UNIVERSIDAD LUTERANA SALVADOREÑA

FACULTAD DE CIENCIAS DEL HOMBRE Y LA NATURALEZA

LICENCIATURA EN CIENCIAS DE LA COMPUTACIÓN

ASIGNATURA

REDES II

TEMA

“FIREWALL CON BALANCEADOR DE DOS ENLACES DE INTERNET”

CATEDRÁTICO

Ingeniero Manuel Flores Villatoro

EQUIPO No. 01

No	*APELLIDOS Y NOMBRES*	*No.CARNET*	*PARTICIPACIÓN*
01	Arias Valle Pablo Moisés	AV02110131	100%
02	Arias Valle Santos Mauricio	AV02110129	100%
03	Martinez Hernández Denis Yosiley	MH01121153	100%

San Salvador, 08 de noviembre de 2014

Índice de contenido

Índice de ilustraciones

Índice de tablas

INTRODUCCIÓN

En el presente documento se detalla la forma en la que se procederá en la configuración del Firewall con balanceador de dos enlaces en Internet. Ya que el balanceador sirve como un equilibrador de carga ya que es una solución de red central encargada de distribuir el tráfico entrante entre al servidor y el mismo contenido de la aplicación . Al equilibrar las solicitudes de aplicaciones a través de múltiples servidores.

Además también Mencionamos los estudios de factibilidad en la implementación de dicho Proyecto las tecnologías involucradas y las etapas de para la implementación del proyecto. y el beneficios que nos traería la implementación del mismo.

Agregamos a este proyecto un marco teórico detallado, como se ha construido, siguiendo los pasos para su respectivas configuraciones y procedimientos que se utilizan para su buen funcionamiento, estableciendo un escenario de pruebas para la verificación de su funcionamiento en general.

OBJETIVOS

OBJETIVO GENERAL

- Configurar un Firewall, utilizando dos enlaces de Internet, para dar acceso a Internet a sus clientes dentro de una red LAN, y explicar de manera precisa su funcionamiento.

OBJETIVOS ESPECÍFICOS

- ➔ Determinar como funciona un Firewall con balanceador de carga a dos enlaces de Internet.
- ➔ Mostrar en detalle las herramientas que se requieren para el desarrollo de la configuración de un Firewall, con balanceador de carga.

1. DESCRIPCIÓN PROYECTO

1.1. FIREWALL CON BALANCEADOR DE DOS ENLACES DE INTERNET

Este proyecto consiste en la configuración de un Firewall(cortafuegos), que utilice dos enlace de Internet para brindar acceso a internet a dos computadoras clientes permitiéndoles a estos clientes que puedan acceder a internet a través del enlace que deseen, como veremos en el diagrama de red

que presentamos a continuación, para ello hemos considerado dos MÓDEMS 3G con internet la cual se conectara a una computadora que se utilizara como Firewall/Gateway, y mediante un Switch, al cual estarán conectadas las computadores clientes de una red LAN.

Este tipo de dispositivos le permitirán al administrador de la red bloquear el acceso a las personas que no estén autorizadas para ingresar a las redes privadas LAN, a la vez se realizara el balanceo de carga en la red a implementar.

Para ello instalaremos las aplicaciones de Apache2, iproute, iptables, Squid.

Apache2: Es un servidor Web HTTP de código abierto para plataformas libres y privadas.
Iproute:que sirve en el balanceo asignándole pesos a cada una de las placas existentes dentro de la computadora.
Iptables: Es una herramienta de cortafuego que permite no solamente filtrar paquetes sino también realizar traducción de direcciones de red.
Squid: Es un servidor Proxy para web con cache, es una de las aplicaciones mas populares de referencia para esta función. Esta mejora el rendimiento de las conexiones de empresas y particulares de Internet y acelera el acceso a un servidor Web, realizando filtrado de seguridad.
Munin: Es una herramienta escrita en Perl, de monitorización de sistema de red que nos muestra gráficos a través de una interfaz web.
Tcpdump: Es una herramienta en linea de comandos, cuya utilidad principal, es analizar el tráfico que circula por la red.
Modems: Es un pequeño dispositivo electrónico que permite a un usuario acceder a internet a través de su PC portatil, cuando no dispone de una conexión a internet o cuando no se encuentra dentro de un zona WiFi.

1.2. Pasos a Seguir

- ✔ Primero vamos a crear un red LAN, configurando las computadoras en un bloque de red en este caso se utilizara, el bloque 192.168.1.0
- ✔ Configurar el balanceador de carga con las aplicaciones mencionadas.
- ✔ Realizar pruebas de funcionamiento de las aplicaciones y su corrección según el caso

1.3. MODELO DE DIAGRAMA DE RED

En el siguiente diagrama se representa de forma breve el desarrollo del proyecto a implementado.

