FIREWALL Y VPN CON OPNET

JULIO CESAR CASTILLO ROMERO
ANDREA CAROLINA VARGAS JARAMILLO

MONOGRAFÍA

PROGRAMA DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA
UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR
CARTAGENA
2011

FIREWALL Y VPN CON OPNET

JULIO CESAR CASTILLO ROMERO
ANDREA CAROLINA VARGAS JARAMILLO

ASESOR
GONZALO LÓPEZ VERGARA

MONOGRAFÍA

PROGRAMA DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA
UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR
CARTAGENA
2011

Nota De Aceptación

_____

_____

_____

_____

_____

_____
Firma Del Presidente Del Jurado

_____
Firma Del Jurado

_____
Firma Del Jurado

Cartagena de indias D. T y C, Enero de 2011

Cartagena de Indias, Enero de 2011

Señores

Comité De Revisión De Monografía

Universidad Tecnológica de bolívar

L.C.

Cordial Saludo

Por medio de la presente nos permitimos informarles que hemos completado la elaboración de nuestra monografía titulada "FIREWALL Y VPN CON OPNET" en conformidad con los objetivos planteados, por ello, presentamos dicha Monografía ante ustedes para su evaluación.

Atentamente

_____	_____
Julio Cesar Castillo Romero	Andrea Carolina Vargas Jaramillo

Cartagena de Indias, Enero de 2011

Señores

Comité De Revisión De Monografía

Universidad Tecnológica de bolívar

L.C.

Cordial Saludo

Por medio de la presente les informo que la monografía titulada "FIREWALL Y VPN CON OPNET" ha sido desarrollada en conformidad con los objetivos planteados.

Como director del proyecto, considero que el trabajo es satisfactorio y amerita ser presentado para su evaluación.

Atentamente

_____

MSC. GONZALO LÓPEZ VERGARA

AUTORIZACIÓN

NOSOTROS, Julio Cesar Castillo Romero y Andrea Carolina Vargas Jaramillo, identificados con c.c. 1.047.381.590 de Cartagena y 1.047.396.469 de Cartagena respectivamente, autorizamos a la Universidad Tecnológica De Bolívar a hacer uso de nuestra monografía y publicarla en el catálogo On-Line de la biblioteca institucional.

_____ _____

Julio Cesar Castillo Romero Andrea Carolina Vargas Jaramillo

DEDICATORIA

A nuestros padres, hermanos, familiares y amigos cercanos, quienes con su apoyo incondicional nos motivaron a esforzarnos por alcanzar nuestro objetivo de ser seres humanos ejemplares y grandes profesionales.

AGRADECIMIENTOS

A Dios, por habernos permitido alcanzar exitosamente nuestras metas y por habernos ayudado en el proceso.

A nuestras familias por su apoyo ante las dificultades y por haber depositado su confianza en nosotros en todo momento y bajo cualquier circunstancia.

A los profesores, profesionales, tutores y monitores que intervinieron en nuestro proceso formativo, por haber aportado una parte de ellos en nuestros pensamientos y nuestra personalidad.

A la Universidad Tecnológica de Bolívar por haber construido un espacio en el cual pudimos relacionarnos con otras personas con las cuales desarrollamos nuestros conocimientos, actitudes y nuestras personalidades.

TABLA DE CONTENIDO

LISTA DE ILUSTRACIONES

LISTA DE TABLAS

LISTA DE ANEXOS

GLOSARIO

DoS: Es la negación de un servicio de red determinado, usualmente es un ataque por parte de un usuario no autorizado quien deshabilita servicios de un servidor.

DMZ: También llamada zona desmilitarizada o red perimetral, es una red local que se ubica entre la red interna de una organización y una red externa, generalmente Internet. El objetivo de una DMZ es que las conexiones desde la red interna y la externa a la DMZ estén permitidas, mientras que las conexiones desde la DMZ sólo se permitan a la red externa, de tal manera que los equipos (hosts) en la DMZ no pueden conectar con la red interna[1].

DS1: Tipo de enlace en telecomunicaciones que permite transmitir información a una tasa de transferencia de 1.544 Mbps.

FIREWALL: Es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas[1].

FTP: Es un protocolo de red para la transferencia de archivos entre sistemas conectados a una red TCP (Transmission Control Protocol), basado en la arquitectura cliente-servidor[1].

GATEWAY: (puerta de enlace), Es un dispositivo, con frecuencia un ordenador, que permite interconectar redes con protocolos y arquitecturas diferentes a todos los niveles de comunicación. Su propósito es traducir la información del protocolo utilizado en una red al protocolo usado en la red de destino[1].

[1] Definición tomada de Wikipedia, La enciclopedia Libre, http://es.wikipedia.org

HACKERS: En la actualidad se usa de forma corriente para referirse mayormente a los criminales informáticos, debido a su utilización masiva por parte de los medios de comunicación desde la década de 1980[1].

HTTP: Hypertext Transfer Protocol o en español protocolo de transferencia de hipertexto, es el protocolo usado en cada transacción de la World Wide Web[1].

IPSEC: (abreviatura de Internet Protocol security) es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando y/o cifrando cada paquete IP en un flujo de datos. IPsec también incluye protocolos para el establecimiento de claves de cifrado[1].

L2F: (Layer 2 Forwarding), es un protocolo diseñado por Cisco para establecer túneles de tráfico desde usuarios remotos hasta sus sedes corporativas. Su nombre indica que trabaja en la capa 2 (Enlace) de modelo de referencia OSI, permitiendo fiabilidad en la transferencia de información y flexibilidad para manejar protocolos distintos al IP. En L2F es que el establecimiento de túneles no depende del protocolo IP (Internet Protocol), por lo tanto es capaz de trabajar directamente con otros medios como Frame Relay o ATM empleando más de una conexión.

L2TP: (Layer 2 Tunneling Protocol), Es un protocolo de comunicaciones que utiliza PPP para proporcionar acceso 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[1].

[1] Definición tomada de Wikipedia, La enciclopedia Libre, http://es.wikipedia.org

NAT: (Network Address Translator), es el proceso de "Traducción de Direcciones de Red" mediante el cual los routers o firewalls modifican direcciones IP privadas para poder acceder a internet mediante una dirección IP Pública. Generalmente este proceso se emplea en redes donde se tienen muchos equipos (con direcciones IP privadas) pero se consta de una o pocas direcciones IP públicas para acceder a internet, por lo tanto, mediante el servicio NAT las direcciones IP públicas se convierten en un recurso compartido que permite a todos los usuarios de la red acceder a internet.

PPTP: (Point-To-Point Tunneling Protocol), Permite el seguro intercambio de datos de un cliente a un servidor formando una Red Privada Virtual, basado en una red de trabajo vía TCP/IP[1].

Protocolos: Es el conjunto de reglas normalizadas para la representación, señalización, autenticación y detección de errores necesario para enviar información a través de un canal de comunicación[1].

Proxy: es un programa o dispositivo que realiza una acción en representación de otro, esto es, si una hipotética máquina *a* solicita un recurso a una *c*, lo hará mediante una petición a *b*; *C* entonces no sabrá que la petición procedió originalmente de *a*. Su finalidad más habitual es la de servidor proxy, que sirve para permitir el acceso a Internet a todos los equipos de una organización cuando sólo se puede disponer de un único equipo conectado, esto es, una única dirección IP[1].

Server: Es un equipo de la red que permite ejecutar determinados servicios y acceder a ellos desde otros equipos de la misma red.

[1] Definición tomada de Wikipedia, La enciclopedia Libre, http://es.wikipedia.org

Spoofing: Hace referencia al uso de técnicas de suplantación de identidad generalmente con usos maliciosos o de investigación[1].

Stateful Packet Inspection (SPI): Es el procedimiento empleado por firewalls para analizar los paquetes que transitan a través de él. Mediante este procedimiento se identifican cuales son los paquetes legítimos que transitan por la red, bajo diferentes tipos de conexión.

Troyano: Se denomina troyano a un software malicioso que se presenta al usuario como un programa aparentemente legítimo e inofensivo pero al ejecutarlo ocasiona daños[1].

Virus: Es un malware que tiene por objeto alterar el normal funcionamiento de la computadora sin el permiso o el conocimiento del usuario. Los virus, habitualmente, reemplazan archivos ejecutables por otros infectados con el código de este[1].

VPN: es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada, como por ejemplo Internet[1].

Workstation: Es una computadora que facilita a los usuarios el acceso a los servidores y periféricos de la red[1].

[1] Definición tomada de Wikipedia, La enciclopedia Libre, http://es.wikipedia.org

RESUMEN

En este documento se trata el tema de la seguridad en las redes informáticas explicando en detalle en qué consisten los firewalls y las VPN, además, se analiza el comportamiento de dichos elementos frente al tráfico de datos mediante simulaciones en el programa OPNET.

INTRODUCCIÓN

En la actualidad, la "INTERNET" es el "corazón" de las comunicaciones globales, esta consiste en una interconexión de redes a nivel mundial a través de las cuales se transmiten datos, archivos multimedia, se comparte información y se corren distintas clases de aplicaciones. Uno de los principales beneficios de internet es su condición de ser útil para toda clase de personas, ya sean usuarios comunes, entidades, empresas o expertos/administradores de red; cada uno de los anteriores le encuentra importancia a internet según la utilidad que representa para cada uno de ellos, por ejemplo:

a. El usuario común utiliza internet para estar conectado con muchas personas alrededor del mundo, compartir recursos, recibir correos, hacer consultas, estudiar, escuchar música, videos, para el ocio, etc.
b. Las entidades o empresas utilizan internet para comunicarse con clientes, proveedores, contratistas y además, recibir órdenes de compra, solicitudes de cotizaciones, hacer pedidos, recibir pagos en línea y en general, para optimizar su modelo administrativo. Cabe resaltar que las empresas también utilizan redes de comunicaciones privadas mediante las cuales optimizan su cadena de producción y las comunicaciones en general.
c. Los expertos y administradores de red, utilizad el internet como medio de trabajo, esto son los que crean páginas de internet, administran el manejo de los recursos de la red, aseguran la efectividad de las conexiones físicas y lógicas, prestan asistencia remota, entre otras actividades.

Si bien son muchas las utilidades de internet, sus inconveniencias pueden ser muchas si no se controla la forma de usarlo, ejemplos de esto serían los virus, los

robos por internet o las pérdidas de información importante, en consecuencia con lo anterior el tema de la seguridad de la información surge como tópico de vital importancia en todas las aplicaciones basadas en el manejo de información a través de las redes de comunicaciones.

Es importante saber que nuestros computadores son vulnerables a accesos no autorizados siempre que se trabaje "en red", sin embargo, con el avance de la tecnología, cada vez se hacen más estrictas las políticas de seguridad de la información y con ello, se hacen más robustos los sistemas operativos que controlan nuestros equipos y se emplean mejores dispositivos dedicados a la seguridad de la información, como son los Firewall.

Además de lo anterior, en los últimos años, se ha vuelto muy frecuente emplear redes privadas virtuales (VPN) para la transmisión segura de datos sobre redes públicas, estas se basan en las redes físicas para "construir redes virtuales" que permiten transmitir datos de manera segura.

En este documento, se tratará el tema de la seguridad de la información sobre redes de comunicaciones, explicando el concepto y funcionamiento de los FIREWALL y las VPN, estos dos elementos serán descritos detalladamente y además, se analizará su comportamiento frente al tráfico de datos mediante simulaciones realizadas empleando el programa OPNET.

1. JUSTIFICACIÓN

Para justificar la importancia de tener seguridad en las redes de comunicación, se hará una analogía con el sistema de tráfico vehicular:

En toda ciudad existen normas y políticas bajo las cuales se debe regir todo ciudadano, estas políticas son comúnmente conocidas y actualizadas de tal manera que pueda existir una convivencia organizada y justa, un ejemplo de lo anterior es el código de tránsito y transporte, el cual contempla las políticas y conductas apropiadas para desplazarnos en nuestros vehículos a través de la ciudad fluidamente, sin embargo, a diario podemos apreciar que las normas contempladas en dicho código son violadas constantemente y por ello, surge la necesidad de que existan los agentes de tránsito para velar por el cumplimiento del código, ya sea penalizando o inmovilizando los vehículos de los conductores que infrinjan la ley.

Un FIREWALL, en las redes de comunicaciones es tan importante como un agente de tránsito para la ciudad, los vehículos se pueden comparar con los datos a transmitir y el firewall se encarga de revisarlos, dejarlos pasar o inmovilizarlos (descartarlos). Por otra parte, una VPN se puede comparar con las vías de un sistema de transporte dedicado dentro de la ciudad, tal como el sistema de Transmilenio en Bogotá/Colombia, este sistema se encuentra dentro de la ciudad pero cuenta con vías dedicadas para su circulación y solo hace paradas en las estaciones que le correspondan, así mismo, una VPN se encuentra dentro de una red pública pero es virtualmente una red privada y solo permite la conexión de los usuarios de dicha red.

Por todo lo anterior, las políticas de transito son a la ciudad como las políticas de manejo de firewalls y VPN a las telecomunicaciones, ambas son necesarias para sostener sistemas de transporte y por ende deben ser conocidas especialmente por personas interesadas en el "transporte" y las telecomunicaciones.

2. PLANTEAMIENTO DEL PROBLEMA

Las redes de comunicación publicas tales como internet, son cruciales al momento de compartir información y de agilizar la comunicación entre personas y empresas de todo el mundo, sin embargo, si no se tienen en cuenta las debidas precauciones, estas redes pueden servir para que usuarios no autorizados tengan acceso a información importante contenida en nuestros equipos y por ende pongan en riesgo la integridad de dicha información.

Casos como el de los bancos, en los que una falla en seguridad de la información puede repercutir en pérdidas exorbitantes de dinero, o como el de grandes compañías, en cuyas bases de datos reposan registros de procesos y estados financieros, son evidencias claras de la importancia de tener mecanismos de seguridad de información.

Cabe resaltar que existen muchos expertos en informática dedicados a desarrollar amenazas cibernéticas (Virus), estos son los llamados hackers, no obstante, los Firewall y las VPN juegan un papel importante en repeler las amenazas generadas por dichos virus y por ello, los administradores de la red deben estar al tanto de las amenazas y de descubrir los puntos débiles de sus sistemas de seguridad para poder generar sistemas más seguros, en otras palabras, entendiendo el funcionamiento de los firewalls y las VPN’s se logra evolucionar en torno a la seguridad de la información.

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Estudiar el funcionamiento de los FIREWALL y de las VPN (Virtual Private Networks) mediante simulaciones en el sistema OPNET, para entender y especificar de qué manera proveen seguridad dichos elementos a las redes de comunicaciones.

3.2 OBJETIVOS ESPECÍFICOS

- Simular redes con firewall y obtener graficas del comportamiento de estos frente al tráfico de datos en internet, para especificar el alcance que tienen estos elementos al brindarle seguridad a las redes.

- Crear un entorno en el que se utilicen firewall integrados con VPN, para determinar la relación que tienen dichos elementos con la seguridad informática.

- Describir las funcionalidades del sistema OPNET para poder aprovechar al máximo dicha herramienta en simulaciones de redes de comunicación.

4. MARCO TEÓRICO

A continuación, se describe el significado y los aspectos importantes de los Firewall, las VPN y el sistema OPNET, además, se mostraran tablas y gráficos que permiten tener una mejor concepción de los anteriores elementos.

4.1 FIREWALL

Un firewall es un sistema que permite ejercer políticas de control de acceso entre dos redes, una de ella puede ser una red privada como una LAN y una red pública como lo es Internet. Los firewalls permiten definir los servicios a los que se pueden acceder desde el interior de la red (LAN) hacia el exterior (Internet) y viceversa, por lo que siempre su configuración se encontrará ligada a las políticas de seguridad de la red. Para ilustrar esta definición podemos observar la Figura 1.

