ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

"SERVIDOR DE SEGURIDAD LINUX EN INTERNET"

TESINA DE SEMINARIO

Previa a la obtención del título de:

LICENCIADO EN REDES Y SISTEMAS OPERATIVOS

AUTORES:

ANA MARÍA PÓLIT ARAGUNDI
LEONARDO JAVIER REGALADO VILEMA

GUAYAQUIL – ECUADOR
2014

AGRADECIMIENTO

Agradecemos a la Escuela Superior Politécnica del Litoral por el tiempo de educación que nos ha brindado, y la enseñanza esencial que cada uno de nosotros necesitamos.

A los Ingenieros Albert Espinal, Fabián Barboza y Rayner Durango por saber impartir con paciencia, compartir sus experiencias y conocimientos; que nos han guiado en la elaboración de este proyecto.

A cada uno de nuestros padres en general por darnos el apoyo necesario y guiarnos por el camino correcto.

Los Autores

DEDICATORIA

A mis amados padres:

José Pólit y Elsy Aragundi de Pólit.

Por el esfuerzo, la paciencia, dedicatoria, abnegación y sobre todo por el inmenso amor que ellos tienen conmigo hasta el día de hoy en el largo camino de mi vida estudiantil, por haber formado a la persona en quien me he convertido hoy.

Ana María Pólit Aragundi.

A Dios, por llenar mi vida de retos, oportunidades y satisfacciones. A mis padres, hermanos y mi querida familia que han sido pilares esenciales para alcanzar este objetivo, gracias por su apoyo incondicional y mil gracias por estar siempre a mi lado.

Leonardo Regalado Vilema

TRIBUNAL DE SUSTENTACION

Ing. Fabián Barboza., MSIA

Profesor del Seminario de Graduación

Ing. Rayner Durango

Profesor delegado por la Unidad Académica

DECLARACIÓN EXPRESA

"La responsabilidad del contenido de esta Tesina de Graduación, nos corresponde exclusivamente; y el patrimonio intelectual de la misma, a la Escuela Superior Politécnica del Litoral"

(Reglamento de Graduación de la ESPOL)

_____

Ana María Pólit Aragundi

_____

Leonardo Javier Regalado Vilema

RESUMEN

Uno de los propósitos fundamentales de los sistemas informáticos, es encontrar los medios que favorezcan la calidad y rendimiento en las distintas gestiones realizadas dentro de las empresas, la utilización de estas herramientas nos proporcionan un nivel adicional de seguridad en nuestras redes.

Los sistemas de defensa perimetral y de detección de intrusos nos proporcionan la estabilidad de tener la información de la empresa protegida, permitiendo cubrir las debilidades de seguridad en la red, pero por lo general la mayoría de estos sistemas son costosos o difíciles de manejar, por lo que resultan difíciles de implementar en una empresa.

El objetivo principal del proyecto es tener una solución simple y sencilla de entender en una interfaz amigable con el usuario, utilizando herramientas open source.

El proyecto consta, además de la Introducción, de cuatro capítulos:

En el capítulo 1 se describe el Análisis de la infraestructura de TI del distrito de salud, donde se describe todo el escenario de red que tienen estructurado.

En el capítulo 2 Diseño de un sistema de Seguridad Perimetral se presenta los conceptos principales basados en el proyecto, detallando los aspectos principales del sistema de seguridad perimetral.

En el capítulo 3 se presenta especificaciones técnicas, las herramientas a utilizarse en el proyecto e imágenes de la aplicación realizada, se describe la instalación y configuración de las herramientas, el diseño y metodología utilizada en el desarrollo del proyecto.

En el capítulo 4 se incluye las políticas de seguridad a utilizarse dentro del distrito, establecimiento de las políticas a la red y utilización de la aplicación mediante las distintas opciones de reglas para mejorar la seguridad dentro del distrito de salud.

ÍNDICE GENERAL

ABREVIATURAS

1. **DHCP:** Dynamic Host Configuration Protocol (Protocolo de configuración dinámica de host).
2. **DNS :** Domain name system **(**Sistema de nombres de dominio).
3. **FTP** : File Transfer Protocol **(**Protocolo de Transferencia de Archivos).
4. **ICMP** : Internet Control Message Protocol (Protocolo de Mensajes de Control de Internet).
5. **IDS** : Intrudion Detection System (Sistema de detección de intrusos).
6. **IP :** Internet Protocol (Protocolo de Internet).
7. **LAN :** Local Area Network **(**Red de área local).
8. **SFTP :** SSH file Transfer Protocol (Protocolo de Transferencia de Archivos Seguro).
9. **SSH :** Secure Shell
10. **TCP** : Transmission Control Protocol (Protocolo de control de transmisión)
11. **TI :** Tecnologías de la información.
12. **TIC :** Tecnologías de la información y la comunicación.
13. **UDP :** User Datagram Protocol (Protocolo de Datagrama de Usuarios).
14. **WAN :** Wide Area Network (Red de área amplia).

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

La definición y el objetivo de la seguridad en redes ha sido el principal concerniente a tratar cuando una organización desea mantener la integridad, disponibilidad y privacidad de la información que se maneja, a través de procedimientos basados en políticas de seguridades las cuales permitan el control adecuado para prevenir el acceso no-autorizado de usuarios a los recursos de la red privada, y protegerse contra la exportación de información privada.

Un sistema de defensa perimetral o Firewall es un sistema que impone una política de seguridad en la organización de red privada y el Internet, este determina cuál de los servicios de red pueden acceder dentro de esta para utilizar los recursos de red pertenecientes a la organización.

Para que un firewall sea efectivo, todo tráfico de información a través del Internet deberá pasar a través del mismo donde podrá ser inspeccionada la información. El firewall podrá únicamente autorizar el paso del tráfico, y el mismo podrá ser inmune a la penetración.

Con estos mecanismos de seguridad se prevé disminuir el porcentaje de ataques a la infraestructura de TI, asegurando y simplificando la gestión de la

seguridad de la red institucional; garantizando confiabilidad de los servicios brindados por la institución y de la disponibilidad de la información para así brindar un mejor servicio a la comunidad.

CAPÍTULO 1

1. Análisis de la infraestructura de TI

1.1 Análisis de la infraestructura TI de la Institución

El Ministerio de Salud Pública mediante la Dirección Nacional de Tecnologías de la Información y Comunicación dio a conocer a las Entidades de Administración Pública decretos y acuerdos relacionados a la utilización de Software Libre en sus sistemas y equipamientos informáticos así como políticas, normas y procedimientos que optimicen la gestión y administración de las tecnologías de la información y comunicaciones, que garanticen la integridad de la información, optimización de recursos, sistematización y automatización de los procesos institucionales.

Para las entidades pertenecientes al Ministerio de salud pública existe una normativa acerca del uso de servicios de red y servicios informáticos que tienen como objetivo la regulación del uso de los recursos informáticos y servicios de red para que sean usados en

temas exclusivamente laborales según sus funciones y solo por personas autorizadas.

El Distrito de Salud No 3 Jipijapa – Puerto López administra actualmente el centro de salud de Jipijapa, centro de salud de Puerto López, subcentros, puestos de salud del Ministerio de Salud Pública. Todas las unidades previenen y atienden problemas médicos generales que afectan a niños, adultos y embarazadas de la Zona Sur de Manabí.

En el distrito de Salud No 3 Jipijapa existen aproximadamente 30 computadoras distribuidas en las diferentes áreas y departamentos, todos estos equipos cuentan actualmente con acceso al servicio de internet para poder acceder a sus cuentas de correo institucional, a páginas de gobierno como la del Ministerio de Salud pública, Ministerio de Finanzas y sus sistemas integrados de administración financiera y sistemas de nóminas, Sistema de gestión documental, entre otros.

El Centro de Salud de Puerto López cuenta actualmente con 6 computadoras y el Subcentro de Puerto Cayo con 5 ambas sedes tienen acceso a internet.

Actualmente en el Distrito de Salud se tiene un servidor Linux que hace la función de router y se usa para el control del tráfico en la red específicamente para el control de ancho de banda asignado a cada usuario, para el bloqueo de contenido web, y para monitorear el tráfico de la red, en este mismo equipo se tiene configurado el servicio DNS.

El distrito de Salud tiene una página web institucional alojada en un servidor externo, este servicio de hosting también ofrece el servicio de correo institucional a la cual acceden cada uno de las personas que laboran en la institución, tienen un servidor de transferencias de archivos.

Existe otro equipo que se lo utiliza para el control de las Cámaras IP existentes en la institución, el administrador de la red, director(a) del distrito y el administrador(a) pueden acceder vía web y desde cualquier localidad a este equipo para monitorear las cámaras IP del edificio.

1.2 Análisis de la Red LAN Y WAN

La mayoría de los equipos de comunicación del distrito de salud de Jipijapa están ubicados en el bloque administrativo y desde el cuarto de rack se distribuye el cableado al resto de los bloques, proporcionando el servicio a los distintos departamentos y oficina ubicados dentro del recinto de salud.

En los últimos meses la institución ha estado planificando cambios en su infraestructura. Lo que se busca es tener un servidor interno para los servicios de correo electrónico, DNS, FTP, WEB y poder de esta manera administrarlo localmente. A la vez se prevé contratar el servicio de internet por fibra óptica con la empresa estatal CNT para brindar un mejor servicio a los departamentos del Distrito de Salud 13D03 y del Centro de Salud Jipijapa.

También se tiene planificado dotar del servicio de internet a más unidades operativas para que están acceder a los servicios institucionales y sistemas que está implementando el Ministerio de Salud Pública.

1.2.1 Esquema de conexión actual de la red de área local del Distrito de Salud 13D03 y del Centro de Salud Jipijapa

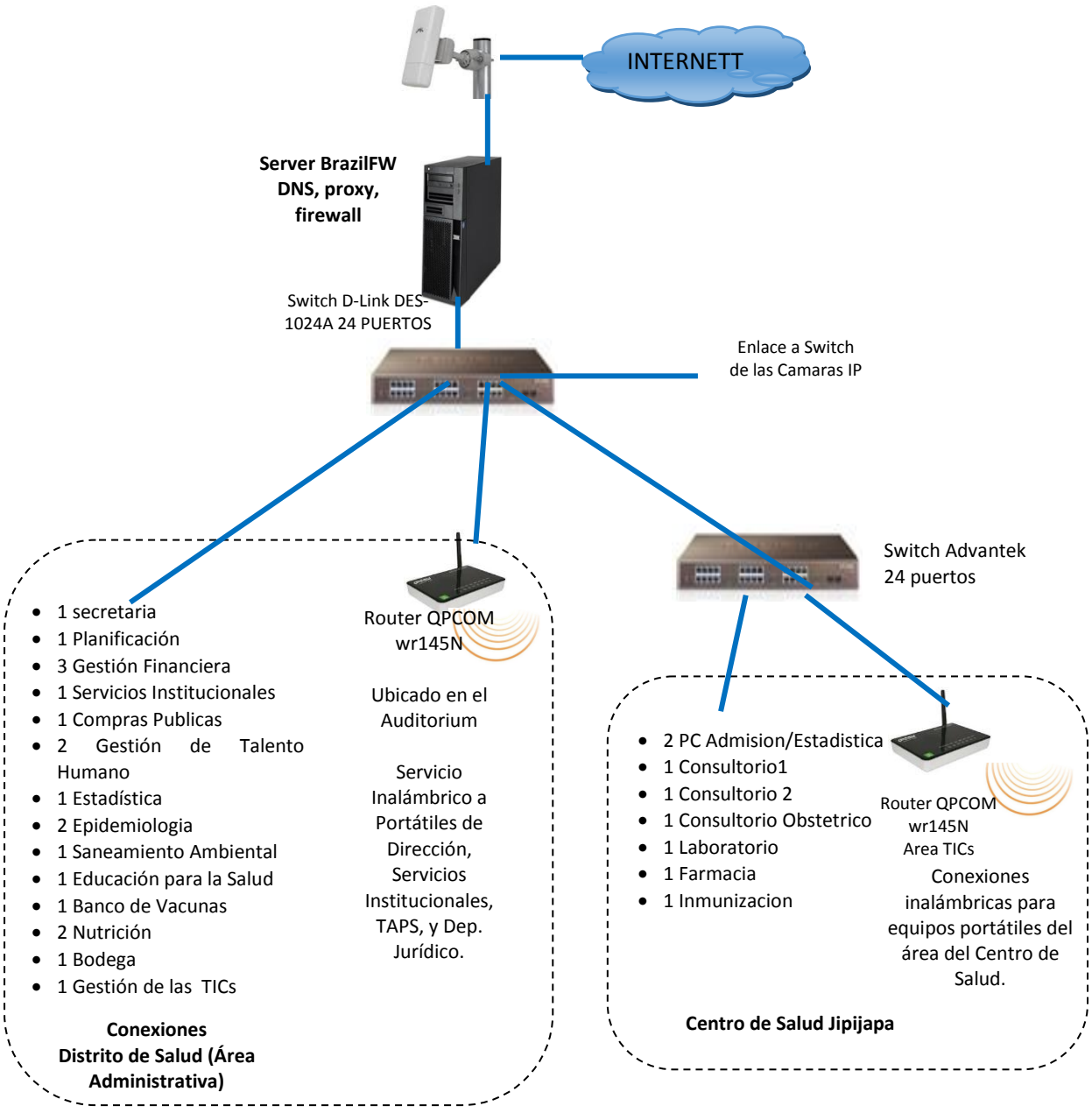

Figura 1. 1 Esquema de la red LAN del Distrito de Salud y Centro de Salud Jipijapa

Este servicio se encuentra contratado con un proveedor local (FLASNETH) y se dispone de 2 MB de ancho de banda con una conexión compartida 2:1. Con la misma conexión se da servicio a los equipos del Distrito de Salud y del Centro de Salud Jipijapa, pues ambos comparten la misma edificación.

1.2.2 Esquema de conexiones de las cámaras

Figura 1. 2 Esquema de conexión de cámaras

Las cámaras están conectadas a un switch independiente que se enlaza en horas de la tarde al switch principal de la institución, esto

con el objetivo de poder ser accedidas desde cualquier lugar por parte del director, y personal del área de las TICs.

1.2.3 Esquema de conexiones a internet existente en Puerto López

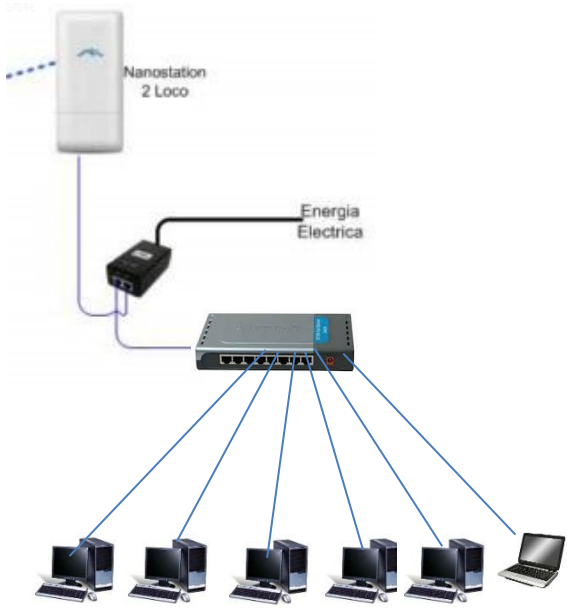

Figura 1. 3 Esquema de conexiones Puerto López

La unidad operativa Puerto López cuenta con el servicio de internet con un proveedor local ROYMIL.NET. Se dispone de 2 MB de ancho de banda con una conexión compartida 8:1.

1.2.4 Esquema de la conexión a internet existente en Puerto Cayo

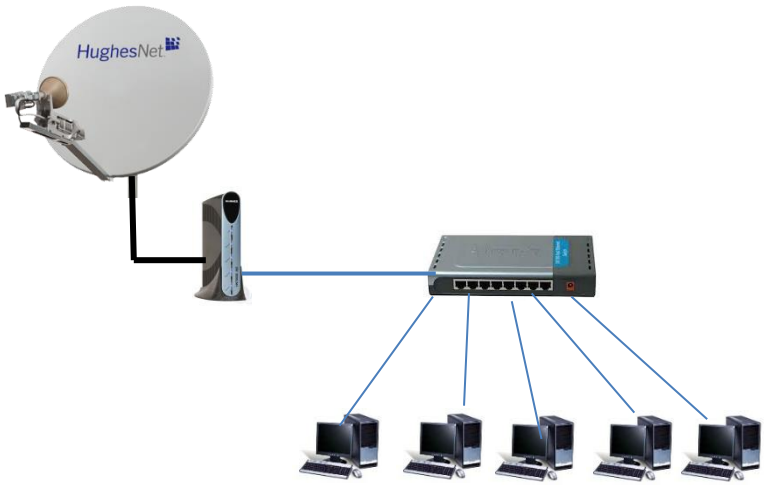

Figura 1. 4 Esquema de conexiones Puerto Cayo

La unidad operativa Puerto Cayo cuenta con el servicio de internet Satelital de CNT. Se dispone de 256 kbps de ancho de banda con una conexión compartida 2:1.

1.2.5 Esquema de conexión WAN del Distrito de Salud

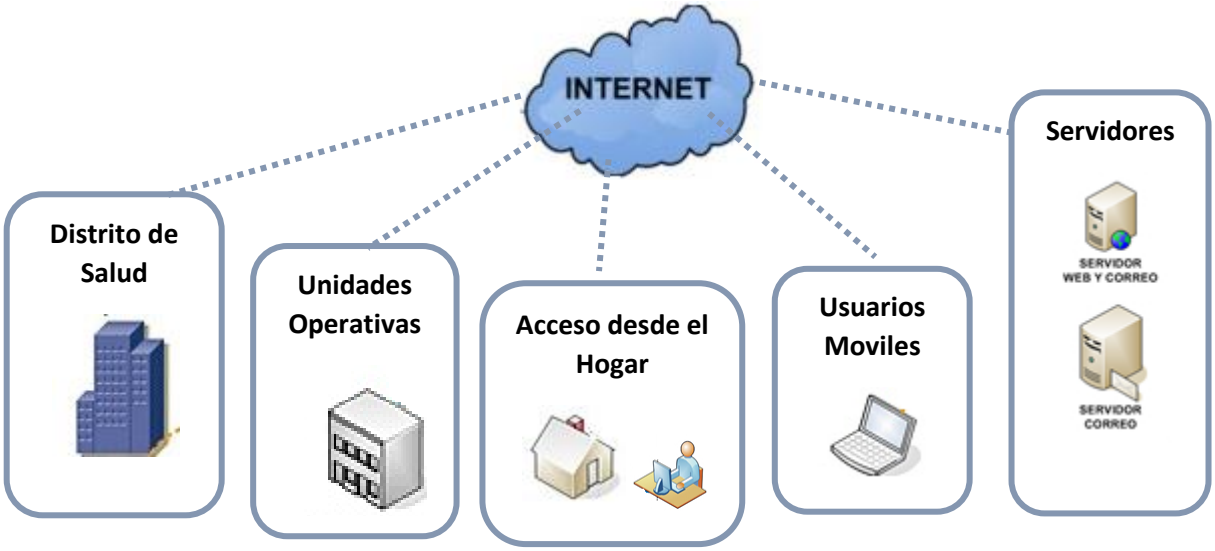

Figura 1. 5 Esquema de conexión WAN

La infraestructura WAN del Distrito de Salud 13D03 está compuesta por enlaces a internet en el caso del Distrito de Salud y El Centro de Salud Jipijapa se dispone de 2 MB de ancho de banda y en el caso de las Unidades Operativas de Puerto López y Puerto Cayo 2 Mb y 256 kbps respectivamente

Cabe indicar que por el momento no se tiene enlaces arrendados para el acceso desde las unidades operativas hacia la sucursal, pero con la restructuración en coordinación con la empresa CNT se quiere disponer de estos tipos de enlaces principalmente con estas 2 unidades operativas.

1.3 Análisis de riesgos de TI

La seguridad debe ser una de las principales prioridades cuando la red privada de la empresa se conecta a Internet. Para obtener resultados y un nivel de protección adecuado, la empresa necesitará de políticas de seguridad estrictas para evitar que usuarios sin autorización tengan acceso a los recursos de la red privada de nuestra institución y protegerla contra la exportación sin autorización de la información confidencial del distrito de salud, los riesgos más importantes encontrados dentro del distrito son:

- No existe el uso de usuarios y contraseñas dentro de las estaciones de trabajo dificultando el trabajo en las auditorias.

- No existe ningún tipo de restricción o regla en las estaciones de trabajo y es muy fácil que toda la información almacenada en los servidores puedan ser manipuladas con facilidad.

- Las autoridades quieren que los usuarios solo utilicen el servicio de internet para consultar páginas relacionadas con el ministerio de salud y el gobierno.

- La infraestructura tecnológica y de comunicaciones, serán responsabilidad de cada usuario en las distintas estaciones de trabajo.

De esta manera el enfoque de seguridad que hay el Distrito comenzó a partir de una decisión estratégica dónde la organización entiende de manera consciente cuáles son los riesgos más importantes, haciendo un balance siempre en proteger lo vital y hacer lo mejor posible por lo que no es vital. La estrategia de seguridad adecuada se encargará de proteger los procesos que son parte esencial de la operación del negocio y hará su mejor esfuerzo por proteger la red interna y así administrar el acceso de tus empleados a sitios específicos de la red y proteger la información sensible.

CAPITULO 2

2. Diseño de un sistema de seguridad perimetral

2.1 Diseño de la infraestructura de TI propuesta

Considerando los planes futuros que tiene el Ministerio de Salud para los Distritos de Salud, las futuras aplicaciones que se quiere implementar en cada una de las Unidades Operativas administradas por los Distritos y los planes de mejora en la infraestructura de TI del Distrito de Salud 13D03 se ha considerado propuesto la siguiente topología.

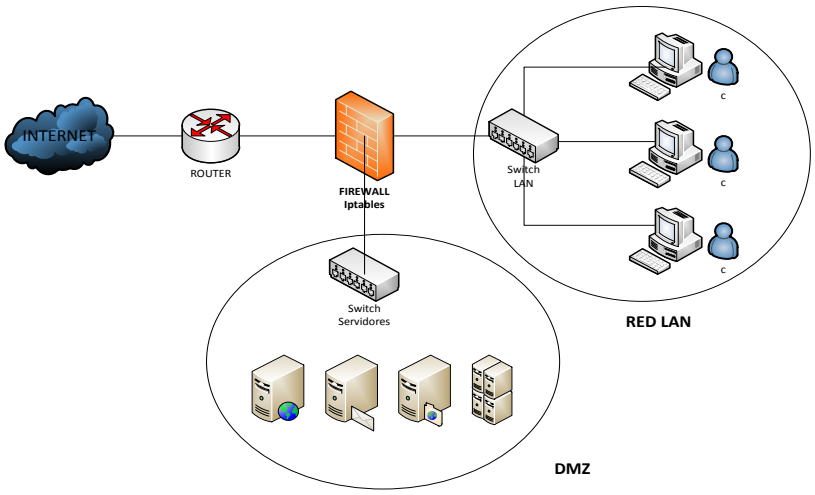

Figura 2. 1 Diseño de Infraestructura de TI propuesta

Como se puede ver en la figura 2.1, en el diseño de la Infraestructura de TI propuesta. Lo ideal es tener 2 áreas bien definidas: la red LAN definida en un segmento de red diferente a la de los servidores los mismos que por motivos de seguridad se ha implementado en una DMZ. Como punto central el Firewall Linux desde donde se controlará el tráfico desde la red LAN hacia los servidores y hacia la red externa así como el tráfico que venga desde la red externa hacía los servidores.

Recomendable que el equipo que hará las funciones de firewall tenga 3 tarjetas de red para controlar por separado cada segmento de la red.

2.2 Seguridad perimetral

El firewall o también llamado cortafuegos se utilizan con frecuencia para evitar que los usuarios de Internet no autorizados tengan acceso a redes privadas conectadas a Internet.

Los firewall pueden ser implementados tanto en hardware o en software, o realizando una combinación de ambos. La existencia de un firewall reduce considerablemente las probabilidades de ataques externos a los sistemas corporativos y redes internas, además puede

servir para evitar que los propios usuarios internos comprometan la seguridad de la red al enviar información sensible como contraseñas no que no estén cifradas o datos sensitivos para la organización hacia el mundo externo.

Si el Firewall "observa" alguna actividad sospechosa: que alguien de fuera esté intentando acceder a nuestro Pc o que algún programa espía trate de enviar información sin consentimiento, el Firewall nos advertirá con una alarma en el sistema.

Para entender el funcionamiento de este sistema, debes saber que el ordenador dispone de varias puertas de salida y entrada cuando se conecta a Internet. Éstas se llaman puertos y cada servicio que utilizas se sirve de un puerto diferente: Los navegadores de internet necesitan el puerto 80, los programas FTP el 21, etc... En general tenemos todos los puertos abiertos.

En Linux el software de filtrado de paquetes es denominado IP-Tables. Existe en Linux las versiones de kernel 2.4 en adelante, las versiones que se utilizaban anteriormente para los filtrados de paquetes son:

- En los Kernel de versiones 2.1.X el paquete de filtrado es el IP-FWADM.
- En los Kernel de versiones 2.2.X el paquete de filtrado es el IP-CHAINS.
- En los Kernel de versiones 2.4.X el paquete de filtrado es el IP-TABLES.

IPtables es un sistema de firewall vinculado al kernel de linux que se ha extendido a partir del kernel 2.4 de este sistema operativo. Al igual que el anterior sistema ipchains, iptables está integrado con el kernel y es parte del sistema operativo.

Para utilizar iptables lo que se hace es aplicar reglas mediante la ejecución del comando iptables, con el que añadimos, borramos, o creamos reglas.

2.3 Diseño de las opciones de seguridad a considerar en la aplicación

En el diseño o la configuración de un firewall existen tres decisiones las cuales deben considerarse al momento de instalar un firewall.

La primera de ellas se basa en las referencias de políticas de seguridad de la organización propietaria del firewall evidentemente, la configuración y el nivel de seguridad dependerá de las necesidades de cada empresa ya sea para bloquear todo el tráfico externo hacia el dominio de su propiedad o donde sólo se intente evitar que los usuarios internos utilicen el internet de forma inadecuada, bloqueando todos los servicios de salida al exterior excepto el correo electrónico.

La segunda decisión de diseño a tener en cuenta es el nivel de monitorización que debamos realizar, redundancia y control deseado en la organización; una vez definida la política a seguir, hay que definir cómo implementarla en el firewall indicando básicamente qué se va a permitir y qué se va a denegar.

La tercera decisión a tomar a la hora de instalar un sistema de detección de intrusos es la economía de la empresa: el valor estimado al sistema dependerá de lo que deseemos proteger, debemos gastar más o menos dinero, o no gastar nada.

Un firewall puede no generar gastos extras para la organización, o suponer un gasto millonario, seguramente un departamento con pocos equipos en su interior utilizando el sistema Operativo Linux, sin

gastarse nada en él, solo el trabajo de programarlo, pero esta solución no va a funcionar cuando el sistema a proteger sea una red de tamaño considerable; en este caso se pueden utilizar sistemas propietarios, que suelen ser caros, o aprovechar los routers de salida de la red, algo más barato pero que requiere más tiempo de configuración.