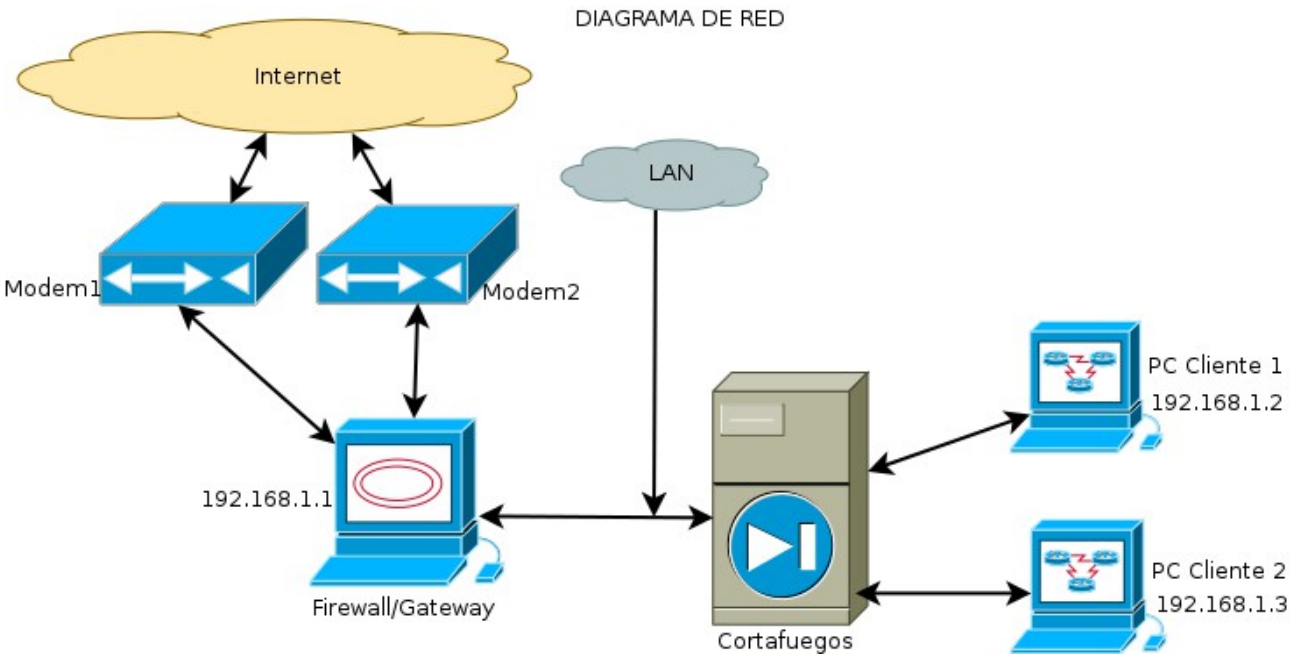

Ilustración 1: Diagrama de Red

2. MARCO TEÓRICO

2.1 FIREWALL

Un cortafuegos (firewall en inglés) es una parte de un sistema o una red que está diseñado para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

Se trata de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios.

Los cortafuegos pueden ser implementados en hardware o software, o una combinación de ambos. Los cortafuegos se utilizan con frecuencia para evitar que los usuarios de Internet no autorizados tengan acceso a redes privadas conectadas a Internet, especialmente intranet. Todos los mensajes que entren o salgan de la intranet pasan a través del cortafuegos, que examina cada mensaje y bloquea aquellos que no cumplen los criterios de seguridad especificados. También es frecuente conectar al cortafuegos a una tercera red, llamada «zona desmilitarizada» o DMZ, en la que se ubican los servidores de la organización que deben permanecer accesibles desde la red exterior.

Un cortafuegos correctamente configurado añade una protección necesaria a la red, pero que en ningún caso debe considerarse suficiente. La seguridad informática abarca más ámbitos y más niveles de trabajo y protección.

El término firewall / fireblock significaba originalmente una pared para confinar un incendio o riesgo potencial de incendio en un edificio. Más adelante se usa para referirse a las estructuras similares, como la hoja de metal que separa el compartimiento del motor de un vehículo o una aeronave de la cabina. La tecnología de los cortafuegos surgió a finales de 1980, cuando Internet era una tecnología bastante nueva en cuanto a su uso global y la conectividad. Los predecesores de los cortafuegos para la seguridad de la red fueron los routers utilizados a finales de 1980, que mantenían a las redes separadas unas de otras. La visión de Internet como una comunidad relativamente pequeña de usuarios con máquinas compatibles, que valoraba la predisposición para el intercambio y la colaboración, terminó con una serie de importantes violaciones de seguridad de Internet que se produjo a finales de los 80.

2.2. PRIMERA GENERACIÓN

El primer documento publicado para la tecnología firewall data de 1988, cuando el equipo de ingenieros Digital Equipment Corporation (DEC) desarrolló los sistemas de filtro conocidos como cortafuegos de filtrado de paquetes. Este sistema, bastante básico, fue la primera generación de lo que se convertiría en una característica más técnica y evolucionada de la seguridad de Internet.

El filtrado de paquetes actúa mediante la inspección de los paquetes (que representan la unidad básica de transferencia de datos entre ordenadores en Internet). Si un paquete coincide con el conjunto de reglas del filtro, el paquete se reducirá (descarte silencioso) o será rechazado (desprendiéndose de él y enviando una respuesta de error al emisor). Este tipo de filtrado de paquetes no presta atención a si el paquete es parte de una secuencia existente de tráfico. En su lugar, se filtra cada paquete basándose únicamente en la información contenida en el paquete en sí (por lo general utiliza una combinación del emisor del paquete y la dirección de destino, su protocolo, y, en el tráfico TCP y UDP, el número de puerto). Los protocolos TCP y UDP comprenden la mayor parte de comunicación a través de Internet, utilizando por convención puertos bien conocidos para determinados tipos de tráfico, por lo que un filtro de paquetes puede distinguir entre ambos tipos de tráfico (ya sean navegación web, impresión remota, envío y recepción de correo electrónico, transferencia de archivos…); a menos que las máquinas a cada lado del filtro de paquetes estén a la vez utilizando los mismos puertos no estándar.

2.3. SEGUNDA GENERACIÓN

Durante 1989 y 1990, tres colegas de los laboratorios AT&T Bell, Dave Presetto, Janardan Sharma, y Nigam Kshitij, desarrollaron la segunda generación de servidores de seguridad. Esta segunda generación de cortafuegos tiene en cuenta, además, la colocación de cada paquete individual dentro de una serie de paquetes. Esta tecnología se conoce generalmente como la inspección de estado de paquetes, ya que mantiene registros de todas las conexiones que pasan por el cortafuegos, siendo capaz de determinar si un paquete indica el inicio de una nueva conexión, es parte de una conexión existente, o es un paquete erróneo. Este tipo de cortafuegos pueden ayudar a prevenir ataques contra conexiones en curso o ciertos ataques de denegación de servicio.

2.4. TERCERA GENERACIÓN

Son aquellos que actúan sobre la capa de aplicación del modelo OSI. La clave de un cortafuegos de aplicación es que puede entender ciertas aplicaciones y protocolos (por ejemplo: protocolo de transferencia de ficheros, DNS o navegación web), y permite detectar si un protocolo no deseado se coló a través de un puerto no estándar o si se está abusando de un protocolo de forma perjudicial.

Un cortafuegos de aplicación puede filtrar protocolos de capas superiores tales como FTP, TELNET, DNS, DHCP, HTTP, TCP, UDP y TFTP (GSS). Por ejemplo, si una organización quiere bloquear toda la información relacionada con una palabra en concreto, puede habilitarse el filtrado de contenido para bloquear esa palabra en particular. No obstante, los cortafuegos de aplicación resultan más lentos que los de estado.

2.5. ACONTECIMIENTOS POSTERIORES

En 1992, Bob Braden y DeSchon Annette, de la Universidad del Sur de California (USC), dan forma al concepto de cortafuegos. Su producto, conocido como "Visas", fue el primer sistema con una interfaz gráfica con colores e iconos, fácilmente implementable y compatible con sistemas operativos como Windows de Microsoft o MacOS de Apple. En 1994, una compañía israelí llamada Check Point Software Technologies lo patentó como software denominándolo FireWall-1.

La funcionalidad existente de inspección profunda de paquetes en los actuales cortafuegos puede ser compartida por los sistemas de prevención de intrusiones (IPS).

Actualmente, el Grupo de Trabajo de Comunicación Middlebox de la Internet Engineering Task Force (IETF) está trabajando en la estandarización de protocolos para la gestión de cortafuegos.

