DISEÑO E IMPLEMENTACIÓN DE UN SERVIDOR FIREWALL EN LINUX

JAVYS PACHECO MENESES
KELLY MARTINEZ MOLINA

FACULTAD DE INGENIERÍA
PROGRAMA DE INGENIERÍA DE SISTEMAS
UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR
CARTAGENA DE INDIAS
2009

DISEÑO E IMPLEMENTACIÓN DE UN SERVIDOR FIREWALL EN LINUX

JAVYS PACHECO MENESES
KELLY MARTINEZ MOLINA

Monografía presentada para optar el título de Ingeniero de Sistemas

Director
ISACC ZÚÑIGA SILGADO
Ingeniero de Sistemas

FACULTAD DE INGENIERÍA
PROGRAMA DE INGENIERÍA DE SISTEMAS
UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR
CARTAGENA DE INDIAS
2009

Nota de aceptación

_____

_____

_____

_____

_____

_____

Firma del Presidente del Jurado

_____

Jurado

_____

Jurado

Cartagena de Indias, Abril de 2009

Señores:

UNIVERSIDAD TECNOLOGICA DE BOLIVAR
Comité de Evaluación de Proyectos
Escuela de Ingenierías
La Ciudad

Respetados Señores:

Cordial saludo, nos dirigimos a ustedes con el fin de presentar para su estudio, consideración y aprobación la monografía titulada **"DISEÑO E IMPLEMENTACIÓN DE UN SERVIDOR FIREWALL EN LINUX",** cómo requisito parcial para optar el título de Ingeniero de Sistemas.

Atentamente,

_____ _____

Javys Pacheco Meneses **Kelly Martinez Molina**

Cartagena de Indias, Abril de 2009

Señores:

UNIVERSIDAD TECNOLOGICA DE BOLIVAR
Comité de Evaluación de Proyectos
Escuela de Ingenierías
La Ciudad

Estimados Señores:

Con el mayor agrado me dirijo a ustedes para poner a consideración el trabajo final titulado **"DISEÑO E IMPLEMENTACIÓN DE UN SERVIDOR FIREWALL EN LINUX",** para su estudio y evaluación, la cual fue realizada por los estudiantes estudiantes JAVYS PACHECO MENESES Y KELLY MARTINEZ MOLINA del cual acepto ser su director.

Cordialmente,

_____

Isaac Zúñiga Silgado
Ingeniero de Sistemas

AUTORIZACIÓN

Cartagena D.T.H. y C. Abril de 2009

Yo JAVYS PACHECO MENESES, identificado con número de cedula 13.852.400 de Barrancabermeja, autorizo a la **Universidad Tecnológica de Bolívar** para hacer uso y publicación de mi trabajo de grado en el catalogo on-line de la Biblioteca.

_____

Javys Pacheco Meneses

C.C 13.852.400 Barrancabermeja

AUTORIZACIÓN

Cartagena D.T.H. y C. Abril de 2009

Yo KELLY MARTINEZ MOLINA, identificado con numero de cedula 45.552.208 de Cartagena, autorizo a la **Universidad Tecnológica de Bolívar** para hacer uso y publicación de mi trabajo de grado en el catalogo on-line de la Biblioteca.

_____

Kelly Martinez Molina

CC. 45.552.208 Cartagena

TABLA DE CONTENIDO

LISTAS ESPECIALES

Lista de Figuras

LISTAS ESPECIALES

Lista de Tablas

RESUMEN

El auge de los nuevos sistema de información han sido creados basados en la experiencia, documentos y utilidades de aprendizaje de los hackers; hoy en día podemos prevenirnos de muchas bandas de crimen informáticos que utilizan estas herramientas para robar información confidencial de los usuarios, falsificar tarjeta de crédito y entre otros delito lo cual ha proporcionado nuevas alternativas de seguridad para la protección de una red perimetral.

Un Firewall es un dispositivo de hardware o una aplicación de software diseñado para proteger los dispositivos de red de los usuarios externos de la red y/o de aplicaciones y archivos maliciosos. Entre sus funciones se destacan: los bloqueos de paquetes que se originan en determinado rango de IP, puertos etc.
Los firewalls los podemos encontrar en el mercado como software o hardware en los cuales tiene una característica común en una red perimetral.
Existen varios tipos de filtrado que puede ejecutar un firewall entre ellos están: los *filtrados a nivel de paquetes* que trabajan en la capa de red del modelo OSI en donde examinan las direcciones IP de origen y destino, numero de puerto que se utilizan para la comunicación; igualmente encontramos los *filtrado de circuito* que trabajan en las capas de transporte y sesión, examinado la información TCP que se envía entre sistema para verificar que sea legítima; y el *filtrado a nivel de aplicación* llamados proxies que opera a nivel de la capa de aplicación verificando el contenido de los datos.

Dentro de la estructuración de los firewall encontramos diferentes arquitecturas como: la arquitectura host de doble acceso la cual tiene dos interfaces de red para la comunicación y protección de una red local con internet; arquitectura host de protección que conecta la red interna por medio de un router siendo accesible tanto del exterior como de la red interna; arquitectura de subred de protección esta introduce dos routers uno externo para la comunicación por internet y otro interno para la comunicación con la red interna entre estos dos routers esta el

host bastión en el cual protege la comunicación que se pueda dar entre ellos.
Es indispensable establecer las políticas de acceso permitidas en los servidores y redes a proteger para que pueda ser implementada en las reglas del firewall, en los cuales existen políticas de denegar todo y dar permisos a aquellas conexiones para la organización, o permitir todo y cerrar los puertos innecesarios.

La configuración de un servidor Firewall debe tener mínimo servicios activos para su buen desempeño ya que comprometen la red a proteger, en el caso que se requiera tener servicios Web, correo entre otros sería útil utilizar una tercera tarjeta de red para ubicar estos servicios en una zona denominada zona desmilitarizadas o DMZ debido a que estos servicios tiene la particularidad de ser acceso libre y requiere de una protección más compleja.

Existe una herramienta llamada iptables que es un programa línea de comandos usados para la configuración de reglas de filtrado de paquetes en los kernels de Linux. Hay dos formas de configurarlas: la primera es por medio de comandos iptables en la Shell de Linux y la segunda es por medio de un script donde se escribirá todas las reglas en un único archivo; en esta investigación se utilizó este último ya que nos permite corregir las reglas antes de ser ejecutadas y organizar la sintaxis de Iptables.

Es importante tener claro que el servidor Linux debe comportarse como un router y hacer una puerta de enlace para los PCs de la red local cuyo destino sea una red externa o Internet es necesario crear las respectivas reglas dentro del script de Iptables para que realice NAT en el cual convierte las direcciones procedentes de la red local para que pueda salir hacia Internet.

La utilización de herramientas como el IPTRAF para el análisis de conexiones entrante y saliente dentro del firewall permite verificar si la comunicación se estableció por las peticiones de los host hacia algún servicio fuera de la red local o viceversa. Existen también herramientas que permite comprobar la veracidad del firewall, de cierta manera ayuda al administrador tener una visión clara de cómo un intruso puede atacar a la red protegida.

Por lo tanto las protecciones en perímetros son necesarias pero también hay que instruir a nuestros usuarios para que no corran el riesgo o infecten la red de una organización accidentalmente; hoy en día hay muchas empresas se encuentran actualizadas con los nuevos virus de acuerdo a estos fabrican parches para sus antivirus comerciales, estas empresas están informando constantemente las nuevas amenazas existentes, por eso es importante firewall actualizado e implementado correctamente para protegernos de posibles ataques o de códigos maliciosos.

1. INTRODUCCION

Actualmente nos encontramos en una evolución constante en las tecnologías de comunicación y transferencia de información que conllevan a una interacción de redes y un mayor volumen de envió de paquetes de datos de forma permanente lo que implica a mayores riesgos a la seguridad de la información de una organización.

El firewall es una herramienta que garantiza una mayor seguridad de los datos que se manejan dentro de una red donde se comparte y se accede a información de todas partes del mundo o desde una red interna y que permite tener una protección contra intrusos de la red de internet o usuarios locales.

Esto es muy diferente a lo que hace algunos años era una red en la que solo era posible hacer consultas y la seguridad no era lo primordial, pero debido al uso masivo de las redes por parte de las grandes empresas se detectaron fallas internas en cuanto a la seguridad y confidencialidad de la información, ya que debido al proceso de globalización y la permanente competencia para la penetración de mercados y posicionamientos de nuevos productos era de vital importancia proteger la información ante la competencia.

De acuerdo con lo anterior se crearon diferentes programas que ayudaban a mitigar en parte esto, pero no daba la seguridad al 100% que sus datos estuvieran bien protegidos. Entonces nacen los firewall o cortafuego que han ido evolucionando con el tiempo y que hoy por hoy se pueden considerar como la aplicación que ofrece mayor garantía en la seguridad y protección de los datos. Conceptualmente los firewalls son sistemas o grupos de sistemas que implementan una política de seguridad de control de acceso entre dos o más redes, es por esto que los firewalls constituyen una herramienta en la cual debemos tener claro el tipo de control de acceso que debemos implementar; en

cuantos a estos se refieren en los firewalls, existen varios tipos de firewalls aplicados a las capas del modelo OSI en el nivel red, trasporte y aplicación.

Con lo mencionado anteriormente se perfila la presente investigación, que presenta en su inicio, la configuración del servidor Cortafuego con distribución Linux Centos 5.2, en donde se configura la herramienta Iptables para la creación de reglas en el tráfico de datos, el análisis de la configuración desde el otro extremo de la red para su verificación y la utilización de una herramienta para generar reportes de las reglas de Iptables.
Antes de la creación de reglas se debe definir la políticas de seguridad por defecto para el trafico que no sea incluido en la reglas de Iptables y luego procedemos a configurar el Servidor cortafuego, los Routers y los hosts que mostraremos con mas detalles en el desarrollo de esta investigación.

2. OBJETIVOS

2.1 Objetivo general

Implementar un Servidor Firewall GNU/Linux como herramienta de administración para la seguridad de una red a nivel Institucional u organizacional.

2.2 Objetivos específicos

- Dar a conocer a la comunidad informática el proceso de implementación de un firewall para garantizar la seguridad en una red local.

- Conocer las características principales de los Firewalls, tales como su concepto, ventajas y desventajas, tipos de firewalls y las arquitecturas más utilizada en la actualidad.

- Diseñar la arquitectura del Firewall a implementar, tanto como las políticas de seguridad para la utilización en esta implementación.

- Conocer e implementar el servidor Cortafuego con la herramienta Iptables, como son las reglas según las políticas de seguridad definidas, y la interconexión entre los diferentes dispositivos como son Router, Switches, PCs.

- Realizar pruebas que depuren la configuración del servidor Cortafuego desde el otro extremo de la red local.

2.3. Justificación

En esta investigación se quiere dar a conocer la importancia de la seguridad informática en las red locales y la externas; especialmente en la implementación de firewalls, ya que este nos permite tener un mayor control en el tráfico de los datos por medio de permisos para que solo accedan los usuarios que están permitidos para ingresar en una red cualquiera.

Existen muchos ejemplos hoy en día con respecto a esta temática una muestra de esto son los ataques de denegación de servicio llamados (DDos) que atacan a un servidor desde un PC con diferentes IP; en el caso de los virus anteriormente cuando no existía la implementación del firewall lo que realizaba específicamente era abrir puertos y por medio de los hackers atacaban fácilmente. En esta era moderna donde manejamos un considerado ancho de banda las diferentes empresas que proveen estos servicios a cada usuario le es entregado un Router con firewall integrados para poder controlar los puertos que deben estar abiertos para diferentes funciones.

Todos estos problemas son controlados por el Firewall ya que nos ayuda a evitar que cualquier intruso robe o inutilice la información de un usuario cualquiera, ya sea de tarjeta de crédito, pagos por Internet, estas son las funciones que cumplen estos contrafuegos.

En los servidores trabajan como una pared que se divide con los usuarios para proteger la información que se guarda en una base datos y evitar ser robadas por piratas informáticos he ahí la importancia que tiene los firewalls en las diferentes aplicaciones.

3. CONCEPTOS BÁSICO DE LOS FIREWALLS

3.1 Definición básica de Firewalls

Un firewall es un sistema que permite ejercer políticas de control de acceso entre dos redes, tales como la red LAN privada e Internet, que es una red pública y vulnerable. El firewall define los servicios que pueden accederse desde el exterior y viceversa. Los medios a través de los cuales se logra esta función varían notoriamente, pero en principio, un firewall puede considerarse como: un mecanismo para bloquear el tráfico y otro para permitirlo. Un firewall constituye más que una puerta cerrada con llave al frente de la red. Es un servicio de seguridad particular.

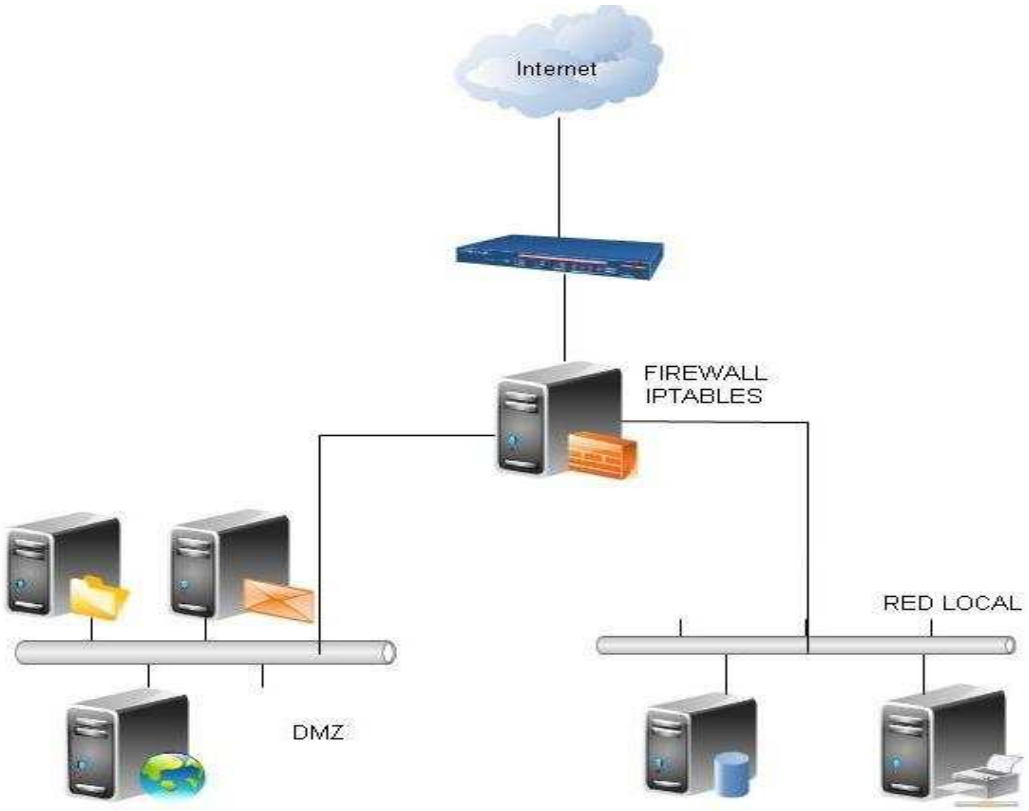

Figura 1. Diseño de Firewall

Los firewalls son también importantes porque proporcionan un único punto de restricción, donde se pueden aplicar políticas de seguridad y auditoría. Un firewall proporciona al administrador de la red, datos, información acerca del tipo y cantidad de tráfico que ha fluido a través del mismo y cuántas veces se ha intentado violar la seguridad. De manera similar a un sistema de circuito cerrado de TV, un firewall no sólo bloquea el acceso, sino también monitorea a aquellos que están merodeando y ayuda a identificar los usuarios que han intentado violar su seguridad[1].

3.2 Funcionalidades básicas de los Firewalls

Dentro de sus funcionalidades se destacan las siguientes:

- Bloqueo de paquetes que se originan en un determinado rango de IP, puertos, dominios, direcciones de correo, etc.
- Bloqueo de paquetes formados por determinados protocolos o aplicaciones.
- Bloqueo de paquetes que sean reconocidos como firmas de ataques a sistemas o redes.
- Herramienta de análisis del comportamiento de sistemas y de red.
- Herramienta de análisis forense.
- Sistemas de defensa contra virus, gusanos y spam.
- Bloqueo de virus, gusanos, Troyanos y malware en general.
- Bloqueo del uso de la red que protegen como origen de ataques.

3.3 Características de los Firewalls.

Para llevar a cabo un buen diseño hay que tener en cuenta las siguientes características:

- *Control de Servicios*: Determina el tipo de servicios de Internet que pueden ser permitidos hacia adentro o hacia afuera.

[1] 3Com Corporation, Seguridad de Redes: Una guía para implementar Firewalls [En línea] http://lat.3com.com/lat/technology/technical_papers.html [Citado en Noviembre 01 de 2008

- *Control de dirección*: Determina en qué dirección cada servicio en particular se le permite circular.
- *Control de Usuarios:* Se implementan controles de acceso a un servicio de acuerdo al usuario que está tratando de acceder.
- *Control de comportamiento:* Controla como son utilizados cada servicio en Particular (ejemplo: filtrado de correo electrónico)

3.4 Clasificación Firewalls

Los firewalls se puede clasificar en virtud de diferentes características como:

3.4.1 Modelo de arquitectura

Dependiendo del lugar donde se coloquen en la red pueden tener distintas funciones. Cuando hay dos o más firewalls implementados en una red, estos se comunican con Internet u otras redes recibiendo el nombre de **firewall de contención**, en cambio el que se encuentra situado internamente y protege redes internas se le denomina **firewall bastión**.

3.4.2 Firewalls de software y hardware

Entre los firewalls de software se encuentra VPN-1/Firewall-1 de Checkpoint, Iptables, ISA server de Microsoft.
En hardware están PIX de Cisco, Netscreen de Juniper Networks.

Teniendo en cuenta que existen soluciones de firewalls de software integrados con aplicaciones como IP-Nokia/Firewall-1, Crossbean/firewall-1, etc. Estas soluciones se clasifican en:

- ✓ Firewalls Software
  - Soportados por varios Sistemas Operativos.
  - Soportados en varias plataformas.
  - Productos Mixtos.

- ✓ Firewalls Hardware
    - Hardware-Aplicación+Sofware preinstalado.
    - Sistemas operativos Fabricantes
    - Funcionalidades añadidas como VPN, cache.
    - Disco duros

3.4.3 Firewall de host y Firewalls de red

Los firewalls host protege los sistemas donde están instalados, y los de Red protegen el entorno de la red o redes donde se han implementados.

- ✓ Firewall red
    - Protegen redes enteras
    - Sistemas dedicado a la función de Firewall
    - Módulos adicionales como IDS/IPS, antivirus
    - Más caros

- ✓ Firewall hosts
    - Firewalls personales.
    - Embebidos en Sistemas operativos.
    - Sistemas de conexión externa a través de VPN
    - Baratos.

3.5. Tipos de filtrado en Firewalls

Hay tres tipos principales de filtrados basados en la capa del modelo OSI en la que los firewalls realizan el filtrado[2].

3.5.1 Filtrado a nivel de paquete

Se realiza a nivel de la capa de Red, examinando la cabecera del paquete. En los cuales se hace una verificación de la cabecera de los paquetes que contienen las direcciones IP y sus opciones, permitiendo o denegando su paso a las redes que

[2] PICOUTO Fernando, LORENTE Iñaki. Hacking y Seguridad en Internet. México: Alfaomega Grupo Editor, S.A, 2008. P 346

protegían. Se puede encontrar en los sistemas operativos, software, routers (acl) o firewall de hardware.

La utilización de un firewall a nivel de red, puede dar o negar acceso a un sitio basándose en variables, como:

- ✓ Dirección de fuente
- ✓ protocolo
- ✓ numero de puerto
- ✓ contenido[3]

3.5.2 Firewall de filtrado de circuito

Trabaja en las capas de transporte y sesión del modelo OSI, su función principal es examinar la información TCP que se envían entre sistemas para verificar que la petición sea legítima.
Los filtros de circuito restringen los accesos que se encuentran en las cabeceras TCP y UDP.
Se permite crear filtros en los cuales se quiere prohibir al sistema “C” usar FTP
Para acceder al sistema “D”, el control de acceso está basado en el flujo de datos TCP y datagramas UDP.

3.5.3 Filtrado a nivel de aplicación (proxies)

Los servidores proxy se ejecutan en unos pocos programas que pueden ser securizados y confiables, estos programas son servicios específicos teniendo en cuenta que cada protocolo soporta su propio servicio proxy y gestionado por un proxy genérico.
La función principal es realizar conexiones punto a punto desde el cliente al proxy y desde este al servicio de red requerido.

[3] ARROYO José. Linux Máxima Seguridad edición especial México: Prentice Hall 2000 P 520

Características de una conexión proxy:

- El usuario realiza la petición de un servicio de internet, como es HTTP, FTP, Telnet entre otras.
- El software instalado en el sistema del cliente lanza la petición de acuerdo con la política de seguridad a utilizar para el servicio de internet requerido.
- Proxy provee conexión actuando como Gateway del servicio remoto.
- Proxy realiza las comunicaciones necesarias para establecer la conexión con los sistemas extremos, mientras protegen los sistemas que están detrás de él.
- Todo el tráfico se enruta entre el usuario interno y el sistema externo a través del Proxy Gateway.
- El sistema Proxy debe ser implementado para ser usado por un solo servicio, sin configurar cuentas de usuarios, ni programas innecesarios.

3.6 Políticas de seguridad de los Firewalls

Una política de seguridad es una declaración formal de las normas que los usuarios deben respetar a fin de acceder a los bienes de tecnología e información. Puede ser tan simple como una política de uso aceptable o contener muchas páginas y detallar cada aspecto de conectividad de los usuarios, así como los procedimientos de uso de redes. La política de seguridad debe ser el punto central acerca de la forma en la que se protege, se supervisa, se evalúa y se mejora una red.

Los procedimientos de seguridad implementan políticas de seguridad que definen la configuración, el inicio de sesión, la auditoría y los procesos de mantenimiento de los hosts y dispositivos de red[4].

Una buena política de seguridad es la que nos permite definir las funciones que debe cumplir el Firewall y también informar al usuario que está permitido o

[4] CISCO SYSTEMS. Currícula CCNA 4.0 Discovery - Networking para el Hogar y Pequeñas Empresas

denegado.

Existen diferentes políticas de seguridad en la cuales tenemos:

1. *Políticas de identificación y autenticación*: especifica las personas autorizadas que pueden tener acceso a los recursos de la red.

2. *Políticas de contraseña*: garantiza que las contraseñas de los usuarios cumpla con los requisitos mínimos y se cambien periódicamente.

3. *Políticas de usos aceptables*: Identifican aplicaciones y usos de red que son aceptables.

4. *Políticas de acceso remoto*: Define como los usuarios remotos pueden obtener acceso a la red y a que elementos disponibles.

3.7 Ventajas y desventajas

Ventajas de un Firewall: entre las ventajas que tiene un firewall para proteger una red tenemos:

- Permite al administrador de la red mantener fuera de la red privada a los usuarios no-autorizados como son: hackers, crackers, espías y los mismos usuarios de la red privada negándole la entrada o salida de datos.
- Ofrece la posibilidad de monitorear la seguridad y si aparece alguna actividad sospechosa, generará una alarma ante la posibilidad que ocurra un ataque.
- Crea un archivo en donde se registra el tráfico que pasa a través del firewall.
- Controla los accesos provenientes de la red privada hacia el Internet.
- Controla los accesos provenientes de Internet hacia la red privada.
- Ayuda a simplificar los trabajos de administración, una vez que se consolida la seguridad auditando el uso del Internet, localizando con precisión los altos tráficos de consumo de ancho de banda.

Desventajas:

- No puede proteger contra los ataques de la Ingeniería Social.
- No puede proteger contra aquellos ataques que se efectúen fuera de su punto de operación.
- No puede prohibir que se copien datos corporativos en disquetes o memorias portátiles.
- No puede ofrecer protección cuando el atacante lo traspasa.
- No cuenta con un sistema de Scan para cada tipo de virus que se puedan presentar en los archivos que pasan a través de él, ya que el Firewall no es un antivirus sino un escudo de protección.

4. DISEÑO DEL SERVIDOR MURO-FIREWALL A IMPLEMENTAR

4.1 Arquitectura de Firewalls

Son las diferentes formas de combinar y conectar los dispositivos que forman los firewalls, como son los enrutadores, Switches, proxies, los hosts bastión y las redes perimetrales.

Las diferentes arquitecturas dependen del grado de seguridad que se requiera implementar, y tiene que ver también con el costo permitido para diseñar el Firewall.

Existen tres arquitecturas básicas que son:

4.1.1 Arquitectura de Host de doble acceso

Figura 2. Arquitectura Host de doble acceso

En esta arquitectura la red está protegida perimetralmente por un solo Firewall, que protege la red interior de la red exterior en el caso típico de conexión a internet y que tiene instalada dos tarjetas de red.
Una ventaja de este tipo de arquitectura es que el host trabaja hasta capas más altas que los enrutadores y puede realizar un filtrado de paquetes más elaborado.
Una desventaja que comprometen el host en el caso de una mala configuración del mismo, se da cuando el atacante tiene entrada libre a la red; esta arquitectura tiende a ser compleja en la configuración por el cual lo hace mucho más vulnerable.
El tener este tipo de arquitectura no significa sencillez en la definición de políticas de seguridad ya que a veces las conexiones desde fuera hacia dentro, hay que realizar políticas para las distintas aplicaciones y protocolos.

Su utilización puede ser en:

- Pequeña cantidad de tráfico dirigido a Internet
- El tráfico dirigido a Internet no crítico
- No ofrecer servicios a usuarios de Internet
- La red protegida sin contener datos muy importantes

En esta arquitectura, este dispositivo host es crítico para la seguridad de la red ya que es el único sistema que puede ser accedido y atacado desde Internet, por lo que debe poseer un alto nivel de protección a diferencia de un host común de la red interna. Estos host suele llamárseles bastión, en los cuales debe instalarse la mínima cantidad necesaria de software para reducir el riesgo de que sea vulnerado.

4.1.2 Arquitectura de Host de protección

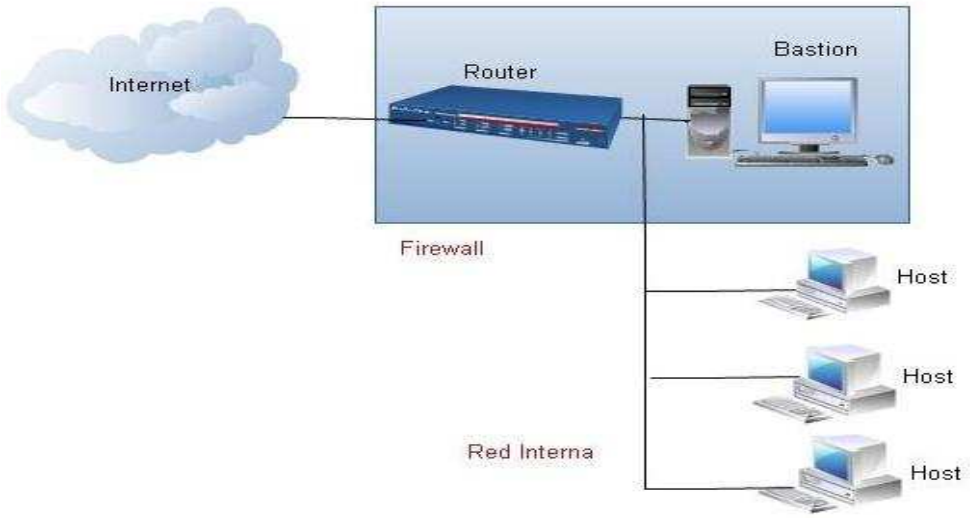

Figura 3. Arquitectura de host de protección

En esta arquitectura el host bastión está conectado en la red interna, siendo accesible tanto desde el exterior como desde la red interna.
La arquitectura Host de protección posee un firewall compuesto por un router para el filtrado de paquetes y un host bastión para el filtrado de conexiones a nivel de circuito y aplicación. La primera línea de protección corresponde al router con filtrado de paquetes, el host bastión se encuentra conectado a la red interna como un host más.
El router está configurado para dirigir todo el trafico proveniente de la red externa al host bastión por lo que es el único que puede ser accedido directamente desde fuera de la red local, por esto, el bastión debe estar altamente protegido. Así mismo, el bastión dirige todo el tráfico proveniente de la red interna al router por lo que es el único que puede establecer una conexión con el exterior.

El router de filtrado de paquetes puede ser configurado de diferentes formas:

- Permitir que ciertos hosts internos puedan abrir conexiones a Internet para ciertos servicios.

- Deshabilitar todas las conexiones desde los hosts internos habilitando solo al host bastión para establecer estas conexiones.
- Es posible que algunos paquetes sean dirigidos, por el router, directamente a los hosts internos.

Esta arquitectura es más segura ya que agrega una capa de seguridad a la arquitectura anterior: un atacante tiene que atravesar primero por el router y luego por el host bastión, dependiendo del uso de una política de seguridad correctamente diseñada.[5]

Es recomendable utilizar este tipo de arquitectura:

- En redes interna con alto nivel de seguridad.
- Sencillas reglas de filtrado.
- Cuando es necesario alta eficiencia y redundancia

4.1.3 Arquitectura de subred de protección

En esta arquitectura introduce dos routers uno externo y uno interno, en medio de estos dos routers se encuentra la red Zona Desmilitarizada, en este caso sería el host bastión. Estará conectado a un segmento de red diferente al que están conectados los hosts de la red privada. Con esta configuración no existe un único punto vulnerable que ponga en riesgo toda la red interna.

[5] Textoscientificos.com, Firewalls Convencionales [En línea] http://www.textoscientificos.com/redes/firewalls-distribuidos/firewalls/convencionales [Citado en marzo 9 de 2009]

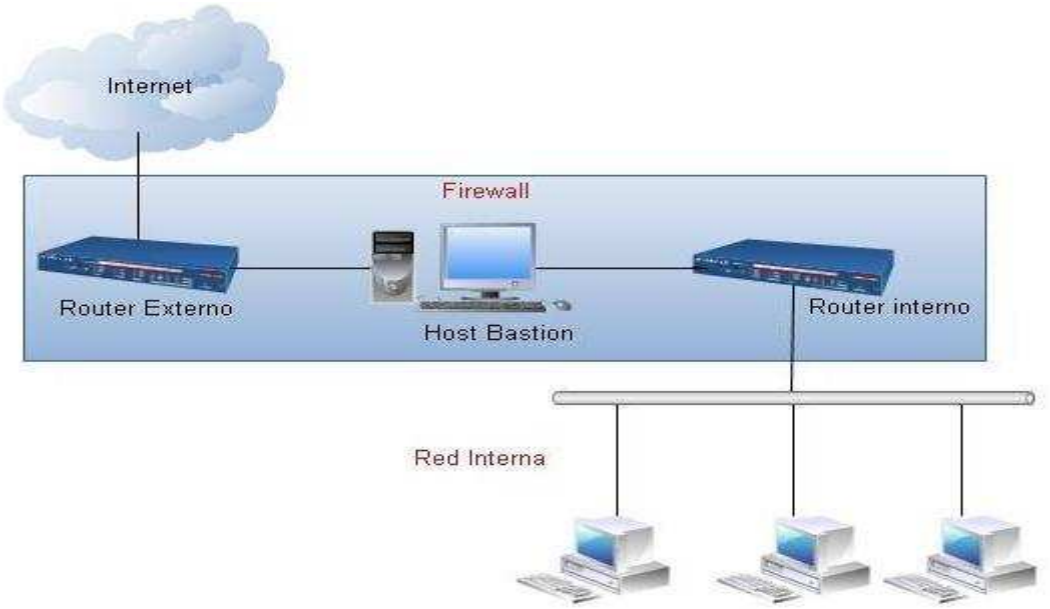

Figura 4. Arquitectura de subred de protección

Con esta arquitectura se agrega una nueva capa de seguridad a la arquitectura anterior que aísla la red local de Internet. Cuando aislamos al host bastión en una red de perímetro, es posible reducir el impacto de que el bastión sea vulnerado por algún ataque.

Si un atacante logra vencer la protección del host bastión, solo podrá acceder a la red perimetral ya que la red interna sigue protegida por el router interno. De esta forma el atacante solo tendrá acceso a la red perimetral, ocultando todo el tráfico de la red local.

