CAPITULO III

3. PROPUESTA PARA LA REALIZACIÓN DEL DESARROLLO Y PRUEBAS DE LOS SERVIDORES DE PROXY Y FIREWALL EN MAQUINAS VIRTUALES VMWARE

SISTEMA OPERATIVO LINUX

Empezaremos con una rápida pero concreta definición del Sistema Operativo Linux y las bondades que este puede brindar a los usuarios de servidores, al tratarse de un Sistema Open Source ha sido ampliamente difundido a nivel mundial por lo que siempre es interesante realizar un análisis.

Linux es probablemente el acontecimiento más importante del software gratuito desde el original Space War, o, más recientemente, Emacs. Se ha convertido en el sistema operativo para los negocios, educación, y provecho personal. Linux ya no es solo para gurus de UNIX que se sientan durante horas frente a sus computadores personales (aunque le aseguramos que un gran número de usuarios pertenece a esta categoría).

Lo que hace a Linux tan diferente es que es una implementación gratuita de UNIX. Fue y aun es desarrollado por un grupo de voluntarios, principalmente en Internet, intercambiando código, comentando fallos, y arreglando los problemas en un entorno abierto. Cualquiera es bienvenido a sumarse al esfuerzo de desarrollo de

Linux: todo lo que se pide es interés en producir un clónico gratuito de UNIX y algunos conocimientos de programación. El presente tema de investigación es una guía que facilitara algunas de las medidas que se deben tomar para garantizar un normal desenvolvimiento de servicios tanto para compartir recursos como para asegurar de manera optima la información de una empresa o institución.

Para entender de mejor manera realizaremos una rápida reseña histórica:

UNIX es uno de los sistemas operativos más populares del mundo debido a su extenso soporte y distribución. Originalmente fue desarrollado como sistema multitarea con tiempo compartido para mini ordenadores y mainframes a mediados de los 70, y desde entonces se ha convertido en uno de los sistemas mas utilizados a pesar de su, ocasionalmente, confusa interfaz con el usuario y el problema de su estandarización.

Linux es una versión de UNIX de libre distribución, inicialmente desarrollada por Linus Torvalds[1] en la Universidad de Helsinki, en Finlandia. Fue desarrollado con la ayuda de muchos programadores y expertos de UNIX a lo largo y ancho del mundo, gracias a la presencia de Internet. Cualquier habitante del planeta puede acceder a Linux y desarrollar nuevos módulos o cambiarlo a su antojo. El núcleo de Linux no utiliza ni una sola línea del código de AT&T o de cualquier otra fuente de propiedad comercial, y buena parte del software para Linux se desarrolla bajo las

[1] torvalds@kruuna.helsinki.fi.

reglas del proyecto de GNU de la Free Software Foundation, Cambridge, Massachusetts.

Inicialmente, solo fue un proyecto de aficionado de Linus Torvalds. Se inspiraba en Minix, un pequeño UNIX desarrollado por Andy Tanenbaum, y las primeras discusiones sobre Linux surgieron en el grupo de News comp.os.minix. Estas discusiones giraban en torno al desarrollo de un pequeño sistema UNIX de carácter académico dirigido a aquellos usuarios de Minix que querían algo más.

El desarrollo inicial de Linux ya aprovechaba las características de conmutación de tareas en modo protegido del 386, y se escribió todo en ensamblador. Linus dice, "Comencé a utilizar el C tras escribir algunos drivers, y ciertamente se acelero el desarrollo. En este punto sentí que mi idea de hacer un `un Minix mejor que Minix' se hacia mas seria. Esperaba que algún día pudiese recompilar el gcc bajo Linux. . . "Dos meses de trabajo, hasta que tuve un driver de discos (con numerosos bugs, pero que parecía funcionar en mi PC) y un pequeño sistema de ficheros. Aquí tenía ya la versión 0.01 [al final de Agosto de 1991]: no era muy agradable de usar sin el driver de disquetes, y no hacia gran cosa. No pensé que alguien compilaría esa versión." No se anuncio nada sobre esa versión, puesto que las fuentes del 0.01 jamás fueron ejecutables: contenían solo rudimentos de lo que seria el núcleo, y se asumía que se tenia acceso a un Minix para poderlo compilar y jugar con el.

El 5 de Octubre de 1991, Linus anuncio la primera versión "oficial" de Linux, la 0.02. Ya podía ejecutar bash (el shell de GNU) y gcc (el compilador de C de GNU),

pero no hacia mucho mas. La intención era ser un juguete para hackers. No había nada sobre soporte a usuarios, distribuciones, documentación ni nada parecido. Hoy, la comunidad de Linux aun trata estos asuntos de forma secundaria. Lo primero sigue siendo el desarrollo del kernel.

Linus escribía en comp.os.minix,

Tras la versión 0.03, Linus salto a la versión 0.10, al tiempo que más gente empezaba a participar en su desarrollo. Tras numerosas revisiones, se alcanzo la versión 0.95, reflejando la esperanza de tener lista muy pronto una versión "oficial". (Generalmente, la versión 1.0 de los programas se corresponden con la primera teóricamente completa y sin errores). Esto sucedía en Marzo de 1992. Año y medio después, en Diciembre del 93, el núcleo estaba en la revisión 0.99.pl14, en una aproximación asintótica al 1.0. Actualmente, el núcleo se encuentra en la versión 1.1 parche 52, y se acerca la 1.2.[2] [2.1]

Hoy Linux es ya un clónico de UNIX completo, capaz de ejecutar X Window, TCP/IP, Emacs, UUCP y software de correo y News. Mucho software de libre distribución ha sido ya portado a Linux, y están empezando a aparecer aplicaciones comerciales. El hardware soportado es mucho mayor que en las primeras versiones del núcleo. Mucha gente ha ejecutado tests de rendimiento en sus sistemas Linux 486 y se han encontrado que son comparables a las estaciones de trabajo de gama media de Sun Microsystems y Digital. >Quien iba a imaginar que este "pequeño"

[2] En el momento de traducir estas líneas la versión estable del núcleo es la 1.2.13, pero el desarrollo continua por la 1.3.47 en versión beta . . .

