Instalación desde un DVD/CD-ROM

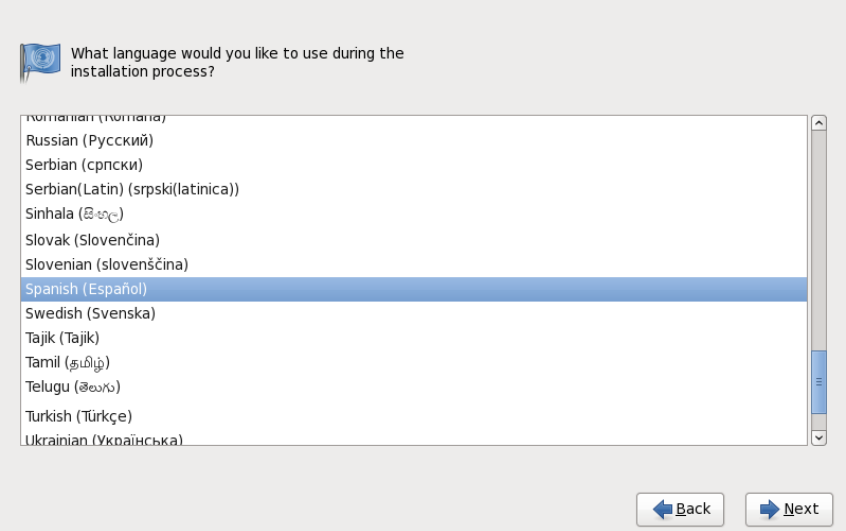
Para instalar Fedora desde un DVD/CD-ROM, introduzca el DVD o CD #1 en el dispositivo de DVD/
CD-ROM e inicie su sistema desde DVD/CD-ROM.

Si el dispositivo de DVD/CD-ROM es encontrado y cargado, el programa de instalación le ofrecerá
la opción de revisar la integridad del DVD/CD-ROM. Este proceso tomará algún tiempo. Usted tiene la opción de saltarse este paso. Sin embargo, si luego encuentra problemas con el programa de instalación, usted deberá reiniciar la máquina y ejecutar la revisión del medio antes de solicitar soporte.

La pantalla de Bienvenida no le pide ninguna información.

Selección del lenguaje

El idioma que escoja aquí será el idioma predeterminado para el sistema operativo una vez lo instale. La selección del idioma apropiado también le ayudará a configurar el huso horario en una etapa posterior del proceso de instalación. El programa de instalación intentará definir el huso horario adecuado basándose en lo que usted especifique en la pantalla.

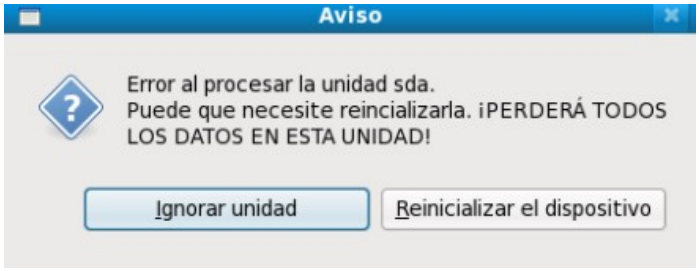


Seleccione configuración del teclado

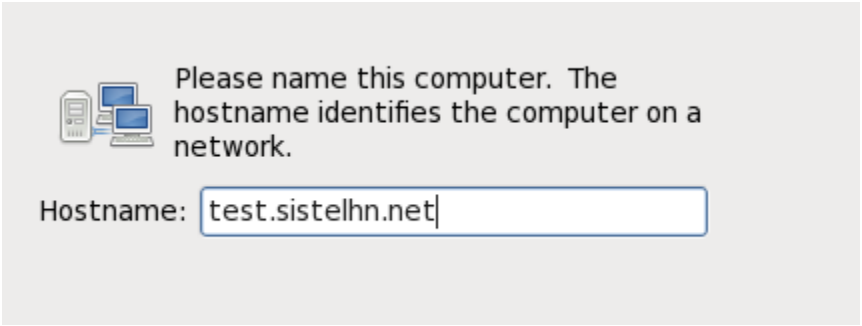
Utilizando el ratón, seleccione el tipo de teclado que le gustaría utilizar durante el proceso de instalación y como teclado predeterminado del sistema.

Inicializar el Disco Duro

Si el programa de instalación no encuentra particiones legibles en los discos rígidos existentes, pregunta si debe inicializar el disco rígido. Esta operación provoca que cualquier dato que se encuentre en el disco sea ilegible. Si su sistema tiene un nuevo disco rígido sin ningún sistema operativo instalado, o si ha eliminado todas las particiones, responda Reinicializar disco.

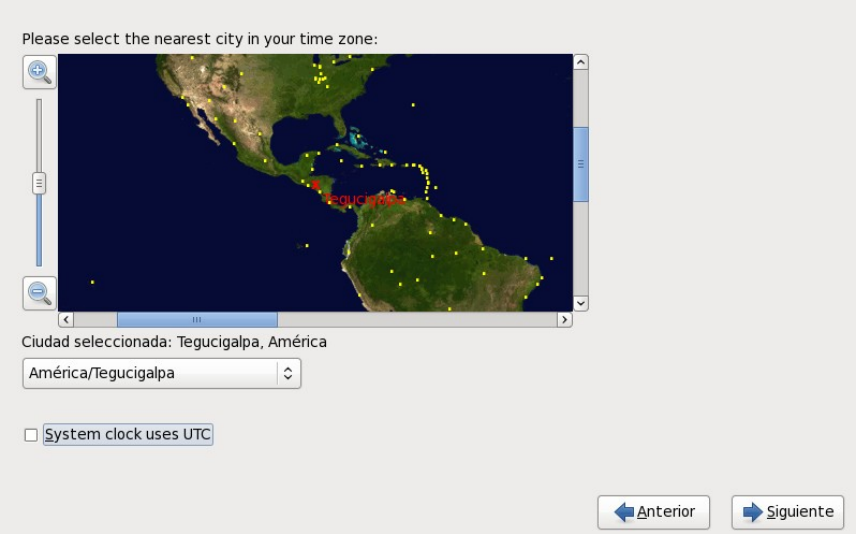


El configurador le pregunta un nombre de equipo y un nombre de dominio para esta computadora, en el formato nombredepc.nombrededominio. Muchas redes tienen el servicio DHCP (Protocolo de Configuración Dinámica de Equipo) que provee automáticamente la información de nombre de dominio a los sistemas, dejando al usuario ingresar el nombre de equipo. A no ser que tenga una necesidad puntual de modificar tanto el nombre de su equipo como el de su dominio, la configuración predeterminada lo define como localhost.localdomain, que para la mayoría de los usuarios es una opción aceptable.



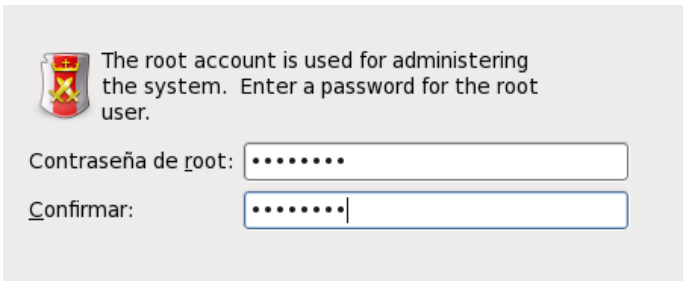
Configuración del uso de horario

Especifique la zona horaria aún si planea usar NTP (Protocolo de Hora de Red) para mantener la precisión del reloj de su sistema. Configure su huso horario seleccionando la ciudad más cercana a la ubicación física de su computador. Haga clic sobre el mapa para ampliar la región geográfica.



Poner la contraseña root

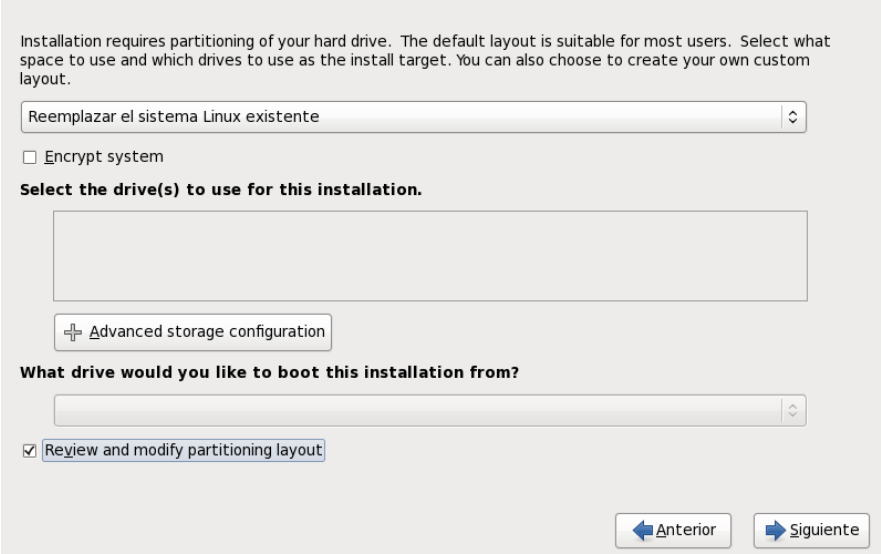
La configuración de la cuenta y la contraseña root es uno de los pasos más importantes durante la instalación. Su cuenta root es similar a la cuenta del administrador usada en las máquinas Microsoft Windows. La cuenta root es usada para instalar paquetes, actualizar RPMs y realizar la mayoría de las tareas de mantenimiento del sistema. Ingresando como root le da control completo del sistema.



