Firewall – Linux: Una Solución De Seguridad Informática Para Pymes (Pequeñas Y Medianas Empresas)

KELLY JOHANNA MARTÍNEZ MOLINA
Estudiante Ingeniería de Sistemas
Universidad Tecnológica de Bolívar
Cartagena, Colombia
kellymartinez812@hotmail.com

JAVYS PACHECO MENESES
Estudiante Ingeniería de Sistemas
Universidad Tecnológica de Bolívar
Cartagena, Colombia
javispas@hotmail.com

ISAAC ZÚÑIGA SILGADO
Magister Administración de Empresas
Profesor Universidad Tecnológica de Bolívar
Cartagena, Colombia
izuniga@unitecnologica.edu.co

Fecha de Recibido: 04/08/2009
Fecha de Aprobación: 02/12/2009

Resumen

Se facilita una solución de seguridad de red personalizada de muy bajo costo para las pequeñas y medianas empresas, permitiéndoles identificar y afrontar con precisión los riesgos y tener una protección integral y completa. Se detectaron las necesidades que tienen las PYMES y se implementó un Servidor Firewall Linux. Básicamente se configura un host con la herramienta Iptables para definir la reglas de filtrado de paquetes según las políticas de seguridad establecidas para la protección del flujo de datos entre dos redes. Se hizo un análisis funcional al firewall, instalando servicios a los hosts de las redes locales para verificar la veracidad y factibilidad de las reglas configuradas, en el cual el comportamiento del firewall fue muy efectivo de acuerdo a las exigencias de las políticas de seguridad creadas.

PALABRAS CLAVE: Seguridad Informática, Pymes, Firewall, Linux Centos, Iptables.

Abstract

It is facilitates a safety solution of personalized network of very low cost for the small and medium companies, allowing them to identify and to confront accurately the risks and to have an integral and complete protection. The needs of SMEs were detected and implemented a Linux Server Firewall. Basically you configure a host with iptables tool to define packet filter rules according to established security policies to protect the flow of data between two networks. It was done a functional analysis to firewall, installing services to hosts on local networks to verify the accuracy and feasibility of the configured rules, in which the firewall behavior was very effective in accordance with the requirements of established security policies.

KEY WORDS: Security Computer, Smes, Firewall, Linux Centos, Iptables.

1. INTRODUCCIÓN

Internet es una actividad esencial para cualquier negocio hoy en día. Con el uso generalizado del correo electrónico, y de nuevas tecnologías tales como los "mensajes instantáneos", la conexión a Internet resulta fundamental para mantener el contacto directo con los clientes y estar al día en las tendencias de la industria y al tanto de los desarrollos competitivos.

Las redes informáticas son el objetivo de ataques constantes de una variedad de amenazas en continua evolución que afectan al rendimiento, las comunicaciones y la confiabilidad. Actualmente, existen bandas de crimen organizado que utilizan todos los recursos y tecnologías presentes en Internet para garantizar su anonimato y cometer todo tipo de felonías: phishing, pharming, scam, clickfraud, worms, zero-day exploits, spam, ataques de denegación de servicio distribuidos (DDoS) y un largo etcétera de amenazas a las que todos somos vulnerables[1].

Un Cortafuegos o Firewall es un dispositivo de hardware o una aplicación de software diseñado para proteger los dispositivos de red de los usuarios externos de la red y/o de aplicaciones y archivos maliciosos, gestionándolo de acuerdo a unas determinadas políticas de configuración. Entre sus funciones se destacan los bloqueos de paquetes que se originan en determinado rango de IP, puertos y direcciones de correo, entre otros. También se utiliza como herramienta de defensa (contra virus, gusanos y spam), de análisis forense y del comportamiento de sistemas y redes.

Existen en el mercado algunas soluciones (hardware y software) específicas para proporcionar a las pequeñas y medianas empresas la mejor protección posible de información. Estas propuestas se han diseñado para reducir los costos, los riesgos y la complejidad, pero aún siguen estando fuera del alcance presupuestal de estas compañías. A lo anterior se suma, que estas familias de dispositivos continúan siendo difíciles de gestionar e ineficientes contra el mal uso de los recursos de la red.

En el presente estudio se recomienda una solución de seguridad informática, especialmente para ayudar a las PYMES que cuentan con poco personal de TI para afrontar el reto de proteger sus redes. Se trata de un firewall bajo el sistema operativo Linux de licencia GNU como es la distribución Centos (es un clon a nivel binario de la distribución Linux Red Hat Enterprise Linux) [1]. Es una herramienta de fácil manejo que combina funciones de prevención de intrusiones y capacidades de filtrado de contenido, entre otras opciones; independientemente de si las amenazas se originan internamente o externamente, tanto en la capa de la red como en la de la aplicación.