2.6. TIPOS DE CORTAFUEGOS

2.6.1. Nivel de Aplicación de Pasarela

Aplica mecanismos de seguridad para aplicaciones específicas, tales como servidores FTP y Telnet. Esto es muy eficaz, pero puede imponer una degradación del rendimiento.

2.6.2. Circuito a Nivel de Pasarela

Aplica mecanismos de seguridad cuando una conexión TCP o UDP es establecida. Una vez que la conexión se ha hecho, los paquetes pueden fluir entre los anfitriones sin más control. Permite el establecimiento de una sesión que se origine desde una zona de mayor seguridad hacia una zona de menor seguridad.

2.6.3. Cortafuegos de Capa de Red o de Filtrado de Paquetes

Funciona a nivel de red (capa 3 del modelo OSI, capa 2 del stack de protocolos TCP/IP) como filtro de paquetes IP. A este nivel se pueden realizar filtros según los distintos campos de los paquetes IP: dirección IP origen, dirección IP destino. A menudo en este tipo de cortafuegos se permiten filtrados según campos de nivel de transporte (capa 3 TCP/IP, capa 4 Modelo OSI), como el puerto origen y destino, o a nivel de enlace de datos (no existe en TCP/IP, capa 2 Modelo OSI) como la dirección MAC.

2.6.4. Cortafuegos de la Capa de Aplicación

Trabaja en el nivel de aplicación (capa 7 del modelo OSI), de manera que los filtrados se pueden adaptar a características propias de los protocolos de este nivel. Por ejemplo, si trata de tráfico HTTP, se pueden realizar filtrados según la URL a la que se está intentando acceder, e incluso puede aplicar reglas en función de los propios valores de los parámetros que aparezcan en un formulario web.

Un cortafuegos a nivel 7 de tráfico HTTP suele denominarse proxy, y permite que los ordenadores de una organización entren a Internet de una forma controlada. Un proxy oculta de manera eficaz las verdaderas direcciones de red.

2.6.5. Cortafuegos Personal

Es un caso particular de cortafuegos que se instala como software en un ordenador, filtrando las comunicaciones entre dicho ordenador y el resto de la red. Se usa por tanto, a nivel personal.

2.6.6. Firewall que existen en el Mercado

2.6.6.1. Sonicwall PRO-VX Y XPRS2 con Global Management System 2.0

SonicWall es conocido en el mercado de firewalls SOHO por ofrecer productos fáciles de usar y de

importantes carácterísticas [Fratto]. Junto con SonicWall Global Management System (GMS) 2.0, SonicWall se convierte en una plataforma sólida para administrar un gran número de firewalls. Presenta algunas características favorables como una fuerte administración centralizada, registro centralizado y características de seguridad de valor agregado. GMS tiene algunas características de administración interesantes que no poseen otros productos. Se dispone de múltiples vistas que le permiten al administrador organizar la forma de presentar los firewalls que son administrados de formas diferentes.

2.6.6.2. Lucent Technologies VPN Firewall Brick y Lucent Security Management Server

La oferta del LSMS y Brick 80 y 201 provee un amplio rango de características apropiadas para la red de un proveedor de servicios [Fratto]. LSMS tiene características avanzadas tales como administración en capas, herramientas de monitoreo de estado y registro de sucesos detallado, recuperación de hardware simple, y la habilidad de hacer cambios a las políticas de los firewalls en un sitio central.

Como en otros productos, cuando los firewalls son instalados en el sistema de administración sone, sitúan en grupos lógicos. En LSMS, cada cliente configurado tiene su propio conjunto único de firewalls Brick, políticas, usuarios y administradores. Cualquier cambio hecho a un cliente se mantiene aislado de los otros. El control de acceso para administración tiene definido tres categorías amplias:

- ✔ Dispositivos,
- ✔ Políticas y VPNs
- ✔ Usuarios y grupos de usuarios

2.6.6.3. Novel Networks Contivity 600 y Optivity NCS

La línea de productos de Contivity de Nortel es más usada para VPNs pero también tienen un firewall de filtrado de paquetes basado en estados como también soporte para el modulo de aplicación de FireWall-1 de Check Point [Fratto]. La estación de administración del Optivity NCS tiene funciones de administración adecuadas. Desafortunadamente, Contivity no ofrece las características adicionales de seguridad de SonicWall, tales como filtrado de URL y contenido, o la

facilidad de instalación del Brick de Lucent.

2.6.6.4. Watchguard Technologies Firebox 1000/2500 y Watchguard NOC Security Software

WatchGuard fue uno de los primeros en administración de firewalls [Fratto]. Su Servicio de Administración de Seguridad (MSS) está basado en un enfoque distribuido, los firewalls tienen importantes características y están basados en unidades proxy. Dispone de una posición de seguridad mas controlable gracias al soporte de bloqueo de contenido, URL y archivos adjuntos de e-mail. De todas formas la estación de administración de MSS tiene algunas características que contribuyen a la carga del sistema.

2.6.6.5. FireWall-1 de CheckPoint Software Technologies

Permite definir una política de seguridad única y global, que proteja a todos los recursos de red [FireWall-1]. Posee una arquitectura de tres capas, utiliza tecnología de Inspección basada en Estados1 (stateful inspection) y funciona sobre la Plataforma Abierta de Securidad2 (OPSEC). Ofrece soluciones altamente escalables, capaces de integrar y administrar de forma central todos los aspectos de la seguridad de una red.

3. LISTA DE ACTIVIDADES

Como equipo de trabajo, para hemos programado las siguientes actividades las cuales posteriormente se reflejaran en un diagrama de gantt.

1. Coordinación y formación de equipo de trabajo.
2. Elección de elementos que utilizaremos en el proyecto de Firewall con balanceador de Internet.
3. Elaboración del perfil del proyecto a implementar o desarrollar.
4. Adquirir tres computadoras una como Firewall/Gateway y dos como cliente; así como también un switch.
5. Pruebas de verificación de recursos con las que contamos.
6. La instalación de el Sistema Operativo GNU/Linux, Debian 7.3.0 Wheezy en las tres computadoras que utilizaremos en el proyecto.