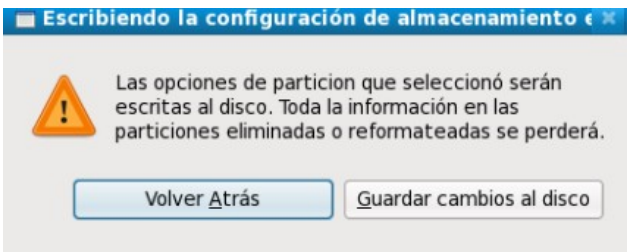
Utilice la cuenta de root tan sólo para la administración de su sistema. Cree una cuenta que no sea root para uso general y ejecute su - para actuar como root cuando necesite configurar algo de forma rápida. Estas reglas básicas minimizarán las posibilidades de que un comando incorrecto o un error de tipografía puedan dañar su sistema.

Particionamiento del Disco Duro

En esta pantalla puede elegir entre crear una disposición predeterminada o realizar un particionamiento manual utilizando la opción Crear un diseño personalizado. Las primeras cuatro opciones le permiten realizar una instalación automatizada sin necesidad de que usted particione el disco. Si no se siente seguro durante la partición manual de su disco, se aconseja que no cree una disposición personalizada y que deje que el programa de instalación haga las particiones por usted.

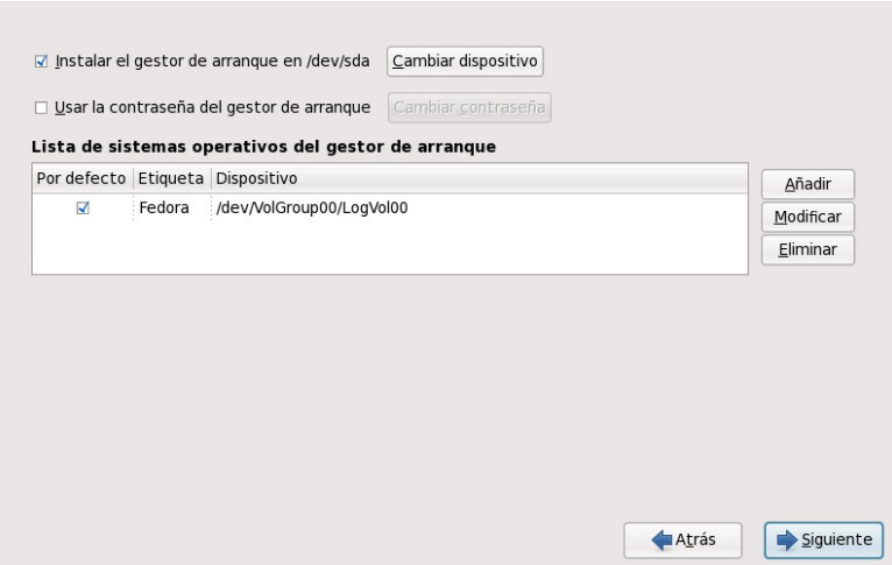


El instalador le pedirá que confirme las opciones de particionamiento elegidas. Haga clic en Guardar los cambios en el disco para permitir que el instalador realice las particiones elegidas en su disco rígido, e instale Fedora.



Configuración del Gestor de Arranque

GRUB (GRand Unified Bootloader), que se instala por defecto, es un gestor de arranque muy potente ya que puede cargar una gran variedad de sistemas operativos gratuitos así como sistemas operativos propietarios con el sistema de cargado en cadena (el mecanismo para cargar sistemas operativos no soportados mediante la carga de otro gestor de arranque, tal como DOS o Windows).

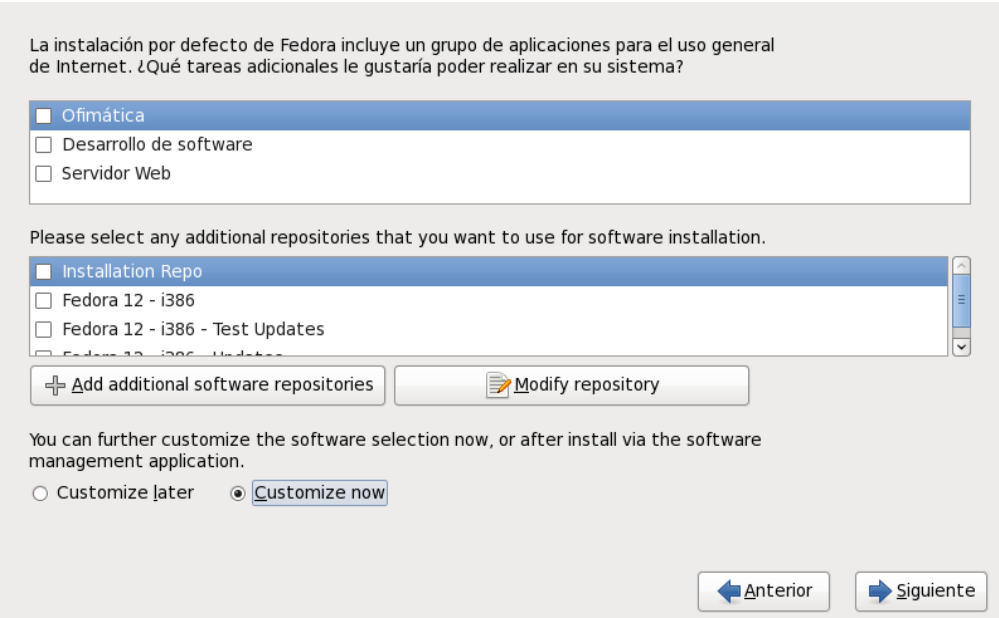


Si no hay ningún sistema operativo en su computadora, o está completando la eliminación de otros sistemas operativos, el programa de instalación instalará GRUB como su cargador de arranque sin ninguna intervención.

Selección de los paquetes

Ahora que ha realizado la mayoría de sus selecciones para la instalación, está listo para confirmar la selección predeterminada de paquetes o personalizar los paquetes para su sistema.

Primero, aparecerá la pantalla Instalación de Paquetes Predeterminados que detalla el conjunto de paquetes predeterminados configurados para la instalación de Fedora.



Por defecto, el proceso de instalación de Fedora carga una selección de software que es apropiado para un sistema de escritorio. Para incluir o quitar software para tareas comunes, seleccione los elementos de la lista:

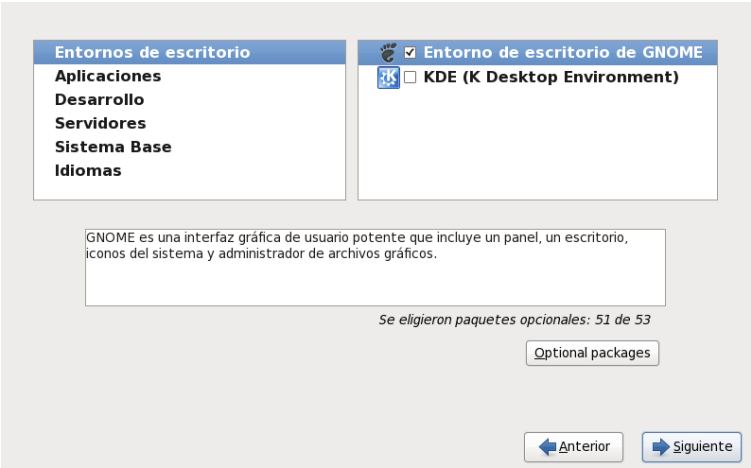
Oficina y Productividad
Esta opción ofrece la suite de productividad OpenOffice.org, la aplicación Planner para gestión de proyectos, herramientas gráficas como GIMP, y aplicaciones multimedia.

Software de Desarrollo
Esta opción provee las herramientas necesarias para compilar software en su sistema Fedora.

Servidor Web
Esta opción provee el servidor Web Apache

Para seleccionar un componente, haga clic en la casilla de verificación al lado de éste.

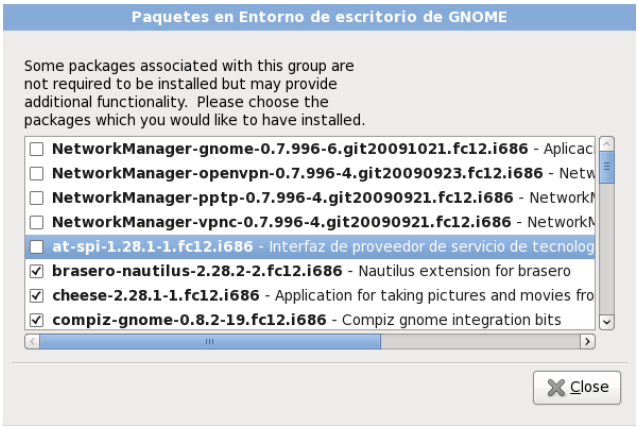
Para personalizar su grupo de paquetes aún más, seleccione la opción Personalizar ahora en la pantalla. Haga clic en Siguiente para ir a la pantalla Selección de Grupos de Paquetes.



