TRABAJO ESPECIAL DE GRADO

MIGRACIÓN Y EXPANSIÓN DE LA RED WAN DE LA EMPRESA CINEX CON INCORPORACIÓN DE UN ADECUADO SISTEMA DE SEGURIDAD PARA LA MISMA

Presentado ante la Ilustre
Universidad Central de Venezuela
Por el Br. Ibarra M., Carlos A.
para optar al Título de
Ingeniero Electricista

Caracas, 2008

TRABAJO ESPECIAL DE GRADO

MIGRACIÓN Y EXPANSIÓN DE LA RED WAN DE LA EMPRESA CINEX CON INCORPORACIÓN DE UN ADECUADO SISTEMA DE SEGURIDAD PARA LA MISMA

Prof. Guía: Ing. Luís Fernández
Tutor Industrial: Ing. Marbeli González

Presentado ante la Ilustre
Universidad Central de Venezuela
Por el Br. Ibarra M., Carlos A.
para optar al Título de
Ingeniero Electricista

Caracas, 2008

UNIVERSIDAD CENTRAL DE VENEZUELA
FACULTAD DE INGENIERIA
ESCUELA DE INGENIERIA ELECTRICA
DEPARTAMENTO DE COMUNICACIONES

CONSTANCIA DE APROBACIÓN

Caracas, 29 de mayo de 2008

Los abajo firmantes, miembros del Jurado designado por el Consejo de Escuela de Ingeniería Eléctrica, para evaluar el Trabajo Especial de Grado presentado por el Bachiller Carlos A. Ibarra M., titulado:

"MIGRACIÓN Y EXPANSIÓN DE LA RED WAN DE LA EMPRESA CINEX, CON INCORPORACIÓN DE UN ADECUADO SISTEMA DE SEGURIDAD PARA LA MISMA"

Consideran que el mismo cumple con los requisitos exigidos por el plan de estudios conducente al Título de Ingeniero Electricista en la mención de Comunicaciones, y sin que ello signifique que se hacen solidarios con las ideas expuestas por el autor, lo declaran APROBADO.

Prof. Paolo Maragno
Jurado

Prof. Franklin Martinez
Jurado

Prof. Luis Fernández
Prof. Guía

Edificio Escuela de Ingeniería Eléctrica, piso 1, oficina 201, Ciudad Universitaria, Los Chaguaramos, Caracas 1051, D.F.
TELÉFONOS. (VOZ) +58 212 6053300 (FAX) +58 212 6053105
Mail: eie-com@elecrisc.ing.ucv.ve

DEDICATORIA

A mi familia y a DIOS.
Por darme la vida, salud, sabiduría, estar siempre a mi lado
y otras tantas bendiciones que me han permitido lograr esta meta.

AGRADECIMIENTOS

A la Escuela de Ingeniería Eléctrica, de la Universidad Central de Venezuela, de quien recibí los conocimientos necesarios para desarrollarme como Ingeniero.

A mi Tutora Industrial, la Ing. Marbeli Gonzáles, así como al Ing. Edgar Benavente y el Ing. Kenny Silva, por el apoyo, dedicación y consejos brindados para la realización de este trabajo, así como por su excelente calidad profesional y humana. Más que compañeros, se han vuelto grandes amigos.

A amigos y compañeros de estudio, quienes me acompañaron en las alegrías como en las penurias, especialmente a Cesar Ugaz, Rafael Romero, Ricardo Ortiz, Juan Colmenares, Hugo Silva, Regulo Guedez, Rocío Fossi, Adriana Zambrano, Mónica Salomón, Jean Michel Ravel, Carlos Luis y tantos otros que faltan por nombrar, pero que saben que los aprecio.

A mis padres Marcia y Alberto, como mi hermano Oscar, por apoyarme en todo momento y estar siempre conmigo.

No solo no hubiera sido nada sin ustedes, sino por toda la gente que estuvo a mi alrededor desde el comienzo… algunos siguen hasta hoy…GRACIAS TOTALES

Ibarra M., Carlos A.

MIGRACIÓN Y EXPANSIÓN DE LA RED WAN DE LA EMPRESA CINEX CON INCORPORACIÓN DE UN ADECUADO SISTEMA DE SEGURIDAD PARA LA MISMA

Profesor Guía: Luis Fernandez. Tutor Industrial: Ing. Marbeli González. Tesis. Caracas. U.C.V. Facultad de Ingeniería. Escuela de Ingeniería Eléctrica. Ingeniero Electricista. Opción: Comunicaciones. Institución: Openlink Sistemas de Redes de Datos C.A. 2007-2008. 107 h. + Anexos

Palabras Claves: VPN (Virtual Private Network) red privada virtual, encriptación de datos, Red de Área Amplia WAN, Autenticación, IPsec (IP secure).

Resumen. Se diseña y se implementa la interconexión de diversos sitios por una red privada virtual a través de una red pública (Internet) basado en la serie de protocolos IPsec para la red de Cinex con sede en Chacaito Caracas, con la finalidad de satisfacer las necesidades de comunicación de este ente. Se realizó un análisis de los requerimientos generales que debían cumplir los equipos para brindar la seguridad necesaria a los datos para luego hacer una preselección entre los equipos disponibles en el mercado y posteriormente escoger el sistema más conveniente. Adicionalmente para la implantación de la red, Cinex solicitó el servicio Frame Relay a CANTV para contar con un direccionamiento estático y confiable para el establecimiento de los enlaces por VPN. Posteriormente se procedió a definir los parámetros para el direccionamiento de la red LAN, debido a que la WAN en las localidades usa servicio ADSL con direccionamiento dinámico. Se definieron los requisitos a cumplir a nivel de seguridad, y por último la configuración de los *routers* destinados a todos los sitios que integran el sistema y el firewall en la principal. Posteriormente se comenzó migrando una localidad, concretamente la del Centro Comercial Lido, para que sirviera como prueba piloto. Al tenerla operando sin contratiempos se comenzaron a instalar las diversas localidades ubicadas a lo largo de todo el país

ÍNDICE GENERAL

LISTA DE FIGURAS

FIGURAS, ILUSTRACIONES O GRÁFICAS Pág.

LISTA DE TABLAS

INTRODUCCIÓN

La empresa Cinex surge como la integración o fusión de 3 empresas pequeñas para entonces, todas del área de entretenimiento cinematográfico en Venezuela; Sur Americana de Espectáculos (Circuito Radonski), Venefilms y el Grupo Blanco. Actualmente tiene 106 salas distribuidas en 28 complejos. Red que esperan ampliar en los próximos años a través de nuevas salas.

La empresa tiene como:

Misión: Dedicarse a ser los mejores en entretener a la gente.

Valores:

Visión: Para desarrollar nuevos negocios oportunamente.

Agresividad Comercial: Para mantener el liderazgo comercial.

Respeto: Para nuestra gente y nuestros huéspedes.

Trabajo: en Equipo y Cooperación.

Dedicación y Compromiso: Para brindar una experiencia inigualable.

Comunicación y Transparencia: En nuestra organización y con nuestros huéspedes.

Excelencia en Servicio: Ofrecer una experiencia inolvidable de entretenimiento con el mejor servicio, comodidad y seguridad en sus instalaciones.

A pesar de esta fusión, las 3 empresas, en cuestiones administrativas siguieron trabajando de forma independiente.

Poco a poco esta nueva empresa, Cinex, fue creciendo y se vio en la necesidad de mantenerse comunicada con sus diferentes localidades a lo largo del territorio del país y a pesar de que ya es una empresa única como Cinex, se mantienen trabajando como 3 familias independientes dentro de un mismo núcleo.

Al crecer cada una de ellas buscó soluciones para mantenerse conectadas entre ellas, pero lo hicieron de manera independiente una de las otras. Lograron trabajar así ya que para su momento eran pocas. Solo centralizaban la información que necesitaran y por correo electrónico a través de Internet. Pero ha decidido unificar toda su red y centralizarlas.

CAPITULO I
PLANTEAMIENTO DEL PROBLEMA

1.1 Justificación

Las oficinas principales de la empresa Cinex (sus 3 núcleos, Sur Americana de Espectáculos, Venefilms y Blanca), se encuentran localizadas en Caracas. Debido al gran crecimiento y desarrollo que ha obtenido la empresa, la misma cuenta con diversas salas distribuidas a lo largo de todo el país, por lo que se vio en la necesidad de buscar formas de mantenerse comunicadas con cada una de ella. Cada uno de los núcleos de Cinex lo hizo a su manera, y solo centralizaban la información que necesitarán prestar a las demás.

Toda esta información que fluye entre las localidades y las sedes principales son de gran importancia para la empresa y cada vez se hace más importante proteger la información privada de la empresa. Debido a que los enlaces WAN se hacen por medios públicos como Internet, esta información pudiera ser capturada por terceros que pueden usarla en perjurio de la empresa; por esto se hace evidente la necesidad de realizar túneles seguros entre las localidades y las sedes, de forma de encriptar y asegurar la data.

Por otro lado, Internet definitivamente llegó para quedarse, y en el caso del cine no es la excepción, pues las empresas involucradas en el mercado han encontrado un buen aliado en la red cuando de vender entradas se trata. El venezolano está empezando a entrar a Internet y realizar operaciones comerciales cada vez con más frecuencia, quizás porque los niveles de confianza han ido mejorando y el temor ha ido superándose. Cinex tiene su sitio en Mipunto.com, donde el internauta puede acceder las 24 horas del día y los 365 días del año. Las entradas se compran mediante tarjeta de crédito y se pueden retirar en la taquilla del cine correspondiente.

Cinex por el momento tiene su sitio hospedado en un tercero puesto que no cuenta con la plataforma necesaria para tenerla y administrarla, la cual cada vez va tomando mayor importancia debido a su creciente demanda por parte del público. Si

gran parte de la industria del cine es la venta de entradas, resulta comprensible que la administración de la venta de entradas (por Internet) este en manos de la empresa y no de un tercero, por lo que se busca la creación de la plataforma necesaria para levantar servicios para responder a las necesidades del público y a las propias demandas del negocio y de esta forma ampliar sus horizontes.

Sur Americana de Espectáculos, la más grande de las tres instituciones que conforman Cinex, esta ubicada en el piso 4 y 5 del Edificio Las Delicias, en la 3ra transversal de Las Delicias. En la actualidad cuenta con 14 localidades ubicadas entre la capital y en el interior del país.

Actualmente, posee comunicación con sus localidades a través de VPN, solo para datos. El establecimiento de VPN de la red de datos de CINEX, es administrado y controlado por un proveedor de servicio. En las siguientes figuras se muestra el escenario actual:

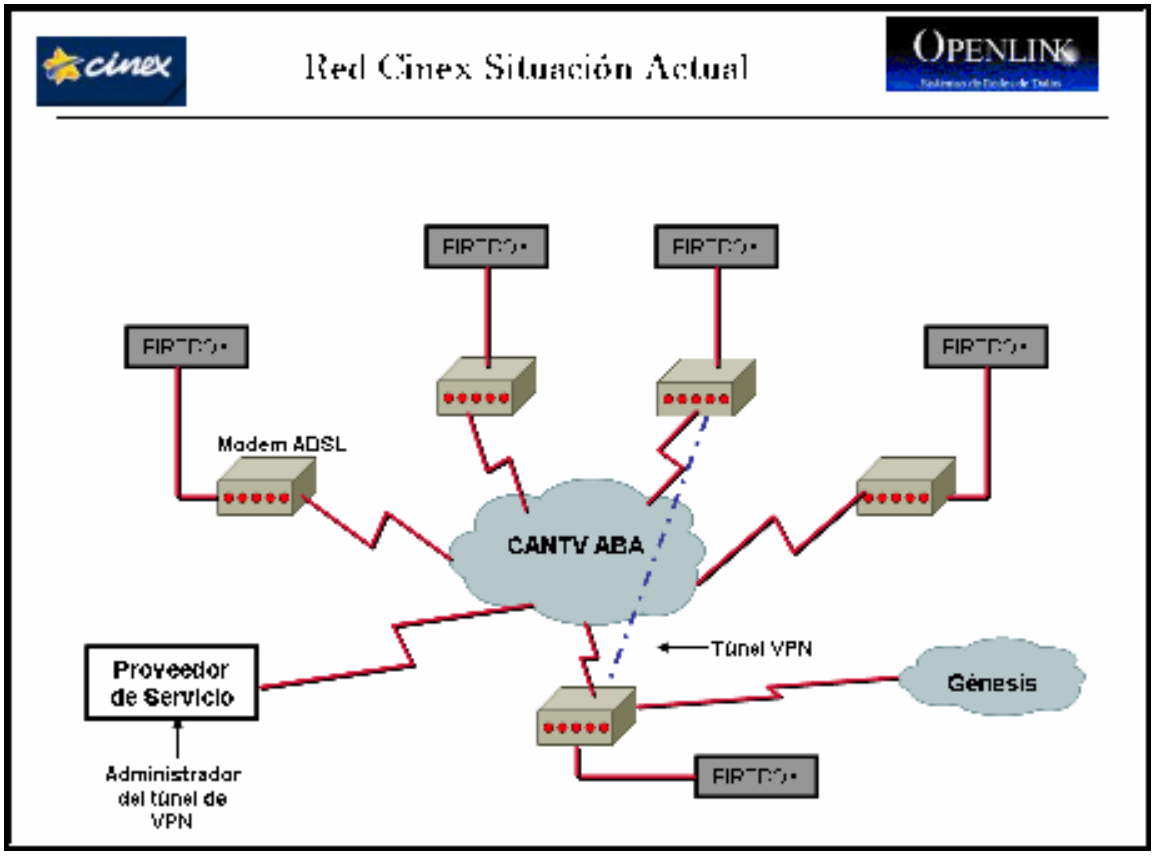

Figura 1. Situación WAN Actual

En esta figura se observa la situación actual de la red de Cinex, y podemos ver que la administración de los túneles de VPN está siendo manejada por un proveedor de servicios.

La red de datos de Cinex está conformada por los siguientes equipos:

Equipos de comunicaciones:

Sede principal

- Switch Allied Telesyn AT-FS724i (1)
- Switch 3Com 3C17300A SuperStack Switch 4200 26 puertos (1)
- Switch Unicom Dyna-Switch /24 (1)
- Terminal de fibra optica (salida para Daycohost)
- Modem ADSL de CANTV ABA

Sedes remotas

- Modem ADSL de CANTV ABA
- Switch Linksys SR2024
- Switch Nexxt de 24 puertos 10/100
- Switch 3Com de 16 puertos
- Switch D-Link Des-1016D de 16 puertos 10/100

En las localidades existe alguno de los switch´s mencionados o incluso combinación de ellos.

Equipo de seguridad:

En la principal:

- Watchguard X500

En las localidades, alguno de estos:

- Watchguard Firebox Edge X15
- Watchguard Firebox Edge X50
- Watchguard Firebox SOHO 6

Servidores: instalados en la LAN de la sede principal

• ISA Server	Server IBM xSeries 206
• Print Server. PBX	Server IBM Netfinity M20
• Domain Controller. SQL Server – Saint	Server HP Hp ProLiant ML350
• Antivirus Server	Server HP Hp ProLiant ML350

Cinex posee servidor de correo pero a través de un proveedor de servicios.

Incluso la pagina www.cinex.com.ve esta hospedada en un servidor externo y no por ellos mismo.

Los principales inconvenientes de la plataforma de Cinex son:

- Los enlaces no son administrados por ellos sino por un proveedor de servicios.
- La plataforma actual no cuenta con las capacidades necesarias para desarrollar a un futuro nuevas necesidades, como telefonía IP.
- Cualquier cambio que se requiera hacer en la red, debe ser llevado al proveedor de servicio lo que amerita de un mayor tiempo y dinero para su ejecución.
- A pesar de contar con firewall, que otorgan seguridad a la red; las amenazas cada día son mayores, por lo que se busca mejorar en este sentido.
- Los enlaces han presentado caídas cada vez mas frecuentes, los cuales no se desean.
- Necesidad de contar con la capacidad de ser servidor de su propio sitio en Internet.

Por estas razones es justificada la incorporación de tecnologías que garanticen la base para el crecimiento de las telecomunicaciones entre las localidades y la sede principal de la empresa,

Esta nueva tecnología debe cubrir los requerimientos de ancho de banda de los suscriptores, que permita el ofrecimiento de servicios actuales como acceso a Internet y comunicación segura entre oficinas y ofrezca un sistema que pueda cubrir las necesidades presentes y pueda prever un aumento en la Red.

Dicho proyecto es encomendado a la empresa Openlink Sistemas de Redes de Datos C.A. y Parther Gold de Cisco System, a través de la cual se desarrolla el proyecto.

1.2 Planteamiento del Problema

Por las razones antes mencionadas, se propone en el presente proyecto un diseño e implementación de una red WAN tipo estrella, a través de túneles VPN que permitan una comunicación segura y confiable entre la sede principal y las demás localidades de la empresa Cinex; y de esta forma unir los tres núcleos que lo conforman bajo una sola red, puesto que hasta ahora no lo están. Esta red debe estar en la capacidad de sustituir la red que posee actualmente Sur Americana de Espectáculos, brindando los servicios que requieren actualmente y estar en la capacidad de adaptarse fácilmente a la implementación de otros servicios, como son: acceso a Internet de forma controlada, Voz sobre IP, IPv6 brindando además la robustez del sistema y calidad de servicio para la transmisión de datos de forma segura, y prevea el crecimiento que proyecta la red Cinex.

1.3 Objetivos

1.3.1 Objetivos Generales

Realizar la migración de la red WAN de la empresa Cinex a través de VPN, en todas sus localidades, para brindar un servicio óptimo a su creciente sistema, a través de la instalación de routers Cisco y un sistema que le proporcione la seguridad necesaria a su plataforma.

1.3.2 Objetivos Específicos

Proponer un modelo de red que cumpla con los requerimientos del cliente Cinex, considerando los siguientes aspectos:

- Arquitectura de la red.
- Protocolos de comunicación y encriptación.
- Alcance y tiempos de implementación.
- Servicios a ofrecer.

- Creación de nueva lista de direccionamiento.
- Instalación de una prueba piloto entre la Oficina Central de Cinex y alguna localidad.
- Establecer los criterios de instalación de los equipos para la VPN en las diversas localidades de Cinex a lo largo de todo el país.
- Instalar e interconectar algunas localidades con la Central de Cinex.

En el capítulo 2 se habla de los conocimientos teóricos necesarios para poder llevar a cabo del desarrollo de los objetivos mencionados anteriormente, dando de este modo una breve reseña de conceptos involucrados con el desarrollo de la tesis.

El capítulo 3 expresa el diseño tomado para dar la solución al problema planteado, basándose en los conocimientos teóricos y recomendaciones adquiridas.

Como cuarto y último capítulo se explica el desarrollo de la implementación de la solución, además de comentar los resultados de dicha implementación hasta la fecha, así como problemas que pudieron surgir al momento de llevarla a cabo.

CAPITULO II
REDES DE AREA AMPLIA (REDES WAN, WIDE AREA NETWORK)

2.1 Redes WAN. Conceptos Básicos. [2] [3] [4]

Una **red de área amplia**, **WAN**, acrónimo de la expresión en inglés '**Wide Area Network**', es un tipo de red de computadoras de gran tamaño, capaz de cubrir distancias desde unos 100 hasta unos 1000 km, dando el servicio a lo largo de un país o un continente. La más grande y conocida red WAN es Internet.

Muchas WAN son construidas por y para una organización o empresa particular y son de uso privado, otras son construidas por los proveedores de Internet (ISP) para proveer de conexión a sus clientes.

Hoy en día Internet proporciona WAN de alta velocidad, y la necesidad de redes privadas WAN se ha reducido drásticamente mientras que las VPN que utilizan cifrado y otras técnicas para hacer esa red dedicada aumentan continuamente.

Normalmente la WAN es una red punto a punto, es decir, red de paquete conmutado. Las redes WAN pueden usar sistemas de comunicación vía satélite o de radio.

Una red de área amplia o WAN (Wide Area Network) se extiende sobre un área geográfica extensa, a veces un país o un continente, y su función fundamental está orientada a la interconexión de redes o equipos terminales que se encuentran ubicados a grandes distancias entre sí. Para ello cuentan con una infraestructura basada en poderosos nodos de conmutación que llevan a cabo la interconexión de dichos elementos, por los que además fluyen un volumen apreciable de información de manera continúa. Por esta razón también se dice que las redes WAN tienen carácter público, pues el tráfico de información que por ellas circula proviene de

diferentes lugares, siendo usada por numerosos usuarios de diferentes países del mundo para transmitir información de un lugar a otro. A diferencia de las redes LAN (siglas de "Local Area Network", es decir, "red de área local"), la velocidad a la que circulan los datos por las redes WAN suele ser menor que la que se puede alcanzar en las redes LAN. Además, las redes LAN tienen carácter privado, pues su uso está restringido normalmente a los usuarios miembros de una empresa, o institución, para los cuales se diseñó la red.

La infraestructura de redes WAN la componen, las líneas de transmisión y los elementos de conmutación. Las líneas de transmisión (también llamadas "circuitos", "canales" o "troncales") mueven información entre los diferentes nodos que componen la red, moviendo los bits de una máquina a otra.

Los elementos de conmutación también son dispositivos de altas prestaciones, pues deben ser capaces de manejar la cantidad de tráfico que por ellos circula. Son computadoras especializadas que conectan dos o más líneas de transmisión. Cuando los datos llegan por una línea de entrada, el elemento de conmutación debe escoger una línea de salida para enviarlos. Aunque no existe una terminología estándar para designar estas computadoras, se les denomina nodos conmutadores de paquetes, sistemas intermedios y centrales de conmutación de datos. También es posible llamarles simplemente enrutadores o routers. Cada host está conectado a una red LAN, que a su vez se conecta a uno de los nodos de conmutación de la red WAN. Este nodo debe encargarse de encaminar la información hacia el destino para la que está dirigida.

El término conmutación, se pudiera definir como la manera en que los nodos o elementos de interconexión, garantizan la interconexión de dos sistemas finales, para intercambiar información.

2.1.1 TIPOS DE REDES WAN

Conmutadas por Circuitos: Redes en las cuales, para establecer comunicación se debe efectuar una llamada y cuando se establece la conexión, los usuarios disponen de un enlace directo a través de los distintos segmentos de la red.

Conmutadas por Mensaje: En este tipo de redes el conmutador suele ser un computador que se encarga de aceptar tráfico de los computadores y terminales conectados a él. El computador examina la dirección que aparece en la cabecera del mensaje hacia el DTE que debe recibirlo. Esta tecnología permite grabar la información para atenderla después. El usuario puede borrar, almacenar, redirigir o contestar el mensaje de forma automática.

Conmutadas por Paquetes: En este tipo de red los datos de los usuarios se descomponen en trozos más pequeños. Estos fragmentos o paquetes, estás insertados dentro de informaciones del protocolo y recorren la red como entidades independientes.

Redes Orientadas a Conexión: En estas redes existe el concepto de multiplexión de canales y puertos conocido como *circuito o canal virtual*, debido a que el usuario aparenta disponer de un recurso dedicado, cuando en realidad lo comparte con otros pues lo que ocurre es que atienden a ráfagas de tráfico de distintos usuarios.

