UNIVERSIDAD LUTERANA SALVADOREÑA

FACULTAD DE CIENCIAS DEL HOMBRE Y LA NATURALEZA

Cátedra:

Redes II

Docente:

Ing. Manuel de Jesús Flores

Tema:

Implementación de firewall

Estudiante

Carnet	Apellidos	Nombres
GG02110806	Gámez Gámez	Noris Marbelis

San Salvador, 21 de Agosto de 2015

Contenido

TABLA DE ILUSTRACIONES

INTRODUCCIÓN

En este documento puedes encontrar como configurar un firewall con iptables ya que prácticamente consiste en filtrar o controlar los puntos de acceso, en este caso hemos utilizado dos interfaces de red y

realizar las configuraciones correspondientes a cada proceso tanto de las interfaces de red de cliente como la del servidor al igual encontraras como hacer un balance de carga y poder probarlo con wireshark.

En todo entorno es importante que exista un control y por supuesto que exista seguridad en los servidores ya que en ellos están las utilidades más importantes de las empresas o de manera muy personal. Al aplicar esta herramienta con iptables puedes aplicar las reglas que mejor te convengan o que creas tu que son las indicadas permitiendo o negando acceso a protocoles en la red. Esta es una de las mejores medidas de seguridad con solo un par de comandos pues permiten decirle al kernel qué hacer con ciertos paquetes que cumplan con ciertas características si lo deja pasar, lo acepta, lo modifica.

OBJETIVOS

Objetivo general.

- Configurar un firewall por medio de IPTABLES, utilizando dos enlaces de internet; para compartir internet a los clientes conectados dentro de una red LAN

Objetivos específicos.

- Aplicar reglas y políticas de IPTABLES para los buenos funcionamientos del firewall

- Configurar una computadora como Reuter para las aplicaciones de las reglas y políticas del IPTABLES

- Configurar el balanceo de carga de los dos enlaces de internet por medio para garantizar la disponibilidad de internet en los equipos clientes

MARCO TEÓRICO

¿Que es un firewall?

Un firewall también es conocido como muro de fuego, este funciona entre las redes conectadas permitiendo o denegando las comunicaciones entre dichas redes. Un firewall también es considerado un filtro que controla el tráfico de varios protocolos como TCP/UDP/ICMP que pasan por el para permitir o denegar algún servicio, el firewall examina la petición y dependiendo de este lo puede bloquear o permitirle el acceso.

Un firewall puede ser un dispositivo de tipo Hardware o software que se instala entre la conexión a Internet y las redes conectadas en el lugar.

La Figura.

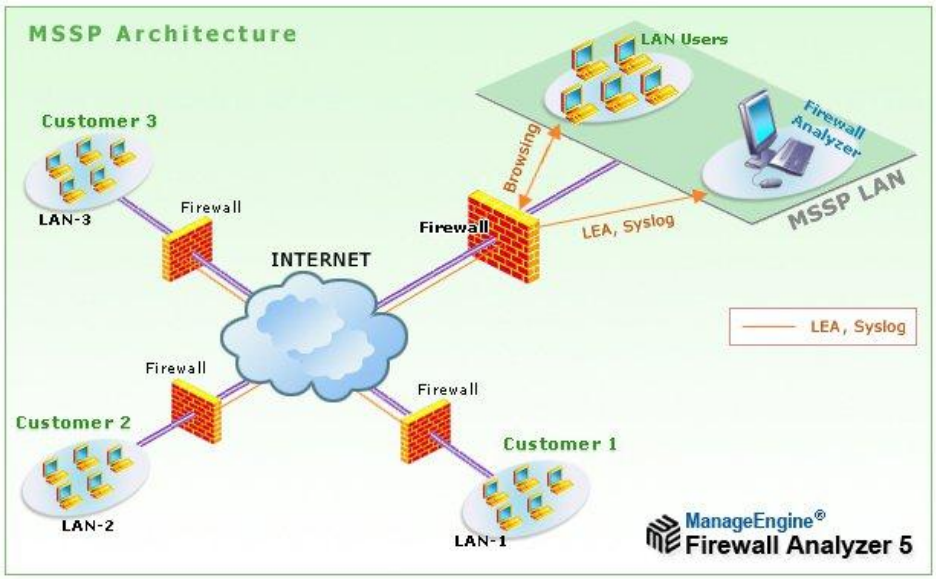


Ilustración 1 ilustra un esquema común de firewall

Sea el tipo de firewall que sea, generalmente no tendrá más que un conjunto de reglas en las que se examina el origen y destino de los paquetes del protocolo tcp/ip. En cuanto a protocolos es probable que sean capaces de filtrar muchos tipos de ellos, no solo los tcp, también los udp, los icmp, los gre y otros

protocolos vinculados a vpns. Este podría ser (en pseudo−lenguaje) un el conjunto de reglas de un firewall del primer gráfico:

Política por defecto ACEPTAR.

Todo lo que venga de la red local al firewall ACEPTAR

Todo lo que venga de la ip de mi casa al puerto tcp 22 ACEPTAR

Todo lo que venga del exterior al puerto tcp 1 al 1024 DENEGAR

Todo lo que venga del exterior al puerto tcp 3389 DENEGAR

Todo lo que venga del exterior al puerto udp 1 al 1024 DENEGAR

Hay dos maneras de implementar un firewall:

Política por defecto ACEPTAR: en principio todo lo que entra y sale por el firewall se acepta y solo se denegará lo que se diga explícitamente.

Política por defecto DENEGAR: todo esta denegado, y solo se permitirá pasar por el firewall aquellos que se permita explícitamente.

Beneficios:

Mayor ancho de Banda:

Varias conexiones simultáneas, en promedio, todas juntas tienen acceso a un mayor ancho de banda, que se extenderá a la suma de los anchos de banda de Internet de todos los enlaces que están siendo equilibrados.

Tolerancia a Fallos:

Cuando tenemos una o más conexiones y cuando falla una salimos automáticamente por la otra que sí que funcione. Si una de las líneas falla, el Routers continua automáticamente la conexión utilizando exclusivamente la segunda.

Balanceo de Carga:

Se puede repartir ancho de banda, podemos usar una conexión a internet para un propósito y la segunda para otro.

Iptables:

Iptables permite al administrador del sistema definir reglas acerca de qué hacer con los paquetes de red. Las reglas se agrupan en cadenas: cada cadena es una lista ordenada de reglas. Las cadenas se agrupan en tablas: cada tabla está asociada con un tipo diferente de procesamiento de paquetes.

Cada regla especifica que paquetes la cumplen (match) y un destino que indica que hacer con el paquete si este cumple la regla. Cada paquete de red que llega a una computadora o que se envía desde una computadora recorre por lo menos una cadena y cada regla de esa cadena se comprueba con el paquete. Si la regla cumple con el datagrama, el recorrido se detiene y el destino de la regla dicta lo que se debe hacer con el paquete. Si el paquete alcanza el n de una cadena predefinida sin haberse correspondido con ninguna regla de la cadena, la política de destino de la cadena dicta que hacer con el paquete. Si el paquete alcanza el fin de una cadena definida por el usuario sin haber cumplido ninguna regla de la cadena o si la cadena definida por el usuario está vacía, el recorrido continúa en la cadena que hizo la llamada (lo que se denomina implicit target RETURN o RETORNO de destino implícito). Solo las cadenas predefinidas tienen políticas. En iptables, las reglas se agrupan en cadenas. Una cadena es un conjunto de reglas para paquetes IP, que determinan lo que se debe hacer con ellos.

