ESTUDIO E IMPLEMENTACIÓN DE LA RED VPN ARKA S.A

FREDY MESA ROMO

UNIVERSIDAD AUTÓNOMA DE OCCIDENTE
FACULTAD DE INGENIERÍA
DEPARTAMENTO DE CIENCIAS DE LA INFORMACION
PROGRAMA INGENIERÍA INFORMATICA
SANTIAGO DE CALI
2008

ESTUDIO E IMPLEMENTACIÓN DE LA RED VPN ARKA S.A

FREDY MESA ROMO

Pasantía para optar al título de Ingeniero Informático

Director
OSCAR HERNAN MONDRAGÓN MARTINEZ
Ingeniero en Electrónica y Telecomunicaciones
Master In Wireless Systems And Related Technologies

UNIVERSIDAD AUTÓNOMA DE OCCIDENTE
FACULTAD DE INGENIERÍA
DEPARTAMENTO DE CIENCIAS DE LA INFORMACION
PROGRAMA INGENIERÍA INFORMATICA
SANTIAGO DE CALI
2008

Santiago de Cali, 04 de Diciembre
Nota de aceptación:

Aprobado por el Comité de Grado en cumplimiento de los requisitos exigidos por la Universidad Autónoma de Occidente para optar al título de Ingeniero Informático

OSCAR HERNAN MONDRAGÓN MARTINEZ
_____
Director

_____
Jurado

_____
Jurado

CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

Pág.

LISTA DE ANEXOS

GLOSARIO

ANCHO DE BANDA (BANDWIDTH): capacidad máxima de transmisión de un enlace. Usualmente se mide en bits por segundo (bps). Es uno de los recursos más caros de toda red y es uno de los temas principales hoy en día pues el ancho de banda es una limitante para el desarrollo de aplicaciones que requieren transferir grandes cantidades de información a muchos puntos diferentes (multimedia, por ejemplo).

APPLICATION: un programa que lleva a cabo una función directamente para un usuario. WWW, FTP, correo electrónico y Telnet son ejemplos de aplicaciones en el ámbito de Internet.

AUTENTICACION: (autentificación) verificación de la identidad de una persona o de un proceso para acceder a un recurso o poder realizar determinada actividad. También se aplica a la verificación de identidad de origen de un mensaje.

BITS PER SECOND (BPS): bits por segundo en comunicaciones asíncronas, medida de velocidad de transmisión de datos. En computación personal, a menudo se usan tasas de bps para medir el desempeño de módems y puertos seriales.

DATA COMUMUNICATION EQUIPMENT (DCE): equipo de comunicación de datos Término utilizado por la especificación que define el puerto serial estándar para describir la electrónica que conecta la computadora a un módem.

DATA TERMINAL EQUIPMENT (DTE): equipo de transmisión de datos término utilizado por la especificación que define el puerto serial estándar, para describir a la computadora conectada a un módem o fax-modem.

DEMONIO CIPE: es el encargado de montar el dispositivo virtual cipcbx, el ruteo de la maquina y establecer el túnel VPN entre el servidor y el cliente.

DESENCRIPTAR: decodificar los datos para obtener la información en claro.

ENCRIPTAR: codificar los datos en función a una clave.

FIREWALL (PARED DE FUEGO): mecanismo utilizado para proteger una red o computadora conectada a Internet de accesos no autorizados. Una firewall puede construirse con software, con hardware o con una combinación de ambos.

FRAME RELAY: protocolo de conmutación de paquetes de alta velocidad que proporciona una transmisión más rápida que X.25. Es más adecuada para la transferencia de datos e imágenes que para la voz.

GATEWAYS (PUERTA DE ACCESO): los gateways son una compuerta de intercomunicación que operan en las tres capas superiores del modelo OSI (sesión, presentación y aplicación). Ofrecen el mejor método para conectar segmentos de red y redes a mainframes.
Se selecciona un gateway cuando se tienen que interconectar sistemas que se construyeron totalmente con base en diferentes arquitecturas de comunicación.

INTERNET: (Internet, La Red) red de telecomunicaciones nacida en 1969 en los EE.UU. a la cual están conectadas millones de personas, organismos y empresas en todo el mundo, mayoritariamente en los países más desarrollados, y cuyo rápido desarrollo está teniendo importantes efectos sociales, económicos y culturales.

IP (INTERNET PROTOCOL; PROTOCOLO INTERNET): (Protocolo Internet) conjunto de reglas que regulan la transmisión de paquetes de datos a través de Internet. La versión actual es IPv4.

ISP (PROVEEDOR DE SERVICIOS INTERNET): proveedor de servicios de acceso a Internet, como característica fundamental, en su práctica totalidad. Habitualmente, no se limitan a dar tan sólo servicio de acceso, sino que facilitan otros servicios, como cuentas de correo o alojamiento de páginas Web en su servidor.

LAN (LOCAL AREA NETWORK; RED DE ÁREA LOCAL): conjunto de computadoras y otros dispositivos comunicados entre sí dentro de un área relativamente pequeña.

LOGS (***LOG = REGISTRO***): es un mecanismo estándar que se encarga de recoger los mensajes generados por los programas, aplicaciones y demonios y enviarlos a un destino predefinido.

OSI: modelo de referencia para la transmisión de información entre dos puntos de una red de telecomunicaciones. Define siete niveles que tienen lugar en los extremos del sistema.

PAQUETE DE SOFTWARE: serie de programas que se distribuyen conjuntamente.

PROTOCOLO: conjunto de directrices que regulan las comunicaciones entre hosts. Existen protocolos para diversas tareas: transferencia de archivos (en cualquier sentido), verificación de errores, control de flujo, etcétera.

PROTOCOLOS TCP: (*Protocolo de Control de Transmisión*) uno de los protocolos fundamentales en Internet Muchos programas dentro de una red de datos compuesta por computadoras pueden usar TCP para crear *conexiones* entre ellos a través de las cuales puede enviarse un flujo de datos.

PROTOCOLOS UDP: ofrece a las aplicaciones un mecanismo para enviar data gramas IP en bruto encapsulado sin tener que establecer una conexión.

PUTTY: programa gratuito para hacer Telnet y SSH, para conectarse a servidores remotos por línea de comandos.

RED: conjunto de equipos e instalaciones que permiten las telecomunicaciones entre dos o más clientes.

RED DE TELECOMUNICACIONES: estructura física de telecomunicaciones con accesos distribuidos. Puede ser punto a punto, por conmutación de paquetes o de circuitos, y tener capacidad (o no) de interconectividad con otras redes.

ROUTER (RUTEADOR): dispositivo físico o lógico que garantiza la conexión entre nodos y redes bajo protocolo TCP/IP. Es el encargado de que los paquetes de octetos (de información) lleguen a su destino.

SISTEMA OPERATIVO: conjunto de programas que se encarga de coordinar el funcionamiento de una computadora, cumpliendo la función de interfase entre los programas de aplicación, circuitos y dispositivos de una computadora. Algunos de los más conocidos son el Windows y UNIX.

TCP/IP (TRANSMISSION CONTROL PROTOCOL/INTERNET PROTOCOL; PROTOCOLO DE CONTROL DE COMUNICACIONES/PROTOCOLO INTERNET): conjunto de protocolos de comunicaciones desarrollado por la DARPA (Defense Advanced Research Projects Agency; Agencia de proyectos avanzados de investigación de defensa) a finales de la década de los 1970. TCP corresponde a la capa de transporte del modelo OSI (Modelo de referencia OSI) y ofrece la transmisión de datos, e IP corresponde a la capa de red y ofrece servicios de datagramas sin conexión. Su principal función es comunicar sistemas diferentes. Fueron diseñados inicialmente para ambientes Unix por Vinton G. Cerf y Robert E. Kahn

TRÁFICO: toda emisión, transmisión o recepción de signos, señales, datos, escritos, imágenes, voz, sonidos o información de cualquier naturaleza que se efectúe a través de una red de telecomunicaciones.

TRANSMISSION CONTROL PROTOCOL (TCP): Protocolo de Control de transmisión en Internet, protocolo (estándar) que permite que dos computadoras conectadas a Internet establezca una conexión confiable.

TUNNELING: proceso por el que se creo una conexión VPN entre ambos extremos a través de una red IP intermedia.

USER DATAGRAM PROTOCOL (UDP): Protocolo de Datagrama de Usuario uno de los protocolos fundamentales de Internet. UDP opera al mismo nivel que el protocolo de control de transmisión (TCP), pero tiene menos sobrecarga y es menos confiable.

VIRTUAL PRIVATE NETWORK (VPN): red privada virtual red muy segura para transmisiones de datos confidenciales (incluyendo transacciones electrónicas comerciales) que utiliza Internet como medio de transmisión.

WAN (WIDE AREA NETWORK; RED DE ÁREA AMPLIA): conjunto de computadoras y otros dispositivos comunicados entre sí colocados dentro de un espacio geográfico de amplias dimensiones.

WINDOWING: mecanismo de ventana que aprovecha el tiempo disponible después de que el transmisor envía el segmento de datos y donde este tiempo se usa para transmitir más datos y la cantidad de segmentos de datos (medida en bytes) que se le permite al transmisor enviar sin recibir, se llama ventana (window).

RESUMEN

Actualmente la empresa Arka S.A quien representa a Kokoriko para el sur occidente colombiano, cuenta con canales dedicados para la interconexión de sus diferentes sedes con la planta; por medio de estos se hace la transmisión y recepción de los domicilios desde el callcenter hacia los puntos de venta de forma automatizada.

Esta solución es entregada por un proveedor (Telecom), el cual tiene a su ves cuenta con tercero (Emcali) el cual provee la ultima milla de la solución; esta ultima a presentado los mayores inconvenientes lo que genera caídas del servicio retrasando la operación haciendo que el servicio sea inoperante generando perdida de dinero y lo mas importante su imagen ante los clientes.

Ante esta situación que es una constante se a plantea una nueva solución de conectividad para la empresa, la cual esta basada en el uso del Internet como medio de conexión sobre la cual se pretende montar un sistemas de VPNs(Red privada virtual), esta permitirá minimizar las caídas del servicio y reducir los costos las comunicaciones notablemente.

En este documento se recoge los motivos y razones por las cuales las Redes Privadas Virtuales están implantándose cada día con más fuerza en el ámbito de la comunicación de datos. También se razona y motiva la elección de un tipo concreto de Red Privada Virtual (CIPE), para su configuración, instalación y prueba.

Las VPNs son una alternativa práctica, segura y eficiente de los enlaces privados que en la actualidad son usados para interconectar redes corporativas y clientes remotos.

La seguridad de la red VPN será basada en IPTABLES con las que se pretende restringir el ingreso de ips deferentes a las permitidas por estas, por lo que solo permitirá acezar a usuarios de la VPN permitidos.

Finalmente se hará un informe de pruebas donde se evaluaran el funcionamiento de la VPN implementada, haciendo un análisis de del trafico, conexión y seguridad de la misma dando a conocer los resultados obtenidos.

INTRODUCCIÓN

Las grandes organizaciones en la actualidad poseen sedes remotas, surgiendo la necesidad de compartir la información para mantener los procesos centralizados permitiéndole al área administrativa llevar acabo cada una de sus tares, además de mantener una comunicación permanente con cada uno de estos puntos que pueden ubicarse en edificios, localidades, regiones y países.

Para cubrir esta demanda en un pasado no muy lejano aparecen las redes de área extensa (WAN) implementándose las interconexiones de muy distinta forma como por ejemplo Redes de telefónica conmutada, Frame Relay, etc.

En la actualidad con la aparición de la Internet y implementándose con tecnologías como la ADSL, surgen aplicaciones que utilizando este medio pueden transmitir la información entre distintos puntos separados geográficamente. El problema está en que no es una red segura y es 'fácil' el acceder a información confidencial y que en malas manos puede ser peligrosa. Por este motivo, en los últimos años se le da mucha importancia a la seguridad, el uso de la encriptación es común y las empresas buscan soluciones lo más eficaces y baratas posibles a la inseguridad de Internet. Para dar solución a estas demandas surgieron las VPN (*redes virtuales privadas)*.

Es una tecnología de red que permite la interconexión de varias redes locales (LAN, Local Área Network) separadas físicamente (remotas), que por medio de una red pública o no controlada (Internet) realizan transmisión de datos entre ellas permanentemente y de un volumen considerable.

Ahora bien, Arka S.A, es una empresa prestadora de servicios que representa una marca de gran trayectoria a nivel nacional e internacional actualmente, como lo es KOKORIKO para quien es de vital importancia mantener óptima calidad en el nivel de servicio y satisfacción del cliente externo e interno.

Para este fin las comunicaciones son vitales, ya que se deben garantizar la conexión y transmisión de datos entre los puntos de venta (sedes) y callcenter (central), para ello se requiere implementar una solución redundante que permita a la organización optimizar sus recursos informáticos y comunicaciones actuales generando ahorro.

Es por ello que se pretende lograr por medio del la red VPN, una comunicación rápida, segura utilizando herramientas como la autenticación y la encriptación de los datos y además garantizando una conectividad permanente entre cada punto o sede remota generando ahorro en las comunicación de la compañía.

1. ANALISIS DE LAS TECNOLOGIAS FRAME RELAY Y VPN.

La presente sección tiene como propósito entregar conocimientos básicos acerca de las tecnologías (VPN y FRAME RELAY), haciendo énfasis en las ventajas y desventajas de las mismas, se pretende dar a conocer el costo-beneficio que le pueden dar a la organización cada una de estas tecnologías de transmisión y recepción de datos.

En este orden de ideas y teniendo en cuenta que en la actualidad las grades compañías tienen sedes remotas, es de vital importancia garantizar una comunicación la cual sea permanente y que además la información este centralizada para proporcionar un mayor control de cada uno de los procesos que se ejecutan dentro y fuera de la empresa.

Para ello las empresas buscan alternativas que sean viables en costo, tiempo y seguridad permitiéndole el sostenimiento en el mercado.

El objetivo de esta sección es llevar acabo un análisis el cual nos permita establecer las ventajas y desventajas de cada una de estas tecnologías dando a conocer los motivos por los cuales la empresa Arka S.A. debe de hacer un cambio de tecnología en sus comunicaciones con cada uno de sus puntos de venta.

Finalmente se realizara una comparación de costo – beneficio el cual dará a conocer el ahorro que genera el cambio de tecnología y los beneficios que con lleva este.

1.2 TECNOLOGIA FRAME RELAY

FRAME RELAY es un protocolo WAN muy utilizado para enlaces dedicados, este trabaja en la capa física y de enlace de datos del modelo de referencia OSI y fue creado originalmente para trabajar en redes RDSI.

Consiste en una forma simplificada de la tecnología de conmutación de paquetes, permite compartir dinámicamente el medio así como también el ancho de banda disponible.

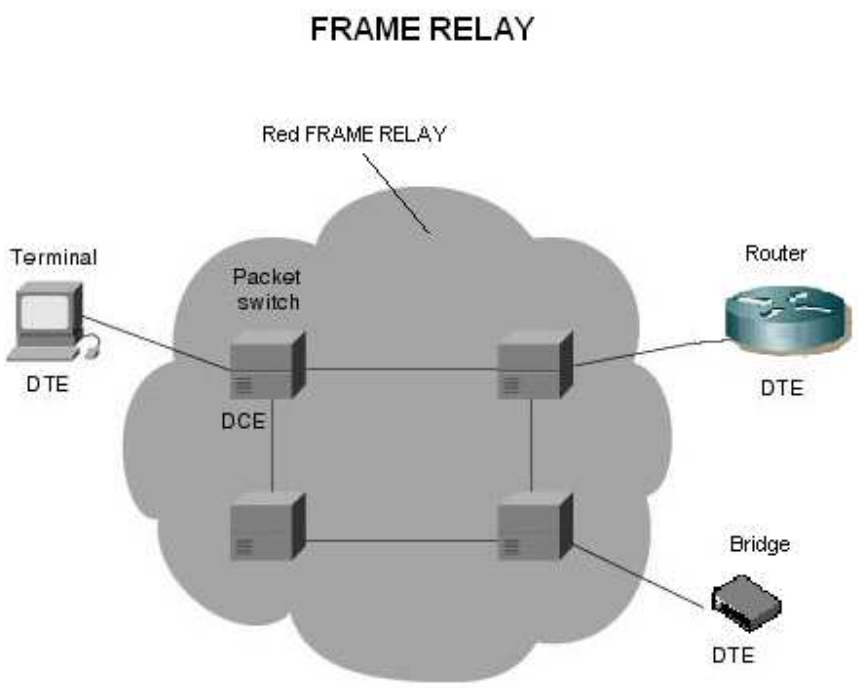
Frame Relay es una evolución de las redes X.25, donde se simplifica y se suprimen muchas de las funciones que hacían su antecesor como la retransmisión de paquetes perdidos ni windowing.

Los dispositivos que maneja la tecnología FRAME RELAY se dividen generalmente en dos categorías: Equipos terminales de datos (DTE) y Equipos Terminales de Circuitos de Datos (DCE); Los equipos DTE generalmente ponen fin a una red especifica, estos se ubican fuera de la red FRAME RELAY y habitualmente son equipos de los clientes, estos pueden ser computadoras personales, routers y bridges. Los equipos DCE son normalmente propiedad del proveedor del servicio, estos proporcionan servicios de conmutación de paquetes en la red y por lo general son packet switch o conmutadores de paquetes.

Las redes FRAME RELAY son redes WAN que generalmente se encuentran del lado del proveedor de la misma por lo que para los clientes, ya sea residenciales y/o corporativos son transparentes.

En el siguiente grafico se muestra un esquema básico de los dispositivos que interactúan en esta tecnología de red.

Figura 1. Dispositivos que interactúan en una red FRAME RELAY.



Fuente: SPAINER, Steve y STEVENSON, TIm. Tecnologías de interconectividad de redes. México: Editorial Prentice Hall, 1998, p. 38.

La interconexión entre un DTE y un DCE consiste de un componente de la capa física y un componente de la capa de enlace para establecer una conexión. El

componente de la capa física define las especificaciones eléctricas, mecánicas, funcionales y de procedimientos para la conexión entre los dispositivos y el componente de la capa de enlace define los protocolos que establecen la conexión entre un DTE (por ejemplo un router), y un DCE, (por ejemplo un switch).

1.2.1 Circuitos virtuales Frame Relay. Los enlaces Frame Relay son orientados a conexión, lo que significa que hay una comunicación definida entre cada par de dispositivos y en cada una de estas se asociada un identificador de conexión, los cuales son conexiones lógicas creadas entre dos dispositivos DTE a través de la red conmutada de paquetes Frame Relay.

Un circuito virtual Frame Relay es una conexión lógica creada entre dos o más dispositivos DCE (Equipos Terminales de Datos) a través de la red Frame Relay.
Los circuitos virtuales Frame Relay se dividen en dos categorías:

- Circuitos virtuales conmutados (SVCs)
- Circuitos virtuales permanentes (PVCs).

➢ **Circuitos virtuales conmutados (SVCs).** Son conexiones temporales y que se usan en situaciones donde la transferencia de datos entre un par de dispositivos DTE es esporádica a través de la red Frame Relay. Los SVCs tienen 4 estados operacionales:

- **Call Setup** (Establecimiento de la llamada): Cuando se establece el circuito virtual entre dos dispositivos DTE Frame Relay.

- **Data Transfer** (Transferencia de datos): Cuando los datos entre los dos DTEs son transmitidos sobre el circuito virtual.

- **Idle** (Ocioso): Cuando la conexión entre los dos DTEs está todavía activa, pero no hay tráfico de datos. Si por cierto periodo de tiempo el circuito se encuentra en este estado, se procede a terminar la conexión.

- **Call Termination** (Terminación de la llamada): Cuando Se da por terminado el circuito virtual entre los dispositivos DTE

Una vez finalizado un circuito virtual y los dispositivos DTEs necesitan transmitir más datos, se deberá establecer un nuevo SVC, y así sucesivamente.

