su comunicación con otras oficinas ubicadas en el exterior del país han implementado VPN, tal es el caso del MINVEC.

1.10 Conclusiones parciales

- Las Redes Privadas Virtuales se definen como redes que se extienden, mediante procesos de encapsulamiento y de encriptación de los paquetes de datos, a distintos puntos remotos mediante el uso de infraestructuras públicas de transporte.
- Se clasifican según su uso, sobre que red pública funciona y si es implementada por software o hardware según su arquitectura.
- Existen varios protocolos para la implementación de VPN, pero resulta de mayor interés por su amplia utilización el IPSec.
- Actualmente de los dos proveedores de servicios solo ETECSA está comenzando a brindar servicios de VPN sobre IP y es muy escasa su utilización en las redes privadas.

CAPITULO 2. Estado actual de las redes en ETECSA. Caracterización del equipamiento y enlaces. Propuesta para el diseño de la VPN

En muchas ocasiones la información a transmitir en una red, es información sensible, y consecuentemente no debe ser accesible a terceros. ¿Cómo podemos transmitir información y que sólo sea accesible al transmisor y al receptor? Parece claro que los sistemas criptográficos son la solución a este problema.

En la actualidad los sistemas criptográficos están ampliamente estudiados y desarrollados, aunque queda mucho por avanzar en este campo, no impide que se utilicen en la transmisión segura de información. Hay que notar, que aunque se utilicen canales privados de comunicación, la tecnología actual, la información y los conocimientos generales están a disposición de cualquiera, por lo que comunicaciones que aparentemente pueden ser seguras como una conexión punto a punto, pueda ser interceptada por un hacker para utilizarla en su propio provecho o para realizar daños a la empresa atacada.

Si una empresa decide utilizar un sistema criptográfico para enviar información, ¿necesita implementar desde cero dichos sistemas o necesitaría aplicaciones específicas para la transmisión de estos datos? La respuesta es NO, ya que en la actualidad existen soluciones que permiten la transmisión ciertamente segura de la información.[6]

Las redes virtuales forman un túnel virtual que permite atravesar la información en cualquiera de los dos sentidos. De ahí el nombre de túnel.

La separación de la información se logra mediante la encriptación de la misma, y el sistema será más seguro, cuanta mayor seguridad nos suministre el sistema criptográfico, siendo deseable que cualquier avance significativo en el campo de la criptografía, pueda ser implementado y transferido a nuestra Red Privada Virtual.

En el caso específico de la tecnología utilizada en ETECSA y a la revisión realizada, el uso tan variado y generalizado de IPSEC como protocolo de túnel se ha escogido para la propuesta de implementación de las Redes Privadas Virtuales.[39]

2.1 Descripción de las distintas redes instaladas en la empresa

La empresa de telecomunicaciones de Cuba, cuenta con presencia en las 14 provincias y en el municipio especial Isla de la Juventud, cada uno provisto de enlaces por la Red Pública de Transmisión de Datos para dos de sus redes que operan ininterrumpidamente.

Red Corporativa: Soporta los servicios que garantizan la gestión de la información Comercial, Contable, Logística, Facturación, Cobro, Configuración de abonados y Gestión de ordenes de servicios. Es accesible desde todas las oficinas comerciales ubicadas por todo el territorio nacional.

Red de Gestión: Soporta la gestión de la tecnología de telecomunicaciones instalada, principalmente los nodos de conmutación, tráfico, abonados y otra parte de los elementos de transmisión que no van por la red de transmisión. Es accesible principalmente desde los Centro de Gestión Territoriales.

Red de Transmisión: Soporta la gestión de la tecnología de telecomunicaciones instalada, principalmente los equipos de Transmisión de la SDH y la microonda nacional. Es accesible principalmente desde los Centro de Gestión Territoriales. Esta red no está soportada por la Red Pública de Transmisión de Datos, funciona de forma independiente y tiene sus propios equipos de conectividad.

En estos momentos, este intercambio de información se realiza utilizando las posibilidades que brida el Protocolo TCP/IP. La información de las estaciones a los servidores se provee por la seguridad implementada sobre las aplicaciones, incluyendo los aspectos correspondientes a la correcta configuración de los Sistemas Operativos, Parches de Seguridad, Firewall y Antivirus.

La conectividad de cada provincia con el Nodo Central en Ciudad de la Habana se realiza utilizando el mismo enrutador pero por interfaces diferentes en el caso de la Red Corporativa y la Red de Gestión.

En el capítulo anterior se hizo alusión a las formas en que se puede implementar VPN, en este caso por las condiciones actuales y en principio la no disponibilidad de equipamiento para cada nodo provincial y tomando en consideración los requerimientos ya descritos en este capitulo referente al protocolo IPSEC como soporte para encriptamiento y autenticación lo mas conveniente es lograr que de extremo a extremo de los equipos de conectividad la información viaje encriptada.

2.2 Caracterización de los distintos equipos de conectividad instalados.

2.2.1 Tecnología CISCO

En el ambiente de los equipos de conectividad de las redes en la empresa ETECSA ha existido una tendencia a la utilización de tecnología CISCO por existir representación de un tercero que garantiza la asistencia técnica.

Cisco en 1993 abordó una iniciativa para diseñar redes prácticas, costos-eficientes para las escuelas, rápidamente se percató que diseñar e instalar las redes no era suficiente. Las escuelas también necesitaban dar mantenimiento a esas redes y el personal de la institución carecía de tiempo y recursos. Un ingeniero dedicado de Cisco empezó a enseñar a los estudiantes cómo dar mantenimiento a sus redes. Las escuelas a través de los Estados Unidos solicitaron programas similares y en respuesta a estas peticiones, Cisco desarrolló un curriculum opcional para los estudiantes, que fue la base de Cisco Networking Academy Program. El programa, lanzado en Octubre de 1997, empezó con 64 instituciones educativas en siete estados: Arizona, California, Florida, Minnesota, Missouri, Nueva York y Carolina del Norte y por la rápida utilización en la actualidad se encuentra desplegada por toda la geografía mundial.

Actualmente para garantizar la interconexión de la Red en cada provincia funciona un router cisco 3640 cuyas prestaciones están muy por encima de la utilización actual.

Características principales del Router CISCO 3640. Véase Anexo I.

Procesador: R4700 100 MHz RISC.

Memoria RAM: 32 MB

Memoria Flash: 8 MB

Algoritmo de cifrado: DES/3DES.

