compAs

GUÍA DE PRÁCTICAS EN ENDIAN

Ing. Alfonso Guijarro Rodríguez, Mgs.
MSc. Jorge Tapia Celi
MSc. Xavier Viteri Guevara
MSc. Jorge Zambrano Santana.

GUÍA DE PRÁCTICAS EN ENDIAN

Autores:

Ing. Alfonso Guijarro Rodríguez, Mgs.
MSc. Jorge Tapia Celi
MSc. Xavier Viteri Guevara
MSc. Jorge Zambrano Santana.

GUÍA DE PRÁCTICAS EN ENDIAN

Autores

Ing. Alfonso Guijarro Rodríguez, Mgs.
MSc. Jorge Tapia Celi
MSc. Xavier Viteri Guevara
MSc. Jorge Zambrano Santana.

Primera edición: enero 2018

Diseño de portada y diagramación:
Grupo Compás
Equipo Editorial
ISBN: 978-9942-770-36-3

INTRODUCCIÓN

Asignaturas como, Seguridad Informática, Administración de Centros de Cómputo, Redes de Computadoras, en su afán de dar cumplimiento a la parte práctica, elaboran talleres desarrollados por estudiantes, con la finalidad de desarrollar la praxis, generando confianza sobre la recreación de soluciones. En este apartado se tratará de instalar varios servicios de manera virtual con ayuda de vmware.

Los temas abordados en este manual corresponden como sigue:

Instalación de endian y http.- Explicación de los requisitos mínimos para instalar el producto Endian, así como la instalación paso a paso, habitación de un primer servicio http desde una maquina cliente.

Firewall y Proxy.- Se mostrara el paso a paso, de cómo crear un proxy, reglas básicas de firewall, en Endian, las diferentes redes en una máquina con sistema operativo CentOS.

Correo, Dns, Antispan.- Se mostrara los requisitos, para la instalación de cada servicio, así como también se explicara de una manera detallada su instalación y configuración para el perfecto funcionamiento de los mismo en un maquina con sistema operativo Centos.

Ftp y Samba.- Se mostrar paso a paso como instalar el protocolo de red para la transferencia de archivos entre las maquinas en red creadas, se probara conectar a un servidor para descargar archivos desde él o para enviarle archivos. También se instalará el protocolo Server Message Block (SMB) para permitir la interconexión de redes Microsoft Windows, Linux, UNIX y otros sistemas operativos juntos en este caso centos con Windows, permitiendo el acceso a archivos.

Índice de Contenido

Índice de Figuras

GLOSARIO DE TÉRMINOS

ACL	Access Control List
ARP	Address Resolution Protocol
CPU	Central Processor Unit
DDoS	Distributed Denial of Service
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
DNS	Domain Name System
DoS	Denial of Service
DTE	Data Terminal Equipment
FTP	File Transfer Protocol
GB	Gigabyte
GE	GigaEthernet
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICMP	Internet Control Message Protocol
IP	Internet Protocol
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security
LAN	Local Area Network
MAC	Media Access Control
MB	Megabyte
NAT	Network Address Translator
NIC	Network Interface Card
NMAP	Network Mapper
PC	Personal Computer
POP3	Post Office Protocol

PSK	Pre-shared Key
PSTN	Public Switched Telephone Network
RAM	Random Access Memory
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management
SPAM	Stupid Pointless Annoying Messages
URL	Uniform Resource Locator
UTM	Unified Threat Management
VLAN	Virtual LAN
VPN	Virtual Private Network
WAN	Wide Area Network
WiFi	Wireless Fidelity
WWW	World Wide Web

PRÁCTICA I: INSTALACIÓN Y CONFIGURACIÓN BÁSICA DE ENDIAN

En esta práctica se procederá con la instalación de Endian Firewall, y se realizarán configuraciones básicas para poder administralo.

ENDIAN

Endian es una distribución OpenSource de Linux, desarrolla para actuar como cortafuego (firewall), es común pensar que Endian solo es un firewall, pero Endian es toda una solución integral que protege su red, Endian ofrece todos los servicios que brinda un UTM. (Endian, 2009).

Funciona como proxy, canales VPN, enrutador, antivirus y filtrado de datos, anti spam entre otras. Es bastante fácil de administrar y de instalar.

ESQUEMA DE RED A IMPLEMENTAR

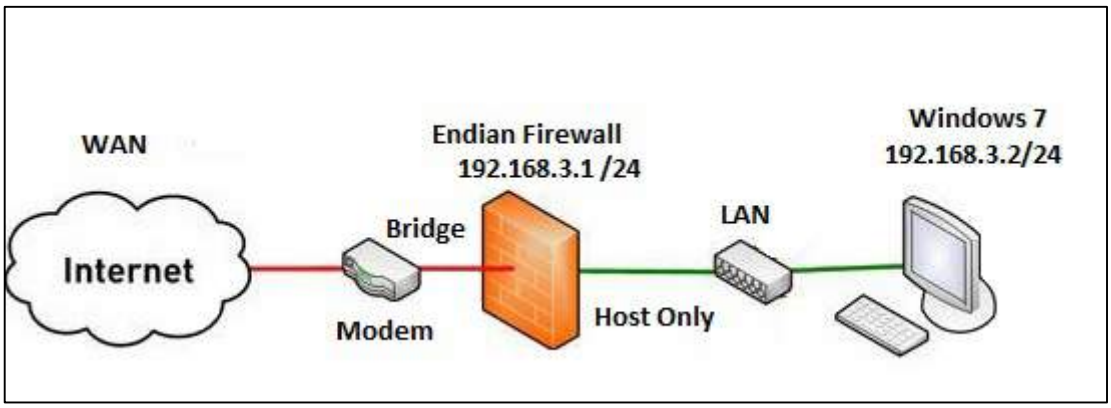


Figura 1. Diagrama de Red de Endian

En este escenario se encuentra la forma de cómo realizar la instalación completa de Endian Firewall, así como los requisitos necesarios para su correcto funcionamiento y su configuración básica la cual se realiza paso a paso, de esta manera se pretende dejar preparado el ambiente para poder seguir con las prácticas que corresponden a la configuración de Proxy y firewall.

REQUERIMIENTOS PARA LA PRÁCTICA

- La dirección de internet debe ser pública (DHCP)
- La dirección de LAN debe ser privada

- La puerta de enlace será el firewall Endian
- Dar acceso a Internet a todos los usuarios de la pequeña LAN, haciendo NAT.
- Denegar el acceso del tráfico desde la red WAN hacia la red LAN.
- Verificar Requisitos mínimos
- Bajar de la página oficial la imagen iso http://www.endian.com/community/download/
- VMWare para virtualización - maquina física con procesador de 3 núcleos (mínimo), 3 gb de RAM (mínimo).

GUÍA DE INSTALACIÓN DE ENDIAN

Antes de instalar Endian necesitamos realizar algunos pasos previos a la instalación los cuales son los siguientes:

REQUISITOS MÍNIMOS IMPLEMENTADOS PARA INSTALACIÓN DE ENDIAN

Requisitos del sistema / Soporte para Hardware

*** CPU:**

Intel x86 compatible (500MHz mínimo, 1GHz recomendado), incluyendo VIA, AMD Athlon, Athlon 64, Opteron, Intel Core 2 Duo, Xeon, procesadores Pentium y Celeron

*** Procesador múltiple:**

Soporte incluido para Multiprocesador simétrico (SMP)

*** RAM:**

256MB mínimo (512MB recomendados)

*** Discos:**

Discos SCSI, SATA, SAS o IDE requeridos (8GB mínimo)

*** Software RAID:**

Para software RAID1 (mirroring) dos discos del mismo tipo (las capacidades no deben ser iguales) son requeridos.

*** CDROM:**

Un dispositivo IDE, SCSI o USB CDROM es requerido para la instalación (no es necesario después de la instalación)

*** Tarjetas de Red:**

Las tarjetas de red interfaz más populares tienen soporte incluyendo Gigabit y NIC fibra

*** Monitor/teclado:**

Sólo necesarios para la instalación, pero no para la configuración y el uso

*** Sistema operativo:**

Endian Firewall incluye el sistema operativo basado en Hardened Linux

INSTALACIÓN

Ejecutar Vmware (ver instalacion de VMWare en anexo A) y comenzar el asistente para la creación de la máquina virtual como se aprecia en la figura 2 , escoger la opción Typical para crear la maquina con opciones preestablecidas de wmware o Custon si por el contrario somos nosotros quienes configuremos esas opciones para esta practica se escojera typical, dar clic en siguiente.

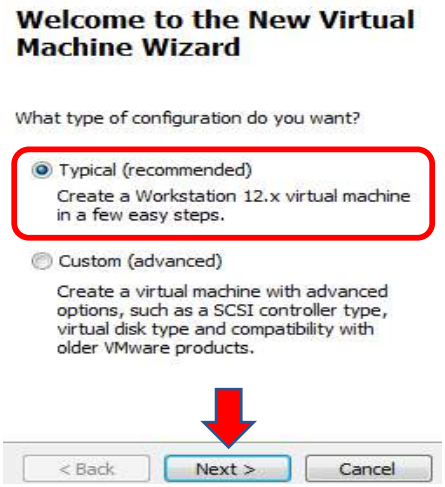


Figura 2. Creación de máquina virtual mediante VMWare.

En la figura 3 se indica la forma de cargar el instalador de la cual se escogerá una de las 3 opciones.

Installer disc: si se instalará desde un disco físico.

Installer disc image file (iso): si se instalara desde una imagen ISO.

I will install the operating syste, later: indicando que más adelante se cargará la ISO

Para la práctica se elige la tercera opción y se procede a dar clic en siguiente.

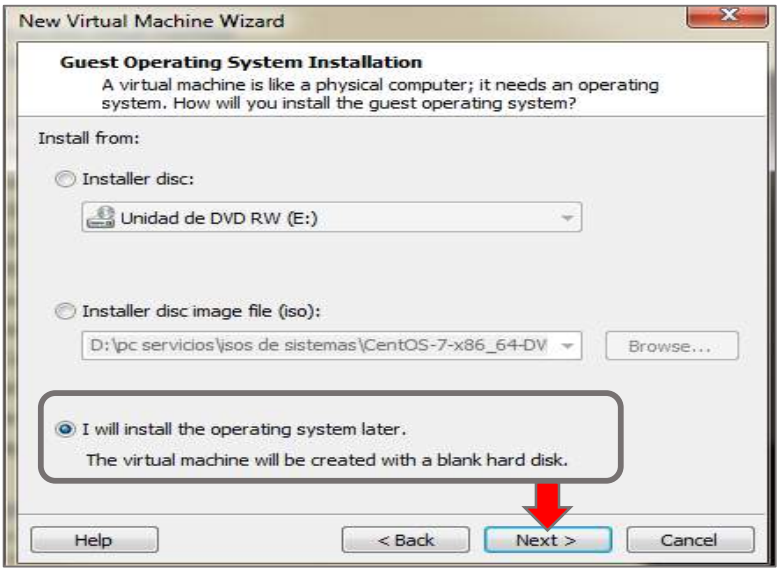
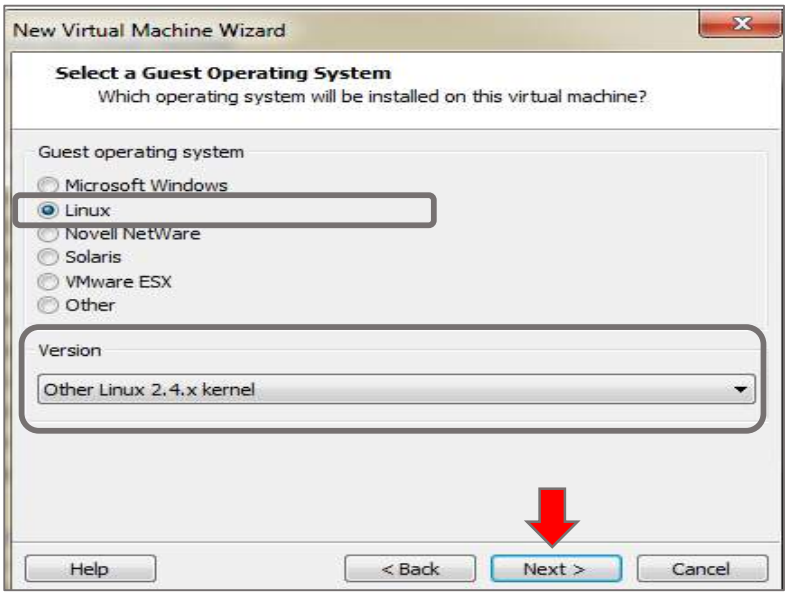


Figura 3 Carga de la ISO de Endian

Como se aprecia en la figura 4 se selecciona el sistema operativo a instalar, en este caso se escoge Linux. Todas las distribuciones de Linux vienen con un Kernel o Núcleo integrado el kernel para que Endian funcione correctamente es other Linux 2.4.x kernel. clic en siguiente.



.

Figura 4 Selección de Linux para su instalación.

En la figura 5 muestra la pantalla donde se colocará el nombre que se desee para la máquina virtual y la locación, es recomendable dejarla como está, pero si prefiere puede elegir la ruta de su preferencia. Clic en siguiente.

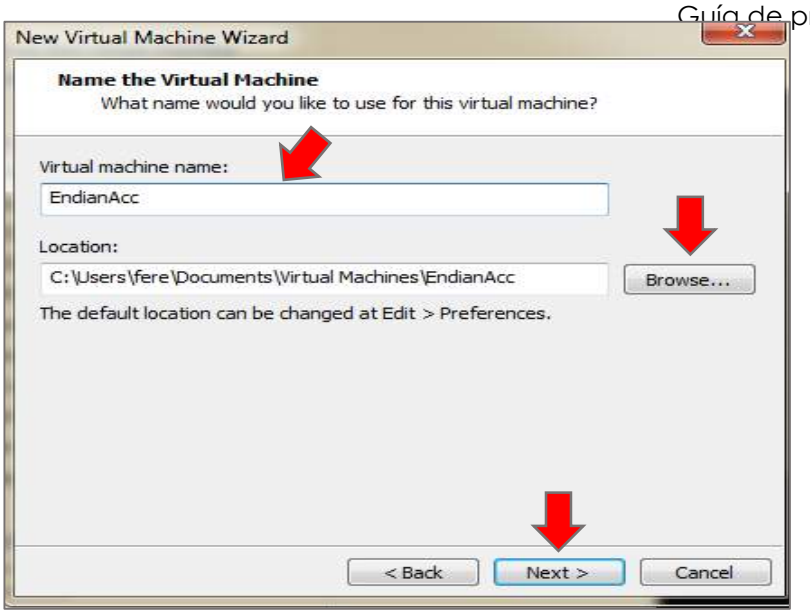


Figura 5 Asignarle nombre a nuestra máquina Virtual.

La figura 6 muestra la opción de asignarle un tamaño de disco, como mínimo se definirá el tamaño del disco duro en 8 gb, porque la red en la que trabajaremos las practicas solo contará con 4 máquinas virtuales, Clic en siguiente.

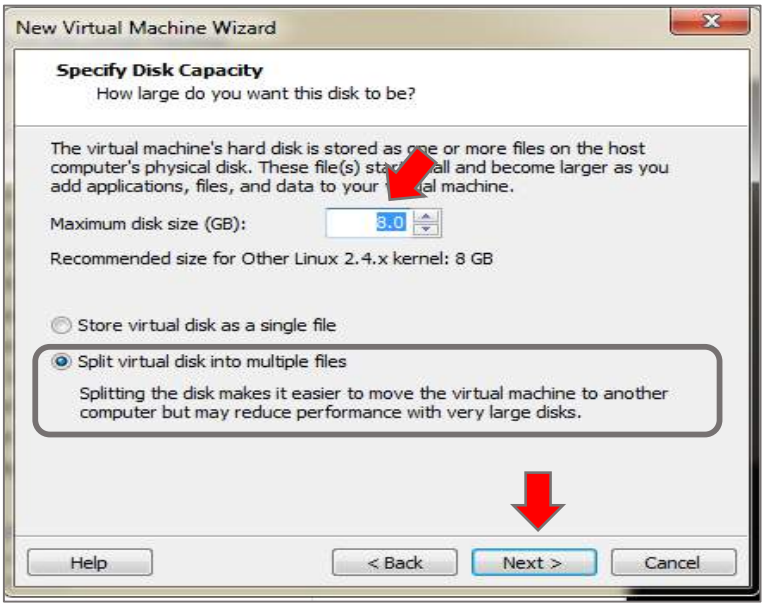


Figura 6. Definir el tamaño del disco duro que ocupará nuestra máquina virtual.

La figura 7 muestra la configuración seleccionada anteriormente para la máquina virtual a instalar, Antes de finalizar hacemos click en la opción customize hardware, aquí nos permitirá personalizar la configuración del hardware.

Importante: Las características a seleccionar no deben ser igual o sobrepasar las características de la maquina anfitrión.

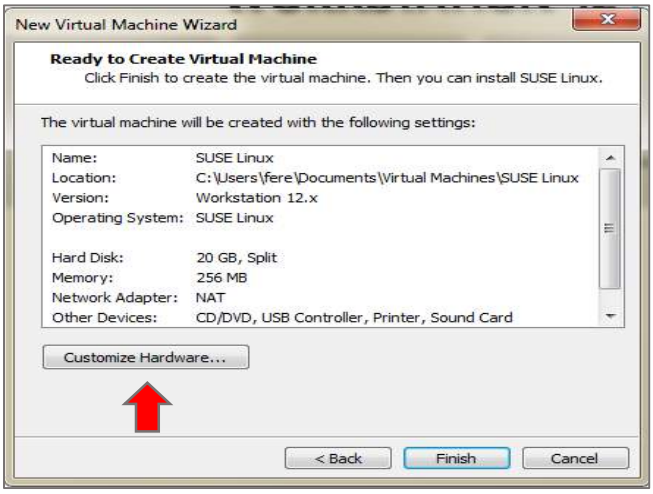


Figura 7. Personalización del Hardware de la máquina virtual.

La figura 8 muestra cómo se añade otra tarjeta de red, dando clic en add y seleccionando network adapter y next.

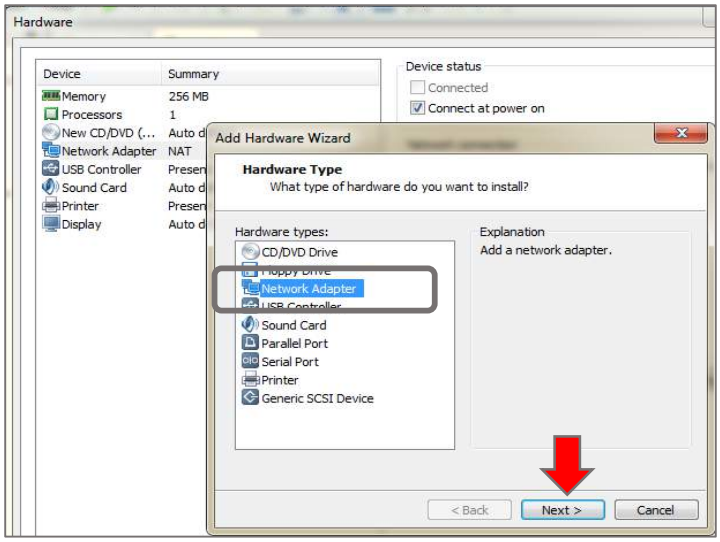


Figura 8. Añadir una tarjeta de red adicional.

Se definirá la network como bridged y luego dar clic en la opción Finish. Como muestra la figura 9.

Características de cada network

- **Adaptador puente (Bridge):** en este modo, se crea una tarjeta de red virtual en el anfitrión que intercepta el tráfico de red y puede inyectar paquetes en la red, de manera que el huésped se configura como si estuviera conectado por un cable a la tarjeta de red virtual del anfitrión.

- **NAT:** NAT Es el modo por defecto de la tarjeta de red virtual. Este modo permite al huésped navegar por Internet, descargar ficheros y leer el correo electrónico sin necesidad de configurar el sistema operativo huésped.

- **Red Interna**: en este modo, se crea una red virtual visible entre las máquinas virtuales, pero invisible al anfitrión o a máquinas externas a la red.

- **Adaptador Sólo-Anfitrión**: en este modo se crea una tarjeta de red virtual en el anfitrión que puede conectarse con las máquinas virtuales sin necesitar que el anfitrión tenga una tarjeta de red.

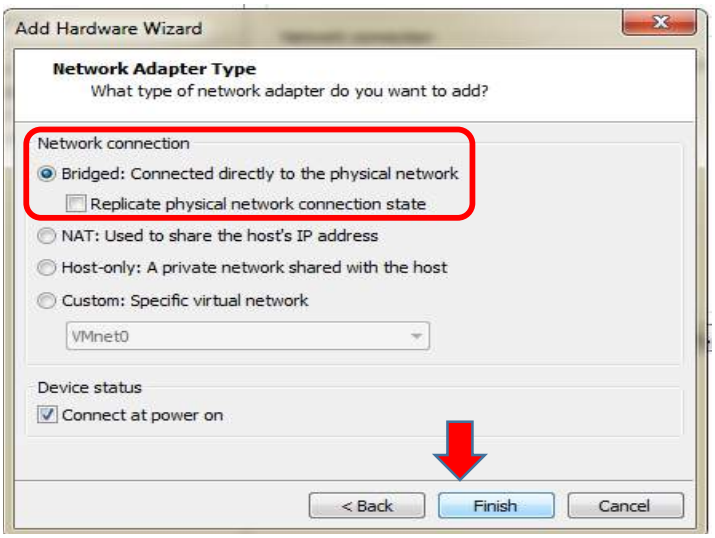


Figura 9. Definir la tarjeta de red como Bridged

Modificar la otra tarjeta de red seleccionándola y escogiendo la opción host-only como muestra la figura 10.

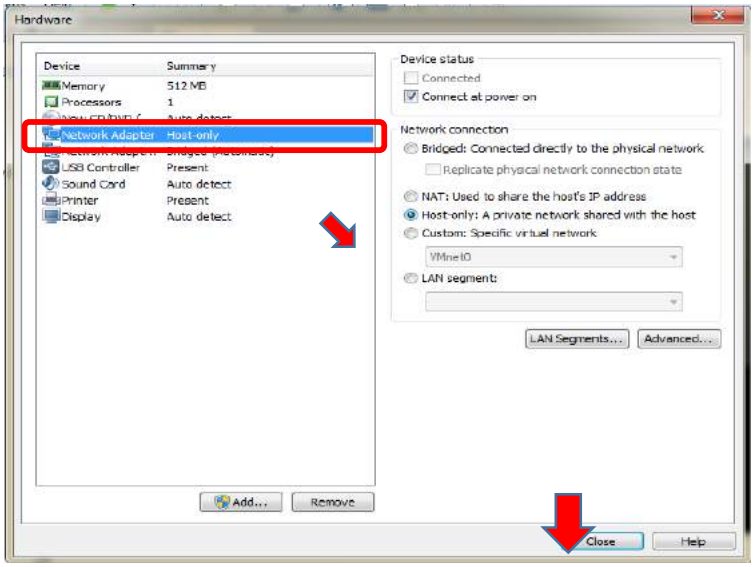


Figura 10. A nuestra tarjeta de red principal la pondremos como Host-only.

La figura 11 mustra como se Selecciona la iso a instalar , dando clic en la opción cd/ dvd, y seleccionando la opción use ISO physical drive, seguido escoger la iso de su ubicación correspondiente con browser.

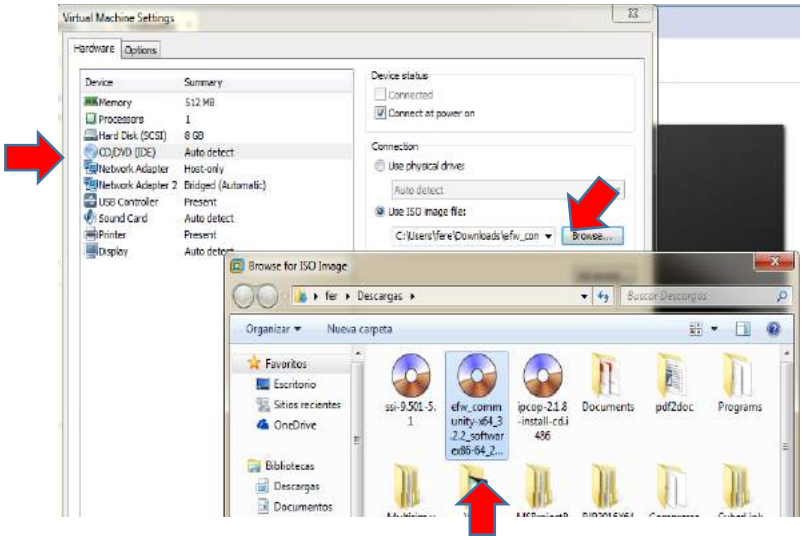


Figura 11. Elegiremos la ISO correspondiente con nuestro browser

Ya completada la configuración de hardware, finalizar con finish. Inicializar la máquina virtual creada , esperar que cargue la iso y la pantalla de instalación.

Como primer punto escoger el idioma como lo muestra la imagen 12, en este caso inglés y presionar el botón enter.

Figura 12. Escogemos idioma

Aquí aparece una advertencia, que dice que la instalación borrara todos los datos que contenga el disco duro y si queremos continuar la instalación, seleccionamos **NO.**

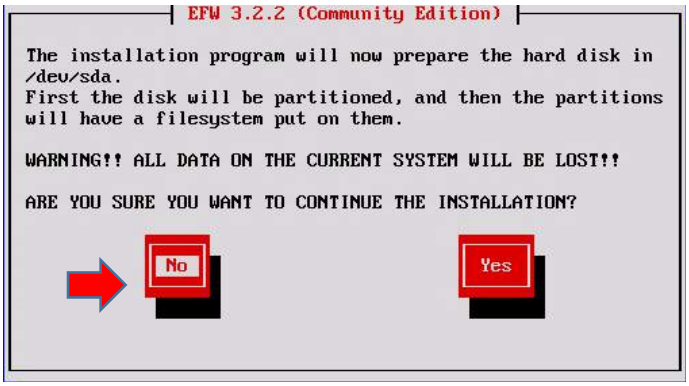


Figura 13. **Borramos los datos que contenga nuestro disco duro.**

En la figura 14 muestra la ventana que pregunta si se desea activar el servicio de consola, dar Enter en **NO**.

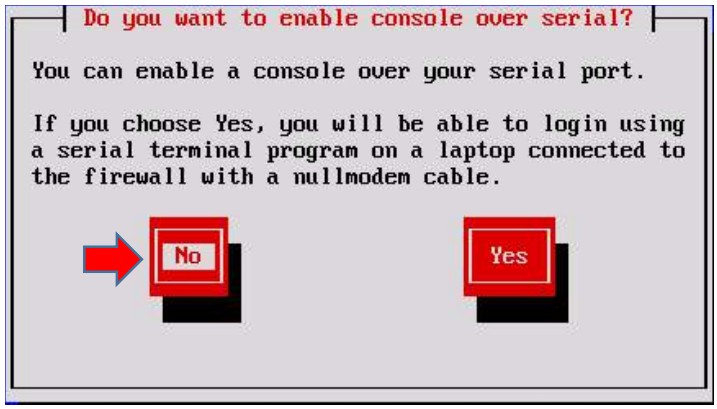


Figura 14. No activamos el servicio de consola

Luego de la instalación, aparece una pantalla (figura 15) en la cual se deberá configurar la dirección IP de la interfaz de red local (verde) la cual permitirá la configuración y administración a través de un navegador web. Click en ok .

Figura 15. Configuramos nuestra IP local (verde).

NOTA: Recordemos que el Gateway, debe ser en función de la topología de red LAN.

En la Figura 16 indica que ya está instalado el programa y las URL para acceder por medio del browser y seguir realizando las configuraciones necesarias, damos Ok.

Figura 16. Programa instalado con éxito, presionamos OK.

Y esta es la pantalla final figura 17 donde se ingresará al terminal para administrar y configurar algunas herramientas de Endian.