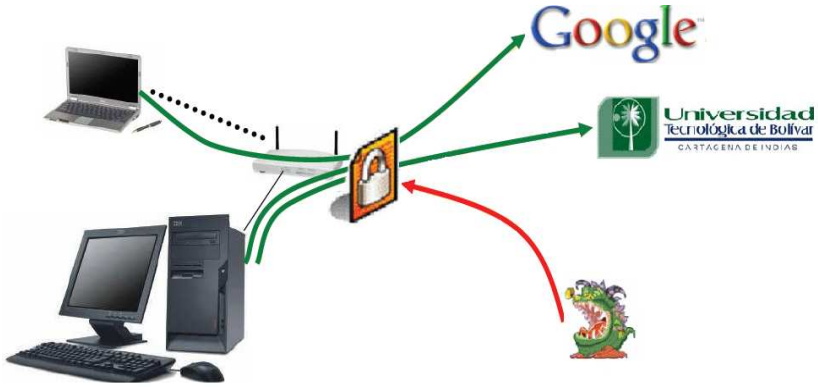

Ilustración 1: Esquema de Funcionamiento General del Firewall

"Un firewall constituye más que una puerta cerrada con llave al frente de su red, es su servicio de seguridad particular" [5]

[5] 3COM, Corporation, Seguridad de redes: Una guía para implementar Firewalls [En linea] http://salaam.cs.buap.mx/EBOOKS/SEGURIDAD/SS3_Firewall_WP_Span.pdf

4.1.1 OBJETIVO BÁSICO DE UN FIREWALL

El propósito de implementar en las redes un firewall, es proteger y mantener segura la información de la red permitiendo:

- Filtrado del tráfico de salida, con el fin de restringir el uso de Internet y el acceso a localidades remotas no deseadas.
- Prohibición del acceso desde Internet a usuarios no autorizados.
- Bloqueo de datos entrantes que pueden contener el ataque de un "hacker".
- Servicio Network Address Translator (NAT), el cual permite realizar la "traducción" de las direcciónes IP, interpretando y convirtiendo en tiempo real las direcciones utilizadas por los paquetes transmitidos.
- Dividir la red en zonas con distintas necesidades de seguridad.

En términos generales si usamos firewalls para acceder a Internet, éste podrá examinar los datos a transmitir y decidir si son seguros o si necesitan ser retransmitidos a su destinatario.

Al implementar los firewall en una red como sistema de protección es importante tener en cuenta contra que pueden proteger y contra que no, tal diferencia puede ser apreciada en la siguiente tabla.

Tabla 1: Contra que protege o no protege un firewall.

Contra Que Protege Un Firewall	Contra Que "NO" Protege Un Firewall
Contra accesos no autenticados del exterior.	Contra accesos externos que no van por el cortafuegos.
Contra tráfico no autorizado del exterior.	Contra ataques desde el interior.
Contra virus y troyanos.	Contra virus, troyanos introducidos mediante "túneles".
Proteger contra "logins" interactivos sin autorización expresa, desde cualquier parte del mundo.	Contra salida de información por otro medio (CD, USB, DVD, etc.)

Una de las razones por las que se plantea que los firewall protegen y no protegen de los virus, es debido a que hay demasiados modos de codificación binaria de ficheros para transmitirlos a través de la red y también son demasiadas las diferentes arquitecturas y virus que intentan introducirse en ellas. En el tema de los virus, la mayor responsabilidad recae casi siempre en los usuarios de la red, los cuales deben tener un gran control sobre los programas que ejecutan y donde se ejecutan.

4.1.2 CARACTERÍSTICAS BÁSICAS DE FIREWALL

Teniendo en cuenta los diversos beneficios que nos brinda la implementación de firewall, estos poseen diversas características para llevar a cabo un buen diseño tales como:

- Control de servicio: establece los servicios de internet que pueden ser permitidos desde el interior de la red a afuera de la misma.
- Control de dirección: establece las direcciones por las que se pueden circular un servicio en particular.
- Control de usuario: se establecen accesos a usuarios de acuerdo a los servicios.
- Control de comportamiento: se establecen controles sobre el uso particular de cada servicio.

4.1.3 AMENAZAS COMBATIDAS POR LOS FIREWALL

Es importante tener en cuenta la naturaleza de los diversos tipos de amenazas que existen contra la seguridad de las redes, para poder escoger el tipo de firewall ideal para combatirlas. Existen tres tipos de ataques que pueden potencialmente impactar en forma negativa los equipos de la red:

- Hurto de información: Robo de información confidencial, tal como registros de clientes, empleados o elementos de propiedad intelectual.
- Sabotaje de información: Cambios a la información, en un intento de dañar la reputación de una persona o empresa, como por ejemplo publicando contenido malintencionado en su sitio Web.

- Negación de servicio (DoS, Denial of Service): Bloqueo de los servidores o red de su empresa, de forma que los usuarios legítimos no puedan acceder a la información o que se impida la operación normal de su empresa.

4.1.4 TIPOS DE FIREWALL

Existen varias formas en que se pueden clasificar los firewall:

a) Conceptualmente, existen dos tipos de firewalls, los de nivel de red y los de nivel de aplicación:

   - Nivel de red: este tipo de firewall, toma las decisiones basándose en la fuente, dirección de destino y puertos, todo ello en paquetes individuales IP.

   - Nivel de aplicación: son generalmente hosts que corren bajo servidores proxy, que no permiten tráfico directo entre redes y que realizan "logines" elaborados y auditan el tráfico que pasa a través de ellas

b) Según la Asociación Internacional de Seguridad de Computadoras (ICSA) los firewalls se clasifican en tres categorías:

   - Firewalls de filtración de paquetes: este firewall verifica la dirección IP de donde proviene el tráfico de datos entrantes y rechaza cualquier tráfico que no coincida con la lista de las direcciones IP que conoce como confiables, implementando reglas para negar el acceso según la información contenida en el paquete, por ejemplo: el número del puerto TCP/IP, la dirección IP de la fuente/origen o el tipo de datos. Las restricciones pueden ser tan estrictas o tan flexibles como se requiera. Los router comúnes que se usan en una red pueden realizar un filtrado al tráfico entrante por dirección IP, pero los denominados "hackers" se valen de trucos "spoofing", con los cueles pueden hacer parecer a los datos que provienen de fuentes malignas

como confiables. Desafortunadamente, el firewall de filtración de paquetes es propenso al "spoofing" de IP y son muy difíciles de configurar. Cualquier error en su configuración, puede dejarlo vulnerable a los ataques.

- Servidores proxy a nivel de aplicación: los servidores proxy examinan las aplicaciones usadas por cada paquete IP, con el fin de verificar su autenticidad. El tráfico de cada aplicación, tales como HTTP y FTP, requieren de la instalación y configuración de un proxy de aplicaciones diferente. Con frecuencia, los servidores requieren que los administradores reconfiguren su red y aplicaciones para soportar el proxy, lo cual puede resultar en un proceso muy trabajoso.

- Firewalls de inspección de paquetes (SPI, Stateful Packet Inspection): considerado como la última generación en la tecnología de firewall, los SPI examinan todos y cada uno de los componentes de un paquete IP para decidir si estos son aceptados o rechazados. Este firewall mantiene un registro de todas las solicitudes de información que se originan de la red, para luego inspeccionar todas comunicaciones entrantes y verificar si realmente fueron solicitadas, de tal manera que se rechace cualquiera que no lo haya sido. Los datos solicitados aprobados proceden al siguiente nivel de inspección y el software determina el estado de cada paquete de datos. Además, se realizan filtrados en base a las cabeceras, así el paquete se intercepta a nivel de red, pero se extrae información de los datos para analizarlos en función de la aplicación, manteniendo una tabla dinámica de estados con información para las decisiones de seguridad.

c) Según el tipo de ubicación, se pueden diferenciar los siguientes:

- Firewall personales (PC): Protegen el PC controlando el stackIP e inspeccionando las aplicaciones más comunes. Permiten filtros de entrada y salida, utilizables en PC en LAN, Modems o ADSL.

- Firewall para pequeñas oficinas: SmallOffice HomeOffice (SOHO): Protegen a varios usuarios en pequeñas oficinas (típicamente entre 2 y 50) Suelen ser pequeños equipos instalados antes del router o incluso integrados.

- Equipo hardware específico (Appliances): Utilizados en oficinas medias y sucursales, fáciles de configurar, con funcionalidades básicas y gestionados centralizadamente, utilizan sistemas operativos propios del hardware en el que están implantados.

- Cortafuego corporativo: El punto central de accesos a Internet de una empresa, donde se implanta la política de seguridad de la empresa, puede conectar múltiples redes. Software que se instala en grandes servidores con configuraciones tolerantes a fallos.

4.1.5 FUNCIONES ADICIONALES DE LOS FIREWALL

Los firewall además de sus características generales poseen funciones adicionales, entre estas figuran:

- Firewalls con zona desmilitarizada (DMZ): estos firewall son considerados como una solución efectiva para empresas que ofrecen la posibilidad de conectarse a su red a partir de cualquier medio externo, ya sea a través de Internet o cualquier otra ruta. La decisión de optar por un firewall con DMZ debe basarse en la cantidad de usuarios externos que acceden a la red y la frecuencia con la que lo hacen. Los firewalls con DMZ crean áreas de

información protegida consideradas como zona "desmilitarizada" en la red, en donde los usuarios externos pueden ingresar al área protegida, pero no pueden acceder al resto de la red, lo cual permite a los usuarios externos acceder a la información que usted quiere que vean y previene que ellos obtengan información no autorizada.

- Filtración de contenido: filtro de contenido o también conocido como filtro de sitios Web, extiende las capacidades del firewall para bloquear el acceso a ciertos sitios Web. Esta funcionalidad le permite definir categorías de material inadecuado y obtener un servicio que lista miles de sitios Web que incluyen dicho tipo de material. Como siguiente paso, puede escoger si quiere bloquear totalmente el acceso a estos sitios o permitir su uso, pero manteniendo un registro del mismo. Tal servicio debe actualizar automática y regularmente la lista de sitios Web que no pueden ser accedidos.

- Redes Privadas Virtuales (VPN): Una VPN es una red privada de datos que utiliza la infraestructura de la red pública (Internet) permitiendo a empresas obtener las mismas capacidades como si se implementaran líneas telefónicas privadas; las VPN permiten compartir recursos públicos en forma segura, usando técnicas de encriptación que garantizan que solamente los usuarios autorizados puedan ver o entrar en la red privada de la empresa.

- Protección a través de antivirus: es importante tener en cuenta que los firewalls no están diseñados para remover o limpiar virus, pero estos si pueden ayudar a detectarlos, estos virus con una amenaza constante y pueden dañar rápidamente toda una red si inadvertidamente, bajan material desconocido o diseminan virus peligrosos en las redes. Un servidor de acceso remoto o una PC con un módem puede servir como puerta de acceso a la red, el cual puede burlar las medidas de seguridad del firewall.

Lo mismo puede ocurrir cuando un empleado introduce un diskette infectado con un virus en su PC. El lugar más apropiado para instalar el software antivirus es en la PC de cada usuario

4.2 VIRTUAL PRIVATE NETWORKS (VPN's)

Una VPN (Virtual Private Network) o red privada virtual no es más que la interconexión de varias redes locales (LAN, Local Area Network) que están separadas físicamente pero realizan un intercambio de datos mediante un túnel o conducto dedicado de un sitio a otro a ser través de Internet, permitiendo que estas se comporten como si se trataran de una única red local, para una mejor percepción, véase la siguiente figura:

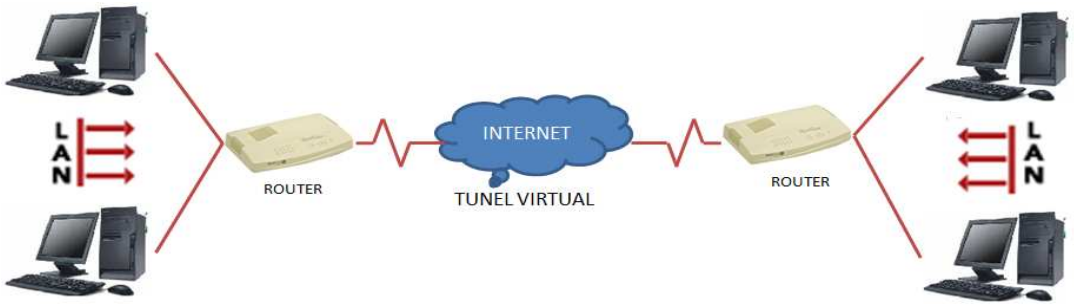

Ilustración 2: Esquema general de una VPN

Para que el tránsito de información sea seguro a través del túnel "tunnelling", el sistema de red VPN actúa a través de dos mecanismos simultáneos:

1. Certificación: Cada uno de los gateways o proxy que pretendan unirse a la VPN debe garantizar de alguna forma que está autorizado. Esto se hace a través de algún mecanismo de firma digital, normalmente a través de una autoridad de certificación, que suelen ser doble, incluye un elemento electrónico y un número de identificación personal o PIN, reduciendo

drásticamente el problema de que alguien pueda falsear una identidad para entrar al sistema, puesto que debe poseer ambos elementos.

2. Encriptación: Una vez dentro de la VPN, cada uno de los gateways envían su clave pública a todos los demás gateways pertenecientes al sistema. Con el uso de sistemas de encriptación simétricos, de clave pública y clave privada, la información se encripta matemáticamente de tal forma que es extremadamente complejo desencriptar la información sin poseer las claves. Existe un proceso de gestión de dichas claves (Key management) que se encarga de su distribución, su refresco cada cierto tiempo, y revocarlas cuando sea necesario hacerlo. Se ha de conseguir un balance entre los intervalos de intercambio de las claves y la cantidad de información que se transfiere: Un intervalo demasiado corto sobrecargaría los servidores de la VPN con la generación de claves, mientras que uno excesivamente largo podría comprometer la clave y la información que esta protege.[6]

4.2.1 COMO FUNCIONA UNA VPN

Los paquetes de datos de una VPN viajan por medio de un túnel virtual "tunnelling", que está definido en la red pública (internet), por el cual se establece una conexión dedicada entre dos puntos; para obtener esta conexión dedicada se hace necesario un protocolo de encapsulamiento para cada paquete que incluya los campos de control necesarios para crear, gestionar y deshacer "el túnel", por lo tanto, los paquetes deben realizar un proceso consecutivo que incluye los estados de encriptado, cifrado, autenticación, transito y descifrado como se muestra a continuación:

[6] Redes Privadas Virtuales, VPN - Redes Privadas Virtuales, Jose Luis Ruiz González, Marzo 2002

1. Proceso de encriptado y cifrado de los paquetes: La encriptación es la forma cómo se codifica la información para que esta sea difícil e imposible de leer, y el cifrado es la forma en cómo se decodifica la información para ser leída nuevamente; la información que se encuentra codificada se denomina texto cifrado y la información sin codificar texto claro. Un ejemplo de esto se muestra en la siguiente figura, en donde el Gateway de origen encripta la información en texto cifrado antes de enviarlo, mientras que el Gateway receptor desencripta la información, es decir texto claro, para luego ser enviado a la LAN.

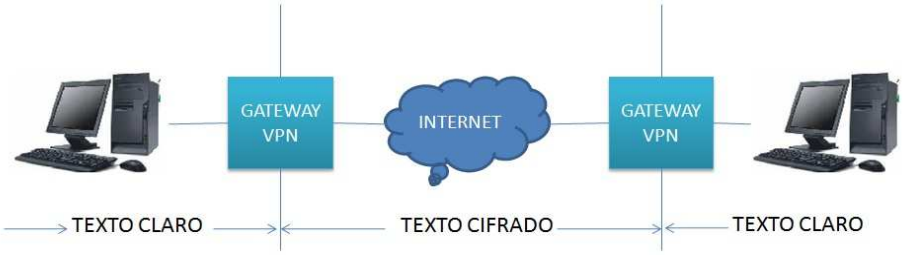

Ilustración 3: Cifrado de VPN

2. Proceso de autenticación, el cual nos permite obtener la identidad de todos los participantes de la VPN garantizando que estos posean las autorizaciones para establecer las conexiones.

3. Proceso de encapsulamiento de las paquetes IP, para lo cual es necesario la implementación de protocolos especial como PPTP, L2TP e IPSEC, entre otros.

4. Los paquetes transitan por el túnel.

5. Los paquetes son descifrados en su destino.

4.2.2 TIPOS DE VPN

Para diferenciar los tipos de VPN, se han clasificado en tres categorías, estas son: VPN de acceso remoto, de intranet y de extranet. A continuación se explica cada una de ellas:

1. VPN de Acceso Remoto

   Este tipo de VPN es implementada para establecer una conexión entre usuarios remotos o móviles y la intranet. Los usuarios remotos son quienes generalmente no poseen un sito de trabajo estático y necesitan tener un acceso directo a los servicios de una red interna desde lugares distantes. La siguiente figura muestra este tipo de conexión.

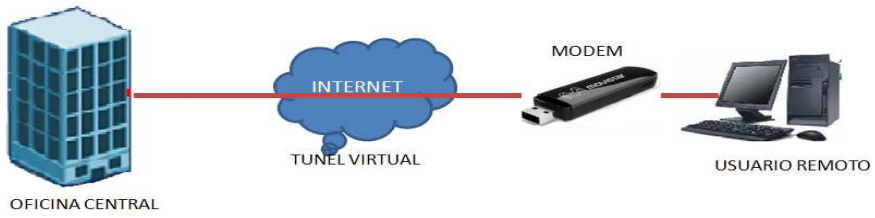

Ilustración 4: VPN de Acceso Remoto

   Por lo general este tipo de VPN proporciona el acceso a través de una red pública teniendo en cuenta las mismas políticas de la red privada, manteniendo la seguridad correspondiente y aplicando las técnicas de cifrado, encriptación instaladas en la maquina del cliente.