Requiere actualización de la versión de IOS (Sistema Operativo)

2.2.2 Tecnología Huawei

En las condiciones actuales donde las relaciones con China se ha fortalecido la tendencia a la utilización de tecnología procedente de este país se ha incrementado

sustancialmente, actualmente se han introducido una variedad de equipos de acceso a las redes a nivel de usuario, redes y tecnología de acceso de banda ancha.

Huawei ha estado operando en 13 países en América Latina: Argentina, Chile, Uruguay, Colombia, Venezuela, México, Ecuador y Brasil. La compañía ha escogido Brasil como la oficina matriz para América Latina y ha estado en el país desde 1999. En un corto período de tiempo, Huawei ha sido señalado como uno de los principales jugadores del mercado. [40]

Características principales del Router AR 28. Véase Anexo III.

Memoria Boot ROM: 512 KB

Memoria SDRAM: 128MB

Máximo SDRAM: 128MB

Memoria Flash: 32MB

Encriptación IPSec para creación de VPN

2.2.3 Tecnología de Juniper Networks

Juniper Networks es el proveedor líder en ofrecer comunicaciones seguras y fiables sobre una red IP única. Las plataformas IP personalizadas de alto rendimiento de la compañía, permiten a sus clientes dar soporte a múltiples servicios y aplicaciones. Proveedores de servicios, empresas, entidades gubernamentales e instituciones de educación e investigación de todo el mundo confían en Juniper Networks para comercializar productos con los que construir redes que se adapten a las necesidades de sus clientes, servicios y aplicaciones. La gama de soluciones de redes y seguridad de Juniper Networks soportan las demandas complejas de escalabilidad, seguridad y rendimiento de las redes críticas más exigentes del mundo.

Juniper Networks y el logo de Juniper Networks son marcas comerciales registradas de Juniper Networks, Inc. en los Estados Unidos y otros países.

Características principales del Firewall / IPSec VPN SSG-550M-SH. Véase Anexo II.

Protocolo de interconexión de datos	Ethernet, Fast Ethernet, Gigabit Ethernet, HDLC, Frame Relay, PPP, MLPPP, FRF.15, FRF.16
Red / Protocolo de transporte	NetBEUI/NetBIOS, L2TP, IPSec, PPPoE
Protocolo de direccionamiento	OSPF, RIP-1, RIP-2, BGP, IGMPv2, IGMP, PIM-SM, direccionamiento IP estático, PIM-SSM
Protocolo de gestión remota	SNMP 2, SNMP, Telnet, HTTP, HTTPS
Rendimiento	Capacidad 3DES : 300 Mbps Capacidad del cortafuegos (paquetes grandes) : 650 Mbps o más Capacidad del cortafuegos (IMIX) : 600 Mbps
Capacidad	Sesiones concurrentes : 64000 Políticas de seguridad : 1000 Conexión / cantidad de usuarios : ilimitado Usuarios autentificados (base de datos interna) : 1500 Túneles VPN concurrentes : 500 Interfaces de túnel VPN : 100 Zonas de seguridad : 60 Rutas estáticas : 20000

En la actualidad existen otros fabricantes dedicados al desarrollo de equipamiento para VPN con gran variedad de modelos para los distintos entornos empresariales. Véase Anexo IV.

2.3 Guía para la propuesta de las VPN

2.3.1 Etapa 1. Necesidad de la implementación de la Red Privada Virtual

Paso 1 Definir la VPN a implementar.

Se define a partir del estudio de las redes independientes existente y de las proyecciones actuales de la Empresa.

Paso 2 Definir dónde están los extremos de la VPN.

Se define en qué lugares estarán los extremos de la VPN y el Listado de Sitios que formarán la extranet.

Paso 3 Definir tamaño de la red.

Se define a partir de la cantidad de usuarios en el Directorio Activo de la Red Corporativa de cada Provincia. Es un criterio que permite obtener cantidad de usuarios.

Paso 4 Definir los servicios que formarán parte de la VPN.

Para ganar en claridad de la necesidad de la empresa de implantar una Red Privada Virtual, es importante obtener un listado de los servicios que necesitan la VPN y el nivel de seguridad que estos requieren. Estos puede que se estuvieran brindando hasta ese momento o que se proyecten para el futuro de la empresa. Véase Tabla 1

No	Servicio	Descripción	Seguridad requerida
1	....		
2	....		
3	....		

Tabla 1 Listado de Servicios que se implantarán con la VPN

Paso 5 Calcular los costos de los servicios, sin la VPN.

Partiendo de los enlaces disponibles y su situación, se deben obtener los costos de cada uno ellos y el costo total por ese concepto.

2.3.2 Etapa 2. Diseño de la Red Privada Virtual

Paso 6 Decidir el protocolo de encapsulamiento a utilizar.

A partir de la posibilidad del equipamiento disponible y sus características se define el protocolo de encapsulamiento que se debe utilizar. Además hay que tener en cuenta la convergencia de los protocolos de encriptamientos actuales. Se recomienda IPSec.

Paso 7 Definir parámetros del protocolo IPSec. [41]

Se recomiendan los siguientes valores para los parámetros de IPSec. Véase Tabla 2.

Parámetro	Valor recomendado
Encriptación de los datos	AES o 3DES

Integridad de los datos	SHA
Llave de Asociaciones de Seguridad (SA)	Llaves pre-compartidas
IKE	3DES
Diffie-Hellman	Grupo 2 (1024 bits)
Modo	Túnel

Tabla 2 Parámetros recomendados de IPSec.

Esos son los valores recomendados, pero no siempre será necesario configurarlos todos, pues dependerá de otras decisiones que se tomaran en pasos posteriores.

Paso 8 Definir el mecanismo de autenticación en el extremo red.

Para VPN IPSec redes a redes, hay dos métodos de autenticación en los extremos: las llaves pre-compartidas (IKE) y los certificados digitales (PKI). Por tanto se debe escoger entre ambos métodos.

Con las llaves pre-compartidas, dos o más extremos de la red (por ejemplo pasarelas VPN) intercambian de forma segura (*pre-share*) una clave secreta previa a la negociación del cualquier túnel.

La ventaja de usar las llaves pre-compartidas es que constituyen una manera relativamente rápida y barata de implementar la autenticación de un extremo de red. La desventaja es que no es muy escalable. Los certificados son una opción más escalable para la autenticación del extremo de red; sin embargo, ellos o requieren la implementación de una autoridad de certificado (CA) o la compra de certificados a una tercera CA.

