UTMACH

UNIDAD ACADÉMICA DE INGENIERÍA CIVIL

CARRERA DE INGENIERÍA DE SISTEMAS

TEMA:
CONFIGURACIÓN DE SERVICIOS DE RED EN UNA INTRANET UTILIZANDO EL SISTEMA OPERATIVO CENTOS 7.0 PARA CONTROLAR LA INFORMACIÓN.

TRABAJO PRÁCTICO DEL EXAMEN COMPLEXIVO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERA DE SISTEMAS

AUTORA:
PINTA QUITO DIANA BEATRIZ

MACHALA - EL ORO

CESIÓN DE DERECHOS DE AUTOR

Yo, PINTA QUITO DIANA BEATRIZ, con C.I. 0705191260, estudiante de la carrera de INGENIERÍA DE SISTEMAS de la UNIDAD ACADÉMICA DE INGENIERÍA CIVIL de la UNIVERSIDAD TÉCNICA DE MACHALA, en calidad de Autora del siguiente trabajo de titulación CONFIGURACIÓN DE SERVICIOS DE RED EN UNA INTRANET UTILIZANDO EL SISTEMA OPERATIVO CENTOS 7.0 PARA CONTROLAR LA INFORMACIÓN.

- Declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional. En consecuencia, asumo la responsabilidad de la originalidad del mismo y el cuidado al remitirme a las fuentes bibliográficas respectivas para fundamentar el contenido expuesto, asumiendo la responsabilidad frente a cualquier reclamo o demanda por parte de terceros de manera EXCLUSIVA.

- Cedo a la UNIVERSIDAD TÉCNICA DE MACHALA de forma NO EXCLUSIVA con referencia a la obra en formato digital los derechos de:

  a. Incorporar la mencionada obra al repositorio digital institucional para su democratización a nivel mundial, respetando lo establecido por la Licencia Creative Commons Atribución-NoComercial-CompartirIgual 4.0 Internacional (CC BY-NC-SA 4.0), la Ley de Propiedad Intelectual del Estado Ecuatoriano y el Reglamento Institucional.

  b. Adecuarla a cualquier formato o tecnología de uso en internet, así como incorporar cualquier sistema de seguridad para documentos electrónicos, correspondiéndome como Autor(a) la responsabilidad de velar por dichas adaptaciones con la finalidad de que no se desnaturalice el contenido o sentido de la misma.

Machala, 26 de noviembre de 2015

PINTA QUITO DIANA BEATRIZ
C.I. 0705191260

1. INTRODUCCION

Actualmente con el avance tecnológico y la necesidad eminente para la comunicación, la Internet ha sido una parte importante del desarrollo del siglo XXI. Es por esto que mi trabajo se enfoca en la seguridad en redes de computadoras, en donde las empresas pueden confiar que su información valiosa, puede estar protegida ante distintas amenazas.

En este proyecto se realizara la configuración de algunos servicios que nos ayudaran a compartir información, para el desarrollo del mismo configuramos en el sistema operativo CENTOS 7.0; con el Webmin donde se configuro los servicios que nos ayudar a controlar y organizar la información.

La seguridad en redes se da en don tipos: física y lógica, en la primera donde se debe estar atento y tomar medidas preventivas como son de los desastres naturales e instalaciones eléctricas, etc. En la segunda debe tener cuidado con aquellas personas que no están autorizadas para el acceso de la información, y es ahí donde entran los piratas informáticos uno de estos son los crackers y hacker. Es por eso que se deben tener medidas preventivas para combatir estos ilícitos, ya sea con políticas de seguridad de la organización, de herramientas de seguridad para los sistemas operativos, y también dar la capacitación al personal, que es fundamental para tener una buena seguridad.

1.1 MARCO CONTEXTUAL

La constante necesidad de tener disponibles los mejores recursos humanos, técnicos o tecnológicos en las organizaciones, con el fin de competir con servicio y una buena infraestructura, ha incrementado también la utilización de aplicaciones, la adecuación de nuevas estaciones de trabajo, así como de la vinculación del personal que las administra. En el afán de entregar los resultados esperados, las empresas dejan de lado el análisis de las implicaciones que puede traer consigo, una mala implantación de los procesos, al no tener en cuenta o no aplicar la política de seguridad en la organización. Es común ver como varias personas que laboran en la organización manejan con idéntica contraseña una aplicación de uso frecuente y confidencial, que tienen acceso a todo sin excepción y que no dimensionan la delicadeza de sus contenidos. Además, no hay respaldo de la información de cada estación de trabajo, teniendo un alto riesgo de perderse por la misma inseguridad que se maneja en la red.
En la mayoría de las empresas no se ha cuantificado el daño económico o de impacto organizacional que podría acarrear un manejo inadecuado de los recursos tecnológicos y de la información en sí misma. Actualmente en algunas organizaciones, no existe un esquema de seguridad informática que permita tener un punto de referencia ante posibles ataques informáticos o evitarlos de alguna manera, constituyéndose cada vez en un punto principal de la organización. (César, 2015)

1.2 PROBLEMA

En la actualidad las empresas tienen problemas o inconvenientes activos en cuanto a la seguridad de red. No cuenta con una red lógica estable, su esquema de seguridad es débil, el nivel de comunicación es pésimo, la información es mal procesada y desviada, hay muchas empresas que no cuentan con servicios de red bien especificados para su mejor funcionamiento, los puntos de trabajo no tienen restricciones de esta forma los usuarios y empleados acceden de forma deliberada a cualquier punto de trabajo y así no se dedican a brindar un mejor servicio para la comunidad, en muchos campos se dedican más a entrar a páginas que no competen a su trabajo una de estas son las redes sociales. Todos estos puntos hacen que el servicio que brindan sea pésimo. (Mikeliunas, 2014)

1.3 OBJETIVO GENERAL

Configurar los servicios de red utilizando Centos 7.0, para organizar y establecer controles de seguridad de la información.

2. DESARROLLO

2.1 MARCO TEORICO

2.1.1 SERVIDOR DNS

El servicio de DNS o Domain Name System (Sistema de nombres de dominio) que permite el acceso de los usuarios a Internet utilizando nombres significativos y semánticos como www.linuxhq.com o news.mozilla.org. (Félix, 1998)

2.1.2 SERVIDOR DHCP

Dynamic Host Configuration Protocol es utilizado por muchas redes basadas en Ethernet para la entrega de las direcciones IP a los dispositivos cliente (PC) de una manera fácil y escalable. (Haskins, 2007).

2.1.3 XAMMP

Xampp es un servidor independiente en base a software libre, con el cual podemos disponer de un servidor propio o simplemente usarlo para hacer pruebas de nuestras páginas web, bases de datos, para desarrollar aplicaciones en php, con conexión a base de datos sql (LAMPP= Linux + Apache + MySQL + PHP + Perl) (Desarrollo de Aplicaciones Web, 2015).

2.1.4 SERVIDOR WEB

Es la maquina o computador donde se almacena su página web. Toda la información publicada en cada sitio web se almacena en un espacio destinado para este fin. De lo contrario no habría forma de divulgar el contenido. (Empresamia, 2003).
El servidor web más utilizado es Apache, el servidor web más utilizado debido a la implementación de protocolos actualizados y a la rapidez con que muestra la información. Apache además cuenta con los constantes aportes de un grupo de voluntarios que trabaja en el mejoramiento del mismo y tiene el soporte de la Fundación Apache, la cual vela por ofrecer un software de alta calidad. (Empresamia, 2003).

2.1.5 SERVIDOR PROXY

El servidor proxy otorga grandes ventajas respecto a la seguridad y centralización en cierta medida del control de la red. Un proxy es un equipo o dispositivo que actúa como intermediario entre el usuario final e internet, la función del proxy es filtrar el contenido que pueden ver los usuarios en páginas y sitios de internet además de registrar el uso de internet. (Matew, 2014)
El servidor proxy que se va a utilizar en la siguiente actividad es SQUID el cual es una de las aplicaciones Open Source más populares y funciona como servidor proxy para web con caché, y así cuando los

usuarios hagan de nuevo una petición a la misma página, el servidor no tendrá que ir de nuevo hasta internet si no que entregar desde su caché. (Matew, 2014)

2.1.6 SERVIDOR DE CORREO

El correo electrónico (correo-e, conocido también como e-mail), es un servicio de red que permite a los usuarios enviar y recibir mensajes y archivos mediante sistemas de comunicación electrónicos. El correo electrónico gira alrededor del uso de las casillas de correo electrónico. Cuando se envía un correo electrónico, el mensaje se enruta de servidor a servidor hasta llegar al servidor de correo electrónico de destino. Más precisamente, el mensaje se envía al servidor del correo electrónico (llamado MTA, del inglés Mail Transport Agent [Agente de Transporte de Correo]) que tiene la tarea de transportarlos hacia el MTA del destinatario. En Internet, los MTA se comunican entre sí usando el protocolo SMTP, y por lo tanto se los llama servidores SMTP (o a veces servidores de correo saliente). Para su funcionamiento necesitan de los servidores DNS que les indican cuales son los servidores de correo de un determinado domino. (Mikeliunas, 2014)

2.1.7 FIREWALL

Un firewall o cortafuegos es un elemento hardware o software utilizando en una red de computadoras para controlar las comunicaciones, permitiéndola o prohibiéndolas según la política que haya definido la organización responsable de la red.
La ubicación habitual de un firewall es el punto de conexión de la red interna de la organización con la red exterior, que normalmente es internet; de este modo se protegen los sistemas internos de acceso no autorizado desde internet, que puedan aprovechar vulnerabilidades de los mismos. (aspl, 2015).

