



UNIVERSIDAD LUTERANA SALVADOREÑA
FACULTAD DE CIENCIAS DEL HOMBRE Y LA NATURALEZA
LICENCIATURA EN CIENCIAS DE LA COMPUTACION

ASIGNATURA

REDES II

TEMA

FIREWALL CON BALANCEADOR DE DOS ENLACES DE INTERNET

CATEDRATICO

ING. MANUEL FLORES VILLATORO

APELLIDOS	NOMBRES	CARNET	APORTACION
CORADO ESCOBAR	PABLO RODRIGO	CE02110289	100%
RAMIREZ ARIAS	WILLIAM GILBERTO	RA02110334	100%

SAN SALVADOR, 08 DE NOVIEMBRE DE 2014

Contenido

INTRODUCCION.....	4
OBJETIVOS	5
OBJETIVO GENERAL.....	5
ESPECIFICOS	5
DESCRIPCION DEL PROYECTO	6
DIAGRAMA DE RED	7
MARCO TEORICO	7
Que es un firewall.	7
Que es un balance de carga	8
MÓDEM.....	8
Características de Iptables.....	10
CORTAFUEGOS QUE HAY:	10
1- IPCop Firewall	10
2- Shorewall.....	10
3- UFW - Firewall sin complicaciones	11
4- Vuurmuur.....	11
5- PfSense.....	11
6- IPFire.....	11
7- SmoothWall y SmoothWall Express	11
8- Endian.....	11
Firewall 9- ConfigServer Seguridad	12
WIRESHARK:	12
Características:	12
TCPDUMP:	13
DESCRIPCION TECNICA A IMPLEMENTAR	15
LISTA DE ACTIVIDADES A REALIZAR.....	15
ALCANCE Y LIMITACIONES.....	16
Factibilidad.	16

DIAGRAMA DE GANT ACTUALIZADO	17
LISTA DE ACTIVIDADES QUE SE REALIZAN.....	18
ALCANCE Y LIMITACIONES.....	19
Factibilidad.....	19
CONFIGURACIONES.....	20
Balanceador de carga.....	20
CONCLUSIONES.....	25
RECOMENDACIONES.....	25
BIBLIOGRAFIA.....	26

INTRODUCCION

En este documento se realizara una de las formas como hacer una configuracion con un firewall con balanceo de carga de dos enlaces a internet, mediante configurar una maquina que podría ser una laptop o una computadora de escritorio, la cual se configurara como router, y es mediante esta máquina que al configurarla para que sea utilizada como servidor configuramos dos modem que pueden ser de la misma o de diferentes compañías telefónicas, con el fin de el trafico de red salga a través de dichas modem a internet y así equilibrar la carga, siendo que si una de estas se cae la otra automáticamente toma su lugar y no dejar perder la conexión a internet,

Y esto se hará además un firewall el cual en este trabajo se hará con iptables, utilizando las reglas para su configuracion y que tome el centro del acceso permitido o no a ciertos sitios en la red,

Utilizando las maquinas con sistemas operativo libres (Linux) en este caso seria debían la configuracion de **Firewall con Balanceador de dos enlaces de Internet,**

OBJETIVOS

OBJETIVO GENERAL

- Configurar el firewall con balanceador de carga de dos enlaces a internet y su posible funcionamiento

ESPECIFICOS

- Saber cómo aplicar el balanceo de carga entre dos enlaces a internet y su funcionamiento
- Estudiar las diferentes formas como configurar la conexión de red a través de modem inalámbricos y su funcionamiento
- Aprender su utilidad sobre el balanceo de carga configurando un iptables para más seguridad en una red

DESCRIPCION DEL PROYECTO

En el presente documento se hablara sobre la configuracion de un firewall con balanceador de carga el cual nos ayudara a controlar el tráfico de las redes que se utiliza dentro del internet, ya que tendremos varios clientes conectados al mismo o tiempo, y se utilizaran dos modem de 3G, además de configurarlos también lo haremos con tres computadoras, una como servidor y dos como clientes, seguido a esto también se instalarán paquetes o programas los cuales nos servirán para realizar aplicaciones como ip router, iptables y wireshark.

