UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES
ARAGÓN

"ESTUDIO DE LOS PROCESOS DE SEGURIDAD QUE INTERVIENEN EN LOS ENLACES DE COMUNICACIÓN ENTRE REDES PUNTO A PUNTO Y DE TIPO VPN."

T E S I N A

QUE PARA OBTENER EL TÍTULO DE:
INGENIERO EN COMPUTACIÓN

P R E S E N TA:
VERGARA ALBA JOHANA MONTSERRAT

ASESOR: ING. ENRIQUE GARCÍA GUZMÁN

MÉXICO 2010

Gracias primero a Dios por estar conmigo en cada paso que doy, por fortalecer mi corazón e iluminar mi mente y gracias por haber puesto en mi camino a todas las personas que han aportado en este trabajo.

En especial a

Mi familia que me ayudaron enormememnte para poder finalizar este trabajp, por apoyarme y permitirme poder darles esta satisfacción en la vida.

a Alfonso que sin duda sus regaños me hicieron a tiros y jalones lograr este paso en la vida,

Para mis asesor que sin duda fue una gran apoyo en la culmincion de este . . .

ÍNDICE

Página

Página

ÍNDICE DE FIGURAS

Página

Página

ÍNDICE DE TABLAS

ÍNDICE DE DIAGRAMAS

Página

52

DIAGRAMA 19. Ruteadores del enlace de comunicación telecomm-inbursa 57

INTRODUCCIÓN

En el presente trabajo se expusieron parte de los conocimientos adquiridos en el diplomado “Tecnologías de la Información y Comunicaciones”, especialmente en su modulo 6 de “Seguridad Informática” el cual se refiere a la seguridad en las redes, aplicando y demostrando estos conocimientos en casos prácticos dentro de las redes de Telecomm (Organismo público descentralizado de la Secretaría de Comunicaciones y Transportes) en su interconexión con instituciones bancarias como Banamex® e Inbursa®.

En la actualidad ya no es posible comprender un ambiente computacional ajeno al uso de las redes, tómese la Internet como el principal y más claro ejemplo, el uso de las redes se ha globalizado de manera muy acelerada y con ello, la implementación de diferentes métodos y herramientas para la seguridad de las mismas.

Si bien es cierto que con el uso de las redes se obtiene una enorme gama de beneficios, la correcta implementación será parte fundamental para aprovechar al máximo estos recursos, pero no se hace referencia exclusivamente a la implementación e interconexión de los diferentes dispositivos que intervienen en ella, recuérdese que en la actualidad, la información es el bien más preciado para cualquier empresa y el correcto uso de esta marca la diferencia en un ambiente tan globalizado y competitivo como el que actualmente se tiene. Es por ello que parte fundamental en el establecimiento de una red será la implementación de las políticas y procesos necesarios inherentes a la seguridad informática.

Al hablar de la seguridad informática, o bien de los procesos que intervienen en ella, se debe hacer mención y dejar muy claro desde el principio, que estos se dan en dos grandes grupos:

- **Físicos.**
- **Lógicos.**

Físicos: Entiéndase que serán todas aquellas medidas de seguridad que se deben de tomar para salvaguardar la integridad de la información y de la comunicación que se tenga (red).

Lógicos: Este grupo engloba todos los procesos informáticos que son llevados a cabo vía software o hardware para salvaguardar la integridad de una red y de la información que en ella circula.

El presente trabajo se enfoca principalmente al estudio de los estos últimos sin dejar a un lado los procesos físicos que como ya se menciono no dejan de ser menos importantes.

Para ayudar a tener un panorama más amplio de las implicaciones que conlleva la seguridad informática tómese en cuenta el siguiente caso práctico:

Muy a menudo se permite a un usuario acceder fácilmente al equipo de otro usuario utilizando debilidades bien conocidas, relaciones de confianza y opciones predeterminadas. La mayor parte de estos ataques necesitan poca o ninguna habilidad computacional, poniendo la integridad de una red en riesgo.

La mayoría de los empleados no necesitan y no deben tener acceso al resto de equipos, funciones administrativas, dispositivos de red, etcétera. Sin embargo, debido a la cantidad de flexibilidad necesaria para la función normal, las redes internas no pueden permitirse una seguridad máxima. Por otro lado, sin ninguna seguridad, los usuarios internos pueden ser una importante amenaza para muchas redes corporativas.

Un usuario de la empresa ya tiene acceso a muchos recursos internos y no necesita evitar cortafuegos *[firewall]* u otros mecanismos de seguridad que previenen que las fuentes no confiables, como usuarios de la Internet, accedan a la red interna. Dichos usuarios internos, equipados con mucha habilidad, pueden penetrar satisfactoriamente y conseguir derechos de administración remota de red mientras que asegura que su abuso sea difícil de identificar o incluso de detectar.

Una pobre seguridad de red también significa que, si un intruso externo fuerza un equipo de red, podrá acceder al resto de la red interna más fácilmente. Esto habilitaría a un atacante especializado donde podría leer y posiblemente filtrar correo y documentos confidenciales; equipos basura, haciendo creer en pérdidas de información; y más. Por no mencionar que entonces utilice la red y recursos para volverse e iniciar el ataque a otros sitios, que cuando sean descubiertos le apuntarán a los administradores de una empresa, no al intruso.

La mayoría de ataques, contra vulnerabilidades conocidas, podrían ser fácilmente resueltos y, por lo tanto, ser detenidos por los administradores de red si conocieran la vulnerabilidad en primer lugar.

OBJETIVOS

Al contar con la comunicación entre los nodos centrales de Telecomm hacia Banamex e Inbursa se podrán brindar servicios financieros de banca básica (consulta de saldos, depósitos bancarios y retiro de efectivo) en las más de 4000 administraciones con las que cuenta Telecomm a lo largo de la república mexicana, el establecimiento de estos enlaces de comunicación dará surgimiento a una nueva red en donde la seguridad informática será el principal punto de estudio.

Los enlaces de comunicación de las redes trabajaran bajo esquemas "punto a punto" en el caso Telecomm-Inbursa® y de tipo "VPN" para la comunicación entre los nodos Telecomm-Banamex® es por ello que considerando este breve panorama general puedo plantear lo siguiente:

"El correcto establecimiento de los mecanismos de seguridad y configuración de los mismos dentro de los equipos que intervendrán en la comunicación de las redes WAN permitirán un control detallado de los procesos y usuarios que se encuentren trabajando de forma remota dentro de las redes, evitando así comprometer la integridad de las redes"

Al establecer la seguridad en la redes WAN esta por demás mencionar que se deberá de hacer un trabajo igual de minucioso en lo inherente a la seguridad dentro de las redes LAN, en este caso se abordaran los trabajos realizados dentro del nodo de Telecomm y con ello se busca alcanzar objetivos particulares como:

- Comunicar eficientemente entre los nodos principales de Telecomm, Inbursa® y Banamex®.
- Establecer herramientas para el monitoreo de los enlaces de comunicación.
- Crear de una VPN en sus diferentes fases.
- Estudiar y aplicar el ruteo estático.
- Crear de grupos de trabajo utilizando switch y VLAN.
- Aplicar permisos para bloquear procesos y usuarios en especifico utilizando contrafuegos *[Firewall]*
- Establecer herramientas para el monitoreo de procesos que puedan causar afectación en el funcionamiento de las redes.

Dentro de la conclusión de este trabajo se retomaran estos aspectos esperando haber cumplido con cada uno de ellos en su correcta implementación.

CAPÍTULO I

CONCEPTOS INVOLUCRADOS EN LA SEGURIDAD DE ENLACES DE COMUNICACIÓN

1.1 MODELO DE REFERENCIA OSI DE ISO.

Puede decirse que las redes de computadoras comenzaron a verse como una gran ventaja para las empresas en la década de los 80 que es cuando explota la proliferación de estos recursos. En un principio, el principal problema que se tenía al trabajar con las redes era la compatibilidad entre los equipos y protocolos de los diferentes fabricantes que competían en el mercado, lograr esta compatibilidad era excesivamente difícil además de costosa, una computadora o bien un equipo de telecomunicaciones presentaban diferencias en:

- El procesador central.
- La velocidad.
- La memoria.
- Los dispositivos de almacenamiento.
- La interfaz para las comunicaciones.
- Los códigos de caracteres.
- Los sistemas operativos.

Este fue el principal problema que las redes tuvieron que afrontar en su surgimiento es por ello que para enfrentar el problema de incompatibilidad de redes, la Organización Internacional para la Estandarización (ISO) investigó modelos de conexión como la red de Digital Equipment Corporation (DECnet), la Arquitectura de Sistemas de Red (SNA) y TCP/IP a fin de encontrar un conjunto de reglas aplicables de forma general a todas las redes. Con base en esta investigación, la ISO desarrolló un modelo que ayuda a los fabricantes a crear redes que sean compatibles con otras redes, resultado de estos trabajos es el modelo de referencia OSI (Open Systems Interconnection - Interconexión de Sistemas Abiertos) de ISO.

Lo que el modelo de referencia OSI realiza es dividir el problema general de la comunicación, en problemas específicos, facilitando así la obtención de una solución a dicho problema.

Esta estrategia establece dos importantes beneficios:

- Mayor comprensión del problema.
- La solución de cada problema específico puede ser optimizada individualmente.

Este modelo de referencia también persigue un objetivo claro y bien definido, mismo que puede resumirse de la siguiente manera:

Formalizar los diferentes niveles de interacción para la conexión de computadoras habilitando así la comunicación del sistema de cómputo independientemente de:

- El fabricante.
- La arquitectura.
- La localización.
- El sistema operativo.

Este objetivo tiene las siguientes aplicaciones:

- Obtener un modelo de referencia estructurado en varios niveles en los que se contemple desde el concepto BIT hasta el concepto APLICACION.
- Desarrollar un modelo en el cual cada nivel define un protocolo que realiza funciones específicas diseñadas para atender el protocolo de la capa superior.
- No especificar detalles de cada protocolo.
- Especificar la forma de diseñar familias de protocolos, esto es, definir las funciones que debe realizar cada capa.

El objetivo perseguido por el modelo de referencia OSI establece también una estructura que presenta las siguientes particularidades:

- Estructura multinivel: Se diseñó una estructura multinivel con la idea de que cada nivel se dedique a resolver una parte del problema de comunicación, esto es, cada nivel ejecuta funciones específicas.
- El nivel superior utiliza los servicios de los niveles inferiores: Cada nivel se comunica con su similar en otras computadoras, pero debe hacerlo enviando un mensaje a través de los niveles inferiores en la misma computadora. La comunicación internivel está bien definida. El nivel N utiliza los servicios del nivel N-1 y proporciona servicios al nivel N+1.
- Puntos de acceso: Entre los diferentes niveles existen interfaz llamadas "puntos de acceso" a los servicios.
- Dependencias de Niveles: Cada nivel es dependiente del nivel inferior y también del superior.
- Encabezados: En cada nivel, se incorpora al mensaje un formato de control. Este elemento de control permite que un nivel en la computadora receptora se entere de que su similar en la computadora emisora esta enviándole información. Cualquier nivel dado, puede incorporar un encabezado al mensaje. Por esta razón, se considera que un mensaje está

constituido de dos partes: Encabezado e Información. Entonces, la incorporación de encabezados es necesaria aunque representa un lote extra de información, lo que implica que un mensaje corto pueda ser voluminoso.

En base a todas estas características que se han mencionado el modelo de referencia OSI presenta una estructura de 7 capas (***FIGURA 1***):

- Capa 1: Física.
- Capa 2: Enlace.
- Capa 3: Red.
- Capa 4: Transporte.
- Capa 5: Sesión.
- Capa 6: Presentación.
- Capa 7: Aplicación.

En donde como se mencionó para su correcto funcionamiento, la capa N necesita de los servicios de la capa N-1 para proporcionar a su vez los servicios necesarios para la capa N+1. Por ejemplo la capa 4 de Transporte (N), necesita que la capa 3 de Red (N-1) funcione correctamente para que entonces se brinden los servicios que la capa 5 de Sesión (N+1) necesita.

FIGURA 1. MODELO DE REFERENCIA OSI DE ISO

En los subsecuentes puntos se explicará la función de cada una de estas capas que deben funcionar todas para que la comunicación se dé correctamente en base a este modelo.

1.1.1 CAPA 1 FÍSICA.

Es el primer nivel del modelo OSI y en él se definen y reglamentan todas las características físicas-mecánicas y eléctricas que debe cumplir el sistema para poder operar. Como es el nivel más bajo, es el que se va a encargar de las comunicaciones físicas entre dispositivos y de cuidar su correcta operación.

En este nivel, se encuentran reglamentadas las interfases de sistemas de cómputo y telecomunicaciones (RS-232 o V.24, V.35) además de los tipos de conectores o ensambles mecánicos asociados a las interfases (DB-24 y RJ-45 para RS-232 o V.24, así como el coaxial)

En este nivel, se ubican también todos aquellos dispositivos pasivos y activos que permiten la conexión de los medios de comunicación como:

- Repetidores de redes LAN
- Repetidores de microondas y fibra óptica
- Concentradores de cableado (*HUB*)
- Conmutadores de circuitos físicos de telefonía o datos
- Equipos de modulación y demodulación (modems)
- Hasta los aparatos receptores telefónicos.

Como resumen de los cometidos de esta capa, puede decirse que se encarga de transformar un paquete de información binaria ("*Frame*") en una sucesión de impulsos adecuados al medio físico utilizado en la transmisión. Estos impulsos pueden ser eléctricos (transmisión por cable); electromagnéticos (transmisión inalámbrica) o luminosos (transmisión óptica). Cuando actúa en modo recepción el trabajo es inverso; se encarga de transformar estos impulsos en paquetes de datos binarios que serán entregados a la capa de enlace.

FIGURA 2. DISPOSITIVOS QUE INTERVIENEN PARA LA INTERCONEXIÓN DE REDES

1.1.2 CAPA 2 ENLACE.

Esta capa traslada los mensajes hacia y desde la capa física a la capa de red. Especifica cómo se organizan los datos cuando se transmiten en un medio particular. Esta capa define como son los cuadros, las direcciones y las sumas de control de los paquetes Ethernet.

Además del direccionamiento local, se ocupa de la detección y control de errores ocurridos en la capa física, del control del acceso a dicha capa y de la integridad de los datos y fiabilidad de la transmisión .Para esto agrupa la información a transmitir en bloques, e incluye a cada uno una suma de control que permitirá al receptor comprobar su integridad. Los datagramas recibidos son comprobados por el receptor, si alguno se ha corrompido se envía un mensaje de control al remitente solicitando su reenvío.

La capa de enlace puede considerarse dividida en dos subcapas:

- El Control Lógico de Enlace LLC: Define la forma en que los datos son transferidos sobre el medio físico, proporcionando servicio a las capas superiores.

- El Control de Acceso al Medio MAC: Esta subcapa actúa como controladora del hardware subyacente (el adaptador de red). De hecho, el controlador de la tarjeta de red es denominado a veces "*MAC driver*", y la dirección física contenida en el hardware de la tarjeta (***FIGURA 3***) es conocida como dirección. Su principal función consiste en arbitrar la utilización del medio físico para facilitar que varios equipos puedan competir simultáneamente por la utilización de un mismo medio de transporte.

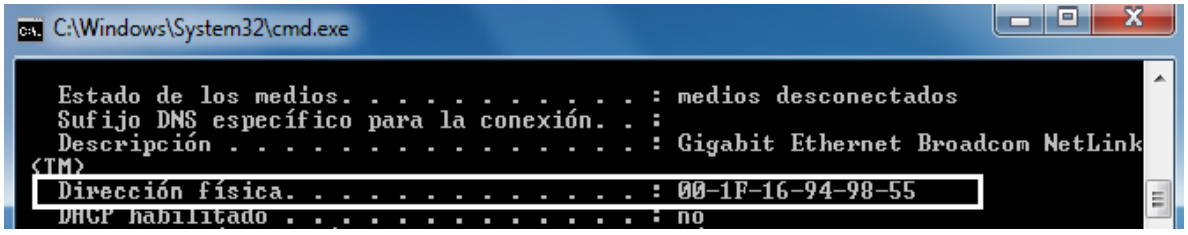

FIGURA 3. DIRECCIÓN FÍSICA (MAC ADDRESS) DE UNA TARJETA DE RED.

En resumen puede decirse que esta capa se ocupa del:

- Direccionamiento físico.
- Topología de la red.
- Acceso a la red.
- Notificación de errores.
- Distribución ordenada de tramas.
- Control del flujo.

1.1.3 CAPA 3 RED.

El objetivo de la capa de red es hacer que los datos lleguen desde el origen al destino, aun cuando ambos no estén conectados directamente. Los dispositivos que facilitan tal tarea se denominan encaminadores, aunque es más frecuente encontrar el nombre inglés *router* y, en ocasiones enrutadores.

Los ruteadores trabajan en esta capa, aunque pueden actuar como conmutador de nivel 2 en determinados casos, dependiendo de la función que se le asigne. Los cortafuegos actúan sobre esta capa principalmente, para descartar direcciones de máquinas.

En este nivel se realiza el direccionamiento lógico y la determinación de la ruta de los datos hasta su receptor final, es decir que a pesar de estar trabajando dentro de un segmento cualquiera dentro de una red no se podrá tener acceso a todos los recursos de la misma, solamente a aquellos que hayan sido definido en los equipo de ruteo vía la dirección IP.

El número **IP** es la dirección lógica que identifica a tu ordenador en una red (ya sea local o externa).

Esta dirección es única para cada equipo en el mundo única dentro de cada red local y la llamamos dirección lógica porque solamente con conocer el IP, cualquier enrutador es capaz de dirigir los datos al ordenador de destino (o a otro enrutador que probablemente sea capaz de enviar los datos al ordenador de destino.

Una dirección IP (***FIGURA 4***) es un número que identifica de manera lógica y jerárquica a una interfaz de un dispositivo (habitualmente una computadora) dentro de una red.

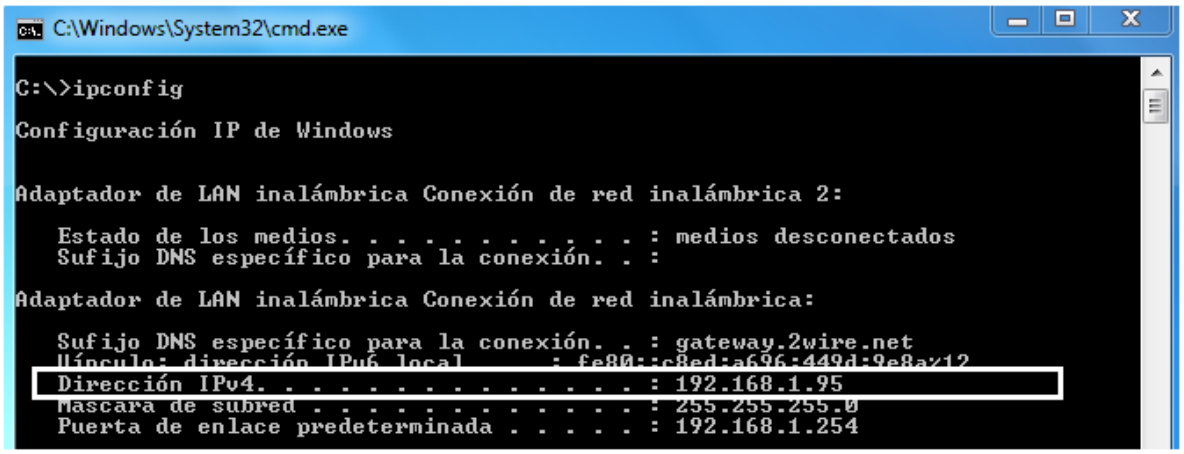

FIGURA 4. DIRECCION LOGICA (IP) DE UNA TARJETA DE RED.

Los sitios de la Internet que por su naturaleza necesitan estar permanentemente conectados, generalmente tienen una dirección IP fija (comúnmente, IP fija o IP estática), es decir, no cambia con el tiempo. Los servidores de correo, DNS, FTP públicos, y servidores de páginas web necesariamente deben contar con una dirección IP fija o estática, ya que de esta forma se permite su localización en la red.

A través de Internet, las computadoras se conectan entre sí mediante sus respectivas direcciones IP. Sin embargo, a los seres humanos nos es más cómodo utilizar otra notación más fácil de recordar y utilizar, como los nombres de dominio; la traducción entre unos y otros se resuelve mediante los servidores de nombres de dominio DNS.

1.1.4 CAPA 4 TRANSPORTE.

Esta capa es la encargada de efectuar el transporte de los datos (que se encuentran dentro del paquete) de la máquina origen a la de destino, independizándolo del tipo de red física que se esté utilizando.

Sus protocolos son TCP y UDP el primero orientado a conexión y el otro sin conexión.

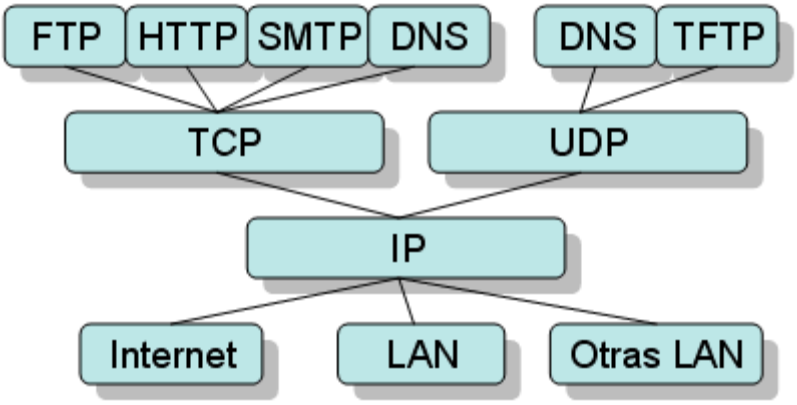

DIAGRAMA 1. Servicios que brindan los protocolos TCP y UDP.

Una vez que los paquetes de datos pasan a través de la capa de red, la capa de Transporte,[la Capa 4] da por sentado que puede usar la red como una "nube" para enviar paquetes de datos desde el origen hacia el destino. La nube resuelve cuestiones tales como:

- ¿Cuál de estas rutas es la mejor para un recorrido en particular?
- ¿Qué ruta muestra un menor tiempo para llegar al destino?
- ¿Qué camino genera un menor costo y un mayor beneficio?

La frase "calidad del servicio" se usa a menudo para describir el propósito de la Capa 4, [la capa de Transporte]. Sus funciones principales son

transportar y regular el flujo de información desde el origen hasta el destino de manera fiable y precisa.

A continuación se presenta una breve descripción de los dos principales protocolos que utiliza esta capa.

TCP: Ofrece un circuito virtual entre aplicaciones de usuario final. Sus características son las siguientes:

- Orientado a conexión.
- Fiable.
- Divide los mensajes salientes en segmentos.
- Reensambla los mensajes en la estación destino.
- Vuelve a enviar lo que no se ha recibido.
- Reensambla los mensajes a partir de segmentos entrantes.

Este protocolo TCP agrega ciertos campos a las tramas de información que circulan por la red. A continuación se ve la definición de estos campos que se agregan:

- Puerto origen: Número del puerto que realiza la llamada.
- Puerto destino: Número del puerto que recibe la llamada.
- Número de secuencia: Número que se usa para garantizar el secuenciamiento correcto de los datos entrantes.
- Número de acuse de recibo: Próximo octeto TCP esperado.
- HLEN: Cantidad de palabras de 32 bits del encabezado.
- Reservado: Se establece en cero.
- Bits de código: Funciones de control (como, por ejemplo, .configuración y terminación de una sesión).
- Ventana: Cantidad de octetos que el emisor desea aceptar.
- Checksum: Checksum calculada del encabezado y de los campos de datos.
- Marcador urgente: Indica el final de los datos urgentes.
- Opción una opción: Tamaño máximo de segmento TCP.
- Datos: Datos de protocolo de capa superior.

+	Bits 0 - 3	4 - 7	8 - 15	16 - 31
0	Puerto Origen			Puerto Destino
32	Número de Secuencia			
64	Número de Acuse de Recibo (ACK)			
96	longitud cabecera TCP	Reservado	Flags	Ventana
128	Suma de Verificación (Checksum)			Puntero Urgente
160	Opciones + Relleno (opcional)			
192	Datos			

DIAGRAMA 2. Campos que se agregan con el protocolo TCP.

UDP: Es un protocolo simple que intercambia datagramas (paquetes de datos), sin acuse de recibo ni entrega garantizada. El procesamiento de errores y retransmisión deben ser manejados por otros protocolos. Por ejemplo, para un mail o página web hace falta una conexión: se establece la conexión y se transfieren los datos. En cambio para una emisora de radio por la Internet no hay ningún tipo de conexión, se está transmitiendo continuamente y el que quiera se "engancha" a esa emisora en la Internet.

Las siguientes son sus principales características:

- No orientado a conexión.
- Poco fiable.
- Transmite mensajes (llamados Datagramas del Usuario).
- No ofrece verificación de software para la entrega de segmentos (poco confiable).
- No reensambla los mensajes entrantes.
- No utiliza acuses de recibo.
- No proporciona control de flujo.

1.1.5 CAPA 5 SESIÓN.

La quinta capa del modelo OSI es la capa de sesión o nivel de sesión para algunos, ésta capa tiene como principal objetivo permitir que los usuarios de diferentes máquinas establezcan sesiones entre ellos.

Esto se logra a través de una sesión, en ésta se puede llevar a cabo un transporte de datos ordinario (como en la capa de transporte) a diferencia que aquí se mejoran los servicios que esta proporciona y que utilizan algunas aplicaciones. Es decir, la capa de sesión permite a un usuario entrar a un sistema de tiempo compartido a distancia o bien, compartir archivos a distancia.

Entre la gestión y finalización de las sesiones se llevan a cabo algunos servicios claves para el correcto funcionamiento de esta capa, los cuales son los siguientes:

- EL control de la sesión.
- Mantener los puntos de verificación.
- El control de concurrencia (evitar que se topen dos procesos a la misma vez).

Por lo tanto, el funcionamiento de esta capa es crucial para las comunicaciones en los equipos, debido a que asegura o mantiene el enlace entre dos computadoras; una de las mejoras que ofrece esta capa es que permite la reanudación de tareas en caso de alguna interrupción.

1.1.6 CAPA 6 PRESENTACIÓN.

Para esta capa su objetivo es encargarse de la representación de la información, de manera que aunque distintos equipos puedan tener diferentes representaciones internas de caracteres los datos lleguen de manera reconocible.

Esta capa es la primera en trabajar más el contenido de la comunicación que el cómo se establece la misma. En ella se tratan aspectos tales como la semántica y la sintaxis de los datos transmitidos, ya que distintas computadoras pueden tener diferentes formas de manejarlas.

Esta capa también permite cifrar los datos y comprimirlos. En pocas palabras es un traductor que involucra a la gran cantidad de caracteres que existen en el mundo computacional, los ejemplos más claros son:

- Los sistemas de numeraciones
- El Código ASCII
- El Código Unicote
- Formatos de Audio y Vídeo.

1.1.7 CAPA 7 APLICACIÓN.

Esta última capa del modelo OSI es la que probablemente presenta una mayor interacción con el usuario, al hablar de que esta capa trabaja sobre la aplicación que el usuario está ejecutando no precisamente se debe de confundir que es la encargada de hacer que funcionen las hojas de cálculo, procesadores de palabras, etcétera. Esta capa es la encargada de asignar los protocolos necesarios para el intercambio de información entre las aplicaciones, los principales protocolos que maneja esta capa son:

- HTTP: Protocolo empleado por el navegador de la Internet.
- FTP: Protocolo empleado para transferencia de archivos.
- TELNET: Protocolo para establecer comunicación con dispositivos.
- POP3: Protocolo empleado por los clientes de correo electrónico.

1.2 RUTEADOR.

Un ruteador es un dispositivo hardware principalmente aunque los hay de software que se encarga de mover paquetes de datos de una red a otra (pueden ser entre redes LAN o WAN o una combinación de ambas), este dispositivo opera en la

capa tres del modelo OSI (nivel de red). Su funcionamiento se basa en tablas y protocolos de ruteo. Los ruteadores leen las direcciones IP de red a dónde van los paquetes y le asignan la mejor ruta posible para que logren llegar. Esta “mejor ruta” depende en gran medida de los protocolos de ruteo que se estén empleando pues algunos de estos protocolos consideran diferentes factores para determinar dicha ruta siempre y cuando no se esté empleando un ruteo estático. Algunos de los factores (métricas) que son considerados por los diferentes protocolos de ruteo son:

- Número de saltos necesarios para llegar al destino.
- Trafico que está circulando por la red.
- Costos.
- Distancias.
- Velocidades.
- Ancho de Banda.

FIGURA 5. ROUTER MARCA INTERCRON MODELO G3-501

1.2.1 PROTOCOLOS DE RUTEO.

Los protocolos ruteables son transportados por los protocolos de ruteo sobre una red. Los protocolos ruteables actúan en una variedad de funciones requeridas para la comunicación entre dispositivos de una aplicación de usuario fuente y un destino.

En base a los puntos expuestos hasta el momento a continuación presento los principales protocolos de ruteo y formas de enrutar paquetes dentro de la red más comunes:

- ***Entrega directa.*** La entrega directa se realiza cuando las dos computadoras que se comunican están en la misma red física, por lo que los paquetes se entregan de forma directa, sin pasar por ruteadores, no es realmente una técnica de enrutado.

- ***Salto al siguiente.*** Es la forma más sencilla de enrutamiento, es usado en redes pequeñas que saben que todo lo que no esté en su red se lo va a tener que pasar a otro router mejor conectado. Por ejemplo; si se tienen dos redes (A y B) “A” tiene un ruteador hacia la Internet y otro hacia la otra red,” B” sólo tiene un ruteador hacia la otra red (el ruteador que conecta ”A”

y ”B” es uno solo). El ruteador “A”-“B” conoce las máquinas de la red de “A” y las de la red de “B”, por lo que si le piden que enrute una dirección que no está ni en A ni en B lo tendrá que pasar al ruteador “A”-Internet.

- ***RIP.*** (*Routing Information Protocol*) , Es un protocolo de enrutamiento interno, es decir para la parte interna de la red, la| que no está conectada al *Backbone* de Internet. Es muy usado en sistemas de conexión a Internet, en el que muchos usuarios se conectan a una red y pueden acceder por lugares distintos. Cuando un usuario se conecta el servidor de terminales (equipo en el que finaliza la llamada) avisa con un mensaje RIP al ruteador más cercano advirtiendo de la dirección IP que ahora le pertenece. Así puede verse que RIP es un protocolo usado por distintos ruteadores para intercambiar información y así conocer por dónde deberían enrutar un paquete para hacer que éste llegue a su destino.

- ***OSPF.*** Bajo el lema el camino más corto primero, OSPF se usa, como RIP, en la parte interna de las redes, su forma de funcionar es bastante sencilla. Cada ruteador conoce los ruteadores cercanos y las direcciones que posee cada ruteador de los cercanos. Además de esto, cada ruteador sabe a qué distancia (medida en ruteador) está cada ruteador. Así cuando tiene que enviar un paquete, lo envía por la ruta por la que tenga que dar menos saltos.

- ***BGP.*** El protocolo de la pasarela externa BGP es un protocolo muy complejo que se usa en la interconexión de redes conectadas por un Backbone de la Internet. Este protocolo usa parámetros como ancho de banda, precio de la conexión, saturación de la red, denegación de paso de paquetes, etcétera. para enviar un paquete por una ruta o por otra. Un ruteador BGP da a conocer sus direcciones IP a los ruteadores BGP y esta información se difunde por los ruteadores BGP cercanos y no tan cercanos. BGP tiene sus propios mensajes entre ruteadores, no utiliza RIP.

1.2.2 RUTEO ESTÁTICO.

Es una ruta fija preprogramada por el administrador de la red. Las rutas estáticas no pueden utilizar los protocolos de enrutamiento y no se actualizan por sí solas después de recibir mensajes de actualización, deben actualizarse manualmente.

Parte fundamental en este método de ruteo son precisamente las tablas de ruteo que no es más que una lista ordenada de las direcciones IP que accederán y hacia qué dirección IP deben de ser enviadas, además de precisar claramente que se harán con las direcciones IP que no estén definidas en esta tabla de ruteo, en estos casos es cuando se hace uso de una ruta por default, esto

quiere decir que todo el tráfico que no se reconozca será enviado a esa ruta para descartarlo.

Las principales características del ruteo estático son:

- Rutas establecidas por el administrador de red.
- Los cambios deben ser introducidos manualmente.
- Permite localizar más fácilmente un paquete dentro de la red.
- Incrementan seguridad ya que las rutas estáticas no son enviadas por toda la red.
- Son útiles para establecer una ruta por default.
- Es útil si se desea controlar que ruta debe seleccionar un ruteador.
- Facilita el probar un enlace en particular en la red.
- Permite conservar el ancho de banda que se disponga.

1.2.3 RUTEO DINÁMICO.

Este tipo de ruteo es el que utiliza los protocolos de enrutamiento, esos protocolos calculan automáticamente las rutas a partir de los mensajes de actualización. La mayoría de las redes son dinámicas.

Las tablas de ruteo son actualizadas periódicamente por protocolos de ruteo, reflejando los cambios en la topología de red

Algunas de las principales características del ruteo dinámico son las siguientes:

- Ocurre cuando los ruteadores se envían actualizaciones automáticas de ruteo entre ellos.
- Recalcula de forma automática la nueva mejor ruta dentro de la red, para llegar al destino.
- Actualización automática de la tabla de ruteo.
- Los ruteadores pueden ajustarse dinámicamente a los cambios en las condiciones de la red.
- Trabaja mejor cuando el ancho de banda y grandes cantidades de tráfico de red no son prioritarios.

1.3 SWITCH 3COM 4400

El *Switch* (o conmutador) trabaja en las dos primeras capas del modelo OSI, es decir que éste distribuye los datos a cada máquina de destino, mientras que el conmutador (*Hub*) envía todos los datos a todas las máquinas que responden. Este dispositivo esta diseñado para trabajar en redes con una cantidad de máquinas ligeramente más elevado que el hub, éste elimina las eventuales

colisiones de paquetes (una colisión aparece cuando una máquina intenta comunicarse con una segunda mientras que otra ya está en comunicación con ésta, la primera reintentará luego).

FIGURA 6. SWITCH MARCA TYCO MODELO MDI-X

El conmutador segmenta económicamente la red dentro de pequeños dominios de colisiones, obteniendo un alto porcentaje de ancho de banda para cada estación final.

No están diseñados con el propósito principal de un control íntimo sobre la red o como la fuente última de seguridad, redundancia o manejo.

Al segmentar la red en pequeños dominios de colisión, reduce o casi elimina que cada computadora compita por el medio, dando a cada una de ellas un ancho de banda comparativamente mayor al que se tuviera si se trabajase con Hubs.

Uno de los principales factores que determinan el éxito del diseño de una red, es la habilidad de la red para proporcionar una satisfactoria interacción entre cliente/servidor, pues los usuarios juzgan la red por la rapidez de obtener un acceso a su aplicación y la confiabilidad del servicio.

Hay diversos factores que involucran el incremento de ancho de banda en una red LAN y con ello el uso de uno o varios conmutadores, estos factores pueden ser:

- El elevado incremento de nodos en la red.
- El continúo desarrollo de procesadores más rápidos y poderosos en estaciones de trabajo y servidores.
- La necesidad inmediata de un nuevo tipo de ancho de banda para aplicaciones intensivas cliente/servidor.
- Cultivar la tendencia hacia el desarrollo de granjas centralizadas de servidores para facilitar la administración y reducir el número total de servidores.

1.3.1 GRUPOS DE TRABAJO (VLAN).

Dentro de una organización se tienen varios departamentos que trabajan en conjunto pero no siempre se deben de compartir los recursos que cada uno de ellos tienen, es aquí donde interviene el concepto “grupo de trabajo”.

Cada grupo de trabajo albergara en si mismo los dispositivos que se interconectan directamente a un conmutador pero que están destinados a la función de una tarea en específico, por mencionar un ejemplo considérese un esquema de trabajo como el que se presenta a continuación:

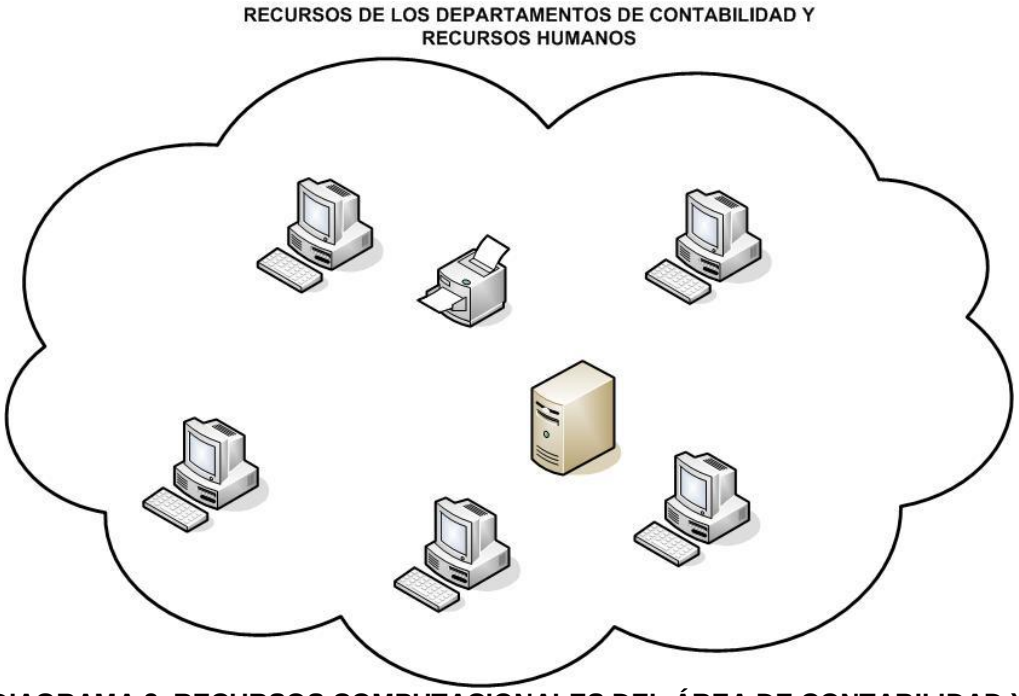

DIAGRAMA 3. RECURSOS COMPUTACIONALES DEL ÁREA DE CONTABILIDAD Y RECURSOS HUMANOS EN ALGUNA INSTITUCIÓN.