➢ **Circuitos virtuales permanentes (PVCs).** Son conexiones establecidas en forma permanente y se utilizan en donde la transferencia de datos es frecuente y constante entre dispositivos DTE a través de la red Frame Relay. La comunicación

a través de un PVC no requiere los estados de establecimiento de llamada y finalización como los SVCs. Los PVCs tienen 2 estados operacionales:

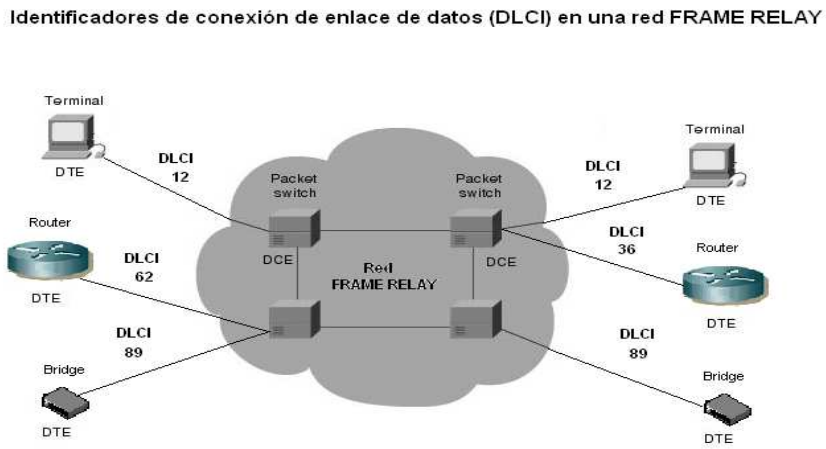
- **Data transfer** (Transferencia de datos): Cuando los datos entre los dos DTEs son transmitidos sobre el circuito virtual.

- **Idle** (Ocioso): Cuando no hay transferencia de datos, pero la conexión sigue activa. A diferencia de los SVCs, un PVC puede estar indefinidamente en este estado y el enlace no se darán por finalizados en ninguna circunstancia.

Los dispositivos DTE pueden comenzar la transferencia de datos en cuanto estén listos, pues el circuito está establecido de manera permanente.

1.2.2 Identificador de Conexión del Enlace de Datos. Los circuitos virtuales de Frame Relay se identifican a través de los DLCIs (Identificadores de Conexión del Enlace de Datos). Los valores de DLCI son asignados por el proveedor de los servicios y tienen solo significado local, lo que significa pueden haber varios DLCIs con el mismo valor, pero no puede haber varios DTEs con un mismo DLCI conectados al mismo Packet Switch.

Figura 2. Ejemplo Identificador de Conexión del Enlace de Datos en una red FRAME RELAY.



Fuente: SPAINER, Steve y STEVENSON, TIm. Tecnologías de interconectividad de redes. México: Editorial Prentice Hall, año, p. 40.

En la figura 2 muestra como que pueden existir valores DLCI repetidos pero estos no pueden estar conectados a un mismo Packet Switch, además los extremos PVC pueden tener valores diferentes.

La empresa ARKA S.A actualmente cuenta con una red de comunicaciones basada en la tecnología FRAME RELAY, Esto lo podemos ver en el Anexo A de este documento.

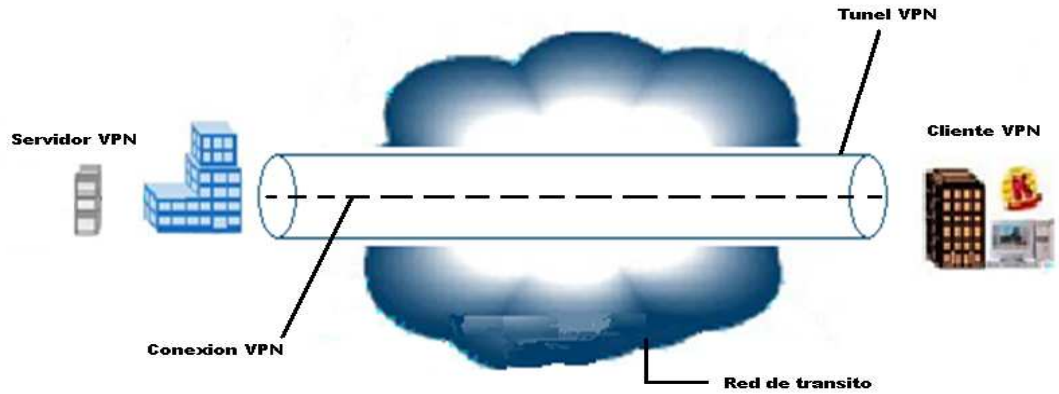
1.3 TECNOLOGIA VPN

VPN (Virtual Prívate Network) es una tecnología de red que tiene muchas de las ventajas que ofrece los canales privados o dedicados, la diferencia es que esta trabaja sobre una infraestructura publica donde las conexiones son transparentes y seguras a través de Internet.

Para cumplir este objetivo la VPN utiliza una técnica llamada tunneling, la cual consiste en capsular y encriptar los datos para que al salir a la red IP viajen seguros hasta su destino.

Para asegurar la privacidad de esta conexión los datos transmitidos entre emisor y el receptor son encriptados por el *Point-to-Point Protocol*, también conocido como PPP el cual utiliza algoritmos de encriptación para cifrar los datos y posteriormente son enrutados o encaminados sobre una conexión previa ya sea remota o LAN WAN por un dispositivo virtual.

Figura 3. Esquema básico de red VPN utilizando túnel.



En la grafica se muestra la manera de cómo se hace un enlace VPN con la técnica de tunneling entre un servidor y un cliente de la red VPN a través de la red de transito o publica (Internet).

1.3.1 Tecnología de las redes privadas virtuales. Antes de implementar la VPN hay que tener en cuenta su arquitectura ya que estas deben basarse en elementos esenciales de la tecnología para proteger la privacidad, mantener la calidad y confiabilidad, y asegurar la operatoria de la red en toda la empresa.

Los elementos que hay que tener en cuenta en las redes VPNs son, garantizar la seguridad usando túneles para que la información no vaya ser filtrada por algún intruso en la red publica, la encripción de datos para que solo los pueda ver el receptor del mismo, la autenticación de usuarios y paquetes y control de acceso.

La calidad del servicio es un elemento importante ya que haciendo uso de las colas, dando manejo a la congestión de la red, priorizando el tráfico y clasificando los paquetes que viajan a través del mismo se brinda una red eficiente para la organización.

Por ultimo debemos a lo largo de la VPN implementar políticas de seguridad que le permitan a la empresa minimizar el riesgo de ataques informáticos por terceros.

- **Redes Privadas Virtuales por Software.** Como se ha comentado con anterioridad, existe un amplio abanico de implementaciones de Redes Privadas Virtuales por Software. Pasaremos a describir las más utilizadas con sus ventajas e inconvenientes, para finalmente elegir aquella que más seguridad, fiabilidad y ventajas presente frente a las otras.

- **Redes Privadas Virtuales por Software más comunes.** De todos los tipos disponibles, podemos citar por ser las más utilizadas.

- **IPSec:** IPSec (Protocolo de seguridad en IP), es en realidad una colección de protocolos diseñada por la Internet Engineering Task Forse (IETF) para proporcionar seguridad a los paquetes de nivel de red. Inicialmente se desarrolló para usarse con el estándar IPv6 y posteriormente se adaptó a IPv4 como una alternativa de seguridad en IP.

IPsec Añade los servicios de autenticación y cifrado por lo que ayuda a crear paquetes autenticados y confidenciales para el nivel y protocolo IP. IPSec actúa dentro del modelo OSI en la capa 3 (capa de red). No está ligado a ningún algoritmo de encriptación o autenticación, tecnología de claves o algoritmos de seguridad específico.

IPsec funciona de dos modos distintos ya que puede trabajar en modo túnel y en modo transporte, la diferencia de estos dos modos es que en el modo transporte no protege la cabecera IP, solo protege la información que viaja del nivel de transporte y en el modo túnel protege el paquete IP completo.

IPSec se compone de dos protocolos de seguridad distintos los cuales son AH (cabecera de autenticación) donde este ofrece la autenticación, la integridad y la anti-repetición, el otro protocolo es ESP (sobrecarga de seguridad de la encapsulación) este ofrece los mismos servicios el anterior pero con encriptación de datos.

- **PPTP:** El PPTP es un protocolo de red que permite el tráfico seguro de datos desde un cliente remoto a un servidor corporativo privado, estableciéndose así una Red Privada Virtual (VPN) basada en TCP/IP.

El protocolo de tunneling punto a punto (PPTP) soporta múltiples protocolos de red (IP, IPX y NetBEUI) y puede ser utilizado para establecer redes virtuales a través de redes públicas o privadas como líneas telefónicas, redes de área local o extensa (LAN's y WAN's) e Internet u otras redes públicas basadas en TCP/IP.

- **L2TP:** L2TP (Layer 2 Tunneling Protocol) este protocolo se emplea para crear una VPDN (Virtual Prívate Dial Network, Red privada virtual mediante llamada telefónica) este es multiprotocolo e independiente del medio.

L2TP fue creado para corregir las deficiencias de los protocolos PPTP y L2F y establecerse como un estándar. El transporte de L2TP está definido para una gran variedad de tipos de paquete, incluyendo X.25, Frame Relay y ATM. A pesar de que L2TP ofrece un acceso económico, con soporte multiprotocolo y acceso a redes de área local remotas, no presenta unas características criptográficas especialmente robustas ya que no tiene los mecanismos de para generación automática de claves, o refresco automático de claves. Esto puede hacer que alguien que escuche en la red y descubra una única clave tenga acceso a todos los datos transmitidos.

También permite que los usuarios soliciten políticas de seguridad corporativas a través de cualquier enlace VPN o VPDN como una extensión de sus propias redes internas; L2TP es una mejor elección para las VPNs de acceso remoto que precisen soporte multiprotocolo.

- **SSL/TLS:** SSL/TLS es un protocolo de nivel de transporte, proporciona servicios de seguridad extremo a extremo para aplicaciones que usan un protocolo de trasporte fiable como TCP. La idea de este protocolo es proporcionar servicios de seguridad para transacciones en Internet.

SSL proporciona autentificación y privacidad de la información entre extremos sobre Internet mediante el uso de criptografía. Habitualmente, sólo el servidor es autentificado (es decir, se garantiza su identidad) mientras que el cliente se mantiene sin autentificar; Este protocolo permite la autentificación mutua, la idea es proporcionarle a los clientes una infraestructura de claves públicas con el objetivo de prevenir escuchas (eavesdropping), la falsificación de la identidad del remitente y mantener la integridad del mensaje, por lo que puede ser usado para tunelar una red completa y crear una red privada virtual (VPN).

- **OpenVPN:** OpenVPN es una solución de conectividad basada en software, este ofrece conectividad punto-a-punto con validación, jerarquía de usuarios y hosts conectados remotamente. Este ofrece dos modos básicos de funcionamiento ya que puede trabajar en la capa de enlace de datos y de red del modelo OSI.

Hay dos tipos básicos de túneles que se pueden crear con OpenVPN, el Túnel IP y el Puente Ethernet; El primero es usado para encaminar tráfico IP punto-a-punto sin broadcast es mas fácil de configurar que el puente Ethernet y el segundo es apropiado para aplicaciones que se comunican utilizando difusión (broadcast), tales como la red de Windows y juegos de área local (LAN).

- **CIPE:** CIPE es una implementación de VPN desarrollada principalmente para Linux. CIPE utiliza paquetes IP encriptados que son encapsulados, o «wrapped», en paquetes (UDP) de datagramas.

A los paquetes CIPE se les da un encabezado con la información de destino y son encriptados usando un mecanismo de encriptación de CIPE. Los paquetes son luego transferidos sobre IP como paquetes UDP a través del dispositivo de red virtual de CIPE (cipcb*x*) sobre el túnel hasta llegar al nodo remoto destino.

1.4 VENTAJAS Y DESVENTAJAS (FRAME RELAY VS VPN)

Las tecnologías de red que interviene en este proyecto poseen ventajas y desventajas, las cuales hay que tener en cuenta para saber cual es la más viable para la compañía.

A continuación se listaran cada una ellas.

1.4.1 Ventajas FRAME RELAY. Las siguientes son algunas de las ventajas de la tecnología FRAME RELAY.

- Seguridad y confiabilidad en la transmisión de la información.

- El servicio es prestado por un proveedor, por ende es responsable del 100% de la comunicación con cada una de las sedes remotas.

- Servicio de comunicación dedicado (solo se transmite información de la compañía).

1.4.2 Desventajas FRAME RELAY. Las siguientes son algunas de las desventajas de la tecnología FRAME RELAY.

- Solo ha sido definido para velocidades de hasta 1.544/2.048 MBPS (T1/E1).

- Sigue siendo una tecnología antigua ya que no inventa nuevos protocolos ni mejora los dispositivos de la red; sino que limita a eliminar parte de la carga de protocolo y funciones del X.25

- A mayor distancia mayor costo.

- Dependencia de un tercero por parte del proveedor del servicio (Emcali).

- Mayor numero de equipos en el punto de venta (sede), por lo que se incrementa el riesgo de alguna falla de los mismos.

- Poco ancho de banda para la implementación de nuevas aplicaciones (datos, voz y video).

- Los costos son muy altos con respecto a las velocidades que ofrece (64 Kbps) para las sedes de la compañía.

1.4.3 Ventajas VPN. Las siguientes son algunas de las ventajas de la tecnología VPN.

- Existe una gran variedad de Redes Privadas Virtuales desarrolladas por software, donde elegir y que están continuamente mejorando sus prestaciones.

- Puede extenderse a cualquier sitio sin incurrir en costos adicionales.

- Múltiples clases de servicio para aplicaciones de datos, voz y video.

- Pueden dar cobertura tanto a redes internas (intranet) como redes externas.

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

- Alta seguridad en la transmisión de la información de extremo a extremo (Autenticación y encriptación).

- Bajo costo de la nueva solución.

- Mayor ancho de banda a menor precio.

- Si en INTERNET un enlace se cae o congestiona demasiado, existen rutas alternas para hacer llegar los paquetes a su destino.
- Facilidad para agregar o retirar conexiones Remotas, pues todas son conexiones virtuales

1.4.4 Desventajas VPN. Las siguientes son algunas de las desventajas de la tecnología VPN.

- Es necesario instalar y configurar un software en una máquina, por lo que existe el riesgo de des configuración del mismo.

- Tener que dedicar solo una maquina (servidor VPN) para que maneje todos los enlaces VPN.

- Si el software es de libre distribución, éste puede estar modificado y contener puertas traseras.

- Sus comunicaciones van sobre una red pública (INTERNET).

- El servicio VPN lo proporciona la empresa y no un proveedor.

1.5 COSTOS Y BENEFICIOS

Los costos y los beneficios de la solución actual con respecto a la solución propuesta disminuyen de manera considerable los costos ($) ya que por cada canal de comunicaciones implantado se disminuyen los costos en un 80 % aproximadamente; Además le permitirá a la compañía obtener beneficios como el ahorro del tiempo de desplazamiento debido el soporte técnico hacia los puntos de

venta se puede hacer remotamente, mejora de la red actual (incremento en el ancho de banda) entre otros.

A continuación se darán a conocer los costos reales de cada una de las tecnologías planteadas anteriormente, también se hará una comparación con respecto a los costos de cada una de ellas y el ahorro que le genera a la compañía.

1.5.1 Costos por mes tecnología actual (FRAME RELAY). Los costos de los canales dedicados (FRAME RELAY) de cada uno de los almacenes (sedes) y la descripción respectiva de cana uno de ellos se muestra la siguiente tabla:

Tabla 1. Costos tecnología de red actual (FRAME RELAY).

ALMACEN	DIRECCION	DESCRIPCION DEL SERVICIO	ANCHO DE BANDA	TOTAL FACTURA
kkk1	AVE 6 NORTE 12-12	INTER LAN	64 kbps	$ 535.891
kkk2	Unicentro local 3	INTER LAN	64 kbps	$ 535.891
kkk10	AVE 3 NORTE # 47C-06	INTER LAN	64 kbps	$ 535.891
kkk12	AEROPUERTO ALFONSO BON	INTER LAN	64 kbps	$ 535.891
kkk16	CARRERA 1 # 61A-30	INTER LAN	64 kbps	$ 535.891
kkk8	CARRERA 6 # 10-41	INTER LAN	64 kbps	$ 535.891
kkk20	AVE 6 NORTE # 33-06	INTER LAN	64 kbps	$ 535.891
kkk21	CALLE 13 #	INTER LAN	64 kbps	$ 535.891
kkk7	BUENAVENTURA	INTERLAN NACIONAL	256 kbps	$ 1.453.770
kkk6	PALMIRA	INTERLAN NACIONAL	256 kbps	$ 774.300
kkk11	CALLE 5#57-102	INTER LAN	64 kbps	$ 535.891
		Valor total		**$ 6.743.769**

En la tabla se muestra el almacén (sedes), la dirección donde se encuentra ubicada, la descripción del servicio dado por el proveedor del mismo, el ancho de banda que maneja el canal dedicado (Kbps) y la tarifa fija mensual manejada por cada una de las sedes de Arka S.A.

El costo total por cada canal dedicado que tiene por cada una de las sedes de Arka S.A. es de **$ 6.743.769** mensual**.**

1.5.2 Costos por mes solución propuesta (VPN). Los costos de la tecnología de red (VPN) propuesta por cada uno de los almacenes (sedes) y la descripción respectiva de cana uno de ellos se muestra en la siguiente tabla:

Tabla 2. Costos tecnología de red propuesta (VPN).

ALMACEN	DIRECCION	DESCRIPCION DEL SERVICIO	ANCHO DE BANDA	VALOR TOTAL
kkk1	AVE 6 NORTE 12-12	DUO BANDA ANCHA-LOCAL ILIM	1000 Kbps	116000
kkk2	Unicentro local 3	DUO BANDA ANCHA-LOCAL ILIM	1000 Kbps	116000
kkk10	AVE 3 NORTE # 47C-06	DUO BANDA ANCHA-LOCAL ILIM	1000 Kbps	116000
kkk12	AEROPUERTO ALFONSO BON	DUO BANDA ANCHA-LOCAL ILIM	1000 Kbps	116000
kkk16	CARRERA 1 # 61A-30	DUO BANDA ANCHA-LOCAL ILIM	1000 Kbps	116000
kkk8	CARRERA 6 # 10-41	DUO BANDA ANCHA-LOCAL ILIM	1000 kbps	116000
kkk20	AVE 6 NORTE # 33-06	DUO BANDA ANCHA-LOCAL ILIM	1000 kbps	116000
kkk21	CALLE 13 #	DUO BANDA ANCHA-LOCAL ILIM	1000 kbps	116000
kkk7	BUENAVENTURA	DUO BANDA ANCHA-LOCAL ILIM	1000 kbps	116000
kkk6	PALMIRA	DUO BANDA ANCHA-LOCAL ILIM	1000 kbps	116000
kkk11	CALLE 5#57-102	DUO BANDA ANCHA-LOCAL ILIM	1000 kbps	116000
		Valor total		**$ 1.276.000**

En la tabla se muestra el almacén (sedes), la dirección donde se encuentra ubicada, la descripción del servicio dada por el proveedor, el ancho de banda que va a manejar la VPN (Kbps) y la tarifa fija mensual manejada por cada una de las sedes de Arka S.A.