Modem

El modem USB 3G, una especie de modem inalámbrico de tipo WiFi, utiliza la red de los operadores de telefonía para conectarse a Internet. Al igual que los teléfonos móviles, el modem USB 3G posee un lugar reservado para una tarjeta SIM. Para que funcione, es necesario que previamente se haya suscrito a un plan en un operador de telefonía

Balanceo de Carga

La Solución de balanceo de carga permite dividir las tareas que tendría que soportar una única máquina, con el fin de maximizar las capacidades de proceso de datos, así como de ejecución de tareas. Esta Solución permite que ningún equipo sea parte vital del servicio que queremos ofrecer. De esta forma evitamos sufrir una parada del servicio debido a una parada de una de las maquinas.

El balanceo de carga nos permite tener mayor ancho de banda; eso no significa que se tenga mayor velocidad de carga o descarga, si no que como se mencionó anteriormente, el trabajo se divide entre los IPS conectados, es decir que si se tienen 2 ISPś (como nuestro caso) el tráfico se distribuirá entre los 2 ISPś.

NAT

Usada cuando se desea hacer los paquetes sean enrutados a una máquina cliente dentro de una red local, pero también podremos enmascarar un red local y tener salida hacia internet.

Una vez abordados los conceptos abordados previamente pasamos a dar solución a nuestra problemática.

Wireshark

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. Cuenta con todas las características estándar de un analizador de protocolos de forma únicamente hueca.

La funcionalidad que provee es similar a la de tcpdump, pero añade una interfaz gráfica y muchas opciones de organización y filtrado de información. Así, permite ver todo el tráfico que pasa a través de una red (usualmente una red Ethernet, aunque es compatible con algunas otras) estableciendo la configuración en modo promiscuo.

Permite examinar datos de una red viva o de un archivo de captura salvado en disco. Se puede analizar la información capturada, a través de los detalles y

sumarios por cada paquete. Wireshark incluye un completo lenguaje para filtrar lo que queremos ver y la habilidad de mostrar el flujo reconstruido de una sesión de TCP.

Munin

Es un programa de monitorización de servidores que genera estadísticas sobre su funcionamiento de los recursos de nuestros servidores, como memoria, disco duro y servicios. Utiliza las herramientas RRDTool para generar gráficas de rendimiento de los parámetros del sistema analizados. Utiliza una interfaz web para mostrar las gráficas generadas, permite trabajar de forma distribuida, mostrando la información de varios servidores. Para ello se instala en una SERVER la parte servidora de Munin y en el resto la parte cliente, que mandará los datos recopilados al servidor para que éste los muestre. Está hecho en perl y permite el uso de plugins, lo cual lo hace realmente versátil.

wvdial

Es una utilidad que ayuda a realizar conexiones a Internet basadas en módem y que se incluye en algunas distribuciones de GNU/Linux importantes.

wvdial es un marcador de Protocolo Punto-a-Punto: marca con un módem y comienza pppd en orden a conectar aInternet. Cuando comienza wvdial, primero carga su configuración de /etc/wvdial.conf que contiene la información básica sobre el puerto del módem, velocidad, y cadena init (de inicialización), así como información sobre el ISP, como el número de teléfono, nombre de usuario y contraseña.

Descripción de proyecto

El proyecto que se implementará consiste configurar un **Firewall** ó llamado también **Cortafuegos con iptables** , utilizando dos interfaces de red que serían en este caso dos modem en donde el propósito es que se conecten y compartan internet con el cliente a partir de cualquier interface, utilizando un balance entre las dos interfaces simulando la caída de cualquier de ellas con el propósito de que el cliente no sepa tal hecho además de eso con la red y firewall lo que se busca es que el servidor pueda controlar el flujo de datos en donde aplicara políticas a su conveniencia.

Diagrama de red

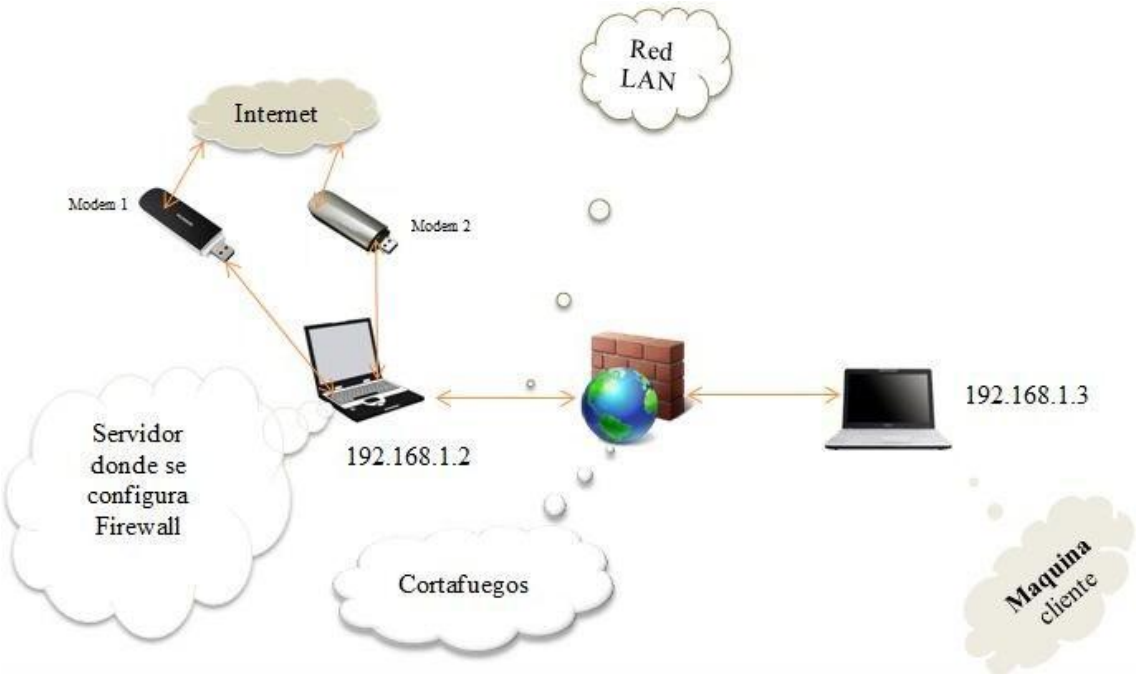


Ilustración 2 diagrama de red

Lista de actividades

1. Buscar y analizar información pertinente al tema.
2. Realizar el perfil de proyecto
3. Instalar los sistemas base en las computadoras a usar.
4. Realizar los cables de red a utilizar
5. Busca de información acerca de las configuraciones que se necesitan hacer.
6. Configurar la computadora que se utilizara como router o servidor
7. Configurar la interfaz de red con wvdial
8. Verificar la funcionalidad de las interfaces de red
9. Configuración de maquina cliente
10. Configurar las reglas de navegación
11. Instalar los programas de monitoreo
12. Documentar el proceso de implementación
13. Realizar pruebas de funcionalidad
14. Entrega de proyecto
15. Diagrama de actividades

Diagrama de actividades

Actividades	*agosto*			*Septiembre*				*Octubre*				*Noviembre*			
	2	*3*	*4*	*1*	*2*	*3*	*4*	*1*	*2*	*3*	*4*	*1*	*2*	*3*	*4*
Buscar y analizar información pertinente al tema			*x*	*x*											
Realizar el perfil de proyecto					*x*										
Instalar los sistemas base en las computadoras a usar						*x*									
Realizar los cables de red a utilizar							*x*								
Busca de información acerca de las configuraciones que se necesitan hacer.								*x*							
Configurar la computadora que se utilizara como								*x*							
Realizar prueba de funcionalidad									*x*						
Configura las interfaces del cliente									*x*						
Configurar los modem con wvdial										*x*					
Realizar prueba de funcionalidad										*x*					
Instalar los programas de monitoreo											*x*				
Configurar las reglas de navegación												*x*			
Realizar pruebas de funcionalidad												x			
Realizar documento													*x*		
Entrega y defensa de proyecto														x	

Viabilidad de proyecto

Factibilidad técnica:

Es posible el realizarlo porque se cuentan con los conocimientos necesarios de redes informáticas para la operatividad, además de conocer las funcionalidades de cada dispositivo a usar.