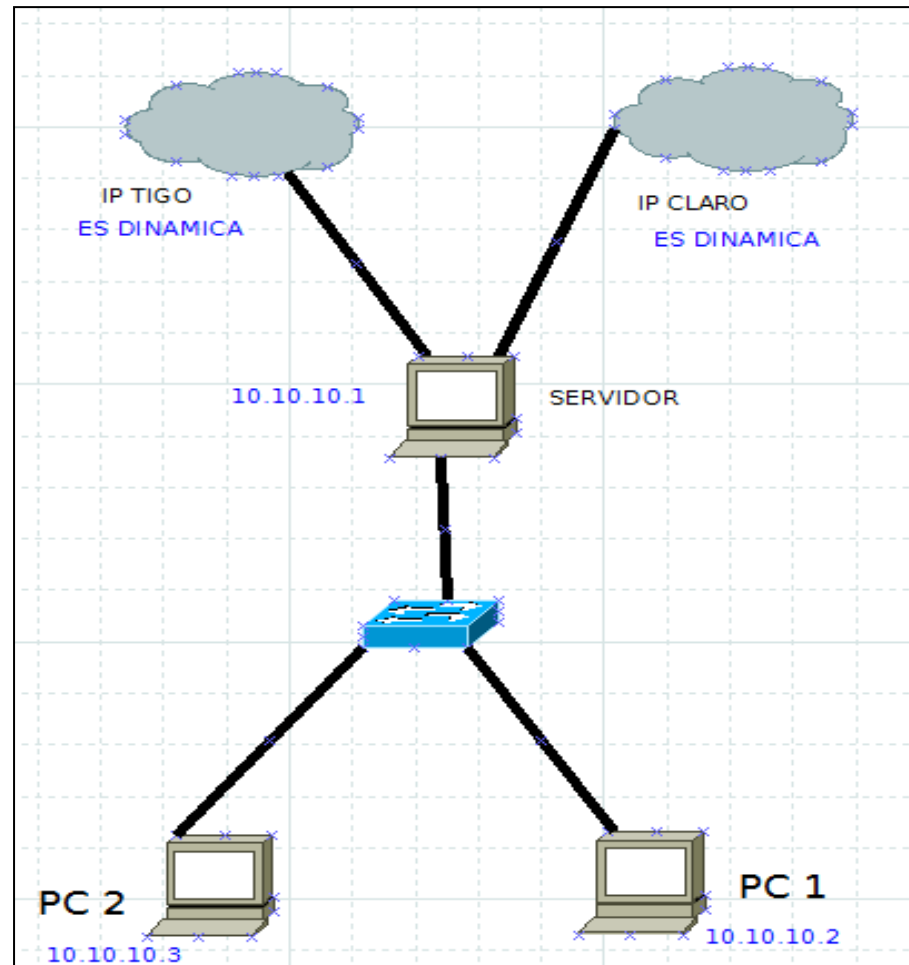
Iproute nos servirá para saber cómo asignar ip a los modem además el balanceo de carga y su asignación de pesos a cada computadora

Iptables: esta es una herramienta que nos servirá como un firewall o filtrar paquetes y que traduce direcciones de red

Wireshark:

Se dice llamar un tiburón de cables antes conocido como Ethereal, es un analizador de protocolos utilizado para realizar análisis y solucionar problemas en redes de comunicaciones, para desarrollo de software y protocolos, y como una herramienta didáctica.

DIAGRAMA DE RED



MARCO TEORICO

Que es un firewall.

Un firewall o cortafuegos es un dispositivo de hardware o un software que nos permite gestionar y filtrar la totalidad de tráfico entrante y saliente que hay entre 2 redes u ordenadores de una misma red.

Básicamente la función de un firewall es proteger los equipos individuales, servidores o equipos conectados en red contra accesos no deseados de intrusos que nos pueden robar datos confidenciales, hacer perder información valiosa o incluso denegar servicios en nuestra red.

Que es un balance de carga

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

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

En un escenario donde hay un balanceo de carga de servidores, hay dos o más servidores Web que evitan la sobrecarga. En el caso de que uno de los servidores reciba mucho tráfico, el balanceador de carga recibe una petición de una página Web, la cual es enviada a un servidor disponible. El servidor disponible entonces responde a la petición, y el tráfico es redirigido a otro servidor que tiene la capacidad de recibir el tráfico entrante. Lo mejor del balanceo de carga es que el sitio Web está arriba y funcionando incluso cuando alguno de los servidores está apagado debido a mantenimiento o un fallo de cualquier tipo. Cuando balanceas el tráfico usando varios servidores y uno de ellos falla, el tráfico simplemente será redirigido a otros servidores que pueden coger las peticiones.

Que son los Módems:

MÓDEM

Es un acrónimo formado por dos términos: modulación y de modulación. Se trata de un aparato utilizado en la informática para convertir las señales digitales en analógicas y viceversa, de modo tal que éstas puedan ser transmitidas de forma

inteligible. De esta manera, su función primordial se relaciona con Internet porque todos los datos que queremos transferir a través de la red necesitan de este dispositivo como si fuera un traductor. Aunque también puede ser utilizado como fax e incluso como medio de contacto con una red local.

IPTABLES QUE ES:

Es un sistema de firewall vinculado al kernel de Linux que se ha extendido enormemente a partir del kernel 2.4 de este sistema operativo. Al igual que el anterior sistema ipchains, un firewall de iptables no es como un servidor que lo iniciamos o detenemos o que se pueda caer por un error de programación iptables está integrado con el kernel, es parte del sistema operativo. ¿Cómo se pone en marcha? Realmente lo que se hace es aplicar reglas.

Para ellos se ejecuta el comando iptables, con el que añadimos, borramos, o creamos reglas. Por ello un firewall de iptables no es sino un simple script de Shell en el que se van ejecutando las reglas de firewall. Las reglas de firewall están a nivel de kernel, y al kernel lo que le llega es un paquete (digamos, un marrón ;) y tiene que decidir qué hacer con él. El kernel lo que hace es, dependiendo si el paquete es para la propia maquina o para otra máquina, consultar las reglas de firewall y decidir que hacer con el paquete según mande el firewall *Redes // 6* se usa para crear, mantener y revisar las tablas de filtrado de paquetes en el kernel de Linux una herramienta de cortafuegos que permite no solamente filtrar paquetes, sino también realizar traducción de direcciones de red (NAT) para IPv4 o mantener registros Cuenta con todas las características estándar de un analizador de protocolos de forma únicamente hueca.