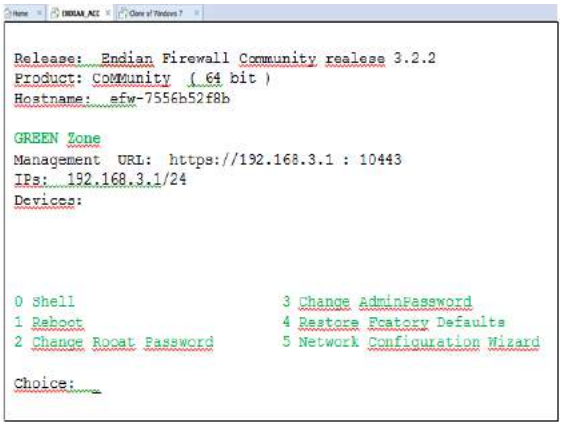


Figura 17. Pantalla mediante la cual se podrá acceder a la terminal de Endian.

ADMINISTRACIÓN DEL FIREWALL ENDIAN DESDE UN CLIENTE AUTORIZADO.

En una máquina virtual que va a ser integrante de nuestra red interna configurar su Ip estática autorizada (192.168.3.2) en relación con a la misma red en que se configuró el firewall Endian. Mascara subred igual al del firewall 255.255.255.0 Y nuestra puerta de enlace será el firewall Endian 192.168.3.1 como lo muestra la figura 18. Los DNS serán los de Google 8.8.8.8 y alternativo 4.4.4.4 ya que estos servidores DNS están especialmente optimizados para proteger frente al phishing, malware y todo tipo de las amenazas para la seguridad o la privacidad de los datos.

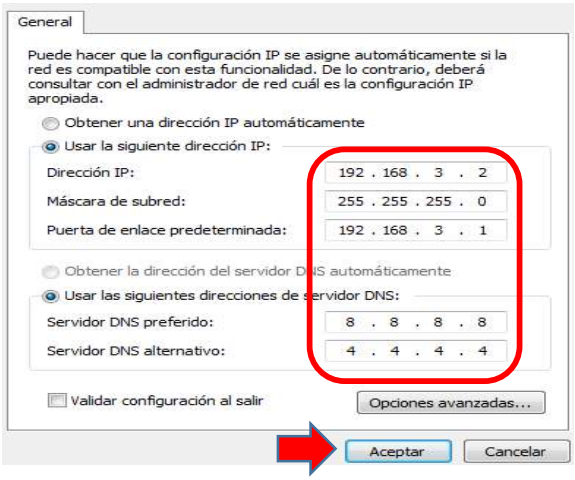


Figura 18. Configuramos nuestra IP estática.

Una vez cargado Endian se accederá desde una máquina perteneciente a la red LAN (ejemplo la IP 192.168.3.2) al entorno gráfico de administración mediante un navegador web; digitar la dirección IP que fue asignada al servidor Endian. Como muestra la figura 19.

https://192.168.3.1:10443/

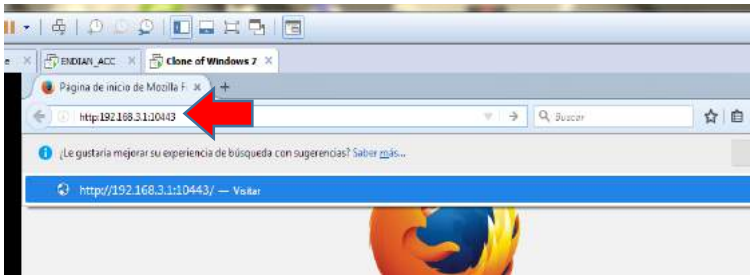


Figura 19. Accedemos a Endian mediante su entorno gráfico en la Web.

Aparecerá que la conexión no es segura, esto se debe a que cuando IE se conecta a una página segura (es decir, la URL empieza por "https://"), debe comprobar que el certificado que proporciona la página es válido y que la encriptación es lo suficientemente fuerte para que proteja la privacidad de forma adecuada. Si el certificado no se puede validar o la encriptación es débil, IE interrumpirá la conexión con la página y te mostrará dicho mensaje, teniendo que añadirla como excepción de seguridad para poder continuar.

Figura 20. Conexión No segura

Añadir la excepción de Seguridad como muestra la figura 21.

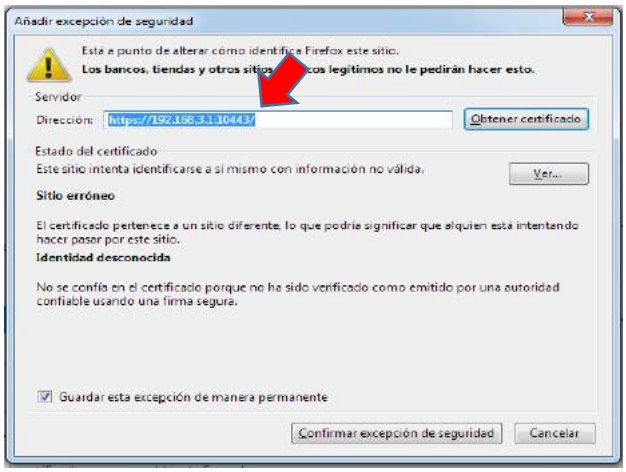


Figura 21. Añadir excepción de seguridad en el navegador.

Una vez añadida la excepción se podrá acceder al administrador de Endian como lo muestra la figura 22.

Figura 22. Mensaje de bienvenida de Endian Firewall

Seleccionar el idioma y la zona horaria correspondiente a su criterio. Como se aprecia en la figura 23.

Seguido aceptamos el acuerdo de licencia.

Figura 23. Escogemos idioma y zona horaria.

Como es la primera vez que se instala Endian no se tiene Backup por lo tanto se debe escoger la opción **NO**. en caso de tener un backup seleccionar **SI** y luego clic en >**>>**.como se aprecia en la figura 24.

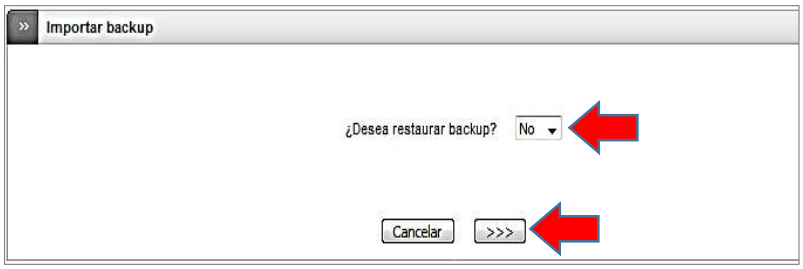


Figura 24 Opción Importar Kackup

Insertar las contraseñas correspondientes con la seguridad debida tanto para el usuario que nos permite ingresar por la interfaz rafica (Admin) como para el usuario qur nos permite ingresar via ssh (Root).

Figura 25. Asignamos contraseñas.

Acto seguido aparecerá el asistente de configuración de red, donde elegiremos el enrutamiento y su correspondiente tipo de enlace que será Ethernet por DHCP es decir dinámico. Como se aprecia en la figura 26.

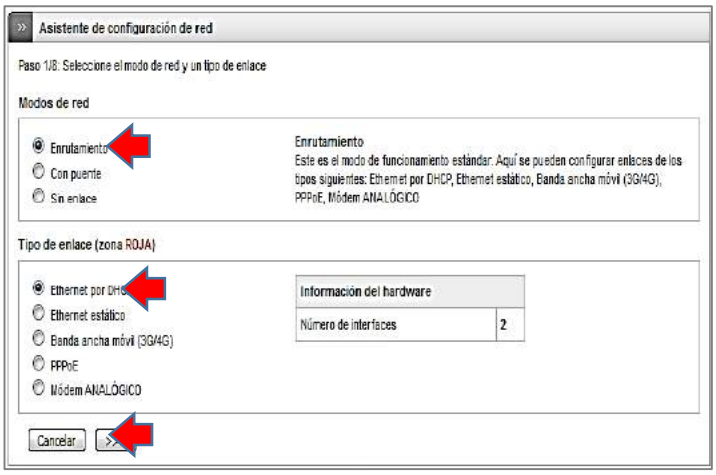


Figura 26. Configuración de red ROJA

Como solo existen dos zonas de red (roja y verde), escoger ninguno. Más adelante si desea añadir servidores tendrá que añadirlos junto con una nueva tarjeta de red para el **Firewall Endian** y proceder a su configuración desde el correspondiente administrador. Como se puede apreciar en la figura 27.

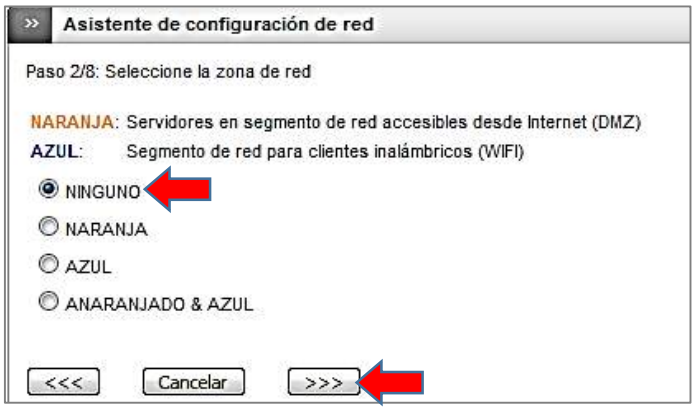


Figura 27. Configuración de red NARANJA

La zona verde será la red privada LAN, donde se podrá cambiar la dirección IP del firewall si se desea, definiendo el nombre de host, dominio. Como lo muestra la

figura 28.

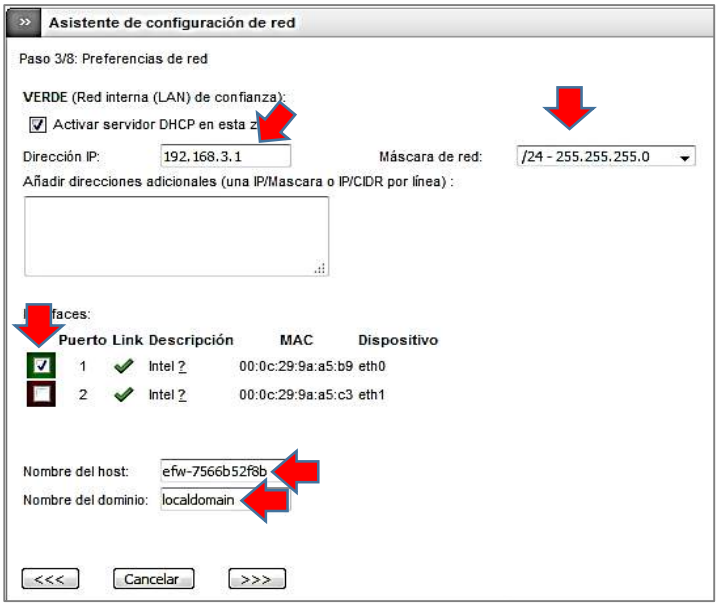


Figura 28. Configuración de red VERDE

La zona roja es la conexión hacia el internet, en esta parte se definirá un DNS manual. Como se ve en la figura 29.

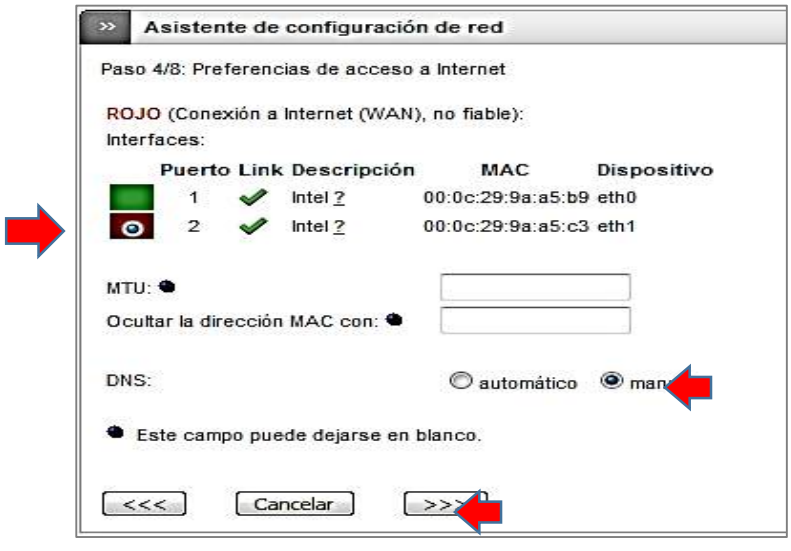


Figura 29. Configuración de red ROJO

Definir el DNS, en caso de no tener servidores DNS propios definir los de Google Como se aprecia en la figura 30, los DNS serán los de Google 8.8.8.8 y alternativo 4.4.4.4 ya que estos servidores DNS están especialmente optimizados para proteger frente al phishing, malware y todo tipo de las amenazas para la seguridad o la privacidad de los datos.

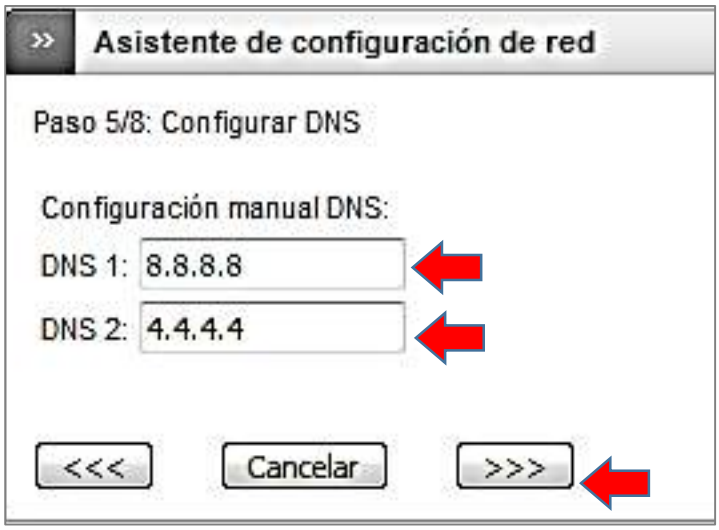


Figura 30. Configuración de DNS.

Configuración de correo electrónico administrativo para notificaciones al administrador. Según figura 31.

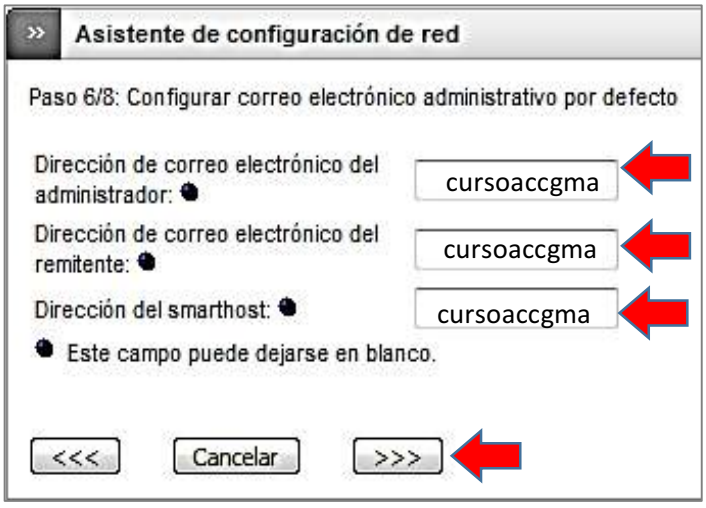


Figura 31. Configuración de Correo Electrónico.

Aceptar y aplicar la configuración.

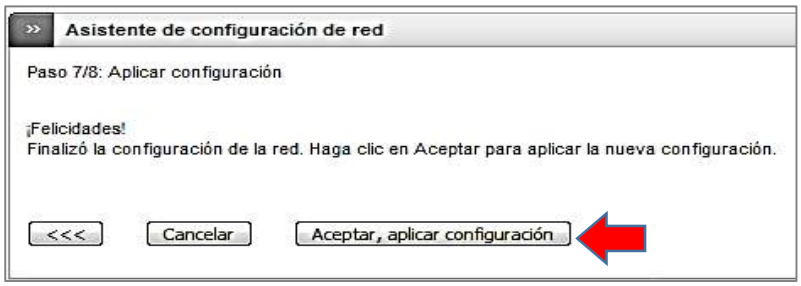


Figura 32. Aceptar y aplicar configuración de red

Finalización del proceso

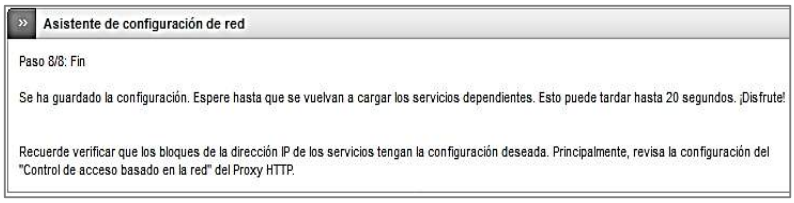


Figura 33. Mensaje de Finalización

La página web se refrescará automáticamente y pedirá ingresar las credenciales de admin para poder seguir editando las diferentes opciones desde la interfaz web con la nueva contraseña y el usuario por defecto "Admin" como se ve en la figura 34.

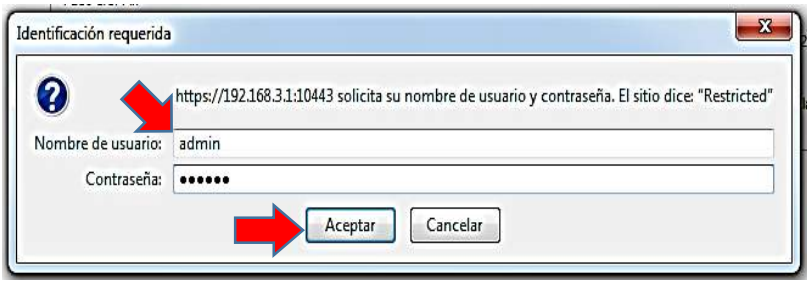


Figura 34. Acceso al administrador de Endian

Y ya se podrá administrar la red, aprovechando una gran variedad de herramientas que provee ENDIAN FIREWALL.

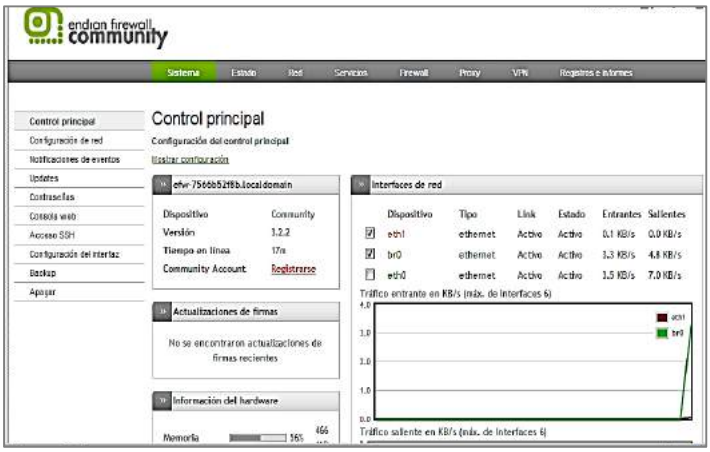


Figura 35. Endian Configurado y listo para usarse.

PRÁCTICA II: INSTALACIÓN DE FIREWALL Y PROXY

En esta práctica se procederá con la implementación de un firewall y un proxy; filtrando así el contenido que aparece en la red mediante mecanismos de filtrado.

FIREWALL

Un firewall es simplemente un filtro que controla todas las comunicaciones que pasan de una red a la otra y en función de lo que sean permite o deniega su paso. Para permitir o denegar una comunicación el firewall examina el tipo de servicio al que corresponde, como pueden ser el web, el correo o el IRC. Dependiendo del servicio el firewall decide si lo permite o no. Además, el firewall examina si la comunicación es entrante o saliente y dependiendo de su dirección puede permitirla o no.

CREACIÓN DE FIREWALL EN LINUX CON ENDIAN

En este escenario se encuentra paso a paso como crear un proxy, crear reglas básicas de firewall desde el Endian entre las diferentes redes en una maquina con sistema operativo Centos. Una vez configurado se procederá a realizar las pruebas de accesos a sitios que estén en la lista blanca y negra y comprobar que las reglas configuradas estén en activas y funcionando correctamente.

La implementación de un firewall basado en una distribución de Linux administrado vía web, da facilidad al momento de implementar las políticas en dicho firewall.

Donde a su vez el firewall contará con 3 redes: LAN, WAN Y DMZ.

- DMZ=Linux (Centos) - ip: 192.168.4.2/24.

- LAN=Windows xp - ip: 192.168.3.2/24 (Administración de Endian Firewall - ip: 92.168.3.1/24).

- WAN= Linux (Ubuntu) - Ip: 192.168.10.132/24.

ESQUEMA DE RED A IMPLEMENTAR

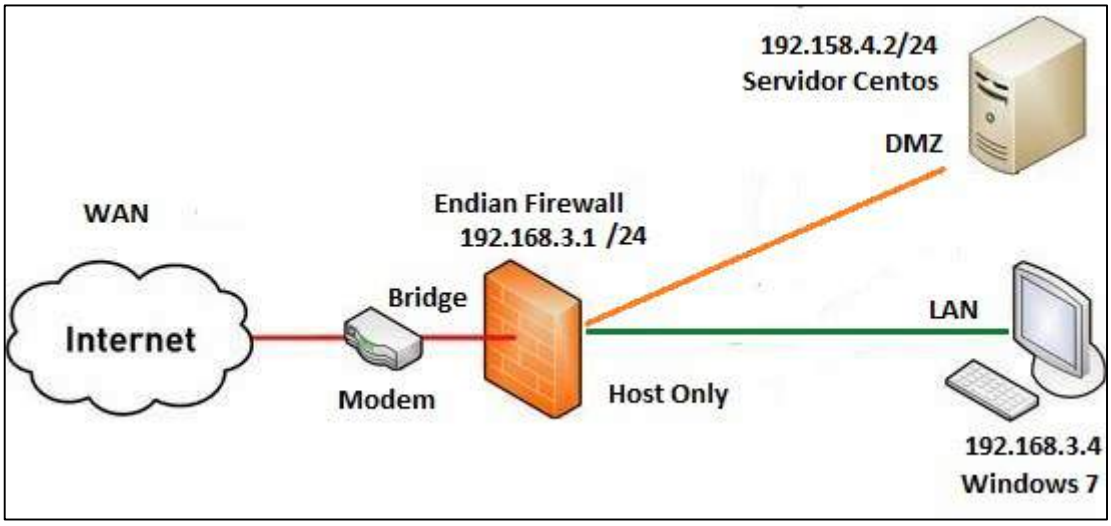


Figura 36. Esquema de red

A continuación, configurar el tipo de conexión que tendrá la interfaz o tarjeta de red que va a estar conectada de cara al internet, en el diagrama de la red se puede observar que se están utilizando 3 adaptadores, la primera está conectada a nuestra LAN (verde) y es la que se configuró anteriormente en la instalación del Endian, la segunda es la que se configurará en este momento (roja) donde se selecciona **ETHERNET ESTÁTICO.** Como se aprecia en la figura 37.

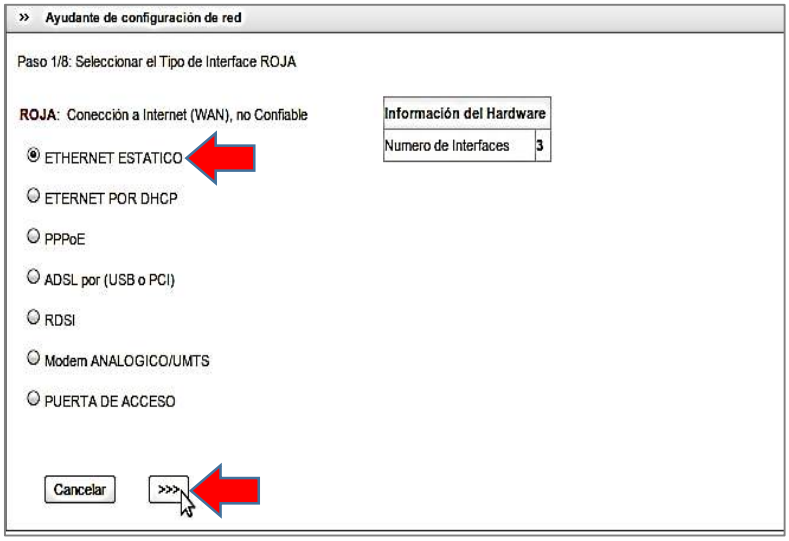


Figura 37. Firewall. Paso 1

En la figura 38 se observa la selección de la interfaz para la zona naranja, donde a su vez se procede a la configuración de la misma zona que es el DMZ.

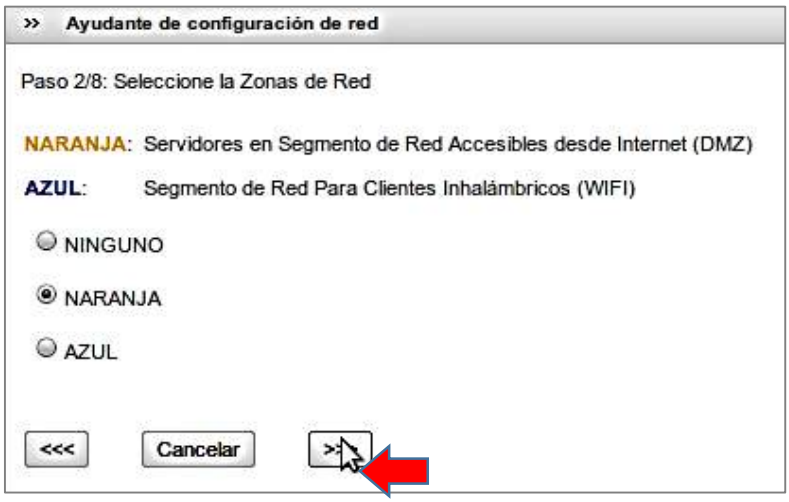


Figura 38. Firewall. Paso 2

En la figura 39 se aprecia la fase de selección se va a configurar la WAN, asignando la dirección IP por donde va a pasar el tráfico de la red y el Gateway.

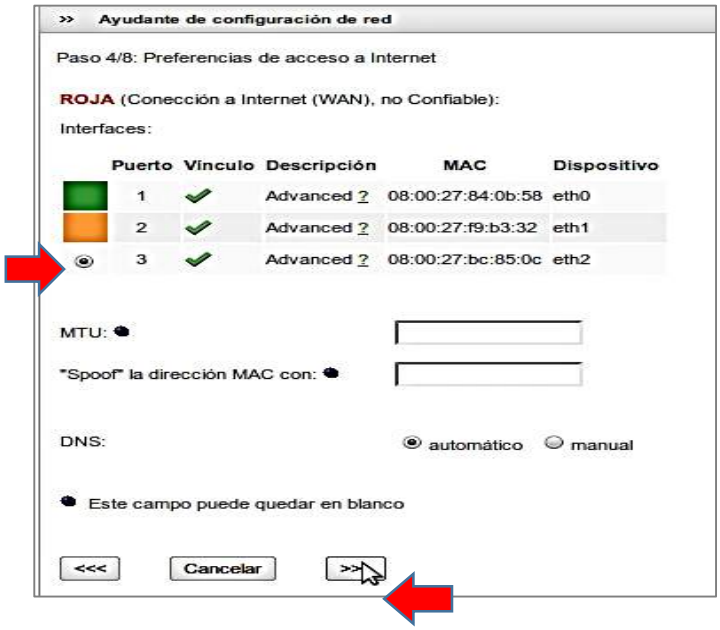


Figura 39. Firewall. Paso 4

En la figura 40 muestra el paso de la configuración del DNS; se lo deja automático por default, luego clic en >>> .

Figura 40. Firewall. Paso 5

En la figura 41 como podemos observar, Endian solicita la información acerca del administrador.

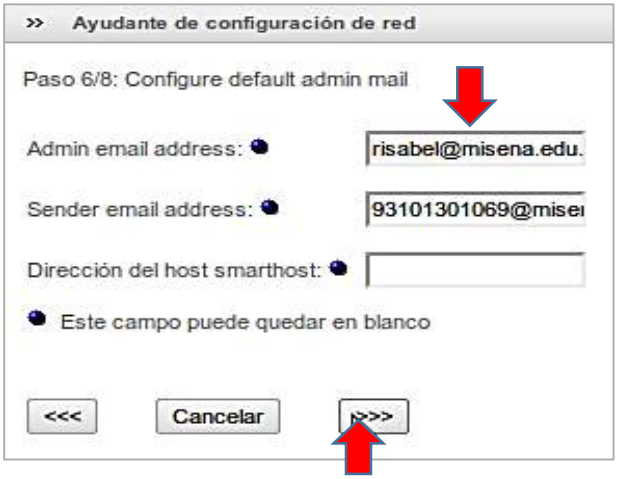


Figura 41. Firewall. Paso 6

En este proceso de instalación observamos que Endian va a aplicar la configuración de la red que ya se encuentra lista, para ello dar clic en Aceptar, aplicar configuración, como se aprecia en la figura 42.