En base a este diagrama en este momento todos los dispositivos están conectados a un mismo conmutador y por esa causa todos los dispositivos se pueden ver entre si, lo cual no es muy recomendable pues pueden utilizar servicios que son específicos para un área solamente y estos radican en el servidor.

Al crear grupos de trabajo lo que se hace es segmentar los puertos del conmutador y a pesar de que todos los dispositivos estén conectados al mismo conmutador no podrán verse entre si, dejaran de compartir recursos entre las diferentes áreas.

Este es un buen parámetro para establecer seguridad dentro de una red, debe de considerarse que en la gran mayoría de los casos al momento de administrar una red se pone especial atención a los ataques que pueden venir de “afuera” de la red, pero recordemos que dentro de ella también pueden

suscitarse y deben de planearse las posibles soluciones, el uso de VLAN es un paso para solucionar esta situación.

1.4 CORTAFUEGOS (FIREWALL).

Un cortafuegos es un dispositivo de seguridad vía hardware, software o la combinación de ambos que funciona como guardia de seguridad entre redes, permitiendo o denegando las transmisiones de paquetes de información de una red a la otra. Un uso típico es situarlo entre una red local (LAN) y la Internet, como dispositivo de seguridad para evitar que los intrusos puedan acceder a información confidencial, este esquema se aprecia en el ***Diagrama 3.***

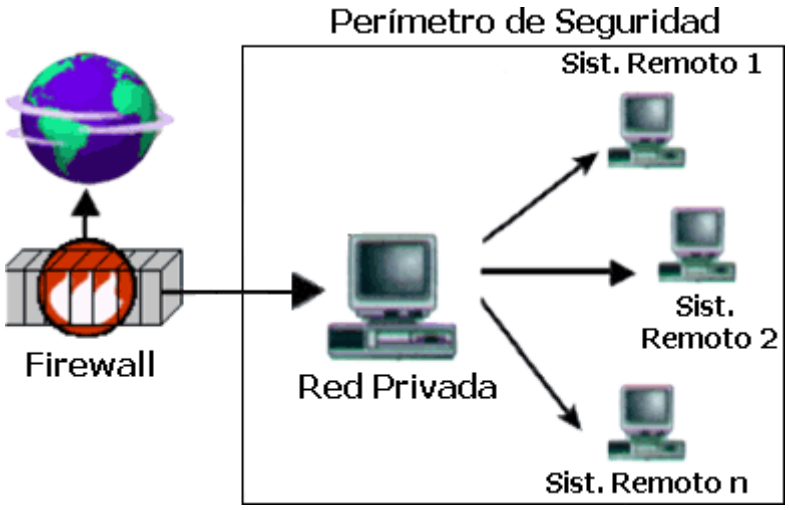

DIAGRAMA 4. MODELO TIPICO DE CONECTIVIDAD DE UN CORTAFUEGOS.

Un cortafuegos es simplemente un filtro que controla todas las comunicaciones que pasan de una red a la otra y en función de lo que sean permite o deniega su paso.

Para permitir o denegar una comunicación el firewall examina diferentes factores en la información que se esta transmitiendo, algunos de estos factores puede ser:

- Tipo de servicio al que corresponde, como pueden ser http, pop3, ftp, etcétera.
- El puerto origen y destino de donde fluye la comunicación.
- Dirección IP origen y destino de los paquetes de comunicación.
- Direcciones MAC de origen y destino.
- Permisos de trabajo sobre dispositivos en específico dentro de la red.
- Subred a la que las computadoras pertenecen.

Dependiendo del servicio el firewall decide si lo permite o no. Además, el cortafuegos examina si la comunicación es entrante o saliente y dependiendo de su dirección puede permitirla o no.

De este modo, un cortafuegos puede permitir desde una red local hacia la Internet servicios de web, correo y ftp, pero no a servicios de mensajería instantánea que pueden ser innecesarios para el desarrollo del trabajo y la productividad de la organización.

También se pueden configurar los accesos que se hagan desde Internet hacia la red local y se pueden denegar todos o permitir algunos servicios como el de la web, (si es que se tiene un servidor web y se quiere acceder desde la Internet).

Dependiendo del cortafuegos que se tenga, también se puede permitir algunos accesos a la red local desde Internet si el usuario se ha autentificado como usuario de la red local., un ejemplo de esto es el uso del escritorio remoto de Windows.

Un firewall puede ser un dispositivo software o hardware como ya se menciono, es decir un dispositivo que se conecta entre la red y el cable de la conexión a la Internet, o bien un programa que se instala en la máquina que tiene el modem que conecta con la Internet. Incluso se pueden encontrar computadoras muy potentes y con software específicos que lo único que hacen es monitorizar las comunicaciones entre redes.

Quizá uno de los elementos más publicitados a la hora de establecer seguridad, sean estos elementos. Aunque deben ser uno de los sistemas a los que más se debe prestar atención, distan mucho de ser la solución final a los problemas de seguridad. De hecho, los cortafuegos no tienen nada que hacer contra técnicas como la Ingeniería Social.

Como puede observarse en el ***Diagrama 4***, el cortafuegos, sólo sirve de defensa perimetral de las redes, no defienden de ataques o errores provenientes del interior, como tampoco puede ofrecer protección una vez que el intruso lo traspasa.

Algunos cortafuegos aprovechan esta capacidad de que toda la información entrante y saliente debe pasar a través de ellos para proveer servicios de seguridad adicionales como la encriptación del tráfico de la red. Se entiende que si dos cortafuegos están conectados, ambos deben "hablar" el mismo método de encriptación-desencriptación para entablar la comunicación y brindar un mayor grado de seguridad a la red.

Enseguida se mencionara y explicara muy brevemente las formas más comunes de conectar y emplear un cortafuegos:

1.- Filtrado de Paquetes: Se utilizan ruteadores con filtros y reglas basadas en políticas de control de acceso. El ruteador es el encargado de filtrar los paquetes basados en cualquiera de los siguientes criterios:

1. Protocolos utilizados.
2. Dirección IP de origen y de destino.
3. Puerto TCP-UDP de origen y de destino.

Estos criterios permiten gran flexibilidad en el tratamiento del tráfico. Restringiendo las comunicaciones entre dos computadoras (mediante las direcciones IP) se permite determinar entre cuales máquinas la comunicación está permitida. El filtrado de paquetes mediante puertos y protocolos permite establecer que servicios estarán disponibles al usuario y por cuales puertos. Se puede permitir navegar en la Internet (puerto 80 abierto); pero no acceder a la transferencia de archivos vía FTP (puerto 21 cerrado).

Debido a su funcionamiento y estructura basada en el filtrado de direcciones y puertos este tipo de cortafuegos trabajan en los niveles de Transporte y de Red del Modelo OSI y están conectados a ambos perímetros (interior y exterior) de la red. Tienen la ventaja de ser económicos, tienen un alto nivel de desempeño y son transparentes para los usuarios conectados a la red. Sin embargo, presenta debilidades como:

1. No protege las capas superiores a nivel OSI.
2. Las necesidades aplicativas son difíciles de traducir como filtros de protocolos y puertos.
3. No son capaces de esconder la topología de redes privadas, por lo que exponen la red al mundo exterior.
4. Sus capacidades de auditoría suelen ser limitadas, al igual que su capacidad de registro de actividades.
5. No soportan políticas de seguridad complejas como autentificación de usuarios y control de accesos con horarios prefijados.

2.-Proxy-Gateways de Aplicaciones: Para evitar las debilidades asociadas al filtrado de paquetes, los desarrolladores crearon software de aplicación encargados de filtrar las conexiones. Estas aplicaciones son conocidas como Servidores Proxy y la máquina donde se ejecuta recibe el nombre de Gateway de Aplicación o Bastion Host. El Proxy, instalado sobre el Nodo Bastión, actúa de intermediario entre el cliente y el servidor real de la aplicación, siendo transparente a ambas partes. Cuando un usuario desea un servicio, lo hace a través del Proxy. Este, realiza el pedido al servidor real devuelve los resultados al cliente. Su función fue la de analizar el tráfico de red en busca de contenido que viole la seguridad de la misma ***(Diagrama 5)***.

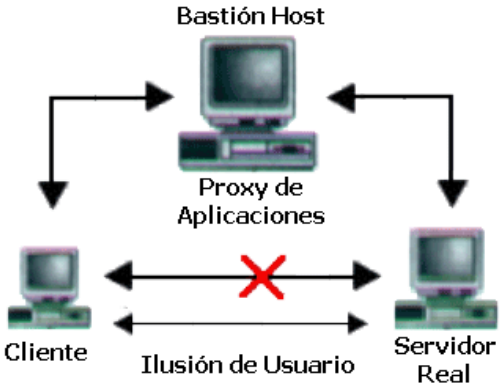

DIAGRAMA 5. CONECTIVIDAD DE UN CORTAFUEGO EN ESQUEMA PROXY-GATEWAYS.

3.- *Dual-Homed Host* (host de base doble) :Son dispositivos que están conectados a ambos perímetros (interior y exterior) y no dejan pasar paquetes IP (como sucede en el caso del Filtrado de Paquetes), por lo que se dice que actúan con el "*IP-Forwarding* desactivado". Un usuario interior que desee hacer uso de un servicio exterior, deberá conectarse primero al cortafuego, donde el Proxy atenderá su petición, y en función de la configuración impuesta en dicho cortafuego, se conectará al servicio exterior solicitado y hará de puente entre este y el usuario interior, véase el siguiente diagrama ***(Diagrama 6)***.

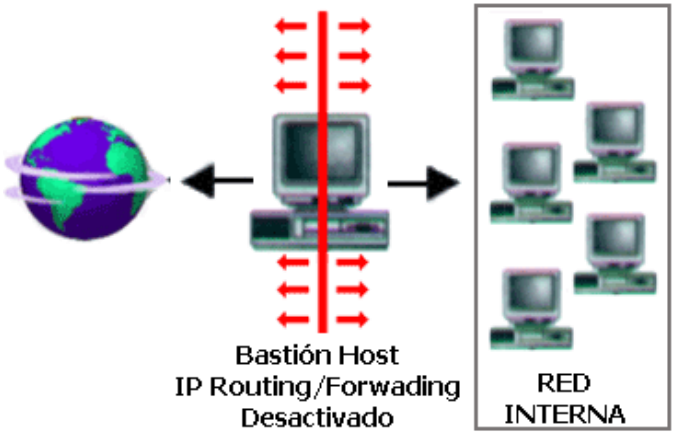

DIAGRAMA 6. CONECTIVIDAD DE UN CORTAFUEGO EN ESQUEMA DUAL-HOMED HOST.

Es decir que se utilizan dos conexiones. Una desde la máquina interior hasta el Firewall y el otro desde este hasta la máquina que albergue el servicio exterior.

4.- *Screened Host*: En este caso se combina un ruteador con un concentrador bastión y el principal nivel de seguridad proviene del filtrado de paquetes ***(Diagrama 7)***. En el bastión, el único sistema accesible desde el exterior, se ejecuta el Proxy de aplicaciones y en el estrangulador se filtran los paquetes considerados peligrosos y sólo se permite un número reducido de servicios.

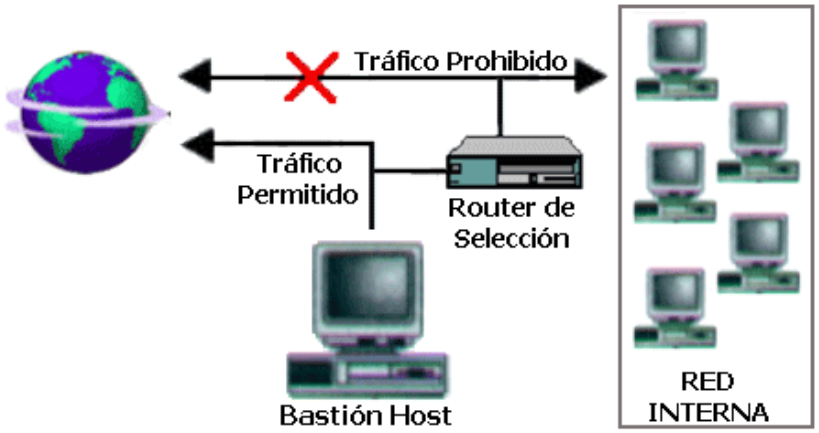

DIAGRAMA 7. CONECTIVIDAD DE UN CORTAFUEGO EN ESQUEMA SCREENED HOST.

5.- *Screened Subnet*: En este diseño se intenta aislar la máquina más atacada y vulnerable del cortafuego, el Nodo Bastión. Para ello se establece una Zona Desmilitarizada (DMZ) de forma tal que si un intruso accede a esta máquina no consiga el acceso total a la subred protegida. ***(Diagrama 8)***.

En este esquema se utilizan dos ruteadores: uno exterior y otro interior. El ruteador exterior tiene la misión de bloquear el tráfico no deseado en ambos sentidos: hacia la red interna y hacia la red externa. El ruteador interior hace lo mismo con la red interna y la DMZ (zona entre el Router externo y el interno).

Es posible definir varios niveles de DMZ agregando más ruteadores, pero destacando que las reglas aplicadas a cada uno deben ser distintas ya que en caso contrario los niveles se simplificarían a uno solo.

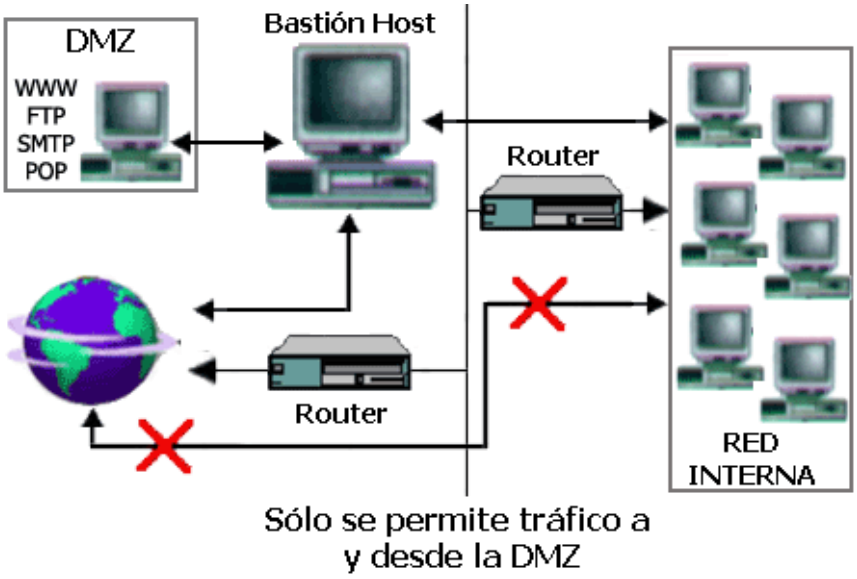

DIAGRAMA 8. CONECTIVIDAD DE UN CORTAFUEGO EN ESQUEMA SCREENED SUBNET.

Como puede apreciarse la Zona Desmilitarizada aísla físicamente los servicios internos, separándolos de los servicios públicos. Además, no existe una conexión directa entre la red interna y la externa.

6.- Inspección de Paquetes: Este tipo de cortafuegos se basa en el principio de que cada paquete que circula por la red es inspeccionado, así como también su procedencia y destino. Se aplican desde la capa de Red hasta la de Aplicaciones. Generalmente son instalados cuando se requiere seguridad sensible al contexto y en aplicaciones muy complejas.

7.-Cortafuegos Personales: Estos cortafuegos son aplicaciones disponibles para usuarios finales que desean conectarse a una red externa insegura y mantener su computadora a salvo de ataques regularmente en la Internet.

1.4 VPN (RED PRIVADA VIRTUAL).

Hace unos años no era tan necesario conectarse a la Internet por motivos de trabajo. Conforme ha ido pasando el tiempo las empresas han visto la necesidad de que las redes de área local (LAN) superen la barrera de lo local permitiendo la conectividad de su personal y oficinas en otros edificios, ciudades, comunidades autónomas e incluso países.

Desgraciadamente, en el otro lado de la balanza se encontraban las grandes inversiones que era necesario realizar tanto en hardware como en software y por supuesto, en servicios de telecomunicaciones que permitieran crear estas redes deservicio.

Afortunadamente con la aparición de Internet, las empresas, centros de formación, organizaciones de todo tipo e incluso usuarios particulares, tienen la posibilidad de crear una Red Privada Virtual (VPN) que permite, mediante una moderada inversión económica y utilizando la Internet, la conexión entre diferentes ubicaciones salvando la distancia entre ellas.

Las redes virtuales privadas utilizan protocolos especiales de seguridad que permiten obtener acceso a servicios de carácter privado, únicamente a personal autorizado, de una empresas, centros de formación, organizaciones, etcétera.; cuando un usuario se conecta vía Internet, la configuración de la red privada virtual le permite conectarse a la red privada del organismo con el que colabora y acceder a los recursos disponibles de la misma como si estuviera tranquilamente sentado en su oficina.

Tratando de explicar un poco más que es una VPN se puede definir como una red virtual que se crea dentro de otra red real, como puede ser la Internet.

Realmente una VPN no es más que una estructura de red corporativa implantada sobre una red de recursos de carácter público, pero que utiliza el mismo sistema de gestión y las mismas políticas de acceso que se usan en las redes privadas, al fin y al cabo no es más que la creación en una red pública de un entorno de carácter confidencial y privado, que permitirá trabajar al usuario como si estuviera en su misma red local.

En la mayoría de los casos, la red pública es la Internet, pero también puede ser una red con enlaces dedicados.

Desde el punto de vista del usuario que se conecta a ella, el funcionamiento de una VPN es similar al de cualquier red normal, aunque realmente para que el comportamiento se perciba como el mismo hay un gran número de elementos y factores que hacen esto posible.

La comunicación entre los dos extremos de la red privada a través de la red pública se hace estableciendo túneles virtuales entre esos dos puntos y usando sistemas de encriptación y autentificación que aseguren la confidencialidad e integridad de los datos transmitidos a través de esa red pública. Debido al uso de estas redes públicas, generalmente Internet, es necesario prestar especial atención a las cuestiones de seguridad para evitar accesos no deseados.

La tecnología de túneles (Tunneling) es un modo de envío de datos en el que se encapsula un tipo de paquetes de datos dentro del paquete de datos propio de algún protocolo de comunicaciones, y al llegar a su destino, el paquete original es desempaquetado volviendo así a su estado original.

En el traslado a través de la Internet, los paquetes viajan encriptados, por este motivo las técnicas de autenticación son esenciales para el correcto funcionamiento de las VPN, ya que se aseguran de que emisor y receptor que están intercambiando información lo hagan con el usuario o dispositivo correcto.

La autenticación en redes virtuales es similar al sistema de inicio de sesión a través de usuario y contraseña, pero se tienen necesidades mayores de aseguramiento de validación de identidades.

La mayoría de los sistemas de autenticación usados en VPN están basados en sistema de claves compartidas. La autenticación se realiza normalmente al inicio de una sesión, y luego, aleatoriamente, durante el transcurso de la sesión, para asegurar que no haya algún tercer participante que se haya podido entrometer en la conversación.

Todas las VPN usan algún tipo de tecnología de encriptación, que empaqueta los datos en un paquete seguro para su envío por la red pública. La encriptación hay que considerarla tan esencial como la autenticación, ya que

permite proteger los datos transportados de poder ser vistos y entendidos en el viaje de un extremo a otro de la conexión.

Existen dos tipos de técnicas de encriptación que se usan en las VPN:

- **Encriptación con clave secreta:** Se utiliza una contraseña secreta conocida por todos los participantes que van a hacer uso de la información encriptada. La contraseña se utiliza tanto para encriptar como para desencriptar la información. Este tipo de sistema tiene el problema que, al ser compartida por todos los participantes debe mantenerse secreta, al ser revelada, tiene que ser cambiada y distribuida a los participantes, lo que puede crear problemas de seguridad.

- **Encriptación de clave pública:** Implica la utilización de dos claves, una pública y una secreta. La primera es enviada a los demás participantes. Al encriptar, se usa la clave privada propia y la clave pública del otro participante de la conversación. Al recibir la información, ésta es desencriptada usando su propia clave privada y la pública del generador de la información. La gran desventaja de este tipo de encriptación es que resulta ser más lenta que la de clave secreta.

En las redes virtuales, la encriptación debe ser realizada en tiempo real, de esta manera, los flujos de información encriptada a través de una red lo son utilizando encriptación de clave secreta con claves que son válidas únicamente para la sesión usada en ese momento.

1.6 Definición del concepto "falso-positivo" en la seguridad de una red.

Un falso positivo para un antivirus, se refiere a la detección de un archivo como virus (o alguna otra clase de malware) por parte de un antivirus, cuando en realidad no es ningún virus o malware. Estos errores suelen ser pocos, aunque dependiendo de algunos factores (como la heurística) puede aumentar la probabilidad de la aparición de estos.

Este concepto cobra una mayor relevancia cuando se esta trabajando con cortafuegos pues se debe de recordar que con este medio se puede permitir o denegar la ejecución de procesos y aplicaciones en especifico, un claro ejemplo es sí se tiene bloqueada la aplicación de Messenger que viene preinstalada en los sistemas operativos Windows, el usuario tratará de iniciar su sesión, al momento de enviar la petición el cortafuego bloqueara el puerto y con

esto no permitirá que se establezca el inicio de sesión, el usuario cerrara la aplicación pero en los parámetros de configuración que están establecidos por default la aplicación se minimizara a la bandeja de tareas y cada determinado tiempo tratara de iniciar sesión enviando peticiones y a su vez el cortafuego bloqueándolas, estas peticiones se verán reflejadas en el cortafuego cayendo en un falso-positivo ***(Figura 7)***.

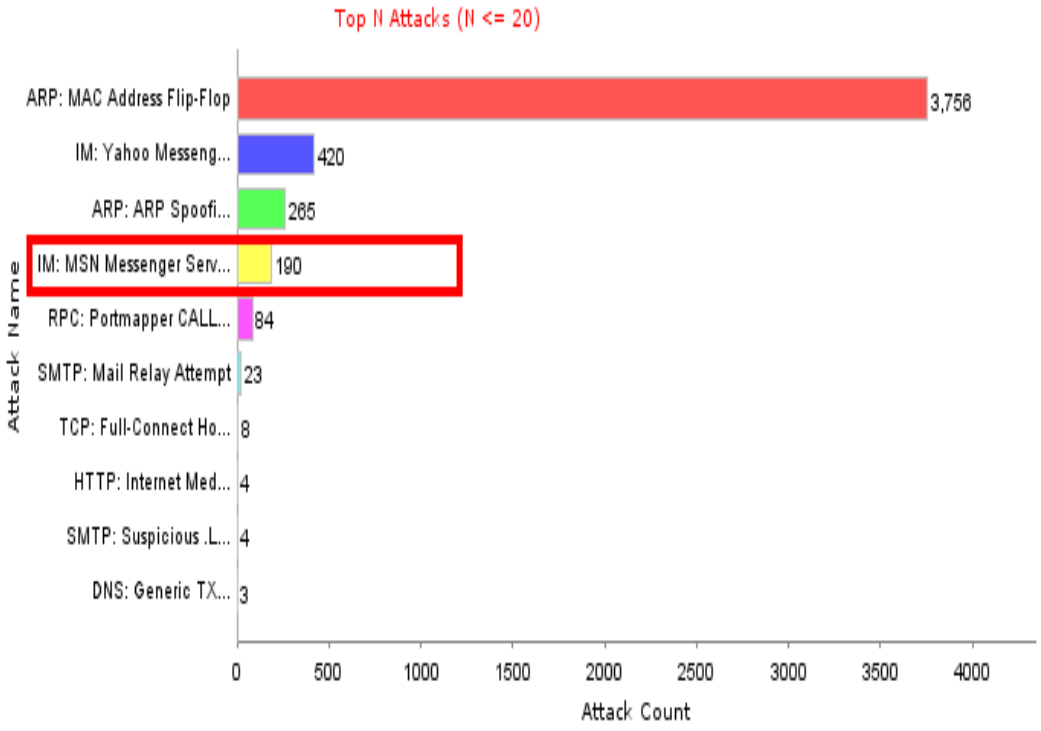

FIGURA 7. LOG GRAFICO DE OPERACIÓN DE UN FIREWALL JUNIPER.

En la anterior imagen se aprecia el registro de sesiones de Messenger, pero no fueron establecidas ya que el firewall bloqueo las peticiones, falso-positivo.

CAPÍTULO II

COMUNICACIÓN DE LAS REDES

2.1 CLASIFICACIÓN DE LAS REDES.

Las redes de computadoras son clasificadas principalmente en base al tamaño que tienen, y la distribución lógica que manifiestan en su operación, principalmente se agrupan en tres grandes grupos LAN, MAN y WAN, aunque en la actualidad y con el desarrollo de las nuevas tecnologías hay quienes aseguran que estos grupos están creciendo

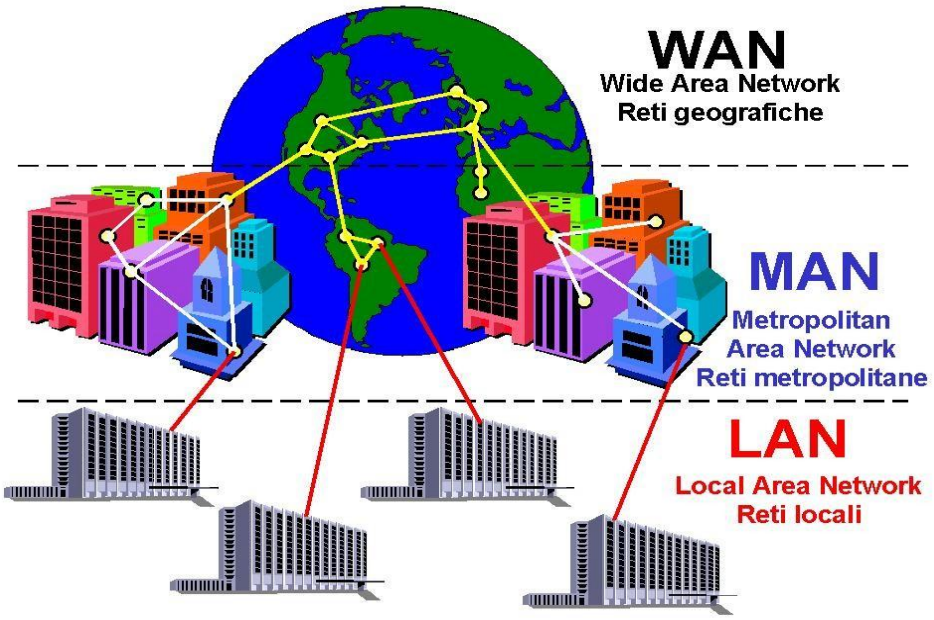

DIAGRAMA 9. LOS TRES PRINCIPALES GRUPOS DE REDES QUE EXISTEN.

1.- LAN (redes de área local): Este tipo de redes llevan mensajes a velocidades relativamente grandes entre computadoras conectadas a un único medio de comunicación como:

- Cable de par trenzado.
- Un cable coaxial.
- Fibra Óptica

Un segmento es una sección de cable que da servicio y que puede tener varias computadoras conectadas, el ancho de banda del mismo se reparte entre dichas computadoras.

Las redes de área local mayores están compuestas por varios segmentos interconectados por conmutadores (switches) o concentradores (hubs). El ancho de banda total del sistema es grande y la latencia pequeña, salvo cuando el tráfico es muy alto.

En los años 70's se han desarrollado varias tecnologías de redes de área local, destacándose Ethernet como tecnología dominante para las redes de área amplia; en lo que respecta a la distribución lógica de estas redes, regularmente hacen referencia a las comunicaciones que se dan dentro del mismo lugar físico en donde se encuentran los equipos, no se interconectan lugares ajenos a donde se encuentran trabajando.

2.- MAN (redes de área metropolitana): Se basan en el gran ancho de banda de los cableados de cobre y fibra óptica recientemente instalados para la transmisión de videos, voz, y otro tipo de datos. Varias han sido las tecnologías utilizadas para implementar el encaminamiento en las redes LAN, desde Ethernet hasta ATM. IEEE ha publicado la especificación 802.6[IEEE 1994], diseñado expresamente para satisfacer las necesidades de las redes WAN.

Las conexiones de línea de suscripción digital ,DLS(digital subscribe line) y los MODEM de cable son un ejemplo de esto. DSL utiliza generalmente conmutadores digitales sobre par trenzado a velocidades entre 0.25 y 6.0 Mbps; la utilización de este par trenzado para las conexiones limita la distancia al conmutador a 1.5 kilómetros . una conexión de MODEM por cable utiliza una señalización análoga sobre el cable coaxial de televisión para conseguir velocidades de 1.5 Mbps con un alcance superior que DSL.

En lo referente a la distribución lógica de estas redes, pueden definirse como la comunicación existente entre diferentes lugares dentro de una ciudad, es decir la conexión de los edificios que están a las orillas de una misma ciudad formarían una red MAN.

3.- WAN (redes de área extensa): Estas redes pueden llevar mensajes entre nodos que están a menudo en diferentes organizaciones y quizás separadas por grandes distancias incluso puede hablarse de continentes, pero a una velocidad menor que las redes LAN. El medio de comunicación esta compuesto por un conjunto de circuitos, equipos de computo, y equipos de comunicación dedicados llamados rotures o en caminadores.

Esto gestiona la red de comunicaciones y encaminan mensajes o paquetes hacia su destino. En la mayoría de las redes se produce un retardo en cada punto de la ruta a causa de las operaciones de encaminamiento, por lo que la latencia total de la transmisión de un mensaje depende de la ruta seguida y de

la carga de trafico en los distintos segmentos que atraviese. La velocidad de las señales electrónicas en la mayoría de los medios es cercana a la velocidad de la luz, y esto impone un límite inferior a la latencia de las transmisiones para las transmisiones de larga distancia.

4.- REDES INALÁMBRICAS: La conexión de los dispositivos portátiles y de mano necesitan redes de comunicaciones inalámbricas(wireless networks). Algunos de ellos son la IEEE802.11(wave LAN) son verdaderas redes LAN inalámbricas (wireless local área networks; WLAN) diseñadas para ser utilizadas en vez de las redes LAN convencionales. También se encuentran las redes de area personal inalámbricas, incluida la red europea mediante el Sistema Global para Comunicaciones Moviles, GSM(global system for mobile communication). En los Estados Unidos , la mayoría de los teléfonos móviles están actualmente basados en la análoga red de radio celular AMPS, sobre la cual se encuentra la red digital de comunicaciones de Paquetes de Datos Digitales Celular, CDPD(Cellular Digital Packet Data).

Dado el restringido ancho de banda disponible y las otras limitaciones de los conjuntos de protocolos llamados Protocolos de Aplicación Inalámbrica WAP (Wireless Aplication Protocol), este tipo de redes dista mucho de ser una verdadera solución para problemas de comunicación.

2.2 DEFINICIÓN DE RED PUNTO A PUNTO.

Este tipo de redes usan muy frecuentemente el protocolo llamado PPP Protocolo Punto a Punto; le permite a una computadora establecer la comunicación con una red de datos remota y así convirtiéndose en un host o nodo de dicha red, esto le permitirá a dicho host tener la posibilidad de hacer uso de todos los servicios tal cual lo haría si esa computadora estuviese conectada a la Ethernet directamente en su red interna.

Lo que se requiere para realizar este tipo de conexión es tener disponible algún puerto de comunicación o serial en una computadora, un módem y una línea telefónica convencional que servirá como medio físico de transmisión de datos.

El protocolo PPP solamente establece la comunicación de transferencia de datos pero la computadora donde se está efectuando la comunicación requerirá hacer uso también del protocolo TCP/IP (Transport Control Protocol / Internet Protocol), el cual en muchos casos está relacionado directamente con el software de conexión de PPP. Por ejemplo en el caso de Windows si utilizamos algún software como el Trumnpet este estará actuando para establecer el enlace vía PPP y buscara establecer el protocolo TCP/IP ya que solicitara la dirección de internet (IP) para realizar su funcionamiento, grabándola temporalmente en el archivo winsock.dll

Una vez establecida la conexión se requerirá un software de comunicación, un software que interactué con la red de datos, es decir programas que conviertan la información de las aplicaciones de alto nivel en tramas que puedan viajar por la red; programas que controlen el flujo de las tramas de información, que verifiquen su arribo a la computadora de destino y controlen la cantidad de tramas que pueden ser enviadas a la red, tomando en cuenta el tráfico en ella, dispositivos electrónicos que transformen las tramas de información a señales eléctricas, electromagnéticas u ópticas que puedan viajar por algún medio físico determinado.

Los programas que permitan que una computadora interactúe con la red implantan lo que se denomina Protocolos, y éstos pueden catalogarse de acuerdo a su función específica en el mecanismo de comunicación

El protocolo PPP está definido dentro de la familia de protocolos denominados TCP/IP que es la utilizada en muchas redes locales y en toda la Internet. El PPP se ubica en los niveles bajos de la familia TCP/IP y permite que la computadora se comunique a la red utilizando líneas de comunicación seriales de baja velocidad.

Los programas que implantan el PPP en una computadora además de el protocolo mismo implantan las capas superiores de la familia TCP/IP necesarias para una interacción total con una red de datos, que a su vez también debe estar implantada con los protocolos TCP/IP.

En el caso de los dispositivos electrónicos de comunicación cuando se utiliza PPP, en su esquema original de trabajo indica que se requiere utilizar uno de los puertos seriales de la computadora, a la cual se conectara un módem que se encargara de convertir las señales digitales en señales que puedan viajar a través de la línea telefónica. Estas señales serán recibidas por otro módem que se encargara de convertirlas nuevamente a señales digitales que pueden ser procesadas dentro de una red de datos. Nótese que en este esquema original de trabajo la velocidad de transmisión de datos de la computadora utilizando PPP estará en función de la velocidad máxima del puerto serial de la computadora, las velocidades máximas de operación de los módems locales y remotos y de la calidad de líneas telefónicas.

Una vez que se ha establecido el PPP en la computadora, aunado a los programas relacionados (tales como telnet , ftp, e-mail, www), es posible:

DIAGRAMA 10. ESQUEMA ORIGINAL DE UNA COMUNICACIÓN PUNTO A PUNTO.

Cabe hacer mención que en la actualidad pueden intervenir más dispositivos para mejorar este esquema de comunicación el cual es bidireccional.

2.3 DEFINICIÓN DE UNA RED VÍA VPN.

Las redes de área local (LAN) son las redes internas de las organizaciones, es decir las conexiones entre los equipos de una organización particular. Estas redes se conectan cada vez con más frecuencia a Internet mediante equipos de interconexión. Muchas veces, las empresas necesitan comunicarse por Internet con filiales, clientes o incluso con el personal que puede estar alejado geográficamente.

Sin embargo, los datos transmitidos a través de Internet son mucho más vulnerables que cuando viajan por una red interna de la organización, ya que la ruta tomada no está definida por anticipado, lo que significa que los datos deben atravesar una infraestructura de red pública que pertenece a distintas entidades. Por esta razón, es posible que a lo largo del camino, un usuario no autorizado, intercepte los paquetes de información de la red o incluso secuestre la señal. Por lo tanto, la información confidencial de una organización o empresa no debe ser enviada bajo tales condiciones.

La primera solución para satisfacer esta necesidad de comunicación segura implica conectar redes remotas mediante líneas dedicadas haciendo uso de enlaces punto a punto. Sin embargo, como la mayoría de las compañías no pueden conectar dos redes de área local remotas con una línea dedicada, a veces es necesario usar Internet como medio de transmisión.

Una buena solución consiste en utilizar Internet como medio de transmisión con un protocolo de túnel, que significa que los datos se encapsulan antes de ser enviados de manera cifrada. El término Red privada virtual (abreviado VPN) se utiliza para hacer referencia a la red creada artificialmente de esta manera.
Se dice que esta red es virtual porque conecta dos redes "físicas" (redes de área local) a través de una conexión poco fiable (Internet) y privada porque sólo los

equipos que pertenecen a una red de área local de uno de los lados de la VPN pueden "ver" los datos.

Por lo tanto, el sistema VPN brinda una conexión segura a un bajo costo, ya que todo lo que se necesita es el hardware de ambos lados. Sin embargo, no garantiza una calidad de servicio comparable con una línea dedicada, ya que la red física es pública y por lo tanto no está garantizada.

La palabra "túnel" se usa para simbolizar el hecho de que los datos estén cifrados desde el momento que entran a la VPN hasta que salen de ella y, por lo tanto, son incomprensibles para cualquiera que no se encuentre en uno de los extremos de la VPN, como si los datos viajaran a través de un túnel. En una VPN de dos equipos, el cliente de VPN es la parte que cifra y descifra los datos del lado del usuario y el servidor VPN (comúnmente llamado servidor de acceso remoto) es el elemento que descifra los datos del lado de la organización.

De esta manera, cuando un usuario necesita acceder a la red privada virtual, su solicitud se transmite sin cifrar al sistema de pasarela, que se conecta con la red remota mediante la infraestructura de red pública como intermediaria (Internet); luego transmite la solicitud de manera cifrada. El equipo remoto le proporciona los datos al servidor VPN en su red y éste envía la respuesta cifrada. Cuando el cliente de VPN del usuario recibe los datos, los descifra y finalmente los envía al usuario.