Esta arquitectura es la más segura a las anteriores ya que la red perimetral donde se encuentra el host bastión soporta aspectos de seguridad a nivel de red y de aplicación y provee un sitio seguro para conectar servidores públicos. Ésta red establece una capa de seguridad adicional, entre la red externa y la red interna protegida. Si un atacante penetra el host bastión de la red perimetral, solo será capaz de ver el tráfico en dicha red. Todo el tráfico en esta red deberá ser hacia el host bastión, o desde el host bastión hacia la red externa. Ya que el tráfico de la red interna no pasa por la red perimetral, estará a salvo de ser atacado por un intruso ya que se encuentra dentro de un router interno, inclusive si el host bastión

es vulnerado.

El router externo ofrece protección contra ataques provenientes de la red externa y administra el acceso de Internet a la red perimetral. De igual forma, protege tanto a la red perimetral como a la red interna.
El router interno protege la red interna de la red externa y de la perimetral administrando el acceso de ésta a la red interna; provee una segunda línea de defensa si el router externo es vulnerado.

El host bastión conectado a la red perimetral es el principal punto de contacto para conexiones de entrada desde la red externa, por ejemplo, servidores de correo electrónico (SMTP), conexiones FTP al servidor anónimo del sitio, consultas DNS al sitio, servidores web, entre otras.

4.2 Políticas de Diseño de Firewall

En este capítulo se definen las reglas del firewall que permiten el filtrado entrante y saliente, como el acceso a los protocolos de uso común.

La política de diseño es específica de cada firewall. Las reglas utilizadas para implementar la política de acceso a servicios de red. Debe ser con completo conocimiento de características tales como las limitaciones y capacidades del firewall, y las amenazas y vulnerabilidades asociadas con las tecnologías utilizadas (como TCP/IP). Los firewalls generalmente implementan una de dos políticas de diseño básicas:

- Permitir todo servicio, a menos que sea expresamente restricto, o
- Denegar todo servicio, a menos que sea expresamente permitido.

La primera política es menos deseable, ya que ofrece más vías por las cuales puede accederse a un servicio, evitando el firewall.

La segunda es más fuerte y segura, aunque es más restrictiva para los usuarios; es la más usada en todas las áreas de seguridad de la información[6].

Esta política es la que utilizaremos en la construcción del servidor Muro Cortafuego, donde denegamos todos los servicios y solo permitimos los servicios a utilizar por los usuarios.

A continuación definiremos algunas las reglas para llevar a cabo la implementación[7]:

Reglas del Firewall						
Protocolo	**Protocolo de transporte**	**Red de Origen**	**Puerto Origen**	**Red destino**	**Puerto Destino**	**Acción**
HTTP	TCP	192.168.4.0/24	Cualquiera	Cualquiera	80	Permitir
FTP	TCP	192.168.4.0/24	Cualquiera	Cualquiera	21	Permitir
ICMP		192.168.3.2		192.168.3.0/24		Permitir
ICMP		192168.4.1		192.168.4.0/24		Permitir
HTTP	TCP	Cualquiera		192.168.4.2	80	Permitir
FTP	TCP	192.168.1.2		192.168.4.3	21	Permitir
	TCP	Cualquiera		192.168.3.2	10000	Denegado

Tabla 1. Reglas de Firewall

4.3 Costo de Implementación Firewall en Linux

La implementación en servidores avanzados Firewall en Linux depende mucho de los servicios configurados en el servidor como son (Web, Correos, archivos, etc.), se puede configurar un firewall en el mismo servidor para tal fin.

[6] Textoscientificos.com, Planes de seguridad [En línea] http://www.textoscientificos.com/redes/firewalls-distribuidos/soluciones-seguridad/politicas-seguridad/planes-seguridad [Citado 31 de marzo 2009]
[7] KOMAR Brian, Beekelaar Ronald, Wettern Joern. Firewall For Dummies New York: Wiley Publishing, Inc 2003 P 125

Este es un mecanismo de seguridad excelente contra ataques desde internet o desde otra red local, en donde primero tiene que atravesar el **Firewall de Linux.** De esta manera si hay un ataque este se divide en dos y por lo tanto se dificulta, si el ataque es por email o gusanos simplemente se deniega el servicio.

Los principales beneficios al instalar un servidor FIREWALL LINUX son:

- Protege la información de ataques externos.
- Impide el acceso no autorizado a información valiosa de la red protegida.
- Reduce tráfico innecesario hacia o desde la red.

Estos firewalls pueden ser altamente restrictivos, ya que permiten un control total de la situación, denegando accesos por IP, tipos de paquete, puerto, etc., guardando ficheros log de los accesos y garantizando una seguridad medida.
Pueden incluir balanceo de carga, traducción de direcciones o puertos (NAT, NAPT).
Un firewall Linux es totalmente flexible y adaptable a las necesidades particulares de cada situación. En términos monetarios no hay forma más económica y confiable para filtrar paquetes. El costo de instalar un firewall Linux puede ser hasta diez veces más económico que comprar un firewall por hardware o paquetes de software comerciales[8].

[8] E-proyecta.es, implementación de servidores avanzados firewall en Linux [En Línea] http://www.e-proyecta.es/linux-iptables.html [Citado 01 de abril 2009]

4.4 Topología de la de red del muro Cortafuego

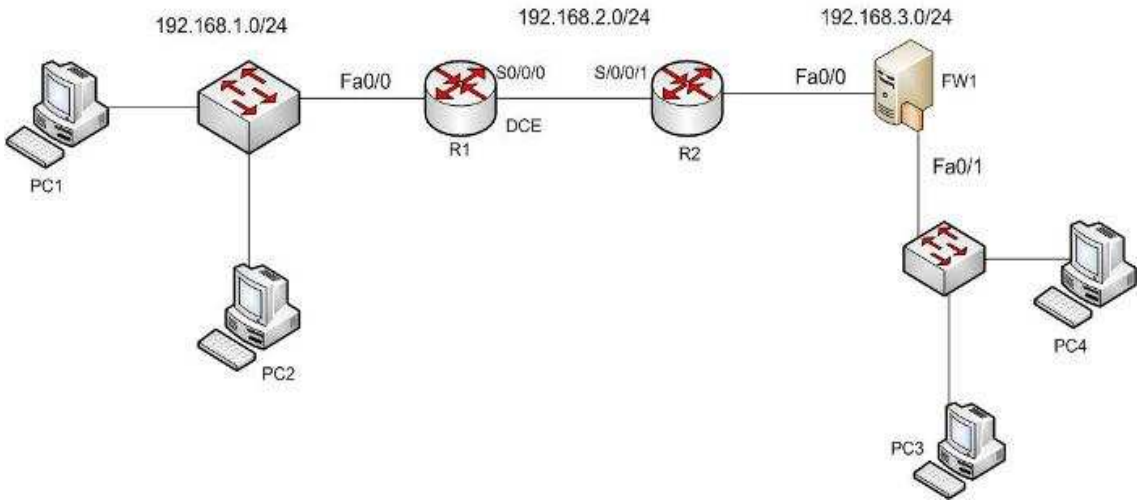

Figura 5. Topología Firewall bastión

Esta topología es una Arquitectura de firewall bastión de acceso en el cual el servidor Firewall tiene dos interfaz de red en donde una comunica a una red LAN 1 y la otra comunica con red local LAN 2.
En este tipo de arquitectura el trafico de intercambio entre la red interna y la red externa está sometido a las reglas de un solo firewall, con lo que debe ser los más robustos posible.

Para el caso de la topología de red a implementar en la figura 5, esta arquitectura se utiliza para proteger subredes donde puede haber servidores críticos de otras subredes que componen la red interna.
Para la implementación de la topología anterior utilizaremos los siguientes dispositivos como son:

- *Dispositivos intermedios*: en los cuales se utilizan dos Switches, dos Routers y un servidor Firewall en los que proporciona conectividad y garantiza que los datos fluyan a través de la red.

- *Dispositivos finales*: en los cuales se utilizaran cuatros hosts.

Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Mascara de Subred	Gateway
R1	Fa0/0	192.168.1.1	255.255.255.0	No aplicable
	S0/0/0	192.168.2.1	255.255.255.0	No aplicable
R2	Fa0/0	192.168.3.1	255.255.255.0	No aplicable
	S0/0/1	192.168.2.2	255.255.255.0	No aplicable
PC1	N/A	192.168.1.2	255.255.255.0	192.168.1.1
PC2	N/A	192.168.1.3	255.255.255.0	192.168.1.1
FW1	Fa0	192.168.3.2	255.255.255.0	192.168.3.1
	Fa1	192.168.4.1	255.255.255.0	
PC3	N/A	192.168.4.2	255.255.255.0	192.168.4.1
PC4	N/A	192.168.4.3	255.255.255.0	192.168.4.1

Tabla 2. Tabla de direccionamiento

En la tabla anterior especificamos el direccionamiento de cada dispositivo que interviene en la topología, con este direccionamiento haremos la practica respectiva para implementación del servidor Firewall Linux.

4.5 Componentes del Sistema Firewall Linux.

Los componentes básicos para la implementación del servidor Firewall Linux son:

- **Requerimientos de Hardware:** Los sistemas GNU/Linux pueden instalarse en equipo con capacidades muy reducidas (o limitadas), para tener un entorno con un buen desempeño y que soporte las nuevas características de los sistemas incluidos en cualquier distribución, se recomienda un equipo con las siguientes características:

  - ✓ Procesador Intel Pentium III / AMD Athlon, 550MHz (o mayor)
  - ✓ 512 MB RAM
  - ✓ 10 GB en disco duro

- ✓ 2 Interfaz de red.

Dentro del proceso práctico en la implementación del servidor Muro cortafuego utilizamos un ordenador con las siguientes características:

- ✓ Procesador Core 2 Duo, 2.80 GHz
- ✓ 4 Gb de ram
- ✓ 6 Gb en disco duro
- ✓ 2 interfaz de red marca (Encore y genérica).
- ✓ Cable directo

- **Requerimientos de software:** Para la implementación de un servidor Muro Cortafuego se tiene disponible las distribuciones de Linux CentOS, Debian, Fedora y RedHat Enterprise, Ubuntu y BSD; La ventaja de instalar un sistema de distribución Linux es la funcionalidad, adaptabilidad y robustez.
  Dentro de la práctica utilizamos el sistema operativo de distribución Linux Centos versión 5.2 el cual tiene una serie de paquetes para ser utilizados a nivel de servidor como son los servicios (DNS, Firewall, Email, Web, etc.).
  Centos tiene numerosas ventajas con respecto algunos de los otros proyectos de software libre, incluyendo la gran creciente y activa comunidad de usuarios, soporte técnico gratuito por vías IRC chat, listas de correo, foros, preguntas más frecuentes.

5. CONSTRUCCIÓN DEL SISTEMA FIREWALL MEDIANTE IPTABLES

5.1 Definición de Iptables

Es una herramienta en línea de comandos usados para configurar reglas de filtrado de paquetes en los kernels de Linux 2.4 y 2.6, soporta IPv4 e IPv6; además Iptables ha demostrado ser una excelente solución como medida de seguridad perimetral[9].

Iptables es un firewall libre ya que se encuentra bajo licencia GNU GPL y trabaja en la capa 2(Internet) del modelo TCP/IP ya que los filtros de paquetes trabaja principalmente en la capa 2.

También se le conoce como la herramienta de espacio de usuario, es decir área de memoria donde todas las aplicaciones, en modo de usuario, pueden ser intercambiadas hacia memoria virtual cuando sea necesario, a través de la cual los administradores crean reglas para cada filtrado de paquetes y módulos de NAT.

5.2 Instalación de Iptables

Para la instalación de Iptables en los sistemas operativos CentOS 4 y 5, Red Hat Enterprise Linux 5 o White Box Enterprise Linux 4 y 5 solo se necesita hacer lo siguiente en la consola de Shell de Linux:

Yum -y install Iptables

Como nos muestra la figura 6.

[9] Netfilter, The netfilter.org Project [En línea] http://www.netfilter.org [Citado en abril 06 de 2009]

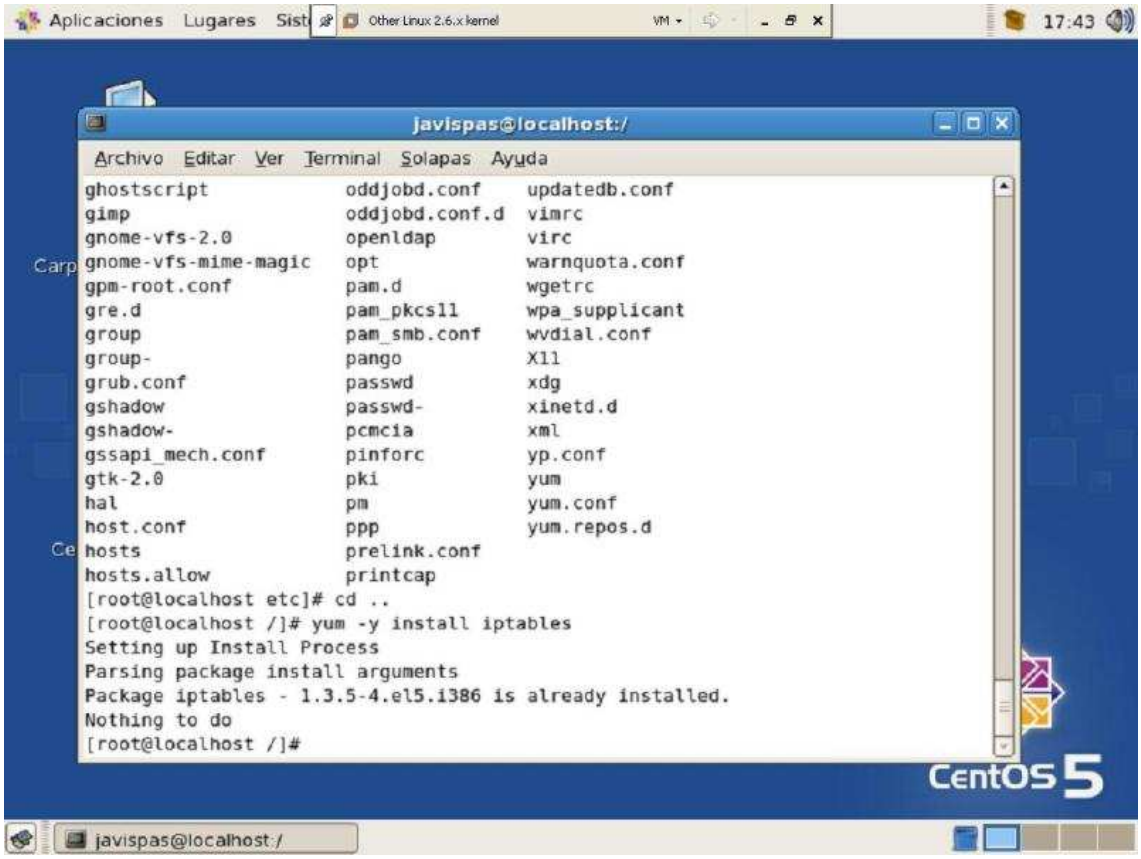

Figura 6. Instalación Iptables

En el caso que la distribución de Linux sea Red Hat Enterprise Linux 4 solo basta por ejecutar el siguiente comando:

Up2date -i Iptables

5.3 Configuración Iptables

La configuración de Iptables se basa en tres tablas diferentes y una serie de cadenas asociadas a cada una de estas tablas. Las tablas son:

- ✓ **Filter:** Revisa el contenido de los paquetes de información que atraviesan el firewall, estableciendo la acción que viene determinada en las directivas. Las cadenas asociadas a la tabla filter son:

  - **Input:** Analiza los paquetes recibidos en una interfaz de red.

- **Output:** Analiza los paquetes que son enviados por la misma interfaz de red.

- **Forward:** Chequea los paquetes que atraviesan una de las interfaces de red del firewall y los envía a la otra.

✓ **NAT:** Convierte las direcciones utilizando NAT, SNAT en origen y en destino DNAT. Las cadenas soportadas por la tabla NAT son:

- **Prerouting:** La cadena modifica los paquetes recibidos por una interfaz de red traduciendo sus direcciones de destino DNAT.

- **Postrouting:** La cadena modifica los paquetes antes de enviarse a través de una interfaz de red traduciendo sus direcciones de origen SNAT.

✓ **Mangle:** Modifica los parámetros TTL y TOS de las cabeceras de los paquetes IP.

- **Prerouting:** La cadena modifica los paquetes recibidos en una interfaz de red cuando llegan[10].

Las acciones que pueden ejecutarse sobre los paquetes que atraviesan el firewall son:

- ACCEPT: Da la orden de aceptación de un paquete para dejarlo travesar las reglas del cortafuego. Esto es lo contrario de los objetivos Drop/Deny, así como también del objetivo reject.

- DROP: En el caso que uno o varios paquetes sean denegados, simplemente son borrados, y no son tomados acciones futuras. No se responde al host emisor que fue denegado, ni el host receptor del paquete es notificado en ninguna forma. El paquete simplemente desaparece.

[10] PICOUTO Fernando, LORENTE Iñaki. Hacking y Seguridad en Internet. México: Alfaomega Grupo Editor, S.A, 2008. P 403

- REJECT: Este es básicamente lo mismo que una política u objetivo Drop/Deny, excepto que solo enviamos una respuesta al host emisor informándole que el paquete fue denegado.

Todos los paquetes están sujetos a una tabla y pueden ser verificados por varias reglas dentro de una misma cadena.

5.4 Configuración Tablas

La sintaxis de los comandos de Iptables es la siguiente:

Iptables [-t <nombre-tabla>] <comando> <nombre-cadena> <parámetros> <opciones>

Las acciones que pueden ejecutarse sobre los paquetes que atraviesan el firewall son ACCEPT; DROP.

- **<nombre-tabla>:** Se selecciona la tabla que se va a utilizar, siendo la tabla por defecto filter.

- **<comando>:** Hace referencia a la acción que va a llevar a cabo, como eliminar, añadir, o modificar reglas de una cadena, que viene especificada en **<nombre-cadena>.** Solo se permite un comando por cadena. Se escriben en mayúsculas.

- **A:** Se añade la regla al final de la cadena especificada.
- **D:** Elimina la regla de una cadena especificada por un numero ordinal.
- **C:** Chequea una regla antes de añadirla a la cadena.
- **F:** Elimina la cadena seleccionada eliminando todas las reglas que la componen.
- **E:** Renombra una cadena.
- **H:** Lista de comandos Iptables.
- **I:** Inserta una regla dentro de una cadena.
- **N:** Crea una nueva cadena y la nombra.
- **R:** Reemplaza una regla en una cadena.
- **L:** Lista las reglas de la cadena especificada tras un comando.

- **X:** Elimina una cadena.
- **P:** Ejecuta la política por defecto sobre una cadena, ya que si los paquetes la atraviesan sin cumplir ninguna regla, se realiza una acción que puede ser ACCEPT o DROP[11].

  - **<parámetros>:** Definen las acciones que la regla produce.
    - **f:** Aplica la regla solo a los paquetes fragmentados.
    - **o:** Configura el adaptador de red de salida para una regla usándose en la cadena UTPUT, FORWARD, y POSTROUTING, en las tablas **nat** y **mangle.**
    - **i:** Configura los adaptadores de entrada de red para ser habilitados por una regla en particular. En Iptables con la tabla filter solo se podrán utilizar cadenas INPUT y FORWARD cuando se utilice por **filter** y PREOROUTING con **nat** y **mangle.**
    - **s:** Especifica la dirección origen del paquete.
    - **p:** Especificará el protocolo al que se aplica la regla; si esta especificación no se lleva a cabo aplicará a todos los protocolos.
    - **d:** Detalla el nombre del sistema destino, dirección IP o IP de red de un paquete.
    - **j:** Especifica la opción de disposición de paquete para esta regla.

  Al configurar una regla para un protocolo determinado, también se puede implementar otro tipo de opciones como son:

    - **dport:** Configura el puerto destino de tráfico. Si se da un puerto o intervalos de puertos, la regla solo se aplica a estos, si no se especifican entonces se aplica a todos los puertos de origen.
    - **Sport:** Configura el puerto de origen del trafico.
    - **Syn:** Este indicador debe estar activado y el indicador ACK debe ponerse a cero en un mensaje TCP, cuando se realiza una petición de establecimiento de conexión. Para configurar el indicador syn, se debe indicar la siguiente sintaxis **-p tcp –syn.**
    - **Tcp-flags:** Selecciona los paquetes TCP con un conjunto de bits o

[11] PICOUTO Fernando, LORENTE Iñaki. Hacking y Seguridad en Internet. México: Alfaomega Grupo Editor, S.A, 2008. P 405

flags específicos para una regla. Esta opción establece dos argumentos: el primero de ellos establece los indicadores que se pueden comprobar y el segundo los que deben estar habilitados. Los valores que se pueden utilizar son: ACK, RST, SYN, URG, PSH.

- **<opciones>:** Para habilitar características en los paquetes TCP se pueden utilizar una serie de indicadores. Este indicador es –m y tiene una serie de opciones.
    - **Estados de Conexión:** Se verifica la pertenencia de un paquete a una conexión dada. Los estados de conexión son: ESTABLISHED, RELATED, INVALID, NEW.
    - **Direcciones MAC de origen:** Para controlar la dirección MAC de origen del paquete.
    - **Puertos Múltiples:** Se pueden seleccionar rangos de puertos tanto de origen como de destino.
    - **Puertos Marcados.**
    - **Limites de Frecuencia.**
    - **ToS:** Se pueden comparar los códigos de servicio.´
    - **TTL:** Se puede verificar un valor dado de TTL.
    - **ID de usuario/grupo/sesión de proceso.**
    - **Propietario del Proceso.**

Un ejemplo de una regla de Iptables aplicando los parámetros anteriores seria:
Iptables -A **FORWARD** -i eth1 -o eth0 -j **ACCEPT**
Esta regla nos permite el reenvió de paquetes desde una interfaz local (eth1) hacia una interfaz de red pública (eth0).

5.5 Establecimiento de rutas de acceso del Firewall

Las rutas que se establecen cuando el tráfico de datos pasa por un Firewall y atraviesan las siguientes tablas y cadenas son:

5.5.1 Fases de un paquete al atravesar el Firewall.

Los pasos necesarios para la aceptación de un paquete cuando atraviesa el Firewall serán descritos a continuación:

Pasos	Tabla	Cadena	Descripción
1			Los datos de entrada, ya por internet.
2			Llegada a la interfaz de red, en este caso sería eth0.
3	mangle	PREROUTING	Cadena usada para modificar paquetes, o para cambiar el TOS.
4	nat	PREROUTING	Cadena usada principalmente para hacer DNAT (traducción de dirección de destino). El SNAT (traducción de dirección de origen)
5			Decisión de enrutamiento
6	mangle	FORWARD	El paquete es enviado a la cadena FORWARD de la tabla mangle
7	filter	FORWARD	El paquete es enrutado hacia la cadena FORWARD. Los paquetes reenviados pasan por aquí y es donde se hace todo el filtrado.
8	mangle	POSTROUTING	Esta cadena se usa para efectuar los tipos específicos de modificación de paquetes que se quiera llevar a cabo después de que todos los tipos de decisiones de Enrutamiento se hayan tomado.
9	nat	POSTROUTING	Cadena usada para efectuar SNAT. Aquí se realiza el enmascaramiento

11			Salida por la interfaz de red en este caso sería eth1.
12			Switch (red Local)

Tabla 3. Pasos de un paquete cuando atraviesa el Firewall.

5.5.2 Fases de entrada de un paquete al Firewall.

Las rutas para el tráfico que llega al Firewall se describen a continuación:

Pasos	Tabla	Cadena	Descripción
1			Los datos de entrada, por internet.
2			Llegada a la interfaz de red, en este caso sería eth0.
3	mangle	PREROUTING	Cadena usada para modificar paquetes, o Para cambiar el TOS.
4	nat	PREROUTING	Cadena usada principalmente para hacer DNAT (traducción de dirección de destino). El SNAT (traducción de dirección de origen)
5			Decisión de enrutamiento
6	mangle	INPUT	cadena Usada para modificar paquetes después de que hayan sido enrutados, antes de que se envíen al Proceso de destino.
7	filter	INPUT	Se filtra todo el tráfico entrante destinado a nuestra red local.
8			Proceso/aplicación local, en este caso programa cliente/servidor.

Tabla 4. Pasos de un paquete cuando llega al Firewall.

5.5.3 Fases de salida de un paquete del Firewall.

Las rutas para el tráfico que se envía desde el Firewall se describen a continuación:

Pasos	Tabla	Cadena	Descripción
1			Proceso/aplicación local.
2			Decisión de enrutamiento, dirección de origen a usar, interfaz de salida, y otra información que necesita ser Recopilada.
3	mangle	OUTPUT	Cadena en donde se modifican los paquetes.
4	nat	OUTPUT	Esta cadena usada para hacer NAT a los paquetes que salen desde el host.
5	filter	OUTPUT	Se filtra los paquetes salientes del Firewall.
6	mangle	POSTROUTING	Se utiliza para modificar los paquetes antes de que dejen el Firewall, después de tomar las decisiones de enrutamiento.
7	nat	POSTROUTING	Se efectúa la traducción de las direcciones de red de origen (SNAT, Source Network Address Translation)
8			Salida por la interfaz de red en este caso sería eth0.

Tabla 5. Fases de salida de un paquete de un firewall

5.6 Conceptos básicos de Scripts Iptables de Linux.

Script Iptables hace referencia a programas escritos para la Shell de UNIX/LINUX, la programación en Shell-script es muy útil para resolver tareas repetitivas, típicas de los Administradores. Son ficheros de texto que contienen comandos y son directamente ejecutables por el sistema.

La Shell permite al usuario interactuar con el Kernel a través de la interpretación de los comandos que el usuario ingresa en la línea de comandos ó a través de los scripts, archivos que ejecutan con un conjunto de comandos[12].

En la implementación de firewall para esta práctica se utilizara Script con las reglas de Iptables y esta a la vez se ejecutará de forma automática cuando el sistema operativo Linux se inicie.

Las ejecuciones de los Scripts se deben configurar en el sistema operativo Linux desde los ficheros rc.

5.6.1 Declaración de un Script.

La declaración de un script se hace insertando en la primera línea del Script
#!/bin/sh
Se llama a sh y éste se encarga de leer línea por línea el archivo y ejecutarlo al mismo tiempo.

[12] Observatorio Tecnológico, Tutorial Shell Scripts I [En Línea] http://observatorio.cnice.mec.es/modules.php?op=modload&name=News&file=article&sid=573[Citado en 15 de abril 2009]

5.6.2 Declaración de Variables.

Para la declaración de variables en los Scripts de Iptables solo basta con asignarle un valor a la variable.

Ejemplos:

Valor =7
IPT=/sbin/Iptables
EXTIF=”eth1”
IP_EXT= “100.101.102.103”

Cuando se vaya a invocar una variable solo basta con colocar el signo $variable.

5.6.3 Comentarios.

Para comentar las reglas de Iptables o colocar encabezado a los scripts se utilizar el símbolo #.

Ejemplo:
# Tarjeta de red y dirección IP externa
IP_EXT= “100.101.102.103”
TARJ_EXT=”eth0”.

Y para los encabezados seria:
```
########################################
#    Scripts de Iptables con una tarjeta de      #
#       Red  externa y otra interna                 #
########################################
```

5.6.4 Cargas de Módulos de Iptables.

Los módulos de Iptables que son necesarios para que funcione el script, ya que nos permite controlar de estado de la conexión, usar el log para el registro entre otros dependiendo de la necesidades. Los módulos más importantes son:

#Módulos a Cargar
/sbin/modprobe ip_tables
/sbin/modprobe iptable_filter
/sbin/modprobe iptable_mangle
/sbin/modprobe iptable_nat
/sbin/modprobe ipt_LOG
/sbin/modprobe ipt_state

5.6.5 Políticas por defecto.

La política por defecto seria denegar todo el tráfico que no esté incluido en las reglas de Iptables. La opción –P cambia una política para una cadena.
En el siguiente ejemplo se descartan con DROP todas las conexiones que ingresen INPUT, todas las conexiones que se reenvíen FORWARD y todas las conexiones que salgan OUTPUT y quedaría así:

Establecemos política por defecto
Iptables -P INPUT DROP
Iptables -P OUTPUT DROP
Iptables -P FORWARD DROP

5.6.6 Limpieza de reglas específicas.

Para crear nuevas reglas se deben borrar las existentes para el tráfico entrante, tráfico reenviado y tráfico saliente así como el NAT.
Iptables -F INPUT
Iptables -F **FORWARD**
Iptables -F OUTPUT
Iptables -F -t nat

5.7 Implementación de Iptables para una Red Local

Al principio de este capítulo se define el funcionamiento de la herramienta Iptables como firewall para la creación de reglas que permite denegar o aceptar el tráfico desde una red pública a una red local o viceversa.

Ahora a partir del concepto de Iptables procedemos hacer la implementación de la topología de red hablada en el capítulo 4.
Para la realización de la practica se utilizó una maquina virtual Linux Centos 5.2 creada con el programa VMware Workstation.

Antes de proceder con la respectiva implementación se debe seguir una serie de pasos previos que se presentan a continuación, para una mejor compresión para el lector y posible administrador de Seguridad de redes.

5.7.1 Esquema de laboratorio.

Retomamos la Topología de red de la figura 5 del capítulo 4

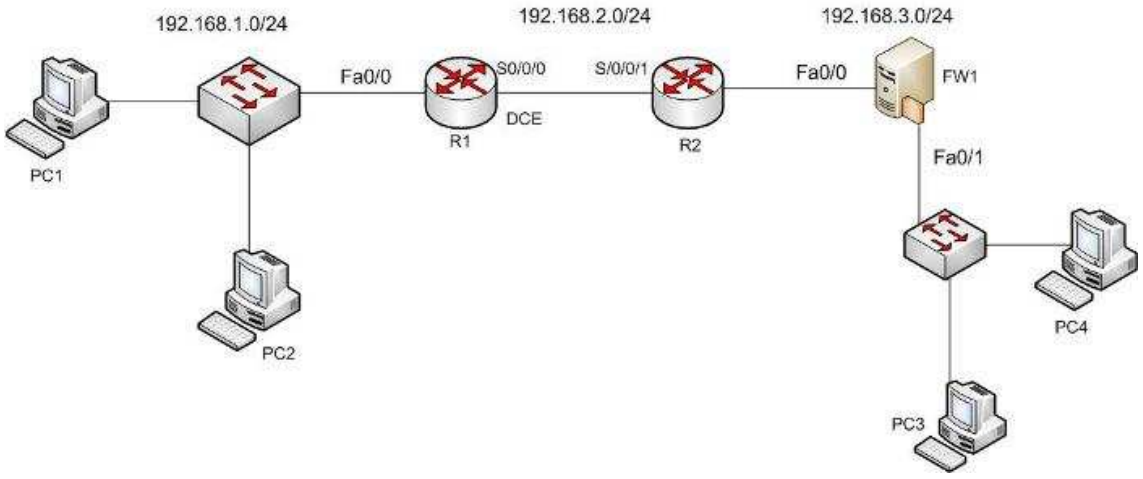

Figura 5. Topología Firewall bastión

Las respectivas configuraciones de red quedarían así:

Configuración del Router 1:

1. Configure la dirección IP en Fa0/0
   a. Dirección IP: 192.168.1.1
   b. Mascara de Subred: 255.255.255.0
   c. Default Gateway: No aplica

2. Configure la dirección IP en S0/0/0
   a. Dirección IP: 192.168.2.1
   b. Mascara de Subred: 255.255.255.0
   c. Default Gateway: No aplica

Configuración del Router 2:

1. Configure la dirección IP en Fa0/0
   a. Dirección IP: 192.168.3.1
   b. Mascara de Subred: 255.255.255.0
   c. Default Gateway: No aplica

2. Configure la dirección IP en S0/0/1
   a. Dirección IP: 192.168.2.2
   b. Mascara de Subred: 255.255.255.0
   c. Default Gateway: No aplica

Configuración del Firewall Linux:

1. Configure la dirección IP eth0
   a. Dirección IP: 192.168.3.2
   b. Mascara de Subred: 255.255.255.0
   c. Default Gateway: 192.168.3.1

2. Configure la dirección IP eth1
    a. Dirección IP: 192.168.4.1
    b. Mascara de Subred: 255.255.255.0
    c. Default Gateway: No aplica.