[2.1] En estos días (1999) esta disponible la versión 2.2.7 del Kernel

clónico de UNIX iba a convertirse en un estándar mundial para los ordenadores personales?

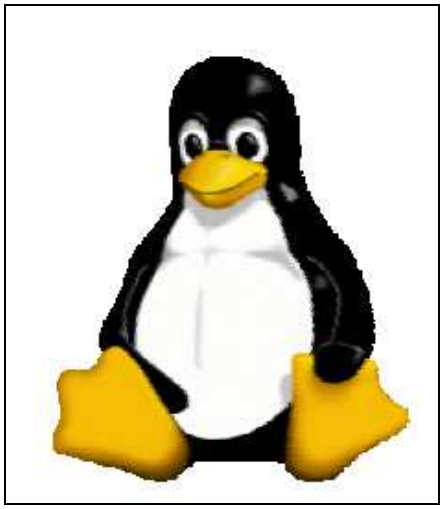


Figura 3.1: Representación Grafica de Linux
Fuente: Grupo Investigador.(www.linux.org)

3.1. Factibilidad

3.1.1. Factibilidad Técnica

El desarrollo de un proyecto en el cual se va a reforzar un departamento de sistemas, y las seguridades de la información es principalmente influenciado por 3 grandes objetivos los mismos que deben ser cumplidos para poder alcanzar la factibilidad técnica:

- Resolver un problema: Esto es cuando ya existe un servidor implementado ya sea para Proxy o firewall y este tiene procesos que ya no satisfacen el desempeño para lo cual fue creado y es necesario hacerles ciertas modificaciones.

- Dar respuesta a directivos: Cuando se hacen modificaciones de tecnología de la información y las comunicaciones y forzosamente es necesario cambiar el sistema de información o hacerle modificaciones que mejore luego aprovechar esta oportunidad ya que, si de por si se va a hacer un cambio de sistema de información se puede hacer el cambio con las nuevas disposiciones legales y con esto seguir siendo competitivo.

- Aprovechar una oportunidad: Un cambio ya sea para ampliar o mejorar el rendimiento económico de la empresa y su competitividad.

Para alcanzar estos objetivos, las empresas emprenden proyectos por una o más de las siguientes razones: capacidad, control, costo, comunicación y competitividad como se lo menciona dentro del Análisis y diseño de Sistemas de Comunicación y Datos.

Capacidad: Las actividades de la empresa están influenciadas por la capacidad de ésta para procesar transacciones con rapidez y eficiencia. Los sistemas de información mejoran esta capacidad en tres formas estas son:

- Aumento de la velocidad de procesamiento.
- Permiten el manejo de un volumen creciente de transacciones.
- Recuperan con rapidez la información.

Control: La falta de comunicación es una fuente común de dificultades que afectan a todos los que laboran en una empresa. Sin embargo, los sistemas de comunicación bien desarrollados tratan de ampliar la comunicación y facilitan la integración de funciones individuales.

Aumento de la comunicación: Muchas empresas aumentan sus vías de comunicación por medios de redes.

Costo: Muchas empresas han desaparecido y muchas otras imposibilitadas para alcanzar el éxito debido al poco control sobre los costos o por el total desconocimiento para el control de estos. Los sistemas de información juegan un papel importante tanto con el control como en la reducción de los costos de operación.

Ventaja competitiva: Los sistemas de información y las comunicaciones son un arma estratégica que puede cambiar la forma en como compite la empresa en el mercado. Los sistemas de información y las comunicaciones mejoran la organización y ayudan a la empresa a ser más competitiva. Por lo contrario si los competidores de la empresa tienen sistemas de información más avanzados, entonces los sistemas de información y comunicación pueden convertirse en una desventaja competitiva. Por lo tanto las capacidades de los sistemas de información son una consideración importante al formular la estrategia de la empresa.

Una empresa puede ganar ventaja competitiva a través de su sistema de información y comunicación en cuatro formas diferentes que garantizan la competitividad en el mercado estos son: clientes, competidores, proveedores y servicios.

Todo proyecto de sistemas de comunicación debe ser desarrollado bajo las actividades de un grupo de trabajo que se haga responsable del inicio y culminación del sistema de información.

El grupo de trabajo va a depender de tamaño de acuerdo al proyecto que va a desarrollarse.

Vamos a mencionar los puestos claves de un grupo de trabajo pero podría ser más grande o mas pequeño o a veces una sola persona puede desarrollar varios puestos, claro como se dijo anteriormente va a depender de esto el tamaño del proyecto. Por tal motivo solo muestra la apreciación personal de acuerdo a la experiencia profesional que se tiene este tema de investigación.

La seguridad, es un aspecto clave para generar en las empresas y en los consumidores la confianza necesaria para que el comercio electrónico se desarrolle. La necesidad de generar confianza, es especialmente importante debido al hecho de que Internet es una red abierta y a la sensación de inseguridad (quizá a veces excesiva) que este hecho genera en los usuarios.

Sin embargo, la seguridad de la red, en este caso Internet, es solo uno de los factores que intervienen en la seguridad del comercio electrónico en conjunto. Más que de la seguridad del pago, los usuarios empiezan a preocuparse sobre todo de problemas como ¿es el vendedor fiable?, ¿podré devolver el producto si no me gusta?, ¿utilizará mis datos personales para enviarme publicidad que no deseo?, ¿cederá esos datos a otras empresas?, en el caso de empresas ¿cuál es la validez de un pedido, factura, etc. hechos electrónicamente?

Así, aunque las características de seguridad de las redes y sistemas de comercio electrónico son, obviamente, muy importantes, el hecho de que los usuarios consideren el comercio electrónico como suficientemente seguro probablemente depende menos de los detalles técnicos, y más de otras cuestiones como la confianza que inspiren las empresas vendedoras, financieras, etc.; la existencia y difusión de normas que, por ejemplo, limiten la responsabilidad del usuario en caso de uso indebido de una tarjeta de crédito y que garanticen su derecho a devolver un producto comprado electrónicamente; la creación de códigos éticos de comportamiento de las empresas y de procedimientos efectivos de solución de conflictos; etc.