El costo total por cada VPN por cada una de las sedes de Arka S.A. es de **$ 1.276.000** mensual**.**

Teniendo encuentra los costos que genera la implantación de red (VPN) beneficios privados que se pueden llevarse acabo con la implantación de la red VPN son los siguientes:

- **Ahorro del tiempo de desplazamiento:** Con la nueva tecnología de red, se pretende reducir o eliminar el tiempo que los trabajadores remotos gastan en desplazarse hacia los puntos de venta a realizar alguna acción que pudiera ser llevada a cabo desde su escritorio, como por ejemplo consultas en la base de datos del aplicativo, imprimir algún registro, etc.

- **Mejora de la red actual:** Con la implantación de la red propuesta (VPN), se pretende mejorar procesos básicos debido a que las velocidades que van a tener con esta solución son altas con respecto a la solución actual, por ende se va a tener ancho de banda mayor pasando de tener 64 Kbps con Frame Relay actual a 1000 Kbps con la red VPN.

- **Beneficios y costos intangibles:** A continuación se muestran los costos y beneficios que no se pudieron valorar (Intangibles). Se tratan de los siguientes:

- Costos: Con la tecnología de red actual no se pueden llevar acabo implementaciones futuras de tecnologías de información, ya que el ancho de banda que maneja es muy reducido.

Además el proveedor actual del servicio dedicado (Frame Relay) necesita de un tercero para poder establecer la comunicación y por ende se puede generar retrasos al momento de una caída del canal de datos.

En este orden de ideas la propuesta par la implantación de red VPN podría generar cambios en las políticas de la organización.

- Beneficios: La implantación de la red VPN como reemplazo de la existente permitirá a los trabajadores remotos tener acceso a la red privada desde cualquier parte donde haya Internet por lo que mejora las condiciones de trabajo del personal de soporte del departamento de sistemas.

1. 6 SOLUCIÓN DE RED ACTUAL (FRAME RELAY) VS PROPUESTA (VPN)

A continuación se hace una comparación por mes de las dos tecnologías, permitiendo conocer el ahorro que podría incurrir la implantación de la tecnología propuesta.

Los costos por mes de cada una de las tecnologías se muestran en la siguiente tabla:

Tabla 3. Costos mensual tecnología de red actual vs tecnología de red propuesta (VPN).

ALMACEN	**FRAME RELAY**	**VPN**	**DIFERENCIA**
kkk1	$ 535.891	$ 116.000	$ 419.891
kkk2	$ 535.891	$ 116.000	$ 419.891
kkk10	$ 535.891	$ 116.000	$ 419.891
kkk12	$ 535.891	$ 116.000	$ 419.891
kkk16	$ 535.891	$ 116.000	$ 419.891
kkk8	$ 535.891	$ 116.000	$ 419.891
kkk20	$ 535.891	$ 116.000	$ 419.891
kkk21	$ 535.891	$ 116.000	$ 419.891
kkk7	$ 1.453.770	$ 116.000	$ 844.375
kkk6	$ 774.300	$ 116.000	$ 844.375
kkk11	$ 535.891	$ 116.000	$ 419.891
VALOR TOTAL	**$ 6.743.769**	**$ 1.276.000**	**$ 5.467.769**

En la tabla se muestra en la primera columna el almacén (sedes), en las columnas siguientes el costo fijo mensual de cada una de las tecnologías y en la última columna la diferencia entre ellas.

El ahorro que se obtiene con la implantación de la tecnología propuesta de **$ 5.467.769** mensual**.**

Los costos por año de cada una de las tecnologías se muestran en la siguiente tabla:

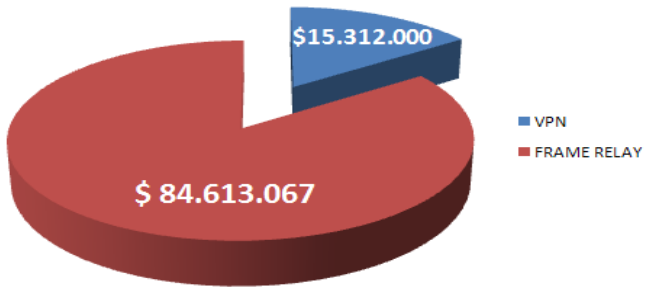
Tabla 4. Costos anuales tecnología de red actual vs tecnología de red propuesta (VPN).

ALMACEN	ACUMULADO FRAME REAY	ACUMULADO VPN	DIFERENCIA
kkk1	$ 6.430.692	$ 1.392.000	$ 5.038.692
kkk2	$ 6.430.692	$ 1.392.000	$ 5.038.692
kkk10	$ 6.430.692	$ 1.392.000	$ 5.038.692
kkk12	$ 6.430.692	$ 1.392.000	$ 5.038.692
kkk16	$ 6.430.692	$ 1.392.000	$ 5.038.692
kkk8	$ 6.430.692	$ 1.392.000	$ 5.038.692
kkk20	$ 6.430.692	$ 1.392.000	$ 5.038.692
kkk21	$ 6.430.692	$ 1.392.000	$ 5.038.692
kkk7	$ 17.445.240	$ 1.392.000	$ 16.053.240
kkk6	$ 9.291.600	$ 1.392.000	$ 7.899.600
kkk11	$ 6.430.692	$ 1.392.000	$ 5.038.692
	$ 84.613.067	**$ 15.312.000**	**$ 69.301.068**

En la tabla se muestran el acumulado por año de las dos tecnologías donde se puede apreciar que para la tecnología actualmente implementada en la organización (FRAME REAY) es de **$ 84.613.067** anuales y para la tecnología propuesta seria de **$ 15.312.000** anuales, el ahorro que se obtendría con la implantación de la tecnología propuesta será de **$ 69.301.068,** el cual será aproximadamente de un 80 % anual.

El ahorro anual se obtiene y que le representa a la compañía la implantación de la tecnología de red (VPN) se ve claramente figura 4 de este documento:

Figura 4. Gráfica costos FRAME RELAY vs VPN.



1.6.1 Requerimientos e inversión. Los siguientes son los cotos de inversión los cuales pueden ser privados o de operación.

- **Costos privados:** En general tendremos los siguientes ítems.

- Compra de hardware (un equipo - servidor) $2’000.000 Aproximadamente.
-Estudios y capacitación (políticas de seguridad) $2’000.000.
-Instalación y configuración para puesta en marcha. $1’500.000.

- **Costos de operación:** Remuneraciones (implantador). $1’500.000 mensual por 2 meses; Comunicaciones (proveedor de Internet). Cargo fijo mensual por ADSL en cada punto de venta.

Nota: Los costos mostrados anteriormente se obtendrían si la organización opta por realizar el cambio de tecnología y apuntarle a las VPNs como medio de comunicación con sus puntos de venta.

- **Conclusión**

Frame Relay constituye un método de comunicación orientado a paquetes para la conexión de sistemas informáticos. Se utiliza principalmente para la interconexión de redes de área local (LANs, local área networks) y redes de área extensa (WANs, wide área networks) sobre redes públicas o privadas.

Generalmente son canales dedicados y son alquilados a una ISP, estos se asocian a una ip pública y a un router asociado dentro de la red Frame Relay. Los paquetes recibidos de múltiples usuarios se multiplexan sobre la línea y se envían a través de la red Frame Relay a sus destinos.

Hacer el estudio de las dos tecnologías (VPN y FRAME RELAY), proporciono información vital y necesaria para decidir cual de las soluciones es mas viable para la compañía.

La Implantación de la red VPN, es una solución que para la empresa es importante debido al ahorro tan grande que esta genera, además de sus ventajas con respecto ala tecnología actual.

2. REDES PRIVADAS VIRTUALES – VPNS

En esta sección, se analizaran las tecnologías VPNs por software mas comunes para crear túneles y enlaces encriptados sobre redes publicas.

Lo anterior permitirá hacer una comparación mostrando las características de cada una de estas tecnologías con el fin de escoger el protocolo más apropiado para la implantación de la VPN en Arka S.A.

Luego se escogerá la tecnología de VPN a utilizar para la implementación en la empresa Arka S.A., donde se definirá que protocolo maneja este software donde será documentado con el fin de entender el funcionamiento y la manera como permite crear enlaces privados a través de Internet describiendo aspectos como la encriptación y autenticación de los datos.

2.1 DEFINICIÓN DE LA TECNOLOGÍA VPN A IMPLEMENTAR

Para la implementación de la red VPN en la empresa Arka S.A se tuvo en cuenta la distribución de Linux la cual es Suse 8.1, en esta vienen incluidas soluciones VPN por software las cuales son Crypto IP Encapsulation (CIPE) y el Protocolo Internet de Seguridad (IPsec); Existen otras alternativas de software para establecer una VPN en Linux como por ejemplo (OpenVPN, PPTP, entre otros.), cada una de estas con características, ventajas y desventajas particulares.

Por ende existen argumentos para usar cada una de ellas como se muestra en la tabla 3, donde se hace una comparación de las tecnologías VPN existentes mas utilizadas para hacer túneles privados a través de una red publica, describen características generales de cada una de ellas, lo cual proporcionara información vital para decidir que tecnología escoger para la implantación de la VPN en la empresa Arka S.A.

Tabla 5. Comparativa de cipe y otras tecnologías VPNs por software.

CARACTERISTICAS	**TECNOLOGIA**			
	CIPE	**IPSEC**	**OPENVPN**	**PPTP**
Permisos	El software de CIPE puede funcionar en el espacio de usuario y administrador.	Son necesario privilegios de administrador	El software de CIPE puede funcionar en el espacio de usuario y administrador.	Son necesario privilegios de administrador
NAT	Ningún problema al realizar NAT en ambos lados de la red.	problemas con NAT	Ningún problema al realizar NAT (ambos lados pueden estar en las redes de NATed)	problemas con NAT
Modelo OSI	Trabaja en la capa 3	Trabaja en la capa 3	Trabaja en la capa 3	Trabaja en la capa 2
Métodos de Encriptación	Algoritmo Blowfish	IKE (Internet Key Exchange Protocol)	SSL/TLS como estándar de criptografía	MPPE (Microsoft Point-to-Point Encription)
Puertos	Es necesarios tan solo 1 puerto en el corta fuegos	Son necesarios varios puertos y protocolos en el cortafuego.	Solamente es necesario un puerto en el cortafuego.	son necesarios el puerto TCP 1723, y el identificador IP 47
Limitaciones	No esta implementada en dispositivos hardware debido a que su creación fue solo como aplicación de seguridad en paquetes udp enviados a través de la red.	Configuración compleja, ya que se debe hace una modificación bastante compleja del stack IP.	No hay ninguna GUI profesional para su administración; sin embargo, hay algunos proyectos interesantes y prometedores, además todavía es algo un poco desconocido y no es compatible con otras tecnologías de VPN por software ejemplo(con ipsec)	Tecnología fácil, pero su configuración no compatible con Linux suse 8.1, la cual es la distribución manejada por la empresa Arka S.A.
Ventajas	Configuración e instalación simple debido a que esta se hace solo modificando archivos, es compatible con NAT y no necesita cambio de hardware y de software.	Estándar de la tecnología VPN y muy bien conocida, para el manejo de esta tecnología existen muchas GUIs. Para su administración.	Tecnología fácil, bien estructurada, modular, su conjuración es fácil, las Interfaces de red y paquetes son estandarizados.	PPTP soporta múltiples protocolos de red (IP, IPX, NetBEUI).

De acuerdo con estas características y las exigencias de la Red VPN a implementar se concluyo que el protocolo y software para VPN más adecuado es CIPE, ya que funciona perfectamente con la distribución de Linux y versión del kernel que se maneja en la empresa Arka S.A., es seguro ya que por medio de un algoritmo encripta los datos y los envía hacia el receptor, el cual con una clave compartida desencripta los datos para ser leídos y finalmente la configuración y instalación no es compleja debido a que se realiza modificando archivos scripts, entre otras ventajas.

CIPE es una implementación de VPN desarrollada principalmente para Linux. CIPE utiliza paquetes IP encriptados que son encapsulados, en paquetes (UDP) de datagramas.

A los paquetes CIPE se les da un encabezado con la información de destino y son encriptados usando algoritmos simétricos los cuales caracterizan por utilizar la misma clave para cifrar y descifrar.

Los paquetes son luego transferidos sobre IP como paquetes UDP a través del dispositivo de red virtual de CIPE (cipcb*x*) sobre una red en este caso la Internet hasta el nodo remoto destino CIPE.

En este orden de ideas, existen otros motivos por los cuales se toma la decisión de implementar la VPN por software con el protocolo CIPE:

- CIPE es una tecnología bien conocida por la distribución de Linux Suse 8.1 y por ello cualquier maquina que tenga esta distribución lo puede ejecutar, por lo que es una ventaja muy importante respecto a las otras aplicaciones de VPN por software ya en la compañía se trabaja con esta distribución de Linux.

- CIPE es una tecnología simple, bien estructurada y su configuración no es compleja ya que esta se hace modificando archivos de texto donde ya vienen los parámetros a configurar y el usuario solo tienen plasmar los datos que se necesite a conveniencia de sus necesidades, además permite que los administradores puedan configurar sus servidores y clientes CIPE remotamente sin la necesidad de utilizar herramientas gráficas pesadas que funcionarían pobremente a través de la red.

- CIPE está desarrollado activamente para funcionar en conjunto con iptables, ipchains y otros cortafuegos basados en reglas. Todo lo que se necesita es aceptación en par de los paquetes UDP CIPE entrantes para coexistir con las reglas del corta fuegos existentes.

- CIPE soporta la encriptación usando cualquiera de los algoritmos estándar de encriptación Blowfish o IDEA; este utiliza Blowfish (por defecto) para encriptar.

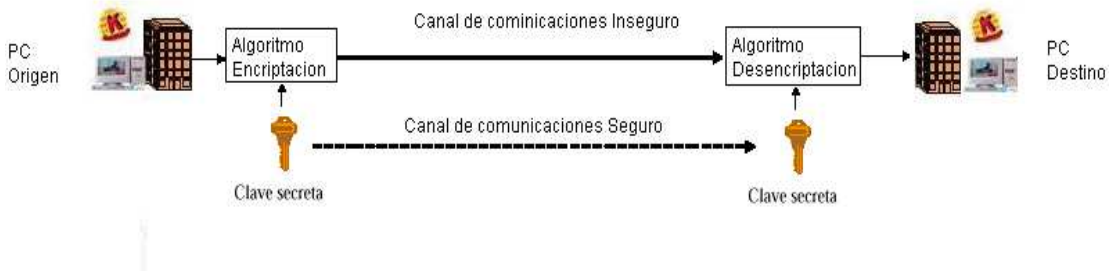
2.2 SEGURIDAD DE PROTOCOLO CIPE

CIPE es un protocolo que fue creado con el objetivo general de proporcionar un servicio seguro es decir teniendo en cuenta problemas de seguridad como por ejemplo ataques de Escuchas clandestinas de datos (Sniffing), Suplantación de datos (Spoofing) entre otros ataque existentes en Internet.

Para estos problemas de seguridad mencionados anteriormente CIPE emplea técnicas de encriptación, autenticación y validación de los datos que viajan a través del túnel.

La seguridad de la VPN usando el protocolo CIPE se basa en los algoritmos estándar de encriptación como lo son Blowfish (Por defecto en CIPE) o IDEA, estos se caracterizan por utilizar la misma llave entre el emisor y el receptor de la conexión.

Figura 5. Esquema básico de algoritmos Simétricos.



La seguridad de los algoritmos utilizados por el CIPE está basada en la privacidad de la clave secreta compartida (Key), esta permite autenticar al emisor y al receptor VPN e decir solo le entrega al cliente que tenga la misma llave para posteriormente descifrar los datos enviados por medio del túnel.

El funcionamiento de estos algoritmos se lleva acabo de la siguiente manera; El emisor del mensaje genera una clave, esta la transmite a través de un canal seguro y construido por la tecnología VPN, luego el receptor procesa la clave donde verifica si la clave es correcta, si lo es se autentica y autoriza que el mensaje enviado pueda ser recibido, des encriptado el mismo por medio del algoritmo que la tecnología escogida para la implantación usa.

2.2.1 Algoritmos de encriptación utilizados por CIPE. Los algoritmos que utiliza CIPE para la encriptación de los datos son Blowfish (Por defecto en CIPE) y el IDEA, estos son algoritmos simétricos y su funcionamiento es el siguiente:

➢ **Blowfish:** Es un algoritmo de cifrado por bloques, este fue diseñado para ser rápido (cifra datos en modo de 32-bit a razón de 26 ciclos de reloj por byte), es compacto (puede correr ocupando menos de 5Kb de memoria), es simple (las únicas operaciones que se utilizan son sumar, XOR, y buscar la tabla de particiones en operaciones de 32-bits), es seguro (la longitud de la clave de Blowfish es variable y puede tener una longitud de hasta 448 bits), y robusto (a diferencia de DES, la seguridad de Blowfish no disminuye por simples errores de programación).

El algoritmo de cifrado por bloques Blowfish, que cifra datos en bloques de 64 bits al mismo tiempo, es dividido en dos partes: claves de expansión y cifrado de datos.

Las claves de expansión convierten una clave de más de 448 bits en varias subclaves que en totalizan 4168 bytes.

El cifrado de datos consiste en una función simple que permite 16 iteraciones. Cada iteración llamada Around consiste en la permutación de una clave dependiente y una substitución de una clave y datos dependiente.

Blowfish utiliza un gran número de subclaves que deben ser preprocesadas antes de cualquier proceso de cifrado o descifrado.

➢ **IDEA (International Data Encryption Algorithm):** Trabaja con bloques de texto de 64 bits y una clave de 128 bits. Puede trabajar con los 4 modos: ECB, CBC, CFB y OFB.

- Electronic CodeBook (ECB): Los bloques de texto se cifran por separado.

- Cipher Block Chainning (CBC): Los bloques del texto cifrado se relacionan entre sí mediante funciones *OR-EXCLUSIVA.*

- Cipher FeedBack (CFB): Se realiza una *OR-EXCLUSIVA* entre caracteres o bits aislados del texto y las salidas del algoritmo. El algoritmo utiliza como entradas los textos cifrados.

- Output FeedBack (OFB): Funciona igual que el CFB, pero utiliza como entradas sus propias salidas, por lo tanto no depende del texto; es un generador de números aleatorios.

Siempre opera con números de 16bits utilizando operaciones como OR-EXCLUSIVA, suma de enteros o multiplicación de enteros.

A continuación se muestra una tabla comparativa de cada uno de los algoritmos que puede manejar el CIPE.

Tabla 6. Cuadro comparativo algoritmos simétricos de cifrado utilizados por CIPE.

Características	**Blowfish**	**IDEA**
Fecha creación y nombre del inventor	Fue desarrollado por Bruce Schneier en 1993.	Fue desarrollado por Xuejia Lai y James L. Massey en 1991.
Tamaño de bloque y tamaño de la clave	El tamaño del bloque es de 64 bits y claves que van desde los 32 bits hasta 448 bits.	El tamaño del bloque es de 64 bits y la longitud de la clave es en de 128 bits.
Tipo	Algoritmo Simétrico.	Algoritmo Simétrico.
Uso de la clave	Encriptado y des encriptado con la misma clave	Encriptado y des encriptado con la misma clave
Algoritmos	CIPE trabaja con blowfish por defecto	Hay que configurarlo para que trabaje con CIPE, además es un algoritmo patentado y puede necesitar licencia comercial para su uso.
Dificultad	Fácil configuración.	Configuración compleja para novatos.

De acuerdo con las características mostradas en la tabla 6, se concluyo que el algoritmo de cifrado mas adecuado es blowfish, ya que nos proporciona una clave que puede ir desde los 32 bits hasta los 448 bits, Siendo mas segura en comparación con el algoritmo IDEA que utilizando una clave que va desde los 64 bits hasta los 128 bits, además es rápido ya que utiliza bloques pequeños para la codificación (64 bits) permitiendo que la encriptación y desencriptación de la información sea rápida.

2.3 ARQUITECTURAS VPN

Existen dos arquitecturas básicas de las VPNs (sitio a sitio y acceso remoto), el éxito de una VPN depende de una buena elección del protocolo a implementar y de la arquitectura a elegir.

