UNIVERSIDAD LUTERANA SALVADOREÑA

FACULTAD CIENCIAS DEL HOMBRE Y LA NATURALEZA

LICENCIATURA EN CIENCIAS DE LA COMPUTACIÓN

Cátedra: Sistemas Operativos de Redes.

Docente: Ing. Manuel de Jesús Flores.

Tema: Firewall de Red

Fecha de Entrega: martes 14 de noviembre 2015

Estudiantes:

Carnet	**Apellidos**	**Nombres**	**Participación**
BA02110776	Benítez Argueta	José Dimas	100%
FM02110857	Flores Martínez	José Manuel	100%
GP02110201	García Pineda	Osiris Stephanie	100%

Índice.

Planteamiento del problema.

Los alumnos de la materia de Sistemas Operativos de Redes, desconocen la Funcionalidad y configuración de la herramienta firewall, por lo tanto se necesita implementar un firewall para la adquisición del conocimiento en seguridad de la red.

Delimitación espacial.

La investigación se llevara a cabo a partir del aula de la Universidad Luterana Salvadoreña en el departamento de San Salvador. Esta investigación se realizó durante el periodo de estudio de la cátedra de sistemas operativos de redes; del ciclo II del presente año. Dicho periodo comprende desde el mes de junio del

mismo año; en la Universidad Luterana Salvadoreña con motivo de aprendizaje. Finalizando con la observaciones realizadas por el Ing. Manuel Flores docente informático de la Universidad Luterana Salvadoreña.

Introducción.

En el presente trabajo se muestra la funcionalidad y elaboración preliminar de un firewall de red; ya que es un tema de gran importancia para la seguridad de las empresas y es por ello que desarrollamos el presente proyecto de investigación y aplicación. Desde que las empresas y las personas comenzaron a comunicarse mediante Internet ha surgido un problema de inseguridad que afecta a los datos de gran importancia y seguridad que mantienen en sus sistemas privados así como aquellos que son enviados a sitios remotos de la red. Esta herramienta es esencial para el manejo de información en nuestra vida cotidiana y más aún en la realización de los negocios.

El firewall de red ofrece una solución a estos problemas, debido a la amplia tecnología se encuentran, como innovación de los últimos tiempos, los Cortafuegos distribuidos, que permiten establecer políticas más flexibles y robustas.

La mayor parte de las compañías utilizan Internet como herramienta clave para realizar sus negocios y dependen de ella para continuar existiendo, lo que puede llevar a exponer información privada poniendo en peligro la confidencialidad de sus operaciones. Muchas organizaciones ofrecen servicios mediante sus sistemas de comunicación, la seguridad de tales servicios requiere el acceso a recursos críticos del sistema de información de la empresa (archivos, dispositivos de almacenamiento, líneas telefónicas, etc.). Dichos recursos deben ser protegidos contra el uso indiscriminado y malicioso por parte de usuarios no deseados. Si un sistema de comunicación es vulnerable a estos tipos de ataques, el riesgo de pérdida de datos es importante. Este riesgo potencial de seguridad aumenta junto

con el nivel de dependencia en tecnología de información, lo que requiere el uso sistemas de seguridad más confiable y robusta.

Justificación.

El firewall de red que se realizo es de vital importancia para el buen desempeño
de los sistemas de información, ya que proporciona los controles necesarios para que los sistemas sean confiables y con un buen nivel de seguridad.
La evaluación y control que se realizo tiene como objetivo fundamental mejorar la seguridad y protección de los hacker; ya que hoy en día hay muchos ataques y muchas vulnerabilidades en la red por lo tanto necesitamos implementar un firewall que nos ayude a detectar anomalías en nuestra red. Para que nuestra red sea más eficaz y poder proteger nuestros datos de cualquier intruso.

Objetivos.

Objetivo general.

- Desarrollar un firewall de red que permita bloquear los accesos de los programas que se les indique bloquear y el cual no permitan acceder a la red local o a Internet. También bloquea los accesos que desde otros ordenadores se realizan para conectarse con programas en tu ordenador.

Objetivos específicos.

- Bloquear puertos lógicos (80.443)
- Bloquear de sitios web especifico
- Bloquear los accesos de cliente y servidor.

Marco teórico.

Cortafuego o firewall de red.

Un firewall o cortafuegos es un dispositivo de hardware o un software que nos permite gestionar y filtrar la totalidad de tráfico entrante y saliente que hay entre 2 redes u ordenadores de una misma red.

Si el tráfico entrante o saliente cumple con una serie de Reglas que nosotros podemos especificar, entonces el tráfico podrá acceder o salir de nuestra red u ordenador sin restricción alguna. En caso de no cumplir las reglas el tráfico

entrante o saliente será bloqueado.

Por lo tanto a partir de la definición podemos asegurar que con un firewall bien configurado podemos evitar intrusiones no deseadas en nuestra red y ordenador así como también bloquear cierto tipo de tráfico saliente de nuestro ordenador o nuestra red.

Historia.

El término firewall / fireblock significaba originalmente una pared para confinar un incendio o riesgo potencial de incendio en un edificio. Más adelante se usa para referirse a las estructuras similares, como la hoja de metal que separa el compartimiento del motor de un vehículo o una aeronave de la cabina. La tecnología de los cortafuegos surgió a finales de 1980, cuando Internet era una tecnología bastante nueva en cuanto a su uso global y la conectividad. Los predecesores de los cortafuegos para la seguridad de la red fueron los routers utilizados a finales de 1980, que mantenían a las redes separadas unas de otras. La visión de Internet como una comunidad relativamente pequeña de usuarios con máquinas compatibles, que valoraba la predisposición para el intercambio y la colaboración, terminó con una serie de importantes violaciones de seguridad de Internet que se produjo a finales de los 80:
Clifford Stoll, que descubrió la forma de manipular el sistema de espionaje alemán.

Bill Cheswick, cuando en 1992 instaló una cárcel simple electrónica para observar a un atacante.

- En 1988, un empleado del Centro de Investigación Ames de la NASA, en California, envió una nota por correo electrónico a sus colegas que decía:

"Estamos bajo el ataque de un virus de Internet! Ha llegado a Berkeley, UC San Diego, Lawrence Livermore, Stanford y la NASA Ames."

- El Gusano Morris, que se extendió a través de múltiples vulnerabilidades en las máquinas de la época. Aunque no era malicioso, el gusano Morris fue el primer ataque a gran escala sobre la seguridad en Internet; la red no esperaba ni estaba preparada para hacer frente a su ataque.

Primera generación – cortafuegos de red: filtrado de paquetes.

El primer documento publicado para la tecnología firewall data de 1988, cuando el equipo de ingenieros Digital Equipment Corporation (DEC) desarrolló los sistemas de filtro conocidos como cortafuegos de filtrado de paquetes. Este sistema, bastante básico, fue la primera generación de lo que se convertiría en una característica más técnica y evolucionada de la seguridad de Internet. En AT&T Bell, Bill Cheswick y Steve Bellovin, continuaban sus investigaciones en el filtrado de paquetes y desarrollaron un modelo de trabajo para su propia empresa, con base en su arquitectura original de la primera generación.
El filtrado de paquetes actúa mediante la inspección de los paquetes (que representan la unidad básica de transferencia de datos entre ordenadores en Internet). Si un paquete coincide con el conjunto de reglas del filtro, el paquete se reducirá (descarte silencioso) o será rechazado (desprendiéndose de él y enviando una respuesta de error al emisor). Este tipo de filtrado de paquetes no presta atención a si el paquete es parte de una secuencia existente de tráfico. En su lugar, se filtra cada paquete basándose únicamente en la información contenida en el paquete en sí (por lo general utiliza una combinación del emisor del paquete y la dirección de destino, su protocolo, y, en el tráfico TCP y UDP, el número de puerto). Los protocolos TCP y UDP comprenden la mayor parte de comunicación a través de Internet, utilizando por convención puertos bien conocidos para determinados tipos de tráfico, por lo que un filtro de paquetes puede distinguir entre ambos tipos de tráfico (ya sean navegación web, impresión remota, envío y recepción de correo electrónico, transferencia de archivos); a menos que las máquinas a cada lado del filtro de paquetes estén a la vez utilizando los mismos puertos no estándar.
El filtrado de paquetes llevado a cabo por un cortafuego actúa en las tres primeras capas del modelo de referencia OSI, lo que significa que todo el trabajo lo realiza entre la red y las capas físicas.
Cuando el emisor origina un paquete y es filtrado por el cortafuegos, éste último comprueba las reglas de filtrado de paquetes que lleva configuradas, aceptando o rechazando el paquete en consecuencia. Cuando el paquete pasa a través de cortafuegos, éste filtra el paquete mediante un protocolo y un número de puerto base (GSS). Por ejemplo, si existe una norma en el cortafuego para bloquear el acceso telnet, bloqueará el protocolo TCP para el número de puerto 23.