Configuración de los equipos Hosts:

1. Configure la dirección IP PC1
    a. Dirección IP: 192.168.1.2
    b. Mascara de Subred: 255.255.255.0
    c. Default Gateway: 192.168.1.1

2. Configure la dirección IP PC2
    a. Dirección IP: 192.168.1.3
    b. Mascara de Subred: 255.255.255.0
    c. Default Gateway: 192.168.1.1

3. Configure la dirección IP PC3
    a. Dirección IP: 192.168.4.2
    b. Mascara de Subred: 255.255.255.0
    c. Default Gateway: 192.168.4.1

4. Configure la dirección IP PC4
    a. Dirección IP: 192.168.4.3
    b. Mascara de Subred: 255.255.255.0
    c. Default Gateway: 192.168.4.1

5.7.2 Configuración de los Routers Cisco.

Ahora procedemos a configurar los Routers cisco con el cable consola conectado al PC en Hyperterminal de Windows Xp.

La configuración sería la siguiente para el Router 1:

Router> Enable

Router# config t

Router(config)# int Fa0/0

Router(config-if) # ip address 192.168.1.1 255.255.255.0

Router(config-if) # no shutdown

Router(config-if) # exit

Router(config)# int s0

Router(config-if) # ip address 192.168.2.1 255.255.255.0

Router(config-if) # clock rate 56000

Router(config-if) # no shutdown

Router(config-if) # exit

Router(config)# Router rip

Router(config-router)# network 192.168.1.0

Router(config-router)# network 192.168.2.0

Router(config-router)# exit

Router(config)# exit

Router# copy run start

La configuración sería la siguiente para el Router 2:

Router> Enable

Router# config t

Router(config)# int Fa0/0

Router(config-if) # ip address 192.168.3.1 255.255.255.0

Router(config-if) # no shutdown

Router(config-if) # exit

Router(config)# int S0/0/1

Router(config-if) # ip address 192.168.2.2 255.255.255.0

Router(config-if) # no shutdown

Router(config-if) # exit

Router(config)# Router rip

Router(config-router)# network 192.168.3.0

Router(config-router)# network 192.168.2.0

Router(config-router)# exit

Router(config)# exit

Router# copy run start

Configurado los Routers solo basta configurar el firewall y los dispositivos finales como son los hosts; hay que tener en cuenta que la conexión del servidor Cortafuego Linux debe estar conectado al Router 2 en la interfaz fa0/0 como lo indica la figura 5 con un **cable directo** por la interfaz eth0 del servidor Firewall Linux.

5.7.3 Configuración de tarjetas de red en VMware

Antes de iniciar la maquina virtual de Linux Centos se debe configurar las tarjetas de red en modo Custom en VMware ya que esta nos permite conectar a la red simulando un equipo físico.

Primero debemos configurar Virtual Network Editor ingresando al menú Edit de VMware 6.5 y realizamos los siguientes pasos:

1. Una vez seleccionado la opción Virtual Network Editor, escogemos la segunda pestaña Automatic Bridging y desactivamos la opción Automatic choose an available, esto con el fin de asignar las tarjetas física manualmente en modo bridged.

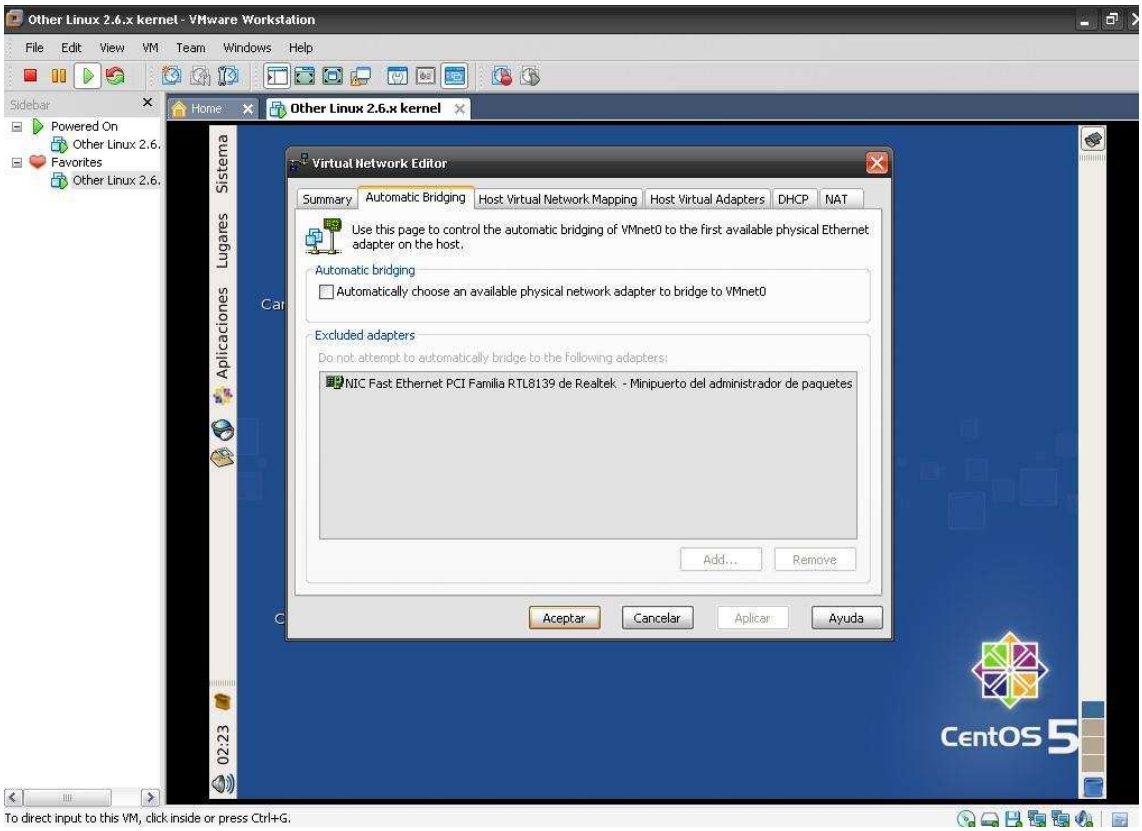

Figura 7. Configuración Bridge automático

2. A continuación se selecciona la tercera pestaña Host Virtual Network y ahí selecciona VMnet0 con una primera tarjeta físico, VMnet2 con otro NIC físico, y así sucesivamente dependiendo del número de tarjetas física que se requiera.

   Para la práctica de esta investigación quedaría de la siguiente manera:

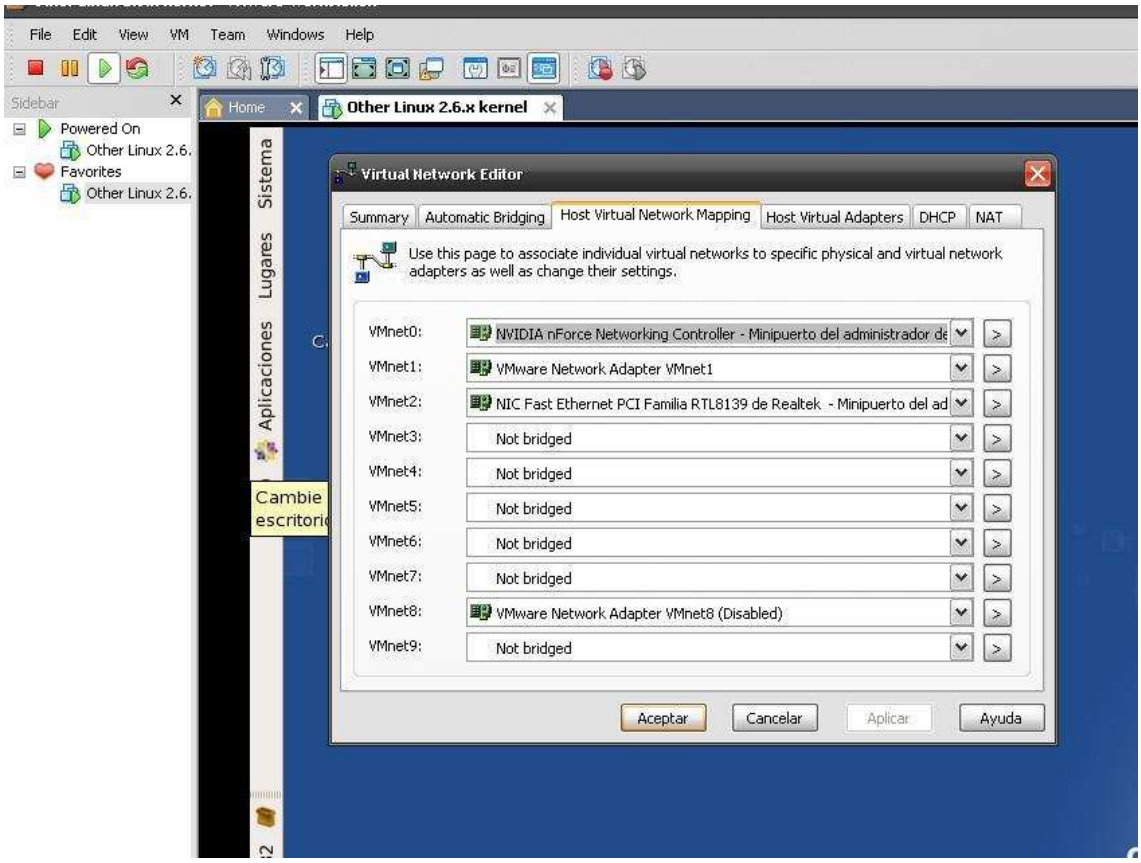

Figura 8. Configuración redes virtuales

Donde tenemos VMnet0 asignada a una tarjeta red física del fabricante Nvidia nForce y VMnet2 otra tarjeta de red fabricante Realtek

3. En la Consola del VMware se debe editar también los parámetros del NIC virtual. En el primer adaptador de red dejarlo en modo Custom y seleccionar VMnet0 (bridged), también hacer lo mismo con el segundo adaptador de red seleccionando VMnet2 (bridged).

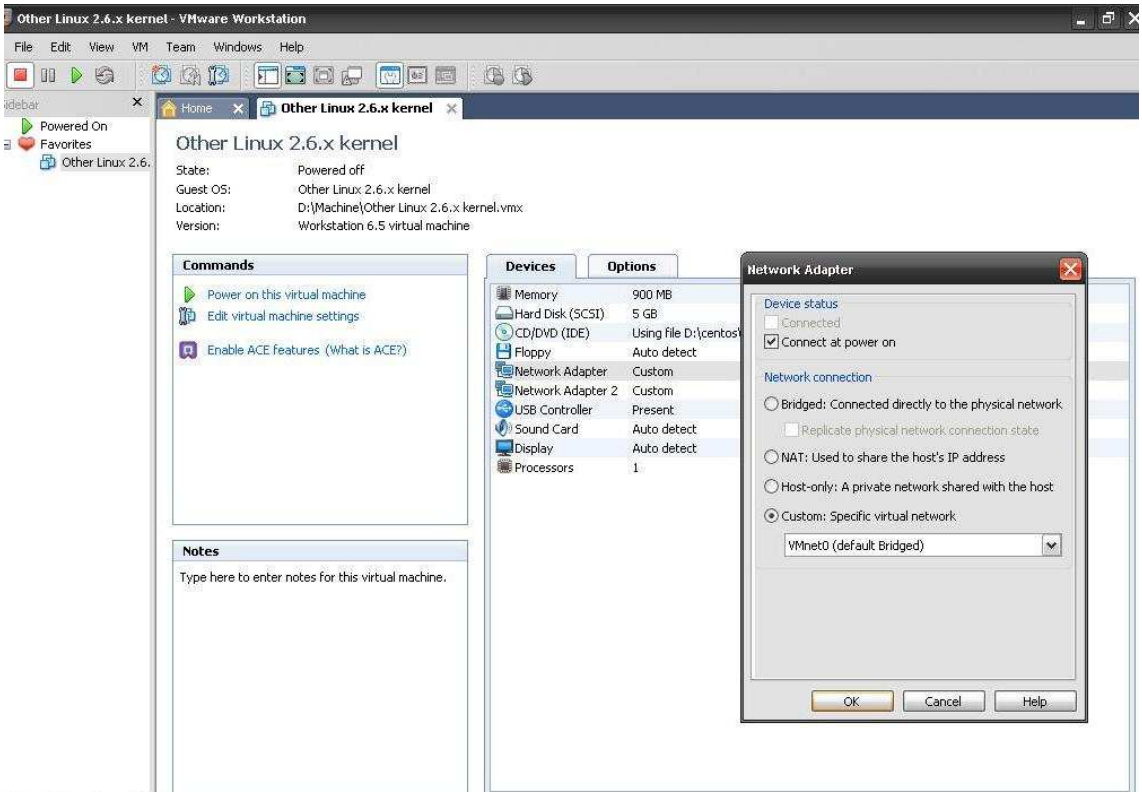

Figura 9. Configuración Nic virtual

Para configurar y adicionar tarjetas de red en WMware se lleva a cabo en la opción Edit virtual machine settings la cual permite agregar o remover dispositivos de almacenamiento, tarjeta de red, sonido entre otras.

5.7.4 Configuración de las IPs en la maquina virtual Linux Centos 5.2.

En la configuración de la IPs en la maquina virtual es necesario ingresar al sistema operativo Centos como administrador en este caso sería **root y Password** creado por el usuario esto con el fin de configurar las Ips de la tarjeta de red y la creación de Script Iptables que se explicara más adelante.

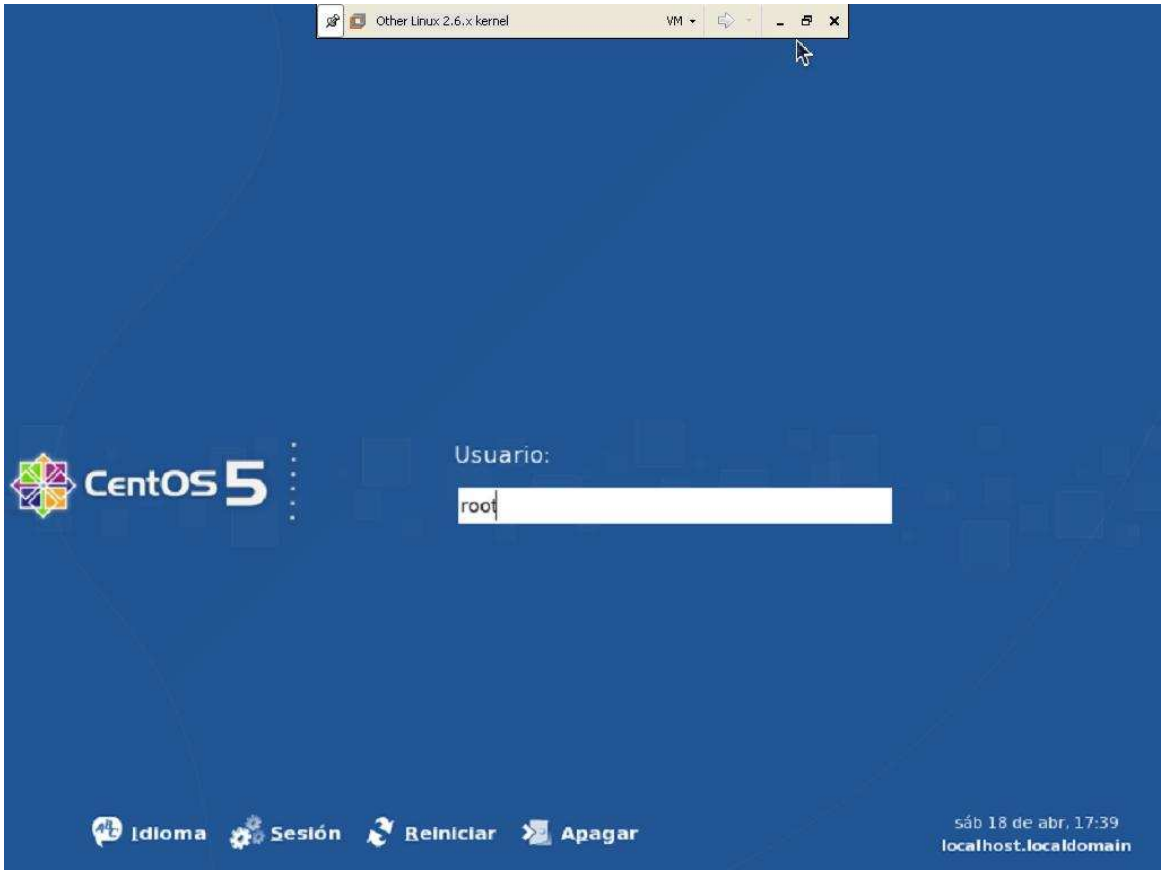

Figura 10. Iniciar Modo Administrador en Centos

Procedemos a configurar las interfaces eth0 y eth1 de Centos en la cual haciendo clic en Sistema, Administración y red como nos muestra la figura 11.

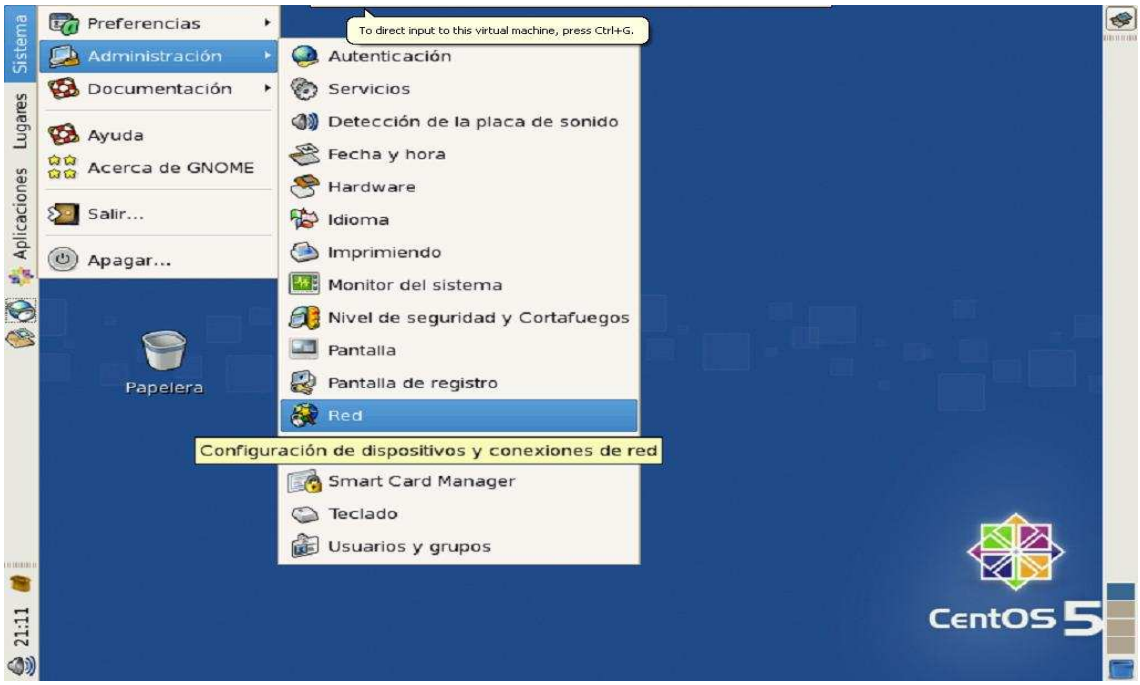

Figura 11. Configuración Tarjetas de red

Al seleccionar el dispositivo Red aparece una ventana con las interfaces eth0 y eth1

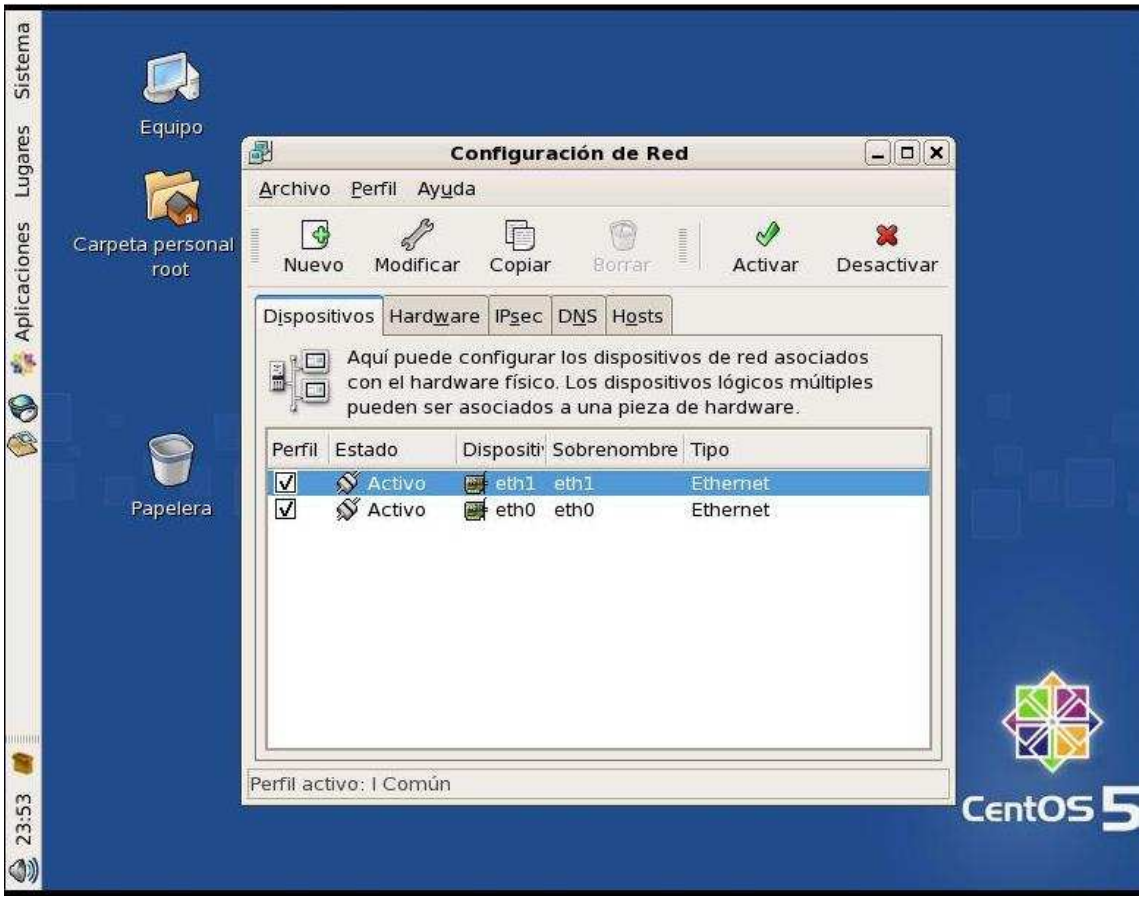

Figura 12. Configuración interfaces de red

Las interfaces en Linux tienen una referencia más un identificador de cantidad nombrada eth# en el cual es el nombre más común a la tarjetas de red, sin embargo pueden existir otros nombres, dependiendo del sistema operativo y el tipo de interfaz de red.

Procedemos a configurar la IP a la interfaz eth0, para la práctica de esta investigación es la que va ir conectada al Router 2, seleccionamos la interfaz eth0 y se ingresa la IP correspondiente. A continuación la figura 13 nos especifica el procedimiento que se debe realizar.

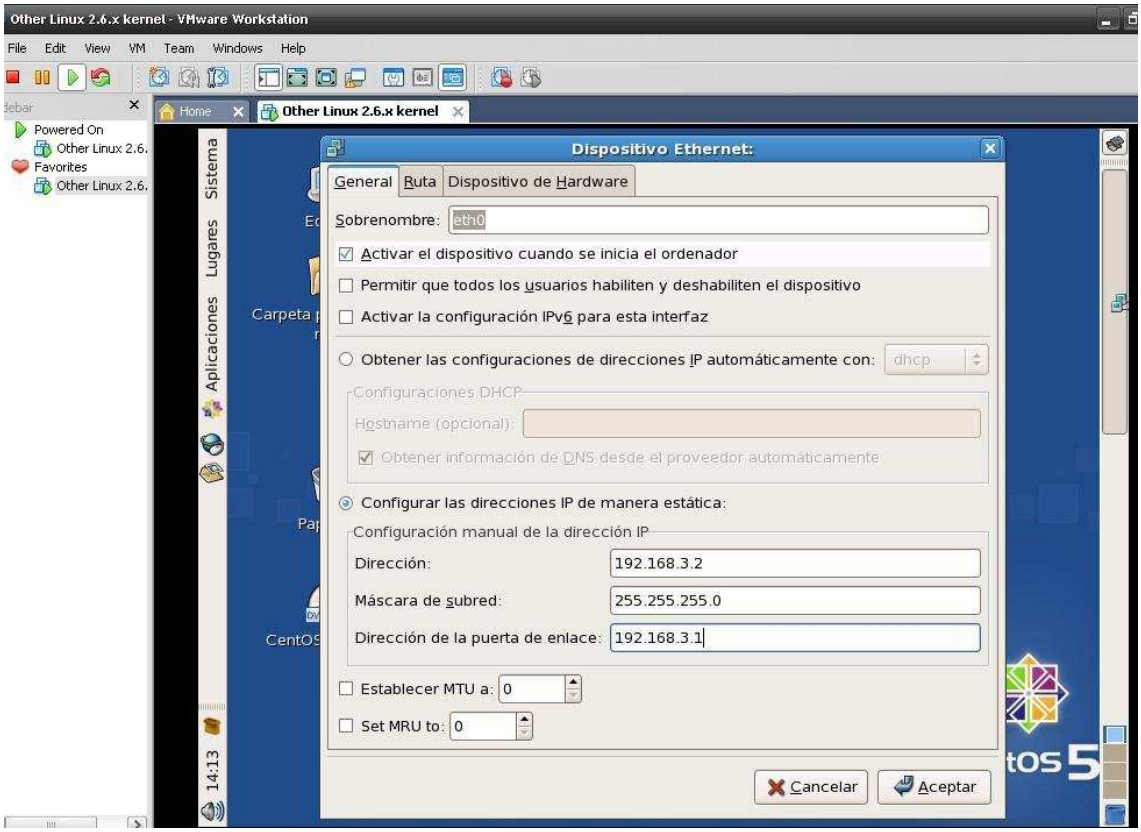

Figura 13. Configuración IP eth0

Y para la interfaz eth1 que es la comunica a la red local y es la red a proteger, el procedimiento de configuración seria igual al eth0.

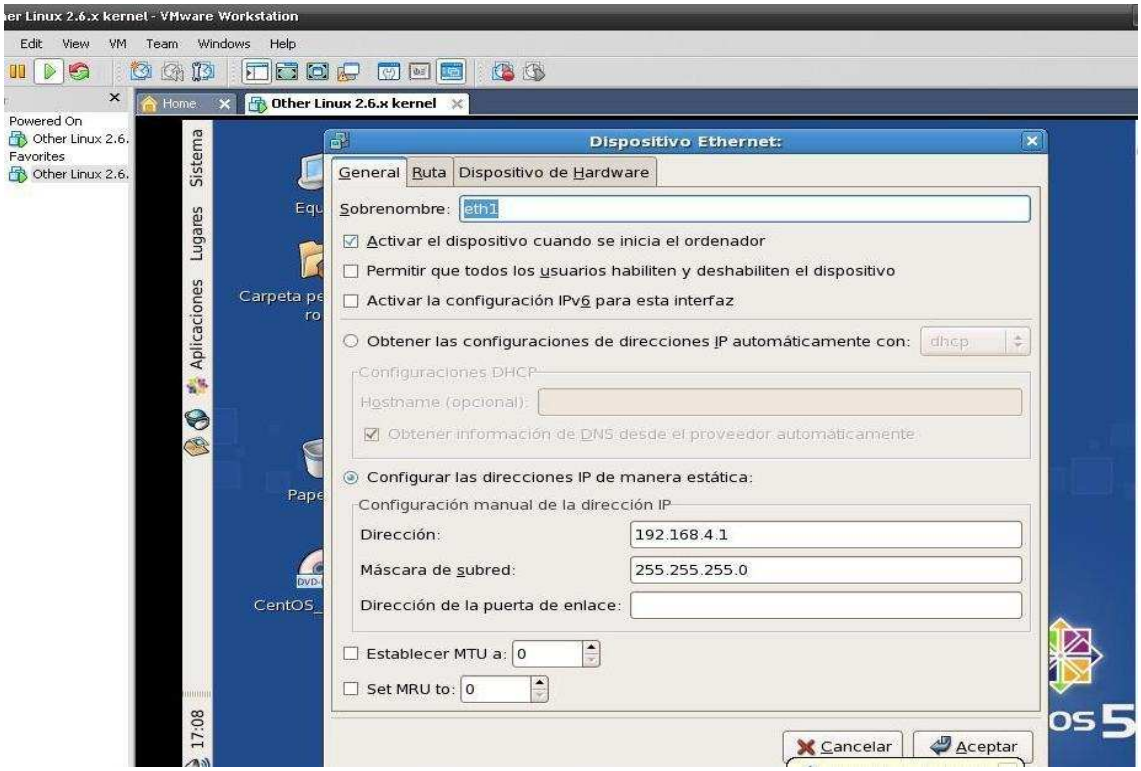

Figura 14. Configuración IP eth1

5.7.5 Configuración del Script Iptables.

En el proceso de la creación de Script dentro del Linux Centos debemos realizar los siguientes pasos:

1. Crear un archivo en dentro del fichero raíz /etc/rc.d/, específicamente en esta implementación se creó un archivo llamado rc.firewall.

   A continuación podremos observar gráficamente el proceso de creación de este archivo en el sistema operativo Centos.

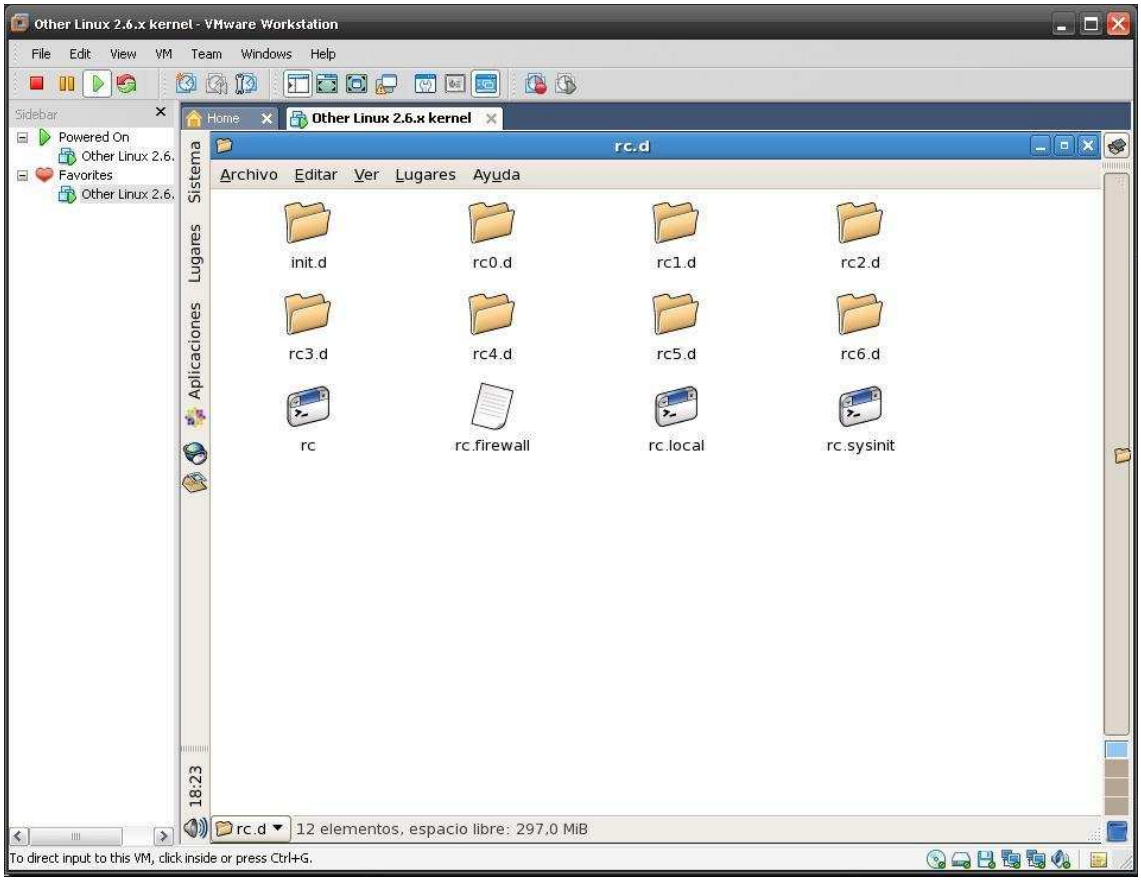

Figura 15. Creación de archivo script

2. Dentro del archivo rc.firewall crearemos las reglas de Iptables para políticas de seguridad que se definieron en un principio en el capítulo 4.