Redes no orientadas a conexión: Llamadas Datagramas, pasan directamente del estado libre al modo de transferencia de datos. Estas redes no ofrecen confirmaciones, control de flujo ni recuperación de errores aplicables a toda la red, aunque estas funciones si existen para cada enlace particular. Un ejemplo de este tipo de red es INTERNET.

Topologías de las redes WAN

En el caso de las redes WAN, su topología física puede llegar a ser más compleja y no responder a las formas básicas de redes mas pequeñas (bus, estrella y anillo), debido a varios factores determinantes: la distancia que deben cubrir las redes, la cantidad enorme de usuarios, el tráfico que deben soportar y la diversidad de equipos de interconexión que deben usar. Existe un grupo establecido de topologías que son las más usadas, y la implementación de cada una de ellas en particular está condicionada por necesidades específicas, como pueden ser: cantidad de nodos a conectar, distancia entre los nodos e infraestructura establecida en ellos. A continuación se presentan las topologías usadas en redes WAN:

Punto a Punto

En esta topología cada nodo se conecta a otro a través de circuitos dedicados, es decir, canales que son arrendados por empresas o instituciones a las compañías telefónicas. Dichos canales están siempre disponibles para la comunicación entre los dos puntos.

Esta configuración es solo funcional para pequeñas WANs ya que todos los nodos deben participar en el tráfico, es decir que si aumenta la cantidad de nodos aumenta la cantidad de tráfico y esto con el consiguiente encarecimiento de la red.

Anillo

En la topología de anillo cada nodo es conectado a otros dos más formando un patrón de anillo. Esta topología tiene dos ventajas: por un lado si existe algún problema en las conexiones en un cable, la información le sigue llegando al nodo usando otro recorrido y si algún nodo esta muy ocupado el tráfico se puede derivar hacia otros nodos.

Extender este tipo de redes es más caro que extender una red punto-a-punto ya que se necesita al menos un enlace más.

Estrella

En esta configuración un nodo actúa como punto central de conexión para todos los demás, permitiendo así que en caso de que exista un fallo en alguno de los cables los demás nodos no pierdan conexión con el nodo central. La principal desventaja de esta topología es que algún problema que exista en el nodo central se convierte en un desastre total para la red ya que se pierde la conexión de todos los nodos.

Malla

En esta topología la esencia es buscar la interconexión de los nodos de tal manera que si uno falla los demás puedan redireccionar los datos rápida y fácilmente. Esta topología es la que más tolerancia tiene a los fallos porque es la que provee más caminos por donde puedan viajar los datos que van de un punto a otro.

La principal desventaja de las redes tipo malla es su costo, es por esto que se ha creado una alternativa que es la red de malla parcial en la cual los nodos más críticos (por los que pasa mas trafico) se interconectan entre ellos y los demás nodos se interconectan a través de otra topología (estrella, anillo).

Los canales suelen proporcionarlos las compañías telefónicas, con un determinado costo mensual si las líneas son alquiladas, y un costo proporcional a la utilización si son líneas normales conmutadas.

El enrutador puede estar conectado tanto a una línea analógica como a una línea digital. Se conectan a las líneas analógicas a través de módem o a líneas digitales a través de Unidades de Servicio de Canal/Unidades de Servicio de Datos

(CSU / DSUs: Channel Service Unit / Data Service Units). El tipo de servicio de transmisión determina la clase de equipo que el área extensa necesita para su funcionamiento.

Líneas Dedicadas y Líneas Conmutadas

Las redes WAN pueden incluir tanto líneas dedicadas como líneas conmutadas.

Una línea dedicada es una conexión permanente entre dos puntos que normalmente se alquila por meses.

Un servicio de línea conmutada no requiere conexiones permanentes entre dos puntos fijos. En su lugar, permite a los usuarios establecer conexiones temporales entre múltiples puntos cuya duración corresponde a la de la transmisión de datos. Existen dos tipos de servicios conmutados: servicios de conmutación de circuitos, similares a los servicios utilizados en las llamadas telefónicas; y los servicios de conmutación de paquetes, que se ajustan mejor a la transmisión de datos.

2.2 Ancho de Banda

El ancho de banda digital (o más apropiadamente el flujo de datos) es la cantidad de datos que se puede transmitir en una unidad de tiempo. La unidad de medida fundamental para el ancho de banda digital es bits por segundos (bps) a diferencia del ancho de banda analógico que se mide en Hertz. La relación entre el ancho de banda digital y el ancho de banda analógico es lo que se conoce como eficiencia espectral y se mide en bits por segundo/Hertz. [4]

2.3 Consideraciones físicas.

En vista que las redes WAN deben cubrir grandes extensiones geográficas, resulta muy costoso y complicado para cada empresa, tener que disponer de conexiones propias hacia cada localidad. Por esto dichas conexiones son alquiladas o adquiridas a proveedores de servicios.

2.3.1 Proveedores de servicios.

Son empresas dedicadas a conectar a los usuarios a las distintas redes que tengan, y dar el mantenimiento necesario para que el acceso funcione correctamente. También ofrecen servicios relacionados, como alojamiento web o registro de dominios entre otros.

Estas conexiones son ofrecidas de distintas formas, según las necesidades y velocidades de acceso que requieran como pueden ser, xDSL, Frame Relay, ATM, Fibra Óptica entre algunos cableados o enlaces inalámbricos.

2.3.2 Medios de transporte (DSL, Frame Relay, Metro Ethernet, ATM, Fibra)

Entre los medios de transporte cableados mas usados para enlaces de banda ancha tenemos:

xDSL: (Líneas de Suscripción Digital). Tecnología de transmisión de datos que permite que los cables de cobre telefónicos (pots) transfieran hasta 16 Mbps.

- **ADSL**

  ” (Asymmetric digital subscriber line). Soporta una velocidad de recepción de datos entre 128 kbps y 9 Mbps., envía entre 16 y 640 kbps. ADSL requiere un módem especial ADSL para adecuar la señal.”[5]

- **SDSL**

  ” (Symmetric digital subscriber line). SDSL soporta velocidades de hasta 3 Mbps. SDSL funciona enviando pulsos digitales en el área de alta frecuencia de las líneas telefónicas y no puede operar simultáneamente con las conexiones de voz en la misma línea. SDSL requiere un módem especial SDSL. Permite la misma velocidad de subida como de bajada.” [5]

- **VDSL**

  ” Very High DSL). Es una tecnología DSL que ofrece grandes velocidades de transmisión de datos en distancias cortas. Mientras más corta la distancia, más velocidad de transmisión.” [5]

- **HDSL**

  "(High bit rate Digital Subscriber Line) Línea Digital de Abonado de alta velocidad. Permite transferencia de información utilizando cables de pares tranzados, típicos en conexiones telefónicas. Los módems HDSL permiten el establecimiento por un par telefónico de un circuito digital unidireccional de 1,544 Mbps (T1) ó 2,048 Mbps (E1), por lo que para la comunicación bidireccional son necesarios dos pares, uno para cada sentido (subida y bajada)." [5]

FRAME RELAY [2]

Frame Relay es una técnica de comunicación mediante retransmisión de tramas, introducida por la ITU-T a partir de la recomendación I.122 de 1988. Consiste en una forma simplificada de tecnología de conmutación de paquetes que transmite una variedad de tamaños de tramas o marcos ("*frames*") para datos, perfecto para la transmisión de grandes cantidades de datos.

La técnica **Frame Relay** se utiliza para un servicio de transmisión de voz y datos a alta velocidad que permite la interconexión de redes de área local separadas geográficamente a un costo menor.

Ofrece mayores velocidades y rendimiento, a la vez que provee la eficiencia de ancho de banda que viene como resultado de los múltiples circuitos virtuales que comparten un puerto de una sola línea. Los servicios de Frame Relay son confiables y de alto rendimiento. El Frame Relay es ideal para usuarios que necesitan una conexión de mediana o alta velocidad para mantener un tráfico de datos entre localidades múltiples y distantes.

Frame Relay proporciona conexiones entre usuarios a través de una red pública, del mismo modo que lo haría una red privada punto a punto, esto quiere decir que es orientado a la conexión.

Las conexiones pueden ser del tipo permanente, (PVC, *Permanent Virtual Circuit*) o conmutadas (SVC, *Switched Virtual Circuit*).

Con Frame Relay se contrata un ancho de banda digital determinado en un tiempo determinado. A este ancho de banda se le conoce como CIR (*Commited Information Rate*). Esta velocidad, surge de la división de Bc (*Committed Burst*), entre Tc (el intervalo de tiempo). No obstante, una de las características de Frame Relay es su capacidad para adaptarse a las necesidades de las aplicaciones, pudiendo usar una mayor velocidad de la contratada en momentos puntuales, adaptándose muy bien al tráfico en ráfagas.

Estos Bc bits, serán enviados de forma transparente. No obstante, cabe la posibilidad de transmitir por encima del CIR contratado, mediante los Be (*Excess Burst*). Estos datos que superan lo contratado, serán enviados en modo *best-effort*, activándose el bit DE de estas tramas, con lo que serán las primeras en ser descartadas en caso de congestión en algún nodo. Este flujo adicional al Bc es permitido siempre que la red no se encuentre congestionada

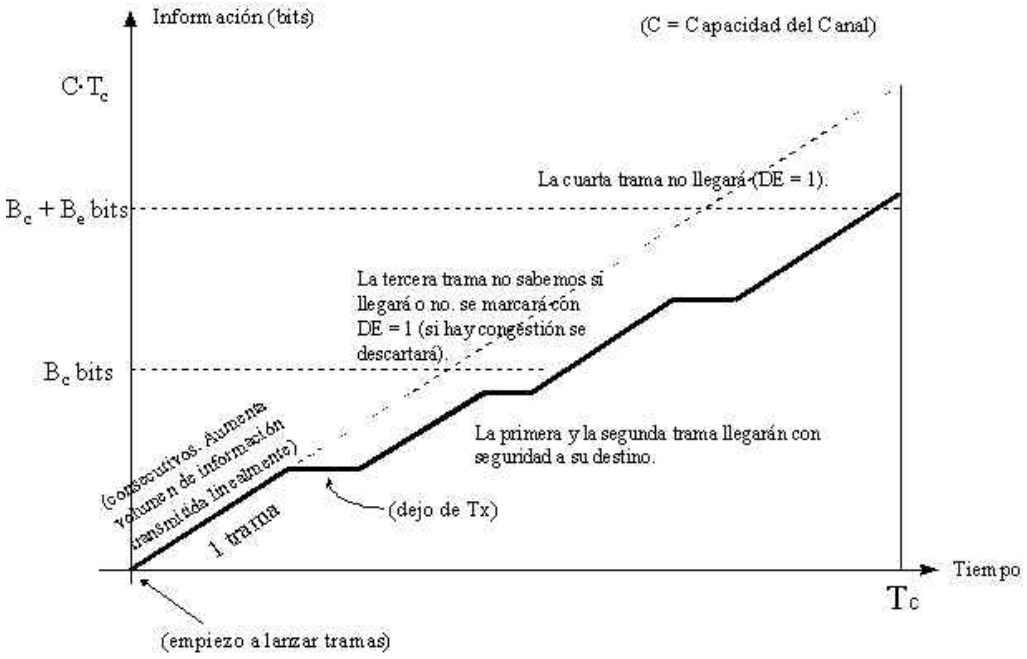

Figura 2. Transmisión Frame Relay.

Fuente:http://www.it.uc3m.es/~prometeo/rsc/apuntes/frame/frame.html

2.4 Direcciones IP [2] [6]

Para que dos sistemas se comuniquen, se deben poder identificar y localizar entre sí.

Una **dirección IP** es un número que identifica de manera lógica y jerárquica a una interfaz de un dispositivo (habitualmente una computadora) dentro de una red que utilice el protocolo IP (*Internet Protocol*), que corresponde al nivel de red o nivel 3 del modelo de referencia OSI. Cada equipo conectado a una red tiene una dirección IP asignada, distinta a todas las demás direcciones que estén vigentes en ese momento en el conjunto de redes visibles por el equipo.

Para asegurar que la parte de identificación de red de una dirección Internet es única, todas las direcciones son asignadas por una autoridad central, el Centro de Información de Red (NIC, Network Information Center).

Cada dirección IP tiene una longitud fija de 32 bits (en IPv4), separados en 4 octetos. En la práctica se expresa en forma decimal: viene dado por 4 enteros separados por puntos, donde cada número se corresponde con el valor de un octeto de

la dirección IP. Una dirección IP tiene un formato de dos partes que son la dirección de red y la dirección local o de host.

2.4.1 Clasificación

Las direcciones IP, de acuerdo a su accesibilidad se clasifican en:

- Direcciones Públicas. Son visibles en todo Internet.
- Direcciones IP privadas (reservadas), Son visibles únicamente por otros equipos de su propia red o de otras redes privadas interconectadas.

A su vez las direcciones IP, de acuerdo a su permanencia en el tiempo, puede ser:

- Direcciones IP estáticas (fijas). Un equipo que se conecte a la red con dirección IP estática siempre lo hará con una misma IP. Las direcciones IP públicas estáticas son las que utilizan los servidores de Internet.
- Direcciones IP dinámicas. Un equipo que se conecte a la red mediante dirección IP dinámica, cada vez lo hará con una dirección IP distinta. Va variando su dirección IP. [4]

2.4.2 Direcciones para clases de redes

Las direcciones IP se dividen en clases para definir las redes de tamaño pequeño, mediano y grande.

Tabla Nº 1 Clases de direcciones IP

Clase	Bit de mayor peso	Intervalo del primer octeto	Nº de bits en la dirección de red	Cantidad de redes	Cantidad de hosts por red
A	0	0-127	8	126	16.777.216
B	10	128-191	16	16.384	65.535
C	110	192-223	24	2.097.152	254
D	1110	224-239	28	No es aplicable	No es aplicable

La clase D se creó para permitir multicast en una dirección IP. Una dirección multicast es una dirección exclusiva de red que dirige los paquetes con esa

dirección destino hacia grupos predefinidos de direcciones IP. Una sola estación puede transmitir de forma simultánea una sola corriente de datos a múltiples receptores.

Se ha definido una dirección Clase E. Sin embargo, la Fuerza de Tareas de Ingeniería de Internet (IETF) ha reservado estas direcciones para su propia investigación; por lo tanto, no se han emitido direcciones Clase E para ser utilizadas en Internet. Los primeros cuatro bits de una dirección Clase E siempre son 1s. Por lo tanto, el rango del primer octeto para las direcciones Clase E es 11110000 a 11111111, o 240 a 255. [4]

2.4.3 Direcciones IP especiales y reservadas. [4] [7]

Ciertas direcciones de host son reservadas y no pueden asignarse a dispositivos de la red. Estas direcciones de host reservadas incluyen:

- **Dirección de red:** Utilizada para identificar la red en sí. La dirección IP que tiene ceros binarios en todas las posiciones de bits de host queda reservada para la dirección de red, conocida como el ID (identificador) de la red

- **Dirección de broadcast:** Utilizada para realizar el broadcast de paquetes hacia todos los dispositivos de una red. Para enviar información a todos los dispositivos de la red, se necesita una dirección de broadcast. Un broadcast se produce cuando una fuente envía datos a todos los dispositivos de una red. Para asegurar que todos los demás dispositivos de una red procesen el broadcast, el transmisor debe utilizar una dirección IP destino que ellos puedan reconocer y procesar. Las direcciones IP de broadcast terminan con unos binarios en toda la parte de la dirección que corresponde al host.

No todas las direcciones comprendidas entre la 0.0.0.0 y la 223.255.255.255 son válidas para un equipo: algunas de ellas tienen significados especiales. Las

principales direcciones especiales se resumen en la siguiente tabla. Su interpretación depende del equipo desde el que se utilicen.

Tabla Nº 2. Direcciones IP especiales

Bits de red	Bits de host	Significado	Ejemplo
Todos 0		Mi propio equipo	0.0.0.0
Todos 0	Equipo	Equipo indicado dentro de mi red	0.0.0.10
Red	Todos 0	Red indicada	192.168.1.0
Todos 1		Difusión a mi red	255.255.255.255
Red	Todos 1	Difusión a la red indicada	192.168.1.255
127	Cualquier valor válido de equipo	Loopback (mi propio equipo)	127.0.0.1

Se han reservado varios bloques de direcciones para su uso en redes que no se van a conectar a la Internet y que no van a necesitar conectividad con otra organización. Las direcciones de redes siguientes se encuentran reservadas por el RFC 1918, para su uso en redes privadas (intranets). Una dirección IP que pertenezca a una de estas redes se dice que es una dirección IP privada.

Tabla Nº 3. Rango de direcciones IP reservadas o privadas.

Clase	Intervalo de direcciones internas RFC 1918
A	10.0.0.0-10.255.255.255
B	172.16.0.0-172.31.255.255
C	192.168.0.0-192.168.255.255

2.5 Protocolos para supervisión y gestión

2.5.1 Protocolos SNMP [2] [6]

Iniciales de Simple Network Management Protocol. Es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red. Es parte de la familia de protocolos de Internet utilizando un servicio no orientado a la conexión como es UDP. Generalmente escucha por los puertos 161 y 162. SNMP permite a los administradores supervisar el desempeño de la red.

Está basado en un conglomerado de agentes. Cada agente es un elemento de la red que ofrece unas determinadas variables al exterior, para ser leídas o modificadas. Asimismo estos agentes pueden enviar alertas (Traps) a otros agentes para avisar de eventos que sucedan. Generalmente se llama gestor al agente encargado de recibir estas notificaciones de eventos.

Las variables ofrecidas para consulta por los agentes SNMP se definen a través de una base de información de gestión, llamada MIB (Management Information Base), formando una estructura de árbol. Así se va a determinar la información que ofrece un dispositivo SNMP y la forma en que se representa. Cada agente SNMP ofrece información dentro de una MIB, tanto de la base de datos general como de aquellas extensiones que desee proveer cada uno de los fabricantes. Así por ejemplo los fabricantes de routers han extendido las MIB estándar incluyendo información específica de sus equipos.

Algunos ejemplos de aplicaciones con este protocolo son: Supervisar el estado de un enlace punto a multipunto para detectar cuando está congestionado y así tomar medidas oportunas, que un servidor envíe una alerta cuando la carga de su sistema se incrementa significativamente, entre otras. Este protocolo también va a permitir la modificación remota de la configuración de dispositivos, de forma que se pueden configurar ciertos parámetros de interés por el administrador del sistema.

Este protocolo presenta las siguientes versiones:

- SNMP v1: Primera versión del protocolo establecida en el RFC 1157.

- SNMP v2: Presenta autentificación a través de las llamadas secuencias de comunidades.
- SNMP v 3: Presenta un conjunto de mejoras adicionales en el aspecto de seguridad, pero no ha sido mayormente aceptado en la industria.

2.5.2 TELNET [2] [4]

Es un protocolo que sirve para acceder mediante una red a una maquina perteneciente a la misma, y poder manejarla como si se estuviera frente al dispositivo que se desea. Esta conexión se realiza generalmente por el puerto 23. Solo nos permite una conexión modo Terminal, sin gráficos, pero es una herramienta muy útil para corregir fallos, consultar datos y gestionar ciertos parámetros del equipo a distancia, sin necesidad de presencia física en el sitio donde se encuentra.

Su mayor problema es de seguridad, ya que todos los nombres de usuario y contraseñas necesarias para entrar en las máquinas viajan por la red como *texto plano* (cadenas de texto sin cifrar). Esto facilita que cualquiera que espíe el tráfico de la red pueda obtener los nombres de usuario y contraseñas, y así acceder él también a todas esas máquinas.

2.5.3 SSH (Secure SHell)

Es el nombre de un protocolo y del programa que lo implementa, y sirve para acceder a máquinas remotas a través de una red. Permite manejar por completo la computadora mediante un intérprete de comandos. SSH trabaja de forma similar a como se hace con telnet. La diferencia principal es que SSH usa técnicas de cifrado que hacen que la información que viaja por el medio de comunicación vaya de manera no legible y ninguna tercera persona pueda descubrir el usuario y contraseña de la conexión ni lo que se escribe durante toda la sesión.

Además de la conexión a otras máquinas, SSH nos permite copiar datos de forma segura (tanto ficheros sueltos como simular sesiones FTP cifradas), gestionar

claves RSA para no escribir claves al conectar a las máquinas y pasar los datos de cualquier otra aplicación por un canal seguro tunelizado mediante SSH. [2]

2.6 Redes privadas Virtuales (VPN) [1]

Una Red Privada Virtual, mejor conocida por sus siglas "VPN", es una red que utiliza recursos de transmisión y conmutación compartidos, de una red pública tal como la Internet, ATM y/o Frame, para disponer a usuarios remotos los recursos y servicios disponibles en una red corporación, utilizando métodos de seguridad y protección para salvaguardar tanto la plataforma corporativa como los datos intercambiados (encapsulamiento y encriptación).

La esencia de ésta tecnología reside en que esa parte "pública" no será accesible por ningún usuario no autorizados, lo que la convierte en una red "privada virtual", dado a que no es una red privada real.

Los paquetes de datos de la red privada viajan por medio de un "túnel" definido en la red pública. Una VPN conjuga la seguridad y velocidad de una red privada con la flexibilidad (fácil expansión) y economía (bajo costos operativos) de un medio de comunicación como Internet.

Con el túnel, la fuente encapsula los paquetes pertenecientes a otro protocolo en datagramas IP con el fin de poder atravesar la infraestructura de Internet. El proceso de encapsulación está basado en la adición de una cabecera IP al datagrama original, el cual representa la carga (*payload*). En el extremo remoto, el receptor desencapsula el datagrama IP (eliminando la cabecera IP) y entrega el datagrama original intacto. El uso de un túnel abarca todo el proceso de encapsulación, enrutamiento y desencapsulación

Los ahorros se estiman aproximadamente entre un 30% y 50% para la interconexión de las sedes principales con sus sucursales.

En los últimos años se ha observado una fuerte tendencia al desarrollo redes virtuales privadas utilizando Internet, ya que así se reducen aún más los costos de implementación y se alcanza la conectividad global. Por ello, se habla de *intranet*,

donde se utilizan tecnologías de Internet a lo largo de la organización y de *extranet*, donde se extiende fuera de las fronteras de la organización el acceso a clientes, socios, proveedores, etc.

2.7 Fuentes de Seguridad

La seguridad informática va adquiriendo una importancia creciente con el aumento del volumen de información importante que se halla en las computadoras distribuidas. Por lo mismo se buscan maneras de que la información solo sea alcanzada por la gente adecuada, y no por terceros que no deberían tener acceso a ella. Para ello se han desarrollado diversos métodos.