De cualquier forma, no es recomendable a la hora de evaluar el dinero a invertir en el firewall fijarse sólo en el coste de la instalación y puesta a punto, sino también en el de su mantenimiento.

2.4 Diseño de las opciones de seguridad a considerar en la aplicación.

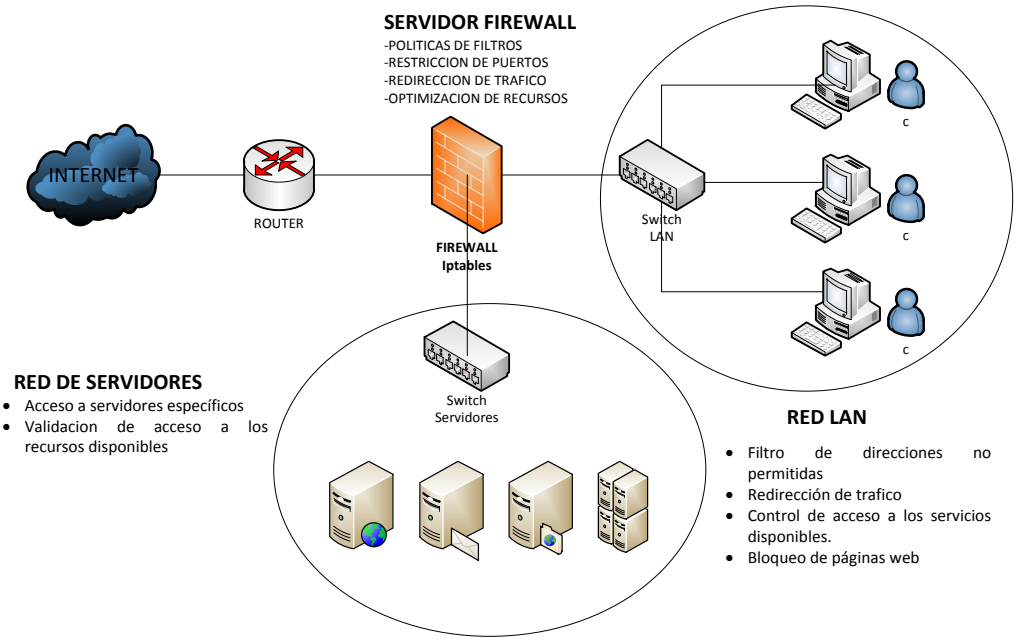

Figura 2. 2 Consideraciones de seguridad para el tráfico de la Red Institucional

Como se puede observar la figura 2.2 existen algunas consideraciones respecto al tráfico permitido desde la Red LAN hacia el exterior y hacia la zona de los servidores. De igual manera en el diseño del firewall se considera el bloqueo o acceso de tráfico que viene desde la red WAN hacia la red institucional.

Primeramente debemos entender que son las reglas a utilizarse en la aplicación del proyecto, tenemos tres tipos de reglas las cuales son

FILTER, NAT, MANGLE es una de las que poco se usa por su complejidad.

- Las reglas tipo **FILTER** son reglas básicas que permiten denegar o permitir tráfico a nuestra red y define en qué sentido va a aplicar la regla ya sea tráfico de Entrada o de salida.

- Las reglas tipo **NAT** se utilizan para manipular paquetes, para alterar las direcciones o puertos que traen en el origen o destino, antes o después de que se decidió la ruta que va a seguir.

- Las reglas tipo **MANGLE** se utilizan para alterar las opciones a seguir de un paquete en específico. Es donde se encuentran todas las cadenas que pueden contener reglas que hagan filtrado de paquetes acepten, rechacen o denieguen paquetes.

Las reglas van en un orden específico que le indica al kernel qué hacer cuando encuentra un paquete con las características que están indicadas en la misma regla. Las reglas están contenidas dentro de cadenas y las cadenas están dentro de las tablas.

Es así que el o los paquetes pasarán por cada tabla, primero la tabla FILTER, luego, NAT y finalmente por la regla MANGLE. En cada una pasa por las cadenas que tenga sentido y buscara la regla que coincida. En caso de no coincidir con ninguna se aplicara la decisión por default que se defina a la cadena, entonces la política para toda la cadena default bien podría ser. ACCEPT que se acepte y deje pasar el paquete, DENY esto significa que el paquete no pase pero que envié un mensaje o alerta y finalmente DROP, que no pase y que no se le avise a nadie.

Es así que las opciones a considerarse son cuatro acciones principales en la aplicación:

- Listar los servicios disponibles en el servidor
- Listar las reglas iptables
- Administrar los servicios iptables
- Administrar las reglas iptables.

En la primera opción: “Listar los servicios disponibles en el servidor”, tendremos una tabla completa especificando el nombre. El protocolo, el estado y su respectivo puerto.

Con esta, muestra completa de servicios, podremos trabajar y así conocer tipo de información están trabajando en el distrito.

```
+-------------------------------------------------------+
|  NOMBRE  |  ESTADO  |  PROTOCOLO -> DIRECCION:PUERTO   |
+-------------------------------------------------------+
|   smb    | RUNNING  | tcp ->
|          |          |   IPv6_ALL:445
|          |          |   IPv6_ALL:139
|          |          |   IPv4_ALL:445
|          |          |   IPv4_ALL:139
|  named   | RUNNING  | tcp ->
|          |          |   IPv6_Localhost:953
|          |          |   IPv6_Localhost:53
|          |          |   IPv4_Localhost:953
|          |          |   IPv4_Localhost:53
|          |          |   192.168.12.1:53
|          |          | udp ->
|          |          |   IPv6_Localhost:53
|          |          |   IPv4_Localhost:53
|          |          |   192.168.12.1:53
|  squid   | RUNNING  | tcp ->
|          |          |   IPv6_ALL:8080
|          |          | udp ->
|          |          |   IPv6_ALL:42779
|          |          |   IPv4_ALL:53725
| sendmail | RUNNING  | tcp ->
|          |          |   IPv4_ALL:25
```

Figura 2. 3 Lista de servicios habilitados en el servidor

En la segunda opción: “Listar las reglas iptables”. Tendremos una vista de todas las reglas divididas por las tres reglas que se utilizan en iptables las reglas de Iptables tipo Filter, Mangle y NAT. Cada una subdivida con sus respectivas opciones de Input. Output y forward respectivamente a la que se aplique.

En la tercera opción: “Administrar los servicios iptables”. Tendremos las opciones de detener el servicio iptables, restaurar el servicio iptables, iniciar el servicio iptables, listar las reglas y borrar todas las reglas habilitadas.

En la cuarta opción: “Administrar las reglas iptables”, dentro de esta opción está el corazón de la aplicación, es aquí donde van a ser creadas las reglas en sus divisiones de Filter, MANGLE y NAT cada una con sus subdivisiones de regla en cada tipo.

2.4.1 Tipos de reglas o cadenas predefinidas

Como se menciono anteriormente hay tres tablas ya incorporadas, cada una de las cuales contiene ciertas cadenas predefinidas. El administrador puede crear y eliminar cadenas definidas por usuarios dentro de cualquier tabla.

A continuación se presenta un listado de las cadenas predefinidas en cada una de las tablas.

CADENA	PAQUETES ANALIZADOS	TABLA DONDE SE UTILIZA
INPUT	Paquetes entrantes que están destinados a la PC donde está operando el iptables.	FILTER, MANGLE
OUTPUT	Paquetes en el monento de ser recibidos por la estación donde está operando iptables. Esta cadea analiza paquetes propios o enrutados.	FILTER, MANGLE, NAT
FORWARD	Paquetes que son enrutados por la PC donde está operando iptables.	FILTER, MANGLE
PREROUTING	Paquetes en el momento de ser recibidos por la estación donde está operando el iptables. Esta cadena analiza paquetes propios y enrutados	NAT, MANGLE
POSTROUTING	Paquetes en el momento de ser enviados por la estación donde está operando el iptables. Esta cadena analiza los paquetes propios y enrutados.	NAT, MANGLE

Tabla 2. 1 Reglas o cadenas predefinidas

2.4.2 Especificación de las reglas

La mayoría de las formas de comandos de iptables requieren que se les indiquen una especificación de reglas, que es usada para comparar un subconjunto particular del tráfico de paquetes de red procesados por una cadena. La especificación de regla incluye también un destino que especifica qué hacer con paquetes que son comparados por la regla. Las siguientes opciones se usan

(frecuentemente combinadas unas con otras) para crear especificaciones de reglas.

-p [protocolo]	Protocolo al que pertenece el paquete.
-s [origen]	Dirección de origen del paquete, puede ser un nombre de host, una dirección IP normal, o una dirección de red (con máscara, de forma dirección/máscara).
-d [destino]	Al igual que el anterior, puede ser un nombre de host, dirección de red o dirección IP singular.
-i [interfaz-entrada]	Especificación del interfaz por el que se recibe el paquete.
-o [interfaz-salida]	Interfaz por el que se va a enviar el paquete.
[!] -f	Especifica que la regla se refiere al segundo y siguientes fragmentos de un paquete fragmentado. Si se antepone !, se refiere sólo al primer paquete, o a los paquetes no fragmentados. Y además, uno que nos permitirá elegir qué haremos con el paquete:
-j [target]	Nos permite elegir el target al que se debe enviar ese paquete, esto es, la acción a llevar a cabo con él.
-sport	Permite especificar el puerto de origen. Para especificar un rango valido de puertos, separe ambos números de rango con dos puntos (:)
-dport	Permite especificar el puerto de destino. Para especificar un rango valido de puertos, separe ambos números de rango con dos puntos (:)

Tabla 2. 2 Opciones comunes para creación de reglas

CAPITULO 3

3. Implementación del sistema de seguridad perimetral

3.1 Requerimiento de hardware mínimo para implementar el sistema de seguridad perimetral

Los cortafuegos de filtrado no son exigentes en recursos de hardware, son tan sencillos como los enrutadores simples. La implementación del sistema se lo realizo tomando como base Centos 6.3 que es una distribución Linux de clase empresarial, una bifurcación a nivel binario de la distribución Linux Red Hat Enterprise Linux RHEL, compilado por voluntarios a partir del código fuente liberado por Red Hat.

Como el firewall que se va a ocupar para la red institucional es Iptables, una herramienta que nos permite configurar las reglas de filtrado de paquetes del kernel de Linux, los requerimientos de hardware mínimos recomendados para operar se detallan a continuación.

Sin entorno de escritorio:

- Memoria RAM: 64 MB(mínimo)
- Espacio de Disco duro: 1024(mínimo) – 2 GB (recomendado)
- Procesador: arquitecturas i386, x86-64

Con entorno de escritorio:

- Memoria RAM: 2 GB (mínimo)
- Espacio de Disco duro: 20 GB(mínimo) – 40 GB (recomendado)
- Procesador: arquitecturas i386, x86-64

Centos soporta casi las mismas arquitecturas que Red Hat Enterprise Linux, Intel x86-compatible (32 bits) (Intel Pentium/AMD 64).

Para satisfacer las necesidades el servidor va a estar ubicado entre el Internet y los servidores de la organización; Este servidor va a tener como mínimo 2 interfaz de red 10/100/1000 Mbps una que va a estar dando la cara al internet y la otra para conectarse a la red interna de servidores y equipos.

3.2 Configuración del hardware para implementar el firewall

Para el correcto funcionamiento del firewall se procedió a configurar las tarjetas de red y las direcciones IP la meta es proveer dos conexiones de red. Una es sobre internet y otra es sobre la red LAN.

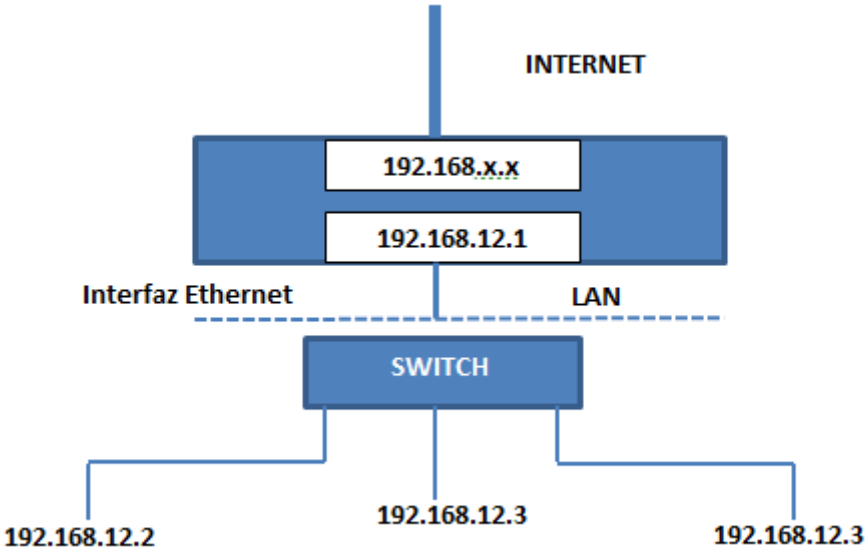

Figura 3. 1 Esquema de configuración de tarjetas de red

Debe tener una dirección IP válida ante Internet. Esta dirección puede ser asignada permanentemente al ordenador por un ISP mediante un enlace dedicado o puede ser dinámica asignada a través de una conexión conmutada. En nuestro caso será una dirección IP estática asignada permanentemente al ordenador.

Para las pruebas al servidor se configurará la dirección IP de la WAN la dirección 192.168.x.x/24 y como dirección IP de la LAN la red

192.168.12.1/24. A las maquinas que se usarán para las pruebas se las configurara en este segmento de red LAN.

3.3 Instalación de aplicaciones necesarias para el funcionamiento del sistema

3.3.1 Instalación de iptables

El firewall que se va a ocupar para la red institucional es Iptables, una herramienta que nos permite configurar las reglas de filtrado de paquetes del kernel de Linux, permitiéndonos crear firewall de acuerdo a nuestras necesidades. Su funcionamiento es simple, ya que un paquete debe cumplir reglas específicas, además se especifica para esa regla una acción o target.

Esta herramienta viene instalada por default en la distribución de Centos 6.3, pero en el caso de no tenerla instalada se necesita realizar lo siguiente para instalar o actualizar el equipamiento lógico necesario:

Yum –y install iptables

Hecho esto verificamos la versión de la herramienta instalada

```
[root@espol Desktop]# iptables --version
iptables v1.4.7
[root@espol Desktop]#
```

Figura 3. 2 Versión de iptables instalada

3.3.2 Instalación de dialog

El lenguaje de scripting puede ser una excelente herramienta para la administración de sistemas. Brinda la flexibilidad propia del lenguaje con estas características y a su vez es muy potente.

Una de las herramientas más utilizadas por los administradores de sistemas tipo UNIX es el propio interprete de comandos para generar Shell script, siguiendo con la filosofía de usar pequeñas herramientas simples que hacen cosas puntuales.

En este mundo de solo texto, se tiene el problema de que la interface de usuario no es muy cómoda que digamos. Por suerte existen formas de desarrollar con Bash o sh y tener una mejor interface con el uso de dialog o Xdialog(el primero para entorno de caracteres y el segundo para X).

Dialog, cdialog y X-Dialog permiten el uso de ventanas y “cajas” para hacer la experiencia de interactuar con un programa desarrollado en Shell script más amena. Su estructura es muy simple de comprender y cuenta con una serie de parámetros que indicaran, al ser llamado el programa dialog desde el script, que es lo que tiene que mostrar.

Para el correcto funcionamiento de la aplicación que permitirá configurar el firewall se necesita tener instalado Dialog. Para lo cual se deberá ejecutar lo siguiente:

Yum –y install dialog

Hecho esto verificamos la versión del comando dialog instalado.

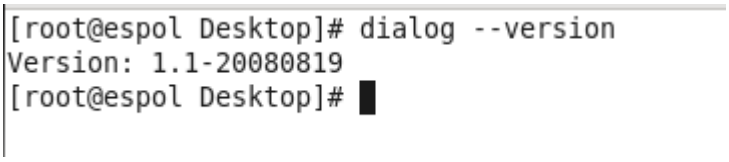

Figura 3. 3 Versión de dialog instalado

3.4 Instalación y configuración de aplicaciones específicas para el firewall.

Para la configuración y administración de las reglas de firewall se diseñó un script el mismo que a través de sus diferentes opciones

permite administrar el servicio y crear reglas específicas de acuerdo al tráfico entrante y saliente que se quiera permitir o bloquear.

Para la ejecución del script se deberá tener privilegios de administrador. Para el funcionamiento del script el requisito necesario es la instalación del aplicativo dialog, como se explicó en líneas anteriores este permitirá el uso de ventanas de dialogo para una mejor interacción con el usuario final.

A continuación se detalla el funcionamiento del script para la configuración del firewall.

3.4.1 Procedimiento para la administración y configuración del firewall

Para la ejecución del script se deberá ejecutar desde la línea de comandos lo siguiente

./firewall.sh

Después de ejecutar la instrucción anterior se mostrará el menú principal de la aplicación:

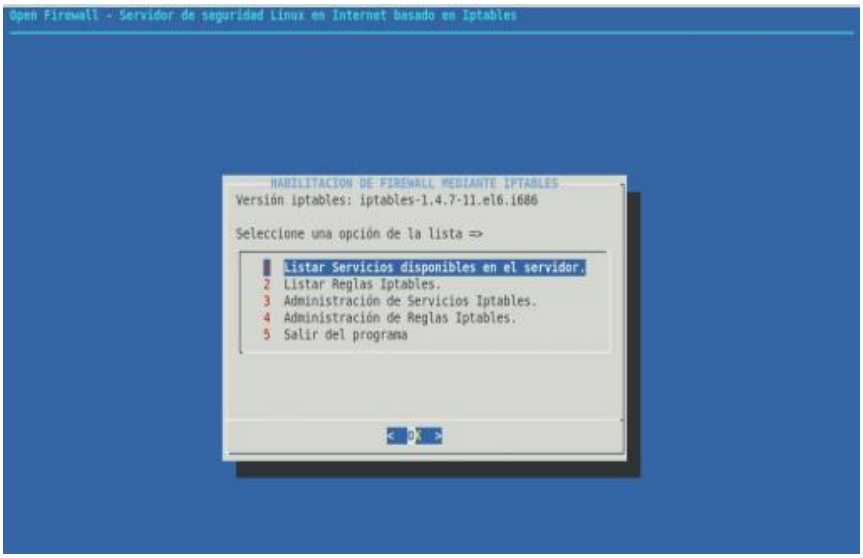

Figura 3. 4 Menú principal de la aplicación

En la imagen se muestra un menú con 5 opciones:

- “Listar servicios disponibles en el servidor”: mostrara por pantalla un reporte de los servicios que se tienen actualmente disponibles en el servidor.

- “Listar reglas IPtables”: mediante un menú de opciones le permitirá visualizar por pantalla las diferentes reglas de firewall que han sido configuradas

- “Administración de Servicios Iptables”: Esta opción sirve principalmente para realizar como detener y reanudar el servicio, listar las reglas habilitadas, eliminación de las reglas habilitadas.

- “Administración de reglas iptables”: mediante esta opción se podrá crear y eliminar reglas para el firewall.

- “Salir del programa”: permite finalizar la ejecución del script. Cuando seleccione esta opción se visualizar el siguiente mensaje.

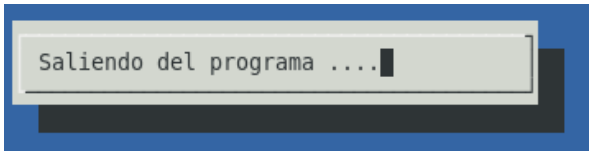

Figura 3. 5 Mensaje de salida de la aplicación

3.4.1.1 Listar servicios disponibles en el servidor

Mediante esta opción se podrá visualizar por pantalla el nombre del servicio, su estado, el protocolo, la dirección y el puerto. Esta información será útil para configurar las reglas del firewall.

Al seleccionar esta opción del menú principal de la aplicación se mostrara la siguiente ventana con la información acerca del estado de los servicios disponibles en el servidor.

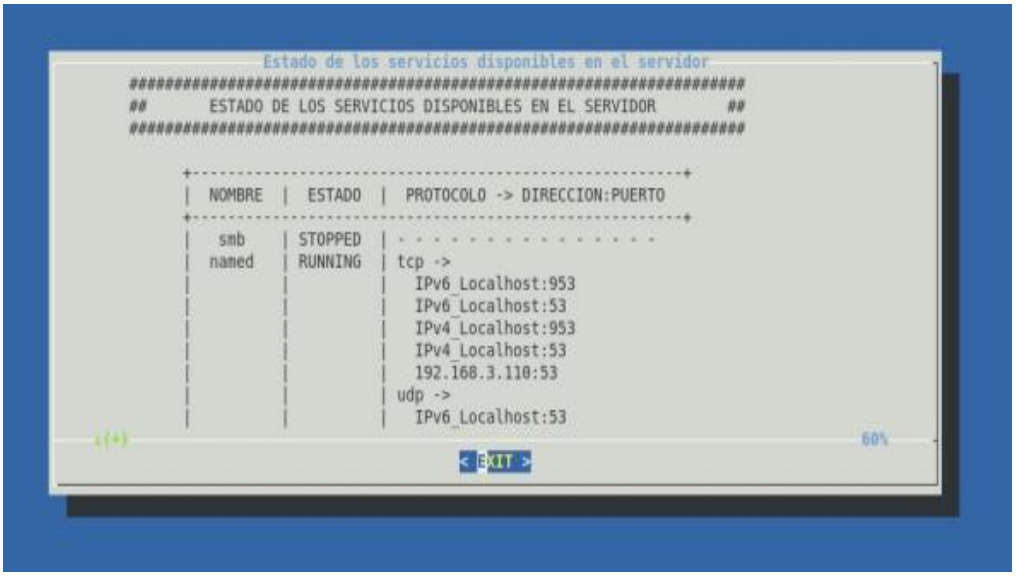

Figura 3. 6 Informe de estado de los servicios disponibles

Si en la ventana no se visualiza toda la información del informe, como la figura anterior que solo muestra el 60%. Se podrá visualizar el resto de la información para lo cual se hará uso de las teclas direccionales.

Para regresar al menú principal de la aplicación se tendrá que seleccionar la opción **Exit**.

3.4.1.2 Listar reglas Iptables

Esta opción nos permite visualizar las reglas configuradas para iptables. Al seleccionar se visualizara un submenú con las siguientes opciones:

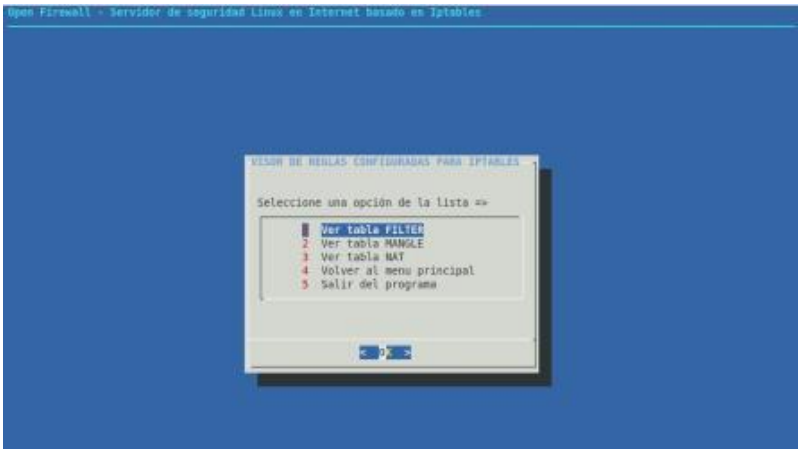

Figura 3. 7 Menú listar reglas Iptables

Dependiendo de la información que quiera visualizar se selecciona el tipo de tabla: FILTER, MANGLE, NAT.

Para retornar al menú principal de la aplicación se deberá seleccionar la opción 4. En caso de que se desee salir de la aplicación el usuario tendrá que seleccionar la opción 5 “Salir del programa”.

3.4.1.2.1 Vista de reglas de la tabla FILTER

La tabla FILTER es la responsable del filtrado(es decir, de bloquear o permitir que un paquete continúe su camino). Mediante este menú se podrá mostrar todas las cadenas definidas en la tabla FILTER o seleccionar las reglas definidas en una cadena especifica: INPUT, OUTPUT o FORWARD.

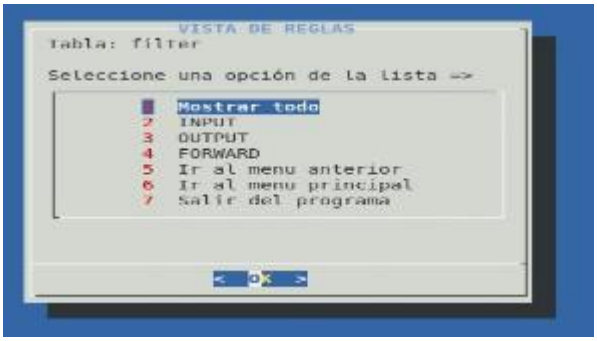

Figura 3. 8 Submenú vista de reglas de tabla FILTER

En caso de que se desee seleccionar otro tipo de tabla, podrá retornar al menú anterior seleccionando la opción 5.

Si lo que desea es retornar al menú principal lo podrá hacer mediante la opción 6. Si no desea continuar ejecutando la aplicación entonces podrá seleccionar la opción 7 “Salir del programa”.

A continuación se detallará la información que muestra cada uno de los informes que se muestra en el menú que se muestra en la figura anterior.

- Si selecciona “**Mostrar todo”** se visualizará por pantalla un listado de todas las reglas configuradas en la tabla FILTER.

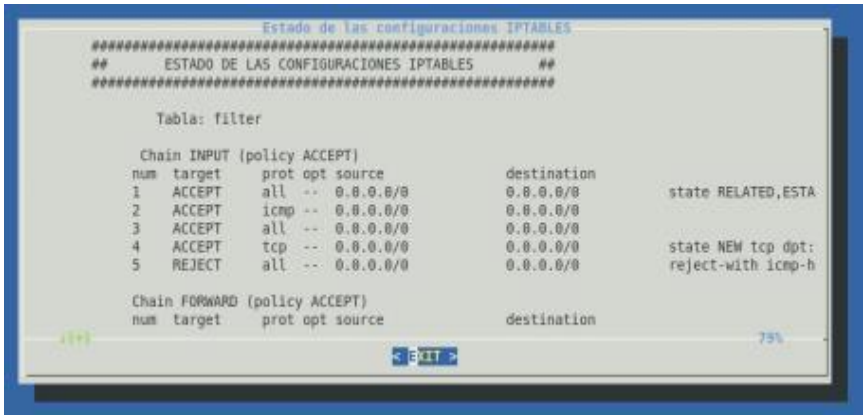

Figura 3. 9 Informe de reglas definidas en tabla FILTER

Si en la ventana no se visualiza toda la información del informe, como la figura anterior que solo muestra el 79%. Se podrá visualizar el resto de la información para lo cual se hará uso de las teclas direccionales.

Para regresar al menú principal de la aplicación se tendrá que seleccionar la opción “Exit”.