Componentes de seguridad

Las condiciones que debe reunir una comunicación segura a través de Internet (o de otras redes) son en general las siguientes:

- Confidencialidad: evita que un tercero pueda acceder a la información enviada.

- Integridad: evita que un tercero pueda modificar la información enviada sin que lo advierta el destinatario.
- Autenticación: permite a cada lado de la comunicación asegurarse de que el otro lado es realmente quien dice ser.
- No repudio o irrefutabilidad: Permite a cada lado de la comunicación probar fehacientemente que el otro lado ha participado en la comunicación. En el caso de no repudio de origen, el remitente del mensaje no puede negar haberlo enviado. En el caso de no repudio de destino, el destinatario del mensaje no puede negar haberlo recibido.

La herramienta básica para cumplir las condiciones anteriores son las técnicas criptográficas, en particular los métodos de cifrado simétrico (usan una misma clave secreta para cifrar y descifrar) o asimétrico (cada usuario tiene una pareja de claves, una pública y otra privada, con la propiedad de que lo que se cifra con una de las claves sólo se puede descifrar con la otra). Para evitar posibles suplantaciones de identidad, es necesario contar con una tercera parte fiable que acredite de forma fehaciente cuál es la clave pública de cada persona o entidad. Esta es la función básica de las autoridades de certificación.

Un certificado digital emitido por una de estas autoridades contiene la identidad de un usuario, su clave pública y otros datos adicionales (por ejemplo, el periodo de validez del certificado), todo ello firmado digitalmente con la clave privada de la autoridad de certificación, con el fin de que el certificado no se pueda falsificar. Pueden existir varios tipos de certificados, válidos para diferentes usos, según la información y garantías que la autoridad de certificación

(directamente o a través de una autoridad de registro) pide al usuario antes de emitir el certificado.

3.1.2. Factibilidad Económica

Al tratarse de seguridades y de compartir recursos como lo es el Internet siempre puede sonar a gastos extremadamente fuertes, pero al tener las empresas e instituciones instalado equipos de ultima generación y en algunos casos configurables como son los casos de las computadores personales que pueden trabajar como servidores claro con la ayuda de las maquinas virtuales VMWARE o en el caso de sistemas operativos como Microsoft crean sus propias maquinas como son el Microsoft Virtual PC.

Al contar con todo implementado nuestro trabajo y el de los administradores de los departamentos de Sistemas fue de otorgar una Maquina Virtual para cada servicio y de está manera se puede asignar puertos y protocolos que va a servir de enlace entre los servidores y los usuarios de la red, cabe recalcar que siempre es bueno tener más de una tarjeta de red la misma que pueden ser asignadas para cada uno de los recursos.

Lo que se desea llegar es a proporcionar a las empresas una alternativa de Intranet a bajos costos utilizando normas y protocolos de Internet, para permitir a los miembros de una organización comunicarse y colaborar entre si con mayor eficiencia, aumentando la productividad.

La factibilidad económica esta dada por la implementación de un corta fuegos(firewall) y un servidor Proxy los mismos que regularían el acceso a la Intranet y el servidor de firewall existente pasaría a controlar tanto interna como externamente.

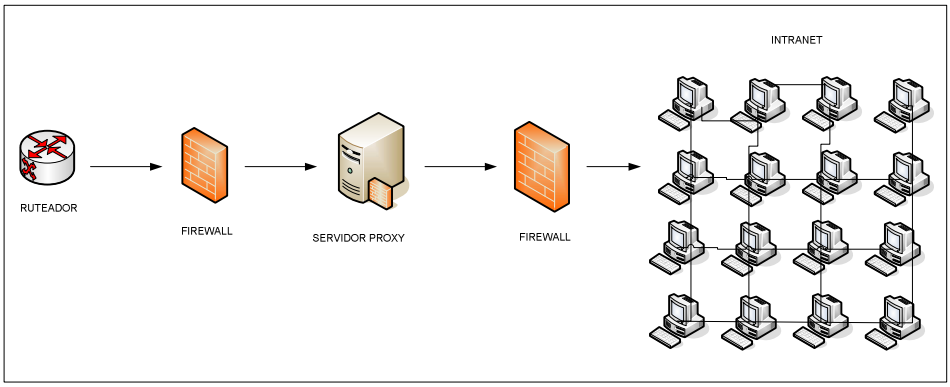


Figura 3.2: Representación Grafica de Factibilidad Económica
Fuente: Grupo Investigador.

3.1.3. Factibilidad Operacional

Un servidor Proxy hace de un portero entre la intranet y el Internet o entre ciertos servidores de archivos y la intranet. Cuando una maquina cliente tiene prohibido solicitar directamente a los servidores en nombre de la maquina cliente. Los servidores Proxy pueden también comprobar el tráfico de entrada. Al igual que en un encaminador, un servidor Proxy verifica las reglas que el administrador ha listado (para ver si el contacto esta autorizado) antes de permitir el paso de trafico. Los servidores Proxy son específicos para las aplicaciones, por ejemplo los servidores Proxy de correo protege al servidor de correo y un servidor Proxy, FTP protege al servidor de FTP.

Los servidores Proxy también pueden inspeccionar el contenido de un paquete y aceptarlo o rechazarlo, según las reglas del administrador. Así, si un servidor Proxy para cualquier servicio contiene una regla de negación, este simplemente niega la acción, así de forma general este diga que se lo debe realizar.

Los servidores Proxy pueden examinar, más cosas que la dirección.

Los intrusos extremos del tipo humano van desde el curioso al maligno y a los individuos motivados por el beneficio económico. En su mayoría, los piratas solían ser estudiosos y experimentados benignos. Los primeros piratas veían el ciberespacio como un lugar público gigantesco de juegos electrónicos y en realidad, más bien como un puzzle absorbente y desafiante. El intento de entrar en un sistema (y salir sin que los atrapasen) era un deporte de competición.