2.1.8 SERVIDOR DE REDES

La Real Academia Española da como definición de servidor: “unidad informática que proporciona diversos servicios a computadoras conectadas con ella a través de una red” (Quees.la, 2014)

2.1.9 METODOLOGIA DEL DESARROLLO EN CISCO

Las redes en los negocios se han convertido en una de los factores importantes para el desarrollo de las operaciones, así como para el crecimiento del mismo, por lo que no es de menos pensar deben estar funcionando a su más alto rendimiento y que la seguridad y estabilidad son factor importante que se debe tener en cuenta. (cisco system, 2002).

- **Fases del Ciclo de la Red Preparación –** "Desarrollo plan de negocios para justificar la inversión tecnológica ". (cisco system, 2002)

- **Planeación -** "Evaluación del estado actual de la red para soportar la solución propuesta ". (cisco system, 2002)

- **Diseño -** "Creación de un diseño detallado para manejar requerimientos técnicos y de negocios ". (cisco system, 2002)

- **Implementación -** "Despliegue de la nueva tecnología ". (cisco system, 2002)

- **Operación -** "Mantenimiento de la salud de la red en el día a día de las operaciones ". (cisco system, 2002)

- **Optimización -** "Alcance de la excelencia operacional a través de mejoras permanentes ". (cisco system, 2002)

2.2 MARCO METODOLOGICO

2.2.1 METODOLOGIA DEL DESARROLLO BASADO EN CISCO

FASE DE PREPARACIÓN
En esta fase vamos hacer referencia a las necesidades de la empresa, el sistema en el que se trabajara y los software a utilizar para el establecer la red.

PLANEACIÓN
Aquí se verá la infraestructura de red a configurar con los diferentes servicios de red:

- **DHCP**
  ASIGNAMOS LAS IPS.

He configurado el servicio DHCP en el WEBMIN, primero nos dirigimos a la pestaña de Servidores y entramos donde dice Servidor DHCP. → Aquí configuramos para que asigne automáticamente direcciones IP a los dispositivos que se conecten a esta red, para esto se añade una subred en la sección SUBREDES Y REDES COMPARTIDAS → Aquí se ingresara los campos de **subnet description**, **dirección de red, rango de direcciones IP, mascara de subred.** → Luego de esta configuración básica se creara correctamente nuestra subred.

PARA ASIGNAR UNA IP A UNA MAQUINA FIJA EN UN SERVIDOR DHCP MEDIANTE UNA MAC:

Debemos dirigirnos: MAQUINAS Y GRUPOS DE MAQUINAS, donde añadimos un maquina nueva. → ingresamos nombre de la nueva máquina para diferenciar de las otras. → añadimos la Mac de la maquina a la que se le va asignar la IP mediante la Mac → crear y listo.

- **DNS**

  CREAMOS EL DOMINIO.

Dentro del Webmin nos colocamos en sección servidores, aquí seleccionamos DNS BIND, nos aparecerá la pantalla de configuración global.→ seleccionamos **Crear Zona Master** → luego que hemos creado la zona podemos editar la misma, creamos los registros NS, marcamos nombres y direcciones de reenvió que es la zona directa → y salvar.

- **PROXY**

  RESTRINCIONES, ASIGNACION Y AUTENTICACION.

En Webmin nos colocamos donde dice servidores → seleccionamos Squid Servidor Proxy una vez instalado el paquete → clic en puertos y trabajo en red → colocamos la IP de nuestro equipo → luego en icono Control de Acceso para crear los **Acl** y una expresión regular de Url → luego creamos Acl para negar ciertas páginas con contenido XXX en el navegador → luego en control de acceso hacemos lo mismo, nos vamos en restricciones y nos aparecerá los Acl creados, nos dirigimos a denegar all → en opciones administrativas, en la casilla Nombre de Maquina Visible agregamos un nombre en el que sadra navegador negado → salvar

- **SERVIDOR WEB**

  CREACION DE UN SISTEAMA WEB CON BASE DE DATOS.

Para este servicio hemos trabajado con easyPHP un paquete completo que incluye Apache, PHP, MySQL, PHPMyAdmin y SQLiteManager.
Xammp un paquete con el cual podemos trabajar desarrollando páginas web en un entorno seguro.

Para instalar lo hacemos desde la consola:

```
sudo tar xvfz xampp-linux-1.8.1.tar.gz -C /opt
```

Para desarrollar aplicaciones siempre hay que arrancar Xammp lo podemos hacer de una interfaz gráfica que nos permite hacerlo de forma fácil todos los servicios uno por uno. Se lo abre con la siguiente comando:

```
sudo /opt/lampp/share/xampp-control-panel/xampp-control-panel
```

Luego de esto podemos a queda creado nuestro servidor local para programar en PHP con base de datos y lo que es seguridad.

- **CORREO ELECTRONICO**

  CREACION DE CORREO INSTITUCIONAL BAJO UN DOMINIO CONTROLAR CORREOS INTERNOS.

Nos colocamos donde dice servicio Sedmail y nos aparecerá una pantalla donde se procede a configurar. →debemos configurar puertos y las direcciones IP donde queremos que el sedmail se ponga a la escucha para envía recibir sms esto es en Network Ports. → para especificar nuestros dominios y que

sean escuchados debemos ingresar a Local Domains para regístralos y nuestros correos no sean rechazados.

- **FIREWALL**
  CONTROLAR LA COMUNICACIÓN ENTRE REDES LAN Y WAN

La configuración se la realizo en la terminal de Centos 7.0 para ello hemos hecho uso de algunos comandos:

```
iptables -A INPUT -i lo -j ACCEPT
iptables -A INPUT -p tcp -m tcp --dport 80 -j ACCEPT
iptables -A INPUT -p tcp -m tcp --dport 443 -j ACCEPT
iptables -A INPUT -p tcp -m tcp --dport 25 -j ACCEPT
iptables -A INPUT -p tcp -m tcp --dport 465 -j ACCEPT
iptables -A INPUT -p tcp -m tcp --dport 110 -j ACCEPTiptables -A INPUT
-p tcp -m tcp --dport 995 -j ACCEPT
iptables -A INPUT -p tcp -m tcp --dport 143 -j ACCEPT
iptables -A INPUT -p tcp -m tcp --dport 993 -j ACCEPT
```

Estas son ciertas reglas que se aplicaron para el cortafuegos.

DISEÑO
Disponibilidad, soporte, confiabilidad y seguridad de la red.
Diseño de esquema lógico y físico. (Ver Anexo 5.1)

IMPLEMENTACIÓN
Configuramos los servicios que harán posible el correcto funcionamiento de nuestro esquema de seguridad.

OPERACIÓN
Pruebas son la conexión y el funcionamiento adecuado del servidor y los clientes.

OPTIMIZACIÓN
Manejo de los servicios de red y funcionamiento de página web.

2.3 RESULTADOS

2.3.1 Resolver el Servidor DHCP

Realizamos subneting para nuestras 3 subredes.

$$2^6 = 64 - 2 = 62 \text{ host}$$

Red Lan 1
IP validas 192.1681.1 hasta 192.168.1.62
Subred 192.168.1.0 hasta 192.168.63

Red Lan 2
IP validas 192.168.1.65 hasta 192.168.1.126
Subred 192.168.1.64 hasta 192.168.127

Red Lan 3
IP validas 192.1681.129 hasta 192.168.1.90
Subred 192.168.1.128 hasta 192.168.191

Servidor DNS

Para configurar el Servicio de nombre de dominio se realiza una serie de comandos donde se editara los diferentes archivos que resuelven la petición www.xyz.com (Ver Anexo 5.2)

Ilustración 1: Creación de Dominio

Ilustración 2: Dominio a Prueba

Servidor de Firewall

Para especificar qué tipos de paquetes acceden o salen de nuestro equipo, tenemos que describirlos de una forma determinada para que IPtables nos comprenda. Para esto necesitamos órdenes y parámetros con los que formular la regla debidamente. (Ver Anexo 5.3)

Ilustración 3: Prueba Antes de Desactivar Puerto 80 = ACCEPT

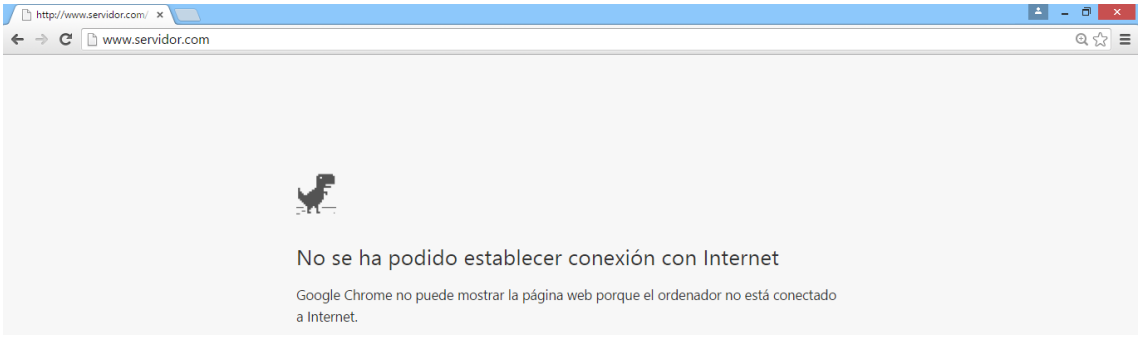


Ilustración 4: Puerto 80 = DROP Denegado

Servidor Web

Se visualiza en este imagen la pagina web donde se realiza el ingresos de la informacion en la base de datos:

Ilustración 5: Servidor Web - Base de Datos

Servidor Proxy

Se puede ver que no permite ingresar a las páginas prohibidas que hemos bloqueado por medio de los ACL.