- Si no quiere visualizar todas las reglas definidas en la tabla FILTER sino, solo las cadenas INPUT, OUTPUT o las cadenas FORWARD; entonces deberá seleccionar una de estas opciones para visualizar el contenido específico. Por ejemplo si quiero seleccionar solo las reglas de tipo INPUT se mostrará el siguiente informe.

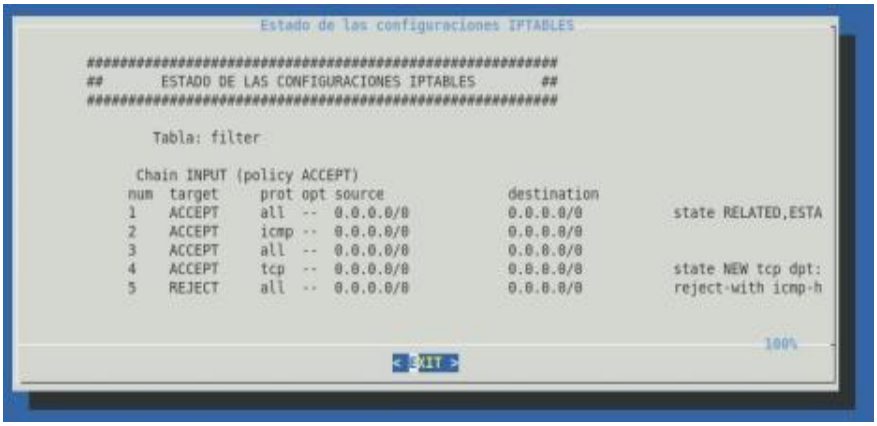

Figura 3. 10 Informe de reglas de tipo INPUT tabla FILTER

Observe en el gráfico que al emitir el informe se mostrará la tabla seleccionada "Tabla: filter" y el tipo de cadena "Chain INPUT".

Se podrá usar las teclas direccionales para visualizar el resto de información en caso de que exista.

Para cerrar esta ventana y retornar al menú anterior se deberá seleccionar "EXIT".

En caso de que no existan cadenas definidas en la tabla filter se desplegara por pantalla el siguiente mensaje.

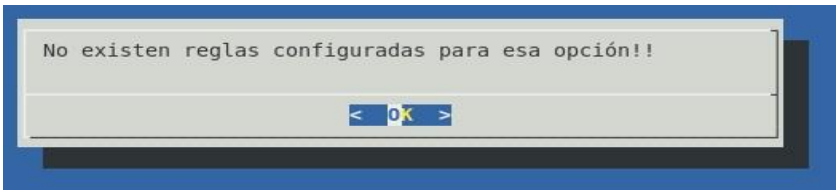

Figura 3. 11 Mensaje advertencia tabla seleccionada vacía

3.4.1.3 Administración de servicios Iptables

Esta opción nos muestra un submenú con opciones básicas para administrar el servicio Iptables. Al seleccionar se visualizara un submenú con las siguientes opciones:

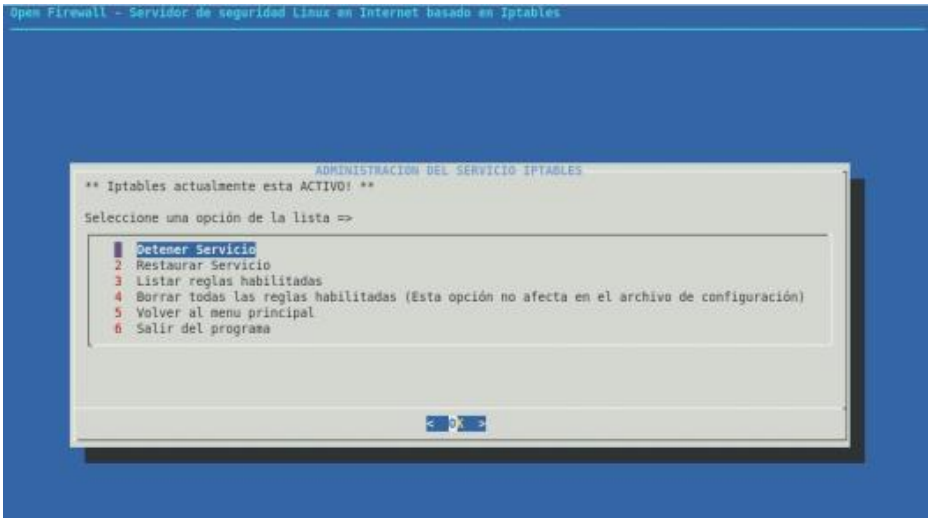

Figura 3. 12 Submenú Administración del Servicio Iptables

En este grafico se puede ver las opciones disponibles en este submenú, también se puede visualizar el estado actual del servicio "** Iptables actualmente está ACTIVO! **". A continuación se da una breve descripción de lo que realiza cada una de las opciones.

- Al seleccionar la opción “Detener Servicio”, el servicio iptables pasara a un estado INACTIVO. Se mostrara el siguiente mensaje indicando el éxito de la acción realizada.

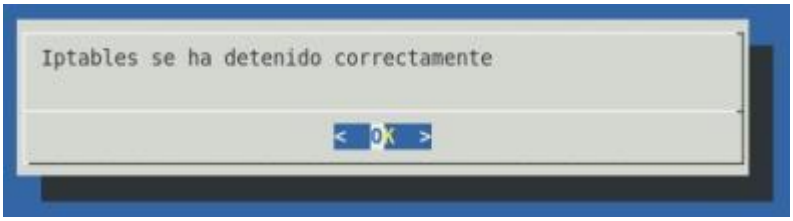

Figura 3. 13 Mensaje opción Detener Servicio

Cuando se detiene el servicio el menú de Administración del servicio cambia, ahora solo tendrá 3 opciones. Además se puede visualizar el estado actual del servicio “** Iptables actualmente está INACTIVO! **”.

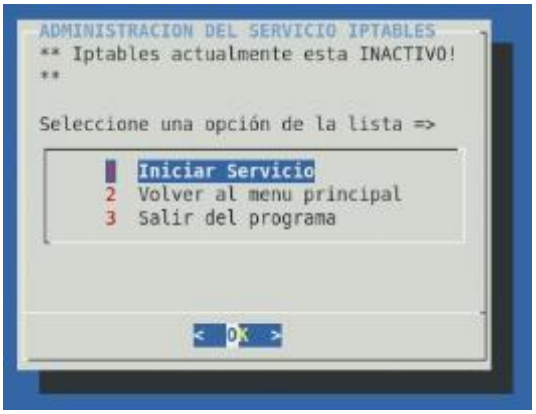

Figura 3. 14 Submenú cuando servicio Iptables está detenido

Si desea iniciar el servicio Iptables entonces tendrá que seleccionar la primera opción de este menú. Cuando seleccione la opción entonces se mostrará el siguiente mensaje indicando la operación exitosa y el

menú de Administración nuevamente mostrará las 6 opciones que mostro cuando el servicio estaba activo.

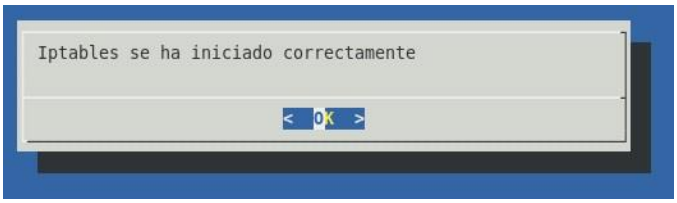

Figura 3. 15 Mensaje de opción Iniciar Servicio

Cabe indicar que mientras el servicio este detenido no se podrá tener acceso a las opciones “Listar Reglas iptables” y “Administración de reglas Iptables” que se encuentran en el menú principal de la aplicación. Si el usuario intenta seleccionar estas opciones se mostrará el siguiente mensaje.

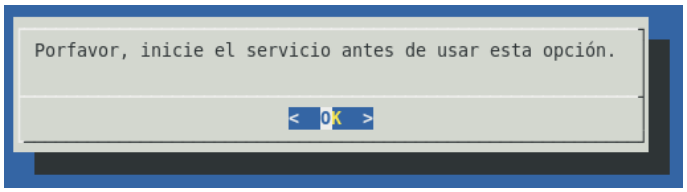

Figura 3. 16 Mensaje error servicio detenido

- La opción “**Restaurar Servicio**”, permitirá restaurar el servicio Iptables, esto hará que los cambios hechos tras modificar la configuración surtan efecto. Si existe alguna regla que no ha sido guardada esta entonces será eliminada de la configuración.

  Esto se debe a que se vuelve a cargar en el núcleo el conjunto de reglas guardadas previamente en el archivo de reglas.

Al seleccionar esta opción se mostrara el siguiente mensaje indicando el éxito de la operación realizada.

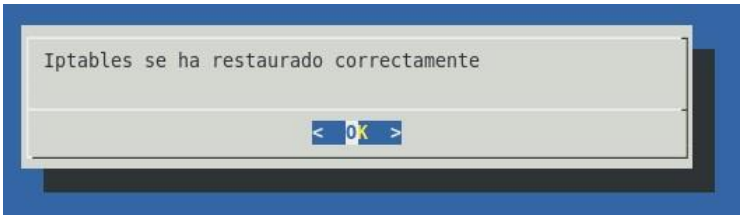

Figura 3. 17 Mensaje de reinicio del servicio Iptables

Este mensaje indicara al usuario que el conjunto de reglas se ha cargado correctamente en el núcleo y todo debería funcionar.

- La opción "**Listar reglas habilitadas**", mostrará el submenú para mostrar las reglas de la tabla: FILTER, MANGLE y NAT que se explicó en líneas anteriores.

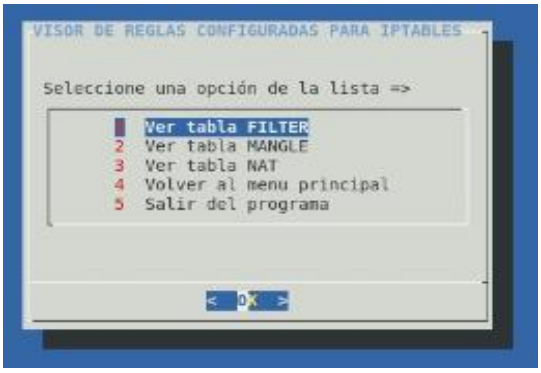

Figura 3. 18 Submenú Mostrar reglas habilitadas

- La opción “**Borrar todas las reglas habilitadas**”, esta opción permite eliminar las reglas existentes para el tráfico entrante, tráfico saliente, tráfico reenviado así como el NAT. Esta opción se la selecciona principalmente con el objetivo de crear nuevas reglas y no afecta al archivo de configuración.

  Al seleccionar esta opción se mostrara el siguiente mensaje indicando el éxito de la operación realizada.

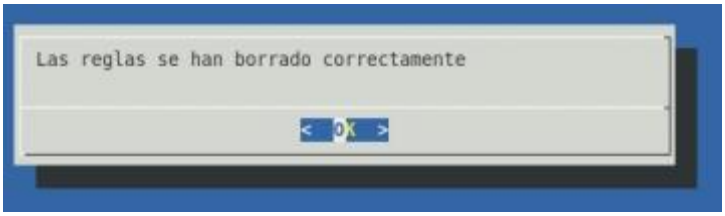

Figura 3. 19 Mensaje de confirmación de eliminación de reglas

Si después de esta acción desea restaurar las reglas que estaban previamente definidas en el archivo de configuración de las Iptables, entonces deberá seleccionar la opción de “restaurar servicio”.

3.4.1.4 Administración de reglas Iptables

Esta opción nos muestra un submenú con opciones que permitirán al usuario administrador crear y eliminar cadenas definidas por usuarios dentro de cualquier tabla. Al seleccionar esta opción se visualizara el siguiente menú:

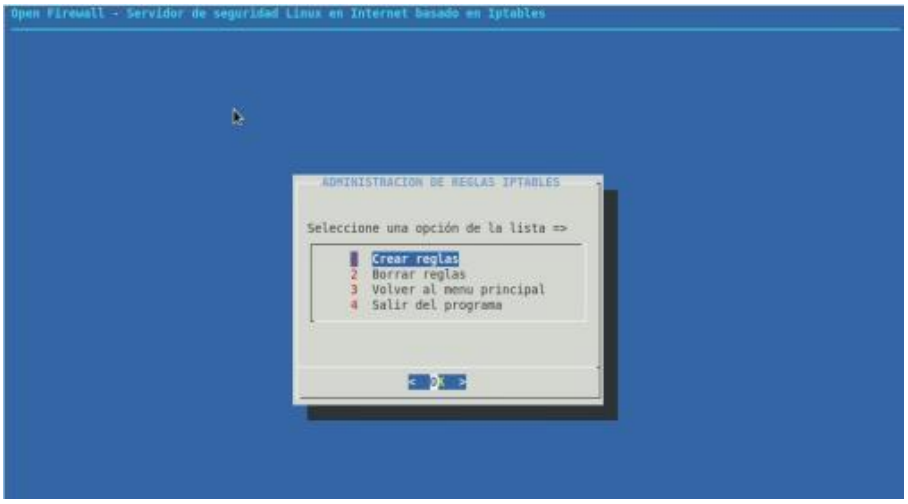

Figura 3. 20 Submenú Administración de reglas Iptables

Si lo que desea realizar es crear una regla entonces se deberá seleccionar la opción 1 “Crear reglas”. Hay tres tablas ya incorporadas, cada una de las cuales contiene ciertas cadenas predefinidas. Las cadenas predefinidas y que se muestran en el menú son FILTER, MANGLE, NAT.

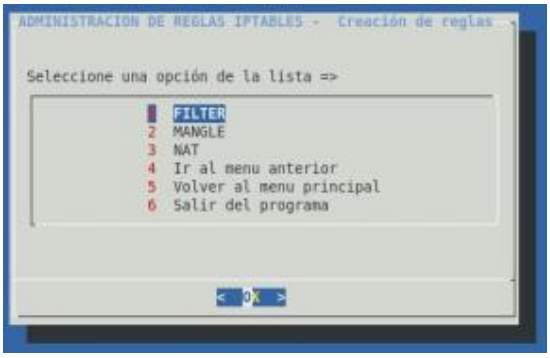

Figura 3. 21 Submenú de creación de reglas

3.4.1.4.1 Crear regla de tabla FILTER

La tabla FILTER es la responsable del filtrado(es decir, de bloquear o permitir que un paquete continúe su camino). Todos los paquetes pasan a través de la tabla de filtros. Contiene las siguientes cadenas predefinidas y cualquier paquete pasará por una de ellas: INPUT, OUTPUT y FORWARD.

- **Creación de cadena INPUT**: Para crear una regla primeramente deberá seleccionar INPUT

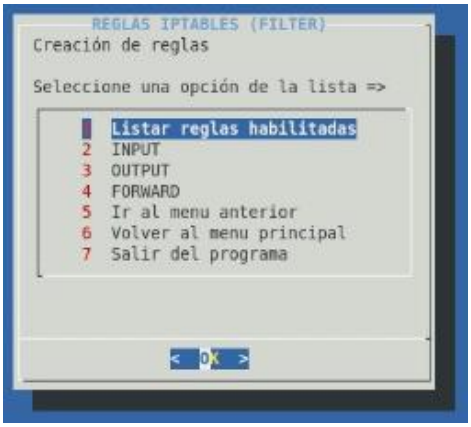

Figura 3. 22 Submenú selección tipo de cadena a crear

El primer parámetro que se tendrá que configurar en este caso es la interfaz a través de la cual un paquete va a ser recibido, para la cual se mostrará el siguiente menú.

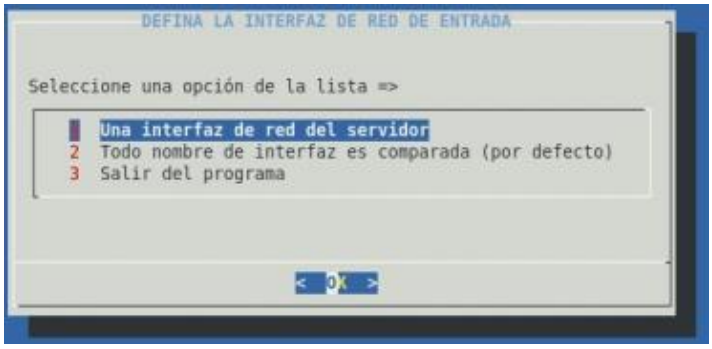

Figura 3. 23 Submenú definición interfaz de entrada

Se podrá seleccionar una interfaz de red del servidor o seleccionar la opción por defecto en cuyo caso toda interfaz de red disponible en el servidor será comparada. Si selecciona la primera opción se mostrara la siguiente ventana.

Figura 3. 24 Selección de Interfaz disponibles

En esta ventana se mostrara las interfaz disponibles actualmente en el servidor entonces proceda a seleccionar una de ellas.

Después se tendrá que definir la dirección de origen.

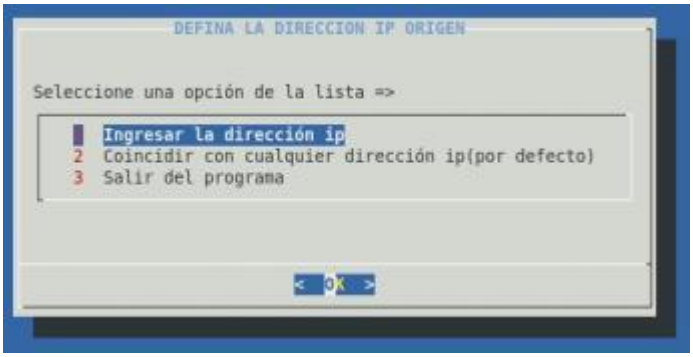

Figura 3. 25 Submenú definición de dirección origen

En este caso se podrá ingresar una dirección con la que se comparará los paquetes IP que vienen de la dirección de origen especificada. Si se selecciona la segunda opción se asume cualquier dirección IP de origen y automáticamente se configura el parámetro 0/0 para la dirección IP.

Si se selecciona la primer opción entonces se mostrará un dialogo donde se podrá ingresar la dirección IP origen.

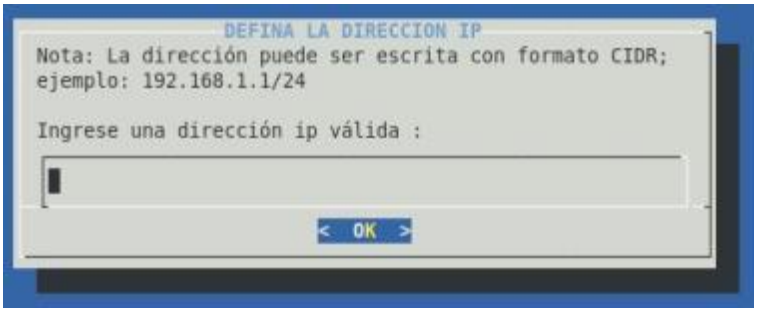

Figura 3. 26 Ingreso de dirección IP origen

La dirección de origen puede ser una dirección IP o una dirección IP con un prefijo de red asociado.

Luego se tendrá que ingresar la dirección IP destino con la que se compararán los paquetes. La dirección IP destino también la puede ingresar el usuario administrador.

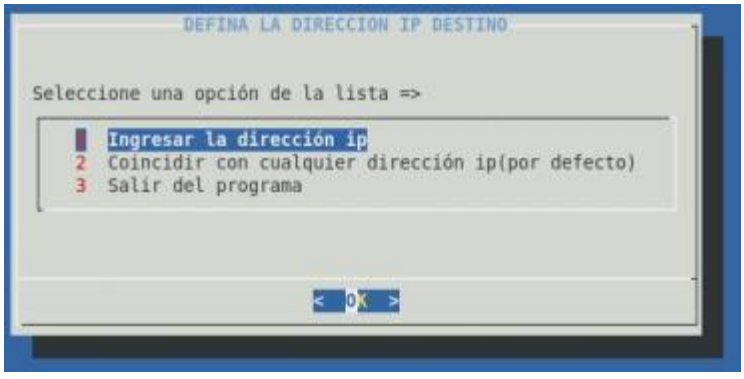

Figura 3. 27 Submenú selección IP destino

Al seleccionar ingresar la dirección IP destino, se mostrará un dialogo en el cual se deberá proporcionar la dirección IP o una segmento de red para lo cual se especificara el prefijo de red asociado.

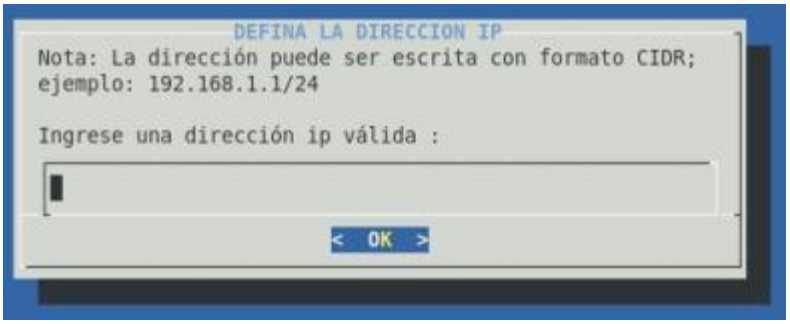

Figura 3. 28 Ingreso de dirección IP destino

El siguiente paso consiste ahora en seleccionar el protocolo, esto lo realizaremos seleccionando una opción del siguiente menú.

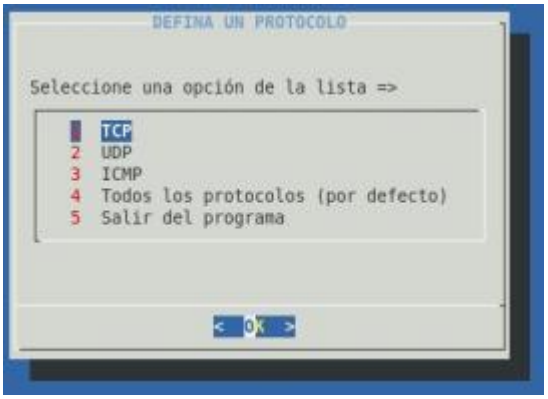

Figura 3. 29 Submenú de selección del protocolo

Si se quiere crear una cadena en la que no se tiene un protocolo específico se deberá seleccionar la opción 4 “Todos los protocolos”.

Luego se tendrá que seleccionar el puerto, para lo cual se tiene 2 alternativas posibles que se muestran en el siguiente menú.

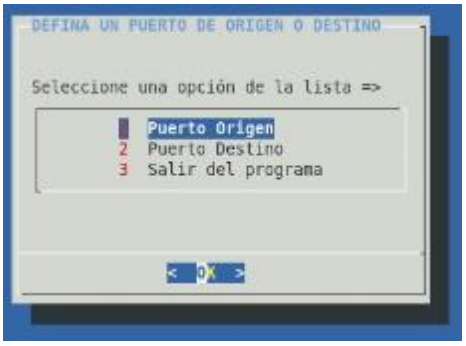

Figura 3. 30 Submenú de selección de puerto

Después de haber seleccionado el tipo de puerto, usted podrá seleccionar entre 2 opciones ingresar el puerto o dejar todos los puertos por default

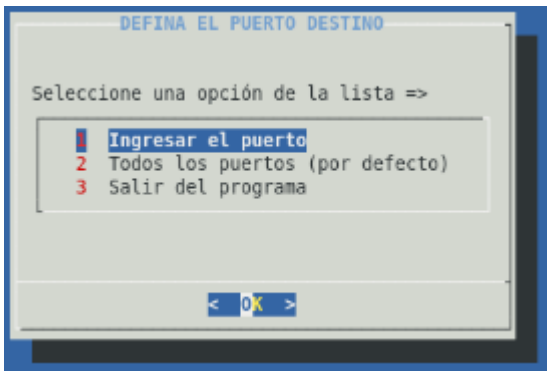

Figura 3. 31 Definición del puerto

Si selecciona la primera opción tendrá que ingresar el puerto que desea incluir en la cadena de entrada que está creando. Selecciona la segunda opción se omite el proceso de ingreso y se asume todo el rango de puerto disponible para el protocolo seleccionado.

Al seleccionar la primera opción se mostrará el siguiente cuadro de dialogo.

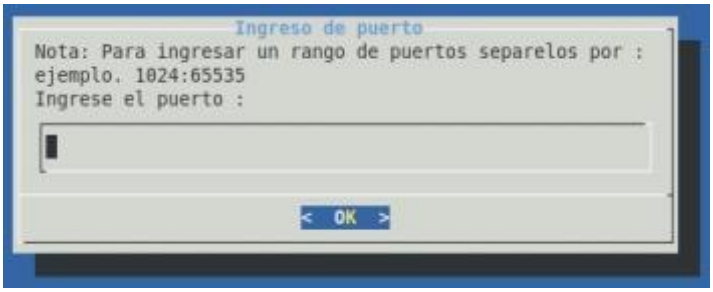

Figura 3. 32 Ingreso de puerto

En este cuadro de dialogo se deberá ingresar un numero de puerto o un rango de puertos, en este último caso se tendrá que separar el rango inicial y final de puerto usando dos puntos(:), como se indica en el ejemplo mostrado en el cuadro de dialogo.

Después de haber definido los parámetros necesarios para la construcción de la regla de firewall, se procede a seleccionar la acción o el destino de una regla ACCEPT, REJECT, DROP.

Figura 3. 33 Definición de la acción para la regla creada

Seleccione **ACCEPT**(aceptar) para que se acepte el paquete. El significado de esto depende de cual sea la cadena realizando esta aceptación. Un paquete que se acepta en la cadena de ENTRADA se le permite ser recibido por el sistema(host), un paquete que se acepta en la cadena de SALIDA se le permite abandonar el sistema y un paquete que se acepta en la cadera de FORWARD se le permite ser encaminado a través del sistema.

Seleccione **DROP** (descartar) para que se descarte el paquete sin ningún otro tipo de procesamiento. El paquete simplemente desaparece sin ningún tipo de indicación al sistema o aplicación de origen, de que fue descartado en el sistema de destino.

Seleccione **REJECT**(rechazo) para rechazar un paquete. Este destino tiene el mismo efecto que “DROP”, salvo que envía un paquete de error a quien envió originalmente. Se usa principalmente en las cadenas ENTRADA y de REDIRECCION de la tabla de filtrado.

Después de seleccionar la acción a realizar con el paquete se mostrara la siguiente ventana

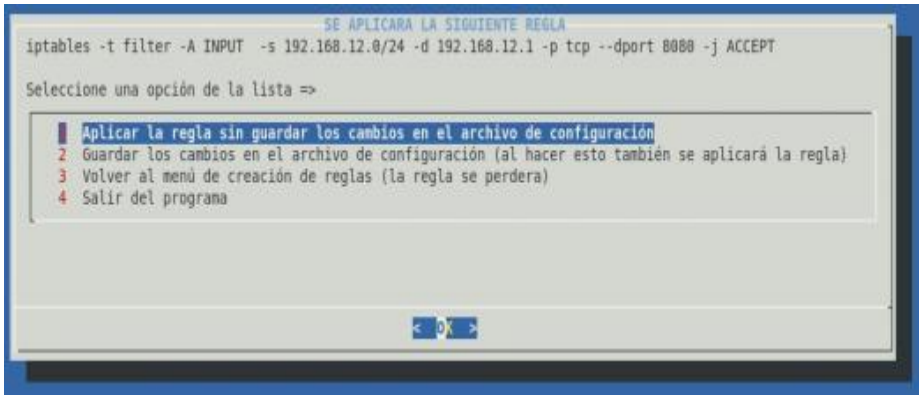

Figura 3. 34 Acción a realizar con la acción creada

En esta ventana se visualiza la regla creada en la parte superior de la ventana. Una vez verificada la regla podemos seleccionar una de las 3 primeras opciones.