A continuación mostraremos el script del firewall que será usado finalmente en el archivo rc.firewall.

```
#!/bin/sh
#####################################################################
#  Scripts de Iptables para la creación del Firewall en Centos 5.2 con una  #
#  Tarjeta eth0 que comunica con una red exterior y una tarjeta eth1 que   #
#   comunica con la red local  a la que tiene que proteger.                 #
#####################################################################

##Variables
# Variables Tarjeta de red eth0 y dirección IP.
IP_EXT="192.168.3.2"
TARJ_EXT="eth0"

# Variables Tarjeta de red eth1 y dirección IP.
IP_INT="192.168.4.1
TARJ_INT="eth1"

# Variables Localhost.
IP_LO="172.0.0.1"
ADAP_LO="lo"

##Módulos de Iptables
#Carga de Módulos
/sbin/depmod –a

#Módulos a cargar
/sbin/modprobe ip_tables
/sbin/modprobe iptable_filter
/sbin/modprobe iptable_mangle
/sbin/modprobe iptable_nat
/sbin/modprobe ipt_LOG
/sbin/modprobe ipt_state
```

##Reglas

echo “ Aplicando Reglas del Firewall…”

#Eliminación de cualquier regla existente

iptables −F

iptables −X

iptables −Z

iptables −t nat –F

#Establecemos Política por defecto

iptables -P INPUT DROP

iptables -P OUTPUT DROP

iptables -P FORWARD DROP

iptables -t nat -P PREROUTING ACCEPT

iptables -t nat -P POSTROUTING ACCEPT

 # Acceso aplicaciones locales (localhost para conexiones locales)

iptables -A INPUT -i $ADAP_LO -j ACCEPT

iptables -A OUTPUT -o $ADAP_LO -j ACCEPT

#Establecer Nat solo a los puertos que se necesiten que salgan al exterior.

#Permite dar puerta de enlace a los host interno, en donde la puerta de enlace enruta los paquetes desde un nodo de la LAN hasta su nodo destino

iptables -A FORWARD -i $TARJ_INT -j ACCEPT

iptables -A FORWARD -o $TARJ_INT -j ACCEPT

 # Aceptamos que naveguen por el protocolo HTTP puerto 80

iptables -t nat -A POSTROUTING -o $TARJ_EXT -p tcp -m tcp --dport 80 -j MASQUERADE

#Aceptamos que naveguen por el protocolo FTP puerto 21

iptables -t nat -A POSTROUTING -s 192.168.4.0/24 -o $TARJ_EXT -p tcp -m tcp --dport 21 -j MASQUERADE

iptables -t nat -A POSTROUTING -s 192.168.4.0/24 -o $TARJ_EXT -p tcp -m tcp --dport 1024 -j MASQUERADE

##Filtramos el acceso de la red exterior a la red local.

REDIRECCIONES

Todo lo que venga por el exterior para puerto 80 lo redirigimos

A una maquina interna de la red local.

iptables -t nat -A PREROUTING -i $TARJ_EXT -p tcp --dport 80 -j DNAT --to-destination 192.168.4.2

#Los accesos de un IP determinada a FTP se redirigen a una

#maquina interna de la red local con ese servicio.

iptables -t nat -A PREROUTING -s 192.168.1.2 -p tcp --dport 21 -j DNAT --to-destination 192.168.4.3

#Permite hacer ping a host de la red local pero no viceversa.

iptables -A OUTPUT -p icmp --icmp-type echo-request -j ACCEPT

#Permite hacer ping a la red externa pero no viceversa.

iptables -A INPUT -p icmp --icmp-type echo-reply -j ACCEPT

#regla que permite desde un host de la red externa entrar al webmin del firewall por el puerto 10000

iptables -A INPUT -p tcp --dport 10000 -j ACCEPT

iptables -A OUTPUT -p tcp --sport 10000 -j ACCEPT

#Habilitar reenvió entre tarjetas de red del Firewall

echo 1 > /proc/sys/net/ipv4/ip_forward

 # Fin del script

Gráficamente la funcionalidad del firewall quedaría de la siguiente manera:

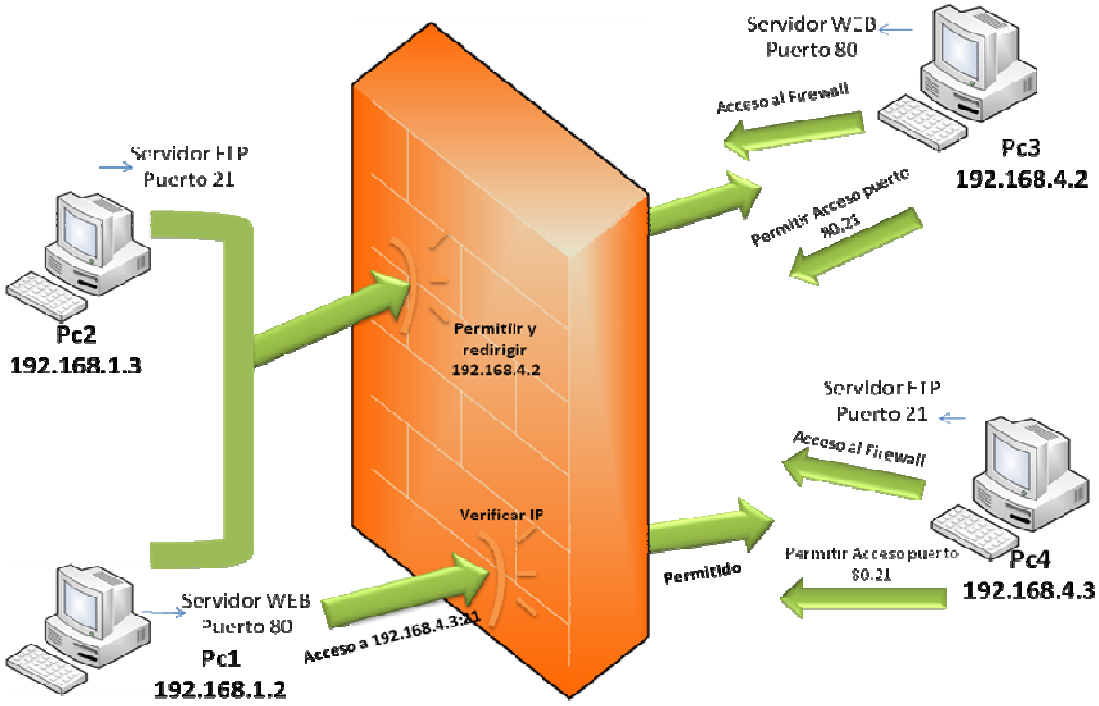

Figura 16. Funcionalidad del Firewall creado.

El script anexado al archivo rc.firewall se vería de la siguiente forma:

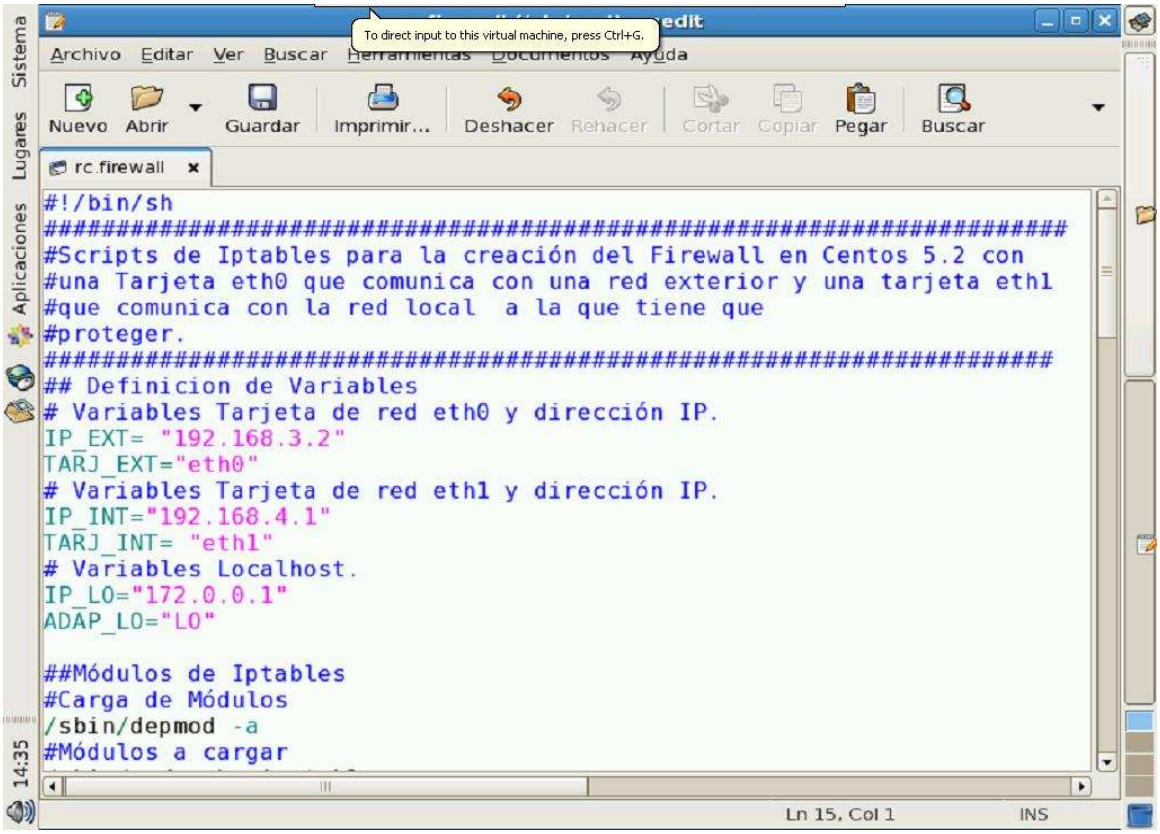

Figura 17.Script firewall

Ahora le damos los permisos de ejecución al archivo rc.firewall desde la terminal en modo **root** la sintaxis sería la siguiente manera:

#chmod +x rc.firewall

La figura 18 nos saca de cualquier duda para efectuar el permiso necesario para el script.

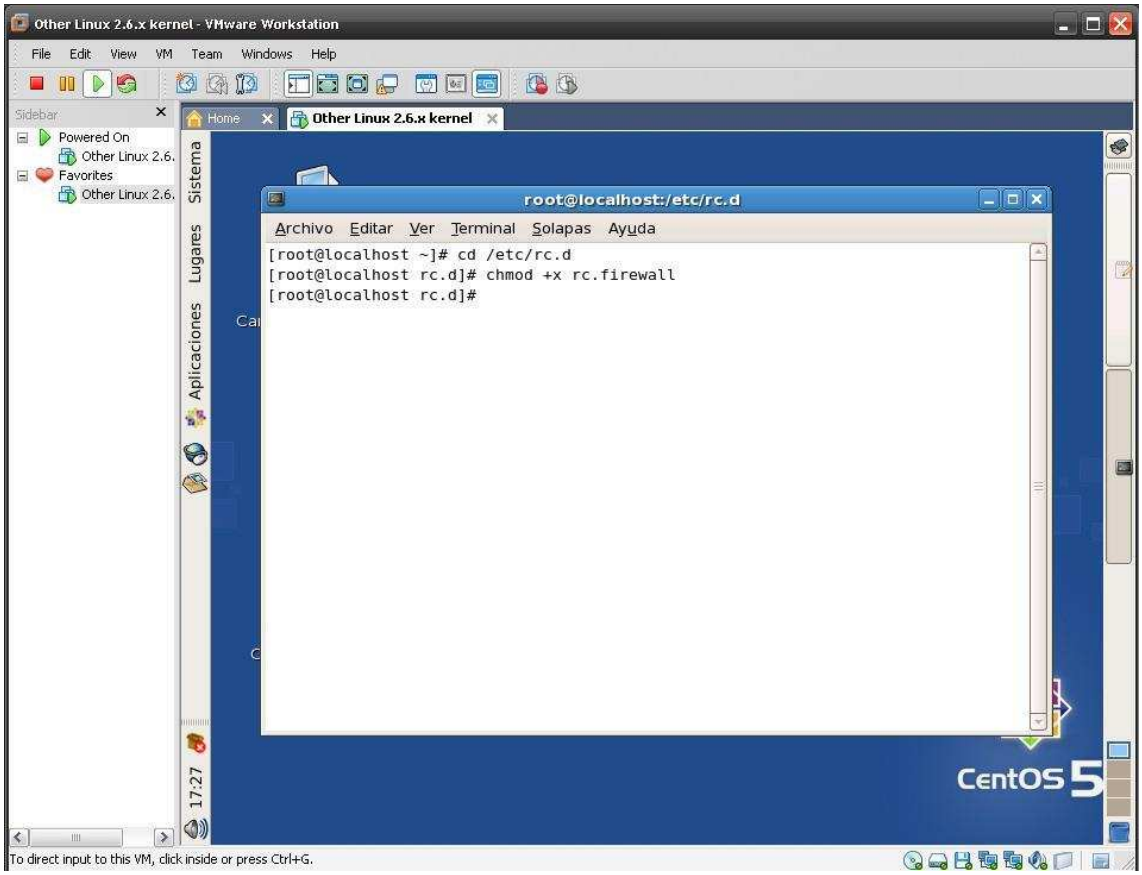

Figura 18. Permisos para archivo Script rc.firewall

Para que las reglas del Script rc.firewall se aplican al iniciar el sistema operativo es necesario editar el archivo rc.local ubicado en /etc/rc.d y agregarle al final la siguiente línea:

/etc/rc.d/rc.firewall

Se guarda los cambios.

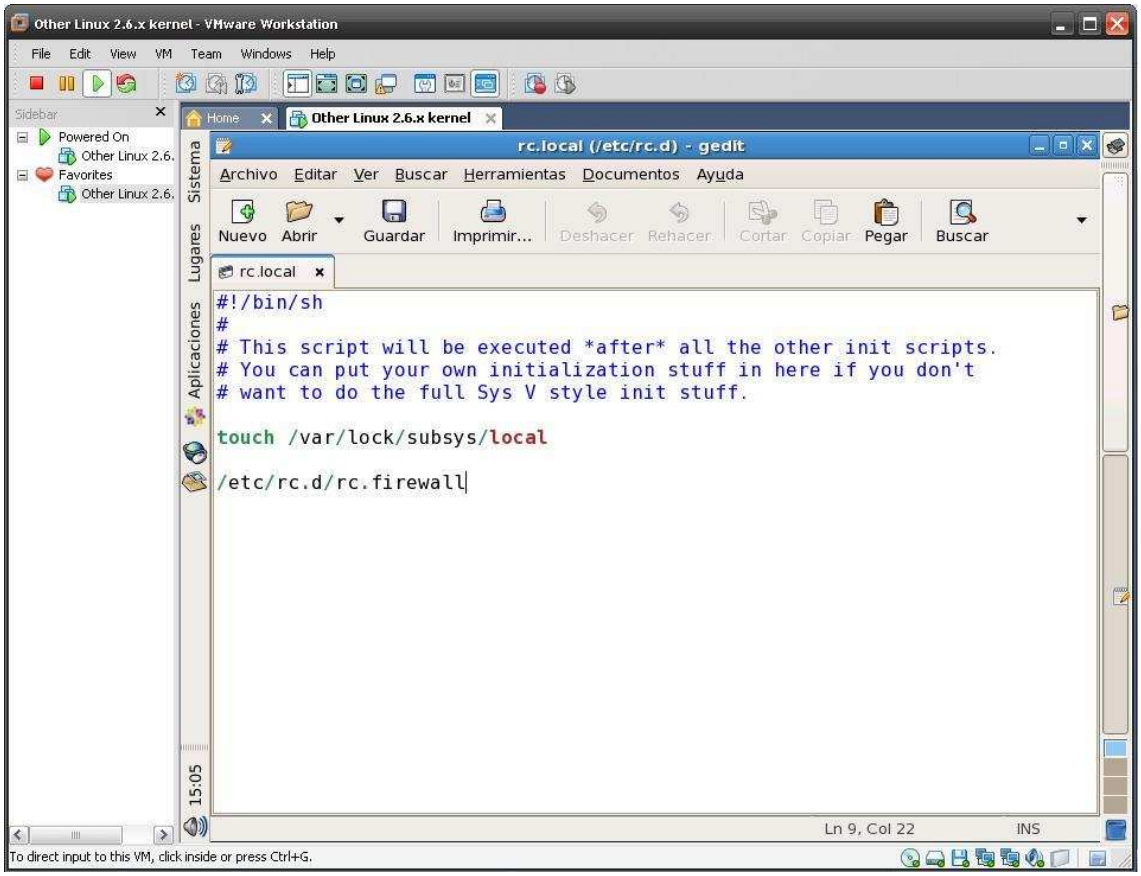

Figura 19. Modificación archivo rc local.

Por último desde la consola terminal se aplican las reglas sin necesidad de reiniciar la maquina ejecutando la siguiente línea:

#./rc.firewall.

Con este paso finalizamos la implementación del firewall ejecutándose de forma permanente sin ningún inconveniente en el sistema operativo Centos con el script creado, solo faltaría analizar que el firewall este cumpliendo con las reglas creadas; este tema será abarcado en el siguiente capítulo con los reportes de Iptables y análisis de vulnerabilidades para el escaneo de los posibles puertos que pueda tener abierto el firewall.

Para completar esta implementación fue necesario instalar servicios en los equipos hosts para simular posibles servidores y poder analizar el funcionamiento del Script Iptables creado anteriormente, esto con el fin que el lector o administrador de seguridad de redes pueda crear reglas según el criterio

requerido y pueda entender mejor la sintaxis de Iptables.

5.7.6 Configuración de los Hosts.

La configuración de los hosts se basa en instalar servicios en cada unos de los PCs, funcionando así como Servidores. En los cuatros PCs utilizado para la implementación se le instalará la herramienta Apache para simular un servidor Web, y la herramienta Easy FTP Server para la transferencia de archivo como es el protocolo de Transferencia FTP.

Las herramientas utilizadas para los hosts son:
Easy FTP Server
Appserv win32-2.5.10

En los PC2 y PC3 se instalará la herramienta Appserv para simulación de un servidor Web configurando por el puerto 80 como lo muestra la figura 20.

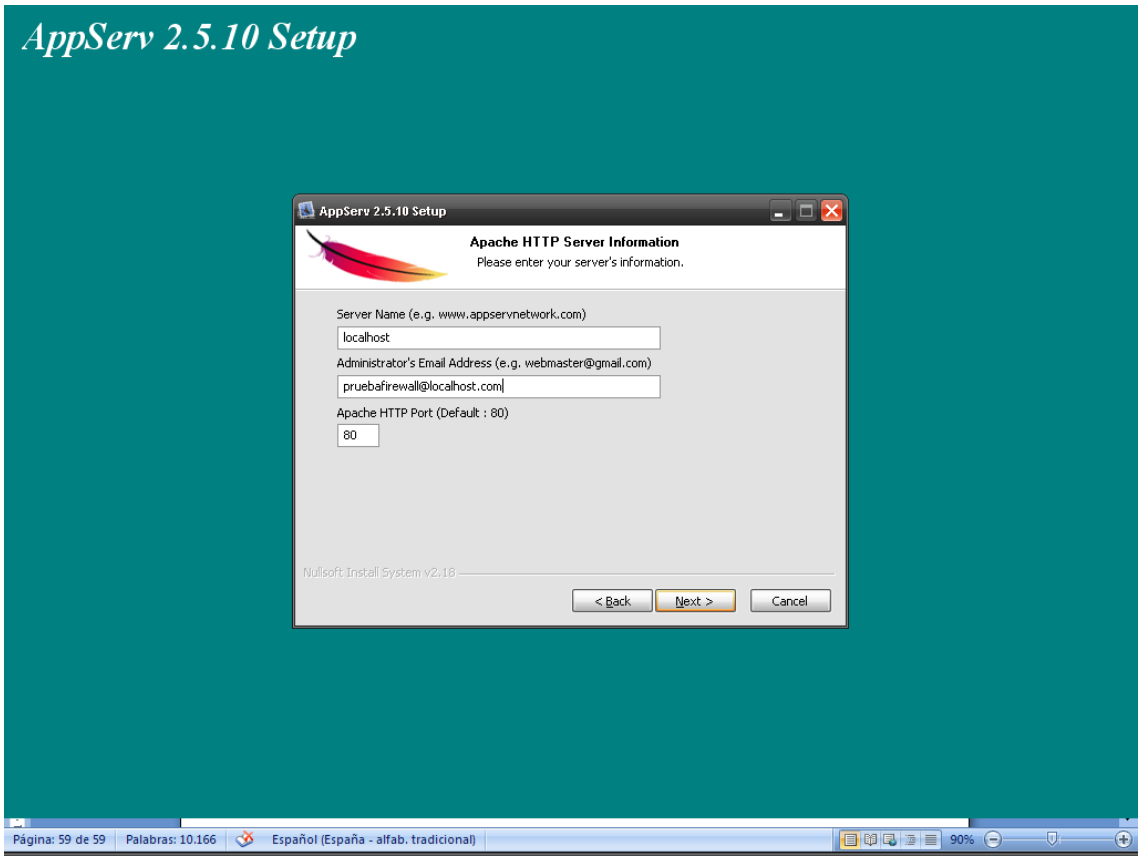

Figura 20. Configuración Apache

Los PC1 y PC4 servirán de servidores FTP y la herramienta a utilizar Easy FTP Server configurada por el puerto 21.

Lo primero sería crear un usuario, luego seleccionar una carpeta a compartir para que los posibles usuarios FTP puedan descargar información e iniciar el servicio tal como nos muestra la figura 21.

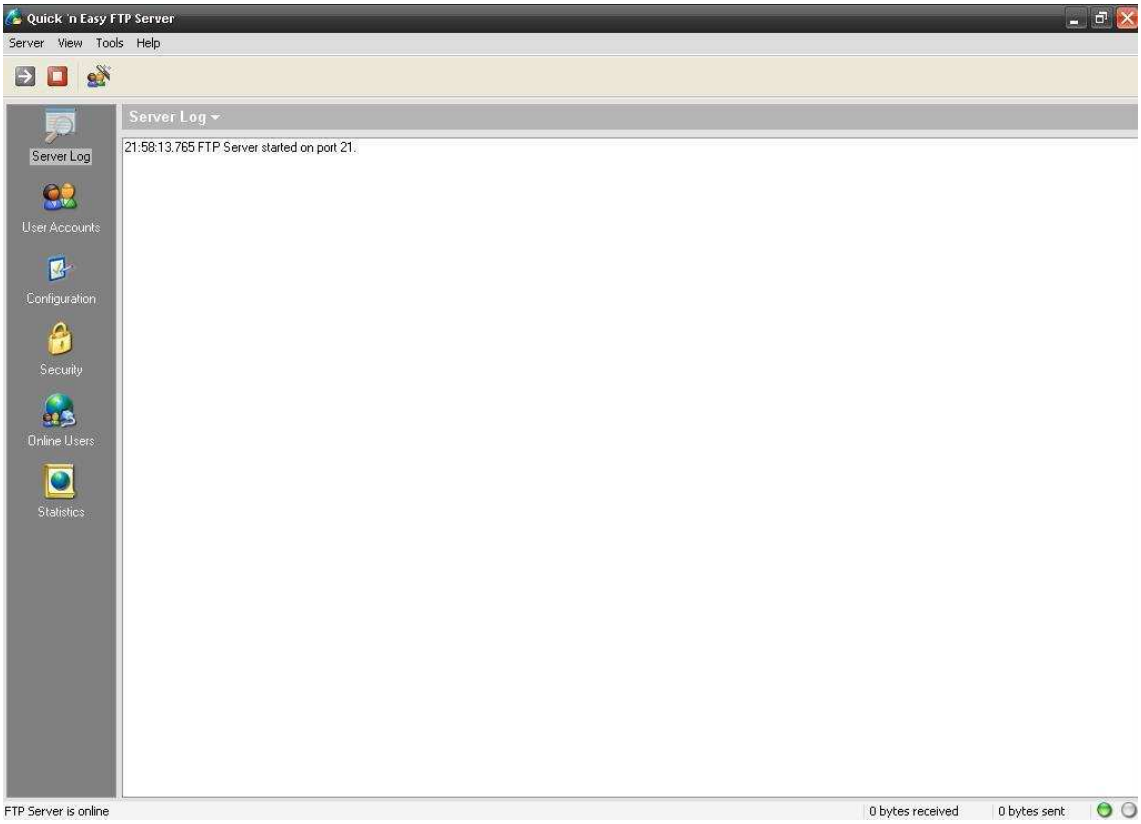

Figura 21. Configuración servidor FTP

Instalar los servicios anteriores nos permite verificar la eficacia del Muro cortafuego en función de cumplir las reglas creada en el Script Iptables, en el siguiente capítulo se hará las respectivas pruebas de cada uno de estos servicios.

6. ANÁLISIS FUNCIONAL DEL MURO CORTAFUEGO

6.1 Prueba de las reglas del firewall

Los puertos de red permiten la comunicación entre los equipos, clientes y los servidores. Debido al nivel de riesgo dentro de la red en una empresa, ya sea de carácter educativo o centro de cómputo es indispensable reforzar medidas restrictivas para evitar posibles ataques; lo más recomendable es cerrar aquellos puertos de red que no sean utilizados o sean innecesarios mediante servidores de seguridad dedicados, basados en host o filtros de seguridad de protocolo Internet.

Una empresa u organización que necesite proteger una red lo puede hacer de dos maneras: la primera consiste en denegar todo y solo abrir los puertos que utilicen o la segunda es aceptar todo y cerrar los puertos innecesarios.

En esta implementación del firewall se utilizó la política de denegar todo y solo abrir los puertos a utilizar; para que un usuario pueda navegar desde una red local hacia la red externa. Un administrador de seguridad en redes puede utilizar la siguiente regla:

 # Aceptamos que naveguen por el protocolo HTTP puertos 80
iptables -t nat -A POSTROUTING -o $TARJ_EXT -p tcp -m tcp --dport 80 -j MASQUERADE

iptables: iptables es un aplicativo del espacio de usuario que le permite a un administrador de sistema configurar las tablas, cadenas y reglas.
-t tabla: Hace que el comando se aplique a la tabla especificada. Si esta opción se omite, el comando se aplica a la tabla filter por defecto.
Nat: Esta tabla es la responsable de configurar las reglas de reescritura de direcciones o de puertos de los paquetes.
A:<comando> hace referencia a la acción que va llevar a cabo, en este caso sería agregar una regla.

POSTROUTING: la cadena modifica los paquetes antes de enviarse a través de una interfaz de red traduciendo sus direcciones de origen.

O: <parámetros> configura los adaptadores de red de salida para la regla creada usándose con la cadena POSTROUTING de la tabla nat.

$TARJ_EXT: hace referencia a la tarjeta eth0.

P: específica el protocolo al que se aplica la regla, en este caso sería TCP.

-m: Especifica un módulo que debe ser usado.

dport: configura el puerto de destino del tráfico.

j: Especifica el objetivo para una regla.

MASQUERADE: enmascarar las IPs de la red local con otra diferente.

En la anterior regla nos permite convertir las direcciones privadas de la red local para que pueda salir hacia exterior y pueda navegar por el protocolo HTTP.

En el host PC4 vemos que puede navegar por el puerto 80 hacia el PC2 donde se tiene instalado el Apache. *Ver anexo 1* en el cual funciona como un servidor web, en la figura 22 nos mostrará con detalle lo realizado.

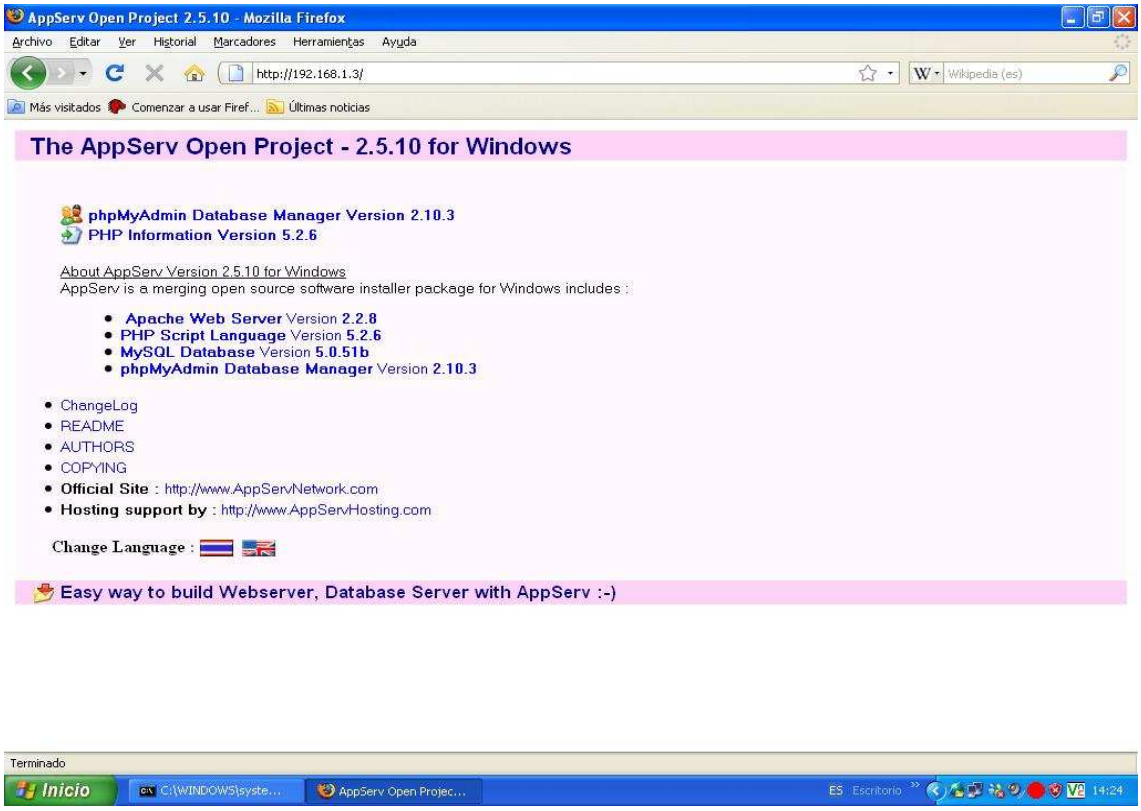

Figura 22.navegacion puerto 80 desde pc4

A igual forma se hizo la respectiva prueba desde PC3 al PC2.

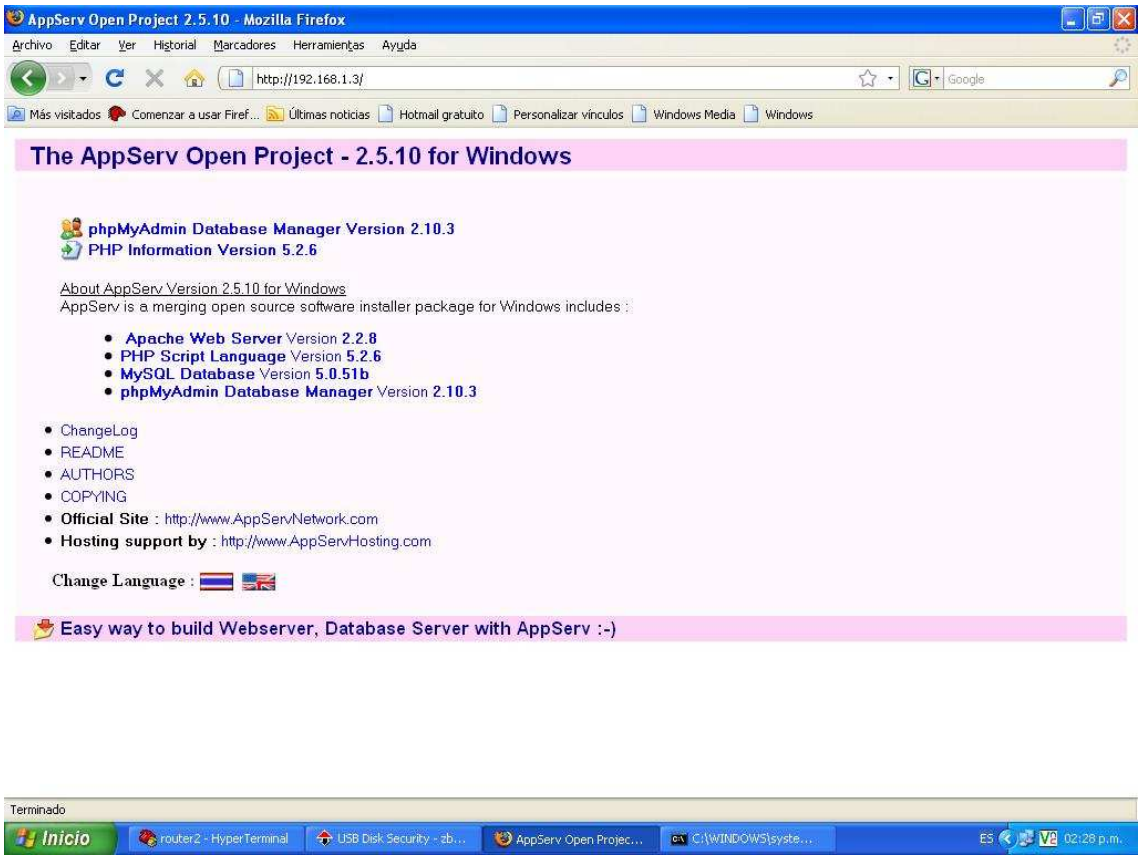

Figura 23.navegacion puerto 80 desde pc3

Con estas pruebas verificamos que se cumple el objetivo de la regla para la navegación por el puerto 80.