Ilustración 6: Acceso Denegado Se Aplicó ACL

Servidor de Correo

Para realizar la prueba del servicio se ha enviado un correo desde servidor cliente,

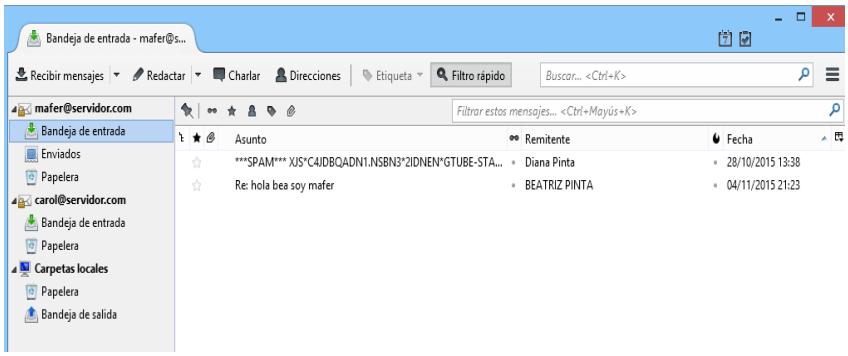


Ilustración 7: Prueba de Correo

3. CONCLUSIONES

He concluido que los servicios de red son indispensables para la comunicación y transmisión de información entre los usuarios en la infraestructura de red. También se demostró el correcto funcionamiento del sitio WEB y la comunicación interna que se logró interconectar las sucursales atreves de salidas a internet entre las diferentes empresas fortaleciendo la comunicación.
Al terminal se verificó que todos los servicios como son: DHCP, DNS, PROXY, FIREWALL, CORREO, están operables y en ejecución siendo este proyecto satisfactorio para la empresa ya que resolviendo las necesidades requeridas al inicio de la investigación.

4. BIBLIOGRAFÍAS

(10 de 2014). Obtenido de Quees.la: http://quees.la/servidor-de-redes/

Apache, s. (02 de 10 de 2010). Apache. Recuperado el 10 de 2015, de https://httpd.apache.org

aspl. (2015). Servidor Firewall Linux. Obtenido de http://www.aspl.es/portal/servicios/instalacion-de-servidores-linux/servidor-firewall-linux

César, C. R. (2015). Política de Seguridad Informática para Apostar S.A. Obtenido de http://ribuc.ucp.edu.co:8080/jspui/bitstream/handle/10785/1503/CDMIST26.pdf?sequence=1

cisco system. (2002). Recuperado el 2015, de https://www.cisco.com/web/LA/productos/servicios/docs/Cisco_Optimization_services_datasheet_Spanish.pdf

CISCO SYSTEMS. (s.f.). CISCO.COM. Recuperado el 23 de OCTUBRE de 2015, de https://www.cisco.com/web/LA/productos/servicios/docs/Brochure_LCS_062006_SP_Spanish.pdf

civianes, f. (2010). Servicios en red. madrid: Paraninfo S.A.

Desarrollo de Aplicaciones Web. (0 de 2015). Murcia, España, Europa.

Dueñas, J. B. (07 de 04 de 2013). alcancelibre. Recuperado el 01 de 10 de 2015, de http://www.alcancelibre.org/

Empresamia. (2003). Obtenido de http://empresamia.com/crear-empresa/crear/item/644-que-es-un-servidor-web

Félix, A. d. (1998). Dialnet. Obtenido de http://dialnet.unirioja.es/servlet/articulo?codigo=4691596

Gomez, J. A. (2010). Servicios en Red. madrid: Editex.

Haskins, R. (FEBRERO de 2007). Dialnet. Obtenido de http://dialnet.unirioja.es/servlet/articulo?codigo=4957100

Jaime, J. (12 de 11 de 2008). Laboratorios Virtuales GNS3. Recuperado el 1 de 10 de 2015, de http://d3ny4ll.blogspot.com/2008/11/laboratorios-virtuales-gns3.html

Jorge, G. (28 de 06 de 2011). slideshare. Recuperado el 1 de 10 de 2015, de http://es.slideshare.net/josegregoriob/servidor-web-8451426

Langue, E. (17 de 04 de 2014). shideshare. Recuperado el 05 de 10 de 20015, de http://es.slideshare.net/eduardoelange/diferencias-entre-enrutamiento-esttico-y-dinmico

Lobato, M. P. (01 de 07 de 2007). recursostic. Recuperado el 01 de 10 de 2015, de http://recursostic.educacion.es/observatorio/web/fr/software/software-general/462-monografico-maquinas-virtuales?start=2

Loja, I. N. (Septiempre de 2015). Caso de estudio. Recuperado el 01 de octubre de 2015, de Google Drive: https://drive.google.com/file/d/0B8LcNkfGWPH0cGNFQV9oVFpxQUk/view?pli=1

Matew, A. (2014). Servidor Web. Obtenido de http://es.slideshare.net/Rooccck/squi-don-redhat

McConnell, S. (1996). Rapid Development. Mexico: Pearon Educacion.

Mikeliunas, A. S. (2014). Administración de Infraestructuras. Obtenido de https://www.fing.edu.uy/tecnoinf/mvd/cursos/adminf/material/adi05-servidor-correo-configuracion.pdf

norfipc. (15 de 03 de 2014). Obtenido de https://norfipc.com/internet/instalar-servidor-apache.html

Oracle. (15 de 02 de 2015). Oracle. Recuperado el 01 de 10 de 2015, de http://www.oracle.com/es/products/mysql/overview/index.html

Política de Seguridad Informática para Apostar S.A. (2015). Obtenido de http://ribuc.ucp.edu.co:8080/jspui/bitstream/handle/10785/1503/CDMIST26.pdf?sequence=1

RUiz, P. (13 de 08 de 2013). somebooks. Recuperado el 1 de 10 de 2015, de http://somebooks.es/?p=3366

Sommerville, I. (2005). Ingenieria del Software. Pearson.

5. ANEXOS

5.1 Esquema Lógico de Red

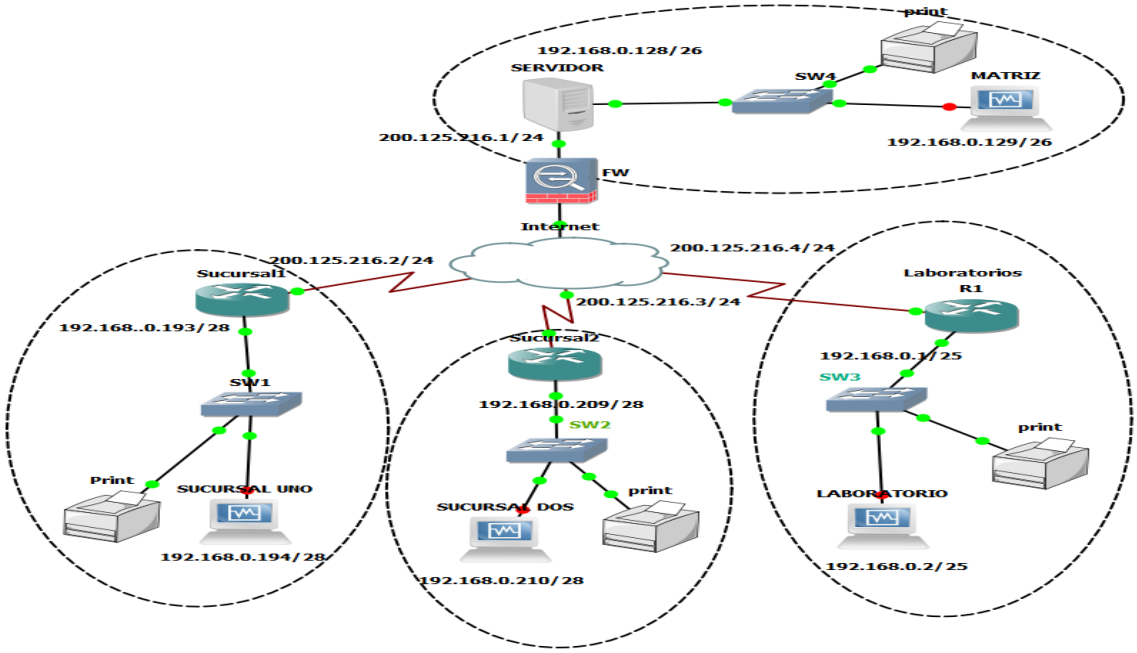
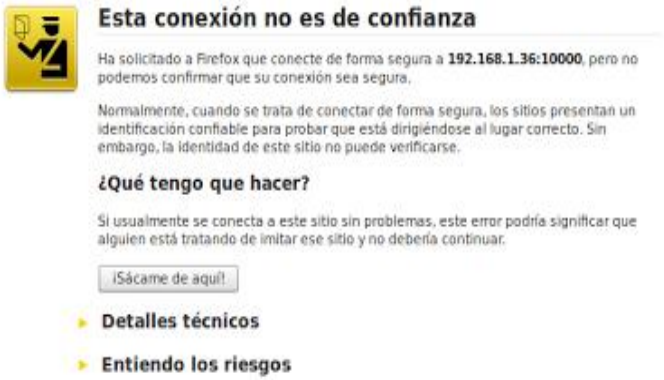


Ilustración 8: Esquema Logico Y Seguridad

5.2 INSTALACIÓN Y CONFIGURACIÓN DE SERVIDOR PROXY CON WEBMIN

Paso 1:

Digitamos en nuestro navegador nuestra dirección IP con el puerto 10000.