Un intruso puede inyectar un virus o piratear e interceptar, cambiar o robar datos. Y lo hacen. El espionaje industrial es uno de los crímenes informáticos en auge y una vía de ataque.

Todavía hay muchos piratas que pretenden asustar, que se cuelan y miran pero no hacen daño real. Aunque su intrusión es fastidiosa, su principal motivación es la sensación de logro y poder. A su manera, su atención hacia nuestra red puede ser positiva y puede servir para recordarnos que siempre somos vulnerables y para poner de relieve algunas deficiencias especificas en nuestra protección.

3.2. Distribución de equipos en una Red

3.2.1. Acceso Ilimitado a Internet

Hoy en día la gente se encuentra inundada de información y a menudo recibía más de la que podría manejar. El diluvio de información, con más revistas que leer, más publicaciones comerciales a mantener, más anuncios, más llamadas telefónicas y más reuniones, se convirtió en la corriente interminable de los bits de información.

Una de las ventajas es la navegación a altas velocidades sin restricción alguna, pero la seguridad en cambio se ve limitada y puede la empresa ser presa fácil de los piratas electrónicos que podrían incluso desde alterar información hasta perjudicar económicamente a una empresa.

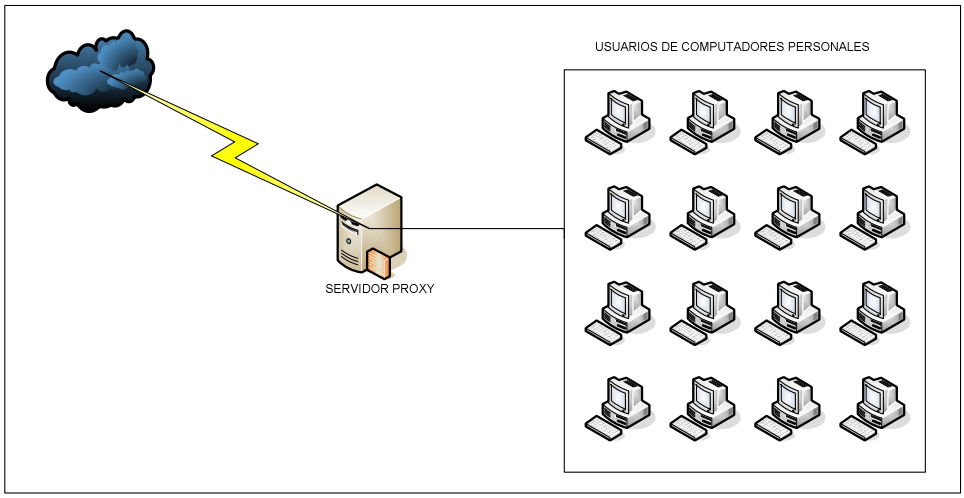


Figura 3.3: Representación Grafica del Acceso Ilimitado a Internet
Fuente: Grupo Investigador

3.2.2. Acceso Limitado a Internet

En este caso vamos a tomar en cuenta las configuraciones que se siguieron para poder configurar el servidor Proxy, el mismo que nos sirvió para distribuir de manera adecuada el ancho de banda como también nos permitió interactuar con un servidor firewall para restringir el acceso libre a nuestra red desde el exterior de la misma.

1. Empezamos cargando Linux con la contraseña del administrador que para el caso del código abierto es el *root,* como podemos observar en el caso del Linux Red Hat Enterprise 5 de 32 bits cuenta con un entorno parecido a todas las versiones de la empresa Red Hat.

Figura 3.4: Representación Grafica del Acceso a Linux Red Hat 5
Fuente: Grupo Investigador

2. El entorno del sistema operativo es el siguiente en el cual, procedemos acudir al Terminal el mismo que nos ayudara para interactuar con el Linux mediante una consola de comandos.

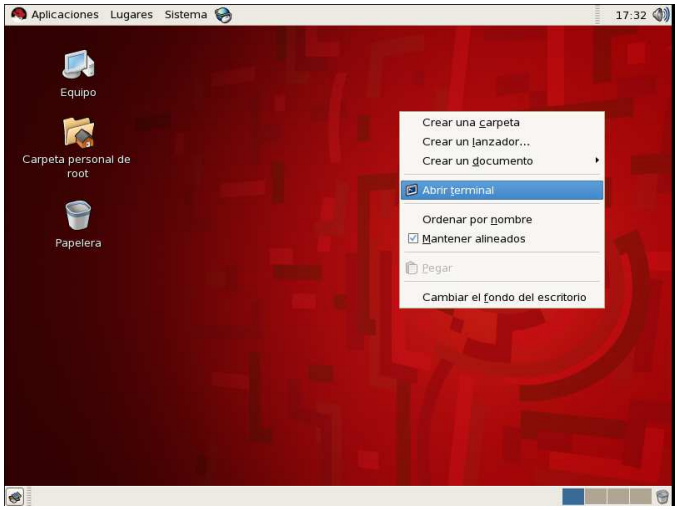


Figura 3.5: Escritorio de Linux Red Hat 5
Fuente: Grupo Investigador

3. En la Terminal, configuramos las tarjetas de red, con las direcciones IP (Internet Protocol), la mascara de subred, la puerta de enlace que va a ser en nuestro caso quien nos va a proveer el servicio de Internet. El comando para está actividad es: *[root@tesis /] setup*

   Una vez puesto este comando obtenemos las siguientes pantallas:

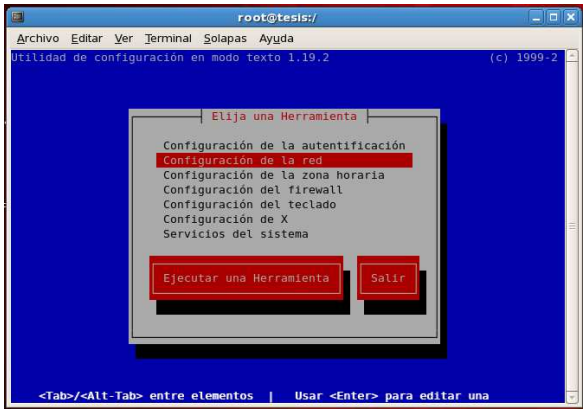


Figura 3.6: Configuración de la red en Linux
Fuente: Grupo Investigador

4. El siguiente paso es configurar o habilitar el servicio del squid, el mismo que nos servirá para poder compartir el recurso de Internet es decir este servicio es del Proxy, el comando para poder habilitar el servicio del squid es:

[root@tesis /] ntsysv; aparece una pantalla en la cual debemos habilitar cualquiera de los servicios que se deseen configurar, para habilitar se debe presionar la tecla de back space.

