UNIVERSIDAD CATÓLICA ANDRÉS BELLO
FACULTAD DE INGENIERÍA
ESCUELA DE INGENIERÍA DE TELECOMUNICACIONES

Implementar una plataforma de Interconexión Independiente del Esquema de Direccionamiento IP usado por los ISP en Venezuela

REALIZADO POR: Leonardo Leoni
José Daniel Rodríguez

PROFESOR GUÍA: Ing. Alexander Padilla

FECHA: Caracas, 8 de julio de 2008

UNIVERSIDAD CATÓLICA ANDRÉS BELLO
FACULTAD DE INGENIERÍA
ESCUELA DE INGENIERÍA DE TELECOMUNICACIONES

Implementar una plataforma de Interconexión Independiente del Esquema de Direccionamiento IP usado por los ISP en Venezuela

Este Jurado; una vez realizado el examen del presente trabajo ha evaluado su contenido con el resultado: Diez y nueve puntos (19/20)

J U R A D O E X A M I N A D O R

Firma:
Nombre: María Méndez

Firma:
Nombre: Carlos Guerrero

Firma:
Nombre: ALEXANDER PADILLA

REALIZADO POR: Leonardo Leoni
José Daniel Rodríguez

PROFESOR GUÍA: Ing. Alexander Padilla

FECHA: Caracas, 8 de julio de 2008

Agradecimientos

Nuestros agradecimientos van dirigidos, en primer lugar a la Universidad Católica Andrés Bello por brindarnos las herramientas científicas y humanistas para comenzar con buen pie nuestra vida profesional, inculcándonos una serie de valores morales y éticos que han contribuido a nuestra formación integral, para ser capaces de alcanzar logros propuestos con responsabilidad, respeto y honestidad como futuros ingenieros del país.

A la profesora Lourdes Ortiz, quien con su dedicación, paciencia y espíritu pedagógico se mostró siempre dispuesta a brindarnos su ayuda en todas las etapas del desarrollo de esta investigación.

A nuestros familiares y amigos, en especial a nuestros padres, quienes a través de su enseñanza, sacrificio y amor, nos han brindado su apoyo incondicional en todo momento a lo largo de nuestra carrera universitaria.

A nuestro tutor, el ingeniero Alexander Padilla y a nuestro revisor, el ingeniero Carlos Fuenmayor, por su aporte y colaboración a lo largo del desarrollo del Trabajo Especial de Grado.

A la empresa Altermedios Technologies C.A., y su personal técnico y administrativo, quienes nos han brindado su apoyo y dedicación, pues gracias a ellos tuvimos la oportunidad de comprender en un ambiente pragmático el complejo mundo de la conectividad y seguridad en redes.

Por último, y no menos importante, queremos agradecer a Francisco Flores y a Franlen Marcano por su disposición y contribución para poder culminar esta investigación de forma exitosa.

Implementar una Plataforma de Interconexión Independiente del Esquema de Direccionamiento IP usado por los ISP en Venezuela

Leoni Moreno, Leonardo Alfonso
leoleoni@gmail.com

Rodríguez Núñez, José Daniel
josedan@gmail.com

Resumen

Considerando la existencia del problema presente por causa del esquema de direccionamiento IP utilizado actualmente por los proveedores de servicio de Internet en Venezuela, conocido con el nombre de IPv4, el cual presenta una limitante en cuanto a la cantidad de direcciones públicas que puede manejar y al nivel de seguridad que este puede otorgar, se propuso un proyecto cuyos objetivos son estudiar el esquema de direccionamiento IP provisto por los principales proveedores del servicio de Internet en Venezuela, analizar el funcionamiento de los routers más utilizados actualmente en el mercado venezolano, realizar las pruebas para elegir los equipos más adecuados e implementar una plataforma de interconexión independiente al esquema de direccionamiento IP usado.

Para alcanzar los objetivos planteados, se utilizó una metodología que consta de un análisis de los diferentes protocolos usados en Internet, los cuales brindan un grado de seguridad apropiado. Posteriormente, se hace un análisis comparativo entre los principales ISP presentes en el territorio nacional, tomando en cuenta el ancho de banda, el esquema de direccionamiento IP y la compatibilidad con conexiones VPN que estos presentan. Seguidamente, se procede a la realización de las pruebas pertinentes involucrando los routers escogidos en la fase anterior e implementando

una plataforma independiente al esquema de direccionamiento IP ofrecido por los diferentes ISP utilizados durante el desarrollo del proyecto.

Como resultado de lo antes descrito se logró implementar esta plataforma de interconexión haciendo uso de un servidor central con una dirección IP fija y alcanzable desde cualquier localidad remota con acceso a Internet. De lo descrito se concluye que sin importar el esquema de direccionamiento IP que presenten los clientes al servidor siempre van a poder establecer una red privada virtual con otros clientes que se encuentren enviando sus datos a través de dicho servidor.

Palabras Claves: Internet, direccionamiento IP, seguridad, plataforma

Índice General

Agradecimientos ii

Resumen iii

Índice General v

Índice de Figuras vii

Índice de Tablas viii

Introducción ix

Capítulo I. Planteamiento del Proyecto 1

I.1. Planteamiento del Problema: 1
I.2. Objetivos: 1
I.2.1. Objetivo General: 1
I.2.2. Objetivos Específicos: 1
I.3. Justificación: 2
I.4. Limitaciones y alcances: 2
Capítulo II. Marco Teórico 3

II.1. VPN (Virtual Private Network): 3
II.2. Protocolos para establecer Redes VPN a través de túneles: 4
II.2.1. IPSEC (Internet Protocol Secure): 5
II.2.2. PPTP (Point to Point Tunneling Protocol): 8
II.2.3. L2TP (Layer 2 Tunneling Protocol): 9
II.3. Diferencias entre los principales ISP en Venezuela: 11
II.4. Estudio de los Routers más utilizados en el mercado venezolano: 14
Capítulo III. Metodología 19

III.1. Fases de la metodología. 19
Capítulo IV. Desarrollo 22

IV.1. Análisis. 22
IV.1.1. Estudio de protocolos de redes privadas virtuales (VPN). 22
IV.1.2. Estudio de los proveedores de servicio de Internet (ISP) 23
IV.1.3. Estudio de routers utilizados en el mercado venezolano. 23
IV.2. Pruebas de conexión 24
IV.2.1. Simulación de una VPN haciendo uso de un router cumpliendo la función del ISP 24
IV.2.2. Establecimiento de una conexión VPN a través de Internet 25
IV.3. Diseño de la plataforma 30
IV.3.1. Modelos elaborados para el diseño de la plataforma 31
IV.4. Implementación de la plataforma 32
Capítulo V. Resultados 33

V.1. Análisis 33

V.1.1. Selección del protocolo para el establecimiento de las VPN 33
V.1.2. Características de los ISP usados en Venezuela para el funcionamiento de las VPN 34
V.1.3. Tipos de routers con las especificaciones técnicas requeridas para el funcionamiento adecuado de la red privada virtual 34
V.2. Pruebas de Conexión 35
V.2.1. Simulación de una VPN haciendo uso de un router cumpliendo la función del ISP 35
V.2.1.1. Pruebas realizadas con equipos comerciales de bajo costo 35
V.2.1.2. Pruebas realizadas con equipos comerciales con un nivel de configuración más avanzado 36
V.2.2. Establecimiento de una conexión VPN a través de Internet 37
V.2.2.1. Pruebas realizadas con equipos comerciales con un nivel de configuración más avanzado 37
V.2.2.2. Pruebas realizadas con equipos comerciales con un nivel de configuración más avanzado conectados remotamente a un servidor con dirección IP fija 38
V.3. Selección de equipos y proveedores de servicio de Internet 38
V.3.1. Selección de equipos 39
V.3.2. Selección de los ISP 39
V.3.2.1. Proveedores seleccionados en relación a los equipos terminales 39
V.3.2.2. Proveedores seleccionados en relación al servidor utilizado en la plataforma de interconexión 40
V.4. Diseño de la plataforma 41
V.4.1. Modelos de implementación 41
V.5. Implementación de la plataforma 43
Capítulo VI. Conclusiones y Recomendaciones 45
Capítulo VII. Bibliografía 48
Lista de Acrónimos 50
Apéndices 52
Apéndice A. Configuración para establecimiento de una VPN con equipos de marca WatchGuard, modelo Firebox SOHO 6: 53

Índice de Figuras

Figura 1. Simulación de establecimiento de VPN 25
Figura 2. Establecimiento de la VPN con equipos WatchgGuard 26
Figura 3. Configuración de equipo Terminal 27
Figura 4. Parámetros de la VPN 28
Figura 5. Estadísticas del protocolo IPSEC 29
Figura 6. Modelo establecido con routers avanzados a través de Internet 31
Figura 7. Modelo establecido utilizando el servidor 32
Figura 8. Establecimiento del Tunel VPN con el protocolo IPSEC. 36
Figura 9. Expiración del túnel VPN 37
Figura 10. Plataforma de interconexión utilizando un servidor 38
Figura 11. Modelo de Plataforma de interconexión utilizando routers Watchguard 42
Figura 12. Modelo de Plataforma de interconexión utilizando routers Watchguard y el servidor 43
Figura 13. Tabla de rutas del servidor 44

Índice de Tablas

Tabla 1. Estructura de una cabecera del protocolo AH 6
Tabla 2. Estructura de una cabecera del protocolo ESP 7
Tabla 3. Diferencias entre los principales ISP en Venezuela 13
Tabla 4. Características de los routers de marca WatchGuard 15
Tabla 5. Características de los routers D-Link 16
Tabla 6. Características de los routers Linksys 17
Tabla 7. Características de los routers Netgear 18
Tabla8. Resumen de las fases de la metodología 21
Tabla 9. Modelo de equipos compatibles con la plataforma 39
Tabla 10. ISP compatibles con los equipos terminales 40
Tabla 11. ISP compatibles con el servidor de la plataforma 41

Introducción

A través de los tiempos, las redes de comunicación han formado parte de la humanidad. Éstas comienzan a desarrollarse desde tiempo primitivos, donde se utilizaban medios físicos para poder transmitir mensajes. Luego de años de avances tecnológicos se llega al desarrollo del teléfono; primera invención relevante y el primer paso para lo que conocemos hoy como telefonía a niveles de última generación.

Posteriormente, en Estados Unidos en 1969 se diseña una red experimental denominada ARPANET, la cual se vuelve operativa en el año 1975. Esta red adopta el conocido protocolo TCP/IP en el año 1983 y evoluciona a lo que se conoce como Internet. Aunque TCP/IP en su estructura aparenta ser un solo protocolo, realmente está dividido en dos, una parte que se encarga de la integridad y transporte de los datos (TCP) y otra que se encarga del direccionamiento en la red (IP), éste ultimo, obliga a que cada computador conectado a la red, posea un identificador único, el cual consiste en un número compuesto por 4 octetos de 8 bits denominado dirección IP.

En la actualidad, las organizaciones se ven obligadas a utilizar el servicio de Internet como medio de transporte de data corporativa. Para poder establecer este tipo de conexión son necesarios una serie de elementos de red que encripten y envíen la información, para evitar que cualquier otra persona con acceso a la red logre ver lo que está siendo enviado. Por esta razón, se necesita diseñar una plataforma que brinde seguridad en cualquier escenario de red, en el cual se encuentren viajando los datos. Los distintos escenario presentes en Venezuela son consecuencia directa del esquema de direccionamiento ofrecido por los ISP, los cuales otorgan direcciones dinámicas en su gran mayoría; aspecto negativo para el establecimiento de una conexión segura

entre dos localidades remotas, por causa de posibles caídas del enlace por cambios repentinos de dirección IP.

Es por esto, que se estudian los diferentes protocolos existentes, para así poder encontrar una solución eficiente a través del uso de las redes privadas virtuales. Luego se hace un análisis de los diferentes servicios ofrecidos por los proveedores del servicio de Internet en Venezuela, para después hacer un estudio de mercado sobre los diferentes equipos que pueden ser usados para establecer esta plataforma de interconexión.

El siguiente informe está estructurado en una serie de capítulos. En el primer capítulo se explica el planteamiento del proyecto, en el cual se menciona el problema a resolver, los objetivos, la justificación, alcance y limitaciones del mismo. El segundo capítulo contiene el marco teórico, donde se definen los conceptos necesarios para comprender el desarrollo de la investigación. Luego, en el capítulo III se explica la metodología y sus diferentes fases para llevar a cabo el proyecto.

El capítulo IV está compuesto por el desarrollo del proyecto, desde la investigación teórica de las redes privadas virtuales y sus protocolos, hasta la implementación de la plataforma de interconexión independiente del esquema de direccionamiento IP usado por los ISP en Venezuela. Seguidamente, en el capítulo V se explican los resultados obtenidos en las etapas del desarrollo.