- **VPNs sitio a sitio:** En este caso, múltiples redes remotas de la misma compañía son conectadas entre si usando una red pública, convirtiéndolas en una sola LAN corporativa lógica, y con todas las ventajas de la misma.

- **VPNs de Acceso Remoto**: En este caso, un host remoto crea un túnel para conectarse a la Intranet corporativa. El dispositivo remoto puede ser un computador personal con un software cliente para crear una VPN, y usar una conexión conmutada, o una conexión de banda ancha permanente.

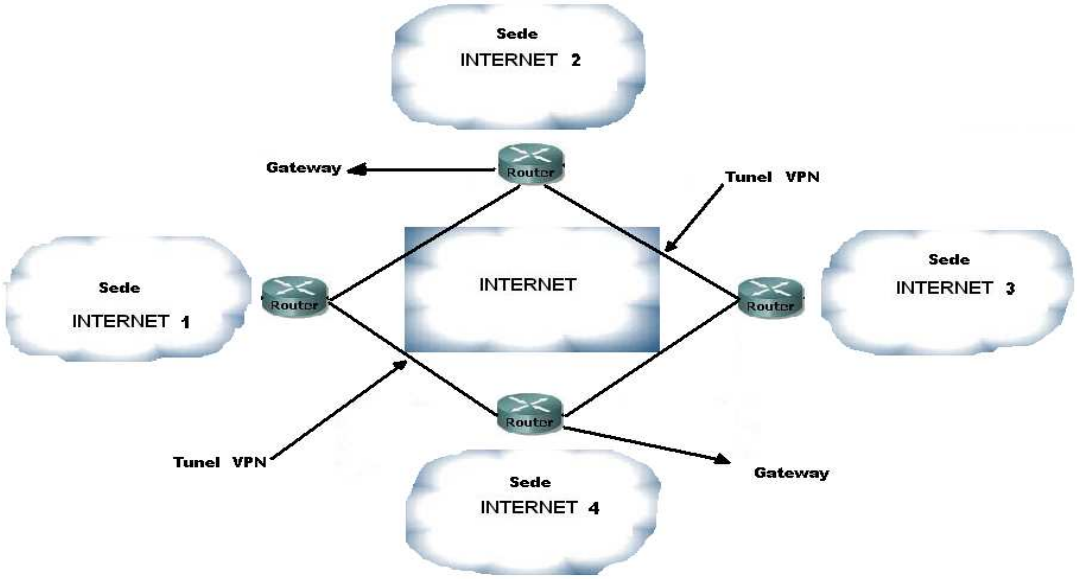
2.3.1 VPNs sitio a sitio. Las VPN sitio a sitio pueden emplearse para conectar sitios corporativos. En el pasado, esta operación se realizaba mediante una línea alquilada o una conexión FRAME RELAY. En la actualidad, la mayor parte de las empresas disponen de acceso a Internet. Con el, las costosas líneas alquiladas y FRAME RELAY pueden ser sustituidas con VPNs sitio a sitio, las cuales pueden emplearse para ofrecer conexión a la red.

Las VPNs pueden soportar las intranets de la compañía y las extranets de los socios.

Una VPN sitio a sitio es una extensión de una WAN clásica que tiene las mismas políticas y el mismo rendimiento, y que puede construirse usando routers, firewalls y hubs VPN.

La figura 2 ilustra la conexión de cuatro sedes de una misma compañía usando una arquitectura VPN sitio a sitio.

Figura 6. Esquema de una solución VPN sitio a sitio.



Nótese que los túneles VPN que aparecen señalados no son enlaces físicos sino lógicos que viajan por Internet. El único equipo que tiene que adquirir la compañía

para cada sede a conectar es un Gateway VPN que tiene, por lo general, un puerto LAN (Ethernet o Fast Ethernet) para conectarse a la LAN Corporativa, y un puerto LAN o WAN para conectarse hacia la ISP. Muchos de estos Gateway VPN trabajan como firewalls y tiene un switch 10/100 incorporado de 4 u 8 puertos, debido a esto son llamados dispositivos Todo en Uno.

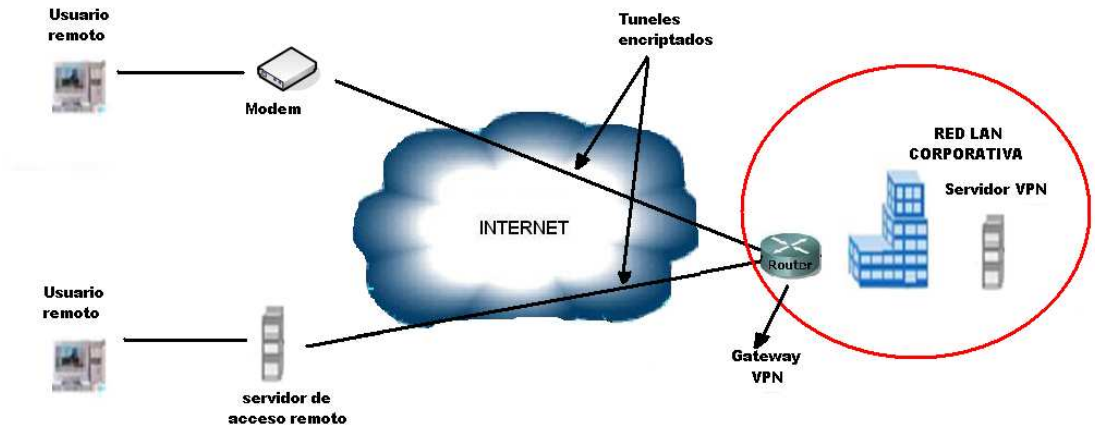
Con una arquitectura VPN sitio a sitio se puede lograr el objetivo de interconectar dos o más sitios de una red corporativa y a un bajo costo.

2.3.2 VPNs de Acceso Remoto. Las VPNs de esta categoría son las que proveen acceso remoto a la intranet o extranet corporativo a través de la red pública (Internet), conservando las mismas políticas, como seguridad y calidad de servicio, que en la red privada. Permite el uso de múltiples tecnologías como discado, ISDN, xDSL, cable, o IP para una conexión segura entre sucursales remotas este tipo de VPN se centra en tecnologías tunneling y en los protocolos que son necesarios para asegurar cualquier tipo de VPN.

Este tipo de VPN conecta con seguridad los usuarios remotos (Ejemplo, usuarios móviles y tele trabajadores) con la empresa.

La figura 7 se ilustra dos conexiones VPNs de accesos remoto, una utilizando Internet banda ancha y la otra con un modem análogo común.

Figura 7. Esquema típico de VPNs de acceso remoto.



El usuario remoto crea un túnel el cual es encriptado, esté puede tener acceso por medio de una conexión banda ancha (puede ser x DSL) o por medio de un módem análogo común, en cualquiera de estos casos el usuario remoto podría estar en

otra ciudad o incluso en otro país solo necesita tener Internet independientemente de la ISP.

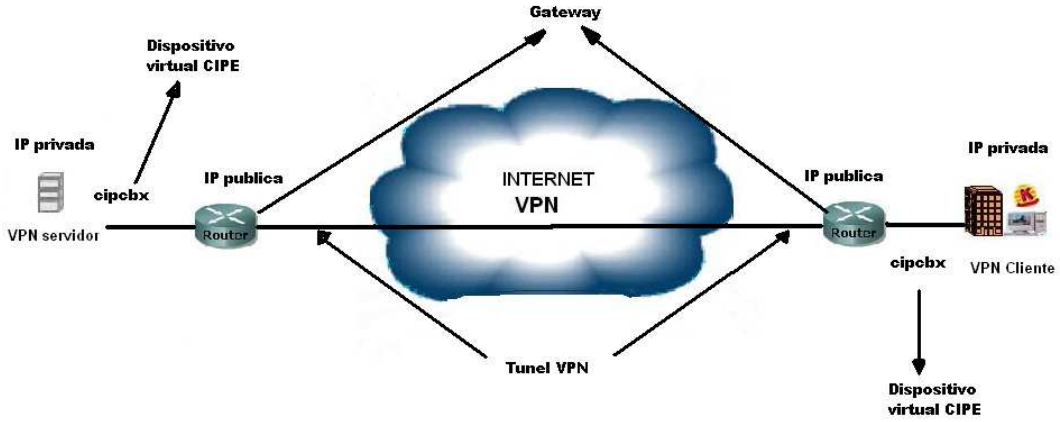
Para la implantación de la VPN en Arka S.A se va a manejar una arquitectura sitio a sitio, ya que la compañía necesita interconectar todas las sedes y ver estas como una sola LAN.

Las VPNs sitio a sitio permiten conectar dos redes o sedes separadas geográficamente, cada una de estas esta conectada a la Internet común con computadoras que pueden ser clientes o servidores VPN. Una vez que la conexión VPN se establece a través del Internet, los usuarios que estén en cualquiera de las redes pueden intercambiar datos como si estuvieran en la misma red.

Además la VPN a implementar es basada en software utilizando el protocolo CIPE el cual interconectara cada uno de los nodos destinos desde un servidor (Cliente - servidor).

La figura 8 se muestra la arquitectura (VPN sitio a sitio) y la solución VPN basada en software (CIPE) a utilizar en la implantación de manera general.

Figura 8. Esquema general. Arquitectura VPN (sitio a sitio) y software VPN (CIPE).



En la grafica se ilustra un esquema general de la arquitectura a implementar y el protocolo CIPE a usar; Básicamente en cada extremo de la red se va a utilizar un router (Gateway) para tener acceso a Internet, este es independiente de la ISP.

La ISP nos provee un router y asigna una IP pública, si el router utiliza NAT configuramos la IP privada directamente en el router sino tendremos que utilizar dos tarjetas de red eth0 y eth1 para asignarle a cada una la IP privada y IP publica respectivamente.

Por ultimo configuramos el CIPE dándole a este cada uno de los parámetros, creando así un dispositivo mas (cipcbx) el cual crea el túnel entre las dos redes encapsulando la información a enviar, asignándoles una clave (key) y posteriormente encriptado los datos que viajan a través del túnel.

3. INSTALACION Y CONFIGURACION DE LA VPN

En esta sección se pretende ilustrar como se implementa una red VPN (del inglés, Virtual Private Network), en la empresa Arka S.A. Donde inicialmente se hará una prueba piloto en donde se conectara la planta con uno de sus puntos de venta (sede).

El objetivo no es explicar en que consiste una VPN ni explicar sobre que protocolos se puede establecer una red VPN, sino de dar a conocer cómo se instala y se configura una conexión VPN en un sistema LINUX que para este caso se hará en una distribución Suse 8.1 con una versión de kernel 2.4.

Para establecer dicha conexión entre redes, lo haremos usando el protocolo CIPE versión 1.5.4 escogido anterior mete. Esta tecnología de VPN por software es un paquete que viene integrado la distribución de Linux Suse 8.1, por lo tanto está disponible para todas las máquinas Suse Linux que se desee conectar a su Intranet.

Finalmente se implementara la seguridad de la VPN, esta se hará utilizando las reglas IPtables, las cuales lo que hacen básicamente es permitir o denegar el acceso a usuarios no aceptados por las mismas, actuando de manera muy similar a un corta fuego común.

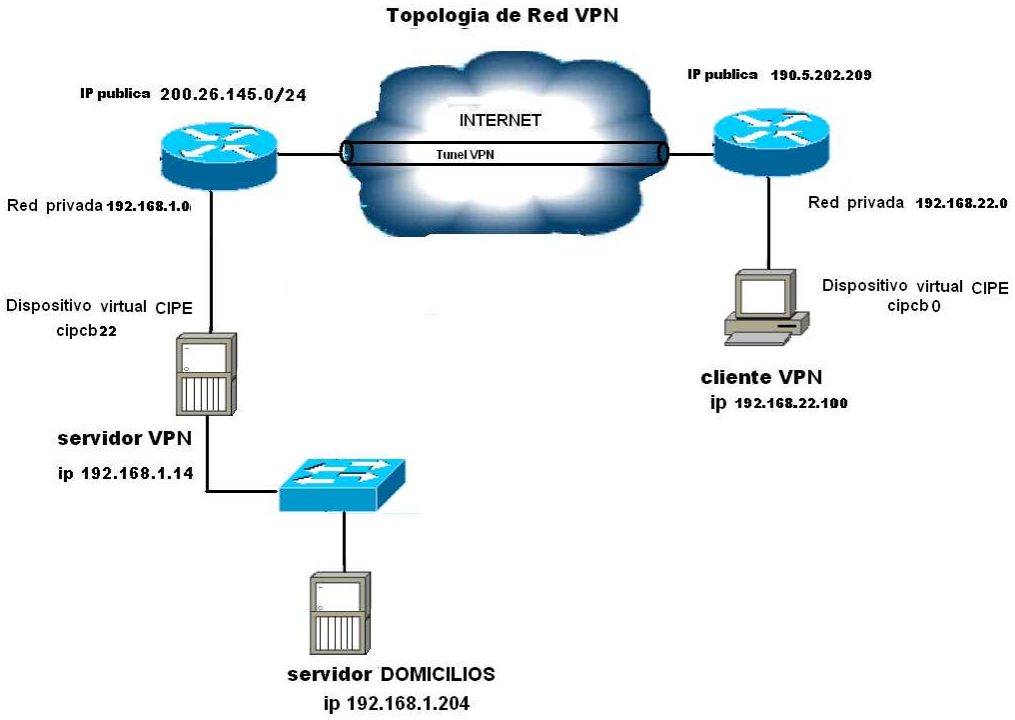
3.1 ESCENARIO DE LA RED VPN A IMPLANTAR EN ARKA S.A

Para la implantación de la red VPN se pretende conectar dos redes que pertenecen a la misma compañía en este caso la planta con uno de sus puntos de venta, estas se necesita unir para compartir recursos como por ejemplo acceso al servidor de domicilios, utilizar el aplicativo de la compañía remotamente, etc.

Las dos redes se encuentran separadas físicamente y lo que se necesita es unirlas a través de un medio público como puede ser una línea ADLS que da acceso a Internet

En este orden de ideas, el escenario que se va a manejar para la red VPN se muestra en la figura 1, detallando los dispositivos Hardware y el software VPV (CIPE) que se van a utilizar para la implementación de la red VPN en la empresa Arka S.A:

Figura 9. Topología de red VPN para Arka S.A.



En la figura 9 se muestra la arquitectura de red VPN entre el servidor VPN, servidor Domicilios y un cliente VPN; Para llevar acabo la conexión entre las redes 192.168.1.0/24 (servidor) y 192.168.22.0/24 (cliente) a través de Internet hay que utilizar dispositivos hardware como dos routers los cuales me dan acceso a la red publica estos tienen direcciones publicas dadas por la ISP (proveedor de servicios de Internet), dos equipos o estaciones de trabajo el Cliente y el Servidor VPN.

En este caso el servidor VPN debe de tener 2 tarjetas de red, en una se configura la ip pública y en la otra la ip privada; Para el cliente se va a utilizar 1 tarjeta de red ya que el router permite hacer NAT y es posible configurar la ip publica en el mismo y en el equipo cliente se configura la tarjeta de red con la ip privada.

A continuación se muestra una descripción de los equipos hardware a utilizar para la implantación de la VPN.

3.2 EQUIPOS UTILIZADOS

- Un equipo DELL referencia ThinkCentre A55 Intel® Core 2 Duo Processor E4500, Memoria RAM 1 GB, Disco Duro 160GB 7200RPM SATA HDD, dos tarjetas de red Linksys 10/100 Ethernet, actuando como servidor VPN.

- Un equipo ***Hewlett-Packard referencia*** PROLIANT ML 350 G4 P SCSI con Procesador Xeon de 3.4 GHZ 2MB CACHE (Soporta 2 procesadores), Memoria RAM 1 GB PC 3200, Disco Duro 250 GB 10K U320 HP /Compaq, soporta hasta 6 Discos, actuando como servidor de domicilios.

- Un equipo DELL, Optiplex 320 Desktop, con procesador Pentium 4531/3.00GHz, Memoria RAM 1 GB 533MHz DDR2, Disco Duro 160GB Sata 3.0GB/s and 8MB Data Bursy cache, una tarjeta de red Dell, actuando como cliente VPN.

- 1 enrutador Cisco 800 series, actuando como router físico en la estación de trabajo del servidor.

- 1 enrutador Linksys SD208, actuando como router físico en la estación de trabajo del cliente.

- 1 switch cisco system catalyst 2950 de 24 puertos, actuando como puente entre el servidor de VPNs y el Servidor de domicilios.

3.3 INSTALACIÓN DE CIPE (CRYPTO IP ENCAPSULATION)

La instalación de CIPE es el equivalente a instalar una interfaz de red bajo Linux.

El paquete RPM que viene ya instalado en el Linux suse 8.1 es el paquete (cipe-1.5.4.tar.gz), este contiene los archivos de configuración del cipe y después de instalar el paquete, se crea una directorio cipe en la ruta /etc/cipe/ donde se encuentran los archivos de configuración.

El CIPE necesita para su ejecución los siguientes componentes instalados en el sistema:

- las fuentes del kernel: primero se necesita estar seguro de la versión del kernel de Linux esta corriendo. Para nuestro caso usamos el comando.

```
vpnserver:~ # uname -r
2.4.19-4GB
```

- IP Forwarding

El siguiente paso es habilitar la ip_forward y básicamente lo que permite pasar trafico IP de una interface a otra. Para activarlo se hace ejecutando el siguiente.

```
vpnserver:~ # echo 1 > /proc/sys/net/ipv4/ip_forward
vpnserver:~ # cat /proc/sys/net/ipv4/ip_forward
1
```

Este funciona como un switch (on = 1, off = 0) para habilitarlo basta con colocar el valor de ip_forward en 1.

- El dispositivo /dev/urandom

El CIPE necesita este dispositivo particularmente para generar las claves dinámicas, para consultarlo en la maquina ejecutamos el siguiente comando.

```
vpnserver:~ # ls -l /dev/urandom
crw-r--r--    1 root     root        1,   9 Nov 11 10:09 /dev/urandom
```

- Modutils

También se necesita tener instalados los modutils, para saber si tengo el paquete instalado ejecuto el siguiente comando.

```
vpnserver:~ # rpm -qai | egrep modutil
Name        : modutils                     Relocations: (not relocateable)
Group       : System/Kernel                 Source RPM: modutils-2.4.19-39.src.rpm
```

Este paquete se utiliza para cargar el modulo del kernel de CIPE que se implementa en el dispositivo de red virtual.

- la librería OpenSSL: Si se quiere usar la pkcipe para intercambio de la clave pública, es necesario agregar el paquete OpenSSL.

Teniendo todo los requerimientos anteriormente mencionados he instalados en el equipo en el cual se va a instalar la VPN, procedemos con la configuración y compilación del paquete CIPE.

Para nuestro caso el paquete CIPE que para nuestra ditribucion de Linux ya viene instalado la versión (cipe-1.5.4.tar.gz) por lo tanto los archivos de configuración de ejemplo encontrados en /usr/share/doc/cipe-*version*/samples/. Luego los copiamos en la ruta respectiva en /etc/cipe.

En el caso que la implementación se quisiera ejecutar en un S.O Linux que no venga por defecto el paquete CIPE instalado, tendremos que hacer los siguientes pasos:

- Descargamos el paquete por ejemplo podría ser (cipe-1.5.4.tar.gz)

- Descomprimir el paquete con el comando.

  #tar xvfz cipe-1.5.4.tar.gz

- Este descomprime todo en una carpeta con el mismo nombre cipe-1.5.4.

- Ingresamos a la carpeta cipe-1.5.4 y le damos el comando ./configure el cual es el encargado de configurar y crear un archivo 'Makefile' que será utilizado por 'make' para compilar/instalar el programa que estas instalando.