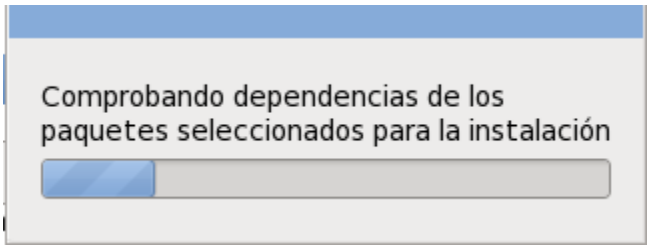
Para ver los grupos de paquetes por categoría, seleccione la categoria desde la lista a la izquierda. La lista a la derecha muestra los grupos de paquetes de la categoría seleccionada actualmente.

Para especificar un grupo de paquetes para su instalación, tilde la casilla que se encuentra junto al grupo que desea instalar. La casilla cerca del borde inferior de la pantalla muestra los detalles del grupo de paquetes que actualmente está seleccionado. Ninguno de los paquetes de un grupo serán instalados a menos que la casilla perteneciente a ese grupo sea tildada. Si selecciona un grupo de paquetes, Fedora automáticamente instala los paquetes imprescindibles y básicos de ese grupo. Para modificar los paquetes opcionales que de un grupo determinado serán instalados, seleccione el botón Paquetes Opcionales bajo la descripción de ese grupo. Luego utilice la casilla junto a los nombres de los paquetes individuales para cambiar la selección.

Después de haber elegido los paquetes deseados, seleccione Siguiente para continuar. Fedora verifica su selección, y automáticamente añade cualquier paquete extra que sea necesario para utilizar el software que usted ha seleccionado. Cuando finalice de elegir los paquetes, haga click sobre Cerrar para guardar su selección de paquetes optativos, y regrese a la pantalla principal de selección de paquetes.

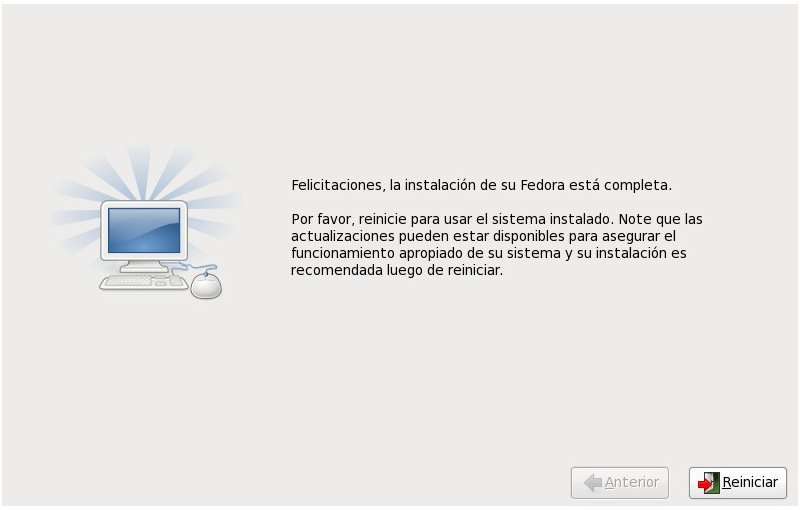


Una vez seleccionando los paquetes comprobara las dependencias.

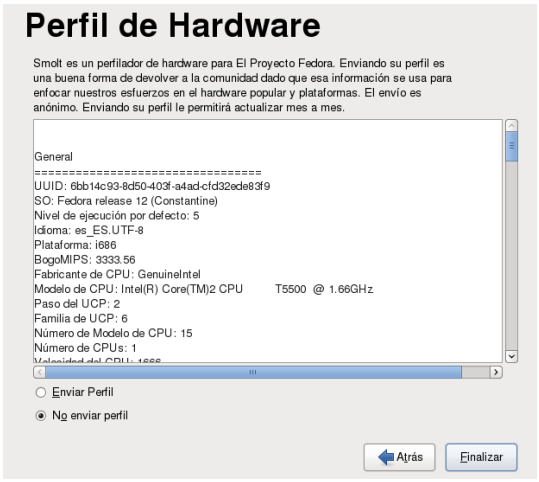


Luego de comprobar las dependencias empezara el proceso de instalación.

Al terminar le pedirá reiniciar el Sistema Operativo.

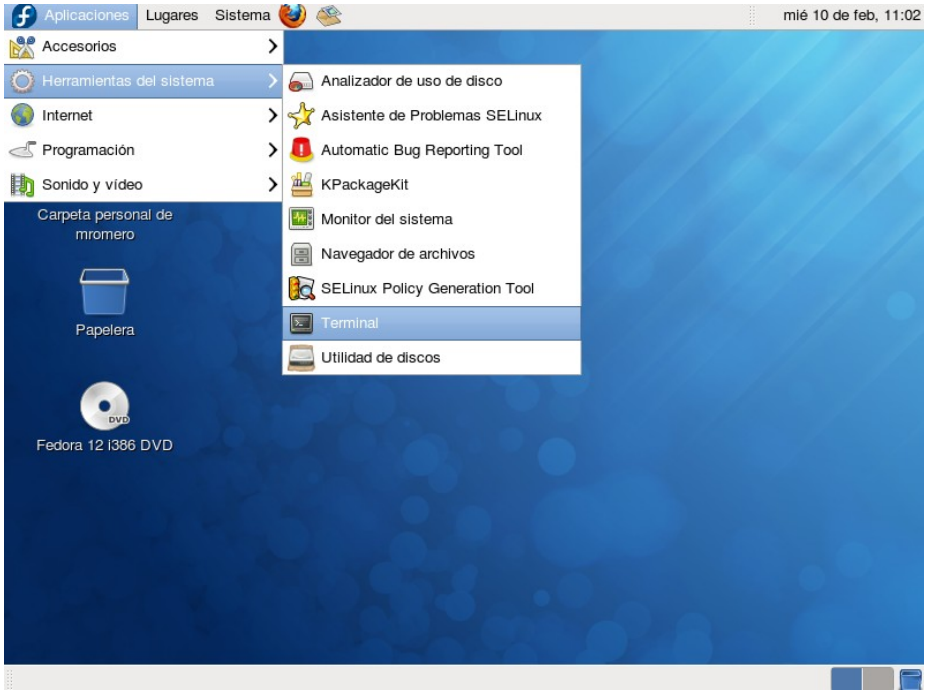


Luego ya estarás listo para usar Fedora, solo tienes que crear un usuario verificar que la fecha y hora concuerde con la actual y mandar la información de perfil de hardware para contribuir con la comunidad de Fedora.

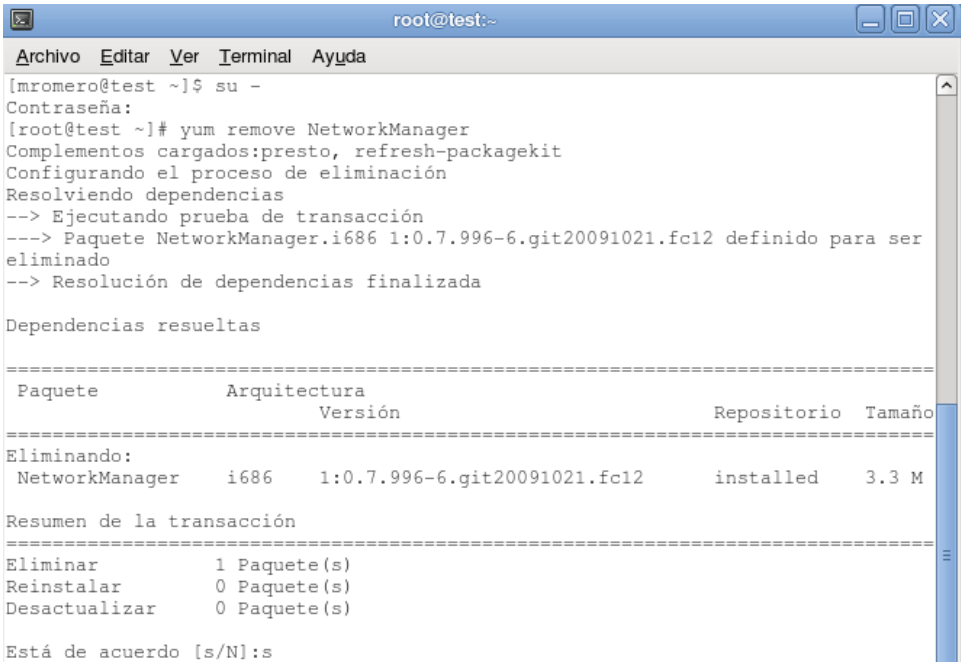


Configurando el Servidor Firewall

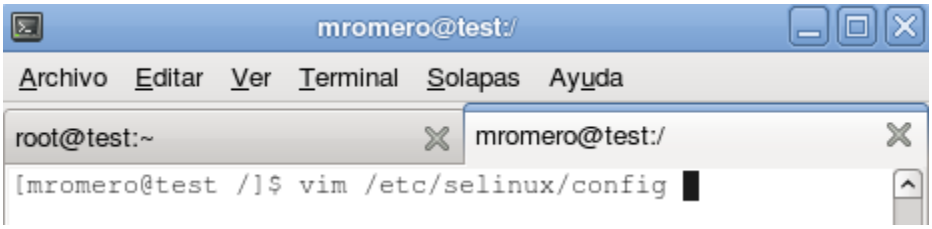
Iniciamos sesión y abrimos una terminal, ya que todo lo haremos mediante línea de comandos.