2. VPN de Intranet

   Este tipo de VPN permite conectar localidades fijas a la red corporativa usando conexiones dedicadas, permitiendo conectar una oficina central con sucursales remotas estableciendo un canal lógico que permite ver a ambas

como si estas fueran una sola; este tipo de VPN se conoce como conexión LAN-LAN o punto-punto. La siguiente figura muestra este tipo de conexión.

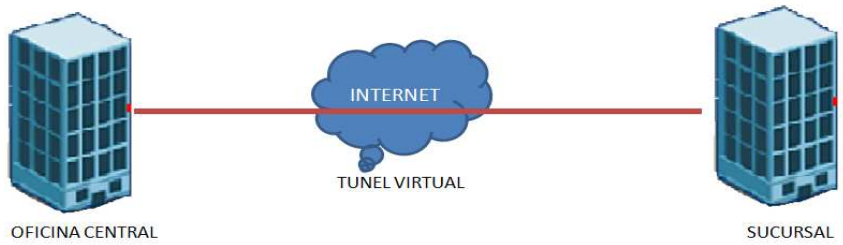

Ilustración 5: VPN de Intranet.

3. <u>VPN de Extranet</u>

   Este tipo de VPN es creado entre los proveedores o clientes con una empresa, proporcionando un acceso limitado de los recursos de la empresa a los clientes y proveedores, es decir, se crea un acceso de información común para todos a través de una estructura pública.

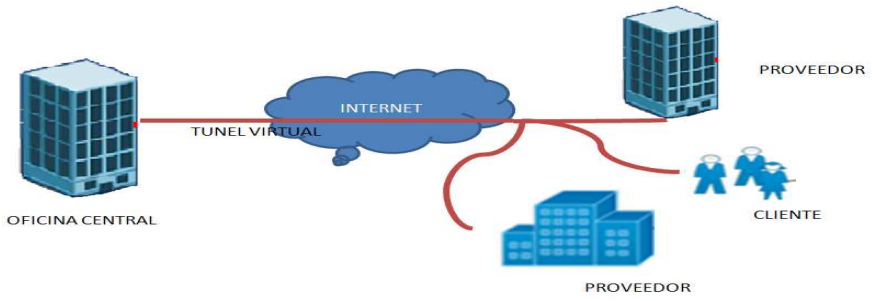

Ilustración 6: VPN de Extranet

4.2.3 PROTOCOLOS DE VPN

Los siguientes protocolos son los más usados en las conexiones de redes virtuales:

- PPTP (Point-to-Point Tunneling Protocol)

  Este es un protocolo desarrollado por Microsoft, que permite mantener un seguro intercambio de datos entre los clientes y un servidor local de una red privada, encapsulando los paquetes PPP (point-to-point-protocol) en datagramas IP para su transmisión bajo redes basadas en TCP/IP, es decir, TCP mantiene el control de la conexión a la red privada, entre el equipo remoto y el servidor del túnel e IP mantiene el funcionamiento del túnel entre el equipo remoto y el servidor de túneles.

- L2TP (Layer Two Tunnelig Protocol)

  Esta es una extensión del protocolo PPTP (Point-to-Point Protocol), mezclado con L2F de Cisco, usado para conectar redes VPN a través de Internet de manera segura. Este cuenta principalmente de un LAC (Access Concentrator), que es el dispositivo que físicamente termina una llamada y un LNS (NetworkServer), que es el dispositivo que autentifica y termina el enlace PPP. L2TP implementa redes conmutadas de paquetes para hacer posible que los extremos de la conexión estén ubicados en distintas computadoras. El usuario tiene una conexión L2 al LAC, el cual crea el túnel de paquetes PPP, así los paquetes pueden ser procesados en el otro extremo de la conexión o bien, terminar la conexión desde un extremo. El proceso de tunneling involucra tres protocolos diferentes: el protocolo pasajero representa el protocolo de nivel superior que debe encapsularse (IP); el protocolo encapsulador indica el protocolo que será empleado para la creación, mantenimiento y destrucción del túnel de comunicación (L2F), y

el protocolo portador será el encargado de realizar el transporte de todo el conjunto (PPP).[7]

- IPSEC (Internet Protocol security)

  Este es un protocolo que permite establecer sesiones seguras entre dos hosts comunicados a través de IP, proporcionando encriptación a nivel de la capa de red; con él se definen nuevos formatos de paquete que son, la Cabecera de autentificación (AH) la y el ESP (Encapsulating Security Payload). Por un lado, AH protege la integridad y autenticidad de los datos, incluyendo los campos invariantes de la cabecera IP; esta cabecera no proporciona confidencialidad. Por otro lado, ESP protege tanto la confidencialidad como la integridad y la autenticidad de los datos.

[7] guia práctica sobre redes privadas virtuales laurie paillier vasquez karen rocio arzuaga araujo universidad tecnológica de bolívar 2004

4.3 OPNET

OPNET (Optimized Network Egineering Tools), es una herramienta que permite simular, modelar y analizar protocolos a través de diseños de redes de comunicaciones; la plataforma de OPNET fue desarrollada por MIL3 Inc, que es usada para desarrollar nuevos protocolos, optimizar protocolos existentes y estudiar las diferentes topologías existentes en las redes de comunicaciones. OPNET posee librerías que contienen los modelos de protocolos y equipos de comunicaciones más utilizados como los protocolos Ethernet, TCP, UDP, IP, ATMA, Frame Relay y como los equipos de host servidores etc.

En la página WEB http://www.opnet.com se puede encontrar gran cantidad de información relativa al programa, así como también se puede descargar el software. Este es un software registrado y con derechos de autor, por lo tanto tiene un valor comercial, sin embargo, para efectos educativos existe una versión académica la cual será la utilizada para realizar las simulaciones de firewall y VPN.
A continuación se describirán las características básicas del software y de su entorno gráfico para poder usarlo en las simulaciones de firewall y VPN.

4.3.1 COMO DESCARGAR OPNET ACADEMIC EDITION

Para descargar OPNET se debe acceder al siguiente enlace:

http://www.opnet.com/university_program/itguru_academic_edition/

Una vez en la pagina, se debe presionar Register and Download, realizar un proceso de registro con los datos personales y posteriormente se podrá descargar el programa.

4.3.2 COMO INSTALAR OPNET

La instalación de OPNET es realmente sencilla, solo es necesario presionar "NEXT" a las instrucciones que va generando el instalador, sin embargo, es preferible leer todo antes de presionar dicho botón para familiarizarse con los derechos del programa y con el directorio en el cual será instalado.

4.3.3 INTRODUCCIÓN AL ENTORNO GRÁFICO DE OPNET

OPNET consta de un entorno grafico para facilitar las simulaciones de redes, a continuación, se explican los elementos y consideraciones básicas necesarias para poder crear un nuevo proyecto y manejar el programa en general.

Para crear un nuevo proyecto, se realiza un procedimiento consecutivo que depende del proyecto que se quiera desarrollar, sin embargo, los pasos son comúnmente los siguientes:

1) Seleccionar "File", "New…" para generar un nuevo proyecto.

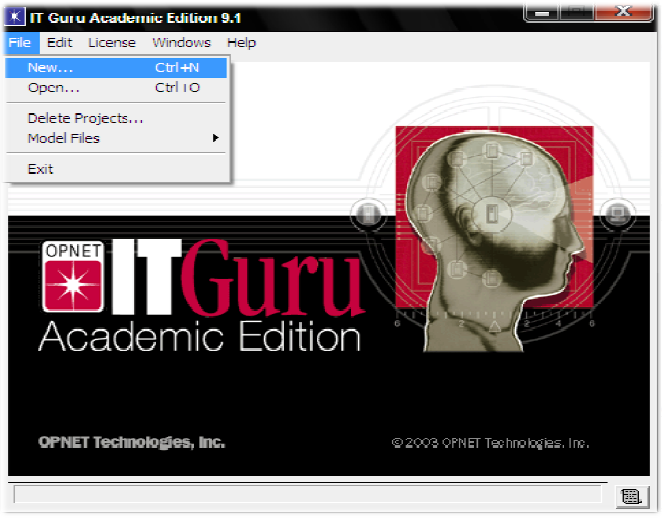

Ilustración 7: Ventana inicial OPNET

2) Dar click en OK para confirmar que se desea un nuevo proyecto.

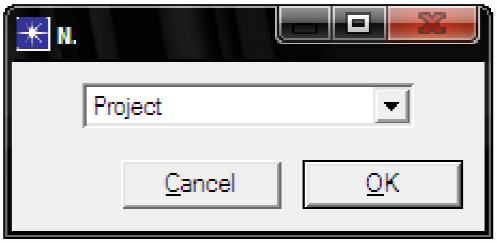

Ilustración 8: Aceptar Proyecto OPNET

3) Escoger nombre del proyecto y del escenario. Nótese que el nombre del proyecto es general y el del escenario es alusivo a la red a diseñar, esto es debido a que en un mismo proyecto se pueden manejar varios escenarios, lo que permite comparar resultados simultáneamente.

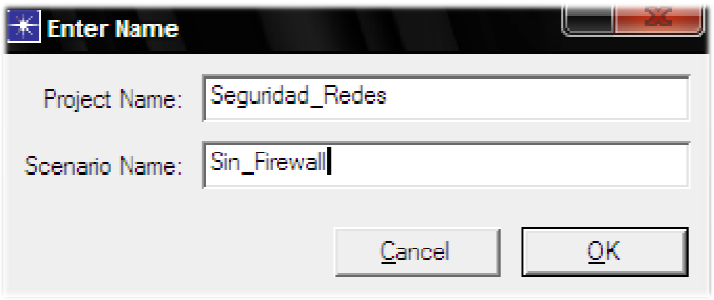

Ilustración 9: Asignar Nombres a Proyecto y escenario OPNET.

4) Dar click en Create Empty Scenario para crear un escenario nuevo y "vacio".

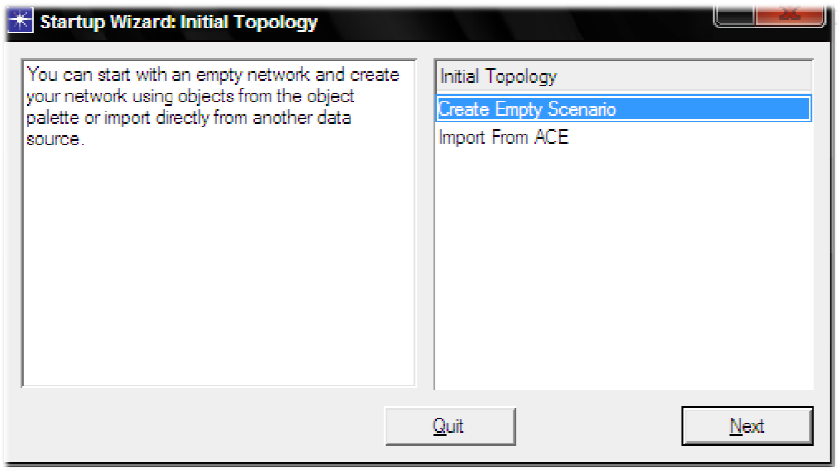

Ilustración 10: Topología del escenario OPNET

5) Escoger la escala de la red y sus dimensiones, para que el fondo del escenario sea conforme con nuestro proyecto. en este ejemplo, escogeremos el fondo "world" y con ello la escala de nuestro proyecto será el mundo.

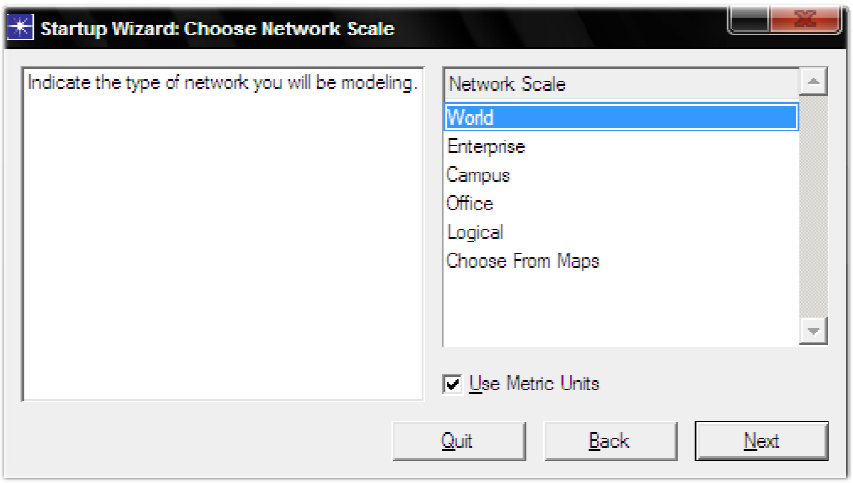

Ilustración 11: Escala de la Red OPNET

6) Escoger una zona geográfica para poner un mapa como fondo de pantalla de nuestro proyecto.

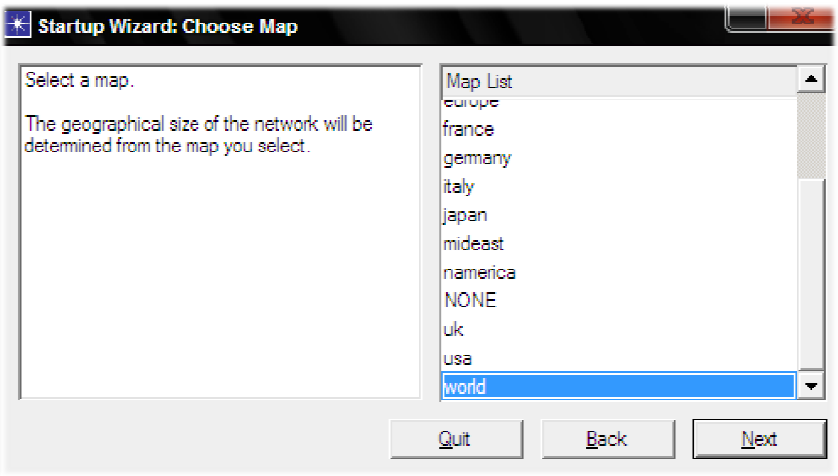

Ilustración 12: Escoger Mapa de Escenario OPNET

7) Escoger el tipo de tecnología a emplear en la red a simular. Esta escogencia depende de la simulación que se desee realizar, en nuestro caso, solo se presiona "Next" para que el programa incluya las que tiene por default.

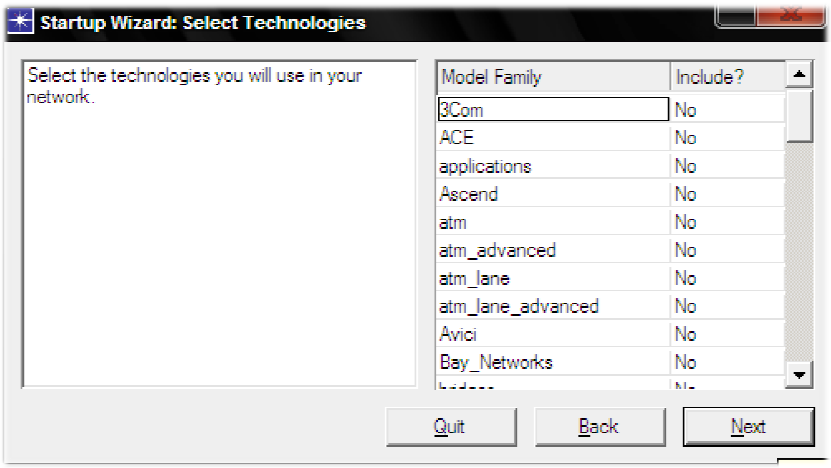

Ilustración 13: Seleccionar Tecnologías de Proyecto OPNET

8) Confirmar los datos seleccionados y pulsar ok.