Factibilidad económica.

Si nos referimos a los sistemas operativos, no los compraremos porque usaremos sistemas de código abierto ahí se ahorraría mucho. Solamente se comprarían los dispositivos hardware (CABLES UTP, MODEM, SWITCH, MAQUINAS) así que se considera que se puede hacer.

Factibilidad operativa:

Técnicamente se cuenta con las herramientas necesarias para dar marcha al proyecto

A continuación se presentan las herramientas técnicas a usar:

1. Dos computadora con microprocesador procesador con memoria ram de 512 mb disco duro de 500GB y con sistema operativo Debian yessie 8
2. MODEMS 3G
3. Cables UTP
4. Conectores RJ45
5. Una ponchadora para cable RJ45
6. Un Switch de 8 puertos
7. Probador de cable RJ45

Presupuesto de herramientas a utilizar en realizar proyecto

Herramientas	Cantidad	Precio p/u	Precio Total
Computadoras	2	5000	$1000
Cable utp	4m	0.50	$2.00
Capuchones	4	0.50	$2.00
Encriptora	1	15	$15
Probador de cable RJ45	1	30	$30
Swith	1	25	$20
módems	2	25	$50
Internet	mensual	50	$150
Otros (gastos de papel ò	-	-	$50
Monto Total			$1,319

Procedimiento de implementación de firewall

Plan de direcciones:

La LAN interna cuenta con este pool de direcciones 192.168.1.0/1 - 192.168.1.0/254, y cabe resaltar que el que los Módems 3g funcionan como servidor DHCP ipv4.

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

PROCEDIMIENTO:

Para que nuestra computadora trabaje como router utilizando los sistemas operativos GNU/Linux es necesario modificar algunos archivos.

Las configuraciones se realizan en la PC que funcionará como router de la siguiente manera:

1. Configuración de interfaces de red.

Para asignar direcciones ip a las interfaces de red de nuestra pc lo podemos hacer de 2 formas.

Se pueden asignar direcciones a una interfaz escribiendo en la terminal lo siguiente: ifconfig ethn dirección_ip/marcada_subred up

Donde n es el número de la interfaz que está conectada a nuestra pc, por ejemplo considere que se quiere asignar la dirección 192.168.1.1 que tiene una máscara de subred de 255^3 en la interfaz eth0, la manera de escribirlo sería: ifconfig eth0 192.168.1.1/24 up; con esto se asigna la dirección a la interfaz, pero esta persiste solo mientras está encendida la pc, una vez se reinicia o se apaga, al configuración se pierde.

Escribir en la terminal **nano /etc/network/interfaces** y se abrirá un archivo en la que configuraremos las interfaces a nuestro gusto. Utilizando la dirección e interfaz antes mencionada el archivo se tendría que configurar de la siguiente manera.

Para nuestro proyecto la forma en que quedarían configuradas las interfaces seria de la siguiente forma.

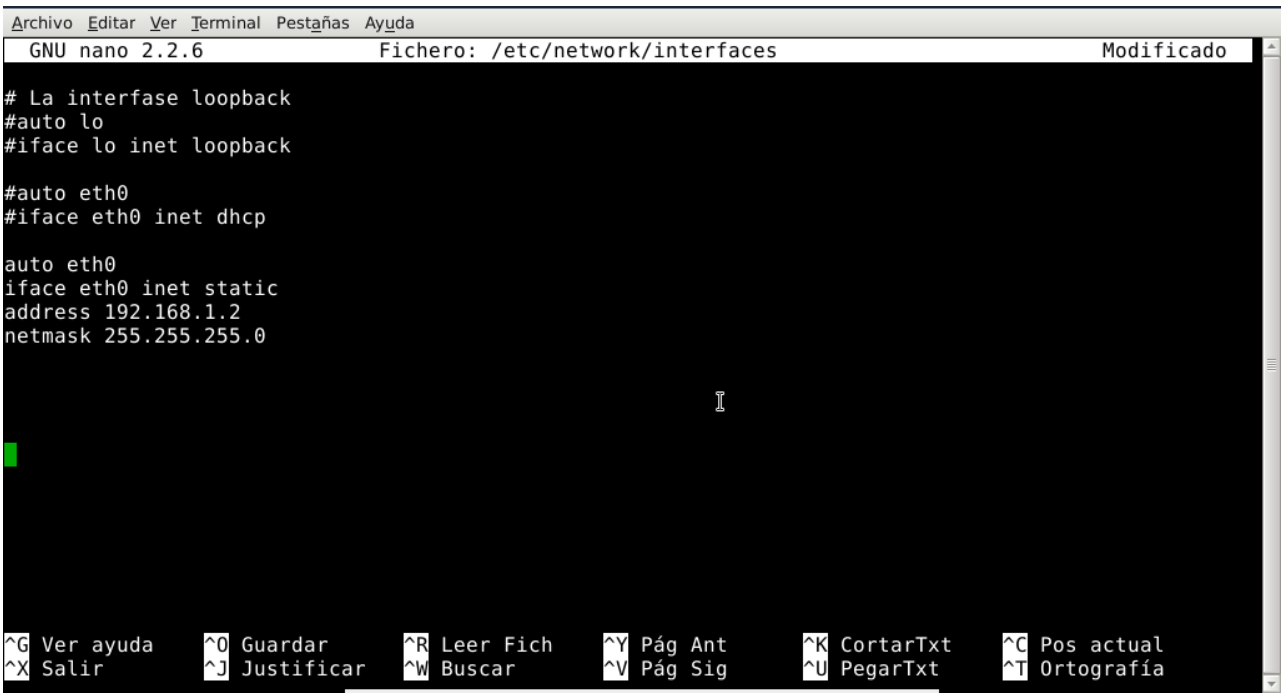


Ilustración 3 configuración de interfaces de red de servidor

Reiniciamos nuevamente el servicio de redes para que se muestren los cambios con la línea de comandos ***/etc/init.d/networking restart*** podemos ver nuestra configuración con el comando ifconfig –a para mostrar toda la información de nuestros dispositivos de red conectados y su respectiva configuración