Paso 9 Esquematizar la topología de la red existente.

Con el objetivo de colocar luego los dispositivos VPN, que se incorporarán es importante obtener un esquema de la topología actual, especificando el hardware y el software que se utiliza hasta ese momento.

Paso 10 Definir los dispositivos para implementar la VPN.

Se determinan los dispositivos que serán utilizados para implementar las VPN. (Pasarelas VPN, Cortafuegos, Router, Autenticador de conexiones)

Paso 11 Esquematizar la topología de la nueva red.

Luego de tomar estas decisiones es posible realizar el esquema de la topología de la nueva red.

Paso 12 Definir niveles de redundancia.

Se debe considerar la redundancia dentro del propio dispositivo en forma de dobles componentes críticos (las fuentes de alimentación y unidades centrales) o redundancia entre dos pasarelas VPN para el caso de fallo del dispositivo completo. En esta decisión influirá el aspecto económico. Puede decidirse no incluir redundancia en el desarrollo inicial, sino que incluirla a medida que crece la red.

El modo de fallos más probable está en el camino de la red al hardware mismo, en consecuencia, se deben utilizar protocolos de redundancia de enrutamiento convencionales como el *Border Gateway Protocol* (BGP).

Paso 13 Realizar análisis costo beneficio.

Calcular los costos de los servicios sin la VPN y con la VPN. Se debe realizar un análisis costo-beneficio para tener una idea aproximada de lo que ahorrará la empresa cuando la instale.

Paso 14 Analizar la escalabilidad.

Analizar cuan escalable será el diseño que se obtiene, hasta donde podrá crecer la red, que recursos serán necesario para ese crecimiento y qué lo limita.

2.3.3 Etapa 3. Implementación de la Red Privada Virtual

La implementación depende en gran medida de la solución que se haya escogido pues la configuración cambia según el software o hardware que se instale. Parte de la base de que los sistemas operativos y equipos funcionando tienen configurados los elementos de red. En líneas generales es necesario seguir los siguientes pasos:

Paso 15 Instalar y configurar el hardware.

Paso 16 Revisar las listas de acceso de los extremos.

Paso 17 Si se decidió utilizar Certificados Digitales, es necesario implementar la autoridad de Certificación o utilizar una ya implementada.

Paso 18 Establecer el enlace extremo-extremo.

2.4 Conclusiones parciales

Tomando en cuenta las principales características de los equipos de conectividad utilizados en las redes de Gestión y Corporativas de la empresa ETECSA y luego de un análisis se obtiene una guía para implantar una VPN formada por tres etapas:

- Etapa 1. Necesidad de la implementación de la Red Privada Virtual.
- Etapa 2. Diseño de la Red Privada Virtual.
- Etapa 3. Implementación de la Red Privada Virtual.

La guía obtenida no se ajusta a ningún vendedor, sino que constituye una orientación general que deja espacios, en muchos casos, a decisiones de quien la aplica aunque siempre recomienda qué parámetro o elemento seleccionar. Además esta guía incluye elementos que no están presentes en otras, entre los que se encuentra el análisis de los costos de la implementación y que se adaptan a las condiciones y necesidades actuales de conectividad de ETECSA no solo en su propia red sino tomando en cuenta sus necesidades de diversificación en su cartera de servicios como proveedor de Internet del país.

CAPITULO 3. Propuesta de implementación de la VPN en ETECSA aprovechando el uso del equipamiento y enlaces disponibles

Se propone la implementación de VPN desde el Nodo Central en Ciudad de la Habana a cada nodo provincial como solución para lograr la conectividad de una forma más segura, cuestión esta vital por la naturaleza de la información que se maneja. Se analiza la tecnología instalada y los enlaces existentes optimizando su uso y proponiendo modificaciones en correspondencia con las necesidades actuales.

La etapa de implementación no incluye pruebas al no estar concebidas para esta etapa. Requiere de la disponibilidad del equipamiento y enlaces, además de capacitación necesaria para cada especialista de los nodos principales.

A continuación se describen varias etapas para garantizar los estudios necesarios a realizar para lograr una implementación lo mas acorde posible con los objetivos propuestos.

3.1 Diseño de las VPN.

3.1.1 Condiciones de aplicación.

Utilización de los router 3640 ubicados en cada provincia (Ver Anexo 1).

Utilizar el Firewall NetScreen SSG-550M-SH existente en la Habana con la posibilidad de implementar VPN.

Extremos de la VPN: Extremo en cada provincia y el municipio especial Isla de la Juventud con extremo en Ciudad Habana como concentrador de las redes.

3.1.2 Aplicación de la Etapa 1

Paso 1 Definir la VPN a implementar.

Se propone una VPN por la que se encripten los paquetes correspondientes a las aplicaciones que por su nivel de seguridad lo requiera. La información correspondiente a las aplicaciones que no necesiten de encriptamiento se enrutarán normalmente según listas de accesos definidas anteriormente.

Paso 2 Definir dónde están los extremos de la VPN

Extremos de la VPN:

	Institución	**Localización Física**	**ISP**
Extremo Principal	ETECSA, Nodo Buenavista	Ciudad de la Habana.	ENET
Extremo 1	Dirección Territorial ETECSA, Pinar del Río	Pinar de Río	ENET
Extremo 2	Dirección Territorial ETECSA, Provincia Habana	Ciudad Habana	ENET
Extremo 3	Dirección Territorial ETECSA, Matanzas	Matanzas	ENET
Extremo 4	Dirección Territorial ETECSA, Cienfuegos	Cienfuegos	ENET
Extremo 5	Dirección Territorial ETECSA, Villa Clara	Santa Clara	ENET
Extremo 6	Dirección Territorial ETECSA, Santi Spiritus	Santi Spiritus	ENET
Extremo 7	Dirección Territorial ETECSA, Ciego de Ávila	Ciego de Ávila	ENET
Extremo 8	Dirección Territorial ETECSA, Camaguey	Camaguey	ENET
Extremo 9	Dirección Territorial ETECSA, Tunas	Tunas	ENET
Extremo 10	Dirección Territorial ETECSA, Holguín	Holguín	ENET
Extremo 11	Dirección Territorial ETECSA, Granma	Bayamo	ENET
Extremo 12	Dirección Territorial ETECSA, Santiago de Cuba.	Santiago de Cuba	ENET

Extremo 13	Dirección Territorial ETECSA, Guantánamo	Guantánamo	ENET
Extremo 14	Dirección Territorial ETECSA, Isla de la Juventud.	Isla de la Juventud	ENET

Tabla 1 Listado de Sitios

Paso 3 Definir tamaño de la red.