La implementación de este firewall funciona bajo la configuración de reglas de filtrado basándose en las políticas de seguridad como es Iptables[2] [2]. Se obtuvo un resultado positivo en la comprobación de estas reglas, de igual forma se definieron las salidas hacia la red externa indicando los puertos de salida de la conexión de los hosts y así evitar toda comunicación indeseable hacia el exterior.

El artículo está organizado de la siguiente manera: la sección 2, está dedicada a la elaboración del estado de arte; la sección 3, titulada Materiales y Métodos, describe la metodología y los materiales utilizados en la implementación de un Servidor Firewall en Linux; la sección 4, describe los experimentos y resultados obtenidos en la implementación; y en la sección 5, se evidencian las conclusiones y recomendaciones para futuros trabajos.

2. ESTADO DEL ARTE

Existe una serie de sucesos que determinaron la necesidad de crear alternativas de protección frente a ataques que amenazaron la privacidad de algunas organizaciones. Por mencionar algunos: el ex presidente de EE UU, Ronald Reagan, filtró deliberadamente tecnología defectuosa a la URSS para sabotear sus industrias claves; Kevin Mitnick, un hacker que evadió a la policía, al FBI y a los US Marshall durante 2 años; Carnivore un programa del FBI de los Estados Unidos que espía a los usuarios de Internet [3].

Hoy en día las técnicas de espionaje se han perfeccionado tanto que cualquier medio puede ser portador de un código maligno que amenace nuestra privacidad. Desde recibir un e-mail hasta recibir ataques premeditados son peligros que ponen a prueba nuestra capacidad de respuesta ante la peor situación.

En febrero del presente año, tres de las principales consultoras internacionales (Price Water House Cooper, Ernst & Young y Deloitte) especializadas en realizar estudios sobre distintos aspectos de la información,

1 BARROSO David, Suites de Seguridad [En línea]http://www.revistanex.com/downloads.asp>[Citado en agosto 13 de 2008]

2 El término "Iptables" hace referencia a una herramienta en línea de comandos usados para configurar reglas de filtrado de paquetes en los kernels de Linux 2.4 y 2.6.

han publicado sus informes sobre el estado global de la Seguridad de la Información a finales de 2008 y principios de 2009[3]. Algunas de las conclusiones: los niveles de seguridad implementados siguen siendo reactivos, necesitando justamente que los procesos implementados deban ser proactivos y que permitan la prevención de problemas, vulnerabilidades y desastres; la información confidencial, privada y personal todavía no cuenta con las medidas de protección adecuadas; los insiders (atacantes internos) son una preocupación cada vez mayor y las compañías deben trabajar más en este aspecto [4].

De acuerdo con los antecedentes históricos mencionados anteriormente y debido a las fallas del sistema junto con las acciones de personas inescrupulosas para obtener información y atentar contra la seguridad de las redes, son algunas razones por las cuales se han aplicado diferentes medidas para obtener protección frente a estas vulnerabilidades.

En el segundo trimestre de 2008, la Asociación Colombiana de Ingenieros de Sistemas – ACIS, publicó los resultados de la investigación "Seguridad Informática en Colombia, tendencias 2008" donde se muestra el panorama colombiano y su futuro. Se da a conocer que la seguridad de la información se ha convertido en un elemento clave para la formalización de las estrategias de negocios en la mediana empresa. Los resultados también presentan el software no autorizado y los accesos no autorizados a la web como las fallas más frecuentes en Colombia. Las cifras del 2008 muestran a los antivirus, las contraseñas, los firewalls de software y hardware como los mecanismos de seguridad más utilizados, seguidos por los sistemas VPN y proxies [5].

Existen soluciones diseñadas para ayudar a enfrentar estos problemas de seguridad en las organizaciones de cualquier tamaño. Las tendencias muestran que los fabricante líderes de networking en el mercado están proporcionando herramientas para las PYMES (empresas que cuentan con poco personal de TI para proteger sus redes frente a amenazas externas) con la mejor protección y máximo rendimiento posible; productos que combinan funciones de firewall de inspección profunda de paquetes, SSL VPN, VPN IPSec, antivirus por capas, antispyware, prevención de intrusiones y capacidades de filtrado de contenido Web, entre otros. Por otro lado, para disminuir la carga administrativa de TI y alcanzar los máximos niveles de desempeño se han creado los firewalls integrados en hardware (gateway routers de cable e inalámbricos, switches y tarjetas PCI) que protegen a los servidores, PCs y portátiles de toda la empresa, dentro y fuera del perímetro corporativo [6] [7] [8].

