

# **Universidad Tecnológica de El Salvador**

**FACULTAD DE INFORMATICA Y CIENCIAS APLICADAS  
TECNICO EN INGENIERIA DE REDES COMPUTACIONALES**



**TEMA:**

“ELABORACIÓN DE GUÍAS DE ADMINISTRACIÓN Y CONFIGURACIÓN DE  
LOS SERVICIOS SQUID, IPTABLE, DNS, Y DHCP PARA FORTALECER LAS  
COMPETENCIAS DE LA ASIGNATURA ADMINISTRACIÓN DE REDES DE LA  
UNIVERSIDAD TECNOLÓGICA DE EL SALVADOR”.

**TRABAJO DE GRADUACIÓN PRESENTADO POR:**

Alejandra Verónica Colindres Velásquez

Rommel Lenin Vargas Cáceres

Carlos Miguel Díaz Sánchez

**PARA OPTAR AL GRADO:**

TECNICO EN INGENIERIA DE REDES COMPUTACIONALES

ABRIL 2017

SAN SALVADOR, EL SALVADOR, CENTRO AMERICA

**PAGINA DE AUTORIDADES**

ING. NELSON ZÁRATE SÁNCHEZ

**RECTOR**

LIC. JOSÉ MODESTO VENTURA

**VICERRECTOR ACADEMICO**

ING. FRANCISCO ARMANDO ZEPEDA

**DECANO**

**JURADO EXAMINADOR**

ING. VICENTE ANTONIO ZARCEÑO

**PRESIDENTE**

ING. OSCAR ERNESTO RODRIGUEZ

**PRIMER VOCAL**

LIC. WALTER MAURICIO NAVARRETE

**SEGUNDO VOCAL**

ABRIL, 2017

**SAN SALVADOR, EL SALVADOR, CENTROAMÉRICA**

## ACTA DE EXAMEN PROFESIONAL

HABIÉNDOSE REUNIDO EL JURADO CALIFICADOR INTEGRADO POR:

Ing. Oscar Ernesto Rodríguez, Ing. Vicente Antonio Zarceño Jaco, Lic. Walter Mauricio Navarrete, a las 12:30m del día Sábado, 10 de Diciembre de dos mil dieciséis.

Y LUEGO DE HABER DELIBERADO SOBRE EL EXAMEN PROFESIONAL DE LOS ALUMNOS:

|                                                 |                            |
|-------------------------------------------------|----------------------------|
| <u>1-Alejandra Verónica Colindres Velásquez</u> | <u>Carnet 26-4958-2014</u> |
| <u>2-Romel Lenin Vargas Cáceres</u>             | <u>Carnet 26-2646-2014</u> |
| <u>3-Carlos Miguel Díaz Sánchez</u>             | <u>Carnet 26-2363-2014</u> |

QUIENES PRESENTARON DEFENSA DE SU TRABAJO DE GRADUACION TITULADO:

"Elaboración de guías de administración y configuración de los servicios SQUID, IPTABLE, DNS y DHCP para fortalecer las competencias de la asignatura de administración de redes de la Universidad Tecnológica de El Salvador"

PARA OPTAR AL GRADO DE:

### **TÉCNICO EN INGENIERIA DE REDES COMPUTACIONALES**

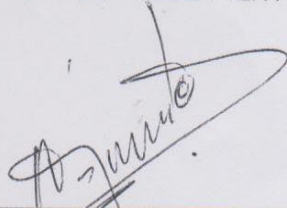
Y DEL CUAL TAMBIEN EVALUARON LOS CONOCIMIENTOS RELACIONADOS CON EL TEMA DEL MISMO. POR LO QUE ESTE JURADO RESUELVE DECLARAR EL EXAMEN COMO:

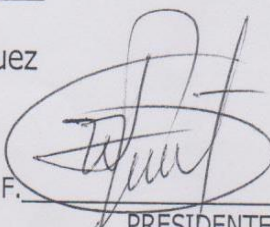
Aprobado

YA QUE CUMPLE CON LOS REQUISITOS ESTABLECIDOS EN EL REGLAMENTO DE GRADUACION DE LA UNIVERSIDAD.

San Salvador, 10 de Diciembre de dos mil dieciséis.

F.   
PRIMER VOCAL  
Ing. Oscar Ernesto Rodríguez

F.   
SEGUNDO VOCAL  
Ing. Vicente Antonio Zarceño Jaco

F.   
PRESIDENTE  
Lic. Walter Mauricio Navarrete

## ÍNDICE

|                                                    |    |
|----------------------------------------------------|----|
| Introducción .....                                 | i  |
| Capítulo I Planteamiento del problema              |    |
| 1.1 situación problemática .....                   | 1  |
| 1.2 justificación .....                            | 2  |
| 1.3 Objetivos .....                                | 3  |
| 1.3.1 general .....                                | 3  |
| 1.3.2 específico .....                             | 3  |
| 1.4 alcances .....                                 | 4  |
| 1.5 limitaciones de estudio .....                  | 4  |
| Capítulo II Marco teórico                          |    |
| 2.1 Debián Sistema Operativo .....                 | 5  |
| 2.2 principios de una red segura .....             | 7  |
| 2.2.2 evolución de la seguridad en las redes ..... | 8  |
| 2.2.3 dominios de seguridad en las redes .....     | 8  |
| 2.3 servicios de red .....                         | 10 |
| 2.4 servicios .....                                | 10 |
| 2.4.1 servicio Webmin .....                        | 10 |
| 2.4.2 DHCP .....                                   | 11 |
| 2.4.3 DNS .....                                    | 11 |
| 2.4.4 Squid .....                                  | 12 |
| 2.4.5 Iptables .....                               | 12 |
| 2.4.6 características de Iptables .....            | 14 |

|                                                      |    |
|------------------------------------------------------|----|
| 2.5 Netfilter .....                                  | 14 |
| 2.5.1 ¿qué puedo hacer con Netfilter/IPtables? ..... | 15 |
| 2.6 arquitectura y teoría de Firewall .....          | 15 |
| 2.6.1 Firewall .....                                 | 15 |
| 2.6.2 Firewall e Internet .....                      | 16 |
| 2.6.3 que puede hacer un Firewall .....              | 16 |
| 2.7 tipos de Firewall.....                           | 16 |
| 2.7.1 Hardware .....                                 | 16 |
| 2.7.2 Software .....                                 | 17 |
| Capitulo III: Metodología de la investigación        |    |
| 3.1 Metodología de la Investigación .....            | 18 |
| 3.1.1 participantes .....                            | 18 |
| 3.1.2 método.....                                    | 19 |
| 3.1.3 instrumentos .....                             | 19 |
| 3.1.4 procedimientos .....                           | 20 |
| 3.1.4.1 guía de instalación Debían .....             | 20 |
| 3.1.4.2 guía de configuración DHCP .....             | 37 |
| 3.1.4.3 guía de configuración DNS .....              | 44 |
| 3.1.4.4 guia de configuración Webmin .....           | 48 |
| 3.1.4.5 guia de configuración Squid.....             | 52 |
| 3.1.4.6 guia de configuración Iptables .....         | 56 |
| 3.2 análisis de Datos.....                           | 62 |
| 3.3 conclusiones .....                               | 65 |
| 3.4 referencias .....                                | 67 |

|                                                                               |    |
|-------------------------------------------------------------------------------|----|
| 3.5 anexos.....                                                               | 68 |
| 3.5.1 encuesta .....                                                          | 68 |
| 3.5.2 tabla de explicación de comandos dentro de consola para Iptables .....  | 70 |
| 3.5.3 tabla de explicación de parámetros dentro de consola para Iptable ..... | 70 |
| 3.6 Glosario .....                                                            | 71 |

## Introducción

En el presente trabajo tiene como objetivo crear una guía en el cual se muestre configuración y administración básica sobre los servicios PROXY (Squid), Iptables, DNS, Webmin en el sistema operativo Debían creándose paso a paso, los estudiantes logaran realizar prácticas en las cuales obtendrán el conocimiento para el manejo de los servicios.

Esta guía será un beneficio que obtendrán los estudiantes de la asignatura administración de redes, de la carrera Tecnico en Ingeniería de Redes Computacionales de la Universidad Tecnologica de El Salvador. Para mejorar la información didáctica y poder contribuir al fortalecimiento de competencias y aplicar los conocimientos para estar a la vanguardia de la tecnología en configuración del sistema operativo Debían.

Unas de las limitantes que se presento es la falta de estudiantes y docentes que no poseen los materiales para poder darle seguimiento a la configuración paso a paso de los servicios DNS, DHCP, Squid, Webmin e Iptables para aplicarlos en un sistema operativo y poder crear un Firewall con el cual permita que el cliente restrinja los accesos a páginas web no deseadas o respuesta de ICMP.

# **Capítulo I**

## **Planteamiento del Problema**

### *1.1 Situación Problemática*

En la Universidad Tecnológica de El Salvador, una de las carreras impartidas es: Técnico en Ingeniería de Redes Computacionales, en la cual los estudiantes cursan la asignatura de: Administración de Redes, en el contenido de esta asignatura se presenta la configuración de sistemas operativos como Windows Server, GNU/Linux, Centos, Ubuntu y Debían.

La facultad de Informática y Ciencias Aplicadas, de funcionamiento de diferentes sistemas operativos que tienen la finalidad de ser utilizados para realizar prácticas en el laboratorio de redes. Para esto se necesitarán guías de apoyo, ya que los libros que la Universidad posee, proporcionan solamente la información básica de los diferentes sistemas operativos.

## *1.2 Justificación.*

Esta guía será un beneficio que obtendrán los estudiantes de la asignatura Administración de Redes, de la carrera Técnico en Ingeniería de Redes Computacionales de la Universidad Tecnológica de El Salvador. Para mejorar la información didáctica y poder contribuir al fortalecimiento de competencias y aplicar todos los conocimientos para estar realizar configuración del sistema operativo Debían, tomando en cuenta la importancia de su conocimiento y el acceso directo al material facilitaría al estudiante para realizar las configuraciones de este

Se utilizara la distribución debían porque a comparación de otras distribuciones Debían posee una instalación más sencilla, y es un software de mayor seguridad. Además que es un software con estabilidad existen muchos casos de máquinas que trabajan durante más de un año seguido sin reiniciarse, de la misma forma que hay casos de equipos que son reiniciados debido a un fallo en el servicio de corriente o actualización de hardware; comparado con otros sistemas que colapsan varias veces al día.

Los estudiantes de la Universidad Tecnológica de El Salvador tendrán la oportunidad de acceder a la guía didáctica que se encontrará disponible en la Biblioteca de dicha universidad.

## 1.3 Objetivos

### 1.3.1 general

Crear un manual en el cuál se muestre la instalación, configuración, administración básica sobre los servicios PROXY (squid), iptable, DNS, y DHCP en el sistema operativo debían utilizando Webmin así los cursantes de la asignatura Administración de Redes en la Universidad Tecnológica de El Salvador, logran realizar prácticas en las cuales obtendrán el conocimiento necesario para el manejo de los servicios.

### 1.3.2 específico

- Ilustrar el Proceso de configuración de Servicios y aplicación de algunas reglas de firewall utilizando Webmin para su fácil entendimiento en configuración.
- Realizar un documento donde el estudiante pueda apoyarse en cualquier momento para desarrollar un proceso de aprendizaje autónomo o colaborativo, y orientarse a las funcionalidades.
- Plasmar guías prácticas comprensivas sobre configuración de Squid, Iptables, DNS, y DHCP con un seguimiento sistematizado (Paso a Paso), el cual facilite a los estudiantes La comprensión y ejecución de las actividades planteadas en cada una de ellas.

#### *1.4 Alcances*

- Que los alumnos sin base previa puedan configurar con solo la guía didáctica y tengan la comprensión de todos los pasos a seguir utilizando un lenguaje comprensible, dándole así un conocimiento nuevo que ellos puedan poner en práctica.
- El alumno con facilidad pueda ir a la biblioteca a solicitar la guía para poder realizar la respectiva práctica, facilitándolo a que pueda realizar sus prácticas en el laboratorio de redes apoyándose en el material didáctico
- Que los alumnos entiendan y ejecuten cada uno de los servicios, siguiendo cada paso explicado en la guía

#### *1.5 Limitación de estudio*

- La falta de documentación acerca de la distribución Debían combinado con los servicios Iptable los alumnos no tienen una base previa acerca de este sistema operativo
- El periodo de recolección de datos e información de la investigación comprende 5 meses a partir de agosto de 2016.

## Capítulo II

### Marco Teórico

#### 2.1 Debían sistema operativo

Debían es un sistema operativo (S.O.) libre, para su computadora. El sistema operativo es el conjunto de programas básicos y utilidades que hacen que funcione su computadora.

Debían ofrece más que un S.O. puro; viene con 43000 paquetes, programas recompilados distribuidos en un formato que hace más fácil la instalación en su computadora.

*Tabla 1:* Tabla comparativa de distribuciones Linux

Comparativa de distribuciones de Linux I

| Distribución                                                                   | Tipo      | Usos                                            | Ciclo de vida                                                                                                                  |
|--------------------------------------------------------------------------------|-----------|-------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------|
| CentOS<br>Basado sobre Red Hat™<br>Enterprise Linux<br>Mantenido por comunidad | Gratuita  | Servidores<br>Est. trabajo<br><b>Producción</b> | <b>10 años</b><br>· 5½ años actualizaciones<br>· 1 año mantenimiento<br>· 3½ años parches críticos                             |
| Red Hat™ Enterprise Linux<br>Mantenido por Red Hat, Inc.                       | Comercial | Servidores<br>Est. trabajo<br><b>Producción</b> | <b>10 años</b><br>· 5½ años actualizaciones<br>· 1 año mantenimiento<br>· 3½ años parches críticos<br>3 años soporte extendido |
| SUSE™ Linux Enterprise<br>Mantenido por SUSE                                   | Comercial | Servidores<br>Est. trabajo<br><b>Producción</b> | <b>10 años</b><br>· 7 años actualizaciones<br>· 3 años parches críticos<br>3 años soporte extendido                            |

### Comparativa de distribuciones de Linux I

| <b>Distribución</b>                                                 | <b>Tipo</b>           | <b>Usos</b>                                      | <b>Ciclo de vida</b>                                     |
|---------------------------------------------------------------------|-----------------------|--------------------------------------------------|----------------------------------------------------------|
| Ubuntu™ Server LTS<br>Mantenido por Canonical                       | Gratuita<br>Comercial | Servidores<br><b>Producción</b>                  | <b>5 años</b>                                            |
| Ubuntu™ LTS<br>Mantenido por Canonical                              | Gratuita<br>Comercial | Est. trabajo<br>Escritorios<br><b>Producción</b> | 3 años                                                   |
| Ubuntu™ (estándar)<br>Mantenido por Canonical                       | Gratuita              | Escritorios<br><b>Vanguardia</b>                 | 9 meses                                                  |
| Debian™ Linux<br>Mantenido por comunidad                            | Gratuita              | Multiuso<br><b>Producción</b>                    | Sin ciclos fijos<br>1 año tras siguiente versión estable |
| Fedora™<br>Mantenido por comunidad y Red Hat, Inc.                  | Gratuita              | Multiuso<br><b>Vanguardia</b>                    | 12 a 18 meses                                            |
| OpenSUSE™<br>Mantenido por comunidad y SUSE                         | Gratuita              | Escritorio<br><b>Vanguardia</b>                  | 36 meses                                                 |
| ALDOS<br>Alcance Libre Desktop OS<br>Mantenido por AlcanceLibre.org | Gratuita              | Escritorio<br>Est. trabajo<br><b>Producción</b>  | <b>5 años</b>                                            |
| LinuxMint<br>Mantenido por comunidad                                | Gratuita              | Escritorio<br><b>Vanguardia</b>                  | 3 años                                                   |
| Gentoo Linux<br>Mantenido por comunidad                             | Gratuita              | Multiuso<br><b>Vanguardia</b>                    | Lanzamiento continuo.                                    |
| Slackware Linux<br>Mantenido por comunidad                          | Gratuita              | Multiuso<br><b>Vanguardia</b>                    | Sin ciclos fijos                                         |

## *2.2 Principios de una red segura*

Mantener una red segura garantiza la seguridad de la red y la de los usuarios y protege los intereses comerciales. Esto requiere vigilancia de parte de los profesionales de seguridad en redes quienes deberán estar constantemente al tanto de las nuevas y evolucionadas amenazas y ataques a las redes, así como también de las vulnerabilidades de los dispositivos y aplicaciones. La mayor motivación de la seguridad en redes es el esfuerzo por mantenerse un paso más delante de los hacker mal intencionados.

La complejidad de la seguridad en redes dificulta dominar todo lo que esta abarca. Varias organizaciones han creado dominios que subdividen el mundo de la seguridad de redes en segmentos más fácilmente manejables. Estas organizaciones establecen estándares, fomentan la colaboración y proveen oportunidades de desarrollo para los profesionales de la seguridad.

Tal como la seguridad en redes está compuesta de dominios, los ataques a las redes son clasificados para hacer más fácil aprender de ellos y abordarlos apropiadamente. Los virus, los gusanos y los troyanos son tipos específicos de ataque a las redes. Generalmente los ataques a las redes se clasifican como ataques de reconocimiento, de acceso o de denegación de servicio.

Los profesionales de la seguridad en redes son responsables de crear y mantener la política de seguridad de red. Todas las prácticas de seguridad en redes están relacionadas y guiadas por las políticas de seguridad implementadas en las redes.

### *2.2.2 evolución de la seguridad en redes*

Hoy en día internet es una red muy diferente a la que era en sus comienzos en los años sesenta. El trabajo de un profesional en redes incluye asegurarse de que el personal este muy capacitado en herramientas, procesos, técnicas, protocolos y tecnologías de seguridad en redes. Es crítico que los profesionales de seguridad en redes mantengan una paranoia saludable para manejar la colección de amenazas a las redes en constante evolución.

### *2.2.3 dominios de seguridad en las redes*

Los dominios proveen un marco organizado para facilitar el aprendizaje sobre la seguridad en redes. Es importante entender el funcionamiento de cada uno de estos dominios de la seguridad de redes.

Existen 12 dominios de seguridad descritos por ISO/IEC27002 que sirven para organizar a alto nivel la información dentro de la seguridad en redes. Estos dominios tienen algunos paralelismos significativos con los dominios definidos por la certificación CISSP. Los 12 dominios están diseñados para servir como base común para desarrollar los estándares de seguridad en las organizaciones y las prácticas de administración de seguridad efectiva, así como también para ayudar a construir confianza en las actividades que tienen como lugar dentro de la organización

Los dominios de la seguridad en redes proveen una separación conveniente para los elementos de la seguridad en redes. Estos 12 dominios sirven como referencia útil para avanzar en el trabajo como profesional de la seguridad en redes.

- Evaluación de Riesgos: es el primer paso en el proceso de administración de riesgos. Determina el valor cuantitativo y cualitativo del riesgo relacionado con una amenaza reconocida o situación determinada
- Política de seguridad: es un documento que trata de las restricciones y comportamientos de los miembros de una organización y generalmente especifica cómo se puede acceder a los datos y quien puede hacerlo
- Organización de la seguridad de la información: Es el modelo de gobierno establecido por una organización para la seguridad de la información
- Administración de los bienes: es un inventario y esquema de clasificación para los bienes
- Seguridad de los recursos humanos: trata de sobre los procedimientos de seguridad que guardan relación con los empleados de una organización que entran, se mueven en ella
- Seguridad física y ambiental: describe la protección de las instalaciones reales de los ordenadores dentro de una organización
- Administración de las comunicaciones y las operaciones: describe la administración de los controles técnicos de seguridad en sistemas y redes
- Control de acceso: describe la restricciones derechos a redes sistemas, aplicaciones, funciones de datos
- Adquisición, desarrollo y mantenimiento de los sistemas de información: describe la integración de seguridad a las aplicaciones
- Administración de incidentes de seguridad de la información: describe como anticipar y responder a las fisuras de seguridad de la información

- Administración de la continuidad de los negocios: describe la protección , mantenimiento y recuperación de procesos y sistemas críticos para los negocios
- Conformidad: describe el proceso de asegurar la conformidad con las regulaciones, los estándares y las políticas de la seguridad, de la información

### *2.3 Servicios de Red*

Cuando abrimos un navegador de Internet e ingresamos una URL, accedemos a un servicio de red. La URL específica, entre otras cosas, la dirección remota de un equipo al que queremos acceder. Esta dirección remota (bajo una red TCP/IP) se denomina dirección IP.

El protocolo del servicio, que pertenece a la capa 7 o a la aplicación del modelo de referencia OSI, establecer las pautas sobre la comunicación entre la aplicación cliente y servidor.

### *2.4 Servicios*

#### *2.4.1 Webmin*

Webmin está dividido en diversos módulos. Cada uno de estos se encarga de la administración de una parte concreta del sistema operativo y de los diferentes servicios que tengamos instalados.

Crea una configuración para cada uno de los módulos basándose en la estructura de ficheros y configuración predeterminada para la versión y distribución de Linux seleccionadas.

Los módulos incluidos por defecto en Debían nos permiten administrar entre otros servicios Apache, Squid, Bind, Exim, Fetchmail, Samba, MySQL, etc.

Webmin también permite controlar varias máquinas a través de una interfaz simple, o iniciar sesión en otros servidores Webmin de la misma subred o red de área local.

#### *2.4.2 DHCP:*

Dynamic Host Configuration Protocol (DHCP). Asigna automáticamente direcciones IP y otra información de configuración de red a los ordenadores en una red.

Un cliente configurado para DHCP enviará una solicitud de difusión para el servidor DHCP solicita una dirección. El servidor DHCP emitirá entonces un "arrendamiento " y asignarlo a ese cliente. El período de tiempo de un contrato de arrendamiento válido se puede especificar en el servidor. DHCP reduce la cantidad de tiempo necesario para configurar los clientes y permite pasar de un ordenador a varias redes y configurarse con la máscara de dirección IP, puerta de enlace y de subred adecuada. Los servidores DHCP pueden asignar una dirección IP " estática " de hardware especificado.

#### *2.4.3 DNS:*

Domain Name System o DNS (en español «Sistema de Nombres de Dominio»). Es un sistema de nomenclatura jerárquico descentralizado para dispositivos conectados a redes IP como Internet o una red privada. Este sistema

asocia información variada con nombres de dominios asignado a cada uno de los participantes.

Su función más importante es "traducir" nombres inteligibles para las personas en identificadores binarios asociados con los equipos conectados a la red, esto con el propósito de poder localizar y direccionar estos equipos mundialmente.

#### *2.4.4 servicios Squid:*

Squid es un servido para web con cache. Es una de las aplicaciones más populares y de referencia para esta función, software libre publicado bajo licencia GPL. Entre sus utilidades está la de mejorar el rendimiento de las conexiones de empresas y particulares a Internet guardando en caché peticiones recurrentes a servidores web y DNS, acelerar el acceso a un servidor web determinado o añadir seguridad realizando filtrados de tráfico.