Por último, en el capítulo VI se muestran las conclusiones y recomendaciones del proyecto estudiado, dando respuesta al problema planteado inicialmente, cumpliendo con los objetivos establecidos al principio de esta investigación.

Capítulo I. Planteamiento del Proyecto

En el siguiente capítulo se da a conocer el problema acerca del direccionamiento Ipv4 actualmente utilizado a nivel mundial, del cual surge la necesidad de buscar soluciones inmediatas que proporcionen una respuesta efectiva en relación a lo que se plantea en esta investigación. También están incluidos los objetivos necesarios para llevar a cabo este Trabajo Especial de Grado, la justificación, las limitaciones y el alcance del mismo.

I.1. Planteamiento del Problema:

Actualmente nos enfrentamos al grave problema que existe en el diseño de arquitectura de Internet, debido a que el direccionamiento IPv4 está cercano a agotarse y, por tanto, el crecimiento de Internet se pararía por no poder incorporar nuevos usuarios a la red.

En respuesta a este problema, es necesario plantear una solución inmediata que proporcione conectividad de forma segura, la cual permita a los usuarios permanecer conectados a la red con un nivel de confiabilidad más alto que el proporcionado por cualquier proveedor de servicio de Internet (ISP).

I.2. Objetivos:

I.2.1. Objetivo General

Implementar una plataforma de interconexión independiente del esquema de direccionamiento IP de acuerdo al menos tres (3) ISP diferentes ubicados en Venezuela.

I.2.2. Objetivos Específicos:

a) Estudiar el esquema de direccionamiento IP de los principales ISP en Venezuela.

b) Analizar el funcionamiento de los routers más utilizados en el mercado venezolano actualmente.

c) Realizar pruebas con redes VPN para establecer conexión entre dos puntos terminales sin importar el esquema de direccionamiento del ISP respectivo.

d) Diseñar una plataforma de interconexión entre dos localidades remotas, a través de cualquier tipo de direccionamiento IP.

e) Implementar una plataforma de interconexión entre dos localidades remotas, a través de cualquier tipo de direccionamiento IP.

I.3. Justificación:

La conectividad privada virtual permite a las sucursales y trabajadores remotos, transferir la información de forma privada y segura usando un medio público, tal como Internet.

Con la implementación de una plataforma de interconexión independiente de los proveedores del servicio de Internet, se podrán realizar conexiones de forma segura y permanente, brindando así, una alternativa rentable en tecnología para el intercambio de información entre distintas localidades a través de Internet.

I.4. Limitaciones y alcances:

Este trabajo no permitió la posibilidad de abarcar todos los tipos de equipos terminales, es decir, los routers existentes en el mercado venezolano, ya que por razones de tiempo y de costo no se pudieron cubrir todas las marcas y modelos por la gran cantidad de equipos que dicho mercado ofrecía.

Capítulo II. Marco Teórico

En el inicio de este marco teórico se definen algunos términos que serán necesarios dominar para comprender el contenido de esta investigación, y poder realizar el análisis de los resultados a los cuales se quiere llegar.

II.1. VPN (Virtual Private Network):

Según VPN Consortium (2006) en su página web localizada en la dirección "http://www.vpnc.org/vpn-technologies.html", una VPN se define como una red privada de voz, datos y video, la cual hace uso de una infraestructura de telecomunicaciones pública, ya que es capaz de mantener privacidad mediante el establecimiento de túneles, respetando ciertos procedimientos de seguridad.

Las VPN o redes privadas virtuales pueden ser comparadas con redes que usen líneas de transmisión privadas, a las cuales no se pueda acceder desde otros lugares que no se encuentren físicamente conectados a la misma, sin embargo, las VPN tienen como propósito principal el de proporcionar redes seguras generando costos inferiores, ya que éstas usan una infraestructura pública y compartida.

En el segmento de las VPN podemos encontrar tres tipos de redes, la primera es conocida con el nombre de "*Secure VPN*" o red privada virtual segura, la cual requiere que todo el tráfico que viaja por ella esté debidamente encriptado y autenticado, que todos los parámetros de seguridad seán aceptados por todos los terminales de la red y que nadie encontrado fuera de dicha red pueda acceder y cambiar dichos parámetros. En este tipo de VPN pueden ser usados tres tipos de protocolos, entre los cuales tenemos IPsec con cifrado tanto en modo túnel como en modo de transporte, IPsec encapsulado en L2TP como se explica, según la IETF (*Internet Engineering Task Force*) en su página web localizada en la dirección "http://www.ietf.org/rfc.html", en el RFC 3193, y el SSL 3.0 o TLS con cifrado como

se describe en el RFC 2246.

La segunda red "Trusted VPN" o red privada virtual confiable, es un tipo de red que sólo puede ser establecida mediante un servicio provisto por un ISP, permitiendo al cliente crear su propio esquema de direccionamiento privado, brindando la posibilidad de que éste establezca sus propias rutas. Para el correcto funcionamiento de este tipo de red, es necesario que nadie, a excepción del proveedor de servicio tenga acceso a realizar cambios en las rutas establecidas previamente, ni cambiar, insertar o borrar datos correspondientes al flujo de dicha VPN, y que el enrutamiento y direccionamiento utilizado sea configurado antes de realizar el establecimiento de la VPN. Para poder implementar este tipo de redes es necesario trabajar con tecnologías como los circuitos ATM, Frame Relay y transporte de L2F sobre MPLS.

Como tercer tipo encontramos las redes híbridas que como su nombre lo indica comparte parámetros de las dos que se explicaron previamente, la cual combina los aspectos positivos o fortalezas, tanto de las "Trusted" como de las "Secure", para optimizar el funcionamiento de las VPN en general.

Se puede decir que las VPN son usadas en escenarios donde es necesario manejar información que no puede ser vista por terceros, estableciendo túneles encriptados para evitar que en la intercepción de dichos paquetes, éstos puedan ser descifrados causando una brecha o fuga de información indeseada.

II.2. Protocolos para establecer Redes VPN a través de túneles:

Entre los protocolos más usados para el establecimiento de redes VPN se encuentran IPSEC, PPTP y L2TP.

II.2.1. IPSEC (Internet Protocol Secure):

Según la IETF (Internet Engineering Task Force) en su RFC 2402 publicado en noviembre del año 1998 y ubicado en la página web "http://www.ietf.org/rfc/rfc2402.txt", IPSec es la unión de un conjunto de protocolo que proporcionan servicios de seguridad a las conexiones que son establecidas a través de redes privadas virtuales, a nivel de capa tres (3) del modelo OSI. Este protocolo permite cambiar en su algoritmo una serie de parámetros de conexión, dentro de los cuales tenemos: el tipo de protocolo de seguridad que será utilizado, el método de autenticación y la clave de cifrado requerida para lograr establecer la conexión adecuadamente.

El funcionamiento de IPSec usa dos tipo de protocolos para proporcionar seguridad en el tráfico, el *Authentication Header* (AH) o Cabecera de autenticación, y *el Encapsulating Security Payload* (ESP) o encapsulado de seguridad de carga útil.

De acuerdo al IETF (Internet Engineering Task Force) en su RFC 2402 publicado en noviembre del año 1998 y ubicado en la página web "http://www.ietf.org/rfc/rfc2402.txt", el protocolo AH está dirigido a garantizar integridad sin conexión y autenticación de los datos de origen de los datagramas IP. Para ello, calcula un *Hash Message Authentication Code* (HMAC) a través de algún algoritmo hash operando sobre una clave secreta, el contenido del paquete IP y las partes inmutables del datagrama. Este proceso restringe la posibilidad de emplear NAT, que puede ser implementada con NAT transversal. Por otro lado, AH puede proteger opcionalmente contra ataques de repetición utilizando la técnica de ventana deslizante y descartando paquetes viejos. AH protege la carga útil IP y todos los campos de la cabecera de un datagrama IP excepto los campos mutantes, es decir, aquellos que pueden ser alterados en el tránsito.

A continuación se muestra la estructura de una cabecera AH con sus respectivos tamaños y como está distribuida en campos:

0 - 7 bit	8 - 15 bit	16 - 23 bit	24 - 31 bit
Next header	Payload length	RESERVED	
Security parameters index (SPI)			
Sequence number			
Hash Message Authentication Code (variable)			

Tabla 1. *Estructura de una cabecera del protocolo AH*

Fuente: IETF (Internet Engineering Task Force) en su RFC 2402 publicado en noviembre del año 1998 y ubicado en la página web "http://www.ietf.org/rfc/rfc2402.txt

Leyenda de los campos de la cabecera:

Next header

Identifica el protocolo de los datos transferidos.

Payload length

Tamaño del paquete AH.

RESERVED

Reservado para uso futuro (hasta entonces todo ceros).

Security parameters index (SPI)

Indica los parámetros de seguridad que, en combinación con la dirección IP, identifican la asociación de seguridad implementada con este paquete.

Sequence number

Un número siempre creciente, utilizado para evitar ataques de repetición.

HMAC

Contiene el valor de verificación de integridad (ICV) necesario para autenticar el paquete; puede contener relleno.

Según la IETF (Internet Engineering Task Force) en su RFC 2406 publicado en noviembre del año 1998 y ubicado en la página web "http://www.ietf.org/rfc/rfc2406.txt", el encapsulado de seguridad de carga útil (ESP) proporciona autenticidad de origen, integridad y protección de confidencialidad de un paquete. ESP también soporta configuraciones de sólo cifrado y sólo autenticación, pero utilizar cifrado sin autenticación está altamente desaconsejado porque es inseguro. Al contrario que con AH, la cabecera del paquete IP no está protegida por ESP (aunque en ESP en modo túnel, la protección es proporcionada a todo el paquete IP interno, incluyendo la cabecera interna; la cabecera externa permanece sin proteger). ESP opera directamente sobre IP.

A continuación se muestra de un paquete ESP con sus respectivos tamaños y como está distribuida en campos:

<table>
<tr><td>0 - 7 bit</td><td>8 - 15 bit</td><td>16 - 23 bit</td><td>24 - 31 bit</td></tr>
<tr><td colspan="4">Security parameters index (SPI)</td></tr>
<tr><td colspan="4">Sequence number</td></tr>
<tr><td colspan="4">Payload data (variable)</td></tr>
<tr><td></td><td colspan="3">Padding (0-255 bytes)</td></tr>
<tr><td colspan="2"></td><td>Pad Length</td><td>Next Header</td></tr>
<tr><td colspan="4">Authentication Data (variable)</td></tr>
</table>

Tabla 2. *Estructura de una cabecera del protocolo ESP*

Fuente: IETF (Internet Engineering Task Force) en su RFC 2406 publicado en noviembre del año 1998 y ubicado en la página web http://www.ietf.org/rfc/rfc2406.txt

Leyenda de los campos de la cabecera:

Security parameters index (SPI)

Identifica los parámetros de seguridad en combinación con la dirección IP.

Sequence number

Un número siempre creciente, utilizado para evitar ataques de repetición.

Payload data

Los datos a transferir.

Padding

Usado por algunos algoritmos criptográficos para rellenar por completo los bloques.

Pad length

Tamaño del relleno en bytes.

Next header

Identifica el protocolo de los datos transferidos.

Authentication data

Contiene los datos utilizados para autenticar el paquete.

Tanto AH como ESP son protocolos de control de acceso, los cuales están basados en la distribución de claves criptográficas y en la administración de flujos de tráfico para ofrecer un alto grado de seguridad a la información que se transmite por una infraestructura pública de la cual no tenemos control alguno, como es el caso de Internet. Es importante saber que estos protocolos pueden ser combinados para ofrecer un mayor nivel de seguridad a la conexión.

II.2.2. PPTP (Point to Point Tunneling Protocol):

Según la IETF (Internet Engineering Task Force) en su RFC 2637 publicado en noviembre del año 1999 y ubicado en la página web "http://www.ietf.org/rfc/rfc2637.txt", el protocolo PPTP se usa para establecer túneles de extremo a extremo a través de redes IP. Este protocolo no presenta

diferencia alguna con el protocolo PPP, sin embargo tiene un mecanismo de transporte distinto, el cual proporciona un encapsulado adicional para ofrecer mayor seguridad a las transmisiones punto a punto de la nube.

El protocolo PPTP presenta una arquitectura de cliente – servidor, la cual se encuentra presente en servidores que se utilizan en la actualidad.