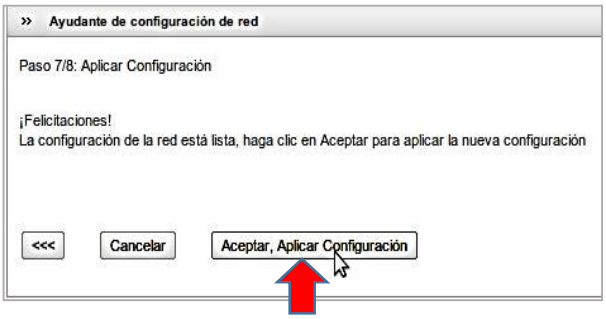


Figura 42. Firewall. Paso 7

Finalmente aparecerá una ventana similar a la de la figura 43 donde indica que el proceso de instalación ha finalizado.

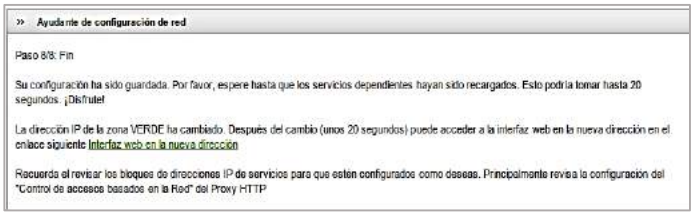


Figura 43. Firewall. Paso 8

CREACIÓN DE UNA REGLA NAT

Se procederá con la Creación de una nueva regla de NAT. Como se observa en la figura 44.

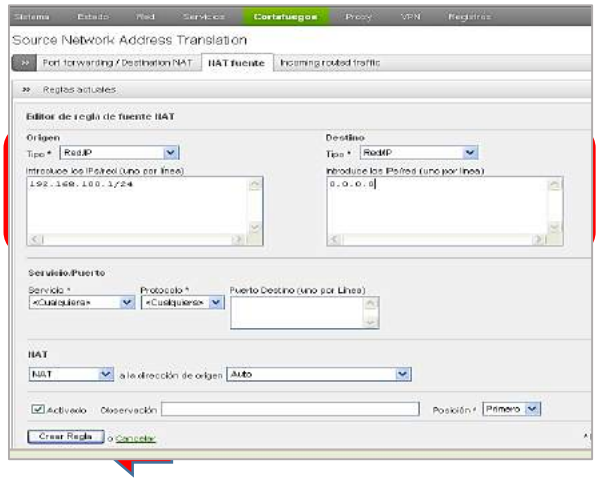


Figura 44. Firewall. Regla NAT

En el panel cortafuegos se configura la regla NAT, esta será creada para dar salida a Internet. Luego en **NAT FUENTE**, proceder a llenar los campos solicitados introduciendo la dirección IP que se usará en la zona verde que es la dirección de origen y destino, y a su vez a la creación de una nueva regla NAT tal como se pude apreciar en la figura 45.

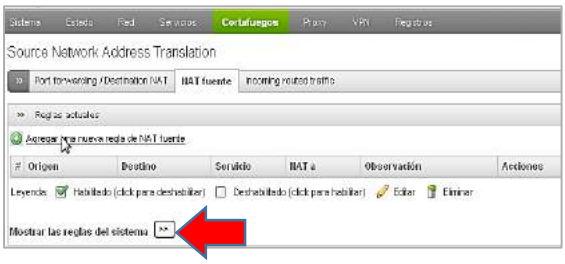


Figura 45. Firewall. Origen-destino

En la figura 46 aparece una alerta mediante un mensaje explicando que "las Reglas de NAT de origen han sido cambiadas y necesitan ser aplicadas para activar los cambios", proceder a dar clic en Aplicar para que se ejecute la función de dicha alerta.

Figura 46. Firewall. Aplicar cambios

Este proceso confirma que la regla NAT ha sido aplicada exitosamente.

Figura 47. Firewall. Confirmación

Para comprobar la Salida a Internet, proceder a realizar un ping en la página web de elección como lo muestra la figura 48.

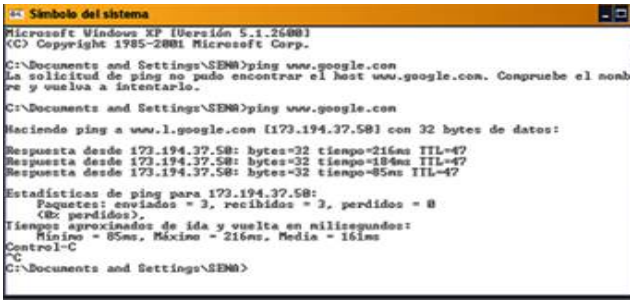


Figura 48. Firewall. Realización del Ping

En el tráfico entre zonas se procede a la configuración de las reglas que permitirá saber cuáles zonas tienen permiso y cuáles no. En este proceso se realizará una regla en donde se puede observar que la zona verde puede comunicarse con la zona naranja. Continuar dando clic en aplicar y guardar, como se observa en la figura 49.

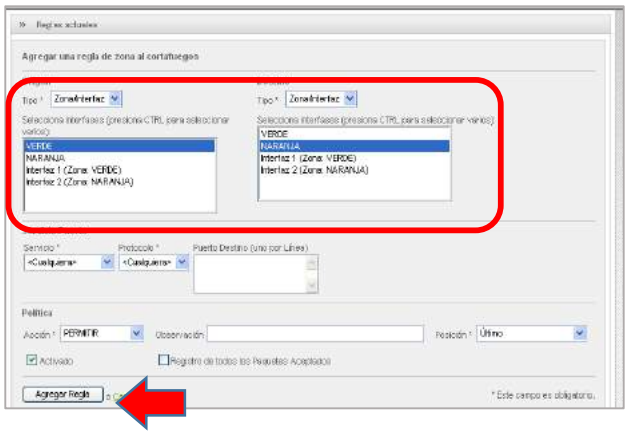


Figura 49. Firewall. Tráfico entre zonas

De la misma manera se deberá colocar otra regla que diga que la zona naranja no se podrá comunicar con la zona verde, Como se aprecia en la figura 50.

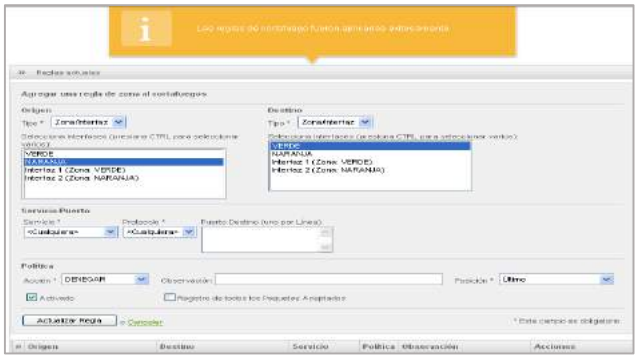


Figura 50. Firewall. Tráfico entre zonas

Ahora se procederá a bloquear el acceso de la zona roja a la zona verde, en donde el tráfico de origen de la zona roja hacia la zona verde se denegará, como se ve en la figura 51.

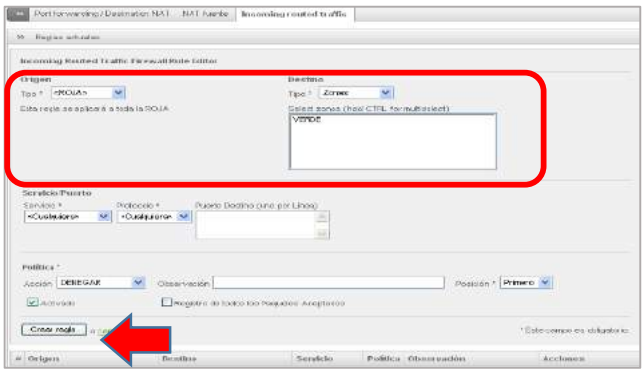


Figura 51. Firewall. Tráfico entre zonas

En la figura 52 aparecen las reglas que fueron añadidas en el proceso, cada una con su origen y su destino correspondiente.

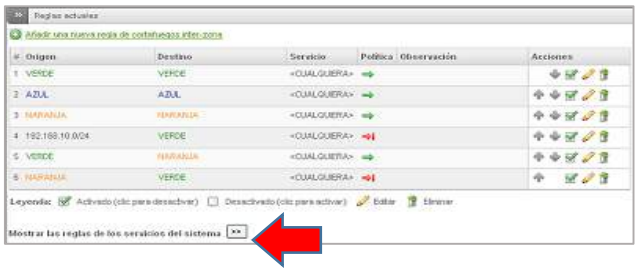


Figura 52. Firewall. Reglas

CONFIGURACIÓN DEL PORT FORWARDING.

Recordar que el Port Forwarding, es abrir los puertos de la red privada para que cualquier usuario externo pueda acceder a un servicio interno y a los datos de un usuario o terminal específico, el destino puede ser un puerto de red predeterminado como se observa en la figura 53.

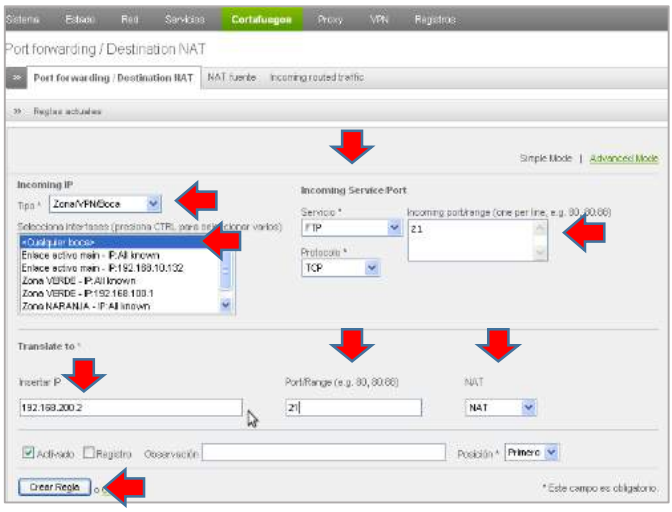


Figura 53. Firewall. Port Forwarding.

CREACIÓN DE PROXY EN LINUX CON ENDIAN

¿QUÉ ES UN PROXY?

Un proxy es un programa o dispositivo que realiza una tarea de acceso a Internet en lugar de otro ordenador, también podemos recalcar que un proxy es un punto intermedio entre un ordenador conectado a Internet y el servidor que está accediendo como lo muestra la *Figura 54*.

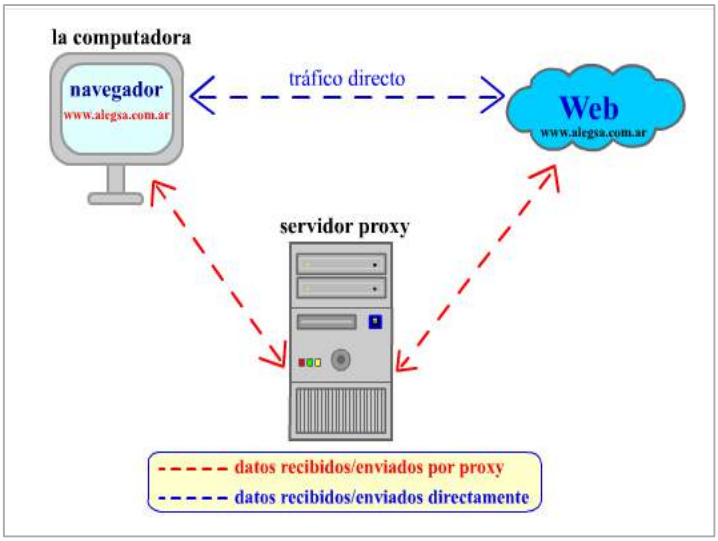


Figura 54. Proxy. Escenario de proxy

A continuación, elegir la opción Proxy que aparecerá en la parte superior de Endian, luego proceder a dar clic en el botón de habilitar Proxy HTTP.

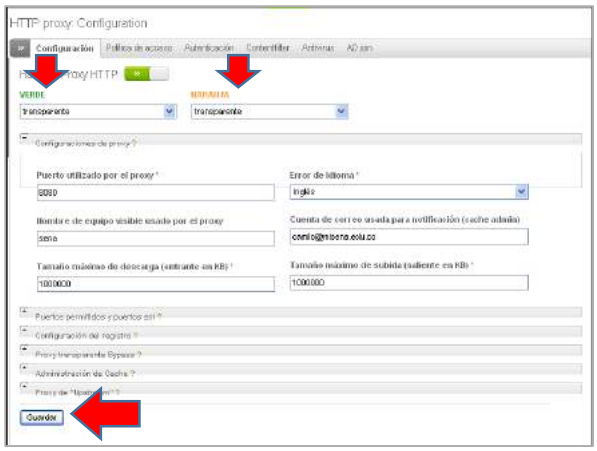


Figura 55. Proxy. Ventana de configuración

En la *figura 56* se puede observar la ventana de puertos, donde se pondrá en modo transparente si se desea que el proxy esté por defecto en el sistema, o No trasparente si se quiere agregar el proxy manualmente en cada browser. También se deberá elegir el puerto por donde correrá el proxy, el

idioma para el despliegue de error, un nombre cualquiera, una dirección de correo cualquiera, y elegir los tamaños de descarga y de subida de archivos.

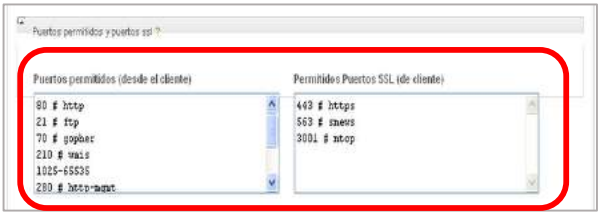


Figura 56. Proxy. Ventana de puertos

En el proceso siguiente habilitar los registros que se vayan a utilizar, como lo muestra la *Figura 57*.

Figura 57. Proxy. Registros

Después ingresar a la administración de Cache, donde se deberá llenar los campos con * que son obligatorios en este proceso, luego habilitar el modo cache fuera de línea. Como se observa en la figura 58.

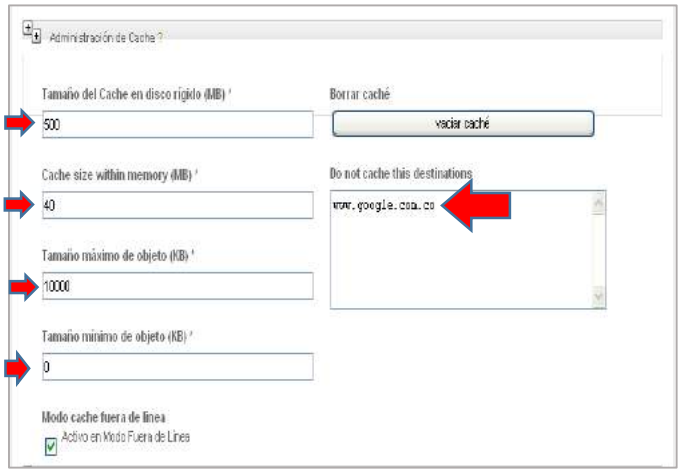


Figura 58. Proxy. Sitio de cache

En la figura 59 se aprecia que aparecerá un mensaje de alerta donde se deberá dar clic en aplicar para así poder guardar los cambios realizados en la configuración del proxy,

Figura 59. Proxy. Aplicación de reglas

Luego de aplicar las reglas guardadas, realizar las restricciones por usuario, ingresando a Contenfilter donde se deberá crear un perfil para definir la autenticación la como se muestra en la figura 60.

Figura 60. Proxy. Creación de Perfil

Proceder a la creación del perfil, ingresando el nombre a nuestra elección.

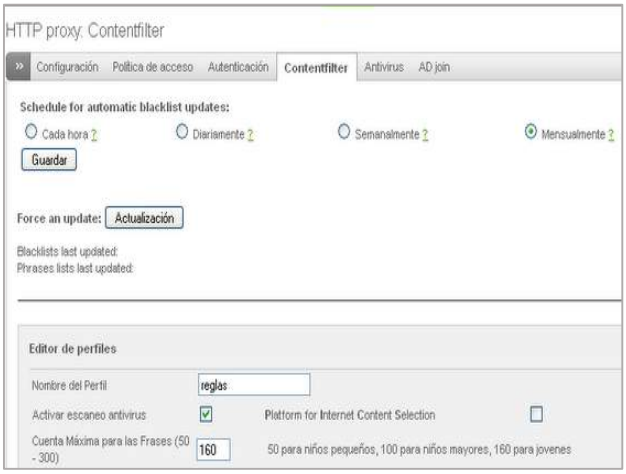


Figura 61. Proxy. Edición de perfil

Luego aparecerá la ventana de listas negras y blancas personalizadas, donde se deben bloquear los sitios web deseados, en este caso YouTube, Hotmail y Facebook, como se puede apreciar en la figura 62.

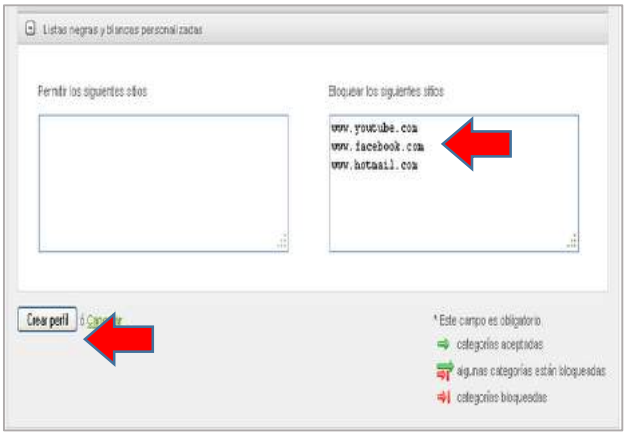


Figura 62. Proxy. Listas negras y blancas

Proceder a Autenticación, donde se elegirá el modo de autenticación a usar como lo muestra la *figura 63*, luego continuar llenando los campos necesarios para después poder dar clic en Guardar.

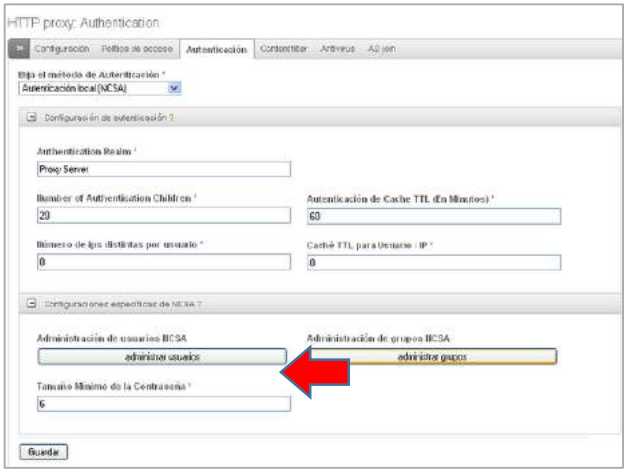


Figura 63. Proxy. Ventana de autenticación

Aparece una ventana como la figura 64, para ahí poder crear el usuario se debe agregar el nombre de usuario y la contraseña correspondiente, luego dar clic en Crear usuario.

Figura 64. Proxy. Creación de usuario

Después se continúa con la creación del grupo donde estará nuestro usuario, para ello se debe volver a Autenticación y dar clic en administrar grupos.

Figura 65. Proxy. Agregar usuario a grupo

A continuación, nos mostrara una venta como en la figura 66, se procede a agregar el nombre del grupo y seleccionar los usuarios pertenecientes al mismo, después se debe ir a Política de acceso para definir a quienes le aplicaremos estas políticas.

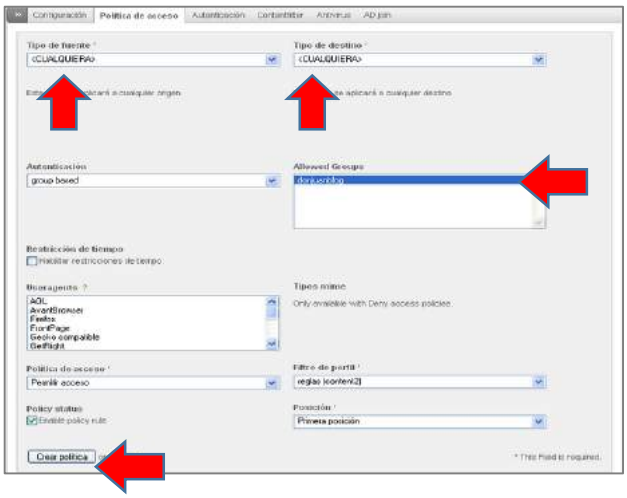


Figura 66. Proxy. Ventana de políticas de acceso.

En autenticación escoger el tipo de fuente y de destino; si se quiere que sea por grupo o por usuario o para cualquiera, en Filtro de perfil buscar el perfil anterior llamado reglas, y le dar clic en crear política tal como se pude observar en la imagen 67.

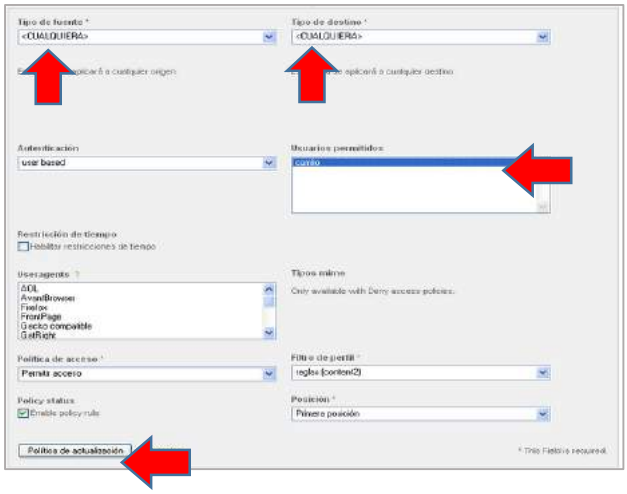


Figura 67. Proxy. Autentificación por grupo o usuario

Como se pude observar en la figura 68 luego de crear la política de acceso aparecerá una alerta de mensaje donde se dará clic en aplicar para así poder guardar los cambios realizados.

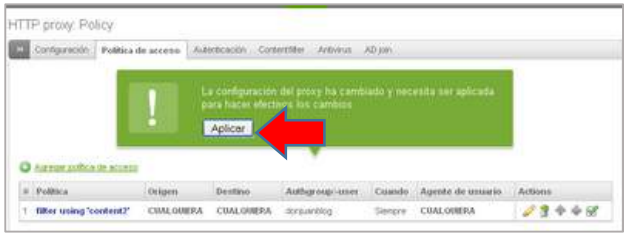


Figura 68. Proxy. Aplicar regla

Luego de aplicar la regla, verificar si se tiene el proxy en modo no trasparente, y a continuación se lo agregará al browser, como se observa en la figura 69.

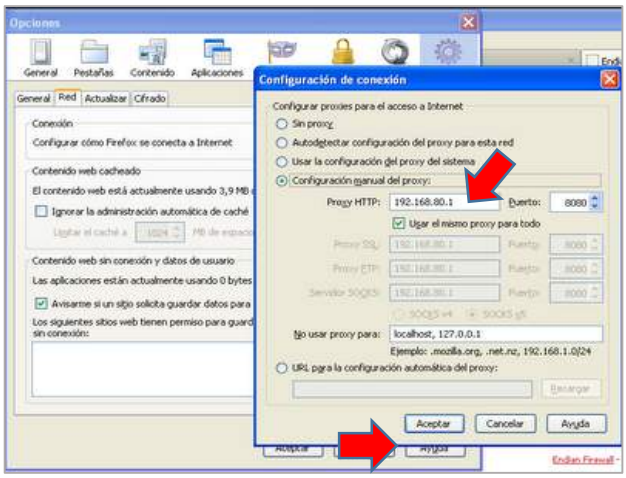


Figura 69. Proxy. Añadiendo al navegador

Después de agregar el proxy en modo transparente y añadirlo al browser, se procederá a realizar las pruebas correspondientes ingresando al navegador y autenticarnos, como se muestra en la figura 70.

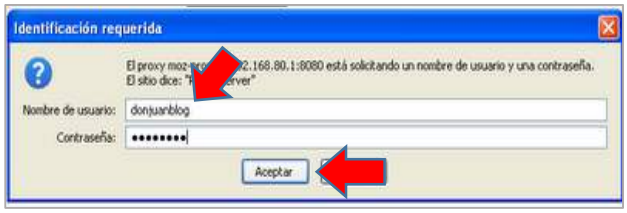


Figura 70. Proxy. Ventana de identificación

En la Figura 71 aparece un mensaje de error, porque se lo tiene en autenticación por grupo entonces al intentar ingresar a www.youtube.com pedirá un registro.

Figura 71. Proxy. Prueba - YouTube

Este mensaje a la que hace referencia la figura 72 aparecerá cuando se intente ingresar a un sitio restringido, en este caso se denegará el acceso a YouTube porque es la página que anteriormente se restringió.

Figura 72. Proxy. Prueba- YouTube

PRÁCTICA III: CORREO, DNS Y ANTISPAM

ANTISPAM – CORREO

Esta práctica ilustrará los pasos necesarios para configurar el proxy de correo electrónico para el spam de entrada y salida y el filtrado de virus en un dispositivo Endian típico.

Ejemplo de configuración (Inbound)

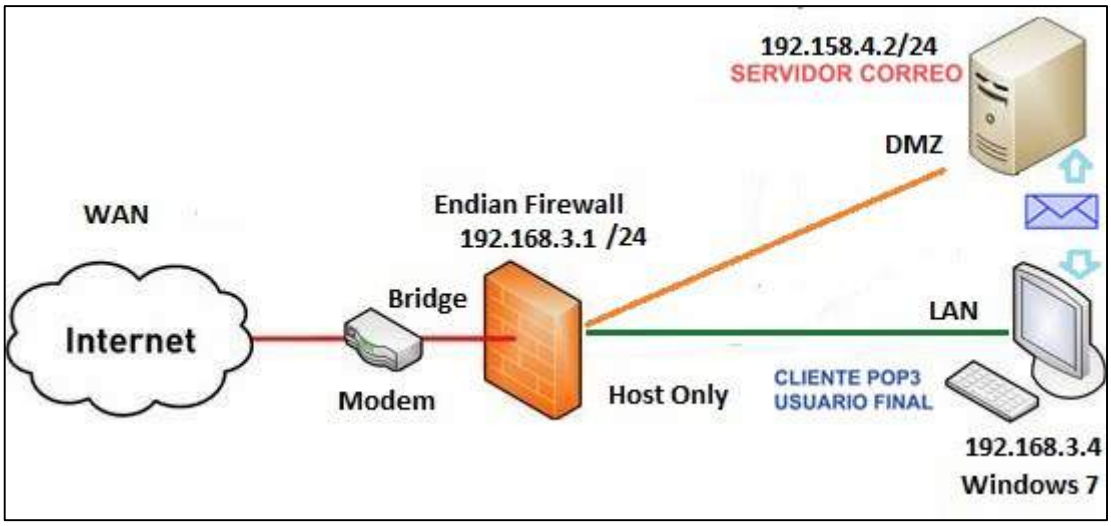


Figura 73. Diagrama de Red

Con el fin de filtrar el correo electrónico antes de llegar a nuestro servidor de correo interno, vamos a configurar el Endian para recibir todos los correos electrónicos de Internet y filtrar adecuadamente antes de entregarlo fuera del servidor de correo. También puede utilizar el dispositivo Endian para agregar un segundo nivel de filtrado si ya tiene filtrado de correo interno para proporcionar varias capas de filtrado y seguridad de correo electrónico.