2.7.1 Firewalls [2] [9]

Un **cortafuegos** (o ***firewall*** en inglés), es un elemento de hardware o software utilizado en una red de computadoras para controlar las comunicaciones, permitiéndolas o prohibiéndolas según las políticas de red que haya definido la organización responsable de la red. Su modo de funcionar es indicado por la recomendación RFC 2979, que define las características de comportamiento y requerimientos de interoperabilidad. La ubicación habitual de un cortafuegos es el punto de conexión de la red interna de la organización con la red exterior, que normalmente es Internet; de este modo se protege la red interna de intentos de acceso no autorizados desde Internet, que puedan aprovechar vulnerabilidades de los sistemas de la red interna.

También es frecuente conectar al cortafuegos una tercera red, llamada zona desmilitarizada o DMZ, en la que se ubican los servidores de la organización que deben permanecer accesibles desde la red exterior.

Sin embargo un Firewall no protege por sí mismo la red corporativa de las amenazas de ataque presente en la Internet, dado que información importante como: nombres de usuarios, contraseñas, direcciones de servidores, entre otros, son visibles para los *hackers*. Por ello en una VPN se habilita un tunel privado, a través del uso de algoritmos de encriptamiento, lo que posibilita el uso de un medio público y compartido como la Internet para transmisión de datos seguros.

2.7.2 Encriptación [1]

Las Redes Virtuales Privadas basan gran parte de su seguridad en los sistemas criptográficos modernos.

Un criptosistema o sistema de cifrado es un método de alterar mensajes de tal forma que sólo personas que conozcan esa alteración, puedan conocer el mensaje de origen. Criptografía es el arte de crear criptosistemas. Criptoanálisis es el arte de romper criptosistemas, es decir ver el mensaje original a través de las modificaciones aplicadas sobre este sin ser la persona receptora del mensaje.

El mensaje original es conocido como "texto puro" o “texto en claro” y el mensaje modificado se conoce como "texto cifrado". Encriptar es el proceso de crear "texto cifrado" a partir de "texto puro". Desencriptar es crear, por medio de cualquier proceso, "texto puro" a partir de "texto cifrado"

Un criptosistema está compuesto normalmente por una colección de algoritmos.

La teconólgia VPN apoyada en las técnicas de criptogría, encripta la información de la siguiente forma: en ambos extremos del tunel VPN se coloca un *Gateway* ó traductor en hardware ó software. En el extremo trasmisor dicho gateway encripta la información dentro de un “Cipher-Text” antes de enviar la información encriptada a través de la Internet. El gateway receptor restaura la información encriptada a un “Clear-Text”.

En la criptografía moderna tenemos 2 tipos:

- Criptografía Simétrica
- Criptografía Asimétrica

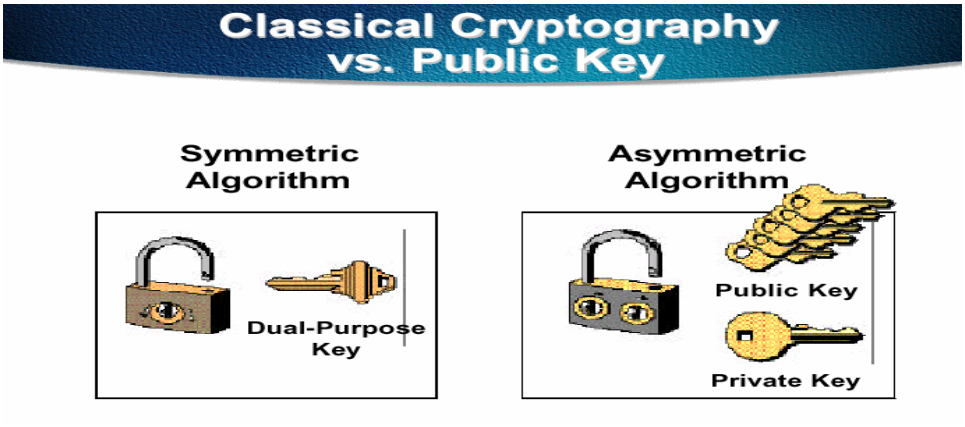

Figura 3. Clasificación de Criptografías. Fuente: [8], pag 31

2.7.2.1 Simétrica

En un criptosistema clásico, tenemos el mensaje P (de plaintext en inglés), una función de encriptación E(k) y una función de desencriptación D(k) que utilizan una clave k de tal forma que:

$$D(k)\,[E(k)\,[P]\,] = P$$

Es la forma más clásica de criptografía. Con este tipo de criptografía A y B comparten una clave secreta k que utilizan para encriptar y desencriptar mensajes. Esto requiere un acuerdo previo entre A y B mediante un canal seguro para acordar y comunicar dicha clave secreta.

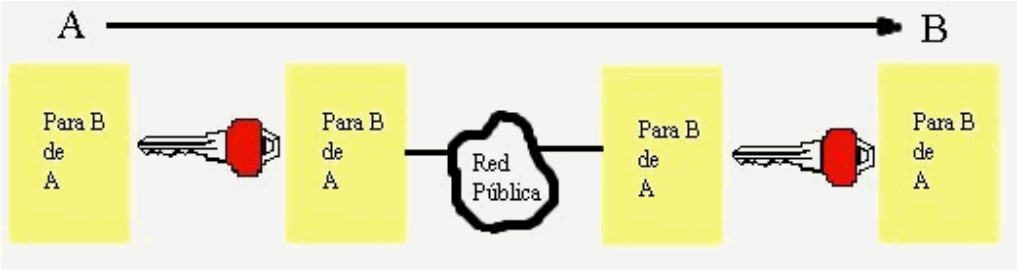

Figura 4. Esquema general de Criptografía Simétrica. Fuente: [1] pag. 32

Existen sistemas para comunicarse de forma segura a través de redes públicas usando claves simétricas; el más notable es Kerberos. Sin embargo estos sistemas no soportan bien comunidades grandes de usuarios, pierden seguridad y necesitan de medidas extras, como almacenar la clave simétrica en un servidor seguro centralizado.

2.7.2.2 Asimétrica o Claves Públicas.

En contraste con la criptografía simétrica, la criptografía de clave pública es relativamente joven. Fue concebida por Diffie and Hellman en 1976 y en 1977 Rivest, Shamir y Adelman inventaron el criptosistema RSA, la primera realización de un sistema de clave pública.

Siguiendo la nomenclatura de la clave simétrica anterior diríamos que:

$$D(k')\,[E(k)\,[P]\,] = P$$

La criptografía de clave pública se basa en la utilización de dos claves k y k', en contraste con la criptografía simétrica que sólo utiliza k. La particularidad del sistema de encriptación de clave pública se fundamenta en la relación entre estas dos claves. El resultado de encriptar un texto con una de las claves sólo es recuperable desencriptando con su pareja y viceversa. Una de las claves la guarda el usuario manteniéndola en secreto (clave privada) y distribuye libremente la otra (clave pública).

La propiedad básica de un sistema de encriptación de clave pública es que dada una clave de encriptación k es técnicamente imposible calcular la clave de desencriptación k'. Esta propiedad permite a B públicar su clave k. Cualquiera puede utilizar esta clave para encriptar un mensaje que sólo la clave privada k' de B puede desencriptar. Decimos así que B posee el par de claves.

El proceso para encriptar un mensaje con un sistema de clave pública es computacionalmente mucho más pesado que hacer lo mismo con un sistema de clave simétrica. Esto ha llevado a que en la práctica el proceso de encriptación se realice mediante una clave simétrica y después encriptar la propia clave simétrica con un sistema de clave pública como RSA. Así decimos que el sistema de clave pública transporta la llave simétrica.

Ya que la clave simétrica K es más corta que el mensaje a encriptar, esta técnica resulta significantemente más rápida que hacer lo mismo con un sistema de clave pública.

$$D(k') [E(k) [K]] = K$$

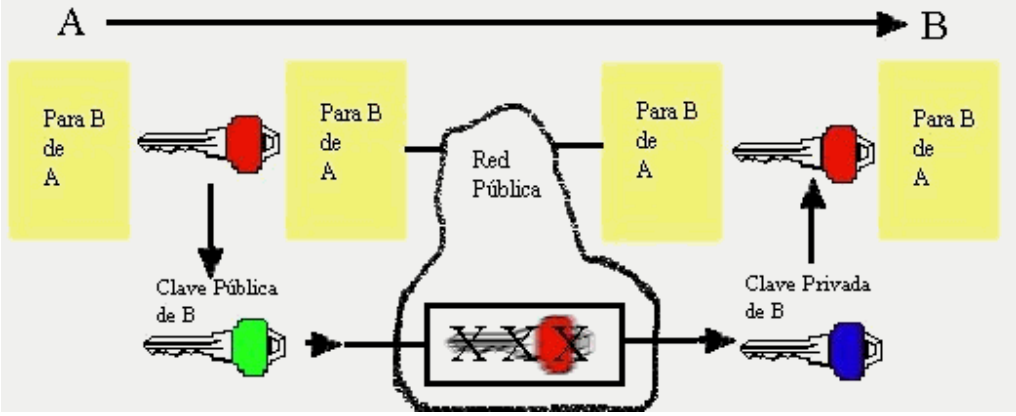

Figura 5. Esquema detallado de Criptografía Asimétrica. Fuente [1] pag. 34

2.7.3 Autenticación en origen

Por autenticación se entiende cualquier método que permita comprobar de manera segura alguna característica sobre un objeto. Dicha característica puede ser su origen, su integridad, su identidad, etc.

Autenticación de mensaje. Es aquel donde se desea garantizar la procedencia de un mensaje conocido, de forma que podamos asegurarnos de que no es una falsicación. Este mecanismo se conoce habitualmente como firrma digital.

2.7.4 Función Hash

Una función hash se usa para crear un extracto o digesto del mensaje (message digest) que puede ser usado para generar la firma digital. Las funciones Hash sirven para comprimir un texto en un bloque de longitud fija. Se utiliza en autenticación y firma digital.

Se procesa un mensaje para producir un condensado del mensaje, luego se encripta el extracto del mensaje con la clave privada y se envía anexo al mensaje. Cuando el receptor recibe el mensaje, procesa el mensaje con la misma función hash, descifra el extracto y lo compara con el que el que él obtuvo. Si son iguales, el mensaje se considera válido y no alterado.

Así, el proceso de firma de un mensaje se compone de dos pasos: el primero es la ejecución del proceso hash sobre el mensaje a firmar H(M), que genera una huella digital. La huella digital hash resultante se encripta con la clave privada produciendo la firma digital E[H(M)] y se envía al destinatario junto con el mensaje.

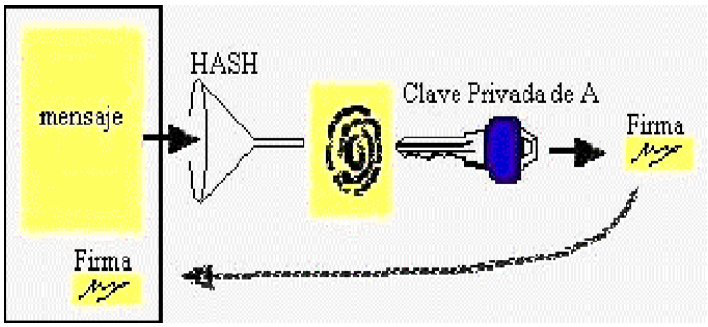

Figura N° 6. Firma Digital: resumen encriptado de un mensaje. Fuente [8] pag. 34

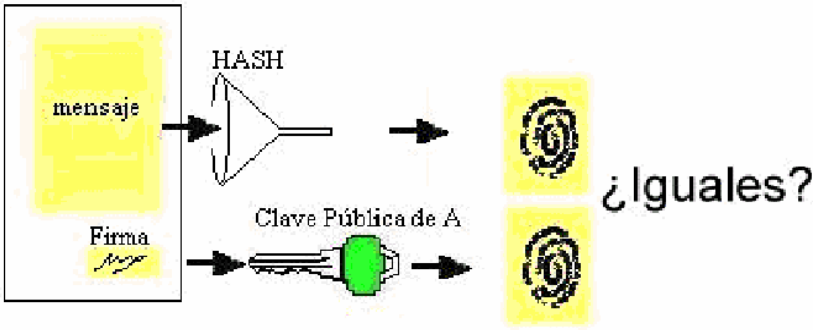

Figura N° 7. Prueba de la autenticidad de un mensaje. Fuente [8] pag 34

La funciones de Hash son públicas e irreversibles. No encriptan, sólo comprimen los textos en un bloque de longitud fija. Es decir, no se puede recuperar el texto desde el resumen, pero deben cumplir las siguientes condiciones:

- Tranformar un texto de longitud variable en un bloque de longitud fija.
- Ser irreversibles
- Conocido un mensaje y su función Hash debe ser imposible encontrar otro mensaje con la misma función Hash. Esto se debe cumplir para evitar que los criptoanalistas firmen un mensaje propio como si fueran otra persona.
- Es imposible inventar dos mensajes cuya función Hash sea la misma.

Los algoritmos más utilizados son:

MD5 (Message Digest 5) Inventado en 1992 por Riverst. La longitud del bloque es de 128 bits. Es de libre circulación.

SHA. (Security Hash Algorithm) Inventado en 1994 por la agencia americana NIST. La longitud del bloque es de 160 bits. Para su utilización se necesita permiso de los E.E.U.U.

2.7.5 Diffie-Hellman

Este es el método del establecimiento de una llave comunitaria sobre un medio inseguro. Solamente se puede usar para intercambiar claves simétricas, pero ésta es una de las principales funciones de los algoritmos asimétricos; por ello está muy extendido en sistemas de Internet con confidencialidad de clave simétrica como VPNs.

Está basado en un algoritmo discreto. Está función es la inversa de la potencia discreta, es decir, de calcular una potencia y aplicar una función mod.

La generación de claves públicas es la siguiente:

- Se busca un número grande y primo llamado q.
- Se busca α raiz primitiva de q. Para ser raiz primitiva debe cumplir que:
  A mod q, α^2 mod q, α^3 mod q, …, α^{q-1} mod q son números diferentes.
- α y q son claves públicas.

Para compartir una clave simétrica se realiza el proceso indicado en la Figura XX.

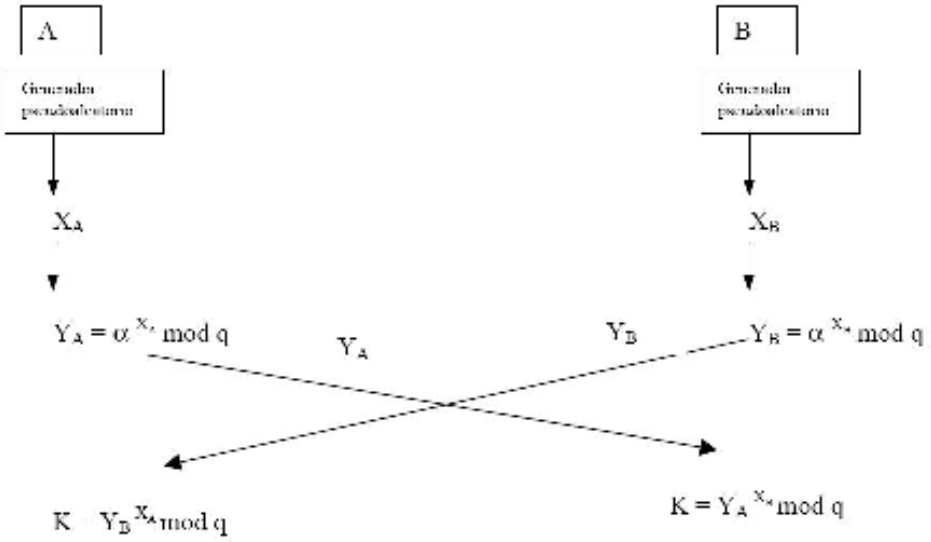

Figura 8. Transmisión de clave secreta con Diffie-Hellman.

"La K calculadas por los dos usuarios son iguales por la propiedad distributiva de la multiplicación, así:

$K = Y_B^{X_A} \bmod q = (\alpha^{X_B} \bmod q)^{X_A} \bmod q = \alpha^{X_A X_B} \bmod q =$

$(\alpha^{X_A} \bmod q)^{X_B} \bmod q = Y_A^{X_B} \bmod q = K$

Los criptoanalistas sólo disponen de las Y_i, q y α. Por lo tanto necesitan conocer alguna de las dos X_i, para esto deben realizar el logaritmo discreto $Ind_{\alpha,q}(Y_i)$ y esta operación no tiene una solución analítica para números grandes.

En un sistema con múltiples usuarios que quieren compartir claves simétricas uno a uno se publican todas las Y_i en un directorio accesible. Cuando se quiere enviar un mensaje encriptado con otro usuario se realiza el proceso:

1. El emisor coge del directorio la Y_R del receptor.
2. El emisor calcula la clave K con su número secreto X_E.
3. Se envía el mensaje encriptado con K.
4. El receptor, para calcular K, utiliza su número secreto X_R y coge del directorio la Y_E del emisor." [9]

2.8 Protocolos de VPNs [1]

Existen diversos tipos de protocolos al momento de usar VPNs, de los cuales se mencionarán solo alguno de ellos.

2.8.1 PPTP (Point-to-Point Tunneling Protocol):

"Es un protocolo de red creado por Microsoft que permite la realización de transferencias seguras desde clientes remotos a servidores emplazados en redes privadas, empleando para ello tanto líneas telefónicas conmutadas como Internet.

En el escenario típico de PPTP, el cliente establecerá una conexión a través de una linea telefónica *dial-up* con el servidor de acceso a red (NAS) del proveedor del servicio, empleando para ello el protocolo PPP.

Una vez conectado, el cliente establecerá una segunda conexión con el servidor PPTP el cual estará situado en la red privada. Dicho servidor será utilizado como intermediario de la conexión, recibiendo los datos del cliente externo y transmitiéndolos al correspondiente destino en la red privada.

PPTP encapsula los paquetes PPP en datagramas IP. Una vez que los datagramas llegan al servidor PPTP, son desensamblados con el fin de obtener el paquete PPP y desencriptados de acuerdo al protocolo de red transmitido. PPTP soporta los protocolos de red IP, IPX, y NetBEUI. Se utiliza una versión modificada del Generic Routing Encapsulation (GRE) para encapsular los paquetes PPP como datos para el túnel, de forma que estos puedan viajar cifrados y comprimidos." [1]

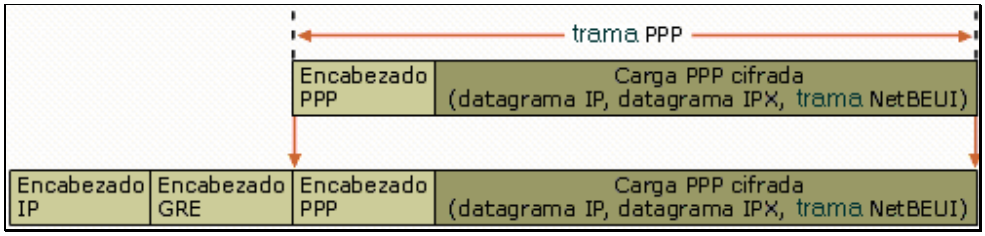

Figura 9. Estructura de un paquete PPTP. Fuente [1] pag. 38

2.8.2 L2F (Layer 2 Forwarding):

Desarrollado por Cisco Systems, tiene como objetivo proporcionar un mecanismo de tunneling para el transporte de tramas a nivel de enlace (HDLC, PPP, SLIP, etc.). El proceso de tunneling involucra tres protocolos diferentes: Protocolo pasajero, protocolo encapsulador, y protocolo portador.

El protocolo pasajero representa el protocolo de nivel superior que debe encapsularse (PPP, SLIP, etc). A continuación, el protocolo encapsulador indica el protocolo que será empleado para la creación, mantenimiento y destrucción del túnel de comunicación. En este caso, el protocolo encapsulador será L2F. Por último, el protocolo portador será el encargado de realizar el transporte de todo el conjunto.

Por lo general, este protocolo suele ser IP, dadas sus capacidades de enrutamiento, su acople a los diferentes medios y su estandarización dentro del ámbito de Internet.

Entre las principales ventajas que ofrece el protocolo L2F, cabe destacar el soporte multiprotocolo, la multiplexación de múltiples sesiones remotas (minimizando el número de túneles abiertos en un momento dado), y la gestión dinámica de los túneles, en la cual los recursos de los servidores de acceso a la red se minimizan al iniciar los túneles únicamente cuando existe tráfico de usuario. Además, por cada túnel L2F establecido, el proceso de seguridad genera una clave aleatoria como medida de prevención ante posibles ataques basados en falsificación de la fuente (*spoofing*). A su vez, en el interior de los túneles, cada una de las sesiones multiplexadas mantiene un número de secuencia para evitar problemas debidos a la duplicidad de paquetes. [1] [Cisco.com]

2.8.3 L2TP (Layer 2 Tunneling Protocol):

Este protocolo de túnel de capa 2 es el resultado de la combinación de los protocolos L2F y PPTP. Permite la creación de túneles a través de una gran variedad de tipos de redes (IP, SONET, ATM) para el transporte de tráfico PPP.

Los túneles L2TP pueden llevarse a cabo tanto en redes públicas IP como en redes privadas. Esto provoca que tanto los paquetes de control como los paquetes de datos sean vulnerables frente a posibles ataques como *snooping,* negación de servicio, modificaciones, o incluso interceptación de los procesos de negociación de la encriptación (ECP) y de la compresión (CCP) con el fin de provocar la supresión de los mecanismos de confidencialidad o en su caso, obtener el acceso a las contraseñas de los usuarios.

Para evitar todas estas posibles situaciones, el protocolo de seguridad debe proporcionar autenticación así como mecanismos para asegurar la integridad y la protección de los paquetes de control, además de la confidencialidad de todos los paquetes. Para poder alcanzar este nivel, es que usualmente se utiliza L2TP conjuntamente con IPSec.

2.8.4 SSL (Secure Socket Layer):

La Capa de conectores seguros es un protocolo que suministra un canal seguro. Con SSL, el cliente y el servidor utilizan una cierta técnica para acordar el nivel de seguridad que quieren usar durante la sesión. La identificación ocurre sobre un canal seguro y toda la información se transmite sobre las sesiones encriptadas.

"SSL proporciona sus servicios de seguridad cifrando los datos intercambiados entre el servidor y el cliente con un algoritmo de cifrado simétrico, que puede elegirse entre DES, triple-DES, RC2, RC4 o IDEA entre otros, y cifrando la clave de sesión de los algoritmos anteriores mediante un algoritmo de cifrado de clave pública, típicamente el RSA. La clave de sesión es la que se utiliza para cifrar los datos que vienen del y van al servidor seguro. Se genera una clave de sesión distinta para cada transacción, lo cual permite que aunque sea reventada por un atacante en una transacción dada, no sirva para descifrar futuras transacciones. MD5 o SHA se pueden usar como algoritmos de resumen digital (hash). Esta posibilidad de elegir entre tan amplia variedad de algoritmos dota a SSL de una gran flexibilidad criptográfica.

Durante el protocolo SSL, el cliente y el servidor intercambian una serie de mensajes para negociar las características de seguridad. Este protocolo sigue las siguientes fases (de manera muy resumida):

La fase *Hola*, se usa para ponerse de acuerdo sobre el conjunto de algoritmos para mantener la confidencialidad y para la autenticación. El navegador le informa al servidor de los algoritmos que posee disponibles. Normalmente se utilizarán los más fuertes que se puedan acordar entre las dos partes. En función de las posibilidades criptográficas del navegador, el servidor elegirá un conjunto u otro de algoritmos con una cierta longitud de claves.