Este protocolo, lo que hace es encapsular los paquetes del protocolo punto a punto PPP (Point to Point Protocol) que a su vez; ya vienen encriptados en un paso previo, para poder enviarlos a través de la red. El proceso de encriptación es gestionado por PPP y luego es recibido por PPTP, este último utiliza una conexión TCP llamada conexión de control para crear el túnel, y una versión modificada de la Encapsulación de Enrutamiento Genérico (GRE, *Generic Routing encapsulation*) para enviar los datos en formato de datagramas IP. El proceso de autenticación de PPTP utiliza los mismos métodos que usa PPP al momento de establecer una conexión, dentro de lo cuales encontramos el protocolo PAP (*Password Authenticaction Protocol*) y el protocolo CHAP (*Challenge-Handshake Authentication Protocol*). El método de encriptación que usa PPTP es el *Microsoft Point to Point Encryption*, MPPE, y solo es posible utilizarlo cuando se emplea CHAP (o MS-CHAP en los NT) como medio de autenticación. MPPE trabaja con claves de encriptación de 40 o 128 bits. Cliente y servidor deben emplear la misma codificación, si un servidor requiere de más seguridad de la que soporta el cliente, entonces el servidor rechaza la conexión.

II.2.3. L2TP (Layer 2 Tunneling Protocol):

Según la IETF (Internet Engineering Task Force) en su RFC 2661 publicado en noviembre del año 1999 y ubicado en la página wel "http://www.ietf.org/rfc/rfc2661.txt", el protocolo L2TP fue diseñado para mejorar sustituir los protocolos PPTP y L2F. L2TP utiliza PPP para proporcionar acces

telefónico que puede ser dirigido a través de un túnel por Internet hasta un punto determinado. L2TP define su propio protocolo de establecimiento de túneles, basado en L2F. El transporte de L2TP está definido para una gran variedad de tipos de paquete, incluyendo X.25, Frame Relay y ATM.

Al utilizar PPP para el establecimiento telefónico de enlaces, L2TP incluye los mecanismos de autenticación de PPP, PAP y CHAP.

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. Por ejemplo:

- Sólo se realiza la operación de autenticación entre los puntos finales del túnel. Esto puede dar lugar a suplantaciones de identidad en algún punto interior al túnel.
- Sin comprobación de la integridad de cada paquete, sería posible realizar un ataque de denegación del servicio por medio de mensajes falsos de control que den por terminado el túnel L2TP o la conexión PPP subyacente.
- L2TP no cifra en principio el tráfico de datos de usuario, lo cual puede dar problemas cuando sea importante mantener la confidencialidad de los datos.
- A pesar de que la información contenida en los paquetes PPP puede ser cifrada, este protocolo no dispone de mecanismos para generación automática de claves, o refrescamiento 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.

A causa de estos inconvenientes, el grupo del IETF que trabaja en el desarrollo de PPP consideró la forma de solventarlos. Ante la opción de crear un nuevo conjunto de protocolos para L2TP, del mismo estilo de los que se están realizando para IPSec, y dado la duplicación del trabajo respecto al propio grupo de

desarrollo de IPSec que supondría, se tomó la decisión de utilizar los propios protocolos IPSec para proteger los datos que viajan por un túnel L2TP.

L2TP es en realidad una variación de un protocolo de encapsulamiento IP. Un túnel L2TP se crea encapsulando una trama L2TP en un paquete UDP, el cual es encapsulado a su vez en un paquete IP, cuyas direcciones de origen y destino definen los extremos del túnel. Siendo el protocolo de encapsulamiento más externo IP, los protocolos IPSec pueden ser utilizados sobre este paquete, protegiendo así la información que se transporta por el túnel.

II.3. Diferencias entre los principales ISP en Venezuela:

Las principales diferencias entre los proveedores de servicios de Internet a nivel de conexiones, básicamente radican en el tipo de tecnología utilizado por éstos para ofrecer a sus clientes. Entre otros factores determinantes están el precio de los servicios, ubicación / alcance, modalidades de contratación y/o conexión (ancho de banda), esquema de direccionamiento IP, etc.

De acuerdo a la documentación provista por la empresa Altermedios Technologies C.A., entre los principales ISP existentes en Venezuela, se puede tildar a CANTV como uno de los gigantes en telecomunicaciones del país, ya que no sólo cubre el sector de telefonía en sus muy diversas áreas, sino que también cuenta con la mayoría de los usuarios que utilizan el servicio de Internet. La industria de la televisión por suscripción también ofrece diferentes soluciones de acceso a Internet utilizando la tecnología de fibra óptica, entre las cuales se encuentran Intercable (llamado ahora Inter), Supercable y Net-Uno. Aunque el mercado de Telefónica-Movistar está orientado en su mayoría a telefonía móvil, también ofrece su opción de banda ancha utilizando la tecnología WLL (Wireless Local Loop) que permite la transmisión y recepción por canales separados utilizando el espectro radioeléctrico como medio en frecuencias que oscilan entre los 3,4 GHz y 3,6 GHz. Génesis

Telecom se perfila como uno de los ISP con mayor desempeño y estabilidad en cuanto a conexión se refiere, pero una de sus limitantes es que sólo provee servicios en el área de Caracas, y sólo a clientes empresariales. Por último, tenemos a MOVILMAX, el cual aplica la tecnología de Wimax que utiliza conexiones inalámbricas en un área determinada.

En la tabla 1 se muestran las principales características de los ISP más importantes en Venezuela, entre las cuales se encuentran el tipo de tecnología que ofrecen, los anchos de banda que manejan, el esquema de direccionamiento IP que usan, si permiten establecer redes VPN, y de hacerlo, con cuál protocolo.

Estudio de los ISP en Venezuela				VPN		
ISP	**Tecnología**	**Anchos de Banda**	**Esquema de direcciones**	**IPSec**	**PPTP**	**L2TP**
CANTV	ADSL	512-2048 Kbps	Públicas Certificadas Dinámicas(DHCP)	Si	Si	Si
	Frame Relay	64-2 Mb	Publicas Estáticas	Si	Si	Si
	Banda Ancha Móvil	Hasta 1536 Kbps	Públicas Certificadas Dinámicas(DHCP)	Si	Si	
Telefónica Movistar	WLL	Hasta 1024 Kbps	Públicas Dinámicas	De acuerdo al plan		
Génesis Telecom	LMDS y WLL	64-2048 Kbps	Públicas Estáticas	Si	Si	Si
Intercable	Fibra Óptica	256-4096 Kbps	Públicas Dinámicas	De acuerdo al plan		
		256-2048 Kbps	Privadas Estáticas			
Net-Uno	Cable de fibra óptica	256-1024 Kbps	Públicas Dinámicas	De acuerdo al plan		
Supercable	Cable de fibra óptica	128-384Kbps	Públicas Certificadas Dinámicas(DHCP)	De acuerdo al plan		
MOVILMAX	Wimax	1-4 Mb	Públicas Estáticas	De acuerdo al plan		

Tabla 3. *Diferencias entre los principales ISP en Venezuela*

Fuente: Documentación la empresa.

II.4. Estudio de los Routers más utilizados en el mercado venezolano:

Para analizar los distintos tipos de routers en el mercado nacional, es necesario buscar equipos que cuenten con características específicas tales como: NAT Routing, DHCP Server, DHCP client, DHCP relay, DNS Proxy, Dynamic DNS, VPN Authentication, VPN Encryption, IPSec Server, IPSec client, IPSec passthrough, para poder llevar a cabo las pruebas de interconexión. Esta búsqueda se hace mediante páginas Web de venta de artículos electrónicos y de computación, donde las marcas que más se repitan son las catalogadas como las más utilizadas a nivel nacional.

A continuación, según Speedguide en su catálogo de equipos actualizado constantemente y ubicado en la en la World Wide Web: "http://www.speedguide.net/broadband.php", en las tablas 2, 3, 4 y 5 se muestran los routers que se consideran más utilizados en el mercado venezolano, y que cuentan con las características necesarias para realizar las pruebas y poder establecer una red VPN entre dos puntos terminales utilizando una plataforma de interconexión:

Marca	WatchGuard Firebox Edge e-Series			Firebox SOHO
Modelo	**FB X55e**	**FB X20e**	**FB X10e**	**SOHO 6**
Router				
NAT Routing	x	x	x	x
DHCP server	x	x	x	x
DHCP client	x	x	x	x
DHCP relay	x	x	x	x
DNS proxy	x	x	x	x
Dynamic DNS	x	x	x	x
DSL				
PPPoE	x	x	x	x
VPN				
VPN Authentication	MD5, SHA1, IKE	MD5, SHA1, IKE	MD5, SHA1, IKE	MD5, SHA1, IKE
VPN Encryption	AES, DES, 3DES	AES, DES, 3DES	AES, DES, 3DES	AES, DES, 3DES
Concurrent Sessions	10000	8000	6000	6001
IPSec				
IPSec server	x	x	x	x
IPSec client	x	x	x	x
IPSec passthrough	x	x	x	x
IPSec simultaneous tunnel	25	15	5	6
L2TP				
L2TP server				
L2TP client				
L2TP passthrough				
PPTP				
PPTP client				
PPTP server				
PPTP passthrough	x	x	x	x

Tabla 4. *Características de los routers de marca WatchGuard*

Fuente: *Watchguard ubicado en la en la World Wide Web: http://www.watchguard.com/*

Marca	D-Link	D-Link
Modelo	DI-524	DI-824VUP
Router		
NAT Routing	x	x
DHCP server	x	x
DHCP client	x	x
DHCP relay		
DNS proxy		
Dynamic DNS		
DSL		
PPPoE		x
VPN		
VPN Authentication		MD5, SHA1, IKE
VPN Encryption		DES, 3DES, IPSEC ESP
Concurrent Sessions		
Mobile User VPN tunnels		
IPSec		
IPSec server		x
IPSec client		x
IPSec passthrough	x	x
IPSec simultaneous tunnel		40
L2TP		
L2TP server		x
L2TP client		x
L2TP passthrough	x	x
PPTP		
PPTP client		
PPTP server		x
PPTP passthrough	x	x
PPPT simultaneous tunnels		

Tabla 5. *Características de los routers D-Link*

Fuente: *Speedguide en su catálogo de equipos actualizado constantemente y ubicado en la en la World Wide Web: http://www.speedguide.net/broadband.php*

Marca	**Linksys**					
Modelo	**BEFVP41**	**RV0041**	**WAG54G**	**WRT54G**	**WRT54GL**	**WRT54GS**
Router						
NAT Routing	x	x		x	x	x
DHCP server	x	x	x	x	x	x
DHCP client	x	x	x	x	x	x
DHCP relay	x	x	x	x	x	x
DNS proxy		x	x	x	x	x
Dynamic DNS		x	x	x	x	x
DSL						
PPPoE	x	x	x	x	x	x
VPN						
VPN Authentication	MD5, SHA1, IKE	MD5, SHA1, IKE				
VPN Encryption	DES, 3DES	DES, 3DES				
Concurrent Sessions						
Mobile User VPN tunnels						
IPSec						
IPSec server	x		x	x	x	
IPSec client	x	x	x	x	x	x
IPSec passthrough	x	x		x	x	x
IPSec simultaneous tunnel	50		5			5
L2TP						
L2TP server						
L2TP client						
L2TP passthrough		x	x	x	x	x
PPTP						
PPTP client				x	x	
PPTP server				x	x	
PPTP passthrough		x	x	x	x	x
PPPT simultaneous tunnels						

Tabla 6. *Características de los routers Linksys*

Fuente: Speedguide en su catálogo de equipos actualizado constantemente y ubicado en la en la World Wide Web: http://www.speedguide.net/broadband.php

Marca	Netgear			
Modelo	WGT-624	DGFV338	FVS318	FWG114P
Router				
NAT Routing	x	x	x	x
DHCP server	x	x	x	x
DHCP client	x	x	x	x
DHCP relay	x	x	x	x
DNS proxy	x	x	x	x
Dynamic DNS	x	x	x	x
DSL				
PPPoE	x	x	x	x
VPN				
VPN Authentication		MD5, SHA1, IKE	MD5, SHA1	
VPN Encryption		DES, 3DES, AES	DES, 3DES, AES	
Concurrent Sessions				
IPSec				
IPSec server		x	x	x
IPSec client		x	x	x
IPSec passthrough	x	x	x	x
IPSec simultaneous tunnel		50	8	2
L2TP				
L2TP server				
L2TP client				x
L2TP passthrough	x	x		
PPTP				
PPTP client			x	
PPTP server			x	
PPTP passthrough	x	x		x
PPPT simultaneous tunnels				

Tabla 7. *Características de los routers Netgear*

Fuente: Speedguide en su catálogo de equipos actualizado constantemente y ubicado en la en la World Wide Web: http://www.speedguide.net/broadband.php

Capítulo III. Metodología

Para llevar a cabo esta investigación se plantearon una serie de objetivos, de los cuales surge la necesidad de desarrollar un modelo estratégico para lograr la implementación de un sistema basado en las fases, alcances y limitaciones del proyecto. Estas estrategias se dividen en varias etapas para poder cumplir con los objetivos planteados y así obtener los resultados de forma satisfactoria.