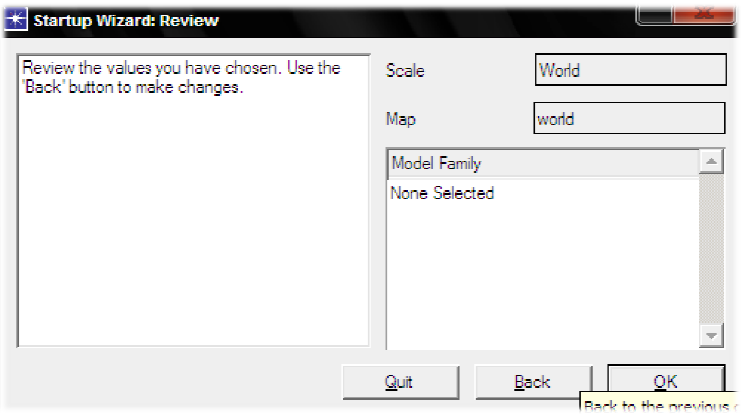

Ilustración 14: Confirmación de Datos de Proyecto OPNET

Una vez creado el nuevo proyecto, deberá aparecer la ventana del escenario:

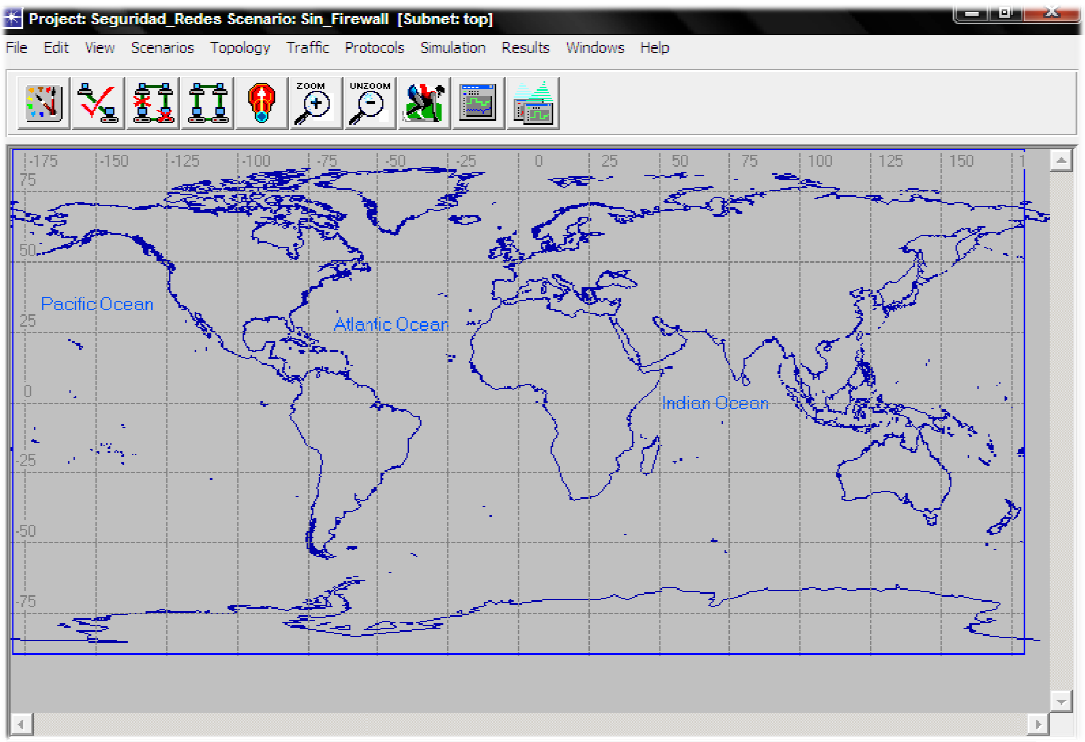

Ilustración 15: Apariencia del Escenario OPNET

En la anterior ventana, se realizan los diseños de la red, para ello, existen los siguientes botones de acción:

a. **b.** **c.** **d.** **e.** **f.** **g.** **h.** **i.** **j.**

Ilustración 16: Botones de acción OPNET

A continuación, se explica la utilidad de los anteriores botones:

a. Permite abrir la "paleta" de objetos, en la cual se encuentran todos los elementos necesarios para realizar simulaciones, tales como routers, Hostos, links etc. Dicha paleta se muestra a continuación.

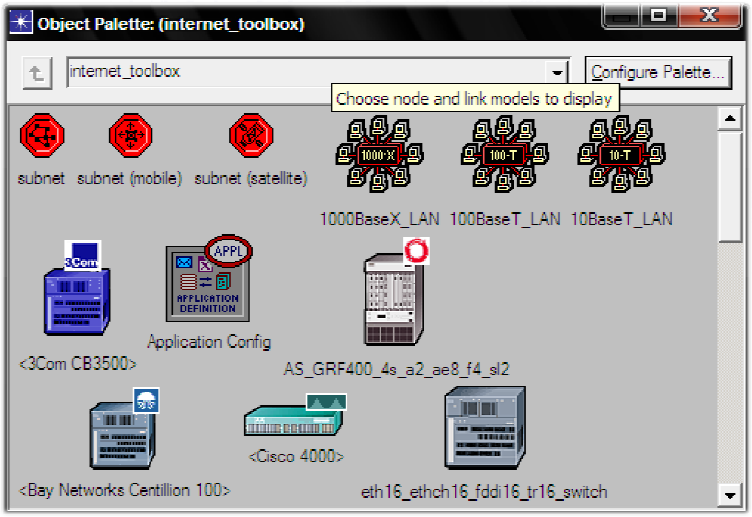

Ilustración 17: Paleta de Objetos OPNET

b. Permite verificar la consistencia de los enlaces de la red.

c. Permite marcar el nodo o enlace seleccionado como fallido.

d. Permite marcar el nodo o enlace seleccionado como recuperado.

e. Permite ir a un nivel superior en la jerarquía de la red.

f. Hacer zoom a determinada área del escenario.

g. Alejar zoom.

h. Permite configurar y correr una simulación.

i. Permite ver los gráficos y tablas de las estadísticas recolectadas.

j. Mostrar o esconder todos los gráficos.

5. METODOLOGÍA

Para estudiar el comportamiento de los Firewal y las VPN, Se realizarán simulaciones mediante tres (3) escenarios en OPNET, el primero sin seguridad, el segundo con firewall y el tercero con VPN, luego se compararán los resultados y se sacaran las respectivas conclusiones. Los escenarios constaran de servidores de información a los cuales se podrá acceder dependiendo de los privilegios del usuario, ya sea en presencia de firewall y VPN o en ausencia de los mismos.

5.1 ELEMENTOS NECESARIOS PARA LAS SIMULACIONES

Para las simulaciones, se deberán escoger de la paleta de objetos los siguientes elementos:

a. **b.** **c.** **d.** **e.** **f.** **g.** **h.**

Ilustración 18: Elementos de las Simulaciones

A continuación se explica la funcionalidad de cada uno de ellos:

- **a.** Application Config: Permite definir las aplicaciones que se tendrán en la red, tales como video conferencia, voz sobre IP, E-mail etc.
- **b.** Profile Config: Permite definir los perfiles que pueden tener los usuarios de la red, tales como comercio electrónico, persona de ventas, investigador, usuario multimedia, etc.
- **c.** ip32_cloud: Permite simular la conectividad a una red extensa de conectividad IP.

d. ppp_wkstn: Es la terminal utilizada por los usuarios, se puede configurar de acuerdo a diferentes privilegios deseados.

e. ppp_server: Permite simular y configurar un servidor de información.

f. ethernet4_slip8_gtwy: Permite simular y configurar la acción de un router.

g. Ip VPN Config: Permite establecer los parámetros de la VPN tales como encriptación y "tunneling".

h. ethernet2_slip8_firewall: Permite simular y configurar un firewall.

Cabe resaltar que para realizar los enlaces entre dichos elementos se emplea un enlace PPP_DS1:

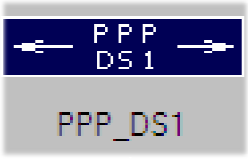

Ilustración 19: Enlace PPP_DS1 en OPNET

Este tipo de enlace permite conectar dos nodos usando el protocolo PPP a una tasa de 1.544 Mbps. Por otra parte, es preciso especificar que los ppp_server y ppp_wkstn soportan el protocolo SPLI (serial line internet protocol) a una tasa de datos ajustable, y los ethernet4_slip8_gtwy representan un Gateway basado en IP que soporta 4 interfaces de Ethernet y 8 interfaces seriales; este router utiliza el protocolo RIP (Routing Information Protocol) o el OSPF (Open Shortest Path First) dinámicamente y genera automáticamente las tablas de ruteo necesarias para un correcto direccionamiento de los datos.

5.2 CREACIÓN DEL ESCENARIO SIN PROTECCIÓN

Se deberá crear un nuevo proyecto tal y como se explica en la sección 4.3.3.1 de este documento; se asignará como nombre del proyecto "Seguridad_Redes" y como nombre del primer escenario "Sin_Firewall". Una vez creado el escenario se puede quitar el fondo de pantalla seleccionando View - Background - Set Border Map - NONE - OK.

Por otra parte, se deberán introducir los elementos que se encuentran en la siguiente tabla:

Tabla 2: Elementos Necesarios para el Escenario Sin Protección

Nombre	Cantidad
Application Config	1
Profile Config	1
ip32_cloud	1
ppp_wkstn	2
ppp_server	1
ethernet4_slip8_gtwy	3
PPP_DS1	6

Dichos elementos se escogen de la paleta de objetos y para ello, se debe hacer click en el objeto, click en el escenario y luego click derecho para deseleccionarlo. Una vez ingresados todos los elementos al proyecto se deberán conectar mediante los enlaces PPP_DS1 y personalizar los nombres de los elementos (click derecho - Set Name) de tal manera que sean nemotécnicos. La conexión debe ser similar a la de la Ilustración 20.

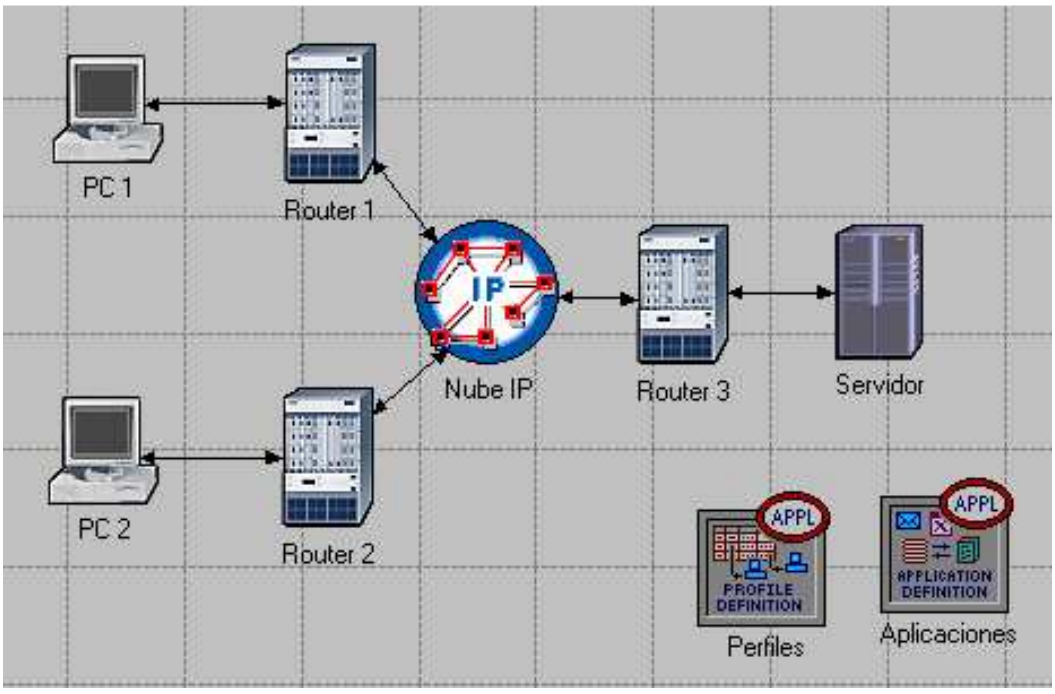

Ilustración 20: diseño de red de Escenario sin Firewall

Se debe proceder entonces a asignarle la configuración adecuada a cada uno de los elementos de la red, es decir, se deberá configurar:

- Aplicaciones
- Perfiles
- Servidor
- Hosts

Para ello se realiza el procedimiento descrito a continuación:

1. Configurar las Aplicaciones: hacer click derecho en Aplicaciónes, seleccionar "Edit atributes", ubicar "Application Definitions" y colocar "Default" como valor de dicho atributo, después presionar OK (Véase Ilustración 21).

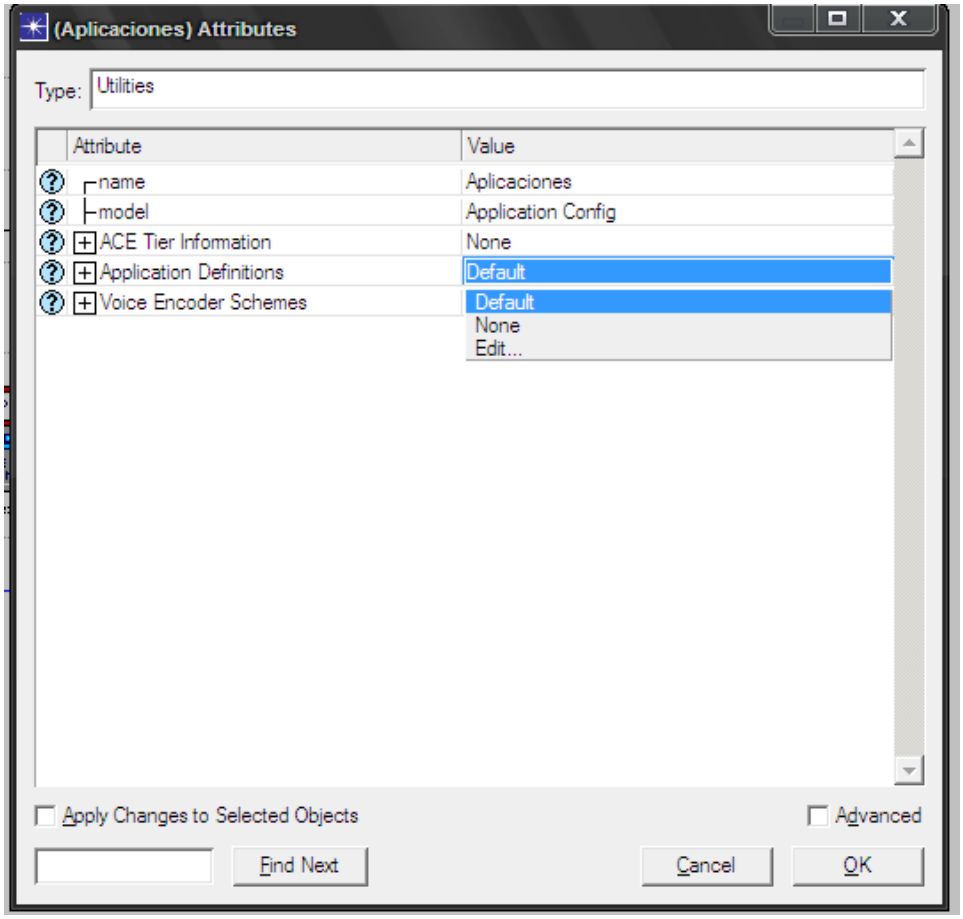

Ilustración 21: Configuración de la Aplicaciones del Proyecto

2. Configurar los Perfiles: hacer click derecho en Perfiles, seleccionar "Edit atributes", ubicar "Profile Configuration" y colocar "Sample Profiles" como valor de dicho atributo, después presionar OK (Véase Ilustración 22).