Iptables / Netfilter Es el más popular firewall basado en línea de comandos. Es la primera línea de defensa de una seguridad del servidor Linux. Muchos administradores de sistemas utilizan para puesta a punto de sus servidores. Filtra los paquetes en la pila de red dentro del propio kernel. Puede encontrar una descripción más detallada de Iptables aquí.

Características de Iptables

- ❖ En él se enumeran los contenidos del conjunto de reglas de filtrado de paquetes.
- ❖ Es rápido relámpago, ya que inspecciona sólo los encabezados de los paquetes.
- ❖ Se puede añadir / quitar / modificar las reglas de acuerdo a sus necesidades en los conjuntos de reglas de filtrado de paquetes.
- ❖ Listado / puesta a cero contadores de cada regla de los conjuntos de reglas de filtrado de paquetes.
- ❖ Soporta copia de seguridad y restauración con los archivos.

CORTAFUEGOS QUE HAY:

Entre el cortafuego o el filtro de contenido que se encuentra podemos mencionar, los cuales son de la misma línea del Iptables.

1- IPCop Firewall

IPCop Es una distribución de cortafuegos de código abierto Linux, equipo IPCop está trabajando continuamente para ofrecer un estable, más seguro, el usuario del sistema de gestión de Firewall de usar y altamente configurable a sus usuarios.

IPCop ofrece una interfaz web bien diseñada para administrar el servidor de seguridad. Es muy útil y bueno para las pequeñas empresas y los PC locales.

Puede configurar un PC antiguo como una VPN segura de proporcionar un entorno seguro en internet.

También se mantiene un poco de información que se utiliza con frecuencia para proporcionar una mejor experiencia de navegación web a sus usuarios.

2- Shorewall

Shorewall o Shoreline Firewall es otro servidor de seguridad de código abierto muy popular especializado para GNU / Linux. Está construido sobre el sistema Netfilter integrado en el kernel de Linux que también es compatible con IPV6.

3- UFW - Firewall sin complicaciones

UFW es la herramienta de servidor de seguridad predeterminada para los servidores de Ubuntu, está básicamente diseñado para menor la complejidad del firewall iptables y hace que sea más fácil de usar. Una interfaz gráfica de usuario de la UFW, Gufw también está disponible para los usuarios de Ubuntu y Debian.

4- Vuurmuur

Vuurmuur es otro potente gestor de firewall de Linux incorporado o es propietario de reglas de iptables para su servidor o red. Al mismo tiempo, su muy fácil de usar para administrar, no hay iptables previos conocimientos de trabajo necesarios para utilizar Vuurmuur.

5-. PfSense

PfSense es otro de código abierto y un firewall muy fiable para servidores de FreeBSD. Su basado en el concepto de filtrado de estado de paquetes. Ofrece amplias gamas de característica que normalmente está disponible sólo en los cortafuegos comerciales caros.

6- IPFire

IPFire es otro de los firewalls basados código abierto Linux para Small Office, Home Office (SOHO) entornos. Su diseñado con modularidad y altamente flexibilidad. Comunidad IPFire también se hizo cargo de la Seguridad y la desarrolló como un Stateful Packet Inspection (SPI).

7- SmoothWall y SmoothWall Express

SmoothWall es un servidor de seguridad de código abierto Linux con una interfaz basada en Web altamente configurable. Su interfaz basada en Web que se conoce como WAM (gerente Web Access). Una versión de libre distribución de SmoothWall se conoce como SmoothWall Express.

8- Endian

Firewall Endian es otro cortafuego de estado concepto de Inspección de paquetes basado en que se puede implementar como routers, proxy y puerta de enlace VPN con OpenVPN. Su originalmente desarrollado a partir de cortafuegos IPCop que también es un tenedor de Smoothwall.

Firewall 9- ConfigServer Seguridad

Por último, pero no el último de seguridad y firewall ConfigServer. Es una plataforma cruzada y un Firewall muy versátil, también se basa en el concepto de inspección de estado de paquetes (SPI). Es compatible con casi todos los entornos de virtualización como Virtuozzo, OpenVZ, VMware, Xen, KVM y VirtualBox.

WIRESHARK:

Es uno de esos programas que muchos administradores de red le encantaría ser capaz de utilizar, pero a menudo se les impide conseguir lo que quieren de Wireshark a causa de la falta de documentación.

Wireshark es un analizador de paquetes de red. Un analizador de paquetes de red tratará de capturar paquetes de red y trata de mostrar que los paquetes de datos que se detallan como sea posible.