III.1. Fases de la metodología.

- Análisis: en esta fase se recopiló la información referente a las redes privadas virtuales y los protocolos de seguridad utilizados para el establecimiento de las mismas. También se realizó un estudio de los principales proveedores de servicio de Internet en el país, tomando en cuenta las características más importantes, dentro de las cuales encontramos las siguientes: tecnología de acceso utilizada, rangos de ancho de banda, esquema de direccionamiento IP y si ofrecen servicios VPN (redes privadas virtuales). Por último se efectuó una comparación entre las principales marcas de routers utilizadas en el mercado venezolano, de los cuales se evaluaron las características necesarias para poder realizar las pruebas referentes a esta investigación.

- Pruebas de conexión: una vez efectuado el análisis inicial de esta investigación, se procedió a realizar todas las pruebas necesarias para examinar la conectividad de los equipos, tomando en cuenta el esquema de direccionamiento IP utilizado por el ISP, así como otros factores externos los cuales pudieran afectar de alguna manera dicha conectividad.

- Selección de equipos y proveedores de servicio de Internet: una vez realizadas las pruebas de conexión, se escogieron los equipos que cumplieran con todas las características requeridas para el establecimiento de la plataforma de

interconexión, así como las condiciones necesarias con respecto al direccionamiento IP para garantizar una conexión segura y continua.

- Diseño de la plataforma: luego de seleccionar los equipos y los proveedores de servicio adecuados, se procedió a realizar un diseño que nos permitiera crear un mecanismo para implementar una plataforma de interconexión que fuera independiente al esquema de direccionamiento IP provisto por los ISP a los clientes asociados a la empresa.

- Implementación de la plataforma: Finalmente, se implementó el mecanismo diseñado en la fase anterior para conectar dos localidades remotas a través de una VPN confiable y continua.

En la siguiente tabla se muestra gráficamente un resumen de la metodología empleada en este proyecto y su relación con el capítulo de desarrollo:

	Fases de la metodología				
	Análisis	**Pruebas de conexión**	**Selección de equipos y proveedores de Internet**	**Diseño de la plataforma**	**Implementación de la plataforma**
Desarrollo	Estudio de protocolos de una VPN Estudio de los ISP Estudio de los routers en el mercado venezolano	Simulación de una VPN haciendo uso de un router cumpliendo la función del ISP Establecimiento de una conexión VPN a través de Internet	Selección de equipos Selección de ISP	Modelos elaborados para el diseño de la plataforma	Implementación
Resultados	Selección del protocolo para el establecimiento de las VPN Características de los ISP usados en Venezuela para el funcionamiento de las VPN Tipos de routers con las especificaciones técnicas requeridas para el funcionamiento adecuado de la red privada virtual	Simulación de una VPN haciendo uso de un router cumpliendo la función del ISP Pruebas realizadas con equipos comerciales de bajo costo Pruebas realizadas con equipos comerciales con un nivel de configuración más avanzado Establecimiento de una conexión VPN a través de Internet	Selección de equipos Selección de los ISP Proveedores seleccionados en relación a los equipos terminales Proveedores seleccionados en relación al servidor utilizado en la plataforma de interconexión	Modelos de implementación	Implementación

***Tabla8**. Resumen de las fases de la metodología*

Fuente: Elaboración propia

Capítulo IV. Desarrollo

En la actualidad, las empresas tienen la necesidad de interconectar sus distintas localidades, para de esta forma manejar toda la información en un sólo sistema que brinde una mayor seguridad tanto a las empresas como a los clientes. Para esto es necesario diseñar una plataforma que permita el acceso y la transmisión de datos de forma segura y continua. A continuación se muestran las diferentes etapas del desarrollo.

IV.1. Análisis.

A continuación se muestra el estudio de los protocolos utilizados en el establecimiento de redes VPN, el análisis de los ISP y de los routers utilizados en el mercado venezolano, con el soporte obtenido del marco teórico previamente elaborado.

IV.1.1. Estudio de protocolos de redes privadas virtuales (VPN).

Al inicio de la investigación se hizo un estudio sobre las redes privadas virtuales (VPN) y los diferentes protocolos utilizados para establecer conexiones de forma segura a través de estas redes, de los cuales se analizaron sus diferentes características y parámetros de conexión.

Durante el desarrollo de esta fase, se realizaron búsquedas en las páginas web donde se encontraba la explicación detallada acerca del funcionamiento de los distintos protocolos utilizados que se relacionara con el establecimiento de redes privadas virtuales.

Otros documentos que fueron consultados durante la investigación de los protocolos de interconexión a través de túneles VPN, fueron los RFC 2401 en el cual

se habla de la arquitectura de seguridad utilizada en el protocolo IP y el RFC 2246 donde se explica cómo se implementa la seguridad en la capa de transporte del modelo OSI

Una vez adquirida esta recopilación de información, se hizo un resumen tomando en cuenta los aspectos que influyeran en el desarrollo de esta investigación.

IV.1.2. Estudio de los proveedores de servicio de Internet (ISP)

Luego de finalizar el estudio de los protocolos utilizados en el establecimiento de redes privadas virtuales, se procedió a analizar las diferencias entre los principales proveedores del servicio de Internet (ISP) y sus principales características. En principio se consultaron las páginas Web de cada proveedor, en las cuales se buscaban las principales características tales como la tecnología utilizada, tipos de servicios ofrecidos, esquema de direccionamiento IP, tipo de conexión, ancho de banda, entre otros. La información encontrada en estas páginas Web no fue suficiente, ya que había características específicas que no eran posibles ubicar por este medio, debido al enfoque comercial que se le daba a los servicios ofrecidos por los distintos ISP. Por tanto, se recurrió a documentación interna de la empresa para complementar la información obtenida a través de Internet.

IV.1.3. Estudio de routers utilizados en el mercado venezolano.

En la siguiente etapa de la investigación, se realizó un estudio de los routers más utilizados actualmente en el mercado venezolano por las pequeñas y medianas empresas. En principio se encontraron las distintas marcas existentes, a través de buscadores de Internet y páginas Web de venta de artículos electrónicos y de computación, de donde se seleccionaron las marcas con mayor demanda a nivel nacional, tales como Linksys, D-link y Netgear. Posteriormente, se hizo una clasificación de los distintos modelos ofrecidos por estas marcas, en base a sus

especificaciones técnicas y a los protocolos de establecimiento de túneles VPN que estos manejaban.

IV.2. Pruebas de conexión

Después de culminar la fase anterior, se efectuaron las distintas pruebas de interconexión, para evaluar la factibilidad del establecimiento de una plataforma de interconexión que fuera independiente al esquema de direccionamiento IP utilizado por los ISP, los cuales fueron investigados anteriormente.

IV.2.1. Simulación de una VPN haciendo uso de un router cumpliendo la función del ISP

Inicialmente, se realizó la simulación para establecer una VPN dentro de un escenario en el cual se utilizaron dos routers de uso comercial y de bajo costo como equipos terminales, un equipo de marca D-Link, modelo DI-524, en un extremo y un equipo de marca Netgear, modelo WGT-624, en el otro. Ambos equipos fueron administrados directamente a través del puerto ethernet, ingresando a sus parámetros de configuración a través de la dirección IP 192.168.0.1:80, para modificarlos de la forma más adecuada para intentar realizar la conexión VPN. Estos equipos se encontraban conectados a través de un equipo de marca Watchguard, modelo SOHO 6, el cual hacía la función de un ISP con un esquema de direccionamiento DHCP, otorgando direcciones IP dinámicas y alcanzables a ambos equipos terminales.

El tercer equipo de marca Watchguard fue configurado con un esquema de direccionamiento de DCHP haciendo el papel del ISP, ingresando a su configuración a través de la dirección IP 192.168.1.111:80 para así configurar sus interfaces de tal forma que asignara direcciones IP dinámicas a los otros dos equipos que se encontraban conectados a él. Asimismo, se configuraron las direcciones IP de ambas

máquinas, de tal forma que pertenecieran a la misma familia, con una misma máscara subred, para que fueran alcanzables de un punto a otro como en una red privada.

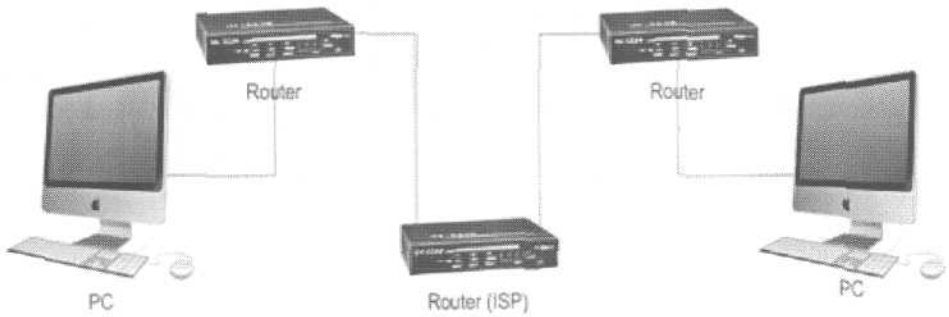

Figura 1. *Simulación de establecimiento de VPN*

Fuente: Elaboración propia

IV.2.2. Establecimiento de una conexión VPN a través de Internet

Luego de culminadas las pruebas simuladas, se realizaron las pruebas a nivel remoto, utilizando dos puntos de red en distintas localidades, siguiendo el mismo esquema usado en las pruebas simuladas.

Se realizaron las pruebas con equipos de marca *Watchguard* modelo SOHO 6, los cuales integran la función de router y firewall en un mismo *Hardware*. De esta forma, se conectaron tales equipos a dos puntos remotos de acceso a Internet, utilizando un esquema de direccionamiento DHCP provisto por el ISP CANTV para el establecimiento de la VPN a través de la nube, como se muestra en la siguiente figura:

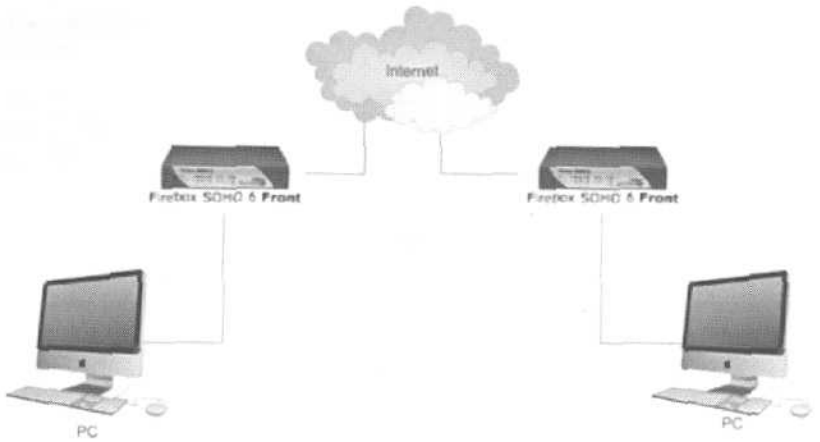

Figura 2. *Establecimiento de la VPN con equipos WatchgGuard*

Fuente: Elaboración propia

Luego se realizó la configuración de la VPN donde se administraron los equipos de acuerdo al protocolo IPSec, dividido en 2 fases. En la fase 1 se ingresaron los parámetros en ambos equipos. Entre los parámetros que fueron configurados estaban las direcciones IP de origen y destino para el establecimiento del túnel VPN (*Local ID y Remote ID*) las cuales habían sido asignadas previamente por el ISP (en este caso CANTV).

En la fase 2 se colocan las familias de las redes locales y remotas, es decir, la familia de la dirección IP que asigna el SOHO (la que tiene el computador). Todos los parámetros deben coincidir en ambos puntos terminales (algoritmo de autenticación, algoritmo de encriptación, etc.) excepto las direcciones IP, donde si en un equipo se coloca xxx.xxx.xxx.xx1 como remota, en la otra se coloca dicha dirección como local.