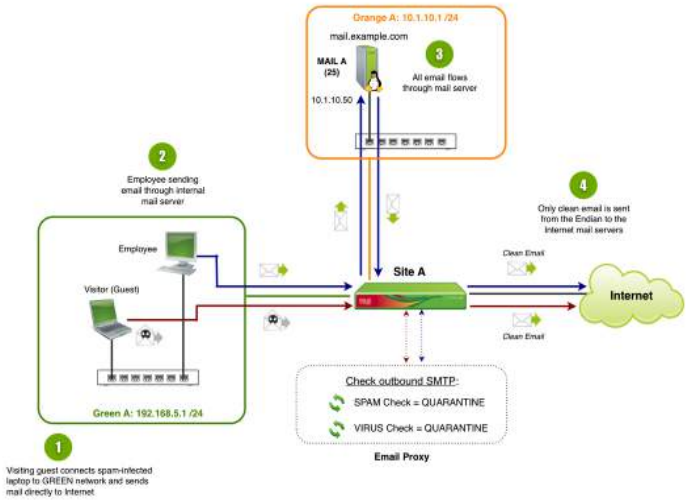


Figura 74. Ejemplo de configuración de salida

También configuraremos el Endian para escanear y filtrar de forma transparente todo el correo SMTP saliente. Esto garantizará que todos los correos electrónicos de nuestro servidor de correo, así como cualquier computadora interna que pueda estar enviando correo electrónico directamente a Internet, se filtren adecuadamente antes de enviarlos a Internet.

HABILITAR EL PROXY SMTP

Figura 75. Habilitación del SMTP

El primer paso es habilitar el proxy SMTP haciendo clic en el botón gris (debe convertirse en verde). Una vez hecho esto, podemos configurar el modo de filtrado de correo saliente (1) para cada una de nuestras redes internas (VERDE, NARANJA, AZUL) a "Transparente" ya que esto asegurará que todo el tráfico SMTP saliente se escanee automáticamente sin cambios del lado del cliente. Por último, podemos (2) habilitar el filtrado de correo electrónico entrante seleccionando el modo "Activo" bajo la interfaz ROJA. Como se pude observar en la Figura 75.

CONFIGURACIÓN DE CORREO NO DESEADO

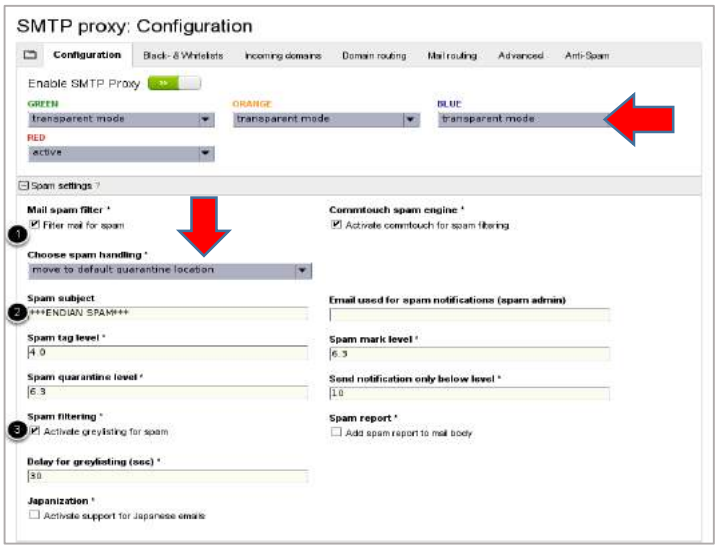


Figura 76. Configuración para correo no deseado

A continuación, activaremos (1) el filtrado de correo no deseado marcando la casilla y configurando la acción predeterminada para los mensajes marcados como spam (utilizaremos la cuarentena predeterminada). A continuación, puede proporcionar una línea de asunto de Spam que se agregará a cualquier mensaje de spam marcado. Por lo general, no se recomienda alterar los niveles de identificación predeterminados de Spam (etiqueta, marca, cuarentena). Por último, habilitaremos greylisting para proporcionar una capa adicional de protección contra correo no deseado. Tal como se observa en la figura 76.

Nota:

Greylisting es un método utilizado para reducir el spam rechazando automáticamente todos los correos electrónicos desconocidos. Si el correo electrónico fue legítimo, entonces el servidor de correo de origen volverá a enviar el correo electrónico en qué punto sería aceptado. La teoría es que cualquier bot de spam masivo no intentará reenviar el correo electrónico rechazado para que sólo los correos electrónicos válidos deban pasar.

CONFIGURAR LA CONFIGURACIÓN DE VIRUS

Figura 77. Configuración de virus

En la figura 77 se aprecia cómo es activada la detección de virus y se configurará la acción predeterminada para los mensajes marcados como que contengan un virus (usaremos la cuarentena predeterminada). También puede proporcionar un correo electrónico de administración que se copiará para todos los avisos de virus.

CONFIGURAR EXTENSIONES DE ARCHIVO

Endian Firewall sirve como proxy de correo. Entre muchas de las habilidades que provee, bloquea los archivos con determinadas extensiones incluidas en los mensajes de correo, estas extensiones vienen una lista definida y no tiene forma desde su herramienta de administración de agregar nuevas.

En este paso se seleccionará las extensiones que deseamos bloquear, tal como se metra en la imagen.

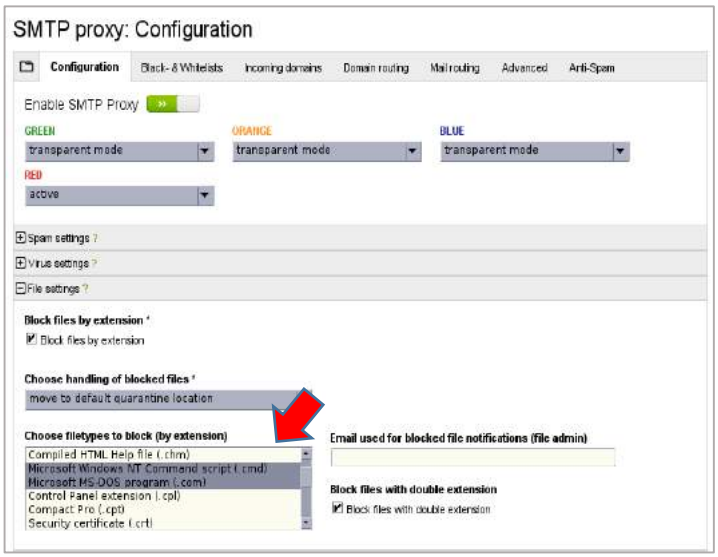


Figura 78. Configuración de extensiones de archivos

Opcionalmente, también puede configurar el bloqueo de ciertas extensiones de archivo si tiene una necesidad o requisito para hacerlo.

Una vez completada la configuración, haga clic en Guardar y continuar.

CONFIGURAR LISTAS NEGRAS EN TIEMPO REAL (RBL)

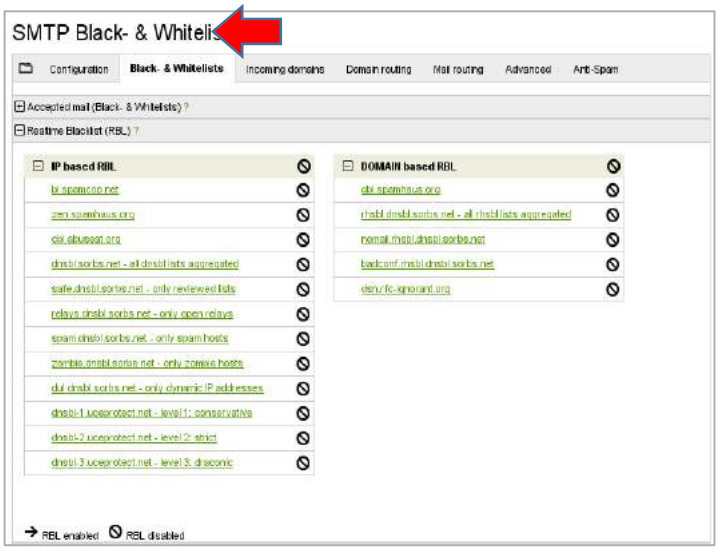


Figura 79. Configuración de listas negras

A continuación, debemos habilitar las listas negras en tiempo real para que Endian utilice en la comprobación de servidores de correo electrónico en

lista negra conocidos. Endian es compatible con RBLs basados en IP y DNS, tal como se aprecia en la figura 79.

Una vez completado, haga clic en Guardar y continuar.

(Opcional) Configuración de Greylisting

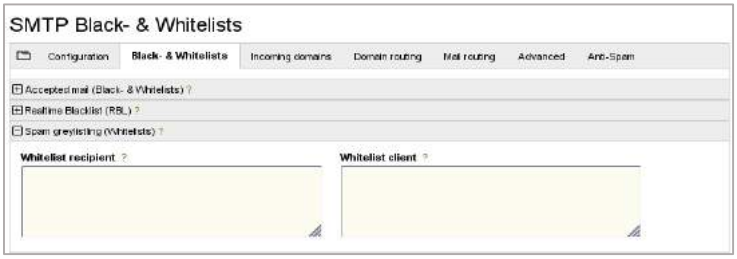


Figura 80. Configuración de Greylisting

Si utiliza greylisting de spam, opcionalmente puede optar por configurar la lista blanca de greylisting para todos los destinatarios, dominios y servidores de correo conocidos. Esto puede ayudar a reducir el retraso de entrega de correo inherente asociado con greylisting para fuentes de correo bien conocidas.

CONFIGURAR EL SERVIDOR DE CORREO ENTRANTE

Figura 81. Configuración de correos entrantes.

A continuación, se configurarán todos los dominios del servidor de correo interno que necesitan ser filtrados para recibir correo electrónico añadiendo la dirección IP del dominio y del servidor de correo para ese dominio, como se observa en la figura 81.

Una vez completado, haga clic en Guardar y continuar.

CONFIGURACIÓN AVANZADA DE PROXY DE CORREO

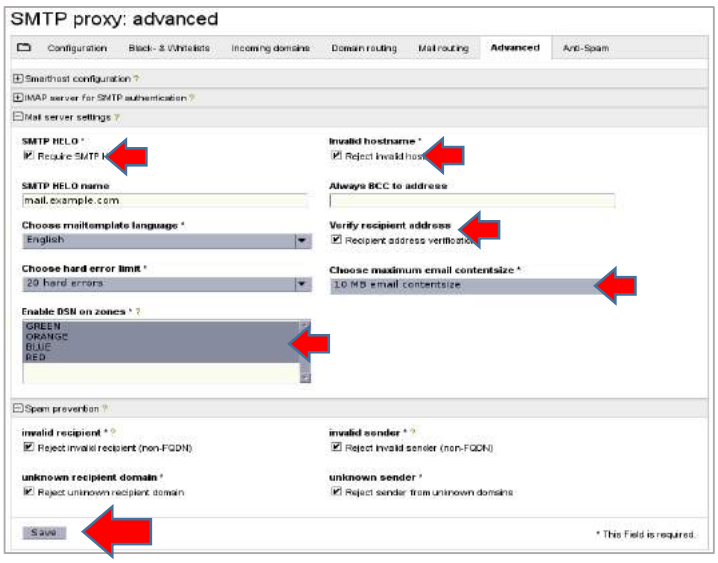


Figura 82. Configuración avanzada de Proxy

El último paso es configurar cualquier configuración avanzada de proxy de correo que se recomiende y habilite de forma predeterminada. Éstos incluyen cosas para comprobar y verificar la sintaxis de SMTP y los mecanismos de validación de remitente / destinatario (registro A o MX válido, dirección del destinatario válida, etc.). También puede establecer el tamaño máximo de correo electrónico y el nombre HELO SMTP.como se aprecia en la figura 82.

Una vez que se haya completado, haga clic en Guardar y ya está

SERVIDOR DNS

Uno de los roles más importantes dentro de todo el proceso de gestión y configuración de un servidor es el DNS (Domain Name System – Sistema de Nombres de Dominio) el cual nos permite traducir las direcciones IP a nombres de dominio y viceversa, de este modo es mucho más fácil tener presente Solvetic.com y no 178.33.118.246.

Este rol es fundamental para todo el proceso de transferencia de información y permite que como administradores y usuarios frecuentes de la red tengamos claridad qué sitios visitamos.
En esta guía se analizará cómo configurar este rol DNS en CentOS 7 de una forma práctica.

BIND (Berkeley Internet Name Domain) es un software libre, de código abierto que cumple las funciones de DNS en un sistema, su nombre se debe al sitio donde fue desarrollado, la universidad Berkeley en California en el año

de 1980. Gracias a BIND podemos contar con una plataforma segura y estable que cumple a cabalidad con todos los estándares de DNS.

A continuación, veremos cómo configurar e instalar este servidor DNS en CentOS 7 y de este modo comenzar a disfrutar al máximo de este importante rol.

Es importante validar que contamos con conectividad a la red, para esto podemos realizar un ping a cualquier sitio web:

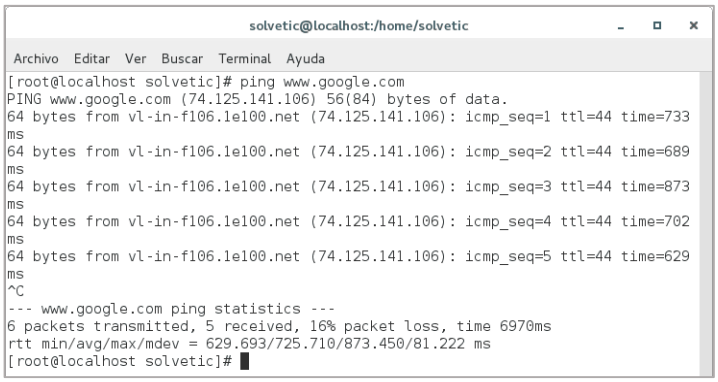


Figura 83. Validación de red

1. ¿CÓMO INSTALAR BIND9 EN CENTOS 7

Paso 1

En primer lugar, actualizaremos todos los paquetes de CentOS 7 usando el siguiente comando:

- yum update

Paso 2

Una vez concluya el proceso de actualización de CentOS, procedemos a instalar BIND y sus utilidades usando el comando yum, para ello ingresaremos el siguiente comando. Aceptamos la descarga y respectiva instalación de BIND y sus componentes, como se muestra en la figura 84.

- yum install bind bind-utils

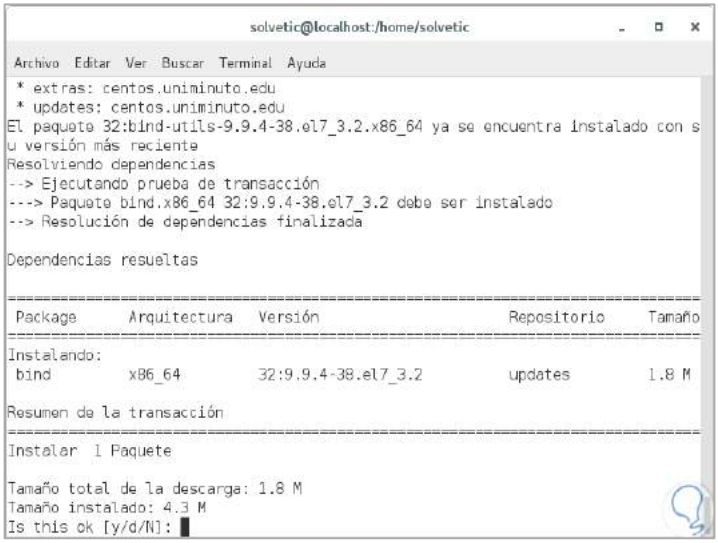


Figura 84. Instalación de BIND

2. CÓMO INICIAR LOS SERVICIOS DE BIND EN CENTOS 7

Paso 1

Una vez todos los paquetes de BIND hayan sido instalados procedemos a iniciar el respectivo servicio usando los siguientes comandos en su orden, como indica el texto y la figura 85.

- systemctl enable named
- systemctl start named
- systemctl status named

Figura 85. Inicialización de Servicios BIND

3. CÓMO CONFIGURAR EL SERVIDOR DNS CON BIND EN CENTOS 7

Con esto en mente iniciaremos la configuración del servidor DNS en CentOS 7.

Paso 1

El archivo de configuración de BIND lo encontramos en la **ruta /etc/named.conf** por lo cual debemos acceder a él usando el editor preferido, en este caso usaremos nano:

- nano /etc/named.conf

Paso 2

En el archivo abierto realizaremos las siguientes tareas, que se pueden apreciar en la figura 86.

- Comentamos, con el símbolo #, las siguientes líneas:
- listen-on port 53 {127.0.0.1;};
- listen-on-v6 port 53 {:1;};

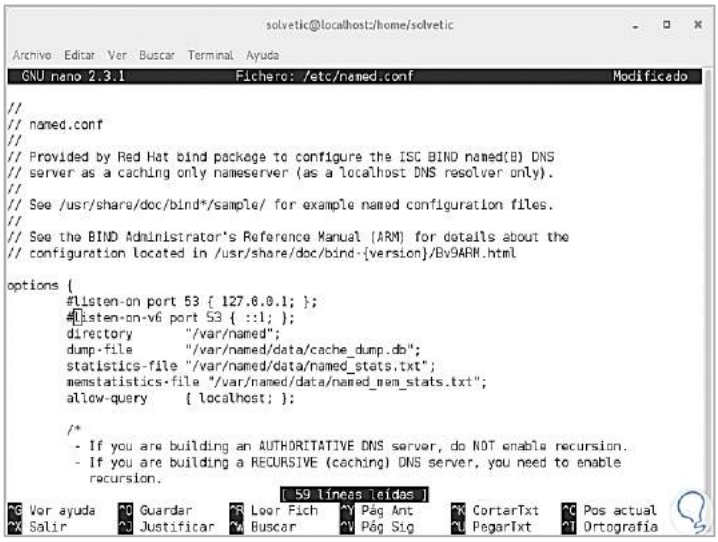


Figura 86. Configuración de DNS con BIND

Agregamos la dirección IP sobre la cual los equipos cliente consultarán el DNS, adicional podemos agregar la dirección IP de un segundo servidor en caso de tenerlo, esto se muestra en la figura 87, usaremos las siguientes líneas:

- allow-query {localhost;IP/Red; };
- allow-transfer {Ip segundo servidor; };

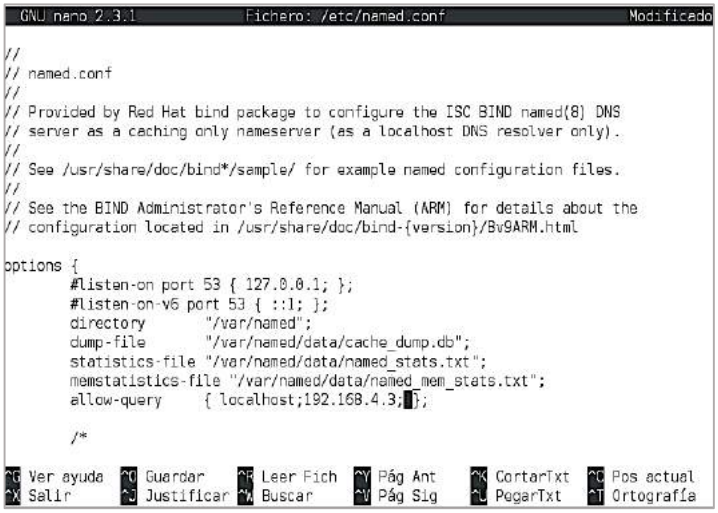


Figura 87. Agregar IP para consultas de DNS

- **Guardamos los cambios** usando la combinación de teclas

Ctrl + **O**

y **salimos del editor** usando las teclas:

Ctrl + **X**

4. CÓMO CREAR LAS ZONAS DE BIND EN CENTOS 7

Una vez definidos estos parámetros el siguiente paso será crear y configurar las respectivas zonas directa e inversa las cuales deben ser agregadas en el archivo **named.conf**.

Paso 1

Accedemos a dicho archivo usando el siguiente comando:

- nano /etc/named.conf

Paso 2

Configuramos la primera zona de esta manera:
Los parámetros configurados son:

- **Solvetic.local:** Nombre del dominio
- **Master:** Es el DNS primario
- **fwd. solvetic. local.db:** Indica la zona directa

- **allow-update:** Hace referencia al DNS primario.

Agregamos las siguientes líneas para la zona inversa:

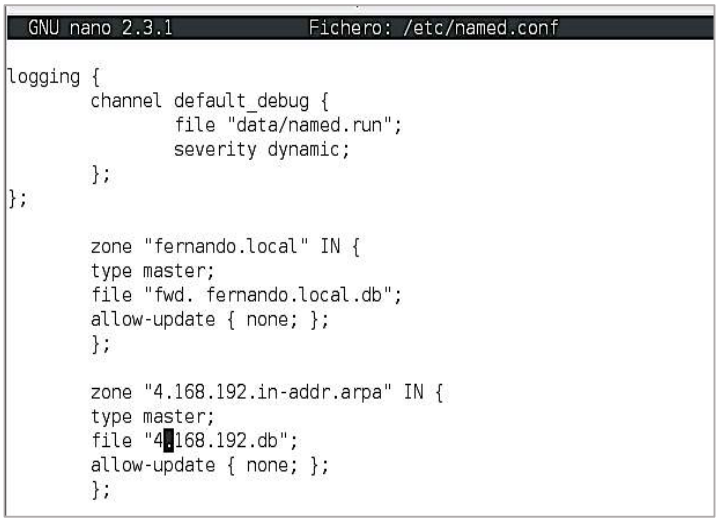


Figura 88. Zonas de BIND

Paso 5

Guardamos los cambios usando la combinación de teclas siguiente:

Ctrl + **O**

5. CÓMO CREAR LOS ARCHIVOS DE ZONA DE BIND EN CENTOS 7

Hemos creado las zonas, ahora debemos crear los archivos de dichas zonas.

Paso 1

El primer archivo a crear será el de la zona directa, ejecutamos lo siguiente:

- nano /var/named/fwd.fernando.local.db

Paso 2

Esto creará un nuevo archivo donde ingresaremos lo que se observa en la figura 89

Figura 89. Creación de archivos en zona BIND

Paso 3

Los parámetros de dicho archivo son:

A – Grabador
NS – Nombre del servidor
MX – Email de Exchange
CN – Nombre canónico

Paso 4

Guardamos los cambios y cerramos el editor. Ahora crearemos el archivo para la zona inversa ejecutando lo siguiente:

- nano /var/named/4.168. 192.db

Paso 5

En el archivo en blanco agregaremos lo siguiente:

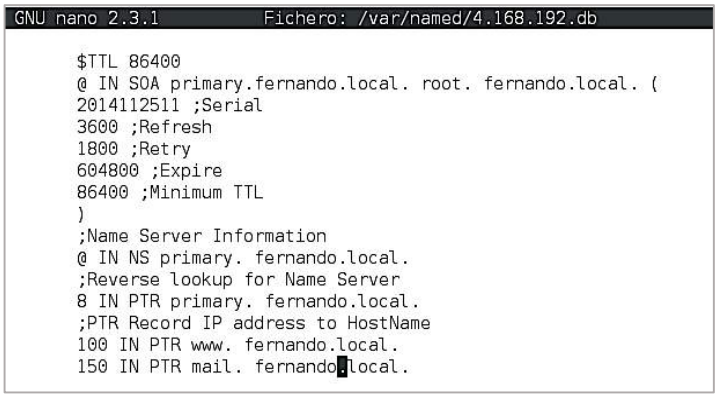


Figura 90. Creación de archivo para zona inversa de BIND

Guardamos los cambios en el archivo y salimos del archivo.

6. CÓMO REINICIAR SERVICIOS DE BIND EN CENTOS 7

Una vez configurados estos parámetros el siguiente paso será reiniciar los servicios para su respectiva aplicación.

Paso 1

Para ello ejecutaremos los siguientes comandos en su orden, esto se puede apreciar en la figura 91.

- chmod 777 /var/named/fwd.fernando.local.db
- chmod 777 /var/named/4.168. 192.db
- systemctl restart named.service

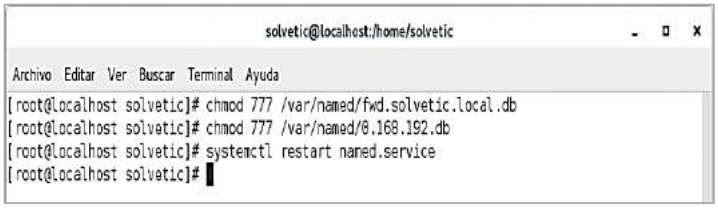


Figura 91. Reinicio de Servicios BIND en Centos 7

Paso 2

Si deseamos consultar el estado del servicio ejecutaremos el siguiente comando. Podemos comprobar que su estado es activo y ejecutándose, en la figura 92.

- systemctl status named.service

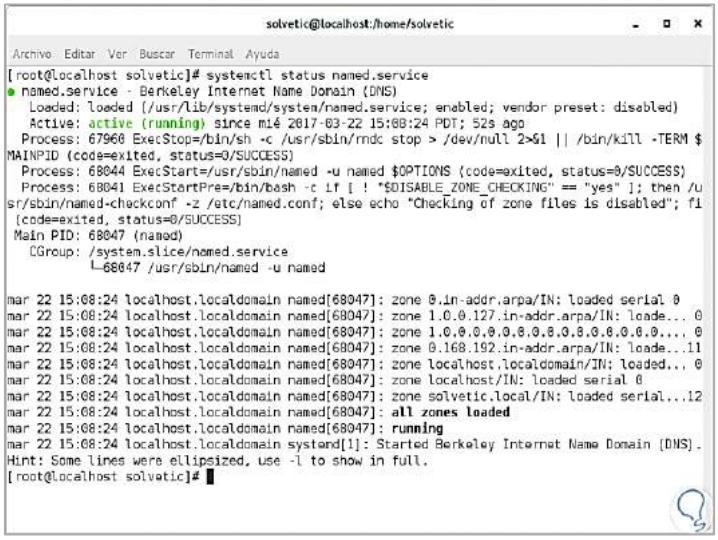


Figura 92. Estado de servicio en ejecución

7. CÓMO COMPROBAR LAS ZONAS EN LOS EQUIPOS CLIENTE DE BIND EN CENTOS 7

Ahora que BIND ha sido configurado resta configurar la maquina cliente para que tome el DNS y a través del resuelva las direcciones IP.

Paso 1

Para esto iniciamos sesión en algún maquina cliente, en este caso en Ubuntu, y accedemos al archivo /etc/resolve.conf:

- nano /etc/resolve.conf

Paso 2

Allí agregaremos la siguiente sintaxis:

- nameserver (Dirección IP del servidor DNS)

Paso 3

A continuación, se ejecuta el siguiente comando para comprobar la zona directa, esto se aprecia en la figura 93.

- dig nombre del servidor

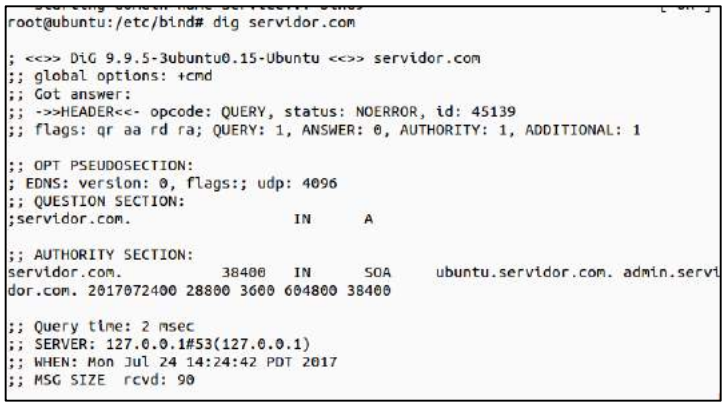


Figura 93. Comprobación de zona directa

Paso 4

Ahora, para verificar la zona inversa ejecutaremos el siguiente comando:

- dig -x (Ip de la maquina cliente)

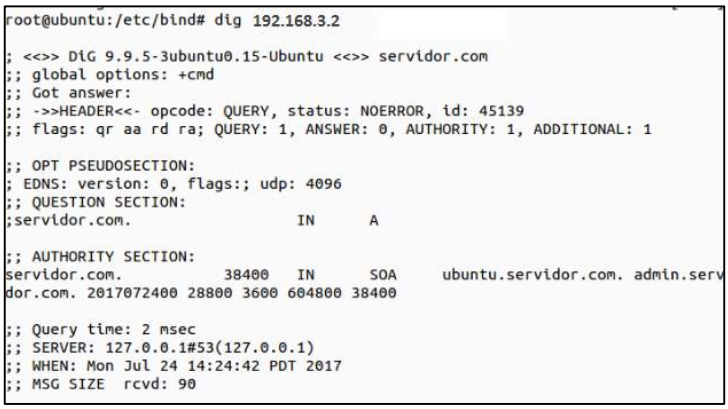


Figura 94. Zona inversa

Recordemos la importancia de un servidor DNS en nuestra organización ya que sin el más de un usuario puede perder la cabeza aprendiendo direcciones IP en lugar de nombres de dominio. Si te interesa el tema de servidores en Linux, no te pierdas cómo instalar un servidor FTP en CentOS7.