Ejemplo: https://192.168.1.44:10000/ y después de superar la pantalla de excepción

Ilustración 9: Puerto 10000

Procedemos a logearnos:

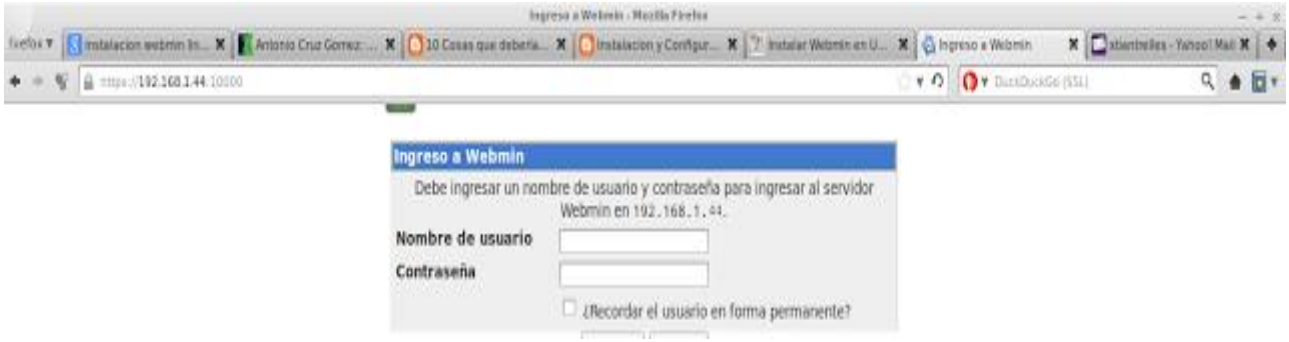


Ilustración 10: Ingreso al Webmin

Paso 2:
Procedemos a la instalación de nuestro servidor proxy haciendo clic en "Pulse aquí"

Ilustración 11: Configuración de Proxy

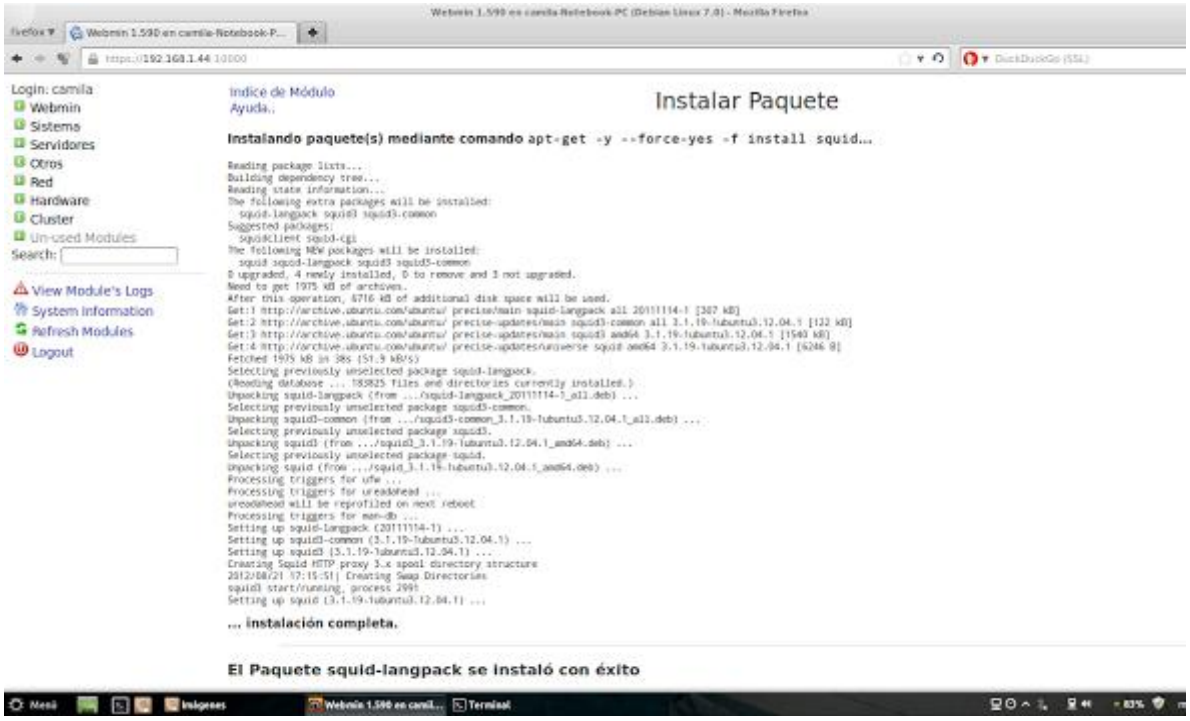


Ilustración 12: Instalar un Paquete

Paso 3:
Culminada la instalación, en el menú principal ingresamos a "**Servidores - Squid Servidor Proxy**" para luego configurarlo haciendo clic en "**Control de Acceso**"

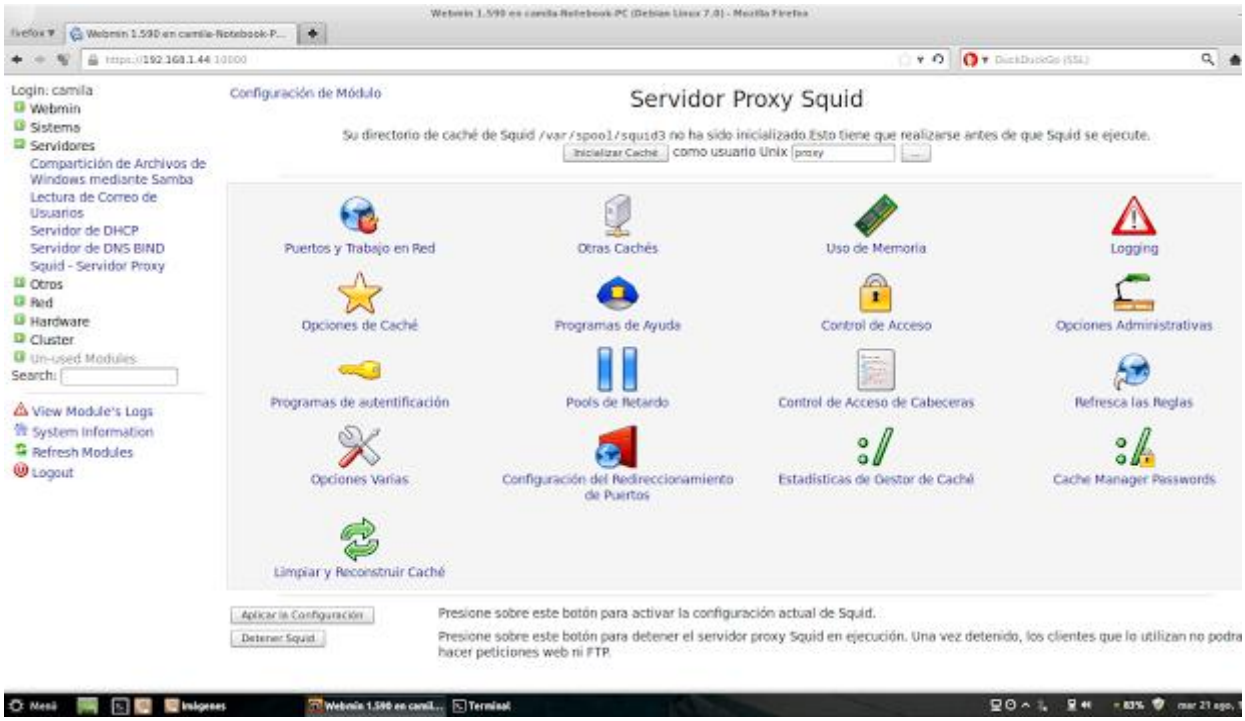


Ilustración 13: Panel del Proxy

Paso 4:
Procedemos a editar los permisos permitiendo o negando acceso según sea el caso.