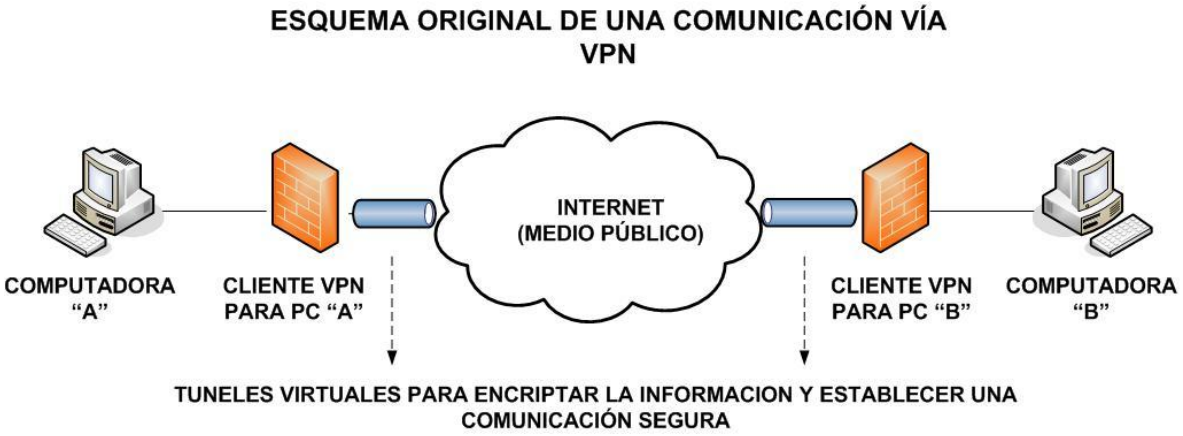

DIAGRAMA 11. ESQUEMA ORIGINAL DE UNA COMUNICACIÓN VÍA VPN.

Los principales protocolos de túnel son:

- **PPTP (Protocolo de túnel punto a punto)** es un protocolo de capa 2 desarrollado por Microsoft, 3Com, Ascend, US Robotics y ECI Telematics.
- **L2F (Reenvío de capa dos)** es un protocolo de capa 2 desarrollado por Cisco, Northern Telecom y Shiva. Actualmente es casi obsoleto.
- **L2TP (Protocolo de túnel de capa dos)**, incluye todas las características de PPTP y L2F. Es un protocolo de capa 2 basado en PPP.

- **IPSec** es un protocolo de capa 3 creado por el IETF que puede enviar datos cifrados para redes IP, este protocolo se basa en tres módulos:

  1ro. Encabezado de autenticación IP (AH), que incluye integridad, autenticación y protección contra ataques de REPLAY a los paquetes.

  2do. Carga útil de seguridad encapsulada (ESP), que define el cifrado del paquete. ESP brinda privacidad, integridad, autenticación y protección contra ataques de REPLAY.

  3ro. Asociación de seguridad (SA) que define configuraciones de seguridad e intercambio clave. Las SA incluyen toda la información acerca de cómo procesar paquetes IP (los protocolos AH y/o ESP, el modo de transporte o túnel, los algoritmos de seguridad utilizados por los protocolos, las claves utilizadas, etc.). El intercambio clave se realiza manualmente o con el protocolo de intercambio IKE (en la mayoría de los casos), lo que permite que ambas partes se escuchen entre sí.

2.3.1 FASES NECESARIAS PARA LA IMPLEMENTACIÓN DE UNA VPN.

Ahora hablaré de cómo configurar un firewall PIX (equipo que levantara el túnel en la VPN) usando el soporte de claves precompartidas para IPSec, entre las principales tareas se tiene:

- Tarea1: Preparación para IPSec.
- Tarea 2: Configuración de IKE.
- Tarea 3: Configuración de IPSec.
- Tarea 4: Comprobación y verificación de la configuración de la VPN.

Tarea 1: Preparación para IPSec:

Poner en marcha satisfactoriamente una red basada en IPSec requiere una preparación previa antes de comenzar la configuración de los firewalls PIX individualmente. Dentro de esta planificación que se menciona habrá que considerar los siguientes pasos:

- **Paso 1: Determinación de la norma IKE (fase uno del IKE).** Se determinan las normas IKE entre las dos redes, esto se refiere a identificar claramente el número de firewalls PIX o bien equipos que soportarán el IPSec que intervendrán directamente al momento de establecerse la comunicación entre las redes.

- **Paso 2: Determinación de la norma IPSec (fase dos del IKE).** En este paso se debe de acordar los procesos a los cuales se estará permitido recurrir en la comunicación de las redes, como puede ser un simple ping, Telnet, o un ftp; de esta forma las dos redes deberán de habilitar los procesos para que su operación se pueda llevar a cabo.

- **Paso 3: Verificación de la configuración actual.** Accediendo al firewall PIX se puede hacer uso de la gama de comandos *show* para verificar la configuración actual, entre los parámetros más importantes están los mapas, políticas y modo de encriptación.

- **Paso 4: Asegurarse de que la red funciona sin cifrado.** En este punto se debe de verificar que existe conectividad entre los firewalls PIX, para realizar esta prueba basta con hacer uso del comando *ping* en MS-DOS.

- **Paso 5: Asegurarse de que las listas de acceso son compatibles con IPSec.** Aquí ya estamos seguros de que la comunicación entre los firewalls PIX existe, ahora verificaremos los equipos host, switchs y ruteadores que estén involucrados dentro del enlace de comunicación.

Tarea 2: Configuración del IKE:

La siguiente tarea en la configuración del firewall PIX consiste en configurar los parámetros del IKE, esto se logra siguiendo los siguientes pasos:

- **Paso 1:** Habilitación o deshabilitación del IKE con el comando *isakmp enable.*

- **Paso 2:** Creación de normas IKE con el comando *isakmp policy*, aquí se definirán claramente las políticas de seguridad del firewall, tanto interna como externamente en lo que se conocen como las zonas “trust & untrust”.

- **Paso 3:** Configuración de las claves precompartidas con el comando *isakmp key*, en este punto le indicaremos al firewall con quién se comunicará y se establecerán las contraseñas, direcciones IP o bien llaves públicas y privadas de las cuales hará uso, dependiendo lo que se desee.

- **Paso 4:** Verificación de la configuración del IKE con el comando show isakmp [policy].

Tarea 3: Configuración de IPESec:

El primer paso para realizar la configuración del IPSec consiste en configurar las listas de acceso de cifrado donde se indicará el tráfico y el flujo que se analizará, para ello se hará uso del comando *acces-list* el cual tiene la siguiente sintaxis:

acces-list *nombre-lista-acceso* **[deny | permit]** protocolo origen *máscara de red-origen [operador puerto [puerto]]* destino *máscara de red-destino [operador puerto [puerto]]*

El cómo trabaja cada campo se muestra enseguida:

→ nombre-lista-acceso: Nombre o número de la lista de acceso que se está configurando, puede decirse que es asignar un nombre al enlace.

→ deny: Indica que no habrá revisión del IPSec para ningún paquete de información.

→ permit: Indica que habrá revisión del IPSec para los paquetes de información.

→ protocolo: Se indicará el número o nombre del protocolo IP, entre las opciones se encuentra icmp, ip, tcp o udp, para éste enlace de comunicación se usará IP.

→ origen: Dirección IP desde donde el paquete está siendo enviado.

→ destino: Dirección IP de la interfaz del PIX que recibe las tramas de información.

→ máscara de red-origen: Se ingresa la máscara de red del equipo que está enviando las tramas de información.

→ máscara de red-destino: Se ingresa la máscara de red del equipo que está recibiendo las tramas de información.

→ operador: Este campo es opcional y lo que hace es comparar los puertos de origen y destino, los operadores válidos son: it (menor que), gt (mayor que), eq (igual), neq (no igual), all (todos) y range (rango). En la configuración que se establecerá se usará la opción all, esto ayudará cuando en operación se llegue a saturar o fallar el puerto, sólo basta con cambiarse de puerto y la VPN vuelve a la normalidad.

→ puerto: Son los servicios IP permitidos basándose en el protocolo TCP o UDP.

Tarea 4: Comprobación y verificación de la configuración de la VPN:

En la siguiente lista está la descripción de alguno de los comandos con los cuales podemos verificar el estado de configuración de la VPN:

→ *show acces-list* : Se utiliza para verificar que las listas de acceso de cifrado seleccionan el tráfico deseado.

→ *show crypto* : Muestra el algoritmo empleado en la encriptación de las políticas definidas.

→ *show isakmp* : Muestra la configuración de la clave precompartida.

→ *show crypto ipsec* : Muestra los parámetros del IPSec así como la configuración de las listas de acceso.

Ahora bien, el principal de estos comandos y con el cual podemos verificar el correcto estado de operación de la VPN es *debug crypto isakmp*, una vez ejecutado este comando se deberán de recibir las leyendas:

→ ! El IKE ha negociado satisfactoriamente una coincidencia de norma IKE.

→ ! El IKE ha autenticado el igual IPSec.

→ ! El modo principal IKE está completo; return status is IKMP_NO_ERROR.

2.4 IMPORTANCIA DE LAS REDES.

El organismo público Telecomunicaciones de México descentralizado de la Secretaría de Comunicaciones y Transportes brinda en sus más de 1400 administraciones a lo largo de la republica mexicana servicios a la comunidad como:

- Giro telegráfico nacional e internacional.
- Servicio de Western Union.
- Cobranza por cuenta de terceros.
- Remesas de dinero para servicios bancarios.
- Pago de programas sociales.
- Fax público nacional e internacional.
- Internet.

Como se aprecia dentro de la gama de servicios que se brindan, los servicios financieros se encuentran presentes lo cual nos indica que Telecomunicaciones de México cuenta con una infraestructura optima para el trabajo de recursos financieros y por ende el agregar nuevos servicios a esta red, como pueden ser servicios financieros de banca básica. Hablando un poco más de su infraestructura se debe hacer mención que tiene una cobertura nacional, a través de dos subredes principalmente, la red Metropolitana y la red Telsat ***(Diagrama 12)***.

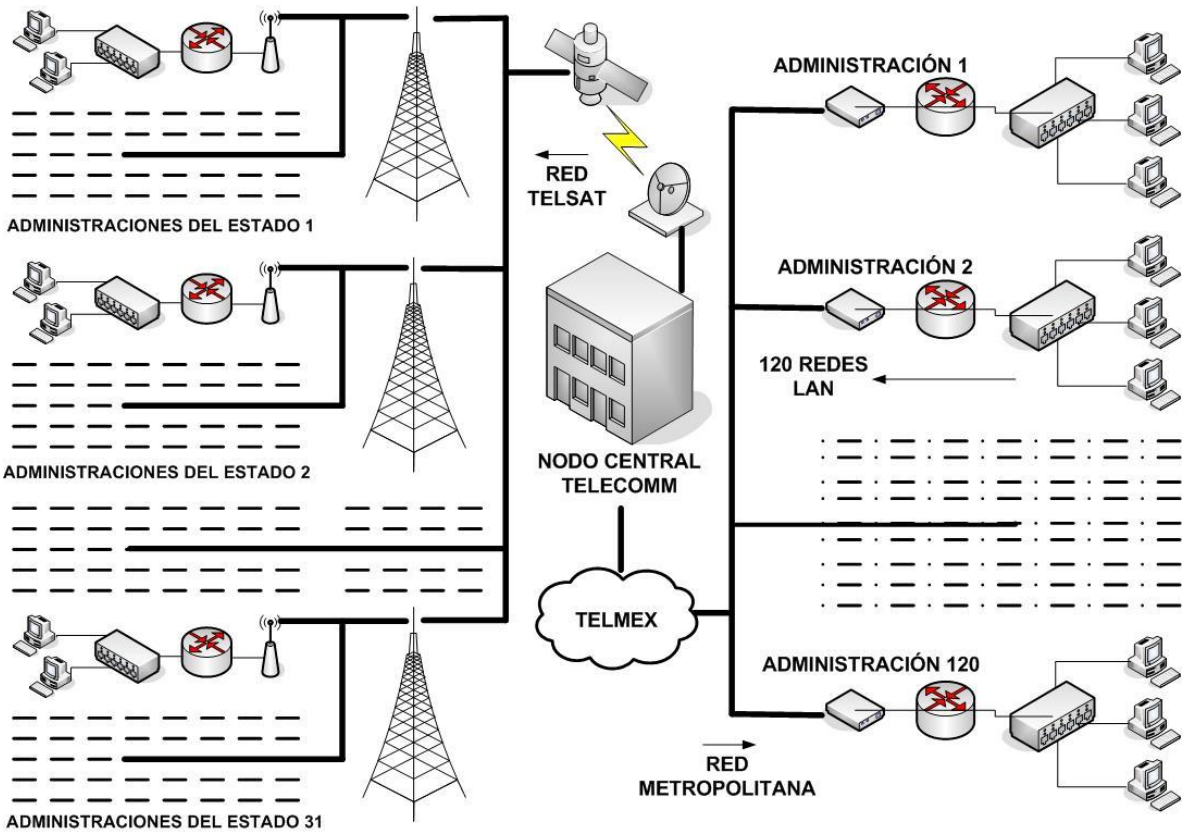

DIAGRAMA 12. REDES TELSAT Y METROPOLITANA DE TELECOMM.

La red metropolitana abarca el distrito federal y área metropolitana en donde Telmex es proveedor de carrier y la red Telsat que es una comunicación vía satélite para las administraciones que están en el interior de la republica mexicana.

Al tratarse Telecomunicaciones de México (TELECOMM) de un organismo público descentralizado este como meta principal no busca obtener un lucro o ganancias significantes al momento de brindar sus servicios, su principal objetivo es llevar toda su gama de servicios a las comunidades más apartadas a lo largo y ancho de la republica mexicana. Al establecer los enlaces de comunicación entre los nodos principales de las instituciones bancarias Inbursa – Banamex se conseguirá ampliar esta gama de servicios para la comunidad y se podrá acceder a "servicios financieros de banca básica" acercando ahora a la banca a esas comunidades más alejadas de nuestro país. Con esto se estimula un mayor flujo de comercio en ciertas zonas del país, además de dar mayor seguridad a los habitantes de una comunidad al momento de realizar operaciones bancarias. Al concluir los trabajos necesarios para el establecimiento de los enlaces de comunicación entre los tres nodos principales de las redes, Telecomm, Inbursa y Banamex se tendrá una infraestructura como la que se muestra a continuación ***(Diagrama 13)***:

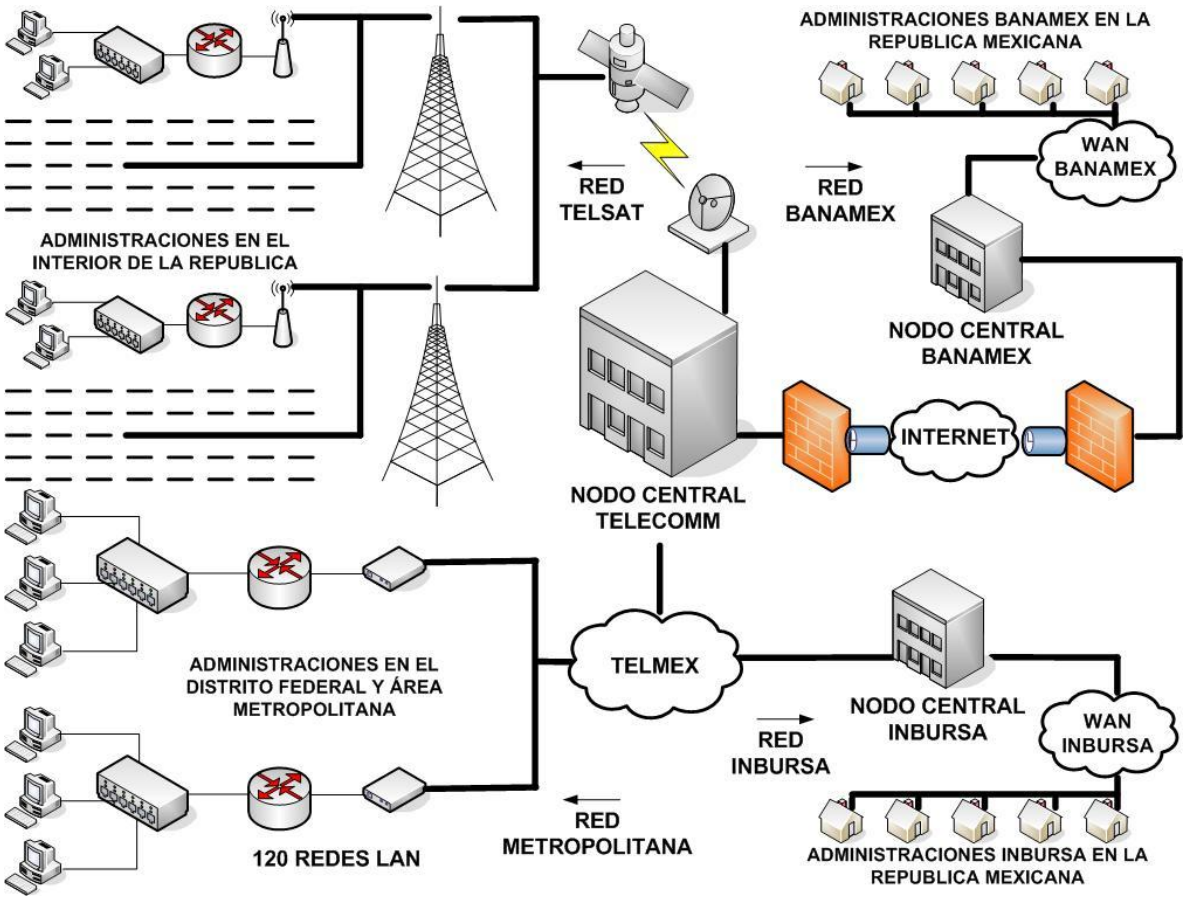

DIAGRAMA 13. INTERCONEXIÓN DE LOS NODOS DE COMUNICACIÓN TELECOMM, BANAMEX E INBURSA.

2.5 ESQUEMA DE COMUNICACIÓN DE UNA RED TIPO "PUNTO A PUNTO".

La comunicación de red tipo "punto a punto" se establecerá entre el nodo central de Telecomm y el nodo central de Inbursa, en este enlace se tendrá la participación de un tercero que será TELMEX el cual fungirá en un papel de proveedor de carrier para la comunicación ***(Diagrama 14)***.

Al estar presente un proveedor de carrier lo que se esta haciendo es contratar un canal de comunicación privado y exclusivo para una comunicación entre dos nodos, es por ello del nombre de comunicación "punto a punto" entre los nodos emisores y receptores solo se tiene a las centrales del proveedor de carrier por donde se retransmite la información.

A grandes rasgos el esquema de comunicación entre los nodos y el proveedor de carrier es el siguiente:

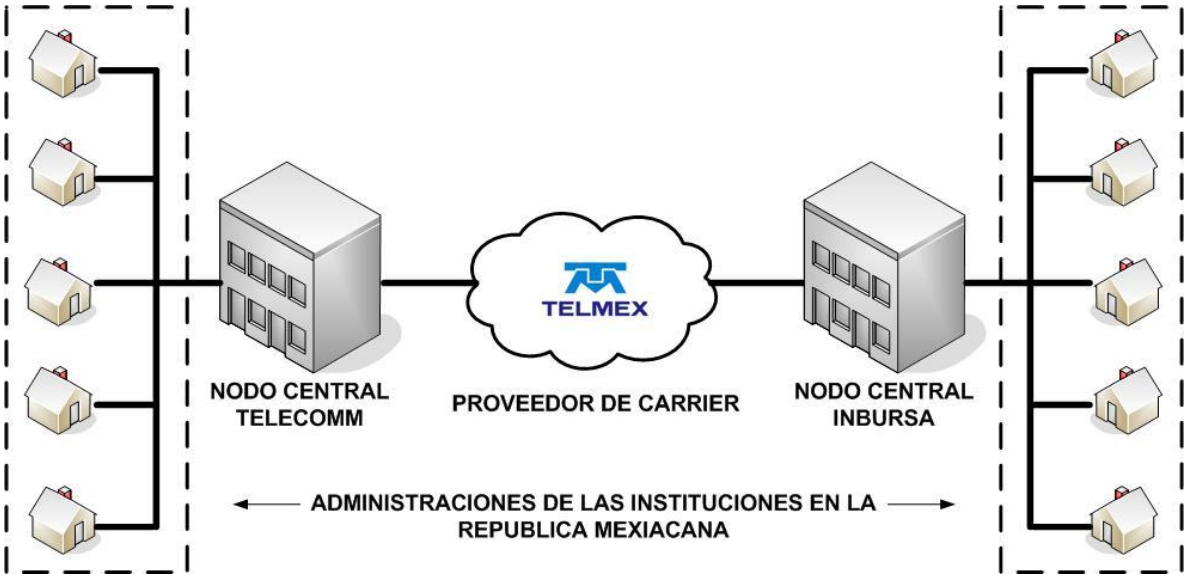

DIAGRAMA 14. ESQUEMA PARA CONECTAR EL NODO TELECOMM – INBURSA.

Lo que se puede apreciar en el ***Diagrama 14*** es un esquema de operación centralizado, el cual resulta practico cuando el número de usuarios remotos a ese nodo es elevado y su principal bondad radica en la administración de este tipo de redes con un número elevado de usuarios, además de que la implementación de las políticas de seguridad es teóricamente fácil de llevar a cabo.

Al momento de entrar en operación este esquema de comunicación entre estos nodos se va a trabajar de la siguiente manera; al llevarse a cabo una operación bancaria en alguna de las administraciones de Telecomm enviará la petición a través de algunas de las subredes de Telecomm hacia su nodo central en donde este a su vez retransmitirá dicha petición al nodo principal de Inbursa, para llevar a cabo esta retransmisión se usara al proveedor de carrier que es la empresa TELMEX, a través de un canal dedicado exclusivamente para los nodos de Telecomm y de Inbursa, una vez retransmitida esta petición llegara al nodo central de Inbursa en donde sea autenticada por los diferentes mecanismos que tengan implementados y la respuesta será enviada siguiendo el mismo camino que hasta el momento la petición a recorrido pero en sentido inverso, lo mismo sucederá cuando la petición se origine en alguna de las administraciones de Inbursa.

Ahora en el ***Diagrama 15*** se muestran los equipos que intervendrán para llevar a cabo la comunicación entre los nodos:

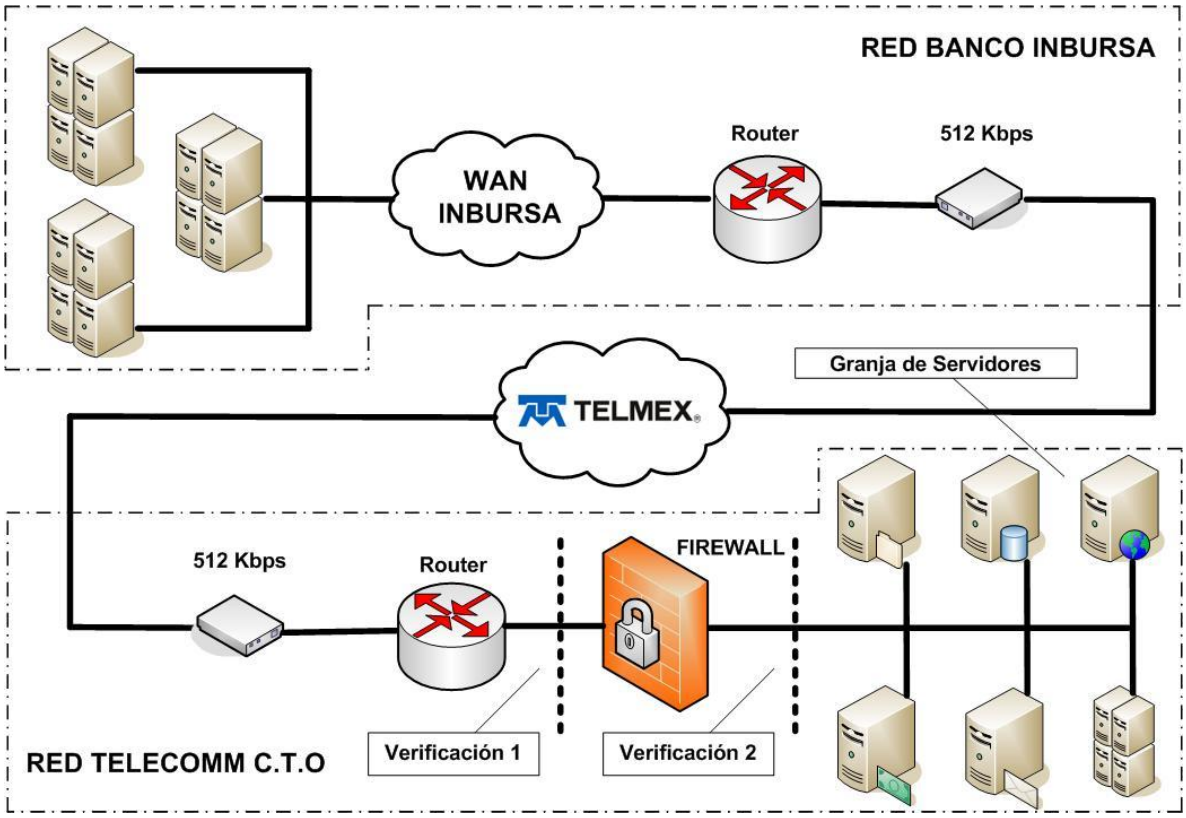

DIAGRAMA 15. CONEXIÓN DEL NODO TELECOMM – INBURSA.

En el anterior diagrama se aprecia en la parte superior el nodo de Inbursa, al centro Telmex como proveedor de carrier y en la parte inferior la red de nodo central de Telecomm.

Con este esquema de comunicación su pueden vislumbrar varios elementos en seguridad, tales como:

- Ruteo Estático.
- Uso de un enlace de comunicación dedicado.
- Autenticación y comprobación de la misma vía Firewall físico.
- Trabajo de usuarios dentro de la intranet con VLAN's.
- Acceso solo a servidores en específico.
- Acceso solo a servicios TCP permitidos.

El siguiente paso para continuar con la implementación de este enlace de comunicación así como la seguridad inherente al mismo es definir el direccionamiento IP que los equipos tendrán. Para ello se presenta el siguiente diagrama ***(Diagrama 16)*** con dicha propuesta:

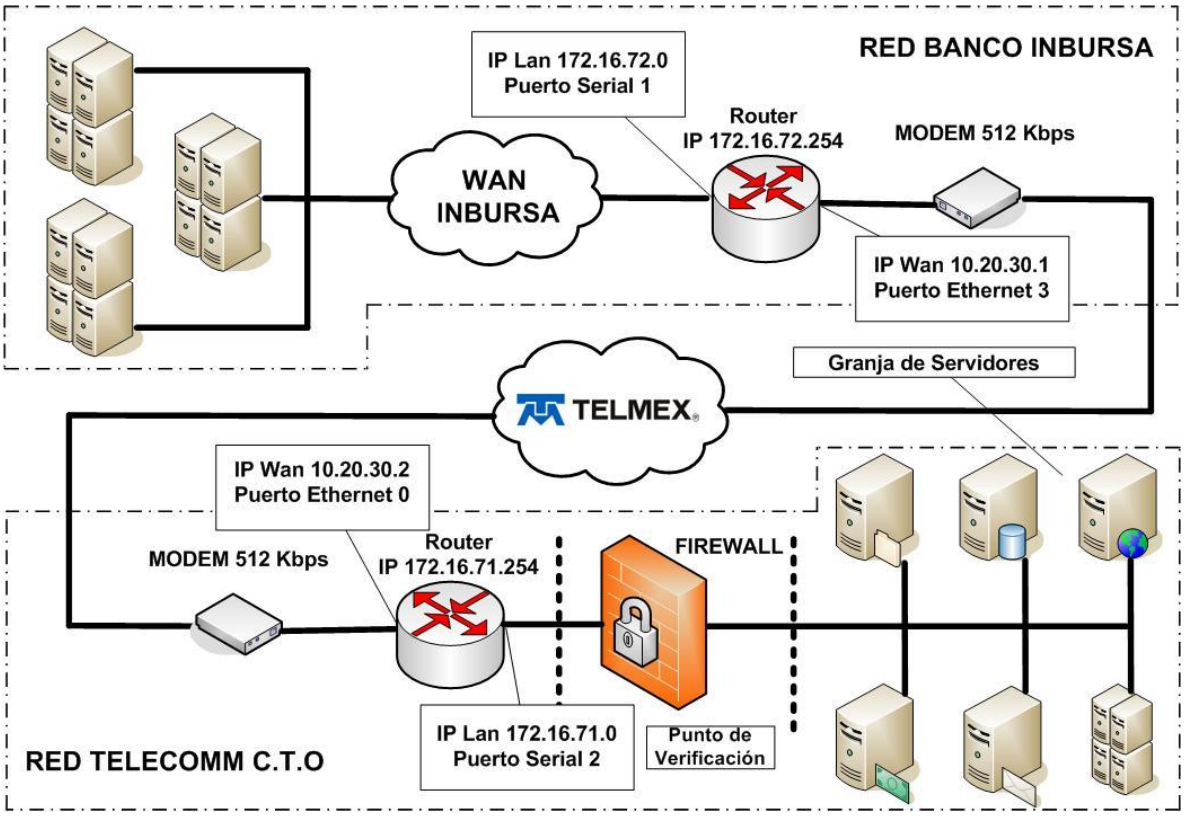

DIAGRAMA 16. CONEXIONDEL NODO TELECOMM – INBURSA CON DIRECCIONAMIENTO IP

En este momento se puede apreciar que se han asignado direcciones IP para los equipos ruteadores, tanto para el dispositivo como para una de sus interfaces de red LAN y WAN, esto en las redes de los nodos principales tanto de INBURSA como de TELECOMM.

El direccionamiento IP en los equipos ruteadores que ha sido asignado debe de cumplir con algunas reglas, ellas son:

- No utilizar direcciones IP públicas.
- La dirección IP de las redes WAN debe de ser continúa.
- La asignación de IP del ruteador debe de ser manual y no de forma dinámica como puede ser por medio de un servidor DHCP.

Una vez tomado en cuenta estos parámetros se procede a configurar los equipos ruteadores que serán los que propiamente permitirán la comunicación entre los nodos.

Ahora explicare brevemente el proceso de comunicación que se dará entre los nodos, para ello considérese la siguiente situación:

"*Un individuo necesita hacer un deposito en su cuenta bancaria de Inbursa, pero acude a una administración de Telecomm a realizar dicha operación*".

Tómese en cuenta que la comunicación se da en el sentido Telecomm a Inbursa, con esto los procesos son los siguientes:

1.- El empleado de Telecomm en la ventanilla de la administración solicita la operación a través del sistema, dicha petición viaja hasta el nodo central de Telecomm haciendo uso de una de sus subredes principales, red metropolitana (DF y Edo. De México) o red Telsat (Estados de la Republica Mexicana), esto dependiendo de la ubicación geográfica de la administración donde se está realizando la operación del cliente de Inbursa. Al enviar la solicitud a través de la administración de Telecomm se pasa por los filtros de seguridad implantados en la subred en la que se esté trabajando (**Filtro de seguridad 1**)

2.- Una vez que la petición llega al nodo central de Telecomm es procesada en la granja de servidores, en donde el servidor de producción retransmitirá la solicitud de depósito bancario hacia una cuenta de Inbursa al equipo Firewall de la marca Juniper que cuenta con funciones de ruteo. El equipo Firewall analizara el paquete recibido por el servidor, verificara IP origen, IP destino, permiso de ejecutar el proceso, puerto de comunicación que se está utilizando (**Filtro de seguridad 2**). Una vez comprobados estos parámetros y siendo correctos el equipo Firewall pasa la trama de paquetes al equipo ruteador.

3.- Cuando el equipo ruteador recibe el paquete de información acudirá a sus tablas de ruteo ya que en todo momento se está trabajando con ruteo estático (**Filtro de seguridad 3**), y enviará las tramas de información que fueron recibidas en su interface de red LAN 172.16.71.0 a su interfaz de red WAN 10.20.30.2 para que a través de la red WAN salga la petición hacia el servidor en producción de Inbursa.

4.- El equipo modem que aparece en el diagrama es el dispositivo que se encargara de retransmitir la información hasta el rack de la empresa TELMEX que recordemos es solamente nuestro proveedor de carrier.

5.- Después de viajar las tramas de información por todas las centrales del proveedor de carrier son entregadas a Inbursa en su nodo principal.

6.- Son descanalizadas y reenviadas a la interfaz Wan del router de Inbursa con el modem que esta en el lado de Inbursa.

7.- Recibida la petición en la interfaz Wan del router de inbursa este revisa su tabla de ruteo (**Filtro de seguridad 4**) y envía la petición a su interfaz Lan.

8.- Ya que la trama accedió a la red Lan de Inbursa se vuelve a revisar la tabla de ruteo donde se hará la comparación de IP origen con IP destino (**Filtro de seguridad 5**) para que entonces las tramas de información lleguen al servidor en producción. Inbursa no se ve obligado en ningún momento a revelar el funcionamiento o configuración de su red LAN pero obviamente en ella interactúan

al menos un equipo firewall que como en el caso de telecomm analizara los paquetes de información (**Filtro de seguridad 6**).

En los anteriores 8 puntos se resume el cómo funciona la comunicación entre estos dos nodos, se analizó una situación en donde Telecomm accede a Inbursa, en caso de que Inbursa quisiera acceder a Telecomm se seguiría el mismo proceso pero de forma inversa, iniciando en la ventanilla de una administración de Inbursa y concluyendo en el servidor en producción de Telecomm.

2.6 ESQUEMA DE COMUNICACIÓN DE UNA RED TIPO VPN.

En puntos anteriores de este trabajo ya se ha tocado el concepto VPN, recordemos que es una comunicación entre dos puntos en donde no se contrata un enlace dedicado de comunicación, se utiliza la nube de Internet como infraestructura para la comunicación. Al hacer uso de un medio público como internet se debe de tener especial atención en la seguridad del enlace. Se empleara una VPN para comunicar el nodo principal de Telecomm con el nodo principal de Banamex y con, para ello considérese el siguiente esquema de operación:

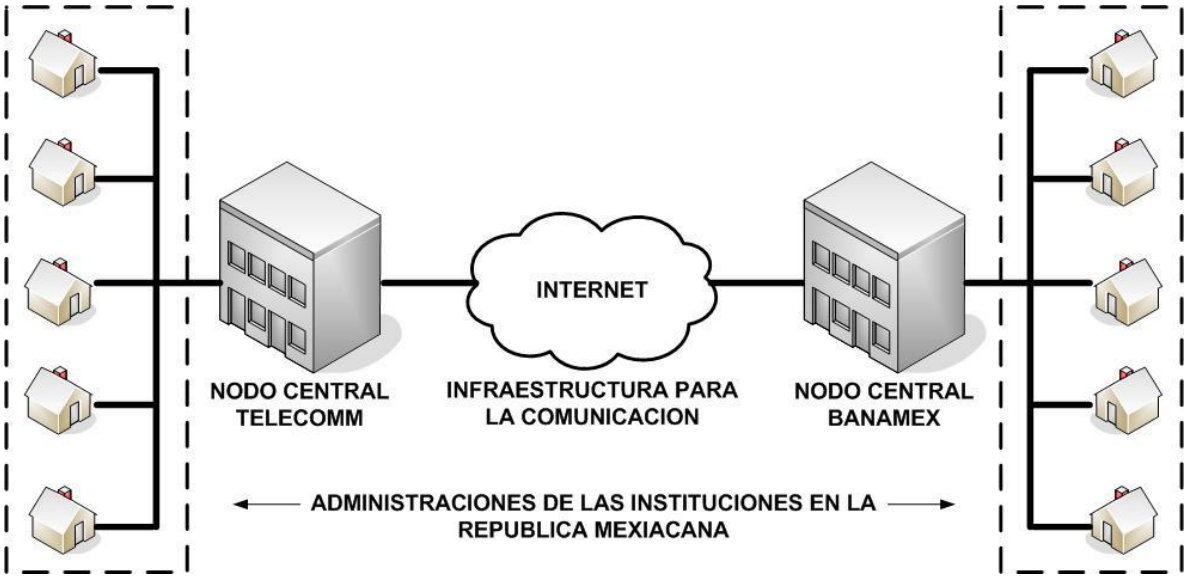

DIAGRAMA 17. ESQUEMA PARA CONECTAR EL NODO TELECOMM – BANAMEX.

Nótese que Banamex trabaja también bajo un esquema centralizado entre sus administraciones y nodo principal.

Para poder llevar a cabo la conectividad en este enlace los diferentes dispositivos que intervienen contarán con un direccionamiento IP estático y habrá que prestar especial atención a los equipos firewalls que serán los

encargados de levantar los procesos de la VPN para encriptar y desencriptar la información que viaje a través de ella.