SERVIDOR DE CORREO

Uno de los principales objetivos que tenemos como administradores de sistemas o como personal de soporte es velar por la correcta comunicación entre los usuarios de la organización y una de las formas más fundamentales como logramos este objetivo es gracias al servidor de correo que tengamos configurado para que a través de él todos los mensajes, tanto entrantes como salientes, lleguen al destinatario correcto de forma segura e íntegra.

De una correcta comunicación en la organización dependen muchas tareas y metas propuestas para cada día escalar y mejorar los procesos corporativos.

¿QUÉ ES UN SERVIDOR DE CORREO?

Antes de analizar cómo implementar el servidor de correo en CentOS 7 debemos conocer algunos términos relacionados con el tema. Un servidor de correo es básicamente una aplicación que nos brinda la posibilidad de enviar mensajes, en forma de correos, entre los distintos usuarios de la organización o fuera de ella independiente de la red a la cual estén conectados. Los términos básicos que usaremos en un servidor de correo son:

POP3

POP (Post Office Protocol – Protocolo de Oficina de Correos) es el protocolo que permite que el mensaje sea recibido y este protocolo no requiere de una conexión permanente a internet para su funcionamiento.

IMAP

IMAP (Internet Message Access Protocol – Protocolo de Acceso de Mensajes de Internet) es un protocolo que permite que el cliente de correo electrónico se conecte a la cuenta de correo y despliegue los mensajes de correo almacenados.

SMTP

SMTP (Simple Mail Transfer Protocol – Protocolo Simple de Transferencia de Correo) es un protocolo basado en texto que es usado para el intercambio de mensajes de correo entre diferentes dispositivos.

MTA

MTA (Mail Transfer Agent – Agente de Transferencia de Correo) es un servidor cuya función es transferir correos y la gestión de los mismos en internet. Algunos MTAs conocidos son Sendmail, Postfix, etc.

DOVECOT

Dovecot es un servidor de correo entrante el cual soporta los protocolos mencionados anteriormente. Con estos conceptos en mente procederemos a la configuración de nuestro servidor de correo en CentOS 7.

1. INSTALAR REPOSITORIOS EPEL

En primer lugar, debemos instalar los repositorios de EPEL para posteriormente instalar el MTA a usar para el servicio de correo, recordemos que EPEL son los paquetes adicionales para Enterprise Linux que nos brinda complementos para los paquetes de software en las ediciones **CentOS, RHEL y Fedora.**

Para instalar dichos repositorios usaremos el comando:

- sudo yum -y install epel-release

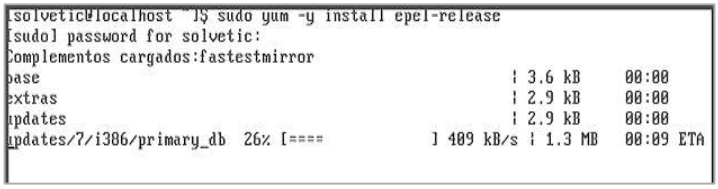


Figura 95. Repositorios EPEL

Nota. - Recordemos que si se ejecutan estos comandos con un usuario diferente al root debemos anteponer el término **sudo**

2. INSTALAR APACHE PARA GESTIÓN DE SERVIDOR DE CORREO

El siguiente paso consiste en instalar Apache usando el parámetro **– -disablerepo=epel*** el cual nos permite realizar la instalación directamente de los repositorios oficiales. Usaremos el siguiente comando, como se muestra en la figura 96.

- sudo yum -y install --disablerepo=epel*

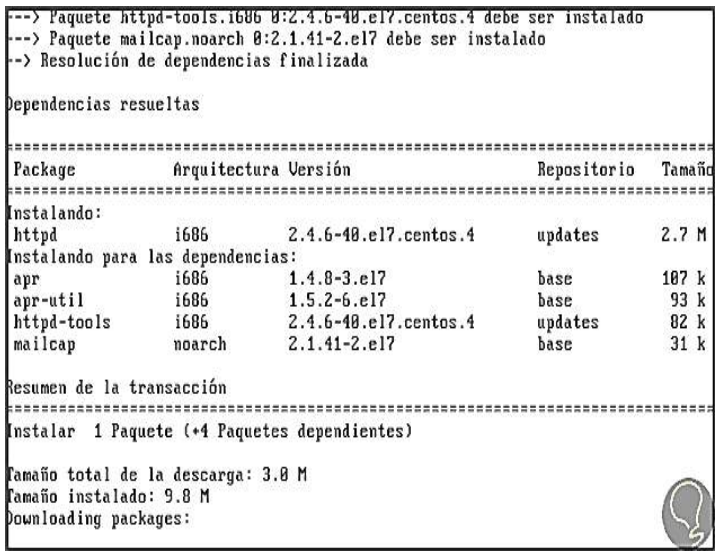


Figura 96. Instalación de Apache

3. INSTALACIÓN DE APLICACIONES NECESARIAS

Una vez realizado el proceso anterior instalaremos las siguientes aplicaciones:

- Sendmail (El cual será usado para el envío de los correos)
- Dovecot
- Squirrelmail (Será nuestro cliente web de correos)

Paso 1

Para ello usaremos el siguiente comando

- sudo yum -y install sendmail sendmail-cf dovecot squirrelmail

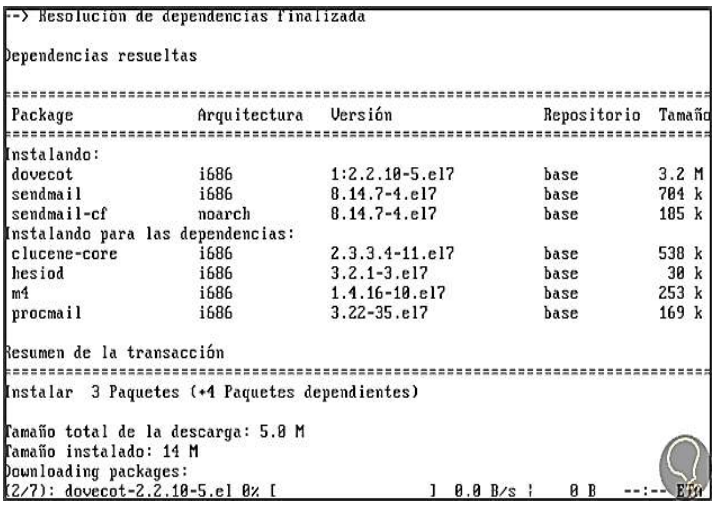


Figura 97. Instalación de aplicaciones necesarias

Paso 2

Ahora validaremos el servicio Postfix. Este servicio por defecto viene instalado en CentOS 7, procedemos a buscarlo y en caso de encontrarlo procedemos a detenerlo, para ello usaremos los siguientes comandos.

- rpm -qa | grep postfix
- systemctl stop postfix

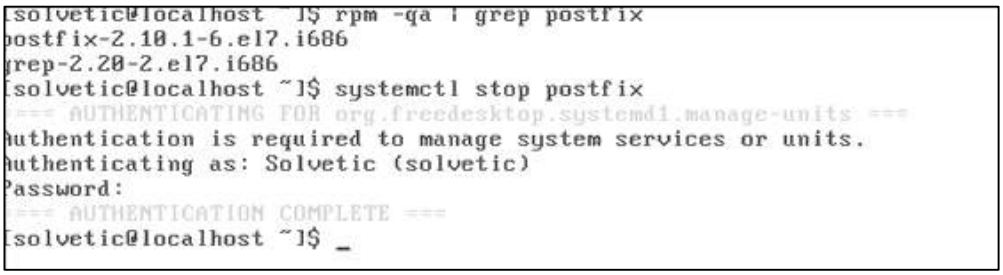


Figura 98. Validación del servicio Postfix

Paso 3

A continuación, modificaremos el nombre del equipo por un nombre de dominio válido, en este caso usaremos el nombre solvetic.com e ingresaremos lo siguiente en CentOS 7:

- sudo hostname acc.com

4. CONFIGURACIÓN DE DOVECOT

Paso 1

Para configurar los parámetros de Dovecot se debe ingresar en la siguiente ruta **/etc/dovecot/dovecot.conf**, se puede usar el editor preferido, en este caso nano.

- sudo nano /etc/dovecot/dovecot.conf

Se apreciará que se despliega lo siguiente en la figura 99.

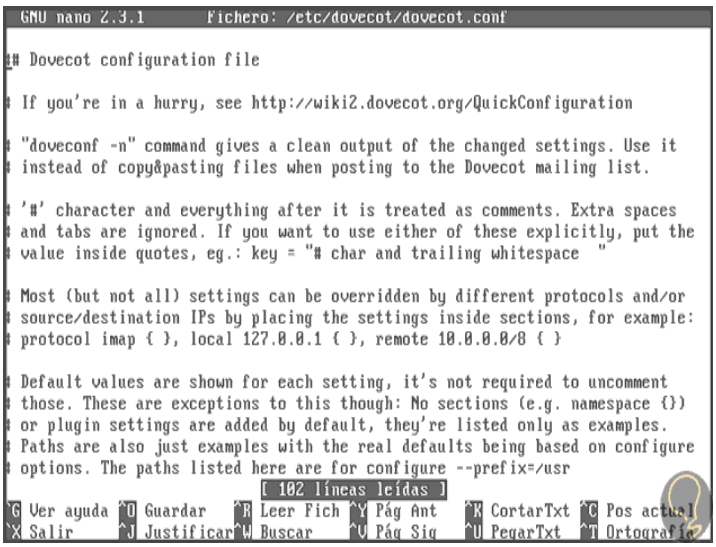


Figura 99. Configuración de Dovecot

Paso 2

En esta configuración debemos ubicar la línea siguiente

- Protocols we want to be serving

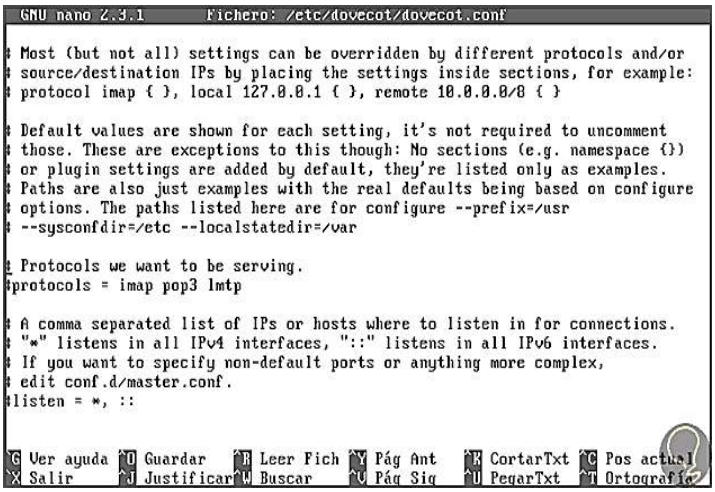


Figura 100. Dovecot

Paso 3

Se descomenta la línea Protocols = imap pop3 lmtp (Quitando el símbolo #) y se deja los protocolos que se usarán, en este caso IMAP y pop3.

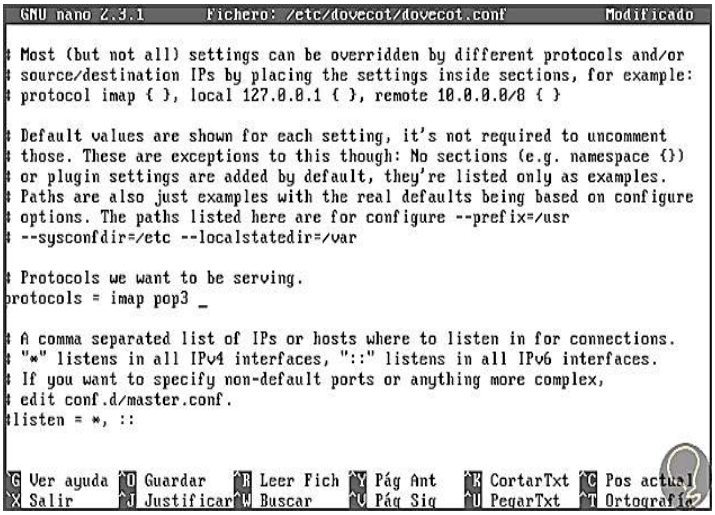


Figura 101. Protocolos a utilizar

Paso 4

Guardar los cambios usando la combinación de teclas:

Ctrl + **O**

Y salir del editor usando la combinación

Ctrl + **X**

Paso 5

Ingresar en la ruta /etc/dovecot/conf.d/10-mail.conf para su edición, como podemos ver en la figura 102.

- sudo nano /etc/dovecot/conf.d/10-mail.conf

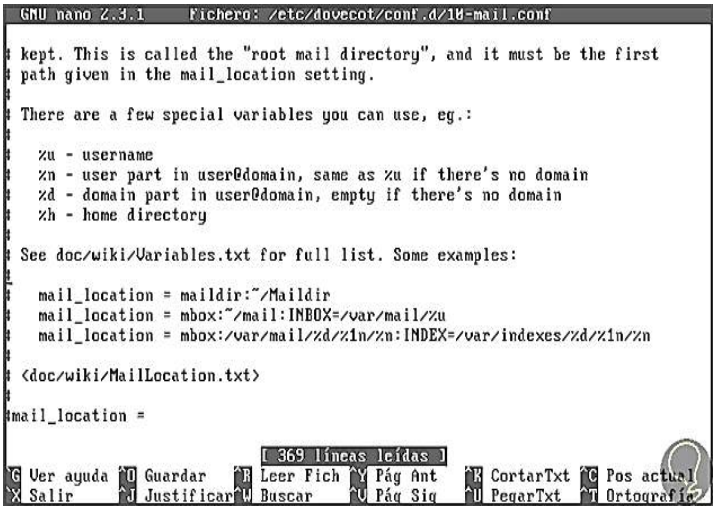


Figura 102. Ruta para la edición de dovecot

Paso 6

Allí debemos copiar la línea mail_location = mbox: ~/mail:INBOX=/var/mail/%u y pegarla en el campo mail_location debajo de la línea <doc/wiki/MailLocation.txt> y teniendo en cuenta quitar el símbolo #, como se aprecia en la figura 103.

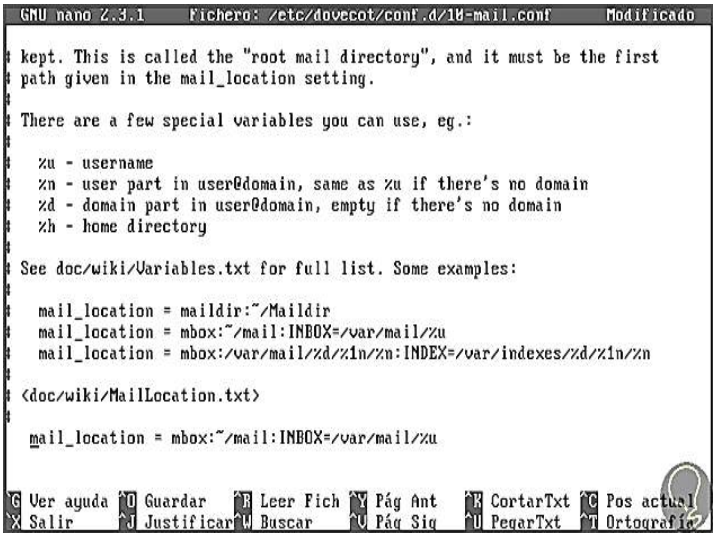


Figura 103. Locación de mail

Paso 7

Finalmente accedemos al archivo ubicado en la ruta /etc/dovecot/conf.d/10-auth.conf, como podemos ver en la figura 104.

- sudo nano /etc/dovecot/conf.d/10-auth.conf

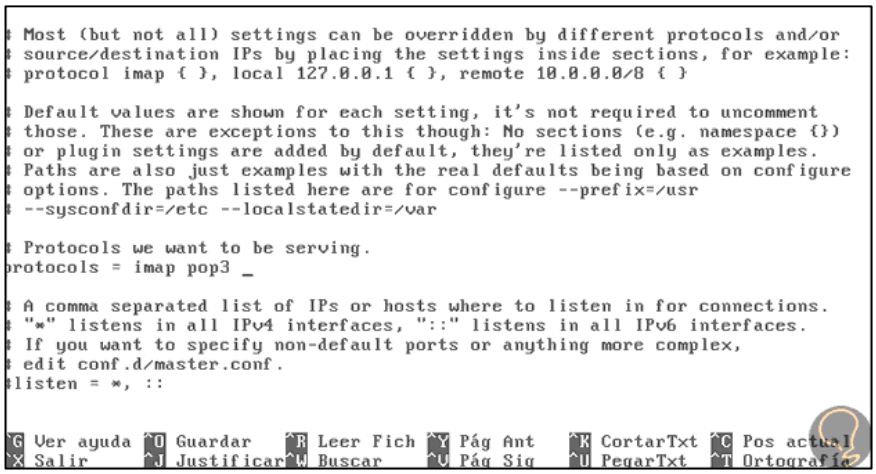


Figura 104. Abrir Dovecot

Paso 8

Se debe descomentar (quitar símbolo #) de la línea disable_plaintext_auth = yes, como se ve en la figura 105.

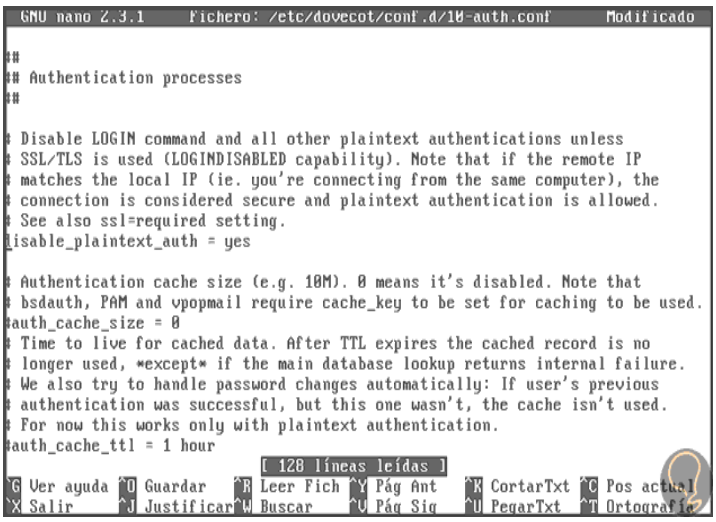


Figura 105. Comentarios

Paso 9

Guardamos los cambios usando la combinación de teclas:

Ctrl + **O**

y salimos del editor usando la combinación:

Ctrl + **X**

5. CONFIGURACIÓN DE SENDMAIL

Paso 1

En la figura 106 se debe acceder a la siguiente ruta **/etc/mail/sendmail.mc** para efectuar los cambios en la configuración de Sendmail, usaremos nano para acceder a la edición.

- sudo nano /etc/mail/sendmail.mc

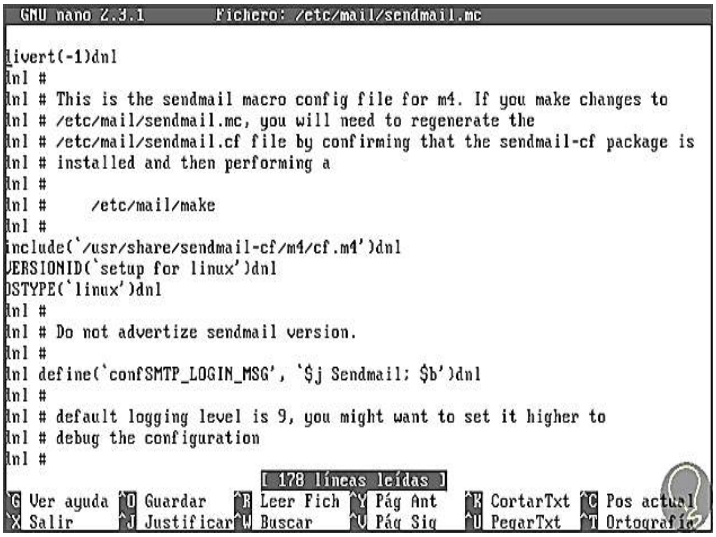


Figura 106. Configuración de Sendmail

Paso 2

En la figura 107 se debe ubicar la línea:

- DAEMON_OPTIONS ("port=smtp,Addr=127.0.0.1, Name=MTA")dn1

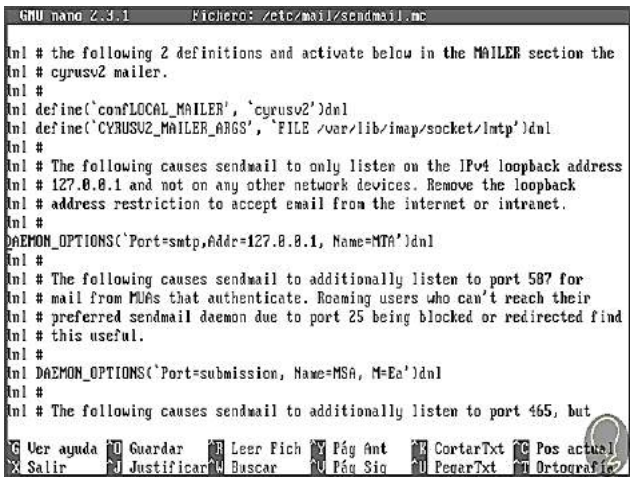


Figura 107. Opciones Demon

Paso 3

En esta línea removemos el apartado asociado a Addr quedando la línea, como en la figura 108.

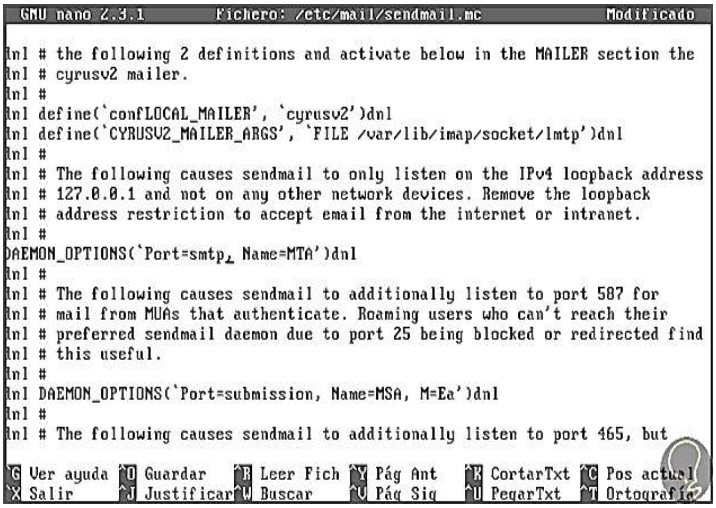


Figura 108. Remoción de apartado

Paso 4

Guardamos los cambios. Una vez ejecutado este cambio usaremos el comando m4 para modificar el formato de Sendmail de .mc a .cf (Es una compilación), para ello usaremos el siguiente comando.

- sudo m4 /etc/mail/sendmail.mc > /etc/mail/sendmail.cf

6. CONFIGURACIÓN DE SQUIRRELMAIL

Paso 1

El siguiente paso consiste en acceder a la ruta **/**etc/mail/local-host-names usando nano para realizar algunos ajustes, ingresaremos.

- sudo nano /etc/mail/local-host-names

Paso 2

Allí ingresaremos el nombre del dominio, en este caso solvetic.com.

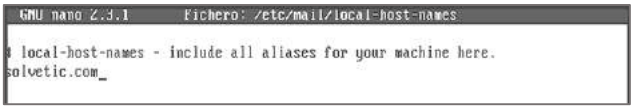


Figura 109. Guardar cambios

Paso 3

Guardar los cambios. Luego, acceder usando nano a la siguiente ruta, como se ve en la figura 110.

- /etc/mail/Access

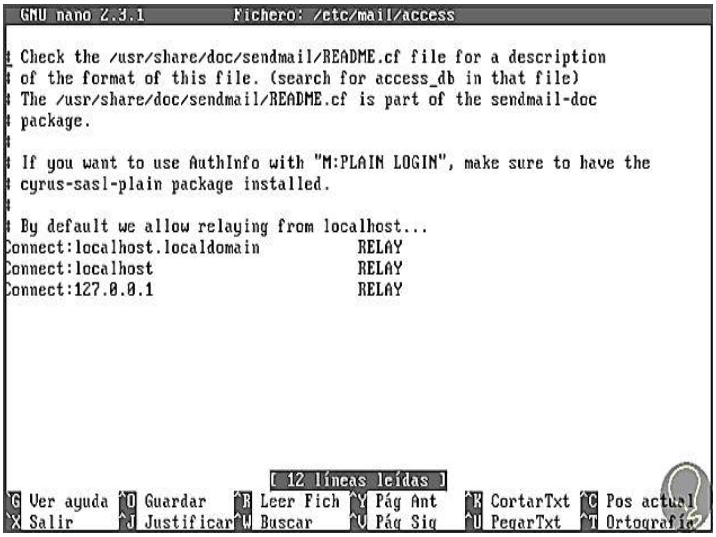


Figura 110. Acceso

Paso 4

Allí debemos añadir una línea con el **nombre de nuestro dominio. Guardamos** los cambios usando.

Ctrl + **O**

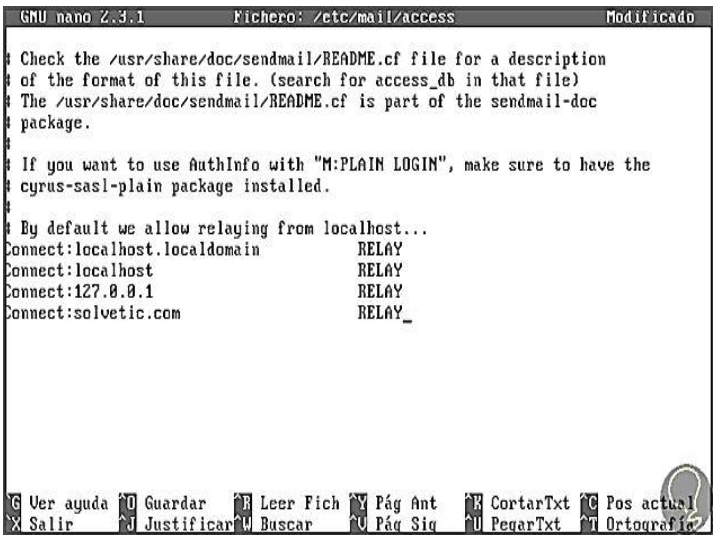


Figura 111. Dominio

Paso 5

Una vez efectuados estos cambios procedemos a reiniciar los servicios para que se pueda apreciar los cambios realizados usando los siguientes comandos:

- systemctl start httpd para iniciar el servicio de httpd como se aprecia en la figura 112
- systemctl start sendmail.service para iniciar el servicio de correo como se aprecia en la figura 112
- systemctl start dovecot.service para iniciar el servicio de dovecot como se aprecia en la figura 112

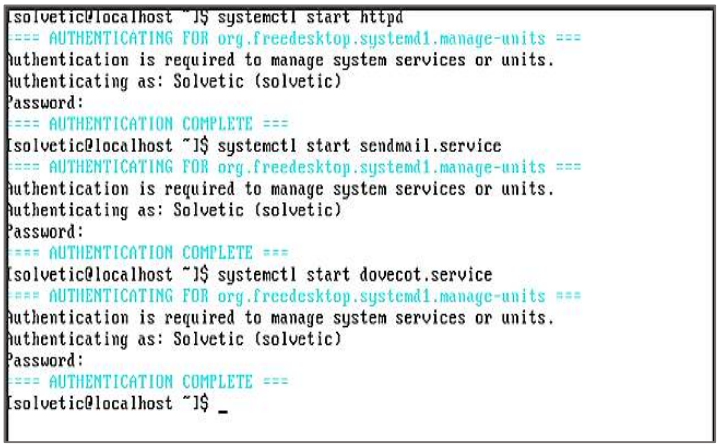


Figura 112. Reinicio de Servicios

7. ACCEDER A LA CONSOLA WEB

Para este análisis hemos creado dos usuarios usando el comando **useradd** llamados correosolvetic y solvetic1.