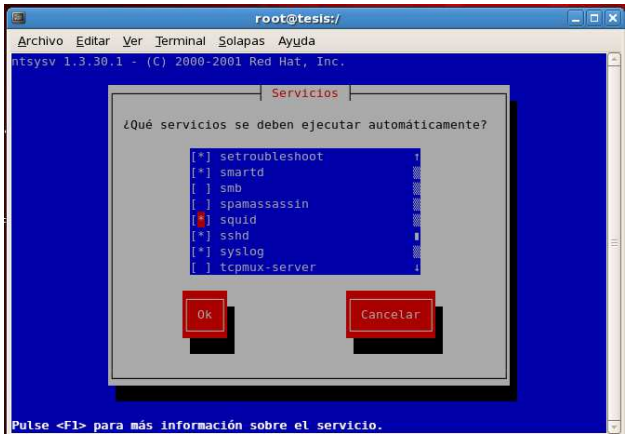


Figura 3.7: Configuración del squid en Linux
Fuente: Grupo Investigador

5. Al ser una pantalla de configuraciones cada uno de los servicios aquí indicados cuentan con sus respectiva ayuda este es el caso por ejemplo del squid, que menciona las bondades que este puede proporcionar.

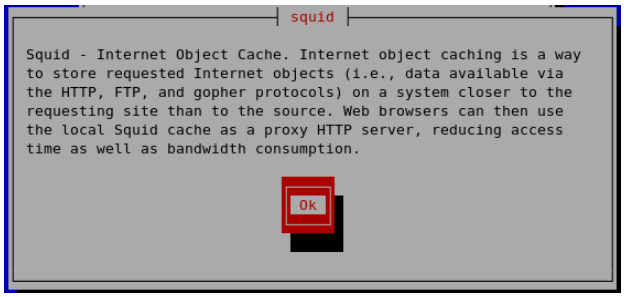


Figura 3.8: Ayuda del squid en Linux
Fuente: Grupo Investigador

6. Con el siguiente extracto podemos ver como se encuentra ya habilitado el servicio del squid y por lo tanto está listo para poder ser configurado y

puesto en marcha de acuerdo a las necesidades que pueda tener una empresa o alguna institución que lo requiera.

Figura 3.9: Comando de verificación de servicio squid
Fuente: Grupo Investigador

7. Una vez habilitado la función del squid como se ve en la grafica anterior, procedemos a mirar si se creo la carpeta y el archivo de configuración dentro de la carpeta que lleva este nombre y que al listarle aparece todos los archivos que tienen.

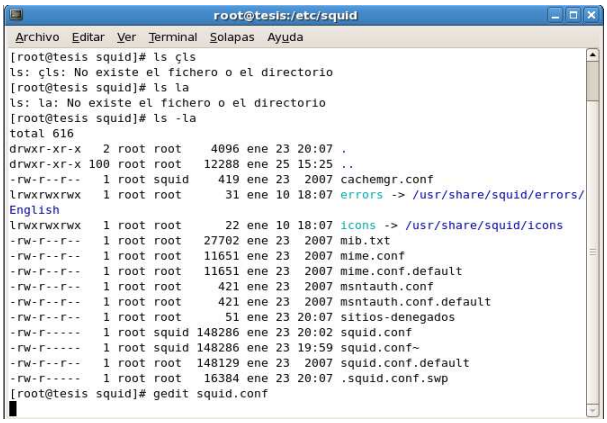


Figura 3.10: Ubicación y privilegios del servicio squid
Fuente: Grupo Investigador

8. Con un editor de texto procedemos a editar las configuraciones del squid.conf, luego de lo cual debemos otorgar a ciertas direcciones IP a las maquinas que van acceder al servicio de Internet, y las maquinas que van a tener las limitaciones, según los perfiles de los usuarios de ser el caso o no.

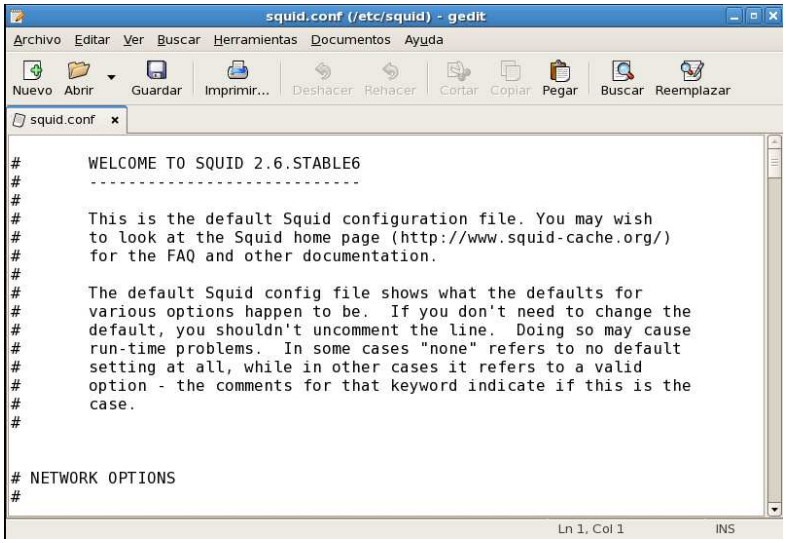


Figura 3.11: Ubicación y privilegios del servicio squid
Fuente: Grupo Investigador