A continuación ***(Diagrama 17)*** se presenta un diagrama con los equipos que se verán involucrados para realizar dicha comunicación:

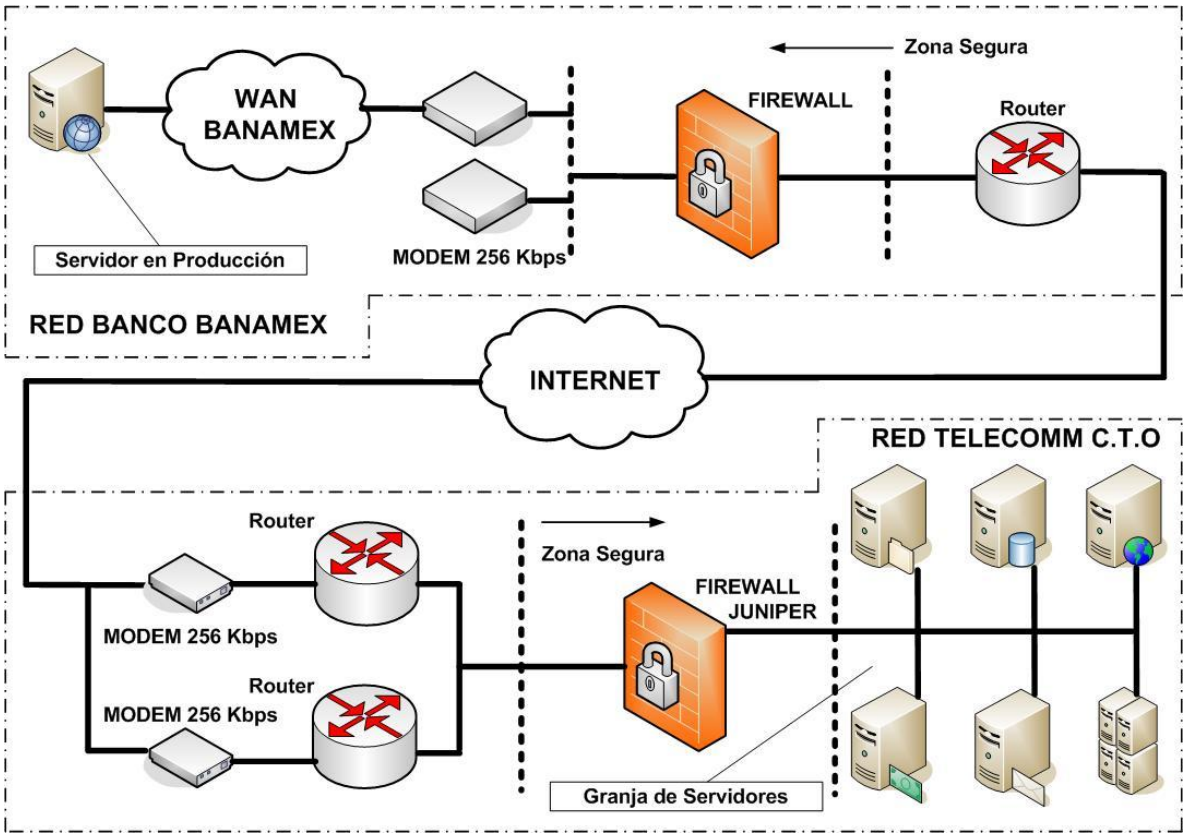

DIAGRAMA 18. CONEXIÓN DEL NODO TELECOMM – BANAMEX.

Ahora se explica brevemente el proceso de comunicación que se dará entre los nodos, para ello considérese la siguiente situación:

"*Un individuo necesita hacer un deposito en su cuenta bancaria de Banamex, pero acude a una administración de Telecomm a realizar dicha operación*".

Tómese en cuenta que la comunicación se da en el sentido Telecomm a Banamex, con esto los procesos son los siguientes:

1.- El empleado de Telecomm en la ventanilla de la administración solicita la operación a través del sistema, dicha petición viaja hasta el nodo central de Telecomm haciendo uso de una de sus subredes principales, red metropolitana (DF y Edo. De México) o red Telsat (Estados de la Republica Mexicana), esto dependiendo de la ubicación geográfica de la administración donde se está realizando la operación del cliente de Banamex. Al enviar la solicitud a través de la

administración de Telecomm se pasa por los filtros de seguridad implantados en la subred en la que se esté trabajando (**Filtro de seguridad 1**).

2.- Una vez recibida la petición en el servidor de producción de Telecomm enviara la información hasta el servidor que se encuentra en producción en Banamex, el primer paso es vía un ruteo estático (**Filtro de seguridad 2**) enviar la trama de información al firewall que llevara a cabo el proceso de la VPN.

3.- Una vez recibida la información en el firewall este agregara encabezados a la trama propios del proceso de comunicación de una VPN, estos encabezados son resultado del IKE, incluirá el proceso que desea llevarse a cabo (**Filtro de seguridad 3**) además de adjuntar la llave con la cua se autenticaran los equipos para poder comunicarse (**Filtro de seguridad 4**). Si al momento de realizar la transmisión de datos alguna persona capta los paquetes de información o parte de ellos no podrán saber su contenido ya que no cuentan con la clave para desencriptar dicha información, pues la llave que contiene dicha información reside únicamente en los equipos firewalls en su llave privada, la llave que viaja por Internet es una llave pública, para desencriptar la información de los paquetes es necesario hacer uso de las dos llaves (**Filtro de seguridad 5**).

4.- Una vez recibida la información y habiendo sido encriptada, vía rute estático será enviada al equipo ruteador (**Filtro de seguridad 6**) que haciendo uso de los equipos modems enviara la información a Internet, cabe mencionar que en el ***diagrama 18*** se muestran dos modems al igual que dos equipos ruteadores, estos equipos se encuentran trabajando en “alta disponibilidad” quiere decir que de encontrarse saturado uno de los canales de comunicación de forma automática pasa la información al otro equipo para que sea enviada a Internet, con esto se brinda una mayor fiabilidad al enlace hacia Internet (**Filtro de seguridad 7**), no debe de hacerse ningún cambio físico o lógico por que los dos equipos conocen la ruta que se debe de seguir. Debe de considerarse que al estar haciendo uso de Internet como medio de comunicación la IP a la cual se enviaran los paquetes es una IP pública, en este momento se deja de lado el direccionamiento IP privado.

5.- La información viaja através de la infraestructura de Internet haciendo uso del “túnel” de la VPN (**Filtro de seguridad 8**) este túnel virtual es realizado propiamente por los procesos del protocolo IPSec en donde agrego una cabecera denominada AH que lleva la información de la IP origen además de la trama denominada ESP que indica el tipo de cifrado que el paquete lleva, esta información es necesaria para el equipo receptor pues de otra manera no sabrá el tipo de algoritmo que debe de aplicar para desencriptar la información.

6.- Después de viajar la información por la infraestructura de Internet llega a la interfaz WAN del router de Banamex el cual debe de hacerse mención tiene una dirección de IP tipo pública pues de otra manera no podría encontrarse el destinatario en Internet. El equipo de ruteo canaliza por el camino asignado hacia las subredes de Banamex la trama de información con ruteo estático (**Filtro de**

seguridad 9) en este caso entregara las tramas al equipo Firewall para continuar con los procesos de la VPN.

7.- Una vez recibida la información encriptada en la interfaz WAN del firewall de Banamex se hara uso de las llave privada del IKE (**Filtro de seguridad 10**), al coincidir estas llaves entonces se verificara la cabecera AH para verificar la dirección IP del remitente (**Filtro de seguridad 11**) autenticando este aspecto desecha esa cabecera y procede a verificar ahora a la cabecera ESP la cuál indicara el tipo de cifrado que lleva el paquete y procederá a aplicar el algoritmo correspondiente para su desencriptacion (**Filtro de seguridad 12**), con esto la trama vuelve a su estado original que es al momento de generarse la petición del servicio y previo a entrar a la VPN, ahora el firewall analiza la trama como cualquier otro paquete de información y verifica que no se trate de código malicioso (**Filtro de seguridad 13**), una vez validado esto su interfaz LAN enviará vía ruteo estático la trama al equipo que Banamex tenga destinado para que este canalice la trama de información por el segmento de red correspondiente.

8.- Finalmente la petición es entregada al servidor de producción de Banamex para que este la procese.

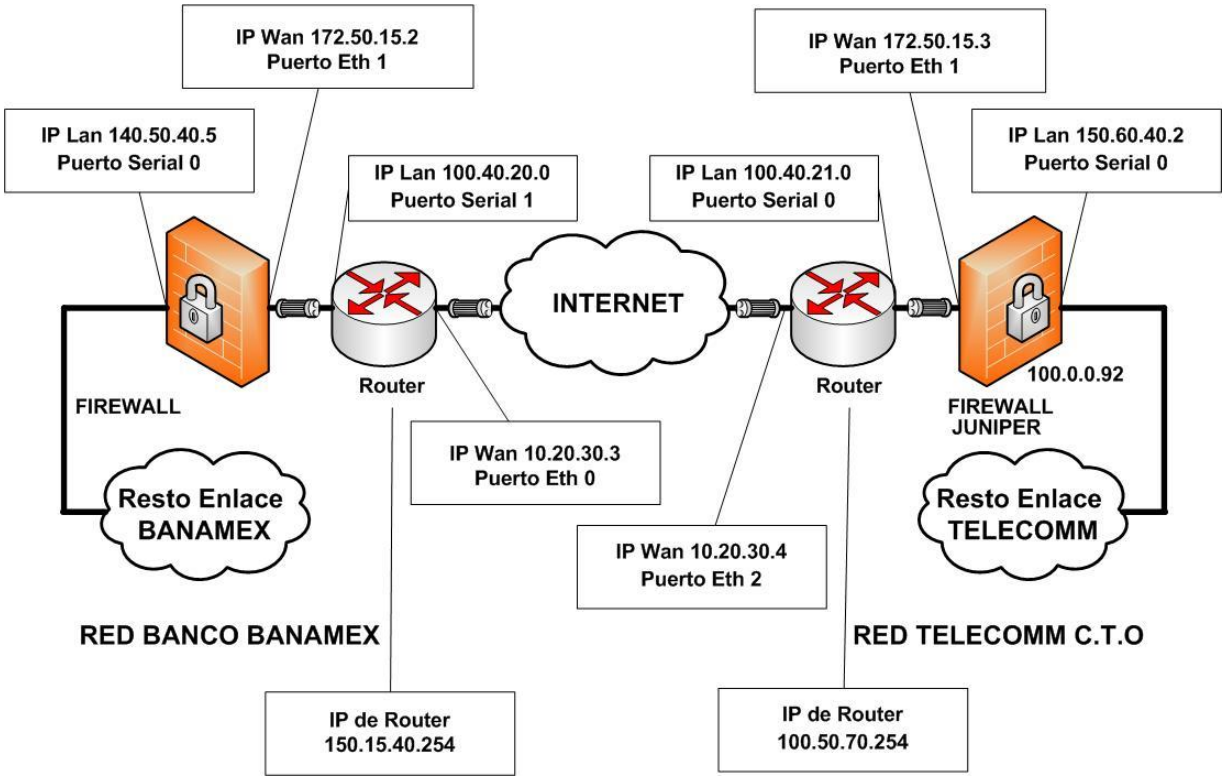

DIAGRAMA 19. CONEXIÓN DEL NODO TELECOMM – BANAMEX Y DIRECCIONAMIENTO IP.

Para concluir con el análisis de este enlace de comunicación en el ***Diagrama 19*** se muestra el direccionamiento IP que se utilizará para llevar a cabo la comunicación entre ambos nodos.

A destacar es el uso de direcciones IP públicas en la interfaz WAN de los equipos ruteadores de ambas redes.

Como ya sabemos los equipos de cómputo se comunican a través de Internet y las intranets donde residen mediante el protocolo IP (Protocolo de Internet). Este protocolo utiliza direcciones numéricas denominadas direcciones IP compuestas por cuatro números enteros (4 bytes) entre 0 y 255, y escritos en el formato xxx.xxx.xxx.xxx. Por ejemplo, 172.16.71.185 es una dirección IP en formato técnico. Los equipos de una red utilizan estas direcciones para comunicarse, de manera que cada equipo de la red tiene una dirección IP exclusiva.

Dicho número no se ha de confundir con la dirección MAC que es un número hexadecimal fijo que es asignado a la tarjeta o dispositivo de red por el fabricante, mientras que la dirección IP se puede cambiar.

Los sitios de Internet que por su naturaleza necesitan estar permanentemente conectados, generalmente tienen una dirección IP fija (comúnmente, IP fija o IP estática), es decir, no cambia con el tiempo. Los servidores de correo, DNS, FTP públicos, y servidores de páginas web necesariamente deben contar con una dirección IP fija o estática, ya que de esta forma se permite su localización en Internet.

A través de Internet, los equipos de cómputo se conectan entre sí mediante sus respectivas direcciones IP. Sin embargo, a los seres humanos nos es más cómodo utilizar otra notación más fácil de recordar y utilizar, como los nombres de dominio; la traducción entre unos y otros se resuelve mediante los servidores de nombres de dominio DNS, es por ello que se hace uso de IPs públicas en las interfaces WAN para acceder a las redes LAN de los nodos.

A lo largo de la descripción que se realizo en el proceso de comunicación a través de una VPN se muestran los diferentes filtros de seguridad que se aplican y podemos ver que no hay procesos en donde quede al margen la seguridad que esta por demás mencionar es de suma importancia y más cuando estamos utilizando un medio público como es la infraestructura de Internet.

Obviamente en este caso se reducen gastos pues es más caro contar con un canal dedicado por un proveedor de carrier pero en contra parte tenemos el gasto que se genera para implementar una VPN pues si bien es cierto que puede hacerse vía software haciendo uso de una aplicación cliente-servidor no se compara con el desempeño que se obtiene al habilitarla con hardware como fue en este caso, es aquí en donde se debe hacer el balance general costo – beneficio y hasta cierto punto hacernos la interrogante ¿Cuánto cuesta mi información?

CAPÍTULO III

DISPOSITIVOS DE COMUNICACIÓN QUE INTERVIENEN EN LOS ENLACES DE LAS REDES Y CONFIGURACIÓN DE LOS PARAMETROS DE SEGURIDAD.

3.1 RUTEADORES CISCO 4000

Los equipos ruteadores que serán empleados en los procesos de comunicación por parte de Telecomunicaciones de México (TELECOMM) serán de la marca CISCO y específicamente se habla de la familia 4000 y en algunos casos serán utilizados equipos más pequeños que serían de la familia 2500, estos últimos cuentan con las mismas funciones que la familia 4000 pero con una menor capacidad en el manejo de puertos Ethernet, que recordemos un puerto Ethernet es el equivalente al manejo de una red WAN.

La familia 4000 (***FIGURA 8***) nos ofrece las siguientes características:

- De uno a seis puertos Ethernet (número de puertos capaces de manejar redes WAN) dependiendo del modelo en específico.
- Un puerto fast-ethernet.
- Uno o dos puertos TOKEN RING.
- Un puerto multi-modo.
- Dos puertos seriales (número de puertos capaces de manejar redes LAN).
- Puertos para comunicaciones T1, E1,E3.

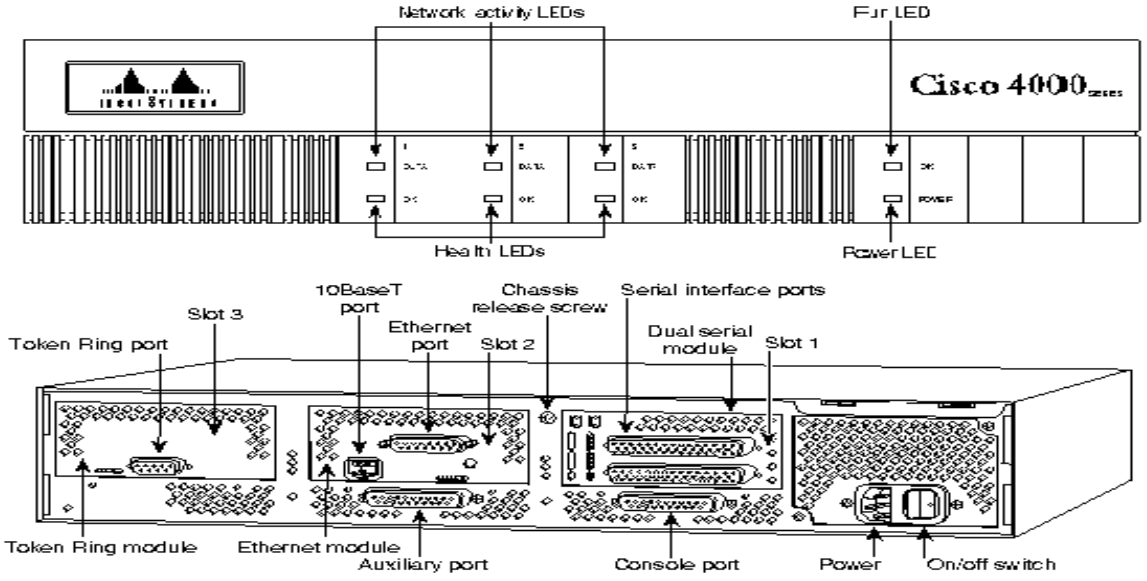

FIGURA 9. VISTA FRONTAL Y POSTERIOR DEL ROUTER CISCO FAMILIA 4000

3.1.1 CONFIGURACIÓN DE LAS TABLAS DE RUTEO ESTÁTICO.

Las tablas de ruteo estático recordemos que son las instrucciones que debe de seguir el equipo de ruteo para dirigir los paquetes de información dentro y fuera de una red. Consideremos el siguiente diagrama (***Diagrama 20***) que es un extracto del enlace de comunicación que se planteo entre Telecomm – Inbursa.

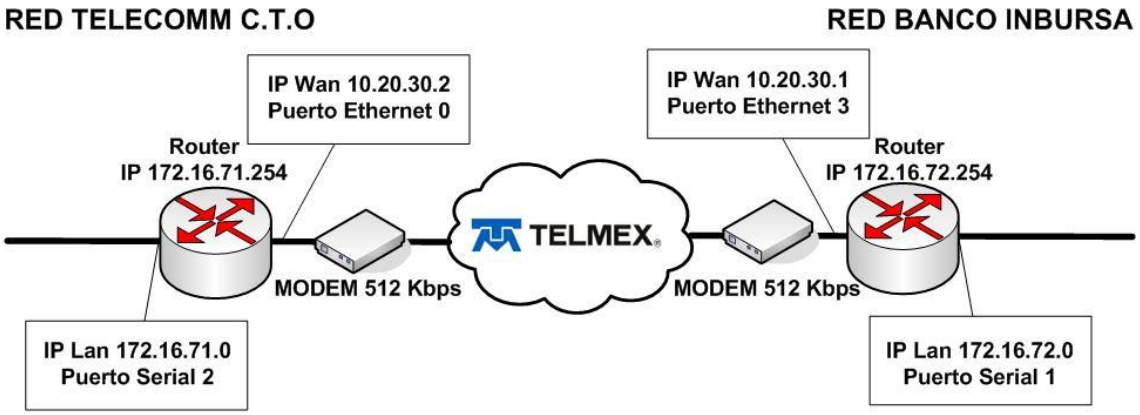

DIAGRAMA 20. RUTEADORES DEL ENLACE DE COMUNICACIÓN TELECOMM – INBURSA.

A continuación se mostraran los pasos necesarios para llevar a cabo la configuración de los equipos ruteadores, cabe señalar que las pantallas de configuración que se muestran serán el resultado de haber configurado el o los equipos por el lado del nodo de Telecomunicaciones de México, de emplear el mismo método que aquí se presente el nodo Inbursa obtendrá las mismas pantallas obviamente con los parámetros que a ellos les corresponden.

Iniciaremos sesión en una computadora con sistema operativo Windows, en este caso se utiliza la versión XP Professional Edition, desde la computadora conectaremos un cable que va desde la tarjeta de red hacia el puerto de consola que se encuentra ubicado en la parte posterior del equipo ruteador. Una vez realizada la conexión desde la computadora se procederá a abrir una terminal de MS-DOS (***Figura 10***) para que vía Telnet se comience a realizar la configuración del equipo ruteador.

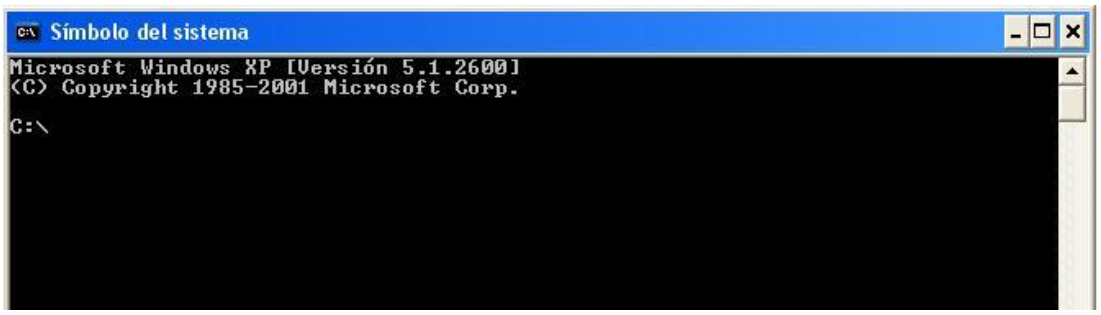

FIGURA 10. PANTALLA DE MS-DOS EN WINDOWS XP PROFESSIONAL EDITION.

A continuación se ingresara al equipo de ruteo estableciendo una sesión de trabajo para su configuración vía el protocolo telnet, una vez conectados nos deberemos de autenticar vía login y password (***Figura 11***) en el equipo.

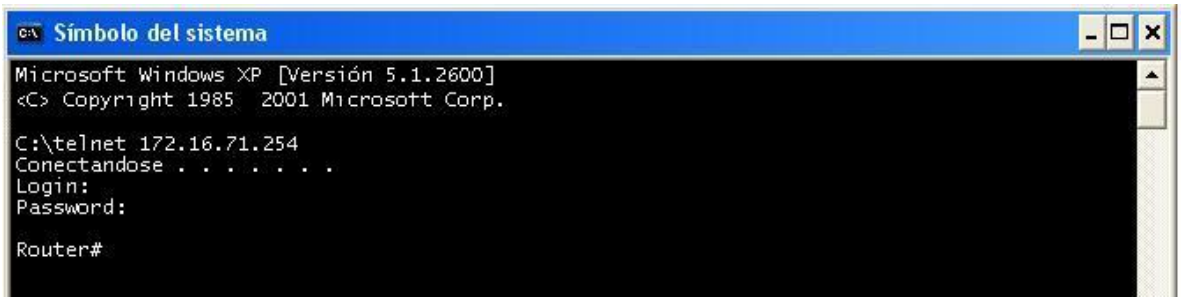

FIGURA 11. CONEXIÓN Y AUTENTICACIÓN CON EQUIPO RUTEADOR VIA TELNET.

Cuando se está configurado por primer vez un ruteador se recomienda iniciar con la configuración de la red WAN (***Figura 12***) que como se ha mencionado en el presente trabajo corresponde a uno de los puertos Ethernet del equipo, en base al ***Diagrama 20*** la WAN de Telecomm es la 10.20.30.2 tómese en cuenta que como regla las direcciones IP de las redes WAN que se van a comunicar deberán de ser continúas.

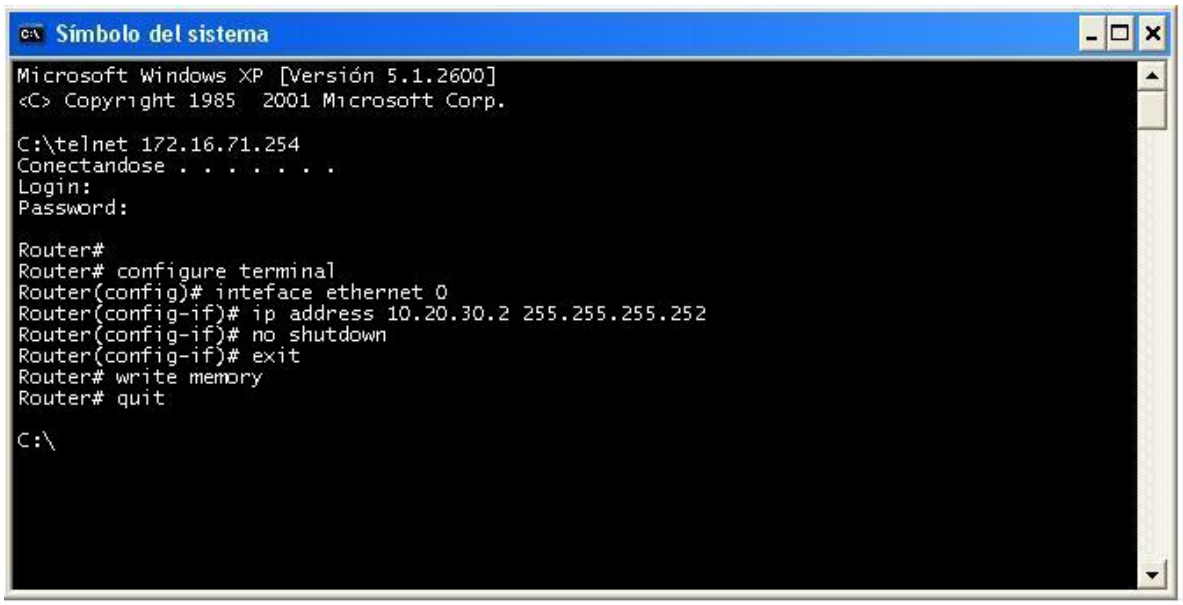

FIGURA 12. CONFIGURACION DE IP PARA RED WAN, PUERTO ETHERNET.

Como se puede apreciar en la anterior imagen se ha llevado a cano la configuración del puerto Ethernet del equipo ruteador, esto es el equivalente al establecer la dirección IP de la red WAN, se ha ingresado como máscara de red los valores 255.255.255.252 con esto estamos diciendo que solo tres direcciones IP tendrán el derecho de acceder al equipo, para su administración, operación y mantenimiento que requiera.

El siguiente paso para continuar con la configuración y establecimiento de las tablas de ruteo será el asignar la dirección IP de la red LAN con la que se trabajara y será asignada directamente esta dirección a un puerto Serial que son los que trabajan con las redes LAN. El procedimiento continúa siendo muy similar, nos conectaremos vía telnet al equipó, nos autenticaremos e indicaremos la interface que se configurara para después asignarle los valores correspondientes, en la siguiente imagen se muestra el procedimiento realizado:

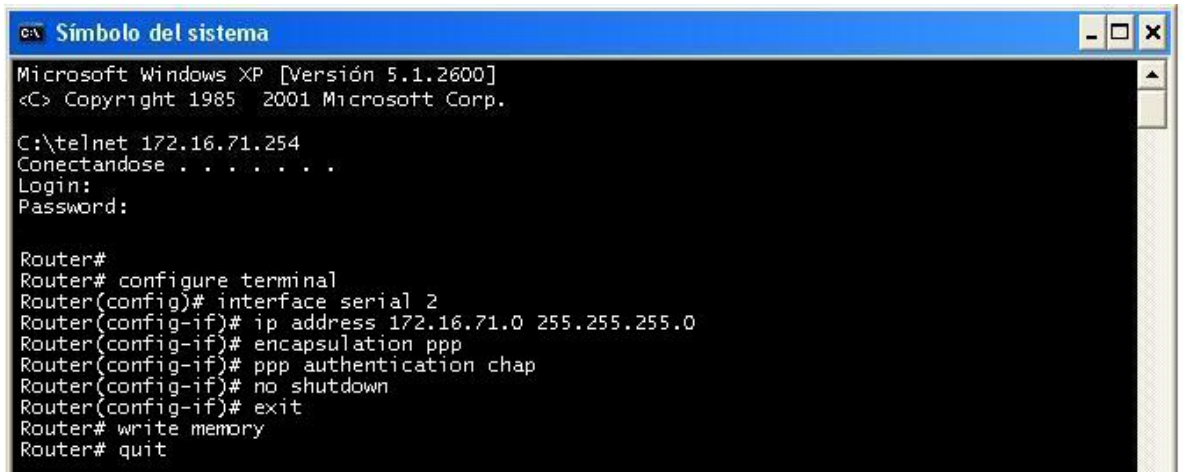

FIGURA 13. CONFIGURACION DE IP PARA RED LAN, PUERTO SERIAL.

Puede apreciarse que después de haber asignado la dirección IP a la interface de rede LAN se indica el tipo de encapsulamiento del enlace que al tratarse de un enlace punto a punto se asigna el mismo “ppp” y después se le dice que la comunicación iniciara tras haber utilizado el método de autenticación “chap”, el cual es un protocolo ya establecido y comúnmente utilizado en este tipo de enlaces de comunicación. Por último se realiza propiamente la configuración de la tabla de ruteo estático para que de esta manera tengamos siempre control sobre el flujo de información que hay en la red, la configuración se muestra a continuación:

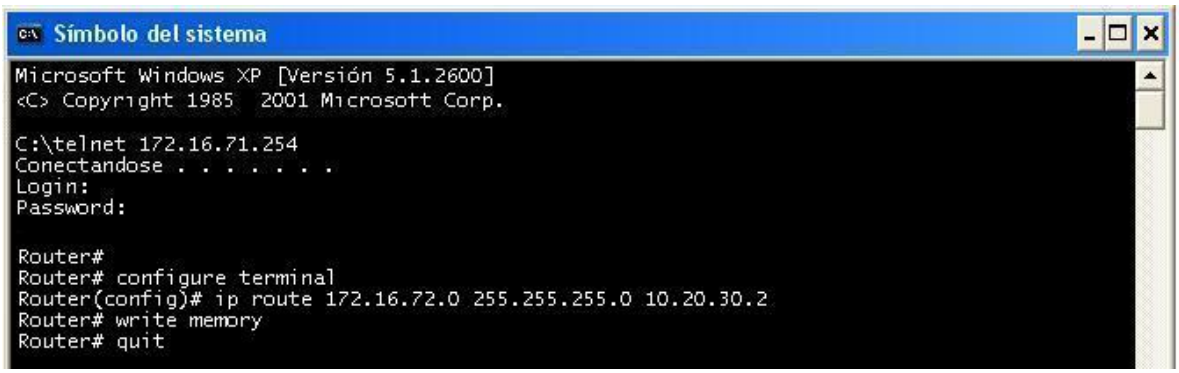

FIGURA 14. ASIGNACIÓN DE UNA RUTA ESTATICA.

Con el uso del comando empleado “ip route” se esta creando la tabla de rute estático, en donde se maneja la siguiente estructura:

Ip route “*IP de LAN a alcanzarse*” “*mascara de red para trabajar*” “*Ip WAN propia*”

En resumen se pueden englobar de la siguiente manera los pasos que se necesitan llevar a cabo para configurar una tabla de ruteo estático:

- Conexión física entre una computadora con S.O. Windows y el puerto de consola ubicado en la parte posterior del router.
- Establecer comunicación con el equipo ruteador vía telnet.
- Autenticarse vía el uso de un login y password.
- Entrar a modo configuración.
- Indicar la interface a configurar y asignarle los parámetros (dirección IP y mascara de red).
- Indicar el tipo de encapsulamiento del enlace y como se autenticaran los equipos al momento de comunicarse entre sí.
- Ingresar la tabla de ruteo estático, indicando primero la dirección Ip a la cual se enviara el trafico seguido de la máscara de red que indicara cuantos equipos se podrán conectar a dicha red y por último la dirección IP de nuestro equipo a través de la cual enviaremos el trafico.

- Guardar la configuración realizada.
- Concluir la sesión de telnet.

3.2 SWITCH 3COM 4400

En el ámbito de las redes un switch es el dispositivo que permite interconectar redes, este dispositivo trabaja en la capa 2 del modelo OSI, capa que se encarga del enlace de datos. Un switch interconecta dos o más partes de una red, funcionando como un puente que transmite datos de un segmento a otro. Su empleo es muy común cuando existe el propósito de conectar múltiples redes entre sí para que funcionen como una sola. Un switch suele mejorar el rendimiento y seguridad de una red de área local.

El switch es el resultado que se dio de mejorar dispositivos como el Hub, incluso al switch se le conoce como un Hub inteligente, debido a que cumple con las funciones primarias de interconectar segmentos de red, pero además se le puede indicar haga otro tipo de tareas que le dan la "inteligencia" con la que el Hub no cuenta.

El funcionamiento de un switch también llamado conmutador tiene lugar porque el mismo tiene la capacidad de aprender y almacenar direcciones de red de dispositivos alcanzables a través de sus puertos. A diferencia de lo que ocurre con un hub o concentrador, el switch hace que la información dirigida a un dispositivo vaya desde un puerto origen a otro puerto destino, a diferencia del hub que muestra la información a todos los dispositivos que se encuentran conectados a él.

El Switch 3Com de la familia 4400 (***FIGURA15***) será el dispositivo utilizado por Telecomm para que cumpla con su tarea cuando se requiera, entre sus características puedo mencionar que es escalable en 10/100 Mbps. Su desempeño dentro de grupos de trabajo en una ethernet es de alto rendimiento desde el punto de vista de la conexión.

El Switch 3Com 4400 permite hacer instalaciones en cascada (pila), esto es posible cuando los módulos de expansión se instalan en la parte trasera de la unidad, con esto se logra conectar un mayor número de equipos de computo a un segmento determinado de red o grupo de trabajo pues al conectarse dos o más switches con este modulo de expansión el número de puertos disponibles crece.

Este switch cuenta con 24 puertos para poder hacer las conexiones necesarias.

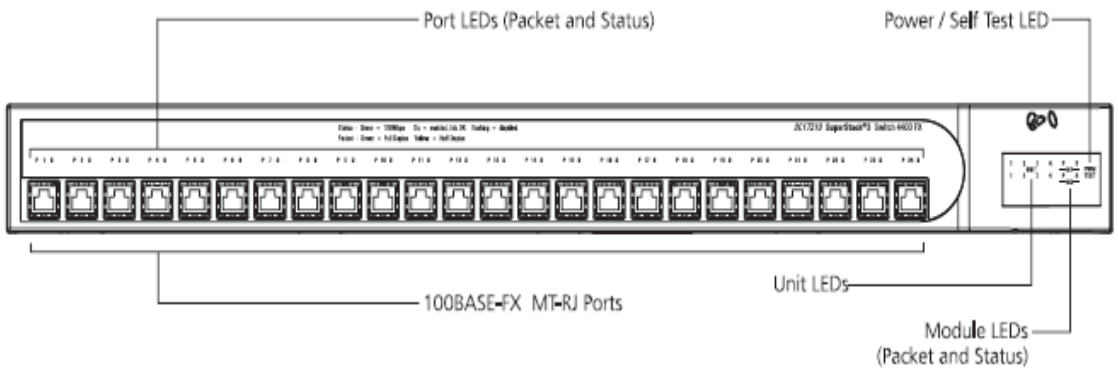

FIGURA 15. VISTA FRONTAL SWITCH 3COM FAMILIA 4400.

Enseguida se muestra cómo interpretar las indicaciones visuales de este switch, para los puertos que en él operan:

Verde:	Comunicación Full duplex, los paquetes están siendo transmitidos y recibidos a una velocidad alta de 100 Mbps, el puerto está habilitado.
Verde Parpadeando.	El puerto trabaja a una velocidad alta de 100 Mbps pero el puerto está desactivado.
Amarillo.	El puerto trabaja a una baja velocidad de 10Mbps.
Amarillo Parpadeando.	El puerto trabaja a una baja velocidad de 10Mbps, pero el puerto está desactivado.
Amarillo parpadeo lento.	El puerto falló y automáticamente ha sido deshabilitado.

3.2.1 CREACIÓN DE GRUPOS DE TRABAJO VÍA VLAN.

Este modelo de switch 3Com 4400 con el que estamos trabajando tiene la posibilidad de permitir la creación de grupos de trabajo, con esto se consigue el poder compartir información y recursos entre varios equipos de computo que estén conectados al switch.

Considérese que necesitamos incluir dos segmentos de red más al corporativo y además es necesario que exista comunicación entre sí para los miembros de cada uno de los grupos pero no con los integrantes del otro grupo, para ello solamente se cuenta con un switch donde actualmente están conectadas las computadoras del área de ingeniería y desea conectar las computadoras de los departamentos de Marketing y de ventas. Para dar solución a esta problemática se procede a realizar la implementación de VLANs con lo cual el esquema final de trabajo quería como el que se muestra en el ***Diagrama 21***.

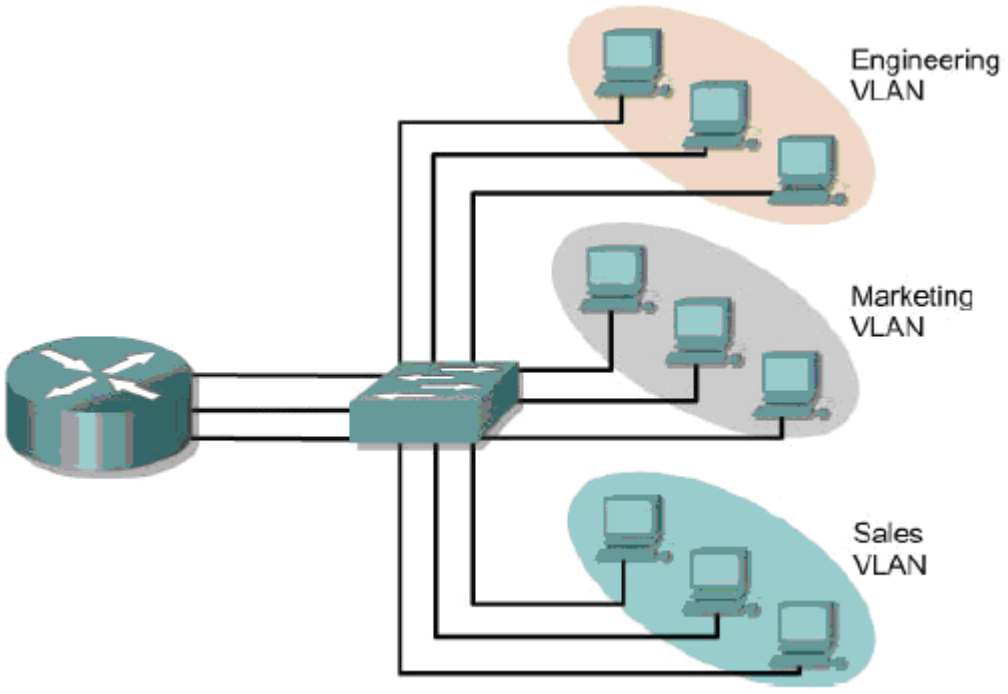

DIAGRAMA 21. GRUPOS DE TRABAJO PARA CREACION DE VLAN.

Para realizar la configuración inicial de un switch de este tipo solo basta con conectarse a uno de sus puertos y vía el navegador que se tiene instalado en la PC ingresar a la dirección IP que el switch tenga instalada por default, en el manual del fabricante podremos consultarla.

Tras registrar el switch que es la primera vez que se conectan a él, pedirá los parámetros iniciales con los cuales se iniciara su configuración, estos parámetros son:

- Nombre de la persona que administrara el equipo.
- Ubicación del administrador del equipo.
- Dirección IP que tendrá el switch dentro de la red.
- Nombre que tendrá el equipo para su identificación.