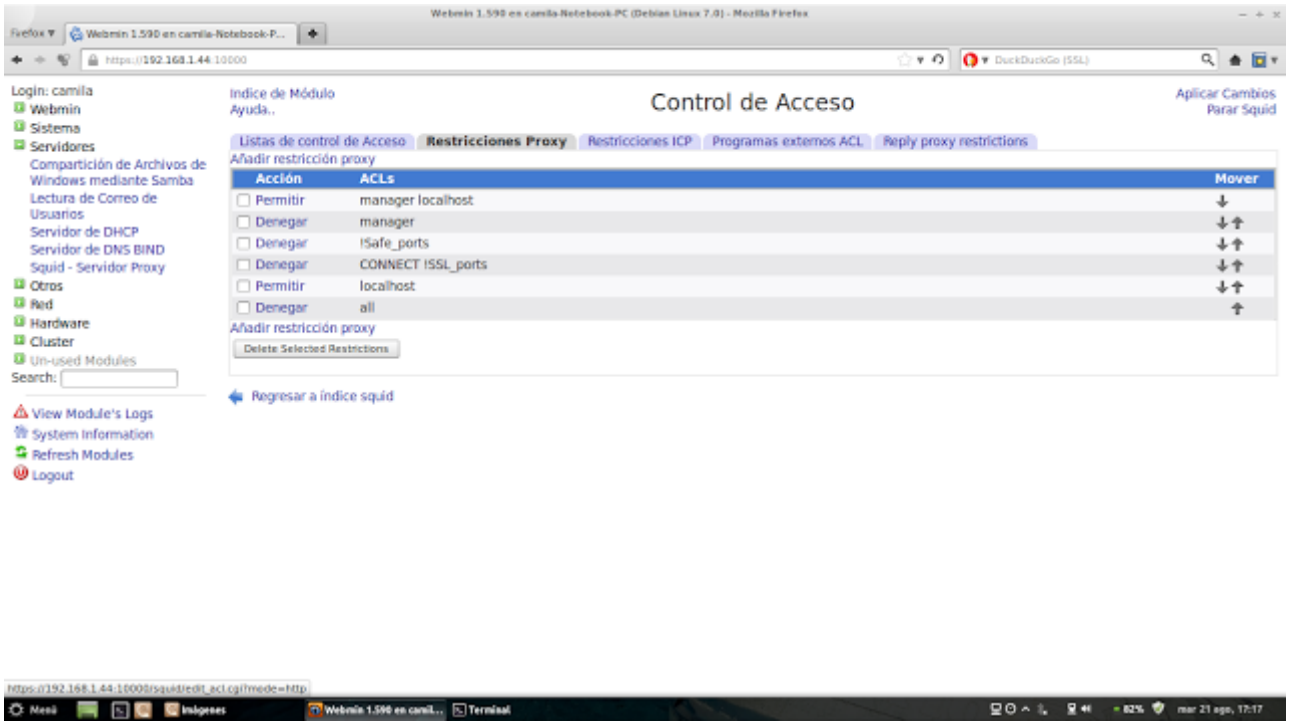


Ilustración 14: Control Acceso

Paso 5:
Regresamos al menú principal en donde escogeremos "**Puertos y Trabajo en Red**" para poder editar nuestros puertos
Luego la editaremos quedando como se muestra

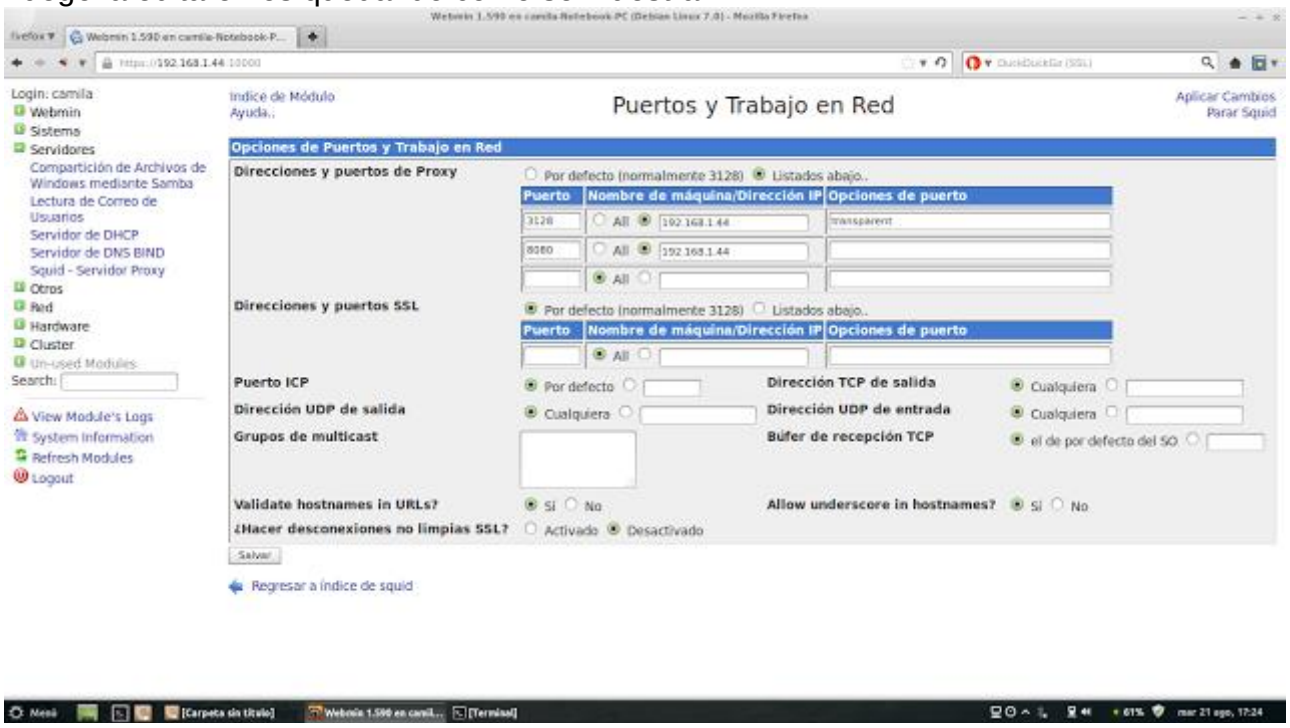


Ilustración 15: Editar Puertos de Acceso

Paso 6:
En el cliente de nuestro servidor proxy nos ubicamos en la pestaña "**Editar**" de nuestro navegador ubicaremos la opción "**Preferencias**" y ubicaremos la pestaña "**Avanzado - Red**" y en Conexión editamos en el botón "**Configuraciones**"

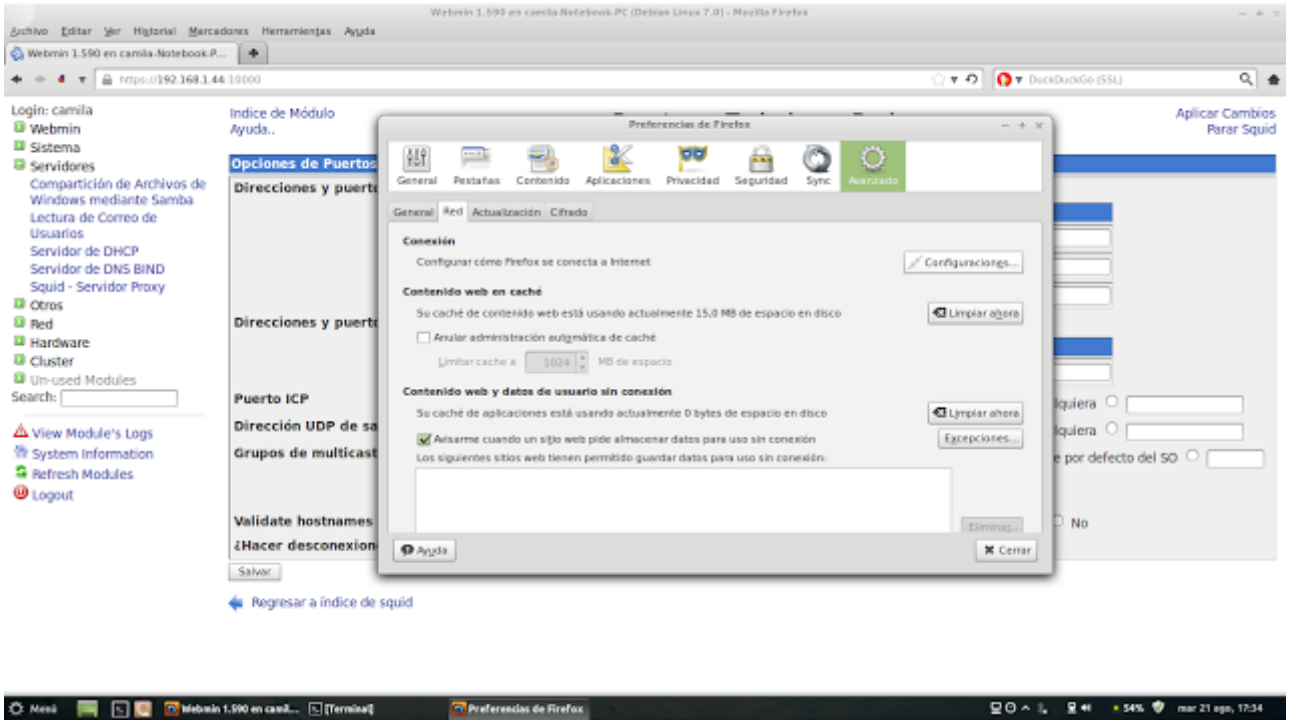


Ilustración 16: Configuracion De Conexión

Paso 7:
Configuramos las opciones de nuestro navegador en el cliente como se muestra direccionando con el IP de nuestro servidor proxy