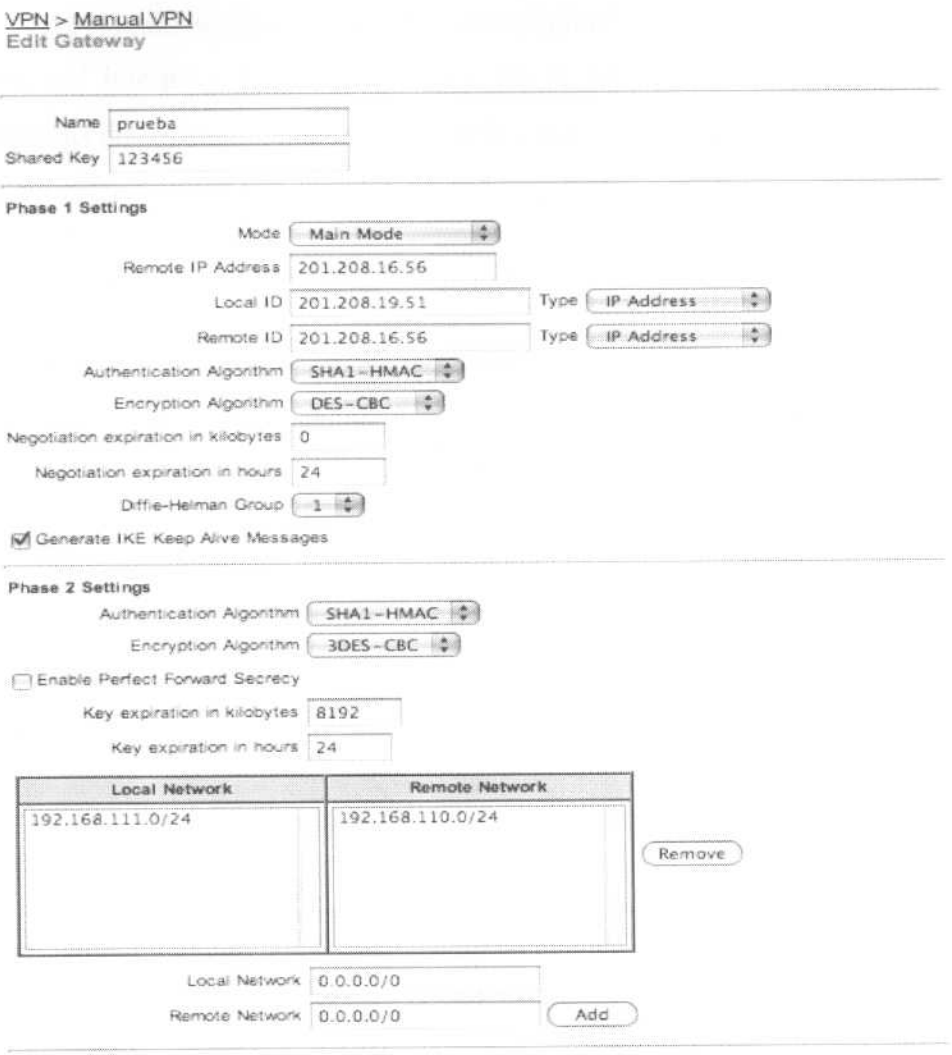

Figura 3. *Configuración de equipo Terminal.*

Fuente: Interfaz de configuración VPN del equipo Watchguard, modelo SOHO 6

Una vez colocados los parámetros en ambos equipos terminales, cuidando de que todos los datos coincidieran en ambos equipos (nombre de la VPN, clave compartida, direcciones IP local y remota, familias de red, tipo de autenticación, algoritmos de encriptación, etc.), se estableció el túnel de forma manual, logrando la implementación de un túnel VPN haciendo uso del protocolo IPSEC.

En la siguiente figura se muestran los parámetros de la VPN (protocolo IP, red externa, red interna y la tabla de rutas). En la tabla de rutas (*Routing Table)* se observan las direcciones de los nodos por lo cuales se establece el túnel y se muestra el uso del protocolo IPSec:

IP

```
IP:     Up for 49 minutes 53 seconds
        Network Buffers Allocated/Total (0/40) Memory Total/Largest Block (10289328/10173792)
        Sockets Allocated/Total (16/80) NAT Ports Avail (1000)RAM Disk (249344)
        Tx: packets (1547)
        Rx: packets (1353) hdr Err(168) delivered (1075)
        forward (83)
```

External Network

```
eth0:   Link encap:Ethernet  HWaddr 00:90:7f:15:03:3e inet addr:201.208.19.51
        RX packets:81 errors:0 bcast:28 disc:0 unk:0
        TX packets:69 errors:0 bcast:115
```

Trusted Network

```
eth1:   Link encap:Ethernet  HWaddr 00:90:7f:15:03:3f inet addr:192.168.111.1
        RX packets:1060 errors:0 bcast:297 disc:0 unk:39
        TX packets:1362 errors:0 bcast:8
```

Optional Network

```
eth2:   network is not active
```

Routing Table

Destination	Gateway	Genmask	Iface
201.208.0.0	201.208.19.51	255.255.224.0	eth0 (external)
192.168.111.0	192.168.111.1	255.255.255.0	eth1 (trusted)
192.168.111.2	201.208.0.1	255.255.255.255	eth0 (external)
192.168.110.1	201.208.0.1	255.255.255.255	eth0 (external)
201.208.16.56	201.208.16.56	255.255.255.255	eth0 (external)
192.168.110.0	201.208.16.56	255.255.255.0	ipsec (tunnel)
0.0.0.0	201.208.0.1	0.0.0.0	eth0 (external)

Figura 4. *Parámetros de la VPN*

Fuente: Interfaz de configuración VPN del equipo Watchguard, modelo SOHO 6

En la siguiente figura se observan las estadísticas del protocolo IPSec, donde vemos el tipo de autenticación y el algoritmo de encriptación que se está utilizando.

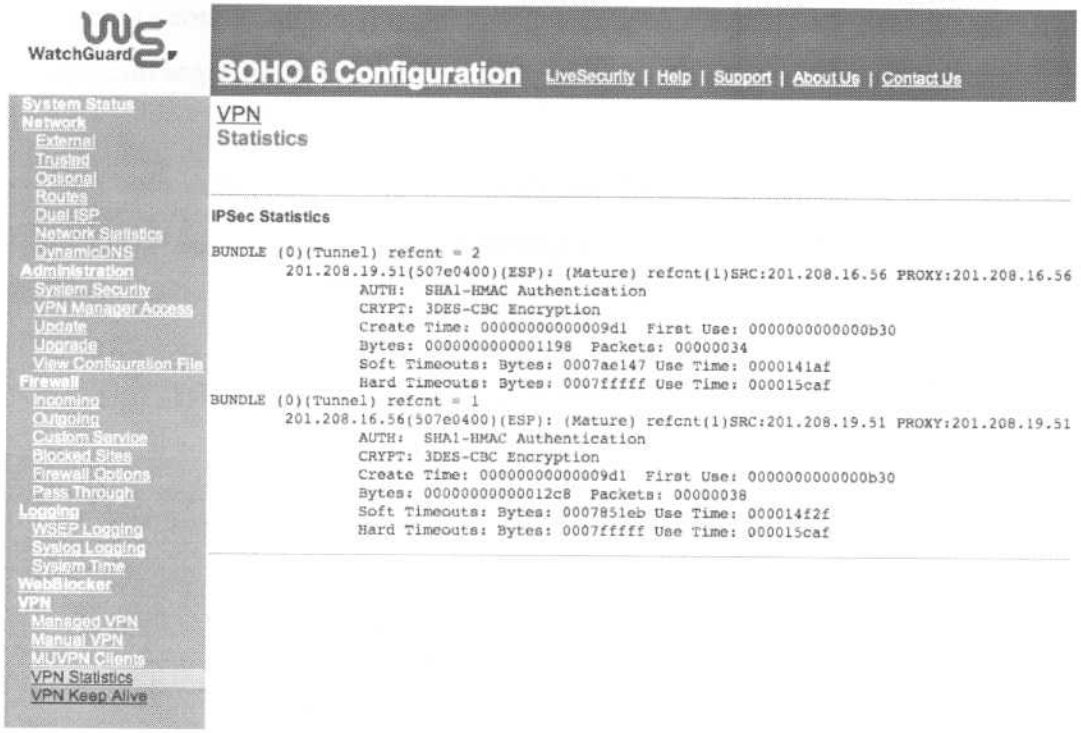

Figura 5. *Estadísticas del protocolo IPSEC*

Fuente: Interfaz de configuración VPN del equipo Watchguard, modelo SOHO 6

No sólo podemos trabajar con direcciones IP para establecer conexiones VPN, también podemos hacerlo con dominios asociados a una dirección IP, es decir, un DNS dinámico, el cual resulta mejor al momento en el que el ISP (por DHCP) cambia o reasigna las direcciones IP que se les había otorgado a los equipos, ya que los equipos asimilan el cambio de dirección IP de manera automática y no hay que volver a configurar la VPN de forma manual. Selección de equipos y proveedores de servicio de Internet

Una vez culminadas las pruebas de conexión, se hizo una comparación entre los equipos D-Link, Netgear y Watchguard, usados tanto en la simulación, como en el desarrollo de las pruebas a través de Internet, tomando en cuenta los aspectos de software y hardware ofrecidos por parte de dichos equipos terminales, para poder

establecer la comunicación entre dos puntos de acceso remoto a través de un esquema de conexión seguro por medio Internet.

Continuando con el desarrollo de esta fase, se seleccionaron los equipos que contaban con las características necesarias para configurar y establecer redes privadas virtuales.

Por otra parte, luego de obtener los equipos a ser usados, se realizó una lista acerca de todos los parámetros que causaran un impacto negativo en los resultados de nuestra investigación por parte de los ISP, tomando como base fundamental las pruebas de conexión realizadas a través del servicio de ABA (acceso de banda ancha) ofrecido por CANTV en la fase anterior, para de esta forma realizar una comparación con los servicios ofrecidos por otros ISP.

IV.3. Diseño de la plataforma

En esta fase, se realiza el diseño de una plataforma de interconexión en base a los análisis ejecutados en la parte inicial del proyecto y las pruebas de conexión culminadas durante las etapas previamente descritas a lo largo de esta investigación.

Para el diseño de la plataforma se realizó un estudio de los parámetros que influyen en la misma, definiendo varios modelos de implementación. Una vez elegido el mejor modelo, se procedió a la definición de otras características importantes del diseño como la selección de equipos, los ISP que cumplían con las condiciones necesarias para establecer la plataforma, el protocolo de seguridad, etc.

Los equipos utilizados cumplieron con una serie de parámetros, los cuales manejaban un esquema de interconexión y protocolos específicos, para lograr brindar seguridad a la información que fue transmitida a través de la red.

Se utilizó un esquema de direccionamiento IP específico tanto en los equipos terminales, como en el servidor que fue utilizado para el establecimiento de la red privada virtual.

IV.3.1. Modelos elaborados para el diseño de la plataforma

A partir de las pruebas realizadas para establecer la conexión VPN surgieron 2 modelos para la implementación de la plataforma de interconexión, de los cuales se eligió el que cumpliera con todos los requerimiento necesarios para llevar a cabo esta investigación.

En el primer modelo se planteó un escenario el cual consiste en conectar dos routers de mayor costo comparados con los routers comerciales utilizados en las pruebas simuladas. Estos routers se colocaron en los puntos terminales de la red privada virtual, de forma tal que pudieran ser administrados colocándoles direcciones IP públicas otorgadas por el ISP utilizado. A continuación se observa el diseño del modelo descrito:

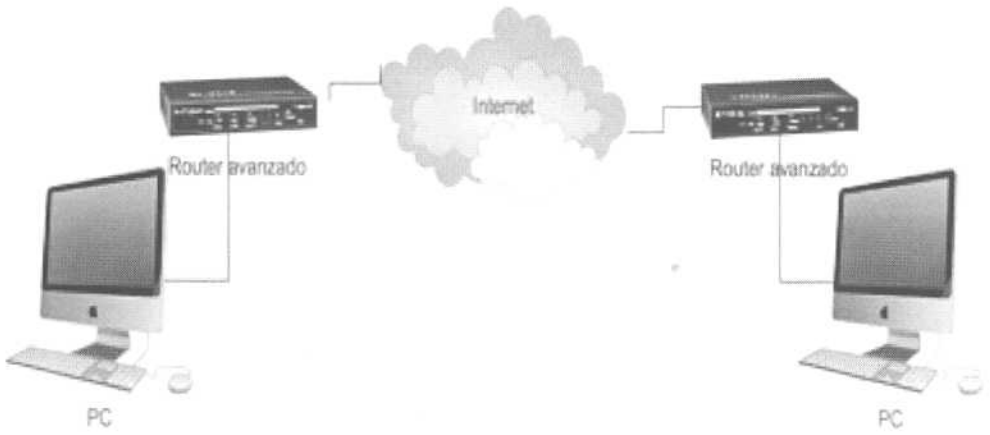

Figura 6. *Modelo establecido con routers avanzados a través de Internet*

Fuente: Elaboración propia

Para el segundo modelo se estableció un escenario similar al anterior, con la variante de la presencia de un servidor entre los dos equipos que iban a crear la VPN. En la siguiente se muestra dicho modelo:

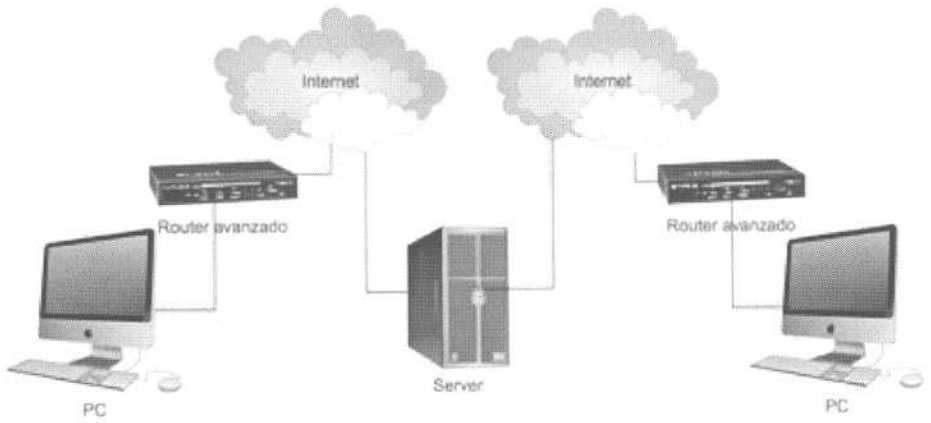

Figura 7. *Modelo establecido utilizando el servidor*

Fuente: Elaboración propia

IV.4. Implementación de la plataforma

Una vez diseñada la plataforma de interconexión y seleccionados los equipos necesarios para su implementación, se hizo la evaluación y asignación del modelo del establecimiento de la red privada virtual tomando en cuenta la rentabilidad y seguridad que dicho modelo ofrecía.