- Seleccionemos la opción número 1 “**Aplicar la regla sin guardar los cambios en el archivo de configuración**”, si queremos cargar la regla en el núcleo del sistema sin guardar la misma en el archivo de configuración. Cuando se selecciona esta opción se mostrará un mensaje indicando el éxito de la operación seleccionada.

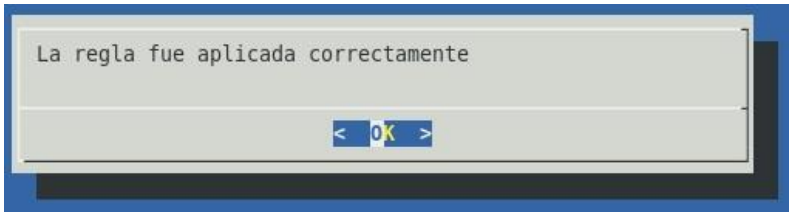

Figura 3. 35 Mensaje de confirmación de aplicación de regla

- Seleccionamos la opción número 2 “**Guardar los cambios en el archivo de configuración**”, si queremos aplicar la regla en el núcleo del sistema y al mismo tiempo guardar la mismas en el archivo de configuración. Cuando se selecciona esta opción se mostrará un mensaje indicando el éxito de la operación seleccionada.

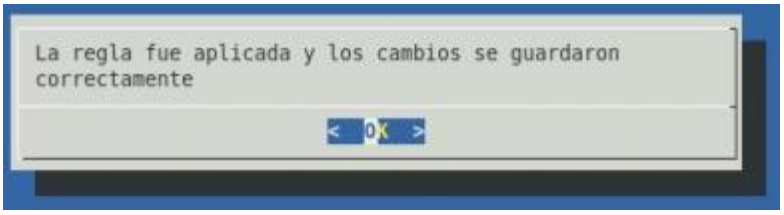

Figura 3. 36 Confirmación de aplicación y almacenamiento de regla creada

- Selecciona la tercer opción “**Volver al menú de creación de reglas**”, si desea cancelar y dejar sin efecto la regla creada. En este caso el control del programa retorna al menú de creación de reglas de tipo FILTER.

3.4.1.4.2 Crear regla de tabla MANGLE

La tabla MANGLE es la responsable de ajustar las opciones de los paquetes, como por ejemplo la calidad del servicio. Todos los paquetes pasan por esta tabla. Debido a que está diseñada para efectos avanzados, contiene todas las cadenas predefinidas posibles: PREROUTING, INPUT, FORWARD, OUTPUT Y POSTROUTING.

Para crear una regla de tipo MANGLE, primero debemos seleccionar esta opción del menú de creación de reglas, luego se mostrará un submenú con los tipos de cadenas que se pueden crear para esta tabla.

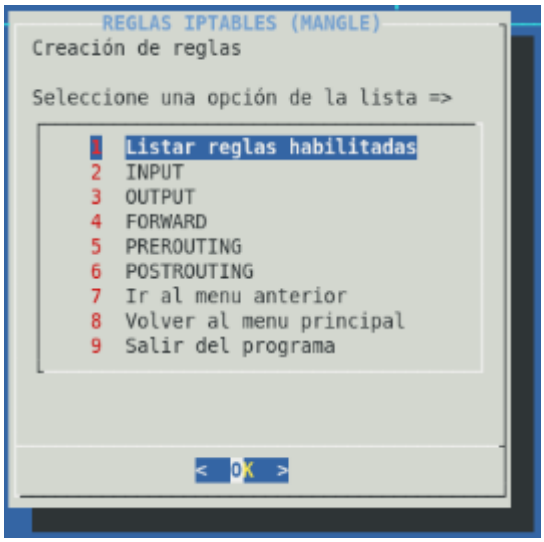

Figura 3. 37 Submenú tabla MANGLE

Luego seleccionamos el tipo de regla a crear por ejemplo una regla de tipo FORWARD

El primer parámetro que se tendrá que configurar en este caso es la interfaz a través de la cual un paquete va a ser recibido, para la cual se mostrará el siguiente menú.

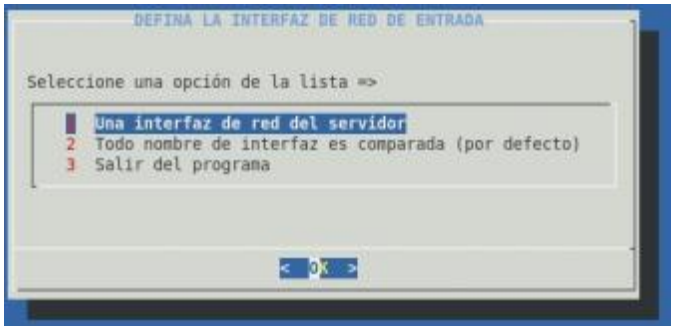

Figura 3. 38 Submenú definición interfaz de entrada

Se podrá seleccionar una interfaz de red del servidor o seleccionar la opción por defecto en cuyo caso toda interfaz de red disponible en el servidor será comparada. Si selecciona la primera opción se mostrara la siguiente ventana.

Figura 3. 39 Selección de interfaz

En esta ventana se mostrara las interfaz disponibles actualmente en el servidor entonces proceda a seleccionar una de ellas. Luego de esta selección se tendrá que definir la dirección de origen.

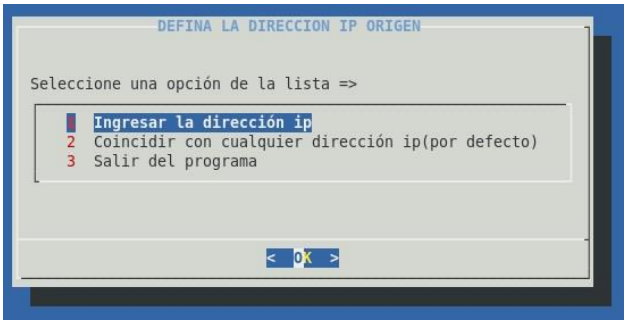

Figura 3. 40 Submenú definición de dirección origen

En este caso se podrá ingresar una dirección con la que se comparará los paquetes IP que vienen de la dirección de origen especificada. Si se selecciona la segunda opción se asume cualquier dirección IP de origen y automáticamente se configura el parámetro 0/0 para la dirección IP.

Si se selecciona la primer opción entonces se mostrará un dialogo donde se podrá ingresar la dirección IP origen.

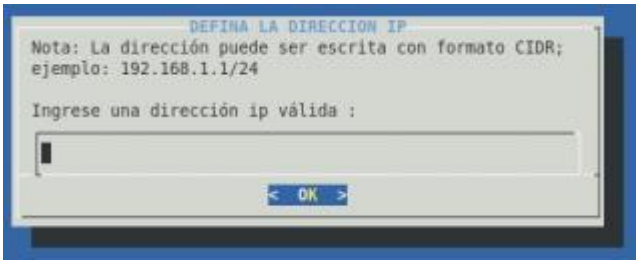

Figura 3. 41 Ingreso de dirección IP origen

La dirección de origen puede ser una dirección IP o una dirección IP con un prefijo de red asociado. Para aceptar la dirección ingresada se deberá seleccionar "**OK"**

Después se mostrará un cuadro de dialogo de selección de la interfaz destino, es decir el nombre de una interfaz a través de la cual un paquete va a ser enviado(esto por lo general en las cadenas de FORWARD, OUTPUT y POSTROUTING).

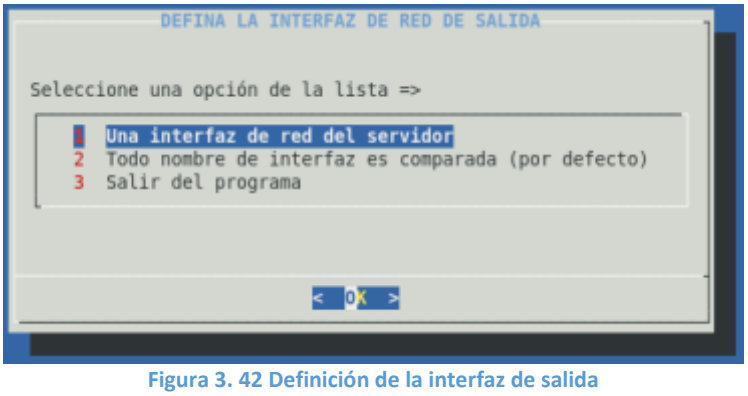

Figura 3. 42 Definición de la interfaz de salida

Se podrá omitir la selección de este parámetro en cuyo caso se tendrá que seleccionar la opción 2. En caso de que usted quiera definir la interfaz de salida entonces seleccione la opción 1, en este último caso se mostrara la ventana de selección de la interfaz.

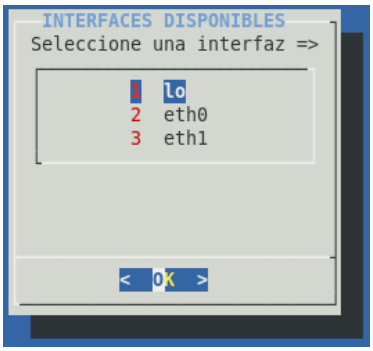

Figura 3. 43 Submenú Interfaz disponibles

Seleccione la interfaz de salida y luego seleccione “**OK”**

Luego se tendrá que ingresar la dirección IP destino con la que se compararán los paquetes o seleccionar la opción “Coincidir con cualquier dirección IP” para que se asuma cualquier dirección IP destino(0/0).

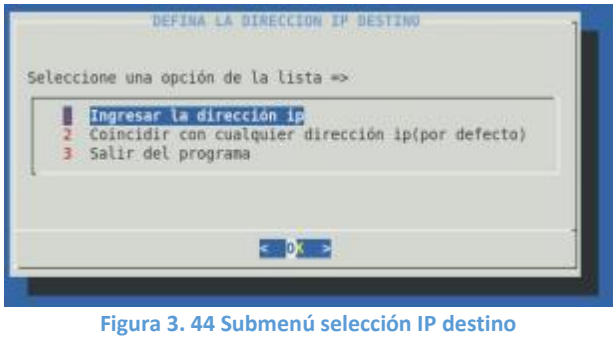

Figura 3. 44 Submenú selección IP destino

Al seleccionar ingresar la dirección IP destino, se mostrará un dialogo en el cual se deberá proporcionar la dirección IP o una segmento de red para lo cual se especificara el prefijo de red asociado.

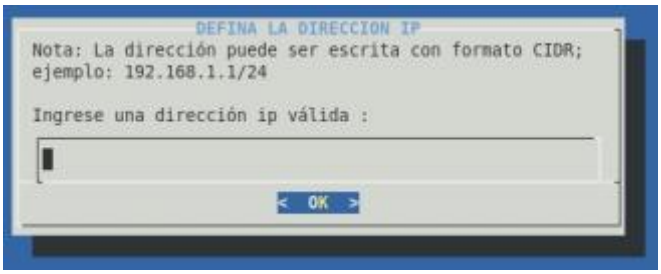

Figura 3. 45 Ingreso de dirección IP destino

El siguiente paso consiste ahora en seleccionar el protocolo, esto lo realizaremos seleccionando una opción del siguiente menú.

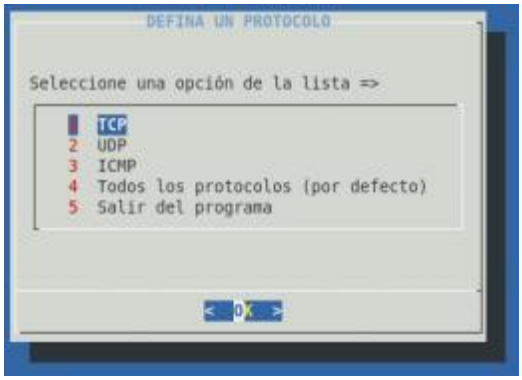

Figura 3. 46 Selección del protocolo

Si se quiere crear una cadena en la que no se tiene un protocolo específico se deberá seleccionar la opción 4 “Todos los protocolos”.

Luego se tendrá que seleccionar el puerto, para lo cual se tiene 2 alternativas posibles que se muestran en el siguiente menú.

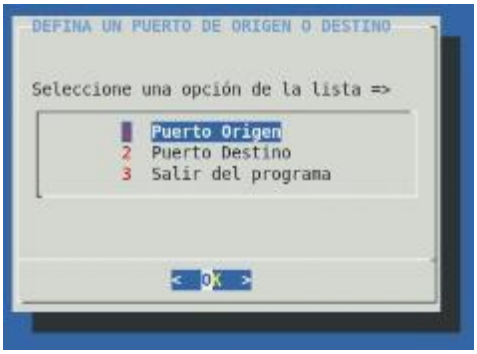

Figura 3. 47 Submenú selección de puerto

Después de haber seleccionado el tipo de puerto, usted podrá seleccionar entre 2 opciones ingresar el puerto o dejar todos los puertos por default

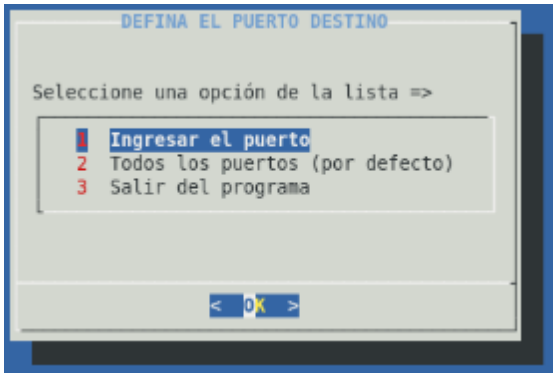

Figura 3. 48 Submenú definición del puerto

Si selecciona la primera opción tendrá que ingresar el puerto que desea incluir en la cadena de entrada que está creando. Selecciona la segunda opción se omite el proceso de ingreso y se asume todo el rango de puerto disponible para el protocolo seleccionado.

Al seleccionar la primera opción se mostrará el siguiente cuadro de dialogo.

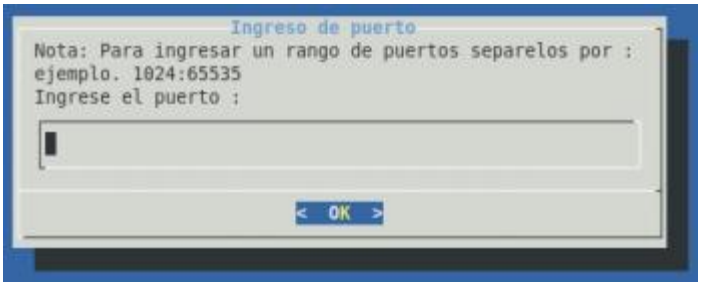

Figura 3. 49 Ingreso de puerto

En este cuadro de dialogo se deberá ingresar un numero de puerto o un rango de puertos, en este último caso se tendrá que separar el rango inicial y final de puerto usando dos puntos(:), como se indica en el ejemplo mostrado en el cuadro de dialogo.

Después de haber definido los parámetros necesarios para la construcción de la regla de firewall, se procede a seleccionar la acción o el destino de una regla ACCEPT, REJECT, DROP.

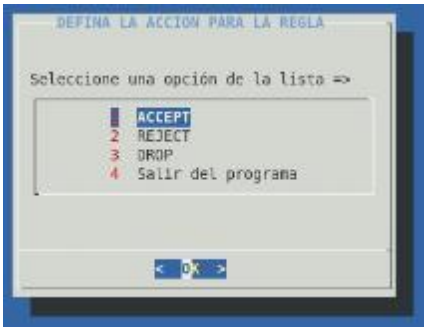

Figura 3. 50 Definición de la acción para la regla creada

Después de seleccionar la acción a realizar con el paquete se mostrara la siguiente ventana

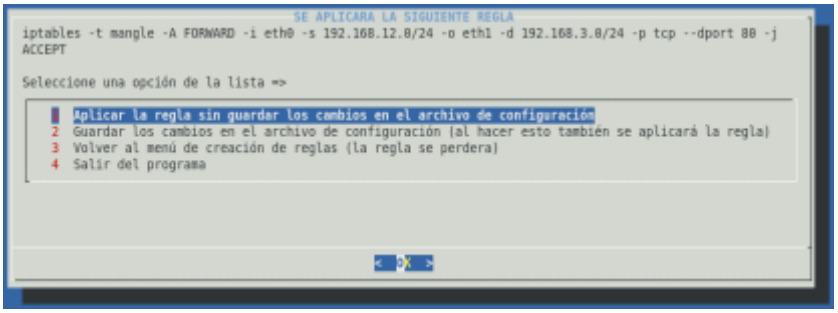

Figura 3. 51 Submenú Acción a realizar con la acción creada

En esta ventana se visualiza la regla creada en la parte superior de la ventana. Una vez verificada la regla podemos seleccionar una de las 3 primeras opciones.

- Seleccionemos la opción número 1 “**Aplicar la regla sin guardar los cambios en el archivo de configuración**”, si queremos cargar la regla en el núcleo del sistema sin guardar la misma en el archivo de configuración. Cuando se selecciona esta opción se mostrará un mensaje indicando el éxito de la operación seleccionada.

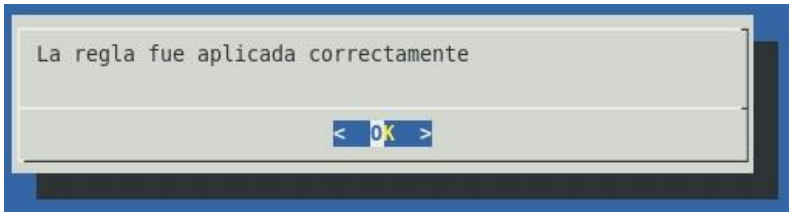

Figura 3. 52 Mensaje de confirmación de aplicación de regla

- Seleccionamos la opción número 2 “**Guardar los cambios en el archivo de configuración**”, si queremos aplicar la regla en el núcleo del sistema y al mismo tiempo guardar la mismas en el archivo de configuración. Cuando se selecciona esta opción se mostrará un mensaje indicando el éxito de la operación seleccionada.

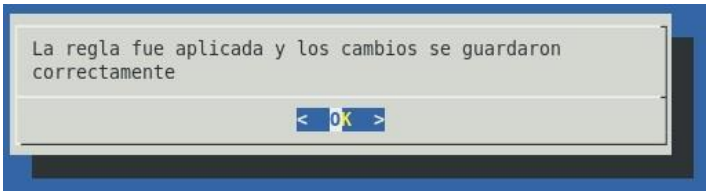

Figura 3. 53 Mensaje de confirmación de aplicación y almacenamiento de regla

- Selecciona la tercer opción “**Volver al menú de creación de reglas**”, si desea cancelar y dejar sin efecto la regla creada. En este caso el control del programa retorna al menú de creación de reglas de tipo MANGLE.

3.4.1.4.3 Crear regla de tabla NAT

La tabla NAT(Tabla de traducción de direcciones de red) es la responsable de configurar las reglas de reescritura de direcciones o de puertos de los paquetes. El primer paquete en cualquier conexión pasa a través de esta tabla. Contiene las siguientes cadenas predefinidas: PREROUTING, POSTROUTING

Para crear una regla de tipo NAT, primero debemos seleccionar esta opción del menú de creación de reglas, luego se mostrará un submenú con los tipos de cadenas que se pueden crear para esta tabla.

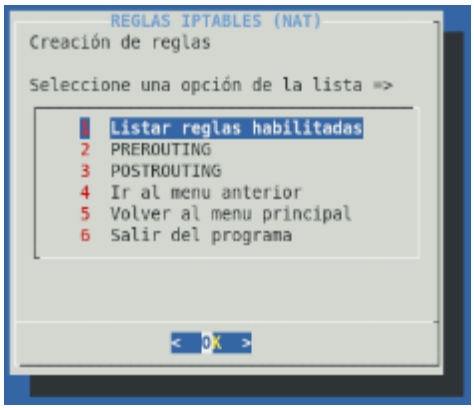

Figura 3. 54 Submenú tabla NAT

Luego seleccionamos el tipo de regla a crear en este caso tenemos 2 alternativas:

“PREROUTING” (cadena de PRERUTEO) los paquetes entrantes pasan a través de esta cadena antes de que se consulte la tabla de ruteo local, principalmente para DNAT(destination-NAT o traducción de direcciones de red de destino)

“POSTROUTING” (cadena de POSRUTEO) Los paquetes salientes pasan por esta cadena después de haberse tomado la decisión de ruteo, principalmente para SNAT(source-NAT o traducción de direcciones de red de origen)

Dependiendo del tipo de cadena a crear se solicitaran los parámetros. Si por ejemplo se selecciona el tipo de cadena PREROUTING el primer parámetro que se tendrá que configurar en este caso es la interfaz a través de la cual un paquete va a ser recibido, para la cual se mostrará el siguiente menú.

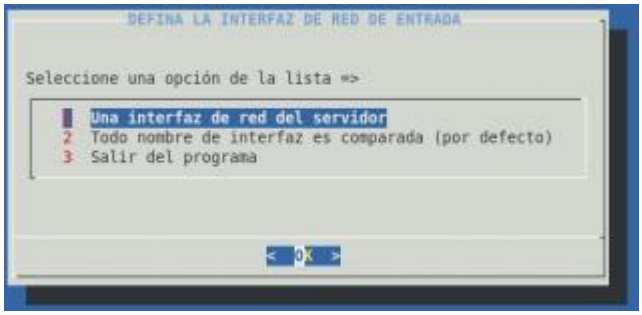

Figura 3. 55 Submenú definición de interfaz de entrada

Se podrá seleccionar una interfaz de red del servidor o seleccionar la opción por defecto en cuyo caso toda interfaz de red disponible en el servidor será comparada. Si selecciona la primera opción se mostrara la siguiente ventana.

Figura 3. 56 Selección de interfaz de origen

En esta ventana se mostrara las interfaz disponibles actualmente en el servidor entonces proceda a seleccionar una de ellas. Luego de esta selección se tendrá que definir la dirección de origen.

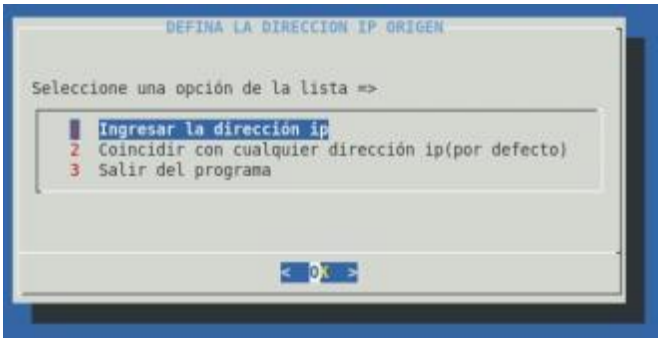

Figura 3. 57 Submenú de definición de dirección origen

En este caso se podrá ingresar una dirección con la que se comparará los paquetes IP que vienen de la dirección de origen especificada. Si se selecciona la segunda opción se asume cualquier dirección IP de origen y automáticamente se configura el parámetro 0/0 para la dirección IP.

Si se selecciona la primer opción entonces se mostrará un dialogo donde se podrá ingresar la dirección IP origen.

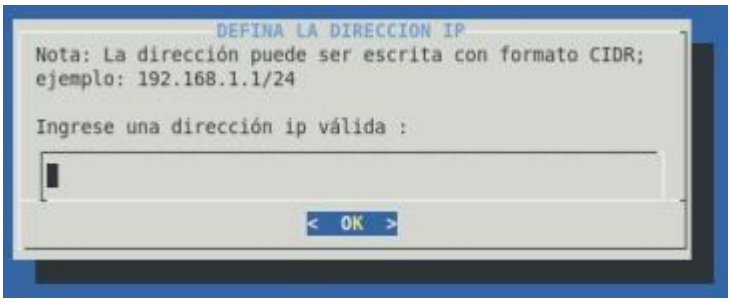

Figura 3. 58 Ingreso de dirección IP origen

La dirección de origen puede ser una dirección IP o una dirección IP con un prefijo de red asociado. Para aceptar la dirección ingresada se deberá seleccionar **OK**

Para las cadenas de PREROUTING no se ingresará la interfaz de destino. Luego se tendrá que ingresar la dirección IP destino con la que se compararán los paquetes o seleccionar la opción “Coincidir con

cualquier dirección IP" para que se asuma cualquier dirección IP destino(0/0).

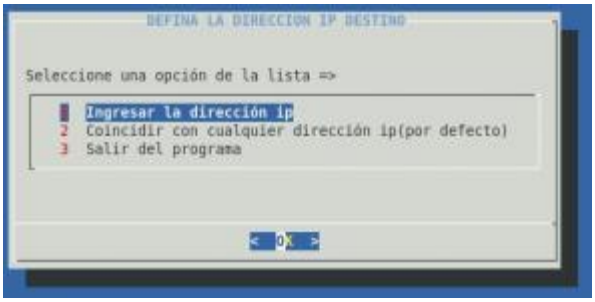

Figura 3. 59 Submenú selección IP destino

Al seleccionar ingresar la dirección IP destino, se mostrará un dialogo en el cual se deberá proporcionar la dirección IP o una segmento de red para lo cual se especificara el prefijo de red asociado.

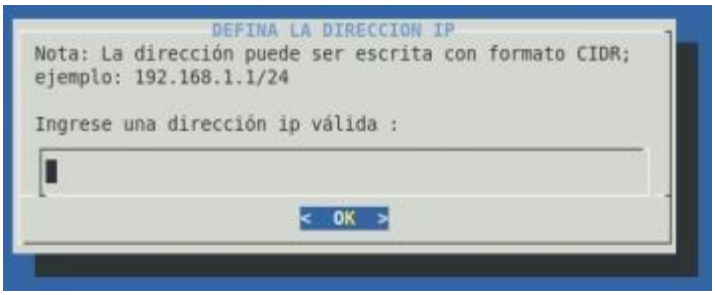

Figura 3. 60 Ingreso de dirección IP destino

El siguiente paso consiste ahora en seleccionar el protocolo, esto lo realizaremos seleccionando una opción del siguiente menú.

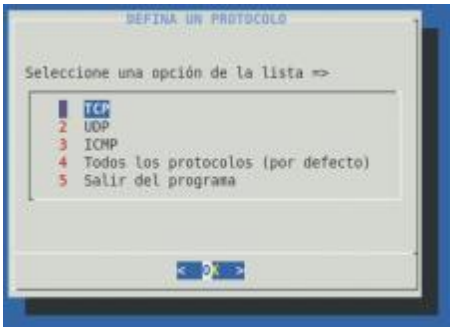

Figura 3. 61 Selección del protocolo

Si se quiere crear una cadena en la que no se tiene un protocolo específico se deberá seleccionar la opción 4 “Todos los protocolos”.

Luego se tendrá que seleccionar el puerto, para lo cual se tiene 2 alternativas posibles que se muestran en el siguiente menú.