Segunda generación – cortafuegos de estado-

Durante 1989 y 1990, tres colegas de los laboratorios AT&T Bell, Dave Presetto, Janardan Sharma, y Nigam Kshitij, desarrollaron la segunda generación de servidores de seguridad. Esta segunda generación de cortafuegos tiene en cuenta, además, la colocación de cada paquete individual dentro de una serie de paquetes. Esta tecnología se conoce generalmente como la inspección de estado de paquetes, ya que mantiene registros de todas las conexiones que pasan por el cortafuego, siendo capaz de determinar si un paquete indica el inicio de una nueva conexión, es parte de una conexión existente, o es un paquete erróneo. Este tipo de cortafuegos pueden ayudar a prevenir ataques contra conexiones en curso o ciertos ataques de denegación de servicio.

Tercera generación - cortafuegos de aplicación

Son aquellos que actúan sobre la capa de aplicación del modelo OSI. La clave de un cortafuegos de aplicación es que puede entender ciertas aplicaciones y protocolos (por ejemplo: protocolo de transferencia de ficheros, DNS o navegación web), y permite detectar si un protocolo no deseado se coló a través de un puerto no estándar o si se está abusando de un protocolo de forma perjudicial.

Un cortafuegos de aplicación es mucho más seguro y fiable cuando se compara con un cortafuegos de filtrado de paquetes, ya que repercute en las siete capas del modelo de referencia OSI. En esencia es similar a un cortafuegos de filtrado de paquetes, con la diferencia de que también podemos filtrar el contenido del paquete. El mejor ejemplo de cortafuegos de aplicación es ISA (Internet Security and Acceleration).

Un cortafuego de aplicación puede filtrar protocolos de capas superiores tales como FTP, TELNET, DNS, DHCP, HTTP, TCP, UDP y TFTP (GSS). Por ejemplo, si una organización quiere bloquear toda la información relacionada con una palabra en concreto, puede habilitarse el filtrado de contenido para bloquear esa palabra en particular. No obstante, los cortafuegos de aplicación resultan más lentos que los de estado.

Acontecimientos posteriores

En 1992, Bob Braden y DeSchon Annette, de la Universidad del Sur de California (USC), dan forma al concepto de cortafuegos. Su producto, conocido como "Visas", fue el primer sistema con una interfaz gráfica con colores e iconos, fácilmente implementable y compatible con sistemas operativos como Windows de Microsoft o MacOS de Apple En 1994, una compañía israelí llamada Check Point Software Technologies lo patentó como software denominándolo FireWall-1.

La funcionalidad existente de inspección profunda de paquetes en los actuales cortafuegos puede ser compartida por los sistemas de prevención de intrusiones (IPS).

Actualmente, el Grupo de Trabajo de Comunicación Middlebox de la Internet Engineering Task Force (IETF) está trabajando en la estandarización de protocolos para la gestión de cortafuegos.

Otro de los ejes de desarrollo consiste en integrar la identidad de los usuarios dentro del conjunto de reglas del cortafuego. Algunos cortafuegos proporcionan características tales como unir a las identidades de usuario con las direcciones IP o MAC. Otros, como el cortafuego NuFW, proporcionan características de identificación real solicitando la firma del usuario para cada conexión.

Tipos de reglas que se pueden implementar en un firewall.

El tipo de reglas y funcionalidades que se pueden construir en un firewall son las siguientes:

1. **Administrar los accesos de los usuarios a los servicios** privados de la red como por ejemplo aplicaciones de un servidor.

2. **Registrar todos los intentos de entrada y salida** de una red. Los intentos de entrada y salida se almacenan en logs.

3. Filtrar paquetes en función de su origen, destino, y número de puerto. Esto se conoce como filtro de direcciones. Así por lo tanto con el filtro de direcciones podemos bloquear o aceptar el acceso a nuestro equipo de la IP 192.168.1.125 a través del puerto 22. Recordar solo que el puerto 22 acostumbra a ser el puerto de un servidor SSH.

4. Filtrar determinados tipos de tráfico en nuestra red u ordenador personal. Esto también se conoce como filtrado de protocolo. El filtro de protocolo permite aceptar o rechazar el tráfico en función del protocolo utilizado. Distintos tipos de protocolos que se pueden utilizar son **http, https, Telnet, TCP, UDP, SSH, FTP**, etc.

5. **Controlar el número de conexiones que se están produciendo desde un mismo punto** y bloquearlas en el caso que superen un determinado límite. De este modo es posible evitar algunos ataques de denegación de servicio.

6. **Controlar las aplicaciones que pueden acceder a Internet**. Así por lo tanto podemos restringir el acceso a ciertas aplicaciones, como por ejemplo dropbox, a un determinado grupo de usuarios.

7. **Detección de puertos que están en escucha y en principio no deberían estarlo**. Así por lo tanto el firewall nos puede advertir que una aplicación quiere utilizar un puerto para esperar conexiones entrantes.

Limitaciones de los firewall.

Lógicamente un Firewall dispone de una serie de limitaciones. Las limitaciones principales de un firewall son las siguientes:

1. Un firewall en principio es probable que no nos pueda proteger contra ciertas vulnerabilidades internas. Por ejemplo cualquier usuario puede borrar el contenido de un ordenador sin que el firewall lo evite, introducir un USB en el ordenador y robar información, etc.

2. Los firewall solo nos protegen frente a los ataques que atraviesen el firewall. Por lo tanto no puede repeler la totalidad de ataques que puede recibir nuestra red o servidor.

3. Un firewall da una sensación de seguridad falsa. Siempre es bueno tener sistemas de seguridad redundantes por si el firewall falla. Además no sirve de nada realizar una gran inversión en un firewall descuidando otros aspectos de nuestra red ya que el atacante siempre intentará buscar el eslabón de seguridad más débil para poder acceder a nuestra red. De nada sirve poner una puerta blindada en nuestra casa si cuando nos marchamos dejamos la ventana abierta.

Tipos de firewall existentes.

Existen 2 tipos de firewall. Existen **dispositivos de hardware firewall** como por ejemplo un firewall cisco o Routers que disponen de esta función.

Los dispositivos de hardware son una solución excelente en el caso de tengamos que proteger una red empresarial ya que el dispositivo protegerá a la totalidad de equipos de la red y además podremos realizar la totalidad de la configuración en

un solo punto que será el mismo firewall.

Además los firewall por hardware acostumbran a implementar funcionalidades interesantes como pueden ser CFS, ofrecer tecnologías SSL o VPN, antivirus integrados, antispam, control de carga, etc.

Los firewall por software son los más comunes y los que acostumbran a usar los usuarios domésticos en sus casas.

El firewall por software se instala directamente en los ordenadores o servidores que queremos proteger y solo protegen el ordenador o servidor en el que lo hemos instalado. Las funcionalidades que acostumbran a proporcionar los firewall por software son más limitadas que las anteriores, y además una vez instalado el software estará consumiendo recursos de nuestro ordenador.

Tipos de cortafuegos.

Nivel de aplicación de pasarela.

Aplica mecanismos de seguridad para aplicaciones específicas, tales como servidores FTP y Telnet. Esto es muy eficaz, pero puede imponer una degradación del rendimiento.

Circuito a nivel de pasarela.

Aplica mecanismos de seguridad cuando una conexión TCP o UDP es establecida. Una vez que la conexión se ha hecho, los paquetes pueden fluir entre los anfitriones sin más control. Permite el establecimiento de una sesión que se origine desde una zona de mayor seguridad hacia una zona de menor seguridad.

Cortafuegos de capa de red o de filtrado de paquetes.

Funciona a nivel de red (capa 3 del modelo OSI, capa 2 del stack de protocolos TCP/IP) como filtro de paquetes IP. A este nivel se pueden realizar filtros según los distintos campos de los paquetes IP: dirección IP origen, dirección IP destino. A menudo en este tipo de cortafuegos se permiten filtrados según campos de nivel de transporte (capa 3 TCP/IP, capa 4 Modelo OSI), como el puerto origen y destino, o a nivel de enlace de datos (no existe en TCP/IP, capa 2 Modelo OSI) como la dirección MAC.

Cortafuegos de capa de aplicación.

Trabaja en el nivel de aplicación (capa 7 del modelo OSI), de manera que los filtrados se pueden adaptar a características propias de los protocolos de este nivel. Por ejemplo, si trata de tráfico HTTP, se pueden realizar filtrados según la URL a la que se está intentando acceder, e incluso puede aplicar reglas en función de los propios valores de los parámetros que aparezcan en un formulario web.