La fase de *autenticación*, es aquella en la que el servidor envía al navegador su certificado x.509v3 que contiene su clave pública y solicita a su vez al cliente su certificado X.509v3 (sólo si la aplicación exige la autenticación de cliente).

La fase de *creación de clave*, es aquella en la que el cliente envía al servidor una clave de sesión a partir de la cual ambos extremos cifrarán los datos intercambiados posteriormente haciendo uso del algoritmo de cifrado simétrico acordado previamente. El navegador envía cifrada esta clave usando la clave pública del servidor, que extrajo de su certificado." [1]

Por último, la fase *Fin*, es aquella en la que se verifica mutuamente la autenticidad de las partes implicadas y que el canal seguro ha sido correctamente establecido. Una vez finalizada esta fase, ya se puede comenzar la sesión segura.

De ahí en adelante, durante la sesión segura abierta, SSL proporciona un canal de comunicaciones seguro entre los servidores Web y los clientes (los navegadores) a través del cual se intercambiará cifrada la información relevante, tal como el URL y los contenidos del documento solicitado, los contenidos de cualquier formulario enviado desde el navegador, las cookies enviadas desde el navegador al servidor y viceversa y los contenidos de las cabeceras HTTP.

2.8.5 IPSec (IP Secure) [1] [10]

Representa un conjunto de mecanismos de seguridad de alta calidad basado en claves criptográficas. Proporciona un canal seguro para los datos a través de la red,

ofreciendo para ello un control de acceso, así como una integridad en los datos transmitidos, además de mecanismos de autenticación y confidencialidad. IPSec opera sobre la capa 3 de red, la capa del protocolo de Internet (IP).

Los servicios IPSec son llevados a cabo mediante el uso de dos protocolos de seguridad: *Authentication Header (AH)* y *Encapsulating Security Protocol (ESP)*, así como mediante un conjunto de protocolos necesarios para la gestión de claves criptográficas, llamado IKE (*Internet Key Exchange*). IKE se verá mas adelante.

El protocolo AH proporciona únicamente mecanismos de autenticación. Los datos de autenticación AH son insertados entre el encabezado IP y los datos referentes al paquete de nivel superior (TCP, UDP, ICMP), tal como se muestra en la siguiente figura.

Figura 10. Un paquete IPSec con el encabezado AH. Fuente [1] pag. 41

ESP ofrece confidencialidad (además de proporcionar autenticación, integridad y protección contra réplica) para la carga IP. ESP hace uso de una amplia variedad de algoritmos de encriptación entre los cuales cabe destacar DES, 3DES, CAST128 y *Blowfish*. Por ejemplo, Bianca en el equipo A envía datos a Carlos en el equipo B. La carga IP está cifrada y firmada para garantizar su integridad. Al recibirse, una vez completado el proceso de comprobación de la integridad, se descifra la carga de datos del paquete. Carlos puede estar seguro de que fue Bianca quien le envió la información, de que la información no ha sufrido cambios y de que nadie más ha podido leerla.

ESP se identifica en el encabezado IP con el Id. de protocolo IP 50. Como se muestra en la figura siguiente, el encabezado ESP se coloca delante de la carga IP, y tras ella se incluye un finalizador ESP y un finalizador de autenticación ESP.

Figura 11. Un paquete IPSec com el encabezado y cola ESP. Fuente [1] pag. 42

La parte firmada del paquete indica dónde se firmó el paquete para confirmar su integridad y autenticación. La parte cifrada del paquete indica qué información del mismo está protegida por confidencialidad. El encabezado IP no se firma y no está necesariamente protegido frente a modificaciones. Para proporcionar integridad de datos y autenticación al encabezado IP, puede utilizarse ESP conjuntamente con AH.

El encabezado ESP contiene los campos siguientes:

1.-Índice de parámetros de seguridad: Identifica la asociación de seguridad correcta para la comunicación cuando se utiliza junto con la dirección de destino y el protocolo de seguridad (AH o ESP). El receptor utiliza este valor para determinar la asociación de seguridad con la que se debe identificar este paquete.

2.-Número de secuencia: Proporciona protección contra la réplica del paquete. El número de secuencia es un número de 32 bits que aumenta de forma incremental (a partir de 1) e indica el número de paquetes enviados a través de la asociación de seguridad de modo rápido para una comunicación dada. El número de secuencia no se puede repetir mientras perdure la asociación de seguridad de modo rápido. El receptor comprueba este campo para asegurarse de que no ha recibido ya un paquete para una asociación de seguridad con este número. Si se recibió alguno, se rechazará este paquete.

La cola ESP contiene los campos siguientes:

1.-Relleno: Es un valor entre 0 y 255 bytes y asegura que la carga cifrada junto con los bytes de relleno se ajuste a los límites de bytes que requieren los algoritmos de cifrado.

2.-Longitud de relleno: Indica la longitud en bytes del campo Relleno. El receptor utiliza este campo para quitar los bytes de relleno una vez descifrada la carga cifrada que los contiene.

3.-Siguiente encabezado: Identifica el tipo de datos de la carga, por ejemplo TCP o UDP.

La cola de autenticación ESP contiene el valor de comprobación de integridad (ICV), también conocido como código de autenticación de mensaje, que se utiliza para comprobar la autenticación del mensaje y su integridad. El receptor calcula el valor de ICV y lo compara con este valor (calculado por el remitente) para comprobar la integridad. El ICV se calcula para el encabezado ESP, los datos de la carga y el finalizador ESP.

El protocolo IPSec que se describe se conoce como el modo *transporte*. Existe también el modo *túnel*, donde se añade una nueva cabecera IP que puede contener direcciones distintas, tales como las direcciones de los firewalls. La cabecera IP interna transporta las direcciones fuente y destino.

El modo túnel protege los paquetes IP completos, pues los trata como una carga AH o ESP. Todo el paquete IP se encapsula con un encabezado AH o ESP y un encabezado IP adicional. Las direcciones IP del encabezado IP externo son los extremos del túnel, y las direcciones IP del encabezado IP encapsulado son las direcciones últimas de origen y de destino.

Como se muestra en la siguiente figura, el modo de túnel AH encapsula un paquete IP con un encabezado AH e IP y firma todo el paquete para asegurar su integridad y autenticación.

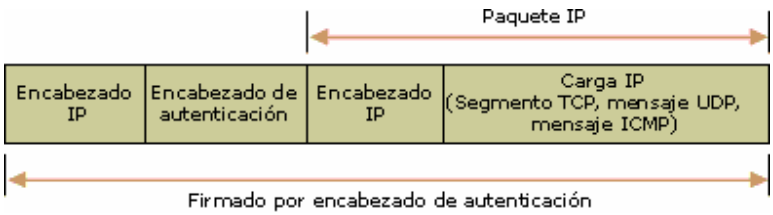

Figura 12. Un datagrama IPSec-AH en modo túnel. Fuente [1] pag 44

El modo túnel ESP encapsula un paquete IP con un encabezado ESP e IP y un finalizador de autenticación ESP. La parte firmada del paquete indica dónde se firmó el paquete para confirmar su integridad y autenticación. La parte cifrada del paquete indica qué información del mismo está protegida por confidencialidad.

Debido al nuevo encabezado agregado al paquete para el túnel, todo lo que sigue al encabezado ESP está firmado (excepto el finalizador de autenticación ESP), ya que ahora se encuentra encapsulado en el paquete enviado por el túnel.

El encabezado original se coloca después del encabezado ESP. El paquete entero se anexará con un finalizador ESP antes del cifrado. Todo lo que sigue al encabezado ESP, salvo el finalizador de autenticación ESP, se cifra.

Esto incluye el encabezado original, que ahora se considera parte de los datos del paquete.

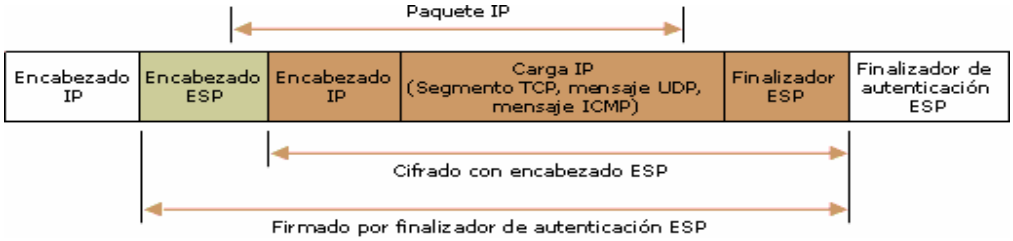

Figura 13. Un paquete IPSec-ESP en modo túnel. Fuente [1] pag 45

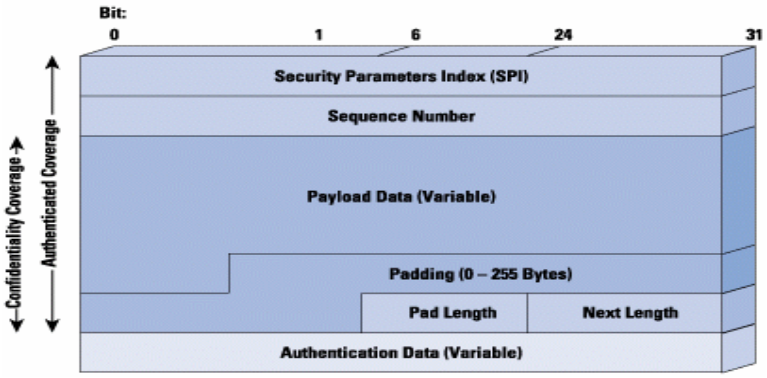

Figura 14. Detalle del header ESP. Fuente [8] pag. 43

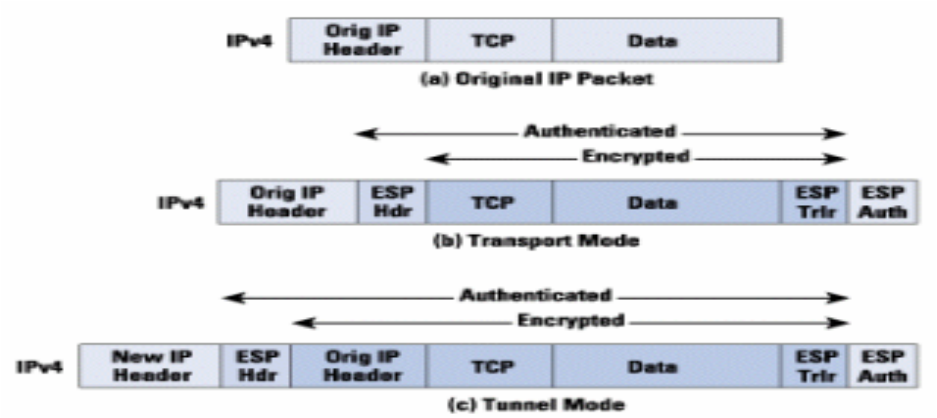

Figura 15. Estructura de los Datagramas. Fuente [8] pag. 43

Toda la carga ESP se encapsula dentro del nuevo encabezado de túnel, el cual no se cifra. La información del nuevo encabezado de túnel sólo se utiliza para enrutar el paquete desde el origen hasta el destino. Si el paquete se envía a través de una red pública, se enrutará hacia la dirección IP del servidor de túnel de la intranet receptora.

En la mayoría de los casos, el paquete irá destinado a un equipo de una intranet. El servidor de túnel descifra el paquete, descarta el encabezado ESP y utiliza el encabezado IP original para enrutar el paquete hacia el equipo de la intranet.

ESP y AH pueden combinarse al utilizar túneles para lograr tanto la confidencialidad del paquete IP enviado por el túnel como la integridad y la autenticación de todo el paquete.

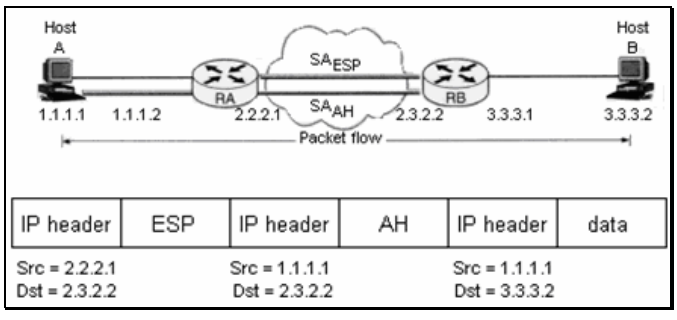

Figura 16. Combinación de ESP y AH. [1] pag. 46

Los túneles IPSec se utilizan principalmente para la interoperabilidad con otros routers, puertas de enlace o sistemas finales que no admiten conexiones L2TP/IPSec o PPTP.

El modo túnel de IPSec se admite como característica avanzada y sólo se utiliza en túneles entre puertas de enlace (también conocidos como túneles entre routers) y para configuraciones de servidor a servidor o de servidor a puerta de enlace.

2.8.6 IKE [1] [10]

Antes de que se pueda intercambiar información protegida, debe establecerse un acuerdo de seguridad entre los dos equipos. En ese acuerdo de seguridad, denominado asociación de seguridad (SA), los dos equipos establecen el modo de intercambiar y proteger la información, como se muestra en la ilustración siguiente.

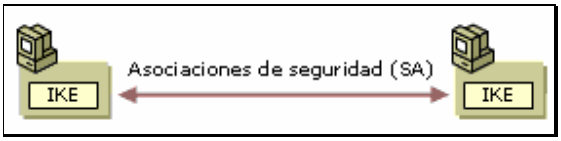

Figura 17. Concepto de la asociación de seguridad. Fuente [1] pag. 46

Con el fin de establecer este acuerdo entre los dos equipos, IETF ha establecido un método estándar de asociación de seguridad y resolución de intercambio de claves denominado Intercambio de claves de Internet (IKE: *Internet Key Exchange*), que es una variante de ISAKMP/Oakley (*Internet Security Association and Key Management Protocol/Oakley Key Determination Protocol*). Este protocolo presenta tres características principales:

- Asegura que la comunicación IPSec y el intercambio de claves se lleve a cabo entre partes autenticadas.
- Negocia los protocolos, algoritmos, y claves que serán utilizados en la comunicación IPSec.
- Proporciona un método seguro para actualizar y renegociar asociaciones una vez que éstas han expirado.

Una asociación de seguridad (SA) es la combinación de una clave negociada, un protocolo de seguridad y el índice de parámetros de seguridad (SPI), que conjuntamente definen el método de seguridad utilizado para proteger la comunicación desde el remitente hasta el receptor. El SPI es un valor único e identificable de la SA utilizado para distinguir entre las múltiples asociaciones de seguridad que existen en el equipo receptor. Por ejemplo, pueden existir varias asociaciones si un equipo mantiene comunicaciones seguras con varios equipos a la vez.

IKE funciona con dos fases. En la primera, los dos extremos crean una asociación bidireccional, estableciendo con ello un canal seguro entre ellos. Ya en la segunda fase, este canal será empleado para realizar la negociación de las asociaciones IPSec. La confidencialidad y la autenticación se aseguran durante cada una de las fases mediante el uso del cifrado y los algoritmos de autenticación acordados entre los dos equipos durante las negociaciones de seguridad. Al estar las tareas divididas entre las dos fases se agiliza la creación de claves.

Los siguientes son brevemente los pasos de que constan las 2 fases de IKE.

Fase I o negociación de modo principal

1. Negociación de directivas: Los cuatro parámetros obligatorios siguientes se negocian como parte de la SA de modo principal son: Algoritmo de cifrado (DES, 3DES o AES), algoritmo de integridad (MD5 o SHA1), Grupo Diffie-Hellman que se utilizará para el material base de generación de claves (768 bits, 1024 bits o 2048 bits), el método de autenticación (Kerberos V5, certificado o autenticación por claves compartidas previamente)

2. Intercambio Diffie-Hellman: Las claves reales no se intercambian en ningún momento. Sólo se intercambia la información básica que requiere el algoritmo de determinación de la clave Diffie-Hellman para generar la clave secreta compartida. Después de este intercambio, el servicio IKE de cada equipo genera la clave principal utilizada para proteger la autenticación.

3. Autenticación: Para impedir un ataque por usuario interpuesto, los equipos intentan autenticar el intercambio de claves Diffie-Hellman. Si se produce un error en

la autenticación, no se continuará con la comunicación. Para autenticar las identidades se utiliza la clave principal junto con los algoritmos y métodos de negociación. Los algoritmos de hash y cifrado se aplican a toda la carga de identidad mediante las claves generadas a partir del intercambio Diffie-Hellman del segundo paso. La carga incluye el tipo de identidad (para autenticación), puerto y protocolo. IPSec utiliza los siguientes tipos de identidad para autenticación: para autenticación de certificados, el nombre completo de certificado y el nombre general; para Kerberos V5 y autenticación por clave compartida previamente, direcciones IPv4, el nombre de dominio completo (FQDN) del equipo y FQDN para el usuario. La carga de identidad queda protegida frente a modificaciones e interpretaciones, independientemente del método de autenticación empleado.

El remitente presenta una oferta para establecer una posible asociación de seguridad con el receptor. El interlocutor de respuesta no puede modificar la oferta. En caso de que se modifique la oferta, el interlocutor inicial rechazará el mensaje del interlocutor que responde. El interlocutor que responde envía una respuesta para aceptar la oferta o bien una respuesta con alternativas.

Los mensajes enviados durante esta fase tienen un ciclo de reintento automático que se repite cinco veces. Si se recibe una respuesta antes de que termine el ciclo de reintento, comienza la negociación de SA estándar.

No hay ningún límite preestablecido en cuanto al número de intercambios que pueden tener lugar. El número de SA que se pueden establecer sólo está limitado por los recursos del sistema.

Fase II o SA de modo rápido

1. Se negocia la directiva: Los equipos con IPSec intercambian la siguiente información para proteger la transferencia de datos: Protocolo IPSec (AH o ESP), algoritmo de hash para la integridad y autenticación (MD5 o SHA1), algoritmo para el cifrado, si se solicita (AES, 3DES o DES). Finalmente se llega a un acuerdo y se establecen dos SA. Una SA para la comunicación entrante y la otra para la comunicación saliente.

2. El material de clave de sesión se actualiza o se intercambia: IKE actualiza el material de generación claves, y se generan nuevas claves compartidas para la integridad de los datos, la autenticación y el cifrado (si se ha negociado). Si es necesario volver a generar las claves, se produce un segundo intercambio Diffie-Hellman o se actualiza la clave Diffie-Hellman original.

3. Las SA y las claves, junto con el SPI, se pasan al controlador de IPSec.

La segunda negociación de la configuración de seguridad y el material de claves (con el fin de proteger los datos) está protegida por la SA de modo principal. Mientras que la primera fase protege la identidad, la segunda fase proporciona protección mediante la actualización del material de las claves antes de enviar los datos. IKE puede dar cabida a una carga de intercambio de claves para realizar un intercambio Diffie-Hellman adicional si es necesario volver a generar las claves; es decir, si está habilitada la confidencialidad directa perfecta (PFS, Perfect Forward Secrecy) de clave de sesión. De lo contrario, IKE actualiza el material de las claves obtenido en el intercambio Diffie-Hellman del modo principal.

El modo rápido produce un par de asociaciones de seguridad, cada una de ellas con su propio SPI y su clave. Una SA se utiliza para la comunicación entrante y la otra para la comunicación saliente.

El uso de una única SA de modo principal para varias negociaciones de SA de modo rápido aumenta la velocidad del proceso. Mientras la SA de modo principal no caduque, no es necesario volver a negociar o a autenticar. El número de negociaciones de SA de modo rápido que pueden realizarse viene determinado por la configuración de la directiva IPSec.

La SA de modo principal se almacena en caché para permitir múltiples negociaciones de SA de modo rápido (salvo en el caso de que esté habilitada PFS de clave de sesión). Cuando se llega a una cierta duración de la clave principal o de sesión, se vuelve a negociar la SA. Además, la clave se actualiza o se vuelve a generar.

Cuando transcurre el periodo predeterminado de tiempo de espera para la SA de modo principal, o cuando se alcanza la duración de la clave principal o de sesión,

se envía un mensaje de eliminación al interlocutor que responde. El mensaje de eliminación de IKE indica al interlocutor que responde que la SA de modo principal ha caducado. De este modo se impide la creación de nuevas SA de modo rápido a partir de la SA de modo principal caducada. IKE no hace caducar la SA de modo rápido, ya que sólo el controlador de IPSec contiene el número de segundos o bytes que han transcurrido hasta alcanzar la duración.

Internet Security Association and Key Management Protocol (ISAKMP)

Este es un protocolo que define los mecanismos de la implementación de protocolos de intercambio de llaves y negociación de políticas de seguridad.

IKE solo existe para establecer SAs para IPsec. Antes de que pueda hacer esto IKE puede negociar aun SA (un ISAKMP SA) relacionado con el par. Ya que IKE negocia su propia política, es posible configurar múltiples declaraciones de política con la configuración de diferentes estados, y luego dejar que los dos anfitriones llegar a un acuerdo. ISAKMP negocia:

- Algoritmo de Encriptación: este se limita a 56-bit DES solamente.
- Algoritmo de cortado: MD5 o SHA
- Autenticación: firmas RSA o llaves pre-compartidas.
- Tiempo de vida de la SA: en segundos.

La negociación IKE se hace por el puerto UDP 500.

2.9 Bloqueo de puertos [8]

Además del filtrado basado en direcciones IP, los routers con filtrado y los firewalls pueden ver información disponible en el nivel de transporte del stack del protocolo y tomar decisiones de envío basadas en ella. El nivel de transporte es responsable de enviar paquetes de modo confiable entre sistemas y para administrar múltiples sesiones a través de la misma conexión de red. Cada sesión tiene su propio canal. Por ejemplo, si se utiliza FTP para pedir un archivo desde un servidor, la peticiones se envían por un canal y el archivo se transmite por otro. El punto final del canal se llama *puerto*. FTP normalmente utiliza los puertos 20 y 21.

La idea básica es bloquear un puerto si no se quiere que alguien lo utilice de modo inapropiado. Por ejemplo, si no ejecuta servicios FTP, se puede configurar el enrutador con filtrado para que bloquee los puertos 20 y 21. Mirando esto de modo diferente, si se quiere suministrar sólo servicios WWW en un servidor conectado directamente con Internet, se puede bloquear los demás puertos excepto el 80, que es el puerto HTTP.

De esta forma se pueden cerrar puertos que utilicen protocolos peer to peer. Bloquear P2P que son los utilizados por programas de descargas como Edonkey/emule, KaZaA, BitTorrent, Ares, entre otros.

2.10 Redunda de equipos

2.10.1 Protocolo de redundancia de router virtual. Virtual Router Redundancy Protocol

Pensando en la posibilidad de que el único enlace WAN que se posee, falle, la IETF definió el estándar RFC 3768 el cual consiste en tener 2 o más salidas WAN diferentes, para que en el momento de que una falle, el tráfico comience a ser enrutado por otro router.