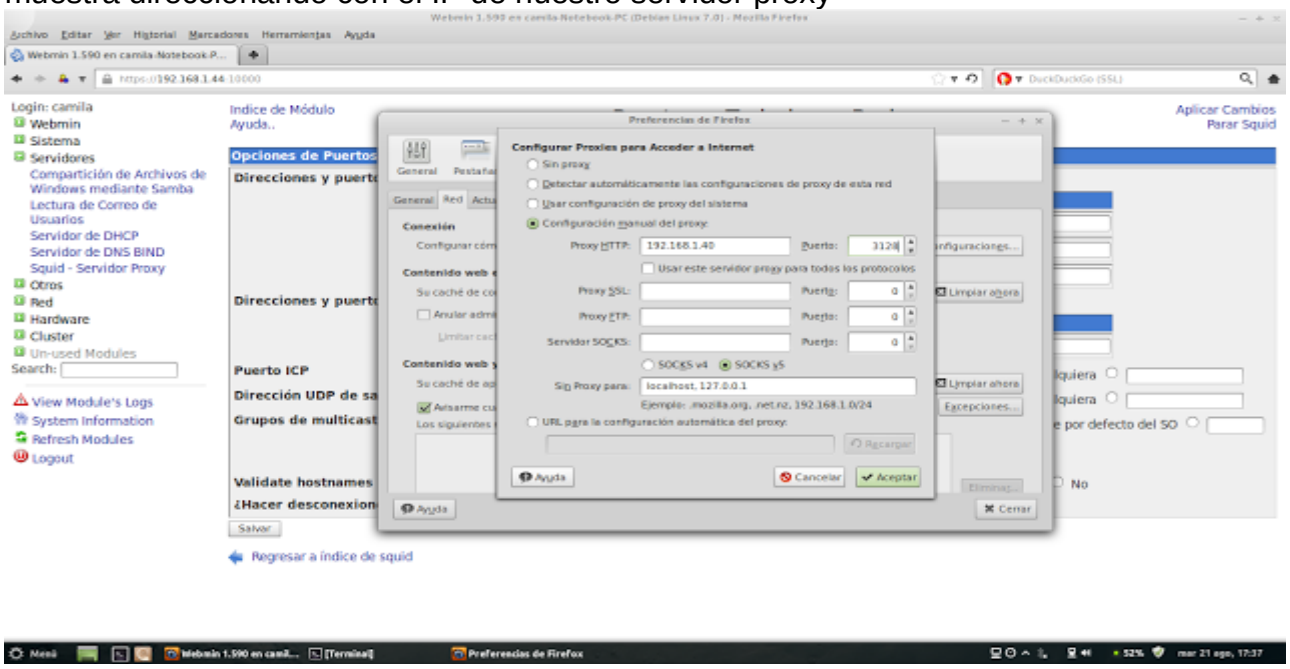


Ilustración 17: Configuración de Navegador

Paso 8:
Regresamos al Menú de **Servidor Proxy Squid** en donde escogeremos "**Control de Acceso**"

Ilustración 18: Menú de Servidor Proxy Squid

Paso 9:
En las **Listas de Control de Acceso** seleccionaremos una "**Autenticación Externa**" y se colocara **Expresión Regular URL**, dando paso a **Crear nueva ACL** Así podremos configurar los accesos o denegarlos según sea la necesidad de la administración las que ubicaremos siempre por encima por "**Denegar All"** y guardamos los cambios que hayamos hecho cliqueando en **"Aplicar cambios"**

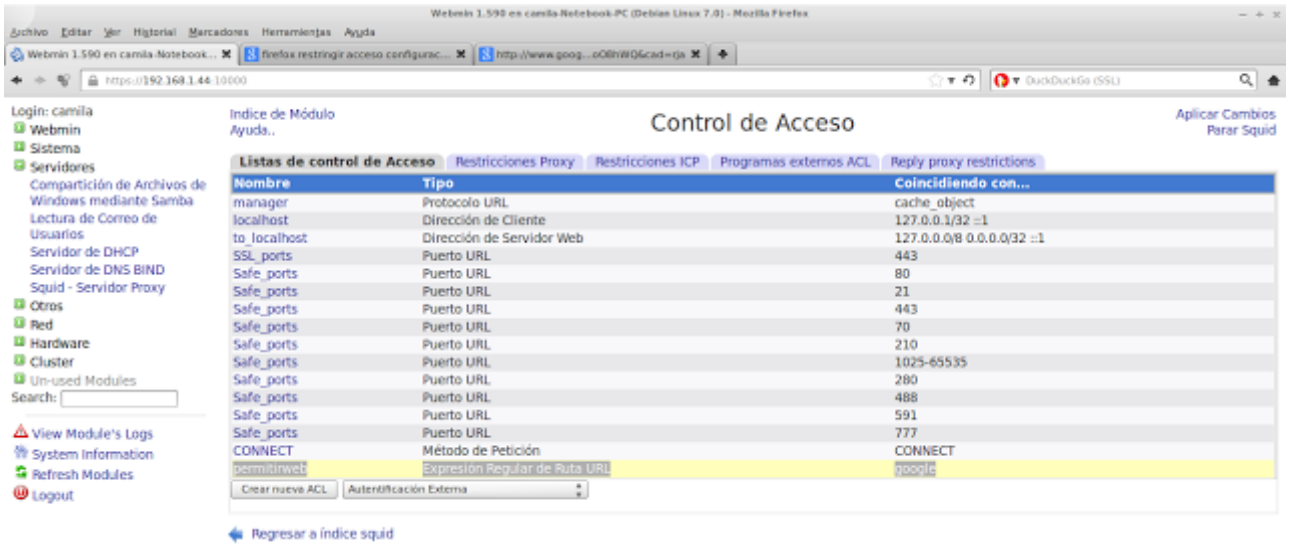


Ilustración 19: Lista de Control De Acceso

CONFIGURACION DE SERVIDOR DHCP

Tenemos nuestro Webmin abierto y nos dirigimos a la sección de servidores, y entramos en el servidor de DHCP:

Ilustración 20: Panel de Servidores

Una vez dentro veremos algo como esto:

Ilustración 21: Servidor DHCP

ASIGNAR CONFIGURACIONES DE RED A DISPOSITIVOS

El uso principal que le daremos a un servidor DHCP es el de asignar automáticamente direcciones IP a los dispositivos que se conecten a la red. Para ello debemos Añadir una nueva subred (en la pantalla del servidor DHCP de Webmin).

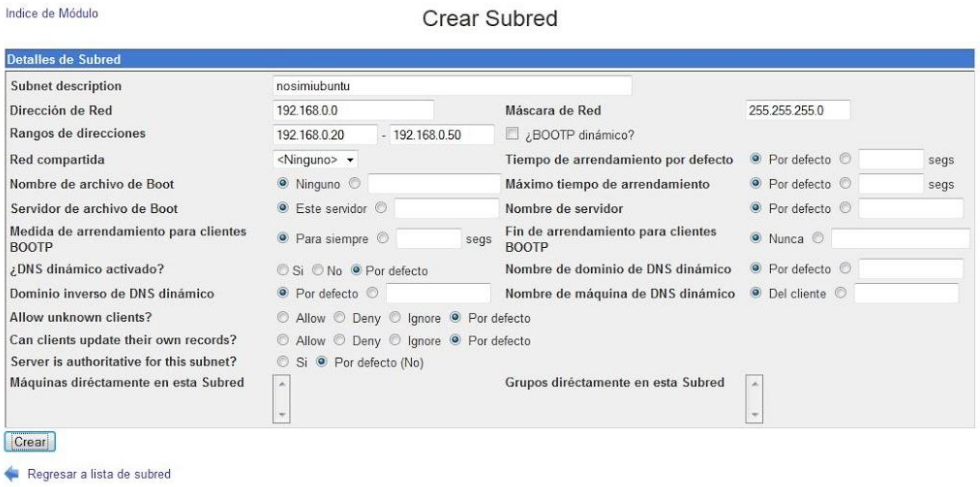


Ilustración 22: Crear una Subred

En “Subnet description” debemos asignar un nombre para poder diferenciar unas de otras, este nombre es irrelevante en el funcionamiento, pero es útil a nivel organizativo.
La dirección de Red, es la dirección de red en la cual va a funcionar el servidor DHCP

Nota:

La dirección de red, recuerdo que es la que tiene la parte de red original, y la parte de host con el número 0. Por ejemplo 192.68.0.0, sería la red 168.68.

El rango de direcciones, se refiere a las direcciones IP que va a poder asignar el servicio. En el ejemplo asigne 30 direcciones libres.

Máscara de Red (subred), debemos poner todos los bytes de la dirección de red en 255 y los de host en 0.