Un cortafuego a nivel 7 de tráfico HTTP suele denominarse proxy, y permite que los ordenadores de una organización entren a Internet de una forma controlada. Un proxy oculta de manera eficaz las verdaderas direcciones de red.

Cortafuego personal.

Es un caso particular de cortafuegos que se instala como software en un ordenador, filtrando las comunicaciones entre dicho ordenador y el resto de la red. Se usa por tanto, a nivel personal.

Circuito a nivel de pasarela.

Aplica mecanismos de seguridad cuando una conexión TCP o UDP es establecida. Una vez que la conexión se ha hecho, los paquetes pueden fluir entre los anfitriones sin más control. Permite el establecimiento de una sesión que se origine desde una zona de mayor seguridad hacia una zona de menor seguridad.

Cortafuegos de capa de red o de filtrado de paquetes

Funciona a nivel de red (capa 3 del modelo OSI, capa 2 del stack de protocolos TCP/IP) como filtro de paquetes IP. A este nivel se pueden realizar filtros según los distintos campos de los paquetes IP: dirección IP origen, dirección IP destino. A menudo en este tipo de cortafuegos se permiten filtrados según campos de nivel de transporte (capa 3 TCP/IP, capa 4 Modelo OSI), como el puerto origen y destino, o a nivel de enlace de datos (no existe en TCP/IP, capa 2 Modelo OSI) como la dirección MAC.

Cortafuegos de capa de aplicación.

Trabaja en el nivel de aplicación (capa 7 del modelo OSI), de manera que los filtrados se pueden adaptar a características propias de los protocolos de este nivel. Por ejemplo, si trata de tráfico HTTP, se pueden realizar filtrados según la URL a la que se está intentando acceder, e incluso puede aplicar reglas en función de los propios valores de los parámetros que aparezcan en un formulario web.

Un cortafuego a nivel 7 de tráfico HTTP suele denominarse proxy, y permite que los ordenadores de una organización entren a Internet de una forma controlada. Un proxy oculta de manera eficaz las verdaderas direcciones de red.

Ventajas de cortafuegos.

Bloquea el acceso a personas y/o aplicaciones.

Limitaciones de un cortafuego.

Las limitaciones se desprenden de la misma definición del cortafuego: filtro de tráfico. Cualquier tipo de ataque informático que use tráfico aceptado por el cortafuego (por usar puertos TCP abiertos expresamente, por ejemplo) o que sencillamente no use la red, seguirá constituyendo una amenaza. La siguiente lista muestra algunos de estos riesgos:

- Un cortafuego no puede proteger contra aquellos ataques cuyo tráfico no pase a través de él.
- El cortafuego no puede proteger de las amenazas a las que está sometido por ataques internos o usuarios negligentes. El cortafuego no puede prohibir a espías corporativos copiar datos sensibles en medios físicos de almacenamiento (discos, memorias, etc.) y sustraerlas del edificio.
- El cortafuego no puede proteger contra los ataques de ingeniería social.
- El cortafuego no puede proteger contra los ataques posibles a la red interna por virus informáticos a través de archivos y software. La solución real está en que la organización debe ser consciente en instalar software antivirus en cada máquina para protegerse de los virus que llegan por cualquier medio de almacenamiento u otra fuente.
- El cortafuego no protege de los fallos de seguridad de los servicios y protocolos cuyo tráfico esté permitido. Hay que configurar correctamente y cuidar la seguridad de los servicios que se publiquen en Internet.

Políticas de cortafuego.

Hay dos políticas básicas en la configuración de un cortafuego que cambian

radicalmente la filosofía fundamental de la seguridad en la organización:

- **Política restrictiva**: Se deniega todo el tráfico excepto el que está explícitamente permitido. El cortafuego obstruye todo el tráfico y hay que habilitar expresamente el tráfico de los servicios que se necesiten. Esta aproximación es la que suelen utilizar las empresas y organismos gubernamentales.

- **Política permisiva**: Se permite todo el tráfico excepto el que esté explícitamente denegado. Cada servicio potencialmente peligroso necesitará ser aislado básicamente caso por caso, mientras que el resto del tráfico no será filtrado. Esta aproximación la suelen utilizar universidades, centros de investigación y servicios públicos de acceso a Internet.

La política restrictiva es la más segura, ya que es más difícil permitir por error tráfico potencialmente peligroso, mientras que en la política permisiva es posible que no se haya contemplado algún caso de tráfico peligroso y sea permitido por omisión.

¿Qué es IPTABLES?

iptables es una aplicación en espacio de usuario que le permite a un administrador de sistema configurar las tablas, cadenas y reglas de netfilter (descritas más arriba). Debido a que iptables requiere privilegios elevados para operar, el único que puede ejecutarlo es el superusuario. En la mayoría de los sistemas Linux, iptables está instalado como /sbin/iptables. La sintaxis detallada del comando iptables está documentada en su página de man, la cual puede verse tecleando el comando "man iptables" desde la línea de comandos.

Cadenas que componen el IPTABLE.

Tipo de paquete de datos:

- Tipo INPUT: paquetes que llegan a nuestra máquina
- Tipo OUTPUT: paquetes que salen de nuestra máquina
- Tipo FORWARD: paquetes que pasan por nuestra máquina

Interfaz por la que entran (-i = input) o salen (-o = output) los paquetes

- eth0, eth1, wlan0, ppp0, ...

IP origen de los paquetes (-s = source)

- IP concreta, ej: 10.0.1.3
- Rango de red, ej: 10.0.1.0/8

IP destino de los paquetes (-d = destination)

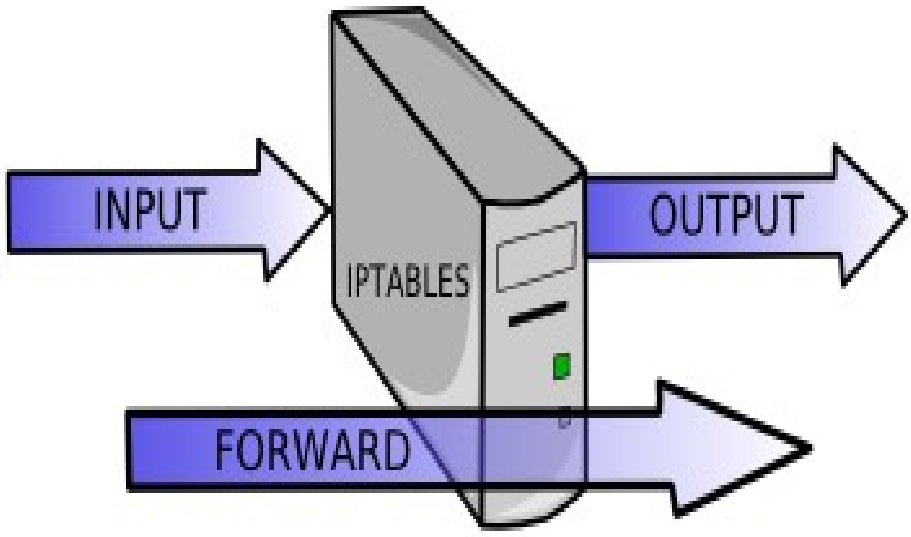
- IP concreta, ej: 10.0.1.3
- Rango de red, ej: 10.0.1.0/8

Protocolo de los paquetes (-p = protocol)

- Tcp, udp, icmp...

Hacer NAT (modificar IP origen y destino para conectar nuestra red a otra red o a Internet) y...

- Filtrar antes de enrutar: PREROUTING
- Filtrar después de enrutar: POSTROUTING



Los paquetes pueden entrar, salir o pasar.

Una forma sencilla de trabajar con iptables es permitir las comunicaciones que nos interesen y luego denegar el resto de las comunicaciones. Lo que se suele hacer es definir la política por defecto aceptar (ACCEPT), después crear reglas concretas para permitir las comunicaciones que nos interesen y finalmente, denegar el resto de comunicaciones. Lo mejor será crear un script en el que dispondremos la secuencia de reglas que queremos aplicar en nuestro sistema.

Opciones usadas en comandos iptables.

Las reglas para el filtrado de paquetes se ponen en funcionamiento ejecutando el comando iptables. Con frecuencia se utilizan los aspectos siguientes del paquete como el criterio:

- Tipo de paquete — Dicta qué tipo de paquetes filtra el comando.
- Fuente/Destino del paquete — Específica cuáles paquetes filtra el comando basándose en el origen o destino del paquete.
- Objetivo — Indica qué acción es tomada en paquetes que cumplen los criterios mencionados anteriormente.

Las opciones usadas con las reglas iptables dadas deben estar agrupadas lógicamente, basándose en el propósito y en las condiciones de la regla general, para que la regla sea válida. El resto de esta sección explica las opciones usadas comúnmente para el comando iptables.