Capítulo V. Resultados

En este capítulo se muestran los resultados obtenidos a partir del desarrollo descrito anteriormente para lograr establecer una plataforma de interconexión independiente al esquema de direccionamiento IP provisto por los ISP en Venezuela.

V.1. Análisis

A continuación se muestran los resultados de los protocolos utilizados en el establecimiento de redes VPN, el resultado del estudio de los ISP y de los routers utilizados en el mercado venezolano.

V.1.1. Selección del protocolo para el establecimiento de las VPN

En primer lugar, luego de realizar la búsqueda acerca de los diferentes protocolos que eran utilizados, se obtuvo como resultado que los protocolos más usados en el establecimiento de redes privadas virtuales eran IPSec, PPTP y L2TP. Para estudiar cada uno de los protocolos, se consultaron los RFC 3585, 2637 y 2661 correspondientes a los protocolos mencionados anteriormente, provistos por la base datos publicada por la IETF (Internet Engineering Task Force) en la web.

Luego de profundizar en la información referente a cada uno de ellos, se hizo una comparación en base a los métodos de autenticación y encriptación que éstos usaban y la forma en que funcionaba cada uno. Finalmente se determinó que IPSec es el protocolo más apropiado para garantizar la seguridad en las comunicaciones a través de las redes privadas virtuales, debido a que este trabaja en la capa tres del modelo OSI proporcionando un nivel mas alto de seguridad, a diferencia de los protocolos PPTP y L2TP, los cuales presentaron menos beneficios en cuanto a interoperabilidad y seguridad en el desarrollo de las redes IP.

V.1.2. Características de los ISP usados en Venezuela para el funcionamiento de las VPN

Se obtuvieron resultados relacionados con los ISP que podían ser utilizados, tomando en cuenta las diferentes características que habían sido recopiladas durante el desarrollo de este estudio. Estos resultados indicaron que todos los proveedores del servicio de Internet que fueron estudiados, tomando en cuenta el tipo de tecnología de acceso utilizada, ancho de banda, esquema de direccionamiento IP, entre otros; a pesar de tener distintas características en cuanto a los servicios que estos ofrecían, no eran un factor determinante que influyera directamente en el alcance de nuestra investigación.

V.1.3. Tipos de routers con las especificaciones técnicas requeridas para el funcionamiento adecuado de la red privada virtual

Se realizó el estudio de los routers más usados en el mercado venezolano, de los cuales se hizo una selección de los equipos que cumplieran con las características necesarias mínimas para lograr establecer la conexión VPN.

Dentro de las especificaciones de los equipos terminales seleccionados, una de las características principales, era que manejaban el protocolo IPSec, para lograr establecer conexiones, en las cuales los envíos de paquetes viajaran de forma segura y confiable. Por lo tanto, una vez obtenida la lista de los equipos que manejaban este protocolo, fue necesario agruparlos en base a ciertos parámetros de configuración para que las conexiones pudieran ser establecidas de forma exitosa. Dichos parámetros de configuración eran los que permitían realizar el enlace, conocidos como *IPSec Server*, *IPSec Client* y *IPSec passthrough*, los cuales introducían las reglas requeridas para que ambos puntos terminales fueran capaces de interpretar la información que iba a ser enviada sin presentar incompatibilidades al momento de intercambiar los datos.

Las opciones de *IPSec Server* y *IPSec Client* permiten que los equipos que actúen como puntos terminales puedan reconocer los paquetes encriptados con el protocolo IPSec y que la información que viaja a través de la red VPN, pueda ser procesada en el destino e interpretar lo que fue enviado por el origen, mientras que *IPSec passthrough* permite que los equipos que actúen como nodos reconozcan los paquetes encriptados con el protocolo IPSec y los dejen pasar hacia su destino final.

V.2. Pruebas de Conexión

En esta etapa de la investigación, se realizaron una serie de pruebas simuladas y reales, con la finalidad de crear una plataforma capaz de establecer una red privada virtual punto a punto entre dos equipos terminales.

V.2.1. Simulación de una VPN haciendo uso de un router cumpliendo la función del ISP

En este apartado, se realizan las pruebas simuladas haciendo uso de equipos comerciales de bajo costo y de otros equipos comerciales con un nivel de configuración mas avanzado.

V.2.1.1. Pruebas realizadas con equipos comerciales de bajo costo

Se realizaron las pruebas utilizando equipos de bajo costo, implementando un ISP simulado con un equipo de marca *Watchguard* entre ambos equipos terminales, el cual otorgaba direcciones IP dinámicas a estos puntos de acceso.

La conexión presentó fallas de comunicación al intentar mandar paquetes a través de esta configuración, debido a la limitante que estos tenían en cuanto a los parámetros que podían manejar, produciendo un resultado negativo en la realización de esta prueba.

V.2.1.2. Pruebas realizadas con equipos comerciales con un nivel de configuración más avanzado

Luego de probar con equipos comerciales de bajo costo y observar su incompatibilidad para establecer conexiones a través de redes privadas virtuales, surge la necesidad de buscar un producto con un costo un poco más elevado que cumpla con las especificaciones requeridas para lograr establecer una comunicación de tipo VPN entre los dos equipos terminales. Por tanto, se recurre a equipos de marca *Watchguard*, los cuales ofrecen una solución integral proporcionando tanto seguridad, como establecimiento de túneles de forma segura.

Posteriormente, se realizan las mismas pruebas realizadas en el punto anterior, con equipos de esta marca y finalmente se logra establecer una VPN fundamentada en el protocolo IPSEC.

A continuación se observa el log de eventos donde podemos ver el establecimiento del túnel IPSEC:

2008-05-29-18:06:41	**MONITOR**	Administrator access allowed from 192.168.111.4
2008-05-29-18:05:32	**IP**	discard from 217.125.41.10 port 1041 to 201.208.19.51 port 137 UDP (SIP discarded)
	IP	entry duplicated 1 times
2008-05-29-18:04:47	**IP**	discard from 81.37.105.12 port 29192 to 201.208.19.51 port 44774 TCP SYN (default)
2008-05-29-18:04:44	**MONITOR**	IPSEC tunnel is active
2008-05-29-18:04:44	**IP**	discard from 81.37.105.12 port 29192 to 201.208.19.51 port 44774 TCP SYN (default)
	IP	entry duplicated 2 times
2008-05-29-18:03:21	**IP**	discard from 201.234.182.4 port 1401 to 201.208.19.51 port 44774 TCP SYN (default)

Figura 8. *Establecimiento del Tunel VPN con el protocolo IPSEC.*

Fuente: Interfaz de configuración VPN del equipo Watchguard, modelo SOHO 6

V.2.2. Establecimiento de una conexión VPN a través de Internet

V.2.2.1. Pruebas realizadas con equipos comerciales con un nivel de configuración más avanzado

Luego de realizar las simulaciones con los equipos comerciales de bajo costo, se descarta la posibilidad de ejecutar estas mismas pruebas a través de Internet. Asimismo, observando el buen desempeño de los equipos comerciales de mayor costo con especificaciones técnicas más avanzadas, se procedió a probar el mismo escenario utilizando un ISP real, que para efectos de prueba de laboratorio, se eligió el servicio ofrecido por el ISP provisto por CANTV.

Una vez configurados los parámetros en ambos equipos terminales, cuidando que las direcciones IP de las máquinas detrás de estos equipos se encontraran dentro de la misma familia de red, se logró establecer la red privada virtual, realizando intercambio de paquetes a través de un túnel fundamentado en el protocolo IPSec. El túnel permaneció activo por un tiempo, casi una hora hasta que al momento de culminarse el tiempo de expiración del mismo, la conexión se cayó por falta de presencia de tráfico entre ambos routers, ocasionando así, la caída de la red privada virtual. En la figura siguiente se puede observar el tiempo de expiración del túnel:

```
IP

IP:     Up for 49 minutes 53 seconds
        Network Buffers Allocated/Total (0/40) Memory Total/Largest Block (10289328/10173792)
        Sockets Allocated/Total (16/80) NAT Ports Avail (1000)RAM Disk (249344)
        Tx: packets (1547)
        Rx: packets (1353) hdr Err(168) delivered (1075)
        forward (83)
```

***Figura 9**. Expiración del túnel VPN*

Fuente: Interfaz de configuración VPN del equipo Watchguard, modelo SOHO 6

V.2.2.2. Pruebas realizadas con equipos comerciales con un nivel de configuración más avanzado conectados remotamente a un servidor con dirección IP fija

En esta prueba, se realizó la conexión entre dos puntos de acceso remoto a través de un servidor que posee una dirección IP estática (fija) ubicado en la empresa, logrando así el establecimiento de un túnel VPN de forma segura y continua, es decir, si el ISP cambia o reasigna la dirección IP de alguno de los puntos terminales utilizando el esquema de direccionamiento IP DHCP, el dispositivo ubicado en ese punto sigue conectado al túnel a través de la dirección estática provista por el servidor de la empresa. En la siguiente figura se muestra la conexión al servidor:

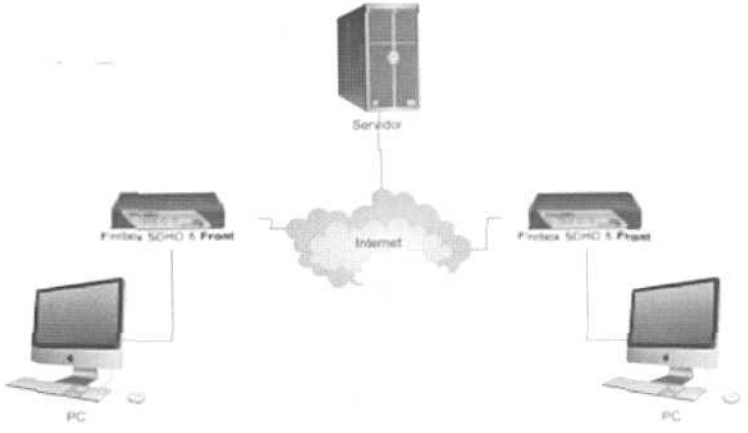

Figura 10. *Plataforma de interconexión utilizando un servidor*

Fuente: Elaboración propia

V.3. Selección de equipos y proveedores de servicio de Internet

A continuación se muestra resumido en tablas los equipos terminales o routers y los proveedores de servicio de Internet o ISP seleccionados luego de culminada la fase de las pruebas de conexión.

V.3.1. Selección de equipos

Al culminar las pruebas donde se tomaron en cuenta los parámetros de los equipos se obtuvieron una serie de equipos los cuales se encuentran reflejados en las tablas mostradas a continuación:

Marca	WatchGuard Firebox Edge e-Series			Firebox SOHO
Modelo	**FB X55e**	**FB X20e**	**FB X10e**	**SOHO 6**

Tabla 9. *Modelo de equipos compatibles con la plataforma*

Fuente: Elaboración propia

V.3.2. Selección de los ISP

En esta sección se muestran los posibles ISP que puede ser utilizados por los equipos terminales y por el servidor implementado en la plataforma de interconexión.