7. Instalaciones de la herramientas de prueba.
8. Configuración final del Firewall
9. Pruebas y seguimiento del proyecto.
10. Preparación del proyecto final y defensa

4. DIAGRAMA DE GANTT

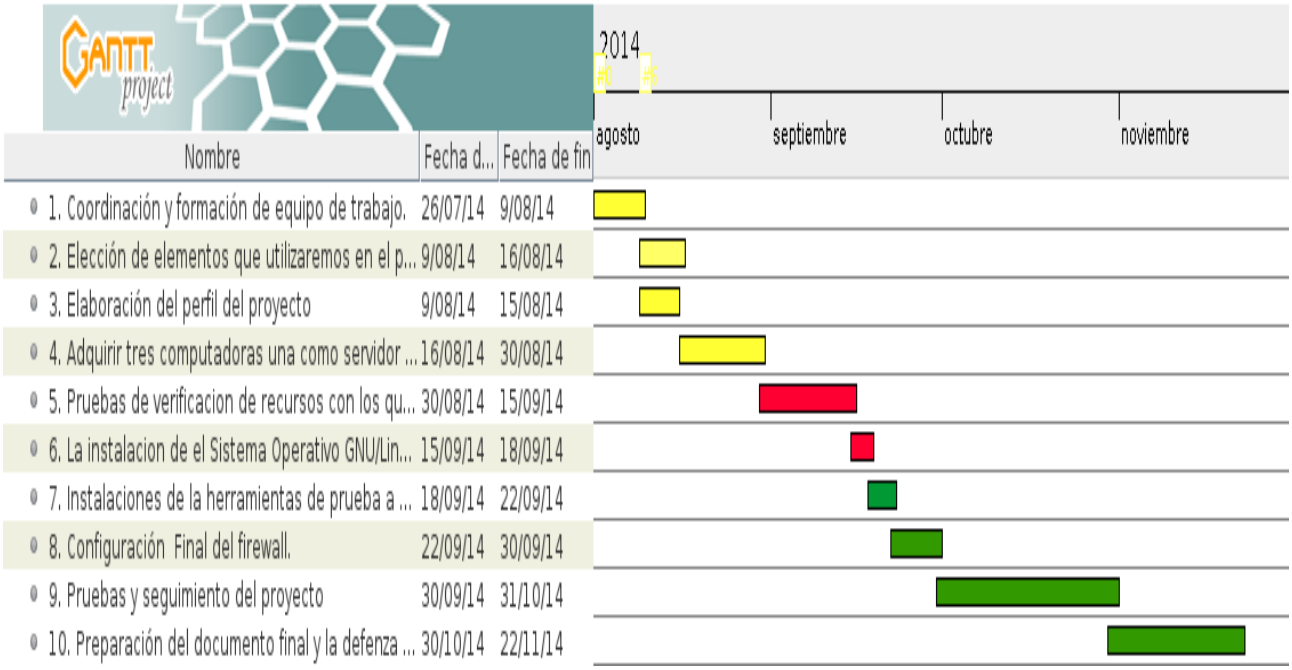

Ilustración 2: Diagrama de desarrollo del proyecto

5. VIABILIDAD O FACTIBILIDAD DEL PROYECTO

5.2. Requerimientos Técnicos.

5.2.1. Requerimientos de Hardware.

- ✗ Una computadora con microprocesador Movile AMD Sempron(TM)procesador 3100+

Memoria RAM de 512 MB

Sistema Operativo Debian 7.3.0 Wheezy

- ✗ Una computadora con microprocesador Intel Atom CPU N2100 1.60GHz*2

Memoria RAM 2GiB

Sistema Operativo Debian 7.4 Wheezy de 32-bit

- ✗ Una computadora con micro procesador Movile AMD Sempron(TM)procesador 3100+, 789 Ghz, 384 Mb de memoria RAM.

Sistema Operativo Debian 7.4 Wheezy de 32-bit

- ✗ 2 MODEMS 3G
- ✗ 4 cables UTP categoría 5 o 7
- ✗ 10 conectores RJ45
- ✗ 10 capuchones 45
- ✗ Una cripadora o ponchadora para cable RJ45
- ✗ Un Switch de 8 puertos
- ✗ Probador de cable RJ45
- ✗ Una memoria USB

5.2.2. Requerimientos de Software.

Sistema multiplataforma GNU/Linux

Forma manual (individual):

- ✔ Ganttproyect
- ✔ suite de Ofimática en entorno libre
- ✔ DÍA

Navegadores

- ✔ Google Chrome
- ✔ Mozilla
- ✔ Epiphany
- ✔ Iceweasel y
- ✔ Otros

5.3. FACTIBILIDAD TÉCNICA:

Se cuenta con los conocimientos básicos en el funcionamiento de redes informáticas, y a la ves contamos con acceso a las herramientas a utilizar en el desarrollo del proyecto.

5.4. FACTIBILIDAD OPERATIVA:

Es el equipo de trabajo destinado para la ejecución del proyecto.

5.5. FACTIBILIDAD LEGAL:

Se utilizara software libre.

5.6.FACTIBILIDAD ECONÓMICA:

Como se utilizara software libre no tendría ninguna valoración económica, pero para algunos equipo si tendríamos que utilizar recursos económicos.

5.6.1. PRESUPUESTO DEL PROYECTO CONFIGURACIÓN DE FIREWALL

"FIREWALL CON BALANCEADOR DE DOS ENLACES DE INTERNET"					
MATERIALES Y EQUIPO	***COSTO UNITARIO(MONEDA LOCAL)***	***CANTIDAD***	***UNIDAD DE MEDIDA***	***COSTO TOTAL (MONEDA LOCAL)***	***OBSERVACIONES***
COMPUTADORAS	400	3	UNIDAD	$1200.00	SE UTILIZARA UNA COMO FIREWALL/GATEWAY Y DOS COMO CLIENTES
CABLES UTP CATEGORÍA 5 O 6	0.40	8	METROS	3.20	PARA REALIZAR LAS CONEXIONES DE RED
CONECTORES RJ45	0.10	10	UNIDAD	1.00	PREPARACIÓN DEL CABLEADO ESTRUCTURADO
CAPUCHONES RJ45	0.10	10	UNIDAD	1.00	PREPARACIÓN DEL CABLEADO ESTRUCTURADO
CRIPADORA O PONCHADORA PARA CABLE RJ45	10.00	1	UNIDAD	10.00	PREPARACIÓN DEL CABLEADO ESTRUCTURADO
SWITCH DE 8 PUERTOS	15.00	1	UNIDAD	15.00	PREPARACIÓN DEL CABLEADO ESTRUCTURADO
PROBADOR DE CABLE RJ45	25.00	1	UNIDAD	25.00	PREPARACIÓN DEL CABLEADO ESTRUCTURADO
MODEMS CON INTERNET	30	2	UNIDAD	60.00	PARA CONEXIÓN DE INTERNET
MEMORIA USB	8.00	2	UNIDAD	16.00	PARA TRASLADAR INFORMACIÓN
PASAJES	10.00	3	POR PERSONA	30.00	DESPLAZAMIENTOS DEL GRUPO
FOLDERS	0.15	4	UNIDAD	0.60	PARA PRESENTAR REPORTES
COPIAS DE FOLLETOS	1.50	8	FOLLETO	12.00	PARA ESTUDIANTES
IMPRESIONES	0.10	200	PÁGINA	20.00	PARA IMPRIMIR REPORTES
PAGINAS DE PAPEL BOND BASE 20	0.01	200	UNIDAD	2.00	PARA PRESENTAR REPORTES
MONTO TOTAL DEL PROYECTO					***$ 1,395.80***

Tabla 1: Presupuesto del proyecto

6. INFORMACIÓN DE LA CONSTRUCCIÓN DEL PROYECTO

6.1.Balanceo de Carga

El balanceo de carga es un concepto utilizado en informática, el cual se refiere a la técnica, usada para compartir el trabajo y realizar varios procesos, ordenadores, discos u otros recursos. Esta íntimamente ligado a los sistemas multiprocesamiento o que hacen uso de una unidad de procesamiento, para realizar labores útiles.