El VRRP (*Virtual Router Redundancy Protocol*) es un protocolo que se encarga de asignar dinámicamente la función de router virtual a uno de los routers dentro de una LAN. El router que controla la dirección asociada al router virtual se denomina *Master*, y se encarga de encaminar los paquetes enviados a través de esa dirección IP. Cuando el *Master* deja de encontrarse disponible, otro de los routers VRRP asume la responsabilidad de encaminamiento sobre la dirección del router virtual, proporcionando de este modo recuperación dinámica frente al fallo producido. Esto permite que cualquiera de las direcciones IP asociadas al router virtual pueda ser utilizada como dirección de primer salto (o ruta por defecto) de los equipos que se encuentran en la red LAN.

La principal ventaja obtenida de la utilización del VRRP es una mayor disponibilidad del router por defecto sin necesidad de configurar encaminamiento dinámico o protocolos de descubrimiento de routers en cada equipo final. El VRRP está diseñado para eliminar el punto único de fallo inherente en los entornos configurados con ruta por defecto estática. [11]

2.10.2 Hot Standby Router Protocol (HSRP)

Cisco Systems ha desarrollado el Hot Standby Router Protocol (HRSP), el cual es un protocolo de redundancia que se ha desarrollado para el segmento LAN, donde hay una gran cantidad de routers y dispositivos que utilizan solamente una dirección IP estática para el gateway predeterminado.

A intervalos regulares, los routers, intercambian información para determinar cuales de ellos siguen estando presentes y son capaces de reenviar tráfico. Si falla el router principal, master o primario, de un grupo de routers con HSRP, hay un router de reserva en el mismo grupo que empieza a reenviar el tráfico. Dado que los routers deciden por si mismos cuál reenvía el tráfico a la dirección virtual y dado que las estaciones de trabajo de un segmento sólo conocen la dirección IP virtual como su gateway predeterminado, un fallo del router principal es prácticamente indetectable por parte de los usuarios de estaciones de trabajo y no requiere intervención por parte del usuario o del administrador de la red.

HSRP es muy flexible. El administrador de red puede controlar todo el comportamiento de los routers de un grupo (incluyendo que router es el principal, cuales son los routers de reserva, si éstos conservan la función de reenvío cuando pueda volver a utilizarse el router principal, y la capacidad de otra interfaz del router para conducir el tráfico al router de reserva). [12]

CAPITULO III
DISEÑO DE LA RED WAN PARA CINEX

3.1 Diseño de red WAN.

Como se mencionó en el primer capitulo, el sistema de comunicaciones de Sur Americana de Espectáculos de la empresa Cinex ha presentado inconvenientes con la perdida de conexión y no se encuentra en la capacidad de una rápida expansión para crear la estructura necesaria para integrar las localidades de Venefilms y Blancica y soportar futuros servicios que se puedan agregar a la red, además de no contar con la administración de la misma y un elevado costo por el servicio. Se plantea por tanto la necesidad de crear una nueva red WAN tipo estrella, que cumpla ciertos parámetros mínimos exigidos por la empresa, debido a la necesidad de poseer una conexión constante hacia las localidades remotas y estar en la capacidad de un posterior crecimiento de forma sencilla.

Los parámetros de diseño para la red WAN, serán las características mínimas que deberán poseer los equipos a adquirir por Cinex. Este sistema deberá prestar un adecuado servicio de comunicación entre la sede principal y sus localidades para la transmisión constante de datos. Deberá prever un posterior crecimiento del número de localidades y cubrir los servicios adicionales que la empresa pueda exigir en un futuro cercano, como es la Voz sobre IP, migración a IPv6 entre otros.

Podemos mencionar los siguientes parámetros mínimos que debe cumplir la red WAN:

- Se plantea la necesidad de que la red WAN esté en funcionamiento con celeridad, puesto que va a sustituir a la que poseen actualmente e incluir el resto de localidades que no tienen interconectadas a su red.
- Se requiere que los sistemas manejen una tecnología actual, eficiente, que permita cubrir las necesidades de la empresa y que prevea el crecimiento de la red y servicios a futuro. Además debe estar respaldado por un servicio técnico por parte del proveedor de los equipos y que permita luego la aplicación

modular del sistema. Este producto debe ser de comprobada calidad en el mercado, y debe tener presencia en sistemas similares.

- Se debe interconectar una gran área con un adecuado ancho de banda, puesto que las localidades de la empresa están dispersas por todo el país.
- La red debe disponer de un ancho de banda capaz de cubrir los requerimientos para la navegación en Internet, transmisión de datos entre la central y la localidad, que permita la conexión a equipos (computadoras) para administración remota desde la sede principal y posteriores servicios que se quieran implementar.
- Poseer un grado de confiabilidad y seguridad adecuada en los enlaces entre las localidades y la sede principal, puesto que los datos que se manejan son de gran importancia para la empresa y no deben ser visto por cualquiera.
- Capacidad del sistema para gestión remota, vía SNMP, Telnet o SSH, para actualización del sistema o configuración de algún parámetro especifico.
- Debe poder manejar técnicas para asegurar la calidad de servicio, como filtrado de paquetes, control de servicios y listas de acceso.

De esta forma la topología prevista para esto es la siguiente:

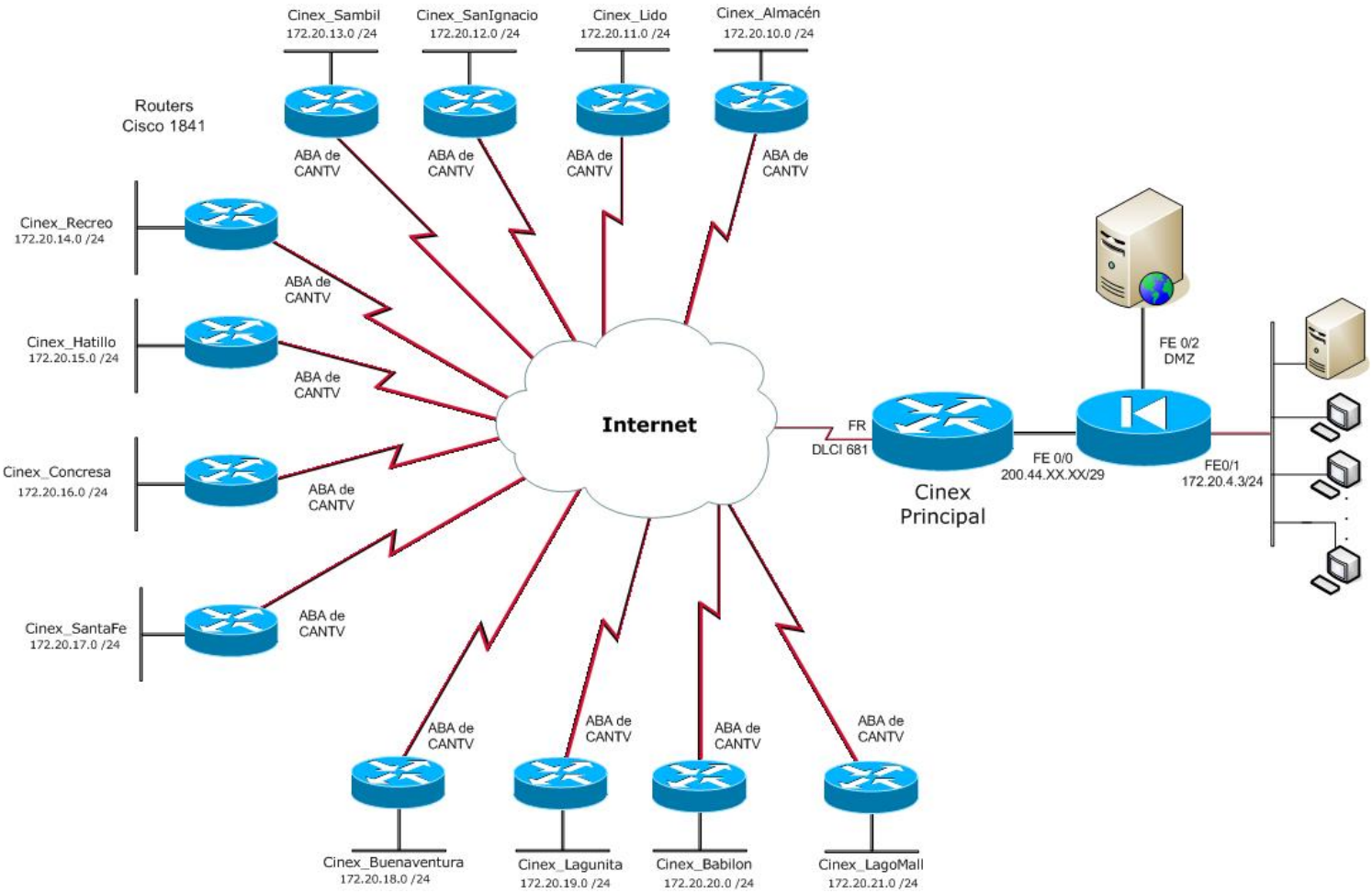

Figura 18. Topología propuesta para Cinex.

Esta es la topología propuesta para Sur Americana de Espectáculos, conformada por 12 localidades. Posteriormente se irán agregando las localidades de Blancica y Veneflims de la misma forma. En las localidades remotas se requiere por lo tanto de un router con salida a Internet.

Este diseño contempla un router en la sede Principal para dar conexión WAN y a su vez un concentrador de VPN y un equipo de seguridad, por lo que se propuso la implementación de un firewall.

3.1.1. Consideraciones preliminares importantes

Sur Americana de Espectáculos de Cinex cuenta con enlaces a 12 localidades, las cuales se concentran en un equipo en la sede principal. Estos enlaces debían permanecer activos hasta que entre en funcionamiento el nuevo, por lo que no se podía desincorporar de una vez el equipo principal del otro proveedor de servicios hasta que todos los enlaces fuesen migrados.

Al tratarse de una red tan extendida a lo largo de todo el país, son pocos los proveedores de servicios que logran ofrecer su servicio en todas las zonas. Sin embargo, en vista que en la mayoría de las localidades ya cuentan con el servicio de ABA de CANTV, que es un servicio ADSL para conectarse a Internet, la empresa prefirió concentrar todos sus enlaces con este proveedor, puesto que al ser numerosos en cantidad, es más sencillo tenerlos todos con una misma compañía. Además con los servicios de ADSL existentes se logra obtener el ancho de banda necesario para la implementación de la red que se desea en estos momentos. Adicional se dispone de disponibilidad de servicio las 24 horas del día, los 365 del año por parte del Proveedor de Servicios.

Puesto que los datos van a viajar por la red pública, Internet, cualquiera podría interceptar los mismos, por lo que se desea proporcionar un canal seguro para que estos datos no sean vistos por cualquiera que lo desee. Por esto el uso de VPN (Virtual Private Network) es muy importante de forma que otorguen la seguridad necesaria a la hora de crear los túneles para las comunicaciones de la empresa.

3.1.2 Consideraciones de diseño a nivel de capa física y de enlace

Tomando en consideración que el tráfico que va a viajar por los túneles VPN se trata solo de datos, por el momento, para el manejo remoto de host (conexión a escritorio remoto de computadoras), información de ventas de boletos y caramelearías, servicio de correo y acceso a ciertas paginas web; un enlace ABA con un ancho de banda de 512kbps se considera adecuado para cada localidad. Además no todos los hosts de la LAN de cada localidad tienen acceso a Internet, a parte de estar restringido a ciertas páginas nada más, por lo que el consumo del ancho de banda no se verá tan apremiado. Incluso con el ancho de banda de 512kbps se puede disponer de 2 líneas de VoIP con calidad de servicio y encriptación para que viaje por la VPN de aproximadamente 32kbps cada línea; y disponer de ancho de banda suficiente para seguir prestando los demás servicios.

La conexión a escritorio remoto de computadoras "...sólo transfiere los datos mínimos (como los datos de pantalla y los datos de teclado) para controlar de forma remota el equipo host. De este modo, incluso las conexiones a Internet de bajo ancho de banda le permiten controlar de forma remota el equipo distante, ya que el diseño de este software permite incluso el control, usando conexiones de baja velocidad como el clásico módem de conexión telefónica a 56 Kbps". [13]

Este servicio es posible conseguirlo a través de enlaces ADSL suministrados por los proveedores de servicios en nuestro país a precios económicos en comparación con otros servicios similares como LMDS (Servicio de Distribución Local Multipunto) y WLL (Wireless local loop). Además por ser un servicio que opera sobre el par trenzado telefónico se encuentra bien extendido a lo largo de todo el país.

De esta forma se dispondría de un enlace de última milla de par trenzado de tecnología ADSL, normalmente terminado en conectores RJ-11. Este enlace daría la conexión con la Internet, asignándo la puerta de enlace y la dirección IP de forma dinámica por DHCP.

Para la sede principal se necesita un enlace más robusto con direccionamiento fijo y público, para que de esta forma las demás localidades puedan tener un sitio fijo y donde apuntar y contra el cual cerrar los túneles VPN.

Este sitio central debe contar con mayor ancho de banda tanto de subida como de bajada, puesto que poseerá banco de datos de almacenamiento, servidores que utilizarán las localidades remotas, desde donde se harán las conexiones remotas de escritorios con los hosts de otra localidad y además brindar la salida a Internet al personal que trabaja en esta sede.

Para este enlace se utilizó tecnología Frame Relay, que garantiza un enlace estable y de gran ancho de banda, con un direccionamiento público, del cual se explicarán sus características mas adelante. Según un breve estudio del tráfico de la red en la sede principal, la misma cuenta con un tráfico pico de 800kbps en la interfaz de entrada. Este estudio se hizo a través del programa Cisco ASDM Launcher 5.2 con el que se monitoreó el tráfico que existía en la sede principal, tomando reportes a varias horas del día, en distintos días de la semana e inclusive realizando las pruebas de conexión a escritorio remoto.

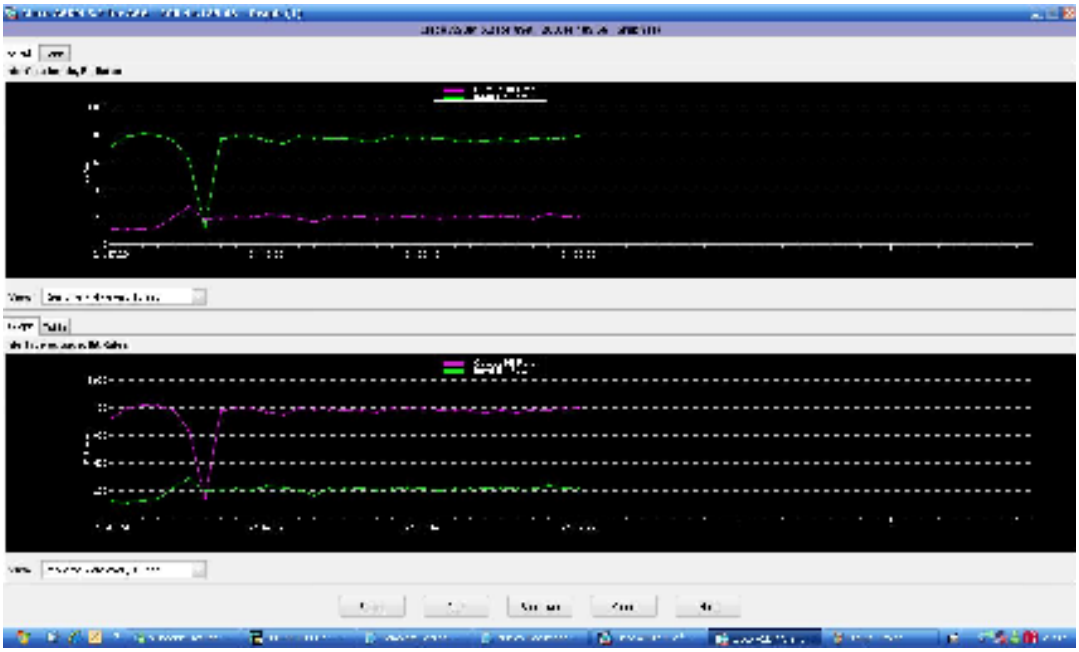

Figura 19. Captura de tráfico en la sede principal

Se recomienda un enlace de contingencia, otra forma de salir a Internet en caso de que el enlace principal se caiga. Este debe pertenecer a otro proveedor de servicios y poseer características similares al enlace principal, dirección IP pública y estática, aunque puede ser un enlace con un ancho de banda menor, puesto que este enlace solo va a actuar en caso de que se caiga el principal, de resto se mantendrá en hot standby, habilitando la salida por un router adicional que se mantendrá en HSRP (The **Hot Standby** Router Protocol) el cual se activa al observar que el enlace principal se cae, desviando el tráfico al secundario. Por el momento la empresa no tiene previsto colocar esta solución, debido al costo adicional que representa.

3.2. Consideraciones de capa de red

3.2.1. Direccionamiento IP

Esta parte del diseño consistió en estructurar y organizar el plan de direccionamiento IP a ser asignado a la empresa.

Se contará con un pool de direcciones IP públicas en la sede principal. Estas direcciones permitirán acceder a la red de Cinex desde cualquier parte. Serán direcciones clase C, por no requerir de tantas y ser más económicas; entregadas por CANTV. Del pool, conformado por 6 direcciones se usará: una para el router de salida (Internet total), una para el equipo de seguridad que además va a concentrar los túneles VPN´s, una para el servidor de correos que será implementado a corto plazo y una para realizar NAT de salidas, que es el que permite tomar las direcciones privadas o no validas de las maquinas de la LAN y transformarlas en una dirección publica o privada. Este será aclarado mas adelante. Lo que deja 2 direcciones validas para cualquier otro fin.

Para la red interna de la empresa Cinex, las direcciones que se utilizaran son direcciones privadas. Se usará una clase B puesto que es la que están usando actualmente Sur Americana de Espectáculos pero con una mascara que permita un mayor número de usuarios.

3.2.2 Asignación de direcciones a los elementos de la red

Se prevén bloques de 254 direcciones para hosts para cada localidad de Cinex.

Las direcciones a asignar se harán creando subredes de los bloques de direcciones IP:

- desde la 172.20.10.X para Sur Americana de Espectáculos.
- desde la 172.20.30.X para Venefilms
- desde la 172.20.50.X para Blanca

Esto se hará variando el tercer octeto de la dirección IP para cada una de las localidades, de la siguiente manera:

172.20.10.0/24 Sur Americana de Espectáculos, localidad 1.

172.20.11.0/24 Sur Americana de Espectáculos, localidad 2.

172.20.12.0/24 Sur Americana de Espectáculos, localidad 3.

Y así sucesivamente hasta cubrir todas las localidades.

La distribución completa de las direcciones IP con su correspondiente localidad se encuentra detallada en los anexos.

La primera dirección de subred de cada bloque se asignará a la interfaz Ethernet del router de cada localidad, por ejemplo 172.20.10.1, 172.20.30.1, etc. que va a constituir el gateway o puerta de enlace para las redes de la empresa Cinex.

Para la salida de las localidades, al poseer conexión por módem ADSL de CANTV, estas obtienen dirección IP de forma dinámica, por lo que estarán en constante variación. El tráfico proveniente de la LAN de cada localidad saldrá a través de un NAT.

3.2.3. Enrutamiento

Todas las localidades disponen de una sola salida a Internet, por lo que todo su tráfico va a salir por la única interfaz conectada a la WAN.

Se usará la ruta por defecto, 00.00.00.00 que saldrá por la interfaz ADSL. Esta ruta indica que todo el tráfico va a tomar esa salida.

3.2.4 NAT dinámico saliente

Tanto las localidades como la sede principal de Cinex poseen direcciones no validas o privadas en su red LAN, de los bloques 172.20.X.X. Para que los equipos pudieran tener acceso a redes externas, es decir fuera de la LAN, a través de los routers, es preciso realizar un proceso de traducción de estas direcciones IP de origen no validas a direcciones IP validas; este proceso es conocido como NAT (Network Address Translation – Traducción de Dirección de Red). Tiene gran importancia puesto que nos permite dar acceso a Internet a un número mayor de hosts con una única dirección valida. Esto lo logra haciendo cambios de:

- IP de origen: sustituida con la dirección externa valida.
- Puerto de origen: sustituido con un puerto no en uso de la dirección valida de salida, escogido aleatoriamente (por ejemplo, 53136).

Ni la máquina interna, ni el Proveedor de Servicio de Internet se dan cuenta de estos pasos de traducción. Para la máquina interna, el sistema NAT es simplemente una pasarela a Internet. Para el Proveedor de Servicio de Internet, los paquetes parecen venir directamente del sistema NAT; ni siquiera se da cuenta de que existe la estación interna.

En la sede principal se cuenta con un grupo de 6 direcciones validas, de las cuales se asignaron como previamente se describió, una para el router de acceso (Internet Total) y otra para el equipo de seguridad encargado de cerrar los túneles. El resto de direcciones validas o pool de direcciones se utilizó para dar salida a las demás redes, al grupo de host que así lo requieran. En un futuro cercano se dispondrá de un servidor de correos propio por lo que se le asignará una dirección IP valida, tomada de este pool.

Se muestra a continuación un diagrama donde se puede apreciar este proceso:

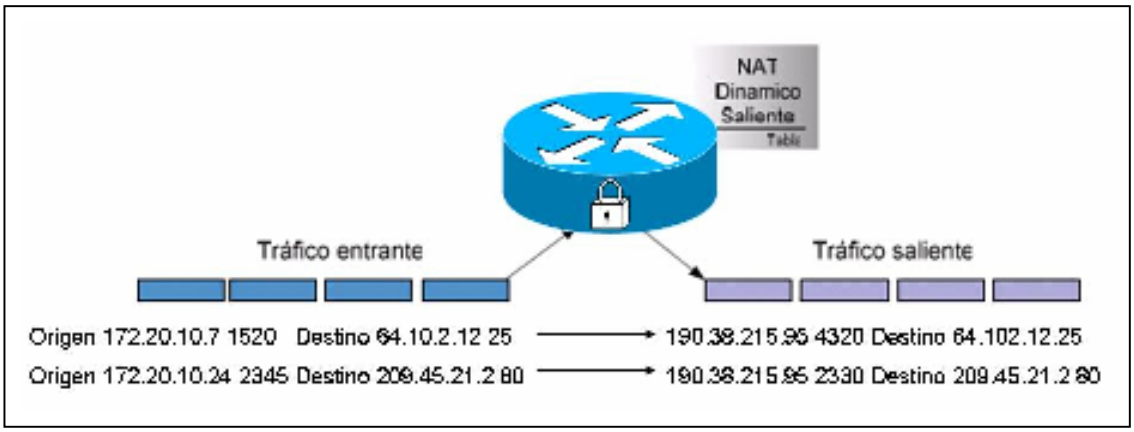

Figura 20. NAT saliente

En el NAT dinámico saliente una dirección IP valida puede ser utilizada por muchas direcciones IP no validas, de allí que con el grupo de direcciones validas, se pueda ofrecer este servicio a muchos equipos que pertenecen a la empresa. Dependiendo del tipo de tráfico, una IP valida podría soportar unas 4000 direcciones no validas, de ahí el término de dinámico. Esta característica se expresa como "overflow" u "overload" en la configuración. También conocido como PAT (Port Address Translation – Traducción de dirección de puerto). NAT es descrito en el RFC 1631.