Squid es otro filtro a nivel de aplicación que puede complementar a iptables. Squid es un servidor proxy para web con caché, es muy popular y libre, además es multiplataforma. Aunque se puede usar para mejorar el rendimiento de las conexiones a Internet, también se puede usar con fines de seguridad. Desde que se inició el proyecto en los años 90

#### *2.4.5 Iptables*

Iptables permite al administrador del sistema definir las reglas acerca de qué hacer con los paquetes de red. Las reglas se agrupan en cadenas, cada cadena es una lista ordena de reglas. Las cadenas se agrupan en tablas; cada tabla está asociada con

un tipo diferente de procesamiento de paquetes. Forma parte del proyecto netfilter, que además de Iptables se compone por ip6tables, Ebtables, Arptables e Ipset.

Es un firewall muy configurable y flexible como la mayoría de elementos de Linux, y a pesar de haber tenido alguna vulnerabilidad, no por ello deja de ser especialmente potente. Al estar dentro del núcleo, se inicia con el sistema y se mantiene activo todo el momento y al estar al nivel del kernel, recibirá paquetes y estos serán aceptados o rechazados consultando las reglas de Iptables.

Cada paquete de red llega a un computador o que se envía desde una computadora recorre por lo menos una cadena y cada regla de esa cadena se comprueba con el paquete.

Si la regla cumple con el datagrama, el recorrido se detiene y el destino de la regla dicta lo que se debe hacer con el paquete. Si el paquete alcanza el fin de una cadena predefinida sin haberse correspondido con ninguna regla de la cadena dicta que hacer con el paquete, si el paquete alcanza el fin de una cadena o sin la cadena definida por el usuario.

En Iptables las reglas se agrupan en cadenas es un conjunto de reglas para paquetes IP, que determina qué hacer con ellos. Cada regla puede desechar el paquete de la cadena él lo cual otras cadenas no serán consideradas. Una cadena puede tener un enlace a otra cadena: si el paquete pasa a través de esa cadena entera o si cumple una regla de destino de retorno.

Va a continuar en la primera cadena, no hay un límite respecto de cuan anidadas pueden estar las cadenas hay tres cadenas básicas (input, output, forward:

entrada salida y reenvió). Y el usuario puede crear tantas como desee, una regla puede ser simplemente un puntero a una cadena.

Es posible crear nuevas tablas mediante módulos de extensión. El administrador puede cargar y eliminar cadenas definidas por usuarios dentro de cualquier tablas inicialmente, todas las cadenas vacías y tiene un política de destino que permite que todos los paquetes pasen sin ser bloqueados o alterados.

#### *2.4.6 características de Iptables.*

- Filtrado de paquetes sin estado (ipv4 e ipv6)
- Filtrado de paquetes de estado (ipv4 e ipv6)
- Todo tipo de dirección de red y traducción de puertos, por ejemplo, NAT/NAPT ipv4 e ipv6)
- Infraestructura flexible y extensible
- Múltiples capas de la API para extensiones de tercera parte

### *2.5 Netfilter*

Netfilter es un Framework disponible en el núcleo Linux que permite interceptar y manipular paquetes de red, este permite realizar el manejo de paquetes en diferentes estados del procesamiento.

El componente más popular construido sobre Netfilter es Iptables, una herramienta de cortafuegos que permite no solamente filtrar paquetes, sino también realizar traducción de direcciones de red (NAT) para IPv4 o mantener registros de log.

El proyecto Netfilter no sólo ofrece componentes disponibles como módulos del núcleo sino que también ofrece herramientas de espacio de usuario y librerías.

#### *2.5.1 ¿Qué puedo hacer con Netfilter / Iptables?*

- Construir los cortafuegos de internet basado con el filtrado de paquetes sin estado y con estado.
- implementar clústeres de firewall sin estado y con estado de alta disponibilidad.
- Utilizar NAT y haciéndose pasar por compartir el acceso a internet si usted no tiene suficientes direcciones IP públicas.
- Utilizar NAT para implementar Proxies transparentes
- Hacer aún más manipulación de paquetes como la alteración de los bits /ecn TOS / DSCP d la cabecera IP.

### *2.6 Arquitectura y teoría de Firewall.*

Los filtros de paquetes, son una forma eficaz de control de tráfico entrante y saliente hacia una red. La gran ventaja es que al trabajar sobre las capas IP y TCP/IP, no deben hacer cambios a nivel de la aplicación.

#### *2.6.1 Firewall.*

El Firewall surge como una herramienta principal para ejecutar la política de seguridad de una organización. Al trabajar en todas las capas del modelo son complementarios a los filtros de paquete.

### *2.6.2 Firewall e Internet.*

El Firewall se instala entre la conexión de la red interna y el enlace a internet. Todo el tráfico que viene y sale a Internet pasa por el Firewall, su configuración, debe de estar en concordancia con la política de seguridad definida. Hoy en día una red conectada a Internet sin un Firewall es altamente riesgosa.

### *2.6.3 ¿qué puede hacer un Firewall?*

Ser una fuente de decisiones de seguridad. Permite concentrar las medidas de seguridad en un solo punto de red. Refuerza las políticas de seguridad.

La mayoría de los servicios que los usuarios demandan de Internet, son inseguros. Por ejemplo, el uso de NFS desde fuera de la organización.

Almacenar su relación con Internet. Por ser “cuello de botella”. Es factible registrar lo que ocurre entre la red protegida y la externa. Limitar la exposición. Se puede usar un Firewall interno, es decir, dentro de la misma organización.

## *2.7 Tipos de Firewall.*

### *2.7.1 Hardware*

Este tipo de sistema es colocado sobre los dispositivos usados para ingresar a Internet, los llamados “Routers”. Frecuentemente la instalación ya se encuentra realizada cuando compramos el Router. En caso contrario es muy recomendable realizar la instalación. La colocación del Firewall en este caso es muy compleja, es hecha gracias a un navegador que tiene acceso a Internet.

Host de base dual: este tipo de equipo utiliza dos tarjetas, una de las tarjetas conecta el equipo con una red interna y la otra con las redes externas.

Host de bastión: Se trata de un computador con una sola tarjeta de red. Un Router de selección de filtro de paquetes, se interpone entre la red externa y el bastión. De esta forma se introduce un nivel adicional de seguridad al momento de tratar de penetrar las redes.

#### *2.7.2 Software:*

Pueden ser distinguidos dos tipos de estos Firewalls, el primero es el gratuito: también conocido bajo el nombre de software firewall, que puede ser usado con total libertad y de manera totalmente gratuita como su nombre indica.

Su objetivo es rastrear y no permitir acceso a ciertos datos a las computadoras personales. Este sistema es caracterizado por su fácil instalación, al que pueden ser sumados otros sistemas para asegurar la computadora, cuando deja de funcionar, es la misma PC quien se encarga de avisarlo, no es requerido un sistema de Hardware para colocarlo y generalmente son utilizado en una sola computadora.

## Capítulo III

### *3.1 Metodología de la Investigación:*

#### *3.1.1 participantes*

En la Universidad Tecnológica de El salvador se realizó una Encuesta a 15 alumnos que cursaban la materia de Administración de Redes en el ciclo 01-2016, con el fin de identificar el si había necesidad de guías de configuración de sistemas Operativos como Debían, dichos alumnos se escogieron por mostrar mayor interés en la materia y presentar un CUM más alto que otros. Se realizaron Las siguientes preguntas cerradas:

- ¿Ha trabajado usted con algún servidor?
- ¿Tiene acceso a Pc para realizar las prácticas de configuración?
- ¿Son importantes las guías de Configuración de sistemas operativos para la Asignatura Administración De redes?
- ¿has utilizado la consola de la distribución Debían?
- ¿Tiene acceso a Guías de configuración de Debían?
- ¿utilizaría un servidor Debían?

Como población disponible para el estudio son alumnos del técnico en ingeniería de Redes computacionales que cursaron la materia administración de redes en el ciclo 01-2016

### 3.1.2 método:

El estudio de los alumnos de la Materia Administración de Redes se lleva a cabo Siguiendo los parámetros de Método inductivo de investigación tomando en cuenta una porción de los estudiantes para concluir de forma general.

Hemos llevado a cabo una encuesta tomando en cuenta a 15 alumnos cursantes de la materia Administración de redes; Los quince alumnos tienen acceso a una pc para realizar las configuraciones al igual que tienen conocimientos de sistemas operativos.

### 3.1.3 instrumentos:

La investigación fue realizada apoyándonos con los Catedráticos que han impartido la materia de Administración de Redes Ciclo 01-2016 Juan Carlos Aguilar y William Enrique García, mostrando en que temas nuestra guía podría ayudar a los alumnos.

*Tabla 2:* Temas de Administración de redes en los que apoyarían las guías de configuración.

| Nº Unidad | Tema a Impartir                      | Apoyo de Guías              |
|-----------|--------------------------------------|-----------------------------|
| Unidad 2  | Administración de La seguridad       | Configuración de Iptables.  |
| Unidad 4  | Implementación de Servicios en Linux | Configuración de DHCP y DNS |

Willian G. (2016). *Investigación/Catedrático de Administración de Redes*

A través de la investigación por medio de la biblioteca de La Universidad Tecnológica De El Salvador identificamos que no posee material didáctico para realizar dichas configuraciones del sistema operativo Debían.

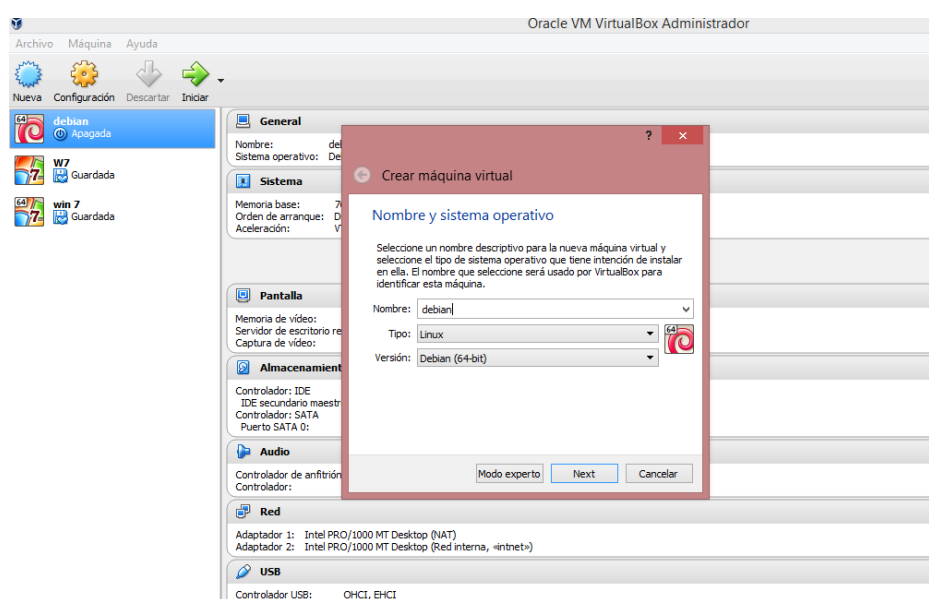
*Tabla 3: Herramientas necesarias para elaboración de guías didácticas y realización de prácticas*

| Producto        | Costo                                                                                  |
|-----------------|----------------------------------------------------------------------------------------|
| <b>Hardware</b> | \$0.00 (El lab. de redes cuenta con 40 computadoras a disposición para las prácticas.) |
| <b>Software</b> | \$0.00 (incluido con el equipo.)                                                       |

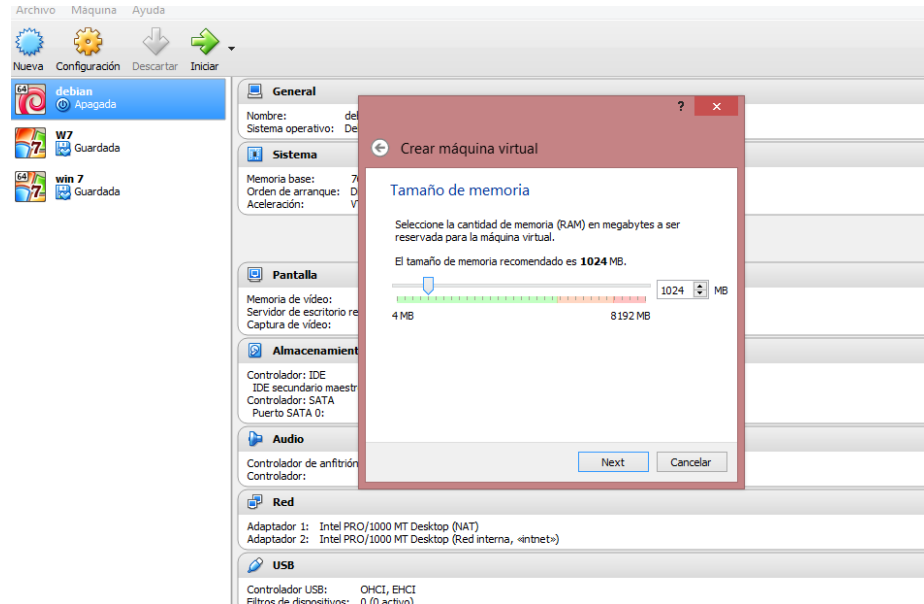
### 3.1.4 Procedimientos, guías de configuración

#### 3.1.4.1 instalación Debían

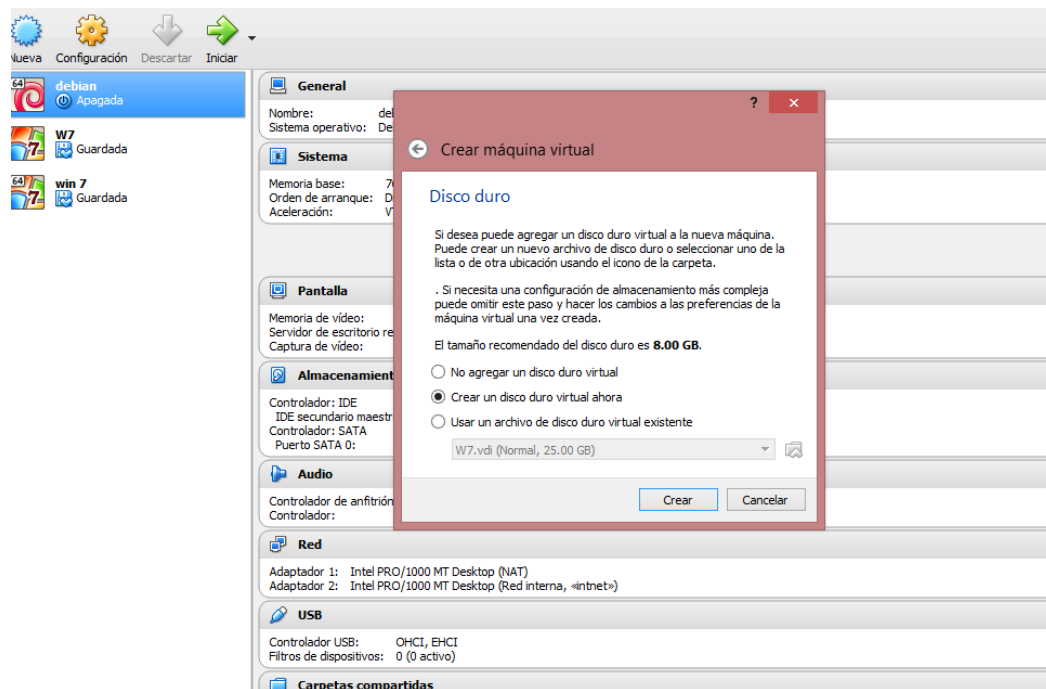
- 1- Abrimos virtual box y creamos una nueva máquina con el nombre de Debían



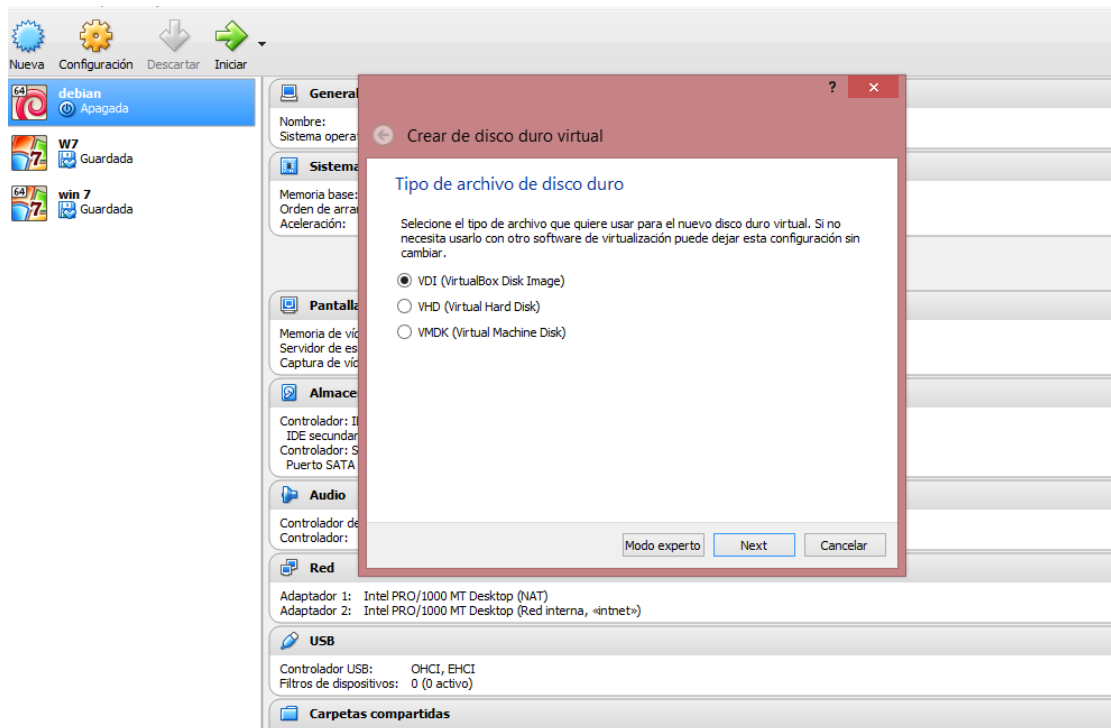
- 2- En el siguiente paso escogemos la memoria RAM que tendrá nuestro sistema operativo.



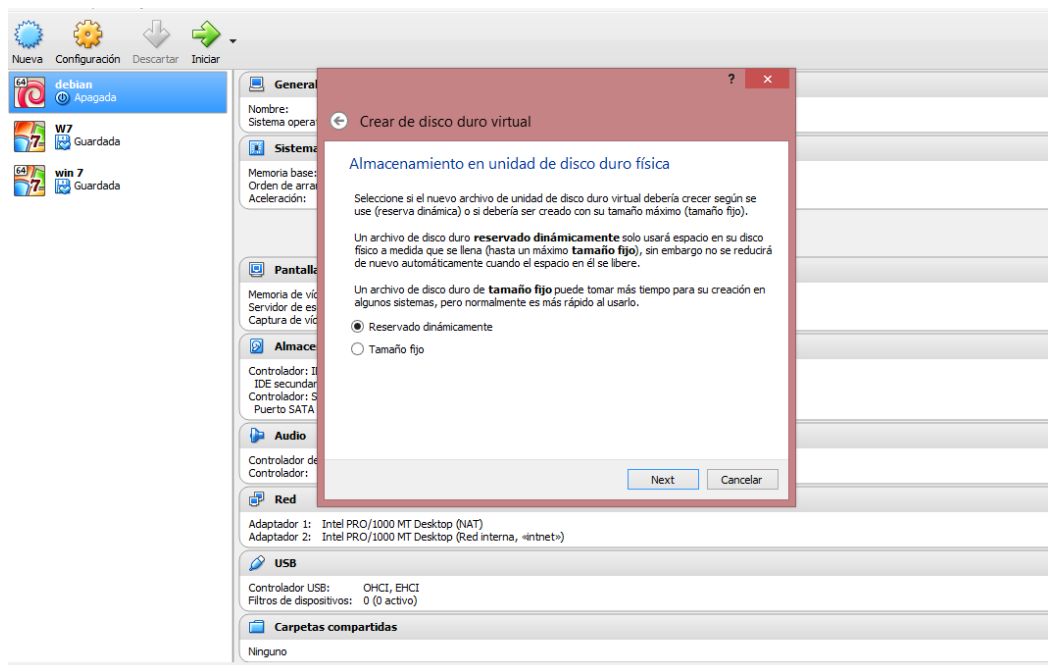
- 3- Crearemos un disco duro virtual.



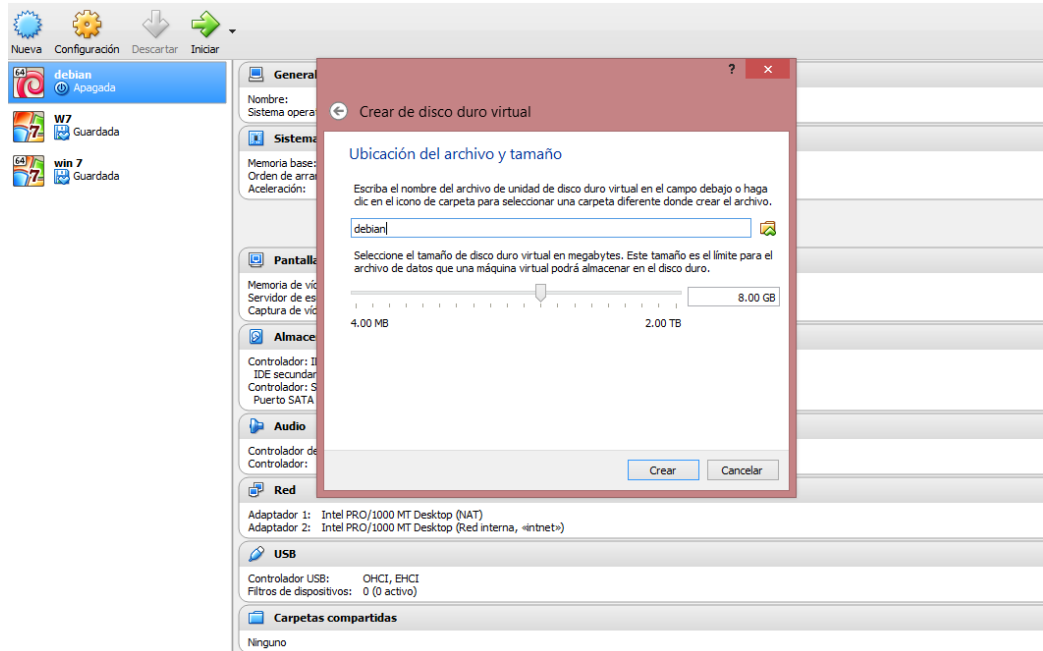
4- En este paso proseguiremos a escoger el tipo de disco duro virtual.