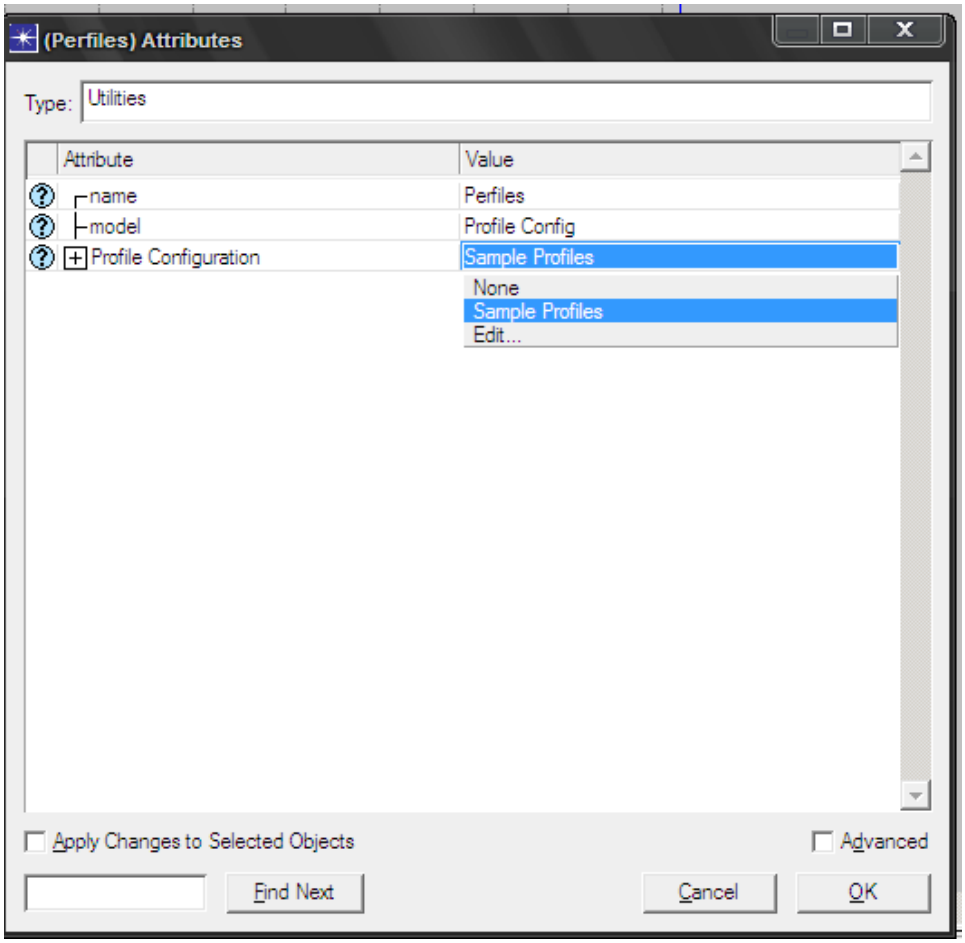

Ilustración 22: Configuración de los Perfiles del Proyecto

3. Configurar el Servidor: hacer click derecho en Perfiles, seleccionar "Edit atributes", ubicar "Application: Supported Services" y colocar "all" como valor de dicho atributo, después presionar OK (Véase Ilustración 23).

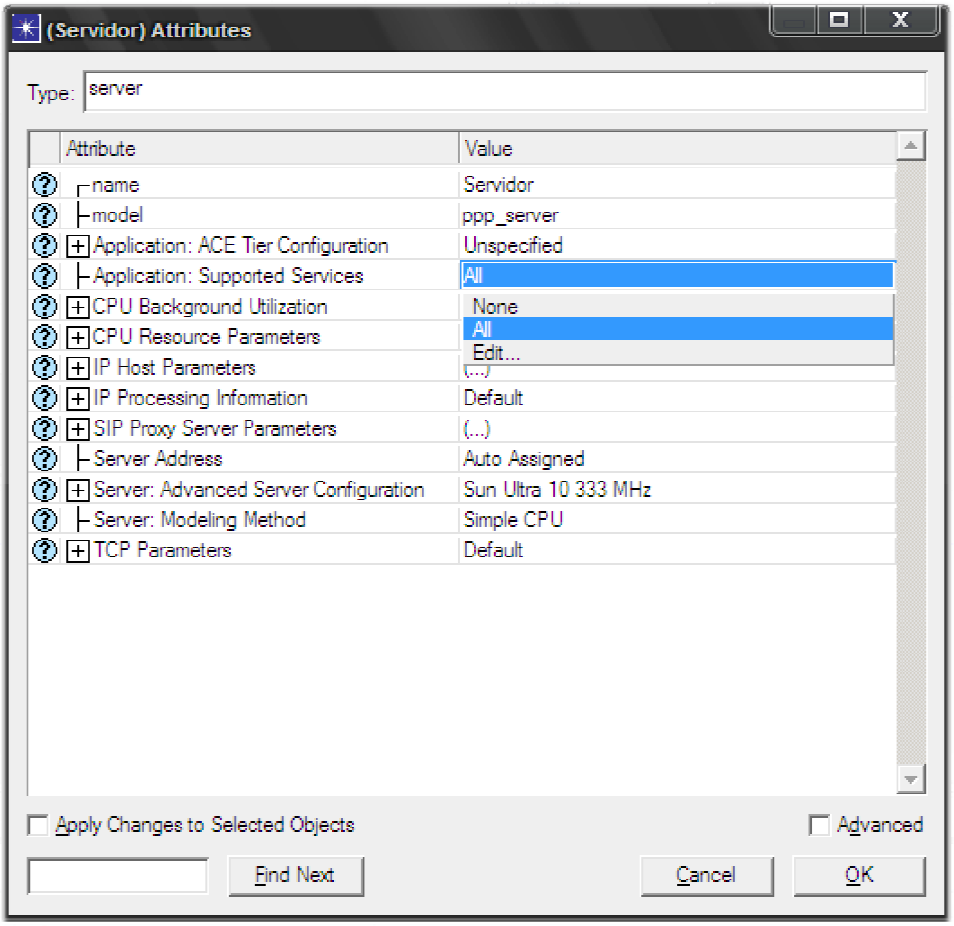

Ilustración 23: Configuración del Servidor de información.

4. Configurar los Hosts (PC): hacer click derecho en PC 1 o PC 2, presionar "Select Similar Nodes", nuevamente hacer click derecho en PC 1 o PC 2, seleccionar "Edit atributes", y realizar lo siguiente (Véase Ilustración 24 y 25):
    a) Marcar la casilla "Apply Changes to Selected Objects".
    b) Expandir el atributo "Application: Supported Profiles", establecer las filas (rows) a 1, se mostrará un nuevo submenú llamado "Row 0".
    c) Expandir "Row 0" y seleccionar el "Profile Name" a "Sales Person".
    d) Presionar OK.

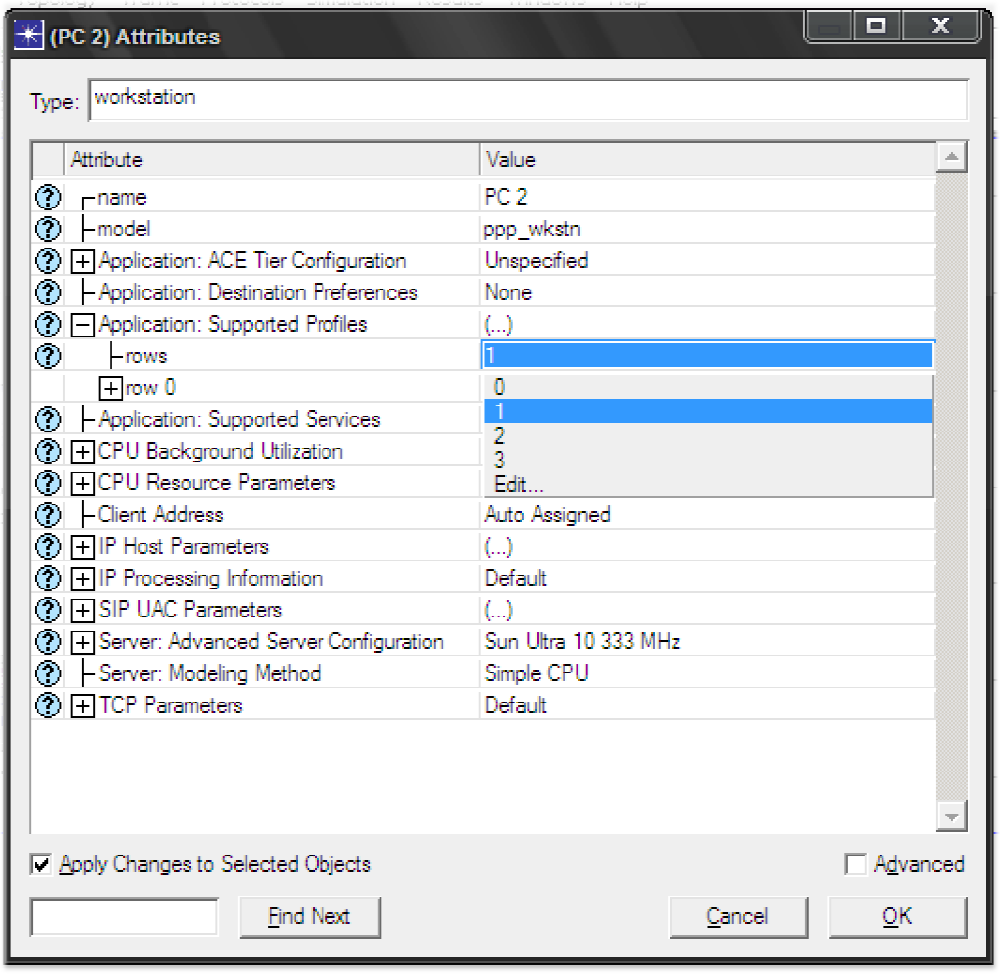

Ilustración 24: Configuración de Hosts 1

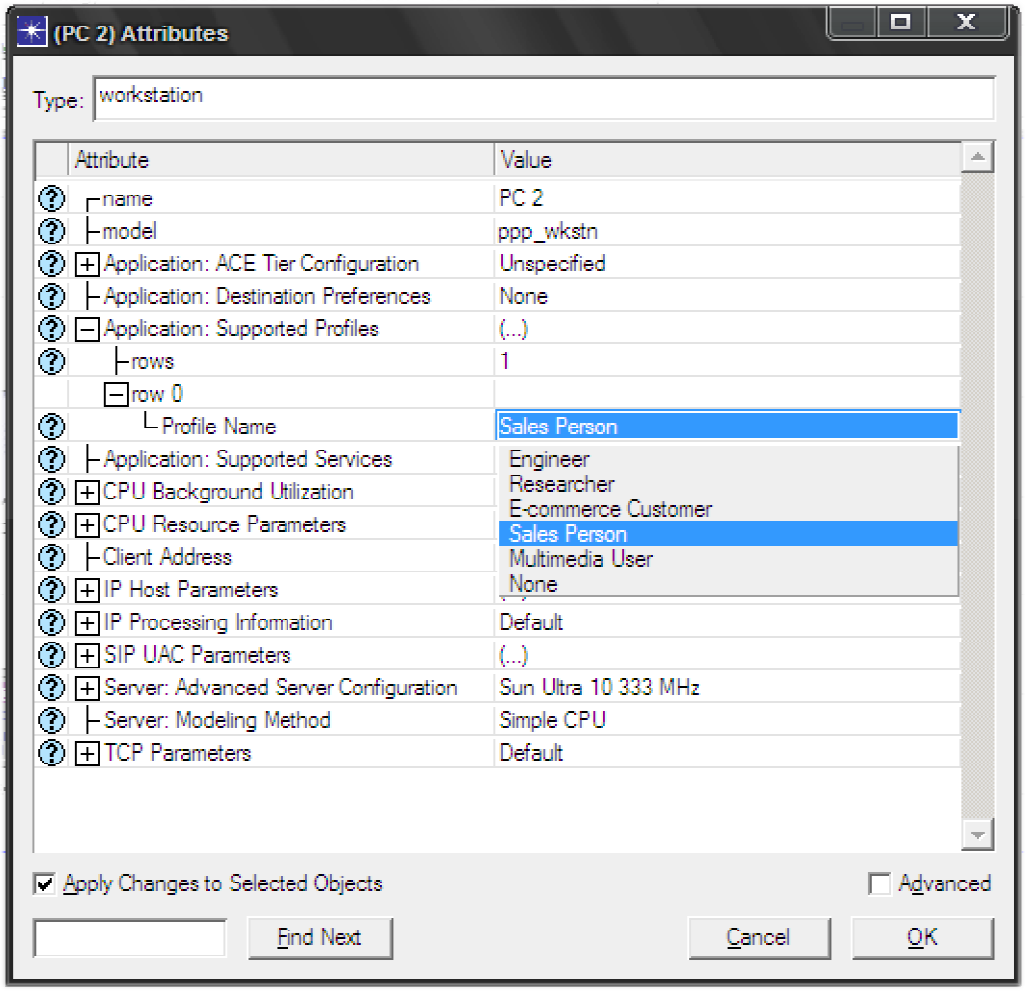

Ilustración 25: Configuración de Hosts 2

Mediante el anterior procedimiento se ha finalizado la configuración del escenario sin protección, es pertinente guardar el proyecto. Nótese que se han configurado los Hosts con el perfil de una persona que trabaje en ventas, con lo cual este podría acceder a aplicaciones del servidor tales como bases de datos, E-mail y explorar la web, esto se especificó en "Profile Configuration".

Por otra parte, para poder realizar simulaciones se debe escoger cuales serían los datos estadísticos a recolectar por el programa, para ello se realiza el siguiente procedimiento:

Click derecho en cualquier parte del escenario y seleccionar "Choose Individual Statistics", se abrirá una ventana llamada "Choose Results" en la que deberá escoger los datos estadísticos globales a ser recolectados, para ello se debe desplegar el menú "Global Statistics" y realizar el siguiente procedimiento:

a) Expandir "DB Query" y habilitar "Response Time (sec)"
b) Expandir "HTTP" y habilitar "Page Response Time (sec)".
c) Presionar OK.

Cabe resaltar que DB Query Response Time (Sec) es en español el tiempo de respuesta de una consulta realizada por una base de datos, en otras palabras es el tiempo que se mide desde que se envía una solicitud al servidor mediante la aplicación de consulta de la base de datos, hasta que se recibe un paquete de respuesta. Por otra parte "HTTP Page Response Time" es el tiempo de respuesta de una página HTTP, es decir, el tiempo requerido para recibir toda la pagina con todos los objetos en línea.

Siguiendo con el procedimiento, se debe hacer click en PC 1, seleccionar "Choose Individual Statistics" y realizar el siguiente procedimiento:

a) Expandir "Client DB" y habilitar "Traffic Recived (bytes/sec)",
b) Expandir "Client HTTP" y habilitar "Traffic Recived (bytes/sec)",
c) Presionar OK y realizar el mismo procedimiento para PC 2.

5.3 CREACIÓN DEL ESCENARIO CON FIREWALL

Un firewall nos permite proteger la información del servidor de cualquier usuario, para ello se debe realizar el siguiente procedimiento (Véase Ilustración 26):

a) Duplicar el escenario sin protección: desplegar el menú "Scenarios", seleccionar "Duplicate Scenario" y asignarle nombre, en este caso se llamará "Con_Firewall", después presionar OK.

b) Introducir el firewall: Click derecho en Router 3, seleccionar "Edit Atributes", ubicar el atriburo "Model" y escoger "ethernet2_slip8_firewall" como valor de dicho atributo.

c) Cambiar el Nombre del elemento (name) a "Firewall".

d) Expandir el atributo "Proxy Server Information", expandir "Row 1", ubicar "Proxy server deployed" y asignar NO como valor de dicho atributo.

e) Presionar OK.

Con la anterior configuración, el firewall no permite el paso de tráfico relacionado a la base de datos que se encuentra en el servidor, por lo tanto, dicha información está protegida de acceso externo. El nuevo escenario debe lucir como la Ilustración 27.