Para que un usuario pueda acceder a un servidor de transferencia de archivo desde una red local hacia la red externa, un administrador de seguridad de red puede utilizar la siguiente regla:

 # Aceptamos que naveguen por el protocolo FTP puertos 21

iptables -t nat -A POSTROUTING -s 192.168.4.0/24 -o $TARJ_EXT -p tcp -m tcp --dport 21 -j MASQUERADE

iptables -t nat -A POSTROUTING -s 192.168.4.0/24 -o $TARJ_EXT -p tcp -m tcp --dport 1024 -j MASQUERADE

iptables: iptables es un aplicativo del espacio de usuario que le permite a un

administrador de sistema configurar las tablas, cadenas y reglas.

-t tabla: Hace que el comando se aplique a la tabla especificada. Si esta opción se omite, el comando se aplica a la tabla filter por defecto.

Nat: Esta tabla es la responsable de configurar las reglas de reescritura de direcciones o de puertos de los paquetes.

A:<comando> hace referencia a la acción que va llevar a cabo, en este caso sería agregar una regla.

POSTROUTING: la cadena modifica los paquetes antes de enviarse a través de una interfaz de red traduciendo sus direcciones de origen.

-s: especifica la dirección origen del paquete.

O: <parámetros> configura los adaptadores de red de salida para la regla creada usándose con la cadena POSTROUTING de la tabla nat.

$TARJ_EXT: hace referencia a la tarjeta eth0.

P: específica el protocolo al que se aplica la regla, en este caso sería TCP.

-m: Especifica un módulo que debe ser usado.

dport: configura el puerto de destino del tráfico.

j: Especifica el objetivo para una regla.

MASQUERADE: enmascarar las IPs de la red local con otra diferente.

El servidor siempre crea el canal de datos en su puerto 21, mientras que en el lado del cliente el canal de datos se asocia a un puerto aleatorio mayor que el 1024 para poder hacer la transferencia desde el servidor al cliente.

Desde el PC4 se verifico que podría acceder a un servidor FTP instalado en el host 1 por el puerto 21 como lo muestra la figura 24.

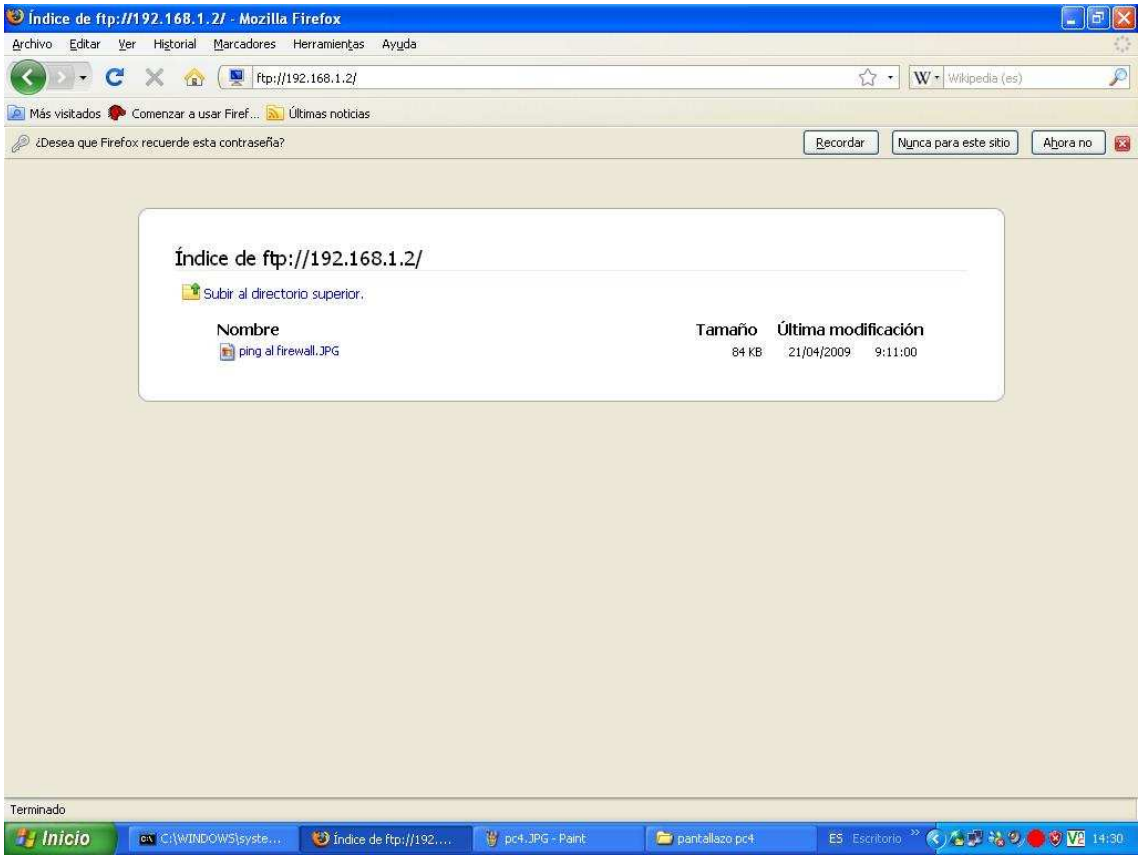

Figura 24. Acceso al servidor FTP desde PC4

Las reglas mencionadas anteriormente permitirán el acceso desde la red local a la red externa por los puertos 80, 21; por lo cual cualquier host que se encuentre dentro de la red 192.168.4.0/24 podrá acceder al exterior por dichos puertos.

Cuando un administrador de seguridad en redes quiera configurar el Firewall para enviar paquetes ICMP con respuestas desde los host remotos para verificar si hay comunicación en la red; se puede utilizar la siguiente regla:

#permite hacer ping a host de la red local pero no viceversa.
iptables -A OUTPUT -p icmp --icmp-type echo-request -j ACCEPT

iptables: iptables es un aplicativo del espacio de usuario que le permite a un administrador de sistema configurar las tablas, cadenas y reglas.
-t tabla: Hace que el comando se aplique a la tabla especificada. Si esta opción se omite, el comando se aplica a la tabla filter por defecto.

A:<comando> hace referencia a la acción que va llevar a cabo, en este caso sería agregar una regla.

OUTPUT: analiza los paquetes que son enviados por la misma interfaz de red.

p: específica el protocolo al que se aplica la regla, en este caso sería ICMP.

icmp-type: Especifica el tipo de ICMP.

j: Especifica el objetivo para una regla.

Con esta regla comprobamos que el firewall puede hacer ping a los host que se encuentre dentro de la subred 192.168.4.0/24 en este caso sería la red local como lo detalla el siguiente grafico.

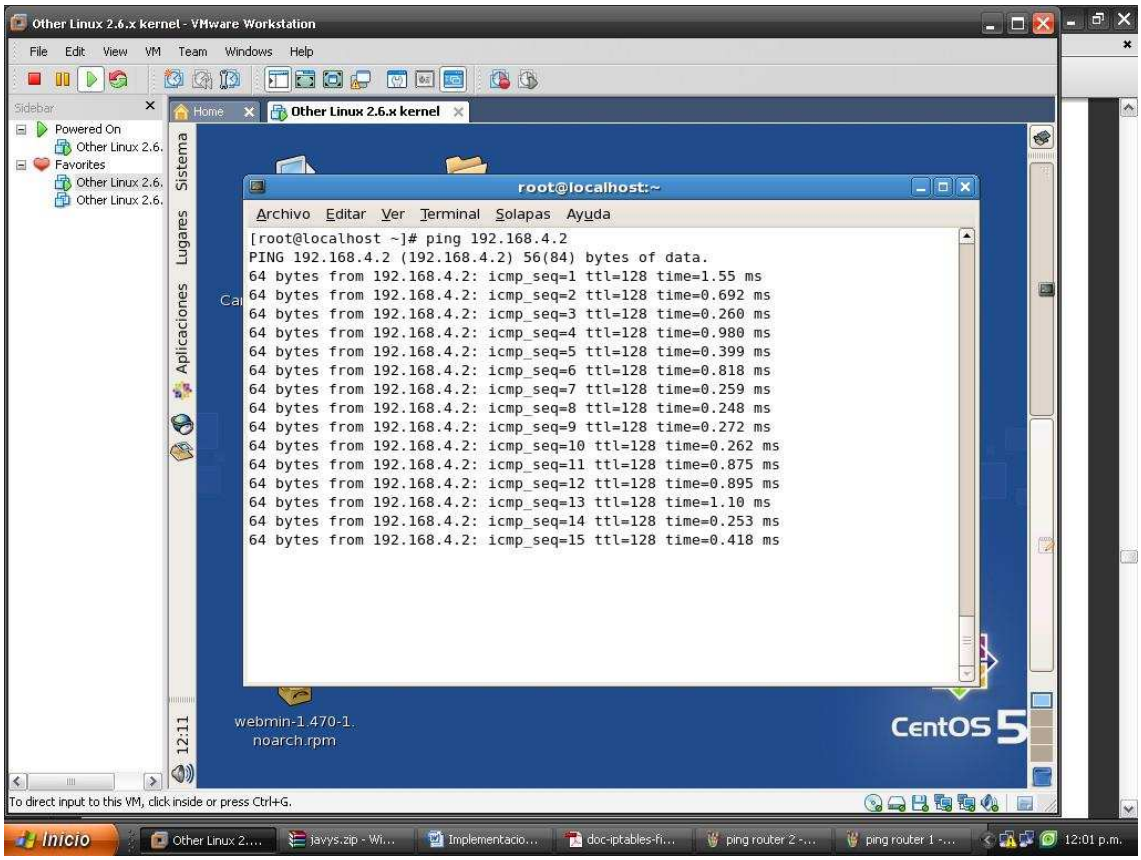

Figura 25. Ping a host locales desde Firewall.

Ahora en el caso que el host quiera hacer ping al firewall este no será permitido ya que el Firewall puede sufrir posibles ataques como ping de la muerte por parte de un usuario interno.

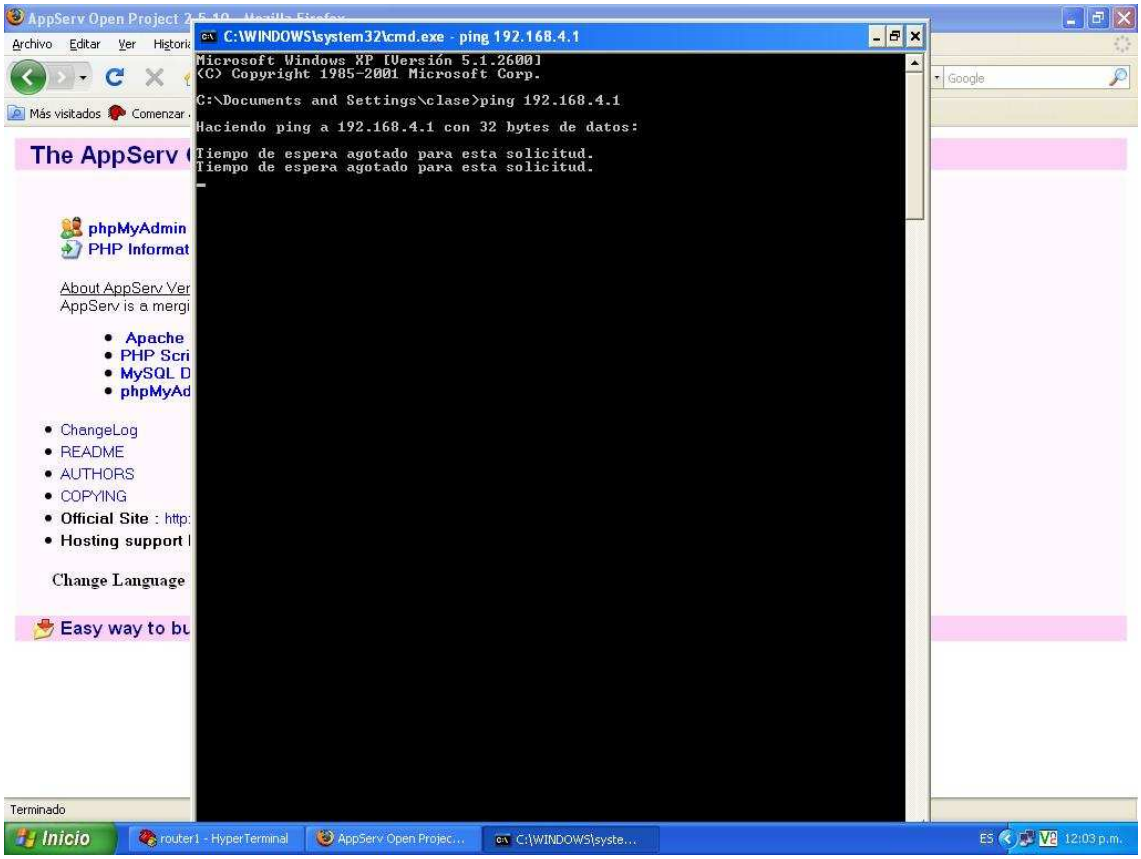

Figura 26. Ping desde PC3 al Firewall.

Regla para enviar paquetes ICMP desde el Firewall:

#Permite hacer ping a la red externa pero no viceversa.

iptables -A INPUT -p icmp --icmp-type echo-reply -j ACCEPT

iptables: iptables es un aplicativo del espacio de usuario que le permite a un administrador de sistema configurar las tablas, cadenas y reglas.

-t tabla: Hace que el comando se aplique a la tabla especificada. Si esta opción se omite, el comando se aplica a la tabla filter por defecto.

A:<comando> hace referencia a la acción que va llevar a cabo, en este caso sería agregar una regla.

INPUT: Analiza los paquetes que son enviados por la misma interfaz de red.

p: específica el protocolo al que se aplica la regla, en este caso sería ICMP.

icmp-type: Especifica el tipo de ICMP.

j: Especifica el objetivo para una regla.

Esta regla funciona igual a la anterior pero en la red externa, en donde el firewall puede hacer ping a los Routers y a los host y no viceversa.

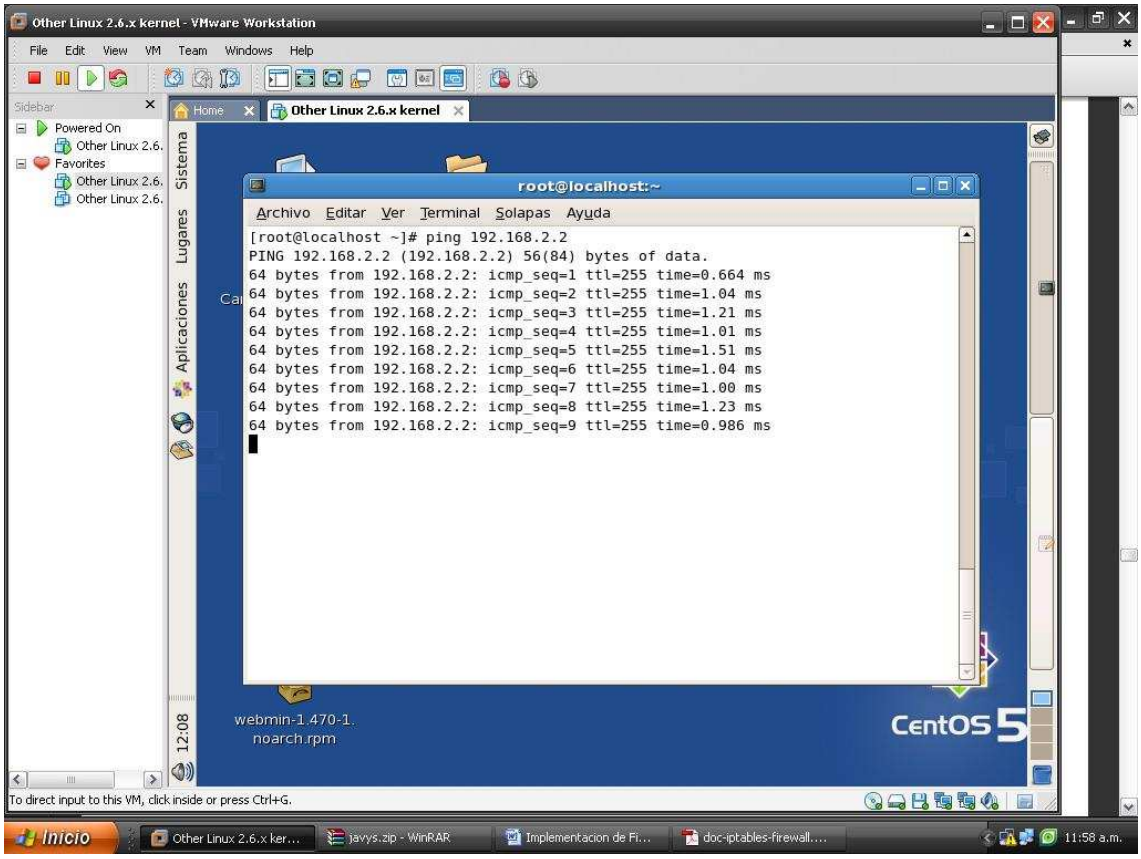

Figura 27. Ping al Router 2 desde servidor Firewall.

En el caso contrario el ping no será permitido hacia el Firewall.

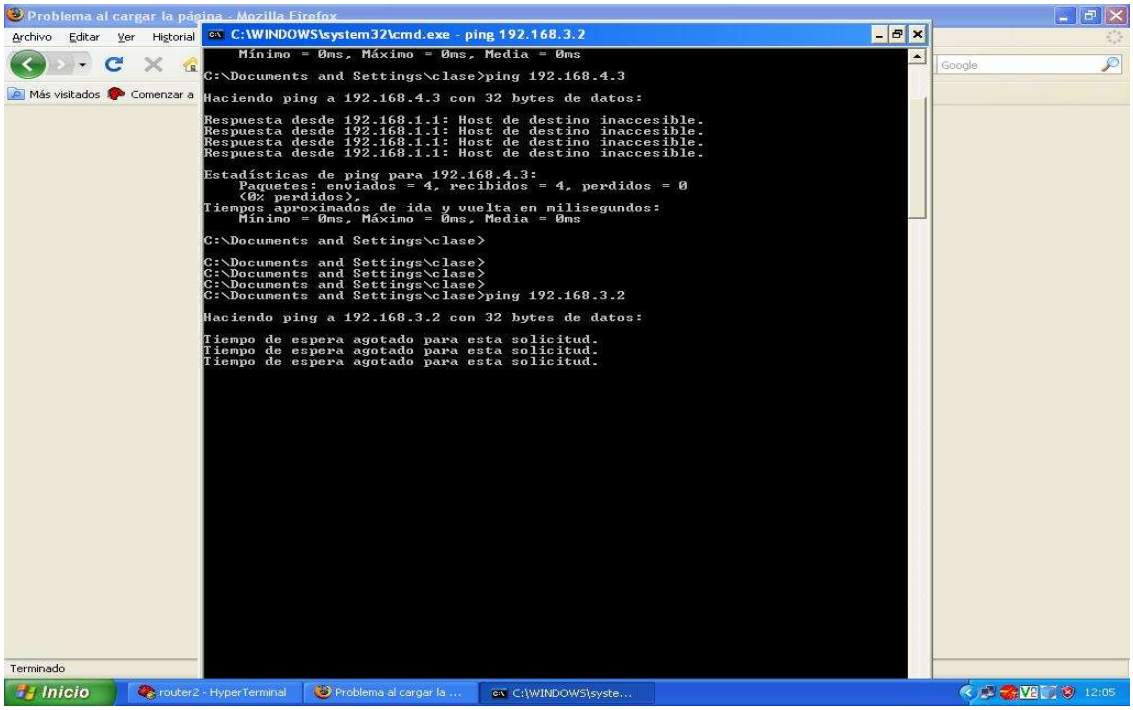

Figura 28. Ping desde PC2 a firewall

La regla de salida de paquetes de protocolo ICMP desde firewall nos permite verificar si existe comunicación con cada unos de los dispositivos de cada red y así ayudaría al administrador de red solucionar posibles problemas técnicos con los usuarios.

6.2 Análisis de las conexiones que entren y salen.

Para el análisis de conexiones entrante y saliente del firewall se utilizo una herramienta llamada IPTraf para los enlaces del tráfico de datos con conexiones entre Ips.

IPTraf es una consola basada en estadísticas de utilidad para Linux. Reúne una variedad de figuras como la conexión de paquetes de TCP, con una interfaz de estadísticas e indicadores de actividad de trafico TCP / UDP y cuenta con una utilidad llamada la estación de la LAN de paquetes donde muestra el total de bytes utilizado en cada interface[13].

[13] IPTRAF, IP Network Monitoring Software [En línea] http://iptraf.seul.org/ [citado en 18 de abril]

IPTraf también nos permite observar si la conexiones se establecen o no; muestra en tiempo real el tráfico que atraviesa nuestra máquina origen/destino de ips y puertos, tráfico total según la interfaz de red, y tiene una opción llamada filtros para captar solo aquello que nos interesa en el caso que haya muchas conexiones.

En la práctica el IPtraf se configuro en el servidor muro cortafuego para observar las conexiones y el tráfico por las interfaces eth0 y eth1, durante la verificación de la regla de acceso por el puerto 80 se permitió simultáneamente tomar información de todas las interfaces de red del servidor cortafuego con la opción IP traffic monitor de IPTraf. A continuación la figura 25 nos muestra la prueba realizada.

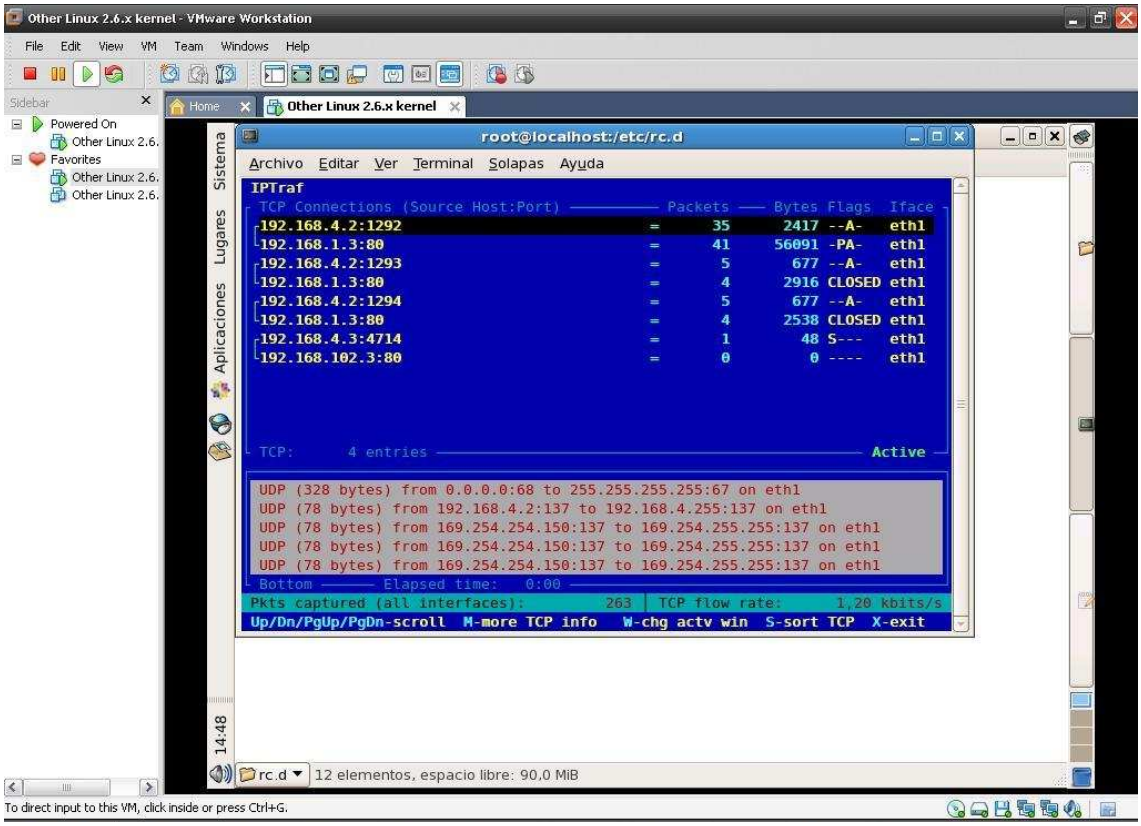

Figura 29. Información de las interfaces

Los datos mostrados durante la petición de los accesos al puerto 80 específica que la IP 192.168.4.2 del host 3 accede a la IP 192.168.1.3:80 correspondiente al host 2 en la interface eth1 estableciendo así la conexión:

A: es un reconocimiento (ACK) del paquete recibido.

P: son los pedidos de prioridad para poder ser trasladados al principio de la cola.

CLOSED: El paquete de finalización ha sido reconocido por el host 2.

En la regla de acceso por el puerto 21 correspondiente a FTP se tomaron también los datos de la conexión establecida entre la IP 192.168.4.3 del host 4 a la IP 192.168.1.2 correspondiente al host 1 donde tiene el servicio de transferencia de archivo, como lo muestra el siguiente grafico.

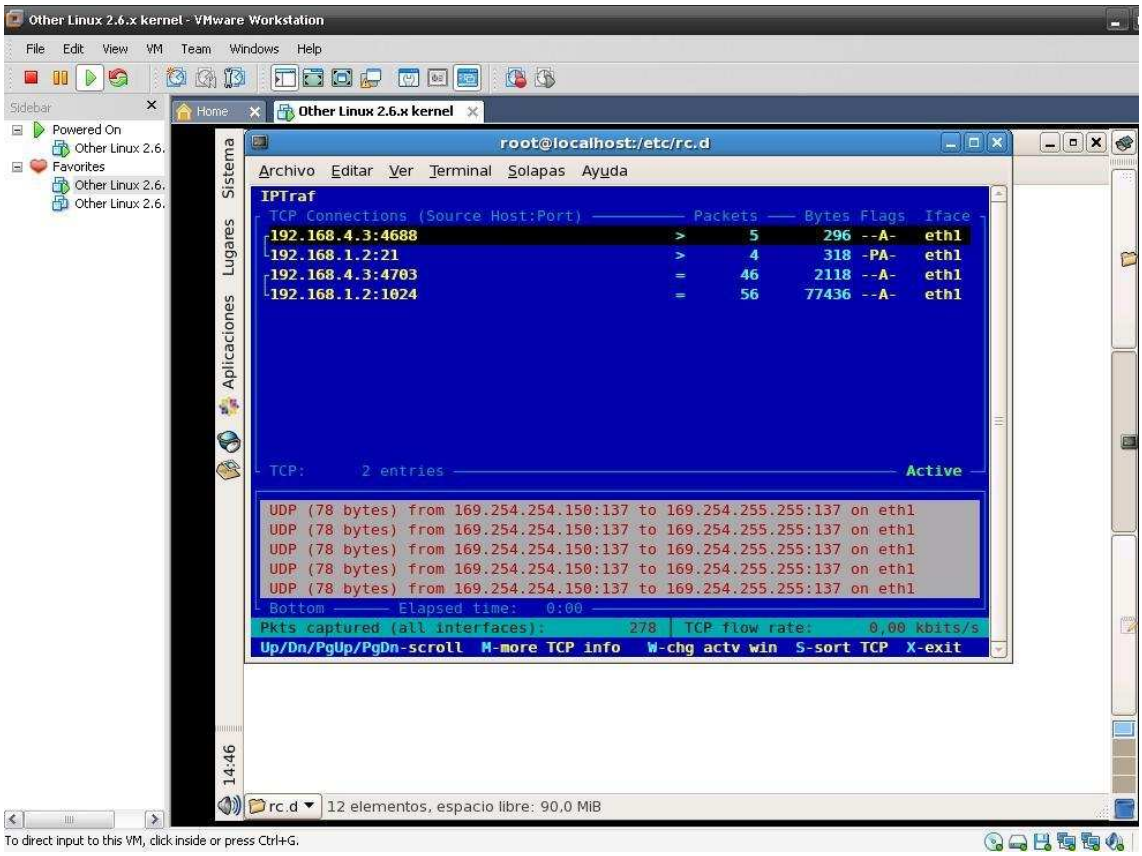

Figura 30. Información interface eth1 del host 4

La opción ALL interfaces del menú IP traffic monitor permite mostrar todas la conexiones efectuadas por todas la interfaces, en este caso sería eth0 y eth1 ya que esas están implementada en el servidor Firewall; la información mostrada es contadores de paquetes, contadores de bytes y estado de las opciones (flags) donde se explicaron anteriormente.

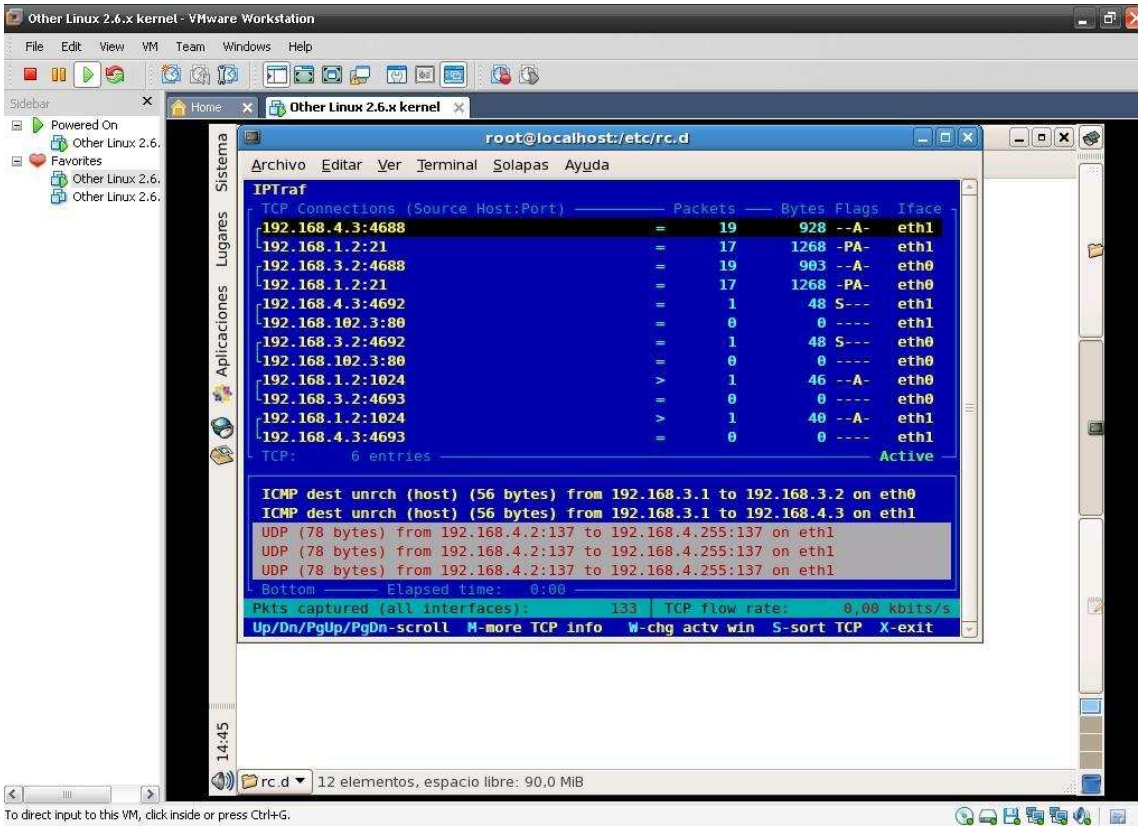

Figura 31. Conexiones establecidas en todas las interfaces

6.3 Depuración de las reglas del Firewall

Cuando se implementa un Firewall en el cual está instalado, activado y por alguna razón un usuario se encuentra bloqueado es posible hacer una depuración para verificar que las reglas funcionen correctamente.