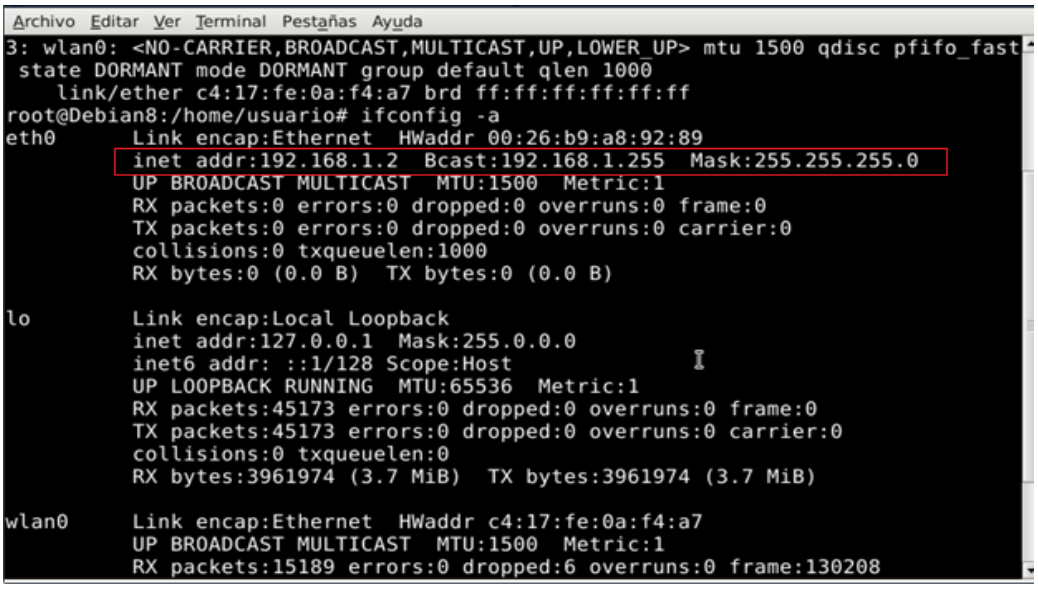


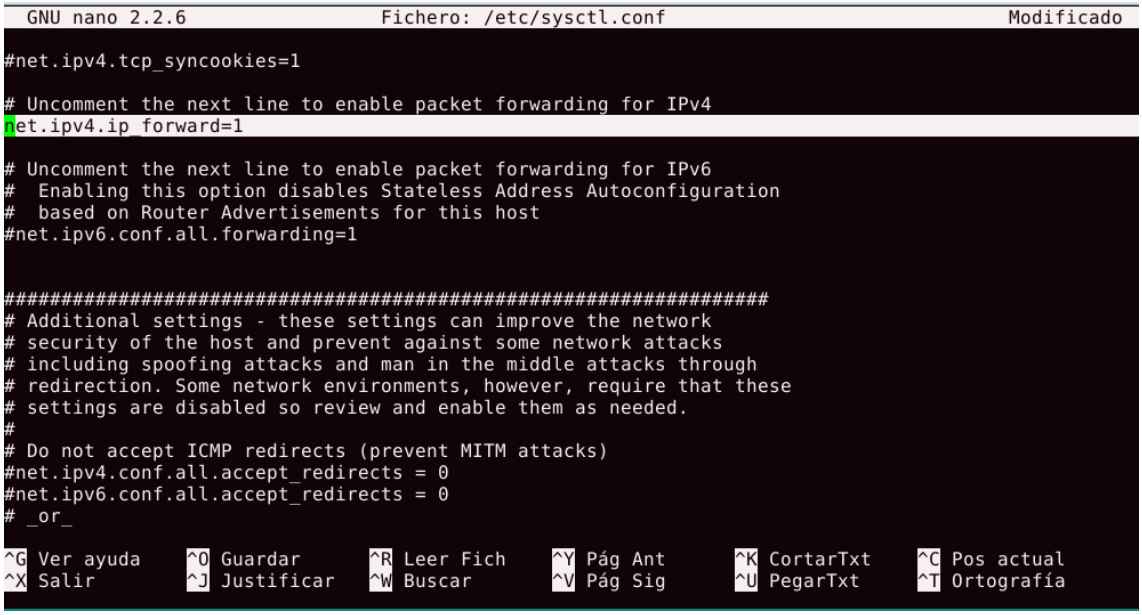
Ilustración 4 verificación de ip asignada

2. configuración de sysctl.conf

a. Escribir en la terminal nano */proc/sys/net/ipv4/conf/all/forwarding* y se abrirá un archivo, por defecto este tiene valor de 0, lo editamos y lo cambiamos por el valor de 1, presionamos las teclas Ctrl+O para guardar y luego Ctrl+X para salir; con esto nuestra pc se convierte en Router mientras está encendida. Una vez se reinicia la PC o se apaga, esta configuración se pierde.

b. Escribir en la terminal *nano /etc/sysctl.conf* y se abre un archivo, descomentamos lo siguiente para que nuestra computadora sea router y que no se pierda la configuración aunque la pc se reinicie o se apague y cambiamos en valor de 0 por uno como se muestra en la siguiente línea

net.ipv4.ip_forward=1



3. Instalación de wvdial

Para seguir con la configuración es necesario instalar el paquete wvdial, caso que no lo tengamos instalado, lo hacemos de la siguiente manera

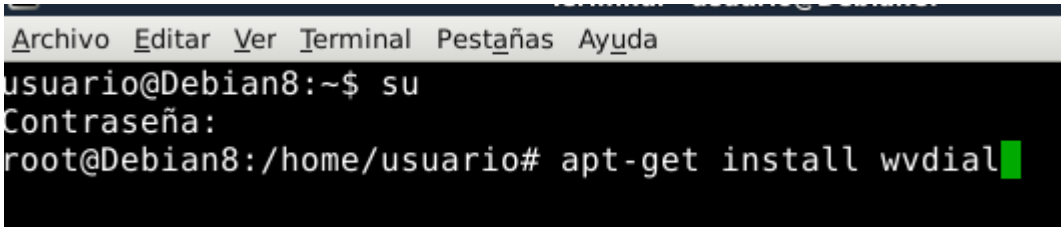


Ilustración 5 instalación de wvdial

4. configurar archivo wvdial

Una vez finalizado el proceso de actualización es necesario configurar el archivo *wvdial.conf*, para eso digitamos en consola lo siguiente: *nano /etc/wvdial.conf* y digitamos la siguiente información.

Ingresas a la terminal **nano *<u>/etc/wvdial.conf</u>***

Nuestro archivo ya editado quedo como el siguiente

Ilustración 6 configuración de modem claro

Ilustración 7 configuración de modem 3G

En caso de no conocer la información del puerto del modem es decir (/dev/ttyUSB0 o /dev/ttyUSB1, etc) utilizamos el siguiente comando para poder ver a detalle la información ***wvdialconf /etc/wvdial.conf***

La información que nos devuelve es la siguiente:

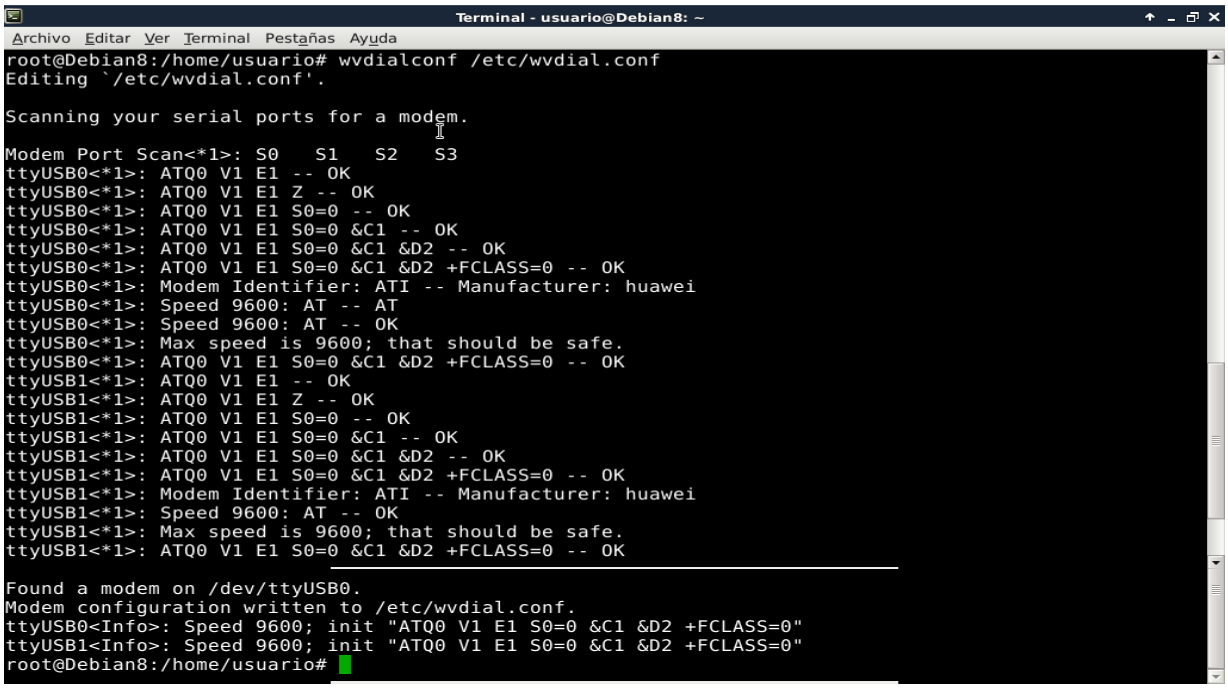


Ilustración 8 resultado de wvdial

Para probar si nuestro dispositivo ha sido reconocido como modem y es funcionando como tal podemos nuevamente ver los dispositivos conectador con **ifconfig –a**