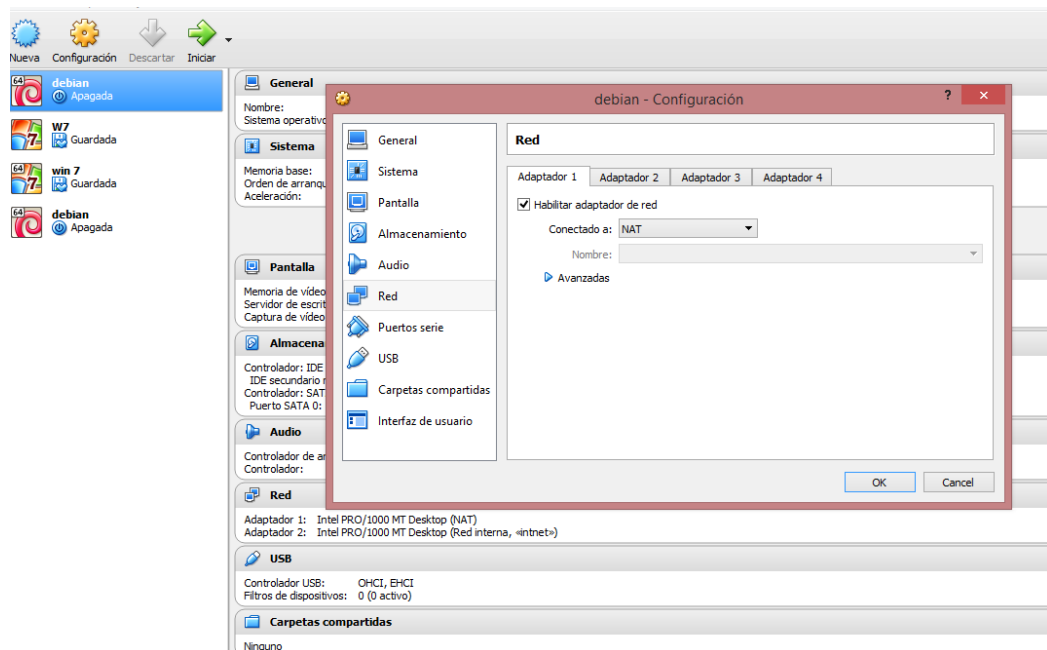
5- Seleccionamos una unidad reservado dinámicamente.



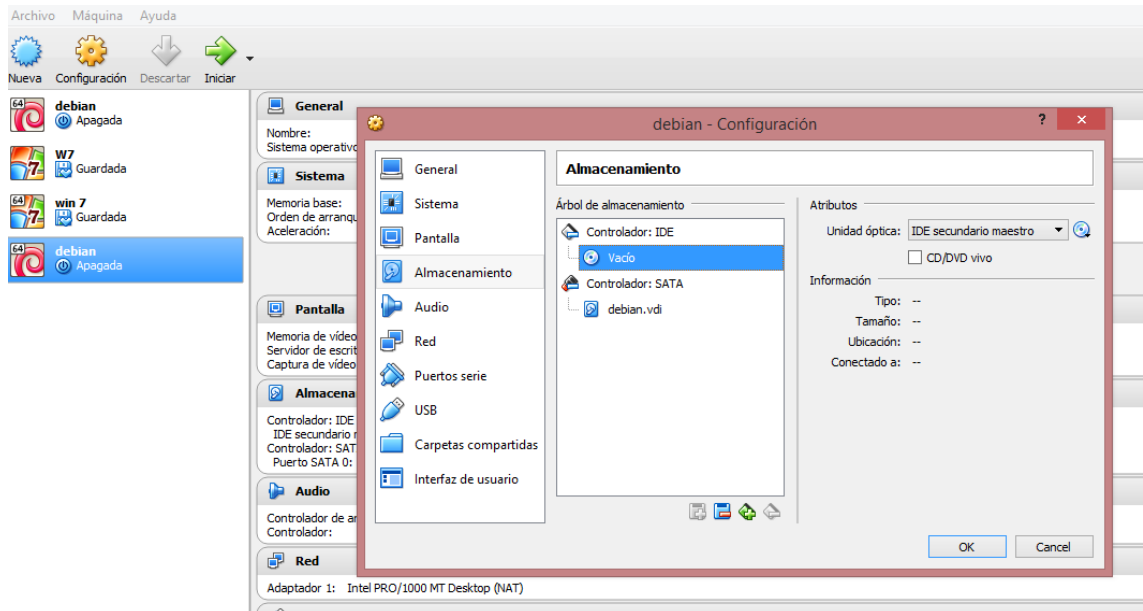
- 6- Seleccionaremos el tamaño del disco duro que utilizaremos en el sistema operativo.



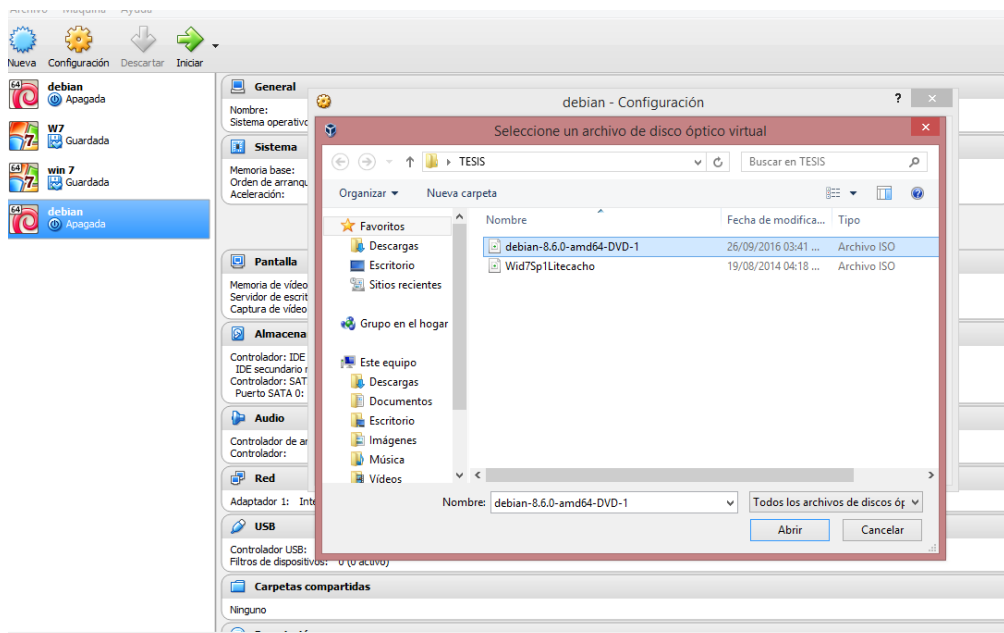
- 7- Tenemos que entrar en configuración de la máquina virtual y activamos el adaptador 1 conectado a la NAT.



8- Nos vamos a opción de Almacenamiento y nos dirigimos a la opción de controlador IDE.



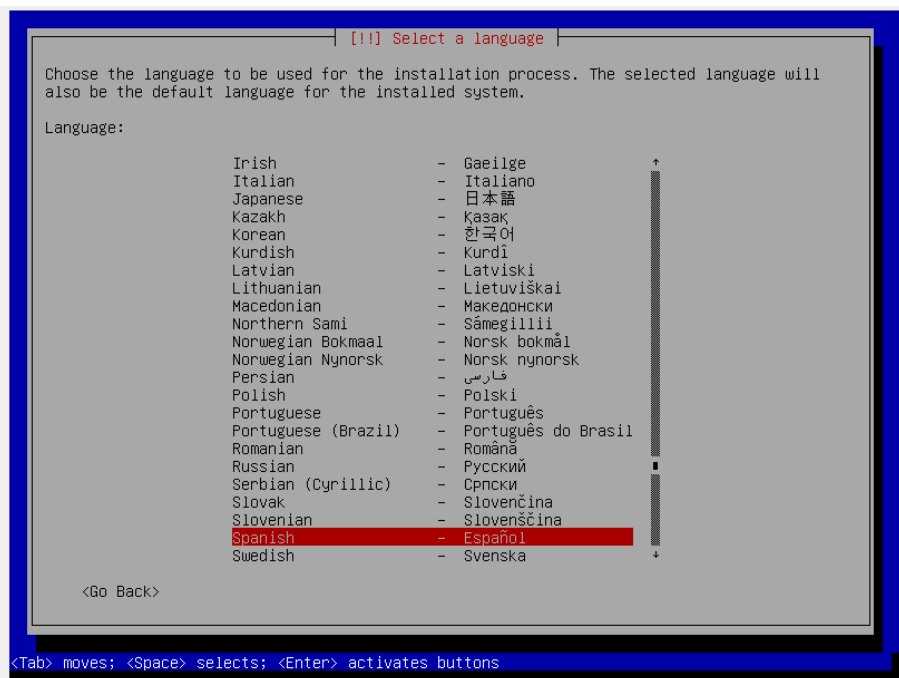
9- Luego seleccionamos la ISO de debían 8 (última versión actualmente)



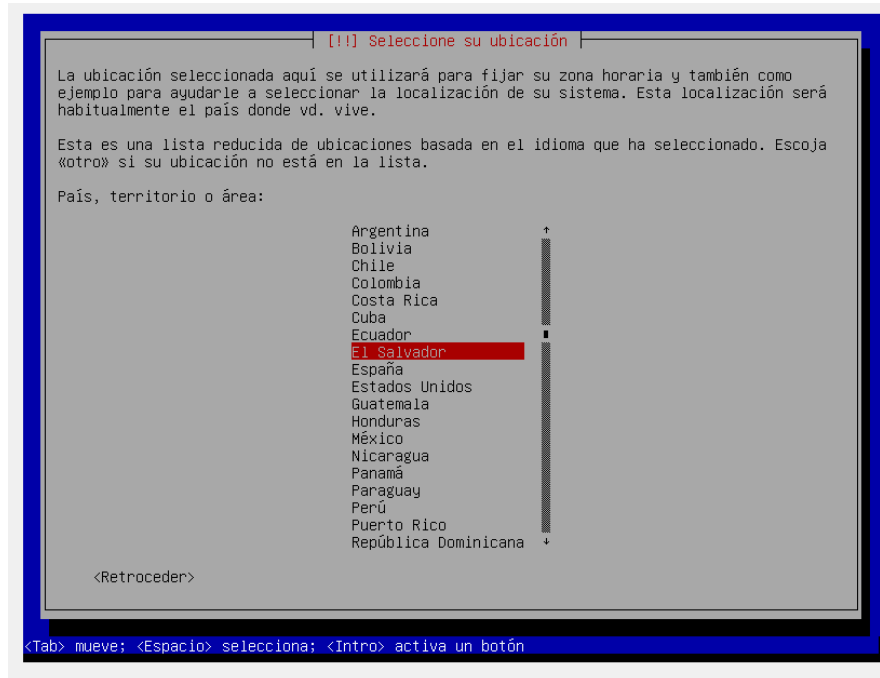
10- Siguiendo el siguiente paso iniciamos la máquina virtual y se nos mostrara el perfil de debían y escogemos a la opción de instalar.



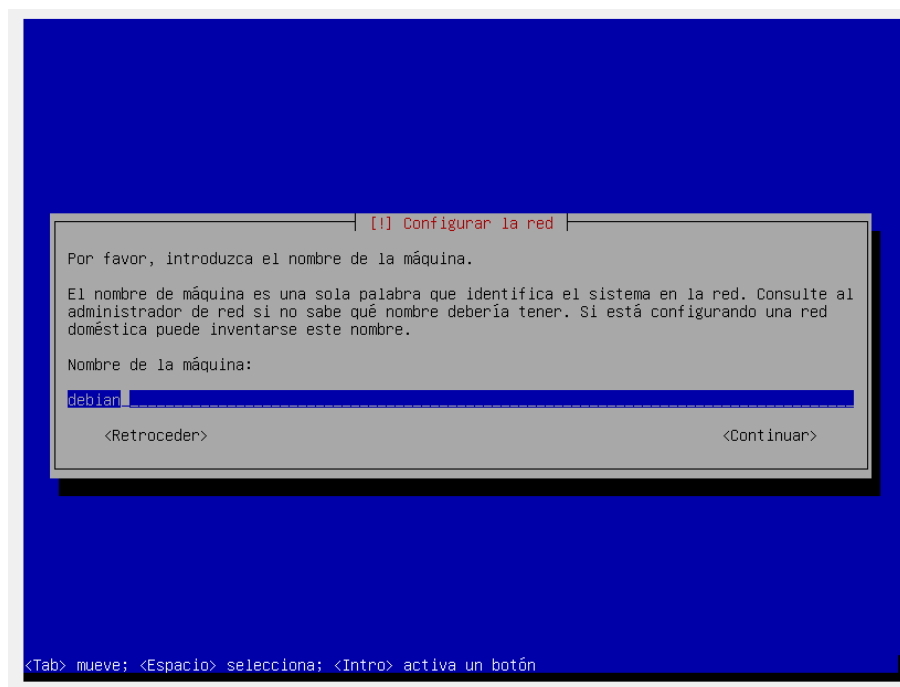
11- Luego proseguiremos a escoger el tipo de idioma que utilizaremos.



12- Luego escogemos el país para configurar la zona horaria.



13- En el siguiente paso continuaremos en poner el nombre de nuestra máquina.



## 14- Luego nombraremos el dominio.

[!!] Configurar la red

El nombre de dominio es la parte de su dirección de Internet a la derecha del nombre de sistema. Habitualmente es algo que termina por .com, .net, .edu, o .org. Puede inventárselo si está instalando una red doméstica, pero asegúrese de utilizar el mismo nombre de dominio en todos sus ordenadores.

Nombre de dominio:

acl.debian

<Retroceder> <Continuar>

<Tab> mueve; <Espacio> selecciona; <Intro> activa un botón

## 15- Proseguiremos a poner la contraseña del súper usuario.

[!!] Configurar usuarios y contraseñas

Necesita definir una contraseña para el superusuario («root»), la cuenta de administración del sistema. Podría tener graves consecuencias que un usuario malicioso o un usuario sin la debida cualificación tuviera acceso a la cuenta del administrador del sistema, así que debe tener cuidado y elegir una contraseña para el superusuario que no sea fácil de adivinar. No debería ser una palabra que se encuentre en el diccionario, o una palabra que pueda asociarse fácilmente con usted.

Una buena contraseña debe contener una mezcla de letras, números y signos de puntuación, y debe cambiarse regularmente.

La contraseña del usuario «root» (administrador) no debería estar en blanco. Si deja este valor en blanco, entonces se deshabilitará la cuenta de root creará una cuenta de usuario a la que se le darán permisos para convertirse en usuario administrador utilizando la orden «sudo».

Tenga en cuenta que no podrá ver la contraseña mientras la introduce.

Clave del superusuario:

<Retroceder> <Continuar>

<Tab> mueve; <Espacio> selecciona; <Intro> activa un botón

16- Nos volverá a pedir la contraseña para comprobar.

[!!] Configurar usuarios y contraseñas

Por favor, introduzca la misma contraseña de superusuario de nuevo para verificar que la introdujo correctamente.

Vuelva a introducir la contraseña para su verificación:

<Retroceder> <Continuar>

<Tab> mueve; <Espacio> selecciona; <Intro> activa un botón

17- Luego nos pedirá el nombre completo para el usuario nuevo.

[!!] Configurar usuarios y contraseñas

Se creará una cuenta de usuario para que la use en vez de la cuenta de superusuario en sus tareas que no sean administrativas.

Por favor, introduzca el nombre real de este usuario. Esta información se usará, por ejemplo, como el origen predeterminado para los correos enviados por el usuario o como fuente de información para los programas que muestren el nombre real del usuario. Su nombre completo es una elección razonable.

Nombre completo para el nuevo usuario:

userac

<Retroceder> <Continuar>

<Tab> mueve; <Espacio> selecciona; <Intro> activa un botón

18- Luego nos pedirá el nombre de usuario para la cuenta.

!!! Configurar usuarios y contraseñas

Seleccione un nombre de usuario para la nueva cuenta. Su nombre, sin apellidos ni espacios, es una elección razonable. El nombre de usuario debe empezar con una letra minúscula, seguida de cualquier combinación de números y más letras minúsculas.

Nombre de usuario para la cuenta:

userac1

<Retroceder> <Continuar>

<Tab> mueve; <Espacio> selecciona; <Intro> activa un botón

19- Luego nos pedirá una contraseña para el nuevo usuario.

!!! Configurar usuarios y contraseñas

Una buena contraseña debe contener una mezcla de letras, números y signos de puntuación, y debe cambiarse regularmente.

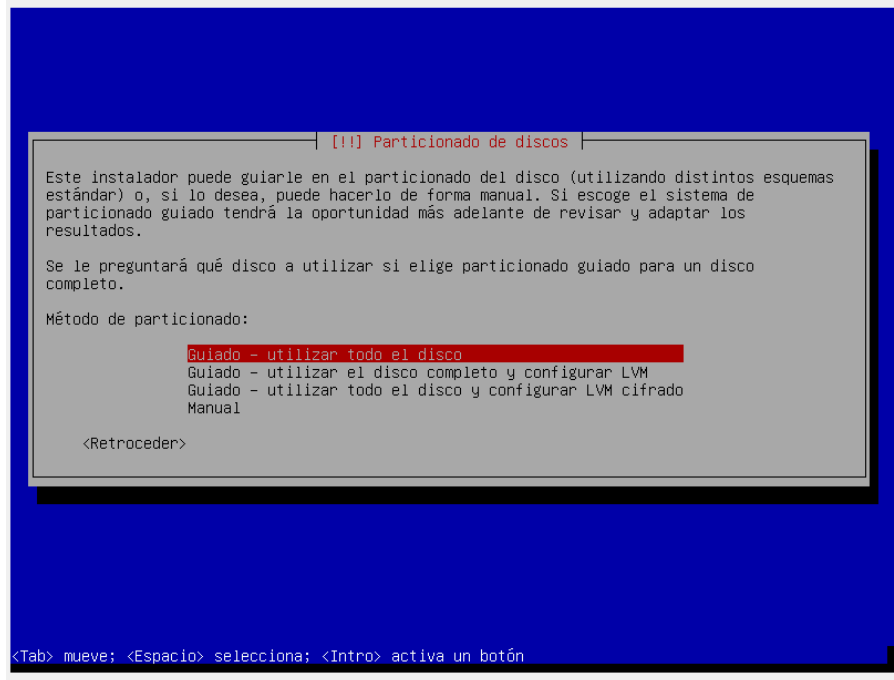
Elija una contraseña para el nuevo usuario:

\*\*\*\*\*

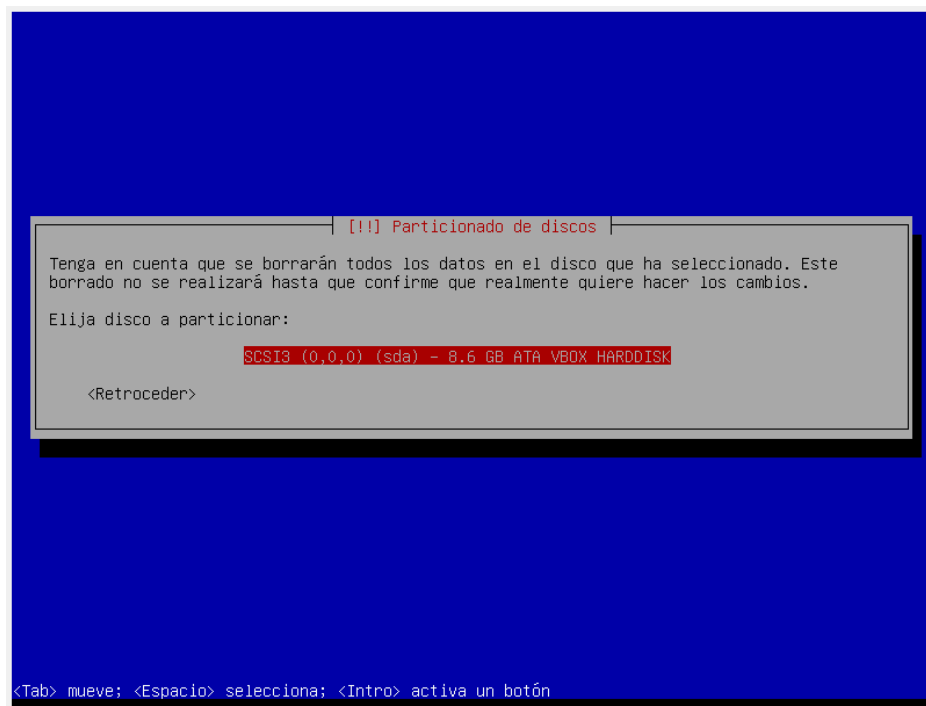
<Retroceder> <Continuar>

<Tab> mueve; <Espacio> selecciona; <Intro> activa un botón

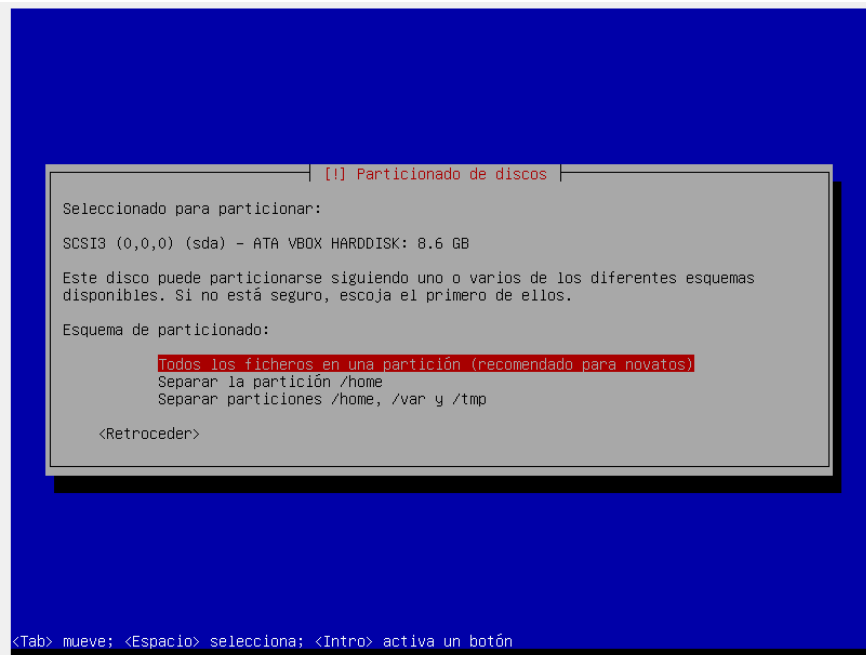
20- Luego nos pedirá el método de partición del disco.