En Iptables existen comandos para listar las reglas que han sido aplicadas desde la consola de comando o de un script y la sintaxis es las siguientes:

iptables -vn -L

Para cada cadena existen también comandos para verificar dichas reglas como son:

- INPUT

  > iptables -n -L INPUT

  Con la ejecución este comando en el firewall implementado mostraría las siguientes reglas aplicadas para esta cadena como indica la figura 32.

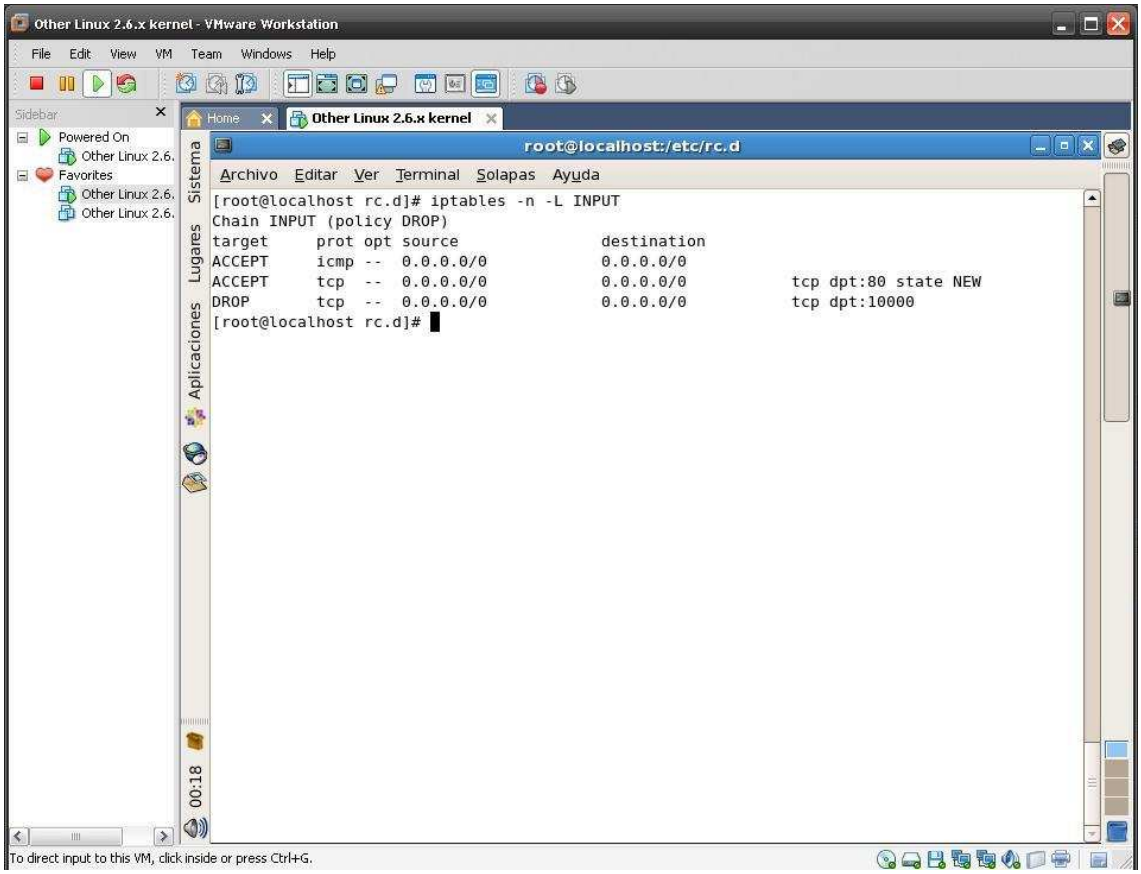

Figura 32 Reglas input

Línea 1: Identifica el listado como procedente de la cadena input, la directiva predeterminada de la cadena input es DENY.

Línea 2: Contiene los siguientes encabezados de columna:

- ✓ **Target**: Se refiere a la disposición del destino de un paquete que coincide con la regla ACCEPT, DENY o REJECT.
- ✓ **Prot**: Es la abreviatura de protocolo, que puede ser all, tcp, udp o icmp.
- ✓ **Opt:** Es la abreviatura de opciones de paquete, o bits de indicador.
- ✓ **Source:** Es la dirección origen del paquete.
- ✓ **Destination:** Es la dirección destino del paquete.
- ✓ **Ports:** Lista tanto el puerto origen como el destino, el tipo de mensaje ICMP, o n/a si no se han especificado puertos en la regla[14].

Línea 3: Acepta los paquetes procedentes de servidores web remotos.

Línea 4: Deniega los paquetes procedentes al puerto 10000 que es referente Webmin.

[14] ZIEGLER, Robert**.** Firewalls Linux. México: Prentice Hall 2001. P 237

- OUTPUT: son las reglas de de salida por una interfaz.

  iptables -L OUTPUT

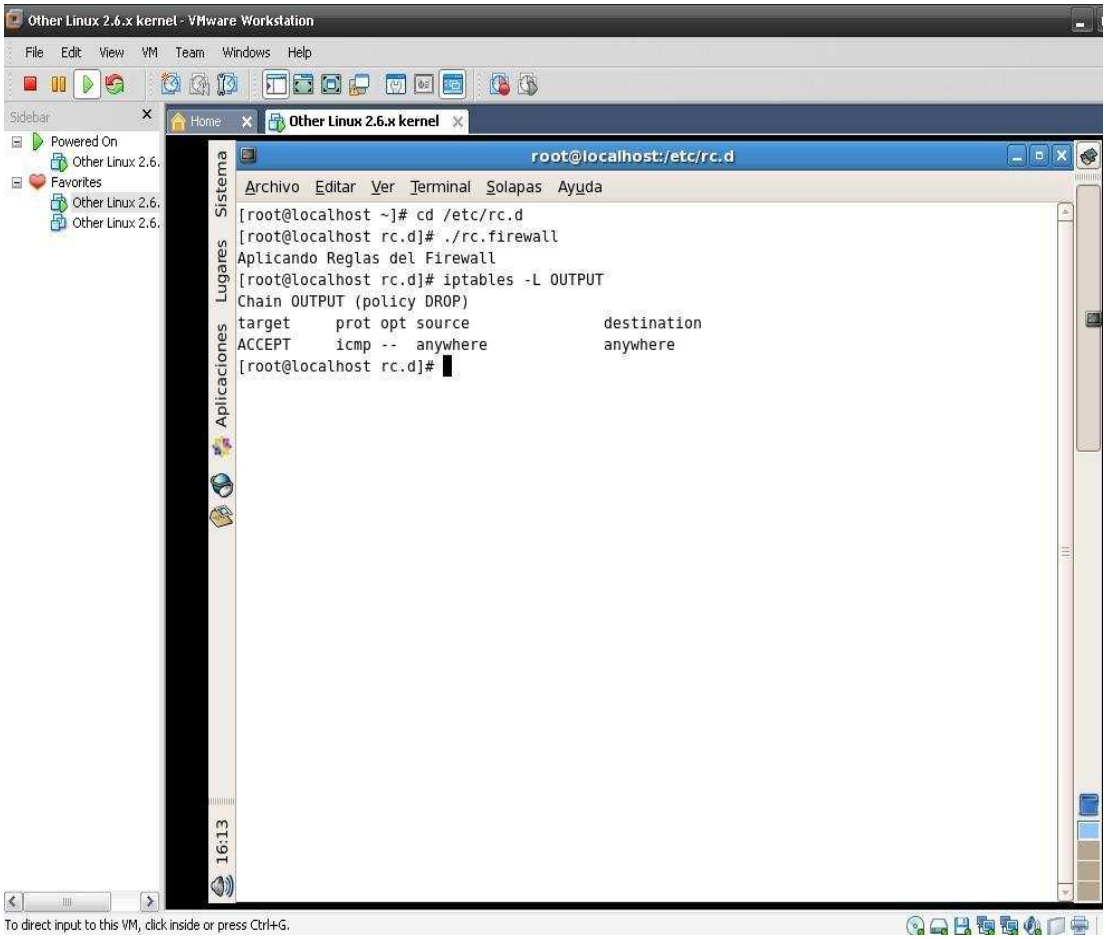

Figura 33 Reglas OUPUT

Se permite que los mensajes de flujo ICMP de tipo se dirijan desde cualquier parte interna de la red hacia el Firewall.

- Tabla nat: el siguiente comando permite listar las reglas que aplica a la tabla nat.

  iptables -t nat -vn -L

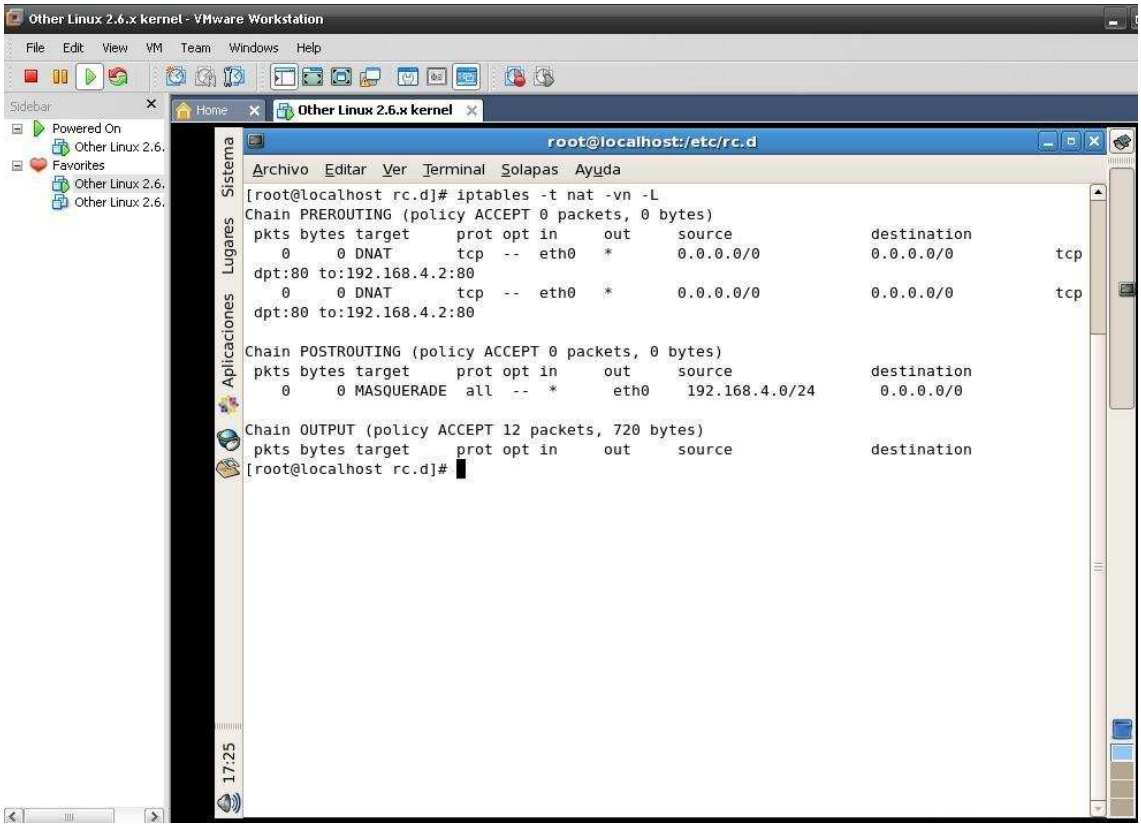

Figura 34 Regla tabla nat

- ✓ **Pkts:** es el número de paquetes que coincide con la regla.
- ✓ **Bytes:** es el número de bytes que contiene un paquete que coincide con la regla.
- ✓ **Target**: Se refiere a la disposición del destino de un paquete que coincide con la regla ACCEPT, DROP, LOG o REJECT.
- ✓ **Prot**: Es la abreviatura de protocolo, que puede ser all, tcp, udp o icmp.
- ✓ **Opt:** Es la abreviatura de opciones de paquete, o bits de indicador.
- ✓ **In:** hace referencia a la interfaz de red entrante donde puede ser eth0 o eth1 a los que se aplica la regla.
- ✓ **Out.:** hace referencia a la interfaz de red saliente donde puede ser eth0 o eth1 a los que se aplica la regla.
- ✓ **Source:** Es la dirección origen del paquete.
- ✓ **Destination:** Es la dirección destino del paquete.

6.4 Análisis de Vulnerabilidades

Cuando un hacker planea realizar un ataque, debe plantearse una serie de pasos a seguir antes de realizar cualquier ofensiva. Existen muchas formas de entrar en determinados lugares con acceso restringido, cuyo objetivo principal puede ser la conquista de una maquina remota o simplemente la subida de privilegios de un usuario en un servidor o de un ordenador local[15].

Con solo saber la IP que tiene un servidor y las estaciones de trabajo que tiene conectados a la red, que servicios están iniciados y en que puertos están trabajando y las aplicaciones que utiliza.

Durante la implementación del firewall se hizo un análisis con la herramienta GFiLanguard 8.0[16] la cual permitió analizar la red y puertos para detectar, evaluar y rectificar vulnerabilidades de seguridad con el mínimo esfuerzo administrativo.
Esta herramienta se instalo en un host de la red externa en donde se ingresó la IP del Servidor firewall para buscar vulnerabilidades y arrogo los siguientes datos:

[15] PICOUTO Fernando, LORENTE Iñaki. Hacking y Seguridad en Internet. México: Alfaomega Grupo Editor, S.A, 2008. P 90
[16] GFI.GFiLANguard: Seguridad de red [En línea] http://www.gfi.nl/es/lannetscan/ [Citado 22 de Abril 2009]

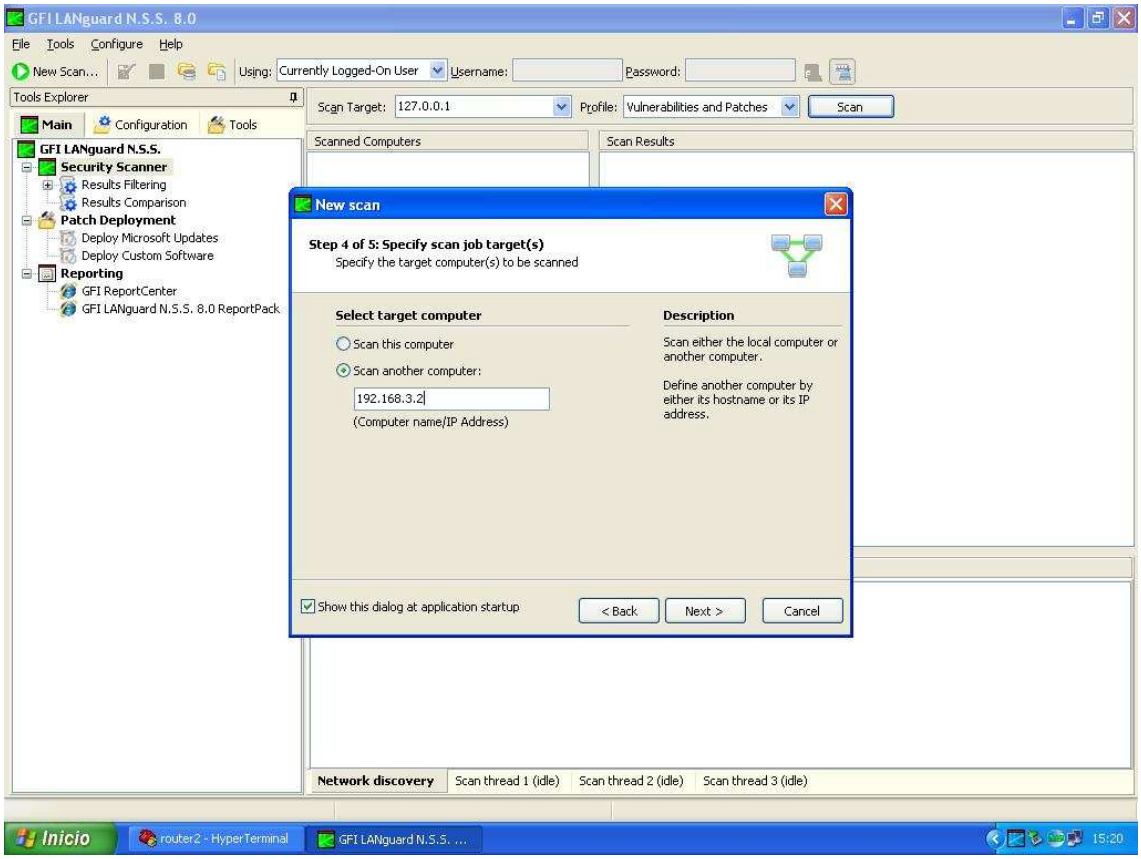

Figura 35. GFI ingreso de la IP Firewall

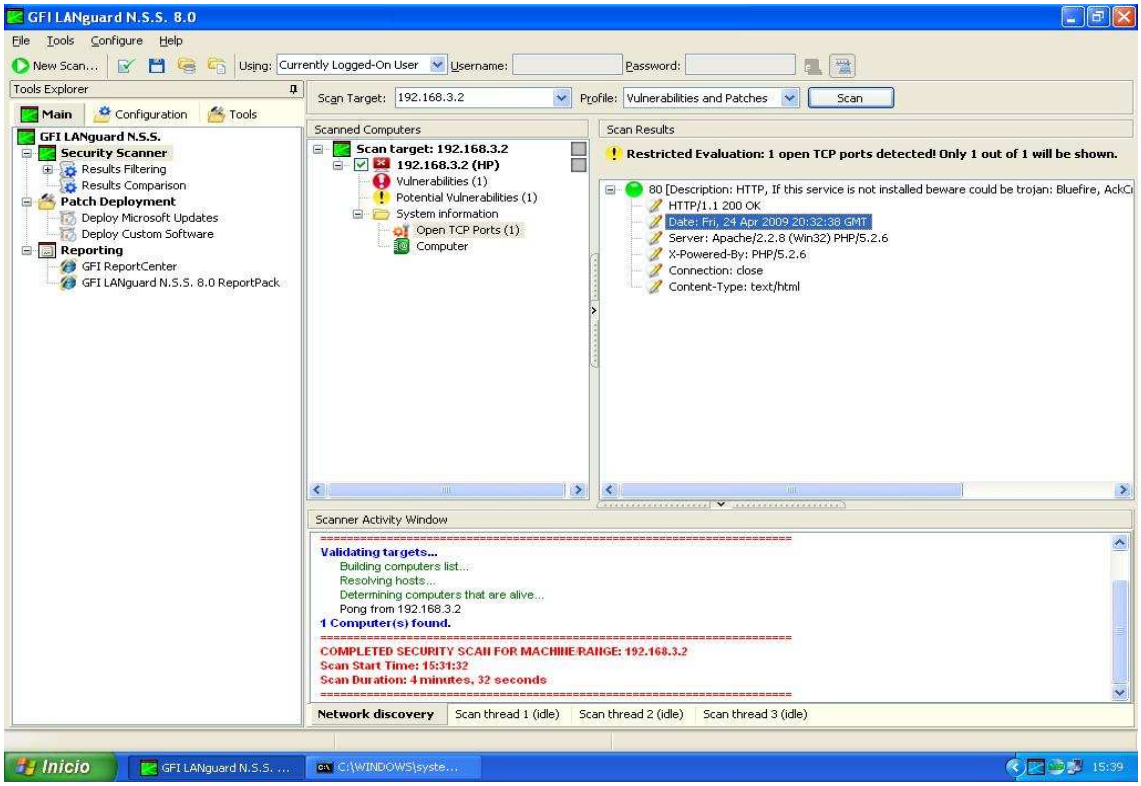

Figura 36. Datos del servidor

De acuerdo a los datos presentados en la figura anterior podemos afirmar que dentro la red local protegida por el firewall hay un host que funciona como servidor web que relaciona las reglas creadas en el firewall para permitir el acceso al puerto 80 correspondiente a ese host.

7. CONCLUSIONES

Durante el proceso de desarrollo de esta monografía y basados de acuerdo a la documentación tomada como referencia en la implementación del servidor firewall en Linux, nos permitió profundizar conocimientos y comprobar físicamente las teorías planteadas por los diferentes autores citados durante este trabajo de investigación.

Como resultado del proceso de implementación logramos reafirmar el objetivo de conocer los firewalls en su entorno aplicativo, en esta investigación nos basamos principalmente en los firewalls de filtrado de paquetes a nivel de la capa de Red del modelo OSI donde los filtros que se usan son para examinar las direcciones IP de origen y destino; el numero de puerto que esté utilizando el protocolo para llevar a cabo la comunicación.

En el diseño de la arquitectura firewall se basó en host de doble acceso para la protección de una red local en donde se simuló una red externa (internet) y a partir de ahí se definieron las políticas de seguridad para lograr protección, control del tráfico de datos, mayor seguridad y confiabilidad en el intercambio de la información.

Dentro de los procesos de implementación observamos la importancia de la herramienta Iptables como medio de protección y seguridad en el acceso a las redes en la circulación de información entre ellas; igualmente se pudo comprobar que existen reglas utilizadas por algunas empresas para su seguridad que no son eficientes de acuerdo al nivel de protección exigido por sus políticas.

Los firewalls son de gran utilidad siempre y cuando se definan claramente las políticas de acceso y se cumplan eficazmente; estos por sí solos no son la solución a la implementación de seguridad en una red, ya que la seguridad no es un concepto estático, sino dinámico por los continuo ataques que puede sufrir una red y se necesita destreza por parte del administrador de redes, donde se

requiere de una vigilancia continua, con el uso de herramientas que nos faciliten ésta tarea para garantizar el buen funcionamiento del firewall.

Cabe descartar que la implementación de esta investigación del servidor Firewall se llevo acabo en una maquina virtual con el sistema operativo Linux distribución Centos, esto debido a la gran demanda existente en la virtualizacion de servidores que se estan realizando en las empresas, como una medida que permite una reducción de costos, una menor inversión en los Hardware, y una mayor optimización de estas herramientas utilizadas a fin de que se tenga una estrategia de innovación del proceso de protección de la información en las organizaciones de hoy frente a la inestabilidad económica global.

8. RECOMENDACIONES

En el desarrollo de esta investigación se debe tener claro los conceptos y características de los firewalls a la hora de ser implementando utilizando el criterio de evaluación por el administrador de seguridad de redes en una organización, definiendo el tipo de firewall que debe ejecutar, luego del diseño de la topología de red y la tabla de enrutamiento para el servidor Firewall se permite tener claro los componentes que se interconectarán.
A partir de esto, esta investigación ha sido redactada de manera que el lector pueda profundizar los pasos necesarios para llevar a cabo una implementación de Firewall en Linux; en cada capítulo han sido explicados de forma detallada para su mayor profundización.

De acuerdo a lo planteado anteriormente este trabajo de investigación está dirigido a todas las empresas, estudiantes, centros de cómputos, universidades, administradores de seguridad en redes que deseen profundizar sobre la implementación de firewalls en Linux mostrando la información de forma simple y organizada para el fácil entendimiento.

Como recomendaciones finales para tener presente al leer esta investigación se podrá enfatizar sobres los siguientes ítems en los cuales ayudarán en la implementación de servidores firewalls:

- ✓ Se puede tomar como base esta investigación para implementar Arquitecturas de red con tres interfaces para la ubicación de posibles servidores en una organización o empresa como son las zonas desmilitarizadas (DMZ).
- ✓ Otro aspecto que puede ser complemento de esta investigación son los Firewalls a nivel de aplicación llamados Proxy en donde estos provee aplicaciones especificas de acuerdo con las políticas de seguridad.
- ✓ Se puede mejorar los scripts de iptables con las direcciones MAC de

cada usuario de la red en el caso que exista servidores DHP para la asignación de IPs.

- ✓ Es importantes asistir a seminarios, congresos entre otros para aumentar los conocimientos en el área de la seguridad en redes y estar actualizado a las nuevas vulnerabilidades.

9. GLOSARIO

A

ACK: mensaje que se envía para confirmar que un mensaje o un conjunto de mensajes han llegado.

B

BSD: Distribución estándar de Berkeley. Término utilizado para describir cualquiera de una serie de sistemas operativos de tipo UNIX basados en el sistema operativo BSD de la UC Berkeley.

C

Cracker: Es cualquier persona que viola la seguridad de un sistema informático de forma similar a como lo haría un hacker, sólo que a diferencia de este último, el cracker realiza la intrusión con fines de beneficio personal o para hacer daño.

D

*DDos***:** Es un ataque de Denegación de servicios (DoS) realizado al mismo tiempo desde varios ordenadores, contra un servidor.

DNS: Domain Name System. Son nombres de dominio para simbolizar los números de las direcciones IP para la salida hacia Internet

*DMZ: (Z*ona desmilitarizada) es una red local que se ubica entre la red

interna de una organización y una red externa para ubicar los servidores DNS, WWW, correo entre otros.

E

Enrutador: Se denomina así al dispositivo capaz de dirigir la información, dividida en paquetes, por el camino más idóneo, examinando la dirección y el destino y utilizando mapas de red.

Espía: es aquel que, sin permiso o conciencia de sus actos por parte de un afectado, adquiere información privada para beneficio propio o de terceros.

F

Frame Relay: Es un sistema de transmisión de datos que utiliza tramas (frames, bloques de información delimitados) y no paquetes. Permite altas velocidades y tráfico, incluyendo voz y datos (servicios Frame Relay - Data Voz) a través de los servicios de Telefónica.

FTP: (File Transfer Protocol - Protocolo de Transferencia de Archivos) en informática, es un protocolo de red para la transferencia de archivos entre sistemas conectados a una red TCP, basado en la arquitectura cliente-servidor.

G

Gateway: Es un ordenador que permite las comunicaciones entre distintos tipos de plataformas, redes, ordenadores o programas. Para lograrlo

traduce los distintos protocolos de comunicaciones que éstos utilizan. Es lo que se conoce como pasarela o puerta de acceso.

GNU/Linux: Término empleado para referirse al sistema operativo Unix-like que utiliza como base las herramientas de sistema de GNU y el núcleo Linux. Todo el código fuente puede ser utilizado, modificado y redistribuido libremente por cualquiera bajo los términos de la Licencia Pública General (GPL).

H

HTTP: Es el protocolo o las reglas de funcionamiento de los servidores WWW, que son los encargados de mantener este tipo de páginas.

Host: Computador central o principal en un entorno de procesamiento distribuido. Por lo general se refiere a un gran computador de tiempo compartido o un computador central que controla una red.

Host Bastión: Sistema que actúa como intermediario en el contacto de los usuarios de la red interna de una organización con otro tipo de redes. El host bastión filtra tráfico de entrada y salida; esconde la configuración de la red hacia fuera.

Hacker: Término utilizado para llamar a una persona con grandes conocimientos en informática y telecomunicaciones y que los utiliza con un determinado objetivo. Este objetivo puede o no ser maligno o ilegal.

I

IDS: (Intrusión Detección Sistema). Sistema de detección de intrusos. Herramienta de seguridad que intenta detectar o monitorizar los eventos

ocurridos en un determinado sistema informático en busca de intentos de comprometer la seguridad de dicho sistema.

IP: Dirección IP. Matrícula que identifica a un ordenador de la red. A los ordenadores personales se les asigna una IP adress para que naveguen por la red, que cambia en cada sesión de acceso a Internet.

Interfaz: Parte de un programa que permite el flujo de información entre un usuario y la aplicación, o entre la aplicación y otros programas o periféricos. Esa parte de un programa está constituida por un conjunto de comandos y métodos que permiten estas intercomunicaciones.

IRC: (***Internet Relay Chat***) Protocolo de comunicación en tiempo real basado en texto, que permite debates en grupo o entre dos personas y que está clasificado dentro de los servicios de comunicación en tiempo real. Se diferencia de la mensajería instantánea en que los usuarios no deben acceder a establecer la comunicación de antemano, de tal forma que todos los usuarios que se encuentran en un canal pueden comunicarse entre sí, aunque no hayan tenido ningún contacto anterior.

ISA server de Microsoft: Gateway integrado de seguridad perimetral que protege una red local frente a amenazas basadas en Internet y permite a los usuarios un acceso remoto rápido y seguro a las aplicaciones y los datos.

K

Kernel: Es el núcleo de una sistema operativo en el cual se asegura que haya comunicación entre los programas informático y el hardware.

M

Máscara de subred: La máscara de subred es un código numérico que forma parte de la dirección IP (Dirección de una computadora usada en internet) de los computadores, tiene el mismo formato que la dirección IP, pero afecta sólo a un segmento particular de la red. Se utiliza para dividir grandes redes en redes menores, facilitando la administración y reduciendo el tráfico inútil, de tal manera que será la misma para ordenadores de una misma subred.

N

NNTP: (Network News Transport Protocol) Protocolo de transferencia de Noticias. Es un Protocolo de red basado en tiras de textos enviados sobre canales TCP de 7 bit ASCII. Es usado para subir y bajar así como para transferir artículos entre servidores.

*NAT***: (**Traducción de Dirección de Red) es un mecanismo utilizado por routers IP para intercambiar paquetes entre dos redes que se asignan mutuamente direcciones incompatibles. Consiste en convertir en tiempo real las direcciones utilizadas en los paquetes transportados.

Netscreen: es una solución eficiente y robusta para las empresas que desean utilizar el ancho de banda en su acceso a Internet y a la vez disponer de un máximo nivel de seguridad en la red de área local evitando así cualquier posible ataque externo.

P

Phishing: es un tipo de engaño creado por hackers malintencionados, con el objetivo de obtener información importante como números de tarjetas de crédito, claves, datos de cuentas bancarias y datos más importantes.

Pharming: es la explotación de una vulnerabilidad en el software de los servidores DNS (Domain Name System) que permite a un atacante redireccionar un nombre de dominio a otra máquina distinta. De esta forma un usuario que introduzca un determinado nombre de dominio, que haya sido redireccionado, en su explorador de internet, accederá a la página web que el atacante haya especificado para ese nombre de dominio.

Protocolo: conjuntos de reglas que rigen la comunicación.

Proxy: Utilizado en las redes de área local, un proxy es un servidor virtual que realiza la conexión con el servidor real de Internet y a través del cual se conectan el resto de los ordenadores clientes.

PIX de Cisco: es una de las soluciones de seguridad ofrecidas por Cisco Systems; se trata de un firewall completamente hardware.

PSH: Es un bit que se encuentra en el campo del código en el protocolo TCP. Cuando PSH está activado indica que los datos de ese segmento y los datos que hayan sido almacenados anteriormente en el buffer del receptor deben ser transferidos a la aplicación receptora lo antes posible.

R

RST: Es un bit que se encuentra en el campo del código en el protocolo TCP, y se utiliza para reiniciar la conexión. Un ejemplo práctico de utilización es el que realiza un servidor cuando le llega un paquete a un puerto no válido: este responde con el RST activado.

S

SMTP: Protocolo Simple de Transferencia de Correo, es un protocolo de la capa de aplicación. Protocolo de red basado en texto utilizado para el intercambio de mensajes de correo electrónico entre computadoras u otros

dispositivos (PDA's, teléfonos móviles, etc.).

SYN: es un byte de control dentro del segmento TCP, se usa para sincronizar los números de secuencia en tres tipos de segmentos: petición de conexión, confirmación de conexión (con ACK activo) y la recepción de la confirmación (con ACK activo).

Shell: Es un intérprete de comandos que actúa como interfaz de usuario para comunicar al usuario con el sistema operativo mediante una ventana que espera órdenes escritas los interpreta y los entrega al sistema operativo para su ejecución.

Script: Guion o archivo de órdenes o archivo de procesamiento por lotes. Es un programa usualmente simple, que generalmente se almacena en un archivo de texto plano. El uso habitual de los scripts es realizar diversas tareas como combinar componentes, interactuar con el sistema operativo o con el usuario.

Scam: Tipo de fraude informático, híbrido entre el phishing y las pirámides de valor.