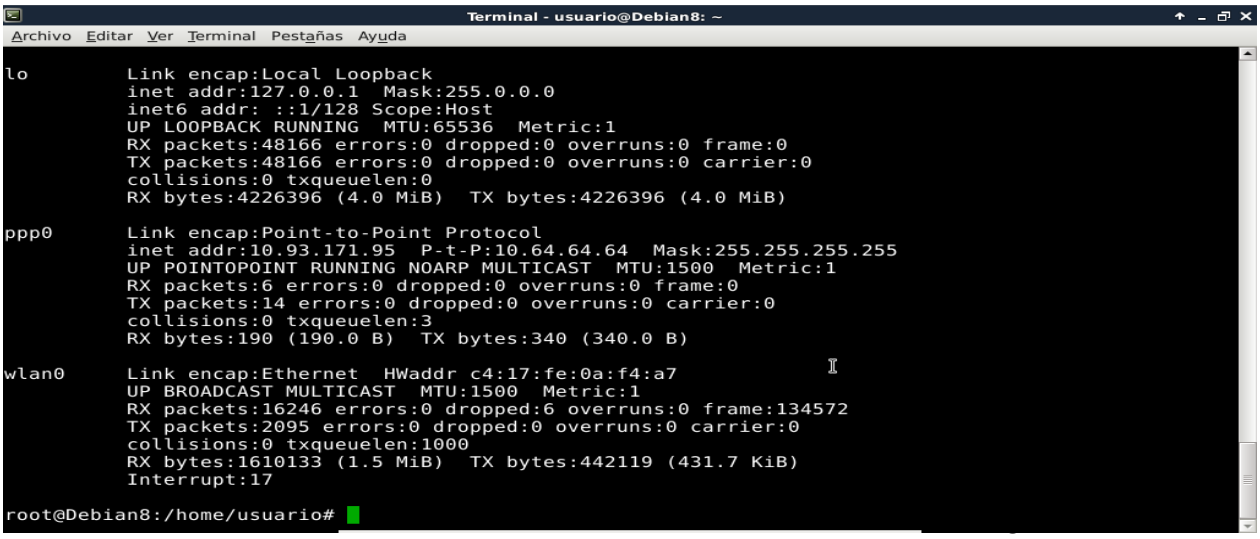


Ilustración 9 verificación de modem

Ejecutamos wvdial en la terminal para conectar el modem

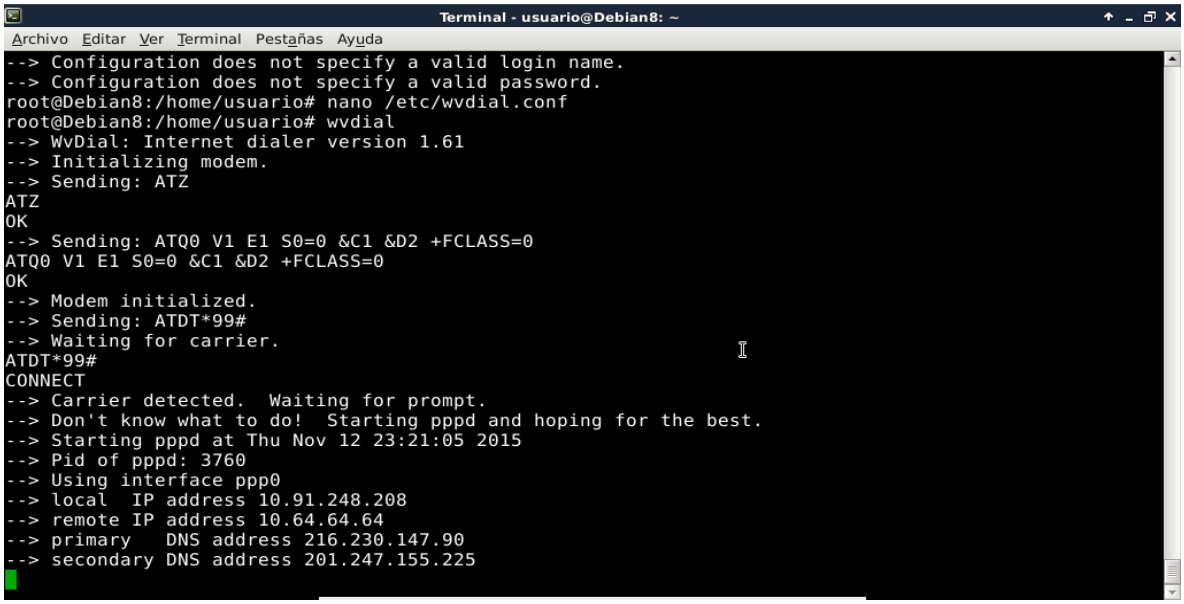


Ilustración 10 verificación con wvdial

7. Creación y configuración de tablas y reglas NAT

Para lograr esta parte se creó un archivo con nombre firewall.sh, el cual ejecutaremos antes de querer compartir internet con el resto de PC clientes conectadas a nuestro Router. El archivo contiene la siguiente estructura.

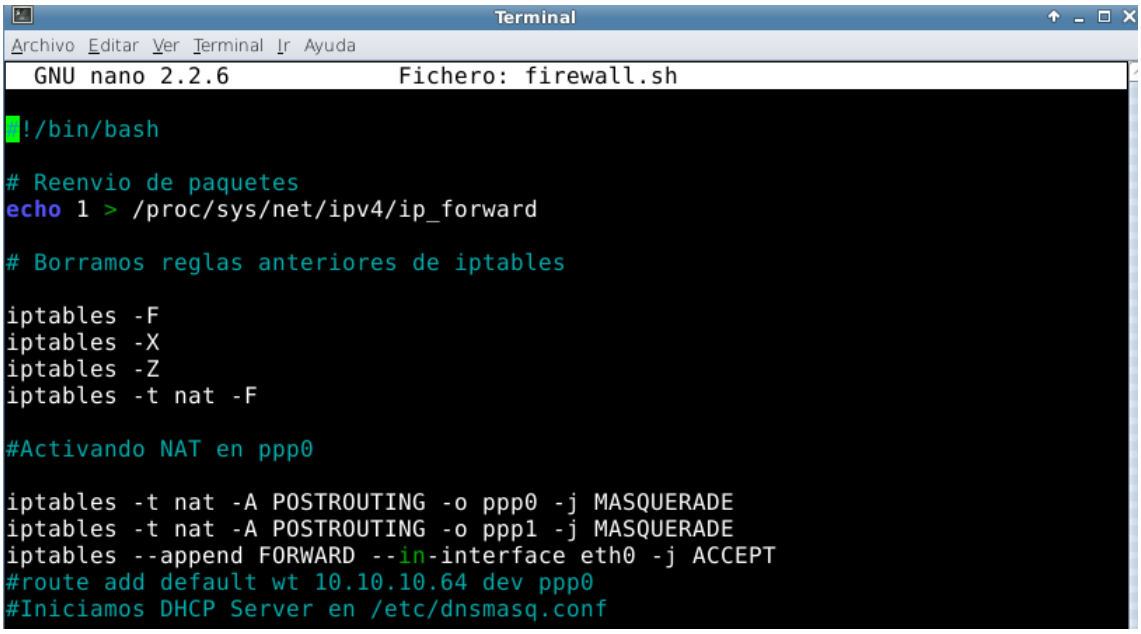


Ilustración 11 estructura de archivo .sh

NAT básicamente reemplaza la ip de origen de cada paquete por la ip que nosotros definamos que puede ser una ip estática o una dinámica. La regla del NAT es como sigue. Iptables –t nat –A POSTROUTING –s dirección_origen_a convertir/marcara_subred –o interfaz_de_salida –j MASQUERADE