Estructura de las opciones iptables

Muchos comandos iptables tienen la siguiente estructura:

```
iptables [-t <table-name>] <command> <chain-name> <parameter-1> \
         <option-1> <parameter-n> <option-n>
```

La opción <*table-name*> permite al usuario seleccionar una tabla diferente a la tabla predeterminada filter a usar con el comando. La opción <*command*> indica una acción específica a realizar, tal como anexar o eliminar la regla especificada

por la opción <*chain-name*>. Luego de la opción <*chain-name*> se encuentran un par de parámetros y opciones que definen qué pasará cuando un paquete coincide con la regla.

Cuando miramos la estructura de un comando iptables, es importante recordar que, al contrario que la mayoría de los comandos, la longitud y complejidad de un comando iptables puede cambiar en función de su propósito. Un comando para borrar una regla de una cadena puede ser muy corto, mientras que un comando diseñado para filtrar paquetes de una subred particular usando un conjunto de parámetros específicos y opciones puede ser mucho más largo. Al crear comandosiptables puede ser de ayuda reconocer que algunos parámetros y opciones pueden crear la necesidad de utilizar otros parámetros y opciones para especificar más aún la petición de la opción anterior. Para construir una regla válida, esto deberá continuar hasta que todos los parámetros y opciones que requieran otro conjunto de opciones hayan sido satisfechos.

Escriba iptables -h para ver una lista detallada de la estructura de los comandos iptables.

Opciones de comandos.

Las opciones de comandos le dicen a iptables que realice una acción específica. Solamente una opción de comando se permite por comando iptables. Excepto el comando de ayuda, todos los comandos se escriben en mayúsculas.

Los comandos de iptables son los siguientes:

- -A — Añade la regla iptables al final de la cadena especificada. Este es el comando utilizado para simplemente añadir una regla cuando el orden de las reglas en la cadena no importa.
- -C — Verifica una regla en particular antes de añadirla en la cadena especificada por el usuario. Este comando puede ser de ayuda para construir reglas iptablescomplejas pidiéndole que introduzca parámetros y opciones adicionales.
- -D — Borra una regla de una cadena en particular por número (como el 5 para la quinta regla de una cadena). Puede también teclear la regla entera e iptablesborrará la regla en la cadena que corresponda.
- -E — Renombra una cadena definida por el usuario. Esto no afecta la

estructura de la tabla.

- -F — Libera la cadena seleccionada, que borra cada regla de la cadena. Si no se especifica ninguna cadena, este comando libera cada regla de cada cadena.
- -h — Proporciona una lista de estructuras de comandos, así como también un resúmen rápido de parámetros de comandos y opciones.
- -I — Inserta una regla en una cadena en un punto especificado por un valor entero definido por el usuario. Si no se especifica ningún número, iptables colocará el comando en el tope de la cadena.

Información sobre la construcción del proyecto, detallando cada uno de los pasos, comandos, artefactos, procedimientos que se realizaron.

Tecnologías, artefactos involucrados en el proyecto.

Para la implementación y presentación del proyecto contamos con las siguientes tecnologías informáticas:

- **Tres mini-laptop marca HP, con sistemas operativo Debían.**
- **Un switch administrable de 24 pines.**
- **Sistema operativo GNU/LINUX Debian jessie 8.1.**
- **Tres cables de red.**

Procedimientos que se realizaron y comandos aplicados.

Código del prototipo del Firewall de red.

```
#!/bin/bash
#
#   Script para aplicar reglas del firewall Iptables (solo navegacion web)
#
################################################################################
##

#Limpiar reglas
iptables -F INPUT
iptables -F FORWARD
iptables -F OUTPUT

#Flush chains
iptables -X

#Pondemos a 0 el contador de paquetes y bytes
iptables -Z

#Flush de la tabla NAT
iptables -t nat -F

#POLÍTICAS POR DEFECTO (se aplicarán a la tabla filter) Para mayor seguridad bloquearemos
todo en un principio
echo "Aplicando politicas..."
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP

#Permitimos operatividad con localhost para servicios internos del sistema
iptables -A INPUT -s 127.0.0.1 -i lo -j ACCEPT
iptables -A OUTPUT -d 127.0.0.1 -o lo -j ACCEPT

#Permitimos navegación por HTTP(80), HTTPS(443)
iptables -A OUTPUT -j ACCEPT -o eth0 -p tcp --sport 1024:65535 -m multiport --dports 80,443

#Permitimos consultas DNS
iptables -A OUTPUT -o eth0 -p udp --sport 1024:65535 --dport 53 -m state --state NEW -j ACCEPT

#Permitir conexiones entrantes que estén relacionadas o establecidas anteriormente, es decir,
HTTP, HTTPS Y DNS
iptables -A INPUT -i eth0 -m state --state ESTABLISHED,RELATED -j ACCEPT

#Guardar reglas
iptables-save > /root/fwrules

#Resumen
echo "Configuración final de iptables:"
iptables -L -v
```

Agregar guía de pasos del firewall

Manual para el uso de Firewall

Ip tables –L para ver estado de politicas.
Iptables -X borra todas las politicas.

1. Verificar tres entradas de firewall.

2. si una de las entradas esta en drop lo permitamos con iptable -P FORWARD ACCEPT.

3. bloquea cliente que entra al firewall.

Iptable -A IMPUT -s 192.168.100.10 -i etho -j DROP
Iptable -A OUTPUT – d 192.168.100.11 -o eth0 -j DROP

4. bloqueo de cliente por FORWARED (Interface)
iptable -A FORWAD -s 192.168.100.11 -i eth0
-d 0/0 -p tcp - - dport 80 –o wlan0 – j DROP

5. para habilitar el bits de 0 a 1 es para habilitar compuesrtas de trafico de una interface a otras
vi /etc/sysctl.conf quitar el # a net.ipv4.ip_forward=0 ponerlo en 1

6. para borrar una politica
iptables -D FORWAD 1 EL NUMERO CAMBIA
IMPUT
OUTPUT.

7. para bloquear un sitio web p.provivienda.con.sv
iptables -A FORWARD -S 192.168.100.10 -i eth0 -d 93.104.208.141 – P tcp - - dport 80 – 0 wlan0 -j DROP.

En mejoramiento de ip/ sirve para que enmascare las ips internas y públicas.
Iptables -t nat -A POSROUTING -o wlan0 -j MASQUERADE.

8. Para bloques de todas las redes a una pc.
Para bloqueo de todas las redes iptables -A FORWARD – s 192.168.100.10 – i eth0 – d 0/0 -o wlan0 -j DROP.

-j es para bloquear.

CONFIGURAR IP RANGO 192.160.100.1 1 13.

Una breve descripción del producto final, que indique como funcionara y que componentes tendrá.

Un cortafuego (firewall) es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

Nuestro proyecto se basara en configurados un firewall para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios.

Nuestro cortafuegos ser implementara en hardware o software, o en una combinación de ambos. Nuestro se utilizara con frecuencia para evitar que los usuarios de Internet no autorizados tengan acceso a redes privadas conectadas a Internet, especialmente Todos los mensajes que entren o salgan de la intranet pasan a través del cortafuego, que examinara y bloqueara IP y páginas web a las que nosotros queramos aquellos que no cumplen los criterios de seguridad especificados. También es frecuente conectar los cortafuegos a una tercera red,

Diagrama de red Firewall.