Una parte de la configuración la misma que nos permite conectar detallamos a continuación:

```
#Recommended minimum configuration:
acl all src 0.0.0.0/0.0.0.0
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
acl SSL_ports port 443 563
acl Safe_ports port 80          # http
acl Safe_ports port 21          # ftp
acl Safe_ports port 443 563     # https, snews
acl Safe_ports port 70          # gopher
acl Safe_ports port 210         # wais
acl Safe_ports port 1025-65535  # unregistered ports
acl Safe_ports port 280         # http-mgmt
acl Safe_ports port 488         # gss-http
acl Safe_ports port 591         # filemaker
acl Safe_ports port 777         # multiling http
acl CONNECT method CONNECT
acl Red src 10.0.0.0/255.255.255.0
#Sitios denegados
acl negados url_regex "/etc/squid/sitios-denegados"
#Autentificacion de usuarios
#acl password proxy_auth REQUIRED
#  TAG: http_access
#     Allowing or Denying access based on defined access lists
#
#     Access to the HTTP port:
#     http_access allow|deny [!]aclname ...
#
#     NOTE on default values:
#
#     If there are no "access" lines present, the default is to deny
#     the request.
#
```

```
#      If none of the "access" lines cause a match, the default is the
#      opposite of the last line in the list.  If the last line was
#      deny, then the default is allow.  Conversely, if the last line
#      is allow, the default will be deny.  For these reasons, it is a
#      good idea to have an "deny all" or "allow all" entry at the end
#      of your access lists to avoid potential confusion.
#
#Default:
# http_access deny all
#
#Recommended minimum configuration:
#
# Only allow cachemgr access from localhost
http_access allow manager localhost
http_access deny manager
# Deny requests to unknown ports
http_access deny !Safe_ports
# Deny CONNECT to other than SSL ports
http_access deny CONNECT !SSL_ports
```

3.3. Implementación de seguridades Lógicas mediante Firewall

3.3.1. Local (Interna)

Para garantizar la información interna de una empresa o institución hay que tomar en cuenta tres factores que son decisivos a la hora de implementar seguridades tanto a nivel de red como de servidores. Estos dos factores son:

- Administración del Acceso a Red
- Administración de los privilegios
- Administración de las Contraseñas

3.3.1.1.Administración del Acceso a Red

El acceso a la información y los procesos de negocio debe ser controlados sobre la base de los requerimientos la seguridad y de los negocios.

Se deben implementar procedimientos formales para controlar la asignación de derechos de acceso a los sistemas y servicios de información. Los procedimientos deben comprender todas las etapas del ciclo de vida de los accesos de usuario, desde el registro inicial de nuevos usuarios hasta la privación final de derechos de los usuarios que ya no requieren acceso a los sistemas y servicios de información. Se debe conceder especial atención, cuando corresponda, a la necesidad de controlar la asignación de derechos de acceso de privilegio, que permiten a los usuarios pasar por alto los controles de sistema.

3.3.1.2.Administración de privilegios

Se debe limitar y controlar la asignación y uso de privilegios (cualquier característica o servicio de un sistema de información multi-usuario que permita que el usuario pase por alto los controles de sistemas o aplicaciones). El uso inadecuado de los privilegios del sistema resulta frecuentemente en el más importante factor que contribuye a la falla de los sistemas a los que se ha accedido ilegalmente.

Los sistemas multi-usuario que requieren protección contra accesos no autorizados, deben prever una asignación de privilegios controlada mediante un proceso de autorización formal. Se deben tener en cuenta los siguientes pasos:

a) Deben identificarse los privilegios asociados a cada producto del sistema por ej. Sistema operativo, sistema de administración de bases de datos y aplicaciones, y las categorías de personal a las cuales deben asignarse los productos.

b) Los privilegios deben asignarse a individuos sobre las bases de la necesidad de uso y evento por evento, por ej. el requerimiento mínimo para su rol funcional solo cuando sea necesario.

c) Se debe mantener un proceso de autorización y un registro de todos los privilegios asignados. Los privilegios no deben ser otorgados hasta que se haya completado el proceso de autorización.

d) Se debe promover el desarrollo y uso de rutinas del sistema para evitar la necesidad de otorgar privilegios a los usuarios.

e) Los privilegios deben asignarse a una identidad de usuario diferente de aquellas utilizadas en las actividades comerciales normales.

3.3.1.3.Administración de Contraseñas

Las contraseñas constituyen un medio común de validación de la identidad de un usuario para acceder a un sistema o servicio de información. La asignación de contraseñas debe controlarse a través de un proceso de administración formal, mediante el cual debe llevarse a cabo lo siguiente:

a) requerir que los usuarios firmen una declaración por la cual se comprometen a mantener sus contraseñas personales en secreto y las contraseñas de los grupos de trabajo exclusivamente entre los miembros del grupo (esto podría incluirse en los términos y condiciones de empleo.

b) Garantizar, cuando se requiera que los usuarios mantengan a sus propias contraseñas, que se provea inicialmente a los mismos de una contraseña provisoria segura, que deberán cambiar de inmediato. Las contraseñas provisorias, que se asignan cuando los usuarios olvidan su contraseña, solo debe suministrarse una vez identificado el usuario;

c) Requerir contraseñas provisorias para otorgar a los usuarios de manera segura. Se debe evitar la participación de terceros o el uso de mensajes de correo electrónico sin protección (texto claro). Los usuarios deben acusar recibo de la recepción de la clave (password);

Las contraseñas nunca deben ser almacenadas en sistemas informativos sin protección. Se resulta pertinente, se debe considerar el uso de otras tecnologías de identificación y autenticación de usuarios, como la biométrica, por Ej... verificación de huellas dactilares, verificación de firma y uso de “tokens” de hardware, como las tarjetas de circuito integrado (“chip-cards”).

3.3.2. Externa

Administrar la seguridad de la información dentro de la organización. Debe establecerse un marco gerencial para iniciar y controlar la implementación de la seguridad de la información dentro de la organización.