Para nuestros propósitos escribimos la siguiente línea para salir a internet

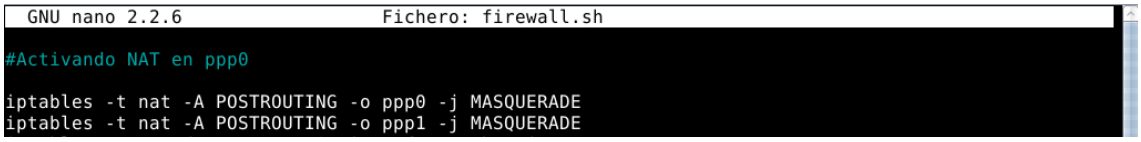


Ilustración 12 comando para compartir internet

MASQUERADE automáticamente convierte nuestra IP de la red local a IP pública

El archivo queda como se muestra a continuación en la figura 4.

8. Probar nuestra conexión por medio del comando ping

Resultados después de ejecutar ping a 8.8.8.8 y ping a youtube.com

por medio de nuestro modem.

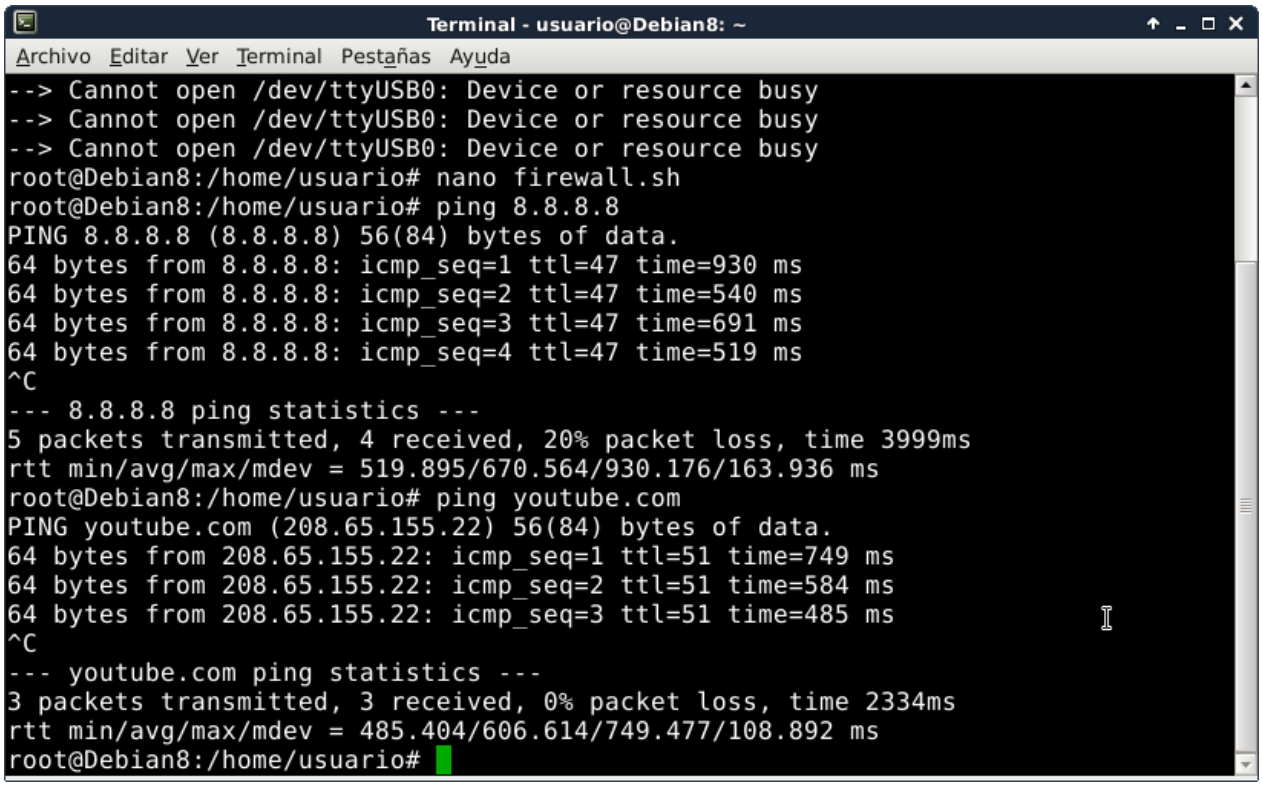


Ilustración 13 verificando internet

9. Configuración de PC cliente (la cual le brindaremos internet)

Para realizar la configuración de nuestra PC cliente cambiaremos los parámetros de la conexión IPV4 de la siguiente manera:

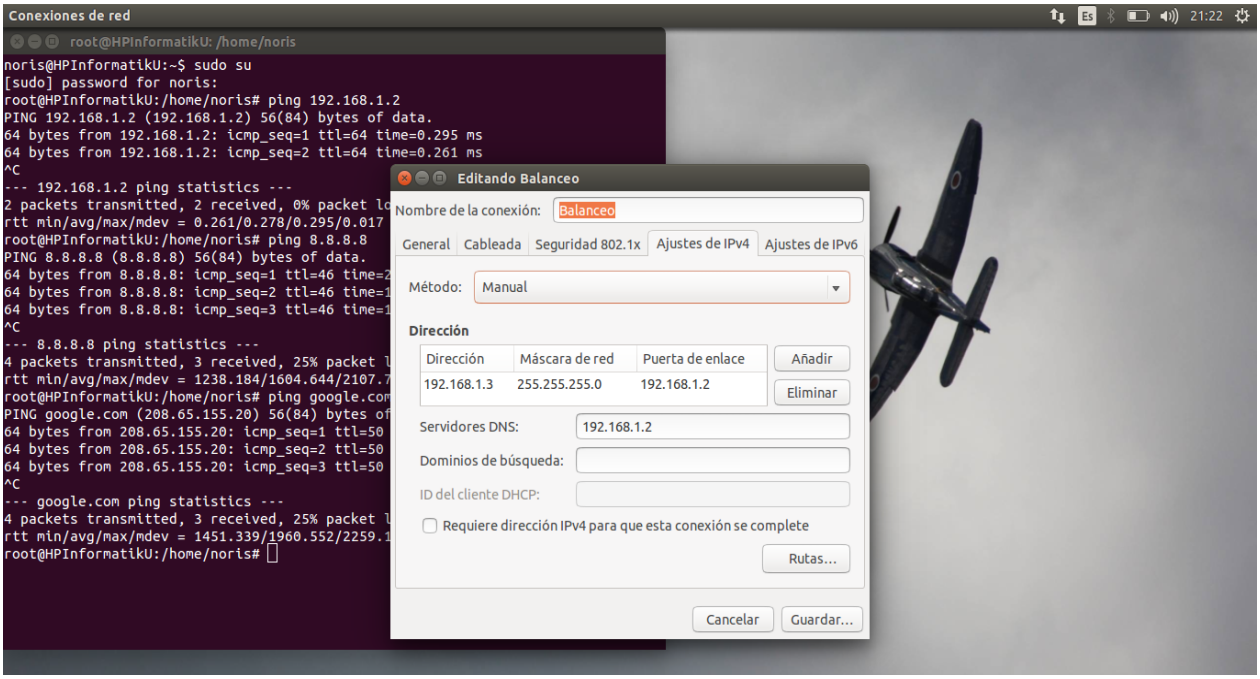


Ilustración 14 configurar parámetros de red de cliente

La IP utilizada es 192.168.1.3

Mascara de red 255.255.255.0

Puerta de enlace 192.168.1.2 (esta es la IP de nuestro servidor que funciona como router)