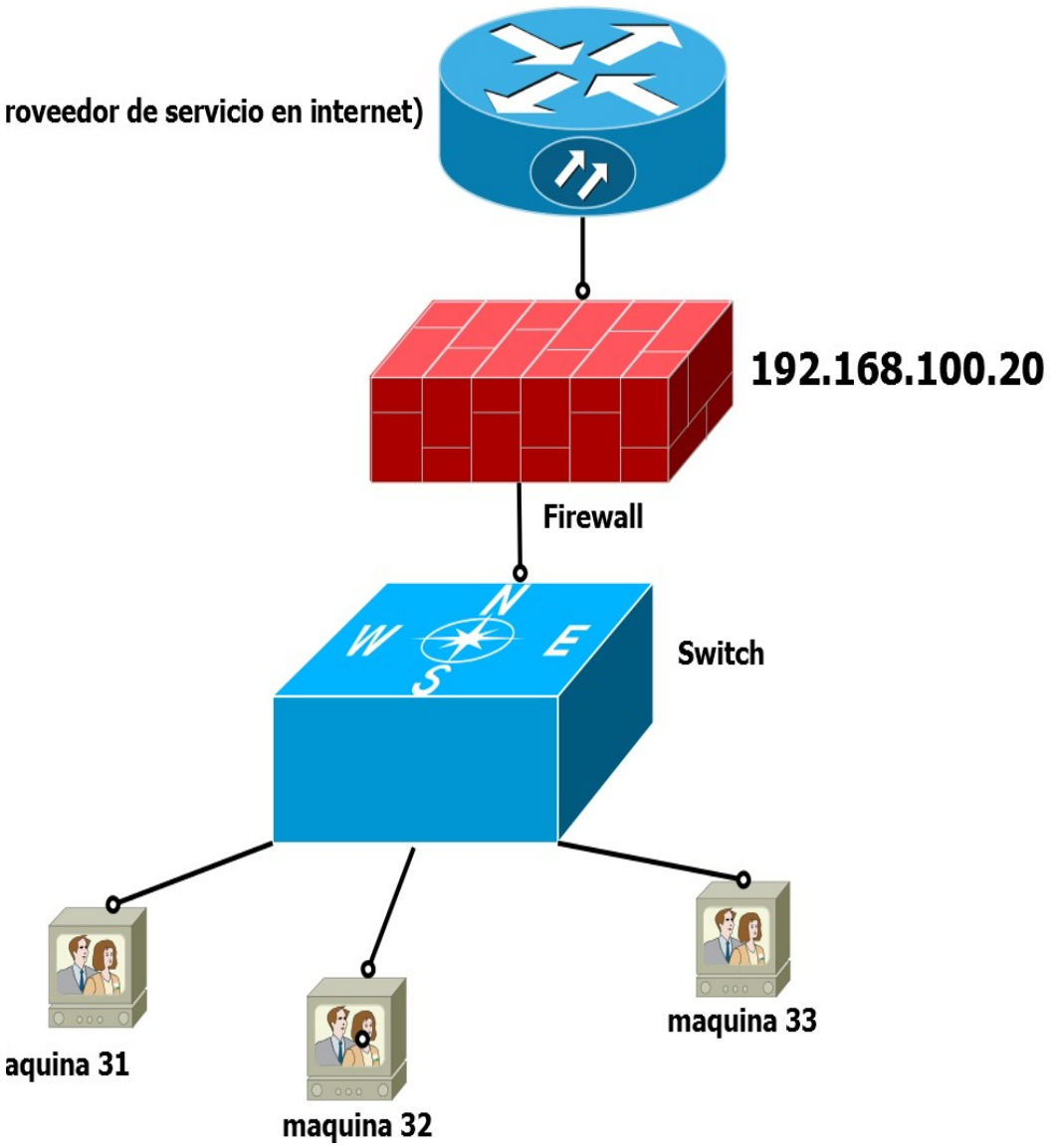
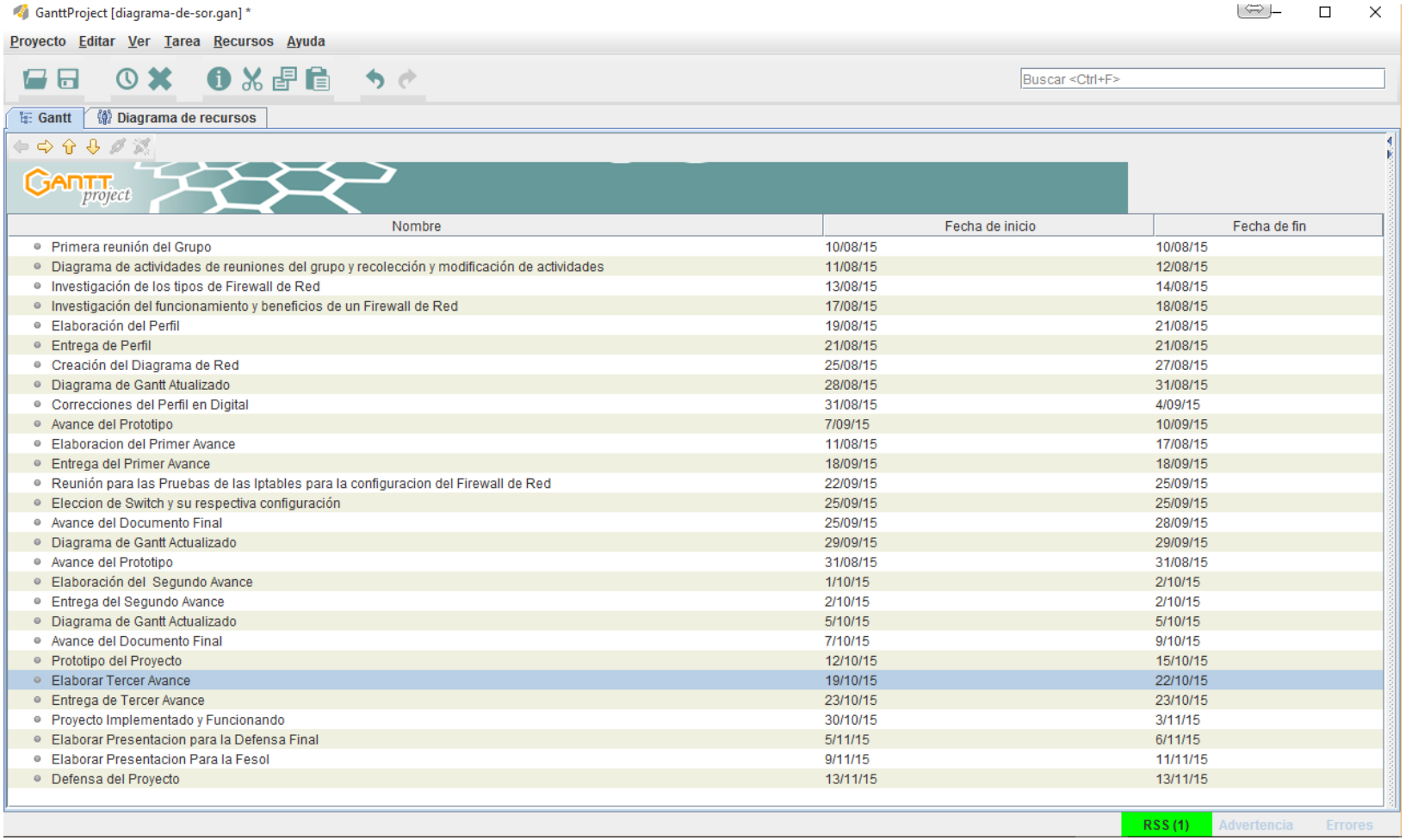
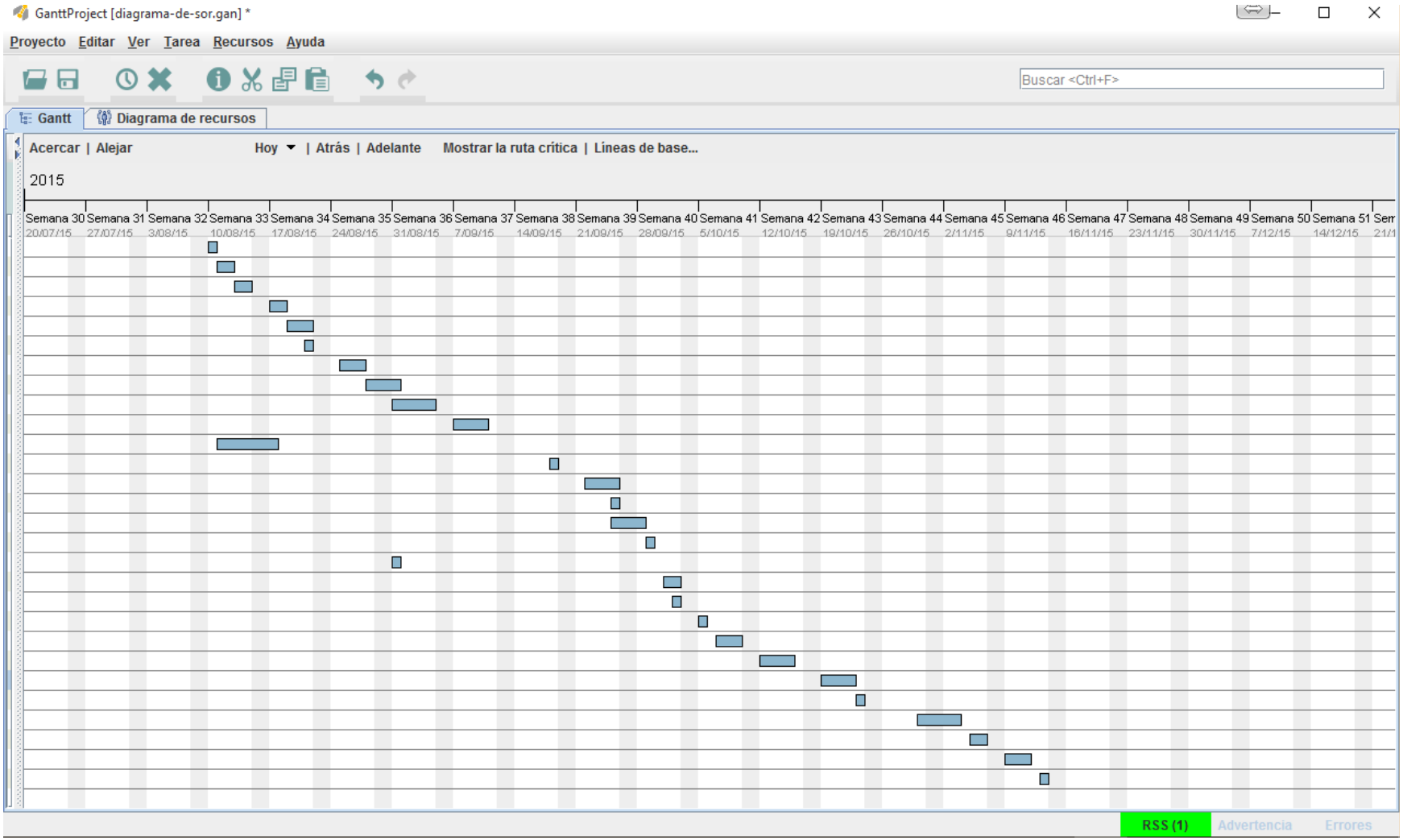