Spam: se denomina con este término al correo electrónico que se recibe de forma indeseada, generalmente con carácter comercial.

T

TELNET: Protocolo mediante el cual se puede realizar una conexión a servidores basados en UNIX.

U

UDP: (protocolo de datagramas de usuario) es un protocolo simple que intercambia datos sin acuse de recibo ni garantía de entrega. UDP se apoya en las aplicaciones para manejar la retransmisión y el procesamiento de errores.

V

*VPN (*Virtual Private Network): red privada que trabaja dentro de una red pública como es el internet.

Vmware: Máquina anfitriona (host) hace referencia a la computadora o sistema operativo que ejecuta el proceso VMware Workstation. En tanto, el sistema operativo (o aplicación virtual) que se ejecuta dentro de la máquina virtual es llamado huésped (guest).

W

Worms: Programa informático que se autoduplica y autopropaga. En contraste con los virus, los gusanos suelen estar especialmente escritos para redes.

10. BIBLIOGRAFIA

Libros

- **PICOUTO Fernando, LORENTE Iñaki, GARCIA Jean Paul, Ramos Antonio.** Hacking y Seguridad en Internet. México D.F. Edit. Alfaomega Grupo Editor 2008.
- **ZIEGLER Robert**. Firewalls Linux. México D.F. Edit. Prentice Hall 2001.
- **ARROYO José**. Linux Máxima Seguridad edición especial. México D.F. Edit. Prentice Hall 2000.
- **KOMAR Brian, BEEKELAAR Ronald, WETTERN Joern**. Firewall For Dummies. New York. Edit. Wiley Publishing Inc. 2003.
- **SUEHRING Steve, ZIEGLER Robert.** Linux Firewalls Third Edition. Edit. Sams Publishing 2005.
- **NOONAN Wes, DUBRAWSKY Ido.** Firewall Fundamentals. Edit. Cisco Press 2006.

Páginas Web

- **3Com Corporation**. Seguridad de Redes: Una guía para implementar Firewalls.

  http://lat.3com.com/lat/technology/technical_papers.html

- **MOLINA** Hernán D. Universidad Nacional de Lujan. Firewalls distribuidos. Noviembre 24 de 2006.

http://www.textoscientificos.com/redes/firewalls-distribuidos

- **MOLINA** Hernán D. Universidad Nacional de Lujan. Planes de seguridad Noviembre 24 de 2006. http://www.textoscientificos.com/redes/firewalls-distribuidos/soluciones-seguridad/politicas-seguridad/planes-seguridad

- **E-PROYECTA** Implementación de servidores avanzados firewall en Linux. http://www.e-proyecta.es/linux-iptables.html

- **NETFILTER.** What is netfilter.org. http://www.netfilter.org

- **MARTÍNEZ,** Javier. Tutorial Shell Scripts I. Marzo 25 2008. http://observatorio.cnice.mec.es/modules.php?op=modload&name=News&file=article&sid=573

- **IPTRAF**, IP Network Monitoring. http://iptraf.seul.org/

- **SEGURIDAD INFORMATICA,** Universidad del Cauca. Práctica con Iptables. http://gseguridad.unicauca.edu.co/index.php?option=com_content&task=view&id=141&Itemid=13

- **CENTOS, Conmmunity Enterprise Operating System**. IPTables. Noviembre 11 2008. http://wiki.centos.org/es/HowTos/Network/IPTables

- **UNIVERSIDAD ICESI, Administración de Plataformas y Seguridad.** Guía de configuración de NAT/PAT en Linux. http://www.icesi.edu.co/ocw/tic/administracion_plataformas_y_seguridad/nat-pat-firewall/practica-de-nat-pat-con-iptables/view

- **UNIVERSIDAD ICESI, Administración de Plataformas y Seguridad.** Guía de Configuración de Firewall en Linux. http://www.icesi.edu.co/ocw/tic/administracion_plataformas_y_seguridad/nat-pat-firewall/practica-de-firewall-con-iptables-nat-pat/view

ANEXOS

ANEXOS 1. Tutorial de Instalación del APPSERV

¿Qué es AppServ?

AppServ Es una herramienta OpenSource para Windows que facilita la instalación de Apache, MySQL y PHP en una sola herramienta, esta característica facilita la tarea al usuario ya que se configuran las aplicaciones de forma automática los siguientes programas:

- ✓ Apache WebServer: Servidor HTTP multiplataforma.
- ✓ PHP Script Language: Lenguaje de programación dinámico que utilizan la mayoría de gestores de contenidos más populares.
- ✓ MySQL: gestor de bases de datos, rápido y seguro
- ✓ phpMyAdmin: interfaz gráfica de administración para MySQL

Se puede conseguir

AppServ se encuentra disponible en su página oficial en la dirección http://www.appservnetwork.com/, en donde se puede descargar la última versión.

¿Cómo se instala?

Una vez descargado el archivo ejecutable del AppServ que ocupa unos 16,4 MB.

Pulsando sobre el icono se comienza con la instalación.

En primer lugar se empiezan a preparar los archivos e inicia con la Correspondiente pantalla de bienvenida:

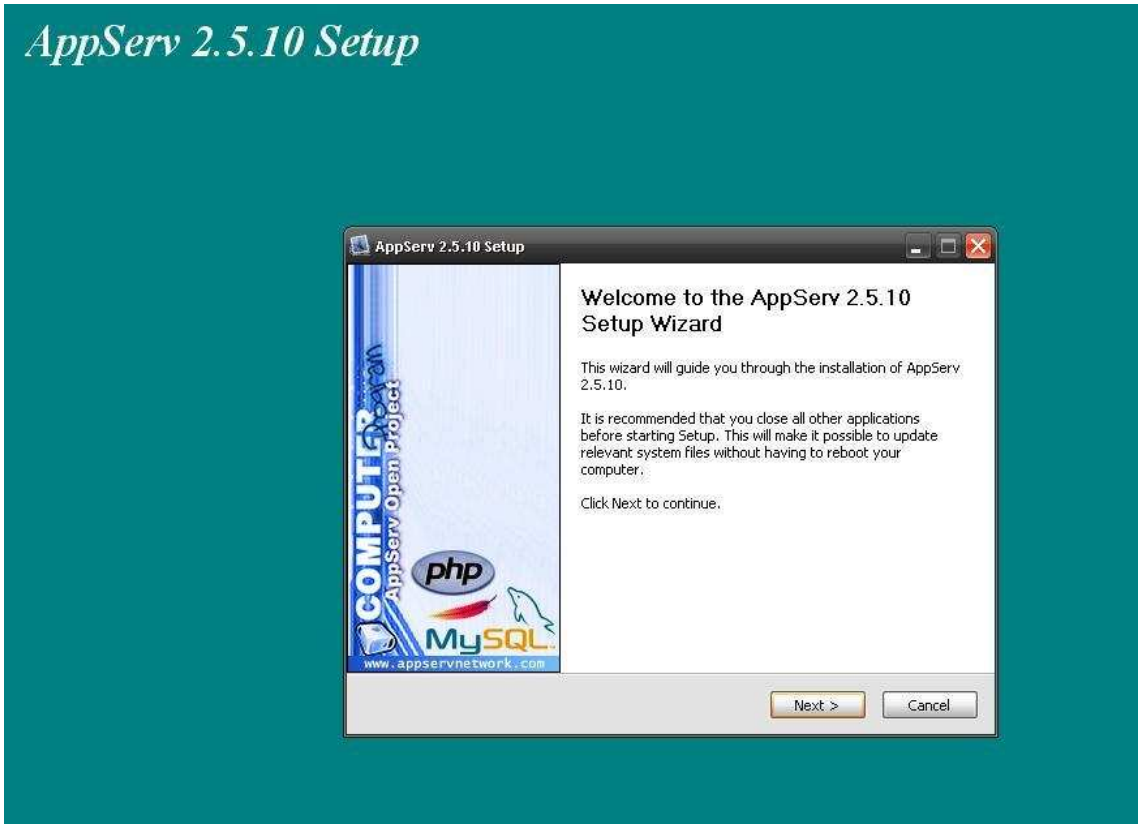

Figura 37. Instalación AppServ I

Una vez pulsado el Next> el programa nos preguntará en donde queremos instalar los archivos correspondientes, podemos dejar por defecto C:\AppServ y se creará una carpeta en el disco C con este nombre:

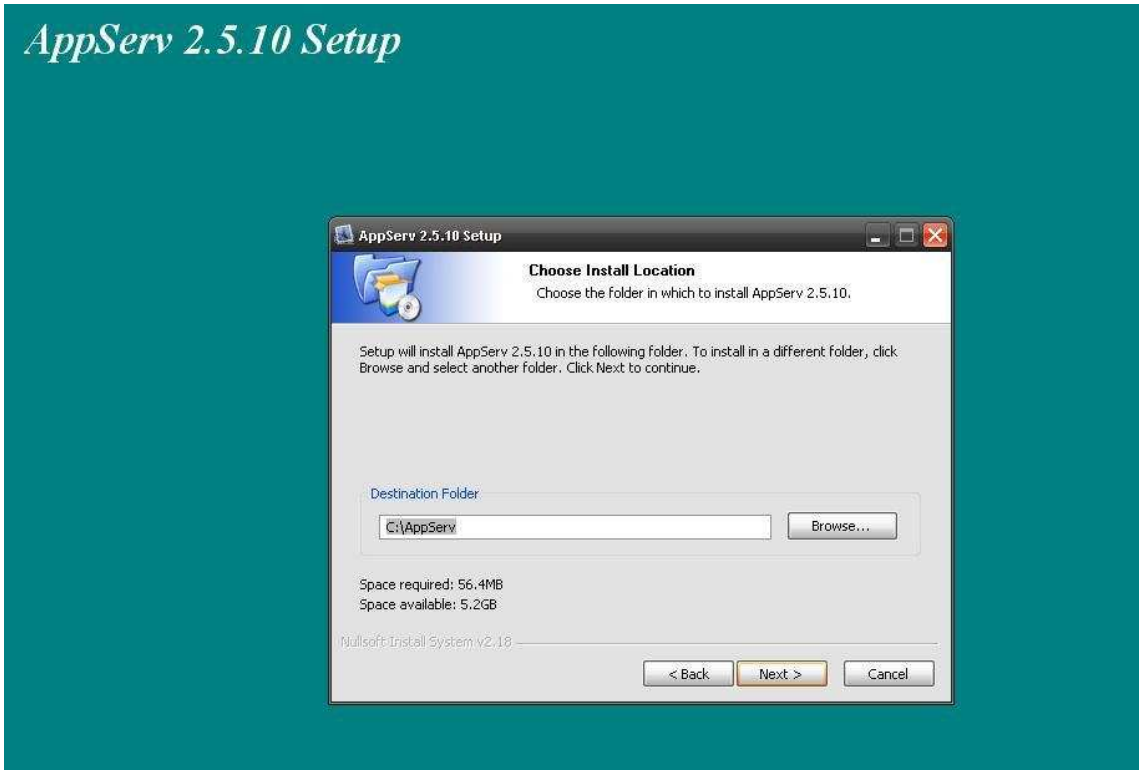

Figura 38. Instalación AppServ II

En este punto llegamos a la configuración del servidor Apache, se deja por defecto el localhost

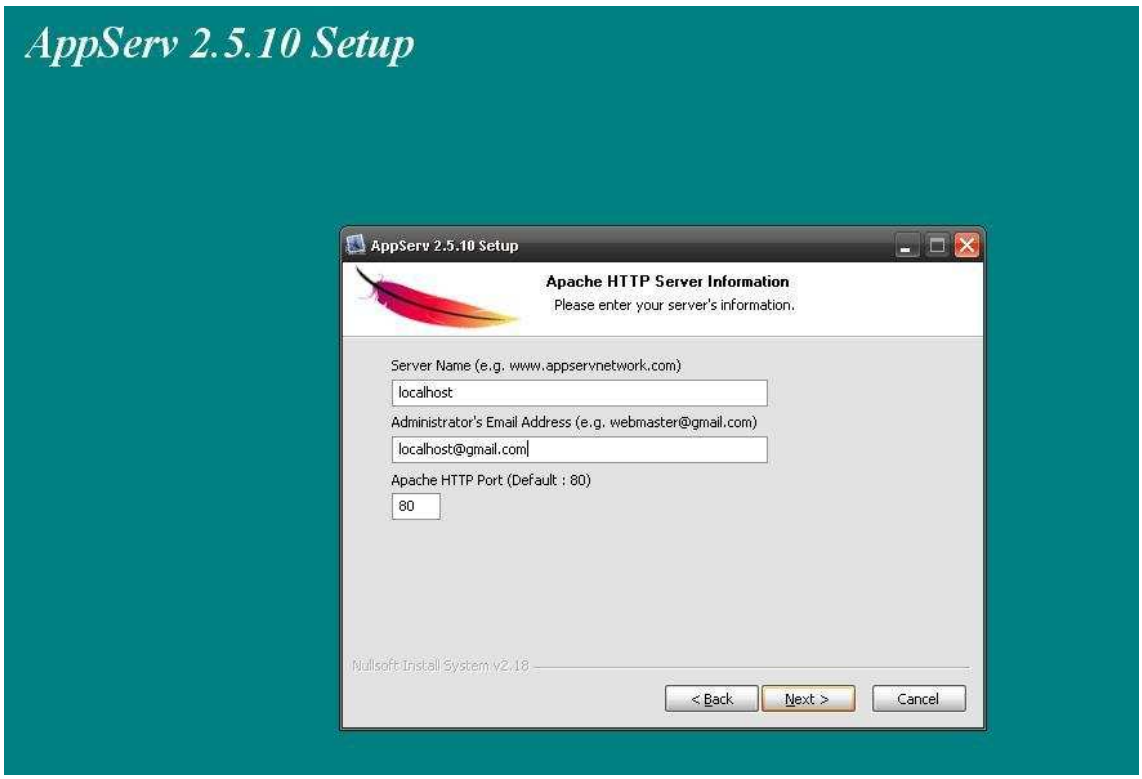

Figura 39. Instalación AppServ III

Desde el navegador preferido se ingresa la dirección: http://localhost/ y aparecerá la pagina inicio de Appserv.

ANEXO 2. Manual de Instalación y Configuración del Servidor Firewall

Firewalls

- Es un dispositivo de hardware o una aplicación de software diseñado para proteger los dispositivos de red de los usuarios externos de la red o de aplicaciones y archivos maliciosos.
- El firewall define los servicios que pueden accederse desde el exterior y viceversa.
- Los firewalls son también importantes porque proporcionan un único punto de restricción, donde se pueden aplicar políticas de seguridad y auditoría

Características de los Firewalls.

- ***Control de Servicios*:** Determina el tipo de servicios de Internet que pueden ser permitidos hacia adentro o hacia afuera.
- ***Control de dirección***: Determina en qué dirección cada servicio en particular se le permite circular.
- ***Control de Usuarios:*** Se implementan controles de acceso a un servicio de acuerdo al usuario que está tratando de acceder.
- ***Control de comportamiento****:* Controla como son utilizados cada servicio en Particular (ejemplo: filtrado de correo electrónico)

Tipos de filtrado en Firewalls

- **Filtrado a nivel de paquete:** Se realiza a nivel de la capa de Red, examinando la cabecera del paquete. En los cuales se hace una verificación de la cabecera de los paquetes que contienen las direcciones IP.

Figura 40. Filtrado de paquete

Criterios de Filtrado

- Dirección de origen: se puede crear reglas para las IPs de la red local.
- Dirección de destino: se puede crear reglas para las IPs de la red externa o internet, en el caso que un host de esa red quiera acceder al firewall para administrarlo , o acceder a un servicio que esté disponible dentro de la red local.
- Puerto de origen: hace referencia al puerto donde va salir una petición por parte de un usuario. Puede ser TCP o UDP.
- Puerto de destino: hace referencia al puerto donde se encuentra disponible un servicio como puede ser HTTP, FTP entre otros.
- Tipo de paquetes: se refiera a los protocolos TCP, UDP, ICMP etc.
- Interfaces de entrada: hace referencia a los adaptadores de red, que puede ser cualquiera que esté cumpliendo una función de entrada según estipulada en las reglas.

- Interfaces de salida: se refiere a los adaptadores de red, pero en este caso es de salida en el caso que un usuario este haciendo una petición, la interfaz de salida seria la conecta con la red local.

Firewall de Filtrado de Circuito.

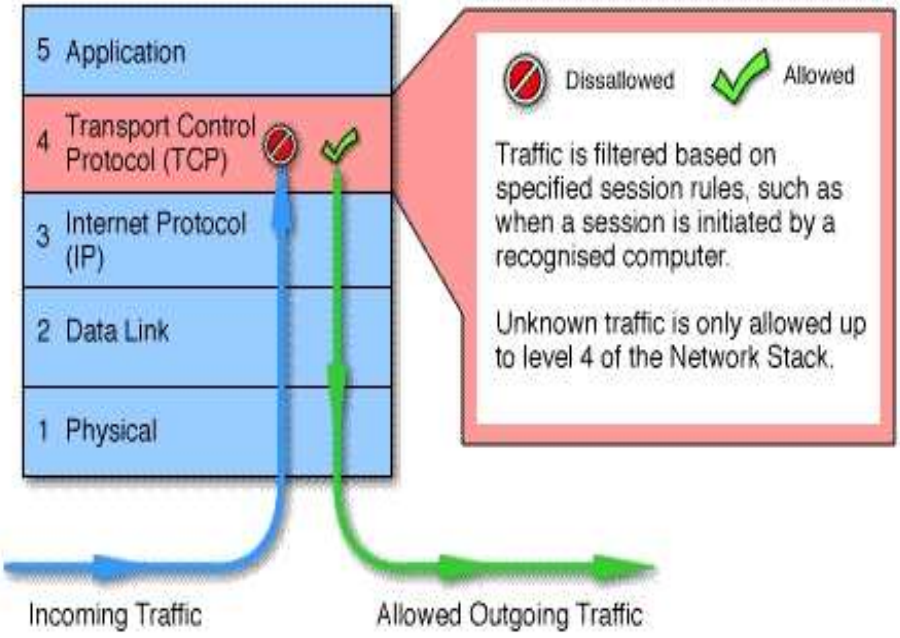

Figura 41. Filtrado de circuito

Trabaja en las capas de transporte y sesión del modelo OSI, su función principal es examinar la información TCP que se envían entre sistemas para verificar que la petición sea legítima.

Filtrado a nivel de aplicación (proxies)

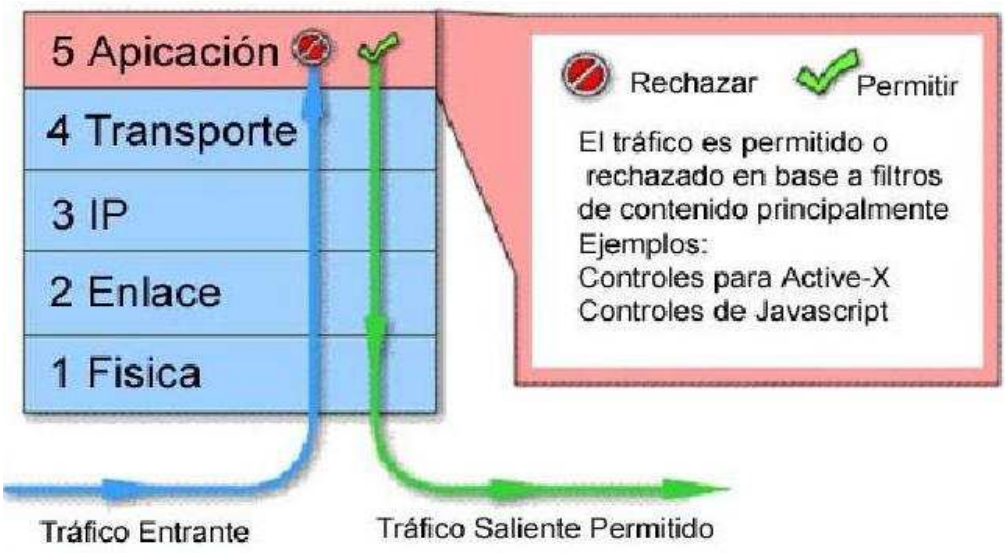

Figura 42. Filtrado a nivel de aplicación

La función principal es realizar conexiones punto a punto desde el cliente al proxy y desde este al servicio de red requerido.

Arquitectura de Firewalls

- **Arquitectura de Host de doble acceso**: En esta arquitectura la red está protegida perimetralmente por un solo Firewall, que protege la red interior de la red exterior en el caso típico de conexión a internet y que tiene instalada dos tarjetas de red.

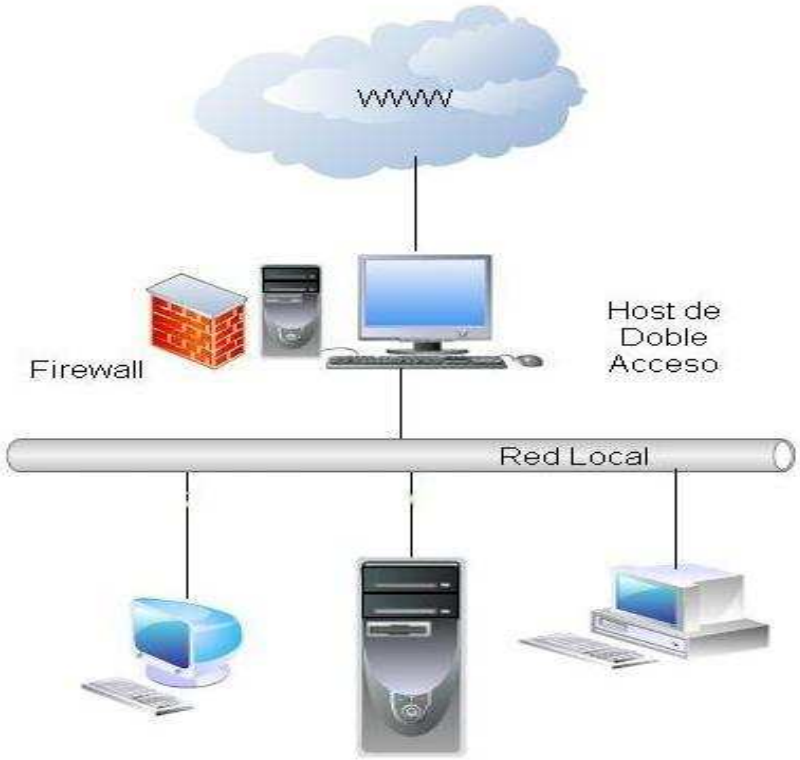

Figura 2. Arquitectura Host de doble acceso

El dispositivo host es crítico para la seguridad de la red ya que es el único sistema que puede ser accedido y atacado desde Internet, por lo que debe poseer un alto nivel de protección a diferencia de un host común de la red interna.

Utilización

- Pequeña cantidad de tráfico dirigido a Internet
- El tráfico dirigido a Internet no crítico
- No ofrece servicios a usuarios de Internet
- La red protegida no contiene datos muy importantes

- **Arquitectura de Host de protección**: Firewall compuesto por un Router para el filtrado de paquetes y un host bastión para el filtrado de conexiones a nivel de circuito y aplicación.

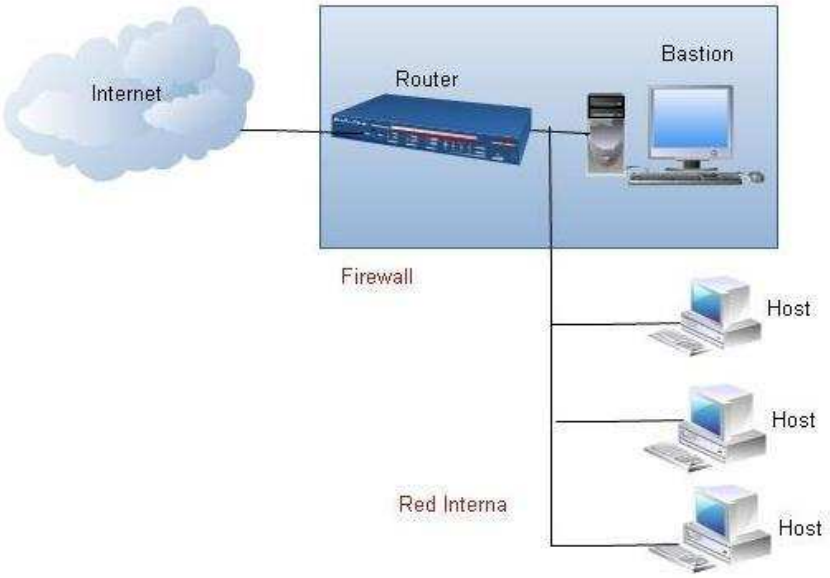

Figura 3. Arquitectura de host de protección

Configuraciones del Router como filtrado de paquetes:

- ✓ Permitir que ciertos hosts internos puedan abrir conexiones a Internet para ciertos servicios.
- ✓ Deshabilitar todas las conexiones desde los hosts internos habilitando solo al host bastión para establecer estas conexiones.
- ✓ Es posible que algunos paquetes sean dirigidos, por el Router, directamente a los hosts internos.

- **Arquitectura de subred de protección:**

- ✓ Arquitectura introduce dos Routers uno externo y uno interno, en medio de estos dos Routers se encuentra la red Zona Desmilitarizada, en este caso sería el host bastión.
- ✓ Con esta configuración no existe un único punto vulnerable que ponga en riesgo toda la red interna.
- ✓ El Router externo ofrece protección contra ataques provenientes de la red externa y administra el acceso de Internet a la red perimetral.
- ✓ El Router interno protege la red interna de la red externa y de la perimetral administrando el acceso de ésta a la red interna.

- ✓ El host bastión conectado a la red perimetral es el principal punto de contacto para conexiones de entrada desde la red externa, por ejemplo, servidores de correo electrónico (SMTP), conexiones FTP al servidor anónimo del sitio, consultas DNS al sitio, servidores web, entre otras.

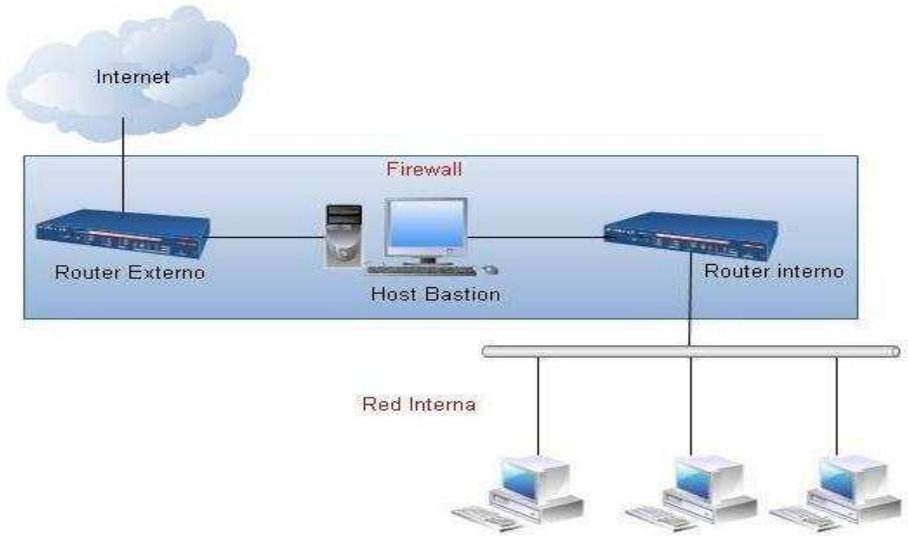

Figura 4. Arquitectura de subred de protección

Políticas de Seguridad

- Una política de seguridad es una declaración formal de las normas que los usuarios deben respetar a fin de acceder a los bienes de tecnología.
- Los firewalls generalmente implementan una de dos políticas de diseño básicas:
  - ➢ Permitir todo servicio, a menos que sea expresamente restricto, o
  - ➢ Denegar todo servicio, a menos que sea expresamente permitido.

Reglas de Firewall

Reglas del Firewall						
Protocolo	**Protocolo de transporte**	**Red de Origen**	**Puerto Origen**	**Red destino**	**Puerto Destino**	**Acción**
HTTP	TCP	192.168.4.0/24	Cualquiera	Cualquiera	80	Permitir
FTP	TCP	192.168.4.0/24	Cualquiera	Cualquiera	21	Permitir
ICMP		192.168.3.2		192.168.3.0/24		Permitir
ICMP		192168.4.1		192.168.4.0/24		Permitir
HTTP	TCP	Cualquiera		192.168.4.2	80	Permitir
FTP	TCP	192.168.1.2		192.168.4.3	21	Permitir
	TCP	Cualquiera		192.168.3.2	10000	Denegado

Tabla 1. Reglas de Firewall

Implementación y Configuración del Servidor Firewall

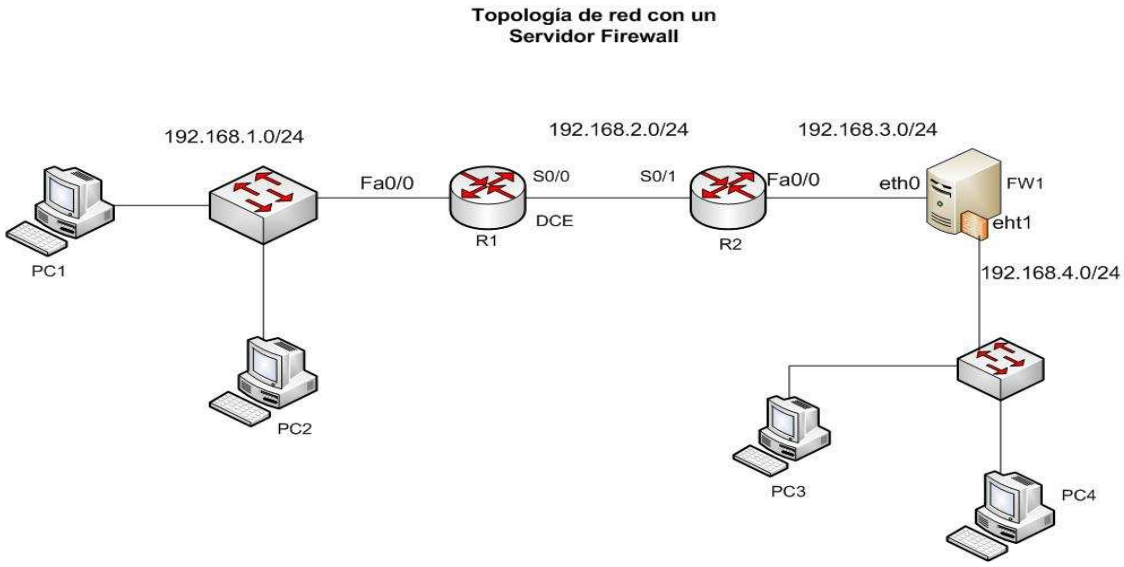

Figura 43. Topología del Servidor Firewall

Esta topología es una Arquitectura de firewall Host de doble acceso en el cual el servidor Firewall tiene dos interfaz de red en donde una comunica a una red LAN 1 y la otra comunica con red local LAN 2.

Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Mascara de Subred	Gateway
R1	Fa0/0	192.168.1.1	255.255.255.0	No aplicable
	S0/0/0	192.168.2.1	255.255.255.0	No aplicable
R2	Fa0/0	192.168.3.1	255.255.255.0	No aplicable
	S0/0/1	192.168.2.2	255.255.255.0	No aplicable
PC1	N/A	192.168.1.2	255.255.255.0	192.168.1.1
PC2	N/A	192.168.1.3	255.255.255.0	192.168.1.1
FW1	Fa0	192.168.3.2	255.255.255.0	192.168.3.1
	Fa1	192.168.4.1	255.255.255.0	
PC3	N/A	192.168.4.2	255.255.255.0	192.168.4.1
PC4	N/A	192.168.4.3	255.255.255.0	192.168.4.1

Tabla 2. Tabla de direccionamiento

Componentes del Sistema Firewall Linux.

- **Requerimientos de Hardware:** Los sistemas GNU/Linux pueden instalarse en equipo con capacidades muy reducidas (o limitadas).

  - ✓ Procesador Intel Pentium III / AMD Athlon, 550MHz (o mayor)
  - ✓ 512 MB RAM
  - ✓ 10 GB en disco duro
  - ✓ 2 Interfaz de red**.**

- **Requerimientos de software:** Para la implementación del servidor Muro Cortafuego se utilizo la distribución de Linux CentOS junto con la herramienta Iptables.