Paso 1

A continuación, debemos ir a un navegador e ingresar la siguiente sintaxis:

- http://Dirección_IP/webmail

En nuestro caso ingresamos

- http://192.168.0.11/webmail tal como se aprecia en la figura 113

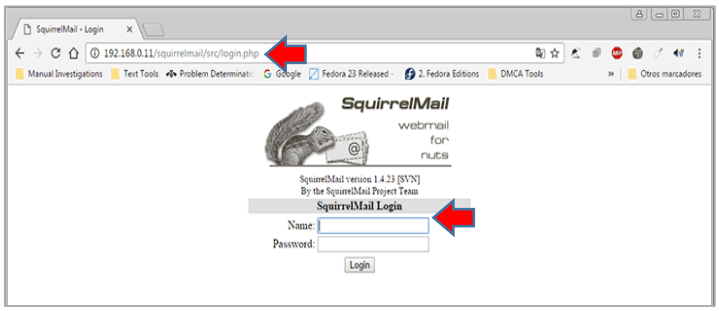


Figura 113. Probando Navegador

Paso 2

Ingresamos nuestras credenciales y veremos el siguiente error que se aprecia en la figura 114.

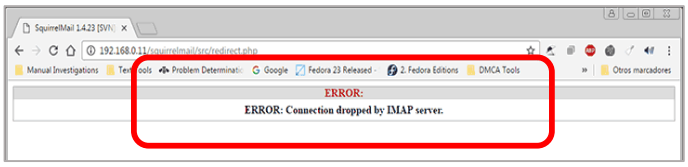


Figura 114. Error

Paso 3

Este error de debe a que la carpeta que contendrá la información del servidor de correo no existe. Para solucionar esto debemos usar el siguiente comando para crear la respectiva carpeta en la raíz del usuario seleccionado, en este caso correosolvetic (y aplicarlo a cada uno de los usuarios creados)

- touch /home/estudiante/mail/.imap/INBOX

Paso 4

Posteriormente debemos modificar el propietario de la carpeta usando los siguientes comandos:

- sudo chown -R estudiante:estudiante /var/www/html/correosolvetic

Paso 5

Ahora de nuevo intentamos acceder y veremos lo que se pude observaren la figura 115.

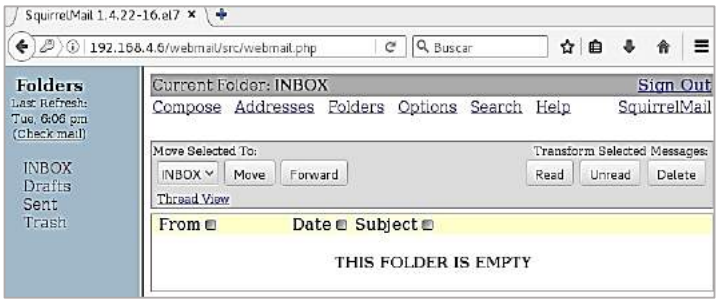


Figura 115. Acceder a ruta

Paso 6

Vemos que ya tenemos dos mensajes en nuestra bandeja de entrada, estos fueron enviados desde la consola usando la siguiente sintaxis:

- mail usuario
- Subject (Motivo)
- Cuerpo del mensaje

8. VISUALIZAR Y ENVIAR MENSAJES DESDE EL CLIENTE

Paso 1

Para ver los mensajes almacenados en nuestro buzón basta con seleccionarlo y obtendremos el motivo del correo. Tal como se pude observar en la figura 116.

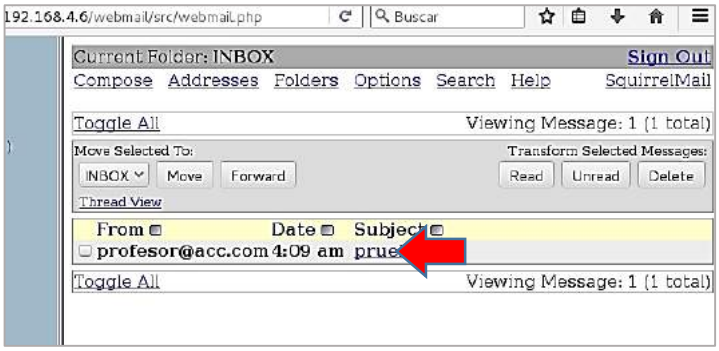


Figura 116. Mensajes de nuestro buzón

Paso 2

Para enviar un mensaje a otro correo, por ejemplo, hemos iniciado sesión con el usuario **profesor** y enviaremos un mensaje al usuario **estudiante**, debemos seleccionar la opción **Compose** ubicada en la parte superior y

especificar el destinatario, motivo y mensaje. Tal como se parecía en la imagen 117.

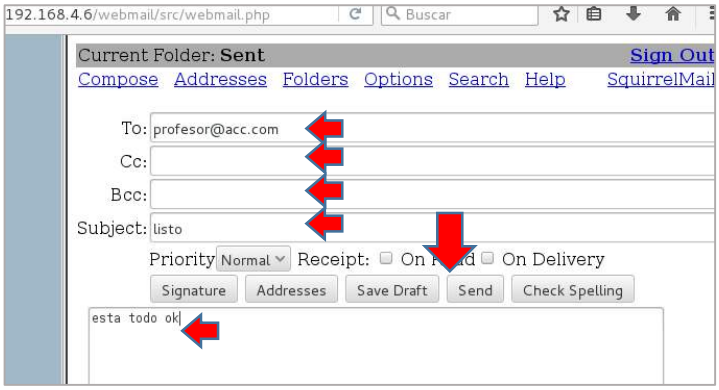


Figura 117. Envío de nuevo mensaje

3

Paso 3

Iniciar sección con el usuario estudiante, nos dirigimos a la bandeja de entrada (INBOX) y vemos que el mensaje enviado desde la cuenta profesor esta en nuestro inbox, como se puede aprecia en la figura 118 y ya se pude visualizar.

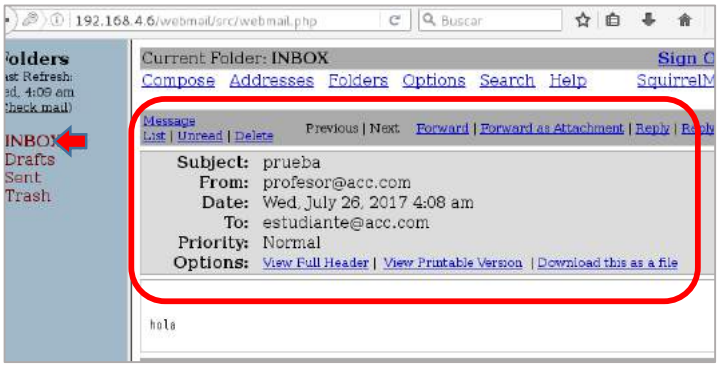


Figura 118. Enviar nuevo mensaje

Asimismo, se puede loguear en cualquier parte que tengamos permitidos de nuestra red. En este caso ingresaremos a nuestra zona verde y digitamos en el navegador la ip de nuestro servidor de correo 192.168.4.6/webmail/, loguear y acceder con los usuarios disponibles.

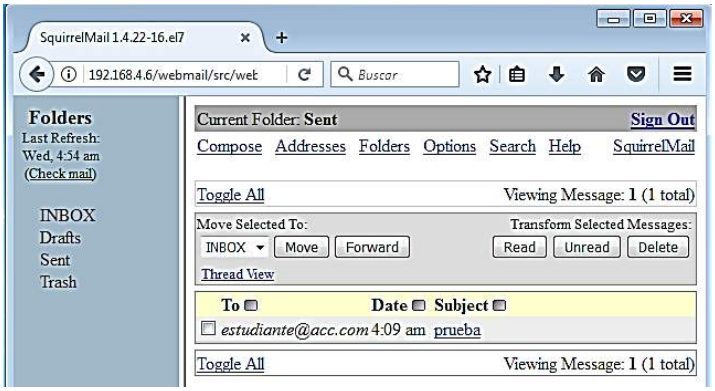


Figura 119. Usuario estudiante

Usando este método podemos configurar un servidor de correo en sistemas Linux, en este caso CentOS 7 para permitir la intercomunicación entre los diversos usuarios de forma sencilla y práctica.

ANEXO A INSTALACIÓN DE MÁQUINA VIRTUAL VMWARE WORKSTATION

¿QUÉ ES UNA MÁQUINA VIRTUAL?

Una máquina virtual no es más que un software capaz de cargar en su interior otro sistema operativo haciéndole creer que es un PC de verdad. Tal y como su nombre indica, el concepto es tan sencillo como crear una máquina (PC, consola, móvil o lo que sea) que en vez de ser física es virtual o emulada.

Lo primero que debes saber es que hay dos tipos de máquinas virtuales diferenciadas por su funcionalidad: las de sistema y las de proceso, si bien la gran mayoría de las veces que se habla de una máquina virtual casi seguro que se estarán refiriendo a las de sistema.

Máquinas virtuales de sistema

Una máquina virtual de sistema es aquella que emula a un ordenador completo. En palabras llanas, es un software que puede hacerse pasar por otro dispositivo -como un PC- de tal modo que puedes ejecutar otro sistema operativo en su interior. Tiene su propio disco duro, memoria, tarjeta gráfica y demás componentes de hardware, aunque todos ellos son virtuales.

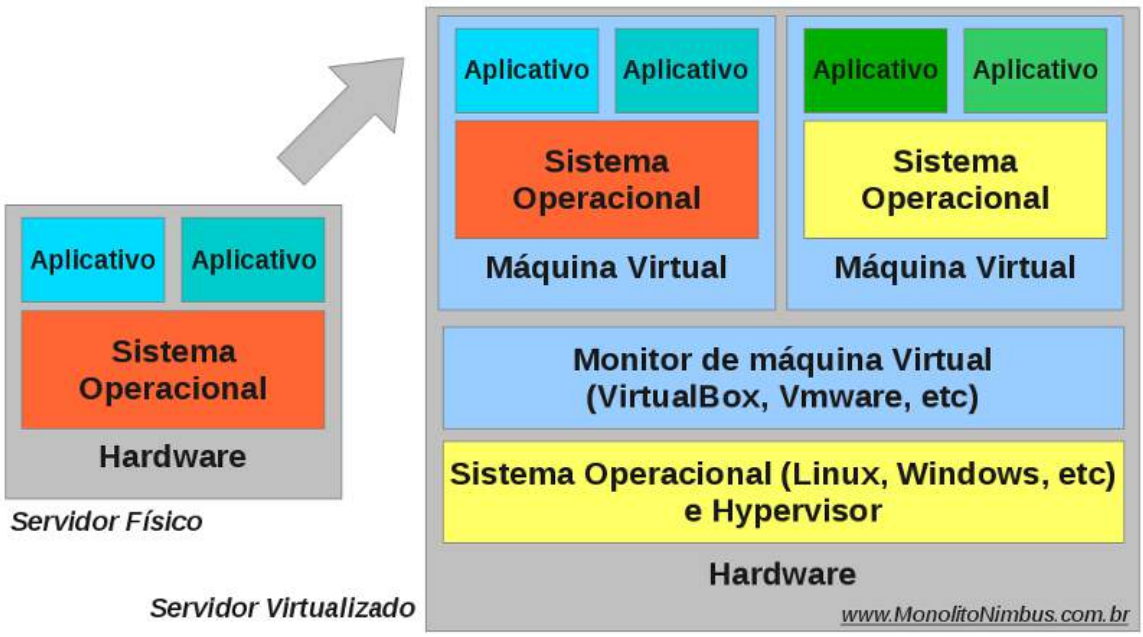


Figura 120 Esquema De una Máquina Virtual

Para el sistema operativo que se ejecuta dentro de la máquina virtual toda esta emulación es transparente e invisible. Todo funciona igual a si se estuviera ejecutando en un PC normal, sin que sepa que en verdad está metido dentro de una burbuja dentro de otro sistema operativo.

REQUERIMIENTOS MÍNIMOS PARA EJECUTAR VMWARE WORKSTATION

- Sistema operativo: Windows o Linux de 64 bits
- CPU (procesador):
- Para ejecutar máquinas virtuales de 32 bits: 64 bits y 1,3 GHz o más.
- Para ejecutar máquinas virtuales de 32 bits: los requerimientos anteriores junto con soporte VT-x si tienes un procesador Intel (asegúrate de que esté activado en el BIOS), o los requerimientos anteriores junto con soporte de modo largo si tienes un procesador AMD.
- RAM: lo mínimo es 1 GB, pero se recomienda tener 2 GB.
- GPU (unidad de procesamiento gráfico): al menos un adaptador de pantalla de 16 o 32 bits (lo más probable es que ya tengas un adaptador de pantalla de 32 bits). Si quieres que en tus máquinas virtuales de Windows funcionen los gráficos Windows Aero, entonces

debes tener una tarjeta gráfica NVIDIA GeForce 8800GT o superior, o una ATI Radeon HD 2600 o superior.

- Espacio disponible en el disco duro: se requieren 3,5 GB para instalar el programa solo, pero las máquinas virtuales ocuparán aún más espacio.

INSTALACIÓN DE MÁQUINA VIRTUAL VMWARE WORKSTATION

Para empezar con la instalación de VMware Workstation 10 ejecutamos el programa de instalación, en Windows 8.1 para que existan problemas en la posterior ejecución y creación de máquinas virtuales ejecutaremos el programa de instalación de la siguiente manera, seleccionamos el programa de instalación, VMware-workstation-full-10.0.0-1295980.exe, y pulsamos el botón derecho del ratón, nos aparece un menú con diferentes opciones, seleccionamos la opción 'Ejecutar como administrador', como se ve en la Figura 121 marcado con el recuadro verde, y se iniciará el instalador.

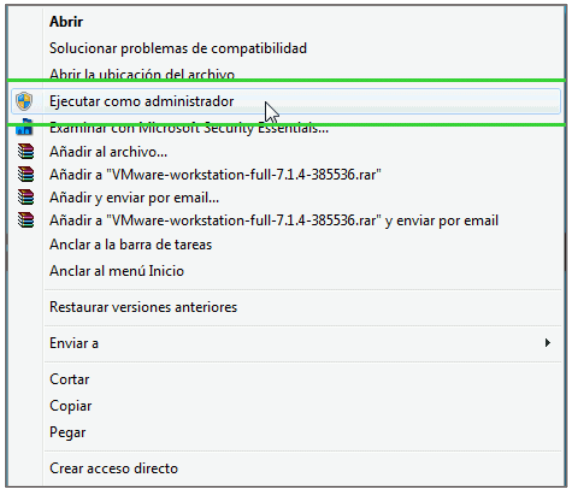


Figura 121 Ejecutar como administrador

Transcurridos unos segundos nos aparecerá esta ventana del asistente de instalación del VMware Workstation 12. Pulsamos sobre el botón next para iniciar la instalación, como se muestra en la figura 122.

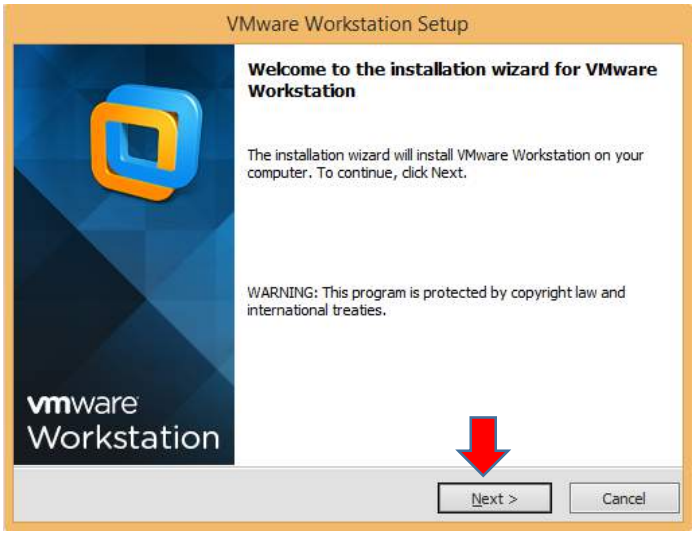


Figura 122 Asistente de Instalación.

En la siguiente ventana del asistente de instalación de VMware aparece el Acuerdo de Licencia del producto, aceptar el acuerdo y dar clic en el botón Next.

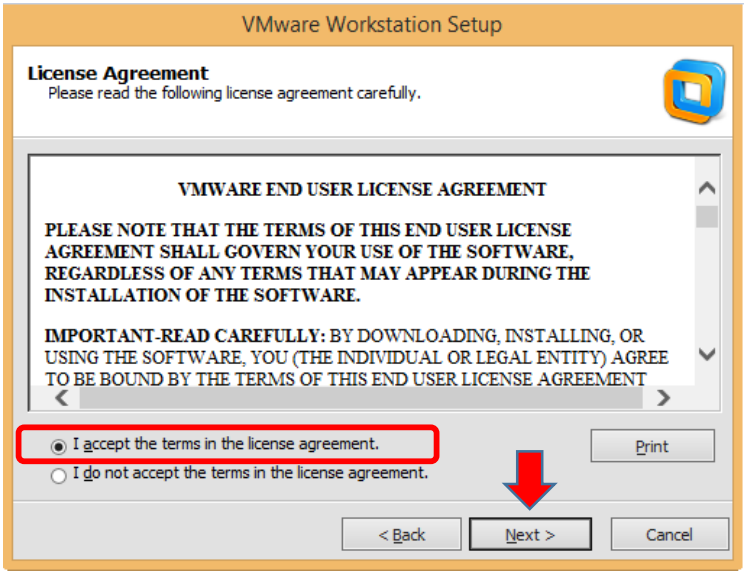


Figura 123 Acuerdo de Licencia.

La primera ventana del proceso de instalación nos brinda dos posibilidades para determinar cómo queremos realizar la instalación de VMware:
Typical, esta opción realizará la instalación de los componentes mínimos y necesarios para poder trabajar con VMware Custom, con esta opción podemos decidir la instalación de complementos o funciones adicionales para poder usar funcionalidades específicas de VMware.

Una vez hayamos decidido el tipo de instalación que vamos a realizar pulsamos sobre el botón adecuado, Tipical o Custom, como se muestra en la figura 124.

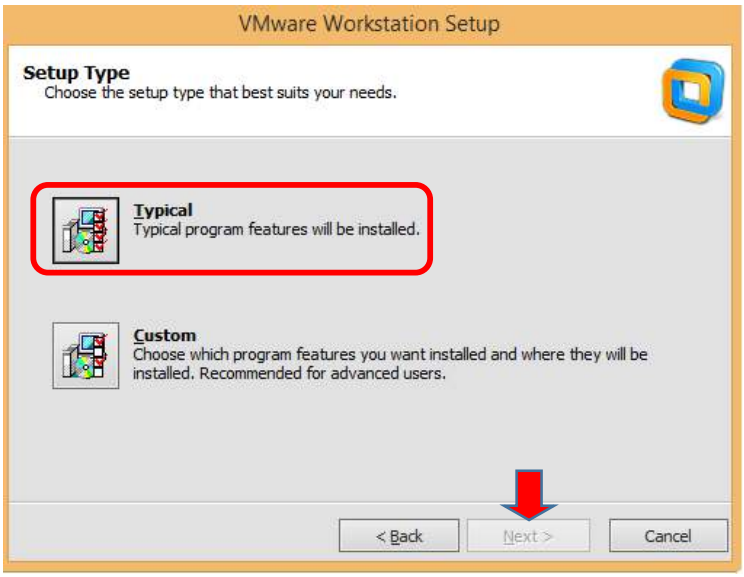


Figura 124 Setup Type.

En la figura 125 la opción Custom nos permitirá añadir 3 elementos adicionales a nuestro VMware, Visual Studio PlugIn, este plugin nos aporta la funcionalidad de interactuar con Visual Studio para desarrollo de aplicaciones con máquinas virtuales.

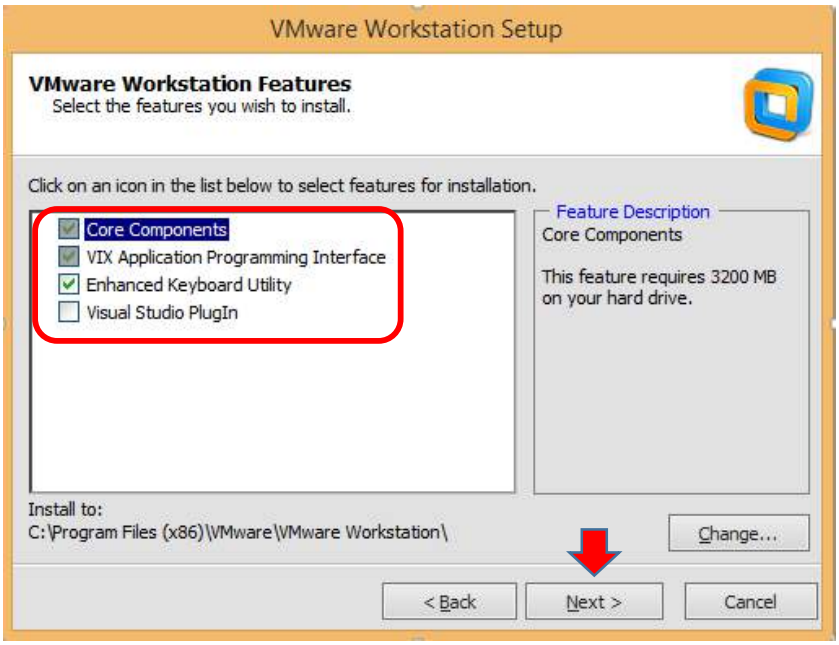


Figura 125 Selección de características.

Ahora nos aparece la información sobre el directorio donde se va a instalar el software, si lo deseamos podemos cambiar el directorio destino pulsando en el botón change, para continuar pulsamos el botón Next.

La figura 126 muestra la siguiente ventana del asistente nos permite determinar el directorio donde se podrá guardar las máquinas virtuales para compartirlas con otros usuarios, hacer clic sobre el botón Change... para cambiar el directorio para compartir, también se puede cambiar el puerto. Una vez establecido los valores pulsar el botón Next.

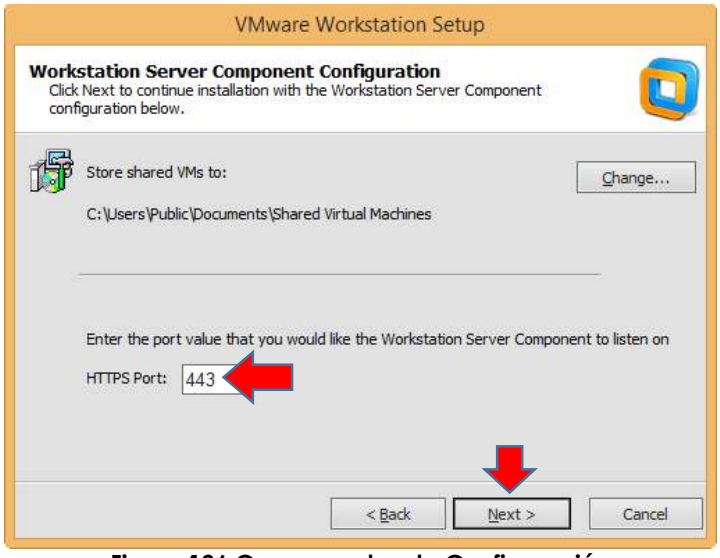


Figura 126 Componentes de Configuración

Software update, por defecto aparece chequeada la opción '*Check for product updates on startup*', esta opción hará que cada vez que se inicie el VMware realizará una comprobación sobre si hay actualizaciones del software e informará si hay disponibilidad de una nueva versión, si no quieres tener esa información deschequea la opción. Para continuar pulsamos el botón next, como se muestra en la figura 127.

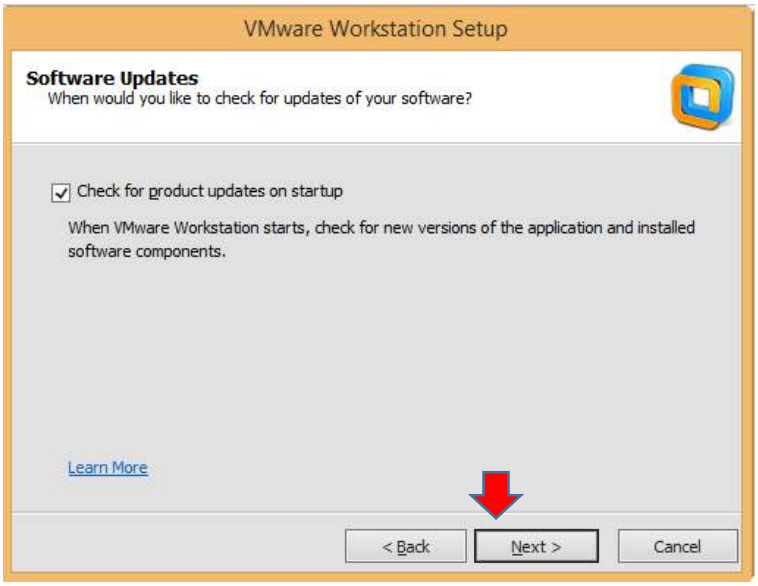


Figura 127 Actualización de Software.

User Experiences…, esta opción habilita a enviar información de tu sistema para labores de análisis de rendimiento, etc., si no deseas que esto ocurra deschequea la opción, para continuar pulsamos el botón Next, como se muestra en la figura 128.

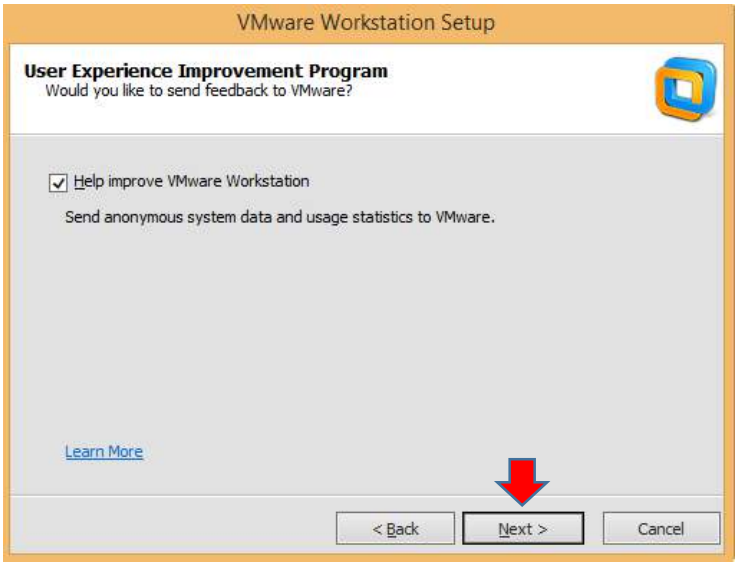


Figura 128 Experiencia de Usuario.

Shortcuts, aquí el asistente de instalación creará los iconos de VMWare en el escritorio, la carpeta de inicio y la barra de inicio rápido, si no deseas alguna de las opciones des chequéala. Para continuar pulsamos el botón Next, como se muestra en la figura 129.