Deben establecerse adecuados foros de gestión liderados por niveles gerenciales, a fin de aprobar la política de seguridad de la información, asignar funciones de seguridad y coordinar la implementación de la seguridad en toda la organización. Si resulta necesario, se debe establecer y hacer accesible dentro de la organización, una fuente de asesoramiento especializado en materia de seguridad de la información. Deben desarrollarse contactos con especialistas externos en materia de seguridad para estar al corriente de las tendencias de la industria, monitorear estándares y métodos de evaluación y proveer puntos de enlace adecuados al afrontar incidentes de seguridad. Se debe alentar la aplicación de un enfoque multidisciplinario de la seguridad de la información, por ej., comprometiendo la cooperación y colaboración de gerentes, usuarios, administradores, diseñadores de aplicaciones, auditores y personal de seguridad, y expertos en áreas como seguros y administración de riesgos.

Bajo estas premisas nosotras hemos planteado la opción de la implementación de un firewall mediante la utilización de los IPTABLE los mismos que su configuración se asemeja mucho la del squid salvo con algunas actividades que vamos a detallar a continuación:

IPTABLE.

iptables incluye un módulo que permite a los administradores inspeccionar y restringir conexiones a servicios disponibles en una red interna conocido como *seguimiento de conexiones*. El seguimiento de conexiones almacena las conexiones en una tabla, lo que permite a los administradores otorgar o negar acceso basado en los siguientes estados de conexiones:

- NEW. Un paquete solicitando una nueva conexión, tal como una petición HTTP.
- ESTABLISHED. Un paquete que es parte de una conexión existente.
- RELATED. Un paquete que está solicitando una nueva conexión pero que es parte de una conexión existente, tal como las conexiones FTP pasivas donde el puerto de conexión es 20, pero el puerto de transferencia puede ser cualquiera desocupado más allá del puerto 1024.
- INVALID. Un paquete que no forma parte de ninguna conexión en la tabla de seguimiento de conexiones.

Puede utilizar la funcionalidad de vigilancia continua de seguimiento de conexiones de iptables con un protocolo de red, aún si el protocolo mismo es sin supervisión (tal como UDP).

La configuración del Firewall es la siguiente mediante la utilización de los IPTABLES

1. Al igual que la configuración del Proxy se debe acudir al comando

   Ntsysv,

Figura 3.12: Ubicación y privilegios del servicio iptable
Fuente: Grupo Investigador

2. Verificamos si está instalado el servicio mediante el comando *rpm –q iptables,* y este debería darnos la versión del iptable.

3. Las configuraciones que tenemos para la protección de la red quedaría de la siguiente manera;

```
# Política denegar y solo se permitirá pasar por el firewall aquello que
se permita explícitamente.

# Carga del modulo NAT (esto carga también los otros).
modprobe iptable_nat

# Carga de módulos para solucionar problema de FTP en con IPTABLES
modprobe ip_conntrack_ftp
modprobe ip_nat_ftp

# Reseteo de las reglas ( flush )
iptables -F
iptables -t nat -F

# SNAT en POSTROUTONG de la interfase pública (eth0) para los paquetes
# provenientes de 10.0.0.0/23 (red administrativa)
# y 10.0.0.0/23 (red académica)
```

```
iptables -t nat -A POSTROUTING -s 10.0.0.0/23  -o eth0 -j SNAT --to-
source 192.168.0.133
iptables -t nat -A POSTROUTING -s 10.0.0.0/23  -o eth0 -j SNAT --to-
source 192.168.0.133
iptables -t nat -A POSTROUTING -s 192.168.0.153/255.255.255.0 -o eth0 -j
SNAT --to-source 192.168.0.133

#Filtrado de paquetes entre la RED LAN LOCAL y los DMZ.

#iptables -A FORWARD -d 192.168.0.155 -p tcp --dport 80 -j ACCEPT
iptables -A FORWARD -i eth0 -p tcp --dport 80 -j ACCEPT
iptables -A FORWARD -o eth0 -p tcp --dport 80 -j ACCEPT
iptables -A FORWARD -s 10.2.0.0/23 -d 192.168.0.155/29 -p tcp --dport 80
-j ACCEPT
iptables -A FORWARD -s 192.168.0.155/29 -d 10.2.0.0/23 -p tcp --dport 80
-j ACCEPT

# negamos todo

iptables -A FORWARD -d 192.168.0.152/29 -j DROP


# Filtrado de paquetes entre las redes internas eth1 (administrativa)
# y eth2 (academic)

iptables -A FORWARD -i eth1 -o eth2 -d 10.0.0.2 -p tcp --dport 80 -j
ACCEPT
iptables -A FORWARD -i eth2 -o eth1 -s 10.0.0.2 -p tcp --sport 80 -j
ACCEPT
iptables -A FORWARD -i eth1 -o eth2 -d 10.0.0.2 -p tcp --dport 5101 -j
ACCEPT
iptables -A FORWARD -i eth2 -o eth1 -s 10.0.0.2 -p tcp --sport 5101 -j
ACCEPT


# Regla que permite el paso de paquetes de la red administrativa al
Servidor de Internet red académica
iptables -A FORWARD -i eth1 -o eth2 -d 10.0.0.3 -p tcp --dport 80 -j
ACCEPT
iptables -A FORWARD -i eth2 -o eth1 -s 10.0.0.3 -p tcp --sport 80 -j
ACCEPT
iptables -A FORWARD -i eth1 -o eth2 -d 10.0.0.3 -p tcp --dport 3306 -j
ACCEPT
iptables -A FORWARD -i eth2 -o eth1 -s 10.0.0.3 -p tcp --sport 3306 -j
ACCEPT
iptables -A FORWARD -i eth1 -o eth2 -d 10.0.0.3 -p tcp --dport 22 -j
ACCEPT
iptables -A FORWARD -i eth2 -o eth1 -s 10.0.0.3 -p tcp --sport 22 -j
ACCEPT
iptables -A FORWARD -i eth1 -o eth2 -d 10.0.0.3 -p tcp --dport 23 -j
ACCEPT
iptables -A FORWARD -i eth2 -o eth1 -s 10.0.0.3 -p tcp --sport 23 -j
ACCEPT

#negamos todo
iptables -A FORWARD -i eth2 -o eth1 -j DROP
iptables -A FORWARD -i eth1 -o eth2 -j DROP


# Regla que envía los pedidos 192.188.58.157:5101 del firewall
# a 10.0.0.3:5101 en el servidor de la red interna
iptables -t nat -A PREROUTING -i eth0 -p tcp -d 192.168.0.133 --dport
5101 -j DNAT --to 10.0.0.3:5101
```

```
# Activa el reenvié de IP (IP forwarding)
echo 1 > /proc/sys/net/ipv4/ip_forward
```