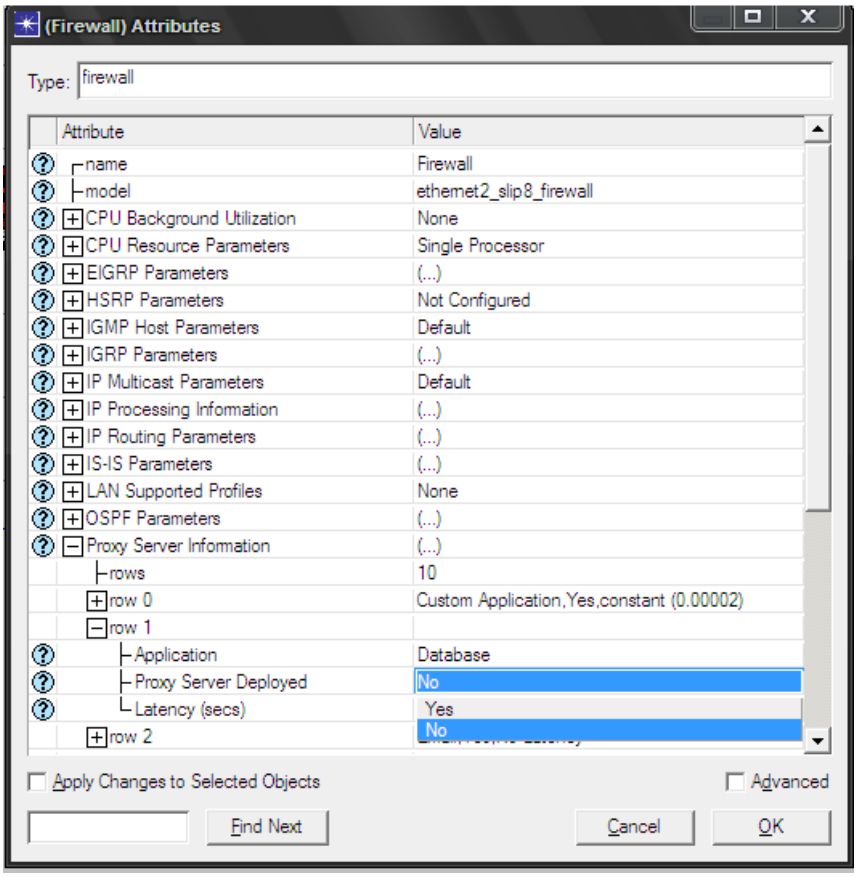

Ilustración 26: Configuración de Firewall

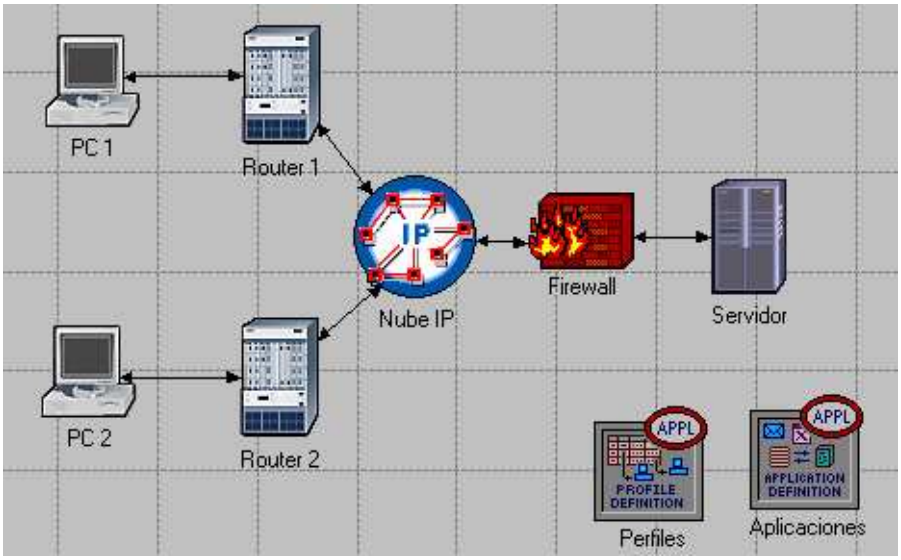

Ilustración 27: Escenario Con Firewall

5.4 CREACIÓN DEL ESCENARIO CON FIREWALL Y VPN

Una VPN es una forma de añadir seguridad a la información y a su vez, nos permite acceder al servidor de información incluso en presencia de un firewall, esto se debe a que la información pasa a través de un "tunel" dedicado en el cual se encapsulan los packetes IP en datagramas IP.

Para crear el escenario que contenga la VPN, se realiza el siguiente procedimiento (Véase Ilustración 28):

a) Duplicar el escenario Con_Firewall: desplegar el menú "Scenarios", seleccionar "Duplicate Scenario" y asignarle nombre, en este caso se llamará "Con_VPN", después presionar OK.
b) Quitar el enlace entre el Firewall y el servidor.
c) Abrir la paleta de objetos en el menú "Internet Toolbox" y añadir al escenario un "ethernet4_slip8_gtwy" y una "IP VPN Config".
d) Cambiar nombre a los elementos añadidos, en este caso se pondrá "Router 3" y "VPN" respectivamente.
e) Conectar el Router 3 al Firewall y al servidor mediante links PPP_DS1.
f) Guardar el proyecto.

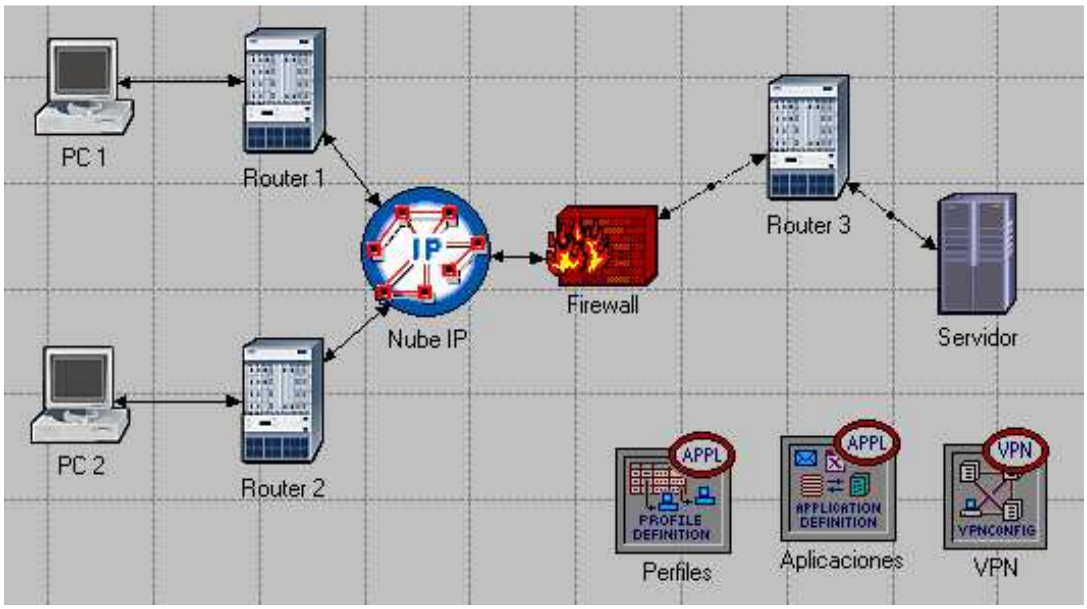

Ilustración 28: Escenario con Firewall y VPN

Se debe proceder a configurar la VPN mediante el siguiente procedimiento (Véase ilustración 29):

a) Hacer click derecho en "VPN" y seleccionar "Edit Atributes".
b) Expandir "VPN Configuration" y establecer "Rows" a 1,
c) Expandir "Row 0" y cambiar el valor de "Tunnel Source name" a "Router 1"
d) Cambiar el valor de "Tunnel Destination Name" a "Router 3".
e) Expandir "Remote client List" y establecer "Rows" a 1.
f) Expandir "Row 0" y cambiar el valor de "Client Node Name" a "PC 1"
g) Presionar OK y Guardar el proyecto.

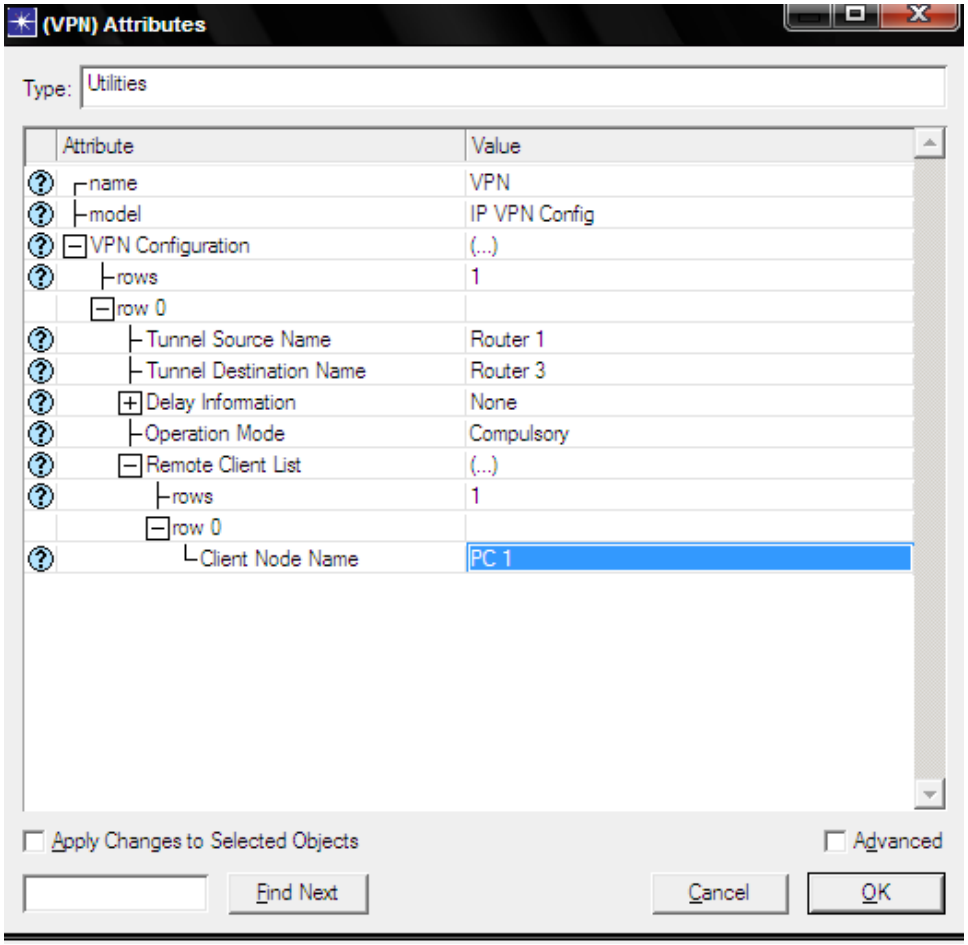

Ilustración 29: Configuración de la VPN

5.5 SIMULACIONES

Se desea realizar la simulación simultánea de los 3 escenarios con el fin de comparar los comportamientos de cada uno de ellos, esto se realiza mediante el siguiente procedimiento (Véase Ilustración 30):

a) Desplegar el menú "Scenarios" y seleccionar "Manage Scenarios".
b) Cambiar a "Collect" el campo results en todos los escenarios (Ver ilustración 30).

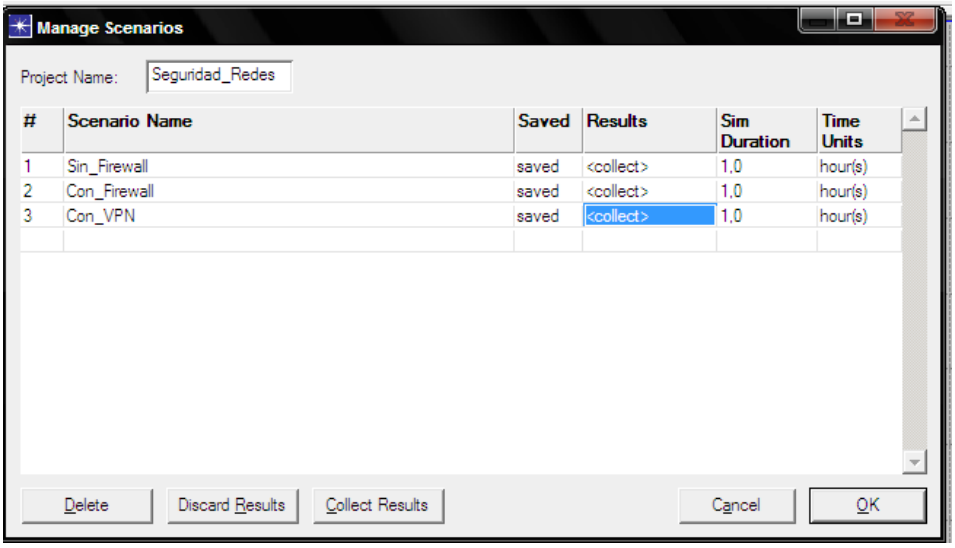

Ilustración 30: Recolección de Resultados para Simulación

c) Presionar "OK", Esperar que se ejecute la recolección de datos de las tres simulaciones, presionar "Close" y después guardar el proyecto.

6. RESULTADOS

Para visualizar los resultados se debe expandir el menú "Results" y seleccionar compare results, aparecerá una ventana en la que se podrá escoger entre las opciones escogidas previamente en "Choose individual statistics", con ello, se podrán visualizar los gráficos representativos de los datos recolectados en la simulación (Véase ilustración 31).

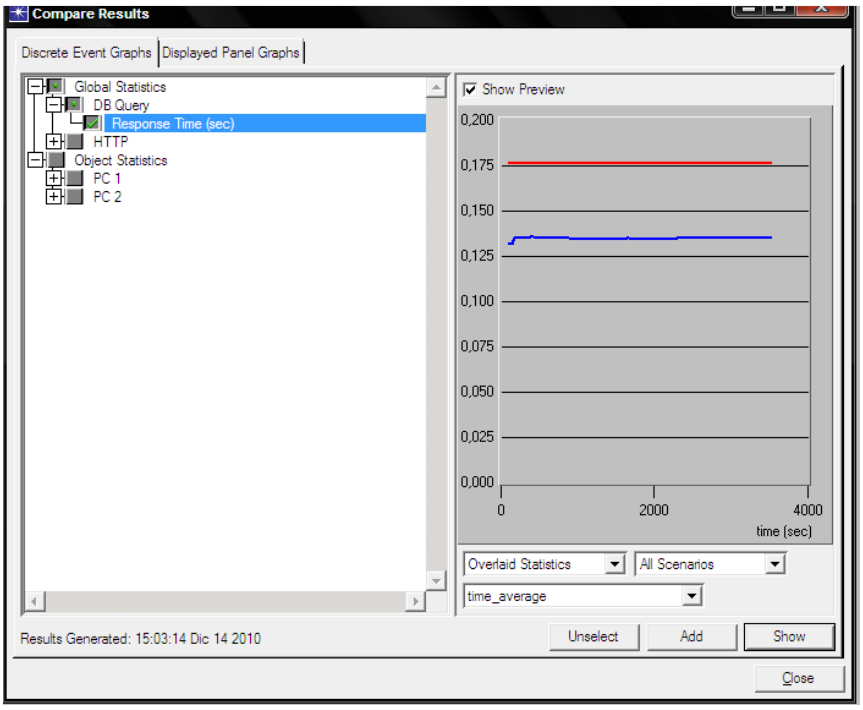

Ilustración 31: Pantalla para Escoger Gráficos

Para una mejor visualización de los resultados, se escoge la opción "time average" (promedio en el tiempo), también se escoge "All Scenarios" para mostrar los gráficos de todos los escenarios y "Overlaid statistics" para que se vean superpuestos. A continuación se muestran y analizan los gráficos resultantes de las simulaciones realizadas.

6.1 RESULTADOS GLOBALES

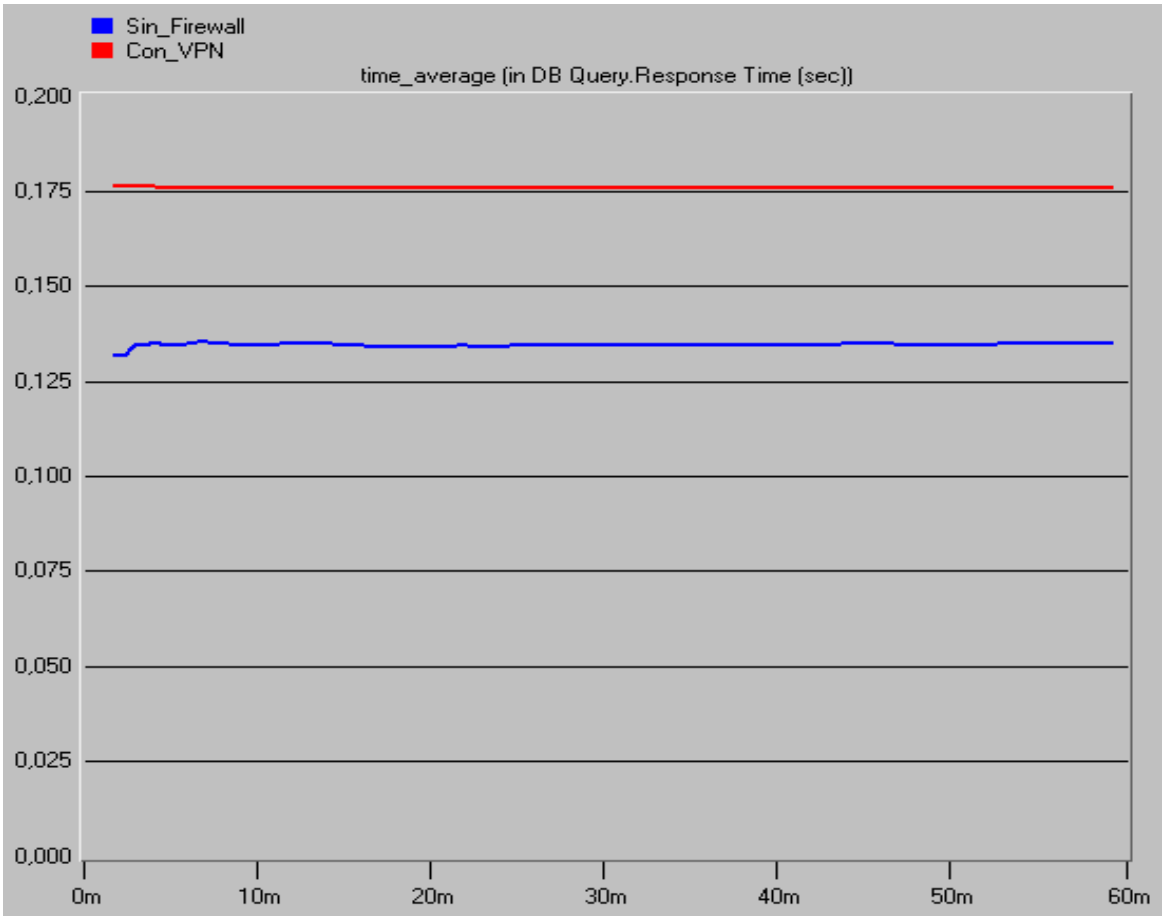

Ilustración 32: Tiempo de respuesta de consulta a base de datos (Promedio).