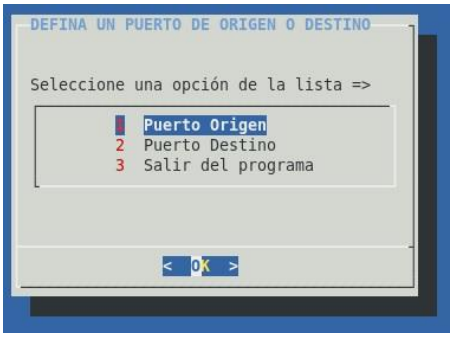

Figura 3. 62 Submenú de selección del puerto

Después de haber seleccionado el tipo de puerto, usted podrá seleccionar entre 2 opciones “ingresar el puerto” o dejar “todos los puertos por default”

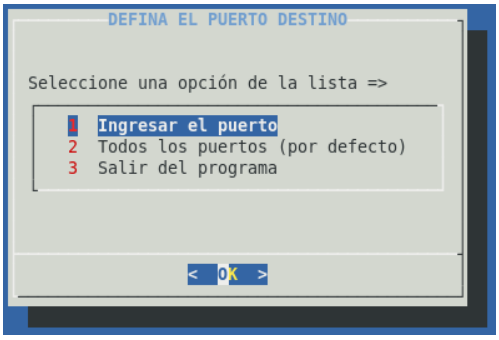

Figura 3. 63 Definición del puerto

Si selecciona la primera opción tendrá que ingresar el puerto que desea incluir en la cadena de entrada que está creando. Selecciona la segunda opción se omite el proceso de ingreso y se asume todo el rango de puerto disponible para el protocolo seleccionado.

Al seleccionar la primera opción se mostrará el siguiente cuadro de dialogo.

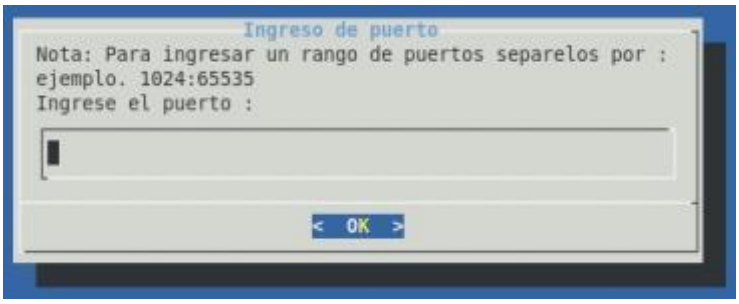

Figura 3. 64 Ingreso del puerto

En este cuadro de dialogo se deberá ingresar un numero de puerto o un rango de puertos, en este último caso se tendrá que separar el

rango inicial y final de puerto usando dos puntos(:), como se indica en el ejemplo mostrado en el cuadro de dialogo.

Después de aceptar el ingreso se mostrará el siguiente cuadro de dialogo.

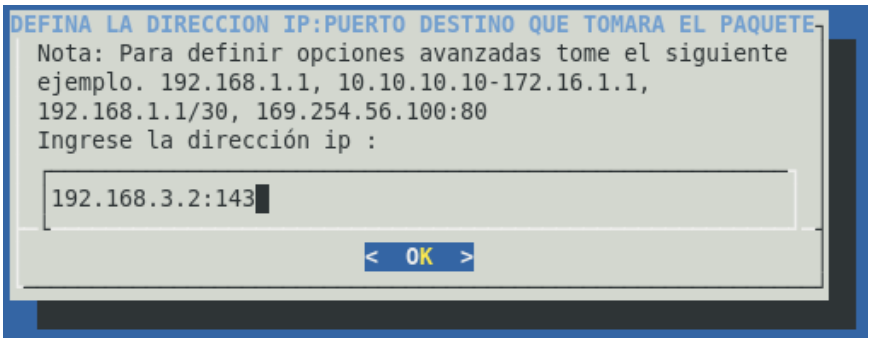

Figura 3. 65 Ingreso de dirección IP:Puerto que tomará el paquete

En esta ventana se procederá a ingresar la dirección que tomara el paquete o a donde se quiere redirigir los accesos al firewall. Se puede ingresar una dirección ip, un rango de direcciones ip, o un segmento de red; adicional a esto se puede indicar el puerto destino al cual se va a redirigir el paquete para esto después de la dirección IP se deberá escribir dos puntos (:) seguido del número de puerto.

Después de aceptar el ingreso realizado se mostrará la siguiente ventana

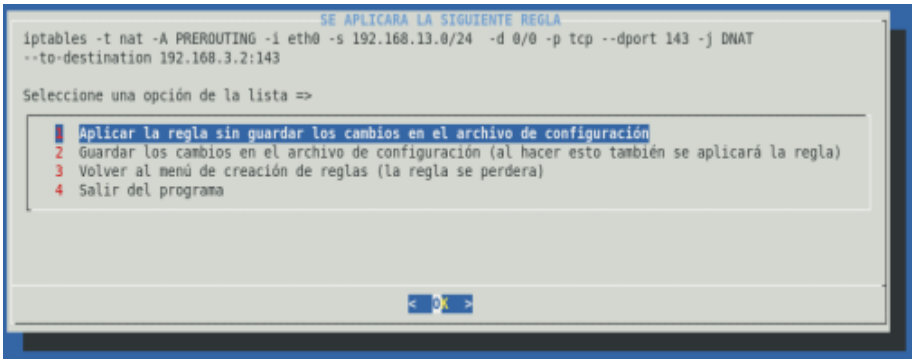

Figura 3. 66 Acción a realizar con la regla creada

En esta ventana se visualiza la regla creada en la parte superior de la ventana. Una vez verificada la regla podemos seleccionar una de las 3 primeras opciones.

- Seleccionemos la opción número 1 "**Aplicar la regla sin guardar los cambios en el archivo de configuración**", si queremos cargar la regla en el núcleo del sistema sin guardar la misma en el archivo de configuración. Cuando se selecciona esta opción se mostrará un mensaje indicando el éxito de la operación seleccionada.

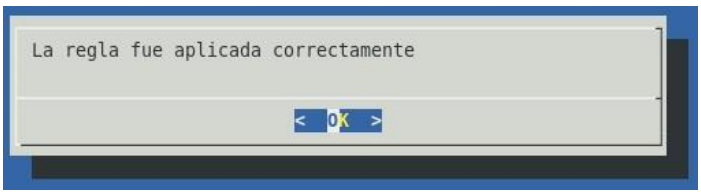

Figura 3. 67 Mensaje de confirmación de aplicación de regla

- Seleccionamos la opción número 2 “**Guardar los cambios en el archivo de configuración**”, si queremos aplicar la regla en el núcleo del sistema y al mismo tiempo guardar la mismas en el archivo de configuración. Cuando se selecciona esta opción se mostrará un mensaje indicando el éxito de la operación seleccionada.

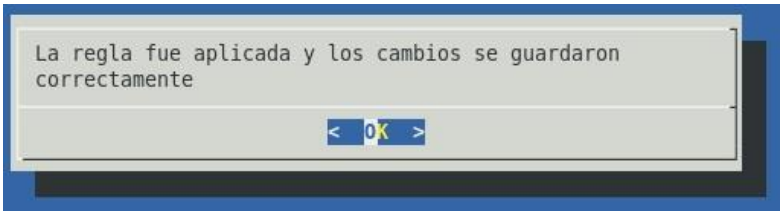

Figura 3. 68 Mensaje de confirmación de aplicación y almacenamiento de la regla

- Selecciona la tercer opción “**Volver al menú de creación de reglas**”, si desea cancelar y dejar sin efecto la regla creada. En este caso el control del programa retorna al menú de creación de reglas de tipo NAT.

3.4.1.4.4 Borrar reglas

Es posible eliminar una regla de cualquiera de las tablas disponibles(FILTER, MANGLE, NAT). Para eliminar una regla en el menú de “Administración de reglas Iptables” se tendrá que seleccionar

la opción “borrar reglas”. Se mostrará un submenú con los tipos de tablas disponibles en la aplicación.

Figura 3. 69 Submenú de eliminación de reglas

Se tendrá que seleccionar la tabla de la cual se desea eliminar una regla, por ejemplo la tabla FILTER. Inmediatamente se visualizara otro submenú para seleccionar el tipo de cadena de la regla que se desea eliminar.

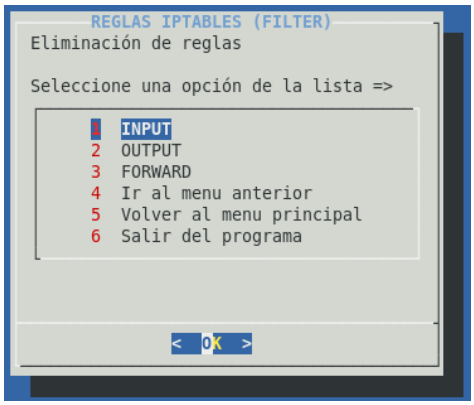

Figura 3. 70 Submenú de selección de cadena a eliminar

Dependiendo del tipo de cadena a eliminar seleccione una de las 3 primeras opciones. Al seleccionar una de las opciones se visualizara un cuadro de dialogo de ayuda que indica al usuario como proceder para eliminar una regla.

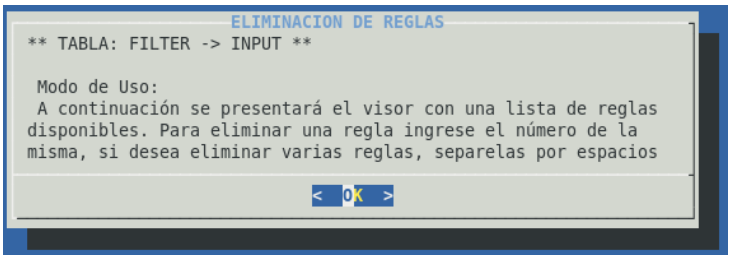

Figura 3. 71 Dialogo explicativo para eliminación de reglas

En esta ventana de dialogo usted puede comprobar en la parte superior un mensaje con la tabla seleccionada y el tipo de cadena que se procederá a eliminar(** TABLA: FILTER -> INPUT **). Para continuar seleccione OK.

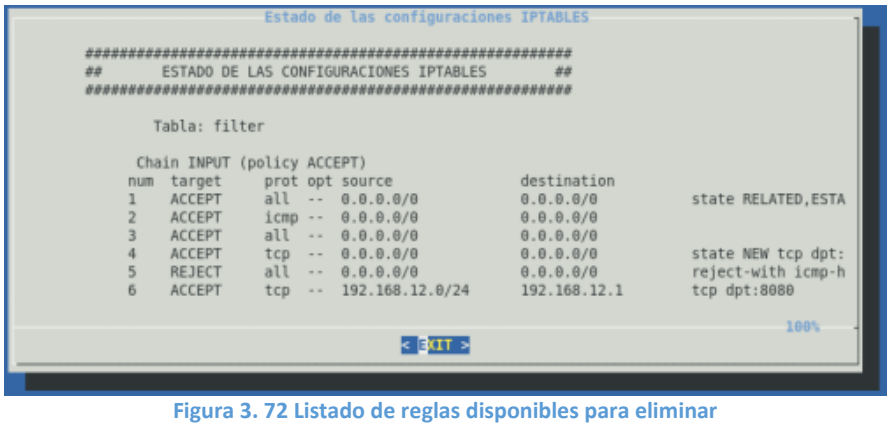

Figura 3. 72 Listado de reglas disponibles para eliminar

En esta ventana se mostrará un listados dependiendo de qué tipo de tabla y tipo de regla hayamos seleccionado. Este listado nos servirá para conocer el número de regla a eliminar. Para continuar seleccionamos “EXIT”, luego se visualizara por pantalla el siguiente cuadro de dialogo.

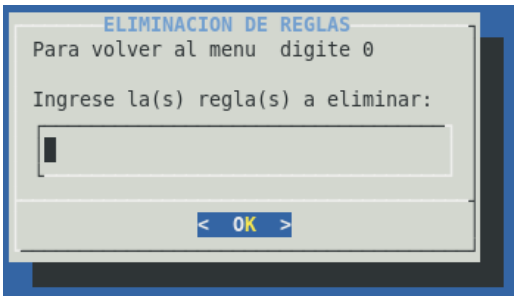

Figura 3. 73 Ingreso de número de regla a eliminar

En este cuadro de dialogo se tendrá que proporcionar el número de regla a eliminar. En caso de que no se quiera eliminar la regla y se quiera regresar al submenú de eliminación de reglas se deber ingresar 0.

Se podrá proporcionar más una regla a eliminar para lo cual se tendrá que ingresar los números de reglas separados por un espacio. Por ejemplo 2 4 6.

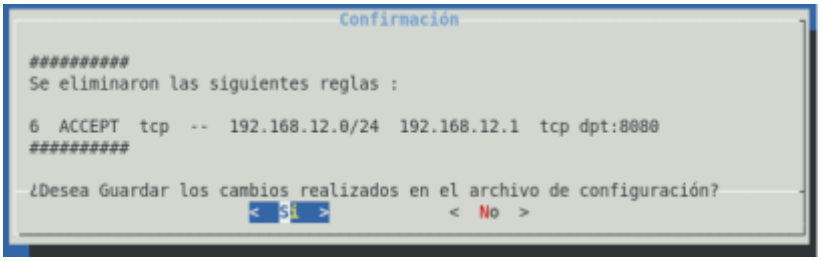

Figura 3. 74 Mensaje de confirmación de regla eliminada

Cuando este mensaje aparece significa que la regla(s) han sido eliminadas del listado de reglas que se están ejecutando actualmente. En este dialogo le pedirá confirmación de que si desea guardar los cambios realizados(reglas eliminadas) en el archivo de configuración para hacer permanentes los cambios.

Si el usuario selecciona **SI** entonces se confirmaran los cambios realizados

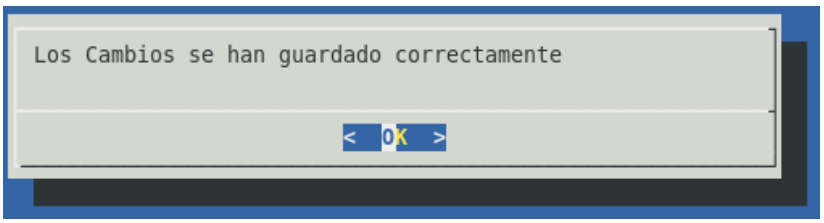

Figura 3. 75 Mensaje de confirmación de almacenamiento de cambios

Si el usuario selecciona **NO** entonces la regla solo será eliminada del listado de las reglas que se ejecutan actualmente, pero no del archivo de configuración.

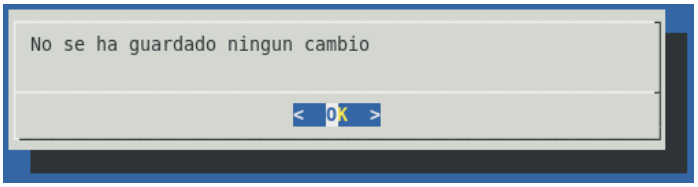

Figura 3. 76 Mensaje de confirmación de cambios no guardados

3.5 Configuración de reglas que permitan el tráfico de red requerido

Los firewalls se pueden usar en cualquier red. Es habitual tenerlos como protección de internet en las empresas, aunque ahí también suelen tener una doble función: controlar los accesos externos hacia dentro y también los internos hacia el exterior. En esta sección se va ver una configuración de firewall iptables tomando una tipología clásica de un firewall, que se adapta a la estructura de red de la institución.

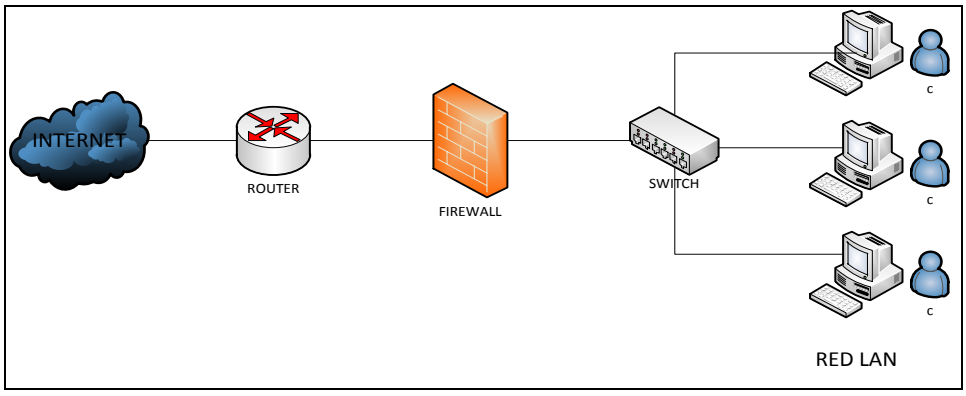

Figura 3. 77 Esquema típico de firewall a configurar

En la gráfica se presenta un esquema típico de firewall para proteger una red local conectada a internet a través de un router. El firewall debe colocarse entre el router(con un único cable) y la red local(conectado al switch de la LAN).

Se tendrá un conjunto de reglas en las que se examina el origen y destino de los paquetes del protocolo tcp/ip. Se bloquearan protocolos no solo tcp, también los udp e icmp. A continuación se presenta en pseudo-lenguaje un conjunto de reglas de firewall para el esquema de red presentado en el gráfico anterior:

- Política por defecto ACEPTAR
- Todo lo que venga de la red local al firewall ACEPTAR
- Todo lo que venga de la ip externa de un usuario administrador al puerto tcp 22(ssh) ACEPTAR
- Todo lo que venga de la ip de casa de un usuario administrador dirigidos a servicios internos se ACEPTA
- Todo lo que venga del exterior al puerto 80 redirigirlo
- Se abre el acceso a los puertos de correo electrónico.
- Se acepta consulta al DNS desde la red local
- Todo lo que venga de la red local y vaya al exterior ENMASCARAR

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

En resumen lo que se va a realizar es: Habilitar el acceso a puertos de administración a determinadas IPs privilegiadas; Enmascarar el tráfico de la red local hacia el exterior(NAT, una petición de un PC de la LAN saldrá al exterior con la ip pública), para poder salir a internet; Denegar el acceso desde el exterior a puertos de administración y a todo lo que este entre 1 y 1024

3.5.1 Reglas a aplicarse en la red.

En las reglas de filtrado que se aplicarán en el ejemplo. Se asume que la interfaz eth0 es el interfaz conectado al router y eth1 a la LAN.

- Se realiza un FLUSH de las reglas actuales

  iptables –F

  iptables -X

  iptables -Z

  iptables -t nat –F

- Se establece una política por defecto antes de aplicar las reglas personalizadas

  iptables -P INPUT ACCEPT

  iptables -P OUTPUT ACCEPT

  iptables -P FORWARD ACCEPT

  iptables -t nat -P PREROUTING ACCEPT

  iptables -t nat -P POSTROUTING ACCEPT

- Todo lo que venga por el exterior y vaya al puerto 80 lo redirigimos a una maquina interna

  iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j DNAT --to 192.168.12.1:80

- El localhost se deja (por ejemplo conexiones locales a mysql u otro servicio)

  iptables -A INPUT -i lo -j ACCEPT

- Al firewall tenemos acceso desde la red local

  iptables –A INPUT –s 192.168.12.0/24 –i eth1 –j ACCEPT

- Abrimos el acceso a puertos de correo. Abrimos el puerto 25, y el puerto pop3

  iptables –A INPUT –s 0.0.0.0/0 –p tcp --dport 25 –j ACCEPT

  iptables –A INPUT –s 0.0.0.0/0 –p tcp --dport 110 –j ACCEPT

- Se abre el puerto ssh para la ip del adsl de un administrador externo a un servicio interno

  iptables –A INPUT –s 211.45.176.24 –p tcp --dport 22 –j ACCEPT

- A un usuario administrador externos se da acceso a usar el FTP

  iptables –A INPUT –s 80.37.45.194 –p tcp –dport 20:21 –j ACCEPT

Ahora con una regla FORWARD filtramos el acceso de la red local al exterior. Como se explica antes, a los paquetes que no van dirigidos al propio firewall se les aplican reglas de FORWARD

- Aceptamos que vayan a puertos 80

iptables –A FORWARD –s 192.168.12.0/24 –i eth1 –p tcp –-dport 80 –j ACCEPT

- Aceptamos que vayan a puertos https

  iptables –A FORWARD –s 192.168.12.0/24 –i eth1 –p tcp -–dport 443 –j ACCEPT

- Aceptamos que consulten los DNS

  iptables –A FORWARD –s 192.168.12.0/24 –i eth1 –p tcp --dport 53 –j ACCEPT

  iptables –A FORWARD –s 192.168.12.0/24 –i eth1 –p udp --dport 53 –j ACCEPT

- Y denegamos el resto.

  iptables –A FORWARD –s 192.168.12.0/24 –i eth1 –j DROP

- Ahora hacemos enmascaramiento de la red local

  iptables -t nat -A POSTROUTING –s 192.168.10.0/24 -o eth0 -j SNAT --to-source 192.168.3.1

- Ahora se cierra los accesos indeseados del exterior, 0.0.0.0/0 significa cualquier red. Cerramos el rango de puerto bien conocido

iptables –A INPUT –s 0.0.0.0/0 –i eth0 –p tcp –dport 1:1024 –j DROP

iptables –A INPUT –s 0.0.0.0/0 –i eth0 –p udp –dport 1:1024 –j DROP

- Cerramos el puerto del servicio SSH, solo abierto para un usuario administrador

  iptables –A INPUT –s 0.0.0.0/0 –i eth0 –p tcp --dport 22 –j DROP

CAPITULO 4

4. Políticas de Seguridad

4.1 Función y uso de las políticas de seguridad en nuestra infraestructura de TI

Para la interfaz gráfica que hemos diseñado, el uso del firewall es más sencillo de utilizar ya que podemos entender de manera más fáciles las reglas a medida que las creamos.

El punto más importante de las tareas que realizará el firewall será la de permitir o denegar determinados servicios dependiendo de los distintos usuarios y su ubicación.

Los usuarios internos con permiso de salida para servicios restringidos, utilizaremos una serie de redes y direcciones a los que denominaremos usuarios con validaciones o Trusted. Estos usuarios, cuando provengan del interior, van a poder acceder a determinados

servicios externos los cuales hayan sido definidos en las políticas definidas por el distrito.

Los usuarios externos con permiso de entrada desde el exterior a la red del distrito serán los que van a ser vigilados ya que son casos sensibles. Estos usuarios externos son los que por algún motivo deben acceder para consultar los distintos servicios de la red interna desde otras redes dentro del distrito.

Para las pruebas de desempeño en el ambiente del distrito, el tráfico general que lo compone en su mayoría es una combinación de paquetes TCP y UDP; los cuales serían revisados por el firewall para redirigir los distintos paquetes a sus respectivos destinos dependiendo de la acción que tome.

4.2 Establecimiento de políticas de seguridad de la red institucional

Existen dos posturas las cuales son las que debemos tomar en cuenta al momento de crear una política de seguridad y esas son:

- "No todo lo específicamente permitido está prohibido"
- "Ni todo lo específicamente prohibido está permitido"

La primera postura asume que un firewall puede obstruir todo el tráfico y cada uno de los servicios o aplicaciones deseadas necesariamente para ser implementadas básicamente caso por caso. La desventaja es que el punto de vista de "seguridad" es más importante que facilitar el uso de los servicios y éstas limitantes numeran las opciones disponibles para los usuarios de la comunidad.

La segunda postura asume que el firewall puede desplazar todo el tráfico y que cada servicio potencialmente peligroso necesitará ser aislado básicamente caso por caso. La desventaja de esta postura se basa en la importancia de "facilitar el uso" que la propia seguridad del sistema.

4.2.1 Política de seguridad interna.

Es la de mayor importancia la cual define todos los aspectos en competentes al perímetro de defensa del distrito de salud. Para que esta sea exitosa, la organización debe de conocer que es lo se está protegiendo. La política de seguridad se basara en una conducción cuidadosa analizando la seguridad, la asesoría en caso riesgo, y la situación en la que se encuentra su red, si no se especifica la información detallada de las políticas que quieren seguir, aunque sea

un firewall cuidadosamente desarrollado y armado, estará exponiendo la red privada a un posible atentado.

4.3 Tipos de políticas de seguridad

Las políticas de seguridad son un complemento para tener una mayor protección dentro de nuestras instituciones.

Existen varias políticas de seguridad a seguir dentro del distrito de salud.

1. Responsabilidad individual por parte de cada usuario de una estación de trabajo, las personas responsables deberán ser responsables de sus actividades, ya que toda acción que ellos realicen serán registradas y monitoreadas para luego ser examinadas por el administrador. Por esto determinaremos cuentas y claves para cada uno de los usuarios en las distintas estaciones de trabajo y estableciendo el intervalo de cambio de contraseñas para cada uno.

2. Control y autorización a los usuarios para realizar distintas acciones y utilizar de manera explícita en que forma puede utilizar la información y los recursos dentro del distrito de salud, solo los

usuarios confirmados podrán acceder desde otra red a los recursos e información del distrito

3. Los privilegios que tenga cada estación de trabajo serán asignadas y evaluadas para que ingresen a los recursos que necesita para realizar y desempeñar bien el trabajo de cada usuario, deberemos restringir todo tipo de software. Para evitar los ataques de virus.

4. Las obligaciones que tiene cada departamento deberán ser divididas entre los usuarios que lo componen, con la finalidad de que ninguna persona cause problemas o algún tipo de ataque sin que sea detectado, la separación de las funciones de cada usuario es mejor cuando cada uno está relacionado con distintas actividades y puntos de vista, de esta manera no hay competencia entre ellos y que llegue haber rencores entre las personas de un mismo departamento

5. Debemos tener auditorías por el personal administrativo de sistemas para revisar el trabajo y obtener resultados de los monitoreos realizados

6. Hay que tener redundancia al momento de obtener información ya que debemos tener copias de lo realizado ya que manejamos información muy sensible estas copias deberán ser guardadas frecuentemente en distintos servidores.

4.3.1 Criterios al manejar las políticas de seguridad

Al asumir una política de seguridad existen distintos criterios o puntos de vista de lo que se deber utilizar a medida que estas se van desarrollando por lo cual un modelo a seguir debe ser aplicado.

- Aplicar una política de manera precisa y válida, deberemos crearla de una manera clara y saber qué es lo que se está tratando de validar y justificar al utilizarla.

- El sistema debe ayudar a comprender la lógica de las acciones que se están realizando.

- Un modelo debe saber utilizar un soporte de seguridad y saber si este funciona en los distintos aspectos y situaciones en la que se pueda encontrar una entidad.

- Las políticas deberán ser razonables al momento de aplicarlas para trabajar de una manera adecuada sin afectar el rendimiento de los usuarios.
- Estas reglas deberán ser creadas por partes analizándolas y luego unirlas y formar un sistema completo y seguro para la verificación de su estado sea correcta.

- Las pruebas de estas reglas deberán ser realizadas en un ambiente de prueba simulando la actividad de la empresa antes de lanzarla al ambiente real.

4.3.2 Integridad al manejar la información

La integridad es cuando la información no sufre ningún tipo de alteración.