Servidor DNS 192.168.1.2

Una vez configurado reiniciamos los servicios de red y ejecutamos las pruebas respectivas de conexión

10. Probando nuestra red y conexión a internet por medio de ping

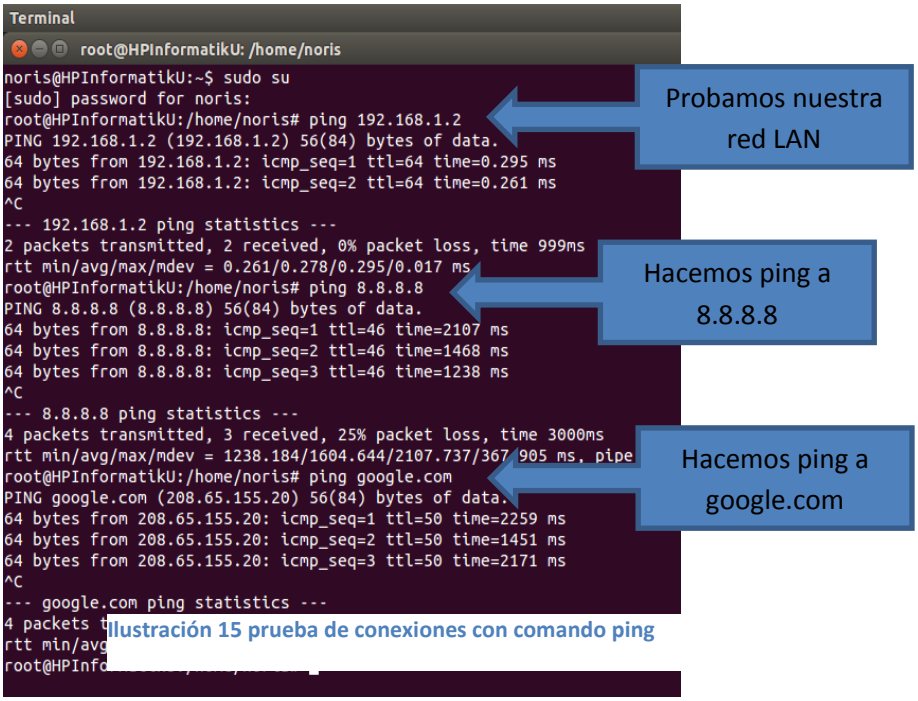


Ilustración 15 prueba de conexiones con comando ping

Podemos comprobar que efectivamente tenemos la conexión esperada ahora probaremos una página en nuestro navegador para comprobarlo

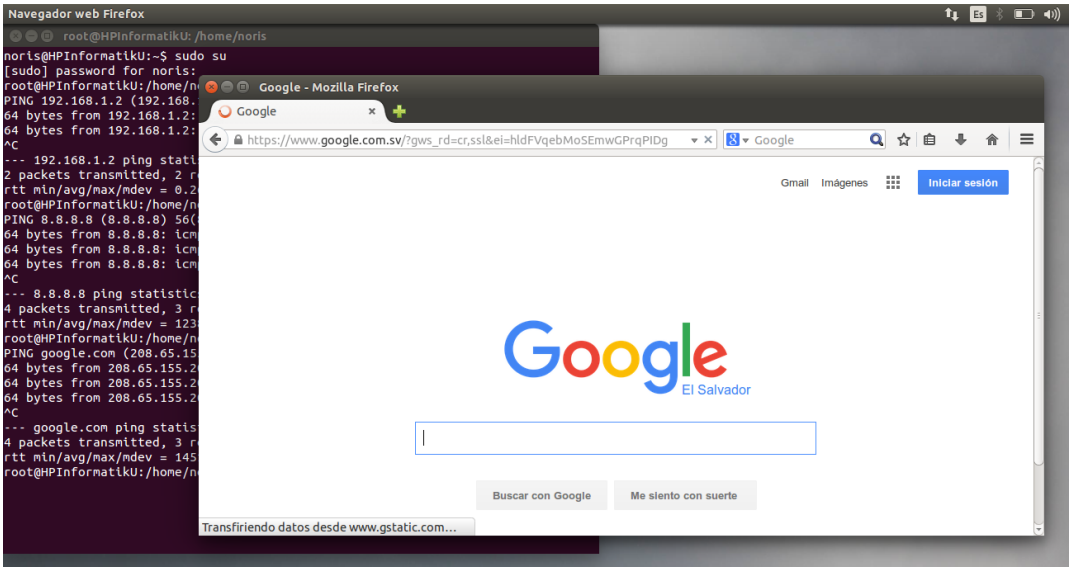
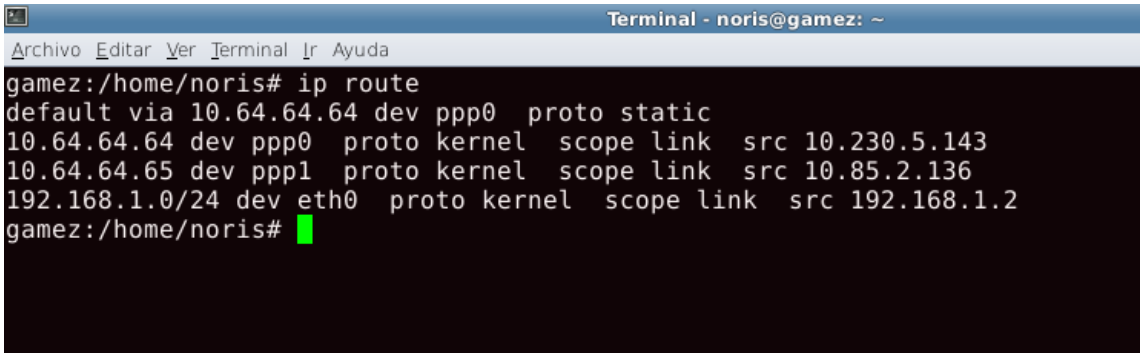