Tamaño de la Red Corporativa: Mediana (hasta 500 usuarios simultáneamente). Se obtiene a partir de la cantidad de usuarios máximos en el directorio activo de cada Dirección Territorial.

Tamaño de la Red de Gestión: Pequeña (hasta 20 usuarios simultáneamente).

Tamaño de la Red de Transmisión: Pequeña (hasta 5 usuarios simultáneamente).

Paso 4 Definir los servicios que formarán parte de la VPN.

Red Corporativa.

No	Servicio	Descripción	Seguridad requerida
1.	Acceso al Sistema de Contabilidad y Finanzas	Sistema de Gestión Económico	Alta
2.	Acceso al Sistema de facturación	Sistema de gestión de facturas y procesos de facturación	Alta
3.	Acceso al Sistemas de Recarga de Tarjetas Telefónicas	Sistemas de Recarga de Tarjetas Telefónicas de la plataforma propia (160 y 166)	
4.	Acceso al sistema de Cobro de los Servicios	Sistema de gestión de cobro	Alta
5.	Acceso al sistema de gestión y configuración de de servicios telefónicos.	Gestión y configuración de los servicios telefónicos que se le brindan a los clientes	Alta
6.	Acceso a los sistemas de gestión y supervisión	Sistemas de Antivirus, Parches, Trazas, supervisión de eventos de	Alta

	que soportan la Red	seguridad.	

Red Gestión.

No	Servicio	Descripción	Seguridad requerida
1	Acceso al sistema de gestión y configuración de de servicios telefónicos.	Gestión y configuración de los servicios telefónicos que se le brindan a los clientes	Alta
2	Acceso a la gestión y supervisión de las centrales telefónicas y de sistemas de transmisión.	Sistemas de gestión de las centrales y nodos de transmisión	Alta
3	Acceso a la información de facturación	Información para generar las facturas de los abonados	Alta

Red Transmisión.

No	Servicio	Descripción	Seguridad requerida
1	Acceso a los sistemas de gestión y configuración de los equipos de transmisión.	Gestión y configuración de los equipos de transmisión.	Alta

Todos los servicios antes descritos requieren ser asegurados.

Paso 5 Calcular los costos de los servicios, sin la VPN.

En consultas realizadas a la Filial de Datos de ETECSA no se obtiene el precio a comercializar 5Mbit/s, aparece como velocidad máxima 2 Mbit/s a 2120 CUC. En el caso 128 Kbits/s a 600 CUC y 512 Kbits/s a 1300 CUC. Teniendo en cuenta 5 Mbits/s podría estimarse en entre unos 4000 o 5000 CUC.

3.1.3 Aplicación de la Etapa 2

Paso 6 Decidir el protocolo de encapsulamiento a utilizar.

Se usará IPSec por la tendencia de su uso en los distintitos equipos de conectividad (Router, Concentradores VPN) como solución de encriptamiento para la seguridad de los datos y por ser un protocolo integrado a IPv6, garantizando sin ninguna dificultad la migración de IPv4 a IPv6.

Paso 7 Definir parámetros del protocolo IPSec

Se utilizarán los parámetros de IPSec que se recomiendan. La encriptación de los datos se hará con el algoritmo 3DES, ambas tecnologías disponibles Cisco y NetScreen lo soportan.

Paso 8 Definir el mecanismo de autenticación en el extremo red

Se utilizaran claves precompartidas en esta etapa inicial.

Paso 9 Esquematizar la extensión de la red existente.

En la figura 5 se muestra el alcance la Red Corporativa y su extensión a las distintas provincias. Se utilizan Router Cisco 3640.

Figura 5 Red Corporativa (Velocidad del enlace a 5 Mbit/s**)**

En la figura 6 se muestra el alcance la Red de Gestión y su extensión a las distintas provincias. Se utilizan Router Cisco de la serie 2100 principalmente.

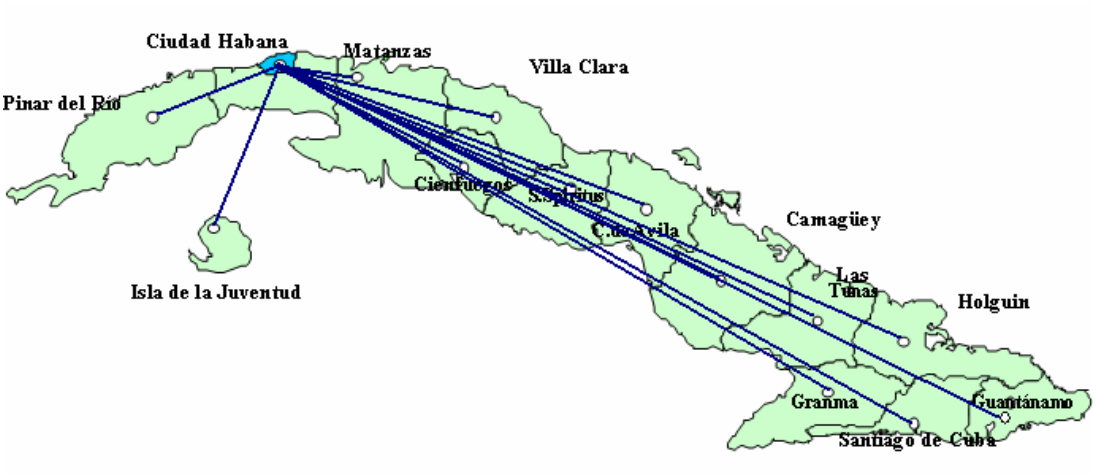

Figura 6 Red de Gestión de las Telecomunicaciones (Velocidad del enlace a 512 Kbit/s)

En la figura 7 se muestra el alcance la Red de Transmisión y su extensión a las distintas provincias. Se utilizan Router Cisco principalmente, aunque puede encontrarse la utilizacion de Router Huawei.

Figura 7 Red de Transmisión (Velocidad de enlaces a 2 Mbit/s con los centros concentradores y de estos a los demás a 128 Kbit/s)

Como se puede apreciar para el caso de la Red de Gestión y la Corporativa se representan de igual forma, la diferencia radica en que cada uno utiliza un enlace independiente. La red de Transmisión concentra en tres regiones y de ahí al nodo en Ciudad Habana.