3.3. Consideraciones de Seguridad

3.3.1 Listas de Acceso

Los routers se sirven de las listas de control de acceso (ACL) para identificar el tráfico.

Esta identificación puede usarse para filtrar el tráfico y conseguir una mejor administración del tráfico global de la red. Las listas de acceso constituyen una eficaz herramienta para el control de la red, ya que añaden la flexibilidad necesaria para filtrar el flujo de paquetes que entra y sale de las diferentes interfaces del router.

Cuando un paquete llega a una interfaz, el router comprueba si el paquete puede ser retransmitido verificando su tabla de enrutamiento. Si no existe ninguna

ruta hasta la dirección de destino, el paquete es descartado. A continuación, el router comprueba si la interfaz de destino esta agrupada en alguna lista de acceso. De no ser así, el paquete puede ser enviado al búfer de salida. Si el paquete de salida está destinado a un puerto, que no ha sido agrupado a ninguna lista de acceso de salida, dicho paquete será enviado directamente al puerto destinado. Si el paquete de salida está destinado a un puerto y ha sido agrupado en una lista de acceso saliente, antes de que el paquete pueda ser enviado al puerto destinado será verificado por una serie de instrucciones de la lista de acceso asociada con dicha interfaz. Dependiendo del resultado de estas pruebas, el paquete será admitido o denegado. [14]

De esta forma el cliente quiere restringir el uso de Internet en las localidades a ciertas páginas de su elección de forma que los empleados no tengan libre acceso a Internet.

Estás listas de accesos pueden ser cambiadas en un momento dado inclusive de forma remota, de manera de tener control sobre la red.

En la sede principal el control de acceso a Internet es regido por un servidor PROXY, de manera que no es necesaria la creación de listas de acceso en el router o en el firewall que denieguen la salida a ciertas direcciones o páginas.

De esta forma además de controlar el acceso a la red, se controla en cierta medida el ancho de banda, evitando que sea ocupado por tráfico innecesario.

3.3.2. VPN

Protocolos de seguridad

A continuación se presenta una tabla comparativa de los aspectos más importante de los protocolos IPsec y SSL:

Tabla 4. Comparación entre los Protocolos SSL Vs. IPSec

Protocolos / Características	SSL (Socket Secure Layer)	IPSec (IP Secure)
Maneja Tecnología PKI	SI	SI
Longitud de Clave	128bits	128bits
Presencia en Modelo (OSI)	Capa 6 (Aplicaciones)	Desde Capa 3
Acceso Subredes con control de Acceso Requerido	NO	SI
Compatibilidad con Árbol de Directorio	NO	LDAP, Kerberos
Implementación Típica	Bancaria	Corporativa Militar Gubernamental
Clientes a Conectarse	No Controlado	Conocidos e Identificados
Instalación en la del Cliente	Automático	Semi Automático

Como se muestra en la tabla anterior IPSec y SSL poseen características similares en el manejo de claves públicas. Sin embargo existen diferencias según la aplicabilidad que éstos tienen en distintos escenario.

El protocolo a utilizar fue el IPsec debido a que es necesaria la autorización y autenticación para el establecimiento de la sesión; además representa un conjunto de mecanismos de seguridad de alta calidad basado en claves criptográficas, proporcionando un canal seguro para los datos a través de la red, ofreciendo para ello mecanismos de autenticación y confidencialidad soportadas en toda la red pública. IPSec opera sobre la capa 3 de red, la capa del protocolo de Internet (IP).

Es un protocolo seguro y sencillo, altamente aplicado y recomendado por Cisco y aplicado por diversas empresas en Venezuela.

Los servicios IPSec son llevados a cabo mediante el uso de dos protocolos de seguridad: Authentication Header (AH) y Encapsulating Security Protocol (ESP), así

como mediante un conjunto de protocolos necesarios para la gestión de claves criptográficas, llamado IKE (Internet Key Exchange).

Se formarán túneles IPSec entre cada nodo o localidad y la LAN de Cinex a través de la nube pública de Internet, que actuará como puente. Cada nodo local sólo utilizará el túnel para el envío de datos estadísticos a los servidores de aplicaciones, ubicados en la principal. El tráfico dirigido hacia Internet, no usará el túnel aunque sí el mismo medio físico. La configuración de túneles se realiza en dos partes: primero se crea el túnel con sus características propias y luego, se determina el tipo de tráfico que lo utilizará.

De forma inversa el túnel será utilizado desde la sede principal, para administraciones remotas de hosts y consulta de datos en el servidor de cada localidad.

3.3.3. Autenticación y encriptación

El tipo de negociación de claves que se contempló en el diseño, es ISAKMP pre-compartida. Debe ser igual en ambos extremos del túnel. Esta es la primera clave que se negocia para autenticar quien se quiere conectar.

Se usó ESP ("Encapsulating Security Protocol") en modo transporte porque se requiere que los datagramas estén autenticados y encriptados. El modo Transporte sólo cifra los datos, dejando intacto el encabezamiento IP, lo que permite ver toda la red como si fuera una misma LAN.

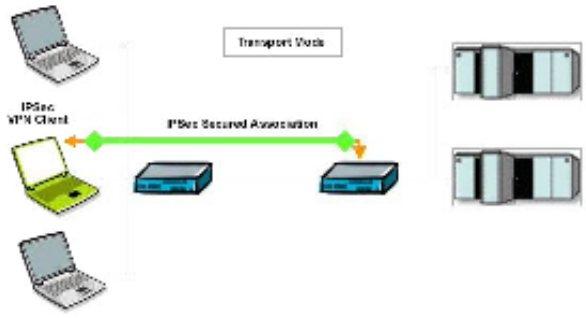

Figura 21. Túnel modo transporte. Fuente:
http://www.thegreenbow.com/es/vpn_faq.html

Para el tipo de cifrado, los equipos Cisco presenta diversas opciones, entre las que tenemos: DES (56-bit), 3DES (168-bit) y AES entre otros. En un principio se seleccionó trabajar con AES por ser mas reciente y bastante seguro, pero necesita de una licencia adicional y a veces origina problemas de compatibilidad entre equipos; se optó por usar 3DES por su mayor robustez frente a DES. El tiempo de cifrado/descifrado no es relevante en este caso por tratarse de datos.

Luego de la creación de los túneles se debe establecer el tipo de tráfico que fluirá a través de ellos. Para esto deben crearse las políticas o normas (IPSec Policy) en el equipo. Estos utilizarán un algoritmo hash SHA, ya que es más seguro que el MD5 a pesar de ser más lento. Se usará para Diffie-Hellman el grupo 2 con 1024 bit, muy recomendado para este tipo de túneles según las practicas de Openlink Sistemas de Redes de Datos C.A.

3.3.4. D.M.Z (Demilitarized Zone)

En redes de datos, una D.M.Z. (zona desmilitarizada) es un equipo o una serie de equipos colocados en una "zona neutral" entre una red privada y la red publica del exterior. Previene a usuarios exteriores del acceso directo a la red de datos de la compañía

Una D.M.Z es un enfoque opcional y más seguro, que conjuntamente con un firewall, actúa efectivamente como una barrera ante ataques externos o internos.

En el caso que un usuario externo penetre la seguridad del host dentro de la D.M.Z., solo podrá afectar dicha área, pero ningún otro tipo de información dentro de la red privada de la compañía se expondría.

Los equipos y servicios que suelen hospedarse en una D.M.Z., son el Web Server y el Mail Server.

Por el momento Cinex no dispone de servidores Web ni de correos propios. Debido a esto no se hará uso de DMZ en el proyecto, pero si planean colocar ambos servidores de un mediano a corto plazo, ya que en un futuro utilizarán esta zona

desmilitarizada para alojarlos. Esto implicaría además un aumento del ancho de banda de Internet por el cual se accedan a dichos servicios.

3.4. Evaluación de equipos de la solución VPN

Openlink Sistemas de Redes de Datos C.A. es una organización Gold Parther de Cisco, por lo que se especializa en la venta de equipos de esta marca reconocida a nivel mundial. Por tanto los equipos que se van a utilizar serán de la casa Cisco.

Por tratarse de una red WAN, se necesitaron Routers, Firewall y un concentrador de VPN. La red LAN no será modificada por el momento y seguirán usando los equipos con los que cuenta Cinex actualmente.

A continuación la descripción de los equipos que conforman la topología implementada en Cinex y el porque de los mismos:

3.4.1. ROUTER 2811

Descripción Básica del Equipo

El router Cisco 2800 está diseñado específicamente para resolver los requisitos de crecimiento de las pequeñas y medianas industrias. Cisco 2800 series proporciona una gran gama de opciones para conectividad combinada con las características fundamentales de disponibilidad y de confiabilidad. Además, el software del IOS de Cisco maneja los protocolos de transporte, de las herramientas de Quality-of-Service (QoS) y de los usos avanzados de la seguridad y de la voz. Con la incorporación de versiones de IOS apropiados es posible configurar características de voz y/o seguridad de acuerdo a las funcionalidades del equipo. Y necesidades de la solución que requiera la empresa

Figura 22. Router Cisco Modular 2811. Fuente:
http://www.cisco.com/en/US/products/ps5881/prod_view_selector.html

Las características básicas del equipo son:

1.- Arquitectura Modular: Es posible seleccionar entre más de 90 módulos, Wan Interface Card (WIC), Voice Interface Card (VIC), Networks Module y AIMs, considerando los requisitos de la solución, con fácil actualización de acuerdo al crecimiento y evolución de la red.

2.- Hardware Acelerador de Seguridad Incluido: Para el manejo de tráfico encriptado, la serie 2800 incluye un acelerador de procesos. Con los módulos y actualizaciones adecuadas es posible el manejo de Servicios de VPN y Enlaces de Seguridad WAN.

3.-Posibilidad de Incrementar la Capacidad de Memoria: El router 2811 trae por defecto una memoria de 64MB de Flash y 256MB de DRAM, con una capacidad máxima de 256MB y 768MB respectivamente.

4.- Puertos FastEthernet integrados: 2 puertos 10/100 RJ45 integrados para conexión Ethernet.

5.- Soporte de Cisco IOS Release 12.3: Soporte de las últimas versiones de IOS para manejo de características de seguridad, calidad de servicio y manejabilidad del ancho de banda.

6.- Posibilidad de Alimentación PoE (Power over Ethernet): Con la realización de las actualizaciones necesarias en la fuente de poder es posible activar Power over Ethernet para la alimentación de ciertos equipos.

7.- Integración opcional de una fuente de poder DC.

8.- Conector integrado para sistema RPS (Redundant Power Suply), para fuente de poder redundante.

Especificaciones Técnicas Básicas:

Tabla 5. Especificaciones del router 2811

ARQUITECTURA	CISCO ROUTER 2811
DRAM	Default: 256MB Máximo: 768MB
Flash	Default: 64MB Máximo: 256MB
Puertos USB	2
Puertos LAN	2Puertos 10/100Mbps
AIM Slot	2
Interface Card Slots	4 slots (WIC, HWIC, VWIC, VIC)
Network Module	1 slots
PVDM Slots	2
VPN Hardware Aceleration	DES, 3DES, AES 128, AES 192, and AES 256
Puerto de Consola |	1
Puerto Auxiliar	1
IOS Mínimo	12.3(8)T
Voltaje de Entrada AC	100-240VAC
Frecuencia	47-63Hz

Para conocer más detalles de las especificaciones del Router 2811, se puede acceder al siguiente enlace:
http://www.cisco.com/en/US/partner/products/ps5854/products_data_sheet0900aecd8016fa68.html

Funcionalidades del equipo Router 2811 para la Solución propuesta:

Es uno de los equipos que conforman el portafolio de Cisco para servicios integrados de Voz y Seguridad. Este equipo es el equipo a colocarse en la sede principal. En este caso se seleccionó una configuración con servicio integrado de seguridad para el levantamiento de las VPN en la sede principal y con servicio de voz pensando en la incorporación a futuro de una solución de telefonía IP.

Las funcionalidades del equipo en el escenario propuesto son las siguientes de acuerdo a la configuración:

1.- 1 Interfaz WIC: se incluye en la configuración del equipo una tarjeta de conexión destinada para la conexión de salida al enlace de Internet dedicado, Frame Relay.

3.4.2. ASA 5510:

Descripción Básica del Equipo:

Definir políticas de seguridad en una organización contemplando las necesidades, e integrar equipos que permitan ejecutar esas políticas dentro de la red es vital para el buen funcionamiento de la misma. El Cisco ASA500 Series "Adaptive Security Appliance" es una plataforma modular que integra servicios de VPN, IPS (Intrusion Prevention System) y Firewall. El Cisco ASA combina un sistema enfocado en servicios para suplir las necesidades específicas de seguridad dentro de la red de una empresa, como Firewall. Al mismo tiempo, las 5500 series de Cisco ASA permiten a la estandardización en una sola plataforma, para reducir el costo operacional total de seguridad.

Las características fundamentales de esta plataforma son:

- Ofrece servicio SSL (Secure Socket Layer) y servicios de VPN de acuerdo a los firewall existentes en el mercado.

- Integración con soluciones Trend Micro de Antivirus, anti-spyware, anti-spam, filtrado de paquetes y filtrado de contenido, entre otros.
- Ofrece Servicios Avanzados para la detección de intrusos, contemplando ataques a nivel del sistema, ataques de bugs (bichos; errores de programación), ataques de spyware y ataques de mensajería instantánea entre otros.
- Elemento integral de fácil manejabilidad.

El modelo ASA seleccionado es el ASA 5510 debido a que es el que permite levantar hasta 250 túneles, ya que su modelo más sencillo solo permite 25 y se van a interconectar 27 localidades por el momento. Esto permitirá su futuro crecimiento sin ningún problema respecto al número de túneles.

Especificaciones Técnicas del ASA 5510:

Tabla 6. Características del ASA 5510

ASA 5510	Características
Throughput de Firewall Máximo (Mbps)	300
Throughput 3DES/AES/ VPN Máximo (Mbps)	170
Máximo site-to-site de VPN Peers	250
Máximo Web VPN Peers	250
Conexiones Máxima	50000
Máximas conexiones por segundo	6000
Memoria (MB)	256
Flash (MB)	64
Puertos Integrados	3 10/100, 1 10/100
Máxima cantidad de VLAN	10
SSM Expation Slot	Si
Acelerador VPN	Si

Figura 23. Cisco ASA 5510. Fuente: http://www.cisco.com/cdc_content_elements/images/products/security_vpn/asa5500/asa5510.jpg

Para información más detallada de las especificaciones técnicas del ASA 5510, visitar el enlace: http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6032/ps6094/ps6120/product_data_sheet0900aecd802930c5.html

Funcionalidad del ASA 5510 en la solución planteada:

Dentro de la solución propuesta, este equipo está integrado dentro de la Red LAN y tiene como finalidad ser el punto de concentración para cerrar todos los túneles de VPN levantados desde las sedes remotas, proporcionando así la seguridad necesaria. Adicionalmente, este equipo puede ser configurado para la detección de ataques, y además operar como firewall para protección de la red de ataques externos, filtrado de contenidos y establecimiento de las políticas de seguridad para la restricción de acceso de algunos usuarios

3.4.3. El router Cisco 1841

Posee características similares al 2800 pero a una menor escala.

Las características básicas del equipo son:

1.- Arquitectura Modular: Es posible seleccionar entre más de 30 módulos, Wan Interface Card (WIC), múltiples tarjetas troncales (voice/WICs [VWICs] solo para

datos) Networks Module y AIMs, considerando los requisitos de la solución, con fácil actualización de acuerdo al crecimiento y evolución de la red.

2.- Hardware Acelerador de Seguridad: Para el manejo de tráfico encriptado. Con los módulos y actualizaciones adecuadas es posible el manejo de Servicios de VPN y Enlaces de Seguridad WAN.

3.-Posibilidad de Incrementar la Capacidad de Memoria: El router 2811 trae por defecto una memoria de 32MB de Flash y 128MB de SDRAM (synchronous dynamic RAM).

4.- Puertos FastEthernet integrados: 2 puertos 10/100 RJ45 integrados para conexión Ethernet.

5.- Soporte de Cisco IOS Release 12.3: Soporte de las últimas versiones de IOS para manejo de características de seguridad, calidad de servicio y manejabilidad del ancho de banda.

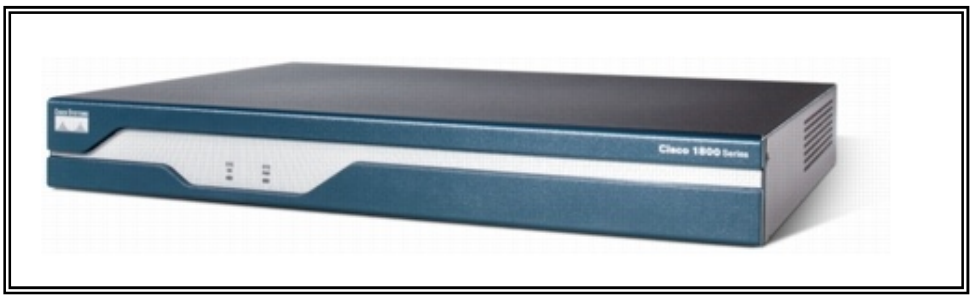

Figura 24. Router Cisco 1841. Fuente:
http://www.cisco.com/en/US/products/ps5875/prod_view_selector.html

Especificaciones Técnicas Básicas:

Tabla 7. Caracterìsticas del router 1841

ARQUITECTURA	CISCO ROUTER 1841
DRAM	Default: 128MB Máximo: 384MB
Flash	Default: 32MB Máximo: 128MB
Puertos USB	1
Puertos LAN	2Puertos 10/100Mbps
AIM Slot	1 (Interna)
Interface Card Slots	2 slots
VPN Hardware & Software encryption	DES, 3DES, AES 128, AES 192, and AES 256
Puerto de Consola |	1
Puerto Auxiliar	1
IOS Mínimo	12.3(8)T
Voltaje de Entrada AC	100-240VAC
Redundancia de Poder	No
Frecuencia	50-60Hz

Para información más detallada del equipo visitar: http://www.cisco.com/en/US/prod/collateral/routers/ps5853/product_data_sheet0900aecd8016a59b.html

Funcionalidad del equipo Router 1841 en la solución propuesta.

Este es el equipo que se instalará en cada localidad. En este caso se seleccionó una configuración con servicio integrado de seguridad para el levantamiento de las VPN hacia la sede principal.

Las funcionalidades del equipo en el escenario propuesto son las siguientes de acuerdo a la configuración:

1.- Interfaz ADSL: se incluye en la configuración del equipo una tarjeta de conexión ADSL destinada para la conexión de salida al enlace de Internet, ABA de CANTV.

2. - Proporcionar la seguridad necesaria para realizar los túneles

3.5. Cisco IOS Software

EL software IOS de Cisco o **Internetwork Operating System (**Sistema Operativo de Interconexión de Redes) está desarrollado para adaptarse mejor a las necesidades que tienen los clientes en sus redes. De esta forma disponemos de diversos tipos del mismo, destinado a funciones básicas, de telefonía, seguridad, entre muchos otros. Debido a que la finalidad en este proyecto es enviar datos de manera segura por la red pública como es Internet, se seleccionó un Software de "Seguridad Avanzada" (ADVANCED SECURITY) para los routers.

Este fue desarrollado para prestar una infraestructura segura de redes. Como un componente fundamental de la Red de Auto defensa de Cisco, el Software Cisco IOS ofrece un sofisticado conjunto de capacidades de seguridad, con enfoque de seguridad de varios niveles en toda su infraestructura de la red. La tecnología de seguridad del Cisco IOS ayuda a defender procesos de negocio críticos contra los ataques y alteraciones, la protección de la privacidad, y apoyar la formulación de políticas y el cumplimiento de las normas de control.

El modelo de la imagen de IOS que se instaló en los routers y el ASA son los siguientes:

Tabla 8. Software utilizado en los equipos.

Imagen IOS	Equipo	Versión	Cisco 1841 (archivo)
ADVANCED SECURITY	Routers	12.4 (3g)	c1841-advsecurityk9-mz.124-3g.bin
Cisco Adaptive Security Appliance Software Version	ASA	7.2(2)	asa722-k8.bin

3.6. Administración remota de los equipos

La misma se realizará a través del protocolo SSH2 (Secure Shell), ya que es más seguro que Telnet, dado que este encripta la sesión de conexión, haciendo imposible que alguien pueda obtener contraseñas no encriptadas, como es el caso de Telnet donde los datos viajan como texto plano.

Se usará para su encriptación AES de 256 bit; de esta forma las claves no viajarán de forma plana por la red pública donde podrían ser capturadas por cualquiera.

Adicionalmente se planteó utilizar el ASDM (Adaptative Security Device Manager), que es una aplicación de uso sencillo, a través de ventanas Web, que permiten configuraciones rápidas, editar las existentes; realizar diagnósticos poderosos como capturas de paquetes, información de eventos, trazas de paquetes; monitoreo en tiempo real con informaciones gráficas, contenidos de seguridad, permitiendo tabular métricas para activar respuestas rápidas a incidentes de seguridad. Con esta aplicación se logra la administración y monitoreo de la red central, tanto en la parte de seguridad, tráfico y congestión del enlace y estado de los túneles VPN.

CAPITULO IV INSTALACION DE LA RED WAN

4.1 Componentes de la red WAN

Para la implementación de la red WAN, se adquirió un enlace Frame Relay (Internet Total) de 1024 Kbps con un EIR (Tasa de información excesiva) de 128 Kbps a CANTV. Para esto se conectó el equipo terminal DCE al puerto serial V35 del router usando el cable apropiado. Een las localidades, una gran mayoría ya disponía de enlaces ABA de CANTV (ADSL), y a los pocos que no, se les adquirieron; a excepción de 2 localidades donde el servicio es provisto por el Centro Comercial. La mayoría de los enlaces ADSL son de 512 Kbps y algunos pocos que se encontraron en 384 Kbps se pretenden subir a 512 Kbps.

Al momento de la implementación, se tuvo que tomar en consideración la existencia de la actual Red, de forma de que continuara operativa mientras se hacen los cambios.

Para esto, la red LAN en la principal, debía seguir trabajando de forma transparente con todas sus localidades, ya fuera con las localidades migradas como las no migradas.

En vista de la disponibilidad de gran numero de routers, ya que las primeras a instalar son las de Sur Americana de Espectáculos, la única que posee los túneles y que se deben migrar; y las de Blancica y Venefilms son túneles nuevos que se van a integrar a la red de Cinex; como solución temporal se dispuso un router en la LAN principal cuyo único propósito será enrutar las peticiones según se soliciten a los túneles de Daycohost o a los nuevos túneles, en vista de que el equipo de Daycohost no se puede administrar.