V.3.2.1. Proveedores seleccionados en relación a los equipos terminales

En cuanto a los ISP, como se mencionó anteriormente en la fase de análisis referente al estudio y selección de los mismos, se obtuvo que de acuerdo a las especificaciones técnicas que estos ofrecían, como el tipo de tecnología de acceso utilizado, ancho de banda, esquemas de direccionamiento IP, entre otros; todos los proveedores investigados resultaron ser compatibles con el esquema de la plataforma *que se implementó en los puntos de acceso remoto de los equipos utilizados.*

En la siguiente tabla se muestran los proveedores de servicio de Internet seleccionados para el establecimiento de una plataforma de interconexión a través de redes privadas virtuales:

ISP	Compatible con equipos terminales	No compatible con equipos terminales
CANTV	x	
Movistar	x	
Génesis Telecom	x	
Intercable	x	
Net-Uno	x	
Supercable	x	
Movilmax	x	

Tabla 10. *ISP compatibles con los equipos terminales*

Fuente: Elaboración propia

V.3.2.2. Proveedores seleccionados en relación al servidor utilizado en la plataforma de interconexión

Con respecto al servidor, la mayoría de los ISP eran compatibles con la plataforma de interconexión, siempre y cuando contaran con un esquema de direccionamiento capaz de otorgar direcciones IP estáticas o fijas para poder ser alcanzados en todo momento a través de los equipos terminales.

A continuación se muestra la tabla de los ISP que otorgan direcciones IP estáticas o fijas, que son compatibles con el servidor y con todos sus parámetros de configuración:

ISP	Compatible con el servidor	No compatibles con el servidor
CANTV	x	
Movistar	x	
Génesis Telecom	x	
Intercable	x	
Net-Uno		x
Supercable		x
Movilmax		x

Tabla 11. *ISP compatibles con el servidor de la plataforma*

Fuente: Elaboración propia

V.4. Diseño de la plataforma

En esta fase, se realizó el diseño de una plataforma de interconexión en base a los análisis ejecutados en la parte inicial del proyecto y las pruebas de conexión culminadas durante las etapas previamente descritas a lo largo de esta investigación.

V.4.1. Modelos de implementación

A partir de las pruebas realizadas para establecer la conexión VPN surgieron 2 modelos para la implementación de la plataforma de interconexión.

En el primer modelo se planteó un escenario en el cual se conectaron dos routers de marca WatchGuard, modelo SOHO 6, de mayor costo comparados con los routers comerciales como el D-Link 524 y el NetGear WTG-624, pero con especificaciones de Hardware y Software mucho más avanzadas. Estos routers se colocaron en los puntos terminales de la red privada virtual, los cuales fueron administrados y configurados para establecer una VPN a través de Internet, utilizando un esquema de direccionamiento IP DHCP provisto por el ISP CANTV proporcionado por su servicio ABA, el cual le otorgó direcciones dinámicas públicas a cada uno de los routers. A continuación se observa el diseño del modelo descrito:

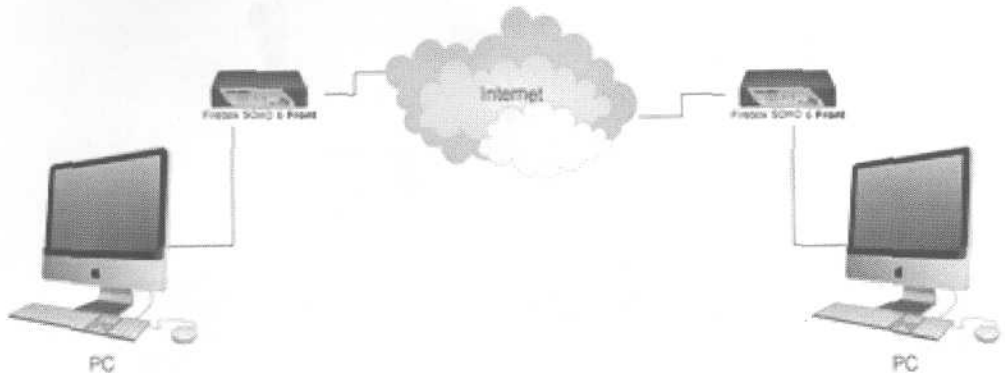

Figura 11. *Modelo de Plataforma de interconexión utilizando routers Watchguard*
Fuente: Elaboración propia

Este escenario resultó poco efectivo por el inconveniente de que al momento de que el ISP, en este caso CANTV, reasignaba o cambiaba las direcciones IP de algunos de los routers conectados a la VPN por medio del esquema de direccionamiento IP dinámico DHCP, el enlace VPN se caía. Por lo tanto, el modelo planteado dependía del esquema de direccionamiento IP provisto por el ISP evitando así continuidad en el enlace establecido.

En el segundo modelo se estableció un escenario similar al anterior, con la variante de la presencia de un servidor entre los dos equipos ubicados en los extremos del enlace VPN. En la siguiente se muestra dicho modelo:

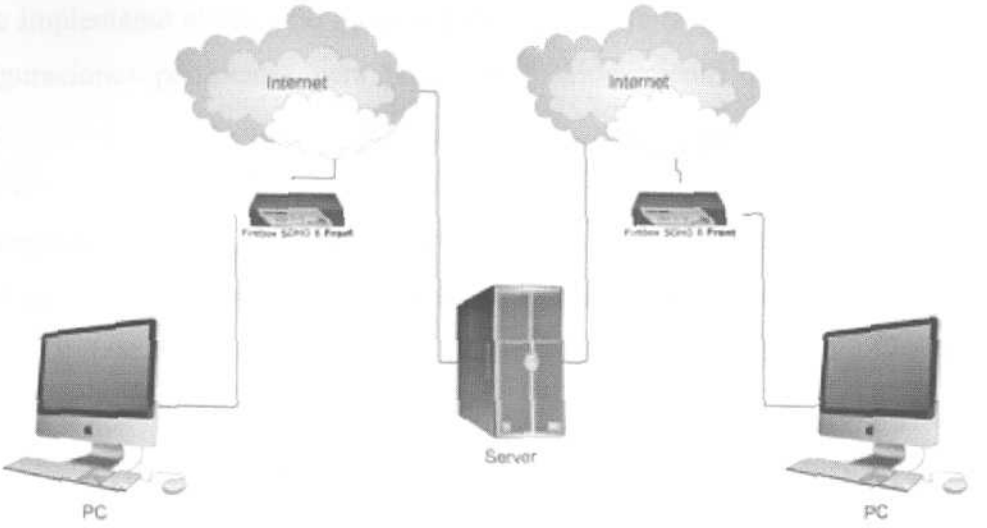

Figura 12. *Modelo de Plataforma de interconexión utilizando routers Watchguard y el servidor*
Fuente: Elaboración propia

Este escenario resultó ser efectivo porque la conexión entre los routers ubicados en los extremos de la red privada virtual se mantenía por tiempo ilimitado, ya que en el momento en el que el ISP, CANTV, reasignaba o cambiaba las direcciones IP de algunos de los equipos terminales, estos equipos estaban configurados para que siempre se conectaran a una dirección IP estática o fija provista por el servidor central ubicado en el medio del enlace, el cual mantenía activa la VPN proporcionando seguridad y confiabilidad en el envío de datos a través de la misma.

V.5. Implementación de la plataforma

En esta parte se culmina el desarrollo del proyecto, donde se arreglaron los últimos detalles luego de culminar el diseño de la plataforma de interconexión independiente al esquema de direccionamiento IP utilizado por los diferentes ISP en Venezuela.

Se implementó el segundo modelo culminado en la fase de diseño, ajustando las configuraciones pertinentes para poner en funcionamiento dicho esquema de conexión.

Luego se estableció la comunicación de forma exitosa entre ambas máquinas pasando a través de los routers configurados para el establecimiento de la VPN, para comenzar a realizar pruebas a través de la misma generando tráfico para probar que ésta se mantuviera activa todavía.

Finalmente, se realizó un seguimiento del paquete utilizando el comando "trace xxx.xxx.xxx.xxx" para saber los diferentes saltos por los cuales pasaba el paquete y comprobar que el túnel se había establecido de forma correcta.

A continuación se muestra una imagen con los diferentes saltos a través de los cuales pasó el paquete, el default Gateway y la dirección IP de todos los clientes VPN (direcciones IP privadas) conectados al servidor para llegar a su destino final con éxito.

Destination	Gateway	Genmask	Flags	MSS Window	irtt	Iface
192.168.16.248	0.0.0.0	255.255.255.248	U	0 0	0	eth1
192.168.188.248	0.0.0.0	255.255.255.248	U	0 0	0	eth1
201.206.0.0	0.0.0.0	255.255.224.0	U	0 0	0	eth0
192.168.19.248	0.0.0.0	255.255.255.248	U	0 0	0	eth1
192.168.182.248	0.0.0.0	255.255.255.248	U	0 0	0	eth1
192.168.20.248	0.0.0.0	255.255.255.248	U	0 0	0	eth1
192.168.68.248	0.0.0.0	255.255.255.248	U	0 0	0	eth1

Figura 13. *Tabla de rutas del servidor*

Fuente: Interfaz del servidor

Capítulo VI. Conclusiones y Recomendaciones

A continuación se plantean una serie de conclusiones obtenidas, a partir de los objetivos establecidos al inicio de la investigación y de los resultados procedentes de la misma. Adicionalmente, se mencionan algunas recomendaciones relacionadas con el área de redes y conectividad a través de una plataforma de interconexión utilizando cualquier esquema de direccionamiento IP sobre dicha plataforma.

A través de la historia de la humanidad, el hombre ha utilizado diferentes formas de comunicarse, desde la comunicación con señas, hasta la comunicación a distancia por medio de dispositivos tecnológicos avanzados.

Los avances logrados en el área de telecomunicaciones han permitido que el hombre se desempeñe de una manera más eficiente, y es esta eficiencia lo que en gran medida, ha motivado a empresas nuevas que día a día exigen mayores retos a quienes lo desarrollan. De esta forma, se ha llegado a alternativas de gran impacto a través del tiempo como son: Internet, seguridad en redes, establecimiento de redes privadas virtuales, entre otros.

Al inicio de esta investigación, se estudiaron los diferentes ISP en Venezuela para elegir el que brindara los mejores beneficios en base a las características necesarias para el establecimiento de la plataforma de interconexión independiente de su esquema de direccionamiento IP, así como también, se hizo un análisis de los posibles routers que pudieran ser implementados en la plataforma de interconexión como puntos terminales.

En base a esto, se realizaron una serie de pruebas, las cuales permitieron concluir que la solución para establecer una plataforma de interconexión independiente del esquema de direccionamiento IP utilizando cualquier proveedor de servicio de Internet, es contar con un servidor que esté conectado al ISP a través de

una o varias direcciones IP estáticas o fijas, sirviendo de enlace entre varios puntos de acceso remoto para el intercambio de información de forma segura y continua.

A pesar de que se utilizaron equipos de mayores costos en el modelo implementado en el desarrollo de este proyecto, comparado con los routers comerciales analizados previamente en la investigación, resulta mucho más económico utilizar este tipo de plataforma de interconexión que pedir una dirección IP fija a un ISP o pagar por un servicio de enlace dedicado. Lo único que se necesita para implementar esta plataforma es:

- Contar con equipos terminales que agrupen las características necesarias para establecer una VPN, utilizando el protocolo IPSec, el cual es mejor a PPTP y L2TP en materia de seguridad en redes. Los equipos de marca WatchGuard cumplen con estas especificaciones, ya que son dispositivos que integran una serie de funciones en un mismo hardware.
- Poseer un servidor que cuente con una o varias direcciones IP fijas el cual funcione como una especie de mediador entre los routers ubicados en localidades remotas, proporcionando de esta manera conectividad de forma segura y confiable.

Otra ventaja de utilizar esta plataforma de interconexión es que se ahorran muchas direcciones IP al momento de interconectar varias localidades remotas que tengan uno o más usuarios conectados, ya que varios usuarios se pueden conectar a un solo equipo Watchguard y pueden enviar información a través de los mismos. De este modo, se provee una solución inmediata al problema existente de escasez de direcciones Ipv4 proporcionando una respuesta efectiva y rentable para el sector corporativo, ya que la versión 6 de IP (Ipv6) todavía no se ha implementado a nivel mundial por lo que es una solución a largo plazo.

Es recomendable ser cuidadoso al momento de configurar los equipos terminales o routers para el establecimiento de una VPN, ya que un mínimo error en la configuración de algún parámetro de estos equipos, puede traer como consecuencia que no se establezca la conexión entre ambos dispositivos.