En términos generales, el panorama mundial muestra que se están desarrollando soluciones de seguridad informática para las pequeñas y medianas empresas que se caracterizan por ser cada vez más fiables y fáciles de gestionar.

También se aprecia que se está reduciendo el costo total de inversión en la implementación de la estrategia de protección del recurso informático, sin embargo el precio de estas herramientas siguen estando por fuera de los alcances presupuestales de estas compañías nacionales de los sectores manufacturero y de servicios. La técnica presentada en este documento describe la implementación de un Firewall bajo plataforma Linux para dar respuesta a los problemas de seguridad informática para las PYMES. Se propone una solución para conectar un pequeño negocio a Internet, con defensa integrada, protección automática contra amenazas y necesidad de inversión y administración casi nulas.

Para la implementación de un Firewall existen algunas arquitecturas para determinar la ubicación del firewall más adecuada, como son: a) Arquitectura de Host de protección: posee un firewall compuesto por un Router para el filtrado de paquetes y un host bastión para el filtrado de conexiones a nivel de circuito y aplicación; b) Arquitectura de subred de protección: posee dos Routers uno externo y uno interno, en medio de estos dos Routers se encuentra la red Zona Desmilitarizada, en este caso sería el host bastión; c) Arquitectura de Host de doble acceso: la red está protegida perimetralmente por un solo Firewall, que protege la red interior de la red exterior en el caso típico de conexión a internet y que tiene instalada dos tarjetas de red [9].

De las arquitecturas mencionadas, la utilizada en el proceso de la implementación de la solución que se propone en este trabajo fue la arquitectura host de doble acceso, ya que el host trabaja hasta capas más altas que los enrutadores y puede realizar un filtrado de paquetes más elaborado.

3 http://blog.segu-info.com.ar/2009/02/publicado-el-boletin-130-14022009.html

3. MATERIALES Y MÉTODOS

La implementación de servidor Firewall en Linux se realizó en las instalaciones del laboratorio de redes de la Universidad Tecnológica de Bolívar en la ciudad de Cartagena de Indias. Se utilizaron dos Routers para simulación de una red WAN, dos Switches para las redes locales, cuatros PC para la simulación de servidores y un host donde se configuró el Firewall.

A continuación se describe los pasos necesarios para la implementación.

1) Diseño topología para la respectiva implementación.

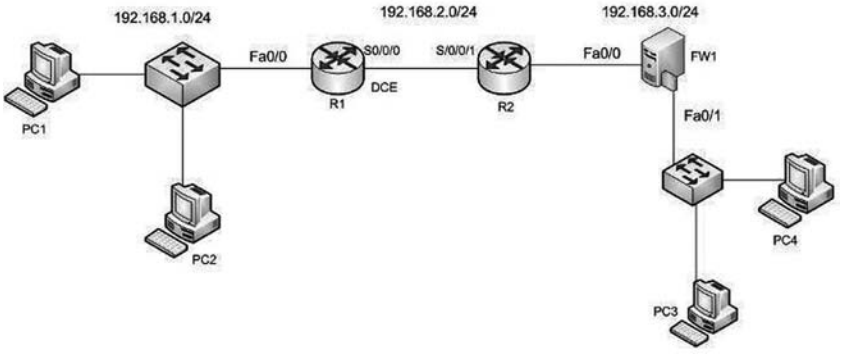

Figura 1. *Topología de Servidor Firewall por el cual el servidor muro cortafuego protegerá la red local donde se encuentra los hosts 3 y 4.*

Es un Firewall de doble acceso, en donde el servidor Firewall tiene dos tarjetas de red, una que comunica con la red externa y otra que comunica a la red local.

En esta arquitectura el tráfico de intercambio entre la red interna y la red externa está sometido a las reglas de un solo firewall, por lo que debe ser lo más robusto posible.

2) Definir las políticas de seguridad para la correcta utilización de los servicios de red como son los protocolos de servicios Web, FTP, Telnet, etc. [10].

Las políticas de seguridad aplicadas para restringir o permitir un acceso a un servicio que se encuentra detrás del muro cortafuego se resumen de la siguiente manera:

- La política por defecto es restringir (denegar) todo servicio, a menos que sea expresamente permitido.
- Cualquier usuario que se encuentra desde la Red Externa puede acceder a un Servicio Web en la red Local, sola accediendo a la IP del Servidor Cortafuego, el cual se encargará de redirigir el tráfico.
- Los servicios (FTP, HTTP, ICMP, etc) están definidos por puertos específicos, cualquiera que se intente acceder por otro puerto diferente, debe ser denegado.
- Desde el Servidor Firewall se puede verificar cualquier problema de comunicaciones con los dispositivos interconectados (hacer ping a los Routers y Hosts) pero no viceversa.