Una vez realizada esta configuración se procede a ingresar nuevamente a él, pero utilizando la dirección IP que se le asigno, para este caso se utilizara la IP 20.0.0.246 en nuestro navegador ingresaremos la dirección IP (***FIGURA16***):

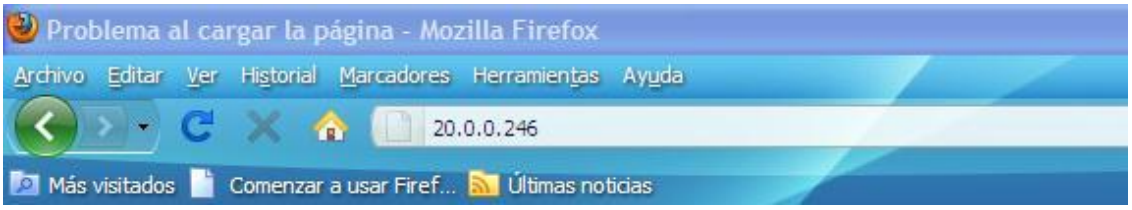

FIGURA 16. INGRESO VIA WEB AL SWITCH CON DIRECCION IP 20.0.0.246

La primera pantalla que nos mostrara el equipo será la de autenticación en donde se ingresara un nombre de usuario y una contraseña (***FIGURA17***):

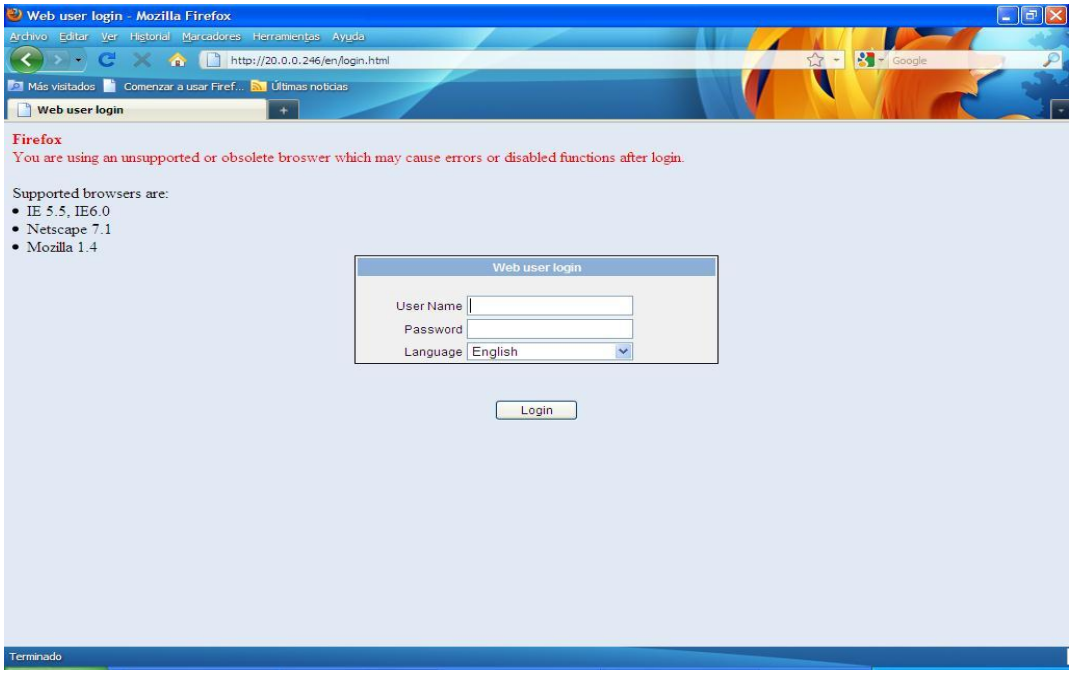

FIGURA 17. PANTALLA DE AUTENTICACION VIA NOMBRE DE USUARIO Y CONTRASEÑA.

Después de haberse autenticado correctamente el Switch nos permitirá acceder a su pantalla de la consola de configuración en donde podremos tener rápidamente un breve panorama de la configuración que contiene, se pueden apreciar las pestañas con acceso a los submenús más relevantes además de la posibilidad de desplegar subrutinas de trabajo para definir una correcta configuración dependiendo de las necesidades de trabajo que se tengan.

En esta pantalla principal (***FIGURA18***) también se aprecian los parámetros que se ingresaron en la configuración inicial del switch (datos de contacto):

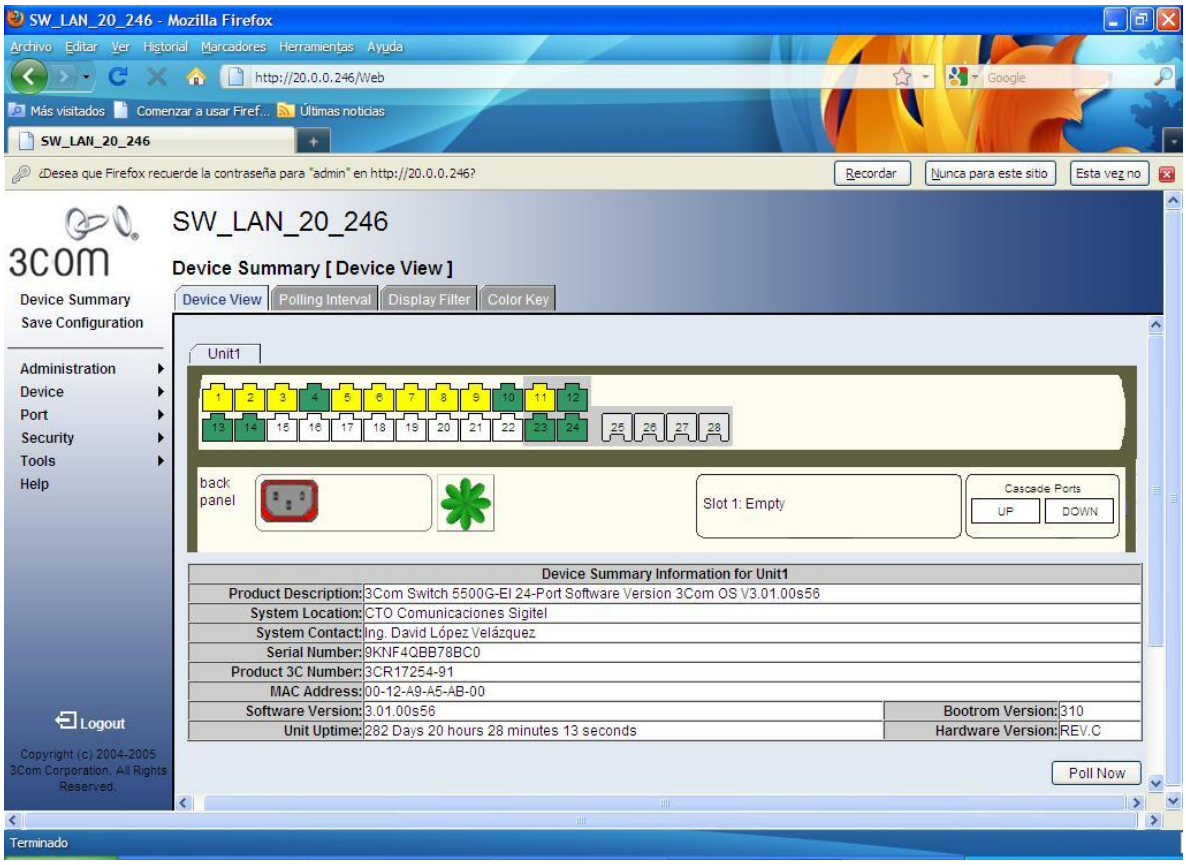

FIGURA 18. PANTALLA PRINCIPAL DE SWITCH 3COM 4400.

El siguiente paso para llevar a cabo la configuración de los grupos de trabajo de la VLAN será acceder al menú correspondiente, para ello en la columna izquierda del menú de configuración se accederá a la opción “Device”, esta opción desplegara un submenú para poder configurar parámetros como:

- Tablas de ruteo.
- Definir el protocolo de ruteo.
- Habilitar puerto para el uso de voz IP.
- Definir otro switch para que trabajen como cascada.
- Establecer grupos de trabajo vía VLAN.
- Asignar identificadores lógicos para VLAN’s.
- Editar aspectos de carácter general como el bloqueo de puertos en especifico o bien modificar su velocidad.

A nosotros la opción que nos interesa es “VLAN” (***FIGURA19***) accedemos a ella:

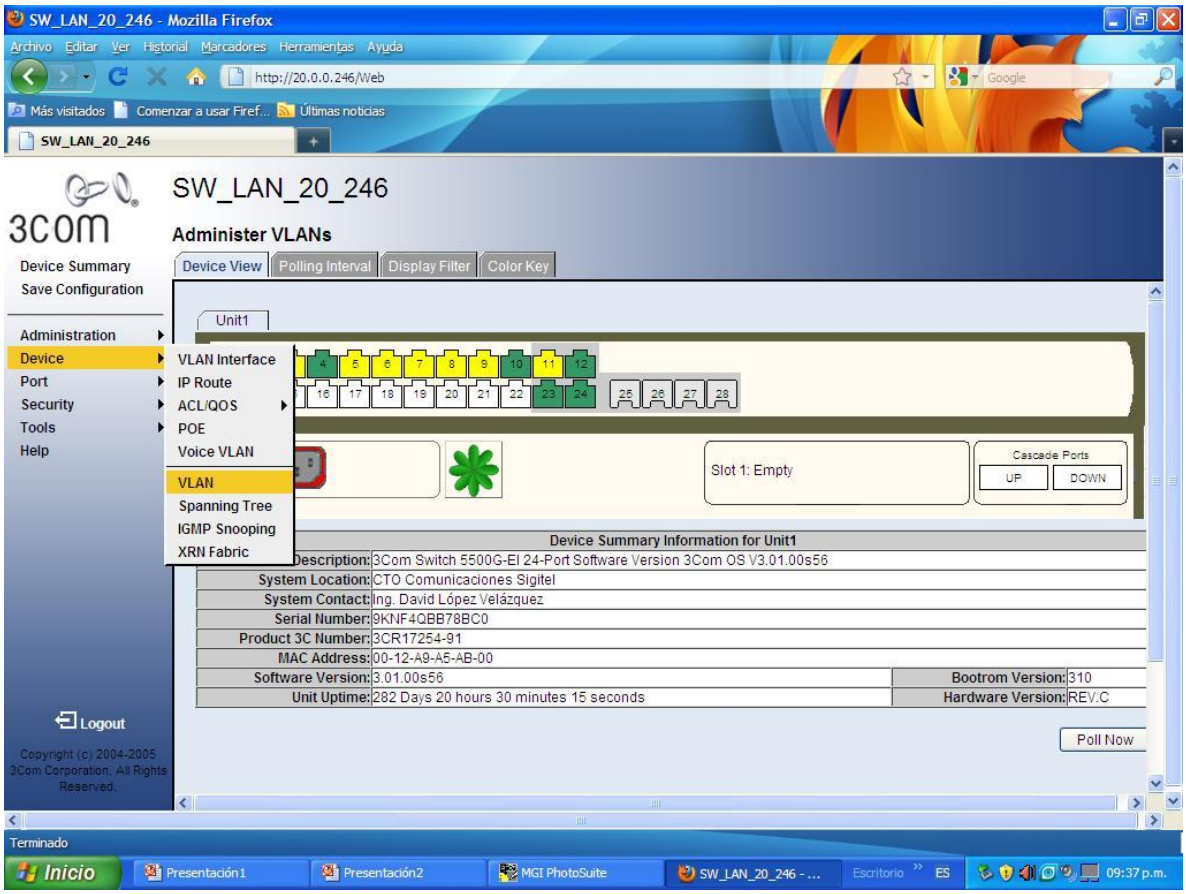

FIGURA 19. ACCESO A LA OPCION VLAN DENTRO DEL SUBMENU DEVICE.

El primer paso para configurar la VLAN es asignarle un identificador lógico (nombre), este será el único parámetro que se ingrese en esta pantalla de configuración (***FIGURA 20***).

El asignar un identificador lógico además de ser indispensable para la creación de la VLAN nos permitirá poder llevar a cabo tareas como:

- Crear más de una VLAN o grupo de trabajo dentro de un mismo switch, se pueden llegar a crear hasta 24 VLANs (una para cada puerto disponible) dentro de un mismo switch o bien 48 si se está trabajando en cascada.
- Permite identificar vía el ID asignado los diferentes grupos de trabajo asignados.
- Se inhibe el tráfico de la red hacia la VLAN que esta creada por default en la configuración del switch por los parámetros establecidos por el fabricante.
- La VLAN por default del dispositivo trabajara como esclava recibiendo todo el tráfico que entre y no esté destinado a alguna de las VLANs creadas en la configuración que se esta estableciendo.

A continuación se presenta la pantalla donde se ingresa el identificado lógico para la VLAN:

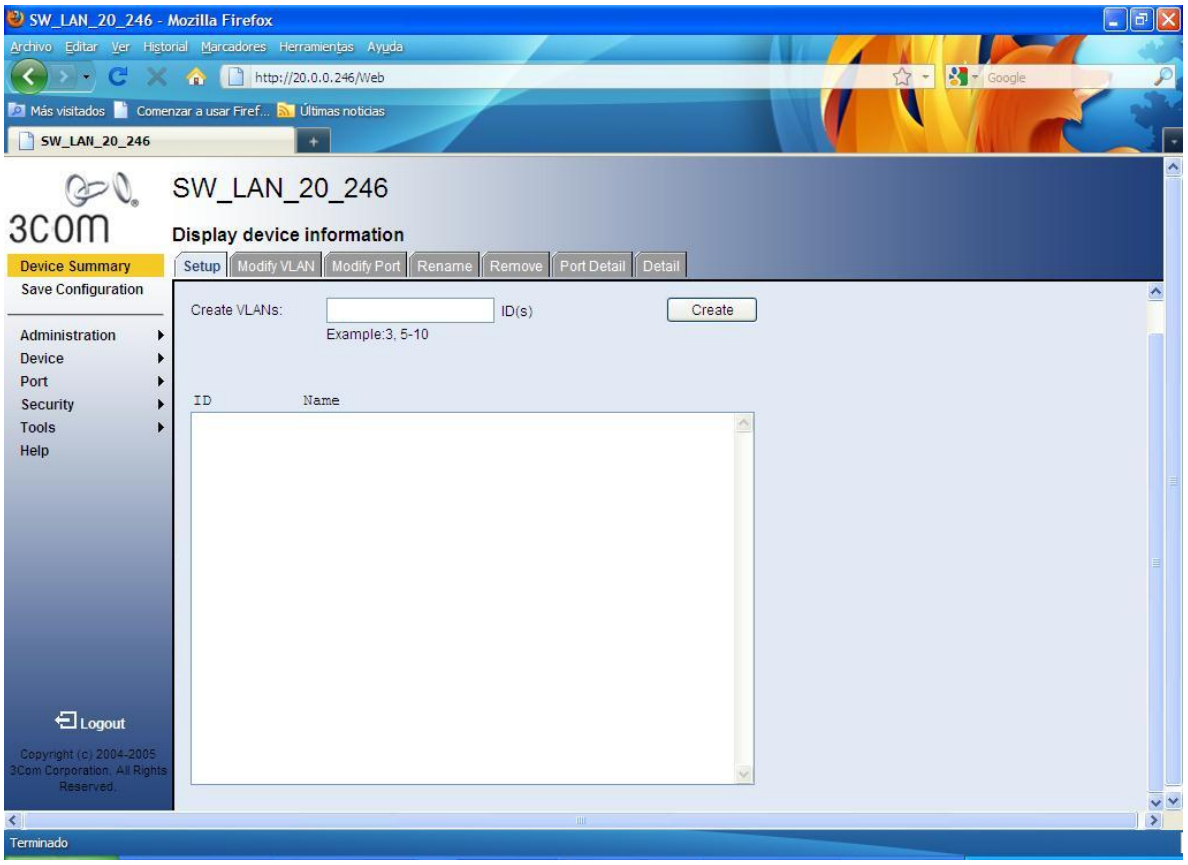

FIGURA 20. PANTALLA PARA ASIGNAR IDENTIFICADOR LOGICO A LA VLAN.

El siguiente paso dentro de la configuración de la VLAN será llevar a cabo la asignación de puertos para cada una de las VLANs que hayan sido creadas.

Para llevar a cabo la asignación de puertos (***FIGURA 20***) en la pantalla de configuración se solicitara que ingresemos la siguiente información:

- El puerto o número de puertos que se agregaran a la VLAN, o en su defecto que se retiraran de una VLAN.
- Definir si los cambios se aplicaran a una o a todas las VLANs que se encuentran creadas en el dispositivo.
- Definir si los puertos del switch serán clasificados como:

  Untagged: Todos los puertos etiquetados de esta forma indican que forman parte de la VLAN.

  Tagged: Todos los puertos etiquetados de esta forma indican que no son parte de la VLAN pero pueden ser usados en otra.

  Not Member: Se utiliza cuando no se quiere habilitar un puerto en especifico para que trabaje dentro de ninguna VLAN.

- Por último se mostrara un mapa con los puertos que el switch contiene y de esta forma se puede reconocer de una manera rápida los puertos que el switch tiene configurados para que trabajan dentro o fuera de una VLAN.

Ahora bien para establecer la configuración que hasta el momento se ha descrito y poder asignar los puertos que pertenecen a la VLAN que previamente creamos debemos de dirigirnos en la parte superior de la pantalla a la pestaña de nombre "Modify VLAN", entonces obtendremos la pantalla de configuración que necesitamos (***FIGURA 21***):

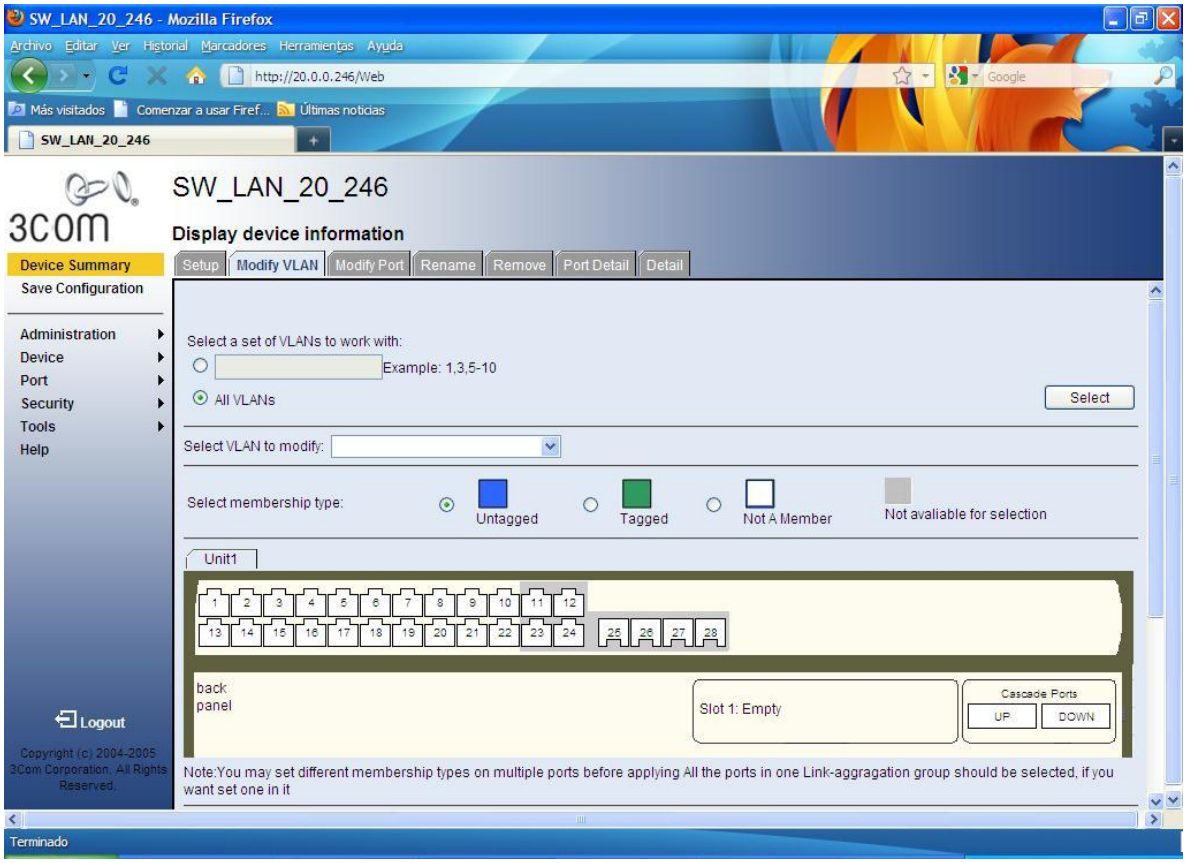

FIGURA 21. PANTALLA PARA AGREGAR O REMOVER PUERTOS A UNA O VARIAS VLAN

Con los pasos que hasta el momento se han descrito es como se lleva a cabo la configuración de una VLAN, siempre que nos conectemos a un switch 3Com como ha sido el caso para llevar a cabo alguna configuración, podemos acceder de manera muy rápida y general a un resumen grafico de su configuración lo cual nos permite tener un panorama muy rápido de la configuración y estado de operación que guarda el switch, no se debe de confundir con la pantalla principal de configuración del switch pues en ella solo encontraremos los datos para contactar al administrador del equipo así como la ubicación física de switch.

Para verificar de manera gráfica la configuración con la que el switch termino después haberlo configurado, nos dirigiremos a las pestañas superiores y seleccionaremos la de nombre “Device View” y veremos una pantalla como la que se muestra enseguida (***FIGURA 22***):

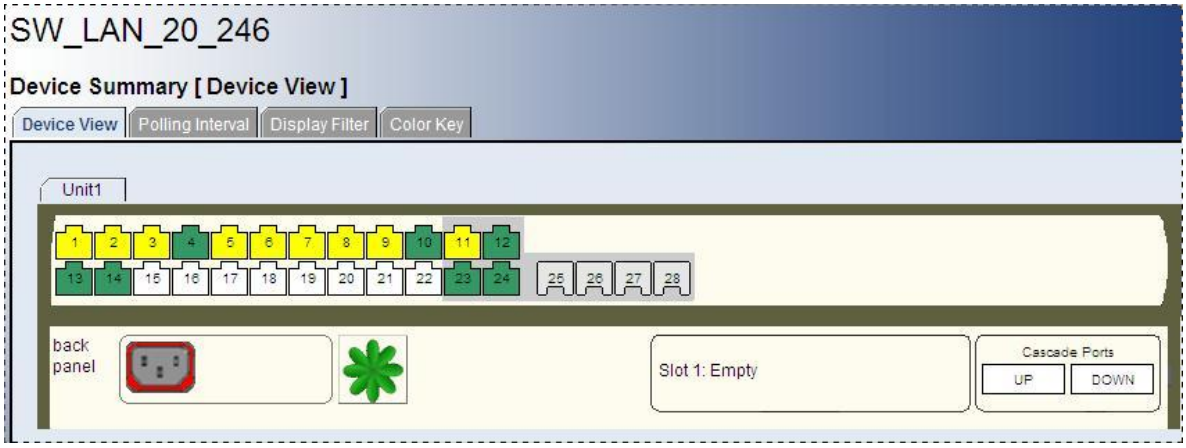

FIGURA 22. RESUMEN GRAFICO DE LA CONFIGURACIÓN ESTABLECIDA.

En la pantalla se aprecian los puertos del dispositivo así como los que son o no miembros de los grupos de trabajo creados.

3.3 HUB AXTEL

Hablando en términos generales otro dispositivo para interconexión de equipos es el Hub o también conocido como concentrador el cual incluso fue desarrollado antes que el switch, en la actualidad su uso continua dándose principalmente por el bajo costo que representa y su fácil implementación, pero no debe dejarse de lado y tener siempre en cuenta el hecho de que mientras más fácil sea la implementación de un dispositivo o software presenta el mismo grado de complejidad vulnerar su seguridad.

Hablando más sobre su definición un Hub es un dispositivo que permite centralizar el cableado de una red y poder ampliarla (***FIGURA 23***). Esto significa que recibe una señal y repite esta señal emitiéndola por todo sus puertos.

Los Hubs no logran dirigir el tráfico que llega a través de ellos, y cualquier paquete de entrada es transmitido a otro puerto (que no sea el puerto de entrada). Dado que cada paquete está siendo enviado a través de cualquier otro puerto, aparecen las colisiones de paquetes como resultado, que impiden en gran medida la fluidez del tráfico. Cuando dos dispositivos intentan comunicar simultáneamente, ocurrirá una colisión entre los paquetes transmitidos, que los dispositivos transmisores detectan. Al detectar esta colisión, los dispositivos dejan de transmitir y hacen una pausa antes de volver a enviar los paquetes.

Dentro del modelo OSI el Hub o concentrador opera a nivel de la capa física, capa dos, y puede ser implementado utilizando únicamente tecnología analógica.

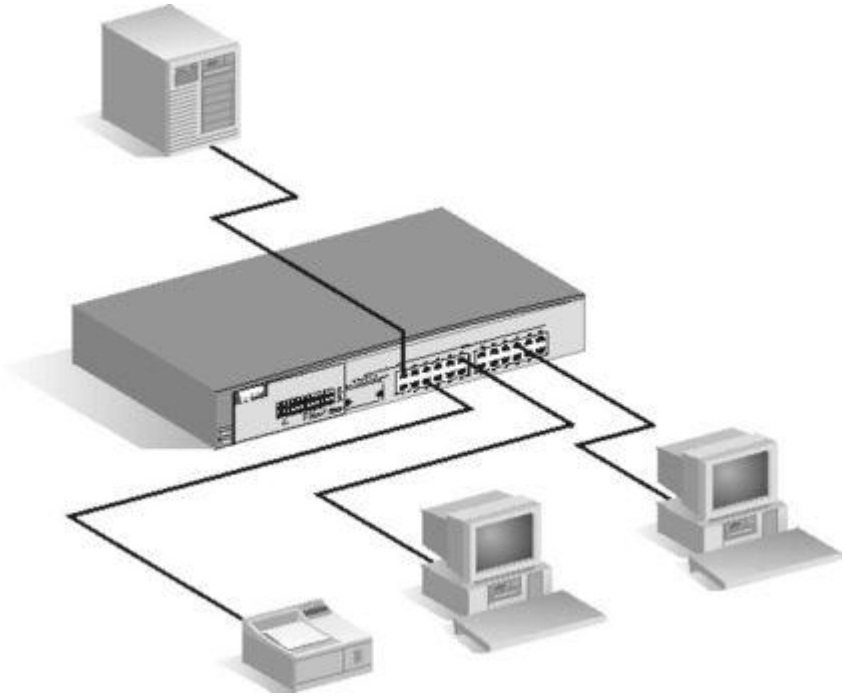

FIGURA 23. CONEXIÓN DE DISPOSITIVOS PARA AUMENTAR UNA RED A UN HUB.

En base a como se conectan dentro de una red y con el fin que se hace, los Hubs se pueden clasificar de diferentes maneras, entre ellas:

- Pasivo: Solo repiten la señal en la red. No necesita energía eléctrica.
- Activo: Regeneran y amplifican la señal. Necesita alimentación.
- Inteligente: También llamados smart hubs, incluyen microprocesador. Hacen lo que los activos pero además pueden ser administrados. Un administrador de red puede monitorear cada puerto e incluso obtener información estadística acerca de ello, tienen mejores funciones de direccionamiento. Todos los concentradores actuales son inteligentes.
- Solos: Son simplemente una caja con conexiones, normalmente se adhieren a una pared desde donde trabajan, son normales en las conexiones de las oficinas pequeñas y hogares donde no se necesita ampliarse, donde el promedio de usuarios es de 12.
- Apilables: Son montables uno sobre el otro, y se conectan uno con otro por medio de un cable. Al apilarse uno sobre el otro son casi modulares y evitan a las empresas invertir en los chasis que involucra un concentrador modular.
- Modulares: Consisten en una serie de tarjetas que se conectan de un chasis, de ahí mismo se interconectan y forman parte de la red. Estas constituyen el punto más alto de manejo y capacidad de conexiones, así

que solo se les ve en conexiones verdaderamente industriales o centrales telefónicas.

Otro de los puntos que nunca se debe de perder de vista son las ventajas y desventajas que nos presentara el implementar una solución a partir de un Hub, entre las principales encontramos:

Ventajas.

- El precio es barato por ser un dispositivo simple.
- Permite aislar a un usuario que tenga problemas en el cable de conexión, evitando que los demás usuarios sufran contratiempos.
- Tiene la capacidad de gestión, supervisión y control remoto, prolongando el funcionamiento de la red gracias a la aceleración del diagnostico y solución de problemas.

Desventajas.

- El tráfico añadido genera más probabilidades de colisión.
- A medida que añadimos computadoras a la red también aumentan las probabilidades de colisiones.
- Un Hub funciona a la velocidad del dispositivo más lento de la red.
- El Hub no tiene capacidad de almacenar nada, por lo tanto, en caso de falla es posible que se pierda el mensaje.
- Añade retardos derivados de la transmisión del paquete a todos los equipos de la red (incluyendo los que no son destinatarios del mismo).

3.4 FIREWALL JUNIPER ISG2000

En la actualidad uno de los dispositivos más importantes inherente a los procesos de seguridad es un Firewall, el cual puede encontrarse como software solamente o bien una combinación de hardware y software para su uso en casos mucho más robustos.

En el presente trabajo se estudiara el uso de uno de ellos en la combinación de hardware y software de la marca Juniper en su modelo ISG2000 (***FIGURA 23***), este equipo es capaz de realizar tareas como:

- Ruteo estático.
- Ruteo dinámico.
- Segmentar una red por zonas.
- Capacidad de trabajo para enlaces vía VPN.
- Monitoreo en tiempo real del tráfico circulante.
- Permitir o denegar la ejecución de procesos hacia el interior y exterior de la red donde opere.

En este momento la función principal que se analizara es la capacidad con la que cuenta para poder trabajar con los enlaces de comunicación

vía VPN, que si recordamos es el esquema que se plantea utilizar para llevar a cabo la comunicación entre el nodo principal de Telecomm y Banamex.
Retomando brevemente el concepto de VPN (red privada virtual) esta encriptara la información que se envía entre dos puntos distintos y utilizando internet como infraestructura, el hacer uso de internet se reducen considerablemente los costos de comunicación si se compara con el costo de rentar un proveedor de carrier, pero para poder estar seguros de que nuestra información al momento de viajar por internet no será interceptada por alguien la VPN creara un túnel virtual a lo largo de todo el camino para que la información siempre permanezca segura.

FIGURA 24. FIREWALL DE LA MARCA JUNIPER MODELO ISG 2000.

Este firewall Juniper ISG 2000 es capaz de llevar a cabo las tareas de seguridad comunes a estos dispositivos y además puede manejar enlaces de comunicación vía VPN, lo que llama la atención es la distribución o manejos de enlaces por lo que él denomina “zonas”.

Al momento de configurar y administrar el equipo se puede crear “grupos de trabajo” o bien encontrar afinidades entre los enlaces de comunicación, por ejemplo podemos agrupar todos los enlaces hacia instituciones bancarias y con ello crear una zona que se llame “Bancos”, de esta manera al momento de administrar el equipo los cambios que se realicen en la zona “bancos” afectaran a

todos los enlaces que se encuentren agrupados en dicha zona. Por default el equipo viene configurado con dos zonas, la zona trust y la un trust.

3.4.1 CONFIGURACIÓN DE UNA VPN.

Para llevar a cabo la configuración de una VPN haciendo uso de este firewall Juniper ISG 2000 se empleara el menú gráfico con el que se cuenta para acceder a él primero debemos de conectarnos desde una PC al firewall utilizando el navegador que se tenga instalado, en el campo donde se ingresa la dirección web de un página se ingresara la dirección IP del dispositivo al cual nos queremos conectar, en este caso el firewall cuya dirección IP es 20.0.0.92 después de ingresar estos valores nos redirigirá el navegador a una pantalla para realizar la autenticación de usuario correspondiente (***FIGURA 25***),en la siguiente imagen se muestra dicha pantalla:

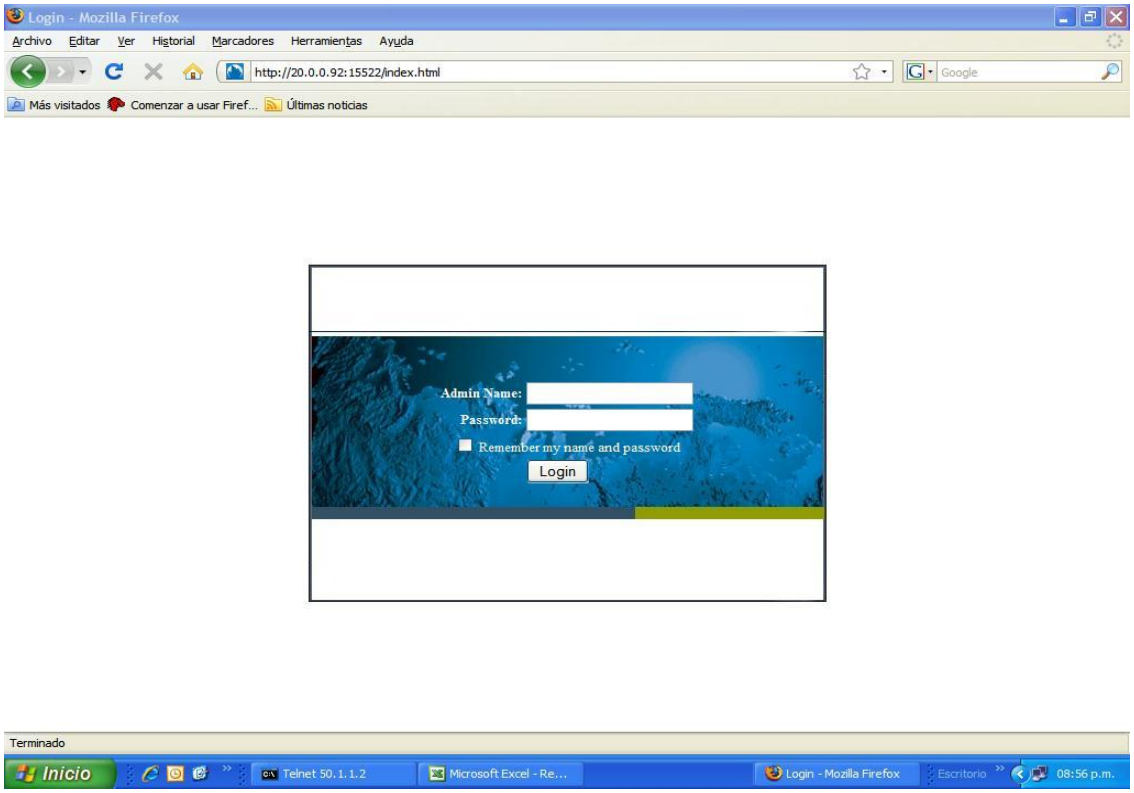

FIGURA 25. PANTALLA DE AUTENTICACION FIREWALL JUNIPER MODELO ISG 2000.

Es una pantalla de autenticación vía nombre de usuario (Admin Name) y contraseña (Password) cabe hacer mención que al momento de instalar este firewall por primera vez se creara la cuenta principal de root, posteriormente se pueden crear más cuentas para la administración de este equipo con los mismos privilegios que la cuenta de root o bien con menores privilegios, lo cual afectara directamente en los cambios que serán posible llevar a cabo o no dentro

de la configuración establecida de la consola, para este caso práctico se hace uso de la cuenta root, los menús mostrados son los mismos para otro tipo de cuentas.

Una vez autenticados correctamente el administrador se encontrara con la pantalla principal del firewall Juniper (***FIGURA 26***), dicha pantalla se muestra a continuación:

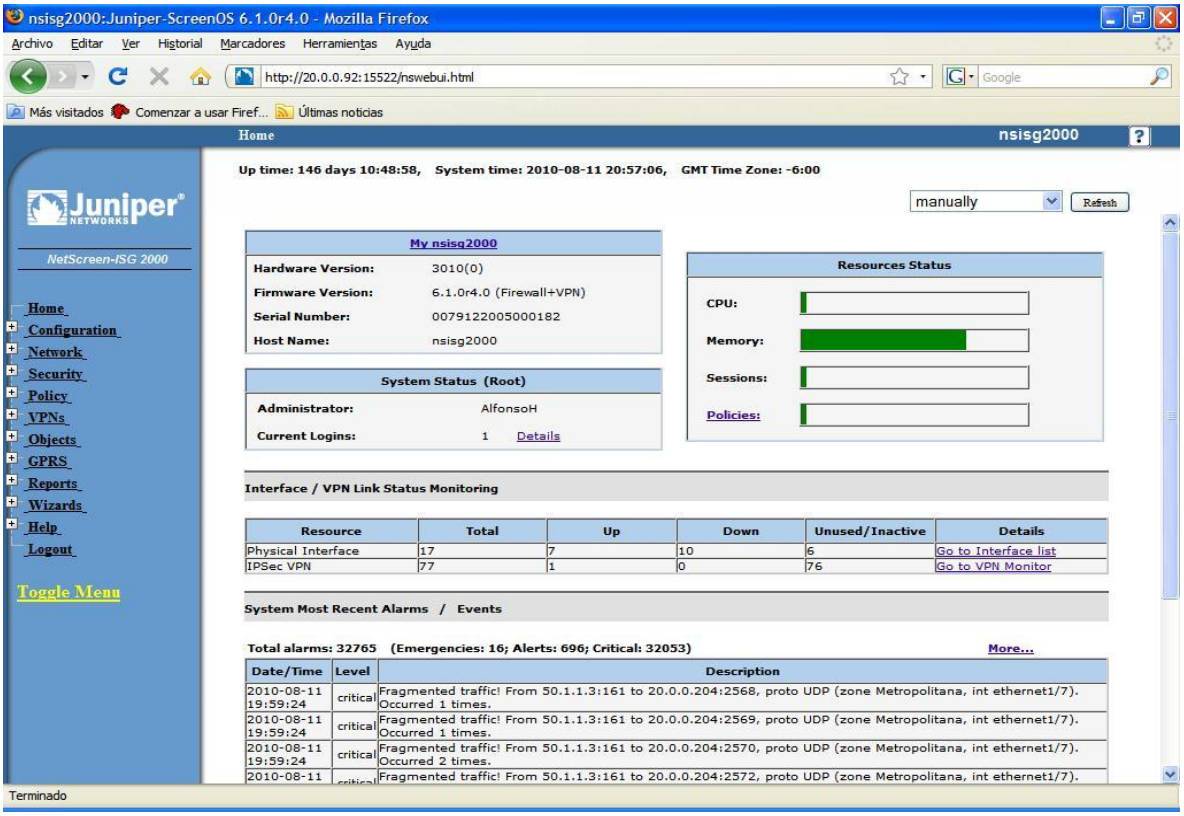

FIGURA 26. PANTALLA PRINCIPAL DE FIREWALL JUNIPER MODELO ISG 2000.