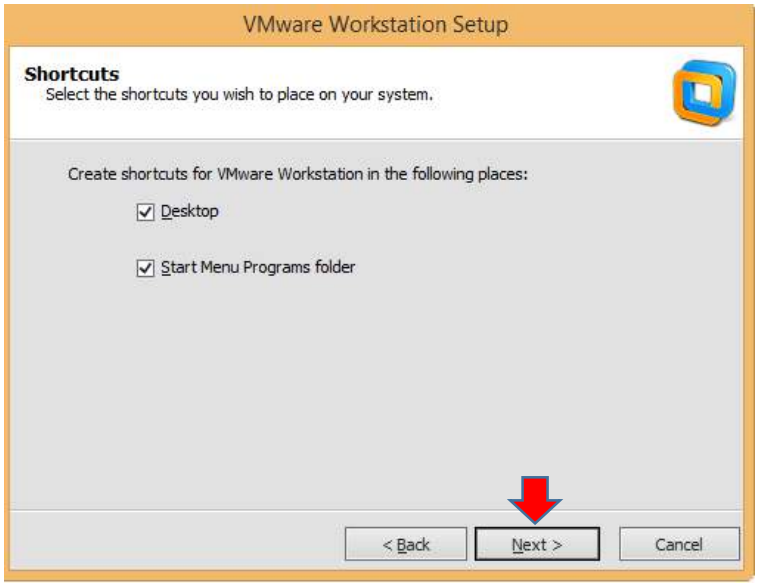


Figura 129 Atajos

El asistente nos informa que está preparado para realizar la instalación de VMware, pulsamos el botón Continue y se iniciará la instalación, como se muestra en la figura 130.

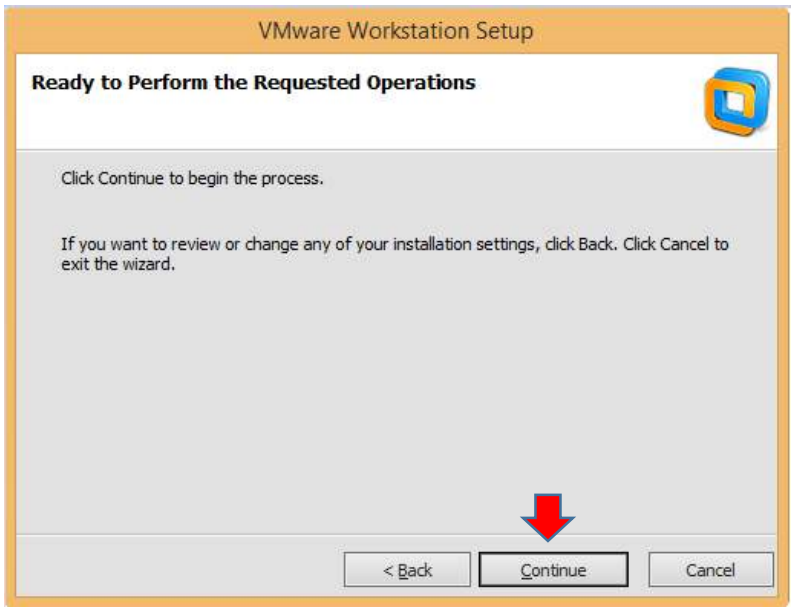


Figura 130 Iniciar Instalación.

La instalación se inicia e iremos viendo su progreso como se ve en la imagen, como se muestra en la figura 131.

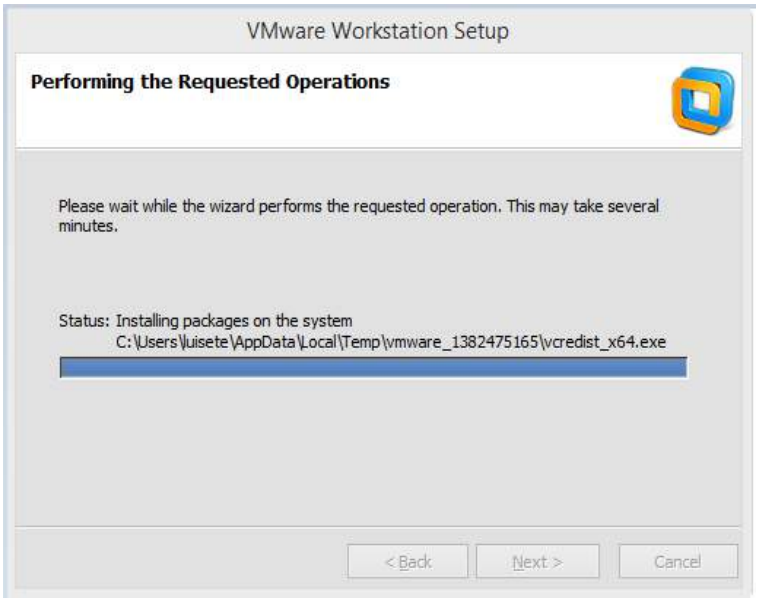


Figura 131 Progreso de Instalación.

Una ha finalizada la fase de instalación del software nos aparece una nueva ventana de instalador, en esta ventana introduciremos la clave de la licencia de VMware, una vez introducida pulsar el botón - Enter > -, en caso de que no tengas la clave de licencia pulsar el botón - Skip > - obtendras de 30 días de prueba.

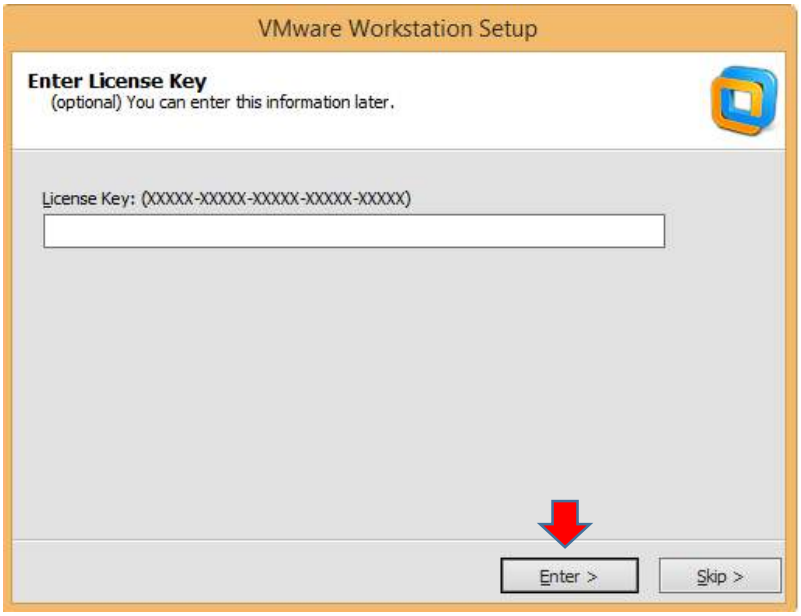


Figura 132 Licencia

La instalación de VMware ha terminado, ya se puede iniciar el VMware y aparecerá la ventana principal, como se muestra en la figura 133.

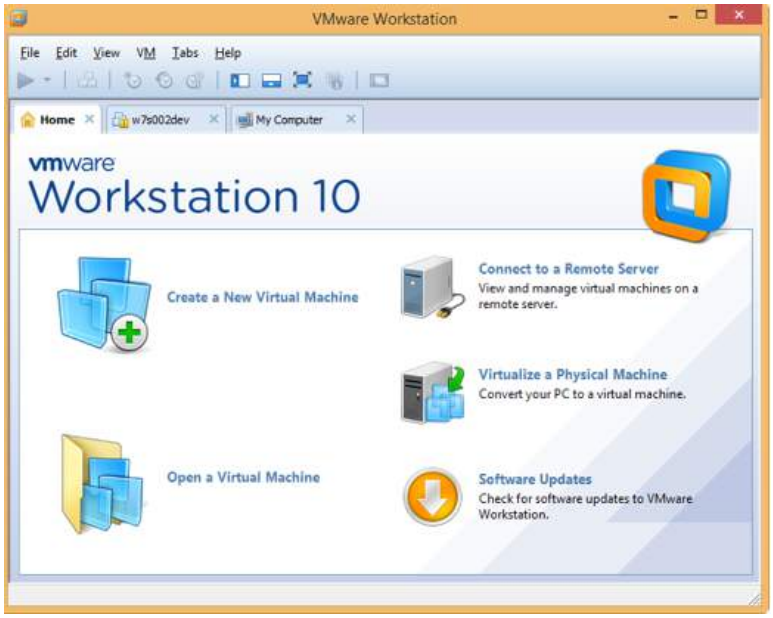


Figura 133 Ventana Principal.

PRÁCTICA IV: FTP Y SAMBA

SERVIDOR FTP

1. INSTALAR Y CONFIGURAR ARCHIVO VSFTPD

Paso 1

En primer lugar, debemos actualizar el sistema para comprobar si hay nuevas mejoras a los paquetes que tenemos instalados y para ello usaremos el siguiente comando:

- sudo yum check-update

Nota
Recordemos que si hemos iniciado sesión **como usuarios root** no debemos anteponer el sudo. En base a las actualizaciones disponibles seleccionamos la que necesitemos.

Paso 2

Sabemos que vsftpd es un servicio que trae por defecto el sistema operativo CentOS 7 y es el que nos da la posibilidad de gestionar todo lo relacionado con el protocolo FTP. Dentro de las principales características que tenemos al usar vsftpd tenemos:

Características vsftpd

- Conectividad IPv6
- Usuarios virtuales
- Configuraciones IP virtuales
- Posibilidad de encriptación al usar el protocolo SSH para las conexiones
- Gran ancho de banda, entre otras.

Paso 3

Para instalar vsftpd en CentOS 7 usaremos el siguiente comando que se encuentra en la figura 134.

- sudo yum -y install vsftpd

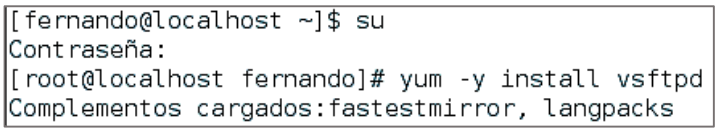


Figura 134. Instalación de vsftpd

Paso 4

Una vez hayamos instalado vsftpd de manera correcta todos los parámetros de configuración del servicio estarán alojados en la siguiente ruta.

- /etc/vsftpd/vsftpd.conf

Nota.- Recomendamos que antes de abrir el archivo y realizar los cambios en el archivo de vsftpd debemos crear una copia de seguridad en caso que algo anormal ocurra.

Paso 5

Para ello usaremos el siguiente comando:

- mv /etc/vsftpd/vsftpd.conf /etc/vsftpd/vsftpd.conf.org

Paso 6

A continuación, accederemos al archivo de configuración usando el editor nano, para ello ingresamos esta línea y veremos lo siguiente en la figura 135.

- sudo nano /etc/vsftpd/vsftpd.conf

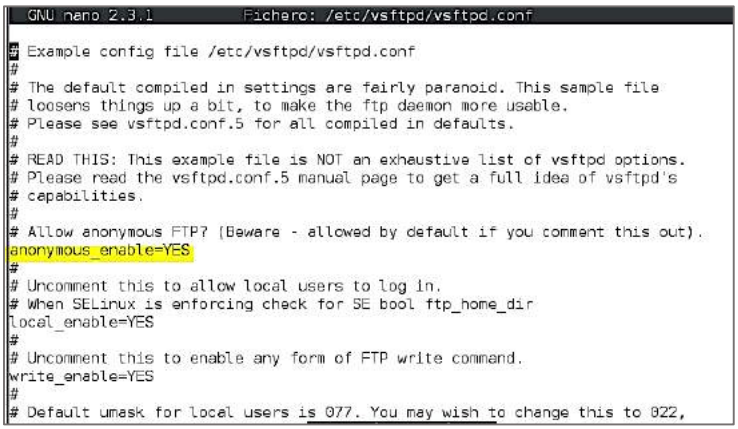


Figura 135. Acceso al archivo de configuración de vsftpd

Paso 7

El primer cambio a realizar es deshabilitar el acceso al usuario anónimo para incrementar la seguridad de nuestro servidor, para ello vamos a la línea 12 llamada.

- anonymous_enable=YES

Y la estableceremos como:

- anonymous_enable=NO

Paso 8

A continuación, quitamos el comentario (Símbolo #) a la línea 100 la cual se llama chroot_local_user=YES para restringir el acceso al directorio home.
Finalmente vamos al final del archivo y debemos añadir las siguientes líneas que nos permitirán habilitar el modo pasivo y permitir que el chroot sea escribible, como se muestra en la figura 136.

- allow_writeable_chroot=YES
- pasv_enable=Yes
- pasv_min_port=40000
- pasv_max_port=40100

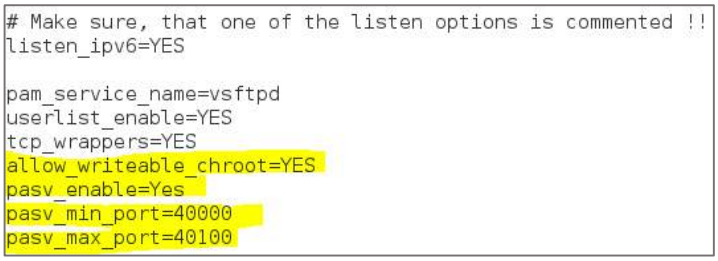


Figura 136. Restricción al directorio home

Paso 9

Guardamos los cambios usando la combinación de teclas

Ctrl + **O**

Y salimos del editor usando

Ctrl + **X**

2. REINICIAR ARCHIVO VSFTPD EN LINUX

Paso 1

Cada vez que se realice alguna modificación en el archivo de configuración debemos reiniciar el servicio para que los cambios sean aplicados, para ello usaremos el siguiente comando:

- systemctl restart vsftpd.service

Paso 2

Y el siguiente comando nos permitirá iniciar de manera automática vsftpd después del reinicio, como se aprecia en la figura 137:

- systemctl enable vsftpd.service

Figura 137. Iniciar de manera automática vsftpd

3. PERMITIR ACCESO DEL SERVICIO DE FTP EN EL FIREWALL EN CENTOS 7

El siguiente paso consiste en permitir que el Firewall habilite el acceso vía FTP y para ello debemos autorizar los puertos por los cuales se realizará la comunicación.

Paso 1

Para ello ingresamos el siguiente comando:

- sudo firewall-cmd --permanent --add-service=ftp

Posteriormente recargamos el servicio usando el comando que se encuentra en la figura 138.

- sudo firewall-cmd –reload

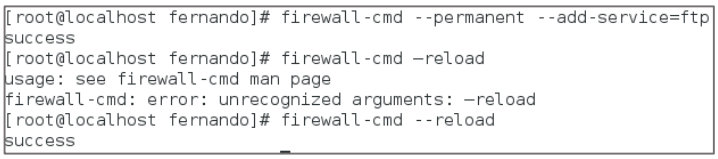


Figura 138. Permitiendo el servicio de FTP

Paso 2

Recordemos que SEinux (Security-Enhanced Linux) es un módulo de seguridad que permite aplicar políticas de seguridad para el acceso de los usuarios. Para habilitarlo en CentOS 7 ingresaremos el siguiente comando:

- sudo setsebool allow_ftpd_full_access on

De esta forma hemos habilitado permisos de FTP dentro de CentOs 7.

4. CREAR EL USUARIO PARA EL ACCESO POR FTP A CENTOS 7

A continuación, crearemos el usuario ftp_acc el cual será el usuario a utilizar para acceder vía FTP a CentOS 7 y lo crearemos en la ruta /sbin/nologin para evitar que el Shell acceda al servidor.

Paso 1

En este caso ingresaremos lo siguiente:

- sudo useradd -m ftp_acc -s /sbin/nologin

Paso 2

Establecemos la contraseña usando el comando passwd.

- sudo passwd ftp_acc

Paso 3

En este punto ya podemos conectarnos usando algún cliente como Putty, Filezilla, etc., usando el puerto 22.

PuTTY es un cliente SSH y Telnet con el que podemos conectarnos a servidores remotos iniciando una sesión en ellos que nos permite ejecutar comandos. El ejemplo más claro es cuando empleamos PuTTY para ejecutar comandos en un servidor VPS y así poder instalar algún programa o configurar alguna parte del servidor.

PuTTY se puede descargar directamente desde su página oficial, que no luce un gran diseño, pero nos permite descargar PuTTY gratis e incluso otras aplicaciones complementarias.
Ventajas de PuTTY

Una pregunta que puede surgir es ¿por qué usar PuTTY? ¿Cuáles son sus ventajas? Esta aplicación es como todas, tiene sus partes buenas y partes malas, pero si es cierto que mayormente tiene grandes ventajas como las siguientes:

- Es gratuito y de código abierto.
- Disponible para varias plataformas (Windows y Linux).
- Es una aplicación portable.
- Interfaz sencilla y manejable.
- Muy completo y ofrece una gran flexibilidad con multitud de opciones.
- Está en constante desarrollo.

USO BÁSICO DE PUTTY

Tras ejecutar PuTTY se muestra el apartado Session con las opciones básicas y tan sólo hay que:

- Introducir la IP o Hostanme del servidor remoto.
- Seleccionar el puerto (normalmente para conectar a través de SSH es el 22 por defecto).
- Seleccionar en connection type la opción SSH (ya suele venir marcada por defecto).
- Hacemos click en el botón Open.
- Puede que se nos muestre alguna advertencia, la cual aceptamos y tras unos segundos nos solicitará nuestro nombre de usuario y contraseña para iniciar sesión en el servidor remoto.

Paso 1
Click en Next para empezar con la instalación de PuTTY, como se muestra en la figura 139.

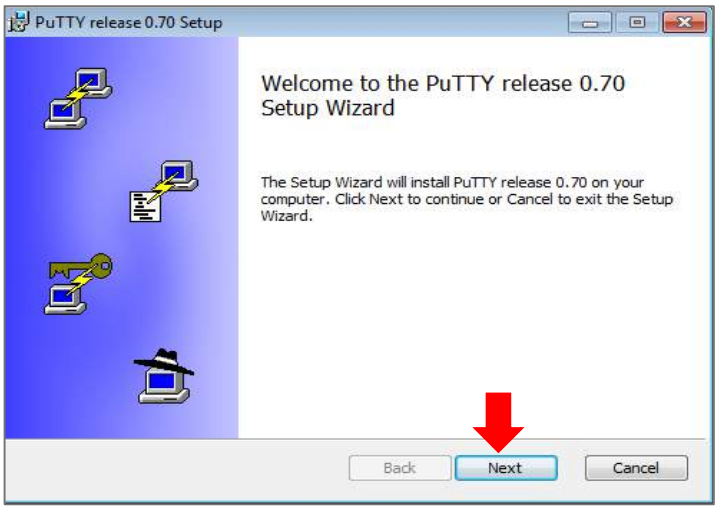


Figura 139. Instalación de PuTTY

Paso 2

Instalar los archivos de PuTTY, seleccionando la opción que se muestra en la figura 140, y luego click en install.

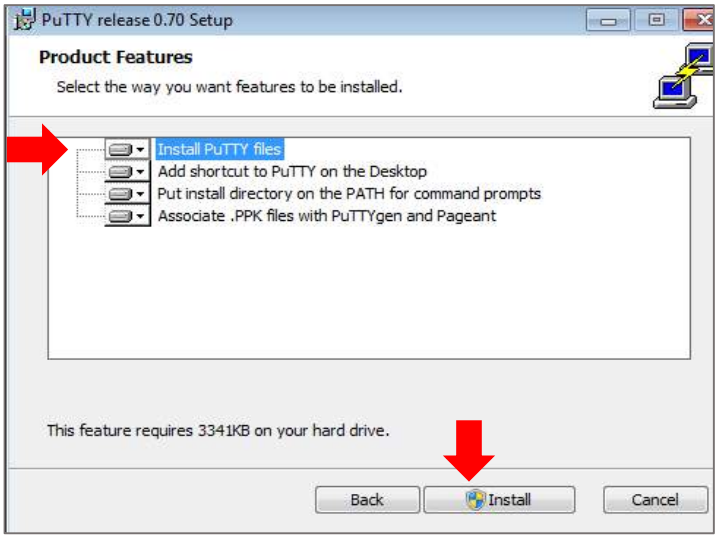


Figura 140. Instalación se archivos PuTTY

Paso 3
Se procede a digitar la Ip y el puerto correspondiente, luego se selecciona la opción SSH, dejando lo demás por default dando click finalmente en Open; como se muestra en la figura 141.

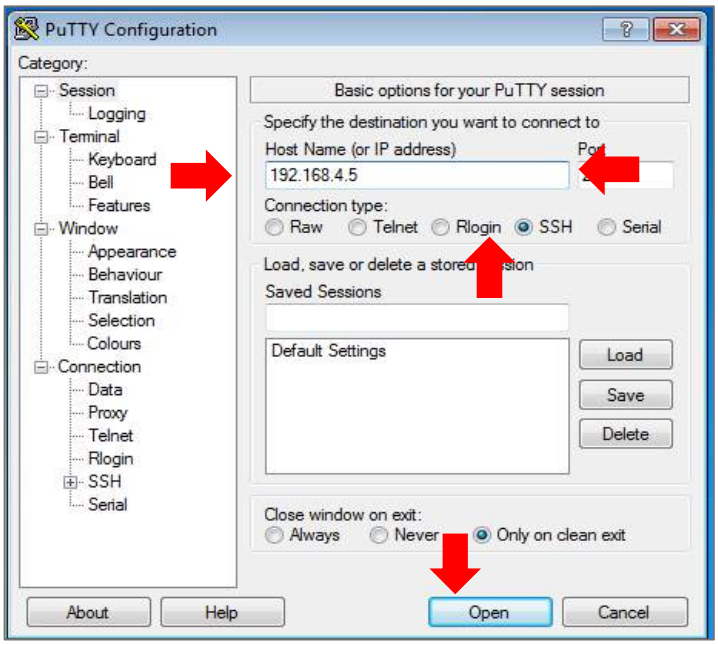


Figura 141. Ingreso de IP y puertos en PuTTY

Paso 4

Se ingresa las credenciales con el usuario recién creado. Se puede acceder de forma segura y rápida al servidor FTP en CentOS 7, como se aprecia en la figura 142.

```
login as: fernando
fernando@192.168.4.5's password:
Last failed login: Thu Jul 27 00:17:12 ECT 2017 from :0 on :0
There was 1 failed login attempt since the last successful login.
Last login: Wed Jul 26 23:30:45 2017
[fernando@localhost ~]$ ls
Descargas   Escritorio  Música      Público
Documentos  Imágenes    Plantillas  Videos
[fernando@localhost ~]$ cd documentos
-bash: cd: documentos: No existe el fichero o el directorio
[fernando@localhost ~]$ cd Documentos
[fernando@localhost Documentos]$ ls
apache
[fernando@localhost Documentos]$
```

Figura 142. Ingreso de credenciales

SAMBA

La instalación se realizará sobre una distribución de Linux Centos 7.

1. Verificar si disponemos de los paquetes de Samba:
   - rpm -qa | grep samba

2. Si disponemos de alguna versión ya instalada, procedemos a eliminarla para posterior instalar una versión más reciente como se muestra en la figura 143.

- yum erase samba*
- yum -y install samba*

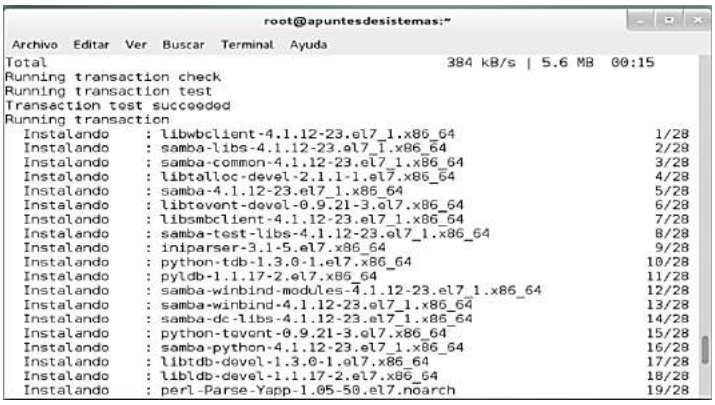


Figura 143. Verificación de disponibilidad de paquetes de Samba

3. Creamos una carpeta para compartirla en nuestra red. (En este caso se la creará en la raíz).

- mkdir -p /samba/publico

4. Como la carpeta será de acceso general le asignamos todos los permisos:

- chmod -R 777 /samba/publico

5. Modificamos la configuración general de Samba:

- vim /etc/samba/smb.conf

- Dentro del contexto [global], se realizan cambios que se aprecian en la figura 144:

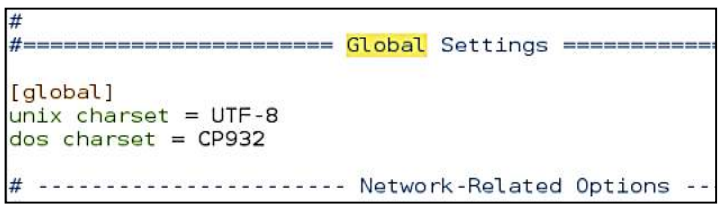


Figura 144. Configuración general de Samba

- En la sección Network-Related Options, se debe buscar el parámetro workgroup para asignarle el nombre del grupo de trabajo de la red windows.

Descomentar (borrar el punto y coma del inicio) la línea hosts allow y escribir la dirección de red desde la cual se quiere permitir el acceso a los recursos compartidos de samba, como se ve en la figura 145.

Figura 145. Descripción del equipo y grupo de trabajo de Samba

Definir los protocolos a usar, como se muestra en la figura 146.

```
# max protocol = used to define the supported protocol. The default is NT1. You
# can set it to SMB2 if you want experimental SMB2 support.
#
        workgroup = SOPTEC
        server string = Samba Server Version %v

;       netbios name = MYSERVER

;       interfaces = lo eth0 192.168.12.2/24 192.168.13.2/24
        hosts allow = 127. 192.168.0. 192.168.0.

;       max protocol = SMB2
```

Figura 146. Protocolos a utilizar

- En la sección Standalone Server Options, incluir una línea para el manejo del usuario "invitado", como se aprecia en la figura 147.

```
# ----------------------- Standalone Server Options ------------------------
#
# security = the mode Samba runs in. This can be set to user, share
# (deprecated), or server (deprecated).
#
# passdb backend = the backend used to store user information in. New
# installations should use either tdbsam or ldapsam. No additional configuration
# is required for tdbsam. The "smbpasswd" utility is available for backwards
# compatibility.
#
        security = user
        map to guest = Bad User
        passdb backend = tdbsam
```

Figura 147. Manejo de usuario invitado

- Al final del fichero en la sección Share Definitions se crea el contexto del recurso compartido y se debe salir del vim guardando los cambios (:wq). En este caso la carpeta a compartir se llama público, como se puede apreciar en la figura 148.

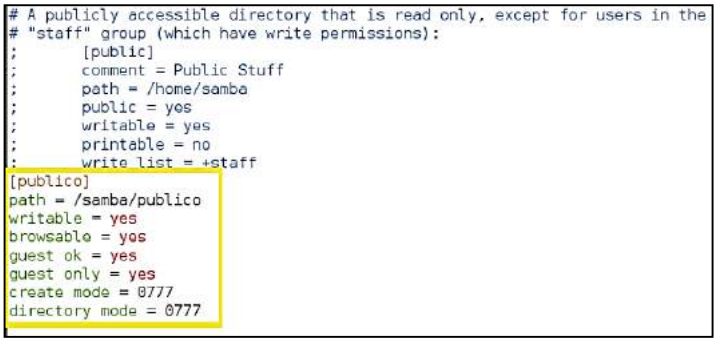


Figura 148. Creación del recurso compartido

6. Se inician los servicios y se los habilita para que arranquen automáticamente en cada inicio.

- systemctl start smb
- systemctl start nmb
- systemctl enable smb
- systemctl enable nmb

7. Se verifica que la configuración esté ejecutándose correctamente con el siguiente comando, que se muestra en la figura 149.