3) Componentes del Sistema Firewall Linux: para implementar el servidor firewall-Linux, inicialmente se debe tener el hardware y software requerido.

Con respecto a los requerimientos del hardware para la instalación del sistema operativo Linux Centos[4] [11] se debe tener un equipo con capacidades muy reducidas (o limitadas), se recomienda un equipo con las siguientes características: Procesador Intel Pentium III / AMD Athlon, 550MHz (o mayor), 512 MB RAM**,** 10 GB en disco duro **y** 2 Interfaz de red.

Dentro del proceso práctico en la implementación del servidor Muro cortafuego se utilizó un ordenador con las siguientes características: Procesador Core 2 Duo, 2.80 GHz, 4 Gb de RAM, 6 Gb en disco duro, 2 interfaz de red marca (Encore y genérica), Cable directo.

La distribución de Linux CentOS cuenta con una serie de paquetes que permiten instalar y configurar los servicios DNS, Firewall, Email y Web, entre otros. La ventaja de instalar un sistema de distribución Linux es la funcionalidad, adaptabilidad y robustez.

4 El término "Linux Centos" se refiere a un clon binario de la distribución Linux Red Hat Enterprise.

4) Configurar la herramienta Iptables en el sistema operativo Centos, el cual es una herramienta que permite hacer filtrado de paquetes y realizar traducciones de direcciones de red (NAT). Iptables permite definir reglas para los paquetes que llegan a nuestra máquina, consultando las reglas del cortafuegos y decide qué hacer con el paquete según dicha regla.

Con Iptables podremos añadir, borrar o crear reglas. Básicamente se divide por las tablas Filter, NAT y Mangle [12] para la tabla filter utiliza las siguientes cadenas:

INPUT: filtrar paquetes que vienen hacia el host.

OUTPUT: filtrar paquetes de salida generados por el host.

FORWARD: filtrar paquetes que llegan al host y lo reenvía por el otro adaptador de red.

Para la tabla NAT utiliza las siguientes cadenas:

POSTROUTING: Enmascara las IPs privadas por la IP pública del Firewall.

PREROUTING: Traduce las direcciones IPs públicas para que pueda acceder a una red interna.

Dentro de las reglas específicas se establecen parámetros entre ellas están:

-A añade una cadena.
-i define una interfaz de tráfico entrante.
-o define una interfaz para tráfico saliente.
-j establece una regla de destino del tráfico, que puede ser ACCEPT, DROP o REJECT.
-m define que regla se aplica si hay una coincidencia específica.
--state define una lista separada por comas de distinto tipos de estados de las conexiones (INVALID, ESTABLISHED, NEW, RELATED).
--to-source define que IP reportar al tráfico externo.
-s define tráfico de origen.
-d define tráfico de destino.
--source-port define el puerto desde el que se origina la conexión.
--destination-port define el puerto hacia el que se dirige la conexión.

5) Configuración de los Scripts Iptables para la creación de las reglas de filtrado de paquetes según las políticas definidas de seguridad. La declaración de un script se hace insertando en la primera línea del Script [13] **#!/bin/sh.**

El **sh** se encarga de leer línea por línea el archivo y ejecutarlo al mismo tiempo.

Declaración de Variables:

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

Ejemplos:

Valor =7

IPT=/sbin/Iptables

EXTIF=”eth1”

IP_EXT= “100.101.102.103”

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

Comentarios:

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

Ejemplo:

Tarjeta de red y dirección IP externa

IP_EXT= “100.101.102.103”

TARJ_EXT=”eth0”