- Por ultimo lo instalamos y compilamos usando el siguiente comando.

  #make all install

Este método es el más común para la instalación de un programa cuando uno mismo lo compila.

3.4 CONFIGURACIÓN DE CIPE (CRYPTO IP ENCAPSULATION)

Inicialmente se necesitan editar los archivos de configuración del CIPE, estos archivos se ubican en el directorio /etc/cipe, el servicio CIPE se ubica en el directorio /etc/init.d/cipe y el demonio CIPE esta ubicado en la ruta (/usr/sbin/ciped-cb), los scripts de la red que cargan el módulo del kernel y activan/desactivan la interfaz CIPE (if*-cipcb).

La configuración del CIPE entre el cliente y el servidor CIPE permite una conexión punto a punto usando la Internet como el medio de transmisión del tráfico WAN.

A continuación se presenta la configuración de cada uno de estos archivos que se necesitan para la conexión y construir el túnel en la red publica entre el servidor y el cliente:

3.4.1 Configuración del servidor VPN. Para la configuración del servidor hay que tener en cuenta los siguientes pasos.

- Habilitar el reenvío de paquetes para IP versión 4.

```
vpnserver:~ # echo 1 > /proc/sys/net/ipv4/ip_forward
vpnserver:~ # cat /proc/sys/net/ipv4/ip_forward
1
```

Esto proceso se hace con el fin de poder tener comunicación entre los equipos de la red 192.168.1.0 que están detrás del servidor y que además sirva como puerta de enlace a los equipos de la red 192.168.22.0 con el cliente que servirá a este como puerta de enlace.

- Generar la clave, con el siguiente comando, sin incluir el guión medio del final:

```
vpnserver:/ # ps -auxw | md5sum
0dbac1cff75af47c7fc2c5dcb6d8ca0b  -
```

La key es de *32 caracteres (128 bits); esta* se copia y se pega en el archivo de configuración del CIPE ubicado en la siguiente ruta /etc/cipe/options.kkk22 en el campo key.

Este archivo de configuración del servidor se describe a continuación.

Nombre del Archivo: **options.kkk22**
Ubicado en la ruta **/etc/cipe/options.kkk22**

En este archivo agregamos la dirección ip de los equipos (servidor y remoto); Las variables que se van a utilizar en este archivo son las siguientes.

- **ipaddr**: dirección ip privada del servidor CIPE . Esta puede ser cualquier dirección IP privada que no se ha utilizado en la red LAN origen.

- **ptpaddr**: dirección ip privada del cliente CIPE . Esta puede ser cualquier dirección IP privada no se haya utilizado en la red LAN destino.

- **my**: dirección ip publica del servidor CIPE, a esta dirección ip se le asigna un número de puerto. El número de puerto puede ser cualquier puerto no utilizado en la máquina origen (servidor).

- **peer**: dirección ip publica del cliente CIPE, a esta dirección ip se le asigna un número de puerto. El número de puerto puede ser cualquier puerto no utilizado en la máquina origen (servidor).

- **key**: clave única. Con esta clave se cifraran todos los datos transmitidos a través del túnel.

El archivo de configuración del servidor queda de la siguiente manera.

Figura 10. Archivo de configuración options.kkk22 del servidor VPN.

```
vpnserver:~ # cat /etc/cipe/options.kkk22
# Surprise, this file allows comments (but only on a line by themselves)

# This is probably the minimal set of options that has to be set

# Without a "device" line, the device is picked dynamically

# the peer's IP address
device=cipcb22
#remote internal(fake) ip adress
ptpaddr          192.168.22.100
# my CIPE (fake)ip address
ipaddr           192.168.1.14
#my real ip adress and cipe port
me               200.26.145.134:9874
#remote real ip adress and cipe port
peer             190.5.202.209:7652

#unique 128 bit key
key              3248fd20adf9c00ccf9ecc2393bbb3e4
```

Este archivo debe de tener permisos de lectura y escritura para que exclusivamente sea modificado por el usuario root; Con el siguiente comando se le colocan los permisos.

chmod 600 /etc/cipe/options.kkk22

Luego se verifica si los permisos fueron cambiados.

```
vpnserver:/etc/cipe # ls -l /etc/cipe/options.kkk22
-rw-------    1 root     root          543 Nov 11 10:48 /etc/cipe/options.kkk22
```

Nota: La llave debe ser la misma en el servidor y en el cliente.

Nombre del Archivo: **ciped.kkk22**
Ubicado en la ruta **/etc/init.d/ciped.kkk22**

Este archivo se ejecuta inmediatamente el servicio CIPE se inicia invocando el demonio ciped-cb y levantando el dispositivo virtual para ese almacén que para este caso es el almacén # 22.

Figura 11. Archivo de configuración ciped.kkk22 del servidor VPN.

```
kkk22:/ # cat /etc/init.d/ciped.kkk22
#!/bin/sh
#
# cipe          This shell script takes care of starting and stopping
#               ciped.
#
[ -f /etc/cipe/options.kkk22 ] || exit 0

prog="ciped"

start() {
   # Start daemons.
   echo -n $"Starting $prog: "
   /sbin/modprobe cipcb
   ##### Definicion de las rutas por cada sucursal #######
#Almacen 22
   /usr/sbin/ciped-cb -o /etc/cipe/options.kkk22
  /sbin/route add -net 192.168.1.0 netmask 255.255.255.0 gw 192.168.22.100 dev cipcb0
  /sbin/route add -host 192.168.1.204 gw 192.168.22.100 dev cipcb0
  /sbin/route add -host 192.168.1.1 gw 192.168.22.100 dev cipcb0
   echo
}
stop() {
   # Stop daemons.
   echo -n $"Shutting down $prog: "
   killall ciped-cb
   echo
}

# See how we were called.
case "$1" in
  start)
        start
        ;;
  stop)
        stop
        ;;
  restart|reload)
        stop
        start
        RETVAL=$?
        ;;
  status)
        ;;
  *)
        echo $"Usage: $0 {start|stop|restart|condrestart|status}"
        exit 1
esac
exit $RETVAL
```

En este archivo se agrega la red a la cual se va a conectar, teniendo como Gateway la ip del servidor de VPNs y utilizando el dispositivo virtual para comunicarse con el cliente VPN, además se agregan los host a los que se desea conectar por medio de la VPN y utilizando el dispositivo virtual para transferir los paquetes, en este caso se conecta

Ya con los archivos configurados en el servidor, se inicia el servicio cipe, para verificar que este se esta ejecutando, se utiliza el siguiente comando.

```
vpnserver:/ # /etc/init.d/cipe status
Checking CIPE daemon(s)
for peer 190.5.202.209.                                          running
```

Como se puede apreciar el servicio CIPE esta corriendo y el por ende el demonio CIPE, la dirección ip (peer) que se muestra es la dirección ip publica del cliente VPN el cual es el equipo remoto al cual se conecta el servidor, este servicio ejecuta los archivos de configuración montando el dispositivo virtual (cipcb22) el cual permite establecer el túnel entre el servidor y el almacén 22.

El dispositivo virtual que se monta en el servidor VPN es el siguiente:

Figura 12. Dispositivo virtual CIPE del servidor.

```
cipcb22   Link encap:IPIP Tunnel  HWaddr
          inet addr:192.168.1.14  P-t-P:192.168.22.100  Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP  MTU:1442  Metric:1
          RX packets:1167 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1240 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:134504 (131.3 Kb)  TX bytes:158264 (154.5 Kb)
```

El dispositivo virtual es el encargado de comunicar el servidor con el cliente, lo que quiere decir que la aplicación VPN en el servidor ya esta configurada.

Los parámetros que tiene esta interfaz de red virtual son:

- Addr: dirección ip privada del cliente 192.168.1.14.
- P-t-P: dirección ip privada del servidor 192.168.22.100
- Mask: la mascara de red 255.255.255.255

Ya el servidor esta configurado completamente y esta listo para establecer el túnel VPN.

3.4.2 Configuración del cliente VPN. Para la configuración del cliente hay que tener en cuenta los siguientes pasos.

- Habilitar el reenvío de paquetes para IP versión 4.

```
vpnserver:~ # echo 1 > /proc/sys/net/ipv4/ip_forward
vpnserver:~ # cat /proc/sys/net/ipv4/ip_forward
1
```

Esto proceso se hace con el fin de poder tener comunicación entre los equipos de la red 192.168.22.0 que están detrás del cliente y que además sirva como puerta de enlace al servidor VPN.

- Copiamos la clave de 128 bits del servidor la cual fue previamente generada en este *y la colocamos en el* archivo de configuración del CIPE ubicado en la siguiente ruta /etc/cipe/options.kkk22 en el campo key.

Este archivo de configuración del cliente se describe a continuación.

Nombre del Archivo: **options.kkk22**
Ubicado en la ruta **/etc/cipe/options.kkk22**

En este archivo agregamos la dirección ip de los equipos (cliente y remoto (servidor), el dispositivo virtual, las ip públicas y la key; Las variables que se van a utilizar en este archivo son las siguientes.

- **ipaddr**: dirección ip privada del cliente CIPE . Esta puede ser cualquier dirección IP privada que no se ha utilizado en la red LAN origen.

- **ptpaddr**: dirección ip privada del servidor CIPE . Esta puede ser cualquier dirección IP privada no se haya utilizado en la red LAN destino.

- **my**: dirección ip publica del cliente CIPE, a esta dirección ip se le asigna un número de puerto. El número de puerto puede ser cualquier puerto no utilizado en la máquina origen (cliente).

- **peer**: dirección ip publica del servidor CIPE, a esta dirección ip se le asigna un número de puerto. El número de puerto puede ser cualquier puerto no utilizado en la máquina origen (cliente).

- **key**: clave única. Con esta clave se cifraran todos los datos transmitidos a través del túnel.

El archivo de configuración del cliente queda de la siguiente manera.

Figura 13. Archivo de configuración options.kkk22 del cliente VPN.

```
kkk22:~ # cat /etc/cipe/options.kkk22
# Surprise, this file allows comments (but only on a line by themselves)

# This is probably the minimal set of options that has to be set

# Without a "device" line, the device is picked dynamically

# the peer's IP address
device          cipcb0
#remote internal(fake) ip adress
ptpaddr         192.168.1.14
# my CIPE (fake) ip adress
ipaddr          192.168.22.100
#my real ip adress and cipe port
me              0.0.0.0:7652
#remote real ip adress and cipe port
peer            200.26.145.134:9874
# unique key is 128 bits in hexadecimal notation.
key             3248fd20adf9c00ccf9ecc2393bbb3e4
```

Este archivo debe de tener permisos de lectura y escritura para que exclusivamente sea modificado por el usuario root; Con el siguiente comando se le colocan los permisos.

chmod 600 /etc/cipe/options.kkk22

Luego se verifica si los permisos fueron cambiados.

```
kkk22:~ # ls -l /etc/cipe/options.kkk22
-rw-------    1 root     root          587 Oct 24 15:18 /etc/cipe/options.kkk22
```

Nombre del Archivo: **ciped.kkk22**
Ubicado en la ruta **/etc/init.d/ciped.kkk22**

Este archivo se ejecuta inmediatamente el servicio CIPE se inicia invocando el demonio ciped-cb y levantando el dispositivo virtual para ese almacén que para este caso es el almacén # 22.

Además en este archivo se agrega la red a la cual se va a conectar, teniendo como Gateway la ip del cliente VPN y utilizando el dispositivo virtual para comunicarse con el servidor.

Por ultimo en este archivo se agregan los host a los cuales el cliente se va a conectar por medio del túnel, estos son el servidor VPN con una IP 192.168.1.14 y el servidor de domicilios con la IP 192.168.1.204.

Figura 14. Archivo de configuración ciped.kkk22 del servidor VPN.

```
start() {
   # Start daemons.
   echo -n $"Starting $prog: "
   /sbin/modprobe cipcb0
   ##### Definicion de las rutas por cada sucursal #######

#Almacen 22
   /usr/sbin/ciped-cb -o /etc/cipe/options.kkk22

   /sbin/route add -net 192.168.1.0 netmask 255.255.255.0 gw 192.168.22.100 dev cipcb0
   /sbin/route add -host 192.168.1.204 gw 192.168.22.100 dev cipcb0
   echo
}

stop() {
   # Stop daemons.
   echo -n $"Shutting down $prog: "
   killall ciped-cb
   echo
}

# See how we were called.
case "$1" in
  start)
        start
        ;;
  stop)
        stop
        ;;
  restart|reload)
        stop
        start
        RETVAL=$?
        ;;
  status)
        ;;
  *)
        echo $"Usage: $0 {start|stop|restart|condrestart|status}"
        exit 1
esac

exit $RETVAL
```

Ya con los archivos configurados en el cliente, se inicia el servicio cipe, para verificar que este se esta ejecutando, se utiliza el siguiente comando.

```
kkk22:~ # /etc/init.d/cipe status
Checking CIPE daemon(s)
for peer 200.26.145.134.                                    running
```

Como se puede apreciar el servicio CIPE esta corriendo y el por ende el demonio CIPE, la dirección ip (peer) que se muestra es la dirección ip publica del servidor VPN el cual es el equipo remoto al cual se conecta el cliente, este servicio ejecuta los archivos de configuración montando el dispositivo virtual (cipcb0) el cual permite establecer el túnel entre los dos equipos.

El dispositivo virtual que se monta en el equipo cliente es el siguiente:

Figura 15. Dispositivo virtual CIPE del cliente.

```
cipcb0    Link encap:IPIP Tunnel  HWaddr
          inet addr:192.168.22.100  P-t-P:192.168.1.14  Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP  MTU:1442  Metric:1
          RX packets:633 errors:0 dropped:0 overruns:0 frame:0
          TX packets:633 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:70896 (69.2 Kb)  TX bytes:83556 (81.5 Kb)
```

El dispositivo virtual es el encargado de comunicar el cliente con el servidor, lo que quiere decir que la aplicación VPN en el cliente ya esta configurada.

Los parámetros que tiene esta interfaz de red virtual son:

- Addr: dirección ip privada del cliente 192.168.22.100.
- P-t-P: dirección ip privada del servidor 192.168.1.14
- Mask: la mascara de red 255.255.255.255

Ya el cliente esta configurado completamente y esta listo para establecer el túnel VPN.

3.5 FUNCIONAMIENTO DE LA VPN.

El funcionamiento del servidor y el cliente VPN se describe detalladamente a continuación.

3.5.1 Funcionamiento del servidor VPN. Con la arquitectura de red ya definida, el servicio CIPE corriendo y las maquinas cliente y el servidor ya configuradas procedemos a verificar y a colocar en funcionamiento la VPN.

Para verificar que el software VPN (CIPE) funciona correctamente en el servidor, seguimos los siguientes pasos:

Se configuran las dos tarjetas de red, en una se le coloca la ip privada y en la otra la ip publica, además ya con el servicio CIPE corriendo debe de ya estar montado e dispositivo virtual CIPE el cual actúa como interfaz de red; para verificar si ya estas se encuentran montadas y funcionando, con el siguiente comando.

Figura 16. Tarjetas de Red (eth0 (IP pública) y eth1 (IP privada)) y dispositivo virtual (cipcb22).

```
vpnserver:~ # ifconfig
cipcb22   Link encap:IPIP Tunnel  HWaddr
          inet addr:192.168.1.14  P-t-P:192.168.22.100  Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP  MTU:1442  Metric:1
          RX packets:1167 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1240 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:134504 (131.3 Kb)  TX bytes:158264 (154.5 Kb)


eth0      Link encap:Ethernet  HWaddr 00:13:F7:A7:75:96
          inet addr:200.26.145.134  Bcast:200.26.145.135  Mask:255.255.255.248
          inet6 addr: fe80::213:f7ff:fea7:7596/10 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:141297 errors:0 dropped:0 overruns:0 frame:0
          TX packets:114461 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:18546191 (17.6 Mb)  TX bytes:17989353 (17.1 Mb)
          Interrupt:3 Base address:0x6f00

eth1      Link encap:Ethernet  HWaddr 00:11:43:04:20:D9
          inet addr:192.168.1.14  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::211:43ff:fe04:20d9/10 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:542624 errors:0 dropped:0 overruns:0 frame:0
          TX packets:33835 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:39453946 (37.6 Mb)  TX bytes:6479361 (6.1 Mb)
          Interrupt:9 Base address:0xddc0 Memory:fe9e0000-0

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:134 errors:0 dropped:0 overruns:0 frame:0
          TX packets:134 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:8738 (8.5 Kb)  TX bytes:8738 (8.5 Kb)
```

El comando ifconfig me permite ver las interfaces de red que poseo en mi equipo, proporcionando información acerca de ellas.

3.5.2 Enrutamiento del servidor VPN. Para verificar que el ruteo se esté llevando acabo de forma efectiva, se ejecuta el comando netstat –r, este muestra la tabla de ruteo “routing table” del sistema, también se obtiene la misma salida con el comando route. Donde se generar la tabla que se muestra en la figura 17:

Figura 17. Tabla de ruteo en el servidor VPN.

```
vpnserver:~ # netstat -r
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
192.168.22.100  *               255.255.255.255 UH       40 0          0 cipcb22
200.26.145.128  *               255.255.255.248 U        40 0          0 eth0
192.168.1.0     *               255.255.255.0   U        40 0          0 eth1
default         200.26.145.129  0.0.0.0         UG       40 0          0 eth0
```

En la tabla de enrutamiento anterior (figura 17), se observa que el dispositivo virtual tiene una bandera UH. La U significa que esta lista a ser usada y el H nos indica que esta ruta pertenece a un host que para nuestro caso es el cliente VPN con la dirección IP 192.168.22.100.

Otras redes pueden ser agregadas a la tabla de enrutamiento. Para especificar la ruta exacta que deben seguir, cada ruta se especificará mediante el comando route. Por ejemplo, para el almacén 22 se necesita agregar la red (192.168.22.0) con máscara 255.255.255.0 a través de un gateway (192.168.1.14) el cual es la ip privada del servidor y utiliza el dispositivo virtual cipcd22 para tener comunicación por medio del túnel. Por ejemplo el comando que se utiliza para agregar la ruta antes mencionada se utiliza la siguiente línea.

#route add -net 192.168.22.0 netmask 255.255.255.0 gw 192.168.1.14 dev cipcb22

Luego se realiza pruebas de conectividad desde el servidor VPN al cliente VPN, estas consisten en alcanzar el cliente VPN por medio del comando ping.

Desde el servidor VPN se ejecutan las pruebas de funcionamiento, estas consisten en lo siguiente:

- Primero hacer un ping a www.google.com para saber si está navegando en internet.

- Luego un ping a la IP del gateway remoto (cliente VPN) 192.168.22.254.

- por último se hace un ping al IP del equipo cliente VPN el cual esta detrás del gateway remoto (192.168.22.100).

Figura 18. Pruebas de funcionamiento del servidor VPN utilizando el comando ping.