Esta pantalla se divide en dos secciones principalmente, la primera de ellas al lado izquierdo presenta un menú por el cual se puede navegar entre las diferentes opciones de configuración y administración del equipo (columna azul) y al lado derecho de este menú se aprecian los datos de rendimiento del equipo firewall, estos datos de performance son:

- Utilización del CPU.
- Utilización de memoria.
- Número de sesiones activas.
- Políticas de seguridad que están activas en el momento.

Posterior a los datos de performance del equipo se mostraran el estado de operación de las interfaces tanto físicas del equipo como las destinadas para el uso exclusivo de VPN, que recordemos es el caso que nos concierne principalmente. Por último se muestra un pequeño log indicando los procesos que

el equipo firewall está llevando a cabo, esto incluye los cambios sobre la configuración que tiene y quien los lleva a cabo.

Para iniciar con la configuración de nuestra VPN primero debemos de dirigirnos al menú de la consola y buscar el apartado “VPN” (***FIGURA 27***), en este apartado encontraremos las opciones necesarias para configurar y modificar el funcionamiento de las VPN que se tengan configuradas.

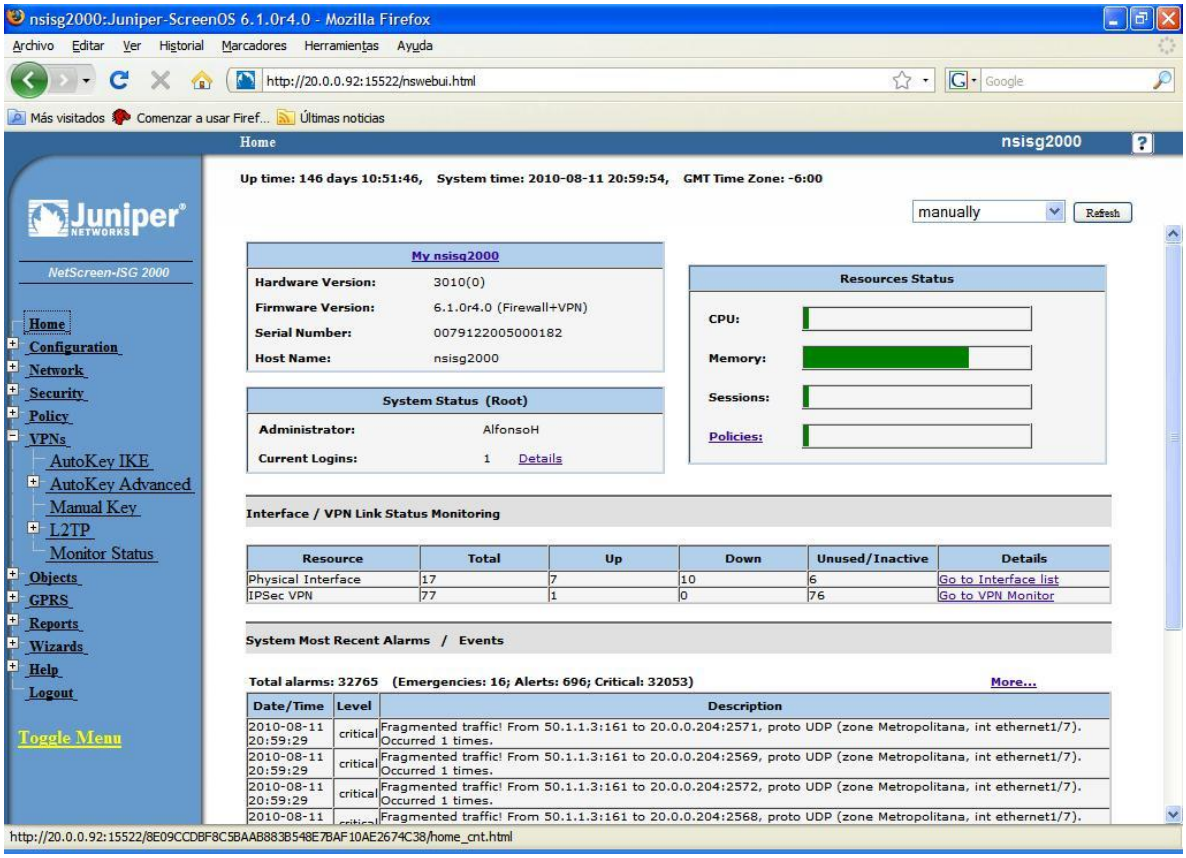

FIGURA 27. PANTALLA CON SUBMENU VPN DE FIREWALL JUNIPER MODELO ISG 2000.

Una vez desplegado el submenú de la opción VPN para poder configurar una VPN como es el caso del enlace de comunicación entre Telecomm y Banamex se deberá de elegir la opción “AutoKey IKE”, recordando el apartado del presente trabajo, al analizar el enlace de comunicación entre Telecomm y Banamex se dijo que la VPN utilizaría una clave pre-compartida (IKE).

Al crear una VPN vía el submenú “AutoKey IKE” lo que se está haciendo es automatizar los procesos de comunicación, cada vez que se quiera enviar información por la VPN, el firewall de forma automática enviara la contraseña para poder establecer el túnel virtual de la VPN con su contraparte en el otro extremo del enlace de comunicación. En casos muy específicos y en base a las necesidades que se tengan si no de desear automatizar el proceso de comunicación de la VPN, entonces se deberá de crear la VPN vía el submenú “Manual Key”, ejecutando la configuración de esta manera se deberá de ingresar

de forma manual la clave IKE de la VPN cada vez que se dese establecer comunicación entre los dos extremos de la VPN:

La creación de la VPN haciendo uso del ambiente grafico es un proceso realmente sencillo, para ello el firewall en la pantalla de configuración del submenú “AutoKey IKE” (***FIGURA 28***) solicitara que se ingresen en los campos correspondientes los siguientes datos que enlistan en orden de aparición:

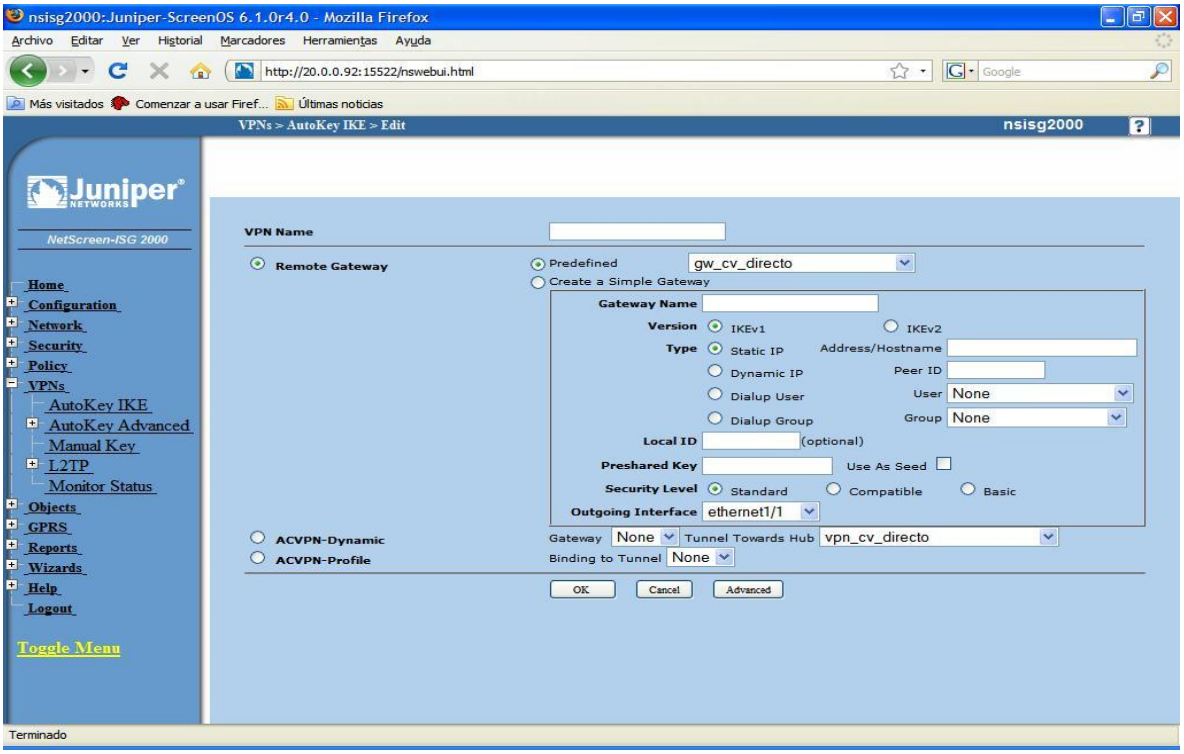

FIGURA 28. PANTALLA PARA CREAR UNA VPN EN FIREWALL JUNIPER ISG 2000.

- Nombre de la VPN (ID).

- Gateway remoto a utilizar (hace referencia a la interface del otro extremo de comunicación de la VPN, este dato lo proporciona el administrador de red del otro extremo de la VPN).

- Gateway local, que es la interface por donde se enviara la información (puede ser dirección IP o bien un ID que haga referencia a esa dirección IP, comúnmente usado cuando se declara el mismo Gateway en varios enlaces de VPN)

.

- Se debe seleccionar entre el estándar de encapsulación de la clave ya mencionada pre-compartida IKE, regularmente se utiliza IKEv1.

- Se indica el tipo de dirección IP que se está empleando, para el enlace entre Telecomm y Banamex es una IP estática.

- El siguiente paso es asignar un local ID, es decir un identificador lógico para el enlace con el cual poder identificarlo rápidamente sin la necesidad de hacer referencia a una dirección IP, se recomienda ingresar el mismo nombre que se le asignó a la VPN al principio de este proceso para evitar posibles confusiones al momento de administrar o editarla VPN.

- El siguiente paso y muy importante es ingresar la clave pre-compartida.

- Se debe definir el nivel de seguridad, se recomienda dejarlo en estándar.

- Definir la interface del firewall que la VPN usara para el enlace.

Una vez ingresados todos estos parámetros solo debemos de dar clic en el botón OK para aceptar la configuración que se ha ingresado hasta el momento, entonces el firewall nos enviara a otra pantalla (***FIGURA 29***) para ingresar los datos faltantes para concluir la configuración de la VPN dentro de nuestro equipo.

FIGURA 29. PANTALLA PARA ASIGNAR POLITICAS DE SEGURIDAD A LA VPN.

Los últimos pasos para concluir con la configuración de la VPN será confirmar el identificador lógico (ID) que ha sido asignado a la VPN en la pantalla anterior y después aplicar las reglas de seguridad que sean necesarias para el correcto y fiable funcionamiento del enlace de comunicación.

Debe de hacerse notar que dentro de la documentación del equipo firewall Juniper ISG-2000 se puede encontrar una tabla de referencia en donde se puede comparar el número de política que está definida y a qué tipo de proceso hace referencia, por ejemplo:

"*Política ID 05, bloquea el comando tracert*"

Como administradores de la red se puede hacer uso de las políticas predefinidas o bien crear nuevas, muy útil para inhibir puertos usados en específico.

Tras concluir con la relación de políticas de seguridad para el enlace VPN, la configuración realizada hasta el momento se activara y comenzara a trabajar el enlace una vez que alguien desee transmitir tráfico por el nuevo enlace, no está de más mencionar que la configuración hasta el momento mostrada es la realizada en el extremo de Telecomm y Banamex realizara algo muy similar dependiendo del ambiente de configuración con el que cuente el equipo receptor de la VPN en su extremo.

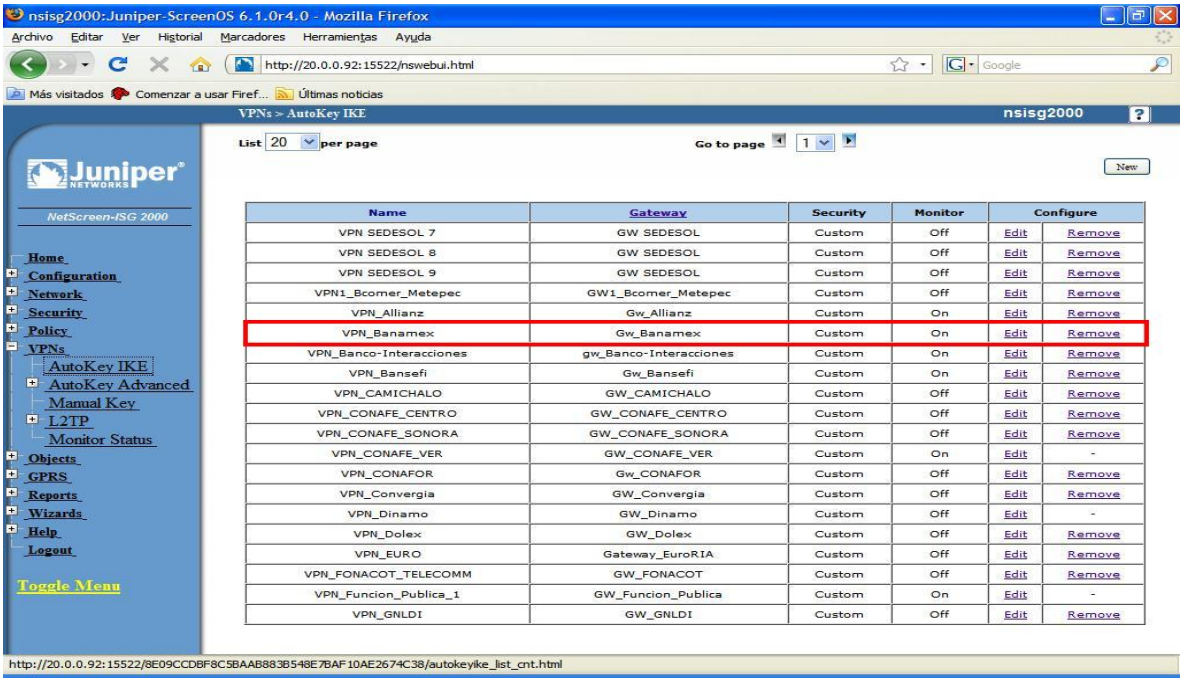

FIGURA 30. PANTALLA DE MONITOR STATUS VPN.

La ***FIGURA 30*** muestra el resultado de elegir la opción "*Monitor Status*" dentro del submenú *VPN*, en esta pantalla se puede verificar de forma rápida y general el estado de operación de todas las VPN que se tengan configuradas en el firewall Juniper ISG 2000.

En dicha pantalla se parecía el nombre de la VPN configurada (ID asignado durante la configuración), el Gateway remoto que se está empleando (equipo al cual se conecta en el otro extremo de la comunicación), nivel de seguridad, Monitor (el estado ON es cuando se encuentra activa la comunicación de la VPN, el estado OF indica que no hay tráfico en la VPN más no que esta se encuentra con problemas de comunicación) y por último se aprecian las opciones Edit para regresar y hacer cambios en la configuración de la VPN o bien Remove para eliminar a la VPN.

3.4.2 CONFIGURACIÓN DE LOS PROCESOS A BLOQUEAR VÍA CORTAFUEGOS [FIREWALL].

Para bloquear procesos de comunicación en específico se puede hacer uso de la consola del firewall Juniper ISG 2000, para ello esta vez no se realizara la configuración en un ambiente gráfico, en esta ocasión se hará uso de la línea de comandos para llevar a cabo las tareas que se desean.

Lo primero que se debe de hacer será conectarse vía telnet al firewall, recuérdese que la dirección IP que tiene el firewall Juniper ISG 2000 dentro del esquema de operación de la intranet de Telecomm es 20.0.0.92 para ello se usara el MS-DOS de Windows como se muestra en la siguiente imagen (***FIGURA 31***):

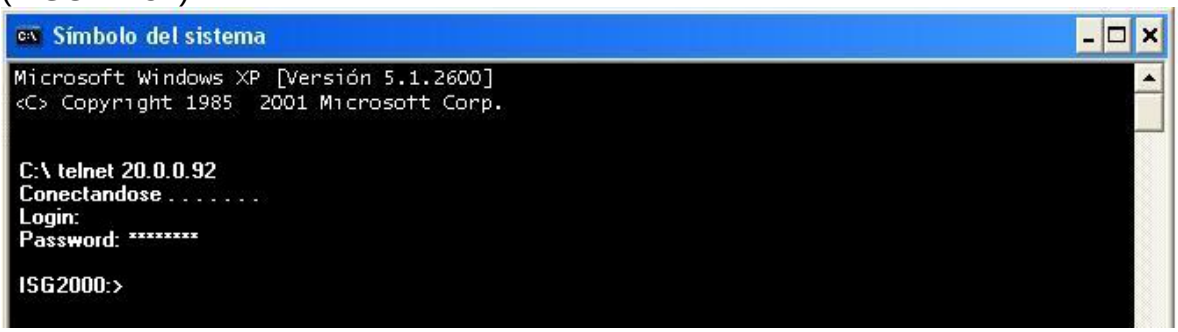

FIGURA 31. PANTALLA DE MS-DOS HACIENDO TELNET AL FIREWALL 20.0.0.92

La configuración para poder negar la ejecución de un proceso es verdaderamente sencilla (***FIGURA 32***), para ello se debe de indicar en un principio la VPN a la cual se aplicaran los cambios, después se negara el o los procesos no permitidos para finalmente guardar los cambios efectuados.

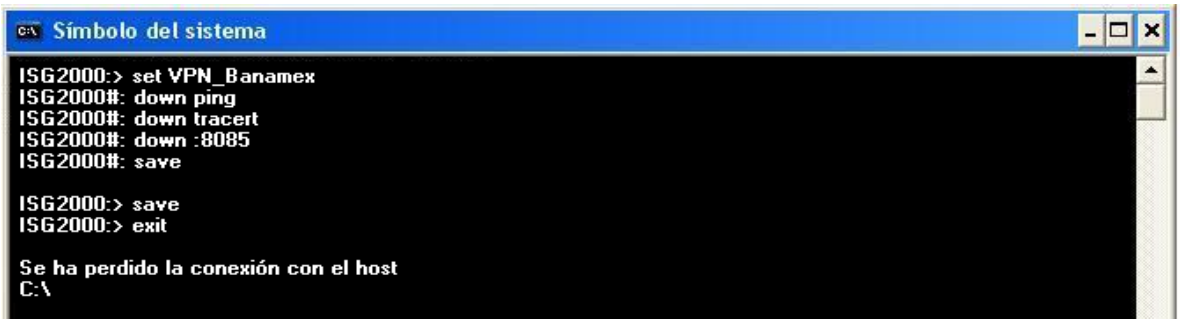

FIGURA 32. PANTALLA DE MS-DOS EN TELNET DANDO DE BAJA SERVICIOS.

Como se puede apreciar para la VPN de Banamex que se ha configurado se negaron en un principio dos servicios, no responderán los comandos de PING y tampoco el comando TRACERT y como un ejemplo de otra forma de negación también se bloqueo el uso del puerto 8085, esta forma de bloquear procesos a través de puertos es muy útil ya que en ocasiones existen aplicaciones exclusivas para intranet y su control y funcionamiento se basa en el uso de los puertos.

CAPITULO IV

HERRAMIENTAS DE MONITOREO DE LA SEGURIDAD DENTRO DE LAS REDES.

4.1 WAN SPY.

Para mantener y guardar un registro diario del comportamiento que se observa en un enlace de comunicación la herramienta Wan Spy es de gran ayuda pues con esta se puede monitorear directamente la interfaz WAN de un equipo de ruteo, recordemos que por la red WAN transita todo el tráfico que entra y sale de una red. Las características de este software (***TABLA 1***) se presentan a continuación:

Nombre	Wan Spy
Versión	1.6
Licencia	Shaware
Idioma	Inglés
Desarrollador	DVS Informatics Pvt. Ltd.
Sitio	www.softpedia.com

TABLA 1. CARACTERISTICAS DEL SOFTWARE WAN SPY.

Una vez descargado el programa se comienza con su instalación la cual resulta un proceso muy sencillo, en un principio el instalador dará la bienvenida e indicara que la instalación está por comenzar (***FIGURA 33***):

FIGURA 33. PASO 1 DEL INSTALADOR DE WAN SPY.

En esta ***FIGURA 33*** se debe de dar por aceptado el hecho de que sabemos que se comenzara con la instalación del software, al hacer clic en la opción “NEXT” pasaremos a una pantalla que contiene las características generales de fabricación del software, de no querer continuar con el proceso de instalación entonces se deberá de elegir la opción “EXIT” desde el momento en el que nos encontramos en la primer pantalla del instalador del sistema, de elegir esta opción el programa solicitara confirmar la selección hecha.

Si continuamos con el proceso de instalación como es el caso la siguiente pantalla es prácticamente informativa y describirá los datos generales del software Wan Spy en su versión 1.6 que es con la que estamos trabajando, esta pantalla no se muestra pues es la información plasmada dentro de la ***TABLA 1*** del presente trabajo de titulación.

La tercera pantalla que aparece durante el proceso de instalación es la referente a la licencia del programa (***FIGURA 34***), aquí es evidente que se deben de aceptar los términos de uso que se especifican en la licencia del programa de lo contrario no podrá continuarse con la instalación del software, elijase por lo tanto la opción "*I agree with the above terms and conditions*" como se muestra en la siguiente imagen:

FIGURA 34. PASO 3 DEL INSTALADOR DE WAN SPY.

Una vez aceptados los términos de la licencia de uso para este software, el siguiente paso es definir la ruta de instalación del software.

Para llevar a cabo la instalación es necesario contar con al menos 12MB de espacio libres en disco duro y no se debe de olvidar que este software está diseñado para trabajar bajo plataforma Windows.

Como la gran mayoría de programas al momento de instalarlo el programa mostrara por default una ruta para su instalación, si se desea cambiar dicha ruta puede hacerse.

En la siguiente imagen (***FIGURA 35***) se muestra la pantalla donde se define la ruta de instalación del software Wan Spy en su versión 1.6, en este caso la instalación se está realizando sobre un sistema operativo Windows 7.

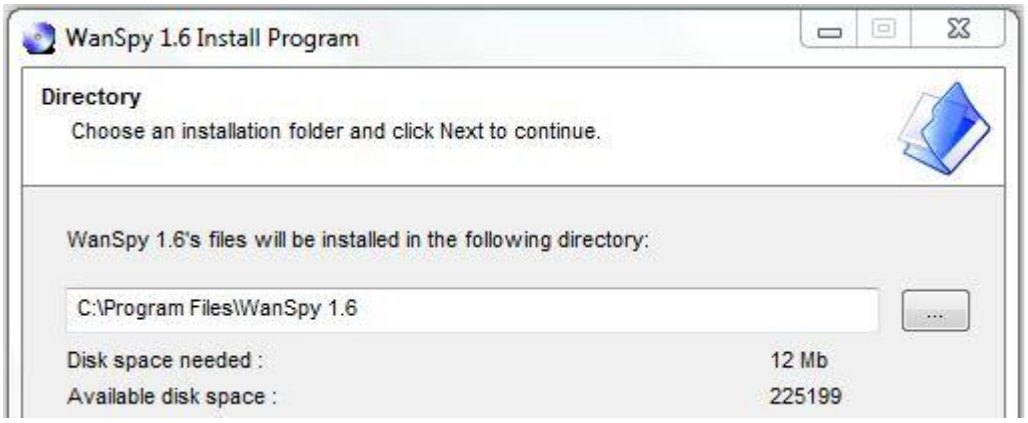

FIGURA 35. PASO 4 DEL INSTALADOR DE WAN SPY.

Una vez definida la ruta de instalación el programa instalara los archivos necesarios además de crear los directorios necesarios para la instalación del software y su correcta operación. Concluido este paso el instalador mostrara una pantalla indicando que el proceso de instalación ha concluido (***FIGURA 36***) como se muestra en la siguiente imagen:

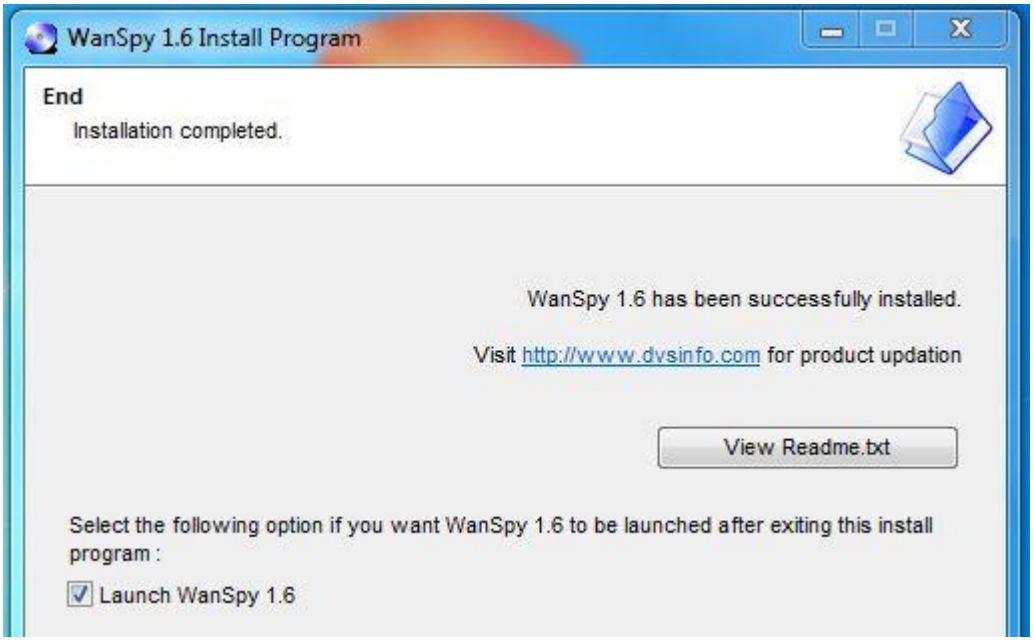

FIGURA 36. PASO 5 DEL INSTALADOR DE WAN SPY.

Se puede desplegar un archivo .txt que contiene información más detallada con respecto al proceso de instalación que se llevó a cabo.

Ya concluido con el proceso de instalación se procederá a iniciar el programa (***FIGURA 37***) puede hacerse desde el menú inicio del sistema operativo o bien haciendo uso del acceso directo que se creó en el escritorio.

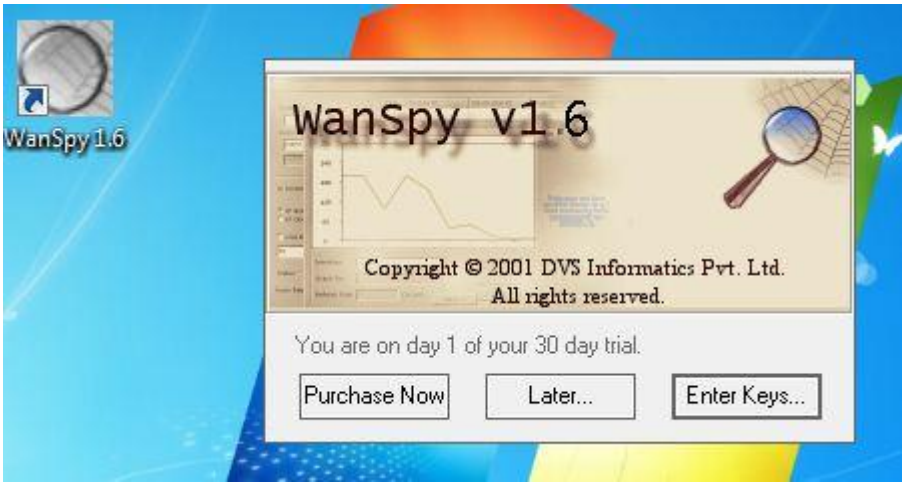

FIGURA 37. EJECUCION DEL PROGRAMA DE WAN SPY DESDE UN ACCESO DIRECTO.

Al ejecutar el programa nos encontraremos con un entorno de trabajo como el que se muestra en la ***FIGURA 38***:

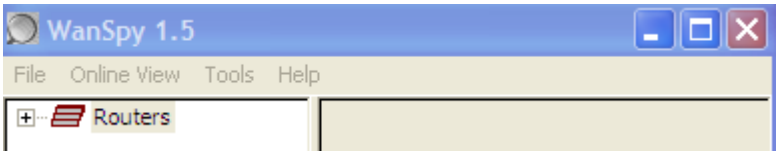

FIGURA 38. AMBIENTE DE TRABAJO EN WAN SPY.

Las principales opciones de las cuales haremos constantemente uso en su barra de menú son: File, Tools y Help cuando se requiera consultar la documentación del programa.

Haciendo uso de estos menús es como se darán de alta los equipos ruteadores y las interfaces que se monitorearan de forma automática, está por demás mencionar que la PC donde se instale esta herramienta deberá de tener acceso a las subredes de los equipos ruteadores que se configurarán.

Para llevar a cabo la configuración de esta herramienta primero se deben de dar de alta los equipos ruteadores haciendo uso del submenú Tools, posteriormente el monitoreo diario se podrá exportar a una hoja de cálculo como Microsoft Excel con la ayuda del submenú File.

El poder exportar los datos a una hoja de cálculo es de gran ayuda pues se puede guardar el monitoreo diario o por un periodo de tiempo determinado con datos como la cantidad de bits que se tienen por minuto tanto de entrada como de salida, además de poder llevar a cabo una gráfica del comportamiento del enlace.

A continuación se describe la función de las principales opciones del menú:

- **Tools:** En este menú la principal opción que usaremos es "Add Router", realizando un proceso muy similar a la configuración de otras herramientas para la administración de redes se deberá de ingresar en primer término un nombre para la identificación del router, seguido se ingresa la dirección IP de la interfaz del router que será escaneada, esto se realiza en una pantalla como la que se muestra en la ***FIGURA 39***.

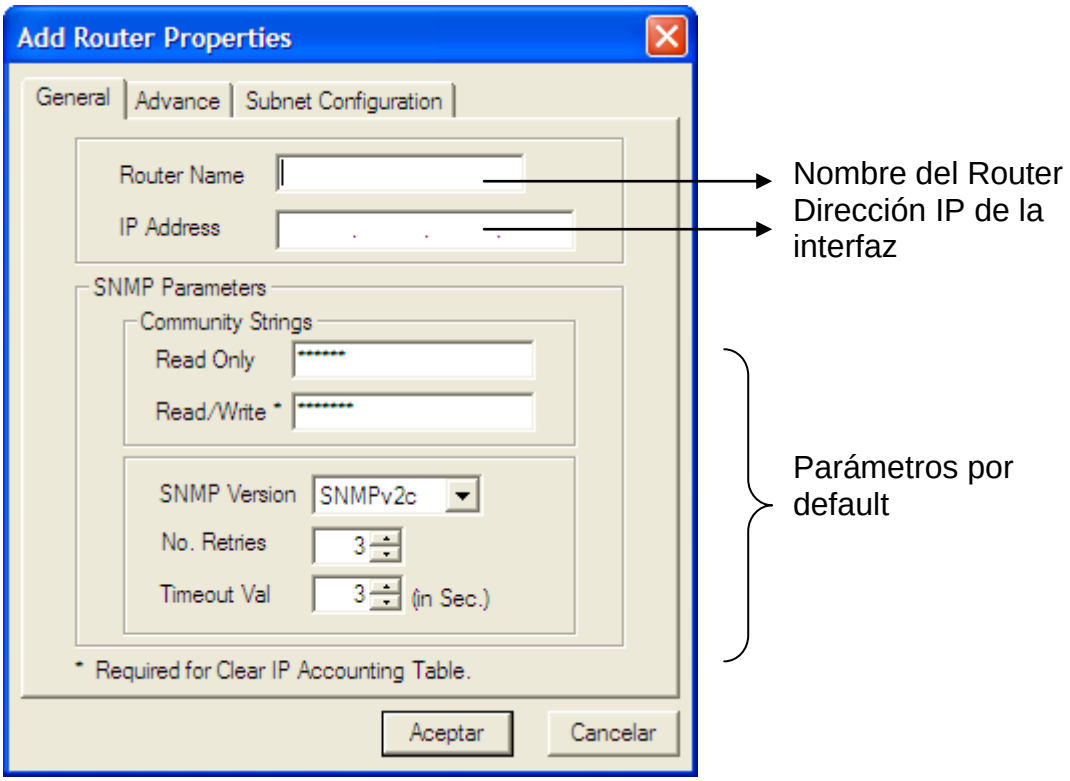

Figura 39. PANTALLA PARA AGREGAR NUEVO ROUTER A MONITOREAR.

- **File:** En la opción de File se encuentra el submenú "*Save Data In*" el cual nos lleva a la opción de "*MS Excel Sheet*" y es aquí donde el monitoreo que se almacena en el buffer del programa, el cual cabe mencionar tiene capacidad para trabajar durante 48 horas, lo guarda en una hoja de cálculo para facilitar su posterior trabajo.

Una vez configurados los diferentes monitoreos que se deseen realizar se tendrá un ambiente de trabajo (***FIGURA* 39**) que contiene al lado

izquierdo una columna con un menú de árbol en donde la raíz tendrá por nombre la palabra Routers.

Al desplegar el menú raíz veremos los dispositivos que hayan sido configurados y las diferentes interfaces que estos contienen, entonces se elegirá la interface que contiene el tráfico de las red Wan que es la que más nos interesa para hacer uso de esta herramienta.

Al monitorear la interface Wan podemos tener un panorama general de cómo se comporta dicho enlace de comunicación a lo largo del día, podríamos darnos cuenta e identificar cuáles son las horas pico en las que se satura dicho enlace o bien verificar si el ancho de banda que se tiene destinado es suficiente o no. Obviamente quedaría registrado si se pierde el enlace, con esta herramienta se tiene una bitácora gráfica y además de un registro en una hoja de cálculo del comportamiento de un enlace minuto a minuto,

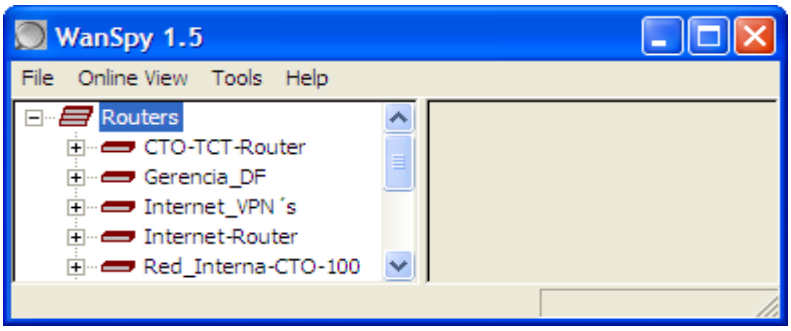

Figura 40. PANTALLA DE WANSPY CON ROUTERS CONFIGURADOS.

Para lanzar el monitoreo basta con desplegar el router a monitorear y dar un clic derecho en su interfaz para entonces seleccionar la opción "*Interface Graphs*", tendremos el monitoreo en tiempo real (***FIGURA 41***):

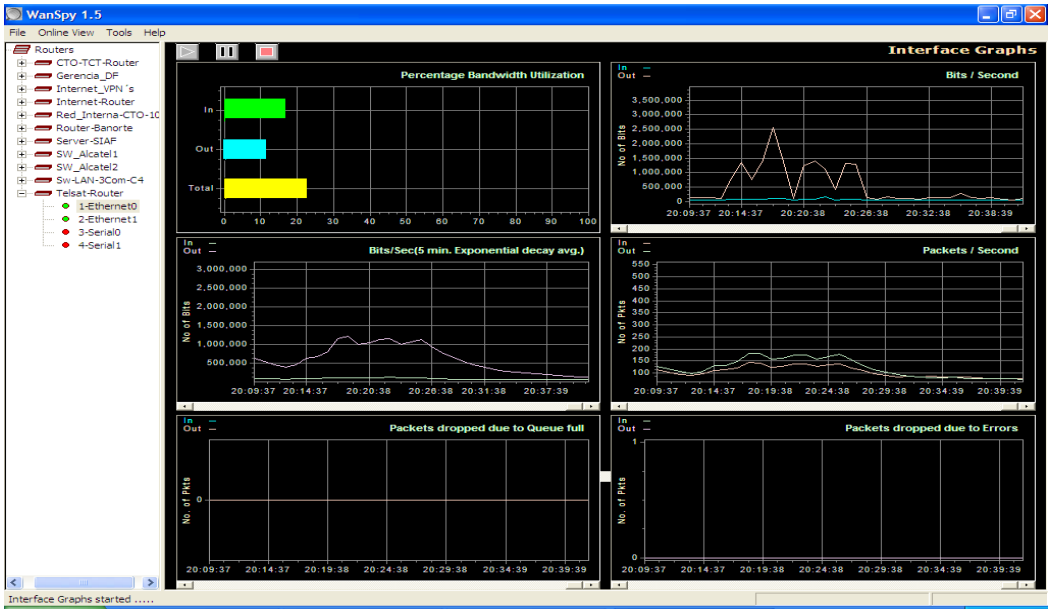

Figura 41. PANTALLA DE WANSPY REALIZANDO MONITOREO EN TIEMPO REAL.

La gráfica de barras representa el total del ancho de banda que se está empleando y es representado por la barra de color amarillo, mientras que la barra en color verde representa el porcentaje de entrada y el color azul es el porcentaje de salida.