El balance de carga se mantiene gracias a un algoritmo que divide la manera mas equitativa posible el trabajo, para evitar así los cuellos de botella.

6.2. Tabla de Información de la Red

DISPOSITIVO	***INTERFAZ***	***DIRECCIÓN IP***	***MASCARA DE SUBRED***	***PUERTA DE ENLACE***
FIREWALL/ GATEWAY	Eth0	192.168.1.1	255.255.255.0	Ips dinámicas
	ppp0	Ip dinámica	No asignada	No asignada
	ppp1	Ip dinámica	No asignada	No asignada
Pc1	Eth0	192.168.1.2	255.255.255.0	192.168.1.1
Pc2	Eth0	192.168.1.3	255.255.255.0	192.168.1.1

Tabla 2: Tabla de información de la Red

Nota: En tal caso las Pc1 y 2, tendrán como puerta de enlace la IP del Firewall/Gateway, quien a su vez se enlazara a internet a través de las Ips dinámicas de los Módems.

6.3. Iniciamos la configuración de la Pc que se utilizara como Firewall/Gateway

Instalamos Iptable, desde la terminal como admnistrador (# ***apt-get install iptable***)

Creamos el bloque de red en la Maquina principal de la siguiente manera:

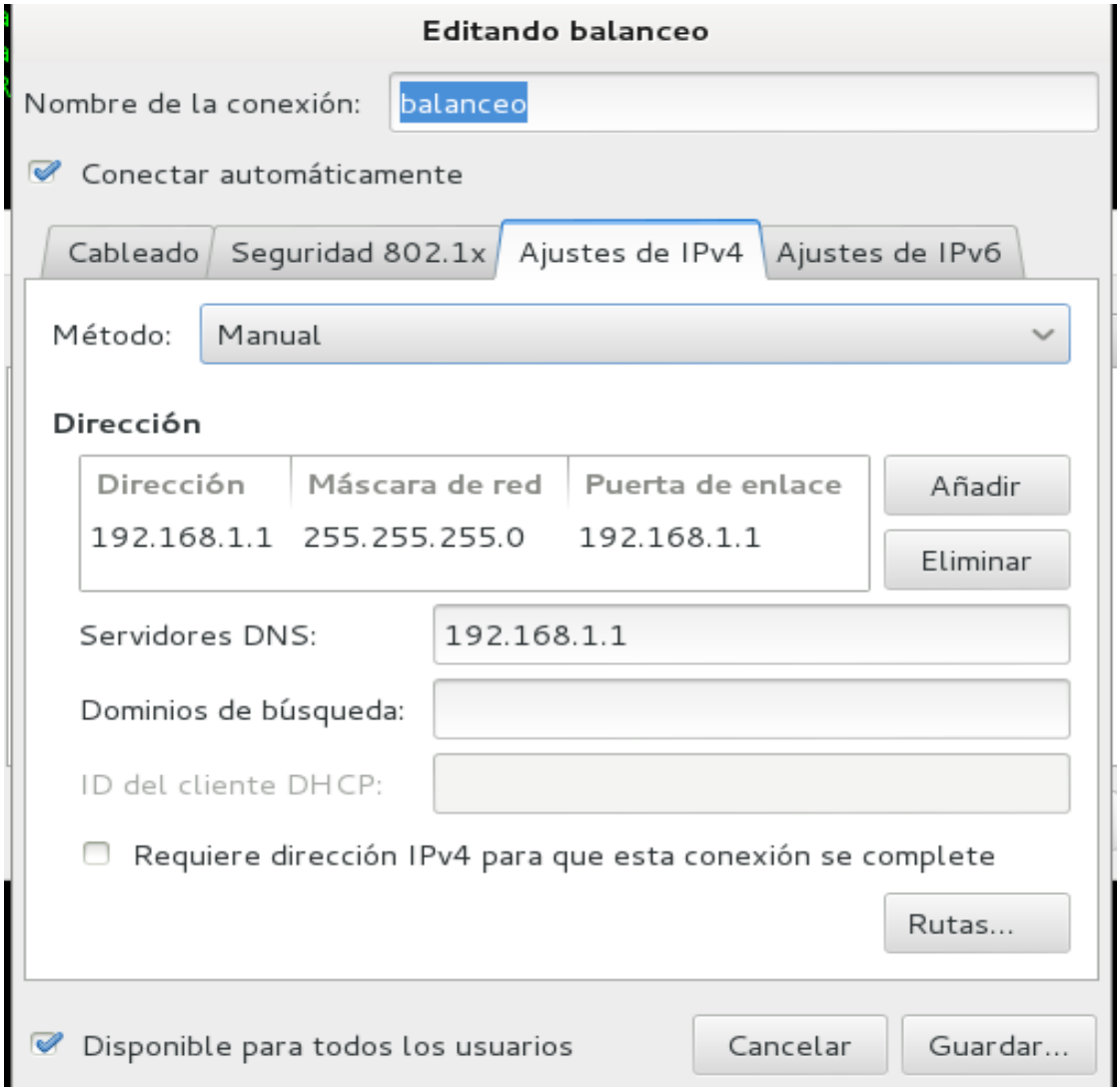

Ilustración 3: Creación de la Red LAN

Como segundo punto, desde la terminal ejecutamos los siguientes comandos para compartir internet con los clientes de nuestra red LAN.

```
root@pablo:/home/pablo# iptables --flush
root@pablo:/home/pablo# iptables --table nat --flush
root@pablo:/home/pablo# iptables --table nat --append POSTROUTING --out-interface ppp0 -j MASQUERADE
root@pablo:/home/pablo# iptables --table nat --append POSTROUTING --out-interface ppp1 -j MASQUERADE
root@pablo:/home/pablo# iptables --append FORWARD --in-interface eth0 -j ACCEPT
root@pablo:/home/pablo# ip route del default
root@pablo:/home/pablo#
```