Las metas de la integridad de información son:

- Mantener la consistencia de los datos
- Prevenir las modificaciones no autorizadas
- Mantener los atributos de la calidad en los datos
- Prevenir transacciones de cualquier tipo en los datos

4.3.3 Recomendaciones básicas de seguridad al utilizar políticas de firewall

1. Debemos recordar que toda estación de trabajo deberá tener instalado un antivirus, sin importar cuál sea su marca/nombre, este siempre deberá estar actualizado

2. Los usuarios o administradores deberán actualizar los parches de los sistemas operativos.

3. Utilizar siempre usuarios y contraseñas en todas las estaciones de trabajo, y que estas contraseñas no sean palabras de diccionario o que estén relacionadas con la persona que trabaja en cada estación ya que podrían ser descubiertas fácilmente

4. Cambiar las claves al menos 3 veces al año, aunque lo recomendable es cambiarla cada mes, para evitar posibles filtros de información al utilizar siempre una clave en particular

5. Las carpetas compartidas, deben estar protegidas por claves de acceso, la misma que deberá ser cambiada cada cierto tiempo

6. No ejecutar ningún archivo de algún remitente desconocido

7. No instalar copias de software pirata, además de faltar a la ley ya impuesta por el gobierno esto traería problemas al distrito de salud.

4.4 Uso de la aplicación de Firewall utilizando las políticas de seguridad.

Nuestro ambiente de prueba son máquinas virtuales las cuales una sirve como servidor con dirección 192.168.12.1/24 utilizando el sistema operativo CentOs 6.3 como muestra la Figura 4.1

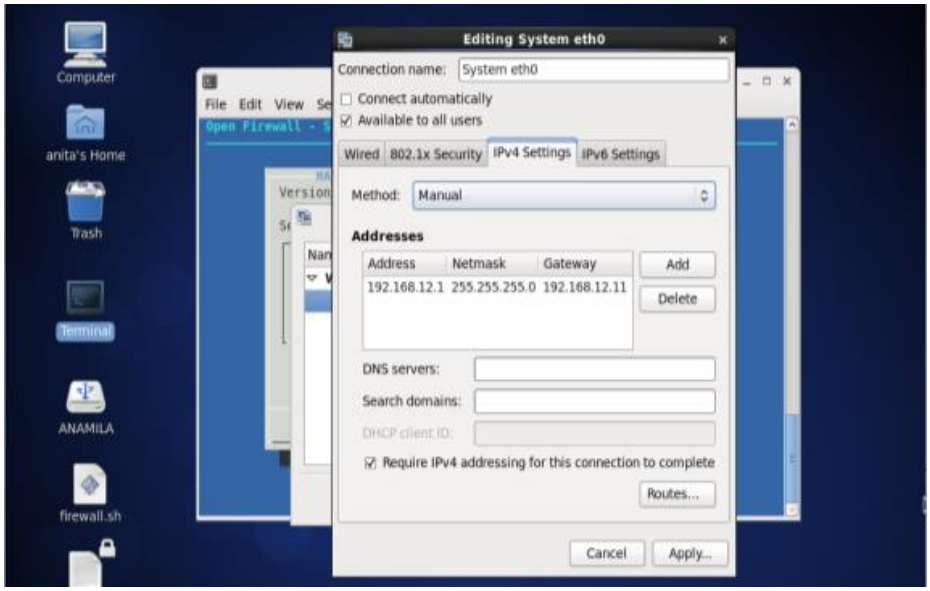

Figura 4. 1Configuración IP del servidor

Dos máquinas host las cuales una utiliza Windows 7 con dirección 192.168.12.2/24 como máquina dentro del distrito Figura 4.2

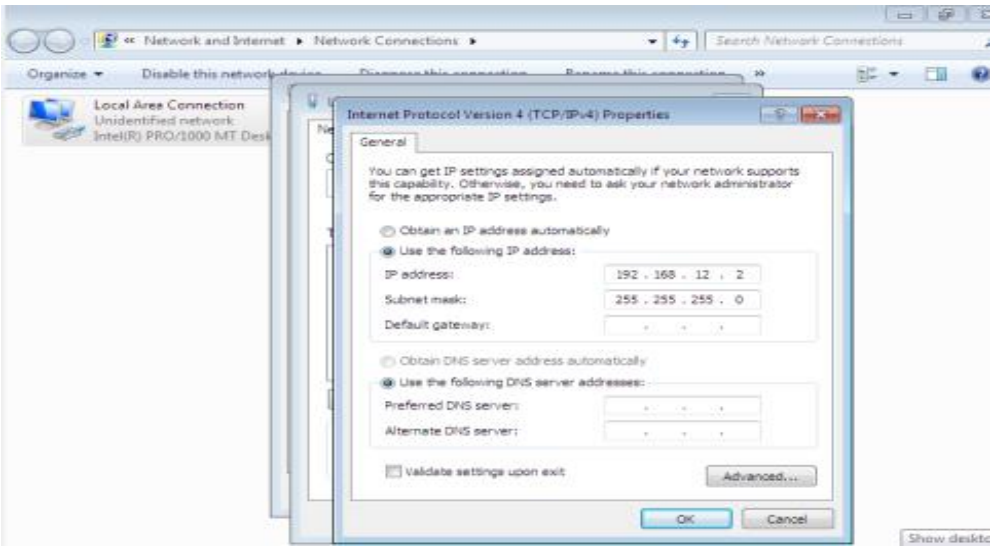

Figura 4. 2 Maquina host Windows 7

Adicionalmente se tiene otro equipo en Windows XP como usuario de ataque con dirección 10.10.10.1/24 como muestra la Figura 4.3. Probaremos las reglas utilizadas en nuestro firewall y observaremos las conexiones que podemos realizar.

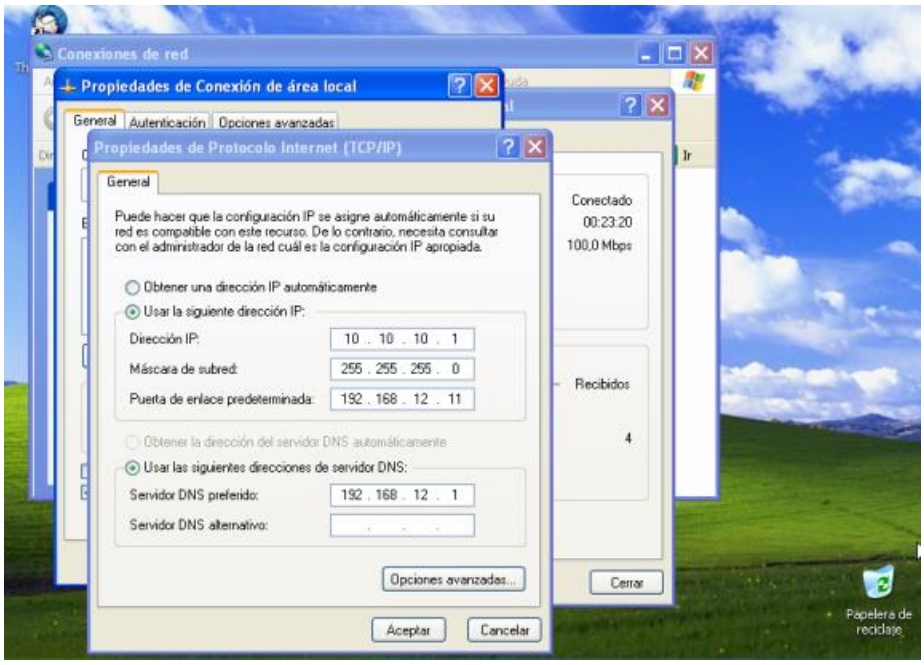

Figura 4. 3 Máquina intruso con Windows XP

4.4.1 Permitir manejo de archivos entre servidor y usuario del distrito con samba protocolo sftp

Comprobación de conectividad al aplicar la regla de firewall para permitir solo que la red 192.168.12.0/24 sea la única que pueda conectarse al servidor (Figura 4.4) mediante el protocolo Sftp

utilizando samba el cual me permite compartir archivos con ambientes Windows. (Figura 4.5)

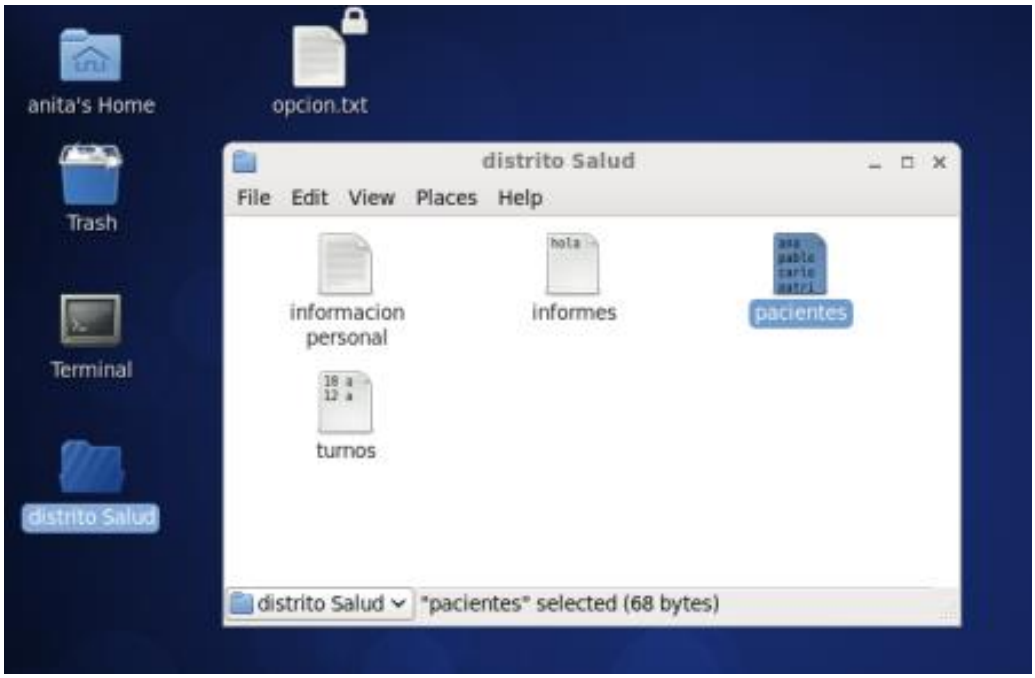

Figura 4. 4 Archivos compartidos con el usuario Windows

Ilustración de los archivos compartidos con el servidor en el ambiente Windows 7 máquina cliente del distrito que se encuentra dentro de la red 192.168.12.0/24.

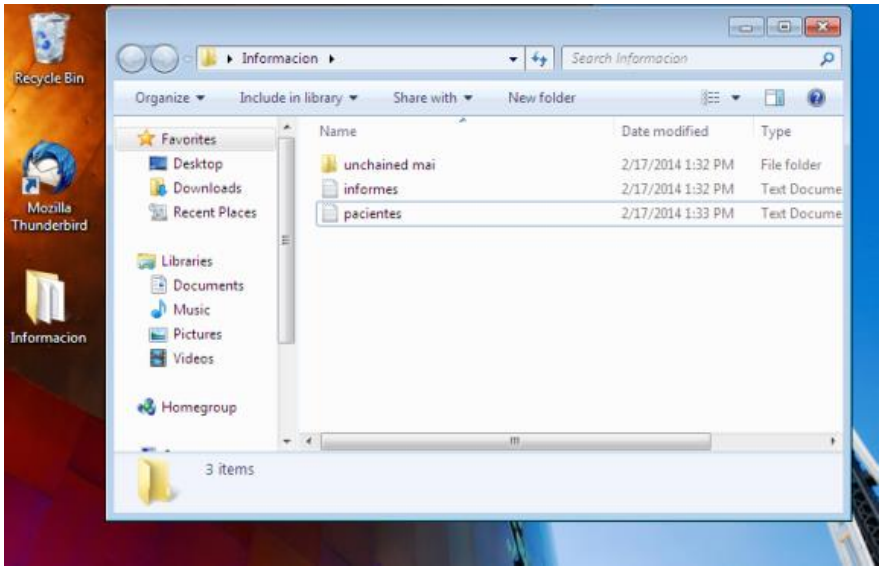

Figura 4. 5 Archivos compartidos con el servidor desde Windows 7

4.4.2 SSH manejo remoto de administrador desde el host hacia el servidor

Para realizar esta prueba se utilizaron dos herramientas TigerVNC y TightVNC en la maquina servidor y la de host del distrito.

4.1.1.1 Uso de TightVNC

Para realizar la conexión entre el servidor y la máquina cliente utilizamos la herramienta TightVNC del lado de la maquina cliente, este programa nos permite hacer conexiones a escritorios remotos

introduciendo el nombre de dominio o simplemente la dirección Ip como muestra la figura siguiente

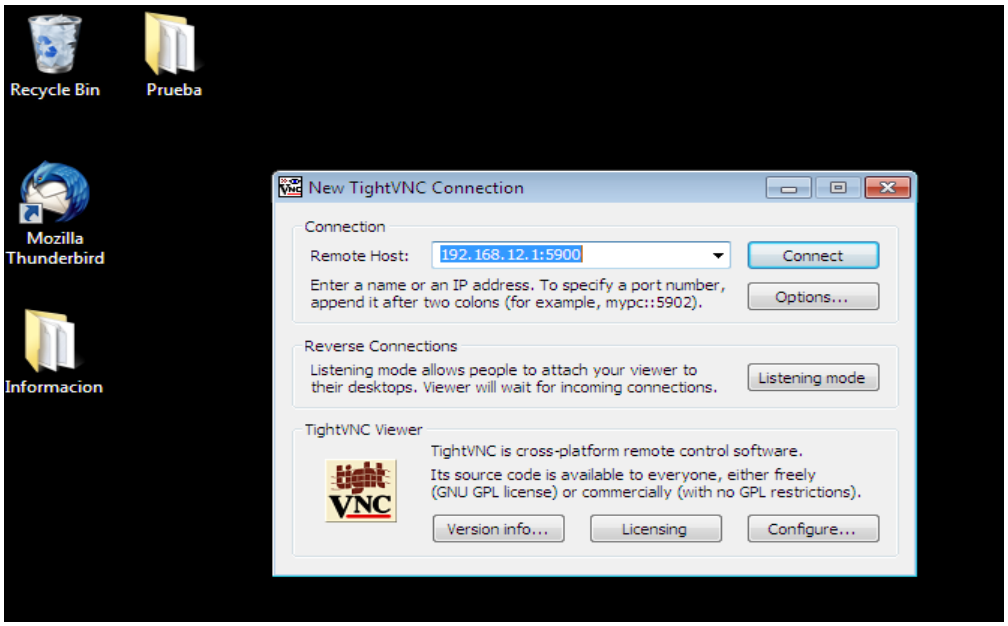

Figura 4. 6 Conexión al servidor usando TightVNC

Conexión al servidor utilizando TigerVNC la Figura 4.7 muestra la petición de conexión.

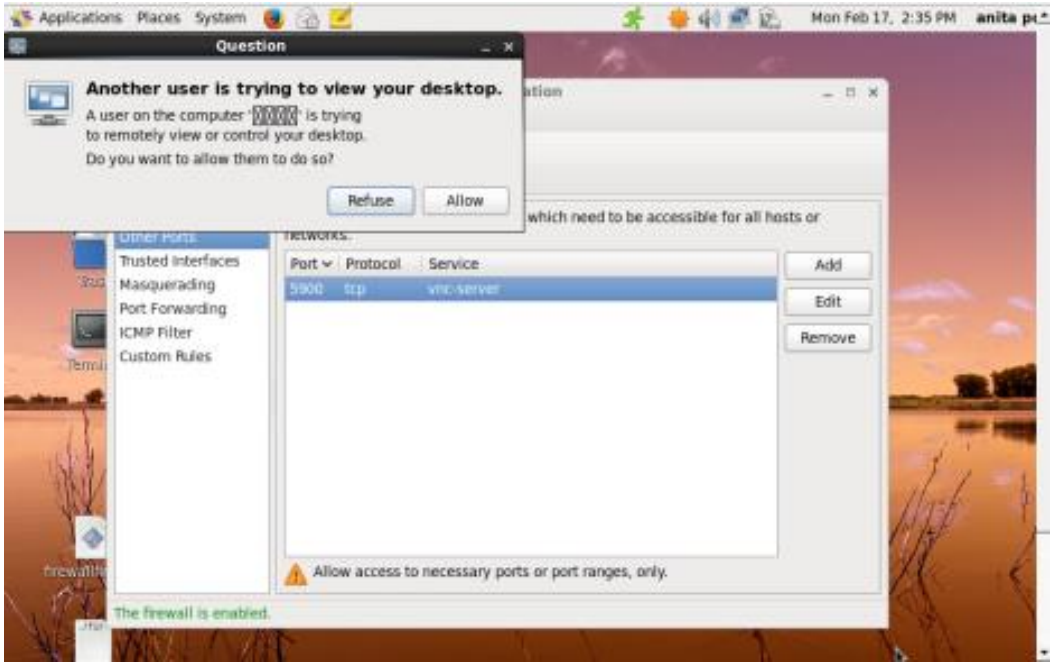

Figura 4. 7 Petición de conexión a escritorio remoto

Luego de permitir la conexión se muestra la siguiente imagen Figura 4.8 de espera de la conexión remota con el servidor.

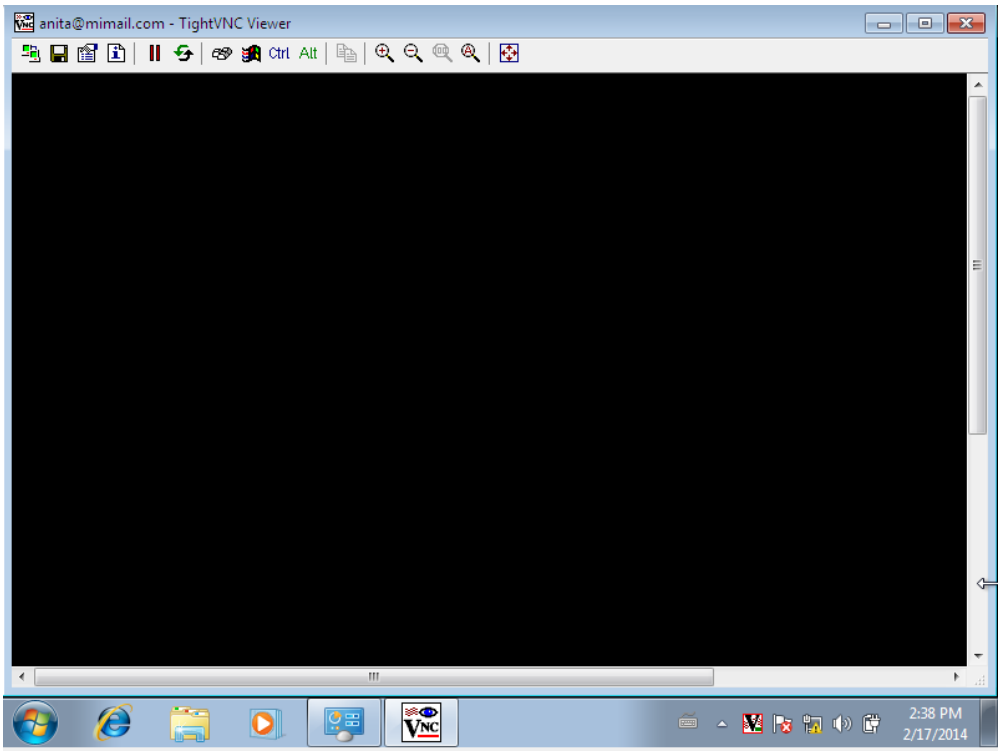

Figura 4. 8 Vista de espera de conexión al servidor

Conexión remota activa entre las dos máquinas usando el protocolo SSH mediante la utilización de los dos programas TigerVNC y TightVnc como lo muestra la Figura 4.9

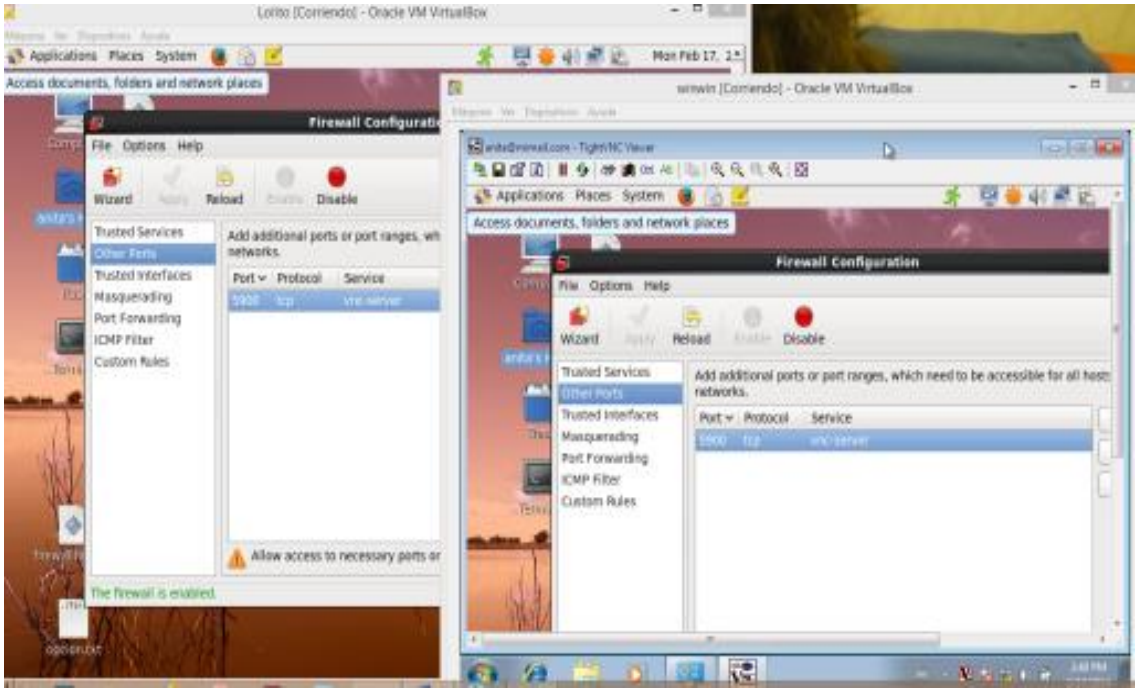

Figura 4. 9 Vista de conexión entre máquinas por escritorio remoto

4.4.3 Visita de páginas web solo del ministerio de salud

Mediante el uso de squid bloquearemos las páginas no autorizadas por la directiva del distrito y solo navegaremos en la paginas del gobierno figura 4.10 mediante las políticas usaremos el uso de navegación por el puerto 8080.

Figura 4. 10 Página web del Ministerio de Salud

4.4.4 Prueba de intruso haciendo ping al host Windows 7 del distrito

Prueba al tratar de hacer un ping a la maquina host dentro del distrito con una maquina intruso Figura 4.11 con la dirección 10.10.10.1/24 con la política agregada de que ningún host fuera del rango de direcciones del distrito pueda hacer ping a las máquinas de su red.

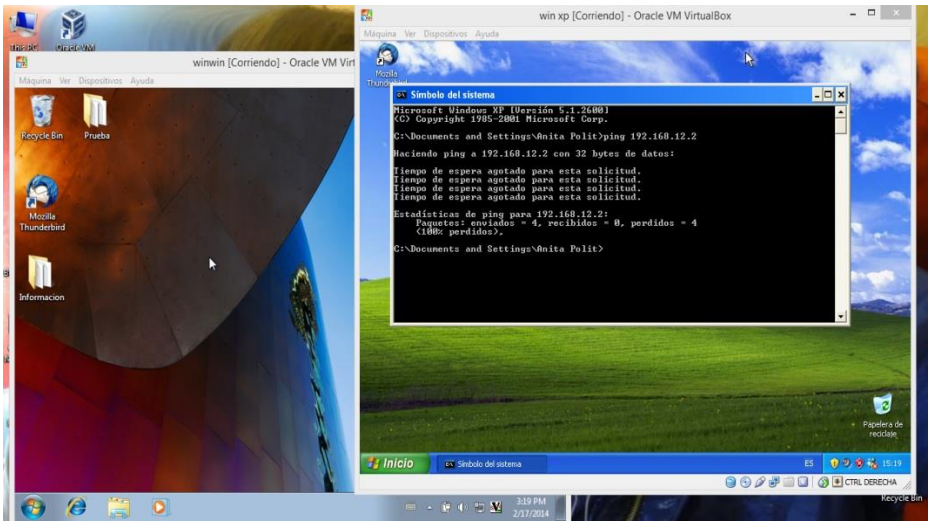

Figura 4. 11 Prueba de ping desde máquina intruso a equipo de la red

4.4.5 Prueba del intruso haciendo ping a la maquina servidor del distrito

Prueba al tratar de hacer un ping al servidor del distrito con una máquina intruso Figura 4.12 con la dirección 10.10.10.1/24 con la política agregada de que ningún host fuera del rango de direcciones del distrito pueda hacer ping a las máquinas de su red.

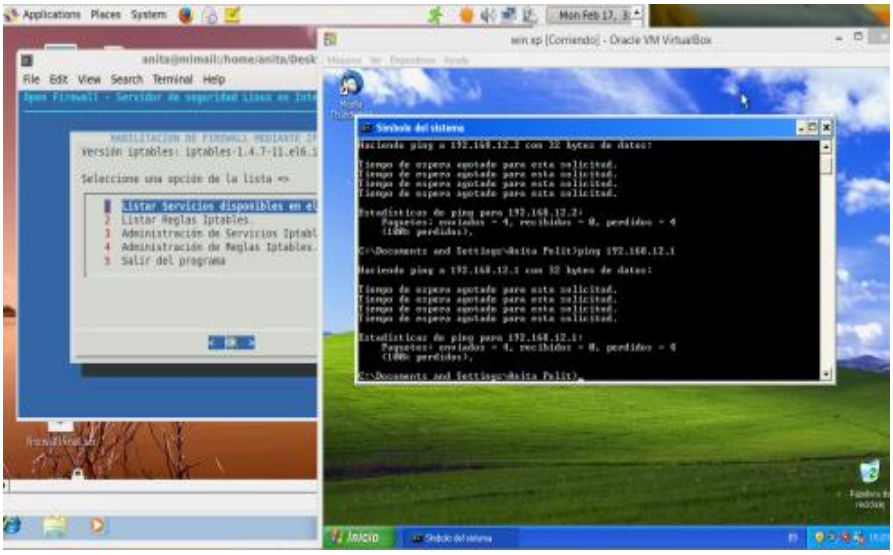

Figura 4. 12 Prueba de ping desde maquina intruso al Servidor

CONCLUSIONES Y RECOMENDACIONES

El crecimiento actual de las redes y el uso de computadoras ha generado también que hallan fallas de seguridad creciendo conjuntamente con los cambios que hay día a día.

1. La mejor forma de estar protegidos dentro de nuestras empresas es tener un sistema que nos proteja de ataques y de esta forma no se roben información confidencial. Es por esto que al utilizar un firewall y los distintos sistemas de protección vamos cerrando las vías de las personas mal intencionadas.

2. La seguridad no debería ser un problema, pero como algunos no tienen conciencia ya que son encaminados por la avaricia, por ambición o simplemente por dañar a alguien por competencia entre profesionales hay que estar preparados y proteger los datos de las empresas y no tener grandes pérdidas.