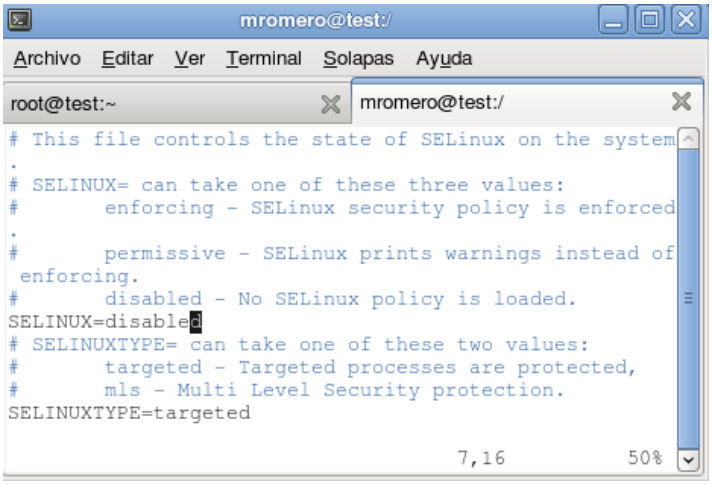
Desde el Terminal, lo primero que haremos será configurar la tarjeta de red para ello deberemos remover el NetworkManager esto lo haremos con el súper usuario (root) y con el comando **yum remove** tal como muestra la figura.



Editamos la configuración del selinux con el comando vim.



Y lo desactivos tal como se muestra en la figura.

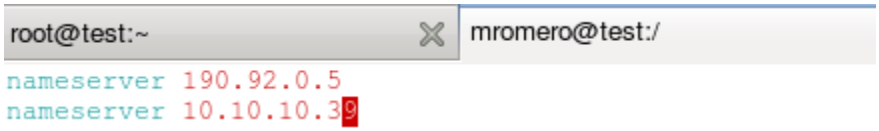


Ahora modificaremos el archivo de configuración para la interfaz eth0 con el comando vim.

El archivo de configuración deberá quedar similar al siguiente:

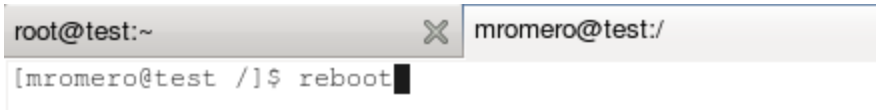
Editamos el archivo de configuración de los servidores de dominios con el comando vim.

El archivo de configuración deberá quedar igual al siguiente:



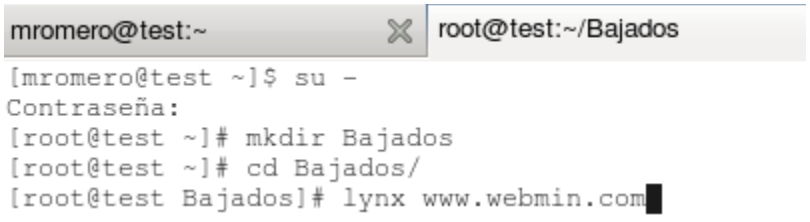
Agregar y quitar los servicios necesarios con el comando **setup**:

Después de haber hecho pruebas de conectividad reiniciamos el sistema con el comando reboot.



Cambiaremos al súper usuario (root) con el comando su, luego crearemos la carpeta de Bajados con mkdir hecho esto con el comando cd nos ubicamos dentro de la carpeta que acabamos de crear donde descargaremos los siguientes paquetes con el comando lynx:

- ✓ Webmin
- ✓ Shorewall



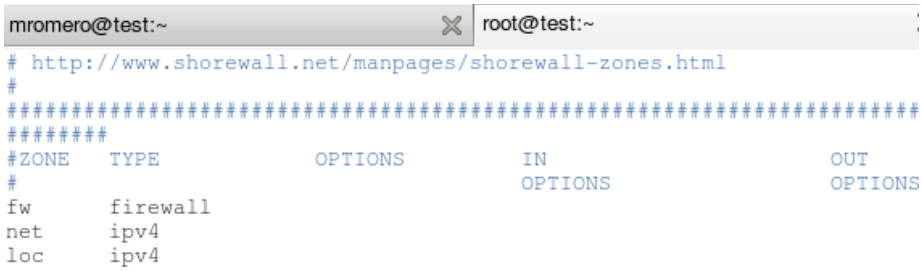
Luego con el comando **rpm –Uvh** instalamos los paquetes rpm que hemos bajado y con **rpmbuid** y **rpm --rebuild** reconstruimos los paquetes fuentes.

```
[root@test Bajados]# ls
webmin-1.500-1.noarch.rpm
[root@test Bajados]# rpm -Uvh webmin-1.500-1.noarch.rpm
advertencia:webmin-1.500-1.noarch.rpm: CabeceraV3 firma DSA: NOKEY, identificado
r de clave 11f63c51
Preparando...                ########################################### [100%]
Operating system is Redhat Linux
   1:webmin                  ##########################                ( 63%)
```

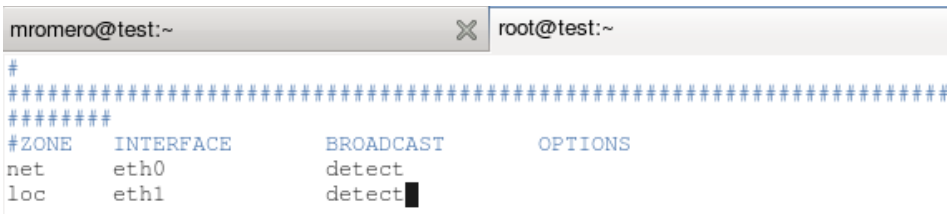
```
[root@test Bajados]# ls
shorewall  webmin-1.500-1.noarch.rpm
[root@test Bajados]# cd shorewall/
[root@test shorewall]# rpmbuild --rebuild shorewall-4.4.6-1.src.rpm
```

Una vez instalado el shorewall configuramos los ficheros básicos, con **vim etc/shorewall/shorewall.conf** activamos el shorewall :

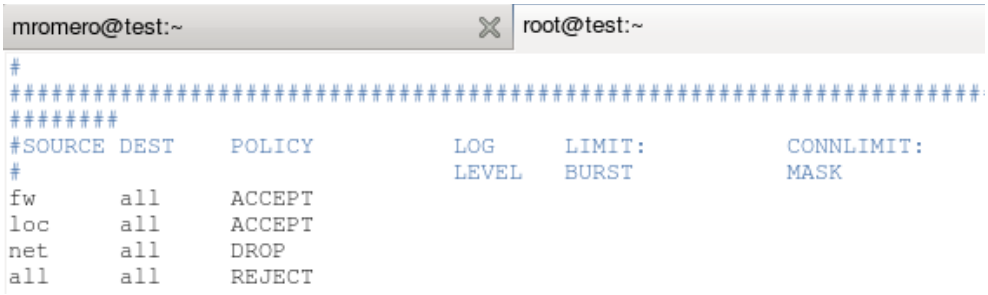
Con **vim /etc/shorewall/zones** agregamos las zonas:



Con **vim /etc/shorewall/interfaces** asignamos las zonas a las interfaces:

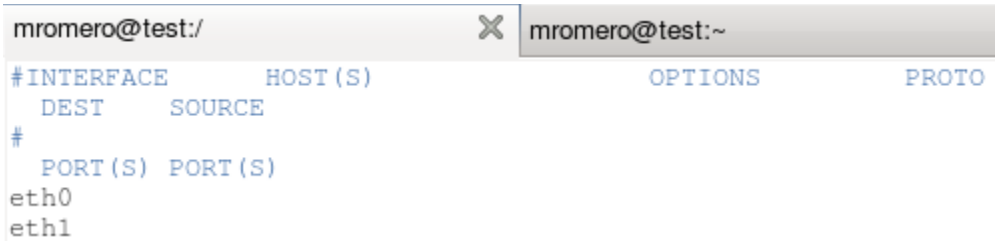


Luego definimos las políticas con **vim /etc/shorewall/policy**



Con **vim /etc/shorewall/rules** agregamos las reglas:

Con **vim /etc/shorewall/routestopped** configuramos que interfaces seguirán activas cuando se apague el shorewall.