Ilustración 4: Comando para compartir Internet

Después verificamos las Ips dinámicas de los Módems, con el comando ifconfig:

```
eth0      Link encap:Ethernet  HWaddr 18:67:b0:32:65:26
          inet addr:192.168.1.1  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::1a67:b0ff:fe32:6526/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:111573 errors:0 dropped:0 overruns:0 frame:0
          TX packets:114969 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:16230290 (15.4 MiB)  TX bytes:76896711 (73.3 MiB)
          Interrupt:40 Base address:0x8000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:26552 errors:0 dropped:0 overruns:0 frame:0
          TX packets:26552 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:4229757 (4.0 MiB)  TX bytes:4229757 (4.0 MiB)

ppp0      Link encap:Point-to-Point Protocol
          inet addr:10.90.100.107  P-t-P:10.64.64.64  Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1
          RX packets:43 errors:0 dropped:0 overruns:0 frame:0
          TX packets:57 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:3
          RX bytes:9514 (9.2 KiB)  TX bytes:6216 (6.0 KiB)

ppp1      Link encap:Point-to-Point Protocol
          inet addr:10.135.144.174  P-t-P:10.64.64.65  Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1
          RX packets:8 errors:0 dropped:0 overruns:0 frame:0
          TX packets:9 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:3
          RX bytes:128 (128.0 B)  TX bytes:185 (185.0 B)

root@pablo:/home/pablo#
```

Ilustración 5: Verificación de Interfaces

Podemos ver que la Ip de ppp0 es 10.90.100.107 y la ppp1 es 10.135.144.174, copiamos estas ips y las editamos en el archivo enrrutamiento.sh así:

```
  GNU nano 2.2.6                    Fichero: enrutamiento.sh

#!/bin/bash
IF1=ppp0
IF2=ppp1
IP1=10.135.98.101
IP2=0.15.5.208
P1=10.64.64.64
P2=10.64.64.65
P1_NET=10.135.98.101
P2_NET=0.15.5.208



echo "ip route add $P1_NET dev $IF1 src $IP1 table 1"
ip route add $P1_NET dev $IF1 src $IP1 table 1
echo "ip route add default via $P1 table 1"
ip route add default via $P1 table 1


echo "ip route add $P2_NET dev $IF2 src $IP2 table 2"
ip route add $P2_NET dev $IF2 src $IP2 table 2
echo "ip route add defaul via $P2 table 2"
ip route add dafaul via $P2 table 2

echo "ip route add $P1_NET dev $IF1 src $IP1"
ip route add $P1_NET dev $IF1 src $IP1

echo "ip route add $P2_NET dev $IF2 src $IP2"
ip route add $P2_NET dev $IF2 src $IP2

echo "ip rule add from $IP1 table T1"
ip rule add from $IP1 table 1

echo "ip rule add from $IP2 table T2" ip rule add from $IP2 table 2


echo "ip route add default scope global nexthop via $P1 dev $IF1 weight 1 nexthop via $P2 dev $IF2 weight 1"
ip route add default scope global nexthop via $IP1 dev $IF1 weight 1 nexthop via $IP2 dev $IF2 weight 1
```

Ilustración 6: Balanceo de Carga

Con este script también se realiza el balanceo para nuestra red y los usuarios de esta no notaran si uno u otro acceso a internet se cae.

Y de esa manera ya hemos compartido internet con los clientes en nuestra red LAN, por lo que para comprobarlo se puede hacer ping con una ip por ejemplo ping 8.8.8.8 y obtendremos el resultado siguiente:

```
root@pablo:/home/pablo# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_req=1 ttl=39 time=131 ms
64 bytes from 8.8.8.8: icmp_req=2 ttl=39 time=200 ms
64 bytes from 8.8.8.8: icmp_req=3 ttl=39 time=2104 ms
64 bytes from 8.8.8.8: icmp_req=4 ttl=39 time=1104 ms
64 bytes from 8.8.8.8: icmp_req=5 ttl=39 time=141 ms
64 bytes from 8.8.8.8: icmp_req=6 ttl=39 time=120 ms
^C
--- 8.8.8.8 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5002ms
rtt min/avg/max/mdev = 120.109/633.858/2104.141/744.943 ms, pipe 3
root@pablo:/home/pablo# ping www.youtube.com
PING youtube-ui.l.google.com (173.194.125.73) 56(84) bytes of data.
64 bytes from mia07s27-in-f9.1e100.net (173.194.125.73): icmp_req=1 ttl=49 time=399 ms
64 bytes from mia07s27-in-f9.1e100.net (173.194.125.73): icmp_req=2 ttl=49 time=399 ms
64 bytes from mia07s27-in-f9.1e100.net (173.194.125.73): icmp_req=3 ttl=49 time=419 ms
^C64 bytes from mia07s27-in-f9.1e100.net (173.194.125.73): icmp_req=4 ttl=49 time=410 ms

--- youtube-ui.l.google.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2999ms
rtt min/avg/max/mdev = 399.602/407.349/419.625/8.360 ms
```

Ilustración 7: comprobando conexión WAN

y también podemos realizar la prueba con nuestra red creada asi:

```
root@pablo:/home/pablo# ping 192.168.1.2
PING 192.168.1.2 (192.168.1.2) 56(84) bytes of data.
64 bytes from 192.168.1.2: icmp_req=1 ttl=64 time=0.261 ms
64 bytes from 192.168.1.2: icmp_req=2 ttl=64 time=0.336 ms
^C
--- 192.168.1.2 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 999ms
rtt min/avg/max/mdev = 0.261/0.298/0.336/0.041 ms
root@pablo:/home/pablo# ping 192.168.1.3
PING 192.168.1.3 (192.168.1.3) 56(84) bytes of data.
64 bytes from 192.168.1.3: icmp_req=1 ttl=64 time=0.277 ms
64 bytes from 192.168.1.3: icmp_req=2 ttl=64 time=0.515 ms
^C
--- 192.168.1.3 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 999ms
rtt min/avg/max/mdev = 0.277/0.396/0.515/0.119 ms
root@pablo:/home/pablo# ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_req=1 ttl=64 time=0.114 ms
64 bytes from 192.168.1.1: icmp_req=2 ttl=64 time=0.070 ms
^C
--- 192.168.1.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1000ms
rtt min/avg/max/mdev = 0.070/0.092/0.114/0.022 ms
root@pablo:/home/pablo#
```

Ilustración 8: Comprobando LAN

Para restringir el protocol icmp en nuestra red interna utilizamos la configuración siguiente:

```
root@pablo:/home/pablo# iptables -F
root@pablo:/home/pablo# iptables -t filter -A OUTPUT -p icmp --icmp-type echo-reply -j DROP
root@pablo:/home/pablo#
```