La funcionalidad que provee es similar a la de tcpdump, pero añade una interfaz gráfica

Software Wireshark captura el tráfico de red y muestra un gráfico con código de color de ese tráfico, por lo que es más conveniente para los administradores de sistemas para detectar ataques de red. Algunos ataques son más sutiles que otros son, pero puede utilizar Wireshark para identificar los intentos de hacking en la red. Examine los resultados con código de color - por ejemplo, el rojo indica la necesidad de atención inmediata y después utilice esta herramienta para investigar más a fondo las posibles amenazas a la red. Instrucciones

Características:

- ❖ Mantenido bajo la licencia GPL.
- ❖ Muy robusto, tanto en modo promiscuo como en modo no promiscuo.

- ❖ Puede capturar datos de la red o leer datos almacenados en un archivo (de una captura previa).
- ❖ Basado en la librería pcap.
- ❖ Tiene una interfaz muy flexible.
- ❖ Gran capacidad de filtrado.
- ❖ Admite el formato estándar de archivos tcpdump.
- ❖ Reconstrucción de sesiones TCP.
- ❖ Se ejecuta en más de 20 plataformas.
- ❖ Es compatible con más de 480 protocolos.
- ❖ Puede leer archivos de captura de más de 20 productos.
- ❖ Puede traducir protocolos TCP IP.
- ❖ Disponible para UNIX y Windows.
- ❖ Captura de paquetes de datos en vivo de una interfaz de red.
- ❖ Importar y exportar datos de paquetes desde y hacia muchos otros programas de captura.
- ❖ Filtrar paquetes en muchos criterios.
- ❖ Colorear muestra de los paquetes en base a filtros.

TCPDUMP:

Es una herramienta en línea de comandos cuya utilidad principal es analizar el tráfico que circula por la red.

Permite al usuario capturar y mostrar a tiempo real los paquetes transmitidos y recibidos en la red a la cual el ordenador está conectado

Por el momento se ha diseñado un perfil de nuestro proyecto final, el cual contempla un tiempo prudencial, el cual nos enviar para investigar acerca del tema en cuestión su desarrollo.

Protocolos a utilizar

FCS

(Frame Check Sequence). Campo de 4 bytes (32 bits) que contiene un valor de verificación CRC. El emisor calcula el CRC de toda la trama, desde el campo destino al campo CRC suponiendo que vale 0. El receptor lo recalcula, si el valor calculado es 0 la trama es válida.

IP (Internet Protocol) es un protocolo no orientado a conexión usado por el origen y el destino para la comunicación de datos a través de una red de paquetes conmutados.

TCP (Transmisión Control Protocol)

TCP es uno de los principales protocolos de la capa de transporte del modelo TCP/IP. En el nivel de aplicación, posibilita la administración de datos que vienen o van al nivel inferior del modelo OSI (IP).

Consulta ARP

Durante la captura de tráfico, se logra capturar la consulta ARP de un equipo que intenta obtener la dirección MAC del Default Gateway. Esta consulta se realiza en dos pasos

Sesión TCP

Establecimiento de conexión (handshake de tres vías) A continuación, procedemos a identificar el inicio de sesión TCP (handshake de tres vías), reconocidos en los paquetes 208, 209 y 210.

Se debe tener en cuenta que las direcciones destino registradas por Wireshark son las direcciones locales del Proxy de navegación utilizado (172.19.34.96) y no las IP de Internet propiamente tal

DESCRIPCION TECNICA A IMPLEMENTAR

N°	DETALLE	CANTIDAD	PRECIO
1	Computadoras	3	\$1200.00
2	modem	2	\$44.00
3	switch	1	\$22.00
4	cables	3	\$2.10
5	Conectores rj45	6	\$1.50
6	ponchadora	1	\$12.00
7	internet	2	\$25.00

LISTA DE ACTIVIDADES A REALIZAR

1. configuración de interfaz de redes desde la terminal

```
ifconfig ethn dirección_ip/marcada_subred up
```

```
nano /etc/network/interfaces
```

2. configuración de la computadora como router

```
nano /proc/sys/net/ipv4/conf/all/forwarding
```

```
nano /etc/sysctl.conf, para que la configuración no se pierda cuando se reinicie o se apague la máquina net.ipv4.ip_forward=1
```

3. creación de tablas

```
nano /etc/iproute2/rt_tables[
```

4. Configuración de reglas de navegación

Estas son las que escogen qué tabla de rutas se utiliza, con una estructura de una regla como la siguiente:

```
ip rule add from direccion_origen/mascara_subred priority prioridad_regla  
table nombre_tabla.
```

Ejemplo. `ip rule add from 172.16.0.0/24 priority 100 table tigo.`

Las reglas de navegación serán asignadas en el archivo.
`/etc/network/interfaces`

ALCANCE Y LIMITACIONES

Factibilidad.

Se cuentan con los conocimientos básicos en el funcionamiento de redes informáticas. Además se tiene acceso a las herramientas a utilizar. Ya que están al alcance de cualquier persona que las quiera utilizar sistemas operativos libres Ya que no ocasionaran mayores gastos de los necesarios, la cual la hace factible para la implementar nuestro Proyecto.

Sobre las limitaciones técnicas o financieras para el desarrollo del proyecto, debido a la naturaleza del las herramientas utilizadas en el software libre. Se puede determinar que el proyecto es viable ya que este tipo de configuraciones son indispensables en las empresas o instituciones para mantener controlados a sus empleados y así no hacer mal uso del servicio de internet y mejorar el aprovechamiento de esta herramienta que es muy importante dentro de toda organización. Y que además se cuentan con los recursos necesarios para llevar a cabo este trabajo.