Prueba de conectividad hacia la internet

```
vpnserver:~ # ping www.google.com
PING www.l.google.com (209.85.165.104) from 200.26.145.134 : 56(84) bytes of data.
64 bytes from eo-in-f104.google.com (209.85.165.104): icmp_seq=1 ttl=245 time=91.6 ms
64 bytes from eo-in-f104.google.com (209.85.165.104): icmp_seq=2 ttl=245 time=90.6 ms
64 bytes from eo-in-f104.google.com (209.85.165.104): icmp_seq=3 ttl=245 time=92.6 ms
64 bytes from eo-in-f104.google.com (209.85.165.104): icmp_seq=4 ttl=245 time=90.8 ms
64 bytes from eo-in-f104.google.com (209.85.165.104): icmp_seq=5 ttl=245 time=90.1 ms

--- www.l.google.com ping statistics ---
5 packets transmitted, 5 received, 0% loss, time 4034ms
rtt min/avg/max/mdev = 90.194/91.205/92.674/0.945 ms
```

Prueba de conexion entre el servidor y el router remoto (cliente)

```
vpnserver:~ # ping 192.168.22.254
PING 192.168.22.254 (192.168.22.254) from 200.26.145.134 : 56(84) bytes of data.
64 bytes from 192.168.22.100: icmp_seq=1 ttl=64 time=43.5 ms
64 bytes from 192.168.22.100: icmp_seq=2 ttl=64 time=45.2 ms
64 bytes from 192.168.22.100: icmp_seq=3 ttl=64 time=41.8 ms
64 bytes from 192.168.22.100: icmp_seq=4 ttl=64 time=46.2 ms
64 bytes from 192.168.22.100: icmp_seq=5 ttl=64 time=42.5 ms
64 bytes from 192.168.22.100: icmp_seq=6 ttl=64 time=43.4 ms

--- 192.168.22.254 ping statistics ---
6 packets transmitted, 6 received, 0% loss, time 5046ms
rtt min/avg/max/mdev = 41.816/43.798/46.289/1.531 ms
```

Prueba de conexion entre el servidor y el cliente a traves del tunel VPN

```
vpnserver:~ # ping 192.168.22.100
PING 192.168.22.100 (192.168.22.100) from 192.168.1.14 : 56(84) bytes of data.
64 bytes from 192.168.22.100: icmp_seq=1 ttl=64 time=43.5 ms
64 bytes from 192.168.22.100: icmp_seq=2 ttl=64 time=45.2 ms
64 bytes from 192.168.22.100: icmp_seq=3 ttl=64 time=41.8 ms
64 bytes from 192.168.22.100: icmp_seq=4 ttl=64 time=46.2 ms
64 bytes from 192.168.22.100: icmp_seq=5 ttl=64 time=42.5 ms
64 bytes from 192.168.22.100: icmp_seq=6 ttl=64 time=43.4 ms

--- 192.168.22.100 ping statistics ---
6 packets transmitted, 6 received, 0% loss, time 5046ms
rtt min/avg/max/mdev = 41.816/43.798/46.289/1.531 ms
```

En la primera prueba de funcionamiento se muestra que el servidor VPN puede navegar en Internet haciendo un ping a una pagina en internet que para el ejemplo fue www.google.com, esto significa que tiene conexión hacia la red publica la cual va hacer el medio donde van a transitar los datos a través del túnel.

La segunda prueba muestra que existe conexión entre el servidor VPN y el router del cliente VPN, esto significa que ya podemos pasar a través de el y llegar a el cliente VPN.

Por ultimo se muestra la conectividad que hay entre el servidor VPN y el cliente VPN por medio del túnel, esto demuestra que ya existe un túnel VPN ya esta establecido proporcionando una conexión VPN utilizando el CIPE como VPN por software.

Para verificar que el túnel está funcionando, se checa el registro (log), el cual se encarga de recoger los mensajes generados por el demonio CIPE, estos registros se guardan en el fichero /var/log/cipe.log, para mostrar la salida del log utilizamos el comando tail –N donde N son las ultimas N líneas del fichero o directorio donde se encuentra ubicado el registro de CIPE, por ejemplo:

Figura 19. Verificación del túnel en funcionamiento.

```
vpnserver:~ # tail -9  /var/log/cipe.log
Oct 31 15:29:42 UP   cipcb22 200.26.145.134:9874 27069 192.168.1.14 192.168.22.100
Oct 31 15:34:38 DOWN cipcb22 200.26.145.134:9874 27069 192.168.1.14 192.168.22.100
Oct 31 15:34:38 UP   cipcb22 200.26.145.134:9874 27449 192.168.1.14 192.168.22.100
Oct 31 15:36:41 DOWN cipcb22 200.26.145.134:9874 27449 192.168.1.14 192.168.22.100
Oct 31 15:36:41 UP   cipcb22 200.26.145.134:9874 27540 192.168.1.14 192.168.22.100
Nov 04 17:17:08 DOWN cipcb22 200.26.145.134:9874 27540 192.168.1.14 192.168.22.100
Nov 05 09:44:09 UP   cipcb22 200.26.145.134:9874 1555 192.168.1.14 192.168.22.100
Nov 06 11:55:05 DOWN cipcb22 200.26.145.134:9874 1555 192.168.1.14 192.168.22.100
Nov 06 11:55:05 UP   cipcb22 200.26.145.134:9874 7971 192.168.1.14 192.168.22.100
```

En la figura 19 se muestra la fecha y la hora en la cual se activo o desactivo el túnel VPN entre las dos redes mostrando las IPs, el dispositivo virtual CIPE con el respectivo puerto utilizado en el servidor para realizar la VPN.

3.5.3 Funcionamiento del cliente VPN. Para verificar que el software VPN (CIPE) funciona correctamente en el cliente, seguimos los siguientes pasos:

Se configuran el router, este router que se maneja en la estación de trabajo del cliente permite hacer NAT, en este colocamos la dirección IP pública fija proporcionada por la ISP y el enrutador por defecto el cual es 192.168.1.254. Luego se configura la tarjeta de red del equipo colocándole la ip privada que para nuestro caso es la 192.168.22.100.

Con el servicio CIPE corriendo en el cliente, este monta el dispositivo virtual CIPE el cual actúa como una interfaz de red; para verificar si ya estas se encuentra montada la tarjeta de red y el dispositivo virtual se debe ejecutar el siguiente comando.

Figura 20. Tarjetas de Red (eth0 (IP privada)) y dispositivo virtual (cipcb0).

```
kkk22:~ # ifconfig
cipcb0    Link encap:IPIP Tunnel  HWaddr
          inet addr:192.168.22.100  P-t-P:192.168.1.14  Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP  MTU:1442  Metric:1
          RX packets:4 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:448 (448.0 b)  TX bytes:528 (528.0 b)

eth0      Link encap:Ethernet  HWaddr 00:14:5E:5C:38:EC
          inet addr:192.168.22.100  Bcast:192.168.22.255  Mask:255.255.255.0
          inet6 addr: fe80::214:5eff:fe5c:38ec/10 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:49 errors:0 dropped:0 overruns:0 frame:0
          TX packets:48 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:7101 (6.9 Kb)  TX bytes:6663 (6.5 Kb)
          Interrupt:11 Memory:d8100000-d8110000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:53 errors:0 dropped:0 overruns:0 frame:0
          TX packets:53 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:4195 (4.0 Kb)  TX bytes:4195 (4.0 Kb)
```

El comando ifconfig me permite ver las interfaces de red que poseo en mi equipo, proporcionando información acerca de ellas.

3.5.4 Enrutamiento del cliente VPN. Para verificar que el ruteo se esté llevando acabo de forma efectiva, se ejecuta el comando netstat –r, este muestra la tabla de ruteo “routing table” del sistema también, también se obtiene la misma salida con el comando route. Donde se generar la siguiente tabla:

Figura 21. Tabla de ruteo en el cliente VPN.

```
kkk22:~ # netstat -r
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
kkkfun.arka.com kkk22.arka.com. 255.255.255.255 UGH      40 0          0 cipcb0
192.168.1.14    *               255.255.255.255 UH       40 0          0 cipcb0
192.168.22.0    *               255.255.255.0   U        40 0          0 eth0
default         192.168.22.254  0.0.0.0         UG       40 0          0 eth0
```

En la figura 21, se observa que el dispositivo virtual cipcb0 esta dos veces lo que quiere decir que existen dos ruteos a través del túnel estos se describen a continuación:

En la primera fila se indica el ruteo que hay entre el cliente (kkk22.arka.com) y el servidor de domicilios (kkkfun.arka.com), este tiene una bandera UGH, la U significa que esta lista ser usada, la G nos indica que en la conexión interviene un Gateway diferente al que se tiene por default y la H que la ruta pertenece a un host.

En la segunda fina nos indica el ruteo que existe entre el cliente y el servidor VPN, este tiene una bandera UH, la U significa que esta lista ser usada y el H nos indica que esta ruta pertenece a un host.

Los enrutamientos del cliente VPN se describen a continuación:

Primero se especifica la ruta mediante el comando route, adicionando el gateway y el dispositivo o interfaz de red que se le asigna, para que por medio de este exista comunicación a través del túnel.

Por ejemplo, para el cliente VPN se utiliza se manejan varios ruteos:

- El primer ruteo se hace para tener comunicación a través del túnel con el servidor de VPNs por medio del dispositivo virtual CIPE (cipcb0), la ip que utiliza este servidor es 192.168.1.14 y tiene como Gateway a la ip 192.168.22.100 la cual es la ip privada del cliente VPN como se muestra a continuación.

route add -host 192.168.1.14 gw 192.168.22.100 dev cipcb0

- el segundo ruteo se usa para comunicarse con el servidor de domicilios a través del túnel por medio del dispositivo virtual CIPE (cipcb0), la ip que utiliza este servidor es 192.168.1.204 y tiene como Gateway a la ip 192.168.22.100 la cual es la ip privada del cliente VPN como se muestra a continuación.

route add -host 192.168.1.204 gw 192.168.22.100 dev cipcb0

Luego se realiza pruebas de conectividad desde el cliente VPN, estas consisten en alcanzar el servidor VPN y el servidor de domicilios por medio del comando ping.

Desde el cliente VPN se ejecutan las pruebas de funcionamiento, estas consisten en lo siguiente:

- hacer un ping a www.google.com para saber si está navegando en internet.

- un ping a la IP del gateway remoto (servidor VPN) 200.26.145.129.

- un ping al IP privada del servidor VPN el cual esta detrás del gateway remoto (192.168.1.14).

- por ultimo un ping al servidor de domicilios que tiene como ip la 192.168.1.204.

Figura 22. Pruebas de funcionamiento del cliente VPN utilizando el comando ping.

Prueba de conectividad hacia internet

```
kkk22:~ # ping www.google.com
PING www.l.google.com (74.125.45.103) from 192.168.22.100 : 56(84) bytes of data.
64 bytes from yx-in-f103.google.com (74.125.45.103): icmp_seq=1 ttl=246 time=90.7 ms
64 bytes from yx-in-f103.google.com (74.125.45.103): icmp_seq=2 ttl=246 time=83.6 ms
64 bytes from yx-in-f103.google.com (74.125.45.103): icmp_seq=3 ttl=246 time=76.5 ms
64 bytes from yx-in-f103.google.com (74.125.45.103): icmp_seq=4 ttl=246 time=92.1 ms
64 bytes from yx-in-f103.google.com (74.125.45.103): icmp_seq=5 ttl=246 time=86.6 ms

--- www.l.google.com ping statistics ---
5 packets transmitted, 5 received, 0% loss, time 4037ms
rtt min/avg/max/mdev = 76.512/85.947/92.101/5.586 ms
```

Prueba de conexion entre el cliente y el router remoto (servidor)

```
kkk22:~ # ping 200.26.145.129
PING 200.26.145.129 (200.26.145.129) from 192.168.22.100 : 56(84) bytes of data.
64 bytes from 200.26.145.129: icmp_seq=1 ttl=248 time=35.7 ms
64 bytes from 200.26.145.129: icmp_seq=2 ttl=248 time=23.5 ms
64 bytes from 200.26.145.129: icmp_seq=3 ttl=248 time=40.9 ms
64 bytes from 200.26.145.129: icmp_seq=4 ttl=248 time=23.9 ms
64 bytes from 200.26.145.129: icmp_seq=5 ttl=248 time=39.9 ms

--- 200.26.145.129 ping statistics ---
5 packets transmitted, 5 received, 0% loss, time 4037ms
rtt min/avg/max/mdev = 23.514/32.828/40.996/7.630 ms
```

Prueba de conexion entre el cliente y el servidor a traves del tunel VPN

```
kkk22:~ # ping 192.168.1.14
PING 192.168.1.14 (192.168.1.14) from 192.168.22.100 : 56(84) bytes of data.
64 bytes from 192.168.1.14: icmp_seq=1 ttl=64 time=24.3 ms
64 bytes from 192.168.1.14: icmp_seq=2 ttl=64 time=63.1 ms
64 bytes from 192.168.1.14: icmp_seq=3 ttl=64 time=36.1 ms
64 bytes from 192.168.1.14: icmp_seq=4 ttl=64 time=25.1 ms

--- 192.168.1.14 ping statistics ---
5 packets transmitted, 4 received, 20% loss, time 4035ms
rtt min/avg/max/mdev = 24.365/37.213/63.196/15.703 ms
```

Prueba de conexion entre el cliente y el servidor de domicilios a traves del tunel VPN

```
kkk22:~ # ping 192.168.1.204
PING 192.168.1.204 (192.168.1.204) from 192.168.22.100 : 56(84) bytes of data.
64 bytes from 192.168.1.204: icmp_seq=1 ttl=63 time=32.8 ms
64 bytes from 192.168.1.204: icmp_seq=2 ttl=63 time=26.4 ms
64 bytes from 192.168.1.204: icmp_seq=3 ttl=63 time=34.4 ms
64 bytes from 192.168.1.204: icmp_seq=4 ttl=63 time=41.9 ms

--- 192.168.1.204 ping statistics ---
6 packets transmitted, 4 received, 33% loss, time 5038ms
rtt min/avg/max/mdev = 26.466/33.948/41.990/5.526 ms
```

En la primera prueba de funcionamiento se muestra que el cliente VPN puede navegar en Internet haciendo un ping a una pagina en internet que para el ejemplo fue www.google.com, esto significa que tiene conexión hacia la red publica la cual va hacer el medio donde van a transitar los datos a través del túnel.

La segunda prueba muestra que existe conexión entre el cliente VPN y el router del servidor VPN, esto significa que ya podemos pasar a través de el y llegar los equipos que están atrás de el.

La tercera prueba muestra la conectividad que hay entre el cliente VPN y el servidor VPN por medio del túnel, esto demuestra que ya existe un túnel VPN ya esta establecido proporcionando una conexión VPN utilizando el CIPE como VPN por software.

Por ultimo la cuarta prueba muestra la conectividad que hay entre el cliente VPN y el servidor de domicilios por medio del túnel.

Para verificar que el túnel está funcionando, se checa el registro (log), el cual se encarga de recoger los mensajes generados por el demonio CIPE, estos registros se guardan en el fichero /var/log/cipe.log, para mostrar la salida del log utilizamos el comando tail –N donde N son las ultimas N líneas del fichero o directorio donde se encuentra ubicado el registro de CIPE, por ejemplo:

Figura 23. Verificación del túnel en funcionamiento en el cliente VPN.

```
kkk22:/ # tail -9 /var/log/cipe.log
Nov 18 12:22:01 DOWN cipcb0 192.168.22.100:7652 3454 192.168.22.100 192.168.1.14
Nov 18 12:22:01 UP   cipcb0 192.168.22.100:7652 4027 192.168.22.100 192.168.1.14
Nov 18 12:24:00 DOWN cipcb0 192.168.22.100:7652 4027 192.168.22.100 192.168.1.14
Nov 18 12:24:00 UP   cipcb0 192.168.22.100:7652 4098 192.168.22.100 192.168.1.14
Nov 18 12:26:00 DOWN cipcb0 192.168.22.100:7652 4098 192.168.22.100 192.168.1.14
Nov 18 12:26:00 UP   cipcb0 192.168.22.100:7652 4157 192.168.22.100 192.168.1.14
Nov 18 12:28:00 DOWN cipcb0 192.168.22.100:7652 4157 192.168.22.100 192.168.1.14
Nov 18 12:28:00 UP   cipcb0 192.168.22.100:7652 4199 192.168.22.100 192.168.1.14
Nov 18 12:30:01 DOWN cipcb0 192.168.22.100:7652 4199 192.168.22.100 192.168.1.14
```

En la figura 23 se muestra la fecha y la hora en la cual se activo o desactivo el túnel VPN entre las dos redes mostrando las IPs, el dispositivo virtual CIPE con el respectivo puerto utilizado en el cliente para realizar la VPN.

3.6 SEGURIDAD DE LA VPN.

Ya que CIPE es un protocolo que está desarrollado activamente para funcionar en conjunto con iptables, ipchains y otros cortafuegos basados en reglas todo lo que

se necesita es aceptación en par de los paquetes UDP CIPE entrantes para coexistir con las reglas de cortafuegos existentes.

IPtables es un sistema de firewall integrado con el kernel de Linux, es parte del sistema operativo, para poner en marcha solo se necesita aplicar reglas. Para ello se ejecuta el comando iptables, con el que añadimos, borramos, o creamos reglas. Por ello un firewall de iptables no es sino un simple script de shell en el que se van ejecutando las reglas de firewall.

Siguiendo este orden de ideas la seguridad que se va a implantar en cada una de las estaciones de trabajo (cliente y servidor) van a ser basadas en IP tables

3.6.1 Reglas iptables para el servidor VPN. Primero configuramos las reglas para tener acceso total solo desde mi pública y privada de mi servidor de VPNs, con los siguientes comandos:

Iptables para dar acceso total a la ip publica del servidor de VPNs.

iptables -A INPUT -s 200.26.145.134 -j ACCEPT
iptables -A OUTPUT -d 200.26.145.134 -j ACCEPT

Iptables para dar acceso total a la ip privada del servidor de VPNs.

iptables -A INPUT -s 192.168.1.14 -j ACCEPT
iptables -A OUTPUT -s 192.168.1.14 -j ACCEPT

Luego niego el acceso de todos los puertos del servidor de VPNs.

iptables -P INPUT DROP

Ahora abro solo los puertos que son estrictamente necesarios por tcp y udp, para nuestro caso solo abrimos el 53(puerto DNS), 80(puerto HTTP) y el 443(Puerto HTTPS/SSL).

iptables -A INPUT -p udp --dport 53 -j ACCEPT
iptables -A INPUT -p tcp --dport 53 -j ACCEPT
iptables -A INPUT -p udp --sport 53 -j ACCEPT
iptables -A INPUT -p tcp --sport 53 -j ACCEPT

iptables -A INPUT -p udp --dport 80 -j ACCEPT
iptables -A INPUT -p tcp --dport 80 -j ACCEPT
iptables -A INPUT -p udp --sport 80 -j ACCEPT
iptables -A INPUT -p tcp --sport 80 -j ACCEPT

iptables -A INPUT -p udp --dport 443 -j ACCEPT
iptables -A INPUT -p tcp --dport 443 -j ACCEPT
iptables -A INPUT -p udp --sport 443 -j ACCEPT
iptables -A INPUT -p tcp --sport 443 -j ACCEPT

Ahora vamos a colocar las iptables para el almacén 22 en el servidor.
Primero acepto todo el tráfico que venga de la ip 192.168.22.100 la cual es la IP del cliente vpn almacén 22.

iptables -I INPUT -s 192.168.22.100 -j ACCEPT

Ahora acepto todo el tráfico entrante por la IP pública del servidor VPNs 200.26.145.134 por medio del puerto 9874 el cual es el puerto de la ip remota o la ip del almacén 22 (cliente VPN).

iptables -I INPUT -d 200.26.145.134 -p udp --dport 9874 -j ACCEPT

Lo anterior se debe repetir para cada uno de las sucursales.

Luego con el comando iptables –L –n se verifica que se han aplicado las reglas correctamente en el servidor de VPN.