Ilustración 9: Restringiendo Protocolo

Para restringir una ip para nuestra red interna por ejemplo de de Facebook, ejecutamos los siguientes comandos:

```
root@pablo:/media# iptables -F
root@pablo:/media# iptables -A OUTPUT -d 173.252.100.27 -j DROP
root@pablo:/media# iptables -A OUTPUT -o eth0 -d 192.168.1.0/24 -j DROP
root@pablo:/media# iptables -A OUTPUT -d 192.168.1.0/24 -j DROP
root@pablo:/media# clear
```

Ilustración 10: Restringiendo Ip de facebook a la LAN

por ultimo realizamos un monitoreo de nuestra red a través de la herramienta Munin según el detalle siguiente:

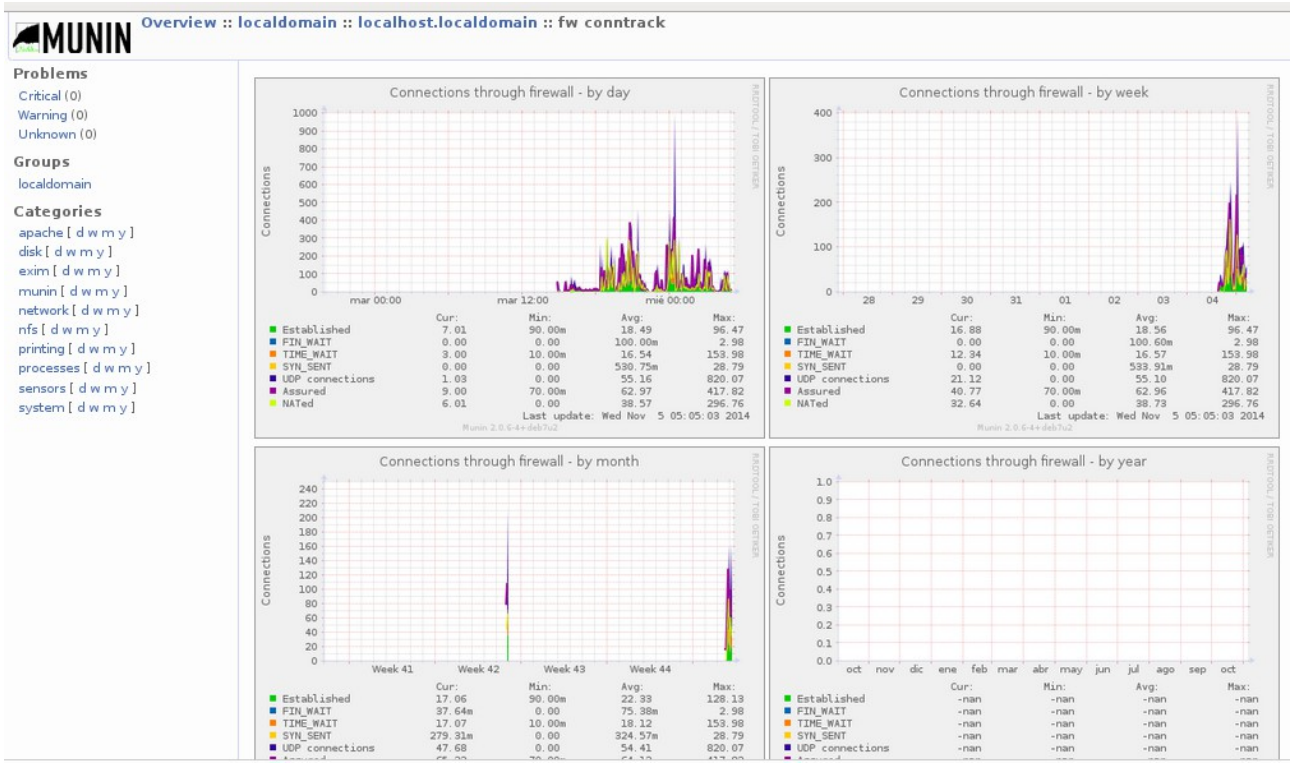

Ilustración 11: Monitoreando Firewall

Ilustración 12: Monitoreando ppp0

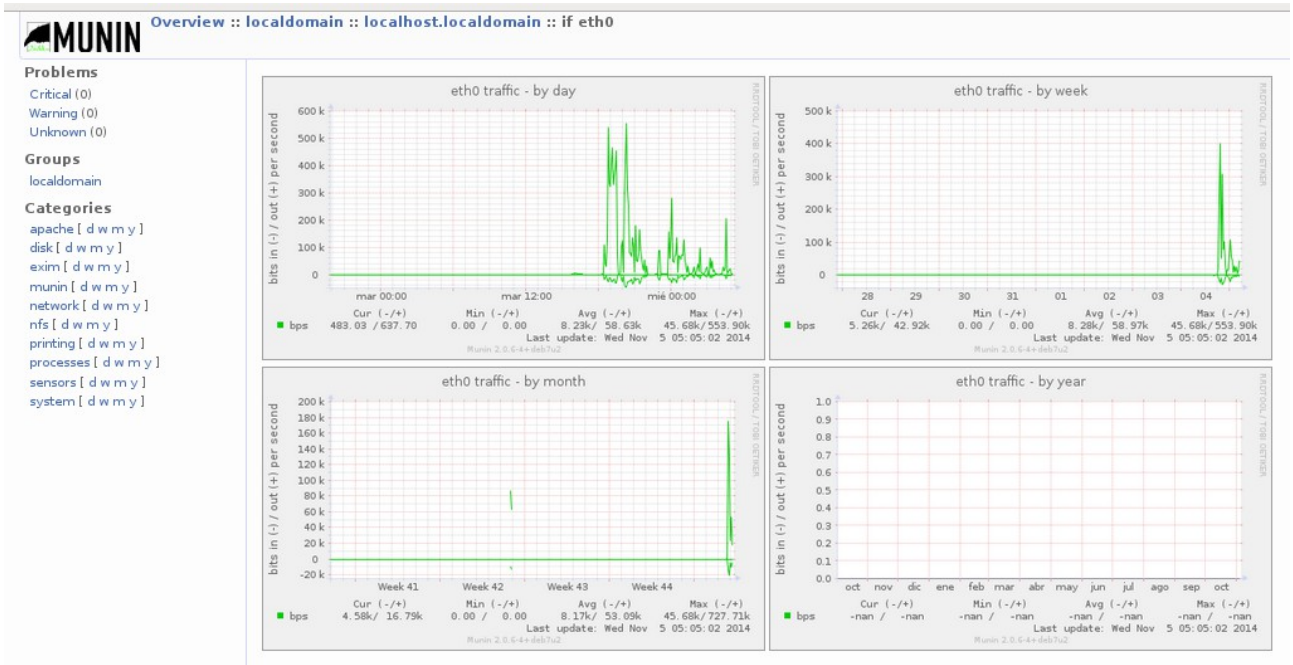

Ilustración 13: Monitoreando la interfaz eth0

En definitiva este seria el trabajo que se hace con la maquina principal que funciona como Firewall/gateway para nuestra red LAN; ahora bien con respecto a los clientes dentro de nuestra red , es sumamente sencillo puesto que solo configuraran la Ip de nuestro bloque y agregaran la puerta de enlace que en este caso sera la ip de la Pc principal o sea 192.168.1.1, de la siguiente manera:

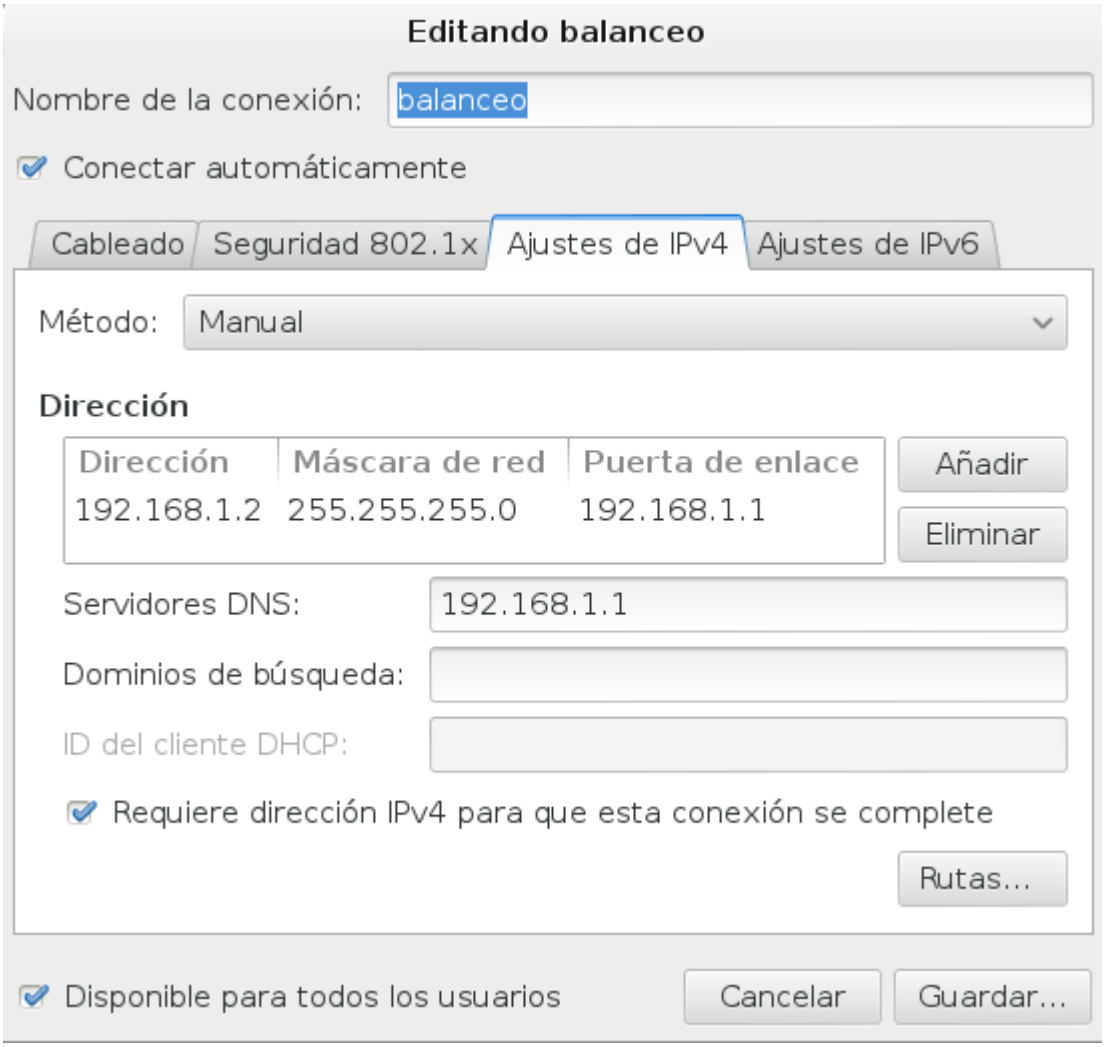

Ilustración 14: Configuración de Cliente a la Red LAN

Debiendo detener y nuevamente dando inicio nuevamentela conexión principal de la siguiente forma:

```
root@YOSILEY:/home/yosiley# /etc/init.d/network-manager stop
[ ok ] Stopping network connection manager: NetworkManager.
root@YOSILEY:/home/yosiley#
```

Ilustración 15: Deteniendo la conexión principal

```
root@YOSILEY:/home/yosiley# /etc/init.d/network-manager start
[ ok ] Starting network connection manager: NetworkManager already started.
root@YOSILEY:/home/yosiley#
```

Ilustración 16: Iniciando conexión principal

Agregamos la puerta de enlace de la siguiente manera:

```
root@YOSILEY:/home/yosiley# route add default gw 192.168.1.1 eth0
root@YOSILEY:/home/yosiley#
```

Ilustración 17: Agregando Ip de puerta de enlace

y listo este procedimiento lo harás con cada nueva Pc que quieras incorporar a la red LAN que hemos creado y esto es todo.

CONCLUSIONES

- Se realizo la recolección de la información, para la configuración del Firewall, con balanceador de dos enlaces a internet dentro de la red LAN, en la cual se ha logrado compartir Internet y Balancear su carga a través de la configuración de Iptables.

- En definitiva hemos logrado realizar las practicas que nos proyectamos y el proyecto se encuentra funcionando tal y como lo proyectamos, creamos la red LAN, posteriormente configuramos el Firewall y el Balanceo de Carga hacia nuestra red.

RECOMENDACIONES

- Con este tipo de proyectos se necesita dedicarles mucho tiempo pero investigando mucho se lograra obtener los resultados esperados, tal y como se proyectan.

- Para lograr los objetivos que te propongas cualquiera que sea la tarea debes ser perseverante y no quedarte esperando la información, sino búscala con empeño y dedicación y lograres cumplir tus metas.

BIBLIOGRAFÍA

1. http://es.wikipedia.org/wiki/Cortafuegos_(informatica). Consultada el 18 de agosto del 2014.

2. “Algunos Firewalls Distribuidos del Mercado” http://www.textoscientificos.com/redes/firewalls-distribuidos/firewalls/distribuidos/mercado. Consultada el 12 de septiembre de 2014.