DIAGRAMA DE GANT ACTUALIZADO

ACTIVIDADES	Agosto				Septiembre				Octubre				Noviembre				Diciembre			
	Semanas				semanas				Semanas				semanas				semanas			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1. Investigación sobre el tema																				
2. Elaboración de perfil																				
3. configuración de las computadoras interfaz de redes																				
4. configurar computadoras como router																				
5. creación de tablas																				
6. configuración de reglas de navegación																				
7. primeras pruebas sobre la configuración																				
8. instalación de paquetes en debían																				
8. configuración de los modem																				
10. realizar pruebas de conectividad																				
11. investigación más a fondo sobre configuración																				
12- configuración de la puerta de entradas de las modem																				
13- errores que se dieron al configurar debían																				
14- pruebas con el programa Wireshark																				
15- capturas de pantalla de los paquetes																				
16- configurar iptables																				
17- instalar y configurar Munin																				
18- instalar WvDial para compartir internet																				
19- realizar pruebas de conectividad con Munin																				
20- tratar de configurar modem para compartir internet																				
21- instalación y configuración de proxy con Squid																				
22- realizar pruebas con la conectividad																				
23- entrega final																				

LISTA DE ACTIVIDADES QUE SE REALIZAN

CONFIGURACIÓN DE LAS COMPUTADORAS INTERFAZ DE REDES

Esto con el fin de de instalar los programas adecuados para realizar el proyecto que se pretende diseñar y su buen funcionamiento

CONFIGURAR COMPUTADORAS COMO ROUTER

Se configuraron las dos computadoras con sus respectivas ip, con el fin de hacer la conectividad con el servidor todos con el sistema debían 7

PRIMERAS PRUEBAS SOBRE LA CONFIGURACIÓN

Se realizaron las primeras pruebas solo con una computadora portátil ya que por el momento no se contaba con la otra y si efectivamente la conectividad entre ambas está funcionando hacen esto con wireshark y con ping

CONFIGURACION DE LOS MODEM

Se configuraron los modem de la compañía tigo y el otro de al compañía claro con el fin de asignarles un a puerta de entrada para realizar el balanceo de carga

INVESTIGACIÓN MÁS A FONDO SOBRE CONFIGURACIÓN

Se investigo más a fondo sobre el proyecto donde se logro descubrir que no solo hay un cortafuego o filtro de contenido sino diez y que son aplicados al sistema operativo Linux

Con sus características

ERRORES QUE SE DIERON AL CONFIGURAR DEBÍAN

Se cometieron varios errores ya que al configurar el servidor estaba conectado a la computadora del cliente mediante un switch y se eliminaron varios programas instalados en la computadora del cliente.

ALCANCE Y LIMITACIONES

Factibilidad.

Se cuentan con los conocimientos básicos en el funcionamiento de redes informáticas. Además se tiene acceso a las herramientas a utilizar. Ya que están al alcance de cualquier persona que las quiera utilizar sistemas operativos libres Ya que no ocasionaran mayores gastos de los necesarios, la cual la hace factible para la implementar nuestro Proyecto.

Sobre las limitaciones técnicas o financieras para el desarrollo del proyecto, debido a la naturaleza del las herramientas utilizadas en el software libre. Se puede determinar que el proyecto es viable ya que este tipo de configuraciones son indispensables en las empresas o instituciones para mantener controlados a sus empleados y así no hacer mal uso del servicio de internet y mejorar el aprovechamiento de esta herramienta que es muy importante dentro de toda organización. Y que además se cuentan con los recursos necesarios para llevar a cabo este trabajo.

Esta es la tabla de información de las IPs que vamos a signar a las maquinas clientes y el servidor

DISPOSITIVO	INTERFAZ	DIRECCION IP	MASCARA DE SUBRED	PUERTA DE ENLACE
Servidor	Eth0	10.10.10.1	255.255.255.0	10.64.64.64 10.64.64.65
	PPP0	IP Dinámica	No Asignada	No Asignada
	ppp1	IP Dinámica	No Asignada	No Asignada
PC1	eth0	10.10.10.2	255.255.255.0	10.10.10.1
PC2	eth0	10.10.10.3	255.255.255.0	10.10.10.1

Las modem USB que van a estar conectadas adquieren IPs dinámicas y cambian continuamente. Por eso siempre la cambiaremos al empezar a trabajar

CONFIGURACIONES

Instalamos iptable

iptables: (es el nombre de la herramienta de espacio de usuario mediante la cual el administrador puede

Definir políticas de filtrado del tráfico que circula por la red.)

aptitude install iptables

Ejecutas estos comandos para compartir internet.

iptables -flush significa que F -flush → borra todas las reglas de una cadena.

iptables --table nat --flush

iptables --table nat --append POSTROUTING --out-interface ppp0 -j

MASQUERADE esto significa aceptar politicas de la interfaz ppp0

iptables --table nat --append POSTROUTING --out-interface ppp1 -j

MASQUERADE significa out interface la regla se aplica a una interfaz de destino.