El resto de las gráficas que arroja este programa son variaciones de la principal y lo que cambia es el tipo de gráfico y las escalas que se emplean pues encontramos gráficas que promedian bits/segundos, paquetes/minuto, etc.

4.2 MCAFEE INTRUSHIELD.

La plataforma Mcafee IntruShield se compone por un server conectado al backbone de la empresa y la instalación del software que es necesario para poder operar la consola de la plataforma y acceder al servidor de operación.

Nombre	Mcafee IntruShield
Versión	Enterprise
Licencia	Shaware
Idioma	Inglés
Desarrollador	Mcafee
Sitio	www.mcafee.com

TABLA 2. CARACTERISTICAS DE LA PLATAFORMA Mcafee IntruShield.

El trabajo en conjunto de toda esta plataforma es muy importante pues en ella es posible detectar los ataques de terceros hacia nuestra red que se encuentra en operación o bien poder detectar cuando un usuario al interior de nuestra red está realizando un ataque o proceso prohibido, el trabajo en conjunto de los diferentes módulos que interactúan en esta plataforma se puede resumir de la siguiente manera:

- El administrador de red configura los sensores que trabajaran en la plataforma.
- El administrador de red elige las políticas de seguridad dentro de una serie de plantillas y crea una o más políticas para aquellas necesidades que se tengan en específico.
- La plataforma entra en operación junto con las políticas de seguridad aplicadas a los sensores, analizara el tráfico de las zonas que se hayan especificado dentro de la red.
- Se guardara en una base de datos toda la información generada por los sensores de la plataforma para consultarla cuando se desee.

Para poder trabajar de manera remota con esta plataforma es necesario instalar la Java Virtual Machine desde la página web www.java.com en la o las PC de monitoreo que se van a implementar.

Una vez instalada toda la infraestructura necesaria para la operación de esta plataforma a continuación se presenta como operar directamente con el servidor desde una computadora de monitoreo. Para ello primero debemos de conectarnos al servidor, se debe de ingresar la dirección IP (***FIGURA 42***) que tiene el sensor principal de la plataforma Mcafee IntruShield, en este ejemplo práctico la dirección IP del sensor es 20.0.0.4 puede hacerse uso del comando ejecutar en el menú inicio del sistema operativo:

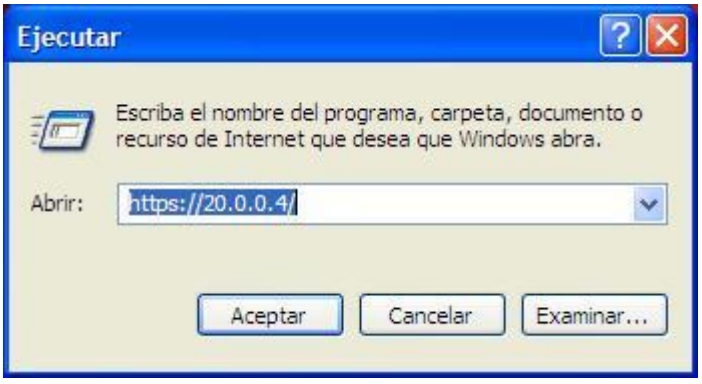

Figura 42. PANTALLA PARA ACCEDER AL SENSOR CONFIGURADO VIA IP.

Después de haber solicitado la conexión al sensor cuya IP es 20.0.0.4 este nos redirigirá a una ventana del navegador de internet que se tenga instalado en donde se solicitara que el usuario se identifique vía un nombre de usuario y contraseña (***FIGURA 43***) como se muestra en la siguiente imagen:

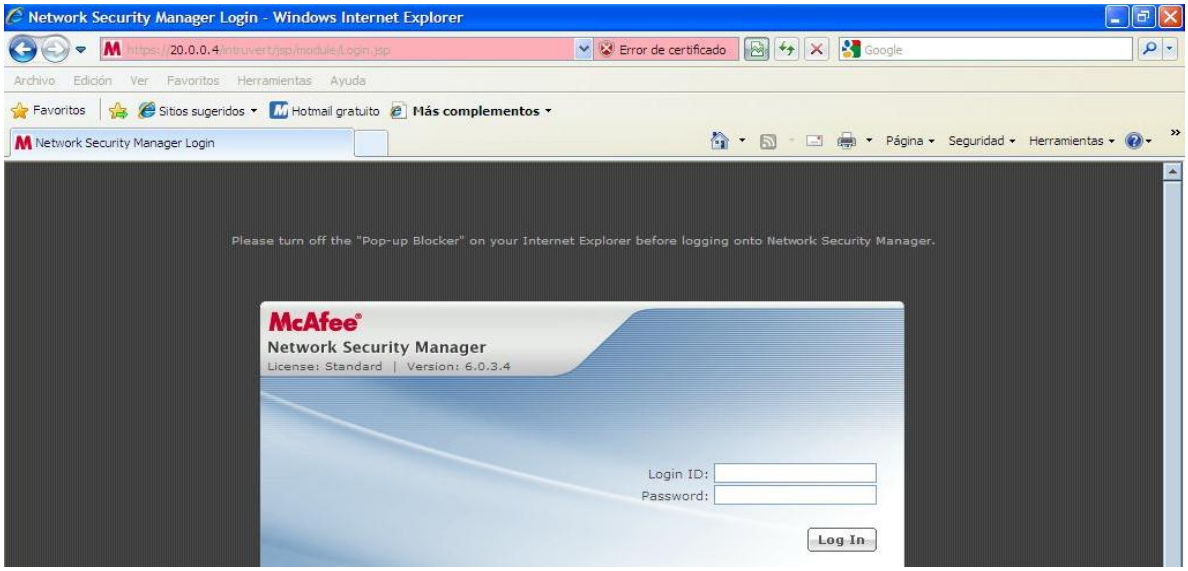

Figura 43. PANTALLA PARA INGRESAR LOGIN Y PASSWORD DEL USUARIO.

Como todo equipo de seguridad en redes y considerando lo delicado de los procesos de configuración, las cuentas de usuarios cuentan con diferentes privilegios, asignados por el administrador, cuenta que en este momento se usa.

Ya superado el proceso de autenticación nos encontraremos con la pantalla principal de la plataforma (***FIGURA 44***) desde aquí podemos llevar a cabo prácticamente todas las tareas necesarias para realizar un análisis en seguridad de los procesos que se ejecutan en nuestra red.

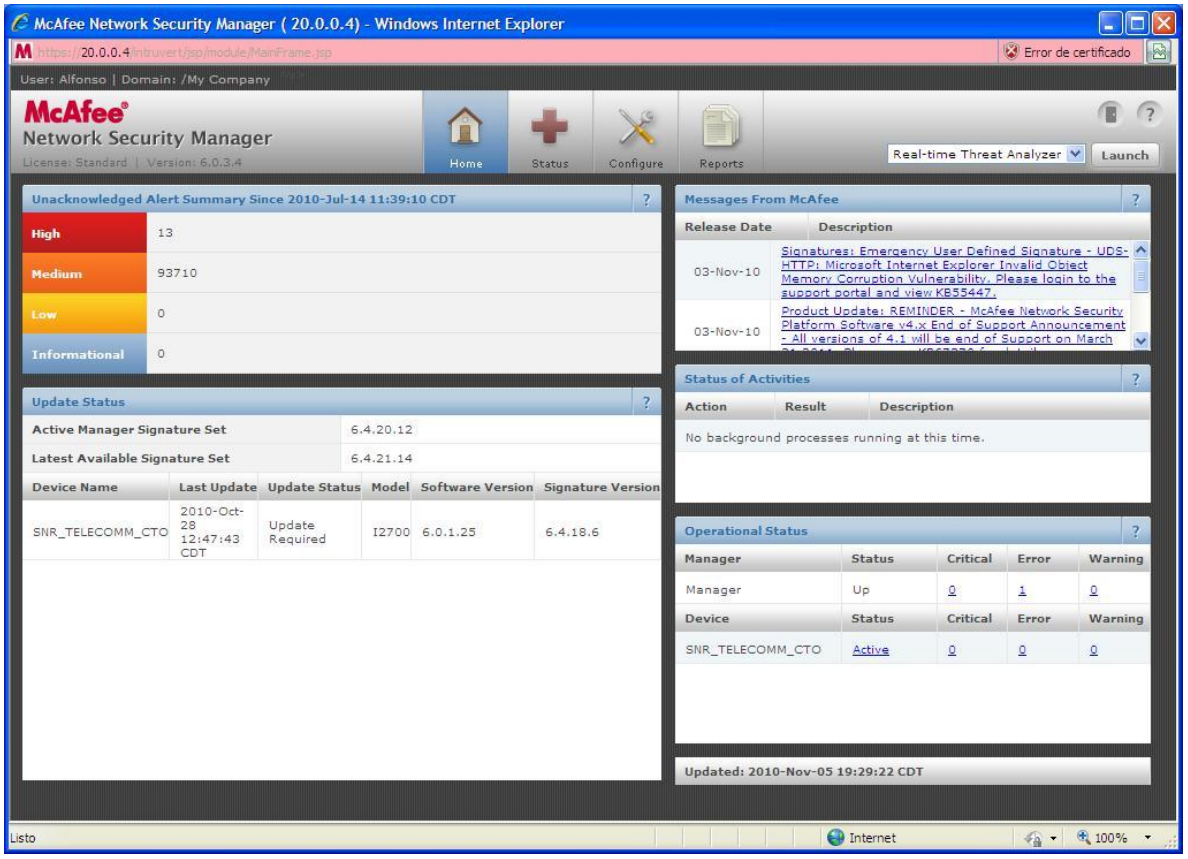

Figura 44. PANTALLA PRINCIPAL DE LA CONSOLA Mcafee IntruShield.

En esta pantalla principal encontraremos en la parte superior la barra de menú de forma gráfica con 4 iconos y una lista desplegable, en esta sección podremos acceder a las principales funciones de la plataforma, para su operación y configuración. Nótese que en esta misma zona del programa al extremo derecho se tiene un botón “Launch”, con el uso de este botón se despliega una de las herramientas más potentes de esta consola; un analizador en tiempo real de forma gráfica, el cual tiene acceso a la base de datos de la plataforma con registros de hasta más de 2 años hacia atrás en consideración a la fecha en uso.

Después de la barra de menú tenemos un identificador gráfico en una zona de cuatro colores diferentes, dicho identificador enumera los diferentes

sucesos que se han llevado a cabo agrupándolos y clasificándolos por prioridades. Al lado derecho se tiene un log detallado de los procesos que han sido llevado a cabo, puede decirse que es el detalle textual de las alarmas graficas que aparecen a su izquierda, este log guarda información de cambios en la configuración de la plataforma y obviamente no es posible editarlo, este resulta ser útil para identificar fallos en la ejecución de comandos por parte del administrador de la red.
Por último en la parte inferior de la pantalla tenemos información sobre el sensor que está en operación. Para obtener más detalles sobre el sensor que se encuentra trabajando podemos desde los iconos de la barra de menú en la parte superior dirigirnos a la opción "*Status*" (***FIGURA 45***), podremos observar una pantalla que contiene datos como:

- Status del sensor de la plataforma.
- Número de alarmas en total y por severidad.
- Status de la base de datos de la plataforma.
- Nombre del sensor y estado de operación.

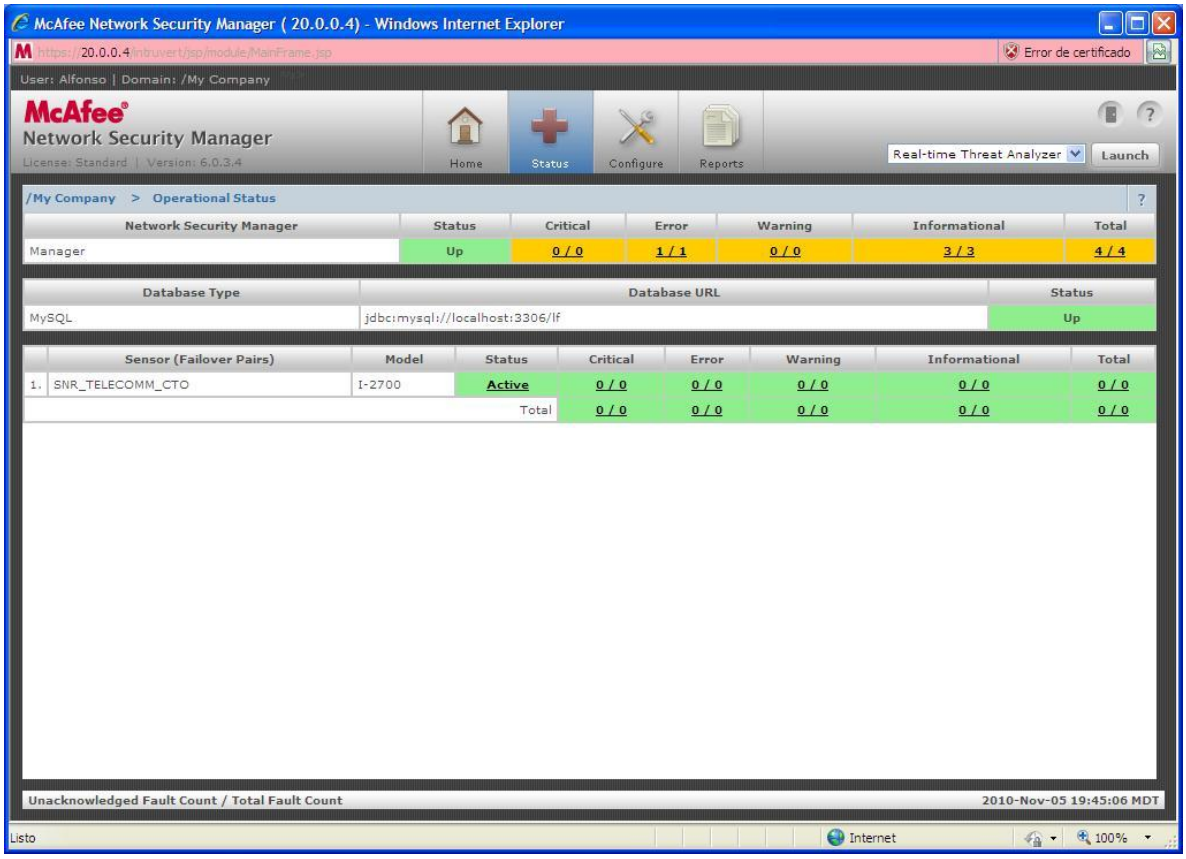

Figura 45. PANTALLA CON DATOS DEL SENSOR DE LA CONSOLA Mcafee IntruShield.

La información sobre el sensor y la base de datos es de gran importancia pues si alguno de estos dos elementos falla, la información generada por la plataforma será comprometida y no podrá validarse su autenticidad para la administración de la red donde opera.

Ahora bien, hablando sobre la opción “Reports” es probablemente una de las herramientas más poderosas que se tienen dentro de la plataforma, al ingresar a esta opción (***FIGURA 46***) podemos encontrarnos una gran cantidad de opciones para generar diferentes tipos de reportes, algunos de ellos son plantillas que ya se encuentran predefinidos y no siempre la información que contienen es completamente necesaria para el desarrollo de nuestro trabajo.
Una de las opciones más nobles y con la que se trabajar comúnmente es la llamada “*Top N Attacks*”, la cual contiene varias opciones de configuración.

Figura 46. PANTALLA PARA ELEGIR TIPO DE REPORTE EN CONSOLA Mcafee IntruShield.

Al elegir la opción “*Top N Attacks*” encontraremos una pantalla (***FIGURA 47***) con los diferentes parámetros que se pueden configurar para el reporte.

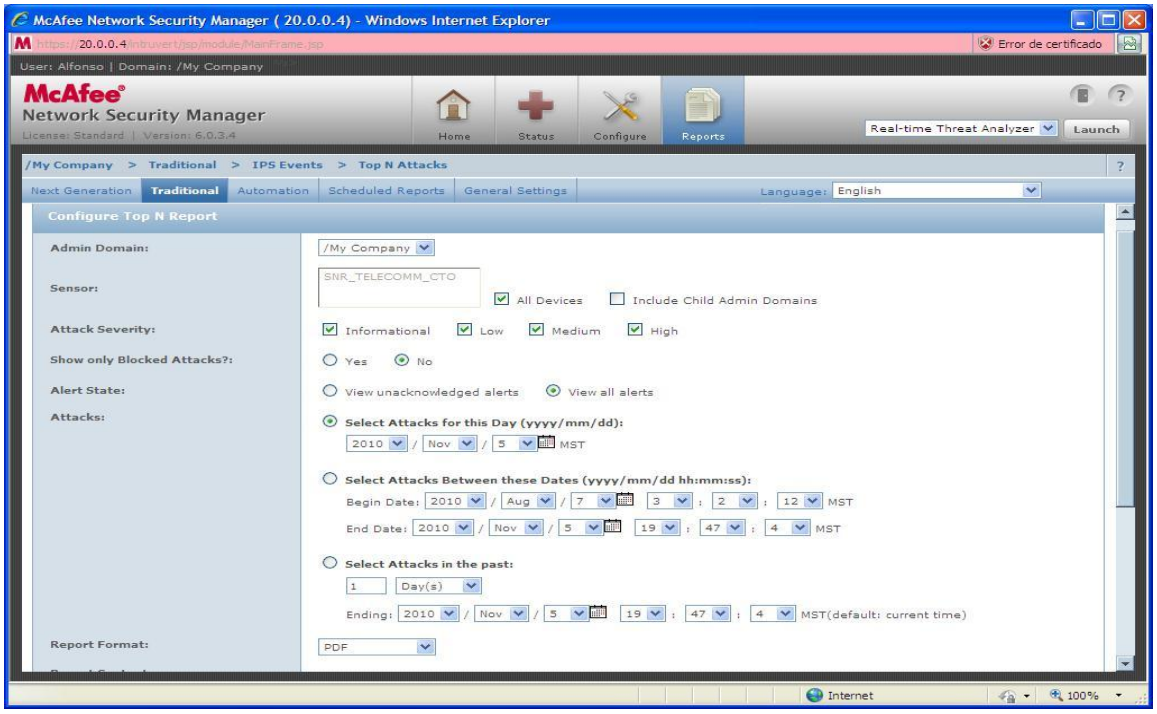

Figura 47. PANTALLA PARA CONFIGUAR REPORTE EN CONSOLA Mcafee IntruShield.

Entre los parámetros que son configurados por el usuario y a su vez hace que la herramienta sea de gran utilidad encontramos:

- Mostrar la severidad en la que se agrupa la alerta en seguridad informática.
- Mostrar si el ataque es bloqueado o no por la plataforma.
- Indicar el período de tiempo que el reporte abarca, para que este acceda a su base de datos y extraiga la información.
- Indicar en que formato queremos que se genere el reporte.

A continuación (***FIGURA 48***) se presenta un reporte generado por la plataforma Mcafee IntruShield:

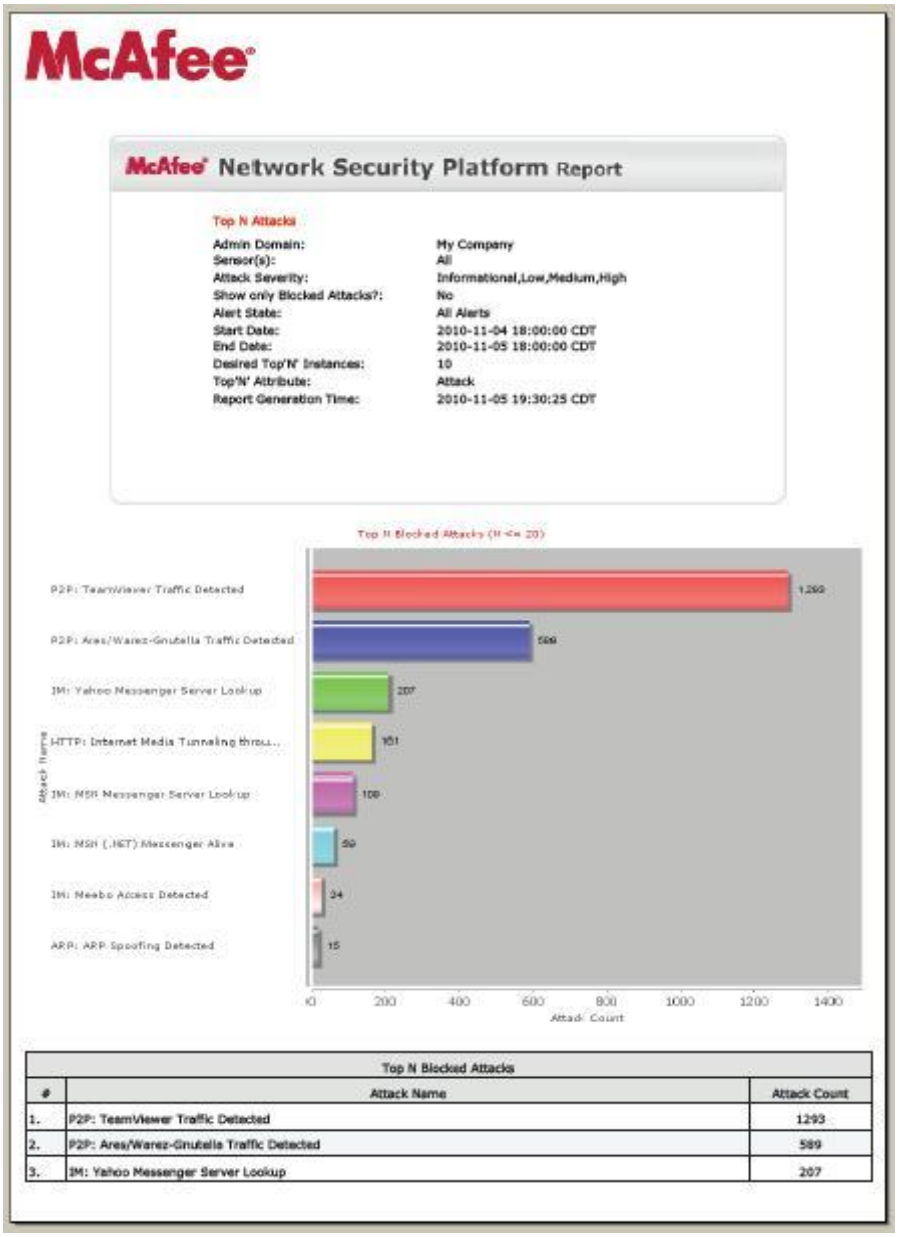

Figura 48. REPORTE GENERADO EN LA CONSOLA Mcafee IntruShield.

En resumen con el uso de esta herramienta es posible:

- Detectar los procesos que provoquen alertas en seguridad informática.
- Clasificar por grado de peligrosidad las alertas disparadas.
- Clasificar las alertas en seguridad informática y con esto separar las alertas que son generadas por un falso – positivo.
- Permite mantener un control del número de alertas que son generadas por hora, día, semana, mes e incluso año y con esto se tiene un mejor panorama de los hábitos y vulnerabilidades de nuestra red.

4.3 NETSCOUPE.

Esta plataforma se encarga de monitorear de una forma muy detallada el tráfico de una red en específico y para ello se tiene destinado toda una consola (hardware) además de la interfaz por medio de la cual el administrador de la red podrá interactuar con toda la plataforma.

Las características generales de esta plataforma son:

Nombre	NetScoute
Versión	Enterprise 5.3
Licencia	Shaware
Idioma	Inglés
Desarrollador	NetScoute & Juniper
Sitio	http://www.netscout.com/Pages/default.aspx

TABLA 3. CARACTERISTICAS DE LA PLATAFORMA NetScoute.

El trabajo con la plataforma NetScoute es sumamente minucioso al momento de su configuración y operación, es recomendable dejar su trabajo automatizado al máximo y analizar al final del día los datos obtenidos en los reportes que son generados y enviados a las cuentas de correo electrónico que se hayan definido en la instalación de la plataforma, dichos datos son:

- Utilización del ancho de banda de un enlace de comunicación en específico.
- Tráfico de las principales aplicaciones que circulan por la red.
- Información sobre las 10 principales conversaciones que se dan entre los equipos dentro de la red que se monitorea.
- Información sobre los 10 principales hosts que están generando tráfico dentro de la red.

Como podemos darnos cuenta esta plataforma agrupa un gran número de herramientas que sin duda alguna serán de gran utilidad para poder llevar a cabo una correcta administración de nuestra red y además facilitar la detección de fallas o áreas de oportunidad que estén presentes.

Ahora analizare brevemente cada una de las herramientas que podemos ver plasmadas en los reportes que la plataforma nos brinda.

1.- Utilización del ancho de banda: esta herramienta mostrara de forma gráfica el porcentaje de ancho de banda que se está utilizando en un período de tiempo determinado (***Figura 48***), en este caso se tiene configurado un monitoreo de 12 horas continuas iniciando a las 9:00 am y concluyendo a las 21:00 pm con esto se contemplan todas las posibles horas pico que se tengan a lo largo del día:

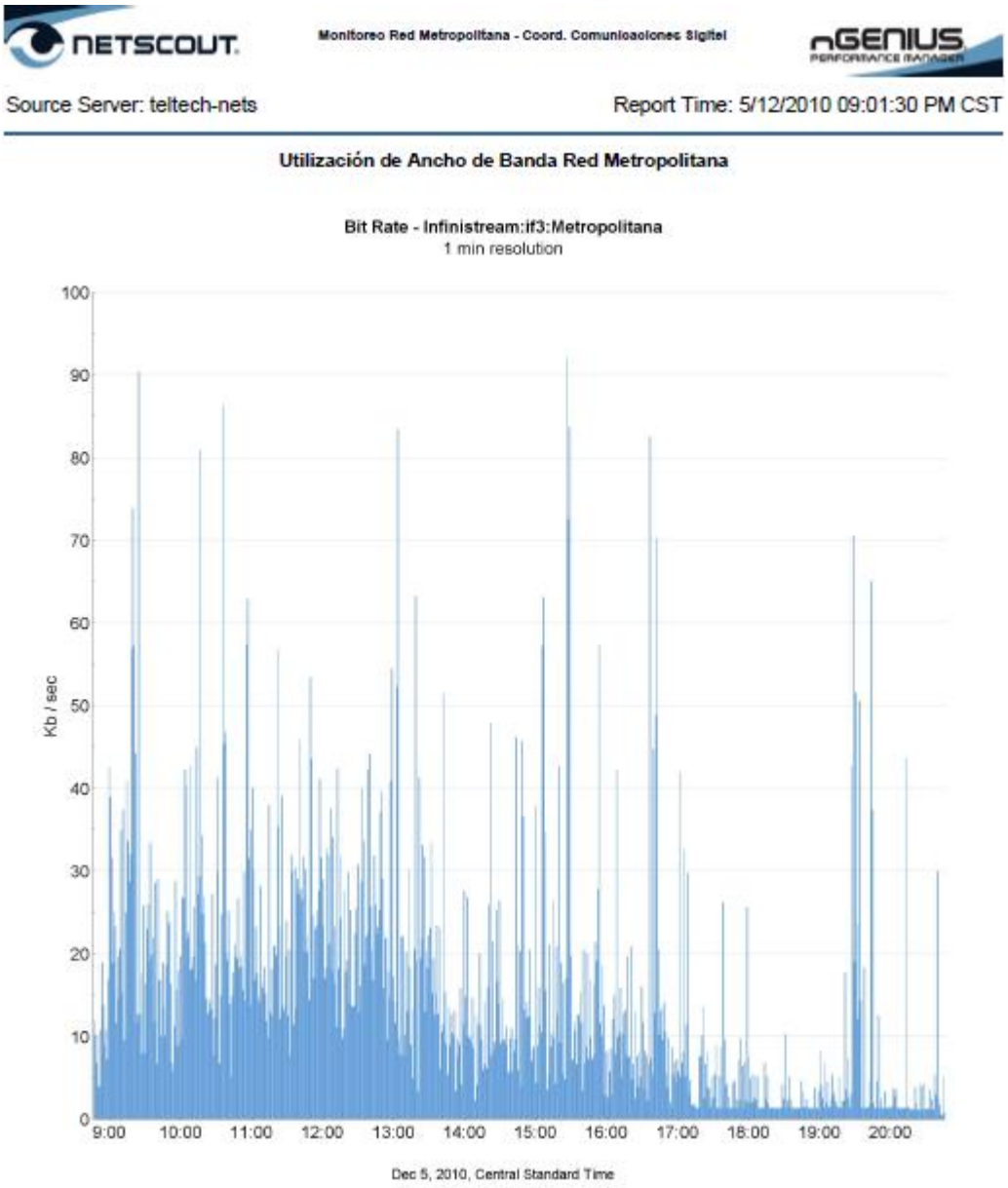

Figura 49. MONITOREO DE ANCHO DE BANDA CON LA PLATAFORMA NetScoute.

El grafico que la plataforma arroja nos muestra los Kb/sec contra el tiempo, aquí solamente podremos ver si el ancho de banda que se tiene destinado es o no suficiente para la operación o demanda de servicios que se tenga.

2.- Tráfico de las principales aplicaciones: Una vez obtenido el ancho de banda que se está consumiendo es interesante saber que aplicaciones están provocando dicho consumo de ancho de banda (***Figura 49***), un ejemplo de esta grafica se muestra a continuación:

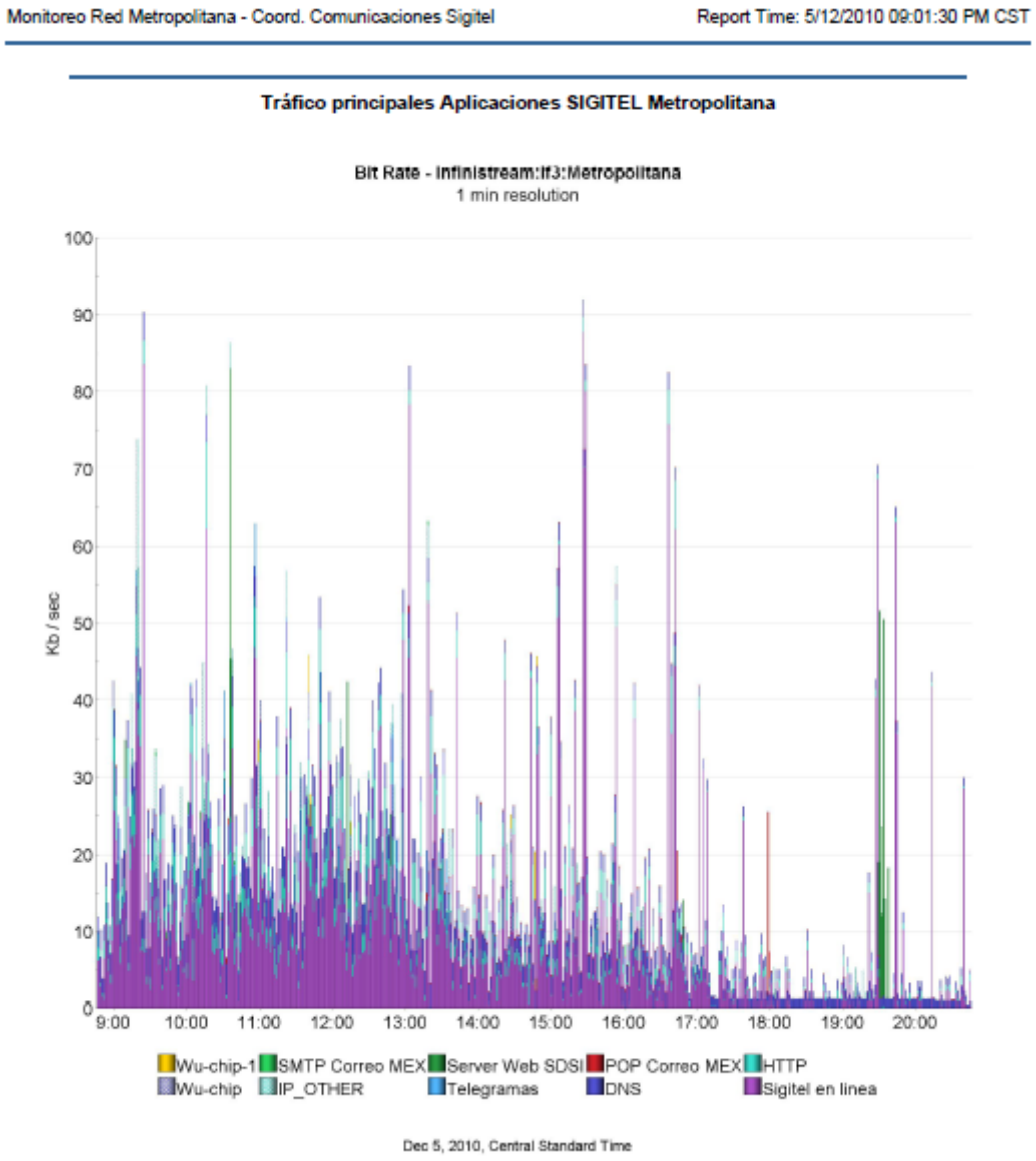

Figura 50. MONITOREO DE TRAFICO DE LAS PRINCIPALES APLICACIONES NetScoute.

El grafico que la plataforma muestra es el mismo al que se desplego en el porcentaje de utilización de ancho de banda pero ahora podemos ver que en el hay tramas de colores y cada una de esas tramas representa una aplicación que se ejecutó en ese lapso de tiempo.

Debajo de la gráfica podemos ver el nombre de las aplicaciones identificadas y el color que le fue asignado para su representación dentro del gráfico, esto nos ayudara a saber cuál de ellas provoca más tráfico en la red.

3.- Principales conversaciones: En esta grafica (***Figura 50***) la plataforma analiza el tráfico que se ha generado y reporta cuales han sido los dos equipos que más información han intercambiado entre sí en lo que se puede considerar una conversación entre hosts.

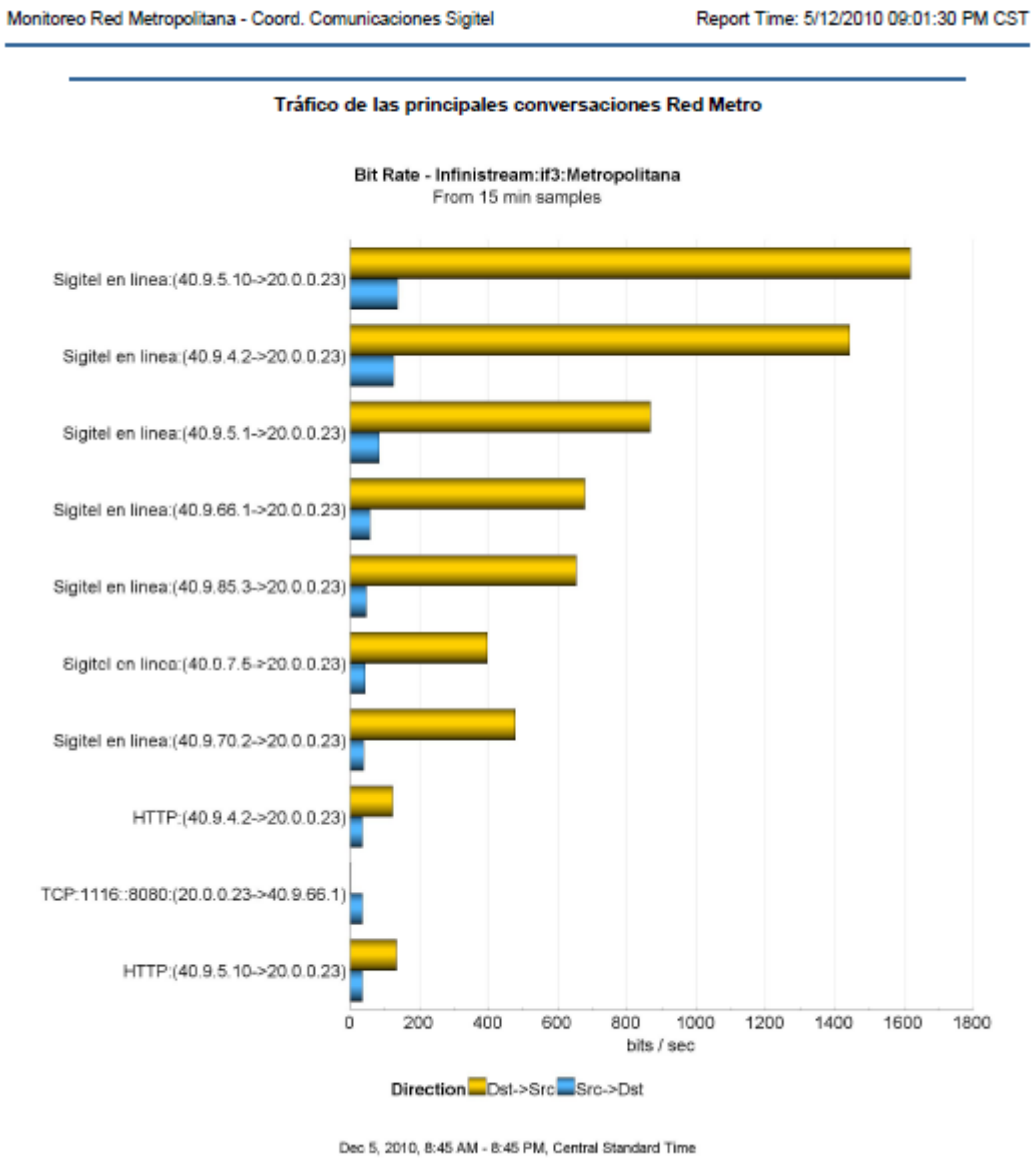

Figura 50. MONITOREO DE LAS PRINCIPALES CONVERSACIONES CON NetScoute.

El grafico muestra del lado izquierdo en un principio la dirección IP origen y después la dirección IP destino, seguido de esto mostrara el cálculo de bits/sec que en promedio empleo dicha conversación. La información que se obtiene con este grafico es de suma importancia pues de interpretar correctamente esta información podremos detectar incluso equipos que se encuentren infectados por algún virus y están generando trafico basura o bien, podemos detectar si un host dentro de nuestra red está generando más tráfico de

lo normal hacia alguno de nuestros servidores siendo que no sea esa su función principal del operador.