El Script utilizado para la implementación es el siguiente:

```
#!/bin/sh

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

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

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

##Variables

 # Variables Tarjeta de red eth0 y dirección IP

IP_EXT="192.168.3."

TARJ_EXT="eth0"

 # Variables Tarjeta de red eth1 y dirección IP

IP_INT="192.168.4.1

TARJ_INT="eth1"

 # Variables Localhost

IP_LO="172.0.0.1"

ADAP_LO="lo"

##Módulos de Iptables

 # Carga de Módulos

/sbin/depmod –a

#Módulos a cargar

/sbin/modprobe ip_tables
/sbin/modprobe iptable_filter
/sbin/modprobe iptable_mangle
/sbin/modprobe iptable_nat
/sbin/modprobe ipt_LOG
/sbin/modprobe ipt_state

Reglas

echo " Aplicando Reglas del Firewall…"

#Eliminación de cualquier regla existente

iptables −F
iptables −X
iptables −Z
iptables −t nat –F

#Se establece política por defecto

iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP
iptables -t nat -P PREROUTING ACCEPT
iptables -t nat -P POSTROUTING ACCEPT

 # Acceso aplicaciones locales (localhost para conexiones locales)

iptables -A INPUT -i $ADAP_LO -j ACCEPT
iptables -A OUTPUT -o $ADAP_LO -j ACCEPT

 # Establecer NAT solo a los puertos que se necesiten que salgan al exterior. Permite dar puerta de enlace a los host interno, en donde la puerta de enlace enruta los paquetes desde un nodo de la LAN hasta su nodo destino

iptables -A FORWARD -i $TARJ_INT -j ACCEPT
iptables -A FORWARD -o $TARJ_INT -j ACCEPT

 # Se acepta navegar por el protocolo HTTP puerto 80

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

#Se acepta navegar por el protocolo FTP puerto 21

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

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

##Se filtra el acceso de la red exterior a la red local

Redirecciones

Todo lo que venga por el exterior para puerto 80 lo redirigimos a una máquina interna de la red local

iptables -t nat -A PREROUTING -i $TARJ_EXT -p tcp --dport 80 -j DNAT --to-destination 192.168.4.2 [14]

#Los accesos de un IP determinada a FTP se redirigen a una máquina interna de la red local con ese servicio

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

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

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

#Permite hacer ping a la red externa pero no viceversa

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

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

iptables -A INPUT -p tcp --dport 10000 -j ACCEPT
iptables -A OUTPUT -p tcp --sport 10000 -j ACCEPT [15]

 # Habilitar reenvió entre tarjetas de red del Firewall

echo 1 > /proc/sys/net/ipv4/ip_forward
 # Fin del script

El archivo del script anterior deber ser guardado en el fichero raíz /etc/rc.d/ con el nombre rc.firewall y para los permisos de ejecución se debe realizar desde la terminal en modo root la sintaxis de la siguiente manera:

#chmod +x rc.firewall, y para iniciar el Firewall con la nuevas reglas solo es ejecutar el comando desde la misma consola con *service iptables start.*