Figura 24. Reglas iptables del servidor VPN.

```
[root@vpnserver root]# iptables -n -L
Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     udp  --  0.0.0.0/0            200.26.145.134      udp dpt:9874
ACCEPT     all  --  192.168.22.100       0.0.0.0/0
ACCEPT     all  --  192.168.1.0/24       0.0.0.0/0
ACCEPT     udp  --  0.0.0.0/0            0.0.0.0/0           udp dpt:53
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:53
ACCEPT     udp  --  0.0.0.0/0            0.0.0.0/0           udp spt:53
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp spt:53
ACCEPT     udp  --  0.0.0.0/0            0.0.0.0/0           udp dpt:80
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:80
ACCEPT     udp  --  0.0.0.0/0            0.0.0.0/0           udp spt:80
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp spt:80
ACCEPT     udp  --  0.0.0.0/0            0.0.0.0/0           udp dpt:443
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:443
ACCEPT     udp  --  0.0.0.0/0            0.0.0.0/0           udp spt:443
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp spt:443

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  0.0.0.0/0            200.26.145.134
ACCEPT     all  --  192.168.1.0/24       0.0.0.0/0
[root@vpnserver root]#
```

En la figura 24 se muestra la configuración de seguridad para el servidor VPNs, donde básicamente se acepta la ip privada del cliente (192.168.22.100) y el puerto donde este ingresa (9874), además se restringe el acceso a los equipos de mi red para que solo puedan ser modificadas las reglas desde el equipo donde estas se encuentran en este caso en el servidor VPNs.

Estas reglas nos dan la plena seguridad de que un intruso no pueda ingresar a el servidor VPN, ha modificar las reglas o en el peor de los casos dañar el sistema completamente ya que solo puede acceder el cliente.

3.6.2 Reglas iptables para el cliente VPN. Primero configuramos las reglas para tener acceso total solo desde mi IP privada, con los siguientes comandos:

```
iptables -A INPUT -s 192.168.22.100 -j ACCEPT
iptables -A OUTPUT -s 192.168.22.100 -j ACCEPT
```

Luego niego el acceso de todos los puertos del servidor de VPNs.

```
iptables -P INPUT DROP
```

Ahora abro solo los puertos que son estrictamente necesarios por tcp y udp, para nuestro caso solo abrimos el 53(puerto DNS), 80(puerto HTTP) y el 443(Puerto HTTPS/SSL).

```
iptables -P INPUT DROP
iptables -A INPUT -p udp --dport 53 -j ACCEPT
iptables -A INPUT -p tcp --dport 53 -j ACCEPT
iptables -A INPUT -p udp --sport 53 -j ACCEPT
iptables -A INPUT -p tcp --sport 53 -j ACCEPT

iptables -A INPUT -p udp --dport 80 -j ACCEPT
iptables -A INPUT -p tcp --dport 80 -j ACCEPT
iptables -A INPUT -p udp --sport 80 -j ACCEPT
iptables -A INPUT -p tcp --sport 80 -j ACCEPT

iptables -A INPUT -p udp --dport 443 -j ACCEPT
iptables -A INPUT -p tcp --dport 443 -j ACCEPT
iptables -A INPUT -p udp --sport 443 -j ACCEPT
iptables -A INPUT -p tcp --sport 443 -j ACCEPT
```

Ahora vamos a colocar las iptables para el almacén 22 para el cliente. Primero acepto todo el tráfico que venga de la ip 192.168.1.14 la cual es la ip del servidor vpn.

```
iptables -I INPUT -s 192.168.1.14 -j ACCEPT
```

Ahora acepto todo el tráfico entrante por la IP pública del servidor VPNs 192.168.22.100 por medio del puerto 7652 el cual es el puerto de la ip remota o la ip del almacén 22 (cliente VPN).

iptables -I INPUT -d 192.168.22.100 -p udp --dport 7652 -j ACCEPT

Lo anterior se debe repetir para cada uno de los sucursales.

Estas reglas nos dan la plena seguridad de que un intruso no pueda ingresar al cliente VPN, ha modificar las reglas o en el peor de los casos dañar el sistema completamente, ya que solo puede acceder el servidor VPN.

Figura 25. Reglas iptables del cliente VPN.

```
kkk22:~ # iptables -n -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     udp  --  0.0.0.0/0            192.168.22.100      udp dpt:7652
ACCEPT     all  --  192.168.1.14         0.0.0.0/0
ACCEPT     all  --  192.168.22.100       0.0.0.0/0
ACCEPT     udp  --  0.0.0.0/0            0.0.0.0/0           udp dpt:53
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:53
ACCEPT     udp  --  0.0.0.0/0            0.0.0.0/0           udp spt:53
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp spt:53
ACCEPT     udp  --  0.0.0.0/0            0.0.0.0/0           udp dpt:80
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:80
ACCEPT     udp  --  0.0.0.0/0            0.0.0.0/0           udp spt:80
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp spt:80
ACCEPT     udp  --  0.0.0.0/0            0.0.0.0/0           udp dpt:443
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:443
ACCEPT     udp  --  0.0.0.0/0            0.0.0.0/0           udp spt:443
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp spt:443

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  192.168.22.100       0.0.0.0/0
kkk22:~ #
```

En la figura 25 se muestra la configuración de seguridad del cliente VPN, donde básicamente se acepta la ip privada del servidor VPN (192.168.1.14) y el puerto donde este ingresa (7652), además se restringe el acceso a los equipos de mi red para que solo puedan ser modificadas las reglas desde el equipo donde estas se encuentran en este caso en el cliente VPN.

Las reglas iptables nos da la plena seguridad de que un intruso no pueda ingresar al cliente VPN, ha modificar las reglas o en el peor de los casos dañar el sistema completamente.

4. PLAN DE PRUEBAS

En esta sección, se mostrarán las pruebas del servicio de conexión de la VPN implementada, además de las de conectividad, tráfico y seguridad de la VPN. Algunas de las pruebas realizadas son para validar el correcto funcionamiento del proyecto realizado.

Las pruebas del servicio de conectividad, trafico y seguridad de la VPN se realizaran con el comando ping el cual valida si existe o no conexión a través del túnel, también se utilizara la aplicación iptraf, este es un programa informático basado en consola que proporciona estadísticas de red.

La seguridad de la VPN esta basada en reglas mediante IPTABLES, estas lo que hacen es permitir el acceso a denegar el mismo.

Para hacer las pruebas de la VPN se utilizará el método de la caja negra, el cual consiste en intentar penetrar la red sin tener conocimientos del sistema emulando ser un usuario común.

El objetivo de esa sección es realizar un Informe de pruebas entre el servidor VPN y el cliente VPN, validando el servicio de conexión, trafico y seguridad de la VPN y utilizando la metodología de prueba de caja negra para verificar la eficiencia del sistema de seguridad configurado en las maquinas.

4.1 PRUEBA DE CONEXIÓN

Para probar que una red funcione de manera adecuada, existe una utilidad muy práctica que se suministra como una prestación estándar con la mayoría de los sistemas operativos. Se trata del comando ping. Los ping le permiten enviar paquetes de datos a un equipo en una red y evaluar el tiempo de respuesta.

Para conectarnos tanto al servidor como al cliente VPN de forma remota y por línea de comandos, utilizamos una aplicación llamada PuTTY (este es un programa de distribución gratuita que puede ser utilizada bajo un entorno Windows XP o Windows vista el cual permite hacer Telnet y SSH, a maquinas de manera remota, además se puede descargar de forma gratuita por Internet).

Para todas las pruebas se harán los siguientes pasos:

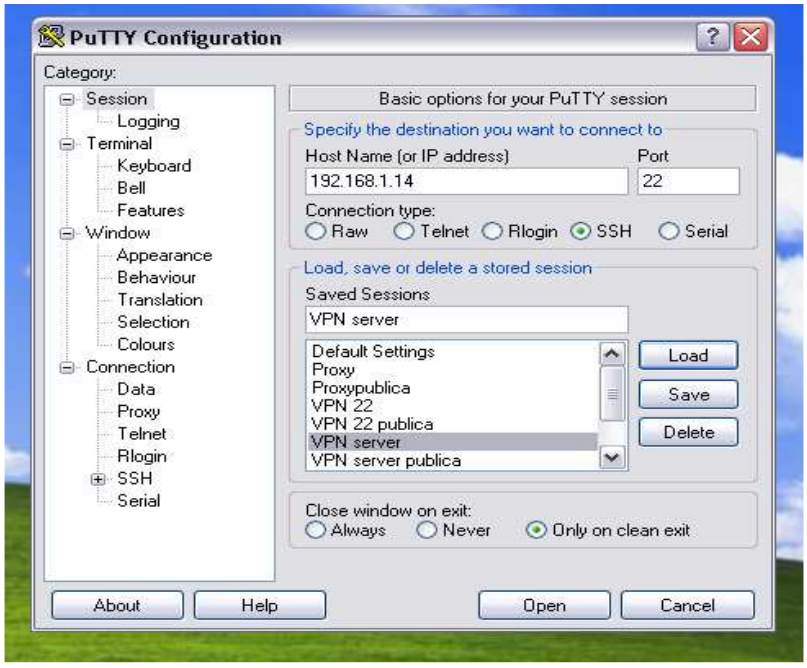
- Empezaremos por ejecutar el PuTTY desde un equipo localizado fuera de la Red LAN de la empresa, que haya sido autorizado previamente en el servidor a través de las IPTABLES, y que además tenga acceso a Internet.

- Luego escribimos la dirección IP del servidor al cual queremos accesar en la casilla llamada **Host Name (or IP address).**

- Digitamos el numero de puerto por el cual se quiere acceder en la casilla llamada **Port.**

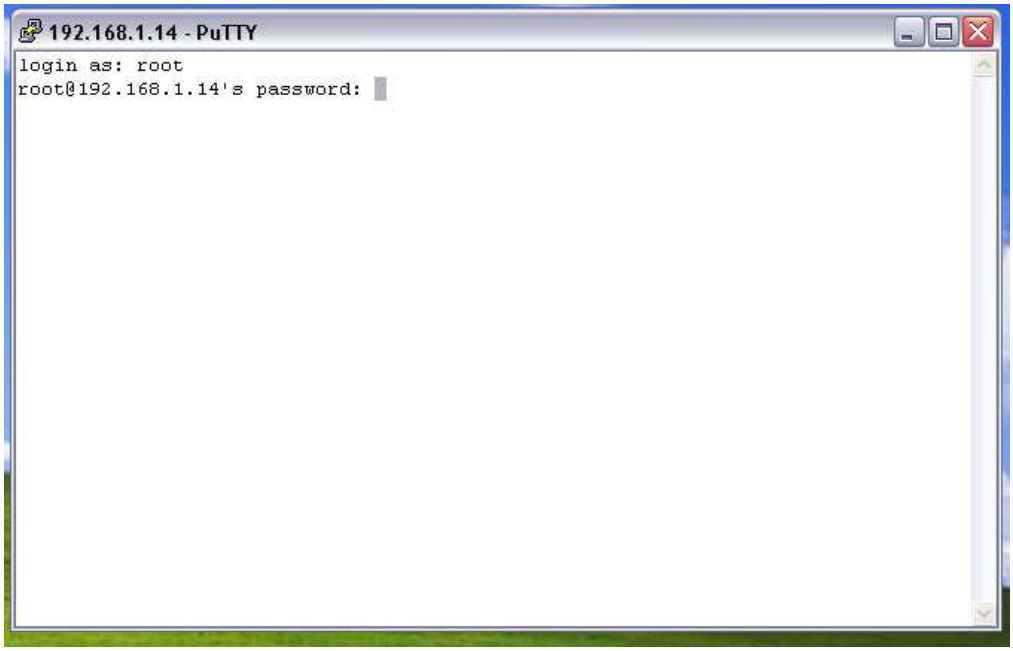
- Seleccionamos la opción de la función que queremos ejecutar (para este primer caso haremos un SSH) y hacemos click en la opción **Open**, tal como se muestra en la figura 26.

Figura 26. Muestra como ingresar al servidor o al cliente VPN desde la aplicación PuTTY.



- Entonces de manera remota acceso por medio de SSH hasta el servidor de VPNs que tiene la IP 192.168.1.14 y tiene como puerto de acceso el 22, y muestra una ventana en la cual me pide digitar el login y el password y allí ya podré trabajar dentro de este, tal como se muestra en la figura 27.

Figura 27. Ventana de Ingreso al servidor VPN



- Ahora el proceso Será, dentro del servidor del servidor VPN hacer la prueba de conexión con el cliente VPN utilizando el comando ping como se denota en la figura 28.

Figura 28. Prueba de conexión entre el servidor y el cliente VPN

```
vpnserver:~ # ping 192.168.22.100
PING 192.168.22.100 (192.168.22.100) from 192.168.1.14 : 56(84) bytes of data.
64 bytes from 192.168.22.100: icmp_seq=1 ttl=64 time=43.4 ms
64 bytes from 192.168.22.100: icmp_seq=2 ttl=64 time=42.2 ms

--- 192.168.22.100 ping statistics ---
2 packets transmitted, 2 received, 0% loss, time 1010ms
rtt min/avg/max/mdev = 42.228/42.860/43.493/0.665 ms
```

- Hacemos el mismo procedimiento para el cliente VPN como se muestra en la figura 29.

Figura 29. Pruebas de conexión entre el cliente y el servidor VPNs.

```
kkk22:~ # ping 192.168.1.14
PING 192.168.1.14 (192.168.1.14) from 192.168.22.100 : 56(84) bytes of data.
64 bytes from 192.168.1.14: icmp_seq=1 ttl=64 time=42.4 ms
64 bytes from 192.168.1.14: icmp_seq=3 ttl=64 time=44.0 ms
64 bytes from 192.168.1.14: icmp_seq=4 ttl=64 time=42.2 ms

--- 192.168.1.14 ping statistics ---
4 packets transmitted, 3 received, 25% loss, time 3018ms
rtt min/avg/max/mdev = 42.248/42.942/44.099/0.823 ms
```

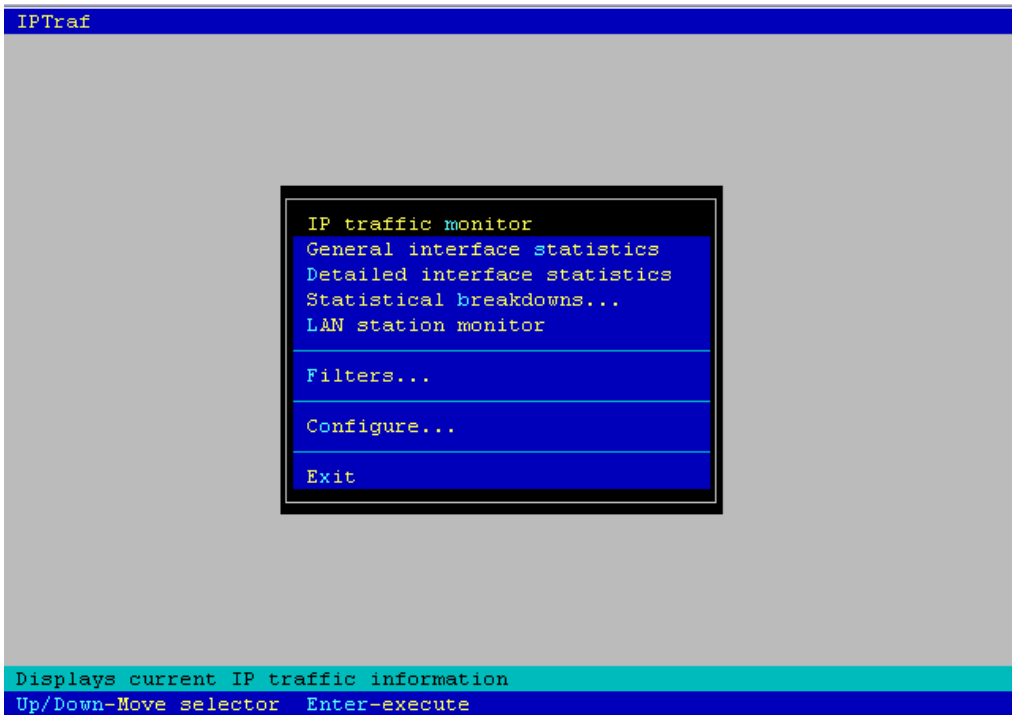
4.2 PRUEBAS DE TRÁFICO

Para las pruebas de trafico se harán con la aplicación IPTraf, el cual funciona recolectando información de las conexiones TCP, como las estadísticas y la actividad de las interfaces, así como las caídas de tráfico TCP y UDP. Se encuentra disponible en sistemas operativos GNU/Linux. La información que entrega esta utilidad de monitoreo de redes es la siguiente:

- Conteo de bytes de paquetes IP, TCP, UDP, ICMP, no-IP
- Direcciones y puertos de fuentes y destinos TCP
- Paquetes TCP y conteo de bytes
- Estados de banderas TCP
- Información de fuentes y destinos UDP
- Estadística de servicios TCP y UDP
- Interfaz de conteo de paquetes
- Interfaz de indicadores de actividad
- Estadística de la estación LAN

El comando para ejecutar la aplicación es iptraf, este se inicia en modo interactivo, con facilidad de acceder a sus opciones a través de un menú como se muestra en la figura 30.

Figura 30. Monitoreo de trafico IP en IPTraf



Para las pruebas a realizar se va a usar la primera opción del menú de iptraf la cual es monitor de tráfico IP. Este es un sistema de monitoreo en tiempo real que intercepta todos los paquetes en todas las interfaces de red detectadas.

En la interfaz de monitoreo del programa IPTraf se muestra dos ventas, estas se describen a continuación:

La ventana superior muestra las conexiones TCP detectadas actualmente. La información entregada en esta ventana es:

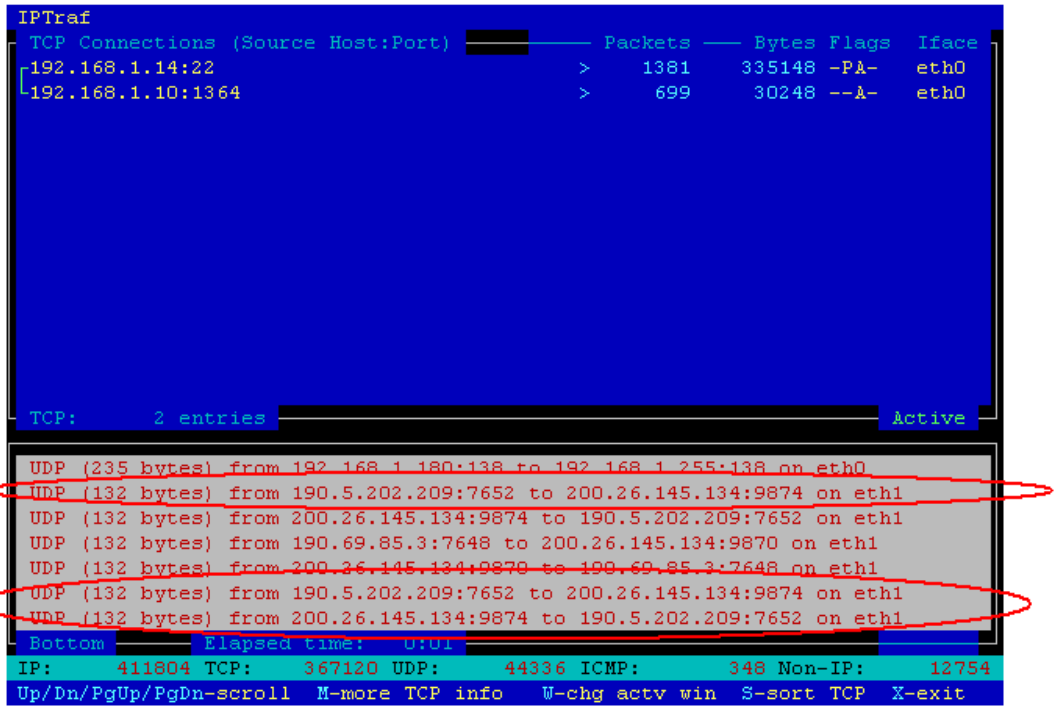
- Dirección de la fuente y puerto
- Conteo de paquetes
- Conteo de bytes
- Tamaño del paquete
- Estado de las banderas TCP
- Interfaz utilizada

La ventana inferior muestra información acerca de otros tipos de tráfico en la red. Los protocolos detectados son los siguientes:

- User Datagram Protocol (UDP)

- Internet Control Message Protocol (ICMP)
- Open Shortest-Path First (OSPF)
- Interior Gateway Routing Protocol (IGRP)
- Interior Gateway Protocol (IGP)
- Internet Group Management Protocol (IGMP)
- General Routing Encapsulation (GRE)
- Address Resolution Protocol (ARP)
- Reverse Address Resolution Protocol (RARP

Figura 31. Pruebas de tráfico entre el servidor y el cliente VPN.