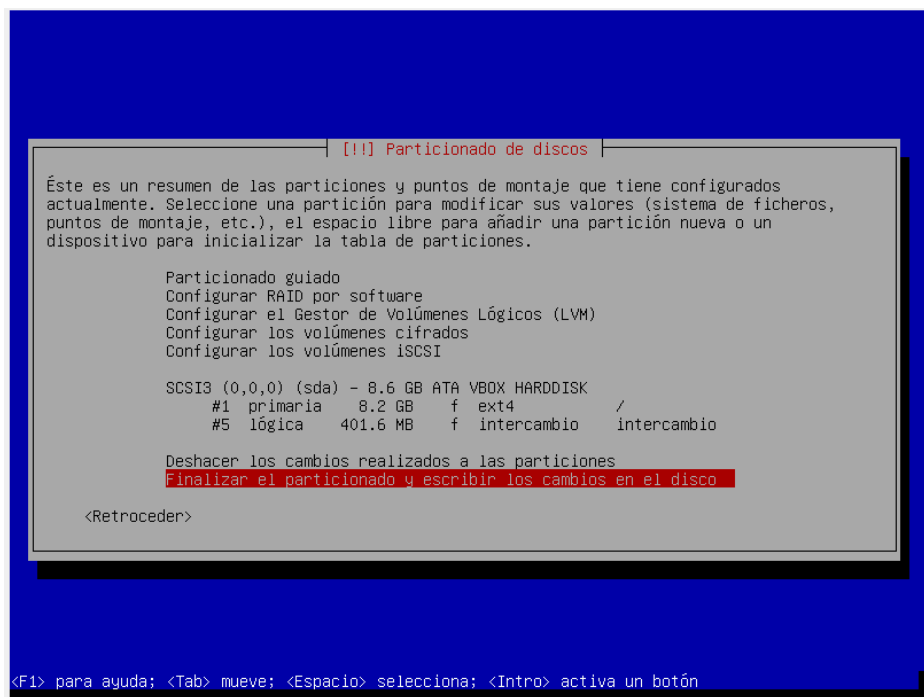
21- Luego escogeremos el disco para particionar.



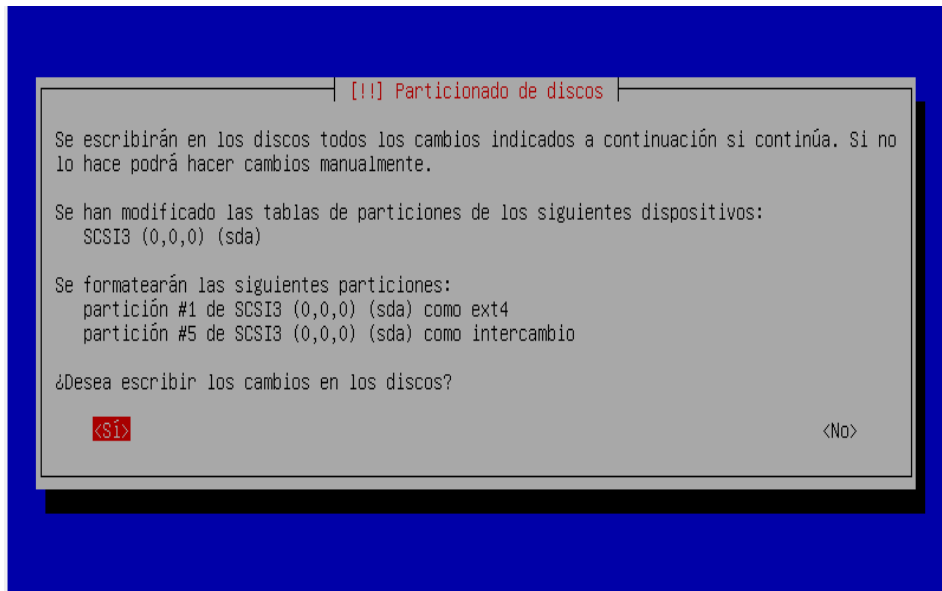
22- Luego procederemos a escoger a escoger el esquema de particionado.



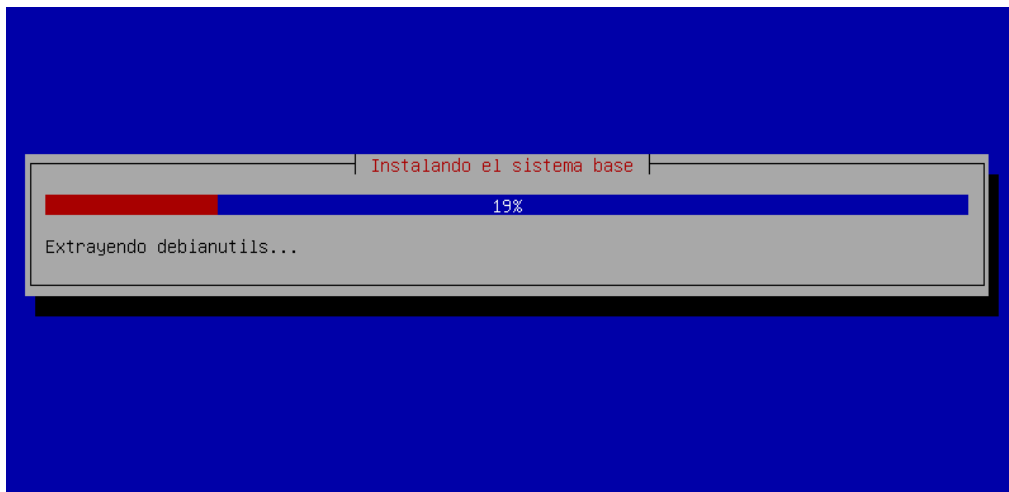
23- Luego nos mostrara el resumen de las particiones y la finalización del procedimiento de partición del disco.



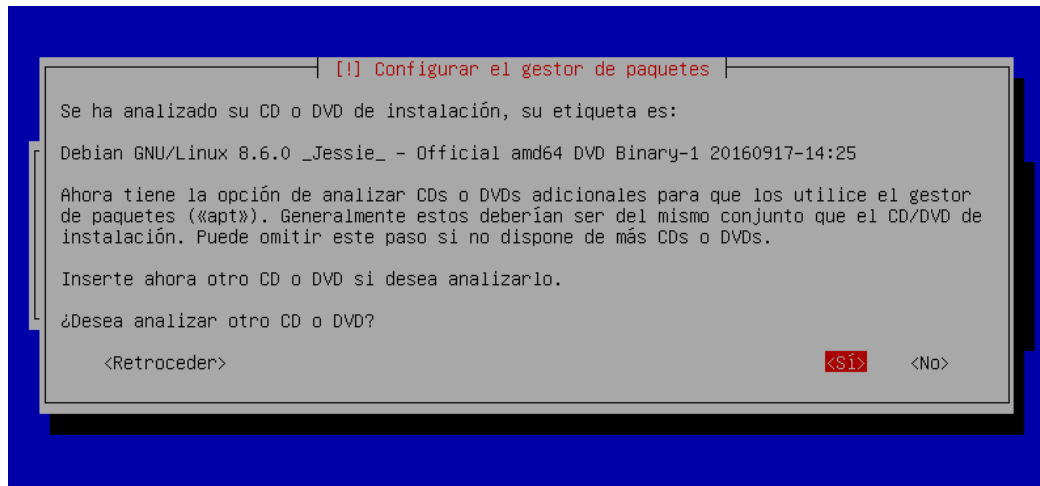
24- Luego nos mostrar una opción de si estamos seguros de escribir los cambios del disco.



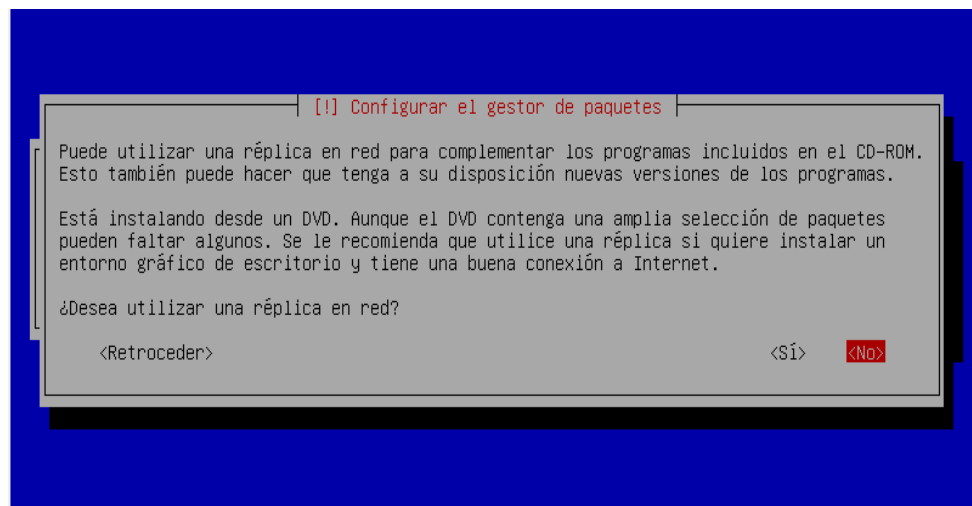
25- Luego esperamos la instalación del sistema base.



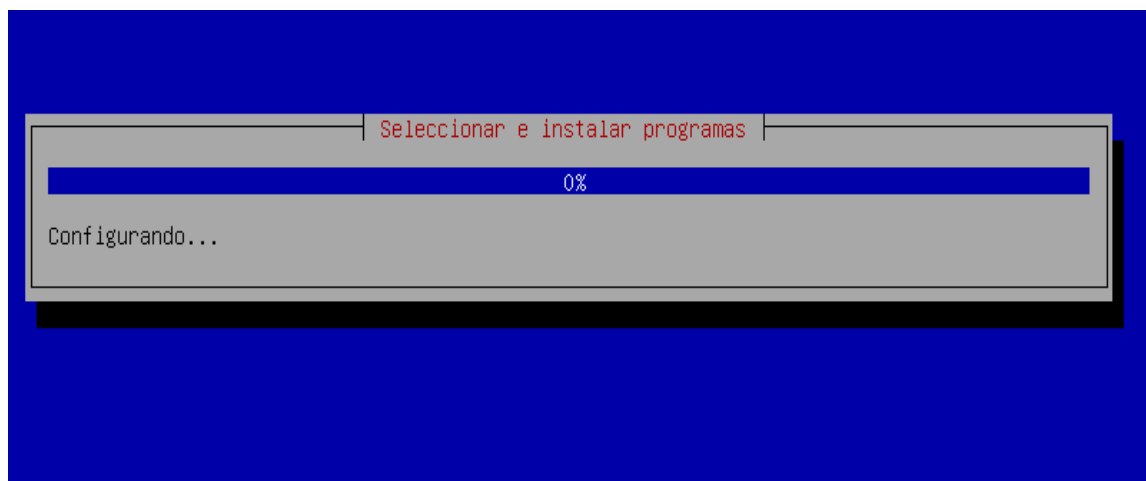
26- Luego nos pedirá si tenemos otro cd o dvd para agregarlo a la instalación.



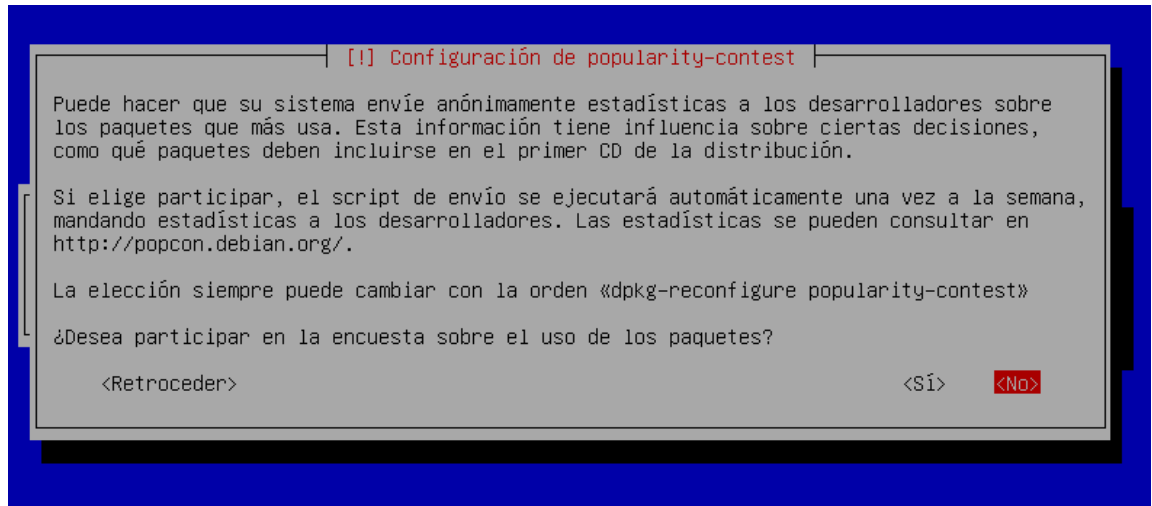
27- Luego se nos presenta esta opción para realizar una réplica de red



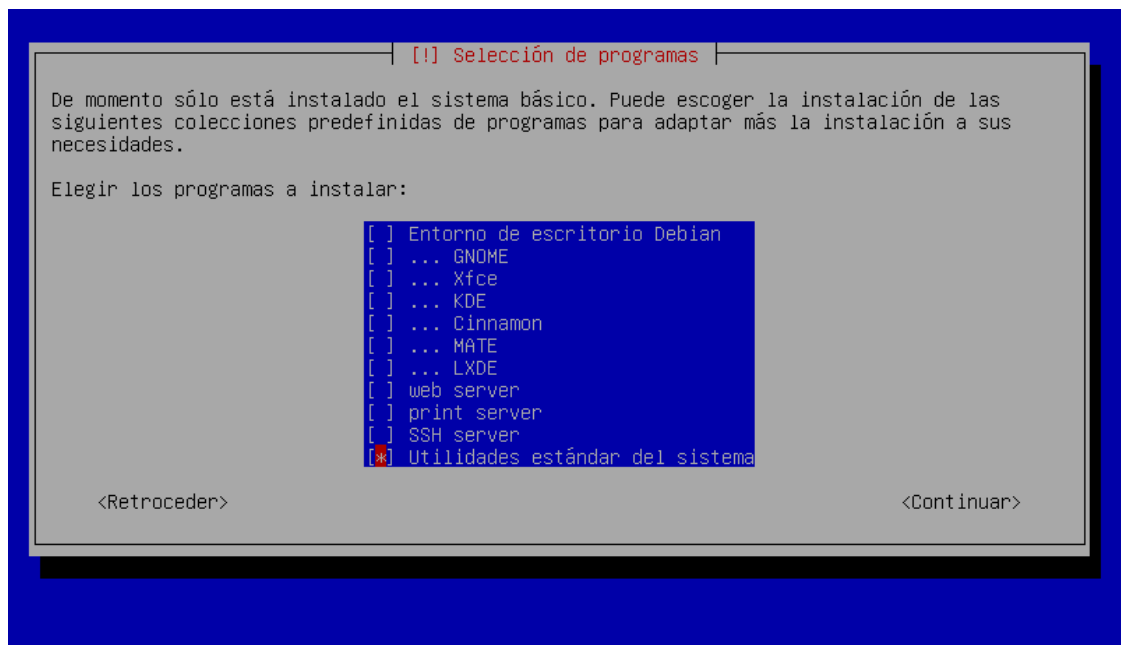
28- Tenemos que esperar un momento mientras se instalan los paquetes.



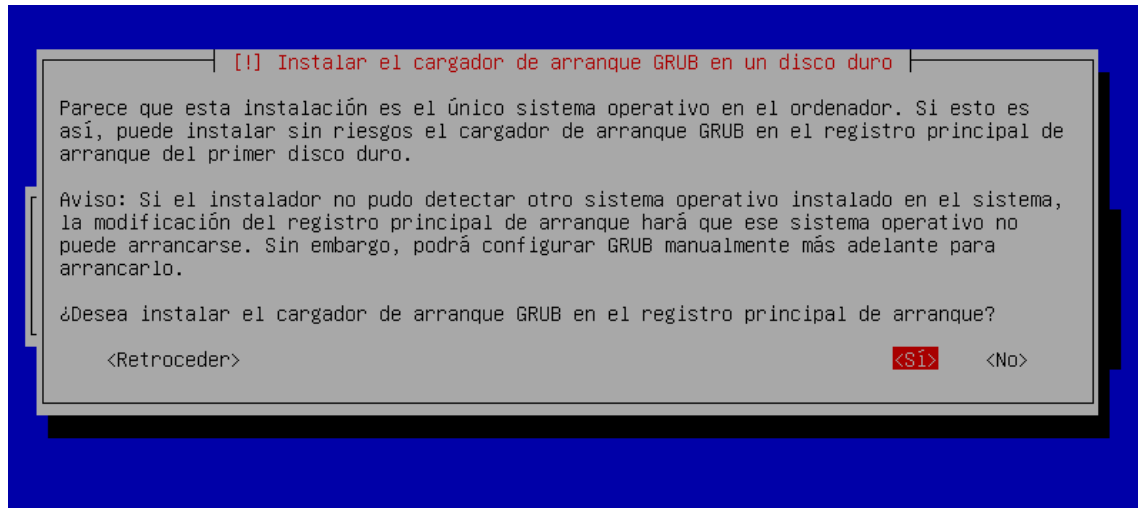
29- Luego nos aparecerá una ventana donde nos dará una opción de una encuesta sobre el uso de los paquetes.



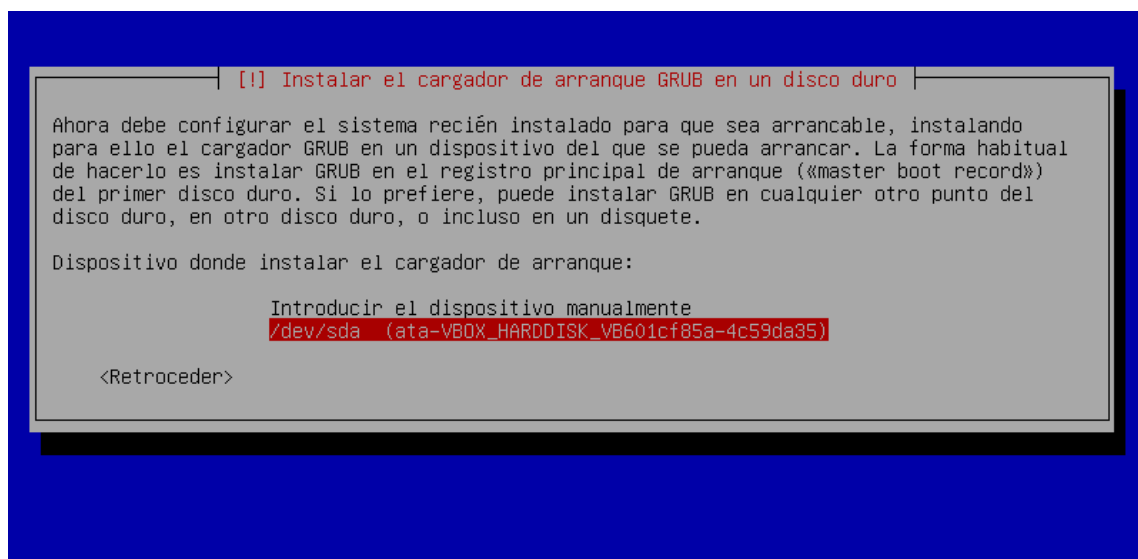
30- Luego nos aparecerá el listado de programas a instalar.



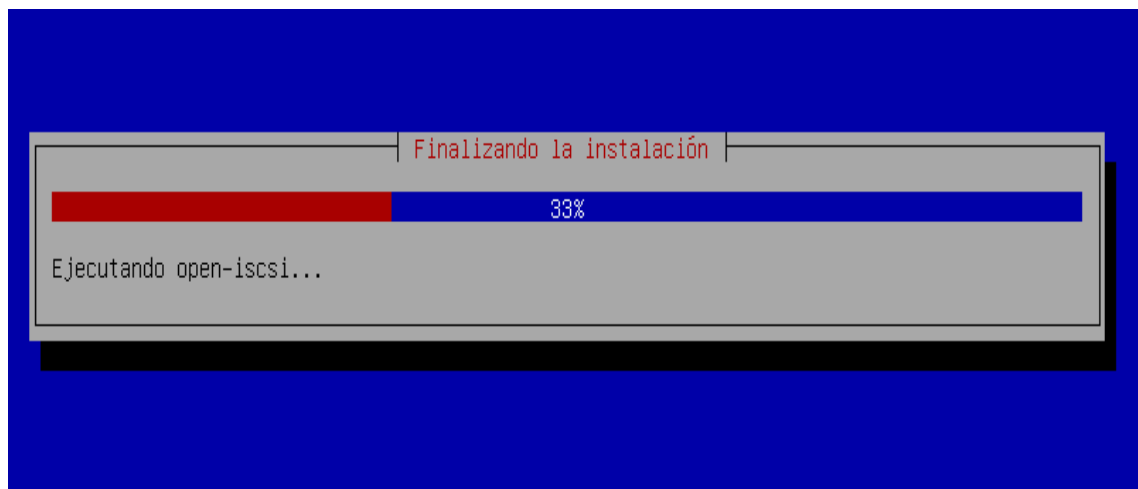
31- Siguiente paso nos mostrara si deseamos instalar el cargador de arranque GRUB en el registro principal de arranque.



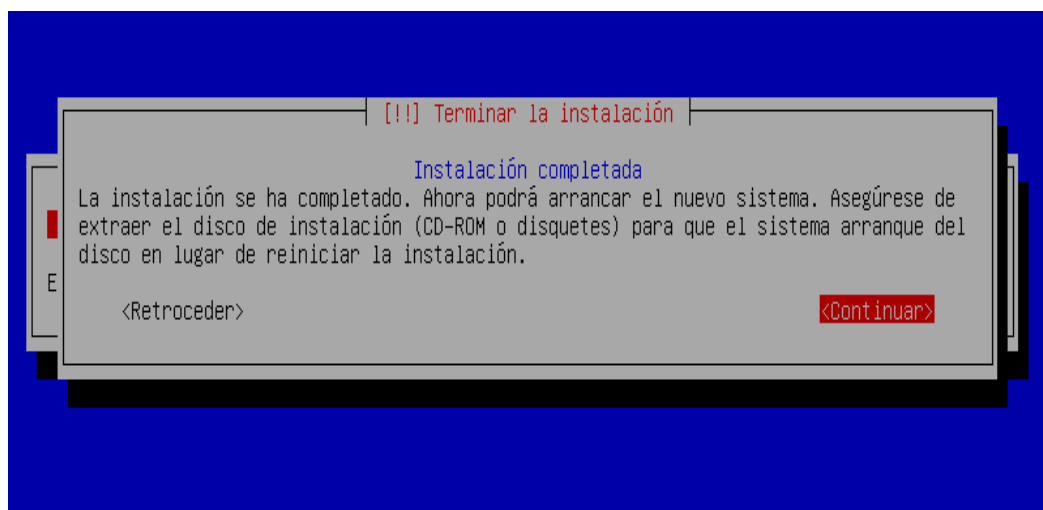
32- En el siguiente paso escogeremos donde instalar el cargador de arranque.