roveedor de servicio en internet)
192.168.100.20
Firewall
Switch
aquina 31
maquina 32
maquina 33

Diagrama de Gantt:




GanttProject [diagrama-de-sor.gan] *
Proyecto Editar Ver Tarea Recursos Ayuda
Buscar <Ctrl+F>
Gantt
Diagrama de recursos
Acercar | Alejar
Hoy | Atrás | Adelante
Mostrar la ruta crítica | Líneas de base...
2015
Semana 30 Semana 31 Semana 32 Semana 33 Semana 34 Semana 35 Semana 36 Semana 37 Semana 38 Semana 39 Semana 40 Semana 41 Semana 42 Semana 43 Semana 44 Semana 45 Semana 46 Semana 47 Semana 48 Semana 49 Semana 50 Semana 51
20/07/15 27/07/15 3/08/15 10/08/15 17/08/15 24/08/15 31/08/15 7/09/15 14/09/15 21/09/15 28/09/15 5/10/15 12/10/15 19/10/15 26/10/15 2/11/15 9/11/15 16/11/15 23/11/15 30/11/15 7/12/15 14/12/15
RSS (1)
Advertencia
Errores

Viabilidad y factibilidad del proyecto el cual debe incluir un presupuesto para la implementación del proyecto.

N°	DESCRIPCIÓN	CANTIDAD	VALOR	TOTAL
1	**RECURSO HUMANO**			
	Técnico en Seguridad de la Red	2	$50.00	$100.00
2	**EQUIPO INFORMATICO**			
	Computadoras	3	$300.00	$900.00
	Switch Administrable de 24 Puertos	1	$800.00	$800.00
			TOTAL NETO	**$1,800.00**

Conclusiones.

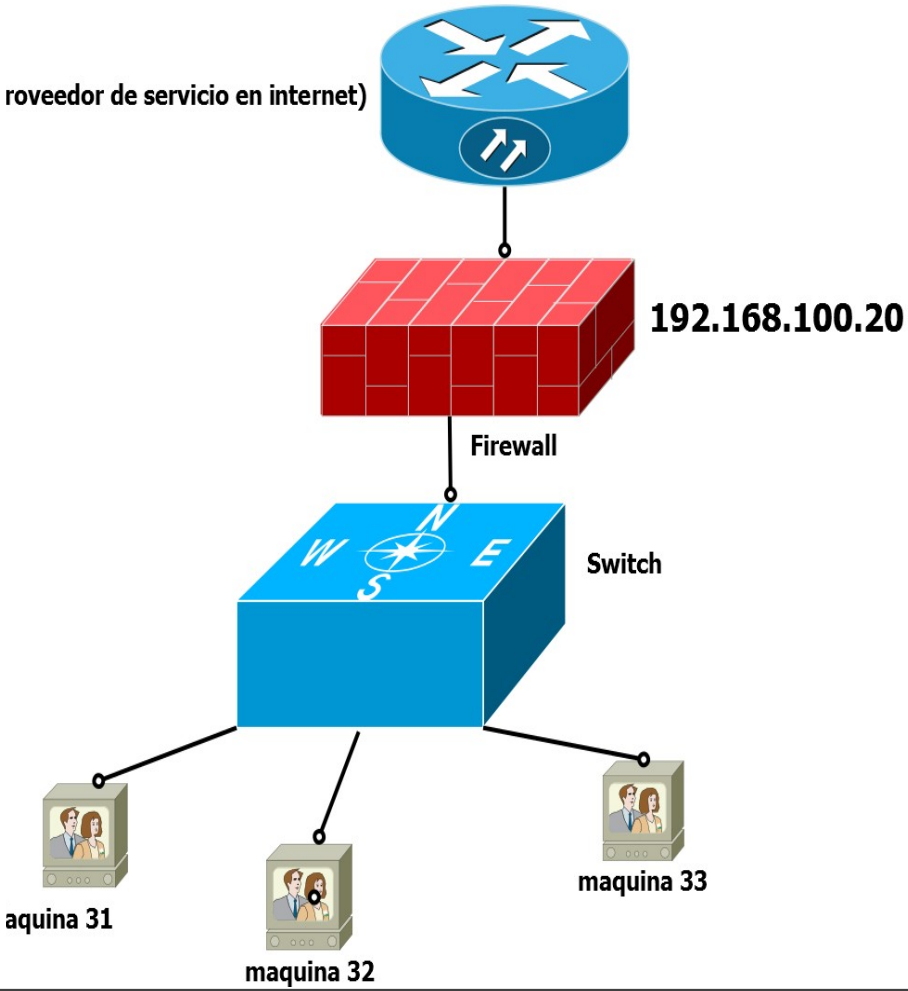
Como grupo de trabajo de sistema operativo de redes concluimos que el Firewall es necesario porque proporciona la seguridad para la red, mediante la imposición de políticas de seguridad, en el acceso a los recursos de la red y hacia la red externa, es importante establecer que un monitoreo constante del registro base, nos permita detectar un posible intruso y así proteger la información. Es inevitable que protejamos nuestra red de hackers que quieran filtrarse dentro de cualquier organización existente

Recomendaciones.

Recomendamos Los firewall a los administradores de red ya Son de gran ayuda para mantener el sistema protegido de cualquier intruso que se quiera infiltrar dentro de la empresa. Finalmente, una de las recomendaciones futuros trabajos sería implementar lo mismo pero para redes inalámbricas puesto que es un campo vulnerable e inseguro en servicios de IP y por la carencia de control de autenticación.

Anexos.

Diagrama de red Firewall.



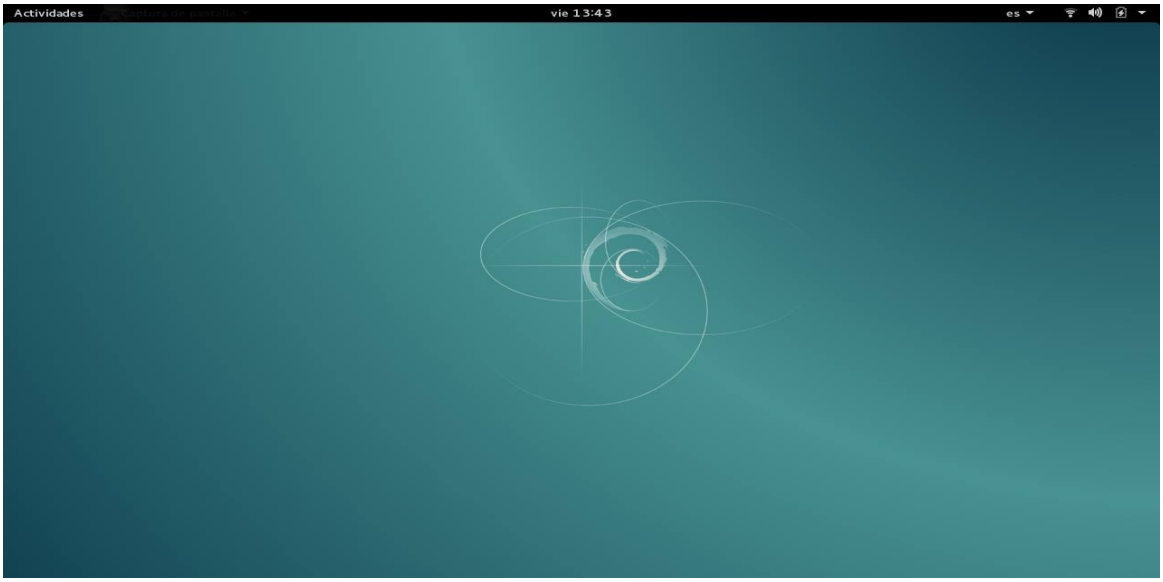
- En esta imagen hemos presentado la elaboración y estructuración de nuestro firewall de red, el cual cuenta con un proveedor de servicios en internet ISP.
- Cuenta con un firewall de red con IP 192.168.100.20
- Utilizamos un Switch de 24 pines.
- Contamos con tres notebook marca HP el cual cuenta con sistema operativo Debian Jessi 8.1