Paso 10 Definir los dispositivos VPN a utilizar.

Firewall Netscreen SSG-550M

Enrutador Cisco 3640

Paso 11 Esquematizar la topología de la nueva red

Luego de tomar estas decisiones es posible realizar el esquema de la topología de la nueva red. Quedando de esta manera integrada las tres redes a un enlace de 7 Mbits/s como propuesta para poder evacuar todo el tráfico. En ancho de banda hay que observarlo para prever su crecimiento en la medida que los servicios lo requieran. Se propone la utilización de los Router CISCO 3640 existentes y la actualización de su sistema operativo para soporte VPN(Véase Figura 8)

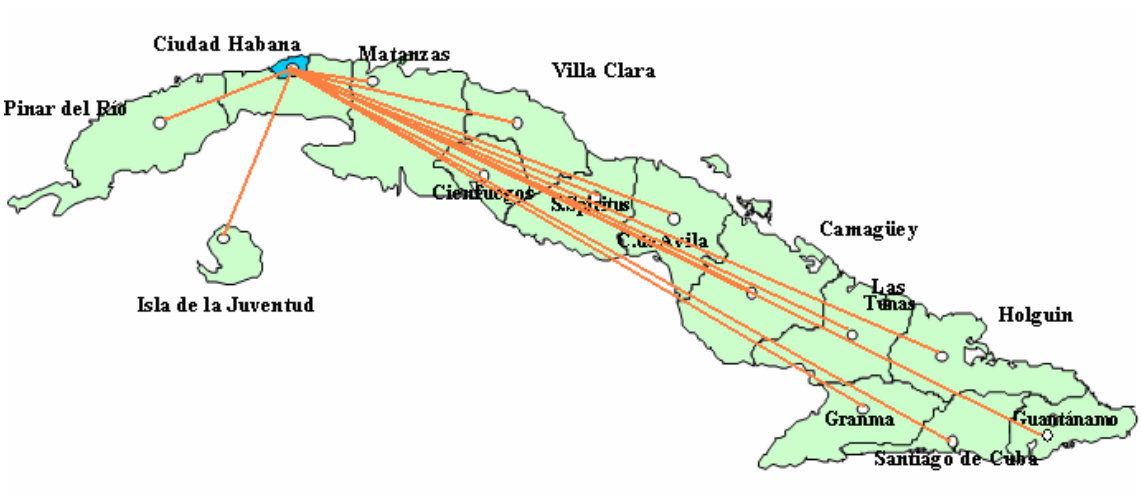

Figura 8 Red Integrada para solución VPN.

Paso 12 Definir niveles de redundancia

Por razones económicas, no se incluirá hardware redundante en esta etapa y se utilizará la que se provee por defecto la Red Pública de Trasmisión de Datos.

Paso 13 Realizar análisis costo beneficio

El mayor beneficio que las VPN propuesta le aporta ETECSA es la posibilidad de contar con un medio de comunicación más eficiente y sobre todo **más seguro** y de realizar la comunicación por un mismo enlace de comunicación; teniendo en cuenta las prestaciones de los equipos instalados de restringir el ancho de banda para cada VPN en correspondencia con la necesidad de cada red. A pesar de estos beneficios

se incrementa el tráfico por conceptos de incrementos de paquetes de autenticación y encabezamientos no disponibles anteriormente.

Paso 14 Analizar la escalabilidad

En el diseño propuesto utilizando IPSec es perfectamente posible la utilización de otra tecnología que no sea Cisco o de integrarla a esta, como es el caso de los equipos de Huawei, ya sea Firewall que implementan VPN o de enrutadores que hoy son cada vez mas utilizados y adquirido por la empresa para la Red de Transmisión de Datos o para la implementación de las NGN para los servicios integrados de voz, datos y videos sobre IP, con la seguridad y calidad de servicio en correspondencia con los niveles definidos. Por otra parte se garantiza la incorporación de nuevas redes con solo tener que aumentar el ancho de banda si es necesario.

3.1.4 Aplicación de la Etapa 3

La implementación depende en gran medida de la solución que se haya escogido pues la configuración cambia según el software o hardware que se instale. Se toma como punto de partida de que, los sistemas operativos y equipos están funcionando y que tienen configurados los elementos de red. En líneas generales es necesario seguir los siguientes pasos:

Paso 15 Instalar y configurar el hardware.

Se configuran los equipos de los extremos de cada provincia con el segmento de red seleccionado para crear el túnel y el del Nodo central de Ciudad Habana. Se permite el encaminamiento de la información que no necesita de encriptamiento.

Paso 16 Revisar las listas de acceso de los extremos.

Es imprescindible permitir que los paquetes IPSec puedan entrar y salir al *gateway*.
Por tanto es necesario permitir:

- IKE: UDP puerto 500
- ESP: UDP puerto 50
- AH: UDP puerto 51

Paso 17 Si se decidió utilizar Certificados Digitales, es necesario implementar la autoridad de Certificación o utilizar una ya implementada.

No se utilizarán certificados digitales por lo engorroso que resulta el tema de acuerdo a las regulaciones de los órganos competentes en esta materia y por no considerarse dada las condiciones existentes en la empresa para esta primera etapa.

Paso 18 Establecer el enlace extremo-extremo.

Habilitar el enlace solicitado por la Red Pública de 7 Mbit/s para garantizar el flujo de las tres redes de interés.

3.2 Conclusiones parciales

Se diseñó una Red Privada Virtual a partir de la guía propuesta; que resuelve, de una forma segura, los problemas de conectividad con las provincias, utiliza un solo enlace, el mismo equipamiento instalado y permite de forma flexible incorporar nuevas redes con el menor costo de instalación y administración.

Aplicar la guía permitió realizar el diseño y la propuesta de implementación de la VPN de una manera rápida y organizada, proporcionando una secuencia de pasos a seguir para facilitar la tarea.

CONCLUSIONES

- Se estudiaron de las diferentes alternativas de redes privadas virtuales con una importante búsqueda bibliográfica
- A partir del equipamiento instalado se logró definir el protocolo IPSEC como el más adecuado para la implementación de seguridad de red.
- La guía obtenida le permite haciendo uso de cada uno de sus pasos proponer una VPN que pudiera adaptarse a otro entorno empresarial.
- La diversidad de tecnología para la implementación de VPN deja muchas aristas de investigación para proponer otros equipamientos de acuerdo a aspectos de factibilidad económica que permitan ser alternativas en caso de afectación de los existentes o por razones reales ante el bloqueo económico impuesto al país.
- Se logra un nivel de encriptación que permite dar un nivel adecuado de seguridad a la información que viaja por la red y que en verdad lo requiere.
- Se integran las redes y liberan de esta forma el equipamiento instalado en otras dos que puede ser utilizado como respaldo o en otras implementaciones.
- Se considera necesario encriptar solo la información que por su seguridad lo requiere.