Cuando terminemos estas configuraciones básicas le damos a crear en la parte inferior de la página y veremos que se ha creado correctamente:

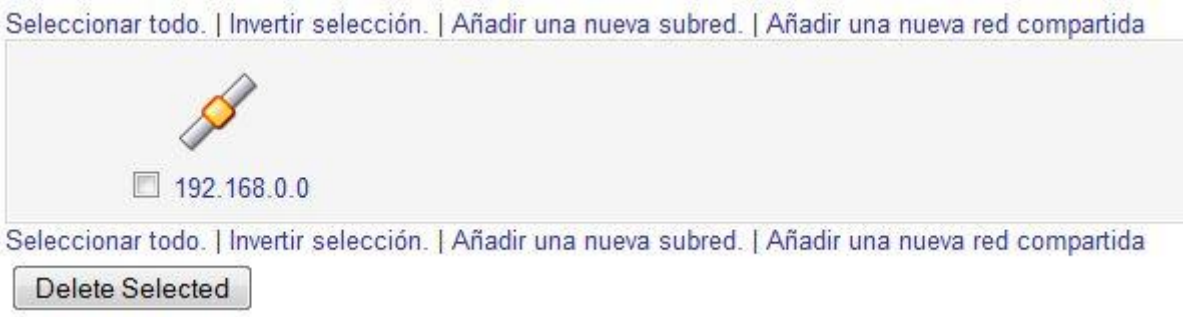
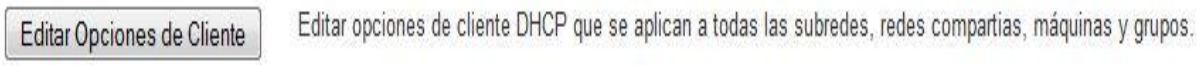


Ilustración 23: Red Creada

Hasta ahora solamente hemos proporcionado al dispositivo una dirección IP, una máscara de subred, y una red. Nos queda asignarle una puerta de enlace, para que tenga salida a internet y a otros ordenadores de otras áreas locales. Y además los servidores DNS para resolver direcciones IP.

Ahora debemos dirigirnos a “Editar Opciones de Cliente” para agregar unas características comunes a todas las subredes creadas como en el paso anterior.



Una vez dentro veremos algo como esto:

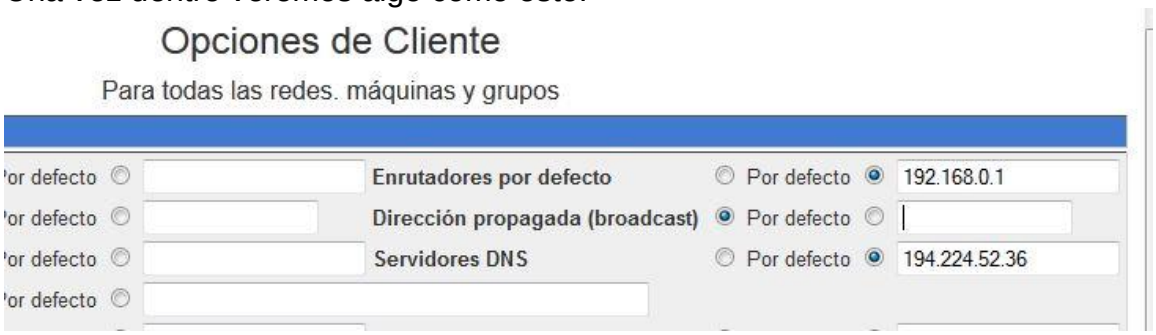


Ilustración 24: Opciones De Cliente

En enrutadores por defecto, debemos poner la dirección IP del router y en servidores DNS, las dirección del servidor DNS que nos proporcione el ISP (proveedor del servicio de Internet) o un DNS público como el de la imagen.

SELECCIONAR INTERFAZ DE RED

Si tenemos varias tarjetas de red, debemos elegir en cual debe funcionar el servidor DHCP. En la página inicial de DHCP, debemos hacer click en “Edit Network Interface” y allí nos saldrán todas las interfaces que tiene nuestro ordenador, allí elegiremos la que deseamos. En mi caso solo hay una, sin contar la de loopback.

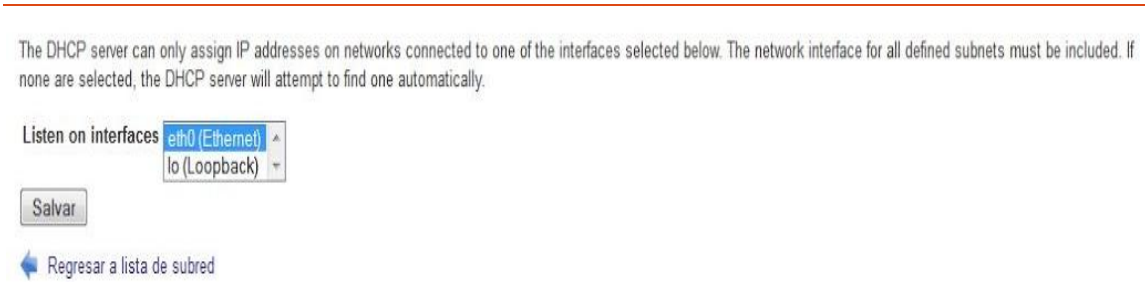
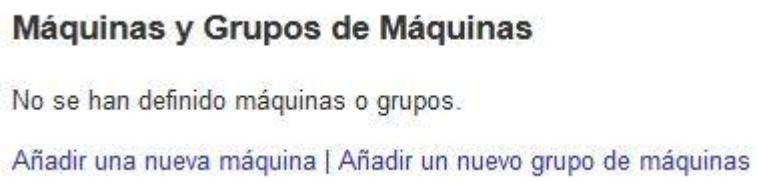


Ilustración 25: Selección De Interfaz De Red

ASIGNAR UNA DIRECCIÓN FIJA A UNA MÁQUINA EN UN SERVIDOR DHCP MEDIANTE DIRECCIÓN MAC

Debemos estar en la página principal y dirigirnos a Máquinas y Grupos de Máquinas y añadir una nueva máquina.



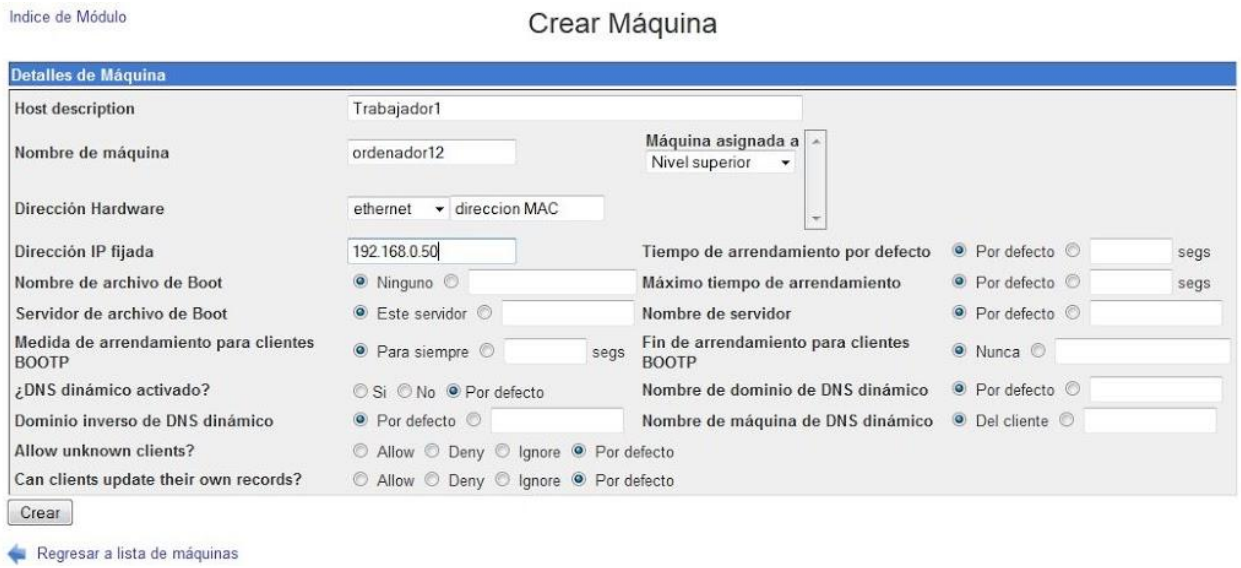
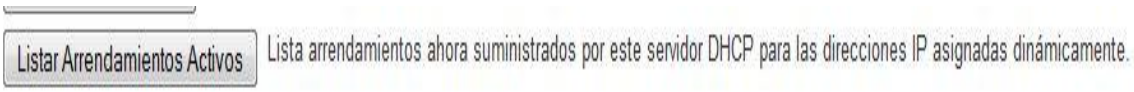
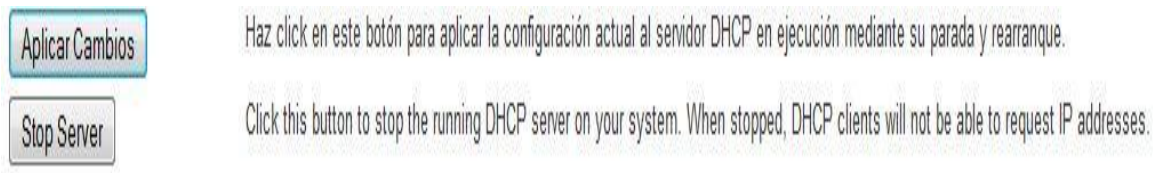


Ilustración 26: Crear Maquina Asignar MAC

Una vez ahí, debemos añadir un nombre para diferenciarlo, el nombre de la máquina.
Debemos añadir también la dirección hardware (en la imagen sale dirección MAC) y la IP que queremos asignar. Seleccionamos crear y listo.