33- Luego esperamos a la finalización de la instalación.



34- Luego terminaremos la instalación y proseguimos a continuar.



35- Y al finalizar la instalación nos mostrar la ventana de modo en consola.

```
Debian GNU/Linux 8 debian tty1
debian login: useracl
Password:
Linux debian 3.16.0-4-amd64 #1 SMP Debian 3.16.36-1+deb8u2 (2016-10-19) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

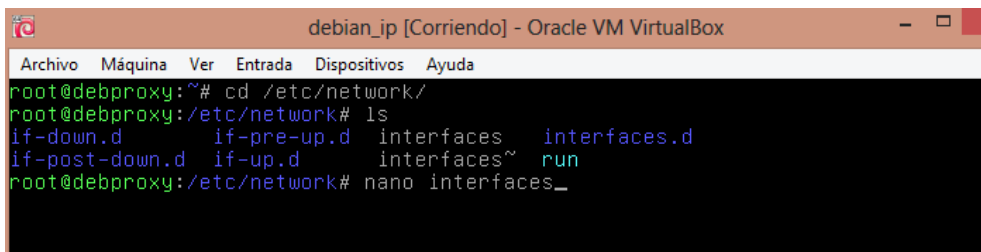
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
useracl@debian:~$ _
```

### 3.1.4.2 configuración de DHCP

1. Como primer pasó configuramos nuestra tarjeta de red la cual le colocaremos una dirección estatica.

La mayor parte de la configuración de la red se puede hacer desde el archivo de configuración interfaces en /etc/network/interfaces. Aquí, usted puede dar a su tarjeta de red una dirección IP (o usar dhcp), establecer la información de enrutamiento, configurar el enmascaramiento IP, poner las rutas por defecto y mucho más.

Entraremos empezando de cd /etc/network/ y editamos el archivo con el comando nano interfaces



```
root@debproxy:~# cd /etc/network/
root@debproxy:/etc/network# ls
if-down.d      if-pre-up.d  interfaces    interfaces.d
if-post-down.d if-up.d      interfaces~   run
root@debproxy:/etc/network# nano interfaces_
```

```
GNU nano 2.2.6          Fichero: interfaces

# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo eth1 eth0
iface lo inet loopback

# The primary network interface
allow-hotplug eth0
iface eth0 inet dhcp
        post-up iptables-restore < /etc/iptables.up.rules

# secondary
iface eth1 inet static
        address 192.168.5.254
        netmask 255.255.255.0
        broadcast 192.168.5.255
        network 192.168.5.0
```

En nuestro caso la interfaz que editaremos es “eth1” que será la red interna

2. Luego instalamos el servicio dhcp con el comando:

`Apt-get install isc-dhcp-server`

(DHCP Es un servicio de red que permite a los equipos host que se asignará automáticamente la configuración de un servidor en lugar de configurar manualmente cada host de la red. Los equipos configurados para ser clientes DHCP no tienen control sobre los ajustes que reciben del servidor DHCP, y la configuración es transparente para el usuario de la computadora.)

```
debian_ip [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
root@debproxy:/etc/network# apt-get install isc-dhcp-server
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
isc-dhcp-server ya está en su versión más reciente.
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 0 no actualizados.
root@debproxy:/etc/network# _
```

- Después que el servicio fue instalado como siguiente paso Es probable que tenga que cambiar la configuración por defecto editando `/etc/dhcp/dhcpd.conf` para sus necesidades y configuración particular, rango el cual asignara el servidor dhcp  
Vamos desde raíz con `cd /etc/dhcp/`  
Ls (para verificar que hay en la carpeta)  
Configuramos `dhcpd.conf` con `(nano dhcpd.conf)`



```
debian_ip [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
root@debproxy:/etc/network# cd /etc/dhcp/
root@debproxy:/etc/dhcp# ls
dhclient.conf          dhclient-exit-hooks.d  dhcpd.conf.lock
dhclient-enter-hooks.d  dhcpd.conf
root@debproxy:/etc/dhcp# nano dhcpd.conf_
```

- Entramos a `dhcpd.conf` y luego:

Se debe asignar una dirección IP estática a la interfaz que va a utilizar para DHCP. Si va a utilizar `eth1` para proporcionar direcciones en la subred `192.168.1.x`, entonces debería asignar por ejemplo IP `192.168.1.1` a la interfaz `eth1`. Sin este paso obtendrá un error de `dhcpd` al iniciar el servicio.

Al terminar guardamos dando `(control+O)` luego `enter` y luego `(control+X)` para salir.

```
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
GNU nano 2.2.6  Fichero: dhcpd.conf  Modificado

option broadcast-address 10.254.239.31;
option routers rtr-239-32-1.example.org;
}

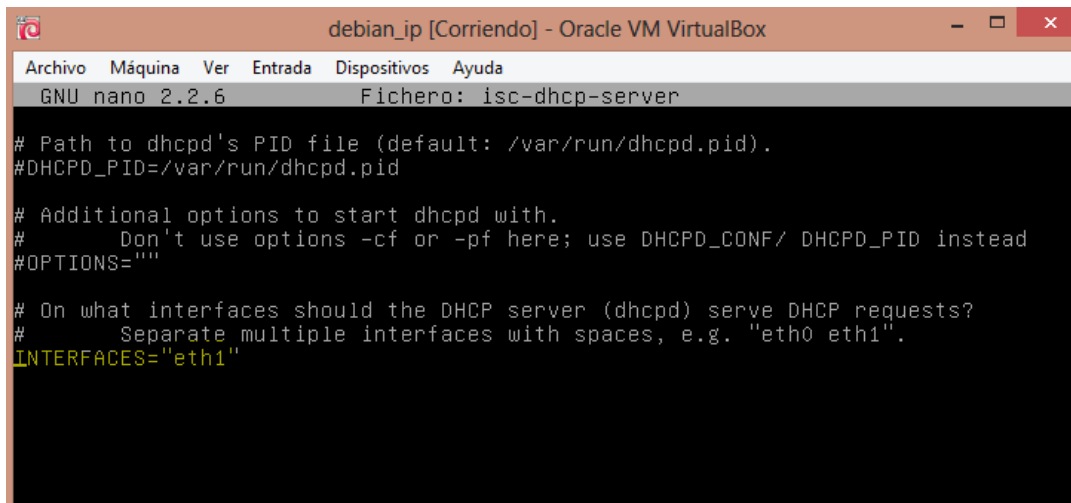
A slightly different configuration for an internal subnet.
subnet 192.168.2.0 netmask 255.255.255.0 {
  range 10.5.5.26 10.5.5.30;
  option domain-name-servers 192.168.2.1;
  option domain-name "debacl.net";
  option routers 192.168.2.1;
  option broadcast-address 192.168.2.255;
  default-lease-time 600;
  max-lease-time 7200;
}

Hosts which require special configuration options can be listed in
host statements.  If no address is specified, the address will be
allocated dynamically (if possible), but the host-specific information
will still come from the host declaration.
```

5. Luego también tendrá que editar / etc / default / isc-dhcp-server para especificar las interfaces que dhcpd debería escuchar. Por defecto se escucha eth0. Configuramos con el comando  
Cd /etc/default/ y luego colocaremos en nuestro caso la interfaz ETH1  
Y para editar damos nano isc-dhcp-server

```
debian_ip [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
root@debproxy:~# cd /etc/default/
root@debproxy:/etc/default# ls
acpid      bsdmainutils  dbus      halt      locale      rcS      useradd
anacron    console-setup devpts    hwclock   networking  rsyslog
bind9      crda          exim4     isc-dhcp-server  nfs-common  ssh
bluetooth  cron         grub      keyboard   nss         tmpfs
root@debproxy:/etc/default# nano isc-dhcp-server _
```

6. Buscamos hasta al final la opción INTERFACES="" (en las comillas colocamos la tarjeta por la que dará dhcp)



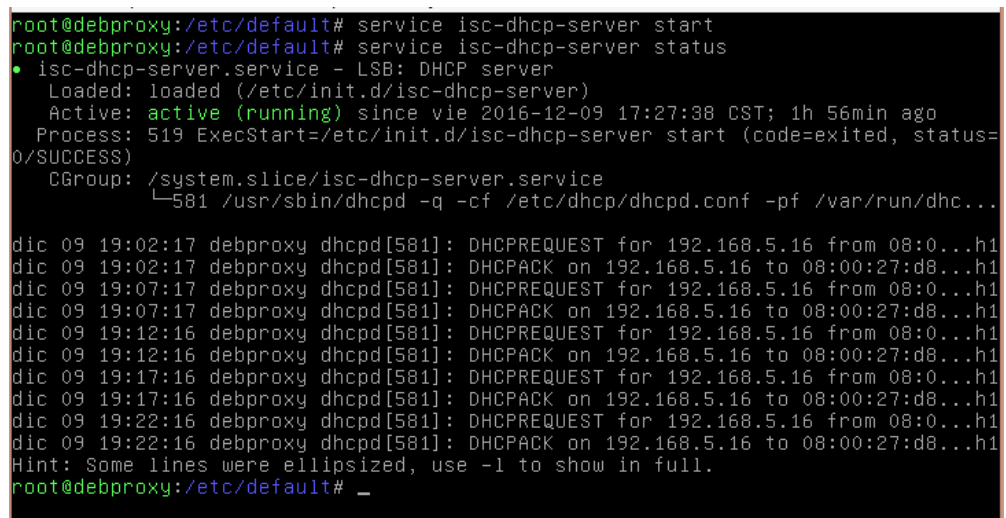
```
debian_ip [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
GNU nano 2.2.6  Fichero: isc-dhcp-server

# Path to dhcpd's PID file (default: /var/run/dhcpd.pid).
#DHCPD_PID=/var/run/dhcpd.pid

# Additional options to start dhcpd with.
# Don't use options -cf or -pf here; use DHCPD_CONF/ DHCPD_PID instead
#OPTIONS=""

# On what interfaces should the DHCP server (dhcpd) serve DHCP requests?
# Separate multiple interfaces with spaces, e.g. "eth0 eth1".
INTERFACES="eth1"
```

7. Con esto ahora levantamos nuestro servicio dhcp con el comando `service isc-dhcp-server start`



```
root@debproxy:/etc/default# service isc-dhcp-server start
root@debproxy:/etc/default# service isc-dhcp-server status
• isc-dhcp-server.service - LSB: DHCP server
   Loaded: loaded (/etc/init.d/isc-dhcp-server)
   Active: active (running) since vie 2016-12-09 17:27:38 CST; 1h 56min ago
   Process: 519 ExecStart=/etc/init.d/isc-dhcp-server start (code=exited, status=0/SUCCESS)
   CGroup: /system.slice/isc-dhcp-server.service
           └─581 /usr/sbin/dhcpd -q -cf /etc/dhcp/dhcpd.conf -pf /var/run/dhc...

dic 09 19:02:17 debproxy dhcpd[581]: DHCPREQUEST for 192.168.5.16 from 08:0...h1
dic 09 19:02:17 debproxy dhcpd[581]: DHCPACK on 192.168.5.16 to 08:00:27:d8...h1
dic 09 19:07:17 debproxy dhcpd[581]: DHCPREQUEST for 192.168.5.16 from 08:0...h1
dic 09 19:07:17 debproxy dhcpd[581]: DHCPACK on 192.168.5.16 to 08:00:27:d8...h1
dic 09 19:12:16 debproxy dhcpd[581]: DHCPREQUEST for 192.168.5.16 from 08:0...h1
dic 09 19:12:16 debproxy dhcpd[581]: DHCPACK on 192.168.5.16 to 08:00:27:d8...h1
dic 09 19:17:16 debproxy dhcpd[581]: DHCPREQUEST for 192.168.5.16 from 08:0...h1
dic 09 19:17:16 debproxy dhcpd[581]: DHCPACK on 192.168.5.16 to 08:00:27:d8...h1
dic 09 19:22:16 debproxy dhcpd[581]: DHCPREQUEST for 192.168.5.16 from 08:0...h1
dic 09 19:22:16 debproxy dhcpd[581]: DHCPACK on 192.168.5.16 to 08:00:27:d8...h1
Hint: Some lines were ellipsized, use -l to show in full.
root@debproxy:/etc/default# _
```

8. También podemos iniciar parar o reiniciar los servicios, parar o ver en qué estado está por el comando:  
`/etc/init.d/isc-dhcp-server start`

```
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
root@debproxy:/etc/default# /etc/init
init/          init.d/          initramfs-tools/
root@debproxy:/etc/default# /etc/init.d/isc-dhcp-server start
[ ok ] Starting isc-dhcp-server (via systemctl): isc-dhcp-server.service.
root@debproxy:/etc/default# /etc/init.d/isc-dhcp-server status
• isc-dhcp-server.service - LSB: DHCP server
   Loaded: loaded (/etc/init.d/isc-dhcp-server)
   Active: active (running) since vie 2016-12-09 17:27:38 CST; 1h 59min ago
   Process: 519 ExecStart=/etc/init.d/isc-dhcp-server start (code=exited, status=0/SUCCESS)
   CGroup: /system.slice/isc-dhcp-server.service
           └─581 /usr/sbin/dhcpd -q -cf /etc/dhcp/dhcpd.conf -pf /var/run/dhc...
dic 09 19:02:17 debproxy dhcpd[581]: DHCPREQUEST for 192.168.5.16 from 08:0...h1
dic 09 19:02:17 debproxy dhcpd[581]: DHCPACK on 192.168.5.16 to 08:00:27:d8...h1
dic 09 19:07:17 debproxy dhcpd[581]: DHCPREQUEST for 192.168.5.16 from 08:0...h1
dic 09 19:07:17 debproxy dhcpd[581]: DHCPACK on 192.168.5.16 to 08:00:27:d8...h1
dic 09 19:12:16 debproxy dhcpd[581]: DHCPREQUEST for 192.168.5.16 from 08:0...h1
dic 09 19:12:16 debproxy dhcpd[581]: DHCPACK on 192.168.5.16 to 08:00:27:d8...h1
dic 09 19:17:16 debproxy dhcpd[581]: DHCPREQUEST for 192.168.5.16 from 08:0...h1
dic 09 19:17:16 debproxy dhcpd[581]: DHCPACK on 192.168.5.16 to 08:00:27:d8...h1
dic 09 19:22:16 debproxy dhcpd[581]: DHCPREQUEST for 192.168.5.16 from 08:0...h1
dic 09 19:22:16 debproxy dhcpd[581]: DHCPACK on 192.168.5.16 to 08:00:27:d8...h1
Hint: Some lines were ellipsized, use -l to show in full.
root@debproxy:/etc/default# _
```

9. Ahora que tenemos nuestro servicio dhcp probaremos con una pc (cliente) que detecte el dhcp de la red interna

```
C:\Windows\system32\cmd.exe
C:\Users\clientew7>ipconfig

Configuración IP de Windows

Adaptador de Ethernet Conexión de área local 2:

    Sufijo DNS específico para la conexión. . . : sitelocal.com
    Vínculo: dirección IPv6 local. . . : fe80::18b:89f3:deae:16b%14
    Dirección IPv4. . . . . : 192.168.5.16
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada . . . . . : 192.168.5.254

Adaptador de túnel isatap.sitelocal.com:

    Estado de los medios. . . . . : medios desconectados
    Sufijo DNS específico para la conexión. . : sitelocal.com

Adaptador de túnel Conexión de área local* 2:

    Estado de los medios. . . . . : medios desconectados
    Sufijo DNS específico para la conexión. . :

C:\Users\clientew7>_
```

Al terminar la configuración manual de dhcp y se tenga ya instalado webmin, para mayor entendimiento y manejo de los servicios webmin le da la opción de configurarlo tal y como se guio por comando.

← → 192.168.5.254:10000

Login: root

Configuración de Módulo

## Servidor DHCP

DHCPd versión 4.3.1 de ISC

### Subredes y Redes Compartidas.

Seleccionar todo | Invertir selección | Añadir una nueva subred | Añadir una nueva red compartida

192.168.5.0

Seleccionar todo | Invertir selección | Añadir una nueva subred | Añadir una nueva red compartida

[Delete Selected](#)

### Máquinas y Grupos de Máquinas

No se han definido máquinas o grupos.  
 Añadir una nueva máquina | Añadir un nuevo grupo de máquinas

### DNS Zones

No DNS zones have been defined yet.  
 Add a new DNS zone.

[Editar Opciones de Cliente](#) Editar opciones de cliente DHCP que se aplican a todas las subredes, redes compartidas, máquinas y grupos.

[Edit TSIG-keys](#) Edit TSIG-keys (used for authenticating updates to DNS servers)

[Manually Edit Configuration](#) Edit configuration file manually text

[Edit Network Interface](#) Set the network interfaces that the DHCP server listens on when started.

[Listar Arrendamientos Activos](#) Lista arrendamientos ahora suministrados por este servidor DHCP para las direcciones IP asignadas dinámicamente.

[Aplicar Cambios](#) Haz click en este botón para aplicar la configuración actual al servidor DHCP en ejecución mediante su parada y reanque.

[Stop Server](#) Click this button to stop the running DHCP server on your system. When stopped, DHCP clients will not be able to request IP.

Login: root

Índice de Módulo

## Editar Subred

### Detalles de Subred

**Subnet description** A slightly different configuration for an internal subnet.

**Dirección de Red** 192.168.5.0 **Máscara de Red** 255.255.255.0

**Rangos de direcciones** 192.168.5.10 - 192.168.5.30 ☐ ¿BOOTP dinámico? ☐ ¿BOOTP dinámico?

Red compartida ☐ Ninguno ☐ Este servidor

Nombre de archivo de Boot

Servidor de archivo de Boot

Medida de arrendamiento para clientes BOOTP ☐ Si ☐ No ☐ Por defecto  segs

¿DNS dinámico activado? ☐ Por defecto ☐ Nunca

Dominio inverso de DNS dinámico ☐ Por defecto ☐ Del cliente

Allow unknown clients? ☐ Allow ☐ Deny ☐ Ignore ☐ Por defecto

Can clients update their own records? ☐ Allow ☐ Deny ☐ Ignore ☐ Por defecto

Server is authoritative for this subnet? ☐ Si ☐ No

Máquinas directamente en esta Subred

Grupos directamente en esta Subred

[Salvar](#) [Editar Opciones de Cliente](#) [List Leases](#)

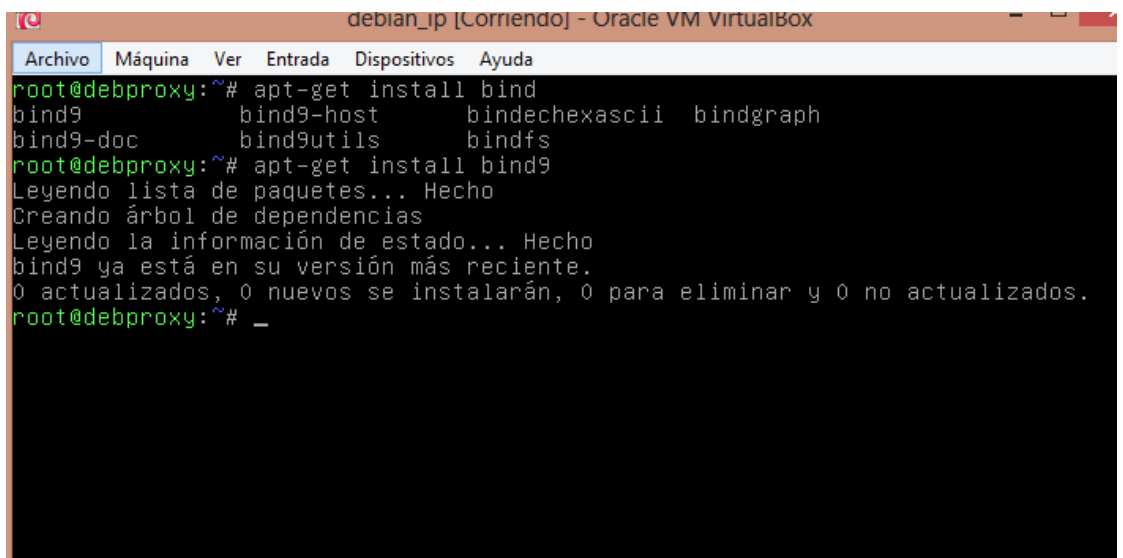
Añadir una nueva máquina Añadir un nuevo grupo de máquinas

### Paquetes de direcciones para Subred

### 3.1.4.3 guía de Configuración de DNS

1. Después de haber instalado el servicio dhcp nos vamos a la configuración de DNS empezando en instalar el servicio con el comando:

Apt-get install bind9

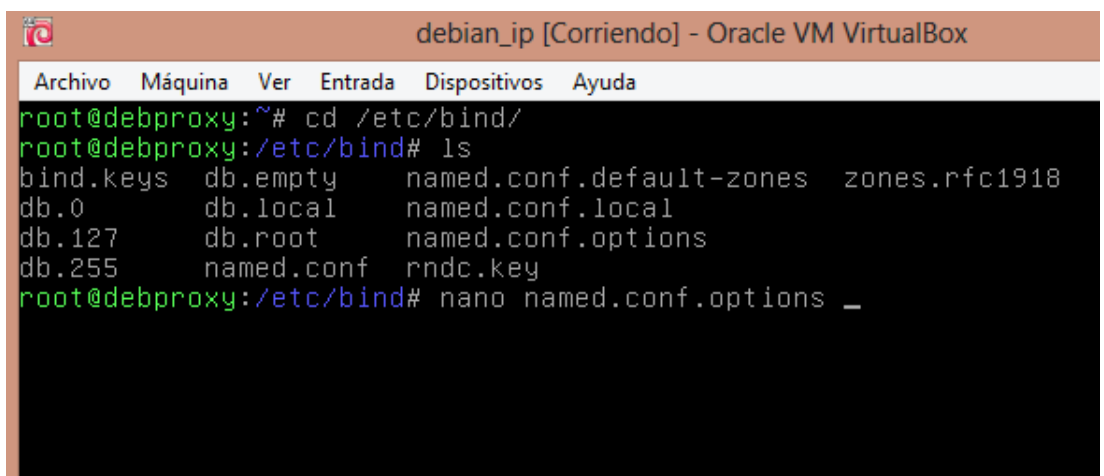


```
debian_ip [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
root@debproxy:~# apt-get install bind
bind9          bind9-host    bindehexascii bindgraph
bind9-doc      bind9utils    bindfs
root@debproxy:~# apt-get install bind9
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
bind9 ya está en su versión más reciente.
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 0 no actualizados.
root@debproxy:~# _
```

2. Como siguiente paso editaremos un archivo (resolv.conf) el cual editaremos para colocar la loopbak con los comandos:

Cd /etc/bind/ (entramos a la carpeta del servicio)

Ls (verificamos que tenemos en la carpeta y buscamos l archivo  
named.conf.options



```
debian_ip [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
root@debproxy:~# cd /etc/bind/
root@debproxy:/etc/bind# ls
bind.keys  db.empty    named.conf.default-zones  zones.rfc1918
db.0       db.local    named.conf.local
db.127     db.root     named.conf.options
db.255     named.conf  rndc.key
root@debproxy:/etc/bind# nano named.conf.options _
```