En el gráfico 1 se aprecian los tiempos de respuesta en consultas a la base de datos de los tres escenarios, nótese que se obtuvo un tiempo mayor en el escenario con VPN (0,175 seg aprox) comparado con el escenario sin firewall (0,135 seg aprox), esto es debido a que en el primero se tiene el Firewall y la VPN los cuales realizan procedimientos adicionales con los datos, cabe resaltar que si no se tuviera la VPN en este escenario, no se podrían realizar consultas a la base de datos, ese es el caso del escenario "con firewall" el cual no refleja ningún dato en el gráfico.

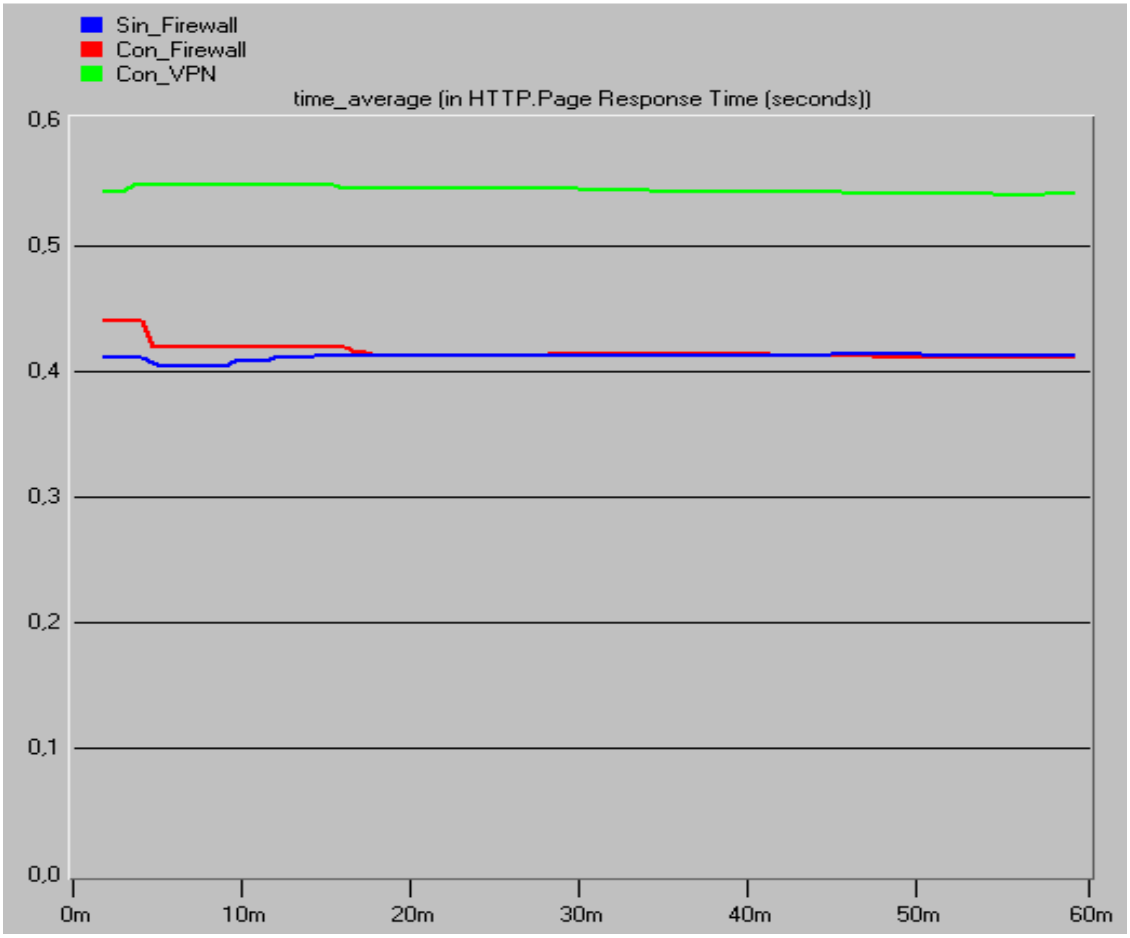

Ilustración 33: Tiempo de respuesta de pagina HTTP (promedio).

En el gráfico 2 se aprecia el tiempo de respuesta de una página HTTP para los tres escenarios, nótese que el escenario sin firewall tiene los tiempos de respuesta menores y que a su vez estos son muy similares a los del escenario con firewall, el cual en ocasiones presenta tiempos de respuesta superiores por los procesos de filtrado de información. El mayor tiempo de respuesta es originado en el escenario con VPN debido a los procesos adicionales de la VPN tales como encriptado, autenticación, etc.

6.2 RESULTADOS ESPECÍFICOS

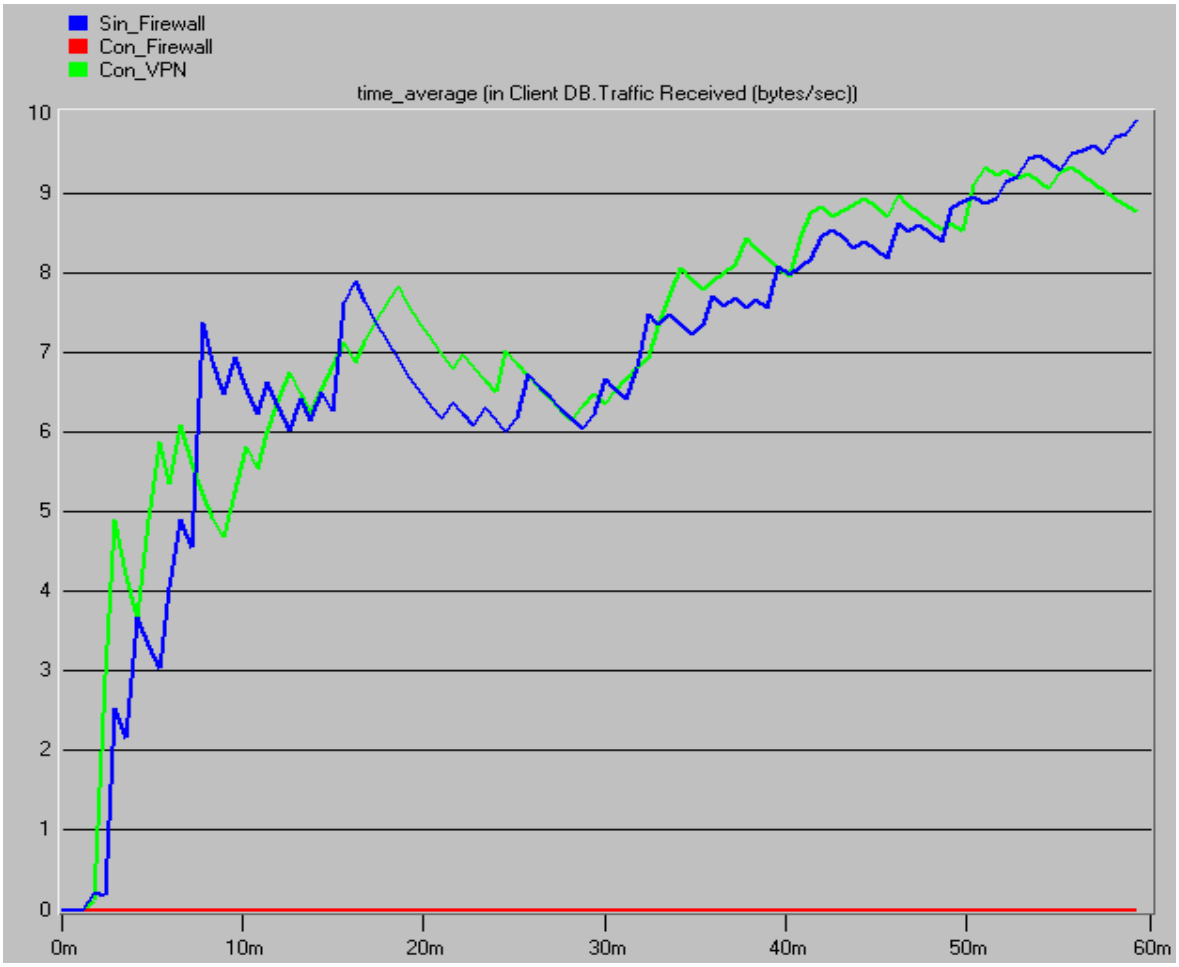

Ilustración 34: Tráfico recibido (bytes/sec) en cliente de base de datos (PC 1).

En el gráfico 3 se aprecia el Tráfico que recibe el PC1 (bytes/sec) que proviene de la base de datos (los tres escenarios están superpuestos), dicho tráfico depende de la cantidad y el tipo de datos que se consulten, por lo tanto los valores son variables, sin embargo, en el escenario "Con Firewall" el trafico es cero evidenciándose la acción del firewall al prohibir el acceso a la base de datos.

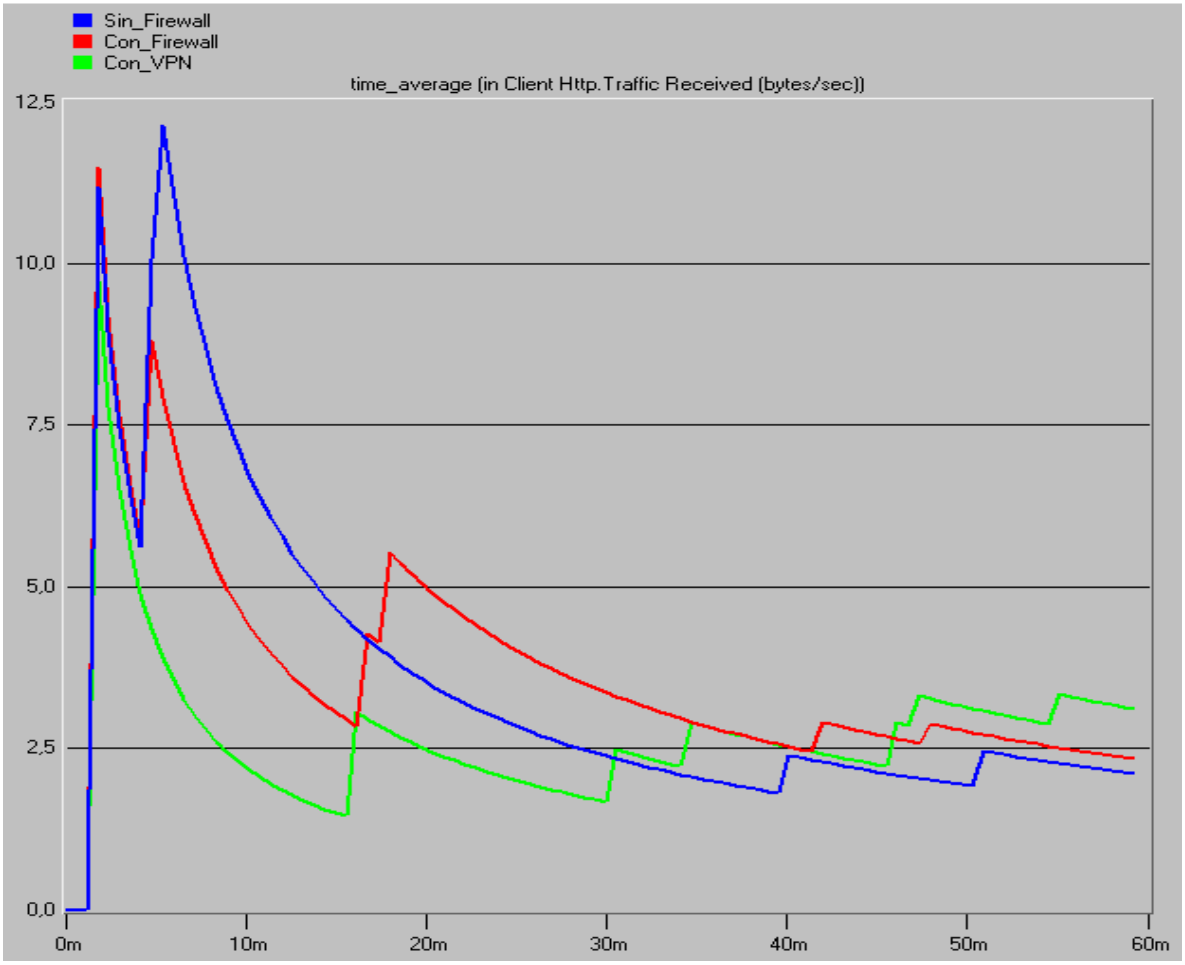

Ilustración 35 : Tráfico recibido (bytes/sec) en cliente HTTP (PC 1).

El gráfico 4 muestra el tráfico que recibe el PC 1 proveniente de una página HTTP (los tres escenarios están superpuestos), nótese que no está bloqueada ninguna conexión a paginas HTTP y que por lo tanto el tráfico de las consultas es variable y dependerá de las paginas consultadas.

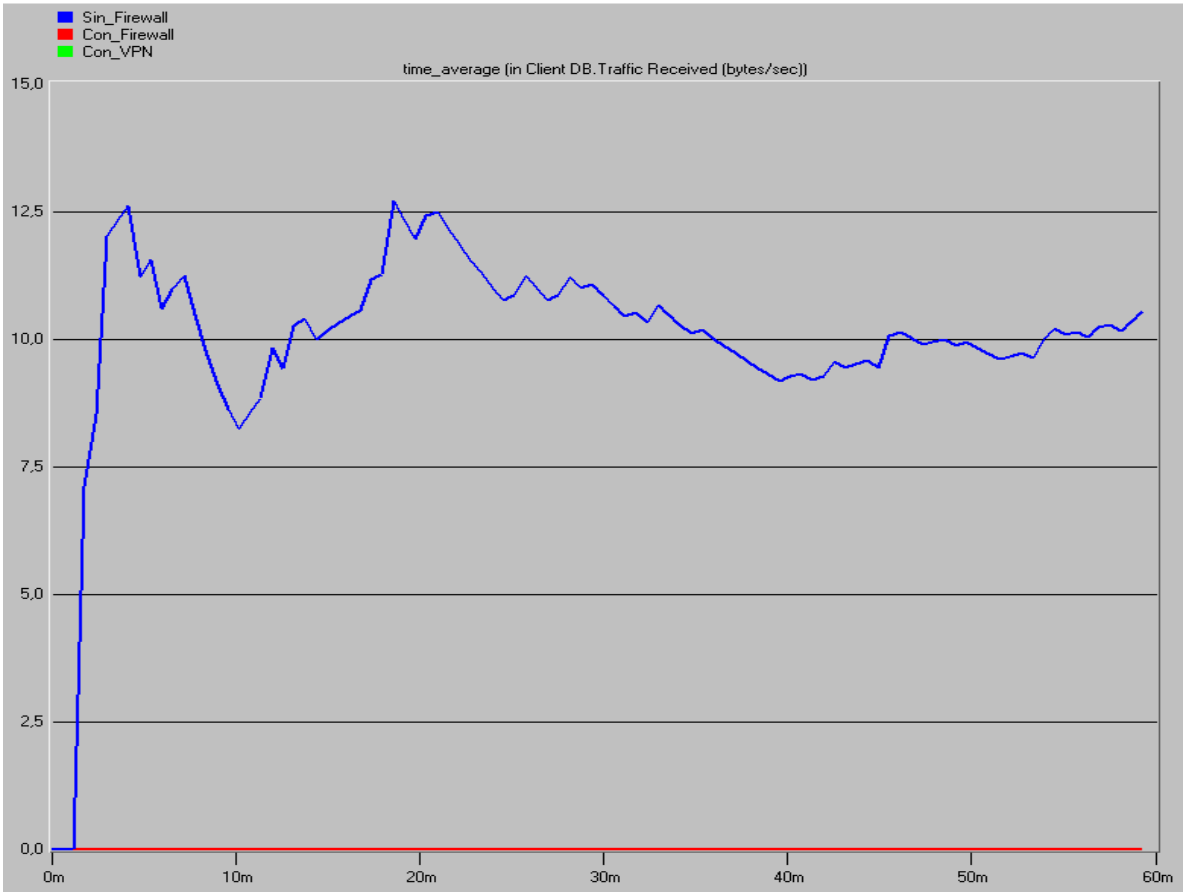

Ilustración 36: Tráfico recibido (bytes/sec) en cliente de base de datos (PC 2).