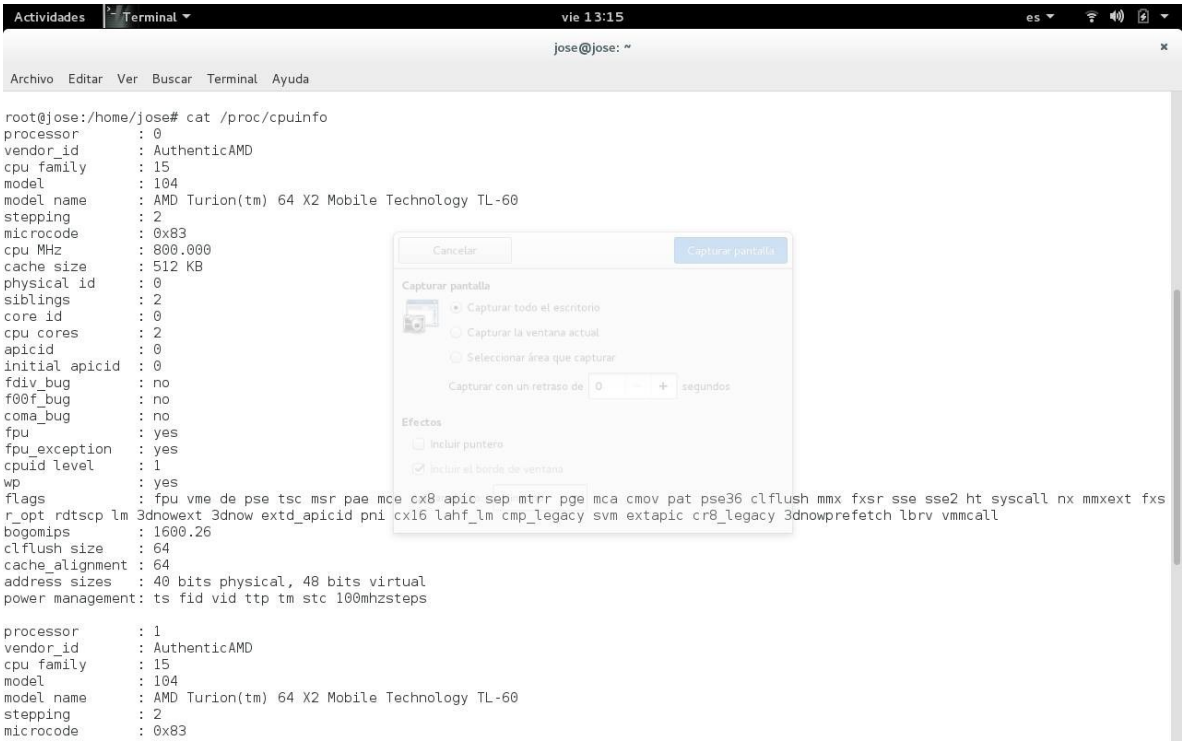
Tecnologías, artefactos involucrados en el proyecto.

- Tres mini-laptop marca HP, con sistemas operativo Debían.

- Primer equipo informatico.
- Contamos con tres notebook marca HP el cual cuenta con sistema operativo Debian Jessi 8.1 instalado.
- Cuenta con un procesador Pemtium ® Dual-core CPU E2500 @2.50GHZ.
- Memoria RAM de 2GB
- Disco duro 150 GB.

Equipo dos y capacidades del equipo.





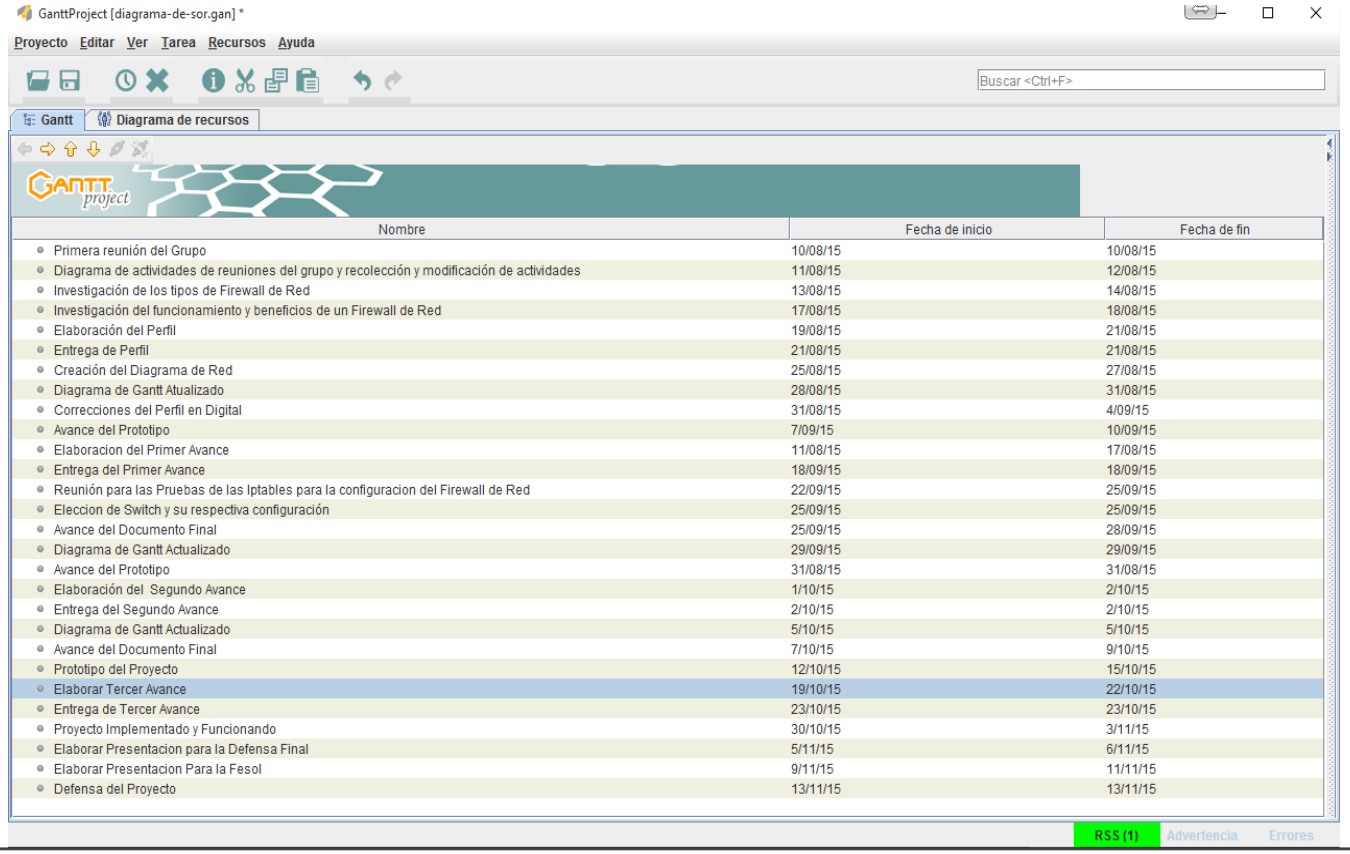
- **Un switch administrable de 24 pines.**

EL modelo del Switch es marca D”link modelo DES – 3528; es un switch administrable de 24 puertos.