Instalación del Sistema Operativo Centos 5.2

Se inserta el primer CD de instalación de CentOS 5 antes de arrancar el sistema y después de aparecer el Boot de Linux presionamos la tecla Enter para la instalación grafica.

Figura 44. Instalación de Centos I

Se Selecciona **«Skip»** cuando el espacio en disco no tiene ningún problema.

Figura 45. Instalación de Centos II

Hacemos clic sobre el botón «Next» en cuanto aparezca la pantalla de bienvenida de CentOS.

Figura 46. Instalación de Centos III

Se selecciona los requerimientos mínimos de software, en este caso solo se habilita la interfaz de escritorio.

Figura 47. Instalación de Centos IV

Concluida la instalación de los paquetes, se hace clic sobre el botón **Reiniciar.**

Figura 48. Instalación de Centos V

Instalación y configuración de Iptables

Iptables es una herramienta en línea de comandos usados para configurar reglas de filtrado de paquetes en los kernels de Linux 2.4 y 2.6, soporta IPv4 e IPv6.

Instalación de Iptables

En la consola de Shell de Linux ejecutamos la siguiente línea de comando:

Yum -y install Iptables

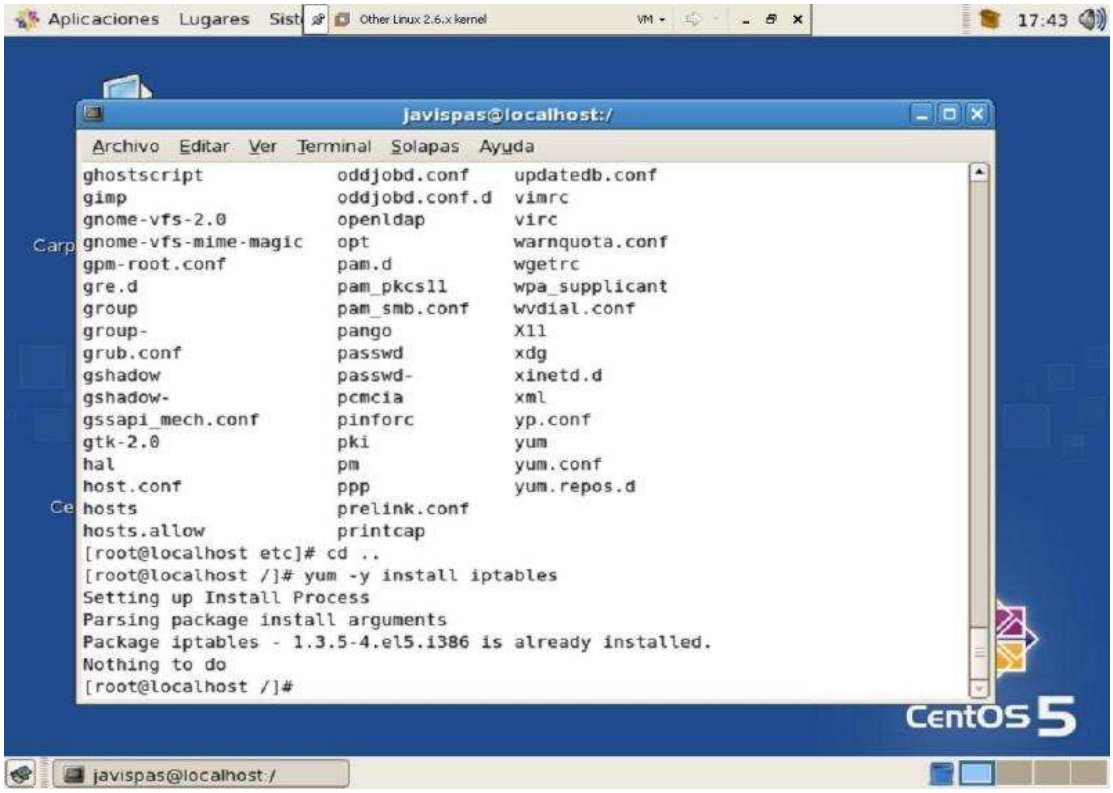

Figura 6. Instalación Iptables

Configuración de Iptables

La configuración de Iptables se basa en tres tablas diferentes y una serie de cadenas asociadas a cada una de estas tablas:

- **Filter:** Revisa el contenido de los paquetes de información que atraviesan el firewall. Las cadenas asociadas son:
  - ✓ Input: Analiza los paquetes recibidos en una interfaz de red.

- ✓ Output: Analiza los paquetes que son enviados por la misma interfaz de red.
- ✓ Forward: Chequea los paquetes que atraviesan una de las interfaces de red del firewall y los envía a la otra.

➢ **NAT:** se emplea principalmente para la traducción de direcciones de red. Las cadenas asociadas son:

- ✓ Prerouting: Esta cadena se usa principalmente para la traducción de direcciones de red de destino.
- ✓ Postrouting: Cadena utilizada para la traducción de las direcciones de red de origen.

La sintaxis de los comandos de Iptables es la siguiente:

Iptables [-t <nombre-tabla>] <comando> <nombre-cadena> <parámetros> <opciones>

<nombre-tabla>: Se selecciona la tabla que se va a utilizar, siendo la tabla por defecto filter.

<comando>: Hace referencia a la acción que va a llevar a cabo, como eliminar, añadir, o modificar reglas de una cadena.

- ✓ **A**: Se añade la regla al final de la cadena especificada.
- ✓ **D**: Elimina la regla de una cadena especificada por un número ordinal.
- ✓ **C**: Chequea una regla antes de añadirla a la cadena.
- ✓ **F**: Elimina la cadena seleccionada eliminando todas las reglas que la componen.

<nombre-cadena>: Solo se permite un comando por cadena. Se escriben en mayúsculas.

<Parámetros>: Definen las acciones que la regla produce.

- ✓ **o**: Configura el adaptador de red de salida para una regla usándose en la cadena UTPUT, FORWARD, y POSTROUTING, en las tablas nat.

- ✓ **i**: Configura los adaptadores de entrada de red para ser habilitados por una regla en particular. En Iptables con la tabla filter solo se podrán utilizar cadenas INPUT y FORWARD cuando se utilice por filter y PREOROUTING con nat.
- ✓ **s**: Especifica la dirección origen del paquete.
- ✓ **p**: Especificará el protocolo al que se aplica la regla; si esta especificación no se lleva a cabo aplicará a todos los protocolos.
- ✓ **d**: Detalla el nombre del sistema destino, dirección IP o IP de red de un paquete.
- ✓ **j**: Especifica la opción de disposición de paquete para una regla.

Se puede implementar otro tipo de opciones como son:

- ✓ dport: Configura el puerto destino de tráfico.
- ✓ Sport: Configura el puerto de origen del trafico[17].

Implementación de Iptables para una Red Local

La configuración sería la siguiente para el Router 1:

Router> Enable

Router# config t

Router(config)# int Fa0/0

Router(config-if) # ip address 192.168.1.1 255.255.255.0

Router(config-if) # no shutdown

Router(config-if) # exit

Router(config)# int s0/0

[17] PICOUTO Fernando, LORENTE Iñaki. Hacking y Seguridad en Internet. México: Alfaomega Grupo Editor, S.A, 2008. P 405

Router(config-if) # ip address 192.168.2.1 255.255.255.0

Router(config-if) # clock rate 56000

Router(config-if) # no shutdown

Router(config-if) # exit

Router(config)# Router rip

Router(config-router)# network 192.168.1.0

Router(config-router)# network 192.168.2.0

Router(config-router)# exit

Router(config)# exit

Router# copy run start

La configuración sería la siguiente para el Router 2:

Router> Enable

Router# config t

Router(config)# int Fa0/0

Router(config-if) # ip address 192.168.3.1 255.255.255.0

Router(config-if) # no shutdown

Router(config-if) # exit

Router(config)# int S0/1

Router(config-if) # ip address 192.168.2.2 255.255.255.0

Router(config-if) # no shutdown

Router(config-if) # exit

Router(config)# Router rip

Router(config-router)# network 192.168.3.0

Router(config-router)# network 192.168.2.0

Router(config-router)# exit

Router(config)# exit

Router# copy run start

Configuración de tarjetas de red en VMware

Seleccionamos cada tarjeta física que está instalada en el sistema operativo en las opciones del VMware.

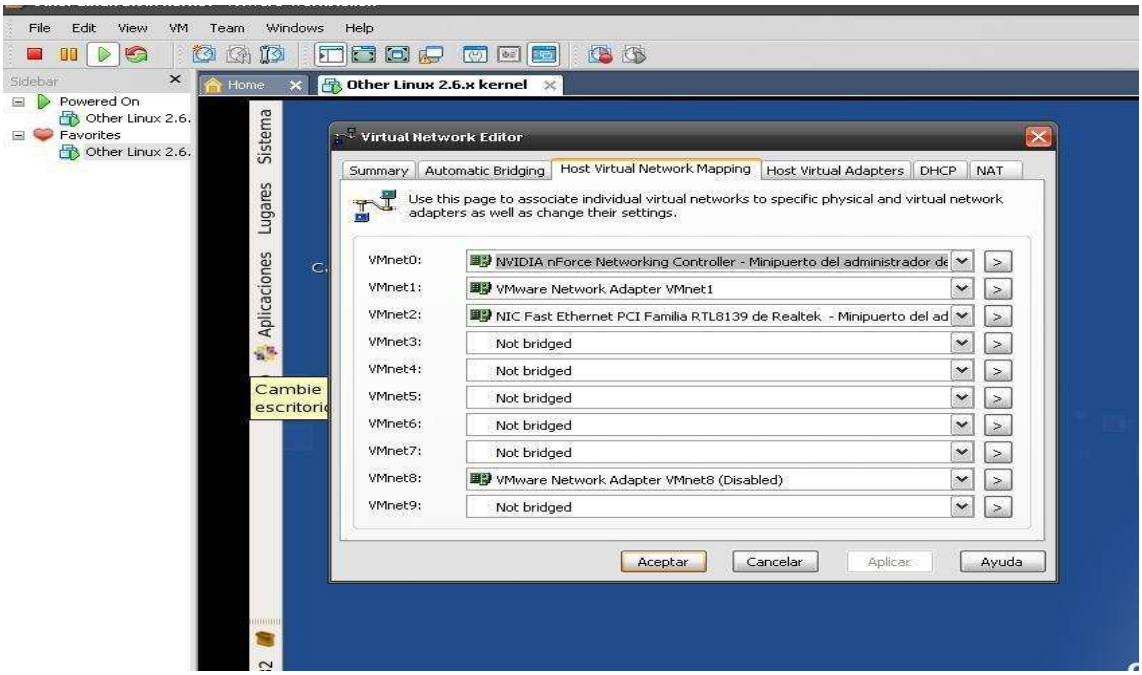

Figura 8. Configuración redes virtuales

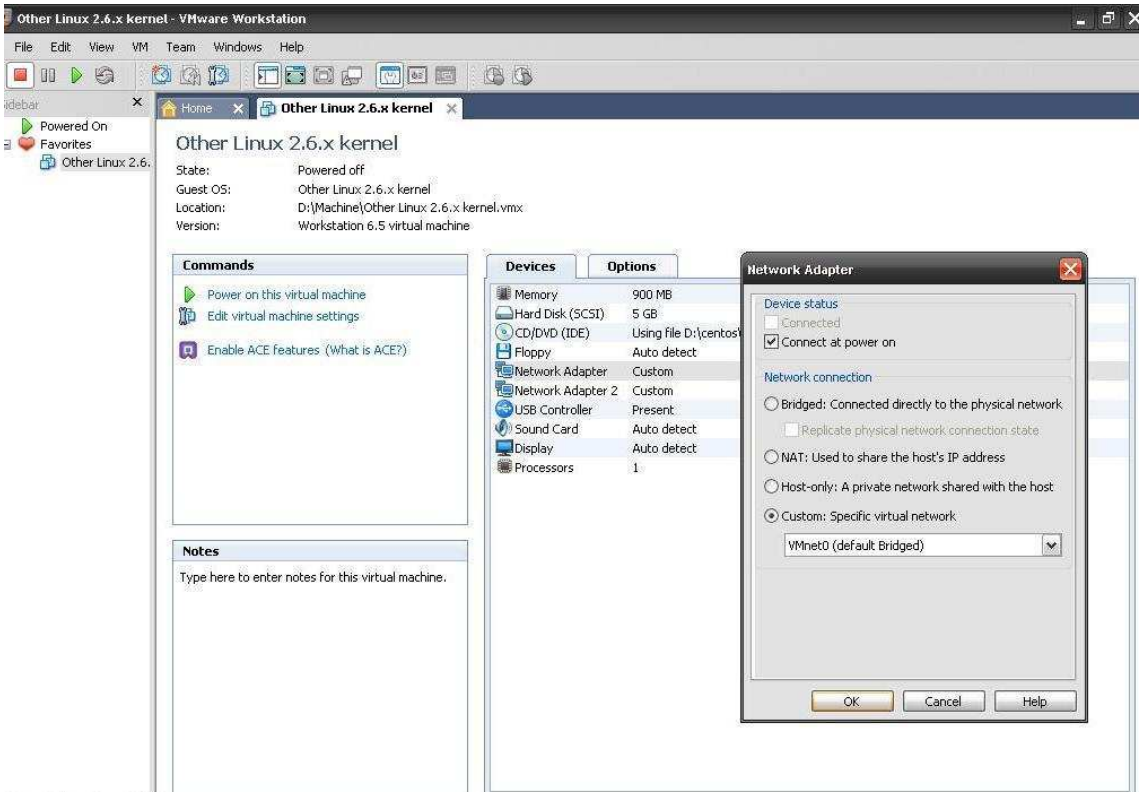

Figura 9. Configuración Nic virtual

Configuración de las IPs en la maquina virtual Linux Centos 5.2

Procedemos a configurar las interfaces eth0 y eth1 de Centos en la cual haciendo clic en Sistema, Administración y red

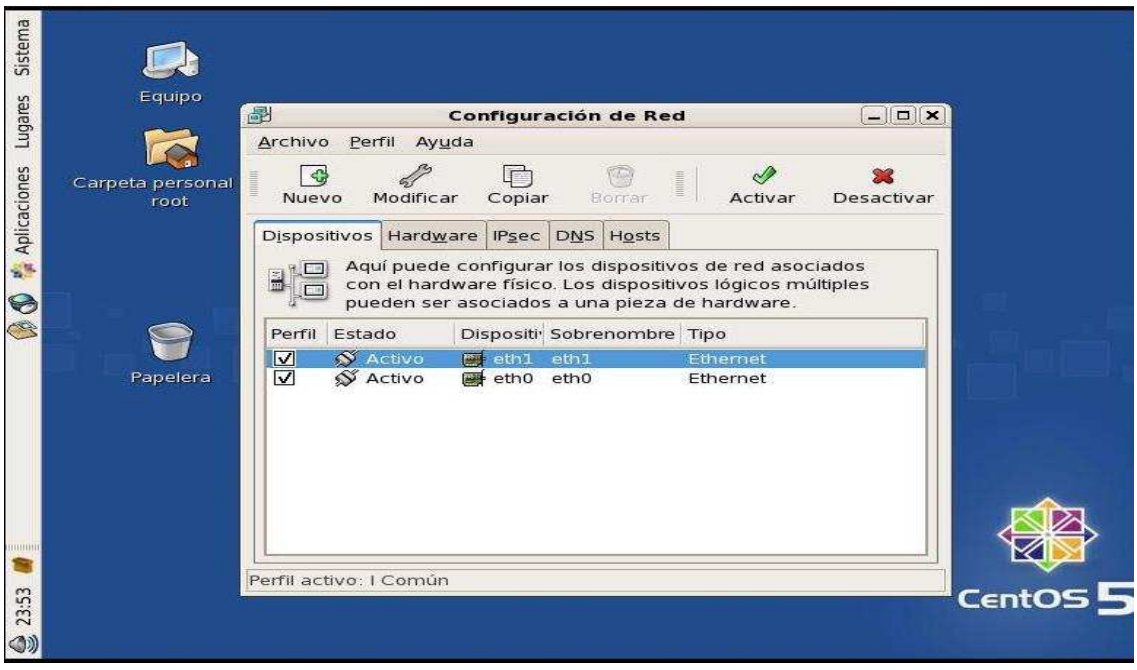

Figura 12. Configuración interfaces de red

Procedemos a configurar la IP a la interfaz eth0 y eth1

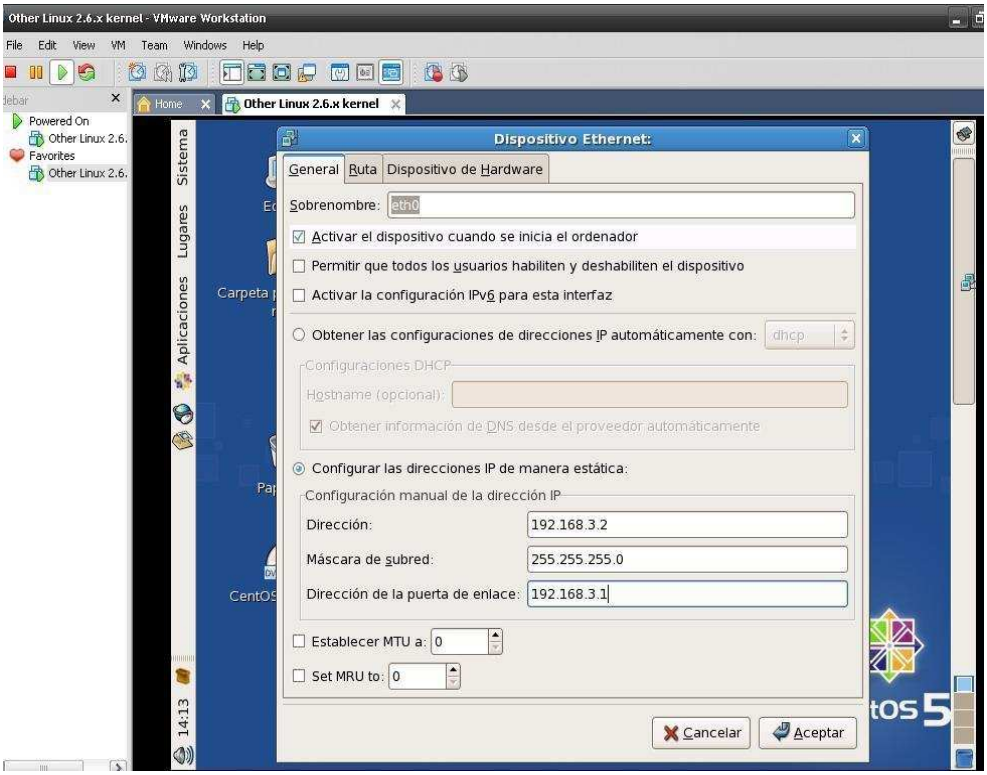

Figura 13. Configuración IP eth0

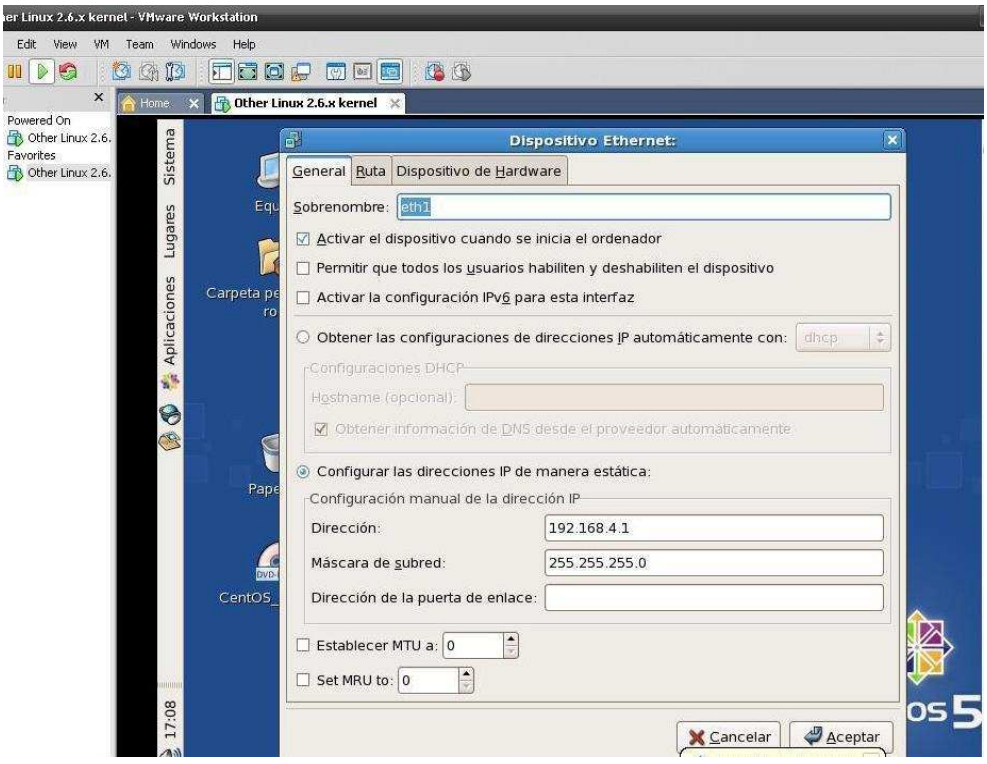

Figura 14. Configuración IP eth1

Configuración del Script Iptables.

- ✓ Script iptables hace referencia a programas escritos para la Shell de Linux.
- ✓ Son archivos que ejecutan un conjunto de comandos.

Pasos para la creación de un script Iptables:

1. Crear un archivo en dentro del fichero raíz /etc/rc.d, específicamente en esta implementación se creó un archivo llamado rc.firewall.

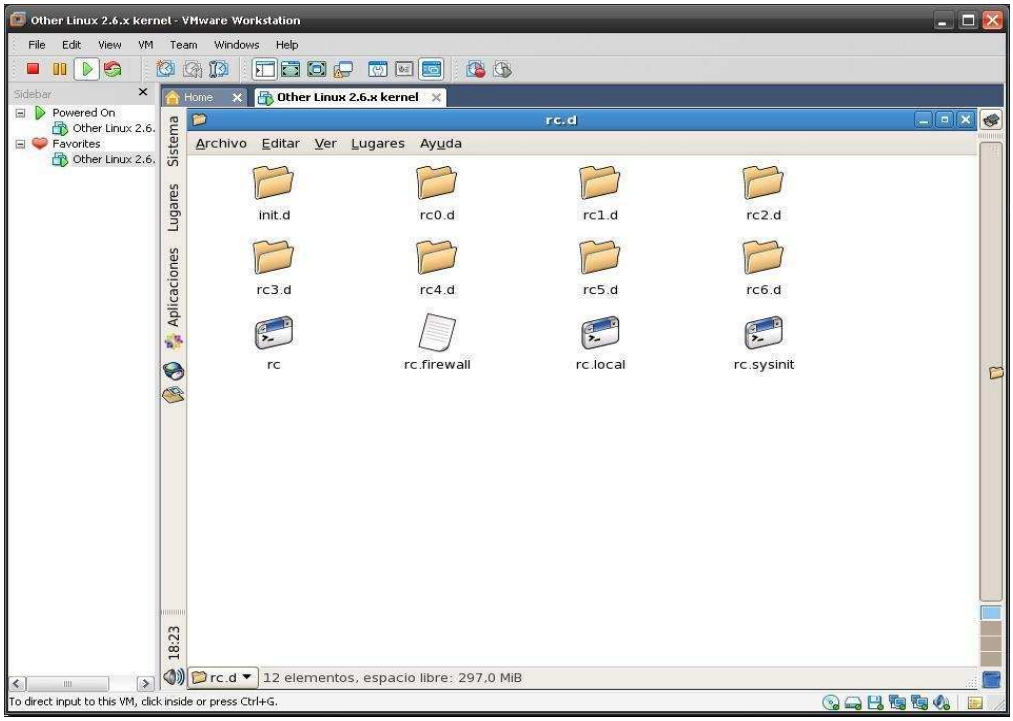

Figura 15. Creación de archivo script

2. Dentro del archivo rc.firewall se crea las reglas de Iptables para políticas de seguridad.

```
#!/bin/sh

#####################################################################

#  Scripts de Iptables para la creación del Firewall en Centos 5.2 con una  #

#  Tarjeta eth0 que comunica con una red exterior y una tarjeta eth1 que  ## comunica con la red local a la que tiene que proteger. ###################################################################
```

##Variables

 # Variables Tarjeta de red eth0 y dirección IP.

IP_EXT=“192.168.3.2”

TARJ_EXT=”eth0”

 # Variables Tarjeta de red eth1 y dirección IP.

IP_INT=”192.168.4.1

TARJ_INT=”eth1”

 # Variables Localhost.

IP_LO=”172.0.0.1”

ADAP_LO=”lo”

##Módulos de Iptables

#Carga de Módulos

/sbin/depmod –a

#Módulos a cargar

/sbin/modprobe ip_tables

/sbin/modprobe iptable_filter

/sbin/modprobe iptable_mangle

/sbin/modprobe iptable_nat

/sbin/modprobe ipt_LOG

/sbin/modprobe ipt_state

##Reglas

echo “ Aplicando Reglas del Firewall…”

#Eliminación de cualquier regla existente

iptables −F

iptables −X

iptables −Z

iptables −t nat –F

#Establecemos Política por defecto

iptables -P INPUT DROP

iptables -P OUTPUT DROP

iptables -P FORWARD DROP

iptables -t nat -P PREROUTING ACCEPT

iptables -t nat -P POSTROUTING ACCEPT

 # Acceso aplicaciones locales (localhost para conexiones locales)

iptables -A INPUT -i $ADAP_LO -j ACCEPT

iptables -A OUTPUT -o $ADAP_LO -j ACCEPT

#Establecer Nat solo a los puertos que se necesiten que salgan al exterior.

#Permite dar puerta de enlace a los host interno, en donde la puerta de enlace enruta los paquetes desde un nodo de la LAN hasta su nodo destino

iptables -A FORWARD -i $TARJ_INT -j ACCEPT

iptables -A FORWARD -o $TARJ_INT -j ACCEPT

 # Aceptamos que naveguen por el protocolo HTTP puerto 80

iptables -t nat -A POSTROUTING -o $TARJ_EXT -p tcp -m tcp --dport 80 -j

MASQUERADE

#Aceptamos que naveguen por el protocolo FTP puerto 21

iptables -t nat -A POSTROUTING -s 192.168.4.0/24 -o $TARJ_EXT -p tcp -m tcp --dport 21 -j MASQUERADE

iptables -t nat -A POSTROUTING -s 192.168.4.0/24 -o $TARJ_EXT -p tcp -m tcp --dport 1024 -j MASQUERADE

##Filtramos el acceso de la red exterior a la red local.

REDIRECCIONES

Todo lo que venga por el exterior para puerto 80 lo redirigimos

A una maquina interna de la red local.

iptables -t nat -A PREROUTING -i $TARJ_EXT -p tcp --dport 80 -j DNAT --to-destination 192.168.4.2

#Los accesos de un IP determinada a FTP se redirigen a una

#maquina interna de la red local con ese servicio.

iptables -t nat -A PREROUTING -s 192.168.1.2 -p tcp --dport 21 -j DNAT --to-destination 192.168.4.3

#Permite hacer ping a host de la red local pero no viceversa.

iptables -A OUTPUT -p icmp --icmp-type echo-request -j ACCEPT

#Permite hacer ping a la red externa pero no viceversa.

iptables -A INPUT -p icmp --icmp-type echo-reply -j ACCEPT

#regla que permite desde un host de la red externa entrar al Webmin del firewall por el puerto 10000

iptables -A INPUT -p tcp --dport 10000 -j ACCEPT

iptables -A OUTPUT -p tcp --sport 10000 -j ACCEPT

#Habilitar reenvió entre tarjetas de red del Firewall

echo 1 > /proc/sys/net/ipv4/ip_forward

Fin del script

El script escrito en el archivo rc.firewall se vería de la siguiente forma:

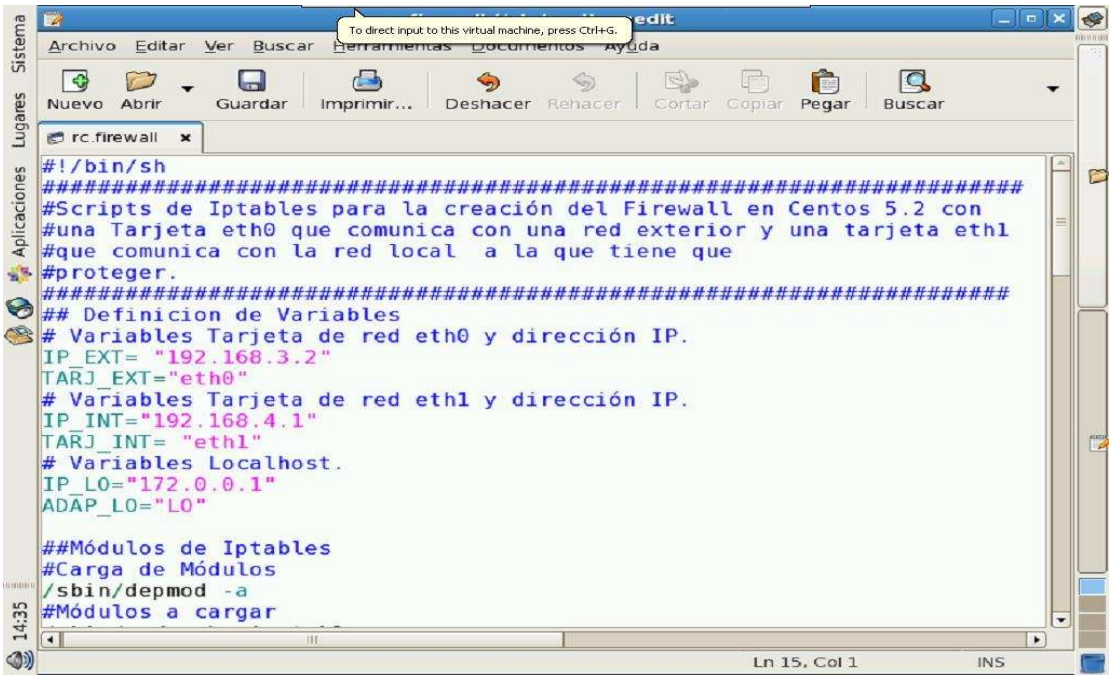

Figura 17.Script firewall

Le damos los permisos de ejecución al archivo rc.firewall desde la terminal en modo **root** la sintaxis sería la siguiente manera:

#chmod +x rc.firewall

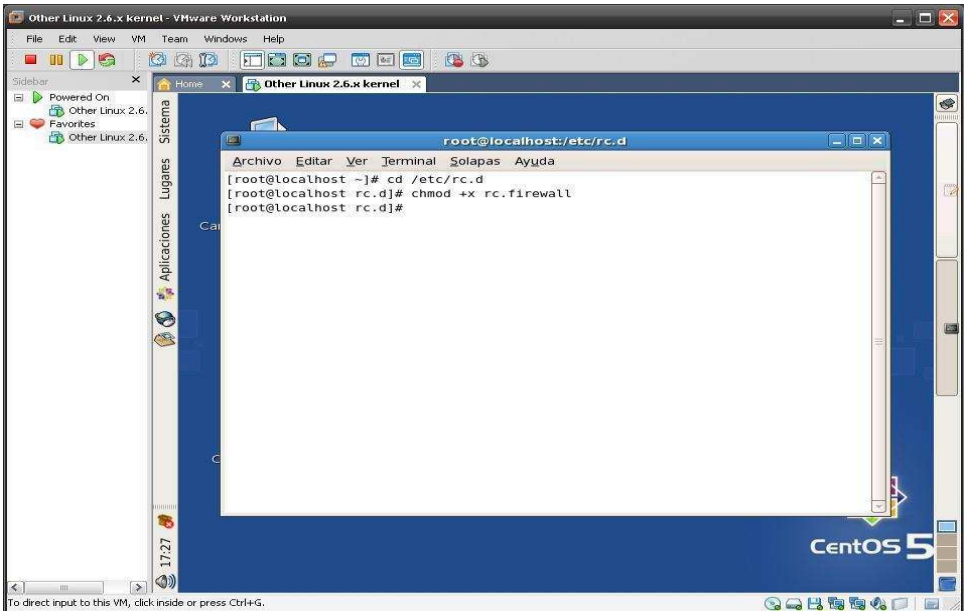

Figura 18. Permisos para archivo Script rc.firewall

Para aplicar las reglas sin necesidad de reiniciar el sistema operativo ejecutamos la línea de comando:

#./rc.firewall