RECOMENDACIONES

- Incluir en la Guía propuesta una Etapa de Prueba e implantación de la VPN.
- Incluir en la Guía propuesta una Etapa de Monitoreo y Supervisión de la VPN.
- Difundir y aplicar la guía entre las empresas cubanas que requieran de esta tecnología.
- Proponer a la Unidad de Negocios de Tecnología y Software que se implemente esta alternativa como solución integrada de seguridad de las redes existentes y en respuesta a las solución de vulnerabilidades detectadas.

REFERENCIAS BIBLIOGRAFICAS

1. Ramiro J. Caire. *Introducción alas Redes Privadas Virtuales sobre GNU/LINUX*. 2003 [consultado 2007].
2. Didier Fallas. *VPN (Redes Virtuales Privadas)*. 2006 [consultado 2007]; en: http://www.internexo.co.cr/blog/2006/07/vpn-redes-virtuales-privadas.html.
3. Roselló, V.J.A. *Implementación de Redes Privadas Virtuales (VPN) utilizando el protocolo IPSec*. 2002 [consultado 2007]; en: http://beta.redes-linux.com/manuales/vpn/trabajo.pdf.
4. Gómez Valdivia Javier Rafael. *Redes Privadas Virtuales(VPN)*. 2006 [consultado 2007]; en: http://telematica.cicese.mx/revistatel/archivos/Telem@tica_AnoIII_No22.pdf.
5. Wikipedia. *Red privada virtual*. 2007 [consultado 2007]; en: http://es.wikipedia.org/wiki/Red_privada_virtual.
6. Fernández Hernández Jesús, J.L.A.B., Carlos G.-Figuerola Paniagua, Ángel F. Zazo Rodríguez. *Redes Privadas Virtuales*. 2006 [consultado 2007]; en: http://reina.usal.es/pub/fernandez2006redes.pdf.
7. WORLD METEOROLOGICAL ORGANIZATION. *Guide for Virtual Private Networks (VPN) via the Internet between GTS centres*. 2004 [consultado Febrero 2007]; en: http://www.wmo.ch/web/www/TEM/ICT-ISS2002/guideVPN.doc.
8. Soulari Torres Litza, *Recomendaciones para la implantación de una Red Privada Virtual que brinde seguridad a la información intercambiada*. 2003, ISPJAE.
9. Microsoft. *Configuración común de un servidor VPN*. 2007 [consultado 2007]; en: http://www.microsoft.com/winwdows/windows200/es/server/help/sag_sag_VPN_usa.htm.
10. Microsoft. *VPN basadas en intranet*. 2007 [consultado 2007]; en: http://microsoft.com/technet.
11. 3com Tecnology. *Características y ventajas de las VPN*. 2007 [consultado 2007]; en: www.3com.com.
12. CISCO SYSTEMS. *Seguridad y VPN-Soluciones Tecnológicas*. 2007 [consultado 2007]; en: www.cisco.com/web/es/solutions/ent/avvid_solutions/vpn_home.html.

13. Microsoft. *Introducción a la serie de soluciones de Informáticas para empresas*. 2007 [consultado 2007]; en: http://www.microsoft.com/spain/technet/mediana/51-250/intro/mit_intro_3.mspx.
14. Grupo de Software Libre Peru. *VPN con Linux*. 2007 [consultado 2007]; en: http://infoacceso.upv.es/english/accpub/linux/vpnlinux.htm.
15. Alexander Moldovyan, N.M., Doug Summerville, ladimir Zima, ed. *Protected Internet, Intranet, & Virtual Private Networks*. 2003.
16. CISCO SYSTEMS. *Migración a IP VPN genera ahorros hasta de un 60%* 2007 [consultado 2007]; en: http://www.ciscoredaccionvirtual.com/redaccion/titulares/default.asp?Id=268.
17. Hitachi Software Engineering. *VPN Implementation*. 2006 [consultado Febrero 2007]; en: http://www.hitachi-soft.com/tsg/services/security/vpn.html.
18. Logic Linux. *Redes Privadas Virtuales - VPN*. 2007 [consultado 2007]; en: http://www.logiclinux.com/content/view/35/64/lang,es.
19. IETF. *Cisco Layer Two Forwarding (Protocol) "L2F",*. 1998 [consultado 2007]; en: tools.ietf.org/html/rfc2341.txt
20. Network Working Group, IETF. *Point-to-Point Tunneling Protocol - PPTP*. 1999 [consultado 2007]; en: http://www.ietf.org/rfc/rfc2637.txt.
21. IETF. *IETF Web Site*. 2007 [consultado 2007]; en: www.ietf.org.
22. W. Townsley, Cisco Systems. *Layer Two Tunneling Protocol - L2TP*. 2002 [consultado 2007]; en: http://www.ietf.org/rfc/rfc3438.txt.
23. Naganan Doraswamy; Dan Hankings, *IPSec - The New Security Standard for the Internet Intranets and VPN - 2nd Edition*. 2003.
24. IPSEC Working Group. *IPSEC*. 2002 [consultado 2007]; en: http://www.ietf.org/html.charters/ipsec–charter.html.
25. D. Harkins, D. Carrel, Cisco Systems. *The Internet Key Exchange (IKE)*. 1998 [consultado 2007]; en: http://www.rfc-editor.org/rfc/rfc2409.txt.
26. IETF. *The TLS Protocol*. 1999 [consultado 2007]; en: http://www.ietf.org/rfcc/rfc2246.txt.
27. Microsoft. *Secure Socket Layer*. 2007 [consultado 2007]; en: http://www.windowsecurity.com/artcles/Secure_Socket_Layer.html.
28. IETF. *Internet X.509 Public Key Infrastructure. Certificate Policy and Certification Practices Framework*. 1999 [consultado 2007]; en: http://www.ietf.org/rfc/rfc2527.txt.
29. AGUIRRE JORGE RAMIO, *LIBRO ELECTRÓNICO DE SEGURIDAD INFORMÁTICA Y CRIPTOGRAFÍA*. 2006.