Instalamos las dependencias:
[mromero@test ~]# **yum install perl-Net-SSLeay perl-CPAN php-gd php-pear gnome-rdp php-xml pptp poptop* ppp pcre-devel libpcap-devel mysql-devel php-adodb**

Creamos una carpeta donde se descargaran los programas:
[mromero@test ~]# **mkdir /root/BAJADOS**
[mromero@test ~]# **cd /root/BAJADOS**
[mromero@test ~]# **mkdir FW**

Con el comando wget descargamos los programas que necesarios para el servidor firewall, instalamos y configuramos como se muestra:

Descompresor de Archivos Unrar:

[mromero@test ~]# **cd /root/BAJADOS/FW**
[mromero@test ~]# **wget http://dl.atrpms.net/all/unrar-3.8.4-1.src.rpm**
 # Con este comando creamos la paquetería y la reconstruimos:
[mromero@test ~]# **rpmbuild --rebuild unrar-3.8.4-1.src.rpm**
#Con rpm –Uvh instalamos el aplicativo del paquete que reconstruimos:
[mromero@test ~]# **rpm -Uhv /root/rpmbuild/RPMS/i586/unrar-3.8.4-1.fc11.i586.rpm**

Antivirus Clamav:
[mromero@test ~]# **cd /root/BAJADOS/FW**
[mromero@test ~]# **wget http://packages.sw.be/clamav/clamav-0.95.3-1.rf.src.rpm**
 # Con este comando creamos la paquetería y la reconstruimos:
[mromero@test ~]# **rpmbuild --rebuild clamav-0.95.3-1.rf.src.rpm**
[mromero@test ~]# **rpm -Uhv /root/rpmbuild/RPMS/i586/clam***
 # Para Actualizar la Base de Datos de virus se utiliza el comando:
[mromero@test ~]# **freshclam**
 # Instalamos los modulos perl:
[mromero@test ~]# **perl -MCPAN -e shell**
[mromero@test ~]# **vim /etc/clamd.conf**

Configuración de Servidor Ftp:

[mromero@test]# **vim /etc/vsftpd/vsftpd.conf**
anonymous_enable=NO
chroot_local_user=YES
chroot_list_enable=YES

chroot_list_file=/etc/vsftpd/chroot_list
[mromero@test]# **touch /etc/vsftpd/chroot_list**
[mromero@test]# **service vsftpd restart**

Configuración de Squid Proxy:

 # Editamos el archivo de configuración con vim y agregamos/cambiamos las siguientes opciones:
[mromero@test]# **vim /etc/squid/squid.conf**
 # Opciones para proxy transparente y acceso solo a la red local
http_port 3128 transparent
cache_dir ufs /var/spool/squid 5000 16 256
#acl localnet src 10.0.0.0/8   # RFC1918 possible internal network
acl localnet src 127.0.0.1/32
#acl localnet src 172.16.0.0/12 # RFC1918 possible internal network
#acl localnet src 192.168.0.0/16   # RFC1918 possible internal network
 # Agregamos estos puertos para aplicaciones varias:
acl Safe_ports port 777   # multiling http
acl Safe_ports port 3000
acl Safe_ports port 10000
acl Safe_ports port 8080
acl Safe_ports port 8081
acl Safe_ports port 1863
acl Safe_ports port 7001
acl socks_port port 1080
acl SSL_ports port 8443
acl Safe_ports port 8443
acl SSL_ports port 10000
acl CONNECT method CONNECT

 # Paginas para las cuales no hará cache:

```
        acl LISTANOCACHE1 url_regex sistelhn.net
        acl LISTANOCACHE2 url_regex www.sistelhn.net
        acl LISTANOCACHE3 url_regex otro.com
        acl LISTANOCACHE4 url_regex www.otro.com
        no_cache deny LISTANOCACHE1
        no_cache deny LISTANOCACHE2
        no_cache deny LISTANOCACHE3
        no_cache deny LISTANOCACHE4
```

 # Nombre que aparecerá del proxy:

```
        access_log  none
        visible_hostname firewall.sistelhn.net
```

Configuración Dansguardian

[mromero@test]# **yum install dansguardian**
[mromero@test]# **cd /etc/dansguardian**
 # Hacemos copias de las listas para los diferentes grupos:
[mromero@test]# **cp -rp lists lists2**
[mromero@test]# **cp -rp lists lists3**
[mromero@test]# **cp -rp lists lists4**
[mromero@test]# **cp -rp lists lists5**
[mromero@test]# **cp -rp lists lists6**
[mromero@test]# **cp -rp lists lists7**
[mromero@test]# **cp -rp lists lists8**
[mromero@test]# **cp -rp lists lists9**
[mromero@test]# **vim dansguardianf1.conf**
 # El límite de frases excedidas para que la pagina sea bloqueada:

```
        naughtynesslimit = 180
        enablepics = on
        bypasskey = 'jg567511123123sqqw12354wq123qwe9'
```

 # Copiamos el archivo de configuración para cada grupo y dentro de ellos agregamos la ruta de su respectiva lista:

[mromero@test]# **cp -rp dansguardianf1.conf dansguardianf2.conf**

#Remplazar todos los list con list2 con el comando:

:%s/lists/lists2/g

[mromero@test]# **cp -rp dansguardianf1.conf dansguardianf3.conf**

#Remplazar todos los list con list3 con el comando:

:%s/lists/lists3/g

[mromero@test]# **cp -rp dansguardianf1.conf dansguardianf4.conf**

#Remplazar todos los list con list4 con el comando:

:%s/lists/lists4/g

[mromero@test]# **cp -rp dansguardianf1.conf dansguardianf5.conf**

#Remplazar todos los list con list5 con el comando:

:%s/lists/lists5/g

[mromero@test]# **cp -rp dansguardianf1.conf dansguardianf6.conf**

#Remplazar todos los list con list6 con el comando:

:%s/lists/lists6/g

[mromero@test]# **cp -rp dansguardianf1.conf dansguardianf7.conf**

#Remplazar todos los list con list7 con el comando:

:%s/lists/lists7/g

[mromero@test]# **cp -rp dansguardianf1.conf dansguardianf8.conf**

#Remplazar todos los list con list8 con el comando:

:%s/lists/lists8/g

[mromero@test]# **cp -rp dansguardianf1.conf dansguardianf9.conf**

#Remplazar todos los list con list9 con el comando:

:%s/lists/lists9/g

[mromero@test]# **vim dansguardian.conf**

 # Cambiamos lenguaje español de Argentina:

language = 'arspanish'

filterip =

 # Agregamos el número de grupos o filtros que usaremos:

filtergroups = 9

 # Opciones para el antivirus:

contentscanner = '/etc/dansguardian/contentscanners/clamdscan.conf'

daemonuser = 'clamav'

 # Pluglins que utilizaremos:

authplugin = '/etc/dansguardian/authplugins/proxy-basic.conf'

authplugin = '/etc/dansguardian/authplugins/ip.conf'

[mromero@test]# **vim /etc/dansguardian/contentscanners/clamdscan.conf**

 # Verificamos que el clamd corra en este archivo

clamdudsfile = '/var/run/clamav/clamd.sock'

[mromero@test]# **vim /etc/clamd.conf**
User
Sock
[mromero@test]# **service clamd restart**
 # Damos permiso al antivirus para que revise los logs del dansguardian:
[mromero@test]# **chown clamav -R /var/log/dansguardian/**
[mromero@test]# **service dansguardian restart**

[mromero@test]# **vim /etc/dansguardian/lists/authplugins/ipgroups**

INSTRUCCIONES/NOTAS:

#No 1.: BLOQUEO TOTAL; En este grupo van todas las direcciones IP por Omisión o No Definidas. Esto ayuda para que cualquier persona NO pueda usar el sistema sino está definida aquí.

#No 2: INTERMEDIO; Filtra en base a Listas pre-configuradas y ponderación de palabras e Imágenes (Accesos a actualizaciones del Sistema Operativo, AntiVirus y Utilitarios necesarios para su Red). No se permite bajar archivos de Correos Electrónicos Gratuitos como Yahoo y Hotmail, al igual que se bloquean las conexiones al Chat. Recomendado para la Mayoría de Usuarios de su Red.

#No 3: ACCESO TOTAL: Deja pasar toda la navegación Web. Recomendado para Gerentes, y/o personas que lo necesitan. Advertencia: El uso de esta lista puede generar problemas de saturación de Ancho de Banda y problemas de Virus, a causa del uso que los usuarios le den.

#No 4: INTERMEDIO CHAT: Filtra en base a Listas pre-configuradas y ponderación de palabras e Imágenes (Accesos a actualizaciones del Sistema Operativo, AntiVirus y Utilitarios necesarios para su Red). Si se permite bajar archivos de Correos Electrónicos Gratuitos como Yahoo y Hotmail, al igual que se permiten las conexiones al Chat (Yahoo/MSN). Recomendado para la Mayoría de Usuarios de su Red.

#No 5: BLOQUEO ACTIVO A: Bloquea TODAS las páginas Web, menos las que estan en la lista "Exception site (domain) list" (Dominios/paginas configuradas tienen accesto total) y la lista "Grey site (domain) list" (Dominios/paginas se filtran normal, y se bloquean si sobrepasan una ponderacion o revision normal). Las Exception Site List sobre-escriben o imperan sobre las Grey Site List. Util para dar acceso a un grupo de persona a ver únicamente las páginas web que el Administrador desea.