3. Es por esto que con la solución propuesta se cumple en su totalidad con el objetivo propuesto del Distrito de Salud de Jipijapa. Ya que al utilizar las soluciones Open source generamos un gran ahorro de costo con respecto a las distintas soluciones comerciales que existen en el mercado.

Es recomendable seguir los siguientes puntos como consideraciones a tener para la integración y el uso de la herramienta:

1. Todas las herramientas utilizadas en esta tesina de seminario de grado han sido de código abierto, demostrando la compatibilidad entre ellas y consistencia durante el desarrollo de esta tesina de seminario. No se presentó ningún problema de conexión y nos permitió explorar las bondades de trabajar con software de código abierto.

2. Para poder trabajar con el sistema, es necesario definir políticas y procedimientos de seguridad dentro de la empresa. Esto es una iniciativa para la protección de la información.

3. Se recomienda capacitar al personal encargado del mantenimiento de la solución Firewall de la empresa, que se requiere conocimientos técnicos para saber manejar el Firewall.

4. Se recomienda mantener actualizado los paquetes y las reglas conjunto con un cambio de claves cada cierto tiempo de archivos compartidos debido a que se puede registrar un ataque si el sistema está desprotegido.

ANEXOS

ANEXO A
Decreto del gobierno al ministerio de salud

Ministerio de Salud Pública

No 00002880

LA MINISTRA DE SALUD PÚBLICA

CONSIDERANDO:

Que; la Constitución de la República del Ecuador reconoce a la salud como un derecho que garantiza el Estado, cuya realización se vincula al ejercicio de otros derechos, entre ellos el derecho al agua, la alimentación, la educación, la cultura física, el trabajo, la seguridad social, los ambientes sanos y otros que sustentan el buen vivir.

El Estado garantizará este derecho mediante políticas económicas, sociales, culturales, educativas y ambientales; y el acceso permanente, oportuno y sin exclusión a programas, acciones y servicios de promoción y atención integral de salud, salud sexual y salud reproductiva. La prestación de los servicios de salud se regirá por los principios de equidad, universalidad, solidaridad, interculturalidad, calidad, eficiencia, eficacia, precaución y bioética, con enfoque de género y generacional.";

Que; mediante Decreto Ejecutivo No. 1014 de 10 de abril de 2008, publicado en el Registro Oficial No. 322 de 23 de los mismos mes y año, se establece como política pública para las Entidades de la Administración Pública Central, la utilización de Software Libre en sus sistemas y equipamientos informáticos;

Que; el Estatuto Orgánico de Gestión Organizacional por Procesos del Ministerio de Salud Pública, emitido mediante Acuerdo Ministerial No. 00001034 de 1 de noviembre de 2012, dispone como misión de la Dirección Nacional de Tecnologías de la Información y Comunicaciones: "Proponer, implementar y administrar políticas, normas y procedimientos que optimicen la gestión y administración de las tecnologías de la información y comunicaciones (TIC's), garantizando la integridad de la información, optimización de recursos, sistematización y automatización de los procesos institucionales, así como el soporte tecnológico institucional";

Que; se hace necesario emitir lineamientos que, en base a las disposiciones legales vigentes permitan el adecuado uso de los servicios de red e informáticos del Ministerio de Salud; y,

Que; mediante Memorando No. MSP-DNTIC-1226-2012 de 5 de diciembre de 2012, el Director Nacional de Tecnologías de la Información y Comunicaciones, solicita la elaboración del presente Acuerdo Ministerial.

EN EJERCICIO DE LAS ATRIBUCIONES LEGALES CONCEDIDAS POR LOS ARTICULOS 151 Y 154, NUMERAL 1 DE LA CONSTITUCIÓN DE LA REPÚBLICA DEL ECUADOR Y POR EL ARTÍCULO 17 DEL ESTATUTO DEL RÉGIMEN JURÍDICO Y ADMINISTRATIVO DE LA FUNCIÓN EJECUTIVA

ANEXO B

CODIGO FUENTE DE LA APLICACIÓN

```
#!/bin/bash
ADMIN="root"
DOMAIN="mimail.com"

###################################
# FUNCTION FOR DIFFERENTS PROCESS #
#################################################################
####################
# FUNCIONES PARA PROTOCOLO/PUERTO IP_ORIGEN/DESTINO
INTERFAZ_ENTRADA/SALIDA ACCION
#################################################################
####################


ip_prot () {


#################################################################
    # Funcion que permite ingresar el puerto origen o destino
segun sea el caso
    # recibe como parametro una parabra clave que indica si se
trata del puerto
    # origen o destino

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

    ip_port () {
      dr=$1 ; local rsp=$2
      dir=$( [[ $dr == "--sport" ]] && echo "ORIGEN" || echo
"DESTINO" )
      fleg=""
      while : ; do
        clear
     #Linea modificada adicionada para enviarla a la funcion
opts_menu este serÃ¡ el titulo
        #de la ventana a mostrar
     ms="DEFINA EL PUERTO $dir"

        local menu=(
          "Ingresar el puerto"
          "Todos los puertos (por defecto)"
        )
        opts_menu menu[@] opt ms
```

```
        case $opt in
          1) while : ; do
               clear
               #linea modificada: se uso una instrucciÃ³n
dialog, un cuadro de dialogo inputbox para
               #aceptar el ingreso del puerto por parte del
usuario
           fopt=$(dialog --clear --title "Ingreso de puerto" -
-nocancel --inputbox --stdout "Nota: Para ingresar un rango de
puertos separelos por : ejemplo. 1024:65535 \nIngrese el
puerto : " 10 60)

               egrep "^[0-9]+(:[0-9]+)?$" <<< "$fopt"
&>/dev/null  && fleg="$dr $fopt" && break
             done
             break;;
          2) fleg="" && break ;; #Si no se ingresa el puerto
entonces se asume vacio este parametro de la cadena
        esac
      done
      #Se almacena el valor del puerto y se retorna
      eval $rsp="'$fleg'" &>/dev/null
    }

    ##############################################
    #Submenu de definicion del puerto
    #Este submenu permite seleccionar si se trara de un puerto
origen o puerto destino
    #Dependiendo de la opcion seleccionada se llama a la
funcion ip_port y se le envia como parametro
    #la palabra reservada --sport o --dport respectivamente
    ##############################################
    menu_port () {
      spawn=$1
      while : ; do
      clear
     #Linea modificada: adicionada para enviar el titulo de la
ventana a la funcion opts_menu
     ms="DEFINA UN PUERTO DE ORIGEN O DESTINO"

        local menu=(
          "Puerto Origen"
          "Puerto Destino"
        )
      opts_menu menu[@] opt ms

      case $opt in
        1) ip_port "--sport" sportt ; break ;;
        2) ip_port "--dport" sportt ; break ;;
```

```
      esac
      done

      eval $spawn="'$sportt'" &>/dev/null
    }

    local rsp=$1

    while : ; do
      clear
     #Linea modificada: adicionada para enviarle a la funcion
opts_menu el titulo de la ventana
     ms="DEFINA UN PROTOCOLO"

        local menu=(
          "TCP"
          "UDP"
          "ICMP"
          "Todos los protocolos (por defecto)"
        )
      opts_menu menu[@] opt ms

      case $opt in
        1) menu_port final_protopoart ; prtt="-p tcp
$final_protopoart" ; break ;;
        2) menu_port final_protopoart ; prtt="-p udp
$final_protopoart" ; break ;;
        3) prtt="-p icmp" ; break ;;
        4) prtt="" ; break ;;
      esac

    done
    eval $rsp="'$prtt'" &>/dev/null
  }



#################################################################
  #FunciÃ³n que muestra por pantalla un submenu con la accion
a tomar con la regla iptable definida
  #dependiendo del tipo de cadena creada se muestra un submenu
o se ingresa nueva informaciÃ³n

#################################################################
  ip_act () {
    dr=$1 ; rsp=$2
    while : ; do
      clear
```

```
      #Esta condicion es el caso de que se trate de una cadena
tipo INPUT, OUTPUT O FORWARD
      if [[ $dr == ARD ]]; then
        clear
     #Linea modificada: adicionada para enviar a la funcion
opts_menu el titulo de la ventana
     ms="DEFINA LA ACCION PARA LA REGLA"

        local menu=(
          "ACCEPT"
          "REJECT"
          "DROP"
        )
        opts_menu menu[@] opt ms

      #En el caso de que se trate de una cadena de PREROUTING
se pasa el control del programa a esta parte
      elif [[ $dr == PRE ]] ; then
        final="DNAT --to-destination" ; flog="" ; opt=""
        while : ; do
           clear
           #Linea modificada: Se muestra un cuadro de dialogo
para aceptar el ingreso de la direccion IP
           #y puerto destino que tomara el paquete

         fopt=$(dialog --clear --title "DEFINA LA DIRECCION
IP:PUERTO DESTINO QUE TOMARA EL PAQUETE" --nocancel --inputbox
--stdout "Nota: Para definir opciones avanzadas tome el
siguiente ejemplo. 192.168.1.1, 10.10.10.10-172.16.1.1,
192.168.1.1/30, 169.254.56.100:80 \nIngrese la direcciÃ³n ip :
" 10 60)

           [[ ${#fopt} != 0 ]] && flog="$final $fopt" && break
        done
      #En el caso de que se trate de una cadena POSTROUTING se
pasa el control del programa a esta parte
      elif [[ $dr == POST ]] ; then
        final="SNAT --to-source" ; flog="" ; opt=""
        while : ; do
           clear
         #Linea modificada: se muestra una caja de dialogo para
aceptar el ingreso de la direccion y
           #Puerto origen que tomara el paquete

         fopt=$(dialog --clear --title "DEFINA LA DIRECCION
IP:PUERTO ORIGEN QUE TOMARA EL PAQUETE" --nocancel --inputbox
--stdout "Nota: Para definir opciones avanzadas tome el
siguiente ejemplo. 192.168.1.1, 10.10.10.10-172.16.1.1,
```

```
192.168.1.1/30, 169.254.56.100:80 \nIngrese la direcciÃ³n ip :
" 10 60)

           [[ ${#fopt} != 0 ]] && flog="$final $fopt" && break
        done
      fi

      [[ ${#opt} != 0 ]] && (( $opt > 0 )) && (( $opt <=
"${#menu[@]}" )) && acx="${menu[$opt-1]}" && break
      [[ ${#flog} != 0 ]] && acx="$flog" && break
    done
    eval $rsp="'-j $acx'" &>/dev/null
  }

  ########################################################
  # Funcion que muestra un submenu para definir la direcciÃ³n
IP, si esta va a ser ingresada
  #o se tomara el valor por defecto que es todas las
direcciones0/0
  ########################################################
  ip_ip () {
    dr=$1 ; rsp=$2 ; flag=""
    dir=$( [[ $dr == "-s" ]] && echo "ORIGEN" || echo
"DESTINO" )
    while : ; do
      clear
     #Linea modificada: adicionada para enviar a la funcion
opts_menu el titulo de la ventana
     ms="DEFINA LA DIRECCION IP $dir"

      local menu=(
        "Ingresar la direcciÃ³n ip"
        "Coincidir con cualquier direcciÃ³n ip(por defecto)"
      )
      opts_menu menu[@] opt ms

      if [[ ${#opt} != 0 ]] && (( $opt == 1 )) ; then
        while : ; do
          clear
          #Linea modificada, el mensaje se paso como texto de
un dialog en funciÃ³n validip
          #echo -e "\n\n\n\n\tNota: La direccion puede ser
escrita con formato CIDR; ej: 192.168.1.1/24\n"
          validip ipp && flag=0 && break
        done
      fi
      [[ ${#flag} != 0 ]] && break
      [[ ${#opt} != 0 ]] && (( $opt == 2 )) && ipp='0/0' &&
break
```

```
    done
    eval $rsp="'$dr $ipp'" &>/dev/null
  }

  ################################################
  #Funcion que muestra un submenu para definir la interfaz, si
esta se trata de una interfaz de entrada
  # o de salida
  ################################################
  menu_interfaces () {
    taran=$1

    while : ; do
      clear
     #Linea modificada adicionada para enviarla a la funcion
opts_menu
     ms="DEFINA UNA INTERFAZ PARA LA REGLA"
      #echo -e "\n\n\t\t## UNA INTERFAZ PARA LA REGLA ##\n"
      local menu=(
        "Interfaz de Entrada"
        "Interfaz de Salida"
      )
      opts_menu menu[@] opt ms

      case $opt in
        1) ip_ifc -i finalin ; eval $taran="'$finalin'"
&>/dev/null ; break ;;
        2) ip_ifc -o finalin ; eval $taran="'$finalin'"
&>/dev/null ; break ;;
      esac

    done
  }

  ################################################################
  #Funcion que muestra un submenu para definir la interfaz de
red, si esta se trata de una interfaz del servidor
  #o si no se especificara este parametro y se asumira la
opcion por defecto
  ################################################################
  ip_ifc () {
    dr=$1 ; rsp=$2
    dir=$( [[ $dr == "-i" ]] && echo "ENTRADA" || echo
"SALIDA" )
    while : ; do
      clear
     #Linea modificada adicionada para enviarla a la funcion
opts_menu
     ms="DEFINA LA INTERFAZ DE RED DE $dir"
```

```
      #echo -e "\n\n\t\t## DEFINA LA INTERFAZ DE RED DE $dir
##\n"
      local menu=(
        "Una interfaz de red del servidor"
        "Todo nombre de interfaz es comparada (por defecto)"
      )
      opts_menu menu[@] opt ms

      if [[ ${#opt} != 0 ]] && [[ $opt == 1 ]] ; then
        while : ; do
          clear
          ifcfg=($(ip link show | awk '/^[0-
9].*/{sub(":","",$2); printf("%s ",$2)}'))
       declare -a args=()  #linea modificada definido para
crear las opciones del menu dialog

          for ((i=0;i<${#ifcfg[@]};i++)) ; do
           args+=("$((i+1))" "${ifcfg[$i]}")   #linea
modificada agrega las interfaz disponibles
          done

     #Linea modificada agregada para mostrar el menu de
seleccion de la interfaz
     dialog --backtitle "Open Firewall - Sistema de Defensa
Perimetral basado en Iptables" --title "INTERFACES
DISPONIBLES" --nocancel --menu "Seleccione una interfaz => " 0
0 0 "${args[@]}" 2>opcion.txt
     opt=$(<opcion.txt)

          [[ ${#opt} != 0 ]] && (( $opt > 0 )) && (( $opt <=
${#ifcfg[@]} )) && ifc="$dr ${ifcfg[$opt-1]}"
          [[ ${#ifc} != 0 ]] && break
        done
        [[ ${#ifc} != 0 ]] && break
      elif [[ ${#opt} != 0 ]] && [[ $opt == 2 ]] ; then
        ifc=""
        break
      fi
    done
    eval $rsp="'$ifc'" &>/dev/null
  }



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

# FUNCIONES PARA CREACION Y ELMINACION DE REGLAS
```

```
# create_rules() recibe como parametro el tipo de tabla a
crear y el tipo de cadena
################################################################
####################

create_rules () {
     tablet="-t $1"
     typot="-A $2"
     #linea modificada se agregaron las lineas input y output
porque de acuerdo a las reglas de iptables
     #cuando es una cadena de tipo Input, forward y prerouting
se ingresa la interfaz de entrada
     #y cuando es una cadena de tipo output, forward y
postrounting la interfaz de salida.
     #se procede a ingresar los parametros para construir la
cadena de la regla de firewall

      [[ $typot =~ INPUT ]] && ip_ifc -i interface
      [[ $typot =~ OUTPUT ]] && ip_ifc -o interface2
      #[[ $typot =~ FORWARD ]] && menu_interfaces interface
      [[ $typot =~ FORWARD ]] && ip_ifc -i interface
      [[ $typot =~ PREROUTING ]] && ip_ifc -i interface
      [[ $typot =~ POSTROUTING ]] && ip_ifc -o interface2
      ip_ip -s source_ip
      [[ $typot =~ FORWARD ]] && ip_ifc -o interface2
      ip_ip -d destination_ip
      ip_prot proto_port
      [[ $typot =~ PREROUTING ]] && ip_act PRE action
      [[ $typot =~ POSTROUTING ]] && ip_act POST action
      if [[ $typot =~ INPUT ]] || [[ $typot =~ OUTPUT ]] || [[
$typot =~ FORWARD ]]  ; then
        ip_act ARD action
      fi

      ################################
      #si existe reglas creadas en esta tabla entonces se le
pregunta al usuario que quiere hacer con la
      #regla creada, aÃ±adirla al final o insertarla antes de
otra regla definida en una tabla especifica
      #Si la tabla no tiene reglas creadas entonces la opcion
por defecto va ser aÃ±adirla.
      ################################

     #se verifica si existen regla en esta tabla y para este
tipo de cadena
     if $(exist_rules $1 $2) ; then
             #Si existen reglas creadas entonces se le pide al
usuario que seleccione que hacer con la
               #Regla creada aÃ±adirla o insertarla
```

```
          dialog --title "CREACION DE REGLA" --nocancel --
menu "QuÃ© desea hacer con la regla creada? " 10 50 2 1
"AÃ±adirla al final de la tabla" 2 "Insertar la regla entre
otras" 2>opcion.txt
          opt=$(<opcion.txt)

          #Si el usuario selecciona insertar la regla
entonces se solicitaran otros parametros al usuario
               if [[ ${#opt} != 0 ]] && [[ $opt == 2 ]] ;
then
               #Se muestra un cuadro de dialogo indicando
como proceder con la insercion de la regla
               #y se muestra el listado de reglas existentes
               dialog --title "INSERTAR REGLA" --msgbox "Para
insertar una regla deberÃ¡ ingresar la posiciÃ³n en la cual
desea insertar la nueva regla. Verifique el listado de reglas
creadas antes de proceder con el ingreso" 10 60
                    views "$1" "$2"
               #Se captura el numero total de reglas
existentes para validar el ingreso
               maximo=$(iptables -t filter -nL INPUT --line-
numbers | tail -1 | awk '{ print $1 }')

               while : ; do

               #Se muestra un cuadro de dialogo para que el
usuario ingrese la posicion en la que se va
               #a ingresar la nueva regla

                    posicion=$(dialog --clear --title
"CREACION DE REGLAS" --nocancel --inputbox --stdout "Ingrese
el nÃºmero de regla(entre 1 - $maximo) sobre la cual desea
insertar la nueva regla creada : " 8 50)
                    typot="-I $2 $posicion"

               #Verifica si la posiciÃ³n ingresada es
correcta, deberÃ¡ estar comprendida
               #entre 1 y el valor maximo de reglas
existentes en esta tabla

               if (( $posicion >= 1 )) && (( $posicion <=
$maximo )) ; then
                    break;
               else
                    ms="Ingreso incorrecto, Ingrese una
posiciÃ³n correcta" ; alert ms
               fi
               done
          fi
```

```
      fi


      #Linea modificada: Se crea la cadena o regla de firewall
      rulet="iptables $tablet $typot $interface $source_ip
$interface2 $destination_ip $proto_port $action"

      while : ; do
        clear
     #Linea modificada: adicionada para enviar a la funcion
opts_menu el titulo de la ventana
     ms="SE APLICARA LA SIGUIENTE REGLA"
     local menu=(
          "Aplicar la regla sin guardar los cambios en el
archivo de configuraciÃ³n"
          "Guardar los cambios en el archivo de configuraciÃ³n
(al hacer esto tambiÃ©n se aplicarÃ¡ la regla)"
          "Volver al menÃº de creaciÃ³n de reglas (la regla se
perdera)"
        )
        opts_menu menu[@] opt ms rulet

        case $opt in
         1)
            $( $rulet ) ;
            ms="La regla fue aplicada correctamente" ; alert
ms ; break ;;
         2)
            $( $rulet ; service iptables save &>/dev/null ) ;
            ms="La regla fue aplicada y los cambios se
guardaron correctamente" ; alert ms ; break ;;
         3) break ;;
        esac
      done
  }

#########################################################
#Funcion que permite eliminar las reglas existentes
#########################################################
delete_rules () {
    tb_tp="${!1}"
    tabb="$(awk '{print $1}' <<< "$tb_tp")"
    typp="$(awk '{print $2}' <<< "$tb_tp")"
    back="${!2}"
    while : ; do
      clear
     #Lineas modificada: Se muestra una ventana para indicar
al usuario como proceder con la eliminacion
```

```
        #de reglas posteriormente se muestra las reglas
existentes para el usuario verifique cual va a
        #proceder a eliminar.
     dialog --title "ELIMINACION DE REGLAS" --msgbox "**
TABLA: $( tr [a-z] [A-Z] <<< $tabb) -> $typp **\n\n Modo de
Uso: \n A continuaciÃ³n se presentarÃ¡ el visor con una lista
de reglas disponibles. Para eliminar una regla ingrese el
nÃºmero de la misma, si desea eliminar varias reglas,
separelas por espacios" 0 0
          views "$tabb" "$typp"

      #Se solicita al usuario el la posiciÃ³n de la regla a
eliminar
      rlz=$(dialog --clear --title "ELIMINACION DE REGLAS" --
nocancel --inputbox --stdout "Para volver al menu $anterior
digite 0\n\nIngrese la(s) regla(s) a eliminar: " 0 0)

     if [[ ${#rlz} != 0 ]] ; then
        [[ $rlz == 0 ]] && break
        #rul=""

        #************************************************
     #Primero se localizan las reglas a eliminar para crear
una cadena de salida con las reglas
        #que van a ser eliminadas
     #************************************************
        declare -a rul=()
     for rl in ${rlz[@]} ; do
       if [[ $rl =~ [1-9][0-9]?+ ]] ; then
           if (iptables -t $tabb -L $typp --line-numbers |
grep ^$rl &>/dev/null) ; then
              rul+=( "$(iptables -t $tabb -nL $typp --line-
numbers | grep ^$rl )" )
            fi
          fi
        done
        #************************************************
     #Luego se procede a eliminar las reglas. La variable
linea_eli permite seleccionar de forma correcta
     #la posicion de la regla a eliminar, principalmente
cuando se trata de eliminacion de varias reglas
     #************************************************
     linea_eli=0
        for rl in ${rlz[@]} ; do
       if [[ $rl =~ [1-9][0-9]?+ ]] ; then
              let rl2=rl-linea_eli

              if (iptables -t $tabb -L $typp --line-numbers |
grep ^$rl2 &>/dev/null) ; then
```

```
              let linea_eli+=1
              $(iptables -t $tabb -D $typp $rl2)
            fi
          fi
        done

        if [[ ${#rul[@]} != 0 ]] ; then
          while : ; do
            clear
          #**************************************
          #Bloque que permite construir el mensaje de salida,
para indicar al usuario cuales son las
          #reglas que han sido eliminadas
          #**************************************
          MSG="$(echo -e "\n##########")"
          MSG="$MSG$(echo -e "\nSe eliminaron las siguientes
reglas : ")"
          MSG="$MSG$(echo -e "\n ")"

          #Linea agregada contador necesario para el el alto
del cuadro de dialogo a mostrar
           numlin=10
          for rl in "${rul[@]}" ; do
              #echo -e "$rl\n"
           MSG="$MSG$(echo -e "\n$rl")"
           let numlin+=1
            done
          MSG="$MSG$(echo -e "\n##########")"
          MSG="$MSG$(echo -e "\n\nÂ¿Desea Guardar los cambios
realizados en el archivo de configuraciÃ³n? ")"
          MSG="$MSG$(echo -e "\n ")"

             #Se muestra un cuadro de dialogo para que el
usuario confirme si desea guardar o no los cambios realizados
          dialog --yes-label "Si" --title "ConfirmaciÃ³n"  --
yesno "$MSG" $numlin 80
          case $? in
                0) $(service iptables save)
                flagger="1"
                ms="Los Cambios se han guardado correctamente"
; alert ms
                ;;
                1|255) flagger="1"
                ms="No se ha guardado ningun cambio" ; alert
ms
                ;;
           esac
           break;
```

```
          done
          [[ ${#flagger} != 0 ]] && break
        fi
      fi
    done
  }


##############################################
# Funcion que muestra los submenu para la creacion y
eliminacion de reglas tipo NAT
##############################################

iptables_nat () {
    act="${!1}"
    tbb="nat"

    while : ; do
      clear
     #Linea modificada: adicionada para enviar a la funcion
opts_menu el titulo de la ventana
     ms="REGLAS IPTABLES (NAT)"

      if [[ "$act" == "-A" ]] ; then
     ms2="CreaciÃ³n de reglas"
        local menu=(
          "Listar reglas habilitadas"
 #         "OUTPUT"
          "PREROUTING"
          "POSTROUTING"
          "Ir al menu anterior"
          "Volver al menu principal"
        )
        opts_menu menu[@] opt ms ms2

        case $opt in
          1) view_all nat ;;
#          2) create_rules $tbb OUTPUT ;;
          2) create_rules $tbb PREROUTING ;;
          3) create_rules $tbb POSTROUTING ;;
          4) break ;;
          5) main_menu ;;
        esac


      else
     #Linea modificada adicionada para enviar a la funcion
opts_menu el titulo de la ventana
     ms2="EliminaciÃ³n de reglas"
```

```
        local menu=(
          "OUTPUT"
          "PREROUTING"
          "POSTROUTING"
          "Ir al menu anterior"
          "Volver al menu principal"
        )
        opts_menu menu[@] opt ms ms2

        tbtp="$tbb ${menu[$opt-1]}"
        lim=${#menu[@]} ; lim1=$(($lim-1))
        [[ ${#opt} != 0 ]] && (( $opt > 0 )) && (( $opt <
$lim)) && flag=$opt || flag="v"

        case $opt in
          $flag ) if $( exist_rules $tbb ${menu[$opt-1]} ) ;
then
                    delete_rules tbtp
                  else
                    ms="No existen reglas configuradas para
esa opciÃ³n!!" ; alert ms
                  fi
                  ;;
          $lim1 ) break ;;
          $lim ) main_menu ;;
        esac
     fi
    done
  }

##############################################
# Funcion que muestra los submenu para la creacion y
eliminacion de reglas tipo MANGLE
##############################################

  iptables_mangle () {
    act="${!1}"
    tbb="mangle"
    while : ; do
      clear

      if [[ "$act" == "-A" ]] ; then

     #Linea modificada adicionada para enviar a la funcion
opts_menu el titulo de la ventana y texto adicional
     ms="REGLAS IPTABLES (MANGLE)"
     ms2="CreaciÃ³n de reglas"
        local menu=(
```

```
          "Listar reglas habilitadas"
          "INPUT"
          "OUTPUT"
          "FORWARD"
          "PREROUTING"
          "POSTROUTING"
          "Ir al menu anterior"
          "Volver al menu principal"
        )
        opts_menu menu[@] opt ms ms2

        case $opt in
          1) view_all mangle ;;
          2) create_rules $tbb INPUT ;;
          3) create_rules $tbb OUTPUT ;;
          4) create_rules $tbb FORWARD ;;
          5) create_rules $tbb PREROUTING ;;
          6) create_rules $tbb POSTROUTING ;;
          7) break ;;
          8) main_menu ;;
        esac

      else
     #Linea modificada adicionada para enviar a la funcion
opts_menu el titulo de la ventana y texto adicional
     ms="REGLAS IPTABLES (MANGLE)"
     ms2="EliminaciÃ³n de reglas"
        #echo -e "\t\t** Eliminacion de reglas **\n"
        local menu=(
          "INPUT"
          "OUTPUT"
          "FORWARD"
          "PREROUTING"
          "POSTROUTING"
          "Ir al menu anterior"
          "Volver al menu principal"
        )
        opts_menu menu[@] opt

        tbtp="$tbb ${menu[$opt-1]}"
        lim=${#menu[@]} ; lim1=$(($lim-1))
        [[ ${#opt} != 0 ]] && (( $opt > 0 )) && (( $opt <
$lim1 )) && flag=$opt || flag="v"

        case $opt in
          $flag ) if $( exist_rules $tbb ${menu[$opt-1]} ) ;
then
                    delete_rules tbtp
                  else
```

```
                    ms="No existen reglas configuradas para
esa opciÃ³n!!" ; alert ms
                   fi
                   ;;
          $lim1 ) break ;;
          $lim ) main_menu ;;
        esac
     fi
    done
  }

##########################################
# Funcion que muestra los submenu para la creacion y
eliminacion de reglas tipo FILTER
##########################################

  iptables_filter () {
    act="${!1}"
    tbb="filter"
    while : ; do
      clear

      if [[ "$act" == "-A" ]] ; then
        #echo -e "\t\t** Creacion de reglas **\n"
     #Linea modificada adicionada para enviarla a la funcion
opts_menu
     ms="REGLAS IPTABLES (FILTER)"
     ms2="CreaciÃ³n de reglas"
        local menu=(
          "Listar reglas habilitadas"
          "INPUT"
          "OUTPUT"
          "FORWARD"
          "Ir al menu anterior"
          "Volver al menu principal"
        )
        opts_menu menu[@] opt ms ms2

        case $opt in
          1) view_all filter ;;
          2) create_rules $tbb INPUT ;;
          3) create_rules $tbb OUTPUT ;;
          4) create_rules $tbb FORWARD ;;
          5) break ;;
          6) main_menu ;;
        esac

      else
```

```
     #Linea modificada adicionada para enviarla a la funcion
opts_menu
     ms="REGLAS IPTABLES (FILTER)"
     ms2="EliminaciÃ³n de reglas"
        local menu=(
          "INPUT"
          "OUTPUT"
          "FORWARD"
          "Ir al menu anterior"
          "Volver al menu principal"
        )
        opts_menu menu[@] opt ms ms2

        tbtp="$tbb ${menu[$opt-1]}"
        lim=${#menu[@]} ; lim1=$(($lim-1))
        [[ ${#opt} != 0 ]] && (( $opt > 0 )) && (( $opt <
$lim1 )) && flag=$opt || flag="v"

        case $opt in
          $flag ) if $( exist_rules $tbb ${menu[$opt-1]} ) ;
then
                    delete_rules tbtp
                  else
                    ms="No existen reglas configuradas para
esa opciÃ³n!!" ; alert ms
                  fi
                  ;;
          $lim1 ) break ;;
          $lim ) main_menu ;;
        esac
     fi
    done
  }

############################################################
# FUNCION PARA ADMINISTRACION DE REGLAS IPTABLES
# Muestra un submenu con los tipos de tablas disponibles para
la creacion de reglas
############################################################
  rules () {
    act="${!1}"
    while : ; do
      clear

     #Linea modificada adicionada para enviarla a la funcion
opts_menu
       [[ "$act" == "-A" ]] && tipomenu="CreaciÃ³n de reglas"
|| tipomenu="EliminaciÃ³n de reglas"
       ms="ADMINISTRACION DE REGLAS IPTABLES -  $tipomenu"
```

```
      local menu=(
        "FILTER"
        "MANGLE"
        "NAT"
        "Ir al menu anterior"
        "Volver al menu principal"
      )
      opts_menu menu[@] opt ms

      case $opt in
       1) if [[ $act == "-A" ]] ; then
             iptables_filter act
           else
             $(exist_rules filter) && iptables_filter act ||
ms="No existen reglas configuradas para esa opciÃ³n!!" ; alert
ms
           fi
           ;;
      2) if [[ $act == "-A" ]] ; then
             iptables_mangle act
           else
             $(exist_rules mangle) && iptables_mangle act ||
ms="No existen reglas configuradas para esa opciÃ³n!!" ; alert
ms
           fi
           ;;
       3) if [[ $act == "-A" ]] ; then
             iptables_nat act
           else
             $(exist_rules nat) && iptables_nat act || ms="No
existen reglas configuradas para esa opciÃ³n!!" ; alert ms
           fi
           ;;
        4) break ;;
        5) main_menu ;;
      esac
    done
  }

#######################################################
#Funcion que muestra un submenu con las opciones para la
administracion de reglas Iptables
#######################################################
  rules_iptables () {
   if service iptables status &>/dev/null ; then
      while : ; do
        clear
     #Linea modificada adicionada para enviar a la funcion
opts_menu el titulo de la ventana
```

```
     ms="ADMINISTRACION DE REGLAS IPTABLES"
        local menu=(
          "Crear reglas"
          "Borrar reglas"
          "Volver al menu principal"
        )
        opts_menu menu[@] opt ms

        if [[ ${#opt} != 0 ]] ; then
         [[ $opt == 1 ]] && flag="-A"
         [[ $opt == 2 ]] && flag="-D"
        fi

        case $opt in
          1) rules flag ;;
          2) rules flag ;;
          3) main_menu ;;
        esac
      done
    else
      ms="Porfavor, inicie el servicio antes de usar esta
opciÃ³n." ; alert ms
    fi
  }

####################################
# FUNCTION IPTABLES ADMINISTRATION #
####################################################################
####################

# FUNCION PARA ADMINISTRAR EL SERVICIO DE IPTABLES

  admin_iptables () {
    while : ; do
      clear

      #Linea modificada adicionada para enviar a la funcion
opts_menu el titulo de la ventana
     ms="ADMINISTRACION DEL SERVICIO IPTABLES"
      if service iptables status &>/dev/null ; then

     ms2="** Iptables actualmente esta ACTIVO! **" #linea
modificada se agrego en reemplazo de echo
        local menu=(
          "Detener Servicio"
          "Restaurar Servicio"
          "Listar reglas habilitadas"
          "Borrar todas las reglas habilitadas (Esta opciÃ³n
no afecta en el archivo de configuraciÃ³n)"
```

```
          "Borrar todas las reglas habilitadas y establecer
polÃticas por defecto"
          "Volver al menu principal"
        )
        opts_menu menu[@] opt ms ms2

        case $opt in
          1) $( service iptables stop &>/dev/null )
             mail="El usuario $USER ha detenido el servicio
iptables"
             mailx -s "HAN DETENIDO EL SERVICIO IPTABLES"
$ADMIN@$DOMAIN <<< "$mail"
             ms="Iptables se ha detenido correctamente" ;
alert ms ;;
          2) $( service iptables restart &>/dev/null )
             ms="Iptables se ha restaurado correctamente" ;
alert ms ;;
          3) stats_iptables ;;
          4)$( iptables -F &>/dev/null )
             ms="Las reglas se han borrado correctamente" ;
alert ms ;;

          5)
          ##FLUSH de reglas
          $( iptables -F &>/dev/null )
          $( iptables -X &>/dev/null )
          $( iptables -Z &>/dev/null )
          $( iptables -t nat -F &>/dev/null )
          #Se establece las politicas por defecto aceptar
          $( iptables -P INPUT ACCEPT &>/dev/null )
          $( iptables -P OUTPUT ACCEPT &>/dev/null )
          $( iptables -P FORWARD ACCEPT &>/dev/null )
          $( iptables -t nat -P PREROUTING ACCEPT &>/dev/null )
          $( iptables -t nat -P POSTROUTING ACCEPT &>/dev/null
)
          dialog --title "ConfirmaciÃ³n de operaciones
realizadas" --msgbox "*** Las reglas se han borrado
correctamente *** \n\nSe ha establecido las siguientes
politicas por defecto ACEPTAR: \n\niptables -P INPUT ACCEPT
\niptables -P OUTPUT ACCEPT \niptables -P FORWARD ACCEPT
\niptables -t nat -P PREROUTING ACCEPT \niptables -t nat -P
POSTROUTING ACCEPT \n\nTodo el trÃ¡fico que entra y sale por
el Firewall se acepta" 0 0 ;;

          6) main_menu ;;
        esac
      else
     #Linea modifica para enviar a la funcion opts_menu un
texto adicional
```

```
     ms2="** Iptables actualmente esta INACTIVO! **"

        local menu=(
          "Iniciar Servicio"
          "Volver al menu principal"
        )
        opts_menu menu[@] opt ms ms2

        case $opt in
        1) $(service iptables start &>/dev/null )
           mail="El usuario $USER ha iniciado el servicio
iptables"
           mailx -s "HAN INICIADO EL SERVICIO IPTABLES"
$ADMIN@$DOMAIN <<< "$mail"
           ms="Iptables se ha iniciado correctamente" ; alert
ms ;;
        2) main_menu ;;
        esac
      fi
    done
  }

############################
# FUNCTION IPTABLES STATUS #
#################################################################
##
# FUNCION PARA PRESENTAR EL ESTADO ACTUAL DEL SERVICIO
IPTABLES
# Dependiendo del tipo de tabla que reciba como parametro
mostrara submenu con los tipos de cadenas
# que se quieran visualizar
#################################################################
##

  view_all () {
    tab="$1"
    if $(exist_rules $tab) ; then
      while : ; do
        clear
     #Linea modificada adicionada para enviar a la funcion
opts_menu el titulo de la ventana y texto adicional
     ms="VISTA DE REGLAS"
     ms2="Tabla: $tab"

        [[ $tab == "filter" ]] && local menu=(
          "Mostrar todo"
          "INPUT"
          "OUTPUT"
          "FORWARD"
```

```
          "Ir al menu anterior"
          "Ir al menu principal"
        )

       [[ $tab == "mangle" ]] && local menu=(
          "Mostrar todo"
          "INPUT"
          "OUTPUT"
          "FORWARD"
          "PREROUTING"
          "POSTROUTING"
          "Ir al menu anterior"
          "Ir al menu principal"
        )

       [[ $tab == "nat" ]] && local menu=(
          "Mostrar todo"
          "PREROUTING"
          "POSTROUTING"
          "OUTPUT"
          "Ir al menu anterior"
          "Ir al menu principal"
        )

        opts_menu menu[@] opt ms ms2
        lim=${#menu[@]} ; lim1=$(($lim-1))
        [[ ${#opt} != 0 ]] && (( $opt > 1 )) && (( $opt <
$lim1 )) && flag=$opt || flag="v"

        case $opt in
          1 ) views $tab ;;
          $flag ) typ="${menu[$opt-1]}" ; views $tab $typ ;;
          $lim1 ) break ;;
          $lim ) main_menu ;;
        esac

      done
    else
      ms="No existen reglas configuradas para esa opciÃ³n!!" ;
alert ms ;
    fi
  }

########################################
# Funcion que permite visualizar por pantalla las reglas
creadas en cada tabla
# el tipo de tabla y tipo de cadenas se reciben como parametro
########################################
views () {
```

```
    tabb="$1" ; typp="$2"
    if $(exist_rules $tabb $typp) ; then

      MSG="$(echo -e
"\n\t##############################################################
")"
      MSG="$MSG$(echo -e "\n\t##       ESTADO DE LAS
CONFIGURACIONES IPTABLES        ##")"
      MSG="$MSG$(echo -e
"\n\t##############################################################
")"
      MSG="$MSG$(echo -e "\n\n\t\tTabla: $tabb\n \n ")"
      MSG="$MSG$(iptables -t $tabb -nL $typp --line-numbers |
sed -r 's/(^\w.*$)/            \1/g')"
      MSG="$MSG$(echo -e "\n ")"

      #Linea modificada en reemplazo de less se utilizo una
instrucciÃ³n de dialog la salida de less
      #se la redirigio a un archivo texto luego ese archivo es
mostrado en una ventana
      less <<< "$MSG" 1>salida.txt
      dialog --title "Estado de las configuraciones IPTABLES"
--textbox salida.txt 20 100

    else
      ms="No existen reglas configuradas para esa opciÃ³n!!" ;
alert ms ;
    fi
  }

  ##########################################
  # Funcion que muestra un submenu para seleccionar el tipo de
tabla de la cual
  # se quiere visualizar las reglas creadas
  ##########################################
  stats_iptables () {
   if service iptables status &>/dev/null ; then
      while : ; do
        clear
     #Linea modificada adicionada para enviarla a la funcion
opts_menu
     ms="VISOR DE REGLAS CONFIGURADAS PARA IPTABLES"
        local menu=(
          "Ver tabla FILTER"
          "Ver tabla MANGLE"
          "Ver tabla NAT"
          "Volver al menu principal"
        )
        opts_menu menu[@] opt ms
```

```
        case $opt in
          1) view_all filter ;;
          2) view_all mangle ;;
          3) view_all nat ;;
          4) main_menu ;;
        esac
      done
    else
      ms="Porfavor, inicie el servicio antes de usar esta
opciÃ³n." ; alert ms
    fi
  }

############################
# FUNCTION SERVICES STATUS #
#############################################################
# FUNCION PARA PRESENTAR SERVICIOS DISPONIBLES EN EL SISTEMA
# En esta funcion se puede personalizar para que el usuario
adicione mas servicios a mostrar
#############################################################
  services () {
    SRVS=(
      "   smb    "
      "  named   "
      "  squid   "
      " sendmail "
      "   sshd   "
      "  httpd   "
    )

    srv_stat () {
      if grep "run" &>/dev/null  <<< $(service $srv status) ;
then
        echo -en "run"
      elif grep "stop" &>/dev/null <<< $(service $srv status)
; then
        echo -en "stop"
      fi
    }

    prot_port (){
      netstat -plan | awk '
                            /'"$srv"'/ && ($1~/^[tu][cd]p/) {
                              if($1=="tcp"){
                                vtcp=$4"  "vtcp;
                              }else{
                                vudp=$4"  "vudp;
                              }
```

```
                                }
                                END {
                                 if( vudp && vtcp ){
                                   printf " tcp -> %s\n",vtcp;
                                   printf "             |
|          | udp -> %s",vudp;
                                 }else if(vtcp){
                                   printf " tcp -> %s",vtcp;
                                 }else if(vudp){
                                   printf " udp -> %s",vudp;
                                 }
                               }
                             '
    }

    #Linea modificada : se crea las cadenas de salida para ser
mostrada en una ventana de dialogo

    MSG="$(echo -en
"\n\t##############################################################
############")"
    MSG="$MSG$(echo -e "\n\t##       ESTADO DE LOS SERVICIOS
DISPONIBLES EN EL SERVIDOR        ##")"
    MSG="$MSG$(echo -e
"\n\t##############################################################
############")"
    MSG="$MSG$(echo -e "\n\n             +--------------------
----------------------------------+")"
    MSG="$MSG$(echo -e "\n             |  NOMBRE  |  ESTADO  |
PROTOCOLO -> DIRECCION:PUERTO  ")"
    MSG="$MSG$(echo -e "\n             +----------------------
----------------------------------+")"

    for srv in "${SRVS[@]}" ; do
      MSG="$MSG$(echo -e "\n             |$srv")|"
        srv=$( tr -d " "<<< $srv)
        if [[ "$(srv_stat)" == "run" ]] ; then
          MSG="${MSG}$(echo -en " RUNNING  |")"
          MSG="${MSG}$(prot_port)"
        elif [[ "$(srv_stat)" == "stop" ]] ; then
          MSG="${MSG}$(echo -en " STOPPED  | - - - - - - - - - -
- - - - - - ")"
        else
          MSG="${MSG}$(echo -en "     **  NOT INSTALLED **
")"
        fi
   done
```

```
    MSG="$(echo -en "$MSG" | sed -r 's/::1:([0-
9]+)/IPv6_Localhost:\1/g;
                                        s/:::([0-
9]+)/IPv6_ALL:\1/g;
                                        s/127.0.0.1:([0-
9]+)/IPv4_Localhost:\1/g;
                                        s/0.0.0.0:([0-
9]+)/IPv4_ALL:\1/g')"
    MSG="$(echo -e "$MSG" | sed -r 's/(((IPv[46]_[Aa-
Zz]+)|([0-9]+\..*[0-9]+)):[0-9]+)/\n             |          |
|   \1/g' )"

    MSG="$MSG$(echo -en "\n             +----------------------
----------------------------------+\n ")"


      #Linea modificada en reemplazo de less de utilizo una
instrucciÃ³n de dialog la salida de less
      #se la redirigio a un archivo texto y el contenido de
este archivo es mostrado en un textbox
      #less <<< "$MSG"
      less <<< "$MSG" 1>salida.txt
      dialog --title "Estado de los servicios disponibles en
el servidor" --textbox salida.txt 20 100

  }

######################
# FUNCTION MAIN MENU #
######################################################
# FUNCION que muestra el menu principal del sistema
######################################################

  main_menu () {
     echo 1 > /proc/sys/net/ipv4/ip_forward
    while : ; do
      clear

      #Linea modificada adicionada para enviar a la funcion
opts_menu el titulo de la ventana y texto adicional
     ms="HABILITACION DE FIREWALL MEDIANTE IPTABLES"
     ms2="VersiÃ³n iptables: $(rpm -q iptables)"
      local menu=(
        "Listar Servicios disponibles en el servidor."
        "Listar Reglas Iptables."
        "AdministraciÃ³n de Servicios Iptables."
        "AdministraciÃ³n de Reglas Iptables."
       )
     opts_menu menu[@] opt ms ms2
```

```
      local opts=(
        "services"
        "stats_iptables"
        "admin_iptables"
        "rules_iptables"
      )
      case_menu opts[@] $opt

    done
  }


#########################
# FUNCTION MENU OPTIONS #
#########################################################
# FUNCION PARA PRESENTAR Y VALIDAR LAS OPCIONES DE LOS MENUS
#########################################################
opts_menu () {
    declare -a fopts=("${!1}")
    local popt="$2"
    declare -a args=()  #definido para crear las opciones del
menu dialog
    msg="${!3}" #linea modificada creado para recibir como
parametro el titulo de la ventana
    msg2="${!4}" #linea modificada creado para recibir como
parametro texto adicional a mostrar
    for ((i=0;i<${#fopts[@]};i++ )) ; do
     args+=("$((i+1))" "${fopts[$i]}")   #linea modificada
agregada las opciones al menu
    done

    #Linea modificada: se agrega la opcion salir del programa
al submenu creado
    args+=("$((i+1))" "Salir del programa") #Esta linea agrega
la opcion de salida al menu
dialog --backtitle "Open Firewall - Servidor de seguridad
Linux en Internet basado en Iptables" --title "$msg" --
nocancel --menu "$msg2\n\nSeleccione una opciÃ³n de la lista
=> " 0 0 0 "${args[@]}" 2>opcion.txt
     fopt=$(<opcion.txt)
     #Linea modificada para mostrar un mensaje temporal, se
modifico la opcion de salida y se reemplazo el mensaje
     #empleando dialog.
     #[[ "$fopt" == '0' ]] && { echo -e "\nSaliendo del
programa..."; sleep 2; clear; exit 0;}
    [[ "$fopt" == $((i+1)) ]] && { dialog --sleep 2 --infobox
"Saliendo del programa ...." 3 40 ; clear; exit 0;}
     eval $popt="'$fopt'" &>/dev/null
```

```
  }


case_menu () {
    declare -a fopts=("${!1}")
    popt="$2"
    for ((i=0;i<${#fopts[@]};i++ )) ; do
      if (( $popt == $i+1 )) &>/dev/null ; then
        $(awk '{ print $1 }' <<< "${fopts[$i]}")
        if [[ $(awk '{print NF}' <<< "${fotps[$i]}") == 1 ]] ;
then
          alert
        fi
        break
      fi
    done
}

########################################
# Funcion para mostrar mensajes de alerta por pantalla
# Recibe como parametro el mensaje a mostrar
########################################
alert () {
    msg="${!1}" ; [[ ${#msg} != 0 ]] && dialog --msgbox "$msg"
6 60
  }


###################################
#Funcion para verificar si existen reglas para una tabla y
tipo de reglas especifica
###################################
  exist_rules () {
    tbba=$1 ; tppa=$2
    if iptables -t $tbba -L $tppa --line-numbers | grep ^[0-
9].* &>/dev/null ; then
      return 0
    else
      return 1
    fi
  }

########################
# FUNCTIONS VALIDATORS #
############################################
# FUNCIONES PARA VALIDAR EL INGRESO DE DATOS DE LAS
DIRECCIONES IP
############################################
validip () {
```

```
    add_cidr () {
      fip=$1
      rang=$(sed -r 's/([0-9]+)\..*/\1/g' <<< $fip)
      if (( "$rang" < "128" )) ; then
        CIDR='\/8'
      elif (( "$rang" >= 128 )) && (( "$rang" < "192" )) ;
then
        CIDR='\/16'
      elif (( "$rang" >= 192 )) && (( "$rang" < "224" )) ;
then
        CIDR='\/24'
      fi
      fip=$(sed -r 's/(.*)/\1'$CIDR'/g' <<< $fip)
      echo $fip
    }

    local lip=$1
    regexp_cidr='^(((25[0-5]|2[0-4][0-9]|[01]?[0-9][0-
9]?)\.){3}(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?))(/(3[0-
2]$|[1-2]?[0-9]$))?$'
#    regexp_ip='^(((25[0-5]|2[0-4][0-9]|[01]?[0-9][0-
9]?)\.){3}(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?))$'
    regexp_ip='^((25[0-5]|2[0-4][0-9]|[01]?[0-9][0-
9]?)\.){3}0$'

    #Linea modificada: se muestra un cuadro de dialogo para
solicitar la direccion IP
    fip=$(dialog --clear --title "DEFINA LA DIRECCION IP" --
nocancel --inputbox --stdout "Nota: La direcciÃ³n puede ser
escrita con formato CIDR; ejemplo: 192.168.1.1/24 \n\nIngrese
una direcciÃ³n ip vÃ¡lida : " 10 60)

    if grep -E "$regexp_cidr" <<< "$fip" &>/dev/null ; then
      grep -E "$regexp_ip" <<< "$fip" &>/dev/null && { nip=$(
add_cidr $fip ) && fip=$nip ;}
      eval $lip="'$fip'"
      return 0
    else
      ms="Esa no es una direccion ip valida." ; alert ms
      return 1
    fi
  }

  validyn () {
      echo -en "\n\tEscoja una opcion (y/n) para continuar: "
; read fopt
      [[ "$fopt" == [YyNn] ]] && return 0 || return 1
  }
```

```
##################
# MENU PRINCIPAL #
#################################################################
#####################
# INICIO DEL PROGRAMA: se verifica que se tenga privilegios de
Root para poder ejecutar eÃ±
# Programa
########################
if id $USER | grep ".*0(root).*" || [[ "$UID" == 0 ]] ; then
      clear
      rpm -q iptables && main_menu || dialog --msgbox "Iptables
no esta instalado en el equipo!" 6 50
else
  clear

  dialog --msgbox "Necesita privilegios de administrador para
usar este script" 6 50
  exit 0 ;
fi
```