- **Sistema operativo GNU/LINUX Debian jessie 8.1.**

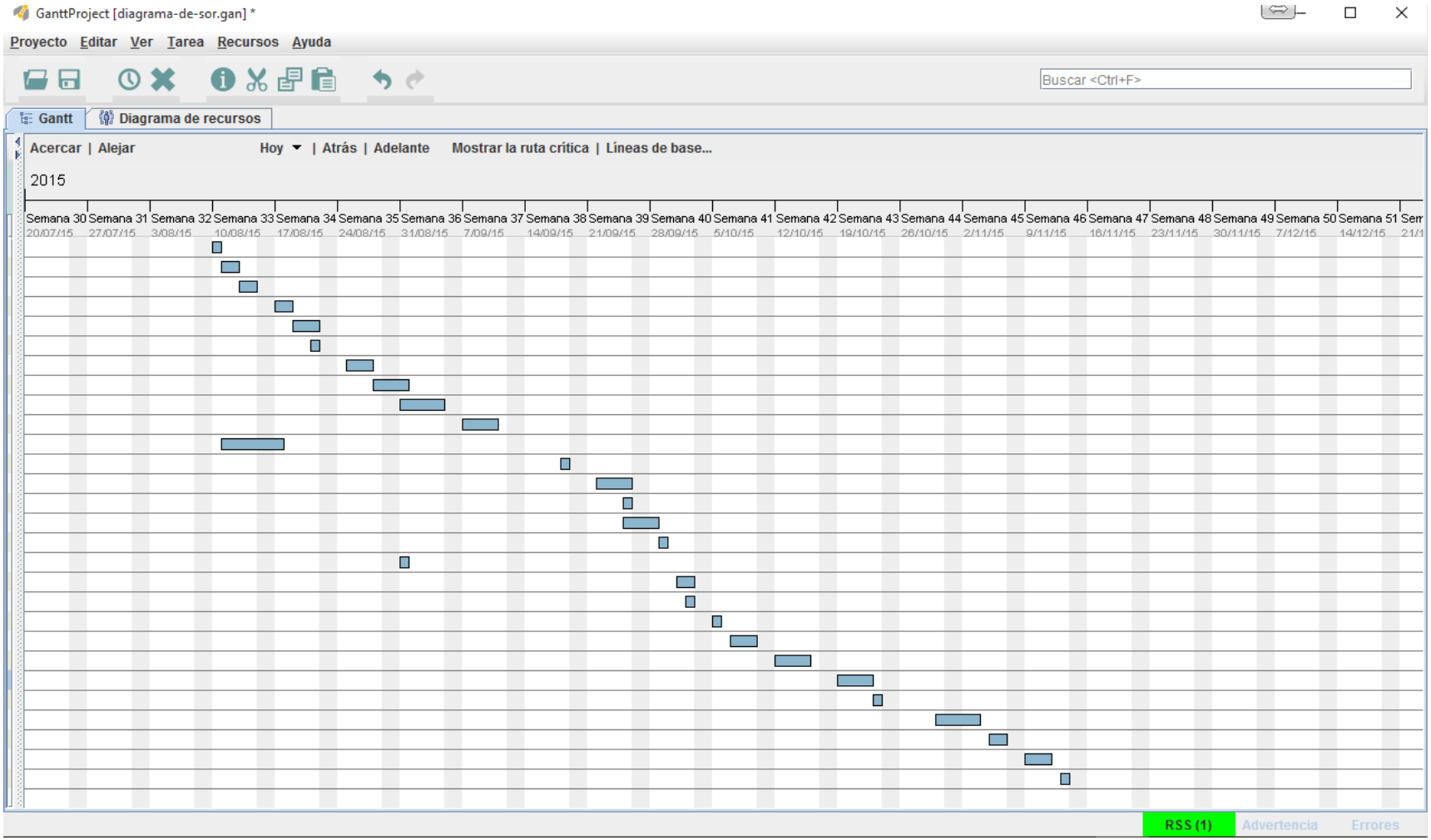
En las notebook se mostrara como imagen principal el logo del sistema operativo Debian Jessie 8.1 el cual está instalado en los equipos.

Diagrama de Gantt.



Nombre	Fecha de inicio	Fecha de fin
Primera reunión del Grupo	10/08/15	10/08/15
Diagrama de actividades de reuniones del grupo y recolección y modificación de actividades	11/08/15	12/08/15
Investigación de los tipos de Firewall de Red	13/08/15	14/08/15
Investigación del funcionamiento y beneficios de un Firewall de Red	17/08/15	18/08/15
Elaboración del Perfil	19/08/15	21/08/15
Entrega de Perfil	21/08/15	21/08/15
Creación del Diagrama de Red	25/08/15	27/08/15
Diagrama de Gantt Atualizado	28/08/15	31/08/15
Correcciones del Perfil en Digital	31/08/15	4/09/15
Avance del Prototipo	7/09/15	10/09/15
Elaboracion del Primer Avance	11/08/15	17/08/15
Entrega del Primer Avance	18/09/15	18/09/15
Reunión para las Pruebas de las Iptables para la configuracion del Firewall de Red	22/09/15	25/09/15
Eleccion de Switch y su respectiva configuración	25/09/15	25/09/15
Avance del Documento Final	25/09/15	28/09/15
Diagrama de Gantt Actualizado	29/09/15	29/09/15
Avance del Prototipo	31/08/15	31/08/15
Elaboración del Segundo Avance	1/10/15	2/10/15
Entrega del Segundo Avance	2/10/15	2/10/15
Diagrama de Gantt Actualizado	5/10/15	5/10/15
Avance del Documento Final	7/10/15	9/10/15
Prototipo del Proyecto	12/10/15	15/10/15
Elaborar Tercer Avance	19/10/15	22/10/15
Entrega de Tercer Avance	23/10/15	23/10/15
Proyecto Implementado y Funcionando	30/10/15	3/11/15
Elaborar Presentacion para la Defensa Final	5/11/15	6/11/15
Elaborar Presentacion Para la Fesol	9/11/15	11/11/15
Defensa del Proyecto	13/11/15	13/11/15

En el diagrama de Gantt describiremos cada una de las actividades que se realizaron en el tiempo estimado desde la calendarización del 10-08-2015 hasta el 13-11-2015


GanttProject [diagrama-de-sor.gan] *
Proyecto Editar Ver Tarea Recursos Ayuda
Buscar <Ctrl+F>
Gantt
Diagrama de recursos
Acercar | Alejar
Hoy | Atrás | Adelante
Mostrar la ruta crítica | Líneas de base...
2015
Semana 30 Semana 31 Semana 32 Semana 33 Semana 34 Semana 35 Semana 36 Semana 37 Semana 38 Semana 39 Semana 40 Semana 41 Semana 42 Semana 43 Semana 44 Semana 45 Semana 46 Semana 47 Semana 48 Semana 49 Semana 50 Semana 51
20/07/15 27/07/15 3/08/15 10/08/15 17/08/15 24/08/15 31/08/15 7/09/15 14/09/15 21/09/15 28/09/15 5/10/15 12/10/15 19/10/15 26/10/15 2/11/15 9/11/15 16/11/15 23/11/15 30/11/15 7/12/15 14/12/15
RSS (1)
Advertencia
Errores

Sección de términos y su definición.

Firewall: Es un dispositivo de hardware o un software que nos permite gestionar y filtrar la totalidad de tráfico entrante y saliente que hay entre 2 redes u ordenadores de una misma red.

Router: Es un dispositivo de red que permite el enrutamiento de paquetes entre redes independientes. Este enrutamiento se realiza de acuerdo a un conjunto de reglas que forman la tabla de enrutamiento.

IP: (IP es un acrónimo para Internet Protocol) son un número único e irrepetible con el cual se identifica una cmputadora conectada a una red que corre el protocolo IP.

ISP: sus siglas en ingles significan “Internet Service Provider “. Es un (proveedor de servicios de Internet) es una organización que ofrece a sus usuarios acceso a la Internet. Muchas compañías telefónicas son ISPs, pero no todas. Éstas ofrecen distintos servicios, como tránsito con Internet, registro de dominios, hosting, acceso vía módem o banda ancha e instalación de líneas.

SWITCH: Se trata de un dispositivo inteligente utilizado en redes de área local (LAN - Local Area Network).

LAN: Son las siglas de Local Área Network, Red de área local. Una LAN es una red que conecta los ordenadores en un área relativamente pequeña y predeterminada (como una habitación, un edificio, o un conjunto de edificios).

WAN: son las siglas de **Wide Area Network**, red de área amplia, una red de ordenadores que abarca un área geográfica relativamente grande. Normalmente, un WAN consiste en dos o más redes de área local (LANs).

PUERTO DE RED: es una interfaz para comunicarse con un programa a través de una red. En el modelo OSI quien se preocupa de la administración de los puertos y los establece en el encabezado de los segmentos es la capa de transporte o capa 4, administrando así el envío y re-ensamblaje de cada segmento enviado a la red haciendo uso del puerto especificado

Ancho de banda: ancho de banda es la cantidad de información o de datos que se puede enviar a través de una conexión de red en un período de tiempo dado.

bibliográficas

- **Libro**

Libro: Firewalls Linux guía avanzada.
Autor: Robert L. Ziegler.
Editorial: PRENTICE HALL EDITORIAL LINUX.

- **URL:**

http://geekland.eu/que-es-y-para-que-sirve-un-firewall/
Título de la página: Que es y para qué sirve un firewalls.
Fecha de la consulta: 23 de octubre de 2015.
Nombre del autor: Joan.