4. EXPERIMENTOS Y RESULTADOS

En esta sección se comprueba la efectividad de las reglas creadas y experimentadas dentro del laboratorio de redes arrojando resultados satisfactorios, en el cual se simuló con los hosts de las redes locales Servidores Web y FTP permitiendo el tráfico por los puertos 80, 21 y 1024 para el intercambio de archivo servidor-cliente. Se realizaron cuatro experimentos fundamentales como base para la implementación de una infraestructura de redes con alto nivel de seguridad.

1) # Se acepta que se navegue por el protocolo HTTP puertos 80

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

La regla anterior permitió convertir las direcciones privadas de la red local hacía el exterior y también permite la navegación por el protocolo HTTP. Cualquier host que se encuentre dentro de la red local puede navegar por el puerto 80.

Un ejemplo para comprobar la regla es realizar la navegación por algún host, en este caso se realizó el experimento desde el host PC4 que mostró como resultado el acceso de navegación por el puerto 80 hacía el PC2 donde se encuentra instalado un servicio web, este proceso se muestra en la Figura 2.

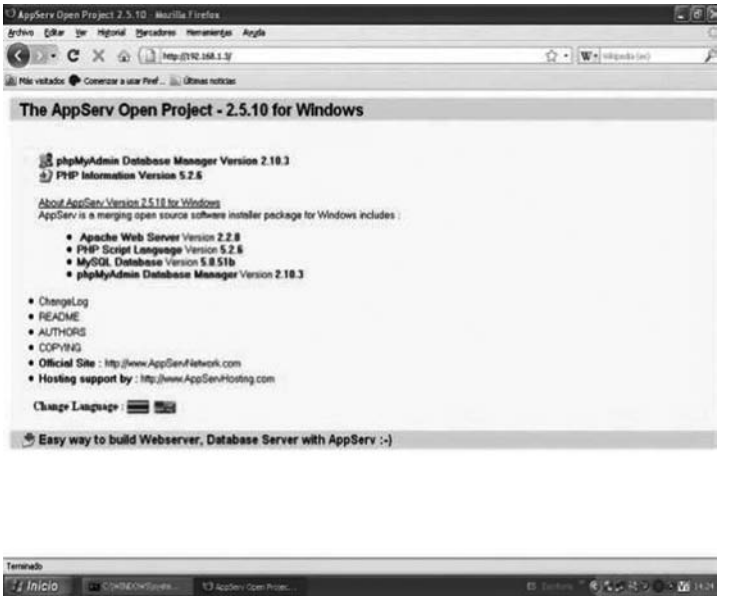

Figura 2. *Navegación puerto 80 desde pc4, en el cual en el navegador se ingresa la Ip donde se encuentra el servicio de web.*

2) # Se acepta que se navegue por el protocolo FTP puertos 21

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

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

La siguiente regla experimentada es para que un usuario pueda acceder a un servidor de transferencia de archivo desde una red local hacia la red externa, en lo cual cualquier host que se encuentra dentro de la red local puede acceder hacia afuera por el puerto 21 y simultáneamente se debe tener el puerto 1024 para que el servidor FTP pueda mostrar los archivos al usuario, este proceso se ilustra en la Figura 3.

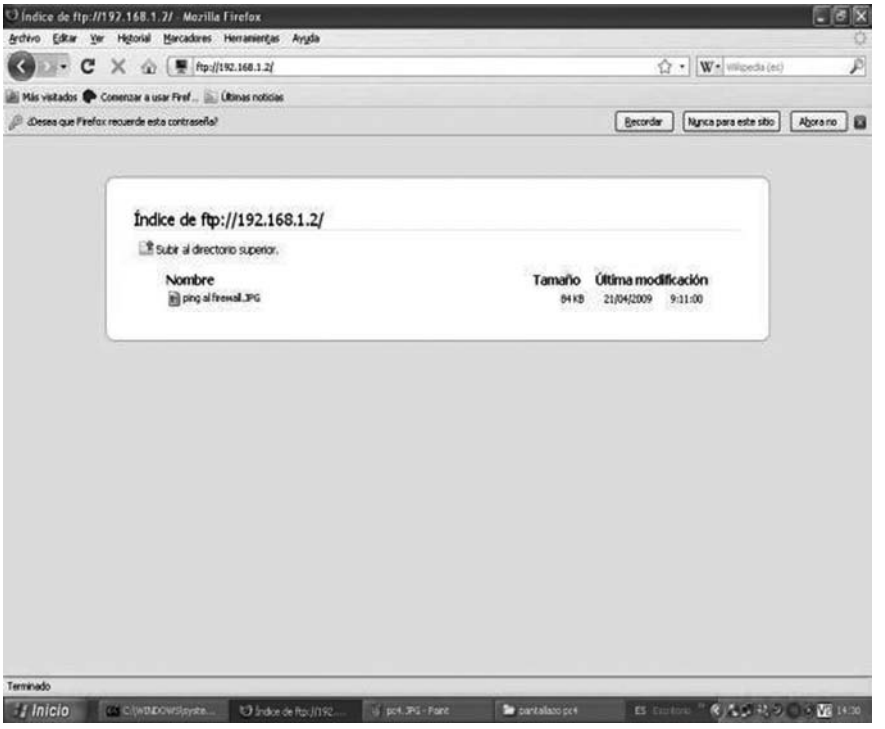

Figura 3. *Acceso al servidor FTP desde PC4, en lo cual se ingresa desde el navegador con el protocolo FTP seguido de la ip donde se encuentra el servidor o el nombre de la página.*

3) #Permitir hacer ping a host de la red local pero no viceversa

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

Con la regla anterior se experimenta el envío de paquetes ICMP desde el Firewall con respuestas desde los host remotos para verificar si hay comunicación en la red; en este caso con los host de la red local. El resultado por el envío de paquetes ICMP con los pings se muestra en la Figura 4.

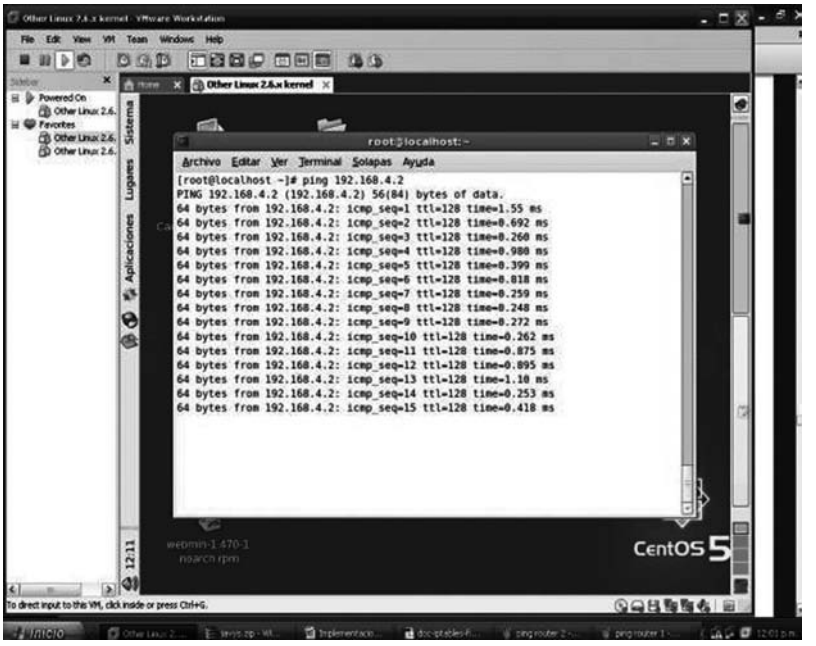

Figura 4. *Ping a host locales desde Firewall, lo cual permite tener más control con las comunicaciones de los diferentes dispositivos interconectados.*

4) #Permitir hacer ping a la red externa pero no viceversa

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

Al igual que la regla anterior esta permite el envío de paquetes ICMP hacia la red externa del experimento realizado. Ver Figura 5.

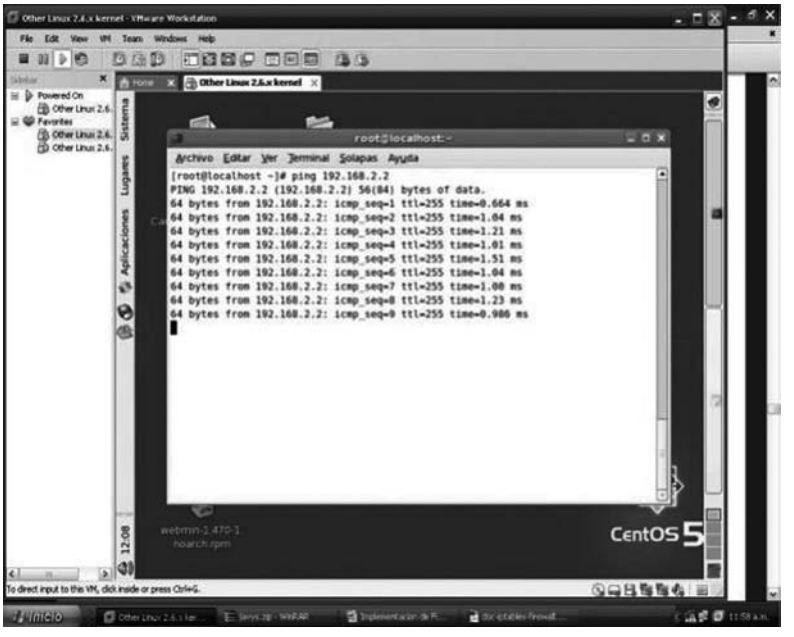