iptables --append FORWARD --in-interface eth0 -j ACCEPT significa hacia adelante en las interfaces eth0 aceptar

ip route del default significa la ruta de la ip por defecto

Balancedor de carga

Ya configurados los módem, pasamos a hacer el balanceo de carga para que cada vez que los clientes lo

Deseen puedan acceder a Internet.

nano enrutamiento.sh

y lo ajustamos según convenga

```
#!/bin/bash
```

```
IF1=ppp0
```

```
IF2=ppp1
```

```
IP1=10.26.40.65
```

IP2=10.147.71.178

P1=10.64.64.64

P2=10.64.64.65

P1_NET=10.26.40.65

P2_NET

Todo esto se empezó a configurar con el fin de poder utilizarlo al momento de hacer el balanceo de carga además, asignar las ip a los diferentes herramientas a utilizar,

ESTE SCRIP ES EL QUE UTILIZAMOS PARA REALIZAR EL BALANCEO DE CARGA

Utilizando en enutamiento.sh y guardándolo en nuestro servidor

```
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 default via $P2 table 2" ip route add default via $P2 table 2
```

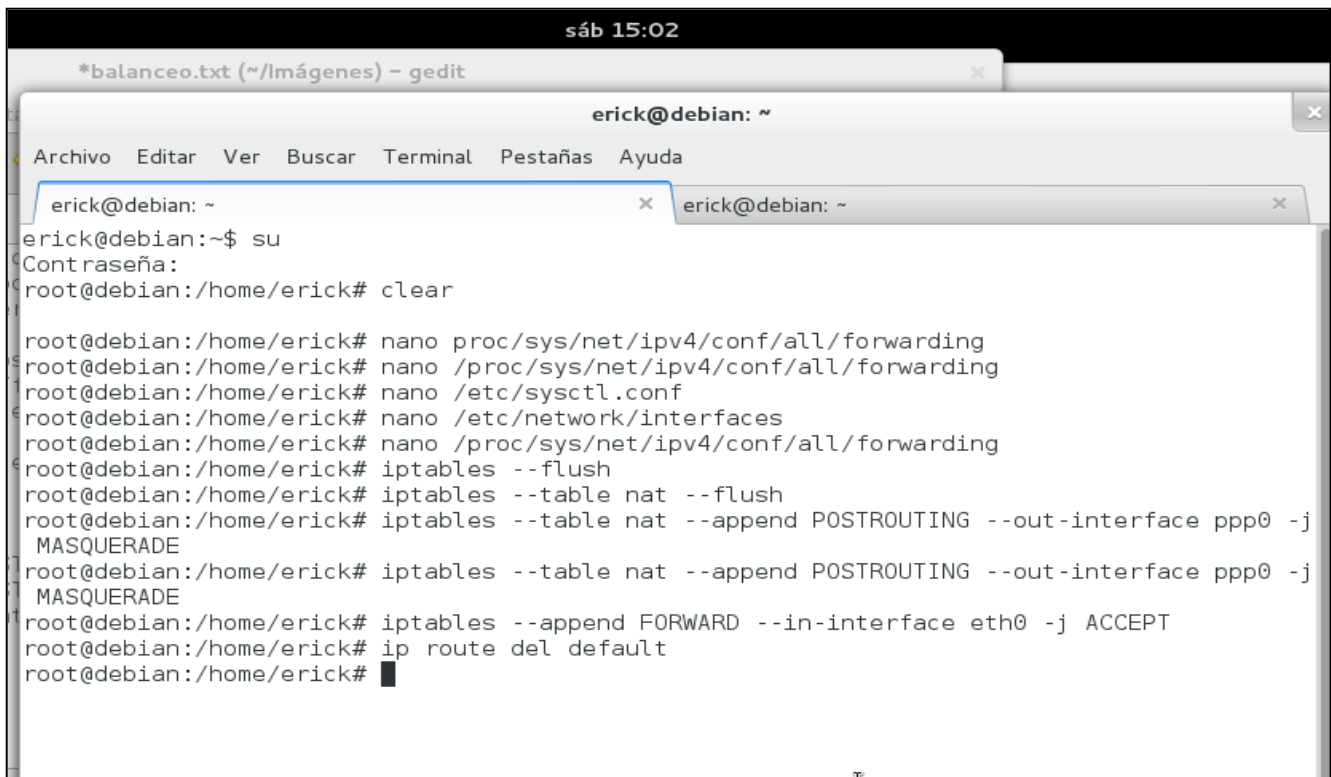
```
echo "ip route add $P1_NET dev $IF1 src $IP1" ip route add $P1_NET dev $IF1 src $IP1
```

```
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 \$P1 dev \$IF1 weight 1 nexthop via \$P2 dev \$IF2 weight 1



The screenshot shows a terminal window titled "erick@debian: ~" with a menu bar containing "Archivo", "Editar", "Ver", "Buscar", "Terminal", "Pestañas", and "Ayuda". The terminal output shows the following sequence of commands and responses:

```
erick@debian: ~  
erick@debian:~$ su  
Contraseña:  
root@debian:/home/erick# clear  
  
root@debian:/home/erick# nano /proc/sys/net/ipv4/conf/all/forwarding  
root@debian:/home/erick# nano /proc/sys/net/ipv4/conf/all/forwarding  
root@debian:/home/erick# nano /etc/sysctl.conf  
root@debian:/home/erick# nano /etc/network/interfaces  
root@debian:/home/erick# nano /proc/sys/net/ipv4/conf/all/forwarding  
root@debian:/home/erick# iptables --flush  
root@debian:/home/erick# iptables --table nat --flush  
root@debian:/home/erick# iptables --table nat --append POSTROUTING --out-interface ppp0 -j MASQUERADE  
root@debian:/home/erick# iptables --table nat --append POSTROUTING --out-interface ppp0 -j MASQUERADE  
root@debian:/home/erick# iptables --append FORWARD --in-interface eth0 -j ACCEPT  
root@debian:/home/erick# ip route del default  
root@debian:/home/erick#
```

COMO PODEMOS OBSERVAR AQUI SE ENCUENTRÁ EL COMANDO

nano /proc/sys/net/ipv4/conf/all/forwarding

Este nos sirve para poner como router nuestra PC

Nos abre una pantalla y colocamos el numero uno por el cero

También se puede hacer de la siguiente forma

Nano /etc/sysctl.conf y descomentamos para que quede libre donde dice ipv4

```
sáb 15:19
Google - Iceweasel
erick@debian: ~
Archivo Editar Ver Buscar Terminal Pestañas Ayuda
erick@debian: ~
GNU nano 2.2.6 Fichero: /etc/network/interfaces

# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

#allow-hotplug eth0

auto eth0
iface eth0 inet static
address 10.10.10.1
netmask 255.255.255.0
gateway 10.10.10.1
dns-nameserver 10.10.10.1

[ 18 líneas escritas ]
^G Ver ayuda   ^O Guardar     ^R Leer Fich   ^Y Pág Ant     ^K CortarTxt   ^C Pos actual
^X Salir       ^J Justificar  ^W Buscar     ^V Pág Sig    ^U PegarTxt    ^T Ortografía
```

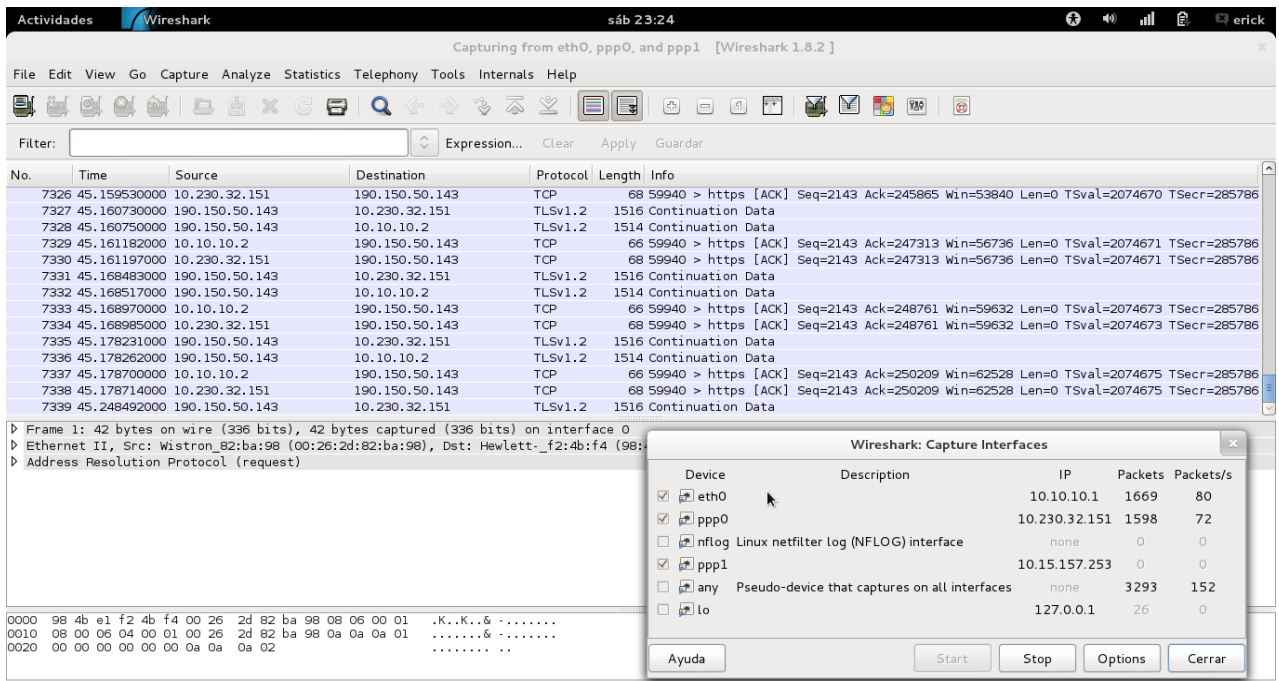
Seguido a esto colocamos otro comando nano /etc/network/interfaces

Este nos sirve para configurar nuestras interfaces de red