30. IEEE. *Ciencia y Tecnología de la Información III-DES*. 2007 [consultado 2007]; en: http://ieee.udistrital.edu.co/concurso/ciencia_tecnologia_info_3/des_1.html.
31. P. Chown. *Advanced Encryption Standard*. 2002 [consultado 2007]; en: http://www.faqs.org/rfcs/rfc3268.html.
32. Rivest, R. *MD5 Algorithm*. 1992 [consultado 2007]; en: http://www.rfc-editor.org/rfc/rfc1321.txt.
33. Postel, J.B. *Simpme Mail Transfer Protocol*. 1982 [consultado 2007]; en: http://www.rfc-editor.org/rfc/rfc0821.txt.
34. IETF. *HTTP Over TLS*. 2007 [consultado 2007]; en: http://www.rfc-editor.org/rfc/rfc2818.txt.
35. OpenVPN Solutions LLC. *OpenVPN*. 2007 [consultado 2007]; en: http://openvpn.net/.
36. Marcelo Andino. *Enrutamiento, Movilidad y Calidad de Servicio en IPv6*. 2006 [consultado 2007; en: http://www.lacnic.net/ipv6tour/docs/p-suarez-ipv6.ppt.
37. Jorge Escribano Salazar. *Diffserv como solucion a la provision de QoS en Internet*. 2007 [consultado 2007]; en: http://www.it.uc3m.es/garcia/articulos/cita2002_diffserv.pdf.
38. Claudia Jacy Barenco Abbas. *Modelo IntServ/Protocolo/RSVP*. 2005 [consultado 2007]; en: http://www.redes.unb.br/material/aprc_osdi/rsvp.pdf.
39. Network Working Group. *A Framework for IP Based Virtual Private Networks*. 2000 [consultado 2007]; en: http://tools.ietf.org/html/rfc2764.
40. Huawei. *Huawei América Latina*. 2007 [consultado 2007]; en: http://www.huawei.com/es/catalog.do?id=321.
41. Izura Altadill Xabier Pello. *Iptables*. 2005 [consultado Febrero 2007]; en: http://www.monografias.com/trabajos25/iptables/iptables.zip.
42. CISCO SYSTEMS. *Soluciones de acceso multiservicio. Series Cisco 3600 y 2600*. 2007 [consultado 2007]; en: http://www.cisco.com/application/pdf/en/us/guest/products/ps274/c1031/ccmigration_09186a00800889d9.pdf.

GLOSARIO

ATM	Modo de transferencia asíncrono (asynchronous transfer mode)
DES	Estándar de encriptación de datos (Data Encryption Standard)
3DES	Tres Estándar de encriptación de datos (3 Data Encryption Standard)
Firmware	Instrucciones de software establecidas de forma permanente o semipermanente en la memoria ROM.
Gateway	Puerta de Enlace
IETF	Grupo Especial sobre Ingeniería de Internet (internet engineering task force)
IP	Protocolo de Internet (internet protocol)
IPSec	Protocolo de seguridad IP (IP security protocol)
ISP	Proveedor de Servicios de Internet (Internet service provider)
ITU	Unión Internacional de Telecomunicaciones (International Telecommunnication Union)
L2F	Envío a Nivel 2(Layer 2 Forwarding)
L2TP	Protocolo de Tunelización de Nivel 2 (Layer 2 Tunneling Protocol)
LSP	Trayecto Conmutado de Etiquetas (Label Switched Path)
MPLS	Conmutación de Etiqueta de Multiprotocolo (Multiprotocol Label Switching)
OSI	Interconexión de sistemas abiertos (open systems interconnection)
PPP	Protocolo Punto a Punto (Point to Point Protocol)
QoS	Calidad de servicio (quality of service)
RFC	Solicitud de comentarios (Request for Comments)
RPV	Red privada virtual
SNMP	Protocolo de gestión de red simple (simple network management protocol)
SSL	Capa de zócalo segura (secure socket layer)
VPN	Red Privada Virtual (virtual private network)
SSL/TLS	Secure Sockets Layer/Transport Layer Security

ANEXOS

Anexo I. Características del Router CISCO 3640

General	
Tipo de dispositivo	Encaminador
Factor de forma	Montable en bastidor - modular
Cantidad de módulos instalados (máx.)	3 (instalados) / 4 (máx.)
Anchura	44.5 cm
Profundidad	40 cm
Altura	8.7 cm
Peso	13.6 kg

Procesador	
Tipo	1 x IDT R4700 100 MHz RISC
Cantidad máxima soportada	1

Memoria	
Memoria RAM	32 MB (instalados) / 128 MB (máx.) - SIMM 72-PIN
Memoria Flash	16 MB (instalados) / 32 MB (máx.)

Conexión de redes	
Tecnología de conectividad	Cableado
Velocidad de conexión	E-1
Velocidad de transferencia de datos	100 Mbps
Protocolo de interconexión de datos	Ethernet, Fast Ethernet
Modo comunicación	Semidúplex, dúplex pleno
Indicadores de estado	Actividad de enlace, velocidad de transmisión del puerto, modo puerto duplex
Características	Capacidad duplex, activable
Cumplimiento de normas	IEEE 802.3, IEEE 802.3u
Algoritmo de cifrado	DES/3DES

Comunicaciones	
Tipo	2 x módem (digital)
N° de puertos digitales	60

Expansión / Conectividad	
Total ranuras de expansión (libres)	2 (2) x PC Card 6 (3) x Ranura de expansión 4 memoria - SIMM 72-PIN 2 memoria - SIMM 80-PIN
Interfaces	1 x red - auxiliar - RJ-45 - 1 1 x gestión - consola - RJ-45 - 1 1 x red - Ethernet 10Base-T - RJ-45 - 1 1 x red - Ethernet AUI - D-Sub de 15 espigas (DB-15) - 1

Diverso	
Cables (Detalles)	1 x cable de datos
Kit de montaje	Incluido
Kit de montaje en bastidor	Incluido
Cumplimiento de normas	Certificado FCC Clase B

Alimentación	
Dispositivo de alimentación	Fuente de alimentación - interno
Voltaje necesario	CA 100/240 V (50/60 Hz)
Potencia suministrada	140 vatios

Software / Requisitos del sistema	
OS prorporcionado	Cisco IOS IP only 12.0(7)XK 8 MB 32 MB
Software incluido	Controladores y utilidades