Capítulo VII. Bibliografía

- VPN Consortium. (2006, Marzo) VPN Technologies: Definitions and Requirements. [Homepage]. Consultado el día 10 de Enero de 2008 de la World Wide Web: http://www.vpnc.org/vpn-technologies.html

- S. Kent and R. Atkinson. (1998, Noviembre) RFC 2401 Security Architecture for the Internet Protocol. [Online Protocol]. Consultado el día 10 de Enero de 2008 de la World Wide Web: http://tools.ietf.org/html/rfc2401

- B. Patel (*Intel*), B. Aboba (*Microsoft*), G. Zorn (*Cisco Systems*). (1998, Noviembre) RFC 3913 Securing L2TP using IPsec. [Online Protocol]. Consultado el día 10 de Enero de 2008 de la World Wide Web: http://www.ietf.org/rfc/rfc3193.txt

- T. Dierks and C. Allen (*Certicom*). (1999, Enero) RFC 2246 The TLS Protocol Version 1.0. [Online Protocol]. Consultado el día 10 de Enero de 2008 de la World Wide Web: http://www.ietf.org/rfc/rfc2246.txt

- W. Townsley, A. Valencia (*Cisco Systems*) A. Rubens (*Ascend Communications*) G. Pall G. Zorn (*Microsoft Corporation*) B. Palter (*Redback Networks*). (1999, Agosto) RFC 2661 Layer Two Tunneling Protocol "L2TP" [Online Protocol]. Consultado el día 10 de Enero de 2008 de la World Wide Web: http://www.ietf.org/rfc/rfc2661.txt

- WatchGuard (1999, Febrero). Firebox® SOHO 6 Datasheet [Online Document]. Consultado el 10 de Enero de 2008 de la World Wide Web: http://www.watchguard.com/docs/html/soho6_ds.asp

- Broadband Hardware (2000, Enero). The SG Broadband Hardware database [Online Catalog]. Consultado el 10 de Enero de 2008 de la World Wide Web: http://www.speedguide.net/broadband.php.

Lista de Acrónimos

ADSL: Asymmetric Digital Subscriber Line

AH: Authentication Header

ATM: Asynchronous Transfer Mode

CHAP: Challenge-Handshake Authentication Protocol

DHCP: Dynamic Host Configuration Protocol

DNS: Domain Name System

DSL: Digital Subscriber Line

ESP: Encapsulating Security Payload

GRE: Generic Routing Encapsulation

IETF: Internet Engineering Task Force

IKE: Internet key exchange

IP: Internet protocol

IPSEC: *Internet protocol security*

ISP: Internet service provider

IT: Information technologie

L2F: *Layer 2 fowarding*

L2TP: Layer 2 tunneling protocol

LMDS: Local Multipoint Distribution System

MPPE: Microsoft Point to Point Encryption

NAT: Network address translator

PAP: Password Authenticaction Protocol

PPP: Point to Point Protocol

PPPoE: Point to Point Protocol over Ethernet

PPTP: Point to point Tunneling Protocol

RFC: Request For Comments

SSL: Secure Sockets Layer

TCP: Transmission Control Protocol

TLS: Transport Layer Security

VPN: Virtual Private Network

WLL: Wireless Local Loop

Apéndices

Apéndice A. Configuración para establecimiento de una VPN con equipos de marca WatchGuard, modelo Firebox SOHO 6:

Los equipos Watchguard, configurados para ser VPN o únicamente Firewall, cuentan con una interfaz, la cual establece comunicación con el equipo o dispositivo que inicia comunicación con Internet, ya sea un *MODEM Dial-up* o cualquiera que establezca salida a velocidades mayores como banda ancha. Esta interfaz es llamada "Externa" y cuenta con varios tipos de configuración dependiendo de los datos suministrados por el ISP.

A continuación se describe cómo establecer una VPN de forma manual:

- Conectar físicamente el "Firebox Edge X" al modem mediante un cable RJ-45
- Establecer conexión entre el equipo y el computador mediante otro cable RJ45
- Entrar en la página principal del equipo usando la dirección IP: 192.168.111.1
- Ingresar al link "External" para configurar el modo de conexión a Internet, los cuales pueden ser los siguiente:
  - DHCP (el más usado)
  - Manual
  - PPoE

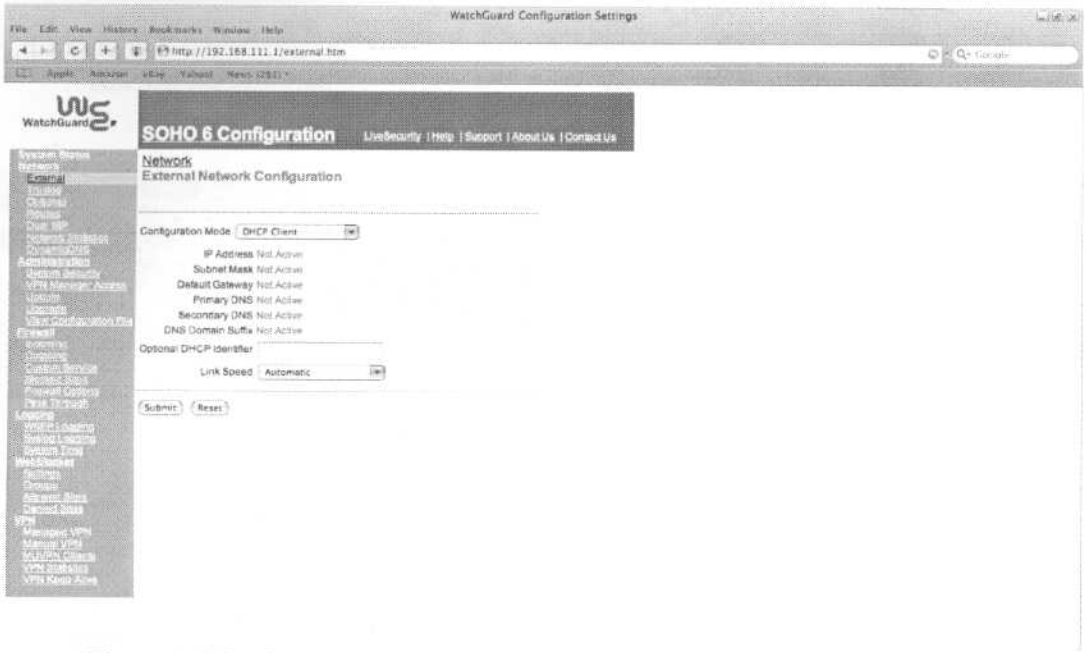

Figura A.1 *Configuración del link "External" de una VPN con equipos Watchguard*

Fuente: Recursos internos de la empresa

- Se ingresa al link "trusted" para configurar el direccionamiento interno de la red y/o las computadoras que van a estar conectadas al equipo.

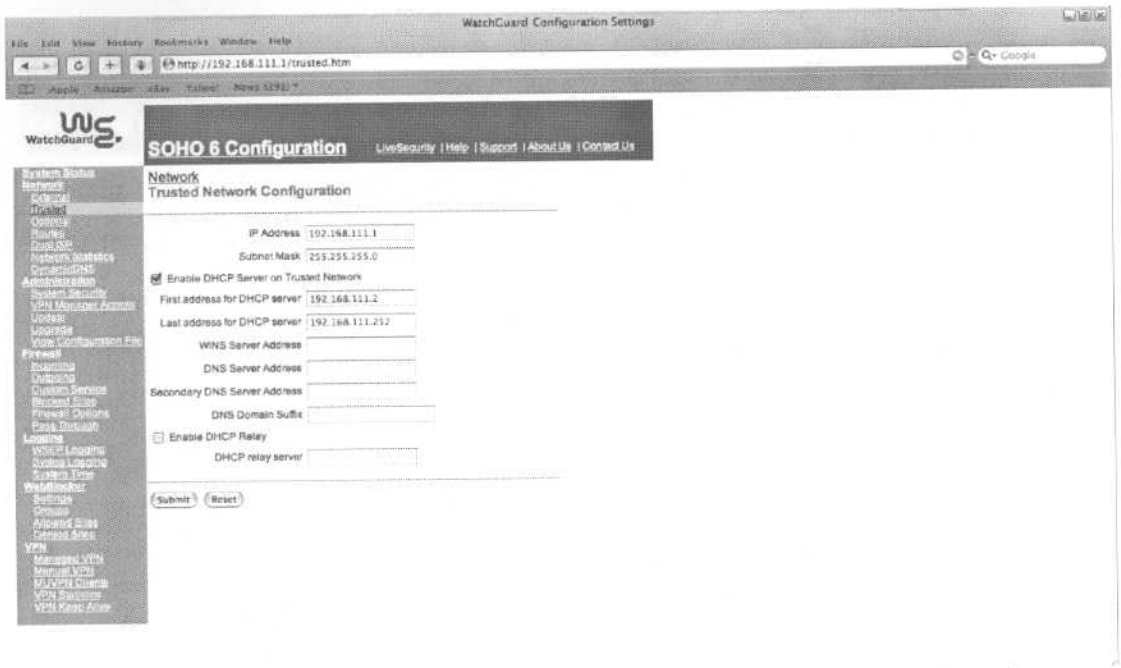

Figura A.2 *Configuración del link "Trusted" de una VPN con equipos Watchguard*

Fuente: Recursos internos de la empresa

- Se ingresa al link "Manual VPN" para establecer los parámetros de conexión de la computadora local y remota. Luego de ingresar a esta página se hace clic en "Add…" para configurar la VPN que se va a establecer.

Figura A.3 *Configuración del link "Manual VPN" de una VPN con equipos Watchguard*

Fuente: Recursos internos de la empresa

- Se crea el nombre y la clave para poder establecer la VPN.
- En la fase 1, se configura el modo de conexión de la VPN, el cual puede ser de tipo agresivo o principal, se coloca la dirección IP del equipo remoto en el campo de "Remote IP Address". También se colocan las direcciones IP de cada punto Terminal en los campos de Local ID y Remote ID, los cuales también pueden ser establecidos con un *dyn dns* que resuelve la dirección IP del Terminal. Por último se coloca el algoritmo de autenticación y encriptación que se va a usar y otros parámetros necesarios para el establecimiento de la VPN.
- En la fase 2 se coloca también el algoritmo de autenticación y encriptación que se va a usar, y se agrega la dirección IP de la red local y de la red remota en las cuales se va a establecer la VPN.

Los datos que se suministran en un equipo terminal para el establecimiento de la VPN deben ser los mismos en el otro equipo terminal para que pueda establecerse el túnel.

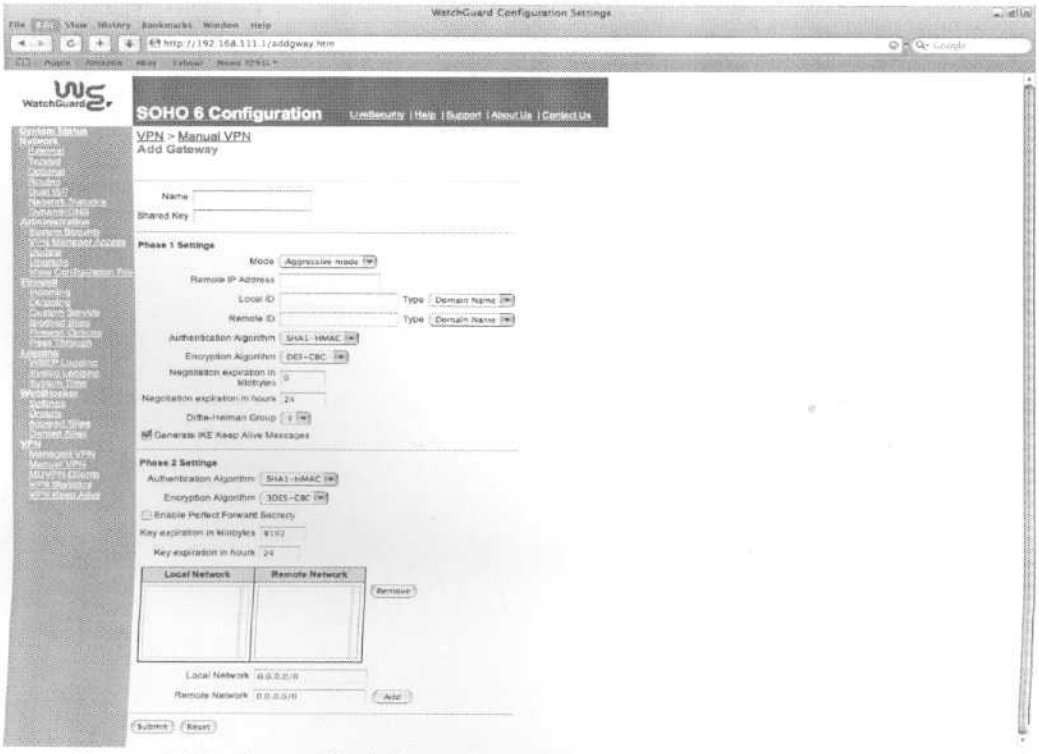

Figura A.4 *Configuración de los parámetros de una VPN con equipos Watchguard*

Fuente: Recursos internos de la empresa