#No 6: BLOQUEO ACTIVO B: Bloquea TODAS las páginas Web, menos las que están en la lista "Exception site (domain) list" (Dominios/paginas configuradas tienen acceso total) y la lista "Grey site (domain) list" (Dominios/paginas se filtran normal, y se bloquean si sobrepasan una ponderación o revisión normal). Las Exception Site List sobre-escriben o imperan sobre las Grey Site List. Util para dar acceso a un grupo de persona a ver únicamente las páginas web que el Administrador desea.

#Grupos 7,8 y 9 estan libres.
####################################

Configuración NTOP:

[mromero@test]# **yum install ntop**
[mromero@test]# **cd /etc**
[mromero@test]# **cp -rp ntop.conf ntop.conf.Original**
[mromero@test]# **vim ntop.conf**
--user ntop
--use-syslog=daemon
--db-file-path /var/lib/ntop
--trace-level 3
#Puertos atraves del cual se conecta al aplicativo web:
-w 3000 -W 3001
--disable-schedyield
--skip-version-check=yes
#Interfaces que monitoreara el ntop:
--interface eth0,eth1,eth2,eth3
--local-subnets 192.168.4.0/24,10.10.10.0/24
--no-interface-merge
--no-mac
--disable-decoders
[mromero@test]# **ntop**

Configuración de VPN PPTP POPTOP:

[mromero@test]# **cd /root/BAJADOS/FW**
[mromero@test]# **wget http://downloads.sourceforge.net/project/poptop/pptpd/pptpd-1.3.4/pptpd-1.3.4.tar.gz?use_mirror=hivelocity**
[mromero@test]# **rpmbuild -tb pptpd-1.3.4.tar.gz**
[mromero@test]# **rpm --Uhv /root/rpmbuild/RPMS/i586/pptpd-1.3.4-1.fc11.i586.rpm**
[mromero@test]# **cd /etc/**
[mromero@test]# **cp -rp ppp ppp.Original**
[mromero@test]# **vim ppp/chap-secrets**
mromero pptpd fernando "*"
[mromero@test]#

Configuración dhcp:

[mromero@test]# **yum install dhcp**
[mromero@test]# **vim /etc/dhcp/dhcpd.conf**

```
subnet 192.168.4.0 netmask 255.255.255.0 {
        option domain-name-servers 192.168.4.5;
        option routers 192.168.4.5.;
        range 192.168.4.50 192.168.4.150;
 }
```

[mromero@test]# **service dhcpd restart**

Configuración CBQ:

[mromero@test]# **yum -y install iproute**
#Vamos a la carpeta donde se encuentran los archivos de configuración:
[mromero@test]# **cd /etc/sysconfig/cbq/**
#Copiamos el archivo de ejemplo como respaldo:
[mromero@test]# **cp –rp cbq-0000.example cbq-0000.example.original**
#A partir del archivo de ejemplo creamos los personalizados:
[mromero@test]# **mv cbq-0000.example cbq-0001.web**
#Interfaz que usara, ancho de banda de la interfaz y peso:

```
DEVICE=eth1,10Mbit,1Mbit
```

#Ancho de banda y peso de la clase:

```
RATE=1024Kbit
WEIGHT=204Kbit
```

#La prioridad que tendrá sobre otras reglas de ancho de banda:

```
PRIO=5
```

#Regla de Filtración:

```
RULE=192.168.4.0/16
PARENT=100
```

#Copiamos el archivo binario dentro de init.d para que lo trate como cualquier otro servicio:
[mromero@test]# **cp -a /sbin/cbq /etc/init.d**
#Para comprobar que la configuración este correcta:

[mromero@test]# **service cbq compile**
[mromero@test]# **service cbq start**

[mromero@test]# **mkdir /root/RESPALDOS**

Configuración DNS:

[mromero@test]# **vim /etc/named.conf**

```
        Options {
                listen-on port 53 { any; };
                listen-on-v6 port 53 { any; };
                directory       "/var/named/";
                dump-file       "/var/named/data/cache_dump.db";
          statistics-file "/var/named/data/named_stats.txt";
              allow-recursion    {    127.0.0.1;    localhost;    10.10.10.0/24;    192.168.4.0/24;
190.92.31.6; };
                allow-query    {    127.0.0.1;    localhost;    10.10.10.0/24;    192.168.4.0/24;
190.92.31.6; };
                recursion yes;
        };
        logging {
        channel default_debug {
                file "data/named.run";
                 severity dynamic;
                 };
        };
        zone "." IN {
                type hint;
                file "named.ca";
        };
        zone "6.31.92.190.in-addr.arpa" in {
                type master;
                file "31.92.190.in-addr.arpa.zone";
                };
        zone "sistelhn.net" in {
```

```
        type master;
        file "ext.sistelhn.net.zone";
        allow-query {
                any;
                };
    };
[mromero@test]#
```

Configuración snort:

[mromero@test]# **cd /root/BAJADOS/FW**
[mromero@test]# **wget http://dl.snort.org/snort-current/snort-2.8.5.3.tar.gz**
[mromero@test]# **rpmbuild --with mysql -tb snort-2.8.5.3.tar.gz**
[mromero@test]# **rpm -Uhv /root/rpmbuild/RPMS/i586/snort-2.8.5.3-1.i586.rpm**
[mromero@test]# **rpm -Uhv /root/rpmbuild/RPMS/i586/snort-mysql-2.8.5.3-1.i586.rpm**
[mromero@test]# **mv rules.rar /etc/snort/rules/**
[mromero@test]# **cd /etc**
[mromero@test]# **cp -rp snort snort.Original**
[mromero@test]# **vim /snort/snort.conf**

```
    var RULE_PATH rules
    #preprocessor dcerpc2
    #preprocessor dcerpc2_server: default
    #include $RULE_PATH/netbios.rules
```

#Agregamos el usuario que creamos para el snort junto con su contraseña y base de datos:

output database: log, mysql, detail=full user=snortsql password=passSnortF dbname=snort host=localhost

output database: alert,mysql,detail=full user=snortsql password=passSnortF dbname=snort host=localhost

#Con el usuario root creamos la base de datos del snort:

[mromero@test]# **mysql –u root -p create snort**

#Con el usuario root ejecutamos el script para que se genere la base de datos:

[mromero@test]# **mysql –u root -p snort < /usr/share/snort-2.8.5.3/schemas/create_mysql**

#Con el usuario root añadimos el usuario snortsql con contraseña passSnortF para que pueda conectarse a la base de datos:

[mromero@test]# **mysql –u root -p**

mysql>grant all on snortsql.* to snort@localhost identified by 'passSnortF';

mysql> flush privileges;

[mromero@test]# **cd /snort**

[mromero@test]# **cp -rp classification.config rules/**

[mromero@test]# **cd /snort/rules**

#Copiamos las reglas y las descomprimimos:

[mromero@test]# **unrar e rules**

#Comentamos la siguiente línea:

[mromero@test]# **vim /etc/sysconfig/snort**

#SNORT_OPTIONS="-A fast -b -l /var/log/snort -d"

[mromero@test]# **cd /BAJADOS/FW**

[mromero@test]#**wget http://sourceforge.net/projects/secureideas/files/BASE/base-1.4.4/base-1.4.4.tar.gz/download**

[mromero@test]# **tar xvfz base-1.4.4.tar.gz**

#Movemos la carpeta al directorio donde se buscara la aplicación y damos permisos al servidor web para que la pueda utilizar:

[mromero@test]# **mv base-1.4.4 /var/www/html/base**

[mromero@test]# **chown apache.apache -R /var/www/html/base**

#Agregamos un alias al directorio donde se encuentra la aplicación:

[mromero@test]# **vim /etc/httpd/conf/httpd.conf**

Alias /base /var/www/html/base

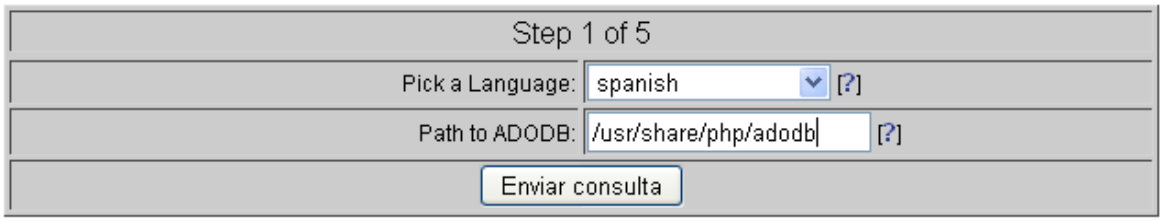
#Editamos el archivo php.ini con lo siguiente:

[mromero@test]# **vim /etc/php.ini**

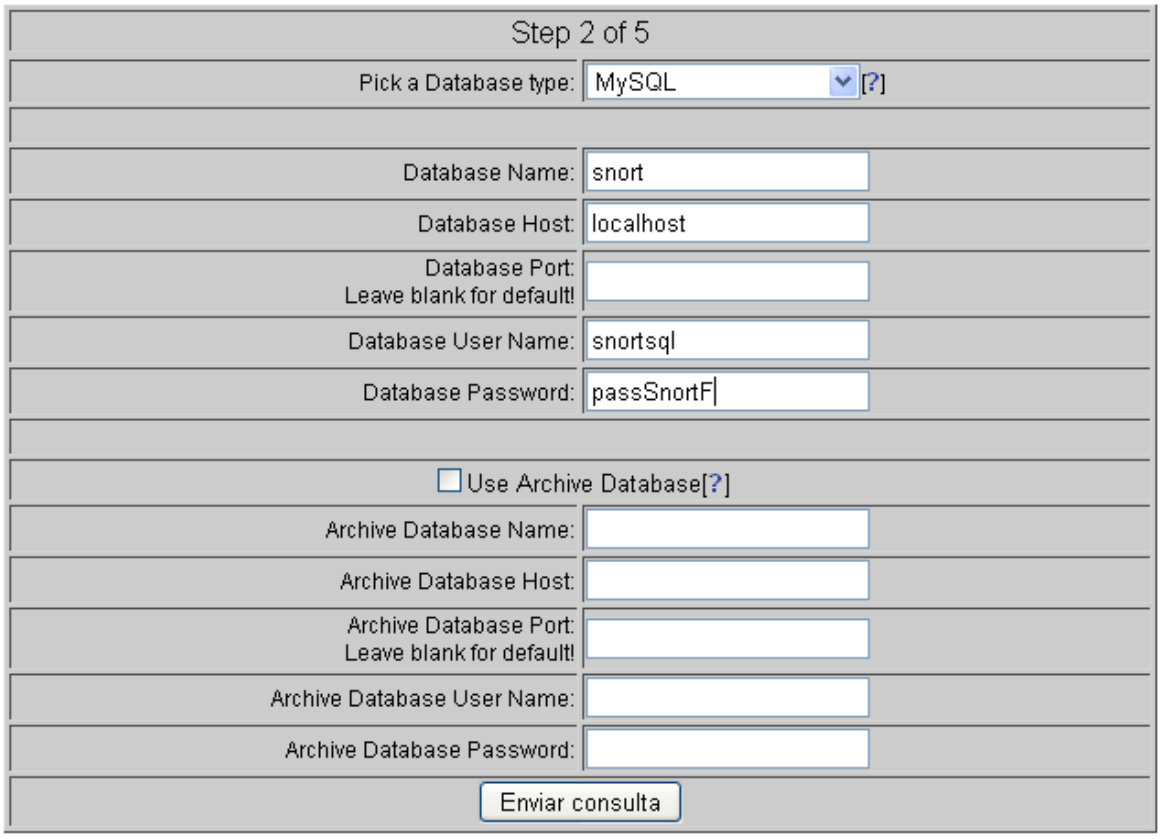
error_reporting = E_ALL & ~E_NOTICE
[mromero@test]# **service httpd restart**

Introducimos en el Navegador la Url del CBQ https://sistelhn.net/base y nos aparecerá la siguiente pantalla donde le damos continuar para configurar la interfaz web por primera vez:

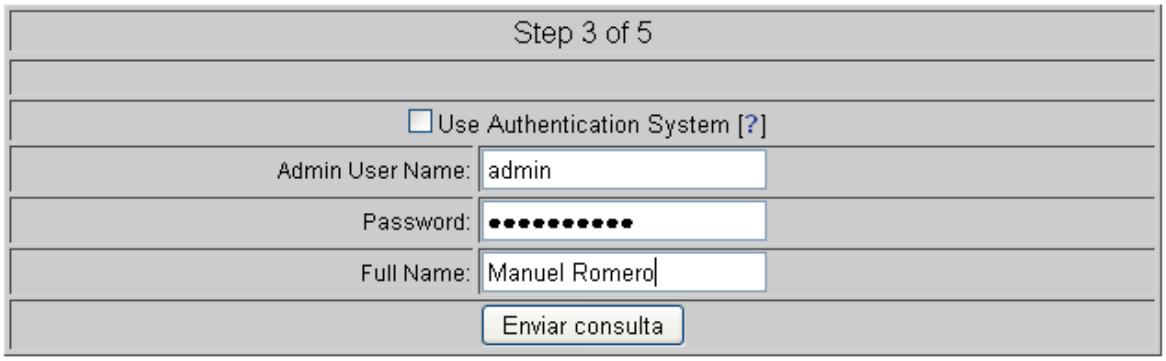
Seleccionamos el idioma y la ruta de la librería adodb:



Escribimos el nombre de la base de datos que creamos, usuario de la base de datos y su contraseña:



Creamos un usuario y contraseña para el detector de intrusos:



Y ya estará listo para usar:

Step 4 of 5		
Operation	**Description**	**Status**
BASE tables	Adds tables to extend the Snort DB to support the BASE functionality • snort	Create BASE AG

Step 4 of 5		
Operation	**Description**	**S**
BASE tables	Adds tables to extend the Snort DB to support the BASE functionality • snort	DONE

The underlying Alert DB is configured for usage with BASE.

Additional DB permissions
In order to support Alert purging (the selective ability to permanently delete alerts from the database) and DNS/whois lookup caching, the DB user "snortsql" must have the DELETE and UPDATE privilege on database "snort@localhost"

Now continue to **step 5**...

Basic Analysis and Security Engine (BASE)

- Alertas de hoy:	**Único**	**lista**	**IP Origen**	**IP Destino**
- Alertas de los últimos 24 horas:	**Único**	**lista**	**IP Origen**	**IP Destino**
- Alertas de los últimos 72 horas:	**Único**	**lista**	**IP Origen**	**IP Destino**
- Más reciente15 Alertas:	**cualquier protocolo**	**TCP**	**UDP**	**ICMP**
- Últimos puertos de origen:	**cualquier protocolo**	**TCP**	**UDP**	
- Últimos puertos de destino:	**cualquier protocolo**	**TCP**	**UDP**	
- Puertos de origen más frecuentes:	**cualquier protocolo**	**TCP**	**UDP**	
- Puertos de destino más frecuentes:	**cualquier protocolo**	**TCP**	**UDP**	
- Más frecuente 15 Direcciones::	**Origen**	**Destino**		
- **Más reciente15 Alertas únicas**				
- **Más frecuente 5 Alertas únicas**				

Añadido 1972 alerta(s) al escondrijo
Consultado en : Tue March 02, 201
Base de datos: snort@localhost (**Versión de esqu**
Ventana de tiempo: [2010-02-27 12:38:20] - [2010-03-0

Buscar
Hacer gráfica de datos de alerta
Hacer gráfica del tiempo de detectar alertas

Sensores/Total: 1 / 1
Alertas únicas: 27
Categorías: 9
Número de Alertas en Total: 3236

- Orig. direcciones IP: 148
- Dest. direcciones IP: 63
- Enlaces IP Únicas 301
- Puertos de Origen: 612
  - TCP (595) UDP (17)
- Puertos de Dest: 64
  - TCP (50) UDP (14)

Perfil de Tráfico por Protocolo

TCP (62%)

UDP (5%)

ICMP (29%)

Trafico de Exploración de Puertos (3%)

Mantenimiento de Grupos de Alertas | **Cache & Estado** | **Administración**

BASE 1.4.4 (dawn)(por **Kevin Johnson** y el equipo del **proyecto BASE**
Basado en ACID por Roman Danyliw)

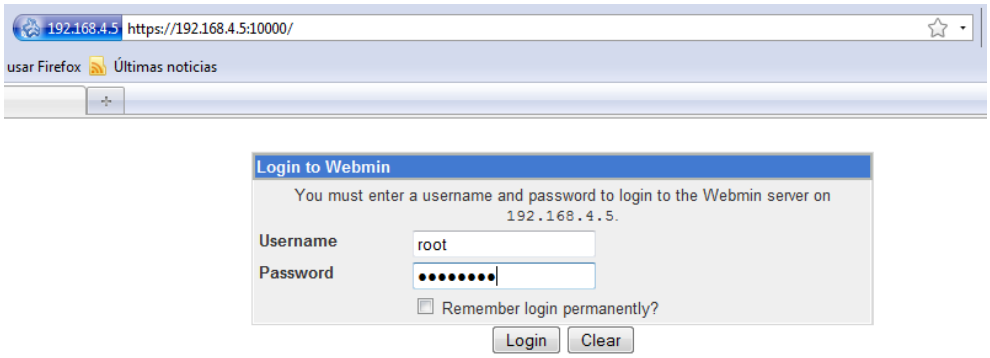
[Cargado en 0 seconds]

Con el comando setup verificar que estén corriendo los siguientes servicios:

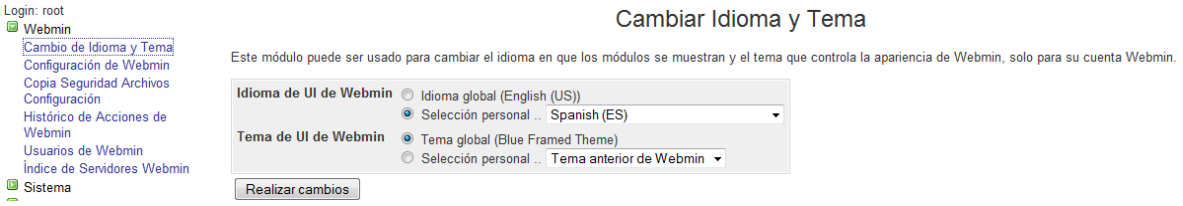
1. acpid
2. atd
3. clamd
4. cpuspeed
5. cron
6. dansguardian
7. dhcpd
8. gpm
9. httpd
10. messagebus
11. mysqld
12. named
13. network
14. ntop
15. ntpd
16. ntpdate
17. openvpn
18. poppassd
19. pptpd
20. rsyslog
21. snortd
22. squid
23. sshd
24. shoewall
25. vsftpd
26. webmin
27. xinetd

Personalización del Webmin

Para acceder a la interfaz de administración web colocamos en el url la dirección de nuestro servidor a través del puerto 10000 que usa el webmin https://192.168.4.5:10000/ donde introducimos el usuario y contraseña:



Lo primero que haremos será cambiar el idioma esto lo hacemos en webmin – Change Language and Theme y lo pasamos a español como se muestra en la imagen:

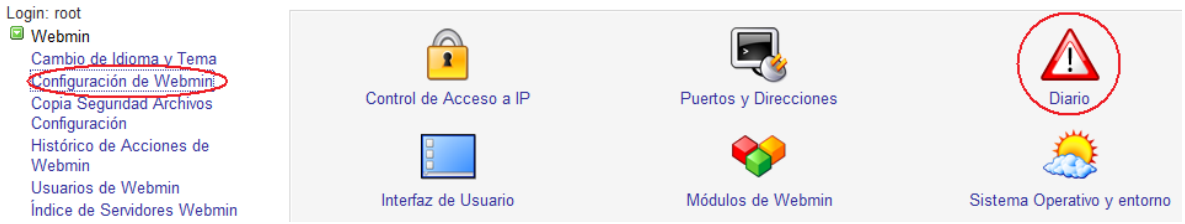


Luego nos vamos a configuración del webmin seleccionamos el icono de autentificación:

Hacemos los siguientes cambios:

1. opción Auto-logout after 45 minutes of inactivity

Luego nos vamos a configuración del webmin seleccionamos el icono de diario:



Hacemos los siguientes cambios:

1. Utilizar formato combinado de histórico (incluyendo referenciador y agente de usuario) (•) Si ( ) No
2. Periodically clear log files? (•) Yes, every 600 hours ( ) No
3. Include Webmin logins and logouts in actions log? (•) Si ( ) No
4. levar diario de los cambios hechos en archivos por cada acción (•) Si ( ) No
5. Grabar todos los archivos modificados antes de las acciones, para permitir una vuelta atrás
   (•)
   Si ( ) No
6. Also log to syslog? (•) Si ( ) No

Luego nos vamos a Webmin – Usuarios de Webmin – Crear un nuevo grupo de Webmin:

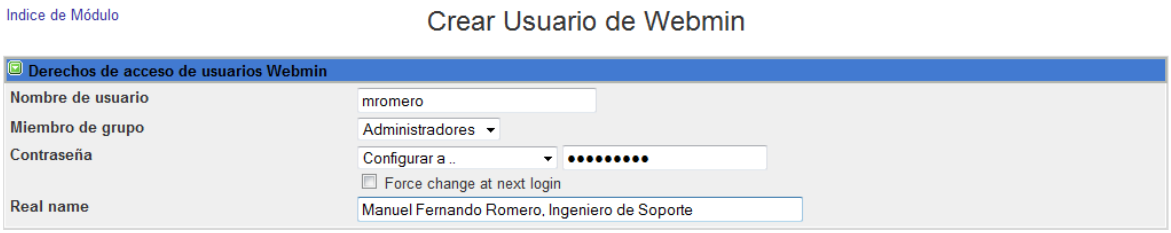
Creamos el grupo Administrador y le damos acceso a los siguientes módulos:

1. Webmin:
    - Cambio de Idioma y Tema
    - Histórico de Acciones de Webmin
2. Sistema:
    - Arranque y Parada

- Cambios de Contraseña
- Usuarios y Grupos

3. Servidores:
    - Dansguardian Filtro de Contenidos Web
    - Squid Servidor Proxy
    - Intrusion Detector
    - NTOP
4. Red:
    - Clase Based Queueing
    - Configuración de Red
    - Configuración de VPN IPSEC
    - Corta Fuegos Shorewall
    - Servidor VPN PPTP
5. Hardware:
    - Hora del Sistema
6. Otros:
    - Comandos Personalizados
    - Explorador de Archivos
    - Estado del Sistema y Servidor.

Luego creamos los usuarios y los añadimos al grupo de Administradores.



NOTAS PARA x64

Configuración de Snort

[mromero@test]# **cd /root/BAJADOS/FW**
[mromero@test]# **wget http://dl.snort.org/snort-current/snort-2.8.5.3.tar.gz**
#Creamos la siguiente carpeta para las librerías de mysql:
[mromero@test]# **mkdir /usr/mysql**
[mromero@test]# **cd /usr/mysql**
#Creamos una liga simbolica para que todo lo que vaya para /lib lo mande a /usr/lib64:
[mromero@test]# **ln -s /usr/lib64 /lib**
[mromero@test]# **cd /root/BAJADOS/FW**
[mromero@test]# **rpmbuild --with mysql -tb snort-2.8.5.3.tar.gz**
[mromero@test]# **rpm -Uhv /root/rpmbuild/RPMS/i586/snort-2.8.5.3-1.i586.rpm**
[mromero@test]# **rpm -Uhv /root/rpmbuild/RPMS/i586/snort-mysql-2.8.5.3-1.i586.rpm**

[mromero@test]# **mv rules.rar /etc/snort/rules/**
[mromero@test]# **cd /etc**
[mromero@test]# **cp -rp snort snort.Original**
[mromero@test]# **vim /snort/snort.conf**

var RULE_PATH rules
#preprocessor dcerpc2
#preprocessor dcerpc2_server: default
#include $RULE_PATH/netbios.rules

#Agregamos el usuario que creamos para el snort junto con su contraseña y base de datos:

output database: log, mysql, detail=full user=snortsql password=passSnortF dbname=snort host=localhost
output database: alert,mysql,detail=full user=snortsql password=passSnortF dbname=snort host=localhost

#Con el usuario root creamos la base de datos del snort:
[mromero@test]# **mysql –u root -p create snort**
#Con el usuario root ejecutamos el script para que se genere la base de datos:
[mromero@test]# **mysql –u root -p snort < /usr/share/snort-2.8.5.3/schemas/create_mysql**
#Con el usuario root añadimos el usuario snortsql con contraseña passSnortF para que pueda conectarse a la base de datos:
[mromero@test]# **mysql –u root -p**

mysql>grant all on snortsql.* to snort@localhost identified by 'passSnortF';
mysql> flush privileges;

[mromero@test]# **cd /snort**
[mromero@test]# **cp -rp classification.config rules/**
[mromero@test]# **cd /snort/rules**
#Copiamos las reglas y las descomprimimos:
[mromero@test]# **unrar e rules**
#Comentamos la siguiente línea:
[mromero@test]# **vim /etc/sysconfig/snort**

#SNORT_OPTIONS="-A fast -b -l /var/log/snort -d"

FUNCIONES OPCIONALES

Autenticación de Usuarios para Navegación Web

#Copiamos las reglas y las descomprimimos:

[mromero@test]# **vim /etc/squid/squid.conf**

 # Duración de la autenticación en una dirección IP

authenticate_ip_ttl 2 hours

auth_param basic credentialsttl 2 hour

 # Le decimos al squid que programa utilizaremos para la autenticación y donde se encuentran los usuarios y contraseñas

auth_param basic program /etc/webmin/squid/squid-auth.pl /etc/webmin/squid/users

 # Mensaje que aparecerá cuando hagamos uso del navegar web

auth_param basic realm INGRESE SU Usuario/Clave PARA NAVEGAR

 # Numero de procesos de autenticación

auth_param basic children 5

 # Especifica si el nombre de usuario distingue entre mayúsculas y minusculas

auth_param basic casesensitive on

 # Definimos una acl que use autenticación y damos acceso http

acl autenticacion proxy_auth REQUIRED

http_access allow autenticación

 # Cantidad de direcciones IP distintas desde la que puede acceder un usuario

acl maximo_ip_aut_usuario max_user_ip -s 1

Los usuarios los creamos desde la interfaz de administración web (Webmin) en:
Webmin --- Servidores --- Squid Servidor Proxy --- Autenticación Proxy

#Reiniciamos el squid:

[mromero@test]# **/etc/init.d/squid restart**

NOTAS:
Basic y Digest son constantes que determinan un tipo de autenticación, solo que una envía los datos encriptados y la otra no:
Basic=0: Para autentificar se envía el usuario y password sin encriptar.
Digest=1: Para autentificar se envía el usuario y password encriptados.