3. Luego en el archivo pasamos a agregar lo que es los dns el loopback la dirección de salida a nuestro router, google nuestro DNS.

```
options {
    directory "/var/cache/bind";

    // If there is a firewall between you and nameservers you want
    // to talk to, you may need to fix the firewall to allow multiple
    // ports to talk.  See http://www.kb.cert.org/vuls/id/800113

    // If your ISP provided one or more IP addresses for stable
    // nameservers, you probably want to use them as forwarders.
    // Uncomment the following block, and insert the addresses replacing
    // the all-0's placeholder.

    forwarders {
        127.0.0.1;
        192.168.1.1;
        8.8.8.8;
        192.168.5.1;
        179.51.50.200;
    };
};
```

Ver ayuda Guardar Leer Fich Pág Ant CortarTxt Pos actu

4. Entramos a dhcpd.conf y configuramos agregando su dns su gateway y sus rango de ip que colocaremos.

Al terminar guardamos dando (control+O) kueo enter y luego (control+X)

```
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
GNU nano 2.2.6  Fichero: dhcpd.conf  Modificado

option broadcast-address 10.254.239.31;
option routers rtr-239-32-1.example.org;
}

A slightly different configuration for an internal subnet.
subnet 192.168.2.0 netmask 255.255.255.0 {
    range 10.5.5.26 10.5.5.30;
    option domain-name-servers 192.168.2.1;
    option domain-name "debacl.net";
    option routers 192.168.2.1;
    option broadcast-address 192.168.2.255;
    default-lease-time 600;
    max-lease-time 7200;
}

Hosts which require special configuration options can be listed in
host statements.  If no address is specified, the address will be
allocated dynamically (if possible), but the host-specific information
will still come from the host declaration.
```

5. Luego de esta basica configuracion completamos ahora iniciando nuestro servicio DNS.

Comando para iniciar servicio DNS es: `service Bind9 start` Y de igual anera se puede monitoriar su estado con el comano: `service bind9 status`

```
root@debproxy:/etc/bind# service bind9 start
root@debproxy:/etc/bind# service bind9 status
• bind9.service - BIND Domain Name Server
   Loaded: loaded (/lib/systemd/system/bind9.service; enabled)
   Drop-In: /run/systemd/generator/bind9.service.d
            └─50-insserv.conf-$named.conf
   Active: active (running) since vie 2016-12-09 17:27:35 CST; 2h 35min ago
     Docs: man:named(8)
  Main PID: 514 (named)
    CGroup: /system.slice/bind9.service
            └─514 /usr/sbin/named -f -u bind

dic 09 20:01:49 debproxy named[514]: error (unexpected RCODE REFUSED) resol...53
dic 09 20:01:49 debproxy named[514]: error (unexpected RCODE REFUSED) resol...53
dic 09 20:01:57 debproxy named[514]: validating @0x7fd45c724230: com SOA: g...re
dic 09 20:01:57 debproxy named[514]: error (no valid RRSIG) resolving 'goog...53
dic 09 20:01:57 debproxy named[514]: validating @0x7fd45c724230: com SOA: v...un
dic 09 20:01:57 debproxy named[514]: validating @0x7fd45c724230: com SOA: n...nd
dic 09 20:01:58 debproxy named[514]: validating @0x7fd45c724230: com SOA: v...un
dic 09 20:01:58 debproxy named[514]: validating @0x7fd45c724230: com SOA: n...nd
dic 09 20:02:16 debproxy named[514]: error (unexpected RCODE REFUSED) resol...53
dic 09 20:02:17 debproxy named[514]: error (unexpected RCODE REFUSED) resol...53
Hint: Some lines were ellipsized, use -l to show in full.
root@debproxy:/etc/bind# _
```

6. Tambien para iniciar, parar o reiniciar sel servicio se puede hacer con el comando `/etc/init.d/bind9 start`

```
root@debproxy:~# /etc/init.d/bind9 start
[ ok ] Starting bind9 (via systemctl): bind9.service.
root@debproxy:~# /etc/init.d/bind9 status
• bind9.service - BIND Domain Name Server
   Loaded: loaded (/lib/systemd/system/bind9.service; enabled)
   Drop-In: /run/systemd/generator/bind9.service.d
            └─50-insserv.conf-$named.conf
   Active: active (running) since vie 2016-12-09 17:27:35 CST; 2h 38min ago
     Docs: man:named(8)
  Main PID: 514 (named)
    CGroup: /system.slice/bind9.service
            └─514 /usr/sbin/named -f -u bind

dic 09 20:05:00 debproxy named[514]: error (unexpected RCODE REFUSED) resol...53
dic 09 20:05:45 debproxy named[514]: validating @0x7fd45c7235a0: com SOA: g...re
dic 09 20:05:45 debproxy named[514]: error (no valid RRSIG) resolving 'micr...53
dic 09 20:05:45 debproxy named[514]: validating @0x7fd45c7235a0: com SOA: v...un
dic 09 20:05:45 debproxy named[514]: validating @0x7fd45c7235a0: com SOA: n...nd
dic 09 20:05:45 debproxy named[514]: validating @0x7fd45c7235a0: TCQ1V6SM7S...un
dic 09 20:05:45 debproxy named[514]: validating @0x7fd45c7235a0: TCQ1V6SM7S...nd
dic 09 20:05:45 debproxy named[514]: error (no valid RRSIG) resolving 'micr...53
dic 09 20:05:45 debproxy named[514]: error (unexpected RCODE REFUSED) resol...53
dic 09 20:05:45 debproxy named[514]: error (unexpected RCODE REFUSED) resol...53
Hint: Some lines were ellipsized, use -l to show in full.
root@debproxy:~# _
```

- Con esta configuracion terminamos la instalacion de nuestro DNS y como tambien como el servicio DHCP este se puede configurar de una manera grafica para mayor facilidad

Reenvío y Transferencias

Indice de Módulo

Login: root

Webmin

Sistema

Servidores

Filtro de Correo Procmail

Lectura de Correo de Usuarios

Servidor de DHCP

**Servidor de DNS BIND**

Servidor SSH

Squid - Servidor Proxy

Otros

Red

Cliente y Servidor NIS

Configuración de Red

Cortafuegos Linux

idmapd daemon

Monitorización de Ancho de Banda

TCP Wrappers

Hardware

Cluster

Un-used Modules

Search:

Opciones globales de reenvío y transferencia de zona

Servidores a los que reenviar consultas

| Dirección IP  | Puerto (opcional)                            |
|---------------|----------------------------------------------|
| 192.168.1.1   | <input checked="" type="radio"/> Por defecto |
| 8.8.8.8       | <input type="radio"/> Por defecto            |
| 192.168.5.1   | <input type="radio"/> Por defecto            |
| 179.51.50.200 | <input type="radio"/> Por defecto            |
| 200.12.232.4  | <input type="radio"/> Por defecto            |
| 200.12.229.1  | <input type="radio"/> Por defecto            |
|               | <input type="radio"/> Por defecto            |
|               | <input type="radio"/> Por defecto            |
|               | <input type="radio"/> Por defecto            |

Mirar directamente si no hay respuesta del remitente ☐ Si ☐ No ☒ Por defecto

Formato de transferencia de zona ☐ Uno cada vez ☐ Muchos ☒ Por defecto

Maximum concurrent incoming transfers per server ☒ Por defecto

Tiempo máximo de transferencia de zona

Máximas transferencias concurrentes de zona

Maximum concurrent outgoing zone transfers

Salvar

Regresar a lista de zonas

- Nos vamos por medio de webmin:
- Damos click en servidores
- Buscamos servidor DNS y BIND

Reenvío y Transferencias

Indice de Módulo

Login: root

Webmin

Sistema

Servidores

Filtro de Correo Procmail

Lectura de Correo de Usuarios

Servidor de DHCP

**Servidor de DNS BIND**

Servidor SSH

Squid - Servidor Proxy

Otros

Red

Cliente y Servidor NIS

Opciones globales de reenvío y transferencia de zona

Servidores a los que reenviar consultas

| Dirección IP  | Puerto (opcional)                            |
|---------------|----------------------------------------------|
| 192.168.1.1   | <input checked="" type="radio"/> Por defecto |
| 8.8.8.8       | <input type="radio"/> Por defecto            |
| 192.168.5.1   | <input type="radio"/> Por defecto            |
| 179.51.50.200 | <input type="radio"/> Por defecto            |
| 200.12.232.4  | <input type="radio"/> Por defecto            |
| 200.12.229.1  | <input type="radio"/> Por defecto            |
|               | <input type="radio"/> Por defecto            |
|               | <input type="radio"/> Por defecto            |
|               | <input type="radio"/> Por defecto            |

### 3.1.4.4 guía de configuración Webmin

1. Actualizamos la información de los repositorios (fundamental antes de instalar cualquier aplicación): `aptitude update`

```
17-14:25] jessie Release
Ign cdrom://[Debian GNU/Linux 8.6.0 _Jessie_ - Official amd64 CD Binary-1 201609
17-14:25] jessie/main amd64 Packages/DiffIndex
Ign cdrom://[Debian GNU/Linux 8.6.0 _Jessie_ - Official amd64 CD Binary-1 201609
17-14:25] jessie/main Translation-es_SV
Ign http://ftp.us.debian.org jessie InRelease
Hit http://security.debian.org jessie/updates InRelease
Hit http://ftp.us.debian.org jessie-updates InRelease
Hit http://ftp.us.debian.org jessie Release.gpg
Hit http://security.debian.org jessie/updates/main Sources
Des: 1 http://ftp.us.debian.org jessie-updates/main Sources [15.4 kB]
Hit http://security.debian.org jessie/updates/main amd64 Packages
Des: 2 http://ftp.us.debian.org jessie-updates/main amd64 Packages/DiffIndex [6,
916 B]
Hit http://security.debian.org jessie/updates/main Translation-en
Des: 3 http://ftp.us.debian.org jessie-updates/main Translation-en/DiffIndex [2,
704 B]
Hit http://ftp.us.debian.org jessie Release
Des: 4 http://ftp.us.debian.org jessie/main Sources [7,059 kB]
Hit http://ftp.us.debian.org jessie/main amd64 Packages
Hit http://ftp.us.debian.org jessie/main Translation-es
Hit http://ftp.us.debian.org jessie/main Translation-en
Descargados 7,084 kB en 20s (340 kB/s)
root@debian:~# aptitude update_
```

2. Instalamos una serie de paquetes que nos hacen falta para la instalación de Webmin y para que se configure con SSL:

`aptitude install perl libnet-ssleay-perl openssl libauthen-pam-perl libpam-runtime libio-pty-perl apt-show-versions`

```
Hit http://security.debian.org jessie/updates InRelease
Hit http://ftp.us.debian.org jessie-updates InRelease
Hit http://ftp.us.debian.org jessie Release.gpg
Hit http://security.debian.org jessie/updates/main Sources
Des: 1 http://ftp.us.debian.org jessie-updates/main Sources [15.4 kB]
Hit http://security.debian.org jessie/updates/main amd64 Packages
Des: 2 http://ftp.us.debian.org jessie-updates/main amd64 Packages/DiffIndex [6,
916 B]
Hit http://security.debian.org jessie/updates/main Translation-en
Des: 3 http://ftp.us.debian.org jessie-updates/main Translation-en/DiffIndex [2,
704 B]
Hit http://ftp.us.debian.org jessie Release
Des: 4 http://ftp.us.debian.org jessie/main Sources [7,059 kB]
Hit http://ftp.us.debian.org jessie/main amd64 Packages
Hit http://ftp.us.debian.org jessie/main Translation-es
Hit http://ftp.us.debian.org jessie/main Translation-en
Descargados 7,084 kB en 20s (340 kB/s)
root@debian:~# aptitude install perl libnet-ssleay-perl openssl libauthen-pam-pe
rl libpam-runtime libio-pty-perl apt-show-versions
No se instalará, actualizará o eliminará ningún paquete.
0 paquetes actualizados, 0 nuevos instalados, 0 para eliminar y 0 sin actualizar
.
Necesito descargar 0 B de ficheros. Después de desempaquetar se usarán 0 B.
```

3. Descargamos la última versión de Webmin (la 1.820 en este caso).

```
wget http://prdownloads.sourceforge.net/webadmin/webmin_1.820_all.deb
```

```
root@debian:~# aptitude install perl libnet-ssleay-perl openssl libauthen-pam-perl libpam-runtime libio-pty-perl apt-show-versions
No se instalará, actualizará o eliminará ningún paquete.
0 paquetes actualizados, 0 nuevos instalados, 0 para eliminar y 0 sin actualizar.
Necesito descargar 0 B de ficheros. Después de desempaquetar se usarán 0 B.

root@debian:~# wget http://prdownloads.sourceforge.net/webadmin/webmin_1.820_all.deb
--2016-12-07 00:29:29-- http://prdownloads.sourceforge.net/webadmin/webmin_1.820_all.deb
Resolviendo prdownloads.sourceforge.net (prdownloads.sourceforge.net)... 216.34.181.59
Conectando con prdownloads.sourceforge.net (prdownloads.sourceforge.net) [216.34.181.59]:80... conectado.
Petición HTTP enviada, esperando respuesta... 301 Moved Permanently
Localización: http://downloads.sourceforge.net/project/webadmin/webmin/1.820/webmin_1.820_all.deb [siguiendo]
--2016-12-07 00:29:30-- http://downloads.sourceforge.net/project/webadmin/webmin/1.820/webmin_1.820_all.deb
Resolviendo downloads.sourceforge.net (downloads.sourceforge.net)... 216.34.181.59
Conectando con downloads.sourceforge.net (downloads.sourceforge.net) [216.34.181.59]:80... =
```

4. Instalamos Webmin:

```
dpkg --install webmin_1.820_all.deb
```

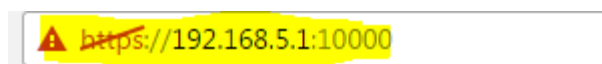
```
n/1.820/webmin_1.820_all.deb
Resolviendo downloads.sourceforge.net (downloads.sourceforge.net)... 216.34.181.59
Conectando con downloads.sourceforge.net (downloads.sourceforge.net) [216.34.181.59]:80... conectado.
Petición HTTP enviada, esperando respuesta... 302 Found
Localización: https://superb-sea2.dl.sourceforge.net/project/webadmin/webmin/1.820/webmin_1.820_all.deb [siguiendo]
--2016-12-07 00:29:30-- https://superb-sea2.dl.sourceforge.net/project/webadmin/webmin/1.820/webmin_1.820_all.deb
Resolviendo superb-sea2.dl.sourceforge.net (superb-sea2.dl.sourceforge.net)... 209.160.57.180
Conectando con superb-sea2.dl.sourceforge.net (superb-sea2.dl.sourceforge.net) [209.160.57.180]:443... conectado.
Petición HTTP enviada, esperando respuesta... 200 OK
Longitud: 15230868 (15M) [application/octet-stream]
Grabando a: "webmin_1.820_all.deb.1"

webmin_1.820_all.de 100%[=====] 14.52M 402KB/s en 38s

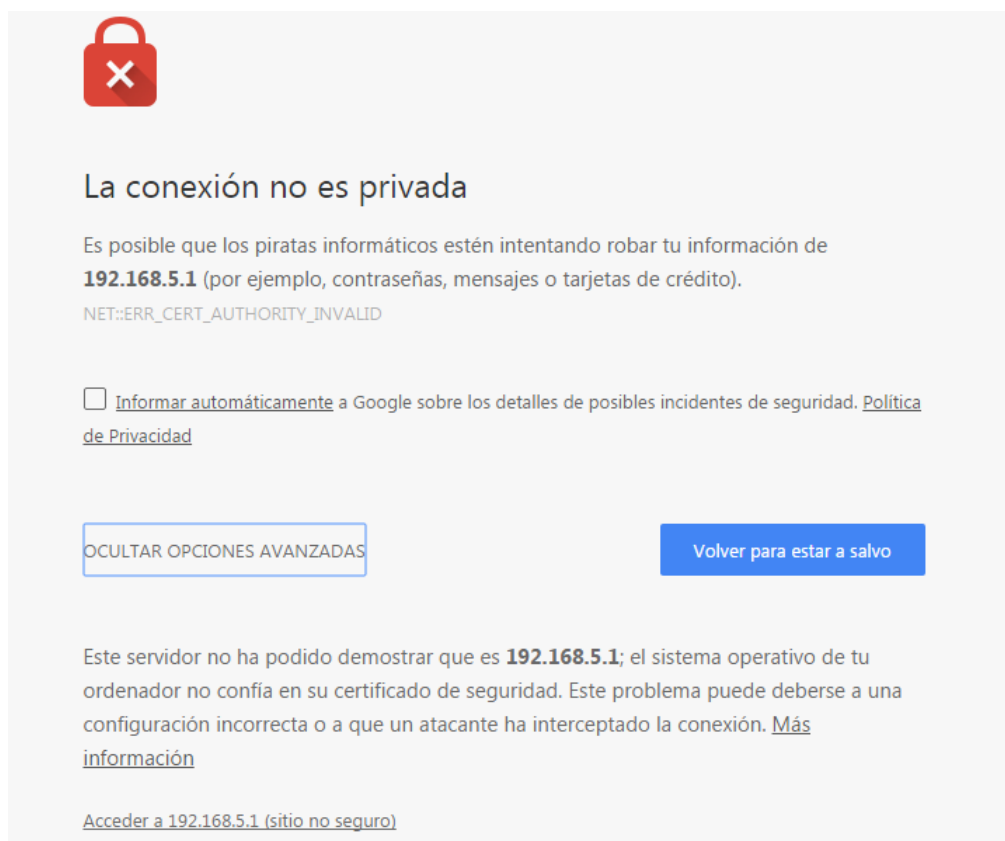
2016-12-07 00:30:09 (397 KB/s) - "webmin_1.820_all.deb.1" guardado [15230868/15230868]

root@debian:~# dpkg --install webmin_1.820_all.deb_
```

5. Una vez instalado podemos acceder a la interfaz web de Webmin usando un navegador y escribiendo la dirección IP del equipo donde está instalado seguido del puerto donde está escuchando, por defecto, el 10.000. Eso sí, debemos estar atentos porque en vez de usar el protocolo HTTP, usaremos el HTTPS. En mi caso la IP es 192.168.5.1



6. En teoría, ya está listo. Sin embargo, nos encontraremos con la siguiente advertencia si accedemos desde chrome:



Para que no nos vuelva a aparecer hacemos clic sobre “acceder a 192.168.5.1...”

- Ahora ya podemos iniciar sesión en Webmin. Como nombre de usuario podemos usar *root* (si lo tenemos habilitado) o cualquier usuario del sistema con privilegios de administrador.

---

---

**Ingreso a Webmin**  
Debe ingresar un nombre de usuario y contraseña para ingresar al servidor Webmin en 192.168.5.1.  
**Nombre de usuario**   
**Contraseña**   
☐ ¿Recordar el usuario en forma permanente?

- Y así accedemos a la interfaz de Webmin.



**System Information**  
System hostname **debian.deb.net** (127.0.1.1)  
Operating system **Debian Linux 8**  
Webmin version **1.820**  
Time on system **Wed Dec 7 00:40:35 2016**  
Kernel and CPU **Linux 3.16.0-4-amd64 on x86\_64**  
Processor information **Intel(R) Core(TM) i5-6400 CPU @ 2.70GHz, 1 cores**  
System uptime **1 hours, 37 minutes**  
Running processes **67**  
CPU load averages **0.00 (1 min) 0.01 (5 mins) 0.05 (15 mins)**  
CPU usage **0% user, 0% kernel, 0% IO, 100% idle**  
Real memory **153.96 MB used, 1.24 GB total**  
Virtual memory **0 bytes used, 383 MB total**  
Local disk space **1.52 GB used, 7.38 GB total**  
Package updates **All installed packages are up to date**

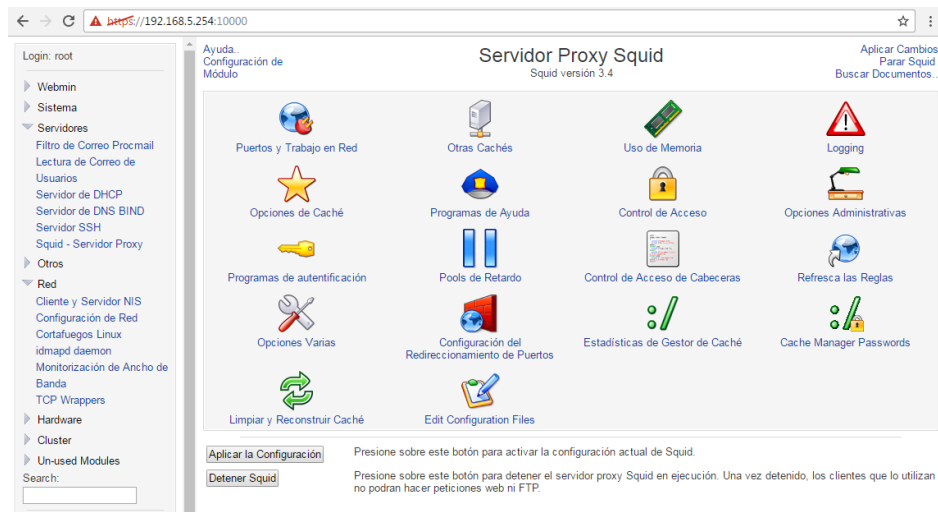
**Recent Webmin logins**

### 3.1.4.5 guía de Configuración Squid

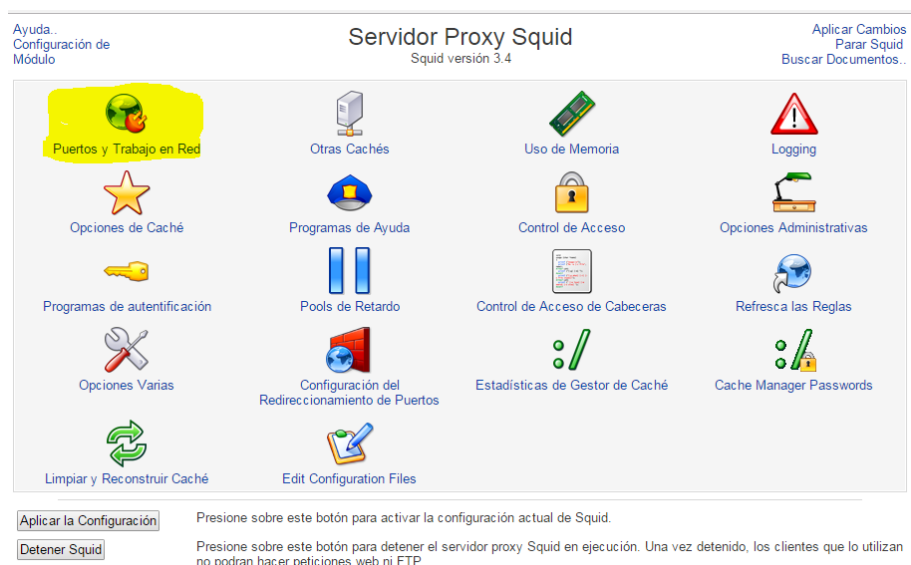
1. Podemos instalar nuestro servicio squid3 por comando o directo desde webmin:

```
root@debproxy:~# apt-get install squid3
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
squid3 ya está en su versión más reciente.
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 0 no actualizados.
root@debproxy:~#
```

Por webmin:



2. Empezaremos configurando los puerto y trabajos de red :



3. Agregaremos el número de puerto por el cual se escuchara y pondremos nuestra dirección de nuestro servidor

Índice de Módulo Ayuda.. **Puertos y Trabajo en Red** Aplicar Cambios Parar Squid

**Opciones de Puertos y Trabajo en Red**

Direcciones y puertos de Proxy ☐ Por defecto (normalmente 3128) ☒ Listados abajo..

| Puerto | Nombre de máquina/Dirección IP                                           | Opciones de puerto |
|--------|--------------------------------------------------------------------------|--------------------|
| 3128   | <input type="radio"/> All <input checked="" type="radio"/> 192.168.5.254 | transparent        |
|        | <input type="radio"/> All <input type="radio"/>                          |                    |

Direcciones y puertos SSL ☒ Por defecto (normalmente 3128) ☐ Listados abajo..

| Puerto | Nombre de máquina/Dirección IP                             | Opciones de puerto |
|--------|------------------------------------------------------------|--------------------|
|        | <input checked="" type="radio"/> All <input type="radio"/> |                    |

Puerto ICP ☒ Por defecto ☐

Dirección UDP de salida ☒ Cualquiera ☐

Dirección TCP de salida ☒ Cualquiera ☐

Dirección UDP de entrada ☒ Cualquiera ☐

Grupos de multicast

Búfer de recepción TCP ☒ el de por defecto del SO ☐

Validate hostnames in URLs? ☒ Sí ☐ No

Allow underscore in hostnames? ☒ Sí ☐ No

¿Hacer desconexiones no limpias SSL? ☐ Activado ☒ Desactivado

Salvar

4. Luego nos vamos a opciones de cache:

Ayuda.. Configuración de Módulo **Servidor Proxy Squid** Squid versión 3.4 Aplicar Cambios Parar Squid Buscar Documentos..