Para finalizar, debemos acordarnos cada vez que realicemos un cambio, reiniciar el servicio mediante la interfaz del webmin.



CONFIGURACION SERVICIO XAMMP PARA PAGINA WEB

Paso 1
Por supuesto que descarga la versión oficial de **Xampp** de su propia web y no de otros sitios mierdas y así evitamos tener versiones desactualizadas

Paso 2
Descomprimimos nuestro archivo descargado.
Pueden comenzar hacerlo de 2 formas, una moviendo el archivo a carpeta de inicio o dejándolo donde **se descargo por defecto que es en la carpeta Descargas** o**Downloads** (dependiendo el idioma) y vamos a entrar a esa carpeta X donde tengamos nuestro archivo **en mi caso es Downloads así que:**
Por cierto "xaelkaz" es mi nick para el usuario, durante todos los comandos veran este nombre, obviamente ustedes deberan remplazar este nombre por el suyo.

```
cd /home/xaelkaz/Downloads/
tar xvfz xampp-linux-1.8.1.tar.gz -C /opt
```

Paso 3
Nos vamos a la carpeta donde se instalo nuestro Xampp para darle **privilegios a la carpeta** donde se guardaran nuetros archivos que vamos a ejecutar como **localhost**.

```
sudo chmod a+w /opt/lampp/htdocs
```

Paso 4
Ahora nos vamos a la carpeta "etc" para a**sociar nuestro nombre de usuario en Linux con la configuración de Apache.**

```
cd /opt/lampp/etc
```

Vamos editar este archivo (httpd.conf) con el editor gedit, recuerden que existe algunos otros como nano, kate, pico … usar uno o el otro es desicion personal.

```
sudo gedit httpd.conf
```

Ahora vamos a la linea donde aparece "User nobody" y lo cambiamos el nobody por tu nombre de usuario en mi caso el cambio es así:

```
User nobody
Group nogroup
```

Lo cambiamos por

```
User xaelkaz
Group nogroup
```

Paso 5
Vamos a modificar ahora el archivo "httpd-xampp.conf" para cambiar ciertos conceptos de seguridad que ha ingresado Xampp en sus ultimas actualizaciones

```
sudo gedit /opt/lampp/etc/extra/httpd-xampp.conf
```

La parte de LocationMatch debe quedarle algo como esto; (osea que solo cambiamos el Deny por "Allow from all")

<LocationMatch
"^/(?i:(?:xampp|security|licenses|phpmyadmin|webalizer|server-status|server-info))">
Order deny,allow
Allow from all
Allow from ::1 127.0.0.0/8 \
fc00::/7 10.0.0.0/8 172.16.0.0/12 192.168.0.0/16 \
fe80::/10 169.254.0.0/16
ErrorDocument 403 /error/XAMPP_FORBIDDEN.html.var
</LocationMatch>

La Parte de Directory debe quedar así; (agregamos Require all granted)

<Directory "/opt/lampp/phpmyadmin"> AllowOverride AuthConfig Limit
Order allow,deny
Allow from all
Require all granted
</Directory>
Todo lo demás lo vamos a dejar como esta

Paso 6 y Final

Simplemente **iniciamos** con el comando

sudo /opt/lampp/lampp start

Con esto ya podemos comprobar si nuestro "servidor" esta funcionando perfectamente, entrando desde el navegador a la dirección **locallhost**

Para reiniciar

sudo /opt/lampp/lampp restart

Para detener

sudo /opt/lampp/lampp stop

En caso les aparezca el error *"***XAMPP is currently only availably as 32 bit application. Please use a 32 bit compatibility library for your system. "**

Tendrán que instalar la librería ia32-libs en el caso de Ubuntu/Debian.

En resumen esto permite que los códigos de 32-bit puedan ejecutarse en una máquina de 64-bit.

sudo apt-get install ia32-libs

Configuración extra

En el caso que no queramos entrar directamente la carpeta **/opt/lampp/htdocs** para agregar un nuevo archivos para que lo corra en el servidor, podemos crear un enlace a lo que es nuestra carpeta personal, con esto ya tenemos nuestros proyectos más accesibles con este comando:

sudo ln -s /opt/lampp/htdocs /home/usuario/Webs

Crear una interfaz gráfica que va trabajar como un panel de control para iniciar y detener los servicios uno por uno, que para mi opinión es mucho más practico ejecutar una línea de comando que esto.

Llamamos al panel:

sudo /opt/lampp/share/xampp-control-panel/xampp-control-panel

Instalamos la siguiente libreria por si nos encontramos con el error "Error importing pygtk2 and pygtk2-libglade"

sudo apt-get install python-glade2

Creamos un archivo desktop para que nos salga en el menú de aplicaciones

sudo gedit /usr/share/applications/xampp-control-panel.desktop

Le agregamos las siguientes configuraciones

[Desktop Entry]

Comment=Start/Stop XAMPP

Name=XAMPP Control Panel

Exec=gksudo python /opt/lampp/share/xampp-control-panel/xampp-control-panel.py

Icon[en_CA]=/opt/lampp/xampp.png

Encoding=UTF-8

Terminal=false

Name[en_CA]=XAMPP Control Panel

Comment[en_CA]=Start/Stop XAMPP

Type=Application

Icon=/opt/lampp/xampp.png

Guardar y cerrar.

CONFIGURACION DE FIREWALL

Ahora podemos empezar a añadir los servicios seleccionados en nuestro filtro de cortafuegos. La primera tal cosa es una interfaz localhost:

iptables -A INPUT -i lo -j ACCEPT

Le decimos a iptables para agregar (-A) una regla a la (INPUT) tabla de filtros de entrada cualquier tráfico que viene a localhost interfaz (-i lo) y aceptar (-j ACCEPT) de ella. Localhost se utiliza a menudo para, por

ejemplo. Su sitio web o correo electrónico del servidor de comunicación con una base de datos instalada localmente. De esta forma nuestra VPS puede utilizar la base de datos, pero la base de datos está cerrada a las hazañas de internet.
Ahora podemos permitir que el tráfico del servidor web:

```
iptables -A INPUT -p tcp -m tcp --dport 80 -j ACCEPT
iptables -A INPUT -p tcp -m tcp --dport 443 -j ACCEPT
```

Hemos añadido los dos puertos (http puerto 80 , y https puerto 443) a la cadena de ACCEPT - permitir el tráfico en en esos puertos . Ahora, vamos a permitir que los usuarios utilizan nuestros servidores SMTP :

```
iptables -A INPUT -p tcp -m tcp --dport 25 -j ACCEPT
iptables -A INPUT -p tcp -m tcp --dport 465 -j ACCEPT
```

Como se dijo antes, si podemos influir en nuestros usuarios , deberíamos más bien utilizar la versión segura , pero a menudo no podemos dictar los términos y los clientes a conectarse utilizando el puerto 25 , que es mucho más fácil tener contraseñas olfatearon de . Ahora procedemos a permitir a los usuarios leer el correo electrónico en su servidor:

iptables -A INPUT -p tcp -m tcp --dport 110 -j ACCEPTiptables -A INPUT -p tcp -m tcp --dport 995 -j ACCEPT

Esas dos reglas permitirán que el tráfico POP3. Una vez más, se podría aumentar la seguridad de nuestro servidor de correo electrónico con sólo usar la versión segura del servicio. Ahora también tenemos que permitir que el protocolo de correo IMAP:

```
iptables -A INPUT -p tcp -m tcp --dport 143 -j ACCEPT
iptables -A INPUT -p tcp -m tcp --dport 993 -j ACCEPT
```

CASO PRÁCTICO

Asignatura: SISTEMAS OPERATIVOS III

Egresada: Diana Pinta

Caso:

Instalar y Configurar servicios de red para una empresa que necesita llevar los siguientes controles Entregables:

- Esquema lógico de red
- Esquema de seguridad de la red
- Determinar la cantidad de servidores con los servicios para mejorar el nivel de procesamiento de la información.
- Se necesita un correo institucional bajo un dominio configurado con su propio servidor (el servicio de correo debe controlar que los correos internos puedan ser enviados con certificados de firmas electrónicas, controlar los SPAM).
- La empresa tiene 3 ips públicas.
- La empresa necesita que 50 usuarios tengan acceso a internet a través de un proxy quien debe restringir el acceso de páginas prohibidas, páginas que consuman mucho de banda, asignación de ancho de banda, llevar un control para acceso por autenticación.
- La empresa tiene 3 sucursales cada una tiene diferente ip de red y debe existir comunicación entre todas las sucursales
- La empresa necesita configurar 2 firewall uno para la LAN y otro para la WAN
- La empresa tiene un sistema web y una base de datos relacional, debe configurar en Linux para que pueda funcionar el sistema (controlar que solo la intranet tenga acceso al sistema web).
- La empresa necesita configurar un servidor DHCP para asignación automática de elementos de red (controlando la asignación con la dirección física MAC), la asignación debe ser a todas las sucursales.
- La empresa necesita compartir recursos (controlar que el acceso sea mediante autenticación).

Docente: Rivas Asanza Wilmer Braulio