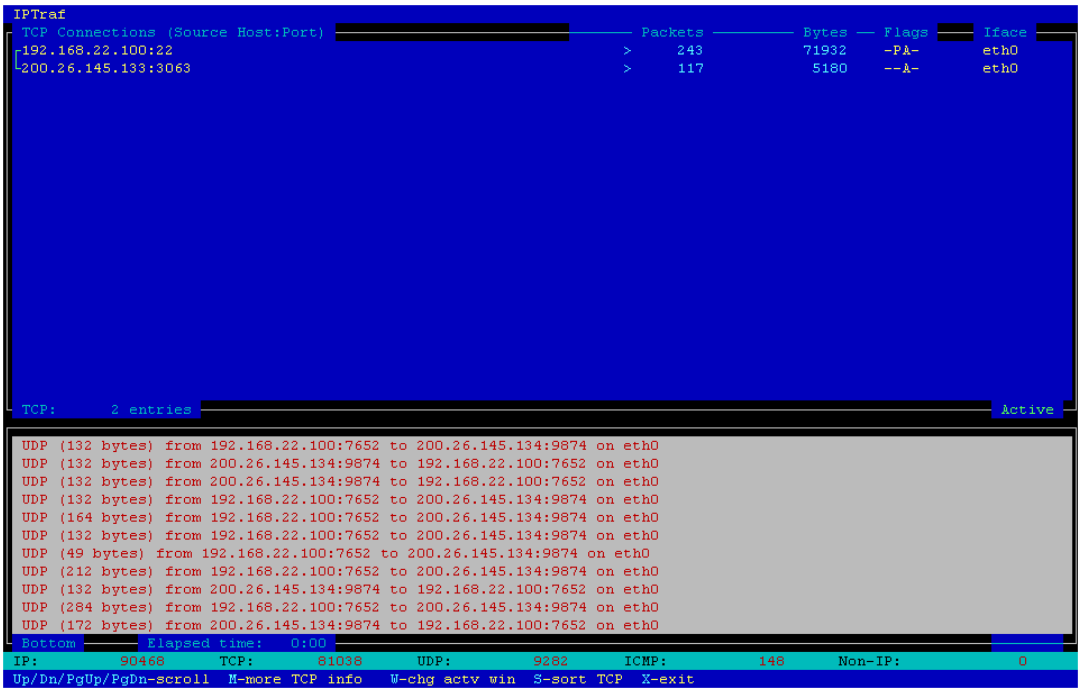
En la figura 31. Se muestra el trafico IP generado por el cliente con el comando ping, enviando paquetes al servidor.

En la ventana superior se muestra las IPs de los equipos conectados entre si en el servidor VPN y los puerto de los mismos.

Para este caso la primera ip que se muestra es la ip del equipo al cual me estoy conectando la cual es 192.168.1.14 y por el puerto 22 el cual es del ssh usado por el PUTTY, la segunda IP que muestra es la IP del equipo remoto, es decir la IP del equipo el cual estoy ejecutando el PUTTY.

Para el cliente hacemos el mismo procedimiento, para ello se utiliza el comando ping desde el servidor enviando paquetes hacia el cliente como se denota en la figura 32.

Figura 32. Pruebas de tráfico entre el cliente y el servidor VPN.



En la ventana superior se muestra las IPs de los equipos conectados entre si en el cliente VPN y los puerto de los mismos.

Para este caso la primera ip que se muestra es la ip del equipo al cual me estoy conectando la cual es 192.168.22.100 y por el puerto 22 el cual es del ssh usado por el PUTTY, la segunda IP que muestra es la IP del equipo remoto, para este caso la ip que muestra es la ip del proxy de la empresa ya que el equipo donde se esta ejecutando el PUTTY esta dentro de la red LAN, por fuera este se identifica con la ip publica del proxy, no hay que olvidar que los paquetes son enviados por medio del servidor VPN y no por el proxy, como se muestra en la ventana inferior donde se muestra los paquetes UDP enviados desde el servidor con el comando ping, donde se muestra la IP publica y el puerto del CIPE del servidor y viceversa.

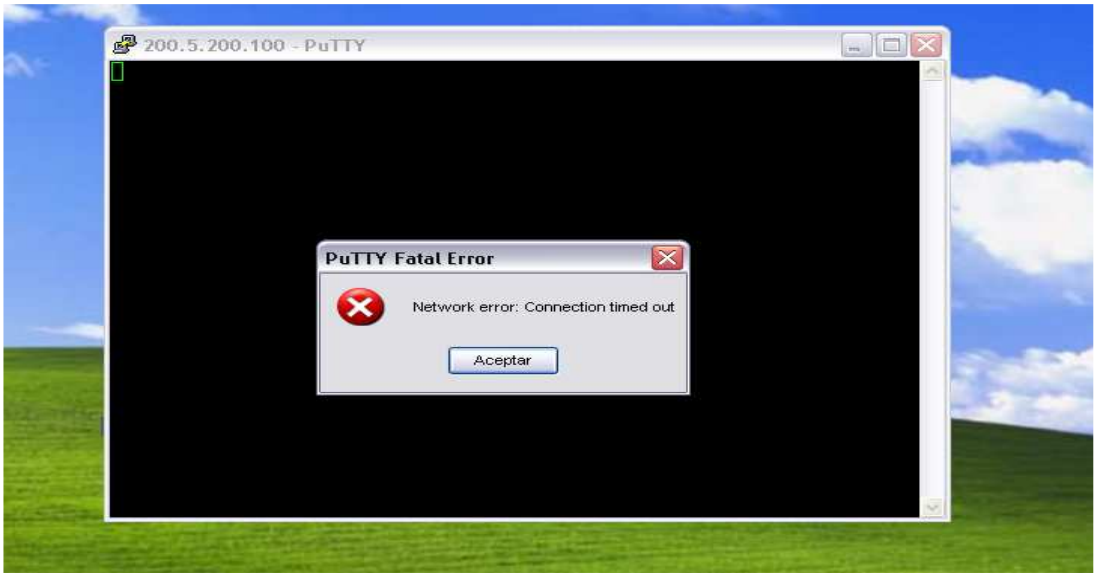
4.3 PRUEBAS DE SEGURIDAD

Las pruebas de seguridad serán basadas en IPTABLES, las cuales son reglas que me permiten o me deniegan el acceso hacia un equipo determinado como se explico en el capitulo de instalación y configuración de la vpn en el punto 3.5 seguridad de este documento.

4.3.1 Prueba de intrusión a un equipo en la red VPN. Desde un equipo cualquiera fuera de la red se ejecuta el PUTTY, y se trata de acceder al cliente VPN.

Debido a que la dirección IP del equipo desde el cual estoy realizando el ssh no es conocida por el equipo VPN, el programa muestra una ventana tipo terminal en negro con un mensaje de error debido a que no encontró conexión, tal como se muestra en la figura 33

Figura 33. Prueba de intrusión desde un equipo cualquiera en Internet hacia un equipo de la red VPN.



Para denegar el acceso a equipos fuera de la red, se utilizan reglas iptables las cuales permiten solo equipos autorizados por las mismas, es decir solo va a aceptar el trafico desde la ip permitida por la regla.

Debido a que este proceso es repetitivo, ya que para cada uno de los puertos habría que ejecutar el mismo comando solo se mostrara un ejemplo.

A continuación se muestra un ejemplo utilizando el cliente vpn, en donde se niega el acceso a todos los usuarios que deseen ingresar por el puerto ssh y solo se permite el ingreso al servidor VPN para que se comunique por medio de este puerto.

Niega a todos los usuarios que quieren tener acceso al cliente VPN por el puerto ssh.

iptables −A INPUT −p tcp −−dport 22 −j DROP

Acepta solo a la ip del servidor vpn por el puerto ssh.

iptables -I INPUT -s 192.168.1.14 -d 192.168.22.100 -p tcp --dport 22 -j ACCEPT

En el cliente se mostrara las reglas con el comando iptables –L –n como se muestra en la figura 34.

Figura 34. Ejemplo. Cerrar el puerto ssh. Y tener acceso para un solo usuario.

```
kkk22:~ # iptables -L -n
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  192.168.1.14         192.168.22.100      tcp dpt:22
DROP       tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:22

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

Para el servidor VPN se hace el mismo proceso, cambiando las IPs y cerrando los puertos que no se necesitan para establecer la conexión.

5. CONCLUSIONES

- Las redes privadas virtuales (VPNs) son una solución real, barata y segura para las comunicaciones de las empresas actuales para el caso de Arka S.A. no se requirió cambio en equipos de hardware ya que se implanto una solución VPN por software, aunque cada vez el mercado proporciona más equipos hardware y se desarrollan aplicaciones software para implementar esta tecnología y por ende administrarlas.

- Las empresas que tiene enlaces dedicados (alquilados) con tecnologías como FRAME RELAY están migrando sus redes de transporté de datos a tecnologías IP como las VPNs, ya que permitiéndole a las compañías reducir los costos de desplazamiento y ahorro en pagos del servicio. Además las ISPs están mejor parados que ninguna otra clase de empresa de telecomunicaciones para explotar este mercado, pues conocen IP desde hace ya varios años y tienen la infraestructura para, con una mínima inversión, proveer este servicio sin mayores problemas

- Con la tecnología de red actual no se pueden llevar acabo implementaciones futuras de tecnologías de información, debido a que el ancho de banda que maneja es muy reducido, y las posibilidades que existen para la caída del canal son bastante ya que además del proveedor actual del servicio dedicado (Frame Relay) necesita de un tercero para poder establecer la comunicación el cual es el proveedor de la ultima milla o ultimo kilómetro, esto puede generar riesgos de caídas del canal así como también retrasos al momento de restablecer el canal; diferente a las la implantación de la tecnología VPNs, Los riesgos de caída en las comunicaciones se disminuye en un 50 %, ya que interviene un solo proveedor en la comunicación por ende si existen problemas el usuario se comunica directamente con la ISP proporcionándole rapidez al momento de una reclamación.

- El nivel de seguridad de la tecnología se mantiene debido a que las VPNs y en este caso por software aplican en la comunicación la autenticación y la encriptación de los datos que viajan a través del túnel. Proporcionando nivel grande de seguridad utilizando estándares de encriptación de la información además que se tiene como mecanismo de seguridad a las maquinas origen y destino las reglas iptables las cuales actual como firewall en estas, lo cual permite mayor seguridad tanto en la transmisión de los datos como en las estaciones de trabajo.

BIBLIOGRAFÍA

ACADEMIA de Networking de Cisco Systems. 3 ed. Madrid: Cisco Systems, 2006. 944 p.

HATCH KOLESNIKOV, Brian Oleg, Redes Privadas Virtuales Con Linux. México: Pearson, 2003. 450 p.

FOROUZAN, Behrouz A. Transmisión de datos y redes de comunicaciones. 2 ed. Madrid: McGraw-Hill, 2002. 887 p.

MILLAS MARTÍNEZ, Coral, Redes virtuales privadas - seguridad en redes telemáticas [en línea]. Madrid: 2000. [Consultado 18 de Agosto, 2008]. Disponible en Internet:
http://asignaturas.diatel.upm.es/seguridad/trabajos/trabajos/vpn.pdf

Algoritmos simétricos [en línea]. Barcelona: Eurologic, 2007. [Consultado 2 de Septiembre, 2008]. Disponible en Internet:
http://www.eurologic.es/cifrado/simetric.htm

YONAN, James, OpenVPN COMO [en línea]. Madrid, 2002. [Consultado 25 de Agosto, 2008]. Disponible en Internet:
http://laurel.datsi.fi.upm.es/~rpons/openvpn_como

OLLER IVARS, Jordi. Conexiones VPN con PPTP bajo Linux [en línea]. Valencia, 2004. [Consultado 2 de Agosto, 2008]. Disponible en Internet:
http://beta.redes-linux.com/manuales/vpn/pptp.pdf

FORD, Merilee; LEW, H. Kim; SPANIER, Steve y STEVENSON, Tim. Tecnologías de interconectividad de redes. México: Prentice-Hall, 1998. 716 p

Universidad Anáhuac de Xalapa. Ingeniería en Tecnologías de la Información [en línea]. México, 1999. [Consultado 30 de Agosto, 2008]. Disponible en Internet:
http://www.angelfire.com/sc/itiuax/framerelay.html

Wikipedia: la enciclopedia libre [en línea]. Florida: Wikipedia Fundation, “Frame Relay, 2006. [Consultado 25 de Agosto, 2008]. Disponible en Internet:
http://es.wikipedia.org/wiki/Frame_Relay

STALLINGS, William. Comunicaciones y Redes de Computadores. 6 ed. Pearson Educación. 650 p.

ANEXOS

Anexo A. Tecnología FRAME RELAY implantada en Arka S.A.

La empresa ARKA S.A actualmente cuenta con una red de comunicaciones basada en la tecnología FRAME RELAY, en esta se implementa la conmutación de paquetes los cuales permite compartir dinámicamente el medio y por ende el ancho de banda disponible por lo que la empresa se beneficia con la transmisión sistematizada de los pedidos de domicilios efectuados al callcenter desde la planta a todos los diferentes puntos de venta punto de venta.

El proveedor de los canales dedicados FRAME RELAY es telefónica Telecom, el cual provee la red WAN para la interconexión de ARKA SA con sus respectivas sedes; el esquema general se observa en la siguiente grafica, la cual fue tomada de la documentación de la red de datos del departamento de sistemas:

La arquitectura de red WAN que maneja la empresa ARKA SA se puede apreciar de forma mas detallada en el siguiente grafico, donde se observa que el último tramo no pertenece al proveedor directo de la solución, ya que esta última milla pertenece a Emcali.

Figura 35. Conexión actual de Red Arka S.A con tecnología FRAME RELAY (Imagen tomada de la documentación del proveedor de la solución actual).

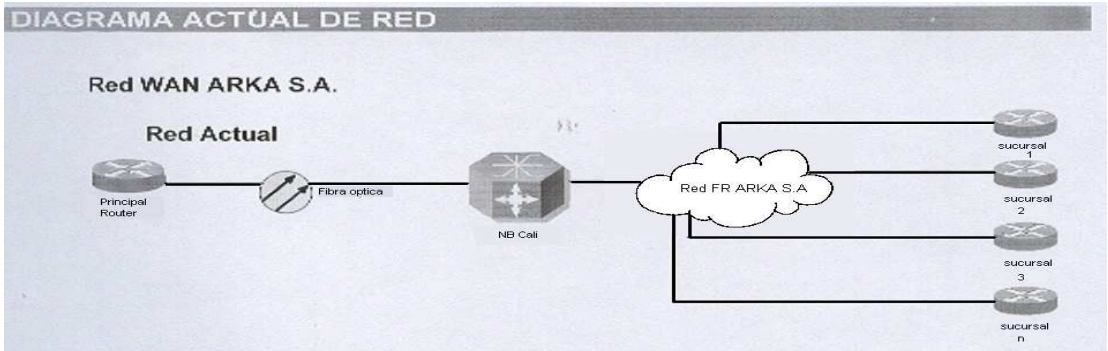
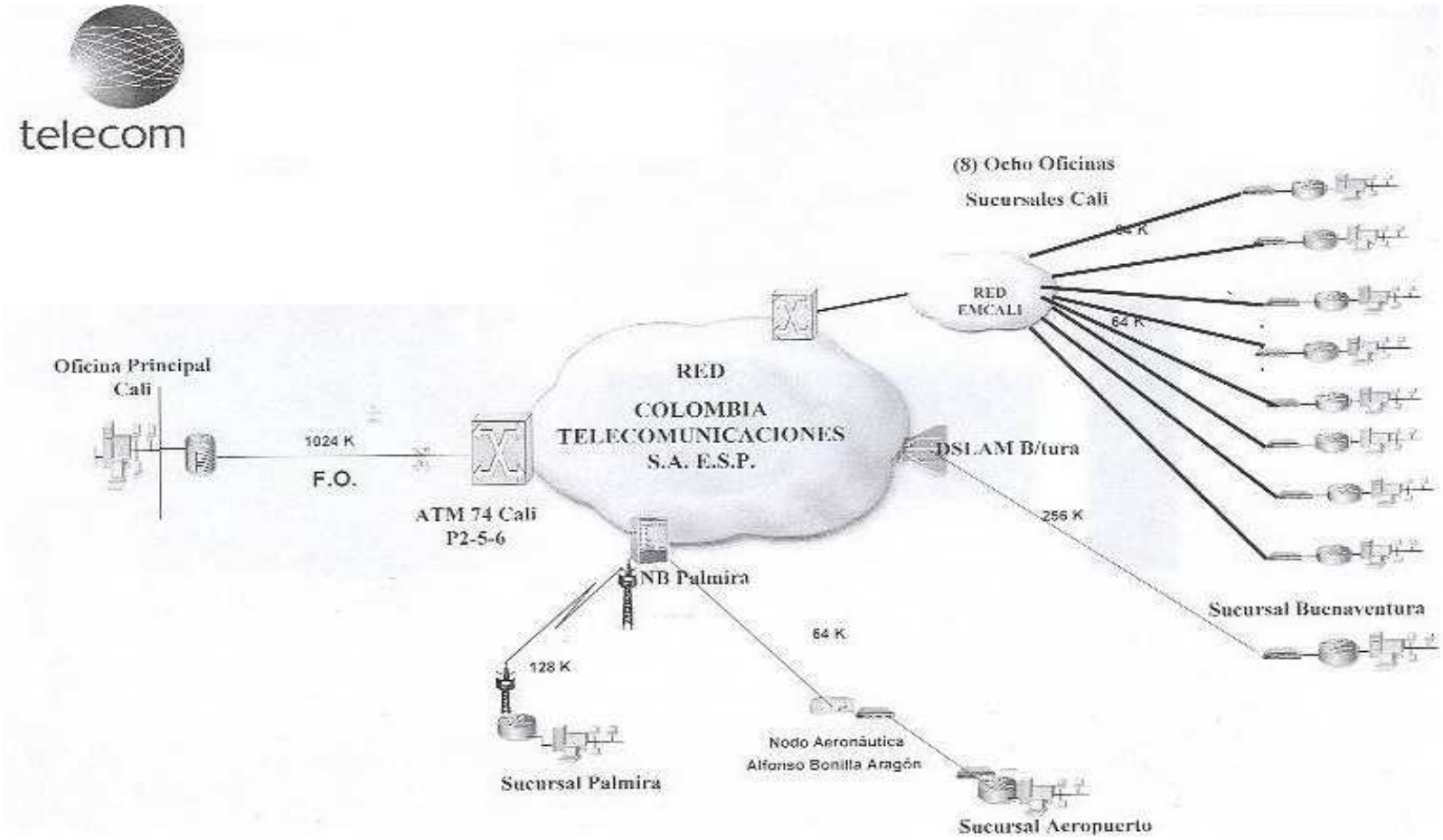


Figura. 2 Diagrama de res posterior a la migración a fibra óptica de la sede principal.

Figura 36. Diagrama general de Red Arka S.A (Imagen tomada de la documentación del proveedor de la solución actual).



Ahora bien, en la empresa se están generando unos costos muy elevados debido al excesivo uso de las líneas telefónicas, ya que para cada punto de venta hay de una o dos líneas telefónicas pertenecientes a un plan de minutos mínimo definido.

Por todo lo anterior vemos que la empresa ARKA SA busca la manera de cómo reducir todos estos costos en las comunicaciones con todas sus sedes, garantizando la conectividad, la autentificación, la encriptación y la seguridad toda la información.