Ilustración 16 prueba de conexiones en navegador web

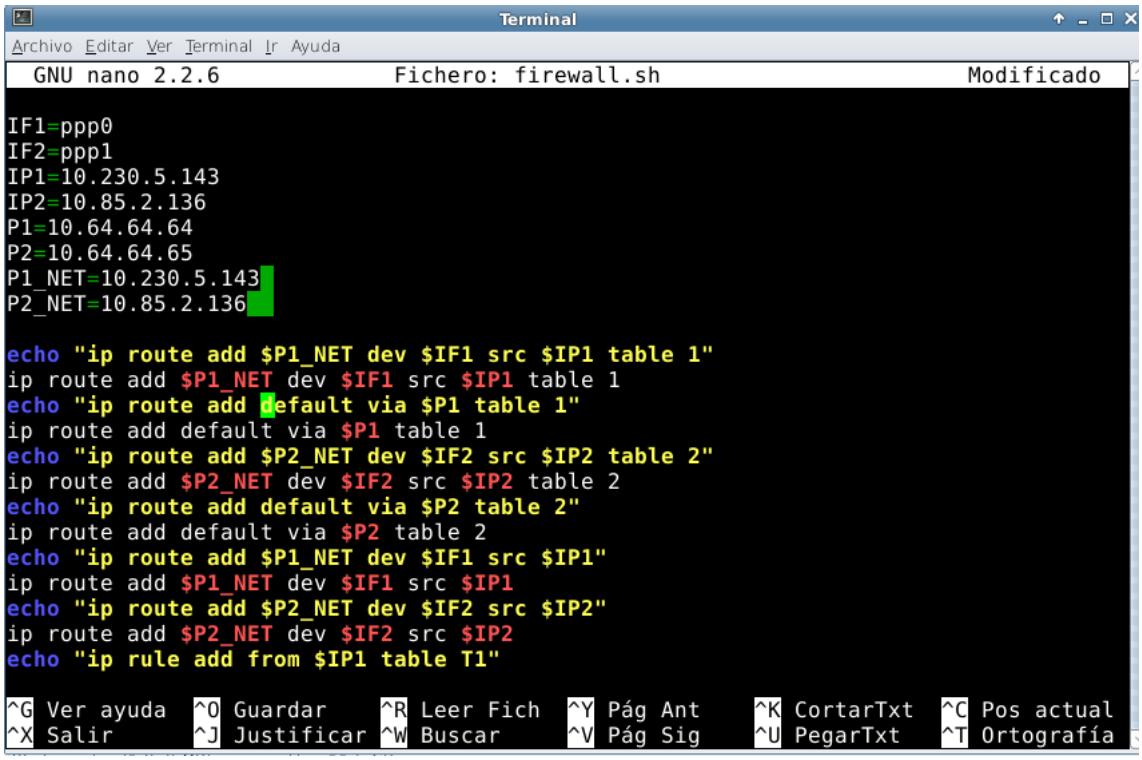
11. Ahora vamos hacer el balance de interfaces de red

Cuando se haga esto tiene que remplazar las ip que las interfaces generen

Ejemplo podemos verla con el comando **ip router**



Creas un archive.sh y lo ejecutas para hacer el balanceo



Nano enrutamiento.sh

#!/bin/bash
IF1=ppp0
IF2=ppp1
IP1=10.230.5.143
IP2=10.168.1.2
P1=10.64.64.64
P2=10.64.64.65
P1_NET=10.230.5.143
P2_NET=10.168.1.2

```
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
```

Verificación da dirección en la cual se va el inter con wireshark

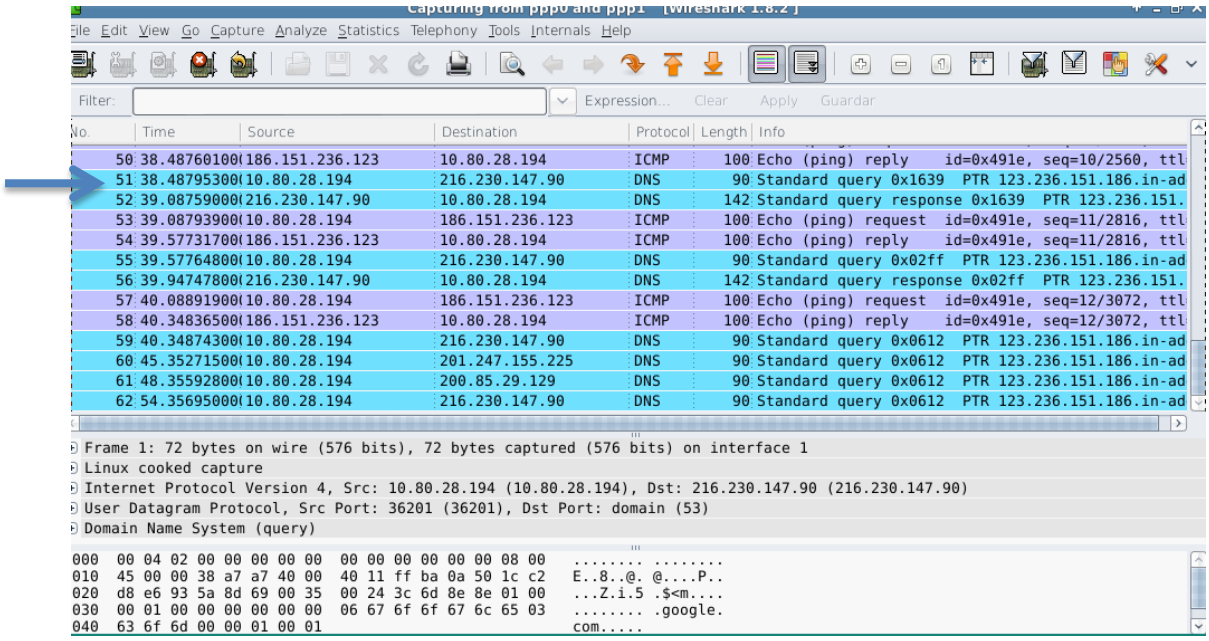


Ilustración 17 verificar en que interface está trabajando

Algunos comandos que puedes ejecutar para bloquear puestos o Facebook.

iptables -I FORWARD -m string –string ‘facebook’ –algo bm -j DROP

Una mejor alternativa puede ser bloquear todas las peticiones por el puerto 443 del siguiente modo:

iptables -I FORWARD -p tcp –dport 443 -m string –string ‘facebook’ –algo bm -j DROP

Con eso ahora intenta navegar a facebook y veras que no logras ingresar tanto por https como por http.

Si tus usuario tienen IP fija y quieres negar el acceso solo a uno en especial coloca la regla asi.

iptables -I FORWARD -s 192.168.221.5 -p tcp –dport 443 -m string –string ‘facebook’ –algo bm -j DROP.

Conclusión

La implementación de un firewall es una parte de seguridad importante que se puede implementar solo necesita como mínimo dos interfaces de red , se puede crear un software como firewall o instalarlo en este caso lo hicimos con dos interfaces de red y se comprobó que es una herramienta poderosa que puede ayudar a que se tenga un mejor control de recurso internet , ya que muchas veces gastamos nuestro tiempo en estar viendo páginas que no nos ayudan a una superación personal.

Iptables es una de las herramientas estándar de las distribuciones de Linux modernas ya que esta desde el kernel 2.4 y lo que hace es que los administradores crean reglas para los filtrados de paquetes.

Bibliografía

Título: Iptables

URL: https://wiki.debian.org/es/iptables

Fecha de consulta: 08/11/2015

Titular: Wireshark

URL: https://www.wireshark.org/ https://es.wikipedia.org/wiki/Wireshark

Fecha de consulta: 15/11/2015

Título: Enrutamiento

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

Fecha de consulta: 05/11/2015

Título: Iniciar conexión con modem 3G desde una terminal
URL: http://www.taringa.net/posts/linux/7804627/Iniciar-conexion-con-modem-3G-desde-una-terminal.html

Fecha de consulta: 20/10/2015

Título: /etc/sysctl.conf

URL: http://sysadmin.vazqueznanini.com.ar/configuraciones/-etc-sysctl-conf

Fecha de consulta:05/11/2015

Título:

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

Fecha de consulta:

Título: balanceo de carga

URL :http://proyectos.uls.edu.sv/wiki/images/5/50/Presentacion-firewall-redesII-2014-equipo-11.pdf

Fecha de consulta:15/10/2015