4.- Tráfico hacia los principales host's: Esta grafica muestra el ID del host en caso de tenerlo además de su dirección IP, seguido a estos datos nos muestra la representación gráfica de KB/sec que fueron empleados por dicho host para transmitir y para recibir información (***Figura 51***), a continuación se presenta un ejemplo de esta gráfica:

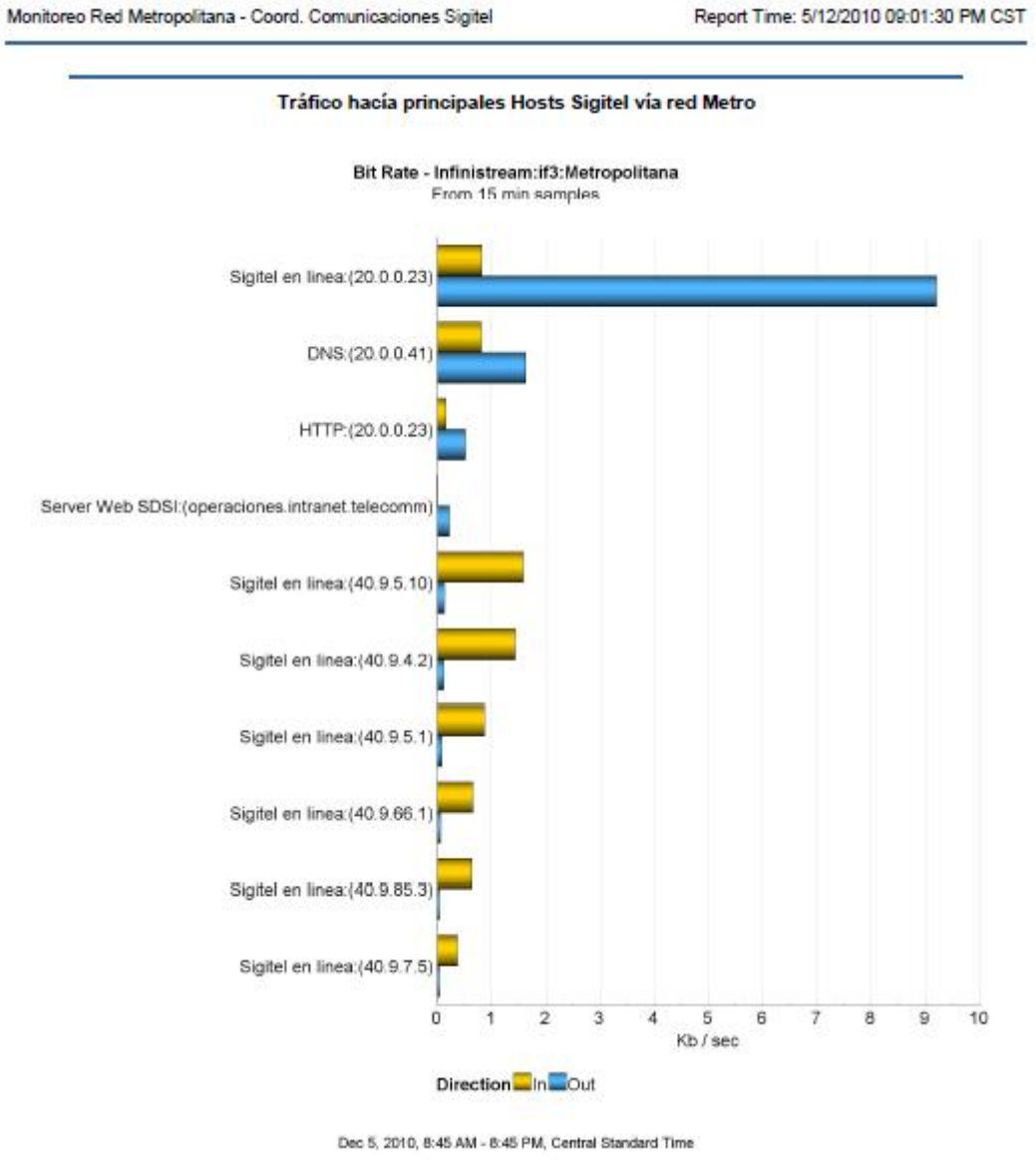

Figura 51. MONITOREO A LOS EQUIPOS QUE MAS TRAFICO GENERAN CON NetScoute.

Con este grafico podemos analizar el ancho de banda que emplean en específico nuestros principales equipos, aquí podemos detectar si algún host que no sea un servidor está consumiendo un ancho de banda superior a lo normal, esto nos puede indicar que el operador de dicha computadora está

haciendo tareas fuera de lo normal o bien que este se encuentra corrompiendo alguna de las políticas de seguridad y su alto consumo de ancho de banda se refiera a que está intercambiando archivos multimedia.

4.4 REAL TIME MANAGER.

La herramienta Real time Manager es un módulo que se vende por separado por parte de la empresa Mcafee y se instala sobre la plataforma Mcafee IntruShield para poder llevar a cabo un monitoreo en tiempo real, sus características se muestran a continuación:

Nombre	Real time Manager
Versión	Módulo for Enterprise
Licencia	Shaware
Idioma	Inglés
Desarrollador	Mcafee
Sitio	www.mcafee.com

TABLA 4. CARACTERISTICAS DE LA HERRAMIENTA Real time Manager.

Hasta el momento cuando se había trabajado con la plataforma Mcafee Intrushield se podía hacer el proceso para generar reportes sobre las alertas en seguridad informática en un espacio de tiempo determinado, esta acción conlleva el trabajo directo con los datos que son almacenados en la base de datos. Ahora veamos cómo podemos ver en tiempo real las alarmas que se disparan dentro de esta plataforma por procesos indebidos o vulnerabilidades en la seguridad de la red.

Para comenzar propiamente el trabajo con la herramienta Real time Manager deberemos de ingresar en primer término a la plataforma Mcafee Intrushield pues recordemos que esta nueva herramienta es un nuevo módulo de la plataforma, para ello nos logearemos con el nombre de usuario y contraseña que tengamos asignados, el proceso es el mismo al explicado en punto 4.2 del presente trabajo.

En la pantalla principal de la consola Mcafee (***FIGURA 52***) deberemos de hacer la petición para que se lance la herramienta Real time Manager en su esquina superior de lado derecho como se muestra a continuación:

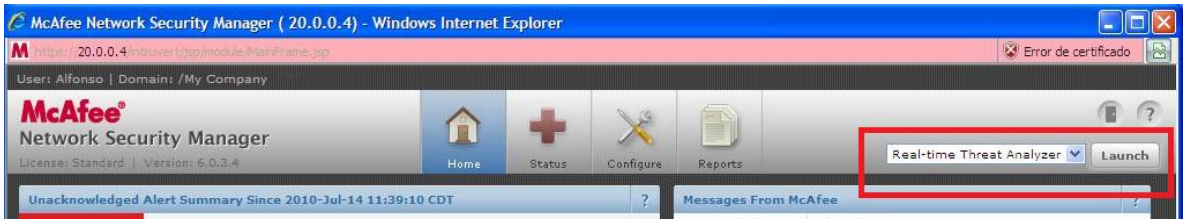

Figura 52. PANTALLA PARA EJECUTAR ANALIZADOR EN TIEMPO REAL.

Al elegir la opción "*Launch*" se iniciará la aplicación, para esto debemos de tener instalada la versión 5.0 o superior de JAVA, pues se trata de una aplicación de tipo cliente-servidor. Para instalar o verificar la versión de JAVA con la que se cuenta en el equipo se puede acceder al sitio en internet del fabricante http://www.java.com/es/download/

Una vez que la JVM de Java ("Java Virtual Machine") haya ejecutado los procesos necesarios para cargar la aplicación nos encontraremos con la pantalla principal de la herramienta Real time Manager (***Figura 53***), en la pantalla principal encontraremos datos de gran interés para la operación de la herramienta.

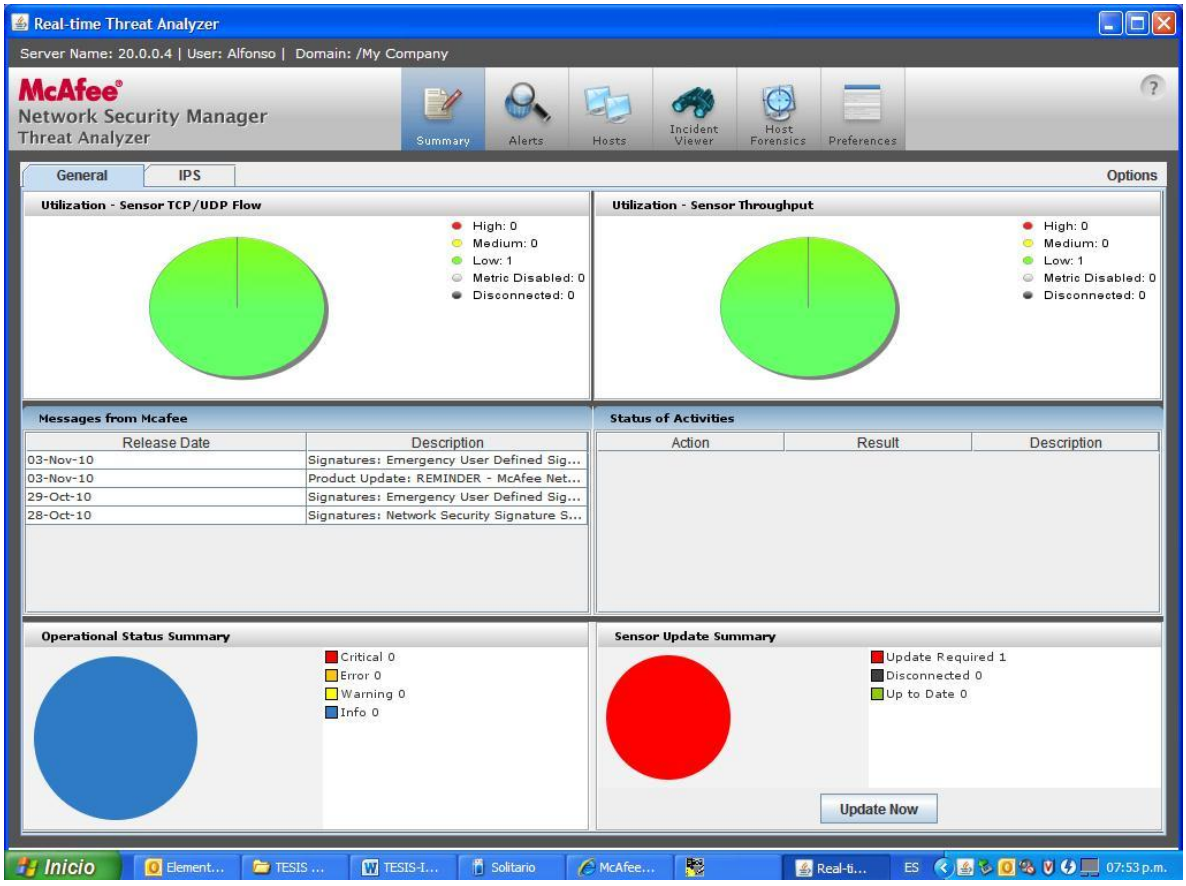

Figura 53. PANTALLA PRINCIPLA DEL ANALIZADOR EN TIEMPO REAL.

En la pantalla principal del analizador en tiempo real (***FIGURA 53***) encontraremos una serie de gráficas que nos indicaran cual es el desempeño de la plataforma y de los sensores que se encuentran en operación, esto es conocido como performance del equipo, se trata de la directa relación que existe entre el desempeño del hardware y software de la plataforma con la carga de trabajo a la que está sometida toda la plataforma.

Dentro de esta pantalla principal también podemos encontrar:

- Representación gráfica de las alertas en seguridad informática que se han presentado y clasificadas por grado de severidad.
- Log sobre los cambios hechos en el servidor.
- Aviso sobre actualizaciones disponibles para alguno de los sensores que está en operación.
- Log de actualizaciones realizadas en la consola de trabajo.

La pantalla que nos interesa a nosotros se encuentra ubicad en la pestaña "*IPS*", al ingresar a esta opción veremos de manera gráfica las alertas en seguridad informática en tiempo real que se están presentando (***FIGURA 54***) en la red:

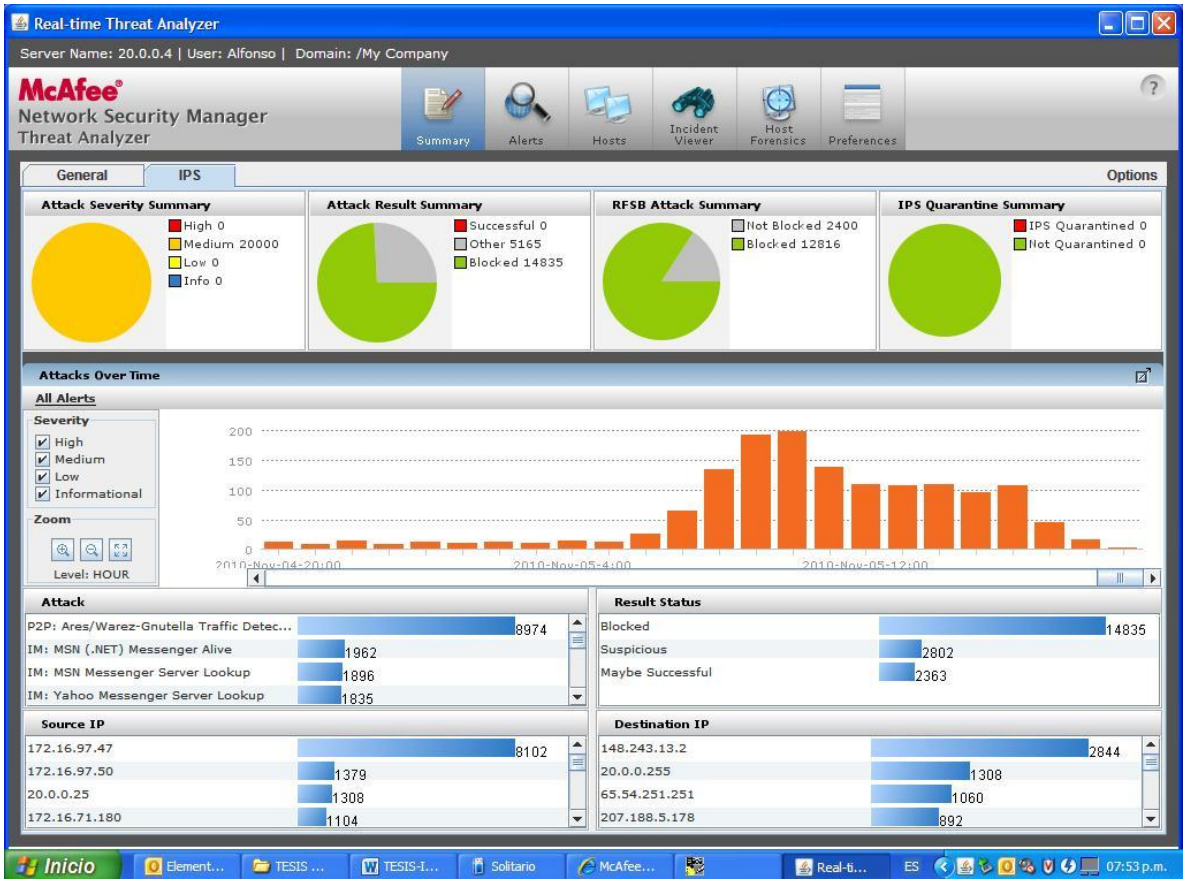

Figura 54. PANTALLA CON ALERTAS EN SEGURIDAD INFORMATICA EN TIEMPO REAL.

En esta pantalla encontraremos en la parte superior representado con gráficas de pastel la siguiente información:

- Número de alertas en seguridad informática clasificadas por severidad.
- Número de ataques que han sido realizados hacia la red, clasificándolos por satisfactorios, bloqueados y resultados desconocidos.
- Número de ataques que pudieron ser bloqueados por la consola.

- Número de direcciones IP que están en cuarentena en la red, esto debido a una posible infección por parte de un virus.

El siguiente segmento es al centro de la pantalla una línea de tiempo donde se está representando en una gráfica de barras el número de alertas en seguridad informática que se están generando en tiempo real, esto es la forma como representa la herramienta todos los eventos anormales que los sensores que se encuentran en operación han detectado. Al operar la consola es posible navegar a través de esta línea de tiempo y consultar el comportamiento en diferentes intervalos de tiempo.

Por último tenemos probablemente el segmento más importante o al menos el que nos brinda más detalles en cuanto a los sucesos que acontecen en nuestra red. Encontramos cuatro recuadros que nos indicarán:

- El número de veces que se ha suscitado una alerta en seguridad informática en específico.
- El número de alertas en seguridad informática que han sido bloqueadas, las que no han podido ser bloqueadas y por último aquellas alertas que no han podido ser del todo analizadas y no se tiene la certeza de saber si fueron o no bloqueadas por la plataforma.
- Las direcciones IP origen que han provocado que se dispare algunos de los sensores y se lleva un contador para cada dirección IP.
- Las direcciones IP destino que son blanco de los procesos no permitidos en la red, de la misma manera se tiene un conteo sobre el número de veces que han sido blanco de un posible ataque.

Para obtener información más detallada además de tener la posibilidad de poder guardarla en un archivo de Excel podemos dar un clic derecho sobre el nombre de una alerta en seguridad informática en específico o bien sobre algunas de las direcciones IP origen o destino que se hayan registrado, aparecerá un menú emergente en donde se deberá de seleccionar la opción "Show Detail" y obtendremos un apantalla como la siguiente (***Figura 55***):

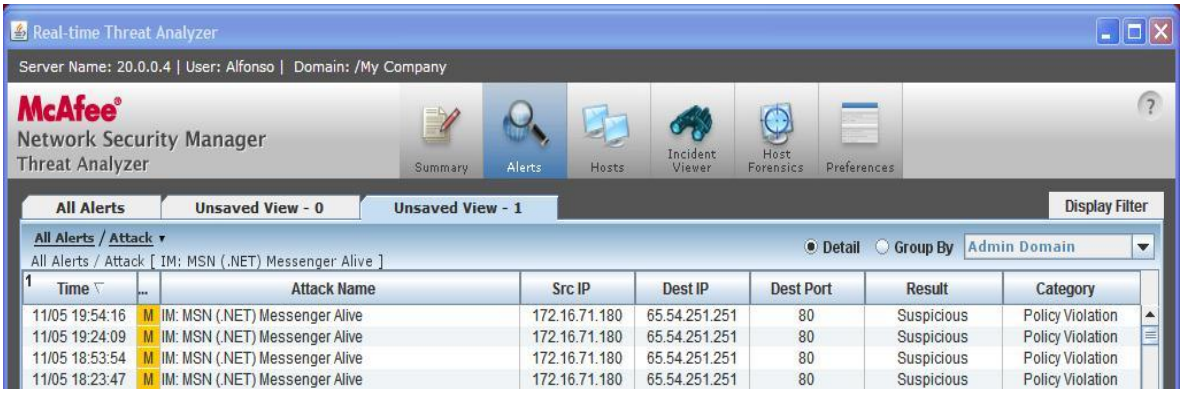

Figura 55. PANTALLA CON DETALLES DE ALERTAS EN SEGURIDAD INFORMATICA.

El contenido de esta pantalla es muy importante y además muestra todos los datos que como administradores de red necesitamos para corregir las vulnerabilidades que se tienen, encontraremos:

- Fecha y hora de cuando se generó la alerta en seguridad.
- Nombre de la alerta en seguridad que fue generada.
- Dirección IP origen que provoco la alerta.
- Dirección IP destino a donde estaba dirigido el tráfico que fue detectado como una posible amenaza.
- Número de puerto destino a donde se dirigía el tráfico comprometido.
- Resultado del ataque, es decir indica si fue o no exitoso.
- Por último muestra el nombre de la política que fue violada en el ataque.

CONCLUSIONES

Para finalizar con este trabajo de titulación abordare las conclusiones a las que he llegado y están sujetas tanto al objetivo principal como a los objetivos particulares que fueron planteados en un principio. Hablando concretamente del objetivo general de este trabajo recordemos que se formuló de la siguiente manera:

"*El correcto establecimiento de los mecanismos de seguridad y configuración de los mismos dentro de los equipos que intervendrán en la comunicación de las redes WAN permitirán un control detallado de los procesos y usuarios que se encuentren trabajando de forma remota dentro de las redes, evitando así comprometer la integridad de las redes*".

Con respecto a este objetivo puedo decir que fue cumplido y llevado a la práctica, en primer lugar fue necesario analizar el problema que se tenía y una vez analizadas también las posibles soluciones se optó por aquella que representaba un menor costo. Fundamental es dentro de nuestro objetivo general el correcto establecimiento y control de los procesos inherentes a la seguridad en las redes, considero que en los dos esquemas de comunicación que se estudiaron fue conseguido con éxito la meta de nuestro objetivo.

Especialmente en redes grandes como con las que se trabajó en este trabajo es fundamental cimentar desde un principio un correcto planteamiento de cómo será la operación al interior y exterior de las redes, obviamente todo esto se verá apoyado en aspectos de seguridad en base a procesos que fueron configurados y permiten que la administración de los enlaces de comunicación sean más fiables, dichos procesos son:

- Asignación de direcciones IP fijas.
- Establecimiento de ruteo estático.
- Uso de encapsulamientos en los procesos de ruteo.
- Creación de grupos de trabajo vía VLANs.
- Bloqueo de procesos vía Firewall.
- Establecimiento de herramientas de monitoreo y administración de las redes en operación.

En el último capítulo de este trabajo se abordaron las diferentes herramientas que se utilizan para monitorear y administrar los enlaces de comunicación, cabe hacer mención que el monitoreo y administración del que se habla se puede dar hacia dentro de la red (LAN) o bien hacia afuera de nuestra red (WAN) en base a la necesidad que se tenga, con esto se está mejorando la meta primaria que se había planteado en nuestro objetivo general donde se establece que se tendrá un control detallado de la comunicación en el extremo WAN de la comunicación.

El control detallado de los procesos que se dan dentro de nuestros enlaces de comunicación es posible y además de que también se tiene control de los usuarios que operan dentro de los mismos, para poder comprobar esto basta con ver los resultados que arrojan las diferentes herramientas y plataformas implementadas para el monitoreo de las redes.

Para terminar con lo referente al planteamiento que se realizó sobre nuestro objetivo general puedo concluir que este se cumplió y se superó a lo que en un principio se había planteado.

Ahora abordare las conclusiones a las que llegue para cada uno de los objetivos particulares que se plantearon:

1.- Comunicación entre los nodos principales de Telecomm, Inbursa y Banamex: Con respecto a este objetivo puedo decir que al establecer los enlaces de comunicación desde el nodo central de Telecomm hacia los otros dos nodos de las instituciones bancarias permitió trabajar con dos esquemas de comunicación diferentes, para la comunicación entre Telecomm – Inbursa se utilizó un "enlace dedicado" donde una tercera empresa que fue Telmex se encarga de proveer de carrier a la comunicación es decir que ambos nodos entregan su información a esta tercer empresa y es ella quien a través de toda su infraestructura hace que la información viaje de un nodo a otro. El segundo caso que fue la comunicación entre Telecomm – Banamex se utilizó un enlace vía VPN donde ahora la infraestructura será el internet, a pesar de utilizar como infraestructura un medio público como lo es internet; nuestra información se encuentra segura gracias al túnel virtual que la VPN crea. Si se debe de elegir entre uno de los dos esquemas de comunicación que se trabajaron en este trabajo se debe de poner en la balanza las bondades que cada uno de ellos nos da, el resultado final es el mismo en ambos casos (una comunicación exitosa) probablemente lo que haga que nos inclinemos por un esquema o por el otro sea el costo, un enlace de tipo VPN requiere una mayor inversión inicial pues se recomienda que la VPN sea implementada vía hardware y no solo software, mientras que el enlace dedicado lleva un menor costo inicial pero a un mediano y largo plazo su costo será mayor pues se debe de estar pagando un cifra mensual por el carrier que se está utilizando en el enlace de comunicación.

2.- Establecimiento de herramientas para el monitoreo de los enlaces de comunicación: Fue alcanzado con éxito este objetivo, las herramientas fueron implementadas y actualmente se pude realizar un monitoreo constante de todo lo que acontece en nuestra red, actualmente en internet existen muchas páginas y foros dedicaos exclusivamente a compartir experiencias sobre el desempeño de diferentes aplicaciones para la administración de redes. La correcta elección de una herramienta de administración no forzosamente se tiene que ver reflejada en la marca del desarrollador o mucho menos en su costo, podemos hacer la elección de una herramienta freeware, lo que si puedo recomendar es que se trate de una

herramienta que no este en versión beta, que se tenga un área de soporte y se puede apoyar uno de las opiniones que otros usuarios tengan al respecto.

3.- Creación de una VPN en sus diferentes fases: Sin duda alguna internet es el medio de comunicación al que cada día más personas tienen acceso y su uso dentro de las empresas es indispensable, esta es probablemente la mayor ventaja que tenga un enlace VPN, su implementación no es precisamente un proceso sencillo pero como toda nueva tecnología con el paso del tiempo y al presentarse una mayor demanda sobre su uso las empresas desarrolladoras de esta tecnología comenzaran a simplificar sus procesos de implementación. La creación de una VPN es un proceso no muy sencillo pero en gran parte se debe también al grado de seguridad que un enlace de tipo VPN nos brinda al momento en que está operando. Durante las XXXX fases que involucran su implementación se establece un túnel virtual cuya función es encriptar la información que viajara a través de internet para que esta no se legible para algún usuario no autorizado que pudiese llegar a interceptar alguna trama de nuestra comunicación.

4.- Estudio y aplicación del ruteo estático: El proceso de ruteo se ve involucrado en prácticamente todo el proceso de comunicación sin importar bajo que esquema se esté trabajando, no importa si es un enlace dedicado o bien si se trata de un enlace vía VPN, el hecho de hacer que nosotros elijamos la ruta que debe de seguir cada paquete de información dentro de nuestra red es de gran ventaja para mantener siempre un control sobre el flujo de información de nuestra red. En contra parte al ruteo estático se encuentra el ruteo dinámico y este en cuanto a beneficios para poner en marcha brinda muchas bondades, entre ellas que se puede hacer de forma automática y no se requiere llevar a cabo una planeación tan detallada de las rutas que se deben de seguir para entregar los paquetes de información dentro de la red, pero su principal desventaja radica también aquí, pues al entregar los paquetes de información por el camino que mejor consideren los equipos de ruteo no sabemos exactamente porque ruta se están enviando nuestros paquetes, de presentarse alguna falla sería más complicado poder detectarla al igual si se desea reemplazar alguno de los equipos de ruteo que se tengan instalados y operando. Puedo decir que personalmente prefiero el ruteo estático que si involucra un mayor trabajo para planear y configurarlo pero esto a un mediano y largo plazo traerá un mayor número de beneficios, además de que no se debe dejar de lado que la seguridad es parte fundamental en el entorno de trabajo de nuestra red, al hacer uso del ruteo estático se está condicionando a que la red también trabaje con direcciones IP fijas y se estaría dando solución a otro posible problema que surge con el uso de direcciones IP dinámicas, el primero de ellos es que se corre el riego de una duplicación de direcciones IP al ser una red grande como con la que estamos trabajando y el segundo de ellos es que evitamos que cualquier persona llegue y al encender su computadora se le genere una dirección IP dinámica y se conecte a nuestra red.

5.- Creación de grupos de trabajo utilizando switchs y VLANs: El uso de switches para segmentar una red y además crear grupos de trabajo es sin duda

una potente herramienta que servirá para administrar los procesos que se ejecutan en la red y el número de usuarios que tienen acceso a la red por cada área de trabajo. El uso de estos dispositivos es en la actualidad la forma más rápida y hasta cierto punto económica de hacer crecer en número de hosts de una red, principalmente hablando de lo que es el tamaño de la parte LAN. Existen en la actualidad equipos de ruteo que tratan de emular las tareas de un switch y además trabajan de forma inalámbrica, en lo personal no recomiendo el uso de estos dispositivos pues si bien dentro de sus tareas primarias esta la reducción de costos al tratar de evitar que se adquiera un switch se descuida en gran parte el segmento de seguridad que en nuestro trabajo ha sido fundamental y más cuando estamos trabajando procesos bancarios dentro de nuestras redes como ha sido el caso en los enlaces de comunicación expuestos en este trabajo. Al trabajar segmentando una red de manera inalámbrica se expone considerablemente la seguridad de nuestros datos pues actualmente un simple dispositivo como un Smartphone puede ser capaz de detectar las señales disponibles y con el uso de las herramientas adecuadas podría acceder de manera inalámbrica a nuestra red, además de que ataques internos como la suplantación de direcciones IP sería un problema recurrente y más difícil de poder detectar la fuente del ataque.

6.- Aplicación de permisos para bloquear procesos y usuarios en específico utilizando Firewalls: Personalmente considero que la tendencia a futuro en el hardware que se utiliza para trabajar con el tráfico de una red es reducir el número de dispositivos que actualmente se emplean y comenzar a agrupar en el menor número de dispositivos las funciones que cada uno de ellos realiza por separado, el firewall es el dispositivo que actualmente comienza llevar a cabo esta unión de servicios en un solo dispositivo. El firewall de la marca Juniper con el que se trabajó cuenta con funciones de ruteo, tiene la posibilidad de escalarse vía módulos de expansión para contar con un mayor número de puertos de red y además de las funciones de seguridad que indudablemente son las más importantes dentro de su función primaria. Con el uso de este dispositivo se facilita de suma manera el poder aplicar las reglas de seguridad en la red bajo la cual opera, pero considero que es estrictamente necesario el haber llevado a cabo una correcta planeación de las posibles vulnerabilidades que nuestra red pueda presentar, pues de nada servirá contar con la herramienta si el análisis que nosotros como administradores de red realizamos es deficiente.

7.- Establecimiento de herramientas para el monitoreo de procesos que puedan causar afectación en el funcionamiento de las redes: Lo más importante para seleccionar e implementar una herramienta de monitoreo fue en primer término determinar claramente que es lo que se deseaba saber sobre el comportamiento que nuestra red presenta. Es importante no perderse entre la amplia gama de herramientas que actualmente hay en el mercado y además no descartar a ninguna de ellas por el hecho de que sea freeware.

Sin duda alguna el trabajo que se ha expuesto a requerido de mucha investigación, practica y muchas horas de trabajo, considero que una gran ventaja han sido los recursos que han estado a mi disposición por parte de

Telecomunicaciones de México no por ello quiero decir que no existen áreas de oportunidad, pero el principal objetivo que desde un principio se plasmo ha sido conseguido satisfactoriamente.

GLOSARIO

B

Backbone. Se refiere a las principales conexiones troncales de Internet. Está compuesta de un gran número de routers comerciales, gubernamentales, universitarios y otros de gran capacidad interconectados que llevan los datos entre países, continentes y océanos del mundo.

Broadcast. Es un modo de transmisión de información donde un nodo emisor envía información a una multitud de nodos receptores de manera simultánea, sin necesidad de reproducir la misma transmisión nodo por nodo.

Browser. Un navegador web o explorador web (del inglés, *navigator* o *browser*) es una aplicación software que permite al usuario recuperar y visualizar documentos de hipertexto, comúnmente descritos en HTML, desde servidores web de todo el mundo a través de Internet.

C

Carrier. En su significado de portadora carrier es una señal o pulso transmitido a través de una línea de telecomunicación. Un carrier es también una empresa que opera en el sector de las telecomunicaciones ofreciendo servicios de telefonía.

C.T.O. Son las siglas del Centro Técnico Operativo del organismo TELECOMM, lugar donde reside el nodo principal de la red.

D

Datagrama. Un datagrama es un fragmento de paquete que es enviado con la suficiente información como para que la red pueda simplemente encaminar el fragmento hacia el receptor, de manera independiente a los fragmentos restantes. Ésto puede provocar una recomposición de forma desordenada o incompleta del paquete en el destino.

DLCI. Significa “Data Line Circuit Identification” es el equivalente a una dirección IP de una computadora pero aplicado a un NTU.

E

Ethernet. Nombre de una tecnología de redes de computadoras de área local (LANs) basada en tramas de datos. El nombre viene del concepto físico de *ether*. Ethernet define las características de cableado y señalización de nivel físico y los formatos de trama del nivel de enlace de datos del modelo OSI. Ethernet se refiere a las redes de área local y dispositivos bajo el estándar IEEE 802.3

E1. Estándar CCITT (ITU-T) de transmisión plesincrona con velocidad de 2.048Mbps.

E2. Estándar CCITT (ITU-T) de transmisión plesincrona con velocidad de 8Mbps.

E3. Estándar CCITT (ITU-T) de transmisión plesincrona con velocidad de 34Mbps.

F

Frame Relay. Es una técnica de comunicación mediante retranmisión de tramas, 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. Son un método económico de enviar datos, convirtiéndolo en una alternativa a las líneas dedicadas. 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.

H

Half Duplex. Un sistema que es capaz de mantener una comunicación bidireccional , es decir que pueden transmitir en los dos sentidos, pero no de forma simultánea.

Host. Se hace referencia a un dispositivo conectado a una red informática. Puede ser una computadora, un servidor de archivos, un dispositivo de almacenamiento por red, una máquina de fax, impresora, etc.

I

IEEE. Corresponde a las siglas de *The Institute of Electrical and Electronics Engineers*, el Instituto de Ingenieros Eléctricos y Electrónicos, una asociación técnico-profesional mundial dedicada a la estandarización, entre otras cosas. Es la mayor asociación internacional sin fines de lucro formada por profesionales de las nuevas tecnologías, como ingenieros eléctricos, ingenieros en electrónica, científicos de la computación e ingenieros en telecomunicaciones, etc.

N

NTU. Los NTU o UTD (Network Terminal Unit) son unidades terminales de red, estos equipos permiten prestar servicios privados de voz, datos analógicos y de datos digitales.

O

OSI. La Organización Internacional para la Estandarización o International Organization for Standardization (ISO), es una organización internacional no gubernamental, compuesta por representantes de los organismos de normalización (ONs) nacionales, que produce normas internacionales industriales y comerciales.

P

Protocolo. Es el conjunto de reglas que especifican el intercambio de datos u órdenes durante la comunicación entre las entidades que forman parte de una red.

R

Red. Es un conjunto de computadoras y/o dispositivos conectados por enlaces, a través de medios físicos (medios guiados) ó inalámbricos (medios no guiados) y que comparten información (archivos), recursos (CD-ROM, impresoras, etc.) y servicios (e-mail, chat, juegos), etc.

S

S.C.T. Son las siglas para nombrar a la Secretaría de Comunicaciones y Transportes en México.

Servidor. Software o Hardware en el que se ejecuta un programa que realiza alguna tarea en beneficio de otras aplicaciones llamada clientes.

SNMP. Protocolo de gestión de red, para supervisar equipos de comunicaciones a distancia.

T

T.C.T. Son las siglas para hacer referencia a la Torre Central de Telecomunicaciones la cual pertenece a la Secretaría de Comunicaciones y Transportes en México.

Telecomm. Son las siglas para hacer referencia al organismo que se encarga de las Telecomunicaciones de México a nivel gubernamental y el cual depende de la Secretaría de Comunicaciones y Transportes.

Telecomunicaciones. Es una técnica consistente en transmitir un mensaje desde un punto a otro, normalmente con el atributo típico adicional de ser bidireccional. El término telecomunicación cubre todas las formas de comunicación a distancia, incluyendo radio, telegrafía, televisión, telefonía, transmisión de datos e interconexión de computadoras (redes).

Telnet. Es el nombre de un protocolo (y del programa informático que implementa el cliente) que sirve para acceder mediante una red a otra máquina, para manejarla como si estuviéramos sentados delante de ella. Para que la conexión funcione, como en todos los servicios de Internet, la máquina a la que se acceda debe tener un programa especial que reciba y gestione las conexiones. El puerto que se utiliza generalmente es el 23.

TELSAT. Nombre de la red que alberga Telecomm en donde se encuentran sus administraciones en el interior de la República y utiliza comunicación vía satelital.

V

VPN. Es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada, como por ejemplo Internet. El ejemplo más común es la posibilidad de conectar dos o más sucursales de una empresa utilizando como vínculo Internet, permitir a los miembros del equipo de soporte

técnico la conexión desde su casa al centro de cómputo, o que un usuario pueda acceder a su equipo doméstico desde un sitio remoto, como por ejemplo un hotel.

Todo ésto utilizando la infraestructura de Internet. Para hacerlo posible de manera segura es necesario proveer los medios para garantizar la autenticación, integridad y confidencialidad de toda la comunicación.

BIBLIOGRAFÍA

Cheswick, Bill and Bellovin.
Firewalls and Internet security.
Addison – Wesley.

Uyless Black
Redes de Computadoras
Macrobit

Hunt, Craig
TCP/IP Network Administration. Second Edition.
O'Reilly

Rainer Handel, Manfred N. Huber and Stefan Shroder
ATM Networks – Concept, Protocols, Applications, Second Edition
Addison Wesley

Mason, Andrew G.
Redes privadas virtuales de Cisco Secure.
Trad Cisco Secure Private Networks
Pearson, 2006.

William Stalling
Handbook of Computer – Comunications Standards, Volumen 3
Howard W. Sam & Company

Zwicky, Cooper & Chapman
Building Internet Firewalls
O'Reilly

James D. Solomon
Mobile IP
Prentice Hall

SITIOS DE INTERES EN INTERNET

http://www.3com.es/

http://www.checkpoint.com/index.html

http://www.cisco.com/mx/index.shtml

http://www.computer.org/portal/site/ieeecs/index.jsp

http://www.dvsinfo.com/

http://www.ieee.org/portal/site

http://www.ipmonitor.com/default.aspx

http://www.juniper.net/training/index.html?from=HomePage-Header-to-Education

http://www.ntop.org/ntop.html

http://www.redaccionvirtual.com/redaccion/default.asp

http://www.telecomm.net.mx/

http://www.vgg.sci.uma.es/redes/