Para ello se dispuso de la dirección 172.20.4.5 para asignarla al router de enrutamiento, que además será la dirección de puerta de enlace para la LAN. De esta forma, por medio de rutas estáticas, las comunicaciones con las localidades que son las 172.20.XX.XX se destinaron que salgan por la 172.20.4.1 para los enlaces que no se hayan migrado y la 172.20.4.4 a los enlaces que ya se hayan migrado.

Una vez concluida la migración de las localidades de Daycohost, se podrá retirar este equipo y ser utilizado en alguna nueva localidad que se vaya a instalar.

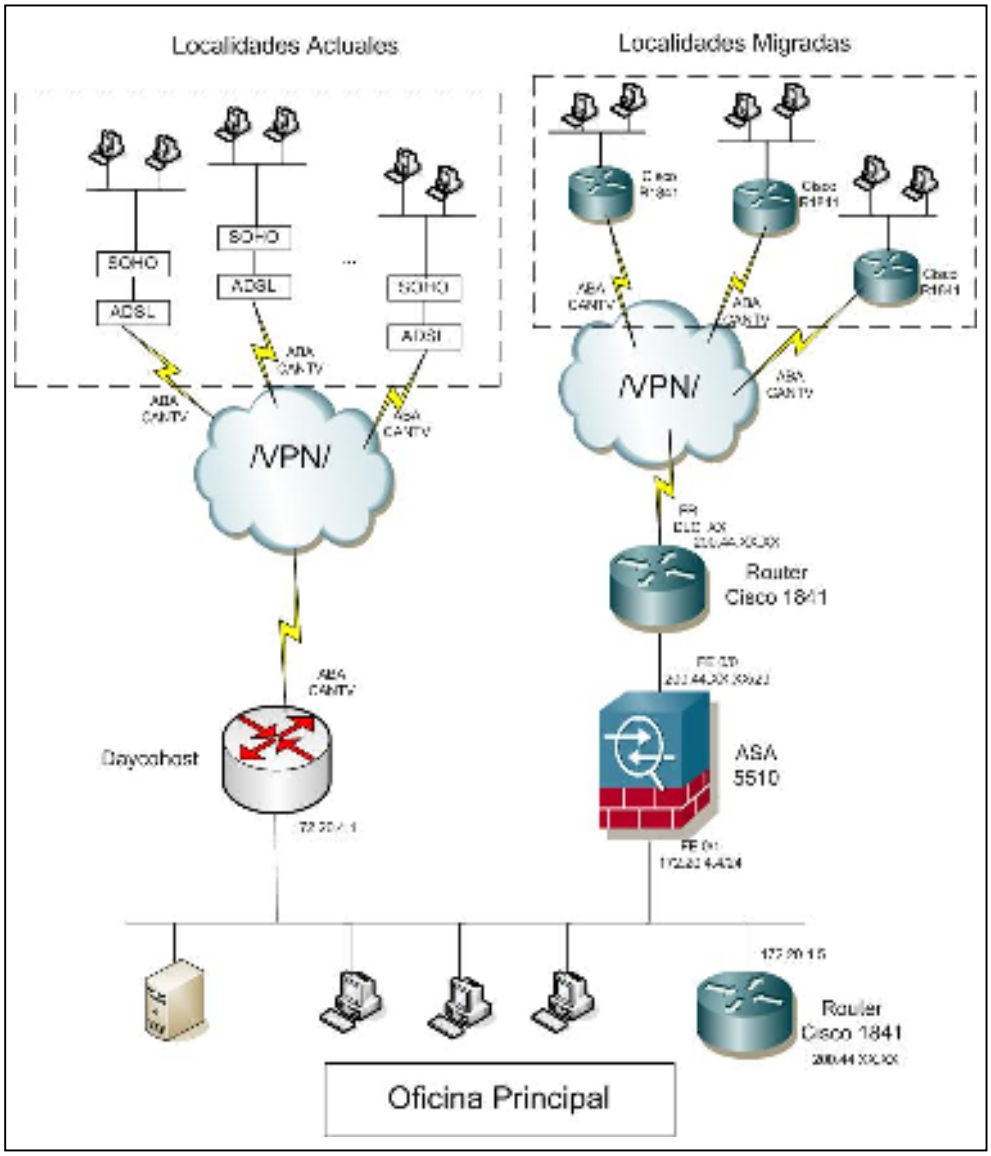

Figura 25. Diagrama actual de la red WAN de Cinex.

En las localidades se retiraran los MODEM ADSL ya que el router Cisco cuenta con la tarjeta para realizar esta función, por lo que se conectan directamente al par trenzado telefónico por RJ-11. El router Cisco se conecta al Switch del que se

dispone en cada localidad, a quien están conectados los diversos equipos con los que cuenta cada sitio.

Las conexiones tanto de router a switch y de router a ASA se realizan con cable directo.

4.2 Configuración de los equipos (scripts)

Las características generales del sistema han sido explicadas en el capítulo III, donde se habló del tipo de autenticación, encapsulamiento, direccionamiento IP y demás características que tienen las instalaciones.

A continuación se presentan las configuraciones detalladas de los routers pertenecientes a la sede principal y a la localidad del Centro Lido. En cuanto a las configuraciones de los sitios remotos restantes, se agregan en los anexos ya que solo difieren en la asignación de las direcciones IP y las listas de acceso.

4.2.1 Configuración del router frontera en la sede principal.

```
version 12.4
service timestamps debug uptime
service timestamps log datetime msec localtime show-timezone
service password-encryption
!
hostname Cinex_Internet
!
enable secret xxxxxxx
!
********* Activa SSH
aaa new-model
username xxxxx privilege xx password xxxxx
crypto key generate rsa
```

```
ip ssh time-out 120
ip ssh version 2
!
line vty 0 4
transport input ssh
transport output telnet ssh
!
!
********* Configuración de Interfaces **********
interface FastEthernet0/0
 ip address 200.44.XX.XX 255.255.255.248
 duplex auto
 speed auto
!
!
interface Serial0/1/0
 no ip address
 encapsulation frame-relay IETF
 frame-relay lmi-type ansi
!
interface Serial0/1/0.681 point-to-point
 description Internet Total Circuito xxxxxxx
 ip address 200.44.XX.XX 255.255.255.252
 frame-relay interface-dlci XXX
!
********** Ruta de salida o próximo salto.
ip classless
ip route 0.0.0.0 0.0.0.0 200.44.XX.XX
!
```

```
!
********** Configuración de password por consola
line con 0
 password XXXXXXXXXXXX
 logging synchronous
 login
line aux 0        **** No se configura línea auxiliar
End
```

Los enlaces Frame Relay cuentan con un protocolo de información local LMI (Link Management Interface). Los tipos de LMI que se pueden configurar son: Cisco, ANSI y Q933a, es importante resaltar que todos son incompatibles entre ellos. El protocolo usado fue el que sigue el estándar de ANSI (*frame-relay lmi-type ANSI*). Esto hace posible que un DTE local pueda enviar tramas a más de un DTE remoto así como permite verificar el estado de los diversos DCE que conforman la red.

La ruta de salida del router es expresada mediante el comando "ip route 0.0.0.0 0.0.0.0 200.44.XX.XX", donde al no conocer una dirección IP, cualquiera que esta sea, el dispositivo enrutará hacia la dirección 200.44.XX.XX, que según el esquema de direccionamiento IP, es la asignada por CANTV como próximo salto.

4.2.2 Configuración de router Gateway temporal en la principal

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname Cinex_Gateway
!
!
```

```
****** Password enable
enable secret 5 XXXXXXX
!
****** Activación SSH
username xxxxx privilege xx password xxxxxx
aaa new-model

crypto key generate rsa

ip ssh time-out 120
ip ssh version 2


line vty 0 4
transport input ssh
transport output telnet ssh
!
!
********** Configuración de Interfaces
interface FastEthernet0/0
 description CONEXION LAN - GATEWAY TEMPORAL
 ip address 172.20.4.5 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
```

```
!
interface ATM0/0/0
 no ip address
 shutdown
 no atm ilmi-keepalive
 dsl operating-mode auto
!
******** Configuración de rutas estáticas
ip classless
ip route 0.0.0.0 0.0.0.0 172.20.4.4
ip route 10.0.3.0 255.255.255.0 172.20.4.4
ip route 172.20.0.0 255.255.255.224 172.20.4.4
ip route 172.20.0.32 255.255.255.240 172.20.4.4
ip route 172.20.0.96 255.255.255.224 172.20.4.4
ip route 172.20.0.128 255.255.255.224 172.20.4.4
ip route 172.20.0.160 255.255.255.224 172.20.4.4
ip route 172.20.0.192 255.255.255.224 172.20.4.4
ip route 172.20.2.0 255.255.255.224 172.20.4.1
ip route 172.20.2.0 255.255.255.224 172.20.4.4
ip route 172.20.2.192 255.255.255.224 172.20.4.4
ip route 172.20.3.32 255.255.255.224 172.20.4.1
ip route 172.20.3.64 255.255.255.224 172.20.4.1
ip route 172.20.5.32 255.255.255.224 172.20.4.1
ip route 172.20.5.64 255.255.255.224 172.20.4.4
ip route 172.20.5.96 255.255.255.224 172.20.4.4
ip route 172.20.6.0 255.255.255.224 172.20.4.1
ip route 172.20.10.0 255.255.255.0 172.20.4.4
ip route 172.20.11.0 255.255.255.0 172.20.4.4
ip route 172.20.12.0 255.255.255.0 172.20.4.4
ip route 172.20.13.0 255.255.255.0 172.20.4.4
```

```
ip route 172.20.14.0 255.255.255.0 172.20.4.4
ip route 172.20.15.0 255.255.255.0 172.20.4.4
ip route 172.20.16.0 255.255.255.0 172.20.4.4
ip route 172.20.17.0 255.255.255.0 172.20.4.4
ip route 172.20.18.0 255.255.255.0 172.20.4.4
ip route 172.20.19.0 255.255.255.0 172.20.4.4
ip route 172.20.20.0 255.255.255.0 172.20.4.4
ip route 172.20.21.0 255.255.255.0 172.20.4.4
ip route 172.20.22.0 255.255.255.0 172.20.4.4
ip route 172.20.30.0 255.255.255.0 172.20.4.4
ip route 172.20.31.0 255.255.255.0 172.20.4.4
ip route 172.20.32.0 255.255.255.0 172.20.4.4
ip route 172.20.33.0 255.255.255.0 172.20.4.4
ip route 172.20.34.0 255.255.255.0 172.20.4.4
ip route 172.20.35.0 255.255.255.0 172.20.4.4
ip route 172.20.36.0 255.255.255.0 172.20.4.4
ip route 172.20.37.0 255.255.255.0 172.20.4.4
ip route 172.20.38.0 255.255.255.0 172.20.4.4
!
!
********* Configuración de línea de consola.
line con 0
 password XXXXXXXX
 login

line aux 0        ****la línea auxiliar no se configuró
!
End
```

Como se observa, esta configuración contiene rutas estáticas hacia las localidades migradas y las que no han sido migradas que se van cambiando a medida que se realizan las migraciones.

Se debe recordar que al terminar las migraciones este router será eliminado de la sede principal.

4.2.3 Configuración del router de la localidad del Centro Lido

```
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname Cinex_Lido
!
******** Password enable
enable secret XXXXXXX
!
****** Activación SSH
username xxxxx privilege xx password xxxxxx
aaa new-model
 !
crypto key generate rsa
 !
ip ssh time-out 120
ip ssh version 2
 !
 !
line vty 0 4
transport input ssh
transport output telnet ssh
```

********* Configuración del túnel VPN
crypto isakmp policy 1
 encr 3des
 hash md5
 authentication pre-share
 group 2
crypto isakmp key vpncinex address 200.44.189.66
!
crypto ipsec transform-set asa-set esp-3des esp-md5-hmac
!
crypto map asa 10 ipsec-isakmp
 set peer 200.44.189.66
 set transform-set asa-set
 match address 115
!
bridge irb
!
******* Configuración de Interfaces
interface ATM0/0/0
 no ip address
 load-interval 30
 no atm ilmi-keepalive
 pvc 0/33
  encapsulation aal5snap
 dsl operating-mode auto
 bridge-group 1
!
interface FastEthernet0/0
 ip address 172.20.11.1 255.255.255.0 Secondary

```
 ip address 172.20.0.1 255.255.255.224
 ip nat inside
 ip virtual-reassembly
!
interface BVI1
 ip address dhcp
 ip nat outside
 ip virtual-reassembly
 crypto map asa          ***** llamado al mapa críptico para la VPN
!
********* Ruta de salida por defecto al próximo salto
ip classless
ip route 0.0.0.0 0.0.0.0 BVI1
!
no ip http server
no ip http secure-server

********* Configuración del NAT y la lista de acceso asociada al mismo y al túnel
VPN que no hace NAT ***********

ip nat inside source route-map NONAT interface BVI1 overload
!
access-list 110 deny   ip 172.20.0.0 0.0.0.31 172.20.4.0 0.0.0.255
access-list 110 deny   ip 172.20.11.0 0.0.0.255 172.20.4.0 0.0.0.255
access-list 110 permit ip 172.20.0.0 0.0.0.31 any
access-list 110 permit ip 172.20.11.0 0.0.0.255 any
access-list 115 permit ip 172.20.0.0 0.0.0.31 172.20.4.0 0.0.0.255
access-list 115 permit ip 172.20.11.0 0.0.0.255 172.20.4.0 0.0.0.255
!
route-map NONAT permit 10
```

```
 match ip address 110
!
!
bridge 1 protocol ieee
bridge 1 route ip
!
**********Configuración de línea de Consola
line con 0
 password XXXXXXXXX
 login
!
end
```

En vista de que las localidades toman su direccionamiento IP público por DHCP, no se pude conocer la ruta de salida o próximo salto, por lo que en este caso se especifica la interfaz por donde va a salir el tráfico (BVI1, Bridge-Group Virtual Interface).

En las listas de acceso se puede observar como se deniega el tráfico que va a la sede principal 172.20.4.0 para que no se le aplique NAT. Esto se ve en la lista de acceso 110, donde da salida a todo lo demás que no es dirigido a la principal. En la lista de acceso 115 se especifica el tráfico que va a ser enrutado por el túnel VPN, el cual comprende toda la subred de la localidad. Esta lista de acceso es llamada en el crypto map del túnel.

4.2.4 Configuración del ASA ubicado en la principal

```
ASA Version 7.2(2)
hostname CinexASA
domain-name cinex.com.ve
```

```
enable password XXXXXXXX encrypted
names
dns-guard
!
interface Ethernet0/0
 nameif outside
 security-level 0
 ip address 200.44.XX.XX 255.255.255.248
!
interface Ethernet0/1
 nameif inside
 security-level 100
 ip address 172.20.4.4 255.255.255.0
!
interface Ethernet0/2
 nameif Daycohost
 security-level 0
 no ip address
!
interface Ethernet0/3
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 shutdown
 no nameif
 no security-level
 no ip address
```

```
!
passwd XXXXXXXX encrypted
boot system disk0:/asa722-k8.bin
ftp mode passive
clock timezone Caracas -4
dns server-group DefaultDNS
 domain-name cinex.com.ve
same-security-traffic permit intra-interface
********** Listas de acceso
object-group network Outside_Networks
 description Redes Localidades Remotas - Cinex
 network-object 172.20.10.0 255.255.255.0
 network-object 172.20.11.0 255.255.255.0
 network-object 172.20.12.0 255.255.255.0
 network-object 172.20.13.0 255.255.255.0
 network-object 172.20.14.0 255.255.255.0
 network-object 172.20.15.0 255.255.255.0
 network-object 172.20.16.0 255.255.255.0
 network-object 172.20.17.0 255.255.255.0
 network-object 172.20.18.0 255.255.255.0
 network-object 172.20.19.0 255.255.255.0
 network-object 172.20.20.0 255.255.255.0
 network-object 172.20.21.0 255.255.255.0
 network-object 172.20.22.0 255.255.255.0
 network-object 172.20.0.32 255.255.255.224
 network-object 172.20.0.0 255.255.255.224
 network-object 172.20.0.96 255.255.255.224
 network-object 172.20.0.128 255.255.255.224
 network-object 172.20.0.160 255.255.255.224
 network-object 172.20.0.192 255.255.255.224
```

network-object 172.20.2.0 255.255.255.224
network-object 172.20.2.192 255.255.255.224
network-object 172.20.5.32 255.255.255.224
network-object 172.20.5.64 255.255.255.224
network-object 172.20.5.96 255.255.255.224
network-object 172.20.6.0 255.255.255.224
network-object 172.20.3.64 255.255.255.224
network-object 172.20.3.32 255.255.255.224
access-list IPSEC extended permit ip 172.20.4.0 255.255.255.0 object-group Outside_Networks
access-list NONAT extended permit ip 172.20.4.0 255.255.255.0 object-group Outside_Networks
access-list ACL_IN extended permit ip any any
access-list ACL_IN extended permit icmp any any
access-list ACL_OUT extended permit icmp any any
access-list ACL_OUT extended permit tcp any host 200.44.189.67 eq telnet

********** Respuestas de ECO (Ping)
icmp unreachable rate-limit 1 burst-size 1
icmp permit any inside

********** Programa ASDM e información de capturas de eventos
logging enable
logging asdm informational
asdm image disk0:/asdm-522.bin
no asdm history enable

arp timeout 14400
******* Configuración de NAT
nat-control

```
global (outside) 10 interface
nat (inside) 0 access-list NONAT
nat (inside) 10 172.20.4.0 255.255.255.0
static (inside,outside) 200.44.189.67 172.20.4.5 netmask 255.255.255.255
access-group ACL_OUT in interface outside
access-group ACL_IN in interface inside
********** Ruta de salida
route outside 0.0.0.0 0.0.0.0 200.44.189.65 1
timeout xlate 3:00:00
********** Password Enable y autenticación
username XXXXXX password XXXXXXXXXX encrypted
aaa authentication ssh console LOCAL
aaa local authentication attempts max-fail 16
http server enable
http 0.0.0.0 0.0.0.0 inside
http 0.0.0.0 0.0.0.0 outside

********** Configuración del Servidor de VPN
crypto ipsec transform-set myset esp-3des esp-md5-hmac
crypto dynamic-map cisco 1 set transform-set myset
crypto map dyn-map 10 ipsec-isakmp dynamic cisco
crypto map dyn-map interface outside
crypto isakmp enable outside
crypto isakmp policy 10
 authentication pre-share
 encryption 3des
 hash md5
 group 2
 lifetime 259200
tunnel-group DefaultL2LGroup ipsec-attributes
```

```
 pre-shared-key *

******* SSH y consola
ssh 0.0.0.0 0.0.0.0 outside
ssh 0.0.0.0 0.0.0.0 inside
ssh timeout 5
console timeout 0
!
****** Lista de inspección de protocolos
class-map inspection_default
 match default-inspection-traffic
!
policy-map type inspect dns migrated_dns_map_1
 parameters
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns migrated_dns_map_1
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
```