Figura 5. *Ping al Router 2 desde servidor Firewall permite verificar la interconexión de los diferentes dispositivos y así poder tener disponibilidad en los servidores que se encuentra en cada red local.*

5. CONCLUSIONES Y TRABAJOS FUTUROS

A pesar de ser una tecnología relativamente nueva para muchos es poco utilizada, los Iptables como herramienta se convierten en una buena alternativa para implementación de un servidor firewall-Linux como opción específica para aplicaciones de seguridad, ya que por las características de la arquitectura utilizada se hace indispensable que los sistemas sean robustos y seguros.

Esta implementación del servidor Firewall se llevó a cabo en una máquina virtual con el sistema operativo Linux distribución Centos, esto debido a la gran demanda existente en la virtualización de servidores que se están realizando en las empresas, como una medida que permite una reducción de costos y gastos administrativos de TI, una menor inversión en los Hardware, y una mayor optimización de estas herramientas utilizadas a fin que se tenga una estrategia de innovación del proceso de protección de la información en las organizaciones de hoy frente a la inestabilidad económica global.

Para trabajos futuros se puede enfatizar sobre los siguientes ítems los cuales ayudarán en la implementación de servidores firewalls:

- Se puede tomar como base esta investigación para implementar Arquitecturas de red con tres interfaces para la ubicación de posibles servidores en una organización o empresa como son las zonas desmilitarizadas (DMZ).

- Otro aspecto que puede ser complemento de esta investigación son los Firewalls a nivel de aplicación llamados Proxy en donde estos provee aplicaciones específicas de acuerdo con las políticas de seguridad.

- Se puede mejorar los scripts de iptables con las direcciones MAC de cada usuario de la red en el caso que exista servidores DHCP para la asignación de IPs.

6. REFERENCIAS

[1] 3Com Corporation. Seguridad de Redes: Una guía para implementar Firewalls. Disponible en: http://lat.3com.com/lat/technology/technical_papers.html [citado Enero de 2001].

[2] NETFILTER. What is netfilter.org. Disponible en: http://www.netfilter.org [citado Diciembre 2008].

[3] Historia de la seguridad digital. Disponible en: http://www.seguridaddigital.info/index.php?option=com_content&task=view&id=23&Itemid=26 [citado 20 de Enero de 2006].

[4] Segu-Info Estudios e Informes sobre estados globales de la Seguridad de la Información. Disponible en: http://www.segu-info.com.ar/articulos/93-informes-estudios-seguridad-informacion.htm [citado 14 de Febrero de 2009].

[5] J.J. Cano, "Seguridad Informática en Colombia, Tendencias 2008" Revista Sistemas ACIS, vol. 105, Abril – Junio 2008, pp. 38-60.

[6] TREND MICRO Soluciones de seguridad "sin complicaciones" para PYMES – IDG Enterprice. Disponible en: http://www.trendmicro.es [citado 2009].

[7] 3COM Soluciones 3Com para PYMES. Dsponible en: http://www.3com.com [citado 2009].

[8] CISCO SECURITY Reduzca los riesgos de TI. Disponible en: http://www.cisco.com [citado 2009].