BIBLIOGRAFÍA

[1] Debian/Centos Linux OS, Manual de iptables, http://manpages .debian .net/cgi-bin/man.cgi?query=iptables , junio 2012

[2] Altadill Izura, Pello Xavier. , Orden de reglas firewall, http://es.tldp.org/Manuales-LuCAS/doc-iptables-firewall/doc-iptables-firewall-html/ ,julio 2013.

[3] Barrios Dueñas, Joel. , Ejemplo de reglas iptables, http://www.alcancelibre.org/staticpages/index.php/introduccion-iptables
, agosto 2011.

[4] Mosse Michael. , Conceptos de firewall, http://www.alipso.com/28524_ firewalls/ , septiembre 2003.

[5] Rodriguez, Juan. , Tipos de firewall, http://www.tecnologiapyme.com/ productividad/ventajas-al-usar-un-dispositivo-de-proteccion-firewall-en-la-red-de-la-empresa ,febrero 2013.

[6] Search Security, Mejores prácticas para el uso de firewalls, http://searchdatacenter.techtarget.com/es/tutorial/Practicas-recomendadas-de-seguridad-de-firewall-Consejos-de-seguridad-de-red-con-firewall ,abril 2013.

[7] Red Iris, Componentes del firewall, http://www.rediris.es/cert/doc/unixsec/node23.html , julio 2002.

[8] Security Network, Reglas firewall, http://www-01.ibm.com/support/docview.wss?uid =swg216182478 ,marzo 2012.

[9] TechTarget, Tipos de ataques en firewalls, http://searchdatacenter.techtarget.com/es/consejo/Implementacion-de-firewall-para-nuevos-tipos-de-ataques , noviembre 2012.

[10] Bustamante, Rubén. , Seguridad en redes , http://www.uaeh.edu.mx/docencia/icbi/licenciatura/documentos/Seguridad%20en%20redes.pdf , abril 2011.

[11] Díaz Villatoro, Anabella. , Control de acceso a redes , http://www.ufm.edu.gt/pdf/3369.pdf , octubre 2001.

[12] Bravo, Lisa. , Intrusos en firewalls, http://www.anti-spyware-1021.com ,marzo 2013.

[13] Redes Linux, Configuraciones Firewall, http://www.redesymas.org/011/07/ configuracion-de-iptables-firewall-en.html , julio 2011.

[14] GoDaddy Support, Escritorio remoto, http://support.godaddy.com/help/article/6012/setting-up-remote-desktop-for-your-centos-or-fedora-linux-dedicated-server , febrero 2013

GLOSARIO

- **DHCP**: protocolo de red que permite a los clientes de una red IP obtener sus parámetros de configuración automáticamente.

- **Hosting**: Alojamiento web, es el servicio que provee a los usuarios de Internet un sistema para poder almacenar información, imágenes, vídeo, o cualquier contenido accesible vía web.

- **Kernel:** un núcleo o kernel es un software que constituye una parte fundamental del sistema operativo.

- **Open Source:** Código abierto es la expresión con la que se conoce al software distribuido y desarrollado libremente

- **OSI:** Open System Interconnection 'sistemas de interconexión abiertos. Modelo de red descriptivo, es un marco de referencia para la definición de arquitecturas en la interconexión de los sistemas de comunicaciones.

- **Router:** Dispositivo que proporciona conectividad a nivel de red o nivel tres en el modelo OSI.

- **SFPT:** Secure SHell File Transfer Protocol, también conocido como SFTP o Secure File Transfer Protocol) es un protocolo del nivel de aplicación que proporciona la funcionalidad necesaria para la transferencia y manipulación de archivos sobre un flujo de datos fiable

- **Samba:** Samba es una implementación libre del protocolo de archivos compartidos permite interactuar con ambientes Microsoft Windows.

- **SSH:** sirve para acceder a máquinas remotas a través de una red

- **Tigervnc:** servidor de control de escritorio remoto

- **TightVNC:** software libre. Con el cual usted puede ver el escritorio de una máquina remota y controlarlo con tu ratón y teclado locales, al igual que lo haría sentado en la parte delantera de ese equipo.