Garantía del fabricante	
Servicio y mantenimiento	3 mes de garantía
Detalles de Servicio y Mantenimiento	Garantía limitada - piezas y mano de obra - 3 mes - introducir

Parámetros de entorno	
Temperatura mínima de funcionamiento	0 °C
Temperatura máxima de funcionamiento	40 °C
Ámbito de humedad de funcionamiento	5 - 95%

Anexo II. Características del Firewall / IPSec VPN SSG-550M-SH

General	
Tipo de dispositivo	Aparato de seguridad
Altura (unidades de bastidor)	2U
Dispositivos integrados	Panel led
Cantidad de módulos instalados (máx.)	0 (6)
Anchura	44.3 cm
Profundidad	53.7 cm
Altura	8.74 cm
Peso	10.4 kg

Procesador / Memoria / Almacenamiento	
RAM instalada (máx.)	1 GB

Conexión de redes	
Factor de forma	Externo
Tecnología de conectividad	Cableado
Protocolo de interconexión de datos	Ethernet, Fast Ethernet, Gigabit Ethernet, HDLC, Frame Relay, PPP, MLPPP, FRF.15, FRF.16
Red / Protocolo de transporte	NetBEUI/NetBIOS, L2TP, IPSec, PPPoE
Protocolo de direccionamiento	OSPF, RIP-1, RIP-2, BGP, IGMPv2, IGMP, PIM-SM, direccionamiento IP estático, PIM-SSM
Protocolo de gestión remota	SNMP 2, SNMP, Telnet, HTTP, HTTPS
Rendimiento	Capacidad 3DES : 300 Mbps Capacidad del cortafuegos (paquetes grandes) : 650 Mbps o más Capacidad del cortafuegos (IMIX) : 600 Mbps
Capacidad	Sesiones concurrentes : 64000 Políticas de seguridad : 1000 Conexión / cantidad de usuarios : ilimitado Usuarios autentificados (base de datos interna) : 1500 Túneles VPN concurrentes : 500 Interfaces de túnel VPN : 100 Zonas de seguridad : 60 Rutas estáticas : 20000

Indicadores de estado	Estado puerto, actividad de enlace, alimentación, estado, despertador, transmitir, recibir
Características	Diseño modular, protección firewall, criptografía 56 bits, encaminamiento, criptografía 168 bits, soporte de DHCP, soporte de NAT, VPN, soporte para PAT, soporte LDAP, soporte VLAN, soporte para Syslog, prevención contra ataque de DoS (denegación de servicio), soporte DiffServ, Alta disponibilidad, filtrado de URL, Transparency, actualizable por firmware, prevención de ataque DDos, Quality of Service (QoS)
Algoritmo de cifrado	DES, Triple DES, RSA, MD5, AES, IKE, SHA-1, PKI
Método de autentificación	SecurID, RADIUS, certificados X.509, Secure Shell v.2 (SSH2), LDAP
Cumplimiento de normas	IEEE 802.1x, X.509

Telefonía IP	
Protocolos VoIP	H.323, MGCP, SCCP, SIP

Expansión / Conectividad	
Total ranuras de expansión (libres)	6 (6) x Ranura de expansión 4 memoria
Interfaces	1 x gestión - consola - RJ-45 4 x red - Ethernet 10Base-T/100Base-TX/1000Base-TX - RJ-45 1 x gestión - auxiliar - RJ-45

Diverso	
Cumplimiento de normas	Certificado FCC Clase B , CE, CSA, UL, C-Tick, BSMI, cUL, VCCI Class A ITE, CB

Alimentación	
Dispositivo de alimentación	Fuente de alimentación - interna
Voltaje necesario	CA 120/230 V (50/60 Hz)
Potencia suministrada	350 vatios

Software / Requisitos del sistema	
OS proporcionado	ScreenOS

Parámetros de entorno	
Temperatura mínima de funcionamiento	0 °C
Temperatura máxima de funcionamiento	50 °C
Ámbito de humedad de funcionamiento	10 - 90%

Anexo III. Características Huawei. Router AR 28.

Parámetros de entorno	
Memoria Boot ROM	512 KB
SDRAM por defecto	128MB
Máximo de SDRAM	128MB
Memoria Flash	32MB
Ámbito de humedad de funcionamiento	10 – 90%
Voltaje Necesario	AC:100V to 240V 50/60Hz DC: 12 V
Modulos	2 Slot
Interfaces Fijas	1 10/100Mbps Ethernet 1 Synchronous/Asynchronous
Interfaces seriales	1 AUX Port 1 Console Port
Características de seguridad	AAA RADIUS, SSH, Firewall, NAT, L2TP, GRE, IPSec, IKE, Encryption card, Huawei- TACACS, RSA, CA
Encriptación	IPSec para creación de VPN

Anexo IV. Otros equipos para Redes Privadas Virtuales.

Equipos para Redes privadas virtuales.

VPN gateway: Dispositivos con un software y hardware especial para proveer capacidad a la VPN. Varias funciones son optimizadas sobre varios componentes de software y hardware.

Algunos ejemplos de esto tenemos Alcatel 7130,Altiga C10, VPN-1 Gateway, Lucent VPN Gateway, Intel Shiva Lan Rover VPN Gateway Plus, TimeStep Permit/Gate 4620 y VPNet VPNware VSU-1010, las cuales incluyen el software y hardware necesario para realizar y administra VPN.

Acatel 7130 Gateways de VPN

Sólo Software: El software está sobre una plataforma PC o Workstation, el software desempeña todas las funciones de la VPN. Algunos ejemplos de esto el Sistema Operativo Windows 9x, ME, NT, 2000 y XP

Basado en Firewall: Funciones adicionales son agregadas al firewall para habilitar capacidades de VPN. Algunos ejemplos de esto son los modelos PIX de Cisco como 506, 515, 525 y 535.

Cisco 535 Secure PIX Firewall 535.

Basado en Router: Funciones adicionales son agregadas al router para habilitar capacidades de VPN, las cuales se encuentran en el IOS de los router de Cisco como los modelos 804, 806, 827, 905, 1710, 1720, 1750, 2611, 2621, 2651, 3620, 3640, 3660, 7120, 7140 y 7200.

Router cisco serie 7200

Aunque los router son mejores que los concentradores, existen algunos capaces de realizar VPN como los modelos 3005, 3015, 3030, 3060 y 3080.[42]

Concentrador Cisco serie 3000