[9] Textoscientificos.com, Firewalls Convencionales. Disponible en: http://www.textoscientificos.com/redes/firewalls-distribuidos/firewalls/convencionales [citado 24 de Noviembre de 2006].

[10] M. Hernán D. Universidad Nacional de Lujan. Planes de seguridad. Disponible en: http://www.textoscientificos.com/redes/firewalls-distribuidos/soluciones-seguridad/politicas-seguridad/planes-seguridad [citado 24 de Noviembre de 2006].

[11] CENTOS, Conmmunity Enterprise Operating System. Disponible en: http://www.centos.org/ [citado 2004 - 2009].

[12] P. Fernando, L. Iñaki, G. Jean Paul, R. Antonio. Hacking y Seguridad en Internet. México D.F. Edit. Alfaomega Grupo Editor 2008.

[13] Martínez, J. Tutorial Shell Scripts I. Disponible en: http://observatorio.cnice.mec.es/modules.php?op=modload&name=News&file=article&sid=573 [citado Marzo 25 2008].

[14] UNIVERSIDAD ICESI, Administración de Plataformas y Seguridad. Manual de Configuración de Firewall en Linux. Disponible en: http://www.icesi.edu.co/ocw/tic/administracion_plataformas_y_seguridad/nat-pat-firewall/practica-de-firewall-con-iptables-nat-pat/view [citado 2008].

[15] CENTOS - The Community Enterprise Operating System: IP Tables. Disponible en: http://wiki.centos.org/HowTos/Network/IPTables [citado 8 de Septiembre de 2009].

7. CURRÍCULUM

Javys Pacheco Meneses. En espera de recibir el título como profesional en Ingeniería de Sistemas en la Universidad tecnológica de Bolívar en la ciudad de Cartagena.

En el año 2009, junto con Kelly Martinez culminó el trabajo de grado "Diseño e Implementación de un Servidor Firewall en Linux". Sus campos profesionales de mayor interés son la seguridad informática, administración de redes de computadores, programación en páginas Web y administración de sistemas operativos Linux y Windows.

Kelly Johanna Martínez Molina. En espera de recibir el título que me acredita como Ingeniera de Sistemas en la Universidad Tecnológica de Bolívar en la ciudad de Cartagena.

En el año 2009, junto con Javys Pacheco Meneses, culminó el trabajo de grado "Diseño e Implementación de un Servidor Firewall en Linux". Sus áreas profesionales más fuertes son la programación, el diseño Web, el manejo de base de datos y la administración y seguridad en redes.

Isaac Zúñiga Silgado, Ingeniero de Sistemas de la Universidad Industrial de Santander. Magíster en Administración de Empresas de la Universidad Autónoma de Bucaramanga en convenio con el Instituto Tecnológico de Estudios Superiores de Monterrey (ITESM).

Especialista en Redes de Computadores de la Universidad del Norte de Barranquilla. Se he desempeñado como docente a lo largo de 18 años a nivel universitario. Docente Investigador del Programa de Ingeniería de Sistemas de la Universidad Tecnológica de Bolívar; Miembro grupo de investigación GRITAS, escalafonado A1 convocatoria de Colciencias 2009. Sus áreas de interés investigativa son: La Informática Educativa y la Calidad de los Servicios en las Redes Telemáticas. En la actualidad, se desempeña como Profesor de Tiempo Completo del Programa de Ingeniería de Sistemas de la Universidad Tecnológica de Bolívar - Cartagena de Indias (Colombia).