En el gráfico 5 se evidencia la acción del firewall al bloquearle al PC 2 el acceso a la base de datos en los escenarios "Con Firewall" y "Con VPN"; dichos escenarios se encuentran en igualdad de condiciones debido a que en el último, el PC 2 no fue configurado para emplear VPN.

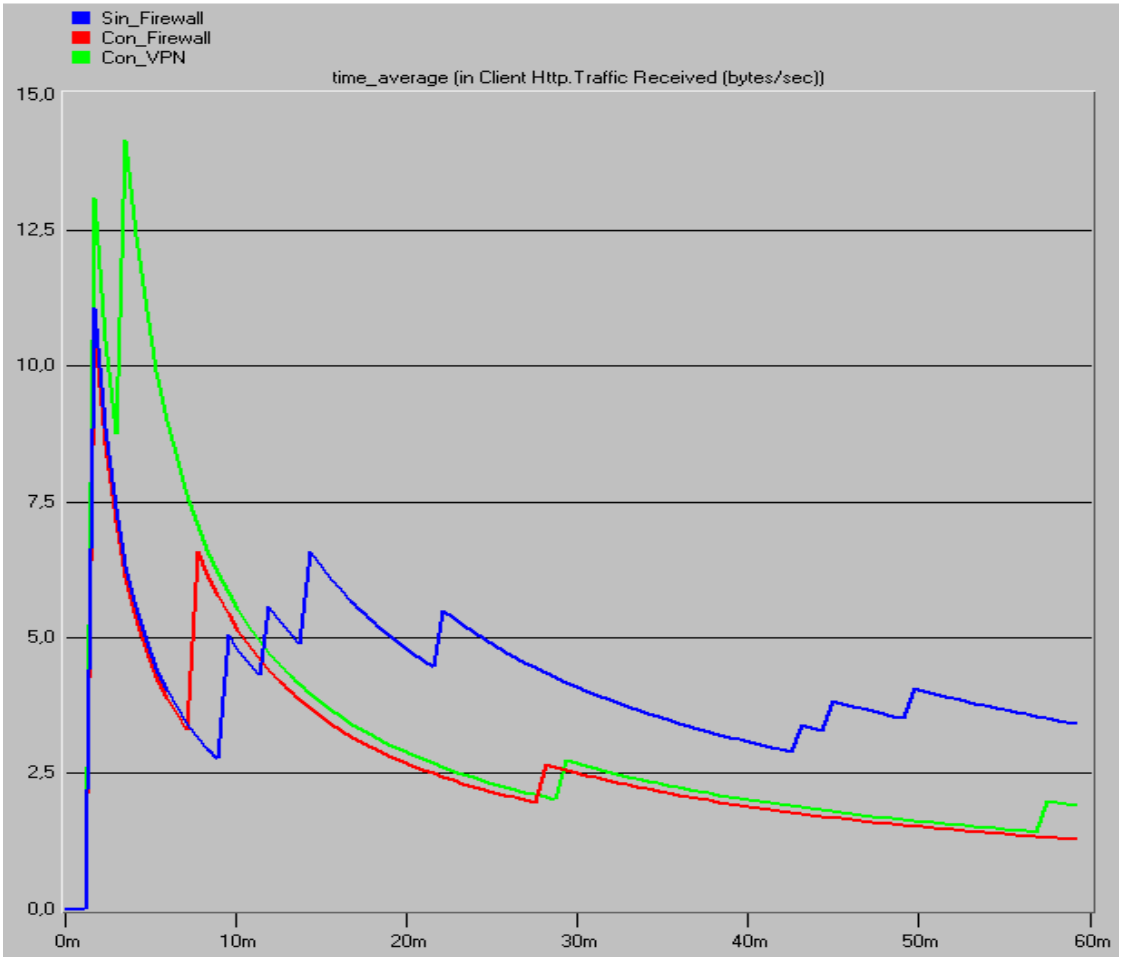

Ilustración 37: Tráfico recibido (bytes/sec) en cliente HTTP (PC 2).

El gráfico 6 muestra el tráfico que recibe el PC 2 proveniente de una página HTTP. Tal como en el PC 1, nótese que no está bloqueada ninguna conexión a paginas HTTP y que por lo tanto se muestra que para los tres (3) escenarios el tráfico de las consultas es variable y dependerá de las paginas consultadas.

6.3 PC 1 VS PC 2 EN ESCENARIO CON VPN

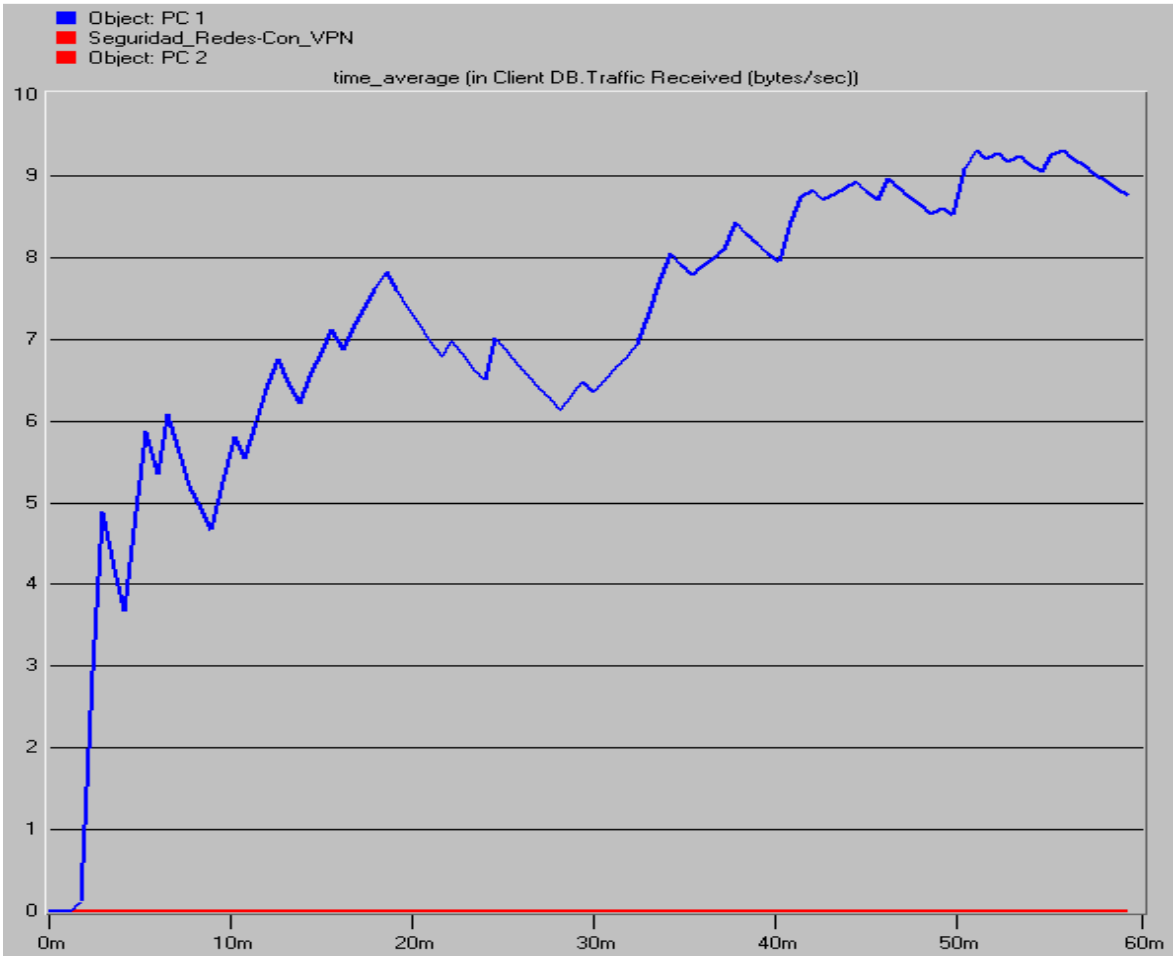

Ilustración 38: Tráfico recibido (bytes/sec) en cliente de base de datos.

El gráfico 7 refleja la diferencia en la configuración del PC 1 y el PC 2 en el escenario "Con VPN". El PC 1 está configurado para implementar una VPN mediante la cual puede acceder a la base de datos pasando a través del firewall sin inconvenientes, contrario a lo que sucede con el PC 2, el cual no implementa VPN y al tratar de acceder a la base de datos es impedido por el firewall.

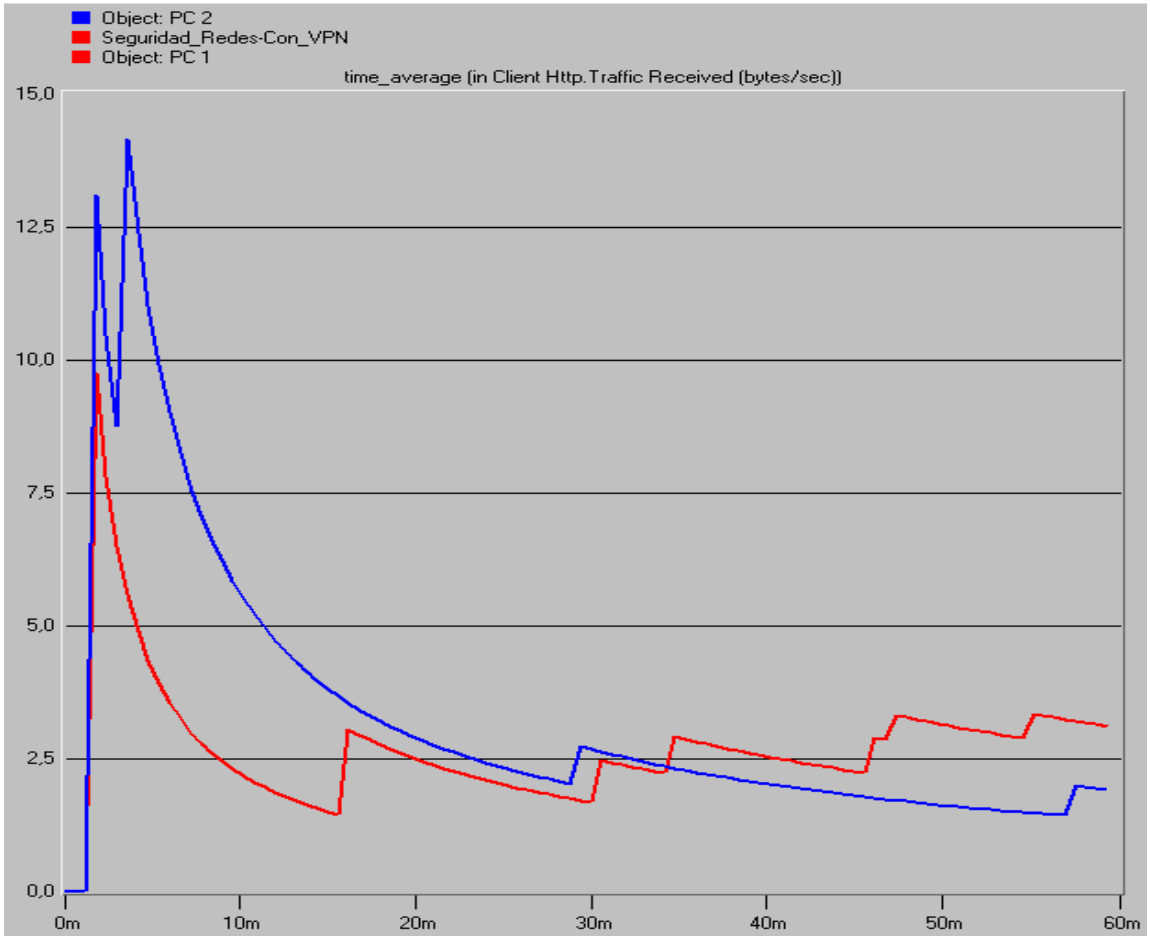

Ilustración 39: Tráfico recibido (bytes/sec) en cliente HTTP.

El gráfico 8 muestra el tráfico que reciben PC 1 y PC 2 proveniente de páginas HTTP. El tráfico de las consultas es variable y dependerá de las páginas consultadas en determinado tiempo.

7. CONCLUSIONES

En conclusión, a pesar de que aun existan redes sin restricciones de uso y acceso, el tema de la seguridad de la información es esencial para las comunicaciones en la actualidad y por esto los firewalls y las VPN cobran importancia.

De las simulaciones realizadas y los respectivos gráficos obtenidos se puede concluir que el firewall es un elemento capaz de brindarle seguridad a las redes de comunicaciones, este permite restringir el acceso de usuarios no autorizados a redes de comunicaciones, páginas de internet y servidores de información. Esto se evidencia en los gráficos 1, 3, 5 y 7 en los cuales el firewall bloquea el acceso del PC1 y el PC2 al servidor de información, obsérvese que el trafico recibido en Bytes/Sec en dichos PC refleja un valor igual a cero (0).

Por otra parte, en una red de comunicaciones puede existir la necesidad de bloquearle el acceso a cualquier usuario que intente conectarse a un servidor de información, sin embargo, puede existir también la necesidad de tener excepciones de tal manera que algunos usuarios puedan acceder a dicho servidor, una excelente solución a esta necesidad es la implementación de VPN entre el usuario y el servidor, con lo cual se crea virtualmente una red privada entre las partes que es "transparente" al firewall, esto es, el firewall permite el paso de paquetes de la VPN pues estos son encriptados y además, hacen parte "virtualmente" de una misma red a pesar de que no estén en el mismo lugar o espacio geográfico. El grafico 7 es un excelente ejemplo de la situación descrita anteriormente, nótese que el PC1 recibe tráfico variable del servidor de información gracias a que está configurado para implementar una VPN con dicho servidor, caso contrario al PC2 permanece en valor cero (0) de tráfico recibido por la acción del firewall.

Por último, cabe resaltar que el sistema OPNET es una herramienta muy útil para entender el funcionamiento y la lógica alrededor de las redes de comunicaciones.

Las simulaciones realizadas en OPNET muestran de una manera acertada el comportamiento de todos los elementos de la red diseñada, por ello, es recomendable que antes de implementar una red física se realicen las simulaciones pertinentes en OPNET para poder tener una visión de cómo sería el comportamiento al implementarla y hacer modificaciones en caso de ser necesario.

BIBLIOGRAFÍA

LIBROS Y ARTÍCULOS

- Ruiz J. VPN: Redes Privadas Virtuales, Marzo 2002.
- Larry P., Bruce D. Computer Networks: A Systems Approach. 3 ed. San Francisco: Morgan Kaufmann Publishers; 2003. 176 p.
- Paillier L., Arzuaga K. Guía Práctica Sobre Redes Privadas Virtuales [Monografía]. Cartagena: Universidad tecnológica de bolívar. Facultad de ingeniería eléctrica y electrónica; 2004.
- CISCO Systems.; Soluciones VPN: Todas sus sedes en una misma red.
- Mestre D., Medrano R. VPN Sobre LINUS Análisis de CIPE y PPTP Estableciendo Túneles [Monografía]. Cartagena: Universidad Tecnológica de Bolívar. Facultad de Ingeniería de Sistemas; 2004.
- Suarez F., Toloza L., Simulacion de Entorno VPN sobre OPNET [Monografía]. Cartagena: Universidad Tecnológica de Bolívar. Facultad de Ingeniería de Sistemas; 2004.
- Jarauta J., Palacios R., Sierra J. Seguridad Informatica: Capitulo 10, Seguridad Perimetral. Curso 5. Madrid: Universidad Pontificia. 2005 – 2006.

PÁGINAS WEB

- Borghello C., Deteniendo intrusos: firewall personales; Technical & Educational Manager de ESET para Latinoamérica; 29 de octubre del 2007.Se encuentra en http://www.eset.com.pa/threat-center/articles/firewall_personales.pdf
- 3COM CORPORATION, Seguridad de redes: Una guía para implementar Firewalls [Articulo de Internet]. http://salaam.cs.buap.mx/EBOOKS/SEGURIDAD/SS3_Firewall_WP_Span.pdf [Consulta: Octubre 15 de 2010].
- Firewall [Artículo en Internet] http://www.cpiicyl.org/ciudadanos/boletines/seguridad/Firewall.pdf [Consulta Noviembre 11 de 2010].

ANEXOS

Anexo 1: Video del procedimiento de las simulaciones.