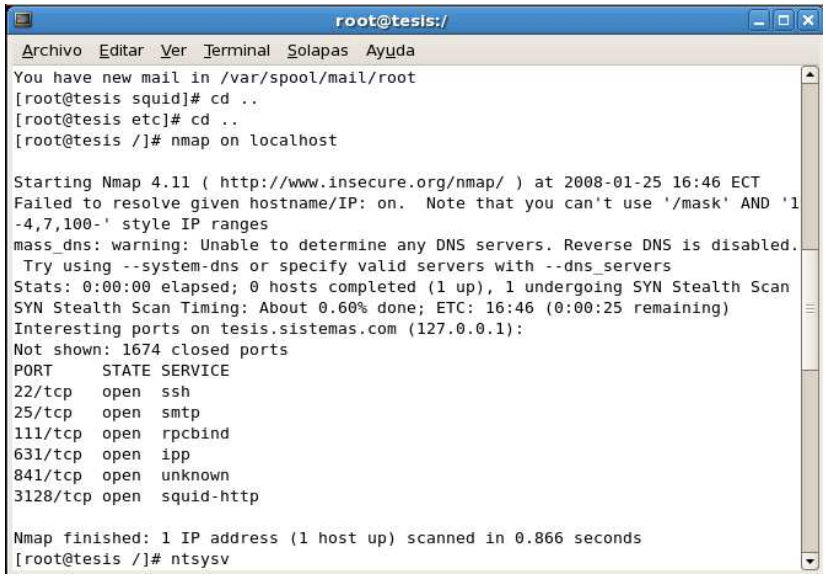
3.4. Asignación de Puertos a cada uno de los servidores

Los puertos están dados de acuerdo al servicio que se desea implementar el comando para la obtención de estos puertos es:

Nmap on localhost

Nmap es una herramienta popular incluida en Red Hat Enterprise Linux que puede ser usada para determinar la distribución de la red. Nmap ha estado disponible por muchos años y es probablemente la herramienta más usada para reunir información. Se incluye una página man (Pagina de Ayuda) excelente con una descripción detallada de sus opciones y uso. Los administradores pueden usar Nmap en una red para encontrar sistemas host y puertos abiertos en esos sistemas.

Nmap es un buen primer paso para una evaluación de vulnerabilidad. Puede mapear todos los hosts dentro de la red y hasta puede pasar una opción que le permite tratar de identificar el sistema operativo que se está ejecutando en un host en particular. Nmap es un buen fundamento para establecer una política de uso de servicios seguros y detener servicios que no se estén usando



3.5. Asignación de IP´s de acuerdo a las necesidades

Para la configuración tanto del squid como del firewall el computador tiene que tener cuando menos 2 tarjetas de red la una que seria quien de la cara al exterior y la otra que va a ser la de configuración de la red interna de las empresas o las instituciones.

Cuando configuramos las tarjetas de red, el Linux por defecto configura todo el rango de direcciones IP, para que puedan acceder todos los usuarios que deseen, pero las reglas que se den en el firewall van a ser las que nos den el numero de maquinas y los privilegios de acceso.

La configuración quedaría de la siguiente manera luego de poner el comando *ifconfig*, que es el comando que detalla las configuraciones de las tarjetas de red.

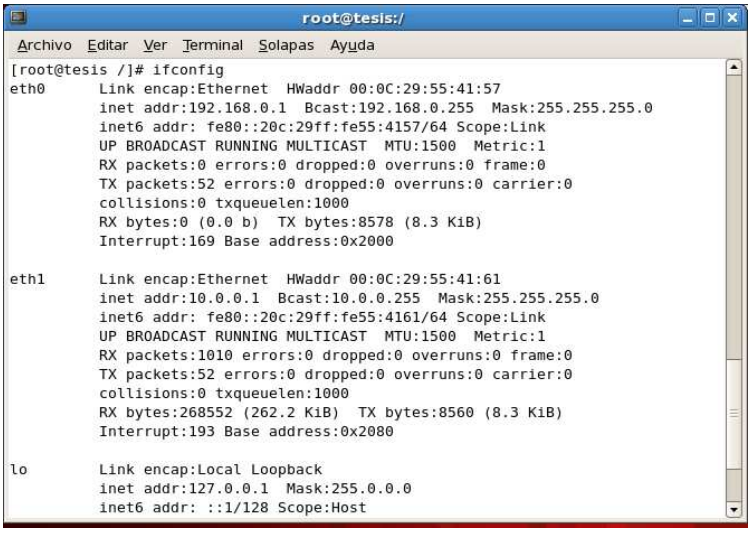


Figura 3.13: Configuración Tarjetas de Red
Fuente: Grupo Investigador

Por lo tanto, se desprende que en nuestro host contamos con 2 tarjetas de red las mismas que tienen las direcciones IP: 192.168.0.1 que es la que va a dar la cara al exterior y la otra tarjeta de red tiene la dirección IP: 10.0.0.1 que seria el servidor de la intranet, o para el Proxy de nuestra red

3.6. Asignación de flujo de trafico de acuerdo a perfiles

Están dadas de acuerdo a las reglas que se pusieron en el firewall, las mismas que fueron dadas para tiempo, impedir que se abran paginas que resten el ancho de banda así como también las paginas denominadas pornográficas o que por su contenido deben ser administradas por personas de criterio formado.