```
sáb 15:21
Google - Iceweasel
erick@debian: ~
Archivo Editar Ver Buscar Terminal Pestañas Ayuda
erick@debian: ~
erick@debian: ~
--- 8.8.8.8 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5004ms
rtt min/avg/max/mdev = 168.114/199.569/268.429/33.383 ms
root@debian:/home/erick# ping 10.10.10.2
PING 10.10.10.2 (10.10.10.2) 56(84) bytes of data.
64 bytes from 10.10.10.2: icmp_req=1 ttl=64 time=0.437 ms
64 bytes from 10.10.10.2: icmp_req=2 ttl=64 time=0.383 ms
64 bytes from 10.10.10.2: icmp_req=3 ttl=64 time=0.407 ms
64 bytes from 10.10.10.2: icmp_req=4 ttl=64 time=0.338 ms
64 bytes from 10.10.10.2: icmp_req=5 ttl=64 time=0.320 ms
64 bytes from 10.10.10.2: icmp_req=6 ttl=64 time=0.392 ms
64 bytes from 10.10.10.2: icmp_req=7 ttl=64 time=0.408 ms
^C
--- 10.10.10.2 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 5998ms
rtt min/avg/max/mdev = 0.320/0.383/0.437/0.043 ms
root@debian:/home/erick# nano /etc/network/interfaces
root@debian:/home/erick# ping www.google.com
PING www.google.com (64.233.176.147) 56(84) bytes of data.
64 bytes from 64.233.176.147: icmp_req=1 ttl=35 time=459 ms
64 bytes from 64.233.176.147: icmp_req=2 ttl=35 time=357 ms
64 bytes from 64.233.176.147: icmp_req=3 ttl=35 time=505 ms
64 bytes from 64.233.176.147: icmp_req=4 ttl=35 time=1303 ms
^C64 bytes from 64.233.176.147: icmp_req=5 ttl=35 time=777 ms

--- www.google.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 19158ms
rtt min/avg/max/mdev = 357.135/680.673/1303.652/341.057 ms, pipe 2
root@debian:/home/erick#
```

Aquí podemos observar al hacer ping a la maquina cliente que es la 10.10.10.2
 Y a www.google.com y nos funciona, quiere decir que tenemos comunicación a internet



Aquí podemos ver lo que captura wireshark la PC 10.10.10.2 que ha hecho contacto con nuestra maquina servidor.

Adema le agregamos a la maquina cliente el comando route add default gw y la ip que seria en nuestro caso 10.10.10.1 eth0, esto es para la puerta de enlace, esto hay que verificarlo cada vez que manipulemos la red cableada porque lo desconfigure y no nos da salida a internet.

CONCLUSIONES

En conclusión podemos decir como equipo que al trabajar en este tipo de proyectos nada está escrito ya que es muy interesante conocer como configurar un firewall o cortafuego, junto a un balanceador de carga de dos enlaces de Internet, pero en nuestro caso no ha sido nada fácil ya que la configuración de los modem USB si se logro realizar dentro del servidor, el cuales utilizo una PC con el sistema operativo debían.

Además podemos decir que es muy interesante este tipo de trabajos ya funcionando como se debe dentro de una organización para llevar un mejor control de las personas que ingresan a cualquier sitio de la web y sobre todo crear una mayor seguridad para nuestro equipos y la información que se maneja dentro de esas corporaciones.

RECOMENDACIONES

Como primer punto una buena recomendación seria que se necesita un poco de más ayuda al buscar este tipo de trabajos, ya que es bastante complejo y no se encuentra información ordenada.

Otra recomendación seria de que al implementar este tipo de trabajos hay que tener mucho cuidado con los equipos que estemos utilizando ya que lo mas probable es que se desconfigure lo que está haciendo y en su peor de los casos es perder mucha información al dañar el equipo con algún comando mal ingresado al sistema.

BIBLIOGRAFIA

NAT en Linux Como realizar NAT iptables en Linux

<http://www.taringa.net/posts/linux/16630880/NAT-en-linux-Como-realizar-NAT-iptables-en-linux.html> consultada el 31/10/2014

Aulas en red, aplicaciones y servicios. Linux

http://www.ite.educacion.es/formacion/materiales/85/cd/linux/m6/cortafuegos_iptables.html

Consultado el día 05/11/2014

Encaminamiento con varios enlaces de salida / proveedores

<http://lartc.org/howto/lartc.rpdb.multiple-links.html>

consultada el día 29/10/2014

IPTABLES en 21 segundos

http://www.pello.info/filez/IPTABLES_en_21_segundos.html

Consultada el día 30/10/2014.

netfilter / iptables dividen acceso con múltiples proveedores de Internet

<https://translate.google.com/translate?sl=en&tl=es&js=y&prev=t&hl=es&ie=UTF-8&u=http%3A%2F%2Fwww.iodigitalsec.com%2Fnetfilter-iptables-split-access-with-multiple-isps%2F&edit-text=>

Consultada el día 07/11/2014

Conección a internet con 2 ISP`s, Balanceo de Carga

<http://www.taringa.net/posts/hazlo-tu-mismo/16780262/Coneccion-a-internet-con-2-ISP-s-Balanceo-de-Carga.html>

Consultada el día 29/10/2014