```
  inspect xdmcp
  inspect icmp
  inspect http
!
service-policy global_policy global
```

El ASA es el concentrador de los túneles VPN, donde se configuran las políticas del mismo para que las localidades se conecten a él. Además, es el encargado de hacer la traducción NAT en la principal, si va a Internet, o no hacer NAT (NAT 0) al tráfico que va por el túnel. El tráfico es decretado por listas de accesos que son agrupadas en "object group". El ASA también se encarga de inspeccionar el tráfico en busca de paquetes maliciosos o de respuestas ajenas a peticiones.

4.3 Instalación de prueba piloto

Para la prueba piloto de la VPN, se seleccionó la localidad del Centro Lido, debido a que es un cine pequeño y entre los de menor venta de boletos. El día para la instalación de la prueba piloto fue un martes en la mañana. Se configuraron los equipos del lado de la principal, y se colocó una maquina con el default gateway apuntando directo al ASA. Del lado de la localidad se eliminó el MODEM ABA de CANTV y el equipo SOHO Watchguard. Instalado el router Cisco y levantado el túnel se realizaron las pruebas desde la sede principal, cargando datos y probando escritorio remoto a diversas maquinas de la localidad.

Por ese día, si se quería tener la información de esa localidad, se debió cambiar el default gateway en host a conectarse con la localidad a 172.20.4.4, para que de esta forma saliera por el túnel VPN.

Al día siguiente se implementó el router gateway en la sede principal y se tuvo que cambiar el default gateway de todas las maquinas a 172.20.4.5 para que este a través de rutas estáticas enrutara según sea el caso.

Esta prueba se dejó por una semana, donde se notó que los túneles VPN tendían a caerse. Esto debido a que los mismos se cerraban por falta de tráfico y en vista de que el túnel se levanta desde la localidad o sitio remoto, hacia la principal; al momento que desde la principal se deseaba consultar o administrar un host de la localidad, no se podía levantar el túnel y el mismo permanecía caído hasta que se generaba un tráfico desde la localidad por el túnel VPN.

Esto fue un inconveniente debido a que esa situación se presentaba constantemente, y antes de continuar con las demás localidades debía ser resuelto.

En vista de que el problema se originaba debido a la falta de tráfico de la localidad hacia la sede principal, lo que ocasionaba que el túnel se cayera, se optó por generar un ping recurrente desde la localidad hacia la dirección privada del ASA. A pesar de que el ASA no responde a esta solicitud, se origina tráfico del lado de la localidad, que es negociado por el túnel. Para esto se empleó el comando "IP SLA Monitor" (SLA: Service Level Agreement) que es un acuerdo formalmente negociado entre dos partes, con una frecuencia de 300 segundos que equivalen a 5 minutos, con el origen del tráfico desde la dirección LAN del router.

4.4 Instalación de demás localidades

Una vez solucionado el inconveniente y que estuvieron convencidos de la funcionalidad del túnel, se planificaron las demás instalaciones.

Comenzando con las localizadas en Caracas y posteriormente con las del interior del país de Sur Americana de Espectáculos.

La segunda localidad en instalar fue el almacén de Cinex, ubicada en la zona industrial de Palo Verde. Este sitio no contaba con UPS, por lo que se recomendó adquirirlo.

Luego se pre-configuraron los routers de forma que el día de la instalación ya se tuvieran preparados y de esta forma fuera más rápido.

Se continuaron con las instalaciones de: el Recreo, San Ignacio y Sambil en un mismo día; Santa Fe, Concresa, el Hatillo y la Lagunita al día siguiente, con el inconveniente en el Hatillo de que el acceso a Internet es prestado por el centro

comercial y el mismo posee Firewall, además que la dirección suministrada es una dirección privada y no una pública, por lo que no se podía cerrar el túnel debido a un NAT del centro comercial y su Firewall.

Existían 2 opciones para solucionar este problema, solicitar una dirección pública al centro comercial, el cual lo podía proveer sin firewall, o solicitar la instalación a CANTV de una línea ADSL. La segunda opción fue la escogida por la gente de Cinex, apoyándose en que el servicio a Internet ofrecido por el centro comercial era muy lento. Por esto esta localidad está aun a espera de la instalación de la línea ADSL nueva. La comunicación a este sitio se mantiene a través del enlace suministrado por Daycohost.

La Lagunita no poseía enlace con la principal.

A continuación se instalaron la localidad de Buenaventura en Guatire y Victoria Plaza en la Av. Victoria, cada una en un día. Con esto se completaban las instalaciones de la Gran Caracas.

Para las demás instalaciones se enviaron los routers por correo, previamente configurados. Las instalaciones fueron realizadas por personal que Openlink tiene en el interior con asistencia telefónica de ser necesaria. En estas instalaciones se encontró que en su mayoría contaban con el Firewall que CANTV dispone para sus líneas ADSL, por lo que hubo que llamar a 0-800-EMPRESA de CANTV y solicitar su desactivación debido a que bloqueaban varios puertos incluyendo el puerto 500 que es por donde se levanta la VPN.

Las localidades del interior del país de Sur Americana de Espectáculos son: Lagomall (C.C. Lagomall Nivel 1. Urbanización Virginia, Av. 2, El Milagro, Maracaibo Estado Zulia), Babilón (Av. Libertador, Calle 19 y 22 C.C. Babilón, Barquisimeto Estado Lara) y Metrópolis (Av. Florencio Jiménez con Av. La Salle, Municipio Irribaren, Barquisimeto Estado Lara).

La Localidad de Lagomall y Babilón se instalaron sin contratiempo con asistencia de mi parte para levantar el túnel y crear la ruta en la principal en el router temporal. La localidad de Metrópolis presentó el inconveniente similar al del Hatillo: el servicio es prestado por el centro comercial y con direcciones privadas que

presentan NAT al momento de salir, por lo que el túnel no se logra cerrar. En este caso también se decidió hacer la solicitud de una línea nueva ADSL a CANTV y por la cual hasta la fecha de esta redacción aun no está lista.

En cuanto se tenga la misma se realizará la instalación y se completarán todas las localidades de Sur Americana de Espectáculos, pudiendo de esta manera retirar por completo el servicio de Daycohost y también eliminar el router temporal en la principal.

Para la desincorporación de este router se planificará un día en la tarde después de las 5:30 p.m. ya que es la hora en la que la gente de Cinex en la sede principal deja de trabajar. Bastará con eliminar el router y cambiar la dirección que posee el ASA a la 172.20.4.5, de esta forma todos los equipos apuntarán directamente a él ya que es la puerta de enlace que tienen en este momento.

En vista de que las instalaciones de las líneas nuevas por parte de CANTV se van a demorar, se comenzaron las instalaciones de las demás localidades, nueve por parte de Venefilms, todas en el interior del país y 3 por Blancica en Caracas.

Se comenzó con las localidades de Venefilms. Todas estas poseían conexión a Internet por ADSL de CANTV. Solo disponían de servicio a Internet con direccionamiento estático en los equipos y usaron el mismo direccionamiento en todas las localidades, por lo que hubo que cambiar todas las direcciones en las maquinas de cada sitio.

Estas instalaciones se están realizando y deberían haber sido culminadas para el mes de Febrero de 2008. De igual forma se pre-configuraron los equipos y se enviaron a cada localidad. Al comprobar que el mismo se encontraba en el sitio, se envió a una persona para su instalación y cambio de las direcciones IP de los equipos de la localidad.

De estas nueve localidades se han instalado Monagas Plaza en Maturín (Av. Alirio Ugarte Pelayo, Centro Comercial Monagas Plaza Maturín Estado Monagas), Marina Plaza en Cumana (Centro Comercial Marina Plaza, Av. Perimetral La Marina Cumanagoto. Cumaná Estado Sucre), Plaza Mayor en Lecherías (Centro Comercial Plaza Mayor, Galería Caribana Lecherías, Estado Anzoátegui), Doral Plaza en

Maracaibo (Centro Comercial Doral Plaza, segundo Nivel, Av. Fuerzas Armadas, Maracaibo Estado Zulia), Galerías Maracaibo (Centro Comercial Galerías Mall, Segundo Nivel Av. La Limpia, Antiguo Hipódromo, Maracaibo Estado Zulia), Valera en Trujillo (Avenida 6 Centro Comercial Plaza, Nivel Feria Estado Trujillo) y Virtudes en Punto Fijo (Centro Comercial Las Virtudes, P.B. Avenida 6, Comunidad Cardón, Punto Fijo Estado Falcón).

Quedan pendientes Alto Prado en Mérida (Centro Comercial Alto Prado, Av. Los Próceres, Mérida Estado Mérida) y Pirineos en San Cristóbal (Carretera 20, barrio Obrero, San Cristóbal Estado Táchira).

Las 3 localidades de Blancica que son El Tolón en el C.C. el Tolón en las Mercedes, Plaza Las Américas en el Cafetal y Centro Plaza en los Palos Grandes, todas en Caracas ya cuentan con una conexión por VPN a la sede Central de Blancica. Ellos usan router Linksys en ambos lados de la conexión. Aprovechando la capacidad de los router Cisco, se mantendrán la VPN con la sede Central de Blancica que cierra en un router Linksys y la VPN a la sede Central. Esto por decisión del cliente. Las características de esta VPN será la misma que tienen en estos momentos, las cuales no desean ser expuestas en este trabajo. Estas localidades mantendrán el direccionamiento IP que poseen, ya que el mismo no afecta a los demás y prefieren mantener el mismo. Son direcciones privadas, 2 con clase A y el tercero clase C.

Estas instalaciones estaban previstas para mediados de Febrero de 2008.

CONCLUSIONES

Luego de realizar el diseño y la implementación del sistema de VPN para Cinex, para prestar comunicación entre la sede principal y las demás localidades a lo largo de todo el territorio nacional, se pueden señalar las conclusiones siguientes:

- Los routers elegido con las caracteristicas de seguridad cumple con los requerimientos preestablecidos por Cinex al inicio del proyecto, establecer comunicaciones con las localidades de forma segura y manejar un ancho de banda razonable.

- Con el enlace Frame Relay en la sede principal con direccionamiento IP estático y público, se asegura el correcto cierre de los túneles de las diversas localidades y provee un ancho de banda acorde para diversas operaciones.

- El equipo ASA 5510 que es el equipo de seguridad y concentrador de túneles VPN cuenta con la capacidad de soportar hasta 100 túneles, lo que ofrece capacidad de expansión y cuenta con una serie de características de seguridad avanzadas para proteger la red en si.

- Administración remota por SSH de los equipos de las localidades, garantizando que los datos viajen seguros por la red pública y permitiendo hacer cambios a las localidades desde la sede principal.

- La disminución de costos en mas un 50% mensual y la posibilidad de escalamiento inmediato en comparación con el sistema con el que contaban antes.

- En líneas generales se logró diseñar e implementar un sistema que le va a brindar a la empresa la capacidad de interactuar de forma inmediata con las diversas localidades y disponer de información al momento de las ventas de entradas a los cines que es su negocio en sí, y de esta forma brindar mejor servicio de venta de los mismos a través de los diversos medios que poseen (por taquilla, teléfono o Internet).

RECOMENDACIONES

- Los enlaces ADSL con los que cuenta Cinex en sus localidades para establecer los túneles VPN presentan problemas regularmente, por lo que se sugiere que se soliciten a otro proveedor estos servicios. De esta manera se contará con dos enlaces, uno activo y otro de respaldo; esto con la finalidad de proporcionarle mayor confiabilidad. Por ejemplo, el enlace Frame Relay en la principal, que a pesar de no haber presentado inconvenientes hasta ahora, si el mismo se cae, se pierden todas las conexiones hacia las localidades.

- Actualmente los servidores de los que dispone Cinex se encuentran en el mismo segmento de la LAN, por lo que es recomendable colocarlos en DMZ, para de este obtener mayor seguridad en la red.

- El equipo instalado en las localidades no cuenta con la capacidad para manejar VoIP, por lo que si se requiere a futuro incorporar este, es necesario cambiar los equipos. Esto fue debido a que el cliente no quiso realizar esta inversión de una vez y optó por estos más sencillos para las localidades. En la sede principal si se cuenta con este servicio y de ser instalado se le debe aplicar calidad de servicio (QoS).

- El tipo de encriptación utilizada es 3DES, pero de ser posible más adelante se debería cambiar a AES, debido a que es más reciente e inclusive más rápida, ya que los equipos están en la capacidad de soportarlos.

REFERENCIAS BIBLIOGRÁFICAS

[1] Echenique S., Pablo J. Implantación de una red privada virtual (VPN) para el acceso seguro y controlado al sistema de información del sector eléctrico venezolano (SISE). (Trabajo Especial de Grado).--Caracas: Universidad Central de Venezuela 2004

[2] Wikipedia. Enciclopedia virtual de consulta http://es.wikipedia.org/wiki/ Consultados: WAN - Frame Relay - Direccionamiento IP - Protocolo SNMP – Telnet - SSH - Firewall [Consulta: 2007].

[3] Forouzan, Behrouz A. Transmisión de datos y redes de comunicaciones, segunda edición. España: McGraw-Hill, 2001.

[4] Cisco Systems CCNA 3.1. Cisco Certified Networking Associate. Módulo 1, 2, 3 y 4.

[5] Alegsa. Enciclopedia virtual de consulta. xDSL http://www.alegsa.com.ar/Dic/. [Consulta 2007]

[6] Román P., Miguel A. Diseño e implementación de un sistema inalámbrico punto – multipunto en la banda de 5,8 GHz para la red platino – INE. Román Miguel (Tesis). -- Caracas: Universidad Central de Venezuela 2007.

[7] Fuenmayor, Carlos. Guia de Sistemas de Banda Ancha. Universidad Central de Venezuela.

[8] Vitti V. Nando A. Diseño e Implantación de una WAN Segura para el Transporte y Procesamiento de Datos Estadísticos del Instituto Nacional de Estadística (INE). (Trabajo Especial). – Caracas: Universidad Central de Venezuela 2003.

[9] Criptologia.pdf. Manuel Pons Martorell. Departamento de Telecomunicaciones. Escuela Universitária Politécnica de Mataró. 2000

[10] Cisco. An Introduction to IP Security (IPSec) EncryptionCisco pdf. Document ID 16439. U.S. 2005.

[11] Teldat. Router Teldat, Protocolo VRRP. Doc DM759 Mayo 2005. http://hondo.diatel.upm.es/manuales/Teldat/V_10_5/Dm759v105_Protocolo_VRRP.pdf

[12] Aprende Redes.com, El Blog CCNA de Ernesto Ariganello. Documento del 4 de Agosto 2006.http://www.aprenderedes.com/?p=56.

[13] Microsoft.com. Póngase en marcha con el escritorio remoto. http://www.microsoft.com/spain/windowsxp/using/mobility/getstarted/remoteintro.mspx

[14] Aprende Redes.com. Listas de Acceso. http://www.aprenderedes.com/?p=109

BIBLIOGRAFÍA

Forouzan, Behrouz A. Transmisión de datos y redes de comunicaciones, segunda edición. España: McGraw-Hill, 2001.

Tanenbaum, Andrew S. Redes de Computadoras, cuarta edición. México: Pearson, 2003.

Cisco Systems. Cisco Certified Networking Associate. Modulo 1, 2, 3 y 4.

Cisco Systems. Cisco Certified Networking Professional. Modulo 1.

Echenique S., Pablo J. Implantación de una red privada virtual (VPN) para el acceso seguro y controlado al sistema de información del sector eléctrico venezolano (SISE). (Trabajo Especial de Grado).--Caracas: Universidad Central de Venezuela 2004

Vitti V. Nando A. Diseño e Implantación de una WAN Segura para el Transporte y Procesamiento de Datos Estadísticos del Instituto Nacional de Estadística (INE). (Trabajo Especial). – Caracas: Universidad Central de Venezuela 2003.

Securing Networks with PIX and ASA, version 4.0. Cisco Systems, Inc. 30/01/2007. Impreso en Canada.

Diccionario de Protocolos. (http://www.javvin.com/protocolsuite.html).

Enciclopedia virtual de consulta. (http://www.wikipedia.com).

GLOSARIO

AES *Advanced Encryption Standard, también conocido como Rijndael, es un esquema de cifrado por bloques adoptado como un estándar de cifrado por el gobierno de los Estados Unidos.*

ADSL *Asymmetric Digital Subscriber Line o Línea de Abonado Digital Asimétrica. ADSL es un tipo de línea DSL. Consiste en una línea digital de alta velocidad, apoyada en el par de cobre que lleva la línea telefónica convencional, siempre y cuando el alcance no supere los 5,5 km. medidos desde la Central Telefónica. ADSL cuenta con mayor capacidad para la descarga de datos que para la subida.*

AH *Authentication Header. La autenticación de cabecera está dirigido a garantizar integridad sin conexión y autenticación de los datos de origen de los datagramas IP*

ANSI *Abreviatura Instituto Nacional Americano para la Estandarización. Es una corporación completamente privada sin fines de lucro que funciona como la coordinación Nacional para la estandarización de interconexión de redes, servicios, señalización y arquitecturas RDSI jerarquía óptica SONET; dentro de los Estados Unidos.*

Certificado X.509v3 *Se trata de una recomendación de la ITU usada para establecer servicios de autenticación de usuarios de directorios de sistemas abiertos*

Cliente *Es un programa que se ejecuta en una máquina local y que solicita un servicio de un servidor.*

Datagrama *Los paquetes en el nivel IP se denominan datagramas, estos paquetes son de longitud variable (Hasta 65.635 bytes) que constan de dos partes: una cabecera y datos.*

DCE *El equipo Terminal de circuito de datos (DCE) incluye cualquier unidad funcional que transmita o reciba datos a través de una red digital o analógica.*

DES y 3DES *Data Encryption Standard y Triple DES, es un algoritmo de cifrado*

Diffie-Hellman *Permite el intercambio secreto de claves entre dos partes que no han tenido contacto previo, utilizando un canal inseguro. Se usa como medio para acordar claves simétricas.*

DLCI *Los DLCI se asignan no solo para definir el circuito virtual entre un DTE y un DCE, sino también para definir un circuito virtual entre dos DCE dentro de la red. Un conmutador asigna un DLCI a cada conexión virtual en una interfaz.*

DNS *Abreviatura Domain Name Service. Asocia un nombre con una dirección IP específica. Esto resulta ser muy útil en el Internet ya que facilita la navegación gracias al uso renombres en las direcciones.*

DSL *Línea de Suscriptor Digital. Tecnología de transmisión digital de datos que permite que los cables de cobre telefónicos transfieran hasta 16 Mbps.*

DTE *El equipo Terminal de datos (DTE) incluye cualquier unidad que funcione como origen o destino para datos digitales binarios.*

ESP *Encapsulating Security Protocol. Es un protocolo que proporciona autenticidad de origen, integridad y protección de confidencialidad de un paquete.*

FTP *Abreviatura File Transfer Protocol. Es un servicio confiable orientado a conexión que utiliza TCP para transferir archivos entre sistemas que admiten FTP. El propósito principal de FTP es transferir archivos desde un computador hacia otro copiando y moviendo archivos desde los servidores hacia los clientes*

FQDN *Fully Qualified Domain Name, es un nombre DNS completo. Incluye el nombre del host y el nombre del dominio asociado a la misma.*

Full-Dúplex *Ambas estaciones pueden enviar y recibir información al mismo tiempo.*

Hash *Una función Hash es una función para resumir o identificar probabilísticamente un gran conjunto de información, dando como resultado un conjunto de imagen finito generalmente*

menor

Host *Es el nombre único que se le da a un dispositivo conectado a una red informática. Puede ser un ordenador, un servidor de archivos, un dispositivo de almacenamiento por red, una máquina de fax, etc.*

HSRP *Hot Standby Router Protocol. Cisco Systems desarrolló este protocolo de redundancia para el segmento LAN, cuando se cuenta con más de un router y dispositivos que utilizan solamente una dirección IP estática como gateway determinado.*

IETF *Grupo de Trabajo de Ingeniería de Internet (Internet Engineering Task Force) es una organización internacional abierta de normalización, que tiene como objetivos contribuir a la ingeniería de Internet.*

IKE *Internet Key Exchange, es un protocolo usado para establecer una asociación segura en el protocolo IPsec.*

IP *Abreviatura de Protocolo de Internet. Es el mecanismo de transmisión utilizado por los protocolos TCP/IP; está basado en datagramas sin conexión y no fiable, y ofrece un servicio de mejor entrega posible.*

IPsec *Internet Protocol Security, es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre IP autenticando y/o cifrando cada paquete IP en un flujo de datos.*

ISAKMP *Internet Security Association and Key Managemnet Protocol, es un protocolo criptográfico que constituye la base del protocolo de intercambio de claves IKE. Definido en el RFC 2408.*

ITU o UIT *La Unión Internacional de Telecomunicaciones (UIT) es el organismo especializado de las Naciones Unidas encargado de regular las telecomunicaciones, a nivel internacional, entre las distintas administraciones y empresas operadoras.*

ISO *Abreviatura de Internacional Standards Organization. Es un organismo multinacional totalmente voluntario dedicado a acuerdos mundiales sobre estándares internacionales. Una de sus misiones es el área de la Tecnología de la Información, que ha resultado en la creación del modelo de Interconexión de Modelos Abiertos (OSI).*

Kerberos	*Es un protocolo de autenticación de redes que permite a dos equipos de una red insegura demostrar su identidad mutuamente basada en criptografía de clave simétrica.*
L2F	*(Layer 2 Forwarding), protocolo desarrollado por Cisco Systems, tiene como objetivo proporcionar un mecanismo de tunneling para el transporte de tramas a nivel de enlace*
L2TP	*(Layer 2 Tunneling Protocol), protocolo de túnel de capa 2. Es el resultado de la combinación de los protocolos L2F y PPTP. Permite la creación de túneles a través de una gran variedad de tipos de redes.*
LAN	*Abreviatura de Local Area Network. Es una red de área loca; generalmente opera dentro de un área muy reducida. Suele conectar enlaces de una única oficina, edificio o campus, dependiendo de las necesidades de la organización.*
LMI	*La información de gestión local es un protocolo añadido a Frame Relay para ofrecer más características de gestión como lo son: control de flujo de datos, comprobación de estado de DCE´s y un mecanismo de sistema de radiado para establecer comunicaciones a varios DTE.*
MD5	*Algoritmo de Resumen del Mensaje 5 (Message Digest Algorithm 5), es un algoritmo de reducción criptográfico de 128 bits.*
NAT	*Network Address Translation*
NIC	*Centro de Información de Red (Network Information Center). Es el encargado de asignar dominios de Internet bajo su dominio de red, sean genéricos o de países, a personas naturales o empresas.*
NIST	*Instituto Nacional de Estándares y Tecnologías (Nacional Institute of Standards and Technology) es una agencia de la Administración de Tecnología del Departamento de Comercio de los Estados Unidos.*
Oakley Key Determination Protocol	*Es un protocolo que usa un mecanismo para realizar el intercambio seguro de llaves autenticadas durante la primera fase de ISAKMP.*

OSI	*Modelo de referencia de Interconexión de Sistemas Abiertos (Open System Interconnection) fue el modelo de red descriptivo creado por ISO; es un marco de referencia para la definición de arquitecturas de interconexión de sistemas de comunicaciones.*
PPPTP	*(Point-to-Point Tunneling Protocol): Es un protocolo de red creado por Microsoft que permite la realización de transferencias seguras desde clientes remotos a servidores emplazados en redes privadas.*
PVC:	*Circuito virtual permanente que se establece entre dos DTE a través del proveedor de servicios de la red. Los dos DTE se conectan en forma permanente a través de conexión virtual. Se asignan DLCI a las interfaces en los extremos de la conexión.*
RFC	*Request For Comments (petición de comentarios). Son una serie de notas sobre Internet que comenzaron a publicarse en 1969. Cada una de ellas es un documento cuyo contenido es una propuesta oficial para un nuevo protocolo de red Internet que explica todo detalle.*
Router o enrutador	*Conectan y permiten la comunicación entre dos redes y determinan la mejor ruta para la transmisión de datos a través de las redes conectadas.*
SA	*Security Association, es una asociación segura. Un acuerdo de seguridad como consecuencia de combinación de claves negociadas.*
SHA	*Algoritmo de Hash Seguro (Secure Hash Algorithm) es un sistema de funciones hash criptográficas relacionas con la Agencia de Seguridad Nacional de los Estados Unidos. Produce una salida resumen de 160 bits*
SSL	*(Secure Socket Layer), La Capa de conectores seguros es un protocolo que suministra un canal seguro. Con SSL, el cliente y el servidor utilizan una cierta técnica para acordar el nivel de seguridad que quieren usar durante la sesión. La identificación ocurre sobre un canal seguro y toda la información se transmite sobre las sesiones encriptadas.*
SSH	*Secure Shell es el nombre de un protocolo y del programa que lo implementa que sirve para acceder a máquinas remotas a través de Internet de forma seguro ya que la información viaja encriptada y no como texto plano.*

Semidúplex	*Cada estación puede tanto enviar como recibir, pero no al mismo tiempo.*
Servidor	*Es un programa que se ejecuta en una máquina remota y que ofrece un servicio a los cliente;, una vez que es iniciado este permanece en ejecución a no ser que ocurra un problema.*
Símplex	*Es un modo de transmisión donde la comunicación es unidireccional, solamente una de las dos estaciones puede transmitir y la otra solo recibir.*
SNMP	*Abreviatura Simple Network Management Protocol. Es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red.*
Switch	*Es un dispositivo electrónico de interconexión de que opera en la capa 2.Un conmutador interconecta dos o más segmentos de red, permitiendo el tráfico de datos de un segmento a otro, de acuerdo a la dirección MAC de los equipos.*
TCP	*Abreviatura de Transmission Control Protocol. Es un protocolo de Capa 4 orientado a conexión que suministra una transmisión de datos full-duplex confiable. Forma parte del TCP/IP.*
TELNET	*Abreviatura de Terminal Network. Es un programa de aplicación cliente-servidor que permite el establecimiento de una conexión con un sistema remoto de forma que el Terminal local aparece como un Terminal del sistema remoto.*
UDP	*Abreviatura de User Datagram Protocol. Es un protocolo de transporte no orientado a conexión de la pila de protocolo TCP/IP. El UDP es un protocolo simple que intercambia datagramas sin acuse de recibo ni garantía de entrega.*
UTP	*Cable de par trenzado; es el tipo más frecuente de medio de comunicación que se usa en redes. Su frecuencia de operación es desde 100Hhz hasta 5MHz. Están conformados por pares trenzados generalmente de cobre y de acuerdo al número de pares de establecen categorías.*
VoIP:	*Abreviatura Voice over Internet Protocol. Es un protocolo que hace posible que la señal de voz viaje a través de Internet y redes IP.*
VPN	*Redes Privadas Virtuales (Virtual Private Network), es una*

	tecnología que permite una extensión de la red local sobre una red pública o no controlada.
VRRP	*Virtual Router Redundancy Protocol, es un protocolo que se encarga de asignar dinámicamente la función de router virtual a uno de los router dentro de una LAN (cuando hay mas de uno).*
WAN	*Abreviatura Wide Area Network. Conectan redes de usuarios dentro de un área geográfica extensa, permiten que las empresas se comuniquen entre sí a través de grandes distancias a través de la interconexión de LAN´s.*