- Testparm

```
[global]
        workgroup = MYGROUP
        server string = Samba Server Version %v
        log file = /var/log/samba/log.%m
        max log size = 50
        dns proxy = No
        cups options = raw
        security = share
        guest account = nobody
[homes]
        comment = Home Directories
        read only = No
        browseable = No

[printers]
        comment = All Printers
        path = /var/spool/samba
        printable = Yes
        browseable = No

[shared]
        comment = Shared Stuff Without username/password
        path = /shared/
        read only = No
        guest ok = Yes
```

Figura 149. Verificación de configuración en ejecución

8. Se habilitan los puertos que requiere samba para su correcto funcionamiento, el 137, 138, 139, 445 y el 901:

- firewall-cmd –permanent –add-port=137/tcp
- firewall-cmd –permanent –add-port=138/tcp
- firewall-cmd –permanent –add-port=139/tcp
- firewall-cmd –permanent –add-port=445/tcp
- firewall-cmd –permanent –add-port=901/tcp

9. Se reinicia el firewall:

- firewall-cmd –reload

10. Se habilita los permisos para la compartición de archivos con el siguiente comando:

- setsebool -P samba_enable_home_dirs on

11. Habilitar el acceso a la carpeta compartida:

- chcon -t samba_share_t /samba/publico/

12. Ingresar desde una máquina con windows al recurso compartido de linux a través de la ip, como se aprecia en la figura 150.

```
[root@apuntesdesistemas ~]# setsebool -P samba_enable_home_dirs on
[root@apuntesdesistemas ~]# chcon -t samba_share_t /samba/publico/
[root@apuntesdesistemas ~]# ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet6 fe80::a00:27ff:fed0:f9c4  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:d0:f9:c4  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 687  bytes 122202 (119.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

enp0s8: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.170  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fe80::a00:27ff:fe4d:b163  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:4d:b1:63  txqueuelen 1000  (Ethernet)
        RX packets 132833  bytes 163017019 (155.4 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 38219  bytes 2579336 (2.4 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Figura 150. Ingreso desde una PC al ingreso compartido de Linux

Se ejecuta la IP, como se muestra en la figura 151:

Figura 151. Ejecución de la IP

Creación de la carpeta de acceso público, que se muestra en la figura 152.

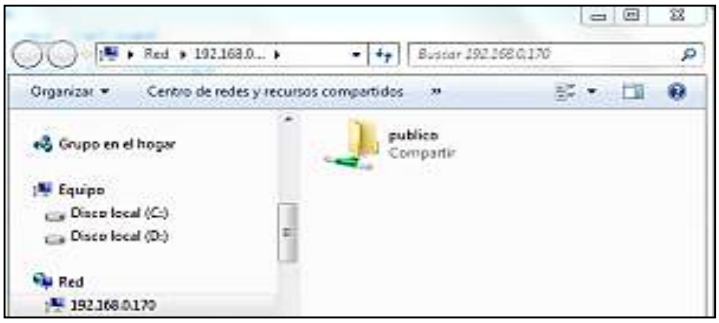


Figura 152. Carpeta de acceso público

Con esto tenemos una carpeta de acceso público, sin contraseña, en nuestro servidor linux. Si se desea crear un recurso con acceso a un usuario especifico, se cambiarían unos detalles en la configuración del smb.conf

1. Creamos un contexto que haga referencia a la carpeta específica que deseamos compartir para el usuario requerido.
2. Si no está creada la carpeta a compartir lo hacemos y le asignamos permisos al usuario
   - mkdir /admin
   - chown lpi:lpi /admin
3. Creamos el usuario en samba con el comando smbpasswd -a:
   - smbpasswd -a lpi
   - Escribimos y confirmamos la contraseña
4. Reiniciamos los servicios smb y nmb.
5. Listo, probamos el funcionamiento.

PRÁCTICA V: MONITOREO

MONITOREO DE RED

El término Monitoreo de red (Monitorización de red) describe el uso de un sistema que constantemente monitoriza una red de computadoras en busca de componentes defectuosos o lentos, para luego informar a los administradores de redes mediante correo electrónico, pacer u otras alarmas. Es un subconjunto de funciones de la administración de redes.

PANEL DE ADMINISTRACIÓN DE ENDIAN

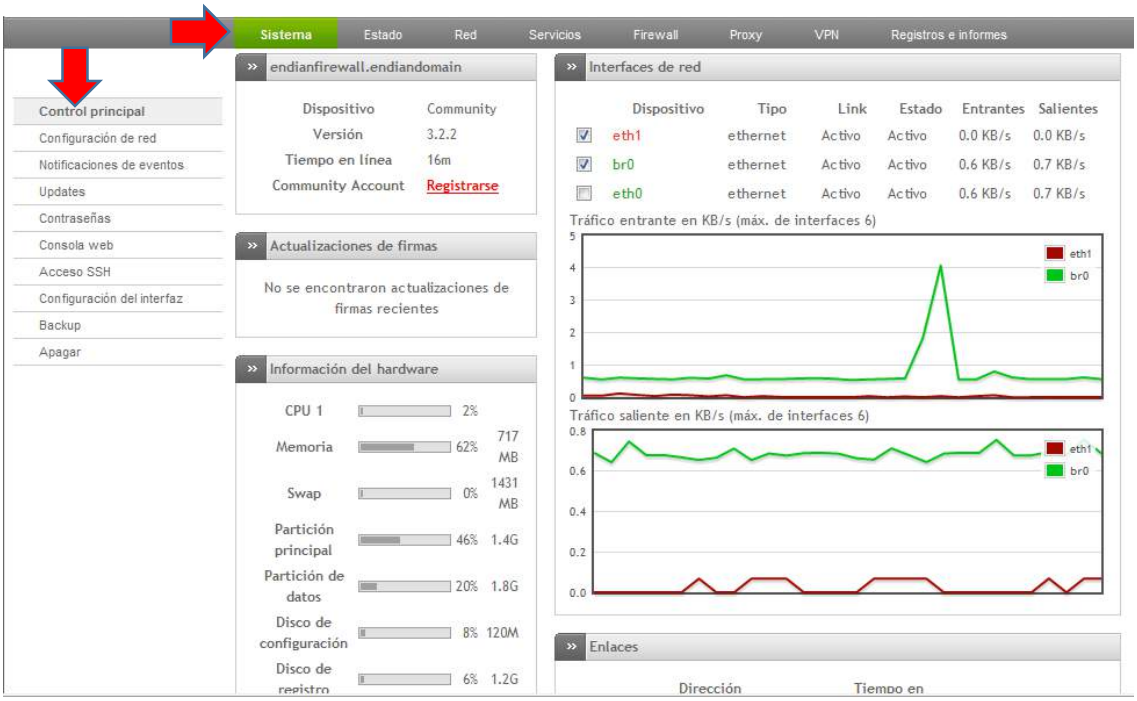


Figura 153 Panel de administración de Endian.

Endian Firewall Comunity, tiene una interfaz administrativa Grafica, donde se administran los servicios de Red, Firewall, Proxy, VPN, Antispam, Antivirus, QoS, Balanceo de carga, Multiwan (2 Proveedores de Internet), Sistema de Detección de Intrusos.

Desde el panel de administración como lo muestra la figura 153 se puede monitorear los servidores en tiempo real.

En la figura 154 nos muestra el Nombre del Endian que configuramos en la instalación así como también la versión instalada y el tiempo que tiene de conexión.

Figura 154 características.

Actualizaciones de firmas: nos indicara si hay alguna actualización de las firmas como nos muestra la figura 155.

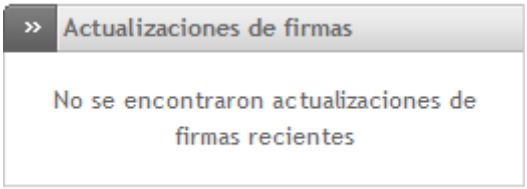


Figura 155 Actualización de firmas.

Información del Hardware: Aquí nos mostrará el estado del CPU, memoria, unidades de discos duros, estos se actualizarán "n" segundos según su configuración, tal como lo muestra la Figura 156.

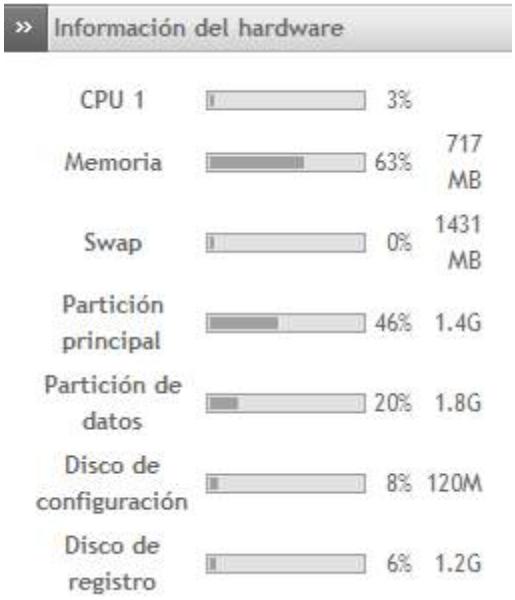


Figura 156 información de hardware.

Log de Servicios: Aquí podemos visualizar el estado de los servicios tales como la detección de intrusos y el tráfico HTTP. De una manera muy intuitiva.

Figura 157 log de servicios.

Interfaces de Red: Nos muestra el tráfico en tiempo real de las interfaces de red del servidor, el número de graficas varia en base al número de tarjetas de red instaladas. (eth0, eth1,br0)

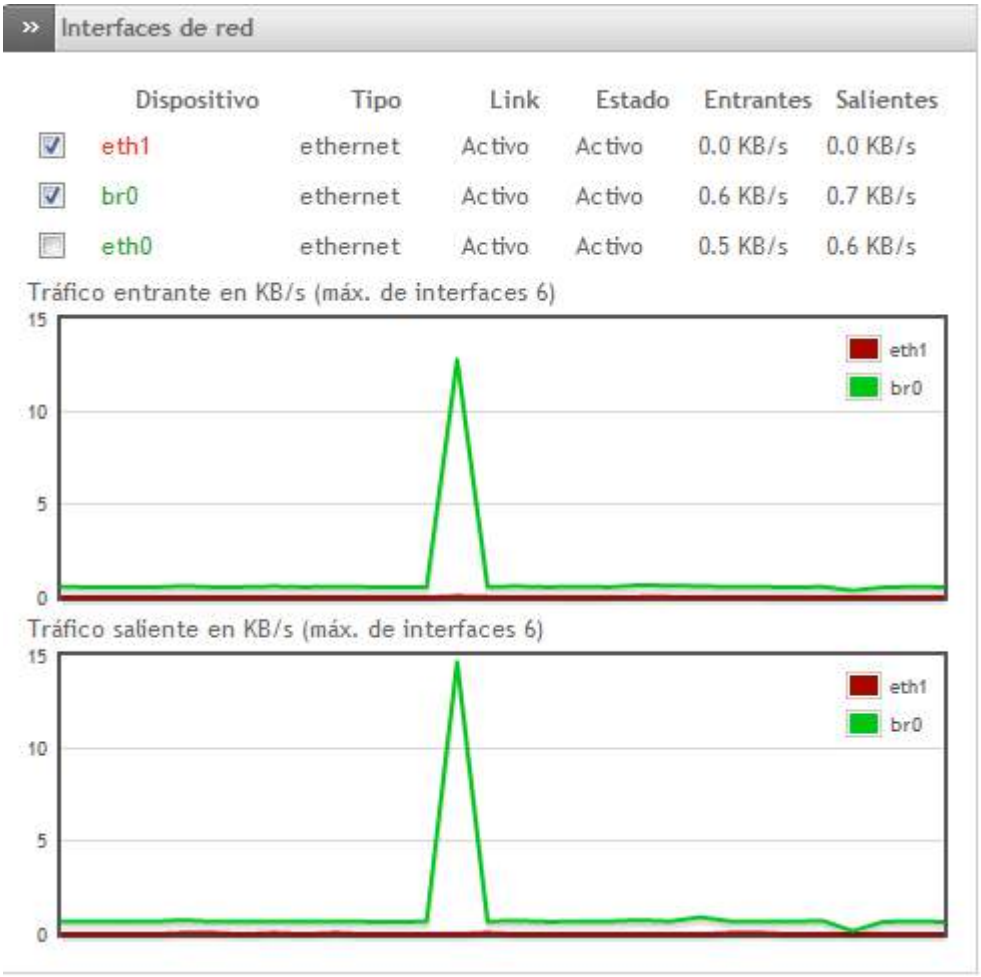


Figura 158 Interfaz de red.

Enlaces Activos: Nos muestra la información del enlace a internet.

Figura 159 Enlaces Activos.

FIREWALL - POLÍTICAS DE ACCESO

Figura 160 Firewall Políticas de Accesos.

El firewall puede ser configurado fácilmente desde su administrador web. En este panel podemos apertura puertos entrantes y salientes, hacer Nat y forwarding

Reenvío de Puertos NAT: Permite crear reglas para redireccionar los puertos hacia un servidor local.

Tráfico de Salida: Permite crear reglas de puertos de salida hacia internet, por defecto las computadoras solo pueden acceder a páginas web y enviar correos.

Tráfico entre Zonas: Permite crear reglas de navegación entre zonas del firewall, solo está disponible si el servidor tiene más de 3 tarjetas de red.

Tráfico VPN: Permite habilitar el tráfico para clientes VPN, esta regla permite habilitar un cortafuegos para los usuarios VPN.

PROXY - CONFIGURACIÓN HTTP

Figura 161 Configuración Proxy.

El proxy de Endian se configura a través de autenticación e integración con active directory, con esto nos permite darle mayor seguridad a los usuarios cuando navegan al internet.

La configuración para el proxy HTTP permite ser configurado de modo transparente, asi las computadoras de la red pasarán por el proxy de manera automática, se configura a través de autenticación e integración con active directory, con esto nos permite darle mayor seguridad a los usuarios cuando navegan al internet.

Configuración: Permite configurar los puertos web que tendrán acceso a través del proxy, también se define los registros Log.

Políticas de Acceso: Permite crear niveles de acceso a internet, se puede filtrar el acceso por MAC o IP.

Filtro de Contenido: Permite crear reglas de filtrado, palabras o sitios que sean bloqueados por el proxy.

REPORTES - LOG DEL SISTEMA

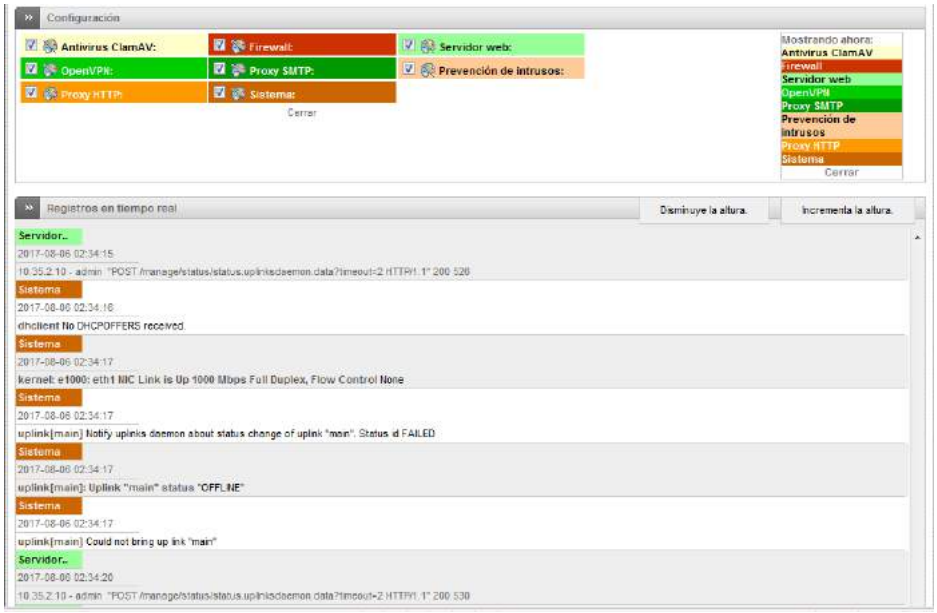


Figura 162 Log del sistema.

El Reporte es por usuario, indica la hora, fecha y tiempo que estuvo en el internet, permite visualizar reportes de navegación y el log de servicios en tiempo real.

Esta herramienta permite detectar y depurar la navegación web y los puertos abiertos.

Conexiones VPN: Esta Grafica indica los puntos remotos y usuarios conectados a través de la VPN

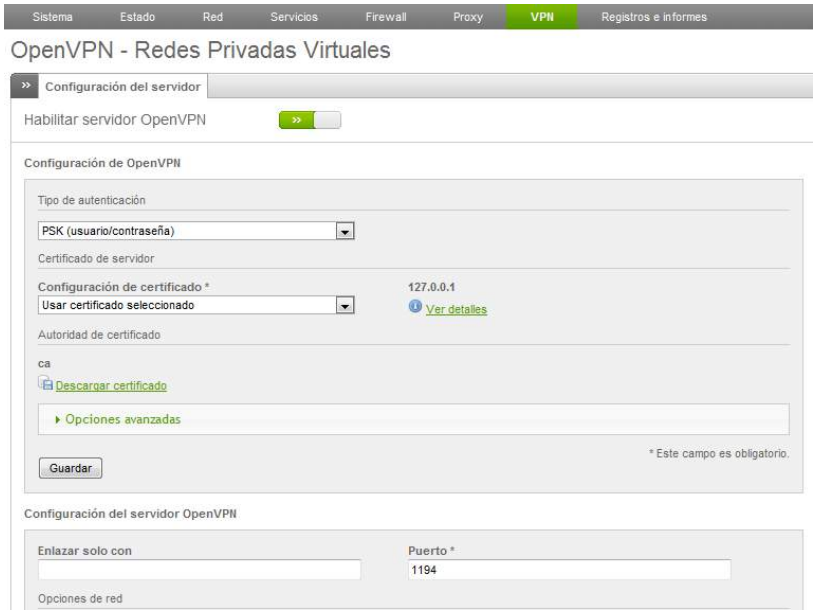


Figura 163 Redes VPN.

INFORMACIÓN DE ESTADO DEL SISTEMA

En la pestaña estado nos aparece la información de los servicios que tengan la red, el estado de la memoria, el uso en tiempo real del disco, el tiempo de servicio y usuarios, los módulos que se han cargado y por último la versión del kernel.

Figura 164 Información del Sistema parte 1

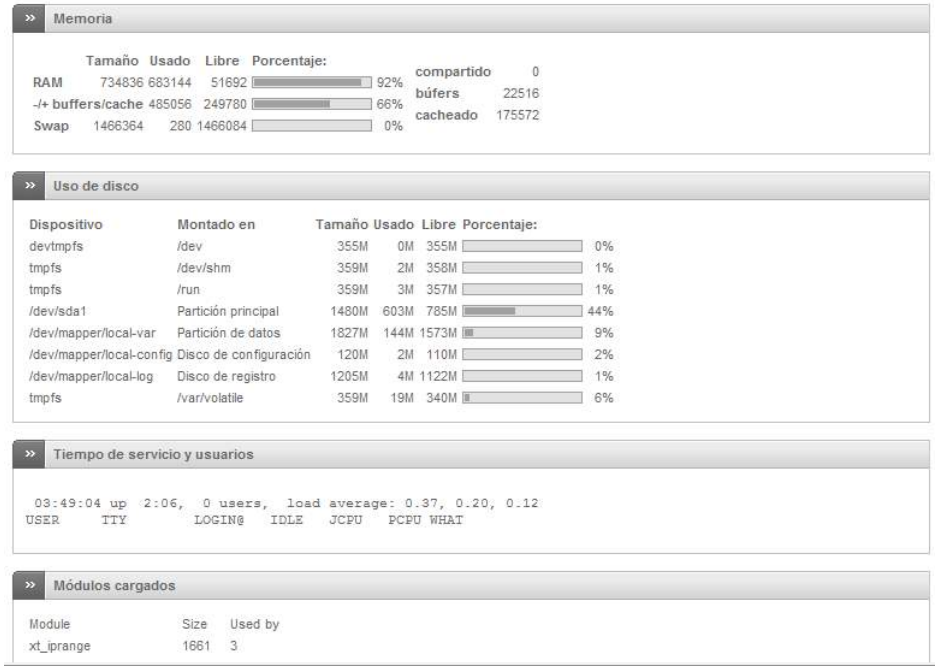


Figura 165 Información del Sistema parte 2

INFORMACIÓN DEL ESTADO DE RED

Aquí se podrá apreciar toda la información y estado de las interfaces , las asignaciones de ip actuales , el estado de las NIC , las entradas de la tabla ARP , todos de una amigable.

Información del estado de la red

Interfaces | Asignaciones dinámicas actuales | Estado de NIC | Entradas de la tabla de enrutamiento | Entradas de la tabla ARP

» Interfaces

```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,PROMISC,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast master br0 state UP qlen 1000
    link/ether 00:0c:29:3f:07:17 brd ff:ff:ff:ff:ff:ff
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether 00:0c:29:3f:07:21 brd ff:ff:ff:ff:ff:ff
6: br0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP
    link/ether 00:0c:29:3f:07:17 brd ff:ff:ff:ff:ff:ff
    inet 10.35.2.2/24 brd 10.35.2.255 scope global br0
       valid_lft forever preferred_lft forever
7: tap0: <BROADCAST,MULTICAST,PROMISC,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast master br0 state UP qlen 100
    link/ether a6:83:e8:8c:d8:d9 brd ff:ff:ff:ff:ff:ff
```

» Asignaciones dinámicas actuales

#	Dirección IP	Dirección MAC	Nombre del host	Caducidad de asignación (local time d/m/y)
1	10.35.2.135	00:0c:29:8e:b2:a8		~~24/07/2017 17:23:10~~
2	10.35.2.133	00:0c:29:8e:b2:b2		~~25/07/2017 01:01:02~~
3	10.35.2.129	00:0c:29:28:91:95		~~24/07/2017 10:05:09~~
4	10.35.2.132	00:0c:29:b2:45:03		~~24/07/2017 17:10:36~~
5	10.35.2.3	00:0c:29:a0:e6:c3		~~24/07/2017 11:09:34~~

Figura 166 Interfaces de Red.

» Estado de NIC

```
1) eth0: Intel Corporation 82545EM Gigabit Ethernet Controller (Copper) (rev 01) - 00:0c:29:3f:07:17 [Enlace
   Velocidad: 1000Mb/s  Completo Doble
   Soporte para negociación automática: Sí  Publicitado  Activado
   Modos de enlaces publicitados:  10baseT/Half 10baseT/Full 100baseT/Half 100baseT/Full 1000baseT/Full
   Modos de enlaces compatibles:  10baseT/Half 10baseT/Full 100baseT/Half 100baseT/Full 1000baseT/Full
2) eth1: Intel Corporation 82545EM Gigabit Ethernet Controller (Copper) (rev 01) - 00:0c:29:3f:07:21 [Enlace
   Velocidad: 1000Mb/s  Completo Doble
   Soporte para negociación automática: Sí  Publicitado  Activado
   Modos de enlaces publicitados:  10baseT/Half 10baseT/Full 100baseT/Half 100baseT/Full 1000baseT/Full
   Modos de enlaces compatibles:  10baseT/Half 10baseT/Full 100baseT/Half 100baseT/Full 1000baseT/Full
```

» Entradas de la tabla de enrutamiento

```
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
10.35.2.0       0.0.0.0         255.255.255.0   U     0      0        0 br0
```

» Entradas de la tabla ARP

```
Address                  HWtype  HWaddress           Flags Mask            Iface
10.35.2.10               ether   00:0c:29:28:91:95   C                     br0
```

Figura 167 estados del NIC Tabla de enrutamiento.

GRÁFICOS DE RED

Permitirán ver el tráfico según la red (roja-verde-naranja) de una manera grafica

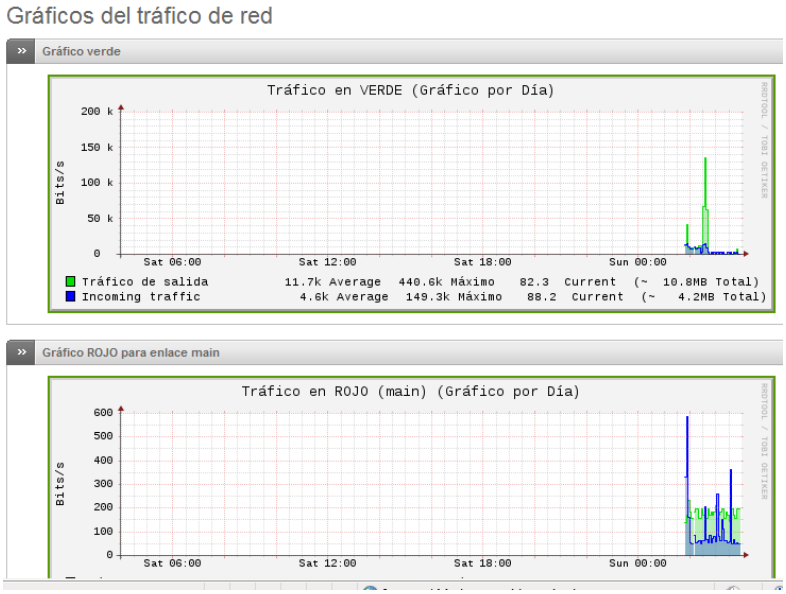


Figura 168 Gráficos de red.

CONEXIONES

Esta pestaña permite visualizar los seguimientos de las conexiones de las p tables en tiempo real.

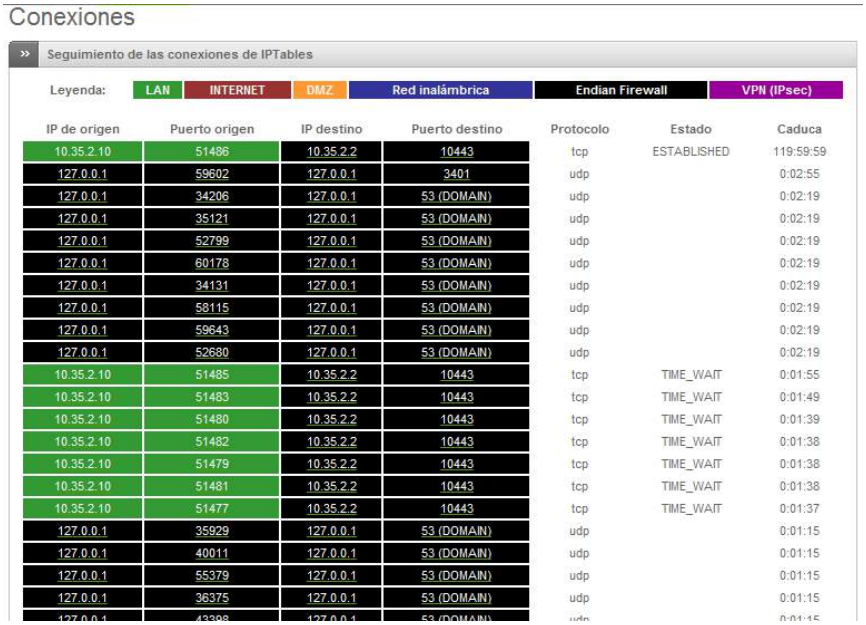


Figura 169 Conexiones.

CONEXIONES VPN

Nos permitirá ver los usuarios que estén conectados mediante VPN, en nuestro caso no tenemos ninguna conexión.

Figura 170 Conexiones VPN.

En la pestaña Registros e informes nos permitirán ver los registros de tráfico en tiempo real de los servicios.

Figura 171 Registros En Tiempo Real.

Bibliografía

[1]Endian, www.endian.com

[2]http://wiki.synaptic.cl/wiki/HowTo_Install_Endian#Requisitos_M.C3.ADnimos_para_instalaci.C3.B3n

[3*] Instalación y configuración de Firewall ENDIAN -SERVICIO NACIONAL DE APRENDIZAJE - DIEGO LEON GIL BARRIENTOS*

[4] *Endian UTM 3.2 Reference Manual — Endian UTM 3.2 Reference Manual.* http://docs.endian.com/3.2/utm/index.html, consultado el 25 de mayo del 2016

[5] *Endian - Secure everyThing: Firewall UTM, Hotspot, VPN, IoT.* http://www.endian.com/, consultado el 23 de mayo del 2016

[6]Guerra, G. J. T., & Guerra, A. G. (1999). *Herramienta de gestión de servidores Samba sobre Linux vía WWW*. Escuela Universitaria de Ingeniería Técnica de Telecomunicación.

[7]González Obando, C. D., Dota, Y., & Antonio, H. (2009). Implementación de un servidor de archivos Linux configurado con SAMBA.

[8]Cholanco, N., & Anibal, J. (2009). *Implementación de un proxy en plataforma linux para el control de transferencia de archivos con FTP, E-mail y Firewall* (Bachelor's thesis, QUITO/EPN/2009).

[9]Montalván Mendoza, E. D., & Cartagena Oñate, M. A. (2009). Manual e implementación de un servidor Hosting utilizando Linux para que residan Páginas Web.

[10]Gonzaga Gonzaga, E. M. (2008). *Tutorial para la implementación de un Firewall usando Linux como sistema operativo e iptables y control de ancho de banda* (Bachelor's thesis, Universidad del Azuay).

ISBN: 978-9942-770-36-3

compAs