Puertos y Trabajo en Red



Opciones de Caché



Programas de autenticación



Opciones Varias



Limpiar y Reconstruir Caché



Otras Cachés



Programas de Ayuda



Pools de Retardo



Configuración del Redireccionamiento de Puertos



Edit Configuration Files



Uso de Memoria



Control de Acceso



Control de Acceso de Cabeceras



Estadísticas de Gestor de Caché



Logging



Opciones Administrativas



Refresca las Reglas



Cache Manager Passwords

5. Colocamos en directorios de cache tachamos la poción por relación agregando en directorio: /var/spool/squid3 con tamaño 100 directorios de primer nivel a 16 y el segundo nivel a 256 aplicamos cambios.

Indice de Módulo Aplicar Cambios  
Ayuda.. Parar Squid

### Opciones de Caché

Opciones de Caché y de Petición

Directorios de Caché ☐ Por defecto (/var/spool/squid3) ☒ Relación...

| Directorio        | Tipo | Tamaño (MB) | Directorios de Primer nivel | Directorios de Segundo nivel | Opciones |
|-------------------|------|-------------|-----------------------------|------------------------------|----------|
| /var/spool/squid3 | UFS  | 100         | 16                          | 256                          |          |
|                   | UFS  |             |                             |                              |          |

Tamaño medio de objeto ☒ Por defecto  kBs

No hacer caché de ☐ all ☐ SSL\_ports ☐ Safe\_ports ☐ CONNECT  
URLs para las ACLs ☐ all

Máximo tamaño de cuerpo de petición ☒ Por defecto  kBs

Máximo salto de lectura hacia delante (read-ahead) ☒ Por defecto  kBs

Objetos por cubo ☒ Por defecto

Tiempo máximo de caché ☒ Por defecto  segundos

Máximo tamaño de cabeceras de petición ☒ Por defecto  kBs

Falló la petición de tiempo de caché ☒ Por defecto  segundos

6. Nos dirigimos a controles de acceso:

Ayuda.. Aplicar Cambios  
Configuración de Módulo Parar Squid  
Módulo Buscar Documentos...

### Servidor Proxy Squid

Squid versión 3.4



Puertos y Trabajo en Red



Otras Cachés



Uso de Memoria



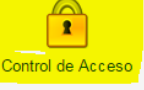
Logging



Opciones de Caché



Programas de Ayuda



Control de Acceso



Opciones Administrativas



Programas de autenticación



Pools de Retardo



Control de Acceso de Cabeceras



Refresca las Reglas



Opciones Varias



Configuración del Redireccionamiento de Puertos



Estadísticas de Gestor de Caché



Cache Manager Passwords



Limpiar y Reconstruir Caché



Edit Configuration Files

7. En este paso agregamos una acl que de la direccion del cliente con la red que creamos este permitir

Indice de Módulo Ayuda... Control de Acceso Aplicar Cambios Parar Squid

Listas de control de Acceso Restricciones Proxy Restricciones ICP Programas externos ACL Reply proxy restrictions

| Nombre     | Tipo                 | Coincidiendo con... |
|------------|----------------------|---------------------|
| SSL_ports  | Puerto URL           | 443                 |
| Safe_ports | Puerto URL           | 80                  |
| Safe_ports | Puerto URL           | 21                  |
| Safe_ports | Puerto URL           | 443                 |
| Safe_ports | Puerto URL           | 70                  |
| Safe_ports | Puerto URL           | 210                 |
| Safe_ports | Puerto URL           | 1025-65535          |
| Safe_ports | Puerto URL           | 280                 |
| Safe_ports | Puerto URL           | 488                 |
| Safe_ports | Puerto URL           | 591                 |
| Safe_ports | Puerto URL           | 777                 |
| CONNECT    | Método de Petición   | CONNECT             |
| all        | Dirección de Cliente | 192.168.5.0         |

Crear nueva ACL Autenticación Externa

Regresar a índice squid

8. Nos vamos a restricción de proxy y le damos permitir a nuestro cliente todo

Indice de Módulo Ayuda... Control de Acceso Aplicar Cambios Parar Squid

Listas de control de Acceso Restricciones Proxy Restricciones ICP Programas externos ACL Reply proxy restrictions

Añadir restricción proxy

| Acción                            | ACLs               | Mover |
|-----------------------------------|--------------------|-------|
| <input type="checkbox"/> Denegar  | ISafe_ports        | ↓     |
| <input type="checkbox"/> Denegar  | CONNECT !SSL_ports | ↓↑    |
| <input type="checkbox"/> Permitir | localhost manager  | ↓↑    |
| <input type="checkbox"/> Denegar  | manager            | ↓↑    |
| <input type="checkbox"/> Permitir | localhost          | ↓↑    |
| <input type="checkbox"/> Permitir | all                | ↑     |

Añadir restricción proxy

Delete Selected Restrictions

9. Creado esto nos daría ya conexión a internet:

Webmin 1.801 en debpr... informatica - Buscar con...

https://www.google.com/sv/webhp?sourceid=chrome-instant&ion=1&espv=2&ie=UTF-8#q=informatica

Google informatica

Todo Imágenes Maps Vídeos Noticias Más Preferencias Herramientas

Cerca de 122,000,000 resultados (0.50 segundos)

Se define como la rama de la tecnología que estudia el tratamiento automático de la información. En 1957 Karl Steinbuch añadió la palabra alemana Informatik en la publicación de un documento denominado Informatik: Automatische Informationsverarbeitung (Informática: procesamiento automático de información).

Informática - Wikipedia, la enciclopedia libre  
https://es.wikipedia.org/wiki/Informática

Acerca de este resultado • Comentarios

Informática - Wikipedia, la enciclopedia libre  
https://es.wikipedia.org/wiki/Informática

La informática, también llamada computación en América latina, es una ciencia que estudia métodos, técnicas, procesos, con el fin de almacenar, procesar y ...

Electrónica digital · Portal:Informática · Proceso · Informática

Definición de Informática - Qué es, Significado y Concepto  
definicion.de/Informatica/

De esta forma, la informática se refiere al procesamiento automático de información mediante

### 3.1.4.6 guía de Configuración Iptable

1. Como primer paso se verifica si nuestro servicio iptables se encuentra instalado (normalmente lo trae ya instalado)

```
root@debproxy:~# apt-get install iptables
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
iptables ya está en su versión más reciente.
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 0 no actualizados.
root@debproxy:~# _
```

2. Empezamos con la regla la cual nos permitirá que desde (eth1) podamos tener salida hacia el internet con el comando:

Iptables -t nat -A POSTROUTING -s 192.168.5.0/24 -o eth0 -j MASQUERADE

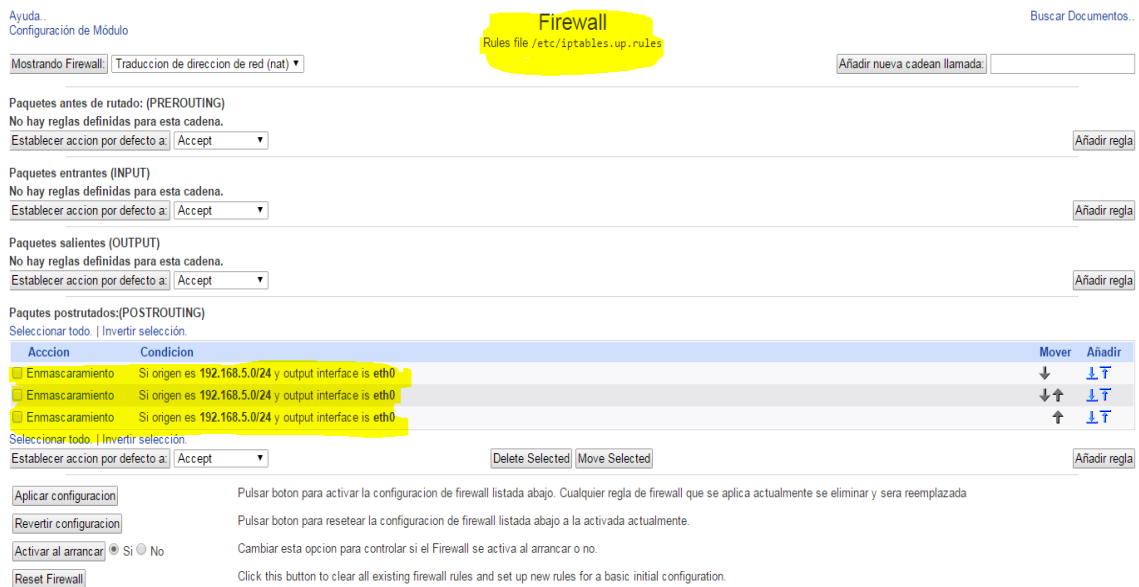
```
debian_ip [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
root@debproxy:~# iptables -t nat -A POSTROUTING -s 192.168.5.0/24 -o eth0 -j MASQUERADE
root@debproxy:~# iptables-save > /etc/iptables.up.rules
root@debproxy:~# _
```

3. luego de configurar nuestra regla para salida hacia internet tenemos que guardar cada regla que pongamos con:

Iptables-save > /etc/iptables.up.rules

```
root@debproxy:~# iptables-save > /etc/iptables.up.rules
root@debproxy:~# _
```

4. Esta regla la podemos observar en el servicio webmin que se a creado de la manera que lo indicamos:

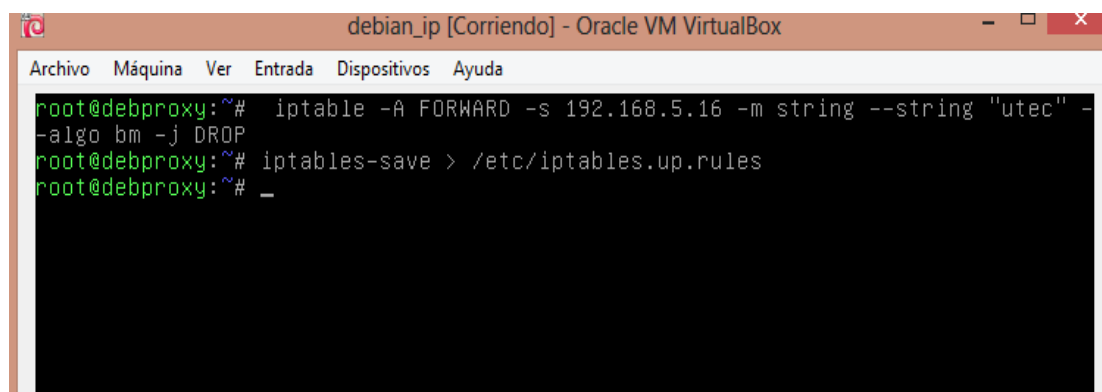


(Esta regla puede estar as de una vez y no nos afecta se pueden borrar pero dejando siempre una regla.)

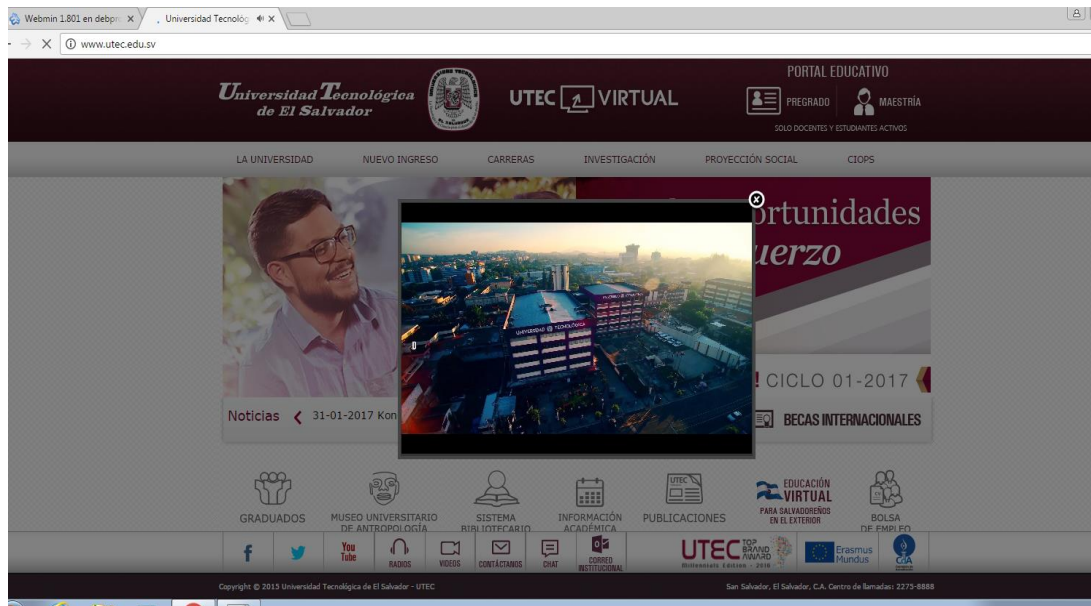
5. Después de la creación de salida hacia la red y que previamente se instaló y se configuro el servicios squid ahora se comenzara con el bloqueo de páginas web.

El comando para el bloqueo de páginas web es:

Iptables -A FORWARD -s 192.168.5.16 -m string --string "dirección a bloquear" --algo bm -j DROP

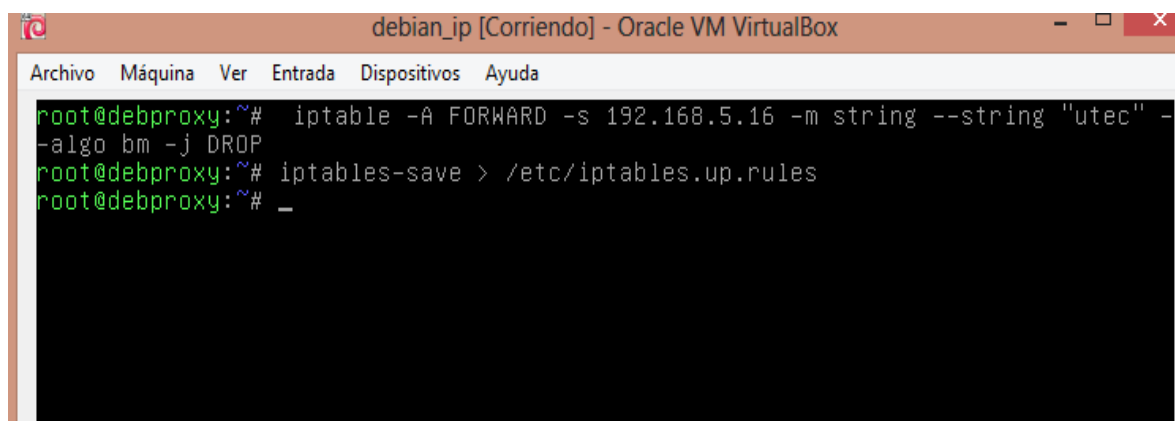


6. buscamos la página y verificamos una palabra clave para que la regla al aplicarla todo dominio que posea dicha palabra bloquee el acceso en este caso tomaremos “UTEC”

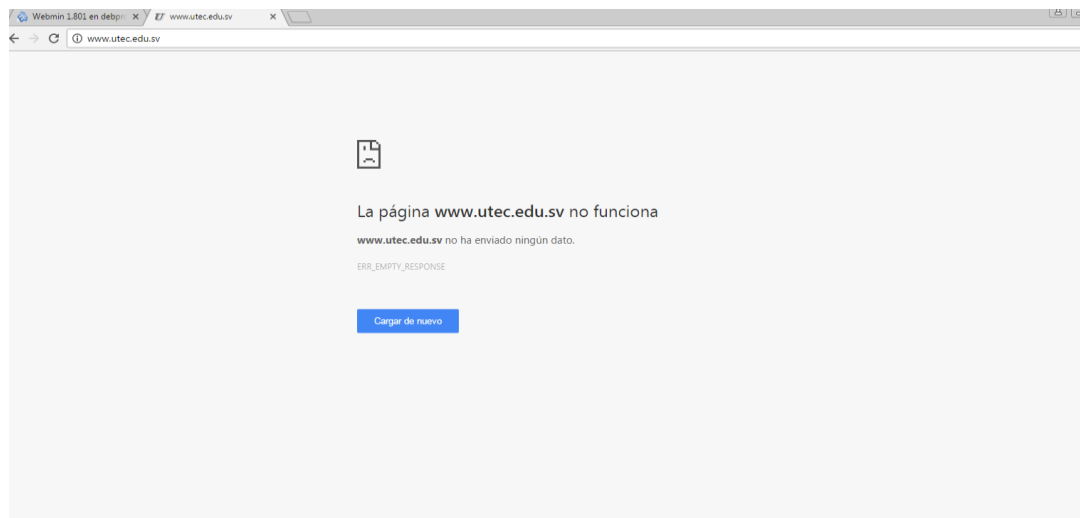


“vemos que tenemos acceso antes de crear nuestro bloqueo”

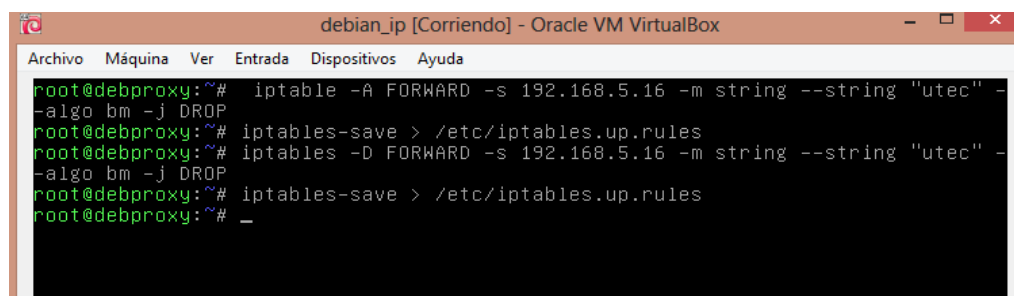
7. ahora procedemos a agregar nuestra regla y guardarla:



8. Ahora vamos a nuestro cliente y verificamos que al guardar nuestra regla nos bloquea al momento la página:



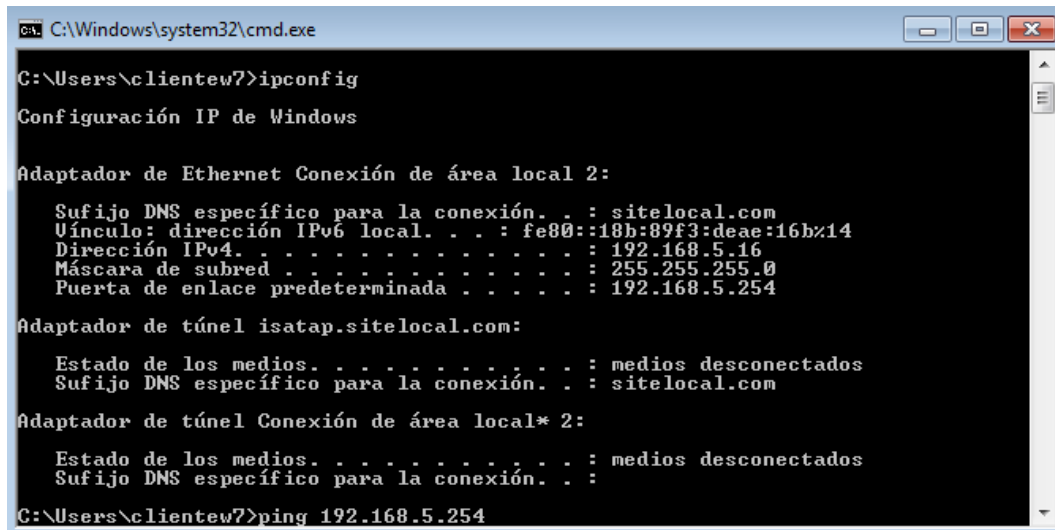
9. Para poder habilitar el acceso a la página nuevamente ejecutamos el mismo comando solamente cambiando un parámetro de `-A` a `-D` para borrarla



Ahora tendremos acceso a la página bloqueada desde el cliente:



10. Bloqueo de ICMP hacia el servidor, en el siguiente paso es una regla as utilizada para la protección de los servidores es muy importante a que maquina se tiene acceso a respuesta del servidor en icmp ya que es una muy fuerte vulnerabilidad



```
C:\Windows\system32\cmd.exe

C:\Users\clientew7>ipconfig

Configuración IP de Windows

Adaptador de Ethernet Conexión de área local 2:

    Sufijo DNS específico para la conexión. . . : sitelocal.com
    Vínculo: dirección IPv6 local. . . : fe80::18b:89f3:deae:16b%14
    Dirección IPv4. . . . . : 192.168.5.16
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada . . . . . : 192.168.5.254

Adaptador de túnel isatap.sitelocal.com:

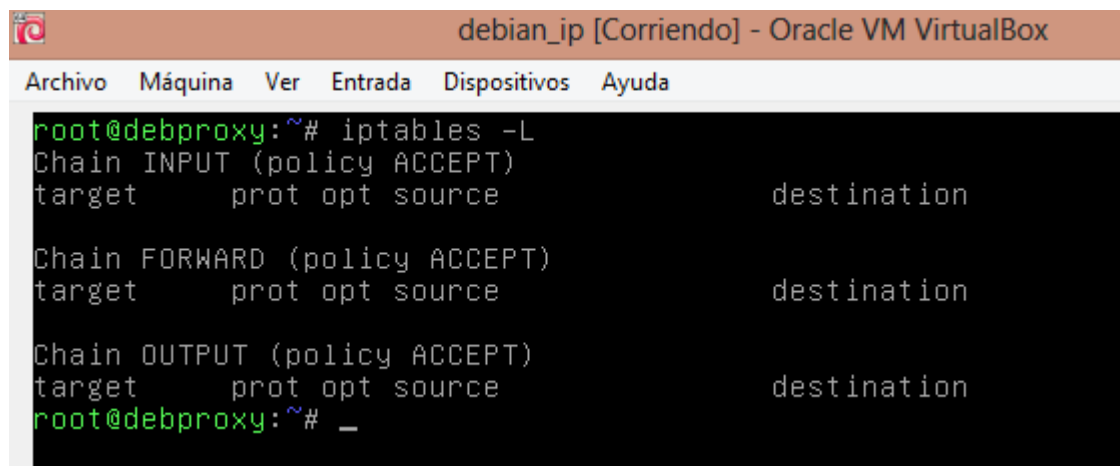
    Estado de los medios. . . . . : medios desconectados
    Sufijo DNS específico para la conexión. . : sitelocal.com

Adaptador de túnel Conexión de área local* 2:

    Estado de los medios. . . . . : medios desconectados
    Sufijo DNS específico para la conexión. . :

C:\Users\clientew7>ping 192.168.5.254
```

11. Empezaremos utilizando el comando iptable -L para listarnos si tenemos alguna creada:



```
debian_ip [Corriendo] - Oracle VM VirtualBox

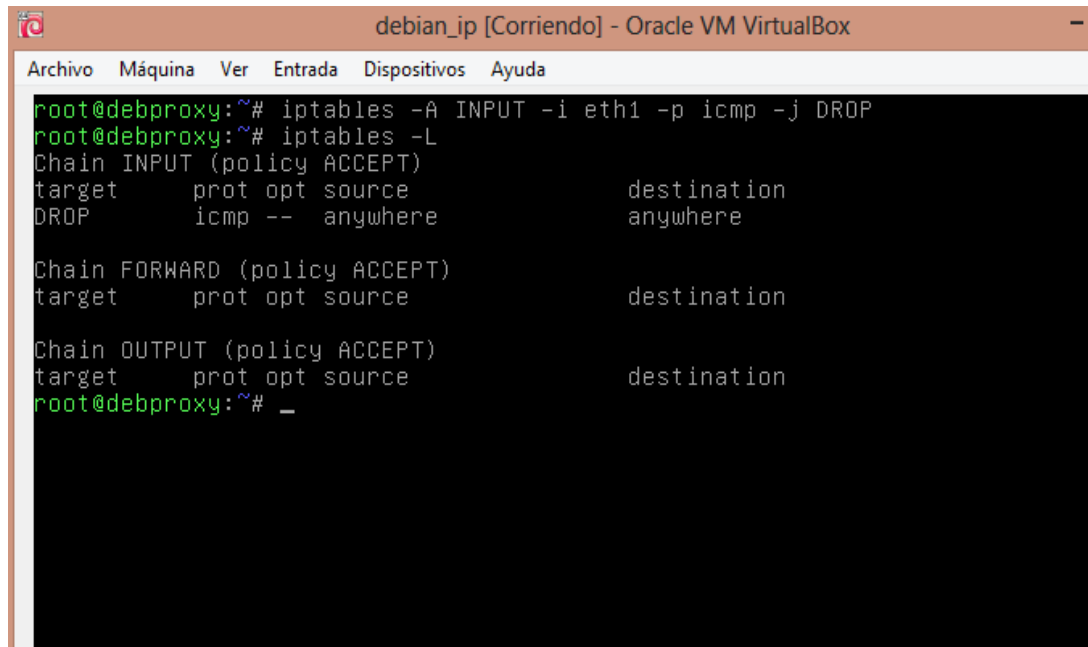
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda

root@debproxy:~# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
root@debproxy:~# _
```

12. Ahora que verificamos si había una regla ya creada empezaremos creándola con el comando: `iptables -A INPUT -i eth1 -p icmp -j DROP`



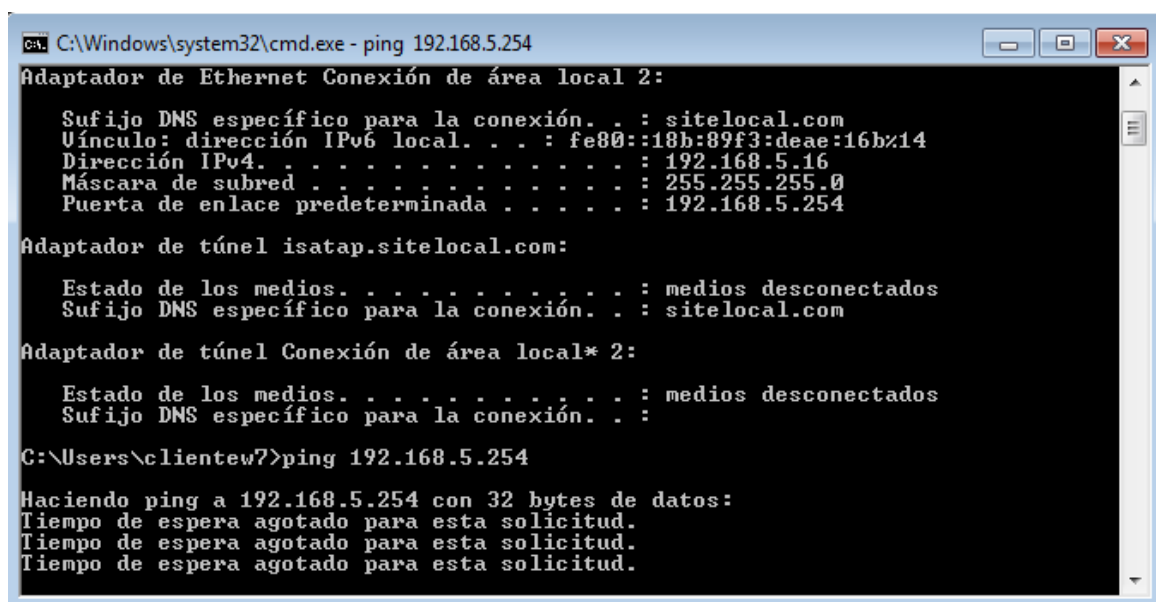
```
debian_ip [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
root@debproxy:~# iptables -A INPUT -i eth1 -p icmp -j DROP
root@debproxy:~# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination
DROP       icmp -- anywhere             anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
root@debproxy:~# _
```

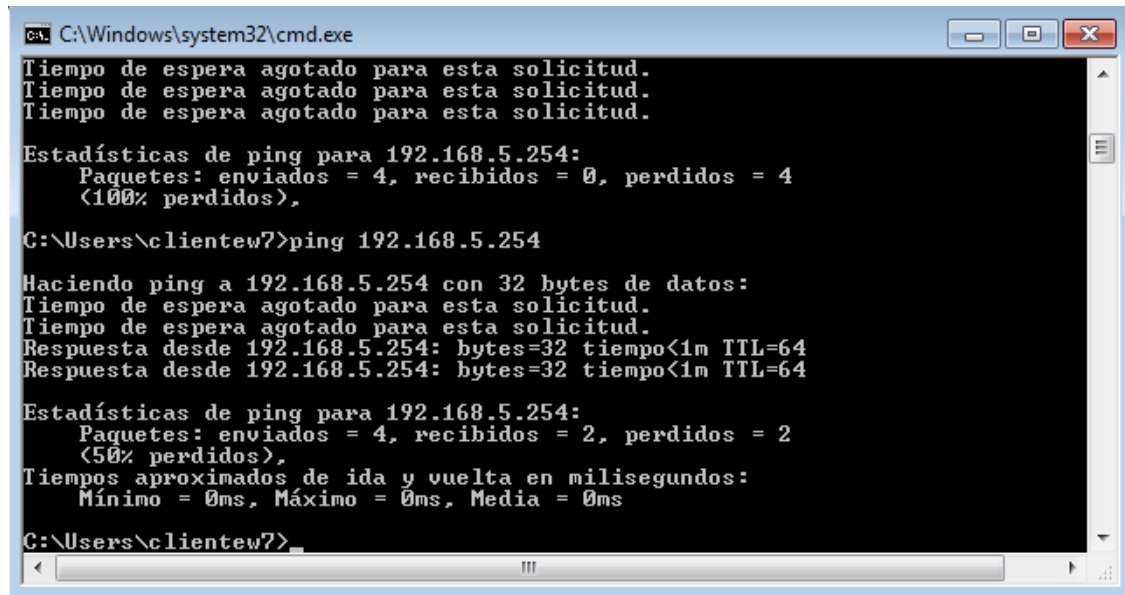
“Esto quiere decir que a iptable le vamos a añadir a eth1 una regla de no permitir los paquetes de ICMP (ping)”

13. nos vamos a nuestro cliente y damos un pin al servidor y no nos tiene que dar respuesta



```
C:\Windows\system32\cmd.exe - ping 192.168.5.254
Adaptador de Ethernet Conexión de área local 2:
    Sufijo DNS específico para la conexión. . . : sitelocal.com
    Vínculo: dirección IPv6 local. . . : fe80::18b:89f3:deae:16b%14
    Dirección IPv4. . . . . : 192.168.5.16
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada . . . . . : 192.168.5.254
Adaptador de túnel isatap.sitelocal.com:
    Estado de los medios. . . . . : medios desconectados
    Sufijo DNS específico para la conexión. . : sitelocal.com
Adaptador de túnel Conexión de área local* 2:
    Estado de los medios. . . . . : medios desconectados
    Sufijo DNS específico para la conexión. . :
C:\Users\clientew7>ping 192.168.5.254
Haciendo ping a 192.168.5.254 con 32 bytes de datos:
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
```

14. Para poder eliminar la regla y que el cliente vuelva a tener acceso a ping al servidor ejecutamos el comando: iptables -F



```
C:\Windows\system32\cmd.exe
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.

Estadísticas de ping para 192.168.5.254:
    Paquetes: enviados = 4, recibidos = 0, perdidos = 4
    (100% perdidos),

C:\Users\clientew7>ping 192.168.5.254

Haciendo ping a 192.168.5.254 con 32 bytes de datos:
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Respuesta desde 192.168.5.254: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.5.254: bytes=32 tiempo<1m TTL=64

Estadísticas de ping para 192.168.5.254:
    Paquetes: enviados = 4, recibidos = 2, perdidos = 2
    (50% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms

C:\Users\clientew7>
```

“al aplicar el comando de borrado rápidamente vuelve a tener permiso para recibir respuesta del servidor.

### 3.2 Análisis de Datos:

En los gráficos siguientes se muestran como explicación del resultado que se obtuvo mediante el método “encuesta”, según las respuestas de los alumnos encuestados.

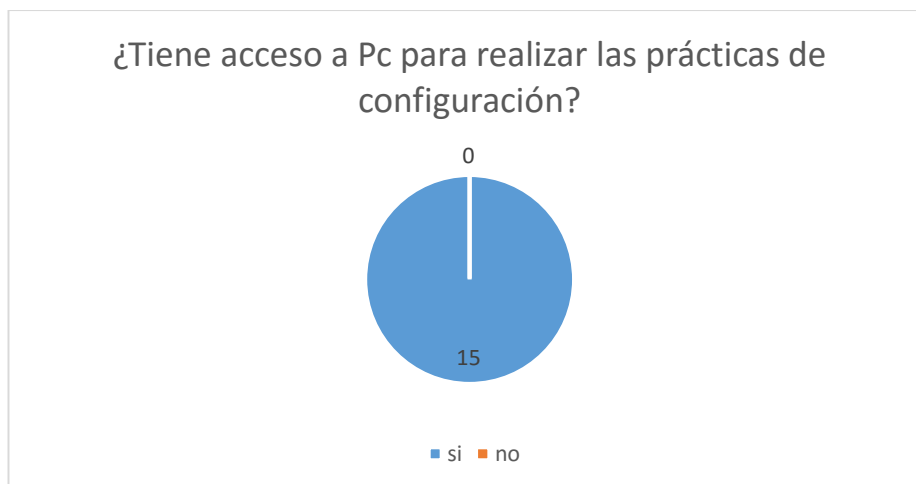
- ¿Ha trabajado usted con algún servidor?

-15 de 15 Alumnos respondieron que SI



- ¿tiene acceso a Pc para realizar las prácticas de configuración?

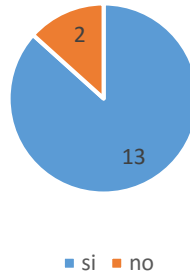
-15 de 15 Alumnos respondieron SI.



- ¿son importantes las guías de configuración de sistemas operativos para la Asignatura Administración de redes?

-13 Alumnos respondieron SI, 2 alumnos respondieron NO

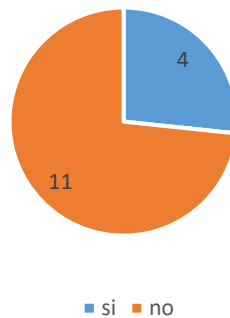
¿Son importantes las guías de Configuración de sistemas operativos para la Asignatura Administración De redes?



- ¿has utilizado la consola de la distribución debían?

-13 de 15 Alumnos respondieron SI.

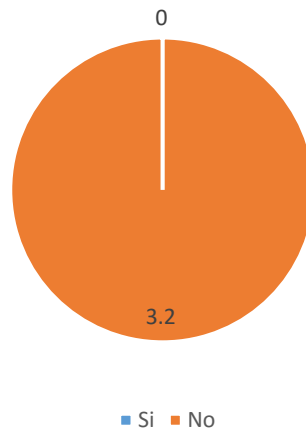
¿has utilizado la consola de la distribución Debían?



- ¿Tiene acceso a Guías de configuración de Debían?

-15 de 15 Alumnos respondieron NO.

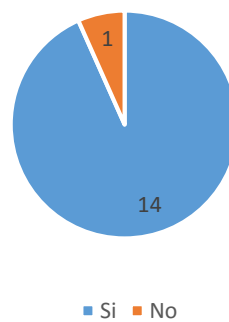
¿Tiene acceso a Guías de configuración de Debían?



- ¿utilizaría un servidor debían?

-14 de 15 Alumnos Respondieron SI.

-¿utilizaría un servidor debían?



### *3.3 Conclusiones:*

La presente tesis tuvo como objetivo mostrar la instalación, configuración, y administración de servicios básicos sobre los servicios PROXY (Squid), Iptable, DNS, y DHCP en el sistema operativo debían y aportar así una ayuda no solo para el alumno sino también para el docente, mostrado apoyo en la distribución Linux junto con Debían.

Además se utiliza un sistema operativo que es catalogado uno de los más estables de la actualidad, es un software gratuito y da la libertad para configurarlo, libertad para copiarlo, y para distribuir las modificaciones; en otras palabras el alumno no tendrá problema para utilizarlo.

Así pues la aportación principal de este trabajo consiste en dar al estudiante el material didáctico, y que sea utilizado en las instalaciones universitarias, así también en la biblioteca virtual de la universidad, extendiéndonos también a la posibilidad de que por medio del sistema de préstamo de libros de la universidad tecnológica de El Salvador el alumno pueda llevar el material para trabajarlo en casa.

Cabe resaltar que en el proceso se utilizó el servicio Webmin como una herramienta para realizar las configuraciones de forma que no se le dificulte el alumno comprenderla al utilizarla.

### 3.4 Referencias

Dueñas, J. B. (2016). *Alcance libre*. Recuperado de <http://www.alcancelibre.org/staticpages/index.php/tabla-comparativa-distros-linux>

Free Software Foundation, Inc. (2016). *El equipo del instalador de debían*. Recuperado de <https://www.debian.org/releases/stable/amd64/>

Gite, V. (2011). *NifCraft*. Recuperado de <https://www.cyberciti.biz/tips/linux-iptables-examples.html>

Velasco, R. (2012). *Configuración del firewall en linux con iptables*. Recuperado de <http://www.redeszone.net/gnu-linux/iptables-configuracion-del-firewall-en-linux-con-iptables/>

Yanez, R. (2002). *Configuración de un cortafuegos en debían*. Recuperado de <http://man-es.debianchile.org/cortafuego.html>

### 3.5 Anexos

#### 3.5.1 encuesta

|                                                                                                                                                                                                                                                                                                                                                                      |                                                                                    |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------|
| <p><b>Universidad Tecnológica de El Salvador</b></p> <p><b>Facultad de Informatica y Ciencias Aplicadas</b></p> <p><b>Tecnico en Ingenieria De Redes Computacionales</b></p> <p>Somos alumnos de Tecnico en Ingenieria de Redes Computacionales; el objetivo de la presente encuesta es determinar la importancia de las guias de configuracion en nuestra area.</p> |  |
| <p>Indicaciones: Marca con una "X" , en el cuadro en blanco según tu criterio</p>                                                                                                                                                                                                                                                                                    |                                                                                    |

1-¿Ha trabajado usted con algún servidor?

Si ☐ No ☐

2-¿Tiene acceso a Pc para realizar las prácticas de configuración?

Si ☐ No ☐

3-¿Son importantes las guías de Configuración de sistemas operativos para la Asignatura Administración De redes?

Si ☐ No ☐

4-¿has utilizado la consola de la distribución Debían?

Si ☐ No ☐

5-¿Tiene acceso a Guías de configuración de Debían?

**Si**

☐

**No**

☐

6-¿utilizaría un servidor debían?

**Si**

☐

**No**

☐

7-¿Tiene acceso a videos didácticos para el tema?

**Si**

☐

**No**

☐

8-¿ha utilizado alguna distribución Linux?

**Si**

☐

**No**

☐

### 3.5.2 tabla de explicación de comandos dentro de consola para iptable

| COMANDO | FUNCION                                                                                                                                                                                   |
|---------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -A      | Agregar nueva regla a la cadena especificada.                                                                                                                                             |
| -I      | Insertar nueva regla antes de la regla número_regla(rulenum) en la cadena especificada de acuerdo a los parámetros sometida.                                                              |
| -R      | Reemplazar la regla (rulenum) en la cadena especificada.                                                                                                                                  |
| -E      | Modifica el nombre de la cadena.<br>[nombre-anterior-cadena por nombre-nueva-cadena]                                                                                                      |
| -L      | Listado de reglas de la cadena especificada. Si no se determina una cadena en particular, listará todas las cadenas existentes.                                                           |
| -N      | Crear nueva cadena asociándola a un nombre.                                                                                                                                               |
| -P      | Modifica la acción por defecto de la cadena preseleccionada.                                                                                                                              |
| -D      | Eliminar la regla_número(rulenum) en la cadena seleccionada.                                                                                                                              |
| -Z      | Pone los contadores de paquetes y bytes a cero en la cadena seleccionada.<br>De no poner seleccionar una cadena, pondrá a cero todos los contadores de todas las reglas en todas cadenas. |

### 3.5.3 tabla de explicación de parámetros dentro de consola para iptable

#### PARAMETROS y su FUNCION

| PARAMETRO      | FUNCION                                                                               |
|----------------|---------------------------------------------------------------------------------------|
| -i             | Interfaz de entrada (eth0,eth1,eth2...)                                               |
| -o             | Interfaz de salida (eth0,eth1,eth2...)                                                |
| --sport        | Puerto de origen                                                                      |
| --dport        | Puerto destino                                                                        |
| -p             | El protocolo del paquete a comprobar, tcp, udp, icmp ó all.<br>Por defecto es all     |
| -j             | Esto especifica el objetivo de la cadena de reglas, o sea una acción                  |
| --line-numbers | Cuando listamos las reglas, agrega el número que ocupa cada regla dentro de la cadena |

### 3.6 glosario

**Red:** Una red de computadoras, también llamada red de ordenadores, red de comunicaciones de datos o red informática

**Router:** es un dispositivo de hardware que permite la interconexión de ordenadores en red. El router o enrutador es un dispositivo que opera en capa tres de nivel de 3.

**Firewall:** Un cortafuegos (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.

**Proxy:** Un servidor proxy es un ordenador que sirve de intermediario entre un navegador web e Internet. El proxy contribuye a la seguridad de la red.

**DNS:** por sus siglas en inglés, Domain Name System es un sistema de nomenclatura jerárquico descentralizado para dispositivos conectados a redes IP como Internet o una red privada.

**DHCP:** significa Protocolo de configuración de host dinámico. Es un protocolo que permite que un equipo conectado a una red pueda obtener su configuración (principalmente, su configuración de red) en forma dinámica (es decir, sin intervención particular).

**Dominio:** en redes de computadoras, puede referirse a tres cosas: El conjunto de computadoras conectadas en una red informática que confían a uno de los equipos de dicha red, la administración de los usuarios y los privilegios que cada uno de los usuarios tiene en dicha red.

**Framework:** Un Framework es un entorno o ambiente de trabajo para desarrollo; dependiendo del lenguaje normalmente integra componentes que facilitan el desarrollo de aplicaciones como el soporte de programa, bibliotecas, plantillas y más

**NAT:** La traducción de direcciones de red o NAT (del inglés Network Address Translation) es un mecanismo utilizado por routers IP para intercambiar paquetes entre dos redes que asignan mutuamente direcciones incompatibles.

**Hardware:** El hardware es la parte física de un ordenador o sistema informático, está formado por los componentes eléctricos, electrónicos, electromecánicos y mecánicos, tales como circuitos de cables y circuitos de luz.

**Software:** Se conoce como software al equipo lógico o soporte lógico de un sistema informático, que comprende el conjunto de los componentes lógicos necesarios que hacen posible la realización de tareas específicas, en contraposición a los componentes físicos que son llamados hardware.

**Netfilter:** es un framework disponible en el núcleo Linux que permite interceptar y manipular paquetes de red

**TCP/IP:** son las siglas de Protocolo de Control de Transmisión/Protocolo de Internet (en inglés Transmission Control Protocol/Internet Protocol), un sistema de protocolos que hacen posibles servicios Telnet, FTP, E-mail, y otros entre ordenadores que no pertenecen a la misma red

**IP:** es la sigla de Internet Protocol o, en nuestro idioma, Protocolo de Internet. Se trata de un estándar que se emplea para el envío y recepción de información mediante una red que reúne paquetes conmutados.